



# Configuring the Cisco IOS Firewall Feature Set

This chapter describes how to configure the Cisco IOS firewall feature set on the Catalyst 6500 series switches. This chapter contains these sections:

- [Cisco IOS Firewall Feature Set Support Overview, page 44-1](#)
- [Cisco IOS Firewall Guidelines and Restrictions, page 44-2](#)
- [Additional CBAC Configuration, page 44-3](#)

## Cisco IOS Firewall Feature Set Support Overview

The firewall feature set images support these Cisco IOS firewall features:

- Context-Based Access Control (CBAC)—The PFC installs entries in the NetFlow table to direct flows that require CBAC to the MSFC where the CBAC is applied in software on the MSFC.
- Authentication Proxy—After authentication on the MSFC, the PFC provides TCAM support for the authentication policy.
- Port-to-Application Mapping (PAM)—PAM is done in software on the MSFC.

For more information about Cisco IOS firewall features, refer to the following publications:

- *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls” chapter and these sections:
  - “Cisco IOS Firewall Overview” at this URL:  
[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_cfg\\_fw\\_all\\_intrsn.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_fw_all_intrsn.html)
  - “Configuring Context-Based Access Control” at this URL:  
[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_cfg\\_content\\_ac.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_content_ac.html)
  - “Configuring Authentication Proxy” at this URL:  
[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_cfg\\_authen\\_prxy.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authen_prxy.html)
- *Cisco IOS Security Command Reference* publication at this URL:  
[http://www.cisco.com/en/US/docs/ios/12\\_2/security/command/reference/fsecur\\_r.html](http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html)

The following features are supported with and without the use of a Cisco IOS firewall image:

- Standard access lists and static extended access lists
- Lock-and-key (dynamic access lists)
- IP session filtering (reflexive access lists)

- TCP intercept
- Security server support
- Network address translation
- Neighbor router authentication
- Event logging
- User authentication and authorization

**Note**

Catalyst 6500 series switches support the Intrusion Detection System Module (IDS) (WS-X6381-IDS). Catalyst 6500 series switches do not support the Cisco IOS firewall IDS feature, which is configured with the **ip audit** command.

## Cisco IOS Firewall Guidelines and Restrictions

When configuring the Cisco IOS firewall features, follow these guidelines and restrictions:

- On other platforms, if you enter the **ip inspect** command on a port, CBAC modifies ACLs on other ports to permit the inspected traffic to flow through the network device. On Catalyst 6500 series switches, you must enter the **mls ip inspect** command to permit traffic through any ACLs that would deny the traffic through other ports. Refer to the [“Additional CBAC Configuration” section on page 44-3](#) for more information.
- Reflexive ACLs and CBAC have conflicting flow mask requirements. Reflexive ACLs are processed in software on the MSFC.
- CBAC is incompatible with VACLs. You can configure CBAC and VACLs on the switch but not in the same subnet (VLAN).

**Note**

The Intrusion Detection System Module (IDS) uses VACLs to select traffic. To use the IDS in a subnet where CBAC is configured, enter the **mls ip ids acl\_name** interface command, where *acl\_name* is configured to select traffic for the IDS.

- To inspect Microsoft NetMeeting (2.0 or greater) traffic, turn on both **h323** and **tcp** inspection.
- To inspect web traffic, turn on **tcp** inspection. To avoid reduced performance, do not turn on **http** inspection to block Java.
- QoS and CBAC do not interact or interfere with each other.
- You can configure CBAC on physical ports configured as Layer 3 interfaces and on VLAN interfaces.
- You cannot configure VACLs and CBAC on the same interface.

## Additional CBAC Configuration

You need to do additional CBAC configuration on the Catalyst 6500 series switches. On a network device other than a Catalyst 6500 series switch, when ports are configured to deny traffic, CBAC permits traffic to flow bidirectionally through the port if it is configured with the **ip inspect** command. The same situation applies to any other port that the traffic needs to go through, as shown in this example:

```
Router(config)# ip inspect name permit_ftp ftp
Router(config)# interface vlan 100
Router(config-if)# ip inspect permit_ftp in
Router(config-if)# ip access-group deny_ftp_a in
Router(config-if)# ip access-group deny_ftp_b out
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# ip access-group deny_ftp_c in
Router(config-if)# ip access-group deny_ftp_d out
Router(config-if)# exit
Router(config)# interface vlan 300
Router(config-if)# ip access-group deny_ftp_e in
Router(config-if)# ip access-group deny_ftp_f out
Router(config-if)# end
```

If the FTP session enters on VLAN 100 and needs to leave on VLAN 200, CBAC permits the FTP traffic through ACLs deny\_ftp\_a, deny\_ftp\_b, deny\_ftp\_c, and deny\_ftp\_d. If another FTP session enters on VLAN 100 and needs to leave on VLAN 300, CBAC permits the FTP traffic through ACLs deny\_ftp\_a, deny\_ftp\_b, deny\_ftp\_e, and deny\_ftp\_f.

On a Catalyst 6500 series switch, when ports are configured to deny traffic, CBAC permits traffic to flow bidirectionally only through the port configured with the **ip inspect** command. You must configure other ports with the **mls ip inspect** command.

If the FTP session enters on VLAN 100 and needs to leave on VLAN 200, CBAC on a Catalyst 6500 series switch permits the FTP traffic only through ACLs deny\_ftp\_a and deny\_ftp\_b. To permit the traffic through ACLs deny\_ftp\_c and deny\_ftp\_d, you must enter the **mls ip inspect deny\_ftp\_c** and **mls ip inspect deny\_ftp\_d** commands, as shown in this example:

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)# mls ip inspect deny_ftp_d
```

FTP traffic cannot leave on VLAN 300 unless you enter the **mls ip inspect deny\_ftp\_e** and **mls ip inspect deny\_ftp\_f** commands. Enter the **show fm insp [detail]** command to verify the configuration.

The **show fm insp [detail]** command displays the list of ACLs and ports on which CBAC is configured and the status (**ACTIVE** or **INACTIVE**), as shown in this example:

```
Router# show fm insp
      interface:Vlan305(in) status :ACTIVE
      acl name:deny
      interfaces:
        Vlan305(out):status ACTIVE
```

On VLAN 305, inspection is active in the inbound direction and no ACL exists. ACL **deny** is applied on VLAN 305 in the outbound direction and inspection is active.

To display all of the flow information, use the **detail** keyword.

If a VACL is configured on the port before configuring CBAC, the status displayed is **INACTIVE**; otherwise, it is **ACTIVE**. If PFC resources are exhausted, the command displays the word “BRIDGE” followed by the number of currently active NetFlow requests that failed, which have been sent to the MSFC for processing.

