TEST PLAN

Mail Gateway Testing

IxLoad

www.ixiacom.com

915-6654-01, 2006

Ixia
26601 West Agoura Road, Calabasas, CA 91302
(877) FOR-IXIA

This Test Plan contains a general outline for testing a particular technology.
Not all the capabilities of Ixia technology have been exposed in this document.
Please feel free to contact us if additional capabilities are required.

Mail Gateway Test Plan

Contents

Mail Gateway Test Plan

This test plan will assist in comprehensively testing your edge-of-network device's performance in handling good (ham) emails, spam emails and virus-infected emails using Ixia's recommended methodology. By creating and running the test cases presented in this test plan, you can validate the ability of a mail gateway device to effectively handle various traffic fowls. The test plan will also provide various performance metrics on how well the device performs under stress.

The recommended testing methodology can be further extended to stress test various email filtering engines, including content filtering and phishing attacks via emails.

Background

As the industry moves further towards unified network security, network edge devices are providing better security services. One of the fastest growing security services running on these devices is virus and spam protection for email messages delivered over industry standard email protocols (SMTP and POP3). Indeed, the growth of such protection is directly related to the rapid rise of virus and spam emails, estimated to comprise 60-80% of all emails sent, which poses a genuine threat to the overall usefulness of email communications.

The initial approach to combating this threat was left to the end user with intelligent host-based detection and remediation processes. However, this intelligence is now being integrated at the core of the network to prevent such threats from infiltrating the network in the first place.

Edge-of-network devices such as firewalls, proxy servers, and email gateway devices are increasingly offering various spam and virus detection vectors to eliminate such threats before they threaten the enterprise network. There are several application-aware engines used to combat such threats: signature-based virus scanning used to detect and eliminate known threats, heuristics-based rules to detect new and suspicious behavior, and pattern-matching approach to detect harmful codes buried in protected and secure environments such as archives files. This is in addition to continually offering new and novel ways to prevent emergent email threats that include Denial-of-Service attacks, Directory Harvesting or using Sender Policy Framework (SPF) to validate emails.

The integration of application-aware intelligence in mail gateway devices has led to a growing recognition that multi-vector threat prevention mechanism is a good one. However, one of the drawbacks to offering several stateful application-aware services in a single device is the potential for degradation of the device’s performance characteristics. Therefore to fully characterize the performance of such devices, real-world conditions must be closely matched by incrementally enabling application-aware inspection engines.

Performance Metrics

To validate the effectiveness of the mail gateway, several performance metrics can be used.

The following terms are defined and used to provide objective performance characteristics for the mail gateway, which is the device under test (DUT) in this test plan.

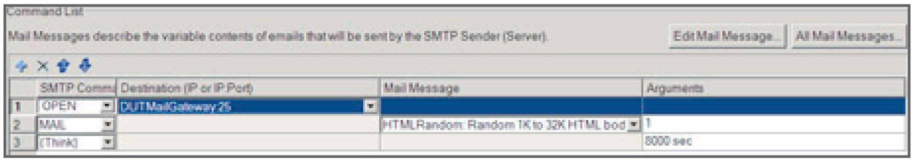
Connection – A single TCP connection between two end hosts, using connection establishment (3-way handshake).

Transaction – A single request for an object from a client to server. A transaction is made within an established Connection.

Concurrent Connections – Multiple TCP connections established between two end hosts.

Connections-per-second – The rate at which new TCP connections are initiated per second.

To accurately measure connections-per-second, this test must be performed while there are several active SMTP connections on the DUT. The active connections ensure a real-world test scenario where the DUT will be serving new connections while actively maintaining established ones. To accomplish this objective, each SMTP connection must only perform a series of SMTP transactions (one or more), and keep the connection active for a period of time (or until ramp-down). The sequence of SMTP commands that can be used to accomplish this test can be as follows: OPEN, HELO, MAIL, RCPT, DATA The commands above will establish a SMTP connection and keep the connection open until ramp downtime is reached. The SMTP connection termination during ramp down is achieved with the QUIT command.



Command List

Mail Messages describe the variable contents of emails that will be sent by the SMTP Sender (Server).

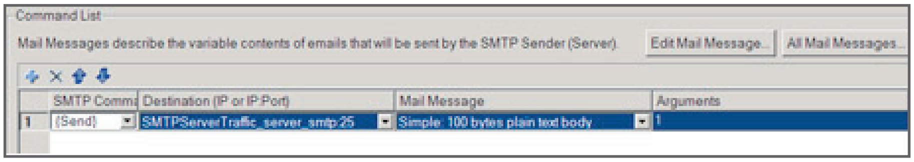
	SMTP Comm	Destination (IP or IP:Port)	Mail Message	Arguments
1	OPEN	DUT:MailGateway:25		
2	MAIL		HTMLRandom: Random 1K to 32K HTML bod	1
3	(Think)			8000 sec

Figure 1. Connections-per-second test command list

Throughput – The rate at which the DUT sends or receives data, measured in bits per second.

To measure the sustained throughput of SMTP traffic of the DUT requires that the SMTP client send emails of varied sizes (as inline content or attachments) to the SMTP server. Throughput can be measured in combination with previously established connections still active, or it can be measured with a complete mail transaction that closes the SMTP connection after the email is delivered. The combination of throughput tests and concurrently active connections is very desirable, and this method can easily be accomplished using the correct sequence of SMTP commands. For this test plan, the later is the recommended method.

To test the throughput of the DUT in handling emails, the following sequence of SMTP commands can be used: OPEN, HELO, MAIL, RCPT, DATA, QUIT. The commands above are a recommended approach. However, a more elaborate test can be created.


Command List

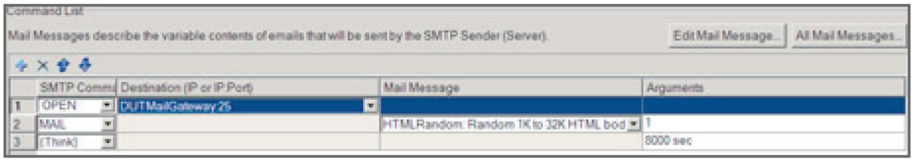
Mail Messages describe the variable contents of emails that will be sent by the SMTP Sender (Server).

	SMTP Comma	Destination (IP or IP:Port)	Mail Message	Arguments
1	(Send)	SMTPServerTraffic_server_smtp:25	Simple: 100 bytes plain text body	1

Figure 2. Throughput test command list

Concurrent Connections – To simulate a large number of concurrent SMTP connections, each client must establish a SMTP connection, engage in some (or many) SMTP transactions, and maintain the TCP connection. New users will initiate connections to simulate a ramp up while existing connections are maintained. The following sequence of SMTP commands can be used to

test concurrent connections: OPEN, HELO, MAIL, RCPT, DATA The commands above will establish a SMTP connection and keep the connection open until ramp down time is reached. The SMTP connection termination during ramp down is achieved with the QUIT command.


Command List

Mail Messages describe the variable contents of emails that will be sent by the SMTP Sender (Server).

	SMTP Comma	Destination (IP or IP:Port)	Mail Message	Arguments
1	OPEN	DUTMailGateway:25		
2	MAIL		HTMLRandom: Random 1K to 32K HTML bod	1
3	(Think)			8000 sec

Figure 3. Concurrent connections test command list

1. SMTP Content Inspection Performance Test – Baseline

Objective

To create a useful testing scenario, the basic operating limits of the DUT must be known. The basic operating limit refers to the stateful mail processing capability of the gateway device without any SMTP filtering engines scanning the mail messages. The SMTP filtering engines include, but are not limited to, any packet inspection capabilities such as virus detection, spam detection (based on RBL, Heuristics algorithm, or custom methods), or any other threat detection vectors (such as phishing attempts, algorithmic image recognition).

This reference baseline test will assess the performance of the DUT using varied email messages using the SMTP client and server protocol.

Performance metrics required: connections per second (CPS), throughput (Mbps), and concurrent connections.

Setup

This setup requires at least one server port and one client port. The SMTP client traffic will pass through the SMTP gateway device to reach the SMTP server. The SMTP client and server ports must be connected to the DUT using a Switched infrastructure.

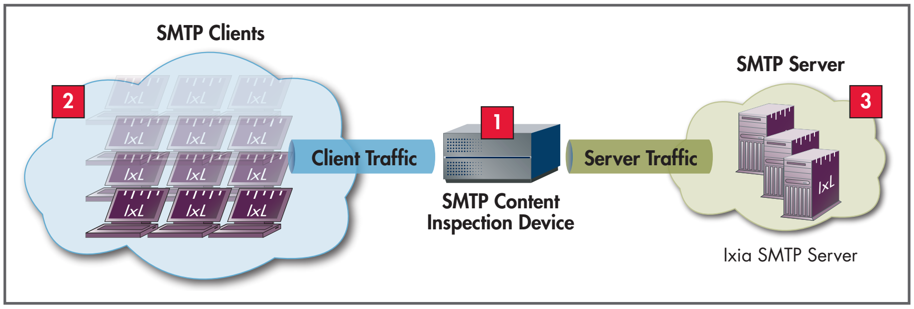


Figure 4. Topology setup for mail gateway Test Case 1

1. **SMTP Content Inspection Device** – Mail gateway device with dual interfaces. There are no content inspection engines enabled for this baseline test.
2. Performance test facility with **SMTP client traffic** generation capabilities including emails with attachments with configurable email payload.
3. Performance test facility with **SMTP server** capabilities.

Input Parameters

Parameter	Description
Number of SMTP clients	Number of SMTP clients required to meet the Objective
Number of connections per client	One or more TCP connection per SMTP client
SMTP client email payload	Varied email payloads per TCP connection
SMTP server connection limit	Limits set high (10000+)
DUT packet filtering rule	Configure NAT or PAT rules to allow client network access to server(s) network – specifically only TCP/25
DUT content inspection mode	*Anti-virus* – Disabled
	Spam inspection – Disabled
Test Objective(s)	Test the DUT using one or all performance metrics including connections-per-second, throughput, and concurrent connections

Table 1. Test Input Parameters for Test Case 1

Methodology

1. Configure the emulated SMTP server. Set the concurrent connection limits high (if configurable). The server's gateway is the interface address of the server network of the DUT.

2. If the DUT is a firewall or proxy device, network address translation (NAT) may or may not be used. The setup topology presented in this test case uses NAT. A packet filtering rule must be configured to allow hosts originating (source) from the Client network to the SMTP server. Note: For the reference test, disable all SMTP inspection engines including anti-virus scanning or spam and content filtering mechanisms.

3. Configure the emulated SMTP clients to establish a TCP connection to the DUT interface followed by performing some SMTP mail delivery transactions. Each SMTP connection can perform single or multiple transactions per TCP connection. The sequence of commands generally used to send an email is presented below: o HELO o MAIL o RCPT o DATA o QUIT.

4. The test tool must be configured with the DUT's IP address. The SMTP client traffic is originating from the WAN segment; therefore, the DUT's "E0" interface IP address is used.

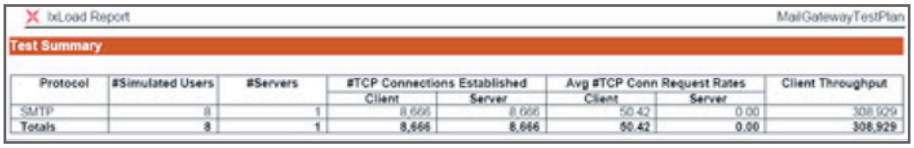
5. Set up the Client-side test tool to perform the test. Set the Objective as required and iterate through the process to achieve a reference baseline capacity of the DUT. The test tool may ramp the number of users too quickly or the total number of TCP connections initiated may overwhelm the DUT (or possibly the SMTP server). To achieve a good baseline capacity, adjust the parameters of the test objective and the client payload and monitor the DUT for any errors such as TCP retries and timeouts.

Refer to the "Performance Metrics" section, which provides a framework for three recommended test Objectives.

Results

The objective of this test case was to determine the DUT's connections-per-second (CPS) performance. The following table summarizes how IxLoad achieved the CPS Objective, using an iterative process to ensure that the DUT was not being overwhelmed, for example, ensuring that the number of TCP connections established by the SMTP Client matched that of the Server.

The high-level summary provided in IxLoad presents quick access to pertinent information, highlighting the key statistics from the tests run.



IxLoad Report MailGatewayTestPlan

Test Summary

Protocol	#Simulated Users	#Servers	#TCP Connections Established		Avg #TCP Conn Request Rates		Client Throughput
			Client	Server	Client	Server	
SMTP	8	1	8,666	8,666	50.42	0.00	308,929
Totals	8	1	8,666	8,666	50.42	0.00	308,929

Figure 5. High-level summary of test simulation to achieve CPS Objective

The graph below shows the sustained connection rate as outlined in the Objective.

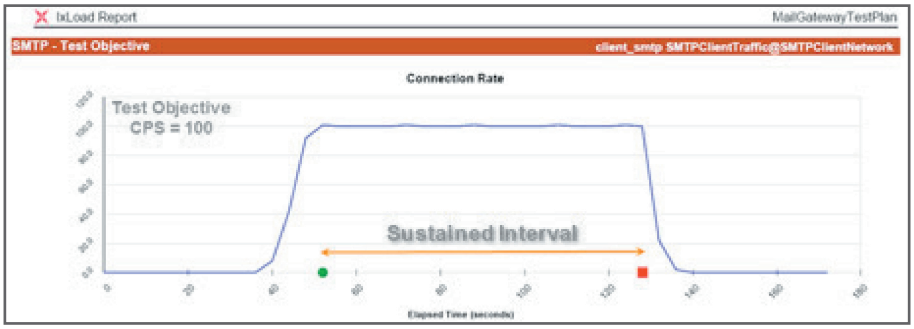
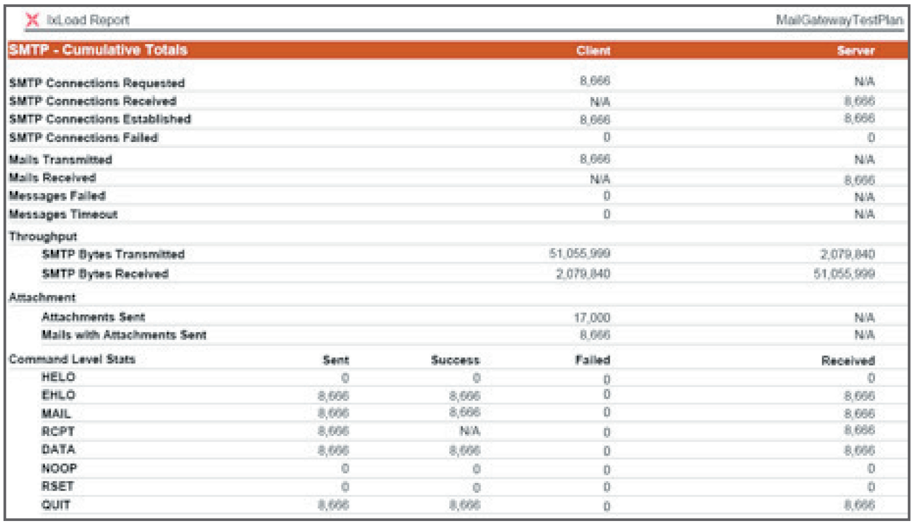


Figure 6. Sustained client CPS over the sustained interval

By reviewing the TCP and SMTP statistics, you can confirm that there were no errors in the transmission. Check for TCP retries or timeouts, via the SMTP statistics, if no failed connections are reported.



IxLoad Report MailGatewayTestPlan

SMTP - Cumulative Totals			Client	Server
SMTP Connections Requested			8,666	N/A
SMTP Connections Received			N/A	8,666
SMTP Connections Established			8,666	8,666
SMTP Connections Failed			0	0
Mails Transmitted			8,666	N/A
Mails Received			N/A	8,666
Messages Failed			0	N/A
Messages Timeout			0	N/A
Throughput				
SMTP Bytes Transmitted			51,055,999	2,079,840
SMTP Bytes Received			2,079,840	51,055,999
Attachment				
Attachments Sent			17,000	N/A
Mails with Attachments Sent			8,666	N/A
Command Level Stats	Sent	Success	Failed	Received
HELO	0	0	0	0
EHLO	8,666	8,666	0	8,666
MAIL	8,666	8,666	0	8,666
RCPT	8,666	N/A	0	8,666
DATA	8,666	8,666	0	8,666
NOOP	0	0	0	0
RSET	0	0	0	0
QUIT	8,666	8,666	0	8,666

Figure 7. Test summary including SMTP connection and command-level statistics

2. SMTP Content Inspection Performance Test – Virus Detection

Objective

This test will extend the testing scenario from the reference performance Test Case 1 to enable the Virus scanning engine on the mail gateway (DUT) and measure the performance impact introduced by the virus inspection engine.

Setup

This setup requires at least one server port and one client port. The SMTP client traffic will pass through the SMTP gateway device to reach the SMTP server. The SMTP client and server ports must be connected to the DUT using a Switched infrastructure.

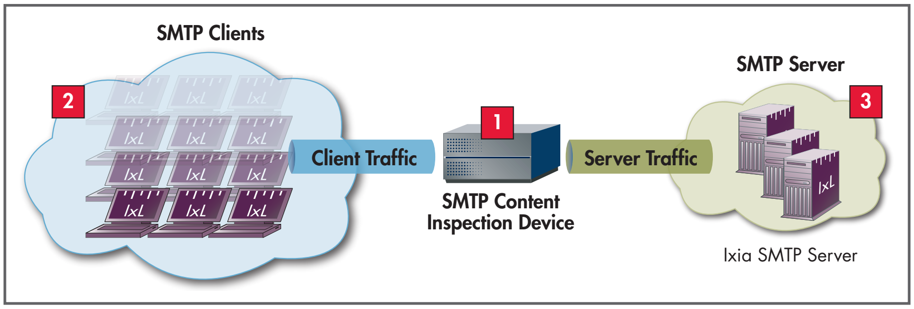


Figure 8. Test topology setup for mail gateway Test Case 2

1. **SMTP Content Inspection Device** – Mail gateway device with dual interfaces. Anti-virus inspection engines is enabled for this test.
2. Performance test facility with **SMTP client traffic** generation capabilities including emails with attachments with configurable email payload.
3. Performance test facility with **SMTP server** capabilities.

Input Parameters

Parameter	Description
Number of SMTP clients	Number of SMTP clients required to meet the Objective
Number of connections per client	One or more TCP connection per SMTP client
SMTP client email payload	Varied email payloads per TCP connection
SMTP server connection limit	Limits set high (10000+)
DUT packet filtering rule	Configure NAT or PAT rules to allow client network access to server(s) network – specifically only TCP/25
DUT content inspection mode	*Anti-virus* – Enabled
	Spam inspection – Disabled
Test Objective(s)	Test the DUT using one or all performance metrics including connections-per-second, throughput, and concurrent connections

Table 2. Test input parameters for Test Case 2

Methodology

1 Configure the emulated SMTP server. Set the concurrent connection limits high (if configurable). The server's gateway is the interface address of the server network side of the DUT.

2. If the DUT is a firewall or proxy device, network address translation (NAT) may or may not be used. The setup topology presented in this test case uses NAT. A packet filtering rule must be configured to allow hosts originating (source) from the Client network to the SMTP server. Note: For the reference test, disable all SMTP inspection engines, including anti-virus scanning or spam and content filtering mechanisms.

3. Configure the emulated SMTP clients to establish a TCP connection to the DUT interface, followed by performing SMTP mail delivery transactions. Each SMTP connection can perform a single or multiple transactions per TCP connection. The sequence of commands generally used to send an email is presented below:

   - HELO
   - MAIL
   - RCPT
   - DATA
   - QUIT

4. The test tool must be configured with the DUT's IP address. The SMTP client traffic originates from the WAN segment; therefore, the DUT's Client-side interface IP address is used.

   Set up the test tool to perform the test. Set the Objective as required and iterate through the process to achieve a reference baseline capacity of the DUT. The test tool may ramp the number of users too quickly or the total number of TCP connections initiated may overwhelm the DUT (or possibly the SMTP server). To achieve a good baseline capacity, adjust the parameters of the test objective and the client payload, and monitor the DUT for any errors such as TCP retries and timeouts.

Refer to the "Performance Metrics" section, which provides a framework for three recommended test Objectives.

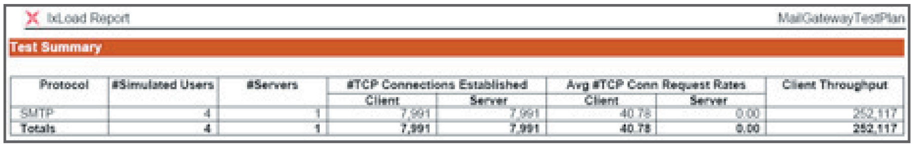
The notable difference here is that the DUT must now be enabled with a virus inspection engine that is capable of scanning all inbound mail messages for viral content.

In addition, the SMTP client can include EICAR.COM sample viral payloads (or real virus payloads viruses if this is feasible) in its random selection of mail messages being sent to the DUT. However, in the event that such payloads are not possible, non-viral, synthetic payloads can still be used to test the performance of the DUT while its virus inspection engine is activated for this test case.

Results

The objective of this test case was to determine the DUT's connections-per-second (CPS) performance. The following table summarizes how IxLoad achieved the CPS Objective, using an iterative process to ensure that the DUT was not being overwhelmed, for example ensuring that the number of TCP connections established by the SMTP Client matched that of the Server.

The high-level summary provided in IxLoad presents quick access to pertinent information, highlighting the key statistics from the tests run with the virus inspection engine enabled.



IxLoad Report — MailGatewayTestPlan

Test Summary

Protocol	#Simulated Users	#Servers	#TCP Connections Established		Avg #TCP Conn Request Rates		Client Throughput
			Client	Server	Client	Server	
SMTP	4	1	7,991	7,991	40.78	0.00	252,117
Totals	4	1	7,991	7,991	40.78	0.00	252,117

Figure 9. High-level summary of test simulation to achieve CPS Objective

The graph below shows the sustained connection rate as outlined in the Objective.

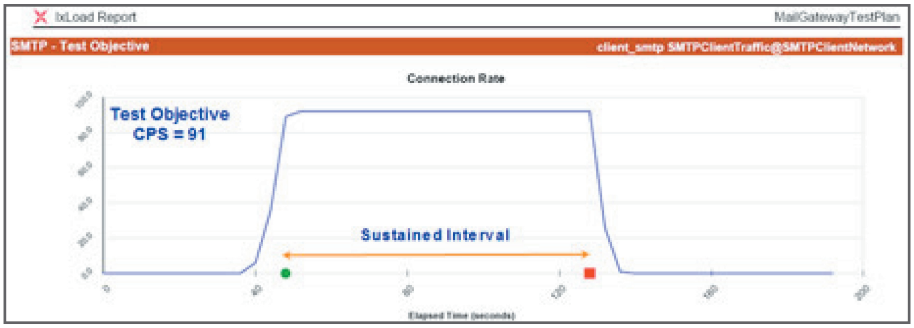
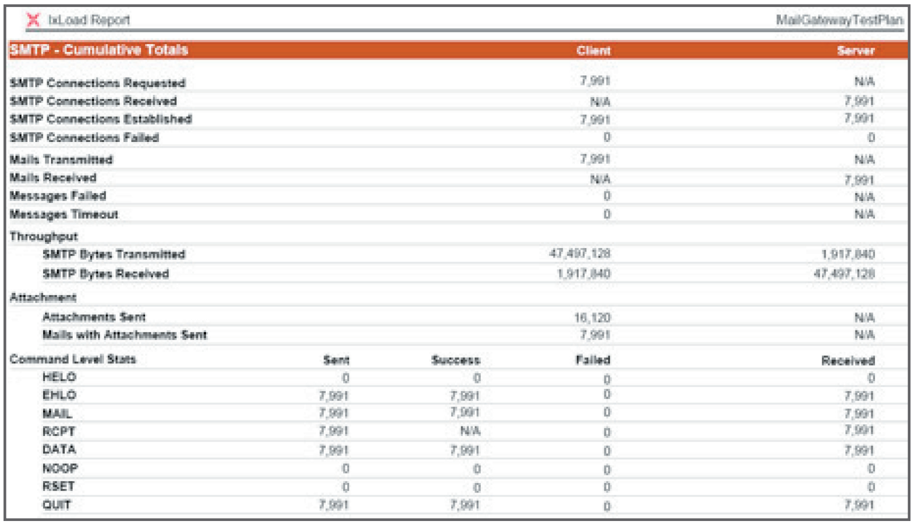


Figure 10. Sustained client CPS over the sustained interval

By reviewing the TCP and SMTP statistics, you can confirm that there were no errors in the transmission. Check for TCP retries or timeouts, via the SMTP statistics, if no failed connections are reported.



IxLoad Report MailGatewayTestPlan

SMTP - Cumulative Totals			Client	Server
SMTP Connections Requested			7,991	N/A
SMTP Connections Received			N/A	7,991
SMTP Connections Established			7,991	7,991
SMTP Connections Failed			0	0
Mails Transmitted			7,991	N/A
Mails Received			N/A	7,991
Messages Failed			0	N/A
Messages Timeout			0	N/A
Throughput				
SMTP Bytes Transmitted			47,497,128	1,917,840
SMTP Bytes Received			1,917,840	47,497,128
Attachment				
Attachments Sent			16,120	N/A
Mails with Attachments Sent			7,991	N/A
Command Level Stats	Sent	Success	Failed	Received
HELO	0	0	0	0
EHLO	7,991	7,991	0	7,991
MAIL	7,991	7,991	0	7,991
RCPT	7,991	N/A	0	7,991
DATA	7,991	7,991	0	7,991
NOOP	0	0	0	0
RSET	0	0	0	0
QUIT	7,991	7,991	0	7,991

Figure 11. Test summary including SMTP connection and command-level statistics

3. SMTP Content Inspection Performance Test – Virus and Spam Detection

Objective

This test further extends the testing scenario from the reference performance Test Case 1 by enabling the Virus scanning and Spam detection engine on the mail gateway (DUT) device, and then measuring the performance impact introduced by both content inspection engines.

Setup

This setup requires at least one server port and one client port. The SMTP client traffic will pass through the SMTP gateway device to reach the SMTP server. The SMTP client and server ports must be connected to the DUT using a Switched infrastructure.

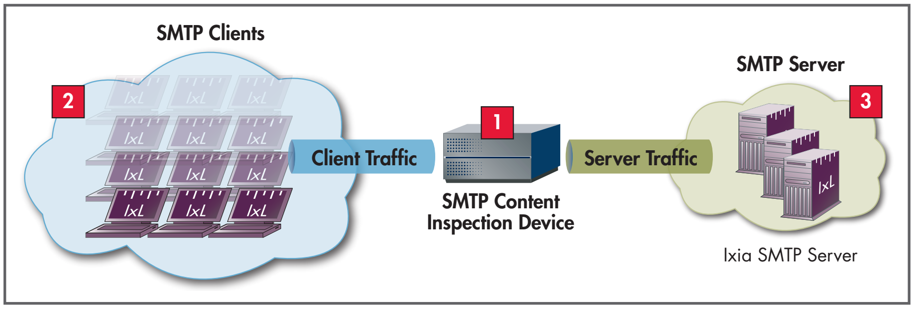


Figure 12. Test topology setup for mail gateway Test Case 3

1. **SMTP Content Inspection Device** – Mail gateway device with dual interfaces. Anti-virus inspection engines is enabled for this test.

2. Performance test facility with **SMTP client traffic** generation capabilities including emails with attachments with configurable email payload.

3. Performance test facility with **SMTP server** capabilities.

Input Parameters

Parameter	Description
Number of SMTP clients	Number of SMTP clients required to meet the Objective
Number of connections per client	One or more TCP connection per SMTP client
SMTP client email payload	Varied email payloads per TCP connection
SMTP server connection limit	Limits set high (10000+)
DUT packet filtering rule	Configure NAT or PAT rules to allow client network access to server(s) network – specifically only TCP/25
DUT content inspection mode	*Anti-virus* – Enabled
	Spam inspection – Enabled
Test Objective(s)	Test the DUT using one or all performance metrics including connections-per-second, throughput, and concurrent connections

Table 3. Test input parameters for Test Case 3

Methodology

1. Configure the emulated SMTP server. Set the concurrent connection limits high (if configurable). The server's gateway is the interface address of the server network side of the DUT.

2. If the DUT is a firewall or proxy device, network address translation (NAT) may or may not be used. The setup topology presented in this test case uses NAT.

3. A packet filtering rule must be configured to allow hosts originating (source) from the Client network to the SMTP server. **Note:** *For the reference test, disable all SMTP inspection engines including anti-virus scanning or spam and content filtering mechanisms.*

4. Configure the emulated SMTP clients to establish a TCP connection to the DUT interface followed by performing SMTP mail delivery transactions. Each SMTP connection can perform single or multiple transactions per TCP connection.

   The sequence of commands generally used to send an email is presented below:

   - HELO
   - MAIL
   - RCPT
   - DATA
   - QUIT

5. The test tool must be configured with the DUT's IP address. The SMTP client traffic is originating from the WAN segment; therefore, the DUT's Client-side interface IP address is used.

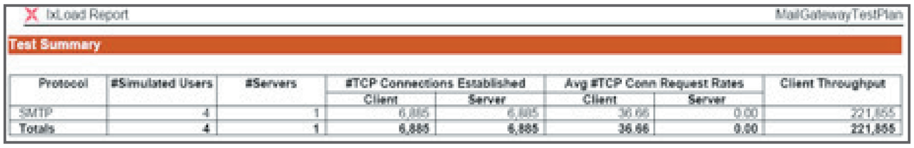
6. Set up the test tool to perform the test. Set the Objective as required and iterate through the process to achieve a reference baseline capacity of the DUT. The test tool may ramp the number of users too quickly or the total number of TCP connections initiated may overwhelm the DUT (or possibly the SMTP server). To achieve a good baseline capacity, adjust the parameters of the test objective and the client payload and monitor the DUT for any errors such as TCP retries and timeouts.

Refer to the "Performance Metrics" section, which provides a framework for three recommended test Objectives.

Results

The objective of this test case was to determine the DUT's connections-per-second (CPS) performance. The following table summarizes how IxLoad achieved the CPS Objective, using an iterative process to ensure that the DUT was not being overwhelmed, for example ensuring that the number of TCP connections established by the SMTP Client equals that of the Server.

The high-level summary provided in IxLoad presents quick access to pertinent information, highlighting the key statistics from the tests run with virus and spam inspection engines enabled.



IxLoad Report MailGatewayTestPlan

Test Summary

Protocol	#Simulated Users	#Servers	#TCP Connections Established		Avg #TCP Conn Request Rates		Client Throughput
			Client	Server	Client	Server	
SMTP	4	1	6,885	6,885	36.66	0.00	221,855
Totals	4	1	6,885	6,885	36.66	0.00	221,855

Figure 13. High-level summary of test simulation to achieve CPS Objective.

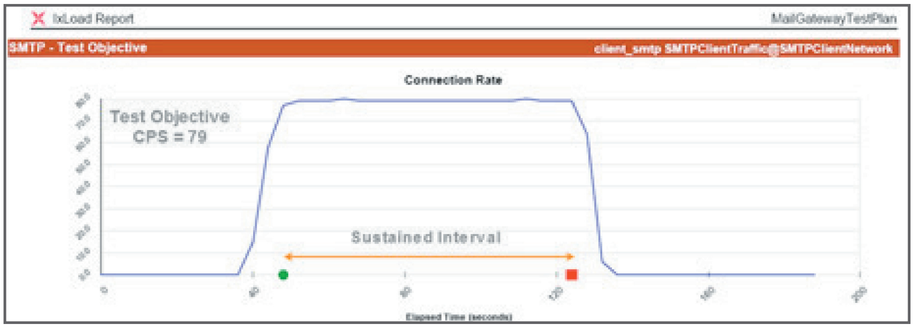
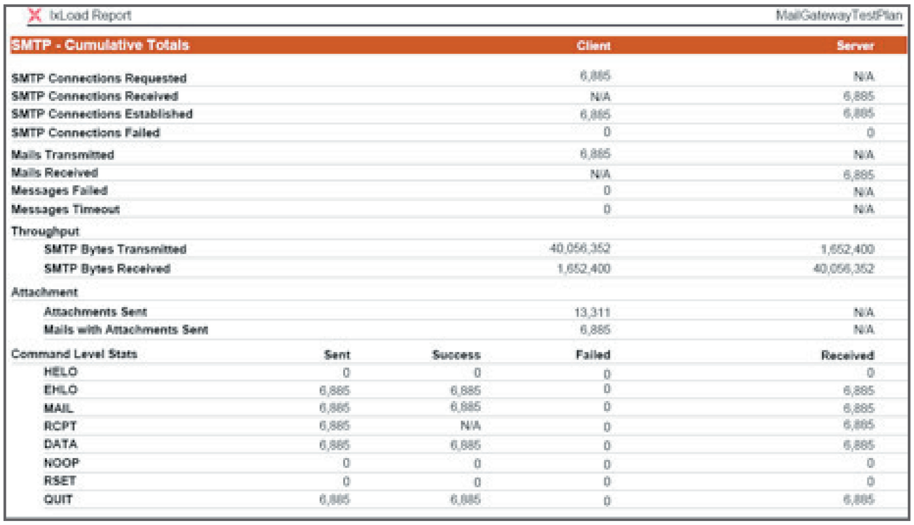


Figure 14. Sustained client CPS over the sustained interval

By reviewing the TCP and SMTP statistics, you can confirm that there were no errors in the transmission. Check for TCP retries or timeouts, via the SMTP statistics, if no failed connections are reported.



IxLoad Report

MailGatewayTestPlan

SMTP - Cumulative Totals	Client	Server
SMTP Connections Requested	6,885	N/A
SMTP Connections Received	N/A	6,885
SMTP Connections Established	6,885	6,885
SMTP Connections Failed	0	0
Mails Transmitted	6,885	N/A
Mails Received	N/A	6,885
Messages Failed	0	N/A
Messages Timeout	0	N/A
Throughput		
SMTP Bytes Transmitted	40,056,352	1,652,400
SMTP Bytes Received	1,652,400	40,056,352
Attachment		
Attachments Sent	13,311	N/A
Mails with Attachments Sent	6,885	N/A

Command Level Stats	Sent	Success	Failed	Received
HELO	0	0	0	0
EHLO	6,885	6,885	0	6,885
MAIL	6,885	6,885	0	6,885
RCPT	6,885	N/A	0	6,885
DATA	6,885	6,885	0	6,885
NOOP	0	0	0	0
RSET	0	0	0	0
QUIT	6,885	6,885	0	6,885

Figure 15. Test summary including SMTP connection and command-level statistics

4. Summary

The performance metrics of the three test cases can be compared to provide insight on the performance impact introduced by content inspection engines such as virus scanners and spam detection engines.

The first test case was used as the reference baseline test with no content inspection engines enabled on the DUT.

The second test case enabled the anti-virus engine on the DUT, and the third test case introduced a heuristics-based algorithm used to parse and detect spam from email messages.

The following table provides a statistical analysis of sample of the performance metrics.

Established TCP Connections					
Objective/ Test Case	**Client CPS**	**Client**	**Server**	**Client Throughput**	**Simulated Users**
CPS 100 – Test 1	100.84	8666	8666	308929	8
CPS 91 – Test 2	81.56	7991	7991	252117	4
CPS 79 – Test 3	73.32	6885	6885	221855	4

Table 4. Statistical analysis of all performance metrics

As illustrated above, the anti-virus engine reduces the connection-per-second capability of the DUT by about 19%, while running the anti-virus engine and the spam detection algorithm further reduces performance from the reference system by about 27%.

Notes:

Notes:

Notes:

Notes:

About Ixia

Ixia is a leading provider of performance test systems for IP-based infrastructure and services. Its highly scalable solutions generate, capture, characterize, and emulate network and application traffic, establishing definitive performance and conformance metrics of network devices or systems under test. Ixia's test systems are used by Network and Telephony Equipment Manufacturers, Semiconductor Manufacturers, Service Providers, Governments, and Enterprises to validate the functionality and reliability of complex IP networks, devices, and applications. Ixia's Triple Play test systems address the growing need to test voice, video, and data services and network capability under real-world conditions. Ixia's vision is to be the world's pre-eminent provider of solutions to enable testing of next generation IP Triple Play networks. Ixia's test systems utilize a wide range of industry-standard interfaces, including Ethernet, SONET, ATM, and wireless connectivity, and are distinguished by their performance, accuracy, reliability, and adaptability to the industry's constant evolution.

Contact Ixia

For more information, contact Ixia or visit our Web Site at **http://www.ixiacom.com**.

Ixia Worldwide Headquarters

Corporate Center
26601 W. Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942
(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805

www.ixiacom.com

Info: info@ixiacom.com

Investors: ir@ixiacom.com

Renewals: renewals@ixiacom.com

Sales: sales@ixiacom.com

Support: support@ixiacom.com

Training: training@ixiacom.com

Ixia USA Sales
Phone: 1.866.355.4942 Email: sales@ixiacom.com

Ixia Canada Sales
Phone: 1.877.367.4942 Email: salescanada@ixiacom.com

Ixia China Sales
Phone: +86.10.84549199 Email: saleschina@ixiacom.com

Ixia Europe, Middle East, & Africa Sales
Phone: +44.1753.722056 Email: salesemea@ixiacom.com

Ixia India Sales
Phone: +91.80.25633570 Email: salesindia@ixiacom.com

Ixia Japan Sales
Phone: +81.3.5365.4690 Email: salesjapan@ixiacom.com

Ixia Oceania Sales
Phone: 1.818.292.1561 Email: salesoceania@ixiacom.com

Ixia South Korea
Phone: +82.11.897.1326 Email: salessouthkorea@ixiacom.com

Ixia Federal Sales
Phone: 1.703.822.7527 Email: salesfederal@ixiacom.com

THIS PUBLICATION IS PROVIDED "AS IS" AND WITHOUT ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. IXIA SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE INFORMATION HEREIN IS FURNISHED FOR INFORMATIONAL USE ONLY, IS SUBJECT TO CHANGE BY IXIA WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY IXIA. IXIA ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES CONTAINED IN THIS PUBLICATION.