

**FORTINET**  
**NSE Training Institute**



# Inside FortiMail 7.2 Features

Mykola Haiovyi

Fortinet Engineer / Trainer

fortinet@muk.ua

2022 Q2

# MUK Training Center – Fortinet Authorized Training Center



11-13/07/2022 - FortiGate Security (FG-S),

3 дня /24 часа

14-15/07/2022 - FortiGate Infrastructure (FG-I),

2 дня/16 часа

**Всем зарегистрированным участникам вебинара  
предоставляется скидка в 10%**

**Контакты:**

+38044 492-29-29

[training@muk.com.ua](mailto:training@muk.com.ua)

# Why Use FortiMail?



Data leak prevention to detect and prevent accidental or intentional leaks of confidential or regulated data



Virus outbreak protection service (VOS) detects and stops malware threats discovered between malware updates



Content disarm and reconstruction (CDR) strips active content from files in real-time, creating a flat sanitized file



Integrated with FortiSandbox provides advanced threat protection



Identity-based encryption, standard transport layer security (TLS), and S/MIME encryption for end-to-end secure email delivery



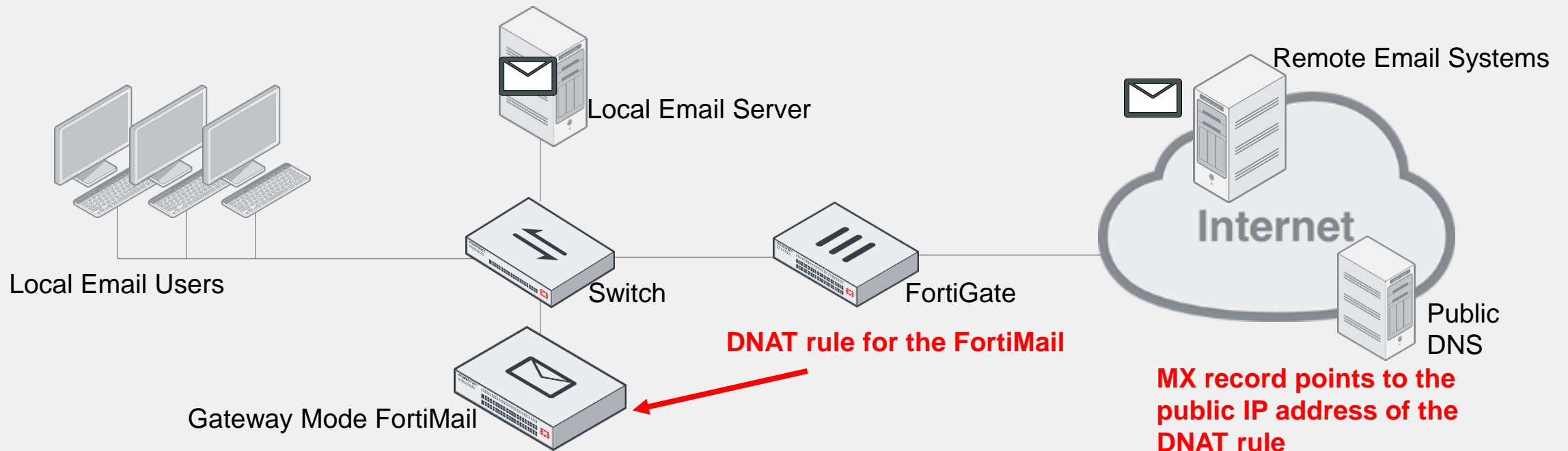
Email archiving for data retention and compliance

# SMTP Device Roles

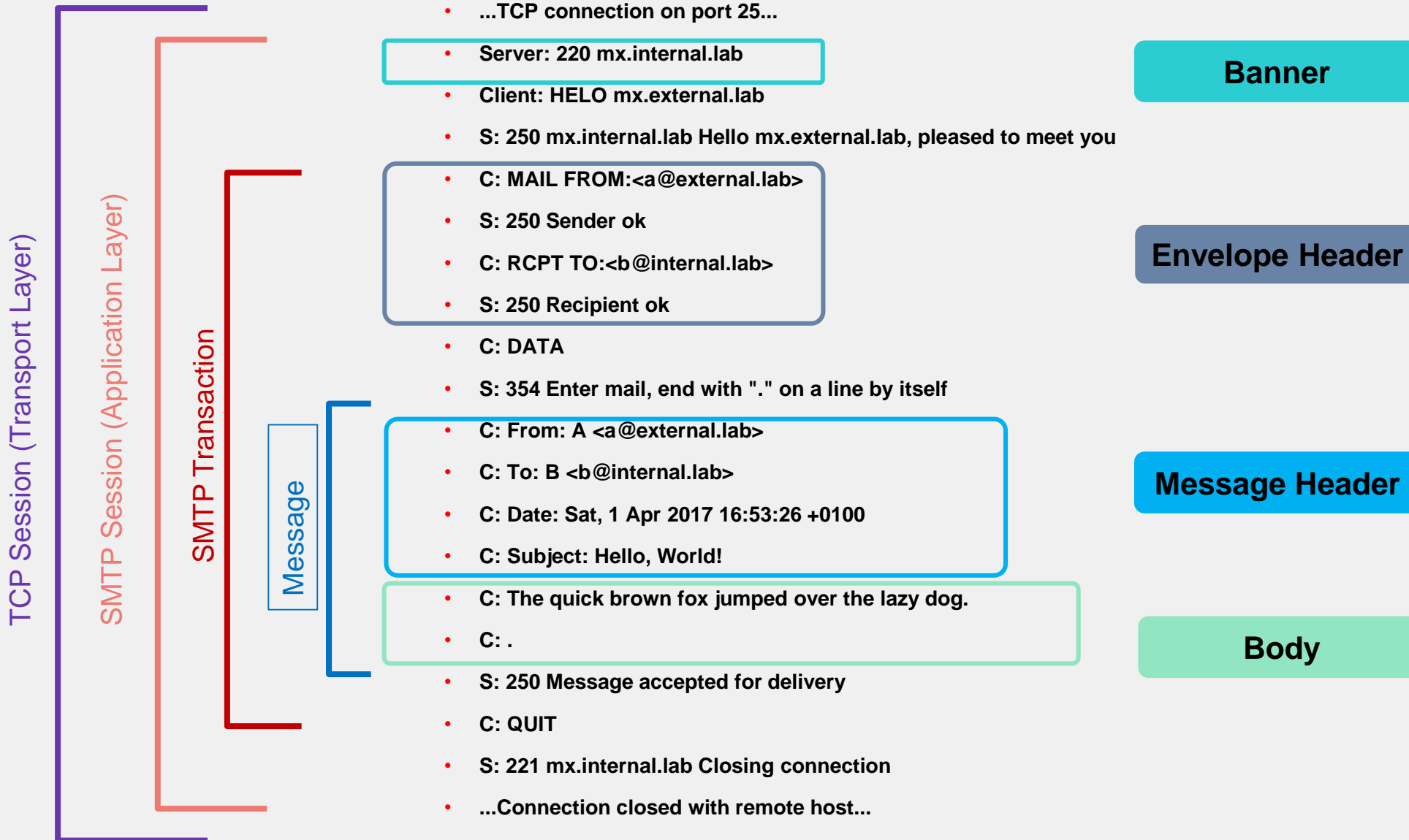
- Mail user agent (MUA)
  - Microsoft Outlook, Thunderbird, Apple Mail
  - SMTP for sending emails
  - POP3 or IMAP for retrieving emails
- Mail transfer agent (MTA)
  - FortiMail, Postfix, Exchange
  - Intermediate hop that processes email; also known as a mail relay
  - Open relays allow unvetted senders and are heavily exploited by spammers
- Mail server
  - Exchange, FortiMail (server mode)
  - The final destination of an email
  - Contains user mailboxes

# Gateway Mode

- Inbound and outbound MTA with application layer security
- Requires a DNS MX record change or a destination NAT rule change
  - All inbound email goes through FortiMail first, then is routed to a back-end mail server



# SMTP Session



# Access Receive Rules

## IP Header:

192.168.3.1:3000 → 172.16.1.1:25

## SMTP Envelope:

EHLO mx.internal.lab

MAIL FROM: <user1@internal.lab>

RCPT TO: <user1@external.lab>

RCPT TO: <user2@external.lab>

DATA

## Message Header:

Received: from mx.internal.lab

Subject: Hello

From: user1@internal.lab

To: user1@external.lab, ...

## Message Body:

Hello, world!

## Policy > Access Control > Receiving

Access Control Rule

Enabled	<input checked="" type="checkbox"/>
Sender pattern:	User Defined *@internal.lab
Recipient pattern:	User Defined *
Sender IP/netmask:	User Defined 10.0.1.99/32
Reverse DNS pattern:	* <input type="checkbox"/> Regular Expression
Authentication status:	Any
TLS profile:	--None-- <a href="#">+ New...</a> <a href="#">Edit...</a>
Action:	Relay
Comments:	

Restrictions on sender IP, as well as sender and recipient patterns

# Access Delivery Rules

- Regulate SMTP sessions initiated by FortiMail to other MTAs

Policy > Access Control > Delivery

Message Delivery Rule

Enabled	<input checked="" type="checkbox"/>		
Sender pattern:	User Defined *		
Recipient pattern:	User Defined *		
Destination IP/netmask:	0.0.0.0/0		
TLS profile:	Enforce_TLS	+ New...	Edit...
Encryption profile:	IBE_Push	+ New...	Edit...
Comments:			

Enforce TLS or apply IBE to specific sessions



# SMTPS and STARTTLS

## STARTTLS

...TCP handshake on port 25...

S: 220 mx.internal.lab

C: EHLO external.lab

S: 250-AUTH PLAIN LOGIN

S: 250-STARTTLS

C: STARTTLS

**Sender chooses to use TLS encryption**

S: 220 Ready to start TLS

...TLS handshake...

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

**STARTTLS encrypts the portion of the session most likely to contain sensitive data. For example, user auth, message header, and body**

## SMTPS

...TCP handshake on port 465...

...TLS Handshake...

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

<encrypted data>

**SMTPS encrypts the entire session including banner, HELO messages, and server extensions**

# IP-Based Policies

- Identify email flow based on the source or destination IP address of the SMTP session
- Apply session profile inspections that are performed on the TCP session and SMTP envelope
- Optionally, configure profiles for SMTP authentication

## Policy > IP Policy > IP Policy

IP Based Policy

Enable

Source: IP/netmask 0.0.0.0 / 0

Destination: IP/netmask 0.0.0.0 / 0

Action: Scan

Comment:

**Profiles**

Session:	a_disabled	+ New...	Edit...
AntiSpam:	--None--	+ New...	Edit...
AntiVirus:	--None--	+ New...	Edit...
Content:	--None--	+ New...	Edit...
DLP:	--None--	+ New...	Edit...
IP pool:	--None--	+ New...	Edit...

**Authentication and Access**

Authentication type: --None--

**Miscellaneous**

Reject different SMTP sender identity for authenticated user

Sender identity verification with LDAP server

LDAP profile: --None-- + New... Edit...

Take precedence over recipient based policy match

- Identify email flow based on the sender or recipient email addresses
- Apply inspection profiles that are applied on the message header and body
- Optionally, configure authentication profiles for SMTP, POP3, IMAP, and webmail
- Separate inbound and outbound policies

## Policy > Recipient Policy > Inbound

Inbound Recipient Policy

Enable

Domain:

Comments:

---

**Sender Pattern**

Type:   @

**Recipient Pattern**

Type:   @

---

**Profiles**

AntiSpam:	<input type="text" value="--None--"/>	<input type="button" value="+ New..."/>	<input type="button" value="Edit..."/>
AntiVirus:	<input type="text" value="AV_In"/>	<input type="button" value="+ New..."/>	<input type="button" value="Edit..."/>
Content:	<input type="text" value="CF_Dictionary"/>	<input type="button" value="+ New..."/>	<input type="button" value="Edit..."/>
DLP:	<input type="text" value="--None--"/>	<input type="button" value="+ New..."/>	<input type="button" value="Edit..."/>
Resource:	<input type="text" value="resource.1"/>	<input type="button" value="+ New..."/>	<input type="button" value="Edit..."/>

---

**Authentication and Access**

Authentication type:

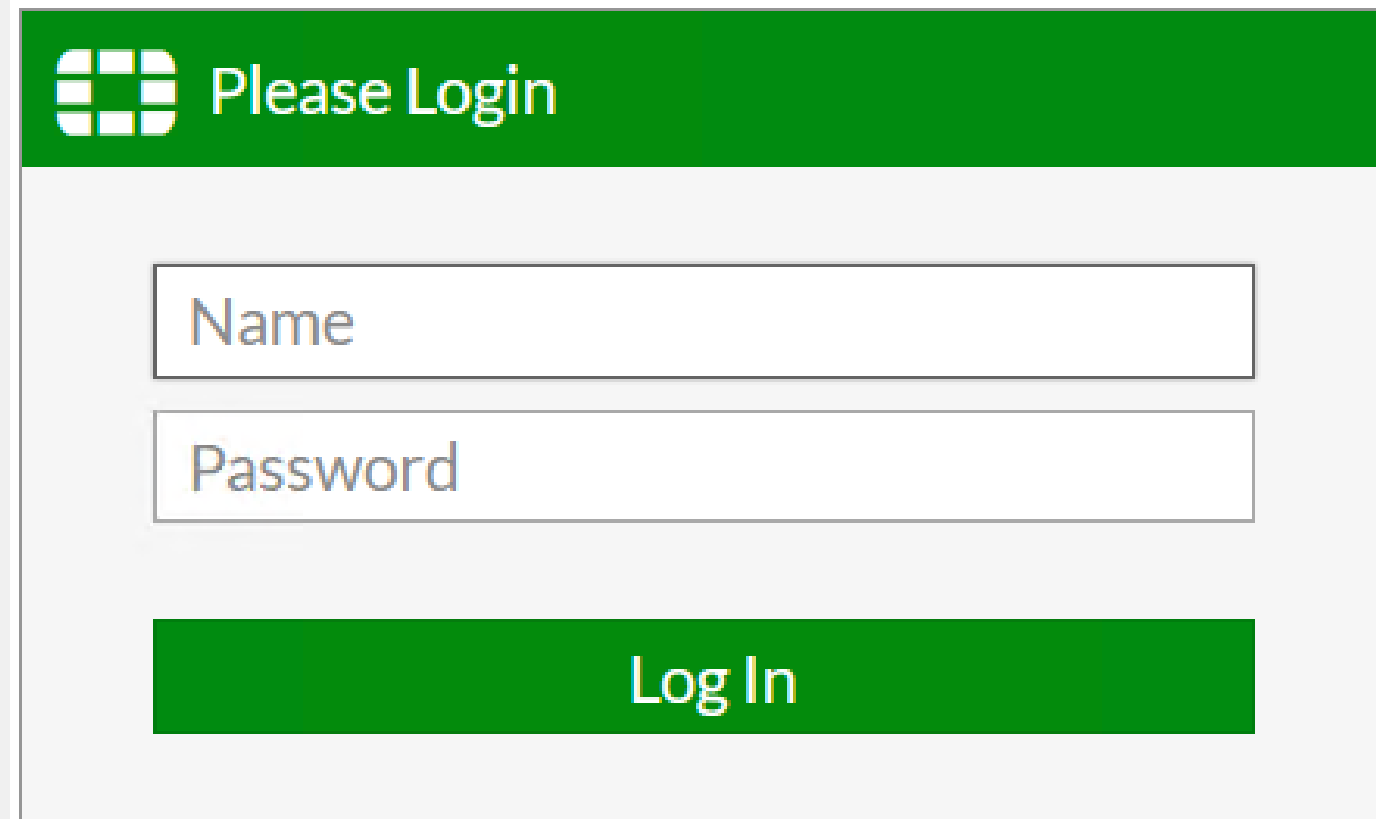
Authentication profile:


Use for SMTP authentication

---

**Advanced Settings**

# Let's go to online Demo



 Please Login

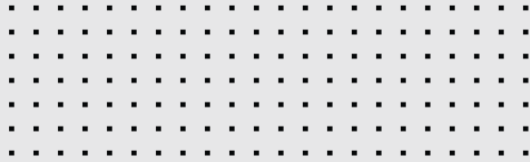
Name

Password

Log In

# Review

- ✓ New GA releases will be tagged as "**Maturity**" or "**Feature**" release.
- ✓ New execute **factoryreset2** Command: Reset the FortiMail unit to its default settings for the currently installed firmware version, while retaining all network settings
- ✓ CLI Access Control: Added **privilege levels** to access CLI in admin profiles
- ✓ **Replacement Custom Message** Enhancement: Separate replacement messages for body and attachment parts.
- ✓ **URL Neutralization**: Added URL neutralization action to CDR and content profile actions.
- ✓ New **Variables** in **Quarantine** Summary: Added "ORIG\_ENVELOPE\_TO" and "ORIG\_TO" (Header To) to quarantine summary reports.
- ✓ **Block/Safe List** Tracking: Added auto aging and retention option to the block/safe lists.



# **FORTINET** **NSE Training Institute**



## **Q&A**

I hope you found this information helpful and interesting. We learned some cool facts together and we saw the world of new modern FortiMail ESG features.

## **Stay safe in 2022.**

fortinet@muk.ua