Cisco IOS Firewall을 사용하여 알려진 사이트의 Java 애플릿을 허용하고 나머지는 거부함

목차

소개

이 샘플 컨피그레이션에서는 Cisco IOS® Firewall을 사용하여 지정된 인터넷 사이트의 Java 애플릿을 허용하고 다른 모든 애플릿을 거부하는 방법을 보여 줍니다. 이러한 차단 유형은 아카이브되거나 압축된 파일에 포함되지 않은 Java 애플릿에 대한 액세스를 거부합니다. Cisco IOS Firewall은 Cisco IOS Software 릴리스 11.3.3.T 및 12.0.5.T에 도입되었습니다. 특정 기능 세트를 구매하는 경우에만 표시됩니다.

Software Advisor를 통해 IOS 방화벽을 지원하는 Cisco IOS 기능 집합을 확인할 수 있습니다(등록된 고객만 해당).

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 1751 라우터
- Cisco IOS 소프트웨어 릴리스 c1700-k9o3sy7-mz.123-8.T.bin

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

인터넷에서 Java 애플릿 거부

다음 절차를 수행합니다.

1. ACL(Access Control List)을 생성합니다.
2. **ip inspect http java** 명령을 컨피그레이션에 추가합니다.
3. **ip inspect** 및 **access-list** 명령을 외부 인터페이스에 적용합니다.**참고:** 이 예에서 ACL 3은 친숙한 사이트(10.66.79.236)에서 Java Applet을 허용하지만 다른 사이트에서 Java Applet을 암시적으로 거부합니다. 이 예는 Lab에서 구성 및 테스트되었으므로 라우터 외부에 표시된 주소는 인터넷 라우팅이 불가능합니다.**참고:** Cisco IOS Software Release 12.3.4T 이상을 사용하는 경우 **액세스** 목록을 외부 인터페이스에 적용할 필요가 **없습니다**. 이는 새로운 방화벽 ACL 바이패스 기능에 설명되어 있습니다.

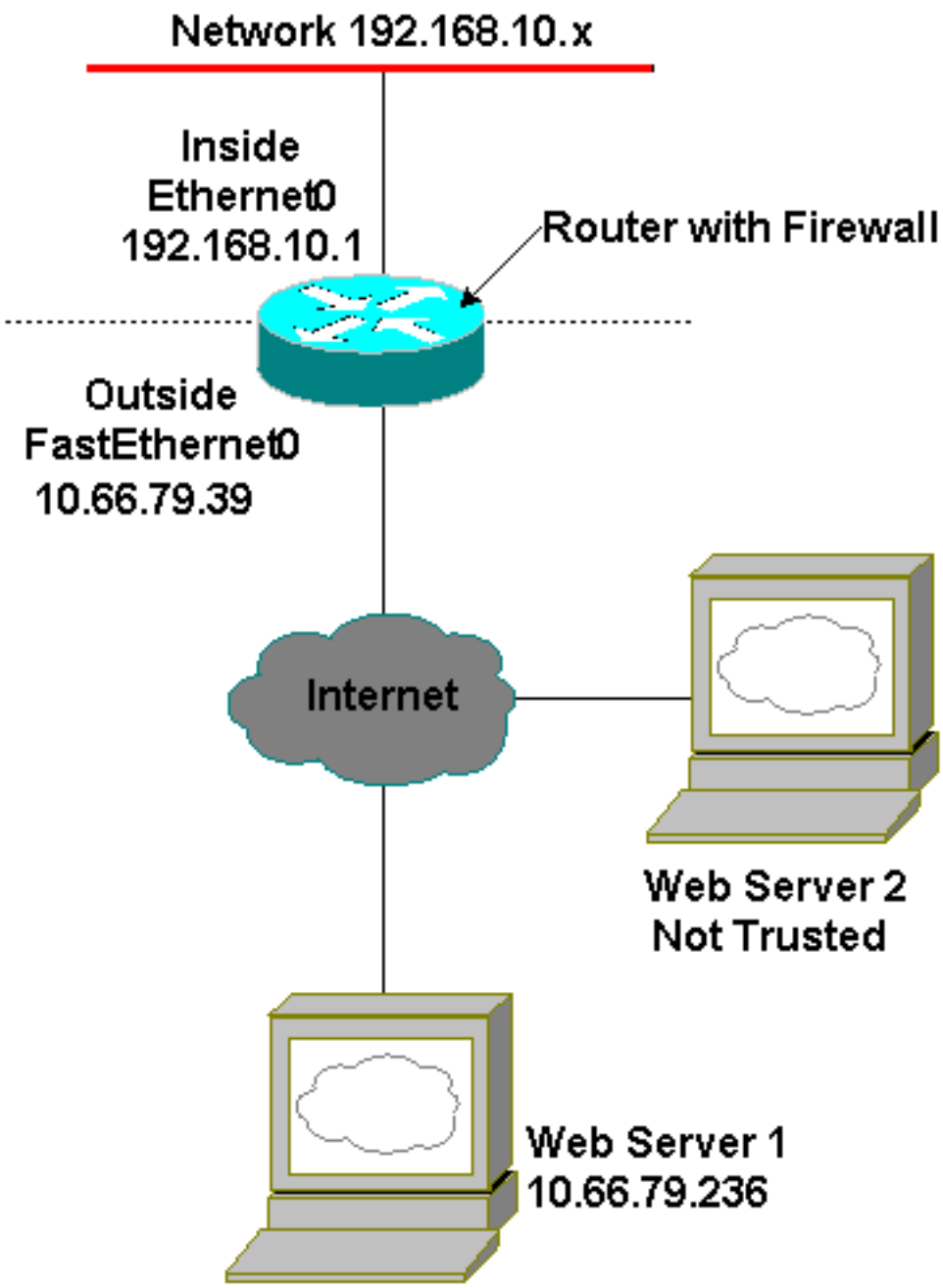
구성

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 사용할 수 있는 정보를 제공합니다.

참고: 이 문서에서 사용하는 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 참조하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

라우터 컨피그레이션

```
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 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
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show ip inspect sessions *[detail]*—**Cisco IOS Firewall에서 현재 추적 및 검사하는 기존 세션을 표시합니다. 선택적 키워드 **detail은** 이러한 세션에 대한 추가 정보를 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **no ip inspect alert-off** - Cisco IOS Firewall 알림 메시지를 활성화합니다. http 거부가 구성된 경우 콘솔에서 볼 수 있습니다.
- **debug ip inspect** - Cisco IOS Firewall 이벤트에 대한 메시지를 표시합니다.

이는 ACL에 정의된 대로 10.66.79.236의 웹 서버 및 Java Applet이 있는 또 다른 신뢰할 수 없는 사이트에 연결을 시도한 후 **debug ip inspect detail** 명령의 샘플 디버그 출력입니다.

Java 거부 로그

```
*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)
```

JAVA 허용 로그

```
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)
```

관련 정보

- IOS 방화벽 지원 페이지
- 컨텍스트 기반 액세스 제어: 소개 및 구성
- Cisco 라우터의 보안 개선
- 기술 지원 및 문서 – Cisco Systems