# Cisco IOS Firewall/IPS clásico: Configurar el Control de acceso basado en el contexto (CBAC) para la protección del servicio negado

## Contenido



## Introducción

Este documento describe el procedimiento que ajusta para los parámetros de la negación de servicio (DOS) en el Firewall clásico del ® del Cisco IOS con el CBAC.

El CBAC proporciona las funciones avanzadas del filtrado de tráfico y se puede utilizar como parte integrante de su escudo de protección de la red.

El DOS refiere generalmente a la actividad de la red que intencionalmente o involuntariamente abruma a los recursos de red tales como ancho de banda de link PÁLIDO, tablas de conexiones del Firewall, memoria del host extremo, CPU, o capacidades de servicio. En un escenario de caso peor, la actividad DOS abruma (o apuntado) el recurso vulnerable a la punta que el recurso llega a ser inasequible, y prohíbe el acceso de la conectividad WAN o del servicio a los usuarios legítimos.

El Firewall Cisco IOS puede contribuir a la mitigación de la actividad DOS si mantiene los contadores del número de conexiones TCP “medio abiertas”, así como de la velocidad de conexión total a través del software del Firewall y de la prevención de intrusiones en el Firewall clásico (el **IP examina**) y el Firewall Zona-basado de la directiva.

## prerrequisitos

## Requisitos

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

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

# Antecedentes

Las conexiones entreabiertas son las conexiones TCP que no han completado el apretón de manos de tres vías SYN-SYN/ACK-ACK que es utilizado siempre por los pares TCP para negociar los parámetros de su conexión mutua. Un gran número de conexiones entreabiertas pueden ser indicativas de la actividad maliciosa, tal como DOS o ataques de denegación de servicio distribuido (DDoS). Un ejemplo de un tipo de ataque DOS es conducido por el software malévolo, intencional-desarrollado, tal como gusanos o los virus que infectan a los host múltiples en Internet e intentan abrumar a los servidores de Internet específicos con los Ataques SYN, donde un gran número de conexiones SYN son enviadas a un servidor por los host múltiples en Internet o dentro de la red privada de una organización. Los Ataques SYN representan un peligro a los servidores de Internet puesto que las tablas de conexiones de servidores se pueden cargar con los intentos de conexión “falsos” SYN que llegan más rápidamente que el servidor pueden ocuparse de las nuevas conexiones. Éste es un tipo de ataque DOS porque el número grande de conexiones en la lista de la conexión TCP del servidor de la víctima previene el acceso de usuario legítimo a los servidores de Internet de la víctima.

El Firewall Cisco IOS también mira las sesiones del User Datagram Protocol (UDP) con el tráfico en solamente una dirección como “medio abierto” porque muchas aplicaciones que utilizan el UDP para el transporte reconocen la recepción de los datos. Las Sesiones UDP sin el tráfico de retorno son probablemente indicativas de la actividad o de las tentativas DOS de conectar entre dos host, donde uno de los host ha llegado a ser insensible. Muchos tipos de tráfico UDP, tales como mensajes del registro, tráfico de administración de red SNMP, fluyendo el medio de video y de voz, y la señalización de tráfico, solamente tráfico del uso en una dirección para llevar su tráfico. Muchos de estos tipos de tráfico aplican la inteligencia específica a la aplicación de evitar que los modelos de tráfico unidireccional afecten al contrario al Firewall y al IPS de comportamiento DOS.

Antes del Cisco IOS Software Release 12.4(11)T y de 12.4(10), la inspección de paquetes stateful del Cisco IOS proporcionó a la protección contra los ataques DOS como valor por defecto cuando una regla del examen era aplicada. El Cisco IOS Software Release 12.4(11)T y 12.4(10) modificaron las configuraciones DOS del valor por defecto para no aplicar el protección DoS

automáticamente, pero los contadores de la actividad de la conexión son todavía activos. Cuando el protección DoS es activo, es decir, cuando los valores predeterminados se utilizan en más viejas versiones de software, o los valores se han ajustado al rango que afectan al tráfico, el protección DoS se habilita en la interfaz donde está aplicado el examen, en la dirección en la cual el Firewall es aplicado, para que los Protocolos de configuración de las políticas del firewall examinen. El protección DoS se habilita solamente en el tráfico de la red si el tráfico ingresa o deja una interfaz con el examen aplicado en la misma dirección del tráfico inicial (paquete SYN o primer paquete UDP) para una conexión TCP o una Sesión UDP.

El examen del Firewall Cisco IOS proporciona varios valores ajustables para proteger contra los ataques DOS. Las versiones de Cisco IOS Software antes de 12.4(11)T y de 12.4(10) tienen valores predeterminados DOS que puedan interferir con la operación de la red adecuada si no se configuran para el nivel adecuado de actividad de la red en las redes donde las velocidades de conexión exceden los valores por defecto. Estos parámetros permiten que usted configure las puntas en las cuales el protección DoS de su router de escudo de protección comienza a tomar el efecto. Cuando los contadores DOS de su router exceden el valor por defecto o los valores configurados, el router reajusta una vieja conexión entreabierta para cada nueva conexión que exceda el max-incomplete o los valores altos configurados del minuto hasta el número de descensos medio abiertos de las sesiones debajo de los valores bajos del max-incomplete. El router envía un mensaje de Syslog si se habilita la registración, y si un Sistema de prevención de intrusiones (IPS) se configura en el router, el router de escudo de protección envía un mensaje de firma DOS con el intercambio del evento del dispositivo de seguridad (SDEE). Si los parámetros DOS no se ajustan al comportamiento normal de su red, la actividad de la red normal puede accionar el mecanismo del protección DoS, que causa las fallas de la aplicación, el rendimiento de la red pobre, y CPU elevada la utilización en el router del Firewall Cisco IOS.

# Configurar

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

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

## Servicio negado que ajusta para el Firewall y el sistema de prevención de intrusiones clásicos del Cisco IOS Software (el IP examina)

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

El examen clásico del Firewall del Cisco IOS proporciona la protección contra el ataque DOS por abandono cuando un Firewall clásico es aplicado. El protección DoS se habilita en todas las interfaces donde está aplicado el examen, en la dirección en la cual el Firewall es aplicado, para cada servicio o protocolo que las políticas del firewall se configuren para examinar. El Firewall clásico proporciona varios valores ajustables para proteger contra los ataques DOS. Las configuraciones predeterminadas de la herencia (de las imágenes del software antes de la versión 12.4(11)T) mostradas en el cuadro 1 pueden interferir con la operación de la red adecuada si no se configuran para el nivel adecuado de actividad de la red en las redes donde las velocidades de conexión exceden los valores por defecto. Las configuraciones DOS se pueden ver con el **IP del** exec command show **examinan los config**, y las configuraciones se incluyen con la salida del **IP**

**sh examinan todos**.

El CBAC utiliza los descansos y los umbrales para determinar cuánto tiempo manejar la información del estado para una sesión, así como determinar cuando caer las sesiones que no se establecen completamente. Estos descansos y umbrales se aplican global a todas las sesiones.

| **Límites clásicos del protección DoS del valor por defecto del Firewall del cuadro 1** | | |
|---|---|---|
| **Valor del protección DoS** | **Antes de 12.4(11)T/12.4(10)** | **12.4(11)T/12.4(10) y posterior** |
| valor alto del max-incomplete | 500 | Ilimitado |
| valor bajo del max-incomplete | 400 | Ilimitado |
| valor alto del minuto | 500 | Ilimitado |
| valor bajo del minuto | 400 | Ilimitado |
| *valor del* host del max-incomplete tcp | 50 | Ilimitado |

El Routers configurado para aplicar el Firewall que reconoce VRF del Cisco IOS mantiene un conjunto de los contadores para cada VRF.

El contador para el “IP examina el alto del minuto” y el “IP examina el punto bajo del minuto” mantiene una suma de todo el TCP, UDP, y intentos de conexión del Internet Control Message Protocol (ICMP) dentro del minuto anterior de la operación del router, si las conexiones han sido acertadas o no. Una velocidad de conexión de levantamiento puede ser indicativa de una infección del gusano en una red privada o de un ataque frustrado DOS contra un servidor.

Mientras que usted no puede “inhabilitar” el protección DoS de su Firewall, usted puede ajustar el protección DoS de modo que no tome el efecto a menos que un gran número de conexiones entreabiertas estén presentes en la tabla de la sesión de su router de escudo de protección.

## Protección mediante firewall DOS

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

1. Esté seguro que su red no está infectada con los virus o los gusanos que pueden llevar a los valores erróneamente grandes de la conexión entreabierta o a las velocidades de conexión frustradas. Si su red no es “limpia,” no hay manera de ajustar correctamente el protección DoS de su Firewall. Usted debe observar la actividad de su red dentro de un período de actividad típica. Si usted ajusta las configuraciones del protección DoS de su red dentro de un período de actividad de la red baja u ociosa, los niveles de actividad normal exceden probablemente las configuraciones del protección DoS.
2. Fije los valores altos del max-incomplete mismo a los valores 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 al protección

DoS mientras que usted observa los modelos de la conexión de su red. Si usted desea dejar el protección DoS inhabilitado, ahora pare este procedimiento.**Nota:** Si su router ejecuta el Cisco IOS Software Release 12.4(11)T o Posterior, o 12.4(10) o más adelante, usted no necesita aumentar los valores predeterminados del protección DoS; se fijan ya a sus límites máximos por abandono.**Nota:** Si usted quiere habilitar la prevención host-específica más agresiva del servicio negado TCP que incluye el bloqueo del lanzamiento de conexión a un host, usted debe fijar el bloque-tiempo especificado en el **comando ip inspect tcp max-incomplete host**

3. Borre las estadísticas del Firewall Cisco IOS con este comando:
   **show ip inspect statistics reset**
4. Deje el router configurado en este estado por algún tiempo, quizás mientras 24 a 48 horas, así que usted puedan observar el modelo de la red encima por lo menos un día entero del ciclo de actividad de la red típica.**Nota:** Mientras que los valores se ajustan a los niveles muy altos, su red no se beneficia del Firewall Cisco IOS o del IPS de protección DoS.
5. Después del período de observación, marque los contadores DOS con este comando: **show ip inspect statistics** Los parámetros que usted debe observar con cuál para ajustar su protección DoS se resaltan en **intrépido**:
```
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. **El IP de la** configuración **examina el max-incomplete arriba a un** valor 25-percent más arriba que el valor medio abierto indicado de la cuenta de sesiones del maxever de su router. 1.25 un espacio libre de las ofertas 25-percent del multiplicador sobre la conducta observada, 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 de establecer los límites para dedicar el protección DoS. Si usted observa su red dentro de los picos de la actividad de la red típica, esto debe proporcionar la capacidad adecuada para evitar la activación del protección DoS del router bajo todos sino las circunstancias anormales. Si su red considera periódicamente las explosiones grandes de la actividad de la red legítima que exceden este valor, el router dedica las capacidades del protección DoS, que pueden causar un impacto negativo en algo del tráfico de la red. Usted debe monitorear sus registros del router para las detecciones de actividad DOS y ajustar el **IP examine el alto del max-incomplete** y/o el **IP examina los altos** límites del **minuto** para evitar accionar el DOS, después de que usted determine que los límites fueron encontrados como resultado de la actividad de la red legítima. Usted puede reconocer la aplicación del protección DoS por la presencia de

mensajes del registro tales como esto:

7. **El IP de la** configuración **examina el max-incomplete bajo al** valor que su router visualizó para su valor medio abierto de la cuenta de sesiones del maxever, 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 el **IP examina el alto del minuto** y el **punto bajo del minuto** mantiene una suma de todo el TCP, UDP, y intentos de conexión del Internet Control Message Protocol (ICMP) dentro del minuto anterior de la operación del router, si las conexiones han sido acertadas o no. Una velocidad de conexión de levantamiento puede ser indicativa de una infección del gusano en una red privada, o de un ataque frustrado DOS contra un servidor. Una estadística adicional del examen fue agregada al **IP de la demostración examina la** salida de las **estadísticas** en 12.4(11)T y 12.4(10) para revelar la marca de alta para la tarifa de la creación de sesión. Si usted funciona con una versión de Cisco IOS Software anterior que 12.4(11)T o 12.4(10), las estadísticas del examen no contienen esta línea:`Maxever session creation rate [value]`Las versiones de Cisco IOS Software antes de 12.4(11)T y de 12.4(10) no mantienen un valor para la velocidad de conexión del minuto del maxever del examen, así que usted debe calcular el valor que usted se aplica basado en “los valores observados de la cuenta de sesiones del maxever”. Las observaciones de varias redes que utilizan la inspección con estado de la versión 12.4(11)T del Firewall Cisco IOS en la producción han mostrado que las tarifas de la creación de sesión del maxever tienden a exceder la suma de los tres valores (establecido, medio abierto, y terminando) en la “cuenta de sesiones del maxever” por el áspero diez por ciento. Para calcular el IP examine el valor bajo del minuto, multiplican 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 el Cisco IOS Software Release 12.4(11)T o Posterior, o 12.4(10) o más adelante, usted puede aplicar simplemente el valor mostrado en “la estadística del examen de la tarifa de la creación de sesión del maxever”:`Maxever session creation rate 330`Configure`ip inspect one-minute low 330`
9. Calcule y el **IP de la** configuración **examina el alto del minuto**. El IP examina el valor alto del minuto debe ser 25-percent mayores que el valor bajo calculado del minuto, 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 de establecer los límites para dedicar el protección DoS. Si usted observa su red dentro de los picos de la actividad de la red típica, esto debe proporcionar la capacidad adecuada para evitar la activación del protección DoS del router bajo todos sino las circunstancias anormales. Si su red considera periódicamente las explosiones grandes de la actividad de la red legítima que exceden este valor, el router dedica las capacidades del protección DoS, que pueden causar un impacto negativo en algo del tráfico de la red. Usted debe monitorear sus registros del router para las detecciones de actividad DOS y ajustar el **IP examine el alto del max-incomplete** y/o el **IP examina los altos** límites del **minuto** para evitar accionar el DOS, después de que usted determine que los límites fueron encontrados como resultado de la actividad de la red legítima. Usted puede reconocer la aplicación del protección DoS por la presencia de mensajes del registro tales como esto:
10. Usted necesita definir un valor para el **IP examina el host del max-incomplete tcp** de acuerdo con su conocimiento de la capacidad de sus servidores. Este documento no puede proporcionar las guías de consulta para la configuración del protección DoS del por-host

puesto que este valor varía basado extensamente en el funcionamiento del hardware y software del host extremo. Si usted es incierto sobre los límites apropiados configurar para el protección DoS, usted tiene con eficacia dos opciones con las cuales definir el DOS limite:La opción preferible es configurar el protección DoS basado en el router del por-host a un valor alto (inferior o igual el valor máximo de 4,294,967,295), y aplica la protección host-específica ofrecida por el sistema operativo de cada host o un sistema basado en el host externo de la protección contra intrusos tal como Cisco Security Agent (CSA).Examine la actividad y el funcionamiento abre una sesión sus Host de red y determina su velocidad de conexión sostenible máxima. Puesto que el Firewall clásico ofrece solamente un contador global, usted debe aplicar el valor máximo que usted determina después de que usted marque todos sus Host de red para sus tarifas de la cantidad máxima de conexiones. Es todavía recomendable que usted utiliza los límites OS-específicos de la actividad y un IPS basado en el host tal como CSA.**Nota:** El Firewall Cisco IOS ofrece la protección limitada contra los ataques dirigidos en las vulnerabilidades específicas del sistema operativo y de la aplicación. El protección DoS del Firewall Cisco IOS no ofrece ninguna garantía de la protección contra el compromiso sobre los servicios de host extremo que se exponen a los entornos potencialmente hostiles.
11. Monitoree la actividad del protección DoS su red. Idealmente, usted debe utilizar a un servidor de Syslog, o idealmente, Cisco monitoreando y señalando las estaciones (MARTE) a los acontecimientos de registro de la Detección de ataque DOS. Si sucede la detección muy con frecuencia, usted necesita monitorear y ajustar sus parámetros del protección DoS.Para más información sobre los ataques DOS TCP SYN, refiera a definir las estrategias para proteger contra los establecimientos de rechazo del 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.

## Troubleshooting

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