Firewall/IPS clásico de Cisco IOS: Configuración del control de acceso basado en el contexto (CBAC) para la protección frente a denegación de servicio

Contenido

Introducción

Este documento describe el procedimiento de ajuste para los parámetros de denegación de servicio (DoS) en Cisco IOS® Classic Firewall con CBAC.

CBAC proporciona funciones avanzadas de filtrado de tráfico y se puede utilizar como parte integral de su firewall de red.

DoS generalmente se refiere a la actividad de red que, intencionalmente o no, sobrecarga los recursos de red como el ancho de banda de enlace WAN, las tablas de conexión de firewall, la memoria de host final, la CPU o las capacidades de servicio. En el peor de los casos, la actividad de DoS sobrecarga el recurso vulnerable (o dirigido) hasta el punto de que el recurso deja de estar disponible y prohíbe la conectividad WAN o el acceso al servicio a usuarios legítimos.

El Cisco IOS Firewall puede contribuir a la mitigación de la actividad de DoS si mantiene contadores del número de conexiones TCP "semirabiertas", así como la velocidad de conexión total a través del firewall y el software de prevención de intrusiones tanto en el firewall clásico (**ip inspect**) como en el firewall de políticas basado en zonas.

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.

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. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Las conexiones semirabiertas son conexiones TCP que no han completado el intercambio de señales de tres vías SYN-SYN/ACK-ACK que siempre utilizan los peers TCP para negociar los parámetros de su conexión mutua. Un gran número de conexiones semiabiertas puede indicar actividad maliciosa, como DoS o ataques de denegación de servicio distribuida (DDoS). Un ejemplo de un tipo de ataque de DoS se lleva a cabo mediante software malicioso desarrollado intencionalmente, como gusanos o virus que infectan varios hosts en Internet e intentan saturar servidores de Internet específicos con ataques SYN, donde muchos hosts en Internet o en la red privada de una organización envían grandes cantidades de conexiones SYN a un servidor. Los ataques SYN representan un peligro para los servidores de Internet, ya que las tablas de conexión de los servidores se pueden cargar con intentos de conexión SYN "falsos" que llegan más rápido de lo que el servidor puede gestionar con las nuevas conexiones. Se trata de un tipo de ataque DoS porque el gran número de conexiones en la lista de conexiones TCP del servidor víctima impide el acceso legítimo del usuario a los servidores de Internet víctimas.

Cisco IOS Firewall también considera que las sesiones UDP (protocolo de datagramas de usuario) con tráfico en una sola dirección son "semirabiertas" porque muchas aplicaciones que utilizan UDP para el transporte reconocen la recepción de datos. Las sesiones UDP sin tráfico de retorno son probablemente indicativas de actividad DoS o intentos de conexión entre dos hosts, donde uno de los hosts se ha vuelto insensible. Muchos tipos de tráfico UDP, como mensajes de registro, tráfico de administración de red SNMP, transmisión de medios de voz y vídeo y tráfico de señalización, sólo utilizan tráfico en una dirección para transportar su tráfico. Muchos de estos tipos de tráfico aplican inteligencia específica de la aplicación para evitar que los patrones de tráfico unidireccionales afecten negativamente al comportamiento de DoS de IPS y firewall.

Antes de las versiones 12.4(11)T y 12.4(10) del software Cisco IOS, la inspección exhaustiva de paquetes de Cisco IOS ofrecía protección frente a ataques DoS como valor predeterminado cuando se aplicaba una regla de inspección. Las versiones 12.4(11)T y 12.4(10) del software del IOS de Cisco modificaron la configuración predeterminada de DoS para que la protección de DoS no se aplique automáticamente, pero los contadores de actividad de conexión sigan activos. Cuando la protección DoS está activa, es decir, cuando se utilizan los valores predeterminados en versiones de software anteriores o los valores se han ajustado al rango que afecta al tráfico, la

protección DoS se habilita en la interfaz donde se aplica la inspección, en la dirección en que se aplica el firewall, para que los protocolos de configuración de políticas de firewall inspeccionen. La protección DoS sólo se habilita en el tráfico de red si el tráfico entra o sale de una interfaz con una inspección aplicada en la misma dirección del tráfico inicial (paquete SYN o primer paquete UDP) para una conexión TCP o una sesión UDP.

La inspección de Cisco IOS Firewall proporciona varios valores ajustables para protegerse contra los ataques de DoS. Las versiones del software Cisco IOS anteriores a 12.4(11)T y 12.4(10) tienen valores de DoS predeterminados que pueden interferir con el correcto funcionamiento de la red si no se configuran para el nivel adecuado de actividad de la red en redes donde las velocidades de conexión exceden los valores predeterminados. Estos parámetros le permiten configurar los puntos en los que comienza a surtir efecto la protección DoS del router de firewall. Cuando los contadores DoS del router exceden los valores predeterminados o configurados, el router restablece una conexión semirabierta antigua para cada conexión nueva que exceda los valores máximos incompletos configurados o altos de un minuto hasta que el número de sesiones semirabiertas caiga por debajo de los valores bajos máximos incompletos. El router envía un mensaje de registro del sistema si se habilita el registro y si se configura un sistema de prevención de intrusiones (IPS) en el router, el router de firewall envía un mensaje de firma de DoS a través del intercambio de eventos del dispositivo de seguridad (SDEE). Si los parámetros de DoS no se ajustan al comportamiento normal de su red, la actividad normal de la red puede activar el mecanismo de protección de DoS, que causa fallas en las aplicaciones, bajo rendimiento de la red y alto uso de la CPU en el router Cisco IOS Firewall.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Ajuste de denegación de servicio para firewall y sistema de prevención de intrusiones Cisco IOS Software Classic (IP Inspect)

El firewall Cisco IOS clásico mantiene un conjunto global de contadores DoS para el router, y todas las sesiones de firewall para todas las políticas de firewall en todas las interfaces se aplican al conjunto global de contadores de firewall.

Cisco IOS Classic Firewall Inspection proporciona protección contra ataques DoS de forma predeterminada cuando se aplica un firewall clásico. La protección DoS se habilita en todas las interfaces donde se aplica la inspección, en la dirección en que se aplica el firewall, para cada servicio o protocolo que la política de firewall se configura para inspeccionar. El firewall clásico proporciona varios valores ajustables para proteger frente a los ataques de DoS. Los parámetros predeterminados heredados (de las imágenes de software anteriores a la versión 12.4(11)T) que se muestran en la tabla 1 pueden interferir con el correcto funcionamiento de la red si no se configuran para el nivel adecuado de actividad de la red en redes donde las velocidades de conexión exceden los valores predeterminados. La configuración de DoS se puede ver con el comando exec **show ip inspect config**, y la configuración se incluye con el resultado de **sh ip inspect all**.

CBAC utiliza los tiempos de espera y los umbrales para determinar cuánto tiempo debe

administrar la información de estado de una sesión, así como para determinar cuándo deben interrumpirse las sesiones que no se han establecido completamente. Estos tiempos de espera y umbrales se aplican globalmente a todas las sesiones.

Tabla 1 Límites de protección DoS predeterminados de firewall clásico		
Valor de protección DoS	Anterior a 12.4(11)T/12.4(10)	12.4(11)T/12.4(10) y posteriores
valor máximo incompleto	500	Ilimitado
valor mínimo incompleto	400	Ilimitado
valor alto de un minuto	500	Ilimitado
valor bajo de un minuto	400	Ilimitado
valor máximo de host incompleto tcp	50	Ilimitado

Los routers configurados para aplicar el firewall que reconoce VRF de Cisco IOS mantienen un conjunto de contadores para cada VRF.

El contador para "ip inspect one-minute high" y "ip inspect one-minute low" mantiene una suma de todos los intentos de conexión TCP, UDP y protocolo de mensajes de control de Internet (ICMP) en el minuto anterior a la operación del router, independientemente de si las conexiones se han realizado correctamente o no. Una velocidad de conexión en aumento puede indicar una infección de gusanos en una red privada o un intento de ataque de DoS contra un servidor.

Aunque no puede "inhabilitar" la protección DoS de su firewall, puede ajustar la protección DoS para que no surta efecto a menos que haya un gran número de conexiones semirabiertas en la tabla de sesiones del router de firewall.

Protección de firewall DoS

Siga este procedimiento para ajustar la protección DoS de su firewall a la actividad de su red:

1. Asegúrese de que su red no está infectada con virus o gusanos que puedan generar valores de conexión medio abiertos erróneamente grandes o tasas de intentos de conexión. Si su red no está "limpia", no hay forma de ajustar correctamente la protección DoS de su firewall. Debe observar la actividad de su red en un período de actividad habitual. Si ajusta los parámetros de protección de DoS de su red en un período de actividad de red baja o inactiva, los niveles de actividad normales probablemente excedan los parámetros de protección de DoS.
2. Establezca los valores altos máximos incompletos en valores muy altos:

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

Esto evita que el router proporcione protección DoS mientras observa los patrones de conexión de la red. Si desea dejar desactivada la protección de DoS, detenga este procedimiento ahora.**Nota:** Si su router ejecuta Cisco IOS Software Release 12.4(11)T o posterior, o 12.4(10) o posterior, no necesita elevar los valores predeterminados de la Protección DoS; ya se han fijado sus límites máximos de forma predeterminada.**Nota:** Si desea habilitar la prevención de denegación de servicio más agresiva específica del host TCP que incluye el inicio del bloqueo de la conexión a un host, debe establecer el tiempo de bloqueo especificado en el comando **ip inspect tcp max-complete host**

3. Borre las estadísticas de Cisco IOS Firewall con este comando:

   ```
   show ip inspect statistics reset
   ```

4. Deje el router configurado en este estado durante algún tiempo, tal vez hasta 24 a 48 horas, para que pueda observar el patrón de red durante al menos un día completo del ciclo de actividad de red típico.**Nota:** Mientras que los valores se ajustan a niveles muy altos, su red no se beneficia de la protección de DoS de IPS o firewall de Cisco IOS.
5. Después del período de observación, verifique los contadores de DoS con este comando:

   ```
   show ip inspect statistics
   ```

   Los parámetros que debe observar para ajustar la protección de DoS se resaltan en **negrita**:

   ```
   Packet inspection statistics
      [process switch:fast switch]
     tcp packets: [218314:7878692]
     udp packets: [501498:65322]
      packets: [376676:80455]
      packets: [5738:4042411]
     smtp packets: [11:11077]
     ftp packets: [2291:0]
   Interfaces configured for inspection 2
   Session creations since subsystem
      startup or last reset 688030
   Current session counts
      (estab/half-open/terminating) [0:0:0]
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   Last session created 00:00:05
   Last statistic reset never
   Last session creation rate 1
   Maxever session creation rate 330
   Last half-open session total 0
   TCP reassembly statistics
     received 46591 packets out-of-order; dropped 16454
     peak memory usage 48 KB; current usage: 0 KB
     peak queue length 16
   ```

6. Configure **ip inspect max-complete high** a un valor 25 por ciento superior al valor de semirreabierto de conteo de sesiones maxever indicado de su router. Un multiplicador de 1,25 ofrece un margen de maniobra del 25% por encima del comportamiento observado, por ejemplo:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   56 * 1.25 = 70
   ```

Configure

```
router(config)
   #ip inspect max-incomplete high 70
```

Nota: Este documento describe el uso de un multiplicador de 1,25 veces la actividad típica de su red para establecer límites para comprometer la protección de DoS. Si observa su red en los picos de actividad de red típicos, esto debe proporcionar un espacio suficiente para evitar la activación de la protección de DoS del router en todas las circunstancias excepto en las atípicas. Si su red detecta periódicamente grandes ráfagas de actividad de red legítima que exceden este valor, el router utiliza las capacidades de protección de DoS, lo que puede causar un impacto negativo en parte del tráfico de red. Debe monitorear los registros del router para detectar la actividad de DoS y ajustar el **ip inspect max-complete high** y/o **ip inspect one-minute high** limit para evitar activar DoS, después de determinar que los límites se encontraron como resultado de la actividad de red legítima. Puede reconocer la aplicación de protección DoS mediante la presencia de mensajes de registro como este:

7. Configure **ip inspect max-complete low** con el valor que su router muestra para su valor de semirrido máximo de conteo de sesiones, por ejemplo:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

Configure

```
router(config)
   #ip inspect max-incomplete low 56
```

8. El contador para **ip inspect one-minute high** y **one-minute low** mantiene una suma de todos los intentos de conexión TCP, UDP y protocolo de mensajes de control de Internet (ICMP) en el minuto anterior de la operación del router, independientemente de si las conexiones se han realizado correctamente o no. Una tasa de conexión en aumento puede indicar una infección de gusanos en una red privada o un intento de ataque de DoS contra un servidor. Se agregó una estadística de inspección adicional a la salida **show ip inspect statistics** en 12.4(11)T y 12.4(10) para revelar la marca de agua alta para la tasa de creación de sesión. Si ejecuta una versión de software del IOS de Cisco anterior a 12.4(11)T o 12.4(10), las estadísticas de inspección no contienen esta línea:

```
Maxever session creation rate [value]
```

Las versiones del software Cisco IOS anteriores a 12.4(11)T y 12.4(10) no mantienen un valor para la velocidad máxima de conexión de un minuto, por lo que debe calcular el valor que aplica en función de los valores de "número máximo de sesiones" observados. Las observaciones de varias redes que utilizan la inspección con estado de Cisco IOS Firewall Release 12.4(11)T en producción han demostrado que las tasas de creación de sesiones Maxever tienden a exceder la suma de los tres valores (establecidos, semirabiertos y terminados) en el "número máximo de sesiones" en aproximadamente un diez por ciento. Para calcular el valor bajo de un minuto de inspección ip, multiplique el valor "establecido" indicado por 1.1, por ejemplo:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

Configure

```
ip inspect one-minute low 328
```

Si el router ejecuta Cisco IOS Software Release 12.4(11)T o posterior, o 12.4(10) o posterior, simplemente puede aplicar el valor mostrado en la estadística de inspección "Maxever session create rate":

```
Maxever session creation rate 330
```

Configure

```
ip inspect one-minute low 330
```

9. Calcule y configure **ip inspect one-minute high**. El valor alto de un minuto de inspección ip debe ser un 25% mayor que el valor bajo de un minuto calculado, por ejemplo:
   ```
   ip inspect one-minute low (330) * 1.25 = 413
   ```
   Configure
   ```
   ip inspect one-minute high 413
   ```
   Nota: Este documento describe el uso de un multiplicador de 1,25 veces la actividad típica de su red para establecer límites para comprometer la protección de DoS. Si observa su red en los picos de actividad de red típicos, esto debe proporcionar un espacio suficiente para evitar la activación de la protección de DoS del router en todas las circunstancias excepto en las atípicas. Si su red detecta periódicamente grandes ráfagas de actividad de red legítima que exceden este valor, el router utiliza las capacidades de protección de DoS, lo que puede causar un impacto negativo en parte del tráfico de red. Debe monitorear los registros del router para detectar la actividad de DoS y ajustar el **ip inspect max-complete high** y/o **ip inspect one-minute high** limit para evitar activar DoS, después de determinar que los límites se encontraron como resultado de la actividad de red legítima. Puede reconocer la aplicación de protección DoS mediante la presencia de mensajes de registro como este:
10. Debe definir un valor para **ip inspect tcp max-complete host** de acuerdo con su conocimiento de la capacidad de sus servidores. Este documento no puede proporcionar pautas para la configuración de protección DoS por host, ya que este valor varía ampliamente según el rendimiento de hardware y software del host final. Si no está seguro de cuáles son los límites adecuados para configurar la protección de DoS, tiene dos opciones con las que definir los límites de DoS:La opción preferible es configurar la protección DoS basada en router por host a un valor alto (inferior o igual al valor máximo de 4.294.967.295) y aplicar la protección específica del host ofrecida por el sistema operativo de cada host o un sistema de protección contra intrusiones basado en host externo como Cisco Security Agent (CSA).Examine los registros de actividad y rendimiento de sus hosts de red y determine su velocidad máxima de conexión sostenible. Dado que el firewall clásico solo ofrece un contador global, debe aplicar el valor máximo que determine después de comprobar todos los hosts de la red para conocer sus velocidades de conexión máximas. Todavía es recomendable que utilice límites de actividad específicos del SO y un IPS basado en host como CSA.**Nota:** Cisco IOS Firewall ofrece una protección limitada frente a ataques dirigidos en vulnerabilidades específicas de aplicaciones y sistemas operativos. La protección DoS del firewall Cisco IOS no ofrece ninguna garantía de protección frente a riesgos en los servicios de host final que están expuestos a entornos potencialmente hostiles.
11. Supervise la actividad de protección de DoS de su red. Idealmente, debe utilizar un servidor syslog o, idealmente, una estación de supervisión y generación de informes (MARS) de Cisco para registrar los casos de detección de ataques de DoS. Si la detección se produce con mucha frecuencia, debe supervisar y ajustar los parámetros de protección de DoS.Para obtener más información sobre los ataques DoS TCP SYN, refiérase a Definición de Estrategias para Proteger contra los Ataques de Negación de Servicio TCP SYN.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems