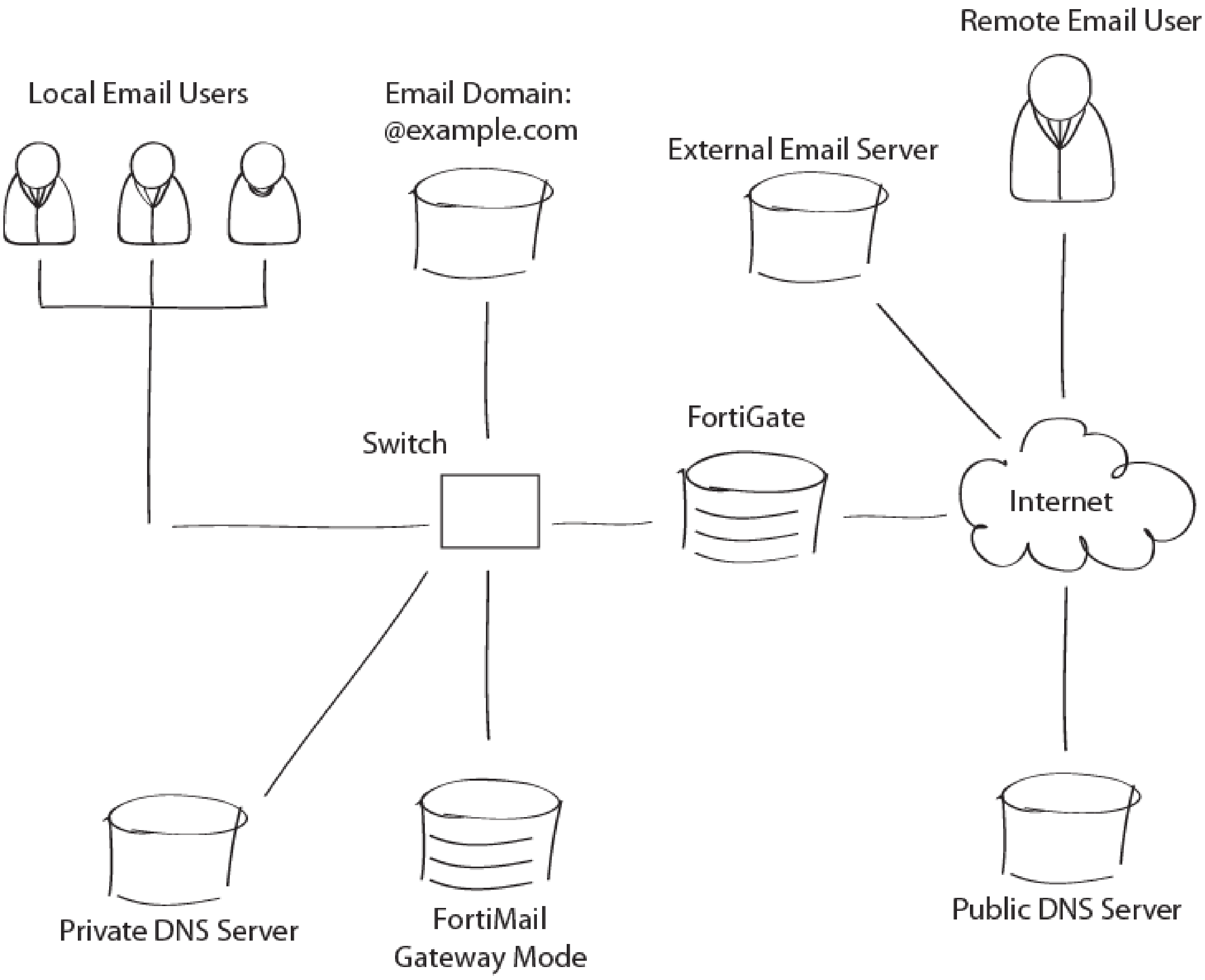
Deploying FortiMail Gateway Mode



This recipe focuses on how to deploy FortiMail gateway mode when positioned within a private network and behind a firewall.

The FortiMail unit, the protected email server, and the email users' computers are positioned within a private network behind a firewall. The FortiMail unit, however, is located in the demilitarized zone (DMZ) of the firewall, separated from the local email users and the protected email server, which are located on the internal network of the firewall.

Remote email users' computers and external email servers are located on the Internet, outside of the network protected by the firewall. The FortiMail unit protects accounts for email addresses ending in “@example.com”, which are hosted on the local email server.

Deploying FortiMail in gateway mode involves the following steps:

1. Connecting to FortiMail
2. Setting up FortiMail
3. Configuring DNS records
4. Configuring firewall policies
5. Configuring MUAs to use FortiMail
6. Testing the installation

Connecting to FortiMail

FortiMail port1’s default IP address is 192.168.1.99. To access FortiMail’s web UI, make sure you PC’s IP address is on the same subnet as FortiMail (192.168.1.98).

1. Go to 192.168.1.99/admin.
2. Enter “admin” as the user name and no password by default.
3. Select gateway mode from the **Operation Mode** dropdown menu.

Setting up FortiMail

Now that you’ve loaded the FortiMail web interface, you can now run the Quick Start Wizard.

The Quick Start Wizard helps you configure some of your basic network an email settings when you load the interface for the first time.

To run the Quick Start Wizard, simply select the Quick Start Wizard Button in the corner.

Follow the onscreen instructions to configure the settings.

Now that the Quick Start Wizard is finished, deploy the FortiMail server into your network.

Note: This setup uses the FortiMail default IP address; however, in most cases you will need to change the IP address to deploy the unit into your network.

Configuring DNS Records

Regardless of your private network topology, in order for external MTAs to deliver email to the FortiMail unit, you must configure the public MX record for each protected domain to indicate that the FortiMail unit is its email gateway.

Example: If the fully qualified domain name (FQDN) of the FortiMail unit is fortimail.example.com, and example.com is a protected domain, the MX record for example.com would be:

example.com IN MX 10 fortimail.example.com

An A record must also exist to resolve the host name of the FortiMail unit into an IP address.

FortiMail IN A 10.10.10.1

If your FortiMail unit will relay outgoing email, you should also configure the public reverse DNS record. The public IP address of the FortiMail unit, or the virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit, should be globally resolvable into the FortiMail unit’s FQDN. If it is not, reverse DNS lookups by external SMTP servers will fail.

Example: If the public network IP address of the FortiMail unit is 10.10.10.1, a public DNS server’s reverse DNS zone file for the 10.10.10.0/24 subnet might contain:

1 IN PTR fortimail.example.com.

where fortimail.example.com is the FQDN of the FortiMail unit.

Configuring Firewall Policies

No matter if you put FortiMail behind a firewall, such as a FortiGate unit, or in DMZ, you must configure a few firewall policies to allow the traffic.

For more information about how to create firewall policies, see your firewall documentation.

Configuring MUAs to use FortiMail

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the FortiMail IP address, 192.168.1.5; for remote email users, this is the virtual IP address on the wan1 network interface of the FortiGate unit that maps to the FortiMail unit, 10.10.10.1 or fortimail.example.com.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

Testing the Installation

To test the installation, send email messages by using the following test paths.

If you have problems with email delivery and receiving, check the following:

- Make sure the email clients use FortiMail as the incoming and outgoing email server.
- Make sure FortiMail can access the DNS servers.
- Make sure the Firewall policies allow SMTP traffic.

If you still have problems, please contact Fortinet Technical Support.