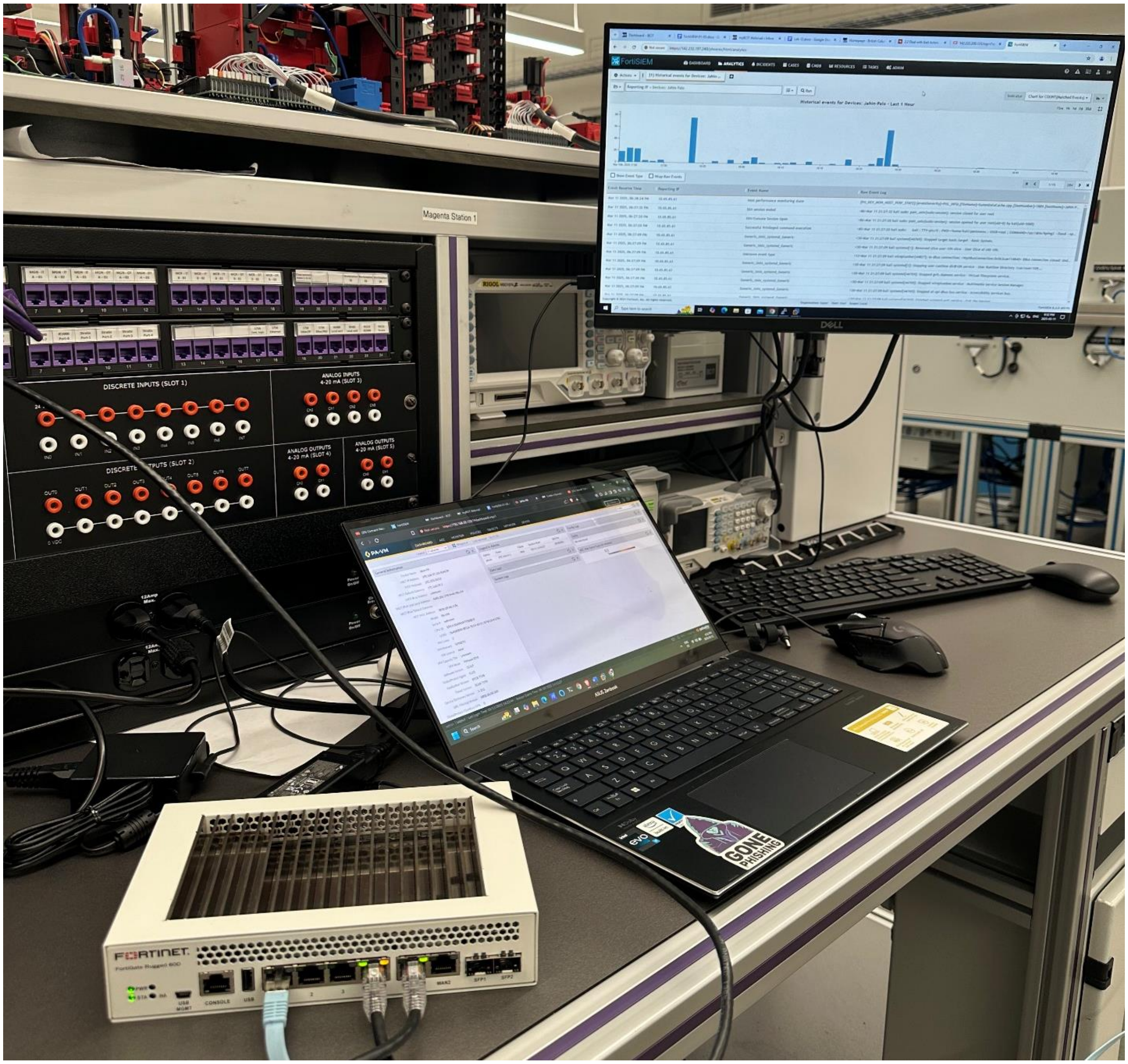
Advanced Cybersecurity (SOC) Lab for Threat Detection, Monitoring, Incident Response & Vulnerability Management

By **Md Muhtashim Jahin**

Date: Mar 11, 2025

This project simulates a fully functional enterprise-grade **Security Operations Center (SOC)** environment using **Fortinet**, **Cisco** & **Palo Alto** hardware and integrated cybersecurity platforms (**FortiSIEM**, **Suricata**, **Tenable Nessus**). This project performs Cyberattacks and supports real-time **Threat Detection** & **Monitoring**, **Incident Response**, and continuous **Vulnerability Management**, showcasing the workflows of a professional **Tier I/II SOC Analyst** & **SIEM Engineer**

Overview of Lab



The lab infrastructure consists of:

Firewalls: FortiGate Rugged 60D (Hardware) and Palo Alto NGFW (VM)

Router: Cisco ISR 4300 Router (Connected through Patch Panel), Cisco CSR Router (VM)

Switch: Cisco Catalyst C9200-48P (Connected through Patch Panel)

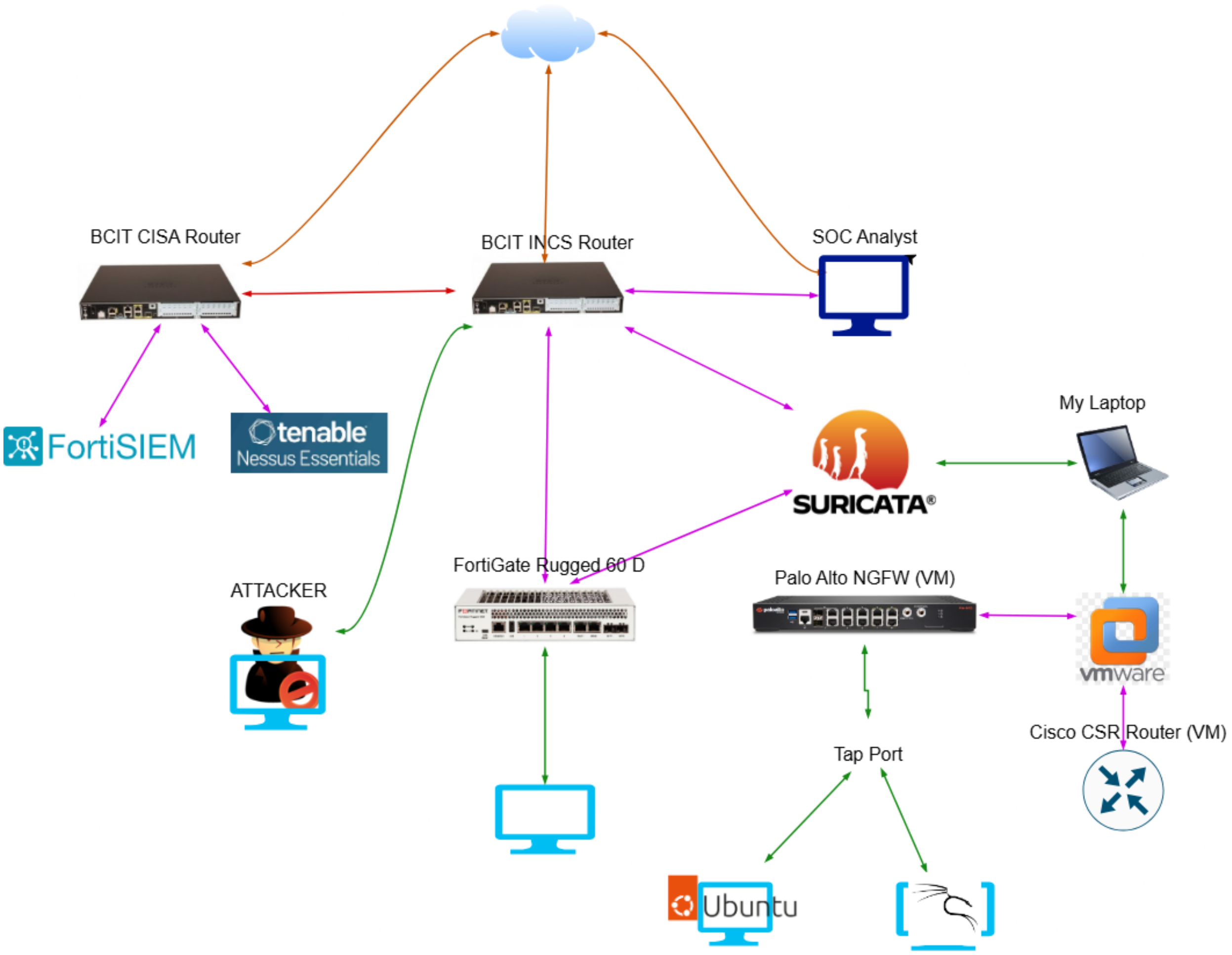
SIEM: FortiSIEM (Security Monitoring, Log Management Solution, Log Collector, Ticketing)

IDS: Suricata (NIDS/Network Intrusion Detection System)

Vulnerability Scanner: Tenable Nessus (API integrated with FortiSIEM)

All network devices and security appliances forward **Syslog** and **SNMP** logs to FortiSIEM, enabling centralized event correlation and Alert Generation.

Network Diagram



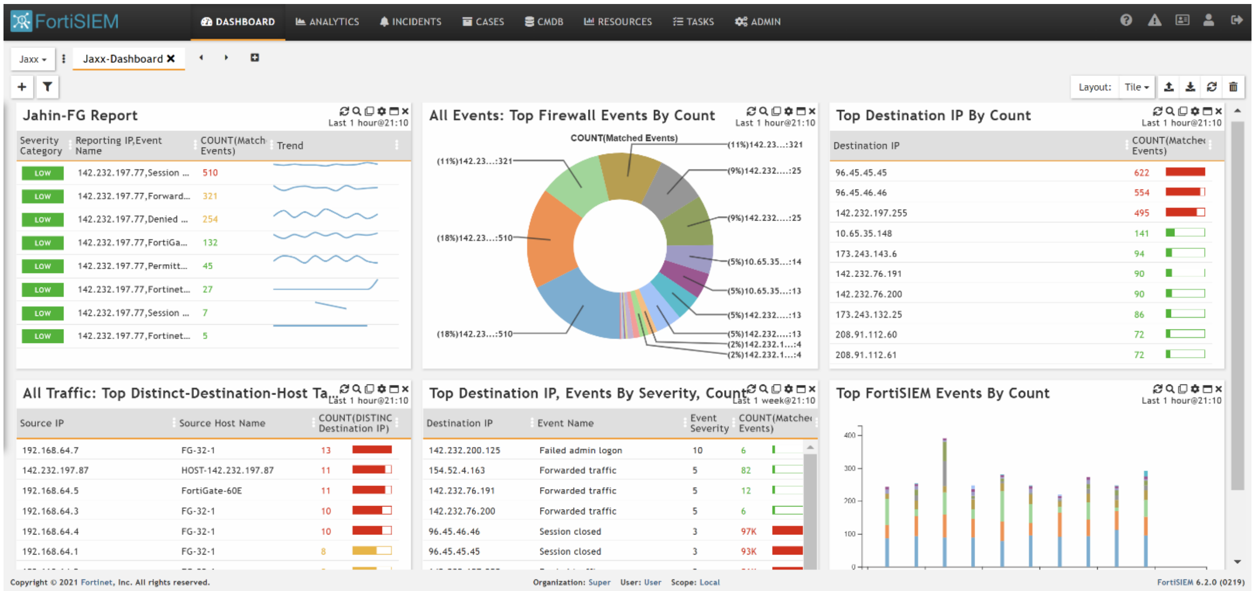
Custom **correlation rules** were created within FortiSIEM to **generate alerts** based on **event severity**, ranging from **low to critical**. To validate detection and response capabilities, a series of **controlled attacks** were executed from an attacker machine connected to the internet, including:

- Distributed Denial of Service (DDoS) Attacks
- Credential Dumping
- Dictionary Attacks

These simulated threats triggered FortiSIEM alerts, which were promptly analyzed and triaged. Incidents were tracked using FortiSIEM's integrated **ticketing system**, with documented workflows for investigation, containment, and remediation.

Active incident response was performed by blocking malicious IP addresses through firewall policies on both FortiGate and Palo Alto devices. Tickets were closed after verification of mitigation effectiveness via log review and vulnerability reassessment using Nessus.

FortiSIEM Dashboard



Jahin-FG Report

Last 1 hour@21:10

Severity Category	Reporting IP,Event Name	COUNT(Match Events)	Trend
LOW	142.232.197.77,Session ...	510	
LOW	142.232.197.77,Forward...	321	
LOW	142.232.197.77,Denied ...	254	
LOW	142.232.197.77,FortiGa...	132	
LOW	142.232.197.77,Permitt...	45	
LOW	142.232.197.77,Fortinet...	27	
LOW	142.232.197.77,Session ...	7	
LOW	142.232.197.77,Fortinet...	5	

All Events: Top Firewall Events By Count

Last 1 hour@21:10

Top Destination IP By Count

Last 1 hour@21:10

Destination IP	COUNT(Matched Events)
96.45.45.45	622
96.45.46.46	554
142.232.197.255	495
10.65.35.148	141
173.243.143.6	94
142.232.76.191	90
142.232.76.200	90
173.243.132.25	86
208.91.112.60	72
208.91.112.61	72

All Traffic: Top Distinct-Destination-Host Ta...

Last 1 hour@21:10

Source IP	Source Host Name	COUNT(DISTINC Destination IP)
192.168.64.7	FG-32-1	13
142.232.197.87	HOST-142.232.197.87	11
192.168.64.5	FortiGate-60E	11
192.168.64.3	FG-32-1	10
192.168.64.4	FG-32-1	10
192.168.64.1	FG-32-1	8

Top Destination IP, Events By Severity, Count

Last 1 week@21:10

Destination IP	Event Name	Event Severity	COUNT(Matched Events)
142.232.200.125	Failed admin logon	10	6
154.52.4.163	Forwarded traffic	5	82
142.232.76.191	Forwarded traffic	5	12
142.232.76.200	Forwarded traffic	5	6
96.45.46.46	Session closed	3	97K
96.45.45.45	Session closed	3	93K

Top FortiSIEM Events By Count

Last 1 hour@21:10

Copyright © 2021 Fortinet, Inc. All rights reserved.

Organization: Super User: User Scope: Local

FortiSIEM 6.2.0 (0219)

Component Configurations

Palo Alto NGFW:

- NAT.
- Policy Creation
- DoS Protection.
- TAP port for continuous packet capture, enabling deep traffic visibility and forensic analysis.

FortiGate Rugged 60D:

- NAT.
- Policy Creation

- DoS protection.
- Application Control.
- SSL inspection.
- Web Filtering.

Suricata IDS:

Edited detection rules to generate alerts on:

- Port scans
- SQL injection attempts
- ICMP ping probes originating from outside the network

FortiSIEM:

- Centralized log ingestion via **Syslog** and **SNMP** from all devices.
- Created custom correlation rules to generate severity-based alerts.
- Managed incident lifecycle using the integrated ticketing system.
- Custom Dashboard

Tenable Nessus:

- Integrated via API with FortiSIEM.

Cisco CSR Router:

- Provided core routing and switching infrastructure to support lab network segmentation and traffic flow.

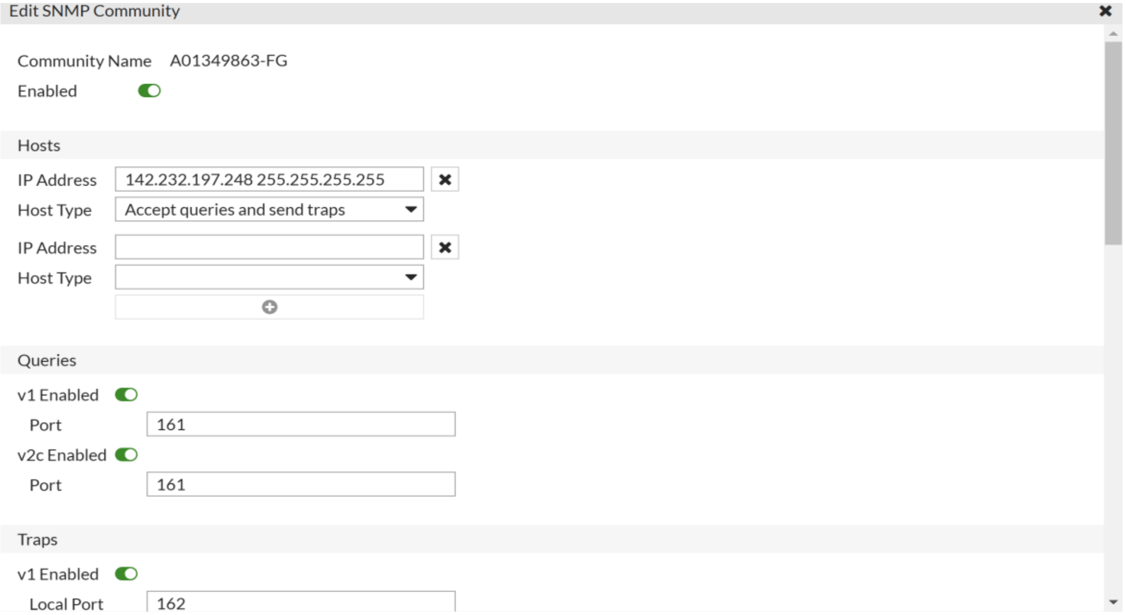
This lab reflects a real-world security operations environment that strengthens skills in threat detection, incident response, and vulnerability remediation using best-in-class hardware and software tools.

Connecting FortiGate, Palo Alto NGFW, Cisco CSR Router to send logs to FortiSIEM.

Configuring SNMP on FortiGate

1. Go to **System > SNMP** and create an SNMPv1/2 with the following information

Parameter	Value
Community Name	Up to you
IP Address	FortiSIEM IP Address
Agent	Enable



Edit SNMP Community

Community Name A01349863-FG

Enabled ●

Hosts

IP Address 142.232.197.248 255.255.255.255

Host Type Accept queries and send traps

IP Address

Host Type

Queries

v1 Enabled ●

Port 161

v2c Enabled ●

Port 161

Traps

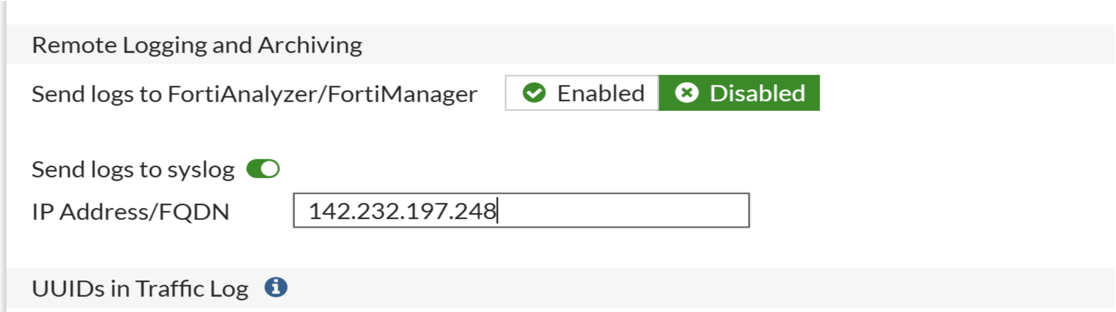
v1 Enabled ●

Local Port 162

Go to **FortiGate> Interfaces**, in administrative access, allow SNMP on the port connected to the NAT.

Configuring Syslog on FortiGate

1. Go to **Log& Report > Log Settings> Enable Send the Log to syslog** and enter the IP Address:**142.232.197.248**



Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager ✓ Enabled ☒ Disabled

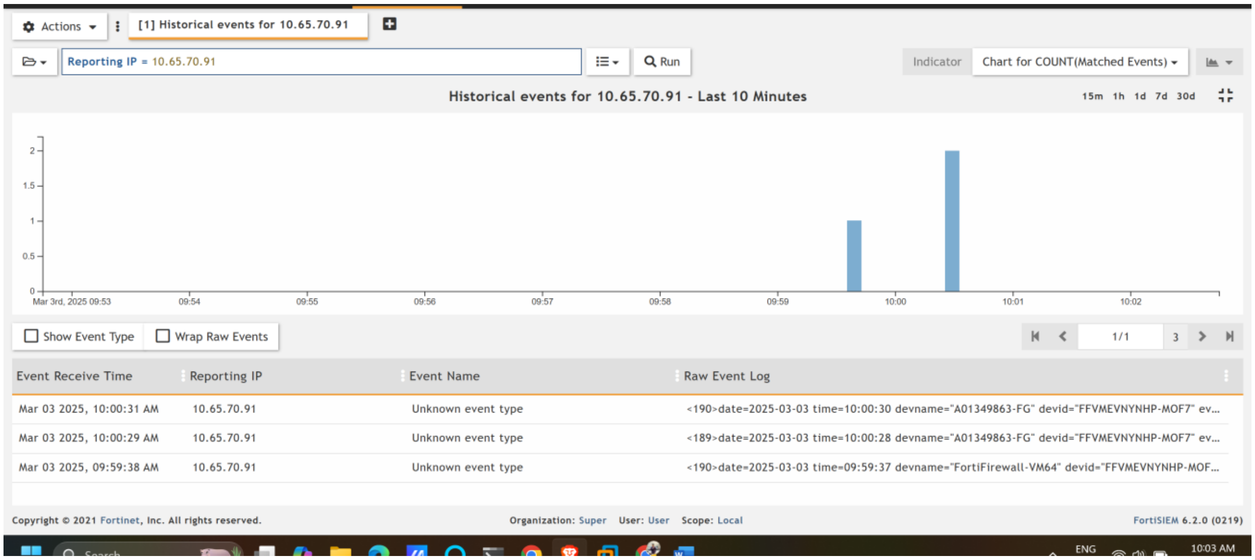
Send logs to syslog ●

IP Address/FQDN 142.232.197.248

UUIDs in Traffic Log

Go to FortiSIEM and navigate to **Analytics> Attributes.** Provide the following information:

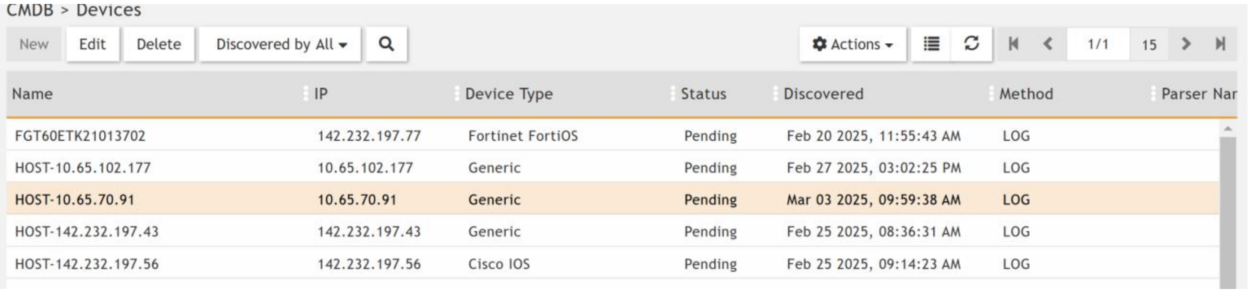
Attribute	**Value**
Reporting IP	Your FortiGate IP Address



Event Receive Time	Reporting IP	Event Name	Raw Event Log
Mar 03 2025, 10:00:31 AM	10.65.70.91	Unknown event type	<190>date=2025-03-03 time=10:00:30 devname="A01349863-FG" devid="FFVMEVNYNHP-MOF7" ev...
Mar 03 2025, 10:00:29 AM	10.65.70.91	Unknown event type	<189>date=2025-03-03 time=10:00:28 devname="A01349863-FG" devid="FFVMEVNYNHP-MOF7" ev...
Mar 03 2025, 09:59:38 AM	10.65.70.91	Unknown event type	<190>date=2025-03-03 time=09:59:37 devname="FortiFirewall-VM64" devid="FFVMEVNYNHP-MOF...

Copyright © 2021 Fortinet, Inc. All rights reserved. Organization: Super User: User Scope: Local FortiSIEM 6.2.0 (0219)

I



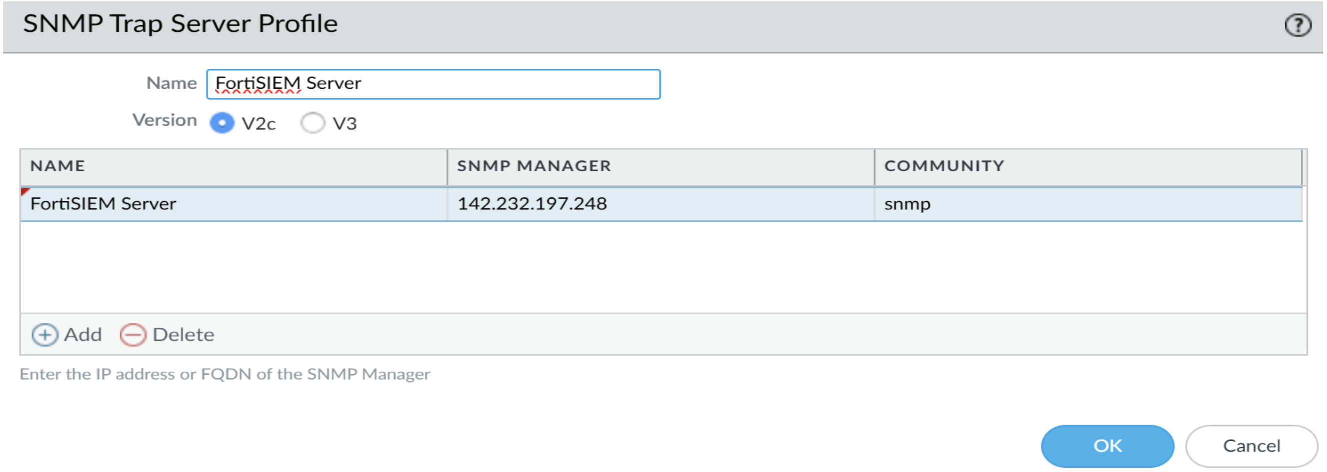
Name	IP	Device Type	Status	Discovered	Method	Parser Nar
FGT60ETK21013702	142.232.197.77	Fortinet FortiOS	Pending	Feb 20 2025, 11:55:43 AM	LOG	
HOST-10.65.102.177	10.65.102.177	Generic	Pending	Feb 27 2025, 03:02:25 PM	LOG	
HOST-10.65.70.91	10.65.70.91	Generic	Pending	Mar 03 2025, 09:59:38 AM	LOG	
HOST-142.232.197.43	142.232.197.43	Generic	Pending	Feb 25 2025, 08:36:31 AM	LOG	
HOST-142.232.197.56	142.232.197.56	Cisco IOS	Pending	Feb 25 2025, 09:14:23 AM	LOG	

n **CMDB>Firewalls,** to know your Firewall has been added successfully

Palo Alto NGFW SNMP & Syslog log forwarding to FortiSIEM

Configure SNMP

1. Log in to the management console for your firewall with administrator privileges.
2. In the **Device** tab, click **Setup**.
3. Click on **MGMT Interface Services**, make sure **SSH, Ping, and SNMP** are selected.
4. Go to **Device> SNMP Trap** and set your **SNMP** Manager and Community String. SNMP Manager should be Collector or Supervisor IP address (142.232.197.248).



SNMP Trap Server Profile

Name: FortiSIEM Server

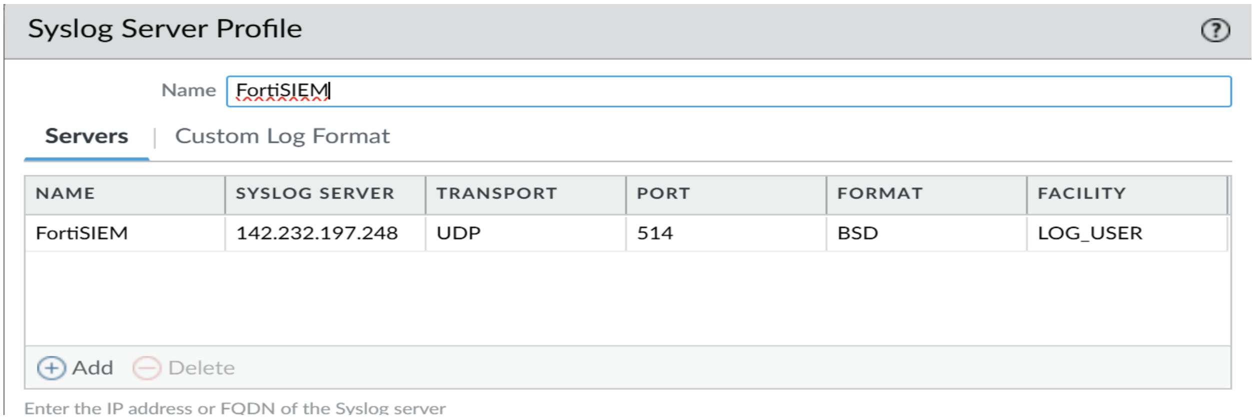
Version: ● V2c ○ V3

NAME	SNMP MANAGER	COMMUNITY
FortiSIEM Server	142.232.197.248	snmp

Enter the IP address or FQDN of the SNMP Manager

Configure Syslog

1. Create a profile for Syslog in the **Device > Syslog**. Syslog Server should be Collector or Supervisor IP address (142.232.197.248)



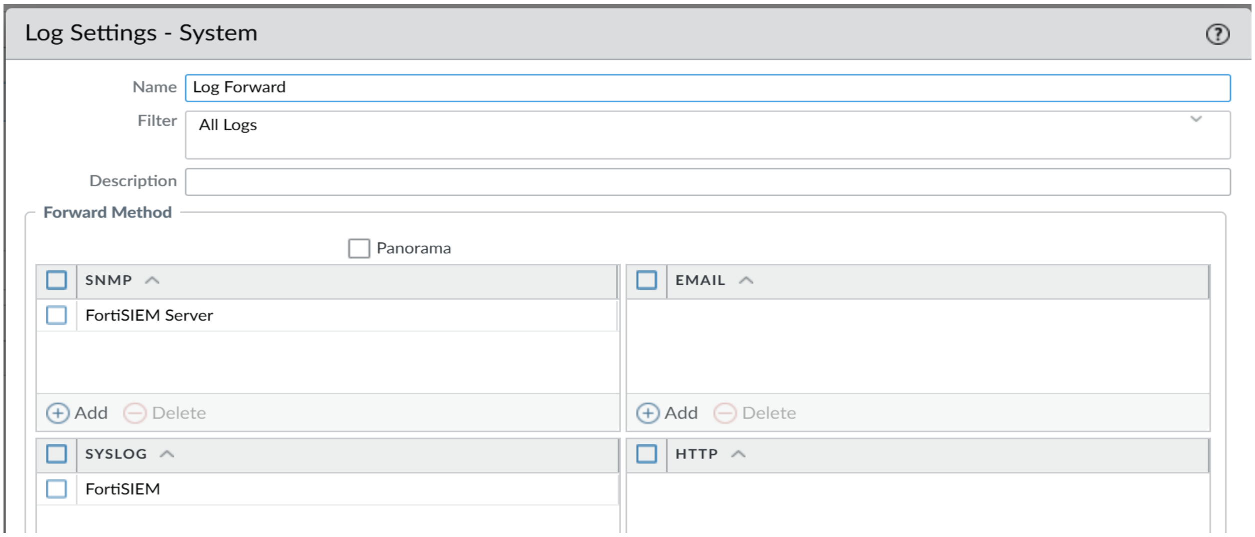
Syslog Server Profile

Name: FortiSIEM

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
FortiSIEM	142.232.197.248	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

Assign the SNMP and Syslog Profile you have created in the previous step in the **Device > log Settings> System**



Log Settings - System

Name: Log Forward

Filter: All Logs

Description:

Forward Method

□ Panorama

□	SNMP
□	FortiSIEM Server

□	EMAIL

□	SYSLOG
□	FortiSIEM

□	HTTP

Cisco CSR Router Syslog logs forward to FortiSIEM.

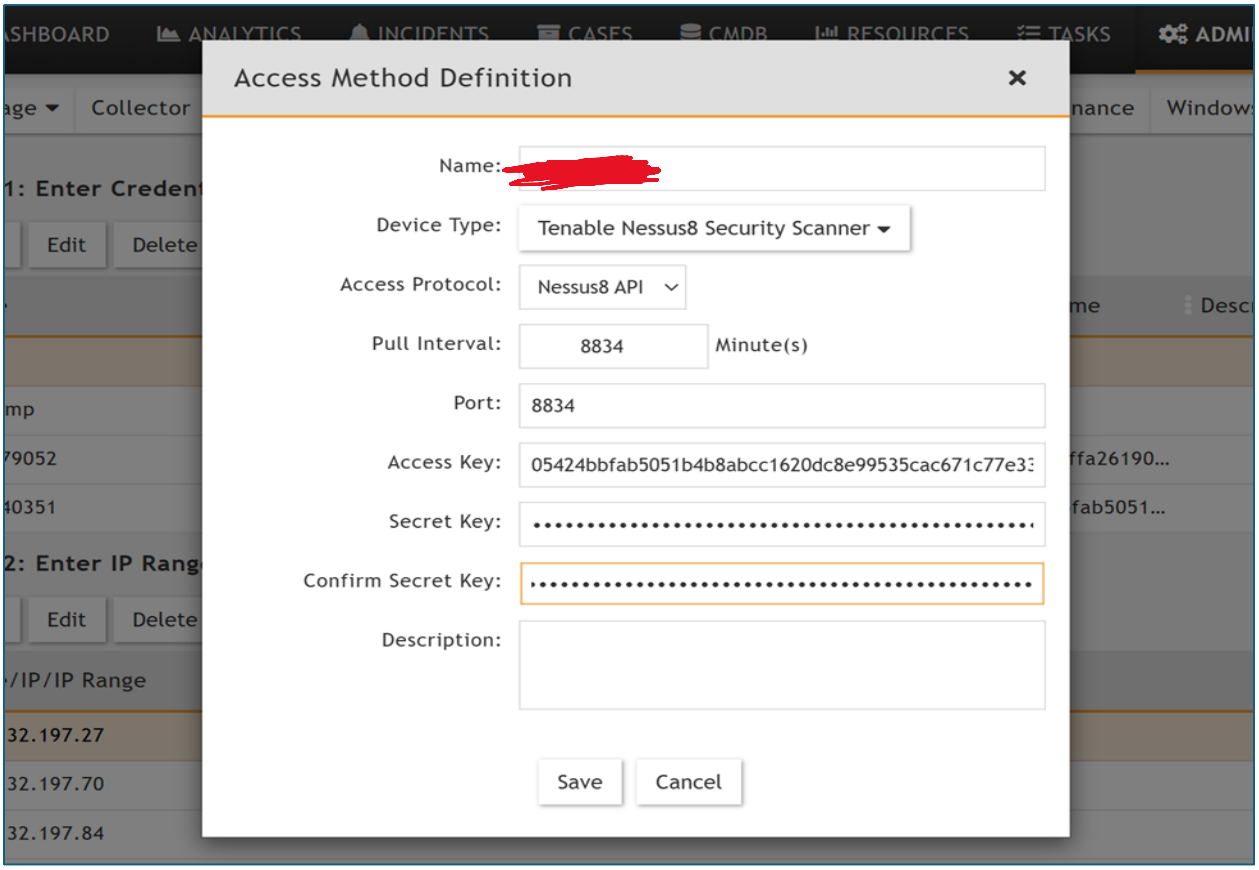
```
(config)# logging trap debugging
```

```
(config)# logging host [YOUR FortiSIEM SERVER IP] transport udp port 514
```

Connect Nessus API to FortiSIEM

Step 1: Enter Credentials

Go to ADMIN>SETUP> CREDENTIALS>New in FortiSIEM to create credentials.



Access Method Definition ×

Name: [redacted]

Device Type: Tenable Nessus8 Security Scanner

Access Protocol: Nessus8 API

Pull Interval: 8834 Minute(s)

Port: 8834

Access Key: 05424bbfab5051b4b8abcc1620dc8e99535cac671c77e33

Secret Key: ••

Confirm Secret Key: ••

Description:

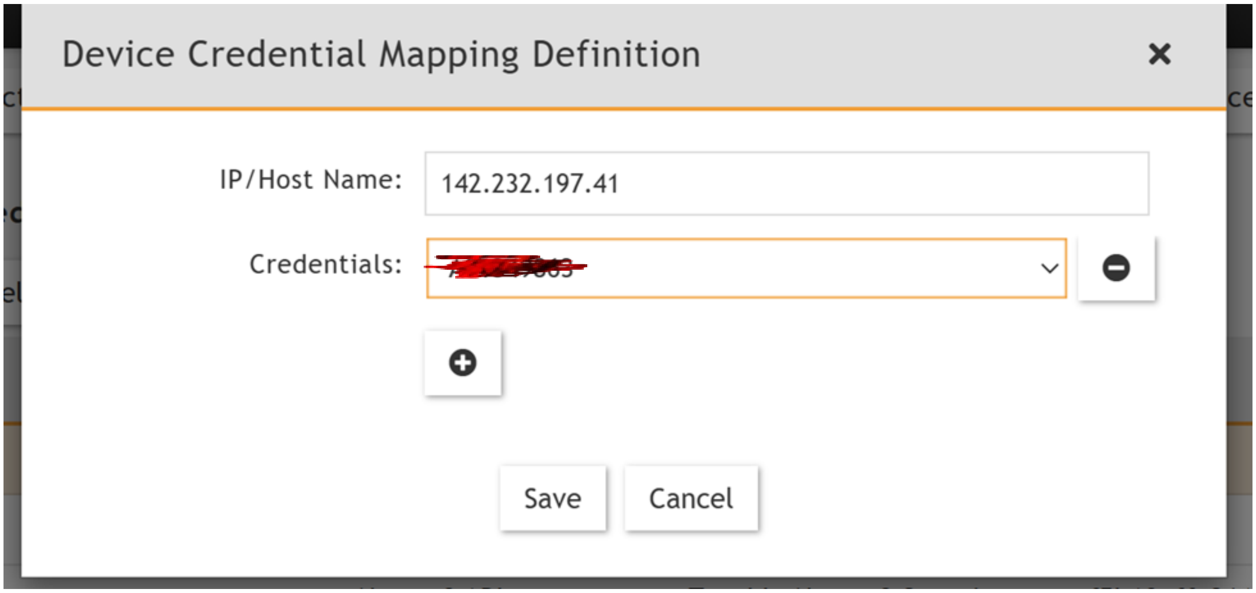
Save Cancel

Step 2: Enter IP Range to Credential Associations

Assign Nessus IP to the credentials you created in step1 with following information:

IP/Host Name: 142.232.1xx.x (Nessus Essentials host IP).

Credentials: Name of profile you created in Step1



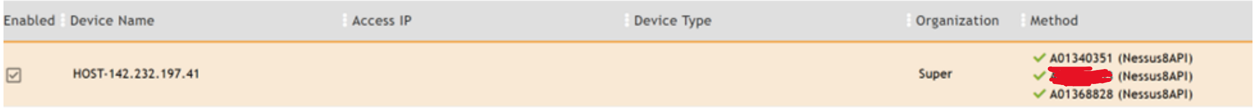
Device Credential Mapping Definition

IP/Host Name: 142.232.197.41

Credentials: [redacted]

Go to ADMIN -> Setup -> Pull Events

The yellow icon beside the Nessus pull job should turn green



Enabled	Device Name	Access IP	Device Type	Organization	Method
☑	HOST-142.232.197.41			Super	✓ A01340351 (Nessus8API) ✓ [redacted] (Nessus8API) ✓ A01368828 (Nessus8API)

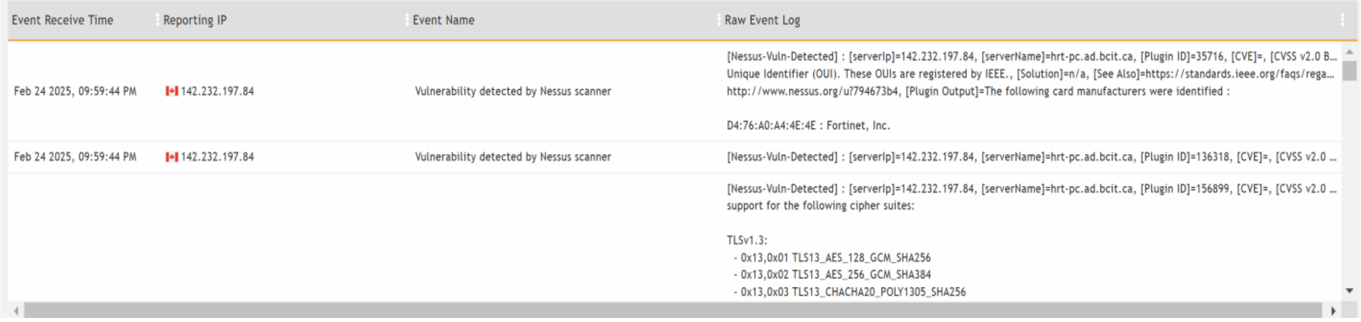
Threat Detection, Incident Response & Vulnerability Management

Vulnerability Management: Vulnerability management is a proactive process that involves identifying, assessing, prioritizing, and remediating security weaknesses of Systems & Software.

Nessus Essentials is a free vulnerability management tool, specifically a vulnerability scanner, developed by Tenable. It's used to identify security weaknesses and vulnerabilities in systems, software, and networks before attackers can exploit them. Nessus scans target systems, analyzes them for known vulnerabilities, and provides detailed reports with remediation recommendations.

I have integrated the Nessus Scanner API to FortiSIEM.

Nessus Logs in FortiSIEM.



Event Receive Time	Reporting IP	Event Name	Raw Event Log
Feb 24 2025, 09:59:44 PM	142.232.197.84	Vulnerability detected by Nessus scanner	[Nessus-Vuln-Detected] : [serverIp]=142.232.197.84, [serverName]=hrt-pc.ad.bcit.ca, [Plugin ID]=35716, [CVE]=, [CVSS v2.0 B... Unique Identifier (OUI). These OUIs are registered by IEEE., [Solution]=n/a, [See Also]=https://standards.ieee.org/faqs/rega... http://www.nessus.org/u?794673b4, [Plugin Output]=The following card manufacturers were identified : D4:76:A0:A4:4E:4E : Fortinet, Inc.
Feb 24 2025, 09:59:44 PM	142.232.197.84	Vulnerability detected by Nessus scanner	[Nessus-Vuln-Detected] : [serverIp]=142.232.197.84, [serverName]=hrt-pc.ad.bcit.ca, [Plugin ID]=136318, [CVE]=, [CVSS v2.0 ...
			[Nessus-Vuln-Detected] : [serverIp]=142.232.197.84, [serverName]=hrt-pc.ad.bcit.ca, [Plugin ID]=156899, [CVE]=, [CVSS v2.0 ... support for the following cipher suites: TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

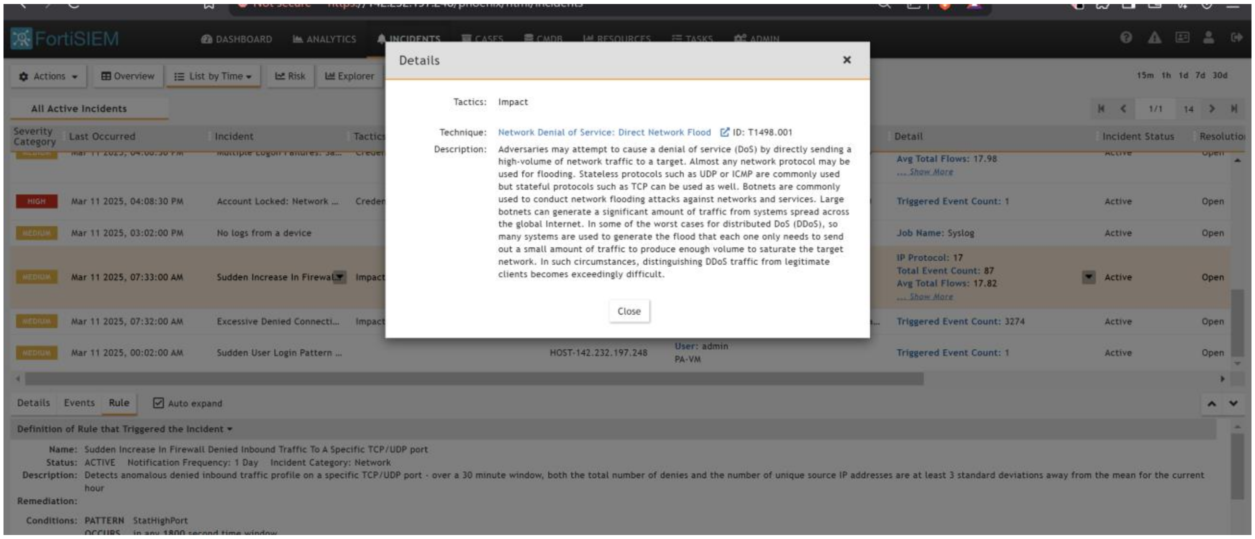
Threat Detection: Threat detection using SIEM (Security Information and Event Management) involves leveraging a centralized platform to monitor, analyze, and correlate security data from various sources to identify potential threats and security incidents. SIEM systems use log data, security alerts, and threat intelligence to detect unusual activities, policy violations, and suspicious patterns indicative of cyberattacks or insider threats.

All components in our Network are Sending Logs to FortiSIEM.

At first, the attacker launched a DDoS Attack on FortiGate Rugged 60D Firewall.

We can detect that on FortiSIEM.

DDoS Threat Detection on FortiSIEM



Severity Category	Last Occurred	Incident	Tactics			Detail	Incident Status	Resolution
MEDIUM	Mar 11 2025, 04:00:30 PM	Multiple Logon Failures: Sa...	Creden			Avg Total Flows: 17.98 ... Show More	Active	Open
HIGH	Mar 11 2025, 04:08:30 PM	Account Locked: Network ...	Creden			Triggered Event Count: 1	Active	Open
MEDIUM	Mar 11 2025, 03:02:00 PM	No logs from a device				Job Name: Syslog	Active	Open
MEDIUM	Mar 11 2025, 07:33:00 AM	Sudden Increase In Firewal	Impact			IP Protocol: 17 Total Event Count: 87 Avg Total Flows: 17.82 ... Show More	Active	Open
MEDIUM	Mar 11 2025, 07:32:00 AM	Excessive Denied Connecti...	Impact			Triggered Event Count: 3274	Active	Open
MEDIUM	Mar 11 2025, 00:02:00 AM	Sudden User Login Pattern ...		HOST-142.232.197.248	User: admin PA-VM	Triggered Event Count: 1	Active	Open

Details

Tactics: Impact

Technique: Network Denial of Service: Direct Network Flood ID: T1498.001

Description: Adversaries may attempt to cause a denial of service (DoS) by directly sending a high-volume of network traffic to a target. Almost any network protocol may be used for flooding. Stateless protocols such as UDP or ICMP are commonly used but stateful protocols such as TCP can be used as well. Botnets are commonly used to conduct network flooding attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global Internet. In some of the worst cases for distributed DoS (DDoS), so many systems are used to generate the flood that each one only needs to send out a small amount of traffic to produce enough volume to saturate the target network. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult.

Close

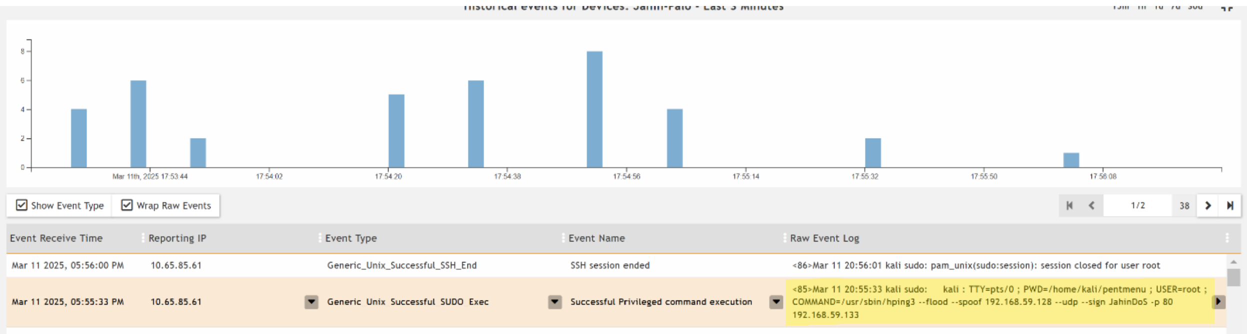
Details Events Rule ☑ Auto expand

Definition of Rule that Triggered the Incident

Name: Sudden Increase In Firewall Denied Inbound Traffic To A Specific TCP/UDP port
Status: ACTIVE Notification Frequency: 1 Day Incident Category: Network
Description: Detects anomalous denied inbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denies and the number of unique source IP addresses are at least 3 standard deviations away from the mean for the current hour
Remediation:
Conditions: PATTERN StatHighPort
OCCURS in any 1800 second time window

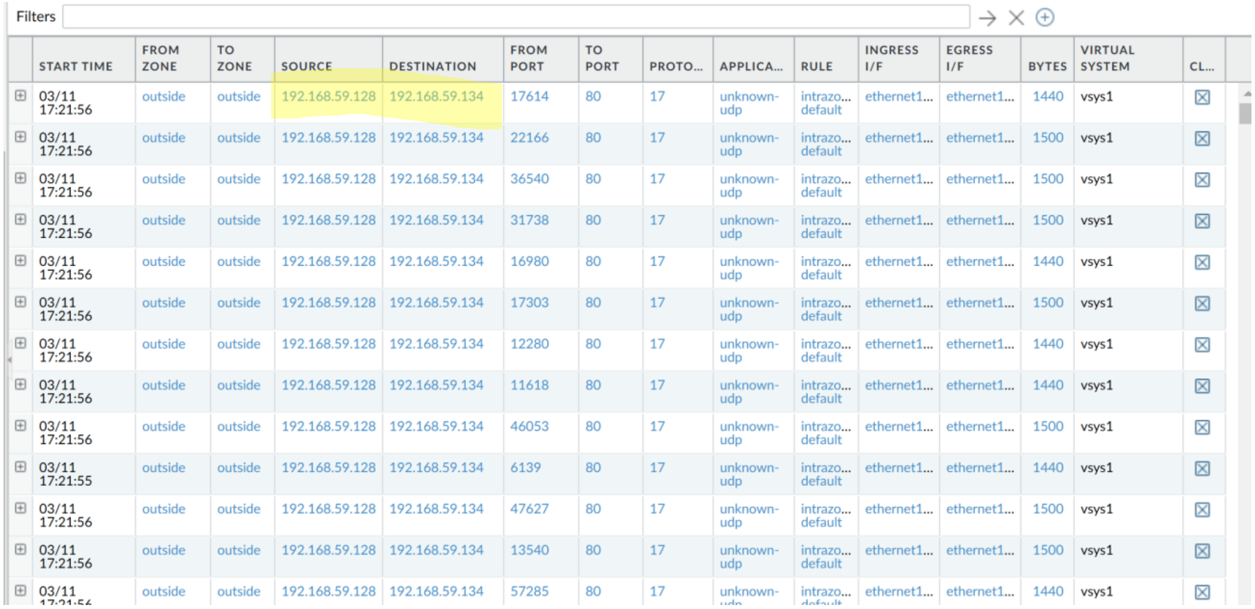
The attacker launched a UDP Flood on the Palo Alto Firewall.

UDP Flood Detection on FortiSIEM



Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log
Mar 11 2025, 05:56:00 PM	10.65.85.61	Generic_Unix_Successful_SSH_End	SSH session ended	<86>Mar 11 20:56:01 kali sudo: pam_unix(sudo:session): session closed for user root
Mar 11 2025, 05:55:33 PM	10.65.85.61	Generic Unix Successful SUDO Exec	Successful Privileged command execution	<85>Mar 11 20:55:33 kali sudo: kali : TTY=pts/0 ; PWD=/home/kali/pentmenu ; USER=root ; COMMAND=/usr/sbin/hping3 --flood --spoof 192.168.59.128 --udp --sign JahinDoS -p 80 192.168.59.133

Palo Alto UDP Flood



	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTO...	APPLICA...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CL...
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	17614	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	22166	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	36540	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	31738	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	16980	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	17303	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	12280	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	11618	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	46053	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:55	outside	outside	192.168.59.128	192.168.59.134	6139	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	47627	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	13540	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1500	vsys1	☒
⊞	03/11 17:21:56	outside	outside	192.168.59.128	192.168.59.134	57285	80	17	unknown-udp	intrazo... default	ethernet1...	ethernet1...	1440	vsys1	☒

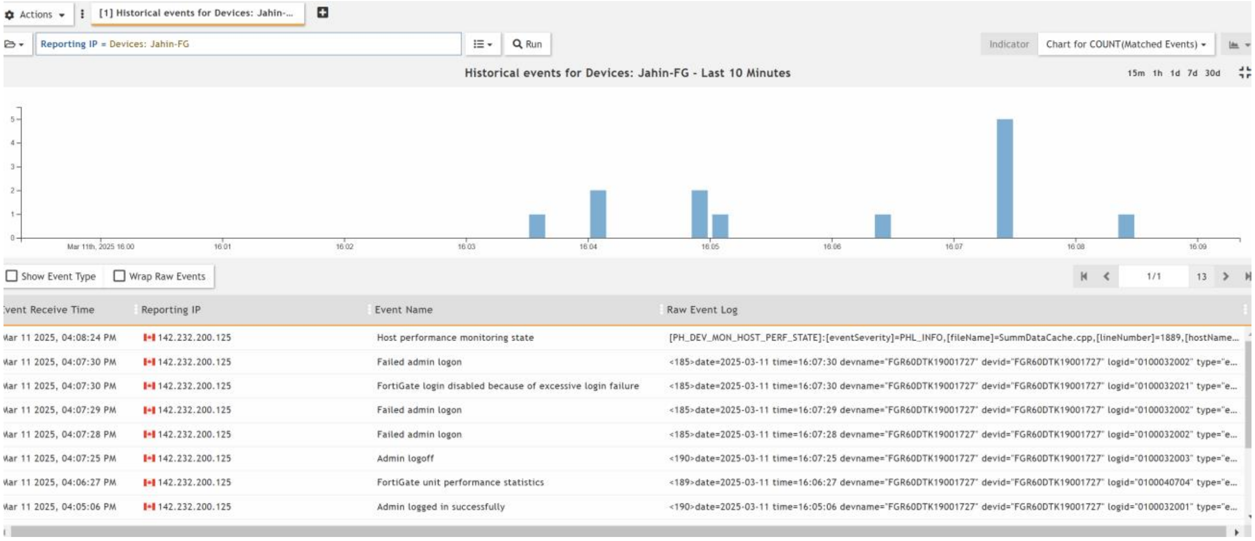
Later, the Attacker did a Credential Dump and a Brute-Force attack on the FortiGate Firewall. Through FortiSIEM, I can detect that FortiSIEM generated Incidents and Events, the severity is high, as I made the rule to generate a High Alert.

Difference between Credential Dump and Brute-Force Attack: A Credential Dump attack and a Brute-Force attack are both methods used by attackers to gain unauthorized access to accounts, but they differ in their approach.

A credential dump attack leverages lists of leaked or stolen username/password combinations, often obtained from previous data breaches.

A brute force attack, on the other hand, systematically tries different username and password combinations until the correct one is found, regardless of whether they are leaked or not.

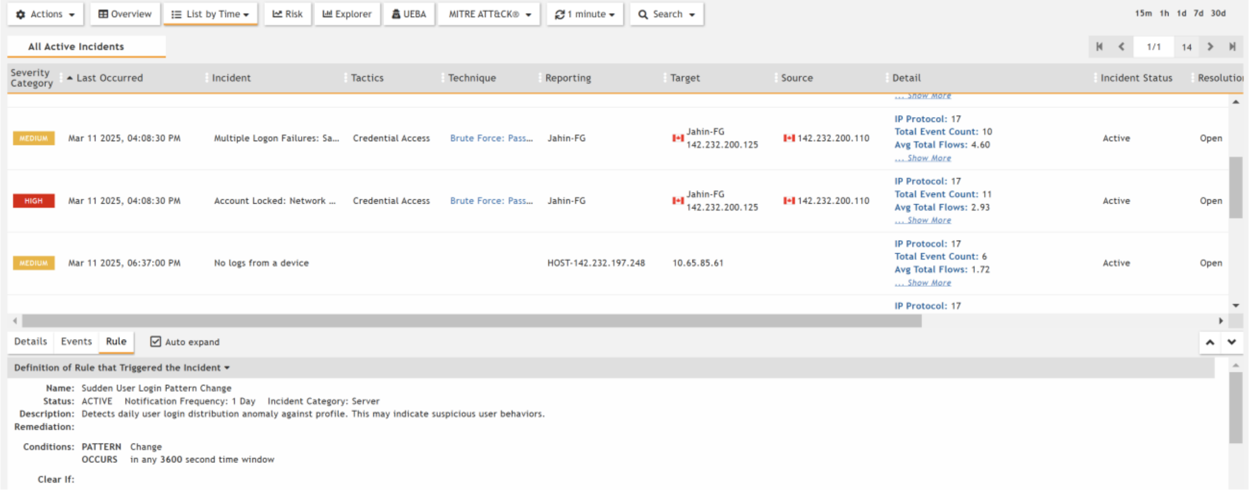
FortiGate Credential Dump Attempt Detection



Historical events for Devices: Jahin-FG - Last 10 Minutes

Event Receive Time	Reporting IP	Event Name	Raw Event Log
Mar 11 2025, 04:08:24 PM	142.232.200.125	Host performance monitoring state	[PH_DEV_MON_HOST_PERF_STATE]:[eventSeverity]=PHL_INFO,[fileName]=SummDataCache.cpp,[lineNumber]=1889,[hostName...
Mar 11 2025, 04:07:30 PM	142.232.200.125	Failed admin logon	<185>date=2025-03-11 time=16:07:30 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032002" type="e...
Mar 11 2025, 04:07:30 PM	142.232.200.125	FortiGate login disabled because of excessive login failure	<185>date=2025-03-11 time=16:07:30 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032021" type="e...
Mar 11 2025, 04:07:29 PM	142.232.200.125	Failed admin logon	<185>date=2025-03-11 time=16:07:29 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032002" type="e...
Mar 11 2025, 04:07:28 PM	142.232.200.125	Failed admin logon	<185>date=2025-03-11 time=16:07:28 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032002" type="e...
Mar 11 2025, 04:07:25 PM	142.232.200.125	Admin logoff	<190>date=2025-03-11 time=16:07:25 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032003" type="e...
Mar 11 2025, 04:06:27 PM	142.232.200.125	FortiGate unit performance statistics	<189>date=2025-03-11 time=16:06:27 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100040704" type="e...
Mar 11 2025, 04:05:06 PM	142.232.200.125	Admin logged in successfully	<190>date=2025-03-11 time=16:05:06 devname="FGR60DTK19001727" devid="FGR60DTK19001727" logid="0100032001" type="e...

Brute-Force Incident Alert was generated by FortiSIEM after detecting the brute force attempt pattern mentioned in the rule.



Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Target	Source	Detail	Incident Status	Resolutio
MEDIUM	Mar 11 2025, 04:08:30 PM	Multiple Logon Failures: Sa...	Credential Access	Brute Force: Pass...	Jahin-FG	Jahin-FG 142.232.200.125	142.232.200.110	IP Protocol: 17 Total Event Count: 10 Avg Total Flows: 4.60 ... Show More	Active	Open
HIGH	Mar 11 2025, 04:08:30 PM	Account Locked: Network ...	Credential Access	Brute Force: Pass...	Jahin-FG	Jahin-FG 142.232.200.125	142.232.200.110	IP Protocol: 17 Total Event Count: 11 Avg Total Flows: 2.93 ... Show More	Active	Open
MEDIUM	Mar 11 2025, 06:37:00 PM	No logs from a device			HOST-142.232.197.248	10.65.85.61		IP Protocol: 17 Total Event Count: 6 Avg Total Flows: 1.72 ... Show More	Active	Open
								IP Protocol: 17		

Definition of Rule that Triggered the Incident

```
         Name:  Sudden User Login Pattern Change
       Status:  ACTIVE    Notification Frequency: 1 Day    Incident Category: Server
  Description:  Detects daily user login distribution anomaly against profile. This may indicate suspicious user behaviors.
  Remediation:

   Conditions:  PATTERN   Change
                OCCURS    in any 3600 second time window

     Clear If:
```

Incident Response

Incident response in a Security Operations Center (SOC) is the process of detecting, analyzing, containing, and recovering from security incidents like cyberattacks or data breaches.

Incident Response Plan for Detected Threats

Incident Type: Denial-of-Service (DoS) / UDP Flood Attack

1. Detection & Alerting

- FortiSIEM received **Syslog/SNMP alerts** from both FortiGate and Palo Alto firewalls.
- Predefined **correlation rules** triggered security incidents based on:

    - Unusual volume of traffic
    - Repeated UDP packet patterns
    - Connection attempts to closed ports (port 80 on Palo Alto, ICMP Echo DDoS Attack on FortiGate)
- Alerts tagged as "Sudden Increase in Firewall Denied Inbound Traffic/DDoS" with **Severity**.

2. Initial Triage

I reviewed the incidents in FortiSIEM's **incident**

- **management console**.
- Verified:
    - **Source IPs** and affected destination interfaces/services.
    - **Traffic volume and frequency** from the logs.

3. Investigation

- Performed **log analysis** across:
    - FortiGate & Palo Alto logs in FortiSIEM.
    - Suricata IDS alerts (for any lateral or additional abnormal behavior).
- Used **FortiSIEM dashboards** and **event drilldowns** to:
    - Confirm multiple high-rate connections from **specific external IPs**.
    - Identify patterns matching UDP flood and generic DDoS behavior.

4. Containment

- Added **firewall block rules**:
    - Blocked attacker IP (142.232.200.110 & 192.168.59.128) on both FortiGate and Palo Alto.
- Verified containment by:
    - Confirmed drop in alert volume.

5. Eradication & Recovery

- Ensured firewalls were no longer receiving malicious traffic.
- Rechecked **Suricata** and FortiSIEM to confirm no residual activity.
- Ran **Nessus scan** to ensure no new vulnerabilities were exposed or exploited during the attack.

6. Incident Closure

- Updated the **ticket in FortiSIEM** with:
    - Description of the attack
    - Source IPs involved
    - Timeline of detection and response
    - Actions taken (blocking, validation, containment)