

Fiche savoirs technologiques : Filtrage protocolaire

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 antivirus, analyse antispam, filtrage URL, ...) peuvent être activées : il s'agit du **Filtrage applicatif**.

Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise et prendre en compte les **bonnes pratiques** telles que préconisées par l'**ANSSI**.

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 de la couche transport** 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

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT										
(1) Block all Editer Exporter ⓘ										
FILTRAGE NAT										
Rechercher...										
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire		
Remote Management: Go to System - Configuration to setup the web administration application access (contient 2 règles, de 1 à 2)										
1	on	passer	Any	firewall_all	firewall_srv https		IPS	Admin from eve...		
2	on	passer	Any	firewall_all	Any	icmp (requête Echr	IPS	Allow Ping fro...		
Default policy (contient 1 règles, de 3 à 3)										
3	on	bloquer	Any	Any	Any		IPS	Block all		

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.

Analyse des politiques prédéfinies de filtrage

La découverte des règles déjà définies dans les deux premières politiques prédéfinies de filtrage, permet de comprendre le fonctionnement des règles de filtrage sur un pare-feu Stormshield.

- Ouvrir le menu **Configuration / Politique de sécurité / Filtrage et NAT / Filtrage**
- Dans la liste déroulante des politiques de sécurité, choisir **(1) Block all**.

Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.

La règle numéro 1 autorise l'accès en **https (443)** et sur le port prédéfini **1300 pare-feu_srv** à toutes les interfaces du pare-feu, elle permet donc l'administration à distance depuis n'importe quel réseau.

La règle numéro 2 autorise les requêtes **ICMP Echo** vers toutes les interfaces du pare-feu, afin de pouvoir vérifier la présence du pare-feu à l'aide des commandes ICMP.

- Dans la liste déroulante des politiques de sécurité, choisir **(2) High**.

Cette politique est un peu moins restrictive que la précédente, elle autorise plus de chose à partir des réseaux internes.

La règle numéro 1 autorise l'accès à des services web en **http, https, dns** ⇒ elle permet l'accès à des sites web.

La règle numéro 2 autorise l'accès à des services **ftp**.

La règle numéro 3 autorise l'accès à des services de messagerie en **imap, smtp, pop3** elle permet l'envoi et la réception de messages.

La règle numéro 4 autorise les requêtes **ICMP Echo** vers n'importe quelle destination des réseaux internes, afin de pouvoir vérifier la présence du pare-feu et des services en DMZ à l'aide des commandes ICMP.

Vous remarquerez que pour toutes ces règles la colonne « Inspection de sécurité » stipule **IPS (Intrusion Prevention System)** qui est le niveau le plus élevé de filtrage avec inspection du contenu et le cas échéant blocage si l'on suspecte un comportement anormal ou une tentative d'intrusion.

Trafics sortants :

- Votre réseau interne (DMZ incluse) doit pouvoir joindre les serveurs FTP et Web de vos voisins.
- Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine est 192.168.x.200.
- Votre serveur de messagerie peut envoyer des mails vers les serveurs publiés par vos voisins.
- Votre réseau interne, à l'exception de vos serveurs en DMZ, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec www.visitkorea.or.kr).
- L'accès au site <https://www.cnn.com> doit être bloqué depuis le réseau interne, en utilisant un objet FQDN.

Trafics entrants :

- Les utilisateurs de l'autre agence peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
- Le serveur mails de l'autre agence est autorisés à transmettre des e-mails à votre serveur de messagerie
- Les utilisateurs de l'autre agence sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure.
- Le formateur est autorisé à pinger l'interface externe de votre SNS.
- Les utilisateurs de l'autre agence peuvent se connecter à votre SNS : via l'interface web et en SSH. Ces événements devront lever des alarmes majeures.

Retour

- [Mise en oeuvre de l'UTM Stormshield](#)

From:
/ - Les cours du BTS SIO

Permanent link:
[/doku.php/fiche7filtrageprotocolaire?rev=1665993947](http://doku.php/fiche7filtrageprotocolaire?rev=1665993947)

Last update: **2022/10/17 10:05**

