# e Cisco IOS Firewall to Allow Java Applets From Known Sites w

# Table of Contents

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

## Introduction

This sample configuration demonstrates how to use the Context−based Access Control (CBAC) feature of the Cisco IOS Firewall to allow Java applets from specified sites from the Internet, while denying 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 11.3.3.T and 12.0.5.T, and is only present when certain feature sets are purchased.

You can see which Cisco IOS feature sets support IOS Firewall by using Software Advisor, which is linked from the Cisco TAC Tools for Security Technologies page. To use Software Advisor, you must be a registered user and you must be logged in.

### To Deny Java Applets from the Internet:

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.

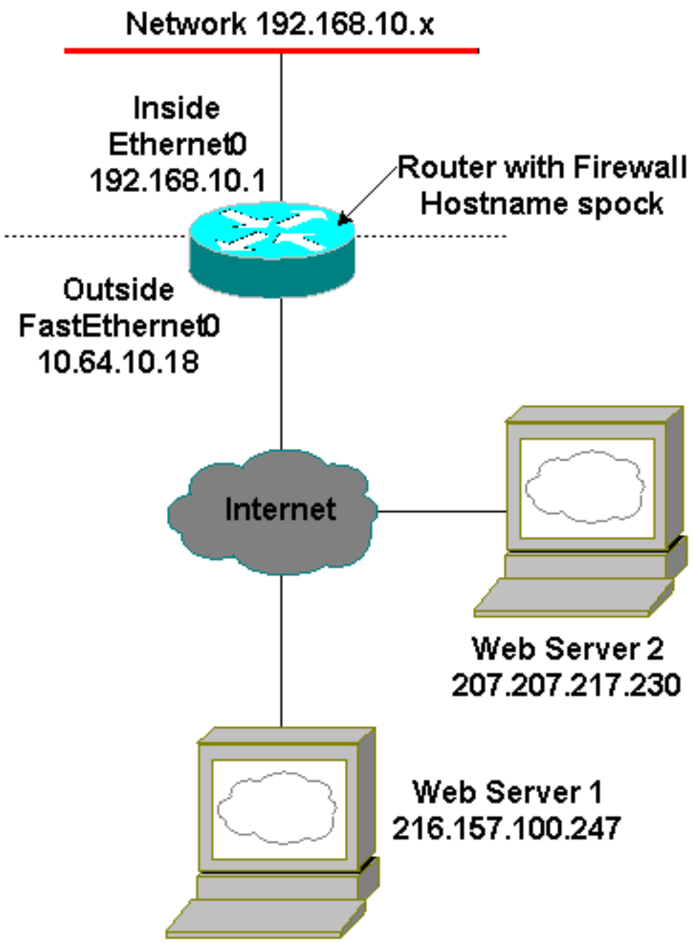
**Note:** In this example, ACL 3 allows Java from a friendly site (216.157.100.247) while implicitly denying Java from other sites. Addresses shown on the outside of the router are not Internet−routable because this example was configured and tested in a lab.

### Hardware and Software Versions

This configuration was developed and tested using the software and hardware versions below.

- Cisco 1700 router
- Cisco IOS Software version c1700−o3sy756i−mz.121−5.yB1.bin

## Network Diagram



**Router A Configuraton**

```
Current configuration : 1110 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname spock
!
no logging buffered
logging rate-limit console 10 except errors
!
memory-size iomem 25
ip subnet-zero
!
no ip finger
no ip domain-lookup
!
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 audit notify log
ip audit po max-events 100
no ip dhcp-client network-discovery
!
interface Ethernet0
ip address 192.168.10.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet0
ip address 10.64.10.18 255.255.255.224
!--- ACL used to block inbound traffic
!--- except that permitted by inspects
ip access-group 100 in
ip nat outside
ip inspect firewall out
speed auto
half-duplex
!
!--- ACL used for NAT
ip nat inside source list 1 interface FastEthernet0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.1
no ip http server
!
!--- ACL used for NAT
access-list 1 permit 192.168.10.0 0.0.0.255
!--- ACL used for Java
access-list 3 permit 216.157.100.247
!--- ACL used to block inbound traffic
!--- except that permitted by inspects
access-list 100 deny ip any any
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

## debug and show Commands

Before issuing any debug commands, please see Important Information on Debug Commands.

- **no ip inspect alert−off** − Enables CBAC alert messages. If http denies are configured, you can view them from the console.
- **debug ip inspect** − Shows messages about CBAC events.
- **show ip inspect sessions *[detail]*** − Shows existing sessions currently being tracked and inspected by CBAC. The optional keyword **detail** shows additional information about these sessions.

## Sample Debug Output

The following is sample debug output from the **debug ip inspect detail** command after trying to connect to web servers on 216.157.100.247 and 207.207.217.230. This shows what is to be expected of the debug from friendly Java, and Java being blocked from a non−friendly site (as defined on the ACL).

```
spock#

  00:35:17: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1771)
  sent 255 bytes −− responder (216.157.100.247:80) sent 4072 bytes
  00:35:18: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1772)
  sent 343 bytes −− responder (216.157.100.247:80) sent 204 bytes
  00:35:18: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1773)
  sent 344 bytes −− responder (216.157.100.247:80) sent 204 bytes
  00:35:19: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1774)
  sent 343 bytes −− responder (216.157.100.247:80) sent 204 bytes
  00:35:19: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1775)
  sent 344 bytes −− responder (216.157.100.247:80) sent 0 bytes
  00:35:32: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1777)
  sent 360 bytes −− responder (216.157.100.247:80) sent 206 bytes
  00:35:32: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1776)
  sent 265 bytes −− responder (216.157.100.247:80) sent 16906 bytes
  00:35:33: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1780)
  sent 369 bytes −− responder (216.157.100.247:80) sent 206 bytes
  00:35:33: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1784)
  sent 354 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:34: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1788)
  sent 309 bytes −− responder (216.157.100.247:80) sent 206 bytes
  00:35:34: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1787)
  sent 294 bytes −− responder (216.157.100.247:80) sent 206 bytes
  00:35:34: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1794)
  sent 315 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:34: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1795)
  sent 314 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:35: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1796)
  sent 315 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:35: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1797)
  sent 316 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:36: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1798)
  sent 316 bytes −− responder (216.157.100.247:80) sent 205 bytes
  00:35:42: %FW−3−HTTP_JAVA_BLOCK: JAVA applet is blocked from (207.207.217.230:80)
  to (192.168.10.2:1804).
  00:35:42: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1804)
  sent 215 bytes −− responder (207.207.217.230:80) sent 0 bytes
  00:35:44: %FW−3−HTTP_JAVA_BLOCK: JAVA applet is blocked from (207.207.217.230:80)
  to (192.168.10.2:1808).
  00:35:44: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1808)
  sent 215 bytes −− responder (207.207.217.230:80) sent 0 bytes
  00:35:46: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1801)
  sent 285 bytes −− responder (207.207.217.230:80) sent 211 bytes
  00:35:46: %FW−3−HTTP_JAVA_BLOCK: JAVA applet is blocked from (207.207.217.230:80)
  to (192.168.10.2:1812).
  00:35:46: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1812)
  sent 215 bytes −− responder (207.207.217.230:80) sent 0 bytes
  00:35:46: %FW−6−SESS_AUDIT_TRAIL: http session initiator (192.168.10.2:1803)
  sent 362 bytes −− responder (207.207.217.230:80) sent 162 bytes
  00:35:47: %FW−3−HTTP_JAVA_BLOCK: JAVA applet is blocked from (207.207.217.230:80)
  to (192.168.10.2:1815).
```

## Tools Information

For additional resources, refer to Cisco TAC Tools for Security Technologies.

## Related Information

- **IOS Firewall in IOS Documentation**
- **More IOS Firewall Technical Tips**
- **IOS Firewall Product Support Page**
- **Context−Based Access Control: Introduction and Configuration**
- **Improving Security on Cisco Routers**
- **Cisco Secure Integrated Software Configuration Cookbook**

Updated: May 07, 2002 Document ID: 13815