Использование брандмауэра Cisco IOS для того, чтобы разрешить приложения Java от известных сайтов и запретить остальные

Содержание

Введение

Этот пример конфигурации демонстрирует, как использовать Cisco IOS® Firewall, чтобы позволить приложения Java от указанных сайтов и запретить всех других. Этот тип блокирования запрещает доступ к приложениям Java, которые не встроены в заархивированный или сжатый файл. Межсетевой экран Cisco IOS был представлен в Cisco IOS Software Release 11.3.3. T и 12.0.5. T. Когда определенные наборы функций куплены, это только присутствует.

Вы видите, какие наборы функций Cisco IOS поддерживают Межсетевой экран IOS с Software Advisor (только зарегистрированные клиенты).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Маршрутизатор Cisco 1751
- Cisco IOS Software Release c1700-k9o3sy7-mz.123-8. T. bin

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Запретите приложения Java из Интернета

Придерживайтесь следующего порядка действий:

1. Создайте списки контроля доступа (ACL).
2. Добавьте **команды ip inspect http java** к конфигурации.
3. Примените **ip inspect** и **команды access-list** к внешнему интерфейсу.**Примечание:** В данном примере ACL 3 позволяет приложения Java от дружественного узла (10.66.79.236), в то время как это неявно запрещает приложения Java от других узлов. Адреса, показанные за пределами маршрутизатора, не Интернет-маршрутизируемы, потому что данный пример был настроен и протестирован в лабораторной работе.**Примечание: Access-list больше не требуется, чтобы** быть примененным на внешний интерфейс при использовании Cisco IOS Software Release 12.3.4T или позже. Это задокументировано в новую Функцию Обхода ACL Межсетевого экрана.

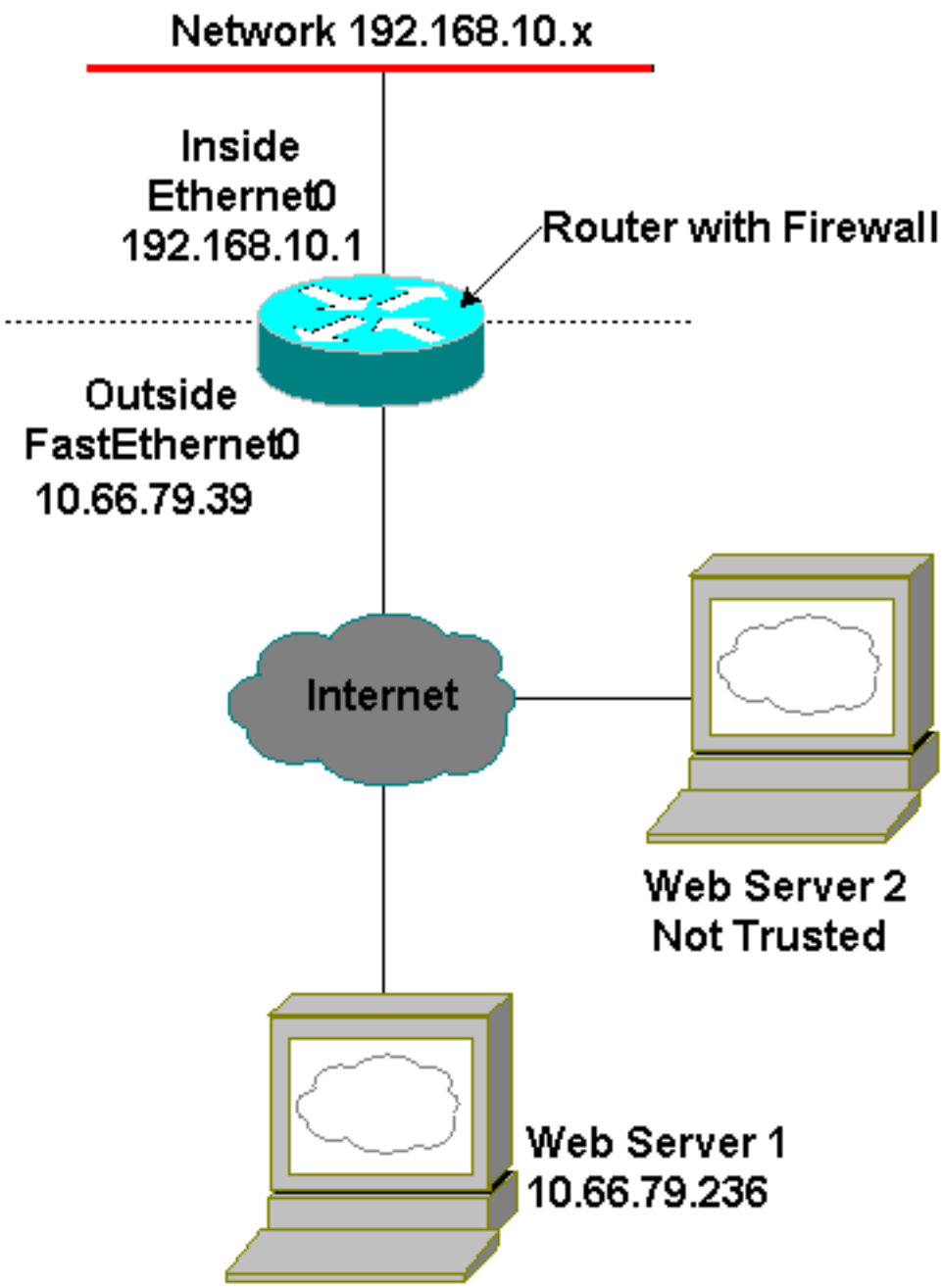
Настройка

В данном разделе приводятся сведения о настройке функций, описанных в этом документе.

Примечание: Для обнаружения дополнительных сведений об использовании этого документа команд обратитесь к Средству поиска команд Command Lookup Tool (только зарегистрированные клиенты).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

В данном документе используется следующая конфигурация:

Маршрутизатор Configuraton
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
```

Проверка

В данном разделе содержатся сведения для проверки правильности конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- *show ip inspect sessions [detail]* — Показывает существующие сеансы, в настоящее время отслеживаемые и осмотренные межсетевым экраном Cisco IOS. **Подробность** дополнительного ключевого слова показывает дополнительные сведения об этих сеансах.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Команды для устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику

выходных данных команды show.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- **предупреждение no ip inspect - прочь** — Включает сигнальные сообщения межсетевого экрана Cisco IOS. Если http запрещает, настроены, можно просмотреть их от консоли.
- **debug ip inspect** — Показывает сообщения о событиях Cisco IOS Firewall.

Это - пример отладочных выходных данных от **команды debug ip inspect detail** после попытки соединиться с Web-серверами на 10.66.79.236 и другой недоверяемый узел, который имеет приложения Java (как определено на ACL).

Java запрещенный журнал

```
*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 разрешенный журнал

```
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)
```

Дополнительные сведения

- Страница поддержки межсетевого экрана IOS
- Контроль доступа на основе контекста: Введение и конфигурация
- Повышение уровня безопасности маршрутизаторов Cisco
- Cisco Systems – техническая поддержка и документация