FORTINET™

REAL TIME NETWORK PROTECTION

FortiMail™ Secure Messaging Platform

Technical Note:
Deployment for outgoing spam filtering
Rev 1.3

November 6, 2008

Table of Contents

Change Log

Revision	Description
1.0	2008/10/12 Initial Release
1.1	2008/10/19
1.2	2008/10/23
1.3	2008/11/06

Comments: nrivat@fortinet.com

Trademarks
Products mentioned in this document are trademarks or registered trademarks of their respective holders.

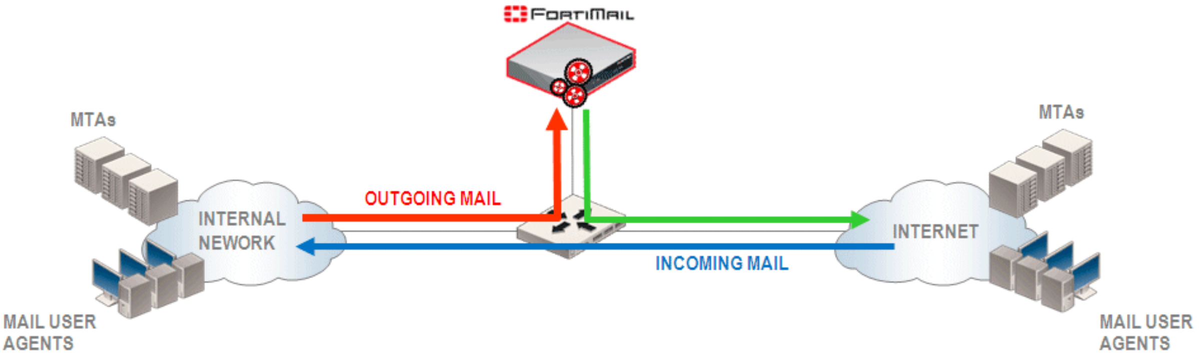
1 Objective – IP address protection

As a method to detect and prevent spam, dedicated Internet servers publish in an easily queried format (DNS) a list of IP addresses linked to spamming: DNSBL (DNS BlackList).
MTAs (Mail Transport Agent) may be configured to query those DNSBL servers and reject or flag messages which have been sent from blacklisted IP addresses. Today DNSBL queries is a popular technique to prevent spam.

ISPs may dynamically assign public IP addresses to their subscribers. In the event that one of those IP addresses is used to send out spam, it would quickly be blacklisted by DNS Black List services. If this IP address is then dynamically assigned to a different subscriber, this new subscribers would inherit the blacklisted state and would be seen as a spam source and be unable to send mail out. The destination mail server would consider, via a DNSBL query, the source IP to be a known spam source.

Even more concerning is the situation where private IP addresses are assigned to subscribers while outgoing traffic is NATed behind few public IP addresses. A single spammer whose connection is NATed behind one of these public IP addresses will cause this IP address to be blacklisted and in that way prevent all users NATed behind the same address to send out mail. This one public, to many private address relationship creates a situation where the providers infrastructure (the public IP address) is compromised and the entire providers subscriber base can find themselves unable to send mail.

Protecting public IP addresses from being blacklisted is essential for Service Providers to guarantee an acceptable level of service to all subscribers.
This protection is achieved by filtering all outgoing mail through a FortiMail unit, the Fortinet purpose-built antispam appliance.



The internal network can be a mobile network providing 3G access to laptops and smart phones or an ADSL network prov iding Internet access to resident subscribers.

2 Requirement – Transparency

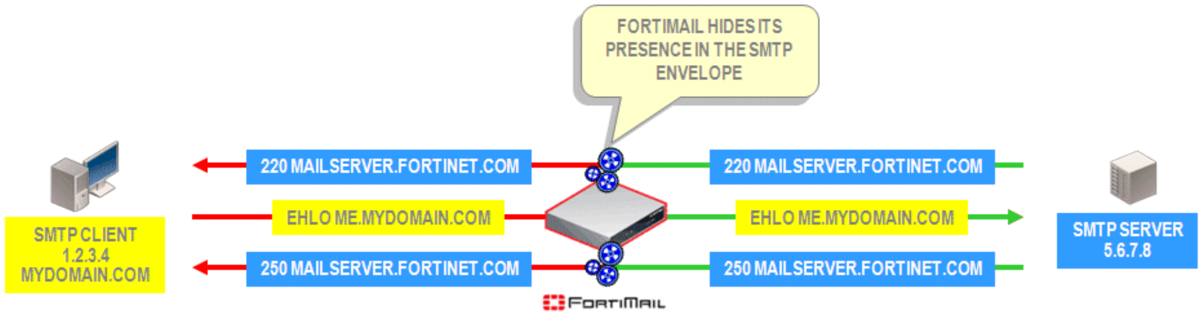
2.1 SMTP transparency

2.1.1 Transparent proxy

The SMTP session initiated by an MUA targets the SMTP server that's specified on the mail client setup. It is inconceivable to ask users to change this target IP address each time they connect to the ISP network. It is inconceivable to enforce outgoing relay settings on the subscribers side, especially for mobile 3G connections. The antispam solution must be a transparent proxy.
Even though mail are not destined to the FortiMail, the appliance is able to intercept the traffic and scan it for spam detection. As a transparent proxy, FortiMail intercepts mail not destined to any of its local IP addresses.

2.1.2 Envelope transparency

As a transparent proxy, FortiMail will hide itself in the SMTP envelope.
It will stay invisible in the SMTP 220 banner, the HELO/EHLO exchange (and any other SMTP command), as shown below:


FORTIMAIL HIDES ITS PRESENCE IN THE SMTP ENVELOPE
SMTP CLIENT 1.2.3.4 MYDOMAIN.COM
220 MAILSERVER.FORTINET.COM
EHLO ME.MYDOMAIN.COM
250 MAILSERVER.FORTINET.COM
220 MAILSERVER.FORTINET.COM
EHLO ME.MYDOMAIN.COM
250 MAILSERVER.FORTINET.COM
SMTP SERVER 5.6.7.8
FORTIMAIL

The SMTP client actually sees the 220 banner as displayed by the SMTP server and not the FortiMail 220 banner. As well, it receives the EHLO arguments as sent by the SMTP server.

2.1.3 Header transparency

FortiMail will hide itself in the headers: even though it has processed and relayed the mail, it does not appear as a relay agent in the headers. The few lines below illustrate this header transparency; it displays the mail headers as received by the SMTP server [5.6.7.8] while the mail sent from client [1.2.3.4] has been processed by FortiMail.
It is important to note that the FortiMail does not add any information related to this activity in the headers.

```
Received: from me.mycompany.com [1.2.3.4]
          by mailserver.fortinet.com [5.6.7.8];
          Wed, 08 Oct 2008 18:50:20 +0200
```

2.1.4 Transparent authentication

Any SMTP authentication request or TLS request are processed transparently by FortiMail and passed to the backend mail server. FortiMail does not interfere in the SMTP negotiation.

2.1.5 Mail queueing prevention

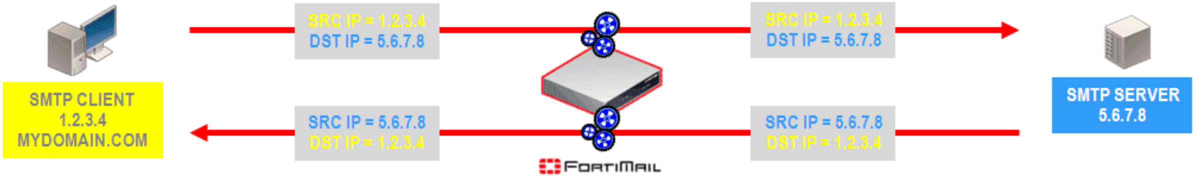
The ISP is not in charge of managing SMTP server availabilities. If the backend mailserver is not reachable, FortiMail should not queue mail.
To fulfill this requirement FortiMail does not accept a client connection if the backend SMTP server can’t be reached. It leaves to the sender the responsibility to queue the mail and initiate a new session later.

2.2 Network transparency

FortiMail hides itself in the IP layer.

2.2.1 Source IP address and transparency

FortiMail does not modify the source IP address while forwarding datagrams on the Internet: it keeps the original source IP address of the sending SMTP clients.
This IP transparency is valid for both interface mode: route mode or bridge mode.



This transparency is critical for large networks of ADSL resident subscribers. There can be a significant amount of connections initiated from the internal network to popular public mail servers, such as Hotmail. Those servers keep track of the number of connections/mail initiated by SMTP clients and would stop responding to an IP addresses where large volumes of traffic originate – as a way to prevent spam. If the antispam solution modifies the source IP address of all sessions it filters with its own IP address, the public mailserver would quickly throttle and blacklist the relay.

By using the original sender IP address, FortiMail prevents this blacklisting from happening while still filtering all outgoing mail.

2.2.2 Destination IP address and transparency

Subscribers are configured with a direct SMTP access to the Internet: they send mail straight to the server IP address as configured in their mail software settings (MUA), or as retrieved by DNS MX queries (MTAs).
FortiMail forwards datagrams to the original destination IP address, the one selected by the sender. It does query a DNS server to retrieve MX information for the recipient domain, it does not take any mail routing decision: it will not override the SMTP server IP address targeted by the client.

3 Deployment

3.1 Dual-arm attachment

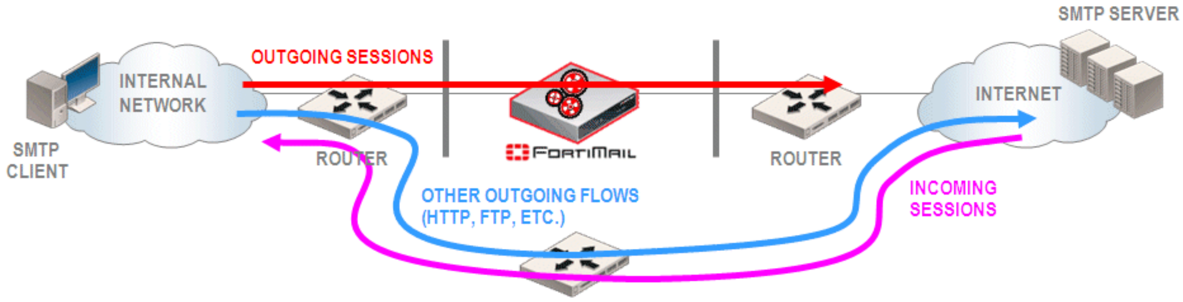
It is recommended to implement FortiMail in a dual-arm attachment. If traffic needs further analysis (sniffer traces for instance) the dual-arm configuration provides natural isolation of traffic before inspection and traffic after analysis.

FortiMail could of course be deployed in single arm attachment to fit any existing network contraints/requirements.

3.2 Policy based routing to redirect outgoing mail traffic

The ISP network design should enforce outgoing SMTP traffic originating from the internal network and destined to the Internet to reach FortiMail for processing.

- There is no need for the antispam appliance to receive the non-SMTP flows going out to the Internet. This would result in unnecessary processing and resource usage, as this traffic may represent a large amount of the bandwidth.
- There is no need to scan incoming SMTP sessions, i.e. the mail sent from the Internet to SMTP servers located on the internal network. This service could as well be provided by FortiMail but would not help outgoing spam filtering, and as such, is out of the scope of this technical note.



In order to extract SMTP traffic from the internal network and to redirect it to FortiMail, the following routing policies should be configured on the ISP network:
[(source IP = internal IP addresses) + (destination port = TCP 25)] -> dedicated route allowing the flow to traverse FortiMail

The response from the Internet SMTP server back to the client should go via the FortiMail which needs to see the full session, i.e. both flows:

- from client -> SMTP server
- + return flow from SMTP server -> client.

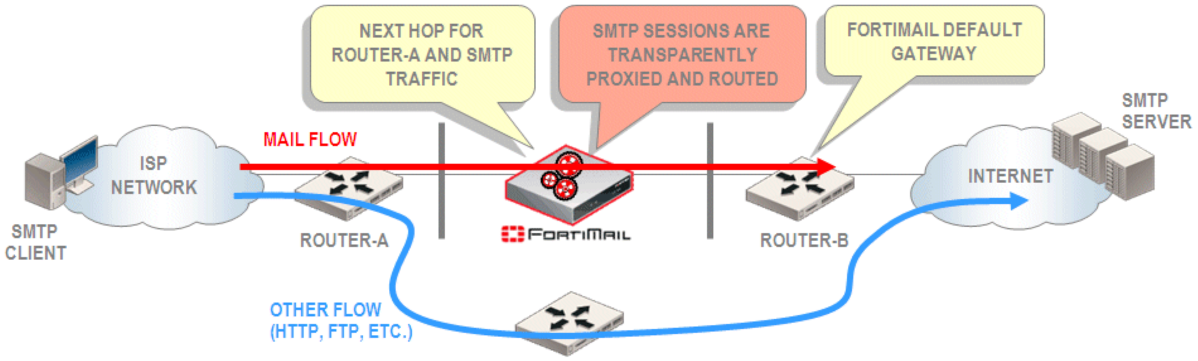
The return packets can be identified with their destination IP address and their TCP source port, as shown below:
[(destination IP = internal IP addresses) + (source port = TCP 25)] -> dedicated route allowing the flow to traverse FortiMail

3.3 Interface mode

FortiMail interfaces can either route or bridge packets.

3.3.1 Acting as a router

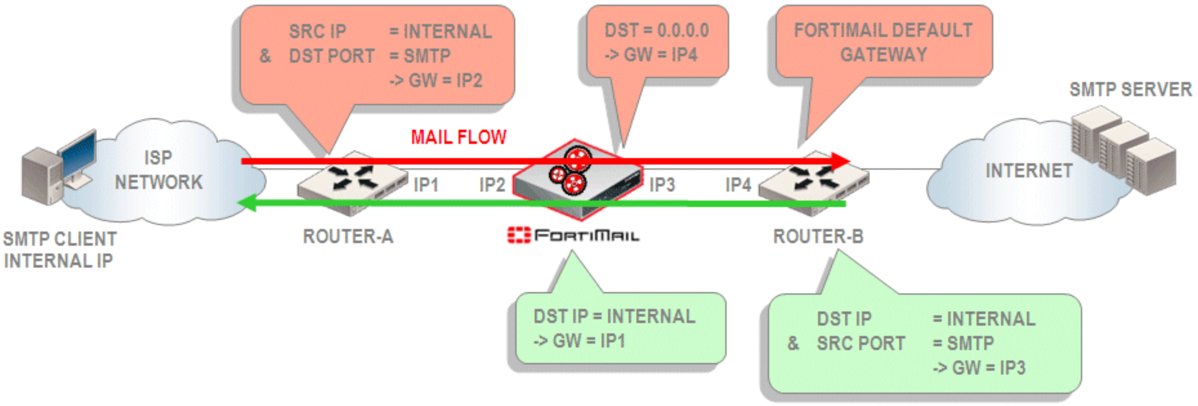
FortiMail interface can be configured to intercept packets as a router would do: i.e. based on the destination MAC address which should be its own interface MAC address.
In this case each interface has a dedicated IP address and will reply to ARP requests.


NEXT HOP FOR ROUTER-A AND SMTP TRAFFIC
SMTP SESSIONS ARE TRANSPARENTLY PROXIED AND ROUTED
FORTIMAIL DEFAULT GATEWAY
SMTP SERVER
MAIL FLOW
ISP NETWORK
INTERNET
SMTP CLIENT
ROUTER-A
FORTIMAIL
ROUTER-B
OTHER FLOW (HTTP, FTP, ETC.)

Example:

The FortiMail unit is configured with two interfaces, one interface is connected on the internal side (port2), the other one is connected on the Internet side (port3).
FortiMail has a dedicated IP address on each port:

- port2 is configured with IP2
- port3 is configured with IP3.



Routing tables are set as presented below:

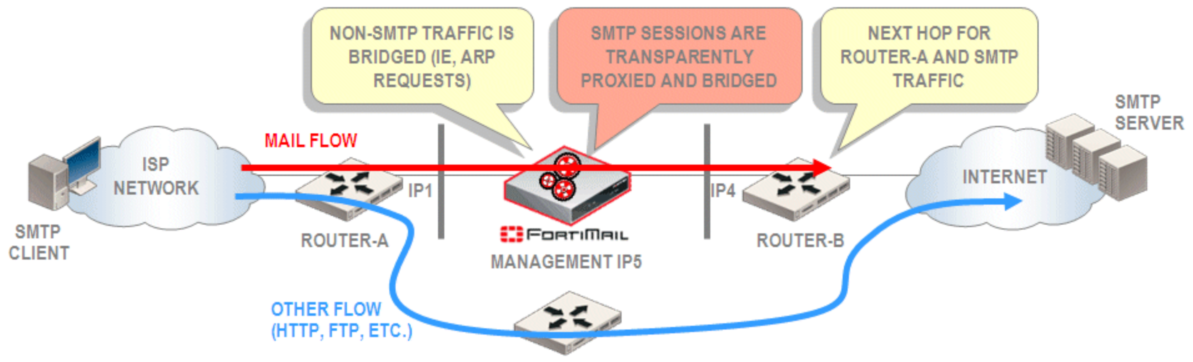
- FortiMail default gateway = IP4
  FortiMail static route to internal addresses = IP1
- Router-A policy based routing:
  (src IP = internal-subnet + dst port = TCP 25) -> next hop = IP2
- Router-B policy based routing
  (dst IP = internal-subnet + src port = TCP 25) -> next hop = IP3

3.3.2 Acting as a bridge

FortiMail can be configured to intercept packets, as a bridge would do.
Packets are not destined for the FortiMail MAC address, instead they are sent to the MAC address of the next hop equipment connected on the other side of FortiMail.

- SMTP sessions are silently intercepted and scanned.
- Non-SMTP traffic is bridged (such as ARP request).

Bridge ports do not have a local IP address. They are associated to the management IP address (IP5), which belongs to the same subnet as IP1 and IP4.


NON-SMTP TRAFFIC IS BRIDGED (IE, ARP REQUESTS)
SMTP SESSIONS ARE TRANSPARENTLY PROXIED AND BRIDGED
NEXT HOP FOR ROUTER-A AND SMTP TRAFFIC
SMTP SERVER
MAIL FLOW
ISP NETWORK
SMTP CLIENT
IP1
ROUTER-A
FortiMail
MANAGEMENT IP5
IP4
ROUTER-B
INTERNET
OTHER FLOW (HTTP, FTP, ETC.)

Routing tables are set as defined below:

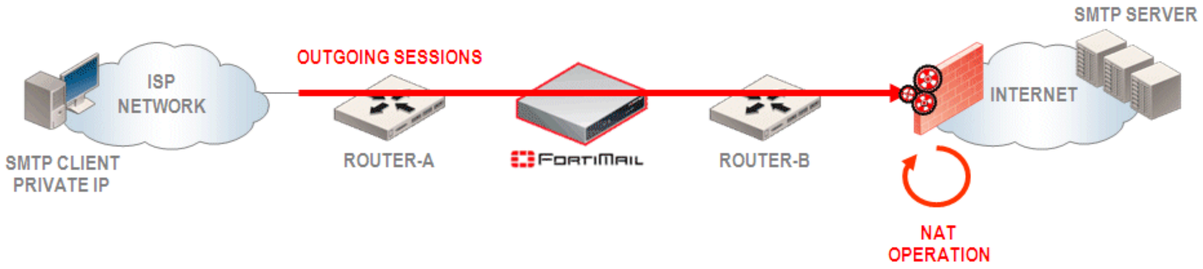
- FortiMail default gateway = IP4
  FortiMail static route to internal addresses = IP1
- Router-A policy based routing:
  (src IP = internal-subnet + dst port = TCP 25) -> next hop = IP4
- Router-B policy based routing
  (dst IP = internal-subnet + src port = TCP 25) -> next hop = IP1

Note: although FortiMail acts as a bridge when intercepting SMTP packets, it still acts as a router when forwarding datagrams:

- It looks up its routing table to select the outgoing interface. This is why a route to the Internet and a route to the internal network is still required.
- And when delivering SMTP packets to the Internet, FortiMail sends them out with its outgoing interface MAC address..

3.4 Where to connect FortiMail

The FortiMail should see the original IP address of the client sessions. If there is a NAT device hiding internal addresses behind few public IP addresses (many-to-one NAT or many-to-many NAT), FortiMail should be placed between the NAT device and the internal network in order to see sessions BEFORE NAT is applied. It should NOT be placed between the Internet and the NAT device.



Antispam filters such as local sender reputation, session rate limiting, mail rate limiting, computes statistics per client – therefore FortiMail needs to uniquely identify each source of mail (by its IP address), NAT would not make it possible reducing the effectiveness of the implementation.

3.5 FortiMail queries

3.5.1 FortiGuard queries

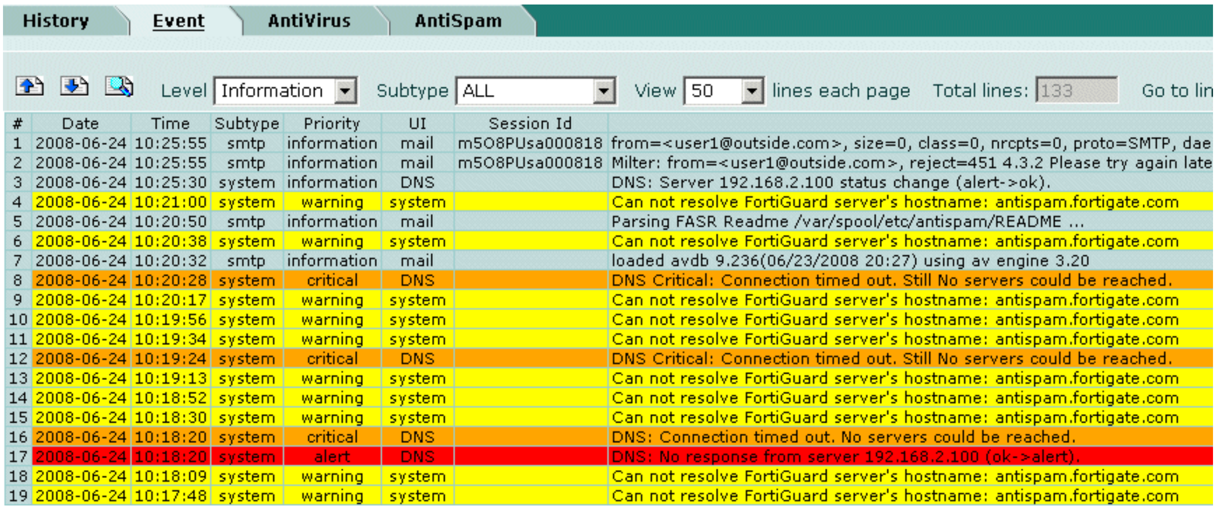
FortiMail needs to query the FortiGuard Database on the Internet to determine well-known spam checksums, spam URIs. The unit achieves this by querying FortiGuard servers on UDP port 8889. The Internet firewall should allow this type of traffic originating from the outgoing interface IP address (route mode) or the management IP address (bridge mode).

Alternatively a private FortiGuard Database Server (FDS) may be locally implemented as part of the ISP network infrastructure. A FortiManager appliance delivers this local FortiGuard service. In such a scenario

FortiMail would locally query the FortiManager appliance which would itself receive regularly and timely updates from the public FDS database.

3.5.2 DNS queries

FortiMail uses DNS queries as part of its antispam techniques. It is important to have fast DNS answers to avoid unnecessary latencies ; it is highly recommended to implement two local DNS servers (primary and secondary) for redundancy and monitor FortiMail logs for any slow-down of the DNS answers as shown below:



Level Information Subtype ALL View 50 lines each page Total lines: 133 Go to lin

#	Date	Time	Subtype	Priority	UI	Session Id	
1	2008-06-24	10:25:55	smtp	information	mail	m5O8PUsa000818	from=<user1@outside.com>, size=0, class=0, nrcpts=0, proto=SMTP, dae
2	2008-06-24	10:25:55	smtp	information	mail	m5O8PUsa000818	Milter: from=<user1@outside.com>, reject=451 4.3.2 Please try again late
3	2008-06-24	10:25:30	system	information	DNS		DNS: Server 192.168.2.100 status change (alert->ok).
4	2008-06-24	10:21:00	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
5	2008-06-24	10:20:50	smtp	information	mail		Parsing FASR Readme /var/spool/etc/antispam/README ...
6	2008-06-24	10:20:38	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
7	2008-06-24	10:20:32	smtp	information	mail		loaded avdb 9.236(06/23/2008 20:27) using av engine 3.20
8	2008-06-24	10:20:28	system	critical	DNS		DNS Critical: Connection timed out. Still No servers could be reached.
9	2008-06-24	10:20:17	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
10	2008-06-24	10:19:56	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
11	2008-06-24	10:19:34	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
12	2008-06-24	10:19:24	system	critical	DNS		DNS Critical: Connection timed out. Still No servers could be reached.
13	2008-06-24	10:19:13	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
14	2008-06-24	10:18:52	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
15	2008-06-24	10:18:30	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
16	2008-06-24	10:18:20	system	critical	DNS		DNS: Connection timed out. No servers could be reached.
17	2008-06-24	10:18:20	system	alert	DNS		DNS: No response from server 192.168.2.100 (ok->alert).
18	2008-06-24	10:18:09	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com
19	2008-06-24	10:17:48	system	warning	system		Can not resolve FortiGuard server's hostname: antispam.fortigate.com

3.5.3 Ports for originating traffic

Service	Ports
Syslog to send log messages to remote syslog servers and to FortiAnalyzer.	UDP 514
Archiving and mail data storage on external NAS server using NFS.	TCP 2049
Archiving to external FTP and SFTP servers.	TCP 21 / TCP 22
SNMP traps	UDP 162
DNS lookup	UDP 53
NTP synchronization	UDP 123
FortiGuard Antivirus updates (pull).	TCP 443
FortiGuard Antivirus updates (push)	UDP 9443
FortiGuard and AntiSpam ratings.	UDP 8889

4 3G mobile network and FortiMail related features

4.1 RADIUS and MSISDN association

An MSISDN is the number associated with a SIM card on a mobile network. As IP addresses are dynamically assigned to 3G enabled laptops, mobile operators may prefer:

- to work with MSISDN reputation instead of IP scoring as a technique to block spam sources
- and get antispam reports based on MSISDN numbers rather than IP addresses.

Subscribers get a dynamic IP address when they connect to the network and FortiMail can dynamically learn the IP address associated to each connecting MSISDN. This mapping is retrieved from RADIUS accounting packets. When a subscriber connects to the 3G network, the session is processed by a RADIUS server which receives the MSISDN information, authenticates the user and results in a dynamic IP address being assigned to the user. The RADIUS server for every new connection is aware of the IP/MSISDN association.

To let a RADIUS server work with Fortimail, the following configuration is needed on the RADIUS server side:

- Send out RADIUS Accounting-Request packets (start/stop) to the Fortimail IP address (management address in bridge mode or interface address in route mode), on UDP port 1646 or 1813.
- 3 attributes are recognized, they are:
    - ➢ Acct-Status-Type, its value can be either Start or Stop
    - ➢ Calling-Station-ID, its value is the MSISDN of user, usually a mobile phone number
    - ➢ Framed-IP-Address, its value is the IP address of the mobile station.

With this information, FortiMail is able to associate an IP address with a MSISDN, thus to find out a mail sender's MSISDN.

4.2 MSISDN reputation

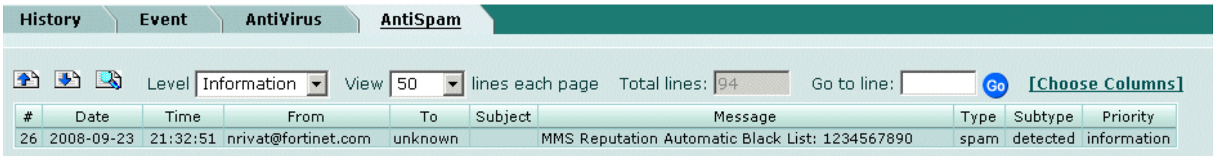
When used on a mobile phone network, the FortiMail unit can examine messages for spam. If a user sends multiple spam messages, all messages from the user will be blocked for a time. The Fortimail unit automatically blacklists repeat offenders.

The number of spam messages and the length of time further messages will be blocked are configurable by the FortiMail administrator.
If a sender sends more than a defined number of spam messages within the auto blacklist window, the sender will be blacklisted and further messages will be blocked for the auto blacklist duration period.

The auto blacklist score trigger value (the number of spam messages), the auto blacklist window size (the time during which the spam messages are detected), and the auto blacklist duration (the length of time the MSISDN is auto blacklisted), are all configurable.

In addition to auto blacklisting, senders can be manually blacklisted and their messages will be blocked indefinitely.
Senders can also be manually added to the exempt list to prevent auto blacklisting.

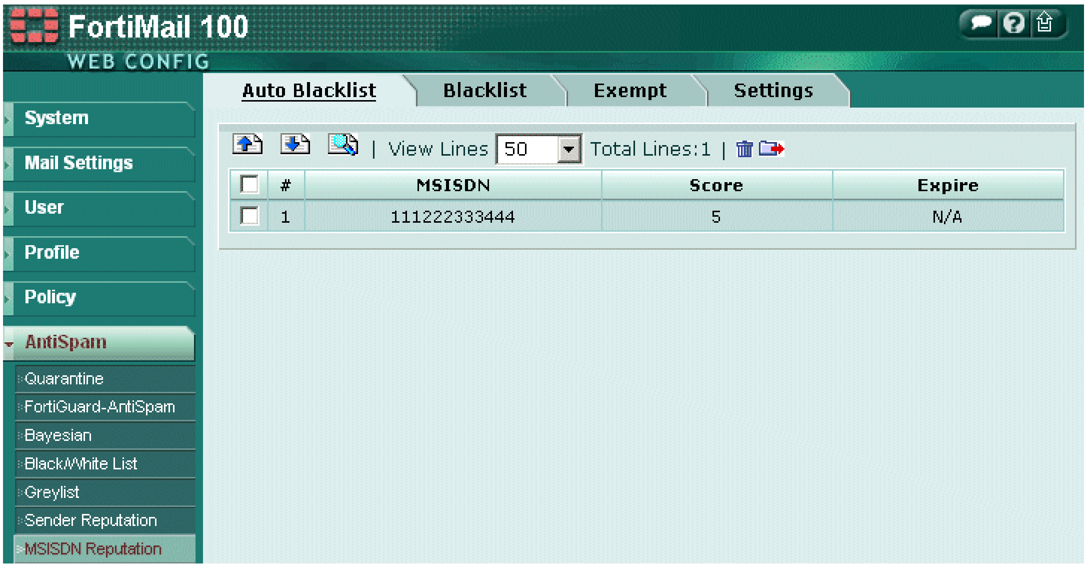
When a connection is refused because of auto blacklisting, the antispam log would store the event with the MSISDN number:



Level Information View 50 lines each page Total lines: 94 Go to line:

#	Date	Time	From	To	Subject	Message	Type	Subtype	Priority
26	2008-09-23	21:32:51	nrivat@fortinet.com	unknown		MMS Reputation Automatic Black List: 1234567890	spam	detected	information

The current scoring against each MSISDN is available for review and displayed from the graphical interface:



View Lines 50	Total Lines:1

□	#	MSISDN	Score	Expire
□	1	111222333444	5	N/A

4.3 MSISDN based reporting

FortiMail provides statistic reports based on MSISDN:

- Top Sender MSISDN
- Top Client MSISDN
- Top Spam MSISDN
- Top Virus MSISDN

Each report is available by: Date, By Hour Of Day, By Day Of Week, By Day Of Month, By Week Of Year, By Month.

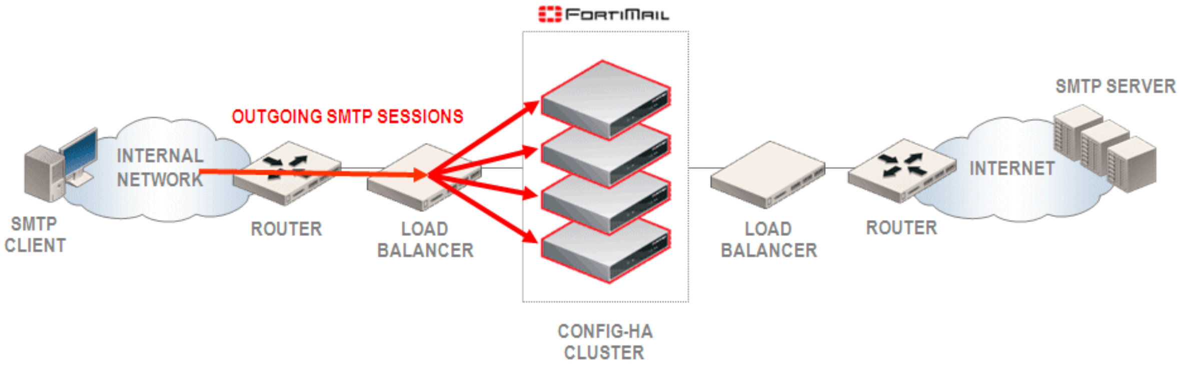
This allows Service Providers to quickly identify bad senders and take appropriate actions (such as contacting the subscribers, offering antivirus services, etc.).

5 Sizing

5.1 Scalability

To handle the traffic load, more than one FortiMail unit may be needed.
To increase the spam filtering throughput a load-balancer is used to distribute traffic to multiple FortiMail units.

Flows from the same IP address should be maintained to the same FortiMail unit – to avoid traffic from the same source to be split among multiple units and make sure FortiMail can accurately maintain IP statistics. Most load-balancers would support IP persistency.



The return flow should be sent to the same FortiMail unit that initially processed the flow on its way to the Internet. To achieve this, the return flow should hit another load-balancer which will then take the decision to forward the flow to the appropriate FortiMail unit: load-balancers should be deployed on both sides of FortiMail.

If only one load-balancer is available on the network, it is possible to connect the two FortiMail interfaces to the same unit - if the load-balancer supports this configuration (i.e. F5 Big-IP).

Some load-balancers would not support to see the same session on two different ports (i.e. Foundry IronServer). In this case you would have to deploy FortiMail in single-arm attachment.

5.2 Clustering

To simplify configuration management, FortiMail may be configured as a config mode cluster.
The settings related to mail protection (such as filtering policies, filtering profiles) are shared and automatically synchronized between all cluster members, while the network related parameters (such as the IP addresses) are kept local.

5.3 Central logging

Logs and reports need to be centrally managed with a FortiAnalyzer appliance.
FortiAnalyzer acts as a central server for log repository and offers advanced search tools: search based on a group of FortiMail appliances, search across multiple log types (event log, antispam log, history logs). It computes statistics and reports based on aggregated data (logs) retrieved from multiple FortiMail units.

5.4 Central quarantine

It may be required to enable quarantine services. Spam would be sent to a system quarantine, for administrator review.
As multiple FortiMail units are active and simultaneously quarantining spam, a central quarantine service is needed.
An active-passive cluster of FortiMail units would can provide a centralized quarantine service. Multiple terabytes of storage are available on a FortiMail 4000A.

5.5 Sizing

Sizing any antispam solution requires a number of parameters be known to make an accurate assessment, the more information that is available the more accurate the assement can be to avoid under sizing, or over engineering any implementation.
The list below shows some typical parameters, the peak session rate is a key value which must be provided.

- Number of subscribers
- Number of subscribers simultaneously connected to the network
- Number of subscribers sending mail simultaneously
- Peak session rate: number of mail/second or mail/hour
- Number of internal IP addresses assigned to subscribers
- Average mail size

5.6 Licensing

FortiMail supports an unlimited of mailboxes. Antispam protection is offered to any SMTP sessions regardless of mailbox or domain count.