Fonctionnalité et configuration de détection de menace ASA

Contenu

Introduction

Ce document décrit la fonctionnalité et la configuration de base de la fonction de détection des menaces du Dispositif de sécurité adaptatif (ASA) dédié Cisco. La détection de menace fournit à des administrateurs de Pare-feu les outils nécessaires pour identifier, comprendre, et arrêter des attaques avant qu'elles atteignent l'infrastructure de réseau interne. Afin de faire ainsi, la caractéristique se fonde sur un certain nombre de déclencheurs et de statistiques différents, qui sont décrites dans davantage de détail dans ces sections.

La détection de menace peut être utilisée sur n'importe quel Pare-feu ASA qui exécute une version de logiciel de 8.0(2) ou plus tard. Bien que la détection de menace ne soit pas une substitution pour une solution dédiée IDS/IPS, elle peut être utilisée dans les environnements où un IPS n'est pas disponible pour fournir une couche ajoutée de protection à la fonctionnalité du noyau de l'ASA.

Fonctionnalité de détection de menace

La caractéristique de détection de menace a trois composants principaux :

1. Détection de base de menace
2. Détection avancée de menace
3. Détection de balayage de menace

Chacun de ces composants est décrit en détail dans ces sections.

Détection de base de menace (débits au niveau système)

La détection de base de menace est activée par défaut sur toute l'exécution ASA 8.0(2) et plus tard.

La détection de base de menace surveille les débits auxquels des paquets sont lâchés pour différentes raisons par l'ASA dans son ensemble. Ceci signifie que les statistiques générées par détection de base de menace s'appliquent seulement à l'appliance entière et ne sont généralement pas assez granulaires pour fournir des informations sur la source ou la nature spécifique de menace. Au lieu de cela, l'ASA surveille les paquets relâchés pour ces événements :

- **Baisse d'ACL (acl-baisse)** - Des paquets sont refusés par des Listes d'accès
- **Mauvais paquets (mauvais-paquet-baisse)** - Le paquet non valide formate, qui inclut les en-têtes L3 et L4 qui ne se conforment pas aux normes RFC
- **Limite conn. (conn.-limite-baisse)** - Paquets qui dépassent une limite configurée ou globale de connexion
- **Attaque DoS (DOS-baisse)** - Attaques du Déni de service (DOS)
- **Pare-feu (FW-baisse)** - Contrôles de sécurité du pare-feu de base
- **Attaque d'ICMP (ICMP-baisse)** - Paquets méfiants d'ICMP
- **Examinez (examiner-baisse)** - Refus par inspection d'application
- **Interface (interface-baisse)** - Paquets relâchés par des contrôles d'interface
- **Balayage (lecture-menace)** - Attaques de lecture de réseau/hôte
- **Attaque de synchronisation (synchronisation-attaque)** - Attaques inachevées de session, qui inclut les attaques de synchronisation de TCP et les sessions unidirectionnelles d'UDP qui n'ont aucune donnée de retour

Chacun de ces événements a un ensemble spécifique de déclencheurs qui sont utilisés pour identifier la menace. La plupart des déclencheurs sont attachés de nouveau aux raisons spécifiques de baisse d'ASP, bien que de certains Syslog et actions d'inspection soient également considérés. Quelques déclencheurs sont surveillés par de plusieurs catégories de menace. Certains des déclencheurs les plus communs sont tracés les grandes lignes dans cette table, bien que ce ne soit pas une liste exhaustive :

Menace de base	Déclencheurs/raisons baisse d'ASP
acl-baisse	acl-baisse
mauvais-paquet-baisse	non valide-TCP-HDR-longueur non valide-IP-en-tête examiner-dn-PAK-trop-long examiner-dn-id-non-apparié
conn.-limite-baisse	conn.-limite
DOS-baisse	fournisseur de services-Sécurité-échoué

	examiner-ICMP-seq-numérique-non-apparié
	examiner-dn-PAK-trop-long
FW-baisse	examiner-dn-id-non-apparié
	fournisseur de services-Sécurité-échoué
	acl-baisse
ICMP-baisse	examiner-ICMP-seq-numérique-non-apparié
examiner-baisse	Baisses de vue déclenchées par une engine d'inspection
interface-baisse	fournisseur de services-Sécurité-échoué
	NO--artère
	tcp-3whs-failed
	TCP-non-synchronisation
	fournisseur de services-Sécurité-échoué
lecture-menace	acl-baisse
	examiner-ICMP-seq-numérique-non-apparié
	examiner-dn-PAK-trop-long
	examiner-dn-id-non-apparié
synchronisation-attaque	Syslog %ASA-6-302014 avec la raison de désinstallation du « délai d'attente de synchronisation »

Pour chaque événement, la détection de base de menace mesure les débits que ces baisses se produisent sur une période configurée. Cette période s'appelle l'**intervalle de débit moyen (ARI)** et peut s'étendre de 600 secondes à 30 jours. Si le nombre d'événements qui se produisent dans ARI dépasse les seuils de débit configuré, l'ASA considère ces événements une menace.

La détection de base de menace a deux seuils configurables pour quand elle considère comme étant des événements une menace : **le débit moyen** et le **débit de rafales**. Le débit moyen est simplement le nombre moyen de baisses par seconde au cours du délai prévu d'ARI configuré. Par exemple, si le seuil de débit moyen pour des baisses d'ACL est configuré pour 400 avec ARI de 600 secondes, l'ASA calcule le nombre moyen de paquets qui ont été lâchés par ACLs dans les 600 dernières secondes. Si ce nombre s'avère être plus grand que 400 par seconde, l'ASA se connecte une menace.

De même, le débit de rafales est très semblable mais regarde de plus petites périodes des données d'instantané, appelées l'**intervalle de débit de rafales (BRI)**. Le BRI est toujours plus petit qu'ARI. Par exemple, la construction sur l'exemple précédent, ARI pour des baisses d'ACL est toujours de 600 secondes et a maintenant un débit de rafales de 800. Avec ces valeurs, l'ASA calcule le nombre moyen de paquets relâchés par ACLs dans les 20 dernières secondes, où 20 secondes est les BRI. Si cette valeur calculée dépasse 800 gouttes par seconde, une menace est enregistré. Afin de déterminer quel BRI est utilisé, l'ASA calcule la valeur de la 1/30th d'ARI. Par conséquent, dans l'exemple précédemment utilisé, le 1/30th de 600 secondes est de 20 secondes. Cependant, la détection de menace a BRI 10 secondes au minimum, ainsi si le 1/30th d'ARI est moins de 10, l'ASA utilise toujours 10 secondes comme BRI. En outre, il est important de noter que ce comportement était différent dans les versions antérieures à 8.2(1), qui ont utilisé une valeur de la 1/60th de l'ARI, au lieu du 1/30th. Le minimum BRI de 10 secondes est identique pour toutes les versions de logiciel.

Quand une menace de base est détectée, l'ASA génère simplement le Syslog %ASA-4-733100 pour alerter l'administrateur qu'un danger potentiel a été identifié. La moyenne, le courant, et le nombre total d'événements pour chaque catégorie de menace peuvent être vus avec la commande de **débit de menace-détection d'exposition**. Le nombre total d'événements cumulatifs est la somme du nombre d'événements vus dans les 30 derniers échantillons BRI.

La détection de base de menace ne prend aucune mesure afin d'arrêter le trafic offensant ou

empêcher de futures attaques. Dans ce sens, la détection de base de menace est purement informationnelle et peut être utilisée comme surveillance ou mécanisme d'enregistrement.

Détection avancée de menace (statistiques d'objet et dessus de niveau N)

Àla différence de la détection de base de menace, la détection avancée de menace peut être utilisée pour dépister des statistiques pour des objets plus granulaires. L'ASA prend en charge dépister des statistiques pour l'hôte IPS, les ports, les protocoles, l'ACLs, et les serveurs protégés par l'Interception TCP. La détection avancée de menace est seulement activée par défaut pour des statistiques d'ACL.

Pour l'hôte, le port, et les objets de protocole, la détection de menace maintient le nombre de paquets, d'octets, et de baisses qui ont été envoyées et reçues par cet objet au cours d'une période spécifique. Pour ACLs, la détection de menace maintient les 10 as principaux (l'autorisation et refusent) qu'étaient frappés plus au cours d'une période spécifique.

Les délais prévus dépistés en tout de ces cas sont de 20 minutes, de 1 heure, de 8 heures, et de 24 heures. Tandis que les délais prévus eux-mêmes ne sont pas configurables, le nombre de périodes qui sont dépistées par objet peut être ajusté avec le mot clé de « nombre-de-débit ». Voyez le pour en savoir plus de section de configuration. Par exemple, si le « nombre-de-débit » est placé à 2, vous voyez toutes les statistiques pour 20 minutes, 1 heure et 8 heures. si le « nombre-de-débit » est placé à 1, vous voyez toutes les statistiques pendant 20 minutes, 1 heure. N'importe ce que, les 20 débits minute sont toujours affichés.

Quand l'Interception TCP est activée, la détection de menace peut maintenir les 10 serveurs principaux qui sont considérés sous l'attaque et protégés par l'Interception TCP. Les statistiques pour l'Interception TCP sont semblables à la détection de base de menace dans le sens que l'utilisateur peut configurer le débit-intervalle mesuré avec les débits spécifiques de moyenne (ARI) et de rafale (BRI). Les statistiques avancées de détection de menace pour l'Interception TCP sont seulement disponibles dans ASA 8.0(4) et plus tard.

Des statistiques avancées de détection de menace sont visualisées par l'intermédiaire des **statistiques de menace-détection d'exposition** et **affichent des** commandes de **dessus de statistiques de menace-détection**. C'est également la caractéristique responsable de remplir graphiques « supérieurs » sur le tableau de bord de Pare-feu de l'ASDM. Les seuls Syslog qui sont générés par détection avancée de menace sont %ASA-4-733104 et %ASA-4-733105, qui sont déclenchés quand la moyenne et les débits de rafales (respectivement) sont dépassés pour des statistiques d'Interception TCP.

Comme la détection de base de menace, la détection avancée de menace est purement informationnelle. Aucune mesure n'est prise de bloquer le trafic basé sur les statistiques avancées de détection de menace.

Détection de balayage de menace

La détection de balayage de menace est utilisée afin de maintenir les attaquants suspectés qui créent des connexions trop d'hôtes dans un sous-réseau, ou beaucoup de ports sur un hôte/sous-réseau. La détection de balayage de menace est désactivée par défaut.

Constructions de balayage de détection de menace sur le concept de la détection de base de

menace, qui définit déjà une catégorie de menace pour une attaque de lecture. Par conséquent, le débit-intervalle, le débit moyen (ARI), et les configurations du débit de rafales (BRI) sont partagés entre la détection de base et de lecture de menace. La différence entre les 2 caractéristiques est que tandis que la détection de base de menace indique seulement que la moyenne ou les seuils de débit de rafales ont été franchis, la détection de balayage de menace met à jour une base de données des adresses IP d'attaquant et de cible qui peuvent aider à fournir plus de cadre autour des hôtes impliqués dans le balayage. Supplémentaire, seulement le trafic qui est reçu réellement par l'hôte de cible/sous-réseau est considéré en balayant la détection de menace. La détection de base de menace peut encore déclencher une menace de lecture même si le trafic est abandonné par un ACL.

La détection de balayage de menace peut sur option réagir à une attaque en évitant l'IP d'attaquant. Ceci fait à détection de menace de lecture le seul sous-ensemble de la caractéristique de détection de menace qui peut activement affecter des connexions par l'ASA.

Quand la détection de balayage de menace détecte une attaque, %ASA-4-733101 est enregistré pour l'attaquant et/ou la cible IPS. Si la caractéristique est configurée pour éviter l'attaquant, %ASA-4-733102 est enregistré quand la détection de balayage de menace génère un évitement. %ASA-4-733103 est enregistré quand l'évitement est enlevé. La commande de lecture-**menace de menace-détection d'exposition** peut être utilisée afin de visualiser la base de données entière de menace de lecture.

Limites

- La détection de menace est seulement disponible dans ASA 8.0(2) et plus tard. Il n'est pas pris en charge sur la plate-forme ASA 1000V.
- La détection de menace est seulement prise en charge en mode de contexte unique.
- Seulement des menaces d'à travers-le-case sont détectées. Le trafic envoyé à l'ASA elle-même n'est pas considéré par détection de menace.
- Des tentatives de connexion TCP qui sont remises à l'état initial par le serveur visé n'est pas comptées comme attaque de synchronisation ou menace de lecture.

Configuration

Détection de base de menace

La détection de base de menace est activée avec la commande de base-**menace de menace-détection**.

```
ciscoasa(config)# threat-detection basic-threat
```

Les débits par défaut peuvent être visualisés avec l'**exposition exécutent toute la** commande de menace-**détection**.

```
ciscoasa(config)# show run all threat-detection
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
```

```
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

Afin d'accorder ces débits avec des valeurs en douane, modifiez simplement la commande de **débit de menace-détection** pour la catégorie appropriée de menace.

```
ciscoasa(config)# threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate
550
```

Chaque catégorie de menace peut avoir un maximum de 3 débits différents définis (avec des id de débit de débit 1, de débit 2, et de débit 3). L'ID particulier de débit qui est dépassé est mis en référence dans le Syslog %ASA-4-733100.

Dans l'exemple précédent, la détection de menace crée le Syslog 733100 seulement quand le nombre de baisses d'ACL dépasse 250 gouttes/seconde plus de 1200 secondes ou 550 gouttes/seconde plus de 40 secondes.

Détection avancée de menace

Employez la commande de **statistiques de menace-détection** afin d'activer la détection avancée de menace. Si aucun mot clé de caractéristique spécifique n'est fourni, les commandes enables dépistant pour toutes les statistiques.

```
ciscoasa(config)# threat-detection statistics ?
configure mode commands/options:
access-list Keyword to specify access-list statistics
host Keyword to specify IP statistics
port Keyword to specify port statistics
protocol Keyword to specify protocol statistics
tcp-intercept Trace tcp intercept statistics
<cr>
```

Afin de configurer le nombre d'intervalles de débit qui sont dépistés pour l'hôte, le port, le protocole, ou les statistiques d'ACL, utilisez le mot clé de nombre-de-**débit**.

```
ciscoasa(config)# threat-detection statistics host number-of-rate 2
```

Le mot clé de nombre-de-débit configure la détection de menace pour dépister seulement le nombre le plus court *n d'*intervalles.

Afin d'activer des statistiques d'Interception TCP, utilisez la commande d'**Interception TCP de statistiques de menace-détection**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept
```

Afin de configurer les débits faits sur commande pour des statistiques d'Interception TCP, utilisez le débit-**intervalle**, le **débit moyen**, et les mots clé de **débit de rafales**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept rate-interval 45
burst-rate 400 average-rate 100
```

Détection de balayage de menace

Afin d'activer la détection de menace de lecture, utilisez la commande de lecture-**menace de menace-détection**.

```
ciscoasa(config)# threat-detection scanning-threat
```

Afin d'ajuster les débits pour une lecture-menace, utilisez la même commande de **débit de menace-détection** utilisée par détection de base de menace.

```
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 250
burst-rate 550
```

Afin de permettre à l'ASA pour éviter un IP d'attaquant de lecture, ajoutez le mot clé d'**évitement à la** commande de lecture-**menace de menace-détection**.

```
ciscoasa(config)# threat-detection scanning-threat shun
```

Ceci permet à la détection de menace de lecture pour créer une une heure évitent pour l'attaquant. Afin d'ajuster la durée de l'évitement, utilisez la lecture-**menace de menace-détection évitent la** commande de **durée**.

```
ciscoasa(config)# threat-detection scanning-threat shun duration 1000
```

Dans certains cas, vous pouvez encore vouloir empêcher l'ASA d'éviter certain IPS. Afin de faire ceci, créez une exception avec la lecture-**menace de menace-détection évitent excepté la** commande.

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.1
255.255.255.255
ciscoasa(config)# threat-detection scanning-threat shun except object-group no-shun
```

Représentation

La détection de base de menace a l'incidence des performances très petite sur l'ASA. La détection avancée et de lecture de menace sont beaucoup plus de ressource intensive parce qu'ils doivent maintenir de diverses statistiques dans la mémoire. Seulement la détection de balayage de menace avec la fonction d'évitement activée peut activement affecter le trafic qui autrement aurait été permis.

Pendant que les versions de logiciel ASA ont progressé, l'utilisation de mémoire de la détection de menace a été sensiblement optimisée. Cependant, le soin devrait être pris pour surveiller l'utilisation de mémoire de l'ASA avant et après que la détection de menace soit activée. Dans certains cas, il pourrait être meilleur d'activer seulement certaines statistiques (par exemple, des statistiques d'hôte) temporairement tout en activement dépannant une problématique spécifique.

Pour une vue plus détaillée de l'utilisation de mémoire de la détection de menace, exécutez la commande de menace-**détection d'app-cache de show memory [détail]**.

Actions recommandées

Ces sections fournissent quelques recommandations générales pour les mesures qui peuvent être

prises quand les événements liés à la détection de diverse menace se produisent.

Quand un débit de base de baisse est dépassé et %ASA-4-733100 est généré

Déterminez la catégorie spécifique de menace mentionnée dans le Syslog %ASA-4-733100 et corrélez ceci avec la sortie du **débit de menace-détection d'exposition**. Avec ces informations, vérifiez la sortie de la **baisse d'asp d'exposition** afin de déterminer les raisons pour lesquelles le trafic est abandonné.

Pour une vue plus détaillée du trafic qui est abandonné pour une raison spécifique, utilisez une capture de baisse d'ASP avec la raison en question afin de voir tous les paquets qui sont lâchés. Par exemple, si les menaces de baisse d'ACL sont enregistré, capture sur la raison de baisse d'ASP de l'acl-**baisse** :

```
ciscoasa# capture drop type asp-drop acl-drop

ciscoasa# show capture drop

1 packet captured

1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53: udp 34 Drop-reason:
(acl-drop) Flow is denied by configured rule
```

Cette capture prouve que le paquet étant lâché est un paquet UDP/53 de 10.10.10.10 à 192.168.1.100.

Si %ASA-4-733100 signale une menace de lecture, il peut également être utile d'activer temporairement la détection de menace de lecture. Ceci permet à l'ASA pour maintenir la source et la destination IPS impliquées dans l'attaque.

Puisque le trafic de base de moniteurs de détection de menace en grande partie qui déjà est abandonné par l'ASP, aucune action directe est exigé pour lever un danger potentiel. Les exceptions à ceci sont des menaces d'attaques et de lecture de synchronisation, qui impliquent le trafic traversant l'ASA.

Si les baisses vues dans la capture de baisse d'ASP sont légitimes et/ou prévues pour l'environnement de réseau, accordez les intervalles de débit de base à une valeur plus appropriée.

Si les baisses affichent le trafic illégitime, des mesures devraient être prises pour bloquer ou raté limit le trafic avant qu'il atteigne l'ASA. Ceci peut inclure ACLs et QoS sur les périphériques en amont.

Pour des attaques de synchronisation, le trafic peut être bloqué dans un ACL sur l'ASA. L'Interception TCP pourrait également être configurée pour protéger les serveurs visés, mais ceci pourrait simplement avoir comme conséquence une menace de limite conn. étant enregistré à la place.

Pour des menaces de balayage, le trafic peut également être bloqué dans un ACL sur l'ASA. La détection de balayage de menace avec l'option d'**évitement** peut être activée permettre à l'ASA pour bloquer proactivement tous les paquets de l'attaquant pendant une période définie.

Quand une menace de lecture est détectée et %ASA-4-733101 est enregistré

%ASA-4-733101 devrait répertorier l'hôte de cible/sous-réseau ou l'adresse IP d'attaquant. Pour la liste complète de cibles et d'attaquants, vérifiez la sortie de la lecture-**menace de menace-détection d'exposition**.

Les captures de paquet sur les interfaces ASA faisant face à l'attaquant et/ou aux cibles peuvent également aider à clarifier la nature de l'attaque.

Si le balayage détecté est non prévu, des mesures devraient être prises pour bloquer ou raté limit le trafic avant qu'il atteigne l'ASA. Ceci peut inclure ACLs et QoS sur les périphériques en amont. Ajouter l'option d'**évitement au** config de détection de menace de lecture peut également permettre à l'ASA pour relâcher proactivement tous les paquets de l'IP d'attaquant pendant une période définie. En dernier recours, le trafic peut également être bloqué manuellement sur l'ASA par l'intermédiaire d'un ACL ou d'une stratégie d'Interception TCP.

Si le balayage détecté est un faux positif, ajustez les intervalles de débit de menace de lecture à une valeur plus appropriée pour l'environnement de réseau.

Quand un attaquant est évité et %ASA-4-733102 est enregistré

%ASA-4-733102 répertorie l'adresse IP de l'attaquant évité. Utilisez la menace-**détection d'exposition évitent la** commande afin de visualiser une liste complète d'attaquants qui ont été évités par détection de menace spécifiquement. Utilisez l'**exposition évitent la** commande afin de visualiser la liste complète de tous les IPS qui activement sont évités par l'ASA (de sources y compris autres que la détection de menace).

Si l'évitement fait partie d'une attaque légitime, aucune action supplémentaire n'est exigée. Cependant, il serait salutaire de bloquer manuellement le trafic de l'attaquant comme loin en amont vers la source comme possible. Ceci peut être fait par l'intermédiaire d'ACLs et de QoS. Ceci s'assure que les périphériques intermédiaires n'ont pas besoin de gaspiller des ressources traitant le trafic illégitime.

Si la menace de lecture qui a déclenché l'évitement était un faux positif, enlevez manuellement l'évitement avec la menace-**détection claire évitent [la** commande d'**IP_address]**.

Quand %ASA-4-733104 et/ou %ASA-4-733105 est enregistré

%ASA-4-733104 et %ASA-4-733105 répertorie l'hôte visé par l'attaque qui actuellement est protégée par l'Interception TCP. Pour plus de détails sur les taux d'attaque et les serveurs protégés, vérifiez la sortie de l'**Interception TCP de dessus de statistiques de menace-détection d'exposition**.

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins Sampling interval: 30 secs
------------------------------------------------------------------------------
1 192.168.1.2:5000 inside 1249 9503 2249245 Last: 10.0.0.3 (0 secs ago)
2 192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3 192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4 192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5 192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6 192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7 192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
```

```
8 192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9 192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10 192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Quand la détection avancée de menace détecte une attaque de cette nature, l'ASA protège déjà le serveur visé par l'intermédiaire de l'Interception TCP. Vérifiez les limites configurées de connexion pour s'assurer qu'elles assurent la protection adéquate pour la nature et le débit de l'attaque. En outre, il serait salutaire de bloquer manuellement le trafic de l'attaquant comme loin en amont vers la source comme possible. Ceci peut être fait par l'intermédiaire d'ACLs et de QoS. Ceci s'assure que les périphériques intermédiaires n'ont pas besoin de gaspiller des ressources traitant le trafic illégitime.

Si l'attaque détectée est un faux positif, ajustez les débits pour une attaque d'Interception TCP à une valeur plus appropriée avec la commande d'**Interception TCP de statistiques de menace-détection**.

Comment déclencher manuellement une menace

Pour tester et dépannage des buts, il peut être utile de déclencher manuellement de diverses menaces. Cette section contient des conseils pour déclencher quelques types communs de menace.

Menace de base - Baisse, Pare-feu, et lecture d'ACL

Afin de déclencher une menace de base particulière, référez-vous à la table dans la section précédente de fonctionnalité. Choisissez une raison spécifique de baisse d'ASP et envoyez le trafic par l'ASA qui serait relâchée par la raison appropriée de baisse d'ASP.

Par exemple, les menaces toutes de baisse d'ACL, de Pare-feu, et de lecture considèrent le débit de paquets abandonné par acl-baisse. Terminez-vous ces étapes afin de déclencher ces menaces simultanément :

1. Créez un ACL sur l'interface extérieure de l'ASA qui relâche explicitement tous les paquets TCP envoyés à un serveur de cible sur l'intérieur de l'ASA (10.11.11.11) :`access-list outside_in extended line 1 deny tcp any host 10.11.11.11`
   ```
   access-list outside_in extended permit ip any any
   access-group outside_in in interface outside
   ```
2. D'un attaquant sur l'extérieur de l'ASA (10.10.10.10), nmap d'utilisation afin d'exécuter un balayage de synchronisation de TCP contre chaque port sur le serveur de cible :`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Remarque: T5 configure le nmap pour exécuter le balayage aussi rapide comme possible. Selon les ressources en PC d'attaquant, ceci peut encore ne pas être assez rapide pour déclencher certains des débits par défaut. Si c'est le cas, diminuez simplement les débits configurés pour la menace que vous voulez voir. Établissement d'ARI et du BRI à 0 détections de base de menace de causes pour déclencher toujours la menace indépendamment du débit.
3. Notez que des menaces de base sont détectées pour des menaces de baisse, de Pare-feu, et de lecture d'ACL :`%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,`
   ```
   max configured rate is 10; Current average rate is 9 per second,
   max configured rate is 5; Cumulative total count is 5538
   %ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
   ```

```
max configured rate is 0; Current average rate is 2 per second,
max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
max configured rate is 0; Current average rate is 2 per second,
max configured rate is 0; Cumulative total count is 1483
```
Remarque: Dans cet exemple, la baisse et le Pare-feu ARIs et BRIs d'ACL ont été placés à 0 ainsi qu'elles déclenchent toujours une menace. C'est pourquoi les débits configurés maximum sont répertoriés en tant que 0.

Menace avancée - Interception TCP

1. Créez un ACL sur l'interface extérieure qui permet tous les paquets TCP envoyés à un serveur de cible sur l'intérieur de l'ASA (10.11.11.11) :
```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```
2. Si le serveur de cible n'existe pas réellement, ou il remet à l'état initial les tentatives de connexion de l'attaquant, configurez une fausse entrée d'ARP sur l'ASA au blackhole le trafic d'attaque l'interface interne :`arp inside 10.11.11.11 dead.dead.dead`
3. Créez une stratégie simple d'Interception TCP sur l'ASA :
```
access-list tcp extended permit tcp any any
class-map tcp
match access-list tcp
policy-map global_policy
class tcp
set connection conn-max 2
service-policy global_policy global
```
D'un attaquant sur l'extérieur de l'ASA (10.10.10.10), nmap d'utilisation pour exécuter un balayage de synchronisation de TCP contre chaque port sur le serveur de cible :`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Notez que la détection de menace maintient le serveur protégé :
```
ciscoasa(config)#  show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins Sampling interval: 30 secs

-------------------------------------------------------------------------------
1 10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2 10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3 10.11.11.11:46126 outside 0 0 1 Last: 10.10.10.10 (6 secs ago)
4 10.11.11.11:3695 outside 0 0 1 Last: 10.10.10.10 (6 secs ago)
```

Menace de balayage

1. Créez un ACL sur l'interface extérieure qui permet tous les paquets TCP envoyés à un serveur de cible sur l'intérieur de l'ASA (10.11.11.11) :
```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```
Remarque: Pour que la détection de menace de lecture dépiste la cible et l'attaquant IPS, on doit permettre le trafic par l'ASA.
2. Si le serveur de cible n'existe pas réellement, ou il remet à l'état initial les tentatives de connexion de l'attaquant, configurez une fausse entrée d'ARP sur l'ASA au blackhole le trafic d'attaque l'interface interne :`arp inside 10.11.11.11 dead.dead.dead`Remarque: Des connexions qui sont remises à l'état initial par le serveur de cible ne sont pas comptées en tant qu'élément de la menace.
3. D'un attaquant sur l'extérieur de l'ASA (10.10.10.10), nmap d'utilisation pour exécuter un balayage de synchronisation de TCP contre chaque port sur le serveur de cible :`nmap -sS -T5`

`-p1-65535 -Pn 10.11.11.11`Remarque: T5 configure le nmap pour exécuter le balayage aussi rapide comme possible. Selon les ressources en PC d'attaquant, ceci peut encore ne pas être assez rapide pour déclencher certains des débits par défaut. Si c'est le cas, diminuez simplement les débits configurés pour la menace que vous voulez voir. Établissement d'ARI et du BRI à 0 détections de base de menace de causes pour déclencher toujours la menace indépendamment du débit.

4. Notez qu'une menace de lecture est détecté, l'IP de l'attaquant est dépisté, et l'attaquant est évité :
```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Informations connexes

- Guide de configuration ASA
- Référence de commandes ASA
- Guide de Syslog ASA
- Support et documentation techniques - Cisco Systems