

FortiMail: Configuration Best Practices

This page presents best practice configuration items for FortiMail and is organized by topic.



Best practices are intended to be encompassing of most environments. The user is however expected to assess the recommendations and gain an understanding of whether they are correct in his specific use case.

Network and base configuration

Setup date and time parameters

Log analysis is complex without the correct timezone being configured.

The screenshot shows the FortiMail VM08 configuration interface. The left sidebar is expanded to 'System' > 'Configuration'. The main content area is titled 'Time' and contains the following settings:

- System time: 7/31/2018 10:33:48 (with a Refresh button)
- Time zone: (GMT-5:00)Eastern Time(US & Canada)
- Automatically adjust clock for daylight saving time changes:
- Set date: Synchronize with NTP Server
- Server: pool.ntp.org
- Sync Interval: 60

Setup forward DNS Setup forward DNS to organization standard DNS, keeping in mind that DNS is used for a number of controls and if internal zone queries are needed (e.g. usage of internal hostnames in the configuration), the unit should point to recursive servers that can resolve those.

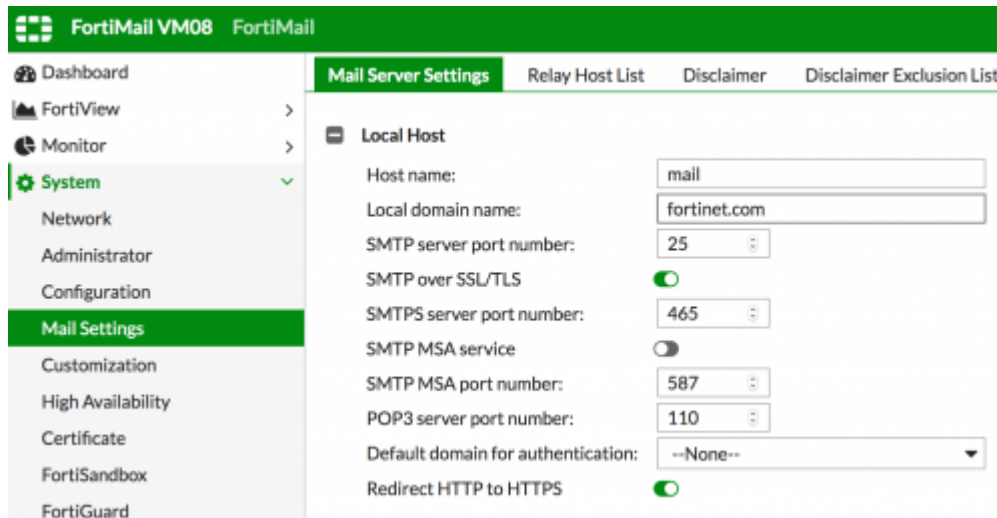
The screenshot shows the FortiMail VM08 configuration interface. The left sidebar is expanded to 'System' > 'Network'. The main content area is titled 'DNS' and contains the following settings:

- Primary DNS server: 208.91.112.53
- Secondary DNS server: 208.91.112.52

MTA Parameters

Setup hostname and local domain name

This information is used by the MTA as its identity for both incoming and outgoing SMTP connection. It should be set to a hostname for which forward lookup points to the FortiMail public IP address used for establishing outbound connections.



The screenshot shows the FortiMail VM08 configuration interface. The left sidebar contains a navigation menu with options: Dashboard, FortiView, Monitor, System (selected), Network, Administrator, Configuration, Mail Settings (highlighted), Customization, High Availability, Certificate, FortiSandbox, and FortiGuard. The main content area is titled 'Mail Server Settings' and includes tabs for 'Relay Host List', 'Disclaimer', and 'Disclaimer Exclusion List'. Under the 'Local Host' section, the following settings are visible:

Host name:	mail
Local domain name:	fortinet.com
SMTP server port number:	25
SMTP over SSL/TLS:	<input checked="" type="checkbox"/>
SMTPS server port number:	465
SMTP MSA service:	<input type="checkbox"/>
SMTP MSA port number:	587
POP3 server port number:	110
Default domain for authentication:	--None--
Redirect HTTP to HTTPS:	<input checked="" type="checkbox"/>

Security Profiles

Antispam profile: generally recommended settings

Configure two URI filter profiles, or edit existing default profiles “phishing” and “unrated” to ensure they match the following:

URI Filter Profile

Profile Name:

Fortiguard Categories

- Potentially Liable
- Adult / Mature Content
- Bandwidth Consuming
- Security Risk
 - Dynamic DNS
 - Malicious Websites
 - Newly Observed Domain
 - Newly Registered Domain
 - Phishing
 - Spam URLs
- General Interest-Personal
- General Interest-Business
- Unrated

URI Filter Profile

Profile Name:

Fortiguard Categories

- Potentially Liable
- Adult / Mature Content
- Bandwidth Consuming
- Security Risk
 - Dynamic DNS
 - Malicious Websites
 - Newly Observed Domain
 - Newly Registered Domain
 - Phishing
 - Spam URLs
- General Interest-Personal
- General Interest-Business
- Unrated

The following screenshot shows the default recommended options for inbound antispam filtering:

AntiSpam Profile

Default action:

Scan Configurations

<input checked="" type="checkbox"/> FortiGuard	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> IP Reputation <ul style="list-style-type: none"> <input type="checkbox"/> Extract IP from Received Header 	Action: <input type="text" value="--Default--"/>
URI filter	
<input checked="" type="checkbox"/> Primary <input type="text" value="phishing"/>	Action: <input type="text" value="Discard"/>
<input checked="" type="checkbox"/> Secondary <input type="text" value="unrated"/>	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> Spam outbreak protection	
<input checked="" type="checkbox"/> Greylist	
<input checked="" type="checkbox"/> SPF check	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> DMARC check	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> Behavior analysis	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Header analysis	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Impersonation analysis	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> Heuristic	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> SURBL [Configuration...]	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> DNSBL [Configuration...]	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Banned word [Configuration...]	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Safelist word [Configuration...]	
<input type="checkbox"/> Dictionary	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Image spam	Action: <input type="text" value="--Default--"/>
<input type="checkbox"/> Bayesian	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> Suspicious newsletter	Action: <input type="text" value="--Default--"/>
<input checked="" type="checkbox"/> Newsletter	Action: <input type="text" value="--Default--"/>

Do note that two controls in this list can result in email delivery delay:

- Greylisting: will delay delivery the first time we see a sender, but not afterwards
- Spam outbreak protection: may delay delivery when emails are perceived as suspicious

This recommendation assumes that user quarantine is being leveraged. If not desired, system quarantine can be used instead.

From:
<http://inside.fortinet.com/> - **Inside Fortinet**

Permanent link:
http://inside.fortinet.com/doku.php?id=fortimail_best_practices

Last update: **2018/07/31 15:05**

