



FortiMail Email Protection - Step by Step Guide

Jhonattan Ferreras

System Engineer

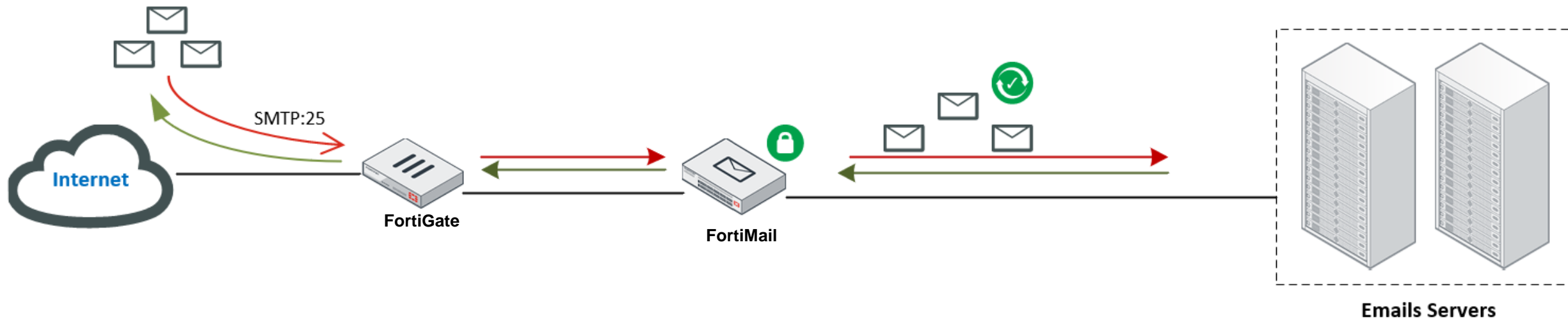
Objective

- ✓ Design
- ✓ Notes
- ✓ 4 Inbound Step by Step Guide
- ✓ 4 Outbound Step by Step Guide
- ✓ Logs Verifications

Design

Design

Note: This guide provide you how to implement a FortiMail as a Gateway Mode to protect all your inbound and outbound email traffic.



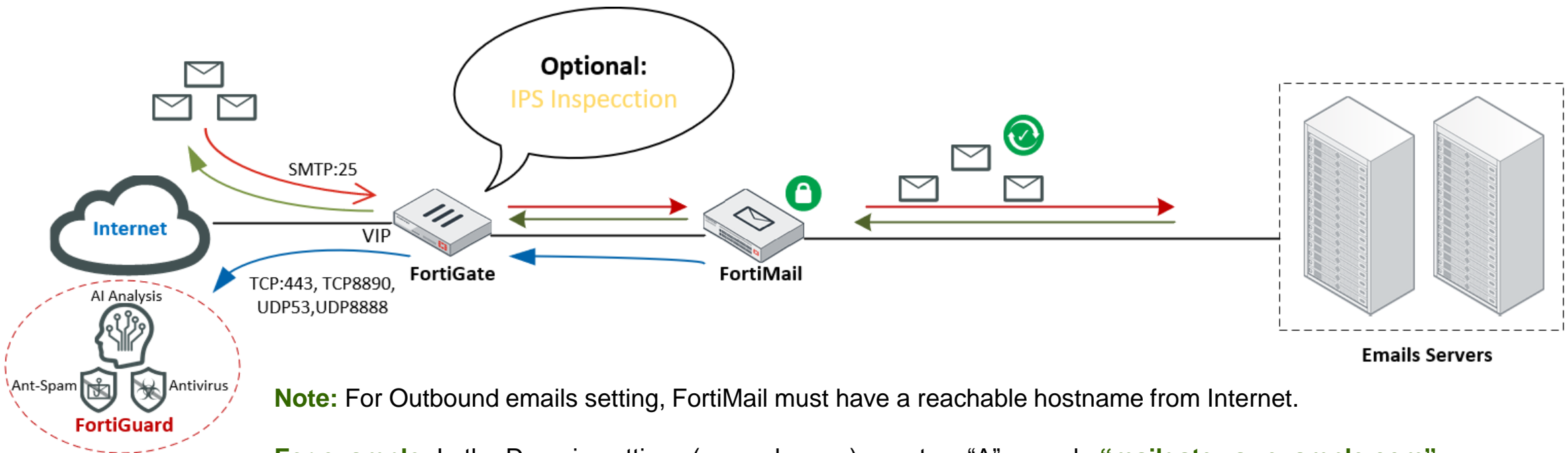
FortiMail unit receives email for defined email domains and control relay of email to other domains. Email passing through the FortiMail unit can be scanned for viruses and spam.

Policies and profiles govern how the FortiMail unit scans email and what it does with email messages containing viruses or spam. On the next slides you will see how configure policies and how to assign profiles.

Notes

Smart thing to consider before start!

1. Keep in mind, if you have a FortiGate or a third-party firewall, the SMTP traffic (port:25) must be route to the FortiMail.
 - **Optional:** For more security features you can inspect the traffic applying an IPS profile (based on Protect Email Server).
2. You must allow access to FortiMail to send emails via SMTP port (25) and access to FortiGuard to validate Licensing, AI analysis and DB updates.
 - **FortiGuard Ports:** TCP443, TCP8890, UDP53, UDP8888



Note: For Outbound emails setting, FortiMail must have a reachable hostname from Internet.

For example: In the Domain settings (example.com), create a "A" record: **"mailgateway.example.com"**

Inbound - Step by Step

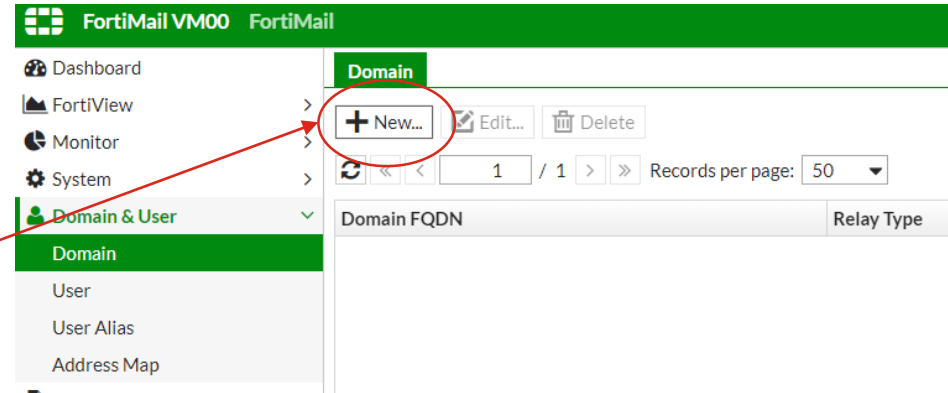
Step #1

Protected Domains

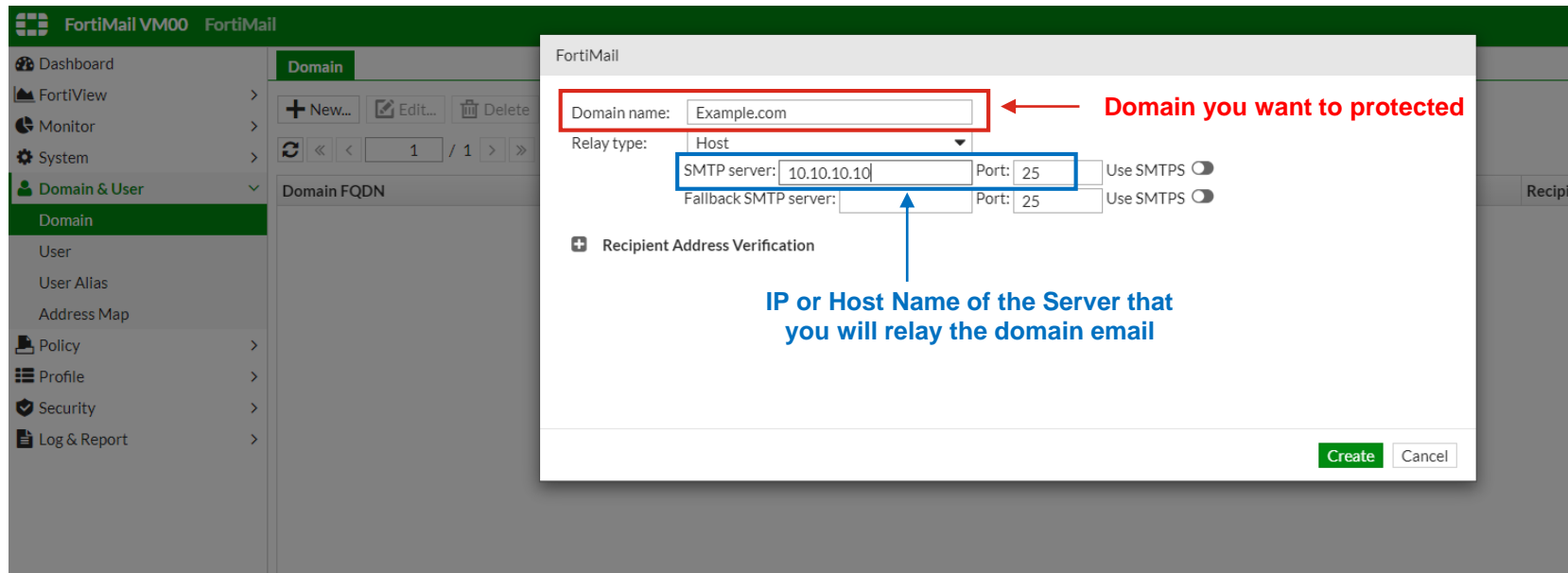
Protected Domains are the domains which are protected by FortiMail, once you configure the protected domain, FortiMail allows you to apply all security features associated with that domain.

Protected Domains

1. Navigate through Domain & User → Domain:



2. Once you click on +New, a new box show up, where you will put the required information



Step #2

Recipients Policy - Inbound

There are two types of recipient-based policies: inbound and outbound. The FortiMail unit applies inbound policies to the incoming mail messages and outbound policies to the outgoing mail messages, associated with the protected domain configured.

Recipients Policy - Inbound

1. Navigate through Policy → Recipient Policy: Here you can edit the default policy or create a new one, your choice!

The screenshot shows the FortiMail VM00 interface. On the left is a navigation menu with options: Dashboard, FortiView, Monitor, System, Domain & User, Policy (selected), Access Control, IP Policy, and Recipient Policy. The main area is titled 'Inbound' and 'Outbound'. Below this is a table of policies. The table has columns: Enable..., ID..., Recipient Pattern, AntiSpam, AntiVirus, Content, and Resource. The first row shows a policy with ID 1, Recipient Pattern '*@*', AntiSpam 'AS_Inbound', AntiVirus 'AV_SysQuarantine', Content 'CF_Inbound', and Resource 'Res_Default'. Below the table is a form for 'Inbound Recipient Policy' with fields for Enable (checked), Domain (system), and Comments. Below the form is a 'Recipient Pattern' section with a 'Type' dropdown set to 'User' and a text field containing '* @ example.com'. Below this is a 'Profiles' section with four rows: AntiSpam (AS_Inbound), AntiVirus (AV_SysQuarantine), Content (CF_Inbound), and Resource (Res_Default). Each row has '+ New...' and 'Edit...' buttons. At the bottom is an 'Authentication and Access' section.

Enable...	ID ...	Recipient Pattern	AntiSpam	AntiVirus	Content	Resource
<input checked="" type="checkbox"/>	1	*@*	AS_Inbound	AV_SysQuarantine	CF_Inbound	Res_Default

2. On the next box that will show up, if you create or edit a policy, you must specify the protected domain on the recipient pattern field.

For example:

Edit [***** **@** *****] for [***** **@** example.com]

The screenshot shows the 'Inbound Recipient Policy' configuration form. It has fields for 'Enable' (checked), 'Domain' (system), and 'Comments'. Below these is the 'Recipient Pattern' section with a 'Type' dropdown set to 'User' and a text field containing '* @ example.com'. Below this is the 'Profiles' section with four rows: AntiSpam (AS_Inbound), AntiVirus (AV_SysQuarantine), Content (CF_Inbound), and Resource (Res_Default). Each row has '+ New...' and 'Edit...' buttons. At the bottom is an 'Authentication and Access' section. Red arrows point from the text 'For example: Edit [* @ *] for [* @ example.com]' to the 'Recipient Pattern' field and the 'Profiles' section. A red arrow points from the text '1. Here you can see all security profiles assigned by default.' to the 'Profiles' section. Another red arrow points from the text '2. You can edit or assigned new profiles and customize them as you want.' to the 'Edit...' button for the 'AntiSpam' profile.

1. Here you can see all security profiles assigned by default.
2. You can edit or assigned new profiles and customize them as you want.

Step #3

IP Policy

The IP Policies section of the Policies tab lets you create policies that apply profiles to inspect SMTP connections based on the IP addresses of SMTP clients and/or servers with the help of FortiGuard.

IP Policy

1. This is a default IP policy, allows to inspect all IP connection by default. Do not make any change here at least you want to specify the source IP from where all incoming emails will be received.

FortiMail VM00 FortiMail

Dashboard
FortiView
Monitor
System
Domain & User
Policy
Access Control
IP Policy
Recipient Policy

IP Policy

+ New... Clone... Edit... Delete Move

1 / 1 Records per page: 50 Search:

Enable...	ID...	Source	Session
<input checked="" type="checkbox"/>	1	0.0.0.0/0	Inbound Session
<input checked="" type="checkbox"/>	2	::/0	Inbound Session

1. Here you can see a security profiles assigned by default in the IPv4 and IPv6 policy.
2. You can edit or assign a new session profile and customize them as you want.

Step #4

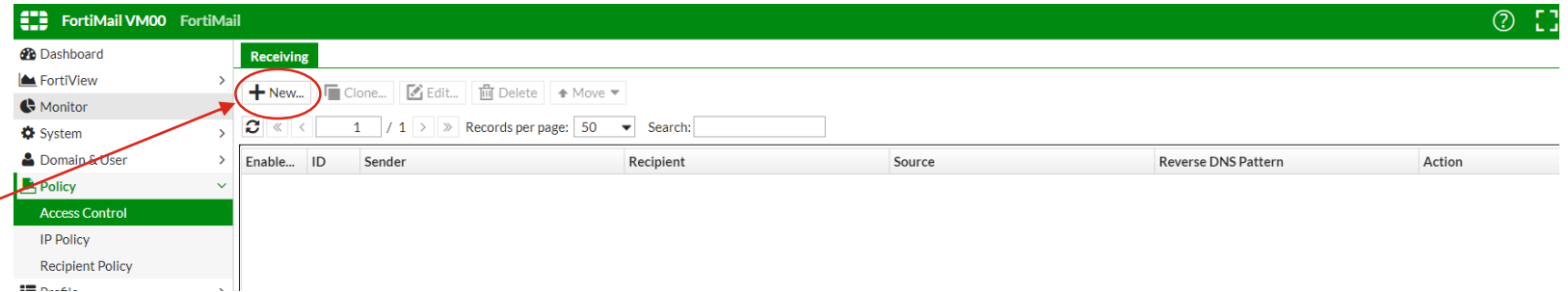
Access Control Policy - Inbound

Access Control Policy by default just shows you a receiving tab and here do not display any rules that apply to SMTP sessions being received by the FortiMail unit.

Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages for SMTP sessions that are initiated by SMTP clients.

Access Control Policy

1. By default the receiving tab, do not display any rules, so here we are going to create a new ACL for allow any sender can send email to the protected domain.

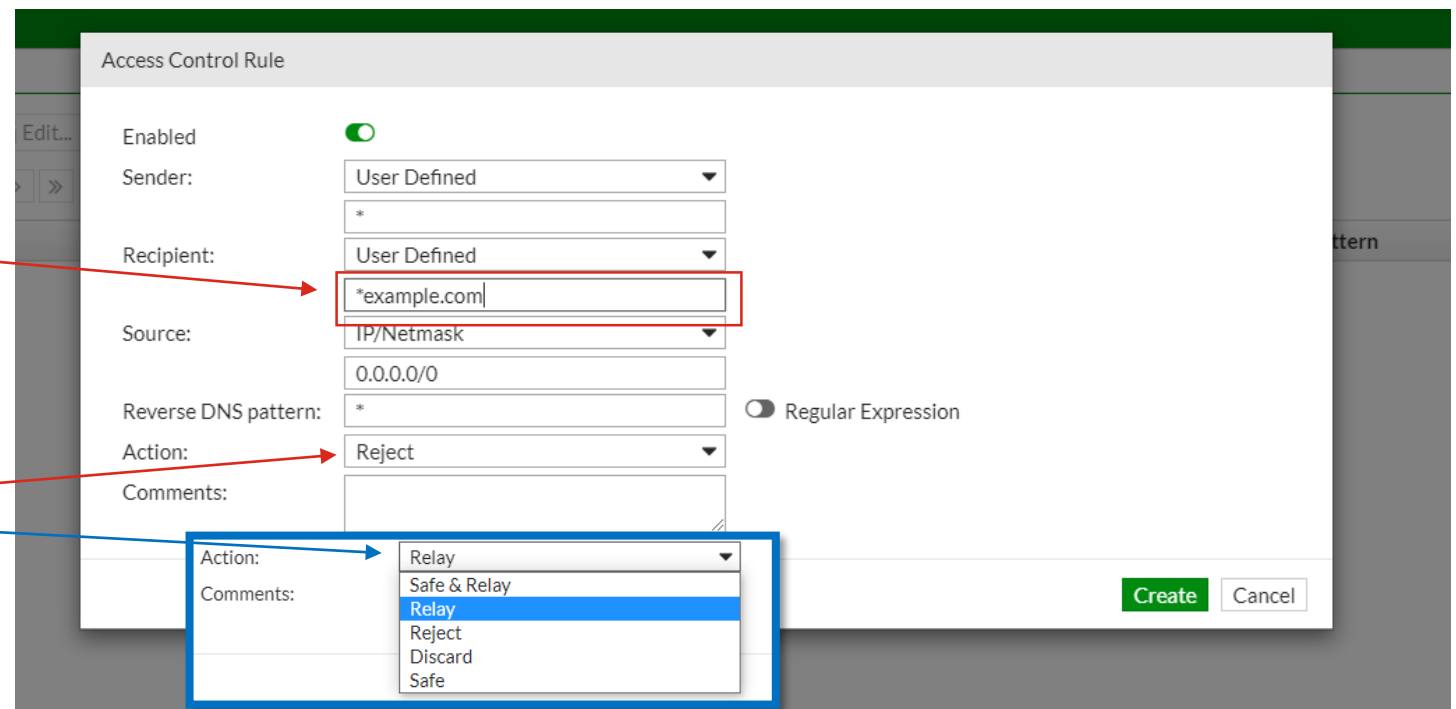


2. Click on +New: a new box show up, is recommended put the protected domain on the recipient field.

3. Then change the Action:

For example:

Change "Reject" to "Relay"



Outbound - Step by Step

Step #1

Mail Setting

Mail setting option allow you to configure the hostname of the FortiMail unit with a local domain name.

Mail Setting

1. Navigate through System → Mail Setting:
2. In the Host name field, put the desired hostname for the FortiMail unit.
3. In the Local domain name field, put the local domain that you will use it to reach the FortiMail from internet.

FortiMail VM00 FortiMail

Mail Server Setting Disclaimer Disclaimer Exclusion List

Local Host

Host name: Mailgateway

Local domain name: example.com

SMTP server port number: 25

SMTP over SSL/TLS: ☒

SMTPS server port number: 465

SMTP MSA service: ☐

SMTP MSA port number: 587

POP3 server port number: 110

Default domain for authentication: --None--

Apply Cancel

Note: For Outbound emails setting, FortiMail must have a reachable hostname from Internet.

For example: In the Domain settings (example.com), create a “A” record: **“mailgateway.example.com”**

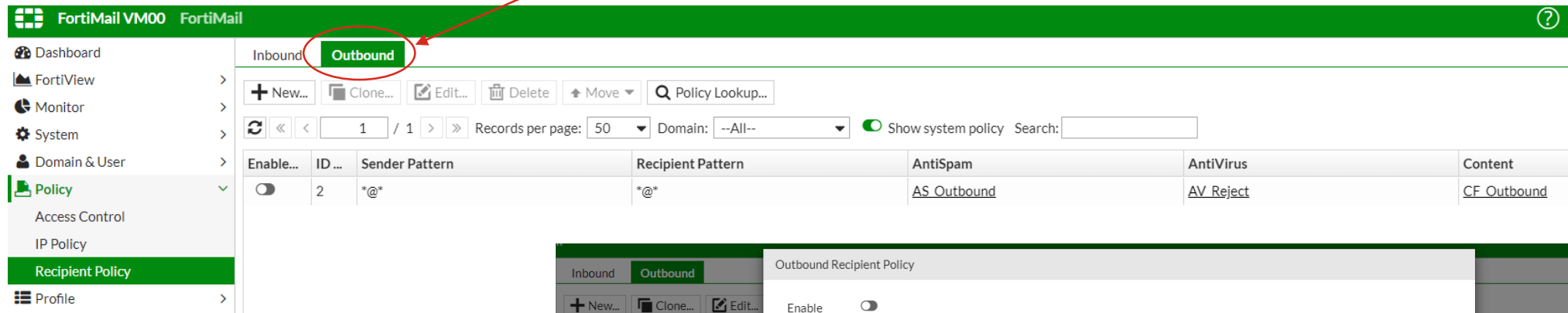
Step #2

Recipients Policy - Outbound

There are two types of recipient-based policies: inbound and outbound. The FortiMail unit applies inbound policies to the incoming mail messages and outbound policies to the outgoing mail messages, associated with the protected domain configured.

Recipients Policy - Inbound

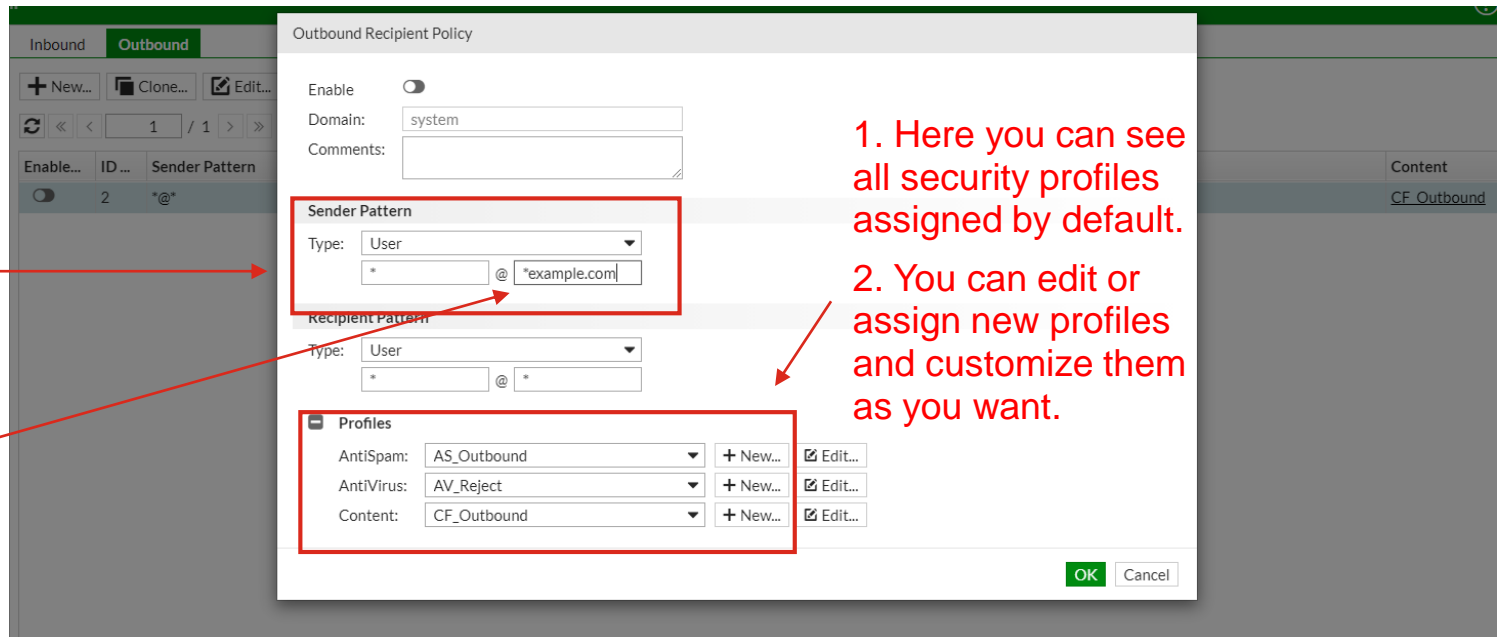
1. Navigate through Policy → Recipient Policy → Outbound Tab: Here you can edit the default policy or create a new one, your choice!.



2. A new box show up, when you create or edit a policy, you must specify the protected domain, now on the sender pattern field.

For example:

Edit [***** @ *****] for [***** @ example.com]



1. Here you can see all security profiles assigned by default.

2. You can edit or assign new profiles and customize them as you want.

Step #3

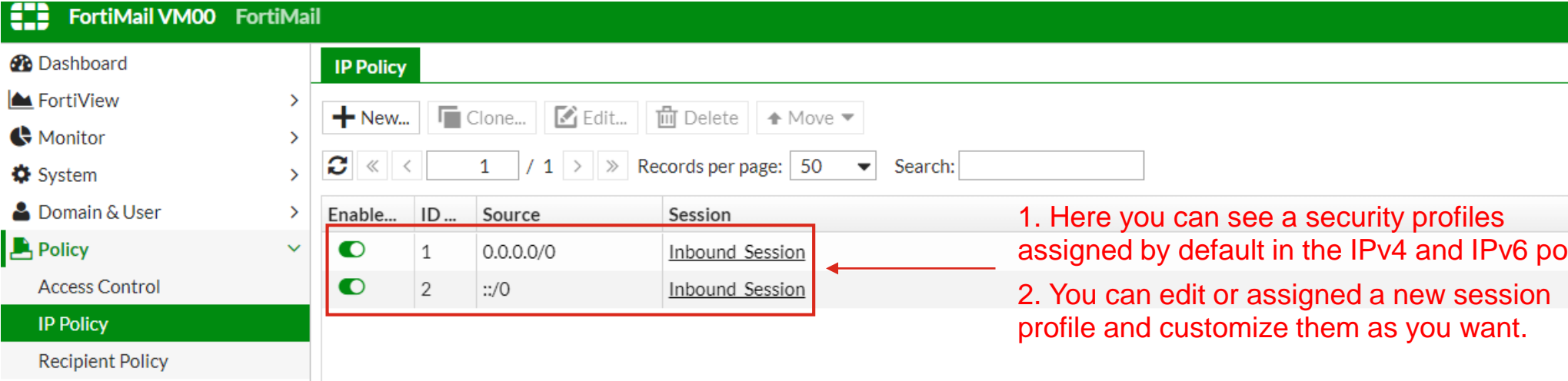
IP Policy

The IP Policies section of the Policies tab lets you create policies that apply profiles to SMTP connections based on the IP addresses of SMTP clients and/or servers with the help of FortiGuard.

IP Policy

1. This is a default IP policy, allows to inspect all IP connection by default. Do not make any change here at least you want to specify the source IP from where all outbound emails will be sent.

2.



FortiMail VM00 FortiMail

IP Policy

+ New... Clone... Edit... Delete Move

Records per page: 50 Search:

Enable...	ID...	Source	Session
<input checked="" type="checkbox"/>	1	0.0.0.0/0	Inbound Session
<input checked="" type="checkbox"/>	2	::/0	Inbound Session

1. Here you can see a security profiles assigned by default in the IPv4 and IPv6 policy.

2. You can edit or assigned a new session profile and customize them as you want.

Step #4

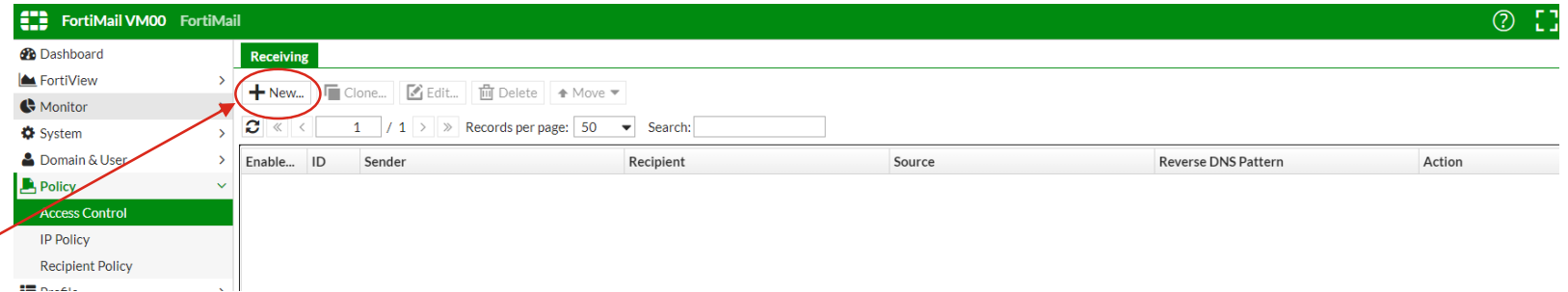
Access Control Policy - Outbound

Access Control Policy by default just show you a receiving tab and here do not display any rules that apply to SMTP sessions being sent it by the FortiMail unit.

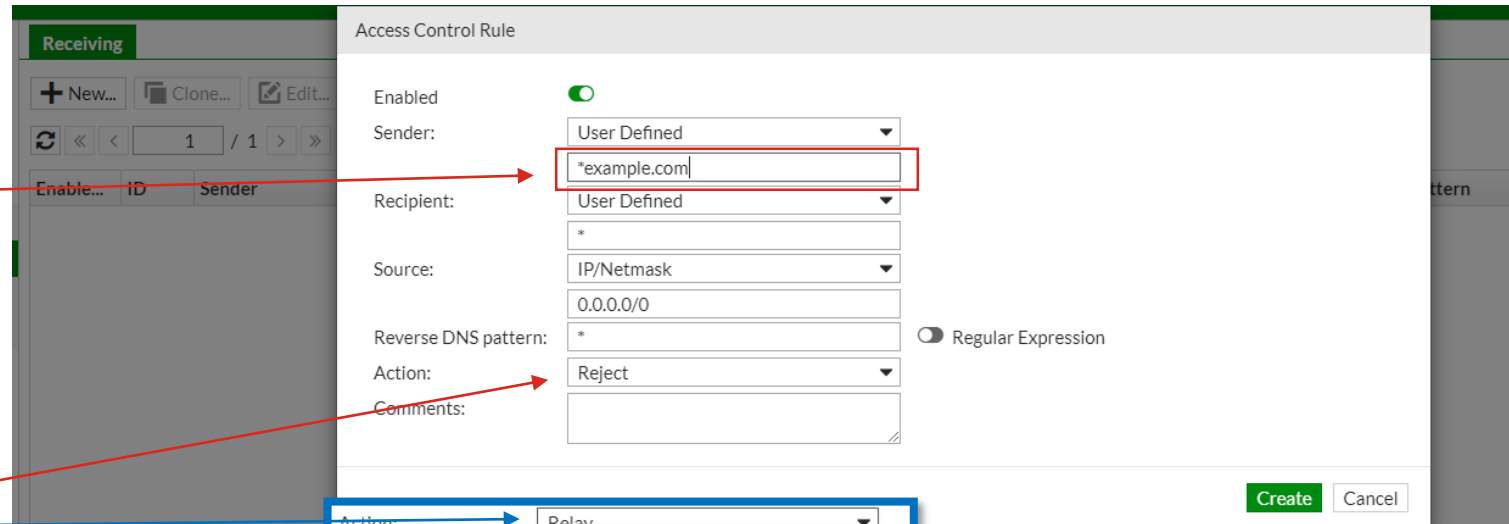
Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages for SMTP sessions that are initiated by SMTP clients.

Access Control Policy

1. By default the receiving tab, do not display any rules for outbound emails, so here we are going to create a new ACL for allows protect domain can send email to any recipient.



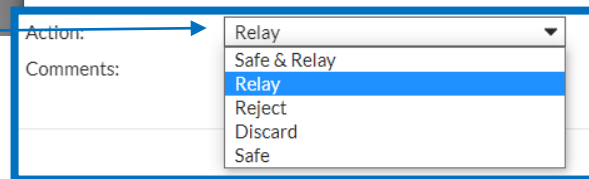
2. Click on +New: A new box show up, is recommended to put the protect domain on the sender field.



3. Then change the Action:

For example:

Change "Reject" to "Relay"



Logs Verifications

Logs Verification

FortiMail VM04 FortiMail

History System Event Mail Event AntiVirus AntiSpam Encryption

2020-09-2

List View Search Export

Records per page: 500 Go to line:

#	Date	Time	Disposition	Classifier
38	2020-09-28	08:13:32.746	System Quarantine;Defer Disposition	FortiSandbox File
39	2020-09-28	08:12:59.448	System Quarantine;Defer Disposition	FortiSandbox File
40	2020-09-28	08:11:37.542	Accept;Defer Disposition	Not Spam
41	2020-09-28	08:11:37.289	Quarantine;Defer Disposition	FortiGuard Outbreak
42	2020-09-28	08:11:37.284	Quarantine;Defer Disposition	FortiGuard Outbreak
43	2020-09-28	08:11:21.220	System Quarantine;Defer Disposition	FortiSandbox File
44	2020-09-28	08:09:43.783	System Quarantine;Defer Disposition	FortiSandbox File
45	2020-09-28	08:09:37.584	Accept;Defer Disposition	Not Spam
46	2020-09-28	08:09:37.284	Quarantine;Defer Disposition	FortiGuard Outbreak
47	2020-09-28	08:09:37.259	Quarantine;Defer Disposition	FortiGuard Outbreak
48	2020-09-28	08:08:37.366	Quarantine	FortiGuard AntiSpam-IP

1. Click on Monitor → Log: Here you can see a series of emails events where they are taking a “Disposition” depend on what “Classifier” they are tag.
2. Little more on the right, you will see the “Direction” field indicated the email direction, in or out.
3. Next to “Direction” you will see too, a “Policy” field, this field show you the matching policy, which the email must have passed through to be a successful email delivery in both direction (in or out).

Location	Client Name ...	Direction	Policy
ZZ (Reserved)		out	1:3:2:
US (United States)	mail-dm6nam...	in	2:1:1:
US (United States)	mail-dm6nam...	in	2:1:1:
US (United States)	mail-qv1-f47....	in	2:1:1:
ZZ (Reserved)		out	1:3:2:
ZZ (Reserved)		out	1:3:2:
CA (Canada)	mx0b-gslb05....	in	2:1:1:

“2” The first number match with the “access control policy”

“1” The second number match with the “IP Policy”

“1” The third number match with the “Recipient Policy”

FORTINET®