

# Premières règles de filtrage

## Ressources

Aidez-vous des fiches suivantes :

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

## 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.

**Étape 1 :** Copiez la politique de filtrage/NAT (1) **Block all** vers une autre politique vide où nous allons les copier les règles de NAT.

- Dans la liste déroulante des politiques de sécurité, choisissez (1) **Block all**.

FILTRAGE		NAT									
		Rechercher...	+ Nouvelle règle	Supprimer	↑	↓	Copier	Coller	Chercher dans les logs	Chercher dans la supervision	Commentaire
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité				
<b>Remote Management: Go to System - Configuration to setup the web administration application access (contient 2 règles, de 1 à 2)</b>											
1	on	passer	Any	firewall_all	firewall_srv https	IPS				Admin from everywhere	
2	on	passer	Any	firewall_all	Any	icmp (requête Echo (Ping))	IPS			Allow Ping from everywhere	
<b>Default policy (contient 1 règles, de 3 à 3)</b>											
3	on	bloquer	Any	Any	Any	IPS				Block all	

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

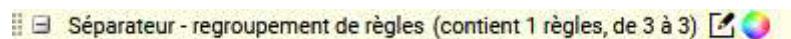
La règle numéro 1 autorise l'accès en **https** et sur le port prédéfini **1300 firewall\_srv** à toutes les interfaces du firewall, elle permet donc l'administration à distance.

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

- Cliquez **Éditer** puis **copier vers** et choisissez une politique vide (par exemple **Filter 06**).
- Cliquez **Sauvegarder les modifications...**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée (**06** **Block all**). Cliquez **Éditer** puis **Renommer** et renommez-là en **UtilisateursBlock all & NAT, puis Mettre à jour.** \* **Cliquez sur le bouton Appliquer puis Activer la politique "UtilisateursBlock all & NAT".** \* **Dans la liste des politiques de sécurité, choisissez la politique précédente (05) AgenceX / onglet NAT puis sélectionnez les 6 règles et cliquez sur Copier.** \* **Dans la liste des politiques de sécurité, choisissez la politique (06) AgenceX\_Block all & NAT / onglet NAT puis cliquez sur Coller.** **Les 6 règles de NAT/PAT sont copiées.**

**Étape 2 :** Nous allons mettre en place une première série de règles sur le Trafic sortant. Nous vous proposons d'utiliser les bandeaux séparateurs en indiquant le rôle de chaque règle pour plus de lisibilité.

a) **Votre réseau interne doit pouvoir émettre un ping vers n'importe quelle destination.** \* Cliquez la règle numéro 2 qui passe en surbrillance et choisissez **Nouvelle règle / séparateur - Regroupement de règle**.



\* **Cliquez le symbole du crayon et modifiez le nom du séparateur en ping vers n'importe quelle destination.** \* **Cliquez Nouvelle règle / règle simple** \* **Action : Passer** ; \* **Source** : L'adresse IP ou le réseau source, ici **Networkinternals** ; \* **Protocole dest : laisser Any**. \* **Double-cliquez sur Protocole et remplir les champs comme ci-dessous :** \* **Type de protocole : Protocole IP** ; \* **Protocole IP : icmp** ; \* **Message ICMP : choisir au milieu de la liste requête Echo (Ping, type 8, code 0)**

EDITION DE LA RÈGLE N° 3

- Général
- Action
- Source
- Destination
- Port / Protocole**
- Inspection

### PORT ET PROTOCOLE

**Port**

Port destination: **Any**

**Protocole**

Type de protocole: **Protocole IP**

Protocole applicatif: **Aucune analyse applicative**

Protocole IP: **icmp**

Message ICMP: **requête Echo (Ping)**

**Suivi des états (stateful)**

La nouvelle règle se présente ainsi :

3 Network\_Internal Any Any icmp (requête Echo (Ping)) IPS

\* Double-cliquez sur le bouton **off** pour passer la règle à l'état **on**, puis cliquez **Appliquer** puis **Oui, activer la politique**. b) Votre réseau interne doit pouvoir accéder aux serveurs privés de la DMZ (DNS, WEB (ports 80 et 808 pour le webmail), FTP et SMTP). \* Ajoutez un séparateur nommé **Accès aux serveurs DMZ**, choisissez **Nouvelle règle / séparateur - Regroupement de règle** puis éditez-le. \* Cliquez **Nouvelle règle /règle simple** \* **Action : Passer** ; \* **Source : Networkin** ; \* **Destination : srvftppriv** ; \* **Port dest : Port destination, ici ftp**.

4 Network\_in srv\_ftppriv ftp IPS

\* Cliquez sur **Copier** puis **Coller** pour créer la deuxième règle à partir de la précédente : \* **Action : Passer** ; \* **Source : Networkin** ; \* **Destination : srvhttppriv** \* **Port dest : Port destination, ici http**

5 Network\_in srv\_web\_priv http IPS

\* Cliquez sur **Copier** puis **Coller** pour créer la troisième règle pour le webmail à partir de la précédente : \* **Action : Passer** ; \* **Source : Networkin** ; \* **Destination : srvhttppriv** ; \* **Port dest : Port destination, ici webmail (port TCP 808)**.

6 Network\_in srv\_web\_priv webmail IPS

\* Cliquez sur **Copier** puis **Coller** pour créer la quatrième règle pour le serveur mail smtp à partir de la précédente : \* **Action : Passer** ; \* **Source : Networkin** ; \* **Destination : srvmailpriv** ; \* **Port dest : Port destination, ici smtp**.

7 Network\_in srv\_mail\_priv smtp IPS

c) Seul votre serveur DNS interne (172.16.x.10) sera autorisé à résoudre vers l'extérieur, et plus précisément vers l'IP publique du DNS de Google (8.8.8.8). \* Cliquez **Nouvelle règle /règle simple** \* **Action : Passer** ; \* **Source : srvdnspriv** ; \* **Destination : DNSGoogle** ; \* **Port dest : Port destination, ici dnsudp**.

8 srv\_dns\_priv FWOUT\_Siege dns\_udp IPS

Double cliquez sur le symbole **off** des règles pour les passer à l'état **on**, puis cliquez **Appliquer et Oui, activer la politique**. Les règles actuellement mises en place sont les suivantes :

## Politique de sécurité / Filtrage et NAT

Filtrage NAT						
	État	Action	Source	Destination	Port dest.	Protocole
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
2	on	passer	* Any	firewall_all	* Any	icmp (requête Echo (Ping)) IPS
ping vers n'importe quelle destination depuis réseau interne (contient 1 règles, de 3 à 3)						
3	on	passer	Network_internals	* Any	* Any	icmp (requête Echo (Ping)) IPS
Accès aux serveurs DMZ (contient 4 règles, de 4 à 7)						
4	on	passer	Network_in	srv_ftp_priv	ftp	IPS
5	on	passer	Network_in	srv_web_priv	http	IPS
6	on	passer	Network_in	srv_web_priv	webmail	IPS
7	on	passer	Network_in	srv_mail_priv	smtp	IPS
Résolution DNS (contient 1 règles, de 8 à 8)						
8	on	passer	srv_dns_priv	FWOUT_Siege	dns_udp	IPS
Default policy (contient 1 règles, de 9 à 9)						
9	on	bloquer	* Any	* Any	* Any	IPS

**Étape 3 :** Vous allez mettre en place une deuxième série de règles sur les trafics entrants et sortants qui respecteront le cahier des charges ci-dessous (utilisez les séparateurs en indiquant le rôle de chaque règle).

==== 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](http://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 autorisé 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/activite5filtrage?rev=1665948512](https://doku.php/activite5filtrage?rev=1665948512)

Last update: 2022/10/16 21:28

