

Cisco IOS Firewall Performance Guidelines for Cisco Integrated Services Routers

Performance guidelines for Cisco Zone-Based Policy Firewall implementation with NAT/PAT on Cisco 800, 1800, 2800, and 3800 Series Integrated Services Routers.

Abstract

Cisco IOS® Software Release 12.4(6)T introduced a new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers, increased control of firewall policy application, and a default deny-all policy that prohibits traffic between firewall zones until an explicit policy is applied to allow desirable traffic.

This document provides performance guidelines for Cisco IOS Firewall implementation with Network Address Translation (NAT) and Port Address Translation (PAT) on Cisco® 800, 1800, 2800, and 3800 Series Integrated Services Routers.

This performance analysis provides following test results with Cisco IOS Software Release 12.4(6)T:

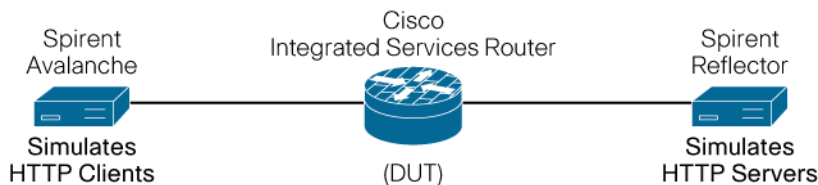
- Maximum Connections per Second (CPS) with HTTP traffic
- Maximum Throughput with 100% HTTP traffic for different object size (from 4 to 512 KB)

Cisco Zone-Based Policy Firewall Performance Testing and Results

Performance Testing

Firewall testing was performed with different object sizes to test the firewall limitations in both connections per second (small object size) and packet processing power (large object size). A small object size tests the router's ability to set up and tear down TCP connections; a large object size will not stress the TCP setup rate but will stress the packet inspection and forwarding features of the platform.

Figure 1. Cisco IOS Firewall Test-Bed



The test bed is comprised of a Spirent Web Avalanche (simulates HTTP clients) and a Spirent Web Reflector (simulates HTTP servers). Clients initiate TCP sessions and perform a "HTTP GET" from the server through the Cisco Integrated Services Router or device under test (DUT). The number of TCP connections per second is increased until "unsuccessful" is observed in TCP/IP transactions.

Various page sizes provide a range of HTTP throughput rates under different traffic conditions. These test results can be used as a guideline to determine which Cisco Integrated Services Router platform to deploy in each network environment.

Performance Results

In the firewall performance testing, the firewall is only responsible for opening and closing ports based on its TCP or UDP state tables without having to look deeper than Layer 4 of the OSI model. Figure 2 shows the maximum connections per second with HTTP traffic. Figure 3 shows the maximum HTTP throughput with Cisco Zone-Based Policy Firewall.

Figure 2. Maximum Connections per Second with HTTP Traffic

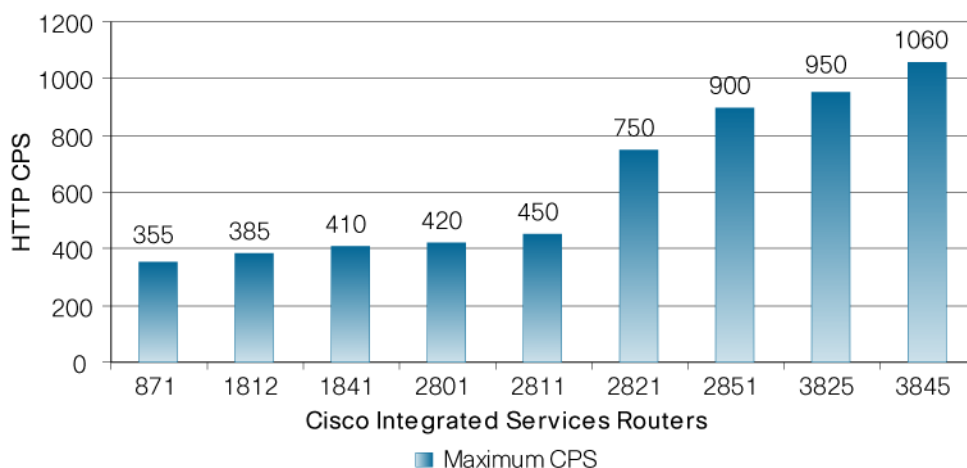
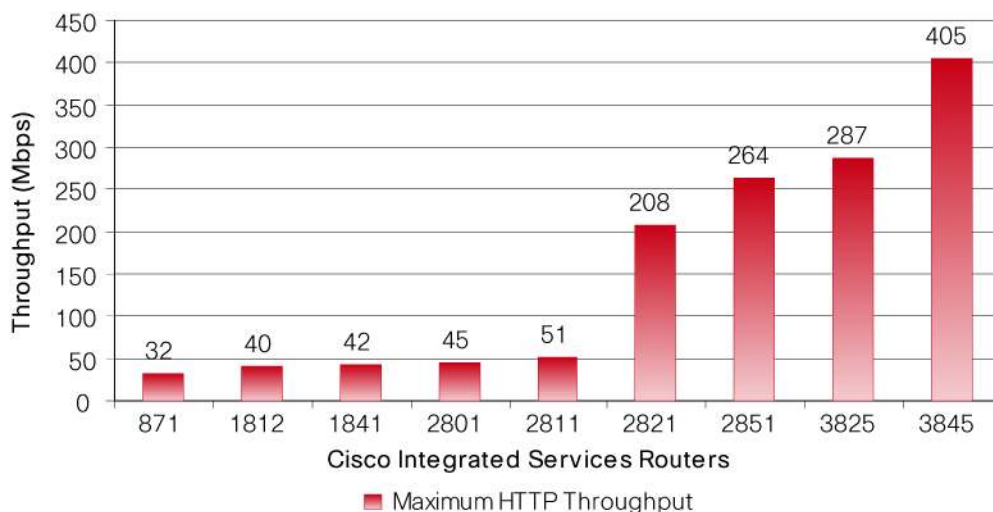


Figure 3. Maximum HTTP Throughput Using 64 KB Object Size



Conclusion

Cisco IOS Firewall performance numbers with TCP traffic are much better than for UDP traffic. Cisco improved TCP session setup performance in Cisco IOS Software Release 12.4(4)T by moving TCP session setup into the Cisco Express Forwarding (CEF) switching path. This reduced CPU impact for TCP session setup, improved TCP session setup rate, and increased TCP throughput.

In contrast, UDP traffic does not provide flow information for Cisco IOS Firewall, so each packet is treated as a new stream, leaving a half-open connection. The half-open connection will not allow a return packet, as there is no state information for the Cisco IOS Firewall to monitor. More CPU utilization is required to open a new connection for each packet.

Additional analysis summary

1. In this case, HTTP traffic is inspected by Cisco IOS Firewall and the inspection rules are configured to inspect TCP and UDP protocols. However, it is observed that performance impact will remain same, if the firewall inspection rules are configured to inspect HTTP and DNS protocols directly, instead of TCP and UDP protocols.
2. The NAT session limit is bound by the amount of available DRAM in the router. Each NAT translation consumes about 160 bytes in DRAM.

Note: These performance tests did not reach the maximum NAT/PAT session limit, as the integrated services router had abundant DRAM. It was the CPU utilization percentage that was limiting the maximum HTTP throughput.

For More Information

For more information, please visit the following links:

Zone-Based Policy Firewall

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html

Discussion of Cisco IOS Software Release 12.4(6)T with Zone-Based Policy Firewall

http://www.cisco.com/en/US/prod/vpndevc/ps5708/ps5710/ps1018/prod_configuration_example0900aecd804f1776.pdf

Zone-Based Policy Firewall Design Guide

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Router Configuration: Zone-Based Firewall with PAT

```
hostname Cisco_ISR
!
ip cef
!
parameter-map type inspect fw-rmap
  max-incomplete high 20000000
  one-minute high 20000000
  tcp max-incomplete host 20000000 block-time 0
!
class-map type inspect match-any fw-cmap
  match protocol tcp
  match protocol udp
!
policy-map type inspect fw-pmap
  class type inspect fw-cmap
    inspect fw-rmap
  class class-default
!
```

