## 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.



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

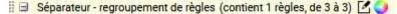
La règle numéro 1 autorise l'accès en **https** et sur le port prédéfini **1300 firewall\_srv** à toutes les interfaces du firewall, elle permet donc l'administration à distance.

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.

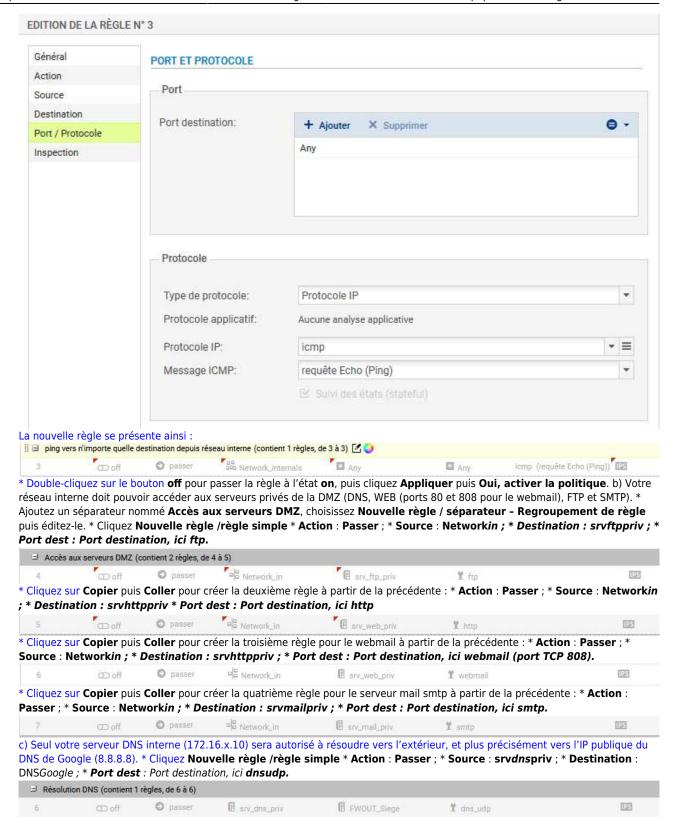
- Cliquez Éditer puis copier vers et choisir une politique vide (par exemple Filter 06).
- Cliquez Sauvegarder les modifications...
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée (06) Block all. Cliquez Éditer puis Renommer et renommez-là en UtilisateursBlock all & 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.

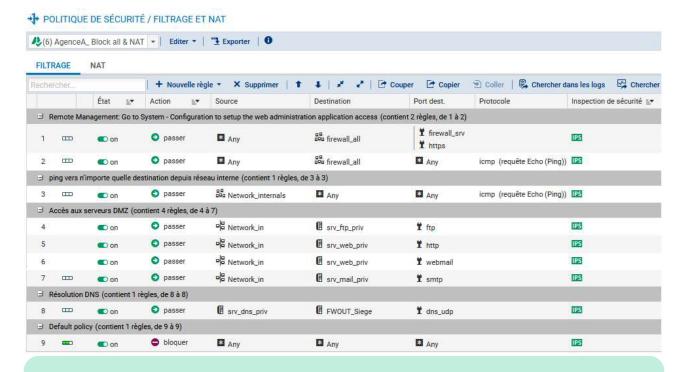


\* Cliquez le symbole du crayon et modifiez le nom du séparateur en ping vers n'importe quelle destination. \* Cliquez Nouvelle règle / règle simple \* Action : Passer ; \* Source : L'adresse IP ou le réseau source, ici Networkinternals ; \* Protocole dest : laisser Any. \* Double-cliquez sur Protocole 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)



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 :

Printed on 2025/11/09 14:47



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). \* 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 emails 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

Last update: 2022/10/16 21:28

