Exemple de configuration du shunning/blocage sur IPS pour routeur ASA/PIX/IOS

Contenu

Introduction

Ce document décrit comment configurer l'abandon sur un routeur PIX/ASA/Cisco IOS à l'aide de Cisco IPS. ARC, l'application de blocage sur le capteur, démarre et arrête les blocs sur les routeurs, les commutateurs Cisco 5000 RSM et Catalyst 6500, les pare-feu PIX, FWSM et ASA. ARC émet un bloc ou une coupure sur le périphérique géré pour l'adresse IP malveillante. ARC envoie le même bloc à tous les périphériques gérés par le capteur. Si un capteur de blocage principal est configuré, le bloc est transféré à et émis à partir de ce périphérique. L'ARC surveille la durée du bloc et retire le bloc une fois le temps écoulé.

Lorsque vous utilisez IPS 5.1, une attention particulière doit être accordée lors du passage aux pare-feu en mode de contexte multiple, car aucune information VLAN n'est envoyée avec la demande de désactivation.

> **Note**: Le blocage n'est pas pris en charge dans le contexte d'administration d'un FWSM de contexte multiple.

Il existe trois types de blocs :

- Host block : bloque tout le trafic provenant d’une adresse IP donnée.
- Bloc de connexion : bloque le trafic d'une adresse IP source donnée vers une adresse IP de destination et un port de destination donnés. Plusieurs blocs de connexion de la même adresse IP source à une autre adresse IP de destination ou à un autre port de destination basculent automatiquement le bloc d'un bloc de connexion à un bloc d'hôte.**Note**: Les blocs de connexion ne sont pas pris en charge par les appliances de sécurité. Les appliances de sécurité prennent uniquement en charge les blocs d'hôtes avec des informations de port et de

protocole facultatives.
- Bloc réseau : bloque tout le trafic provenant d'un réseau donné. Vous pouvez lancer des blocs d'hôte et de connexion manuellement ou automatiquement lorsqu'une signature est déclenchée. Vous ne pouvez lancer des blocs de réseau que manuellement.

Pour les blocs automatiques, vous devez choisir Demander un bloc d'hôte ou Demander une connexion de bloc comme action d'événement pour des signatures particulières, de sorte que SensorApp envoie une requête de bloc à ARC lorsque la signature est déclenchée. Une fois qu'ARC reçoit la demande de bloc de SensorApp, il met à jour les configurations des périphériques pour bloquer l'hôte ou la connexion. Référez-vous à Affecter des actions à des signatures, page 5-22 pour plus d'informations sur la procédure d'ajout des actions d'événement Hôte de bloc de demande ou Connexion de bloc de demande à la signature. Référez-vous à Configuration des remplacements d'action d'événement, page 7-15 pour plus d'informations sur la procédure de configuration des remplacements qui ajoutent les actions d'événement Hôte de bloc de demande ou Connexion de bloc de demande aux alarmes de cotes de risque spécifiques.

Sur les routeurs Cisco et les commutateurs de la gamme Catalyst 6500, ARC crée des blocs en appliquant des listes de contrôle d'accès ou des VACL. Les listes de contrôle d’accès et les listes de contrôle d’accès (VACL) appliquent des filtres aux interfaces, qui incluent respectivement la direction et les VLAN, afin d’autoriser ou de refuser le trafic. . Le pare-feu PIX, FWSM et ASA n'utilisent pas de listes de contrôle d'accès ou de listes de contrôle d'accès. Les commandes **shun** et **no shun** intégrées sont utilisées.

Ces informations sont requises pour la configuration de ARC :

- ID utilisateur de connexion, si le périphérique est configuré avec AAA
- Mot de passe de connexion
- Activer le mot de passe, qui n'est pas nécessaire si l'utilisateur dispose des privilèges d'activation
- Interfaces à gérer, par exemple ethernet0, vlan100
- Toutes les informations ACL ou VACL existantes que vous souhaitez appliquer au début (ACL ou VACL de préblocage) ou à la fin (ACL ou VACL de post-blocage) de la liste ACL ou VACL créée. Cela ne s'applique pas à un pare-feu PIX, un FWSM ou un ASA, car ils n'utilisent pas de listes de contrôle d'accès ou de VACL pour bloquer.
- Si vous utilisez Telnet ou SSH pour communiquer avec le périphérique
- Adresses IP (hôte ou plage d’hôtes) à ne jamais bloquer
- Combien de temps voulez-vous que les blocs durent ?

Conditions préalables

Conditions requises

Avant de configurer ARC pour le blocage ou la limitation de débit, vous devez effectuer les tâches suivantes :

- Analysez la topologie de votre réseau pour savoir quels périphériques doivent être bloqués par quel capteur et quelles adresses ne doivent jamais être bloquées.
- Recueillez les noms d’utilisateur, les mots de passe des périphériques, les mots de passe d’activation et les types de connexion (Telnet ou SSH) nécessaires pour vous connecter à

chaque périphérique.
- Connaître les noms des interfaces sur les périphériques.
- Connaître les noms de la liste de contrôle d'accès ou de la liste de contrôle d'accès préblocage et de la liste de contrôle d'accès ou de contrôle d'accès post-blocage si nécessaire.
- Comprendre quelles interfaces doivent être bloquées et dans quelle direction (entrée ou sortie).

Components Used

Les informations de ce document sont basées sur Cisco Intrusion Prevention System 5.1 et versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Note**: Par défaut, ARC est configuré pour une limite de 250 entrées de bloc. Référez-vous à Périphériques pris en charge pour plus d'informations sur la liste des périphériques bloquants pris en charge par ARC.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Utilisez la page Blocage afin de configurer les paramètres de base requis pour activer le blocage et la limitation de débit.

ARC contrôle les actions de blocage et de limitation de débit sur les périphériques gérés.

Vous devez régler votre capteur afin d'identifier les hôtes et les réseaux qui ne doivent jamais être bloqués. Il est possible pour le trafic d'un périphérique de confiance de déclencher une signature. Si cette signature est configurée pour bloquer le pirate, le trafic réseau légitime peut être affecté. L'adresse IP du périphérique peut être répertoriée dans la liste Jamais bloquer afin d'éviter ce scénario.

Un masque de réseau spécifié dans une entrée Jamais bloquée est appliqué à l'adresse Jamais bloquée. Si aucun masque de réseau n'est spécifié, un masque /32 par défaut est appliqué.

> **Note**: Par défaut, le capteur n'est pas autorisé à émettre un bloc pour sa propre adresse IP car cela interfère avec la communication entre le capteur et le périphérique de blocage. Mais cette option est configurable par l'utilisateur.

Une fois que l'ARC est configuré pour gérer un périphérique de blocage, les mises hors tension du périphérique de blocage et les ACL/VACL utilisées pour le blocage ne doivent pas être modifiées manuellement. Cela peut entraîner une interruption du service ARC et entraîner l'absence de blocs futurs.

> **Note**: Par défaut, seul le blocage est pris en charge sur les périphériques Cisco IOS. Vous pouvez remplacer la valeur par défaut de blocage si vous choisissez Limitation de débit ou Blocage plus Limitation de débit.

Pour émettre ou modifier des blocs, l'utilisateur IPS doit avoir le rôle Administrateur ou Opérateur.

Configurer le capteur pour gérer les routeurs Cisco

Cette section décrit comment configurer le capteur pour gérer les routeurs Cisco. Il contient les rubriques suivantes :

- Configurer les profils utilisateur
- Routeurs et listes de contrôle d’accès
- Configuration des routeurs Cisco à l’aide de l’interface de ligne de commande

Configurer les profils utilisateur

Le capteur gère les autres périphériques à l'aide de la commande **user-profile** *name* afin de configurer les profils utilisateur. Les profils utilisateur contiennent les informations d'ID utilisateur, de mot de passe et de mot de passe actif. Par exemple, les routeurs qui partagent tous les mêmes mots de passe et noms d’utilisateur peuvent se trouver sous un profil utilisateur.

> **Note**: Vous **devez** créer un profil utilisateur avant de configurer le périphérique de blocage.

Complétez ces étapes afin de configurer les profils utilisateur :

1. Connectez-vous à l'interface de ligne de commande avec un compte disposant de privilèges d'administrateur.
2. Passez en mode d'accès au réseau.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Créez le nom du profil utilisateur.
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```
4. Tapez le nom d'utilisateur de ce profil d'utilisateur.
   ```
   sensor(config-net-use)#username username
   ```
5. Spécifiez le mot de passe de l'utilisateur.
   ```
   sensor(config-net-use)# password
   Enter password[]: ********
   Re-enter password ********
   ```
6. Spécifiez le mot de passe enable pour l'utilisateur.
   ```
   sensor(config-net-use)# enable-password
   Enter enable-password[]: ********
   ```

```
Re-enter enable-password ********
```

7. Vérifiez les paramètres.
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. Quittez le sous-mode d'accès au réseau.
```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```
9. Appuyez sur **Entrée** afin d'appliquer les modifications ou saisissez no pour les ignorer.

Routeurs et listes de contrôle d’accès

Lorsque l'ARC est configuré avec un périphérique de blocage qui utilise des listes de contrôle d'accès, les listes de contrôle d'accès sont composées de cette manière :

1. Une ligne d'autorisation avec l'adresse IP du capteur ou, le cas échéant, l'adresse NAT du capteur**Note**: Si vous autorisez le blocage du capteur, cette ligne n'apparaît pas dans la liste de contrôle d'accès.
2. Liste de contrôle d'accès pré-bloc (si spécifiée) : Cette liste de contrôle d’accès doit déjà exister sur le périphérique.**Note**: ARC lit les lignes de la liste de contrôle d'accès préconfigurée et copie ces lignes au début de la liste de contrôle d'accès de bloc.
3. Tout bloc actif
4. **Liste de contrôle d'accès post-blocage** ou **permit ip any any any** :**Liste de contrôle d'accès post-blocage** (si spécifiée) :Cette liste de contrôle d’accès doit déjà exister sur le périphérique.**Note**: ARC lit les lignes de la liste de contrôle d’accès et copie ces lignes à la fin de la liste de contrôle d’accès.**Note**: Assurez-vous que la dernière ligne de la liste de contrôle d’accès est permit ip any any si vous voulez que tous les paquets sans correspondance soient autorisés.**permit ip any any any** (non utilisé si une liste de contrôle d'accès Post-Block est spécifiée)

   Note: Les listes de contrôle d'accès que fait ARC ne doivent jamais être modifiées par vous ou par tout autre système. Ces listes de contrôle d’accès sont temporaires et de nouvelles listes de contrôle d’accès sont constamment créées par le capteur. Les seules modifications que vous pouvez apporter concernent les listes de contrôle d’accès pré et post-blocage.

Si vous devez modifier la liste de contrôle d'accès pré-blocage ou post-blocage, procédez comme suit :

1. Désactivez le blocage sur le capteur.
2. Modifiez la configuration du périphérique.
3. Réactivez le blocage sur le capteur.

Lorsque le blocage est réactivé, le capteur lit la nouvelle configuration de périphérique.

Note: Un seul capteur peut gérer plusieurs périphériques, mais plusieurs capteurs ne

peuvent pas gérer un seul périphérique. Dans le cas où les blocs émis à partir de plusieurs capteurs sont destinés à un seul dispositif de blocage, un capteur de blocage principal doit être incorporé dans la conception. Un capteur de blocage principal reçoit les demandes de blocage de plusieurs capteurs et émet toutes les demandes de blocage au périphérique de blocage.

Vous créez et enregistrez des listes de contrôle d'accès pré-bloc et post-bloc dans la configuration de votre routeur. Ces listes de contrôle d'accès doivent être des listes de contrôle d'accès IP étendues, nommées ou numérotées. Pour plus d'informations sur la création de listes de contrôle d'accès, reportez-vous à la documentation de votre routeur.

Note: Les listes de contrôle d'accès pré-bloc et post-bloc ne s'appliquent pas à la limitation de débit.

Les listes de contrôle d'accès sont évaluées de haut en bas et l'action de première correspondance est effectuée. La liste de contrôle d'accès de préblocage peut contenir une autorisation qui prévaudrait sur un refus résultant d'un blocage.

La liste de contrôle d'accès Post-Block est utilisée pour tenir compte de toutes les conditions qui ne sont pas traitées par la ou les listes de contrôle d'accès Pre-Block. Si vous avez une liste de contrôle d'accès existante sur l'interface et dans la direction où les blocs sont émis, cette liste peut être utilisée comme liste de contrôle d'accès Post-bloc. Si vous n'avez pas de liste de contrôle d'accès Post-Block, le capteur insère permit ip any any à la fin de la nouvelle liste de contrôle d'accès.

Lorsque le capteur démarre, il lit le contenu des deux listes de contrôle d'accès. Il crée une troisième liste de contrôle d'accès avec les entrées suivantes :

- Une ligne d'autorisation pour l'adresse IP du capteur
- Copies de toutes les lignes de configuration de la liste de contrôle d'accès de préblocage
- Une ligne de refus pour chaque adresse bloquée par le capteur
- Copies de toutes les lignes de configuration de la liste de contrôle d'accès Post-Block

Le capteur applique la nouvelle liste de contrôle d'accès à l'interface et à la direction que vous avez désignées.

Note: Lorsque la nouvelle liste de contrôle d'accès de bloc est appliquée à une interface du routeur, dans une direction particulière, elle remplace toute liste de contrôle d'accès préexistante sur cette interface dans cette direction.

Configuration des routeurs Cisco à l'aide de l'interface de ligne de commande

Complétez ces étapes afin de configurer un capteur pour gérer un routeur Cisco afin d'effectuer le blocage et la limitation de débit :

1. Connectez-vous à l'interface de ligne de commande avec un compte disposant de privilèges d'administrateur.
2. Passez en sous-mode d'accès au réseau.
   ```
   sensor#configure terminal
   ```

```
sensor(config)#service network-access
sensor(config-net)#
```

3. Spécifiez l'adresse IP du routeur contrôlé par ARC.
```
sensor(config-net)#router-devices ip_address
```
4. Saisissez le nom de périphérique logique que vous avez créé lors de la configuration du profil utilisateur.
```
sensor(config-net-rou)#profile-name user_profile_name
```
Note: ARC accepte tout ce que vous entrez. Il ne vérifie pas si le profil utilisateur existe.
5. Spécifiez la méthode utilisée pour accéder au capteur.
```
sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
```

Si non spécifié, SSH 3DES est utilisé.**Note**: Si vous utilisez DES ou 3DES, vous devez utiliser la commande **ssh host-key ip_address** afin d'accepter la clé SSH du périphérique.
6. Spécifiez l'adresse NAT du capteur.
```
sensor(config-net-rou)#nat-address nat_address
```
Note: Cette opération modifie l'adresse IP de la première ligne de la liste de contrôle d'accès de l'adresse du capteur à l'adresse NAT. L'adresse NAT est l'adresse du capteur, post-NAT, traduite par un périphérique intermédiaire, située entre le capteur et le périphérique de blocage.
7. Indiquez si le routeur effectue le blocage, la limitation de débit ou les deux.**Note**: La valeur par défaut est le blocage. Vous n'avez pas besoin de configurer les capacités de réponse si vous voulez que le routeur effectue uniquement le blocage.Limitation de débit uniquement
```
sensor(config-net-rou)#response-capabilities rate-limit
```

Blocage et limitation de débit
```
sensor(config-net-rou)#response-capabilities block|rate-limit
```

8. Spécifiez le nom et la direction de l'interface.
```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

Note: Le nom de l'interface doit être une abréviation que le routeur reconnaît lorsqu'il est utilisé après la commande **interface**.
9. (Facultatif) Ajoutez le nom de la liste de contrôle d'accès (blocage uniquement).
```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```
10. (Facultatif) Ajoutez le nom post-ACL (blocage uniquement).
```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```
11. Vérifiez les paramètres.
```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings

   ip-address: 10.89.127.97
   ----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      ----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         ----------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         ----------------------------------------------
      ----------------------------------------------
```

```
        response-capabilities: block|rate-limit default: block
      -----------------------------------------------
    sensor(config-net-rou)#
```

12. Quittez le sous-mode d'accès au réseau.
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. Appuyez sur **Entrée** pour appliquer les modifications ou saisissez **no** pour les ignorer.

Configurer le capteur pour gérer les pare-feu Cisco

Complétez ces étapes afin de configurer le capteur pour gérer les pare-feu Cisco :

1. Connectez-vous à l'interface de ligne de commande avec un compte disposant de privilèges d'administrateur.
2. Passez en sous-mode d'accès au réseau.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Spécifiez l'adresse IP du pare-feu contrôlé par ARC.
```
sensor(config-net)#firewall-devices ip_address
```
4. Saisissez le nom du profil utilisateur que vous avez créé lors de la configuration du profil utilisateur.
```
sensor(config-net-fir)#profile-name user_profile_name
```
Note: ARC accepte tout ce que vous tapez. Il ne vérifie pas si le périphérique logique existe.
5. Spécifiez la méthode utilisée pour accéder au capteur.
```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

Si non spécifié, SSH 3DES est utilisé.**Note**: Si vous utilisez DES ou 3DES, vous devez utiliser la commande **ssh host-key ip_address** afin d'accepter la clé ou ARC ne peut pas se connecter au périphérique.
6. Spécifiez l'adresse NAT du capteur.
```
sensor(config-net-fir)#nat-address nat_address
```
Note: Cette opération modifie l'adresse IP de la première ligne de la liste de contrôle d'accès de l'adresse IP du capteur à l'adresse NAT. L'adresse NAT est l'adresse du capteur, post-NAT, traduite par un périphérique intermédiaire, située entre le capteur et le périphérique de blocage.
7. Quittez le sous-mode d'accès au réseau.
```
sensor(config-net-fir)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
8. Appuyez sur **Entrée** pour appliquer les modifications ou saisissez **no** afin de les ignorer.

Bloquer avec SHUN dans PIX/ASA

L'émission de la commande **shun** bloque les connexions d'un hôte attaquant. Les paquets qui correspondent aux valeurs de la commande sont supprimés et consignés jusqu'à ce que la fonction de blocage soit supprimée. Le **shun** est appliqué indépendamment du fait qu'une connexion avec l'adresse hôte spécifiée soit active ou non.

Si vous spécifiez l'adresse de destination, les ports source et de destination, ainsi que le protocole, vous limitez le shun aux connexions qui correspondent à ces paramètres. Vous ne pouvez avoir qu'une seule commande **shun** pour chaque adresse IP source.

Comme la commande **shun** est utilisée pour bloquer les attaques de manière dynamique, elle n'est pas affichée dans la configuration de l'appliance de sécurité.

Chaque fois qu'une interface est supprimée, tous les shuns qui sont reliés à cette interface sont également supprimés.

Cet exemple montre que l'hôte incriminé (10.1.1.27) établit une connexion avec la victime (10.2.2.89) au protocole TCP. La connexion dans la table de connexion de l'appliance de sécurité se lit comme suit :

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

Afin de bloquer les connexions d'un hôte attaquant, utilisez la commande **shun** en mode d'exécution privilégié. Appliquez la commande **shun** avec les options suivantes :

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

La commande supprime la connexion de la table de connexion de l'appliance de sécurité et empêche également les paquets de 10.1.1.27:555 à 10.2.2.89:666 (TCP) de passer par l'appliance de sécurité.

Informations connexes

- Configuration du capteur pour la gestion des commutateurs de la gamme Catalyst 6500 et des routeurs de la gamme Cisco 7600
- Support et documentation techniques - Cisco Systems