Throughput and Scalability Report

McAfee NGFW 5206, v5.8

DR140912

9 October 2014

Miercom

www.miercom.com

Contents

i. Executive Summary

Intel Security engaged Miercom to perform throughput and scalability testing of the McAfee NGFW 5206 security appliance.

The McAfee NGFW 5206 can be deployed in various security roles, but was configured in this testing primarily as a high-capacity, next-generation firewall. A unique aspect of the McAfee NGFW 5206 in the firewall marketplace is the ability to "cluster" multiple units, up to 16, for environments requiring incrementally greater aggregate throughput.

This report summarizes the McAfee 5206's throughput based on the latest version 5.8 software, with various firewall policies applied and different traffic scenarios. The McAfee 5206 was first tested as a single online node in a multi-node cluster, and then the incremental throughput growth achieved by bringing two, three and four nodes in the cluster online was measured.

To obtain optimum throughput performance results, the McAfee 5206 was rebooted before every test run, along with frequent reboots of the Ixia BreakingPoint test system. This is not an uncommon practice, given the excessive volumes of data applied in the tests.

Key Findings and Conclusions

- **A single McAfee NGFW 5206 can manage up to 120 Gbps (Gigabits per second) of real-time traffic**
- **With Deep Packet Inspection (DPI) applied, the McAfee NGFW 5206 handled sustained throughput over 10 Gbps – one of the highest firewall throughputs we have seen with DPI enabled**
- **Testing showed that additional McAfee NGFW 5206 nodes in a cluster can increase aggregate throughput considerably. Adding a second node in a cluster bolsters throughput from 25 to 100 percent, depending on traffic mix and firewall features enabled**
- **A four-node cluster can boost throughput up to 370 percent – nearly four times a single node's throughput, tests found**
- **Testing confirmed that a single McAfee NGFW 5206 node can effectively process over 50,000 new TCP/HTTP connections per second, exceeding the vendor's published specifications**
- **McAfee NGFW 5206 had much more consistent throughput performance with security features enabled when compared to other products in this class. Other products tested exhibited 75 percent or more performance degradation for DPI, AntiVirus and application control when enabled**

Miercom independently substantiates the throughput performance of the McAfee NGFW 5206 from Intel Security – in standalone mode, as well as the throughput scalability achieved by clustering multiple McAfee NGFW 5206 nodes. McAfee is awarded the ***Miercom Performance Verified Certification*** for the impressive throughputs delivered by the McAfee NGFW 5206.

Robert Smithers

CEO

Miercom

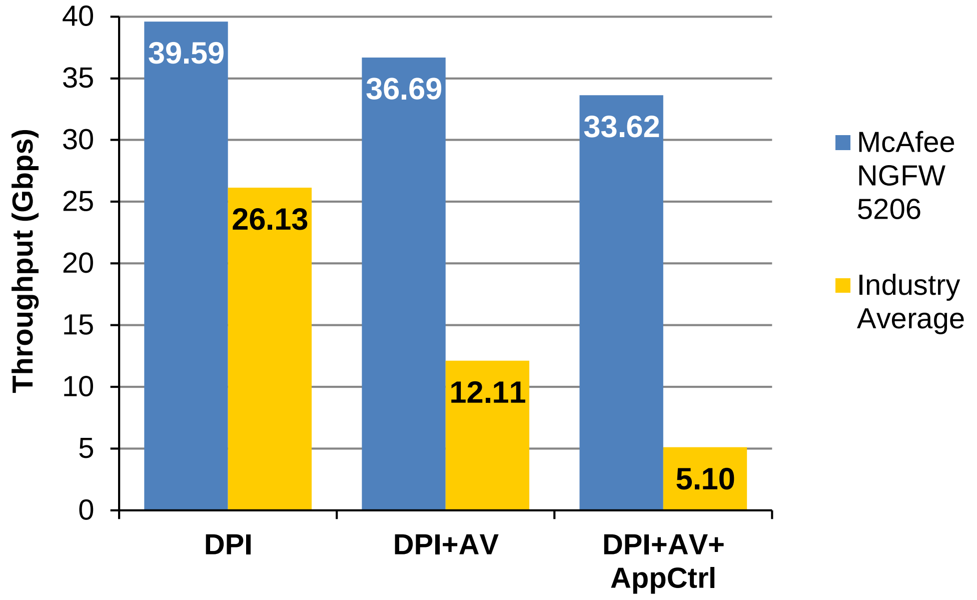
ii. Summary of Throughput Results

	Aggregate Throughput Measured, in Gbps (Gigabits per second)				
Test	**Single Node Standalone**	**Single Node in Cluster** (other three offline)	**Two-Node Cluster** (other two offline)	**Three-Node Cluster** (fourth node offline)	**Four-Node Cluster**
UDP unicast, 1518 byte 'stateful inspection'	**120.00**				
DPI w/ HTTP 21kB	**-**	**10.61**	**24.75**	**35.77**	**39.59**
DPI w/ IMIX	**-**	**12.64**	**21.38**	**31.63**	**35.78**
AntiVirus (+ DPI) w/ IMIX	**-**	**9.55**	**27.07**	**32.70**	**36.69**
DPI + URL Filtering w/ HTTP 21kB	**-**	**15.51**	**26.07**	**34.83**	**39.48**
DPI + URL Filtering w/ IMIX	**-**	**15.93**	**27.22**	**28.22**	**35.23**
Application Traffic + DPI + logging w/ UDP	**-**	**15.30**	**28.04**	**32.64**	**38.71**
Application Traffic + DPI + logging w/ HTTP 21kB	**-**	**10.21**	**13.74**	**17.40**	**33.62**
Application Traffic + DPI + logging w/ IMIX	**-**	**15.73**	**26.03**	**27.30**	**27.90**

iii. Firewall Trends

When comparing the performance of the McAfee NGFW 5206 to other products in this class, we observed much more consistent throughput performance when security features were enabled. Other products tested exhibited 75 percent or more performance degradation for DPI, AntiVirus and application control when enabled.

McAfee NGFW 5206 Performance (Security Features Enabled)



Source: Miercom, October 2014

iv. About the McAfee NGFW 5206 from Intel Security

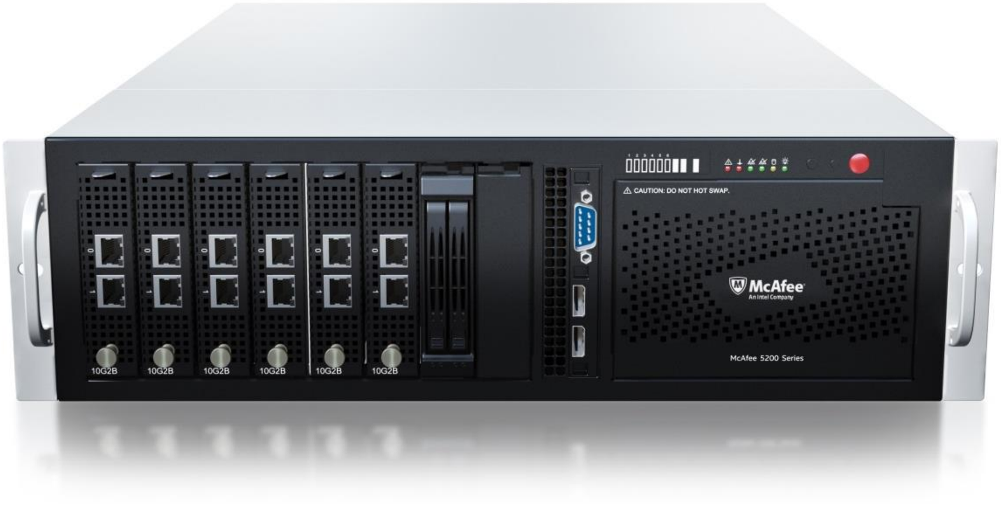
The McAfee NGFW 5206 is a versatile and modular security appliance designed for high-end data centers and large-network central sites. While this testing verified throughput with the NGFW 5206 configured as a firewall, it can also be used in a Firewall/VPN role (Layer 3) for secure routing, for Network Address Translation, and IPsec VPN gateway purposes.

The McAfee NGFW 5206 can be used in an IPS (Intrusion Prevention System) role (Layer 2) in an IDS (intrusion detection system) deployment or an in-line IPS deployment, or in a Layer 2 Firewall role. What's more, all of these roles are available with a single unified software image and invoked just by changing the configuration.

In the IPS and Layer 2 Firewall roles, the McAfee NGFW 5206 becomes transparent to surrounding network devices. In the Firewall/VPN role, the McAfee NGFW 5206 appliance provides high performance with unique clustering capabilities for up to 16 nodes. This provides very high IPsec VPN speeds, as well as high-performance content and application inspection where needed.

The McAfee NGFW 5206 was configured as a next-generation firewall for this testing. Below are some notes and product characteristics pertinent to the throughput tests conducted.

Figure 1: McAfee NGFW 5206



Key characteristics and notes for testing:

- Six-slot chassis
- Tested with two "Dual Port SFP+ 10GB Modules"
- Modules were situated in Slots 1 and 4 for all tests

v. How We Did It

Test System

The test equipment used for all of the tests in this report was the BreakingPoint system, offered by Ixia (www.ixiacom.com). The BreakingPoint is unique among test equipment: It allows customized, full seven-layer traffic to be generated and delivered at wire-speed over many 10GE interfaces.

The BreakingPoint system was installed on a high-performance Ixia XGS12 chassis. BreakingPoint software version 3.3.0 was run on a Windows 7, Service Pack 1 server, which was integral to the chassis system. Within the 12-slot XGS12 chassis were two eight-port PerfectStorm 10GE Fusion modules (model PS10GE8NG), providing 16 x 10GE ports.

We used Routing Robot and Application Simulator test components inside the BreakingPoint for our testing. Test components are virtual devices that enable you to test how well your device will operate at different network layers. A Routing Robot test component determines if a DUT routes traffic properly by sending routable traffic from one interface and monitoring the receiving interface to see if the traffic is successfully received. This test component sends packets with a UDP payload.

The Application Simulator test component generates application traffic flows. This test component uses an App Profile to determine the types of application flows that are to be sent to the DUT, and contains flow specifications that define the protocol, client-type, and server-type the traffic will use.

To minimize the number of variables in the testing, most of the testing was done with two main traffic streams, called Application Profiles in BreakingPoint parlance. The application profile determines the mix of applications simulated, as well as the specifics of what the traffic looks like for those applications. The following application profiles were used:

- **HTTP application profile:** This traffic is composed entirely of TCP-based, connection-oriented HTTP Web traffic. Each HTTP transaction retrieved a 21-kB (kilobyte) return file. For the HTTP application profile, there is only one associated Super Flow.
- **IMIX application profile**: This traffic consisted of a specific mix of IP traffic and protocols. For the IMIX profile, there are 11 associated Super Flows. Each Super Flow then has additional flows that establish the protocol, server, client and sequence of actions that they will perform. The specifics of the IMIX profile are shown in the table on the following page.

IMIX Composition

Traffic/protocol	Weight (of 940 total)	Number of Sessions	Percent of Bandwidth	Percent of Flows
BitTorrent (peer-peer file sharing)	10	2	1.045	1.064
SIP RTP (VoIP call)	10	4	0.522	1.064
AOL Instant Messenger	30	1	6.270	3.191
SSH (secure shell)	40	1	8.359	4.255
FTP (file transfer)	80	5	3.344	8.511
SMTP (email)	180	2	18.809	19.149
Images	40	2	4.180	4.255
HTTP (audio)	40	2	4.180	4.255
HTTP (video)	40	2	4.180	4.255
HTTP (text)	330	2	34.483	35.106
Small images	140	2	14.629	14.894

The BreakingPoint system issues the same sequence of Super Flow composition streams over and over. The granular system interface lets the operator tailor many of the load's parameters, including maximum concurrent TCP connections, cumulative traffic-delivery rate, and maximum TCP connections per second (cps).

These Super Flows consisted of "real" seven-layer client and server traffic. Four different "clients" (1 to 4) and four different "servers" (1 to 4) were defined and the BreakingPoint issued these bi-directional client-server traffic streams. The McAfee 5206 firewall observed the bi-directional traffic streams, as if configured "in-line" on a backbone link or on a monitored "spanned" port.

The test-bed connectivity was quite different between single-standalone-node McAfee 5206 testing and multi-node-cluster testing, although in both cases the traffic loads (application profile and associated Super Flows) and client-server composition issued by the BreakingPoint were the same.

UDP Throughput

Initially, a single test was conducted on a standalone McAfee NGFW 5206. The test was to determine if the McAfee NGFW 5206 could observe a collective 120 Gbps of passing, real-time traffic. 120 Gbps represents the current, fully expanded capacity of the McAfee 5206. For this single test, the BreakingPoint connected to the McAfee 5206 via twelve 10GE (Gigabit Ethernet) connections and delivered UDP (user datagram protocol) traffic, all large 1,518-byte packets, at wire-speed on all connections – a total of 120 Gbps.

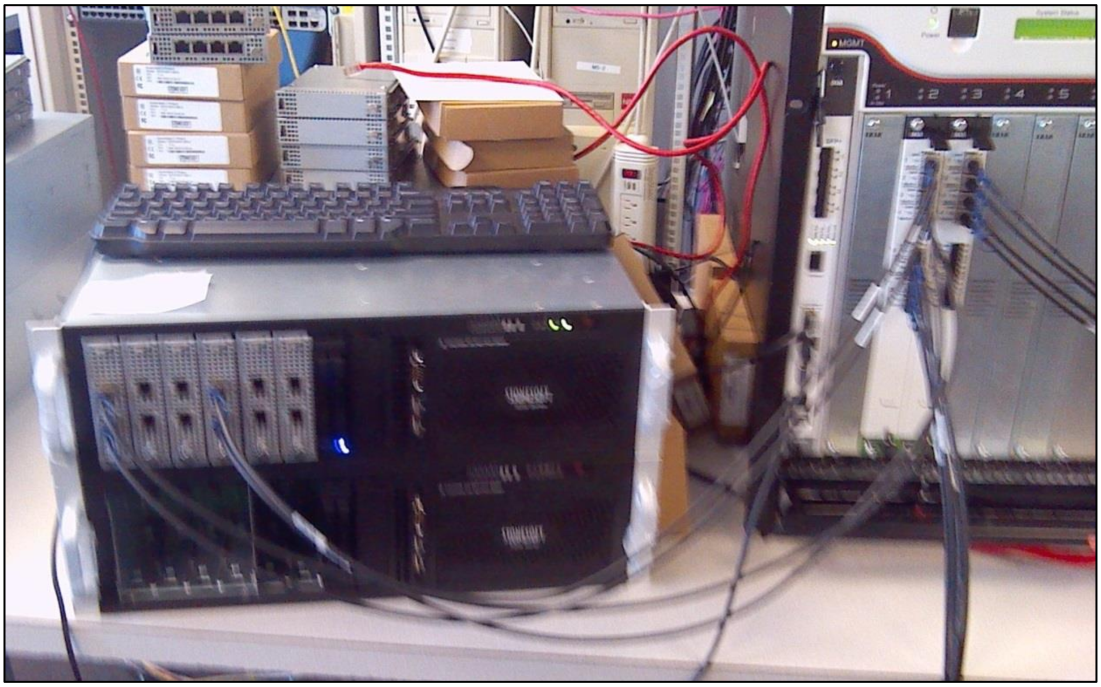
The McAfee NGFW 5206 was set to "Stateful Inspection" for this test, the lowest, default level of data examination. The UDP test traffic is state-less unicast traffic. The result: the McAfee 5206 viewed and passed the full load of 120 Gbps.

Single-Node Standalone

After the initial UDP throughput test, each McAfee NGFW 5206 was configured with two of the 2-port 10GE modules, yielding four 10GE ports. The modules were deployed, per vendor suggestion, in slots 1 and 4 of the six-slot 5206 chassis. Each McAfee 5206 could thus accept a maximum of 40 Gbps.

The test system then connected to the McAfee NGFW 5206 via four 10GE links, as shown in Figure 2, and testing with various stateful firewall inspection settings proceeded. Since all subsequent firewall policy settings employed DPI (deep packet inspection), it was believed that the four links, capable of delivering an aggregate 40 Gbps of test data to the 5206, would be sufficient.

Figure 2: Single-Node Configuration



Multi-Node Cluster

After all tests had been applied to a single, standalone McAfee NGFW 5206, four identically configured McAfee 5206s were interconnected in a cluster for testing multi-node throughput scalability. Four McAfee 5206s were cluster-tested, even though clusters of up to 16 of the McAfee NGFW 5206s are reportedly supported.

All of the tests were applied to each of four cluster configurations: 1) a single-node cluster, where three McAfee 5206s were set "off line" via the SMC management system; 2) a two-node cluster, with two nodes were active and the other two set "off line;" 3) a three-node cluster, with one node set "off line;" and 4) a four-node cluster, with all nodes active and on-line.

Three LANs. Configuring and correctly interconnecting the multi-node cluster for our testing was a tedious process. As shown in **Figure 3: Multi-Node Configuration** on the next page, three discrete LANs were established:

1) One LAN for "heartbeat" synchronization between the four McAfee 5206s, on a dedicated switch and 1GE links;

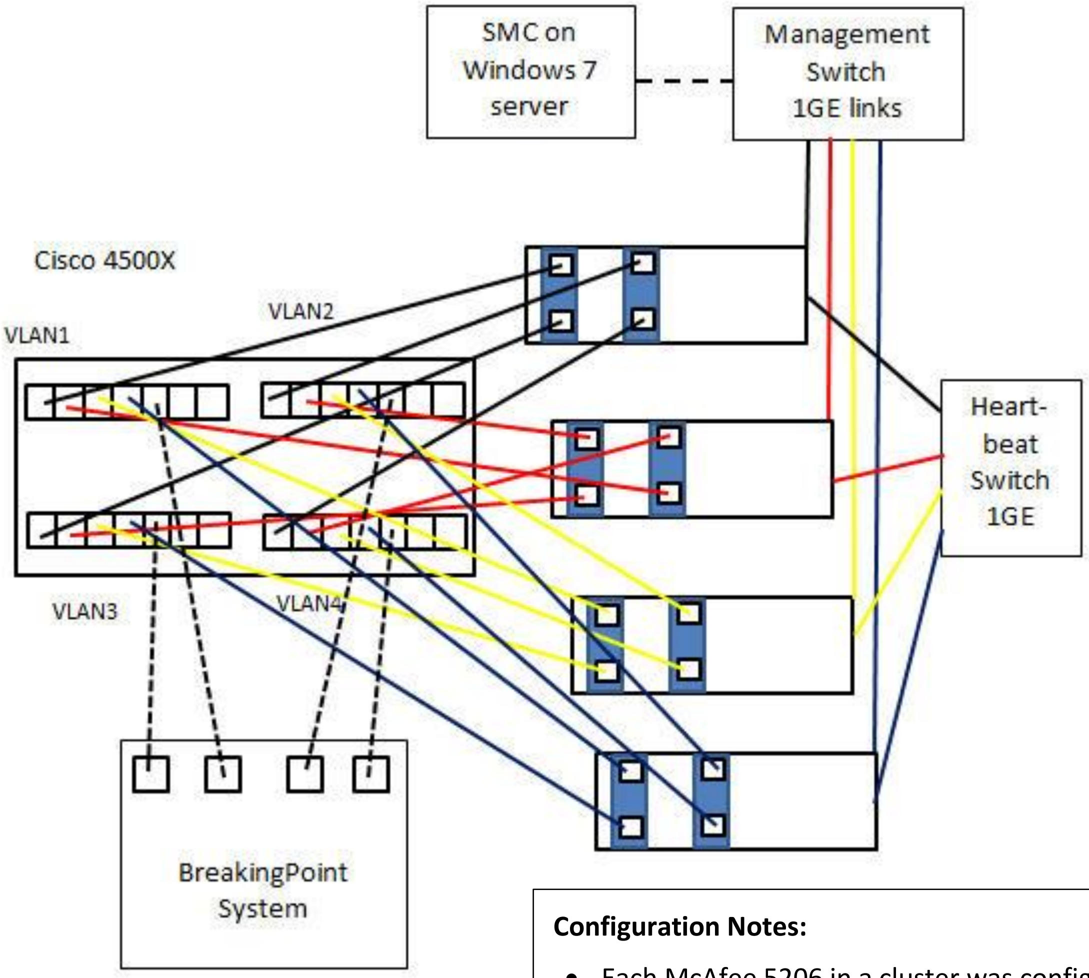
2) Another LAN for management connectivity, between the McAfee Security Management Center (SMC) and the four McAfee 5206s, employing a second dedicated switch and 1GE links;

3) The LAN for delivering test traffic to the McAfee NGFW 5206s. This required a high-capacity switch offering at least 20 x 10GE ports. We employed a Cisco 4500X, featuring 32 x 10GE ports and wire-speed connectivity on all ports.

The multi-node configuration is shown in the picture below and in the diagram on the next page.

***Four-node cluster**. Shown above is the multi-node configuration. Two McAfee NGFW 5206s are on the left and two are on the right. The BreakingPoint test system sits between them. Atop the BreakingPoint is the Cisco 4500X switch.*

Figure 3: Multi-Node Cluster Configuration with Four McAfee NGFW 5206s



Port 1=Client 1<->Server 2 @ 10 Gbps

Port 2=Client 2<->Server 1@ 10 Gbps

Port 3=Client 3<->Server 4 @ 10 Gbps

Port 4=Client 4<->Server 3 @ 10 Gbps

Total Client<->Server load = 40 Gbps

Configuration Notes:

- Each McAfee 5206 in a cluster was configured the same: the same modules and interfaces, and the same firewall policy settings
- Each McAfee 5206 must "see" all traffic in real-time, and so connects to each VLAN. The test system injects a different client-server traffic load (4 clients and 4 servers) into each VLAN
- One McAfee 5206 assumes the role of 'Dispatcher,' allocates traffic-inspection load to other nodes in the cluster based on IP addresses
- Three discrete LANs were deployed: 1) Primary data load, all 10GE links, 2) 'Heartbeat' LAN, for inter-node synchronization, all 1GE links, and 3) Management LAN, all 1GE links.

Determining Max Throughput

A particularly challenging aspect of this testing was determining the maximum throughput processed by the firewall(s) for any particularly test scenario (combination of policy settings on the firewall and traffic settings on the BreakingPoint. We developed the following protocol for ascertaining the maximum throughput value:

- All McAfee NGFW 5206s were cold rebooted prior to each test. The BreakingPoint was likewise reset regularly, usually after three test runs.
- We set the amount of traffic to be delivered by the BreakingPoint to be considerably higher than the expected McAfee 5206 throughput. As a very general rule of thumb, the optimum throughput was achieved with the traffic-delivery setting of the BreakingPoint about double the resulting throughput.
- All tests were run for 6 minutes and 20 seconds. This comprised 2 minutes of ramp-up, 4 minutes of sustained, steady-state traffic, and 20 seconds of ramp-down. During the Ramp Up duration, we set the minimum connection establishment rate to 100 and maximum connection rate to 70,000 per node with 250 increments in connections per every second. In deriving these settings we tried shorter and longer test-run durations. Shorter periods sometimes missed overloads that occurred after two or three minutes. We confirmed that longer, steady-state test periods, up to ten minutes, produced about the same result as the six-minute test.
- Because we sought the maximum **sustainable** throughput that the McAfee 5206(s) could process (and not a transient peak), we applied loads that usually resulted in some net loss. We established 20 percent loss (from the traffic delivered, compared to the amount received) as the maximum we would accept. No result was considered valid if loss exceeded 20 percent. In that case we would repeat the test after reducing the delivered-load setting on the BreakingPoint. Conversely, if a result indicated little or no loss, the delivered-load setting would be increased and the test run again, until throughput tapered off and began to decrease.
- We observed that there is variability in the throughput result from the BreakingPoint. With everything set the same and the same test repeated, we observed that variability of up to five percent in the results was not uncommon.

Key BreakingPoint Settings

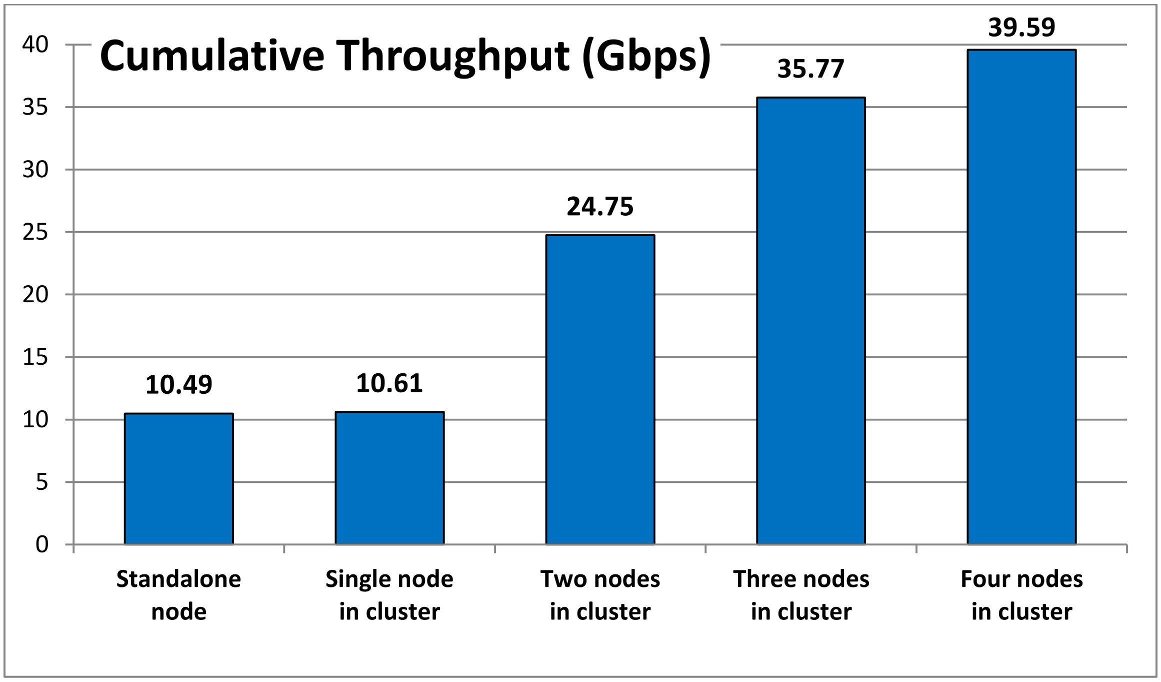
Most of the many traffic settings in the BreakingPoint were kept the same for all the tests. For single-node and two-node clusters we tested with 1,992 IP addresses. For three- and four-node clusters, we tested with 2,490 IP addresses.

Below are some of the different BreakingPoint settings that were applied.

	Single node in 4-node cluster	Two nodes in cluster	Three nodes in cluster	Four nodes in cluster
Connections per second	70,000	140,000	210,000	280,000
Concurrent connections	1.5 million	3 million	4.5 million	6 million
Delivered traffic rate setting	40 Gbps	60 Gbps	80 Gbps	80 Gbps
IP addresses	1,992	1,992	2,490	2,490

1.0 Firewall, DPI and HTTP Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection (only). Traffic delivered by the BreakingPoint was the "HTTP-with-21kB return file" Super Flow.



Results and Observations

Two-, three- and four-node clustered throughput improved incrementally, for this combination of traffic type and firewall policy settings. Indeed, the cumulative throughput of 39.59 Gbps achieved with the four-node cluster essentially means that **all** offered traffic was successfully processed. The test equipment delivered 40 Gbps.

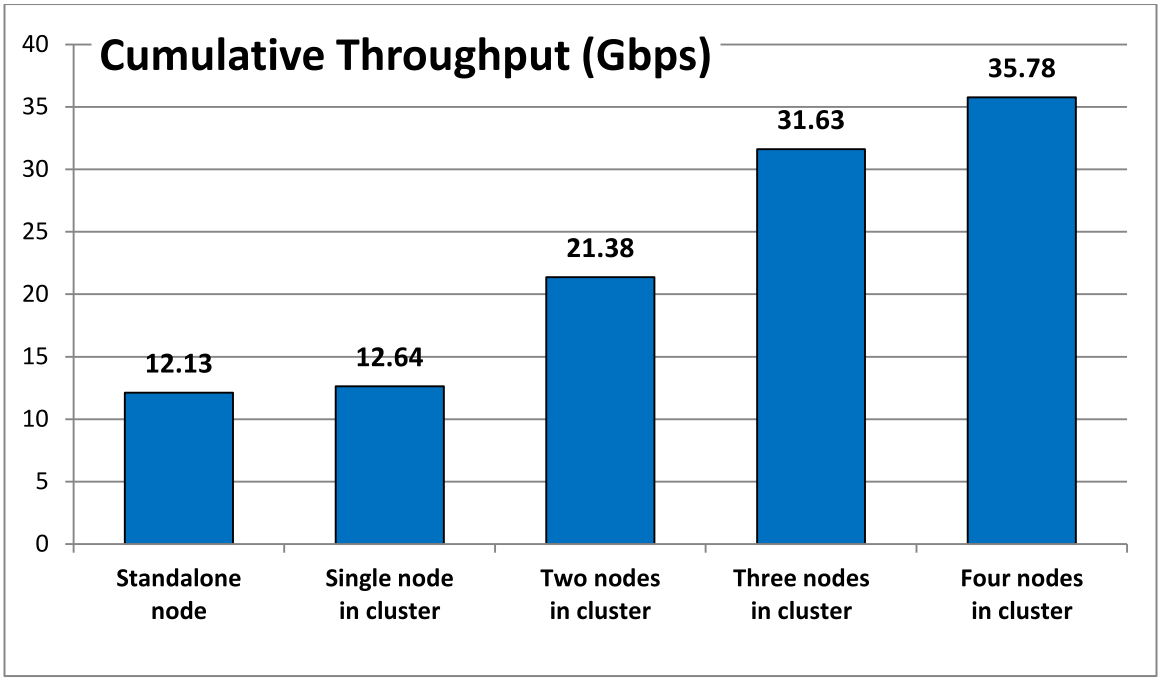
Scalability. For this combination of traffic type and firewall policy settings, incremental growth in throughput was linear as the second, third and fourth nodes in the cluster were brought on-line.

Below are the incremental growths achieved with two-, three- and four-node clusters.

One node in cluster:	10.6 Gbps
Increase with 2nd node:	+14.1 Gbps
Increase with 3rd node:	+10.0 Gbps
Increase with 4th node:	+3.9 Gbps

2.0 Firewall, DPI and IMIX Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection (only). Traffic delivered by the BreakingPoint was the "FW-Enterprise" profile consisting of 11 unique Super Flows, which collectively comprises the IMIX traffic set.



Results and Observations

Scalability. Growth in throughput for this traffic type and firewall policies grew, though somewhat inconsistently, as the second, third and fourth nodes in the cluster were brought on-line and tested.

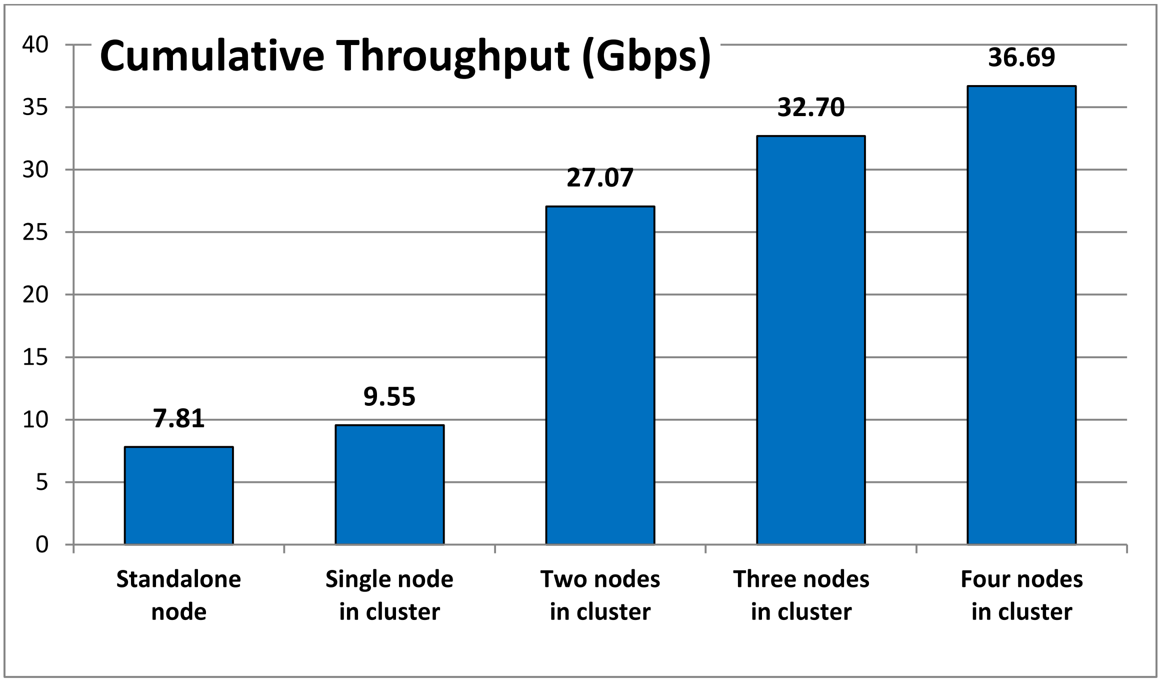
In our opinion, given the mix of protocols, packets and applications in the IMIX traffic assortment, the four-node cluster collective throughput of nearly 36 Gbps likely represents successful processing of the entire offered load of 40 Gbps.

<u>Incremental growth with added cluster nodes (v5.8):</u>

One node in cluster:	12.6 Gbps
Increase with 2nd node:	+8.7 Gbps
Increase with 3rd node:	+10.3 Gbps
Increase with 4th node:	+4.2 Gbps

3.0 Firewall, DPI and AntiVirus, with IMIX Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection and AntiVirus policy was enabled. Traffic delivered by the BreakingPoint was the "FW-Enterprise" profile consisting of 11 different Super Flows (the IMIX assortment).



Results and Observations

Given the IMIX assortment of protocols, packets and applications, the four-node cluster collective throughput of nearly 37 Gbps likely represents successful processing of the entire offered load of 40 Gbps.

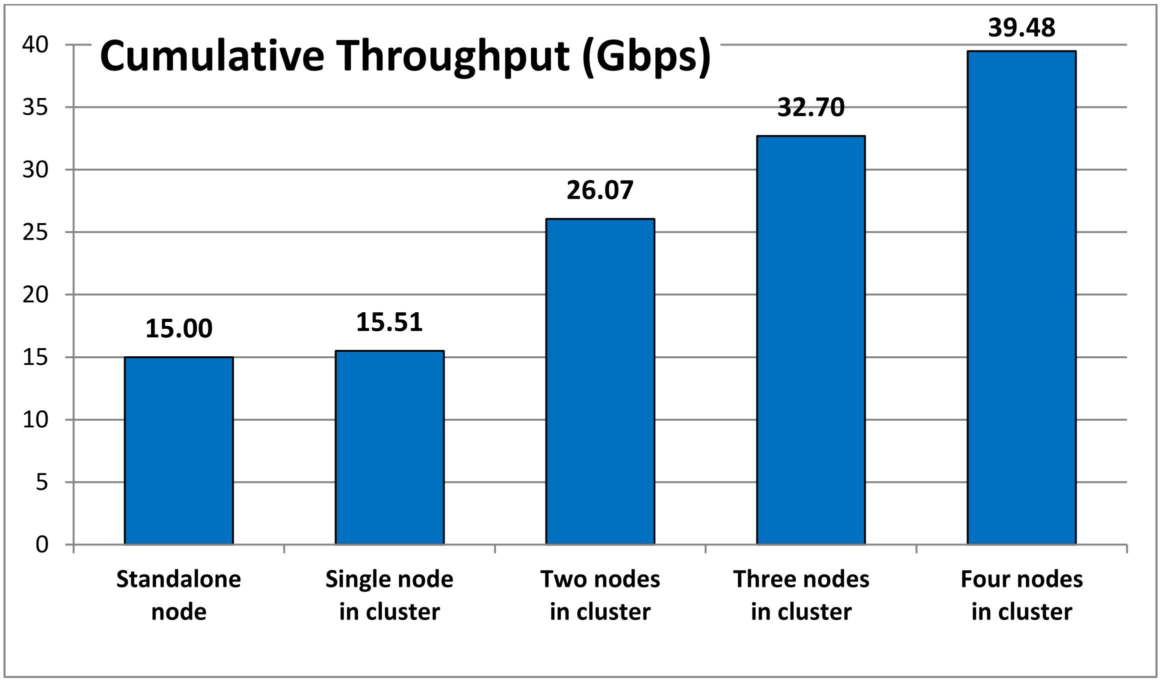
Scalability. Throughput nearly tripled with the second clustered node. And growth with the third and fourth nodes was respectable, though inconsistent, topping off at about 37 Gbps.

Incremental growth with added cluster nodes (v5.8):

One node in cluster:	9.6 Gbps
Increase with 2nd node:	+17.5 Gbps
Increase with 3rd node:	+5.6 Gbps
Increase with 4th node:	+4.0 Gbps

4.0 Firewall, DPI and URL Filtering, with HTTP Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection, plus URL Filtering. Traffic delivered by the BreakingPoint was the "HTTP-with-21kB return file" Super Flow.



Results and Observations

Single-node throughputs were more than 15 Gbps, and incremental throughput with the second, third and fourth nodes grew linearly and impressively.

The four-node cluster collective throughput of 39.5 Gbps likely represents successful processing of the entire offered load of 40 Gbps.

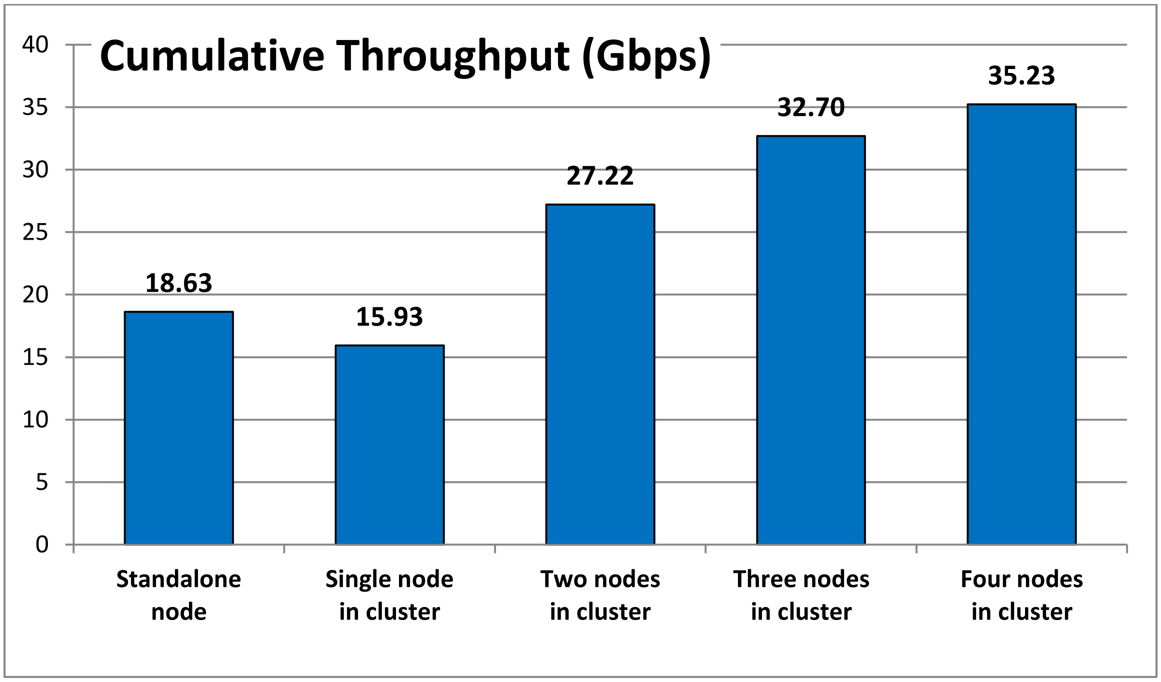
Scalability. Aggregate throughput for this traffic/policy scenario exhibits very linear growth with clustered configurations increasing with two, three and four online nodes.

<u>Incremental growth with added cluster nodes (v5.8):</u>

One node in cluster:	15.5 Gbps
Increase with 2nd node:	+10.6 Gbps
Increase with 3rd node:	+6.7 Gbps
Increase with 4th node:	+6.8 Gbps

5.0 Firewall, DPI and URL Filtering, with IMIX Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection and URL Filtering policy was enabled. Traffic delivered by the BreakingPoint was the "FW-Enterprise" application profile consisting of 11 Super Flows (the IMIX assortment).



Results and Observations

The results are a bit eclectic. Overall throughput for the four-node cluster was likely at or near the maximum achievable (given that the tester delivered 40 Gbps of traffic, over four 10GE links).

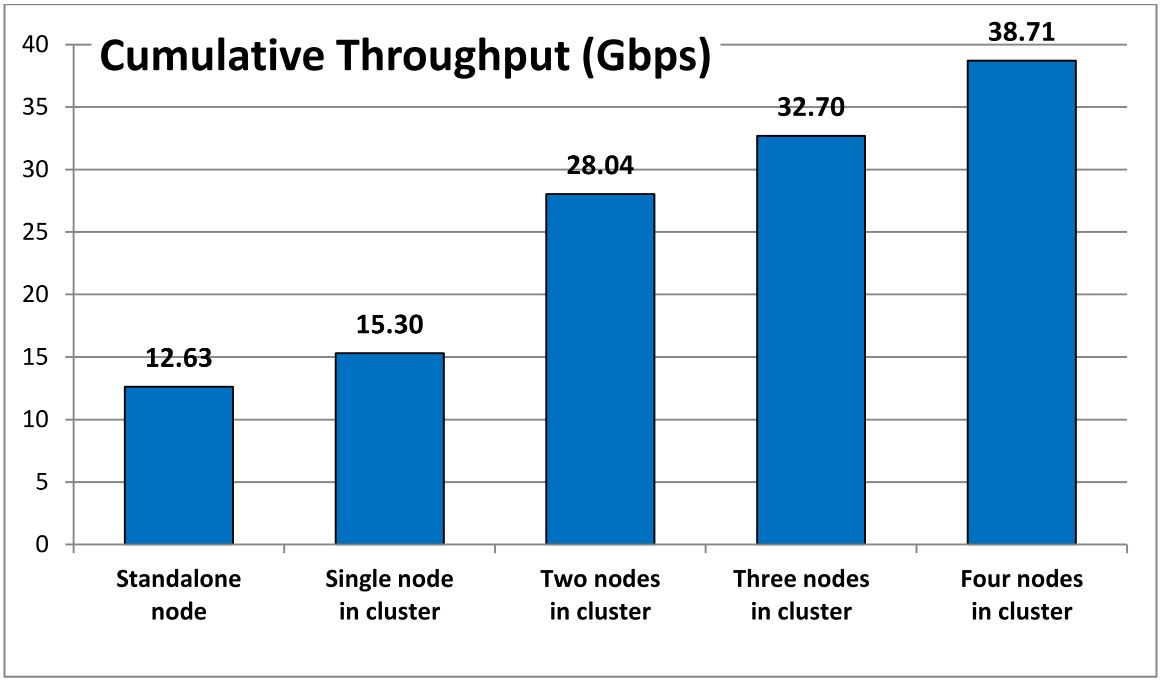
Scalability. The single-node cluster throughput, about 16 Gbps, was slightly lower than the single-node throughput. However, bringing the second node online produced strong incremental throughput growth. This stepped up 5 Gbps more with the third node, and then a few Gbps more with the fourth node, to the max of 35 Gbps.

Incremental growth with added cluster nodes (v5.8):

One node in cluster:	15.9 Gbps
Increase with 2nd node:	+11.3 Gbps
Increase with 3rd node:	+4.5 Gbps
Increase with 4th node:	+2.5 Gbps

6.0 Firewall, DPI and Application Awareness, with UDP Traffic

In this scenario, the McAfee NGFW 5206(s) were set for DPI, and Application Aware policy was enabled. Traffic delivered by the BreakingPoint was stateless UDP, unicast, 1518-byte packets.



Results and Observations

Throughput from this round of testing, of stateless UDP traffic delivered to the firewall(s), was predictably very good. The four-node cluster collective throughput of 38.7 Gbps likely represents successful processing of the entire offered load of 40 Gbps.

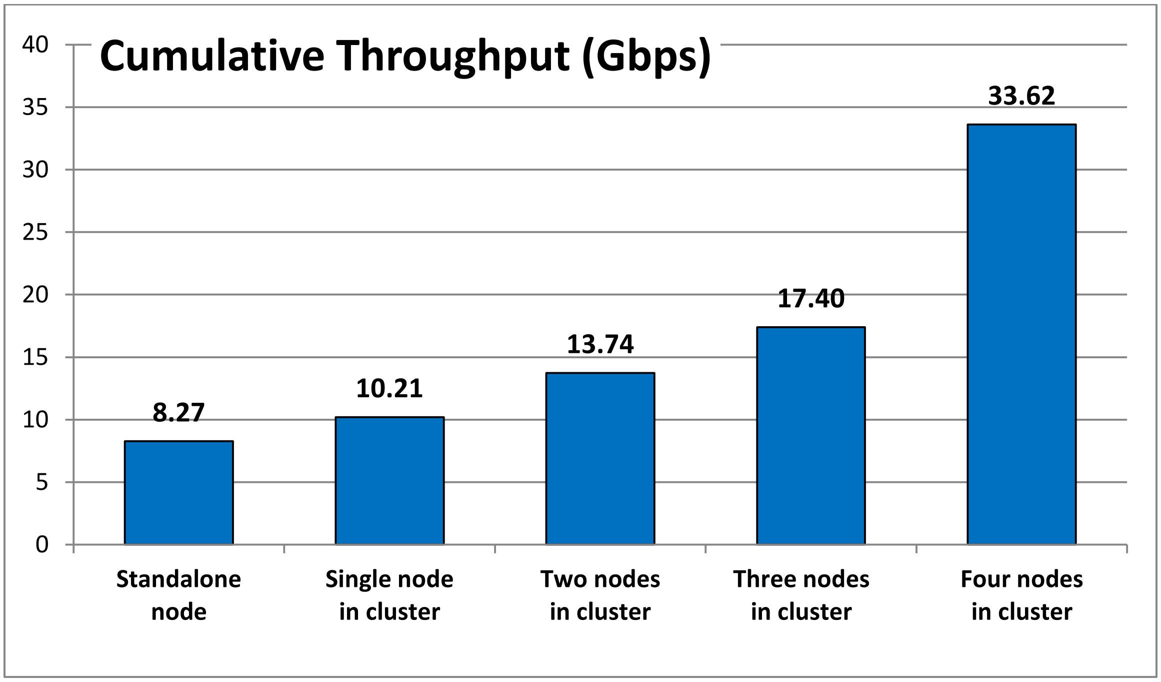
Scalability. Even though the traffic is stateless UDP, the incremental growth of aggregate throughput as additional clustered nodes are brought online is linear.

Incremental growth with added cluster nodes (v5.8):

One node in cluster:	15.3 Gbps
Increase with 2nd node:	+13.1 Gbps
Increase with 3rd node:	+4.7 Gbps
Increase with 4th node:	+6.0 Gbps

7.0 Firewall, DPI and Application Awareness, with HTTP Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection and Application Awareness. Traffic delivered by the BreakingPoint was the "HTTP-with-21kB return file" Super Flow.



Results and Observations

Throughput performance for this traffic type and firewall policy setting was modest for two- and three-node clusters, but then almost doubled when the fourth node in the cluster was brought online.

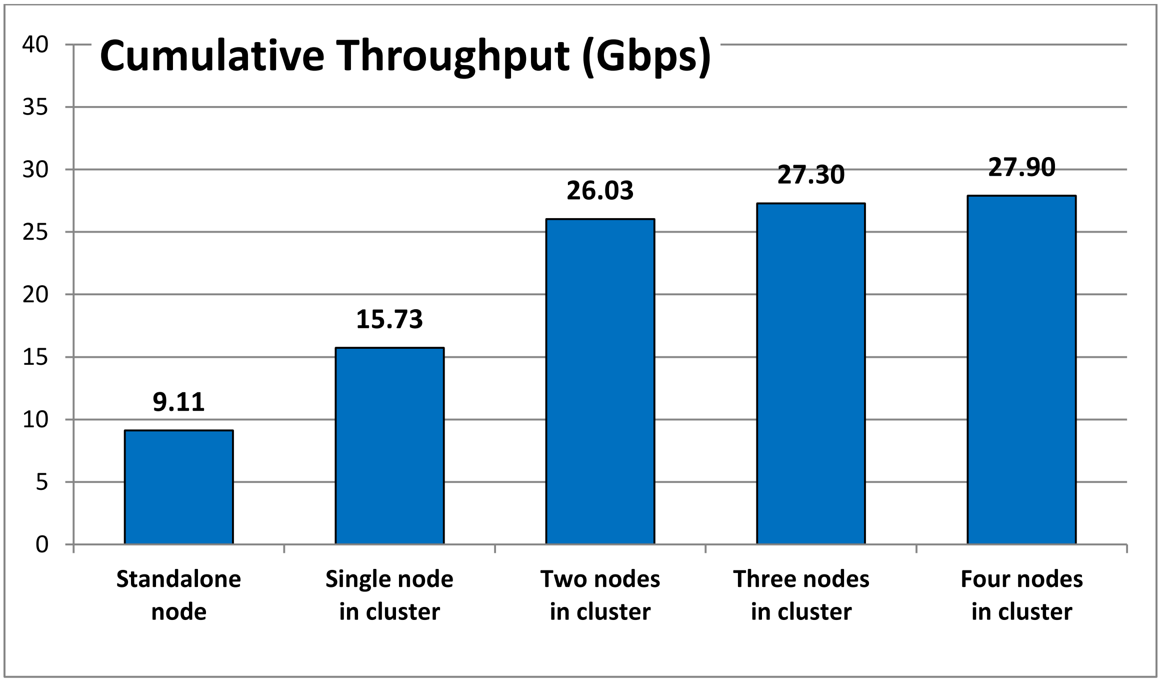
Scalability. There was continual growth in aggregate throughput as the second, third and fourth nodes were brought online. However, the increment with the second and third nodes was fairly small, compared to a sizable jump when the fourth node was brought online.

<u>Incremental growth with added cluster nodes (v5.8):</u>

One node in cluster:	10.2 Gbps
Increase with 2nd node:	+3.5 Gbps
Increase with 3rd node:	+3.7 Gbps
Increase with 4th node:	+15.2 Gbps

8.0 Firewall, DPI and Application Awareness, with IMIX Traffic

In this scenario, the McAfee NGFW 5206(s) were set for Deep Packet Inspection and Application Awareness. Traffic delivered by the BreakingPoint was the "FW-Enterprise" profile consisting of 11 unique Super Flows (the IMIX assortment).



Results and Observations

Results for this test round show respectable improvement in throughput growth for a single node and cluster of two nodes. The same degree of growth was not realized, however, in bringing the third and fourth nodes online in the cluster. Aggregate throughput seems to flatten after the second clustered node.

Scalability. The results for the three- and four-node clusters showed minimal additional throughout growth over two nodes.

Incremental growth with added cluster nodes (v5.8):

One node in cluster:	15.7 Gbps
Increase with 2nd node:	+10.3 Gbps
Increase with 3rd node:	+1.2 Gbps
Increase with 4th node:	+0.6 Gbps

9.0 About Miercom

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

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. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

10.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify with 100-percent certainty.

This document is provided "as is" by Miercom and gives no warranty, representation or undertaking, whether express or implied. Miercom accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or McAfee, Inc. All trademarks used in the document are owned by their respective owners. No one may use any trademark in or as the whole or part of other materials or trademarks in connection with any activities, products or services which are not Miercom's, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.