

Using the Cisco IOS Firewall to Allow Java Applets From Known Sites while Denying Others

Document ID: 13815

Introduction

Prerequisites

Requirements

Components Used

Conventions

Deny Java Applets from the Internet

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This sample configuration demonstrates how to use the Cisco IOS® Firewall to allow Java applets from specified Internet sites, and deny all others. This type of blocking denies access to Java applets that are not embedded in an archived or compressed file. Cisco IOS Firewall was introduced in Cisco IOS Software Releases 11.3.3.T and 12.0.5.T. It is only present when certain feature sets are purchased.

You can see which Cisco IOS feature sets support IOS Firewall with the Software Advisor (registered customers only) .

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

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

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Deny Java Applets from the Internet

Follow this procedure:

1. Create access control lists (ACLs).
2. Add **ip inspect http java** commands to the configuration.
3. Apply **ip inspect** and **access-list** commands to the outside interface.

Note: In this example, ACL 3 allows Java Applets from a friendly site (10.66.79.236) while it implicitly denies Java Applets from other sites. Addresses shown on the outside of the router are not Internet-routable because this example was configured and tested in a lab.

Note: The **access-list** is **no longer required** to be applied on the outside interface if you use Cisco IOS Software Release 12.3.4T or later. This is documented in the new Firewall ACL Bypass Feature.

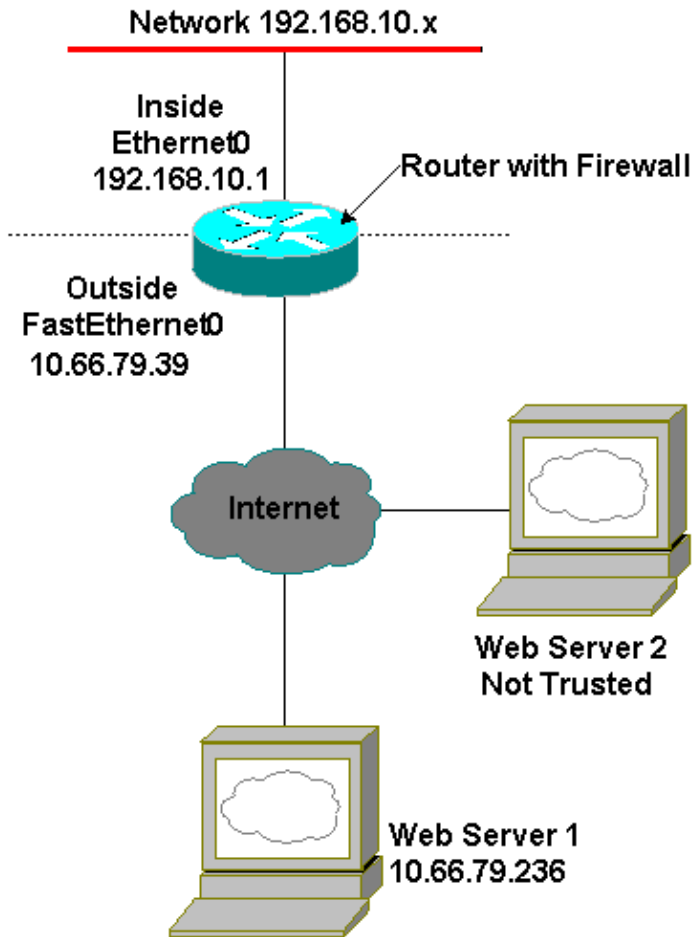
Configure

This section presents you with the information you can use in order to configure the features this document describes.

Note: In order to find additional information on the commands this document uses, refer to the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

This document uses this configuration:

Router Configuraton
<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 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 </pre>

```
!--- 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
```

Verify

This section provides information you can use in order to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show ip inspect sessions [detail]** Shows existing sessions currently tracked and inspected by the Cisco IOS Firewall. The optional keyword **detail** shows additional information about these sessions.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

- **no ip inspect alert-off** Enables Cisco IOS Firewall alert messages. If http denies are configured, you can view them from the console.
- **debug ip inspect** Shows messages about Cisco IOS Firewall events.

This is sample debug output from the **debug ip inspect detail** command after an attempt to connect to web servers on 10.66.79.236 and another untrusted site that has Java Applets (as defined on the ACL).

Java Denied Log

```
*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 Permitted Log

```
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)

```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [IOS Firewall Support Page](#)
- [IOS Firewall in IOS Documentation](#)
- [Context-Based Access Control: Introduction and Configuration](#)
- [Improving Security on Cisco Routers](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 15, 2006

Document ID: 13815