Cisco IPS Performance

Measuring and testing performance on Intrusion Prevention Systems requires both an understanding of the characteristics of the network environment targeted in the IPS deployment, as well as an awareness of the challenges in building an effective test methodology for a sophisticated traffic inspection technology. This document describes the Cisco IPS philosophies and methodologies for characterizing IPS performance.

Delivering Performance

Cisco IPS Sensors are designed to meet the rigors of a broad range of applications and network use. In today's contemporary enterprise, applications are leveraging the Internet as never before. Voice over IP, E-Commerce, streaming video and Web 2.0 enable higher productivity and employee collaboration. These networked applications pose different and varying demands on resources such as connection rates, concurrent connections, flow length, transaction size etc. From a performance perspective, there is a spectrum of application types ranging from media-rich environments that feature converged content to highly transactional environments populated by rapid-fire, lightweight connections.

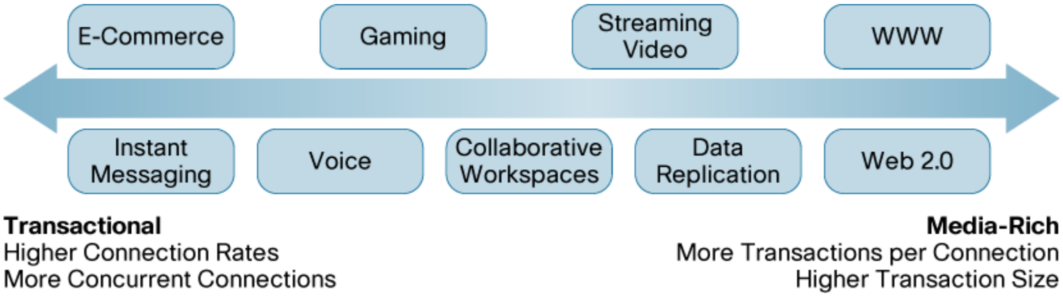
Cisco IPS technology evaluates a diverse suite of metrics in both "media-rich" and "transactional" environments, enabling you to anticipate true IPS performance based on the unique characteristics of your real-world environment.

Media-Rich

Media-rich environments are characterized by content. Content seen on most popular Websites falls on the media-rich end of the spectrum, as do video content and file transfers. If your environment is driven by access to large amounts of data and converged, immersive experiences, your environment is more media-rich.

Transactional

Transactional environments are characterized by connections. Many types of e-commerce environments fall on this end of the spectrum, as can instant messaging and voice. If your environment is driven by connection-intensive applications and small transaction sizes, your environment is more transactional.



Traffic Profiles and Testing Tools

Different environments have different characteristics that each can have a large impact on the relative performance of an IPS processing that traffic. Some of these factors include; protocol of traffic (stateful or stateless; TCP vs UDP), number of new connections per second, number of concurrent connections being tracked, amount of data being sent, amount of data being requested, number of transactions per connection, application being inspected (HTTP vs FTP), and others. Changes in any one of these metrics can change the tested performance of the box.

What type of traffic should be used? The best traffic is your specific network's real traffic. Since that isn't always feasible or even advisable, the next best thing is the closest traffic you can get to your real traffic. Using test tools to approximate real traffic can be difficult. Basic test tools are often stateless, or do not properly replicate a TCP/IP stack. For example, when testing TCP, the tools need to be accepting of a lost packet and it needs to resend that packet. The behavior of the protocol needs to mimic a real conversation as much as possible.

Given that on most typical networks, HTTP traffic makes up a large percentage of the traffic, it makes sense that it make up most or all of the test traffic. This doubly tests IPS systems as HTTP has many relevant attacks, and has characteristics that make it difficult to process: connection based so state must be tracked, large amounts of data to parse, and often short lived so large amounts of new connections are required. This makes HTTP an excellent protocol for background traffic for testing IPS systems. The industry standard tool used to generate this traffic is Spirent's Web Avalanche/Reflector tool.

Using traffic replays to generate background traffic will in most cases generate erroneous results, because in nearly every case, the replayed traffic does not realistically mimic stateful bidirectional protocol and application behavior. For example, replay tools can be flawed because the replay will use the same sequence numbering over and over or it won't be tolerant of packets that get dropped because of congestion, etc.

Attack Protection Profiles for Testing

Different IPS vendors take different stances on the issue of which detection services to enable during testing. Cisco believes that the recommended attack detection profile should be the same one used in performance testing. Otherwise you really have no idea how the sensor will behave when put into actual production. To that end the Cisco IPS is tested with its default and recommended signature policy and inspections during all performance testing.

Performance Metrics for Transactional vs Media Rich Environments

The two different test environments used to test IPS are defined in terms of the parameters used to reproduce them on a Spirent Web Avalanche/Reflector pair.

Table 1. Characteristics of Media-Rich and Transactional test environments

	Media-Rich	Transactional
Traffic Protocols	HTTP	HTTP
URL Length	100 bytes	100 bytes
Connections/sec	Low	High
Transactions per Connection	Multiple	One
Object size per Transaction	Large	Small
Average Packet Size	765 bytes	440 bytes

There are, of course, other important settings while getting a test to run and end up with similar numbers. For complete details, please contact the Cisco IPS team.

When placed in these test environments, the high performance Cisco IPS 4270 sensor produces the following results:

Table 2. Performance characteristics of Cisco IPS 4270 sensor

	Media-Rich	Transactional
Throughput	4 Gbps	2 Gbps
Connections/sec	10,000	20,000
Concurrent Connections	100,000	200,000

It is important to understand that these numbers represent a maximum supported load and were taken while under a >95% CPU load. Both tests were run over a 3 day period and in neither case were Web Avalanche sessions impacted. In a production deployment, we recommend you apply industry standard network device sizing techniques.

Conclusion

Network environments and traffic profiles continue to change and evolve. These changes have resulted in shifts of not only the type of traffic but the characteristics of that traffic. Due to a highly variable performance envelope for an IPS system, there is no such thing as a one size fits all performance metric. Cisco now provides two metrics to use to help appropriately place IPS technology into existing networks. The two metrics used are based on typical transactional and media rich environments. With a better understanding of how devices work in multiple environments, IPS sensors can be more effectively deployed in modern networks.

For More Information

For more information on Cisco IPS products and technology, go to http://wwwin.cisco.com/stg/products/appliances/ids/index.shtml.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-436979-00 10/07