

Cisco – Cisco IOS Firewall Feature Set Frequently Asked Questions

Table of Contents


<u>Cisco IOS Firewall Feature Set Frequently Asked Questions</u>	1
<u>Questions</u>	1
<u>Related Information</u>	6

Cisco IOS Firewall Feature Set Frequently Asked Questions

Questions

- [Inspection of mail through the Cisco IOS firewall does not work properly when I use the `ip inspect smtp` command. What could be the problem?](#)
- [Why don't I see access-list messages for every packet?](#)
- [Is the Transmission Control Protocol \(TCP\) Intercept feature needed with Context Based Access Control \(CBAC\)?](#)
- [What is the processing order in which an Internet Protocol \(IP\) Packet is handled when CBAC, access control lists \(ACLs\) and Network Address Translation \(NAT\) are involved?](#)
- [How does CBAC interact with Passive File Transfer Protocol \(FTP\)?](#)
- [How do I change the port number on the CBAC inspection for a protocol?](#)
- [What should I do if I see a high number of TCP resets on my Cisco IOS firewall?](#)
- [When running IP inspect and IP audit, what do the numbers in a `show ip audit stat` command mean?](#)
- [How are audit byte counts different from interface byte counts?](#)
- [When I enable the `ip http server` command, can I use HTTPS to browse to my router?](#)
- [How can I upgrade the signatures on my Cisco IOS Intrusion Detection System \(IDS\) system?](#)
- [Why are packets being dropped at my Cisco IOS IDS/firewall?](#)

Q. Inspection of mail through the Cisco IOS firewall does not work properly when I use the `ip inspect smtp` command. What could be the problem?

A. CBAC can be configured to inspect Simple Mail Transport Protocol (SMTP) but not Extended SMTP (ESMTP). SMTP is described in [RFC 821](#) . CBAC SMTP inspect does not inspect the ESMTP session or command sequence. Configuring SMTP inspection is not useful for ESMTP, and it can cause problems. To determine whether a mail server is doing SMTP or ESMTP, contact your mail server software vendor, or Telnet to mail server port 25 and observe the banner to see if it reports SMTP or ESMTP.

Q. Why don't I see access-list messages for every packet?

A. When a log message is defined, there is also a timer granularity that can be specified with the `ip access-list logging` command. The number of packets that are collected on an access-list entry prior to the log message appearing is controlled by the `ip access-list log-update threshold` command. If there are too many messages to be handled, or if a particular type of message occurs more often than 1 per second, the logging facility may discard the extra messages. This timer granularity is designed so that a single process cannot overwhelm the logger daemon.

Q. Is the TCP Intercept feature needed with CBAC?

A. CBAC includes session control in the form of the following by default:

```
ip inspect one-minute high
ip inspect one-minute low
ip inspect max-incomplete high
ip inspect max-incomplete low
ip inspect tcp max-incomplete host
ip inspect tcp finwait-time
ip inspect tcp synwait-time
ip inspect tcp idle-time
ip inspect udp idle-time
```

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks. TCP packets matching the access-list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode** command. The TCP intercept code either intercepts or watches the connections.

Cisco IOS IDS/CBAC and the TCP Intercept feature work independently of each other and, in fact, should not be used together due to the fact that they use the same internal engine.

Q. What is the processing order in which an IP Packet is handled when CBAC, ACLs, and NAT are involved?

A. When an outbound packet arrives at an interface, it will be processed in the following order:

1. The inbound ACL of the input interface is applied.
2. The NAT inbound is applied.
3. The NAT outbound is applied.
4. The outbound ACL of the output interface is applied.
5. CBAC processing occurs.
6. The IP Packet goes through the output interface.

CBAC inspects packets after input and output ACL checks. When inspecting, CBAC may insert or remove the ACL items associated with a session depending upon its state and context.

While CBAC is compatible with both NAT and Port Address Translation (PAT), it is important to note that CBAC supports some applications that NAT and PAT do not.

For more information on NAT, refer to the [NAT Order of Operation](#) documentation.

Q. How does CBAC interact with Passive FTP?

A. The following process describes the FTP client inside to the FTP server outside CBAC interaction:

1. The FTP client sends out the synchronize/start (SYN) packet on the control channel:

```
client          SYN
             -----FW-----> server
```

2. The Cisco IOS firewall creates a session for this new connection and holes in ACLs:

```
client          hole
```

3. The TCP handshake is completed:

```
client server    SYN ACK
```

4. When the **ls** command is entered, the FTP client sends **PASV** and **LIST** commands to the server one after the other:

```
client          PASV
             -----FW-----> server
             address/port info
client
```

5. On seeing the address/port in the reply to the **PASV** command, the Cisco IOS firewall creates a pre-gen session and ACL holes:

```
             hole
client -----FW-----> server
             hole
client -----FW-----> server
```

The holes point from the client to the server because the Cisco IOS firewall knows that the client will try to connect to the server at XXXX,y,y to create the data channel as per Passive FTP specifications.

6. The FTP client sends the SYN for this data connection:

```
             SYN DATA
client -----FW-----> server
```

7. On seeing the SYN packet, the Cisco IOS firewall creates holes which will allow synchronize acknowledge (SYN ACK) reply from the server:

```
             hole
client
```

These holes can take 5–10 seconds to create. From the time the user sends the **ls** command to the time these holes are created, there are at least three packets exchanged between the client and the server:

- ◆ PASV
- ◆ Reply to PASV with address/port information
- ◆ SYN to this new address/port

These three packet exchanges might be slow if the FTP server or client is loaded and can easily take up to 5–10 seconds.

The following debugs can help to establish a more detailed timeline of the process:

```
debug ip packet detailed <acl>
debug ip inspect ftp-cmd
debug ip inspect ftp-tokens
debug ip inspect object-creation
```

Q. How do I change the port number on the CBAC inspection for a protocol?

A. Port to Application Mapping allows you to change the port number of the CBAC inspection for a protocol. For example, if you want to inspect SMTP on port 75 (rather than 25), configure the following:

```
ip port-map smtp port 75
```

For further information, refer to the [Port to Application Mapping](#) documentation.

Q. What should I do if I see a high number of TCP resets on my Cisco IOS firewall?

A. Ensure the following commands are correctly set, based upon the load of the system:

```
ip inspect max-incomplete low 400
ip inspect max-incomplete high 500
ip inspect one-minute low 400
```

```
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect tcp idle-time 3600
ip inspect tcp finwait-time 5
ip inspect tcp synwait-time 30
ip inspect tcp max-incomplete host 50 block-time 0
```

Ensure the inspection statement timeouts are correctly set (in most cases, the default is appropriate). If you notice that the resets occur during peak hours, it is advisable to increase the following:

```
ip inspect one-minute high
ip inspect max-incomplete high
ip inspect tcp max-incomplete host
```

If the problem persists, use the following **show** and **debugs** commands to determine the issue:

```
show ip inspect stat
debug ip inspect tcp
debug ip inspect ftp
debug ip inspect http
debug ip inspect detailed
debug ip inspect object-creation
debug ip inspect object-deletion
debug ip inspect events
debug ip inspect function-trace
debug ip inspect timers
debug ip packet detailed
```

Q. When running IP inspect and IP audit, what do the numbers in the show ip audit stat command mean?

A. With IP inspect and IP audit enabled/applied, a **show ip audit stat** command displays output similar to the following:

```
Maxever session counts (estab/half-open/terminating) [4214:16853:566]
```

The values "[4214:16853:566]" are relevant to the following commands:

```
ip inspect max-incomplete high 500
ip inspect max-incomplete low 400
ip inspect one-minute high 500
ip inspect one-minute low 400
```

The first of the three values is related to the **ip inspect one-minute high** and **ip inspect one-minute low** commands. If the value of the **show ip audit stat** command is higher than the number specified in the **ip inspect one-minute high** command, the router will be dropping the difference in the number of packets.

Using the above example of 4214, the **ip inspect one-minute high** command should be greater than 4214 and the **ip inspect one-minute low** command should be less than 4214.

Keep in mind that the performance of the router (Computer Processing Unit (CPU) and memory) may be affected if the value of the **ip inspect one-minute high** is far greater than the value in the **show ip audit stat** command. It is important that you manipulate the values to find the best for your network.

The second value in the Maxever session counts relates to the **ip inspect max-incomplete high** and **ip inspect max-incomplete low** commands, and works in a similar way to the **one-minute high** and **one-minute low** commands. In this case, for example, the values of the commands should sit on either side of 16853. Again, this is adjusted through trial and error under network conditions.

Q. How are audit byte counts different from interface byte counts?

A. Audit log byte count is the count of Layer 7 bytes. Audit byte counts also makes sure that re-transmitted packets are not counted twice (for TCP). Audit byte counts should not be greater than interface byte counts for two reasons:

1. Audit byte counts consider only 17 bytes while interface byte counts consider the entire packet.
2. Audit byte counts skip re-transmitted packets.

The best way to determine whether audit byte counts are correct or not is to run a sniffer and count the number of Layer 7 bytes transferred both ways and compare it to the audit byte counts.

Q. When I enable the `ip http server` command, can I use HTTPS to browse to my router?

A. Cisco IOS does not support HTTPS. You must use HTTP to browse to the router.

Q. How can I upgrade the signatures on my Cisco IOS IDS system?

A. The Cisco IOS IDS signatures are built into the IOS code and hence, require a Cisco IOS image upgrade. Signatures cannot be configured and recompiled on the fly to address vulnerabilities.

Q. Why are packets being dropped at my Cisco IOS IDS firewall?

A. When running Cisco IOS IDS, packets may be dropped due to asymmetric routing. Cisco IOS IDS needs to see all the TCP 3 way handshaking packets to move the connection into the established state. If more than one router is seeing the session, the router that receives the SYN packets will have a lot of half-opened sessions. Eventually IDS starts sending reset (RST) packets to close the oldest half-opened session to make room for the new connection when the counter of half-opened sessions reaches the threshold.

If you are facing a Denial of Service (DOS) attack, the router approaches this based on the values of the following:

```
ip inspect max-incomplete high <n1>
ip inspect max-incomplete low <n2>
```

The default values for n1 and n2 are 500 and 400 respectively. It is recommended that you configure these values and not leave them to the defaults.

If the number of half-open sessions goes beyond 500, messages such as 'getting aggressive' may appear. When any new SYN packets arrive at the router, the "Oldest Half Open" connection is replaced and an RST is sent to the respective server. This continues to take place until the number drops below the minimum threshold, at which point the firewall might show 'calming down' messages. The router then goes back to 'Normal' mode.

RST packets are sent by the Cisco IOS firewall even when the firewall is not enabled. The Cisco IOS firewall and IDS share the same code in detecting/handling DOS attacks. This feature is built in by default. Currently there is no command line interface (CLI) command to turn the DOS attack feature off.

Related Information

- [IOS Firewall in IOS Documentation](#)
 - [More IOS Firewall Technical Tips](#)
 - [IOS Firewall Product Support Page](#)
-

Home	What's New	How to Buy	Login	Profile	Feedback	Search	Map/Help
----------------------	----------------------------	----------------------------	-----------------------	-------------------------	--------------------------	------------------------	--------------------------

All contents are Copyright © 1992—2002 Cisco Systems, Inc. All rights reserved.