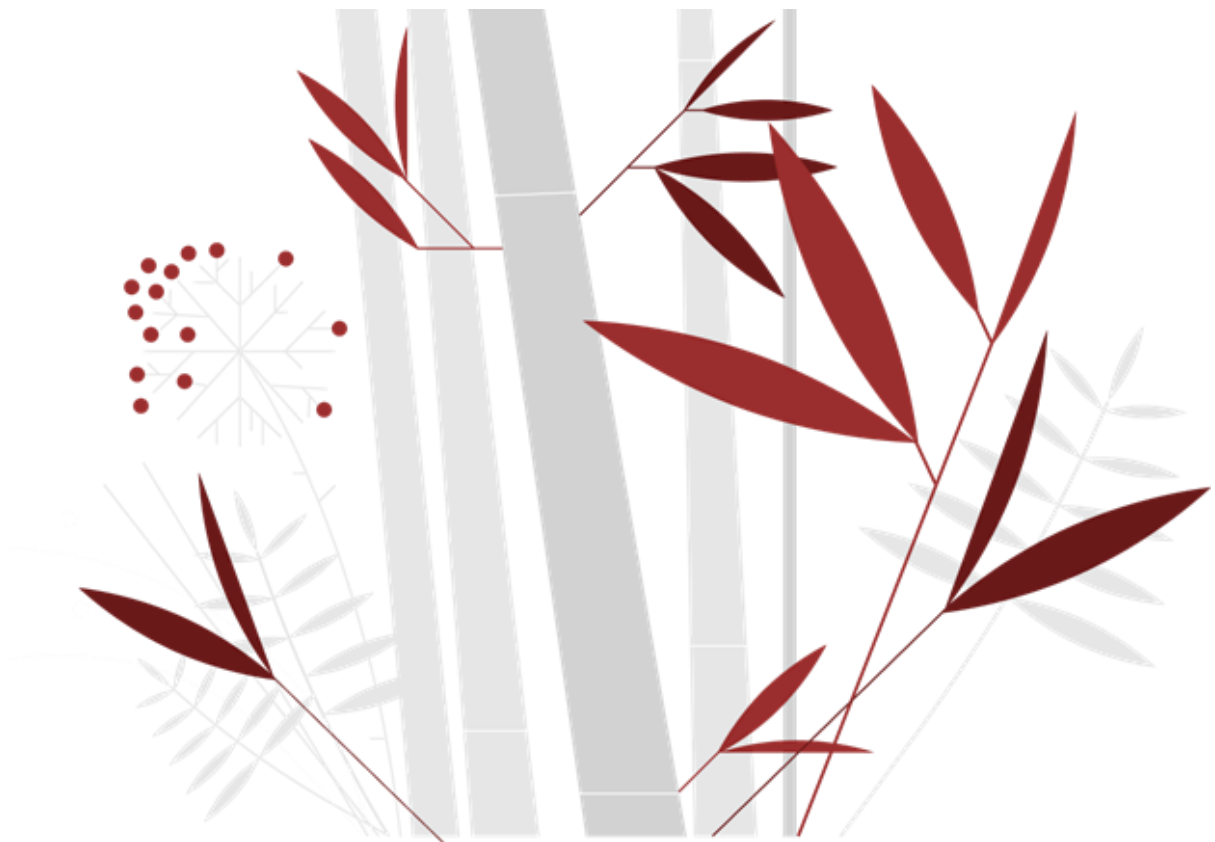


CONFIGURATION D'UN FIREWALL STORMSHIELD

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.

The screenshot displays the Stormshield administration interface. At the top, the browser address bar shows a secure connection to <https://192.168.19.254/admin/admin.html#dashboard>. The interface header includes the version 'v4.3.11', the 'Security' logo, navigation tabs for 'MONITORING' and 'CONFIGURATION', and the device name 'EVA1' with ID 'VMSNSX09K0639A9'. The main content area is titled 'TABLEAU DE BORD' and is divided into several sections:

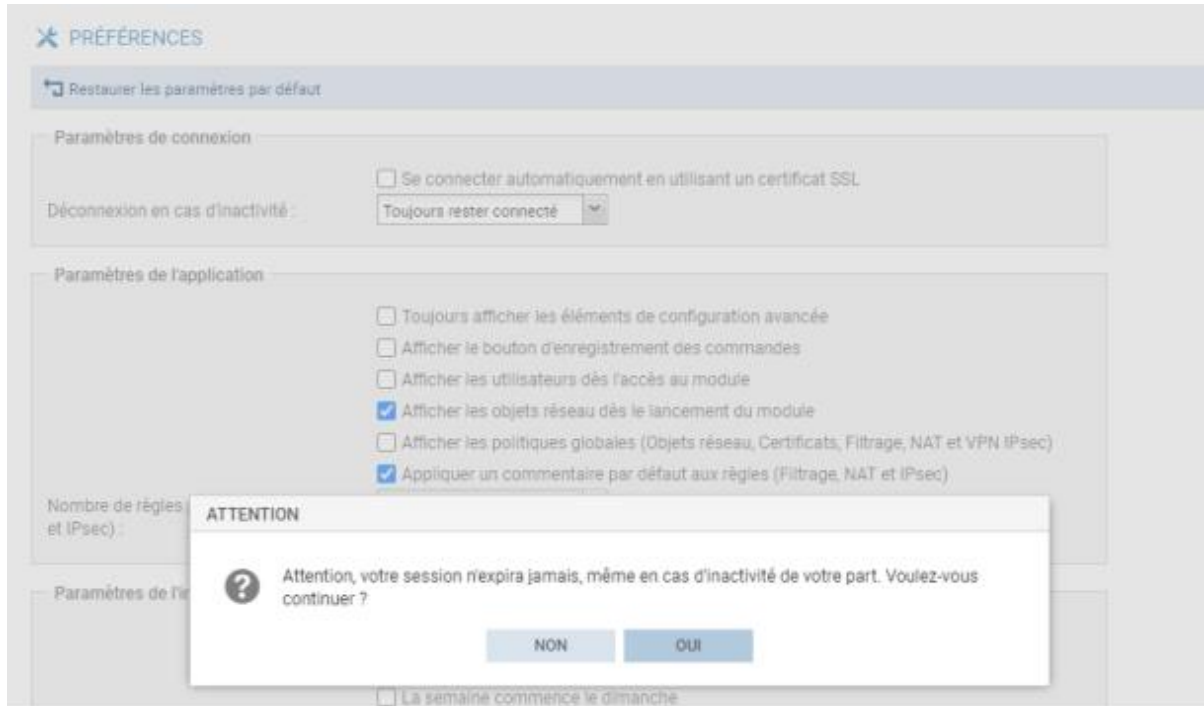
- RÉSEAU**: A section with three status indicators (1, 2, 3) and corresponding icons.
- PROPRIÉTÉS**: A table listing device details:

Nom:	VMSNSX09K0639A9
Modèle:	EVA1
Modèle EVA:	EVA1
Capacité mémoire de l'EVA:	1 Go (1 Go minimum - 2 Go maximum) ⓘ
Nombre de CPU de l'EVA:	1 CPU (1 CPU maximum) ⓘ
Numéro de série:	VMSNSX00Z0000A0
Version:	4.3.16
Durée de fonctionnement (uptime):	29m 21s
Date:	30/09/2024 08:54:10
Date d'expiration de la maintenance:	31/12/2024
- PROTECTIONS**: A table listing active protection rules:

Date	Me...	Action	Priorité ↓	Source	Destination
- MESSAGES**: A list of messages, including a warning: 'Avertissement... Le démon d'authentification utilise le certificat par défaut'.
- SERVICES**: A grid of service status icons including Management Center, Active Update, Sandboxing, Cloud Backup, Antivirus, Reports, Serveur Syslog, Agent SSO, and Radius.
- INDICATEURS DE SANTÉ**: A grid of health indicator icons for Lien HA, Alimentation, Ventilateur, CPU, Mémoire, Disque, RAID, Température, Certificats, and SD-WAN.

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Modification des préférences pour empêcher la déconnexion pour inactivité :



The screenshot shows the 'PRÉFÉRENCES' (Preferences) page in the Stormshield interface. A warning dialog box is overlaid on the page, asking for confirmation to continue because the session will never expire. The dialog box contains the following text: 'ATTENTION', a question mark icon, 'Attention, votre session n'expira jamais, même en cas d'inactivité de votre part. Voulez-vous continuer ?', and two buttons labeled 'NON' and 'OUI'. In the background, the 'Paramètres de connexion' (Connection parameters) section is visible, showing the 'Déconnexion en cas d'inactivité' (Disconnection in case of inactivity) dropdown menu set to 'Toujours rester connecté' (Always stay connected).

Configuration langue du firewall (traces) et fuseau horaire :

Configuration générale

Nom du firewall:

Langue du Firewall (traces):

Clavier (console):

Paramètres de date et d'heure - 30/09/2024 09:00:32

Saisie manuelle

Synchroniser avec votre machine - 30/09/2024 09:00:14

Maintenir le firewall à l'heure (NTP)

Fuseau horaire:

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD



Ssh :

Accès distant par SSH

Activer l'accès par SSH 

Autoriser l'utilisation de mot de passe

Utiliser le shell nsrpc pour les administrateurs autres que le compte admin

Port d'écoute:  

Modifier le mdp root :

SYSTÈME / ADMINISTRATEURS

ADMINISTRATEURS

COMPTE ADMIN

GESTION DES TICKETS

Authentification

Ancien mot de passe:


Nouveau mot de passe:

Confirmer le mot de passe:


Moyen

Exports

Clé privée de l'administrateur:

 Exporter la clé privée

Clé publique du firewall:

 Exporter la clé publique

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

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
<input checked="" type="checkbox"/> Enabled	Alarms	15	614.4 MB
<input checked="" type="checkbox"/> Enabled	Authentication	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	Network connections	28	1.1 GB
<input checked="" type="checkbox"/> Enabled	Filter policy	8	327.7 MB
<input checked="" type="checkbox"/> Enabled	FTP proxy	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	Statistics	1	41 MB
<input checked="" type="checkbox"/> Enabled	Network captures	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	Application connections (plugin)	14	573.4 MB
<input type="checkbox"/> Disabled	POP3 proxy	0	—
<input checked="" type="checkbox"/> Enabled	Vulnerability Manager	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	Router statistics	1	41 MB
<input checked="" type="checkbox"/> Enabled	Sandboxing	1	41 MB
<input checked="" type="checkbox"/> Enabled	Administration (serverd)	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	SMTP proxy	4	163.8 MB
<input checked="" type="checkbox"/> Enabled	SSL proxy	3	122.9 MB
<input checked="" type="checkbox"/> Enabled	System events	1	41 MB
<input checked="" type="checkbox"/> Enabled	IPsec VPN	2	81.9 MB
<input checked="" type="checkbox"/> Enabled	HTTP proxy	10	409.6 MB
<input checked="" type="checkbox"/> 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.

PROPERTIES

Object name:

IPv4 address:

MAC address:

Resolution

None (static IP) Automatic

Comments:

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

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Port

Port:

Plage de ports

Depuis:

Jusqu'à:

Protocole:

Commentaire:

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Routage gateway VPN IPsec :

CREATE A REMOTE GATEWAY

SELECT THE GATEWAY - PEER CREATION WIZARD



Remote gateway:

Name:

IKE version:

CREATE A REMOTE GATEWAY

SUMMARY - PEER CREATION WIZARD

Parameters of the remote site

Name:

Remote gateway:

Peer identification: pre-shared keys

Pre-shared key:

MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

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

The screenshot shows the configuration page for IPsec 01 (01) in Stormshield. The main tab is 'SITE TO SITE (GATEWAY-GATEWAY)'. Below the navigation bar, there is a table with the following data:

	Status	Name	Local network	Peer	Remote network	Encryption
1	on	1933e4826ce_1	Firewall_in	Site_in_Q	Entreprise_Q_Out	StrongEn

Voici tous les tunnels créés entre les deux entreprises :

The screenshot shows the configuration page for IPsec 01 (01) in Stormshield, displaying a list of tunnels. The table below summarizes the visible data:

Etat	Nom	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive
on	1934eef739d_5	Network_in	Site_fw_lha	Entreprise_Q	StrongEncryption	30 s
on	1933e6cef48_2	Network_in	Site_fw_lha	Dmz_in_Q²	StrongEncryption	30 s
on	1933a717c73_2	Network_dmz1	Site_fw_lha	Entreprise_Q	StrongEncryption	30 s
on	1933a7060c3_2	Network_dmz1	Site_fw_lha	Dmz_in_Q²	StrongEncryption	30 s

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

The screenshot shows the 'OBJECTS / NETWORK' configuration page in Stormshield. It displays a list of network objects. The table below summarizes the visible data:

Type	Usage	Name	Value
Hosts (2)			
internet (1)		Internet	
Networks (2)		Network_dmz1	172.16.19.0/255.255.255.0
		Dmz_in_Q²	172.16.17.0/255.255.255.0

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: out	Any	Firewall_Out	ephemeral_fw	Any			
on	Internet Firewall_Out interface: out	Firewall	http	Any	ephemeral_fw	srv_web			

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 :

The screenshot displays the 'SECURITY POLICY / FILTER - NAT' configuration page. It shows a list of 17 filtering rules, categorized into 'Trafics entrants' (rules 1-4 and 13-17) and 'Trafics sortants' (rules 5-12). Each rule is shown with its status, action, source, destination, destination port, protocol, security inspection status, and creation details.

Rule ID	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Trafics entrants (contains 4 rules, from 1 to 4)								
1	on	pass	Network_in	srv_mail_priv2	webmail		on	Created on 2024-11-14 15:19:30 by admin (192.168.1...
2	on	pass	Network_in	srv_dns_priv2	dns		on	Created on 2024-11-14 15:23:25 by admin (192.168.1...
3	on	pass	Network_in	srv_web_priv	http		on	Created on 2024-11-14 15:14:36 by admin (192.168.1...
4	on	pass	Network_in	srvftp_priv	ftp		on	Created on 2024-11-14 15:14:36 by admin (192.168.1...
Trafics sortants (contains 8 rules, from 5 to 12)								
5	on	block	Network_in	geo: Corée du Sud	http, https		on	Created on 2024-11-14 14:18:03 by admin (192.168.1...
6	on	block	Network_in	www.crm.com	http, https		on	Created on 2024-11-14 14:29:16 by admin (192.168.1...
7	on	pass	Network_in	Internet	ftp		on	Created on 2024-11-14 14:30:58 by admin (192.168.1...
8	on	block	pc_200	Any	ftp		on	Created on 2024-11-14 14:33:50 by admin (192.168.1...
9	on	pass	Network_in	Any	Any	icmp (Echo request (Ping))	on	Created on 2024-11-14 14:35:01 by admin (192.168.1...
10	on	pass	Network_in	Internet	ssh		on	Created on 2024-11-14 14:40:26 by admin (192.168.1...
11	on	pass	srv_dns_priv2	Internet	dns		on	Created on 2024-11-14 14:43:48 by admin (192.168.1...
12	on	pass	srv_mail_priv2	Internet	smtp		on	Created on 2024-11-14 14:49:41 by admin (192.168.1...
Trafics entrants (contains 5 rules, from 13 to 17)								
13	on	pass	Internet	srvftp_pub	ftp		on	Created on 2024-11-14 14:56:26 by admin (192.168.1...
14	on	pass	Internet	srv_mail_pub	smtp		on	Created on 2024-11-14 14:58:29 by admin (192.168.1...
15	on	pass	Internet	Firewall_out	https		on	Created on 2024-11-14 15:03:33 by admin (192.168.1...
16	on	pass	Internet	Firewall_out	Any	icmp (Echo request (Ping))	on	Created on 2024-11-14 15:04:41 by admin (192.168.1...
17	on	pass	Internet	Firewall_out	ssh, https		on	Created on 2024-11-14 15:08:30 by admin (192.168.1...

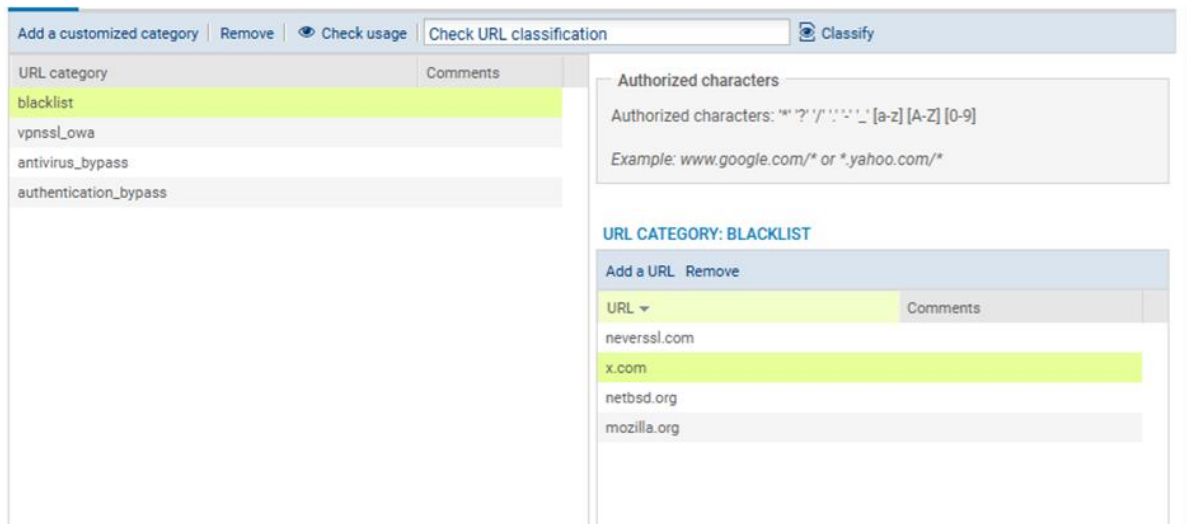
MISE EN PLACE ET CONFIGURATION D'UN FIREWALL STORMSHIELD

Proxy:

1. Sélectionner 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.

The screenshot shows the Stormshield configuration interface for 'EVA1' (VMSNSX09K0639A9). The 'CONFIGURATION' tab is active, and the 'OBJETS / URL' section is selected. The 'NOM DE CERTIFICAT (CN)' tab is active, showing a table with one entry: 'Whitelist' with the comment 'proxysl_bypass'. To the right, the 'Caractères autorisés' section explains the allowed characters: 'Les caractères autorisés sont : '' '' [a-z] [A-Z] [0-9] et ''*'. Le caractère '*' n'est valide que s'il est placé en début d'URL immédiatement suivi d'un point.' Below this, the 'CATÉGORIE DE CERTIFICATS : WHITELIST' section shows a table with three entries: '*.bbc.co.uk', '*.bbci.co.uk', and '*.bbc.com'. The entry '*.bbc.com' is highlighted in yellow.

The screenshot shows the Stormshield configuration interface for 'EVA1' (VMSNSX09K0639A9). The 'CONFIGURATION' tab is active, and the 'OBJETS / URL' section is selected. The 'NOM DE CERTIFICAT (CN)' tab is active, showing a table with three entries: 'Black-list', 'White-list', and 'proxysl_bypass'. The 'Black-list' entry is highlighted in yellow. To the right, the 'Caractères autorisés' section explains the allowed characters: 'Les caractères autorisés sont : '' '' [a-z] [A-Z] [0-9] et ''*'. Le caractère '*' n'est valide que s'il est placé en début d'URL immédiatement suivi d'un point.' Below this, the 'CATÉGORIE DE CERTIFICATS : BLACK-LIST' section shows a table with three entries: '*.twitter.com', '*.netbsd.org', and '*.mozilla.org'. The entry '*.mozilla.org' is highlighted in yellow.

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 X Supprimer ↑ Monter ↓ Descendre ✂ Couper 📄 Copier 📄 Coller					
	État	Action	URL - CN	Commentaire	
1	<input checked="" type="checkbox"/> on	Passer sans déchiffrer	proxyssl_by...	don't decrypt some specific	
2	<input checked="" type="checkbox"/> on	Déchiffrer	any	default rule (decrypt all)	
3	<input checked="" type="checkbox"/> on	Passer sans déchiffrer	White-list		
4	<input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	Black-list		
5	<input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	blacklist		
6	<input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	Shopping		
7	<input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	News		

ONFIGURATION

EVA1

VMSNSX09K0639A9

➔ POLITIQUE DE SÉCURITÉ / FILTRAGE URL

(0) URLFilter_00					
Editer					
Fournisseur de base URL : Extended					
+ Ajouter X Supprimer ↑ Monter ↓ Descendre ✂ Couper 📄 Copier					
	État	Action	Catégorie d'URL	Commentaire	
1	<input checked="" type="checkbox"/> on	BlockPage_00	blacklist		
2	<input checked="" type="checkbox"/> on	BlockPage_00	News		
3	<input checked="" type="checkbox"/> on	BlockPage_00	shopping		
4	<input checked="" type="checkbox"/> on	Passer	Any		