

Usando el Firewall Cisco IOS para permitir las Javas Applet de los sitios conocidos mientras que niega otros

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Niegue las Javas Applet de Internet](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración de muestra demuestra cómo utilizar el Firewall de Cisco IOS® para permitir los subprogramas java de los sitios de Internet especificados, y niega todos los demás. Este tipo de bloqueo niega el acceso a los subprogramas java que no se integran en haber archivado o un archivo comprimido. El Firewall Cisco IOS fue introducido en los Cisco IOS Software Releases 11.3.3.T y 12.0.5.T. Está solamente presente en que compran a ciertos conjuntos de características.

Usted puede ver qué conjuntos de características de Cisco IOS soportan el escudo de protección IOS con el [Software Advisor \(clientes registrados solamente\)](#).

[prerrequisitos](#)

[Requisitos](#)

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 de Cisco IOS Software c1700-k9o3sy7-mz.123-8.T.bin

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](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[Niegue las Javas Applet de Internet](#)

Siga este procedimiento:

1. Cree el 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 exterior**. **Nota:** En este ejemplo, el ACL 3 permite las Javas Applet de un sitio cómodo (10.66.79.236) mientras que niega implícito las Javas Applet de otros sitios. Los direccionamientos mostrados en el exterior del router no son Enrutable por Internet porque este ejemplo fue configurado y probado en un laboratorio. **Nota: La lista de acceso se requiere no más para ser aplicada en la interfaz exterior si usted utiliza el Cisco IOS Software Release 12.3.4T o Posterior.** Esto se documenta en la nueva [característica de puente del Firewall ACL](#).

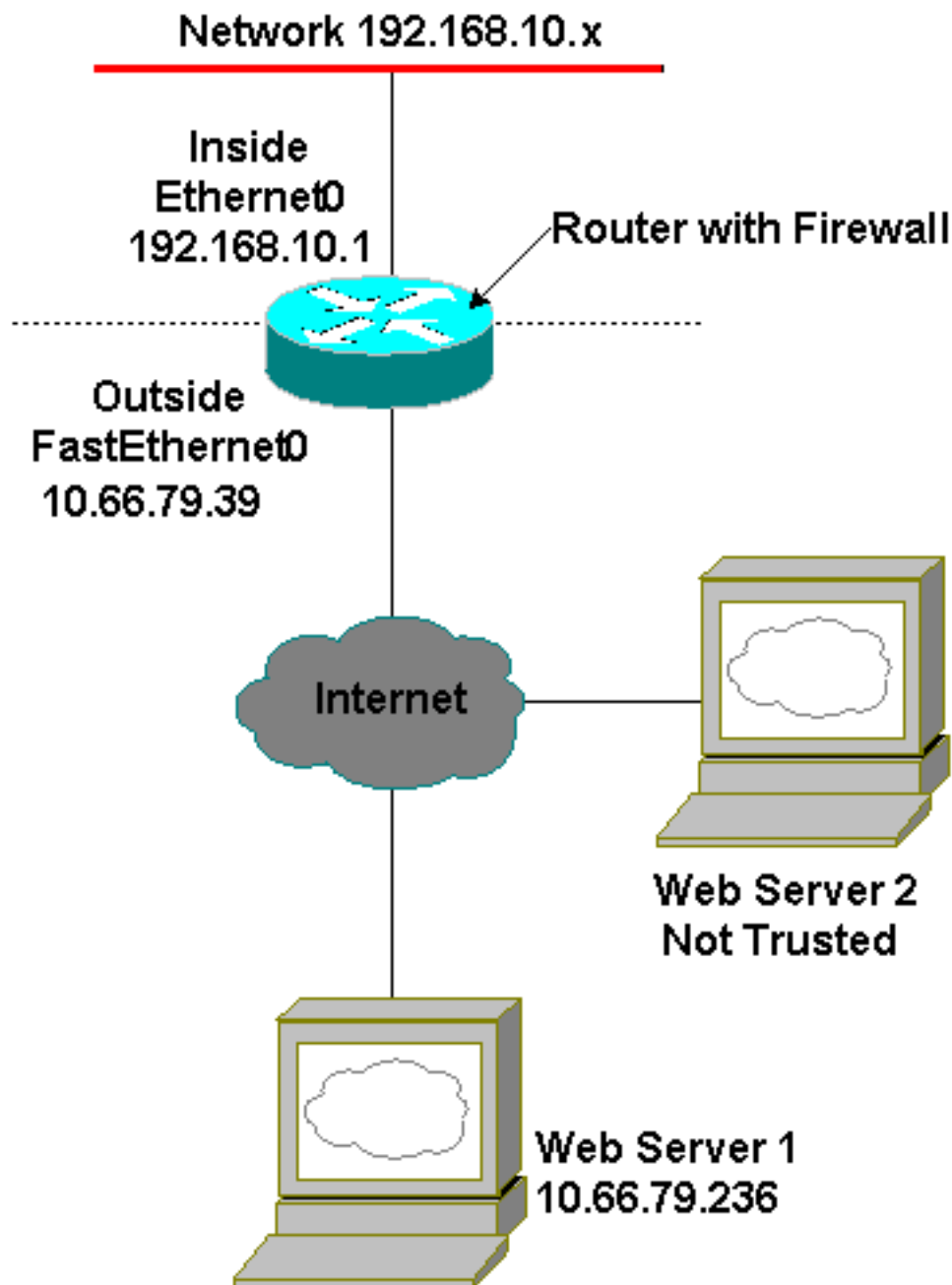
[Configurar](#)

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

Nota: Para encontrar la información adicional en los comandos que este documento utiliza, que refiera a la [herramienta de búsqueda de comandos \(clientes registrados solamente\)](#).

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración:

Configuración del router
<pre> 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 </pre>

```
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 Serial0/0 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]** — Sesiones existentes de las demostraciones seguidas y examinadas actualmente por el Firewall Cisco IOS. **El detalle de la palabra clave optativa** muestra la información adicional sobre estas sesiones.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas 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 un comando de depuración, consulte Información importante sobre comandos de depuración.](#)

- **ningún IP examina la alerta-apagado** — Mensajes de alerta del Firewall Cisco IOS de los permisos. Si se configura el HTTP niega, usted puede verlos de la consola.
- **debug ip inspect** — Muestra los mensajes sobre los eventos del Firewall Cisco IOS.

Éste es ejemplo de salida del debug del **comando debug ip inspect detail** después de que una tentativa de conectar con los servidores Web en 10.66.79.236 y otro sitio untrusted que tenga Javas Applet (según lo definido en el ACL).

Registro negado Javas

```
*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 JAVAS

```
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](#)