

Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

Situation 3 : Mise en œuvre du filtrage protocolaire

Fiches Stormshield associées :

- Fiche 5 – Configuration des objets réseaux
- Fiche 7 – Filtrage protocolaire

Le pare-feu Stormshield utilise la notion d'objet qui est brièvement explicitée dans **le document 1** (exemple : un serveur ou un réseau est représenté sous forme d'objet respectant une convention de nommage sur l'interface d'administration). Sur l'interface d'administration SNS de Stormshield, la création et l'utilisation d'objets sont indispensables à la mise en œuvre des différentes technologies qui nous intéressent ici. *Pour des détails sur les objets, cf. à la fiche 5.*

Le document 2 compare une table de filtrage « papier » et une table de filtrage sur SNS.

Les documents 3 et 4 explicitent une liste de recommandations de l'ANSSI que nous allons mettre en œuvre dans cette situation.

Le DSI de l'entreprise CUB vous propose un extrait de la table de filtrage à implémenter sur chaque site. Voici sa proposition pour le site d'Anvers et qui devra être réadaptée en fonction de chaque zone géographique.

N°	Adresse IP Source	Port S	Adresse IP Destination	Port D	Proto	Action
1	*	>1023	192.168.1.10	*	*	Autoriser
2	*	>1023	192.168.1.11	*	*	Autoriser
3	192.168.1.128/26	*	*	*	*	Autoriser
4	192.168.1.0/25	*	192.168.1.128/26	*	*	Autoriser
5	192.168.1.0/25	>1023	*	22, 80, 443	TCP	Autoriser
6	192.168.1.0/25	>1023	*	53,123	UDP	Autoriser
7	192.168.1.0/25	NA	*	NA	ICMP	Autoriser
8	192.168.1.0/24	*	*	*	*	Autoriser

Légende :

- VLAN de Production de l'Agence d'Anvers = 192.168.1.0/25 ;
- VLAN d'Administration de l'Agence d'Anvers = 192.168.1.128/26 ;
- DMZ de l'Agence d'Anvers = 172.16.1.0/24 ;
- SSH = port 22/TCP, DNS = port 53/UDP, HTTP = port 80/TCP, NTP = port 123/UDP, HTTPS = port 443/TCP.

I Analyse et amélioration de la table de filtrage proposée

L'objectif de cette première partie est de proposer, **à l'aide des documents 3 et 4**, une amélioration de l'extrait de la politique de filtrage initiale « papier » qui tiendra compte à la fois du modèle de sécurité positif (tout ce qui n'est pas explicitement autorisé est interdit) mais également de la structure et des recommandations préconisées par l'ANSSI (5 ou 6 sections distinctes).

Q1. Expliquer les règles n° 1 et 2 et proposer, en justifiant, une éventuelle évolution.

Q2. Expliquer les règles n° 3 et 4 et dire en argumentant si elles sont conformes aux recommandations de l'ANSSI figurant dans le document 4

Le VLAN de Production doit se limiter à des usages réseaux basiques (Web, DNS, NTP). L'accès au web doit absolument être contrôlé par un serveur mandataire (proxy) web dédié pour l'ensemble des réseaux internes afin de renforcer la sécurité. Dans le cas des pare-feu Stormshield, un proxy transparent est inclus dans l'appliance, la redirection sera donc précisée par la suite dans les options des règles de filtrage.

Q3. Dire en argumentant si les règles n°5, 6 et 7 sont conformes à l'exposé ci-dessus.

Q4. Dire quelles sont les deux règles générales manquantes.

Q5. Proposer des modifications et améliorations à apporter aux règles de filtrage en les classant dans les 5 sections préconisées (document 3). *Les règles de filtrage concernant le VLAN de production seront appliquées à l'identique au VLAN Client.*

NB : il est possible que des lignes ne soient pas utilisées.

N°	Adresse IP Source	Port S	Adresse IP Destination	Port D	Proto	Action
Section 1 – Règles d'autorisation à destination du pare-feu						
Section 2 – Règles de protection du pare-feu						
Section 3 – Règles d'autorisation des flux métiers						
Section 4 – Règles d'autorisation pour la DMZ						
Section 5 – Règle d'interdiction finale						

II Mise en œuvre de la politique de filtrage défini

➤ Implémenter sur le pare-feu les règles précédemment définies.



Vous pouvez supprimer vos règles de NAPT mise en œuvre dans la précédente situation et intégrer la redirection de ports permettant l'accès aux services web et dns présents dans la DMZ directement dans les règles de filtrage (règles 1 et 2). L'avantage de cette solution est l'optimisation du traitement du flux.



À noter que si l'administration du pare-feu est permise via l'interface OUT, l'ajout de la règle de redirection vers le protocole HTTPS ne sera jamais évaluée. En effet, le flux HTTPS d'administration du pare-feu étant accepté via une règle implicite, le paquet n'est donc pas confronté aux règles de filtrage ajoutées par l'administrateur.

➤ Tester les règles implémentées

En consultant les traces, vous confirmerez également :

- le traitement de chaque flux par la règle de filtrage qui lui correspond.
- le traçage et la levée des alarmes pour les règles demandées.



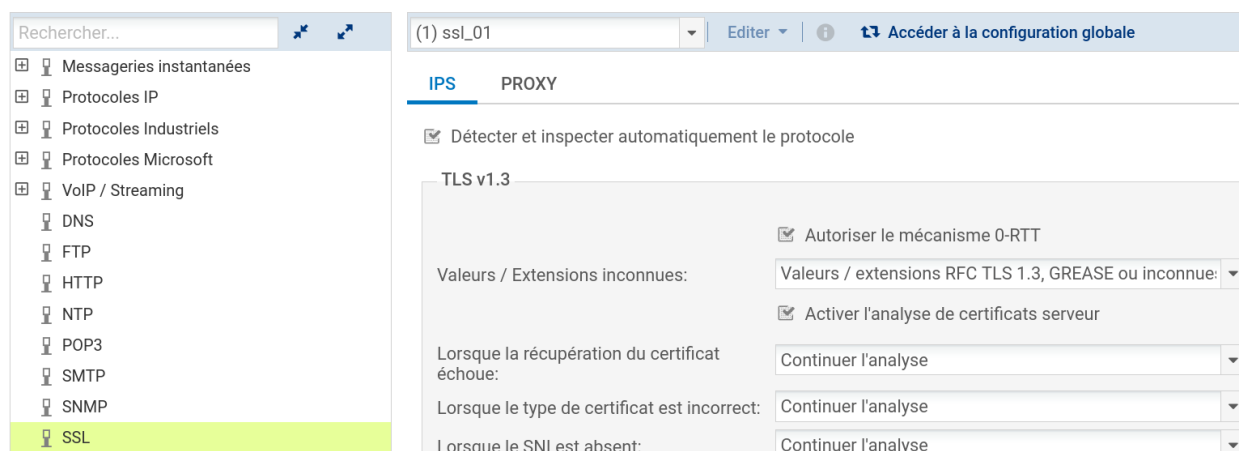
Une fois les règles implémentées et activées, l'accès à internet **via Firefox** peut être bloqué, car ce navigateur active par défaut l'utilisation du « 0-RTT » via TLS 1.3 et, comme le préconise l'ANSSI (recommandation R23 du guide https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf), le pare-feu Stormshield interdit l'utilisation de ce mécanisme (les flux bloqués sont visibles dans « Monitoring → Alarmes »).

Pour désactiver le « 0-RTT » sous firefox, saisir « about:config » dans la barre de recherche du navigateur et passer la valeur de « security.tls.enable_Ortt_data » à « false » :



Il serait à priori possible de permettre 0-RTT sur le pare-feu Stormshield en cochant la case « Autoriser le mécanisme 0-RTT » sur les **deux premiers profils** dans le menu PROTECTION APPLICATIVE / PROTOCOLE puis SSL :

PROTECTION APPLICATIVE / PROTOCOLES



III Implémentation de nouveaux besoins

Suite à une analyse des besoins de l'entreprise et des fonctionnalités avancées de l'appliance Stormshield, le RSSI vous demande de prendre en compte les besoins suivants.

- A) Interdire explicitement les plages d'adresses du groupe RFC 5735¹ provenant d'Internet.
- B) Toutes les machines provenant d'Internet et ayant une réputation de Botnet, Malware, Scanneur, Noeud de sortie Tor, Anonymiseur ou Phishing ont interdiction d'accéder à l'interface externe du firewall.
- C) L'ensemble des hôtes du site ont interdiction de pouvoir émettre des requêtes vers des machines sur Internet considérées comme Botnet, Malware, Scanneur, Noeud de sortie Tor, Anonymiseur ou Phishing.

¹ La RFC 5735 définit les adresses IPv4 réservées à des usages spécifiques et particuliers (<https://tools.ietf.org/html/rfc5735#section-5>).

Documents

Document 1 : la notion d'objets réseaux dans l'interface d'administration SNS

Les objets réseaux sont un concept très important à appréhender pour être à l'aise avec l'administration d'un pare-feu Stormshield. En effet, au lieu de déclarer un hôte, un réseau, un port sous forme d'adresse IP ou de numéro, cela passera par la création et l'utilisation d'un objet qui respectera une convention de nommage propre à chaque structure.

L'intérêt d'utiliser des objets réseaux est multiple :

- une convention de nommage est davantage explicite qu'une adresse IP ou un numéro de port. Elle permet une identification plus rapide de l'information ;
- en cas de changement d'adresse IP ou de numéro de port, il sera nécessaire de modifier uniquement l'information contenue dans l'objet et non dans l'ensemble des règles de sécurité ;
- un certain nombre d'objets réseaux est créé par défaut. Il permet à l'administrateur de gagner du temps lors de la configuration du pare-feu.

Document 2 : comparaison entre une table de filtrage « papier » et une table de filtrage sur SNS

N°	Adresse IP Source	Port S	Adresse IP Destination	Port D	Proto	Action
1	*	>1023	192.168.0.1	25	TCP	Autoriser
2	192.168.192.16	>1023	192.168.192.254	22, 443	TCP	Autoriser
3	*	*	192.168.0.254 192.168.192.16854 192.168.20.254 192.168.30.254 194.0.0.1	*	*	Bloquer
4	192.168.20.0/24	>1023	*	80, 443	TCP	Autoriser
5	192.168.20.0/24	>1023	192.168.30.1	53	UDP	Autoriser
6	192.168.30.1	*	*	53	TCP/ UDP	Autoriser
7	*	*	*	*	*	Bloquer

Cette table de filtrage est celle d'un pare-feu « stateful » ainsi les règles correspondantes à des réponses à une connexion préalablement établie et autorisée sont implicites. Le filtrage se fait ici uniquement en entrée.

Légende aidant à la compréhension du tableau suivant :

- VLAN 10 Administration = 192.168.10.0/24
- VLAN 20 Production = 192.168.20.0/24
- VLAN 30 Serveurs = 192.168.30.0/24
- DMZ = 192.168.0.0/24
- PC d'administration = 192.168.192.16/32
- Serveur DNS récursif = 192.168.30.1/32
- Serveur Mail en DMZ = 192.168.0.1/32
- Interfaces du pare-feu = 192.168.0.254, 192.168.192.254, 192.168.20.254, 192.168.30.254, 194.0.0.1
- N'importe quelles adresses IP = * (Any, Toutes ou 0.0.0.0/0)
- SSH = port 22/TCP, SMTP = port 25/TCP, DNS = port 53, HTTP = port 80/TCP, HTTPS = port 443/TCP, Tous les ports = *, Ports clients = >1023.

(5) Filtrage-SIO

Editer

Exporter

FILTRAGE

NAT

Rechercher...

+ Nouvelle règle

✕ Supprimer

↑

↓

↔

↔

✂ Couper

📋 Copier

📄 Coller

🔍 Chercher dans les logs

🔍 Chercher dans

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
Accès depuis l'extérieur à la DMZ (contient 1 règles, de 1 à 1)							
1	<div><div></div><div>on</div></div>	<div>passer</div>	<div>Internet</div> <div>interface: out</div>	<div>Firewall_out</div> <div>→ srv_mail_dmz</div>	<div>smtp</div>		<div>IPS</div>
Règles de sécurité concernant les connexions au firewall (contient 2 règles, de 2 à 3)							
2	<div><div></div><div>on</div></div>	<div>passer</div>	<div>pc_admin</div>	<div>Firewall_in_vlan10</div>	<div>ssh</div> <div>https</div>		<div>IPS</div>
3	<div><div></div><div>on</div></div>	<div>bloquer</div>	<div>Any</div>	<div>Firewall_all</div>	<div>Any</div>		<div>IPS</div>
Filtrage concernant le VLAN 20 de production (contient 2 règles, de 4 à 5)							
4	<div><div></div><div>on</div></div>	<div>passer</div>	<div>vlan_20_prod</div>	<div>Internet</div>	<div>http</div> <div>https</div>		<div>IPS</div>
5	<div><div></div><div>on</div></div>	<div>passer</div>	<div>vlan_20_prod</div>	<div>srv_dns_vlan30</div>	<div>dns_udp</div>		<div>IPS</div>
Filtrage concernant le VLAN 30 serveurs (contient 1 règles, de 6 à 6)							
6	<div><div></div><div>on</div></div>	<div>passer</div>	<div>srv_dns_vlan30</div>	<div>Internet</div>	<div>dns</div>		<div>IPS</div>
Règle de blocage par défaut (moindres privilèges) (contient 1 règles, de 7 à 7)							
7	<div><div></div><div>on</div></div>	<div>bloquer</div>	<div>Any</div>	<div>Any</div>	<div>Any</div>		<div>IPS</div>

Stormshield permet d'organiser les règles de filtrage à l'aide de séparateurs colorés afin de gagner en lisibilité. Il est également possible de donner un nom à chaque règle. Pour cela, il suffit de demander à afficher la colonne « nom » dans la table de filtrage.

- Le serveur mail disposant d'une adresse IP privée, son accès depuis l'extérieur se fait par l'interface externe du pare-feu. La première règle combine à la fois une autorisation au niveau du filtrage et une redirection de port.
- L'objet Internet correspond à toutes les adresses IP différentes des adresses IP internes alors que l'objet Any englobe absolument toutes les adresses IP.
- L'objet Firewall_all est un groupe contenant l'ensemble des interfaces du pare-feu.
- Les ports sources ne sont, par défaut, pas représentés. Il est toutefois possible de forcer l'utilisation d'une plage de ports particulière si on le souhaite.

Document 3 : extrait « des recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu » publiées par l'ANSSI

L'organisation proposée est construite selon un modèle de sécurité positif (tout ce qui n'est pas explicitement autorisé est interdit), il est possible de la décomposer en 6 sections rigoureusement ordonnées de la façon suivante :

Ordre	Contenu
Section n°1	Règles d'autorisation des flux à destination du pare-feu
Section n°2	Règles d'autorisation des flux émis par le pare-feu
Section n°3	Règle de protection du pare-feu
Section n°4	Règles d'autorisation des flux métiers
Section n°5	Règles "antiparasites" (facultatif)
Section n°6	Règle d'interdiction finale

Section n°1

Les règles de sécurité qui autorisent l'accès aux services proposés par un pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément, en particulier au niveau de leurs adresses sources et de leurs services (HTTPS pour l'accès à l'interface d'administration, SNMPv3 pour la supervision).

Section n°2

Les règles de sécurité qui autorisent les flux ayant pour origine le pare-feu doivent être regroupées dans la politique de filtrage. Ces règles sont peu nombreuses et doivent être définies précisément : service d'envoi de journaux, service d'alerte (trap SNMP), service de sauvegarde (SSH ou HTTPS).

Section n°3

Cette section ne comporte qu'une seule règle dite de protection de la passerelle :

Source	Destination	Service	Action	Journalisation
Toutes	Toutes les interfaces du pare-feu	Tous	Interdire	Oui

La mise en place d'une règle de protection du pare-feu est impérative pour prévenir l'ouverture de flux non légitimes à destination de la passerelle ; la journalisation de cette règle permet de conserver la trace de ces flux illégitimes.

Section n°4

Les règles qui autorisent les flux métiers doivent être regroupées et organisées selon une logique établie et adaptée au contexte. Ces règles constituent l'essentiel de la politique de filtrage, elles doivent être définies précisément au niveau de leurs adresses sources, de leurs adresses de destination et de leurs services.

Il faut être le plus restrictif possible en n'autorisant que le strict nécessaire permettant de respecter les besoins métiers liés à chaque zone du réseau. Éviter lorsque cela est possible des plages d'adresse IP trop larges, des plages de ports trop étendues.

Section n°5 (facultatif)

Les règles "antiparasites" peuvent être utilisées pour alléger les journaux de la passerelle, mais doivent être établies en accord avec la politique globale de journalisation de l'architecture. Elles permettent de rendre les fichiers journaux plus exploitables en évitant de garder des traces (exemple : flux de diffusion netbios, dhcp) inutiles.

Section n°6

L'ajout d'une règle explicite d'interdiction finale journalisée garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de conserver la trace des flux non légitimes.

NB : La règle de blocage par défaut explicite avec journalisation préconisée par l'ANSSI est sujette à interprétation. L'entreprise Stormshield recommande généralement d'éviter cette règle car mal configurée, elle peut générer un bruit conséquent à l'intérieur des fichiers journaux et les rendre ainsi difficilement exploitables. Ainsi cette règle n'est pertinente que si l'ensemble des protocoles bloqués générant du bruit inutile n'est pas journalisé au préalable (NETBIOS par exemple). C'est d'ailleurs ce que recommande clairement l'ANSSI dans son guide de configuration.

Conseils généraux

- Définir une convention de nommage à respecter ;
- Définir une convention de coloration pour avoir une meilleure analyse visuelle ;
- Expliciter à l'aide de commentaires les règles de filtrage créées ;
- Dans la mesure du possible, limiter l'utilisation de règles implicites ;
- Les consignes de filtrage doivent être documentées ;
- La politique de filtrage doit être testée et passée en revue deux fois par an.

Document 4 : extrait « des recommandations pour la sécurisation d'un pare-feu Stormshield SNS » publiées par l'ANSSI

Précisions sur la gestion du réseau d'Administration

Idéalement, un équipement SNS doit être raccordé à un réseau d'administration sur une interface Ethernet dédiée (une sous-interface virtuelle peut être envisagée si aucune interface Ethernet physique n'est disponible). Il ne doit être administrable que depuis ce réseau et cette interface. La politique de filtrage doit être configurée afin de n'autoriser l'accès aux services d'administration de l'équipement (HTTPS et non SSH) qu'aux adresses IP des postes d'administration déclarées dans le groupe défini pour cet usage.

L'administrateur réseau doit séparer ses usages d'administration et de bureautique. Ainsi, son poste dédié à l'administration ne doit pas avoir accès à Internet (où un accès restreint aux serveurs de mises à jour de l'OS uniquement). Il est également d'usage de se connecter avec un compte utilisateur restreint. Lorsqu'il souhaite avoir des usages bureautiques, il doit utiliser un autre poste présent en dehors du réseau d'Administration. Il est envisageable de pouvoir se connecter au poste « bureautique » depuis le poste d'Administration à l'aide d'un protocole de « bureau à distance » comme RDP. La mise en place d'un poste unique mais avec des conteneurs ou VM qui séparent et isolent les usages peut être aussi envisagée (cf QubesOS ou Clip OS).

La technologie Anti-usurpation

Il est important d'activer l'anti-spoofing sur les interfaces réseaux internes. Cette technologie permet au firewall de s'assurer que les adresses IP sources des paquets reçus sont bien légitimes. Sur SNS, lorsque vous définissez une interface comme une interface protégée. Le mécanisme anti-spoofing est effectif.

Recommandations générales

- Il est recommandé de désactiver les interfaces réseau non utilisées.
- Il est recommandé d'interdire explicitement les plages d'adresses du groupe RFC 5735 provenant d'Internet.
- Il est recommandé de renommer la politique de filtrage de production
- Il est recommandé de définir une politique de journalisation locale et une politique de journalisation centralisée