



Firewall ACL Bypass

The Firewall ACL Bypass feature allows a packet to avoid redundant access control list (ACL) checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Thus, input and output dynamic ACLs searches are eliminated, improving the overall throughput performance of the base engine.

Feature History for Firewall ACL Bypass

Release	Modification
12.3(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About Firewall ACL Bypass, page 2](#)
- [How to Use Firewall ACL Bypass, page 2](#)
- [Configuration Examples for Verifying Firewall Session Information, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Glossary, page 9](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Information About Firewall ACL Bypass

To better understand how dynamic ACL bypass works, you should understand the following concepts:

- [Benefits of Firewall ACL Bypass, page 2](#)
- [Firewall ACL Bypass Functionality Overview, page 2](#)

Benefits of Firewall ACL Bypass

Because input and output dynamic ACLs are no longer necessary, the need for context-based access control (CBAC) to create dynamic ACLs on the interface is eliminated. Thus, the following benefits are now available:

- Improved connections per second performance of the firewall
- Reduced run-time memory consumption of the firewall

Firewall ACL Bypass Functionality Overview

Before ACL bypassing was implemented, a packet could be subjected to as many as three redundant searches—an input ACL search, an output ACL search, and an inspection session search. Each dynamic ACL that CBAC creates corresponds to a single inspection session. Thus, a matching dynamic ACL entry for a given packet implies that a matching inspection session exists and that the packet should be permitted through the ACL. Because a matching inspection session is often found in the beginning of IP processing, the input and output dynamic ACL searches are no longer necessary and can be eliminated.

ACL bypassing subjects the packet to one search—the inspection session search—during its processing path through the router. When a packet is subjected to a single inspection session search before the ACL checks, the packet is matched against the list of session identifiers that already exist on the interface. (Session identifiers keep track of the source and destination IP addresses and ports of the packets and on which interface the packet arrived.)

**Note**

Session identifiers are not created on interfaces for inspection sessions that are only Intrusion Detection Sessions (IDS).

How to Use Firewall ACL Bypass

After your firewall is configured for inspection, ACL bypassing is performed by default. That is, you should configure inspection as normal.

To configure CBAC for your firewall, see the following chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*.

Configuration Examples for Verifying Firewall Session Information

After you have configured your firewall for inspection, you can use the **show ip inspect sessions detail** command to view session inspection information. The following examples show how eliminating dynamic ACLs changes the sample output:

- [Old show ip inspect CLI Output: Example, page 3](#)
- [New show ip inspect CLI Output: Example, page 3](#)

Old show ip inspect CLI Output: Example

The following is sample output from the **show ip inspect session detail** command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail

Established Sessions
  Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
    Created 00:00:08, Last heard 00:00:04
    Bytes sent (initiator:responder) [140:298] acl created 2
    Outgoing access-list 102 applied to interface FastEthernet0/0
    Inbound access-list 101 applied to interface FastEthernet0/1

Router# show access-lists

Extended IP access list 101
  permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27 matches)
  deny udp any any
  deny tcp any any
  permit ip any any
Extended IP access list 102
  permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27 matches)
  deny udp any any
  deny tcp any any
  permit ip any any
```

New show ip inspect CLI Output: Example

The following is sample output from the **show ip inspect session detail** command, which shows related ACL information (such as session identifiers [SID]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail

Established Sessions
  Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
    Created 00:00:10, Last heard 00:00:06
    Bytes sent (initiator:responder) [140:298]
    In SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
    Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

```

Router# show access-list

Extended IP access list 101
  deny udp any any (20229 matches)
  deny tcp any any
  permit ip any any (6 matches)
Extended IP access list 102
  deny udp any any
  deny tcp any any
  permit ip any any (1 match)

```

Additional References

The following sections provide references related to Dynamic ACL Bypass.

Related Documents

Related Topic	Document Title
Cisco IOS Firewalls and ACLs	The section “Traffic Filtering and Firewalls” in the <i>Cisco IOS Security Configuration Guide</i>
Cisco IOS Firewall commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section the following modified command. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

- [show ip inspect](#)

show ip inspect

To display Context-based Access Control (CBAC) configuration and session information, use the **show ip inspect** command in privileged EXEC mode.

```
show ip inspect {name inspection-name | config | interfaces | session [detail] | all }
```

Syntax Description	name	Displays the configured inspection rule with the name <i>inspection-name</i> .
	<i>inspection-name</i>	
	config	Displays the complete CBAC inspection configuration.
	interfaces	Displays the interface configuration with respect to applied inspection rules and access lists.
	session [detail]	Displays existing sessions that are currently being tracked and inspected by CBAC. The optional detail keyword allows additional details about these sessions to be shown.
	all	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.2 P	This command was introduced.
	12.3(4)T	The output for the show ip inspect session detail command was enhanced to support dynamic ACL bypass.

Usage Guidelines	Use this command to view the CBAC configuration and session information.
------------------	--

ACL Bypass Functionality

ACL bypass allows a packet to avoid redundant access control list (ACL) checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Examples

The following example shows sample output for the **show ip inspect name myinspectionrule** command, where the inspection rule “myinspectionrule” is configured. In this example, the output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule

Inspection Rule Configuration
Inspection name myinspectionrule
  tcp timeout 3600
  udp timeout 30
  ftp timeout 3600
```

The following is sample output for the **show ip inspect config** command. In this example, the output shows CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output for the **show ip inspect interfaces** command:

```
Interface Configuration
Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

The following is sample output for the **show ip inspect session** command. In this example, the output shows the source and destination addresses and port numbers (separated by colons), and it indicates that the session is an FTP session.

```
Router# show ip inspect session

Established Sessions
  Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
  Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following is sample output for the **show ip inspect all** command:

```
Router# show ip inspect all

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

```
Outgoing inspection rule is not set
Inbound access list is not set
Outgoing access list is not set
Established Sessions
Session 25A6E1C (30.0.0.1:46065)=>(40.0.0.1:21) ftp SIS_OPEN
Session 25A34A0 (40.0.0.1:20)=>(30.0.0.1:46072) ftp-data SIS_OPEN
```

The following is sample output from the **show ip inspect session detail** command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail
```

```
Established Sessions
Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:08, Last heard 00:00:04
  Bytes sent (initiator:responder) [140:298] acl created 2
  Outgoing access-list 102 applied to interface FastEthernet0/0
  Inbound access-list 101 applied to interface FastEthernet0/1
```

The following is sample output from the **show ip inspect session detail** command, which shows related ACL information (such as session identifiers [SID]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail
```

```
Established Sessions
Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:10, Last heard 00:00:06
  Bytes sent (initiator:responder) [140:298]
  In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
  Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

Glossary

connections per second— Metric defined by the number of short-lived connections that can be created and deleted within 1 second by a router running CBAC. (These connections apply only to TCP connections because UDP is a connectionless protocol.)

throughput—Metric defined by the number of packets transferred from the input interface to the output interface within 1 second by a router running CBAC.

**Note**

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

