

Troubleshooting Cisco IOS Firewall Configurations

Document ID: 13897

Introduction

Prerequisites

Requirements

Components Used

Conventions

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides information you can use in order to troubleshoot Cisco IOS® Firewall configurations.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Troubleshoot

Note: Refer to Important Information on Debug Commands before you issue **debug** commands.

- In order to reverse (remove) an access list, put a "no" in front of the **access-group** command in interface configuration mode:

```
int <interface>  
no ip access-group # in|out
```

- If too much traffic is denied, study the logic of your list or try to define an additional broader list, and then apply it instead. For example:

```
access-list # permit tcp any any  
access-list # permit udp any any  
access-list # permit icmp any any  
int <interface>  
ip access-group # in|out
```

- The **show ip access-lists** command shows which access lists are applied and what traffic is denied by them. If you look at the packet count denied before and after the failed operation with the source and destination IP address, this number increases if the access list blocks traffic.
- If the router is not heavily loaded, debugging can be done at a packet level on the extended or ip inspect access list. If the router is heavily loaded, traffic is slowed through the router. Use discretion with debugging commands.

Temporarily add the **no ip route-cache** command to the interface:

```
int <interface>
no ip route-cache
```

Then, in enable (but not config) mode:

```
term mon
debug ip packet # det
```

produces output similar to this:

```
*Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0),
g=10.31.1.21, len 100, forward
*Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9
len 100, forward
```

- Extended access lists can also be used with the "log" option at the end of the various statements:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

You therefore see messages on the screen for permitted and denied traffic:

```
*Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100
-> 10.31.1.161 (0/0), 15 packets
*Mar 1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0)
-> 10.31.1.161(0), 1 packet
```

- If the ip inspect list is suspect, the **debug ip inspect <type_of_traffic>** command produces output such as this output:

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 31957512
seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23)
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 36592193
seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23)
```

For these commands, along with other troubleshooting information, refer to Troubleshooting Authentication Proxy.

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

- [Cisco IOS Firewall Product Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 19, 2007

Document ID: 13897
