



## Application Note

# Tuning Cisco IOS Classic and Zone-Based Policy Firewall Denial-of-Service Protection

**Prior to Cisco IOS® Software Release 12.4(11)T, Cisco IOS Firewall provided denial-of-service (DoS) attack protection as a default when either Classic or Zone-Based Policy Firewall was applied. Cisco IOS Software Release 12.4(11)T modified the default DoS settings so protection is effectively disabled, but the connection activity counters are still active. This document provides procedures to tune Cisco IOS Firewall DoS protection values for both Classic and Zone-Based Cisco IOS Firewall.**

Cisco IOS Firewall 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. 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. Cisco IOS Firewall also regards User Datagram Protocol (UDP) sessions with traffic in only one direction as “half-open,” as nearly all applications that use UDP for transport will acknowledge 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. Large numbers of half-open connections may be indicative of malicious activity such as DoS or distributed-denial-of-service (DDoS) attacks. An example of one type of DoS attack is malicious individuals writing worms or viruses that infect multiple hosts on the Internet and attempt to overwhelm specific Internet servers with SYN attacks, in which large numbers of SYN connections are sent to a server by multiple hosts on the public Internet or within an organization’s private network. SYN attacks represent a hazard to Internet servers, as servers’ connection tables 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 victim server’s TCP connection list prevents legitimate users from gaining access to the victim Internet servers.

When DoS protection is active (that is, the default values are used on older software releases, or the values have been adjusted to the range that will affect traffic), DoS protection monitors connections through the interface where inspection is applied, in the direction in which the firewall is applied, for the protocols that the firewall policy is configured to inspect. Cisco IOS Firewall DoS protection is only applied to network traffic if the traffic enters or leaves an interface with inspection applied in the same direction of the traffic’s initial movement.

Cisco IOS Firewall inspection provides several adjustable values to protect against DoS attacks. Cisco IOS Software releases prior to 12.4(11)T have default DoS values that may interfere with proper network operation if they are not configured for the appropriate level of network activity in networks where connection rates will exceed the defaults. These parameters allow you to configure the points at which your firewall router’s DoS protection begins to take effect. When your router’s DoS counters exceed the default or configured values, the router will reset 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 will send a syslog message if logging is enabled, and if an intrusion prevention system (IPS) is configured on the router, the firewall router will send a DoS signature message via Security Device Event Exchange (SDEE). If the DoS parameters are not adjusted to your network’s normal behavior, normal network activity may trigger the DoS protection mechanism, causing application failures, poor network performance, and high CPU utilization on the Cisco IOS Firewall router.

## TUNING CISCO IOS ZONE-BASED POLICY FIREWALL

Zone-Based Policy Firewall maintains counters of the number of “half-open” TCP and UDP connections, as well as the total connection rate through the firewall and IPS software, for every firewall policy-maps’ class-maps. Thus, every class-map configured with the “inspect” action in a policy-map carries its own set of DoS protection counters. Each class-map’s DoS protection is individually configurable with a parameter-map that modifies the DoS protection values.

Zone-Policy Firewall provides protection from DoS attack *by default* when a Zone-Policy Firewall is applied. The DoS protection is enabled on the zone-pair, in the direction in which the firewall is applied, for each class-map that the firewall policy is configured to inspect. DoS protection is only applied to network traffic if the *inspect* action is applied to traffic matching the class-map. Zone-Policy 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 may interfere with proper network operation if they are not configured for the appropriate level of network activity in networks where connection rates will exceed the defaults.

**Table 1.** Zone-Based Policy Firewall Default DoS Protection Limits prior to Release 12.4(11)T

Value	Limits Per Class-Map For Zone-Based Firewall
max-incomplete high value	500
max-incomplete low value	400
one-minute high value	500
one-minute low value	400
tcp max-incomplete host value	50

These parameters allow you to configure the points at which your firewall router’s DoS protection begins to take effect. When your router’s DoS counters exceed the default or configured values, the router will reset 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 will send a syslog message if logging is enabled, and if Intrusion Protection System (IPS) is configured on the router, an SDEE message will be sent to the monitoring station. If the DoS parameters are not adjusted to your network’s normal behavior, normal network activity may trigger the DoS protection mechanism, causing application failures, poor network performance, and high CPU utilization on the Zone-Policy Firewall router.

The counter for “ip inspect max-incomplete high” and “ip inspect max-incomplete low” maintains a sum of all TCP, UDP, and Internet Control Message Protocol (ICMP) application connection attempts that have not yet reached completion.

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 during the preceding minute of the router’s operation, whether the connections have been successful or not. A rising connection rate could be indicative of a worm infection on a private network, or an attempted DoS attack against a server.

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

Follow this procedure to tune your firewall's DoS protection to your network's activity:

1. Be sure your network is not infected with viruses or worms that could lead to erroneously large half-open connection values and attempted connection rates. If your network is not a "clean slate," there is no way to properly adjust your firewall's DoS protection.
2. Define a parameter-map and set the max-incomplete high values to very high values:

```
parameter-map type inspect DoS-param-map
max-incomplete high 20000000
one-minute high 100000000
tcp max-incomplete host 100000 block-time 0
```

Apply the parameter-map to every class-map's inspection action:

```
policy-map type inspect z1-z2-pmap
class type inspect my-cmap
inspect DoS-param-map
```

**Note:** If your router is running Cisco IOS Software Release 12.4(11)T, you do not need to raise the default DoS Protection values, because they are already set to their maximum limits.

This will prevent the router from providing DoS protection for the time being while you observe your network's connection patterns. If you wish to leave DoS protection disabled, stop following this procedure now.

3. Clear the Cisco IOS Firewall statistics, using the following command:
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's pattern over a full day's activity cycle. *While the values are adjusted to very high levels, your network will not benefit from Cisco IOS Firewall or IPS DoS protection.*
5. After waiting for some observation period, check the DoS counters with the following command. The parameters you must observe to tune your DoS protection are highlighted in **bold** text:

```
router#sh policy-map type inspect zone-pair priv-pub
Zone-pair: priv-pub
```

```
Service-policy inspect : priv-pub-pol
```

```
Class-map: priv-pub-cmap (match-all)
Match: access-group 111
Match: class-map match-any all-protocol-cmap
Match: protocol tcp
    24009 packets, 671569 bytes
    30 second rate 0 bps
Match: protocol udp
    42403 packets, 3244932 bytes
    30 second rate 0 bps
Match: protocol icmp
    6 packets, 240 bytes
    30 second rate 0 bps
```

```

Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [14239:726275]
udp packets: [43748:1572372]
icmp packets: [2:19]

Session creations since subsystem startup or last reset 46282
Current session counts (estab/half-open/terminating) [45:22:10]
Maxever session counts (estab/half-open/terminating) [92:46:33]
  Last session created 00:00:45
  Last statistic reset never
  Last session creation rate 1
Maxever session creation rate 270
  Last half-open session total 0

Class-map: class-default (match-any)
Match: any
Drop (default action)
80254 packets, 8678464 bytes

```

**Note:** If the software image installed in your router is not Cisco IOS Software Release 12.4(11)T or newer, you will not see the “maxever session creation rate” statistic in your “sh policy-map type inspect zone-pair” output.

6. Configure the parameter-map’s “max-incomplete high” to a value 25 percent higher than your router’s indicated *maxever session count half-open* value. A 1.25 multiplier offers 25 percent headroom above observed behavior.

For example:

```
Maxever session count (estab/half-open/terminating) [92:46:33]
```

$46 * 1.25 = 58$ , thus, configure:

```
parameter-map type inspect DoS-param-map
max-incomplete high 58
```

7. Configure “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) [92:46:33]
```

Thus, configure:

```
parameter-map type inspect DoS-param-map
max-incomplete low 46
```

8. Cisco IOS Software Release 12.4(11)T introduced a new counter to track the maximum one-minute rate the router has reached since the last restart or statistic reset. If you have Cisco IOS Software Release 12.4(11)T or a newer software version, you may simply apply the “maxever session creation rate” value for the “one-minute low” value in your parameter map.

For example:

```
Maxever session creation rate 270
```

Thus, configure:

```
parameter-map type inspect DoS-param-map
```

one-minute low 270

9. Configure the parameter-map's "max-incomplete high" to a value 25 percent higher than your router's indicated *maxever session creation rate* value. A 1.25 multiplier offers 25 percent headroom above observed behavior.

For example:

```
Maxever session creation rate 270
```

$270 * 1.25 = 338$  (after rounding), thus, configure:

```
parameter-map type inspect DoS-param-map  
one-minute high 338
```

Proceed to step 12 if your router is running Cisco IOS Software Release 12.4(11)T or newer. Steps 10 and 11 are only needed if you have an older version of Cisco IOS Software that does not support a high-water-mark for the one-minute rate.

10. Cisco IOS Software releases prior to 12.4(11)T did not maintain a value of the maxever session creation rate, so you must calculate the value you will apply based on observed half-open maxever values. The counter for "one-minute high" and "one-minute low" maintains a sum of all TCP, UDP, and ICMP connection attempts during the preceding minute of the router's operation, whether the connections have been successful or not. You may need to experiment with your calculated one-minute value to find the ideal multiplier, but as a starting point, calculate the *ip inspect one-minute low* value by multiplying the indicated "established" value by three.

For example:

```
Maxever session counts (estab/half-open/terminating) [92:46:33]
```

$92 * 3 = 276$ , thus, configure:

```
parameter-map type inspect DoS-param-map  
one-minute low 276
```

11. Calculate and configure "ip inspect one-minute high". The *one-minute high* value should be 25 percent greater than the calculated *one-minute low* value.

For example:

```
ip inspect one-minute low (276) * 1.25 = 345, thus, configure:  
parameter-map type inspect DoS-param-map  
one-minute high 345
```

12. You will need to define a value for "ip inspect tcp max-incomplete host" according to your understanding of your servers' capability.
13. Repeat this procedure for every inspect-type class-map contained within a policy-map that must have unique DoS protection requirements. As mentioned in Step 2 of this procedure, you may define one parameter that has very high DoS parameters for class-maps that will not need DoS protection, and use different parameter-maps for specific class-maps that need unique levels of DoS protection. If DoS protection is not required for a given policy-map's class-map's traffic, you should configure high limits for the DoS protection values, and apply the high limits to all relevant class-maps' inspection. If your router is loaded with Cisco IOS Software Release 12.4(11)T or later, the DoS protection is already effectively disabled through the default high DoS protection values.
14. Monitor your network's DoS protection activity. Ideally, you should use a syslog server and record occurrences of DoS attack detection. If detection happens very frequently, you may need to monitor and adjust your DoS protection parameters.

For more information about TCP SYN DoS attacks, please visit: <http://www.cisco.com/warp/public/707/4.html>

## 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. The 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 2 may interfere with proper network operation if they are not configured for the appropriate level of network activity in networks where connection rates will exceed the defaults.

**Table 2.** Classic Firewall Default DoS Protection Limits Prior to Release 12.4(11)T

Value	Limits Per Device for Classic Firewall
max-incomplete high value	500
max-incomplete low value	400
one-minute high value	500
one-minute low value	400
tcp max-incomplete host value	50

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

These parameters allow you to configure the points at which your firewall router's DoS protection begins to take effect. When your router's DoS counters exceed the default or configured values, the router will reset 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 will send a syslog message if logging is enabled, and if Intrusion Protection System (IPS) is configured on the router, an SDEE message will be sent to the monitoring station. If the DoS parameters are not adjusted to your network's normal behavior, normal network activity may trigger the DoS protection mechanism, causing application failures, poor network performance, and high CPU utilization on the Cisco IOS Classic Firewall router.

The counter for "ip inspect max-incomplete high" and "ip inspect max-incomplete low" maintains a sum of all TCP, UDP, and Internet Control Message Protocol (ICMP) application connection attempts that have not yet reached completion.

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 during the preceding minute of the router's operation, whether the connections have been successful or not. A rising connection rate could be indicative of a worm infection on a private network, or an attempted DoS attack against a server.

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

Follow this procedure to tune your firewall's DoS protection to your network's activity:

1. Be sure your network is not infected with viruses or worms that could lead to erroneously large half-open connection values and attempted connection rates. If your network is not "clean", there is no way to properly adjust your firewall's DoS protection.
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
```

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

This will prevent the router from providing DoS protection while you observe your network's connection patterns. If you wish to leave DoS protection disabled, stop following this procedure now.

3. Clear the Cisco IOS Firewall statistics, using the following 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's pattern over a full day's activity cycle.

**Note:** While the values are adjusted to very high levels, your network will not benefit from Cisco IOS Firewall or IPS DoS protection.

5. After the observation period, check the DoS counters with the following command. The parameters you must observe to tune your DoS protection are highlighted in **bold** text:

```
router#show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [528:22519]
  udp packets: [318:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 766
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [92:46:33]
Last session created 00:12:21
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 270
Last half-open session total 0
```

6. Configure "ip inspect max-incomplete high" to a value 25 percent higher than your router's indicated *maxever session count half-open* value. A 1.25 multiplier offers 25 percent headroom above observed behavior.

For example:

```
Maxever session count (estab/half-open/terminating) [92:46:33]
```

$46 * 1.25 = 57$  (after rounding)

Thus, configure:

```
router(config)#ip inspect max-incomplete high 57
```

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) [92:46:33]
```

Thus, configure:

```
router(config)#ip inspect max-incomplete low 46
```

8. Cisco IOS Software Release 12.4(11)T introduced a new counter to track the maximum one-minute rate the router has reached since the last restart or statistic reset. If you have one of these or newer software versions, you may simply apply the “maxever one-minute rate” value for the “one-minute low” value in your parameter map.

For example:

```
router#show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [528:22519]
  udp packets: [318:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 76
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [92:46:33]
Last session created 00:12:21
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 270
Last half-open session total 0
```

Thus, configure:

```
parameter-map type inspect DoS-param-map
  one-minute low 270
```

9. Configure the parameter-map’s “max-incomplete high” to a value 25 percent higher than your router’s indicated *maxever session count half-open* value. A 1.25 multiplier offers 25 percent headroom above observed behavior.

For example:

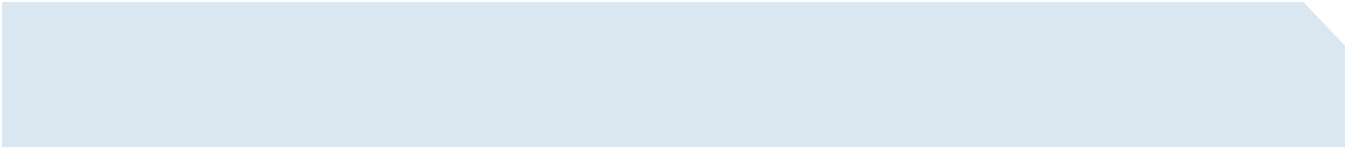
```
Maxever session creation rate 270
```

$270 * 1.25 = 338$  (after rounding), thus, configure:

```
parameter-map type inspect DoS-param-map
  one-minute high 338
```

Proceed to step 12 if your router is running Cisco IOS Software Release 12.4(11)T or newer. Steps 10 and 11 are only needed if you have an older version of Cisco IOS Software that does not support a high-water-mark for the one-minute rate.

10. Cisco IOS Software releases prior to 12.4(11)T did not maintain a value of the maxever one-minute connection rate, so you must calculate the value you will apply based on observed maxever values. While the maximum indicated values for established, half-open, and terminating sessions are unlikely to occur in the same instant, the calculated values used for the one-minute settings have been observed to be reasonably accurate. To calculate the *ip inspect one-minute low* value, add the indicated “established” value by three.



For example:

```
Maxever session counts (estab/half-open/terminating) [92:46:33]
```

$92 * 3 = 276$

Thus, configure:

```
ip inspect one-minute low 276
```

11. Calculate and configure “ip inspect one-minute high”. The *ip inspect one-minute high* value should be 25 percent greater than the calculated *one-minute* low value.

For example:

```
ip inspect one-minute low (276) * 1.25 = 345 (after rounding)
```

Thus, configure:

```
ip inspect one-minute high 345
```

12. You will need to define a value for “ip inspect tcp max-incomplete host” according to your understanding of your servers’ capability.
13. Monitor your network’s DoS protection activity. Ideally, you should use a syslog server and record occurrences of DoS attack detection. If detection happens very frequently, you may need to monitor and adjust your DoS protection parameters.

For more information about TCP SYN DoS attacks, visit: <http://www.cisco.com/warp/public/707/4.html>



**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic  
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy  
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

Printed in USA

C27-372549-00 10/06