1. 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.

1.1. 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.

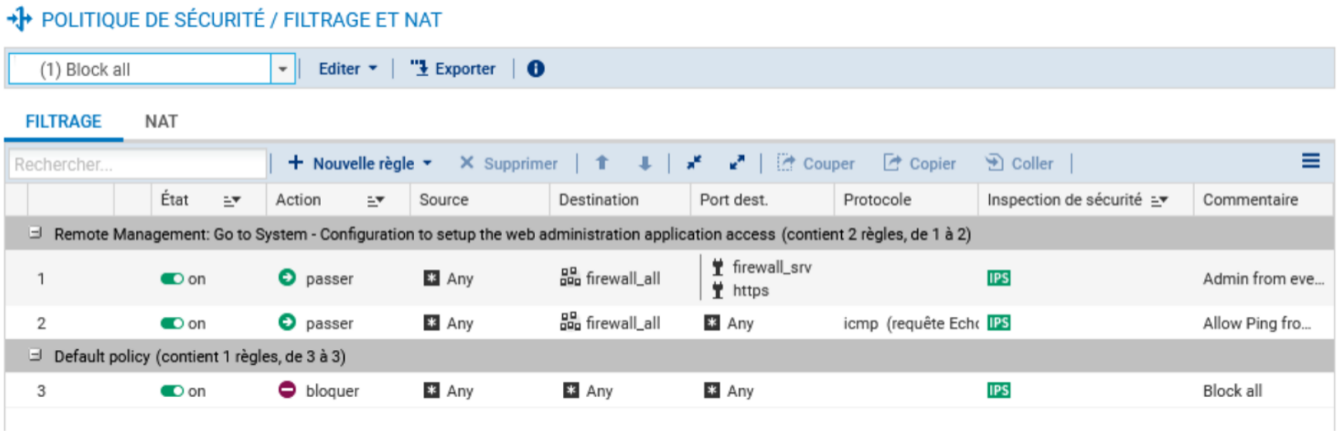
Parmi ces critères, il est notamment possible de préciser :

- 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.

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.

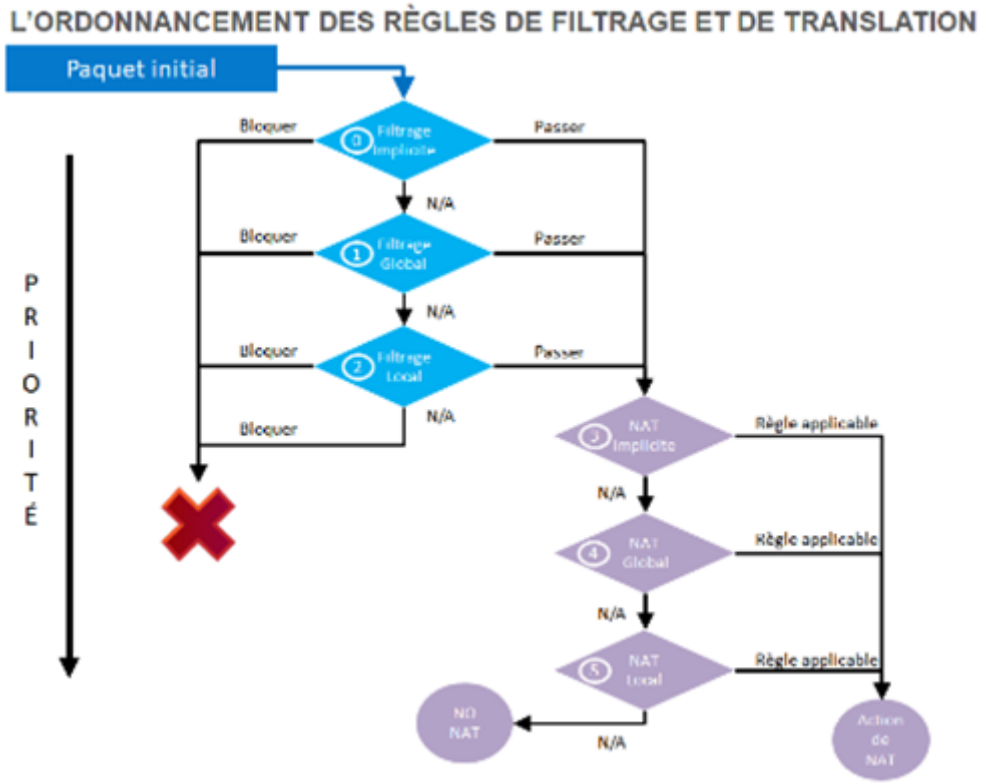


Les firewalls SNS utilisent la technologie **SPI (Stateful Packet Inspection)** qui leur permet de garder en mémoire l'état des connexions TCP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques.

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**.

POLITIQUE DE SÉCURITÉ / RÈGLES IMPLICITES

RÈGLES DE FILTRAGE IMPLICITES

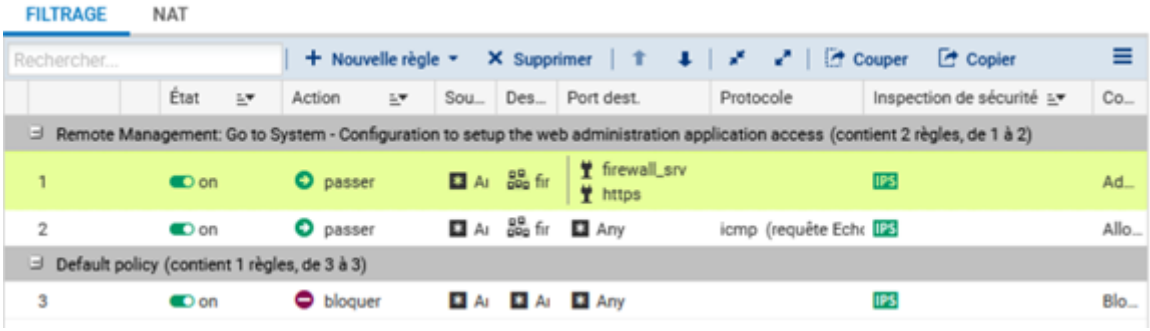
Activé	Nom
Activé	Autoriser l'accès au serveur PPTP
Activé	Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster HA)
Activé	Autoriser ISAKMP (port 500 UDP) et le protocole ESP pour les correspondants VPN IPsec
Activé	Autoriser l'accès au service DNS (port 53) du Firewall pour les interfaces protégées
Activé	Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces modems (dialup)
Activé	Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces ethernet
Désactivé	Autoriser l'accès au serveur d'administration (port 1300) du Firewall pour les interfaces protégées (Serverd)
Activé	Autoriser l'accès au port ssh du Firewall pour les interfaces protégées
Activé	Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces associées aux profils d'authentification (Authd)
Activé	Autoriser l'accès au serveur d'administration web du firewall (WebAdmin)
Activé	Autoriser les requêtes "Bootp" avec une adresse IP spécifiée pour relayer les requêtes DHCP
Activé	Autoriser les clients à joindre le service VPN SSL du firewall sur les ports TCP et UDP
Activé	Autoriser les sollicitations de routeur (RS) en multicast ou à destination du firewall
Activé	Autoriser les requêtes au serveur DHCPv6 et les sollicitations multicast DHCPv6
Activé	Ne pas tracer les paquets IPFIX dans le trafic IPFIX

Chaque règle peut être activée/désactivée.

2. 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**.

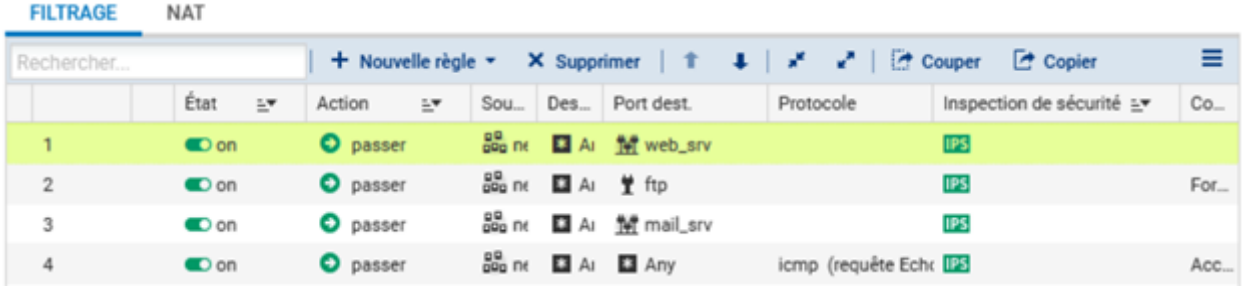


Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.

La règle numéro 1 autorise l'accès en https 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.

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 :

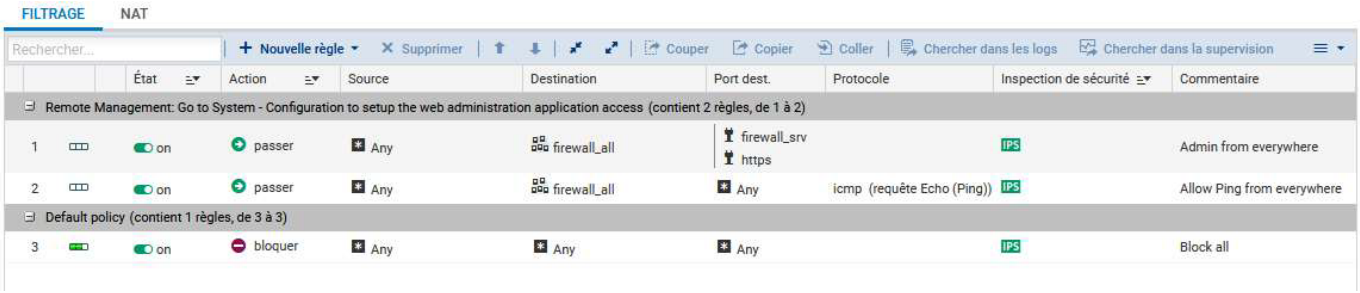
- Nouvelle règle :
  - **Règle simple** : Ajoute une règle de filtrage standard. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à **Any**.
  - **Séparateur – regroupement de règles** : Ajoute un séparateur qui regroupe toutes les règles se trouvant au-dessous (ou jusqu'au 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** : Démarre 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** : Démarre un assistant qui facilite l'ajout de règles pour l'activation du proxy SSL.
  - **Règle de proxy HTTP explicite** : Démarre 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.

2.1. 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 de la politique 5.

- 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 **AgenceX_Block all & NAT**, puis **Mettre à jour**.
- Cliquez sur le bouton **Appliquer** puis **Activer la politique** "AgenceX_Block 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.

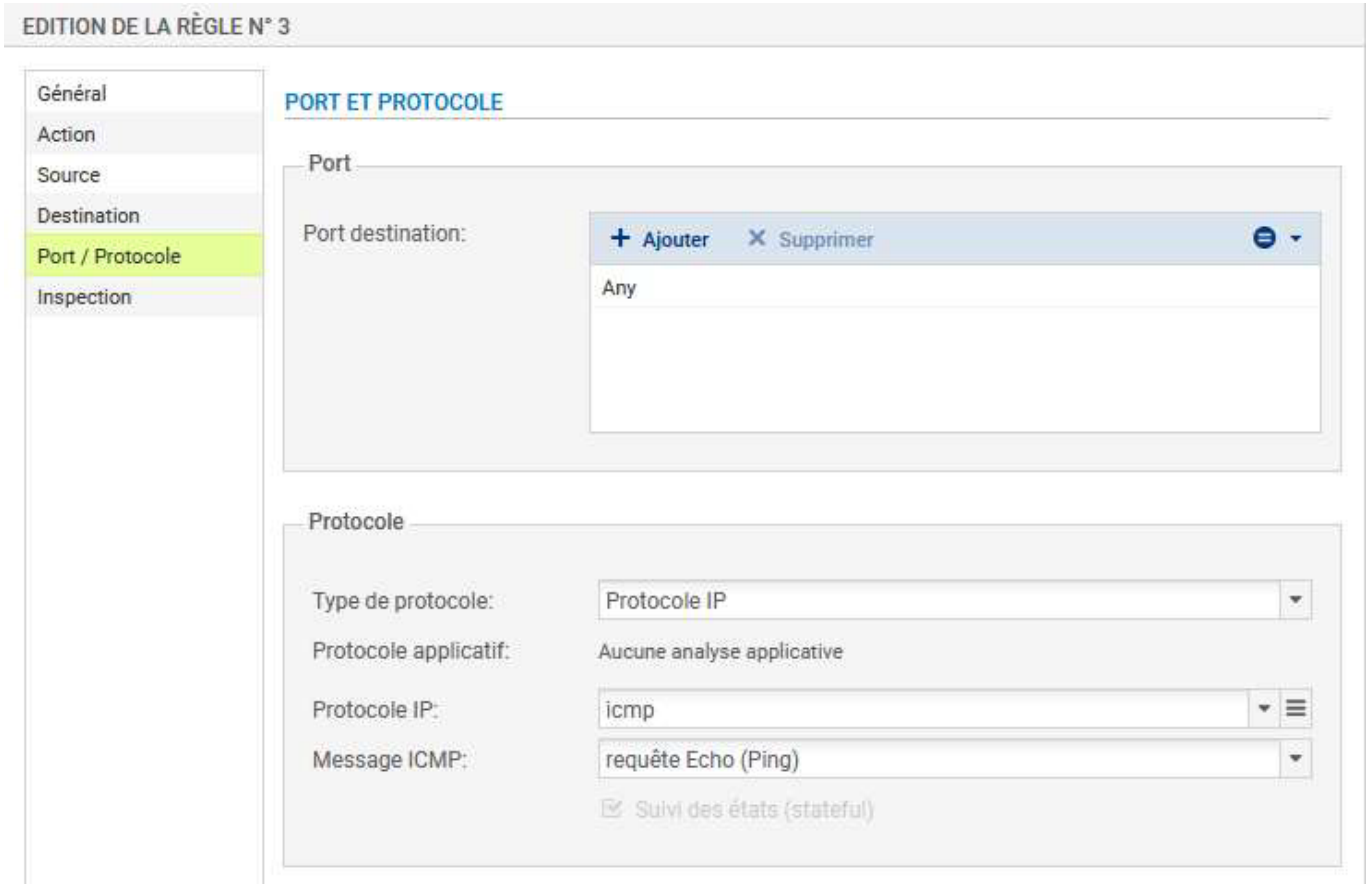
Étape 2 : Nous allons mettre en place une première série de règles sur le Trafic sortant. Nous vous proposons d'utiliser les bandeaux séparateurs en indiquant le rôle de chaque règle pour plus de lisibilité.

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 **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 (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** : **Network_in** ;
  - **Destination** : **srv_ftp_priv** ;
  - **Port dest** : Port destination, ici **ftp**.



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



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



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



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** : **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).

2.1.1. 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.

2.1.2. 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.

2.2. Retour Accueil Stormshield

- Stormshield

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

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/stormshield/fiche5?rev=1665435873

Last update: **2022/10/10 21:04**