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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Fonctionnalité de détection des menaces
  - Détection de base des menaces (taux système)
  - Détection avancée des menaces (statistiques de niveau objet et N premiers)
  - Analyse de la détection des menaces
  - Détection des menaces pour les services VPN (9.20(3)+ / catégories répertoriées)
- Limites
- Configuration
  - Détection des menaces de base
  - Détection avancée des menaces
  - Analyse de la détection des menaces
  - Détection des menaces pour les services VPN
- rendement
- Actions recommandées
  - Lorsqu'un taux d'abandon de base est dépassé et que %ASA-4-733100 est généré
  - Lorsqu'une menace d'analyse est détectée et que %ASA-4-733101 est consigné
  - Lorsqu'un pirate est exclu et que %ASA-4-733102 est consigné
  - Lorsque %ASA-4-733104 et/ou %ASA-4-733105 est consigné
  - Lorsqu'un hôte VPN est désactivé et que %ASA-4-733201 est consigné
- Comment déclencher manuellement une menace
  - Menace de base : suppression de liste de contrôle d'accès, pare-feu et analyse
  - Menace avancée — Interception TCP
  - Menace d'analyse
- Informations connexes

Introduction

Ce document décrit la fonctionnalité de détection des menaces et la configuration sur Cisco Secure Firewall ASA.

Conditions préalables

Exigences

Cisco recommande de connaître l'interface de ligne de commande ASA, le contrôle d'accès et (pour la détection des menaces VPN) le VPN d'accès à distance.

Composants utilisés

- Détection classique des menaces (de base, avancée, analyse) : Logiciel ASA 8.0(2) et versions ultérieures. Les statistiques d'interception TCP nécessitent 8.0(4) / 8.1(2) ou version ultérieure. La durée de shuntage est configurable à partir de 8.0(4) / 8.1(2).
- Détection des menaces pour les services VPN : Introduit dans le train 9.20 à 9.20(3). Cisco documente également ces minimums dans d'autres trains sous 9.16(4)67, 9.17(1)45, 9.18(4)40, 9.19(1).37 et 9.22(1.1) (9.22(1) n'a pas été publié.)

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

La détection des menaces sur ASA fournit une défense de première ligne de couche 3/4. Il établit une ligne de base à partir des statistiques de suppression de paquets et des rapports facultatifs « top » au niveau des objets. Il ne remplace pas un IPS dédié ou un module IPS de nouvelle génération, qui inspecte le trafic autorisé jusqu'à la couche 7 ; les deux peuvent travailler ensemble.



Remarque : Cet article traite de l'ensemble de fonctionnalités CLI ASA. Cisco Secure Firewall Threat Defense (FTD) présente une fonction de détection des menaces associée mais non identique dans les paramètres avancés de la stratégie de contrôle d'accès. Ne considérez pas FTD Threat Detection comme un mappage 1:1 de ces commandes. Pour plus d'informations, reportez-vous à l'article Mappage des fonctionnalités ASA à la défense contre les menaces.

La détection des menaces fournit aux administrateurs de pare-feu des outils pour identifier, comprendre et (pour l'analyse et les services VPN) arrêter les attaques. Il repose sur des déclencheurs de taux, des statistiques au niveau de l'objet et des shuns automatiques facultatifs.

Cette fonction comporte quatre composants :

1. Basic Threat Detection (taux d'abandon au niveau du système) : activé par défaut
2. Advanced Threat Detection (statistiques de niveau objet et N premiers) — Statistiques de liste de contrôle d'accès activées par défaut
3. Analyse de la détection des menaces (base de données du pirate/cible, shun facultatif) : désactivée par défaut
4. Threat Detection for VPN Services (RA VPN DoS protection, automatic shun) : désactivé par défaut ; 9.20(3)+ / trains répertoriés

---

Fonctionnalité de détection des menaces

Détection de base des menaces (taux système)

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

Il surveille les débits auxquels les paquets sont abandonnés pour diverses raisons par l'ASA dans son ensemble. Les statistiques s'appliquent à l'ensemble de l'appliance et ne sont généralement pas assez granulaires pour identifier l'hôte source. L'ASA surveille les paquets abandonnés pour ces événements :

- ACL Drop (acl-drop) : paquets refusés par les listes d'accès.
- Paquets incorrects (bad-packet-drop) : Formats de paquets non valides, y compris les en-têtes L3 et L4 qui ne sont pas conformes aux normes RFC (par exemple, invalid-ip-header ou invalid-tcp-hdr-length).
- Limite conn (conn-limit-drop) : Paquets qui dépassent une limite de connexion configurée ou globale.
- Attaque DoS (dos-drop) : Attaques par déni de service (par exemple, échec de vérification de SPI ou de pare-feu dynamique non valide.)
- Pare-feu (fw-drop) : Taux combiné de pertes liées au pare-feu dans cette liste. Il n'inclut pas les abandons non pare-feu tels que la surcharge d'interface, les échecs d'inspection ou les attaques par analyse détectées.
- Attaque ICMP (icmp-drop) : Paquets ICMP suspects.
- Inspect (inspect-drop) : Refus par contrôle d'application.
- Interface (interface-drop) : Paquets ignorés par les vérifications d’interface (surcharge).

- Analyse (menace d'analyse) : Attaques d’analyse réseau/hôte (par exemple, le premier paquet TCP n’est pas SYN ou la connexion en trois étapes a échoué). La détection complète des menaces par analyse utilise ce taux pour classer les hôtes et, éventuellement, les réfuter.
- Attaque SYN (syn-attack) : Attaques de session incomplètes, y compris les attaques TCP SYN et les sessions UDP unidirectionnelles sans données de retour.

La plupart des déclencheurs correspondent à des motifs de rejet ASP spécifiques ; certains syslogs et certaines actions d'inspection sont également comptabilisés. Certains déclencheurs apparaissent dans plusieurs catégories de menaces. Mappages communs (liste non 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 de base des menaces mesure les taux de chute sur un intervalle de taux moyen configuré (ARI), de 600 secondes à 30 jours. Si les événements de l'ARI dépassent les seuils configurés, l'ASA les traite comme une menace.

Il existe deux seuils : débit moyen et débit en rafale. Le débit moyen est de 400 baisses par seconde sur l'ARI. Le débit en rafale utilise un intervalle de débit en rafale (BRI) plus court. Depuis la version 8.2(1), BRI est 1/30e de l'ARI, ou 10 secondes, selon la valeur la plus élevée. Avant la version 8.2(1), l'accès de base était 1/60e de l'IRA. La durée minimale de 10 secondes s'applique à toutes les versions logicielles.

Exemple : Un taux moyen de perte de liste de contrôle d'accès de 400 avec ARI 600 secondes signifie que l'ASA fait la moyenne des pertes de liste de contrôle d'accès au cours des 600 dernières secondes et consigne une menace si cette moyenne dépasse 400 par seconde. Le débit en rafale 800 avec le même ARI utilise un BRI de 20 secondes (600 / 30). Si la liste de contrôle d’accès abandonne dans cette fenêtre de 20 secondes et dépasse 800 par seconde, une menace est consignée.

Lorsqu'une menace de base est détectée, l'ASA génère le syslog %ASA-4-733100. Si les débits moyen et en rafale sont dépassés, l'ASA peut envoyer deux messages 733100 (un par type de débit), avec un maximum d'un message par type de débit par période de rafale.

Exécutez la commande show threat-detection rate pour afficher les événements moyens, actuels, du nombre de déclencheurs et du total. L'ASA stocke le nombre à la fin de chaque période de rafale pour 30 accès de base terminés. L'accès de base actuel inachevé est normalement exclu de la moyenne. Le nombre total d'événements est la somme des événements de ces 30 échantillons BRI (avec une exception en temps réel si l'échantillon BRI non terminé dépasse déjà l'échantillon le plus ancien).

La vitesse de rafale dans le syslog est calculée à partir des pertes jusqu'à présent dans l'accès de base de données actuel, échantillonnées périodiquement, de sorte qu'une brèche peut être signalée avant la fin de l'accès de base de données (un syslog par type de débit par accès de base de données). Le débit en rafale/actuel dans show threat-detection rate utilise le dernier BRI terminé.

La détection de base des menaces ne supprime pas le trafic. Il est informatif (surveillance et rapports). L'impact sur les performances est négligeable et se produit principalement en cas de pertes ou de menaces potentielles.

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

La détection avancée des menaces suit les statistiques d'objets plus granulaires : IP hôte, ports, protocoles, listes de contrôle d’accès et serveurs protégés par TCP Intercept. Seules les statistiques ACL sont activées par défaut. Les statistiques des hôtes ont un impact significatif sur les performances en cas de trafic élevé ; activez-les temporairement lorsque vous en avez besoin. Les statistiques portuaires ont un impact plus modeste.

Pour les objets d'hôte, de port et de protocole, l'ASA suit les paquets, les octets et les abandons envoyés et reçus dans des fenêtres fixes. Pour les listes de contrôle d’accès, il suit les 10 premières entrées ACE (autoriser et refuser) dans ces fenêtres. Les occurrences ACE autorisées et refusées ne sont pas différenciées dans l'affichage de la liste de contrôle d'accès supérieure.

Les fenêtres fixes sont de 20 minutes, 1 heure, 8 heures et 24 heures. Les fenêtres elles-mêmes ne sont pas configurables. Le nombre de débits {1} | 2 Le mot clé | 3} (hôte, port et protocole uniquement) contrôle le nombre d'intervalles plus longs conservés :

- 1 (valeur par défaut) : seul l'intervalle de débit le plus court permet de limiter l'utilisation de la mémoire
- 2 — les deux intervalles les plus courts
- 3 à 1 heure, 8 heures et 24 heures

Les statistiques d'hôte s'accumulent lorsque l'hôte est actif dans la base de données hôte des menaces d'analyse et sont effacées après 10 minutes d'inactivité.

Lorsque l'interception TCP est activée, la détection des menaces peut suivre les 10 principaux serveurs attaqués. Les statistiques d'interception TCP utilisent une fenêtre de surveillance configurable plus des seuils de moyenne et de rafale (disponibles dans 8.0(4) et versions ultérieures). Par défaut :

- Intervalle de débit (fenêtre d'historique) : 30 minutes (plage 1-1440). L'ASA échantillonne 30 fois au cours de la fenêtre (toutes les 60 secondes par défaut).
- Taux de rafale : 400 attaques/s — syslog %ASA-4-733104
- Taux moyen : 200 attaques/s — syslog %ASA-4-733105

Affichez les statistiques en exécutant les commandes show threat-detection statistics et show threat-détection statistics top. Il s'agit également de la fonctionnalité qui a renseigné les graphiques supérieurs sur le tableau de bord classique du pare-feu ASDM.

La détection avancée des menaces est informative, sauf que TCP Intercept protège déjà le serveur. Aucun bloc supplémentaire n'est appliqué à partir de ces seules statistiques.

Analyse de la détection des menaces

L'analyse de la détection des menaces permet de suivre les hôtes qui créent des connexions sur un trop grand nombre d'hôtes dans un sous-réseau ou sur un trop grand nombre de ports sur un hôte ou un sous-réseau. Elle est désactivée par défaut. Contrairement à la détection d'analyse basée sur les signatures IPS, la détection des menaces d'analyse ASA gère une base de données hôte (connexions sans activité de retour, accès à port fermé, certains comportements TCP, etc.).

Il partage les taux ARI (rate-interval), BRI (average rate) et BRI (burst rate) avec la catégorie de menace d'analyse de base. Vous ne pouvez pas configurer des débits distincts pour l'analyse de base et l'analyse. La différence réside dans la détection des menaces par analyse qui permet de conserver une base de données IP cible et attaquante. Seul le trafic autorisé via l'ASA et créant un flux est compté. La détection des menaces de base peut toujours déclencher une menace d'analyse 733100 pour le trafic ACL refusé ; l'analyse de la détection des menaces ne fonctionne pas.

Si la vitesse d'analyse du trafic provenant d'un hôte est dépassée, cet hôte est un attaquant. S’il est dépassé pour le trafic vers un hôte, cet hôte est une cible. Le journal système %ASA-4-733101 est consigné. Vous pouvez éventuellement désactiver le pirate (%ASA-4-733102 lorsque le shun est ajouté, %ASA-4-733103 lorsqu'il est supprimé). La durée de shuntage par défaut est

de 3 600 secondes (1 heure), configurable de 10 à 2592000 secondes.

L'analyse de la détection des menaces avec shun est l'une des deux fonctionnalités qui peuvent activement abandonner le trafic autorisé par ailleurs (l'autre est la détection des menaces VPN).

Exécutez la commande show threat-detection scan-threat pour la base de données de l'attaquant/cible et show threat-detection shun pour les shuns d'analyse des menaces uniquement.



Remarque : Exempter les hôtes qui envoient un trafic de multidiffusion ou de plan de contrôle légitime élevé (par exemple des routeurs PIM) avec détection de menace analyse-menace shun sauf, ou ces paquets peuvent être abandonnés lorsqu'un shun est installé.

Détection des menaces pour les services VPN (9.20(3)+ / catégories répertoriées)

La détection des menaces VPN protège la tête de réseau VPN d'accès à distance ASA contre les attaques de type DoS IPv4. Les trois services sont désactivés par défaut. Lorsqu'un service est activé et qu'un hôte dépasse son seuil, l'ASA ferme automatiquement cette adresse IPv4 jusqu'à ce que vous supprimiez le shun.

Services :

- remote-access-authentication : Échecs de connexion VPN RA consécutifs (pulvérisation de mot de passe / force brute). Maintien en position basse pendant 1 à 140 minutes ; threshold 1-100. Les échecs d'authentification SAML ne sont pas comptés.
- remote-access-client-initiations : Démarrage d'une connexion SSL/IKEv2 répétée qui ne se termine pas à partir d'un hôte. Maintien en position basse pendant 1 à 140 minutes ; seuil 5-100.
- invalid-vpn-access : tente d'atteindre des groupes de tunnels intégrés qui existent uniquement pour le fonctionnement des périphériques internes. Une adresse IPv4 correspondante est immédiatement mise hors service (retenue/seuil effectif de 1/1).

Ces attaques peuvent consommer des ressources d'authentification et de session même en cas d'échec. Lorsque vous définissez le gel et le seuil, tenez compte de la PAT (hôtels, CGNAT) : de nombreux utilisateurs valides peuvent partager une adresse IP publique. Utilisez des valeurs plus élevées pour que les utilisateurs légitimes puissent terminer de se connecter.

La détection des menaces VPN surveille IPv4 prêt à l'emploi uniquement. Les shuns apparaissent dans show shun, pas dans show threat-detection shun. Syslogs associés : %ASA-6-733200 (info) et %ASA-4-733201 (seuil dépassé ; shun installé.)

Limites

- La détection classique des menaces nécessite ASA 8.0(2) ou version ultérieure. L'ancienne plate-forme ASA 1000V ne prenait pas en charge cette fonctionnalité (cette plate-forme est en fin de vie).
- Contexte de sécurité : À l'exception des statistiques avancées sur les menaces et des services VPN, la détection des menaces est prise en charge en mode de contexte unique uniquement. En mode de contexte multiple, les statistiques TCP Intercept sont les statistiques avancées prises en charge. La détection des menaces VPN est également prise en charge en mode multiple.
- Mode pare-feu : Pris en charge en mode routé et transparent.
- Pour les statistiques de base, avancées et d'analyse, seul le trafic prêt à l'emploi est surveillé. Le trafic envoyé à l'ASA elle-même n'est pas compté.
- Pour les services VPN, seul le protocole IPv4 prêt à l'emploi est surveillé.
- Le trafic refusé par une liste de contrôle d'accès ne déclenche pas la détection des menaces d'analyse (suivi des attaquants/cibles). Les taux de menaces d'analyse de base peuvent augmenter sur les abandons ACL.
- Les tentatives de connexion TCP réinitialisées par le serveur cible ne sont pas comptabilisées comme une attaque SYN ou une menace d'analyse.
- La détection des échecs d'authentification VPN n'inclut pas les échecs SAML.

Configuration

Détection des menaces de base

La détection des menaces de base est activée par défaut. Vous pouvez la réactiver avec :

<#root>

```
ciscoasa(config)#

threat-detection basic-threat
```

Désactivez sans détection de menace de base. Affichage des taux par défaut avec 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
```

Réglez une catégorie en exécutant la commande threat-detection rate. Chaque catégorie peut avoir jusqu'à trois taux (taux 1, 2 et 3). L'ID de débit qui a été dépassé est référencé dans 733100 :

<#root>

```
ciscoasa(config)#
```

threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550

Dans cet exemple, 733100 est généré lorsque les abandons de liste de contrôle d'accès dépassent 250/sec sur 1200 secondes ou 550/sec sur 40 secondes (1200 / 30.)

Le mot clé scan-threat dans cette commande est partagé avec la détection de menace d'analyse. Vous pouvez définir des taux d'analyse même si la détection des menaces de base est désactivée.

Détection avancée des menaces

Exécutez la commande threat-detection statistics pour activer les statistiques avancées. En l'absence de mot clé, tous les types de statistiques sont activés :

<#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>
```

---

no threat-detection statistics (no options) supprime toutes les commandes statistics, y compris la liste d'accès default threat-detection statistics.

Statistiques ACL (par défaut) :

<#root>

```
ciscoasa(config)#

threat-detection statistics access-list
```

Hôte, port ou protocole, avec un nombre facultatif d'intervalles de débit :

<#root>

```
ciscoasa(config)#

threat-detection statistics host number-of-rate 2

ciscoasa(config)#

threat-detection statistics port number-of-rate 2
```

```
ciscoasa(config)#
threat-detection statistics protocol number-of-rate 3
```

Statistiques d'interception TCP (également disponibles en mode de contexte multiple) :

<#root>

```
ciscoasa(config)#
threat-detection statistics tcp-intercept
ciscoasa(config)#
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
```

Analyse de la détection des menaces

<#root>

```
ciscoasa(config)#
threat-detection scanning-threat
ciscoasa(config)#
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
ciscoasa(config)#
threat-detection scanning-threat shun
ciscoasa(config)#
threat-detection scanning-threat shun duration 1000
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
```

Vous pouvez combiner shun et sauf sur une ligne, et entrer la commande plusieurs fois pour exempter plus d'adresses ou de groupes d'objets.

<#root>

```
ciscoasa(config)#

threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
```

Détection des menaces pour les services VPN

<#root>

```
ciscoasa(config)#

threat-detection service invalid-vpn-access

ciscoasa(config)#

threat-detection service remote-access-client-initiations hold-down 10 threshold 20

ciscoasa(config)#

threat-detection service remote-access-authentication hold-down 10 threshold 20
```

Désactivez un service avec la forme no de la même commande. Réinitialisez les compteurs avec le service de détection claire des menaces.

Pour une procédure pas à pas dédiée, référez-vous à Configurer la détection des menaces pour les services VPN d'accès à distance sur le pare-feu ASA sécurisé (ID de document 222315.)

rendement

La détection de base des menaces a très peu d'impact sur les performances. Les statistiques avancées sur les hôtes et la détection des menaces d'analyse sollicitent davantage les ressources, car elles stockent des données par hôte et par objet. Activez temporairement les

statistiques d'hôte pendant que vous dépannez un problème spécifique.

Fonctionnalités permettant d'abandonner le trafic autorisé par ailleurs :

- Analyse de la détection des menaces avec shun
- Services de détection des menaces VPN (désactivation automatique)

Surveillez la mémoire avant et après l'activation des fonctions avancées ou d'analyse :

<#root>

```
ciscoasa#

show threat-detection memory

ciscoasa#

show memory app-cache threat-detection detail
```

---

show threat-detection memory (8.3(1)+) est la commande documentée pour advanced-statistics memory. show memory app-cache threat-detection [detail] affiche le cache de blocs d'applications.

Actions recommandées

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

Notez la catégorie de menace dans 733100 et établissez une corrélation avec show threat-detection rate. Vérifiez ensuite show asp drop pour les raisons de la suppression.

Pour une raison spécifique, utilisez la capture ASP-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
```

Cet exemple est un paquet UDP/53 de 10.10.10.10 à 192.168.1.100.

Si 733100 signale Analyse, activez temporairement l'analyse de la détection des menaces afin que l'ASA puisse enregistrer les adresses IP des hackers et des cibles.

La détection de menaces de base compte principalement le trafic que l'ASP a déjà abandonné, donc aucune action supplémentaire d'abandon n'est requise. Les exceptions sont les attaques SYN et les menaces d'analyse qui impliquent le trafic qui passe par l'ASA.

Si les pertes sont légitimes pour l'environnement, augmentez les intervalles de débit de base. S'il s'agit d'un trafic d'attaque, bloquez ou limitez le débit en amont (ACL, QoS) avant l'ASA.

Pour les attaques SYN, refusez la source dans une liste de contrôle d’accès ou activez TCP Intercept pour protéger la cible (qui peut produire une menace conn-limit à la place). Pour l'analyse, vous pouvez refuser dans une ACL ou activer la détection de menace d'analyse avec shun.

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

733101 répertorie l’hôte/sous-réseau cible ou le pirate. Pour les listes complètes, exécutez la commande show threat-detection scan-threat.

Les captures effectuées sur les interfaces en face de l'attaquant et de la cible permettent de confirmer l'analyse.

Si l'analyse est inattendue, bloquez ou limitez le débit en amont. L'ajout de shun permet à l'ASA d'abandonner tous les paquets de l'attaquant pendant la durée configurée. En dernier recours, bloquez l'ASA avec une liste de contrôle d'accès ou une interception TCP.

S'il s'agit d'un faux positif, augmentez les intervalles de fréquence des menaces d'analyse.

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

733102 répertorie la cible de shuntage des menaces d'analyse. Exécutez la commande show threat-detection shun uniquement pour les shuns d'analyse des menaces. Exécutez show shun pour chaque shun actif sur l'ASA (analyse, détection des menaces VPN et shun manuel.)

Pour une attaque réelle, bloquez également le plus en amont possible, afin que les périphériques intermédiaires ne traitent pas le trafic. Pour les faux positifs, supprimez la shun d'analyse :

<#root>

```
ciscoasa#

clear threat-detection shun

ciscoasa#

clear threat-detection shun 10.1.1.6
```

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

Ces syslogs nomment un hôte déjà protégé par TCP Intercept. 733104 est le débit en rafale ; 733105 est le taux moyen. Vérifier :

<#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)
```

Vérifiez que les limites de connexion sont adéquates. Bloquez l'attaquant en amont si possible. Pour un faux positif, ajustez les taux tcp-intercept des statistiques de détection des menaces.

Lorsqu'un hôte VPN est désactivé et que %ASA-4-733201 est consigné

733201 nomme le service et l'homologue qui a dépassé le seuil. Confirmer avec :

<#root>

```
ciscoasa#

show threat-detection service

ciscoasa#

show threat-detection service remote-access-authentication details

ciscoasa#

show shun
```

Les adresses IP qui ont été désactivées sont retirées de la liste des entrées de service ; le compteur de blocage s'incrémente. Si l'hôte est légitime (PAT partagée, client mal configuré), supprimez le shun :

<#root>

```
ciscoasa#

no shun 192.168.100.101

ciscoasa#

no shun 192.168.100.101 interface outside
```

Si l'adresse est shuntée sur plus d'une interface et que vous omettez l'interface, no shun supprime le shun d'une seule interface seulement (route-lookup). Spécifiez l'interface pour effacer les interfaces supplémentaires ; clear shun supprime toutes les shuns sur toutes les interfaces.

N'exécutez pas clear threat-detection shun pour les shuns VPN ; cette commande s'applique uniquement à l'analyse des détections de menaces.

Si des utilisateurs valides sont rejetés, augmentez le seuil de mise hors service (en particulier

derrière PAT) ou désactivez le service jusqu'à ce que vous l'ayez réglé.

Comment déclencher manuellement une menace

Utilisez ces méthodes de TP pour tester et dépanner. Les exécuter uniquement dans un environnement isolé.

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

Les catégories de base Abandon ACL, Pare-feu et Analyse prennent toutes en compte l'abandon ACL. Pour les déclencher ensemble :

---

1. Créez une liste de contrôle d’accès sur l’interface externe refusant le protocole TCP à une cible interne (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 pirate externe (10.10.10.10), exécutez une analyse TCP SYN :

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



Remarque : T5 exécute nmap aussi vite que possible. Le PC pirate peut être encore trop lent pour les taux par défaut. Réduisez les taux configurés pour la catégorie que vous souhaitez afficher. Si vous définissez ARI et BRI sur 0, la détection de base des menaces se déclenche, quel que soit le débit.

---

3. Les menaces de base sont consignées, par exemple :

```
%ASA-4-733100: [ 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-4-733100: [ 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-4-733100: [ 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, ACL-drop et Firewall ARI/BRI ont été définis sur 0, de sorte qu'ils se déclenchent toujours (les débits maximum configurés sont 0).

Menace avancée — Interception TCP

1. Autorisez le protocole TCP vers la cible interne :

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

---

2. Si la cible n'existe pas ou réinitialise les connexions, blackhole avec une entrée ARP statique :

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

---

3. Créez une stratégie TCP Intercept (embryonic/conn limit) simple :

```
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 du pirate, analysez :

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

<#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)
```

Menace d'analyse

1. Autorisez le protocole TCP vers la cible (analyse des pistes de détection des menaces uniquement, flux créés et autorisés) :

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

---

2. Si nécessaire, trou noir avec ARP statique. Les connexions réinitialisées par un serveur réel ne sont pas comptées.

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

---

3. Analyser à partir du pirate. Réduisez les débits ou définissez ARI/BRI sur 0 si nmap n'est pas assez rapide.

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

---

4. Journaux attendus lorsque le shun est activé :

```
%ASA-4-733100: [ 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 CLI du pare-feu ASA de Cisco Secure Firewall, 9.20 — Threat Detection (également publié le 23/9.24)
- Configurer la détection des menaces pour les services VPN d'accès à distance sur le pare-feu ASA sécurisé (ID de document 222315)
- Référence des commandes ASA — commandes de détection des menaces
- Référence des commandes ASA — Commandes show threat-detection
- Messages Syslog Cisco Secure Firewall ASA (733100-733105, 733200-733201)
- Mappage des fonctionnalités ASA et de défense contre les menaces - Détection des menaces
- 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.