FORTINET

SIMPLE, SCALABLE, SECURE EMAIL WITH OFFICE 365 AND FORTIMAIL

DEPLOYMENT GUIDE

MOVING TO THE CLOUD DOESN'T NEED TO BE SCARY

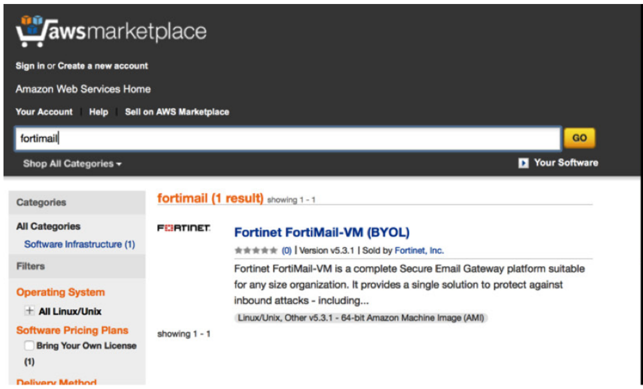
Enterprises and businesses world over are taking a good look at the cloud and cloud services such as Microsoft Office 365 email. Extremely capable of providing an edge over the competition, the cloud helps organizations scale, in a fast and simple manner, while simultaneously bringing down costs. While it does have these wonderful advantages, the primary concern for these organizations during this transition is security. Servers and intellectual property, the lifeblood of the organization, are no longer under lock and key in a building somewhere, but hosted in the cloud.

With Fortinet's slew of virtual appliances, the cloud need not be scary anymore. While FortiGate and FortiWeb can be used to protect the cloud deployment and web resources, respectively, FortiMail is able to protect email, which is the most important productivity tool for any organization.

As more and more organizations move from traditional Microsoft Exchange servers to Office 365 email services, they can completely rely on FortiMail to protect this attack surface. FortiMail has been validated by third-party testing houses such as Virus Bulletin, which has given it the coveted VBSpam+ rating.

Moreover, deploying FortiMail Office 365 email integration is very easy and provides great flexibility in terms of options.

SO WHAT ARE MY OPTIONS?



fortimail

fortimail (1 result) showing 1 - 1

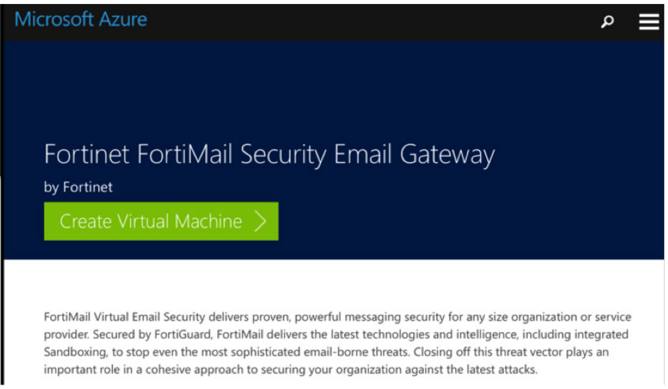
Fortinet FortiMail-VM (BYOL)

★★★★★ (0) | Version v5.3.1 | Sold by Fortinet, Inc.

Fortinet FortiMail-VM is a complete Secure Email Gateway platform suitable for any size organization. It provides a single solution to protect against inbound attacks - including...

Linux/Unix, Other v5.3.1 - 64-bit Amazon Machine Image (AMI)

showing 1 - 1



Fortinet FortiMail Security Email Gateway

by Fortinet

FortiMail Virtual Email Security delivers proven, powerful messaging security for any size organization or service provider. Secured by FortiGuard, FortiMail delivers the latest technologies and intelligence, including integrated Sandboxing, to stop even the most sophisticated email-borne threats. Closing off this threat vector plays an important role in a cohesive approach to securing your organization against the latest attacks.

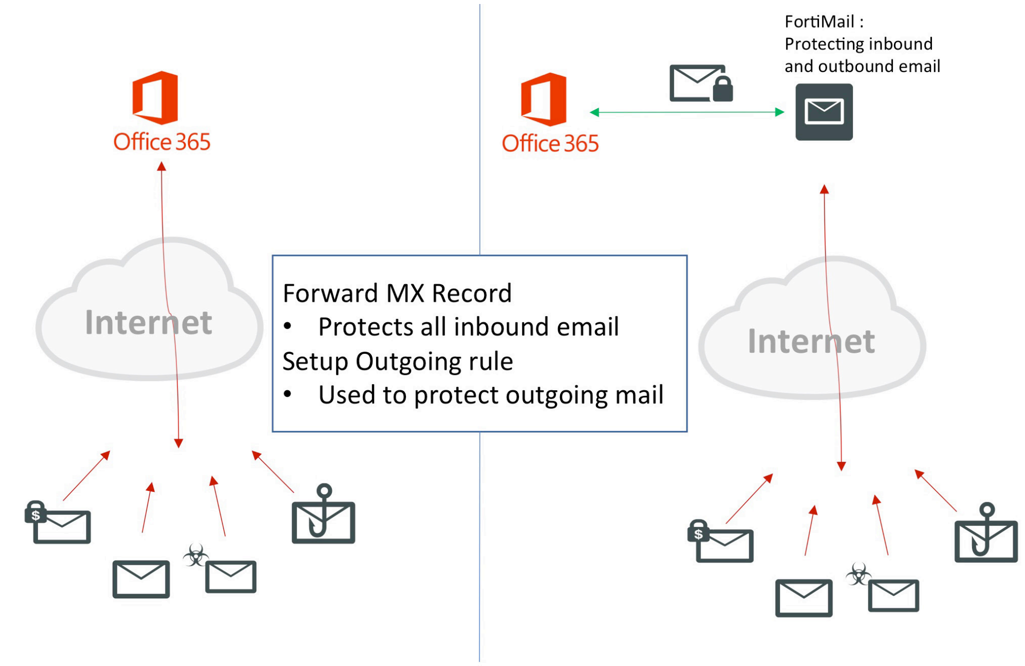
FortiMail allows for a very flexible set of options.

- FortiMail is available as hardware appliances and virtual appliances for the private data center. Both of these can be used for deployments where it is preferred to use the private data center as the hub to secure your deployment.
- Available as a VM in both Amazon Web Services and Microsoft Azure, FortiMail provides flexible sizing options to protect Office 365 email in a scalable fashion. It also has the added advantage of being at a co-located data center.
- For organizations that like the simplicity of Software-as-a-Service (SaaS) applications, they also have the option of using FortiMail Cloud, Fortinet's Cloud-Hosted Email Security offering.

HOW DOES IT WORK?

In order to protect your Office 365 deployment using FortiMail's Enterprise Class Security, it is important to have FortiMail act as a gateway to your Office 365 deployment. By doing this, you are able to ensure that any email threats attempting to get to your organization will always need to be inspected by FortiMail to ensure it does not carry any threats.

The deployment looks as follows:



We will now look at how to protect your Office 365 deployment using FortiMail running in Microsoft Azure.

It is important to note that while this is the method used in this document, it can just as easily be carried out using FortiMail running in a private data center or using FortiMail Cloud.

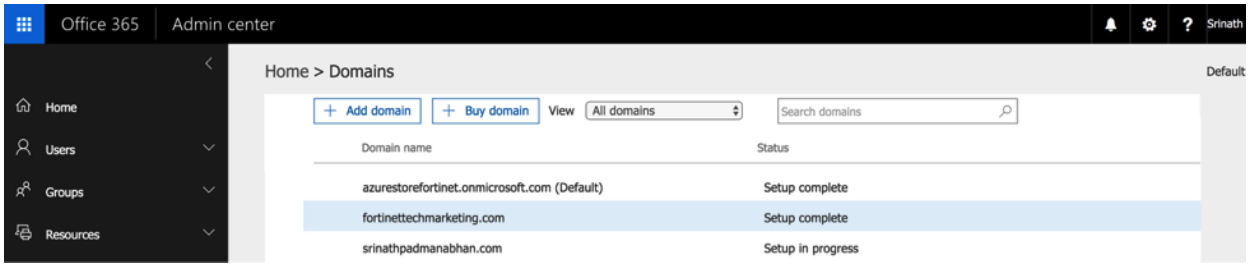
Preparing Office 365—For the scope of this discussion, we assume that the domain has already been added onto Office 365 and we have an existing Office 365 email deployment. There are URLs to additional documents at the end of this guide, which go into deeper detail about how to deploy Office 365 email from scratch.

Checking your domains:

1. Log onto Office 365 Admin center.
2. Click on Domains.
3. Check that your domain has already been added and is completely set up.

If the setup has been correctly executed, you will see the screen shown below with your domain available and showing as Setup complete.

If necessary, you can also set up your domain by clicking on Add domains and following the wizard.

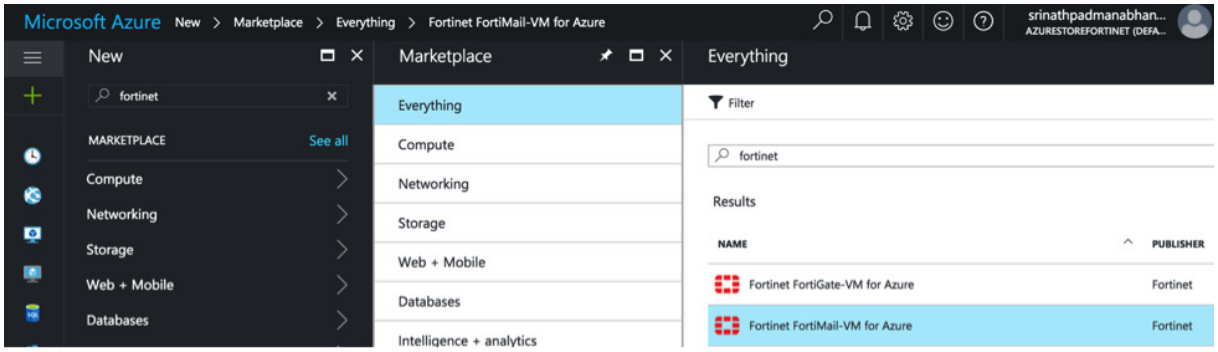


Home > Domains

Domain name	Status
azurestorefortinet.onmicrosoft.com (Default)	Setup complete
fortinettechmarketing.com	Setup complete
srinathpadmanabhan.com	Setup in progress

Deploying FortiMail—The first thing that needs to be done to bring up the integration is to configure FortiMail to accept Office 365 email. This allows FortiMail to perform the necessary inspections on any inbound Office 365 email.

We will first do a quick walkthrough of FortiMail on Microsoft Azure. Deploying Azure on FortiMail is very easy and can be carried out in a few quick steps.


Microsoft Azure New > Marketplace > Everything > Fortinet FortiMail-VM for Azure

srinathpadmanabhan...
AZURESTOREFORTINET (DEFA...

New

fortinet

MARKETPLACE See all

Compute
Networking
Storage
Web + Mobile
Databases

Marketplace

Everything
Compute
Networking
Storage
Web + Mobile
Databases
Intelligence + analytics

Everything

Filter

fortinet

Results

NAME	PUBLISHER
Fortinet FortiGate-VM for Azure	Fortinet
Fortinet FortiMail-VM for Azure	Fortinet

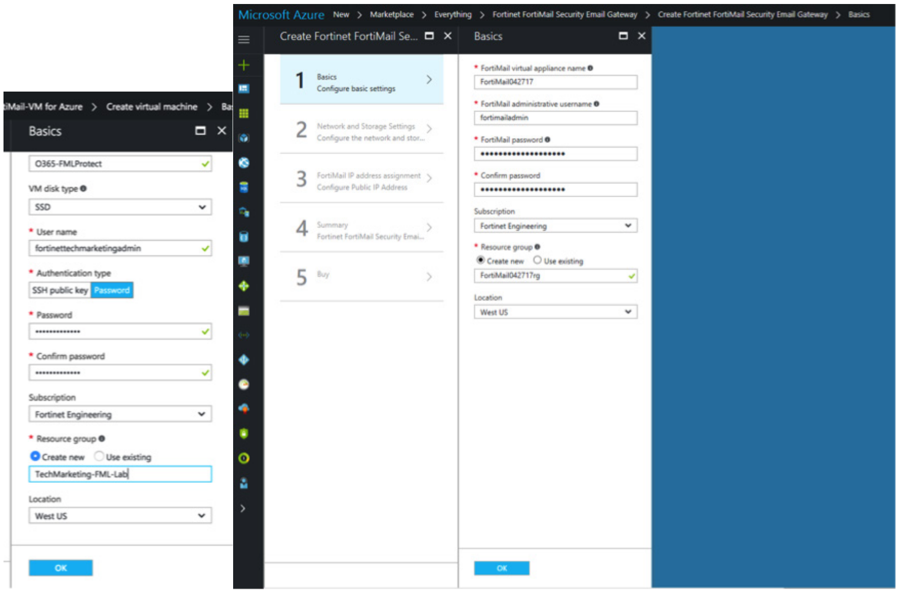
Once logged into Azure, it is very simple to deploy a FortiMail-VM. All one needs to do is go to the marketplace and search for Fortinet to find all the Fortinet Virtual Machines.

Select the FortiMail-VM for Azure and continue.

A few settings would be required, including the VM name, passwords, and the resource group this VM belongs to.

This will be followed by selecting the instance sizes for FortiMail-VM on Azure. There is a wide array of instance sizes supported for Azure, and it is important to keep in mind the number of users and expected email traffic to ensure the VM is of the correct size and capacity to support this deployment.

Please refer to your Deployment Guide or contact your Fortinet Representative to better understand your VM sizing.


iMail-VM for Azure > Create virtual machine > Ba

Basics

O365-FMLProtect

VM disk type
SSD

* User name
fortinettechmarketingadmin

* Authentication type
SSH public key | Password

* Password
••••••••••••••

* Confirm password
••••••••••••••

Subscription
Fortinet Engineering

* Resource group
● Create new ○ Use existing
TechMarketing-FML-Lab

Location
West US

OK

Microsoft Azure New > Marketplace > Everything > Fortinet FortiMail Security Email Gateway > Create Fortinet FortiMail Security Email Gateway > Basics

Create Fortinet FortiMail Se...

1 Basics
Configure basic settings

2 Network and Storage Settings
Configure the network and stor...

3 FortiMail IP address assignment
Configure Public IP Address

4 Summary
Fortinet FortiMail Security Emai...

5 Buy

Basics

* FortiMail virtual appliance name
FortiMail042717

* FortiMail administrative username
fortimailadmin

* FortiMail password
•••••••••••••••••••

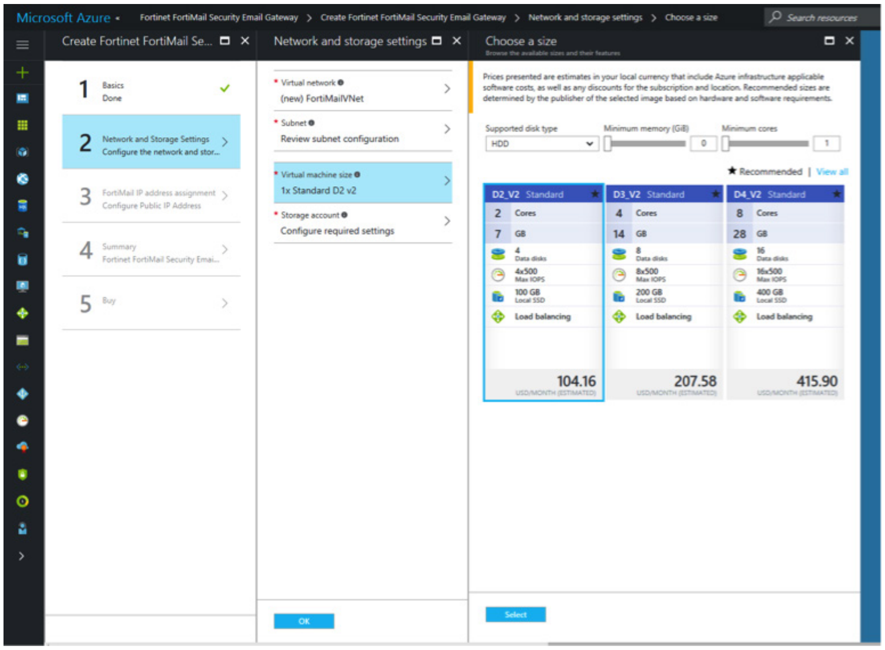
* Confirm password
•••••••••••••••••••

Subscription
Fortinet Engineering

* Resource group
● Create new ○ Use existing
FortiMail042717rg

Location
West US

OK



Microsoft Azure > Fortinet FortiMail Security Email Gateway > Create Fortinet FortiMail Security Email Gateway > Network and storage settings > Choose a size

Create Fortinet FortiMail Se...

1 Basics
Done ✓

2 Network and Storage Settings
Configure the network and stor...

3 FortiMail IP address assignment
Configure Public IP Address

4 Summary
Fortinet FortiMail Security Emai...

5 Buy

Network and storage settings

* Virtual network: (new) FortiMailVNet

* Subnet: Review subnet configuration

* Virtual machine size: 1x Standard D2 v2

* Storage account: Configure required settings

OK

Choose a size
Browse the available sizes and their features

Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

Supported disk type: HDD
Minimum memory (GiB): 0
Minimum cores: 1

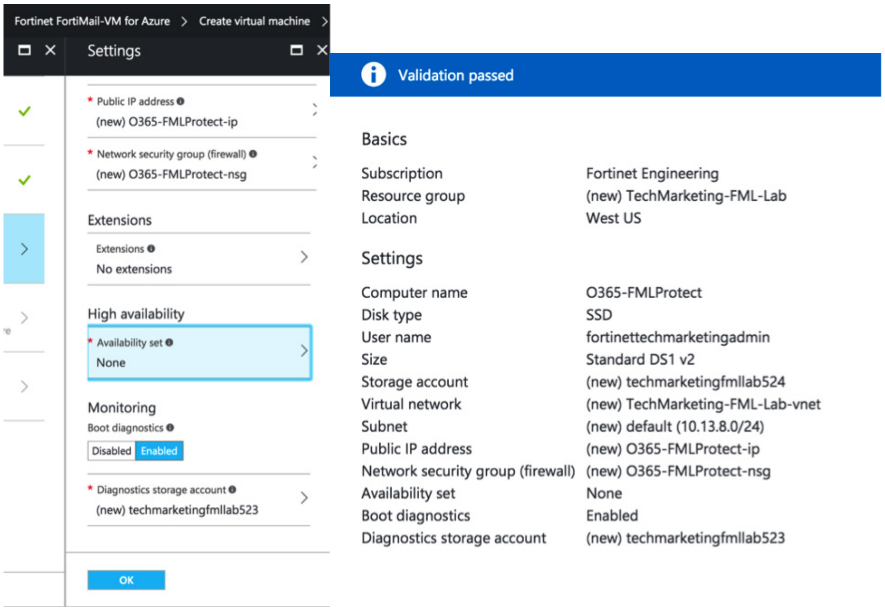
★ Recommended | View all

D2_V2 Standard ★	D3_V2 Standard ★	D4_V2 Standard ★
2 Cores	4 Cores	8 Cores
7 GB	14 GB	28 GB
4 Data disks	8 Data disks	16 Data disks
4x500 Max IOPS	8x500 Max IOPS	16x500 Max IOPS
100 GB Local SSD	200 GB Local SSD	400 GB Local SSD
Load balancing	Load balancing	Load balancing
104.16 USD/MONTH (ESTIMATED)	207.58 USD/MONTH (ESTIMATED)	415.90 USD/MONTH (ESTIMATED)

Select

Configuring the VM and Selecting the Size

Other key information to be provided includes IP address and storage information.



Fortinet FortiMail-VM for Azure > Create virtual machine >

Settings

* Public IP address: (new) O365-FMLProtect-ip

* Network security group (firewall): (new) O365-FMLProtect-nsg

Extensions
Extensions: No extensions

High availability
* Availability set: None

Monitoring
Boot diagnostics: Disabled [✓ Enabled]

* Diagnostics storage account: (new) techmarketingfmllab523

OK

Validation passed

Basics

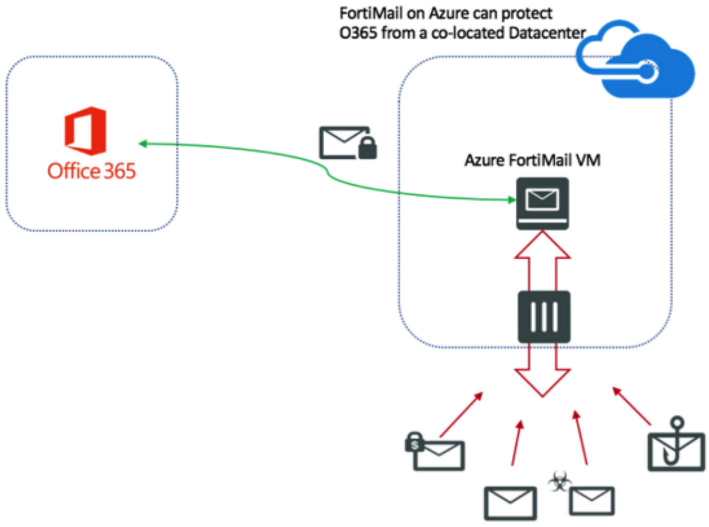
Subscription	Fortinet Engineering
Resource group	(new) TechMarketing-FML-Lab
Location	West US

Settings

Computer name	O365-FMLProtect
Disk type	SSD
User name	fortinettechmarketingadmin
Size	Standard DS1 v2
Storage account	(new) techmarketingfmllab524
Virtual network	(new) TechMarketing-FML-Lab-vnet
Subnet	(new) default (10.13.8.0/24)
Public IP address	(new) O365-FMLProtect-ip
Network security group (firewall)	(new) O365-FMLProtect-nsg
Availability set	None
Boot diagnostics	Enabled
Diagnostics storage account	(new) techmarketingfmllab523

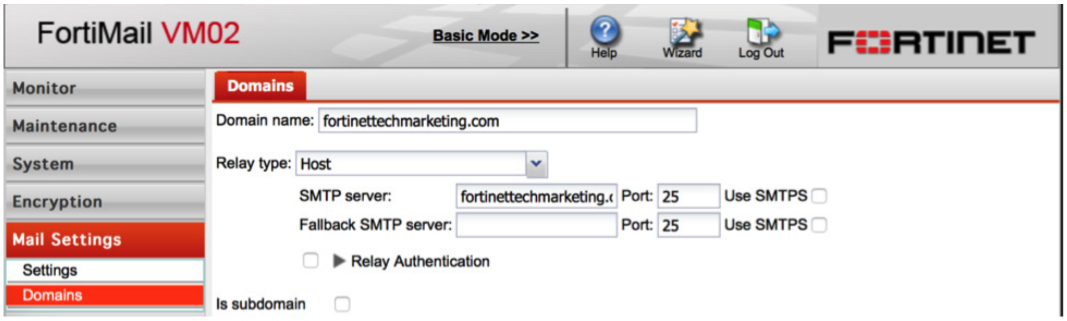
Configuring IP and Validation

With this, your FortiMail-VM should be ready. By selecting the deployment location, it is possible to select a co-located data center to ensure minimum latency and performance impact on integrating the FortiMail-VM.


FortiMail on Azure can protect
O365 from a co-located Datacenter
Office 365
Azure FortiMail VM

PROTECTING OFFICE 365 USING A FORTIMAIL-VM RUNNING ON AZURE

Configuring FortiMail—The first step in bringing up the integration is to prep FortiMail to receive Office 365 mail. To do this, log into FortiMail and add a new domain for the Office 365 account. This includes your domain name, which needs to be protected, and the SMTP server's details.



Domain name: fortinettechmarketing.com

Relay type: Host

SMTP server: fortinettechmarketing.c Port: 25 Use SMTPS □

Fallback SMTP server: Port: 25 Use SMTPS □

□ ▶ Relay Authentication

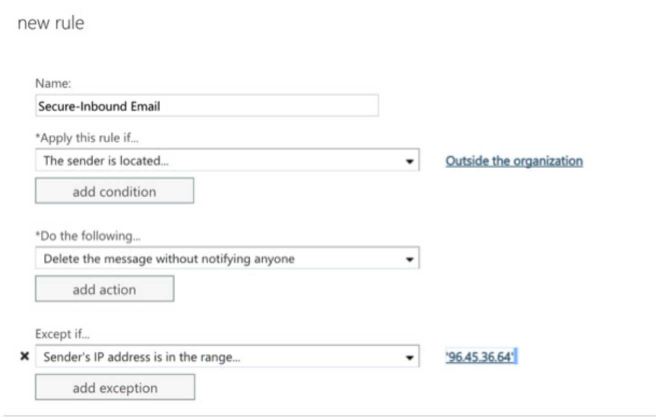
Is subdomain □

Configuring Office 365; Protecting Inbound Email—The next step is to configure the Office 365 console to accept FortiMail.

To do this, create a rule under Admin center to accept email coming in from FortiMail. This will allow FortiMail email to be accepted in Office 365.

To do this, under Admin center > Exchange >

Select Mail Flow > Rules > +



new rule

Name:
Secure-Inbound Email

*Apply this rule if...
The sender is located... — Outside the organization

add condition

*Do the following...
Delete the message without notifying anyone

add action

Except if...
✖ Sender's IP address is in the range... — '96.45.36.64'

add exception

Doing this lets Office 365 know that only accepted email needs to be coming in from FortiMail. Any other inbound email is erroneous and should be deleted, as it could be a threat. Select Enforce this policy to ensure it takes effect.

Configuring Office 365—Set up Office 365 to relay email.

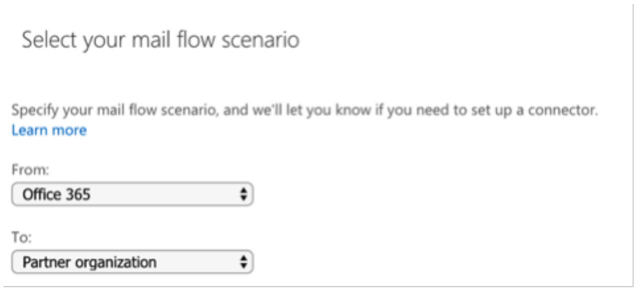
Now we are ready to receive email. As for outgoing email,

Under Mail Flow > Connectors

Select +

This sets up a rule to ensure that any outgoing email within this organization can be inspected using FortiMail.

To do this, follow the steps below.

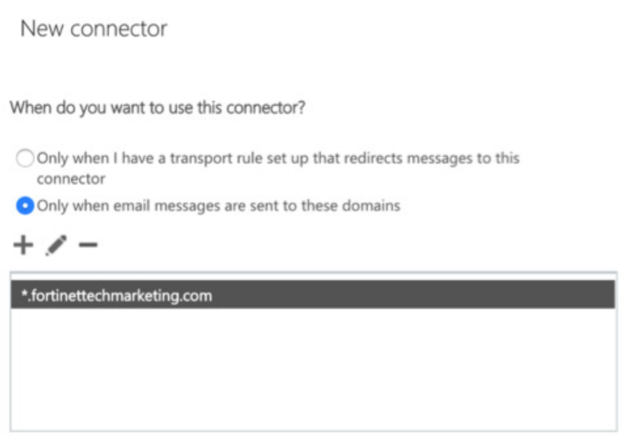


Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
Learn more

From:
Office 365

To:
Partner organization



New connector

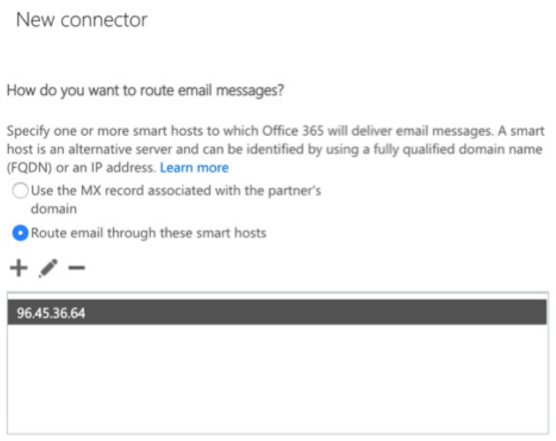
When do you want to use this connector?

○ Only when I have a transport rule set up that redirects messages to this connector

● Only when email messages are sent to these domains

+ ✎ −

*.fortinettechmarketing.com



New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. Learn more

○ Use the MX record associated with the partner's domain

● Route email through these smart hosts

+ ✎ −

96.45.36.64

Once this is validated, Office 365 is ready to send your email to FortiMail when it is destined for your organization.

Managing MX Records—Configure your DNS server.

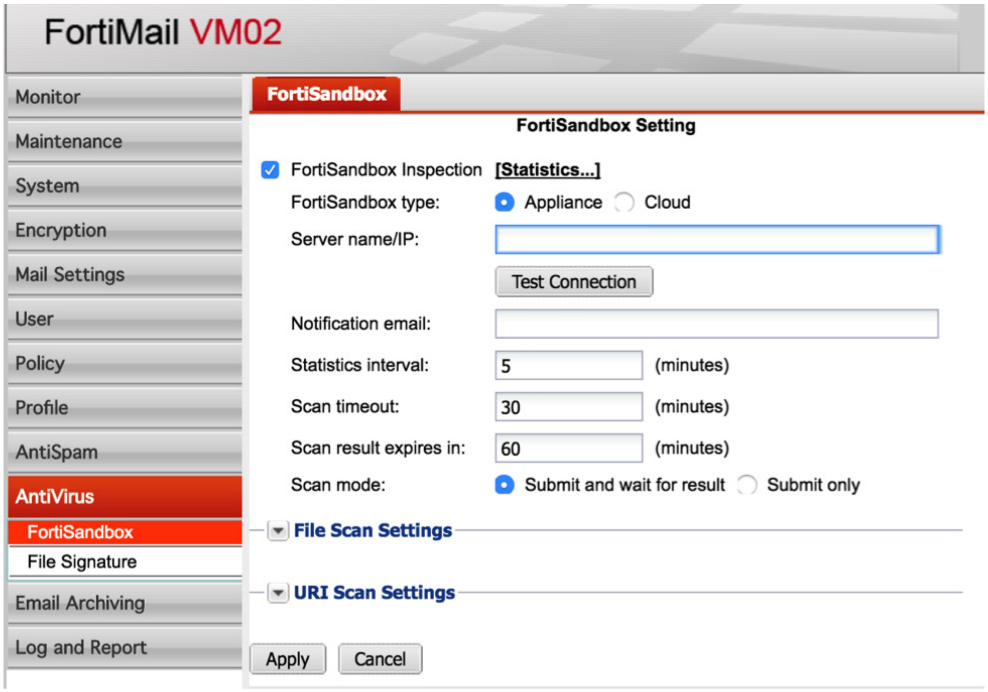
The final step to prepare your entire setup and have mail forwarded as needed involves setting up the MX record so that it points to FortiMail.

By default when set up, the MX record would have been programmed such that it redirects any MX records to your Exchange server. At present, any such incoming mail will be dropped as per our configuration. So we should configure the DNS server to redirect the MX record across to FortiMail Instead. FortiMail will then inspect any incoming email before sending it across to the Office 365 instance.

And voila, you have a fully protected Office 365 email deployment.

THAT'S AWESOME, BUT WHY FORTINET?

When it comes to security, Fortinet is an industry leader. Using intelligence from the respected and renowned FortiGuard Labs, FortiMail is able to protect Office 365 from all kinds of threats. FortiMail is regularly one of the most successful participants in Virus Bulletin's Anti-Spam Testing, receiving the coveted VB Verified Spam+ rating.



FortiSandbox Setting

☑ FortiSandbox Inspection [Statistics...]

FortiSandbox type: ● Appliance ○ Cloud

Server name/IP:

Notification email:

Statistics interval: 5 (minutes)

Scan timeout: 30 (minutes)

Scan result expires in: 60 (minutes)

Scan mode: ● Submit and wait for result ○ Submit only

Beyond this, by means of FortiSandbox integration, FortiMail is able to protect against the latest threats, including zero-day vulnerabilities. This is essential in this day and age when a majority of organizations are hit by threats and malware unique to that organization.

This integration can be carried out with either a dedicated FortiSandbox Appliance or using the FortiSandbox Cloud offering, both of which received "Recommended" ratings in NSS Labs' 2016 BDS Testing.

SUMMARY

When it comes to simplicity and scale, Office 365 is a great offering. With FortiMail's best-in-class protection, your Office 365 email deployment and your organization as a whole can be secure. So while email has always been one of the most popular attack vectors, protecting against email attacks has never been easier using FortiMail protection for Office 365.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

June 23, 2017 9:47 AM