Determinación de la configuración y funcionalidad de detección de amenazas ASA

Contenido

Introducción

Este documento describe los tres componentes principales de la funcionalidad y configuración de detección de amenazas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de

entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe la funcionalidad y la configuración básica de la función de detección de amenazas de Cisco Adaptive Security Appliance (ASA). La detección de amenazas proporciona a los administradores de firewall las herramientas necesarias para identificar, comprender y detener los ataques antes de que lleguen a la infraestructura de red interna. Para hacerlo, la función depende de varios desencadenantes y estadísticas diferentes, que se describen con más detalle en estas secciones.

La detección de amenazas se puede utilizar en cualquier firewall ASA que ejecute una versión de software de la versión 8.0(2) o posterior. Aunque la detección de amenazas no sustituye a una solución IDS/IPS dedicada, se puede utilizar en entornos en los que un IPS no está disponible para proporcionar una capa adicional de protección a la funcionalidad principal de ASA.

Funcionalidad de detección de amenazas

La función de detección de amenazas tiene tres componentes principales:

1. Detección básica de amenazas
2. Detección de amenazas avanzadas
3. Detección de amenazas

Cada uno de estos componentes se describe con detalle en estas secciones.

Detección básica de amenazas (tasas de nivel de sistema)

La detección básica de amenazas se habilita de forma predeterminada en todos los ASA que ejecutan 8.0(2) y versiones posteriores.

La detección básica de amenazas supervisa las velocidades a las que ASA, en su conjunto, descarta paquetes por diversos motivos. Esto significa que las estadísticas generadas por la detección básica de amenazas solo se aplican a todo el dispositivo y, por lo general, no son lo suficientemente granulares como para proporcionar información sobre el origen o la naturaleza específica de la amenaza. En su lugar, ASA monitorea los paquetes descartados para detectar estos eventos:

- ACL Drop (acl-drop): las listas de acceso deniegan los paquetes.
- Paquetes incorrectos (paquetes descartados erróneos): formatos de paquete no válidos, que incluyen encabezados L3 y L4 que no cumplen los estándares RFC.
- Límite de conexión (conn-limit-drop): paquetes que exceden un límite de conexión configurado o global.
- Ataque DoS (eliminación de dos): ataques de denegación de servicio (DoS).
- Firewall (fw-drop): comprobaciones básicas de seguridad del firewall.
- ICMP Attack (icmp-drop): paquetes ICMP sospechosos.
- Inspeccionar (inspeccionar-descartar): denegación por inspección de aplicación.
- Interfaz (interface-drop): paquetes descartados por comprobaciones de interfaz.
- Análisis (amenaza de análisis): ataques de análisis de la red/el host.
- Ataque SYN (ataque SYN): ataques de sesión incompletos, que incluyen ataques SYN TCP y sesiones UDP unidireccionales que no tienen datos de retorno.

Cada uno de estos eventos tiene un conjunto específico de desencadenadores que se utilizan para identificar la amenaza. La mayoría de los disparadores están ligados a razones específicas de caída de ASP, aunque también se consideran ciertos syslogs y acciones de inspección. Algunos desencadenadores están

supervisados por varias categorías de amenazas. Algunos de los desencadenadores más comunes se describen en esta tabla, aunque no es una lista exhaustiva:

Amenaza básica	Desencadenante(s) / Razones de descarte de ASP
acl-drop	acl-drop
bad-packet-drop	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-match
conn-limit-drop	conn-limit
eliminación de dos	sp-security-failed
fw-drop	inspect-icmp-seq-num-not-match inspect-dns-pak-too-long inspect-dns-id-not-match sp-security-failed acl-drop
icmp-drop	inspect-icmp-seq-num-not-match
inspect-drop	Caídas de tramas activadas por un motor de inspección
interface-drop	sp-security-failed no-route
amenaza de exploración	tcp-3whs-failed tcp-not-syn sp-security-failed acl-drop inspect-icmp-seq-num-not-match inspect-dns-pak-too-long inspect-dns-id-not-match
syn-attack	%ASA-6-302014 syslog con motivo de desconexión de "SYN Timeout"

Para cada evento, la detección de amenazas básica mide la velocidad a la que se producen estas caídas durante un período de tiempo configurado. Este período de tiempo se denomina intervalo de velocidad promedio (ARI) y puede oscilar entre 600 segundos y 30 días. Si el número de eventos que ocurren dentro del ARI excede los umbrales de velocidad configurados, ASA considera estos eventos una amenaza.

La detección básica de amenazas tiene dos umbrales configurables para cuando considera que los eventos son una amenaza: la velocidad media y la velocidad de ráfaga. La velocidad promedio es simplemente el número promedio de caídas por segundo dentro del período de tiempo de la ARI configurada. Por ejemplo, si el umbral de velocidad promedio para las caídas de ACL se configura para 400 con una ARI de 600 segundos, ASA calcula el número promedio de paquetes que fueron descartados por las ACL en los últimos 600 segundos. Si este número resulta ser mayor que 400 por segundo, ASA registra una amenaza.

Del mismo modo, la velocidad de ráfaga es muy similar, pero observa períodos más pequeños de datos de instantáneas, denominados intervalo de velocidad de ráfaga (BRI). La BRI es siempre más pequeña que la ARI. Por ejemplo, basándose en el ejemplo anterior, el ARI para las caídas de ACL sigue siendo de 600 segundos y ahora tiene una velocidad de ráfaga de 800. Con estos valores, el ASA calcula el número promedio de paquetes descartados por las ACL en 20 segundos, donde 20 segundos es la BRI. Si este valor calculado supera las 800 caídas por segundo, se registra una amenaza. Para determinar qué BRI se utiliza, el ASA calcula el valor de 1/30 del ARI. Por lo tanto, en el ejemplo utilizado anteriormente, 1/30 de 600 segundos es 20 segundos. Sin embargo, la detección de amenazas tiene una BRI mínima de 10 segundos, por lo que si 1/30 de la ARI es menor que 10, el ASA todavía utiliza 10 segundos como la BRI. Además, es importante tener en cuenta que este comportamiento era diferente en las versiones anteriores a la 8.2(1), que utilizaba un valor de 1/60 del ARI, en lugar de 1/30. La BRI mínima de 10 segundos es la misma para todas las versiones de software.

Cuando se detecta una amenaza básica, el ASA simplemente genera syslog %ASA-4-733100 para alertar al administrador de que se ha identificado una amenaza potencial. El número promedio, actual y total de eventos para cada categoría de amenaza se puede ver con el comando **show threat-detection rate**. El número total de eventos acumulados es la suma del número de eventos observados en las últimas 30 muestras BRI.

La velocidad de ráfaga en syslog se calcula en función del número de paquetes descartados hasta el momento en la BRI actual. El cálculo se realiza periódicamente en una BRI. Una vez que se produce una brecha, se genera un registro del sistema. Es limitado que sólo se genere un syslog en una BRI. La velocidad de ráfaga en "show threat-detection rate" se calcula en función del número de paquetes descartados en la última BRI. El diseño de la diferencia es que syslog es sensible al tiempo, por lo que si ocurre una brecha en la BRI actual, tendría la oportunidad de ser capturado. "show threat-detection rate" es menos sensible al tiempo, por lo que se utiliza el número de la última BRI.

La detección básica de amenazas no realiza ninguna acción para detener el tráfico desviado o evitar futuros ataques. En este sentido, la detección básica de amenazas es puramente informativa y se puede utilizar como mecanismo de supervisión o generación de informes.

Detección de amenazas avanzadas (Estadísticas de nivel de objeto y N primeros)

A diferencia de la detección de amenazas básica, la detección de amenazas avanzada se puede utilizar para realizar un seguimiento estadístico de objetos más granulares. ASA admite estadísticas de seguimiento para IP de host, puertos, protocolos, ACL y servidores protegidos por intercepción TCP. La detección de amenazas avanzadas solo está habilitada de forma predeterminada para las estadísticas de ACL.

Para los objetos de host, puerto y protocolo, la detección de amenazas realiza un seguimiento del número de paquetes, bytes y caídas que ese objeto envió y recibió dentro de un período de tiempo específico. En el caso de las ACL, la detección de amenazas realiza un seguimiento de las 10 ACE principales (tanto de permiso como de denegación) que más se alcanzaron en un período de tiempo específico.

Los períodos de tiempo de seguimiento en todos estos casos son de 20 minutos, 1 hora, 8 horas y 24 horas. Aunque los periodos de tiempo en sí no se pueden configurar, el número de periodos de los que se realiza un seguimiento por objeto se puede ajustar con la palabra clave 'number-of-rate'. Consulte la sección Configuración para obtener más información. Por ejemplo, si 'number-of-rate' está configurado en 2, verá todas las estadísticas para 20 minutos, 1 hora y 8 horas. si 'number-of-rate' está configurado en 1, verá todas las estadísticas para 20 minutos, 1 hora. Pase lo que pase, la tarifa de 20 minutos siempre se muestra.

Cuando la intercepción TCP está habilitada, la detección de amenazas puede realizar un seguimiento de los 10 servidores principales que se consideran atacados y protegidos por la intercepción TCP. Las estadísticas de intercepción de TCP son similares a la detección de amenazas básica en el sentido de que el usuario puede configurar el intervalo de velocidad medido junto con las tasas medias específicas (ARI) y de ráfaga (BRI). Las estadísticas de detección de amenazas avanzadas para la intercepción de TCP solo están disponibles en ASA 8.0(4) y versiones posteriores.

Las estadísticas de detección de amenazas avanzadas se visualizan mediante los comandos **show threat-detection statistics** y **show threat-detection statistics top**. Esta es también la función responsable del llenado de los gráficos "superiores" en el panel de firewall de ASDM. Los únicos registros del sistema generados por la detección de amenazas avanzadas son %ASA-4-733104 y %ASA-4-733105, que se activan cuando se superan las velocidades de ráfaga y promedio (respectivamente) para las estadísticas de intercepción TCP.

Al igual que la detección de amenazas básica, la detección de amenazas avanzada es puramente informativa. No se lleva a cabo ninguna acción para bloquear el tráfico según las estadísticas de detección de amenazas avanzadas.

Detección de amenazas

El análisis de detección de amenazas se utiliza para realizar un seguimiento de los atacantes sospechosos que crean conexiones a demasiados hosts de una subred o a muchos puertos de un host o una subred. El análisis de la detección de amenazas está desactivado de forma predeterminada.

El análisis de la detección de amenazas se basa en el concepto de detección de amenazas básica, que ya define una categoría de amenazas para un ataque de análisis. Por lo tanto, los parámetros de intervalo de velocidad, velocidad media (ARI) y velocidad de ráfaga (BRI) se comparten entre la detección de amenazas básica y la detección de amenazas de exploración. La diferencia entre las dos funciones es que, mientras que la detección básica de amenazas solo indica que se superaron los umbrales de velocidad media o de ráfaga, la detección de amenazas de análisis mantiene una base de datos de direcciones IP de destino y de atacante que puede ayudar a proporcionar más contexto sobre los hosts que participan en el análisis. Además, el análisis de detección de amenazas solo tiene en cuenta el tráfico que recibe realmente el host/subred de destino. La detección básica de amenazas puede activar una amenaza de escaneo incluso si el tráfico es descartado por una ACL.

El análisis de la detección de amenazas puede, opcionalmente, reaccionar ante un ataque rechazando la IP del atacante. Esto convierte a la detección de amenazas de análisis en el único subconjunto de la función de detección de amenazas que puede afectar de forma activa a las conexiones a través de ASA.

Cuando el análisis de detección de amenazas detecta un ataque, se registra %ASA-4-733101 para el atacante o las IP de destino. Si la función está configurada para rechazar al atacante, se registra %ASA-4-733102 cuando el análisis de detección de amenazas genera un rechazo. %ASA-4-733103 se registra cuando se elimina el rechazo. El comando **show threat-detection scanning-threat** se puede utilizar para ver toda la base de datos de amenazas de análisis.

Limitaciones

- La detección de amenazas solo está disponible en ASA 8.0(2) y versiones posteriores. No es compatible con la plataforma ASA 1000V.
- La detección de amenazas solo se admite en el modo de contexto único.
- Solo se detectan las amenazas "mediante el dispositivo". La detección de amenazas no tiene en cuenta el tráfico enviado al propio ASA.
- Los intentos de conexión TCP que reinicia el servidor de destino no se cuentan como un ataque SYN o una amenaza de análisis.

Configuración

Detección básica de amenazas

La detección básica de amenazas se habilita con el comando **threat-detection basic-threat**.

```
<#root>

ciscoasa(config)#

threat-detection basic-threat
```

Las velocidades predeterminadas se pueden ver con el comando **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
```

Para ajustar estas velocidades con valores personalizados, simplemente reconfigure el comando **threat-detection rate** para la categoría de amenaza apropiada.

<#root>

```
ciscoasa(config)#
```

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

Cada categoría de amenaza puede tener un máximo de 3 velocidades diferentes definidas (con ID de velocidad de 1, velocidad 2 y velocidad 3). Se hace referencia al ID de velocidad particular que se excede en el syslog %ASA-4-733100.

En el ejemplo anterior, la detección de amenazas crea syslog 733100 sólo cuando el número de caídas de ACL supera las 250 caídas/segundo en 1200 segundos o las 550 caídas/segundo en 40 segundos.

Detección de amenazas avanzadas

Utilice el comando **threat-detection statistics** para habilitar la detección de amenazas avanzada. Si no se proporciona ninguna palabra clave de función específica, el comando habilita el seguimiento de todas las estadísticas.

<#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>
```

Para configurar el número de intervalos de velocidad de los que se realiza un seguimiento para el host, el puerto, el protocolo o las estadísticas de ACL, utilice la palabra clave **number-of-rate**.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics host number-of-rate 2

La palabra clave number-of-rate configura la detección de amenazas para realizar un seguimiento solamente del número n de intervalos más cortos.

Para habilitar las estadísticas de intercepción TCP, utilice el comando **threat-detection statistics tcp-intercept**.

<#root>

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

Para configurar las velocidades personalizadas para las estadísticas de intercepción TCP, utilice las palabras clave **rate-interval**, **average-rate** y **burst-rate**.

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

Detección de amenazas

Para habilitar la Detección de amenazas de escaneo, utilice el comando **threat-detection-threat**.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat
```

Para ajustar las velocidades de una amenaza de escaneo, utilice el mismo comando **threat-detection rate** que utiliza la Detección básica de amenazas.

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

Para permitir que ASA rechace una IP de atacante de escaneo, agregue la palabra clave **shun** al comando **threat-detection-threat**.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat shun
```

Esto permite que el análisis de detección de amenazas cree una omisión de una hora para el atacante. Para ajustar la duración del rechazo, utilice el comando **threat-detection scanning-threat shun duration**.

```
<#root>
ciscoasa(config)#
```

```
threat-detection scanning-threat shun duration 1000
```

En algunos casos, puede evitar que el ASA rechace ciertas IP. Para ello, cree una excepción con el comando **threat-detection-threat shun exception**.

```
<#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
```

Rendimiento

La detección básica de amenazas tiene un impacto mínimo en el rendimiento de ASA. La detección de amenazas avanzada y de escaneo consume muchos más recursos, ya que debe llevar un registro de varias estadísticas en la memoria. Solo el análisis de la detección de amenazas con la función de rechazo activada puede afectar de forma activa al tráfico que, de lo contrario, se habría permitido.

A medida que las versiones del software ASA han progresado, la utilización de la memoria de la detección de amenazas se ha optimizado significativamente. Sin embargo, se debe tener cuidado para monitorear el uso de memoria de ASA antes y después de habilitar la Detección de amenazas. En algunos casos, sería mejor habilitar sólo ciertas estadísticas (por ejemplo, estadísticas de host) temporalmente mientras se resuelve activamente un problema específico.

Para obtener una vista más detallada del uso de memoria de la detección de amenazas, ejecute el comando **show memory app-cache threat-detection [detail]**.

Acciones recomendadas

En estas secciones se ofrecen algunas recomendaciones generales sobre las acciones que se pueden llevar a cabo cuando se producen diversos eventos relacionados con la detección de amenazas.

Cuando se excede una velocidad de descarte básica y se genera %ASA-4-733100

Determine la categoría de amenaza específica mencionada en el syslog %ASA-4-733100 y correlaciónelo con el resultado de `show threat-detection rate` . Con esta información, compruebe el resultado de `show asp drop` para determinar las razones por las que se descarta el tráfico.

Para obtener una vista más detallada del tráfico que se descarta por una razón específica, utilice una captura de descarte ASP con la razón en cuestión para ver todos los paquetes que se descartan. Por ejemplo, si se registran amenazas de descarte de ACL, capture en el motivo de descarte de 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
```

Esta captura muestra que el paquete descartado es un paquete UDP/53 de 10.10.10.10 a 192.168.1.100.

Si %ASA-4-733100 informa de una amenaza de exploración, también puede ser útil habilitar temporalmente la detección de amenazas de exploración. Esto permite al ASA realizar un seguimiento de las IP de origen y destino involucradas en el ataque.

Dado que la detección básica de amenazas supervisa principalmente el tráfico que ya ha descartado el ASP, no se requiere ninguna acción directa para detener una amenaza potencial. Las excepciones a esto son los ataques SYN y las amenazas de escaneo, que involucran el tráfico que pasa a través del ASA.

Si las caídas observadas en la captura de caídas ASP son legítimas y/o esperadas para el entorno de red, ajuste los intervalos de velocidad básicos a un valor más apropiado.

Si las caídas muestran tráfico ilegítimo, se deben tomar medidas para bloquear o limitar la velocidad del tráfico antes de que llegue al ASA. Esto puede incluir ACL y QoS en dispositivos ascendentes.

Para los ataques SYN, el tráfico se puede bloquear en una ACL en ASA. La intercepción TCP también se podría configurar para proteger los servidores de destino, pero esto podría simplemente dar lugar a una amenaza de límite de conexión que se registra en su lugar.

En el caso de las amenazas de análisis, el tráfico también se puede bloquear en una ACL en el ASA. Análisis de la detección de amenazas con shunse puede habilitar para permitir que el ASA bloquee proactivamente todos los paquetes del atacante durante un período de tiempo definido.

Cuando se detecta una amenaza de escaneo y se registra %ASA-4-733101

%ASA-4-733101 debe enumerar el host/subred de destino o la dirección IP del atacante. Para obtener la lista completa de objetivos y atacantes, consulte el resultado de show threat-detection scanning-threat.

Las capturas de paquetes en las interfaces ASA que se enfrentan al atacante y/o al/los objetivo(s) también pueden ayudar a aclarar la naturaleza del ataque.

Si el análisis detectado es inesperado, se deben tomar medidas para bloquear o limitar la velocidad del tráfico antes de que llegue al ASA. Esto puede incluir ACL y QoS en dispositivos ascendentes. Cuando el shunse agrega a la configuración de Detección de amenazas de escaneo, lo que permite al ASA descartar proactivamente todos los paquetes de la IP del atacante durante un período de tiempo definido. Como último recurso, el tráfico también se puede bloquear manualmente en el ASA a través de una ACL o una política de intercepción TCP.

Si el análisis detectado es un falso positivo, ajuste los intervalos de velocidad de amenaza de análisis a un valor más adecuado para el entorno de red.

Cuando se rechaza un atacante y se registra %ASA-4-733102

%ASA-4-733102 enumera la dirección IP del atacante rechazado. Use el comando show threat-detection shun para ver una lista completa de los atacantes que han sido rechazados específicamente por la detección de amenazas. Use el comando show shun para ver la lista completa de todas las IP que ASA rechaza activamente (esto incluye las de fuentes distintas a la detección de amenazas).

Si el rechazo forma parte de un ataque legítimo, no es necesario realizar ninguna otra acción. Sin embargo, sería beneficioso bloquear manualmente el tráfico del atacante en la dirección ascendente hacia el origen en la medida de lo posible. Esto se puede hacer a través de ACL y QoS. Esto garantiza que los dispositivos intermedios no tengan que desperdiciar recursos en tráfico ilegítimo.

Si la amenaza de escaneo que desencadenó el rechazo es un falso positivo, elimine manualmente el rechazo con el comando clear threat-detection shun [IP_address] comando.

Cuando %ASA-4-733104 y/o %ASA-4-733105 está registrado

%ASA-4-733104 y %ASA-4-733105 enumeran el host objetivo del ataque que está protegido actualmente por la intercepción TCP. Para obtener más información sobre los índices de ataque y los servidores protegidos, consulte el resultado 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)
```

Cuando la detección de amenazas avanzadas detecta un ataque de esta naturaleza, ASA ya protege el servidor objetivo a través de la intercepción TCP. Verifique los límites de conexión configurados para asegurarse de que proporcionan una protección adecuada para la naturaleza y la velocidad del ataque. Además, sería beneficioso bloquear manualmente el tráfico del atacante en la dirección ascendente hacia el origen en la medida de lo posible. Esto se puede hacer a través de ACL y QoS. Esto garantiza que los dispositivos intermedios no tengan que desperdiciar recursos en tráfico ilegítimo.

Si el ataque detectado es un falso positivo, ajuste las velocidades de un ataque de intercepción TCP a un valor más apropiado con el comando threat-detection statistics tcp-interceptcomando.

Cómo desencadenar una amenaza manualmente

Para probar y solucionar problemas, puede resultar útil activar manualmente varias amenazas. Esta sección contiene sugerencias sobre cómo activar algunos tipos de amenazas habituales.

Amenaza básica: eliminación de ACL, firewall y análisis

Para desencadenar una amenaza básica concreta, consulte la tabla de la sección Funcionalidad anterior. Elija un motivo de caída de ASP específico y envíe el tráfico a través de ASA que se interrumpiría por el motivo de caída de ASP adecuado.

Por ejemplo, las amenazas ACL Drop, Firewall y Scanning consideran la velocidad de paquetes descartados por acl-drop. Complete estos pasos para activar estas amenazas simultáneamente:

1. Cree una ACL en la interfaz exterior del ASA que descarte explícitamente todos los paquetes TCP enviados a un servidor de destino en el interior del 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. Desde un atacante en el exterior del ASA (10.10.10.10), utilice nmap para ejecutar un escaneo SYN TCP contra cada puerto en el servidor de destino:

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

   > **Nota**: T5 configura nmap para ejecutar el análisis lo más rápido posible. Según los recursos del equipo atacante, esto aún no es lo suficientemente rápido como para activar algunas de las velocidades predeterminadas. Si este es el caso, simplemente reduzca las tasas configuradas para la amenaza que desea ver. Cuando establece ARI y BRI en 0, la Detección básica de amenazas siempre activa la amenaza, independientemente de la velocidad.

3. Tenga en cuenta que se detectan amenazas básicas para las amenazas de caída de ACL, firewall y análisis:

   ```
   %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
   ```

   > **Nota**: En este ejemplo, la caída de ACL y las ARI y BRI del firewall se han configurado en 0, por lo que siempre activan una amenaza. Esta es la razón por la que las velocidades máximas configuradas se muestran como 0.

Amenaza avanzada: intercepción de TCP

1. Cree una ACL en la interfaz externa que permita todos los paquetes TCP enviados a un servidor de destino en el interior del 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 el servidor de destino no existe realmente, o si restablece los intentos de conexión del atacante, configure una entrada ARP falsa en el ASA para poner en un agujero negro el tráfico de ataque fuera de la interfaz interna:

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

3. Cree una política de intercepción TCP simple en 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
```

Desde un atacante en el exterior del ASA (10.10.10.10), utilice nmap para ejecutar un escaneo SYN TCP en cada puerto del servidor de destino:

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

Tenga en cuenta que la detección de amenazas realiza un seguimiento del servidor protegido:

<#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)
```

Análisis de amenazas

1. Cree una ACL en la interfaz externa que permita todos los paquetes TCP enviados a un servidor de destino en el interior del 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
```

> **Nota**: para que la Detección de amenazas de escaneo rastree las IP de los atacantes y de los objetivos, el tráfico debe estar permitido a través del ASA.

2. Si el servidor de destino no existe realmente, o si restablece los intentos de conexión del atacante, configure una entrada ARP falsa en el ASA para poner en un agujero negro el tráfico de ataque fuera de la interfaz interna:

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

> **Nota**: las conexiones que restablece el servidor de destino no se cuentan como parte de la amenaza.

3. Desde un atacante en el exterior del ASA (10.10.10.10), utilice nmap para ejecutar un escaneo SYN TCP en cada puerto del servidor de destino:

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

> **Nota**: T5 configura nmap para ejecutar el análisis lo más rápido posible. Según los recursos del equipo atacante, esto aún no es lo suficientemente rápido como para activar algunas de las velocidades predeterminadas. Si este es el caso, simplemente reduzca las tasas configuradas para la amenaza que desea ver. Cuando establece ARI y BRI en 0, la Detección básica de amenazas siempre activa la amenaza, independientemente de la velocidad.

4. Tenga en cuenta que se detecta una amenaza de análisis, se realiza un seguimiento de la IP del atacante y este se rechaza:

```
%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
```

Información Relacionada

- **Guía de configuración de ASA**
- **Referencia de Comandos de ASA**
- **Mensajes de registro del sistema de Cisco Secure Firewall ASA Series**
- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).