# Cisco IOS Classic Firewall/IPS: Configuring Context–Based Access Control (CBAC) for Denial–of–Service Protection

**Document ID: 98705**

## Contents

## Introduction

This document describes the tuning procedure for Denial of Service (DoS) parameters in the Cisco IOS® Classic Firewall with CBAC.

CBAC provides advanced traffic filtering functionality and can be used as an integral part of your network firewall.

DoS generally refers to network activity that either intentionally or unintentionally overwhelms network resources such as WAN link bandwidth, firewall connection tables, end–host memory, CPU, or service capabilities. In a worst–case scenario, DoS activity overwhelms the vulnerable (or targeted) resource to the point that the resource becomes unavailable, and it prohibits WAN connectivity or service access to legitimate users.

The Cisco IOS Firewall can contribute to the mitigation of DoS activity if it maintains counters of the number of  half–open  TCP connections, as well as the total connection rate through the firewall and intrusion prevention software in both Classic Firewall (**ip inspect**) and Zone–Based Policy Firewall.

## Prerequisites

### Requirements

There are no specific requirements for this document.

## Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

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

# Background Information

Half−open connections are TCP connections that have not completed the three−way SYN−SYN/ACK−ACK handshake that is always used by TCP peers to negotiate the parameters of their mutual connection. Large numbers of half−open connections can be indicative of malicious activity, such as DoS or distributed−denial−of−service (DDoS) attacks. An example of one type of DoS attack is conducted by malicious, intentionally−developed software, such as worms or viruses that infect multiple hosts on the Internet and attempt to overwhelm specific Internet servers with SYN attacks, where large numbers of SYN connections are sent to a server by multiple hosts on the Internet or within the private network of an organization. SYN attacks represent a hazard to Internet servers since the connection tables of servers can be loaded with bogus SYN connection attempts that arrive faster than the server can deal with the new connections. This is a type of DoS attack because the large number of connections in the TCP connection list of the victim server prevent legitimate user access to the victim Internet servers.

Cisco IOS Firewall also regards User Datagram Protocol (UDP) sessions with traffic in only one direction as half−open because many applications that use UDP for transport acknowledge the reception of data. UDP sessions without return traffic are likely indicative of DoS activity or attempts to connect between two hosts, where one of the hosts has become unresponsive. Many types of UDP traffic, such as log messages, SNMP network management traffic, streaming voice and video media, and signaling traffic, only use traffic in one direction to carry their traffic. Many of these types of traffic apply application−specific intelligence to prevent unidirectional traffic patterns from adversely affecting firewall and IPS DoS behavior.

Prior to Cisco IOS Software Release 12.4(11)T and 12.4(10), Cisco IOS Stateful Packet Inspection provided protection from DoS attacks as a default when an inspection rule was applied. Cisco IOS Software Release 12.4(11)T and 12.4(10) modified the default DoS settings so that DoS protection is not automatically applied, but the connection activity counters are still active. When DoS protection is active, that is, when the default values are used on older software releases, or the values have been adjusted to the range that affect traffic, DoS protection is enabled on the interface where inspection is applied, in the direction in which the firewall is applied, for the firewall policy configuration protocols to inspect. DoS protection is only enabled on network traffic if the traffic enters or leaves an interface with inspection applied in the same direction of the initial traffic (SYN packet or first UDP packet) for a TCP connection or UDP session.

Cisco IOS Firewall inspection provides several adjustable values to protect against DoS attacks. Cisco IOS Software releases prior to 12.4(11)T and 12.4(10) have default DoS values that can interfere with proper network operation if they are not configured for the appropriate level of network activity in networks where connection rates exceed the defaults. These parameters allow you to configure the points at which the DoS protection of your firewall router begins to take effect. When the DoS counters of your router exceed the default or configured values, the router resets one old half−open connection for every new connection that exceeds the configured max−incomplete or one−minute high values until the number of half−open sessions drops below the max−incomplete low values. The router sends a syslog message if logging is enabled, and if an intrusion prevention system (IPS) is configured on the router, the firewall router sends a DoS signature

message through the Security Device Event Exchange (SDEE). If the DoS parameters are not adjusted to the normal behavior of your network, normal network activity can trigger the DoS protection mechanism, which causes application failures, poor network performance, and high CPU utilization on the Cisco IOS Firewall router.

# Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Denial−of−Service Tuning for Cisco IOS Software Classic (IP Inspect) Firewall and Intrusion Prevention System

The classic Cisco IOS Firewall maintains a global set of DoS counters for the router, and all firewall sessions for all firewall policies on all interfaces are applied to the global set of firewall counters.

Cisco IOS Classic Firewall Inspection provides protection from DoS attack by default when a Classic Firewall is applied. DoS protection is enabled on all interfaces where inspection is applied, in the direction in which the firewall is applied, for each service or protocol that the firewall policy is configured to inspect. Classic Firewall provides several adjustable values to protect against DoS attacks. The legacy default settings (from software images prior to Release 12.4(11)T) shown in Table 1 can interfere with proper network operation if they are not configured for the appropriate level of network activity in networks where connection rates exceed the defaults. The DoS settings can be viewed with the exec command **show ip inspect config**, and the settings are included with the output of **sh ip inspect all**.

CBAC uses timeouts and thresholds to determine how long to manage state information for a session, as well as to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply globally to all sessions.

| Table 1 Classic Firewall Default DoS Protection Limits | | |
|---|---|---|
| **DoS Protection Value** | **Prior to 12.4(11)T/12.4(10)** | **12.4(11)T/12.4(10) and later** |
| max−incomplete high *value* | 500 | Unlimited |
| max−incomplete low *value* | 400 | Unlimited |
| one−minute high *value* | 500 | Unlimited |
| one−minute low *value* | 400 | Unlimited |
| tcp max−incomplete host *value* | 50 | Unlimited |

Routers configured to apply Cisco IOS VRF−Aware Firewall maintain one set of counters for each VRF.

The counter for  ip inspect one−minute high  and  ip inspect one−minute low  maintains a sum of all TCP, UDP, and Internet Control Message Protocol (ICMP) connection attempts within the prior minute of the operation of the router, whether the connections have been successful or not. A rising connection rate can be indicative of a worm infection on a private network or an attempted DoS attack against a server.

While you cannot disable the DoS protection of your firewall, you can adjust the DoS protection so that it does not take effect unless a very large number of half–open connections are present in the session table of your firewall router.

## DoS Firewall Protection

Follow this procedure to tune the DoS protection of your firewall to the activity of your network:

1. Be sure that your network is not infected with viruses or worms that can lead to erroneously large half–open connection values or attempted connection rates. If your network is not clean, there is no way to properly adjust the DoS protection of your firewall. You must observe the activity of your network within a period of typical activity. If you tune the DoS protection settings of your network within a period of low or idle network activity, normal activity levels likely exceed the DoS protection settings.
2. Set the max–incomplete high values to very high values:

    ```
    ip inspect max-incomplete high 20000000
    ip inspect one-minute high 100000000
    ip inspect tcp max-incomplete host 100000 block-time 0
    ```

    This prevents the router from providing DoS protection while you observe the connection patterns of your network. If you wish to leave DoS protection disabled, stop this procedure now.

    **Note:** If your router runs Cisco IOS Software Release 12.4(11)T or later, or 12.4(10) or later, you do not need to raise the default DoS Protection values; they are already set to their maximum limits by default.

    **Note:** If you want to enable the more aggressive TCP host–specific denial–of–service prevention that includes the blocking of connection initiation to a host, you must set the block–time specified in the **ip inspect tcp max–incomplete host** command
3. Clear the Cisco IOS Firewall statistics with this command:

    ```
    show ip inspect statistics reset
    ```
4. Leave the router configured in this state for some time, perhaps as long as 24 to 48 hours, so you can observe the network pattern over at least one full day of the typical network activity cycle.

    **Note:** While the values are adjusted to very high levels, your network does not benefit from Cisco IOS Firewall or IPS DoS protection.
5. After the observation period, check the DoS counters with this command:

    ```
    show ip inspect statistics
    ```

    The parameters you must observe with which to tune your DoS protection are highlighted in **bold**:

    ```
    Packet inspection statistics
      [process switch:fast switch]
     tcp packets: [218314:7878692]
     udp packets: [501498:65322]
      packets: [376676:80455]
      packets: [5738:4042411]
     smtp packets: [11:11077]
     ftp packets: [2291:0]
    Interfaces configured for inspection 2
    Session creations since subsystem
       startup or last reset 688030
    Current session counts
       (estab/half-open/terminating) [0:0:0]
    ```

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
   received 46591 packets out-of-order; dropped 16454
   peak memory usage 48 KB; current usage: 0 KB
   peak queue length 16
```

6. Configure **ip inspect max–incomplete high** to a value 25–percent higher than the indicated maxever session count half–open value of your router. A 1.25 multiplier offers 25–percent headroom above observed behavior, for example:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

Configure:

```
router(config)
   #ip inspect max-incomplete high 70
```

**Note:** This document describes the use of a multiplier of 1.25 times the typical activity of your network to set limits to engage DoS protection. If you observe your network within typical network activity peaks, this must provide adequate headroom to avoid the activation of the DoS protection of the router under all but atypical circumstances. If your network periodically sees large bursts of legitimate network activity that exceed this value, the router engages the DoS protection capabilities, which can cause a negative impact on some of the network traffic. You must monitor your router logs for detections of DoS activity and adjust the **ip inspect max–incomplete high** and/or **ip inspect one–minute high** limits to avoid triggering DoS, after you determine that the limits were encountered as a result of legitimate network activity. You can recognize DoS protection application by the presence of log messages such as this:

7. Configure **ip inspect max–incomplete low** to the value your router displayed for its maxever session count half–open value, for example:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

Configure:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. The counter for **ip inspect one–minute high** and **one–minute low** maintains a sum of all TCP, UDP, and Internet Control Message Protocol (ICMP) connection attempts within the prior minute of the router operation, whether the connections have been successful or not. A rising connection rate can be indicative of a worm infection on a private network, or an attempted DoS attack against a server. An additional inspection statistic was added to the **show ip inspect statistics** output in 12.4(11)T and 12.4(10) to reveal the high–water–mark for the session creation rate. If you run a Cisco IOS Software Release earlier than 12.4(11)T or 12.4(10), the inspection statistics do not contain this line:

```
Maxever session creation rate [value]
```

Cisco IOS Software Releases prior to 12.4(11)T and 12.4(10) do not maintain a value for inspection maxever one–minute connection rate, so you must calculate the value you apply based on observed maxever session count values. Observations of several networks that use the stateful inspection of Cisco IOS Firewall Release 12.4(11)T in production have shown that Maxever session creation rates

tend to exceed the sum of the three values (established, half–open, and terminating) in maxever session count by roughly ten per cent. In order to calculate the ip inspect one–minute low value, multiply the indicated established value by 1.1, for example:

```
Maxever session counts
    (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

Configure:

```
ip inspect one-minute low 328
```

If the router runs Cisco IOS Software Release 12.4(11)T or later, or 12.4(10) or later, you can simply apply the value shown in the Maxever session creation rate inspection statistic:

```
Maxever session creation rate 330
```

Configure:

```
ip inspect one-minute low 330
```

9. Calculate and configure **ip inspect one–minute high**. The ip inspect one–minute high value must be 25–percent greater than the calculated one–minute low value, for example:

```
ip inspect one-minute low (330) * 1.25 = 413
```

Configure:

```
ip inspect one-minute high 413
```

**Note:** This document describes the use of a multiplier of 1.25 times the typical activity of your network to set limits to engage DoS protection. If you observe your network within typical network activity peaks, this must provide adequate headroom to avoid the activation of the DoS protection of the router under all but atypical circumstances. If your network periodically sees large bursts of legitimate network activity that exceed this value, the router engages the DoS protection capabilities, which can cause a negative impact on some of the network traffic. You must monitor your router logs for detections of DoS activity and adjust the **ip inspect max–incomplete high** and/or **ip inspect one–minute high** limits to avoid triggering DoS, after you determine that the limits were encountered as a result of legitimate network activity. You can recognize DoS protection application by the presence of log messages such as this:

10. You need to define a value for **ip inspect tcp max–incomplete host** in accordance with your knowledge of the capability of your servers. This document cannot provide guidelines for per–host DoS protection configuration since this value varies widely based on end–host hardware and software performance. If you are uncertain about the appropriate limits to configure for DoS protection, you effectively have two options with which to define the DoS limits:

    a. The preferable option is to configure router–based per–host DoS protection to a high value (less than or equal to the maximum value of 4,294,967,295), and apply host–specific protection offered by the operating system of each host or an external host–based Intrusion Protection System such as Cisco Security Agent (CSA).
    b. Examine activity and performance logs on your network hosts and determine their peak sustainable connection rate. Since Classic Firewall only offers one global counter, you must apply the maximum value that you determine after you check all of your network hosts for their maximum connection rates. It is still advisable that you use OS–specific activity limits and a host–based IPS such as CSA.

**Note:** Cisco IOS Firewall offers limited protection against directed attacks on specific operating

system and application vulnerabilities. The DoS protection of the Cisco IOS Firewall offers no guarantee of protection from compromise on end–host services that are exposed to potentially hostile environments.

11. Monitor the DoS protection activity your network. Ideally, you must use a syslog server, or ideally, a Cisco Monitoring and Reporting Stations (MARS) to record occurrences of DoS attack detection. If detection happens very frequently, you need to monitor and adjust your DoS protection parameters.

For more information about TCP SYN DoS attacks, refer to Defining Strategies to Protect Against TCP SYN Denial of Service Attacks.

# Verify

There is currently no verification procedure available for this configuration.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

# Related Information

- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation – Cisco Systems**