

Fiche savoirs technologiques 5 : Filtrage protocolaire

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de filtrage afin de sécuriser l'accès à votre réseau et interdire certains flux.

La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers de l'UTM Stormshield Network.

Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, ...) peuvent être activées (Cela sera détaillé dans la partie **Filtrage applicatif**).

Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise.

Présentation des fonctionnalités

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 (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.

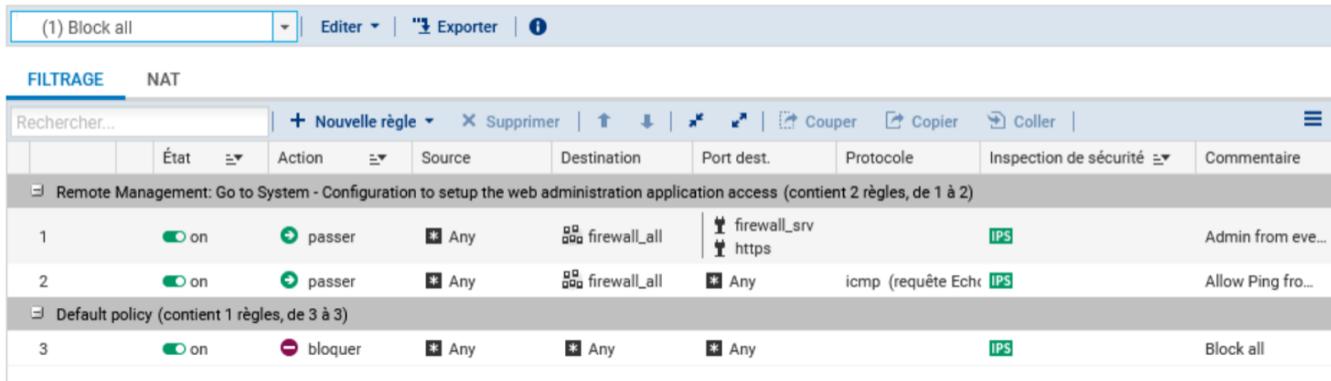
Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall SNS.

Le premier paquet appartenant à chaque nouveau flux reçu par le pare-feu 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** (règle n° 3 de la politique de sécurité « Block all »).

Dans les recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu publiées par l'ANSSI le 30 mars 2013, il est précisé que la règle finale qui consiste à bloquer et journaliser tout ce qui n'est pas autorisé par les règles précédentes doit apparaître explicitement à la fin de la politique de filtrage appliquée. L'ajout de cette règle explicite garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de s'assurer que la trace des flux non légitimes est conservée.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT



The screenshot shows the SNS Firewall configuration interface. At the top, there's a toolbar with buttons for 'Editer' (Edit) and 'Exporter' (Export). Below it, a search bar and a 'Nouvelle règle' (New Rule) button. The main area is titled 'FILTRAGE' and shows a table of rules:

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	on	passer	Any	firewall_all	firewall_srv https	IPS		Admin from eve...
2	on	passer	Any	firewall_all	Any	icmp (requête Echo)	IPS	Allow Ping fro...
3	on	bloquer	Any	Any		IPS		Block all

The rules are grouped under sections: 'Remote Management: Go to System - Configuration to setup the web administration application access' (containing rules 1 and 2), and 'Default policy' (containing rule 3). Rule 1 allows traffic from any source to any destination on any port using the 'firewall_all' protocol, inspection type 'IPS', and action 'passer'. Rule 2 allows ICMP echo requests from any source to any destination on any port using the 'firewall_all' protocol, inspection type 'IPS', and action 'passer'. Rule 3 blocks all traffic from any source to any destination on any port using the 'firewall_all' protocol, inspection type 'IPS', and action 'bloquer'.

Les firewalls SNS utilisent la technologie **SPI (Stateful Packet Inspection)** qui leur permet de garder en mémoire l'état des connexions TCP 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.

La figure suivante présente l'ordre d'application des règles de filtrage et de NAT, il est important de noter que les paquets sont filtrés **avant** la phase de traduction (NAPT).

Le premier paquet reçu est confronté aux règles de filtrage des différents niveaux suivant l'ordre présenté dans la figure ci-dessus.

Dès que les éléments du paquet correspondent à une règle dans un niveau, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes.

Si aucune règle de filtrage ne correspond, **le paquet est bloqué par défaut**.

Dans le cas où le paquet est autorisé, il est confronté aux règles de **NAT** des différents niveaux toujours suivant l'ordre présenté ci-dessus.

- **Le filtrage implicite** regroupe les règles de filtrage pré-configurées ou ajoutées dynamiquement par le pare-feu 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 du pare-feu SNS 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 pare-feu 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 du pare-feu SNS.

Les règles implicites sont accessibles depuis le menu **CONFIGURATION / POLITIQUE DE SÉCURITÉ / Règles implicites**.

Chaque règle peut être activée/désactivée.

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.

Les règles de filtrage font partie d'une politique présentée précédemment dans la partie **Traduction d'adresses**.

- Ouvrez le menu **Configuration / Politique de sécurité / Filtrage et NAT / Filtrage** ;

L'onglet **FILTRAGE** est composé d'un en-tête pour la gestion des règles de filtrage :

- Nouvelle règle :
 - **Règle simple** : Ajoute une règle de filtrage standard. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à **Any**.
 - **Séparateur - regroupement de règles** : Ajoute 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 qui facilite l'ajout d'une règle dont le rôle est de rediriger les connexions des utilisateurs non-authentifiés vers le portail captif.
 - **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.

Mise en place des règles de filtrage

Vous allez mettre en place une nouvelle politique de sécurité, il faudra commencer par désactiver la règle de filtrage **Pass all** et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.

Au besoin ajoutez les adresses IP privées de vos serveurs et les IP publiques des serveurs de vos voisins dans les **Objets Réseaux** (cf Partie 3 Objets réseau).

srvdnspriv : 172.16.x.0

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/reseau/stormshield/fiche5?rev=1665435223>

Last update: **2022/10/10 22:53**

