Vérification de la configuration et des fonctionnalités de détection des menaces ASA

Table des matières

Introduction

Ce document décrit les trois principaux composants de la fonctionnalité et de la configuration de détection des menaces.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

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. Threat Detection fournit aux administrateurs de pare-feu les outils nécessaires pour identifier, comprendre et stopper les attaques avant qu'elles n'atteignent l'infrastructure réseau interne. Pour ce faire, la fonctionnalité s'appuie sur un certain nombre de déclencheurs et de statistiques différents, qui sont décrits plus en détail dans ces sections.

La détection des menaces peut être utilisée sur n'importe quel pare-feu ASA exécutant une version logicielle 8.0(2) ou ultérieure. Bien que la détection des menaces ne remplace pas une solution IDS/IPS dédiée, elle peut être utilisée dans les environnements où un IPS n'est pas disponible pour fournir une couche de protection supplémentaire à la fonctionnalité principale d'ASA.

Fonctionnalité de détection des menaces

La fonction de détection des menaces comporte trois composants principaux :

1. Détection des menaces de base
2. Détection avancée des menaces
3. Analyse de la détection des menaces

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

Détection de base des menaces (taux système)

La détection des menaces de base est activée par défaut sur tous les ASA qui exécutent 8.0(2) et versions ultérieures.

La détection des menaces de base surveille les taux auxquels les paquets sont abandonnés pour diverses raisons par l'ASA dans son ensemble. Cela signifie que les statistiques générées par la détection de base des menaces ne s'appliquent qu'à l'ensemble de l'appliance et ne sont généralement pas suffisamment précises pour fournir des informations sur la source ou la nature spécifique de la menace. Au lieu de cela, l'ASA surveille les paquets abandonnés pour ces événements :

- Abandon de liste de contrôle d’accès (acl-drop) : les paquets sont refusés par les listes d’accès.

- Paquets incorrects (bad-packet-drop) : formats de paquet non valides, qui incluent des en-têtes L3 et L4 non conformes aux normes RFC.
- Conn Limit (conn-limit-drop) : paquets qui dépassent une limite de connexion configurée ou globale.
- Attaque DoS (dos-drop) : attaques par déni de service (DoS).
- Pare-feu (fw-drop) : vérifications de sécurité de base du pare-feu.
- Attaque ICMP (icmp-drop) - Paquets ICMP suspects.
- Inspect (inspect-drop) - Refus par contrôle de l'application.
- Interface (interface-drop) : paquets abandonnés par les vérifications d'interface.
- Analyse (menace d'analyse) : attaques d'analyse réseau/hôte.
- Attaque SYN (syn-attack) - Attaques de session incomplète, y compris les attaques SYN TCP et les sessions UDP unidirectionnelles sans données de retour.

Chacun de ces événements comporte un ensemble spécifique de déclencheurs qui sont utilisés pour identifier la menace. La plupart des déclencheurs sont liés à des raisons d'abandon ASP spécifiques, bien que certaines actions syslog et d'inspection soient également prises en compte. Certains déclencheurs sont surveillés par plusieurs catégories de menaces. Certains des déclencheurs les plus courants sont décrits dans ce tableau, bien qu'il ne s'agisse pas d'une liste exhaustive :

Menace de base	Déclencheur(s) / Raison(s) d'abandon ASP
perte d'appel	perte d'appel
abandon de paquets erronés	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-match
conn-limit-drop	conn-limit
désintoxication	sp-security-failed
fw-drop	inspect-icmp-seq-num-not-match inspect-dns-pak-too-long inspect-dns-id-not-match sp-security-failed perte d'appel
icmp-drop	inspect-icmp-seq-num-not-match
inspecter-larguer	Pertes de trames déclenchées par un moteur d'inspection

interface-drop	sp-security-failed route interdite
menace d'analyse	tcp-3whs-failed tcp-not-syn sp-security-failed perte d'appel inspect-icmp-seq-num-not-match inspect-dns-pak-too-long inspect-dns-id-not-match
syn-attack	%ASA-6-302014 syslog avec le motif de démontage « SYN Timeout »

Pour chaque événement, la détection des menaces de base mesure le taux de ces abandons sur une période configurée. Cette période est appelée intervalle de débit moyen (ARI) et peut aller de 600 secondes à 30 jours. Si le nombre d'événements qui se produisent dans l'ARI dépasse les seuils de débit configurés, l'ASA considère ces événements comme une menace.

La détection de base des menaces comporte deux seuils configurables pour le moment où elle considère les événements comme une menace : le taux moyen et le taux de rafales. Le taux moyen est simplement le nombre moyen de pertes par seconde au cours de la période de temps de l'ARI configuré. Par exemple, si le seuil de débit moyen pour les abandons de liste de contrôle d'accès est configuré pour 400 avec un ARI de 600 secondes, l'ASA calcule le nombre moyen de paquets qui ont été abandonnés par les listes de contrôle d'accès au cours des 600 dernières secondes. Si ce nombre s'avère supérieur à 400 par seconde, l'ASA consigne une menace.

De même, le débit en rafale est très similaire, mais il examine de plus petites périodes de données instantanées, appelées intervalles de débit en rafale (BRI). L'accès de base est toujours plus petit que l'accès ARI. Par exemple, sur la base de l'exemple précédent, le délai d'interruption de l'ARI pour les listes de contrôle d'accès est toujours de 600 secondes et a maintenant un taux de rafale de 800. Avec ces valeurs, l'ASA calcule le nombre moyen de paquets abandonnés par les listes de contrôle d'accès en 20 secondes, où 20 secondes est l'accès de base. Si cette valeur calculée dépasse 800 abandons par seconde, une menace est consignée. Afin de déterminer quel BRI est utilisé, l'ASA calcule la valeur de 1/30e de l'ARI. Par conséquent, dans l'exemple précédemment utilisé, 1/30e de 600 secondes est de 20 secondes. Cependant, la détection des menaces a un accès de base BRI minimum de 10 secondes, donc si 1/30e de l'ARI est inférieur à 10, l'ASA utilise toujours 10 secondes comme accès de base BRI. Il est également important de noter que ce comportement était différent dans les versions antérieures à 8.2(1), qui utilisaient une valeur de

1/60e de l'ARI, au lieu de 1/30e. L'intervalle de base minimal de 10 secondes est le même pour toutes les versions de logiciels.

Lorsqu'une menace de base est détectée, l'ASA génère simplement le syslog %ASA-4-733100 pour avertir l'administrateur qu'une menace potentielle a été identifiée. La commande show threat-detection rate permet d'afficher le nombre moyen, actuel et total d'événements pour chaque catégorie de menace. Le nombre total d'événements cumulés est la somme du nombre d'événements observés dans les 30 derniers échantillons BRI.

Le débit en rafale dans Syslog est calculé en fonction du nombre de paquets abandonnés jusqu'à présent dans l'accès de base de données actuel. Le calcul est effectué périodiquement dans un BRI. Dès qu'une attaque se produit, un syslog est généré. Il est limité qu'un seul syslog soit généré dans un BRI. Le débit de rafale dans « show threat-detection rate » est calculé en fonction du nombre de paquets abandonnés dans la dernière BRI. La différence réside dans le fait que syslog est sensible au temps. Par conséquent, si une attaque survient dans l'accès de base de données actuel, elle aura une chance d'être capturée. « show threat-detection rate » étant moins sensible au temps, le numéro du dernier BRI est utilisé.

La détection de base des menaces ne prend aucune mesure pour arrêter le trafic déviant ou empêcher de futures attaques. En ce sens, la détection des menaces de base est purement informative et peut être utilisée comme mécanisme de surveillance ou de signalement.

Détection avancée des menaces (statistiques de niveau objet et N premiers)

Contrairement à Basic Threat Detection, Advanced Threat Detection peut être utilisé pour suivre les statistiques d'objets plus granulaires. L'ASA prend en charge les statistiques de suivi pour les adresses IP hôtes, les ports, les protocoles, les listes de contrôle d'accès et les serveurs protégés par l'interception TCP. La détection avancée des menaces est activée par défaut uniquement pour les statistiques ACL.

Pour les objets d'hôte, de port et de protocole, Threat Detection conserve la trace du nombre de paquets, d'octets et de suppressions qui ont été envoyés et reçus par cet objet au cours d'une période spécifique. Pour les listes de contrôle d'accès, Threat Detection conserve une trace des 10 entrées ACE (permit et deny) qui ont été le plus touchées au cours d'une période spécifique.

Les périodes suivies dans tous ces cas sont de 20 minutes, 1 heure, 8 heures et 24 heures. Bien que les périodes elles-mêmes ne soient pas configurables, le nombre de périodes suivies par objet peut être ajusté à l'aide du mot clé « number-of-rate ». Consultez la section Configuration pour plus d'informations. Par exemple, si « number-of-rate » est défini sur 2, toutes les statistiques sont affichées pour 20 minutes, 1 heure et 8 heures. Si « number-of-rate » est défini sur 1, toutes les statistiques sont affichées pour 20 minutes, 1 heure. Quoi qu'il en soit, le débit de 20 minutes est toujours affiché.

Lorsque l'interception TCP est activée, Threat Detection peut effectuer le suivi des 10 principaux serveurs considérés comme étant attaqués et protégés par l'interception TCP. Les statistiques relatives à l'interception TCP sont similaires à celles de la détection de menace de base, dans le sens où l'utilisateur peut configurer l'intervalle de débit mesuré ainsi que les débits moyens (ARI) et en rafale (BRI) spécifiques. Les statistiques de détection avancée des menaces pour

l'interception TCP sont uniquement disponibles dans ASA 8.0(4) et versions ultérieures.

Les statistiques de détection avancée des menaces sont affichées via les commandes show threat-detection statistics et show threat-detection statistics top. Il s'agit également de la fonctionnalité responsable de la mise en place des graphiques « supérieurs » sur le tableau de bord du pare-feu de l'ASDM. Les seuls syslog qui sont générés par la détection avancée des menaces sont %ASA-4-733104 et %ASA-4-733105, qui sont déclenchés lorsque les taux moyen et de rafale (respectivement) sont dépassés pour les statistiques d'interception TCP.

Tout comme la détection de base des menaces, la détection avancée des menaces est purement informative. Aucune action n'est entreprise pour bloquer le trafic en fonction des statistiques Advanced Threat Detection.

Analyse de la détection des menaces

L'analyse de la détection des menaces permet de suivre les pirates présumés qui créent des connexions avec un trop grand nombre d'hôtes dans un sous-réseau ou de ports sur un hôte/sous-réseau. L'analyse de la détection des menaces est désactivée par défaut.

L'analyse de la détection des menaces s'appuie sur le concept de détection de base des menaces, qui définit déjà une catégorie de menace pour une attaque d'analyse. Par conséquent, les paramètres rate-interval, average rate (ARI) et burst rate (BRI) sont partagés entre Basic et Scanning Threat Detection. La différence entre les deux fonctions est que, tandis que la détection de menaces de base indique uniquement que les seuils de débit moyen ou de débit en rafale ont été dépassés, la détection de menaces d'analyse tient à jour une base de données d'adresses IP d'attaquant et de cible qui peut aider à fournir plus de contexte autour des hôtes impliqués dans l'analyse. En outre, seul le trafic réellement reçu par l’hôte/sous-réseau cible est pris en compte par la détection des menaces d’analyse. La fonction Basic Threat Detection peut toujours déclencher une menace d'analyse même si le trafic est abandonné par une liste de contrôle d'accès.

L'analyse de la détection des menaces peut éventuellement réagir à une attaque en ignorant l'adresse IP de l'attaquant. Cela fait de l'analyse de la détection des menaces le seul sous-ensemble de la fonctionnalité de détection des menaces qui peut affecter activement les connexions via l'ASA.

Lorsque l'analyse de la détection des menaces détecte une attaque, %ASA-4-733101 est consigné pour les adresses IP de l'attaquant et/ou de la cible. Si la fonctionnalité est configurée pour éviter l'attaquant, %ASA-4-733102 est consigné lorsque la détection des menaces d'analyse génère un arrêt. %ASA-4-733103 est consigné lorsque le shun est supprimé. La commande show threat-detection scan-threat peut être utilisée afin d'afficher l'ensemble de la base de données Scanning Threat.

Limites

- La détection des menaces n'est disponible que dans ASA 8.0(2) et versions ultérieures. Elle n'est pas prise en charge sur la plate-forme ASA 1000V.

- La détection des menaces n'est prise en charge qu'en mode contextuel unique.
- Seules les menaces prêtes à l'emploi sont détectées. Le trafic envoyé à l'ASA lui-même n'est pas pris en compte par la détection des menaces.
- Les tentatives de connexion TCP réinitialisées par le serveur cible ne sont pas comptabilisées comme une attaque SYN ou une menace d'analyse.

Configuration

Détection des menaces de base

La détection des menaces de base est activée à l'aide de la commande threat-detection basic-threat.

```
<#root>

ciscoasa(config)#

threat-detection basic-threat
```

Les taux par défaut peuvent être affichés avec la commande show run all threat-detection.

```
<#root>

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'ajuster ces taux avec des valeurs personnalisées, il suffit de reconfigurer la commande

threat-detection rate pour la catégorie de menace appropriée.

<#root>

```
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 taux différents définis (avec des ID de taux de 1, 2 et 3). L'ID de débit particulier qui est dépassé est référencé dans le syslog %ASA-4-733100.

Dans l'exemple précédent, la détection des menaces crée syslog 733100 uniquement lorsque le nombre de pertes de listes de contrôle d'accès dépasse 250 pertes/seconde sur 1200 secondes ou 550 pertes/seconde sur 40 secondes.

Détection avancée des menaces

Utilisez la commande threat-detection statistics afin d'activer la détection avancée des menaces. Si aucun mot-clé de fonction spécifique n'est fourni, la commande active le suivi pour toutes les statistiques.

<#root>

```
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 suivis pour les statistiques d'hôte, de port, de protocole ou de liste de contrôle d'accès, utilisez le mot clé number-of-rate.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics host number-of-rate 2

Le mot clé number-of-rate configure Threat Detection pour suivre uniquement le plus court n nombre d'intervalles.

Afin d'activer les statistiques d'interception TCP, utilisez la commande threat-detection statistics tcp-intercept.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept
```

Afin de configurer des débits personnalisés pour les statistiques d'interception TCP, utilisez les mots clés rate-interval, average-rate et burst-rate.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

Analyse de la détection des menaces

Afin d'activer l'analyse de la détection des menaces, utilisez la commande threat-detection scan-threat.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat
```

Afin d'ajuster les taux pour une menace d'analyse, utilisez la même commande threat-detection rate utilisée par Basic Threat Detection.

```
<#root>

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

Afin de permettre à l'ASA de bouder un IP attaquant d'analyse, ajoutez le mot clé shun à la commande threat-detection scan-threat.

<#root>

```
ciscoasa(config)#
```

threat-detection scanning-threat shun

Cela permet à l'analyse de la détection des menaces de créer un shun d'une heure pour le pirate. Afin d'ajuster la durée du shun, utilisez la commande threat-detection scan-threat shun duration.

<#root>

```
ciscoasa(config)#
```

threat-detection scanning-threat shun duration 1000

Dans certains cas, vous pouvez empêcher l'ASA de bouder certaines adresses IP. Pour ce faire, créez une exception avec la commande threat-detection scan-threat shun exclude.

<#root>

```
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

rendement

La détection des menaces de base a très peu d'impact sur les performances de l'ASA. Les fonctions avancées et d'analyse de la détection des menaces sont beaucoup plus gourmandes en ressources, car elles doivent assurer le suivi de diverses statistiques en mémoire. Seule la détection des menaces par analyse avec la fonction shun activée peut avoir un impact actif sur le trafic qui aurait autrement été autorisé.

À mesure que les versions du logiciel ASA ont progressé, l'utilisation de la mémoire de Threat Detection a été considérablement optimisée. Cependant, vous devez veiller à surveiller l'utilisation de la mémoire de l'ASA avant et après l'activation de la détection des menaces. Dans certains cas, il serait préférable de n'activer que certaines statistiques (par exemple, les statistiques d'hôte) temporairement pendant que vous dépannez activement un problème spécifique.

Pour obtenir une vue plus détaillée de l'utilisation de la mémoire Threat Detection, exécutez la commande show memory app-cache threat-detection [detail].

Actions recommandées

Ces sections fournissent des recommandations générales sur les mesures à prendre en cas d'événements liés à la détection des menaces.

Lorsqu'un taux d'abandon de base est dépassé et que %ASA-4-733100 est généré

Déterminez la catégorie de menace spécifique mentionnée dans le syslog %ASA-4-733100 et établissez une corrélation avec le résultat de `show threat-detection rate` . Avec ces informations, vérifiez le résultat de `show asp drop` afin de déterminer les raisons pour lesquelles le trafic est abandonné.

Pour obtenir une vue plus détaillée du trafic abandonné pour une raison spécifique, utilisez une capture d'abandon ASP avec la raison en question afin de voir tous les paquets qui sont abandonnés. Par exemple, si les menaces de suppression de liste de contrôle d'accès sont consignées, la capture sur la raison de suppression ASP de `acl-drop` :

```
<#root>

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 montre que le paquet abandonné est un paquet UDP/53 de 10.10.10.10 à 192.168.1.100.

Si %ASA-4-733100 signale une menace d'analyse, il peut également s'avérer utile d'activer temporairement la détection des menaces d'analyse. Cela permet à l'ASA de suivre les adresses IP source et de destination impliquées dans l'attaque.

Étant donné que Basic Threat Detection surveille principalement le trafic qui est déjà abandonné par l'ASP, aucune action directe n'est requise pour arrêter une menace potentielle. Les exceptions à cette règle sont les attaques SYN et les menaces d'analyse, qui impliquent le trafic qui passe par l'ASA.

Si les abandons observés dans la capture d'abandon ASP sont légitimes et/ou attendus pour l'environnement réseau, réglez les intervalles de débit de base sur une valeur plus appropriée.

Si les abandons indiquent un trafic illégitime, des actions doivent être entreprises pour bloquer ou limiter le débit du trafic avant qu'il n'atteigne l'ASA. Cela peut inclure les ACL et la QoS sur les périphériques en amont.

Pour les attaques SYN, le trafic peut être bloqué dans une ACL sur l'ASA. L'interception TCP peut également être configurée pour protéger le ou les serveurs ciblés, mais cela peut simplement entraîner une menace de limite de connexion qui est consignée à la place.

Pour l'analyse des menaces, le trafic peut également être bloqué dans une liste de contrôle d'accès sur l'ASA. Analyse de la détection des menaces avec shunpeut être activée pour permettre à l'ASA de bloquer proactivement tous les paquets provenant de l'attaquant pendant une période définie.

Lorsqu'une menace d'analyse est détectée et que %ASA-4-733101 est consigné

%ASA-4-733101 doit répertorier l'hôte/sous-réseau cible ou l'adresse IP du pirate. Pour obtenir la liste complète des cibles et des agresseurs, consultez le résultat de show threat-detection scanning-threat.

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

Si l'analyse détectée n'est pas attendue, des actions doivent être entreprises pour bloquer ou limiter le débit du trafic avant qu'il n'atteigne l'ASA. Cela peut inclure les ACL et la QoS sur les périphériques en amont. Quand le shunest ajoutée à la configuration de détection des menaces d'analyse, elle peut permettre à l'ASA d'abandonner proactivement tous les paquets de l'IP de l'attaquant pendant une période définie. En dernier recours, le trafic peut également être bloqué manuellement sur l'ASA via une politique d'interception ACL ou TCP.

Si l'analyse détectée est un faux positif, réglez les intervalles du taux de menaces d'analyse sur une valeur plus appropriée pour l'environnement réseau.

Lorsqu'un pirate est exclu et que %ASA-4-733102 est consigné

%ASA-4-733102 répertorie l'adresse IP de l'attaquant ignoré. Utilisez show threat-detection shun afin d'afficher la liste complète des pirates qui ont été spécifiquement évités par Threat Detection. Utilisez show shun afin d'afficher la liste complète de toutes les adresses IP qui sont activement rejetées par l'ASA (cela inclut des sources autres que la détection des menaces).

Si le shun fait partie d'une attaque légitime, aucune autre action n'est requise. Cependant, il serait avantageux de bloquer manuellement le trafic du pirate aussi loin en amont que possible vers la source. Cela peut être effectué via les ACL et la QoS. Cela garantit que les périphériques intermédiaires n'ont pas besoin de gaspiller des ressources sur le trafic illégitime.

Si la menace d'analyse qui a déclenché le shun était un faux positif, supprimez manuellement le shun avec le clear threat-detection shun [IP_address] erasecat4000_flash:.

Lorsque %ASA-4-733104 et/ou %ASA-4-733105 est consigné

%ASA-4-733104 et %ASA-4-733105 répertorient l'hôte ciblé par l'attaque qui est actuellement protégé par TCP intercept. Pour plus d'informations sur les taux d'attaque et les serveurs protégés, consultez le résultat de show threat-detection statistics top tcp-intercept .

<#root>

```
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)
```

Lorsque l'Advanced Threat Detection détecte une attaque de cette nature, l'ASA protège déjà le serveur ciblé via l'interception TCP. Vérifiez les limites de connexion configurées afin de vous assurer qu'elles offrent une protection adéquate pour la nature et le taux de l'attaque. En outre, il serait avantageux de bloquer manuellement le trafic du pirate aussi loin en amont que possible vers la source. Cela peut être effectué via les ACL et la QoS. Cela garantit que les périphériques intermédiaires n'ont pas besoin de gaspiller des ressources sur le trafic illégitime.

Si l'attaque détectée est un faux positif, réglez les taux d'une attaque d'interception TCP sur une valeur plus appropriée avec la commande threat-detection statistics tcp-intercepterasecat4000_flash:.

Comment déclencher manuellement une menace

Pour tester et dépanner, il peut être utile de déclencher manuellement diverses menaces. Cette section contient des conseils sur la manière de déclencher quelques types de menaces courantes.

Menace de base : suppression, pare-feu et analyse des listes de contrôle d'accès

Pour déclencher une menace de base particulière, reportez-vous au tableau de la section Fonctionnalités précédente. Choisissez une raison de rejet ASP spécifique et envoyez le trafic via l'ASA qui serait abandonné par la raison de rejet ASP appropriée.

Par exemple, les menaces d'abandon de liste de contrôle d'accès, de pare-feu et d'analyse prennent toutes en compte le taux de paquets abandonnés par abandon de liste. Effectuez ces étapes afin de déclencher ces menaces simultanément :

1. Créez une liste de contrôle d'accès sur l'interface externe de l'ASA qui abandonne explicitement tous les paquets TCP envoyés à un serveur cible à 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. À partir d'un attaquant à l'extérieur de l'ASA (10.10.10.10), utilisez nmap afin d'exécuter une analyse SYN TCP sur chaque port du serveur cible :

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Remarque : T5 configure nmap pour exécuter l'analyse aussi rapidement que possible. D'après les ressources du PC pirate, ce débit n'est toujours pas assez rapide pour déclencher certains des débits par défaut. Si c'est le cas, il vous suffit de réduire les taux configurés pour la menace que vous souhaitez voir. Lorsque vous définissez les paramètres ARI et BRI sur 0, Basic Threat Detection déclenche toujours la menace, quel que soit le taux.

---

3. Notez que des menaces de base sont détectées pour les menaces de suppression de liste de contrôle d'accès, de pare-feu et d'analyse :

```
%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 suppression de liste de contrôle d'accès et les interfaces ARI et BRI du pare-feu ont été définies sur 0, de sorte qu'elles déclenchent toujours une menace. C'est pourquoi les débits maximum configurés sont listés comme 0.

Menace avancée - Interception TCP

1. Créez une liste de contrôle d'accès sur l'interface externe qui autorise tous les paquets TCP envoyés à un serveur cible à 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 cible n'existe pas réellement, ou s'il réinitialise les tentatives de connexion de

l'attaquant, configurez une entrée ARP factice sur l'ASA pour bloquer le trafic d'attaque par l'interface interne :

```
arp inside 10.11.11.11 dead.dead.dead
```

3. Créez une stratégie d'interception TCP simple 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
```

À partir d'un pirate à l'extérieur de l'ASA (10.10.10.10), utilisez nmap pour exécuter une analyse SYN TCP sur chaque port du serveur cible :

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Notez que Threat Detection assure le suivi du serveur protégé :

<#root>

```
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 d'analyse

1. Créez une liste de contrôle d'accès sur l'interface externe qui autorise tous les paquets TCP envoyés à un serveur cible à 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 l'analyse de la détection des menaces puisse suivre les adresses IP de la cible et de l'attaquant, le trafic doit être autorisé via l'ASA.

2. Si le serveur cible n'existe pas réellement, ou s'il réinitialise les tentatives de connexion de l'attaquant, configurez une entrée ARP factice sur l'ASA pour bloquer le trafic d'attaque par l'interface interne :

```
arp inside 10.11.11.11 dead.dead.dead
```

> Remarque : les connexions réinitialisées par le serveur cible ne sont pas comptabilisées dans la menace.

3. À partir d'un pirate à l'extérieur de l'ASA (10.10.10.10), utilisez nmap pour exécuter une analyse SYN TCP sur chaque port du serveur cible :

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> Remarque : T5 configure nmap pour exécuter l'analyse aussi rapidement que possible. D'après les ressources du PC pirate, ce débit n'est toujours pas assez rapide pour déclencher certains des débits par défaut. Si c'est le cas, il vous suffit de réduire les taux configurés pour la menace que vous souhaitez voir. Lorsque vous définissez les paramètres ARI et BRI sur 0, Basic Threat Detection déclenche toujours la menace, quel que soit le taux.

4. Notez qu'une menace d'analyse est détectée, que l'adresse IP de l'attaquant est suivie et que l'attaquant est exclu :

```
%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 des commandes ASA
- Messages Syslog Cisco Secure Firewall ASA
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.