



FORTINET

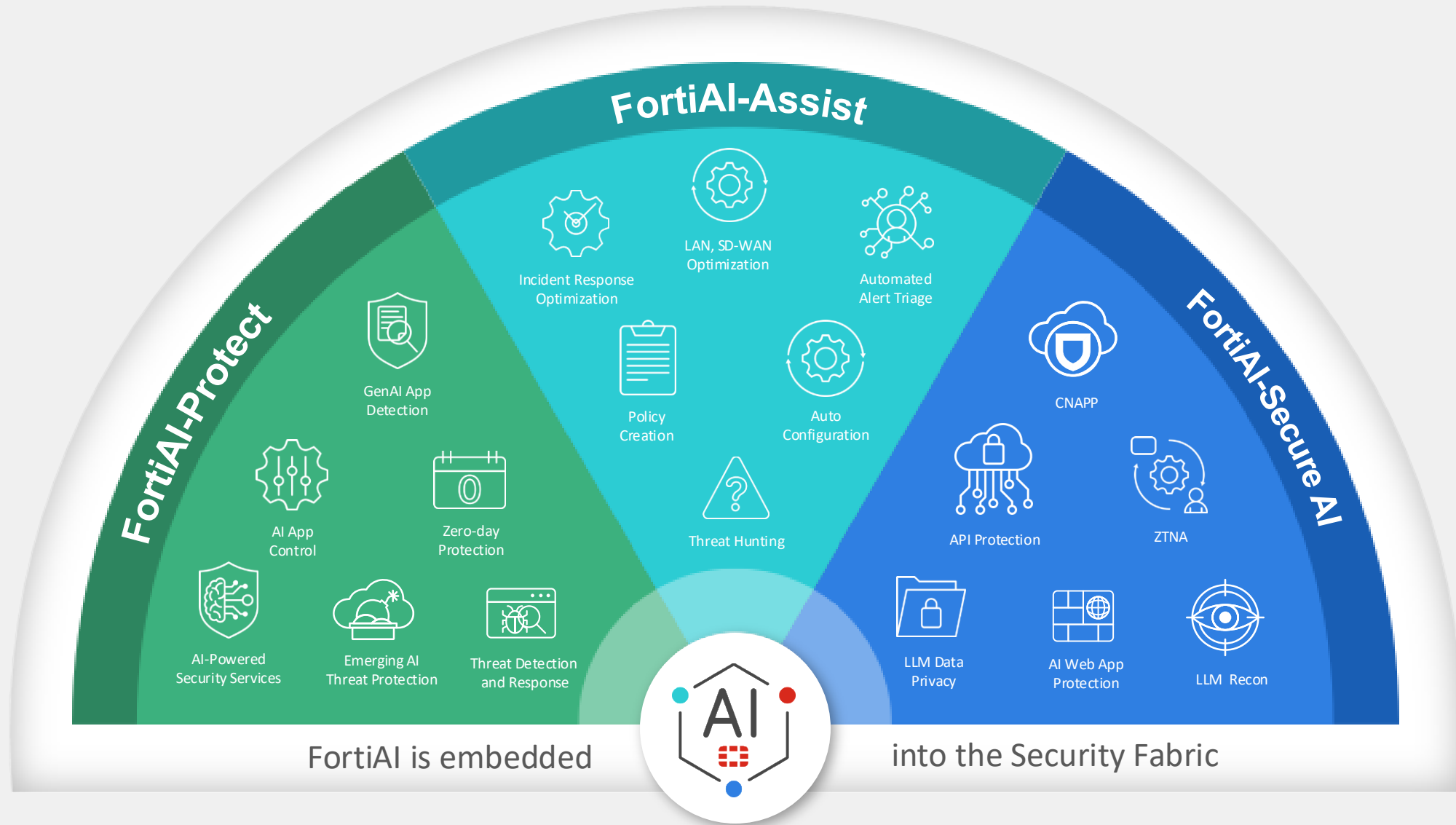
FortiAI

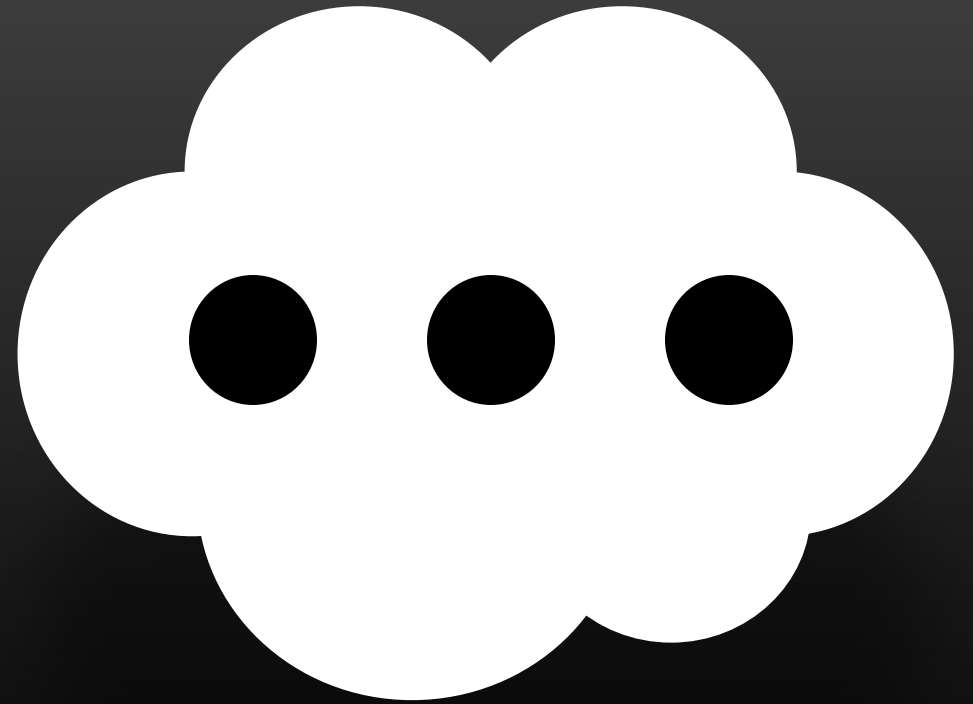
AI-powered Security and Transformation

Ondřej Večl, Principal System Engineer



FortiAI Solutions Supports Broad Range of Use Cases







AI For SD-WAN



OK, can you show me what devices are managed, and their geographic location?

FortiAI

Hi admin, what can I help you with? I can do many things, but I'm only allowed to help with FortiManager tasks, such as:

- Deploy SD-WAN or VPN configurations using a network diagram
- Diagnose SD-WAN or VPN network issues
- Create, validate, and explain CLI scripts and Jinja scripts
- Help to setup Zero Touch Provisioning Templates
- Identify IoT insights – detect IoT devices, vulnerabilities present and recommended actions

Hi there, can you check if any SD-WAN configuration is present on my system right now?

Of course! Let me direct you to the SD-WAN Overlay Templates page to check ... hmm, it looks like presently there are no SD-WAN configurations.

Okay, can you show me what devices are managed and their geographic location?

Certainly! Let me take you to the SD-WAN Monitor page so you can see how it looks and review the current location of all managed devices.

Ask FortiAI for help with device configurations, SDWAN, and more



AI For SD-WAN



Great, thanks. I have an SD-WAN topology diagram I drew – can you help generate an SD-WAN template to deploy?

FortiAI

This is what I read from the diagram:

- Site: HUB1
 - WAN interfaces:
 - port1: 10.198.5.2/29
 - port2: 10.198.6.2/29
 - LAN interfaces:
 - port3: 172.16.1.2/30
- Site: HUB2
 - WAN interfaces:
 - port1: 10.198.7.2/29
 - port2: 10.198.8.2/29
 - LAN interfaces:
 - port3: 172.16.2.2/30
- Site: Br1
 - WAN interfaces:
 - port1: 10.198.1.2/29
 - port2: 10.198.2.2/29
 - LAN interfaces:
 - port3: 10.1.1.0/24 (subnet: 10.1.1.0/24)
- Site: Br2
 - WAN interfaces:
 - port1: 10.198.3.2/29
 - port2: 10.198.4.2/29
 - LAN interfaces:
 - port3: 10.1.2.0/24 (subnet: 10.1.2.0/24)

Are these details correct to proceed?

Ask FortiAI for help with device configurations, SDWAN, and more



AI For SD-WAN



Thanks. Please go ahead
to install the configuration.

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

- Device & Groups
- Scripts
- Provisioning Templates
- Firmware Templates

Monitors

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

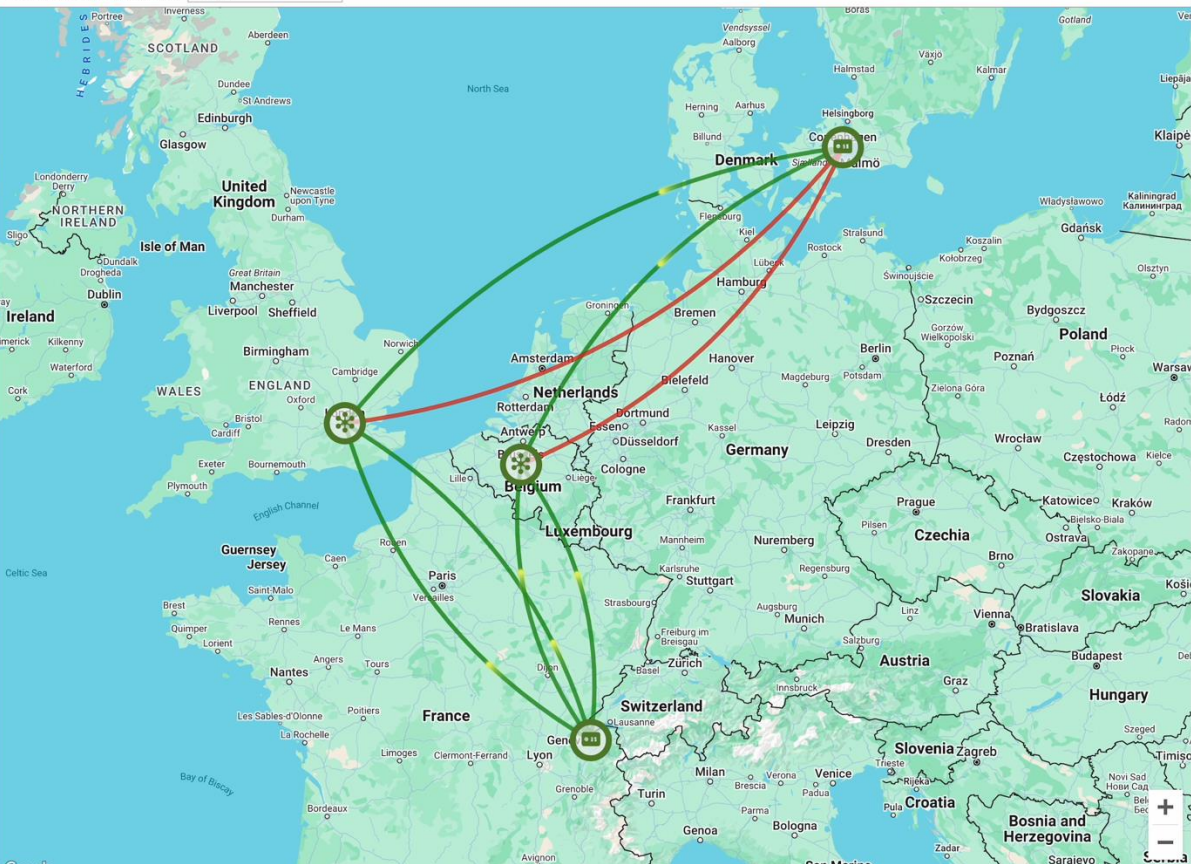
FortiGuard

System Settings

Install Wizard

SD-WAN MonitorVPN MonitorAsset Identity Center

Show Down Tunnels OnlyCorpA



Google

ADOM: CorpA

admin

FortiAI

```
set ike-version 2
set dpd on-idle
set comments "VPN: VPN1 [Created by IPSEC Template]"
set proposal aes256-sha256
set peertype any
set mode-cfg enable
set dpd-retryinterval 60
set net-device disable
set add-route disable
set auto-discovery-sender enable
set ipv4-start-ip 10.10.0.1
set ipv4-end-ip 10.10.31.252
set ipv4-netmask 255.255.224.0
set psksecret *****
set network-overlay enable
set network-id 1
next
```

I have saved the configuration in the SD-WAN Overlay Template table. Please review it, and when ready I can help you install the configuration.

Thanks. Please go ahead to install the configuration.

Installing Configurations to Devices

Br1100%Configurations have been installed to Br1.

Br2100%Configurations have been installed to Br2.

HUB1100%Configurations have been installed to HUB1.

HUB2100%Configurations have been installed to HUB2.

Configurations have been successfully installed to the devices. I am redirecting to the SD-WAN Monitor page so you can monitor the setup.

Ask FortiAI for help with device configurations, SDWAN, and more





AI For SD-WAN



Yes,
please proceed.

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

- Device & Groups
- Scripts
- Provisioning Templates
- Firmware Templates

Monitors

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

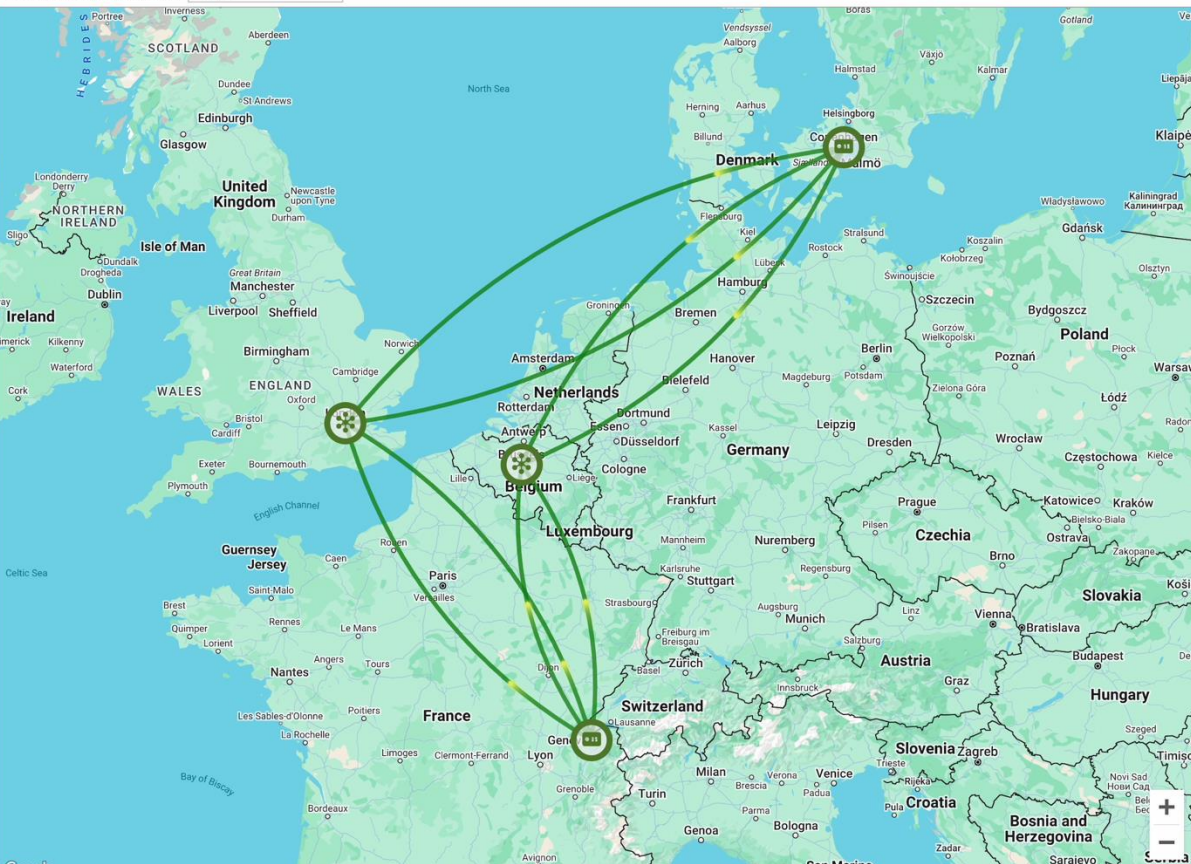
FortiGuard

System Settings

Install Wizard

SD-WAN MonitorVPN MonitorAsset Identity Center

Show Down Tunnels OnlyCorpa



Google

ADOM: CorpA

admin

FortiAI

name: HUB1-VPN1
serial: 1
version: 2
status.admin: up
status.operational: down
type: static
local: 10.198.1.2
remote: 10.198.5.2
mode: main

name: VPN1
serial: 1
version: 2
status.admin: up
status.operational: up
type: dynamic
local: 10.198.5.2
mode: main

Br1 - HUB2-VPN1

HUB2 - VPN1

vd: root/0
name: HUB2-VPN1
serial: 3
version: 2
status.admin: up
status.operational: down
type: static
local: 10.198.1.2
remote: 10.198.7.2
mode: main

vd: root/0
name: VPN1
serial: 1
version: 2
status.admin: up
status.operational: up
type: dynamic
local: 10.198.7.2
mode: main

The problem is caused by the admin status of interface port1 on device Br1 being disabled. To resolve this issue, I recommend the following action plan:

1. Enable the admin status on the port1 interface of device Br1.
2. Install the new configuration to device Br1.
3. Verify the VPN status after the installation.

Would you like to proceed?

Yes, please proceed.

I have enabled the admin status of interface port1 on Br1.

Installing Configurations to Device

Br1

100%

Configurations have been installed to Br1.

All done - please verify the VPN status.

Ask FortiAI for help with device configurations, SDWAN, and more





AI

For SD-WAN



Perfect, it's working. Next I'd like to enable SASE for remote access to this network.
Can you enable the FortiSASE connector?

The screenshot displays the Fortinet SD-WAN Manager interface. On the left is a sidebar with navigation options: FMG-VM64-KVM, Dashboard, AI Insights, Device Manager, Policy & Objects, SD-WAN Manager, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports, FortiGuard, and System Settings. The main area shows a map of Europe with several VPN tunnels connecting various locations. A chat window on the right is titled 'FortiAI' and shows a conversation about enabling SASE for remote access. The chat includes a code block with configuration details for 'HUB2-VPN1' and 'VPN1', a list of steps to resolve an issue with interface port1, and a confirmation of successful configuration installation.

ADOM: CorpA

SD-WAN Monitor VPN Monitor Asset Identity Center

Show Down Tunnels Only CorpA

vd: root/0
name: HUB2-VPN1
serial: 3
version: 2
status.admin: up
status.operational: down
type: static
local: 10.198.1.2
remote: 10.198.7.2

vd: root/0
name: VPN1
serial: 1
version: 2
status.admin: up
status.operational: up
type: dynamic
local: 10.198.7.2
mode: main

The problem is caused by the admin status of interface port1 on device Br1 being disabled. To resolve this issue, I recommend the following action plan:

1. Enable the admin status on the port1 interface of device Br1.
2. Install the new configuration to device Br1.
3. Verify the VPN status after the installation.

Would you like to proceed?

Yes, please proceed.

I have enabled the admin status of interface port1 on Br1.

Installing Configurations to Device Br1

100%

Configurations have been installed to Br1.

All done - please verify the VPN status.

Perfect, it's working. Next, I'd like to enable SASE for remote access to this network. Can you enable the FortiSASE connector?

OK, I found an active SASE instance under your account. I've enabled the connector to it. Here are the current deployment details:

- FortiSASE Advanced License (500 users)
- Security POPs active in Frankfurt, Madrid and Paris
- 450 users actively connected with Secure Internet Access (last 7 days)

Ask FortiAI for help with device configurations, SDWAN, and more





AI For SASE



Yes,
please go ahead.

The screenshot displays the Fortinet SD-WAN Manager interface. On the left is a sidebar menu with options like Dashboard, AI Insights, Device Manager, Monitors, and various management tools. The main area shows a map of Europe with several locations marked by icons and connected by green lines, representing a network topology. A chat window on the right, titled 'FortiAI', shows a conversation where the AI assistant helps with configuration tasks. The chat messages include:

- FortiAI: "Would you like to proceed?"
- User: "Yes, please proceed."
- FortiAI: "I have enabled the admin status of interface port1 on Br1. Installing Configurations to Device Br1. 100% Configurations have been installed to Br1. All done - please verify the VPN status."
- User: "Perfect, it's working. Next, I'd like to enable SASE for remote access to this network. Can you enable the FortiSASE connector?"
- FortiAI: "OK, I found an active SASE instance under your account. I've enabled the connector to it. Here are the current deployment details:
 - FortiSASE Advanced License (500 users)
 - Security POPs active in Frankfurt, Madrid and Paris
 - 450 users actively connected with Secure Internet Access (last 7 days)"
- User: "Okay, can you please connect these SASE notes to my SD-WAN network?"
- FortiAI: "OK, will do. I can also synchronize the security profiles deployed for on-premise SD-WAN users to the SASE users. Would you like to include those changes?"
- User: "Yes, please go ahead."
- FortiAI: "Installing Configurations using FortiSASE Connector FortiSASE 100% Configurations have been installed to FortiSASE. OK, I have updated all SASE configurations. DLP, AV and 10 other security profiles are now active on your FortiSASE instance."

At the bottom of the chat window, there is a prompt: "Ask FortiAI for help with device configurations, SDWAN, and more".





AI For SASE



Perfect,
thanks for your help.

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Device & Groups

Scripts

Provisioning Templates

Firmware Templates

Monitors

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

SD-WAN Monitor

VPN Monitor

Asset Identity Center

Show Down Tunnels Only

CorpA

FortiAI

ADOM: CorpA

admin

OK, I have updated all SASE configurations. DLP, AV and 10 other security profiles are now active on your FortiSASE instance.

Thanks, it looks correct. To simplify the map view, please mute all tunnels which are performing correctly.

OK, I have changed those links to light grey colour.

Perfect, thanks for your help.

You are welcome! If you have any further questions, feel free to ask.

FortiSASE AI Alert!!!

A new remote access connection to the SD-WAN network without zero trust protection has been detected.

Investigate Now

Create A Ticket for Later

Ignore

Investigate now.

Here is a summary of the remote access connection:

- Connecting from Berlin
- Connecting to the Frankfurt POP
- Accessing an application located in the Geneva branch

Recommendation

Enable Zero Trust tags for:

- No critical vulnerabilities detected
- EDR running
- No EDR alerts present

Would you like to enable these changes?

Ask FortiAI for help with device configurations, SDWAN, and more





AI For SASE



OK,
please enable Zero Trust.

The screenshot displays the Fortinet FortiSASE management console. The left sidebar contains a navigation menu with options like Dashboard, AI Insights, Device Manager, and various managers (VPN, AP, FortiSwitch, Extender, FortiView, Log View, Fabric View, Incidents & Events, Reports, FortiGuard, System Settings). The main area shows a map of Europe with network nodes and connections. A top bar includes tabs for SD-WAN Monitor, VPN Monitor, and Asset Identity Center. On the right, a chat window titled 'FortiAI' is active, showing a summary of a remote access connection and a recommendation to enable Zero Trust tags. The chat also displays a progress bar for 'Installing Configurations using FortiSASE Connector' and an alert about a 'Urgent WiFi connectivity issue at Branch 1'.

FortiAI

A new remote access connection to the SD-WAN network without Zero Trust protection has been detected.

[Investigate Now](#) [Create A Ticket for Later](#) [Ignore](#)

[Investigate now.](#)

Here is a summary of the remote access connection:

- Connecting from Berlin
- Connecting to the Frankfurt POP
- Accessing an application located in the Geneva branch

Recommendation

Enable Zero Trust tags for:

- No critical vulnerabilities detected
- EDR running
- No EDR alerts present

Would you like to enable these changes?

[Okay, please enable Zero Trust.](#)

Installing Configurations using FortiSASE Connector

FortiSASE

100%

Configurations have been installed to FortiSASE.

All done. If you need anything else, feel free to ask.

FortiAIops ALERT!!!

Urgent WiFi connectivity issue at Branch 1. Would you like me to query FortiAIops?

[Check details](#)

Ask FortiAI for help with device configurations, SDWAN, and more





AI For AIOps



Yes, please retrieve the analysis of this location from AIOps.

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

Managed FortiAPs

WiFi Maps

SSIDs

Operation Profiles

Connectivity Profiles

Protection Profiles

WiFi Settings

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

Google Map

Floor Map

Back

Zoom in

Zoom out

Edit Mode

MICHAEL

R2 (CH: 36) 15%

CONFERENCE ROOM

R2 (CH: 36) 83%

R2 (CH: 36) 76%

ROOM

ERIN

JIM

PAM

DWIGHT

ANDY

R2 (CH: 36) 78%

PHYLLIS

STANLEY

KITCHEN

THE ANNEX

RYAN

R2 (CH: 36) 72%

MEN'S ROOM

WOMEN'S ROOM

ANGELA

KEVIN

OSCAR

MEREDITH

CREED

DARRYL

ABOL

KELLY

FortiAI

• EDR running

• No EDR alerts present

Would you like to enable these changes?

Okay, please enable Zero Trust.

Installing Configurations using FortiSASE Connector

FortiSASE

100%

Configurations have been installed to FortiSASE.

All done. If you need anything else, feel free to ask.

FortiAIOps ALERT!!!

Urgent WiFi connectivity issue at Branch 1. Would you like me to query FortiAIOps?

Check details

Yes, please retrieve the analysis of this location from AIOps.

Issue Analyzed by FortiAIOps:

Issue

Too many interfering APs (9) on Channel 36 significantly contributing to over-channel-utilization (90%) and availability.

Recommendation

Enable AIOps DRRP on the below APs to configure best channel and power settings to reduce co-channel interference and channel utilization:

• AP-4-02

• AP-4-05

• AP-4-07

Ask FortiAI for help with device configurations, SDWAN, and more





AI For AIOps



Perfect, thanks.

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

Managed FortiAPs

WiFi Maps

SSIDs

Operation Profiles

Connectivity Profiles

Protection Profiles

WiFi Settings

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

Google Map

Floor Map

Back

Zoom in

Zoom out

Edit Mode

MICHAEL

R2 (CH: 100) 0%

CONFERENCE ROOM

R2 (CH: 44) 2%

R2 (CH: 149) 17%

ERIN

JIM

PAM

DWIGHT

PHYLLIS

STANLEY

KITCHEN

THE ANNEX

ANGELA

KEVIN

OSCAR

MEREDITH

CREED

DARRYL

MEN'S ROOM

WOMEN'S ROOM

RYAN

R2 (CH: 56) 2%

R2 (CH: 64) 0%

R2 (CH: 100) 0%

ABOL

KELLY

FortiAI

Issue

Too many interfering APs (9) on Channel 36 significantly contributing to over-channel-utilization (90%) and availability.

Recommendation

Enable AIOps DRRP on the below APs to configure best channel and power settings to reduce co-channel interference and channel utilization:

- AP-4-02
- AP-4-05
- AP-4-07

Are you able to fix this?

Yes, I can enable DARRP on the APs managed by Br1 to optimize it. Note, this will take a few moments and disrupt client connectivity to those APs temporarily. Do you want me to proceed?

Yes, please proceed.

All done - channel interference looks to be stabilizing.

Check details

Perfect, thanks.

You are welcome! If you have any further questions, feel free to ask.

FortiAnalyzer AI Alert!

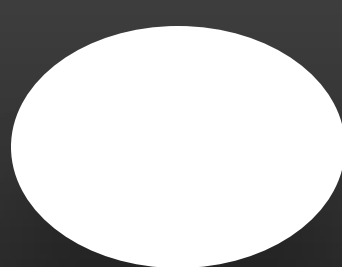
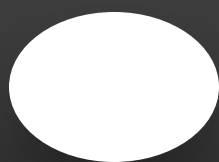
New Incident regarding a slow server at 172.16.88.23. Would you like to investigate this?

Investigate Now

Ignore

Ask FortiAI for help with device configurations, SDWAN, and more





Recap

- ✓ Assisted Navigation & Monitoring
- ✓ SD-WAN Configuration Generation
- ✓ SD-WAN Monitoring
- ✓ SASE Management
- ✓ ZTNA Analysis & Auto Generation
- ✓ Monitoring via AIOps Engine
- ✓ Wireless Corrective Actions

What is Agentic AI?

AI systems designed to act autonomously, **making decisions** and **taking actions**, often focusing on **goal-oriented behavior** and **adapting to changing** circumstances.





AI For AIOps



FortAI,
can you help me to fully investigate this incident?

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

Managed FortiAPs

WiFi Maps

SSIDs

Operation Profiles

Connectivity Profiles

Protection Profiles

WiFi Settings

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

FortiAI

FortiAI Reasoning Agent

1. Understanding the request

2. Check Server and Processes

3. Check IP Reputation

4. Check for more infected devices

5. Uncovering Brute Force Attempts

Incident Summary

The slowness was due to a **Monero miner C2 connection** - attacker used a **brute force login** to access the server and spread to other endpoints.

Recommendations:

1. Quarantine Infected Systems

2. Block Malicious Traffic

3. Enforce Multiple Factor Authentication

4. Patch the vulnerable Systems

Call To Action

Quarantine Infected Systems

Block Malicious Traffic

Assign the Incident Ticket

Hand Over Incident

Send the Email to CISO

Download the Incident Report

Investigate Incident Ticket

Slow Server (IN00000011)

172.16.88.23

1

Reported Issue: High CPU Usage

File Backup Server

172.16.88.23

1

High CPU Process

Suspicious Process Found

nqcloud (PID: 1234)/CPU: 98%

2

C2 Communication

External Connection

136.243.90.99

2

Outbound Connection

Infected Endpoints

10.3.15.254 172.16.115.11

172.16.88.23

3

C2 Communication

Brute Force Attempts

Multiple Failed Logins From 10.100.55.254

5

Suspicious Logins

Threat Intelligence

FortiGuard Analysis

Malicious: Monero Miner

136.243.90.99

3

Investigation revealed cryptocurrency mining activity and multiple compromised endpoints

Replay





AI

For FortiAnalyzer



FortAI,
can you help me to fully investigate this incident?

The screenshot displays the FortiAnalyzer web interface. On the left is a sidebar menu with various management tools. The main content area is titled 'FortiAI' and features a 'FortiAI Reasoning Agent' panel. This panel shows a step-by-step reasoning process for investigating a 'Slow Server' incident, identifying it as linked to a 'File Backup Server' with IP 172.16.88.23. To the right of this panel is a network diagram illustrating the relationship between the incident and the server.

FortiAI Reasoning Agent

1. Understanding the request

The user wants me to check a slow server issue they reported. First, I should see if there is a related incident in FortiAnalyzer.

Found incident **IN00000011**, it's linked to the file backup server (IP: **172.16.88.23**).

Next, I'll investigate this incident.

Investigate Incident Ticket
Slow Server (IN00000011)
172.16.88.23

Reported Issue: High CPU Usage

File Backup Server
172.16.88.23

FortiAnalyzer Sidebar Menu:

- FMG-VM64-KVM
- Dashboard
- AI Insights
- Device Manager
- Policy & Objects
- SD-WAN Manager
- VPN Manager
- AP Manager
- Managed FortiAPs
- WiFi Maps
- SSIDs
- Operation Profiles
- Connectivity Profiles
- Protection Profiles
- WiFi Settings
- FortiSwitch Manager
- Extender Manager
- FortiView
- Log View
- Fabric View
- Incidents & Events
- Reports
- FortiGuard
- System Settings



FortAI,
can you help me to fully investigate this incident?

FortiAI Reasoning Agent

1. Understanding the request

The user wants me to check a slow server issue they reported. First, I should see if there is a related incident in FortiAnalyzer.

Found incident `IN000000013`, it's linked to the file backup server (IP: `172.16.88.23`).

Next, I'll investigate this incident.

Analyzing Output

Private IP Address Alert

NEXT STEP >

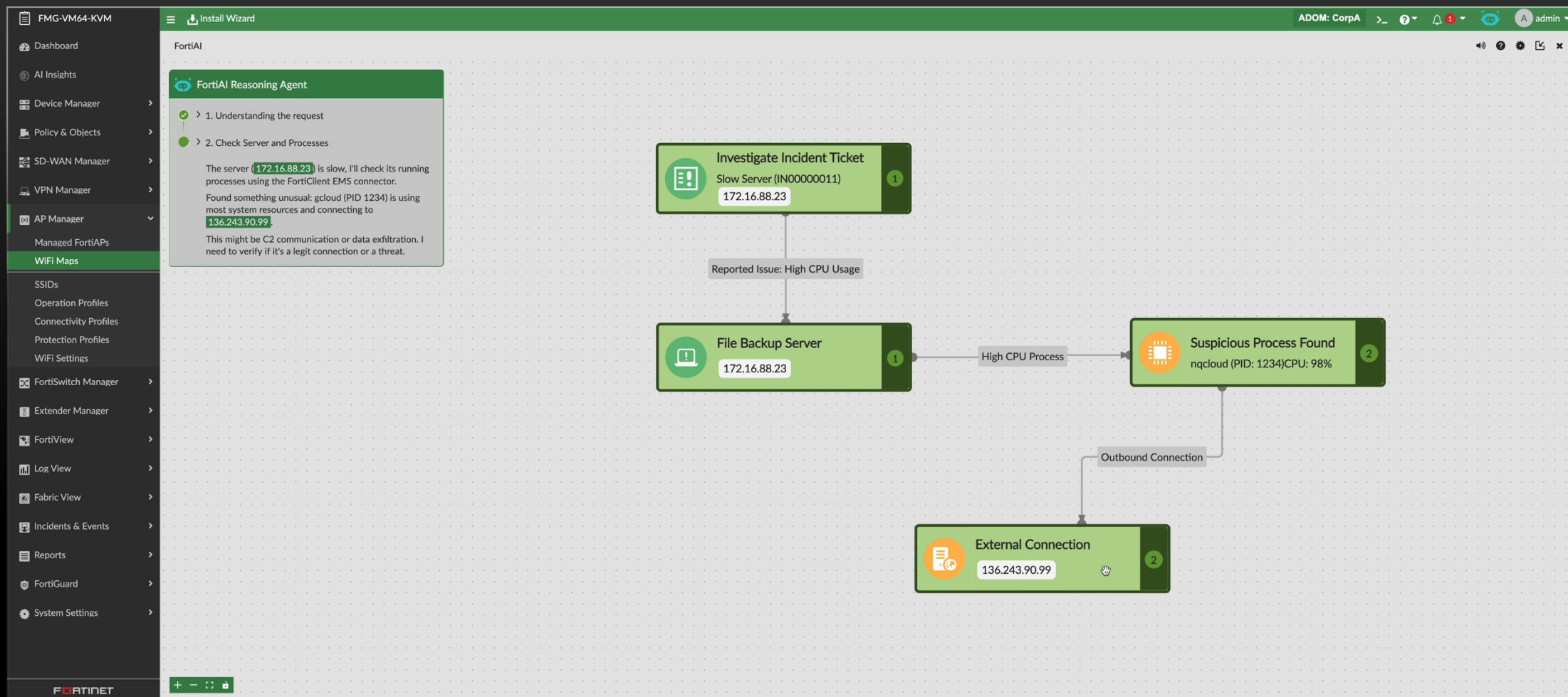
Lookup Endpoint on EMS



AI For FortiAnalyzer

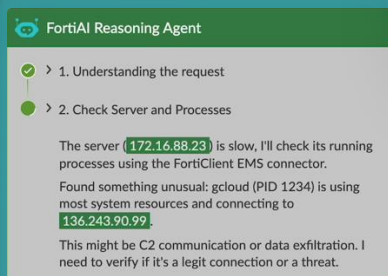


FortAI,
can you help me to fully investigate this incident?





FortAI,
can you help me to fully investigate this incident?



Analyzing Output

Suspicious Public IP

NEXT STEP >

Lookup public IP via FortiTIP

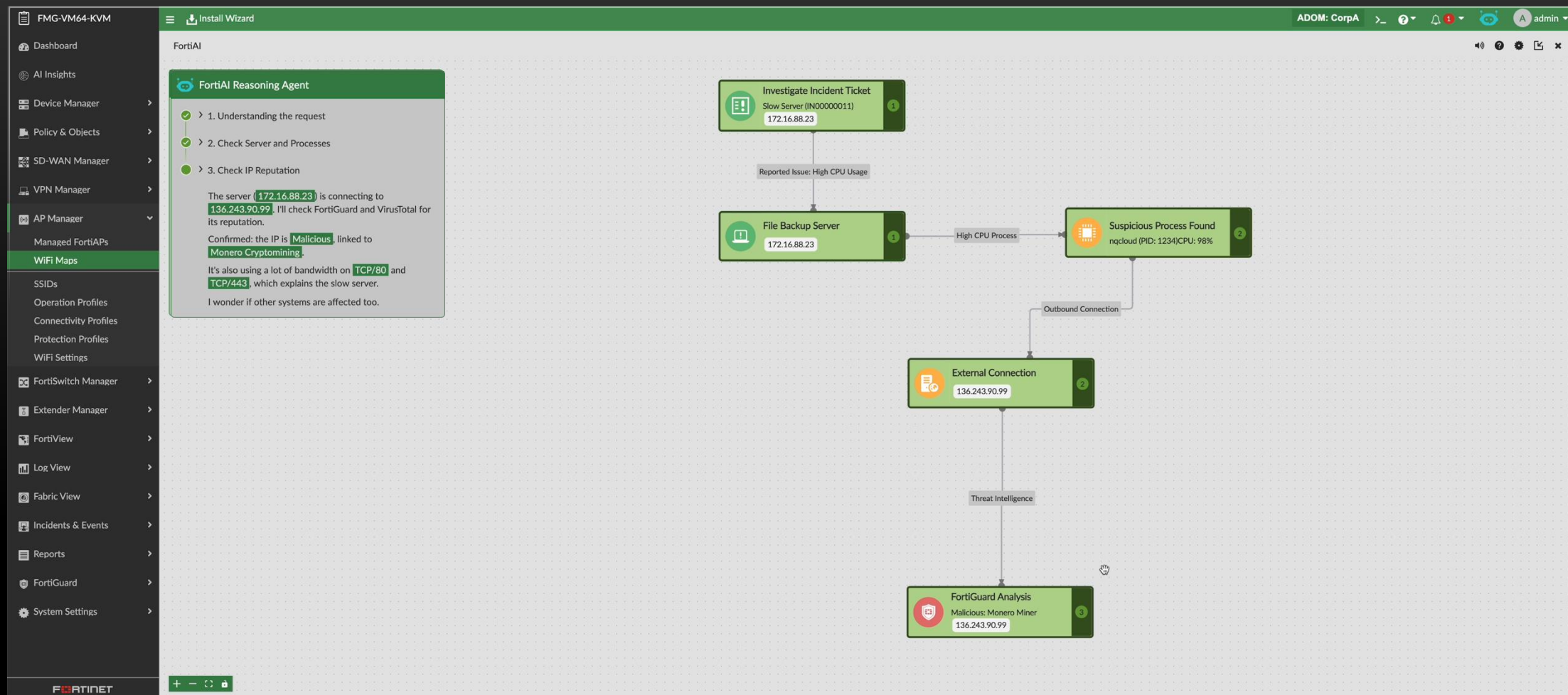


AI

For FortiAnalyzer

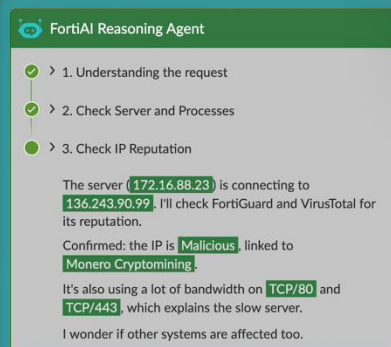


FortAI,
can you help me to fully investigate this incident?





FortAI,
can you help me to fully investigate this incident?



Analyzing Output

Confirmed Infected

NEXT STEP >

Correlate incident across
FortiAnalyzer Data Lake to discover
other infected endpoints.





AI

For FortiAnalyzer



FortAI,
can you help me to fully investigate this incident?

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

Managed FortiAPs

WiFi Maps

SSIDs

Operation Profiles

Connectivity Profiles

Protection Profiles

WiFi Settings

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

FortiAI

FortiAI Reasoning Agent

1. Understanding the request

2. Check Server and Processes

3. Check IP Reputation

4. Check for more infected devices

136.243.90.99 is confirmed malicious, I need to see if other endpoints are connecting to it...

Found three affected devices:

10.3.15.254 (25s)

172.16.88.23 (2m 8s) - the slow server

172.16.115.11 (46s)

This suggests a broader security incident - Let me take a closer look at the slow server first.

Investigate Incident Ticket

Slow Server (IN00000011)

172.16.88.23

Reported Issue: High CPU Usage

File Backup Server

172.16.88.23

High CPU Process

Suspicious Process Found

nqcloud (PID: 1234) CPU: 98%

C2 Communication

Outbound Connection

External Connection

136.243.90.99

C2 Communication

Infected Endpoints

10.3.15.254 172.16.115.11

172.16.88.23

Threat Intelligence

FortiGuard Analysis

Malicious: Monero Miner

136.243.90.99



FortAI,
can you help me to fully investigate this incident?

FortiAI Reasoning Agent

- > 1. Understanding the request
- > 2. Check Server and Processes
- > 3. Check IP Reputation
- > 4. Check for more infected devices

136.243.90.99 is confirmed malicious, I need to see if other endpoints are connecting to it...

Found three affected devices:

- **10.3.15.254** (25s)
- **172.16.88.23** (2m 8s) - the slow server
- **172.16.115.11** (46s)

This suggests a broader security incident - Let me take a closer look at the slow server first.

Analyzing Output

Outbreak Detected

NEXT STEP >

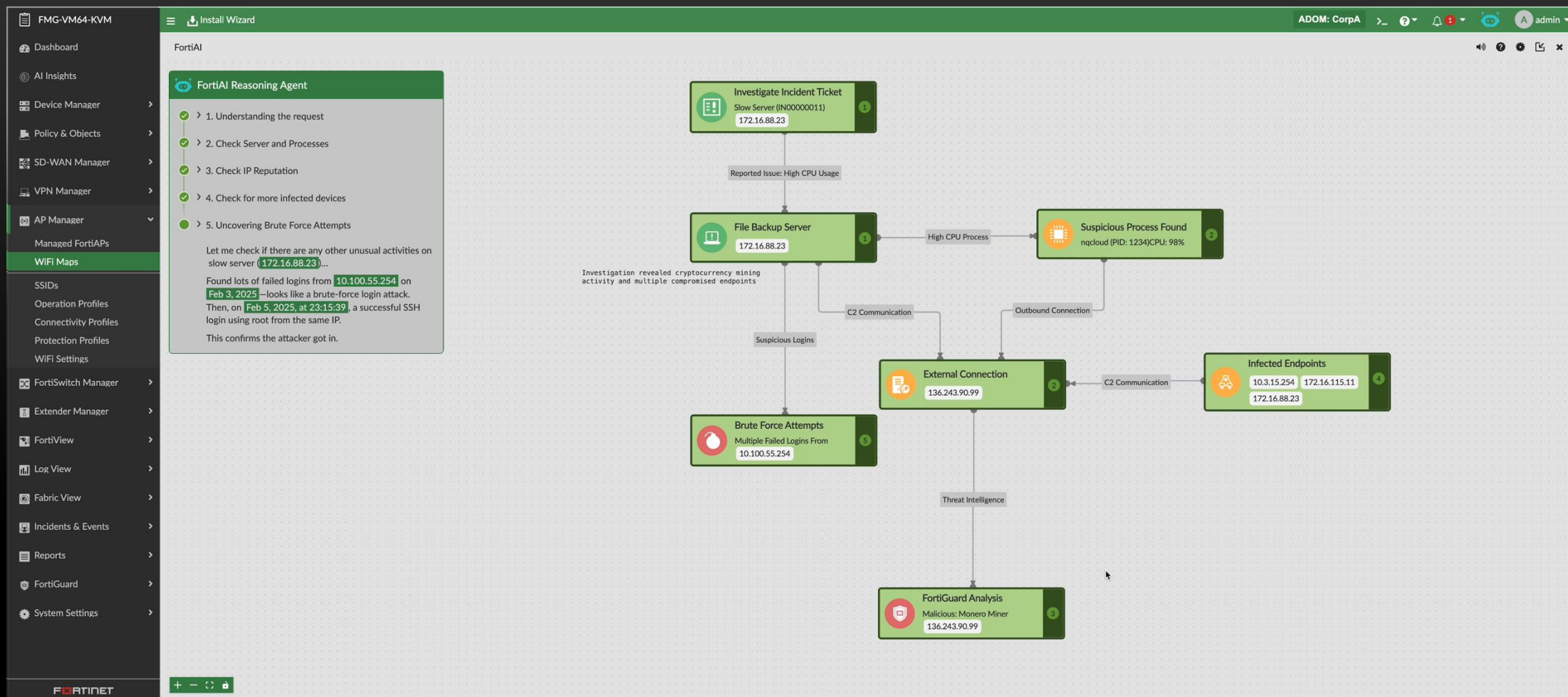
Investigate breach details
on the original server.



AI For FortiAnalyzer



FortAI,
can you help me to fully investigate this incident?





FortAI,
can you help me to fully investigate this incident?

FortiAI Reasoning Agent

- > 1. Understanding the request
- > 2. Check Server and Processes
- > 3. Check IP Reputation
- > 4. Check for more infected devices
- > 5. Uncovering Brute Force Attempts

Let me check if there are any other unusual activities on slow server (172.16.88.23)...

Found lots of failed logins from 10.100.55.254 on Feb 3, 2025 —looks like a brute-force login attack. Then, on Feb 5, 2025, at 23:15:39, a successful SSH login using root from the same IP.

This confirms the attacker got in.

Analyzing Output

Brute Force Attack Detected

NEXT STEP >

Generate incident report and
recommendations for action.



AI For FortiAnalyzer



FortAI,
can you help me to fully investigate this incident?

FMG-VM64-KVM

Dashboard

AI Insights

Device Manager

Policy & Objects

SD-WAN Manager

VPN Manager

AP Manager

Managed FortiAPs

WiFi Maps

SSIDs

Operation Profiles

Connectivity Profiles

Protection Profiles

WiFi Settings

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

Install Wizard

FortiAI

FortiAI Reasoning Agent

1. Understanding the request

2. Check Server and Processes

3. Check IP Reputation

4. Check for more infected devices

5. Uncovering Brute Force Attempts

Incident Summary

The slowness was due to a **Monero miner C2 connection** - attacker used a **brute force login** to access the server and spread to other endpoints.

Recommendations:

1. Quarantine Infected Systems

2. Block Malicious Traffic

3. Enforce Multiple Factor Authentication

4. Patch the vulnerable Systems

Call To Action

Quarantine Infected Systems

Block Malicious Traffic

Assign the Incident Ticket

Hand Over Incident

Send the Email to CISO

Download the Incident Report

Investigate Incident Ticket

Slow Server (IN00000011)
172.16.88.23

Reported Issue: High CPU Usage

File Backup Server
172.16.88.23

Suspicious Process Found
nqcloud (PID: 1234) CPU: 98%

High CPU Process

C2 Communication

Suspicious Logins

Brute Force Attempts
Multiple Failed Logins From
10.100.55.254

External Connection
136.243.90.99

Outbound Connection

C2 Communication

Infected Endpoints
10.3.15.254 172.16.115.11
172.16.88.23

Threat Intelligence

FortiGuard Analysis
Malicious: Monero Miner
136.243.90.99

Investigation revealed cryptocurrency mining activity and multiple compromised endpoints



FortAI,
can you help me to fully investigate this incident?

FortiAI Reasoning Agent

- ✓ > 1. Understanding the request
- ✓ > 2. Check Server and Processes
- ✓ > 3. Check IP Reputation
- ✓ > 4. Check for more infected devices
- ✓ > 5. Uncovering Brute Force Attempts

☐ Incident Summary

The slowness was due to a **Monero miner C2 connection** - attacker used a **brute force login** to access the server and spread to other endpoints.

Recommendations:

1. Quarantine Infected Systems
2. Block Malicious Traffic
3. Enforce Multiple Factor Authentication
4. Patch the vulnerable Systems

Would you like me to proceed?



The image features the Fortinet logo centered on a black background. The logo consists of the word "FORTINET" in a bold, white, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern. Surrounding the logo are several abstract geometric elements: a red horizontal bar in the top left, a red horizontal bar in the top right, a red horizontal bar in the bottom left, a red horizontal bar in the middle right, a grey grid of dots in the bottom right, and various grey squares and rectangles of different sizes and orientations scattered throughout the background.

FORTINET