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

Contenu

Introduction

Ce document décrit comment configurer l'évitement sur un routeur IOS PIX/ASA/Cisco avec l'aide du Cisco IPS. L'ARC, l'application de blocage sur le capteur, commence et des blocs d'arrêts sur des Routeurs, Cisco 5000 Commutateurs RSM et de gamme Catalyst 6500, Pare-feu PIX, FWSM, et ASA. L'ARC émet un bloc ou l'évite au périphérique géré pour l'adresse IP malveillante. L'ARC envoie le même bloc à tous les périphériques que le capteur gère. Si un capteur de blocage principal est configuré, le bloc est expédié à et émis de ce périphérique. L'ARC surveille la durée du bloc et retire le bloc une fois le temps écoulé.

Quand vous utilisez IPS 5.1, le soin particulier doit être pris quand l'évitement aux Pare-feu dans le mode de contexte multiple en tant qu'aucune informations VLAN est envoyé avec la demande d'évitement.

Remarque: Le blocage n'est pas pris en charge dans le contexte d'admin d'un plusieurs contexte FWSM.

Il y a trois types de blocs :

- Bloc d'hôte — Bloque tout le trafic d'une adresse IP donnée.
- Bloc de connexion — Les blocs trafiquent d'une adresse IP de source donnée à une adresse IP et à une destination port de destination donnée.Les plusieurs blocs de connexion de la même adresse IP source à une adresse IP différente ou à la destination port de destination commutent automatiquement le bloc d'un bloc de connexion à un bloc d'hôte.**Remarque:** Des

blocs de connexion ne sont pas pris en charge par des dispositifs de sécurité. Blocs d'hôte de support de dispositifs de sécurité seulement avec les informations facultatives de port et de protocole.
- Bloc de réseau — Bloque tout le trafic d'un réseau donné.Vous pouvez initier des blocs d'hôte et de connexion manuellement ou automatiquement quand une signature est déclenchée. Vous pouvez seulement initier des blocs de réseau manuellement.

Pour les blocs automatiques, vous devez choisir l'hôte de bloc de demande ou la connexion de bloc de demande comme action d'événement pour les signatures particulières, de sorte que SensorApp envoie une demande de bloc DE COURBER quand la signature est déclenchée. Une fois que l'ARC reçoit la demande de bloc de SensorApp, il met à jour les configurations de périphérique pour bloquer l'hôte ou la connexion. Référez-vous à assigner des actions aux signatures, paginez 5-22 pour plus d'informations sur la procédure pour ajouter les actions d'événement d'hôte de bloc de demande ou de connexion de bloc de demande à la signature. Référez-vous à configurer l'action d'événement ignore, pagine 7-15 pour plus d'informations sur la procédure pour la configuration de ignore qui ajoutent les actions d'événement d'hôte de bloc de demande ou de connexion de bloc de demande aux alarmes des évaluations du risque spécifiques.

Sur des Routeurs de Cisco et des Commutateurs de gamme Catalyst 6500, l'ARC crée des blocs en appliquant ACLs ou VACLs. ACLs et VACLs appliquent des filtres aux interfaces, qui inclut la direction, et aux VLAN, respectivement afin de permettre ou refuser le trafic. Le Pare-feu PIX, les FWSM, et l'ASA n'utilisent pas ACLs ou VACLs. La fonction intégrée **évitent** et **aucun évitez la** commande sont utilisés.

Ces informations sont exigées pour la configuration de l'ARC :

- Ouvrez une session l'user-id, si le périphérique est configuré avec l'AAA
- Mot de passe de connexion
- Activez le mot de passe, qui n'est pas nécessaire si l'utilisateur a des privilèges d'enable
- Interfaces à gérer, par exemple, ethernet0, vlan100
- N'importe quelles informations existantes d'ACL ou VACL vous voulez appliqué au début (ACL de Pré-bloc ou VACL) ou à la fin (ACL de POST-bloc ou VACL) de l'ACL ou du VACL qui est créé. Ceci ne s'applique pas à un Pare-feu PIX, à un FWSM, ou à une ASA parce qu'ils n'emploient pas ACLs ou VACLs pour bloquer.
- Si vous employez le telnet ou le SSH pour communiquer avec le périphérique
- Adresses IP (hôte ou plage des hôtes) que vous ne voulez jamais bloqué
- Combien de temps vous voulez que les blocs durent

Conditions préalables

Conditions requises

Avant que vous configuriez l'ARC pour le blocage ou la limitation de débit, vous devez se terminer ces tâches :

- Analysez votre topologie du réseau pour comprendre quels périphériques devraient être bloqués par lesquels le capteur, et qui adresse devrait ne jamais être bloqué.
- Recueillez les noms d'utilisateur, des mots de passe de périphérique, des mots de passe d'enable, et les types de connexions (telnet ou SSH) ont dû ouvrir une session à chaque

périphérique.
- Connaissez les noms d'interface sur les périphériques.
- Connaissez les noms de l'ACL de Pré-bloc ou le VACL et l'ACL de POST-bloc ou le VACL si nécessaire.
- Comprenez quelles interfaces devraient et ne devraient pas être bloquées et dans quelles direction (dans ou).

Composants utilisés

Les informations dans ce document sont basées sur le Système de protection contre les intrusions Cisco 5.1 et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Remarque: Par défaut, l'ARC est configuré pour une limite de 250 blocs entrée. Référez-vous aux périphériques de support pour plus d'informations sur la liste de périphériques en mode bloc pris en charge par l'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 le volet de blocage de Properties afin de configurer les paramètres de base requis pour activer le blocage et la limitation de débit.

L'ARC contrôle des actions de blocage et de limitation de débit sur des périphériques gérés.

Vous devez accorder votre capteur afin d'identifier les hôtes et les réseaux qui devraient ne jamais être bloqués. Il est possible que le trafic d'un périphérique de confiance se déclenche une signature. Si cette signature est configurée pour bloquer l'attaquant, le trafic réseau légitime peut être affecté. L'adresse IP du périphérique peut ne jamais être répertoriée dans la liste de blocage afin d'empêcher ce scénario.

Un netmask spécifié dans jamais un bloc entrée n'est jamais appliqué à l'adresse de bloc. Si aucun netmask n'est spécifié, un masque de /32 de par défaut est appliqué.

Remarque: Par défaut, on ne permet pas au le capteur pour émettre un bloc pour sa propre adresse IP pendant que ceci gêne la transmission entre le capteur et le périphérique en mode bloc. Mais, cette option est configurable par l'utilisateur.

Une fois que l'ARC est configuré pour gérer un périphérique en mode bloc, le périphérique en mode bloc évite et ACLs/VACLs qui sont utilisés pour bloquer ne devrait pas être modifié manuellement. Ceci peut entraîner une interruption du service d'ARC et peut avoir comme conséquence de futurs blocs n'étant pas émis.

Remarque: Par défaut, seulement le blocage est pris en charge sur des périphériques de Cisco IOS. Vous pouvez ignorer le par défaut de blocage si vous choisissez la limitation de débit ou le blocage plus la limitation de débit.

Afin d'émettre ou modifier des blocs, l'utilisateur IPS doit avoir le rôle d'administrateur ou d'opérateur.

Configurez le capteur pour gérer des Routeurs de Cisco

Cette section décrit comment configurer le capteur pour gérer des Routeurs de Cisco. Il contient ces thèmes :

- Configurez les profils utilisateurs
- Routeurs et ACLs
- Configurez les Routeurs de Cisco utilisant le CLI

Configurez les profils utilisateurs

Le capteur parvient les autres périphériques avec la commande de *profile_name de* **profils utilisateurs** afin d'installer des profils utilisateurs. Les profils utilisateurs contiennent l'ID utilisateur, le mot de passe, et les informations de mot de passe d'enable. Par exemple, les Routeurs que tous partagent les mêmes mots de passe et noms d'utilisateur peuvent être au-dessous d'un profil utilisateur.

Remarque: Vous **devez** créer un profil utilisateur avant que vous configuriez le périphérique en mode bloc.

Terminez-vous ces étapes afin d'installer des profils utilisateurs :

1. Ouvrez une session au CLI avec un compte qui a des privilèges d'administrateur.
2. Entrez le mode d'accès au réseau.`sensor#`**`configure terminal`** `sensor(config)#`**`service network-access`** `sensor(config-net)#`
3. Créez le nom de profil utilisateur.`sensor(config-net)#`**`user-profiles`** *`PROFILE1`*
4. Tapez le nom d'utilisateur pour ce profil utilisateur.`sensor(config-net-use)#`**`username`** *`username`*
5. Spécifiez le mot de passe pour l'utilisateur.`sensor(config-net-use)#` **`password`** `Enter password[]: ******** Re-enter password ********`
6. Spécifiez le mot de passe d'enable pour l'utilisateur.`sensor(config-net-use)#` **`enable-password`** `Enter enable-password[]: ******** Re-enter enable-password ********`
7. Vérifiez les configurations.`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 **entrent** afin d'appliquer les modifications ou entrer non pour les jeter.

Routeurs et ACLs

Quand l'ARC est configuré avec un périphérique en mode bloc qui utilise ACLs, l'ACLs se composent de cette façon :

1. Une ligne d'autorisation avec l'adresse IP de capteur ou, si spécifié, l'adresse NAT du capteur**Remarque:** Si vous permettez le capteur à bloquer, cette ligne n'apparaît pas dans l'ACL.
2. ACL de Pré-bloc (si spécifié)Cet ACL doit déjà exister sur le périphérique.**Remarque:** L'ARC lit les lignes dans l'ACL préconfiguré et copie ces lignes sur le début de l'ACL de bloc.
3. Tous blocs actifs
4. L'un ou l'autre : IP tout quel d'autorisation du POST-bloc ACL- **ACL de POST-bloc** (si spécifié)Cet ACL doit déjà exister sur le périphérique.**Remarque:** L'ARC lit les lignes dans l'ACL et copie ces lignes sur la fin de l'ACL.**Remarque:** Assurez-vous la dernière ligne dans l'ACL en est IP tout d'autorisation si vous voulez que tous les paquets inégalés soient permis.- **IP tout quel d'autorisation** (non utilisé si un ACL de POST-bloc est spécifié)

Remarque: L'ACLs que l'ARC fait devrait ne jamais être modifié par vous ou tout autre système. Ces ACLs sont provisoire et nouvel ACLs sont constamment créés par le capteur. Les seules modifications que vous pouvez apporter sont au Pre- et au POST-bloc ACLs.

Si vous devez modifier l'ACL du Pré-bloc ou de POST-bloc, terminez-vous ces étapes :

1. Débronchement bloquant sur le capteur.
2. Apportez les modifications à la configuration du périphérique.
3. Reenable bloquant sur le capteur.

Quand le blocage est réactivé, le capteur indique la nouvelle configuration de périphérique.

Remarque: Un à un seul capteur peut gérer de plusieurs périphériques, mais les plusieurs capteurs ne peuvent pas gérer un à un dispositif. Dans le cas que des blocs émis de plusieurs capteurs sont signifiés pour un périphérique en mode bloc simple, un capteur de blocage principal doit être incorporé à la conception. Un capteur de blocage principal reçoit bloquer des demandes de plusieurs capteurs et fournit toutes les demandes de blocage au périphérique en mode bloc.

Vous créez et sauvegardez le Pré-bloc et le POST-bloc ACLs en votre configuration de routeur. Ces ACLs doit être IP étendu ACLs, nommé ou numéroté. Voir la votre documentation sur le routeur pour plus d'informations sur la façon créer ACLs.

Remarque: Le Pré-bloc et le POST-bloc ACLS ne s'appliquent pas à la limitation de débit.

ACLs sont hiérarchisé évalué et la mesure de premier-correspondance est prise. L'ACL de Pré-bloc peut contenir une autorisation qui aurait la priorité au-dessus d'un refuser qui a résulté d'un bloc.

L'ACL de POST-bloc est utilisé pour expliquer toutes les conditions non manipulées par l'ACL ou les blocs de Pré-bloc. Si vous avez un ACL existant sur l'interface et dans la direction que les blocs sont émis, cet ACL peut être utilisé comme ACL de POST-bloc. Si vous n'avez pas un ACL de POST-bloc, les insertions de capteur permettent l'IP tout à la fin du nouvel ACL.

Quand le capteur démarre, il lit le contenu des deux ACLs. Il crée un ACL de tiers avec ces entrées :

- Une ligne d'autorisation pour l'adresse IP de capteur
- Copies de toutes les lignes de configuration de l'ACL de Pré-bloc
- Une ligne de refuser pour chaque adresse qui sont bloqués par le capteur
- Copies de toutes les lignes de configuration de l'ACL de POST-bloc

Le capteur s'applique le nouvel ACL à l'interface et la direction que vous indiquez.

Remarque: Quand le nouvel ACL de bloc est appliqué à une interface du routeur, dans une direction particulière, elle remplace tout ACL de préexistence sur cette interface dans cette direction.

Configurez les Routeurs de Cisco utilisant le CLI

Terminez-vous ces étapes afin de configurer un capteur pour parvenir un routeur de Cisco pour exécuter le blocage et la limitation de débit :

1. Ouvrez une session au CLI avec un compte qui a des privilèges d'administrateur.
2. Écrivez le sous-mode d'accès au réseau.`sensor#configure terminal sensor(config)#service network-access sensor(config-net)#`
3. Spécifiez l'adresse IP pour le routeur contrôlé par l'ARC.`sensor(config-net)#router-devices ip_address`
4. Écrivez le nom de périphérique logique que vous avez créé quand vous avez configuré le profil utilisateur.`sensor(config-net-rou)#profile-name user_profile_name` L'ARC reçoit n'importe quoi que vous écrivez. Il ne vérifie pas pour voir 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, le SSH 3DES est utilisé.**Remarque:** Si vous utilisez le DES ou le 3DES, vous devez utiliser les **ip_address de clé de hôte de ssh** commandez afin de recevoir le ssh key du périphérique.
6. Spécifiez l'adresse NAT de capteur.`sensor(config-net-rou)#nat-address nat_address` **Remarque:** Ceci change l'adresse IP dans la première ligne de l'ACL de l'adresse du capteur à l'adresse NAT. L'adresse NAT est l'adresse de capteur, POST-NAT, traduite par un périphérique intermédiaire, situé entre le capteur et le périphérique en mode bloc.
7. Spécifiez si le routeur exécute le blocage, la limitation de débit, ou chacun des deux.**Remarque:** Le par défaut bloque. Vous ne devez pas configurer des capacités de réponse si vous voulez que le routeur exécute le blocage seulement.Limitation de débit seulement`sensor(config-net-rou)#response-capabilities rate-limit` Bloquant et limitation de débit`sensor(config-net-rou)#response-capabilities block|rate-limit`
8. Spécifiez le nom et la direction d'interface.`sensor(config-net-rou)#block-interfaces interface_name {in | out}` **Remarque:** Le nom de l'interface doit être une abréviation que le routeur identifie une fois utilisé après la **commande d'interface**.
9. (Facultatif) ajoutez le nom de pré-ACL (bloquant seulement).`sensor(config-net-rou-blo)#pre-acl-name pre_acl_name`
10. (Facultatif) ajoutez le nom de POST-ACL (bloquant seulement).`sensor(config-net-rou-blo)#post-acl-name post_acl_name`
11. Vérifiez les configurations.`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 **entrent** afin d'appliquer les modifications ou entrer **non** pour les jeter.

Configurez le capteur pour gérer des Pare-feu de Cisco

Terminez-vous ces étapes afin de configurer le capteur pour gérer des Pare-feu de Cisco :

1. Ouvrez une session au CLI avec un compte qui a des privilèges d'administrateur.
2. Écrivez le sous-mode d'accès au réseau.`sensor#configure terminal sensor(config)#service network-access sensor(config-net)#`
3. Spécifiez l'adresse IP pour le Pare-feu contrôlé par l'ARC.`sensor(config-net)#firewall-devices ip_address`
4. Écrivez le nom de profil utilisateur que vous avez créé quand vous avez configuré le profil utilisateur.`sensor(config-net-fir)#profile-name user_profile_name` L'ARC reçoit n'importe quoi que vous tapez. Il ne vérifie pas pour voir 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, le SSH 3DES est utilisé.**Remarque:** Si vous utilisez le DES ou le 3DES, vous devez utiliser les **ip_address de clé de hôte de ssh** commandez afin de recevoir la clé ou l'ARC ne peut pas se connecter au périphérique.
6. Spécifiez l'adresse NAT de capteur.`sensor(config-net-fir)#nat-address nat_address` **Remarque:** Ceci change l'adresse IP dans la première ligne de l'ACL de l'adresse IP du capteur à l'adresse NAT. L'adresse NAT est l'adresse de capteur, POST-NAT, traduite par un périphérique intermédiaire, situé entre le capteur et le périphérique en mode bloc.
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 **entrent** afin d'appliquer les modifications ou entrer **aucun** afin de les jeter.

Le bloc avec ÉVITENT dans PIX/ASA

Émettre la commande d'**évitement** bloque des connexions d'un hôte de attaque. Des paquets qui apparient les valeurs dans la commande sont lâchés et connectés jusqu'à ce que la fonction de blocage soit retirée. **L'évitement** est appliqué indépendamment si une connexion avec le host address spécifié est actuellement - de l'active.

Si vous spécifiez l'adresse de destination, source et destinations port, et le protocole, vous rétrécissez l'évitement aux connexions qui apparient ces paramètres.

Vous pouvez seulement faire **éviter** on la commande pour chaque adresse IP source.

Puisque la commande d'**évitement** est utilisée de bloquer des attaques dynamiquement, elle n'est pas affichée dans la configuration de dispositifs de sécurité.

Toutes les fois qu'une interface est retirée, tout évite ce qui sont reliées à cette interface sont également retirées.

Cet exemple prouve que l'hôte offensant (10.1.1.27) établit un rapport avec la victime (10.2.2.89) au TCP. La connexion dans la table de connexion de dispositifs de sécurité lit comme suit :

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

Afin de bloquer des connexions d'un hôte de attaque, utilisez la commande d'**évitement** dans le mode d'exécution privilégié. Appliquez la commande d'**évitement** avec ces options :

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

La commande supprime la connexion de la table de connexion de dispositifs de sécurité et empêche également des paquets de 10.1.1.27:555 à 10.2.2.89:666 (TCP) d'aller par les dispositifs de sécurité.

Informations connexes

- Configuration du capteur gérer les Commutateurs et le Routeurs de la gamme Cisco 7600 de gamme Catalyst 6500
- Configurer le contrôleur de réponse d'attaque pour le blocage et la limitation de débit utilisant IDM 7.0
- Support et documentation techniques - Cisco Systems