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

- 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

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
• **Next-Generation Security** – Combines firewall, antivirus, IPS, web filtering, and application control in one device (UTM).	• **Licensing Costs** – Subscription (FortiGuard services) needed for full protection; can be expensive long-term.
• **High Performance** – Uses custom FortiASIC processors for faster packet inspection.	• **Complexity in Large Deployments** – Advanced features (like IPS tuning, SSL inspection) require expertise.
• **User-Friendly GUI & CLI** – Easy for beginners via GUI, advanced control via CLI.	• **Learning Curve** – Beginners may find CLI configurations and advanced security features difficult.
• **VLAN & Network Segmentation** – Supports inter-VLAN routing with security policies.	• **Performance Drop with Deep Inspection** – SSL/TLS deep inspection and heavy IPS rules may reduce throughput.
• **Centralized Management** – With FortiManager & FortiAnalyzer, admins can manage multiple firewalls and analyze logs centrally.	• **Limited Compatibility** – Some third-party integrations may be less flexible compared to Palo Alto or Check Point.
• **Traffic Shaping & QoS** – Controls bandwidth per user/application (good for Guest vs Admin VLANs).	• **Frequent Updates Required** – Needs regular firmware updates and threat database updates for maximum security.
• **Cloud & VPN Support** – Site-to-site and remote-access VPNs; supports AWS, Azure, GCP deployments.	• **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

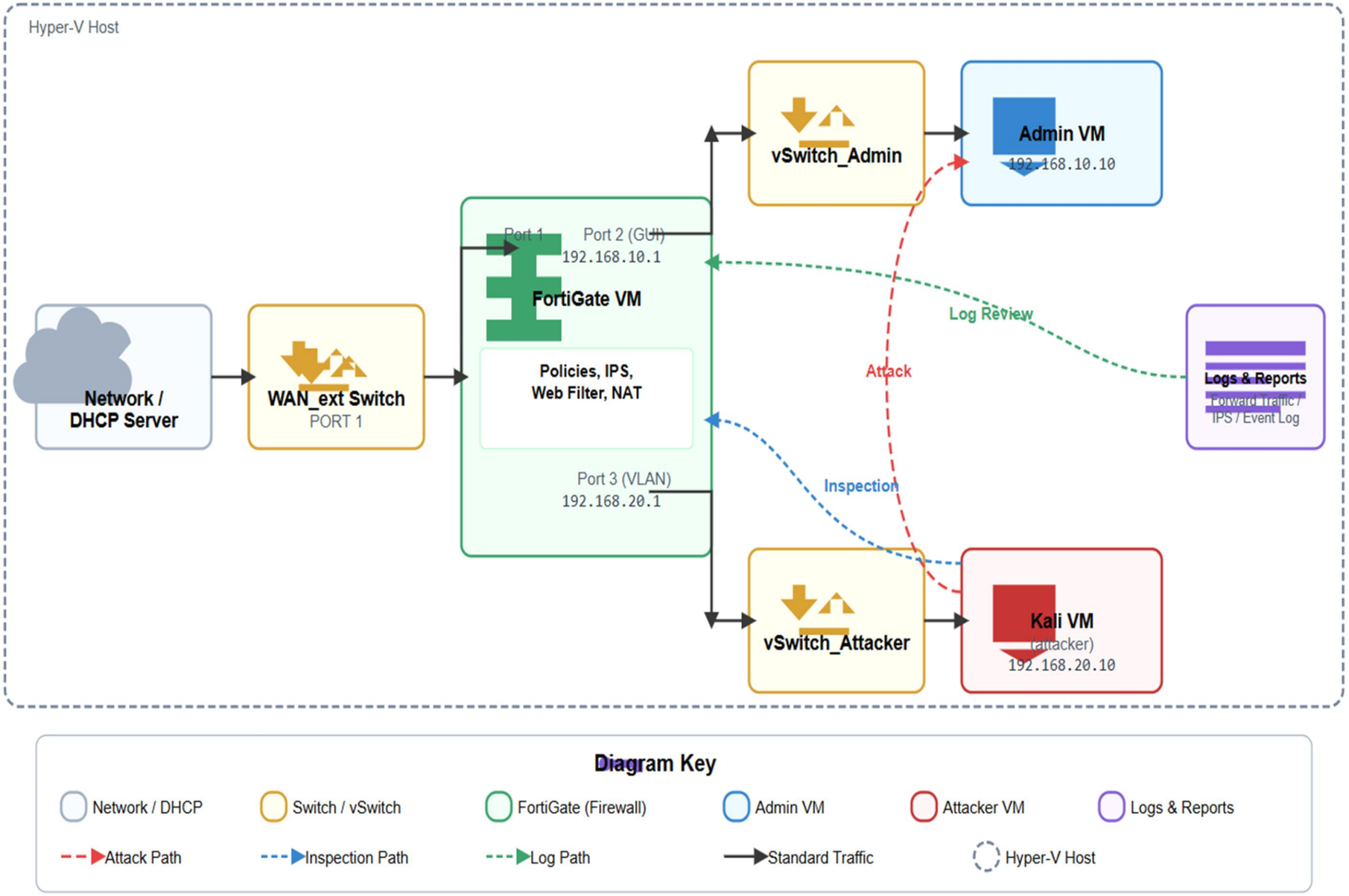
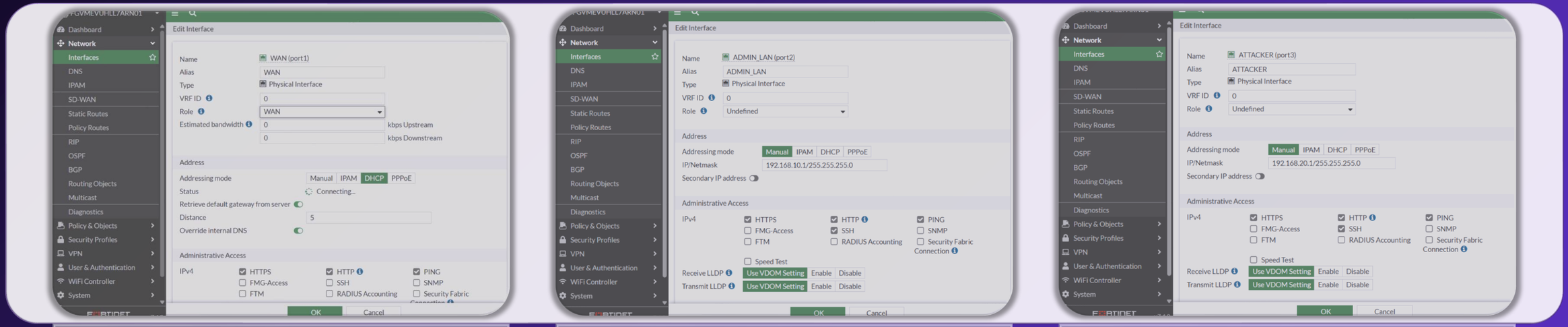


Diagram Key

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



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**

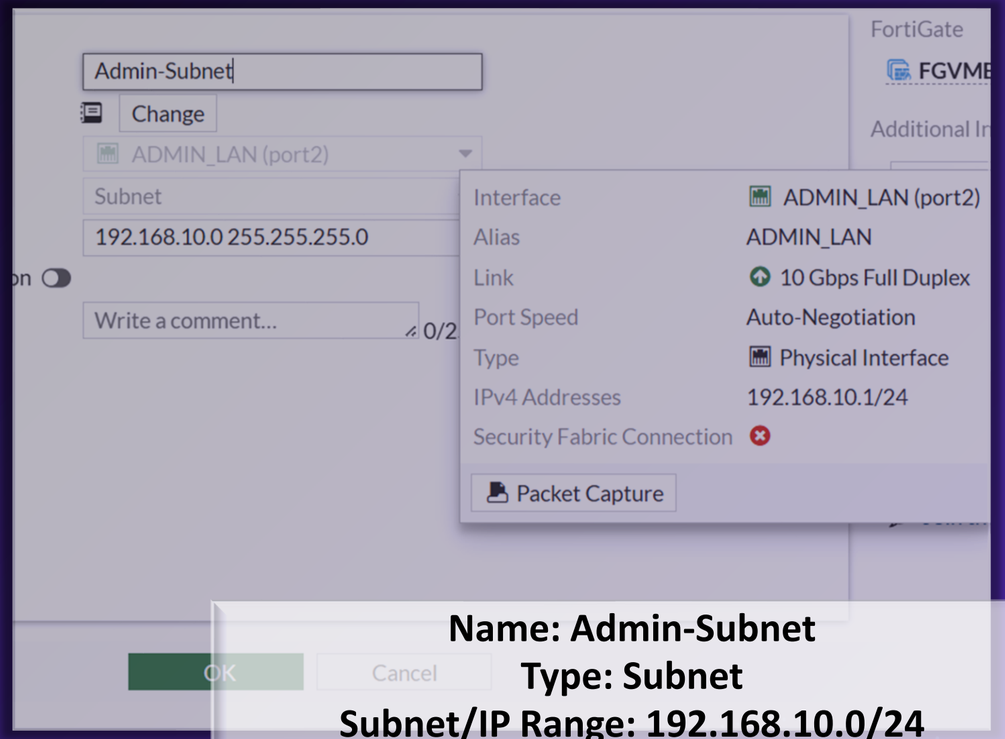
IP/Netmask: **192.168.20.1/24**

Administrative Access: **uncheck** HTTPS/SSH

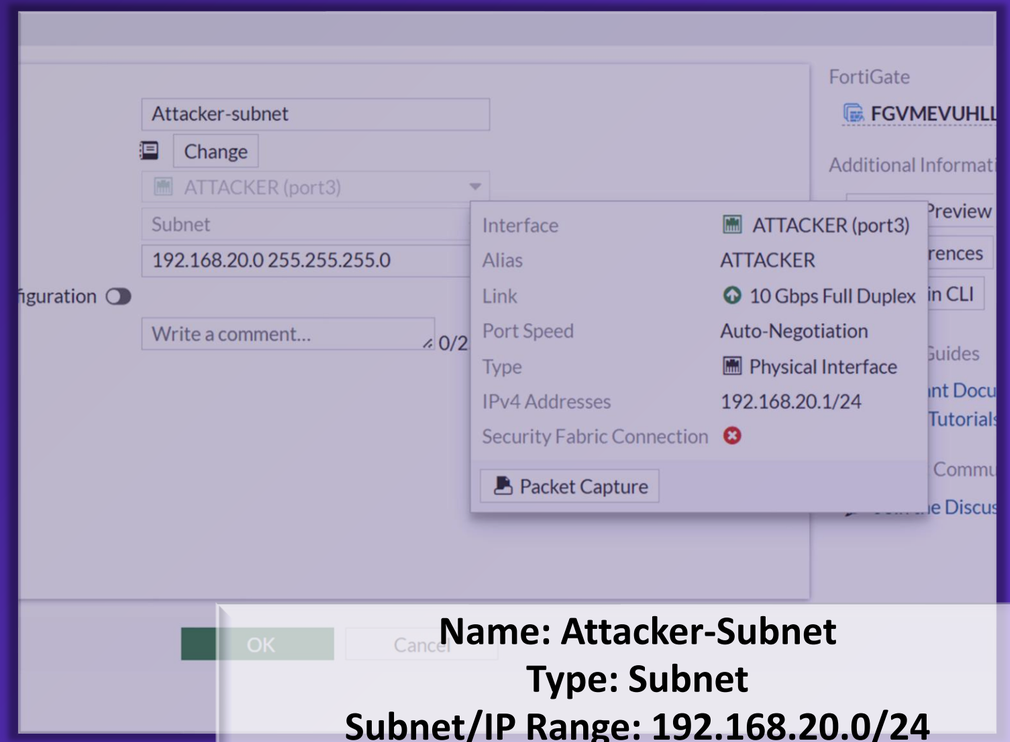
(set only ping)

OK / Save.

Address Objects (GUI)



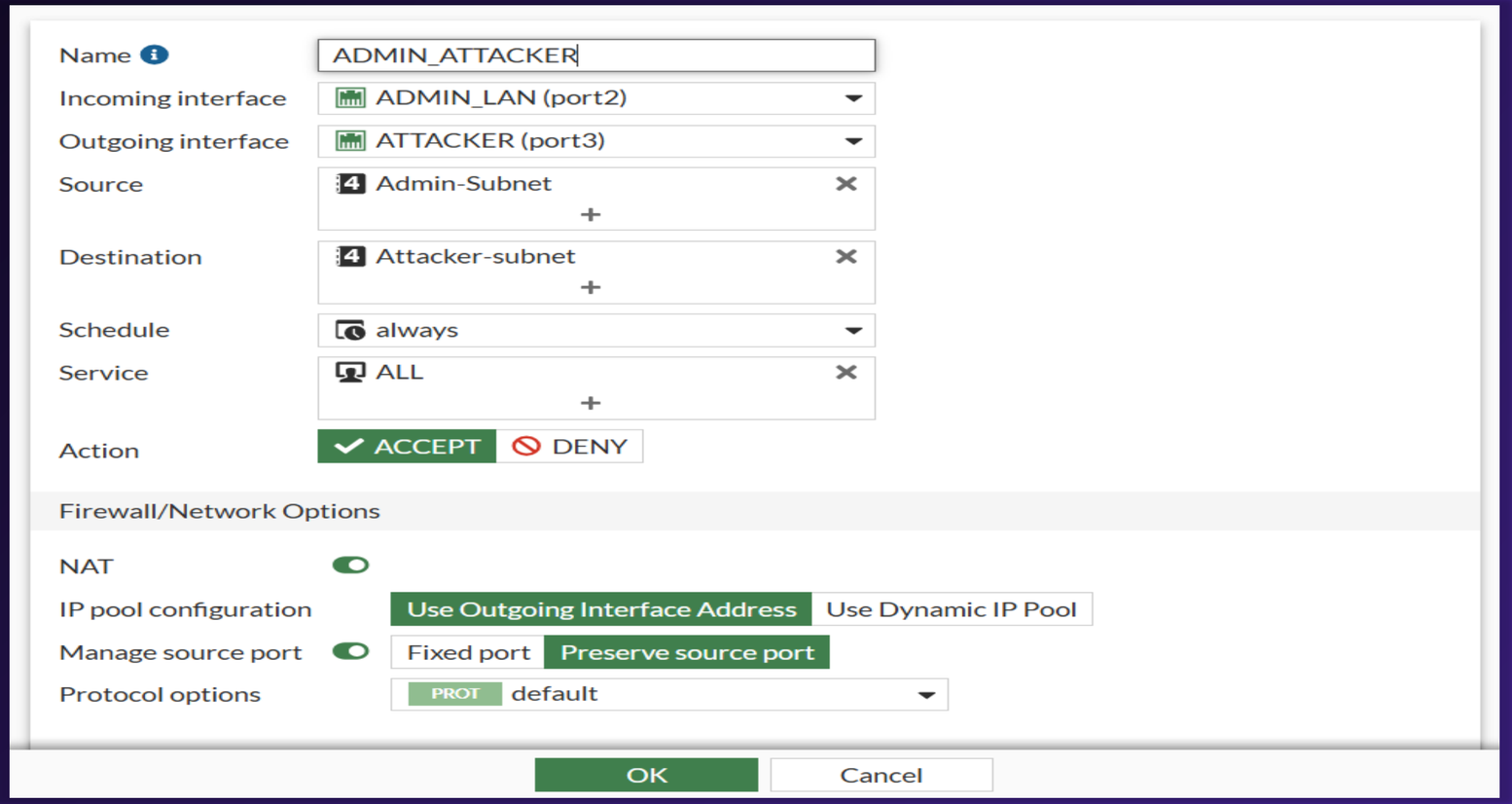
Name: Admin-Subnet
Type: Subnet
Subnet/IP Range: 192.168.10.0/24
Interface: port2



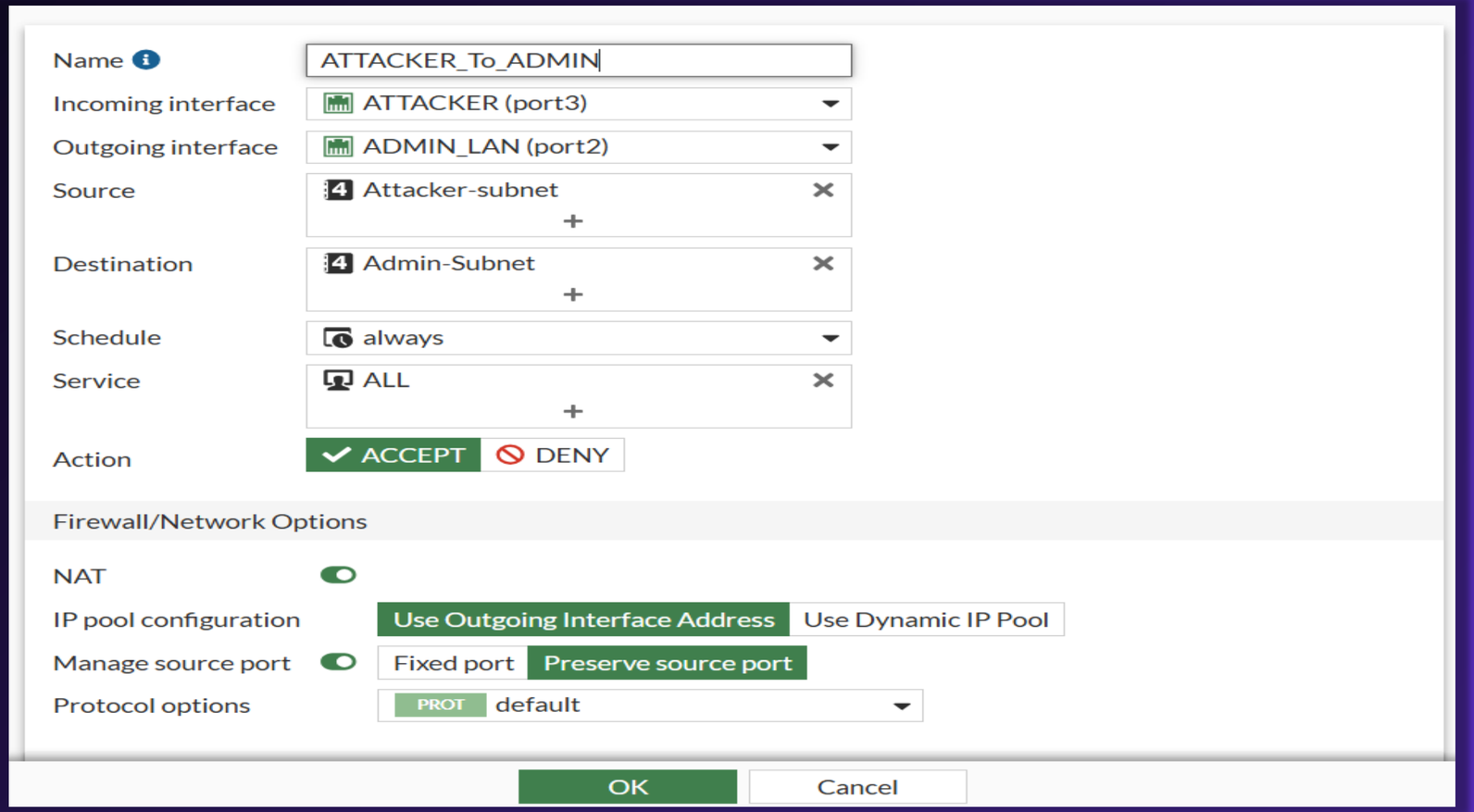
Name: Attacker-Subnet
Type: Subnet
Subnet/IP Range: 192.168.20.0/24
Interface: port3

Firewall Policies

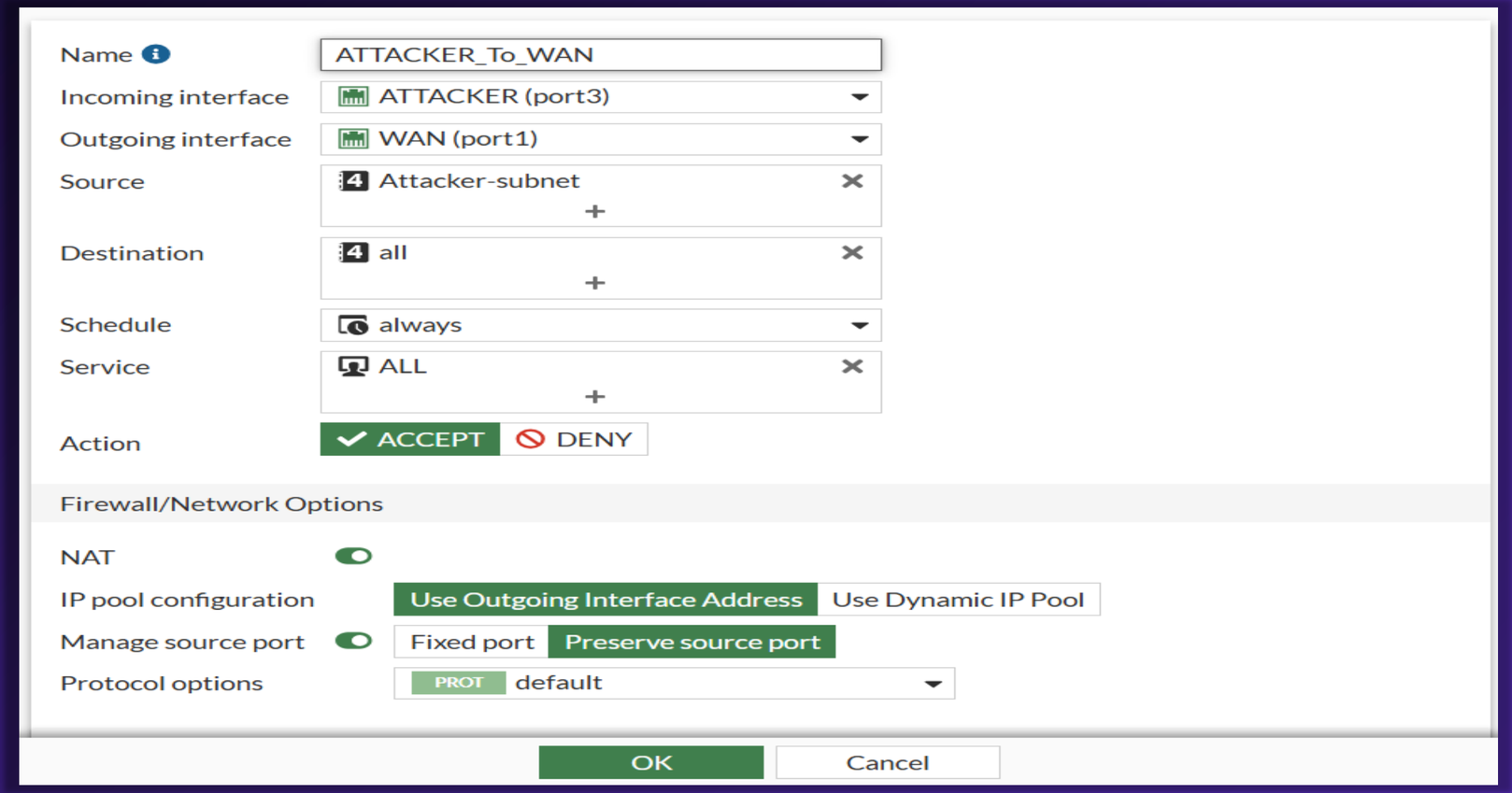
Policy 1: ADMIN_TO_ATTACKER
Purpose:
Allows Admin LAN VM to communicate with the Attacker VM for testing, pings, file transfers, and firewall visibility.



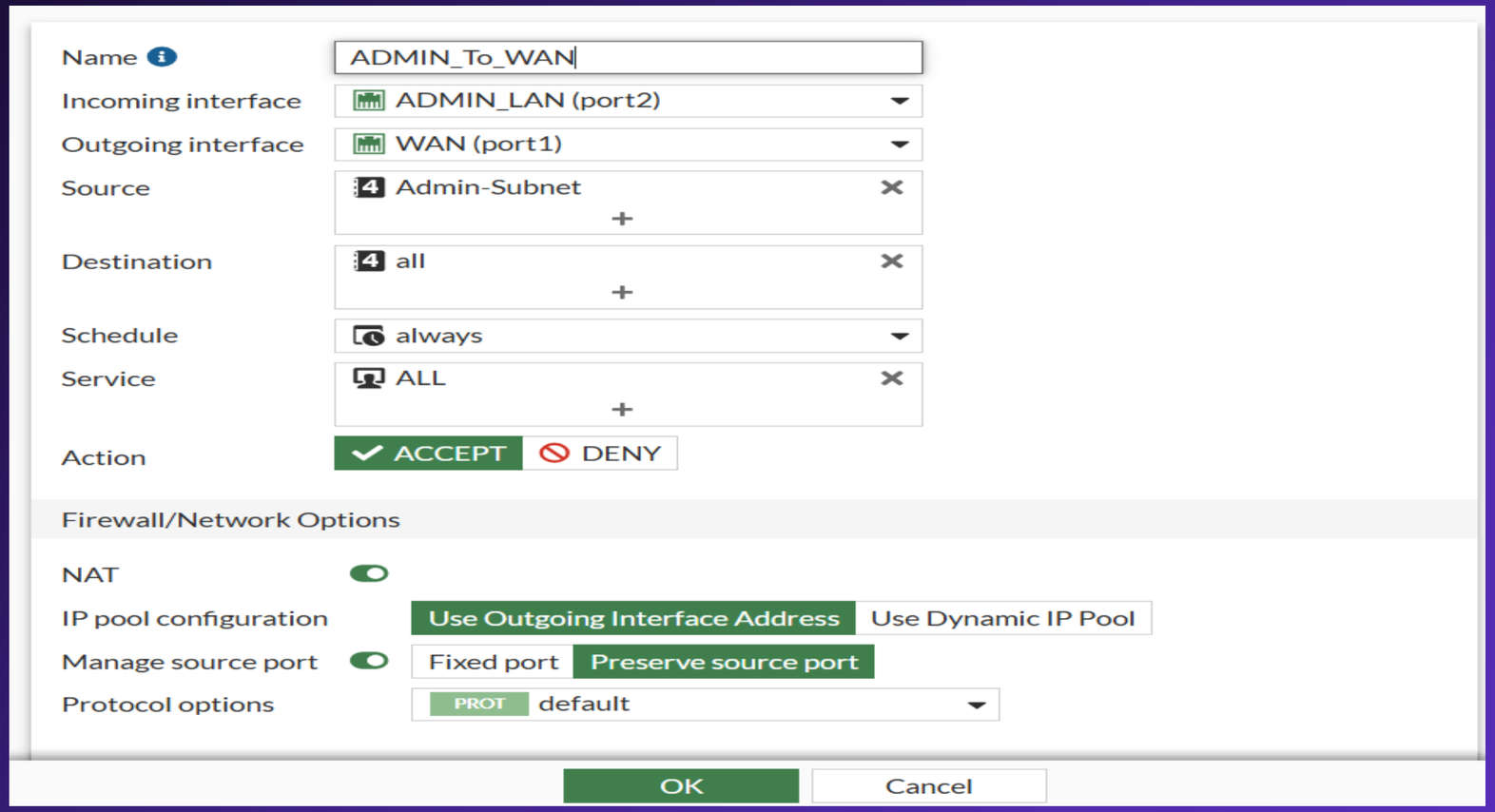
Policy 2: ATTACKER_TO_ADMIN
Purpose:
Allows the Attacker VM to reach the Admin VM.



Policy 3: ATTACKER_TO_WAN
Purpose:
Allows Attacker VM internet access for:
Downloading malware samples (safe lab)
Updating tools
Launching outbound scans



Policy 4: ADMIN_TO_WAN
Purpose:
Provides the Admin VM full internet access for:
Browsing
Testing web filtering
Downloading tools
Creating malware attack simulations



Security Profiles

AntiVirus	AV	default
Web filter	WEB	default
DNS filter	DNS	default
Application control	APP	default
IPS	IPS	default
File filter	FILE	default
SSL inspection	SSL	certificate-inspection

Logging Options

Log allowed traffic — Security events | All sessions

Generate logs when session starts

Comments

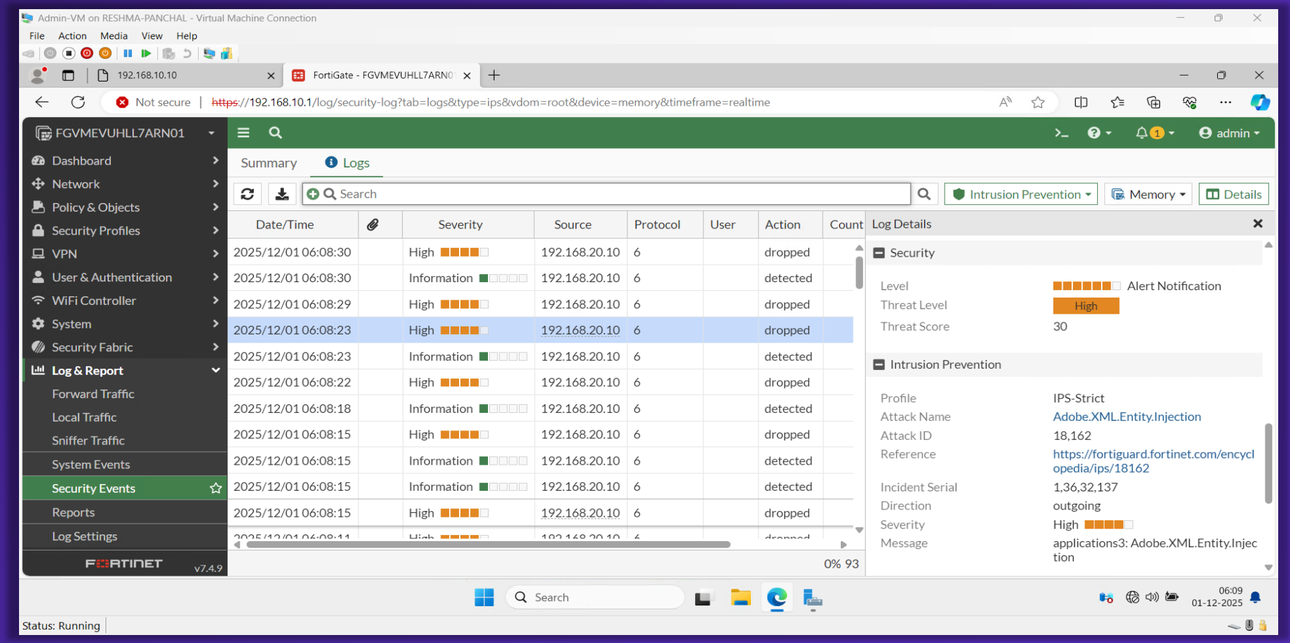
0/1023

Enable this policy

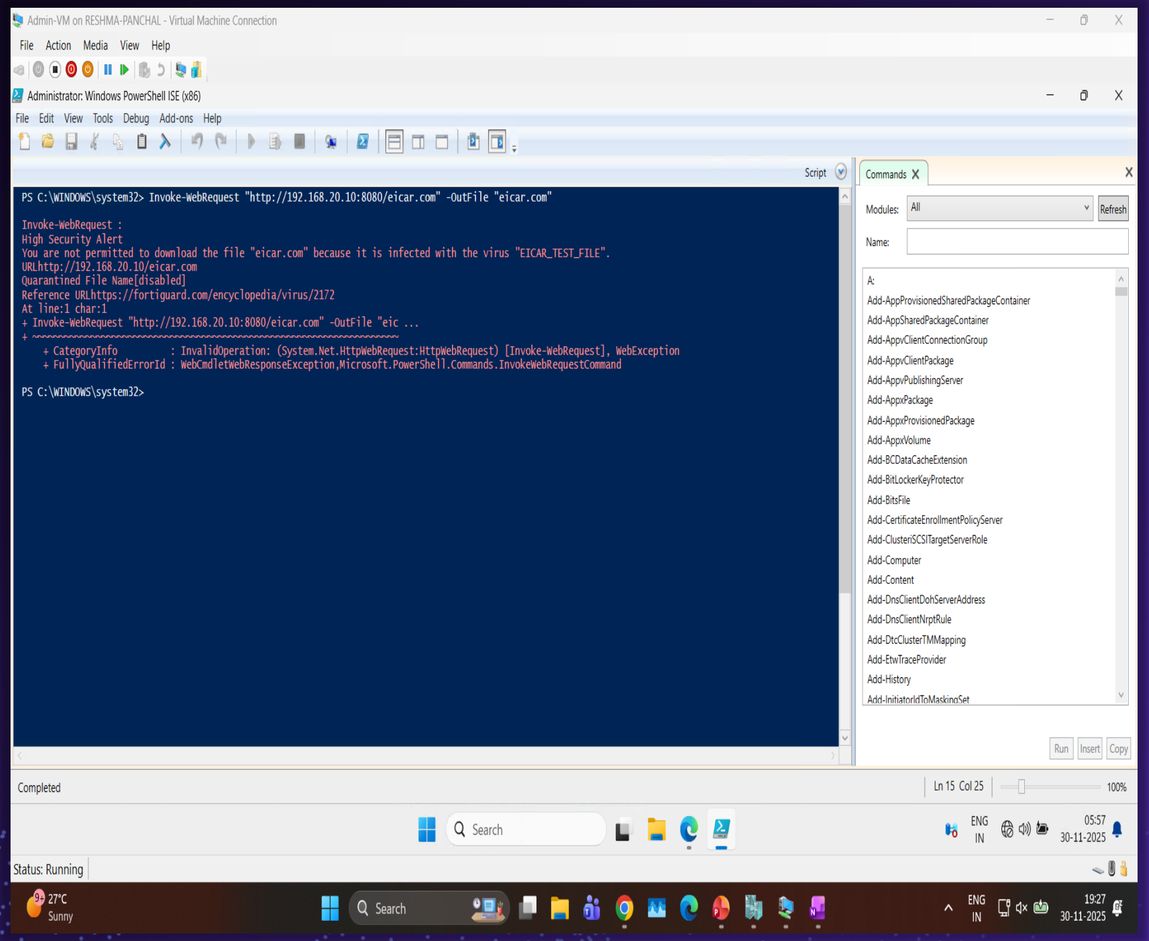
OK Cancel

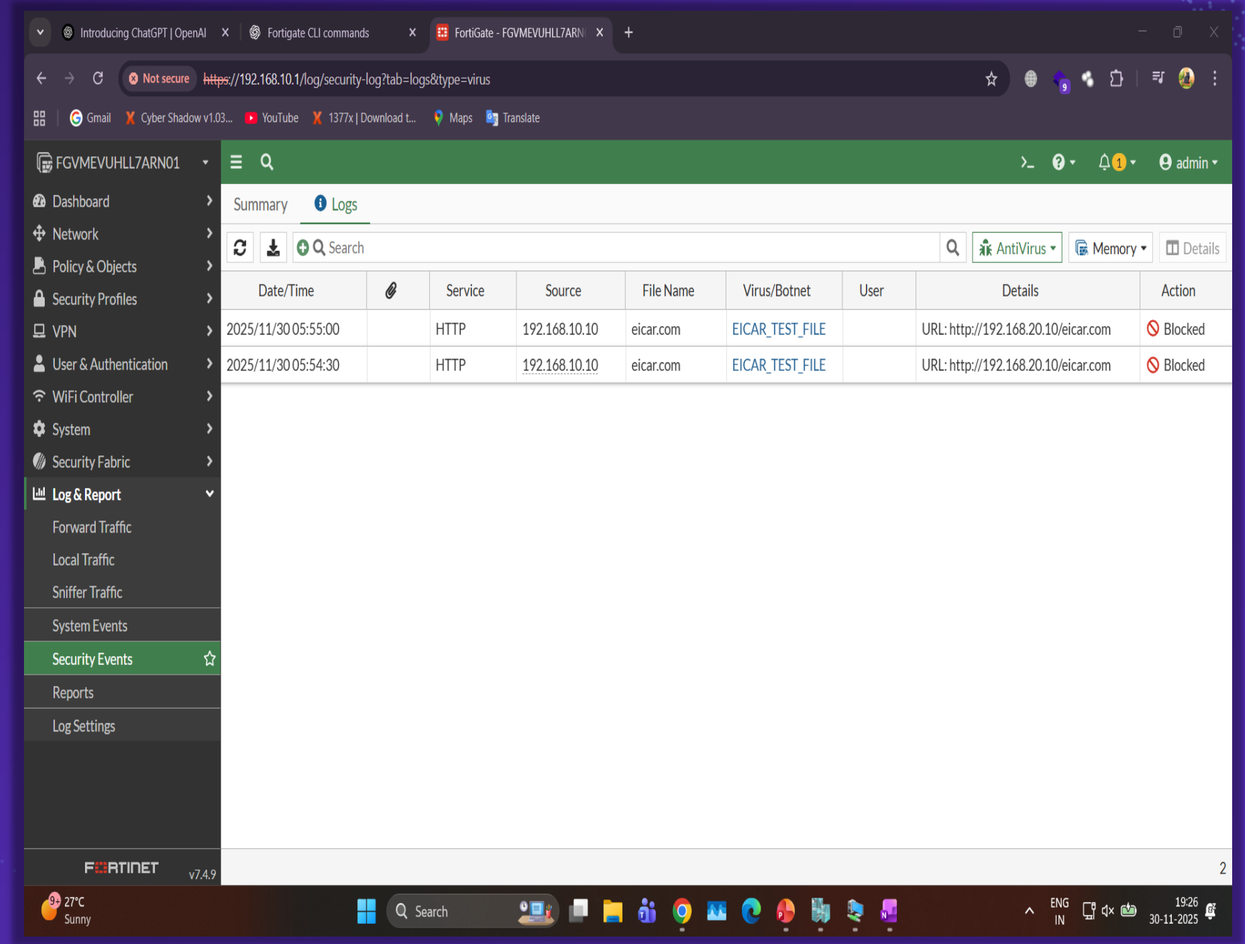
IPS DETECTION BY FORTIGATE FIREWALL

```
┌──(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).
```

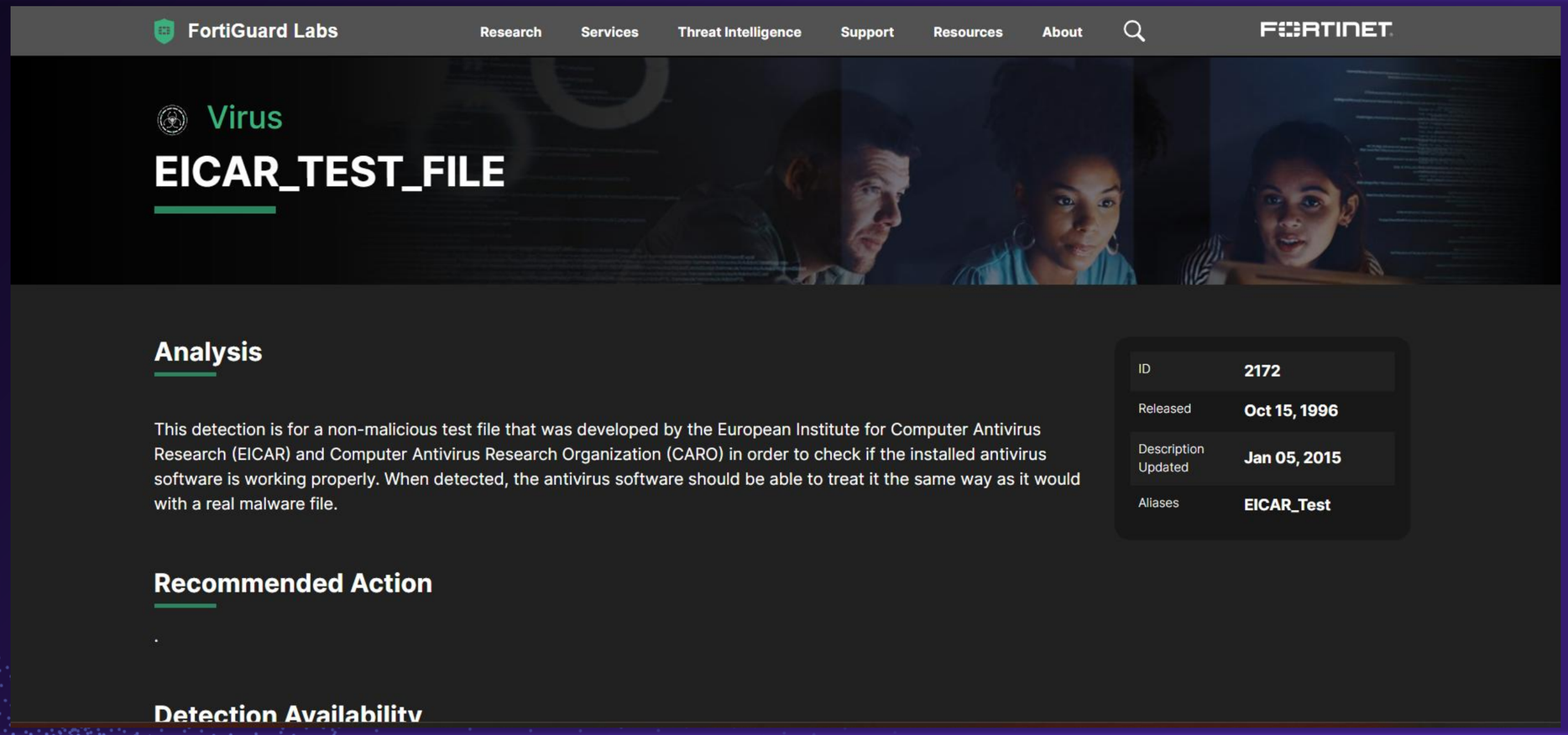


Anti-Virus/malware Detection by Fortigate FIrewall





“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.”

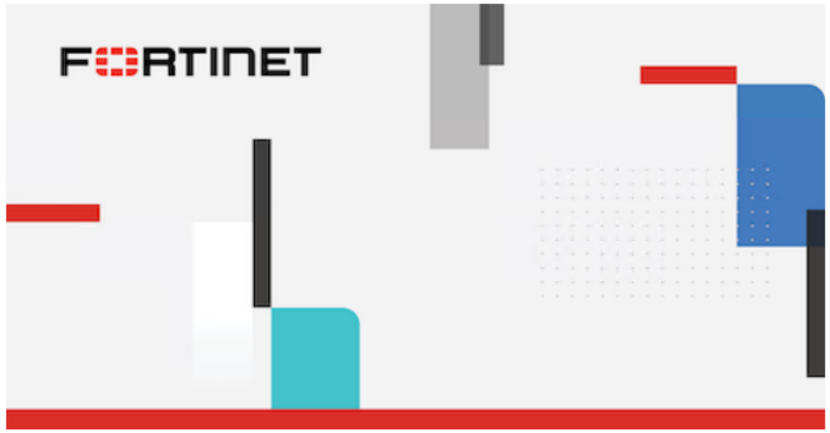


Admin-VM on RESHMA-PANCHAL - Virtual Machine Connection

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

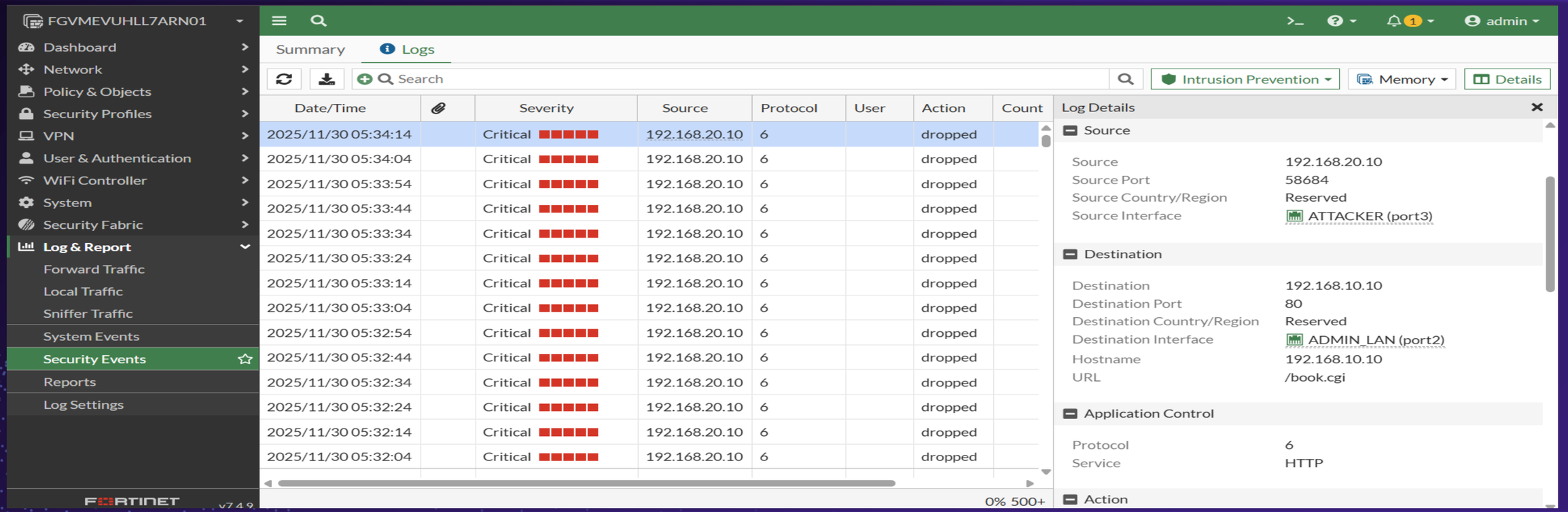
Search 09:45 02-12-2025

Status: Running

18°C Clear Search ENG IN 23:15 02-12-2025

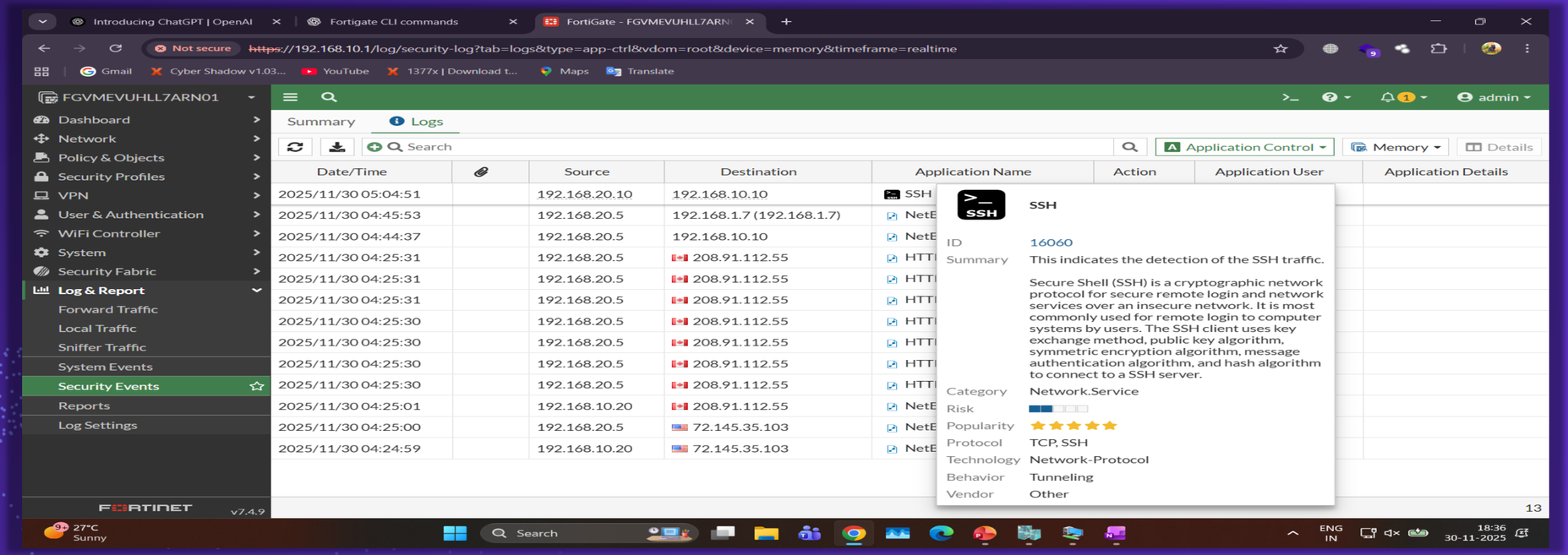
Web Vulnerability detection by FortiGate Firewall

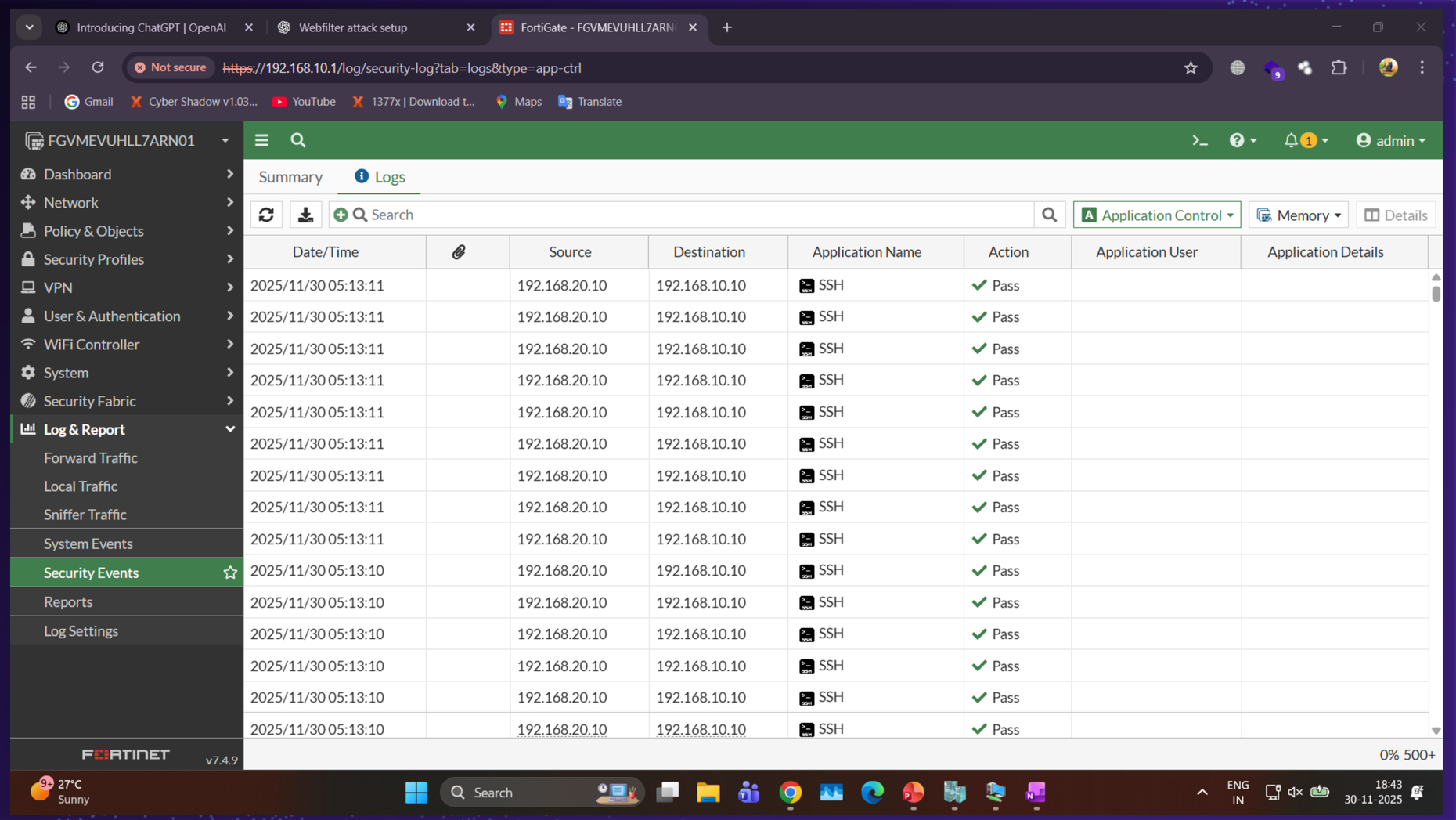
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.10.10
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.10.10
+ Target Hostname:    192.168.10.10
+ Target Port:        80
+ Start Time:         2025-11-30 08:31:53 (GMT-5)
---------------------------------------------------------------------------
+ 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: htt
ps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```



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:EuyeGqkhenSkADBDov7jPDrsIqgPWvdYKKwER7ND0z4
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).
```




Introducing ChatGPT | OpenAI
Webfilter attack setup
FortiGate - FGVMEVUHLL7ARN
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
FGVMEVUHLL7ARN01
admin
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
Summary
Logs
Search
Application Control
Memory
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 05:13:10 192.168.20.10 192.168.10.10 SSH Pass
0% 500+
FORTINET
v7.4.9
27°C
Sunny
Search
ENG
IN
18:43
30-11-2025

THANK YOU