Funciones y configuración de la detección de la amenaza ASA

Contenido

Introducción

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 la amenaza proporciona a los administradores del Firewall con las herramientas necesarias para identificar, para entender, y para parar los ataques antes de que alcancen la infraestructura de red interna. Para hacer así pues, la característica confía en varios diversos activadores y estadísticas, que se describe en el detalle adicional en estas secciones.

La detección de la amenaza se puede utilizar en cualquier Firewall ASA que funcione con una versión de software de 8.0(2) o más adelante. Aunque la detección de la amenaza no sea un substituto para una solución dedicada IDS/IPS, puede ser utilizada en los entornos donde no está disponible un IPS proporcionar una capa agregada de protección a las funciones de la base del ASA.

Funciones de la detección de la amenaza

La característica de la detección de la amenaza tiene tres componentes principales:

1. Detección básica de la amenaza
2. Detección avanzada de la amenaza
3. Analizar la detección de la amenaza

Cada uno de estos componentes se describe detalladamente en estas secciones.

Detección básica de la amenaza (tarifas a nivel sistema)

La detección básica de la amenaza se habilita por abandono en todo el funcionamiento ASA 8.0(2) y posterior.

La detección básica de la amenaza monitorea las tarifas en las cuales los paquetes son caídos por las diversas razones por el ASA en conjunto. Esto significa que las estadísticas generadas por la detección básica de la amenaza se aplican solamente al dispositivo entero y no son generalmente bastante granulares proporcionar la información sobre la fuente o la naturaleza específica de la amenaza. En lugar, el ASA monitorea los paquetes perdidos para estos eventos:

- **Descenso ACL (ACL-descenso)** - Los paquetes son negados por las Listas de acceso
- **Mún pkts (malo-paquete-descenso)** - El paquete no válido formata, que incluye las encabezados L3 y L4 que no se ajustan a los estándares RFC
- **Límite conec (CONN-límite-descenso)** - Paquetes que exceden un límite configurado o de la Conexión global
- **Ataque DOS (DOS-descenso)** - Ataques de la negación de servicio (DOS)
- **Firewall (FW-descenso)** - Revisiones de seguridad básicas del Firewall
- **Ataque ICMP (ICMP-descenso)** - Paquetes icmp sospechosos
- **Examine (examinar-descenso)** - Negación por la Inspección de la aplicación
- **Interfaz (interfaz-descenso)** - Paquetes caídos por las comprobaciones de interfaz
- **El analizar (exploración-amenaza)** - Ataques de la exploración de la red/del host
- **Ataque SYN (Ataque SYN)** - Ataques incompletos de la sesión, que incluye los Ataques SYN TCP y a las Sesiones UDP unidireccionales que no tienen ningún dato de vuelta

Cada uno de estos eventos tiene un conjunto específico de los activadores que se utilizan para identificar la amenaza. La mayoría de los activadores se ligan a las razones específicas del descenso ASP, aunque los ciertos Syslog y acciones del examen también se consideran. Algunos activadores son monitoreados por las categorías múltiples de la amenaza. Algunos de los activadores mas comunes se delinean en esta tabla, aunque no es una lista exhaustiva:

Amenaza básica	Razones del descenso de los activadores/ASP
ACL-descenso	ACL-descenso
malo-paquete-descenso	inválido-TCP-HDR-longitud inválido-IP-encabezado examinar-dns-pak-demasiado-largo
CONN-límite-descenso	examinar-dns-identificación-no-correspondido con CONN-límite
DOS-descenso	SP-Seguridad-fallado
FW-descenso	examinar-ICMP-seq-numérico-no-correspondido con examinar-dns-pak-demasiado-largo

	examinar-dns-identificación-no-correspondido con SP-Seguridad-fallado ACL-descenso
ICMP-descenso	examinar-ICMP-seq-numérico-no-correspondido con
examinar-descenso	Descensos del capítulo accionados por un motor del examen
interfaz-descenso	SP-Seguridad-fallado ninguno-ruta
	tcp-3whs-failed TCP-no-SYN SP-Seguridad-fallado
exploración-amenaza	ACL-descenso examinar-ICMP-seq-numérico-no-correspondido con examinar-dns-pak-demasiado-largo examinar-dns-identificación-no-correspondido con
Ataque SYN	Syslog %ASA-6-302014 con la razón del desmontaje del “tiempo de espera SYN

Para cada evento, la detección básica de la amenaza mide las tarifas que estos descensos ocurren durante un periodo configurado del tiempo. Este período de tiempo se llama el **intervalo de la tasa promedio (ARI)** y puede extenderse a partir de 600 segundos a 30 días. Si el número de eventos que ocurran dentro del ARI excede los umbrales de la velocidad configurada, el ASA considera estos eventos una amenaza.

La detección básica de la amenaza tiene dos umbrales configurables para cuando considera los eventos ser una amenaza: **la tasa promedio** y la **velocidad de ráfaga**. La tasa promedio es simplemente el número medio de descensos por segundo dentro del período de tiempo del ARI configurado. Por ejemplo, si el umbral de la tasa promedio para los descensos ACL se configura para 400 con un ARI de 600 segundos, el ASA calcula el número medio de paquetes que fueron caídos por los ACL en el último 600 segundos. Si este número resulta ser mayor de 400 por segundo, el ASA registra una amenaza.

Asimismo, la velocidad de ráfaga es muy similar pero miradas en períodos más pequeños de datos de la foto, llamados el **intervalo de la velocidad de ráfaga (BRI)**. El BRI es siempre más pequeño que el ARI. Por ejemplo, el emplear el ejemplo anterior, el ARI para los descensos ACL sigue siendo 600 segundos y ahora tiene una velocidad de ráfaga de 800. Con estos valores, el ASA calcula el número medio de paquetes caídos por los ACL en el último 20 segundos, donde están el BRI 20 segundos. Si este valor calculado excede 800 descensos por segundo, se registra una amenaza. Para determinar se utiliza qué BRI, el ASA calcula el valor del 1/30o del ARI. Por lo tanto, en el ejemplo usado previamente, el 1/30o de 600 segundos es 20 segundos. Sin embargo, la detección de la amenaza tiene un mínimo BRI de 10 segundos, así que si el 1/30o del ARI es menos de 10, el ASA todavía utiliza 10 segundos como el BRI. También, es importante observar que este comportamiento era diferente en las versiones antes de 8.2(1), que utilizó un valor del 1/60o del ARI, en vez del 1/30o. El mínimo BRI de 10 segundos es lo mismo para todas las versiones de software.

Cuando se detecta una amenaza básica, el ASA genera simplemente el Syslog %ASA-4-733100 para alertar al administrador que se ha identificado una amenaza potencial. La media, la corriente, y el número total de eventos para cada categoría de la amenaza se pueden considerar con el **comando rate de la amenaza-detección de la demostración**. El número total de eventos acumulativos es la suma del número de eventos considerados en las muestras del último 30 BRI.

La detección básica de la amenaza no toma ningunas medidas para parar el tráfico ofensivo o prevenir los ataques futuros. En este sentido, la detección básica de la amenaza es puramente informativa y se puede utilizar como una supervisión o mecanismo de generación de informes.

Detección avanzada de la amenaza (estadísticas del objeto y top llanos N)

A diferencia de la detección básica de la amenaza, la detección avanzada de la amenaza se puede utilizar para seguir las estadísticas para objetos más granulares. El ASA soporta el seguimiento de las estadísticas para el host IP, los puertos, los protocolos, los ACL, y los servidores protegidos por la Intercepción de tráfico de TCP. La detección avanzada de la amenaza se habilita solamente por abandono para las estadísticas ACL.

Para el host, el puerto, y los objetos del protocolo, la detección de la amenaza no pierde de vista el número de paquetes, de bytes, y de descensos que fueron enviados y recibidos por ese objeto dentro de un período específico. Para los ACL, la detección de la amenaza no pierde de vista los 10 ACE superiores (el permiso y niega) que estaban golpeados más dentro de un período específico.

Los períodos de tiempo seguidos en todos estos casos son 20 minutos, 1 hora, 8 horas, y 24 horas. Mientras que los períodos de tiempo ellos mismos no son configurables, el número de períodos que se sigan por el objeto se puede ajustar con la palabra clave de la “número-de-tarifa”. Vea la sección de configuración para más información. Por ejemplo, si la “número-de-tarifa” se fija a 2, usted ve todas las estadísticas para 20 minutos, 1 hora y 8 horas. si la “número-de-tarifa” se fija a 1, usted ve todas las estadísticas por 20 minutos, 1 hora. No importa qué, la tarifa minuciosa 20 se visualiza siempre.

Cuando se habilita la Intercepción de tráfico de TCP, la detección de la amenaza puede no perder de vista los 10 servidores superiores que se consideran estar bajo ataque y son protegidos por la Intercepción de tráfico de TCP. Las estadísticas para la Intercepción de tráfico de TCP son similares a la detección básica de la amenaza en el sentido que el usuario puede configurar el tarifa-intervalo medido junto con medio específico (ARI) y repartir las tarifas (BRI). Las estadísticas avanzadas de la detección de la amenaza para la Intercepción de tráfico de TCP están solamente disponibles en ASA 8.0(4) y posterior.

Las estadísticas avanzadas de la detección de la amenaza se ven vía las **estadísticas de la amenaza-detección de la demostración** y **muestran los comandos top de las estadísticas de la amenaza-detección**. Ésta es también la característica responsable de poblar los gráficos “superiores” en el panel del Firewall del ASDM. Los únicos Syslog que son generados por la detección avanzada de la amenaza son %ASA-4-733104 y %ASA-4-733105, se accionan que cuando la media y las velocidades de ráfaga (respectivamente) se exceden para las estadísticas de la Intercepción de tráfico de TCP.

Como la detección básica de la amenaza, la detección avanzada de la amenaza es puramente informativa. No se toma ningunas medidas para bloquear el tráfico basado en las estadísticas avanzadas de la detección de la amenaza.

Analizar la detección de la amenaza

Analizar la detección de la amenaza se utiliza para no perder de vista los atacantes sospechosos que crean las conexiones demasiados host en una subred, o muchos puertos en un host/una subred. Analizando la detección de la amenaza se inhabilita por abandono.

Analizando los emplear de la detección de la amenaza el concepto de detección básica de la amenaza, que define ya una categoría de la amenaza para un ataque de la exploración. Por lo

tanto, el tarifa-intervalo, la tasa promedio (ARI), y las configuraciones de la velocidad de ráfaga (BRI) se comparten entre la detección básica y de la exploración de la amenaza. La diferencia entre las 2 características es que mientras que la detección básica de la amenaza indica solamente que la media o los umbrales de la velocidad de ráfaga fue cruzada, analizando la detección de la amenaza mantiene una base de datos del atacante y de los IP Address de destino que pueda ayudar a proporcionar más contexto alrededor de los host implicados en la exploración. Además, solamente el tráfico que es recibido realmente por el host de destino/la subred es considerado analizando la detección de la amenaza. La detección básica de la amenaza puede todavía accionar una amenaza de la exploración incluso si el tráfico es caído por un ACL.

Analizar la detección de la amenaza puede reaccionar opcionalmente a un ataque evitando el IP del atacante. Esto hace detección de la amenaza de la exploración el único subconjunto de la característica de la detección de la amenaza que puede afectar activamente a las conexiones con el ASA.

Cuando analizar la detección de la amenaza detecta un ataque, %ASA-4-733101 se registra para el atacante y/o la blanco IP. Si la característica se configura para evitar el atacante, se registra %ASA-4-733102 al analizar la detección de la amenaza genera un evitar. Se registra %ASA-4-733103 cuando se quita el evitar. El comando de la exploración-**amenaza de la amenaza-detección de la demostración** se puede utilizar para ver la base de datos entera de la amenaza de la exploración.

Limitaciones

- La detección de la amenaza está solamente disponible en ASA 8.0(2) y posterior. No se soporta en la plataforma ASA 1000V.
- La detección de la amenaza se soporta solamente en el solo modo del contexto.
- Solamente se detectan las amenazas del por--cuadro. El tráfico enviado al ASA sí mismo no es considerado por la detección de la amenaza.
- Las tentativas de la conexión TCP que son reajustadas por el servidor apuntado no se cuentan como amenaza del Ataque SYN o de la exploración.

Configuración

Detección básica de la amenaza

La detección básica de la amenaza se habilita con el comando de la básico-**amenaza de la amenaza-detección**.

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

Las velocidades predeterminadas se pueden ver con la **demostración funcionan con todo el** comando de la amenaza-**detección**.

```
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 tarifas con los valores en aduana, configure de nuevo simplemente el **comando rate de la amenaza-detección** para la categoría apropiada de la amenaza.

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

Cada categoría de la amenaza puede tener un máximo de 3 diversas tarifas definidas (con el índice ID de la tarifa 1, de la tarifa 2, y de la tarifa 3). La tarifa determinada ID se excede que se refiere al Syslog %ASA-4-733100.

En el ejemplo anterior, la detección de la amenaza crea el Syslog 733100 solamente cuando el número de descensos ACL excede 250 descensos/en segundo lugar durante 1200 segundos o 550 descensos/en segundo lugar durante 40 segundos.

Detección avanzada de la amenaza

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

```
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 la tarifa que se sigan para el host, el puerto, el protocolo, o las estadísticas ACL, utilice la palabra clave de la número-de-**tarifa**.

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

La palabra clave de la número-de-tarifa configura la detección de la amenaza para seguir solamente la cantidad de intervalos más corta *n*.

Para habilitar las estadísticas de la Intercepción de tráfico de TCP, utilice el comando de la **Intercepción de tráfico de TCP de las estadísticas de la amenaza-detección**.

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

Para configurar las tarifas de encargo para las estadísticas de la Intercepción de tráfico de TCP, utilice el tarifa-**intervalo**, la **tasa promedio**, y las palabras claves de la **velocidad de ráfaga**.

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

Analizar la detección de la amenaza

Para habilitar la detección de la amenaza de la exploración, utilice el comando de la exploración-**amenaza de la amenaza-detección**.

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

Para ajustar las tarifas para que haya una exploración-amenaza, utilice el mismo **comando rate de la amenaza-detección** usado por la detección básica de la amenaza.

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

Para permitir que el ASA evite un IP del atacante de la exploración, agregue la palabra clave del **evitar al** comando de la exploración-**amenaza de la amenaza-detección**.

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

Esto permite el analizar de la detección de la amenaza para crear una una hora evita para el atacante. Para ajustar la duración del evitar, utilice la exploración-**amenaza de la amenaza-detección evitan el** comando de la **duración**.

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

En algunos casos, usted puede todavía querer prevenir el ASA de ciertos IP que evitan. Para hacer esto, cree una excepción con la exploración-**amenaza de la amenaza-detección evitan el comando except**.

```
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 la amenaza tiene impacto del rendimiento muy pequeño en el ASA. La detección avanzada y de la exploración de la amenaza es mucho más uso intensivo de recurso porque tienen que no perder de vista las diversas estadísticas en la memoria. Solamente analizar la detección de la amenaza con la función del evitar habilitada puede afectar activamente el tráfico que habría sido permitido de otra manera.

Mientras que han progresado las versiones de software ASA, la utilización de la memoria de la detección de la amenaza se ha optimizado perceptiblemente. Sin embargo, el cuidado se debe tomar para monitorear la utilización de la memoria del ASA antes y después de que se habilita la detección de la amenaza. En algunos casos, puede ser que sea mejor habilitar solamente ciertas estadísticas (por ejemplo, las estadísticas del host) temporalmente mientras que activamente resolvía problemas un problema específico.

Para una más vista detallada del uso de la memoria de la detección de la amenaza, funcione con el comando de la amenaza-**detección del APP-caché de la memoria de la demostración [detail]**.

Acciones recomendadas

Estas secciones proporcionan algunas recomendaciones generales para medidas que puedan ser tomadas cuando ocurren los eventos Detección-relacionados de la diversa amenaza.

Cuando se excede una tarifa básica del descenso y se genera %ASA-4-733100

Determine la categoría específica de la amenaza mencionada en el Syslog %ASA-4-733100 y correlacione esto con la salida de la **tarifa de la amenaza-detección de la demostración**. Con esta información, marque la salida del **descenso de la demostración ASP** para determinar las razones por las que se está cayendo el tráfico.

Para una más vista detallada del tráfico que se cae por una razón específica, utilice una captura del descenso ASP con la razón en la pregunta para ver todos los paquetes se estén cayendo que. Por ejemplo, si se están registrando las amenazas del descenso ACL, captura en la razón del descenso ASP del ACL-**descenso**:

```
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 que es caído es un paquete UDP/53 de 10.10.10.10 a 192.168.1.100.

Si %ASA-4-733100 señala una amenaza de la exploración, puede también ser útil habilitar temporalmente la detección de la amenaza de la exploración. Esto permite que el ASA no pierda de vista la fuente y el IP de destino implicados en el ataque.

Puesto que la detección básica de la amenaza monitorea sobre todo el tráfico que está siendo caído ya por el ASP, no se requiere ninguna acción directa para parar una amenaza potencial. Las excepciones a esto son las amenazas de los Ataques SYN y de la exploración, que implican el tráfico que pasa con el ASA.

Si los descensos considerados en la captura del descenso ASP son legítimos y/o esperados para el entorno de red, ajuste los intervalos de la velocidad básica a un valor más apropiado.

Si los descensos muestran el tráfico ilegítimo, medidas se deben tomar para bloquear o límite de velocidad el tráfico antes de que alcance el ASA. Esto puede incluir los ACL y QoS en los dispositivos ascendentes.

Para los Ataques SYN, el tráfico se puede bloquear en un ACL en el ASA. La Intercepción de tráfico de TCP se podría también configurar para proteger los servidores apuntados, pero ésta podría dar lugar simplemente a una amenaza del límite conec que era registrada en lugar de otro.

Para analizar las amenazas, el tráfico se puede también bloquear en un ACL en el ASA. Analizar la detección de la amenaza con la opción del **evitar** se puede habilitar para permitir que el ASA dinámico bloquee todos los paquetes del atacante por un período de tiempo definido.

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

%ASA-4-733101 debe enumerar el host de destino/la subred o la dirección IP del atacante. Para la lista completa de blancos y de atacantes, marque la salida de la exploración-**amenaza de la amenaza-detección de la demostración**.

Las capturas de paquetes en las interfaces ASA que hacen frente al atacante y/o a las blancos pueden también ayudar a aclarar la naturaleza del ataque.

Si la exploración detectada es no haber esperado, medidas se deben tomar para bloquear o límite de velocidad el tráfico antes de que alcance el ASA. Esto puede incluir los ACL y QoS en los dispositivos ascendentes. Agregar la opción del **evitar a los** config de la detección de la amenaza de la exploración puede también permitir que el ASA dinámico caiga todos los paquetes del IP del atacante por un período de tiempo definido. Como último recurso, el tráfico se puede también bloquear manualmente en el ASA vía una directiva ACL o de la Intercepción de tráfico de TCP.

Si la exploración detectada es un falso positivo, ajuste los intervalos de la tarifa de la amenaza de la exploración a un valor más apropiado para que haya el entorno de red.

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

%ASA-4-733102 enumera la dirección IP del atacante evitado. Utilice el **comando shun de la amenaza-detección de la demostración** para ver una lista completa de atacantes que han sido evitados por la detección de la amenaza específicamente. Utilice el **comando show shun** para ver la lista completa de todos los IP que estén siendo evitados activamente por el ASA (de fuentes incluyendo con excepción de la detección de la amenaza).

Si el evitar es parte de al ataque legítimo, no se requiere ninguna otra acción. Sin embargo, sería beneficioso bloquear manualmente el tráfico del atacante como lejos por aguas arriba hacia la fuente como sea posible. Esto se puede hacer vía los ACL y QoS. Esto se asegura de que los dispositivos intermedios no necesiten perder los recursos que procesan el tráfico ilegítimo.

Si la amenaza de la exploración que accionó el evitar era un falso positivo, quite manualmente el evitar con la amenaza-**detección clara evitan [ip_address] el** comando.

Cuando se registra %ASA-4-733104 y/o %ASA-4-733105

%ASA-4-733104 y %ASA-4-733105 enumera el host apuntado por el ataque que está siendo protegido actualmente por la Intercepción de tráfico de TCP. Para más detalles en las tarifas de ataque y los servidores protegidos, marque la salida de la **Intercepción de tráfico de TCP superior de las estadísticas de la amenaza-detección de la demostración**.

```
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 avanzada de la amenaza detecta un ataque de esta naturaleza, el ASA está protegiendo ya el servidor apuntado vía la Intercepción de tráfico de TCP. Verifique los límites configurados de la conexión para asegurarse que proporcionan la protección adecuada para la naturaleza y el índice del ataque. También, sería beneficioso bloquear manualmente el tráfico del atacante como lejos por aguas arriba hacia la fuente como sea posible. Esto se puede hacer vía los ACL y QoS. Esto se asegura de que los dispositivos intermedios no necesiten perder los recursos que procesan el tráfico ilegítimo.

Si el ataque detectado es un falso positivo, ajuste las tarifas para que haya un ataque de la Intercepción de tráfico de TCP a un valor más apropiado con el comando de la **Intercepción de tráfico de TCP de las estadísticas de la amenaza-detección**.

Cómo accionar manualmente una amenaza

Para probar y los propósitos de Troubleshooting, puede ser útil accionar manualmente las diversas amenazas. Esta sección contiene las extremidades para accionar algunos tipos comunes de la amenaza.

Amenaza básica - Descenso, Firewall, y exploración ACL

Para accionar una amenaza básica determinada, refiera a la tabla en la sección anterior de las funciones. Elija una razón específica del descenso ASP y envíe el tráfico con el ASA que sería caído por la razón apropiada del descenso ASP.

Por ejemplo, las amenazas todas del descenso ACL, del Firewall, y de la exploración consideran el índice de paquetes que son caídos por el ACL-descenso. Complete estos pasos para accionar estas amenazas simultáneamente:

1. Cree un ACL en la interfaz exterior del ASA que cae 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. De un atacante en el exterior del ASA (10.10.10.10), utilice el nmap para funcionar con una exploración TCP SYN contra cada puerto en el servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Nota: El T5 configura el nmap para funcionar con la exploración tan rápido come sea posible. Dependiendo de los recursos del atacante PC, éste todavía puede no ser rápidamente bastante accionar algunas de las velocidades predeterminadas. Si éste es el caso, baje simplemente las velocidades configuradas para la amenaza que usted quiere ver. Determinación del ARI y del BRI a 0 detecciones básicas de la amenaza de las causas para accionar siempre la amenaza sin importar la tarifa.
3. Observe que las amenazas básicas están detectadas para las amenazas del descenso, del Firewall, y de la exploración ACL:`%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,`
   `max configured rate is 10; Current average rate is 9 per second,`
   `max configured rate is 5; Cumulative total count is 5538`
   `%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,`
   `max configured rate is 0; Current average rate is 2 per second,`

```
max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
max configured rate is 0; Current average rate is 2 per second,
max configured rate is 0; Cumulative total count is 1483
```
Nota: En este ejemplo, el descenso y el Firewall ARI y BRI ACL se han fijado a 0 que accionan tan siempre una amenaza. Esta es la razón por la cual las velocidades configuradas máximas se enumeran como 0.

Amenaza avanzada - Intercepción de tráfico de TCP

1. Cree un ACL en la interfaz exterior que permite 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 no existe el servidor de destino realmente, o reajusta los intentos de conexión del atacante, configure una entrada ARP falsa en el ASA al blackhole el tráfico del ataque hacia fuera la interfaz interior:`arp inside 10.11.11.11 dead.dead.dead`
3. Cree una directiva simple de la Intercepción de tráfico de TCP en el 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`
   De un atacante en el exterior del ASA (10.10.10.10), utilice el nmap para funcionar con una exploración TCP SYN contra cada puerto en el servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`
   Observe que la detección de la amenaza no pierde de vista el servidor protegido:
   ```
   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)
   ```

Analizar la amenaza

1. Cree un ACL en la interfaz exterior que permite 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 la amenaza de la exploración siga la blanco y el atacante IP, el tráfico se debe permitir con el ASA.
2. Si no existe el servidor de destino realmente, o reajusta los intentos de conexión del atacante, configure una entrada ARP falsa en el ASA al blackhole el tráfico del ataque hacia fuera la interfaz interior:`arp inside 10.11.11.11 dead.dead.dead`
   Nota: Las conexiones que son reajustadas por el servidor de destino no se cuentan como parte de la amenaza.
3. De un atacante en el exterior del ASA (10.10.10.10), utilice el nmap para funcionar con una exploración TCP SYN contra cada puerto en el servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`
   Nota: El T5 configura el nmap para funcionar con la exploración tan rápido come sea posible. Dependiendo de los recursos del atacante PC, éste todavía puede no ser rápidamente bastante accionar algunas de las velocidades predeterminadas. Si éste es el

caso, baje simplemente las velocidades configuradas para la amenaza que usted quiere ver. Determinación del ARI y del BRI a 0 detecciones básicas de la amenaza de las causas para accionar siempre la amenaza sin importar la tarifa.

4. Observe que una amenaza de la exploración está detectado, el IP del atacante se sigue, y se evita el atacante:

```
%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 ASA
- Referencia de comandos ASA
- Guía del Syslog ASA
- Soporte Técnico y Documentación - Cisco Systems