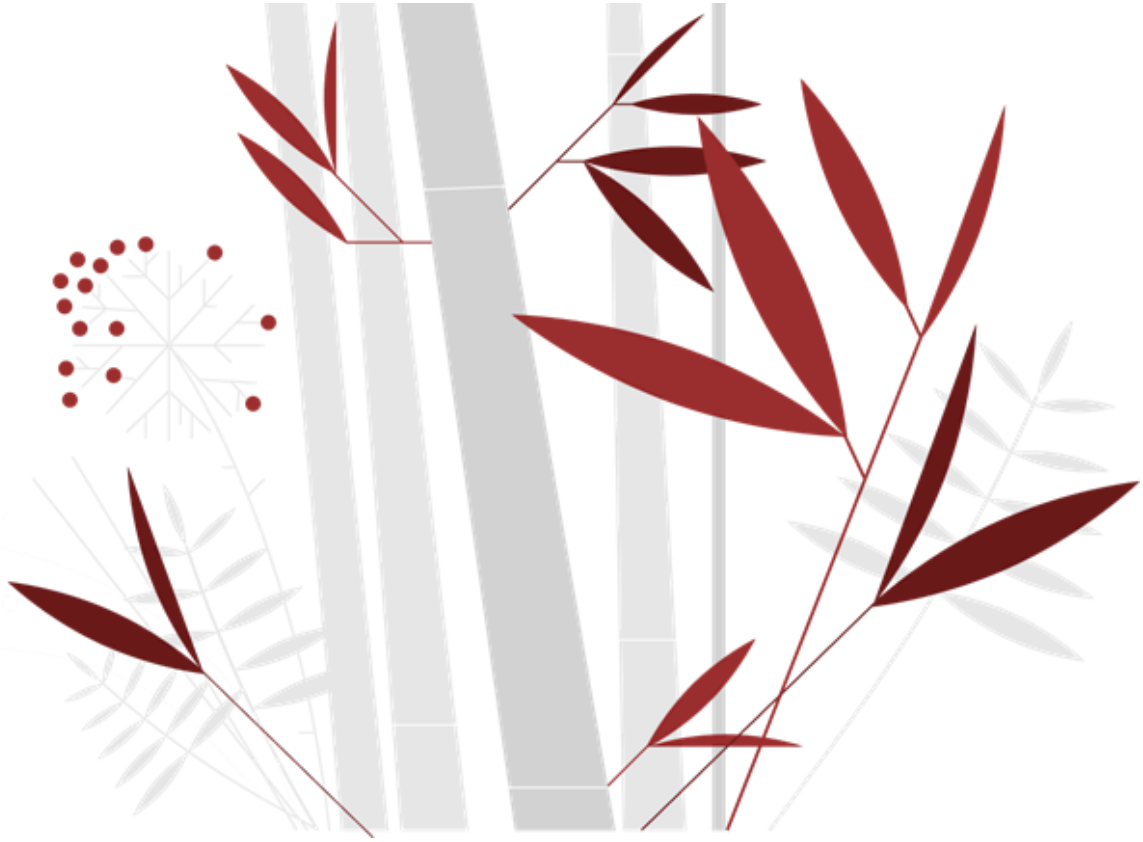
CONFIGURATION D'UN FIREWALL STORMSHIELD

Compétences ciblées : - Mettre en place et vérifier les niveaux d'habilitation associés à un service ; - Vérifier le respect des règles d'utilisation des ressources numériques

Remi POULET-DENECQUE

Gaston Berger



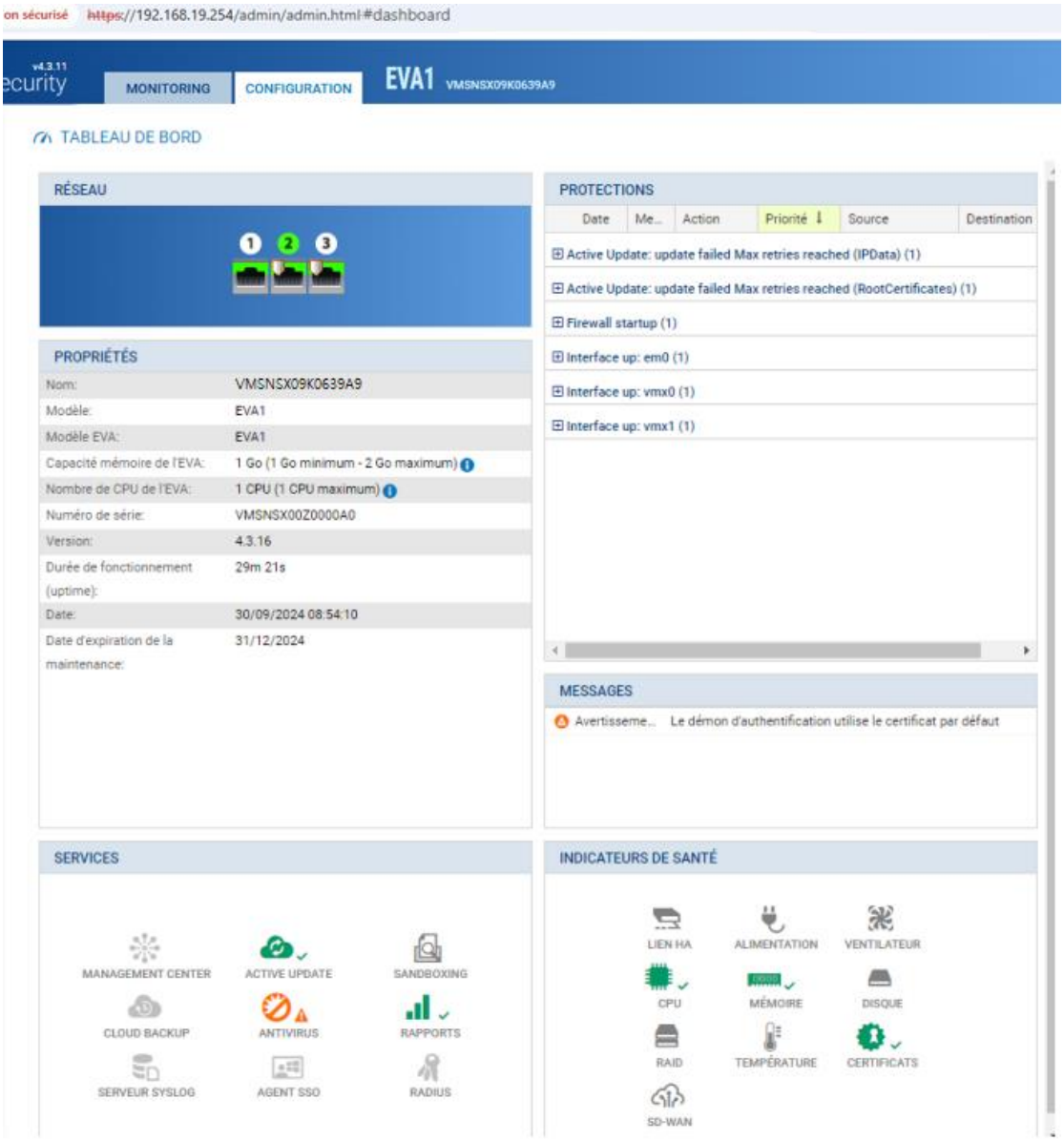
MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Configuration préalable du pare-feu Stormshield

Avant de configurer le VPN et les règles de NAT, plusieurs étapes essentielles ont été réalisées sur le pare-feu Stormshield afin d'assurer son bon fonctionnement et son intégration au réseau.

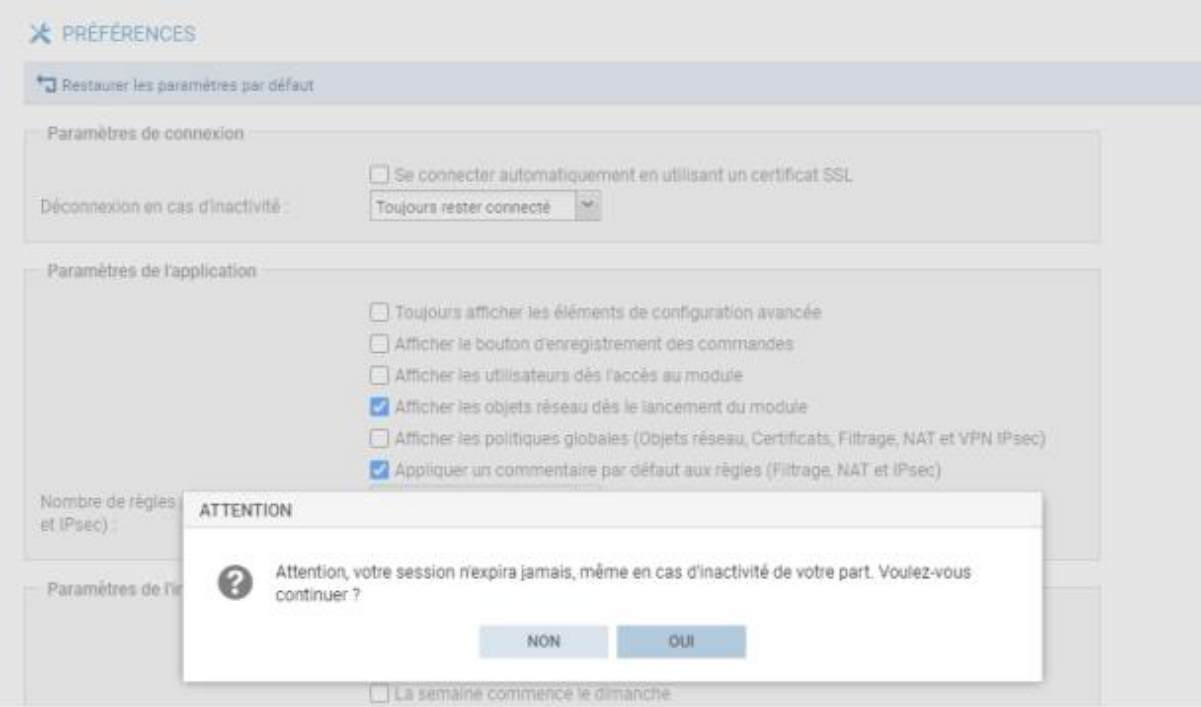
Accès à l'interface d'administration

Connexion à l'interface web du pare-feu via un navigateur en utilisant son adresse IP de gestion.
Authentification avec un compte administrateur.

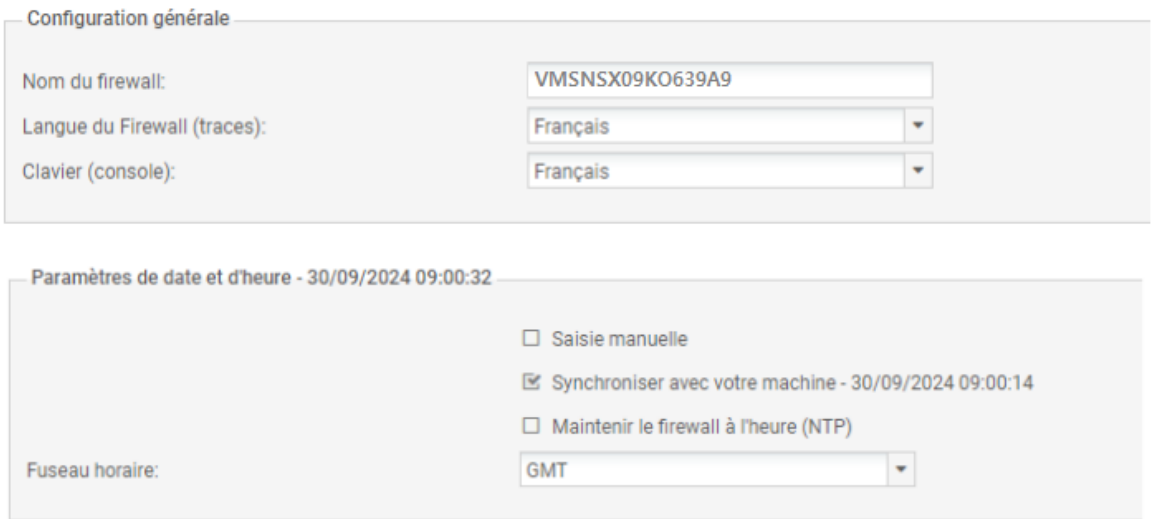


MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Modification des préférences pour empêcher la déconnexion pour inactivité :



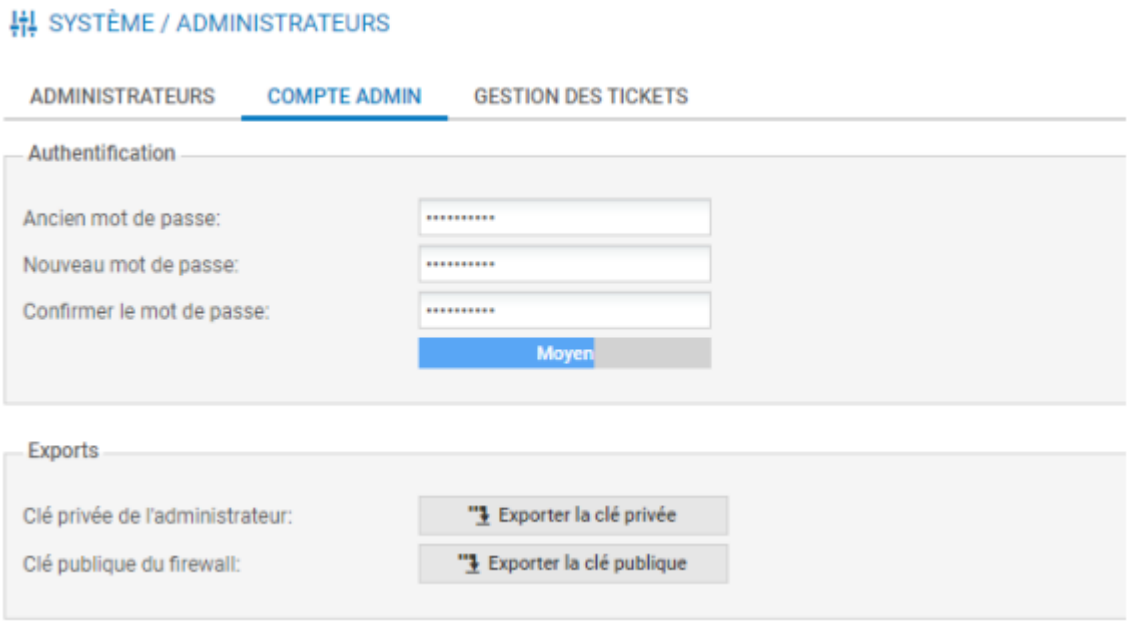
Configuration langue du firewall (traces) et fuseau horaire :



MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Ssh :

Modifier le mdp root :



Vérifiez que le stockage local des logs est activé sur le disque dur de la machine virtuelle. Réallouez le quota d'espace disque de la catégorie « Proxy POP3 » vers la catégorie « Connexions réseau », puis désactivez la catégorie « Proxy POP3 ». Enfin, activez l'enregistrement de tous les autres logs.

CONFIGURATION OF THE SPACE RESERVED FOR LOGS

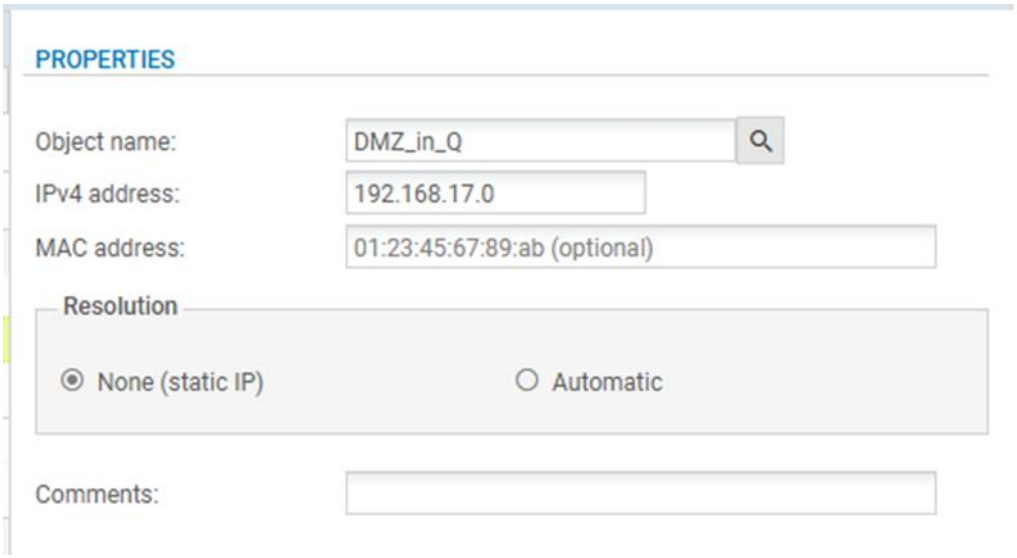
Enable all Disable all

Enabled	Family ↑	Percentage	Disk space quota
Enabled	Alarms	15	614.4 MB
Enabled	Authentication	2	81.9 MB
Enabled	Network connections	28	1.1 GB
Enabled	Filter policy	8	327.7 MB
Enabled	FTP proxy	2	81.9 MB
Enabled	Statistics	1	41 MB
Enabled	Network captures	2	81.9 MB
Enabled	Application connections (plugin)	14	573.4 MB
Disabled	POP3 proxy	0	–
Enabled	Vulnerability Manager	2	81.9 MB
Enabled	Router statistics	1	41 MB
Enabled	Sandboxing	1	41 MB
Enabled	Administration (serverd)	2	81.9 MB
Enabled	SMTP proxy	4	163.8 MB
Enabled	SSL proxy	3	122.9 MB
Enabled	System events	1	41 MB
Enabled	IPsec VPN	2	81.9 MB
Enabled	HTTP proxy	10	409.6 MB
Enabled	SSL VPN	2	81.9 MB

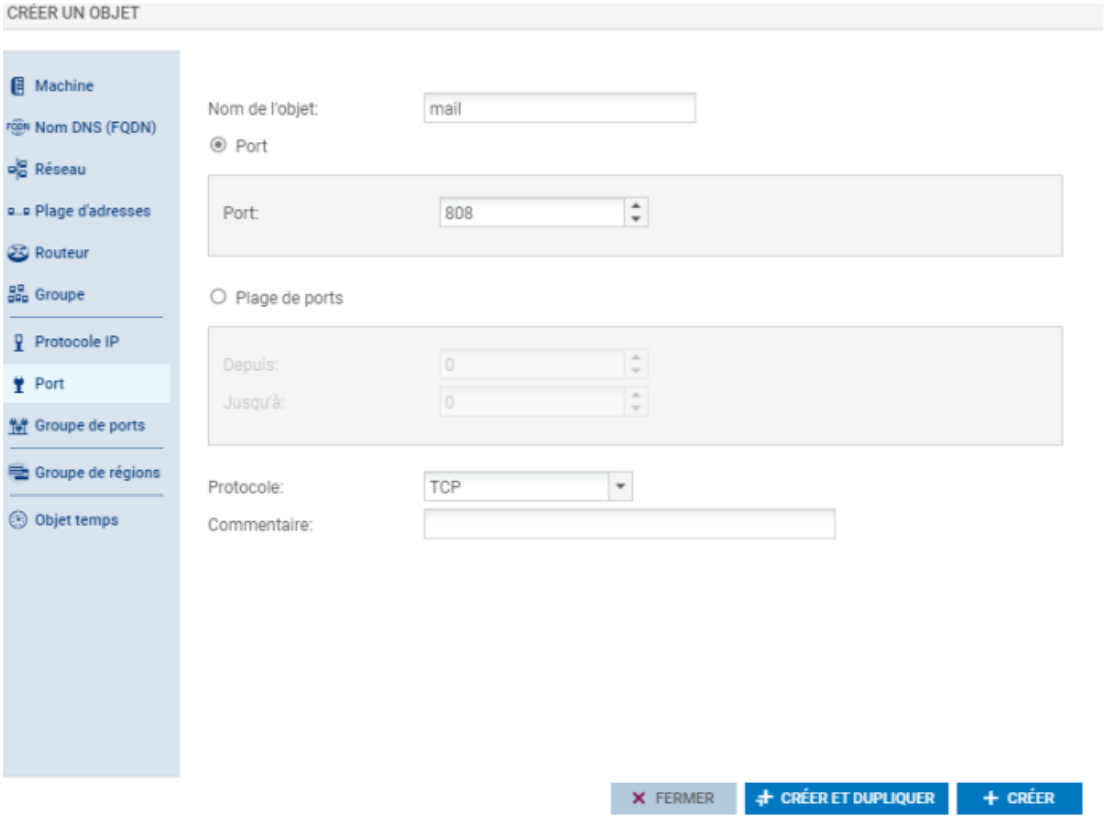
Total space used does not exceed available space (100%

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

1. Créer les objets machines et réseaux pour l'autre compagnie.



2. Ajouter un nouveau service basé sur le protocole TCP, fonctionnant sur le port 808, et le nommer 'webmail' :



Routage gateway VPN IPsec :

CREATE A REMOTE GATEWAY

SELECT THE GATEWAY - PEER CREATION WIZARD

Remote gateway: Entreprise_Q_Out²

Name: Site_in_Q

IKE version: IKEv2

CANCEL PREVIOUS NEXT

CREATE A REMOTE GATEWAY

SUMMARY - PEER CREATION WIZARD

Parameters of the remote site

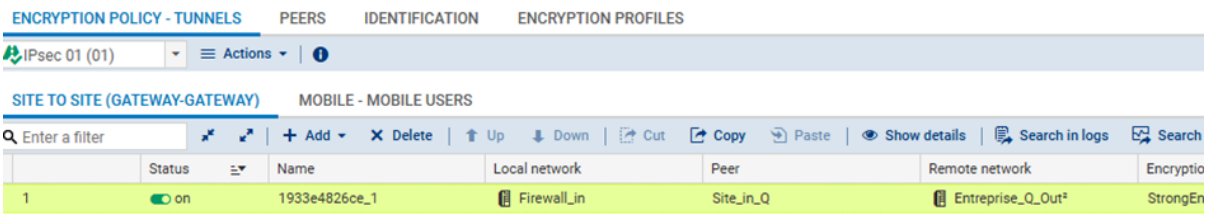
Name:	Site_in_Q
Remote gateway:	Entreprise_Q_Out²

Peer identification: pre-shared keys

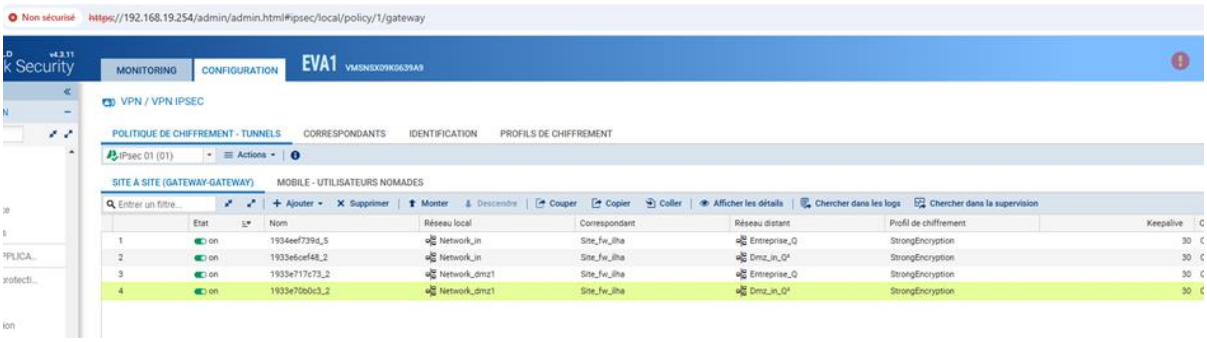
Pre-shared key:	P@ssword59

CANCEL PREVIOUS FINISH

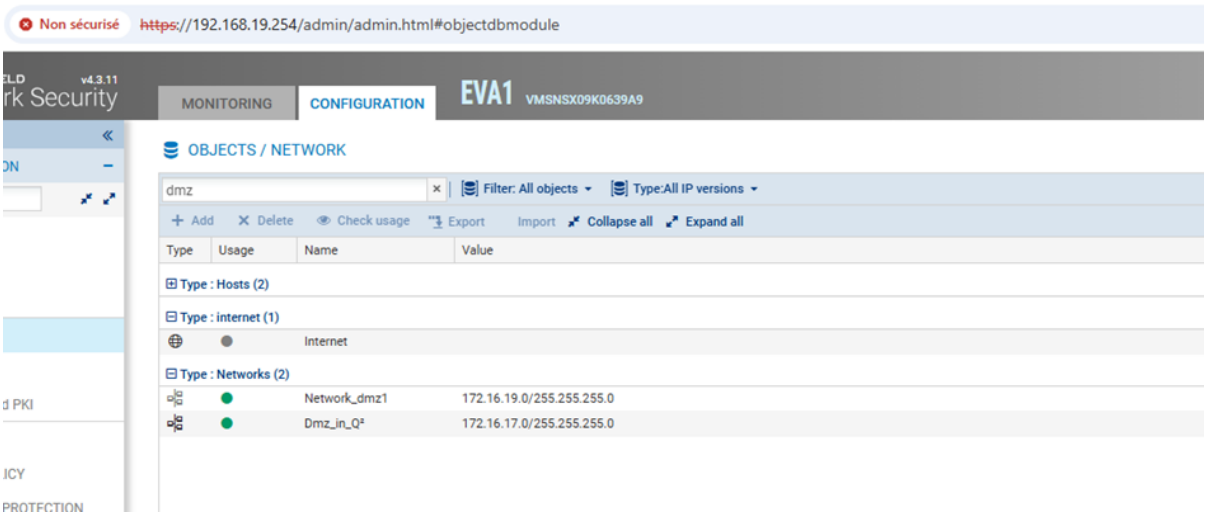
On peut constater que la route IPsec a bien été créée:



Voici tous les tunnels créés entre les deux entreprises :



Les deux DMZ des entreprises sont bien remontées et connectées à l'interface Stormshield :



MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Ping depuis ma machine cliente vers le réseau opposé:

```
user@client-training:~$ ping 192.168.17.254
PING 192.168.17.254 (192.168.17.254) 56(84) bytes of data.
64 bytes from 192.168.17.254: icmp_seq=1 ttl=64 time=27.5 ms
64 bytes from 192.168.17.254: icmp_seq=2 ttl=64 time=9.39 ms
64 bytes from 192.168.17.254: icmp_seq=3 ttl=64 time=8.73 ms
64 bytes from 192.168.17.254: icmp_seq=4 ttl=64 time=5.25 ms
64 bytes from 192.168.17.254: icmp_seq=5 ttl=64 time=2.63 ms
64 bytes from 192.168.17.254: icmp_seq=6 ttl=64 time=2.85 ms
64 bytes from 192.168.17.254: icmp_seq=7 ttl=64 time=8.70 ms
```

Configuration des règles NAT La table ci-dessus présente deux règles NAT configurées sur le pare-feu :

Status	Original traffic (before translation)				Traffic after translation				Protocol	Options
	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port		
on	Network_in	Internet interface: ou	Any	→	Firewall_out	ephemeral_fw	Any			
on	Internet Firewall_out interface: out	Firewall	http	→	Any	ephemeral_fw	srv_wet			

Sortie vers Internet : Cette règle permet aux machines du réseau interne (Network_in) d'accéder à Internet en utilisant l'adresse du pare-feu (Firewall_Out), masquant ainsi leurs adresses IP réelles.

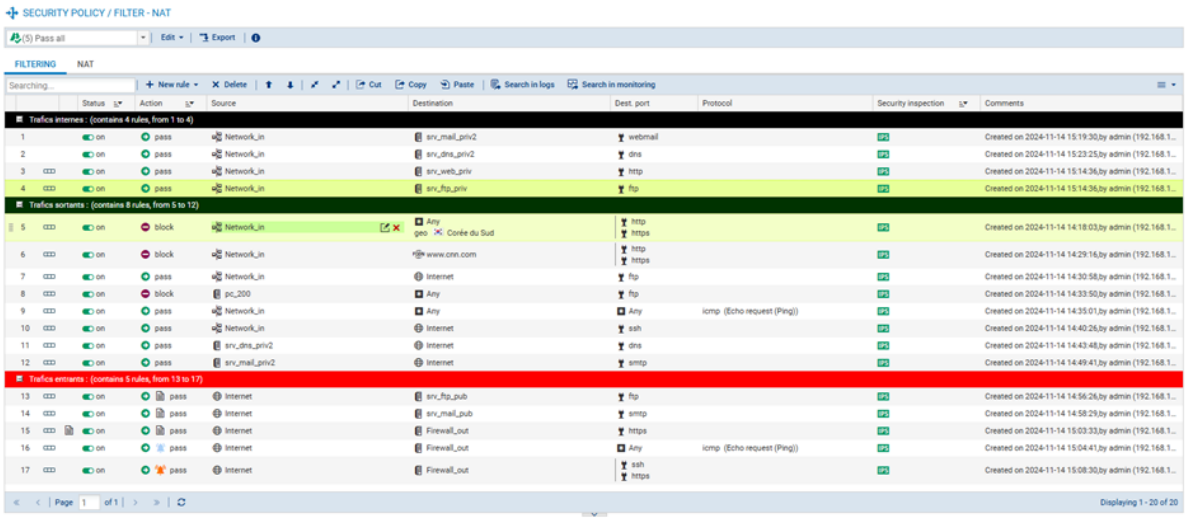
Redirection HTTP : Cette règle redirige le trafic HTTP entrant depuis Internet vers un serveur web interne (srv_web), permettant son accessibilité depuis l'extérieur.

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Connexion avec internet :

```
--- 192.168.19.254 ping statistics ---
19 packets transmitted, 6 received, 68.4211% packet loss, time 443ms
rtt min/avg/max/mdev = 0.570/0.767/1.297/0.244 ms
root@client-training:/home/user/Desktop# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=47 time=34.0 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=47 time=37.1 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=47 time=43.3 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=47 time=47.1 ms
^C
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 34.035/40.368/47.073/5.114 ms
root@client-training:/home/user/Desktop# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=43.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=35.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=45.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 35.605/41.610/45.586/4.319 ms
```

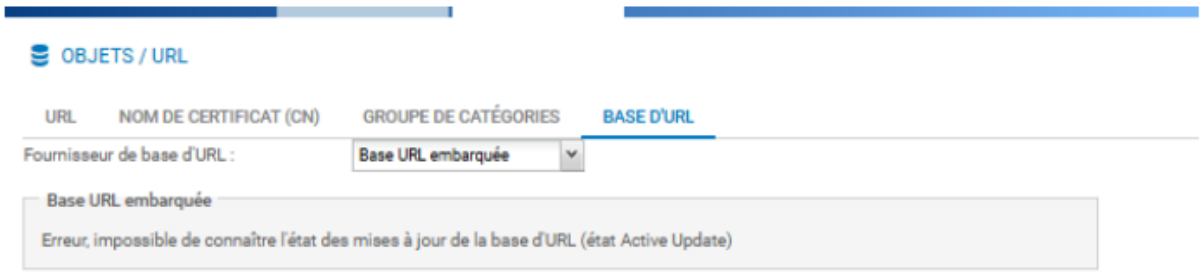
6 Filtrages / règles :



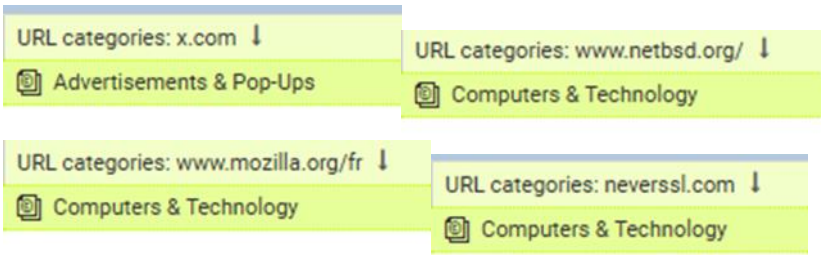
MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

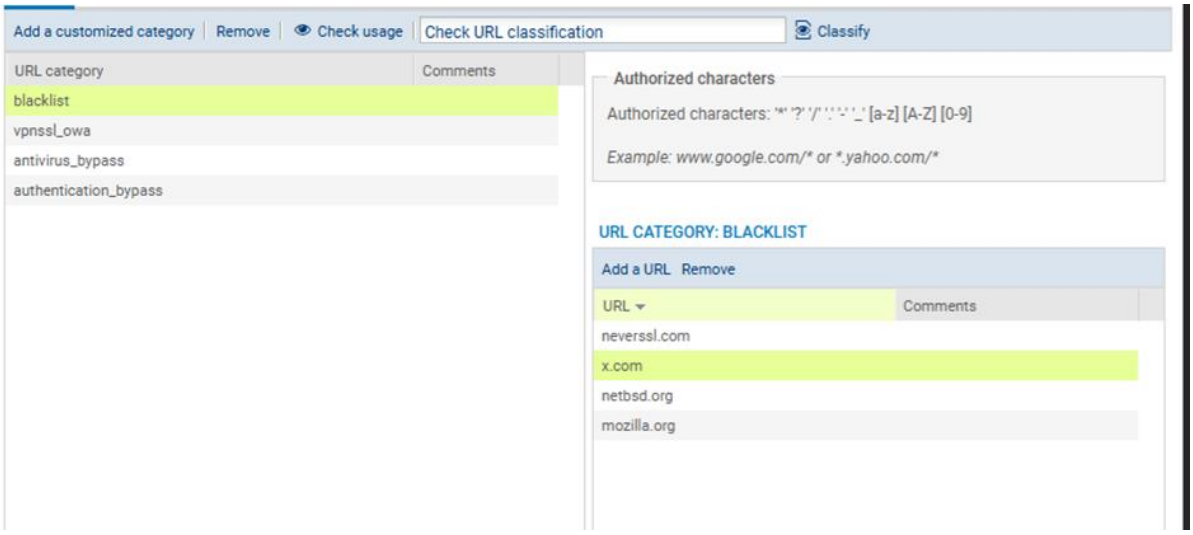
Proxy:

1.Selectionner la base d'URL embarquée



Trouvez les catégories dans lesquelles sont classées les URL twitter.com, www.netbsd.org, www.mozilla.org, neverssl.com:





MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Configurez une politique de filtrage des URL et une politique de filtrage SSL, permettant l'accès à tous les sites web, à l'exception de ceux mentionnés au point 2, ainsi que des sites des catégories 'shopping' et 'news'. Veillez toutefois à garantir l'accès au site bbc.com.

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

RATION **EVA1** VMSNSX09K0639A9

POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00 | Editer | Fournisseur de base URL : Extended Web Contr

+ Ajouter | ✕ Supprimer | Monter | Descendre | Couper | Copier | Coller

	État	Action	URL - CN	Commentaire
1	on	Passer sans déchiffrer	proxyssl_by...	don't decrypt some specific
2	on	Déchiffrer	any	default rule (decrypt all)
3	on	Passer sans déchiffrer	White-list	
4	on	Bloquer sans déchiffrer	Black-list	
5	on	Bloquer sans déchiffrer	blacklist	
6	on	Bloquer sans déchiffrer	Shopping	
7	on	Bloquer sans déchiffrer	News	

ONFIGURATION **EVA1** VMSNSX09K0639A9

POLITIQUE DE SÉCURITÉ / FILTRAGE URL

(0) URLFilter_00 | Editer | Fournisseur de base URL : Extended

+ Ajouter | ✕ Supprimer | Monter | Descendre | Couper | Copier

	État	Action	Catégorie d'URL	Commentaire
1	on	BlockPage_00	blacklist	
2	on	BlockPage_00	News	
3	on	BlockPage_00	shopping	
4	on	Passer	Any	