1. Premières règles de filtrage

1.1. Ressources

Aidez-vous des fiches suivantes :

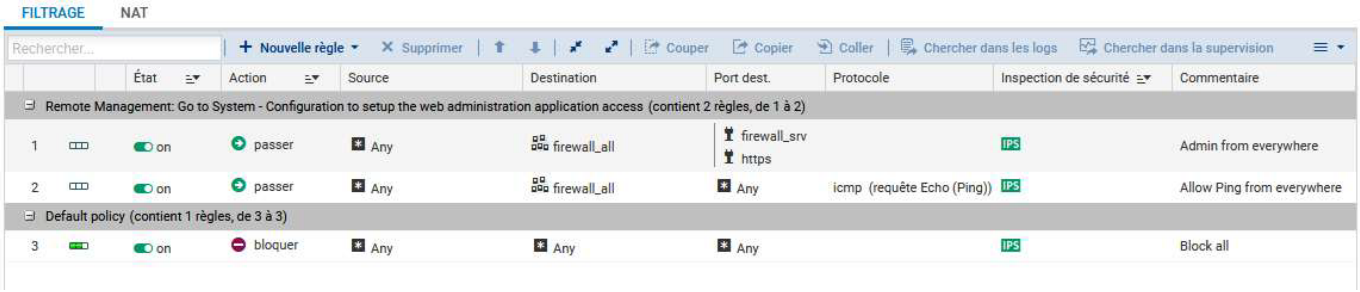
- Fiche 5 – Configuration des objets réseaux
- Fiche 7 – Filtrage protocolaire
- Fiche 6 – Configuration du NAT/PAT

1.2. 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**.



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 choisir 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 **Utilisateurs_Block all & NAT**, puis **Mettre à jour**.
- Cliquez sur le bouton **Appliquer** puis **Activer la politique** "Utilisateurs_Block all & NAT".
- Dans la liste des politiques de sécurité, choisissez la politique précédente, celle où vous avez défini du NAT puis sélectionnez la règle de NAT et cliquez sur **Copier**.
- Dans la liste des politiques de sécurité, choisissez la politique **(06) Utilisateurs_Block all & NAT** / onglet **NAT** puis cliquez sur **Coller**. La règle de NAT/PAT est copiée.

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

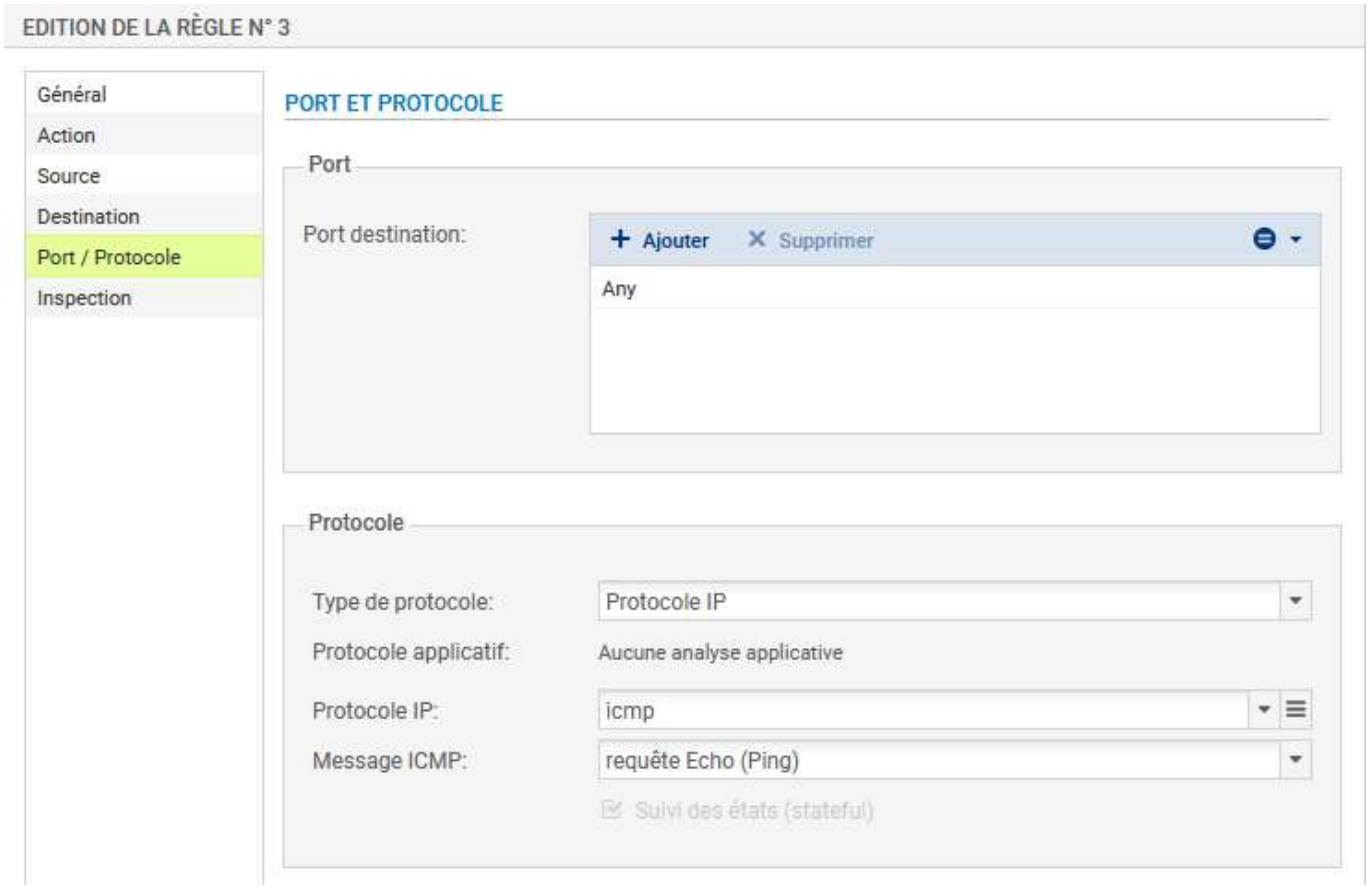
a) Votre réseau interne doit pouvoir émettre un **ping vers n'importe quelle destination**.

- 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 **Network_internals** ;
  - **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)**



La nouvelle règle se présente ainsi :



- 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 pour l'instant).

- Ajoutez un séparateur nommé **Accès aux serveurs DMZ**, choisissez **Nouvelle règle / séparateur – Regroupement de règle** puis éditez-le.
- Cliquez sur **Nouvelle règle /règle simple** :
  - **Action** : **Passer** ;
  - **Source** : **Network_in** ;
  - **Destination** : **srv_http_priv**
  - **Port dest** : Port destination, ici **http**



c) Seul votre serveur DNS interne 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** : **srv_dns_priv** ;
  - **Destination** : DNS_Google ;
  - **Port dest** : Port destination, ici **dns_udp**.



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

(6) AgenceA_ Block all & NAT | Editer | Exporter

FILTRAGE NAT

Rechercher... | + Nouvelle règle | ✕ Supprimer | Couper | Copier | Coller | Chercher dans les logs | Chercher

		État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
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).

1.2.1. Trafics sortants :

- Votre réseau interne (DMZ incluse / VLAN Serveurs) doit pouvoir joindre les serveurs Web de vos voisins. Pour cela, vous devez devez configurer une redirection de port vers votre serveur Web interne.
- 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.

1.2.2. Trafics entrants :

- Les utilisateurs de l'autre agence peuvent joindre votre serveur Web ; ces événements doivent être tracés.
- Les utilisateurs de l'autre agence sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure.
- 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.

1.2.3. 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/activite5filtrage?rev=1666033784

Last update: **2022/10/17 19:09**