

Uso del firewall Cisco IOS per consentire le applet Java da siti noti e negare ad altri

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Nega applet Java da Internet](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questa configurazione di esempio viene illustrato come utilizzare Cisco IOS® Firewall per consentire le applet Java da siti Internet specificati e negarne il download a tutti gli altri. Questo tipo di blocco nega l'accesso alle applet Java non incorporate in un file archiviato o compresso. Cisco IOS Firewall è stato introdotto nel software Cisco IOS versioni 11.3.3.T e 12.0.5.T. È presente solo quando vengono acquistati determinati set di funzionalità.

Per verificare quali set di funzionalità di Cisco IOS supportano IOS Firewall, usare [Software Advisor](#) (solo utenti [registrati](#)).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 1751 router

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Nega applet Java da Internet

Attenersi alla procedura seguente:

1. Creare elenchi di controllo di accesso (ACL).
2. Aggiungere i comandi **ip inspect http java** alla configurazione.
3. Applicare i comandi **ip inspect** e **access-list** all'interfaccia esterna. **Nota:** nell'esempio, ACL 3 consente l'uso di applet Java da un sito descrittivo (10.66.79.236) mentre nega implicitamente l'uso di applet Java da altri siti. Gli indirizzi mostrati all'esterno del router non possono essere indirizzati a Internet perché l'esempio è stato configurato e testato in un laboratorio. **Nota:** l'**elenco degli accessi non deve più** essere applicato all'interfaccia esterna se si usa il software Cisco IOS versione 12.3.4T o successive. Questa condizione viene documentata nella nuova [funzionalità di bypass degli ACL del firewall](#).

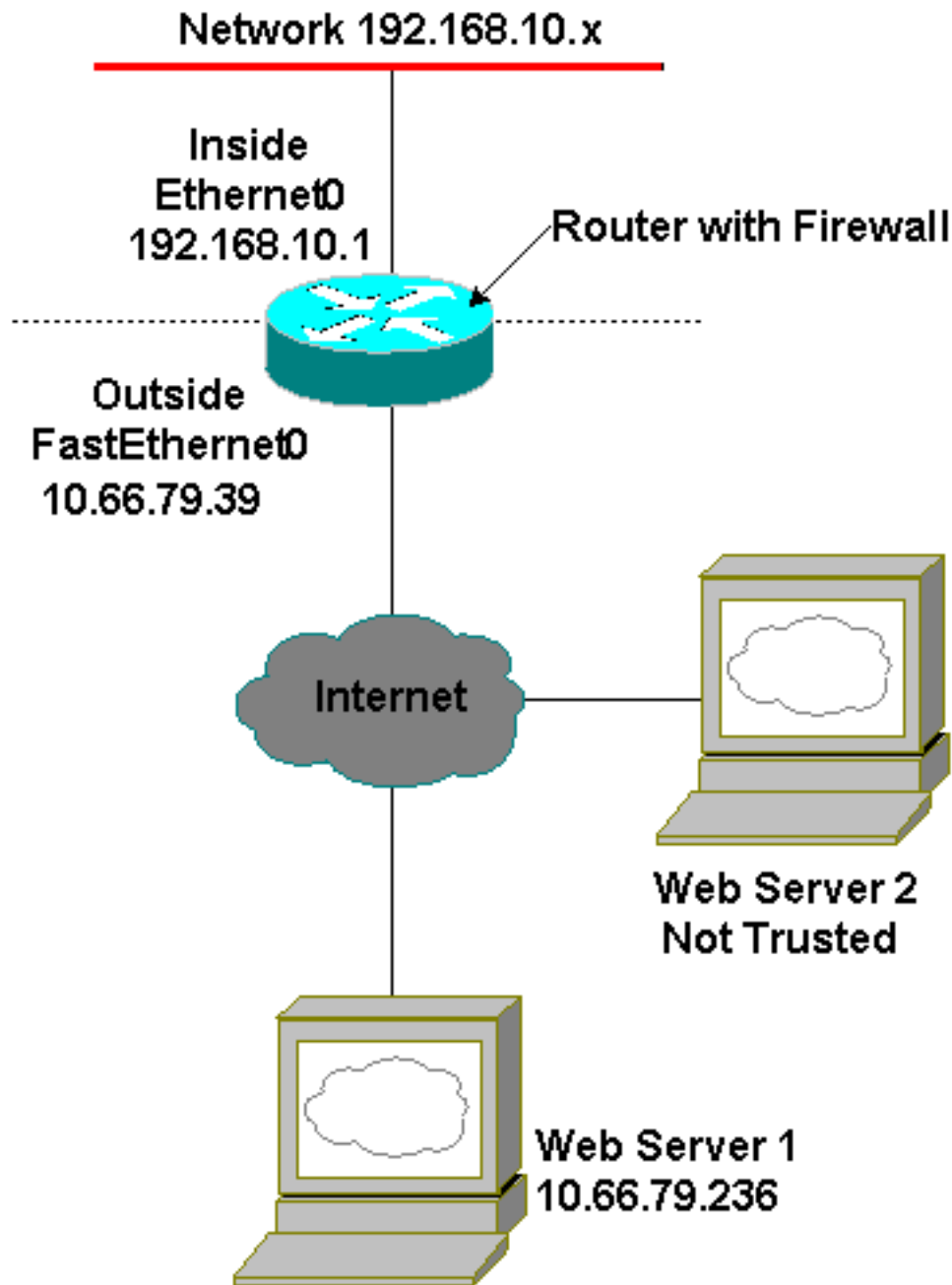
Configurazione

In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le funzionalità descritte nel documento.

Nota: per ulteriori informazioni sui comandi usati da questo documento, consultare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



[Configurazioni](#)

Nel documento viene usata questa configurazione:

Configurazione 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show ip inspect sessions [detail]**: visualizza le sessioni esistenti attualmente tracciate e ispezionate da Cisco IOS Firewall. La parola chiave opzionale **detail** mostra ulteriori informazioni su queste sessioni.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **no ip inspect alert-off**: abilita i messaggi di avviso di Cisco IOS Firewall. Se sono stati configurati i negati http, è possibile visualizzarli dalla console.
- **debug ip inspect**: visualizza i messaggi relativi agli eventi di Cisco IOS Firewall.

In questo esempio, i risultati del comando **debug ip inspect detail** vengono restituiti dopo un tentativo di connessione ai server Web nella versione 10.66.79.236 e a un altro sito non attendibile con applet Java (come definito nell'ACL).

Registro negato 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 JAVA consentito

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)
```

[Informazioni correlate](#)

- [Pagina di supporto di IOS Firewall](#)
- [Controllo degli accessi basato sul contesto: Introduzione e configurazione](#)
- [Miglioramento della sicurezza sui router Cisco](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)