# IxLoad Review – Test of Cisco Catalyst 6500 with Firewall- and Content Switching Module

In August 2004, Ixia commissioned independent tests at European Advanced Networking Test Center (EANTC) to verify Cisco's Catalyst 6500 content switching and firewall performance, using Ixia's IxLoad application.

The tests were commissioned by Ixia. They evaluate the performance, functionality and usability both of the Cisco Catalyst and IxLoad in detail. Cisco Systems provided the system under test and configuration support. Cisco did not contribute to the funding of the test.

The tests were conducted at EANTC lab in Berlin, Germany. Cisco provided a Catalyst equipped with:

- Supervisory Engine 720 (WS-SUP720-BASE), Software 12.2(18)SXD, HW 2.1, FW 7.7(1)
- CEF720 48 port 10/100/1000 Mbit/s Ethernet Module (WS-X6748-GE-TX), Software 12.2(17d)SXB, HW 1.2, FW 12.2(14r)S5
- Content Switching Module (WS-X6066-SLB-APC), Software 4.1(1), HW 1.6
- Firewall Module (WS-SVC-FWM-1), Software 2.2(1)10, HW 2.0, FW 7.2(1).

## IxLoad

IxLoad is a high performance traffic generation and analysis application that can simulate real-world traffic scenarios at the TCP and application layers. Manufacturers and users of current generation content-aware devices can use IxLoad to accurately assess performance and scalability of these devices in a cost-effective manner.

IxLoad simulates clients and servers for the most popular internet protocols — TCP, HTTP, SSL and FTP. IxLoad utilizes Ixia's multi-purpose hardware including the Application Load Module (ALM) and the TXS family of Ethernet Load Modules. Each port of these Load Modules has a CPU running the Linux operating system with a standards compliant TCP/IP protocol stack.

## Test Methodology and Setup

EANTC used the performance test plans of the IETF:

- Benchmarking Terminology for Firewall Performance (RFC 2647)
- Benchmarking Methodology for Firewall Performance (RFC 3511)

The test plans were adapted where necessary to specify the tests on the application layer.

All the tests results reported here were achieved using full TCP connections with HTML data being transferred. The connections follow the SYN – SYNACK – ACK – DATA (request and transfer) – FIN – FINACK – ACK model.

The emulated servers and clients were connected with 46 x 1000 Base-TX ports to the Catalyst 6509. One 100 Base-Tx port was used to inject the DDoS attacks.

## Summary of Test Results

| Test Area | Result |
|---|---|
| HTTP Session Capacity Performance | PASS |
| HTTP Session Rate Performance | PASS |
| DDoS Prevention Performance | PASS |
| FTP Concurrent Session Capacity | PASS |
| Rule Set Based Performance | PASS |
| HTTP Load Balancing Based on URL | PASS |


**EANTC extensively tested Ixia's IxLoad application. It showed expected performance values and usability features under peak load conditions.**

Tested by EANTC 2004

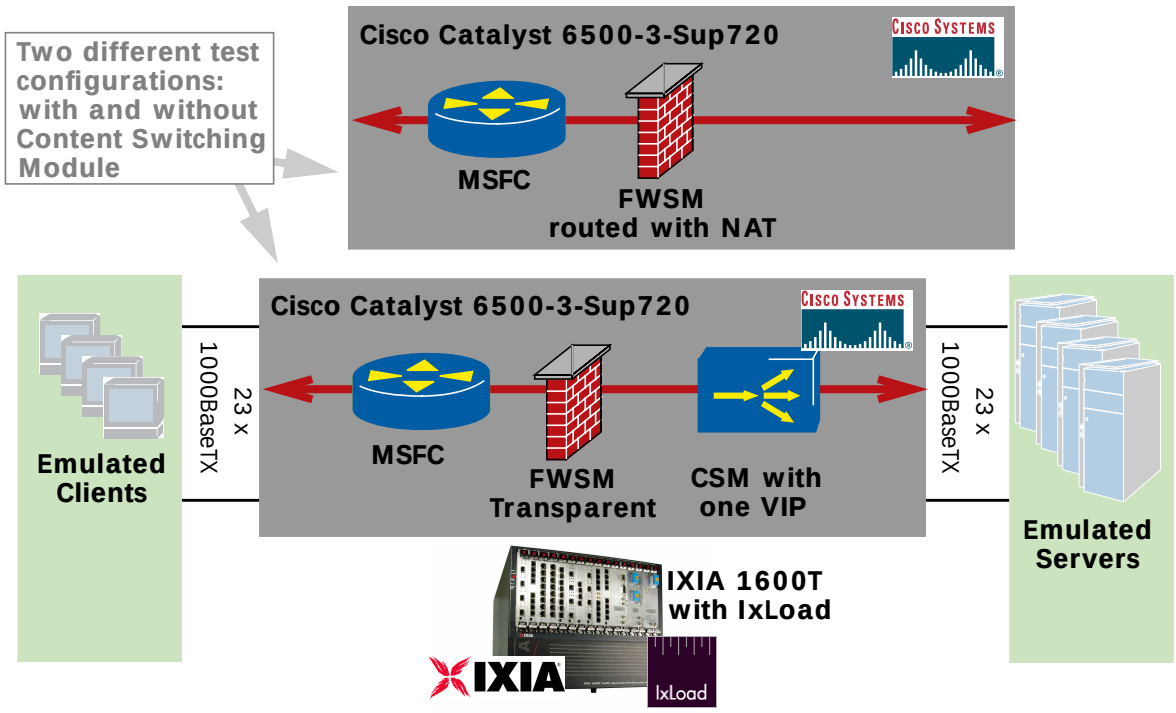
## Test Configuration

EANTC conducted the tests with two different configurations of the Cisco Catalyst 6500. First, we evaluated a regular firewall scenario representative for large enterprises, using only the Firewall Service Module (FWSM) without the Content Switch Module.

For the second scenario, a typical data center configuration, the Content Switch Module (CSM) was configured into the data path between clients and servers. The CSM switches connections to different server farms, based on different layer 4 to layer 7 protocol information like URL contents or TCP ports.

The following sections detail the results of each test case.

### Test Configuration




FWSM: Firewall Switching Module
CSM: Content Switching Module

MSFC: Multi-Service Feature Card
VIP: Virtual IP Address

## HTTP Session Capacity Performance

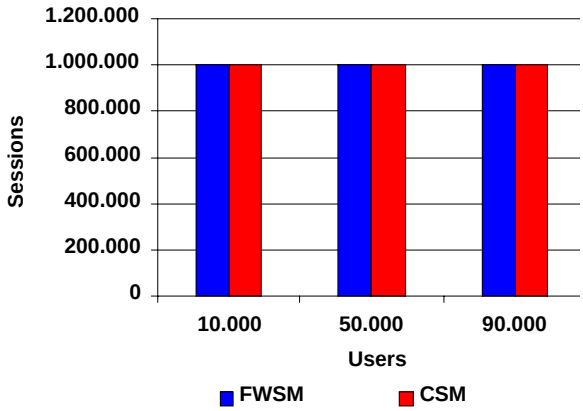
This test verified the maximum number of concurrent HTTP sessions.

**Test Parameters:**

- 90,000 client IPs, 23 server IPs
- 10,000, 50,000 and 90,000 users
- HTTP 1.0 with Keep Alive (one HTTP session per TCP connection)
- 23–120 concurrent TCP connections per user
- Object Size 50 kByte

**Results:** We were able to achieve 999,900 concurrent HTTP sessions in both scenarios, the firewall-only and the content switching configuration

**Diagram 1: HTTP Session Capacity**




## HTTP Session Rate Performance

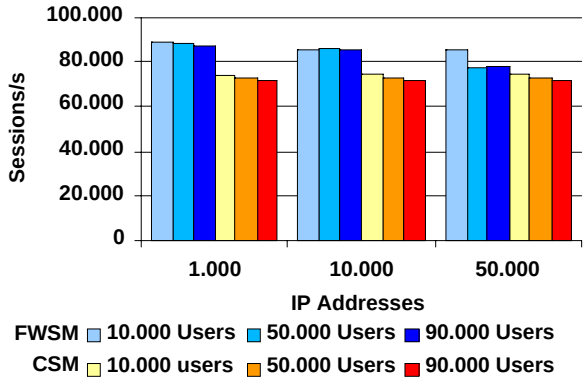
**Purpose:** This test verified how fast the DUT processes new HTTP sessions without session loss.

**Test Parameters:**

- 1,000, 10,000 and 50,000 client IPs
- 10,000, 50,000 and 90,000 users
- 23 server IP addresses
- HTTP 1.1, Object Size 1 kByte
- 1 HTTP request per TCP connection
- 1 concurrent TCP connection per user

**Results:** Without the content switching module, we could achieve a peak performance of 88,753 sessions per second, with the CSM 74,637 was the best result.

**Diagram 2: HTTP Session Rate**




Because the content switch module performs a content verification of each packet, the session setup rate is reduced by 14,000 sessions/s.

## Distributed Denial of Service Prevention Performance

This test group verifies the performance of the system under test when preventing DDoS (distributed denial of service) attacks. We evaluated in how far the overall performance is influenced by comparing the time needed to set up the maximum number of concurrent HTTP sessions with and without an attack.

**Test Parameters:**

- 50,000 client IPs, 23 server IPs
- 50,000 users
- HTTP 1.0, Keep Alive, Object Size 50 kByte
- 23 concurrent TCP connection per user

**Overview of Attack Types, Attack Rates and Cisco Action:**

*Ping Attack:* Flooding the victim (a server or an end user) with ICMP Echo Requests, thus tying it up, 147,928 attacks per second (this is the physical port limit) were sent.
*Cisco action:* Rate-limit ICMP packets.

*Land Attack:* This attack sends TCP packets with a source IP address and port number identical to the victim's IP address and port number. This causes the attacked host to think that it "speaks to itself", often leading to a crash. Attack rate: 147,928 packets/s.
*Cisco action:* Block packets in hardware.

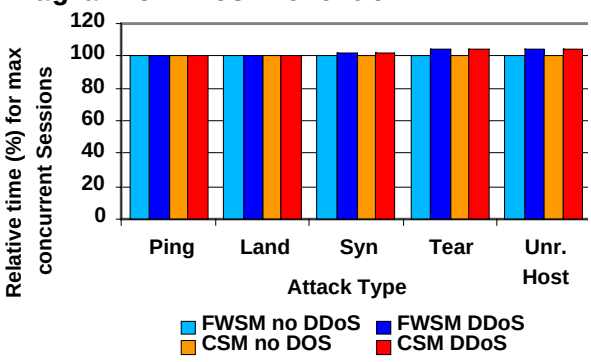
*Syn Attack:* This attack exploits the TCP session open mechanism. The attacker floods the victim with TCP SYN packets, causing the attacked host to spend a lot of time in opening a large number of TCP sessions, sending SYN-ACK's, and waiting for the ACK responses which are never returned. It also fills up the victim's TCP session buffers, thus choking it, and preventing real TCP sessions from being opened. Attack rate: 147,928 packets/s.
*Cisco action:* TCP interception allows only a small number of 'embryonic' connections.

*Tear Drop Attack:* This is a fragmented IP packet where the fragments overlap in a way that destroys the individual packet headers when the victim attempts to reconstruct the message. This may cause the victim to crash or hang up. One attack per second.
*Cisco action:* Allows a certain amount of fragments per interface by default, packet reassembly before sending it out. For this test Cisco didn't allow fragments.

*Unreachable Host Attack:* This attack simply sends ICMP Host Unreachable error messages to the victim, thus tying it up and causing it to drop connections. This type of attack may paralyze the victim even if it is sent at a very low rate. One attack per second.
*Cisco action:* Drop ICMP unreachables in hardware.

**Results:** No significant influence of the DDoS attacks was noticeable, the test results were within the margin of error. During the tests, the DUT ressource utilization regarding CPU or memory did not increase noticeable.

**Diagram 3: DDoS Prevention**




## FTP Concurrent Session Capacity

**Purpose:** This test verified the maximum number of active concurrent FTP sessions that the DUT/SUT can maintain.

**Test Parameter:**

- 23 client and 23 server ports
- 46,000 client IPs
- 460,000 users
- command sequence: login – retrieve test file of 10 kByte – think time (until end of test) – quit
- 1150 FTP connections per second (50 per port)

**Results:** Tests with both configurations (firewall-only and CSM) achieved the maximum of 460,000 concurrent FTP sessions. According to Cisco Systems both configurations should achieve 1 million concurrent connections. With the test setup of 23 client and 23 server ports we could only achieve 460,000 connections. For testing the Catalyst at the limit of 1 million, we would have to expand the test hardware by more than factor 2, as each Ixia ports peak performance was 20,000 concurrent FTP connections.

## Rule Set Based Performance

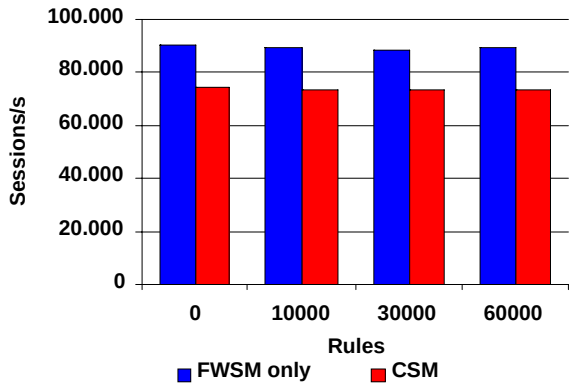
**Purpose:** This test verified the forwarding performance of the firewall services module with an increasing number of security rules (access-list entries).

**Test Parameter:**

- 0, 10,000, 30,000 and 60,000 firewall rules
- 10,000 client IPs and 10,000 users
- 23 server IPs
- HTTP 1.1, Object Size 1 kByte
- 1 concurrent TCP connection per user

**Results:** Compared to the performance figures achieved with no additional rules, the results with the various rule sets do not show a significant deviation.

**Diagram 4: Rule Set Based Performance**




## HTTP Load Balancing Based on URL

**Purpose:** This test verified the performance of the DUT while load balancing HTTP sessions based on different URL types between different server farms.

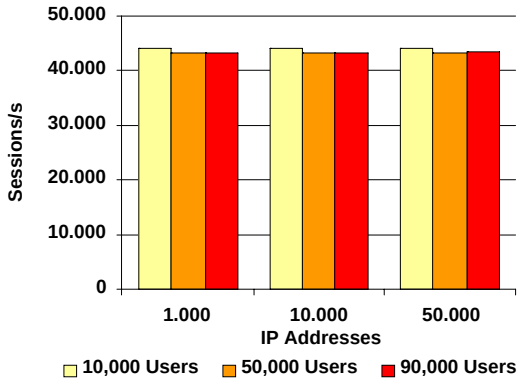
**Test Parameter:**

- URL length 128 Byte, 3 different URL types: *.wav, *.jpg and *.htm
- 1,000, 10,000 and 50,000 client IPs, 23 server IPs
- 10,000, 50,000 and 90,000 users
- HTTP 1.1, Object Size 4 kByte
- 1 concurrent TCP connection per user
- 1 transaction per TCP connection requesting

We configured three different server groups, each serving only one of the given URL types. The test traffic addressed a balanced mixture of the three groups. We verified, that during the test, all packets were delivered to the correct servers.

**Results:** As expected, the total performance in establishing HTTP sessions decreases when the DUT has to parse L7 content and match this content with certain filter rules for further forwarding decisions.

**Diagram 5: URL Based Loadbalancing**




## About EANTC

The European Advanced Networking Test Center (EANTC) offers vendor independent network test facilities for manufacturers, service providers and enterprise customers. Primary business areas include interoperability, conformance and performance testing for IP, ATM, MPLS, and broadband voice related network technologies and applications.

EANTC AG
Einsteinufer 17, 10587 Berlin, GERMANY
URL: www.eantc.com
E-mail: info@eantc.com