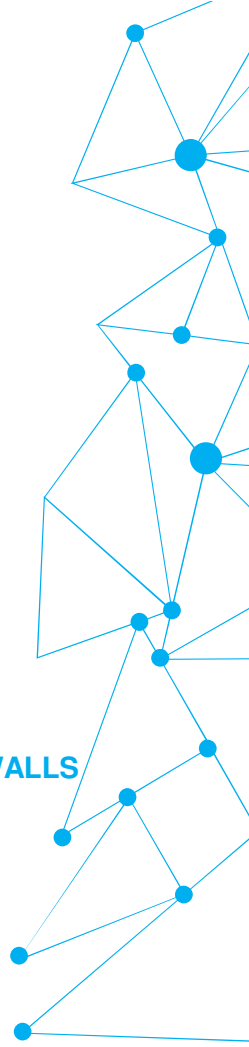




**STORMSHIELD**

SOLUTIONS UNIFIED THREAT MANAGEMENT ET NEXT-GENERATION FIREWALLS

# FORMATION ADMINISTRATEUR STORMSHIELD NETWORK SECURITY





## PRÉREQUIS DE LA FORMATION

Pouvez-vous :

- Expliquer en détails le contenu d'une table de routage ?
- Décrire un « handshake TCP » ?
- Décrire le mécanisme d'une translation d'adresses dynamique ?
- Expliquer le principe d'une redirection ICMP ?
- Expliquer le mécanisme faisant appel à un serveur DNS ?

Si vous doutez à certaines de ces questions, nous vous recommandons de réviser ces concepts techniques, par exemple, grâce au cours [Les réseaux de zéro du site Zeste de savoir](#).



<b>Cursus des formations et des certifications</b>	<b>7</b>
<b>Présentation de Stormshield et de ses produits</b>	<b>10</b>
Présentation de Stormshield	11
Stormshield Data Security	13
Stormshield Endpoint Security	15
Stormshield Network Security	17
Fonctions standards et optionnelles SNS	27
<b>Annexe</b>	<b>29</b>
Fonctions standards	30
Packs de sécurité et options logicielles	34
Options matérielles	38
<b>Prise en main du firewall</b>	<b>40</b>
Enregistrement du firewall et accès aux ressources documentaires	41
Démarrage/Arrêt/Reset	45
Connexion au firewall	48
L'interface d'administration	51
Configuration système	54
Modification du mot de passe du compte "admin"	60
Licence	62
Maintenance	65
Quiz	76
<b>Traces et supervisions</b>	<b>77</b>
Les catégories de traces	78
Configuration et visualisation des traces	81
Supervision et graphiques d'historiques	88
Notifications et rapports supplémentaires	93
Lab – Présentation de la plateforme de Lab	97
Lab 1 – Prise en main du firewall et traces	104
Quiz	106
<b>Annexe</b>	<b>107</b>
Activation du syslog	108
Stormshield Log Supervisor (SLS)	111
Notification par email	113
Rapports	118
<b>Les objets</b>	<b>122</b>
Généralités	123
Les objets réseaux	126
Lab 2 – Les objets	138
Quiz	140



<b>Configuration réseau</b>	<b>141</b>
Modes de configuration	142
Types d'interfaces	148
Lab 3 – Configuration réseau : interfaces	163
Routage système	165
Routage avancé	170
Ordonnancement des types de routage	183
Lab 3 – Configuration réseau : routage	187
Quiz	189
<b>Annexe</b>	<b>190</b>
Interfaces Modem	191
Interfaces Wifi	194
DNS dynamique	200
DHCP	204
Routage multicast statique	209
Proxy cache DNS	212
Routage statique avec Bird	215
Routage dynamique avec Bird	218
<b>Translation d'adresses</b>	<b>222</b>
Généralités	223
Translation dynamique	225
Translation statique par port	228
Translation statique	231
Menu « NAT »	236
Ordre d'application des règles de NAT	247
Lab 4 – Translation d'adresses	251
Quiz	253
<b>Annexe</b>	<b>255</b>
Configurations avancées	256
<b>Filtrage</b>	<b>264</b>
Généralités	265
La notion de « stateful »	267
L'ordonnancement des règles de filtrage et de translation	269
Menus « filtrage »	271
L'analyseur de cohérence et de conformité	288
Lab 5 – Filtrage	292
Quiz	295
<b>Annexe</b>	<b>297</b>
Configurations avancées	298



<b>Protection applicative</b>	<b>303</b>
Activation du mode Proxy	304
Proxy HTTP	307
Proxy HTTPS	320
Analyse antivirus	327
Prévention d'intrusion et inspection de sécurité	332
Lab 6 – Filtrage de contenu (HTTP et HTTPS)	338
Quiz	340
<b>Annexe</b>	<b>342</b>
Breach Fighter	343
Filtrage SMTP et antispam	346
Réputation des machines	354
<b>Utilisateurs &amp; authentification</b>	<b>360</b>
Introduction	361
Liaison à un annuaire	363
Gestion des utilisateurs	373
Les méthodes d'authentification	377
La politique d'authentification	381
Le portail captif	385
Règles de filtrage pour l'authentification	399
Définir de nouveaux administrateurs	403
Lab 7 – Authentification	408
Quiz	410
<b>Annexe</b>	<b>411</b>
Méthode guest	412
<b>Virtual Private Network</b>	<b>416</b>
Les différents réseaux privés virtuels	417
VPN IPsec – Concepts et généralités	419
VPN IPsec – Configuration d'un tunnel site-à-site	425
VPN IPSec – Configuration de tunnels site-à-site multiples	439
VPN IPsec – Virtual Tunneling Interface	446
Lab 8 – VPN IPsec (site à site)	457
Quiz	459
<b>Annexe</b>	<b>461</b>
Point-to-Point Tunneling Protocol	462
VPN IPsec - Correspondant dynamique	466
<b>VPN SSL</b>	<b>477</b>
Concepts et généralités	478
Configuration d'un tunnel	485
Lab 9 – VPN SSL	499
Quiz	502



<b>Annexe - Diagnostic</b>	<b>503</b>
Introduction	504
Avant la création de ticket	506
Éléments primordiaux	509
Éléments complémentaires	512
Accès au firewall	516
<b>Labs - Corrigés</b>	<b>519</b>
Lab 1 – Prise en main du Firewall	520
Lab 2 – Les objets	521
Lab 3 – Configuration réseau	522
Lab 4 – Translation d’adresses	523
Lab 5 – Filtrage	524
Lab 6 – Filtrage de contenu (HTTP et HTTPS)	525
Lab 7 – Authentification	527
Lab 8 – VPN IPsec (site à site)	528
Lab 9 – VPN SSL	530
<b>Quiz - Corrigés</b>	<b>533</b>
<b>Advanced Labs</b>	<b>534</b>
LAB 1 – Mise en place de l’infrastructure	536
LAB 2 – Rapports embarqués	539
LAB 3 – Fonctionnalités DHCP	539
LAB 4 – VLAN et objets routeurs	540
LAB 5 – Filtrage applicatif SMTP avancé	542
LAB 6 – Authentification et comptes temporaires	544
LAB 7 – Authentification et parrainage	545
LAB 8 – VPN SSL et VPN IPsec site-à-site	546
LAB 9 – Routage par VTI	547
<b>Advanced Labs - Corrigés</b>	<b>550</b>

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.



STORMSHIELD

# CURSUS DES FORMATIONS ET CERTIFICATION

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X

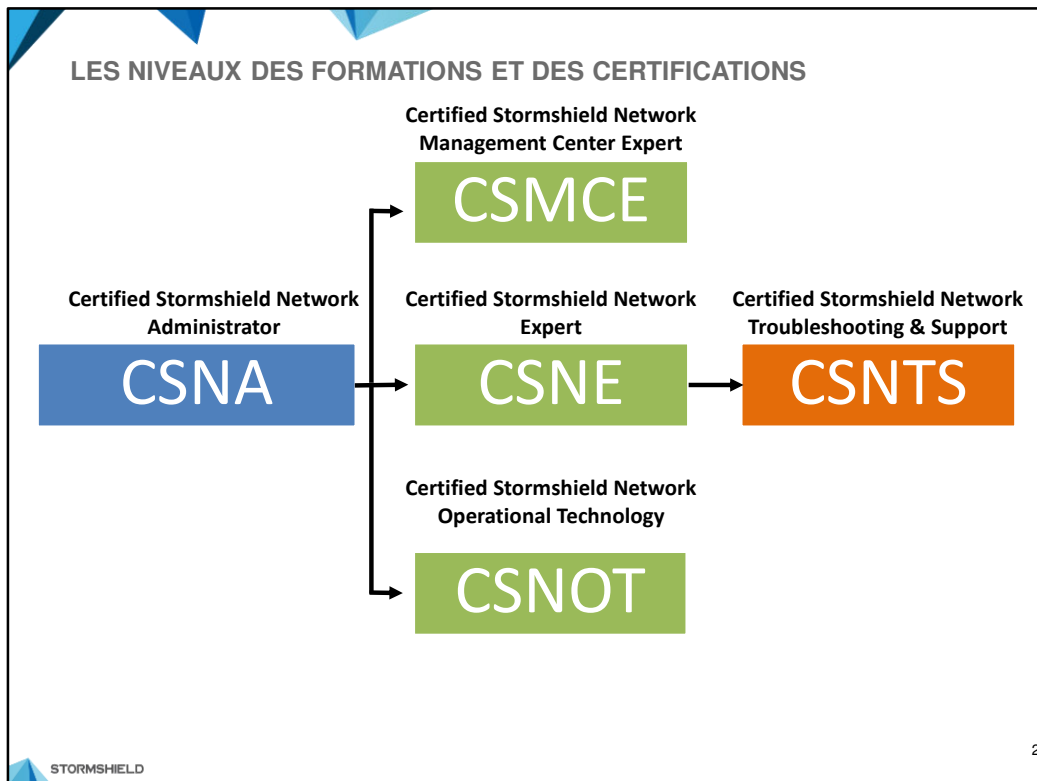


1

## Programme de la formation

- Cours des formations et certification
  - Présentation de l'entreprise et des produits
  - Prise en main du firewall
  - Traces et supervision
  - Les objets
  - Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL

Le contenu de ce module n'est pas évalué dans les examens de certification Stormshield.



Les formations SNS comprennent 5 cursus certifiants :

- **CSNA (Certified Stormshield Network Administrator)** : L'objectif de cette formation est la présentation des gammes de produits Stormshield Network et leurs fonctionnalités principales configurables depuis l'interface d'administration Web. Elle se déroule en 3 jours.
- **CSNE (Certified Stormshield Network Expert)** : Cette formation présente les fonctionnalités avancées des firewalls Stormshield Network configurables également depuis l'interface d'administration Web. Tout comme la CSNA, sa durée est de 3 jours.
- **CSNTS (Certified Stormshield Network Troubleshooting & Support)** : La configuration et le monitoring en mode console seront privilégiés durant cette formation de 4 jours. Cela permet aux participants d'avoir une maîtrise totale du produit afin d'assurer le débogage des configurations et des fonctionnalités.
- **CSMCE (Certified Stormshield Management Center Expert)** : Cette formation permet d'exploiter toutes les fonctionnalités de l'outil SMC dédié à l'administration centralisée Stormshield Network. Sa durée est de 2 jours.
- **CSNOT (Certified Stormshield Network Operational Technology)** : Cette journée de formation permet d'approfondir par la pratique le filtrage des protocoles industriels.

Toutes les formations sont constituées d'une partie théorique (cours) présentant le fonctionnement et la manière de configurer les fonctionnalités et d'une partie pratique (Labs), pour les mettre en œuvre en situation réelle.

## CERTIFICATION CSNA



Accessible sur <https://institute.stormshield.eu/>



Documentation et VM **autorisées** durant l'examen



**70 questions** à choix multiples



**1h30** pour l'examen en **français**, **1h40** pour l'examen en **anglais**



Résultat envoyé sous **24h ouvrées**



**70% de bonnes réponses** nécessaires pour valider la certification

**X2**

**2<sup>ème</sup> passage** ouvert automatiquement **en cas d'échec** à la première tentative

Le stagiaire a droit à deux passages d'examen disponibles sur son compte <https://institute.stormshield.eu/>. L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de trois semaines. En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine supplémentaire.

Le candidat devra obtenir 70% de réponses correctes pour être certifié.

Un examen de Demo 'Demo Exam' est accessible en permanence sur <https://institute.stormshield.eu> pour découvrir l'interface graphique utilisée pour le passage d'examen.

Les certifications Stormshield sont valables 3 ans. Durant cette période, il est possible de suivre une des formations Stormshield suivantes: CSNE, CSNOT, CSMCE. L'obtention de la certification Expert CSNE renouvelle automatiquement la certification CSNA.

Au bout de 3 ans, il est également possible de renouveler son dernier niveau de certification à distance en passant commande d'un Kit de recertification à étudier en autonomie.



STORMSHIELD

# PRÉSENTATION DE STORMSHIELD ET DE SES PRODUITS

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

## Programme de la formation

- ✓ Coursus des formations et certifications
- ➔ Présentation de Stormshield et de ses produits
  - Prise en main du firewall
  - Traces et supervision
  - Les objets
  - Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL

Le contenu de ce module n'est pas évalué dans les examens de certification Stormshield.

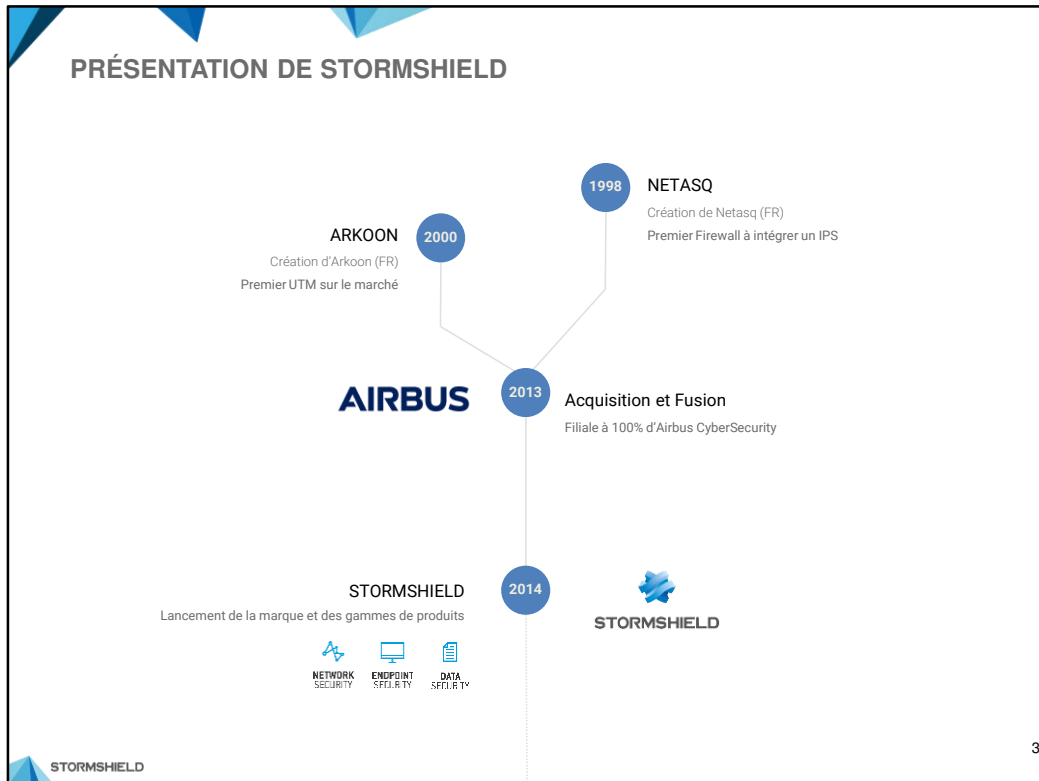


## Présentation de Stormshield

- Stormshield Data Security
- Stormshield Endpoint Security
- Stormshield Network Security
- Fonctions standards et optionnelles SNS

STORMSHIELD

Présentation de Stormshield  
et de ses produits



Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin de s'appuyer sur des partenaires de confiance pour accompagner leur transformation numérique et assurer la cybersécurité de leurs infrastructures, de leurs utilisateurs et de leurs données. Les technologies Stormshield, certifiées au plus haut niveau européen (EU Restreint, NATO/OTAN Restreint, Critères Communs EAL3+/EAL4+, qualifications et visas ANSSI, approuvées et qualifiées par OC-CCN, Organismo de Certificación | Centro Criptológico Nacional, Espagne), répondent aux enjeux de l'IT et de l'OT afin de protéger vos activités. Nos solutions de sécurité vous redonnent la liberté d'entreprendre en toute sérénité.

Pour en savoir plus : [www.stormshield.com](http://www.stormshield.com)

Notre expertise se décline en trois gammes de produits complémentaires pour une sécurité sans failles :

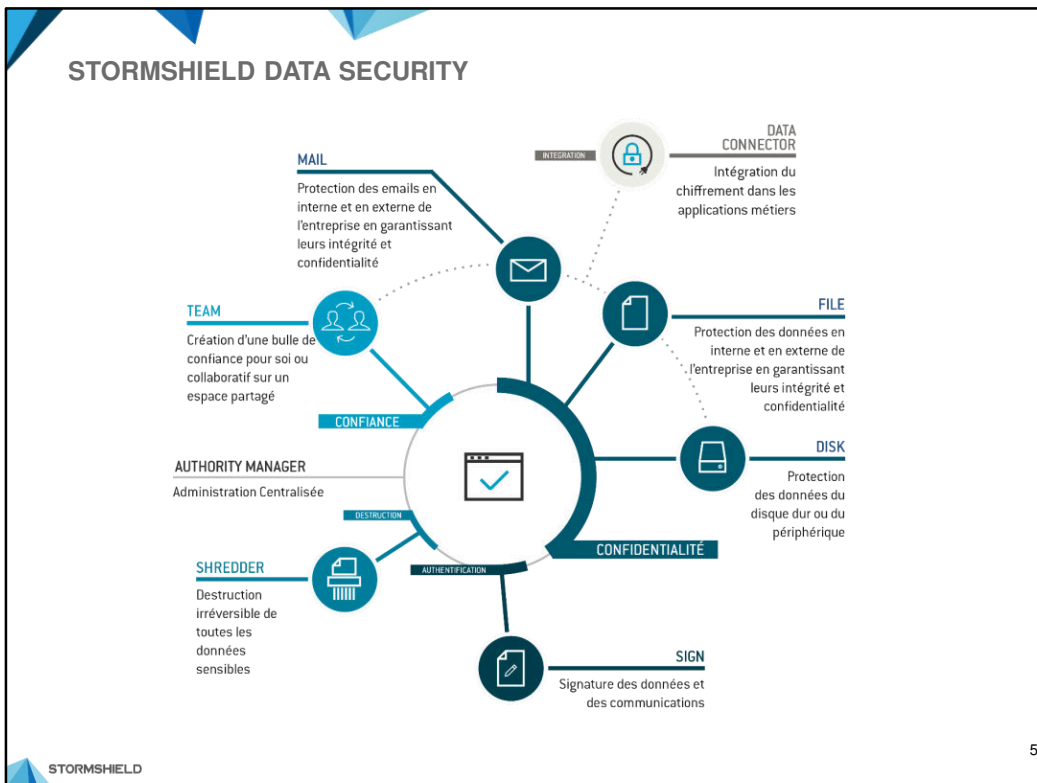
- Protection des réseaux informatiques et industriels - Stormshield Network Security
- Protection des postes et serveurs - Stormshield Endpoint Security
- Protection des données - Stormshield Data Security



- Présentation de Stormshield
- **Stormshield Data Security**
- Stormshield Endpoint Security
- Stormshield Network Security
- Fonctions standards et optionnelles SNS

Présentation de Stormshield  
et de ses produits

STORMSHIELD



**Stormshield Data Security Enterprise** permet aux utilisateurs de maîtriser leurs données en environnement Microsoft selon les possibilités suivantes :

- Chiffrement transparent des répertoires locaux (périphériques USB compris) ou partagés (**Disk, Team**),
- Intégration aux clients de messagerie (Microsoft Outlook et Lotus Notes) afin de chiffrer et/ou signer les courriels (**Mail**),
- Sécurisation des données collaboratives (**Team**),
- Signature de tout type de fichiers pour faciliter la dématérialisation des procédures administratives et commerciales (**Sign**),
- Effacement sécurisé des fichiers et dossiers (**Shredder**),
- Administration par commandelettes Powershell ou API métiers (**Connector**),
- Administration centralisée (**Authority Manager**).

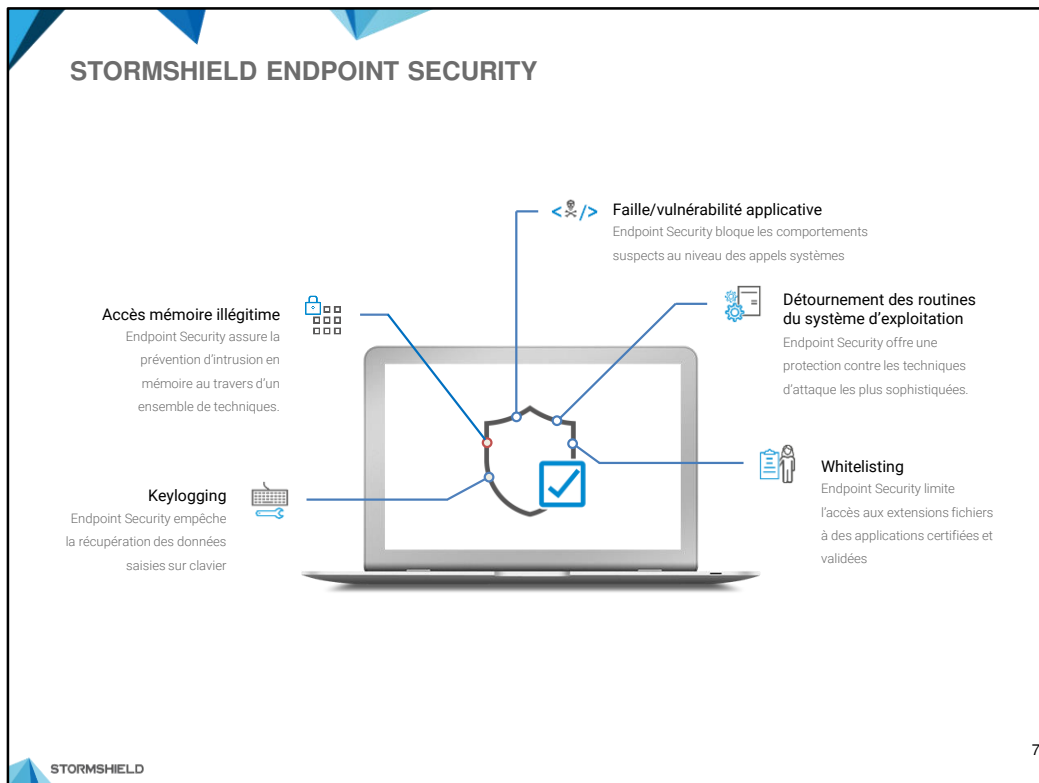
Stormshield Data Security Enterprise version 9.1.2 est [certifié EAL3+](#), pour sa fonction de chiffrement transparent de fichiers (septembre 2016).



- Présentation de Stormshield
- Stormshield Data Security
- ➔ **Stormshield Endpoint Security**
- Stormshield Network Security
- Fonctions standards et optionnelles SNS

Présentation de Stormshield  
et de ses produits

STORMSHIELD



Face aux attaques ciblées ou sophistiquées, Stormshield Endpoint Security Evolution surveille et bloque en temps réel les comportements suspects des programmes – tels que les accès mémoire, enregistreurs de frappe ou exploitation des vulnérabilités – y compris l'utilisation détournée de logiciels légitimes. Son fonctionnement au plus près du système d'exploitation lui confère une efficacité unique contre les attaques de type « Zero-day » ou les ransomwares.

Sans mise à jour de bases de signatures, Stormshield Endpoint Security Evolution maintient des conditions de sécurité optimale pour les environnements soumis aux plus fortes contraintes, comme les systèmes industriels ou les terminaux de points de vente. Cette protection en temps réel, sans impact sur le poste, est entièrement transparente et autonome. Elle ne nécessite aucune connexion vers un système externe. De plus, en cas d'attaque, l'administrateur est immédiatement informé via la console centralisée. Sans base de signatures à maintenir, cette solution est entièrement adaptée aux systèmes en fin de vie ou hors support.

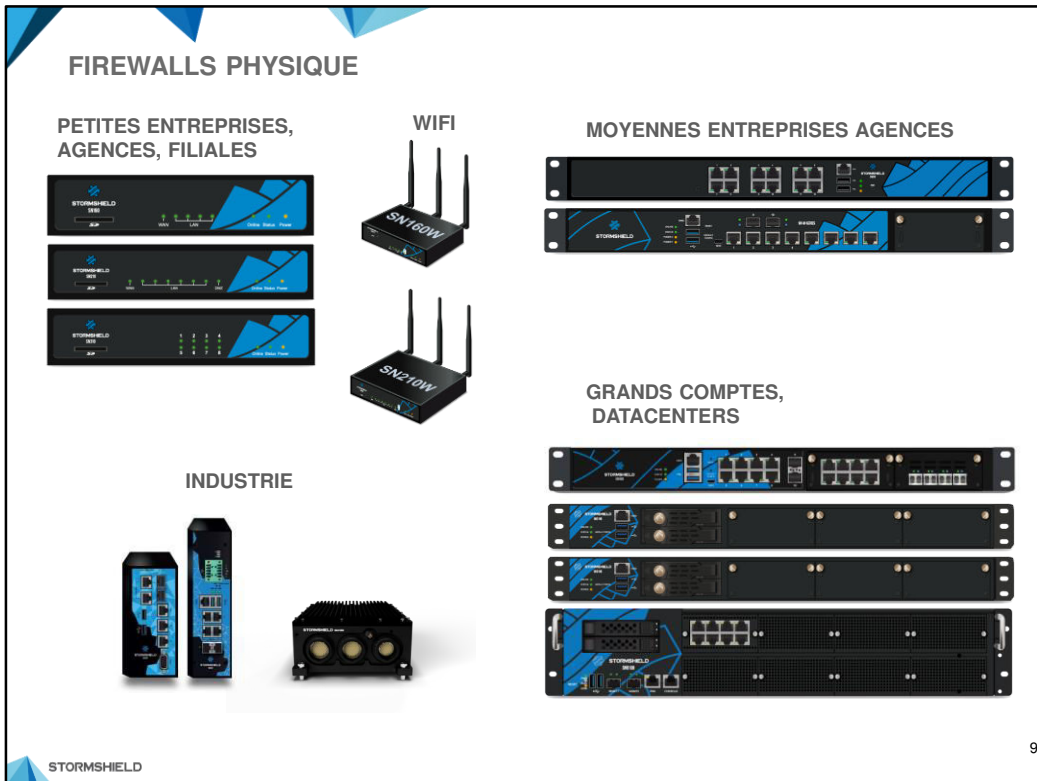
Stormshield Endpoint Security version 7.2.6 est [certifié EAL3+](#), pour son module fonctionnel de chiffrement de surface.



- Présentation de Stormshield
- Stormshield Data Security
- Stormshield Endpoint Security
- **Stormshield Network Security**
- Fonctions standards et optionnelles SNS

Présentation de Stormshield  
et de ses produits

STORMSHIELD



La gamme des produits Stormshield Network Security est composée principalement de deux grandes catégories illustrées dans la figure ci-dessus : les appliances physiques (gamme SN) et les appliances virtuelles (gamme EVA).

- Les produits de la gamme SN sont organisés en quatre familles :
  - SN160, SN210 et SN310 pour les petites entreprises, les agences et les filiales. SN160W et SN210W intègrent une carte WIFI pour assurer des connexions sans fil sécurisées.
  - SNi20, SNi40, SNxr1200 adaptés aux environnements industriels.
  - SN510, SN-M-Series-720 et SN-M-Series-920 pour les organisations moyennes.
  - SN2100, SN3010 et SN6100 pour les grandes organisations et les datacenters.

La technologie de tous les produits Stormshield Network est basée sur un moteur IPS (Intrusion Prevention System) propriétaire intégré dans un noyau FreeBSD.

- Stormshield Network Security version 3.7.9 est :
  - certifié EAL3+ pour les fonctions de filtrage de la suite logicielle Stormshield Firewall embarquée dans les boîtiers.



Les appliances virtuelles sont compatibles avec les hyperviseurs suivants :

- VMware ESXi - version v6.5 ou 6.7 et 7.0
- Citrix XenServer - version v7.6 ou supérieure,
- Microsoft Hyper-V - Windows Server 2012 R2, 2019 et 2022
- Linux KVM - Red Hat Enterprise Linux 8.4

Les appliances virtuelles pour Cloud sont disponibles au niveau des fournisseurs de services 3D Outscale, Amazon AWS (Amazon web services) et Microsoft Azure, ce qui permettra de protéger vos serveurs hébergés chez ce fournisseur.

De plus, Stormshield propose l'offre Stormshield Pay As You Go. Elle est destinée aux fournisseurs de Cloud privé proposant des services hébergés et/ou d'accès à Internet, en SaaS ou en IaaS. En les déployant dans leur infrastructure virtuelle, ils peuvent proposer à leurs clients un service de sécurité réseau avec une facturation mensuelle basée sur le nombre et la taille des firewalls virtuels utilisés.

## PETITES ENTREPRISES, AGENCES ET FILIALES



SN160



SN210



SN310

	SN160(W)	SN210(W)	SN310
Nombre d'interfaces 10/100/1000	1 + 4 ports (switch)	2 + 6 ports (switch)	8
Débit IPS (Gbps)	1	1.6	2.4
Débit VPN IPsec (Mbps AES)	200	350	600
Connexions simultanées	150 000	200 000	300 000
Slot pour carte SD	Oui	Oui	Oui
Disque Dur	-	-	-

## Cas d'usages

- **SN160(W)** : Site distant connecté en VPN, sécurité unifiée pour petite structure. Le SN160W permet la création de deux réseaux Wifi distincts.
- **SN210(W)** : Site distant connecté en VPN, sécurité unifiée pour petite structure avec DMZ ou double accès WAN. Le SN210 permet de créer 2 zones de confiance sur le réseau interne ou de mettre en place de la redondance de liens d'accès Internet. Le SN210W permet également de créer deux réseaux Wifi distincts.
- **SN310** : Sécurité unifiée pour petites structures avec besoin de continuité (haute disponibilité) et de zones de sécurité. Le SN310 offre 8 ports physiques et supporte la fonction Haute Disponibilité.

Pour cette gamme de boîtier, par défaut, le stockage des logs est limité. Il est possible de l'étendre via l'utilisation d'une carte SD.

## MOYENNES ENTREPRISES ET GROSSES AGENCES



	SN510	SNM-SERIES-720	M-SERIES-SN920
Nombre d'interfaces 10/100/1000	12	-	-
Nombre d'interfaces cuivre 2.5Gb	-	8-16	8-16
Nombre d'interfaces cuivre 10Gb	-	0-4	0-4
Nombre d'interfaces fibre 1Gb	-	0-8	0-10
Nombre d'interfaces fibre 10Gb	-	2-6	2-6
Débit IPS (Gbps)	3,3	10	16
Débit VPN IPSec (Gbps AES)	1	4	6
Connexions simultanées	500 000	1 000 000	1 500 000
Disque Dur	> 200 Go	> 200 Go SSD	> 200 Go SSD
Alimentation redondante	-	Oui	Oui

## Cas d'usages

- **SN510** : Organisations de taille moyenne avec un besoin d'archivage local de logs. Le SN510 permet le stockage local et l'archivage de logs sur disque dur.
- **SN-M-SERIES-720** : Organisations de taille moyenne avec un besoin de modularité réseau alliant la densité de ports (jusqu'à 16 ports cuivre) et la fibre 10 Gigabits Ethernet.
- **SN-M-SERIES-920** : Organisations de taille moyenne avec un besoin de flexibilité pour monter en performance.

Les SN-M-Series-720 et SN-M-Series-920 disposent d'un boîtier commun et d'une plateforme logicielle évolutive, permettant par exemple de passer de 300 à 500 utilisateurs par un simple achat de licence.

## GRAND-COMPTES ET DATACENTERS



	SN1100	SN2100	SN3100	SN6100
Nombre d'interfaces 10/100/1000	8/24	2-26	2-26	8-64
Nombre d'interfaces fibre 1/10/40Gb	0-16/2-10	0-24/0-12/0-6	0-24/0-12/0-6	0-64/0-34/0-16
Débit IPS (Gbps)	18	35	55	68
Débit VPN IPSec (Gbps AES)	7,5	10	10	20,5
Connexions simultanées	1 800 000	2 500 000	5 000 000	20 000 000
Disque Dur	512 Go SSD	256 Go SSD (option raid 1)	256 Go SSD (raid 1)	512 Go SSD (raid 1)
Alimentation redondante	(option)	(option)	Oui	oui

## Cas d'usages

- **SN1100** : Organisations et entreprises multisites avec infrastructures complexe. Modularité, performances et sécurité sont les maîtres-mots de ce produit, qui répond aux besoins de protection réseau.
- **SN2100** : Organisations ayant des besoins de performance et d'évolutivité. Le SN2100 offre une grande modularité grâce à des modules d'extension réseau optionnels.
- **SN3100** : Organisations ayant des architectures critiques. Le SN3100 intègre des composants matériels redondants pour une meilleure disponibilité : disques durs SSD en RAID1 et alimentation redondante. Il supporte les mêmes configurations réseau que le SN2100.
- **SN6100** : Grandes entreprises et datacenters. Le SN6100 propose une modularité réseau inégalée sur le marché : il peut supporter jusqu'à 64 ports cuivre ou fibre. Il offre des performances Firewall jusqu'à 170Gbps et la supervision des composants matériels via IPMI.

## INDUSTRIE



	SNi20	SNi40	SNxr1200
Nombre d'interfaces 10/100/1000	2-4	5	5 via connecteurs micro MIL-DTL-38999
Nombre d'interfaces fibre 1G SFP	0-2	0-2	-
Débit IPS (Gbps)	1,6	2,9	1,6
Débit VPN IPsec (Gbps AES)	0,6	1,1	0,6
Connexions simultanées	500 000	500 000	500 000
Disque Dur	Carte SD	32 Go SSD	128 Go SSD
Alimentation redondante	oui	oui	non

STORMSHIELD

14

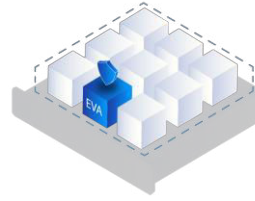
## Cas d'usages SNi20 et SNi40

- Besoin d'utilisation de protocoles industriels (Profinet, Modbus, S7 200-300-400, OPC UA).
- Bypass matériel : la continuité de service dans les milieux industriels est critique. Le SNi20 et le SNi40 intègrent un bypass matériel sur certains ports permettant de laisser passer le trafic réseau en cas de coupure électrique ou de défaillance du boîtier.
- Besoin de résistance aux agressions extérieures (chocs, interférences électromagnétiques, poussières, températures extrêmes), le niveau de protection fourni par le boîtier (IP code) est IP30.
- Format hardware de type rail DIN pour la protection des PLC (Programmable Logic Controller).

## • Cas d'usages SNxr1200

- Résistance à des conditions extrêmes (températures de -40° à +55°C, fort taux d'humidité, altitude dépassant 15 000 mètres) permettant d'être embarqué dans tous types de véhicules (terrestres, aériens, maritimes) intervenant dans des environnements critiques.
- Respect un certain nombre de standards militaires.

## APPLIANCES VIRTUELLES

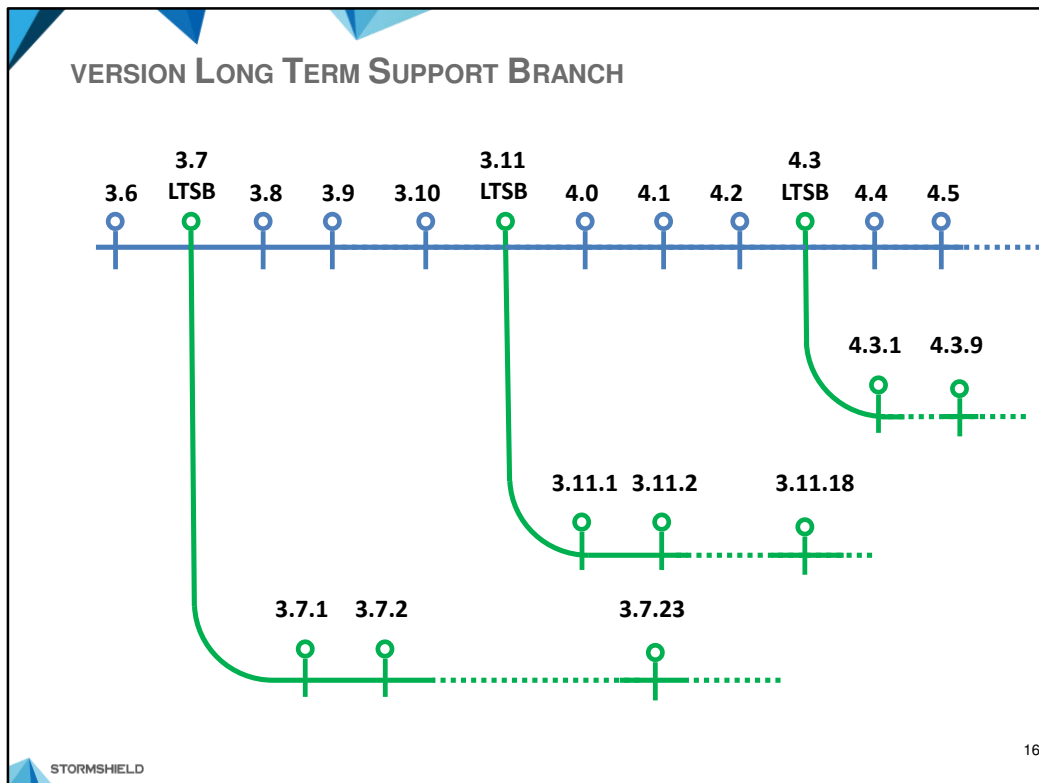


	EVA1	EVA2	EVA3	EVA4	EVAU
Nombre de connexions simultanées	200 000	400 000	1 000 000	1 500 000	5 000 000
Nombre d'interfaces VLANs 802.1q	128	256	512	512	1024
Nombre de tunnels	200	500	750	5 000	10 000
Clients VPN SSL Simultanés	100	150	200	250	500
Nombre max de vCPU/mémoire (Go)	1 / 2	2 / 3	4 / 6	4 / 8	16 / 64

Avec la gamme Elastic Virtual Appliance de Stormshield, les entreprises bénéficient d'une gamme complète de fonctions de sécurité sans coût initial, par simple abonnement aux services, qui inclut les mises à jour du système et des différentes protections.

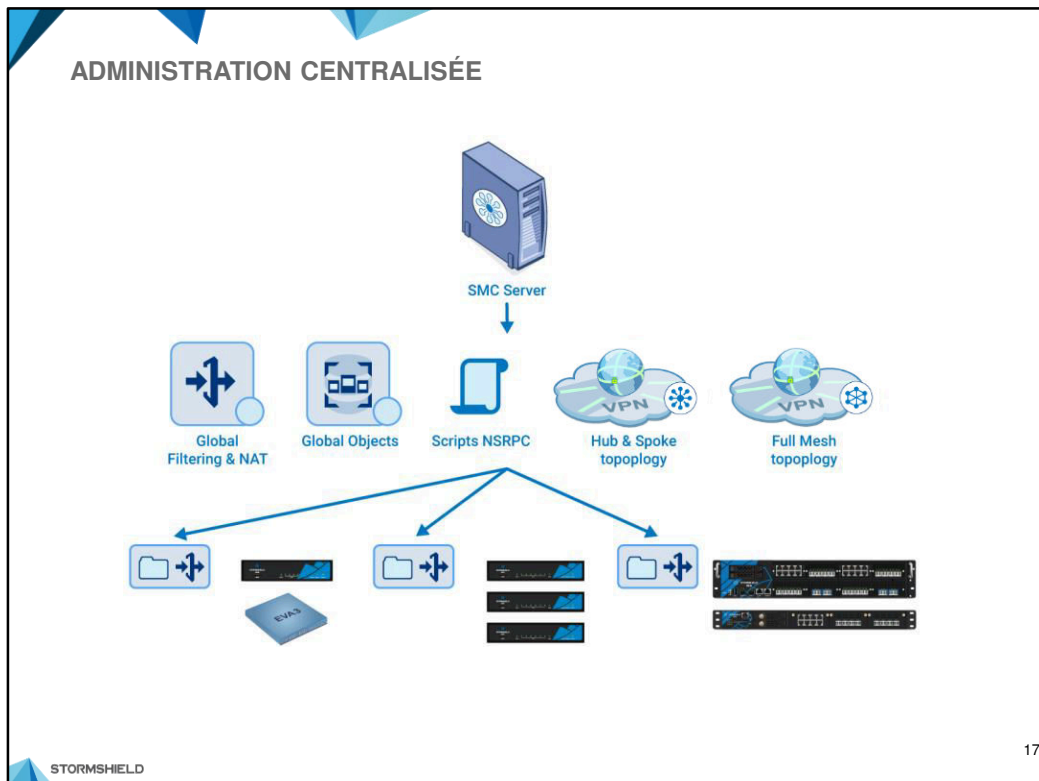
Les performances de ces produits s'adaptent automatiquement aux ressources allouées sur l'hyperviseur. Vous pouvez ainsi contrôler finement vos coûts d'exploitation en fonction des besoins d'évolutions de votre infrastructure.

Stormshield Elastic Virtual Appliance peut également permettre de protéger des serveurs virtuels et des réseaux virtuels hébergés dans un Cloud Amazon Web Services ou Microsoft Azure. La mise en œuvre est simplifiée via l'intégration des firewalls SN dans le Marketplace des fournisseurs de services Cloud.



Les versions majeures ou mineures disposant du label LTSB sont considérées comme des versions stables à long terme. Leur prise en charge est assurée pendant 12 mois minimum. Ces versions sont recommandées pour les clients qui accordent plus d'importance à la stabilité qu'aux nouvelles fonctionnalités et optimisations.

Le cycle de vie des produits SNS est détaillé dans un document dédié disponible dans l'espace client <https://mystormshield.eu/>,



### Stormshield Management Center

SMC, produit sous licence, permet d'administrer un parc complet de Firewalls Stormshield.

Les Firewalls physiques et/ou virtuels à gérer vont être rattachés au serveur SMC à l'aide d'un package de rattachement, qu'ils soient en production ou en configuration d'usine.

Pour simplifier l'administration du parc, les Firewalls seront classés dans des dossiers, l'ensemble des éléments déployables par SMC (et détaillés ci-après), pouvant concerner un Firewall unique, un dossier de Firewalls, ou le parc complet.

Outre l'accès direct par le serveur SMC aux traces et rapports d'activités des Firewalls connectés, l'utilisation de SMC permet :

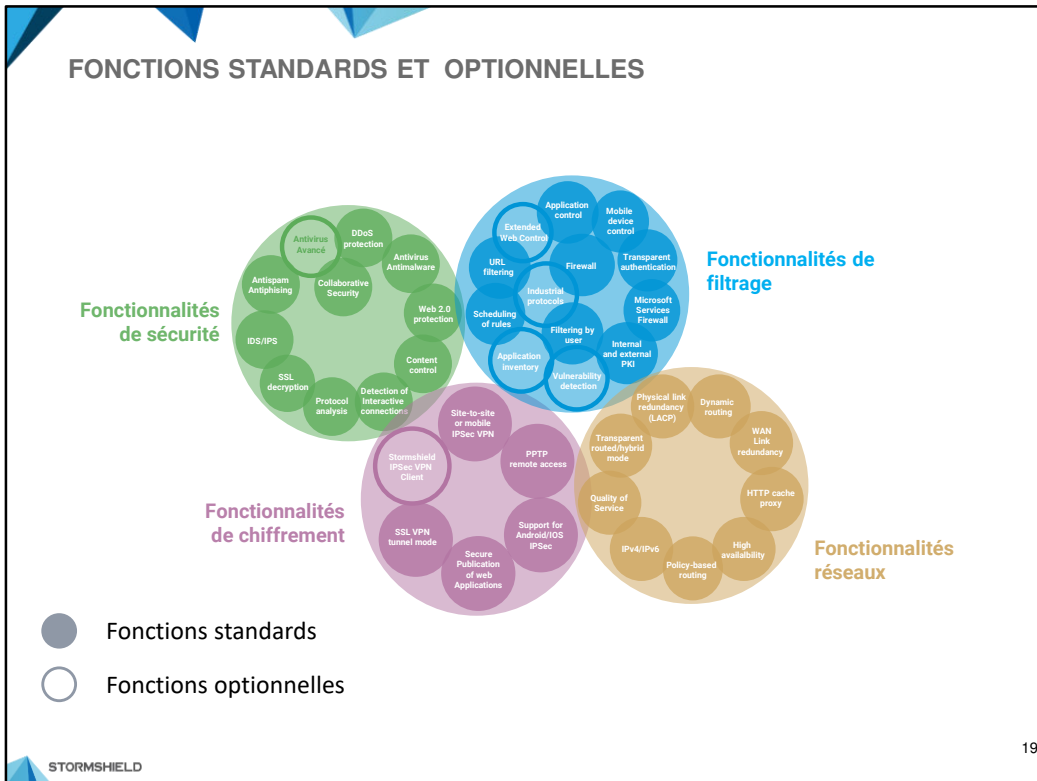
- Le déploiement d'objets globaux.
- Le déploiement de règles de filtrage et de translation.
- Le déploiement de topologies VPN IPsec.
- Le déploiement de scripts NSRPC
- Le déploiement de modèles basés sur des variables globales et/ou locales
- La gestion de certificats (déploiement et renouvellement)
- Surveillance des firewalls (ressources, licences, ...)



- Présentation de Stormshield
- Stormshield Data Security
- Stormshield Endpoint Security
- Stormshield Network Security
- ➔ **Fonctions standards et optionnelles  
SNS**

Présentation de Stormshield  
et de ses produits

STORMSHIELD



Vous trouverez sur le site web [Stormshield.com](http://Stormshield.com) l'ensemble des fiches produits et des fonctionnalités proposées pour la gamme SNS.

Vous trouverez sur le site [documentation.stormshield.eu](http://documentation.stormshield.eu) les guides d'installation des différents produits.



STORMSHIELD

# ANNEXE – PRÉSENTATION DE STORMSHIELD ET DE SES PRODUITS

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



## Fonctions standards

- Packs de sécurité et options logicielles
- Options matérielles

STORMSHIELD

Présentation de Stormshield  
et de ses produits

## LES FONCTIONS STANDARDS

Fonctions - Produits	Gamme Stormshield Network					Appliances virtuelles
	SN160(w)	SN210(w)	SN310, SN510, SN720, SN920, SN1100	SN2100,SN3100, SN6100	SNi20 SNi40 SNxr1200	
<b>Moteur IPS</b>						
<ul style="list-style-type: none"> <li>Analyse protocolaire:                             <ul style="list-style-type: none"> <li>IP, ICMP, TCP, UDP, HTTP, FTP, SIP, RTSP, etc</li> <li>Industriel (SCADA) : MODBUS, S7</li> </ul> </li> </ul>	Oui	Oui	Oui	Oui	Oui	Oui
<ul style="list-style-type: none"> <li>Signatures contextuelles</li> </ul>	Oui	Oui	Oui	Oui	Oui	Oui
<b>Antispam</b>						
<ul style="list-style-type: none"> <li>Analyse heuristique</li> </ul>	Oui	Oui	Oui	Oui	Oui	Oui
<ul style="list-style-type: none"> <li>Analyse par réputation (DNS RBL)</li> </ul>	Oui	Oui	Oui	Oui	Oui	Oui
<b>Antivirus Standard</b>	-	Oui	Oui	Oui	Oui	Oui
<b>Filtrage URL Stormshield</b>	-	Oui	Oui	Oui	Oui	Oui
<b>Système</b>						
<ul style="list-style-type: none"> <li>RAID 1</li> </ul>	-	-	-	Oui	-	-
<ul style="list-style-type: none"> <li>Double partition système</li> </ul>	Oui	Oui	Oui	Oui	Oui	-
<ul style="list-style-type: none"> <li>Haute disponibilité</li> </ul>	-	-	Oui	Oui	Oui	Oui

Les produits Stormshield Network Security intègrent des fonctionnalités de base :

- **Analyse protocolaire IPS:** Regroupe l'ensemble des contrôles effectués sur les protocoles réseaux (IP, TCP, UDP...) et applicatifs (HTTP, FTP...) afin de s'assurer de leur conformité. Depuis la version 2.3, cette analyse permet de contrôler également deux protocoles industriels (SCADA) : MODBUS et S7.
- **Signatures contextuelles IPS :** Une base de signatures d'attaque utilisée en complément de l'analyse protocolaire pour détecter rapidement les attaques connues.
- **Antispam :**
  - **Analyse Heuristique :** Permet la qualification d'un email en SPAM en se basant sur un algorithme particulier qui détermine le degré de légitimité des emails.
  - **Analyse par réputation (DNS RBL : Real time Blackhole List) :** Elle utilise les serveurs RBL qui permettent de savoir si un email est un SPAM en se basant sur la réputation de son émetteur. La liste des serveurs RBL est mise à jour continuellement.
- **Antivirus standard :** Moteur antiviral open source permettant la détection des virus, des chevaux de Troie et des malwares. Sa bibliothèque fournit plusieurs mécanismes pour la détection du format de fichier et des outils pour la prise en charge des archives et des fichiers compressés.
- **Filtrage URL Stormshield :** Une base d'URLs propriétaire, utilisée pour le filtrage web. Les URLs sont classées en 16 catégories.



- **Système :**
  - **RAID 1 (Redundant Array of Independent Disks):** Assure la fiabilité du stockage en disposant une copie conforme des données sur deux disques durs indépendants.
  - **Double partition système (principale et secours) :** Permet le stockage de deux versions du système.
  - **Haute disponibilité :** Assure la continuité de services en utilisant deux firewalls : un en mode actif et l'autre en mode passif. Dans le cas où le firewall actif n'est plus fonctionnel, le firewall passif bascule en mode actif pour assurer la transmission et la protection des données. Cette fonctionnalité monopolise une interface réseau sur chaque firewall.

## LES FONCTIONS STANDARDS

Services - Produits	Gamme Stormshield Network			Appliances virtuelles
	SN160(w)	SN210(w), SN310	SNi20, SNi40, SN510, SN720, SN920, SN1100, SNxr1200, SN2100, SN3100, SN6100	
• Routage Dynamique, Routage par politique	Oui	Oui	Oui	Oui
• Client DHCP	Oui	Oui	Oui	Oui
• Serveur/Relai DHCP	Oui	Oui	Oui	Oui
• Client DynDNS	Oui	Oui	Oui	Oui
• Client NTP	Oui	Oui	Oui	Oui
• Agent SNMP	Oui	Oui	Oui	Oui
• Cache DNS	Oui	Oui	Oui	Oui
• Syslog	Oui	Oui	Oui	Oui
• Tunnels : VPN IPSEC, VPN SSL, GRE, GRE-TAP, VTI	Oui	Oui	Oui	Oui
• RSTP/MSTP	-	-	Oui	Oui
• LACP	-	-	Oui	-
• PKI and CA	Oui	Oui	Oui	Oui
• Logs en Local	Option	Option	Oui	Oui

STORMSHIELD

5

Le tableau ci-dessus présente les services disponibles dans les produits Stormshield Network Security. Il est important de noter que le stockage local des fichiers journaux (logs) est natif sur l'ensemble des produits excepté pour les SN160(w), SN210(w) et SN310 parce qu'ils sont dépourvus de disque dur. Cependant, l'option de licence « Stockage externe », activée par défaut depuis la v4 sur ces modèles, permet le stockage local des logs sur une carte SD amovible.



- Fonctions standards
- **Packs de sécurité et options logicielles**
- Options matérielles

Présentation de Stormshield  
et de ses produits

STORMSHIELD

## LES PACKS SÉCURITÉ

		Best-of-Breed Unified Security	IPS & Application Control
Connectivity	Standard Unified Security		
Remote Office Security Pack	UTM Security Pack	Premium UTM Security Pack	Enterprise Security Pack
SN160(W), SN210(W)	SN160(W), SN210(W), SN310, SN510, SN710, SN910, SN2100, SN3100	All products	SN2100, SN3100, SN6100
Features	Features	Features	Features
✓ NGFW + IPS + VPN (IPSec & SSL) * Vulnerability Manager* * Antivirus* * URL Filtering* * Antispam ✓ SD card * Breach Fighter* * Industrial Protocol*	✓ NGFW + IPS + VPN (IPSec & SSL) * Vulnerability Manager* ✓ Standard Antivirus ✓ Embedded URL Filtering 15 categories ✓ Antispam ✓ SD card * Breach Fighter* * Industrial Protocol*	✓ NGFW + IPS + VPN (IPSec & SSL) ✓ Vulnerability Manager ✓ Advanced Antivirus ✓ Extended URL Filtering 65 categories ✓ Antispam ✓ SD card * Breach Fighter* * Industrial Protocol*	✓ NGFW + IPS + VPN (IPSec & SSL) ✓ Vulnerability Manager ✓ Antivirus* ✓ URL Filtering* * Antispam ✓ SD card * Breach Fighter* * Industrial Protocol*

STORMSHIELD

7

Certaines fonctionnalités supplémentaires sont disponibles après souscription d'un pack de sécurité spécifique :

- **Stormshield Network Vulnerability Manager** : Il a pour but d'identifier et de remonter en temps réel les vulnérabilités et les failles des applications et des services utilisés dans les réseaux protégés. Pour cela, SNVM fonctionne en collaboration avec le moteur de prévention d'intrusion IPS tout en collectant et archivant les informations liées, notamment, au système d'exploitation, aux diverses activités ainsi qu'aux différentes versions d'applications installées. Ces dernières peuvent être des applications clientes (Firefox) ou des services réseaux (Apache, Bind, OpenSSH...). NVM remonte les vulnérabilités détectées en identifiant les machines impliquées et propose aussi les correctifs possibles.
- **Antivirus Avancé** : Développé et intégré par un éditeur de renom, cet antivirus représente l'une des meilleures solutions antivirales disponibles actuellement sur le marché. Son moteur analyse en temps réel les mails entrants et sortants, le trafic Web ainsi que les fichiers, afin de détecter et éliminer toutes les intrusions virales au niveau des réseaux protégés. Pour assurer une détection optimale, la base des signatures virales est mise à jour continuellement. Les points forts de cet antivirus sont son support de nombreux formats d'archive, performance de traitement des fichiers plus élevé que l'antivirus ClamAV, performance accrue du moteur d'analyse heuristique.
- **Filtrage WEB Extended Web Control** : Elle se base sur un fournisseur de base URLs hébergé dans le cloud. La base référence des centaines de millions d'URLs classées en 65 catégories thématiques : achat, éducation, banque, etc. L'avantage majeur de cette nouvelle option est la mise à jour rapide de la base d'URLs qui n'est plus téléchargée au niveau du Firewall.
- **Stockage des logs sur la carte SD « stockage externe »** : Elle permet aux Firewalls disposant d'un slot de carte mémoire SD de stocker les logs sur cette dernière. Sur les produits SN160(w), SN210(w) et SN310, l'utilisation d'une carte SD permet d'activer la génération de tous les rapports d'activité (sans carte SD, seuls 5 rapports peuvent être utilisés).
- **Breach Fighter** : Elle permet d'effectuer dans le Cloud une analyse complémentaire à celle de l'antivirus avancé, pour bloquer des attaques élaborées, avec le soutien d'une équipe de sécurité dédiée.

## LES PACKS SÉCURITÉ

		Best-of-Breed Unified Security	IPS & Application Control
Connectivity	Standard Unified Security		
Remote Office Security Pack	UTM Security Pack	Premium UTM Security Pack	Enterprise Security Pack
SN160(w), SN210(w)	SN160(w), SN210(w), SN310, SN510, SN710, SN910, SN2100, SN3100	All products	SN2100, SN3100, SN6100
Updates	Updates	Updates	Updates
✓ Firmware	✓ Firmware	✓ Firmware	✓ Firmware
✓ IPS	✓ IPS	✓ IPS	✓ IPS
✓ Applications	✓ Applications	✓ Applications	✓ Applications
* Antivirus & Antispam™	✓ Antivirus & Antispam	✓ Antivirus & Antispam	* Antivirus & Antispam™
* URL Database™	✓ URL Database	✓ URL Database	* URL Database™
Services	Services	Services	Services
✓ Support (Certified Partner)	✓ Support (Certified Partner)	✓ Support (Certified Partner)	✓ Support (Certified Partner)
✓ Security Intelligence	✓ Security Intelligence	✓ Security Intelligence	✓ Security Intelligence

STORMSHIELD

8

Stormshield propose des packs de service de sécurité pour répondre à des usages précis. Ces packs assurent :

- Une mise à jour corrective et évolutive continue des systèmes de protection ( firmware, IPS, applications, etc),
- Une maintenance matérielle des produits Stormshield Network en deux niveaux : Echange standard à la réception du produits défectueux ou Echange express dès la détection de la panne,
- L'accès au support technique via un réseau de partenaire,
- L'accès à l'espace de veille sécurité « Stormshield Security Watch » via l'espace client Stormshield. Cet espace liste l'ensemble des vulnérabilités et attaques gérées par les solutions Stormshield Network Security.

Les différents packs :

- **Remote Office Security Pack** : Ce pack est proposé spécialement pour la protection des petits sites distants, connectés directement à leur site central via un tunnel VPN. Il est adapté pour gérer et filtrer finement les accès sur le réseau. Les fonctions de sécurité telles que l'antivirus, l'antispam ou le filtrage d'URL sont alors portées directement par le site central. Ce pack est disponible uniquement sur les produits SN160(w) et SN210(w).

- **UTM Security Pack** : Les entreprises qui souhaitent une protection unifiée contre les menaces transitant par le Web ou la messagerie et désirent contrôler finement les activités de surf des utilisateurs peuvent souscrire à ce pack. Elles bénéficient alors de la technologie de prévention d'intrusion unique de Stormshield Network Security, d'un moteur antispam avancé, d'un antivirus pour la détection des programmes malveillants et de 16 catégories de sites WEB pour définir une politique d'accès à Internet.
- **Premium UTM Security Pack** : Ce pack s'adresse aux entreprises exigeantes en matière de sécurité. Il apporte les meilleures technologies pour contrer les attaques les plus évoluées. Un système antimalware avec technologie d'émulation et le filtrage d'URLs en mode Cloud, basé sur 65 catégories (Extended Web Control), élèvent votre protection jusqu'à un niveau inégalé sur le marché. Le module Stormshield Network Vulnerability Manager offre une visibilité temps-réel sur les vulnérabilités réseau ou applicatives affectant les postes et serveurs du système d'information.
- **Entreprise Security Pack** : Destiné aux entreprises qui disposent de solutions de protection distinctes pour chaque fonction de sécurité, ce pack concentre la valeur ajoutée des produits Stormshield Network Security sur les fonctionnalités Next-Generation Firewall. La mise à jour de la base d'applications destinée au contrôle applicatif est réalisée de manière continue, en intégrant en priorité les applications demandées par nos clients. Le module Stormshield Network Vulnerability Manager offre une visibilité temps-réel sur les vulnérabilités réseau ou applicatives affectant les postes et serveurs du système d'information.



- Fonctions standards
- Packs de sécurité et options logicielles
- ➔ **Options matérielles**

Présentation de Stormshield  
et de ses produits

STORMSHIELD

## LES OPTIONS MATÉRIELLES

Option Matérielles	SN720 (1 module)	SN920 (1 module)	SN1100 (2 modules)	SN2100 (2 modules)	SN3100 (2 modules)	SN6100 (6 modules)
Module d'extension 8 ports cuivre 10x100x1000	Option	Option	Option	Option	Option	Option
Module d'extension 4 ports fibre Gigabit SFP	-	-	-	Option	Option	Option
Module d'extension 8 ports fibre Gigabit SFP	Option	Option	Option	Option	Option	Option
Module d'extension 2 ports fibre 10 Gigabits SFP+	-	-	-	-	-	-
Module d'extension 4 ports cuivre 10 Gigabits SFP+	Option	Option	Option	-	-	-
Module d'extension 4 ports fibre 10 Gigabits SFP+	Option	Option	Option	Option	Option	Option
BIG DATA (disque 1To)	-	-	-	-	Option	Option

STORMSHIELD

11

Les produits (SN710, SN910, SN2000, SN3000 et SN6000) proposent une modularité réseau incomparable sur le marché, grâce à des modules optionnels de connectiques cuivre ou fibre:

- **SN720** intègre 8 ports 10/100/1000/2500 + 2 ports SFP+ et peut supporter en plus 8 ports 10/100/1000/2500, 4 ports SFP+ 10Gbps (1 module d'extension).
- **SN920** intègre 8 ports 10/100/1000/2500 + 2 ports SFP+ et peut supporter en plus 8 ports 10/100/1000/2500, 4 ports SFP+ 10Gbps (1 module d'extension).
- **SN1100** intègre 8 ports 10/100/1000 + 2 ports SFP 10Gbps et peut supporter en plus 8 ports 10/100/1000, 4 ports 10Gbps cuivre ou 8 ports 1Gbps fibre ou 4 ports 10Gbps fibre (2 module d'extension).
- **SN2100** et **SN3100** intègrent 2 ports 10/100/1000 en standard et peuvent supporter en plus 24 ports 10/100/1000, 24 ports SFP 1Gbps, 12 ports SFP+ 10Gbps (3 modules d'extension) ou 6 ports 40 Gbps.
- **SN6100** intègre 8 ports 10/100/1000 de base et peut supporter en plus 62 ports 10/100/1000, 64 ports SFP 1Gbps ou 34 SFP+ 10Gbps (7 modules d'extension), ou 16 ports 40 Gbps.
- **SNi20** intègre 4 ports 10/100/1000 et peut supporter en plus 2 ports SFP 1Gbps.
- **SNi40** intègre 5 ports 10/100/1000 et peut supporter en plus 2 ports SFP 1Gbps.
- **SNxr1200** intègre 5 ports 10/100/1000 via connecteurs MILDTL-38999.



## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de Stormshield et de produits
- Prise en main du firewall
  - Traces et supervision
  - Les objets
  - Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Enregistrement du firewall et accès aux ressources documentaires

- Démarrage/Arrêt / Reset
- Connexion au firewall
- L'interface d'administration
- Configuration système
- Modification du mot de passe du compte "admin"
- Licence
- Maintenance

STORMSHIELD

Prise en main du firewall

## ENREGISTREMENT DU FIREWALL ET ACCÈS AUX RESSOURCES DOCUMENTAIRES

<https://mystormshield.eu>

AUTHENTICATION

**My STORMSHIELD**

Login: john.smith@stormshield.eu

Password: \*\*\*\*\*

Privacy policy Reset password Create an account/register a product Need help? Sign in

STORMSHIELD

3

L'espace personnel MyStormshield permet de gérer le cycle de vie des produits Stormshield. Il existe deux types de compte pour y accéder : client et partenaire.

Les comptes clients permettent d'enregistrer l'ensemble des produits Stormshield d'une même société.

Les comptes partenaires permettent de gérer l'infogérance éventuelle de comptes clients.

Vous devez renseigner le numéro de SIRET ou de SIREN de votre société ou celui de votre client à la création d'un compte MyStormshield.

À la réception d'un produit Stormshield, vous devez l'enregistrer sur votre compte ou celui de votre client afin d'activer le contrat de maintenance.

Il est possible de renseigner plusieurs contacts/utilisateurs au sein d'un compte utilisateur.

Une aide en ligne dédiée et spécifique au site MyStormshield est accessible à partir de sa page d'accueil.

## ENREGISTREMENT DU FIREWALL ET ACCÈS AUX RESSOURCES DOCUMENTAIRES

The screenshot shows the Stormshield web interface. The main content area is titled "Management of your products" and displays a list of products with their serial numbers (e.g., SN300A14G0064A7, SN300A14G0063A7, etc.). A search bar is available at the top of the list. To the right of the list, there is a "Download description of maintenance and options" button. Below this, there is a "Customized description" section with a "Description:" field and a "Project:" field. A "Submit changes" button is located at the bottom of this section. On the right sidebar, there is a "Services" section with a table of services:

Service	Status	Start date	Expires
Support	Activated	2014-08-01	on:2020-07-31
Updates	Activated		Expires on:2020-07-31
Options			
Kaspersky Antivirus	Activated		Expires on:2020-07-31
Extended Web Control	Activated		Expires on:2020-07-31
Vulnerability Manager	Activated		Expires on:2020-07-31
Hardware Warranty			
Standard	Activated		Expires on:2020-07-31
Express	Activated		Expires on:2020-07-31

STORMSHIELD

4

Sur l'espace MyStormshield, vous pourrez entre autres :

- Télécharger les licences d'activation, les nouvelles versions de firmware, les outils d'administration,
- Récupérer les fichiers de configuration sauvegardés dans le Cloud,
- Accéder à la base documentaire (ressources marketing ou légales),
- S'abonner à la newsletter,
- Gérer l'infogérance (sur les comptes de type partenaire),
- Mettre à jour automatiquement certains services du firewall (signatures contextuelles, base d'URL Stormshield, etc.),
- Remonter des suggestions de catégorisation d'URL,
- Ouvrir un ticket auprès du support Stormshield.

## ENREGISTREMENT DU FIREWALL ET ACCÈS AUX RESSOURCES DOCUMENTAIRES

Le site <https://documentation.stormshield.eu> est accessible sans authentification. Il contient l'ensemble des documentations publiques gérées par l'équipe des rédacteurs techniques Stormshield :

- Notes de versions,
- Guides de configuration,
- Notes techniques.

Ce dernier type de document vous permet de mettre en place des configurations évoluées grâce à une présentation pas à pas des notions à maîtriser et des paramètres à définir.

La base de connaissance est accessible à l'URL <https://kb.stormshield.eu>. L'authentification à cette ressource est basée sur les identifiants MyStormshield. Cette base est alimentée et maintenue en permanence par l'équipe du TAC (support technique) SNS.

Vous y trouverez entre autres :

- Les paramètres de configuration spécifiques,
- La liste des limitations fonctionnelles connues,
- L'enregistrement des webinaires créés par le TAC,
- Les procédures de diagnostics.



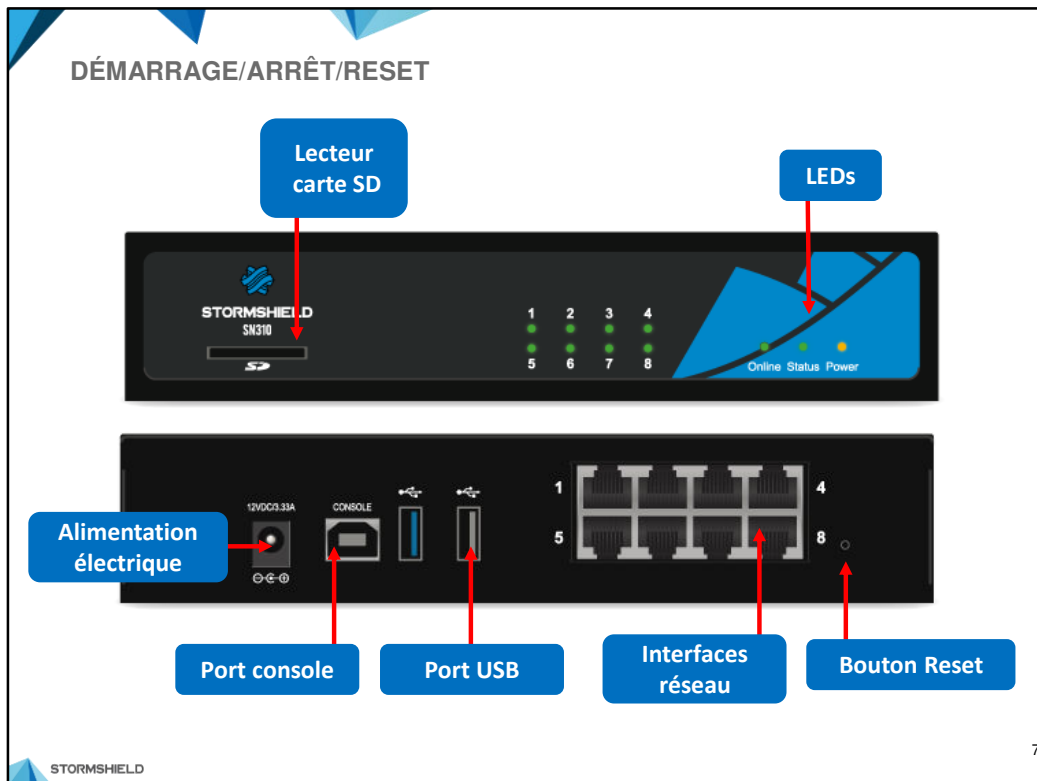
- Enregistrement du firewall et accès aux ressources documentaires

➔ **Démarrage/Arrêt / Reset**

- Connexion au firewall
- L'interface d'administration
- Configuration système
- Modification du mot de passe du compte "admin"
- Licence
- Maintenance

STORMSHIELD

**Prise en main du firewall**



On retrouve une connectique similaire sur les UTM de la gamme, bien que son emplacement puisse varier en fonction du produit concerné :

- Un bouton de démarrage/arrêt,
- Trois LEDs d'état :
  - La première LED « orange » indique que le firewall est sous-tension (câble d'alimentation branché),
  - La deuxième LED « verte » indique que le système d'exploitation du firewall est fonctionnel,
  - La troisième LED « verte » indique que le firewall a fini de démarrer et qu'il est fonctionnel,
- Un lecteur de carte SD : Pour ajouter une carte mémoire sur le firewall,
- Un port clavier PS2 et un connecteur vidéo VGA ou HDMI : Pour brancher un clavier et un écran sur le firewall et y accéder en mode console,
- Un port série ou port USB câblé en interne sur un adaptateur série : Pour brancher une console série sur le firewall,
- Un bouton Reset : Pour restaurer la configuration usine du firewall,
- Un port USB: Permet le branchement d'une clé USB ou d'un modem 3G,
- Des interfaces réseau : Le type et le nombre différent selon le modèle.

**NOTE** : La carte mémoire doit être au minimum de classe 10, au standard SDXC et d'une capacité maximale de 32 Go (2To pour les modèles SN160(W), SN210(W), et SN310 avec une carte SDHC).

**Démarrage du firewall :**

Le démarrage s'effectue en mettant sous-tension le firewall et en appuyant ensuite sur le bouton de démarrage dans le cas où celui-ci est présent. Au début, les deux premières LEDs en partant de l'orange s'allument ce qui indique que le firewall est sous tension et que le système est en cours de démarrage. Une fois ce dernier démarré, la dernière LED s'allume pour indiquer que le firewall est opérationnel. Certains modèles émettent alors un signal sonore.

**Arrêt du firewall :**

L'arrêt s'effectue en appuyant sur le bouton d'arrêt s'il est présent, ou via l'interface d'administration. La première LED verte n'est plus allumée fixe ce qui indique le début de l'arrêt du système. Une fois le système arrêté, les deux LEDs vertes sont éteintes et le firewall s'arrête complètement.

**Restauration de la configuration usine :**

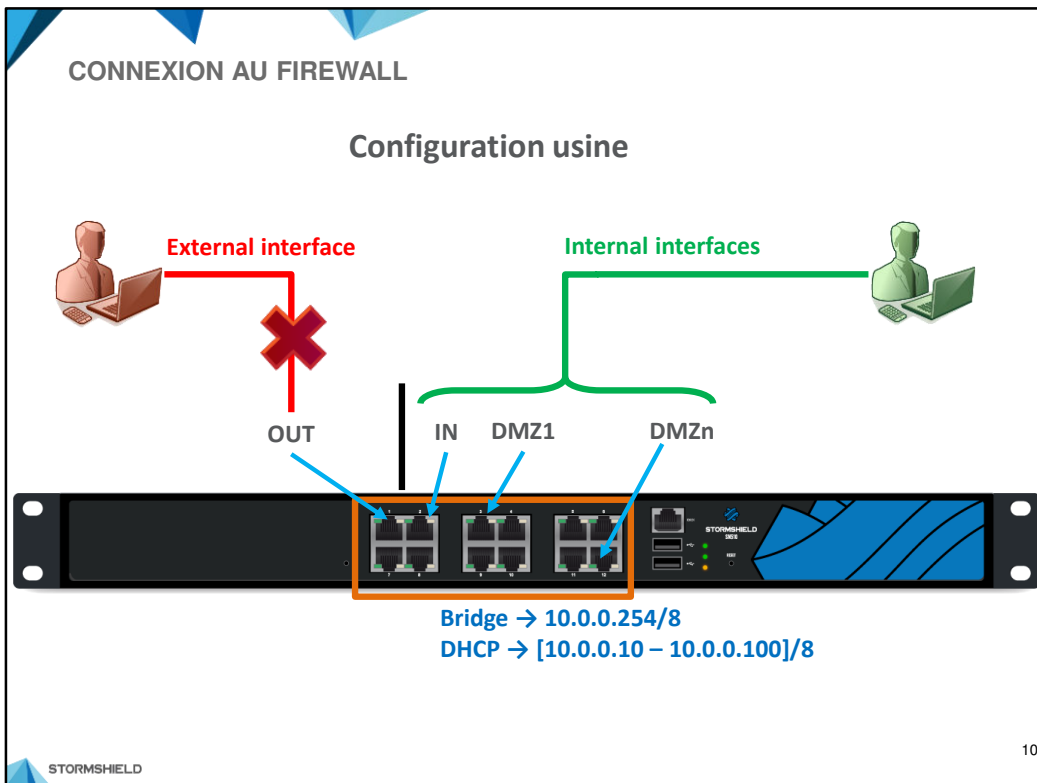
Maintenez le bouton Reset enfoncé 10 secondes (il y aura émission d'un signal sonore sur certains modèles). Le firewall restaure la configuration usine et redémarre automatiquement.



- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- ➔ **Connexion au firewall**
- L'interface d'administration
- Configuration système
- Modification du mot de passe du compte "admin"
- Licence
- Maintenance

STORMSHIELD

Prise en main du firewall



Dans une configuration usine, la première interface du firewall est nommée « OUT », la seconde « IN » et le reste des interfaces « DMZx ». L'interface « out » est une interface externe, utilisée pour connecter le firewall à internet. Les autres interfaces sont internes et servent principalement à connecter le firewall à des réseaux locaux.

La distinction interne/externe pour les interfaces permet de se protéger contre les attaques d'usurpation d'adresse IP.

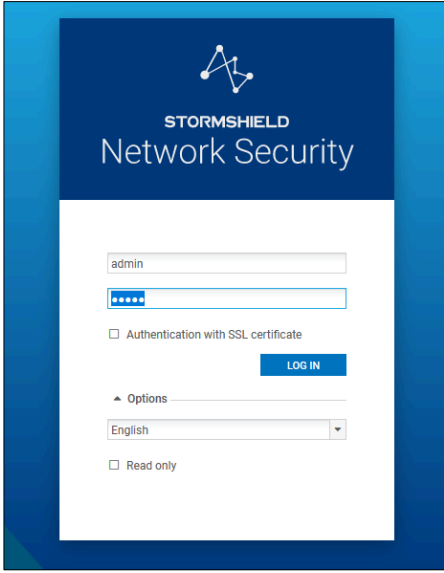
Toutes les interfaces sont incluses dans un bridge dont l'adresse est 10.0.0.254/8. Un serveur DHCP est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre 10.0.0.10 et 10.0.0.100.

Pour accéder à l'interface d'administration du firewall, vous devez connecter votre machine sur une interface interne.

**NOTE :** Avec la configuration usine, connecter une machine sur l'interface externe et ensuite sur une interface interne sera interprété par le firewall comme une tentative d'usurpation d'adresse IP sur le bridge et par conséquent, il bloquera tout le trafic généré par cette machine. Le redémarrage du firewall sera nécessaire pour débloquer cette situation.

CONNEXION AU FIREWALL

<https://10.0.0.254/admin>



Mozilla Firefox

Google Chrome

Microsoft Edge

STORMSHIELD

11

L'accès à l'interface graphique d'administration du firewall s'effectue grâce à un navigateur Web en HTTPS à l'adresse « <https://10.0.0.254/admin> ». Pour un fonctionnement optimal de cette interface, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Edge, Google Chrome et Mozilla Firefox.

L'accès aux pages d'administration nécessite une authentification. Par défaut, seul le compte système **admin**, disposant de tous les privilèges sur le boîtier, existe et peut se connecter. En configuration usine, le mot de passe de ce compte est également **admin** ; pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe.

Pour s'authentifier, l'utilisateur peut également sélectionner un certificat dans le magasin de son navigateur.

Dans les options avancées, l'administrateur peut choisir la langue des menus de configuration ainsi que l'accès en lecture seule, ce qui empêche toute modification de la configuration.



- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- Connexion au firewall

➔ **L'interface d'administration**

- Configuration système
- Modification du mot de passe du compte "admin"
- Licence
- Maintenance

STORMSHIELD

Prise en main du firewall

**L'INTERFACE D'ADMINISTRATION**

**Traces de l'interface d'administration**

L'interface d'administration est découpée en quatre parties :

**1. L'en-tête (partie encadrée en vert) :** Elle contient les informations suivantes :

- Le nom du firewall : le nom par défaut est le numéro de série,
- La version du système (firmware),
- L'utilisateur connecté sur l'interface, ses droits d'accès à la configuration: lecture seule ou écriture et ses droits d'accès aux logs : restreint ou complet,
- Un lien vers l'aide du menu courant ainsi que des informations complémentaires sur les paramètres et les options du menu. Notez que les pages d'aide ne sont pas embarquées mais redirigent vers Internet.

Cliquer sur le nom d'utilisateur permet d'accéder à plusieurs fonctionnalités :

- Le menu « Préférences » permet de configurer plusieurs paramètres en relation avec l'interface d'administration. Les plus importants sont :
  - Le temps d'inactivité avant de déconnecter l'utilisateur de l'interface d'administration (30 minutes par défaut),
  - Les options d'affichage dans les menus (toujours afficher les configurations avancées, nombre de règles de filtrage par page, etc),
  - Liens externes vers les sites Stormshield.
- Acquérir ou libérer les droits d'écriture. Notez qu'à un instant donné, un seul utilisateur peut disposer du droit d'écriture sur le firewall.
- Accéder aux données personnelles.
- Déconnecter l'utilisateur.



2. **Les menus (partie encadrée en rouge)** : Regroupe les menus de configuration, de supervision ainsi que des raccourcis organisés sous forme de listes rétractables. Les menus sont séparés en 2 catégories. L'onglet supervision pour tout ce qui touche à la supervision, les log et l'état du firewall. L'onglet configuration pour les objets et le paramétrage des diverses fonctionnalités.
3. **Le contenu du menu (partie encadrée en bleu)** : Affiche le contenu du menu sélectionné.
4. **Les logs de la webUI (partie encadrée en marron)** : Affiche une liste (paramétrable) des logs de l'interface web. On peut y faire apparaître par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements, ....



- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- Connexion au firewall
- L'interface d'administration

➤ **Configuration système**

- Modification du mot de passe du compte "admin"
- Licence
- Maintenance

STORMSHIELD

Prise en main du firewall

## CONFIGURATION SYSTÈME : GÉNÉRALE

SYSTEM / CONFIGURATION

GENERAL CONFIGURATION    FIREWALL ADMINISTRATION    NETWORK SETTINGS

General configuration

Firewall name:	<input type="text" value="VMSNSX09K0639A9"/>
Firewall language (logs):	<input type="text" value="English"/>
Keyboard (console):	<input type="text" value="English"/>

Cryptographic settings

Enable regular retrieval of certificate revocation lists (CRL)  
 Enable "ANSSI Diffusion Restreinte (DR)" mode

Password policy

Minimum password length:	<input type="text" value="1"/>
Mandatory character types:	<input type="text" value="None"/>
Minimum entropy:	<input type="text" value="20"/>

STORMSHIELD
16

Le menu **CONFIGURATION** ⇒ **SYSTÈME** ⇒ **Configuration** permet de configurer les paramètres systèmes, administratifs et réseaux du firewall. Il est composé de trois onglets :

### 1. CONFIGURATION GÉNÉRALE :

- Le nom du firewall qui par défaut est le numéro de série.
- La langue des traces remontées par le firewall (Anglais ou Français).
- La disposition du clavier utilisée pour un accès console direct (Anglais, Français, Italien, Polonais ou Suisse).
- Les paramètres cryptographiques regroupent deux options qui sont respectivement en relation avec les certificats (présentés dans la formation Expert) et le mode « ANSSI Diffusion Restreinte (DR) ».
- La politique de mots de passe définit la longueur minimale et les caractères obligatoires des mots de passe créés dans les différents menus du firewall (par exemple : mots de passe des utilisateurs dans l'annuaire interne (LDAP), mots de passe qui protègent les fichiers de sauvegarde, mots de passe des certificats créés au niveau du firewall). Par défaut, la longueur minimale est à un et aucun caractère n'est obligatoire. Cependant, l'administrateur peut imposer des mots de passe alphanumériques seulement ou alphanumériques avec des caractères spéciaux, et modifier la valeur minimale de l'entropie des mots de passe.

**NOTE** : L'entropie définit le niveau de robustesse du mot de passe. Plus elle est élevée, plus la robustesse du mot de passe doit être importante. Elle tient compte de la longueur du mot de passe et de la taille du jeu de caractères utilisé.

## CONFIGURATION SYSTÈME : GÉNÉRALE

SYSTEM / CONFIGURATION

GENERAL CONFIGURATION FIREWALL ADMINISTRATION NETWORK SETTINGS

Date/Time settings - 06/03/2021 05:36:01 PM

Manual mode  
 Synchronize with your machine - 06/03/2021 05:36:02 PM  
 Synchronize firewall time (NTP)

Time zone:

LIST OF NTP SERVERS

+ Add X Delete

NTP server (host or group - address range) (max 15)	Authentication k...
ntp1.stormshieldcs.eu	
ntp2.stormshieldcs.eu	

- Les paramètres horaires: date, heure et fuseau horaire. Ces paramètres sont cruciaux pour des fonctionnalités telles que les logs ou l'authentification. La modification du fuseau horaire nécessite le redémarrage du firewall.
- Pour permettre au firewall de synchroniser son horloge automatiquement avec un serveur NTP, il suffit de cocher l'option Maintenir le firewall à l'heure (NTP). Par défaut, deux serveurs NTP appartenant à Stormshield sont préconfigurés dans la liste des serveurs. Cette liste peut être modifiée.

## CONFIGURATION SYSTÈME : ADMINISTRATION FIREWALL

SYSTEM / CONFIGURATION

GENERAL CONFIGURATION FIREWALL ADMINISTRATION NETWORK SETTINGS

Access to the firewall's administration interface

Allow the 'admin' account to log in

Listening port:

[Configure the SSL certificate of the service](#)

Maximum idle timeout (for all administrators):

Enable protection from brute force attacks

Number of authentication attempts allowed:

Freeze time (minutes):

ACCESS TO FIREWALL ADMINISTRATION PAGES

Authorized administration host (host or group - network - address range)

Network\_internals

Disclaimer for access to the administration interface

Disclaimer file:

Remote SSH access

Enable SSH access

Enable password access

Use the nsrpc shell for administrators other than the admin account

Listening port:

## 2. ADMINISTRATION DU FIREWALL :

- Il est possible de ne plus autoriser le compte « admin » à accéder à l'interface d'administration. Cela implique qu'un nouvel administrateur ait été préalablement créé avec des droits suffisants. Dans le contraire, l'accès à l'interface d'administration par ce compte admin ne pourra être restauré que par une modification de configuration en mode commande.
- Le port utilisé pour accéder à l'interface d'administration du firewall peut être un autre port que le standard HTTPS (443/TCP), défini par défaut. L'URL d'accès devient alors : `https://@IP_firewall:port/admin`.
- Par défaut, l'interface d'administration du firewall utilise un certificat issu de l'autorité de certification du firewall. Le lien « Configurer le certificat SSL pour l'accès à l'interface d'administration » renvoie vers le menu qui permet de modifier ce certificat.
- Le délai maximal d'inactivité peut être défini pour tous les administrateurs. Un administrateur peut configurer un temps de déconnexion en cas d'inactivité dans ses préférences (menu accessible en cliquant sur son nom utilisateur), si ce temps de déconnexion est inférieur ou égal au délai maximal paramétré.
- La protection contre les attaques force brute pour l'accès à l'interface d'administration peut être activée/désactivée et le nombre de tentatives ainsi que le temps d'attente (en minutes) sont paramétrables. Par défaut, après 3 tentatives d'authentification infructueuses, l'accès depuis cette adresse IP sera bloqué pendant 1 minute.



- L'accès à l'interface d'administration peut être limité à une machine ou un réseau spécifique. Dans ce cas, la machine ou le réseau doit apparaître dans la liste « Poste d'administration autorisé ». Par défaut, seuls les réseaux internes et représentés par l'objet « Network\_internals » sont autorisés à y accéder.
- Un avertissement pour l'accès à l'interface d'administration peut être affiché. Le fichier d'avertissement peut contenir du texte, ou être au format HTML (mais ne doit pas comporter de Javascript).
- Il est possible d'activer l'accès par SSH (connexion sécurisée) et de modifier le port d'écoute du service qui est par défaut SSH (22/TCP). L'authentification peut se faire par mot de passe si cette option est activée, ou, sinon, par paire de clés.
- Lorsque vous disposez d'un annuaire, vous pouvez accorder à des utilisateurs des droits d'accès à la console en SSH. Si la case « Utiliser le shell nsrpc pour les administrateurs autres que le compte admin » est cochée, seules les commandes CLI (propriétaires Stormshield pour configurer le firewall) seront autorisées. Dans le cas contraire, l'accès sera complet.

**CONFIGURATION SYSTÈME : PARAMÈTRES RÉSEAUX**

GENERAL CONFIGURATION    FIREWALL ADMINISTRATION    NETWORK SETTINGS

---

IPv6 support

OFF

---

Proxy server

ON

Server:

Port:

ID:

Password:

---

DNS resolution

LIST OF DNS SERVERS USED BY THE FIREWALL

+ Add    X Delete

DNS (host)
dns1.google.com
dns2.google.com

20

### 3. PARAMÈTRES RÉSEAUX :

- Les firewalls Stormshield Network supportent le protocole IPv6 et plusieurs fonctionnalités (interface, routage, filtrage, VPN et administration) sont compatibles IPv6. Cependant, ce support est optionnel et son activation s'effectue via le bouton **Activer le support du protocole IPv6 sur ce Firewall**.

**NOTE :** Cette action étant irréversible, la sauvegarde de la configuration du firewall vous sera proposée automatiquement lorsque vous cliquerez sur ce bouton. Le retour à un support IPv4 exclusif (sans IPv6) n'est possible qu'après une remise à la configuration usine (reset) du firewall.

- Dans le cas où le firewall transite par un proxy pour accéder à Internet, les paramètres se renseignent depuis ce menu.
- Un ou plusieurs serveurs DNS peuvent être ajoutés. Le firewall contacte ces serveurs pour toute résolution qu'il émet ou doit relayer. Ces résolutions de noms sont nécessaires pour des fonctionnalités telles que Active Update qui interroge les serveurs de mise à jour pour télécharger les bases de données (signatures contextuelles, antivirus, Vulnerability Manager, ...). Ces serveurs DNS sont également utilisés dans le cas où le service cache DNS est activé en mode transparent (voir annexe Proxy cache DNS).



- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- Connexion au firewall
- L'interface d'administration
- Configuration système
- ➔ **Modification du mot de passe du compte "admin"**
- Licence
- Maintenance

STORMSHIELD

Prise en main du firewall

## MODIFICATION DU MOT DE PASSE DU COMPTE « ADMIN »

The screenshot shows the Stormshield Network Security administration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs. The current page is 'ADMINISTRATOR ACCOUNT' under the 'SYSTEM / ADMINISTRATORS' menu. A red warning icon is visible in the top right corner of the interface. The main content area shows the 'Authentication' section with a message: 'The default password of the admin account has not been changed'. Below this, there are three password input fields: 'Old password:', 'Password:', and 'Confirm password:'. The 'Password:' field is highlighted with a red box and labeled 'Weak'. To the right, a 'Global status: Critical' panel lists various system metrics, with 'Admin password age: Critical' highlighted in red. At the bottom of the page, there are 'Exports' options for the administrator's private key and the firewall's public key.

Tant que le mot de passe de la configuration usine n'a pas été modifié, une erreur critique est affichée dans l'en-tête de l'interface d'administration (encadrés rouges). Le mot de passe du compte « admin » doit être modifié dans l'onglet **COMPTE ADMIN** du menu **CONFIGURATION** ⇒ **SYSTÈME** ⇒ **Administrateurs**. Le mot de passe doit avoir au minimum 5 caractères et doit respecter la politique de mot de passe définie dans le menu **CONFIGURATION**.

La force du mot de passe indique son niveau de sécurité : Très faible, faible, moyen, bon, excellent. Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux pour augmenter le niveau de sécurité.

Les boutons Exporter la clé privée et Exporter la clé publique du firewall permettent respectivement de télécharger la clé privée et clé publique du compte admin. Ces clés permettent de se connecter en SSH au firewall.



- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- Connexion au firewall
- L'interface d'administration
- Configuration système
- Modification du mot de passe du compte "admin"
- **Licence**
- Maintenance

STORMSHIELD

Prise en main du firewall

**LICENCE : GÉNÉRAL**

SYSTEM / LICENSE

GENERAL LICENSE DETAILS

Search for a new license Install the new license

Local firewall date: Thursday 25th August 2022  
Last check for license updates performed on: Thursday 25th August 2022

- License will expire in 5606 days, on Thursday 31st December 2037.
- Maintenance will expire in 2390 days, on Monday 12th March 2029.
- Stormshield Vulnerability Manager will expire in 2390 days, on Monday 12th March 2029.
- Advanced antivirus will expire in 2390 days, on Monday 12th March 2029.
- Extended Web Control option will expire in 2390 days, on Monday 12th March 2029.
- Sandboxing Breach Fighter option will expire in 564 days, on Tuesday 12th March 2024.  
The industrial option has not been subscribed.

Install license

License file :

Install

Advanced properties

Look for license updates :

- never
- every 12 hours
- everyday
- every week
- every month

Install license after it has been downloaded :

- always manual (using the button *install a new license*)
- automatic when possible (no reboot necessary)

CANCEL APPLY

STORMSHIELD 24

Le menu **CONFIGURATION** ⇒ **SYSTÈME** ⇒ **Licence**, affiche toutes les informations concernant la licence. Le firewall possède une licence temporaire valide 3 mois, permettant son fonctionnement immédiatement après sa mise en marche. La licence définitive est à télécharger depuis votre espace privé Stormshield (après enregistrement du firewall) ou à installer automatiquement. Elle se présente sous la forme d'un fichier « .licence ».

Le menu est constitué de deux onglets :

### 1. GÉNÉRAL :

En haut de l'onglet un bouton permet de rechercher les nouvelles licences directement sur les serveurs de mise à jour Stormshield et un autre bouton permet de l'installer. Ils sont suivis d'informations sur la durée de validité de la licence et des différentes options disponibles. La partie **Installation à partir d'un fichier** permet d'installer la licence à partir du fichier « .licence » stocké sur le PC.

Enfin, la partie **Configuration avancée** permet de configurer la fréquence de recherche des mises à jour et également d'en automatiser l'installation.

**NOTE** : Un avertissement en couleur orange indique une expiration de l'option de licence concernée dans un délai inférieur à 90 jours.

## LICENCE : DÉTAILS DE LA LICENCE

GENERAL LICENSE DETAILS	
Search	Search for a new license   Install the new license
Feature	In progress (current license)
<b>Administration (3 elements)</b>	
SN Global Administration	Available
Realtime Monitor	Available
Event Analyzer	Available
<b>Expiry dates (14 elements)</b>	
Antispam DNS blacklists (RBL)	Monday 12th March 2029
ClamAV Antivirus	Monday 12th March 2029
Express Warranty	Tuesday 12th March 2024
Industrial	Option not subscribed
License will be valid until	Thursday 31st December 2037
Contextual protection signatures	Monday 12th March 2029
Antispam: heuristic engine	Monday 12th March 2029
Sandboxing Breach Fighter	Tuesday 12th March 2024
Embedded URL databases	Tuesday 12th March 2024
Extended Web Control URL databases	Monday 12th March 2029
Update	Monday 12th March 2029
Advanced Antivirus	Monday 12th March 2029
Vulnerability Manager	Monday 12th March 2029
Warranty	Monday 12th March 2029
<b>Options (7 elements)</b>	
Custom contextual protection signatures	Available
Express Warranty	Available
External directory (LDAP)	Available
High availability	Master
Industrial	Not available
PIG	Available
Vulnerability Manager	Available
<b>Global (4 elements)</b>	
Comment	No maintenance pack
Id	
Temporary	No

25

## 2. DÉTAILS DE LA LICENCE :

Les boutons de recherche et d'installation de la licence sont également présents ici. Une barre de recherche permet de trouver rapidement la disponibilité d'une option ou d'un service dans la licence.

Le reste de la page détaille le contenu de la licence avec les durées de validité.



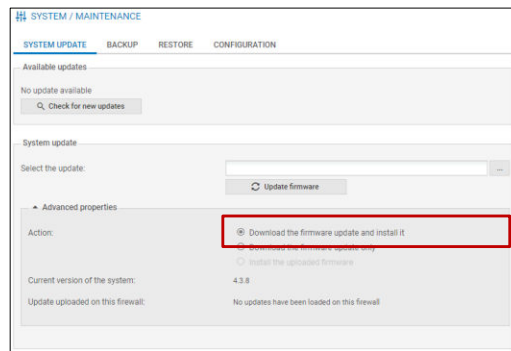
- Enregistrement du firewall et accès aux ressources documentaires
- Démarrage/Arrêt / Reset
- Connexion au firewall
- L'interface d'administration
- Configuration système
- Modification du mot de passe du compte "admin"
- Licence

 **Maintenance**

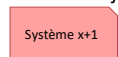
STORMSHIELD

## Prise en main du firewall

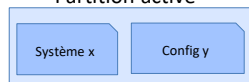
## MAINTENANCE : MISE À JOUR DU SYSTÈME



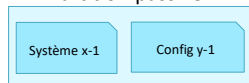
Fichier .maj



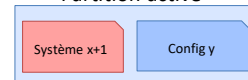
Partition active



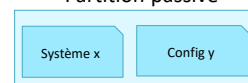
Partition passive

Mise à jour  
système avec  
sauvegarde

Partition active



Partition passive



STORMSHIELD

27

Le menu **CONFIGURATION** ⇒ **SYSTÈME** ⇒ **Maintenance** permet de gérer les mises à jour système ainsi que les sauvegardes/restaurations de configuration. Quatre onglets composent ce menu:

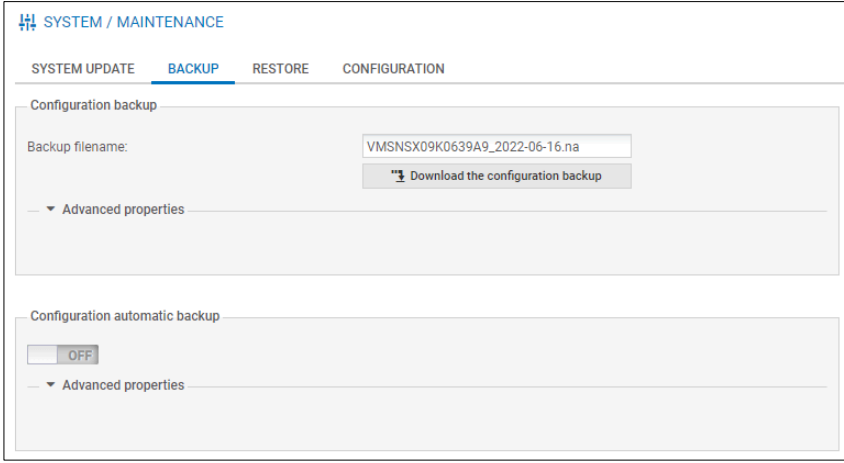
### 1. Mise à jour du système :

Cet onglet permet à l'administrateur de mettre à jour la version du système (firmware). Le fichier de mise à jour « .maj » peut être téléchargé au niveau du compte client Stormshield ou bien récupéré automatiquement par le firewall en appuyant sur le bouton « Recherche de nouvelles mises à jour ».

La figure ci-dessus illustre la mise à jour du système des partitions. La nouvelle version du système « x+1 » remplacera l'ancienne version « x » se trouvant sur la partition active tout en gardant la même configuration « y ». L'administrateur peut choisir ou non de faire une sauvegarde de la partition active sur la partition de sauvegarde (encadré rouge), avant la mise à jour, grâce à l'option « Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le firewall » (Si l'option est cochée, l'ancienne version du système « x-1 » et la configuration « y-1 » seront définitivement perdues).

Dans la « configuration avancée », l'administrateur peut choisir de télécharger et d'activer une mise à jour ou bien de la télécharger uniquement, son activation pourra se faire ultérieurement avec l'option « Activer le firmware précédemment téléchargé ».

## MAINTENANCE : SAUVEGARDER UNE CONFIGURATION



SYSTEM / MAINTENANCE

SYSTEM UPDATE **BACKUP** RESTORE CONFIGURATION

Configuration backup

Backup filename: VMSNSX09K0639A9\_2022-06-16.na

Download the configuration backup

Advanced properties

Configuration automatic backup

OFF

Advanced properties

STORMSHIELD

28

## 2. SAUVEGARDER :

Dans cet onglet, l'administrateur peut effectuer une sauvegarde manuelle de la configuration du firewall qui est téléchargée et enregistrée sous le format d'un fichier chiffré « .na ». Les éléments sauvegardés dans le fichier sont listés ci-dessous:

- Réseau (interface, routage et DNS dynamique),
- Filtrage SMTP,
- Filtrage URL,
- Filtrage SSL,
- Objets web,
- Modules globaux,
- Configuration sécurisée,
- Active Update,
- Services (SNMP, serveur DHCP),
- Profils d'inspection IPS,
- Objets réseaux,
- Filtrage et NAT,
- VPN IPSec,
- Annuaire LDAP.

L'administrateur ne peut pas sauvegarder une partie de la configuration via l'interface web (une sauvegarde partielle est possible en ligne de commande). Le fichier peut être protégé en plus par un mot de passe qui doit être renseigné, avant le téléchargement, dans la partie « configuration avancée ».

**MAINTENANCE : SAUVEGARDER UNE CONFIGURATION**

Configuration automatic backup

ON

Configuration:  Cloud backup  Customized server

▲ Advanced properties

Backup frequency:

Backup file password:

Confirm password:

Password strength

STORMSHIELD 29

L'administrateur peut également activer la sauvegarde automatique du fichier de configuration. Deux options sont possibles :

- **Cloud backup** : En activant cette option, le fichier de configuration est stocké sur un serveur hébergé dans une infrastructure de service nommée « cloud backup service » gérée par Stormshield. La sauvegarde peut être effectuée chaque jour, chaque semaine ou chaque mois. Dans la « configuration avancée », on peut configurer cette fréquence et protéger la configuration par un mot de passe grâce aux paramètres « Fréquence des sauvegardes » et « Mot de passe du fichier de sauvegarde ». La sauvegarde est sécurisée avec une connexion HTTPS et une authentification par certificat. Au maximum, 5 fichiers de configuration par firewall peuvent être sauvegardés sur les serveurs du cloud. Au-delà, le nouveau fichier écrasera le plus ancien. Ces fichiers sont accessibles depuis l'espace client Stormshield.



- Serveur personnalisé : Avec cette option les fichiers de configuration sont stockés sur un serveur dont l'adresse IP est renseignée dans le paramètre « Serveur de sauvegarde ». Plusieurs paramètres peuvent être configurés dans la « configuration avancée » :
  - « Port du serveur » : port d'écoute du serveur de sauvegarde,
  - « Protocole de communication » : HTTP ou HTTPS,
  - « Certificat du serveur » : actif uniquement si le protocole HTTPS est choisi. Il permet de spécifier le certificat présenté par le serveur sur lequel sera envoyée la sauvegarde de configuration. L'objectif est que le firewall puisse s'assurer de l'identité du serveur avant de lui transmettre le fichier de sauvegarde,
  - « Chemin d'accès » : Permet de spécifier le répertoire où seront stockés les fichiers de configuration,
  - « Méthode d'envoi » : Permet de choisir la méthode d'envoi HTTP : authentification basic (auth basic) , authentification digest (auth digest) ou POST,
  - « Identifiant » et « Mot de passe »: Utilisés avec les méthodes d'envoi « auth basic » et « auth digest »,
  - « POST – control name » : Utilisé avec la méthode d'envoi POST,
  - « Fréquence des sauvegardes » : fréquence d'envoi des sauvegardes positionnée par défaut à une semaine,
  - « Mot de passe du fichier de sauvegarde » : protège les fichiers de sauvegarde par un mot de passe.

## MAINTENANCE : RESTAURER UNE CONFIGURATION

SYSTEM UPDATE    BACKUP    **RESTORE**    CONFIGURATION

Select a backup to restore:  ...

▲ Advanced properties

Backup password:

- Restore all modules of the backup file
- Network (interface, routing and dynamic DNS)
- SMTP filtering
- URL filtering
- SSL filtering
- Web objects
- Global modules
- Active Update
- Services (SNMP, DHCP server)
- IPS inspection profiles
- Network objects
- Filtering and NAT
- IPSec VPN
- LDAP directory

**3. RESTAURER :**

La restauration d'une configuration s'effectue à partir d'un fichier « .na » stocké sur la machine. Si le fichier de configuration est protégé par un mot de passe, l'administrateur doit le saisir dans la partie « configuration avancée ».

En fonction des besoins, seule une partie de la configuration peut être restaurée. Dans ce cas, dans la partie *Configuration avancée*, sélectionnez le ou les modules nécessaires. Dans tous les cas, il est conseillé de redémarrer le firewall après une restauration (le redémarrage est proposé uniquement après une restauration complète).

**NOTE :** Le mot de passe de l'utilisateur « admin » n'est pas contenu dans le fichier de configuration. Il ne sera donc ni restauré, ni sauvegardé.

## MAINTENANCE : RESTAURER UNE CONFIGURATION

The screenshot shows a web interface for restoring a configuration. It features a section titled "Restore automatic backup" with a sub-label "Date of the latest backup:". To the right of this label, the text "No backups available" is displayed. Below this, there is a button with a left-pointing arrow and the text "Restore the configuration from the auto...". Underneath the button, there is an expandable section titled "Advanced properties" with a small upward-pointing triangle icon. Inside this section, there is a label "Backup password:" followed by a text input field.

La restauration d'une configuration peut également se faire à partir de la dernière sauvegarde automatique dont la date est indiquée par « **Date de la dernière sauvegarde** ». Dans le cas où la sauvegarde est protégée par un mot de passe, ce dernier doit être renseigné dans la « configuration avancée ».

**MAINTENANCE : CONFIGURATION**

The screenshot shows the 'CONFIGURATION' tab of the Stormshield maintenance interface. It displays system disk information, including the current partition (Main partition 4.2.2) and options to switch to a backup partition (4.1.5) or back up the active partition. Below this, there are buttons for 'Reboot the firewall' and 'Shut down the firewall'. At the bottom, there is a 'Download the system report' button.

The diagram below the screenshot illustrates two possible states of the partitions:

- State 1 (Left):** The 'Principale' partition is active (blue box) and the 'Secours' partition is passive (red box).
- State 2 (Right):** The 'Secours' partition is active (blue box) and the 'Principale' partition is passive (red box).

A double-headed arrow between the two states indicates that the system can switch between these configurations.

STORMSHIELD 33

#### 4. CONFIGURATION :

Tous les UTM physiques Stormshield Network disposent de deux partitions complètement indépendantes qui permettent le stockage de versions de firmware différentes. Chaque partition possède sa propre configuration. Il faut faire la distinction entre les partitions principale/secours et les partitions active/passive. Nous pouvons avoir deux cas de figure illustrés ci-dessus : (1) partition active => principale et partition passive=>secours ou (2) partition active => secours et partition passive => principale.

L'administrateur peut sélectionner la partition qui deviendra active au prochain démarrage du firewall (principale ou de secours). Automatiquement l'autre partition deviendra la partition passive.

Le bouton « sauvegarder la partition active » permet de copier tout le contenu de la partition active (configuration + firmware) sur la partition passive.

Les dernières options de maintenance permettent de redémarrer ou arrêter le firewall et de télécharger le rapport système: fichier texte qui affiche l'état du firewall et de nombreux autres indicateurs utiles au diagnostic par le support technique.

**MAINTENANCE : ACTIVE UPDATE**

SYSTEM / ACTIVE UPDATE

**AUTOMATIC UPDATES**

Status	Module
Enabled	Antispam DNS blacklists (RBL)
Enabled	IPS: contextual protection signatures
Disabled	IPS: custom contextual protection signatures
Enabled	Antivirus: ClamAV antivirus signatures
Enabled	Embedded URL databases
Enabled	Antispam: heuristic engine
Enabled	Vulnerability Manager
Enabled	Root Certification Authorities
Enabled	Geolocation / Public IP reputation

Go to system monitoring

Advanced properties

**UPDATE SERVERS OF THE URL DATABASE**

+ Add X Delete

URL
https://update1-sns.stormshieldcs.eu/1
https://update2-sns.stormshieldcs.eu/1
https://update3-sns.stormshieldcs.eu/1
https://update4-sns.stormshieldcs.eu/1

**UPDATE SERVERS OF CUSTOM CONTEXTUAL PROTECTION SIGNATURES**

+ Add X Delete

URL	CA
	CA

Update frequency: 3h

**UPDATE SERVERS**

+ Add X Delete

URL	CA
https://update1-sns.stormshieldcs.eu/1	CloudServicesSignature
https://update2-sns.stormshieldcs.eu/1	CloudServicesBundle
https://update3-sns.stormshieldcs.eu/1	
https://update4-sns.stormshieldcs.eu/1	
https://custom-update.mydomain	Select a CA for HTTPS URLs

Update frequency: 3h

STORMSHIELD

34

Le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Active Update** permet de contrôler la mise à jour automatique des modules suivants :

- Antispam : listes noires DNS (RBL),
- Bases d'URLs embarquées,
- IPS : Signatures de protection contextuelles,
- Antivirus : signatures Antivirales ClamAV (ou antivirus avancé),
- Antispam : moteur heuristique,
- Management de vulnérabilités (si l'option est active dans la licence),
- Autorités de certification racine.
- IPS : Signatures de protection contextuelle personnalisées.
- Géolocalisation / Réputation IP publiques.

L'administrateur peut activer ou désactiver la mise à jour d'un seul module ou de tous les modules à la fois en utilisant les boutons « Tout autoriser » ou « Tout refuser ».

Les listes des serveurs de mise à jour des différents modules et de la base d'URL sont accessibles dans la partie « configuration avancée ». L'administrateur peut modifier, ajouter ou supprimer des serveurs.

**NOTE** : Le protocole applicatif utilisé pour la mise à jour peut être HTTPS ou HTTP. en cas d'utilisation de HTTPS, il faut ajouter la CA du serveur pour pouvoir valider le certificat présenté.

## RECOMMANDATIONS



- N'utiliser SSH qu'en cas de besoin
- Définir une politique de mot de passe adaptée
- Passer par un miroir ou proxy interne pour mettre à jour
- Configurer des serveurs NTP, DNS maîtrisés
- Sauvegarder automatiquement la configuration
- Définir explicitement les réseaux d'administration
- Dédier une interface pour l'administration
- Configurer correctement la langue (UI, log, console)

L'accès SSH se fait avec le compte admin par défaut, et peut être octroyé à des administrateurs supplémentaires. Il doit donc être occasionnel et suivi. En dehors de ces cas, il doit être désactivé pour réduire la surface d'attaque. Utilisez de préférence une paire de clefs SSH, à défaut d'un mot passe changé très fréquemment.

Un proxy ou un miroir interne permet de :

- Maîtriser l'arrivée des mises à jour,
- Moins consommer de bande passante.

Un serveur NTP interne maintient la cohérence des dates dans les log du système d'information. C'est indispensable en vu de les corrélés.

Un DNS maîtrisé permet de :

- Résoudre les noms des objets locaux et publics,
- Accélérer les résolutions.

L'administration du firewall doit se faire depuis un réseau protégé, identifié et totalement séparé de la production.

Les langues utilisées doivent être comprises par les utilisateurs afin de limiter les erreurs de manipulation du produit.

Sources des recommandations :

- <https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dun-pare-feu-stormshield-network-security-sns/>
- <https://www.ssi.gouv.fr/politique-filtrage-parefeu/>
- <https://www.ssi.gouv.fr/passerelle-interconnexion/>

## RESSOURCES COMPLÉMENTAIRES SUR LES SITES STORMSHIELD



STORMSHIELD

36

Pour aller plus loin, consultez les ressources du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Guide d'installation et de première configuration d'un firewall SNS
- Guide de présentation et d'installation SNS
- Guide de déploiement d'un firewall virtuel SNS EVA
- Guide de déploiement d'un firewall virtuel SNS PAYG
- Manuel d'utilisation et de configuration SNS
  
- Notes techniques:
  - Protéger par mot de passe le panneau de configuration de l'UEFI d'un firewall SNS
  - Activer Secure Boot dans l'UEFI d'un firewall SNS
  - Configuration initiale par clé USB
  - Sauvegardes automatiques
  - EVA sur 3DS OUTSCALE
  - EVA sur Amazon Web Services
  - EVA sur Microsoft Azure
  - Déployer SNS For Cloud (2 interfaces réseau) sur Microsoft Azure
  - VMWare NSX - Firewall SNS dans le rôle d'un routeur périphérique
  - ...

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



# Quiz

STORMSHIELD

Quelques questions pour auto-valider vos acquis :

Q1 - Quel est le mot de passe et le compte administrateur par défaut du SNS ?

- A. Login : admin, password : admin
- B. Login : root, password : password
- C. Login : admin, password : root
- D. Login : root, password : stormshield

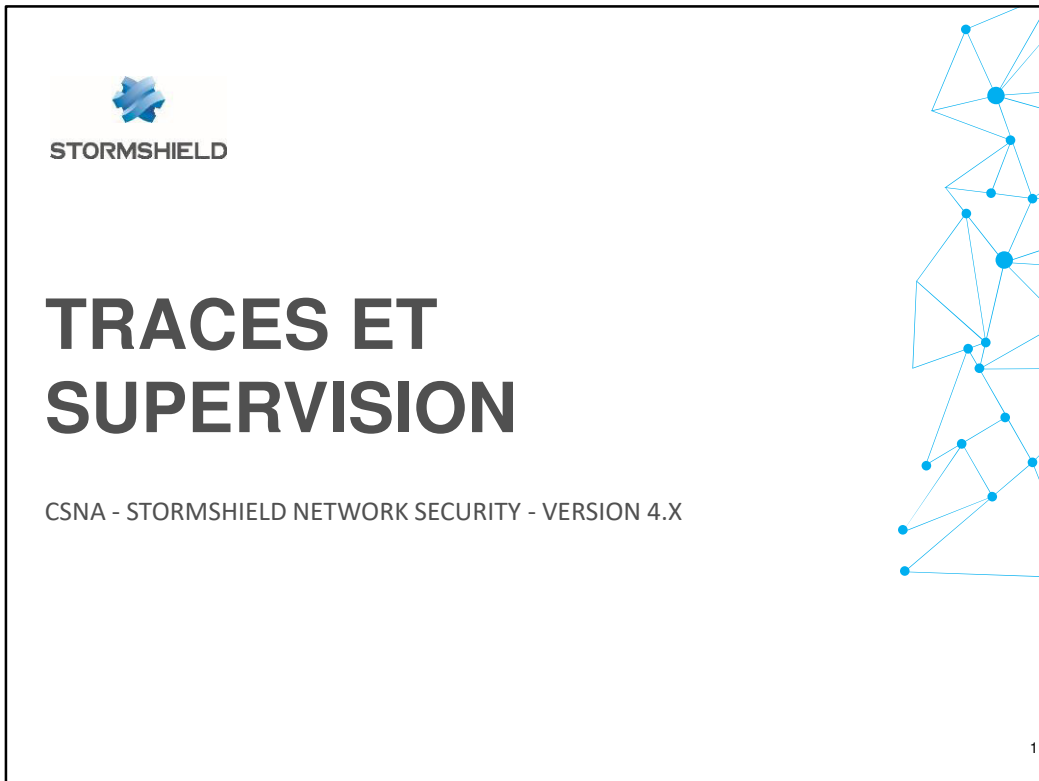
Q2 - Quelle est l'adresse IP par défaut du SNS ?

- A. 10.0.0.254/8
- B. 192.168.1.1/24
- C. 192.168.0.1/24
- D. 10.0.0.1/8

Q3 - En configuration usine, il est possible (si le matériel le supporte) de se connecter au firewall grâce :

- A. A un câble série
- B. Un écran utilisant une connexion HDMI ou VGA
- C. Une connexion SSH
- D. Une connexion HTTPS

Vous trouverez les réponses à la fin du support du document. Si vous avez besoin de plus de détails sur ces réponses, nous vous invitons à relire le cours.



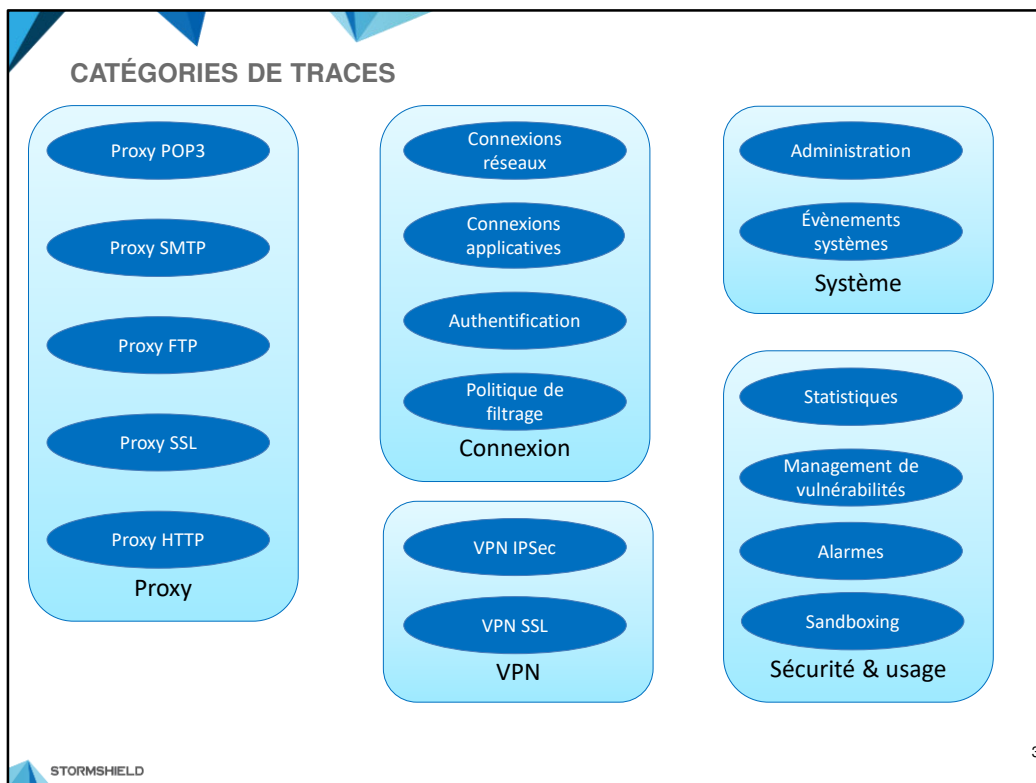
## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ➔ Traces et supervision
  - Les objets
  - Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Les catégories de traces

- Configuration et visualisation des traces
- Supervision et graphiques d'historiques
- Notifications et rapports supplémentaires
- Lab – Présentation de la plateforme de Lab
- Lab – Prise en main du firewall et traces



Les fonctionnalités et services d'un firewall Stormshield Network génèrent des événements qui sont stockés dans des fichiers journaux en local (sur le disque dur) ou sur une carte mémoire SD pour les firewalls de taille réduite disposant de l'option « stockage externe ». Les fichiers journaux sont organisés en plusieurs catégories décrites ci-dessous:

- **Administration** : Regroupe les événements liés à l'administration du firewall. Ainsi, toutes les modifications de configuration effectuées sur le firewall sont journalisées.
- **Authentification** : Regroupe les événements liés à l'authentification des utilisateurs sur le firewall.
- **Connexions réseaux**: Regroupe les événements liés aux connexions TCP/UDP traversant ou à destination du firewall non traitées par un plugin applicatif.
- **Évènements systèmes** : Regroupe les événements liés directement au système : arrêt/démarrage du firewall, erreurs système, allumage/extinction d'une interface, haute disponibilité, mises à jour Active Update, etc.
- **Alarmes** : Regroupe les événements liés aux fonctions de prévention d'intrusions (IPS) et les événements tracés avec le niveau alarme mineure ou majeure de la politique de filtrage et NAT.
- **Proxy HTTP** : Regroupe les événements liés aux connexions traversant le proxy HTTP.



- **Connexions applicatives (plugin):** Regroupe les événements liés aux connexions traitées par un plugin applicatif (HTTP, FTP, SIP, etc).
- **Proxy SMTP:** Regroupe les événements liés aux connexions traversant le proxy SMTP.
- **Politique de filtrage:** Regroupe les événements liés aux règles de filtrage et/ou de NAT, lorsque la journalisation des règles est en mode verbeux.
- **VPN IPSec:** Regroupe les événements liés à la phase de négociation d'un tunnel VPN IPSec.
- **VPN SSL:** Regroupe les événements liés à l'établissement de VPN SSL (mode tunnel ou portail).
- **Proxy POP3:** Regroupe les événements liés aux connexions traversant le proxy POP3.
- **Statistiques:** Synthèse des statistiques sur plusieurs éléments: système, sécurité, interfaces, QoS, etc.
- **Management de vulnérabilités:** Regroupe les événements liés à l'option « Stormshield Network Vulnerability Manager ».
- **Proxy FTP:** Regroupe les événements liés aux connexions traversant le proxy FTP.
- **Proxy SSL:** Regroupe les événements liés aux connexions traversant le proxy SSL.
- **Sandboxing:** Regroupe les événements liés à l'analyse sandboxing des fichiers lorsque cette option a été souscrite et activée.



- Les catégories de traces
- ➔ **Configuration et visualisation des traces**
- Supervision et graphiques d'historiques
- Notifications et rapports supplémentaires
- Lab – Présentation de la plateforme de Lab
- Lab – Prise en main du firewall et traces

## CONFIGURATION ET VISUALISATION DES TRACES

- Configuration du stockage local

LOCAL STORAGE SYSLOG IPFIX

**ON**

Do not eject the SD card when the log storage service is enabled. Reminder: you must disable log storage and apply the configuration before ejecting the SD card.

Storage device

Device: SD Card 7.46 GB Refresh Format

**CONFIGURATION OF THE SPACE RESERVED FOR LOGS**

Enable all	Disable all			
Enabled	Family	Percent.	Disk space quota	
<input checked="" type="checkbox"/>	Administration (server)	2	152.8 MB	
<input checked="" type="checkbox"/>	Authentication	2	152.8 MB	
<input checked="" type="checkbox"/>	Network connections	22	1.6 GB	
<input checked="" type="checkbox"/>	System events	1	76.4 MB	
<input checked="" type="checkbox"/>	Alarms	15	1.1 GB	
<input checked="" type="checkbox"/>	HTTP proxy	10	764.1 MB	
<input checked="" type="checkbox"/>	Application connections (plugin)	14	1 GB	
<input checked="" type="checkbox"/>	SMTP proxy	4	305.6 MB	
<input checked="" type="checkbox"/>	Filter policy	8	611.3 MB	
<input checked="" type="checkbox"/>	IPsec VPN	2	152.8 MB	
<input checked="" type="checkbox"/>	SSL VPN	2	152.8 MB	
<input checked="" type="checkbox"/>	POP3 proxy	3	229.2 MB	
<input checked="" type="checkbox"/>	Statistics	1	76.4 MB	
<input checked="" type="checkbox"/>	Vulnerability Manager	2	152.8 MB	
<input checked="" type="checkbox"/>	FTP proxy	4	305.6 MB	
<input checked="" type="checkbox"/>	SSL proxy	3	229.2 MB	
<input checked="" type="checkbox"/>	Sandboxing	1	76.4 MB	
<input checked="" type="checkbox"/>	Network captures	3	229.2 MB	
<input checked="" type="checkbox"/>	Router statistics	1	76.4 MB	

Total space used does not exceed available space (100%)

CANCEL APPLY

STORMSHIELD

6

Le stockage local des traces est géré dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Traces - Syslog - IPFIX** ⇒ dans l'onglet **STOCKAGE LOCAL**. Les fichiers journaux sont enregistrés sur le disque dur (si le firewall en est équipé) ou sur une carte mémoire SD (si le firewall dispose d'un emplacement prévu à cet effet et si l'administrateur a souscrit à l'option « stockage externe »). Chaque journal occupe un espace réservé sur le support de stockage. L'onglet est composé de:

- **Bouton ON/OFF** : Permet d'activer/désactiver l'enregistrement des journaux. Il est activé par défaut et tous les journaux sont actifs.
- **Support de stockage**: Permet de sélectionner le support de stockage disque dur interne ou carte mémoire SD.
- **Bouton Actualiser** : Actualise les supports de stockage disponibles.
- **Bouton Formater** : Permet de formater le support de stockage sélectionné.
- **Configuration de l'espace réservé pour les traces** : Permet d'activer ou de désactiver l'écriture des traces pour un journal donné en double-cliquant dans la colonne **État** correspondante. Elle permet également de configurer le pourcentage de l'espace disque réservé pour chaque journal dans la partie **Pourcentage**. Il est important de noter que le total des pourcentages ne doit pas dépasser 100%. La taille réelle de l'espace disque réservé à un journal est indiquée dans la partie **Quota d'espace disque**.

Les entrées de journal anciennes sont écrasées par les nouvelles entrées (rotation).

## CONFIGURATION ET VISUALISATION DES TRACES

- Visualisation des traces

The screenshot shows the Stormshield Network Security interface. The main area displays a table of logs with the following columns: Date, Action, User, Source Name, Destination Name, Destination Port, and Message. The logs are sorted by date, showing entries from 10:40:51 AM to 10:40:02 AM. A red box highlights the 'Actions' menu, and a green box highlights the 'Details de la ligne' menu. A blue box highlights the 'Columns' and 'Group by this field' options. A red arrow points from the 'Actions' menu to the 'Expand all the elements' option in the context menu.

Le menu **JOURNAUX D'AUDIT** dans la section **SUPERVISION** permet de visualiser les journaux sauvegardés en local sur le firewall, dans le cas où celui-ci dispose de disque dur (ou d'une carte mémoire SD avec l'option « stockage externe »), regroupés par famille de journaux : trafic réseau, alarmes, web, etc. Exemple : la famille **Trafic réseau** concatène les journaux : Connexions réseaux, filtrage, Proxy FTP, connexions applicatives, Proxy POP3, Proxy SMTP, Proxy SSL, Proxy HTTP, VPN SSL.

Les traces peuvent être limitées à une plage temporelle prédéfinie (dernière heure, aujourd'hui, dernière semaine ou dernier mois) ou personnalisée et sont affichées de la plus récente à la plus ancienne en haut de la liste.

Le nombre de colonnes affiché par défaut est limité. Cependant, toutes les colonnes peuvent être affichées en un clic grâce à l'option **Afficher tous les éléments** du menu **Actions** (encadré rouge). Pour ajouter manuellement une colonne à la fois, cliquez sur la flèche encadrée en bleu et ensuite sur « Colonnes ».

Pour voir l'ensemble des données relatives à une trace, mettez la ligne désirée en surbrillance et cliquez sur la flèche **Détails de la ligne** (encadré vert).

## CONFIGURATION ET VISUALISATION DES TRACES

- Filtre de recherche simple

LOG / NETWORK TRAFFIC

Last hour Refresh verbose Advanced search

SEARCH FROM - 08/23/2021 07:22:32 PM - TO - 08/23/2021 08:22:32 PM

Action	User	So	Source Name	De	Destination Name	Dest. Port Name	Protocol	Rule name
Allow		Anonymized			www.google.com		icmp	icmp_verbose

Search for this value in the "All logs" view

Check this host

Show host details

Blacklist this object

Add this value as a search criterion

Add the host to the objects base and/or add it to a group

Copy the selected line to the clipboard

Add the URL to a group

Go to the corresponding security rule

Add this value as a search criterion

Copy the selected line to the clipboard

Add the service to the objects base and/or add it to a group

Go to the corresponding security rule

ADD URL TO A GROUP

Characters allowed

\* , / , \_ [a-z] are allowed. URL examples:  
www.google.com/\*  
\*yahoo.com/\*

URL to add:

Comments:

GROUP TO WHICH THE OBJECT WILL BE ADDED:

Group:

STORMSHIELD 8

Un champ de recherche simple permet de filtrer les traces en recherchant une chaîne de caractères dans toutes les colonnes de toutes les traces. Dans l'exemple ci-dessus, les critères de recherche font partie du nom d'une règle de filtrage ICMP. Le résultat est affiché, que la colonne concernant les informations soit visible à l'écran ou pas.

En cliquant droit sur un élément d'une ligne de trace, une fenêtre s'affiche pour offrir des raccourcis vers plusieurs fonctionnalités qui diffèrent suivant le type d'élément choisi, dans l'exemple ci-dessus :

- Différentes options permettent de gérer l'objet de type URL, comme de l'ajouter à une liste d'URL définie par l'administrateur (encadrés bleu puis vert),
- ICMP (encadré rouge) peut être ajouté comme critère de recherche, qui remplacera le critère **verbose** dans l'exemple ci-dessus. Dans ce cas, la règle de filtrage correspondante peut être soulignée directement dans la politique de sécurité active.

Ces manipulations permettent à l'administrateur de s'appuyer sur les journaux pour affiner sa politique de sécurité, d'enrichir la base objets du firewall, et de vérifier la configuration effectuée de manière intuitive.

## CONFIGURATION ET VISUALISATION DES TRACES

- Filtre de recherche avancé

LOG / NETWORK TRAFFIC

Today Refresh No predefined filter Save Delete Simple search

FILTER SEARCH FROM - 08/23/2021 12:00:00 AM - TO - 08/23/2021 08:34:54 PM

Action	User	So	Source Name	De	Destination Name
Allow			Anonymized		dns1.google.com
Allow			Anonymized		dns1.google.com

Critère 1 :

NEW FILTER

Field: Destination Name (dstname)

Criterion: contains

Value: stormshield

CLOSE ADD APPLY

Critère 2 :

NEW FILTER

Field: Protocol (proto)

Criterion: equal to

Value: icmp

CLOSE ADD APPLY

Résultat :

LOG / NETWORK TRAFFIC

Today Refresh No predefined filter Save Delete Simple search

FILTER SEARCH FROM - 08/23/2021 12:00:00 AM - TO - 08/23/2021 08:37:12 PM

Action	User	So	Source Name	De	Destination Name	Dest. Port ...	Rule name
Allow			Anonymized		www.stormshield.eu		icmp_verbose

Destination Name contains stormshield

Protocol equal to icmp

ADD a criterion

La recherche avancée permet de créer des filtres complexes en combinant plusieurs critères de sélection.

Les filtres créés peuvent être enregistrés (bouton **Sauvegarder**), et réutilisés dans la même famille de journaux.

## CONFIGURATION ET VISUALISATION DES TRACES

- Accès restreint aux traces

- Accès complet aux traces

STORMSHIELD

10

Pour appliquer la nouvelle réglementation européenne sur les données personnelles, le RGPD (Règlement Général sur la Protection des Données), l'accès aux traces des firewalls SNS est restreint par défaut pour tous les administrateurs. Le super administrateur « admin », ainsi que les administrateurs disposant du droit « Accès aux données personnelles » peuvent accéder aux traces complètes en cliquant simplement sur [Traces : accès restreint..](#)

## CONFIGURATION ET VISUALISATION DES TRACES

- Création des codes d'accès temporaires pour un accès complet aux traces

The screenshot displays the 'TICKET CONFIGURATION' dialog box with the following fields:

- Start date: 07/22/2021 08:00:00 PM
- Valid until: 08/23/2021 12:00:00 AM
- Buttons: CANCEL (with a red X icon) and CREATE (with a blue checkmark icon)

Below the dialog box, the 'TICKET MANAGEMENT' table is visible. The table has the following columns and data:

Ticket ID	Valid from	Valid until	Code for access to private data
3G5R	07/22/2021 08:00:00 PM	08/23/2021 12:00:00 AM	3G5R7BG6F0ZUHLU9

The 'Add a ticket' button in the table is highlighted with a blue box, and a blue arrow points from it to the 'CREATE' button in the dialog box above.

Un administrateur n'ayant pas le droit « Accès aux données personnelles », peut également avoir un accès complet, grâce à un code d'accès temporaire, généré par un autre administrateur ayant le droit « Gestion des accès aux données personnelles ».

La création d'un code d'accès temporaire s'effectue dans le menu **CONFIGURATION** ⇒ **SYSTÈME** ⇒ **Administrateurs** ⇒ onglet **GESTION DES TICKETS**. Un ticket d'accès possède une date de début et une date de fin. Le ticket peut être copié et transmis à l'administrateur qui le renseigne dans la fenêtre qui s'affiche lorsqu'il clique sur le bouton **Accès restreint aux traces**

**NOTE** : un ticket peut être utilisé par plusieurs administrateurs.



- Les catégories de traces
- Configuration et visualisation des traces
- **Supervision et graphiques d'historiques**
- Notifications et rapports supplémentaires
- Lab – Présentation de la plateforme de Lab
- Lab – Prise en main du firewall et traces

## SUPERVISION ET GRAPHIQUES D'HISTORIQUES

## Graphiques et données en temps réel

The screenshot displays the 'MONITOR / HOSTS' interface with a 'REAL TIME' tab selected. It shows a table of hosts and a detailed view of connections.

Name	IP address	Interface	Rep.	Packets	Bytes in	Bytes out	Incoming bandwidth	Outgoing bandwidth	Count	Reputation
10.0.1.1	10.0.1.1	eth0	in	189121	127.43.948	27.17.948	4.03 MB/s	665.99 KB/s		

Date	Protocol	User	Source name	Destination No.	Dest. Port Name	Source interf.	Average thro...	Sent	Received	Duration	Last used	Gateway stat...	GeoLo...	Reputation...
11:36:24 AM	tcp		10.0.1.1	actinapoc001...	ephemeral_f...	in	117.35 KB/s	39.24 KB	29.34 KB	2s	5m 3s			
11:40:17 AM	tcp		10.0.1.1	pb-grip(grip...	http	in	80 kb/s	457 B	702 B	1m 10s	2s			
09:49:41 AM	tcp		10.0.1.1	actinapoc.g...	https	in	8 kb/s	2.14 KB	4.68 KB	10.51m 5s	42s			
11:40:57 AM	udp		10.0.1.1	youkubet(g...	https	in		3.35 KB	2.44 KB		23s			
11:40:27 AM	dns		10.0.1.1	DNS02	dns	in		38 B	55 B		1m 3s			
11:40:46 AM	tcp		10.0.1.1	redmine(gri...	http	in		350 B	1.29 KB		44s			
10:11:28 AM	tcp		10.0.1.1	www.socify.st...	https	in	8 kb/s	2.1 KB	5.22 KB	10.25m 5s	35s			
11:40:17 AM	dns		10.0.1.1	DNS02	dns	in		38 B	55 B		1m 13s			
11:40:17 AM	udp		10.0.1.1	youkubet(g...	https	in		3.49 KB	2.44 KB		1m 13s			
09:49:19 AM	tcp		10.0.1.1	actinapoc001...	ephemeral_f...	in		3.48 KB	341 B		55m 5s	57m 4s		
11:29:51 AM	udp		10.0.1.1	Firewall...	https	in	20.95 KB/s	221.08 KB	1.88 KB		12m 5s			

STORMSHIELD

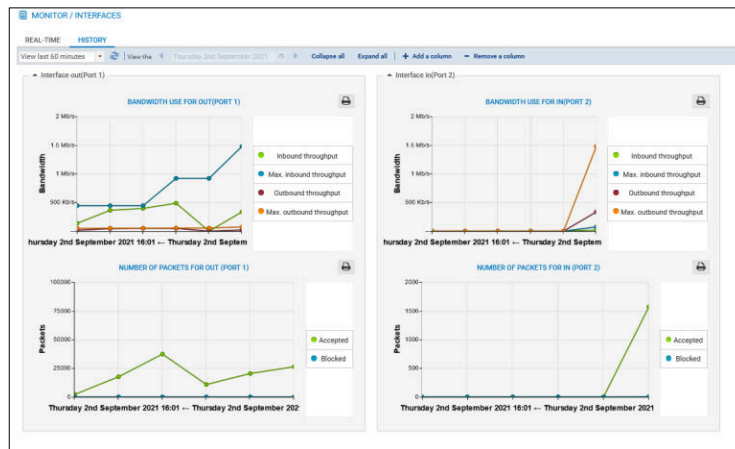
13

Le menu SUPERVISION permet de visualiser des graphiques et des données en temps réel organisés en 12 sous-menus :

- **Matériel/Haute disponibilité** : Température de la CPU, informations HA
- **Système** : Utilisation des ressources système du firewall,
- **Interfaces** : Utilisation des interfaces réseaux,
- **QoS** : Utilisation des files d'attente de la QoS,
- **Machines** : Machines génératrices de flux traversant le firewall,
- **Utilisateurs** : Utilisateurs authentifiés sur le firewall,
- **Connexions** : Connexions ouvertes au travers du firewall,
- **Routage** : Routes et passerelles réseau définies sur le firewall,
- **DHCP** : Baux IP attribués par le service DHCP,
- **Tunnels SSL VPN** : Utilisateurs connectés au firewall via VPN SSL,
- **Tunnels IPsec VPN** : Tunnels conformes à la politique du firewall,
- **Liste noire/Liste blanche** : Hôtes en quarantaine ou liste blanche sur le firewall.

## SUPERVISION ET GRAPHIQUES D'HISTORIQUES

- Consulter les graphiques d'historiques



En plus des graphiques en temps réel, quatre graphiques d'historiques sont accessibles si le bouton **Courbes historiques** est sur **ON** dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Configuration des rapports**. Les graphiques d'historiques concernent :

- La consommation CPU,
- L'utilisation de bande passante par interface,
- L'utilisation de la bande passante par file d'attente QoS,
- La réputation des machines.

À l'instar des rapports, les graphiques d'historiques peuvent être visualisés sur une période de temps configurable : dernière heure, jour choisi spécifiquement, 7 ou 30 derniers jours.

Des rapports supplémentaires sont disponibles et peuvent être activés un par un dans la section **LISTE DES RAPPORTS**.

**Attention : l'activation de rapports peut affecter les performances du firewall.**

## SUPERVISION ET GRAPHIQUES D'HISTORIQUES

- Configuration de la supervision

The screenshot shows the 'NOTIFICATIONS / MONITORING CONFIGURATION' page. It features three dropdown menus for configuring refresh intervals:

- Maximum period displayed (in minutes): 60
- Curve refreshment time (in seconds): 10
- Table refreshment time (in minutes): 5

Below these settings are two tabs: 'INTERFACES CONFIGURATION' and 'QOS CONFIGURATION'. The 'INTERFACES CONFIGURATION' tab is active, showing a table with two entries:

+ Add X Delete	
Name	
1	ethernet0
2	ethernet1

Certains paramètres de la supervision peuvent être configurés dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Configuration de la supervision**.

- **Intervalles de rafraîchissement :**
  - **Période maximale affichée (en minutes)** : La période de données à afficher pour une courbe (15, 30, 45 ou 60 minutes),
  - **Intervalle de rafraîchissement des courbes (en secondes)** : L'intervalle de rafraîchissement des courbes de supervision (5, 10, 15 ou 20),
  - **Intervalle de rafraîchissement des grilles (en minutes)** : L'intervalle de rafraîchissement des données de supervision présentées dans les grilles.

Le reste du menu est organisé en deux onglets :

- **CONFIGURATION DES INTERFACES** : Ajouter/supprimer les interfaces à superviser,
- **CONFIGURATION DE LA QOS** : Ajouter/supprimer les files d'attente à superviser.

## SUPERVISION ET GRAPHIQUES D'HISTORIQUES

- Configuration des graphiques d'historiques

NOTIFICATIONS / REPORT CONFIGURATION

General

Static reports:  OFF

History curves:  ON

Warning: Enabling reports may impact your firewall's performance.

LIST OF REPORTS    LIST OF HISTORICAL GRAPHS

Status	Description
<input checked="" type="checkbox"/> Enabled	Bandwidth use history
<input checked="" type="checkbox"/> Enabled	CPU consumption history
<input checked="" type="checkbox"/> Enabled	History of packets accepted / blocked per interface
<input checked="" type="checkbox"/> Enabled	Vulnerability history

Les graphiques d'historiques peuvent être activés dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Configuration des rapports** si le bouton **Courbes historiques** est sur ON et en activant par la suite les graphes souhaités dans l'onglet **LISTE DES GRAPHES D'HISTORIQUES**.

**NOTE:** Les rapports d'activités et les graphiques d'historiques sont disponibles sur les firewalls ne disposant pas de stockage local des journaux. Cependant, ils sont limités à 5 rapports et graphes au total avec un historique maximum de 7 jours.



- Les catégories de traces
- Configuration et visualisation des traces
- Supervision et graphiques d'historiques
- ➔ **Notifications et rapports supplémentaires**
- Lab – Présentation de la plateforme de Lab
- Lab – Prise en main du firewall et traces

## NOTIFICATIONS ET RAPPORTS SUPPLÉMENTAIRES

- **SYSLOG** : Envoi de traces vers des serveurs SYSLOG.
  - Il est possible d'activer jusqu'à 4 serveurs SYSLOG en même temps et 1 serveur de secours pour chacun d'eux en TCP.
- **SLS (Stormshield Log Supervisor)** : Solution de gestion de traces (SIEM). Elle collecte et analyse les données qui proviennent des firewalls.
- **Notifications par mails** : Transmission automatique de notifications par e-mail pour divers événements.
- **Rapports** : Calcul du top dix d'un événement.

Ces quatre fonctionnalités sont détaillées en annexe dans le module Traces et supervision.

## RECOMMANDATIONS

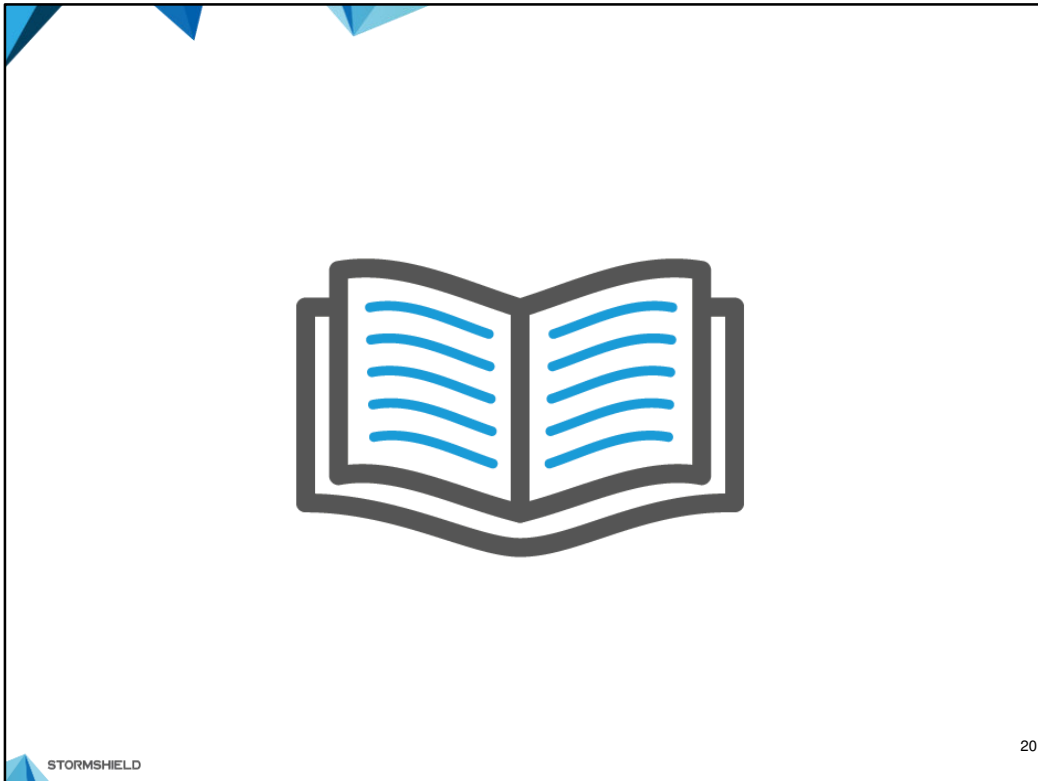


- Définir une politique de journalisation
  - Configurer un stockage de traces local
  - Configurer au moins un serveur syslog externe
  - Examiner périodiquement les traces
- Chiffrer le transfert par TLS entre le firewall et le serveur syslog externe
- Éviter le niveau de trace verbose sur la dernière règle de refus
- Utiliser du SNMPv3, chiffré
- Restreindre les requêtes SNMP aux seules machines de supervision via le filtrage

Une politique de journalisation solide garantit que ceux-ci sont protégés contre l'altération, et facilement accessibles pour le débogage.

Le stockage local est indispensable pour déboguer l'équipement. Le serveur externe sécurise l'accès aux traces et les protège d'une altération en cas de compromission de l'équipement.

Le SNMP doit être utilisé pour surveiller l'équipement tout en maintenant un niveau de sécurité maximum. Cela passe par la mise en place de règles de firewall spécifiques à ces flux.



Pour aller plus loin, consultez les notes techniques du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Description des journaux d'audit
- Se conformer aux règlements sur les données personnelles
- Intégrer les logs SNS dans IBM QRadar

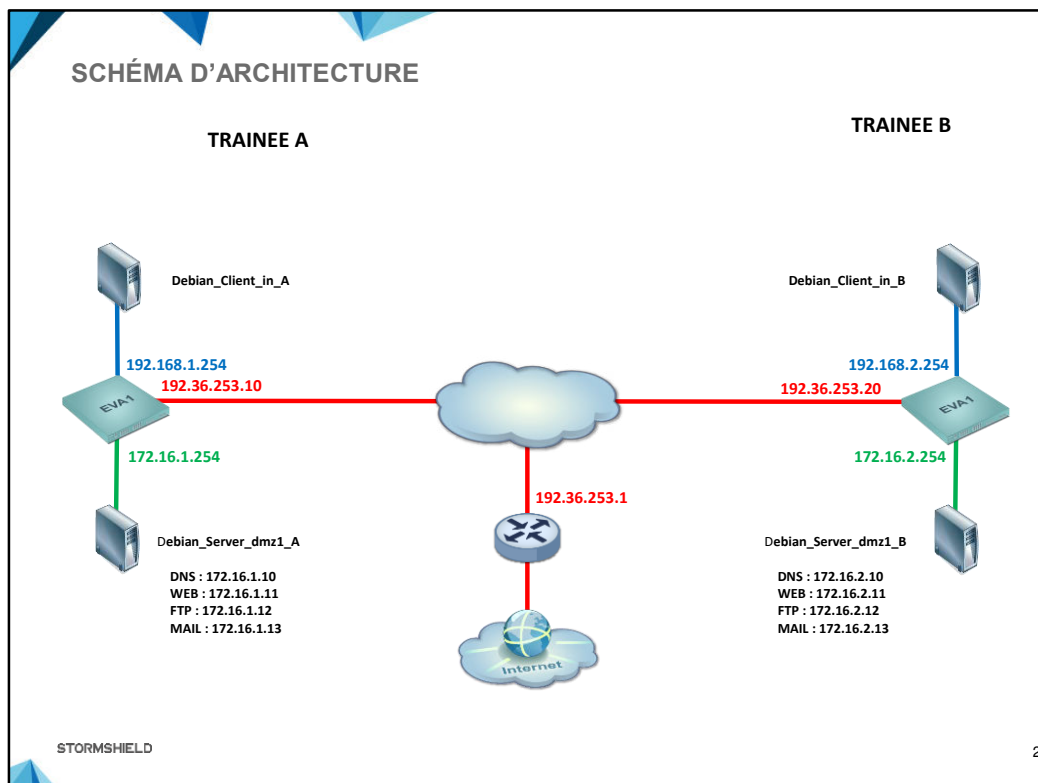
Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu)



- Les catégories de traces
- Configuration et visualisation des traces
- Supervision et graphiques d'historiques
- Notifications et rapports supplémentaires
- ➔ **Lab – Présentation de la plateforme de Lab**
- Lab – Prise en main du firewall et traces

STORMSHIELD

Prise en main du firewall

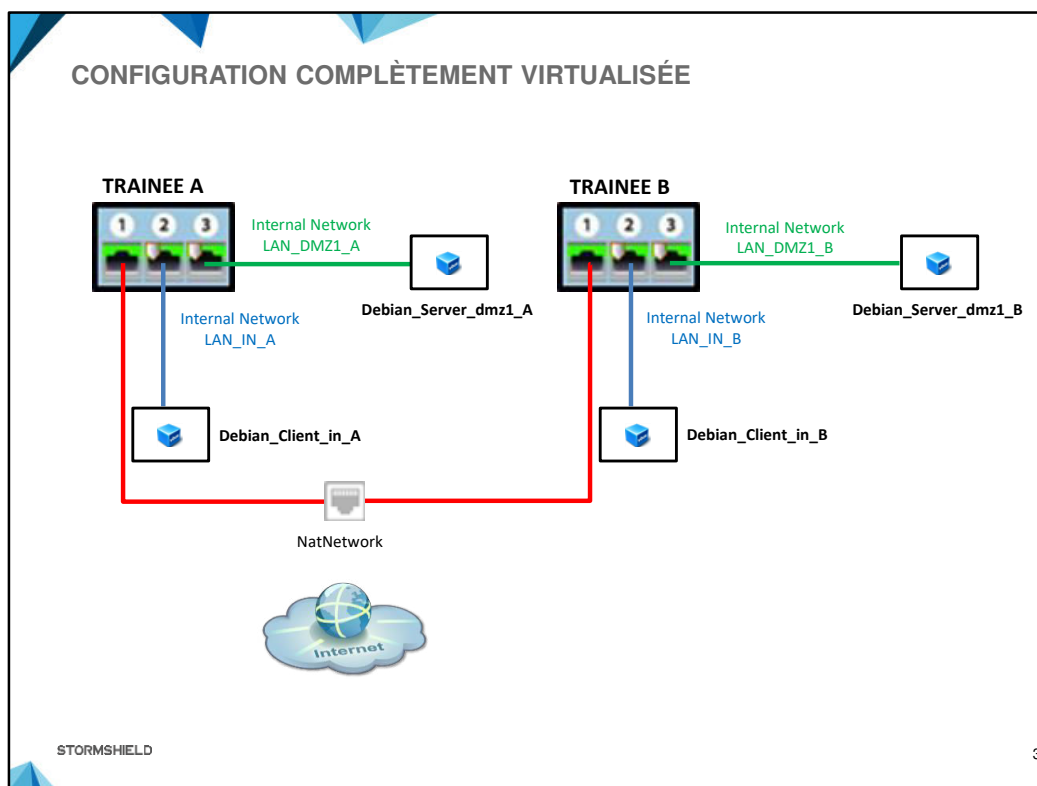


Les labs seront effectués en virtuel sous VirtualBox. La plateforme des labs est présentée ci-dessus, elle est constituée de 2 sites (Trainee A et Trainee B) reliés entre eux via un réseau externe « 192.36.253.0/24 ».

Chaque site possède :

- un firewall SNS\_EVA1\_V4.3,
- une machine Debian\_Training\_Webmail qui embarque 4 serveurs (DNS, WEB, FTP et MAIL), connectée au réseau privé DMZ « 172.16.X.0/24 »
- Une machine graphique Graphical\_client, connectée au réseau privé IN « 192.168.X.0/24 ».

**NOTE :** Sur tous les firewalls, le mot de passe de l'utilisateur « admin » est « admin ».



La configuration réseau des machines virtuelles est décrite sur la figure ci-dessus. Elle permet d'accéder à l'interface Web du firewall SNS d'un site depuis la machine graphique Graphical\_client. Elle permet également aux firewalls de se connecter à Internet via l'interface « NatNetwork ».

**NOTE :** Le réseau VirtualBox « NatNetwork » doit être créé et configuré avant de démarrer les machines virtuelles.

Les réseaux « Internal\_Networks » sont déployés par import de l'OVA.

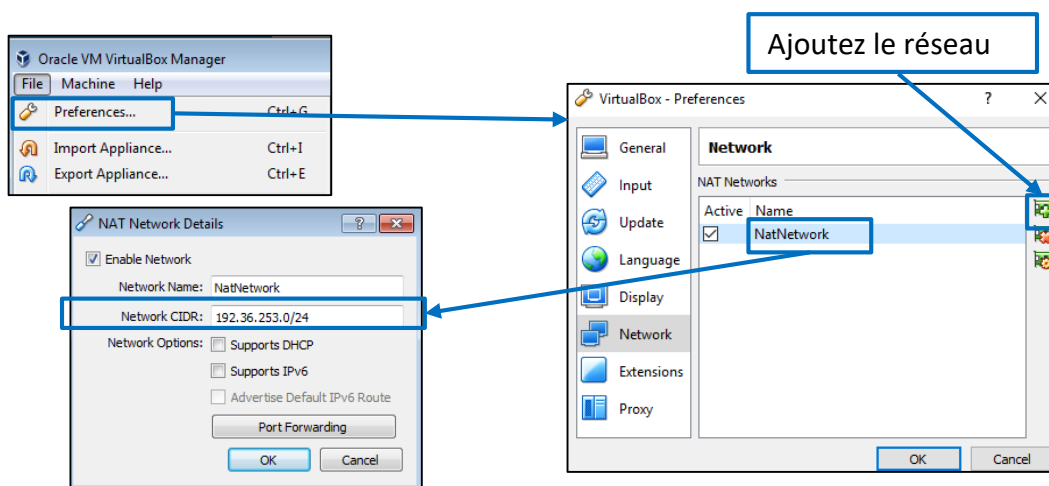
**PRÉREQUIS :** L'infrastructure virtuelle complète décrite ci-dessus nécessite un espace disque minimum de 11,5 Go (les VM fournies ont des disques à allocation dynamique) et une mémoire RAM de 4,2 Go :

- 1024 Mo de RAM par firewall,
- 96 Mo de RAM par Debian\_Server\_dmz1,
- 1024 Mo de RAM par Debian\_Client\_in, nous vous recommandons de multiplier cette valeur par 2, 3 ou 4 si la RAM disponible sur votre hôte physique le permet.

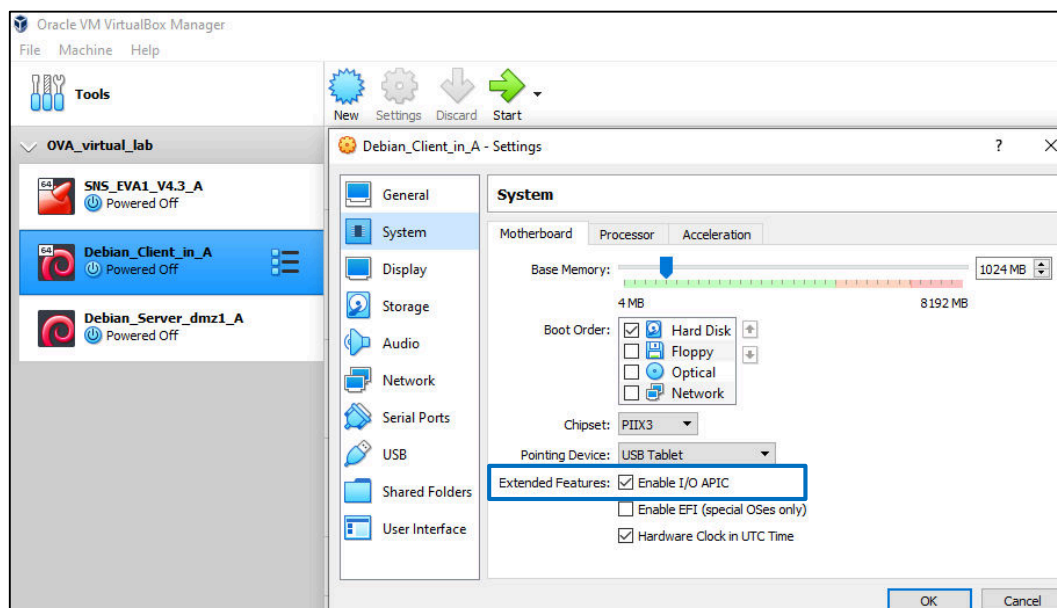


## Installation et préparation de la plateforme virtuelle

1. Installez Virtualbox (nos labs sont compatibles avec les versions 5.2 ou ultérieure, les captures d'écran ci-après ont été faites sur la version 6.1.34).
2. Créez l'interface « NatNetwork » depuis VirtualBox dans le menu Fichier ⇒ Paramètres ⇒ Réseau ⇒ onglet Réseau NAT, configurez la avec le réseau WAN « 192.36.253.0/24 » et désactivez l'option « supporte le DHCP ».

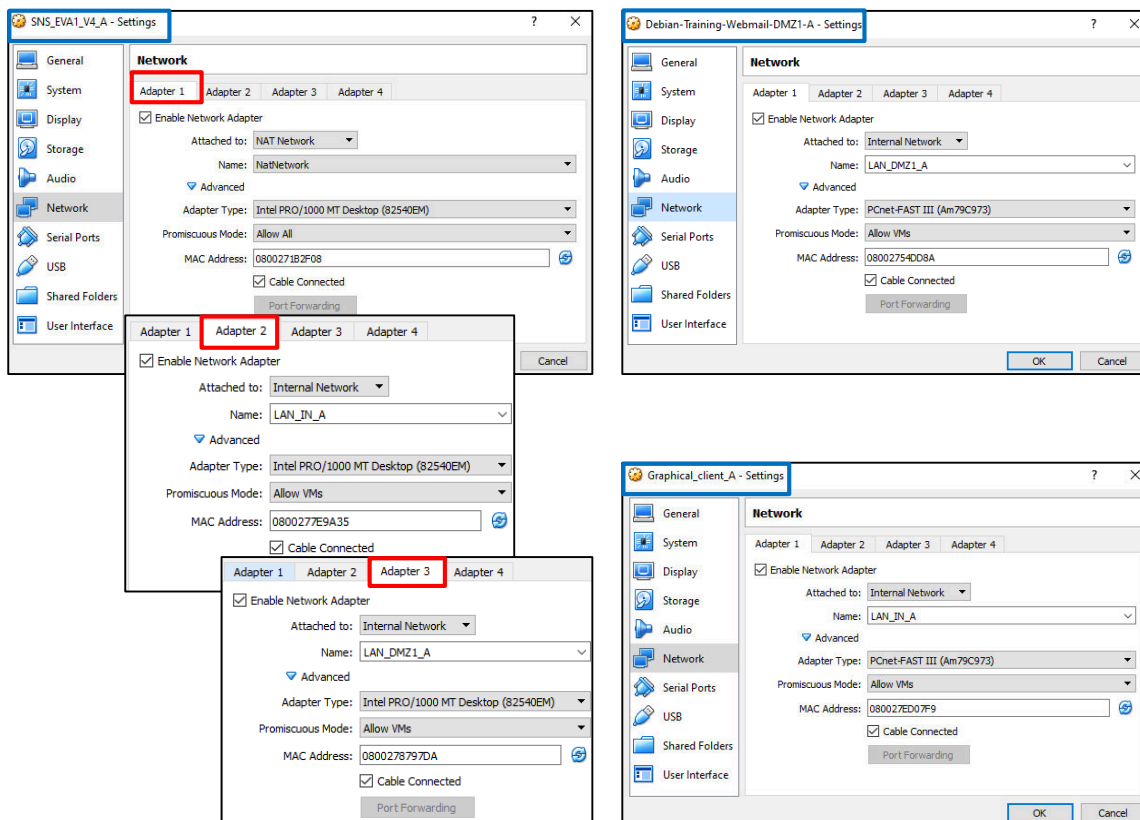


3. Importez le package « CSNx-v4.3-FW-DEBIANS.ova » contenant un firewall et les deux Debian, depuis le menu VirtualBox « Fichier ⇒ Importer un appareil virtuel » ⇒ cochez la case « Réinitialisez l'adresse MAC de chaque carte réseau ». Le Firewall est en configuration usine.
4. Pour un fonctionnement correct de la machine Graphical\_client, dans le menu Configuration ⇒ Système ⇒ Carte mère, cochez la case « Activer les IO-APIC », si elle ne l'est pas.

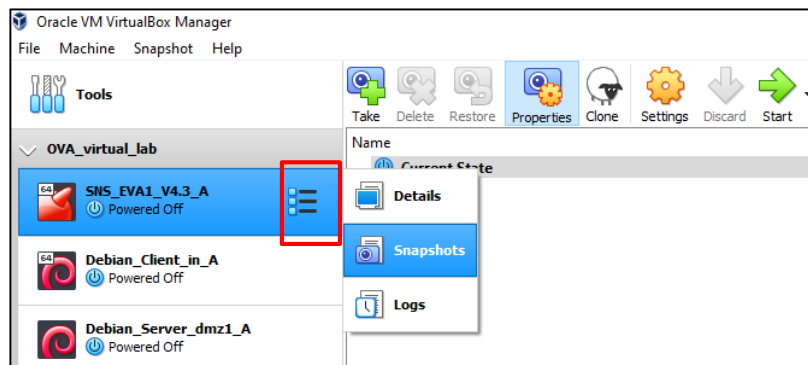




- 5. Vérifiez ou configurez les interfaces réseau des VM selon le schéma de la diapositive n°3. Ces machines sont sur le site de Trainee A.



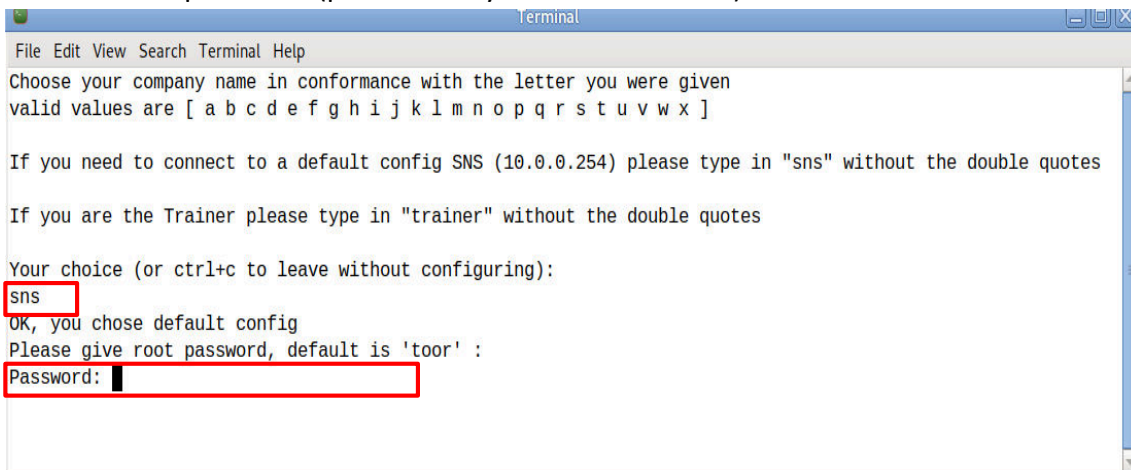
- 6. Clonez chaque VM, en cliquant droit sur une VM ⇒ Cloner. Dans l'assistant qui se lance, renommez votre clone (les VM clonées seront sur le site de Trainee B) et cochez la case « Réinitialisez l'adresse MAC de chaque carte réseau ». Sur la page suivante, cochez la case « Clone intégral » et cliquez sur le bouton cloner (au lieu de cloner, il est également possible d'importer à nouveau le package OVA, le renommage des VM s'effectue alors après import).
- 7. Modifiez les interfaces réseau pour les 3 machines clonées, LAN\_IN\_A et LAN\_DMZ1\_A sont renommées respectivement LAN\_IN\_B et LAN\_DMZ1\_B.
- 8. Effectuez un instantané de chaque VM avant de commencer les labs (avec Oracle VirtualBox, faites l'instantané VM éteinte).





- Démarrez les VM « SNS\_EVA1\_V4\_A » et « Graphical\_client ». Sur cette dernière, double cliquez sur le raccourci bureau «network\_config.sh », puis cliquez sur le bouton « Run in Terminal ». Le firewall SNS étant encore en mode usine, l'option « sns » doit être choisie.

Note : Si l'une des machines ne démarre pas, le passage à 2 CPU peut parfois résoudre ce problème (paramètre System -> Processor.)



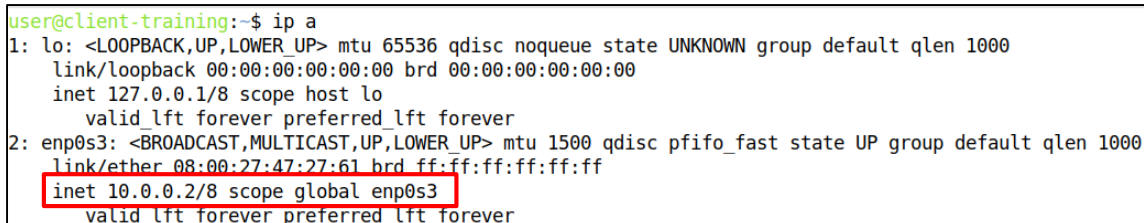
```
Terminal
File Edit View Search Terminal Help
Choose your company name in conformance with the letter you were given
valid values are [ a b c d e f g h i j k l m n o p q r s t u v w x ]

If you need to connect to a default config SNS (10.0.0.254) please type in "sns" without the double quotes

If you are the Trainer please type in "trainer" without the double quotes

Your choice (or ctrl+c to leave without configuring):
sns
OK, you chose default config
Please give root password, default is 'toor' :
Password: 
```

En lançant un terminal, vous pouvez vérifier que l'IP de votre carte réseau est correcte avec la commande « ip address show » (format raccourci « ip a »), et lancer un ping vers 10.0.0.254 (la connectivité avec le SNS est bien établie).



```
user@client-training:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:47:27:61 brd ff:ff:ff:ff:ff:ff
   inet 10.0.0.2/8 scope global enp0s3
       valid_lft forever preferred_lft forever
```

- Recommencez les points 8 et 9 avec les VM du site B.



Nous vous invitons à imprimer et compléter cette page afin d'avoir les informations des Labs à disposition.

### Informations

Les labs seront effectués à l'aide d'une infrastructure composée de plusieurs sites. Chaque site représente ici une compagnie qui possède trois machines :

- Un poste client Windows permettant de naviguer sur Internet et configurer le SNS
- Un firewall Stormshield Network Security (SNS) virtuel (EVA) ou physique (SN310)
- Un serveur Debian qui embarque 4 serveurs (DNS, WEB, FTP et MAIL)

Les compagnies sont nommées par une lettre A, B, C, D, etc. et un chiffre, respectivement 1, 2, 3, 4, etc. qui servira dans la définition des adresses IP.

Deux réseaux privés (net-in-x et net-dmz-x, où x représente la lettre du site) sont configurés sur chaque site : IN « 192.168.y.0/24 » et DMZ : « 172.16.y.0/24 » (où y représente le numéro associé à la compagnie).

Les différents sites sont reliés directement à Internet et possèdent des adresses IP publiques dans la plage 192.36.253.10 à 192.36.253.249. Le reste d'Internet est accessible via le firewall du formateur dont l'adresse IP est 192.36.253.254.

### Adresses IP

Je suis compagnie \_\_\_\_\_ (lettre) numéro \_\_\_\_\_.



#### Serveurs Debian

Serveur DNS :

\_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.10

Serveur web :

\_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. 11

Serveur FTP :

\_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. 12

Serveur mail :

\_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. 13



#### Firewall Stormshield

Adresse IP net-DMZ :

172.16.\_\_\_\_\_.254

Adresse IP publique :

192.36.253 .\_\_\_\_\_.0

Adresse IP net-IN :

192.168 .\_\_\_\_\_. 254



#### Poste client

Adresse IP :

192.168 .\_\_\_\_\_. 2



- Les catégories de traces
- Configuration et visualisation des traces
- Supervision et graphiques d'historiques
- Notifications et rapports supplémentaires
- Lab – Présentation de la plateforme de Lab
- ➔ **Lab – Prise en main du firewall et traces**

STORMSHIELD

Prise en main du firewall



## Lab 1 – Prise en main du Firewall et traces

1. Connectez-vous à l'interface d'administration web (les firewalls « Trainee » sont en configuration usine).
2. Modifiez vos préférences pour ne jamais être déconnecté en cas d'inactivité sur l'interface d'administration. Les préférences se trouvent dans le menu déroulant, accessible en cliquant sur la flèche à droite du nom d'utilisateur, en haut à droite de l'en-tête.
3. Paramétrez la langue (traces et clavier) et le fuseau horaire de votre firewall. Redémarrez le firewall pour que le nouveau fuseau soit pris en compte (icône en haut à droite). Puis mettez votre firewall à l'heure après le redémarrage.
4. Activez le service SSH avec l'authentification par mot de passe.
5. Vérifiez la validité de votre licence et des éventuelles options disponibles, configurez la mise à jour automatique de votre licence avec une vérification hebdomadaire dans les options avancées.
6. Modifiez le mot de passe de l'utilisateur « admin » (il faut choisir un mot de passe d'au moins 8 caractères, sans caractère spécial). Rafraîchissez la page pour vous reconnecter et tester le nouveau mot de passe.
7. Vérifiez que le stockage local des logs est activé sur le disque dur de la VM. Réallouez le quota d'espace disque de la catégorie « Proxy POP3 » à la catégorie « Connexions réseau », puis la désactiver. Activez tous les autres logs.
8. Faites une sauvegarde de la configuration et téléchargez-la sur le poste d'administration. Prenez l'habitude de sauvegarder la configuration à la fin de chaque lab.

### NOTES :

- Pour permettre le bon fonctionnement de chaque lab, vous devez effectuer les configurations demandées sur le site A, puis sur le site B.
- La machine Debian\_Client\_in contient une sauvegarde des labs, pour les sites A et B, dans le dossier /home/user/Documents.
- Lors des labs, si vous levez une alarme « Attaque possible des ressources (connexion) », c'est que vous avez atteint le nombre de connexions maximum autorisé par la licence de la VM pédagogique. Dans ce cas, toutes les nouvelles connexions sont bloquées, patientez quelques minutes, le temps que la table des connexions se purge, pour revenir à un comportement normal.



# Quiz

STORMSHIELD

Q1 – Quelles sont les assertions vraies :

- A. Les pare-feux SNS ne peuvent pas stocker de logs en local.
- B. Il est possible de stocker les logs sur une clef USB connectée au firewall.
- C. 4 serveurs syslog peuvent être configurés, ainsi que 4 serveurs de secours.

Q2 - Par défaut, les logs n'affichent pas les adresses IP de destination à cause de la RGPD.

- A. Vrai
- B. Faux

Q3 - Tous les administrateurs peuvent avoir accès aux informations personnelles dans les log à partir du moment où ils ont un mot de passe temporaire d'accès.

- A. Vrai
- B. Faux

Q4 - Le protocole syslog est utilisable uniquement chiffré avec TLS sur les firewalls Stormshield :

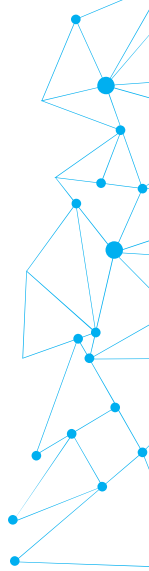
- A. Vrai
- B. Faux



STORMSHIELD

# ANNEXE – TRACES ET SUPERVISION

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



## Activation du syslog

- Stormshield Log Supervisor (SLS)
- Notification par email
- Rapports

STORMSHIELD

Traces et supervision

## ACTIVATION DU SYSLOG

The diagram illustrates the Syslog configuration process. On the left, a Stormshield firewall labeled 'Client Syslog' is shown sending data to three server racks labeled 'Serveurs Syslog'. On the right, a screenshot of the Stormshield web interface shows the 'NOTIFICATIONS / LOGS - SYSLOG - IPFIX' configuration page. The 'SYSLOG PROFILES' table lists four profiles: 'Alarms Syslog Server' (Enabled), 'Users Syslog Server' (Enabled), 'Syslog Profile 2' (Disabled), and 'Syslog Profile 3' (Disabled). The 'Details' panel for the 'Alarms Syslog Server' profile shows the following configuration:

- Name: Alarms Syslog Server
- Comments: (empty)
- Syslog server: srv\_syslog\_alarms
- Protocol: TCP
- Port: syslog-conn
- Certificate authority: (empty)
- Server certificate: (empty)
- Client certificate: (empty)
- Format: RFC5424
- Advanced properties:
  - Backup server: (empty)
  - Backup port: syslog-conn
  - Category (facility): none

Below the details, the 'LOGS ENABLED' section shows a table with columns 'Enable all' and 'Disable all':

Status	Name
Enabled	Alarms
Disabled	Network connections
Disabled	Filter policy

STORMSHIELD

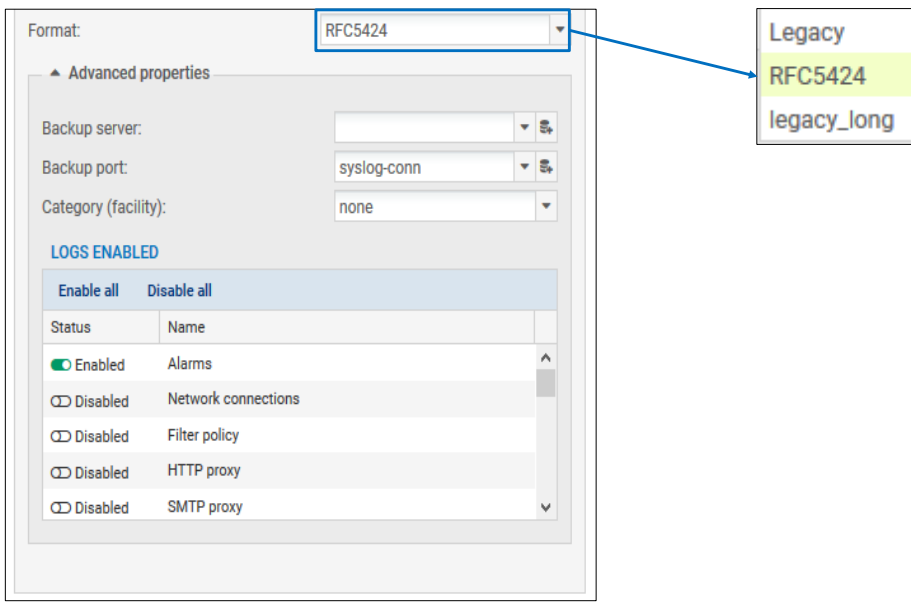
3

Les firewalls Stormshield Network embarquent un client SYSLOG qui peut être activé pour transmettre des traces vers des serveurs SYSLOG externes. Il est possible d'activer jusqu'à 4 serveurs SYSLOG en même temps en personnalisant le protocole de transmission, le format et les catégories de traces pour chaque serveur.

La configuration de ces serveurs s'effectue dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Traces - Syslog - IPFIX** ⇒ onglet **SYSLOG** (un serveur par profil). Dans chaque profil, vous pouvez configurer les paramètres suivants :

- **Nom** : du profil syslog,
- **Commentaire** (facultatif),
- **Serveur Syslog** : objet machine portant l'adresse IP du serveur Syslog,
- **Protocole** : utilisé pour la transmission des traces : UDP, TCP et TLS,
- **Port** : de destination, utilisé pour la transmission des traces. Les ports standards : syslog (UDP/514), syslog-conn (TCP/601), syslog-tls (TCP/6514),
- **Autorité de certification (obligatoire)** : Le certificat de la CA qui a signé les certificats du firewall et du serveur Syslog,
- **Certificat serveur (optionnel)** : le certificat qui doit être présenté par le serveur Syslog pour s'authentifier auprès du firewall,
- **Certificat client (optionnel)** : le certificat qui doit être présenté par le firewall pour s'authentifier auprès du serveur Syslog,

### ACTIVATION DU SYSLOG



Format: RFC5424

Advanced properties

Backup server: [ ]

Backup port: syslog-conn

Category (facility): none

LOGS ENABLED

Enable all	Disable all	Status	Name
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enabled	Alarms
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Network connections
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Filter policy
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	HTTP proxy
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	SMTP proxy

STORMSHIELD

- **Format** : Le format syslog utilisé :
  - LEGACY : limité à 1024 caractères par message syslog.
  - LEGACY-LONG : Le message syslog n'est pas limité.
  - RFC5424 : respectant le format défini par la RFC 5424.
- Dans l'encadré **configuration avancée**, les paramètres suivants peuvent être configurés :
  - **Serveur de secours**,
  - **Port de secours**,
  - **Catégorie (facility)** : identifiant ajouté au début d'une ligne de trace pour identifier un firewall dans le cas où le serveur Syslog reçoit les traces de plusieurs firewalls,
  - **TRACES ACTIVÉES** : permet de sélectionner les catégories de traces qui seront transmises au serveur SYSLOG en double cliquant sur la partie **État** de chaque famille pour activer ou désactiver l'envoi.

#### NOTE :

- Les paramètres Autorité de certification, Certificat serveur et Certificat client sont activés seulement si le protocole TLS est sélectionné.
- Les paramètres Serveur de secours et Port de secours peuvent être utilisés seulement si les protocoles TCP ou TLS sont sélectionnés.



- Activation du syslog
- ➔ **Stormshield Log Supervisor (SLS)**
- Notification par email
- Rapports

STORMSHIELD

Traces et supervision



Stormshield Log Supervisor est une solution de gestion de traces. Elle collecte les données de streaming qui proviennent des firewalls Stormshield Network Security, les analyse, et fournit des aperçus de vos données en temps réel. SLS permet un contrôle strict des réseaux d'entreprise distribués depuis un seul emplacement et offre des capacités de synthétisation des risques sous-jacents liés aux attaques distribuées complexes sur les réseaux de grande taille.

Stormshield Log Supervisor peut être déployé sur deux environnements virtuels :

- VMware ESXi avec le Stormshield Log Supervisor OVA,
- Microsoft Hyper-V avec le Stormshield Log Supervisor Hyper-V VHD.

Pour plus d'informations sur SLS, consultez le manuel d'utilisation et nos guides de déploiement pour OVA ou Hyper-V VHD sur le site Web de documentation technique de Stormshield à l'adresse <https://documentation.stormshield.eu>



- Activation du syslog
- Stormshield Log Supervisor (SLS)
- **Notification par email**
- Rapports

STORMSHIELD

Traces et supervision

## NOTIFICATION PAR E-MAIL

NOTIFICATIONS / E-MAIL ALERTS

CONFIGURATION RECIPIENTS TEMPLATES

RECIPIENT GROUPS

New recipient group Remove Check use

Group name	Comments
SNS_Admins	

Recipients of group: SNS\_Admins

Add new recipient to group Remove

it_management@training.eu
admin_sns@training.net

Cancel Apply

STORMSHIELD

8

Les firewalls Stormshield Network peuvent transmettre automatiquement des notifications par e-mail pour divers événements. La configuration de cette fonctionnalité s'effectue dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Alertes e-mails**.

Commençons par configurer les utilisateurs et/ou les groupes destinataires des notifications.

L'onglet **DESTINATAIRES** permet la création et la configuration de listes de diffusion. Les destinataires d'un groupe peuvent être des adresses e-mail ou des utilisateurs enregistrés dans la base LDAP. Dans ce cas, vérifiez que les utilisateurs ont saisi leurs adresses e-mail au sein de leurs identités LDAP.

## NOTIFICATION PAR E-MAIL

The screenshot shows the 'NOTIFICATIONS / E-MAIL ALERTS' configuration page. It has three tabs: 'CONFIGURATION', 'RECIPIENTS', and 'TEMPLATES'. The 'CONFIGURATION' tab is active. A checkbox labeled 'Enable e-mail notifications' is checked. Below this is the 'SMTP server' section with the following fields:

- Server: dropdown menu with 'srv\_mail\_priv' selected.
- Port: dropdown menu with 'smtp' selected.
- E-mail address: text input field containing 'VMSNSX09K0639A9@training.net'.
- Authentication: unchecked checkbox.
- ID: empty text input field.
- Password: empty text input field.

At the bottom of the configuration area is a button labeled 'Testing the SMTP configuration'.

STORMSHIELD

9

L'onglet **CONFIGURATION** contient les paramètres suivants:

- **Activer les notifications par e-mail** : Activer/désactiver le service,
- **Serveur SMTP** : Permet de configurer tous les paramètres en relation avec le serveur vers lequel les e-mails seront transmis (adresse IP, port, informations d'authentification et nom de domaine). L'adresse e-mail de l'émetteur des notifications par défaut est « nomdufirewall@Domaine\_DNS ».

## NOTIFICATION PAR E-MAIL

NOTIFICATIONS / E-MAIL ALERTS

CONFIGURATION RECIPIENTS TEMPLATES

E-mail sending frequency (in minutes)

Sending frequency : 15

Intrusion prevention alarms

Do not send any e-mails  
 Send according to alarm and event settings  
 Send only major alarms  
 Send major and minor alarms

Message recipient : SNS\_Admins

System events

Do not send any e-mails  
 Send according to alarm and event settings  
 Send only major alarms  
 Send major and minor alarms

Message recipient : SNS\_Admins

Cancel Apply

STORMSHIELD

10

- **Fréquence d'envoi** Indique la fréquence d'envoi des notifications. La valeur doit être comprise entre 1 et 1000 minutes.
- **Alarmes de prévention d'intrusion** et **Évènements systèmes** : permet de sélectionner les informations envoyées dans les notifications concernant les catégories de traces « Alarmes » et « Évènements systèmes » :
  - ne rien envoyer,
  - envoyer uniquement les alarmes majeures,
  - envoyer les alarmes majeures et mineures.

Une des listes de diffusion préalablement créée est utilisée ici.

## NOTIFICATION PAR E-MAIL

NOTIFICATIONS / E-MAIL ALERTS

CONFIGURATION    RECIPIENTS    **TEMPLATES**

- ▼ Vulnerability Manager
  - Detected Vulnerabilities (detailed)
  - Detected Vulnerabilities (summary)
- ▼ Certificate request
  - Approved certificate
  - Rejected certificate
- ▼ User enrolment
  - User enrolment approved
  - User enrolment rejected
- ▼ Sponsorship method
  - Sponsorship request**
- ▼ smtp\_conf
  - Test SMTP configuration

Edit

Sponsoring request

Hello,  
The user John Doe on 192.168.0.1 just asked you to sponsor him.  
Connection timeout: 60 mins  
In order to accept, please click on the following link: [Accept](#)

Have a nice day.

STORMSHIELD

11

L'onglet **MODÈLES** permet également de personnaliser le contenu des e-mails envoyés pour différents évènements, autres que la gestion des alarmes vue préalablement. Le corps des messages peut contenir des paramètres (\$URL, \$UID, etc) qui seront remplacés par des valeurs suivant le contexte de l'évènement.



- Activation du syslog
- Stormshield Log Supervisor (SLS)
- Notification par email

 **Rapports**

STORMSHIELD

Traces et supervision

## RAPPORTS

**NOTIFICATIONS / REPORT CONFIGURATION**

General

Static reports:  ON

History curves:  ON

Warning: Enabling reports may impact your firewall's performance.

**LIST OF REPORTS**    LIST OF HISTORICAL GRAPHS

Search...    in the categories: All     Set status to on    Reset the database

Status	Category	Description	Warning	Private data
<input type="checkbox"/> Disabled	Security	Detection rate by analytics engine (Sandboxing,...		
<input type="checkbox"/> Disabled	Spam	Ratio of spam emails received		
<input type="checkbox"/> Disabled	Network	Top hosts per exchanged volume		<input type="checkbox"/>
<input checked="" type="checkbox"/> Enabled	Network	Top protocols per exchanged volume		
<input type="checkbox"/> Disabled	Network	Top users per exchanged volume	Authentication is disabled	<input type="checkbox"/>
<input type="checkbox"/> Disabled	Network	Top client applications per exchanged volume		
<input type="checkbox"/> Disabled	Network	Top server applications per exchanged volume		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top EtherNet/IP servers per exchanged volume		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top IEC 60870-5-104 servers per exchanged vo...		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top Modbus servers per exchanged volume		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top OPC UA servers per exchanged volume		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top S7 servers per exchanged volume		
<input type="checkbox"/> Disabled	Industrial Netwo...	Top UMAS servers per exchanged volume		
<input type="checkbox"/> Disabled	Web	Top Web categories per exchanged volume	URL Filtering is disabled	
<input type="checkbox"/> Disabled	Web	Top Web domains per exchanged volume		

Enabled reports : 5 on 30    Database size : 108 KB

STORMSHIELD

13

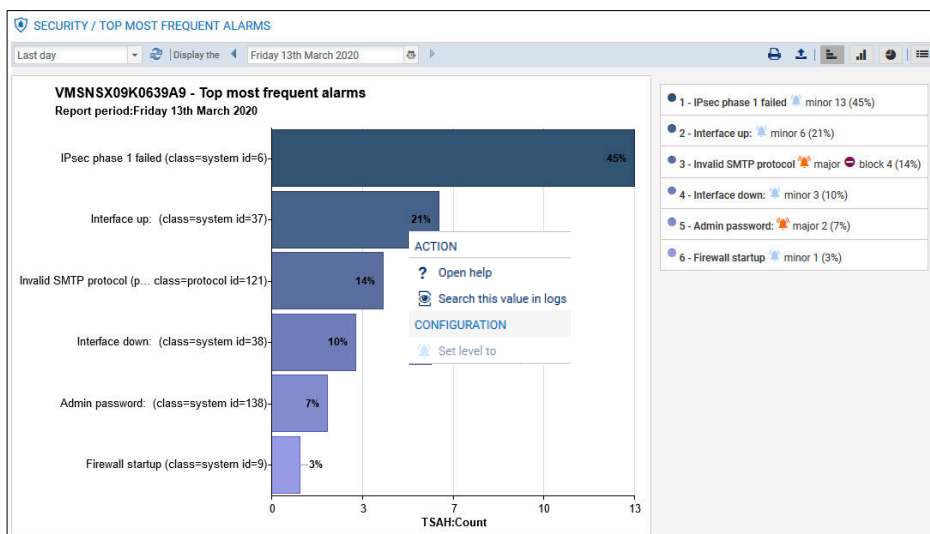
Les rapports sont calculés à partir des fichiers de traces et sont stockés dans une base de données. Le calcul prend en considération seulement les traces depuis l'activation du rapport, l'historique des traces n'est pas considéré.

Le firewall propose par défaut 30 rapports organisés en 8 catégories: spam, réseau, web, sécurité, vulnérabilité, virus, réseaux industriel et sandboxing.

La configuration des rapports s'effectue dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Configuration des rapports**. Par défaut, la fonctionnalité est désactivée, il faut cocher l'option **Activer les rapports** dans l'encadré **Général** pour l'activer.

Par la suite, vous pouvez choisir les rapports à activer/désactiver dans l'onglet **LISTE DES RAPPORTS** en double cliquant sur le champ « **État** » d'un rapport.

## RAPPORTS



STORMSHIELD

14

La consultation des rapports s'effectue dans le menu **RAPPORTS**.

Un rapport calcule les statistiques des 50 évènements les plus importants durant la plage temporelle choisie « dernière heure, vue par jour, 7 ou 30 dernier jours ». Cependant, la page affiche seulement les 10 premiers évènements (top 10) parmi ces 50. Le reste des évènements (du 11<sup>ème</sup> au 50<sup>ème</sup>) sont regroupés dans la catégorie « Autres ».

L'affichage est effectué en deux formats :

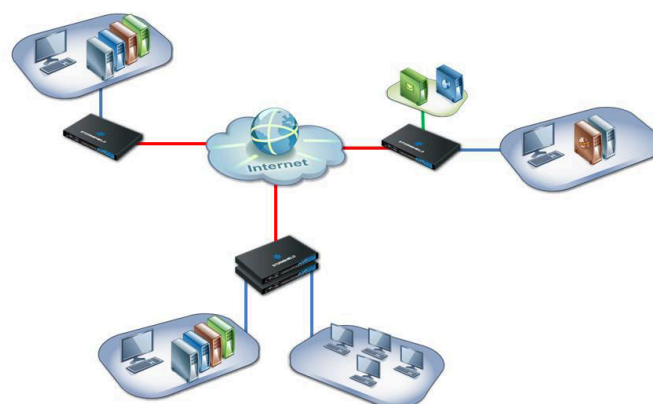
- **Un graphique** : sous la forme d'un histogramme (horizontal ou vertical) ou d'un camembert.
- **Une liste** : ordonnée des statistiques en pourcentage et en chiffres réels du nombre d'évènements.

Depuis certains rapports (par exemple les alarmes), il est possible de modifier des éléments de la configuration en effectuant un simple clic sur la ligne concernée. Par exemple, le niveau de trace ou l'action associés à une alarme sont modifiables directement depuis cet outil, à condition d'avoir le droit d'écriture sur la session en cours.

Enfin, l'interface permet de télécharger le rapport dans un fichier au format « CSV » ou l'imprimer.



ADVANCED LAB – MISE EN PLACE DE L'INFRASTRUCTURE  
ADVANCED LAB – RAPPORTS EMBARQUÉS



STORMSHIELD

15

Advanced Labs disponibles à la fin du support de cours.



## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- Les objets
  - Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Généralités

- Les objets réseaux
- Lab – Les objets

STORMSHIELD

Les objets

## GÉNÉRALITÉS

- Un objet :
  - Représente/porte une valeur (adresse IP, URL, événement temporel,...)
  - Possède un nom et une description
- Les objets sont utilisés pour configurer les paramètres des fonctionnalités :
  - Manipuler des noms d'objets, plus parlant que des valeurs
  - Simplifier la modification des valeurs
- 3 familles d'objets :
  - Réseaux
  - URL (ou Objets Web jusqu'à la version 4.3.10)
  - Certificats et PKI

Les menus de configuration des firewalls Stormshield Network utilisent la notion d'objets qui représentent des valeurs (adresse IP, adresse réseau, URL, événement temporel, etc.). L'utilisation d'objets au lieu de valeurs présente deux avantages majeurs :

1. Cela permet à l'administrateur de manipuler des noms, plus parlants que des valeurs.
2. Dans le cas où une valeur change, il suffira de modifier la valeur de l'objet sans se rendre dans tous les menus où l'objet est utilisé.

Les objets sont classés en 3 familles :

1. **Objets Réseaux** : Regroupe tous les objets en relation avec les valeurs réseaux (adresse IP, numéro de port, numéro de protocole, etc.) et les objets temps.
2. **URL** (ou **Objets Web** jusqu'à la version 4.3.10) : Groupes d'URL (ou groupes de catégories) et groupes de noms de certificats.
3. **Certificats et PKI** : Permet la création et la gestion des autorités de certification et de toutes les identités (de type serveur, utilisateur, ou smartcard) qui en découlent.

Dans ce module, nous nous intéresserons principalement aux objets réseaux. Les objets Web seront abordés dans le module « protection applicative ». La partie Certificats et PKI est, quant à elle, abordée dans la formation CSNE.

## GÉNÉRALITÉS


Préfixes interdits	Caractères interdits dans le nom	Noms d'objets interdits	Caractères interdits dans la description
firewall_	<tabulation>	Any	<tabulation>
Network_	<espace>	None	#
Ephemeral_	!	Anonymous	@
Global_	"	Broadcast	"
Vlan_	#	Internet	
Bridge_	,		
	=		
	@		
	[		
	]		
	\		

**SYSTEM / CONFIGURATION**

GENERAL CONFIGURATION **FIREWALL ADMINISTRATION** NETWORK SETTINGS











Access to the firewall's administration interface

Allow the 'admin' account to log in

Listening port:  

**OBJECTS**

Search...

Type	Object name
	Any
	None
	Internet
	Firewall_out_router
	Firewall_out_dns2
	Firewall_out_dns1
	Firewall_out
	Firewall_in
	Firewall_bridge
	cloudurl-download-sns.stor...

La syntaxe des noms des objets créés par l'administrateur doit respecter quelques restrictions définies dans le tableau ci-dessus. De plus, elle est insensible à la case.

La création et la configuration des objets s'effectuent :

- Dans le menu : **CONFIGURATION ⇒ OBJETS**
- Dans le menu : **OBJETS**
- Depuis n'importe quel autre menu via le bouton encadré en rouge dans la diapositive ci-dessus (création contextuelle).

**NOTE** : Il est possible de créer plusieurs objets portant la même valeur. Cependant, nous vous déconseillons de le faire afin de simplifier la lecture des menus de configuration (principalement les règles de filtrage/NAT) et des bases d'objets. Et également, afin de faciliter leur maintenance.



- Généralités
- ➔ **Les objets réseaux**
- Lab – Les objets

STORMSHIELD

Les objets

## LES OBJETS RÉSEAU

Type	Usage	Name ↑	Value
[-] Type : DNS names (FQDN) (1)			
[-] Type : Region groups (1)			
[-] Type : Groups (5)			
[-] Type : Hosts (37)			
[-] Type : internet (1)			
[-] Type : Networks (21)			
[-] Type : IP Protocols (29)			
[-] Type : Address ranges (1)			
[-] Type : Ports - Port ranges (261)			
[-] Type : Port groups (15)			
[-] Type : Time objects (1)			

STORMSHIELD

6

La base d'objets réseaux est accessible depuis le menu **CONFIGURATION ⇒ OBJETS ⇒ Objets réseaux**. Elle comprend les catégories d'objets suivants :

- **Machine** : Une adresse IP
- **Nom DNS (FQDN)** : Toutes les adresses IP associées à un nom FQDN par résolution DNS
- **Réseau** : Une adresse réseau
- **Plage d'adresses IP** : Une plage d'adresses
- **Port – Plage de ports** : Un port ou une plage de port. Il/Elle peut être limité(e) à un protocole de transport particulier (TCP ou UDP),
- **Protocole IP** : l'ID du protocole au niveau IP,
- **Groupe** : Un groupe d'objets portant une ou plusieurs adresses IP : machines, plages d'adresses IP, réseaux ou d'autres groupes,
- **Groupe de ports** : Un groupe d'objets portant des ports ou des plages de ports, ainsi que d'autres groupes de ports,
- **Groupe de régions** : Un groupe de pays ou de continents. Ce type d'objet peut être utilisé dans la géolocalisation des adresses IP,
- **Routeur** : Permet de renseigner une ou plusieurs passerelles pour un routage par répartition de charge avec ou sans passerelle de secours. Cet objet sera détaillé dans la partie Routage du module Configuration Réseau,
- **Temps** : Un événement temporel (ponctuel, jour de l'année, jour(s) de la semaine ou plage(s) horaire(s)).

## LES OBJETS RÉSEAU

The screenshot shows the 'OBJECTS / NETWORK OBJECTS' interface. At the top, there is a search bar and a toolbar with buttons for '+ Add', 'X Delete', 'Check usage', 'Export', 'Import', 'Collapse all', and 'Expand all'. Below this is a table with columns: Type, Usage, Name, IPv4, IPv6, and Res. The table lists several objects, with 'srv\_web\_priv' highlighted in green. A red box highlights the 'Filter: Host' and 'Type: All IP versions' dropdowns. A red arrow points from this dropdown to a secondary menu on the right, which shows 'All objects', 'All IP versions' (checked), 'IPv4', 'IPv6', and 'MAC address'. A blue arrow points from the 'Filter: Host' dropdown to a secondary menu on the left, which shows 'All objects', 'Host' (checked), 'DNS name (FQDN)', 'Network', 'IP address range', 'Router', 'Group', 'IP protocol', 'Port - port range', 'Port group', 'Time object', and 'Region group'. The 'PROPERTIES' panel on the right shows details for the selected object 'srv\_web\_priv', including its name, IPv4 address (192.168.1.11), MAC address (01:23:45:67:89:ab), and resolution options (None (static IP) or Automatic).

Le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **Objets réseaux** offre plusieurs fonctionnalités pour gérer les objets réseaux :

- **Barre de recherche** : Effectuer une recherche sur le nom, le commentaire ou la valeur de l'objet.
- **Filtre** : Filtrer l'affichage des objets en fonction de leur catégorie (machine, réseau, port, etc.).
- **Type** : Filtrer l'affichage des objets en fonction du type d'adresse utilisé (double pile, IPv4, IPv6, adresse MAC).
- **Ajouter** : Créer un nouvel objet.
- **Supprimer** : Supprimer un objet sélectionné. Si celui-ci est utilisé dans une configuration, une fenêtre s'affichera pour vous permettre de vérifier le module dans lequel l'objet est utilisé, forcer la suppression ou annuler la suppression.
- **Vérifier l'utilisation** : Affiche dans le bandeau de gauche le ou les menus dans lesquels l'objet sélectionné est utilisé.
- **Exporter** : Exporter la base d'objets réseaux dans un fichier CSV.
- **Importer** : Importer des objets à partir d'un fichier CSV.

Le reste du menu est composé de deux parties :

- **Liste des objets** : Affiche tous les objets réseaux organisés selon les filtres d'affichage utilisés. Chaque objet est affiché sur une ligne avec les informations suivantes :
  - La catégorie de l'objet représenté par une icône,
  - L'utilisation : vert signifie que l'objet est utilisé et gris le contraire,
  - Le nom de l'objet,
  - La valeur portée par l'objet.
- **Propriétés** : Affiche les attributs de l'objet sélectionné. Leur modification s'effectue depuis cet encadré.

## LES OBJETS RÉSEAU

- **Objets implicites** : Créés automatiquement par le firewall sur action de l'administrateur (lecture seule)

PROPERTIES

Object name: Firewall\_out

IPv4 address: 192.168.95.18

MAC address: 01:23:45:67:89:ab (optional)

Resolution

None (static IP)  Automatic

Comments:

PROPERTIES

Object name: Network\_internals

Comments:

[Edit this group](#)

Type	Objects in this group
	Network_bridge
	Network_in

- **Objets préconfigurés** : valeurs standardisées et plus...

PROPERTIES

Object name: icmp

Protocol number: 1

Comments:

PROPERTIES

Object name: Internet

Network\_internals

On peut distinguer deux catégories d'objets particuliers en plus des objets qui peuvent être créés par l'administrateur :

- **Objets implicites** : Ils sont créés automatiquement par le firewall et dépendent de la configuration réseau. Ces objets sont en lecture seule et ne peuvent être ni modifiés ni supprimés par l'administrateur. Par exemple, l'objet « Firewall\_out », créé automatiquement lorsqu'une adresse IP est associée à l'interface « OUT » ou l'objet « Network\_internals » qui regroupe tous les réseaux accessibles via les interfaces internes.
- **Objets préconfigurés** : Ils sont présents par défaut dans la liste des objets. Ils représentent des valeurs de paramètres réseaux standardisées (ports, protocoles, réseaux) et des valeurs nécessaires pour le fonctionnement du firewall (adresse IP des serveurs Stormshield pour les mises à jour). Les figures ci-dessus représentent le protocole ICMP et l'objet « Internet ». Ce dernier regroupe l'ensemble des machines ne faisant pas partie des réseaux internes.

**NOTE** : Nous vous conseillons d'utiliser les objets implicites et préconfigurés et d'éviter de créer d'autres objets portant les mêmes valeurs.

## LES OBJETS RÉSEAUX

- Création d'un objet
  - Choix de la catégorie d'objet
  - Nom de l'objet
  - Valeur correspondante

OBJECTS / NETWORK OBJECTS

Searching...

+ Add X Delete Check usage

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: Lan\_B

IPv4 address

Network IP address: 192.168.2.0/24

Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0

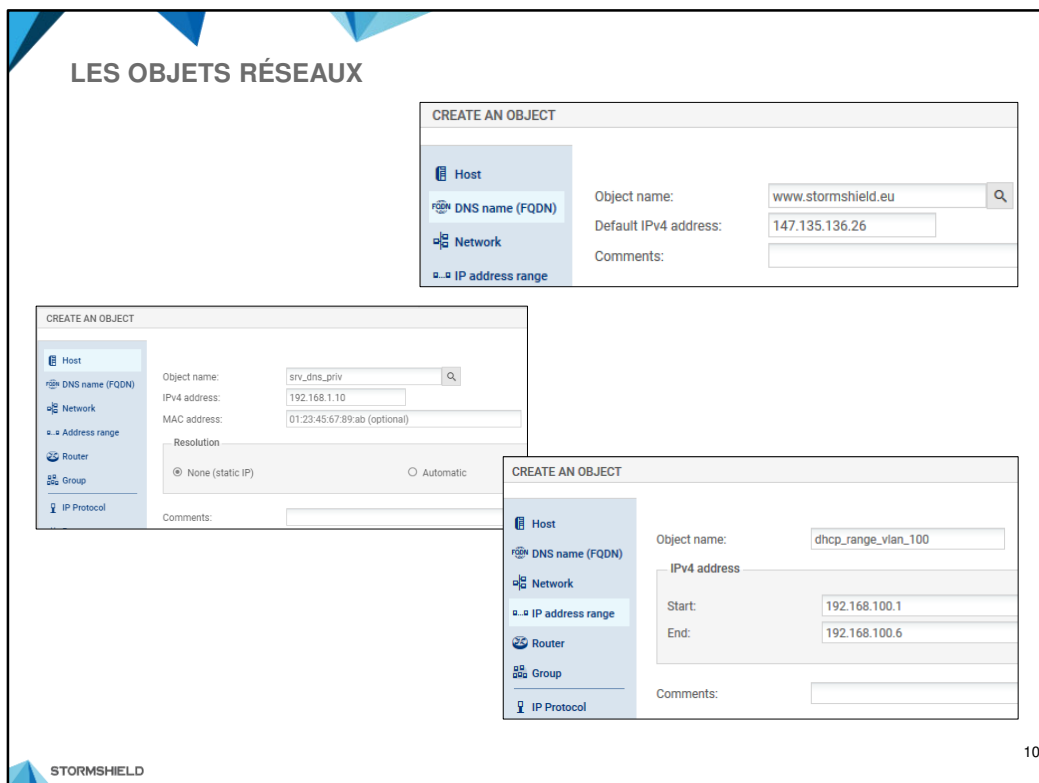
Comments:

CLOSE CREATE AND DUPLICATE CREATE

La fenêtre de création d'objets est composée de plusieurs onglets, un pour chaque catégorie.

Dans la majorité des cas, la création d'un objet consiste à définir deux champs obligatoires, à savoir le nom et la valeur, le champ commentaire est facultatif.

Il est possible de « créer » ou de « créer et dupliquer » l'objet. Ce dernier bouton crée l'objet et maintient la fenêtre de création ouverte pour faciliter la création d'un nouvel objet de même catégorie.



Les captures ci-dessus illustrent la création des objets FQDN, machine et plage d'adresses IP.

Les objets de type hôte dynamique et FQDN sont résolus toutes les cinq minutes par le firewall.

Pour l'objet hôte, le firewall conserve la dernière adresse IP résolue.

Pour l'objet FQDN, le firewall conserve un ensemble des IP résolues dans la base objets. Ce comportement est adapté pour des noms de domaine utilisant de la répartition de charge via DNS.

**NOTE :** Lors de la création d'un objet FQDN ou hôte dynamique, cliquez sur la loupe pour résoudre le nom de l'objet et récupérer une adresse par défaut. Si vous n'avez pas encore accès à un serveur DNS susceptible d'effectuer cette résolution, entrez une adresse IP quelconque, elle sera modifiée dès la résolution effective.

## LES OBJETS RÉSEAU

The image displays two side-by-side screenshots of the 'CREATE AN OBJECT' configuration page in Stormshield. Both screenshots show a left-hand navigation menu with categories: Host, DNS name (FQDN), Network, Address range, Router, Group, IP Protocol, Port, Port group, Region group, and Time object. The 'Port' category is selected in both.

**Left Screenshot (Port Object):**

- Object name: PROXY\_HTTPS
- Port: 3129
- Protocol: TCP

**Right Screenshot (Time Object):**

- Object name: training\_hours
- Description: From 09h00 to 12h00 and 13h30 to 17h30
- GMT+00:00
- Time slot(s):
  - From 09:00 to 12:00
  - From 13:30 to 17:30

Les captures ci-dessus illustrent la création des objets port et temps.

**NOTE :** Un objet temps nommé « workhours » modifiable existe dans la configuration usine.

## LES OBJETS RÉSEAUX

- Création de groupes de machines ou groupes de ports
  - Nom de l'objet
  - Objets inclus dans le groupe

The image displays two screenshots of the Stormshield management interface for creating network objects. Both screenshots are titled 'CREATE AN OBJECT'.

**Left Screenshot:** The 'Group' tab is active. The 'Object name' field contains 'srv\_mail\_priv'. Below it, a search bar shows 'srv'. A table lists objects to be added to the group:

Type	Object name	Create an object
Host	srv_mail_priv	<input type="checkbox"/>
Host	srv_dns_priv	<input type="checkbox"/>
Host	srv_mail_priv	<input type="checkbox"/>
Host	srv_dns_priv	<input type="checkbox"/>

**Right Screenshot:** The 'Port' tab is active. The 'Object name' field contains 'ipfs\_replicator'. A search bar is empty. A table lists objects to be added to the group:

Type	Object name	Create an object
Router	ipfs	<input type="checkbox"/>
Group	kerberos-admin	<input type="checkbox"/>
Group	kerberos-admin-top	<input type="checkbox"/>
Group	kerberos-admin-udp	<input type="checkbox"/>
Group	kerberos-iv	<input type="checkbox"/>
Group	kerberos	<input type="checkbox"/>
Group	kerberos-top	<input type="checkbox"/>
Group	kerberos-udp	<input type="checkbox"/>
Group	kerberos	<input type="checkbox"/>
Group	kerberos-top	<input type="checkbox"/>
Group	kerberos-udp	<input type="checkbox"/>

Pour ajouter un objet (ou plusieurs objets) au groupe, il suffit de sélectionner l'objet et de le basculer de la liste de gauche vers la liste de droite en cliquant sur le bouton →. La suppression de l'objet du groupe se fait par l'opération inverse avec le bouton ←.

Vous pouvez utiliser le champ de recherche sur une partie du nom ou de la valeur des objets souhaités.

## LES OBJETS RÉSEAUX

- Création d'un groupe de régions

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name:

Comments:

Searching...


Type	Object name
	Sahara occidental
	Érythrée
	Éthiopie
	Gabon
	Ghana
	Gambie
	Guinée
	Guinée équatoriale
	Guinée-Bissau
	Kenya
	Comores
	Liberia
	Lesotho
	Libye
	Maroc
	Madagascar

Type	Objects in this group
	Guernesey
	Kenya
	Europe

✕ CLOSE   + CREATE AND DUPLICATE   + CREATE

## LES OBJETS RÉSEAUX

- Exporter la base d'objets dans un fichier CSV



	A	B	C	D	E	F	G	H
1	#type	#name	#ip	#ipv6	#resolve	#mac	#comment	
2	host	rfc4291_loopback		::1	static		IPv6 default loopback	
3	host	dns1.google.com	8.8.8.8	2001:4860:4860::8888			Google Public DNS Server	
4	host	dns2.google.com	8.8.4.4	2001:4860:4860::8844			Google Public DNS Server	
5	host	support1.stormshield.eu	91.212.116.2		dynamic		Stormshield Support	
6	host	support2.stormshield.eu	46.35.17.250		dynamic		Stormshield Support	
7	host	dcp_multicast				01:0e:cf:00:00:00		
8	host	ptcp_multicast				01:80:c2:00:00:0e		
9	host	srv_dns	192.168.1.10		static			
10	#type	#name	#begin	#end	#beginv6	#endv6	#comment	
11	range	dhcp_range	10.0.0.10	10.0.0.100				
12	#type	#name	#ip	#ipv6	#comment			
13	fqdn	telemetry-sns.stormshieldcs.eu	127.0.0.1	::1				
14	fqdn	www.stormshield.eu	147.135.136.26					
15	#type	#name	#ip	#mask	#prefixlen	#ipv6	#prefixlenv6	#comment
16	network	rfc5735_6to4_relay_anycast	192.88.99.0	255.255.255.0		24		
17	network	rfc5735_bench_net	198.18.0.0	255.254.0.0		15		
18	network	rfc5735_link_local	169.254.0.0	255.255.0.0		16		

STORMSHIELD

14

Il est possible d'exporter la base d'objets dans un fichier CSV en cliquant sur le bouton « Exporter ». Le fichier sera proposé en téléchargement pour être stocké en local sur la machine. Le fichier CSV contient les objets machines, plages d'adresses IP, réseaux, FQDN, ports – plages de ports, protocoles, groupes et groupes de ports.

Les objets sont organisés par catégorie et séparés par des lignes contenant les noms des paramètres : #type, #name, #IP, etc... (les paramètres diffèrent en fonction des catégories d'objets). Les attributs d'un objet, quand à eux, sont séparés par des virgules.

## LES OBJETS RÉSEAU

- Importer des objets à partir d'un fichier CSV

OBJECTS / NETWORK OBJECTS

Searching... x Filter: All objects

+ Add X Delete Check usage Export Import

IMPORT A DATABASE

Select a file: C:\fakepath\4\_server\_objects.csv ...

0%

The transfer will stop in the event of an error.  
Existing objects will be replaced with the corresponding transferred objects.  
An objects database transfer may take several minutes. You may stop the operation anytime.

CANCEL CLOSE TRANSFER

IMPORT A DATABASE

Select a file: Select a CSV file containing an objects database ...

Import completed

Import completed successfully: 4 objects imported

Hosts: 4  
DNS names (FQDN): None  
Networks: None  
IP address ranges: None  
Groups: None  
IP protocols: None  
Ports: None  
Port groups: None

CANCEL CLOSE TRANSFER

STORMSHIELD 15

Il est possible d'importer des objets depuis un fichier CSV possédant le même format que le fichier exporté.

Pour cela, il faut cliquer sur le bouton **Importer**, une fenêtre s'affiche pour renseigner le fichier CSV contenant les objets. Cliquer sur **Transférer** pour commencer l'import. Une barre d'avancement permet de visualiser le déroulement de l'import. Et une fois fini, un rapport statistique affiche le nombre d'objets importés par type.

En cas d'erreur d'import, la base d'objets n'est pas modifiée.

**NOTE** : Les objets du fichier écrasent ceux du firewall s'ils portent le même nom. Les autres objets ne sont pas affectés.

## RECOMMANDATIONS



- Utiliser un groupe d'objet d'administration
- Limiter l'usage des objets dynamiques
- Suivre une convention de nommage des objets
- Limiter le nombre d'objets inutilisés
- Eviter les doublons

Un groupe d'objet contenant l'ensemble des IP et des réseaux d'administration permet de réutiliser ce groupe dans toutes les règles de filtrage liées à l'administration et donc de maintenir leur cohérence tout en facilitant leur modification.

Les objets dynamiques (type FQDN et Dynamic Host) génèrent des requêtes DNS régulières, ce qui sollicite le réseau et le firewall: n'utilisez cette fonctionnalité que lorsqu'elle est nécessaire.

Une convention de nommage bien définie et appliquée strictement évite la création de doublon et facilite la lecture des objets.

Les objets inutilisés chargent l'affichage et sont bien souvent oubliés et recréés. Afin d'éviter toute source potentielle de doublon, il est recommandé de ne pas conserver d'objets spécifiques inutilisés dans la configuration.

Les doublons doivent être traqués et supprimés, c'est une source d'erreur courante lors de la modification de règles de filtrage. On se retrouve dans un cas où la modification d'un objet n'impacte pas toutes les règles qui auraient dû l'être, créant ainsi des trous dans la sécurité.



- Généralités
- Les objets réseaux
- ➔ **Lab – Les objets**

STORMSHIELD

Les objets



## Lab 2 – Les objets

**Note :** Dans ce qui suit, le « x » doit être remplacé suivant la lettre de l'entreprise  
A⇒1, B⇒2.

1. Créez les objets machines et réseaux pour l'autre Compagnie :
  - Firewalls distants (adresse des interfaces externes)
    - Exemple : Fw\_B en 192.36.253.20
  - Réseaux distants (adresse des réseaux internes)
    - Exemple : Lan\_in\_B en 192.168.2.0 / 255.255.255.0
2. Ajoutez un nouveau service basé sur TCP fonctionnant sur le port 808, appelé webmail.
3. Créez un objet « pc\_admin » avec l'adresse 192.168.x.2
4. Créez un objet « srv\_dns\_priv » dont l'adresse IP est 172.16.x.10
5. Créez un objet « srv\_web\_priv » dont l'adresse IP est 172.16.x.11
6. Créez un objet « srv\_ftp\_priv » dont l'adresse IP est 172.16.x.12
7. Créez un objet « srv\_mail\_priv » dont l'adresse IP est 172.16.x.13
8. Créez un groupe d'objets dont vous choisirez le nom et qui contiendra les 4 serveurs que vous venez de définir.
9. Remplacez les serveurs DNS par défaut (dns1.google.com et dns2.google.com) configurés sur le firewall par un objet représentant la passerelle par défaut sur le réseau « NatNetwork » : 192.36.253.1.

### Bonus :

- Exportez la base d'objets dans un fichier CSV.
- En vous basant sur le format de ce fichier, créez un autre fichier CSV contenant deux objets machines :
  - « srv\_ftp\_pub » : 192.36.253.x2
  - « srv\_mail\_pub » : 192.36.253.x3
- Importez le fichier créé dans la base d'objets réseaux.





# Quiz

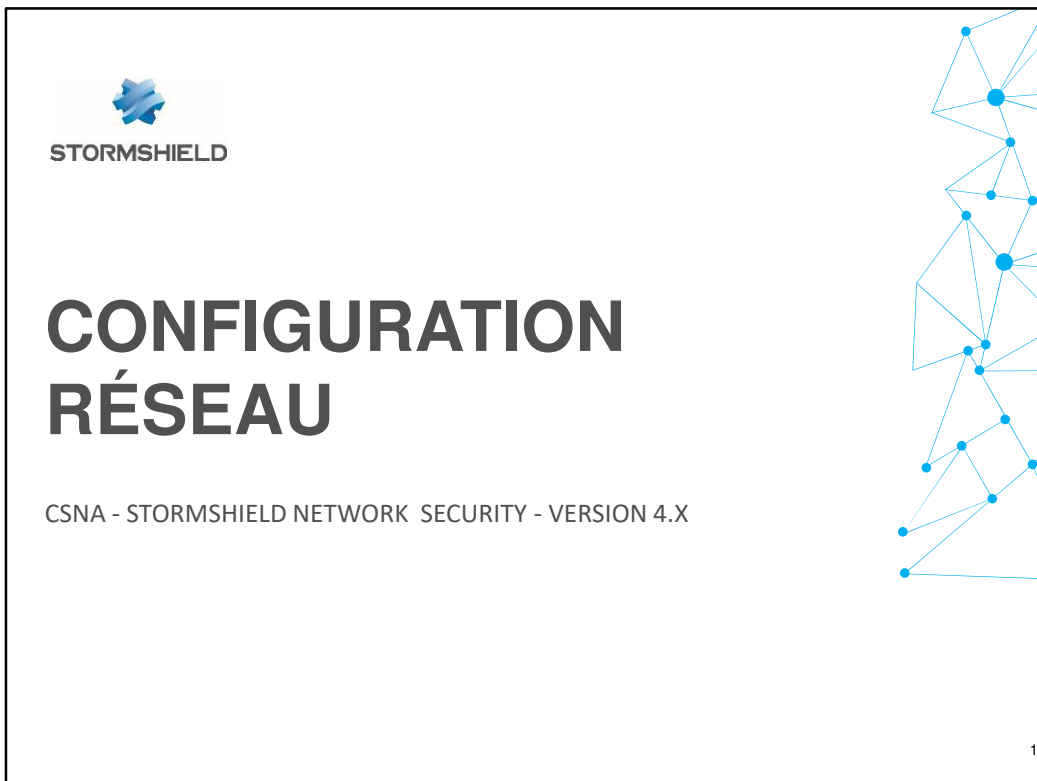
STORMSHIELD

Q1 – Quelles sont les assertions vraies :

- A. L'objet dynamique récupère son IP automatiquement depuis les serveurs DNS
- B. Un objet hôte peut être dynamique ou statique.
- C. Un objet FQDN est toujours résolu automatiquement.
- D. Grâce au DHCP, le pare-feu peut découvrir automatiquement les adresses IP des autres machines du réseau et créer les objets correspondants.

Q2 – Quelles sont les assertions vraies :

- A. Il est impossible de créer manuellement l'objet Firewall\_A.
- B. Il est possible de créer un groupe d'objets FQDN.
- C. L'objet Network\_external est géré automatiquement par le pare-feu.
- D. Il est possible d'exporter les objets sous forme d'un fichier CSV
- E. L'import d'un fichier CSV remplace systématiquement toute la base d'objets. Il faut donc être vigilant et ne pas oublier d'objet dans le fichier au risque de casser la configuration.



## Programme du cours

- ✓ Cursus des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Les objets
- Configuration réseau
  - Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## ➔ Modes de configuration

- Types d'interfaces
- Lab – Configuration réseau : interfaces
- Routage système
- Routage avancé
- Ordonnancement des types de routage
- Lab – Configuration réseau : routage

STORMSHIELD

Configuration réseau

MODES DE CONFIGURATION	
<b>1- Mode Transparent ou mode Bridge</b>	
<b>2- Mode Avancé ou mode Routeur</b>	
<b>3- Mode Hybride</b>	

STORMSHIELD 3

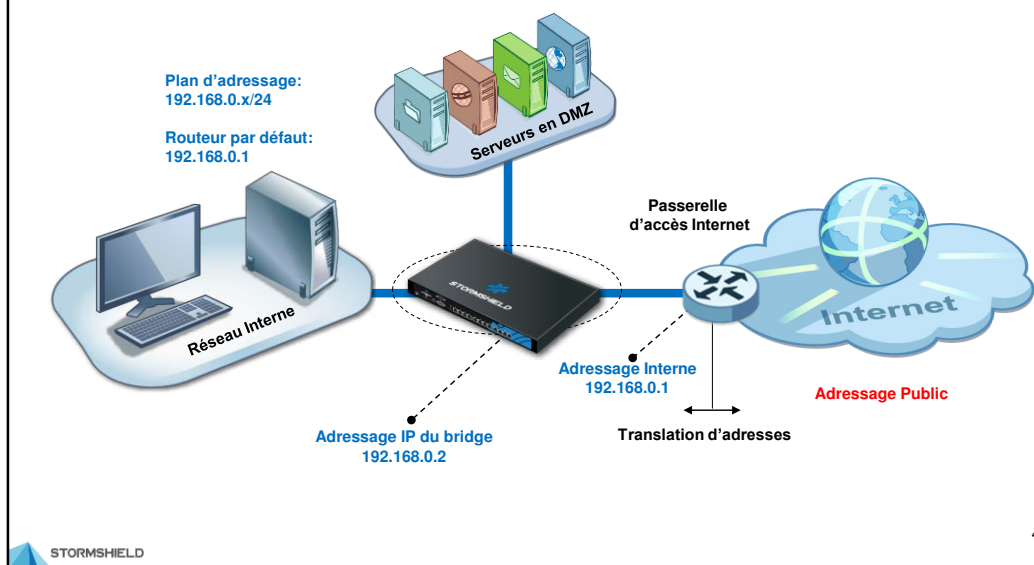
Trois modes de configuration existent sur l'ensemble de la gamme Stormshield Network Security:

- Mode transparent ou mode Bridge,
- Mode avancé ou mode routeur,
- Mode hybride.

Il est important de noter qu'il n'existe pas d'assistant pour la configuration de ces modes, il s'agit uniquement d'une dénomination. La mise en œuvre de chacun des modes s'effectue suivant le besoin, en configurant les interfaces réseaux et les règles de translation.

## MODES DE CONFIGURATION

## 1- Mode Transparent ou Mode Bridge



Grâce au mode transparent, le firewall Stormshield Network s'intègre aisément dans un réseau existant sans devoir en modifier sa configuration.

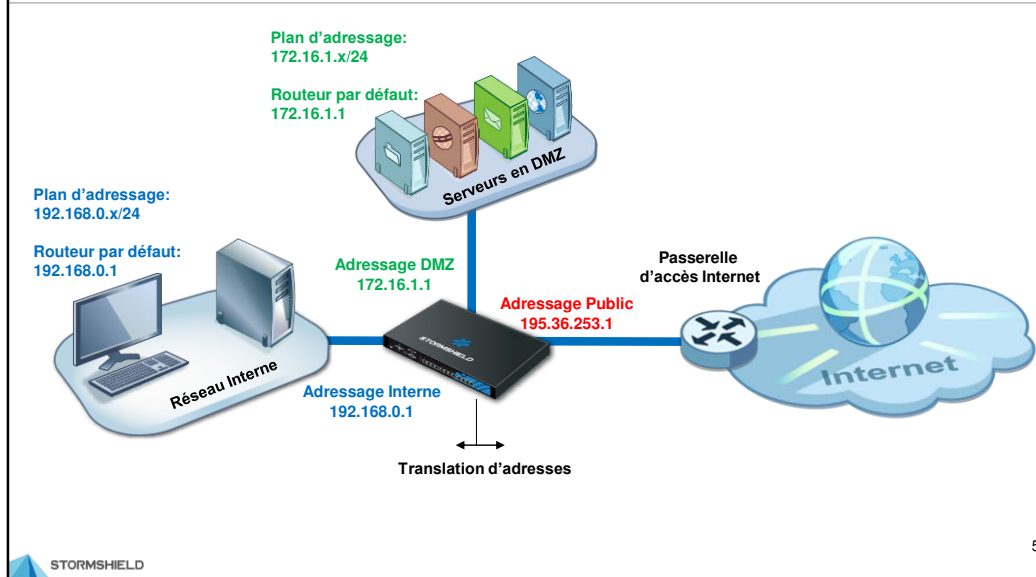
La particularité de ce mode est que toutes les interfaces du firewall sont incluses dans un bridge qui porte une adresse IP du réseau local (IP utilisée pour accéder à l'interface d'administration du firewall). Ceci permet d'avoir plusieurs réseaux physiques (un réseau par interface) partageant le même réseau logique.

La communication entre les réseaux physiques et la passerelle d'accès Internet se fait en mode bridge (niveau 2) sans soustraire les flux transitant entre les interfaces aux contrôles du firewall (filtrage, analyse ASQ, etc.).

Dans la figure ci-dessus, le réseau local utilise une plage d'adresses privée 192.168.0.0/24 et accède à Internet via une passerelle qui assure la translation d'adresses. Le firewall Stormshield Network est positionné en coupure des connexions entre les machines du réseau local et la passerelle d'accès à Internet.

## MODES DE CONFIGURATION

## 2- Mode Avancé ou Mode Routeur



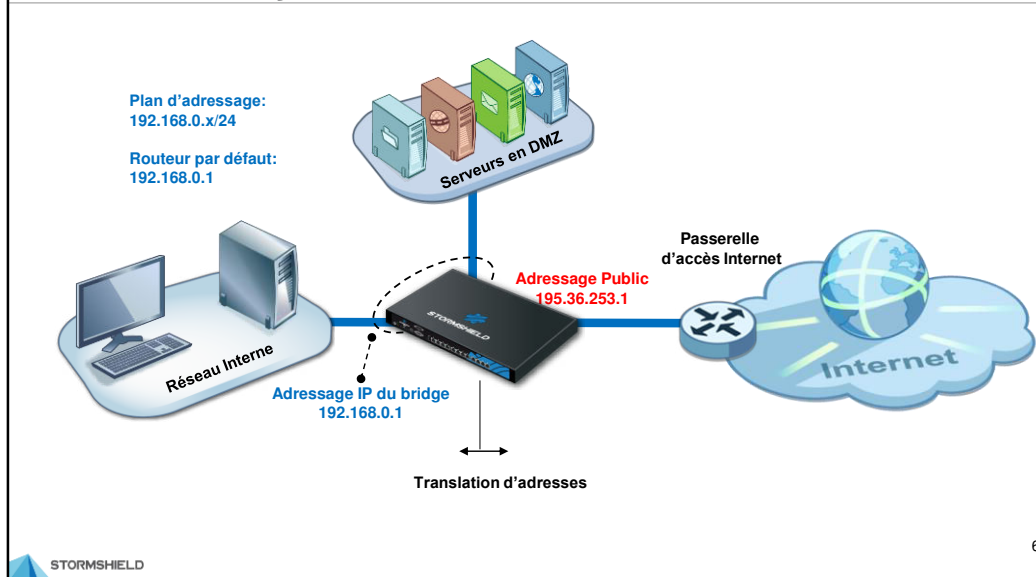
Dans le mode avancé, le firewall fonctionne comme un routeur en gérant plusieurs réseaux logiques (adresses réseaux). Chaque interface est configurée avec un réseau IP particulier, ce qui permet une segmentation du réseau aux niveaux physique et logique.

Dans l'image ci-dessus, le réseau local est composé de deux réseaux logiques : un réseau pour les machines internes et un réseau pour les serveurs en DMZ. Chaque réseau est connecté au firewall via une interface possédant un plan d'adressage IP spécifique. L'adresse IP publique est configurée directement sur une interface externe du firewall.

Dans ce mode, l'UTM Stormshield Network doit gérer les mécanismes de translation d'adresse pour assurer l'accès à l'Internet depuis les réseaux locaux.

## MODES DE CONFIGURATION

## 3- Mode Hybride (1)

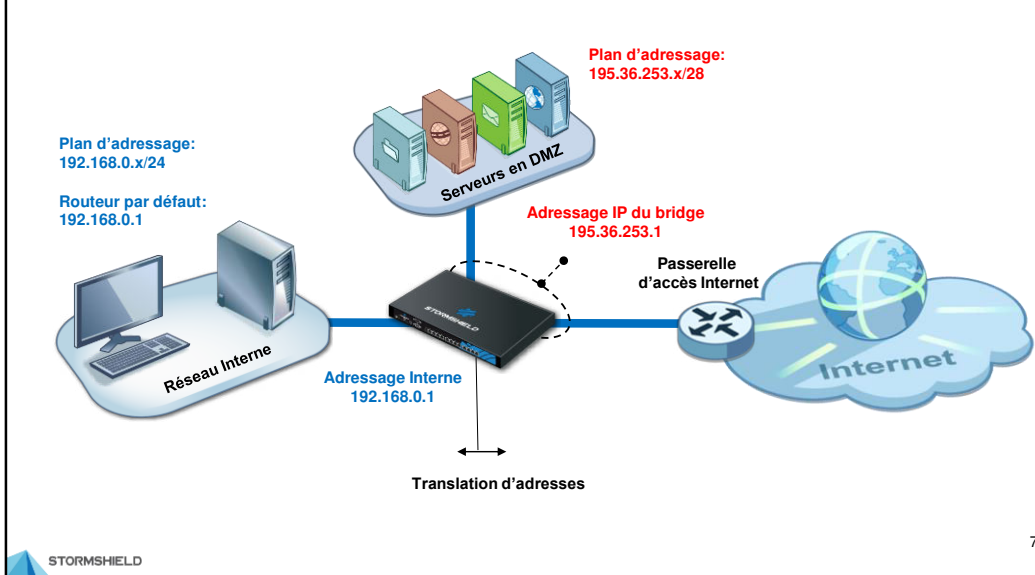


Le mode hybride est une combinaison des modes bridge et avancé. Le principe est d'avoir plusieurs interfaces dans un bridge (même plan d'adressage) et d'autres interfaces indépendantes avec des plans d'adressages différents.

Dans ce mode nous pouvons avoir deux cas de figure. Le premier est illustré ci-dessus. Le réseau des machines internes et le réseau des serveurs en DMZ partagent le même plan d'adressage et ils sont connectés au firewall via des interfaces appartenant au même bridge. La translation d'adresse doit être configurée sur le firewall pour que le réseau local (réseau du bridge) accède à Internet via l'interface externe, configurée avec une adresse IP publique.

## MODES DE CONFIGURATION

## 3- Mode Hybride (2)



Le deuxième cas de figure est illustré ci-dessus. Le réseau des serveurs en DMZ est configuré avec un plan d'adressage IP public. Chaque serveur disposera donc d'une IP publique distincte.

Ce réseau est connecté au firewall par une interface incluse dans le même bridge que l'interface externe où est connecté le routeur d'accès Internet. Les serveurs en DMZ accèdent à Internet via le bridge et aucune translation d'adresse n'est nécessaire (les connexions restent néanmoins soumises aux directives de filtrage et autres analyses applicatives de l'UTM).

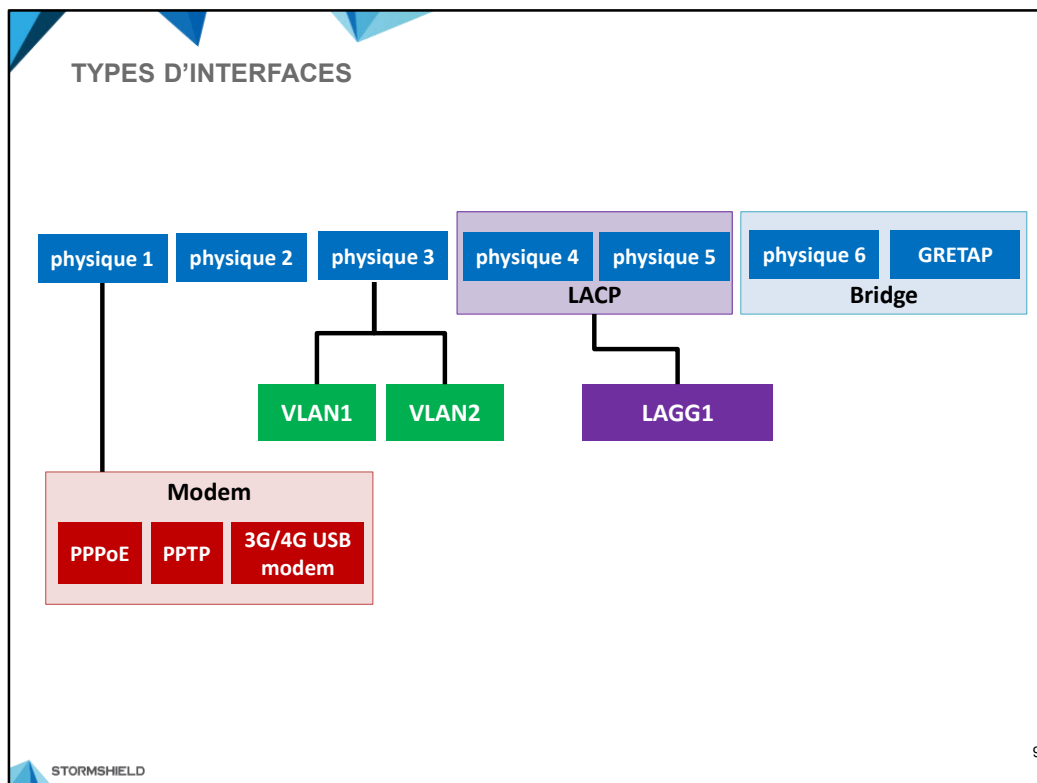
Le réseau des machines internes possède un plan d'adressage privé. Il est connecté au firewall via une interface n'appartenant pas au bridge. Par conséquent, la translation d'adresse doit être configurée pour lui permettre un accès à Internet.



- Modes de configuration
- ➔ **Types d'interfaces**
- Lab – Configuration réseau : interfaces
- Routage système
- Routage avancé
- Ordonnancement des types de routage
- Lab – Configuration réseau : routage

STORMSHIELD

Configuration réseau



Il existe plusieurs types d'interfaces sur le firewall.

Dans le menu **CONFIGURATION** ⇒ **RESEAU** ⇒ **Interfaces**, on peut créer et configurer les types d'interfaces suivants:

- **Les interfaces physiques** : Le nombre dépend du modèle du firewall,
- **Les interfaces bridges** : Association de plusieurs interfaces physiques ou VLAN. Le nombre maximal de bridges dépend du modèle du firewall,
- **Les interfaces VLAN** : Segment réseau attaché à une interface physique du firewall et caractérisée par un tag et un plan d'adressage spécifique. Le nombre maximal d'interfaces VLAN dépend du modèle du firewall,
- **Les interfaces Modem** : Ce type d'interface permet la prise en charge d'une connexion entre le firewall et un modem (ADSL, RNIS, RTC, ...). Les types de connexions possibles sont : PPPoE, PPTP. Elles sont vues en annexes.
- **Les interfaces GRE-TAP** : Permettent d'encapsuler des trames Ethernet dans des paquets IP via le protocole GRE. Il est ainsi possible de relier deux réseaux Ethernet distants.
- **Les interfaces LAGG** : Jusqu'à huit interfaces physiques de même vitesse et duplex peuvent être agrégées en une seule interface logique. Les liens sont surveillés grâce à LACP (Link Aggregation Control Protocol). L'interface résultante est utilisable comme les interfaces physiques, mais est tolérante aux pannes et possède une bande passante multipliée.

D'autres types interfaces peuvent être créés et paramétrés dans le menu **CONFIGURATION** ⇒ **RESEAU** ⇒ **Interfaces virtuelles**:

- **Les interfaces IPsec (VTI : Virtual Tunneling Interfaces)** : Permettent d'établir des tunnels IPsec routés. Elles seront vues en détails dans le chapitre consacré aux VPN IPsec,
- **Les interfaces GRE** : destinées au transport du protocole GRE, lequel permet d'encapsuler des flux IP dans un tunnel IP (vues en CSNE),
- **Les interfaces loopback** : interfaces dites de bouclage, internes au firewall et utiles notamment dans certaines configurations de routage dynamique.

TYPES D'INTERFACES

NETWORK / INTERFACES

Enter a filter

Edit + Add X Delete Monitor Go to monitoring Check usage

Interface	Port	Type	Status	IPv4 address	Comments
bridge		Bridge		10.0.0.254/8	
out	1	Ethernet, 1 Gb/s		DHCP	
in	2	Ethernet, 1 Gb/s		192.168.1.254/24	

Selected interface Modem profiles

IN CONFIGURATION

GENERAL ADVANCED PROPERTIES

Status: ON

General settings:

Name: in

Comments:

This interface is:  Internal (protected)  External (public)

Address range:

Address range:  Address range inherited from the  Dynamic / Static bridge

IPv4 address:  Dynamic IP (obtained by DHCP)  Fixed IP (static)

+ Add X Delete

Address / Mask	Comments
192.168.1.254/24	

STORMSHIELD 10

Le menu **CONFIGURATION** ⇒ **Réseau** ⇒ **Interfaces** est constitué de deux parties :

- L'en-tête (encadré vert) : Offre les fonctionnalités de base pour la gestion des interfaces.
- La liste des interfaces (encadré rouge) : Affiche toutes les interfaces (physique, bridge, vlan, modem) du firewall. Il est possible de faire un glisser-déposer sur les interfaces pour modifier leur configuration. Par exemple, l'ajout d'une interface à un bridge peut se faire en glissant l'interface physique et en la déposant sur l'interface bridge. L'action inverse est possible pour retirer une interface d'un bridge.

Pour configurer une interface (encadré bleu), vous pouvez double cliquer sur sa ligne en surbrillance ou cliquer sur le bouton **Edition**. La fenêtre d'édition est composée de deux onglets pour tous les types d'interface.

Les deux flèches en haut à droite de la fenêtre permettent de confirmer les modifications effectuées et de fermer la fenêtre d'édition.

**NOTE** : l'icône visible dans l'écran ci-dessus indique que l'administrateur est connecté au fire Il via l'interface correspondante.

### TYPES D'INTERFACES

The screenshot displays the 'TYPES D'INTERFACES' management interface. At the top, there is a search bar with the placeholder 'Enter a filter'. To its right are buttons for 'Add', 'Delete', 'Monitor', 'Go to monitoring', and 'Check usage'. The 'Add' button is expanded to show a list of interface types: 'Add a bridge', 'VLAN', 'GRETAP interface', 'Add a modem', and 'USB/Ethernet interface (USB key/modem)'. Below this, a table lists existing interfaces:

Interface	Port	Type	Status	IPv4 address	System name	Comments
bridge		Bridge		10.0.0.254/8		
dmz1	3	Ethernet, 1 Gb/			em2	
dmz2	4	Ethernet, 1 Gb/			em3	

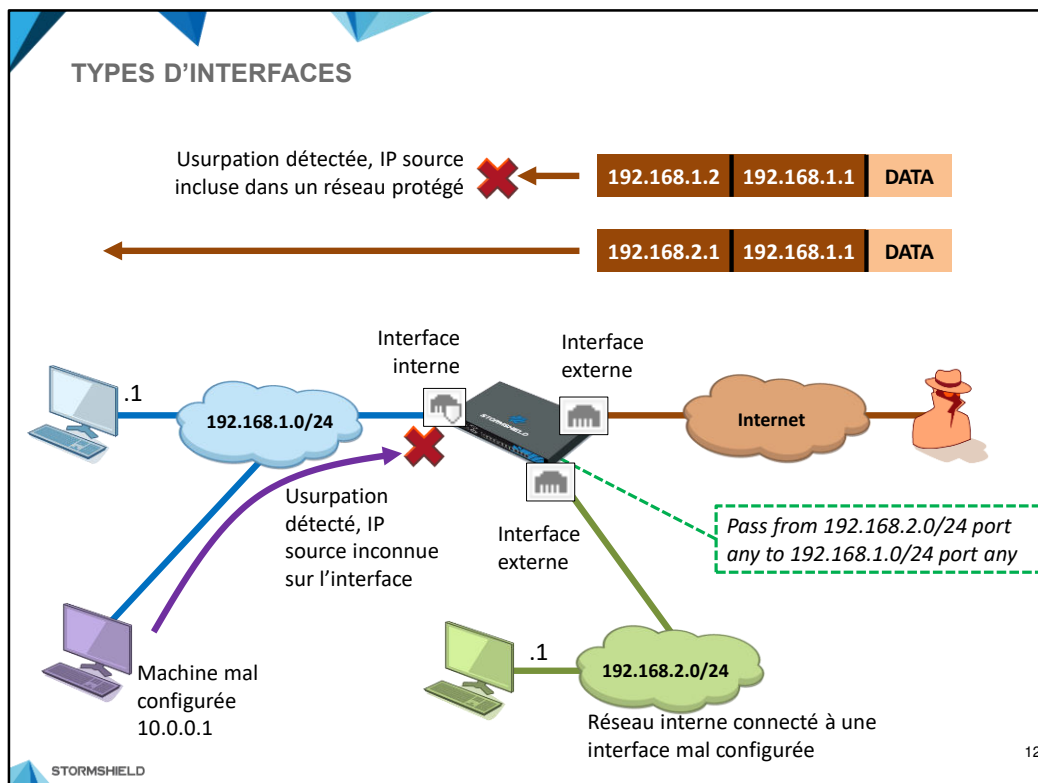
Below the table, there are sorting options: 'Sort Ascending', 'Sort Descending', and 'Columns'. The 'Columns' menu is open, showing a list of columns with checkboxes: 'Port', 'IPv4 address', 'IPv6 address', 'MAC address', 'System name', and 'Comments'. A 'Monitor' button is highlighted in the top bar, and a 'Bouton on /off' button is shown below it.

STORMSHIELD

11

L'en-tête contient :

- **Filtre** : Recherche des interfaces par une partie ou par la totalité des champs : nom, adresse IP ou commentaire,
- **Edition** : Ouverture de la fenêtre de configuration de l'interface courante ou de l'un des 2 profils « Modem »,
- **Ajouter** : Ajout d'une nouvelle interface de type Bridge, VLAN, Modem (ou USB Modem) ou GRETAP,
- **Supprimer** : Suppression de l'interface sélectionnée. Un message d'alerte s'affiche si l'interface est utilisée dans un menu de configuration. Malgré ce message, la suppression peut être forcée,
- **Superviser** et **Accéder à la supervision** : Activation ou désactivation de la supervision d'une interface pour vérifier l'utilisation de la bande passante et le nombre de connexions,
- **Vérifier l'utilisation** : Afficher les menus de configuration dans lesquels l'interface est utilisée. Le résultat de cette vérification s'affiche dans l'encadré de gauche en-dessous de l'icône favoris ★



Les interfaces internes (protégées) n'acceptent que les paquets provenant d'un réseau connu depuis cette interface. Soit le réseau est directement connecté et donc déduit de l'adresse de l'interface. Soit le réseau est connu par une route statique partant de cette interface.

Les interfaces externes (non protégées) acceptent tous les paquets exceptés ceux des réseaux protégés (connus sur une interface interne).

En cas de mauvaise configuration de l'interface, des règles de filtrage un peu laxistes (ne précisant pas d'interface d'entrée) autoriseraient du trafic illégitime à passer au travers du firewall.

L'exemple ci-dessus illustre ce problème de configuration. Le réseau vert (192.168.2.0/24) est relié à une interface externe, il n'est donc pas ajouté dans la table des réseaux protégés. Un pirate présent sur une autre interface externe pourra alors émettre des paquets avec une adresse IP usurpée appartenant au réseau vert. Ce paquet sera considéré comme légitime par le système anti-usurpation.

## TYPES D'INTERFACES

- Interface physique : configuration générale

IN CONFIGURATION

GENERAL ADVANCED PROPERTIES

Status

**ON**

General settings

Name:

Comments:

This interface is:  Internal (protected)  External (public)

Address range

Address range:  Address range inherited from the bridge  Dynamic / Static

IPv4 address:  Dynamic IP (obtained by DHCP)  Fixed IP (static)

+ Add X Delete	
Address/ Mask	Comments
192.168.1.254/24	

13

Une interface physique porte au moins une adresse IP, dynamique ou statique (encadré bleu), les paramètres dans l'encadré rouge sont détaillés ci-après :

- **État** : Interface activée ou désactivée
- **Nom** : Le nom de l'interface est obligatoire, c'est un nom logique différent du nom système de l'interface,
- **Commentaire** : Paramètre facultatif pour ajouter toute remarque informative au sujet de l'interface sélectionnée,
- **Cette interface est** :
  - **interne (protégée)** : Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface (protégeant ainsi contre l'usurpation d'identité), et permet de générer les règles de filtrage implicites lors de l'activation de certains services du firewall (par exemple SSH). Une icône représentant un bouclier est apposée à toute interface protégée.
  - **externe (publique)** : Indique que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

## TYPES D'INTERFACES

- Interface physique : configuration générale

The screenshot shows the configuration interface for a physical interface. At the top, the 'Address range' section has three radio buttons: 'Address range inherited from the bridge', 'Dynamic / Static' (which is selected and highlighted with a blue box), and 'Fixed IP (static)'. Below this, two detailed views are shown, connected by blue arrows from the selected option.

The left view shows 'Advanced DHCP properties' with the following fields:

- DNS name (optional): [ ]
- Requested lease time (seconds): 3600
- Request domain name servers from the DHCP server and create host objects

The right view shows a table of IPv4 addresses:

Address / Mask	Comments
192.168.1.254/24	

STORMSHIELD

14

Les paramètres dans l'encadré **Plan d'adressage** sont détaillés ci-après :

- **Adressage** : Choix entre les deux possibilités suivantes :
  - **Plan d'adressage hérité du bridge** : Se reporter à la section bridge plus loin dans ce chapitre,
  - **Dynamique/statique** : La définition du type d'adresse est précisée sur la ligne suivante : Adresse IPv4.
- **Adresse IPv4** : Choix entre les deux possibilités suivantes :
  - **IP dynamique** (obtenue par DHCP). Un menu de configuration DHCP avancée s'affiche :
    - **Nom DNS (facultatif)** : Indique le nom de domaine envoyé au serveur DHCP,
    - **Durée de bail demandée (secondes)** : Permet de configurer la durée du bail DHCP demandée au serveur DHCP,
    - **Demander les serveurs DNS au serveur DHCP et créer les objets machine** : Le nom des objets créés est Firewall\_<nom\_interface>\_dns\_1, Firewall\_<nom\_interface>\_dns\_2, etc.
  - **IP fixe (statique)** : La sélection de cette option indique que l'interface possède une adresse IP fixe qui doit être renseignée dans la liste en-dessous, accompagnée d'un masque réseau. Le masque peut être écrit aux formats numérique ou CIDR. Plusieurs adresses IP fixes (alias) peuvent être configurées sur une interface, même si elles font partie du même réseau IP.

**NOTE** : aucune configuration n'est prise en considération si elle n'est pas appliquée avec le bouton **Appliquer** .



## TYPES D'INTERFACES

- Interface physique : configuration avancée

IN CONFIGURATION

GENERAL    **ADVANCED PROPERTIES**

Other settings

MTU: 1500

MAC address: Example: 08:00:25:34:55:64

Physical MAC address: 00:0d:54:14:f7:5b

Media

Media: automatic detection

- automatic detection
- 10 Mbps half duplex
- 10 Mbps full duplex
- 100 Mbps half duplex
- 100 Mbps full duplex
- 1 Gbps full duplex
- 10 Gbps full duplex
- 20 Gbps full duplex
- 25 Gbps full duplex
- 40 Gbps full duplex

La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** :

- **MTU** : Indique la taille du MTU de l'interface en octets,
- **Adresse physique (MAC)** : Permet de forcer l'adresse MAC d'une interface,
- **Média** : Permet de choisir la vitesse du lien utilisé par l'interface. Par défaut, la vitesse est détectée automatiquement.

## TYPES D'INTERFACES

- Bridge : création et configuration générale

STORMSHIELD

16

Deux méthodes sont disponibles pour la création d'un bridge :

1. Présélection des interfaces membres du bridge : les interfaces sont mises en surbrillance, la fenêtre de configuration est directement renseignée, comme ci-dessus,
2. Création d'un bridge sans interface membre, le nom du bridge dans la fenêtre de configuration reste grisé, jusqu'à ce qu'au moins deux interfaces soient sélectionnées comme membres du bridge.

L'onglet de **CONFIGURATION GÉNÉRALE** contient :

- **Paramètres généraux** : Nommage de l'interface (champ obligatoire) et commentaire facultatif,
- **Plan d'adressage** : Le bridge peut être configuré avec une adresse IP fixe accompagnée d'un masque réseau ou avec une IP dynamique fournie par un serveur DHCP,
- **Gestion des membres** : Choix des interfaces membres du bridge, qui héritent de ses paramètres IP.

**NOTE** : Le nombre maximum de bridge dépend du modèle.

## TYPES D'INTERFACES

- Bridge : configuration avancée

BRIDGE\_TRAINING CONFIGURATION

GENERAL **ADVANCED PROPERTIES**

Other settings

MTU:

Physical (MAC) address :

Loops detection (Spanning Tree)

Disable Spanning Tree protocols

Enable Rapid Spanning Tree Protocol (RSTP)

Enable Multiple Spanning Tree Protocol (MSTP)

La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** d'un bridge :

- **MTU** : Indique la taille du MTU de l'interface en octets,
- **Adresse physique (MAC)** : Permet de forcer l'adresse MAC du bridge. Toutes les interfaces membres du bridge héritent de son adresse MAC (et de son adresse IP),
- **Détection de boucles (Spanning Tree)** : Permet d'activer le protocole RSTP ou MSTP pour communiquer avec les éléments de couche 2 du réseau et éviter les boucles.

## TYPES D'INTERFACES

- Interface membre d'un bridge : configuration avancée

DMZ1 CONFIGURATION

GENERAL **ADVANCED PROPERTIES**

Other settings

MTU: 1500

Physical (MAC) address : 08:00:27:bd:22:3f

Media

Media: automatic detection

Routing without analysis

Authorize without analyzing:

- IPX
- NetBios
- AppleTalk
- PPPoE
- IPv6

Routing by interface

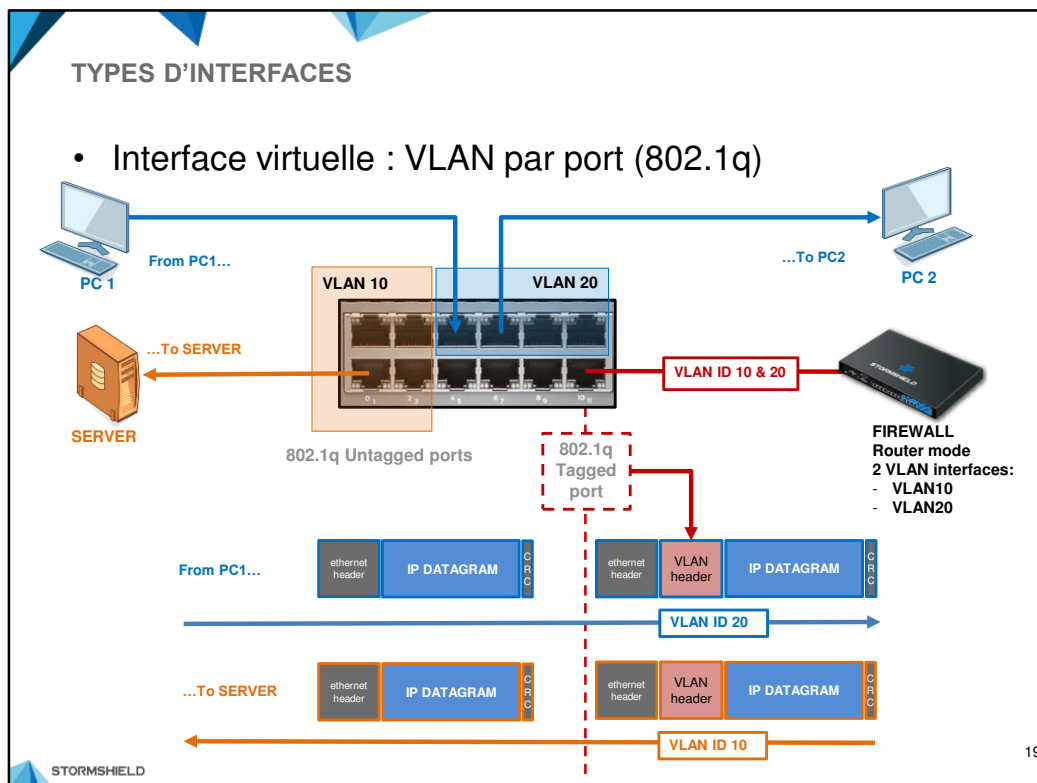
Keep initial routing

STORMSHIELD

18

La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** d'une interface :

- **MTU et Adresse Physique (MAC)** : Les champs sont grisés puisqu'ils sont hérités du bridge (adresse MAC commune à toutes les interfaces membres),
- **Média** : Permet de choisir la vitesse du lien Ethernet utilisé par l'interface. Par défaut, la vitesse est détectée automatiquement,
- **Autoriser sans analyser** : Autorise les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), AppleTalk (pour les machines Macintosh), PPPoE ou IPv6 entre les interfaces du bridge sans aucune analyse ni inspection de niveau supérieur (le firewall fonctionne comme un commutateur).
- **Préserver le routage initial** : Garde l'adresse MAC de destination des trames reçues par une interface membre du bridge et envoyée par une autre interface membre, ce qui permet de préserver le routage initial des paquets. Cette option facilite l'intégration transparente du firewall dans un réseau sans avoir à modifier la route par défaut des machines. **Attention** : L'activation de cette option peut avoir des effets négatifs sur certaines fonctionnalités qui nécessitent la modification des paquets par le firewall.



Les réseaux virtuels (VLAN : Virtual Local Area Network) introduisent la notion de segmentation virtuelle qui permet de constituer des sous-réseaux logiques au sein d'une même architecture réseau physique. Tous les équipements réseaux appartenant au même VLAN peuvent communiquer ensemble et forment un domaine de diffusion. Ainsi, l'utilisation des VLAN dans une architecture réseau améliore les performances en limitant les diffusions et offre une sécurité accrue en séparant les réseaux logiques. Stormshield gère les VLAN normés IEEE 802.1q, pour lesquels un en-tête supplémentaire de 4 octets :

- Est ajouté par un commutateur administrable ou par le firewall à une trame Ethernet sortante sur un port étiqueté 802.1q,
- Est supprimé par un commutateur administrable ou par le firewall à une trame Ethernet entrante sur un port étiqueté 802.1q.

Cet en-tête comprend le champ VLAN id (VID) qui permet d'identifier le VLAN auquel appartient la trame. Ce champ est codé sur 12 bits. Il permet de définir jusqu'à 4094 VLAN différents (le VLANID=0 signifie que la trame n'appartient à aucun VLAN et le VLANID=4095 est réservé). L'en-tête inclut également le champ Priority ou CoS (Class of Service) sur 3 bits qui indique la priorité du paquet définie par le standard IEEE 802.1p.

Dans l'exemple ci-dessus, une trame envoyée depuis PC1 :

- Peut atteindre PC2 sans subir de modification, car les ports du commutateur sur lesquels PC1 et PC2 sont connectés appartiennent au même VLAN.
- Peut atteindre le firewall par un étiquetage 802.1q effectué par le commutateur (Ajout du VID 20).
- Ne peut pas atteindre SERVER directement, puisqu'il est dans un VLAN différent.
- Peut atteindre SERVER via routage par le firewall. Après routage, une nouvelle trame étiquetée par le firewall (Ajout du VID 10) est envoyée vers le serveur. Le commutateur supprime l'étiquette sur le port entrant et transmet la trame au serveur.

## TYPES D'INTERFACES : EXTRÉMITÉ DE VLAN

- VLAN: création et configuration générale

The screenshot displays the Stormshield network configuration interface. On the left, the 'NETWORK / INTERFACES' section shows a list of interfaces: 'out', 'in', 'dmz1', and 'dmz2'. The 'dmz2' interface is highlighted in green. Below this list, a menu offers options: 'Add a bridge', 'VLAN', 'GRETAP interface', 'Add a modem', and 'USB/Ethernet interface (USB key/modem)'. A tooltip for 'VLAN' indicates 'No parent interface' and 'For dmz2'. On the right, the 'DMZ2\_VLAN1 CONFIGURATION' window is open, showing the 'GENERAL' tab. The status is 'ON'. The 'General settings' section includes: Name: 'dmz2\_vlan1', Comments: (empty), Parent interface: 'dmz2', ID: '1', Priority (CoS): '0', and 'This interface is:' set to 'External (public)'. The 'Address range' section shows 'Address range:' set to 'Dynamic / Static bridge' and 'IPv4 address:' set to 'Dynamic IP (obtained by DHCP)'. The 'Advanced DHCP properties' section is partially visible. The page number '20' is in the bottom right corner.

Deux méthodes sont disponibles pour la création d'un VLAN :

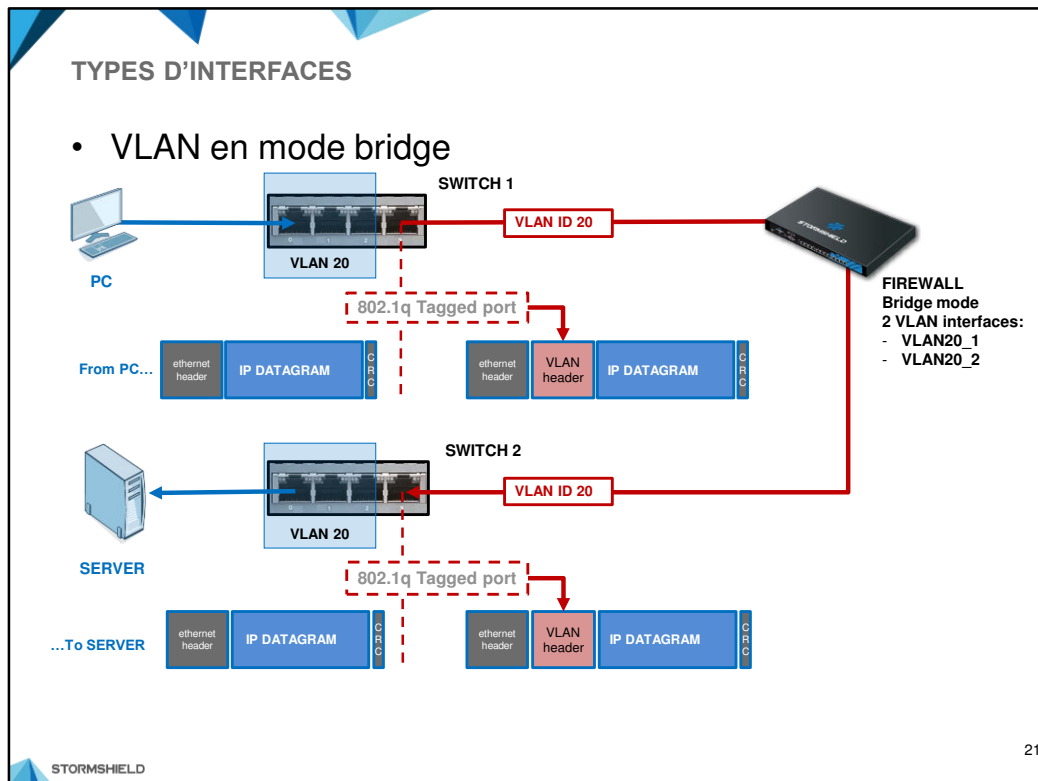
1. Présélection de l'interface parente : L'interface est mise en surbrillance, la fenêtre de configuration est directement renseignée, comme ci-dessus,
2. Création d'un VLAN sans interface parente : L'erreur « ce VLAN n'est pas associé à une interface physique » empêche la création de l'interface tant que le champ **Interface parente** n'est pas renseigné.

L'onglet de **CONFIGURATION GÉNÉRALE** contient :

- **Paramètres généraux** : Nommage de l'interface (champ obligatoire) et commentaire facultatif,
- **Interface parente** : Interface à laquelle sera rattaché le VLAN,
- **Identifiant de VLAN** : Valeur du VLANID [1-4094],
- **Priorité (CoS)** : Valeur inscrite dans le champ CoS sur tous les paquets envoyés par cette interface,
- **Cette interface est** : Choix du type de l'interface, interne ou externe,
- **Plan d'adressage** : L'interface VLAN peut être configurée avec une adresse IP fixe accompagnée d'un masque réseau ou avec une IP dynamique fournie par un serveur DHCP. Elle peut également hériter de l'adresse IP d'un bridge, ce cas spécifique est détaillé sur la diapositive suivante.

## NOTE :

- L'onglet **CONFIGURATION AVANCÉE** d'un VLAN permet de modifier la valeur de la MTU de l'interface,
- Dans le cas ci-dessus, l'interface parente du VLAN est désactivée, ce qui n'empêche en rien la création et le fonctionnement correct de l'interface VLAN.



Le cas d'usage ci-dessus illustre l'ajout d'un firewall en coupure en mode bridge entre deux commutateurs existants et reliés entre eux par un lien étiqueté 802.1q. Après cet ajout, le comportement des commutateurs n'est pas modifié mais le trafic sur le VLAN est analysé par le firewall.

Les étapes de création d'un VLAN en mode bridge sont les suivantes :

1. Création de deux interfaces VLAN ayant le même identifiant (VID) sur deux interfaces parentes différentes,
2. Création d'un bridge contenant ces deux interfaces,
3. Répétition de ces deux étapes autant de fois qu'il y a de VLAN différents devant transiter par le lien entre les deux commutateurs.

Dans l'exemple ci-dessus :

1. Une trame envoyée depuis PC vers SERVER atteint le commutateur (Ajout du VID 20), puis atteint le firewall (suppression du VID 20 sur l'interface entrante),
2. Le firewall analyse le contenu de la trame,
3. La trame est étiquetée par le firewall (Ajout du VID 20 sur l'interface sortante) et envoyée vers le serveur,
4. Le commutateur supprime l'étiquette sur le port entrant et transmet la trame au serveur.

## TYPES D'INTERFACES

- Vérification de la configuration

NETWORK / INTERFACES

Enter a filter

Interface Port Type Status IPv4 address System name Comments

Interface	Port	Type	Status	IPv4 address	System name	Comments
Bridge						
bridge				10.0.0.254/8		
dmz1	3	Ethernet, 1 Gb/s			em2	
out	1	Ethernet, 1 Gb/s		192.168.95.18/24 (DHCP)	em0	
in	2	Ethernet, 1 Gb/s		192.168.1.254/24	em1	
dmz2	4	Ethernet, 1 Gb/s			em3	

VERIFICATION OF THE CONFIGURATION

Warning bridge Bridge bridge consists of 1 interfaces

Error dmz2 Interface dmz2 has been enabled but does not have an IP address

CANCEL APPLY

22

La cohérence de la configuration réseau est analysée en temps réel. Vous pouvez l'afficher en cliquant sur la flèche en bas de l'écran.

Un avertissement n'empêche pas la sauvegarde de la configuration. En revanche, une erreur bloque la sauvegarde (le bouton **Appliquer** est grisé).



- Modes de configuration
- Types d'interfaces
- ➔ **Lab – Configuration réseau : interfaces**
- Routage système
- Routage avancé
- Ordonnancement des types de routage
- Lab – Configuration réseau : routage

STORMSHIELD

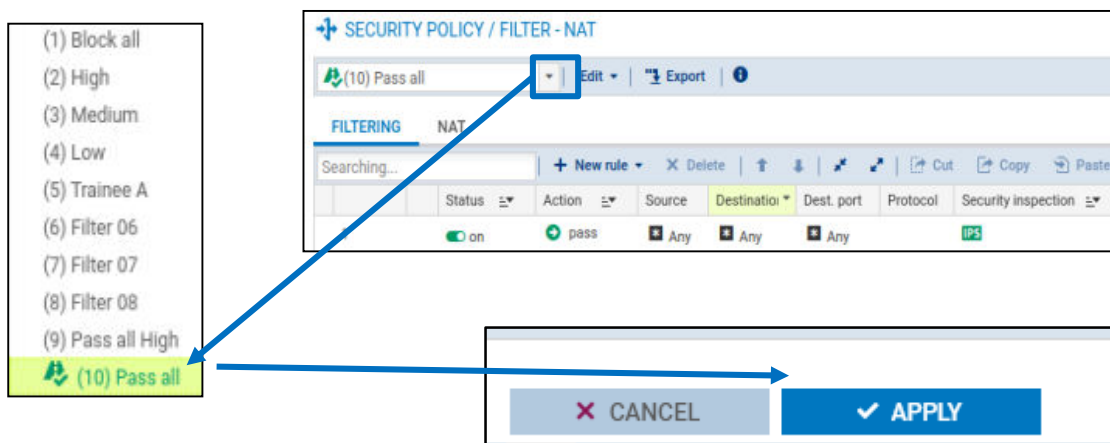
Configuration réseau



### Lab 3 – Configuration réseau : interfaces

Pour la suite des labs, vous devez sélectionner et activer la politique de filtrage **(10) Pass all** dans le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT** qui autorisera tous les trafics traversant ou à destination du firewall.

En bas de page, cliquez ensuite sur le bouton **Appliquer**.



#### • Configuration des interfaces :

1. Configurez les interfaces OUT, DMZ1 et IN de votre firewall comme suit :
  - OUT : 192.36.253.x0/24
  - DMZ1 : 172.16.x.254/24
  - IN : 192.168.x.254/24
2. Si vous utilisez la VM « Client\_TRAINING\_x », double cliquez sur le raccourci bureau « network\_config.sh », et choisissez la lettre de compagnie x. Si vous utilisez votre hôte physique, configurez l'interface réseau « Virtual Host-only Ethernet Adapter #2 ou #3 » de votre station comme suit :
  - Adresse IP : 192.168.x.2/24
  - Passerelle par défaut : 192.168.x.254
  - Serveur DNS : 172.16.x.10



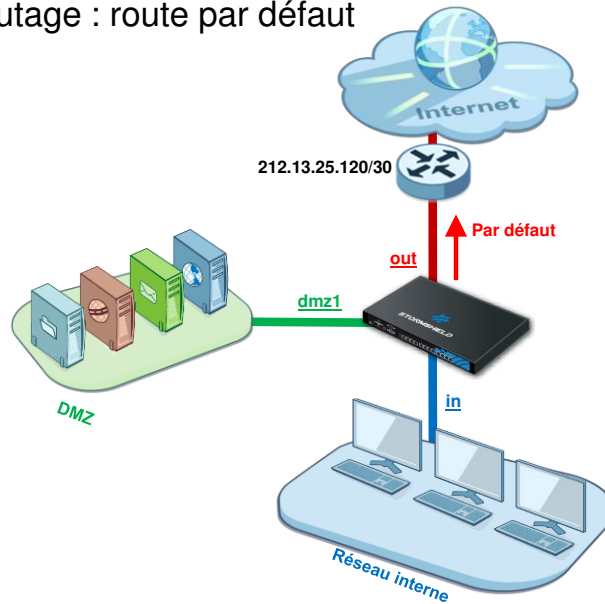
- Modes de configuration
- Types d'interfaces
- Lab – Configuration réseau : interfaces
- ➔ **Routage système**
- Routage avancé
- Ordonnancement des types de routage
- Lab – Configuration réseau : routage

STORMSHIELD

Configuration réseau

## ROUTAGE SYSTÈME

- Routage : route par défaut



STORMSHIELD

2

Le trafic qui ne correspond à aucune route dans la table de routage, quel que soit le type de route : standard (routage statique, dynamique), ou propriétaire Stormshield (routage par politique) est renvoyé vers la passerelle par défaut.

**ROUTAGE SYSTÈME**

- Routage : route par défaut

NETWORK / ROUTING

IPV4 STATIC ROUTES    IPV4 DYNAMIC ROUTING    IPV4 RETURN ROUTES

General

Default gateway (router):

STATIC ROUTES

Searching...    + Add    X Delete

Status    Destination network (host, network ...)

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: RTR\_Default

IPv4 address: 212.13.25.120

MAC address: 01.23.45.67.89.ab (optional)

Resolution

None (static IP)     Automatic

Comments:

X CLOSE    + CREATE

3

La passerelle par défaut est renseignée dans l'onglet **ROUTES STATIQUES IPV4** du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**, paramètre **Passerelle par défaut (routeur)**. Ce paramètre peut prendre comme valeur :

- **Un objet machine** : Pour spécifier une seule passerelle par défaut sans test de disponibilité, sans répartition de charge et sans passerelle de secours (exemple ci-dessus),
- **Un objet routeur** : Les différentes passerelles configurées dans l'objet routeur permettent d'effectuer des tests de disponibilité, de la répartition de charge et d'utiliser des passerelles de secours. Ce type d'objet est décrit plus tard dans ce chapitre.

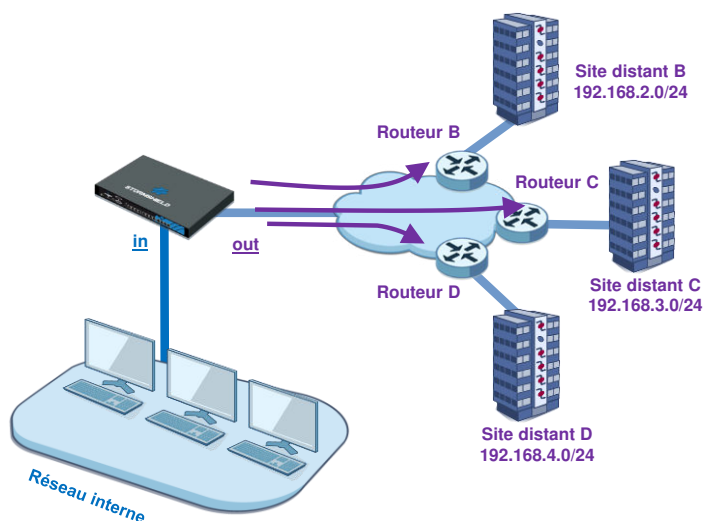
**NOTE** : sur une interface obtenant dynamiquement son adresse IP (par DHCP), l'obtention du bail DHCP donne lieu à la création d'un objet nommé « Firewall\_<nom\_interface>\_router », utilisable en tant que passerelle par défaut.

Par exemple, l'adressage de votre interface out étant dynamique, vous pouvez renseigner le paramètre **Passerelle par défaut (routeur)** avec l'objet : « Firewall\_out\_router ».



## ROUTAGE SYSTÈME

- Routage : route statique



STORMSHIELD

4

Le routage statique consiste à renseigner manuellement la passerelle distante à laquelle sont transmis les paquets devant atteindre un réseau distant. Dans la figure ci-dessus, trois routes statiques sont nécessaires pour atteindre les réseaux distant B, C, D via l'interface de sortie nommée « sites », puis les routeurs Routeur B, Routeur C, Routeur D.

## ROUTAGE SYSTÈME

- Routage : route statique

NETWORK / ROUTING

IPV4 STATIC ROUTES | IPV4 DYNAMIC ROUTING | IPV4 RETURN ROUTES

General

Default gateway (router): Firewall\_out\_router

STATIC ROUTES

Searching... + Add X Delete

Status	Destination network (host, network or group object)	Interface	Address range	Gateway	Comments
on	NET_B	out	192.168.2.0/24	Fw_B	
on	NET_C	out	192.168.3.0/24	Fw_C	
on	NET_D	out	192.168.4.0/24	Fw_D	
on	NET_COMPTA	In	172.16.100.0/24	RTR_INTERNAL	

En cas de configuration incohérente

Optio... 05:34:26 PM Network / Routing: Gateway is not routable 72ms

Clear log

Copy

La configuration des routes statiques s'effectue dans l'encadré **ROUTES STATIQUES IPV4** du premier onglet du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**.

L'encadré contient une barre de recherche et deux boutons pour ajouter ou supprimer une route. Il contient également une fenêtre qui liste toutes les routes statiques et leurs paramètres. Le bouton « Ajouter » ajoute une entrée à la liste. Les paramètres qui doivent obligatoirement être renseignés sur cette ligne sont :

- **État** : On / off
- **Réseau de destination** : Peut être un objet machine, réseau ou un groupe.
- **Passerelle** : Un objet machine ou routeur qui représente l'adresse IP de la passerelle permettant d'atteindre le réseau de destination.
- **Interface** : Choix de l'interface de sortie pour atteindre la passerelle. En se basant sur les paramètres de l'interface, le firewall renseigne automatiquement le champ **plan d'adressage**. Le fait de sélectionner l'interface se justifie dans le cas d'un bridge qui peut contenir des interfaces protégées et non protégées. Seule la sélection de l'interface permet de savoir si le réseau doit être considéré comme protégé ou non. Dans le cas où le plan d'adressage de l'interface et de la passerelle n'est pas le même, un message d'erreur annonce que « la passerelle n'est pas routable ».



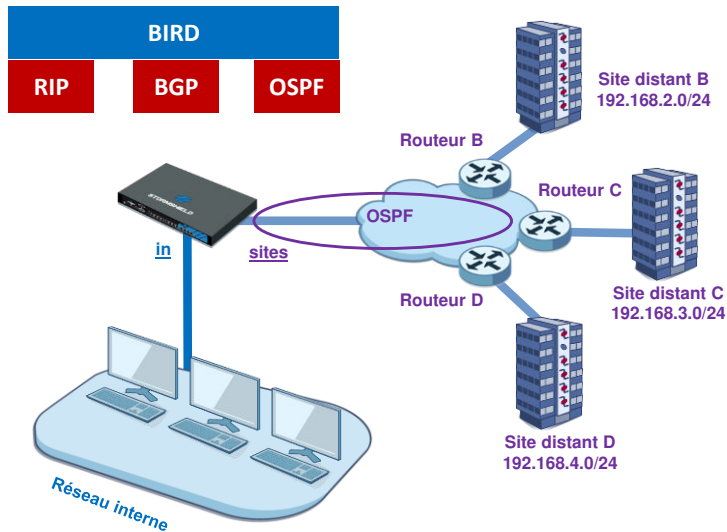
- Modes de configuration
- Types d'interfaces
- Lab – Configuration réseau : interfaces
- Routage système
- **➤ Routage avancé**
- Ordonnancement des types de routage
- Lab – Configuration réseau : routage

STORMSHIELD

Configuration réseau

## ROUTAGE AVANCÉ

- Routage dynamique



Avec le routage dynamique les routes sont apprises automatiquement grâce à un protocole de routage. Les firewalls SNS utilisent le logiciel BIRD pour mettre en œuvre le routage dynamique. BIRD implémente 3 protocoles de routage RIP, OSPF et BGP dont les versions supportées sont renseignées dans la base de connaissances. Dans la figure ci-dessus, le protocole de routage OSPF est activé sur l'interface « sites » du firewall pour lui permettre d'apprendre les routes pour accéder aux réseaux distant B, distant C et distant D.

## ROUTAGE AVANCÉ

- Routage dynamique

The screenshot shows the 'NETWORK / ROUTING' configuration page with the 'IPV4 DYNAMIC ROUTING' tab selected. The 'General' section has a toggle switch set to 'OFF'. Below the toggle is a text area containing configuration comments and code for 'protocol direct', 'protocol kernel', and 'protocol device'. The 'Advanced properties' section is expanded, showing two checkboxes: 'Restart dynamic routing when the firewall becomes active (high availability)' (unchecked) and 'Add IPv4 networks distributed via dynamic routing to the table of protected networks' (checked).

```

NETWORK / ROUTING
IPV4 STATIC ROUTES  IPV4 DYNAMIC ROUTING  IPV4 RETURN ROUTES

General
OFF
# The direct protocol automatically generates device routes to
# all network interfaces.
protocol direct {
}

# This pseudo-protocol performs synchronization between BIRD's routing
# tables and the kernel.
protocol kernel {
  learn;           # Learn all alien routes from the kernel
  persist;        # Don't remove routes on bird shutdown
  scan time 20;   # Scan kernel routing table every 20 seconds
  import all;     # Default is import all
  export all;     # Default is export none
  preference 254; # Protect existing routes
}

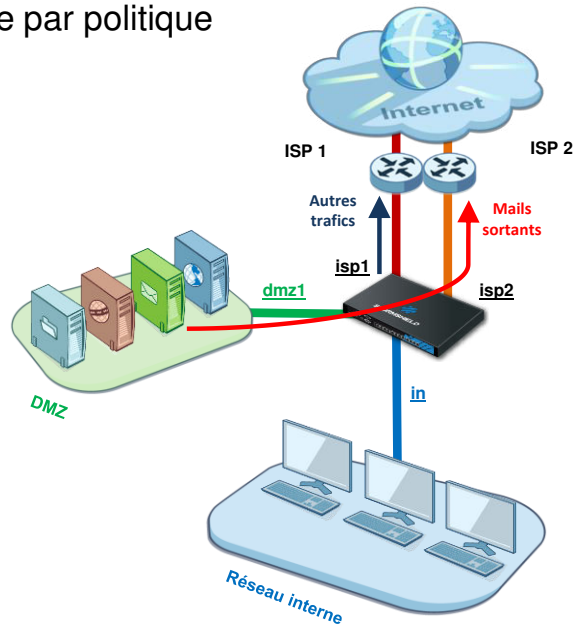
# This pseudo-protocol watches all interface up/down events.
protocol device {
  scan time 10;   # Scan interfaces every 10 seconds
}

Advanced properties
 Restart dynamic routing when the firewall becomes active (high availability)
 Add IPv4 networks distributed via dynamic routing to the table of protected networks
  
```

Le routage dynamique peut se configurer depuis l'interface graphique dans l'onglet **ROUTAGE DYNAMIQUE IPV4** du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**. Les réseaux de destination ajoutés dans la table de routage par un protocole dynamique peuvent être ajoutés à la table des réseaux protégés.

## ROUTAGE AVANCÉ

- Routage par politique



STORMSHIELD

9

Le routage par politique (alias PBR : Policy Based Routing) permet de spécifier une passerelle dans une règle de filtrage. Le flux spécifié par la règle est ainsi envoyé vers une passerelle choisie par l'administrateur.

Dans l'exemple illustré ci-dessus, le trafic des emails sortants est renvoyé vers la passerelle « ISP2 » et le reste du trafic est renvoyé vers la passerelle « ISP1 », laquelle est la passerelle par défaut.

## ROUTAGE AVANCÉ

- Routage par politique : configuration

The screenshot displays the Stormshield configuration interface for a NAT rule. The top section shows a table of rules with the following data:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass Route: ROUTER_ISP2	Network_dmz	Internet	smtp		IPS

The bottom section shows the 'EDITING RULE NO 1' dialog box with the 'ACTION' tab selected. The 'Routing' section is highlighted, showing the following configuration:

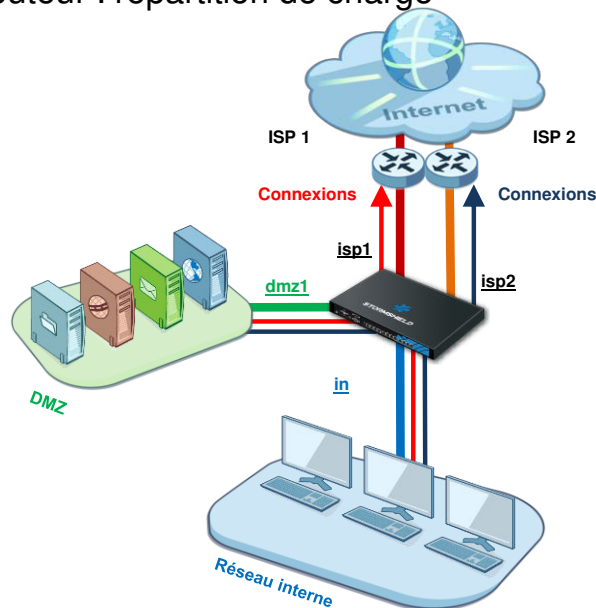
Routing  
Gateway - router: ROUTER\_ISP2

La mise en œuvre d'une directive de routage par politique s'effectue dans le champ Action d'une règle de filtrage. Deux types d'objet peuvent être renseignés au niveau de ce champ :

- **Un objet machine** : Pour spécifier une passerelle,
- **Un objet routeur** : Permet d'utiliser un objet routeur précédemment configuré et d'attribuer ses paramètres d'équilibrage et de répartition de charge à la règle de filtrage.

## ROUTAGE AVANCÉ

- Objet routeur : répartition de charge



STORMSHIELD

11

Un objet routeur regroupe plusieurs passerelles, permettant leur utilisation simultanée, mais donne lieu à l'ajout d'une seule route dans la table de routage. Par ailleurs, il permet d'effectuer des tests de disponibilité, de la répartition de charge et d'utiliser des passerelles de secours.

La répartition de charge permet de répartir les connexions sortantes vers plusieurs passerelles. La répartition peut être équitable, comme elle peut être pondérée pour que chaque passerelle reçoive un pourcentage spécifique du trafic global. Le mode de répartition peut être basé sur l'adresse IP source ou sur les paramètres d'une connexion, à savoir, les adresses IP et les numéros de ports source et destination.

La figure ci-dessus illustre un exemple dans lequel l'ensemble des connexions sortantes sont réparties vers les passerelles « ISP1 » et « ISP2 » selon un mode de répartition choisi (par source ou par connexion).

En utilisant les objets routeur, la répartition de charge peut être appliquée au trafic envoyé vers la passerelle par défaut ou bien pour un trafic particulier via le routage par politique. Dans le premier cas, l'objet routeur doit être spécifié comme passerelle par défaut du firewall (voir la diapositive 2), dans le deuxième cas l'objet routeur doit être renseigné dans le paramètre passerelle du champ Action d'une règle de filtrage (voir la diapositive 10).

## ROUTAGE AVANCÉ

- Objet routeur : création et configuration

12

La configuration d'un routage par répartition de charge s'effectue dans un objet routeur. Les différentes passerelles doivent être ajoutées dans l'onglet **LISTE DES PASSERELLES UTILISÉES**. Chaque ligne permet de renseigner :

- La passerelle avec un objet machine
- Test de disponibilité : Permet de tester la disponibilité de la passerelle en utilisant des pings. Ce paramètre peut avoir plusieurs valeurs :
  - Pas de test de disponibilité** : La disponibilité de la passerelle n'est pas testée.
  - Tester directement la passerelle** : Des commandes ping sont envoyées directement à la passerelle pour tester sa disponibilité.
  - Une machine ou un groupe de machines, se trouvant derrière la passerelle, vers lesquelles les pings sont envoyés pour tester la disponibilité et le fonctionnement de la passerelle.

Par défaut, l'état de chaque passerelle est vérifié toutes les 15 secondes en envoyant un ping à chaque machine renseignée. Dans le cas où aucune réponse n'est reçue au bout de 2 secondes, le firewall recommence 3 fois avant de considérer la passerelle indisponible. L'état des passerelles est visible dans le menu routes de la supervision.

**NOTE** : On ne peut pas tester la disponibilité des passerelles récupérées automatiquement par DHCP ou par une interface modem.

## ROUTAGE AVANCÉ

- Objet routeur : création et configuration

13

Le poids (encadré rouge) permet d'affecter à une passerelle un pourcentage du trafic géré par l'objet routeur selon le calcul suivant :

$$\text{traffic \%} = \frac{\text{weight of the gateway}}{\text{sum of the weight of all gateways}} \times 100$$

Dans l'exemple ci-dessus : poids RTR\_ISP1 = 3, poids RTR\_ISP2 = 7  
 → 30% du trafic passe par RTR\_ISP1, 70% par RTR\_ISP2.

La valeur d'un poids doit être comprise entre 1 et 1024.

L'algorithme utilisé (encadré bleu) pour la répartition de charge est configuré par le paramètre **Répartition de charge (Configuration avancée)** :

- Aucune répartition** : Le trafic est transmis exclusivement à la première passerelle qui apparaît dans la liste.
- Par connexion** : Répartit le trafic en fonction des adresses IP et des numéros de ports source et destination. Cet algorithme est recommandé parce qu'il permet de répartir également les connexions provenant d'une même machine.
- Par Adresse IP source** : Répartit le trafic en fonction de l'adresse source. Il permet de s'assurer que le trafic d'une machine sera toujours renvoyé vers la même passerelle.

## ROUTAGE AVANCÉ

- Objet routeur : création et configuration

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name: RTR\_OBJECT\_INTERNET

Comments:

USED GATEWAYS      BACKUP GATEWAYS

+ Add    X Delete      Move to the list of backups

Host	Device(s) for testing availability	Weight	Comments
RTR_JSP1	Test the gateway directly	3	
RTR_JSP2	dns1.google.com	7	

Advanced configuration

Load balancing: By connection

Enable backup gateways

When all gateways cannot be reached

When at least one gateway cannot be reached

When the number of gateways that can be reached is lower than 2

Enable all backup gateways when unavailable

If no gateways are available: Default route

Default route

Do not route

CLOSE    CREATE AND DUPLICATE    CREATE

14

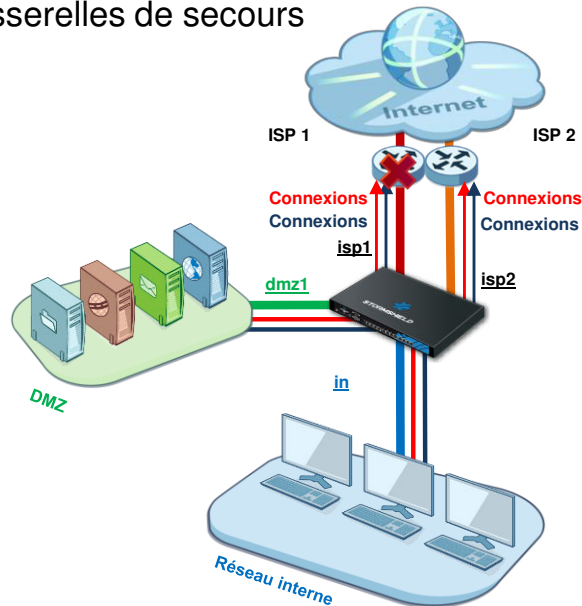
Lorsqu'un objet routeur est utilisé par une règle de filtrage (routage par politique), et qu'aucune passerelle de cet objet n'est joignable, le comportement du firewall peut être configuré par le paramètre **Si aucune passerelle n'est disponible** :

- Routage par défaut** : Le trafic est transmis au routeur par défaut.
- Ne pas router** : Le trafic est bloqué par le firewall.

La répartition de charge peut fonctionner avec 64 passerelles au maximum.

## ROUTAGE AVANCÉ

- Les passerelles de secours



STORMSHIELD

15

Un objet routeur permet également de spécifier une liste de passerelles de secours qui seront utilisées dans le cas où une, plusieurs ou toutes les passerelles principales sont indisponibles.

Dans l'exemple illustré ci-dessus, la passerelle « ISP2 » est considérée comme une passerelle de secours qui sera utilisée pour tout le trafic seulement si la passerelle « ISP1 » n'est plus disponible.

Il est important de noter que grâce aux objets routeur, les passerelles de secours peuvent être utilisées pour le trafic envoyé à la passerelle par défaut, les routes statiques ou bien pour un trafic particulier en utilisant le routage par politique.

## ROUTAGE AVANCÉ

- Les passerelles de secours : création et configuration

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

USED GATEWAYS    BACKUP GATEWAYS

+ Add    X Delete    ↑ ↓    Move to the list of main gateways

	Host	Device(s) for te...	Weight	Comments
1	RTR_ISP3	dns1.google.com	2	
2	RTR_ISP4	dns2.google.com	1	

Advanced configuration

Load balancing: By connection

Enable backup gateways

When all gateways cannot be reached

When at least one gateway cannot be reached

When the number of gateways that can be reached is lower than 2

Enable all backup gateways when unavailable

If no gateways are available: Default route

X CLOSE    + CREATE AND DUPLICATE    + CREATE

16

Plusieurs passerelles de secours peuvent être ajoutées dans l'onglet **LISTE DES PASSERELLES DE SECOURS** d'un objet routeur. Pour chaque passerelle de secours, on peut définir un équipement de test et un poids comme pour les passerelles principales.

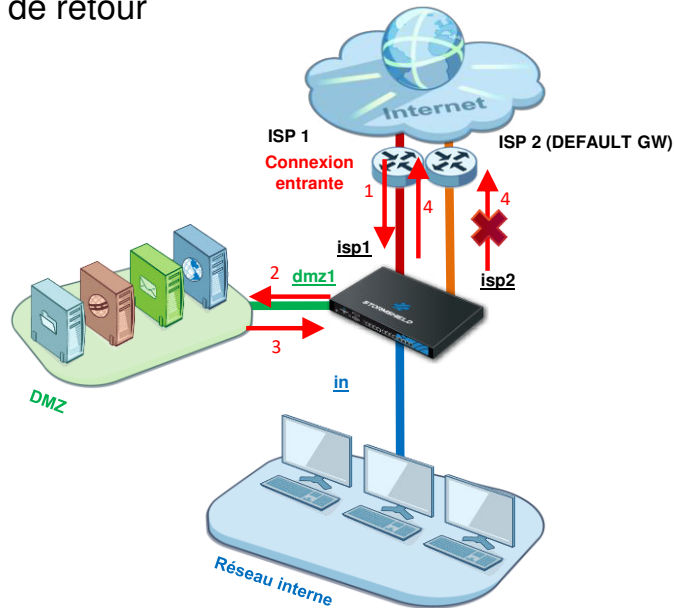
La configuration avancée permet de configurer deux éléments :

- Quand la ou les passerelles de secours doivent être activées :
  - Lorsque toutes les passerelles principales sont injoignables,
  - Lorsqu'au moins une passerelle principale est injoignable,
  - Lorsque le nombre de passerelles principales joignables est inférieur à un certain seuil. ( $1 < \text{seuil} \leq \text{nombre de passerelles principales}$ ).
- S'il faut activer une ou toutes les passerelles de secours : par défaut, seule la première passerelle de secours joignable dans la liste est utilisée sauf si l'option **Activer toutes les passerelles de secours en cas d'indisponibilité** est sélectionnée.

64 passerelles de secours au maximum peuvent être renseignées.

## ROUTAGE AVANCÉ

- Route de retour



STORMSHIELD

17

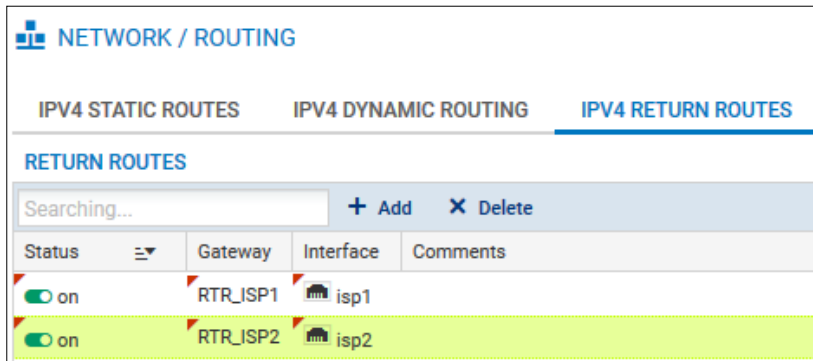
La route de retour permet de spécifier l'interface de sortie pour atteindre une passerelle distante. Ce type de route est utilisé pour forcer le flux sortant d'une connexion entrante à passer via l'interface d'entrée de la connexion.

La figure ci-dessus illustre un exemple dans lequel on dispose de deux accès WAN. L'accès « ISP1 » est réservé exclusivement aux flux emails (entrants et sortants). L'accès « ISP2 » est utilisée comme sortie par défaut pour les autres flux.

Sans route de retour, les réponses des connexions emails entrantes via l'interface « ISP1 » peuvent être renvoyées via l'interface « ISP2 ».

## ROUTAGE AVANCÉ

- Route de retour : création et configuration



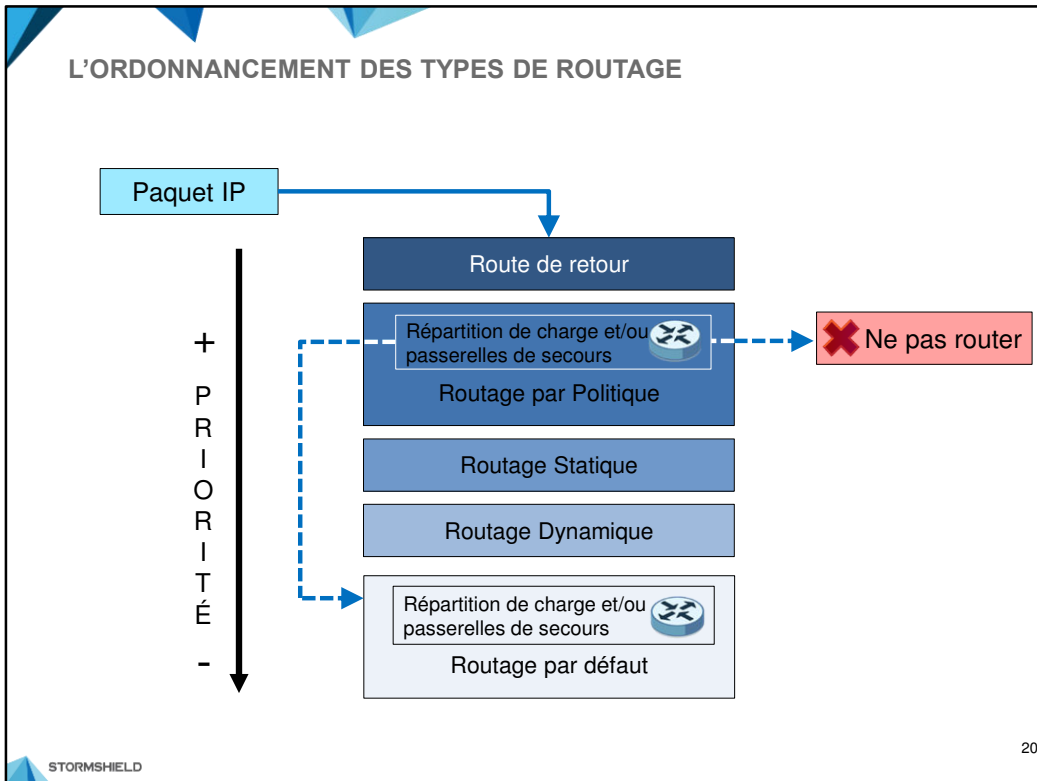
The screenshot shows the 'NETWORK / ROUTING' configuration page. It has three tabs: 'IPV4 STATIC ROUTES', 'IPV4 DYNAMIC ROUTING', and 'IPV4 RETURN ROUTES'. The 'IPV4 RETURN ROUTES' tab is active. Below the tabs is a search bar with 'Searching...' and buttons for '+ Add' and 'X Delete'. A table lists the configured return routes.

Status	Gateway	Interface	Comments
<input checked="" type="checkbox"/> on	RTR_ISP1	isp1	
<input checked="" type="checkbox"/> on	RTR_ISP2	isp2	

La configuration d'une route de retour s'effectue dans l'onglet **ROUTE de RETOUR** du menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage**. Il faut ajouter une ligne pour chaque route, dans laquelle il faut spécifier la passerelle, et l'interface par laquelle elle est joignable.



- Modes de configuration
- Types d'interfaces
- Lab – Configuration réseau : interfaces
- Routage système
- Routage avancé
- ➔ **Ordonnement des types de routage**
- Lab – Configuration réseau : routage



La figure ci-dessus illustre l'ordre d'application des différents types de routage.

**NOTE** : Si un objet routeur est utilisé dans le routage par politique et qu'aucune passerelle n'est joignable, deux options sont possibles : le routage est délégué au routage par défaut ou bien le trafic est bloqué par le firewall. Ces options ne sont pas possibles si l'objet routeur est utilisé dans le routage par défaut.

## RECOMMANDATIONS



- Désactiver les interfaces non utilisées
- Déclarer les interfaces internes
- Définir des routes statiques pour les réseaux internes

Si une interface n'est pas utilisée, il est recommandé de la désactiver pour éviter toute arrivée de trafic par celle-ci.

Afin de profiter des mécanismes d'antispoofing, il est recommandé de déclarer une interface « interne » dès que possible.

Si une alarme de ce type se déclenche, il y a très probablement un problème d'architecture à corriger.

**Attention** : les modes d'inspection IDS et firewall court-circuitent l'antispoofing.

Afin de légitimer les réseaux joignables depuis une interface, il faut qu'ils soient connus par le firewall. Pour cela, il est nécessaire d'avoir une route partant d'une interface protégée vers ces réseaux. A l'inverse, tout réseau injoignable défini dans la table de routage risque d'entraver le mécanisme d'antispoofing. Il est donc recommandé de ne jamais laisser de route inutile dans la table de routage.



Pour aller plus loin, consultez les notes techniques du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Configurer un modem 3G/4G sur SNS
- Encapsulation niveau 2
- Stacking : répartition de trafic sur plusieurs firewalls
- Agrégation de liens LACP
- Routage dynamique BIRD V3
- Configurer la QoS sur les firewalls SNS
- SD-WAN - Sélectionner le meilleur lien réseau

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Modes de configuration
- Types d'interfaces
- Lab – Configuration réseau : interfaces
- Routage système
- Routage avancé
- Ordonnancement des types de routage
- ➔ **Lab – Configuration réseau : routage**

STORMSHIELD

Configuration réseau



## Lab 3 – Configuration réseau : routage

### Configuration du routage :

1. Configurez la passerelle par défaut de votre firewall « 192.36.253.1 ».
2. Configurez le routage statique sur votre firewall pour permettre à votre station « Client\_TRAINING\_x » de joindre le réseau interne « 192.168.x.0/24 » de l'entreprise distante.

### • Configuration du proxy cache DNS :

Activez le proxy cache DNS . Le proxy cache DNS n'est pas abordé en cours, mais il doit être utilisé lors de ces labs pour permettre la résolution de noms DNS de façon correcte. La page suivante donne plus d'indications sur cette option et la manière de la configurer.

Le firewall intercepte les requêtes DNS à destination d'Internet, et effectue lui-même la requête vers le serveur DNS configuré dans le lab 2, point 9.

Si le nom demandé est dans son cache, le firewall répond directement à la demande selon les informations qu'il possède.

Cette technique de Proxy cache DNS est détaillée dans les annexes de la configuration réseau.

Effectuez la configuration comme suit :

- Rendez-vous dans le menu **CONFIGURATION** ⇒ **Réseau** ⇒ **Proxy cache DNS** et activez le cache DNS.
- L'objet autorisé à utiliser ce cache est votre serveur DNS présent sur la DMZ (172.16.x.10), ajoutez-le dans la « liste des clients autorisés à utiliser le cache DNS ».

The screenshot shows the 'NETWORK / DNS CACHE PROXY' configuration window. At the top, there is a toggle switch labeled 'ON'. Below it, the title 'LIST OF CLIENTS ALLOWED TO USE THE DNS CACHE' is displayed. A search bar with the text 'Searching...' and buttons for '+ Add' and 'X Delete' is present. A table lists the authorized clients, with 'srv\_dns' highlighted in green. Below the table, the 'Advanced properties' section is expanded, showing a 'Cache size (in bytes)' field set to '1000000'. There are two checkboxes: 'Transparent mode (intercepts all DNS queries sent by authorized clients)' which is unchecked, and 'Random querying of domain name servers' which is checked. At the bottom, there are 'CANCEL' and 'APPLY' buttons.



# Quiz

STORMSHIELD

Q1 – Les objets routeurs peuvent être utilisés comme route par défaut :


- A. Vrai
- B. Faux

Q2 – Une route de retour est obligatoire pour joindre l'Internet :

- A. Vrai
- B. Faux

Q3 – Un bridge contenant les interfaces dmz1 et dmz2 permet aux machines connectées sur ces deux interfaces de communiquer directement sans filtrage ni analyse.

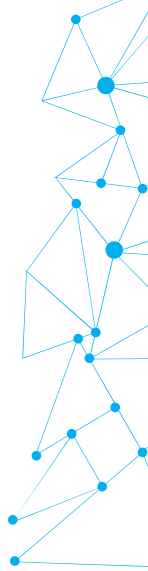
- A. Vrai
- B. Faux



STORMSHIELD

# ANNEXE - CONFIGURATION RÉSEAU

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



## → Interfaces Modem

- Interfaces Wifi
- DNS dynamique
- DHCP
- Routage multicast statique
- Proxy cache DNS
- Routage statique avec Bird
- Routage dynamique avec Bird

STORMSHIELD

Configuration réseau

## INTERFACES MODEM

- Modem PPTP/PPPOE : création et configuration générale

Le firewall peut être raccordé à différents types de modem :

- Un modem ADSL ou câble : raccordé à une interface Ethernet (exemple montré ci-dessus),
- Un modem 3G/4G : raccordé au port USB (diapositive suivante).

Le nombre maximal de modems qui peuvent être raccordés en même temps dépend du modèle de firewall.

La figure ci-dessus illustre l'onglet **CONFIGURATION GÉNÉRALE**, affiché juste après l'avertissement qui précise qu'une route par défaut devra être créée après la configuration du modem :

- **Identification du modem** : nommage de l'interface et ajout d'un commentaire facultatif,
- **Configuration du modem** : les paramètres de ce menu changent en fonction du type du modem choisi:
  - **PPPoE**: Le modem doit être connecté à une interface externe qui doit être choisie dans le paramètre **Interface parente**,
  - **PPTP**: La négociation PPTP nécessite l'adresse IP du serveur PPTP qui doit être renseignée dans le paramètre **Adresse PPTP**,
- **Authentification** : Permet de renseigner l'identifiant et le mot de passe utilisés par la connexion modem. Ces informations sont transmises par le fournisseur d'accès.

**NOTE** : l'onglet **CONFIGURATION AVANCÉE** d'un modem PPTP ou PPPoE permet de choisir si la connectivité est permanente ou à la demande.

### INTERFACES MODEM

- Modem 3G/4G : création du profil et de l'interface

STORMSHIELD

4

Il existe deux types de modems 3G/4G :

- Modem Ethernet over USB : une fois le modem connecté au firewall et configuré, c'est le modem qui porte l'adresse IP publique et opère alors comme un routeur vis-à-vis du firewall,
- Modem USB : une fois le modem connecté au firewall et configuré, c'est le firewall qui porte l'adresse IP publique.

Avant de créer l'interface modem, il faut configurer un profil selon les paramètres de configuration fournis par le constructeur du modem. Pour plus de détails, reportez-vous à la note technique : « Configurer un modem 3G/4G sur SNS ». Les éléments à préciser sur le profil sont déterminés par la procédure de la note technique.

Un redémarrage du firewall est nécessaire après la création du profil.

Après redémarrage, créez l'interface, et attachez le profil préalablement configuré à cette interface.



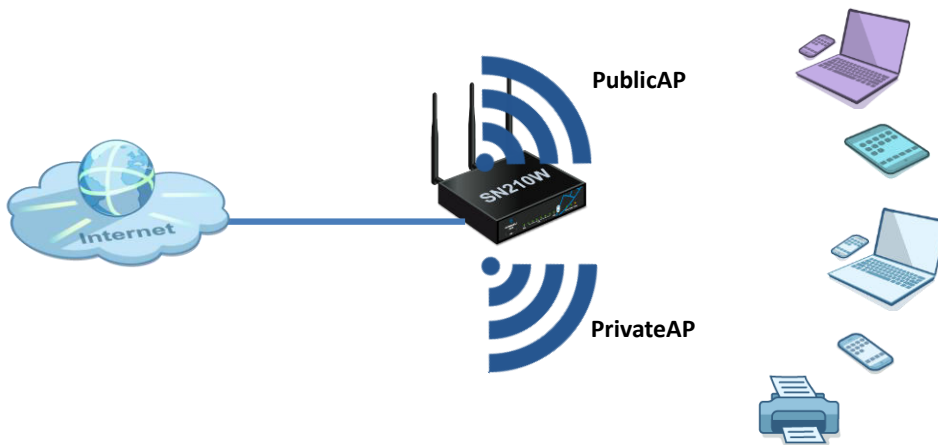
- Interfaces Modem
- ➔ **Interfaces Wifi**
- DNS dynamique
- DHCP
- Routage multicast statique
- Proxy cache DNS
- Routage statique avec Bird
- Routage dynamique avec Bird

STORMSHIELD

Configuration réseau

## INTERFACES WIFI

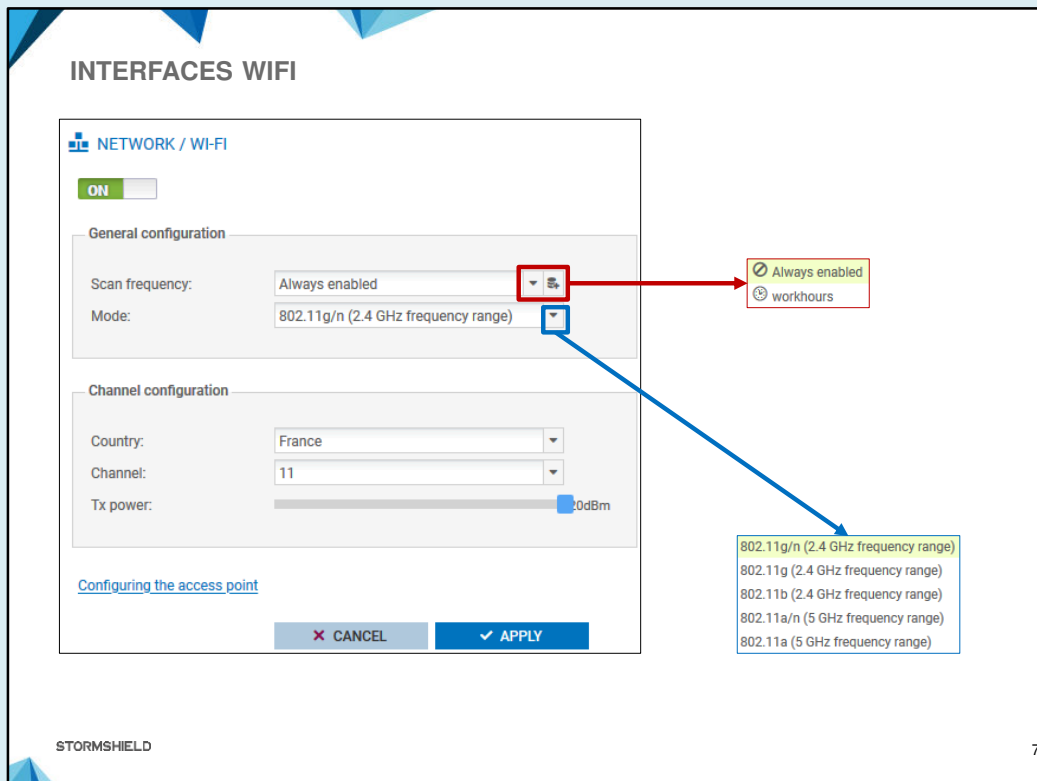
- Disponibles seulement sur SN160W et SN210W
- Possibilité d'activer deux réseaux WIFI



STORMSHIELD

6

Les firewalls SN160W et SN210W embarquent une carte WIFI 802.11 a/b/g/n qui permet de configurer deux points d'accès WLAN distincts pour la connexion des équipements sans fil sur les bandes de fréquence à 2,4 GHz ou 5 GHz.



Pour activer la carte Wi-Fi, cochez l'option **Activer le Wi-Fi** dans le menu **CONFIGURATION ⇒ RÉSEAU ⇒ Wi-Fi**. Le menu permet également de configurer les paramètres suivants :

- **Configuration générale :**

- **Planification** : sélectionner ou créer un objet temps pour définir la période d'activation de la carte Wi-Fi.
- **Mode** : sélectionner la norme de transmission qui est utilisée par la carte WiFi :
  - 802.11b, 802.11g, 802.11g/n à 2,4 GHz.
  - 802,11a, 802,11a/n à 5 GHz.

**INTERFACES WIFI**

**NETWORK / WI-FI**

**ON**

General configuration

Scan frequency: Always enabled

Mode: 802.11g/n (2.4 GHz frequency range)

Channel configuration

Country: France

Channel: 11

Tx power: 0dBm

[Configuring the access point](#)

**CANCEL** **APPLY**

Canaux disponibles :

à 2,4 GHz      à 5 GHz

1	36
2	40
3	44
4	48
5	
6	
7	
8	
9	
10	
11	
12	
13	

STORMSHIELD 8

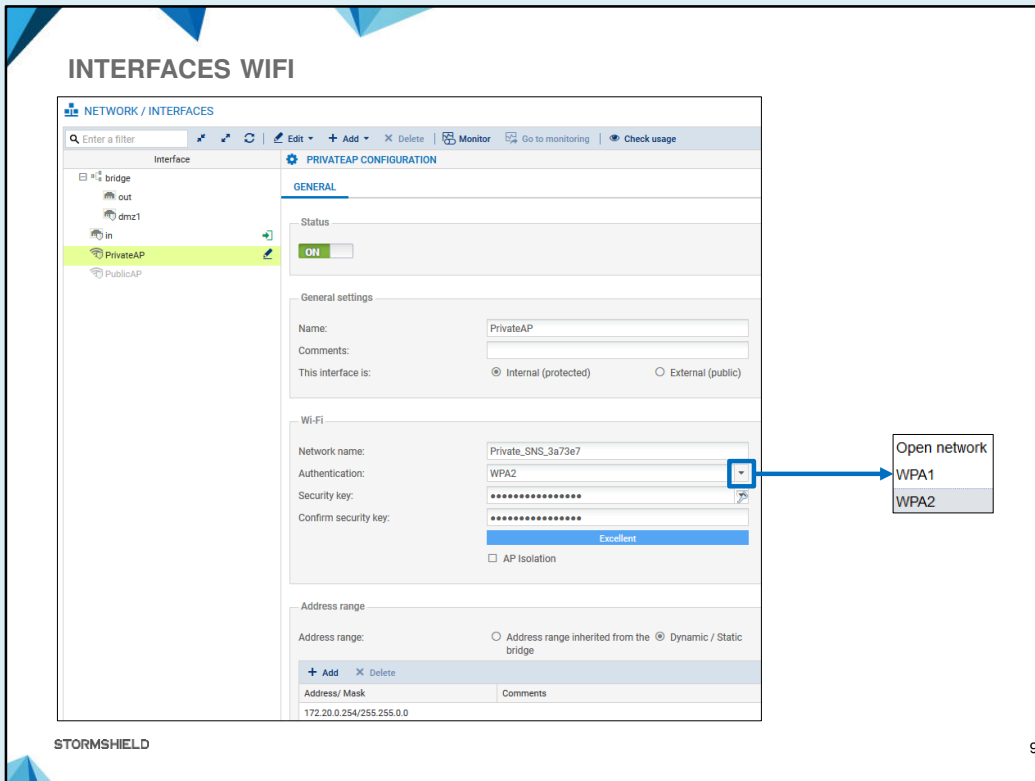
• **Configuration des canaux :**

- **Pays :** choisir le pays dans lequel le firewall est installé pour que la transmission Wi-Fi soit en conformité avec la réglementation du pays. Ce choix influe sur les canaux de communication disponibles ainsi que sur la puissance du signal.
- **Canal :** sélectionner le canal utilisé par la carte Wi-Fi. Les canaux proposés dépendent du pays et du mode sélectionnés.
- **Puissance du signal :** régler la puissance de transmission de la carte Wi-Fi. Les puissances proposées dépendent du pays sélectionné.

- Configuration des points d'accès : renvoie vers le menu **CONFIGURATION ⇒ RÉSEAU ⇒ Interfaces**

**NOTES :**

- Les paramètres ci-dessus sont communs aux deux points d'accès WLAN.
- Si vous avez d'autres points d'accès Wi-Fi dans votre entreprise, évitez l'utilisation de canaux identiques ou se recouvrant pour limiter les interférences sur votre réseau sans-fil :
  - À la fréquence de 2,4 GHz, seuls les 3 canaux 1, 6 et 11 sont non-recouvrants.
  - À la fréquence de 5 GHz, il n'y a pas de recouvrement des canaux.



Après l'activation de la carte Wi-Fi, vous pouvez configurer les deux points d'accès dans le menu **CONFIGURATION ⇒ RÉSEAU ⇒ Interfaces**

Les deux points d'accès correspondent aux interfaces WLAN **PrivateAP** et **PublicAP** qui sont désactivées par défaut. Vous pouvez les activer simultanément avec des configurations différentes, ce qui permet d'avoir deux réseaux WLAN distincts pouvant être gérés séparément dans les autres modules : DHCP, filtrage, translation, authentification, etc.

Les paramètres des deux interfaces sont identiques :

- **Nom** : le nom de l'interface WLAN.
- **Commentaire** (facultatif).
- **Cette interface est** : Permet de spécifier si l'interface WLAN doit être considérée comme « interne (protégée) » ou « externe (publique) », veuillez vous référer au chapitre Types d'interfaces du module Configuration réseau pour avoir plus de détails.
- **Wi-Fi** :
  - **Nom du réseau** : représente le SSID (Service Set Identifier); le nom du réseau Wi-Fi qui est vu par les équipements sans fil,
  - **Authentification** : Trois méthodes sont disponibles :
    - **Réseau ouvert** : aucune méthode d'authentification et aucun chiffrement.
    - **WPA1 (Wi-Fi Protected Access)** : l'authentification se base sur une clé pré-partagée et les données sont chiffrées avec l'algorithme flot RC4 (une clé de 128 bits et un vecteur d'initialisation).



- **WPA2** (recommandée) : C'est une évolution du WPA1, l'authentification se base également sur une clé pré-partagée mais les données sont chiffrées avec CCMP qui utilise l'algorithme AES avec une clé de 128bits.
- **Clé de sécurité** : la clé pré-partagée utilisée pour l'authentification WPA et WPA2.
- **Isolation AP (Access Point)** : Cette fonctionnalité permet d'interdire à deux équipements connectés au réseau WLAN de dialoguer directement entre eux sans passer par le point d'accès, c'est-à-dire, le firewall. Elle est activée par défaut.

**NOTES :**

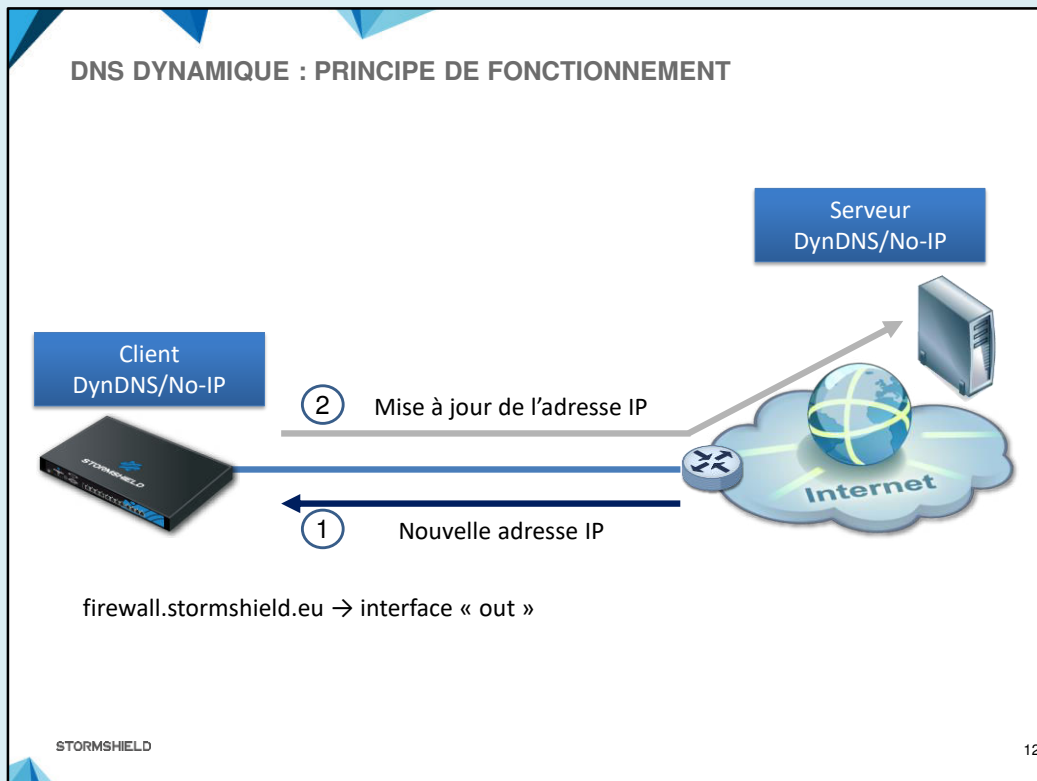
- Après la configuration d'une interface WLAN, vous devez configurer le serveur DHCP pour attribuer automatiquement des adresses IP aux équipements qui se connectent au WLAN. Pour cela, veuillez vous référer au chapitre DHCP de ce module.
- Les interfaces WLAN peuvent appartenir à un bridge.
- Les interfaces VLAN ne peuvent pas avoir pour interface parente une interface WLAN.



- Interfaces Modem
- Interfaces Wifi
- ➔ **DNS dynamique**
- DHCP
- Routage multicast statique
- Proxy cache DNS
- Routage statique avec Bird
- Routage dynamique avec Bird

STORMSHIELD

Configuration réseau



Le DNS dynamique permet d'associer un nom de domaine à un firewall qui ne possède pas une adresse IP publique fixe. Ainsi, le firewall sera toujours accessible en utilisant son nom de domaine. Cette fonctionnalité est basée sur un fournisseur de service DNS. Les firewalls Stormshield Network supportent deux fournisseurs : DynDNS et No-IP.

Le principe de fonctionnement est illustré dans la figure ci-dessus. Elle fait intervenir deux entités : un client intégré au firewall Stormshield Network qui transmet des mises à jour d'adresse IP à un serveur maintenu par le fournisseur de service DNS. Le nom du domaine est associé à une interface. La mise à jour est effectuée à chaque fois que l'adresse IP de l'interface change. Dans le cas où l'adresse ne change pas, une mise à jour est effectuée par défaut tous les 28 jours.

## DNS DYNAMIQUE : MENU DE CONFIGURATION

STORMSHIELD

13

Le DNS dynamique est configurable dans le menu **CONFIGURATION** ⇒ **RÉSEAU** ⇒ **DNS dynamique**.

La page du menu est constituée de deux parties :

1. **Liste des Profils DNS dynamique** : Il est possible d'ajouter, supprimer et de réinitialiser des profils. Un profil peut être activé/désactivé avec un double clic sur le champ **État**. Le bouton **Réinitialiser** s'active pour un profil lorsque la communication avec le fournisseur de service DNS échoue. Ce bouton relance une nouvelle tentative de communication.
2. **Les paramètres du profil DNS dynamique** :
  - **Nom du domaine** : Renseigne le nom du domaine qui sera utilisé pour accéder au firewall. Par exemple : firewall.stormshield.eu.
  - **Interface associée au nom du domaine** : L'interface dont l'adresse IP est associée au nom du domaine. Une interface ne peut pas être utilisée par deux profils différents.
  - **Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard)**: Si cette option est cochée, tous les sous-domaines (www.firewall.stormshield.eu) du domaine renseigné ci-dessus (firewall.stormshield.eu) seront associés à la même adresse IP.
  - **Fournisseur DNS dynamique** : Indique le fournisseur de service DNS utilisé par le profil. Actuellement, deux fournisseurs de service sont supportés : DynDNS et No-IP.



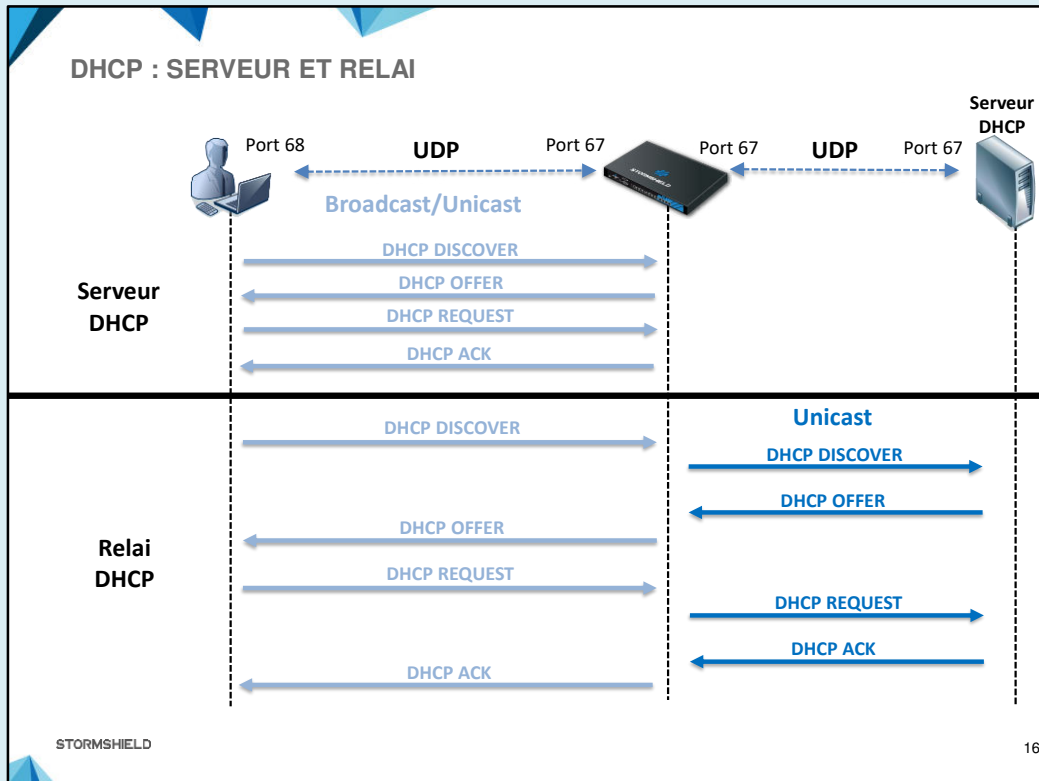
- **Nom d'utilisateur** et **Mot de passe** : L'identifiant et le mot de passe utilisés pour authentifier le client auprès du fournisseur de service DNS.
- **Serveur DNS dynamique** : Indique le serveur du fournisseur de service DNS sous la forme d'un objet machine dont le nom est résolu automatiquement (voir le Module « Objets »).
- **Service DNS dynamique** : Indique le service souscrit auprès du fournisseur de service DNS.



- Interfaces Modem
- Interfaces Wifi
- DNS dynamique
- ➔ **DHCP**
- Routage multicast statique
- Proxy cache DNS
- Routage statique avec Bird
- Routage dynamique avec Bird

STORMSHIELD

Configuration réseau



Le firewall Stormshield Network intègre un serveur et un relai DHCP :

- **Serveur DHCP** : Permet de gérer dynamiquement l'attribution d'adresses IP dans un LAN. Les messages DHCP sont échangés en broadcast ou en unicast entre le client et le firewall en se basant sur le protocole UDP (port 68 côté client et port 67 côté serveur). Ces échanges sont illustrés dans la figure ci-dessus. Les échanges débutent par l'envoi d'un message « DHCP DISCOVER » par le client afin de découvrir le(s) serveur(s) DHCP présent(s) sur le LAN. Le firewall répond par un message « DHCP OFFER » qui contient une offre d'adresse IP avec tous les paramètres nécessaires (passerelle, DNS, etc). Le client retient l'offre en renvoyant un message « DHCP REQUEST » avec l'adresse IP désirée (annoncée pendant le DHCP OFFER). Le serveur termine l'échange en acquittant la requête du client par un message « DHCP ACK ». L'adresse IP sera valable durant un bail déterminé. Le serveur DHCP est opérationnel uniquement sur les interfaces internes (protégées) du firewall.
- **Relai DHCP** : Le firewall va relayer les messages DHCP entre le client et un serveur situé sur un autre réseau. Les messages DHCP sont relayés en unicast entre le firewall et le serveur DHCP.

Le firewall ne peut gérer les fonctions de serveur et relai DHCP simultanément.

### DHCP : SERVEUR ET RELAI

**NETWORK / DHCP**

**General**

ON

DHCP server  
 DHCP relay

**Default settings**

Domain name:

Gateway:

Primary DNS:

Secondary DNS:

**ADDRESS RANGE**

Searching...

Address range	Gateway	Primary DNS	Secondary DNS	Domain name
dhcp_in_range	Firewall_in	srv_dns_priv	default	intranet.training.local
dhcp_wifi_range	Firewall_dmz1	dns1.google.com	dns2.google.com	guest.training.local

STORMSHIELD

17

La configuration du serveur ou du relai DHCP s'effectue dans le menu **CONFIGURATION ⇒ RÉSEAU ⇒ DHCP**. La composition du menu diffère en fonction du service sélectionné :

- **Serveur DHCP:**

L'encadré **Paramètres** permet de définir les informations par défaut transmises aux clients DHCP : **Nom de domaine**, **Passerelle par défaut**, **Serveur DNS primaire** et **Serveur DNS secondaire**. Ces informations peuvent être personnalisées pour chaque plage d'adresse définie dans l'encadré **PLAGE D'ADRESSES**. Les plages doivent respecter les conditions suivantes :

- Une plage doit appartenir au même plan d'adressage que celui d'une interface protégée.
- Deux plages d'adresses IP ne doivent pas se chevaucher.
- La passerelle spécifiée pour une plage doit être dans le même plan d'adressage.

## DHCP : SERVEUR ET RELAI

The screenshot displays the DHCP configuration interface for a server and relay. At the top, the 'RESERVATION' section shows a table with columns for Reservation, Gateway, Primary DNS, Secondary DNS, and Domain name. A reservation for 'pc\_admin' is highlighted, with a blue box around the name and an arrow pointing to its properties.

Reservation	Gateway	Primary DNS	Secondary DNS	Domain name
pc_admin	Firewall_In	srv_dns_priv	default	Default domain

The 'PROPERTIES' section for the reservation 'pc\_admin' shows:

- Object name: pc\_admin
- IPv4 address: 192.168.1.2
- MAC address: 5c:26:da:87:bf:22
- Resolution:  None (static IP)  Automatic
- Comments: DHCP reservation

The 'Advanced configuration' section includes:

- File name: [ ]
- SMTP Server: [ ]
- POP Server: [ ]
- Next server: [ ]
- News Server (NNTP): [ ]
- TFTP Server: [ ]
- Distribute the Web proxy autodiscovery (WPAD) file
- Update DNS server entries
- Assigned lease time:
  - Default (Hour): 24
  - Minimum (Hour): 1
  - Maximum (Hour): 168

STORMSHIELD

18

Toujours dans le même menu, la partie **RÉSERVATION** permet de réserver des adresses IP fixes pour des machines dans le LAN, identifiées par leur adresse MAC.

**Attention** : Les adresses IP réservées doivent être en dehors des plages d'adresses renseignées dans l'onglet précédent.

La réservation s'effectue en ajoutant une ligne dans la liste avec le bouton **Ajouter**. Un objet machine doit être renseigné dans le champ **Réservation**. Cet objet doit contenir l'adresse IP qui sera assignée au client et l'adresse MAC de la machine qui obtiendra cette adresse IP. Si l'objet machine renseigné ne contient pas d'adresse MAC, une erreur s'affiche pour informer de l'impossibilité de trouver une adresse MAC pour la machine. Il est possible de renseigner une passerelle spécifique pour l'adresse IP réservée dans le champ **Passerelle**.

Dans la **configuration avancée**, des éléments complémentaires peuvent être transmis aux clients et la durée de bail attribuée peut être modifiée.

**DHCP : SERVEUR ET RELAI**

NETWORK / DHCP

General

ON

DHCP server

DHCP relay

Default settings

DHCP server(s):

IP address used to relay DHCP queries:

Relay DHCP queries for all interfaces.

LISTENING INTERFACES ON THE DHCP RELAY SERVICE

+ Add X Delete

Interface

STORMSHIELD

19

- **Relai DHCP**

Dans l'encadré **Paramètres** l'objet correspondant au serveur DHCP vers lequel les messages DHCP vont être relayés est à renseigner. L'option **Adresse IP utilisée pour relayer les requêtes DHCP** permet quant à elle de choisir l'adresse IP source des requêtes DHCP relayées par le firewall (interface côté serveur). Par conséquent, seuls les objets « Firewall\_ » y sont listés.

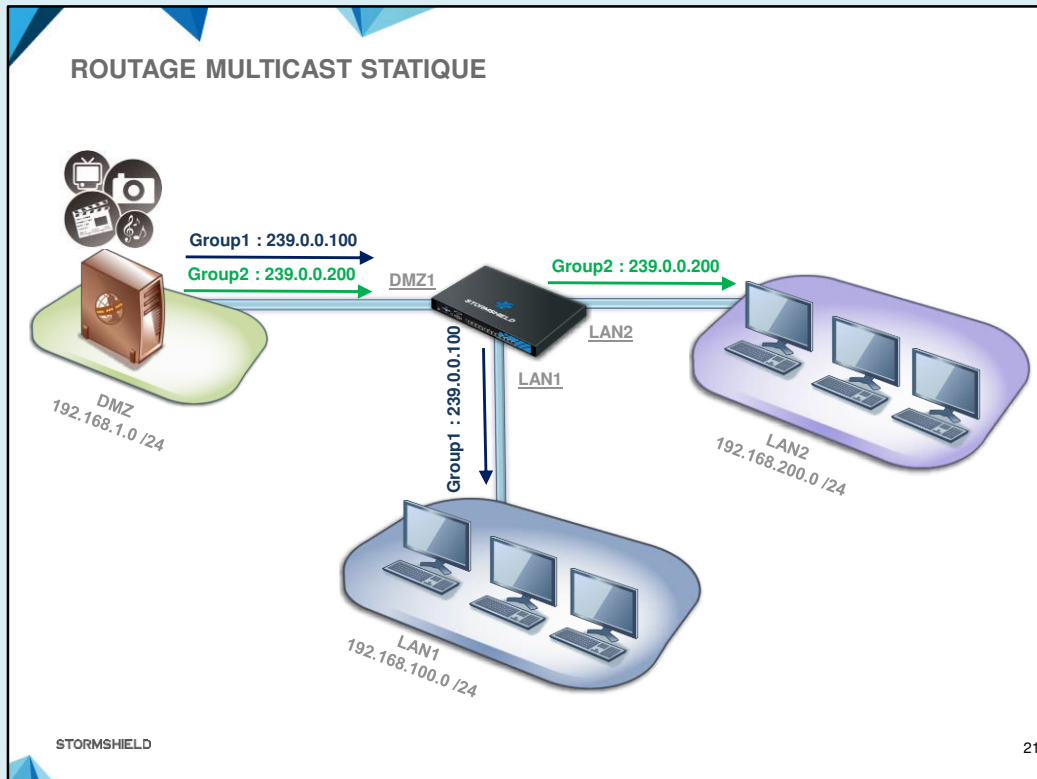
Si l'option **Relayer les requêtes DHCP pour toutes les interfaces** est cochée, le firewall écoutera les requêtes des clients sur l'ensemble de ses interfaces réseaux (la liste suivante est alors grisée). Dans le cas contraire, la liste suivante permet de préciser les interfaces pour lesquelles les requêtes doivent être relayées.



- Interfaces Modem
- Interfaces Wifi
- DNS dynamique
- DHCP
- ➔ **Routage multicast statique**
  - Proxy cache DNS
  - Routage statique avec Bird
  - Routage dynamique avec Bird

STORMSHIELD

Configuration réseau



Contrairement à une transmission unicast où un exemplaire d'un flux est envoyé à chaque destinataire, une transmission multicast permet de diffuser un seul exemplaire d'un flux vers un groupe de destinataires identifié par une adresse IP multicast (classe D 224.0.0.0/8 à 239.255.255.255/8). Ce mode de transmission est utilisé principalement pour diffuser des flux multimédia temps réel (Radios, TVs, conférences, etc.). Pour recevoir un flux, l'utilisateur doit s'abonner au groupe multicast en utilisant le protocole IGMP (Internet Group Management Protocol). Les requêtes IGMP sont reçues par le routeur d'accès qui doit gérer les groupes multicast (abonnement, désabonnement, vérifier la présence des abonnés) au niveau du réseau interne et récupérer les flux multicast en utilisant un protocole de routage multicast (PIM-SM, PIM-DM, PIM-BIDIR, PIM-SSM, DVMRP et MOSPF) avec les autres routeurs.

Le routage multicast statique implémenté sur les Firewalls SNS permet de renvoyer un flux multicast reçu par une interface vers une autre interface, quel que soit leur type (physique, BRIDGE, VLAN, GRE, GRE-TAP) à l'exception des interfaces IPsec et HA (utilisée dans un cluster de haute disponibilité). Dans l'exemple ci-dessus, le serveur dans le réseau DMZ transmet deux flux multicast (GROUP1 et GROUP2) qui sont reçus par l'interface DMZ1. Le GROUP1 et le GROUP2 sont routés respectivement à destination de l'interface LAN1 et LAN2 pour que chaque flux soit reçu seulement par les stations connectées au réseau de l'interface de destination.

**Note :**

- Pour le moment, les firewalls SNS ne permettent pas de gérer les groupes multicast en utilisant IGMP et n'implémentent pas de protocoles de routage multicast.

### ROUTAGE MULTICAST STATIQUE

The image shows the configuration process for static multicast routing in Stormshield. It consists of three main parts:

- NEW ROUTING RULE (Left):** A dialog box titled "SELECTING THE MULTICAST GROUP AND THE SOURCE INTERFACE". It contains fields for "Multicast group" (set to "multicast\_address\_1") and "Source interface" (set to "dmz1").
- NEW ROUTING RULE (Right):** A dialog box titled "SELECTING THE DESTINATION INTERFACES". It features a table with one entry: "LAN1".
- NETWORK / MULTICAST ROUTING (Bottom):** A configuration panel where the "MULTICAST ROUTING" toggle is set to "ON". Below it, a table lists static routes. The "Add" button is highlighted with a blue box, and an arrow points from it to the "NEW ROUTING RULE" dialog.

↑	Status	Source interface	Destination interfaces
1	on	multicast_address_100@dmz1	LAN1

STORMSHIELD

22

La configuration du routage multicast statique s'effectue dans le menu **CONFIGURATION ⇒ RÉSEAU ⇒ Routage multicast**

Pour ajouter une route, il suffit de cliquer sur **Ajouter** qui lance un assistant dont la première fenêtre permet de renseigner l'adresse ou le réseau multicast et l'interface source. La deuxième fenêtre, quant-à-elle, permet de renseigner les interfaces de destination.

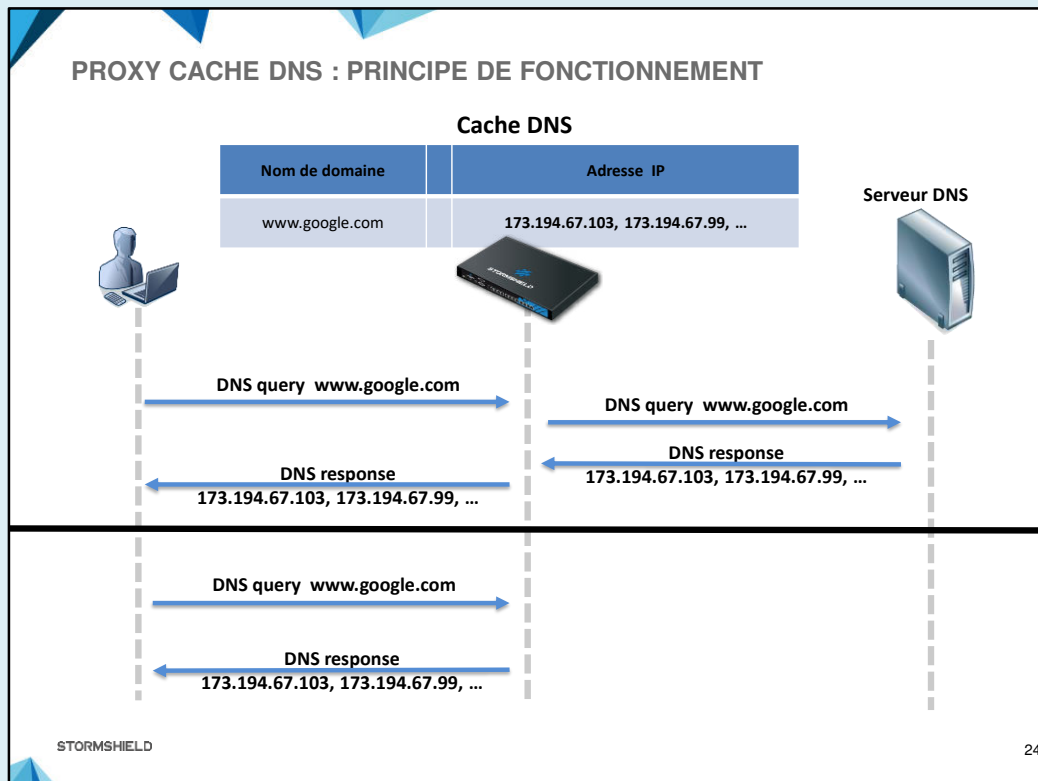
Enfin, il faut activer le routage en cochant le paramètre **Activer le routage multicast statique**.



- Interfaces Modem
- Interfaces Wifi
- DNS dynamique
- DHCP
- Routage multicast statique
- ➔ **Proxy cache DNS**
- Routage statique avec Bird
- Routage dynamique avec Bird

STORMSHIELD

Configuration réseau



La fonctionnalité proxy cache DNS permet de stocker les adresses IP des noms résolus par des requêtes DNS afin de préserver la bande passante en évitant plusieurs résolutions du même nom. Cette fonctionnalité peut être mise en œuvre dans deux cas de figure :

- Dans le premier cas, le réseau local utilise le firewall comme un serveur DNS. La requête DNS est reçue par le firewall qui vérifie la présence du nom dans le cache. Si le nom n'existe pas, il effectue une résolution en utilisant ses serveurs DNS; il ajoute dans le cache le nom accompagné des adresses IP et il envoie enfin une réponse DNS au réseau local. Si le nom existe dans le cache, le firewall envoie une réponse DNS en se basant sur les informations présentes.
- Dans le deuxième cas, le réseau local utilise n'importe quel serveur DNS. La requête DNS destinée au serveur X est interceptée par le firewall qui commence par vérifier la présence du nom dans le cache. Si le nom n'existe pas, il effectue une résolution en utilisant ses serveurs DNS et non le serveur X; il ajoute dans le cache le nom accompagné des adresses IP et enfin il envoie une réponse DNS au réseau local en usurpant l'adresse IP du serveur X ce qui fait croire au réseau local que la résolution a été effectuée par ce serveur. Si le nom existe dans le cache, le firewall envoie une réponse DNS basée sur les informations existantes, en usurpant également l'adresse IP du serveur X.

## PROXY CACHE DNS : MENU DE CONFIGURATION

NETWORK / DNS CACHE PROXY

**ON**

LIST OF CLIENTS ALLOWED TO USE THE DNS CACHE

Searching... + Add X Delete

DNS client [host, network, range, group]

srv\_dns\_priv

Advanced properties

Cache size (in bytes): 1000000

Transparent mode (intercepts all DNS queries sent by authorized clients)

Random querying of domain name servers

X CANCEL ✓ APPLY

STORMSHIELD

25

Le menu **CONFIGURATION** ⇒ **Réseau** ⇒ **Proxy cache DNS** permet d'activer le cache DNS. Les objets autorisés à utiliser ce cache doivent être explicitement ajoutés dans la « liste des clients autorisés à utiliser le cache DNS ». Ces objets peuvent être des machines, des réseaux, des plages d'adresses ou des groupes.

Dans la configuration avancée, il est possible de :

- Modifier la taille du cache qui est par défaut fixée à 1Mo.
- L'option **Mode transparent (intercepte toutes les requêtes DNS émises par les clients autorisés)** doit être cochée pour le fonctionnement du cache DNS dans le 2<sup>ème</sup> cas de figure présenté précédemment.
- L'option **interrogation aléatoire des serveurs DNS** permet au firewall d'utiliser aléatoirement la liste de ses serveurs DNS configurée dans le menu **SYSTÈME** ⇒ **Configuration** ⇒ **PARAMÈTRES RÉSEAUX** ⇒ **Résolution DNS**.



- Interfaces Modem
- Interfaces Wifi
- DNS dynamique
- DHCP
- Routage multicast statique
- Proxy cache DNS
- ➔ **Routage statique avec Bird**
- Routage dynamique avec Bird

STORMSHIELD

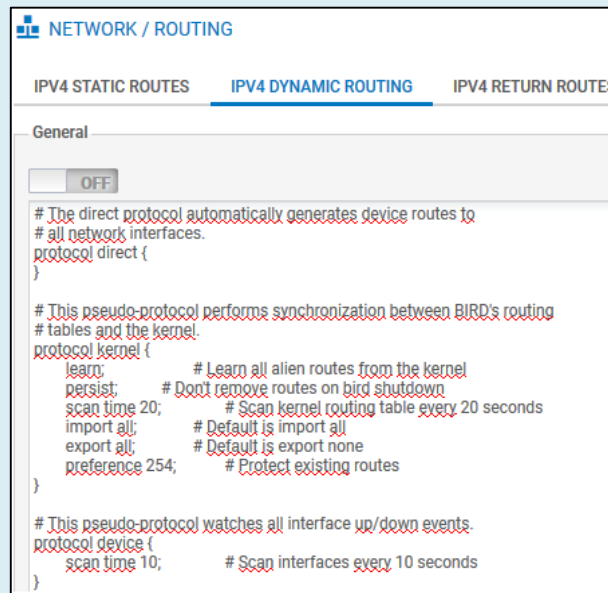
Configuration réseau

## Routage statique avec Bird

### Injection de routes

Bird fournit la possibilité d'injecter des routes dans la table de routage du système FreeBSD, et réciproquement d'apprendre les routes déjà présentes dans la table de routage (pour permettre par exemple leur redistribution via des protocoles de routage dynamique).

Le fichier de configuration Bird par défaut visible en interface graphique est le suivant :



```

NETWORK / ROUTING

IPV4 STATIC ROUTES  IPV4 DYNAMIC ROUTING  IPV4 RETURN ROUTES

General

OFF

# The direct protocol automatically generates device routes to
# all network interfaces.
protocol direct {
}

# This pseudo-protocol performs synchronization between BIRD's routing
# tables and the kernel.
protocol kernel {
  learn;          # Learn all alien routes from the kernel
  persist;       # Don't remove routes on bird shutdown
  scan time 20;  # Scan kernel routing table every 20 seconds
  import all;    # Default is import all
  export all;    # Default is export none
  preference 254; # Protect existing routes
}

# This pseudo-protocol watches all interface up/down events.
protocol device {
  scan time 10;  # Scan interfaces every 10 seconds
}

```

Les sections visibles dans ce fichier (pseudo-protocoles) conditionnent les interactions entre Bird et le système, dans l'ordre :

- Protocol direct : permet l'export vers Bird des routes vers les réseaux directement connectés aux interfaces locales du firewall.
- Protocol kernel : permet la synchronisation entre la table de routage de Bird et celle du système.
- Protocol device : surveille l'état des liens sur les interfaces (lors de la désactivation d'une interface par exemple, les routes devant transiter par cette interface sont supprimées de la table de routage du système).

### Commandes Bird

Pour visualiser des informations sur les routes, l'état des interfaces, ou autres dans Bird, lorsque vous aurez activé le routage dynamique via l'interface web, vous pourrez utiliser les commandes suivantes :

```

VMSNSX09K0639A9>birdc
BIRD 1.6.7 ready.
bird> show ?
show bfd ...           Show information about BFD protocol
show interfaces        Show network interfaces
show memory            Show memory usage
show ospf ...         Show information about OSPF protocol
show protocols [<protocol> | "<pattern>"] Show routing protocols
show rip ...          Show information about RIP protocol
show roa ...          Show ROA table
show route ...        Show routing table
show static [<name>] Show details of static protocol
show status           Show router status
show symbols ...      Show all known symbolic names

```

Testez la commande « show interfaces », par exemple, particulièrement utile pour voir l'état de chaque interface, son nom système et son nom d'usage. Par ailleurs, lorsque vous avez poussé une configuration, prenez l'habitude de comparer la table de routage de Bird (show route), et la table de routage de FreeBSD (netstat -rn).

### **Configuration du routage statique**

La section suivante doit être ajoutée aux sections présentées auparavant :

```
protocol static {
    check link;                # Advertise routes only if link is up
    route 192.168.2.0/24 via 172.20.0.1;
}
```

### **Tolérance aux pannes**

L'utilisation de deux liens avec une priorité différente est fonctionnelle sur les firewalls Stormshield :

```
protocol static via_vti1{
    check link;
    route 192.168.2.0/24 via 172.20.0.1 ;
    preference 200 ;          #high-priority
}
protocol static via_vti2{
    check link;
    route 192.168.2.0/24 via 172.20.0.3 ;
    preference 100 ;         #low-priority
}
```

La détection de panne dépend entre autres de l'état des interfaces. Ce point est inopérant sur une interface VTI, ces dernières étant toujours actives du point de vue d'un firewall. Pour provoquer une bascule rapide en cas de dysfonctionnement d'un lien, il est possible d'utiliser BFD (Bidirectionnal Forwarding Detection). Ce n'est pas un protocole de routage, mais un outil indépendant (fonctionnel également avec le routage dynamique). Il permet une détection de panne sur un lien en surveillant une session créée par l'envoi de paquets UDP (port 3784). Une fois une instance de BFD créée, elle doit être attachée à la route statique correspondante.

```
protocol bfd {
    interface "enc1"{
        interval 1 s;          #frequency of sending BFD control
messages for established BFD session
        multiplier 3;         #failure detection
        idle tx interval 1 s;  #frequency of sending BFD control
messages for not established BFD session
    };
}
```



- Interfaces Modem
- Interfaces Wifi
- DNS dynamique
- DHCP
- Routage multicast statique
- Proxy cache DNS
- Routage statique avec Bird
- ➔ **Routage dynamique avec Bird**

STORMSHIELD

Configuration réseau

## Routage dynamique avec Bird

(exemple avec OSPF)

### Introduction

Certains points importants sont à prendre en considération selon la topologie réseau, avant de configurer OSPF :

- Les liaisons sur lesquelles OSPF sera utilisé (par exemple type point à point).
- Les routes ne devant pas être exportées vers OSPF (par exemple les passerelles par défaut propres à chaque site, les réseaux ayant le même adressage sur tous les sites, etc.).
- Les interfaces sur lesquelles il est inutile d'activer du flux OSPF (interfaces internes d'un site par exemple).

### Éléments de réponse avec Bird

- Parmi les 5 types de réseaux définis par OSPF, le type Point à Point est le mieux approprié sur un lien via VTI, par exemple. Le paramètre `Bird` d'instance OSPF `pointopoint` sera donc utilisé (connexion directe de deux routeurs entre eux sans élection, l'adjacence sera plus rapide).
- Un filtre va préciser les réseaux à ne pas exporter (passerelle par défaut, etc.).
- Les messages OSPF ne seront envoyés qu'aux voisins déclarés avec le paramètre d'instance OSPF `strict nonbroadcast yes`. La liste des voisins sera déclarée avec le paramètre `neighbors`.

### Commandes Bird pour OSPF

Pour visualiser des informations sur les routes, l'état des interfaces, ou autres dans Bird, activez le routage dynamique via l'interface web. Puis, vous pourrez utiliser les commandes suivantes :

`bird>show ospf neighbors [nom_instance]` : état de l'adjacence.

`bird>show route` : toutes les routes connues par bird (route dynamiques et routes noyau).

`bird>show route export kernel1` : les routes exportées par bird vers la table de routage du noyau.

`bird>show ospf interface [nom_instance]`: paramètres détaillés de l'instance OSPF (aire, type de réseau, coût, temporisateurs, etc.).

`bird>show protocols all`: informations sur l'ensemble des pseudo-protocoles et protocoles utilisées (nombre de routes importées, exportées, préférences du protocole, etc.).

La commande « `show route export kernel1` », sera particulièrement utile pour vérifier les routes injectées par Bird dans le noyau, et modifier les filtres d'import-export en conséquence.

## Routage dynamique avec Bird (suite)

**Routage dynamique avec OSPF**

L'exemple ci-dessous se rapporte à une configuration OSPF via interface VTI (point à point) :

```
router id 172.20.0.0;
filter network {
    if net ~ [ 192.168.56.0/24, 0.0.0.0/0 ] then reject;
                                     # networks into [] rejected
    else accept;
}

# the direct protocol automatically generates device routes to
# all network interfaces.
protocol direct {
    preference 251;
}

# this pseudo-protocol performs synchronization between bird's
# routing tables and the kernel.
protocol kernel {
    learn;                # learn all alien routes from the kernel
    persist;             # don't remove routes on bird shutdown
    scan time 20;        # scan kernel routing table every 20s
    import filter network; # default is import all
    export filter network; # default is export none
    preference 254;      # protect existing routes
}

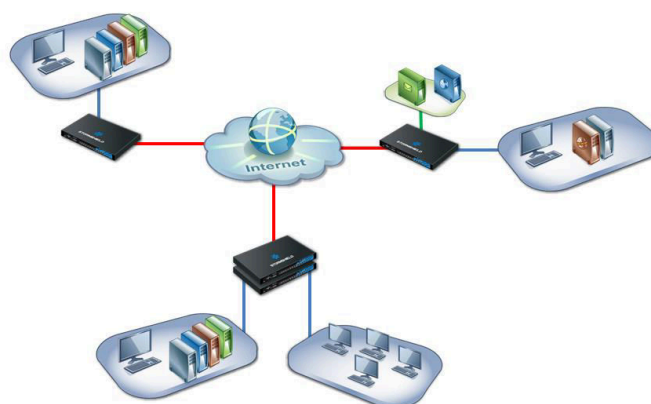
# this pseudo-protocol watches all interface up/down events.
protocol device {
    scan time 10;        # scan interfaces every 10 seconds
}

protocol ospf via_vti1 {
    tick 2;
    rfc1583compat yes;
    area 0 {
        stub no;
        interface "local_vti1_a" {
            # hello 10;
            # retransmit 6;
            # cost 10;
            # transmit delay 5;
            # dead count 5;
            # wait 50;
            type pointopoint;
            neighbors {
                172.20.0.1 eligible;
            };
            strict nonbroadcast yes;
        };
    };
    import filter network;
    export filter network;
}
```

**Note** : La documentation Bird [https://bird.network.cz/?get\\_doc&f=bird.html&v=20](https://bird.network.cz/?get_doc&f=bird.html&v=20) fournit beaucoup d'exemples, notamment de filtres à utiliser.



ADVANCED LAB – FONCTIONNALITÉS DHCP  
ADVANCED LAB – VLAN ET OBJETS ROUTEURS



STORMSHIELD

32

Advanced Labs disponibles à la fin du support de cours.



## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Les objets
- ✓ Configuration réseau
- Translation d'adresses
  - Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Généralités

- Translation dynamique
- Translation statique par port
- Translation statique
- Menu « NAT »
- Ordre d'application des règles de NAT
- Lab – Translation d'adresses

## GÉNÉRALITÉS

- Un réseau privé utilise des plages d'adresses IP qui ne sont pas routées sur Internet (RFC 1918).

Préfixe	Plage adresses IPv4	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536

- NAT (Network Address Translation) : Un mécanisme permettant la modification d'un paquet IP (adresse source/destination, port source/destination).

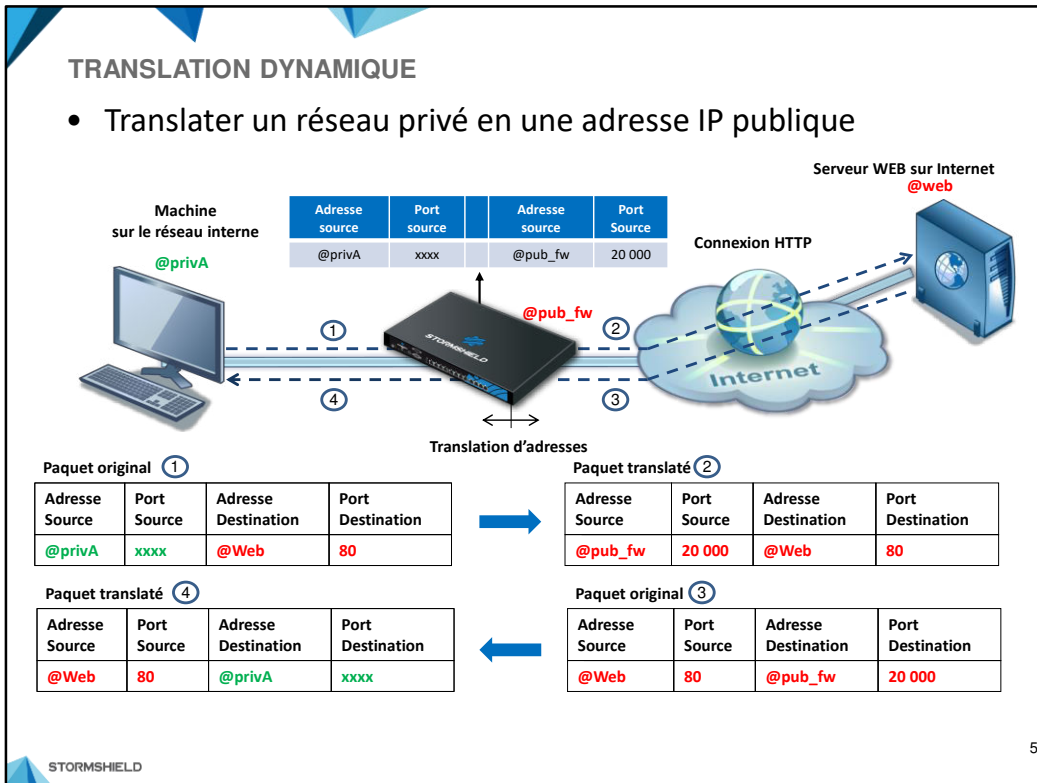
Les mécanismes de translation d'adresses ont été mis au point pour faire face à la pénurie d'adresses IP publiques. Le principe de base consiste à utiliser des adresses IP privées, définies par l'IANA (Internet Assigned Numbers Authority) et renseignées par la RFC 1918 (tableau ci-dessus), pour les réseaux locaux des entreprises et des particuliers, et de relier ces réseaux à Internet via une seule adresse IP publique.



- Généralités
- ➔ **Translation dynamique**
- Translation statique par port
- Translation statique
- Menu « NAT »
- Ordre d'application des règles de NAT
- Lab – Translation d'adresses

STORMSHIELD

Translation d'adresses

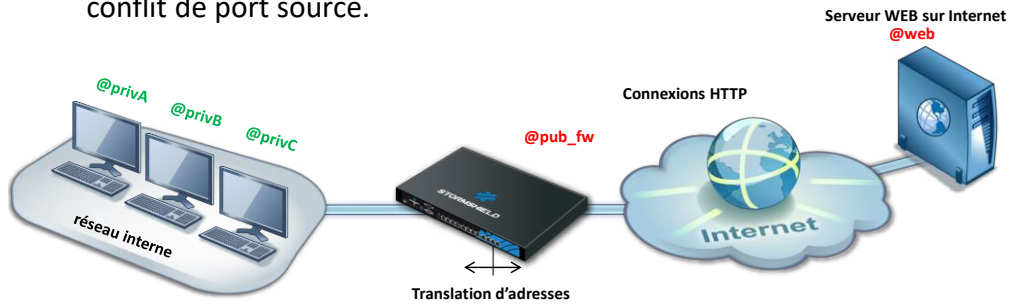


Dans la majorité des cas, ce type de translation est mis en œuvre pour permettre à un réseau local configuré avec des adresses IP privées d'accéder à Internet via une seule adresse IP publique.

La figure ci-dessus illustre le fonctionnement de ce type de translation lorsque la machine « @privA » accède à un serveur WEB « @web » sur internet. Le paquet IP transmis par la machine « @privA » vers le serveur « @web » est intercepté par le firewall qui remplace l'adresse IP source « @privA » par l'adresse IP publique du firewall « @pub\_fw » et le port source « xxxx » (ce port est choisi par le système d'exploitation de la machine « @privA ») par un port dans la plage [20000-59999]. Le firewall garde dans sa mémoire la correspondance de translation entre (l'adresse IP « @privA »/port source « xxxx ») et (l'adresse IP « @pub\_fw »/port source 20000). Cette correspondance est utilisée pour traduire les réponses en provenance du serveur WEB en remplaçant (l'adresse IP destination « @pub\_fw »/port destination 2000) par (l'adresse IP destination « @privA »/port destination « xxxx »).

## TRANSLATION DYNAMIQUE

- Traduire un réseau privé en une adresse IP publique, possible conflit de port source.



Adresse source	Port source	Adresse source	Port Source
@privA	1232	@pub_fw	20000
@privB	20321	@pub_fw	20001
@privC	1232	@pub_fw	20002

Ephemeral\_fw  
[20000, 59999]

La modification du port source se justifie principalement dans le cas où deux machines « @privA » et « @privC » utilisent le même port source pour ouvrir une connexion vers le même serveur WEB. Si le port source n'est pas modifié par le firewall, le serveur web recevra deux demandes de connexion arrivant de la même adresse IP publique « @pub\_fw » et même port source ce qui peut engendrer un dysfonctionnement des deux connexions et une ambiguïté de translation des réponses au niveau du firewall. Ce dernier ne pourra pas savoir à quelle machine il faudra renvoyer les réponses reçues du serveur.

Lorsque l'on utilise l'objet « ephemeral\_fw » en tant que *Port source* de *Trafic après translation*, les ports sources seront choisis dans une plage prédéfinie [20000-59999]. Par défaut, ils seront choisis séquentiellement dans la plage, cependant une option est disponible pour rendre ce choix aléatoire.

Il est possible d'utiliser une plage d'adresses pour masquer l'adresse IP source. La règle de NAT utilisera un objet de type réseau ou plage d'adresses à la place d'un objet de type hôte dans le champ *Source* de *Trafic après translation*. La translation se faisant avec une correspondance 1:1 entre les plages, elles doivent être de la même taille. Il est alors obligatoire de ne pas traduire le port source.



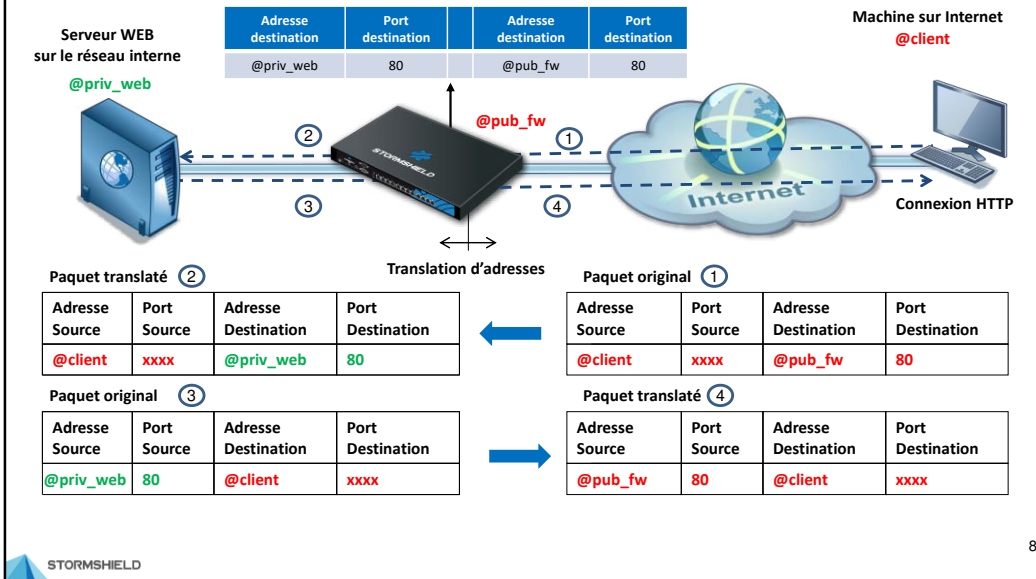
- Généralités
- Translation dynamique
- **Translation statique par port**
- Translation statique
- Menu « NAT »
- Ordre d'application des règles de NAT
- Lab – Translation d'adresses

STORMSHIELD

Translation d'adresses

TRANSLATION STATIQUE PAR PORT

- Donner accès à des ressources internes derrière une seule adresse IP publique



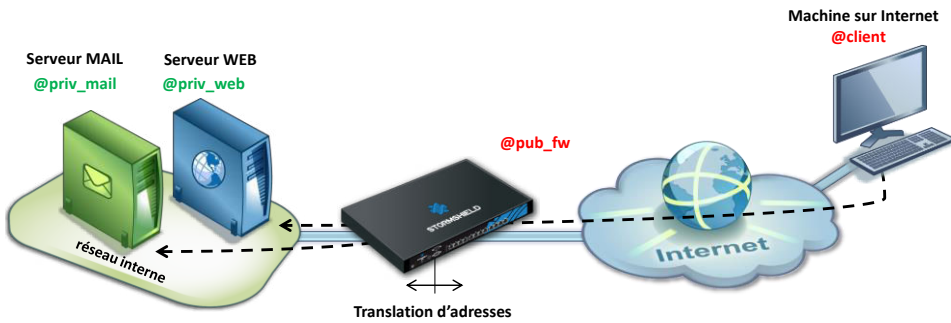
Ce type de translation, appelé communément « redirection de port », permet de rendre accessible des services hébergés dans un réseau local via une seule adresse IP publique.

La figure ci-dessus illustre l'exemple d'un serveur web local « @priv\_web » accessible depuis internet sur l'adresse IP publique du firewall « @pub\_fw ». Sur le firewall, une règle de translation est créée pour la correspondance entre (l'adresse IP publique destination « @pub\_fw »/port destination 80) et (l'adresse IP du serveur local « @priv\_web »/port destination 80).

Ainsi, le paquet émis par la machine « @client » vers l'adresse IP « @pub\_fw » sur le port 80 est modifié avant d'être renvoyé vers le serveur web sur le même port. Et la réponse renvoyée par ce serveur est également modifiée en conséquence avant d'être renvoyée vers la machine « @client ». Il est important de noter que les ports destination avant et après translation peuvent être différents.

## TRANSLATION STATIQUE PAR PORT

- Donner accès à des ressources internes derrière une seule adresse IP publique



Adresse destination	Port destination	Adresse destination	Port destination
@priv_web	80	@pub_fw	80
@priv_mail	25	@pub_fw	25

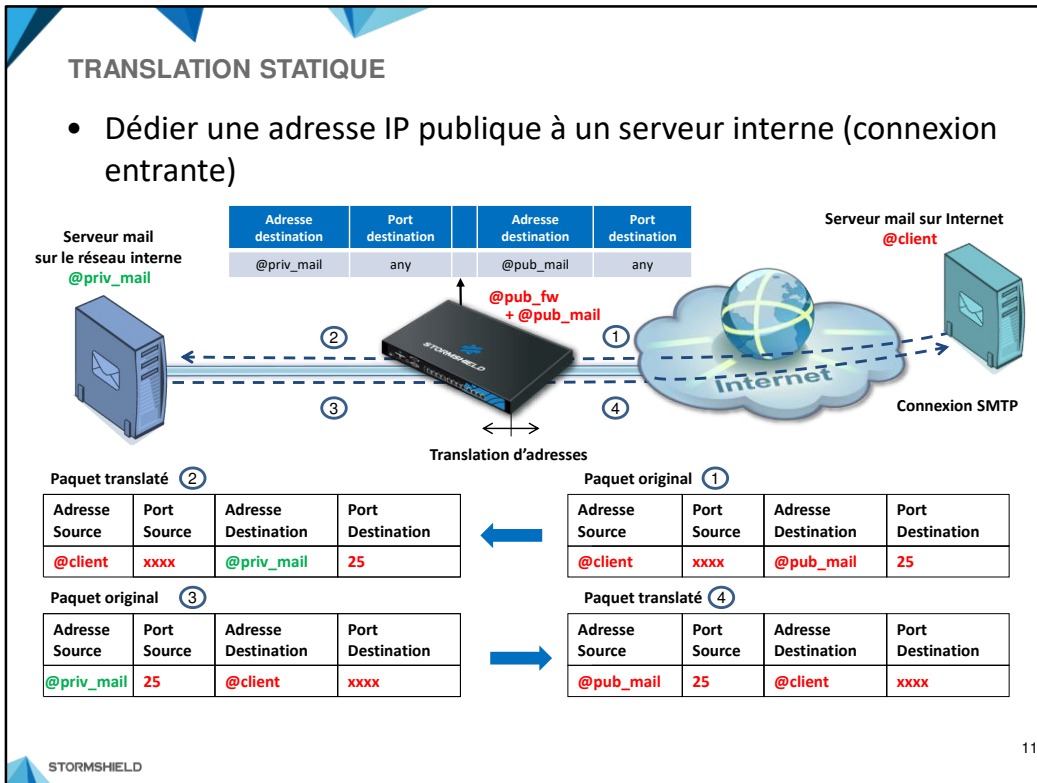
Il est possible de rendre accessibles plusieurs services hébergés sur plusieurs serveurs locaux via une seule adresse IP publique comme l'illustre la figure ci-dessus. La distinction entre les serveurs se base uniquement sur le numéro de port du service.



- Généralités
- Translation dynamique
- Translation statique par port
- ➔ **Translation statique**
- Menu « NAT »
- Ordre d'application des règles de NAT
- Lab – Translation d'adresses

STORMSHIELD

Translation d'adresses

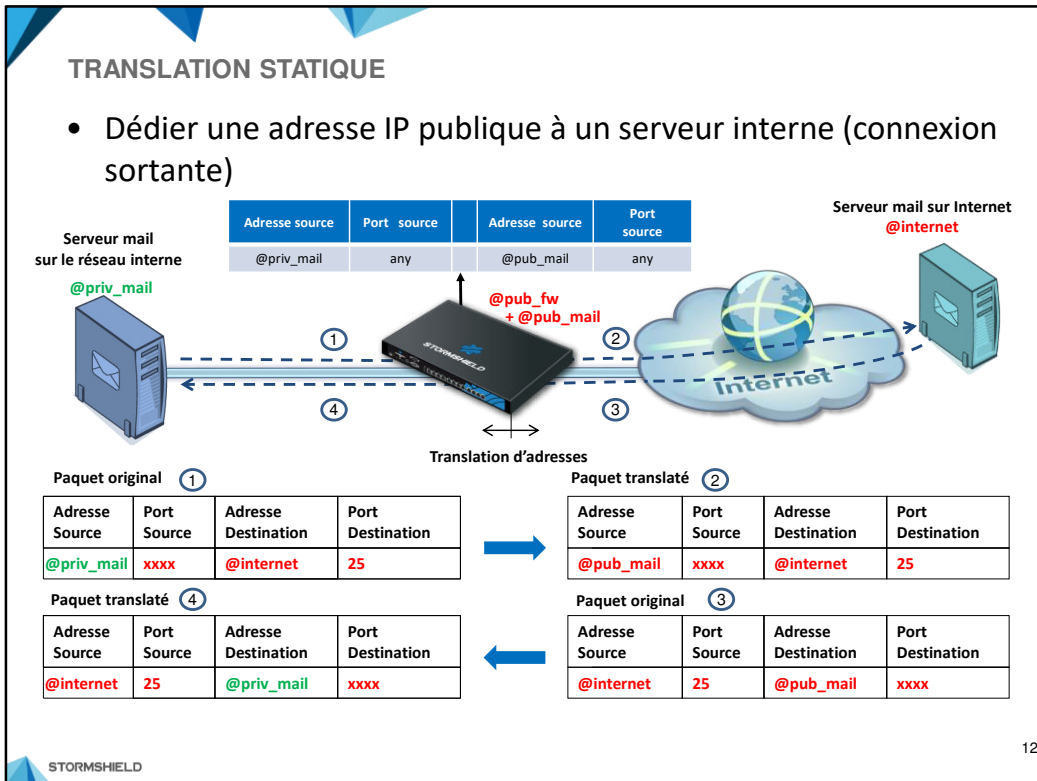


Ce type de translation permet de dédier une adresse IP publique à un serveur local configuré avec une adresse IP privée. Ceci suppose qu'on dispose d'au moins deux adresses IP publiques : « @pub\_fw » configurée sur l'interface externe du firewall et « @pub\_mail » employée sur les règles de translation.

La translation statique doit être bidirectionnelle, ce qui signifie que le serveur local est accessible pour les connexions entrantes, depuis internet, avec son adresse IP publique et les connexions sortantes initiées par ce serveur vers internet doivent avoir comme source la même adresse IP publique. Ceci se traduit par deux règles de translation : une règle pour les connexions entrantes et une autre règle pour les connexions sortantes.

La figure ci-dessus, illustre les modifications que subissent les paquets d'une connexion entrante vers un serveur mail local en se basant sur la règle de translation qui fait la correspondance entre (l'adresse IP publique destination « @pub\_mail ») et (l'adresse IP du serveur local « @priv\_mail »).

Ainsi, le paquet émis par le serveur mail « @internet » vers l'adresse IP « @pub\_mail » est modifié pour être renvoyé vers le serveur mail. Et la réponse renvoyée par ce serveur est également modifiée en conséquence avant d'être renvoyée vers le serveur mail « @internet ». Il est important de noter que les ports source avant et après translation peuvent être restreints à un numéro de port particulier et ils peuvent être différents.

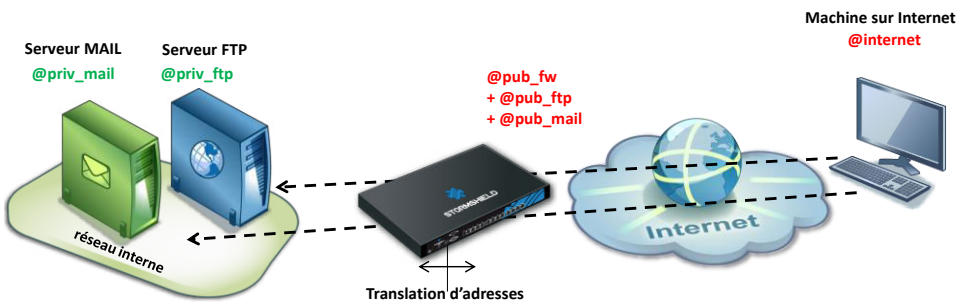


La figure ci-dessus, illustre les modifications que subissent les paquets d’une connexion sortante initiée par le serveur web local vers un serveur sur internet en se basant sur la règle de translation qui fait la correspondance entre (l’adresse IP privée source « @priv\_mail ») et (l’adresse IP source publique « @pub\_mail »).

Ainsi, le paquet émis par le serveur « @priv\_mail » vers une adresse IP sur internet est modifié pour remplacer l’adresse source « @priv\_mail » par l’adresse source « @pub\_mail ». La réponse renvoyée par le serveur externe est aussi modifiée en conséquence avant d’être renvoyée vers le serveur mail local. Il est important de noter que les ports source avant et après translation peuvent être restreints à un numéro de port particulier et ils peuvent être différents.

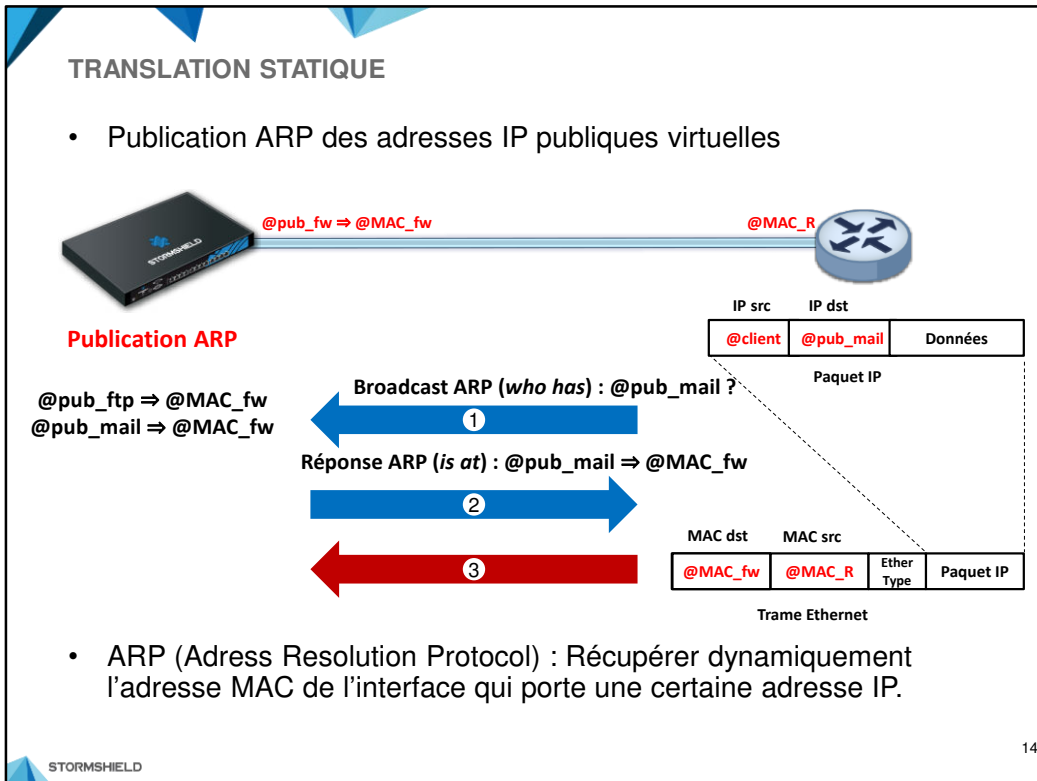
TRANSLATION STATIQUE

- Dédier une adresse IP publique à un serveur interne



Adresse source	Port source	Adresse destination	Port destination	Adresse source	Port source	Adresse destination	Port destination
@priv_mail	Any	Internet	Any	@pub_mail	any		
Internet	Any	@pub_mail	Any			@priv_mail	
@priv_ftp	Any	Internet	Any	@pub_ftp	Any		
internet	Any	@pub_ftp	Any			@priv_ftp	

Si on dispose de plusieurs adresses IP publiques, il est possible de dédier pour chaque serveur une adresse IP spécifique. Chaque serveur nécessite deux règles de translation présentées ci-dessus.



Étant donné que les adresses IP publiques virtuelles ne sont pas configurées sur l'interface externe du firewall, ce dernier ne répondra pas aux requêtes ARP pour la résolution de ces adresses IP en adresse MAC du firewall.

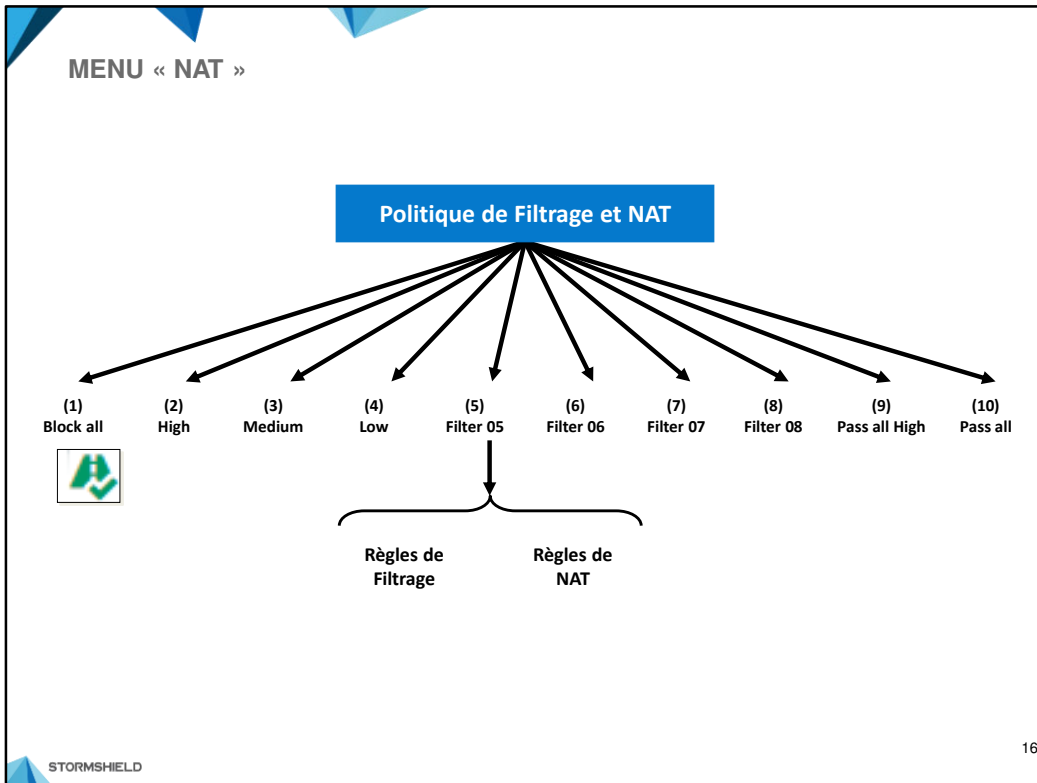
Afin de résoudre ce problème, la publication ARP des adresses IP publiques virtuelles est nécessaire pour le fonctionnement de la translation statique. Elle permet d'ajouter une entrée dans la table ARP du firewall pour faire la correspondance entre chaque adresse IP publique virtuelle et l'adresse MAC de l'interface externe. Ce qui permet au firewall de répondre aux requêtes ARP pour la résolution de ces adresses IP et de recevoir ainsi tous les paquets à leur destination comme l'illustre la figure ci-dessus.




- Généralités
- Translation dynamique
- Translation statique par port
- Translation statique
- **Menu « NAT »**
- Ordre d'application des règles de NAT
- Lab – Translation d'adresses

STORMSHIELD

Translation d'adresses



Dans les firewalls Stormshield Network, les règles de filtrage et NAT (translation d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par l'icône : 

MENU « NAT »

- Édition de la politique de sécurité

SECURITY POLICY / FILTER - NAT

(4) Filter 04 Edit Export ⓘ

FILTERING NAT

Last modification: 12:15:13 PM  
Comments: The profile has no comments

(1) Block all  
(2) High  
(3) Medium  
(4) Filter 04  
(5) LAB\_5\_Filter\_NAT  
(6) LAB\_6\_Content\_Filtering  
(7) LAB\_7\_Authentication  
(8) LAB\_8\_IPSec\_Filter  
(9) LAB\_9\_VPN\_SSL  
(10) Pass all

Rename  
Reinitialize  
Copy to

(1) Block all  
(2) High  
(3) Medium  
(4) Low  
(5) Training lab(active policy)  
(6) Filter 06  
(7) Filter 07  
(8) Filter 08  
(9) Pass all High  
(10) Pass all

STORMSHIELD

17

La configuration des règles de filtrage et NAT s'effectue dans le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT**.

L'entête du menu permet :

- La sélection de la politique de filtrage et NAT grâce à une liste déroulante.
- Éditer** :
  - Renommer** : Modifier le nom de la politique.
  - Réinitialiser** : Remettre les règles de filtrage et NAT par défaut. Attention car cette action ne peut pas se défaire.
  - Copier vers** : Copier une politique vers une autre.
- Exporter** : Permet d'exporter les règles de filtrage/NAT de la politique sélectionnée dans un fichier CSV, cet export est utilisé pour récupérer les règles sur un serveur Stormshield Management Center (SMC).

Le reste du menu est composé de deux onglets :

- Filtrage** : Pour la configuration des règles de filtrage.
- NAT** : Pour la configuration des règles de translation d'adresses.

## MENU « NAT »

- Création d'une règle et entête

SECURITY POLICY / FILTER - NAT

(5) Lab\_5\_Filter\_NAT | Edit | Export

Filtering NAT

Searching... | + New rule | X Delete | ↑ ↓ | ↶ ↷ | Cut | Copy | Paste | Search in logs | Search in monitoring

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Network_in	Internet interface:out	Any	Firewall_out	ephemeral_fw	Any	

Simple rule  
Dynamic rule with port address translation (Dynamic PAT)  
Separator - rule grouping  
Static NAT rule (bimap)

STORMSHIELD

18

L'onglet **NAT** est composé d'un entête pour la gestion des règles de translation:

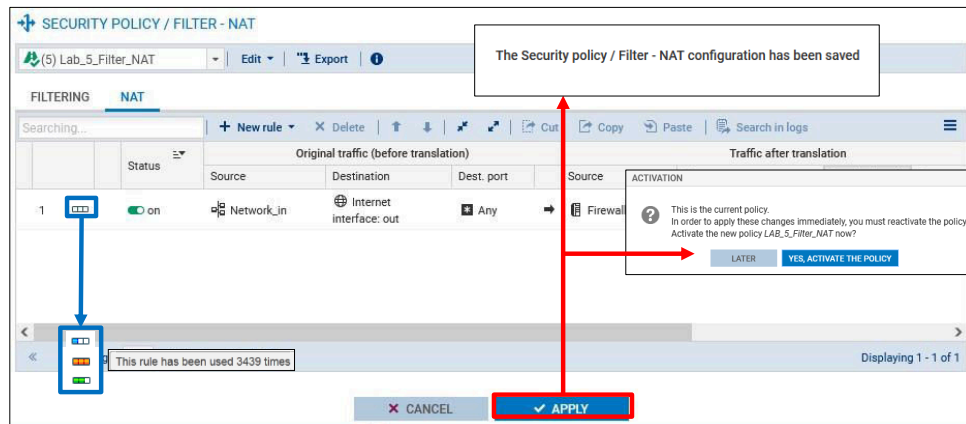
- **Nouvelle règle** :
  - **Règle standard** : Ajouter une règle de translation standard.
  - **Règle de partage d'adresse source (masquering)** : Ajouter une règle pour la translation dynamique en précisant la plage de port **ephemeral\_fw**.
  - **Séparateur – regroupement de règles** : Ajouter un séparateur qui regroupe toutes les règles se trouvant au dessous, ce qui permet de fermer le séparateur pour masquer l'affichage de toutes les règles lui appartenant. De plus, le séparateur peut être personnalisé par une couleur et un commentaire.
  - **Règle de NAT statique (bimap)** : Lancer un assistant qui facilite l'ajout de règles de translation statique bimap.
- **Supprimer** : Supprimer la/les règle(s) sélectionnée(s).
- **Monter / Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.
- **Tout dérouler / Tout fermer** : Dérouler/fermer tous les séparateurs pour afficher/cacher les règles de NAT.
- **Couper** : Couper la/les règle(s) sélectionnée(s).
- **Copier** : Copier la/les règle(s) sélectionnée(s).
- **Coller** : Coller la/les règle(s) auparavant copiée(s)/coupée(s) de la même ou d'une autre politique.
- **Chercher dans les logs** : Chercher le nom de cette règle dans les journaux d'audit.
- **Chercher dans la supervision** : Chercher le nom de cette règle dans la supervision des connexions.
- **Réinitialiser les statistiques des règles** : Réinitialiser les compteurs de toutes les règles filtrage et NAT de la politique. En positionnant la souris sur l'icône, la date de la dernière réinitialisation s'affiche.
- **Réinitialiser Colonnes** : Réinitialiser l'affichage des colonnes qui compose la fenêtre des règles.



- **Trafic avant translation** : Permet de renseigner les valeurs des paramètres du trafic original.
  - **Source** : L'adresse IP ou le réseau source.
  - **Destination** : L'adresse IP ou le réseau destination.
  - **Port dest** : Port destination.
- **Commentaire** : Permet d'ajouter un commentaire. La date, l'heure, l'administrateur et l'adresse IP du PC d'administration sont ajoutés par défaut lors de la création de la règle.
- **Trafic après translation** : Permet de renseigner les nouvelles valeurs des paramètres après translation. Dans le cas où cette partie n'est pas renseignée, le trafic gardera les valeurs originales.
  - **Source** : L'adresse IP ou le réseau source.
  - **Port src** : Port source.
  - **Destination** : L'adresse IP ou le réseau destination.
  - **Port dest** : Port destination.
- **Options** : Le passage d'un flux par une règle de translation n'est pas journalisé en mode standard. En mode « Tracer », le trafic est journalisé dans le journal « Filtrage ». La seconde option permet aussi d'activer le NAT dans un tunnel VPN IPSec.
- **Commentaire** : Permet d'ajouter un commentaire. La date, l'heure, l'administrateur et l'adresse IP du PC d'administration sont ajoutés par défaut lors de la création de la règle.

## MENU « NAT »

- Indicateur d'utilisation des règles de NAT
- Sauvegarde et activation d'une politique de sécurité



STORMSHIELD

20

L'indicateur d'utilisation (encadré en bleu) précise le nombre de fois où un flux traité correspond aux critères de la règle de translation. Le compteur numérique s'affiche en passant la souris par dessus. Il peut afficher 4 couleurs qui sont le résultat d'un rapport mathématique entre le nombre de hits de la règle et le nombre de hits maximum atteint par une règle dans le même slot:

- Blanc (vide) : la règle n'a jamais été appliquée.
- Bleue : la valeur affichée est comprise entre 0 et 2% du hit maximal.
- Vert : la valeur affichée est comprise entre 2% et 20% du hit maximal.
- Orange : la valeur affichée est supérieure ou égale à 20% du hit maximal et est supérieure à 10 000 hits.

Pour sauvegarder une politique, il suffit de cliquer sur le bouton **APPLIQUER**. La sauvegarde est immédiate, une nouvelle fenêtre s'ouvre, permettant par ailleurs de rendre la politique active, ou pas, en cliquant sur le bouton **OUI, ACTIVER LA POLITIQUE**, ou **PLUS TARD**.

## MENU « NAT »

- Affichage des colonnes

The screenshot shows the 'SECURITY POLICY / FILTER - NAT' configuration window. The 'NAT' tab is active, and the 'Columns' menu is open, allowing for the selection of columns to display. The menu options are:

- Status
- Name
- Original traffic (before translation)
  - Source
- Traffic after translation
  - Src. port
  - Destination
  - Dest. port
- Protocol
- Options

The table below shows the current configuration of NAT rules with the selected columns highlighted.

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Network_In	Any		Firewall_Out	ephemeral_fw	Any	
2	on	Network_dmz	Any		Firewall_Out	ephemeral_fw	Any	

L'affichage des colonnes de la fenêtre peut être personnalisé en cliquant sur l'icône indiquée par la flèche bleue ci-dessus, ensuite sur colonnes. Il suffit de sélectionner une colonne pour qu'elle s'affiche.

Les règles de NAT peuvent être déplacées dans la fenêtre par un glisser/déposer en cliquant à gauche sur le numéro de la règle.

**NOTE :** La recherche dans les logs ou la supervision s'effectuant sur le nom d'une règle, vous pouvez afficher la colonne **Nom**, remarquez alors qu'une règle a forcément un nom par défaut, modifiable par l'administrateur.

## MENU « NAT »

- Paramètres d'une règle

The screenshot displays the Stormshield NAT configuration interface. At the top, the breadcrumb is 'MENU « NAT »'. Below it, a list item 'Paramètres d'une règle' is shown. The main interface is titled 'SECURITY POLICY / FILTER - NAT' and shows a table of NAT rules. Rule 1 is selected, and an 'EDITING RULE NO 1' dialog box is open. The dialog has a 'General' tab with fields for 'Status' (set to 'On'), 'Comments' (set to 'Created on 2021-11-09 14:37:25,by admin (192.168.56.20)'), and 'Advanced properties'. The background table shows the rule's configuration: Source: Network\_in, Destination: Internet interface: out, Dest. port: Any, Src. port: Firewall\_out, Destination: ephemeral\_fw, Dest. port: Any.

Les paramètres d'une règle peuvent être renseignés directement dans la fenêtre des règles ou sur une nouvelle fenêtre qui s'affiche en double cliquant sur n'importe quel paramètre de cette règle. Cette fenêtre permet aussi l'accès aux paramètres de configuration avancée.

Les valeurs des paramètres étant des objets, ils peuvent être copiés d'une règle à une autre par un simple glisser/déposer.

MENU « NAT »

- Translation dynamique

23

La règle de NAT dynamique est créée avec le bouton **Nouvelle règle** ⇒ **règle de partage d'adresse source (masquering)** qui ajoute automatiquement la plage de ports **ephemeral\_fw** en tant que **port src** dans le trafic après translation.

La figure ci-dessus présente un exemple d'une règle de NAT dynamique avec les principaux paramètres qui doivent être renseignés. Dans la section **Traffic original (avant translation)**, la source représente le réseau interne **Network\_in** accessible depuis l'interface « in » qui veut accéder à n'importe quelle destination sur n'importe quel port destination. Dans la section **Traffic après translation**, la source est modifiée par l'adresse IP publique portée par l'interface « out » et le port source est traduit par un numéro de port dans la plage **ephemeral\_fw**.

Il est conseillé de cocher l'option **choisir aléatoirement le port source traduit** qui permet de choisir aléatoirement un numéro de port dans la plage **ephemeral\_fw** pour les nouvelles connexions. Cette option offre une protection contre certaines attaques en rendant le port traduit moins prédictible.

MENU « NAT »

- Translation statique par port

SECURITY POLICY / FILTER - NAT

(5) Filter 05 | Edit | Export

FILTERING NAT

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Internet interface: out	Firewall_out	http			srv_web_priv	

SOURCE BEFORE TRANSLATION (ORIGINAL)

GENERAL ADVANCED PROPERTIES

General

User:

Source hosts:

+ Add X Delete

Internet

Incoming interface: out

DESTINATION BEFORE TRANSLATION (ORIGINAL)

GENERAL ADVANCED PROPERTIES

General

Destination hosts:

+ Add X Delete

Firewall\_out

Destination port:

+ Add X Delete

http

EDITING RULE NO 1

General DESTINATION AFTER TRANSLATION

Original source

Original destination

Translated source

General

Translated destination host: srv\_web\_priv

Translated dest. port:

24

La règle de NAT statique par port est créée à partir d'une **règle standard**. Un exemple est présenté dans la figure ci-dessus.

Dans la section Trafic original, la source représente n'importe quelle machine sur le réseau public, ayant pour destination l'adresse IP publique du firewall sur le port 80 (HTTP). Dans la section trafic après translation, l'adresse IP destination est remplacée par l'adresse IP privée du serveur et le numéro de port 80 (HTTP) est maintenu comme port destination. Il est important de noter que les ports destination avant et après translation peuvent être différents.

MENU « NAT »

- Translation statique

Simple rule

- Dynamic rule with port address translation (Dynamic PAT)
- Separator - rule grouping
- Static NAT rule (bimap)**

STATIC NAT WIZARD

Objective: Map a private IP address to a public (virtual) IP address.  
For example, map 1 to 1 between a local server and a public IP address.

General

PRIVATE IP ADDRESS: Private host(s):  VIRTUAL (PUBLIC) IP ADDRESS: Virtual host(s):

Only on the interface:

Advanced properties

Only for the ports:

ARP publication on external destination (public)

SECURITY POLICY / FILTER - NAT

(5) Lab\_5\_Filter\_NAT

FILTERING NAT

+ New rule

	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Network_in	Internet interface: out	Any	Firewall_Out	ephemeral_fw	Any	
2	on	srv_mail_priv	Any interface: out	Any	srv_mail_pub			
3	on	Any interface: out	srv_mail_pub	Any			srv_mail_priv	

STORMSHIELD 25

Les règles de NAT statiques sont créées avec **Nouvelle règle ⇒ règle de NAT statique (bimap)** qui lance un assistant pour renseigner les informations suivantes :

- **Machine(s) privée(s)** : L'adresse IP privée du serveur en interne
- **Machine(s) virtuelle(s)** : L'adresse IP publique virtuelle dédiée au serveur interne
- **Uniquement sur l'interface** : L'interface externe depuis laquelle le serveur est accessible avec son adresse IP publique virtuelle.
- **Uniquement pour les ports** : La règle de NAT statique permet de traduire tous les ports, cependant, il est possible de la restreindre en spécifiant un port ou une plage de ports sur ce paramètre. Il est conseillé de laisser cette valeur à **Any** et de restreindre le port directement dans les règles de filtrage.
- **publication ARP** : Activer la publication ARP pour l'adresse IP publique.

L'exemple illustré dans la figure ci-dessus traduit statiquement un serveur SMTP interne identifié par une adresse IP privée **srv\_mail\_priv** et une adresse IP publique virtuelle dédiée **srv\_mail\_pub**.

L'assistant ajoute deux règles de translation. La première règle pour la translation du flux sortant du serveur interne vers le réseau public et la deuxième pour le flux entrant à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être modifiées par la suite indépendamment l'une de l'autre.



- Généralités
- Translation dynamique
- Translation statique par port
- Translation statique
- Menu « NAT »
- ➔ **Ordre d'application des règles de NAT**
- Lab – Translation d'adresses

STORMSHIELD

Translation d'adresses

## ORDRE D'APPLICATION DES RÈGLES DE NAT

SECURITY POLICY / FILTER - NAT

(5) Lab\_5\_Filter\_NAT Edit Export

FILTERING NAT

Searching...

+ New rule X Delete ↑ ↓ ↻ Cut Copy Paste Search in logs

	Status	Original traffic (before translation)			Traffic after translation			Protocol
		Source	Destination	Dest. port	Source	Src. port	Destination	
STATIC NAT BY PORT (contains 2 rules, from 1 to 2)								
1	<input checked="" type="checkbox"/> on	Internet interface: out	Firewall_out	http	→	srv_web_1		
2	<input checked="" type="checkbox"/> on	grp_public_IP interface: out	Firewall_out	http	→	srv_web_2		

Page 1 of 1

CHECKING THE POLICY

[Rule 2] This rule will never be applied as it is covered by the rule 1..

STORMSHIELD 27

L'ordre d'apparition des règles de translation dans la liste est très important, il définit l'ordre dans lequel les nouvelles connexions sont confrontées aux règles de translation. Ainsi, une nouvelle connexion est confrontée aux règles en partant de la première dans la liste jusqu'à la dernière. Dans le cas où la connexion correspond à une règle, la translation définie par cette règle est appliquée et la connexion n'est plus confrontée aux règles suivantes.

Ce principe de fonctionnement peut engendrer une situation de recouvrement si les règles ne sont pas ordonnées d'une manière cohérente. Un exemple est illustré dans la figure ci-dessus, la deuxième règle de translation ne sera jamais utilisée parce qu'elle est recouverte par une règle plus globale située au-dessus dans la liste (Les réseaux présents dans le groupe **IP\_PUB** sont inclus dans l'objet **Internet**). Le firewall embarque un moteur de cohérence permettant de détecter ce type de recouvrement qui est signalé à l'administrateur par un message d'alerte affiché en bas de fenêtre.

**NOTE** : Une solution simple pour cet exemple consiste à inverser l'ordre des deux règles de translation.



## RECOMMANDATIONS DE SÉCURITÉ

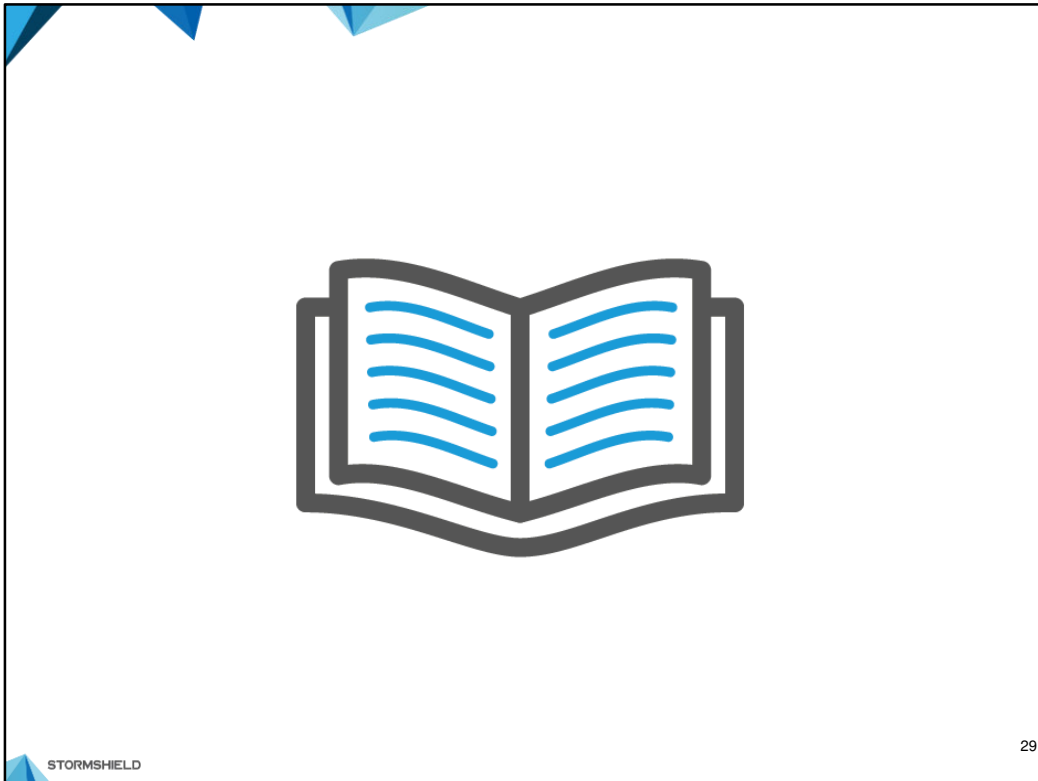


- Renommer la politique de production
- Eviter les chevauchements de règles
- Ne pas laisser de règle inutilisée

Afin de clarifier la lecture des politiques de filtrage, il est recommandé de les nommer explicitement en suivant une convention de nommage précise.

Il est recommandé de ne jamais laisser des règles se recouvrir. Outre l'inutilité de la règle recouverte, cela pourrait mener à laisser des points d'entrée en cas de suppression de la règle couvrante.

Toute règle inutile laisse un point d'entrée potentiel et augmente la surface d'attaque. Elles sont donc à traquer et supprimer régulièrement.



Pour aller plus loin, consultez les ressources du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Note technique - Mise en œuvre d'une règle de NAT

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Généralités
- Translation dynamique
- Translation statique par port
- Translation statique
- Menu « NAT »
- Ordre d'application des règles de NAT

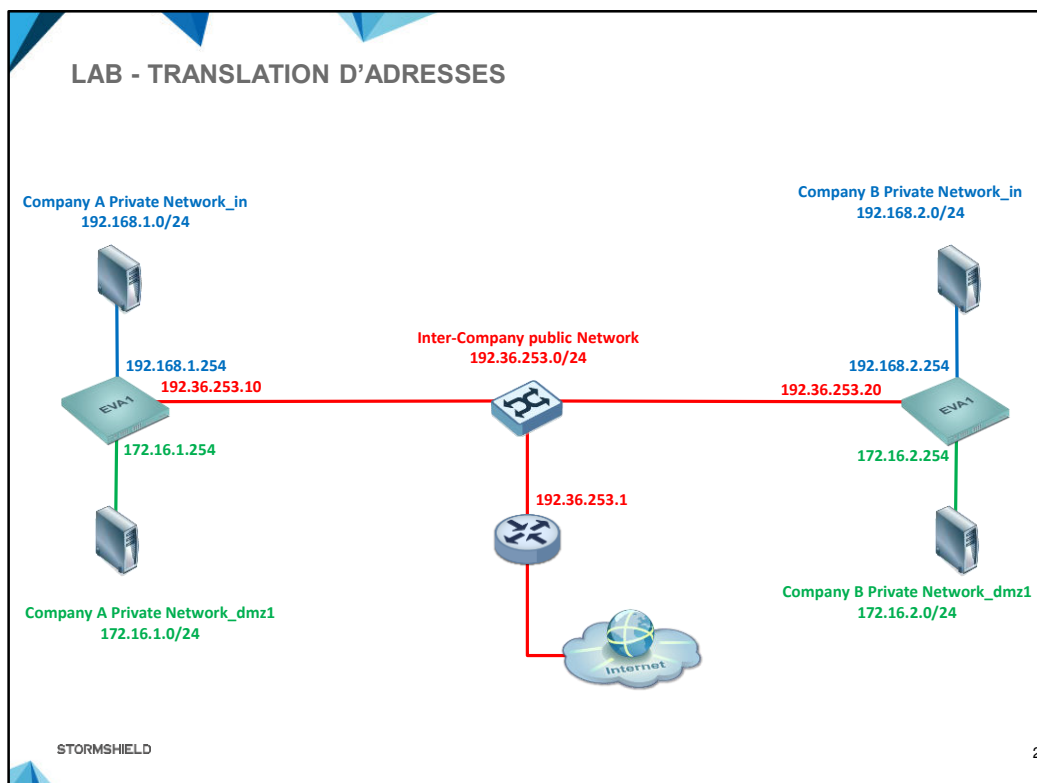
 **Lab – Translation d'adresses**

STORMSHIELD

**Translation d'adresses**



## Lab 4 - Translation d'adresses



Pour ce LAB, nous considérons le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n'est tolérée.

1. Désactivez les routes statiques ajoutées dans le lab précédent.
2. Copiez la politique de filtrage/NAT **(10) Pass all** vers la politique numéro 4. Renommez la politique numéro 4 « Lab\_4 ». Ensuite, activez cette politique.
3. Ajoutez une règle de NAT afin que les machines de vos réseaux internes puissent accéder à Internet sans que leur IP privée n'y soit vue. Ensuite, testez l'accès à Internet depuis votre poste.
4. Vous disposez de 2 adresses IP publiques supplémentaires « 192.36.253.x2 » et « 192.36.253.x3 » réservées respectivement à vos serveurs FTP et MAIL situés en DMZ. Ajoutez les règles de NAT statique (bimap) qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.
5. Ajoutez une règle de NAT statique par port afin que votre serveur WEB situé en DMZ soit joignable grâce à une redirection de port via l'adresse IP publique portée par votre firewall « 192.36.253.x0 ».
6. Avec l'autre entreprise, testez l'accès à l'ensemble des ressources (le serveur MAIL peut être testé à l'aide d'une commande TELNET).

**Bonus :**

- Ajoutez une règle de NAT afin que les machines de votre réseau interne puissent accéder à vos serveurs en DMZ sans que leur adresse IP privée n'y soit vue.
- Quels sont les avantages et inconvénients selon vous de translater les adresses depuis votre réseau interne vers votre DMZ, laquelle est aussi un réseau interne ?



# Quiz

STORMSHIELD

Q1 – La translation d'adresse permet à plusieurs serveurs web d'être accessibles sur la même adresse IP publique et le même port.

- A. Vrai
- B. Faux

Q2 – La translation dynamique nécessite une réécriture de port source :  
Vrai seulement s'il y a plusieurs machines émettant des connexions à traduire

- A. Vrai dans tous les cas
- B. Faux

Q3 – Combien de politique de filtrage et NAT sont disponibles sur les pare-feux Stormshield :

- A. 2
- B. 4
- C. 8
- D. 10
- E. 3



Q4 – Si deux règles de translation ont les mêmes critères de sélection de trafic, c'est la dernière dans la liste qui s'appliquera :

- A. Vrai
- B. Faux

Q5 – Le protocole ARP permet de déterminer automatiquement la passerelle à utiliser pour joindre une machine :

- A. Vrai
- B. Faux

Q6 – La publication ARP permet au pare-feu de répondre aux requêtes ARP sur des adresses IP ne lui appartenant pas (non configurée sur une interface) :

- A. Vrai
- B. Faux



STORMSHIELD

# ANNEXE - TRANSLATION D'ADRESSES

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



➔ Configurations avancées

STORMSHIELD

Translation d'adresses



### CONFIGURATIONS AVANCÉES : L'INTERFACE D'ENTRÉE DANS UNE RÈGLE DE NAT

Original traffic (before translation)				Traffic after translation		
Source	Destination	Dest. port	Source	Src. port	Destination	
Network_new interface: in	Internet interface: out	Any	FirewallLou	ephemeral_fw	Any	
Network_new interface: dmz1	Internet interface: out	Any	virtualL	ephemeral_fw	Any	

EDITING RULE NO 1

General

SOURCE BEFORE TRANSLATION (ORIGINAL)

Original source

Original destination

Translated source

Translated destination

Protocol

Options

GENERAL ADVANCED-PROPERTIES

General

User:

Source hosts: Network\_new\_bridge

Incoming interface: in

STORMSHIELD

3

Sur une règle de NAT, il est possible de spécifier l'interface d'entrée du trafic pour lequel la règle doit s'appliquer. Cette configuration avancée qui s'effectue sur le champ **source** d'une règle permet de répondre à plusieurs cas d'usage.

Le premier cas est présenté ci-dessus, il consiste à traduire deux réseaux physiques (**in** et **dmz1**) appartenant au même réseau logique (**network\_bridge**) avec deux adresses IP publiques **Firewall\_out** et **IP\_pub\_virtuelle**. La spécification de l'interface d'entrée est le seul moyen pour distinguer les deux réseaux physiques.

### CONFIGURATIONS AVANCÉES : L'INTERFACE D'ENTRÉE DANS UNE RÈGLE DE NAT

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule X Delete ↑ ↓ ↕ ↔ Cut Copy Paste Search in logs

	Status	Original traffic (before translation)			Traffic after translation		
		Source	Destination	Dest. port	Source	Src. port	Destination
1	on	Any interface: in	Internet interface: out	Any	→ Firewall_out	ephemeral_fw	Any

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule X Delete ↑ ↓ ↕ ↔

	Status	Original traffic (before translation)		
		Source	Destination	Dest. port
1	on	Network_in Network_in_1 Network_in_2	Internet interface: out	Any

NETWORK / INTERFACES

Enter a filter Edit + Add X Delete Monitor

Interface IN CONFIGURATION

new\_bridge1

dmz2

out

in

dmz1

Address range

Address range:

IPv4 address:

+ Add X Delete

Address/ Mask	Comments
192.168.1.254/24	
192.168.20.254/24	
192.168.40.254/24	

STORMSHIELD

4

Le deuxième cas d'usage est la translation des différents alias réseaux portés par une interface avec l'adresse IP publique du Firewall.

Lors de la configuration d'adresses IP supplémentaires portées par la même interface, le firewall crée des objets supplémentaires.

Dans l'exemple ci-dessus, la configuration de 3 adresses IP dans des plans d'adressage différents donne lieu à la création de 3 objets « hôte » Firewall\_in, Firewall\_in\_1 et Firewall\_in\_2, puis des trois objets réseau correspondants.

Dans ce cas, on devrait ajouter dans la règle tous les réseaux correspondants aux alias, ou un groupe les contenant. La spécification d'une interface sur une règle de translation d'adresse permet d'utiliser **Any** en réseau source afin de traduire tous les alias de cette interface. Attention car cette règle de serait appliquée aussi à des réseaux qui arriveraient sur cette interface n'appartenant pas forcément aux réseaux portés par elle-même : arrivant depuis un routeur qui se trouverait sur l'un des réseaux portés par l'interface.

## CONFIGURATIONS AVANCÉES : L'INTERFACE DE SORTIE SUR UNE RÈGLE DE NAT

The screenshot shows the 'SECURITY POLICY / FILTER - NAT' configuration page. It displays two NAT rules, 'outgoing\_isp1' and 'outgoing\_isp2', both with a status of 'on'. The table below details the configuration for these rules.

	Status	Name	Original traffic (before translation)			Traffic after translation		
			Source	Destination	Dest. port	Source	Src. port	Destination
1	on	outgoing_isp1	Network_in	Internet interface: out	Any	Firewall_out	ephemeral_fw	Any
2	on	outgoing_isp2	Network_in	Internet interface: out2	Any	Firewall_out2	ephemeral_fw	Any

STORMSHIELD

5

Sur une règle de NAT, il est possible également de spécifier l'interface de sortie du trafic pour laquelle la règle doit s'appliquer. Cette spécification s'effectue par le champ **destination** du trafic avant translation ce qui permet de restreindre la règle de translation uniquement au trafic sortant de cette interface (Cette dernière est décidée au préalable par la fonction de routage qui fixe l'adresse MAC destination du paquet avec l'adresse MAC de la passerelle distante).

Les figures ci-dessus illustrent l'utilisation de l'interface de sortie dans le cas où le firewall dispose de deux accès WAN et quand on souhaite mettre en place de la répartition de charge ou un lien de secours.

**NOTE** : Pour rappel, la répartition de charge est mise en place avec un objet routeur.

## CONFIGURATIONS AVANCÉES : RÉPARTITION DE CONNEXIONS REDIRIGÉES

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule Delete Cut Copy Paste Search in logs Search in monitoring

	Status	Name	Original traffic (before translation)			Traffic after translation			
			Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
- Load balancing of outgoing connections (contains 1 rules, from 1 to 1)									
1	on	outgoing_lb	Network_in	Internet	Any	grp_ip_wan	ephemeral_fw	Any	
- Load balancing of incoming connections over several servers (contains 1 rules, from 2 to 2)									
2	on	incoming_lb_srv	Internet interface: out2	Firewall_out2	http			grp_srv_priv	
- Load balancing of incoming connections over several ports (contains 1 rules, from 3 to 3)									
3	on	incoming_lb_ports	Internet interface: out2	Firewall_out2	http	Any		srv_web_priv	port_range
- Load balancing of incoming connections over several servers and several ports (contains 1 rules, from 4 to 4)									
4	on	incoming_lb_srv_ports	Internet interface: out2	Firewall_out2	http	Any		grp_srv_priv	port_range

STORMSHIELD

6

Les paramètres de configuration avancée des règles de translation permettent la répartition des connexions redirigées pour les connexions entrantes et sortantes :

- **Répartition des connexions sortantes (règle 1)** : Elle consiste à traduire les connexions sortantes avec plusieurs adresses IP source.
- **Répartition des connexions entrantes sur plusieurs serveurs ou ports (services)**. On distingue différents cas :
  - **Répartition sur plusieurs machines (règle 2)** : Elle consiste à rediriger les connexions entrantes vers plusieurs machines en renseignant un groupe composé de plusieurs adresses IP comme destination pour le trafic après translation. Elle peut être utilisée dans le cas où un service est hébergé sur plusieurs serveurs.
  - **Répartition sur plusieurs ports (règle 3)** : Elle consiste à rediriger les connexions entrantes vers plusieurs ports destination d'une seule machine en spécifiant une plage de ports pour le trafic après translation. Elle est utilisée dans le cas où la machine héberge plusieurs instances d'une même application. Chacune des instances écoutant sur un port particulier de la plage de ports de destination.
  - **Répartition sur plusieurs machines et plusieurs ports (règle 4)** : Elle représente une combinaison des deux répartitions précédentes. Elle permet de répartir le trafic entrant sur les différents ports de destination de plusieurs machines.

## CONFIGURATIONS AVANCÉES : RÉPARTITION DE CONNEXIONS REDIRIGÉES



Les différents types de répartition peuvent se baser sur quatre types d'algorithmes :

- **Round-robin** : Les adresses IP ou les numéros de port sont utilisés de façon alternée par les connexions.
- **Hachage de l'IP source** : Un haché de l'adresse IP source, de la connexion avant translation, est calculé pour choisir l'adresse IP ou le numéro de port. Cet algorithme permet de garantir que les connexions de la même machine sont toujours associées avec la même adresse IP ou le même numéro de port.
- **Hachage de la connexion** : Un haché des paramètres de connexion avant translation (IP source, port source, IP destination, port destination) est calculé pour choisir l'adresse IP ou le numéro de port. Cet algorithme permet de répartir les connexions provenant de la même machine sur plusieurs adresses IP ou plusieurs numéros de port.
- **Aléatoire** : L'adresse IP ou le numéro de port sont choisis aléatoirement.

**NOTE** : L'accessibilité de l'adresse IP ou du numéro de port choisi n'est pas vérifiée (S'ils ne sont pas accessibles, le firewall continuera à leur transmettre du trafic).

CONFIGURATIONS AVANCÉES : CRITÈRES SOURCES AVANCÉES

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule X Delete | ↑ ↓ | Cut Copy Paste | Search in logs Search in monitoring

	Status	Name	Original traffic (before translation)			Traffic after translation		
			Source	Destination	Dest. port	Source	Src. port	Destination
1	on	trainers_outgoing	Trainers@ Network	Internet interface: out	Any	Firewall_out	ephemeral_fw	Any
2	on	trainees_outgoing	Trainees@ Network	Internet interface: out2	Any	Firewall_out2	ephemeral_fw	Any

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule X Delete | ↑ ↓ | Cut Copy Paste | Search in logs Search in monitoring

	Status	Name	Original traffic (before translation)			Traffic after translation		
			Source	Destination	Dest. port	Source	Src. port	Destination
1	on	dscp26	Network_In DSCP: 26 Class 3, gold (AF31)	Internet interface: out	Any	virtual_IP_pub	ephemeral_fw	Any

STORMSHIELD

8

La configuration avancée des règles de translation d'adresse permet de définir d'autres critères sources. On distingue :

- **La spécification d'utilisateurs ou de groupes d'utilisateurs** : Permet de définir des règles de translation spécifiques aux utilisateurs authentifiés (cela suppose qu'un annuaire et un mécanisme d'authentification ont été préalablement configurés sur le firewall).
- **La spécification de champ (champ DSCP)** : Permet de traduire les adresses en fonction des valeurs du champ DSCP. Ce dernier se trouve dans l'entête IP d'un paquet et indique la classe de service (QoS) à laquelle appartient le trafic.

PARAMÈTRES AVANCÉES : EXCEPTION DE TRANSLATION D'ADRESSE

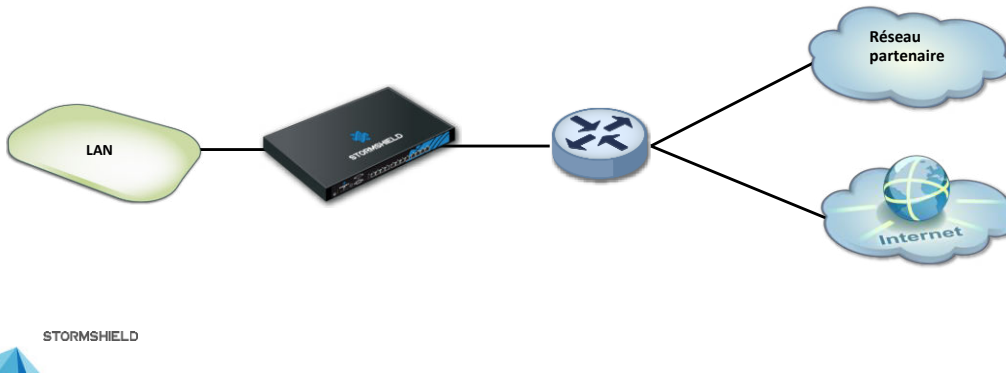
SECURITY POLICY / FILTER - NAT

(7) Filter 07 | Edit | Export

FILTERING NAT

Searching...

	Status	Name	Original traffic (before translation)			Traffic after translation		
			Source	Destination	Dest. port	Source	Src. port	Destination
1	on	outgoing_net_partner	Network_in	net_partner	Any	Network_in		net_partner
2	on	outgoing_internet	Network_in	Internet	Any	Firewall_out	ephemeral_lw	Any



Dans certaines configurations, il peut être nécessaire de ne pas effectuer l'opération de translation pour certains trafics. Dans l'exemple présenté ci-dessus, l'ensemble des adresses du LAN sont traduites sur l'adresse IP de l'interface externe du Firewall à l'exception du trafic à destination du réseau partenaire.

Pour mettre en œuvre cette configuration, une règle de translation spécifique doit être ajoutée pour indiquer que le trafic du réseau interne vers le réseau partenaire ne doit pas être traduit. Dans cette règle, les paramètres du trafic après translation doivent être identiques aux paramètres du trafic avant translation. De plus, cette règle doit être positionnée avant la règle de translation à destination d'Internet pour éviter une situation de recouvrement.

**NOTE :** Il est également possible d'utiliser l'exception de translation pour une machine spécifique d'un réseau traduit.



## Programme de la formation

- ✓ Coursus des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Les objets
- ✓ Configuration réseau
- ✓ Translation d'adresses
- Filtrage
  - Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Généralités

- La notion de « stateful »
- L'ordonnancement des règles de filtrage et de translation
- Menus « filtrage »
- L'analyseur de cohérence et de conformité
- Lab - Filtrage

## GÉNÉRALITÉS

- Définition des flux autorisés et/ou bloqués par le firewall
- Critères d'application de la règle
- Inspections de sécurité selon les flux

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	dns_outgoing	pass	srv_dns_priv	Internet	dns		IPS
2	on	https_outgoing_storms...	pass	Network_in	www.stormshield.eu	https		IPS
3	on	http_outgoing_no_online	pass	Network_internal	Internet geo Europe	http		IPS URL filter: No_online
4	on	smtp_incoming	block	Internet IP rep. bad	Firewall_out	smtp		IPS
5	on	icmp_outgoing	pass	Network_in	Internet	Any	icmp (Echo request)	IPS

STORMSHIELD

3

Grâce à la politique de filtrage, l'administrateur est capable de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers du firewall Stormshield Network. Selon les flux, certaines inspections de sécurité (analyse antivirus, analyse antispam, filtrage URL, ...) peuvent être activées (nous détaillerons ces analyses dans le module « Protection applicative »). Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise.

Pour définir un flux, une règle de filtrage se base sur de nombreux critères ; ce qui offre un haut niveau de granularité. Parmi ces critères, il est notamment possible de préciser :

- L'adresse IP source et/ou destination,
- La réputation et la géolocalisation de l'adresse IP source et/ou destination,
- L'interface d'entrée et/ou sortie,
- L'adresse réseau source et/ou destination,
- Le FQDN source et/ou destination,
- La valeur du champ DSCP,
- Le service TCP/UDP/SCTP (n° de port de destination),
- Le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé),
- L'utilisateur ou le groupe d'utilisateurs devant être authentifié.

Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend du modèle de firewall. Le premier paquet appartenant à chaque nouveau flux reçu par le firewall est confronté aux règles de filtrage de la première à la dernière ligne. Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste.

Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué.



- Généralités
- ➔ **La notion de « stateful »**
- L'ordonnancement des règles de filtrage et de translation
- Menus « filtrage »
- L'analyseur de cohérence et de conformité
- Lab - Filtrage

### LA NOTION DE « STATEFUL »

Adresse source	Port source	Adresse destination	Port destination
@privA	xxxx	@web	80

**FILTERING** NAT

Searching...

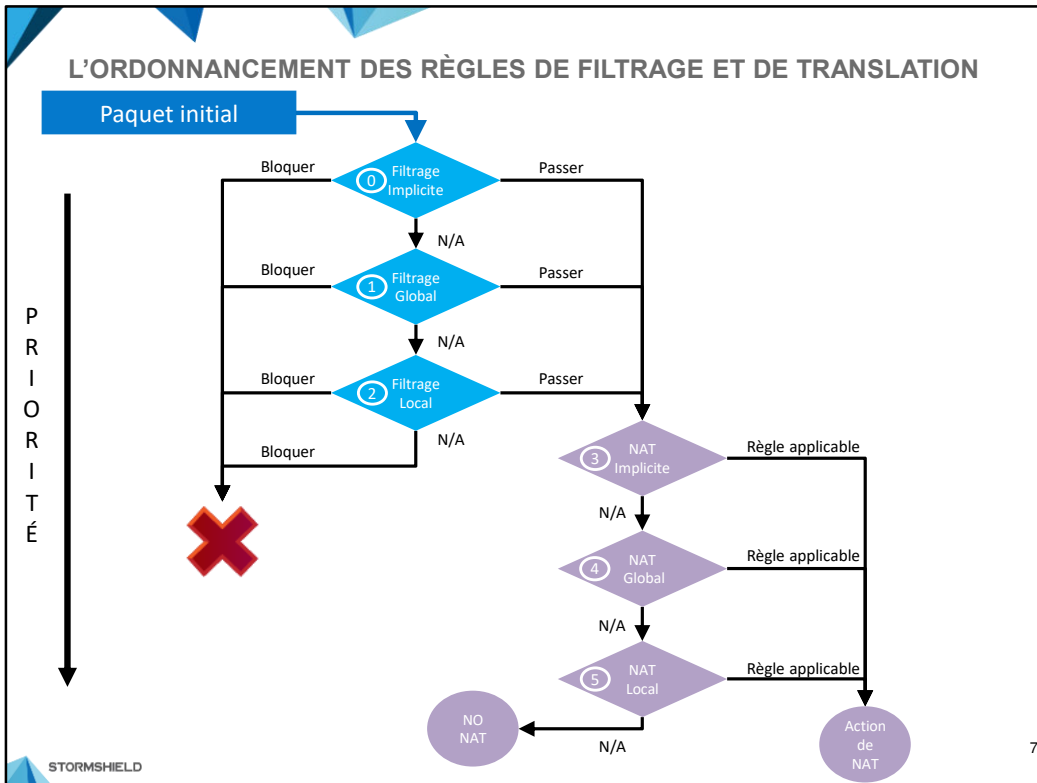
	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security in
1	on	outgoing_internet	pass	Network_in	Internet	Any		IPS
2	on	outgoing_internet	pass	Internet	Network_in	Any		IPS

5

Les firewalls Stormshield Network utilisent la technologie SPI (Stateful Packet Inspection) qui leur permet de garder en mémoire l'état des connexions TCP, SCTP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi « Stateful » est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de l'initiation de la connexion ; les réponses faisant partie de la même connexion sont implicitement autorisées. Ainsi, nous n'avons nul besoin d'une règle de filtrage supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall.



- Généralités
- La notion de « stateful »
- ➔ **L'ordonnancement des règles de filtrage et de translation**
- Menus « filtrage »
- L'analyseur de cohérence et de conformité
- Lab - Filtrage



Dans les firewalls Stormshield Network, les règles de filtrage et de NAT sont organisées en différents niveaux appelés « slot » représentés selon leur priorité dans la figure ci-dessus :

- **Le filtrage implicite** : Regroupe les règles de filtrage préconfigurées ou ajoutées dynamiquement par le firewall pour autoriser ou bloquer certains flux après l’activation d’un service. Par exemple, une règle implicite autorise les connexions à destination des interfaces internes de l’UTM sur le port HTTPS (443/TCP) afin d’assurer un accès continu à l’interface d’administration Web. Autre exemple, dès l’activation du service SSH, un ensemble de règles implicites sera ajouté pour autoriser ces connexions depuis toutes les machines des réseaux internes.
- **Le filtrage global** : Regroupe les règles de filtrage injectées au firewall depuis l’outil d’administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- **Le filtrage local** : Représente les règles de filtrage ajoutées par l’administrateur depuis l’interface d’administration.
- **Le NAT implicite** : Regroupe les règles de NAT ajoutées dynamiquement par le firewall. Ces règles sont utilisées principalement lors de l’activation de la haute disponibilité.
- **Le NAT global** : À l’instar du filtrage global, il regroupe les règle de NAT injectées au firewall depuis l’outil d’administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- **Le NAT local** : Regroupe les règles de NAT ajoutées par l’administrateur depuis l’interface d’administration.



- Généralités
- La notion de « stateful »
- L'ordonnancement des règles de filtrage et de translation
- **Menus « filtrage »**
- **➤** L'analyseur de cohérence et de conformité
- Lab - Filtrage

MENUS « FILTRAGE »

SECURITY POLICY / IMPLICIT RULES

IMPLICIT FILTER RULES

Enabled	Name
<input checked="" type="checkbox"/> Enabled	Allow access to the PPTP server
<input checked="" type="checkbox"/> Enabled	Allow mutual access between the members of a firewall cluster (HA)
<input checked="" type="checkbox"/> Enabled	Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers.
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's DNS service (port 53).
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for modem interfaces (dialup)
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for ethernet interfaces
<input type="checkbox"/> Disabled	Allow protected interfaces (serverd) to access the firewall's administration server (port 1300)
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's SSH port
<input type="checkbox"/> Disabled	Allow interfaces associated with authentication profiles (Authd) to access the authentication portal and SSL VPN.
<input checked="" type="checkbox"/> Enabled	Allow access to the firewall's web administration server (WebAdmin)
<input checked="" type="checkbox"/> Enabled	Allow "Bootp" requests with an IP address specified for relaying DHCP requests
<input checked="" type="checkbox"/> Enabled	Allow clients to reach the firewall SSL VPN service on the TCP and UDP ports
<input checked="" type="checkbox"/> Enabled	Allow router solicitations (RS) in multicast or directed to the firewall
<input checked="" type="checkbox"/> Enabled	Allow requests to DHCPv6 server and DHCPv6 multicast solicitations
<input checked="" type="checkbox"/> Enabled	Do not log IPFIX packets in IPFIX traffic

Advanced properties

Include outgoing implicit rules for hosted services (indispensable)

9

Les règles implicites sont accessibles depuis le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Règles implicites**. Chaque règle peut être activée/désactivée.

**NOTE** : La modification de l'état de ces règles a un impact direct sur le fonctionnement des services du firewall. Pour que le service concerné fonctionne toujours, il faut s'assurer au préalable que le flux est autorisé par les règles de priorité moindre telles que globales ou locales.

MENUS « FILTRAGE »

- Affichage des règles globales

The screenshot illustrates the steps to display global rules. It shows the 'Preferences' menu in the top right, the 'Application settings' dialog where 'Display global policies (Network objects, Certificates, Filter, NAT and IPsec VPN)' is checked, and the 'Security Policy / Filter - NAT' menu where 'Global policy' is selected in the dropdown.

Number of rules per page (filtering, NAT and IPsec): Automatic

Local policy  
Global policy

SECURITY POLICY / FILTER - NAT

Global policy (1) Global Filter 01 Edit Export

FILTERING NAT

Searching...	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	global_block_icmp	block	Internet interface: out	Firewall_out	Any	icmp	IPS

10

Pour afficher les règles globales, il faut cocher l’option **Afficher les politiques globales (Filtrage, NAT, VPN IPsec et Objets)** dans le menu **Préférences** accessible directement depuis l’icône de l’en-tête encadré en rouge. Cette option fait apparaître dans l’en-tête du menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT** une liste déroulante qui permet de sélectionner les politiques globales ou locales. Par défaut, aucune règle de filtrage et NAT n’est présente dans les slots globaux.

## MENUS « FILTRAGE »

- Création d'une règle
- Ajout, édition et colorisation de séparateurs
- Choix des colonnes affichées

The screenshot displays the 'SECURITY POLICY / FILTER - NAT' interface. At the top, there's a search bar and a 'New rule' button. A dropdown menu is open, showing options: 'Simple rule', 'Separator - rule grouping', 'Authentication rule', 'SSL inspection rule', and 'Explicit HTTP proxy rule'. Below, a table lists rules with columns for Name, Action, Source, Destination, Dest. port, Protocol, Security inspection, and Comments. The table is divided into sections by colored separators: blue (outgoing\_dns), red (outgoing\_ntp), and yellow (outgoing\_ftp). A 'Columns' menu is open on the right, showing options like Status, Name, Action, Source, Src. port, Destination, Dest. port, Protocol, and Security inspection.

Les règles de filtrage font partie d'une politique présentée précédemment dans le module « Translation d'adresses ».

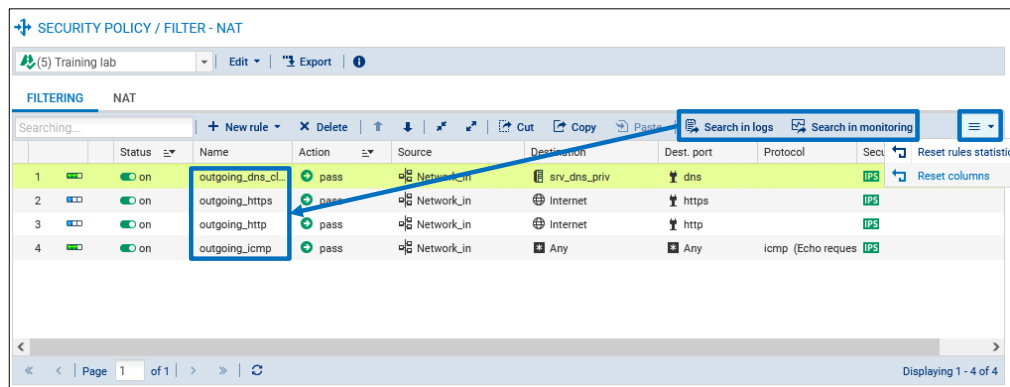
L'onglet **FILTRAGE** est composé d'un en-tête pour la gestion des règles de filtrage:

- **Nouvelle règle** :
  - **Règle simple** : Ajouter une règle de filtrage standard. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à Any.
  - **Séparateur – regroupement de règles** : Ajouter un séparateur qui regroupe toutes les règles se trouvant au-dessous (ou jusqu'au prochain séparateur). Cela permet de faciliter l'affichage d'une politique contenant un nombre de règles important. Le séparateur peut être personnalisé par une couleur et un commentaire.
  - **Règle d'authentification** : Démarrer un assistant facilitant l'ajout d'une règle dont le rôle est de rediriger les connexions des utilisateurs non-authentifiés vers le portail captif (voir module « Utilisateurs et Authentification » pour plus de détails à ce sujet).
  - **Règle d'inspection SSL** : Démarrer un assistant qui facilite l'ajout de règles pour l'activation du proxy SSL.
  - **Règle de proxy HTTP explicite** : Démarrer un assistant qui facilite l'ajout de règles pour l'activation du proxy HTTP explicite.
- **Supprimer** : Supprimer une règle.
- **Monter / Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.



## MENUS « FILTRAGE »

- Nommage des règles
- Options d'en-tête

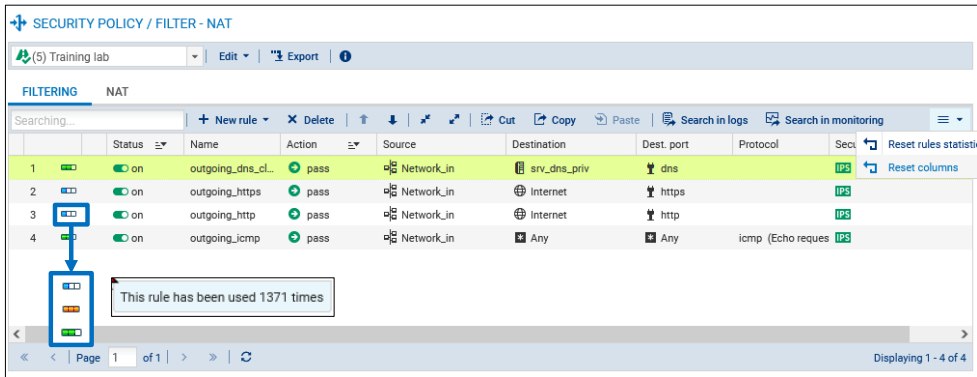


- **Tout dérouler / Tout fermer** : Dérouler/Fermer tous les séparateurs pour afficher/cacher les règles de filtrage.
- **Couper** : Couper la/les règle(s) sélectionnée(s).
- **Copier** : Copier la/les règle(s) sélectionnée(s).
- **Coller** : Coller la/les règle(s) auparavant copiée(s)/coupée(s) de la même ou d'une autre politique.
- **Chercher dans les logs** : Chercher les traces générées par l'application de cette règle dans les journaux d'audit (la recherche s'effectue sur le nom de la règle).
- **Chercher dans la supervision** : Chercher le nom de cette règle dans la supervision des connexions.
- **Réinitialiser les statistiques des règles** : Réinitialiser les compteurs d'utilisation de toutes les règles de filtrage et NAT de la politique active. La date de la dernière réinitialisation s'affiche en positionnant la souris sur l'icône.
- **Reinit Colonnes** : Réinitialiser l'affichage des colonnes qui composent la fenêtre des règles comme le prévoit l'affichage par défaut.

**NOTE** : A la création d'une règle, le système lui attribue un nom (par exemple: 1828cd033db\_6) modifiable et même supprimable par l'administrateur. Bien que la colonne concernée soit cachée par défaut, c'est sur ce nom que s'effectue la recherche dans les logs ou la supervision. Il est par conséquent judicieux de donner à la règle un nom explicite. Plusieurs règles peuvent porter le même nom, ce qui peut-être utile à des fins de regroupement.

MENUS « FILTRAGE »

- Indicateur d'utilisation des règles de filtrage
- Composition d'une règle de filtrage



La fenêtre des règles est composée de plusieurs colonnes listées ci-dessous :

- Numéro de la règle et un indicateur (encadré en bleu) sur le nombre de fois où les éléments du paquet reçu correspondent aux critères de la règle de filtrage. Le compteur numérique s'affiche en passant la souris par dessus. Il peut afficher 4 couleurs qui sont le résultat d'un rapport mathématique entre le nombre de hits de la règle et le nombre de hits maximum atteint par une règle dans le même slot:
  - Blanc (vide) : la règle n'a jamais été appliquée,
  - Bleue : la valeur affichée est comprise entre 0 et 2% du hit maximal,
  - Vert : la valeur affichée est comprise entre 2% et 20% du hit maximal,
  - Orange : la valeur affichée est supérieure ou égale à 20% du hit maximal et est supérieure à 10 000 hits.
- **État** : Permet d'activer/désactiver une règle de filtrage.
- **Action** : Indique l'action appliquée sur la connexion : passer, bloquer, tracer, renvoyer vers un portail captif, etc.
- **Source** : Spécifie la source du trafic : adresse IP ou réseau source, interface d'entrée, utilisateur, etc.
- **Destination** : Spécifie la destination du trafic : adresse IP ou réseau destination, interface de sortie.
- **Port de dest** : Indique le port destination du trafic.

## MENUS « FILTRAGE »

- OmniBox pour éditer tous les champs de la règle à la fois

EDITING RULE NO 1

General STATUS - COMMENT - NAME

Action

Source

Destination

Port - Protocol

Inspection

General

Status:

Comments:

Advanced properties

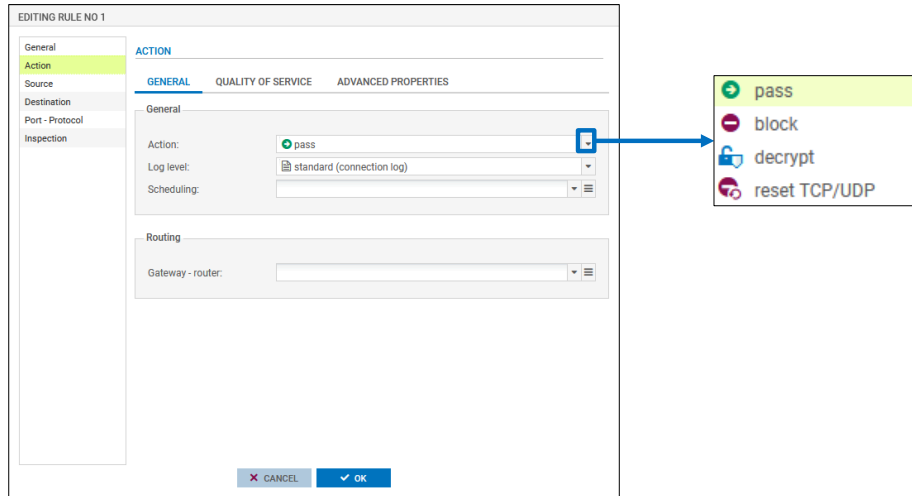
Rule name:

Les paramètres d'une règle peuvent être renseignés directement dans la fenêtre des règles ou sur une nouvelle fenêtre (omnibox) qui s'affiche en double cliquant sur n'importe quel paramètre de cette règle.

Les valeurs des paramètres étant des objets, ils peuvent être copiés d'une règle à une autre par un simple glisser/déposer. Ce procédé permet également de déplacer les règles de filtrage en cliquant à gauche sur le numéro de la règle. Enfin, les nouvelles règles ajoutées doivent être sauvegardées et activées explicitement avec le bouton **Sauvegarder et activer**.

## MENUS « FILTRAGE »

- Menu Action : définition de l'action



Le menu **ACTION** est constitué de plusieurs onglets, nous nous intéresserons principalement à l'onglet **GÉNÉRAL** qui permet de spécifier les paramètres suivants :

- **Action** : Définit l'action à appliquer au paquet correspondant à la règle de filtrage :
  - **passer** : Autorise le paquet,
  - **bloquer** : Bloque le paquet,
  - **déchiffrer** : Renvoie le paquet vers le proxy SSL,
  - **réinit. TCP/UDP** : Dans le cas d'un trafic TCP, le firewall renvoie un paquet « TCP RST » à l'émetteur. Dans le cas d'un trafic UDP, le firewall renvoie une notification ICMP port inaccessible (port unreachable) à l'émetteur.

MENUS « FILTRAGE »

- Menu Action : définition du niveau de trace

The screenshot shows the 'EDITING RULE NO 1' configuration window. The 'ACTION' tab is selected. Under the 'GENERAL' sub-tab, the 'Log level' dropdown menu is open, displaying four options: 'standard (connection log)', 'advanced (connection log and filtering log)', 'minor alarm', and 'major alarm'. A blue arrow points from the dropdown menu to the 'standard (connection log)' option. The 'Action' dropdown is set to 'pass'. There are 'CANCEL' and 'OK' buttons at the bottom of the window.

STORMSHIELD

16

- **Niveau de trace** : Permet de tracer les flux traités par la règle. Il peut avoir plusieurs valeurs :
  - **standard (journal de connexions)** : C'est la valeur par défaut, seules les connexions établies ayant leur couche de transport en TCP/UDP sont journalisées :
    - Dans le journal « Connexions réseau » ou dans le journal « Connexions applicatives » si une analyse applicative est menée par un plugin (en mode IPS, IDS),
    - Les connexions avec action « Bloquer » ne sont pas journalisées.
  - **avancé (journal de filtrage)** : Les flux sont tracés dans le journal « Filtrage ». Cette option n'est utile que pour :
    - Journaliser des flux directement au-dessus d'IP (ICMP, GRE, ESP,...),
    - Journaliser le blocage d'un flux par l'action « Bloquer ».
  - **alarme mineure** : La connexion est tracée dans le journal « Alarmes » avec une alarme mineure.
  - **alarme majeure** : La connexion est tracée dans le journal « Alarmes » avec une alarme majeure.

**NOTE** : L'utilisation du mode verbeux sur une connexion en TCP/UDP est non seulement inutile, mais crée des doublons avec une écriture dans un des journaux de connexions et une écriture dans le journal de filtrage pour le même flux.

## MENUS « FILTRAGE »

- Menu Action : Programmation horaire et routage par politique

The image shows two screenshots from the Stormshield management interface. The left screenshot, titled 'EDITING RULE NO 1', displays the configuration for a rule. It has tabs for 'GENERAL', 'QUALITY OF SERVICE', and 'ADVANCED PROPERTIES'. The 'GENERAL' tab is selected, showing fields for 'Action' (set to 'pass'), 'Log level' (set to 'standard (connection log)'), and 'Scheduling'. A blue box highlights the 'Routing' section, specifically the 'Gateway - router' field. A blue arrow points from this box to the right screenshot. The right screenshot, titled 'CREATE AN OBJECT', shows a dialog for creating a new object. It has a sidebar with categories like 'Host', 'DNS name (FQDN)', 'Network', 'Address range', 'Router', 'Group', 'IP Protocol', 'Port', 'Port group', 'Region group', and 'Time object'. The 'Time object' category is selected. The main area shows 'Object name: custom\_workhours', 'Description: every Monday, Tuesday, Wednesday, Thursday, Friday From 09:00 to 18:00', and a 'Time slot(s)' section with a table for days of the week.

- **Programmation horaire** : Sélection d'un objet temps qui permet de définir des plages horaires hebdomadaires, des événements annuels ou ponctuels. Les objets temps peuvent être créés dans le menu **CONFIGURATION ⇒ OBJETS ⇒ Objets temps** ou en cliquant sur le bouton encadré en bleu. Si ce paramètre est renseigné, la règle de filtrage sera active uniquement durant la plage horaire définie par l'objet temps.
- **Passerelle – routeur** : Ce paramètre permet de mettre en œuvre le routage par politique (présenté dans le module « Configuration réseau »). Dès lors qu'une passerelle est renseignée, tout le trafic traité par cette règle de filtrage sera transmis à cette passerelle et non à la passerelle par défaut si aucune autre directive de routage plus prioritaire n'est configurée.

MENUS « FILTRAGE »

- Menu Source : onglet général

EDITING RULE NO 1

General SOURCE

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

General

User: Searching...

Source hosts: Network\_in

Incoming interface: Select an interface

+ Add X Delete

equal to

different from

[Ethernet]

out

in

dmz1

dmz2

[IPSec]

VTI\_to\_B

[All]

any

+ Add X Delete

Network\_in

Network\_dmz1

srv\_dns\_priv

X CANCEL ✓ OK

STORMSHIELD

18

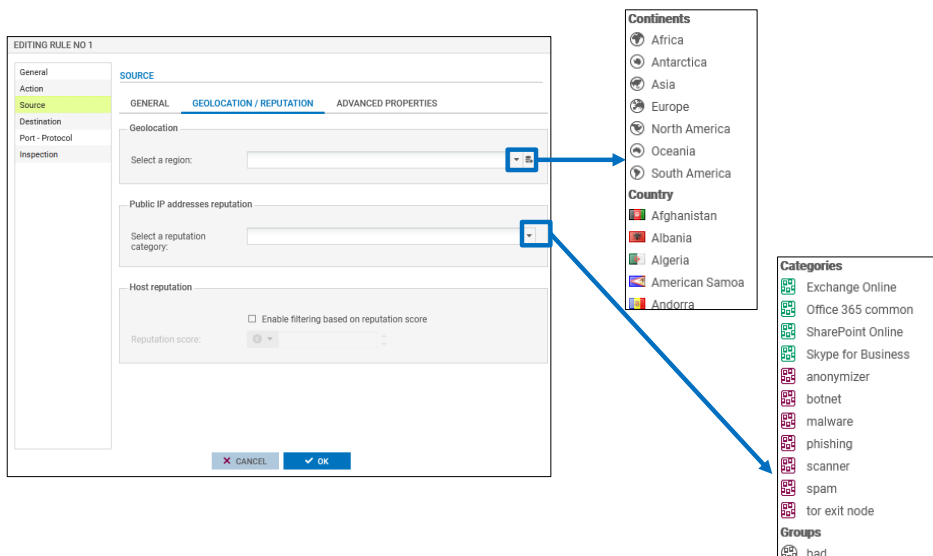
Le menu **Source** ⇒ **GÉNÉRAL** regroupe les paramètres qui identifient la source du trafic concerné par la règle de filtrage :

- **Utilisateur** : Permet de renseigner l'utilisateur ou le groupe d'utilisateurs qui est à l'origine du trafic. Ce paramètre est fonctionnel dans le cadre d'un système d'authentification basé sur un annuaire utilisateurs (voir module « Utilisateurs et Authentification »).
- **Machines sources** : Indique l'adresse IP, le Fully Qualified Domain Name (FQDN) ou l'adresse réseau du trafic. Les icônes « = » ou « ≠ » signifient que le paramètre peut être égal ou différent de la valeur spécifiée. De plus, il est possible de renseigner une liste d'objets en cliquant sur le bouton **Ajouter**, le coin rouge en haut à gauche des objets ajoutés signifie que cet ajout n'a pas encore été sauvegardé.
- **Interface d'entrée** : Permet de préciser l'interface d'entrée du trafic. Ce paramètre est utile dans le cas des bridges où les interfaces partagent le même plan d'adressage.



## MENUS « FILTRAGE »

- Menu Source : onglet géolocalisation et réputation



Le menu **Source** ⇒ **GÉOLOCALISATION / RÉPUTATION** regroupe les paramètres suivants :

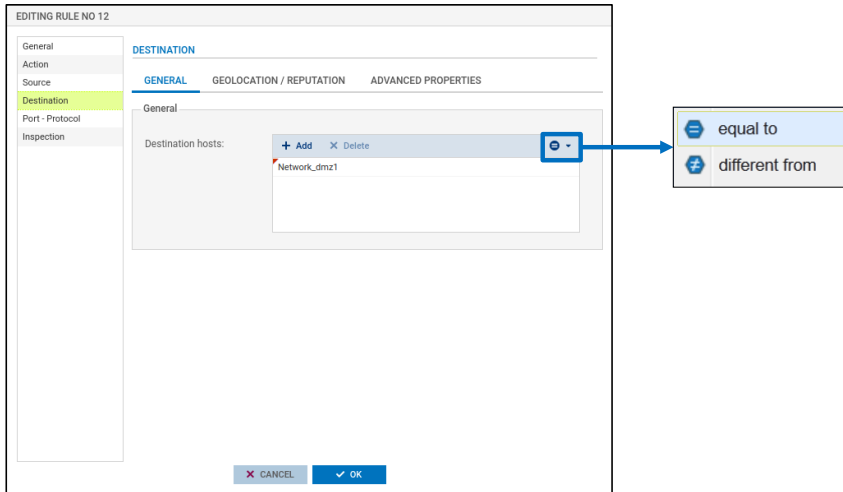
- **Géolocalisation** : Permet de renseigner un continent ou un pays à l'origine du trafic. La liste ne contient pas d'adresses IP, le Firewall détermine le pays auquel appartient une IP, plutôt que de charger toutes les IP (les blocs d'adressage sont très fragmentés sur Internet).
- **Réputation des adresses IP publiques** : Une IP publique peut avoir une réputation à la limite de deux catégories. Le groupe « Bad » regroupe les catégories : anonymizer, botnet, malware, phishing, scanner, spam et tor.
- **Réputation des machines** : Il est possible d'activer le filtrage selon le score de réputation des machines du réseau interne. Il faut au préalable activer la gestion de réputation des machines et définir les machines concernées par le calcul d'un score de réputation, ce point est détaillé dans les annexes.

Dans le menu **Source**, les paramètres **Géolocalisation** et **Réputation des adresses IP publiques** sont utilisés généralement pour qualifier le flux entrant (provenant d'Internet), alors que le paramètre **Réputation des machines** est utilisé pour qualifier le flux sortant.

**NOTE** : Le score de réputation des machines internes, configurable dans ce menu, permet de préciser le score au-dessus duquel ou en-dessous duquel la règle de filtrage s'appliquera aux machines supervisées.

MENUS « FILTRAGE »

- Menu Destination : onglet général



Le menu **Destination** regroupe les paramètres qui identifient la destination du trafic. Dans l'onglet **GÉNÉRAL**, le paramètre **Machines destination** indique l'adresse IP, l'adresse réseau ou le FQDN destination du trafic. Nous pouvons également choisir si le paramètre doit être égal ou différent de la valeur et renseigner une liste d'objets.

La géolocalisation et la réputation des adresses IP publiques ainsi que la réputation des machines peuvent être utilisées également dans les paramètres de destination depuis l'onglet **GÉOLOCALISATION / RÉPUTATION**.

**NOTE** : Lorsque l'objet de destination est un objet FQDN, il doit être le seul objet de la liste.

MENUS « FILTRAGE »

- Menu Destination : configuration avancée

21

Dans l'onglet **CONFIGURATION AVANCÉE**, nous pouvons restreindre l'application de la règle uniquement au trafic sortant par l'interface indiquée dans **interface de sortie**.

**NOTE** : Pour les règles autorisant un flux sortant vers Internet, il n'est pas conseillé de renseigner l'interface de sortie car la route à emprunter pour joindre la destination du flux n'est pas encore connue dans le cas où on utilise plusieurs passerelles (objet routeur).

## MENUS « FILTRAGE »

## • Menu Port – Protocole : définition d'un port

EDITING RULE NO 1

General  
Action  
Source  
Destination  
Port - Protocol  
Inspection

**PORT AND PROTOCOL**

Port

Destination port:

https

Protocol

Protocol type: Automatic protocol detection (default)

Application protocol: Based on default port or content

IP protocol: All

CANCEL OK

equal to  
different from  
lower than  
higher than

22

Le menu **PORT / PROTOCOLE** permet de renseigner le **Port destination** avec la possibilité de choisir s'il doit être égal, différent, inférieur ou supérieur à la valeur sélectionnée. Il est également possible de renseigner une liste de ports de destination.

MENUS « FILTRAGE »

- Menu Port – Protocole : définition d'un protocole

EDITING RULE NO 1

General  
Action  
Source  
Destination  
Port - Protocol  
Inspection

PORT AND PROTOCOL

Port

Destination port: + Add X Delete

Any

Protocol

Protocol type: IP protocol

Application protocol: No applicative analysis

IP protocol: icmp

ICMP message: Echo request (Ping)

Stateful tracking

X CANCEL ✓ OK

- icmpv6
- vpn-ah
- vpn-esp
- gre
- sctp
- udp
- tcp
- igmp
- icmp
- ggp
- ipencap
- egp
- igp
- hmp
- rdp
- ipv6encap
- rsvp
- swipe
- mobile
- ipv6-nonxt
- eigrp
- ospf
- ipip

23

Le menu **PORT / PROTOCOLE** permet également de spécifier le protocole IP concerné par la règle de filtrage. Pour cela, il faut sélectionner le paramètre **Type de protocole** et choisir la valeur **Protocole IP**, puis préciser le protocole dans le champ **Protocole IP**. Si le protocole ICMP est sélectionné, le paramètre **Message ICMP** s'affiche automatiquement pour permettre d'affiner le filtrage en choisissant le type de notification ICMP concerné par la règle de filtrage.

**NOTE :** Le suivi des états « stateful » qui permet de mémoriser et de suivre les connexions traversant le firewall est activé et figé (non modifiable) uniquement pour les protocoles TCP, UDP et ICMP. Pour les autres protocoles (GRE, ESP, etc.), il faut cocher cette option pour activer le suivi.

## MENUS « FILTRAGE »

- Règle de filtrage avec NAT sur destination

SECURITY POLICY / FILTER - NAT

(5) Training lab | Edit | Export

FILTERING NAT

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	incoming_smtp	pass	Internet interface: out	srv_mail_pub srv_mail_priv	smtp		IPS

**DESTINATION**

GENERAL GEOLOCATION / REPUTATION **ADVANCED PROPERTIES**

Advanced properties

Outgoing interface: Select an interface

NAT on the destination

Destination: srv\_mail\_priv

ARP publication on external destination (public)

**PORT AND PROTOCOL**

Port

Destination port: smtp

Protocol

Protocol type: Automatic protocol detection (default)

Application protocol: Based on default port or content

IP protocol: All

Port translation

Translated dest. port: smtp

24

Dans une règle de filtrage, une directive de NAT sur la destination (DNAT) peut être appliquée, sauf si elle contient un objet FQDN, ou des éléments de géolocalisation et /ou de réputation.

**Exemple** : La figure ci-dessus illustre une translation sur la destination d'un trafic SMTP entrant. La règle de filtrage autorise ce trafic en provenance d'un réseau externe et à destination de l'adresse IP publique du serveur SMTP sur le port SMTP/25. L'adresse et le port destination sont tradlatés respectivement par l'adresse IP privée du serveur SMTP et le port SMTP/25 directement dans la règle de filtrage où la publication ARP est également activée. Grâce à cette configuration, il n'est pas nécessaire d'ajouter une règle de translation pour rediriger ce trafic.

Il existe plusieurs avantages à créer une directive de NAT sur destination au sein d'une règle de filtrage:

- Indication rapide du flux autorisé avec redirection vers la machine interne,
- Gestion et supervision des règles entrantes dans un seul menu,
- Optimisation du temps de traitement des règles puisque les règles présentes dans l'onglet NAT ne sont pas parcourues,
- Activation de protections applicatives (filtrage SMTP, antispam, etc.) à des connexions entrantes tradlatées.



- Généralités
- La notion de « stateful »
- L'ordonnancement des règles de filtrage et de translation
- Menus « filtrage »
- **L'analyseur de cohérence et de conformité**
- ➔ Lab - Filtrage

## L'ANALYSEUR DE COHÉRENCE ET DE CONFORMITÉ

The screenshot displays the 'SECURITY POLICY / FILTER - NAT' configuration page. It shows a table of filtering rules with columns for Status, Name, Action, Source, Destination, Dest. port, Protocol, and Security inspection. Below the table, a 'CONFIGURATION VALIDATOR' section shows two warnings: one for Rule 1 (incompatible port and protocol) and one for Rule 3 (covered by Rule 2).

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	outgoing_https	pass	Network_in	Internet	https	udp	IPS
2	on	outgoing_all	pass	Network_in	Internet	Any		IPS
3	on	block_korea	block	Network_in	Internet geo: Republic of Korea	Any		IPS
4	on	incoming_http	pass	Internet	Firewall_out interface: out	http		IPS

**CONFIGURATION VALIDATOR (1 / 1)**

- [Rule 1] The destination port 'https' uses an IP that is incompatible with the value of the protocol column
- [Rule 3] This rule will never be applied as it is covered by the rule 2.

Les firewalls Stormshield Network embarquent un moteur de vérification qui permet de détecter d'éventuelles situations de recouvrement ou d'incohérence créées dans la politique de filtrage. Ce type de situation est signalé par un message d'avertissement en bas du menu.

Trois exemples sont illustrés dans la figure ci-dessus :

- Dans la règle n°1, le port destination HTTP est incompatible avec le protocole UDP parce que le protocole applicatif HTTP utilise le protocole de transport TCP,
- La règle n°3 ne sera jamais utilisée parce qu'elle est recouverte par la règle n°2,
- La règle n°4 souligne que le flux arrive sur un objet dont l'IP peut changer (IP dynamique associée à la patte out), et qu'il faut préciser l'interface d'entrée (dans le champ source).

**NOTE** : Les messages signalés avec une croix rouge bloquent l'activation de la politique.

## RECOMMANDATIONS



- Compléter les règles d'antispoofing par du filtrage
- Désactiver les règles implicites excepté la règle HA
- Utiliser des groupes d'objets
- Supprimer les règles qui se chevauchent ou inutiles
- Nommer les règles

L'antispoofing a ses limites et ne bloque pas les réseaux privés arrivant par internet par exemple. Il est donc nécessaire de compléter la protection avec des règles de blocage déduites de la topologie du réseau. Par exemple bloquer les IP RFC5735 sur les réseaux publics.

Les règles implicites étant évaluées avant les autres, elle peuvent rendre inopérantes des règles créées par l'administrateur. Attention à bien préparer les règles d'autorisation d'accès à l'interface web pour ne pas perdre la main sur le firewall. Le SSH vers le SNS étant accessible par défaut sur toutes les interfaces internes, c'est l'occasion de le limiter.

La règle implicite pour la haute disponibilité ne peut pas être créée explicitement via l'interface web, le plugin ASQ correspondant n'étant pas disponible (protocole hasync).

Les groupes d'objets simplifient la modification des règles. Il est recommandé d'utiliser des groupes plutôt que de créer des listes de machines dans les règles. Cela améliore aussi la lisibilité.

Tout comme pour les NAT, il est recommandé de ne jamais laisser des règles se recouvrir. De même, il faut traquer et supprimer régulièrement toutes les règles inutilisées.

La colonne (par défaut cachée) **nom** permet d'identifier une règle par son nom, c'est un filtre puissant pour rechercher une règle ou pour suivre son comportement en débogage.



Vous trouverez ci-dessous les liens vers deux notes techniques publiées par l'ANSSI

- Recommandations pour la définition d'une politique de filtrage réseau d'un firewall : <https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dun-pare-feu-stormshield-network-security-sns/>
- Recommandations de sécurisation d'un firewall Stormshield Network Security (SNS) : <https://www.ssi.gouv.fr/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/>

Pour aller plus loin, consultez la note technique du site [documentation.stormshield.eu](http://documentation.stormshield.eu) :

- Mise en œuvre d'une règle de filtrage

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](http://kb.stormshield.eu).



- Généralités
- La notion de « stateful »
- L'ordonnement des règles de filtrage et de translation
- Menus « filtrage »
- L'analyseur de cohérence et de conformité

 **Lab - Filtrage**



## Lab 5 – Filtrage

Copiez la politique de filtrage/NAT **(4) Lab\_4** vers la politique numéro 5. Renommez la politique numéro 5 « Lab\_5 », puis activez cette politique. Supprimez la règle **Pass any any any** et ajoutez les règles de filtrage qui respecteront le cahier des charges suivant:

- Utilisez les séparateurs pour indiquer le rôle de chaque bloc de règles.
- Affichez la colonne « Nom » des règles et la compléter pour chaque règle.

### Trafics internes :

1. Votre réseau interne (in : 192.168.y.0/24) doit pouvoir accéder aux serveurs de votre DMZ : DNS, WEB (ports 80 et 808 pour le webmail), FTP et SMTP.

### Trafics sortants :

2. Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec [www.visitkorea.or.kr](http://www.visitkorea.or.kr)).
3. L'accès au site <https://www.cnn.com> doit être bloqué depuis le réseau interne. Pour cela utilisez un objet FQDN.
4. Votre réseau interne doit pouvoir joindre les serveurs FTP d'Internet.
5. Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine (pc\_200) est 192.168.y.200.
6. Votre réseau interne doit pouvoir émettre un ping vers n'importe quelle destination.
7. Votre réseau interne doit pouvoir se connecter en SSH aux firewalls des autres sites.
8. Seul votre serveur DNS interne (172.16.y.10) peut envoyer des requêtes DNS vers l'extérieur.
9. Votre serveur de messagerie peut envoyer des mails vers n'importe quel serveur de mail externe.

### Trafics entrants :

10. Les réseaux externes peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
11. Les serveurs mail externes sont autorisés à transmettre des e-mails à votre serveur de messagerie.
12. Les réseaux externes sont autorisés à pinger l'interface « out » de votre firewall; ce type d'événement doit lever une alarme mineure.



13. Les réseaux externes peuvent se connecter à votre firewall : via l'interface web et en SSH. Ce type d'événement doit lever une alarme majeure.

14. Testez les trafics sortants et faites tester les trafics entrants par les voisins. En consultant les traces, confirmez :

- Le traitement de chaque flux par la règle de filtrage qui lui correspond.
- Le traçage et la levée des alarmes pour les règles demandées.

**NOTE :** Vous pouvez utiliser le service webmail pour envoyer ou recevoir des e-mails en SMTP : les informations nécessaires à la configuration (remplacez « x » par la lettre de l'entreprise : a, b ; et y par sa valeur : 1, 2) :

- Serveur SMTP : mail.x.net
- Accès au webmail : http://172.16.y.11:808
- Utilisateur : user
- Mot de passe : user
- Adresses email : [user@x.net](mailto:user@x.net)



# Quiz

STORMSHIELD

Q1 – Pour autoriser un trafic TCP à passer au travers du pare-feu, il faut impérativement créer une seconde règle pour autoriser les paquets réponses, sinon le client ne recevra jamais les données demandées au serveur.

- A. Vrai
- B. Faux

Q2 – Les règles de filtrage implicites peuvent toute être désactivées :

- A. Vrai
- B. Faux

Q3 – L'action « block » sur une règle de filtrage permet de rejeter une connexion et d'informer le client que ce trafic n'est pas autorisé :

- A. Vrai
- B. Faux

Q4 – Dans quels cas est-il intéressant d'utiliser le niveau de trace avancé ?

- A. Tout le temps si je souhaite avoir des log des connexions traversant le pare-feu.
- B. Si je souhaite avoir des log du trafic ICMP et ESP.
- C. Si je souhaite avoir des log des paquets bloqués.

Q5 – Il n'est pas possible d'utiliser une liste d'objets dans la destination d'une règle de filtrage si on y insère un objet FQDN.

- A. Vrai
- B. Faux



Q6 – Le pare-feu Stormshield permet d'autoriser spécifiquement un message ICMP avec son type et son code.

- A. Vrai
- B. Faux



STORMSHIELD

# ANNEXE – FILTRAGE

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



➔ Configurations avancées

STORMSHIELD

Filtrage

**CONFIGURATIONS AVANCÉES : ACTION « DÉLÉGUER »**

Local policy  
 Global policy

SECURITY POLICY / FILTER - NAT

Global policy (1) Global Filter 01 Edit Export

FILTERING NAT

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	outgoing_http	delegate	Network_in	Internet	http		IPS
2	on	admin_GUI_ssh	pass	pc_admin	Firewall_out	Admin_srv		IPS

```
1 : 1 : jump 1 ipproto tcp from 192.168.1.0-192.168.1.255 to !<Network_internals:4> port 80 rulename "outgoing http"
```

STORMSHIELD 3

Les règles de filtrage global (utilisées le plus souvent par le serveur d'administration centralisée SMC) donnent accès à une nouvelle action qui permet de déléguer le choix de l'action au filtrage local. Ainsi, les paquets qui correspondent à une règle de filtrage global dont l'action est **déléguer** continueront à être confrontés directement aux règles de filtrage local.

Pour voir les politiques globales, rendez-vous en haut à droite de votre écran sur **Admin > Préférences** et cocher la case **Afficher les politiques globales**.

Une fois activée, cette règle est visible en mode console en tapant la commande : **sfctl -s filter**

elle contient l'action « Jump » suivie du nombre de règles à ne pas analyser pour atteindre le filtrage local (1 dans l'exemple ci-dessus où une seule autre règle globale suit la règle avec délégation).

CONFIGURATIONS AVANCÉES : PORT SOURCE

STORMSHIELD

4

Une règle de filtrage permet d'utiliser le port source comme critère d'identification d'un trafic. Ce paramètre n'apparaît pas par défaut dans la fenêtre des règles mais il peut être affiché en sélectionnant la colonne qui lui correspond. Sa configuration peut s'effectuer également via l'onglet **CONFIGURATION AVANCÉE** du champ **source**.

## CONFIGURATIONS AVANCÉES : FILTRAGE BASÉ SUR LA VALEUR DU CHAMP DSCP

SECURITY POLICY / FILTER - NAT							
(4) Filter 04(active policy) Edit Export							
FILTERING				NAT			
Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	outgoing_dscp	pass	Network_in DSCP: 34 Class 4, gold (AF41)	Internet	Any		IPS

EDITING RULE NO 1

General  
Action  
Source  
Destination  
Port - Protocol  
Inspection

**SOURCE**

GENERAL GEOLOCATION / REPUTATION **ADVANCED PROPERTIES**

Advanced properties

Source port: smtp

Via: Any

source DSCP: 34 Class 4, gold (AF41)

Authentication method: None

- 34 Class 4, gold (AF41)
- All
- Customized field
- 00 best effort
- 08 Class 1
- 10 Class 1, gold (AF11)
- 12 Class 1, silver (AF12)
- 14 Class 1, bronze (AF13)
- 16 Class 2
- 18 Class 2, gold (AF21)
- 20 Class 2, silver (AF22)
- 22 Class 2, bronze (AF23)
- 24 Class 3

STORMSHIELD

5

La valeur du champ DSCP peut être utilisée pour identifier un trafic dans une règle de filtrage. La sélection de la valeur s'effectue au niveau du paramètre **DSCP source** dans l'onglet **CONFIGURATION AVANCÉE** du champ **source** qui offre également la possibilité de définir une valeur personnalisée non standard.

**NOTE :** Le champ DSCP fait partie de l'entête IP et indique la classe de service (QoS) à laquelle appartient un paquet IP.

CONFIGURATIONS AVANCÉES : MARQUAGE DU CHAMP DSCP

The screenshot displays the Stormshield management interface. At the top, a table lists filtering rules. Rule 1, named 'outgoing\_dscp', is highlighted. Below the table, the 'EDITING RULE NO 1' dialog is open, showing the 'ACTION' tab. Within this tab, the 'QUALITY OF SERVICE' sub-tab is active. The 'DSCP' section is expanded, showing the 'Impose value' checkbox checked and the 'New DSCP value' dropdown menu set to '20 Class 2, silver (AF22)'. A blue arrow points from the rule name in the table to the 'DSCP' configuration area.

STORMSHIELD

6

Les firewalls Stormshield Network offrent le moyen de forcer la valeur du champ DSCP pour un trafic par le champ **Action** d'une règle de filtrage. Ainsi, les paquets IP appartenant à ce trafic seront marqués avec la valeur du champ DSCP choisie à la sortie du firewall. La configuration de ce marquage s'effectue dans la partie **DSCP** de l'onglet **QUALITÉ DE SERVICE** appartenant au champ **Action**.



## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Les objets
- ✓ Configuration réseau
- ✓ Translation d'adresses
- ✓ Filtrage
- ➔ Protection applicative
  - Utilisateurs & authentification
  - VPN
  - VPN SSL



## Activation du mode Proxy

- Proxy HTTP
- Proxy HTTPS
- Analyse antivirale
- Prévention d'intrusion et inspection de sécurité
- Lab – Filtrage de contenu (HTTP et HTTPS)

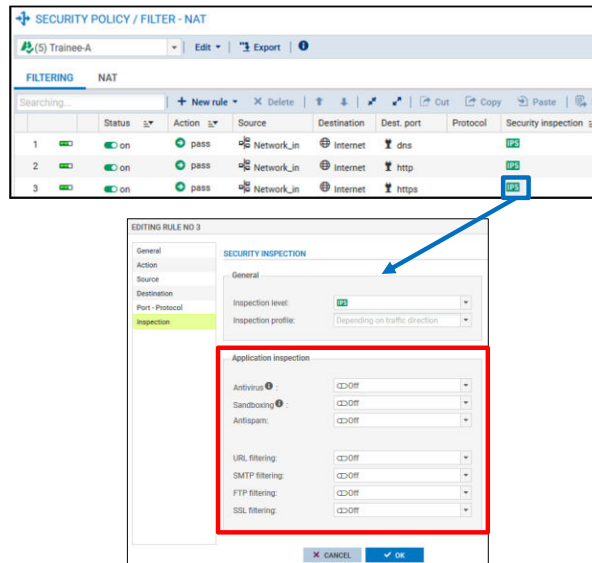
**ACTIVATION DU MODE PROXY**

- Objectifs :
  - Contrôler les accès aux sites web d'Internet (filtrage d'URL et filtrage SSL)
  - Créer une politique anti-relais et antispam (filtrage SMTP)
  - Effectuer une analyse antivirus sur les flux DATA (HTTP, SMTP, FTP, POP3,...)
  - Bloquer les maliciels à l'aide d'une analyse comportementale sur des machines de détonation (sandboxing Breachfighter)

L'analyse applicative complète des flux, qu'ils soient initialement chiffrés ou pas, induit l'utilisation d'un mode Proxy sur les firewalls Stormshield.

## ACTIVATION DU MODE PROXY

- Mise en œuvre :



L'activation d'une inspection applicative (encadré rouge) sur une règle de filtrage du firewall entraîne le démarrage des analyses en mode Proxy transparent :

- Le firewall se fait passer pour le client auprès du serveur et pour le serveur auprès du client,
- La configuration du poste client n'est pas modifiée (c'est le principe du mode transparent), par exemple, le port d'écoute et l'adresse IP du Proxy n'ont pas à être configurés sur son navigateur Internet.

**NOTE :**

- Le mode Proxy explicite des firewalls Stormshield n'est pas évoqué dans ce chapitre. L'utilisation d'un Proxy explicite sur un firewall Stormshield offre moins de fonctionnalités que celle d'un Proxy transparent. Par exemple, un Proxy explicite n'est pas compatible avec l'authentification multi-annuaires ou avec le Proxy SSL (le trafic HTTPS ne peut pas être déchiffré pour subir une analyse antivirale). L'usage du Proxy en mode transparent est donc conseillé.
- Une analyse sur une règle de filtrage en mode IPS seulement n'utilise pas de mécanisme de type Proxy.



- Activation du mode Proxy
- ➔ **Proxy HTTP**
- Proxy HTTPS
- Analyse antivirus
- Prévention d'intrusion et inspection de sécurité
- Lab – Filtrage de contenu (HTTP et HTTPS)

### PROXY HTTP

- Contrôler les accès aux sites web d'Internet en HTTP :
  - Par mots-clés personnalisés
  - Par consultation de sites présents dans une base de données :
    - Base embarquée Stormshield : 16 catégories
    - EWC : Extended Web Control : 65 catégories

La fonction de filtrage des URL permet de contrôler l'accès aux sites web d'Internet pour l'ensemble de vos utilisateurs.

Pour contrôler ces accès, la politique de filtrage URL va se baser sur une liste d'URL rangée au sein de catégories ou de mots clés personnalisés.

Deux fournisseurs de base URL sont disponibles:

1. Base URL embarquée composée de 16 catégories téléchargées sur les serveurs de mise à jour,
2. Base Extended Web Control (EWC) constituée de 65 catégories, toutes hébergées dans le Cloud. Cette solution est disponible en option supplémentaire. Veuillez vous reporter à la section « Fonctionnement d'EWC » pour plus de détails sur son fonctionnement.

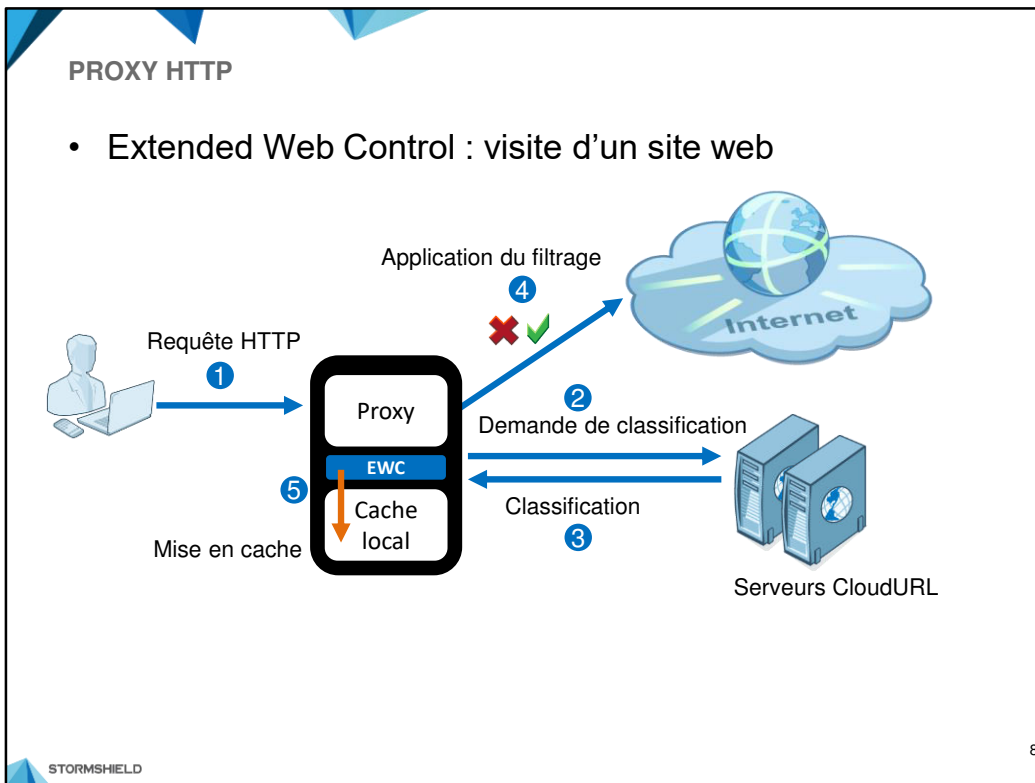
## PROXY HTTP

- Extended Web Control:
  - Solution de filtrage URL
  - Base de données maintenue dans le Cloud
  - Évite toute saturation d'espace disque (surtout pour les produits d'entrée de gamme)

Extended Web Control est une solution de filtrage URL. La base de données est maintenue à jour dans le Cloud.

L'avantage majeur est que la base de données n'est pas téléchargée, ce qui permet d'éviter la saturation de l'espace disque alloué au stockage de la base.

Il s'agit d'une option payante, elle n'est pas intégrée par défaut sur l'ensemble de la gamme.



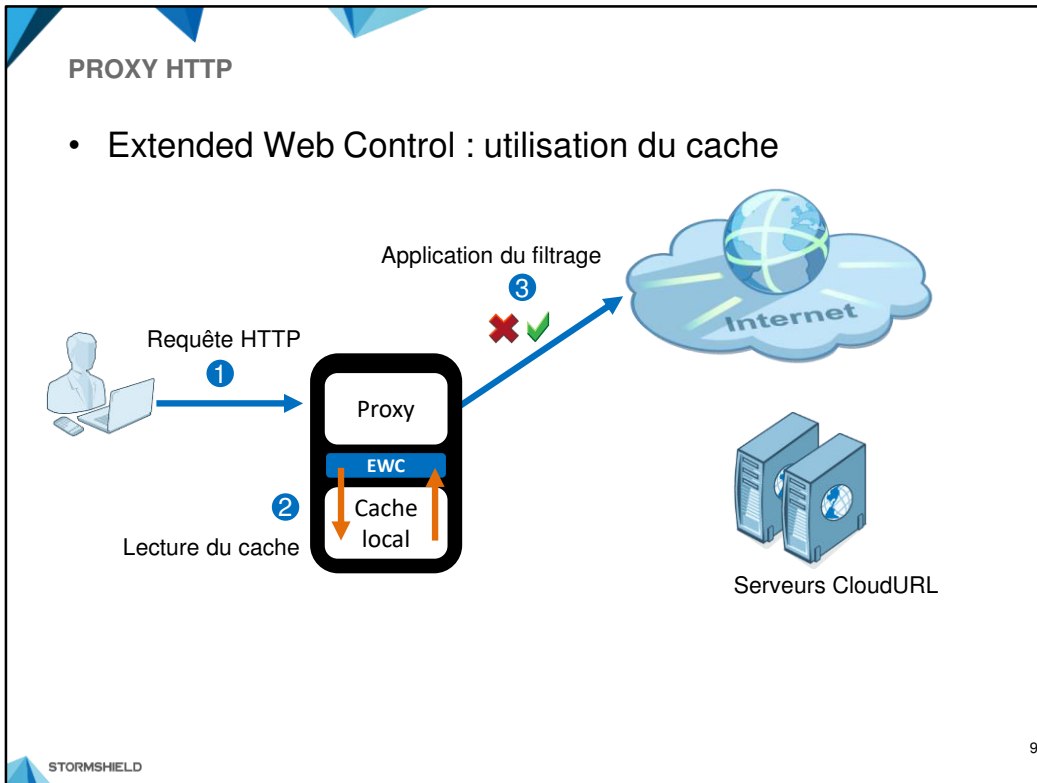
Sur réception d'une connexion HTTP à destination d'un site web sur Internet, le firewall envoie une requête vers un des serveurs Extended Web Control afin de recenser les catégories auxquelles appartient l'URL visitée. Le résultat sera ensuite confronté à la politique de filtrage URL active.

Les serveurs peuvent renvoyer jusqu'à 5 catégories par URL. Par conséquent, une URL peut se trouver simultanément dans une catégorie bloquée et une catégorie autorisée. Dans ce cas, c'est l'ordre des règles de filtrage URL qui prime; assurez-vous donc d'ordonner convenablement vos règles de filtrage URL.

Afin d'optimiser le fonctionnement et éviter l'envoi de plusieurs requêtes vers les serveurs pour la même URL, la solution Extended Web Control utilise un cache. Lorsqu'une requête HTTP est interceptée, le proxy interroge tout d'abord le cache local. Si l'URL n'est pas présente, une requête est alors envoyée aux serveurs Extended Web Control pour connaître les catégories incluant cette URL. Le cache est mis à jour pour conserver la décision appliquée à et l'URL déjà visitée.

La taille du cache, dépendante du modèle, est dimensionnée pour conserver 1 jour de navigation ; son contenu n'est pas visualisable (même en mode console). Le cache est vidé en cas de redémarrage du Firewall ou du daemon gérant les Proxies (tproxyd).

Dans la base objets, les serveurs Extended Web Control (CloudURL) sont nommés `cloudurl[1-5]-sns.stormshieldcs.eu`



Le proxy interroge le cache local, l'URL est présente. Dans ce cas, les serveurs Extended Web Control ne sont pas interrogés.

Le résultat appliqué lors de la dernière visite (donner l'accès ou le bloquer) est également appliqué pour cette connexion.

PROXY HTTP

- Choix de la base d'URL EWC

The screenshot shows the 'OBJECTS / URL' configuration page. A table lists the 'URL DATABASE' as 'Embedded URL database'. A blue box highlights the dropdown arrow. An arrow points from this dropdown to a second dropdown menu showing 'Embedded URL database' and 'Extended Web Control' (highlighted in green). Below this, a 'MIGRATE URL DATABASE' dialog box is displayed with a warning icon and text: 'The current URL database will be deleted, and the database from the provider Extended Web Control will be downloaded. In the meantime, any URL filter policy that uses a category from the current provider will stop working. During the migration, you are advised to apply a URL filter policy that does not need to use URL categories. Confirm change of provider?'. The dialog has two buttons: 'CANCEL' and 'REMOVE CURRENT DATABASE AND INSTALL THE EXTENDED WEB CONTROL DATABASE'.

STORMSHIELD

10

Le choix de la base s'effectue depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **BASE D'URL**.

Le passage de la base URL embarquée à EWC entraîne la suppression des catégories embarquées ; cela vous est notifié par un message d'avertissement.

Après une modification de base, il est conseillé de vérifier la politique de filtrage URL active car le nom des catégories diffère de l'une à l'autre

**Exemple** : la catégorie *Job Search* existe avec *Extended Web Control* mais n'existe pas avec la base embarquée. Par conséquent, l'utilisation de cette catégorie dans le filtrage URL génère un avertissement lors de l'activation de la politique si un retour à la base embarquée a été effectué.

## PROXY HTTP

- Création d'une catégorie personnalisée

OBJECTS / URL

URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE

Add a customized category Remove Check usage Check URL classification Classify

URL category Comments

OBJECTS / URL

URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE

Add a customized category Remove Check usage Check URL classification Classify

URL category Comments

custom\_black\_list

vpnsst\_lowa

antivirus\_bypass

authentication\_bypass

Authorized characters

Authorized characters: '\ \\_ / ' : ; \\_ [a-z] [0-9]

Example: www.google.com/\* or \*.yahoo.com/\*

URL CATEGORY: CUSTOM\_BLACK\_LIST

Add a URL Remove

URL Comments

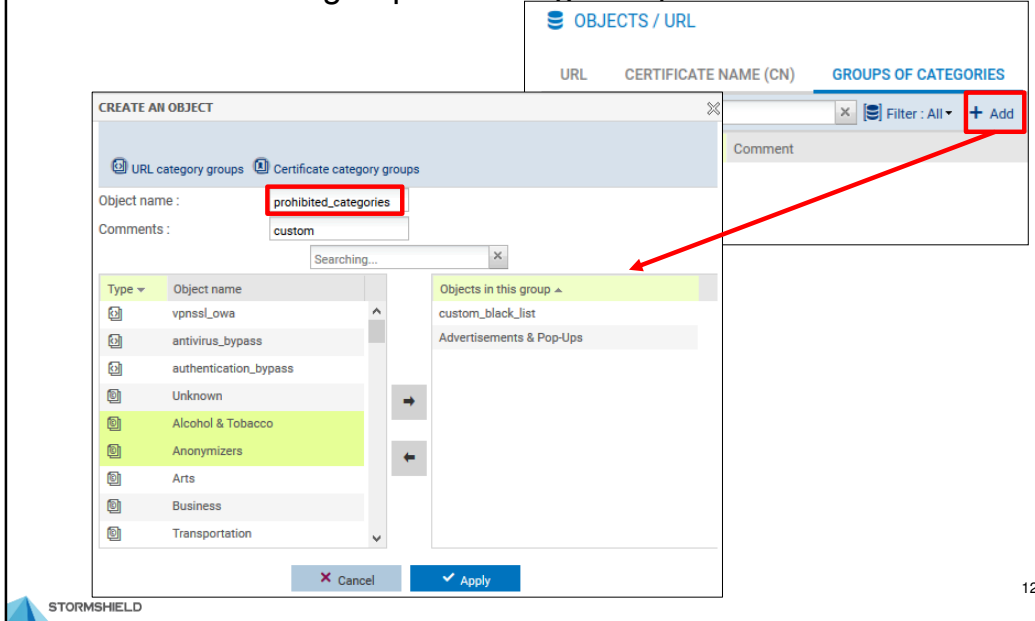
www.perdu.com/\*

STORMSHIELD 11

Depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **URL**, vous pouvez créer vos propres catégories, une catégorie contient une liste d'URL, à ajouter en respectant les suggestions.

## PROXY HTTP

- Création d'un groupe de catégories personnalisé



Depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **GROUPE DE CATÉGORIES**, vous pouvez créer et éditer vos propres groupes de catégories. Choisissez de créer un objet de type **groupe de catégories URLs**.

Un groupe de catégories peut être composé de catégories présentes dans la base (EWC ou embarquée), mais aussi de catégories personnalisées, comme dans l'exemple ci-dessus.

Vous pouvez utiliser les touches CTRL et SHIFT pour présélectionner plusieurs groupes avant de les déplacer.

## PROXY HTTP

- Contenu des groupes ou recherche de classification

The screenshot displays the Stormshield configuration interface for URL classification. The main area shows a table of URL categories with columns for 'URL category' and 'Comments'. The 'URL' tab is selected, and the 'www.stormshield.eu' URL is entered in the 'Add a customized category' field. A red box highlights this URL, and a red arrow points from it to the 'URL categories' field at the bottom of the page, which contains the value 'www.stormshield.eu'. The interface also includes a 'Classify' button, a 'SELECT A CATEGORY' section, and a footer indicating 'No object found'.

Le contenu des catégories ne peut pas être consulté, cependant, l'appartenance d'une URL à un groupe peut être vérifiée par le biais des champs de classification.

Ces champs sont disponibles depuis les menus **URL** ou au sein d'une politique de filtrage URL.

## PROXY HTTP

- Édition de la politique de filtrage URL

SECURITY POLICY / URL FILTERING

(0) Block\_prohibited\_URL Edit URL database provider: Extended Web Control

+ Add X Delete ↑ Up ↓ Down Cut Copy Paste + Add all predefined categories Check URL classification Classify

Status	Action	URL category	Comments
1 on	BlockPage_00	prohibited_categories	
2 on	Pass	Any	
3 on	BlockPage_00	Any	

BlockPage\_00 dropdown menu:

- Block
- Pass
- BlockPage\_00
- BlockPage\_01
- BlockPage\_02
- BlockPage\_03

ERRORS FOUND IN THE URL FILTER POLICY

Line 3: group Any already used in line 2

CANCEL APPLY

Depuis le menu **CONFIGURATION** ⇒ **POLITIQUE DE SÉCURITÉ** ⇒ **Filtrage URL**, choisissez une politique à éditer (dans l'exemple ci-dessus la politique default00 a été renommée Block\_prohibited\_URL).

Il convient ensuite de choisir les sites à autoriser, bloquer ou à rediriger vers l'une des 4 pages de blocage personnalisables.

Le contrôle de cohérence en temps réel affiche les erreurs détectées dans votre politique.



Status	Action	URL category	Comments
1 on	BlockPage_00	Unknown	
2 on	BlockPage_00	Advertisements & Pop-Ups	
3 on	BlockPage_00	Alcohol & Tobacco	
4 on	BlockPage_00	Anonymizers	
5 on	BlockPage_00	Arts	
6 on	BlockPage_00	Business	
7 on	BlockPage_00	Transportation	
8 on	BlockPage_00	Chat	
9 on	BlockPage_00	Forums & Newsgroups	
10 on	BlockPage_00	Compromised	
11 on	BlockPage_00	Computers & Technology	
12 on	BlockPage_00	Criminal Activity	
13 on	BlockPage_00	Dating & Personals	
14 on	BlockPage_00	Download Sites	
15 on	BlockPage_00	Education	
16 on	BlockPage_00	Entertainment	
17 on	BlockPage_00	Finance	
18 on	BlockPage_00	Gambling	

Le bouton **Ajouter toutes les catégories prédéfinies** permet de créer une politique très rapidement.

Cette option ajoute une ligne avec l'action **BlockPage\_00** pour chaque catégorie présente dans la base d'URL courante. Les groupes personnalisés ne sont pas pris en compte et doivent être ajoutés manuellement.

Un site web peut être classé dans plusieurs catégories. Dans ce cas, l'ordre des règles de filtrage définit l'action à appliquer pour le site concerné.

**Exemple** : *www.leroymerlin.fr* fait partie de deux groupes EWC (Leisure and Recreation, Shopping). L'ordre de ces deux groupes dans la politique de filtrage URL active va dicter le comportement à appliquer pour toute visite sur le site *www.leroymerlin.fr*.

## PROXY HTTP

- Application du filtrage URL dans la politique de filtrage

The screenshot displays the Stormshield configuration interface. At the top, it shows the 'SECURITY POLICY / FILTER - NAT' configuration page. A table lists three NAT rules. Rule 3 is highlighted in green and has a blue box around its 'Security inspection' column, which contains 'URL filter: Accept\_only\_news'. Below this, the 'EDITING RULE NO 3' dialog is open, showing the 'SECURITY INSPECTION' tab. In the 'Application inspection' section, the 'URL filtering' dropdown is set to 'Accept\_only\_news' and is highlighted with a red box. To the right, a dropdown menu shows the 'Accept\_only\_news' policy with a list of filters: (00) Block\_prohibited\_URL, (01) Accept\_only\_news (highlighted), (02) URLFilter\_02, (03) URLFilter\_03, (04) URLFilter\_04, (05) URLFilter\_05, (06) URLFilter\_06, (07) URLFilter\_07, (08) URLFilter\_08, and (09) URLFilter\_09. A red arrow points from the 'Accept\_only\_news' policy in the dropdown to the 'URL filtering' dropdown in the rule configuration dialog. The Stormshield logo is visible in the bottom left corner, and the number '16' is in the bottom right corner.

Une fois la politique de filtrage URL définie, il convient de l'appliquer à une règle de filtrage autorisant les flux HTTP sortants, comme le montre l'exemple ci-dessus. Dans cette règle, le réseau nommé Network\_dmz1 n'a accès qu'aux sites classifiés dans la catégorie News.

Cette manière de procéder permet d'activer plusieurs politiques de filtrage URL simultanément ; afin de gérer les accès de différents réseaux ou machines sources.

## PROXY HTTP

- Personnalisation des pages de blocage

```

NOTIFICATIONS / BLOCK MESSAGES

ANTIVIRUS  HTTP BLOCK PAGE

BLOCKPAGE_00  BLOCKPAGE_01  BLOCKPAGE_02  BLOCKPAGE_03

Rename Reset Copy to
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><head>
<title id="header_title">Blocked URL</title>
<meta content="text/html; charset=utf-8" http-equiv="Content-type">
<style type="text/css">
#messages {
display: none;
}
</style>
<script type="text/javascript">
function find_local () {
var local = window.navigator.systemLanguage||window.navigator.userLanguage||window.navigator.language;
if (local.indexOf("-") != -1) {
return local.split("-")[0];
}
return local;
}

function load_text_from_dom (disabled) {
var message_id, message, messages, message_dom;
if (disabled) return;
var dom_msg = document.getElementsByTagName("messages");
var local = find_local();
if (!dom_msg) return;

```

Les pages de blocage peuvent être éditées depuis le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Messages de blocage** ⇒ Onglet **PAGE DE BLOCAGE HTTP**.

Les modifications peuvent s'effectuer grâce l'éditeur HTML, cela permet de personnaliser la page de manière précise.



- Activation du mode Proxy
- Proxy HTTP
- ➔ **Proxy HTTPS**
- Analyse antivirus
- Prévention d'intrusion et inspection de sécurité
- Lab – Filtrage de contenu (HTTP et HTTPS)



### PROXY HTTPS

- Contrôler les accès aux sites web d'Internet en HTTPS :

- Par vérification du SNI, présent dans la requête du client et consultation des catégories de sites dans les bases :

- Embarquée Stormshield : 16 catégories
- Extended Web Control : 65 catégories

```
> Internet Protocol Version 4, Src: 192.168.250.57, Dst: 208.97.177.124
> Transmission Control Protocol, Src Port: 51885, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
    ✓ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
      > Random: 14f2d761b87857b10276673b9d8f1a225335081adc4043ac...
      Session ID Length: 32
      Session ID: 6e60379858c81fd0d248afea87163052a5dae2fcd8185b07...
      Cipher Suites Length: 36
      > Cipher Suites (18 suites)
      Compression Methods Length: 1
      > Compression Methods (1 method)
      Extension Length: 300
      ✓ Extension: server_name (len=14)
        Type: server_name (0)
        Length: 14
        ✓ Server Name Indication extension
          Server Name list length: 12
          Server Name Type: host_name (0)
          Server Name Length: 9
          Server Name: perdu.com
```

- Par déchiffrement du flux HTTPS pour appliquer une politique de filtrage URL comme vu précédemment

Lorsqu'un client initie une connexion vers un site en HTTPS, il envoie en clair au serveur le nom de domaine du site demandé. Ce mécanisme appelé Server Name Indication (SNI) permet au serveur de sélectionner le bon certificat à présenter au client.

Stormshield Network Security s'appuie sur ce système pour contrôler l'accès à ces sites web sans déchiffrer le flux.

**NOTE :** Seules les vérifications par SNI et leur classification pour autoriser ou bloquer le flux sans le déchiffrer sont vues dans ce chapitre. Les traitements approfondis (comme par exemple une politique de filtrage URL ou une analyse antivirus) permis par le déchiffrement du flux HTTPS sont détaillés lors de la formation CSNE.

## PROXY HTTPS

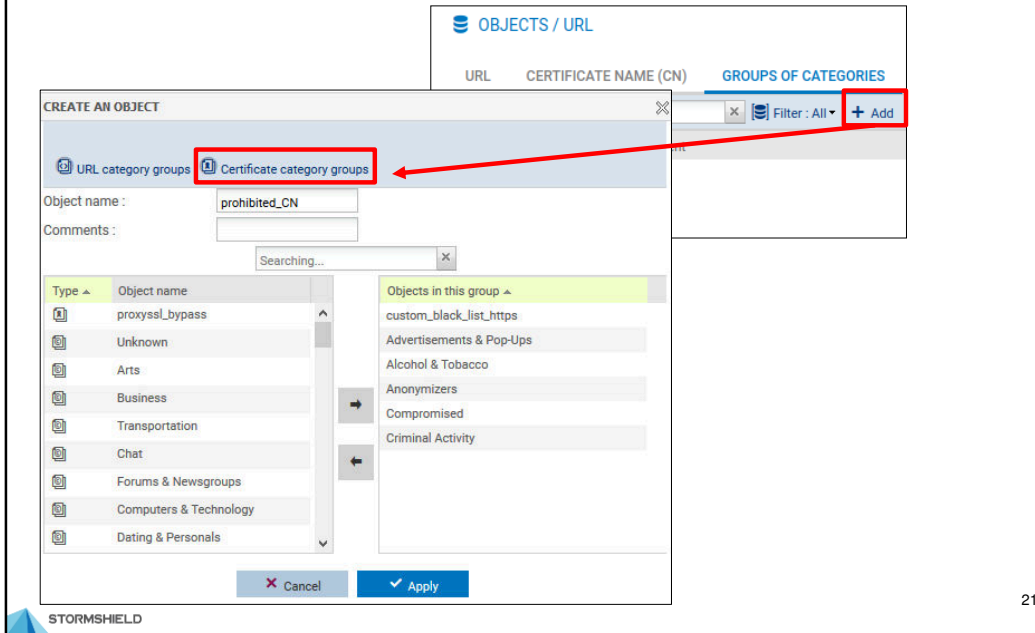
- Création d'une catégorie personnalisée

The screenshot displays the Stormshield configuration interface for 'OBJECTS / URL'. The 'CERTIFICATE NAME (CN)' tab is active. At the top, there are tabs for 'URL', 'CERTIFICATE NAME (CN)', 'GROUPS OF CATEGORIES', and 'URL DATABASE'. Below these, there are buttons for 'Add a customized category', 'Remove', and 'Check usage'. A table lists existing categories: 'Certificate name (CN) category' and 'Comments'. A modal window is open, showing the 'CUSTOM\_BLACK\_LIST\_HTTPS' category. It contains a text area for 'Authorized characters' with the text: '[] [a-z] [A-Z] [0-9] and \* are allowed. The character \* is only valid if placed at the beginning of the URL and immediately followed by a dot.' Below this, there is a button 'Add a certificate name' and a 'Remove' button. A table below shows a single entry: 'Certificate name (C...)' with a 'Comments' column. The entry contains the text '\*.youtube.com'. At the bottom, there is a pagination control showing 'Page 1 of 1'.

Depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **NOM DE CERTIFICAT (CN)**, vous pouvez créer vos propres catégories. Une catégorie contient une liste de CN qui seront comparés aux SNI des connexions SSL/TLS.

## PROXY HTTPS

- Création d'un groupe de catégories



Depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **GROUPE DE CATÉGORIES**, vous pouvez créer et éditer vos propres groupes de catégories. Choisissez de créer un objet de type **groupe de catégories Certificats**.

Un groupe de catégories peut être composé de catégories présentes dans la base (EWC ou embarquée), mais aussi de catégories personnalisées, comme dans l'exemple ci-dessus.

Vous pouvez utiliser les touches CTRL et SHIFT pour présélectionner plusieurs groupes avant de les déplacer.

## PROXY HTTPS

- Édition de la politique de filtrage SSL

SECURITY POLICY / SSL FILTERING

(0) SSLFilter\_00 | Edit | URL database provider: [Extended Web Control](#)

+ Add | X Delete | ↑ Up | ↓ Down | Cut | Copy | Paste | + Add all predefined categories

Status	Action	URL - CN	Comments
1 <input checked="" type="checkbox"/> on	Block without decrypting	custom_black_list_https	
2 <input checked="" type="checkbox"/> on	Pass without decrypting	* any	
3 <input checked="" type="checkbox"/> on	Pass without decrypting	* any	

ERRORS WERE FOUND IN THE SSL FILTER POLICY

Line 3: group any already used in line 2

Depuis le menu **CONFIGURATION** ⇒ **POLITIQUE DE SÉCURITÉ** ⇒ **Filtrage SSL**, choisissez une politique à éditer.

Il convient ensuite de choisir les SNI pour lesquelles les actions **Bloquer sans déchiffrer** et **Passer sans déchiffrer** doivent être appliquées.

Pour rappel, l'action **Déchiffrer**, permettant une analyse approfondie sur le flux HTTPS, sera vue en CSNE.

Le contrôle de cohérence en temps réel affiche les erreurs détectées dans votre politique.

## PROXY HTTPS

- Application du filtrage SSL dans la politique de filtrage

The screenshot shows the Stormshield management interface. On the left, the 'SECURITY POLICY / FILTER - NAT' window displays a list of filtering rules. Rule 2, 'SSL inspection rule', is highlighted with a blue box, and a blue arrow points from it to the 'SSL INSPECTION WIZARD' dialog box on the right. The wizard is configured with the following settings:

- Objective: Inspect encrypted SSL traffic
- Profile of traffic to be decrypted:
  - FROM: Source hosts: Network\_In, Incoming interface: any
  - TO: Destination: Internet, Dest. port: https
- Inspect encrypted traffic:
  - Inspection profile: Depending on traffic direction
  - SSL filter policy: lab6
  - Antivirus: Off

At the bottom of the wizard, the 'FINISH' button is highlighted with a red box. A red arrow points from this button to rule 2 in the 'OUTGOING TRAFFIC' section of the policy editor. This rule is highlighted with a red box and has the following configuration:

Rule ID	Status	Action	Source	Destination	Port	Filter
2	on	decrypt	Network_In	Internet	https	SSL filter: lab6
3	on	pass	Network_In via SSL proxy	Internet	https	URL filter: lab6
4	on	pass	Network_In	Internet	http	URL filter: lab6

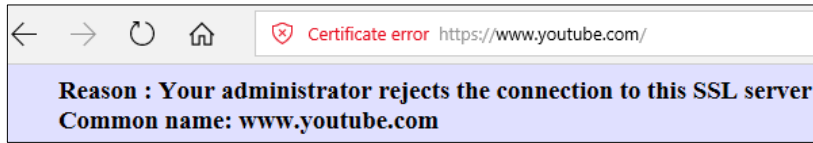
The page number 23 is visible in the bottom right corner of the screenshot.

Une fois la politique de filtrage SSL définie, il convient de l'appliquer, ainsi que l'action **Déchiffrer**, à une règle de filtrage autorisant les flux HTTPS sortants, comme le montre l'exemple ci-dessus.

Cette manière de procéder permet d'activer plusieurs politiques de filtrage SSL simultanément afin de gérer les accès de différents réseaux ou machines sources.

## PROXY HTTPS

- Message affiché sur le navigateur Internet (action Bloquer sans déchiffrer)



Si le CN du site demandé dépend de l'action **Passer sans déchiffrer**, aucune modification n'est effectuée sur la page web demandée.

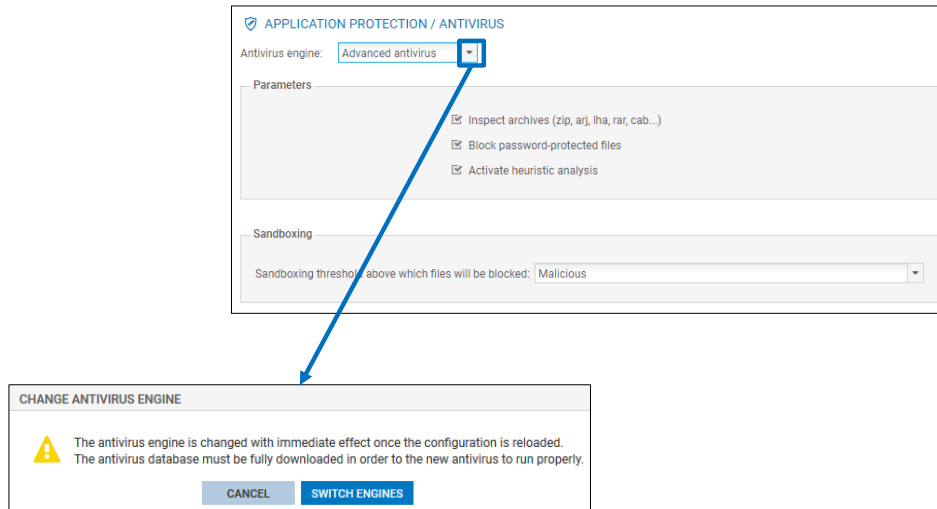
Si le CN du site demandé dépend de l'action **Bloquer sans déchiffrer**, la page web affichée précise seulement que la connexion est rejetée par l'administrateur.



- Activation du mode Proxy
- Proxy HTTP
- Proxy HTTPS
- ➔ **Analyse antivirale**
  - Prévention d'intrusion et inspection de sécurité
  - Lab – Filtrage de contenu (HTTP et HTTPS)

## ANALYSE ANTIVIRALE

- Choix du moteur antivirus



Le choix du moteur antivirus s'effectue depuis le menu **CONFIGURATION** ⇒ **PROTECTION APPLICATIVE** ⇒ **Antivirus**.

L'offre de service antivirus sur les firewalls Stormshield Network se compose de deux solutions:

- ClamAV: Ce moteur antivirus est intégré gratuitement et par défaut dans l'ensemble des produits de la gamme Stormshield Network.
- Antivirus avancé: Pour bénéficier du service antivirus avancé, il est nécessaire de souscrire à un pack de sécurité incluant cette option. Pour plus d'informations sur le service antivirus avancé, veuillez contacter votre revendeur.

En cas de changement de moteur, un message vous indiquera que ce changement nécessite le téléchargement de la base concernée. Par conséquent, et durant toute la durée du téléchargement, l'analyse antivirus échouera.

**NOTE :** L'option « Sandboxing », possible uniquement avec l'Antivirus avancé, dépend d'une option de licence supplémentaire nommée « Sandboxing Breach Fighter », qui est détaillée dans le chapitre « Analyse Breach Fighter ».

## ANALYSE ANTIVIRALE

- Analyse des fichiers

The screenshot shows the 'APPLICATION PROTECTION / PROTOCOLS' configuration page. The 'HTTP' protocol is selected in the left sidebar. The main panel is titled 'ANALYZING FILES' and contains the following settings:

- Transferring files:**
  - Partial download: Block if files analysis is enabled
  - File size limit (KB): 0
  - URLs excluded from the antivirus scan: antivirus\_bypass
- File filter (MIME type):**

Add	Remove	Up	Down	Status	Action	MIME type
				1 Enabled	Detect and block viruses	text/plain
				2 Enabled	Detect and block viruses	text/javascript
				3 Enabled	Pass without analyzing files	text/*
				4 Enabled	Pass without analyzing files	image/*
				5 Enabled	Pass without analyzing files	video/*
				6 Enabled	Pass without analyzing files	audio/*
				7 Enabled	Detect and block viruses	application/flash
				8 Enabled	Detect and block viruses	application/x-flash
				9 Enabled	Detect and block viruses	application/shockwave
- Maximum size for antivirus scan and sandboxing (KB):** 4000
- Action on files:**
  - When a virus is detected: Block
  - When the antivirus scan fails: Block
  - When data collection fails: Pass without scanning

27

Vous trouverez des paramètres additionnels à appliquer aux protocoles pouvant être soumis à une analyse antivirus (voir le menu **CONFIGURATION ⇒ PROTECTION APPLICATIVE ⇒ Protocoles ⇒ HTTP, SMTP, FTP** ou **POP3 ⇒ ANALYSE DES FICHIERS**)

Ce menu est identique pour les protocoles FTP, SMTP et POP3 où il contient :

- La taille maximale pour l'analyse antivirus,
- Les actions sur les messages.

Pour le protocole HTTP, une section supplémentaire contient le comportement de l'antivirus en fonction des types MIME déclarés dans l'entête HTTP.

## ANALYSE ANTIVIRALE

- Réponse émise par l'antivirus à l'utilisateur

**NOTIFICATIONS / BLOCK MESSAGES**

**ANTIVIRUS**    HTTP BLOCK PAGE

---

**POP3 protocol**

Contents of the e-mail :

---

**SMTP protocol**

SMTP error code :

Accompanying message :

---

**FTP protocol**

FTP error code :

Accompanying message :

Depuis le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Messages de blocage**, il est possible de modifier les notifications envoyées aux utilisateurs lorsqu'un mail ou un fichier téléchargé par FTP contient un virus.

Il s'agit d'un paramètre global. Il n'est pas possible de distinguer un message pour les flux entrants et les flux sortants par exemple.

## ANALYSE ANTIVIRALE

- Activation de l'analyse antivirus

The screenshot displays the 'SECURITY POLICY / FILTER - NAT' configuration page. It features a table of NAT rules and a 'SECURITY INSPECTION' configuration panel. The 'Antivirus' option in the 'Application inspection' section is highlighted with a red box and a blue arrow pointing to the 'Security inspection' column of the NAT rules table.

Rule ID	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_in	Internet	dns		IPS Antivirus URL filter: URLFilter_D2
2	on	pass	Network_in	Internet	http		IPS Antivirus
	on	pass	Network_in	Internet	ftp		IPS Antivirus
	on	pass	Network_in	Internet	pop3		IPS Antivirus
	on	pass	Internet	mail_pub, srv_mail_priv	smtp		IPS Antivirus Antispam Mail filter: incoming_emails

**SECURITY INSPECTION Configuration:**

- General
  - Inspection level: IPS
  - Inspection profile: Depending on traffic direction
- Application inspection
  - Antivirus:  On
  - Sandboxing:  Off
  - Antispam:  Off

Les flux pouvant être analysés par le moteur antivirus sont:

- HTTP et HTTPS\*,
- FTP,
- SMTP et SMTPS\*,
- POP3 et POP3S\*.

Pour mettre en œuvre cette analyse, il suffit de sélectionner l'inspection applicative **Antivirus** dans la colonne inspection de sécurité de la règle de filtrage concernée.

**NOTE :** Pour être soumis à une analyse antivirus les flux HTTPS, SMTPS et POP3S doivent au préalable être déchiffrés par une règle d'inspection SSL.

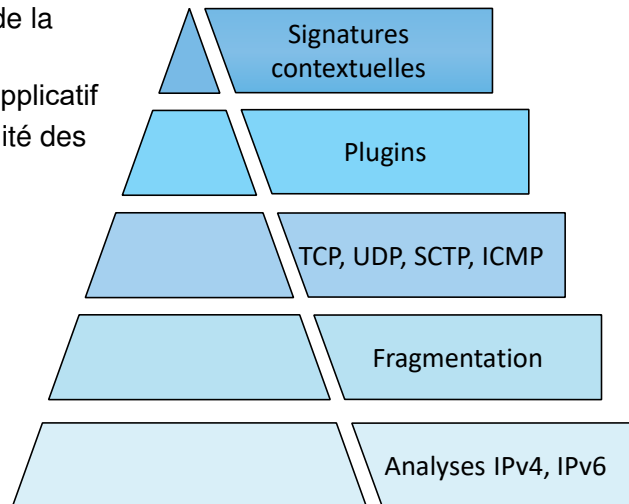


- Activation du mode Proxy
- Proxy HTTP
- Proxy HTTPS
- Analyse antivirus
- **Prévention d'intrusion et inspection de sécurité**
- Lab – Filtrage de contenu (HTTP et HTTPS)

## PRÉVENTION D'INTRUSION ET INSPECTION DE SÉCURITÉ

- Définition

- Analyses à partir de la couche IP
- Jusqu'au niveau applicatif
- Vérifier la conformité des protocoles



Les équipements Stormshield Network sont équipés nativement d'un module de prévention d'intrusion nommé ASQ (Active Security Qualification). Chaque paquet reçu par l'UTM sera soumis à un ensemble d'analyses à commencer par la vérification du protocole IP.

Le rôle principal de l'ASQ est de s'assurer de la conformité du paquet par rapport aux protocoles utilisés de la couche IP jusqu'à la couche applicative (grâce aux plugins) et aux signatures contextuelles (ou Patterns).

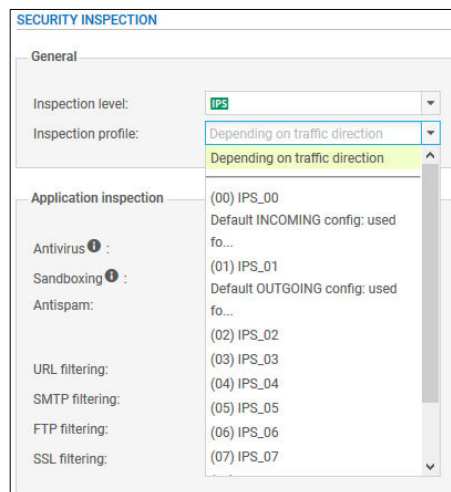
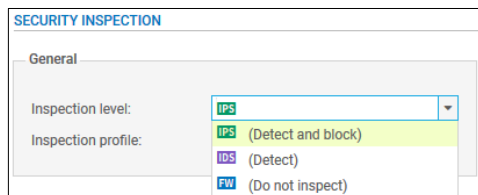
C'est également l'ASQ qui est en charge de filtrer les flux et d'appliquer une opération de NAT si nécessaire.

Le fonctionnement détaillé de l'ASQ ainsi que ses options sont abordés dans le cursus Expert.



## PRÉVENTION D'INTRUSION ET INSPECTION DE SÉCURITÉ

- Interactions avec le module de filtrage
  - Modes d'inspection
  - Profils d'inspection



Chaque paquet reçu par l'UTM est soumis à la politique de filtrage. Par défaut, l'analyse IPS est appliquée, ce qui signifie que le firewall est capable de détecter une anomalie et de bloquer le paquet correspondant.

D'autres modes d'inspection peuvent être utilisés, à des fins de tests ou par nécessité ; par exemple si on contacte un serveur ne respectant pas la RFC des protocoles qu'il gère.

Ces modes sont à sélectionner dans la colonne **Inspection de sécurité** de la règle de filtrage concernée.

- **IPS** : Détecter et bloquer (choix par défaut). L'ASQ va soumettre le paquet à l'ensemble des couches qu'il est capable d'analyser et le bloquer en cas d'anomalie.
- **IDS** : Détecter. L'ASQ effectue une analyse similaire à l'IPS sauf que le paquet est toujours autorisé. C'est un profil permettant de faire un audit rapide pour une règle de filtrage donnée.
- **Firewall** : Ne pas inspecter. L'ASQ ne va effectuer que très peu d'analyses sur le paquet reçu. Pour connaître la liste exhaustive des alarmes qui ne sont pas contournées par le mode Firewall, veuillez vous référer à l'article "*What are the alarms that are not bypassed by Firewall Mode?*" de la base de connaissances du support technique.



L'ASQ est composé de 10 configurations (également nommées profils IPS). Chacune de ces configuration peut être éditée en fonction des besoins de l'administrateur.

Par défaut, et comme indiqué dans le menu **CONFIGURATION ⇒ PROTECTION APPLICATIVE ⇒ Profils d'inspection**, les profils IPS\_00 et IPS\_01 sont appliqués respectivement aux connexions entrantes (paquet dont l'adresse IP source ne fait pas partie d'un réseau protégé) et aux connexions sortantes (paquet dont l'adresse IP source fait partie d'un réseau protégé).

Malgré cette configuration, il est possible, dans la grille de filtrage, de forcer l'utilisation d'un profil ASQ spécifique depuis la colonne **Inspection de sécurité**. Les profils sont ensuite administrables depuis les menus **Protocoles** et **Applications et protections sous CONFIGURATION ⇒ PROTECTION APPLICATIVE**.

## RECOMMANDATIONS



- Adapter les profils d'inspection au rôle de l'équipement
- Adapter les profils d'inspection en fonction du contexte
- Remonter à Stormshield les faux positifs

En fonction de l'utilisation de l'équipement, il peut être utile de désactiver certaines vérifications de l'IPS pour gagner des ressources de calcul. Par exemple, ne pas appliquer un filtrage IPS sur du HTTP si le trafic est ensuite redirigé vers un proxy filtrant.

Par défaut, l'IPS est actif sur toutes les règles de filtrage en mode de détection automatique du protocole. Afin de mieux inspecter les flux, il est recommandé de qualifier manuellement le type de protocole si le port utilisé n'est pas standard. L'IPS risquerait de ne pas détecter correctement l'application.

Si des flux sains déclenchent des alarmes, il sera sûrement nécessaire de modifier les paramètres de l'ASQ pour ne pas bloquer la production. Dans ce cas, les modifications doivent être faites au plus spécifique. De préférence dans un profil dédié qui sera appliqué sur les règles identifiant précisément le trafic concerné. N'hésitez pas à remonter au support technique ou à votre contact privilégié les cas de faux positif en configuration par défaut.

## RESSOURCES COMPLÉMENTAIRES SUR LES SITES STORMSHIELD



Pour aller plus loin, consultez la note technique du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Filtrer les connexions HTTPS

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Activation du mode Proxy
- Proxy HTTP
- Proxy HTTPS
- Analyse antivirus
- Prévention d'intrusion et inspection de sécurité
- ➔ **Lab – Filtrage de contenu (HTTP et HTTPS)**

STORMSHIELD

Protection applicative



## Lab 6 – Filtrage de contenu (HTTP et HTTPS)

Copiez la politique de filtrage/NAT **(5) Lab\_5** vers la politique numéro 6. Renommez la politique numéro 6 « Lab\_6 », puis activez cette politique.

1. Sélectionnez la base d'URL embarquée.
2. Trouvez les catégories dans lesquelles sont classées les URL [twitter.com](https://twitter.com), [www.netbsd.org](https://www.netbsd.org), [www.mozilla.org](https://www.mozilla.org), [neverssl.com](https://neverssl.com).
3. Configurez une politique de filtrage URL, et une politique de filtrage SSL, permettant l'accès à tous les sites Web sauf les sites listés au point 2, les sites des catégories « shopping » et « news ». Cependant, assurez-vous que le site [bbc.com](https://bbc.com) reste joignable.
4. Tentez d'accéder au site [cnn.com](https://cnn.com) et ensuite à [euronews.com](https://euronews.com). Pourquoi la page de rejet du trafic SSL ne s'affiche pas pour [cnn.com](https://cnn.com) ?



# Quiz

STORMSHIELD

Q1 – Les analyses pour le filtrage URL sont effectuées par le module IPS ASQ :

- A. Vrai
- B. Faux

Q2 – La base d'URL extended web control ne peut pas être utilisée sur les petits modèles de pare-feu car l'espace disque est insuffisant :

- A. Vrai
- B. Faux

Q3 – Les catégories personnalisées sont prioritaires sur les catégories intégrées dans le pare-feu :

- A. Seulement si la règle de filtrage est située avant.
- B. Toujours.
- C. Jamais, c'est l'inverse.

Q4 – Il n'est pas possible de filtrer les sites web utilisant HTTPS avec le proxy HTTP (filtrage URL) :

- A. Vrai
- B. Faux

Q5 – Le SNI est un champ dans le handshake TLS/SSL qui contient l'URL demandée par le client :

- A. Vrai
- B. Faux



Q6 – Quel flux le proxy SSL peut-il déchiffrer et analyser ?

- A. SSH
- B. HTTPS
- C. SFTP
- D. FTPS
- E. SMTPS



STORMSHIELD

# ANNEXE – PROTECTION APPLICATIVE

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.

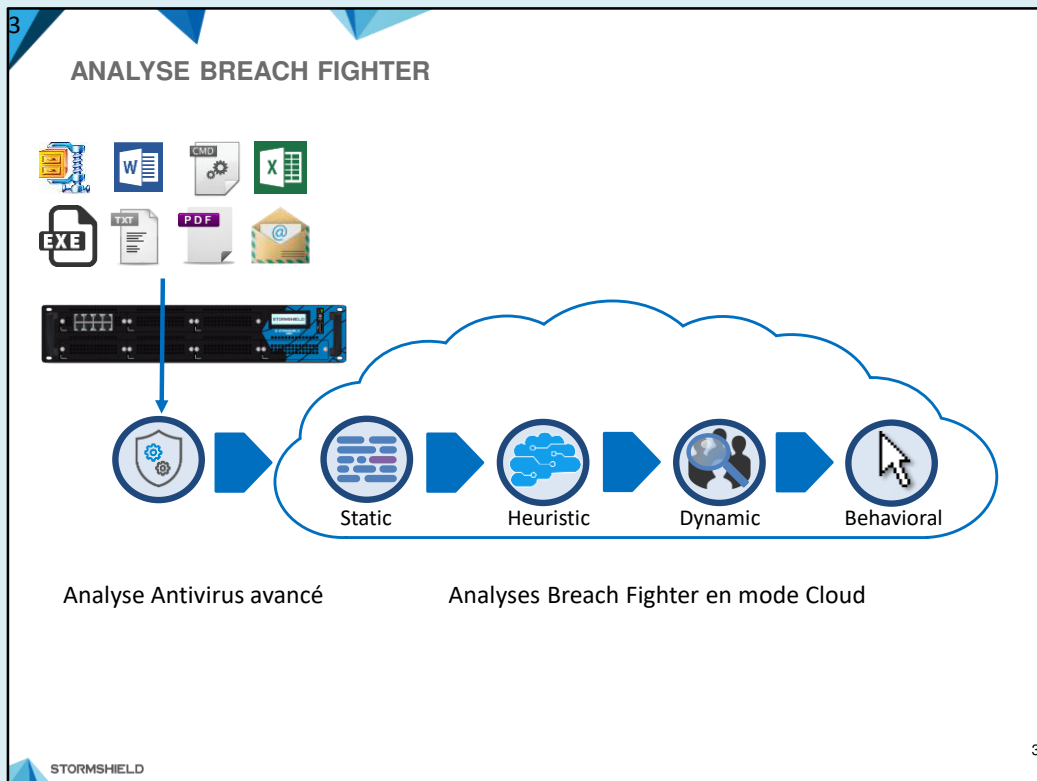


## Breach Fighter

- Filtrage SMTP et antispam
- Réputation des machines

STORMSHIELD

Protection applicative



Breach Fighter est disponible en tant qu'option logicielle supplémentaire après souscription du pack de sécurité contenant l'Antivirus avancé.

Cette option permet de répondre aux nouvelles menaces pour lesquelles une analyse antivirus et heuristique n'est plus suffisante (8 malwares sur 10 échappent aux antivirus classiques).

Les protocoles analysés par le moteur antivirus avancé (FTP, HTTP(s), SMTP(s), POP3(s)) sont pris en compte.

La solution est basée sur un Cloud Stormshield dédié et offre plusieurs niveaux d'analyse pour une protection optimale des systèmes d'exploitation Windows :

- **Analyse statique** : Le hash d'un fichier est comparé aux hashes existants dans la base partagée par la communauté pour que les menaces soient bloquées,
- **Analyse heuristique** : Les variantes d'un malware vont être détectées,
- **Analyse dynamique** : Des règles de détection et de protection contre les nouvelles menaces sont mises en œuvre par notre équipe dédiée de chercheurs en sécurité,
- **Analyse comportementale** : Le comportement des malwares est rejoué sur des environnements virtuels Windows pour simuler une utilisation réelle. L'environnement est nommé Sandbox et intègre les technologies de Stormshield Endpoint Security (SES) pour fournir une protection « Zero Day ».

Tout fichier passant par le boîtier est analysé par l'Antivirus avancé. Un fichier non bloqué par l'antivirus avancé va être soumis aux analyses complémentaires de Breach Fighter. Dès lors qu'un fichier infecté a été détecté, son hash est ajouté à la base partagée, permettant la protection immédiate de tous les clients.

L'équipe dédiée à la « Threat Intelligence » participe à l'optimisation continue des capacités de Breach Fighter.

4

## ANALYSE BREACH FIGHTER

APPLICATION PROTECTION / ANTIVIRUS

Antivirus engine: Advanced antivirus

Parameters

- Inspect archives (zip, arj, rha, rar, cab...)
- Block password-protected files
- Activate heuristic analysis

Sandboxing

Sandboxing threshold above which files will be blocked: Malicious

SECURITY POLICY / FILTER - NAT

(5) Trainee-A

Filtering NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_in	Internet	dns		Antivirus
2	on	pass	Network_in	Internet	http		Antivirus Sandboxing URL filter: URLFilter_02
3	on	pass	Network_in	Internet	ftp		Antivirus Sandboxing
4	on	pass	Network_in	Internet	pop3		Antivirus Sandboxing
5	on	pass	Internet	srv_mail_pub srv_mail_priv	smtp		Antivirus Sandboxing Antispam Mail filter: Incoming_emails

STORMSHIELD

4

L'analyse Breach Fighter peut être activée sur une règle de filtrage avec le paramètre **INSPECTION DE SÉCURITÉ ⇒ INSPECTION APPLICATIVE ⇒ SANDBOXING**. L'analyse antivirus s'active automatiquement avec l'activation de Breach Fighter.

Les fichiers soumis à une analyse sandboxing Breach Fighter se voient attribuer un score sur une échelle de 0 à 100. Un score nul qualifiant un fichier non dangereux.

La configuration de l'analyse sandboxing s'effectue depuis le menu **CONFIGURATION ⇒ PROTECTION APPLICATIVE ⇒ Antivirus**, dans le menu déroulant **Seuil d'analyse sandboxing à partir duquel les fichiers seront bloqués** :

- Mineur (score entre 1 et 30),
- Suspect (score entre 31 et 70),
- Potentiellement malveillant (score entre 71 et 99),
- Malveillant (score de 100).



- Analyse Breach Fighter
- ➔ **Filtrage SMTP et antispam**
- Réputation des machines

STORMSHIELD

Protection applicative

## FILTRAGE SMTP ET ANTISPAM

- Politique de filtrage SMTP

The screenshot displays two panels for configuring SMTP filtering policies. The top panel is for 'outgoing\_emails' and the bottom panel is for 'Incoming\_emails'. Both panels show a table of rules with columns for Status, Action, Sender, Recipient, and Comments.

**SECURITY POLICY / SMTP FILTERING (outgoing\_emails)**

Status	Action	Sender	Recipient (to, cc, cci)	Comments
1 <input checked="" type="checkbox"/> on	Pass	*@mydomain.com	*@*	only allow senders from my own domain

**SECURITY POLICY / SMTP FILTERING (Incoming\_emails)**

Status	Action	Sender	Recipient (to, cc, cci)	Comments
1 <input checked="" type="checkbox"/> on	Block	*@spammer.com	*@*	prohibit domain known as a source of spam
2 <input checked="" type="checkbox"/> on	Block	*@mydomain.com	*@*	prohibit spoofing of my own domain
3 <input checked="" type="checkbox"/> on	Pass	*@*	*@mydomain.com	only allow recipients of my own domain

STORMSHIELD

6

La configuration de la politique de filtrage SMTP s'effectue depuis le menu **CONFIGURATION** ⇒ **POLITIQUE DE SÉCURITÉ** ⇒ **Filtrage SMTP**.

Dix politiques sont disponibles. Les règles sont traitées dans l'ordre (de haut en bas).

## FILTRAGE SMTP ET ANTISPAM

- Connexions SMTP soumises au filtrage mail

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	incoming_emails	pass	Internet	Firewall_out	smtp		IPS Mail filter: incoming_emails
2	on	outgoing_emails	pass	srv_mail_priv	Internet	smtp		IPS Mail filter: outgoing_emails

EDITING RULE NO 2	
General	SECURITY INSPECTION
Action	General
Source	Inspection level: [IP]
Destination	Inspection profile: [Depending on traffic direction]
Port - Protocol	Application Inspection
Inspection	Antivirus: [OFF]
	Sandboxing: [OFF]
	Antispam: [OFF]
	URL filtering: [OFF]
	SMTP filtering: [outgoing_emails]
	FTP filtering: [OFF]
	SSL filtering: [OFF]

STORMSHIELD

7

La politique de filtrage SMTP est appliquée par l'édition de l'inspection applicative des règles de filtrage qui autorisent les flux SMTP entrants et sortants. Pour les flux mail entrants, il est tout à fait possible (même fortement conseillé) de combiner le filtrage mail à une analyse antispam.

## FILTRAGE SMTP ET ANTISPAM

- Connexions SMTP entrantes traduites (translation statique) soumises au filtrage mail :
  - La translation vers le serveur interne doit s'effectuer dans la règle de filtrage

The screenshot displays the Stormshield configuration interface for a filtering rule. The main table shows a rule named 'incoming\_emails' with status 'on', action 'pass', source 'Internet interface: out', and destination 'srv\_mail\_priv'. A blue box highlights the destination field, and an arrow points to the 'APPLICATION PROTECTION / PROTOCOLS' configuration window.

**Filtering Rule Configuration:**

Filtering	NAT							
1	on	incoming_emails	pass	Internet interface: out	srv_mail_pub → srv_mail_priv	smtp	IPS	Mail filter: Incoming_emails

**APPLICATION PROTECTION / PROTOCOLS Configuration:**

- Protocol: smtp\_00
- Filter domain name:  Enable server's domain name filtering
- Connection:  Keep original source IP address

STORMSHIELD

8

Pour les connexions SMTP traduites utilisant une adresse IP publique « IP\_PUBLIQUE\_SMTP » dédiée au serveur mail interne « IP\_PRIVÉE\_SMTP » (translation statique), l'activation du filtrage SMTP doit respecter certaines règles.

Pour les flux SMTP entrants, la translation vers le serveur SMTP interne doit s'effectuer dans la règle de filtrage qui autorise le flux (l'activation de la publication ARP est nécessaire pour ce type de translation).

Pour que le filtrage SMTP soit le plus transparent possible, les adresses IP sources originales des connexions entrantes sont conservées lorsque ces connexions sont renvoyées dans le réseau interne suite au filtrage SMTP. Ce comportement est possible grâce à l'option « conserver l'adresse IP source originale » qui est activée par défaut pour les flux entrants dans l'onglet « proxy » du protocole SMTP (profil entrant smtp\_00).

## FILTRAGE SMTP ET ANTISPAM

- Connexions SMTP sortantes translatées (translation statique) soumises au filtrage mail :

FILTERING		NAT							
Searching...									
+ New rule   X Delete   ↑ ↓   Cut Copy Paste   Search in logs   Search in monitoring									
	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection	
1	on	filter_outgoing_emails	pass	srv_mail_priv	Internet		smtp	IPS	Mail filter: outgoing_emails

FILTERING		NAT							
Searching...									
+ New rule   X Delete   ↑ ↓   Cut Copy Paste   Search in logs   Search in monitoring									
	Status	Name	Original traffic (before translation)			Traffic after translation			
			Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	nst_outgoing_emails	srv_mail_priv	Internet	Any	8080		srv_mail_pub	

APPLICATION PROTECTION / PROTOCOLS

Searching...

(1) smtp\_01 Edit [Go to global configuration](#)

- SMTP
- SNMP

IPS PROXY SMTP COMMANDS ANALYZING FILES

Edit Global configuration [Go to global configuration](#) [Go to profiles](#)

Proxy

Apply the NAT rule on scanned traffic

CANCEL APPLY

Pour le flux SMTP sortant (profil smtp\_01 à priori, mais la configuration globale s'applique sur tous les profils), l'option « appliquer la règle de NAT sur le trafic analysé » doit être activée via la configuration globale du protocole SMTP pour obliger les connexions sortantes du filtrage SMTP à parcourir les règles de NAT. Dans le cas contraire, les connexions SMTP ont comme adresse IP source l'adresse IP de l'interface du firewall par laquelle elles sortent.

## FILTRAGE SMTP ET ANTISPAM

## • Module antispam

APPLICATION PROTECTION / ANTISPAM

GENERAL WHITELISTED DOMAINS BLACKLISTED DOMAINS

Enable reputation-based analysis (DNS blacklists - RBL):  ON

Enable heuristic analysis:  ON

SMTP parameters

SMTP server domain name (FQDN):

Action:

Advanced properties

STORMSHIELD

10

La recherche de spams s'appuie sur deux technologies pour offrir la protection la plus efficace possible:

- L'analyse par réputation (liste noire DNS – RBL) qui consiste à vérifier une liste d'adresses IP de spammeurs et de relais qui ne combattent pas le spam.
- L'analyse heuristique qui s'appuie sur des algorithmes mathématiques. Ces algorithmes s'appliquent sur les mails pour détecter, par exemple, la répétition de caractères non désirés ou la présence de mots caractéristiques. Une fois les calculs terminés, un score est apposé au mail. En fonction de ce score, et des paramètres de l'analyse heuristique, le mail sera considéré comme spam ou légitime.

La configuration de ces deux technologies s'effectue depuis le menu **CONFIGURATION** ⇒ **PROTECTION APPLICATIVE** ⇒ **Antispam**.

## FILTRAGE SMTP ET ANTISPAM

- Module antispam

APPLICATION PROTECTION / ANTISPAM

GENERAL WHITELISTED DOMAINS BLACKLISTED DOMAINS

Advanced properties  Insert X-Spam headers

Reputation-based analysis

DNS BLACKLIST SERVER LIST (RBL)

Enabled	Name	Trust level	Domain name	Comments
<input checked="" type="checkbox"/>	SORBS	3 - High	dnwbl.sorbs.net	SORBS Main List
<input type="checkbox"/>	SPAMCOP	2 - Medium	bl.spamcop.net	SPAMCOP
<input type="checkbox"/>	SPAMHAUS3	1 - Low	bl.spamhaus.org	SpamHaus Combined (DBL+XBL) DNSBL List
<input checked="" type="checkbox"/>	SPAMHAUSBL	3 - High	bl.spamhaus.org	SpamHaus SBL DNSBL List
<input type="checkbox"/>	SPAMHAUSXBL	1 - Low	bl.spamhaus.org	SpamHaus XBL DNSBL List

Heuristic analysis

Advertisement

Detect advertising e-mails

Add advertisement tag to mail subjects (prefix): (ADS)

Spams

Add spam tag to subject fields (prefix): (SPAM \*)

Minimum score for spam definition [1-150]: 100

Scores associated with Level 1: from 100 to 200

Scores associated with Level 2: from 200 to 300

Scores associated with Level 3: from 300 upwards

STORMSHIELD

11

Les paramètres de l'analyse par réputation permettent de choisir le ou les serveurs RBL depuis lesquels les adresses IP des spammeurs et relais sont récupérées.

Les paramètres de l'analyse heuristique permettent quant à eux de:

- Choisir le préfixe à positionner pour les e-mails publicitaires,
- Choisir le préfixe à positionner pour les e-mails considérés comme SPAM,
- Définir le score minimal pour considérer un e-mail comme SPAM.

## FILTRAGE SMTP ET ANTISPAM

- Mise en œuvre de l'analyse antispam

	Status	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	incoming_emails	pass	Internet interface: out	srv_mail_pub srv_mail_priv		smtp	Antispam Mail filter: Incoming_emails

EDITING RULE NO 1

General

SECURITY INSPECTION

General

Inspection level: [On]

Inspection profile: [Depending on traffic direction]

Application inspection

Antivirus: [Off]

Antispam: [On]

URL filtering: [Off]

SMTP filtering: [incoming\_emails]

FTP filtering: [Off]

SSL filtering: [Off]

STORMSHIELD

12

L'analyse antispam peut s'appliquer sur des flux SMTP et POP3. Les flux SMTPS et POP3S, devront au préalable être déchiffrés par une règle d'inspection SSL.

L'exemple montre ici l'activation d'une analyse antispam pour un flux SMTP entrant.



- Analyse Breach Fighter
- Filtrage SMTP et antisпам
- ➔ **Réputation des machines**

STORMSHIELD

Protection applicative

## RÉPUTATION DES MACHINES

STORMSHIELD

14

Depuis la version 3 de SNS, une nouvelle fonctionnalité permet l'utilisation d'un critère de réputation des hôtes internes selon un score de réputation dans une règle de filtrage. Un hôte sain n'ayant jamais généré de trafic réseau a un score de réputation à zéro. La configuration de cette fonctionnalité s'effectue depuis le menu **CONFIGURATION** ⇒ **PROTECTION APPLICATIVE** ⇒ **Réputation des machines**.

Par défaut, le score d'un hôte est susceptible d'augmenter lorsqu'un flux le concernant entraîne :

- La levée d'une alarme,
- La détection d'une charge virale,
- La détection d'un malware par l'outil « Sandboxing Breach Fighter » :
  - Malicieux : l'hôte est infecté,
  - Suspicious : l'hôte a été connecté à des hôtes potentiellement infectés.

Les scores associés à ces risques sont modifiables en fonction de la configuration de votre réseau, selon les valeurs comprises entre crochets. Les scores des machines sont recalculés et pris en compte dans un intervalle de temps allant de 15 à 30 minutes (logd calcule toutes les 15 minutes et l'ASQ récupère les scores toutes les 15min auprès de logd).

En production, le score moyen d'un hôte n'est pas forcément synonyme de problèmes, des tests doivent être menés pour que les valeurs configurées soient cohérentes.

La façon dont le score de réputation va baisser n'est pas configurable par l'interface web d'administration, mais il est possible de réinitialiser le score de réputation de l'ensemble des hôtes supervisés.

Après correction des événements induisant la hausse de ce score, la baisse dépendra des éléments suivants :

- Lorsque le score d'un hôte est à 100, il sera divisé par deux après 6 heures, puis par quatre après 12 heures.
- Un risque sera ignoré s'il est plus ancien que 24 heures.

RÉPUTATION DES MACHINES

APPLICATION PROTECTION / HOST REPUTATION

CONFIGURATION HOSTS MONITORED

INCLUDED LIST

+ Add X Delete

Name

network\_internals

Advanced

EXCLUDED LIST

+ Add X Delete

Name

pentesting\_pc

X CANCEL ✓ APPLY

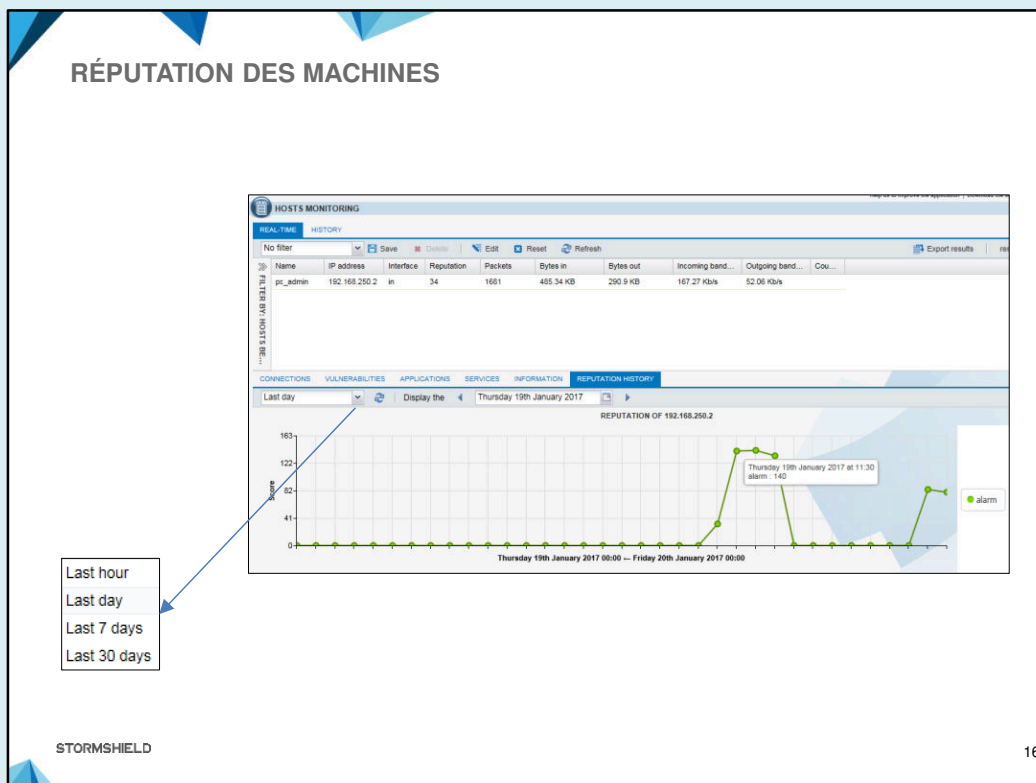
STORMSHIELD 15

L'onglet de configuration des hôtes devant être supervisés permet de choisir des machines ou des réseaux qui feront partie d'une liste d'inclusion ou d'une liste d'exclusion.

Les réseaux et les hôtes internes ne sont pas tous soumis aux mêmes menaces, il sera nécessaire de tester les différents comportements avant une mise en production.



## RÉPUTATION DES MACHINES



Le score de réputation associé à une machine peut être visualisé par le menu **SUPERVISION** ⇒ **Supervision des machines**.

Il faut obtenir le droit d'accès aux données personnelles pour pouvoir visualiser le graphe.

Il faut choisir la machine à superviser puis cliquer sur l'onglet **HISTORIQUE DES RÉPUTATIONS**.

Après avoir choisi la durée de temps voulue, déplacer la souris sur un point du graphe permet de connaître le score de réputation global associé à cette machine à un instant t, et les sous-scores de réputation par type de risque (alarme, antivirus, sandboxing).

### RÉPUTATION DES MACHINES

The screenshot displays the Stormshield management interface. At the top, the title is "RÉPUTATION DES MACHINES". Below it, a navigation bar shows "SECURITY POLICY / FILTER - NAT". A table lists filtering rules, with rule 1 selected. The rule details are shown in a modal window titled "EDITING RULE NO 1". The "SOURCE" tab is active, and the "GEOLOCATION / REPUTATION" sub-tab is selected. The "Host reputation" section is highlighted with a blue box, showing the "Enable filtering based on reputation score" checkbox checked and the "Reputation score" set to 100. A blue arrow points from the "Host reputation" text in the table to the "Host reputation" section in the modal.

Stages	Name	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	to_dmz_smtp	pass	Network_in Host reputation < 100	srv_mail_priv	smtp		IPS

EDITING RULE NO 1

General  
Action  
Source  
Destination  
Port - Protocol  
Inspection

SOURCE

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

Geolocation  
Select a region:

Public IP addresses reputation  
Select a reputation category:

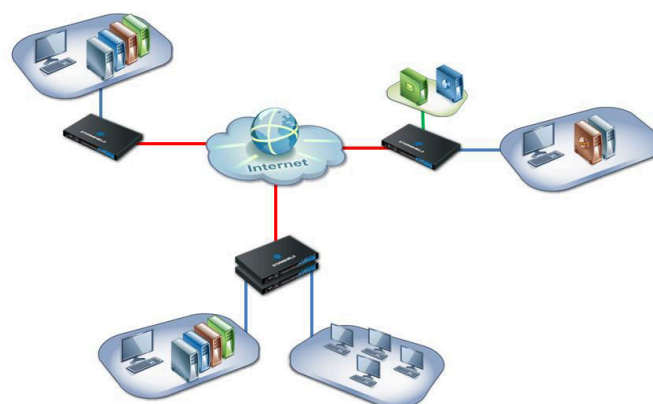
Host reputation  
 Enable filtering based on reputation score  
Reputation score: 100

CANCEL OK

L'ajout d'un critère de réputation des hôtes internes dans une règle de filtrage est possible en **source** ou en **destination** en fonction du sens du flux. Dans l'exemple ci-dessus, un hôte du réseau Network\_in pourra joindre un serveur SMTP via le Firewall, si et seulement si son score de réputation est inférieur à 20.



ADVANCED LAB - FILTRAGE APPLICATIF SMTP AVANCÉ



STORMSHIELD

18

Advanced Lab disponible à la fin du support de cours.



## Programme de la formation

- ✓ Coursus des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Les objets
- ✓ Configuration réseau
- ✓ Translation d'adresses
- ✓ Filtrage
- ✓ Protection applicative
- Utilisateurs & authentification
  - VPN
  - VPN SSL

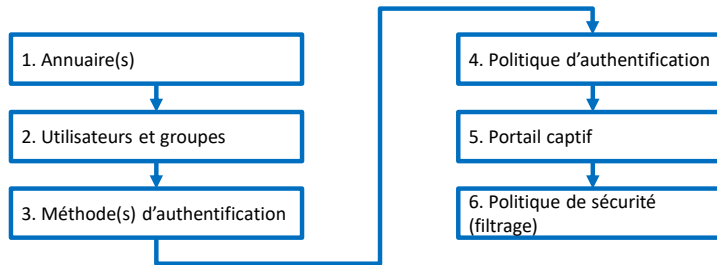


## Introduction

- Liaison à un annuaire
- Gestion des utilisateurs
- Les méthodes d'authentification
- La politique d'authentification
- Le portail captif
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification

## INTRODUCTION

- **Objectif :**  
Accorder aux utilisateurs des droits d'accès spécifiques aux réseaux et aux services (portail captif, VPN SSL, VPN IPsec, administration du firewall, etc.)
- **Les étapes de configuration sur un firewall Stormshield**



STORMSHIELD

3

### Étapes de mise en œuvre sur un firewall Stormshield

Le schéma ci-dessus illustre la logique de mise en œuvre de l'authentification. Les chapitres de ce cours détaillent les étapes dans l'ordre.

1. Les annuaires stockent des informations de manière hiérarchisée dans une arborescence. La norme LDAP permet l'organisation des données dans l'annuaire et fournit un protocole d'interrogation de l'annuaire (RFC 4510), la configuration sur un firewall consiste à établir un lien vers un ou plusieurs annuaires.
2. Les utilisateurs sont stockés dans un annuaire et décrits par des attributs (nom, prénom, identifiant, mot de passe, adresse e-mail, certificat, etc.) utilisés par le firewall pour l'authentification.
3. Les méthodes d'authentification utilisées permettent au firewall de configurer la façon de vérifier l'identité des utilisateurs.
4. La politique d'authentification permet d'accorder aux utilisateurs des droits d'accès aux réseaux et services gérés par le firewall.
5. Le portail captif peut avoir plusieurs usages : authentifier des utilisateurs pour accéder au réseau, enrôler de nouveaux utilisateurs, demander la création d'un certificat, télécharger le client VPN SSL et sa configuration, faire une demande de parrainage pour accéder au réseau, etc.
6. La politique de sécurité contient les règles de filtrage nécessaires pour que les utilisateurs inconnus soient redirigés vers la solution d'authentification retenue (par exemple, via le portail captif).

**NOTE :** En fonction de la méthode d'authentification retenue, certaines étapes de configuration seront facultatives.

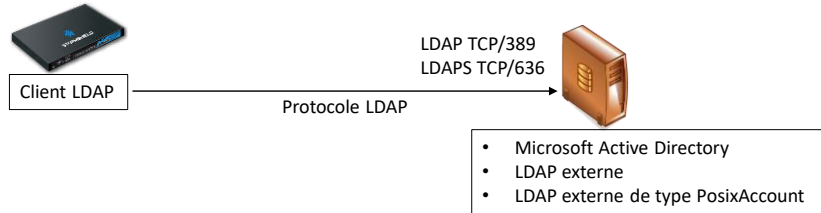


- Introduction
- **→ Liaison à un annuaire**
- Gestion des utilisateurs
- Les méthodes d'authentification
- La politique d'authentification
- Le portail captif
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification

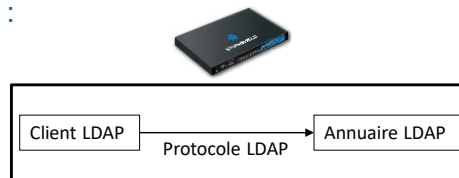
## LIAISON À UN ANNUAIRE

- 4 types d'annuaire LDAP/AD :

- Externes :



- Interne :



Les firewalls supportent quatre types d'annuaire qui peuvent être classés en deux catégories :

- **LDAP/AD externes** : L'annuaire est stocké sur un serveur externe. trois types d'annuaire sont supportés :
  - Microsoft Active Directory (AD),
  - LDAP standard,
  - LDAP de type PosixAccount.
- **LDAP interne** : L'annuaire LDAP est créé sur le firewall et héberge les utilisateurs.

Les firewalls peuvent supporter cinq annuaires simultanément : un LDAP interne et quatre LDAP/AD externes, ou cinq LDAP/AD externes. Ce qui signifie que les firewalls peuvent supporter en même temps cinq domaines différents.

**NOTE :**

- Un client LDAP intégré au firewall permet de se connecter à n'importe quel type d'annuaire (interne ou externe) en utilisant le protocole LDAP (ou LDAPS pour sécuriser les connexions avec les annuaires externes).
- Dans le cas d'un LDAP interne, l'annuaire et les utilisateurs sont automatiquement sauvegardés/restaurés avec la configuration du firewall.

## LIAISON À UN ANNUAIRE

- Ajout et configuration d'un annuaire

Annuaire par défaut

L'ajout et la configuration des annuaires s'effectuent depuis le menu : **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Configuration de l'annuaire**.

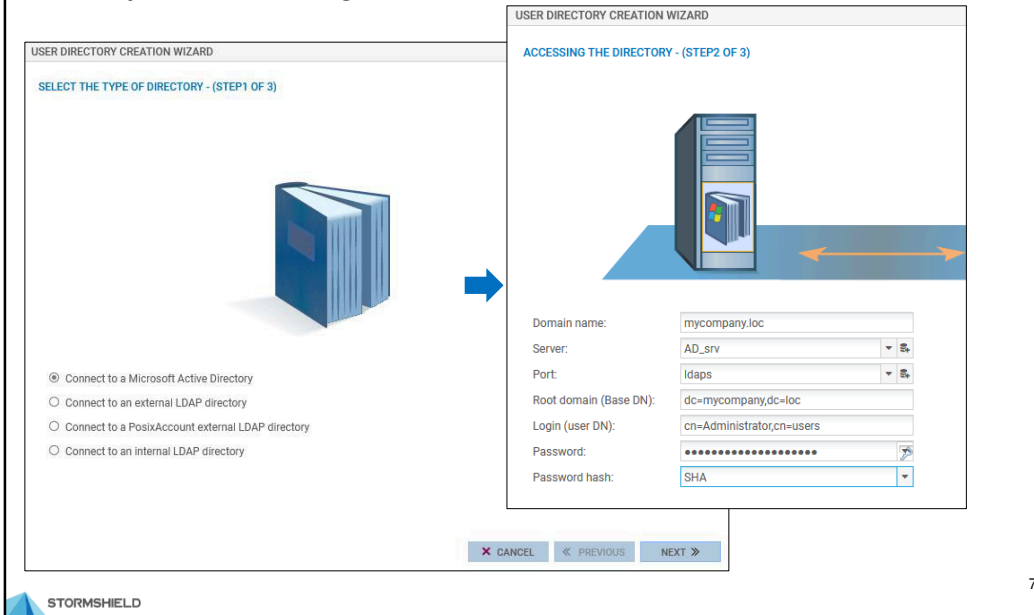
Pour lancer l'assistant d'ajout d'annuaire cliquez sur **Ajouter un annuaire**. Le bouton **Action** permet, quant à lui, d'accéder à plusieurs fonctionnalités :

- Supprimer un annuaire,
- Désigner un annuaire par défaut,
- Vérifier la connexion à l'annuaire,
- Vérifier l'utilisation de l'annuaire,
- Renommer un annuaire.

Le reste du menu liste tous les annuaires ajoutés, parmi lesquels l'annuaire par défaut s'affiche en vert. En cliquant sur un annuaire, ses paramètres s'affichent à droite de la page.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire externe



La configuration des annuaires externes (Microsoft Active Directory, LDAP et LDAP de type PosixAccount) est sensiblement identique. L'assistant de configuration vous demande d'abord de renseigner les paramètres du serveur à contacter :

- **Nom du domaine** : Le nom DNS du domaine,
- **Serveur** : L'objet machine qui porte l'adresse IP du serveur qui héberge l'annuaire,
- **Port** : Le port d'écoute de votre serveur LDAP. Les ports par défaut sont : 389/TCP pour une authentification en clair (ldaps) et 636/TCP pour une authentification en SSL (ldaps),
- **Domaine racine (Base DN)** : Le DN de la racine de votre annuaire (exemple : stormshield.eu ou dc=stormshield,dc=eu),
- **Identifiant (user DN) et le mot de passe** : Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires (exemple : cn=TrainingAdmin,ou=Training).
- **Haché du mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire externe

USER DIRECTORY CREATION WIZARD  
AUTHENTICATION - (STEP 3 OF 3)

Enable authentication profile 0 (internal) on the selected interface:

Select an interface

[ethernet]  
out  
in  
dmz1  
dmz2  
[ipsec]  
ipsec

CONFIGURED DIRECTORIES (MAXIMUM 5)  
+ Add a directory Action  
Domain name  
mycompany.loc

CANCEL PREVIOUS FINISH

STORMSHIELD 8

Par la suite, l'assistant vous propose d'activer le profil d'authentification 0 (internal) sur une interface, dans le cas où le profil n'a pas déjà été activé. Si c'est le cas, cette étape ne s'affiche pas.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire externe

The screenshot displays the Stormshield configuration interface for connecting to an external directory. It is divided into two main sections: CONFIGURATION and STRUCTURE.

**CONFIGURATION:**

- Remote directory:** Includes fields for Server (AD\_srv), Port (ldap), Root domain (Base DN) (dc=mycompany,dc=local), ID (cn=admin,dc=mycompany), and Password.
- Secure connection (SSL):** Includes checkboxes for Enable SSL access, Check the certificate against a Certificate Authority, and Select a trusted Certificate Authority.
- Advanced properties:** Includes Backup server, Use the firewall account to check user authentication on the directory, Do not add the Domain Name (Base DN) to the identifier (ID), and Allow nested groups.

**STRUCTURE:**

- Read-only access:** Includes User selection filter: (&(objectclass=user)!((objectclass=computer))) and User group selection filter: (objectclass=group). A checkbox indicates if the directory is accessed in read-only mode.
- Mapped attributes:** A table mapping Stormshield attributes to External directory attributes. The 'uid' attribute is mapped to 'sAMAccountName'.
- Advanced properties:** Includes Password hash (SSHA), User branch, Group branch, and Certification authority branch (cn=fwca,ou=cas).

Les paramètres d'un annuaire externe sont organisés en deux onglets :

- **CONFIGURATION** : Contient 3 encadrés :
  - **Annuaire distant** : Regroupe les paramètres de connexion à l'annuaire (l'adresse IP du serveur, le numéro de port, le base DN, l'identifiant, etc.).
  - **Connexion sécurisée (SSL)** : Permet d'activer une connexion sécurisée avec l'annuaire en spécifiant l'autorité de certification dont doit être issu le certificat présenté par le serveur d'annuaire.
  - **Configuration avancée** : Permet de définir un serveur de secours, de spécifier l'identifiant (firewall ou utilisateur) utilisé pour se connecter à l'annuaire et d'ajouter ou non le base DN lors de la connexion. Il permet également d'autoriser les groupes imbriqués (un groupe d'utilisateurs contenant d'autres groupes).
- **STRUCTURE** : Contient également 3 encadrés :
  - **Accès en lecture** : Permet de définir les filtres pour la sélection des utilisateurs et des groupes dans l'annuaire. Ces filtres dépendent du type d'annuaire et ils sont préconfigurés en conséquence. L'encadré permet également d'indiquer si l'annuaire est accessible en lecture seule ou lecture/écriture. **NOTE** : Même si un annuaire de type Microsoft Active Directory est en accès lecture/écriture, l'ajout ou la suppression d'utilisateurs à partir du firewall reste impossible. En revanche, la publication de certificats pour les utilisateurs de l'AD reste possible.



- **Correspondance d'attributs** : Permet d'indiquer la correspondance entre les attributs utilisés par le firewall et ceux utilisés par l'annuaire externe. Par exemple, avec un annuaire de type Microsoft Active Directory, l'attribut Stormshield *uid* a comme équivalent Active Directory *sAMAccountName*. Des modèles peuvent être appliqués en fonction du type de l'annuaire.
- **Configuration avancée** :
  - **Hachage de mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.
  - **Branche 'utilisateurs'** et **Branche 'groupes'** : À utiliser dans le cas d'un LDAP externe accessible en lecture/écriture. Il permet de renseigner les branches où seront enregistrés les utilisateurs et groupes créés à partir du firewall. Par exemple ou=users pour la branche utilisateurs.
  - **Branche de l'autorité de certification** : Permet de définir l'emplacement de l'autorité de certification présente dans l'annuaire externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisée pour la méthode d'authentification SSL.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire interne

The image shows two screenshots of the 'USER DIRECTORY CREATION WIZARD' interface, connected by a blue arrow pointing from left to right.

**Left Screenshot: SELECT THE TYPE OF DIRECTORY - (STEP 1 OF 3)**

This screen displays a book icon representing a directory. Below it, there are four radio button options:

- Connect to a Microsoft Active Directory
- Connect to an external LDAP directory
- Connect to a PosixAccount external LDAP directory
- Connect to an internal LDAP directory

At the bottom, there are three buttons: 'CANCEL', 'PREVIOUS', and 'NEXT'.

**Right Screenshot: ACCESSING THE DIRECTORY - (STEP 2 OF 3)**

This screen shows a server rack icon with an orange arrow pointing to a book icon, indicating the connection to the directory. Below the icon, there are several input fields:

- Organization: a-team
- Domain: com
- Password: [masked with dots]
- Confirm: [masked with dots]
- Below the confirm field is a blue button labeled 'Excellent'.
- Password hash: SSHA256 (dropdown menu)

STORMSHIELD

11

La configuration d'un annuaire interne nécessite le renseignement des informations suivantes :

- **Organisation** : Le nom de l'organisation. Par exemple, Stormshield,
- **Domaine** : Le TLD (Top Level Domain) du domaine. Par exemple, pour le domaine « Stormshield.eu », le TLD est « eu »,
- **Mot de passe** : Un mot de passe permettant de se connecter à l'annuaire LDAP depuis un navigateur LDAP.
- **Haché du mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire interne

12

L'étape suivante permet de configurer des paramètres complémentaires :

- **Activer le profil d'authentification 0 (internal) sur une interface** : Dans le cas où le profil n'a pas déjà été activé. Si c'est le cas, cette option sera désactivée (grisée) et un message indique que l'association entre profil d'authentification et interface est déjà réalisée.
- **Activer l' enrôlement des utilisateurs via le profil 0 (interne) du portail Web** : Active le service d'enrôlement sur le profil 0 (interne) permettant aux utilisateurs de remplir un formulaire de création de compte qui sera soumis à l'approbation de l'administrateur.
- **Autoriser l'accès à la base LDAP**: Donne la possibilité d'exposer le service LDAP sur le réseau et d'y accéder depuis un client LDAP. Si cet accès n'est pas nécessaire, il est vivement conseillé de ne pas activer cette option.

## LIAISON À UN ANNUAIRE

- Ajouter et configurer un annuaire interne

Une fois la configuration terminée, il est possible de modifier certains paramètres du LDAP interne :

- **Activer l'utilisation de l'annuaire utilisateur** : Cette option permet de démarrer le service LDAP,
- **Mot de passe** : Le mot de passe permettant de se connecter à l'annuaire, il est possible de le modifier,
- **Activer l'accès non chiffré (PLAIN)** : Active l'accès non chiffré à l'annuaire,
- **Activer l'accès SSL** : Active l'accès sécurisé à l'annuaire, il faut alors renseigner le champ **certificat SSL présenté par le serveur**,
- **Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire** : Si cette option n'est pas cochée, l'authentification s'effectue avec le compte de l'utilisateur. Le compte disposant de tous les droits sur l'annuaire est *cn=NetasqAdmin*.



- Introduction
- Liaison à un annuaire
- **Gestion des utilisateurs**
- Les méthodes d'authentification
- La politique d'authentification
- Le portail captif
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification

**GESTION DES UTILISATEURS**

USERS / USERS AND GROUPS

Searching... Filter any + Add user + Add group X Delete Check usage

user1@a-team.com  
 John Smith  
 user2@a-team.com  
 chief@a-team.com  
 simple\_users@a-team.com

jsmith (Smith John)

ACCOUNT CERTIFICATE MEMBER OF THESE GROUPS

Create or update password Access privileges

ID (login): jsmith  
 Last name: Smith  
 First name: John  
 E-mail address: jsmith@a-team.com  
 Phone number:  
 Description:

Group simple\_users

Group name: simple\_users  
 Description: Group description

Filter... + Add X Delete

user2@a-team.com  
 user1@a-team.com

STORMSHIELD 15

Les utilisateurs et les groupes, de tous les annuaires configurés, peuvent être visualisés depuis le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Utilisateurs**.

Le menu est composé de 3 parties :

- La barre du menu qui offre les fonctionnalités suivantes :
  - Barre de recherche,
  - Filtrer l'affichage en se basant sur le type : groupes ou utilisateurs,
  - Filtrer l'affichage en se basant sur l'annuaire (s'affiche seulement si plusieurs annuaires sont configurés),
  - Ajouter un utilisateur,
  - Ajouter un groupe,
  - Supprimer un utilisateur ou un groupe,
  - Vérifier l'utilisation d'un utilisateur ou d'un groupe.
- **CN** : la liste des utilisateurs et des groupes de tous les annuaires. Pour distinguer les annuaires, un suffixe est ajouté aux utilisateurs et aux groupes pour indiquer le nom de l'annuaire (et non pas le nom du domaine). Par exemple : [user6@institute.com](#)
- Paramètres d'un groupe ou d'un utilisateur : ils apparaissent à droite de la page. Les paramètres d'un utilisateur sont organisés en 3 onglets : les informations de l'utilisateur (**COMPTE**), son certificat (**CERTIFICAT**) et les groupes auxquels il appartient (**MEMBRE DES GROUPES**).

Le lien **Droits d'accès** renvoie vers le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Droits d'accès ⇒ onglet ACCÈS DÉTAILLÉ** pour accorder des droits à l'utilisateur.



**NOTE** : Lors de l'accès à ce menu, la liste des utilisateurs et groupes est toujours vide, c'est un comportement normal. En effet, si vous êtes connecté à un annuaire contenant un grand nombre d'utilisateurs et de groupes, l'affichage sans filtre dans le champ **Recherche** peut avoir un impact sur les performances de l'interface graphique.

Pour voir les utilisateurs ou les groupes :

- Vous pouvez cliquer sur l'un des filtres (utilisateurs ou groupes),
- Vous pouvez ouvrir le menu des préférences du firewall accessible en cliquant sur l'icône représentant des outils dans l'en-tête de l'interface Web, et cocher la case « Afficher les utilisateurs dès le démarrage du module ».

**GESTION DES UTILISATEURS**

- **Création d'un utilisateur**

USERS / USERS AND GROUPS

Searching... All any + Add user + Add group X Delete Check usage

CN

No matching user or group

To create a user, enter at least its ID and name. To assign a certificate to the user, you will need to indicate a valid e-mail address.

ACCOUNT CERTIFICATE MEMBER OF THESE GROUPS

Create or update password

ID (login): jsmith

Last name: Smith

First name: John

E-mail address: jsmith@a-team.com

Phone number:

Description: Hannibal

AUTHENTICATION PASSWORD

Please enter a password:

Confirm password:

X CANCEL X CANCEL ✓ APPLY ✓ OK

17

STORMSHIELD

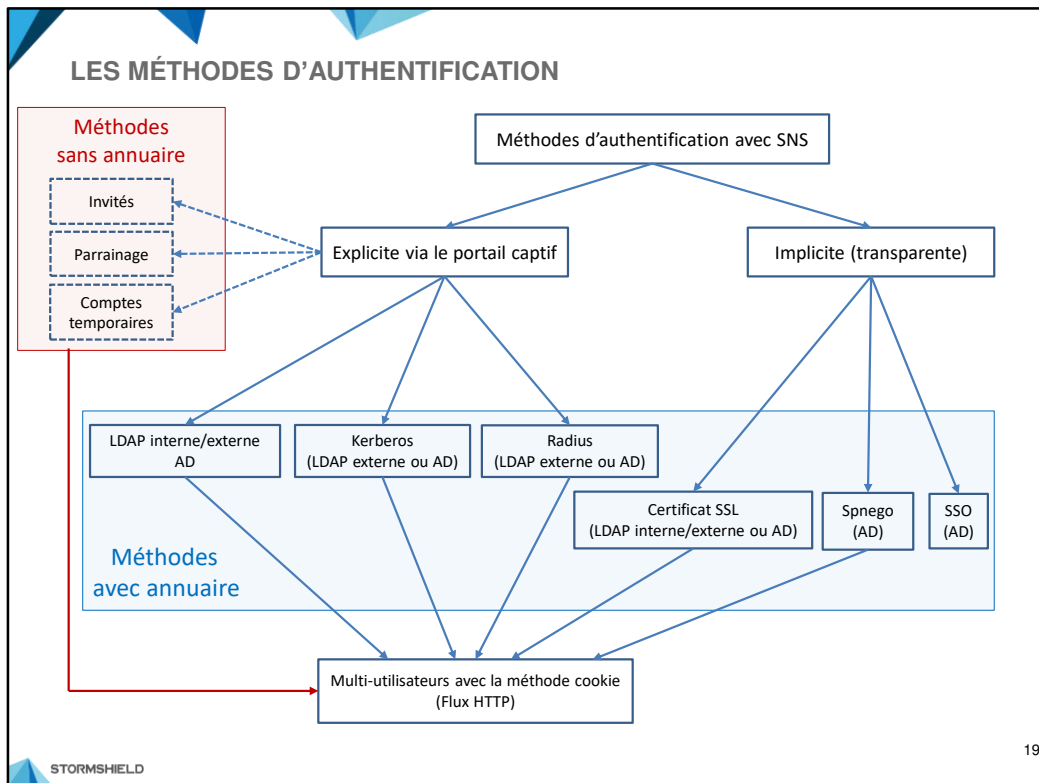
Avec un LDAP interne (ou un LDAP externe accessible en lecture/écriture), il est possible d'ajouter ou de supprimer des utilisateurs et des groupes depuis le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Utilisateurs**.

**NOTE :**

- La création d'utilisateurs et de groupes s'effectue dans l'annuaire désigné par défaut dans le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Configuration de l'annuaire**,
- La création d'utilisateurs est impossible dès qu'une correspondance d'attributs existe entre le firewall et la base LDAP externe (voir la diapositive numéro 9).



- Introduction
- Liaison à un annuaire
- Gestion des utilisateurs
- ➔ **Les méthodes d'authentification**
- La politique d'authentification
- Le portail captif
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification



Les firewalls SNS implémentent plusieurs méthodes d'authentification qui peuvent être classées en deux catégories :

- **Les méthodes explicites via le portail captif** : l'utilisateur est redirigé vers le portail captif pour saisir un identifiant/mot de passe. Ces derniers sont récupérés par le firewall pour vérifier l'identité de l'utilisateur en fonction de la méthode utilisée :
  - **LDAP** : L'identité de l'utilisateur est vérifiée sur un annuaire interne ou externe (LDAP/AD),
  - **RADIUS** : L'identité de l'utilisateur est vérifiée par un serveur Radius externe qui reçoit l'identifiant/mot de passe de l'utilisateur,
  - **KERBEROS** : L'identité de l'utilisateur est vérifiée par un serveur Kerberos externe qui reçoit l'identifiant/mot de passe de l'utilisateur,

Trois autres méthodes d'authentification explicites peuvent être utilisées pour des besoins spécifiques :

- **Comptes temporaires** : Permet à des utilisateurs temporaires de s'authentifier via le portail captif en utilisant un identifiant/mot de passe fournis par l'administrateur,

Les utilisateurs temporaires sont ajoutés par l'administrateur depuis le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Comptes temporaires**, leur mots de passe est généré automatiquement et la validité des comptes peut être limitée dans le temps. Ainsi, l'administrateur n'est pas obligé d'ajouter ces utilisateurs dans l'annuaire (interne ou externe) pour qu'ils puissent s'authentifier.

- **Parrainage** : Permet à un utilisateur identifié par son nom et prénom d'accéder au réseau grâce au parrainage d'un utilisateur local ayant les droits pour cela. L'utilisateur est invité d'abord, depuis le portail captif, à saisir son nom, prénom et l'adresse e-mail du parrain. Ce dernier reçoit alors un e-mail contenant un lien pour valider cette requête. Suite à la validation, le parrainé est automatiquement redirigé du portail captif vers la page Web demandée.
- **Invités** : Permet à un utilisateur d'accéder au réseau après validation des conditions générales d'utilisation sur le portail d'authentification. Cette méthode est généralement utilisée dans des lieux publics tels que les hôtels, les gares ou les hot-spot publics.
- **Les méthodes implicites ou transparentes** : l'authentification est transparente vis-à-vis de l'utilisateur qui n'a pas besoin de renseigner son identité explicitement pour accéder au réseau.
  - **Certificat SSL** : L'utilisateur est authentifié automatiquement au moyen d'un certificat installé sur sa machine (dans son navigateur par exemple),
  - **Authentification transparente (SPNEGO)** : Si l'utilisateur est authentifié sur un domaine Active Directory, il est automatiquement authentifié sur le firewall suite à la connexion à un site en HTTP,
  - **Agent SSO (Single Sign-On)** : Si l'utilisateur est déjà authentifié sur un domaine Active Directory, il est également automatiquement authentifié sur le firewall.

**NOTE :**

- Le « multi-utilisateurs » avec la méthode cookie permet à plusieurs utilisateurs de s'authentifier depuis la même adresse IP. Étant donné que les utilisateurs sont distingués par des cookies dans les requêtes HTTP, cette option fonctionne donc uniquement pour les flux HTTP (ou HTTPS déchiffrés) passant dans le proxy HTTP. Elle est disponible avec toutes les méthodes d'authentification à l'exception de l'agent SSO.
- Les méthodes d'authentification implicites sont détaillées dans la formation Expert CSNE.

### LES MÉTHODES D'AUTHENTIFICATION

The screenshot shows the 'USERS / AUTHENTICATION' configuration page. The 'AVAILABLE METHODS' tab is selected, showing a list of authentication methods. The 'LDAP' method is highlighted in green. A blue arrow points from the 'Add a method' button to a dropdown menu that lists various authentication methods, including LDAP, SSL certificate, RADIUS, Kerberos, and others.

**USERS / AUTHENTICATION**

AVAILABLE METHODS    AUTHENTICATION POLICY    CAPTIVE PORTAL    CAPTIVE PORTAL PROFILES

+ Add a method    X Delete

Method

LDAP    Automatic (see "Directory configuration")

Guest method

Sponsorship method

SSL

RADIUS

Kerberos

Transparent authentication (SPNEGO)

SSO Agent

Temporary accounts

SSO agent 2

LDAP

SSL certificate

RADIUS

Kerberos

Transparent authentication (SPNEGO)

SSO Agent

Guest method

Temporary accounts

Sponsorship method

STORMSHIELD

21

Les méthodes d'authentification utilisées par le firewall peuvent être ajoutées depuis le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Authentification** ⇒ onglet **MÉTHODES DISPONIBLES**. Chaque méthode nécessite de renseigner des paramètres spécifiques.

Suite à la configuration d'un annuaire LDAP pour ce qui concerne l'exemple ci-dessus la méthode d'authentification LDAP est renseignée automatiquement.



- Introduction
- Liaison à un annuaire
- Gestion des utilisateurs
- Les méthodes d'authentification
- ➔ **La politique d'authentification**
- Le portail captif
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification

STORMSHIELD

Utilisateurs & authentification

## LA POLITIQUE D'AUTHENTIFICATION

The screenshot displays the 'USERS / AUTHENTICATION' configuration page. It features a table of authentication rules with columns for Status, Source, and Methods. Rule 9 is highlighted, showing it is enabled for the source 'simple\_users@a-team.com' on the 'net\_secret' network. The methods for rule 9 are SSO Agent, SSL, and LDAP. A dropdown menu is open for the 'Method to use if no rules match' field, showing 'LDAP' selected. The dropdown menu also lists other methods: Block, LDAP, Guest method, Temporary accounts, Sponsorship method, SSL, RADIUS, Kerberos, and Transparent authentication (SPNEGO).

Puisque les firewalls SNS supportent plusieurs annuaires et plusieurs méthodes d'authentification simultanément, il est nécessaire de définir une politique d'authentification pour indiquer la ou les méthodes à appliquer en fonction de deux critères : l'utilisateur ou le groupe d'utilisateurs, et l'adresse IP source ou l'interface d'entrée.

La politique d'authentification est définie dans le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Authentification** ⇒ onglet **POLITIQUE D'AUTHENTIFICATION**. Elle peut être constituée de plusieurs règles appliquées en fonction de leur ordre.

Plusieurs méthodes d'authentification peuvent être utilisées par une seule règle. Dans ce cas, les méthodes sont appliquées suivant l'ordre d'apparition dans la règle. Si une méthode permet d'authentifier l'utilisateur, les méthodes suivantes ne seront pas testées. Par exemple, dans la règle 9, tous les membres du groupe « chief » du domaine « a-team.com » qui se connectent depuis le réseau « net\_secret » doivent, en premier lieu, s'authentifier via la méthode Agent SSO. Si l'authentification échoue, alors on propose à l'utilisateur de sélectionner son certificat. Enfin, si cette seconde méthode n'aboutit pas (pas de certificat pour cet utilisateur par exemple), il est convié à renseigner un couple d'identifiant/mot de passe pour une authentification via la méthode LDAP.

Dans le cas où aucune règle ne correspond aux critères du trafic, la méthode d'authentification par défaut est appliquée.

**NOTE** : lorsqu'elle est utilisée dans une règle, la méthode Agent SSO est automatiquement la plus prioritaire des méthodes parce que cette dernière authentifie l'utilisateur sur le firewall dès son authentification sur le domaine Active Directory.

**LA POLITIQUE D'AUTHENTIFICATION**

- Créer une politique d'authentification

STORMSHIELD

24

Pour ajouter une règle d'authentification, il faut cliquer sur le bouton **Nouvelle règle** ⇒ **Règle Standard**. La création de la règle s'effectue via un assistant en 3 étapes :

- Renseigner les utilisateurs ou les groupes,**
- Renseigner les réseaux ou les interfaces sources.** Dans le cas de la création d'un premier annuaire, le rattachement du profil d'authentification 0 (internal) à une interface est proposé lors de la création de l'annuaire. Sinon le rattachement peut s'effectuer dans le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Authentification** ⇒ **PORTAIL CAPTIF**, en ajoutant une entrée dans la liste **CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE**.

Dans l'entrée, il faut sélectionner l'interface et le profil. La méthode ou l'annuaire par défaut sont renseignés automatiquement en fonction de ce qui est configuré sur le profil sélectionné.

- Choisir les méthodes d'authentification à utiliser** (kerberos, Radius, SSL, SPNEGO, Agent SSO, méthode par défaut et interdire).

Pour les autres méthodes : invités, comptes temporaires et parrainage, l'ajout s'effectue respectivement avec les boutons : **Nouvelle règle** ⇒ **Règle invités**, **Règle comptes temporaires** et **règle Parrainage**.

## LA POLITIQUE D'AUTHENTIFICATION

- Exemple d'une politique d'authentification LDAP

The screenshot displays the 'USERS / AUTHENTICATION' configuration page. It features a navigation bar with tabs for 'AVAILABLE METHODS', 'AUTHENTICATION POLICY', 'CAPTIVE PORTAL', and 'CAPTIVE PORTAL PROFILES'. Below the navigation bar is a search field and a toolbar with actions like '+ New rule', 'X Delete', 'Up', 'Down', 'Cut', 'Copy', and 'Paste'. A table lists the authentication rules:

	Status	Source	Methods (assess by order)
1	Enabled	Any user@a-team.com   Network_internals	LDAP

Below the table, the 'Default method' section is visible, showing a dropdown menu set to 'LDAP' with the label 'Method to use if no rules match:'.

Dans la politique d'authentification, vous pouvez créer une politique pour déterminer les réseaux et les utilisateurs qui utiliseront la méthode LDAP, ou la définir comme la méthode par défaut.



- Introduction
- Liaison à un annuaire
- Gestion des utilisateurs
- Les méthodes d'authentification
- La politique d'authentification



### **Le portail captif**

- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs
- Lab - Authentification

**LE PORTAIL CAPTIF**

- URL du portail : `https://(@IP_firewall | FQDN_firewall)/auth`

STORMSHIELD Network Security

Please enter your authentication password

Username:

Password:

Authentication duration:

STORMSHIELD Network Security

Welcome jsmith. Logout in 04:00

Authentication successful

You have logged in

[» Click here if you are not automatically redirected](#)

STORMSHIELD

27

Le portail captif, ou portail d'authentification, est une page web embarquée sur le firewall et accessible via une connexion sécurisée (HTTPS depuis ses adresses IP (il peut être activé sur toutes les interfaces du firewall)).

Les usages du portail captif sont les suivants : authentifier des utilisateurs pour accéder au réseau, enrôler de nouveaux utilisateurs, créer et télécharger un certificat, télécharger le client VPN SSL et sa configuration, faire une demande de parrainage pour accéder au réseau, etc.

Les utilisateurs peuvent se connecter sur le portail en utilisant leur identifiant/mot de passe d'annuaire. Dans le cas où plusieurs annuaires sont configurés au niveau du firewall, les utilisateurs peuvent ajouter à l'identifiant le nom du domaine auquel ils appartiennent, par exemple, j.doe@company-a.com. Si le nom du domaine n'est pas précisé, l'authentification s'effectuera avec la méthode ou avec l'annuaire défini par défaut au niveau du profil d'authentification.

### LE PORTAIL CAPTIF

USERS / AUTHENTICATION

AVAILABLE METHODS    AUTHENTICATION POLICY    **CAPTIVE PORTAL**    CAPTIVE PORTAL PROFILES

Captive portal

**AUTHENTICATION PROFILE AND INTERFACE MATCH**

+ Add    X Delete

Interface	Profile	Default method or directory
in	Internal	Directory (none)
dmz1	Internal	Directory (none)

SSL server

Certificate (private key):  X

STORMSHIELD 28

La configuration du portail captif s'effectue depuis le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Authentification** ⇒ onglet **PORTAIL CAPTIF**. L'onglet est constitué de plusieurs encadrés :

- **CORRESPONDANCE ENTRE PROFIL D'AUTHEMIFICATION ET INTERFACE** : Il existe 10 profils différents pour le portail captif qui sont nommés profils d'authentification. Pour activer le portail sur une interface, il suffit d'ajouter une ligne dans cet encadré, sur laquelle il faut sélectionner une interface et un profil d'authentification. Un seul profil peut être sélectionné par interface.
- **SSL Server** : Permet de modifier le certificat présenté par le portail captif.

## LE PORTAL CAPTIF

- **Condition d'utilisation de l'accès à Internet** : Permet d'ajouter une charte d'utilisation de l'accès réseau qui doit être acceptée par l'utilisateur une fois authentifié. Elle peut être téléchargée en format PDF ou en format HTML. Le bouton **Réinitialiser la personnalisation des conditions d'utilisation de l'accès à Internet** permet de supprimer une charte préalablement téléchargée.
- **Configuration avancée** :
  - Interrompre les connexions lorsque l'authentification expire,
  - Fichier de configuration du proxy (.pac),
  - Portail captif : Permet de modifier le port du portail captif, et son apparence : masquer le logo Stormshield sur le portail, télécharger un nouveau logo et modifier la feuille de style.

**LE PORTAIL CAPTIF**

USERS / AUTHENTICATION

AVAILABLE METHODS   AUTHENTICATION POLICY   CAPTIVE PORTAL   **CAPTIVE PORTAL PROFILES**

Internal   Rename   ⓘ

Authentication

Default method or directory: Directory (a-team.com)    Enable sponsorship

Conditions of use for Internet access

Enable the display of the conditions of use for Internet access

Display frequency of the Conditions: 18 hours 0 minutes

Customized fields on the captive portal (Guest method only)

Field no. 1: Empty

Field no. 2: Empty

Field no. 3: Empty

Internal  
External  
Guest  
Voucher  
Sponsor  
default05  
default06  
default07  
default08  
default09

STORMSHIELD

30

Les profils d'authentification peuvent être configurés dans le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Authentification** ⇒ **onglet PROFILS DU PORTAIL CAPTIF**. La liste déroulante permet de sélectionner le profil que vous souhaitez modifier. Il existe 10 profils différents, les cinq premiers sont préconfigurés :

- **internal, external** : Ils possèdent la même configuration. Le premier est destiné à être attaché aux interfaces internes et le deuxième aux interfaces externes en utilisant n'importe quelle méthode d'authentification utilisant le portail captif,
- **Guest** : Préconfiguré pour la méthode d'authentification invité,
- **Voucher** : Préconfiguré pour la méthode d'authentification des comptes temporaires,
- **Sponsor** : Préconfiguré pour la méthode d'authentification par parrainage.

## LE PORTAIL CAPTIF

Il faut configurer la méthode ou l'annuaire par défaut utilisé par le profil sélectionné dans l'étape précédente. Dans le cas d'une authentification LDAP, ce paramètre peut prendre deux valeurs :

- **Annuaire LDAP (none)** : Signifie qu'il n'y a aucun annuaire par défaut. Les utilisateurs qui s'authentifient depuis le portail captif doivent renseigner leur identifiant accompagné du domaine, par exemple, [j.smith@institute.com](mailto:j.smith@institute.com). Dans le cas où le domaine n'est pas renseigné, l'authentification échoue.
- **Annuaire LDAP (Domaine)** : Signifie que l'annuaire du domaine sélectionné est utilisé pour authentifier les utilisateurs qui renseignent seulement leur identifiant (sans le domaine) depuis le portail captif, par exemple, j.smith. Les utilisateurs des autres domaines doivent, quant à eux, doivent renseigner le domaine avec l'identifiant pour être authentifiés.

**NOTE** : la méthode ou l'annuaire par défaut, ne restreint pas ce profil seulement à cette méthode ou à cet annuaire. La restriction peut se faire seulement avec une politique d'authentification.

- **Conditions d'utilisation d'accès internet** : Regroupe les paramètres qui contrôlent l'affichage des conditions d'utilisation d'accès internet renseignées dans l'onglet **PORTAIL CAPTIF**. Il contient également trois champs personnalisables qui s'affichent sur le portail d'authentification avec la méthode invité et qui permettent de récupérer différentes informations sur l'invité (Prénom, Nom, Téléphone, E-mail, etc.).

### LE PORTAIL CAPTIF

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Authentication periods allowed

Minimum duration: 0 hour(s) 15 minute(s)

Maximum duration: 4 hour(s) 0 minute(s)

For transparent authentication: 4 hour(s) 0 minute(s)

Advanced properties

Enable the captive portal

Enable logoff page

Allow access to the proxy's configuration file (.pac) for this profile

Prohibit simultaneous authentication of a user on multiple hosts

Expiry of the HTTP cookie: At the end of the authentication period

Authentication page

Select a customized message (HTML file):

User passwords

Users cannot change their passwords

Users can change their passwords

Users must change their passwords

Lifetime (in days): 0

User enrollment

Do not allow user enrollment

Allow Web enrollment for users

Allow Web enrollment for users and create their certificates

Notification of a new enrollment: Do not send messages

STORMSHIELD 32

- **Durées d'authentification autorisées** : Permet de configurer les durées maximum et minimum d'authentification pour l'authentification explicite. L'utilisateur peut choisir une durée comprise dans ces limites lors de l'authentification. Il permet également de choisir la durée d'authentification pour les méthodes transparentes (Certificats SSL et SPNEGO).
- **Configuration avancée** :
  - Gestion du portail (notamment activation pour un profil, activation de la page de déconnexion),
  - Définition de la politique appliquée aux mots de passe des utilisateurs,
  - Gestion de l'enrôlement des utilisateurs depuis le portail captif.

## LE PORTAIL CAPTIF

- Déconnexion depuis le navigateur

The image shows two screenshots of the Stormshield captive portal interface. The left screenshot shows the login page with the following text: "STORMSHIELD Network Security", "Welcome bob.sponge. Logout in 03:59", "To log out, either click on the Logout button or close the tab.", "You are authenticated as bob.sponge, and your authentication period will expire in 4 hours.", and a link "» Click here if you are not automatically redirected". A "Logout" button is highlighted with a blue box. The right screenshot shows the deauthentication page with the following text: "STORMSHIELD Network Security", "Deauthentication successful" (in a green box), "You have logged out", and a link "» Click here if you are not automatically redirected". A blue arrow points from the "Logout" button in the first screenshot to the deauthentication page in the second screenshot.

33

Lorsque la case **Activer la page de déconnexion** est cochée dans le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Authentification ⇒ onglet PROFILS DU PORTAIL CAPTIF** (configuration avancée). Un onglet de déconnexion s'ouvre dans le navigateur de l'utilisateur ayant réussi à se connecter. Pour se déconnecter, l'utilisateur doit simplement cliquer sur le bouton **Déconnexion** de cet onglet.

## LE PORTAIL CAPTIF

- Déconnexion depuis le portail captif

The diagram illustrates the deconnection process from the Stormshield captive portal in three stages:

- Initial Portal:** The user is logged in. The "LOGIN / LOGOUT" menu item is highlighted in red.
- Login Page:** The user clicks on "LOGIN / LOGOUT", leading to the login page. The "Logout" button is highlighted in red.
- Deauthentication Success:** After clicking "Logout", the user is redirected to a page displaying "Deauthentication successful" and "You have logged out".

34

Pour se déconnecter, l'utilisateur doit se connecter de nouveau au portail captif, cliquer sur **Connexion** dans le menu de gauche et ensuite sur le bouton **Déconnexion**.

## LE PORTAIL CAPTIF

- Déconnexion d'un utilisateur depuis l'interface graphique

MONITOR / USERS

No predefined filter Filter X Reset Refresh Export results Configure authentication reset columns

Name	IP address	Directory	Group	Expiry date	Auth. method	Administrator	Sponsor	SSL VPN Portal	SSL VPN Portal ...	SSL VPN	IPsec VPN
jsmith	192.168.20.1	a-team.com	chief	3h 59m 51s	PLAIN						

Search for this value in logs  
Log off this user  
Show host details  
Copy the selected line to the clipboard

The authentication period for the user jsmith@a-team.com (192.168.20.1) has been reset

STORMSHIELD 35

L'administrateur peut déconnecter les utilisateurs depuis l'interface Web dans le menu **Supervision** puis **Utilisateurs**. Cliquez sur l'utilisateur avec le bouton droit, et ensuite sur **Déconnecter l'utilisateur**.

## LE PORTAIL CAPTIF

- Activation de l'enrôlement sur le portail captif

Depuis le profil du portail captif

Lors de l'ajout de la base LDAP interne ou externe

36

L'enrôlement permet aux utilisateurs de s'auto-enregistrer depuis le portail captif. La demande d'enregistrement est envoyée au firewall pour être d'abord soumise à l'approbation de l'administrateur. Une fois approuvé, l'utilisateur est ajouté automatiquement dans l'annuaire.

L'enrôlement peut être activé lors de l'ajout d'un annuaire, mais seulement sur le profil 0 (internal). Sinon, il peut être activé également depuis le profil d'authentification, dans l'encadré **Enrôlement d'utilisateurs** situé dans la **Configuration avancée**.

**NOTE** : l'enrôlement ne peut pas être activé avec un annuaire Active Directory, car sur ce type d'annuaire, il est impossible d'ajouter un utilisateur depuis le firewall.

## LE PORTAIL CAPTIF

- Formulaire d'enrôlement

The image displays two screenshots of the Stormshield Network Security captive portal interface.

**Left Screenshot: Registration Form**

The page header includes the Stormshield Network Security logo and a navigation menu with 'LOGIN / LOGOUT' and 'NEW USER' (highlighted). Below the header, a message reads: "Please enter all the required information".

The form contains the following fields:

- Last Name \*: Baracus
- First name \*: Bosco Albert
- E-mail address \*: bab@a-team.com
- Description
- Telephone number
- Password \*\*: [masked]
- Confirm password \*\*: [masked]

A blue button labeled "Submit request..." is located below the password fields. At the bottom, there are two footnotes: "\* Mandatory fields" and "\*\* Used with the authentication module".

**Right Screenshot: Confirmation Message**

The page header is identical to the left screenshot. A green banner at the top of the main content area displays the message: "Your request has been submitted". Below this, a link is provided: "» Click here if you are not automatically redirected".

The page number "37" is visible in the bottom right corner of the right screenshot.

Lorsque l'enrôlement est activé, les utilisateurs peuvent s'enregistrer en remplissant un formulaire accessible, en cliquant sur le bouton **Nouvel utilisateur** dans le menu de gauche du portail captif. Une fois remplie, l'utilisateur envoie sa demande en cliquant sur **Soumettre ces informations**.

**NOTE** : l'enrôlement est utilisé en règle générale pour enregistrer les utilisateurs externes à l'entreprise dans votre annuaire. Le domaine indiqué dans l'adresse de messagerie est dans ce cas différent du vôtre.

**LE PORTAIL CAPTIF**

- Configuration de l'enrôlement

[USERS / ENROLMENT](#)

△ Advanced properties

User identifier format for empty ID fields

Identifier format :

Example : JOHN.DOE

E-mail notification

Send an e-mail to the user :  when approving/rejecting user's enrolment request

when approving/rejecting user's certificate request

STORMSHIELD 38

L'administrateur peut modifier l'identifiant (login) de l'utilisateur généré automatiquement avec le format par défaut %F.%L, ce qui correspond à FIRSTNAME.LASTNAME (la casse étant respectée).

La modification doit être appliquée avant de valider le premier enrôlement, afin que tous les identifiants respectent les mêmes règles.

Avec l'utilisateur John Doe montré en exemple :

- %f1.%l : Donne « j.doe » (sans espace : première lettre du prénom en minuscule, point, et nom en minuscules),
- %f%L1 : Donne « johnD » (sans espace : prénom en minuscules, première lettre du nom en majuscule).

L'administrateur peut activer également la notification par mail lors de l'acceptation ou le rejet des demandes des utilisateurs. Pour cela un serveur mail doit être configuré sur le firewall dans le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Alertes e-mails**.

## LE PORTAIL CAPTIF

- Validation de l'enrôlement

USERS / ENROLMENT

Type	Name
User	Bosco Albert BARACUS

BARACUS

ID: BOSCO ALBERT.BARACUS

Last Name: BARACUS

First name: Bosco Albert

E-mail address: bab@a-team.com

Description:

Telephone number:

Password: Present

Certificate request: None

Sur l'interface d'administration du firewall, les demandes d'enrôlement sont listées dans le menu **CONFIGURATION** ⇒ **UTILISATEURS** ⇒ **Enrôlement**. L'administrateur peut sélectionner l'utilisateur par un double clic, puis approuver, rejeter ou ignorer la demande. En cas d'approbation, l'identifiant (login) de l'utilisateur est généré automatiquement selon le format choisi à l'étape précédente.



- Introduction
- Liaison à un annuaire
- Gestion des utilisateurs
- Les méthodes d'authentification
- La politique d'authentification
- Le portail captif
- ➔ **Règles de filtrage pour l'authentification**
- Définir de nouveaux administrateurs
- Lab - Authentification

## RÈGLES DE FILTRAGE POUR L'AUTHEMIFICATION

- Créer des règles de filtrage et de NAT spécifiques pour des utilisateurs ou des groupes

The screenshot displays the Stormshield configuration interface. At the top, the 'SOURCE' field is set to 'john.smith@a-team.com'. A dropdown menu is open, showing a list of user groups: 'any', 'none', 'guest\_users.local.domain', 'sponsored\_users.local.domain', 'voucher\_users.local.domain', and 'a-team.com'. Below this, a list of users is shown, including 'No user', 'Any user@none', 'Any user@any', 'Any user@a-team.com', 'Any user@voucher\_users.local.domain', 'Any user@sponsored\_users.local.domain', 'Any user@guest\_users.local.domain', 'Unknown users', 'user1@a-team.com', 'uid=user1,o=a-team,dc=com', 'John Smith@a-team.com', 'uid=jsmith,o=a-team,dc=com', 'user2@a-team.com', and 'uid=user2,o=a-team,dc=com'. The 'FILTERING' section shows a table of rules. Rule 2 is highlighted, showing it is an authentication portal rule for 'authentication\_bypass' with source 'Network\_Internals' and destination 'internet'. Rule 3 is also highlighted, showing it is a NAT rule for 'http' with source 'jsmith@Network\_Internals' and destination 'internet'.

La règle d'authentification permettant seulement de rediriger les utilisateurs inconnus vers le portail captif, il faut impérativement ajouter par la suite d'autres règles permettant aux utilisateurs authentifiés d'accéder au réseau.

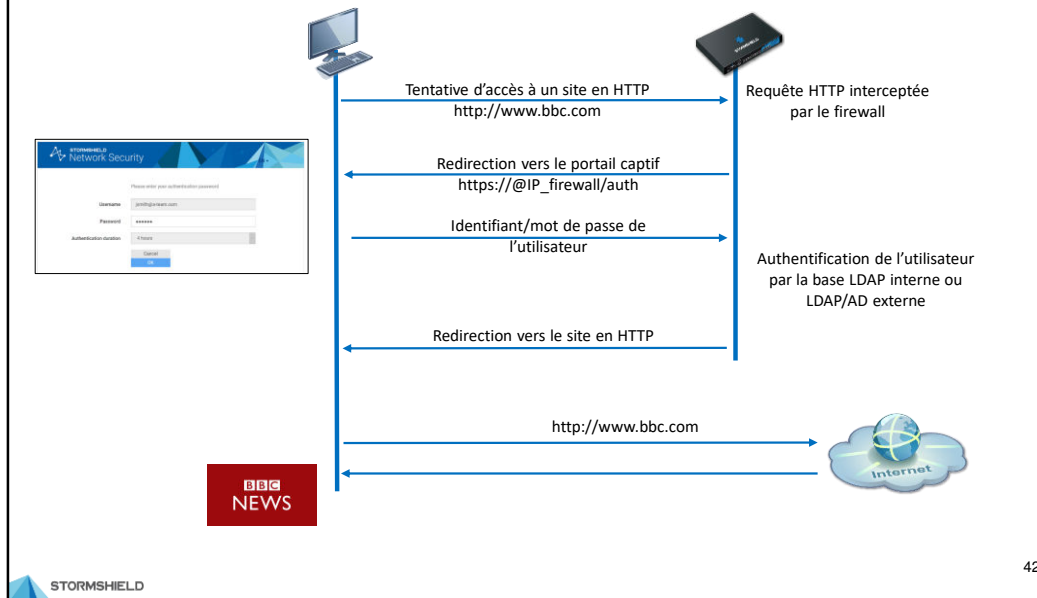
Lors de l'édition de la source d'une règle de filtrage ou de NAT, le champ **Utilisateur** permet de spécifier l'utilisateur (ou le groupe) devant être authentifié pour que la règle s'applique. Plusieurs entrées sont listées :

- **No User** : Choix par défaut lors de l'ajout d'une nouvelle règle. La règle sera appliquée sans prendre en considération le paramètre utilisateur,
- **Any user@any** : Désigne tout utilisateur authentifié, quel que soit l'annuaire ou la méthode d'authentification utilisés,
- **Any user@guest\_users.local.domain** : Désigne tout utilisateur authentifié par la méthode invité,
- **Any user@voucher\_users.local.domain** : Désigne tout utilisateur authentifié par la méthode comptes temporaires,
- **Any user@sponsored\_users.local.domain** : Désigne tout utilisateur se présentant via la méthode parrainage,
- **Any user@<domaine>** : Désigne tout utilisateur authentifié par l'annuaire du domaine,
- **Any user@none** : Désigne tout utilisateur authentifié par une méthode n'utilisant pas un annuaire, par exemple : parrainage, compte temporaire, etc.
- **Utilisateurs inconnus**: Désigne tout utilisateur non authentifié. Cette valeur est principalement utilisée dans une règle d'authentification.
- La liste de tous les utilisateurs et groupes présents dans les annuaires.

Le bouton à droite du paramètre utilisateur permet de filtrer les utilisateurs en fonction de l'annuaire ou de la méthode d'authentification.

## RÈGLES DE FILTRAGE POUR L'AUTHEMIFICATION

- Mécanisme de redirection vers le portail captif



L'authentification LDAP via le portail captif est décrite ci-dessus. L'utilisateur ouvre un navigateur pour accéder à un site en HTTP. La requête HTTP est interceptée par le firewall qui renvoie l'utilisateur vers le portail d'authentification (`https://@IP_firewall/auth`). L'utilisateur introduit son identifiant/mot de passe d'annuaire qui sont envoyés au firewall via une connexion sécurisée (HTTPS). Le firewall authentifie l'utilisateur au niveau de l'annuaire (LDAP interne/externe ou AD). Dans le cas où l'utilisateur est authentifié, le navigateur est renvoyé vers le site web demandé au départ.

**NOTE :** la redirection vers le portail captif peut fonctionner en accédant à des sites en HTTPS, mais cela nécessite l'activation du proxy SSL qui est présenté dans la formation expert CSNE.

La configuration LDAP via le portail captif est détaillée dans les diapositives suivantes.

## RÈGLES DE FILTRAGE POUR L'AUTHENTIFICATION

- Rediriger les requêtes HTTP des utilisateurs non authentifiés vers le portail captif

The screenshot shows the Stormshield configuration interface. At the top, a menu lists rule types: Simple rule, Separator - rule grouping, **Authentication rule** (highlighted), SSL inspection rule, and Explicit HTTP proxy rule. Below this, the 'AUTHENTICATION WIZARD' dialog is open, showing the objective and configuration fields. The 'FINISH' button is highlighted. In the background, the 'FILTERING' table is visible, with a rule (ID 2) highlighted in red, indicating the configuration of the authentication rule.

ID	Status	Action	Source	Src. port	Destination	Dest. port	Protocol	Security Inspection
1	on	pass	DNS_srv	Any	Internet	dns		
2	on	Authentication portal Except: authentication_bypass	unknown @ Network_internals	Any	Internet		http	

La redirection des connexions HTTP vers le portail d'authentification s'effectue par une règle d'authentification dans les règles de filtrage. Cependant, avant d'ajouter cette règle, il faut s'assurer que les connexions DNS sont autorisées pour tous les utilisateurs (authentifiés ou non), car sans résolution DNS, il n'y aura pas de requêtes HTTP et par conséquent, pas de redirection vers le portail captif.

Pour créer la règle d'authentification cliquez sur **Nouvelle règle** ⇒ **Règle d'authentification**. Au niveau de l'assistant, il faut renseigner le réseau source d'où les utilisateurs se connectent, le réseau destination et éventuellement une liste de catégories d'URLs qui sont accessibles sans authentification.



- Introduction
- Liaison à un annuaire
- Gestion des utilisateurs
- Les méthodes d'authentification
- La politique d'authentification
- Le portail captif
- Règles de filtrage pour l'authentification
- ➔ **Définir de nouveaux administrateurs**
- Lab - Authentification

## DÉFINIR DE NOUVEAUX ADMINISTRATEURS

- Droits d'administration particuliers
  - Créer des comptes permettant de visualiser ou modifier la configuration
  - Choix des modules à affecter

Administrator without any privileges  
 Administrator with read-only access  
 Administrator with all privileges  
 Administrator for temporary accounts  
 Administrator with access to private data  
 Administrator without access to private data

SYSTEM / ADMINISTRATORS

ADMINISTRATORS ADMINISTRATOR ACCOUNT TICKET MANAGEMENT

Add an administrator X Delete | ↑ ↓ Copy privileges Paste privileges Grant all privileges Switch to simple view

	user - user group	Logs (R)	Filter (R)	VPN (R)	Access to private data (L)	Logs (W)	Filter (W)	VPN (W)	Management of access to private data	PKI	Monitoring	Content filtering	Objects	Users	Network
1	jsmith@e-team.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	chief@e-team.com	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Depuis le menu **Configuration** ⇒ **Système** ⇒ **Administrateurs** ⇒ **Onglet Administrateurs**, il est possible de définir une politique de droits d'accès en fonction des utilisateurs de la base LDAP. Ainsi, plusieurs statuts sont disponibles :

- Administrateur sans droit,
- Administrateur avec accès en lecture seule uniquement,
- Administrateur avec tous les droits,
- Administrateur de comptes temporaires : autorise la création des comptes pour la méthode d'authentification compte temporaire,
- Administrateur avec accès aux données sensibles : permet d'avoir un accès complet aux logs,
- Administrateur sans accès aux données sensibles : restreint l'accès à certaines informations dans les logs.

L'édition des règles propose deux modes d'affichage, la vue simple et la vue avancée (comme ci-dessus) pour obtenir davantage de détails sur les droits accordés.

**DÉFINIR DE NOUVEAUX ADMINISTRATEURS**

- Chaque administrateur peut modifier son mot de passe
- Un administrateur ne peut pas modifier le mot de passe d'un autre administrateur
- « admin » peut modifier le mot de passe de tout le monde
- Un administrateur avec les droits « utilisateur » peut modifier le mot de passe d'un simple utilisateur

## RECOMMANDATIONS



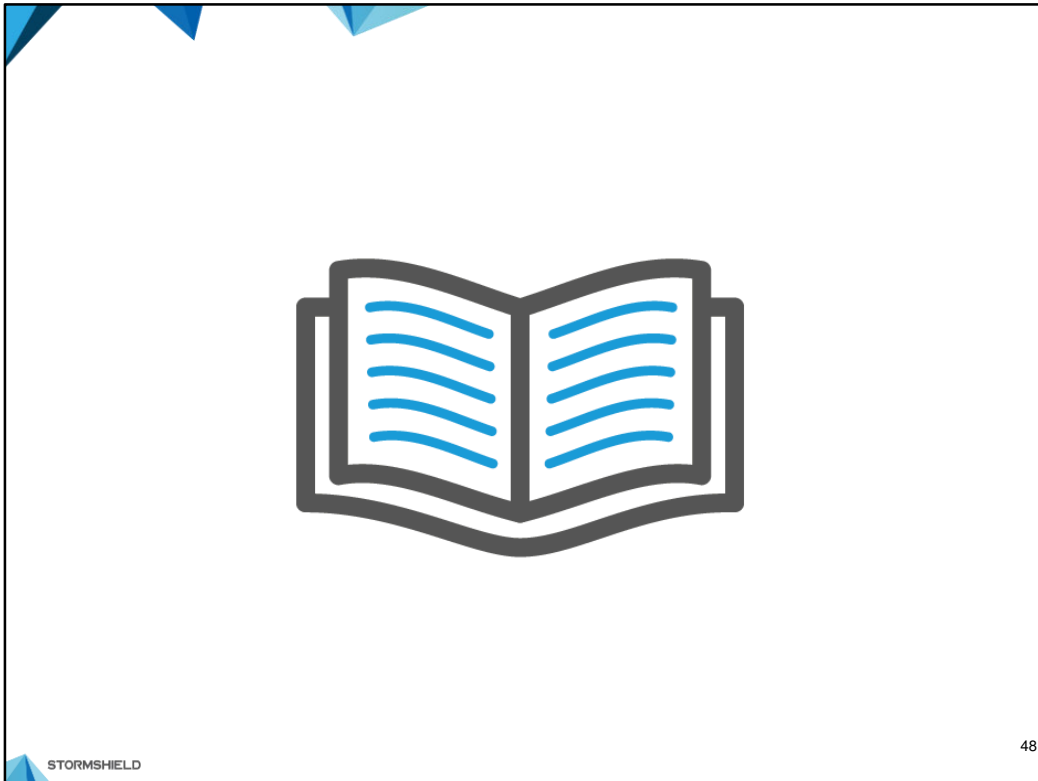
- Protéger le compte administrateur local
- Utiliser des comptes nominatifs
- Utiliser des groupes pour gérer les droits
- Ajuster les droits d'administration, séparer les rôles
  
- Authentifier localement par certificat
  
- Dédier un annuaire externe aux administrateurs
- Configurer LDAP de manière sécurisée
- Utiliser un compte d'accès à l'annuaire restreint et sécurisé

Le mot de passe administrateur doit être conservé au coffre-fort et son utilisation exceptionnelle doit être supervisée et limitée à un ensemble déterminé de personnes. Il ne doit être utilisé que pour l'accès SSH ou pour établir les droits des utilisateurs.

Seul le compte administrateur local peut attribuer les droits administratifs. C'est pour cela qu'il est recommandé d'attribuer des droits à des groupes. Les comptes des utilisateurs seront ensuite répartis dans les groupes (cette opération peut se faire depuis l'annuaire).

Un administrateur dédié à une tâche précise ne doit avoir qu'un périmètre d'action limité. Cela permet de cloisonner les risques en cas de compromission de son compte, ainsi que limiter les modifications involontaires de configuration.

L'accès à l'annuaire LDAP externe doit être configuré de manière sécurisée et redondante. Le compte utilisé pour authentifier le firewall sur l'annuaire doit avoir le minimum de droits (lecture seule) et être spécifique.



Pour aller plus loin, consultez les notes techniques du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Configuration SSO - Microsoft SPNEGO
- Configurer les méthodes d'authentification de type « Guest »
- Installation et déploiement de l'agent SSO
- Se conformer aux règlements sur les données personnelles

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Introduction
- Liaison à un annuaireS
- Gestion des utilisateurs
- Le portail captif
- Les méthodes d'authentification
- La politique d'authentification
- Règles de filtrage pour l'authentification
- Définir de nouveaux administrateurs

 **Lab - Authentification**

## Lab 7 – Authentification

Copiez la politique de filtrage/NAT (6) Lab\_6 vers la politique numéro 7. Renommez la politique numéro 7 « Lab\_7 », puis activez cette politique.

1. Lancez l'assistant LDAP et créez une base LDAP interne :
  - Le nom d'organisation est x, et le domaine est « net ».
  - Activez le profil d'authentification 0 (internal) sur l'interface « IN », ainsi que l'enrôlement des utilisateurs.
  - Testez l'accès au portail captif : <https://192.168.x.254/auth>
2. Créez un utilisateur John Smith :
  - Identifiant : jsmith
  - Mot de passe : password
  - Adresse email : jsmith@x.net
3. En utilisant la fonction d'enrôlement, créez un utilisateur « Peter Wood » avec le mot de passe : password
4. Testez l'authentification de chacun des utilisateurs.
5. Modifiez la politique de filtrage pour que l'envoi de pings depuis votre réseau interne ne soit autorisé qu'à John Smith. Cette règle devra systématiquement lever une alarme mineure.
6. Adaptez la politique de filtrage afin que tous les utilisateurs non authentifiés soient redirigés vers le portail captif lorsqu'ils tentent d'accéder à des sites WEB en HTTP, sauf les sites présents dans la catégorie « it ».
7. Tester l'accès en HTTP à un site appartenant à la catégorie « it » et confirmer la redirection vers le portail pour tout autre site en HTTP n'appartenant pas à cette catégorie.
8. Donnez à John Smith les droits de supervision sur le Firewall.
9. Connectez-vous sur le firewall avec le compte « jsmith » et validez l'accès aux différents menus. Testez également l'authentification avec ce compte sur le portail d'authentification.



# Quiz

STORMSHIELD

Q1 – Une des limites de l’annuaire interne au pare-feu est qu’il ne supporte pas les groupes d’utilisateurs :

- A. Vrai
- B. Faux

Q2 – Il n’est pas possible de rediriger vers le portail captif les utilisateurs visant un site web en HTTPS :


- A. Faux, la règle de redirection permet de le faire de base.
- B. Vrai, c’est impossible car HTTPS est chiffré.
- C. Vrai, mais on peut utiliser le proxy SSL pour cela.

Q3 – Tous les administrateurs du pare-feu peuvent gérer les droits des autres administrateurs :

- A. Vrai
- B. Faux

Q4 – La création d’un utilisateur par enrôlement nécessite obligatoirement une action de la part d’un administrateur :

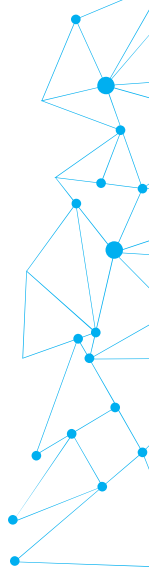
- A. Vrai
- B. Faux



STORMSHIELD

# ANNXE – UTILISATEURS & AUTHENTIFICATION

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



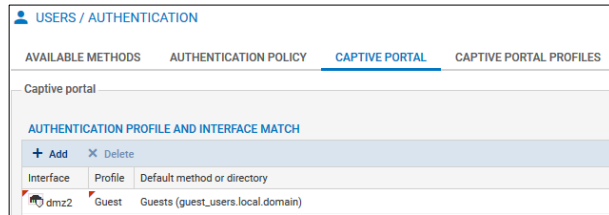
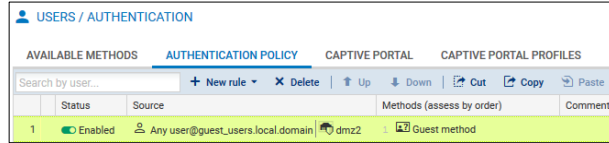
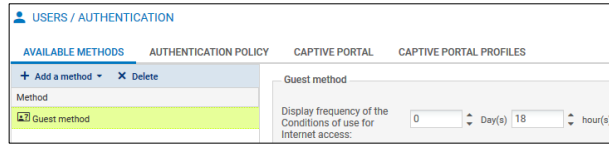
➔ **Méthode guest**

STORMSHIELD

**Utilisateurs & authentification**

## MÉTHODE GUEST

- Activation
- Politique d'authentification
- Activation du portail captif



La méthode Guest est simple et rapide à configurer. Dans la liste des méthodes disponibles, le seul paramètre à renseigner concerne la fréquence d'affichage des conditions d'utilisation (par défaut à une valeur de 18 heures).

Dans l'édition de la politique d'authentification, un assistant est prévu pour facilement configurer la méthode Guest. Cet assistant ne demande que le réseau ou l'interface depuis laquelle les machines clientes vont s'authentifier. La méthode Guest sera donc appliquée à tous les utilisateurs provenant de l'objet ou arrivant sur l'interface.

Enfin, pour permettre à l'utilisateur de valider la charte d'accès lors de sa navigation WEB, il est nécessaire de configurer le portail captif.

## MÉTHODE GUEST

- Choix des fichiers descriptifs de la charte d'accès
- Vérification du profil Guest

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Conditions of use for Internet access

Select the conditions of use for Internet access in HTML format:

Select the conditions of use for Internet access in PDF format:

Reinitialize customization of Conditions of use for Internet access

Advanced properties

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Guest Rename

Authentication

Default method or directory: Guests (guest\_users.local.domain)

Enable sponsorship

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

ID	Status	Action	Source	Destination	Dest. port	Security inspection
1	on	pass	srv_dns_priv	Internet	dns_udp	IPS
2	on	Authentication portal Except: authentication_bypass	unknown @ Network_dmz2	Internet	http	IPS

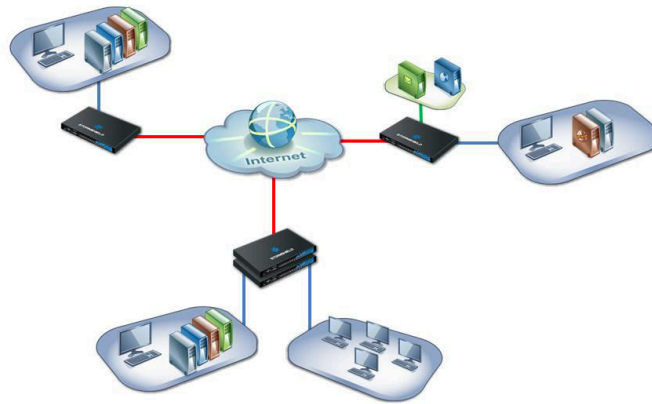
STORMSHIELD

4

Les fichiers au format HTML ou PDF décrivant la charte d'accès aux invités sont ajoutés dans le panneau de configuration du portail captif.

Il reste à écrire une règle de filtrage avec redirection vers le portail captif pour les invités.

ADVANCED LAB - AUTHENTIFICATION ET COMPTES TEMPORAIRES  
ADVANCED LAB - AUTHENTIFICATION ET PARRAINAGE



STORMSHIELD

5

Advanced Labs disponibles à la fin du support de cours.



## Programme de la formation

- ✓ Coursus des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Objets
- ✓ Configuration réseau
- ✓ Translation d'adresses
- ✓ Filtrage
- ✓ Protection applicative
- ✓ Utilisateurs & authentification
- VPN
- VPN SSL



## Les différents réseaux privés virtuels

- VPN IPsec – Concepts et généralités
- VPN IPsec – Configuration de tunnel site-à-site
- VPN IPsec – Configuration de tunnels site-à-site multiples
- VPN IPsec – Virtual Tunneling Interface
- Lab - VPN IPsec (site à site)



## VIRTUAL PRIVATE NETWORK

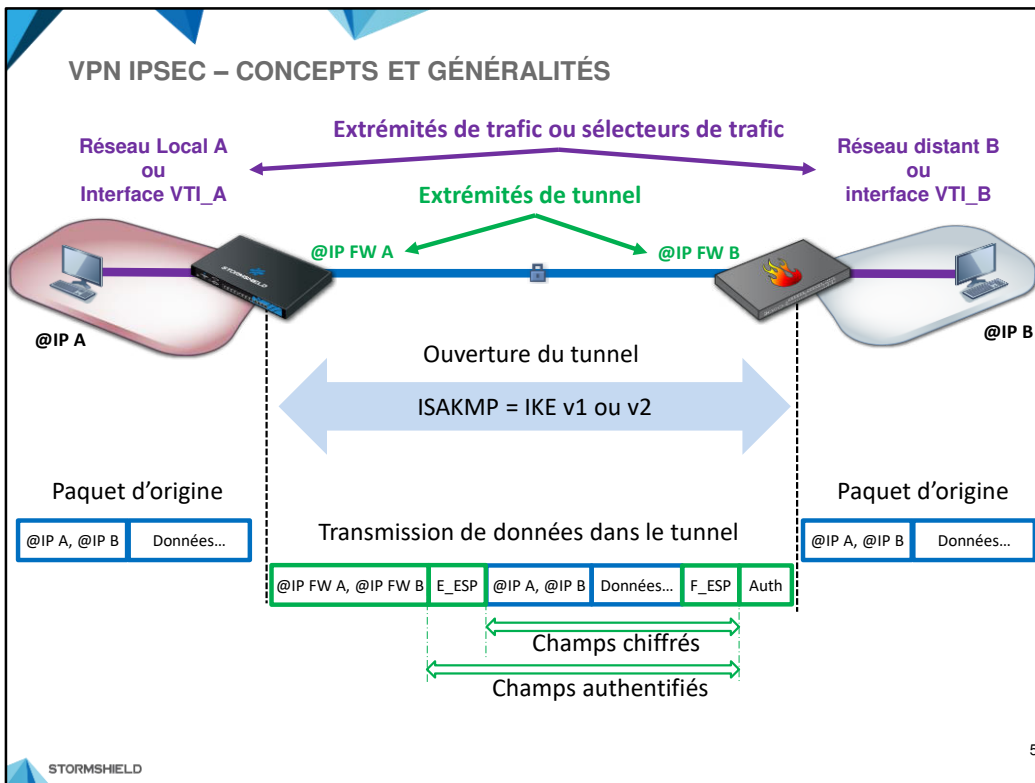
- Trois familles de VPN
  - **PPTP** : Pour clients nomades uniquement (voir en annexes)
    - Solution obsolète, utilisation non recommandée en raison des risques de sécurité
  - **VPN SSL** : Pour clients nomades uniquement
  - **VPN IPsec** : Pour tunnels site-à-site ou clients nomades
  - GRE / GRE-TAP : Site-à-site pour transport de paquets IP ou trame ethernet (vu en CSNE)



- Les différents réseaux privés virtuels
- ➔ **VPN IPsec – Concepts et généralités**
- VPN IPsec – Configuration de tunnel site-à-site
- VPN IPsec – Configuration de tunnels site-à-site multiples
- VPN IPsec – Virtual Tunneling Interface
- Lab - VPN IPsec (site à site)

STORMSHIELD

Virtual Private Network



Le tunnel VPN IPsec site-à-site permet de connecter deux réseaux privés via un réseau public tout en assurant les services de sécurité suivants :

- L'**authentification** : Permet la vérification des identités des deux extrémités de tunnel. Deux méthodes d'authentification sont possibles : clé pré-partagée (PSK : Pre-Shared key) ou certificats (PKI : Public Key Infrastructure),
- L'**intégrité** : Vérifie que les données n'ont pas été modifiées en utilisant les algorithmes de hachage,
- La **confidentialité** : Assure que les données ne peuvent être lues par une personne tierce capturant le trafic,
- L'**anti-rejeu** : Permet d'ignorer des anciens paquets (des paquets dont le numéro de séquence est antérieur à un certain seuil) déjà reçus, s'ils sont transmis à nouveau.

Le tunnel VPN IPsec site-à-site peut s'établir entre le firewall SNS et n'importe quel équipement compatible VPN IPsec. La négociation du tunnel s'effectue avec le protocole ISAKMP (Internet Security Association Key Management Protocol), appelé également IKE (Internet Key Exchange), qui existe actuellement en deux versions V1 (RFC 2409) et V2 (RFC 7296).

La négociation s'effectue entre les extrémités de tunnel qui correspondent aux adresses IP des équipements (@IP FW A et @IP FWB). Le protocole IKE est transmis via le protocole UDP sur le port 500.



Une fois le tunnel établi entre les deux équipements, les extrémités de trafic correspondantes aux réseaux privés peuvent communiquer via le protocole ESP (Encapsulating Security Payload) qui assure la confidentialité et l'intégrité des données. Le protocole ESP (le numéro de protocole IP est 50, défini dans RFC 4303) est encapsulé directement dans un paquet IP.

Deux modes de fonctionnement conditionnent différemment la décision d'encapsuler les paquets IP dans ESP :

- **Correspondance de politique (fonctionnement standard)** : Concordance des adresses IP des usagers avec la politique VPN IPsec ; ce mode de fonctionnement repose sur les critères [IP source + IP de destination] de ces paquets IP en comparaison avec la politique chargée dans les structures IPsec du système. Dans ce mode de fonctionnement, la politique IPsec est évaluée en amont des directives générales de routage IP. Son application repose exclusivement sur la correspondance de politique.
- **Virtual Tunneling Interface (mode de fonctionnement si le routage par VTI est activé)** : Routage via la VTI (Virtual Tunneling Interface) distante dont l'adresse IP appartient au même réseau que la VTI locale. Les interfaces VTI permettent de définir des routes passant par le tunnel IPsec. Elles agissent comme passerelles réciproques l'une de l'autre. Elles sont comme des points d'entrée et de sortie du tunnel. Ce mode de fonctionnement est prioritaire sur la correspondance de politique.

**NOTE :**

- Dans le cas où une extrémité de tunnel est située dans un réseau traduit, NAT-Traversal sera activé automatiquement afin que le protocole UDP sur le port 4500 soit utilisé pour finaliser la négociation IKE et transmettre les paquets ESP (thème abordé dans la formation CSNE).

## VPN IPSEC – CONCEPTS ET GÉNÉRALITÉS

- Les identités des correspondants :

- Site-à-site avec adresses IP fixes



- Site-à-site avec un correspondant dont l'adresse IP est dynamique

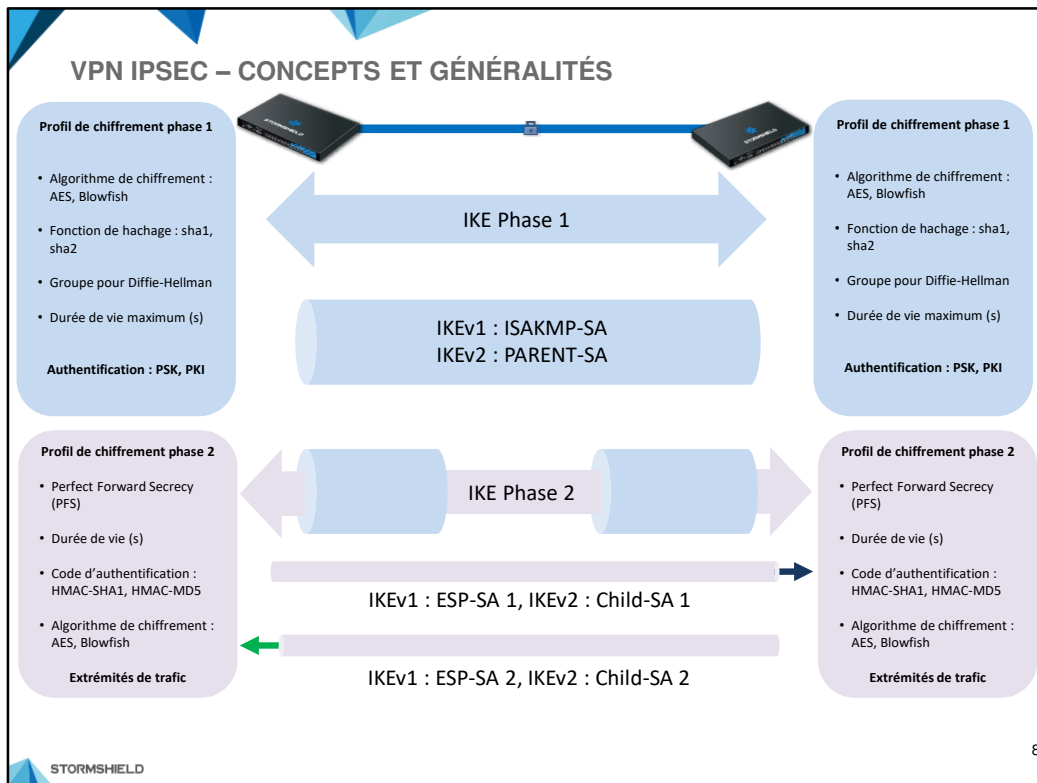


Durant l'authentification, chaque extrémité vérifie l'identité de l'autre. Les identités pouvant représenter une extrémité de tunnel sont :

- L'adresse IP de l'interface réseau externe « Firewall\_out » dans le cas où elle est configurée avec une adresse IP fixe,
- Un FQDN dans le cas où une extrémité ne possède pas d'adresse IP fixe.

En fonction de la méthode d'authentification utilisée, l'identité est associée à :

- Une clé pré-partagée PSK (Pre-Shared Key) : Chaque extrémité fera la preuve qu'elle détient la PSK commune.
- Une PKI (Public Key Infrastructure) : Chaque extrémité présentera un certificat numérique X509 qui doit être signé par une autorité de certification de confiance pour l'autre correspondant. L'utilisation de certificat pour l'authentification est abordée dans la formation expert CSNE.



La négociation IKE pour l'établissement d'un tunnel VPN IPsec se déroule en deux phases :

- Phase 1** : Durant cette phase, les deux extrémités de tunnel négocient un profil de chiffrement phase 1 qui contient les algorithmes de chiffrement/authentification. Durant cette phase également, les deux extrémités s'authentifient avec une clé pré-partagée ou les certificats.

Si les deux extrémités n'arrivent pas à se mettre d'accord sur un profil de chiffrement commun ou à s'authentifier, la phase 1 échoue et la négociation s'arrête.

Dans le cas contraire, un dialogue d'application chiffré, nommé ISAKMP-SA (Internet Security Association Key Management Protocol – Security Association) dans IKEv1 ou PARENT-SA dans IKEv2, est établi entre les deux extrémités. Il permet la négociation de la phase 2 qui sera entièrement chiffrée grâce à la clé de phase 1 ISAKMP-SA.
- Phase 2** : Durant cette phase les deux extrémités négocient le profil de chiffrement phase 2 et les extrémités de trafic qui pourront communiquer via le tunnel VPN IPsec.



Si les deux extrémités ne parviennent pas à faire concorder ces paramètres, la phase 2 échoue, sinon, deux canaux sont ouverts pour la transmission des données (un dans chaque direction). Chaque canal utilise sa propre clé de chiffrement. Elles sont appelées ESP-SA1 et ESP-SA2 en IKEv1 et CHILD-SA1 et CHILD-SA2 en IKEv2. Ainsi chaque extrémité possédera les deux clés symétriques : une pour chiffrer les données transmises et l'autre pour déchiffrer les données reçues.

**NOTES :**

- En IKEv1, la négociation phase 1 peut se faire avec deux modes MAIN ou AGGRESSIVE. Ce dernier est plus simple et plus rapide (échange de 3 paquets au lieu de 6 en mode MAIN) mais est moins sécurisé. Il n'est plus supporté depuis la version 4.2.
- En IKEv1, il est impératif que les extrémités de trafic soient identiques pour les deux correspondants, sinon la phase 2 échoue. Ce n'est, en revanche, pas obligatoire en IKEv2 mais il est fortement recommandé de configurer ces paramètres à l'identique afin d'éviter tout effet de bord indésirable.
- Pour simplifier et conserver une certaine homogénéité dans la présentation des logs, les firewalls SNS utilisent la terminologie de IKEv1 (phase 1 et phase 2) sur IKEv2.
- La négociation du tunnel est déclenchée par le correspondant dont le réseau local a initié du trafic vers le réseau distant. Par conséquent, s'il n'y a pas de trafic entre les réseaux, le tunnel ne sera pas ouvert.



- Les différents réseaux privés virtuels
- VPN IPsec – Concepts et généralités
- ➔ **VPN IPsec – Configuration de tunnel site-à-site**
- VPN IPsec – Configuration de tunnels site-à-site multiples
- VPN IPsec – Virtual Tunneling Interface
- Lab - VPN IPsec (site à site)

STORMSHIELD

Virtual Private Network

**VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE**

**VPN / IPSEC VPN**

**ENCRYPTION POLICY - TUNNELS**    PEERS    IDENTIFICATION    ENCRYPTION PROFILES

IPsec 01 (01)    Actions

**SITE TO SITE (GATEWAY-GATEWAY)**    MOBILE - MOBILE USERS

Enter a filter    + Add    X Delete    ↑ Up    ↓ Down    Cut    Copy    Paste    Show details

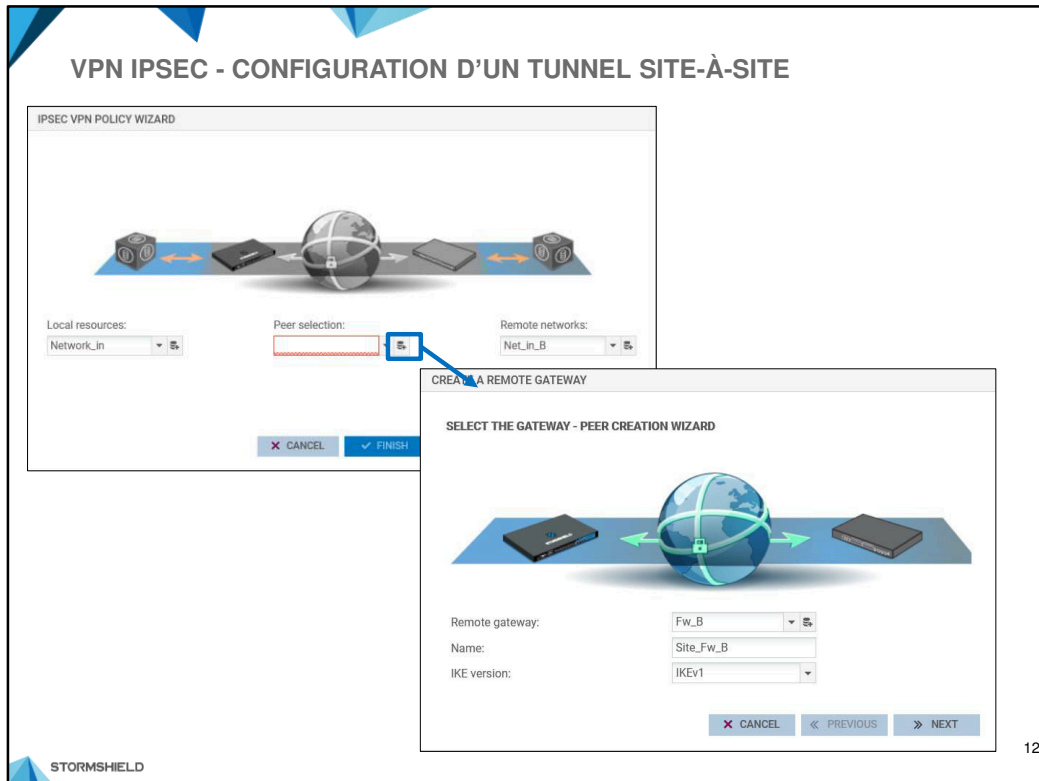
	Status	Remote network	Encryption profile
(1) IPsec 01			
(2) IPsec 02			
(3) IPsec 03			
(4) IPsec 04			
(5) IPsec 05			
(6) IPsec 06			
(7) IPsec 07			
(8) IPsec 08			
(9) IPsec 09			
(10) IPsec 10			

Standard site-to-site tunnel  
Separator (rule grouping)

STORMSHIELD

11

La configuration d'un tunnel VPN IPsec site-a-site s'effectue depuis le menu **VPN ⇒ VPN IPsec > onglet POLITIQUE DE CHIFFREMENT – TUNNELS > onglet SITE À SITE (GATEWAY – GATEWAY)**, en cliquant sur **Ajouter ⇒ Tunnel site à site**.



Un assistant s'affiche pour renseigner les principaux paramètres : les extrémités de trafic (**réseaux local** et **réseau distant**) et l'extrémité de tunnel distante (le **correspondant**).

Si le correspondant n'existe pas, il faut le créer en cliquant sur le bouton **AJOUTER** (bleu) qui sera utilisé pour la négociation du tunnel. Un nouvel assistant s'affiche pour renseigner les paramètres du correspondant : la passerelle distante, le nom et la version IKE (1 ou 2). Par défaut, la version IKE 1 est utilisée.

Le champ **Passerelle distante** permet de renseigner l'objet machine qui porte l'adresse IP du correspondant.

**REMARQUE** : à partir de la version 4.2.4, la version IKE par défaut est IKEv2.

### VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

**CREATE A REMOTE GATEWAY**

**PEER IDENTIFICATION - PEER CREATION WIZARD**

Authentication type:  Certificate  
 Pre-shared key (PSK)

Certificate:  x

Trusted CA:  x

Pre-shared key (PSK):

Confirm:

Enter the key in ASCII characters:

**CREATE A REMOTE GATEWAY**

**SUMMARY - PEER CREATION WIZARD**

Parameters of the remote site

Name:	Site_Fw_B
Remote gateway:	Fw_B

Peer identification: pre-shared keys

Pre-shared key:	ThisIsASecretPassword\$
-----------------	-------------------------


13

Après avoir cliqué sur **Suivant**, l'assistant se poursuit et il est possible de configurer la méthode d'authentification. En sélectionnant PSK, la clé pré-partagée renseignée sera associée à l'identité du correspondant.

Enfin, la dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours. En cliquant sur **Terminer**, on retourne sur l'assistant de création du tunnel VPN.

**VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE**

IPSEC VPN POLICY WIZARD



Local resources: Network\_In

Peer selection: Site\_Fw\_B

Remote networks: Net\_In\_B

↓

**VPN / IPSEC VPN**

ENCRIPTION POLICY - TUNNELS    PEERS    IDENTIFICATION    ENCRYPTION PROFILES

IPsec 01 (01)    Actions

**SITE TO SITE (GATEWAY-GATEWAY)**    MOBILE - MOBILE USERS

Enter a filter    + Add    X Delete    ↑ Up    ↓ Down    Cut    Copy    Paste    Show details

	Status	Local network	Peer	Remote network	Encryption profile
1	on	Network_In	Site_Fw_B	Net_In_B	StrongEncryption

STORMSHIELD

14

Une fois les trois paramètres (**réseau local**, **réseau distant** et le **correspondant**) renseignés, vous pouvez cliquer sur Terminer. Le tunnel VPN IPsec est ajouté sur une ligne distincte de la politique. L'assistant crée une politique désactivée par défaut. Celle-ci doit être activée manuellement en définissant l'**État** sur **ACTIVE** au sein de la politique.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Colonne « Nom » dans la vue « Politique »

The screenshot shows the Stormshield VPN configuration interface. The main view is 'SITE TO SITE (GATEWAY-GATEWAY)'. A table lists the VPN policies. The first row is highlighted in green and has a red box around the 'Name' column, which contains the text 'VPN to remote'. The 'Columns' menu is open, showing a list of columns with checkboxes. The 'Name' checkbox is checked, indicating that the 'Name' column is visible in the current view.

	Status	Name	Local network	Peer	Remote network	Encryption profile
1	on	VPN to remote	Network_in	Site_fw_B	Net_in_B	

La colonne **Nom** peut être cachée par défaut ; pour la faire apparaître, cliquer sur l'en-tête de colonne, puis sélectionner le menu **Colonnes** et cocher l'option **Nom**. Elle affiche le nom des politiques. Dans les traces VPN (I\_vpn), l'entrée **rulename** se rapporte à ce nom.

NOTE: Un champ qui précise le type de règle VPN (tunnel mobile ou tunnel site-à-site) a été ajouté aux traces VPN IPsec également.

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

Q Enter a filter + Add Actions

Remote gateways (1)

Site\_remote\_gateway This is a useful ...

### SITE\_REMOTE\_GATEWAY

**General**

Comment: This is a useful comment

Remote gateway: remote\_gateway

Local address: Any

IKE profile: StrongEncryption

IKE version: IKEv2

**Identification**

Authentication method: Certificate

Certificate: sslvpn-full-default-authority.openvpnserver

Local ID: Enter an ID (optional)

Peer ID: Enter an ID (optional)

Pre-shared key (PSK): Edit

**Advanced properties**

Do not initiate the tunnel (Responder only)

IKE fragmentation

DPD: Passive

DSCP: 00 Best effort

STORMSHIELD 16

L'onglet «Correspondant» liste les correspondants créés avec l'assistant et permet d'en créer d'autres. Dans tous les cas, il offre la possibilité de modifier ou de compléter leur configuration après la création.

Parmi les paramètres modifiables, on trouve notamment :

- **Adresse locale** : ce champ permet de sélectionner l'adresse IP présentée pour établir le tunnel avec le correspondant affiché.
- **ID du correspondant et local ID** : sous forme d'une adresse IP, d'un FQDN ou d'une adresse mail, ce champ représente les extrémités locale et distante du tunnel partageant une PSK. En cas de traversée d'un équipement appliquant du NAT, il est nécessaire de renseigner son localID avec l'adresse IP «publique» apparente après traduction de l'adresse IP d'extrémité locale de tunnel.
- **Ne pas initier le tunnel** : cette option indique au firewall de se mettre en écoute et de laisser l'initiative de la négociation du tunnel au correspondant.
- **Fragmentation IKE** : permet d'activer la fragmentation des paquets IKE lorsque ces derniers dépassent la taille standard paramétrée sur le firewall (plus de détails en CSNTS).

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Les profils de chiffrement phase 1 et phase 2

The screenshot displays the Stormshield VPN configuration interface. The top section shows the configuration for a tunnel named 'SITE\_FW\_B'. Under the 'GENERAL' tab, the 'IKE profile' is set to 'StrongEncryption'. The bottom section shows a table of tunnels with the following data:

ID	Status	Local network	Peer	Remote network	Encryption profile
1	on	Network_in	Site_Fw_B	Net_in_B	StrongEncryption

Annotations in the image point to the 'StrongEncryption' selection in the 'IKE profile' dropdown and the 'StrongEncryption' entry in the table, with labels: 'Profil phase 1 (IKE)' and 'Profil phase 2 (IPSEC)'.

Le profil de chiffrement phase 1 appelé également profil IKE est configuré au niveau du correspondant, tandis que le profil de chiffrement phase 2, appelé profil IPSEC est configuré au niveau du tunnel VPN.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Consulter, modifier et créer des profils de chiffrement phase 1 et phase 2

The screenshot displays the Stormshield VPN configuration interface. The left sidebar shows a tree view with 'IKE (4)' expanded, containing 'DR', 'StrongEncryption', 'GoodEncryption', and 'Mobile'. The 'Add' and 'Actions' buttons are highlighted. The main content area shows the configuration for 'IKE PROFILE: STRONGENCRYPTION' with fields for 'Comments', 'Diffie-Hellman', and 'Maximum lifetime'. Below this is a 'PROPOSALS' table with columns for 'Algorithm', 'Strength', and 'Authentication'. The 'Define the default profile' option in the actions menu is highlighted, with an arrow pointing to it from the text 'New phase 2 profile'. Another arrow points to the 'Add' button from the text 'New phase 1 profile'.

Encryption		Authentication	
Algorithm	Strength	Algorithm	Strength
1 aes	256	sha2_256	256
2 aes	128	sha2_256	256

Pour les deux phases, il existe quatre profils préconfigurés : **StrongEncryption**, **GoodEncryption**, **Mobile** et **DR**. L'onglet PROFILS DE CHIFFREMENT du menu VPN → VPN IPsec permet de :

- Consulter et de modifier la configuration des profils préconfigurés,
- Définir les profils qui seront utilisés par défaut lors de l'ajout des tunnels (à l'aide du paramètre **Définir le profil par défaut** ),
- Créer de nouveaux profils phase 1 et phase 2 personnalisés en cliquant sur le bouton **Ajouter**.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- La fonction Keepalive

The screenshot shows the Stormshield VPN configuration interface. The main window is titled 'VPN / IPSEC VPN' and displays a table of tunnels. The table has columns for 'Status', 'Local network', 'Peer', 'Remote network', 'Encryption profile', 'Keep alive', and 'Comments'. The 'Keep alive' column is currently set to '30'. A context menu is open over the 'Keep alive' column header, showing options to toggle the column's visibility and to edit its value. The 'Keep alive' option is checked, and a dropdown menu is open, showing the current value '30' and other options: '0', '60', '120', '300', and '600'. The '30' option is highlighted in yellow.

STORMSHIELD

19

S'il n'est pas établi, un tunnel IPsec est négocié seulement lors de l'émission de paquets correspondant à la politique IPsec. Cela engendre de la latence et les premiers paquets risquent d'être perdus le temps de la négociation. La fonction **Keepalive** vise à maintenir le tunnel disponible en envoyant à intervalles réguliers un datagramme UDP correspondant aux extrémité du trafic sur le port UDP numéro 9, ce qui provoque la négociation initiale du tunnel, puis ses renégociations périodiques.

La colonne **keepalive** peut être cachée par défaut. Pour la faire apparaître, cliquer sur l'en-tête de colonne, puis sélectionner le menu **Colonnes** et cocher l'option **Keepalive**. Elle permet de configurer la fréquence d'envoi de datagrammes UDP. Un positionnement sur 0 désactive cette fonction.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Les règles implicites autorisent le trafic IKE et ESP en provenance du correspondant distant.

➤ SECURITY POLICY / IMPLICIT RULES

IMPLICIT FILTER RULES

Enabled	Name
<input checked="" type="checkbox"/> Enabled	Allow access to the PPTP server
<input checked="" type="checkbox"/> Enabled	Allow mutual access between the members of a firewall cluster (HA)
<input checked="" type="checkbox"/> Enabled	Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers.
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's DNS service (port 53).

Pour les tunnels VPN IPsec site-à-site configurés avec des adresses statiques de correspondants, des règles implicites sont ajoutées automatiquement lors de la création du tunnel de façon à pouvoir recevoir le trafic constituant un tunnel VPN IPsec : les ports UDP/500, UDP/4500 et le protocole ESP.

Ces règles ne concernent que les flux entrants car les flux sortants sont déjà couverts par les règles flux implicites du Firewall.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Règles de filtrage **explicites** pour autoriser le trafic entre les extrémités de trafic (les réseaux distants)

SECURITY POLICY / FILTER - NAT

(9) Pass all High Edit Export

FILTERING NAT

Searching...	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_in	NET_IN_B	Any		IPS
2	on	pass	via IPsec VPN tunnel	Network_in	Any		IPS

EDITING RULE NO 2

General Action Source Destination Port - Protocol Inspection

SOURCE

GENERAL GEOLOCATION / REPUTATION ADVANCED PROPERTIES

Advanced properties

Source port: Any

Via: IPsec VPN tunnel

STORMSHIELD 21

Le trafic autorisé entre les usagers du tunnel doit être explicitement défini par des règles de filtrage :

- La première règle permet l'initiation de connexions à partir du réseau local Network\_in et à destination du réseau distant NET\_IN\_B.
- La deuxième règle permet, quant à elle, l'initiation de connexions à partir du réseau distant NET\_IN\_B à destination du réseau local Network\_in. La directive **via Tunnel VPN IPsec** a été ajoutée à la source de cette règle pour s'assurer que le trafic du réseau distant provient bien du tunnel VPN IPsec.

**NOTE** : ces règles sont très permissives puisqu'elles ne spécifient pas de flux particuliers ; en situation réelle, il convient de définir une politique de filtrage qui décrit strictement les flux à autoriser afin de couvrir rigoureusement les communications nécessaires entre les différentes machines des deux sites.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- Logs de la négociation IKE

The screenshot shows the Stormshield VPN logs interface. The main log table displays several entries, with the first one highlighted in green. A red box highlights the SPI in and SPI out columns for this entry. A blue arrow points from the SPI out column to the 'LOG LINE DETAILS' panel, which provides a comprehensive view of the log entry's configuration, dates, destination, and message.

Saved at	Message	User	Local network	Destination Name	Source Name	Remote net...	P...	Side	SPI in	SPI out
07/24/2021 10:52:1...	IPSEC SA established		10.0.0.0/24	Remote_peer	Firewall_out	172.29.1.0/24	2	initiator	0xc39cc488	0xc636ed95
07/24/2021 10:52:1...	IKE SA established			Remote_peer	Firewall_out			1	initiator	
07/24/2021 10:52:1...	Charon daemon started									
07/24/2021 10:52:1...	Charon configuration reloaded									
07/24/2021 10:52:1...	Reloading charon configuration									

LOG LINE DETAILS	
<b>Configuration</b>	
Rule name	049ec7261960d1bd4b5854fbf1468...
Rule type	gateway
<b>Dates</b>	
Saved at	07/24/2021 10:52:15 AM
Date and time	07/24/2021 10:52:15 AM
Time difference between local time ...	+0000
<b>Destination</b>	
Destination Name	Remote_peer
Destination	172.18.18.1
Remote network	172.29.1.0/24
Remote identifier	172.18.18.1
<b>Message</b>	
Message	IPSEC SA established

Le menu **TRACES** ⇒ **VPN** affiche les événements relatifs au déroulement de la négociation IKE. Les extrémités de trafic qui ont provoqué les négociations et pour lesquelles le tunnel est disponible apparaissent explicitement sur la ligne de log concernant la négociation de phase 2.

Dans le cadre d'un diagnostic, en particulier en cas de message d'erreur ou d'avertissement, il est essentiel de relever la phase de négociation pour laquelle les messages sont rapportés.

Les colonnes affichées ci-dessus ont volontairement été limitées au minimum nécessaire à l'exemple. Apparaissent notamment les colonnes SPI in et SPI out. Les SPI (Security Parameter Index) sont des valeurs sur 32 bits en forme hexadécimale permettant d'identifier les SA IPsec entrantes (in) et sortantes (out). Sur le correspondant, ces valeurs sont donc les mêmes mais sont inversées (la valeur de SPI in correspond à celle de SPI out et inversement).

Davantage d'informations, plus techniques, peuvent être affichées en cliquant sur la flèche qui se trouve dans l'en-tête de colonnes, puis sélectionnant les colonnes supplémentaires souhaitées.

## VPN IPSEC - CONFIGURATION D'UN TUNNEL SITE-À-SITE

- La politique VPN IPSEC

MONITOR / IPSEC VPN TUNNELS

Refresh Configure the IPsec VPN service

POLICIES

Type	Status	Local traffic endpoint	Local gateway	Local ID	Remote gateway	Peer ID	Remote traffic endpoint
Type: Site-to-site tunnels (2)							
OK	OK	Network_in	Firewall_out	172.18.18.14	Remote_peer	172.18.18.1	remote_net
No tunnels	No tunnels	Network_in	Firewall_out	172.18.18.14	remote-gre	92.61.113.70	remote_net
Type: Exception policies (bypass) (1)							
Bypass		rfc5735_loopback					any

Security Association (SA) IKE

Status:	established	Local ID:	172.18.18.14	Authentication:	sha2_256
Local gateway:	Firewall_out	Peer ID:	172.18.18.1	Encryption:	aes/256
Remote gateway:	Remote_peer	Lifetime lapsed:	14m	PRF:	sha256
Side:	responder	NAT-T:	none	PFS:	14

Security Association (SA) IPsec

Status:	installed	Bytes in:		Authentication:	hmac_sha256
Local gateway:	Firewall_out	Bytes out:	4.43 KB	Encryption:	aes/256
Remote gateway:	Remote_peer	Lifetime lapsed:	14m	ESN:	<input checked="" type="checkbox"/> Enabled
				UDP encapsulation:	<input type="checkbox"/> Disabled

23

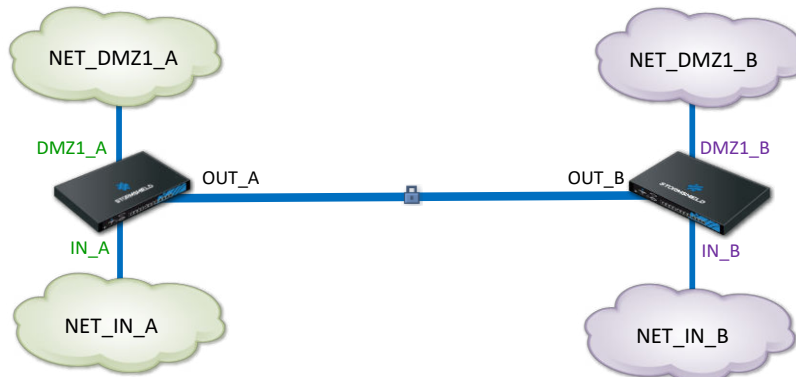
Le menu **Supervision** ⇒ **Tunnels VPN IPsec** permet de visualiser la politique VPN IPsec active sur le firewall.

La section **Tunnels** permet, de superviser les tunnels disponibles. L'âge actuel des SA et les algorithmes retenus lors des négociations apparaissent.



- Les différents réseaux privés virtuels
- VPN IPsec – Concepts et généralités
- VPN IPsec – Configuration de tunnel site-à-site
- ➔ **VPN IPsec – Configuration de tunnels site-à-site multiples**
- VPN IPsec – Virtual Tunneling Interface
- Lab - VPN IPsec (site à site)

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES



L'objectif est de configurer une politique VPN IPsec pour autoriser la communication entre les réseaux locaux IN et DMZ1 des deux sites. Cette configuration peut se faire suivant deux méthodes :

1. Une règle par paire de réseaux à relier.
2. Une seule règle pour tous les réseaux en utilisant les groupes.

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES

LOG / VPN

Last hour Refresh Search... Advanced search

SEARCH FROM - 08/25/2021 05:38:01 PM - TO - 08/25/2021 06:38:01 PM

Message	Local network	Destination Name	Source Name	Remote network	IKE version	Phase	Side
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	172.16.2.0/24	1		
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	192.168.2.0/24	1		
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	172.16.2.0/24	1		
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	192.168.2.0/24	1		

SPI in

SPI out

Message	Local network	Destination Name	Source Name	Remote network	IKE version	Side	SPI in	SPI out
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	172.16.2.0/24	1	Initiator	0xc5cce844	0xc4c69df0

Selon la méthode choisie, le nombre de tunnels pourra être différent en IKEv1 et IKEv2.

Pour mettre ce point en évidence, il faut faire apparaître les colonnes SPI in et out dans les logs VPN.

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES

## 1. Une règle par paire de réseaux à relier

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

IPsec 01 (01) Actions ⓘ

SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS

Enter a filter + Add X Delete ↑ Up ↓ Down Cut Copy Paste Show details

	Status	Local network	Peer	Remote network	Encryption profile	Keep alive
1	on	Network_in	Site_FW_B	Net_in_B	StrongEncryption	30
2	on	Network_in	Site_FW_B	Net_DMZ_B	StrongEncryption	30
3	on	Network_dmz	Site_FW_B	Net_in_B	StrongEncryption	30
4	on	Network_dmz	Site_FW_B	Net_DMZ_B	StrongEncryption	30

STORMSHIELD 27

La première méthode consiste à éditer une règle par paire de réseaux à relier.

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES

Nombre de tunnels identique pour IKEv1 :

LOG / VPN							
Last hour		Refresh		Search...		Advanced search	
SEARCH FROM - 10/31/2022 03:41:05 PM - TO - 10/31/2022 04:41:05 PM							
Message	Local network	Destination Name	Remote netw...	SPI in	SPI out	IKE version	
IPSEC SA established	172.16.1.0/24	FW_B	172.16.2.0/24	0xc61997c2	0xc8a38055	1	
IPSEC SA established	192.168.1.0/24	FW_B	172.16.2.0/24	0xc77ec00d	0xc6a668b2	1	
IPSEC SA established	172.16.1.0/24	FW_B	192.168.2.0/24	0xc760cf07	0xc204ec67	1	
IPSEC SA established	192.168.1.0/24	FW_B	192.168.2.0/24	0xc149202f	0xc19f2aeb	1	

et IKEv2 (les SPI sont différents) :

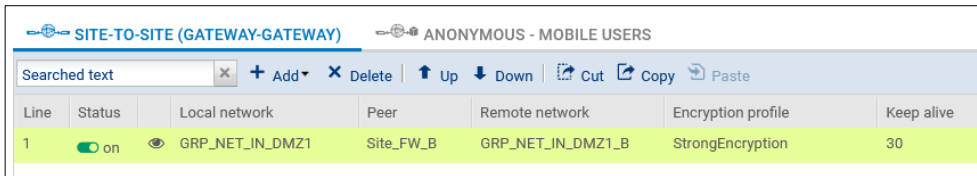
LOG / VPN							
Last hour		Refresh		Search...		Advanced search	
SEARCH FROM - 10/31/2022 02:13:54 PM - TO - 10/31/2022 03:13:54 PM							
Message	Local network	Destination Name	Remote netw...	SPI in	SPI out	IKE version	
IPSEC SA established	172.16.1.0/24	FW_B	172.16.2.0/24	0xc1f10d837	0xc1577535	2	
IPSEC SA established	192.168.1.0/24	FW_B	172.16.2.0/24	0xc8a792a0f	0xc1148ccc	2	
IPSEC SA established	172.16.1.0/24	FW_B	192.168.2.0/24	0xc52c4f15	0xc17a3bca	2	
IPSEC SA established	192.168.1.0/24	FW_B	192.168.2.0/24	0xca56332c	0xc32aea49	2	

28

Dans ce cas, la politique chargée sera identique quelle que soit la version du protocole IKE utilisée, et elle engendrera quatre tunnels distincts, c'est-à-dire quatre paires d'IPsec-SA, reconnaissables par les 4 paires de SPI.

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES

## 2. Une règle pour tous les réseaux en utilisant des groupes



The screenshot shows a configuration window for 'SITE-TO-SITE (GATEWAY-GATEWAY)'. It features a search bar and a table with the following data:

Line	Status	Local network	Peer	Remote network	Encryption profile	Keep alive
1	on	GRP_NET_IN_DMZ1	Site_FW_B	GRP_NET_IN_DMZ1_B	StrongEncryption	30

La deuxième méthode consiste à n'éditer qu'une seule règle pour l'ensemble des réseaux regroupés dans un groupe. Cette configuration est plus concise et donc plus lisible à condition d'adopter, pour le nommage des groupes, une nomenclature rigoureuse et suffisamment descriptive afin d'éviter toute ambiguïté et tout risque de confusion lors d'une relecture ultérieure.

## VPN IPSEC - CONFIGURATION DE TUNNELS SITE-À-SITE MULTIPLES

Différents tunnels pour IKEv1 (les SPI sont différents) :

LOG / VPN									
Last hour Refresh Search... Advanced search									
SEARCH FROM - 08/25/2021 05:38:01 PM - TO - 08/25/2021 06:38:01 PM									
Message	Local network	Destination Name	Source Name	Remote network	IKE version	Side	SPI in	SPI out	
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	172.16.2.0/24	1	initiator	0xc5c0e844	0xc4c69df0	
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	192.168.2.0/24	1	initiator	0xcfe5af29	0xc482196c	
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	172.16.2.0/24	1	initiator	0xcb6700e6	0xca79293d	
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	192.168.2.0/24	1	initiator	0xc6975d4d	0xc5230f61	

Même tunnel pour IKEv2 (les SPI sont identiques) :

LOG / VPN									
Last hour Refresh Search... Advanced search									
SEARCH FROM - 08/25/2021 05:53:23 PM - TO - 08/25/2021 06:53:23 PM									
Message	Local network	Destination Name	Source Name	Remote network	IKE version	Side	SPI in	SPI out	
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	192.168.2.0/24	2	initiator	0xc3ab0967	0xc5de2d3b	
IPSEC SA established	172.16.1.0/24	Remote_peer	Firewall_out	172.16.2.0/24	2	initiator	0xc3ab0967	0xc5de2d3b	
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	192.168.2.0/24	2	initiator	0xc3ab0967	0xc5de2d3b	
IPSEC SA established	10.0.0.0/24	Remote_peer	Firewall_out	172.16.2.0/24	2	initiator	0xc3ab0967	0xc5de2d3b	

Elle engendre un nombre de tunnels différent selon la version du protocole IKE :

- IKEv1 : Quatre tunnels, ce qui est identique à la première configuration.
- IKEv2 : Un tunnel unique, qui servira à faire transiter l'ensemble des communications entre ces différents réseaux. Ce comportement est parfois qualifié de « SharedSA ».

**ATTENTION** : il sera ainsi impératif d'harmoniser la méthode de configuration des politiques pour les tunnels négociés en IKEv2 entre firewalls SNS.

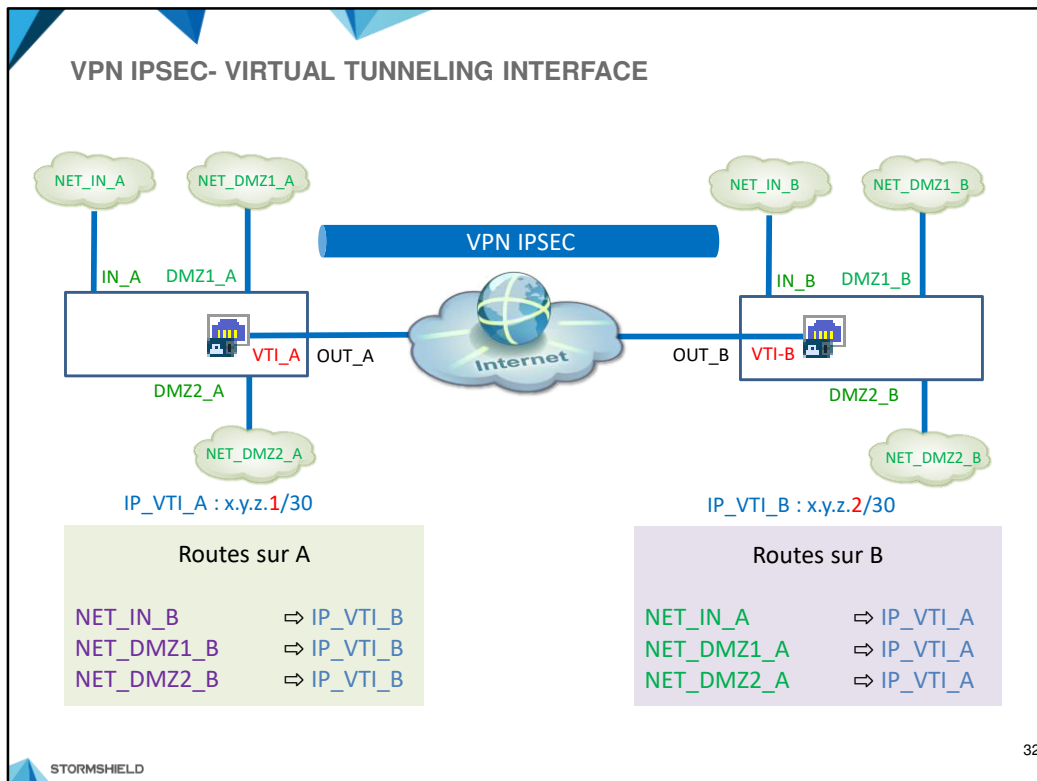


- Les différents réseaux privés virtuels
- VPN IPsec – Concepts et généralités
- VPN IPsec – Configuration de tunnel site-à-site
- VPN IPsec – Configuration de tunnels site-à-site multiples



## **VPN IPsec – Virtual Tunneling Interface**

- Lab - VPN IPsec (site à site)



Une autre approche est rendue possible par l'utilisation d'interfaces **VTI** dédiées à un tunnel IPsec.

Ces **interfaces** IPsec particulières constitueront les **points de passage des flux** en entrée et en sortie de tunnel IPsec. **Elles** agiront comme une **passerelle** l'une envers l'autre pour acheminer les flux entre les réseaux au travers du tunnel IPsec.

Les avantages de cette approche résident dans :

- L'indépendance de la politique IPsec vis-à-vis des adresses IP des usagers du tunnel et des flux à prendre en charge.
- La souplesse et la précision dans la **sélection des flux** à envoyer dans le tunnel.
- La limitation à un seul tunnel (et donc à **une seule négociation de phase 2**) quel que soit le nombre de réseaux IP à relier entre eux.

Les diapositives suivantes détaillent les étapes qui permettent de configurer un tunnel VPN IPsec site-à-site en utilisant les interfaces VTI.

#### **Priorité entre correspondance de politique et routage sur VTI :**

Le routage sur VTI est prioritaire sur la correspondance de politique. C'est-à-dire, si une politique VPN IPsec contient deux tunnels servant à relier les mêmes réseaux, un défini par la correspondance de politique et un deuxième utilisant le routage sur VTI, les paquets seront transmis via le deuxième tunnel.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Comparatif

Paramètre	VPN par politique	VPN par route (VTI)
Maintient de la SA	Tant que du trafic correspond à la politique	Tant que les vti sont actives
Compatibilité avec le routage dynamique	Non	Oui
Compatibilité multi-éditeur	Oui	Non
Addition d'une nouvelle extrémité de trafic distante à joindre de manière sécurisée	Nécessite la création d'un nouveau tunnel	Nécessite l'ajout d'une route via le tunnel existant
Cas d'usage	<ul style="list-style-type: none"> <li>VPN IPsec avec des éditeurs tierce partie</li> <li>Une seule extrémité de trafic sur le réseau distant</li> </ul>	<ul style="list-style-type: none"> <li>Répartition de charge avec objet routeur</li> <li>Tolérance aux pannes par l'usage de routage dynamique</li> <li>Multiples extrémités de trafic</li> </ul>

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Création des interfaces VTI sur chacun des correspondants

Création la VTI sur le correspondant A

NETWORK / VIRTUAL INTERFACES				
IPSEC INTERFACES (VTI)		GRE INTERFACES	LOOPBACK	
Status	Name ↑	IPv4 address	IPv4 mask	
Enabled	VTI_A	172.25.255.1	255.255.255.252	

OBJECTS / NETWORK OBJECTS			
Firewall_VTI_A			
Filter: All objects			
+ Add	× Delete	Check usage	Export Import
Type	Usage	Name	Value
Type: Hosts (1)			
●		Firewall_VTI_A	172.25.255.1 / static

Création de la VTI sur le correspondant B

NETWORK / VIRTUAL INTERFACES				
IPSEC INTERFACES (VTI)		GRE INTERFACES	LOOPBACK	
Status	Name ↑	IPv4 address	IPv4 mask	
Enabled	VTI_B	172.25.255.2	255.255.255.252	

OBJECTS / NETWORK OBJECTS			
Firewall_VTI_B			
Filter: All objects			
+ Add	× Delete	Check usage	Export Import
Type	Usage	Name	Value
Type: Hosts (1)			
●		Firewall_VTI_B	172.25.255.2 / static

STORMSHIELD

34

Les interfaces VTI créées sur les deux correspondants portent chacune un nom commun et une adresse IP du même plan d'adressage :

- Sur le correspondant A : la VTI est nommée « VTI\_A » et son IP est 172.25.255.1/30.
- Sur le correspondant B : la VTI est nommée « VTI\_B » et son IP est 172.25.255.2/30.

Pour éviter toute ambiguïté avec l'architecture existante et ses futures évolutions, il convient de choisir un plan d'adressage dédié à l'usage des VTI, dans une plage officiellement privée et suffisamment originale pour ne pas entrer en collision avec un réseau déjà existant ou le réseau distant d'une interconnexion future.

NOTE : Depuis la V3.3.0, il est possible d'utiliser un réseau en /31 qui convient mieux aux interfaces point-à-point car elles n'utilisent pas les adresses réseau et broadcast.

Les noms communs de ces interfaces seront automatiquement associés à un objet machine implicite, sur chacun des correspondants :

- Sur le correspondant A : Firewall\_VTI\_A.
- Sur le correspondant B : Firewall\_VTI\_B.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Création de l'objet machine qui porte l'adresse IP de l'interface VTI du correspondant distant

Sur A, création de l'objet machine qui porte l'adresse IP de l'interface VTI\_B

OBJECTS / NETWORK OBJECTS

IP\_VTI\_B

Filter: All objects

+ Add X Delete Check usage Export Import

Type	Usage	Name	Value
Type : Hosts (1)			
		IP_VTI_B	172.25.255.2 / static

Sur B, création de l'objet machine qui porte l'adresse IP de l'interface VTI\_A

OBJECTS / NETWORK OBJECTS

IP\_VTI\_A

Filter: All objects

+ Add X Delete Check usage Export Import

Type	Usage	Name	Value
Type : Hosts (1)			
		IP_VTI_A	172.25.255.1 / static

Sur chacun des firewalls, il faut également créer l'objet portant l'adresse IP de la VTI du correspondant distant.

Comme pour tous les objets, il est judicieux de définir une nomenclature rigoureuse en utilisant des noms évocateurs. Cette bonne pratique facilite l'utilisation des VTI sur des architectures VPN IPsec aux correspondants multiples.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Définition de la politique VPN IPsec basée sur les VTI

- Sur le correspondant A

SITE-TO-SITE (GATEWAY-GATEWAY)		ANONYMOUS - MOBILE USERS			
Line	Status	Local network	Peer	Remote network	Encryption profile
1	on	Firewall_VTI_A	Site_FW_B	IP_VTI_B	StrongEncryption

- Sur le correspondant B

SITE-TO-SITE (GATEWAY-GATEWAY)		ANONYMOUS - MOBILE USERS			
Line	Status	Local network	Peer	Remote network	Encryption profile
1	on	Firewall_VTI_B	Site_FW_A	IP_VTI_A	StrongEncryption

Les objets correspondants aux adresses IP des VTI sont définies comme extrémités de trafic du tunnel. Au contraire des configurations IPsec basées sur la correspondance de politique, ce ne sont pas exclusivement les flux de communication entre les deux adresses IP des interfaces VTI qui sont pris en charge par IPsec, mais tout flux qui passe par ces interfaces grâce aux directives de routage.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Définition des routes pour les flux usagers du tunnel  
**routes statiques**
  - Sur le correspondant A

**STATIC ROUTES**

Searching... [+ Add](#) [X Delete](#)

Status	Destination network (host, network or group object)	Interface ↓	Address range	Gateway
<input checked="" type="checkbox"/> on	NET_DMZ1_B	VTLA	172.16.2.0/24	IP_VTLB
<input checked="" type="checkbox"/> on	NET_IN_B	VTLA	192.168.2.0/24	IP_VTLB

- Sur le correspondant B

**STATIC ROUTES**

Searching... [+ Add](#) [X Delete](#)

Status	Destination network (host, network or group object)	Interface ↓	Address range	Gateway
<input checked="" type="checkbox"/> on	NET_DMZ1_A	VTLB	172.16.1.0/24	IP_VTLA
<input checked="" type="checkbox"/> on	NET_IN_A	VTLB	192.168.1.0/24	IP_VTLA

Dans ce mode de fonctionnement, il est essentiel de veiller à ce que le routage des paquets retour coïncide avec le tunnel emprunté par les paquets aller. Ci-dessous, les routes statiques indiquent globalement sur chaque correspondant que les réseaux distants sont joignables par le même tunnel.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Définition des routes pour les flux usagers du tunnel  
**Routage par politique**
  - Une règle de filtrage avec PBR désigne comme passerelle la VTI du correspondant distant :

FILTERING		NAT				
Searching...						
	Status	Action	Source	Destination	Dest. port	
1	on	pass Route: IP_VTI_B	Network_in	NET_IN_B	ssh	

- La définition de la route de retour est impérative

IPV4 STATIC ROUTES	IPV4 DYNAMIC ROUTING	IPV4 RETURN ROUTES
RETURN ROUTES		
Searching...		
+ Add X Delete		
Status	Gateway	Interface
on	IP_VTI_B	VTI_A

L'usage de directives de routage par politique (PBR), impose également de gérer le routage des paquets retour par le même tunnel.

C'est pourquoi, il est nécessaire de définir la route retour par la VTI correspondant au tunnel par lequel les paquets aller sont arrivés.

Ces directives doivent être appliquées sur les deux correspondants si les communications dans le tunnel peuvent être initiées indifféremment par des réseaux côté A vers des réseaux côté B et inversement.

## VPN IPSEC- VIRTUAL TUNNELING INTERFACE

- Autorisation du trafic entre les deux réseaux distants

The screenshot displays the Stormshield NAT configuration interface. At the top, there is a 'FILTERING' tab and a 'NAT' sub-tab. Below this is a search bar and a toolbar with options like '+ New rule', 'Delete', 'Cut', 'Copy', and 'Paste'. A table lists two NAT rules:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_in	NET_IN_B	Any		IPS
2	on	pass	NET_IN_B interface: VTI_A	Network_in	Any		IPS

Below the table is a dialog box titled 'EDITING RULE NO 2'. The 'SOURCE' tab is selected, and the 'GENERAL' sub-tab is active. The 'Incoming interface' field is set to 'VTI\_A' and is highlighted with a blue box. A blue arrow points from the 'interface: VTI\_A' text in the table above to this field in the dialog.

STORMSHIELD 39

Avec les interfaces VTI, la directive **via Tunnel VPN IPsec** ne doit pas être utilisée. À sa place, il faut utiliser l'interface VTI comme interface d'entrée dans la règle autorisant le trafic entrant depuis le tunnel.

## RECOMMANDATIONS



- Utiliser des algorithmes robustes pour IKE et IPsec
- Utiliser IKEv2
  - ↓ A défaut utiliser le mode MAIN de IKEv1
- Utiliser des authentifications par certificat
  - ↓ A défaut utiliser des PSK robustes
- Configurer KeepAlive
- Désactiver PPTP

Il est fortement déconseillé d'employer la fonction de hachage MD5, le chiffrement DES, des clés RSA de taille inférieure à 2048 bits ou des clés ECDSA de taille inférieure à 200bits.

Il est déconseillé d'utiliser 3DES, SHA-1 ou ECDSA avec des clés de moins de 256 bits si des alternatives plus sécurisées telles qu'AES, SHA-2 ou ECDSA avec des clés d'au moins 256 bits sont disponibles.

Attention au groupe de Diffie-Hellman employé. On privilégiera les groupes de modules de taille importante (comme 14 et 15) voire les groupes construits sur des courbes elliptiques d'au moins 256bits.

Pour éviter de perdre des paquets parce qu'un tunnel n'est pas encore établi, il est recommandé d'activer Keepalive qui maintiendra le tunnel monté.

PPTP est un protocole largement obsolète et ne doit plus être utilisé.



Pour aller plus loin, consultez les ressources du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Interfaces virtuelles IPsec
  - Intégration du NAT dans IPsec
  - VPN IPsec Mobile IKEv1 - Authentification par clé pré-partagée
  - VPN IPsec Mobile IKEv2 - Authentification par clé pré-partagée
  - VPN IPsec - Authentification par clé pré-partagée
  - VPN IPsec : Authentification par certificats
  - VPN IPsec : Configuration Hub and Spoke
  - VPN IPsec - Mode Diffusion Restreinte
- 
- Guide d'utilisation SN VPN Client Standard
  - Guide de l'administrateur SN VPN Client Exclusive

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Les différents réseaux privés virtuels
- VPN IPSec – Concepts et généralités
- VPN IPSec – Configuration de tunnel site-à-site
- VPN IPSec – Configuration de tunnels site-à-site multiples
- VPN IPSec – Virtual Tunneling Interface

➔ **Lab - VPN IPsec (site à site)**



## Lab 8 – VPN IPsec (Site à site)

Copiez la politique de filtrage/NAT **(7) Lab\_7** vers la politique numéro 8. Renommez la politique numéro 8 « Lab\_8 », puis activez cette politique.

1. Ajoutez une règle de filtrage **Pass any any any** en tête de cette politique.
2. Configurez un tunnel IPsec avec une authentification par PSK pour relier votre réseau interne « 192.168.x.0/24 » à celui de l'autre entreprise en utilisant les profils de chiffrement par défaut (StrongEncryption).
3. Générez du trafic correspondant aux extrémités de trafic et suivez les étapes de négociation des tunnels et l'activité dans les tunnels depuis les journaux et le menu de supervision correspondants.
4. Modifiez vos politiques IPsec pour relier cette fois vos deux réseaux Internes (IN + DMZ) aux réseaux internes (IN + DMZ) de l'autre entreprise.
  - Activez la fonction keep-alive sur votre tunnel.
  - Regardez le nombre de tunnels négociés dans la supervision.
5. Après avoir vérifié que vos tunnels sont fonctionnels, désactivez la règle de filtrage **Pass any any any** et ajoutez les règles autorisant les réseaux du site distant à joindre à pinger vos réseaux locaux et à joindre vos serveurs FTP et WEB.
6. Créez les profils de chiffrement suivants :
  - IKE Phase 1 : Diffie-Hellman (DH15 MODP), Durée de vie maximum (21600s), algorithme d'authentification (sha2\_512) et algorithme de chiffrement (AES 256bits).
  - IPSEC Phase 2 : PFS (DH15 MODP), durée de vie (3600s), algorithme d'authentification (hmac\_sha512) et algorithme de chiffrement (AES 256bits).
7. Appliquez vos nouveaux profils de chiffrement sur votre VPN. Puis vérifiez que tout fonctionne correctement.
8. Réalisez l'interconnexion de ces mêmes réseaux, mais en configurant des tunnels basés sur des VTI. Avec au choix du routage statique ou par politique (PBR).





# Quiz

STORMSHIELD

Q1 – IPsec utilise TCP pour négocier la connexion, puis se envoie les données chiffrées grâce à UDP :

- A. Vrai
- B. Faux

Q2 – SHA1 est un algorithme de hachage sûr pour les tunnel VPN :

- A. Vrai
- B. Faux

Q3 – Les VTI font partie du standard IKEv2 et ne sont pas disponibles sur IKEv1 :

- A. Vrai
- B. Faux

Q4 – Un tunnel IPsec garantit :

- A. L'authentification
- B. La qualité de service
- C. L'intégrité
- D. La confidentialité
- E. L'anti-rejeu
- F. La réception

Q5 – L'option keepalive permet au pare-feu de détecter des coupures de connexion :

- A. Vrai
- B. Faux



Q6 – La négociation d'un tunnel IPsec est initiée seulement s'il y a des données à envoyer dans le tunnel :

- A. Vrai
- B. Faux

Q7 – Sans VTI, il est impossible de faire fonctionner deux tunnels entre les mêmes réseaux simultanément (pour un besoin de redondance par exemple) :

- A. Vrai
- B. Faux

Q8 – Une route statique est nécessaire pour que le firewall puisse envoyer les paquets dans un tunnel IPsec :

- A. Vrai dans tous les cas
- B. Vrai seulement avec des VTI
- C. Vrai seulement avec de la correspondance de politique (tunnel IPsec standard)
- D. Faux dans tous les cas



STORMSHIELD

# ANNEXE – VIRTUAL PRIVATE NETWORK

CSNA - STORMSHIELD NETWORK SECURITY - VERSION 4.X



1

Cette annexe propose du contenu pédagogique complémentaire qui n'est pas évalué dans les examens de certification Stormshield.



## Point-to-Point Tunneling Protocol

- VPN IPsec – Correspondant dynamique

STORMSHIELD

Virtual Private Network

**PPTP: CONCEPTS**

- **Point-to-Point Tunneling Protocol**
  - Client natif sur tout système Microsoft
  - Canal de contrôle sur TCP/1723 et encapsulation dans GRE (n°47)
  - Authentification MS-CHAP
  - Chiffrement MPPE 40,56,128 bits
  
  - Type PPP : le client crée dynamiquement une interface de type PPP qui porte une adresse IP du LAN à rejoindre
  - Un serveur DNS et un serveur WINS peuvent également être désignés comme associés à cette interface PPP

**CETTE SOLUTION EST OBSOLÈTE**

## PPTP : PARAMÉTRAGE DU SERVICE

- L'objet **Host\_group** décrit des hôtes appartenant au même plan d'adressage que l'une des interfaces du firewall, il peut aussi s'agir d'une plage d'adresses.
- Les **serveurs DNS et WINS** désignés seront livrés au client à l'établissement de la connexion.

**VPN / PPTP SERVER**

Enable PPTP server

IP addresses of PPTP clients (object):

Parameters sent to PPTP clients

DNS server:

WINS server:

Advanced properties

Traffic encryption

Do not encrypt

Accept only encrypted traffic and allow the following algorithms

40-bit MPPE

56-bit MPPE

128-bit MPPE

STORMSHIELD

4

La plage d'adresses allouée aux clients PPTP doit impérativement être dédiée à cet usage; aucune machine du LAN ne doit porter une de ces adresses car cela aboutirait à un conflit d'adresse IP sur le LAN.

## PPTP : DROIT DES UTILISATEURS ET MOT DE PASSE

- Les utilisateurs autorisés à utiliser PPTP sont désignés un à un dans les UAC VPN.
- Un mot de passe dédié à la connexion PPTP leur est affecté.

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS   DETAILED ACCESS   **PPTP SERVER**

Searching...   + Add   x Delete   |   Change password

PPTP username

sponge.bob

**ENTER THE PASSWORD FOR THIS USER**

Please enter a password:

Confirm password:

Excellent

STORMSHIELD

5

Le mot de passe PPTP est indépendant du mot de passe que l'utilisateur présenterait au portail dans le cadre d'une simple authentification.

En conséquence, dans le cas où le firewall s'appuierait sur un LDAP de type Active Directory ou plus généralement un LDAP externe, le mot de passe PPTP n'est pas synchronisé avec le mot de passe d'authentification de l'utilisateur.



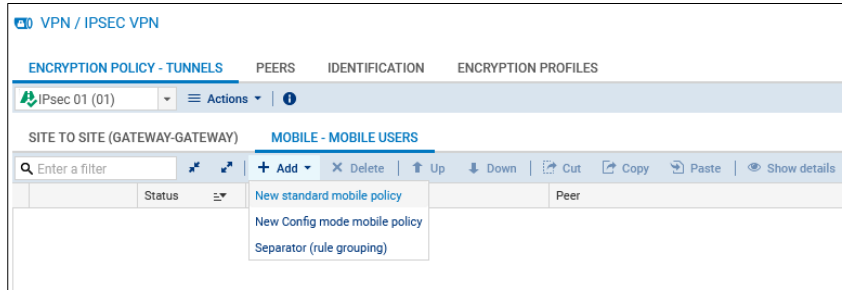
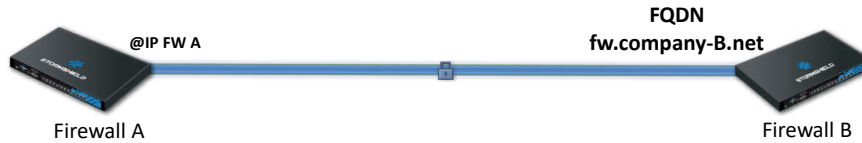
- Point-to-Point Tunneling Protocol
- ➔ **VPN IPsec – Correspondant dynamique**

STORMSHIELD

Virtual Private Network

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Configuration d'un tunnel anonyme



STORMSHIELD

7

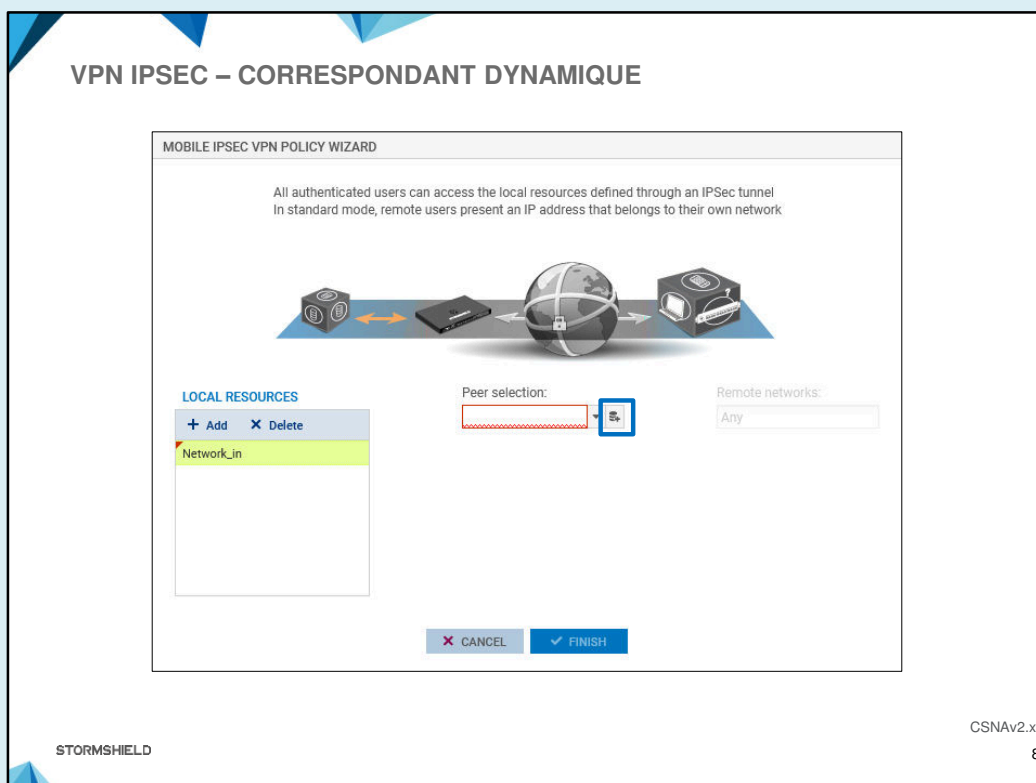
Dans l'exemple ci-dessus, le Firewall B possède une adresse IP dynamique, ce qui rend la configuration d'un tunnel site-à-site impossible sur le Firewall A.

Pour adresser ce cas de figure, un **Tunnel anonyme** peut être configuré sur le Firewall A qui vérifie l'identité du Firewall B en utilisant un nom DNS de type FQDN de ce dernier, associé à une PSK. De l'autre côté, le Firewall B configure un tunnel site-à-site classique car le firewall A possède une adresse IP fixe. Ainsi, il est clair que c'est le Firewall B qui initiera le tunnel VPN IPsec.

La configuration du tunnel anonyme s'effectue via un assistant depuis l'onglet **ANONYME – UTILISATEURS NOMADES**, en cliquant sur le bouton **Ajouter ⇒ Nouvelle politique**.



## VPN IPSEC – CORRESPONDANT DYNAMIQUE



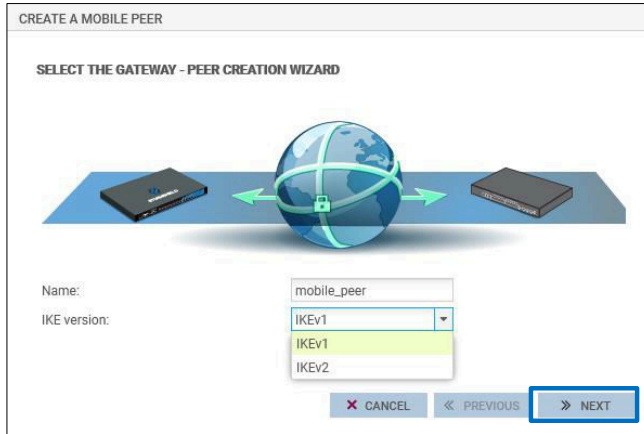
Dans l'assistant de création, les extrémités de tunnels et de trafic distantes sont indéfinies, d'où la dénomination couramment employée de **Tunnels Anonymes**. Seule l'extrémité de trafic locale doit être sélectionnée. Ci-dessus, les machines à rendre joignables par IPsec sont localisées sur **Network\_in**.

L'extrémité de trafic distante est prédéfinie sur **Tous** par l'assistant (encadré bleu). Elle est supposée être imprévisible car, pour le cas des nomades, elle dépend de ce que le client présentera pendant la phase 2 en fonction de sa configuration et du réseau dans lequel il se trouve au moment de la négociation. **Tous** a donc comme signification **Any** en tant qu'entité IP indéfinie; c'est-à-dire n'importe quelle adresse ou plan d'adressage.

Pour configurer des correspondants distants (**nomades**), cliquez sur le bouton **Ajouter**. Un assistant se lance pour créer cette configuration.

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Création d'une configuration pour les correspondants dynamiques



STORMSHIELD

9

Deux fenêtres successives de l'assistant sont présentées ci-dessus. elles permettent de :

- Choisir un nom pour les correspondants dynamiques, remarquez que le préfixe « mobile\_ » est déjà ajouté par le firewall.
- Sélectionner la version IKE.



## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Création d'une configuration pour les correspondants dynamiques

CREATE A MOBILE PEER

**PEER IDENTIFICATION - PEER CREATION WIZARD**

Authentication type:

- Certificate
- Certificate and Xauth (iPhone)
- Pre-shared key (PSK)

- Pour sélectionner l'authentification PSK, cliquez sur **Suivant** puis sur le bouton **Ajouter** pour indiquer la PSK

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Ajout de l'identité du correspondant et de la clé pré-partagée associée

The screenshot displays the 'CREATE A MOBILE PEER' configuration window. The 'IDENTIFICATION SETTINGS' section is active, specifically the 'MOBILE TUNNELS: PRE-SHARED KEYS (PSK)' area. A table with columns 'Identity' and 'Key' is shown. A '+ Add' button is highlighted, and a blue arrow points to it. Another blue arrow points from the 'Add' button to the 'EDITING THE KEY' dialog box. This dialog box contains the following fields:

- User ID (IP address, FQDN or e-mail address): fw.company-B.net
- Pre-shared key (ASCII): [masked]
- Confirm: [masked]
- Enter the key in ASCII characters:

Buttons for 'CANCEL' and 'APPLY' are visible. A third blue arrow points from the 'APPLY' button to a table below. This table shows the result of the configuration:

Identity	Key
fw.company-B.net	0x4c65744d6543686f6f73655374...

The 'STORMSHIELD' logo is visible in the bottom left corner of the screenshot area, and the number '11' is in the bottom right corner.

Ajouter l'identité d'un correspondant dynamique (un firewall dont l'IP est dynamique). L'identité **fw.company-B.net** est de type FQDN (Fully Qualified Domain Name) d'ordinaire un nom d'hôte pleinement qualifié. Le FQDN est associé à une PSK.

### VPN IPSEC – CORRESPONDANT DYNAMIQUE

The screenshot displays two overlapping configuration windows in the Stormshield interface. The background window is titled "CREATE A MOBILE PEER" and contains a "SUMMARY - PEER CREATION WIZARD" section. It shows the "Mobile peer" name as "mobile\_peer" and a "Peer identification: pre-shared keys" section with a note: "Pre-shared keys are listed in the identification tab of the IPsec VPN module". At the bottom of this window are buttons for "CANCEL", "PREVIOUS", and "FINISH". The "FINISH" button is highlighted with a blue box, and a blue arrow points from it to the "FINISH" button of the foreground window.

The foreground window is titled "MOBILE IPSEC VPN POLICY WIZARD". It contains the text: "All authenticated users can access the local resources defined through an IPsec tunnel. In standard mode, remote users present an IP address that belongs to their own network." Below this text is a diagram showing a globe connected to two server racks. The "LOCAL RESOURCES" section lists "Network\_in" with "+ Add" and "X Delete" options. The "Peer selection:" dropdown is set to "mobile\_peer", and the "Remote networks:" field is set to "Any". At the bottom of this window are buttons for "CANCEL" and "FINISH".

STORMSHIELD

12

Finaliser les configurations des correspondants et du tunnel.

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Activer la politique :

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS		PEERS	IDENTIFICATION	ENCRYPTION PROFILES						
IPsec D1 (01)		Actions								
SITE TO SITE (GATEWAY-GATEWAY)		MOBILE - MOBILE USERS								
Enter a filter		+ Add	X Delete	Up Down	Cut	Copy	Paste	Show details	Search in logs	Search in monitoring
	Status	Local network	Peer	Remote network						
1	<input checked="" type="checkbox"/> on	Network_in	mobile_peer	Any						

STORMSHIELD

13

Activer la politique créée (désactivée par défaut).

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Le renseignement du local ID est optionnel

The screenshot shows the configuration page for a dynamic peer in the Stormshield VPN management console. The interface is divided into several sections:

- General:** Includes fields for Comment, Remote gateway (set to Any), Local address (set to Any), IKE profile (set to StrongEncryption), and IKE version (set to IKEv1).
- Identification:** Includes Authentication method (set to Pre-shared key (PSK)), Local ID (with a blue highlight and the text "Enter an ID (optional)"), Peer ID (with the text "Enter an ID (optional)"), and a Pre-shared key (PSK) field with an Edit button.
- Advanced properties:** Includes checkboxes for "Do not initiate the tunnel (Responder only)" and "IKE fragmentation", and dropdown menus for DPD (set to Passive) and DSCP (set to 00 Best effort).

The interface also features a search bar at the top left, a list of mobile peers on the left, and navigation tabs at the top: ENCRYPTION POLICY - TUNNELS, PEERS, IDENTIFICATION, and ENCRYPTION PROFILES. The text "STORMSHIELD" is visible in the bottom left corner of the interface, and "CSNAv2.x" and "14" are in the bottom right corner.

Dans IKEv1, lorsqu'une identité FQDN est définie, la configuration ne passe **PAS** en mode de négociation **AGRESSIF**, contrairement aux versions précédentes. La ID locale pour le firewall A est optionnelle et possède une adresse IP statique.

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- La configuration du correspondant A sur le firewall B

The screenshot displays the Stormshield VPN configuration interface. The main window is titled 'VPN / IPSEC VPN' and shows the configuration for a peer named 'SITE\_FW\_A'. The configuration is divided into several sections:

- General:**
  - Comment: (empty)
  - Remote gateway: fw\_A
  - Local address: Any
  - IKE profile: StrongEncryption
  - IKE version: IKEv1
- Identification:**
  - Authentication method: Pre-shared key (PSK)
  - Local ID: fw.company-B.net (highlighted with a blue box)
  - Peer ID: fw.company-A.net
  - Pre-shared key (PSK): (masked with dots)
- Advanced options:**
  - Do not initiate the tunnel (Responder only)
  - IKE fragmentation
  - Passive: (dropdown menu)
  - 00 Best effort

An inset window shows the 'VPN / IPSEC VPN' overview table:

Status	Local network	Peer	Remote network	Encryption profile	Keep alive
1 on	Network_in	Site_fw_A	Net_In_A	StrongEncryption	30

CSNAv2.x  
15

Sur le Firewall B (qui possède une IP dynamique), la configuration du tunnel VPN IPsec est de type site-à-site avec :

- Les extrémités de **tunnel** pleinement définies.
- Les extrémités de **traffic** également pleinement définies.
- Puisque le firewall B initie le trafic, vous pouvez activer le keep alive pour forcer la montée du tunnel.
- L'identité de ce firewall doit être définie sous la forme d'un FQDN **fw.company-B.net**. Ce dernier est renseigné dans les paramètres du correspondant, champ Local ID qui est dans ce cas obligatoire. L'ID du correspondant est optionnel, mais s'il est renseigné, il doit correspondre à l'ID (FQDN) présenté par le firewall A.
- La PSK associée à l'identité du firewall A dont l'IP est fixe.

## VPN IPSEC – CORRESPONDANT DYNAMIQUE

- Règles de filtrage sur le correspondant A

SECURITY POLICY / FILTER - NAT

(7) Filter 07 Edit Export

FILTERING NAT

Searching... + New rule X Delete ↑ ↓ ↻ Cut Copy Paste Search in logs Search in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Separator - rule grouping (contains 2 rules, from 1 to 2)							
1	on	pass	Internet interface: out geo Europe	Firewall_out	isakmp_natt isakmp		IPS
2	on	pass	Internet interface: out geo Europe	Firewall_out	Any	vpn-esp	IPS
Allow traffic between networks (contains 3 rules, from 3 to 5)							
3	on	pass	Network_in	Net_in_B	Any		IPS
4	on	pass	Net_in_B via IPsec VPN tunnel	Network_in	Any		IPS

STORMSHIELD CSNAv2.x 16

Contrairement aux tunnels site-à-site, aucune règle de filtrage implicite n'est ajoutée automatiquement pour autoriser la montée du tunnel. La politique de filtrage sur le firewall dont l'adresse IP publique est fixe, doit explicitement permettre les négociations et les flux constituant le tunnel (IKE et ESP).

Comme pour les tunnels site-à-site, il faudra également définir des règles de filtrage pour préciser le trafic autorisé au-travers du tunnel IPsec.

Pour améliorer le niveau de sécurité du firewall, il est recommandé de limiter le trafic IKE et ESP entrant en utilisant une limitation géographique (dans cet exemple, l'Europe est autorisée).



## Programme de la formation

- ✓ Cours des formations et certifications
- ✓ Présentation de l'entreprise et des produits
- ✓ Prise en main du firewall
- ✓ Traces et supervision
- ✓ Objets
- ✓ Configuration réseau
- ✓ Translation d'adresses
- ✓ Filtrage
- ✓ Protection applicative
- ✓ Utilisateurs & authentification
- ✓ VPN
- VPN SSL

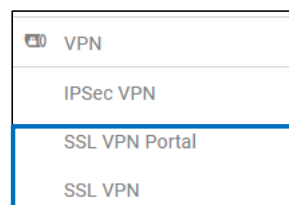


## Concepts et généralités

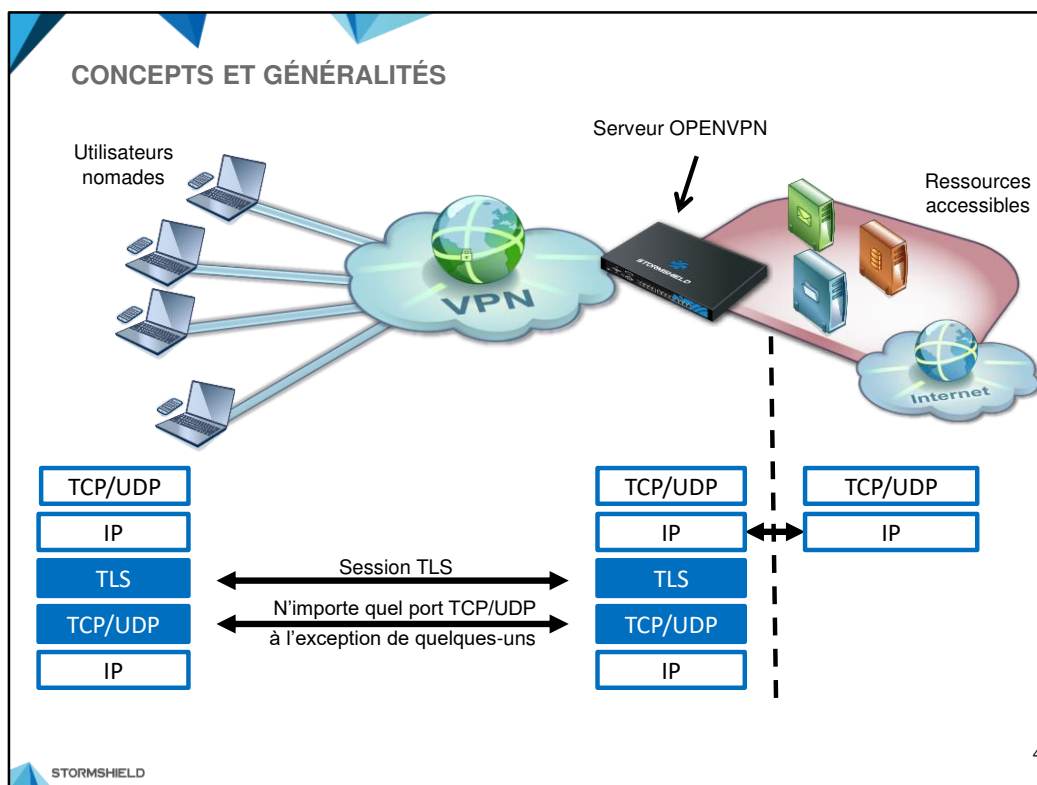
- Configuration d'un tunnel
- Lab – VPN SSL

## CONCEPTS ET GÉNÉRALITÉS

- Les firewalls Stormshield intègrent deux types de VPN SSL
- VPN SSL portail :
  - Accès aux serveurs Web HTTP et serveurs applicatifs via le portail captif après authentification
- VPN SSL (complet) :
  - Utilise un client VPN SSL (gratuit)
  - Accès au réseau interne d'une manière transparente

**Note :**

- Les deux modes VPN SSL (portail et complet) peuvent fonctionner simultanément.
- Le VPN SSL portail n'est pas abordé dans le cadre de cette formation. Toutes les références à « VPN SSL » dans le reste de ce document se rapportent exclusivement au VPN SSL en mode complet.



Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée aux ressources internes d'une entreprise. Les communications entre l'utilisateur distant et le firewall sont encapsulées et protégées via un tunnel TLS chiffré.

Au niveau du firewall, les tunnels VPN SSL sont gérés par le serveur OpenVPN (logiciel libre) qui est intégré dans le firmware en tant que nouveau service. OpenVPN peut fonctionner sur n'importe quel port TCP et/ou UDP, à l'exception de quelques-uns, qui sont utilisés pour les processus internes du firewall :

- smux\_tcp : TCP/199
- ldap : TCP/389, ldaps TCP/636
- firewall\_srv : 1300/TCP
- pptp : TCP/1723
- sld (démon d'authentification) : TCP/4444
- http\_proxy : 8080/TCP
- smtp\_proxy : 8081/TCP
- pop3\_proxy:8082/TCP
- ftp\_proxy : 8083/TCP
- ssl\_proxy : 8084/TCP
- loopback\_proxysql : 8085/TCP

En ce qui concerne les utilisateurs nomades, le tunnel est géré par le client VPN SSL (Stormshield ou OpenVPN standard), qui doit être installé sur les machines. Une fois le tunnel mis en œuvre, l'hôte distant récupère une adresse IP fournie par le serveur VPN SSL. Elle sera considérée comme faisant partie des réseaux internes (protégés) du firewall et l'utilisateur sera vu comme authentifié.

## NOMBRE DE TUNNELS VPN SSL

- Le nombre de tunnels VPN maximum dépend du modèle d'UTM:

UTM	SN160(W) SN160W	SN210(W) SN310	SN510	SN710 SN910	SN2100	SN3100 SN6100	SNi20 SNi40
Nombre d'utilisateurs	5	20	100	150	400	500	100

- Limites des appliances virtuelles:

V-UTM	EVA1	EVA2	EVA3	EVA4	EVAU
Nombre d'utilisateurs	100	150	200	250	500

## CLIENTS VPN SSL

- Pour monter le tunnel, le client peut utiliser :

- L'application standard OpenVPN
  - PC : Windows, macOS ou GNU/Linux
  - Mobile : Android, iOS



- Le client SSL VPN Stormshield
  - PC : Windows

**Clients VPN SSL compatibles :**

- Le client VPN SSL Stormshield Network (basé sur le client OpenVPN) peut être lancé en toute transparence depuis un poste utilisateur Windows avec les droits d'utilisateur (toutefois, son utilisation nécessite des droits administrateur). Ce client est disponible en téléchargement libre depuis votre espace privé [mystormshield.eu](http://mystormshield.eu) et depuis le portail captif du firewall après authentification.
- Un client OpenVPN standard doit être lancé avec les droits d'administration du poste client.
- Les terminaux de type smartphones et tablettes (Android ou iOS) peuvent également se connecter via un VPN SSL avec un client OpenVPN Connect (disponible dans le Google Play Store et l'Apple Store).

## CLIENTS VPN SSL

- Le réseau VPN SSL (TCP ou UDP) défini sur le serveur est considéré comme un réseau interne ⇒ Il ne doit pas chevaucher un réseau interne existant
- Le réseau VPN SSL est découpé en sous-réseaux de /30 :
  - Le premier et le dernier sont utilisés par le serveur
  - Un sous-réseau est utilisé pour chaque client
- Exemple : 192.168.100.0/24 ⇒ 62 clients maximum
  - Serveur [192.168.100.0| .1 | .2 | .3] /30
  - Client 1 [192.168.100.4| .5 | .6 | .7] /30
  - Client 2 [192.168.100.8| .9| .10| .11] /30
  - ...
  - ...
  - Serveur [192.168.100.252| .253| .254| .255] /30

STORMSHIELD

7

Les clients VPN SSL font partie d'un même réseau UDP, ou TCP, défini au niveau du firewall. Ce réseau est considéré comme un réseau interne (protégé): il ne doit donc pas recouvrir un réseau interne existant.

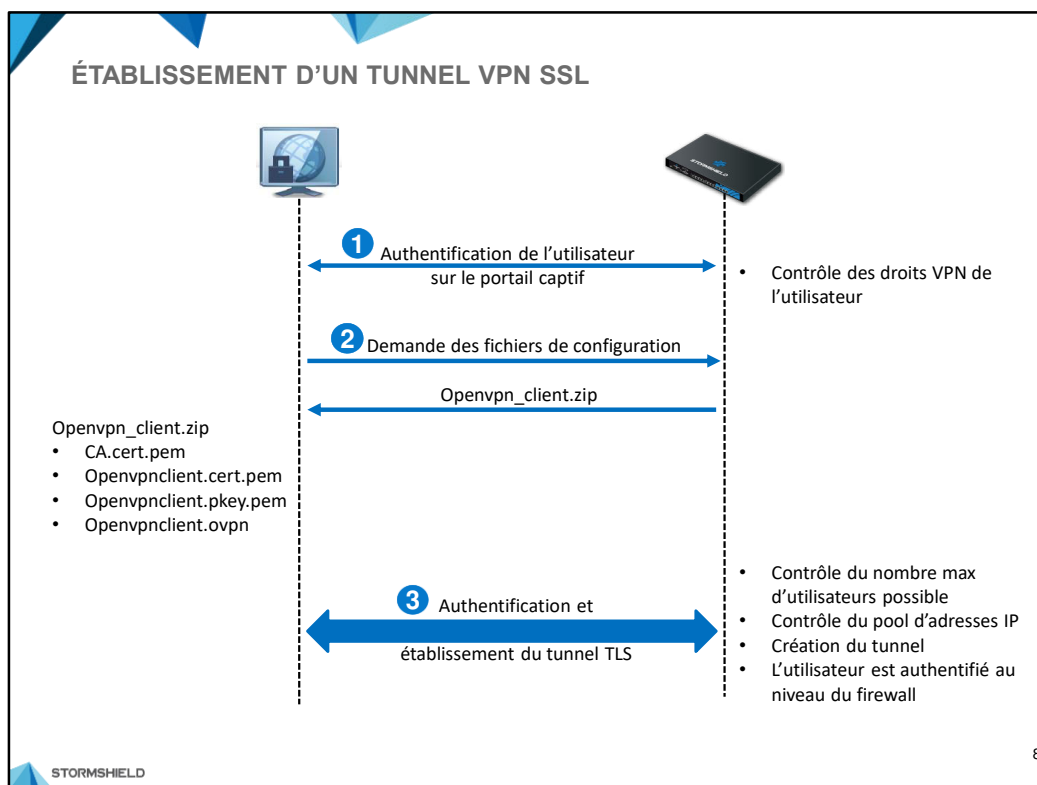
Pour son fonctionnement interne, le serveur se réserve le premier sous-réseau de /30 issu du réseau VPN SSL (une interface « tun0 » est créée et porte la première adresse IP du réseau TCP, l'interface est tun1 pour le réseau UDP, ces interfaces ne sont visibles qu'en ligne de commande), ainsi que le dernier réseau de la plage. Les autres sous-réseaux de /30 sont utilisés par les clients.

Par exemple, si le service SSL/ VPN utilise le réseau 192.168.100.0/24 pour les clients UDP, le premier client VPN SSL UDP utilise le deuxième sous-réseau /30 :

- Adresse réseau : 192.168.100.4
- Adresse de l'interface du tunnel côté serveur : 192.168.100.5
- Adresse de l'interface du tunnel côté client : 192.168.100.6
- Adresse de diffusion : 192.168.100.7

Ainsi, le nombre maximum de clients VPN SSL UDP sur ce réseau est de 62 (64 sous-réseaux de /30, dont deux utilisés par le serveur).

Le calcul reste le même pour le réseau VPN SSL TCP.  
Ce comportement est défini explicitement dans OpenVPN.



La mise en œuvre du tunnel VPN SSL s'effectue en trois étapes principales :

1. Le client VPN SSL STORMSHIELD authentifie l'utilisateur par une connexion préalable et transparente au portail captif. Durant cette étape, le firewall vérifie si l'utilisateur authentifié possède les droits lui permettant d'ouvrir un tunnel VPN SSL.
2. Si l'authentification réussit, le client envoie une requête pour récupérer les fichiers de configuration renvoyés par le firewall dans un dossier compressé « `openvpn_client.zip` ». Le dossier contient les fichiers suivants :
  - Le certificat de l'autorité de certification (**CA.cert.pem**),
  - Le certificat du client et sa clé privée (**openvpnclient.cert.pem** et **openvpnclient.pkey.pem**),
  - La configuration du client OpenVPN.
3. Le client lance le processus de mise en œuvre du tunnel TLS avec authentification par certificat à l'aide des certificats récupérés lors de l'étape précédente. Avant la mise en œuvre du tunnel, le firewall vérifie que le nombre maximal d'utilisateurs n'est pas encore atteint et qu'un sous réseau peut être réservé pour ce nouveau client. Si toutes les conditions sont vérifiées, le tunnel est mis en œuvre et l'utilisateur est considéré comme authentifié.

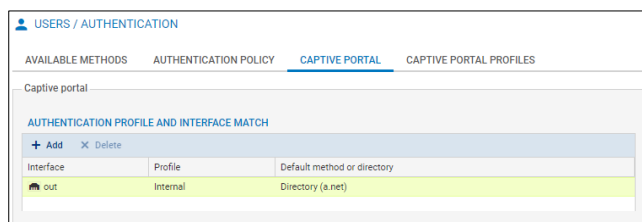
**NOTE** : Si le serveur VPN SSL est accessible via un port UDP ou TCP, le client VPN SSL tente d'abord de mettre en œuvre le tunnel avec le protocole UDP et en cas d'échec, il effectue automatiquement une nouvelle tentative avec le protocole TCP.



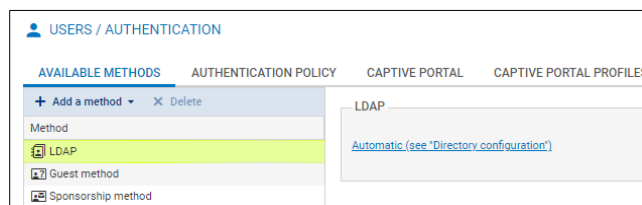
- Concepts et généralités
- **Configuration d'un tunnel**
- Lab – VPN SSL

## EXIGENCES : ANNUAIRE, PORTAIL CAPTIF ET AUTHENTIFICATION

- Un annuaire interne ou externe doit être configuré
- Un profil du portail captif doit être rattaché à l'interface depuis laquelle les utilisateurs se connectent



- Une méthode d'authentification doit être configurée



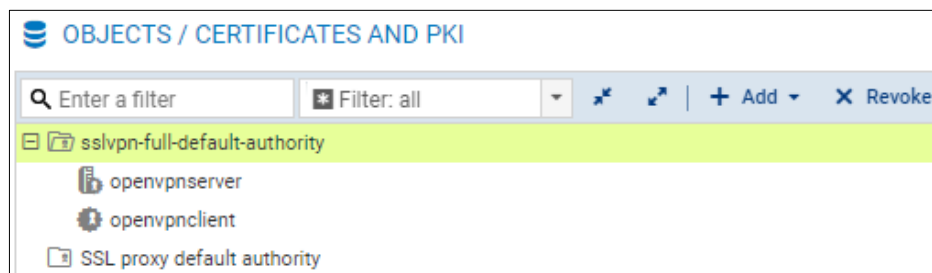
La première étape de mise en œuvre d'un tunnel VPN SSL est l'authentification de l'utilisateur via le portail captif, ce qui signifie que :

- Un annuaire externe ou interne doit être configuré au niveau du firewall,
- Un profil du portail captif doit être rattaché à l'interface depuis laquelle les utilisateurs se connectent,
- Une méthode d'authentification doit être configurée.

Les méthodes d'authentification possibles pour le service VPN SSL sont les méthodes explicites qui nécessitent un couple identifiant/mot de passe, en l'occurrence LDAP (interne, externe ou Microsoft Active Directory), Kerberos et Radius.

**EXIGENCES : L'AUTORITÉ DE CERTIFICATION VPN SSL**

- PKI fournissant les certificats pour le serveur OpenVPN et les clients OpenVPN (le même certificat sera affecté à tous les clients OpenVPN) :



Des certificats seront utilisés pour l'authentification entre le client et le serveur VPN SSL. Pour cela, une autorité de certification racine (CA) existe dans la configuration usine de tous les firewalls Stormshield Network. Cette CA est nommée **sslvpn-full-default-authority**, et elle contient un certificat serveur (qui identifie le serveur VPN SSL), et un certificat client (qui identifie tous les clients; chacun d'entre eux sera ensuite différencié par un couple login/mot de passe).

**NOTE :** Il est naturellement possible de créer une CA dédiée au VPN SSL sans recourir à la CA par défaut. La création des CA est présentée dans le niveau expert.

### DROITS D'ACCÈS VPN SSL

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS
DETAILED ACCESS
PPTP SERVER

When no access rules have been defined for the user

VPN access

SSL VPN portal profile: Block

IPSec policy: Block

SSL VPN policy: Block  
Block  
Allow

Sponsorship policy: Allow

Paramétrage par défaut

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS
DETAILED ACCESS
PPTP SERVER

Searching...

Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	Sponsorship	Description
1 <span style="color: green;">✔</span> Enabled	vpnuser@trainer.local	Block	Block	Allow	Block	

Paramètres personnalisés

12

Pour autoriser un utilisateur à mettre en œuvre un tunnel VPN SSL, vous devez lui attribuer les droits correspondants dans le menu **Configuration** ⇒ **Utilisateurs** ⇒ **Droits d'accès**.

Il est possible de choisir un accès par défaut indépendamment de l'utilisateur connecté dans l'onglet **Accès détaillé** ⇒ encadré **SSL VPN** . Sélectionnez **Autoriser** dans le champ **Politique VPN SSL par défaut**

Cependant, une gestion plus fine des droits d'accès est préconisée en laissant la politique VPN SSL par défaut à Bloquer et en ajoutant les utilisateurs ou les groupes d'utilisateurs dans l'onglet **ACCÈS DÉTAILLÉ** ⇒ **AJOUTER** avec les droits VPN SSL à **Autoriser**.

## RÈGLES DE FILTRAGE IMPLICITES POUR LE VPN SSL

Enabled	Name
<input checked="" type="checkbox"/> Enabled	Allow access to the PPTP server
<input checked="" type="checkbox"/> Enabled	Allow mutual access between the members of a firewall cluster (HA)
<input checked="" type="checkbox"/> Enabled	Allow ISAKMP (UDP port 500) and the ESP protocol for IPsec VPN peers.
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's DNS service (port 53).
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for modem interfaces (dialup)
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for ethernet interfaces
<input type="checkbox"/> Disabled	Allow protected interfaces (server) to access the firewall's administration server (port 1300)
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's SSH port
<input checked="" type="checkbox"/> Enabled	Allow interfaces associated with authentication profiles (Authd) to access the authentication portal and SSL VPN.
<input checked="" type="checkbox"/> Enabled	Allow access to the firewall's web administration server (WebAdmin)
<input checked="" type="checkbox"/> Enabled	Allow "Bootp" requests with an IP address specified for relaying DHCP requests
<input checked="" type="checkbox"/> Enabled	Allow clients to reach the firewall SSL VPN service on the TCP and UDP ports
<input checked="" type="checkbox"/> Enabled	Allow router solicitations (RS) in multicast or directed to the firewall
<input checked="" type="checkbox"/> Enabled	Allow requests to DHCPv6 server and DHCPv6 multicast solicitations
<input checked="" type="checkbox"/> Enabled	Do not log IPFIX packets in IPFIX traffic

Pour permettre aux clients VPN SSL d'accéder au portail d'authentification sur les interfaces associées aux profils d'authentification du firewall, la règle de filtrage implicite nommée **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces associées aux profils d'authentification (Authd)** doit être activée.

Si tel n'est pas le cas, il est impératif d'ajouter des règles de filtrage explicites dans la politique active autorisant les flux à destination de l'interface publique sur le port d'écoute du service, par défaut :

- Port 443 en VPN SSL TCP,
- Port 1194 en VPN SSL UDP.

## CONFIGURATION DU SERVICE VPN SSL

**VPN / SSL VPN**

ON

**Network settings**

UTM IP address (or FQDN) used:	<input type="text" value="192.36.253.10"/>
Available networks or hosts :	<input type="text" value="Network_internals"/> ▼ ↕
Network assigned to clients (UDP):	<input type="text" value="net_ssl_udp"/> ▼ ↕
Network assigned to clients (TCP):	<input type="text" value="net_ssl_tcp"/> ▼ ↕
Maximum number of simultaneous tunnels allowed:	126

STORMSHIELD

14

Le service VPN SSL peut être configuré dans **Configuration ⇒ VPN ⇒ SSL VPN**.

- Encadré **Paramètres réseaux** :

- **Adresse IP (ou FQDN) de l'UTM utilisée** : Il s'agit de l'adresse sur laquelle vont se connecter les clients VPN SSL (adresse publique la plupart du temps). Attention, la saisie d'un FQDN induit une résolution de noms via un service DNS,
- **Réseaux ou hôtes disponibles** : Machines ou réseaux auxquels les utilisateurs peuvent avoir accès une fois le tunnel mis en œuvre (l'accès dépend néanmoins de la politique de filtrage active). Il est possible de choisir l'objet **Any**. Dans ce cas, tous les flux du client VPN passent par le tunnel et sont soumis aux opérations de filtrage et de NAT du firewall.
- **Réseau assigné aux clients (UDP)** : Réseau attribué aux clients nomades une fois le tunnel mis en œuvre via le protocole UDP. La valeur minimale pouvant être choisie ici est un réseau de /28.
- **Réseau assigné aux clients (TCP)** : Réseau attribué aux clients nomades une fois le tunnel mis en œuvre via le protocole TCP. La valeur minimale pouvant être choisie ici est un réseau de /28.
- **Maximum de tunnels simultanés autorisés** : Paramètre non configurable dans l'IHM. Il indique le nombre maximal de tunnels (clients) autorisés, c'est-à-dire le minimum entre le nombre de tunnels autorisés pour le modèle du firewall et le nombre de tunnels possibles calculé à partir du réseau assigné aux clients.

**NOTE** : les réseaux assignés aux client UDP et TCP doivent être différents.

## CONFIGURATION DU SERVICE VPN SSL

Comme vu précédemment, ce réseau est découpé en sous-réseaux de masque /30, dont 2 sont utilisés par le serveur pour son fonctionnement interne, les autres étant utilisés par les clients. Ainsi, un réseau /24 permet un maximum de 62 tunnels.

- Encadré **Paramètres DNS envoyés au client** :
  - **Nom de domaine** : Il s'agit en général du domaine dont dépendent les réseaux accessibles par le client (Windows uniquement).
  - **Serveur DNS primaire (et secondaire)** : Interne à l'entreprise si le client doit pouvoir accéder à des ressources locales. Sinon, le choix d'un serveur public est autorisé.
- Encadré **Configuration avancée** :
  - **Adresse IP de l'UTM pour le VPN SSL (UDP)** : Il s'agit de l'adresse à laquelle vont se connecter les clients du VPN SSL s'ils sont configurés pour utiliser l'UDP (adresse publique la plupart du temps).
  - **Port (UDP)** : Port d'écoute UDP du service VPN SSL (1194 par défaut).
  - **Port (TCP)** : Port d'écoute TCP du service VPN SSL (443 par défaut).

**NOTE** : Attention : certains ports sont réservés à un usage interne et ne peuvent être sélectionnés. Ces ports sont smtp\_proxy : 8081/TCP, ftp\_proxy : 8083/TCP, pop3\_proxy : 8082/TCP, ssl\_proxy : 8084/TCP, http\_proxy : 8080/TCP, loopback\_proxysql : 8085/TCP, firewall\_srv : 1300/TCP, ldap : TCP/389, ldaps TCP/636, pptp : TCP/1723, TCP/4444, TCP/8087, smux\_tcp : TCP/199, isakmp : UDP/500, isakmp\_nat : UDP/4500, bootps : UDP/67, bootpc : UDP/68.



- **Intervalle avant renégociation clé (en secondes)** : Période avant qu'une nouvelle session TLS ne soit renégociée.
  - **Utiliser les serveurs DNS fournis par le firewall** : Lorsque cette option est choisie, le client VPN SSL ajoutera les serveurs DNS qui ont été récupérés via le tunnel VPN SSL à la configuration réseau du poste de travail du client.
  - **Interdire l'utilisation des serveurs DNS tiers** : Lorsque cette option est choisie, le poste de travail du client utilisera uniquement les serveurs DNS qui ont été récupérés via le tunnel VPN SSL.
- 
- Encadré **Script à exécuter sur le client** : Permet de définir les scripts à exécuter lorsque le client se connecte et se déconnecte. Des exemples de scripts sont fournis de façon détaillée dans le document `snetno_SSL_VPN_Tunnel.pdf` accessible via <https://mystormshield.eu>.
  - Encadré **Certificats utilisés** : Personnalise les certificats utilisés. Rappel : le certificat serveur permet d'identifier le serveur VPN SSL alors que le certificat utilisateur permet d'identifier les clients VPN SSL (chaque client sera ensuite identifié par son login). Si ces certificats sont modifiés, s'assurer qu'ils ont bien été émis par la même autorité de certification. Sinon, la configuration ne sera pas appliquée.
  - Encadré **Configuration** : Le fichier de configuration peut être téléchargé au format OpenVPN.

## FILTRAGE ET NAT

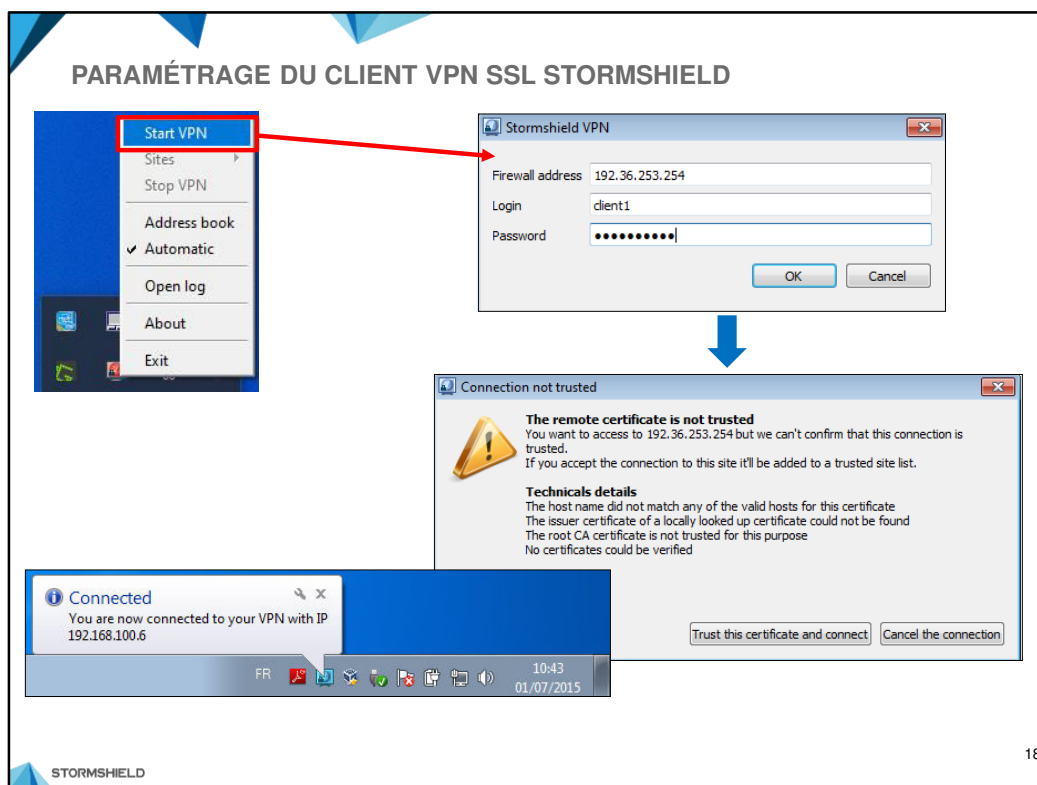
- Il est nécessaire de définir des règles de filtrage explicites pour la gestion du trafic provenant des tunnels :

FILTERING		NAT							
Searching...		+ New rule		X Delete		↑ ↓ ↻ ↺		Cut Copy Paste Search in logs	
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection		
Via ssl vpn traffic (contains 2 rules, from 1 to 2)									
1	on	pass	net_ssl_udp net_ssl_tcp via SSL VPN tunnel	Network_internals	http		IPS		
2	on	pass	net_ssl_udp net_ssl_tcp via SSL VPN tunnel	Internet		dns http https	IPS		

- Une translation d'adresses peut être mise en œuvre si des clients doivent utiliser le VPN SSL pour accéder à Internet :

FILTERING		NAT							
Searching...		+ New rule		X Delete		↑ ↓ ↻ ↺		Cut Copy Paste Search in logs	
	Status	Original traffic (before translation)			Traffic after translation				
		Source	Destination	Dest. port	Source	Src. port	Destination		
1	on	net_ssl_udp net_ssl_tcp	Internet interface: out	Any	Firewall_out		ephemera_fw	Any	

La règle de filtrage n°1 permet l'**initiation de connexions** à partir des clients VPN SSL et à destination des serveurs Web internes,  
 La règle de filtrage n°2 permet l'**initiation de connexions** à partir des clients VPN SSL et à destination d'Internet ; dans ce cas, une règle de NAT doit également être ajoutée.



L'application VPN SSL Stormshield Network peut être téléchargée sur votre espace privé <https://mystormshield.eu> et sur le portail captif du firewall après authentification.

**NOTE** : différents packages sont disponibles pour les versions Microsoft Windows 7 et 10 et le client VPN SSL v3.0.1 ou au-delà doit être utilisé avec les firewalls SNS dans la version 4.3.

Une fois démarré, le client VPN SSL nécessite trois paramètres :

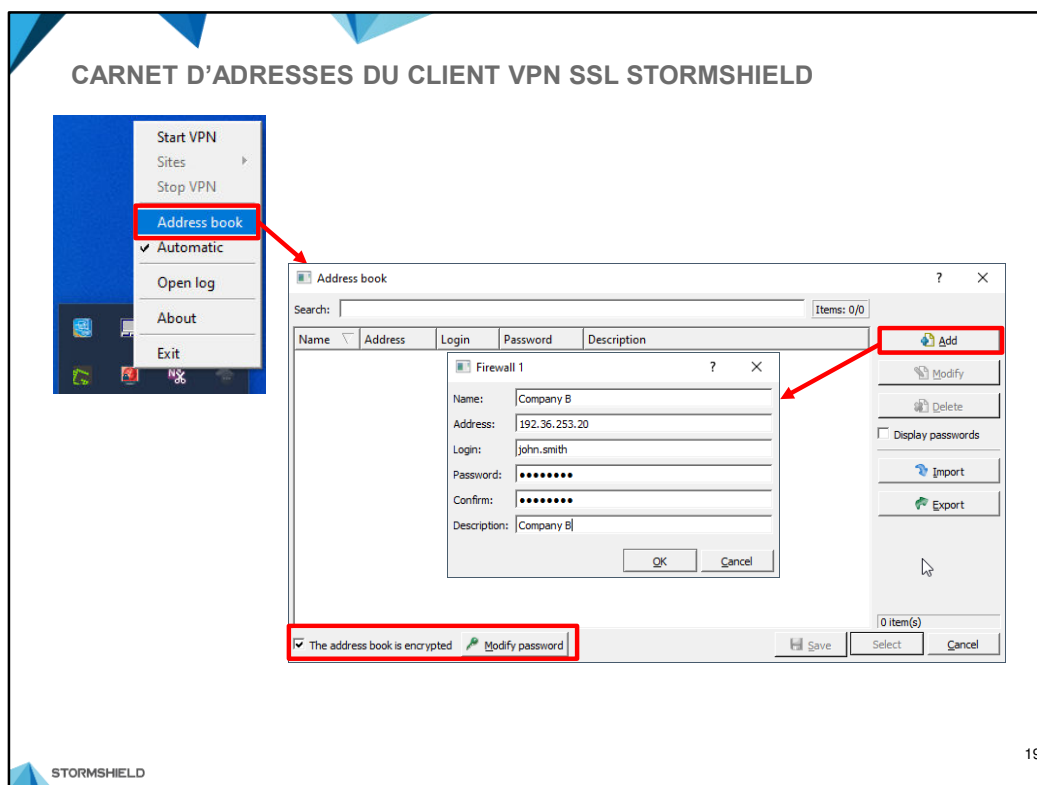
- L'adresse IP ou le FQDN du firewall à contacter,
- L'identifiant de l'utilisateur disposant des droits pour le VPN SSL,
- Le mot de passe de l'utilisateur.

Une fenêtre indique que la connexion à ce site n'est pas sécurisée car le client ne fait pas confiance à la CA signataire du certificat serveur présenté par le portail captif du firewall. Il est donc possible :

- D'afficher le certificat pour savoir quelle CA l'a signé,
- De faire confiance à ce certificat, ce qui signifie que la CA est ajoutée aux autorités de confiance et qu'il est possible de continuer avec la configuration du tunnel,
- D'annuler la connexion, ce qui arrêtera la configuration du tunnel.

En cas d'échec de la configuration du tunnel, faire un clic droit sur l'icône VPN SSL Stormshield Network pour afficher les traces.

Lorsque le tunnel est monté, le poste client disposera d'une interface spécifique au tunnel VPN SSL dont l'adresse IP fait partie de l'objet **Réseau assigné au client** de la configuration serveur.



Le client VPN SSL Stormshield possède une fonction de carnet d'adresses, qui peut aider à sauvegarder différents profils VPN dans un seul fichier chiffré. Le mot de passe utilisé pour protéger le fichier est spécifique.

Pour ajouter une entrée au carnet d'adresses, il suffit de cliquer sur le bouton « Ajouter » et de renseigner les détails, puis de cliquer sur « OK » pour la sauvegarder.

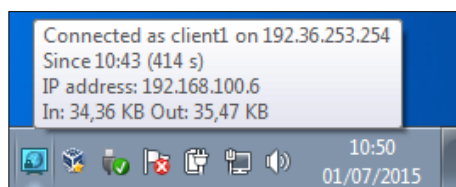
Il est également possible d'importer/exporter des entrées.

Le carnet d'adresses se trouve à l'emplacement suivant :

%USERPROFILE%\AppData\Local\Stormshield\Stormshield SSL VPN Client\AddrBook.gap

## PARAMÉTRAGE DU CLIENT VPN SSL STORMSHIELD

	Déconnecté
	En cours de connexion
	Connecté



L'icône du client VPN SSL Stormshield qui apparaît dans la zone de notification de la barre de tâches de Windows possède un code couleur qui correspond à son état :

- Rouge : Le client est déconnecté,
- Jaune : Le client essaye de mettre en œuvre le tunnel,
- Bleu : Le client est connecté,

Lorsque le client est connecté, des informations sur la connexion apparaissent lorsque le curseur de la souris est positionné sur l'icône.

## TUNNELS VPN SSL DANS LA GUI

MONITOR / SSL VPN TUNNELS

Searching... [Reset this tunnel](#) [Refresh](#) [Export results](#) [Configure the SSL VPN service](#)

User	Directory	VPN client IP address	Real IP address	Received	Sent
vpuser	trainer.local	172.30.30.6	31.20.108.163	4.49 KB	6.64 KB

MONITOR / USERS

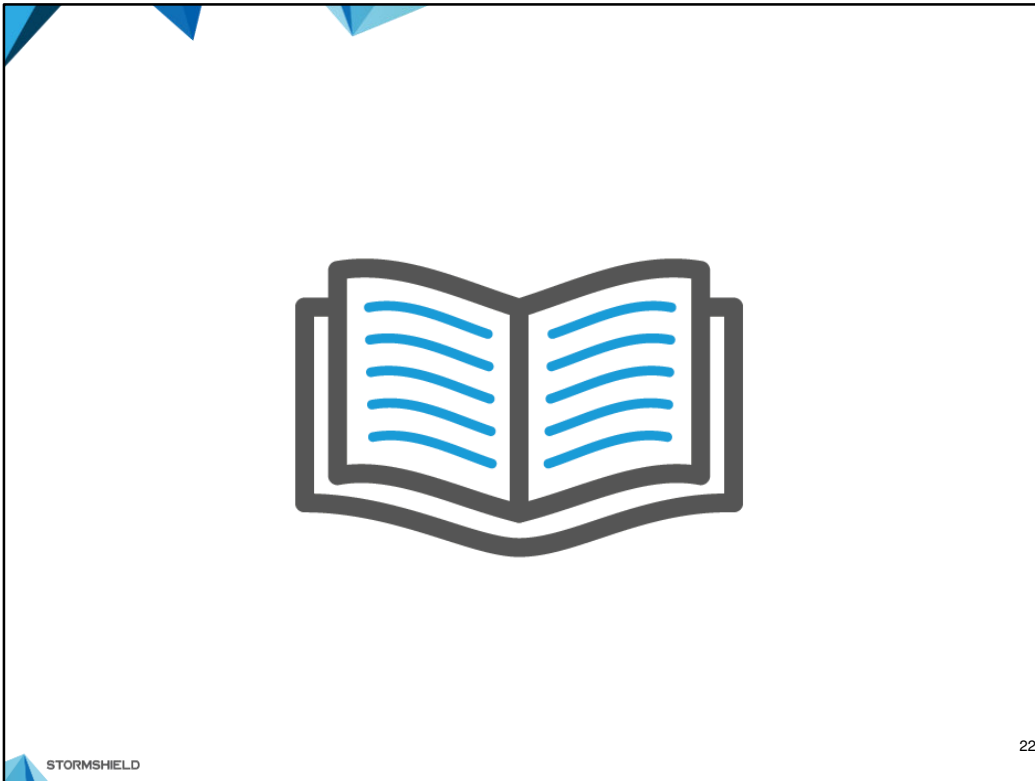
No predefined filter [Filter](#) [Reset](#) [Refresh](#) [Export results](#) [Configure authentication](#)

FILTERS (NO FILTERS CREATED)

Name	IP address	Directory	Group	Expiry date	Auth. method
vpuser	172.30.30.6	trainer.local		6d 23h 57m	OPENVPN

La page de supervision du firewall permet de visualiser les tunnels VPN SSL ouverts dans l'onglet **Supervision => tunnels VPN SSL**. Il est également possible de supprimer un tunnel en effectuant un clic droit sur **Déconnecter cet utilisateur**.

Les utilisateurs connectés via un tunnel VPN SSL sont considérés comme authentifiés et peuvent être visualisés depuis le menu **Utilisateurs**. La colonne **Méthode d'auth.** indique que le client VPN est authentifié via un tunnel VPN SSL.



Pour aller plus loin, consultez la note technique du site [documentation.stormshield.eu](https://documentation.stormshield.eu) :

- Tunnels VPN SSL

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC [kb.stormshield.eu](https://kb.stormshield.eu).



- Concepts et généralités
- Configuration d'un tunnel

 **Lab – VPN SSL**

STORMSHIELD

**VPN SSL**



## Lab 9 – VPN SSL

1. Le client OpenVPN est installé sur la VM graphique fournie par Stormshield. Configurez le firewall pour permettre aux utilisateurs qui se connecteront depuis le réseau externe d'accéder à vos réseaux internes IN et DMZ :
  - Les réseaux distribués aux utilisateurs VPN SSL seront :
    - Pour TCP : Net-SSLVPN\_TCP 172.31.x.0/24
    - Pour UDP : Net-SSLVPN\_UDP 172.30.x.0/24
  - Le serveur DNS annoncé au client correspond à la machine srv-dns.
2. Donnez le droit VPN SSL à l'utilisateur John Smith.
3. Pour le filtrage :
  - Autorisez votre réseau à accéder aux firewalls de vos voisins sur les ports SSLVPN et UDPVPN pour tous les utilisateurs (authentifiés et non authentifiés).
  - Autorisez aux réseaux Net-SSLVPN\_TCP et Net-SSLVPN\_UDP l'accès aux réseaux internes.
4. Récupérez le fichier « Profil VPN SSL pour clients mobiles OpenVPN Connect (fichier unique .ovpn) » via le portail captif sur l'adresse IP publique de l'autre entreprise, il est téléchargé par défaut dans /home/user/Downloads, ouvrez un terminal puis tapez les commandes suivantes :

```
su -  
#Mot de passe root par défaut : toor  
cd /home/user/Downloads  
openvpn openvpn_mobile_client.ovpn
```

Il est possible d'avoir une erreur d'ajout de route si la route poussée est déjà présente. Cela n'empêche pas l'établissement du tunnel.  
Dans un second terminal, consultez votre table de routage pour visualiser les routes ajoutées sur le client, avec la commande `ip route show`.
5. Consultez la liste des utilisateurs authentifiés dans l'ASQ ainsi que les logs relatifs au VPN SSL côté firewall.
6. Validez l'accès aux différents serveurs de la DMZ et par ping sur l'IP interne du firewall sur le réseau LAN.
7. Enfin, fermez le tunnel via le premier terminal avec la combinaison de touches [CTRL+C].

**Bonus :**

1. Sans déconnecter l'utilisateur John Smith, modifiez la configuration du VPN SSL pour donner accès à l'objet « Any ».
2. Ajoutez les règles (NAT + Filtrage) permettant aux réseaux Net-SSLVPN\_TCP et Net-SSLVPN\_UDP d'accéder à Internet une fois le tunnel monté.
3. Ajoutez une politique de filtrage URL pour que seul l'accès aux sites des groupes « it » et « news » soit autorisé.