Technical Note

FortiMail Transparent Mode Options Explained

Revision 0.7

November 16, 2009

Table of Contents

Comments: michal.kulakowski@fortinet.com, nrivat@fortinet.com

Trademarks

1 Introduction

Transparent mode is powerful and unique feature of FortiMail. It is also very often misunderstood. Most of the times the decision on specific mode used during testing or deployment is taken before the device is implemented in the network and seldom changed afterwards. Taking this into account it is vital to know all the consequences before making such long term choice.

1.1 Goal

The goal of this paper is to gather in one place and explain popular options affecting FortiMail transparency layers 2 to 7 of OSI/ISO model as well as to list some best practices concerning choosing and implementing operation mode.

1.2 Scope

Documenting semantics of FortiMail commandline or web administration interface is out of scope of this document. Refer to FortiMail Administration Guide and FortiMail CLI Reference for that purpose. Current versions of these documents can always be retrieved from http://docs.fortinet.com.

This document concerns FortiMail version 3.0 MR5. Earlier versions may differ in functionality.

1.3 Conventions used

Commandline sequences and WebGUI user input are marked with `fixed width font` throughout the document.

Names of WebGUI elements (buttons, tabs, sections) are marked in *italics*.

This technical note refers to situation where FortiMail scans SMTP sessions in transparent mode. Therefore wherever word “client” is mentioned, it points to the host initiating SMTP session intercepted by FortiMail. Client can be MUA or MTA. Word server refers to MTA to which the message is delivered by FortiMail or to which it was originally meant to be delivered.

2 Transparent mode

Transparent mode is one of three modes FortiMail can be configured to work in (server, gateway and transparent). As FortiMail is an application level security gateway, the word “transparent” does relate to the application layer and not the underlying ones:

- Setting the mode to transparent implies that FortiMail is able to intercept SMTP connections which are not destined to itself (it does not own the destination IP address of the SMTP connection) – as opposed to server mode or gateway mode where sessions are destined to the appliance itself.
- It does NOT determine layer 2 or 3 settings though.

2.1 Network layer settings

Bridge mode interface

By default all FortiMail interfaces are attached to a built-in bridge when the appliance is set in transparent mode.

Route mode interface

One can attach and remove network interfaces from the built in bridge. Removing an interface from the bridge automatically set the interface in route mode. A local IP address should be configured and belong to a different subnet than the management IP address.

Note: port1 is the only port permanently attached to the built-in bridge; it cannot be set in route mode.

Intercepting packets

Bridge or route mode determines the way packets are intercepted by FortiMail and NOT the way packets are forwarded.

- In route mode FortiMail intercepts unicast frames destined to its interface mac address,
- while it learns which unicast frames to intercept as a switch would do when frames are received on a bridge interface.

Delivering packets

To deliver SMTP packets, FortiMail DOES NOT leverage its bridging table, it always consider its routing table to determine the outgoing interface. Understanding this is vitally important for successful deployment.

When SMTP packets are sent by FortiMail to the destination SMTP server, FortiMail looks up its routing table to determine the next hop and the outgoing interface. When SMTP packets are sent by FortiMail to the SMTP client, FortiMail also looks up its routing table to determine the next hop and the outgoing interface.

As a consequence FortiMail MUST have a route to the client subnets and a route to the destination servers. Typically a default route to the Internet is configured to reach any external clients/servers and several static routes are configured to reach any internal clients/servers.

Source IP address

FortiMail handles two distinct TCP sessions for every processed SMTP connection:

- the original session flowing from the client to the server and intercepted by FortiMail
- and the new session generated by FortiMail to the destination server (which can be the same or a different server).

If this new session is estabished from a bridge interface FortiMail uses its management IP address as a source IP address. If the new session is initiated from a route mode interface FortiMail uses the interface IP address as a source IP address.

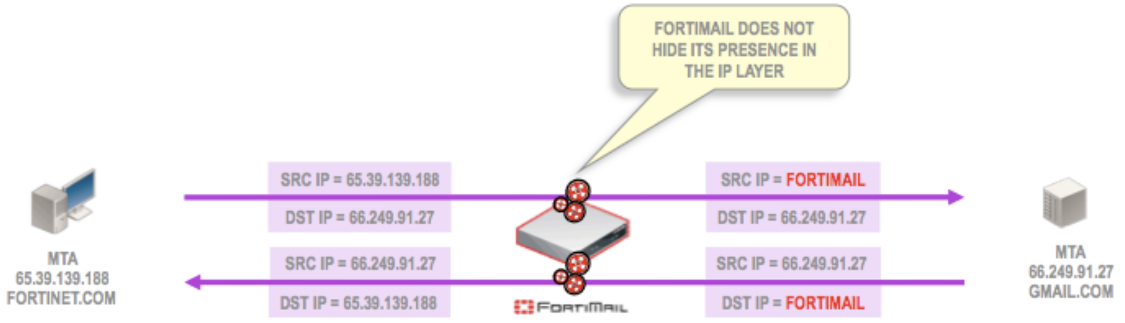

Figure 1 FortiMail does not hide its presence in the IP layer by default

Hiding FortiMail at the IP layer

FortiMail can be configured to masquerade the client IP address when issuing this new session to the destination server. Two distinct cases exist:

1. If the original destination IP matches server known to FortiMail, session is handled by the incoming proxy. In such case domain level setting with command
   `set policy <domainname> modify tp 0 yes yes`
   makes FortiMail hide it's presence by:
   a. Spoofing source address of session going out
   b. Spoofing envelope information
   c. Not adding it's own headers

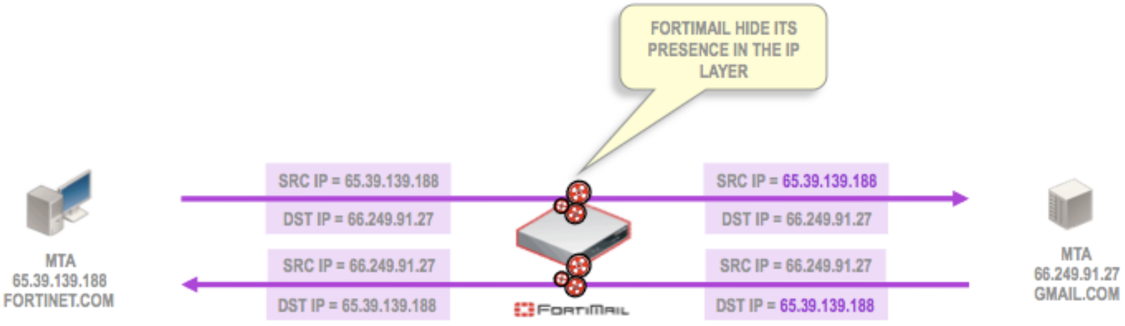

Figure 2 FortiMail IP Layer transparency

2. Otherwise session is handled by the outgoing proxy and its behaviour is regulated by session profile command:
   `set ip_profile <profilename> connection hide enable`

Both settings are used wherever FortiMail should hide its presence. Typical reasons include:

- Avoid to send out too many connections from single IP not to get blacklisted or rate limited (IP pools can be used for that purpose as well)
- Avoid exposing FortiMail IP (IP transparency)
- Avoid FortiMail presence in “Received” headers of message delivered to final recipient (Envelope transparency)

2.2 SMTP Proxy settings

Multiple settings exist which can affect FortiMail behaviour in conversation with other mail agents. Most common are described below.

2.2.1 “Use client-specified SMTP server to send e-mail” (a.k.a. ISP transparent mode)

This setting located under *Mail Settings/Proxies* and accessible from CLI with command:

```
set mailserver proxy smtp unknown yes yes
```

changes the way FortiMail handles e-mail connection completely. Without it defined FortiMail would intercept messages and resolve MX for recipient domain to deliver it. The MX resolution would be performed as configured locally on FortiMail: DNS query or a static entry. If this resolution led to a different IP address than the one established by the client, FortiMail would override the client specified IP address.

If the destination server cannot be reached, FortiMail will queue the mail to deliver it again later.

Typical sequence is shown on Figure 3,below.

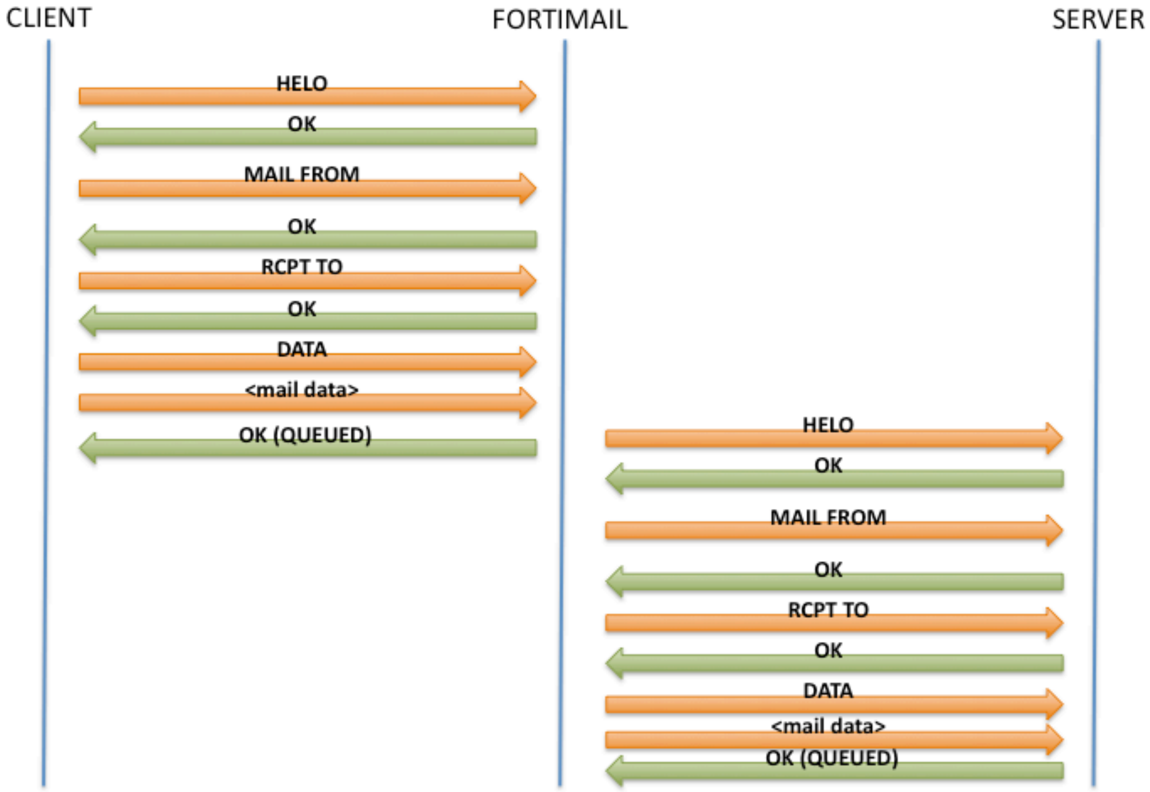

Figure 3 Standard transparent mode behaviour

Note, that although authentication profile can be added to a policy to verify user against the target SMTP server, there is no way to make FortiMail cache the credentials and also authenticate target session. Target session is standard unauthenticated MTA to MTA connection and target MTA should be configured appropriately to accept it (e.g. should accept relaying mail from FortiMail IP).

Enabling the ISP Transparent Mode checkbox will trigger FortiMail into proxying the session as shown on Figure 4, below.

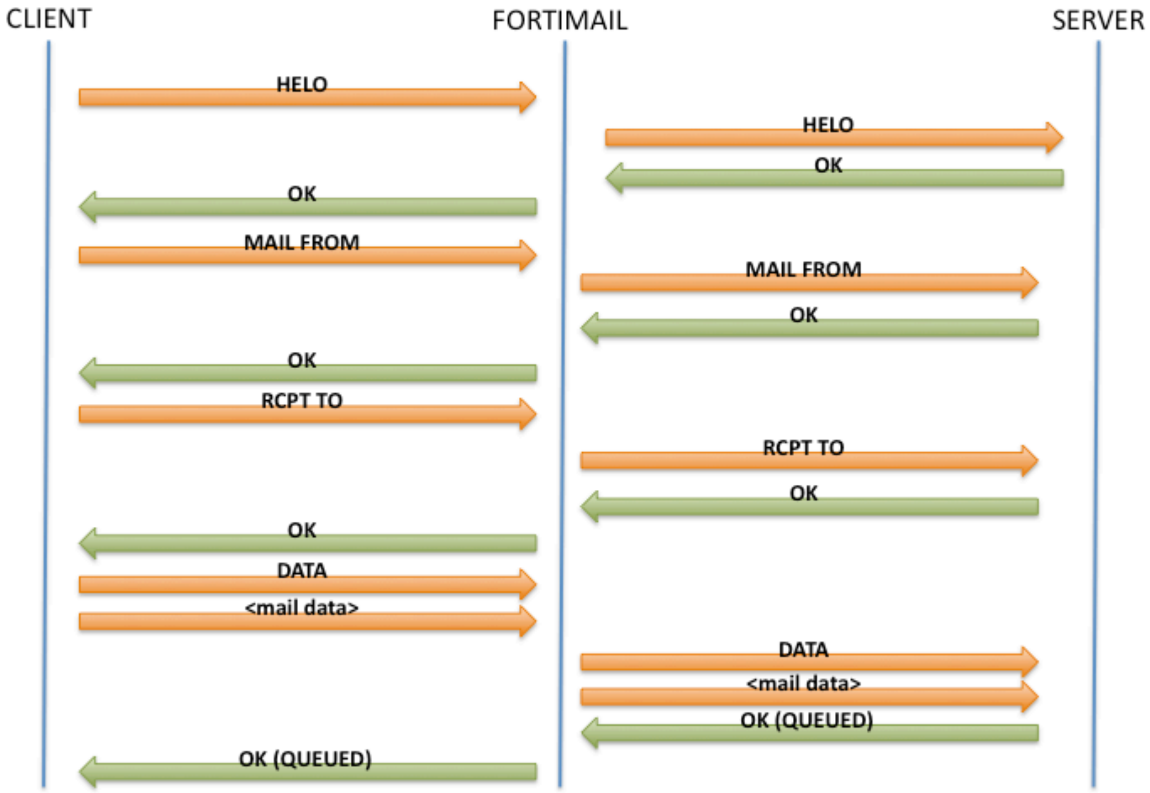

Figure 4 ISP transparent mode behaviour

There are several consequences of this approach. Three most notable of them are:

1. FortiMail would not modify the destination server as chosen by the client. The destination IP address of the new session initiated by FortiMail remains the same. It does not perform any MX resolution.
2. Authentication is now handed over to the target server transparently, so no configuration changes are necessary
3. FortiMail does not queue mail if it cannot be delivered. It processes in real time any client specified command with the server. If delivery is not possible, proper status code gets forwarded to the client side. This way resource management needed to queue mails properly is moved to a sending party, which can be significant advantage in carrier environments. Not only this approach saves resources, but also FortiMail is free from obligation to send delivery notifications of any kind. Such DSN's sent back to fake sender addresses can be treated as spam by other gateways.

Typical application of the setting described above is to scan outgoing ISP's mail traffic to prevent IP pool blacklisting.

2.2.2 "Switch to SPLICE mode after n seconds/kilobytes"

If ISP transparent mode is enabled and client side link is slow it may happen that the server side connection times out before full e-mail data gets transferred. To combat this one can use SPLICE mode defined in session profile and available from CLI by the following command:

```
set ip_profile <profilename> check splice enable <integer>
{seconds | kilobytes}
```

Enabling splicing would trigger FortiMail to scan the arriving data and forward clean chunks to the server side as shown on the Figure 5, below.

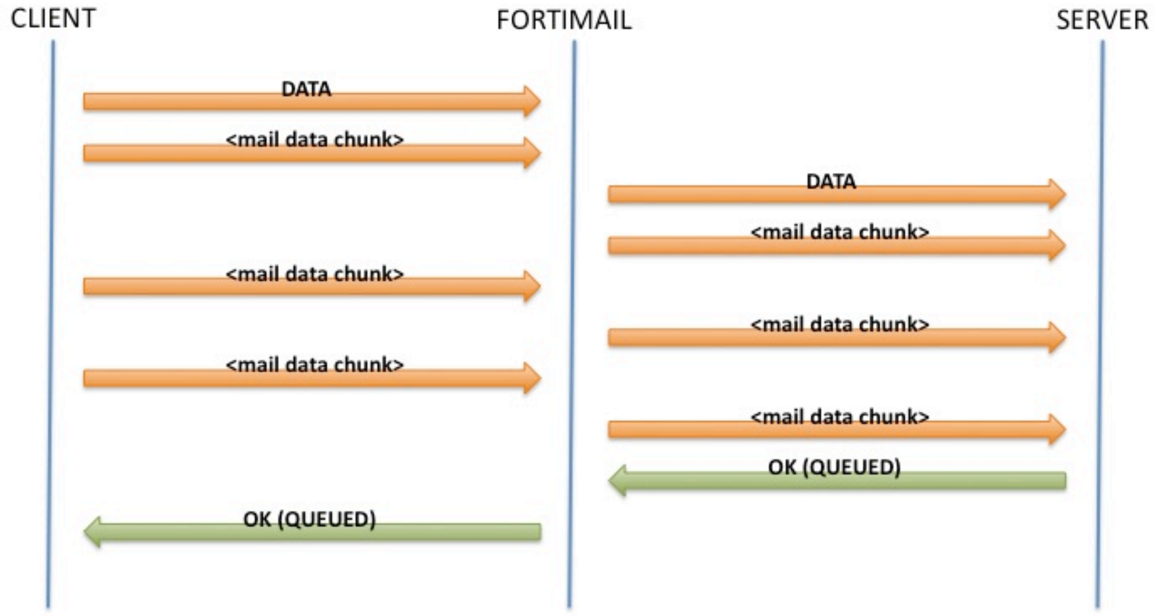

Figure 5 Data handling in SPLICE mode

In case message is spam or contains virus, it can still be kept by terminating server connection without proper <CR><LF>.<CR><LF> sequence and sending SMTP error code to the client.

The advantage of this setting is avoiding timeouts, while the price is slightly increased resource consumption for session management.

3 Deployment guidelines

Transparent mode, and especially its ISP variant has been developed for the purpose of implementing FortiMail in carrier environments to combat outgoing SPAM. For Enterprise class deployments, in vast majority, gateway mode should be the first natural choice. It is usually easier to implement and better understood by customer. Exceptions from that rule cover situations where neither DNS MX records nor IP addresses cannot be modified as well as quick proof of concept installation in complex environments.

Standard transparent mode can be used in such cases. It offers the option to simplify deployments, it should nevertheless be carefully handled and will only work if provided with proper routing table and understanding of the transparency impact on layer-2 / layer-3.