

FORIGATE FIREWALL

Network Security Integration



ABOUT FortiGate

FortiGate is a next-generation firewall developed by Fortinet, a well-known Cybersecurity Company.

It is a hardware or virtual security appliance that provides network protection, visibility and control by combining traditional firewall functions with advanced security features.

FortiGate allows centralized logging and monitoring via FortiAnalyzer and integrates with other Fortinet product like FortiManager, FortiClient, and FortiAP.

It is widely used in enterprises, banks, and government networks for securing internet access, controlling traffic, blocking threats, and setting up secure VPNs.



Key-Security Functions

FUNCTIONS

- Application Control
- Web Filtering
- Intrusion Prevention System
- Antivirus & Antimalware
- SSL Inspection
- Sandboxing



Difference between Traditional and NGFW Firewall

Feature	Traditional Firewall	Next-Generation Firewall (NGFW)
1. Traffic Filtering Level	Filters traffic based on IP address, port, and protocol only.	Filters IP, Port, Protocol + Application + User + Content
2. Application Identification	Cannot identify applications	Identifies apps like YouTube, Facebook, SSH, BitTorrent
3. Security Capabilities	Provides only basic packet filtering and NAT.	Includes advanced security features like IPS, Antivirus, Web Filtering, SSL Inspection.
4. Threat Detection	Limited protection — cannot detect modern threats.	Detects and blocks zero-day, malware, and intrusion attacks using real-time threat intelligence.
5. Visibility & Control	Provides minimal visibility into user activity.	Offers user- and application-level visibility with detailed monitoring and reporting.
6. User Identification & Visibility	Tracks only network IPs, not users or applications.	Provides user-based visibility and control , integrates with Active Directory for identity-based policies.

COMMON THREATS

COMMON THREATS

Threats	Description	FortiGate Protection
• Phishing	• Fake emails/websites tricking users for credentials	• Web filtering, DNS filtering, malicious URL blocking
• SQL Injection / Web Exploits	• Exploiting web application vulnerabilities	• IPS signatures, Web Application Firewall (WAF)
• Brute Force Attacks	• Multiple login attempts to crack passwords	• IPS, login attempt monitoring, geo-blocking
• DDoS (Denial of Service)	• Flooding servers to make them unavailable	• DoS protection, traffic shaping, rate limiting

Advantages of FortiGate Firewall	Challenges of FortiGate Firewall
<ul style="list-style-type: none"> Next-Generation Security – Combines firewall, antivirus, IPS, web filtering, and application control in one device (UTM). 	<ul style="list-style-type: none"> Licensing Costs – Subscription (FortiGuard services) needed for full protection; can be expensive long-term.
<ul style="list-style-type: none"> High Performance – Uses custom FortiASIC processors for faster packet inspection. 	<ul style="list-style-type: none"> Complexity in Large Deployments – Advanced features (like IPS tuning, SSL inspection) require expertise.
<ul style="list-style-type: none"> User-Friendly GUI & CLI – Easy for beginners via GUI, advanced control via CLI. 	<ul style="list-style-type: none"> Learning Curve – Beginners may find CLI configurations and advanced security features difficult.
<ul style="list-style-type: none"> VLAN & Network Segmentation – Supports inter-VLAN routing with security policies. 	<ul style="list-style-type: none"> Performance Drop with Deep Inspection – SSL/TLS deep inspection and heavy IPS rules may reduce throughput.
<ul style="list-style-type: none"> Centralized Management – With FortiManager & FortiAnalyzer, admins can manage multiple firewalls and analyze logs centrally. 	<ul style="list-style-type: none"> Limited Compatibility – Some third-party integrations may be less flexible compared to Palo Alto or Check Point.
<ul style="list-style-type: none"> Traffic Shaping & QoS – Controls bandwidth per user/application (good for Guest vs Admin VLANs). 	<ul style="list-style-type: none"> Frequent Updates Required – Needs regular firmware updates and threat database updates for maximum security.
<ul style="list-style-type: none"> Cloud & VPN Support – Site-to-site and remote-access VPNs; supports AWS, Azure, GCP deployments. 	<ul style="list-style-type: none"> Support & Documentation – Community support is smaller compared to Cisco, though official Fortinet support is available.

FUTURE TRENDS

FortiGate firewalls are set to advance with **AI-driven threat detection**, **Zero Trust Network Access (ZTNA)**, and stronger **cloud integration** across AWS, Azure, and Google Cloud. With the rapid growth of **IoT devices**, **5G**, and **edge computing**, FortiGate will play a key role in delivering enhanced security beyond traditional networks. Additionally, its expanding role in **SD-WAN adoption** and **SOC/SIEM integration** will ensure smarter, faster, and more automated protection against emerging cyber threats.



FortiGate Firewall

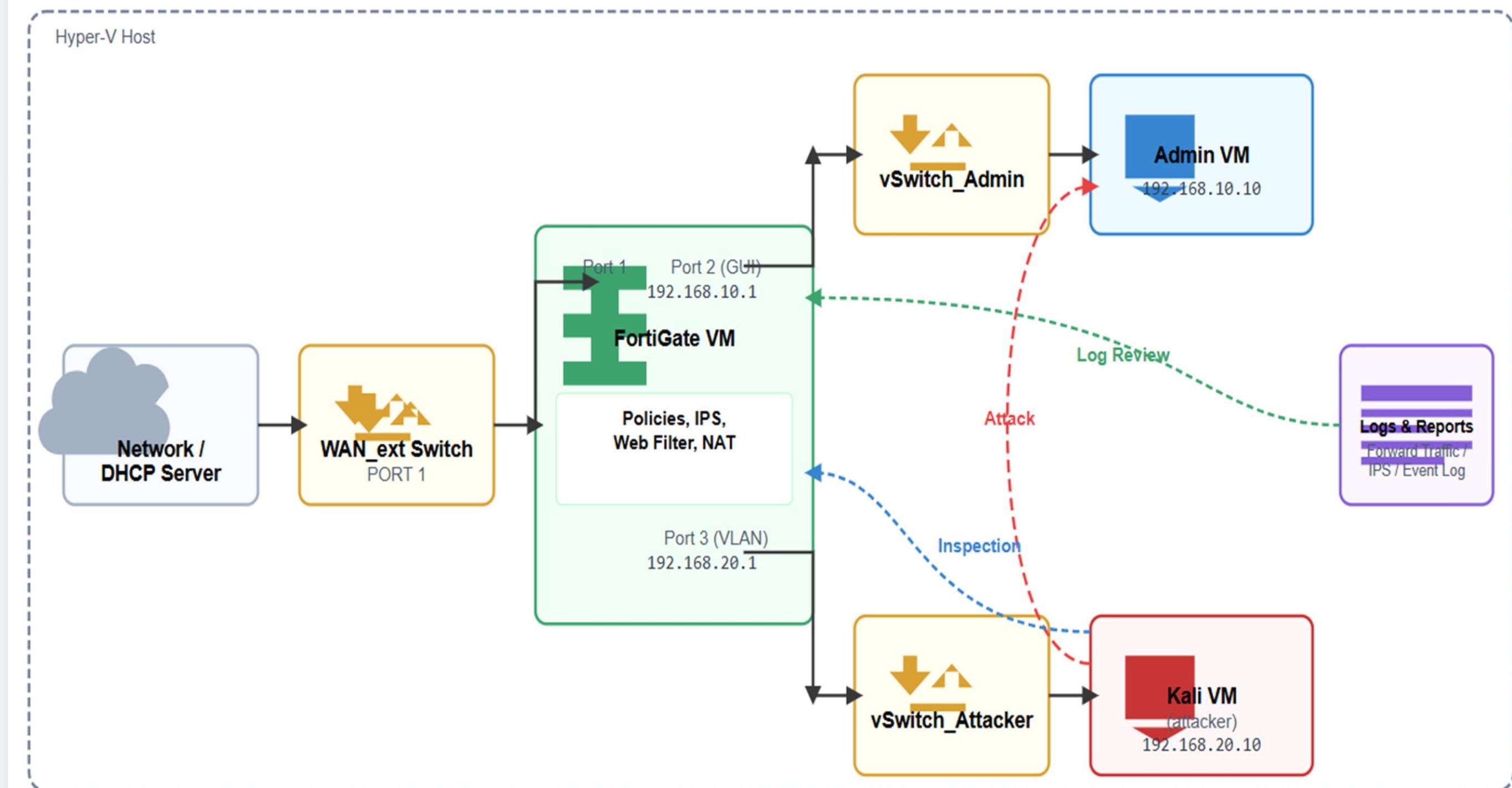


Diagram Key

- | | | | | | |
|---|--|---|---|---|---|
| ○ Network / DHCP | ○ Switch / vSwitch | ○ FortiGate (Firewall) | ○ Admin VM | ○ Attacker VM | ○ Logs & Reports |
| → Attack Path | → Inspection Path | → Log Path | → Standard Traffic | ○ Hyper-V Host | |

Configured Interfaces in GUI of FortiGate firewall

The image shows three separate windows of the FortiGate GUI, each titled "Edit Interface".

- port1 (WAN):** Name: WAN (port1), Alias: WAN, Type: Physical Interface, VRF ID: 0, Role: WAN. Addressing mode: DHCP. IP/Netmask: 192.168.10.1/255.255.255.0. Administrative Access: IPv4 - HTTPS, HTTP, PING, SSH, RADIUS Accounting, FTM, Speed Test, LLDP. IPv6 - None.
- port2 (ADMIN):** Name: ADMIN_LAN (port2), Alias: ADMIN_LAN, Type: Physical Interface, VRF ID: 0, Role: Undefined. Addressing mode: Manual. IP/Netmask: 192.168.10.1/255.255.255.0. Secondary IP address: None. Administrative Access: IPv4 - HTTPS, HTTP, PING, SSH, RADIUS Accounting, FTM, Speed Test, LLDP. IPv6 - None.
- port3 (ATTACKER):** Name: ATTACKER (port3), Alias: ATTACKER, Type: Physical Interface, VRF ID: 0, Role: Undefined. Addressing mode: Manual. IP/Netmask: 192.168.20.1/255.255.255.0. Secondary IP address: None. Administrative Access: IPv4 - HTTPS, HTTP, PING, SSH, RADIUS Accounting, FTM, Speed Test, LLDP. IPv6 - None.

port1 (WAN)

Alias: WAN

Role: WAN

Addressing mode: **DHCP** (or
Static IP if your WAN has static)

Allow Access: **keep ping HTTPS**
HTTP SSH

Save.

port2 (ADMIN)

Alias: ADMIN_LAN

Addressing mode: **Manual**

IP/Netmask: **192.168.10.1/24**

Administrative Access: check
HTTPS (and optionally **SSH** but
restrict later)

OK / Save.

port3 (ATTACKER)

Alias: ATTACKER

Addressing mode: **Manual**

IP/Netmask: **192.168.20.1/24**

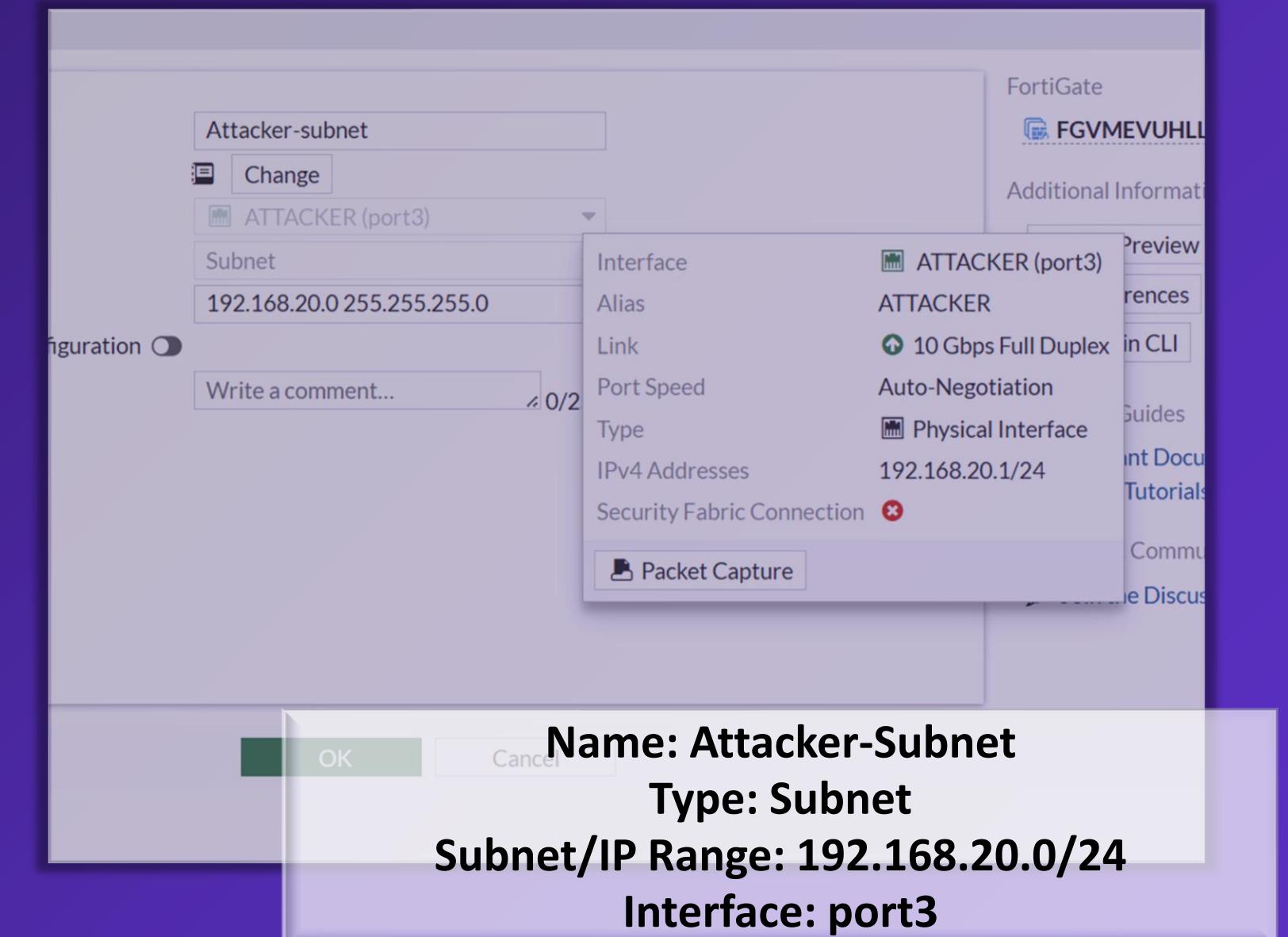
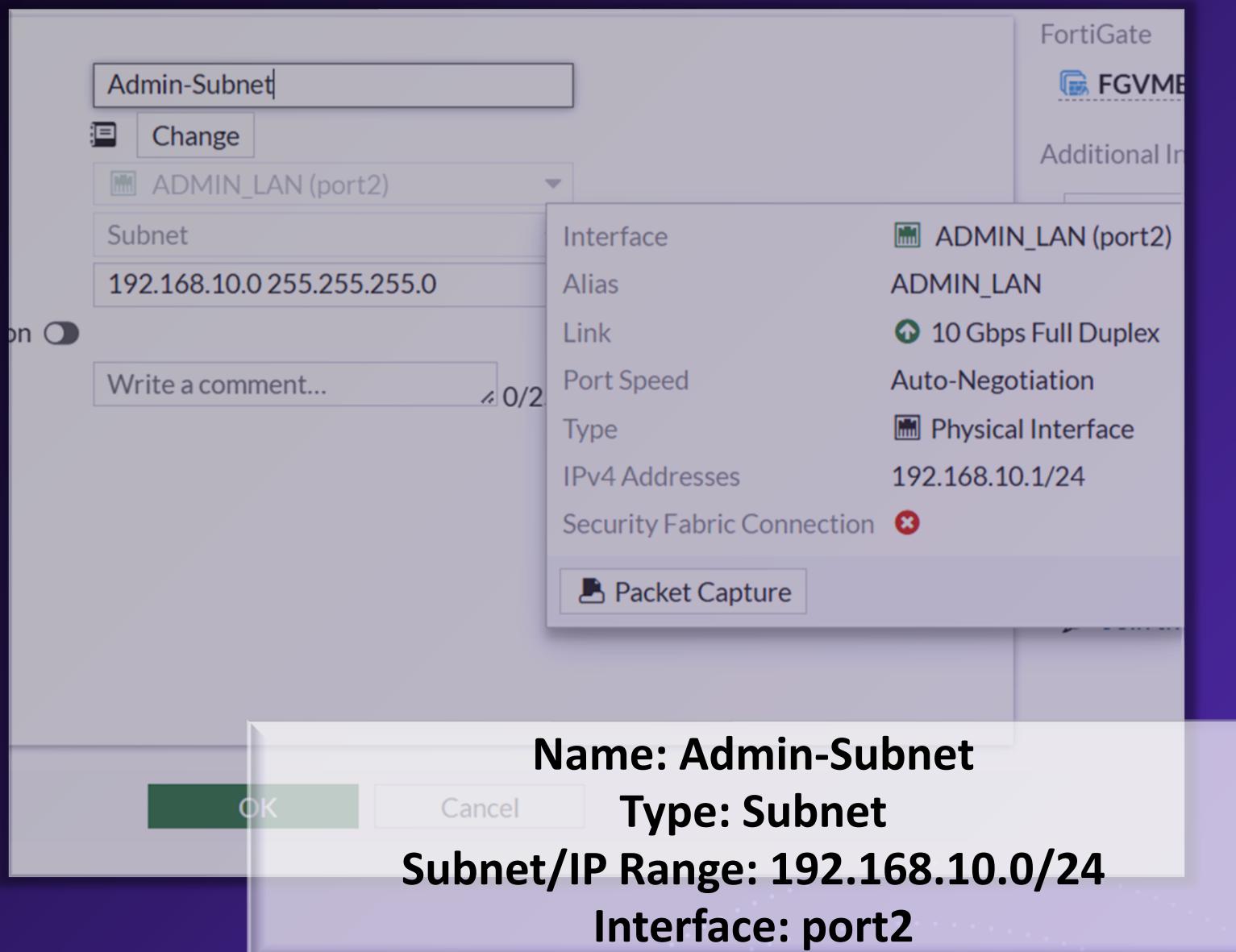
Administrative Access: **uncheck**
HTTPS/SSH

(set only ping)

OK / Save.

Address Objects (GUI)

Address Objects (GUI)



Firewall Policies

Policy 1: ADMIN_TO_ATTACKER

Purpose:

Allows Admin LAN VM to communicate with the Attacker VM for testing, pings, file transfers, and firewall visibility.

Name	<input type="text" value="ADMIN_ATTACKER"/>
Incoming interface	<input type="button" value="ADMIN_LAN (port2)"/>
Outgoing interface	<input type="button" value="ATTACKER (port3)"/>
Source	<input type="button" value="4 Admin-Subnet"/> +
Destination	<input type="button" value="4 Attacker-subnet"/> +
Schedule	<input type="button" value="always"/>
Service	<input type="button" value="ALL"/> +
Action	<input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/>
Firewall/Network Options	
NAT	<input type="checkbox"/>
IP pool configuration	<input type="button" value="Use Outgoing Interface Address"/> <input type="button" value="Use Dynamic IP Pool"/>
Manage source port	<input type="checkbox"/> <input type="button" value="Fixed port"/> <input type="button" value="Preserve source port"/>
Protocol options	<input type="button" value="PROT"/> <input type="button" value="default"/>

Policy 2: ATTACKER_TO_ADMIN

Purpose:

Allows the Attacker VM to reach the Admin VM.

ATTACKER_To_ADMIN

ATTACKER (port3)

ADMIN_LAN (port2)

Attacker-subnet

Admin-Subnet

always

ALL

ACCEPT

DENY

NAT

IP pool configuration

Manage source port

Protocol options

OK Cancel



Policy 3: ATTACKER_TO_WAN

Purpose:

Allows Attacker VM internet access for:
Downloading malware samples (safe lab)
Updating tools
Launching outbound scans

ATTACKER_TO_WAN

ATTACKER (port3)

WAN (port1)

Attacker-subnet

all

always

ALL

ACCEPT

DENY

Firewall/Network Options

NAT

IP pool configuration

Manage source port

Protocol options

OK Cancel



Policy 4: ADMIN_TO_WAN

Purpose:

Provides the Admin VM full internet access for:

Browsing

Testing web filtering

Downloading tools

Creating malware attack simulations

ADMIN_TO_WAN

ADMIN_LAN (port2)

WAN (port1)

Admin-Subnet

all

always

ALL

ACCEPT DENY

Firewall/Network Options

NAT

IP pool configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Manage source port

Fixed port

Preserve source port

Protocol options

PROT default

OK Cancel



Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV default
Web filter	<input checked="" type="checkbox"/> WEB default
DNS filter	<input checked="" type="checkbox"/> DNS default
Application control	<input checked="" type="checkbox"/> APP default
IPS	<input checked="" type="checkbox"/> IPS default
File filter	<input checked="" type="checkbox"/> FILE default
SSL inspection	SSL certificate-inspection

Logging Options

Log allowed traffic	<input checked="" type="checkbox"/> Security events All sessions
Generate logs when session starts	<input checked="" type="checkbox"/>

Comments

0/1023

Enable this policy

OK Cancel

IPS DETECTION BY FORTIGATE FIREWALL

BY RESHMA PANCHAL

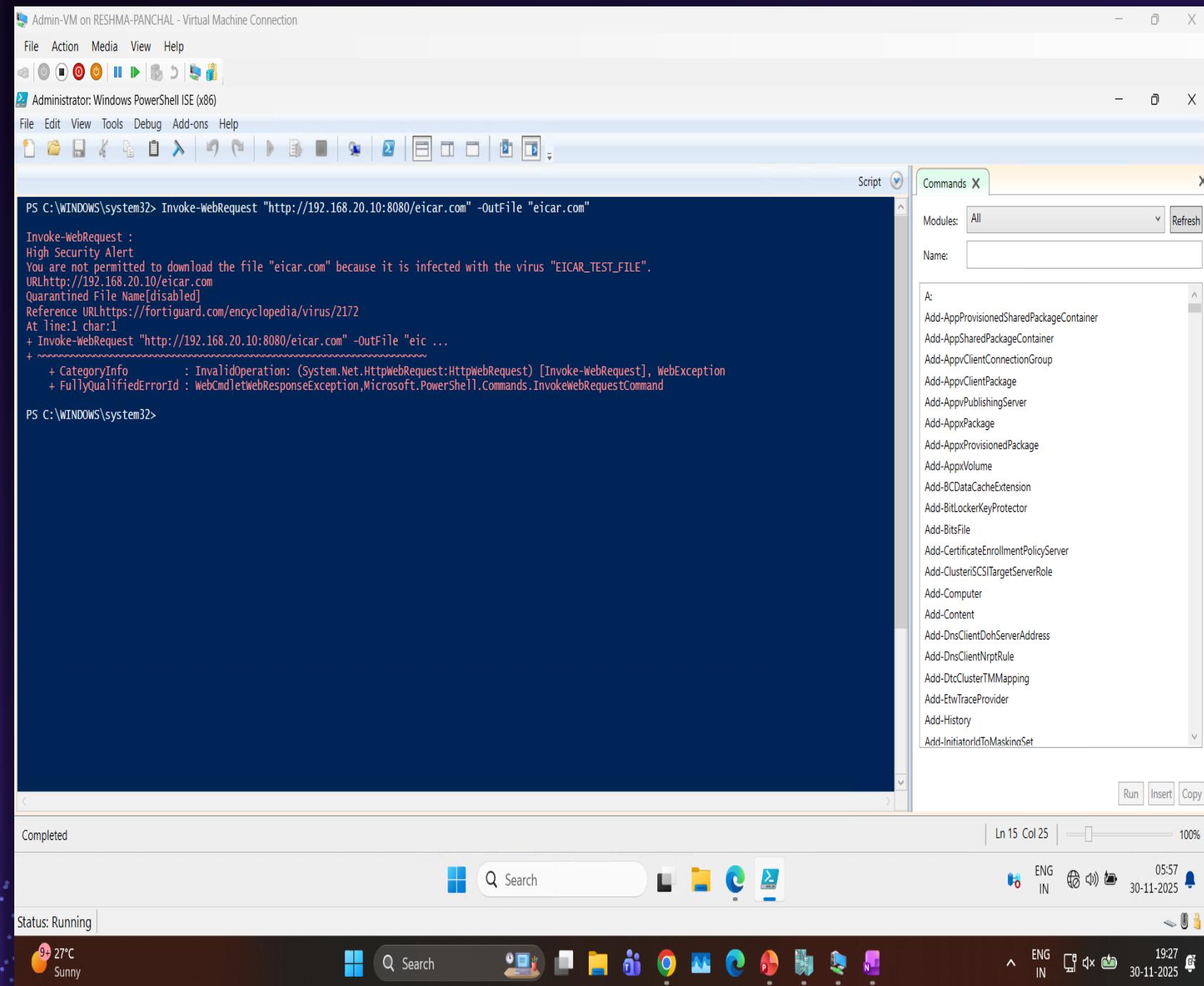
```
(kali㉿kali)-[~]
$ sudo nmap --script http-vuln* 192.168.10.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 09:04 EST
Nmap scan report for 192.168.10.10
Host is up (0.0018s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
5985/tcp  open  wsman

Nmap done: 1 IP address (1 host up) scanned in 106.43 seconds

(kali㉿kali)-[~]
$ sudo nmap -sS -sV -O --script vuln 192.168.10.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 09:07 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|   224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
```

The screenshot shows the FortiGate management interface with the URL <https://192.168.10.10>. The left sidebar navigation includes Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, Log & Report, Forward Traffic, Local Traffic, Sniffer Traffic, System Events, Security Events, Reports, and Log Settings. The main content area is titled "Logs" under "Log & Report". A table lists log entries with columns: Date/Time, Severity, Source, Protocol, User, Action, and Count. One entry is highlighted in blue: "2025/12/01 06:08:23" with "High" severity, source "192.168.20.10", protocol "6", user "", action "dropped", and count "1". To the right of the table is a "Log Details" panel. The "Intrusion Prevention" section shows a profile "IPS-Strict", attack name "Adobe.XML.Entity.Injection", attack ID "18,162", reference "https://fortiguard.fortinet.com/encyclopedia/ips/18162", incident serial "1,36,32,137", direction "outgoing", severity "High", and message "applications3: Adobe.XML.Entity.Injection". The status bar at the bottom indicates "Status: Running" and the date/time "01-12-2025 06:09".

Anti-Virus/malware Detection by Fortigate Firewall

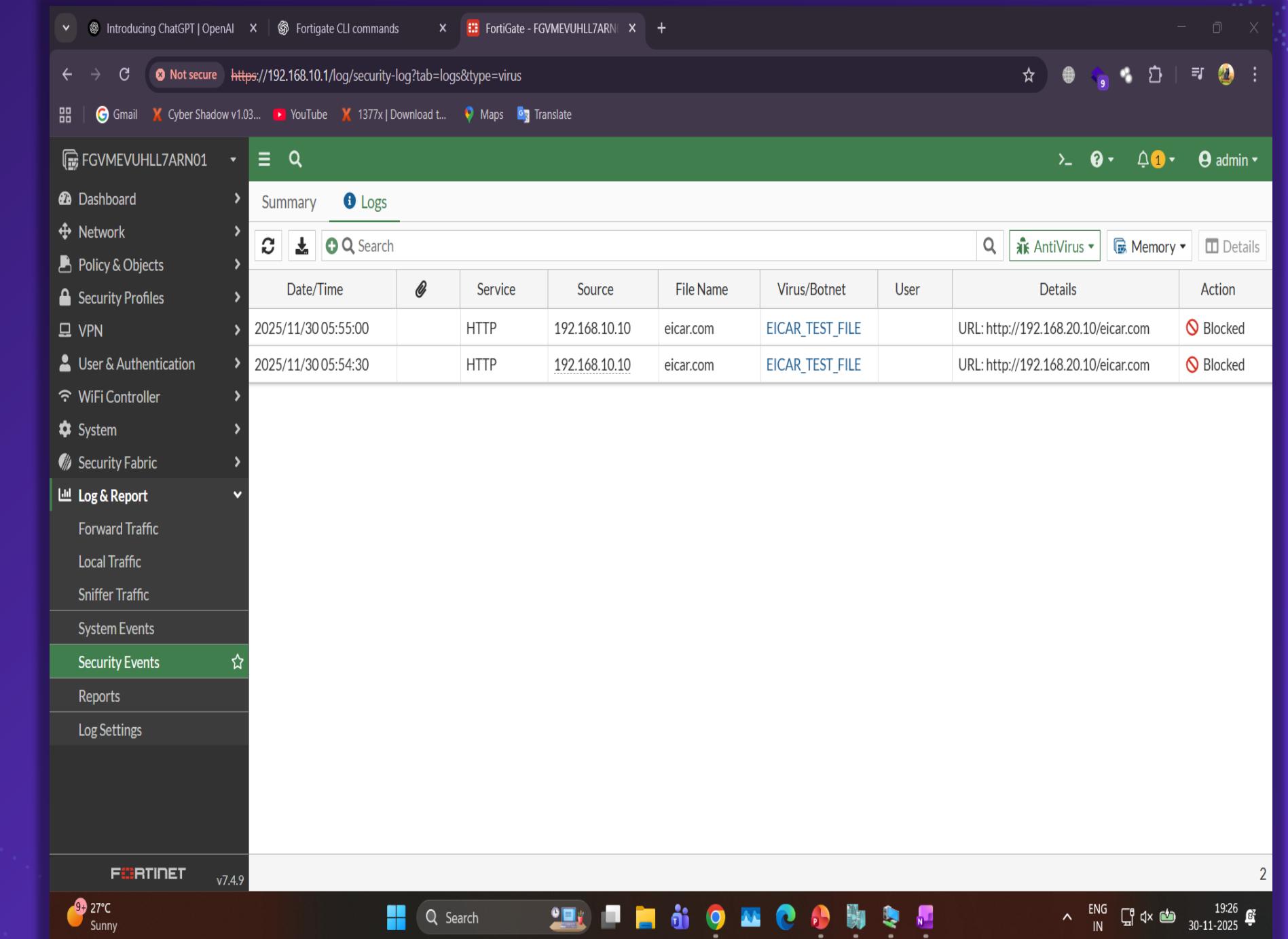


PS C:\WINDOWS\system32> Invoke-WebRequest "http://192.168.20.10:8080/eicar.com" -OutFile "eicar.com"

Invoke-WebRequest :
High Security Alert
You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".
URL: http://192.168.20.10/eicar.com

Quarantined File Name[disabled]
Reference URL: https://fortiguard.com/encyclopedia/virus/2172
At line:1 char:1
+ Invoke-WebRequest "http://192.168.20.10:8080/eicar.com" -OutFile "eic ...
+ ~~~~~
+ CategoryInfo : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\WINDOWS\system32>



Introducing ChatGPT | OpenAI | Fortigate CLI commands | Fortigate - FGVM-EUHLL7ARN01

Not secure https://192.168.10.1/log/security-log?tab=logs&type=virus

Gmail Cyber Shadow v1.03... YouTube 1377x Download t... Maps Translate

FGVM-EUHLL7ARN01

Logs

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action	
2025/11/30 05:55:00	HTTP	192.168.10.10	eicar.com	EICAR_TEST_FILE			URL: http://192.168.20.10/eicar.com	Blocked
2025/11/30 05:54:30	HTTP	192.168.10.10	eicar.com	EICAR_TEST_FILE			URL: http://192.168.20.10/eicar.com	Blocked

Dashboard Network Policy & Objects Security Profiles VPN User & Authentication WiFi Controller System Security Fabric Log & Report Forward Traffic Local Traffic Sniffer Traffic System Events Security Events Reports Log Settings

FORTINET v7.4.9

“When the EICAR test file was blocked, FortiGate provided detailed threat intelligence through the FortiGuard Labs portal. This includes the signature ID (2172), release date, analysis of the threat, and recommended action. This confirms that FortiGate is actively using its malware signature database to identify malicious content.”

The screenshot shows the FortiGuard Labs portal interface. At the top, there's a navigation bar with links for Research, Services, Threat Intelligence, Support, Resources, and About, along with a search icon. The main header features the 'FortiGuard Labs' logo, the word 'Virus', and the specific threat name 'EICAR_TEST_FILE'. Below this, there's a large background image of three people looking at a computer screen. The 'Analysis' section contains a detailed description of the EICAR test file, stating it's a non-malicious test file developed by EICAR and CARO to check antivirus software. To the right of this text is a summary card with the following information:

ID	2172
Released	Oct 15, 1996
Description Updated	Jan 05, 2015
Aliases	EICAR_Test

The 'Recommended Action' section is partially visible below the analysis. At the very bottom, there's a 'Detection Availability' section.

File Action Media View Help



192.168.10.10

High Security Alert

+

Not secure | 192.168.20.10:8080/eicar.com



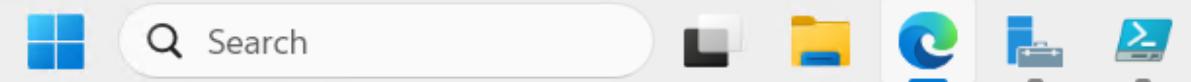
High Security Alert

You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".

URL http://192.168.20.10/eicar.com

Quarantined File Name [disabled]

Reference URL <https://fortiguard.com/encyclopedia/virus/2172>



09:45 02-12-2025

Status: Running



18°C

Clear



Search

ENG
IN

23:15 02-12-2025

Web Vulnerability detection by FortiGate Firewall

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.10.10
- Nikto v2.5.0

+ Target IP:          192.168.10.10
+ Target Hostname:    192.168.10.10
+ Target Port:        80
+ Start Time:        2025-11-30 08:31:53 (GMT-5)

+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

The screenshot shows the FortiGate Management Interface with the 'Logs' tab selected. A single log entry is highlighted, indicating a critical event. The log details are as follows:

Date/Time	Severity	Source	Protocol	User	Action	Count
2025/11/30 05:34:14	Critical	192.168.20.10	6		dropped	

Log Details

- Source**
 - Source: 192.168.20.10
 - Source Port: 58684
 - Source Country/Region: Reserved
 - Source Interface: ATTACKER (port3)
- Destination**
 - Destination: 192.168.10.10
 - Destination Port: 80
 - Destination Country/Region: Reserved
 - Destination Interface: ADMIN_LAN (port2)
 - Hostname: 192.168.10.10
 - URL: /book.cgi
- Application Control**
 - Protocol: 6
 - Service: HTTP
- Action**

The left sidebar shows the navigation menu, and the bottom status bar indicates the interface version is v7.4.9.

Brute-Force/ssh (application control) detection by FortiGate Firewall

```
(kali㉿kali)-[~]
$ ssh testuser@192.168.10.10
The authenticity of host '192.168.10.10 (192.168.10.10)' can't be established.
ED25519 key fingerprint is: SHA256:EuyeGqkhenSkADBDo7jPDrsIqgPWvdYKkwER7ND0z4
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.10.10' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
testuser@192.168.10.10's password:
Permission denied, please try again.
testuser@192.168.10.10's password:
Permission denied, please try again.
testuser@192.168.10.10's password:

zsh: suspended  ssh testuser@192.168.10.10

(kali㉿kali)-[~]
$ hydra -l testuser -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.10.10

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).
```

The screenshot shows the FortiGate Management UI with the URL <https://192.168.10.1/log/security-log?tab=logs&type=app-ctrl&vdom=root&device=memory&timeframe=realtime>. The left sidebar shows navigation options like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, Log & Report, Security Events (which is selected), Reports, and Log Settings. The main area displays a table of security logs. A specific log entry is highlighted in the table:

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2025/11/30 05:04:51	192.168.20.10	192.168.10.10	SSH	SSH		SSH
2025/11/30 04:45:53	192.168.20.5	192.168.1.7 (192.168.1.7)	NetE	NetE		NetE
2025/11/30 04:44:37	192.168.20.5	192.168.10.10	NetE	NetE		NetE
2025/11/30 04:25:31	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:31	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:31	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:30	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:30	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:30	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:30	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:30	192.168.20.5	208.91.112.55	HTTP	HTTP		HTTP
2025/11/30 04:25:01	192.168.10.20	208.91.112.55	NetE	NetE		NetE
2025/11/30 04:25:00	192.168.20.5	72.145.35.103	NetE	NetE		NetE
2025/11/30 04:24:59	192.168.10.20	72.145.35.103	NetE	NetE		NetE

A tooltip for the first log entry provides detailed information:

ID: 16060
Summary: This indicates the detection of the SSH traffic.
Category: Network.Service
Risk: Low
Popularity: ★★★★★
Protocol: TCP, SSH
Technology: Network-Protocol
Behavior: Tunneling
Vendor: Other

Introducing ChatGPT | OpenAI Webfilter attack setup FortiGate - FGVMEUHLL7ARN01

Not secure https://192.168.10.1/log/security-log?tab=logs&type=app-ctrl

Gmail Cyber Shadow v1.03... YouTube 1377x | Download t... Maps Translate

FGVMEUHLL7ARN01 Dashboard Network Policy & Objects Security Profiles VPN User & Authentication WiFi Controller System Security Fabric Log & Report Forward Traffic Local Traffic Sniffer Traffic System Events Security Events Reports Log Settings

Logs

Summary Logs

Search Date/Time Source Destination Application Name Action Application User Application Details

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details								
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:11	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
2025/11/30 05:13:10	192.168.20.10	192.168.10.10	SSH	Pass										
FGTINET v7.4.9	0% 500+													
9+ 27°C Sunny	Search	File	Folder	People	Google Chrome	Photos	OneDrive	Microsoft Edge	PowerPoint	Excel	Word	Teams	Outlook	OneNote
ENG IN	18:43	30-11-2025												

THANK YOU

ELIVIAZ 100