Activité : Premières règles de filtrage

Ressources

Aidez-vous des fiches suivantes :

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

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.

| FILTE | RAGE | NAT | | | | | | | | |
|--------|------------|--------------|----------|------------------|-------------------------------|------------------------------------|----------------------------|----------------------------|----------------------------|---|
| Rechei | cher | | | + Nouvelle | règle • X Supprimer | + + + 2 20 | Couper 🔄 Copier | 🐑 Coller 🖳 Chercher da | ns les logs 🛛 🛱 Chercher (| dans la supervision $\qquad \equiv ullet$ |
| | | État | ±* | Action = | Source | Destination | Port dest. | Protocole | Inspection de sécurité 🖃 | Commentaire |
| ⊐ R | emote Ma | anagement | : Go to | System - Configu | ration to setup the web admir | nistration application access (cor | ntient 2 règles, de 1 à 2) | | | |
| 1 | ⊞ | C on | | passer | Any | pe firewall_all | i firewall_srv | | IPS | Admin from everywhere |
| 2 | œ | 💿 on | | 🖸 passer | * Any | B firewall_all | Any | icmp (requête Echo (Ping)) | IPS | Allow Ping from everywhere |
| 🕀 D | efault pol | licy (contie | nt 1 règ | gles, de 3 à 3) | | | | | | |
| 3 | - | ඟ 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 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, 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.

🗄 🖃 Séparateur - regroupement de règles (contient 1 règles, de 3 à 3) 🗹 🥥

* 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)

| COLLON | DEALE | A10 01 | | |
|--------|------------------|--------|--|--|
| FULLON | REGIE | N | | |
| | 1 Star Collector | | | |

| Général | | PORT ET PR | OTOCOLE | | | | | | |
|--|---|--|--|---|---|---|--|--|--|
| Action | | | | | | | | | |
| Source | | Port | | | | | | | |
| Destination | | | | | | | | | |
| Port / Protoco | ole | Port destination: | | + Ajouter × Supprimer | | | | | |
| Inspection | | | | Any | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | Protocole | | | | | | | |
| | | Type de p | rotocole: | Protocole IP | | | | | |
| | | Protocole | applicatif: | Aucune analyse applicative | | | | | |
| | | Protocole | IP: | icmp | | | | | |
| | | Message ICMP: | | requête Echo (Ping) | | | | | |
| | | | | 🗵 Suivi des états (state | efiul) | | | | |
| nouvelle règ | Jle se préser | ite ainsi : | seau interne (contient 1 | rènles de 3 à 3) 🚺 🥎 | | | | | |
| a ping vers min | P on off | D passer | rag Natwork intern | ala 📕 🛄 Any | El Anu | icmn (requête Echo (Pinc | 1) 1 123 | | |
| ouble-clique | z sur le bou doit pouvoir rveurs DMZ e /règle sin | ton off pour accéder aux , choisissez nple : * Acti | passer la règle à x serveurs privés Nouvelle règle / ion : Passer ; * S | l'état on, puis cliquez Aj de la DMZ (DNS, WEB po / séparateur - Regroug ource : Network <i>in ; * L</i> | ppliquer puis Oui bour l'instant). * Ajo pement de règle Destination : srv | i, activer la politique utez un séparateur no puis éditez-le. * Cliqu httppriv * Port dest | e. b) Vo mmé ez sur <i>: Port</i> | | |
| ces aux ser ouvelle règle stination, i | ci http | | | 7 m | 44 | | | | |
| ces aux ser uvelle règle stination, ic 5 | ci http | O passer | Network_in | ll目_srv_web_priv | I http | | 123 | | |
| ces aux ser uvelle règle stination, i 5 Seul votre se | i ci http Coooff erveur DNS i | O passer nterne sera a | autorisé à résoud | ll srv_web_priv re vers l'extérieur, et plu | I http is précisément vei | rs l'IP publique du DNS | de Goo | | |
| ces aux ser uvelle règle stination, i 5 Seul votre se 8.8.8). * Cliq | ici http | O passer nterne sera a le règle /rè | autorisé à résoude gle simple * Act | re vers l'extérieur, et plu ion : Passer ; * Source | I http is précisément ver : srvdnspriv ; * l | rs l'IP publique du DNS Destination : DNSGoo | de Goo ogle ; * | | |
| ces aux ser puvelle règl stination, i 5 Seul votre se 8.8.8). * Cliq rt dest : Por | ici http off erveur DNS i juez Nouvel rt destination IS (contiant 1 cont | O passer nterne sera a le règle /rè n, ici dnsud | autorisé à résoud gle simple * Act p. | re vers l'extérieur, et plu ion : Passer ; * Source | I http is précisément ver : srvdnspriv ; * l | rs I'IP publique du DNS Destination : DNSGoc | de Goo ogle ; * | | |

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

3/3

| FILI | RAGE | NAI | | | | | | |
|-------|----------------------------|---------------------------------|-----------------------|-----------------------------------|----------------------------------|----------------------------|----------------------------|---------------------------|
| Reche | ercher | | + Nouvelle règ | le 🔹 🗙 Supprimer 🕇 | 🔹 🧩 💉 🖻 Coupe | er 🖸 Copier | 🐑 Coller 🛱 Chercher d | ans les logs 🛛 🛱 Chercher |
| | | État ≞▼ | Action ≞▼ | Source | Destination | Port dest. | Protocole | Inspection de sécurité = |
| ⊒ F | Remote Ma | nagement: Go to | System - Configurati | on to setup the web administrati | ion application access (contient | 2 règles, de 1 à 2) | | |
| 1 | ⊞ | 🜑 on | passer | * Any | newall_all | If firewall_srv If https | | IPS |
| 2 | E | 💽 on | passer | Any | Be firewall_all | * Any | icmp (requête Echo (Ping)) | IPS |
| Эr | oing vers n' | importe <mark>quelle d</mark> e | stination depuis rése | au interne (contient 1 règles, de | : 3 à 3) | | | |
| 3 | | 💿 on | passer | B Network_internals | Any | * Any | icmp (requête Echo (Ping)) | IPS |
| Ξ, | Accès aux s | serveurs DMZ (co | ntient 4 règles, de 4 | à 7) | | | | |
| 4 | | 💽 on | passer | 며 Network_in | srv_ftp_priv | ₿ ftp | | IPS |
| 5 | | 💽 on | passer | Pa Network_in | srv_web_priv | T http | | IPS |
| 6 | | 🔍 on | passer | P Network_in | srv_web_priv | T webmail | | IPS |
| 7 | | 💿 on | passer | Pa Network_in | srv_mail_priv | T smtp | | IPS |
| ∃F | Résolution I | DNS (contient 1 r | ègles, de 8 à 8) | | | | | |
| 8 | E | ඟ on | passer | srv_dns_priv | FWOUT_Siege | T dns_udp | | IPS |
| 30 | Defa <mark>ult</mark> poli | cy (contient 1 règ | les, 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 : ==== * Seul le PC d'administration doti pouvoir accéder à l'administration des serveurs et du SNS ==== Trafics entrants : ==== * 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. ==== Retour ==== * Mise en oeuvre de l'UTM Stormshield

From: / - Les cours du BTS SIO

Permanent link: /doku.php/activite5filtrage?rev=1667757498

Last update: 2022/11/06 18:58

