1. Activité : Mise en œuvre du filtrage

1.1. Ressources

Aidez-vous des fiches suivantes :

- Fiche 5 – Configuration des objets réseaux
- Fiche 6 - configuration du NAT
- Fiche 7 – Filtrage protocolaire

1.2. Présentation de l'activité

Le pare-feu Stormshield utilise la notion d'**objet** qui permet par exemple de représenter un **serveur (Host)** ou un **réseau (Network)** en respectant une convention de nommage sur l'interface d'administration. Des précisions sur le objets sont données dans le **document 1**.

Sur l'interface d'administration SNS de Stormshield, la création et l'utilisation d'objets sont **indispensables** à la mise en œuvre des différentes fonctionnalités du pare-feu.

Exercices

1.2.1. 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.

1.3. Analyse du filtrage proposé

Vous devez mettre en place des règles de règles de filtrage pour sécuriser votre infrastrcture en tenant compte des informations suivantes :

- vous ne devez autoriser que les flux nécessaires entre les différents réseaux. Tous les autres flux doivent être bloqués.
- le serveur DNS (VLAN serveur) a l'adresse IP 192.168.228.125/26

Voici un extrait de la table de filtrage à implémenter sur votre pare-feu.

N°	Adresse IP Source	Port Source	Adresse IP Destination	Port Destination	Proto(cole)	Action
1	*	>1023	192.168.228.125	*	*	Autoriser
2	adresse réseau Wifi	>1023	adresse réseau serveurs	*	*	Autoriser
3	adresse réseau utilisateur	>1023	*	22, 80, 443	TCP	Autoriser
4	adresse réseau utilisateur	>1023	*	53	UDP	Autoriser

Question 1 : expliquez chacune des quatres règles puis proposer éventuellement une modification.

Question 2 : quelles sont les deux règles générales qui manquent ?

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

Question 3 : quel est, selon vous, l'intérêt de la règle 3 ?

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

Voici à titre d'exemple la **traduction** d'une **proposition** de table de filtrage et sa mise en oeuver avec le SNS Stormshield

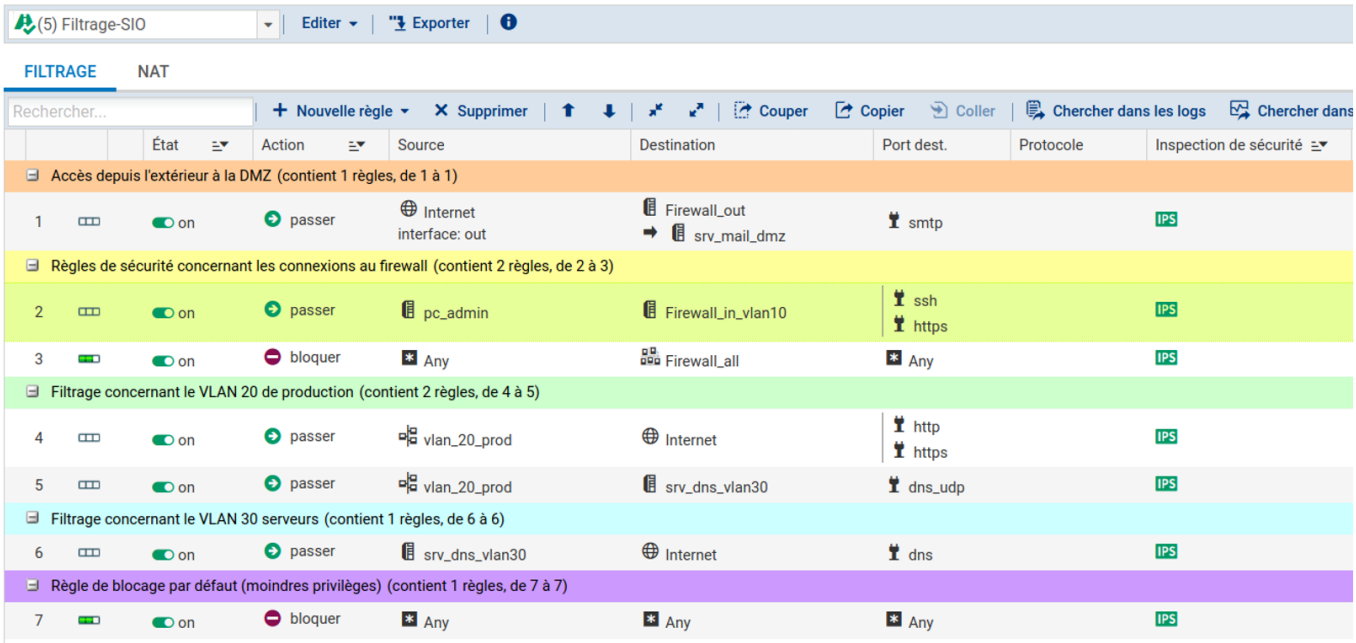
N°	Adresse IP Source	Port S	Adresse IP Destination	Port D	Proto	Action
1	*	>1023	192.168.0.1	25	TCP	Autoriser
2	192.168.192.16	>1023	192.168.192.254	22, 443	TCP	Autoriser
3	*	*	192.168.0.254 192.168.192.254 192.168.20.254 192.168.30.254 194.0.0.1	*	*	Bloquer
4	192.168.20.0/24	>1023	*	80, 443	TCP	Autoriser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

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.

1.3.2. Propositions de modification

Question 4 : Proposez des modifications et améliorations à apporter aux règles de filtrage en les classant dans les 5 sections préconisées.

Pour cela, aidez-vous du **document 3** qui explicite une liste de recommandations de l'ANSSI que vous allez mettre en œuvre dans votre pare-feu.

N°	Adresse IP Source	Port Source	Adresse IP Destination	Port Destination	Proto(cole)	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						

1.3.3. 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

1.3.3.1. 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).

1.3.3.2. 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).

1.3.3.3. 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.

1.3.3.4. 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.

1.3.3.5. 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.

1.3.3.6. 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.

1.3.3.7. 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.

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

1.3.4.1. 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).

1.3.4.2. 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.

1.3.4.3. 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

1.3.5. Retour

- Mise en oeuvre de l'UTM Stormshield

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/activite3filtrage?rev=1695913389

Last update: **2023/09/28 15:03**