BIG-IP Message Security Module

Stop unwanted email from entering your network

Are your anti-SPAM servers overloaded? Are your email users frustrated with unwanted email? Are you required to archive every email that enters your network? Stop SPAM at the edge of your network at the first connection and reclaim your email infrastructure.

The BIG-IP Message Security Module (MSM) is the industry's first reputation-based network edge security module. Leveraging reputation data from Secure Computing's TrustedSource™ multi-identity reputation engine, MSM extends protection for enterprise message applications to the edge of the corporate network – providing businesses with a more powerful and efficient tool for dealing with the growing volume of unwanted email.

Key Benefits:

Stop SPAM at the edge
Emails from reputed spammers are blocked at the SMTP connection, so SPAM never even enters the network.

Eliminates 50% to 70% of unwanted email
Leveraging Secure Computing's TrustedSource™ IP Reputation Score, MSM is able to filter email based upon the real-time reputation of the sender, rather than inspecting the content.

Reduce Cost for Message Management
Since SPAM is stopped at the edge of the network, the traffic load on firewalls, routers, and messaging servers is significantly reduced.

Integrated with BIG-IP LTM
MSM is a module running on BIG-IP Local Traffic Manager, using F5's TMOS operating system for high-performance network intelligence.

A Better Approach to Message Security

To handle ever increasing email volume, as well as high availability and redundancy, most organizations virtualize multiple security gateways and mail servers behind an Application Delivery Networking controller such as BIG-IP® Local Traffic Manager (LTM). These email security gateway products employ multiple techniques, including a virus scanning, deep content inspection, filtering for keywords and heuristics, and custom rules. Rather than continuing to add secure gateway hardware to this infrastructure to handle growing email volumes, MSM takes a better approach by adding intelligence at the network edge, significantly reducing the amount of email that passes on to the email security gateways and servers for further inspection and processing.

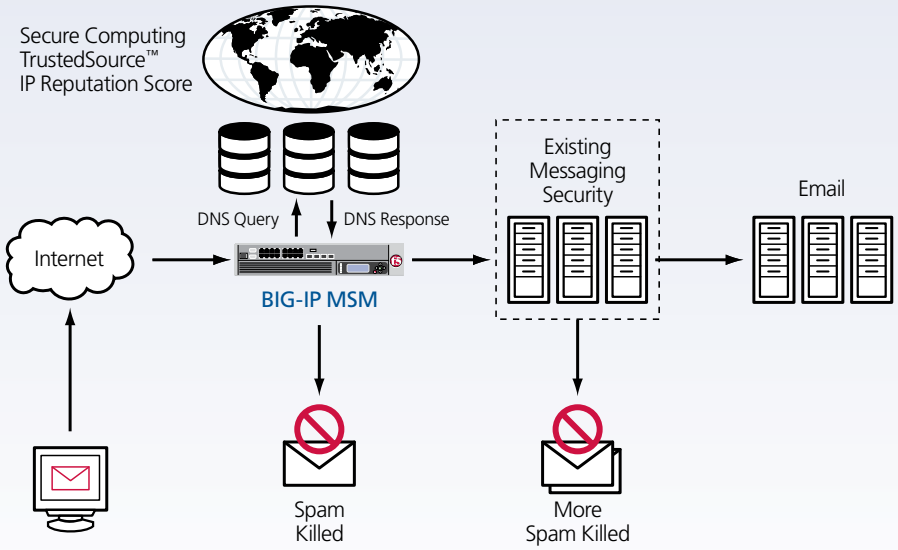
Stopping SPAM at the Edge of the Network

MSM operates by managing and distributing the incoming email (SMTP) connection attempts. It does this by leveraging TrustedSource™, a powerful IP reputation score database that is updated in real-time with very high accuracy and virtually no false-positives. Because it relies on the sender's IP reputation instead of inspecting the content of the message itself, it is very good at blocking sophisticated email threats.

Because MSM does not need to inspect the content of the message to be effective, is very fast, and can process millions of email connections every hour. These connections are denied before the messages' content is sent, so that companies never even receive the spam. This means they are under no requirement to save it, reducing storage costs and hassle.

TrustedSource™ IP Reputation

MSM uses TrustedSource™, Secure Computing's revolutionary reputation system, for information about every sender that attempts to connect to the protected enterprise's mail servers. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists, and outbreak detection with the unparalleled strength of Secure Computing's global customer network of more than 1600 customers in 40 countries, including over one-third of the Fortune 500. It is also the only reputation system available that is able to provide numerical scoring for every IP address across the Internet (approximately 4.2 billion).



Hardware and Ordering

MSM is available as an add-on module for BIG-IP Local Traffic Manager version 9.2 or greater on any of the platforms listed below.

8800 Series

Processor: *Dual CPU, Dual Core (4 processors)*

Base Memory: *4 GB*

ASIC: *Packet Velocity ASIC 10*

Gigabit Ethernet CU Ports: *12 (Copper or Fiber)*

10-Gigabit Fiber Ports: *2 (XFP pluggable optics)*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/48,000/6 Gbps)*

Traffic Throughput: *10 Gbps – L4; 8 Gbps – L7*

Hardware Compression: *6 Gbps*

Input Voltage:
90 – 240VAC +/-10%
90 – 132 9A
180 – 264 4A

8400 Series

Processor: *Dual CPU*

Base Memory: *2 GB*

ASIC: *Packet Velocity ASIC 10*

Gigabit Ethernet CU Ports: *12 (Copper or Fiber)*

10-Gigabit Fiber Ports: *2 (XFP pluggable optics)*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/22,000/2.5 Gbps)*

Traffic Throughput: *10 Gbps*

Available Hardware Option: *Hardware Compression* (2 Gbps)*

Input Voltage:
90 – 240VAC +/-10%
36 – 72VDC (optional)
90 – 132 9A
180 – 264 4A

6800 Series

Processor: *Dual CPU*

Base Memory: *2 GB*

ASIC: *Packet Velocity ASIC 2*

Gigabit CU Ports: *16*

Gigabit Fiber Ports (SFP - GBIC Mini): *4 (2 standard, 2 optional)*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/20,000/2 Gbps)*

Traffic Throughput: *4 Gbps*

Available Hardware Option: *Hardware Compression* (2 Gbps), FIPS Processing***

Input Voltage:
90 – 240VAC +/-10%
90 – 132 9A
180 – 264 4A

6400 Series

Processor: *Dual CPU*

Base Memory: *2 GB*

ASIC: *Packet Velocity ASIC 2*

Gigabit CU Ports: *16*

Gigabit Fiber Ports (SFP - GBIC Mini): *4 (2 standard, 2 optional)*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/15,000/2 Gbps)*

Traffic Throughput: *2 Gbps*

Available Hardware Options: *Hardware Compression* (2 Gbps), FIPS Processing** (8,000 TPS, and 1 GB SSL Throughput)*

Input Voltage:
90 – 240VAC +/-10%
36 – 72VDC (optional)
90 – 132 9A
180 – 264 4A

3410 Series

Processor: *Single CPU*

Base Memory: *1 GB*

ASIC: *Packet Velocity ASIC 2*

Gigabit Fiber Ports (SFP - GBIC Mini): *10*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/5,000/1 Gbps)*

Traffic Throughput: *1 Gbps*

Input Voltage:
90 – 240VAC +/-10%
36 – 72VDC (optional)
90 – 132 6A
180 – 264 3A

3400 Series

Processor: *Single CPU*

Base Memory: *1 GB*

ASIC: *Packet Velocity ASIC 2*

Gigabit CU Ports: *8*

Gigabit Fiber Ports (SFP - GBIC Mini): *2 optional*

Included SSL TPS/ Max TPS/Bulk Crypto: *(100/5,000/1 Gbps)*

Traffic Throughput: *1 Gbps*

Input Voltage:
90 – 240VAC +/-10%
36 – 72VDC (optional)
90 – 132 6A
180 – 264 3A

**The industry's first integrated hardware Compression ASIC cost-effectively centralizes traffic compression processing, improves server capacity by up to 20%, and speeds application response times for end users.*

***FIPS 140-2 Level 2 Certified processing provides enhanced security for SSL keys by storing them in a hardware-secured module. Ideal for sites looking for heightened internal protection of their most sensitive content.*

F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp

Part No. DS-BIG-IP MSM 1007