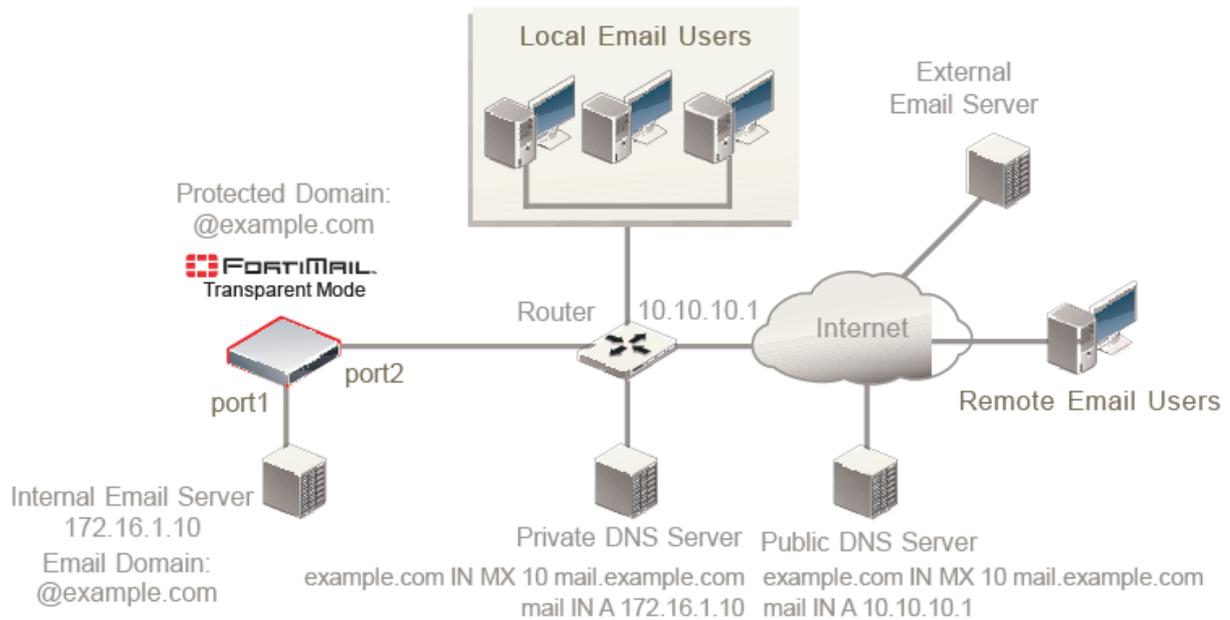


# Deploying FortiMail Transparent Mode



This recipe details how to run a FortiMail unit in transparent mode.

## Connecting to FortiMail from your PC

FortiMail port1's default IP address is 192.168.1.99. To access FortiMail's web UI, make sure your PC's IP address is on the same subnet as FortiMail, for example, 192.168.1.98. Access this URL from a web browser: <https://192.168.1.99/admin>. Remember to include /admin at the end of the URL.

At the login page, enter "admin" as the user name and no password by default.

Go to the dashboard and change the operation mode to transparent.

# Running the Quick Start Wizard

FortiMail web UI comes with a Quick Start Wizard to help you configure some basic network and mail settings for the first time.

To run the Quick Start Wizard, click the Quick Start Wizard button in the upright corner.

The screenshot displays the FortiMail 100C web interface. The top navigation bar includes 'Monitor', 'Status', 'Mail Statistics', 'Sessions', and 'Console'. A red arrow points to the 'Quick Start Wizard' button in the top right corner. The main content area is divided into several sections:

- System Information:** Shows serial number FE100C910000123, up time of 3 days 21 hours 39 minutes 41 seconds, and system time of Mon, 11 May 2015 08:29:32 PDT. It also lists the firmware version (v5.2.0u(0445.150506) (Interim)) and operation mode (Transparent).
- License Information:** Displays the license key 5.00152 (Expires 2020-01-04) and other license details.
- System Resource:** Shows resource usage: CPU usage (0%), Memory usage (29%), Log disk usage (1%), Mail disk usage (0%), and System load (8%).
- Statistics History:** A bar chart titled 'Email History by Day (Number Of Mails)' showing mail volume from May 1 to May 11. The legend indicates 'Access Control-Discard (42.12%)', 'Session Remote (57.87%)', and 'Others (0%)'.
- Statistics Summary:** A table providing a detailed breakdown of mail processing metrics over time.

Message direction: ALL	Total	This Year	This Month	This Week	Today	This Hour	This Minute
Delivery Control	12	12	0	0	0	0	0
Not Spam Classified By	26	26	18	0	0	0	0
Subtotal	38	38	18	0	0	0	0
Session Limits	0%	0%	0%	0%	0%	0%	0%
Session Remote	75	75	75	0	0	0	0
Access Control-Discard	1765468	1765468	1765468	736166	147280	0	0
Access Control-Relay Denied	1284978	1284978	1284978	368083	73640	0	0
Access Control-Relay Denial	1	1	1	0	0	0	0
SMTP Auth Failure	1	1	1	0	0	0	0
Subtotal	3050524	3050524	3050524	1104249	220920	0	0
Virus Infected	99.99%	99.99%	99.99%	100%	100%	0%	0%
Total	0	0	0	0	0	0	0
Total	3050562	3050562	3050542	1104249	220920	0	0

Follow the instructions to configure the settings.

## Configuring DNS Records

If the FortiMail unit is operating in transparent mode, in most cases, configuring [DNS](#) records for protected domain names is not required. Proper DNS records for your protected domain names are usually already in place.

However, you usually must configure public DNS records for the FortiMail unit itself, so that FortiMail can receive web connections, and send and receive email, for its own domain name. Dependent features include:

- delivery status notification (DSN) email
- spam reports
- email users' access to their per-recipient quarantined mail
- FortiMail administrators' access to the web UI by domain name
- alert email

- report generation notification email

### Transparent Mode Specific Settings

First, when configuring protected domains, enable the following options to hide the existence of the FortiMail unit:

- This server is on
- Hide the transparent box
- Use this domain's SMTAP server to deliver the mail
- Second, when configuring the [session](#) profile, optionally enable this feature:
- Hide this box from the mail server

**Note:** Unless you have enabled Take precedence over recipient based policy match in the IP-based policy, the Hide the transparent box option in the protected domain has precedence over this option, and may prevent it from applying to incoming email messages.

## Configuring Proxies

1. Navigate to **System > Network**.
2. Select port 1.
3. Select the **Edit** button.
4. Select the following from the SMTP Proxy section dropdown menu:
  - **Incoming connections:** Drop
  - **Outgoing connections:** Pass through
  - **Local connections:** Allow

FortiMail HTTPS, PING, SSH

### Edit Interface

Interface name: port1/Management IP (00:09:0f:d5:02:a4)

IP/Netmask:  /   
IPv6/Netmask:  /

Access  HTTPS  PING  HTTP  
 SSH  SNMP  TELNET

MTU  Override default MTU value (1500)  
 (bytes)

Administrative status  Up  Down

**SMTP Proxy**

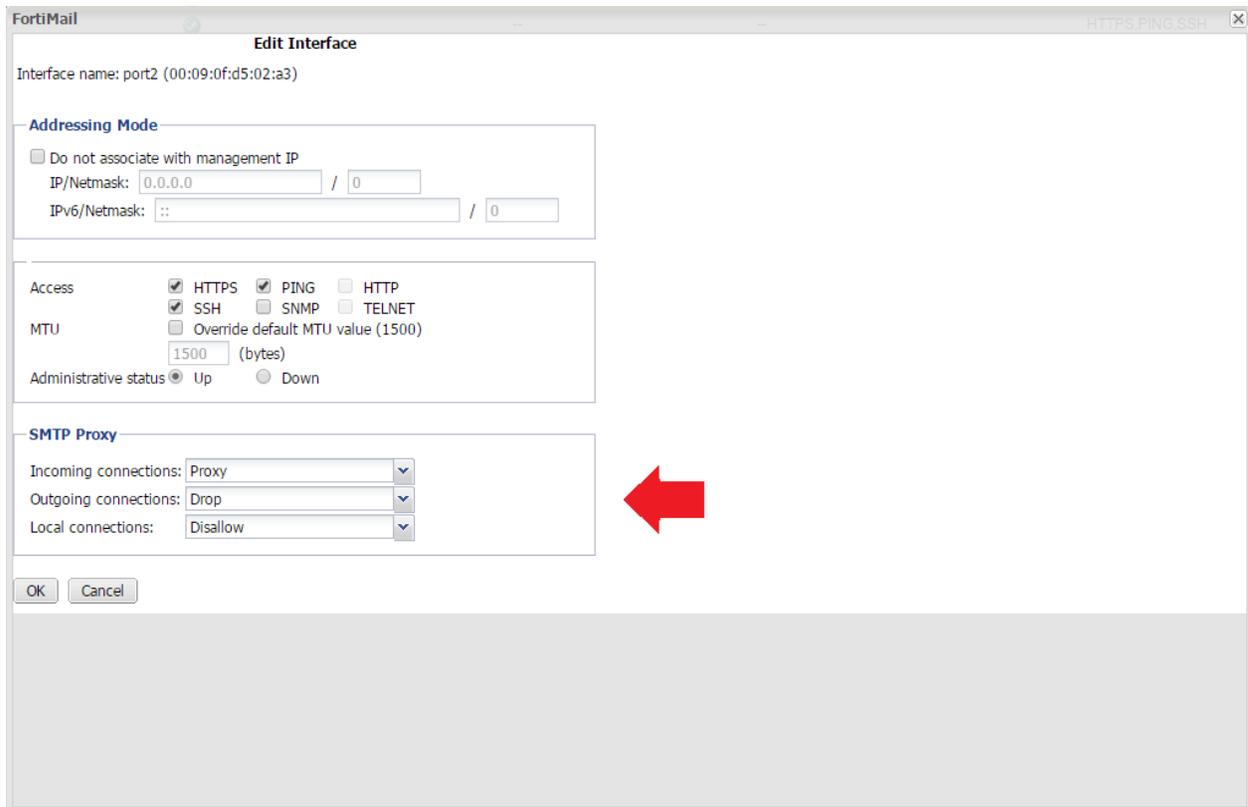
Incoming connections:  ▼

Outgoing connections:  ▼

Local connections:  ▼



5. Select **OK**.
6. Select port 2
7. Select the **Edit** button.
8. Select the following from the **SMTP Proxy** section dropdown menus:
  - **Incoming connections:** Proxy
  - **Outgoing connections:** Drop
  - **Local connections:** Disallow



9. Select **OK**.

## Testing the Installation

To test the installation, send an email message using the test paths illustrates in the diagram.

