Miercom

# Lab Testing Summary Report

July 2012

Report SR120514

Product Category:

**Enterprise Firewall**

Vendor Tested:

CISCO

Products Tested:

**ASA 5515-X**
**ASA 5525-X**
**ASA 5555-X**

Miercom PERFORMANCE VERIFIED

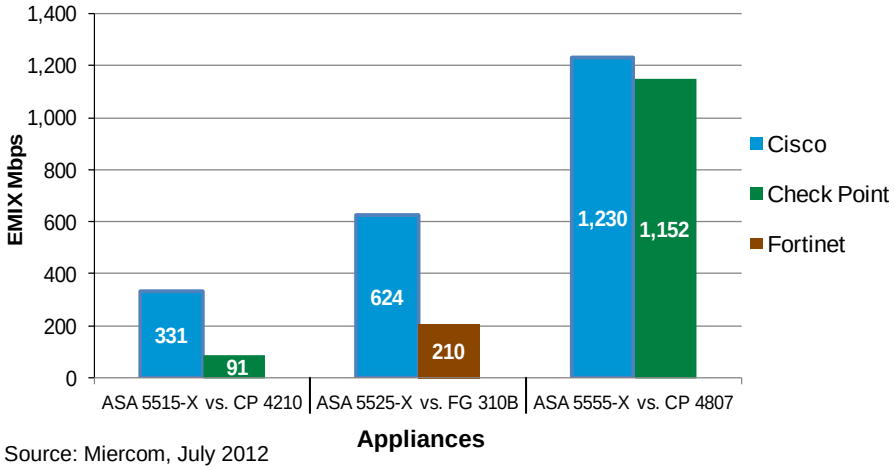
## Key findings and conclusions:

- **On the ASA 5515-X and 5525-X, EMIX traffic was better by 99% or more when compared to their counterparts**
- **UDP throughput - using IMIX (IPv4 and IPv6) - was 57% better on ASA 5500-X series appliances than the competition**
- **HTTP traffic throughput on Cisco appliances was 60% more than comparable competitor products**
- **ASA 5500-X series can process 10% more connections per second over IPv4 and 24% more over IPv6 than competitive products**

Cisco engaged Miercom to evaluate the performance of the newly launched ASA 5500-X Series of Adaptive Security Appliances against comparable products selected on the basis of intended markets and MSRP. Three different comparative scenarios were tested. Products from Check Point and Fortinet were included in the testing and compared to similar offerings from the ASA 5500-X series. The ASA 5515-X was compared to the Check Point 4210, ASA 5525-X with the FortiGate 310B, and the ASA 5555-X with the Check Point 4807 appliances. These products were chosen because they are similar in vendor-intended usage so that a fair comparison could be made.

Multiple use-cases were used to determine the maximum TCP and UDP throughput performance based on real-world scenarios, as well as to assess Next Generation IPv6 and Intrusion Prevention System (IPS) capabilities. Several parameters were recorded including CPU

**Figure 1: Testing with Real-World Traffic Mix with Firewall and IPS Enabled**




Source: Miercom, July 2012

*Intrusion Prevention System (IPS) is a resource taxing feature. Many benchmarks and specification sheets ignore performance with IPS enabled. Turning IPS on for all devices creates a true real-world test case.*

utilization, allocated memory utilization, connections per second (CPS), concurrent connections, real-world HTTP throughput, and TCP EMIX traffic to determine each device's real-world capacities.

The Cisco ASA 5500-X series appliances are purpose-built with dedicated multi-core, multi-threaded processors for firewall, VPN, and IPS security services. The appliances also feature generous RAM configurations, starting at 4 GB in the 5512-X and 16 GB in the 5555-X. The appliance combines an identity-aware firewall, IPS and VPN capabilities in one device, and includes features such as Layer 2 and 3 firewall modes, advanced deep packet inspection engines, among several other firewalling features with an ability to upgrade to more services in the future.

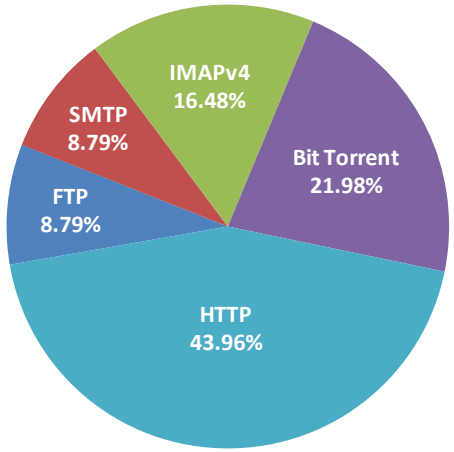
## EMIX Real-World Multi-Protocol Mix

To evaluate the performance of each appliance, a blended mix of packet sizes and protocols were used with a predominance towards TCP-based applications. See *Figure 2*. We also ran an IMIX traffic profile (see subsequent section), but we believe it does not reflect traffic patterns within an enterprise as it uses only UDP as an underlying protocol.

250 virtual hosts with three virtual servers were placed on either side of the firewall and throughput was measured with bi-directional traffic. A simple permit-all policy was configured on all firewalls. Additionally, IPS was enabled on the firewall to simulate real-world deployment. IPS performance heavily depends on the configured IPS signature profile. Because of this, we chose a comparable IPS signature profile across different vendors that mimics a real-life deployment scenario. The final objective was to measure the combined firewall and IPS throughput with a 5% margin of error on failed transactions.

We observed a 1.4Gbps throughput for this mix of traffic on the ASA 5515, 113% higher than the

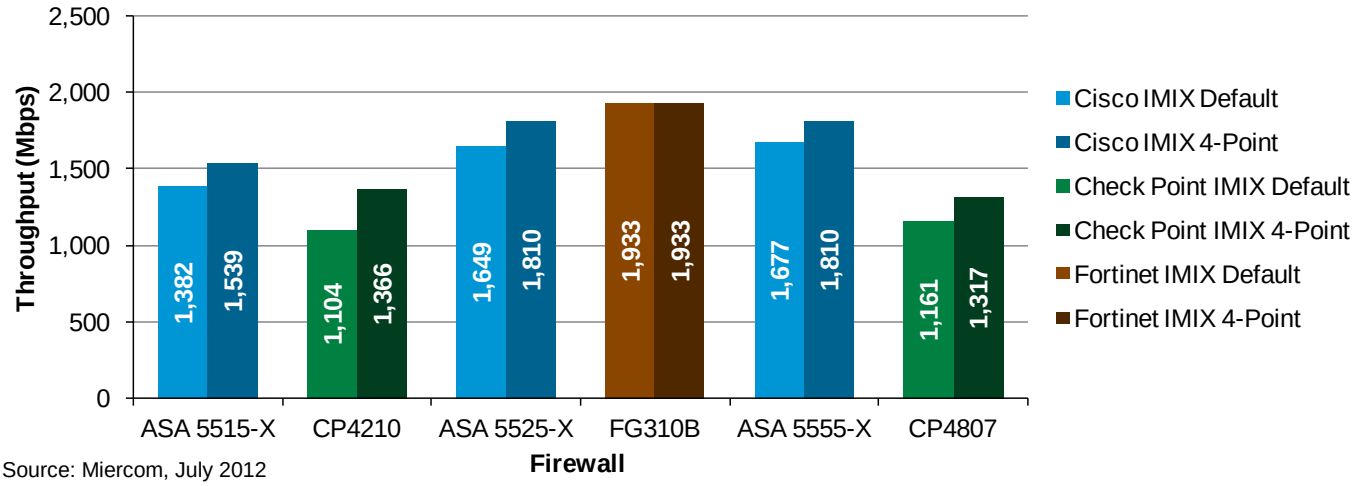
**Figure 2: EMIX Profile**
**EMIX Protocol Distribution**




Source: Miercom, July 2012

*Initial EMIX traffic composition across all devices under test is given as real-world utilization from predetermined network analysis.*

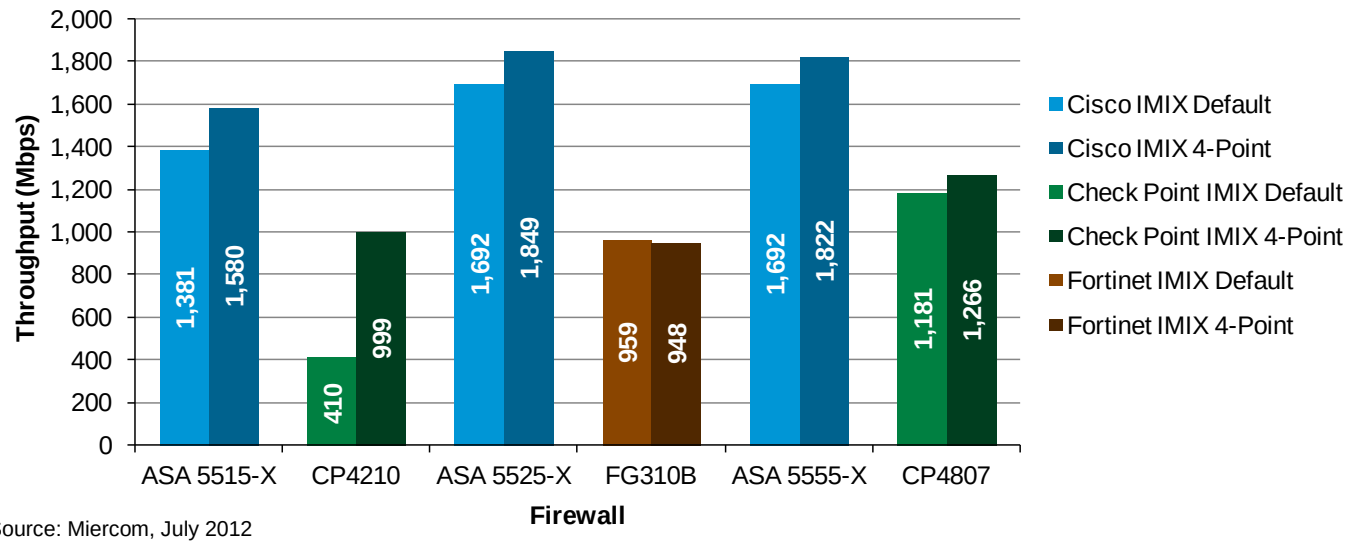
**Figure 3: Cisco ASA 5500-X Series - IPv4 UDP IMIX Traffic Throughput**




Source: Miercom, July 2012

*With the exception of the FortiGate 310B, the ASA appliances stay well above each of their competitors, showing higher numbers in frames per second, indicating their routing capabilities as well as their packet processing speeds.*

**Figure 4: Cisco ASA 5500-X Series – IPv6 UDP IMIX Traffic Throughput**




Source: Miercom, July 2012

*The ASA appliances stay well above each of their respective competitors, showing high numbers in frames per second indicating its routing capabilities and packet processing speeds.*

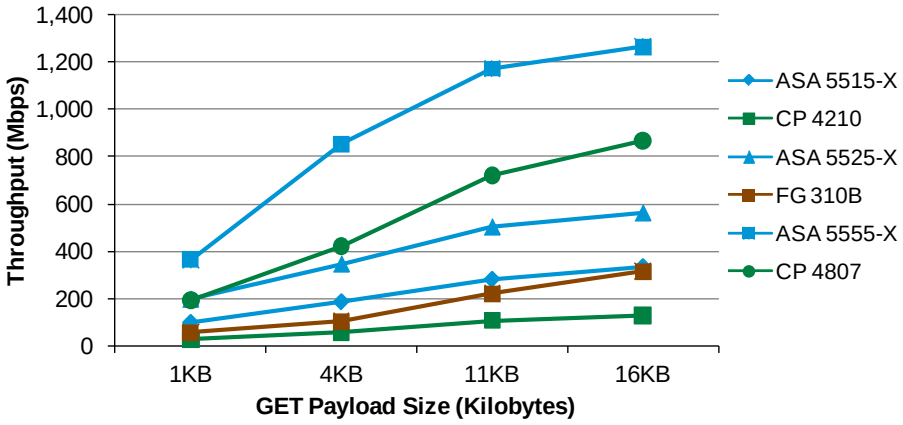
throughput for the Check Point 4210. Similarly, the ASA 5525-X was 99% higher than FortiGate 310B, and the ASA 5555-X was 6% higher than Check Point 4807. The breakdown is shown in *Figure 1* on *page 1.*

## IMIX Throughput

To determine the maximum data rate that could be sustained with no packet loss for a range of fixed packet sizes, up to 1518-byte frames, the RFC 2544 benchmarking throughput test was used with IMIX. Some firewall vendors choose to publish only fixed UDP packet size throughput numbers which we believe is an unrealistic representation of real-world deployment. A better representation of UDP throughput is an IMIX profile that uses a varied range of packet sizes. See *Figure 7* on *page 5*.

250 virtual hosts were used on either side of the firewall to provide bi-directional traffic. We also measured throughput for an IMIX 4-point traffic profile which uses random packet size distribution, instead of a fixed packet size distribution used in an IMIX default profile. See *Figure 3* on *page 2* and *Figure 8* on *page 5*.

**Figure 5: Cisco ASA 5500-X Series Max HTTP Throughput - Multiple GET**




Source: Miercom, July 2012

*IPS is a resource taxing feature. Many benchmarks and specification sheets use empty payloads and ignore IPS performance. By turning IPS on for all devices and using varied payloads, this is a true real-world test case.*

The test duration was set at 60 seconds and test results were recorded at no drop rate. If there was any loss of data, the test was restarted from the beginning with lower input metrics using a binary search algorithm to find the maximum no-drop-rate throughput for each firewall. All results shown are given with 0% data loss at the highest service level achieved for each device under test.

In addition, IPv6 UDP traffic was tested using IPv6-to-IPv6 (6to6) routing as shown in *Figure 4*.

Cisco ASA 5500-X showed similar performance for both IPv4 and IPv6. However, both Check Point and Fortinet exhibited significant degradation in performance for IPv6 as compared to IPv4. Specifically, Check Point 4200 appliance throughput degradation was 41% while Fortinet degraded by 48%. The results of the IPv4 and IPv6 CPS testing can be seen in *Figures 3* and *4* respectively.

## HTTP Maximum Throughput

To understand how well each firewall processed HTTP traffic, a scenario was created using Web traffic of varying packet sizes. We configured our test equipment to deliver an HTTP 1.1 (with persistence) payload of 1, 4, 11 and 16 kilobytes. A single HTTP GET request was generated and there was no delay in generating an HTTP response. By looking at a broad payload distribution, we can accurately estimate how the appliances will interact with all packet sizes and payload distributions. Additionally, IPS was enabled for all appliances to once again mimic a real-world deployment scenario. We recorded the maximum throughput achieved for each appliance without incurring packet loss.

The ASA 5515-X delivered 87% more throughput than the FortiGate 310B with no packet loss, ASA 5525-X delivered 56% more traffic than Check Point 4210, and ASA 5555-X delivered 37% more throughput than Check Point 4807. See *Figure 5* on *page 3*.

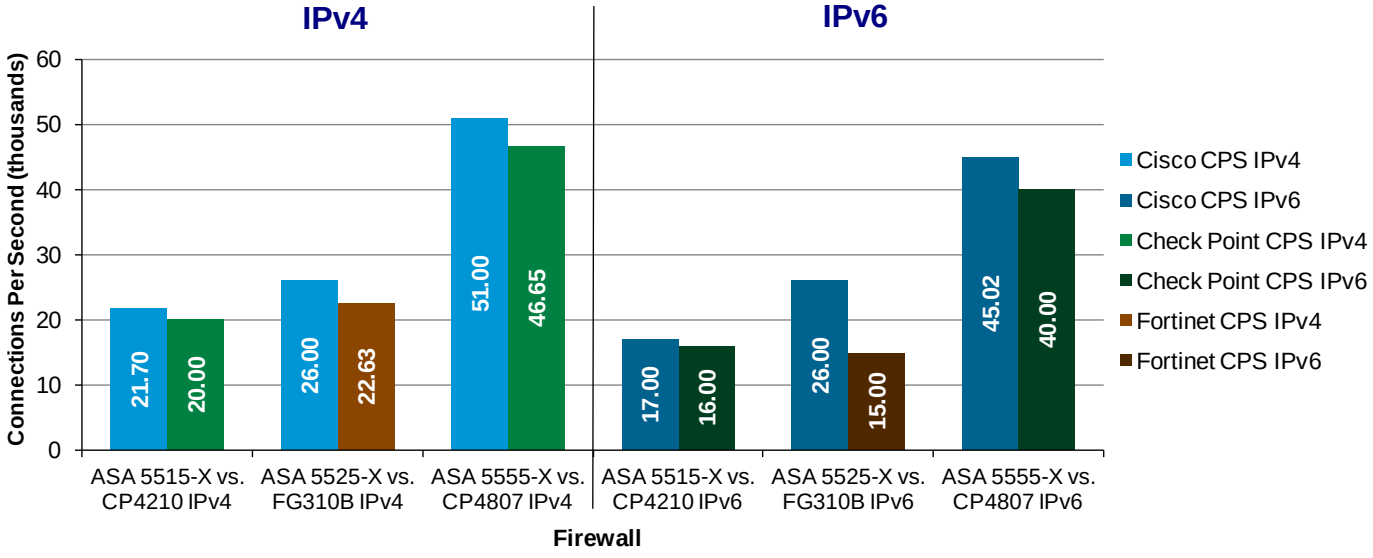
With CPU utilization at maximum during the throughput tests, Fortinet appliance GUI became unresponsive while Check Point and Cisco appliance management was unaffected.

Also, with a larger HTTP payload test, we observed that Fortinet appliances stopped IPS inspection beyond a 200KB payload, unlike the Cisco and Check Point appliances. We believe this is an attempt for performance optimization at the expense of security. Furthermore, the corresponding setting was available through CLI only and not through GUI.

Unlike Cisco and Fortinet appliances, we observed a limitation with Check Point appliances in that only a single IPS protection profile can be used across the entire appliance. It cannot be configured on a per firewall policy basis. Also, Check Point's "recommended profile" for IPS does not enable signatures tagged with 'medium-low' confidence level or signatures classified as 'low-risk.'

Lastly, on Cisco appliances, we enabled reputation-based IPS protection as well. A similar feature was not available on either Fortinet or Check Point.

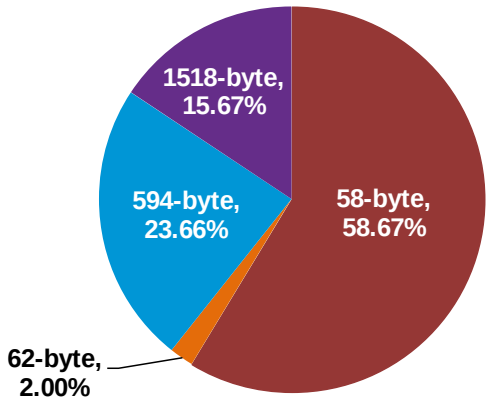
**Figure 6: Cisco ASA 5500-X Series – Connections per Second**




Source: Miercom, July 2012

*Testing full line rate connections per second on all available interfaces, with zero packet loss allowed, shows that the ASA 5500-X series is a next generation appliance, upholding its service levels better than competitors for IPv6 capability.*

**Figure 7: IMIX Default Profile**
**IMIX Composition by Traffic Contribution**




Source: Miercom, July 2012

*IMIX traffic composition across all devices under test is given by Spirent TestCenter as a UDP Internet Mix profile.*

## Connections per Second

The objective of this test is to determine the maximum number of connections per second (CPS) that the firewall can handle over TCP.

Each connection was simulated using a single HTTP 1.0 GET request with a 64-byte payload in the HTTP response with no delay on the server side. The connection was kept alive for the entire duration of the test by enabling the HTTP Keep-Alive option.

Maximum achievable CPS was measured by increasing the connection rate iteratively until there was no connection drop. We ran the test with both IPv4 and IPv6 HTTP traffic. See *Figure 6* on *page 4*.

We found that only the ASA 5500-X was able to meet the published data sheet numbers. One possible explanation for this is that some vendors use a 1-byte TCP payload for the CPS test that would result in higher CPS numbers, although a 1-byte TCP payload is unrealistic in a real-world scenario.

For IPv6, Cisco appliances had a 10% degradation in CPS, while Fortinet had a 34% degradation. Check Point had a maximum 20% degradation. We also observed frequent packet drops at maximum CPS with the Check Point appliance that was not witnessed in Cisco and Fortinet.

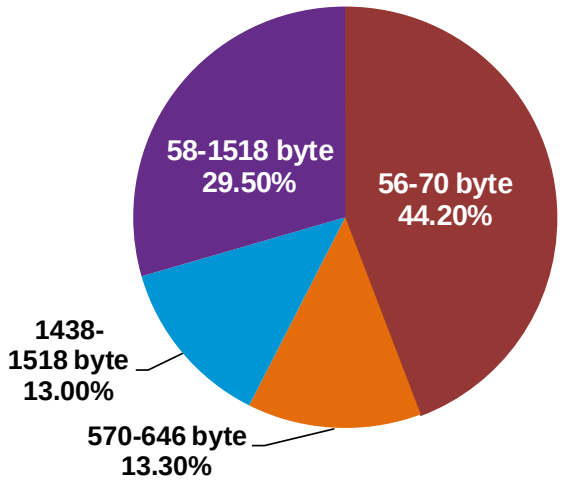
## Bottom Line

Based on the lab testing of the Cisco ASA 5515-X, 5525-X, and 5555-X Adaptive Security Appliances, Miercom verifies that the throughput capabilities of these security appliances are superior to that of its competitors: Check Point 4210, FortiGate 310B, and Check Point 4807.

Firewall and IPS combined performance with real-world traffic was 113%, 99% and 6% better on 5515-X, 5525-X and 5555-X, respectively, when compared to equivalent appliances from other vendors. With UDP traffic (both IPv4 and IPv6), firewall performance on ASA 5500-X appliances was 57% better than comparable appliances. From a connections per second perspective, ASA 5500-X also outperformed other vendors by handling 10% more connections per second for IPv4 and 24% more connections per second for IPv6 traffic.

The Cisco ASA 5515-X, 5525-X, and 5555-X appliances deliver impressive security, scalability and performance that is required for enterprise networks, data centers and Web 2.0 applications. Performance and security features earned the Cisco ASA 5515-X, 5525-X, and 5555-X Advanced Security Appliances the Miercom Performance Verified Certification.

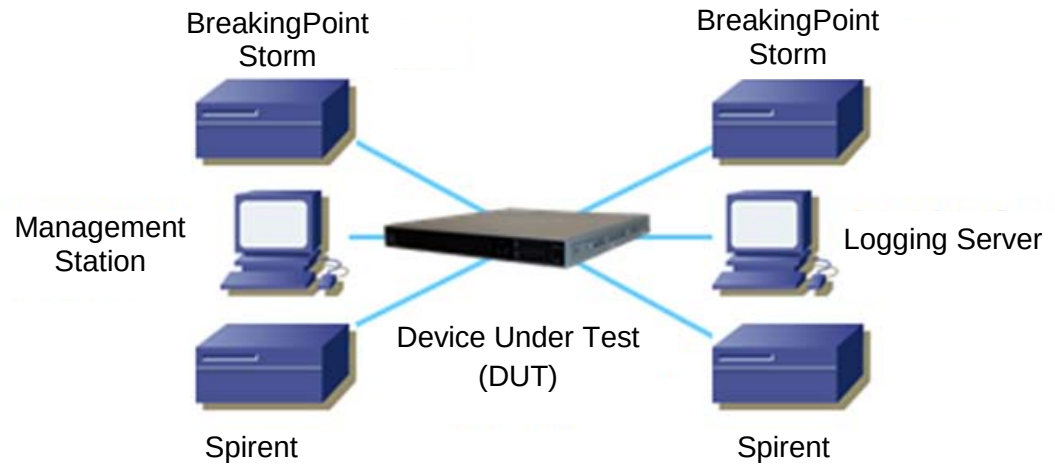
**Figure 8: IMIX 4-Point Profile**
**IMIX Composition by Traffic Contribution**




Source: Miercom, July 2012

*The long term average of this IMIX traffic distribution approaches a default IMIX profile, but the randomized distributions allows for a more realistic use case.*

## Test Bed Diagram




Source: Miercom, July 2012

## How We Did It

To fully exercise the performance of the products, the test bed utilized BreakingPoint Storm and Spirent TestCenter products. Bi-directional test traffic was generated using BreakingPoint version: 2.2.3, strikebuild: 78528, and the Spirent Test Center v3.90. Real-world HTTP tests were performed with HTTP 1.1 while transferring objects of varying sizes. CPS performance tests were conducted using BreakingPoint Storm to generate 64-byte HTTP traffic. Most benchmarks operate without a payload, but to get realistic results we added a 64-byte payload inside of the Syn-Fin HTTP transaction. UDP performance tests utilized Spirent TestCenter to send fixed and randomized frame sizes ranging from 64-byte up to 1,518 byte frame sizes.

The Cisco ASA 5515-X was equipped with six 1GE interfaces, 5525-X with eight 1GE interfaces, and 5555-X with eight 1GE interfaces. Cisco Adaptive Security Appliance (ASA) Software v8.6.1.1 with IPS version 7.1.4 with signature update S615 were used during testing. Default MTU size for TCP traffic was 1,380 bytes to allow for overhead. Default MTU size for UDP traffic was 9,216 bytes.

The Check Point 4210 was equipped with four 1GE interfaces, Fortinet FortiGate 310B with ten 1GE interfaces, and Check Point 4807 with eight 1GE interfaces. Both Check Point firewalls were running software version R75.40, and the FortiNet appliance was using 4.0MR3 release with patch 6. Although all devices had extra ports, this is primarily for functionality and not capacity. Maximum load was achieved using only two 1GE interfaces on each device.

All devices were hardware configured with default options. No external cards, processors, or other supplemental devices were attached to any devices. All devices were on separate VLANs to prevent any inadvertent interactions with one another, and all tests were run individually with large gaps of time in between to ensure no residual packets affected testing.

Both BreakingPoint Storm and Spirent TestCenter performed a binary search algorithm in order to find the highest capacity possible for each device during each test. Each test was repeated using the final value two more times to attain reliable and repeatable results. During the testing, memory and CPU utilization were monitored carefully, primarily to verify that the switches were operating normally.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for details on the configurations applied to the Device Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

## Miercom Performance Verified

The performance of Cisco ASA 5500-X Series Advanced Security Appliance was verified by Miercom. In hands-on testing, Cisco demonstrated advanced performance capabilities such as:

- Average CPS are 10% higher over IPv4, and 24% higher over IPv6 than competitors
- Cisco devices exceeded specifications with IPS enabled; competitors did not
- System performance is not affected when IPS is enabled
- ASA platform was 79% better on average in HTTP maximum throughput

Performance and security features earned the Cisco ASA 5515-X, 5525-X and 5555-X Advanced Security Appliances the Miercom Performance Verified Certification.

**Cisco ASA 5500-X Series**

**Cisco Systems, Inc.**
**170 West Tasman Drive**
**San Jose, CA**
**1-800-553-6387**
**www.cisco.com**

## About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. The Performance Verified program is a thorough and trusted assessment for product usability and performance.