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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Firewall ACL Bypass" section on page 5.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

- Information About Firewall ACL Bypass, page 1
- How to Configure Firewall ACL Bypass, page 2
- Configuration Examples for Verifying Firewall Session Information, page 2
- Additional References, page 4
- Feature Information for Firewall ACL Bypass, page 5
- Glossary, page 5

Information About Firewall ACL Bypass

- Benefits of Firewall ACL Bypass, page 2
- Firewall ACL Bypass Functionality Overview, page 2

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

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 Configure 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:

- Example: Old show ip inspect CLI Output, page 3
- Example: New show ip inspect CLI Output, page 3

Example: Old show ip inspect CLI Output

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
```

Example: New show ip inspect CLI Output

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands	*Cisco IOS Security Command Reference*

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
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Firewall ACL Bypass

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for Firewall ACL Bypass

Feature Name	Releases	Feature Information
Firewall ACL Bypass	12.3(4)T	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. The following commands were introduced or modified: **show ip inspect**.

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.