Configure Mail Relay Host for Email Notifications on FMC

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Troubleshoot
Common Issues
DNS does not Resolve Your SMTP Server
Connection Refused
Connection Timed Out

Introduction

This document describes the procedure to configure an email relay host on Secure Firewall Management Center (FMC) for email notifications.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

• FMC

Components Used

The information in this document is based on these software and hardware versions:

• Firepower Threat Defense for VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Mail Relay Host configuration is needed for FMC to send email notifications and create alerts for security events.

This can be used for correlation and Intrusion policies so you have additional visibility to specific alerts.

Configure

Step 1. Navigate to **System > Configuration**.

	wall Managemer iew / Dashboards / Da					a) Search		Deploy 🔮 🙆	3 admin ~
								Configuration	Health	Monitoring
Home	Summary [Dashboar	d (switch dashboard)					Users	Monitor	Audit
	Provides a summary	y of activity on th	e appliance					Domains	Policy	Syslog
Overview	Network	Threats	Intrusion Events	Status	Geolocation	QoS	Zero Trus	Product Upgrades	Events	Statistics
III Analysis								Content Updates	Exclude	
									Monitor Alerts	Tools
Policies								Licenses		Backup/Restore
								Smart Licenses		Scheduling
Devices										Import/Export
•										Data Purge

Image 1. Navigate to Configuration

Step 2. Navigate to Email Notification.

Access Control Preferences		Save
Access List		
Audit Log	Mail Relay Host	
Audit Log Certificate	Port Number 25	
Change Management	Encryption Method TLS ~	
Change Reconciliation		
DNS Cache	From Address	
Dashboard	Use Authentication	
Database	Test Mail Server Settings	
Email Notification		
External Database Access		

Image 2. Navigate to Email Notification Menu

Step 3. Enter the IP address or Fully Qualified Domain Name (FQDN) for your Email Relay Host, port, encryption method, email address, and authentication for the host if needed.

Step 4. Select **Test Mail Server Settings**, a **Message Sent** appears if your settings are correct and an email is received from the configured sender email to the destination address used on the test. Save your **configuration**.

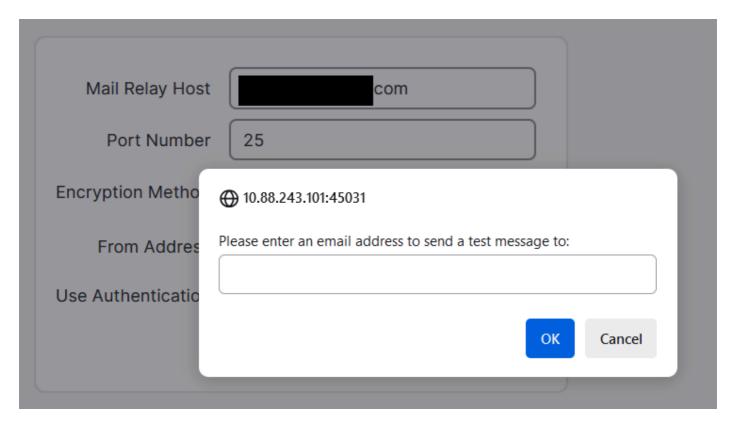


Image 3. Test Mail Server Settings

Mail Relay Host	com
Port Number	25
Encryption Method	None ~
From Address	alertfmc760@
Use Authentication	
 Message sent 	Test Mail Server Settings

Image 4. Successful Configuration Message

Testing Email settings for: firepower.



This is a test message. Your proposed email notification settings function correctly.

Image 5. Successful Configuration Email

Troubleshoot

FMC GUI displays a generic error message when the test fails.

Access Control Preferences			Save
Access List	Mali Dalau Lina	10 00 04044	
Audit Log	Mail Relay Host	10.88.243.11	
Audit Log Certificate	Port Number	25	
Change Management	Encryption Method	None ~	
Change Reconciliation	From Address	alertfmc760@com	
DNS Cache	From Address	aler time you to the	
Dashboard	Use Authentication (Failed to send		
Database	message, check settings.	your Test Mail Server Settings	
Email Notification	settings.		

Image 6. Failed Error Message

You can check the error messages from the mail tests on the FMC CLI. You have to navigate to **expert** and you can enter the command **cat /var/log/messages** | **grep -i ''email**\|**smtp''** to look for your connection tests' messages.

```
<#root>
```

```
>
```

expert

admin@firepower:~\$

```
cat /var/log/messages | grep -i "email\|smtp"
Oct 16 17:57:38 firepower msmtp: host=****.com tls=on auth=off from=alertfmc760@****.com recipients
```

Common Issues

DNS does not Resolve Your SMTP Server

Oct 16 17:32:52 firepower msmtp: host=****.co tls=off auth=off from=alertfmc760@****.com recipient cannot locate host ****.co: Name or service not known

exitcode=EX_NOHOST

.

Verify your email relay hostname, that your DNS servers are reachable, and they can resolve the hostname.

```
admin@firepower:~$ ping ****.***.co
ping: ****.***.co: Name or service not known
```

Connection Refused

<#root>

```
Oct 16 17:33:54 firepower msmtp: host=10.100.150.11 tls=off auth=off from=alertfmc760@****.com recipien
exitcode=EX TEMPFAIL
```

The server is listening to the port, however, it actively refused the connection. Verify your settings and, if applicable, the authentication.

Verify SMTP service is running on the server side.

Connection Timed Out

<#root>

```
Oct 16 17:58:30 firepower msmtp: host=****.com tls=on auth=off from=alertfmc760@****.com recipient exitcode=EX_TEMPFAIL
```

Verify the server is listening to the port used for the connection.