

Uso del Firewall de Cisco IOS para permitir los subprogramas Java desde sitios conocidos mientras se niegan otros

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Denegar los subprogramas de Java de Internet](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Esta configuración de ejemplo muestra cómo utilizar Cisco IOS® Firewall para permitir subprogramas Java desde sitios de Internet especificados y denegar todos los demás. Este tipo de bloqueo deniega el acceso a los subprogramas Java que no están incrustados en un archivo archivado o comprimido. Cisco IOS Firewall se introdujo en las versiones 11.3.3.T y 12.0.5.T del software Cisco IOS. Sólo está presente cuando se compran determinados conjuntos de funciones.

Puede ver qué conjuntos de funciones de Cisco IOS soportan IOS Firewall con el [Software Advisor](#) ([sólo clientes registrados](#)) .

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Router 1751 de Cisco
- Versión c1700-k9o3sy7-mz.123-8.T.bin del software del IOS de Cisco

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

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Denegar los subprogramas de Java de Internet

Siga este procedimiento:

1. Cree listas de control de acceso (ACL).
2. Agregue los comandos **ip inspect http java** a la configuración.
3. Aplique los comandos **ip inspect** y **access-list** a la interfaz externa.**Nota:** En este ejemplo, la ACL 3 permite que los subprogramas Java provengan de un sitio descriptivo (10.66.79.236) mientras que implícitamente niega los subprogramas Java de otros sitios. Las direcciones mostradas en el exterior del router no son enrutables a Internet porque este ejemplo se configuró y probó en un laboratorio.**Nota:** La **lista de acceso ya no es necesaria** para ser aplicada en la interfaz externa si utiliza Cisco IOS Software Release 12.3.4T o posterior. Esto se documenta en la nueva [función de omisión de ACL de firewall](#).

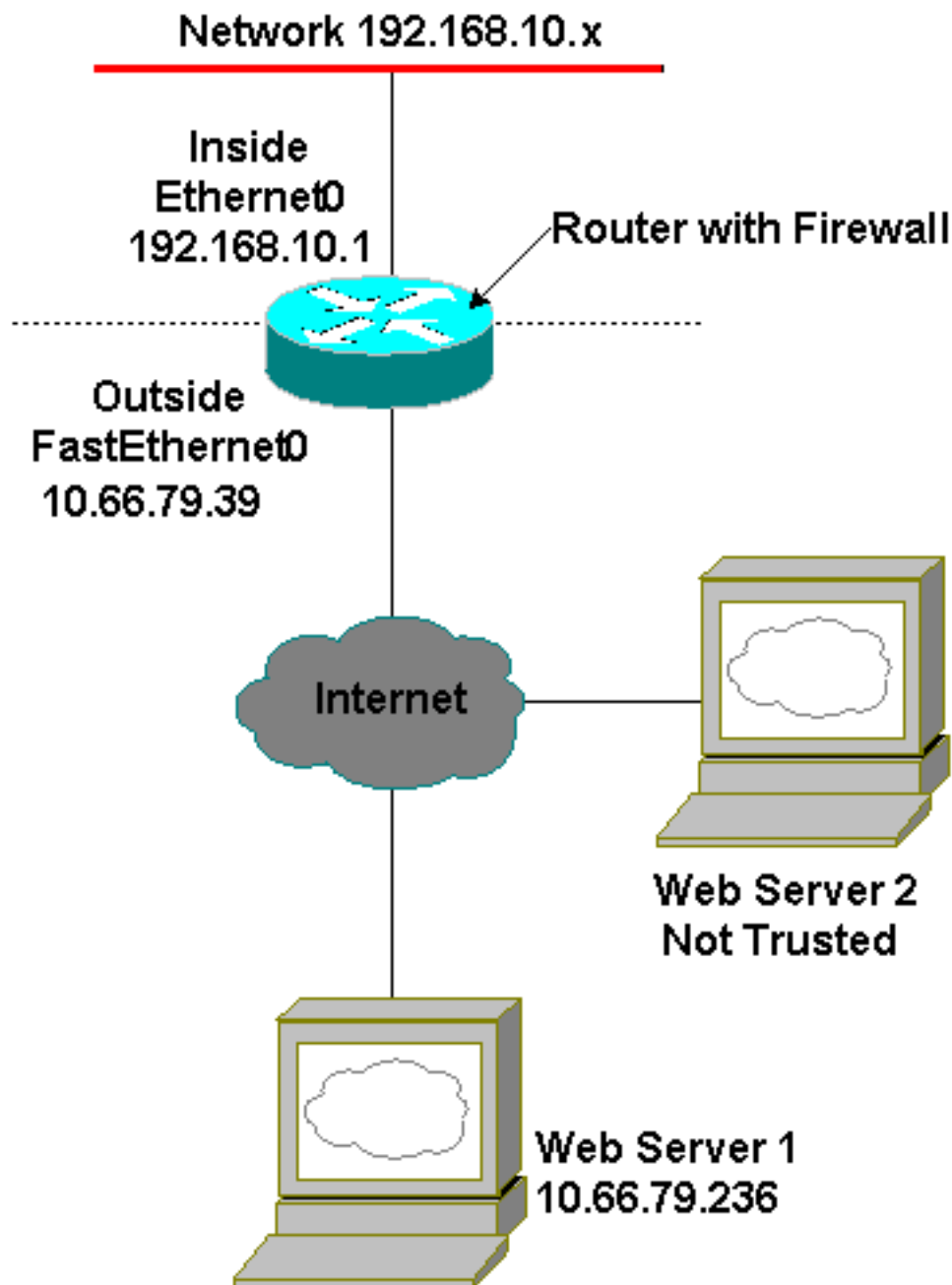
Configurar

Esta sección le presenta la información que puede utilizar para configurar las características que describe este documento.

Nota: Para encontrar información adicional sobre los comandos que utiliza este documento, refiérase a la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



[Configuraciones](#)

Este documento usa esta configuración:

Configuración del router

```

Current configuration : 1224 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Australia
!
boot-start-marker
boot-end-marker
!

```

```
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
ip cef
ip inspect name firewall tcp
ip inspect name firewall udp

!--- ACL used for Java. ip inspect name firewall http
java-list 3 audit-trail on
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet0/0
  ip address 10.66.79.39 255.255.255.224

!--- ACL used to block inbound traffic !--- except that
permitted by inspects. !--- This is no longer required
on Cisco IOS Software !--- Release 12.3.4T or later. ip
access-group 100 in
  ip nat outside
  ip inspect firewall out
  ip virtual-reassembly
  speed auto
!
interface Serial10/0
  no ip address
  shutdown
  no fair-queue
!
interface Ethernet1/0
  ip address 192.168.10.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
  half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.33
no ip http server
no ip http secure-server

!--- ACL used for Network Address Translation (NAT). ip
nat inside source list 1 interface FastEthernet0/0
overload
!

!--- ACL used for NAT. access-list 1 permit 192.168.10.0
0.0.0.255

!--- ACL used for Java. access-list 3 permit
10.66.79.236

!--- ACL used to block inbound traffic !--- except that
permitted by inspects. !--- This is no longer required
on Cisco IOS !--- Software Release 12.3.4T or later.
access-list 100 deny ip any any
!
!
control-plane
!
```

```
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  login  
!  
end
```

Verificación

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show ip inspect sessions [detail]**—Muestra las sesiones existentes actualmente controladas e inspeccionadas por Cisco IOS Firewall. La palabra clave opcional **detail** muestra información adicional sobre estas sesiones.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Comandos para resolución de problemas

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar **comandos debug**, consulte [Información Importante sobre Comandos Debug](#).

- **no ip inspect alert-off:** habilita los mensajes de alerta de Cisco IOS Firewall. Si http denies está configurado, puede verlos desde la consola.
- **debug ip inspect:** muestra mensajes acerca de los eventos de Cisco IOS Firewall.

Este es un ejemplo de resultado de debug del comando **debug ip inspect detail** después de un intento de conectar con servidores web en 10.66.79.236 y otro sitio no confiable que tiene subprogramas Java (como se define en la ACL).

Registro Denegado de Java

```
*Jan 12 21:43:42.919: %FW-6-SESS_AUDIT_TRAIL_START:  
  Start http session: initiator (192.168.10.2:2673)  
  -- responder (128.138.223.2:80)  
*Jan 12 21:43:43.571: %FW-3-HTTP_JAVA_BLOCK:  
  JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2673).  
*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL:  
  Stop http session: initiator (192.168.10.2:2673) sent 276 bytes  
  -- responder (128.138.223.2:80) sent 0 bytes
```

*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2674)
-- responder (128.138.223.2:80)
*Jan 12 21:43:43.823: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2672) sent 486 bytes
-- responder (10.66.79.236:80) sent 974 bytes
*Jan 12 21:43:44.007: %FW-3-HTTP_JAVA_BLOCK:
JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2674).
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2674) sent 276 bytes
-- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2675)
-- responder (128.138.223.2:80)
*Jan 12 21:43:44.439: %FW-3-HTTP_JAVA_BLOCK:
JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2675).
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2675) sent 233 bytes
-- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2676)
-- responder (128.138.223.2:80)
*Jan 12 21:43:44.879: %FW-3-HTTP_JAVA_BLOCK:
JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2676).
*Jan 12 21:43:44.879: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2676) sent 233 bytes
-- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.899: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2677)
-- responder (128.138.223.2:80)

Registro permitido de JAVA

Jan 12 21:44:12.143: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2685)
-- responder (10.66.79.236:80)
*Jan 12 21:44:12.343: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2686)
-- responder (10.66.79.236:80)
*Jan 12 21:44:17.343: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2685) sent 626 bytes
-- responder (10.66.79.236:80) sent 533 bytes
*Jan 12 21:44:17.351: %FW-6-SESS_AUDIT_TRAIL:
Stop http session: initiator (192.168.10.2:2686) sent 314 bytes
-- responder (10.66.79.236:80) sent 126 bytes
*Jan 12 21:44:23.803: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2687)
-- responder (10.66.79.236:80)
*Jan 12 21:44:27.683: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2691)
-- responder (10.66.79.236:80)
*Jan 12 21:44:28.411: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2692)
-- responder (10.66.79.236:80)
*Jan 12 21:44:28.451: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2693)
-- responder (10.66.79.236:80)
*Jan 12 21:44:28.463: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2694)
-- responder (10.66.79.236:80)
*Jan 12 21:44:28.475: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2695)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.487: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2696)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.499: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2697)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.515: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2698)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.527: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2699)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.543: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2700)
-- responder (10.66.79.236:80)

*Jan 12 21:44:28.551: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2701)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.075: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2734)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.135: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2735)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.155: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2736)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.159: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2737)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.215: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2739)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.231: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2740)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.251: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2742)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.395: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2747)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.403: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2748)
-- responder (10.66.79.236:80)

*Jan 12 21:44:29.423: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2749)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.091: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2798)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.095: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2799)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.115: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2800)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.119: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2801)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.123: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2802)
-- responder (10.66.79.236:80)

*Jan 12 21:44:30.191: %FW-6-SESS_AUDIT_TRAIL_START:

Start http session: initiator (192.168.10.2:2803)
-- responder (10.66.79.236:80)
*Jan 12 21:44:30.219: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2804)
-- responder (10.66.79.236:80)
*Jan 12 21:44:30.399: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2805)
-- responder (10.66.79.236:80)
*Jan 12 21:44:30.411: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2806)
-- responder (10.66.79.236:80)
*Jan 12 21:44:30.423: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2807)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.103: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2843)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.115: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2844)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.127: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2845)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.139: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2846)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.147: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2847)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.159: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2848)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.171: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2849)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.183: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2850)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.195: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2851)
-- responder (10.66.79.236:80)
*Jan 12 21:44:31.203: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2852)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.107: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2908)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.123: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2909)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.143: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2910)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.163: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2911)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.175: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2912)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.187: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2913)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.199: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2914)


```
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.211: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2915)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.223: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2916)
-- responder (10.66.79.236:80)
*Jan 12 21:44:32.235: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2917)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.151: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2982)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.163: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2983)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.175: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2984)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.187: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2985)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.199: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2986)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.211: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2987)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.223: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2988)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.235: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2989)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.251: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2990)
-- responder (10.66.79.236:80)
*Jan 12 21:44:33.259: %FW-6-SESS_AUDIT_TRAIL_START:
Start http session: initiator (192.168.10.2:2991)
-- responder (10.66.79.236:80)
```

[Información Relacionada](#)

- [Página de soporte de firewall de IOS](#)
- [Control de acceso basado en contexto: Introducción y configuración](#)
- [Mejora de seguridad de los routers de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)