Secure Network Design and Implementation project

CSCE 5585

Saurav Shinde

Kiran Sahu

Mohana Potluri

Tools Used

Network Emulation: Gns3

Virtualizatio: Vmware Workstation

Pentesting: Kali Linux-nmap,wireshark,hydra,ping

IDS: Fail2ban

Firewall: Watchguard xtmV

Server:Ubuntu Server

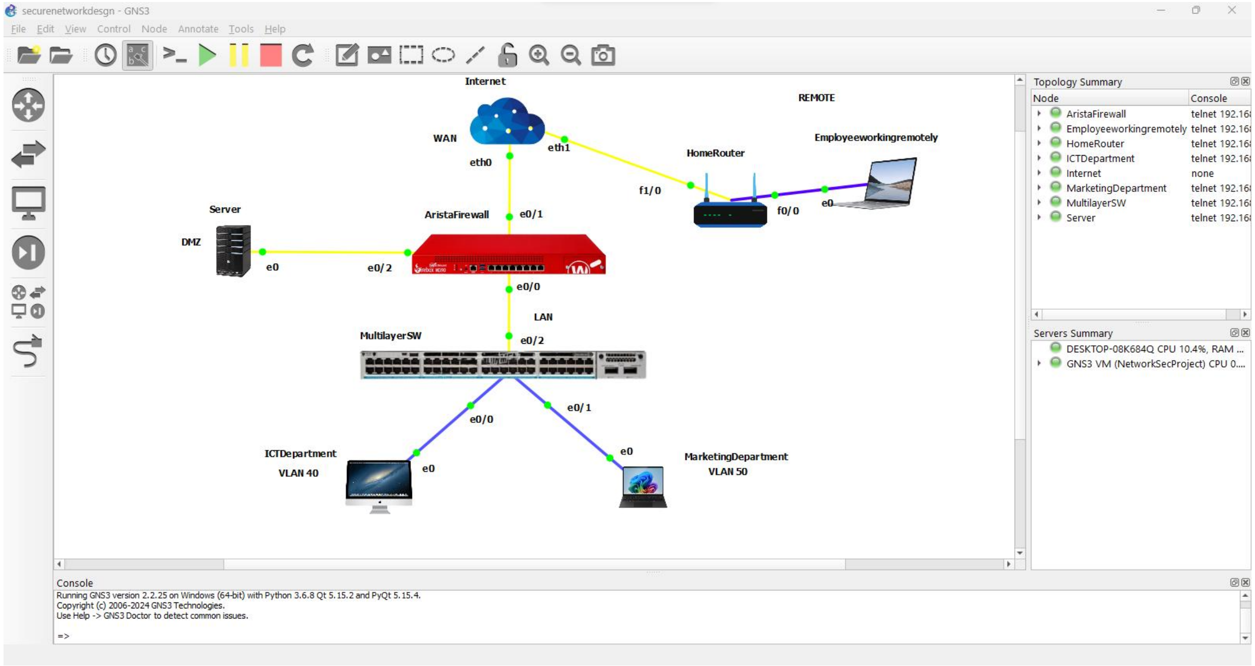
Network Topology and Configuration

Network setup

To do the emulation the network GNS3 emulation application was used . Some were devices was imported from the host machine and some from VMware Workstation. The WatchGuard Firewall, DMZ server (Ubuntu server), and penetration testing machine (Kali Linux) were executed on VMware Workstation; GNS3 server and remote machine were directly with the host system. The screenshot below depicts the network topology already set up in GNS3.

Fig 1.1

Network Topology



Topology Summary

Node	Console
AristaFirewall	telnet 192.16
Employeeworkingremotely	telnet 192.16
HomeRouter	telnet 192.16
ICTDepartment	telnet 192.16
Internet	none
MarketingDepartment	telnet 192.16
MultilayerSW	telnet 192.16
Server	telnet 192.16

Servers Summary

DESKTOP-08K684Q CPU 10.4%, RAM ...
GNS3 VM (NetworkSecProject) CPU 0....

Console

```
Running GNS3 version 2.2.25 on Windows (64-bit) with Python 3.6.8 Qt 5.15.2 and PyQt 5.15.4.
Copyright (c) 2006-2024 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Layer 3 Switch Configuration

The Layer 3 switch was configured to support two VLANs:

ICT Department (VLAN 40)

Marketing Floor Department (VLAN 50)

The VLAN interfaces were enabled for VLAN communication between the VLANs. To manage the IP addresses dynamically a DHCP pool was created for each VLAN. The VLAN traffic was able to pass through the interfaced connecting the switch to the firewall. Below are the configurations executed on the Layer 3 switch:

VLAN and interfaces configuration

```
MultilayerSW(config)# vlan 40
MultilayerSW(config-vlan)# name ICTDepartment
MultilayerSW(config-vlan)# exit
MultilayerSW(config)# vlan 50
MultilayerSW(config-vlan)# name MarketingDepartment
MultilayerSW(config-vlan)# exit

MultilayerSW(config)# interface e0/0
MultilayerSW(config-if)# switchport mode access
MultilayerSW(config-if)# switchport access vlan 40
MultilayerSW(config-if)# no shutdown
MultilayerSW(config-if)# exit

MultilayerSW(config)# interface e0/1
MultilayerSW(config-if)# switchport mode access
MultilayerSW(config-if)# switchport access vlan 50
MultilayerSW(config-if)# no shutdown
MultilayerSW(config-if)# exit
MultilayerSW(config)# interface e0/2
MultilayerSW(config-if)# switchport trunk encapsulation dot1q
MultilayerSW(config-if)# switchport mode trunk
MultilayerSW(config-if)# switchport trunk allowed vlan 40,50
MultilayerSW(config-if)# no shutdown
MultilayerSW(config-if)# exit

MultilayerSW(config)# interface vlan 40
MultilayerSW(config-if)# ip address 192.168.40.1 255.255.255.0
MultilayerSW(config-if)# no shutdown
MultilayerSW(config-if)# exit

MultilayerSW(config)# interface vlan 50
MultilayerSW(config-if)# ip address 192.168.50.1 255.255.255.0
MultilayerSW(config-if)# no shutdown
MultilayerSW(config-if)# exit

MultilayerSW(config)# ip routing
MultilayerSW(config)# ip dhcp pool vlan40
MultilayerSW(dhcp-config)# network 192.168.40.0 255.255.255.0
MultilayerSW(dhcp-config)# default-router 192.168.40.1
```

MultilayerSW(config)# ip dhcp excluded-address 192.168.40.1 192.168.40.40

MultilayerSW(config)# ip dhcp pool vlan50

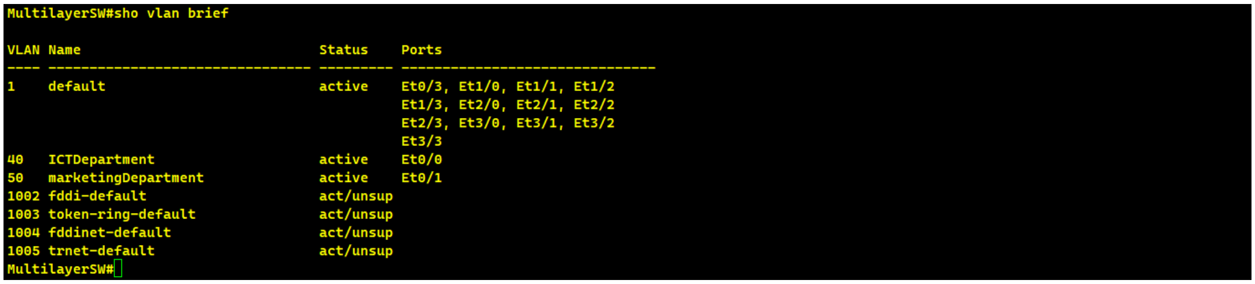
MultilayerSW(dhcp-config)# network 192.168.50.0 255.255.255.0

MultilayerSW(dhcp-config)# default-router 192.168.50.1

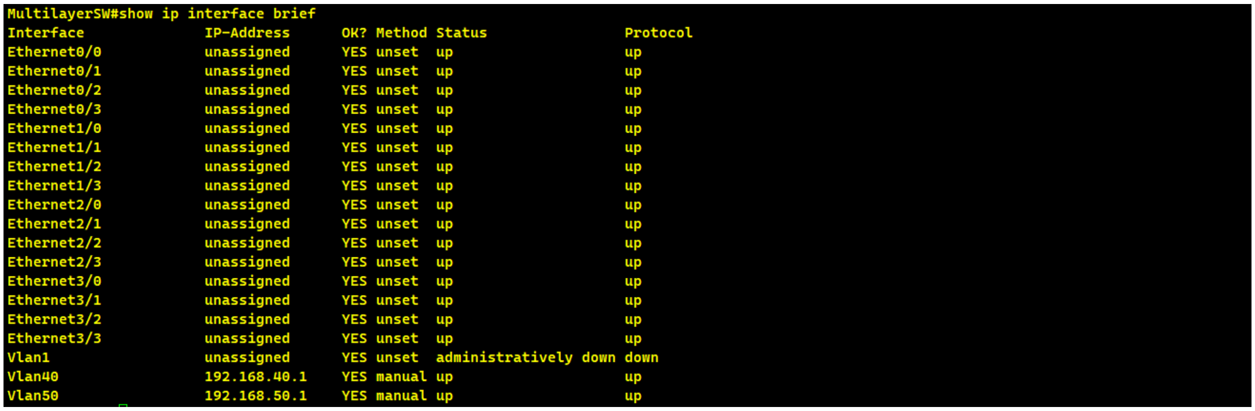
MultilayerSW(config)# ip dhcp excluded-address 192.168.50.1 192.168.50.50

Fig 1.2

Layer 3 configurations



```
MultilayerSW#sho vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/3, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3
40   ICTDepartment                    active    Et0/0
50   marketingDepartment              active    Et0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
MultilayerSW#
```



```
MultilayerSW#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan40                 192.168.40.1    YES manual up                    up
Vlan50                 192.168.50.1    YES manual up                    up
```

Firewall Setup and Configuration

Three interfaces were configured on the WatchGuard Firewall:

- WAN: Configured to use DHCP.
- LAN: Specifically designed to operate as a bridge interface.
- DMZ: Configured with a static IP.

Firewall Policies and VPN Configuration

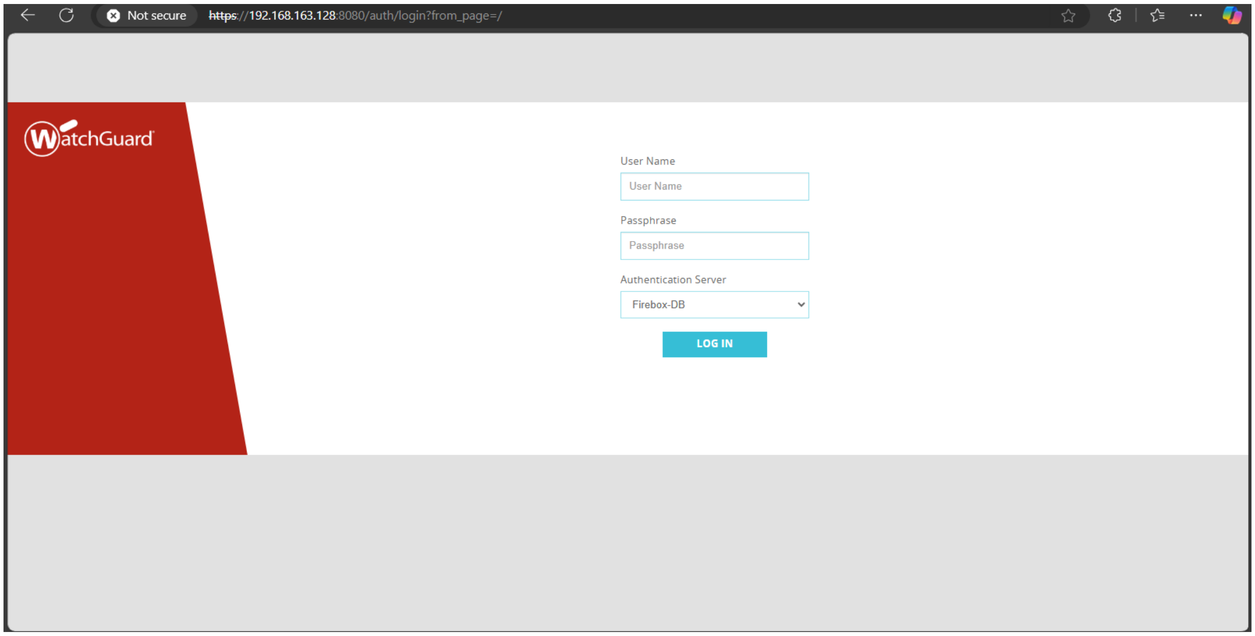
There were also policies enabled to permit only certain traffic between VLANs, HTTP, HTTPS, SMTP, POP3, ICMP for DMZ and traffic to the SSL VPN for LAN.

AES and SHA256 was used for encryption and authentication for SSL VPN for the remote use. This made it possible to manage data access using the identified user groups while the users were authenticated from the firewall level.

The client for the SSL VPN was obtained from the portal of the firewall and then run on the remote machine. Secure access certificate was also installed. The confidentiality of traffic was confirmed by using wireshark protocol.

Fig 1.3

Watchguard Web UI



Not secure https://192.168.163.128:8080/auth/login?from_page=/

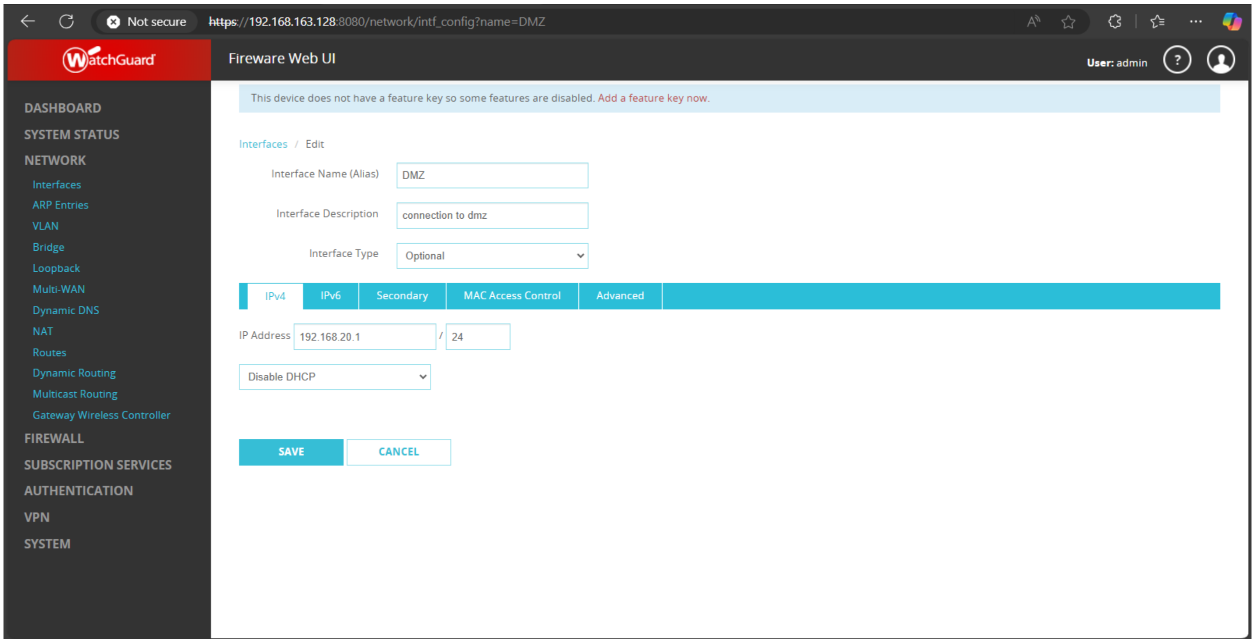
User Name: User Name

Passphrase: Passphrase

Authentication Server: Firebox-DB

Fig 1.4

DMZ interface configuration



Not secure https://192.168.163.128:8080/network/intf_config?name=DMZ

This device does not have a feature key so some features are disabled. Add a feature key now.

Interfaces / Edit

Interface Name (Alias): DMZ

Interface Description: connection to dmz

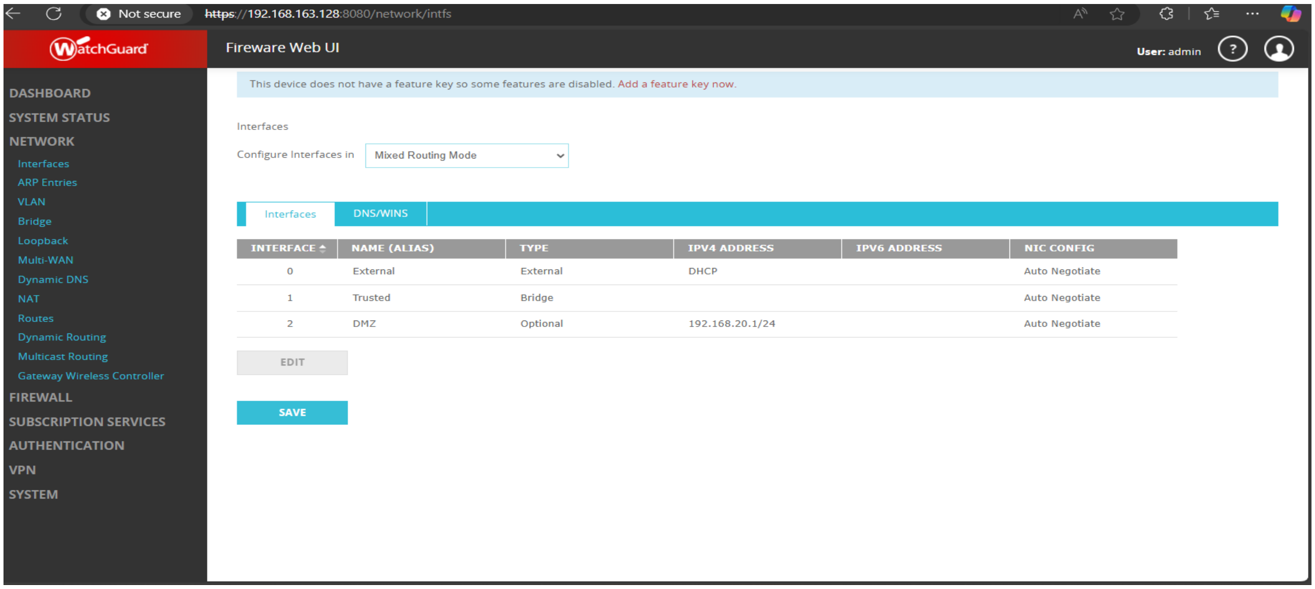
Interface Type: Optional

IP Address: 192.168.20.1 / 24

Disable DHCP

Fig 1.5

LAN,WAN and DMZ interface configured



This device does not have a feature key so some features are disabled. Add a feature key now.

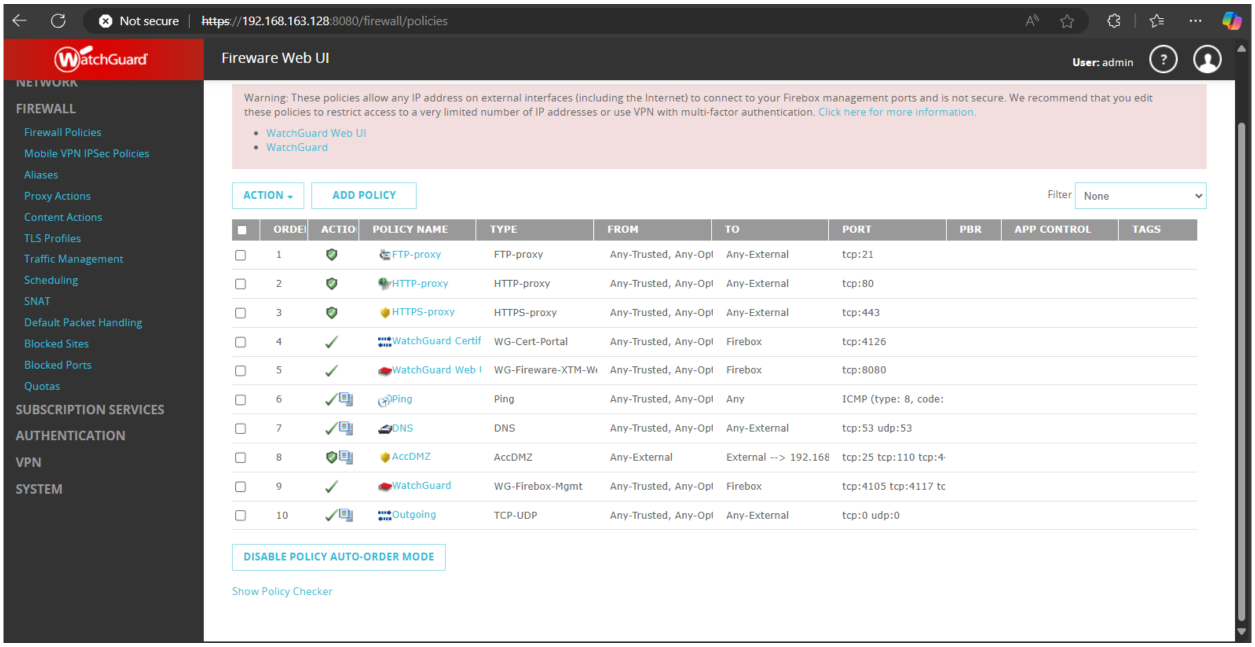
Interfaces

Configure Interfaces in: Mixed Routing Mode

INTERFACE	NAME (ALIAS)	TYPE	IPV4 ADDRESS	IPV6 ADDRESS	NIC CONFIG
0	External	External	DHCP		Auto Negotiate
1	Trusted	Bridge			Auto Negotiate
2	DMZ	Optional	192.168.20.1/24		Auto Negotiate

Fig 1.6

Configured firewall rules/policies



Warning: These policies allow any IP address on external interfaces (including the Internet) to connect to your Firebox management ports and is not secure. We recommend that you edit these policies to restrict access to a very limited number of IP addresses or use VPN with multi-factor authentication. Click here for more information.

- WatchGuard Web UI
- WatchGuard

Filter: None

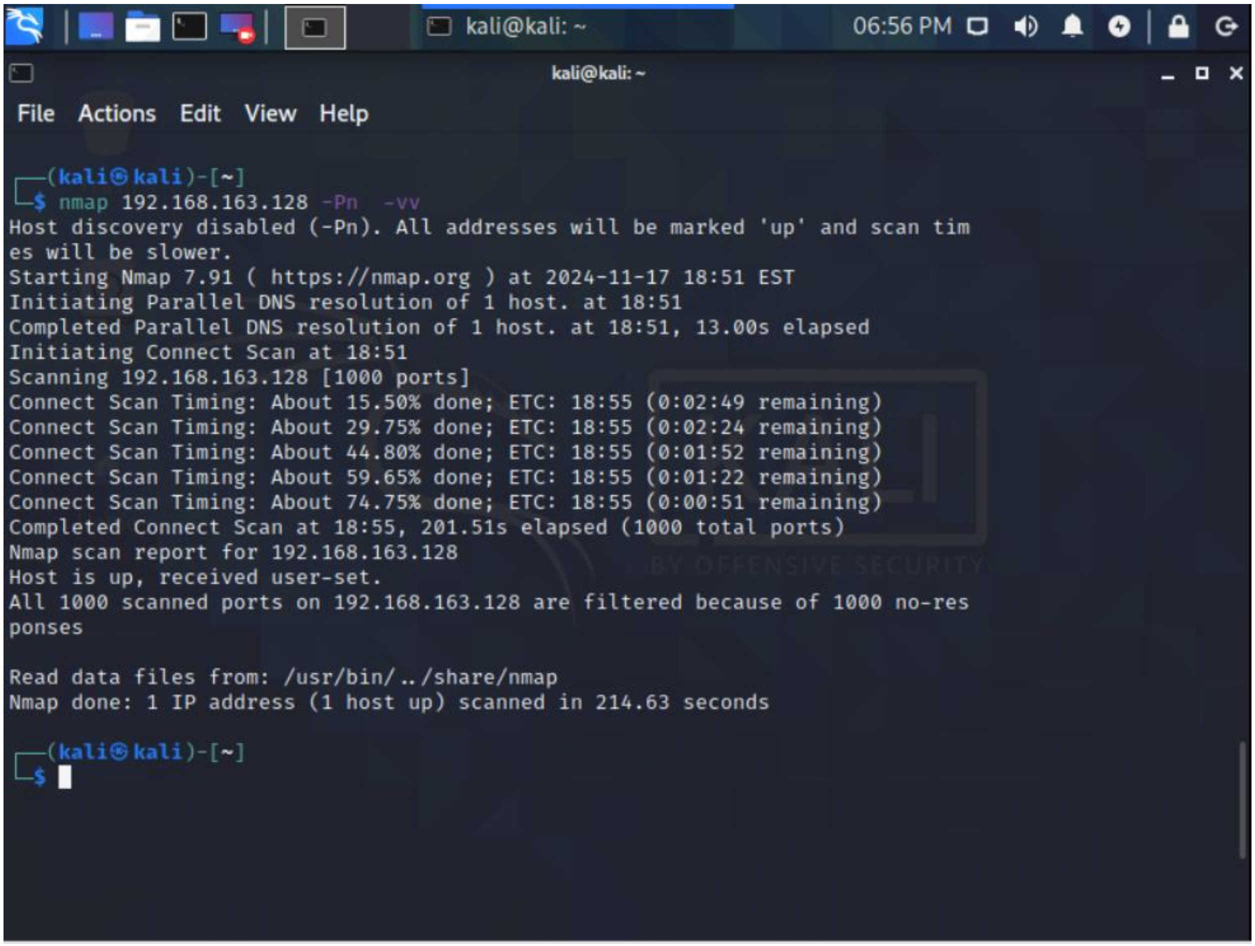
□	ORDEI	ACTIO	POLICY NAME	TYPE	FROM	TO	PORT	PBR	APP CONTROL	TAGS
□	1		FTP-proxy	FTP-proxy	Any-Trusted, Any-Opt	Any-External	tcp:21			
□	2		HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Opt	Any-External	tcp:80			
□	3		HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Opt	Any-External	tcp:443			
□	4	✓	WatchGuard Certif	WG-Cert-Portal	Any-Trusted, Any-Opt	Firebox	tcp:4126			
□	5	✓	WatchGuard Web	WG-Fireware-XTM-W	Any-Trusted, Any-Opt	Firebox	tcp:8080			
□	6	✓	Ping	Ping	Any-Trusted, Any-Opt	Any	ICMP (type: 8, code:			
□	7	✓	DNS	DNS	Any-Trusted, Any-Opt	Any-External	tcp:53 udp:53			
□	8		AccDMZ	AccDMZ	Any-External	External --> 192.168	tcp:25 tcp:110 tcp:4			
□	9	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Opt	Firebox	tcp:4105 tcp:4117 tc			
□	10	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Opt	Any-External	tcp:0 udp:0			

Firewall testing

To test the configured policies and the exposed ports to the internet we used Nmap to scan the internet facing interface / gateway.The policies looked good with only the necessary exposed port and in filtered state.The firewall was also able to drop/deny any traffic violating the policies.

Fig 1.7

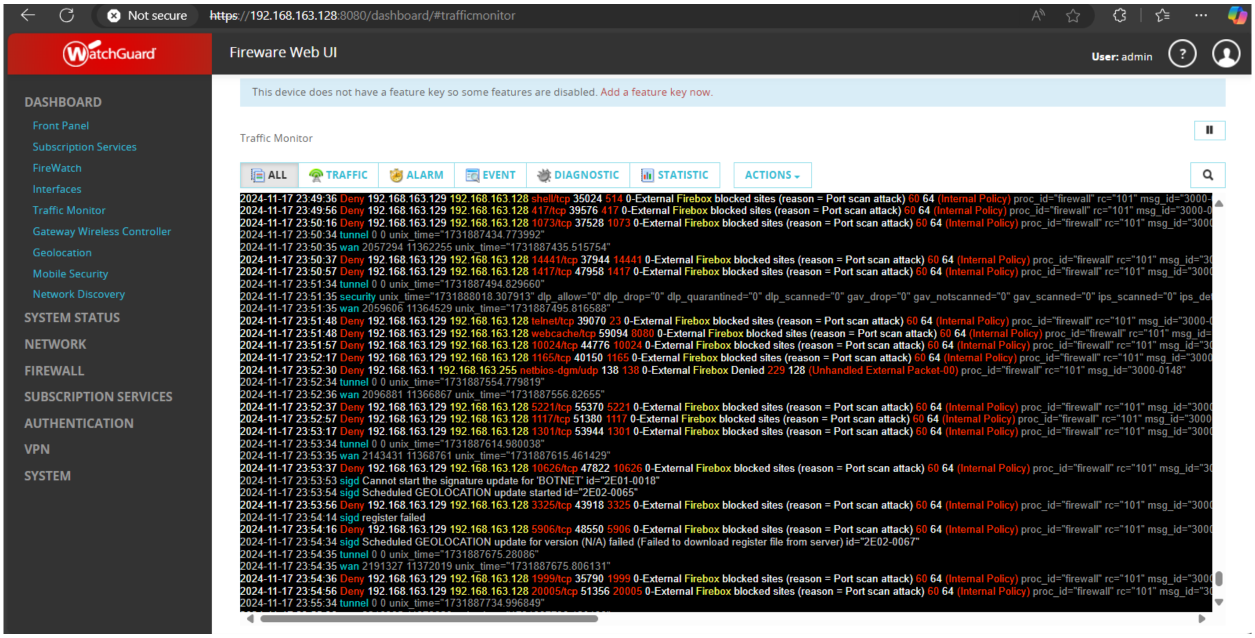
Firewall policies testing with Nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.163.128 -Pn  -vv
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2024-11-17 18:51 EST
Initiating Parallel DNS resolution of 1 host. at 18:51
Completed Parallel DNS resolution of 1 host. at 18:51, 13.00s elapsed
Initiating Connect Scan at 18:51
Scanning 192.168.163.128 [1000 ports]
Connect Scan Timing: About 15.50% done; ETC: 18:55 (0:02:49 remaining)
Connect Scan Timing: About 29.75% done; ETC: 18:55 (0:02:24 remaining)
Connect Scan Timing: About 44.80% done; ETC: 18:55 (0:01:52 remaining)
Connect Scan Timing: About 59.65% done; ETC: 18:55 (0:01:22 remaining)
Connect Scan Timing: About 74.75% done; ETC: 18:55 (0:00:51 remaining)
Completed Connect Scan at 18:55, 201.51s elapsed (1000 total ports)
Nmap scan report for 192.168.163.128
Host is up, received user-set.
All 1000 scanned ports on 192.168.163.128 are filtered because of 1000 no-res
ponses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 214.63 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 1.8

Firewall policies blocking nmap scans



This device does not have a feature key so some features are disabled. Add a feature key now.

Traffic Monitor

```
2024-11-17 23:49:36 Deny 192.168.163.129 192.168.163.128 shell/tcp 35024 514 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000-
2024-11-17 23:49:56 Deny 192.168.163.129 192.168.163.128 417/tcp 39576 417 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000-0
2024-11-17 23:50:16 Deny 192.168.163.129 192.168.163.128 1073/tcp 37528 1073 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:50:34 tunnel 0 0 unix_time="1731887434.773992"
2024-11-17 23:50:35 wan 2057294 11362255 unix_time="1731887435.515754"
2024-11-17 23:50:37 Deny 192.168.163.129 192.168.163.128 14441/tcp 37944 14441 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="30
2024-11-17 23:50:57 Deny 192.168.163.129 192.168.163.128 1417/tcp 47958 1417 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:51:34 tunnel 0 0 unix_time="1731887494.829660"
2024-11-17 23:51:35 security unix_time="1731888018.307913" dlp_allow="0" dlp_drop="0" dlp_quarantined="0" dlp_scanned="0" gav_drop="0" gav_notscanned="0" gav_scanned="0" ips_scanned="0" ips_de
2024-11-17 23:51:35 wan 2059606 11364529 unix_time="1731887495.816588"
2024-11-17 23:51:48 Deny 192.168.163.129 192.168.163.128 telnet/tcp 39070 23 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000-
2024-11-17 23:51:48 Deny 192.168.163.129 192.168.163.128 webcache/tcp 59094 8080 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id=
2024-11-17 23:51:57 Deny 192.168.163.129 192.168.163.128 10024/tcp 44776 10024 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="30
2024-11-17 23:52:17 Deny 192.168.163.129 192.168.163.128 1165/tcp 40150 1165 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:52:30 Deny 192.168.163.1 192.168.163.255 netbios-dgm/udp 138 138 0-External Firebox Denied 229 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148"
2024-11-17 23:52:34 tunnel 0 0 unix_time="1731887554.779819"
2024-11-17 23:52:36 wan 2096881 11366867 unix_time="1731887556.82655"
2024-11-17 23:52:37 Deny 192.168.163.129 192.168.163.128 5221/tcp 55370 5221 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:52:57 Deny 192.168.163.129 192.168.163.128 1117/tcp 51380 1117 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:53:17 Deny 192.168.163.129 192.168.163.128 1301/tcp 53944 1301 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:53:34 tunnel 0 0 unix_time="1731887614.980038"
2024-11-17 23:53:35 wan 2143431 11368761 unix_time="1731887615.461429"
2024-11-17 23:53:37 Deny 192.168.163.129 192.168.163.128 10626/tcp 47822 10626 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="30
2024-11-17 23:53:53 sigd Cannot start the signature update for 'BOTNET' id="2E01-0018"
2024-11-17 23:53:54 sigd Scheduled GEOLOCATION update started id="2E02-0065"
2024-11-17 23:53:56 Deny 192.168.163.129 192.168.163.128 3325/tcp 43918 3325 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:54:14 sigd register failed
2024-11-17 23:54:16 Deny 192.168.163.129 192.168.163.128 5906/tcp 48550 5906 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:54:34 sigd Scheduled GEOLOCATION update for version (N/A) failed (Failed to download register file from server) id="2E02-0067"
2024-11-17 23:54:35 tunnel 0 0 unix_time="1731887675.28086"
2024-11-17 23:54:35 wan 2191327 11372019 unix_time="1731887675.806131"
2024-11-17 23:54:36 Deny 192.168.163.129 192.168.163.128 1999/tcp 35790 1999 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="3000
2024-11-17 23:54:56 Deny 192.168.163.129 192.168.163.128 20005/tcp 51356 20005 0-External Firebox blocked sites (reason = Port scan attack) 60 64 (Internal Policy) proc_id="firewall" rc="101" msg_id="30
2024-11-17 23:55:34 tunnel 0 0 unix_time="1731887734.996849"
```

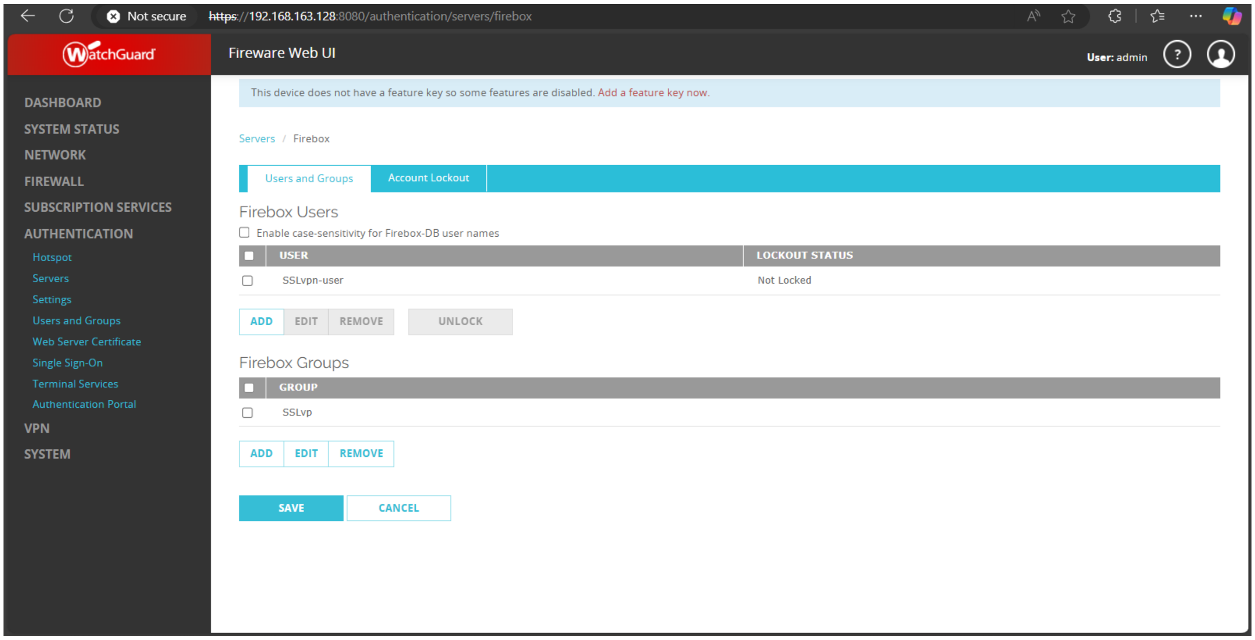
VPN Configuration

We configures SSL vpn to allowa internal resource/service access by the remote machine.AES and SHA256 was used for encryption and authentication for SSL VPN for the remote use. This made it possible to manage data access using the identified user groups while the users were authenticated from the firewall level.

The client for the SSL VPN was obtained from the portal of the firewall and then run on the remote machine. Secure access certificate was also installed. The confidentiality of traffic was confirmed by using wireshark protocol.

Fig 1.9

SSL vpn user and group configuration



Not secure https://192.168.163.128:8080/authentication/servers/firebox

Fireware Web UI

User: admin

This device does not have a feature key so some features are disabled. Add a feature key now.

Servers / Firebox

Firebox Users

□ Enable case-sensitivity for Firebox-DB user names

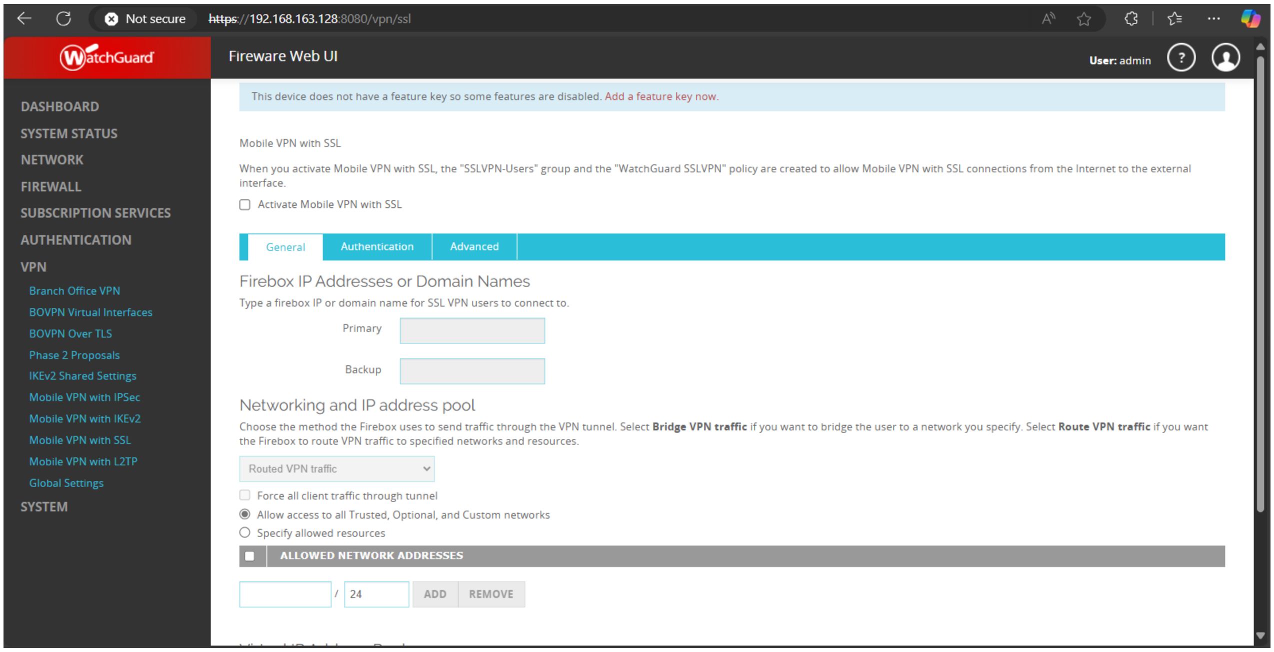
□	USER	LOCKOUT STATUS
□	SSLvpn-user	Not Locked

Firebox Groups

□	GROUP
□	SSLvp

Fig 2.0

SSL vpn configuration



This device does not have a feature key so some features are disabled. Add a feature key now.

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

□ Activate Mobile VPN with SSL

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

Backup

Networking and IP address pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

□ Force all client traffic through tunnel

● Allow access to all Trusted, Optional, and Custom networks

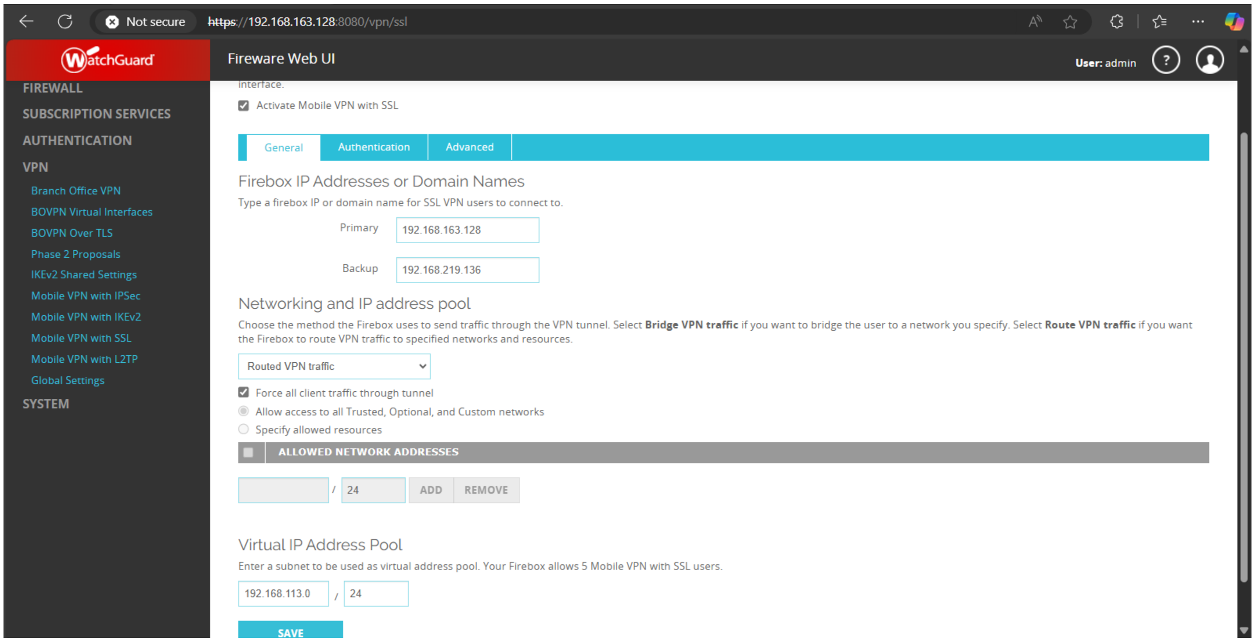
○ Specify allowed resources

□ ALLOWED NETWORK ADDRESSES

/ 24

Fig 2.1

Configured firewall rules/policies



interface.

☑ Activate Mobile VPN with SSL

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary 192.168.163.128

Backup 192.168.219.136

Networking and IP address pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

☑ Force all client traffic through tunnel

● Allow access to all Trusted, Optional, and Custom networks

○ Specify allowed resources

□ ALLOWED NETWORK ADDRESSES

/ 24

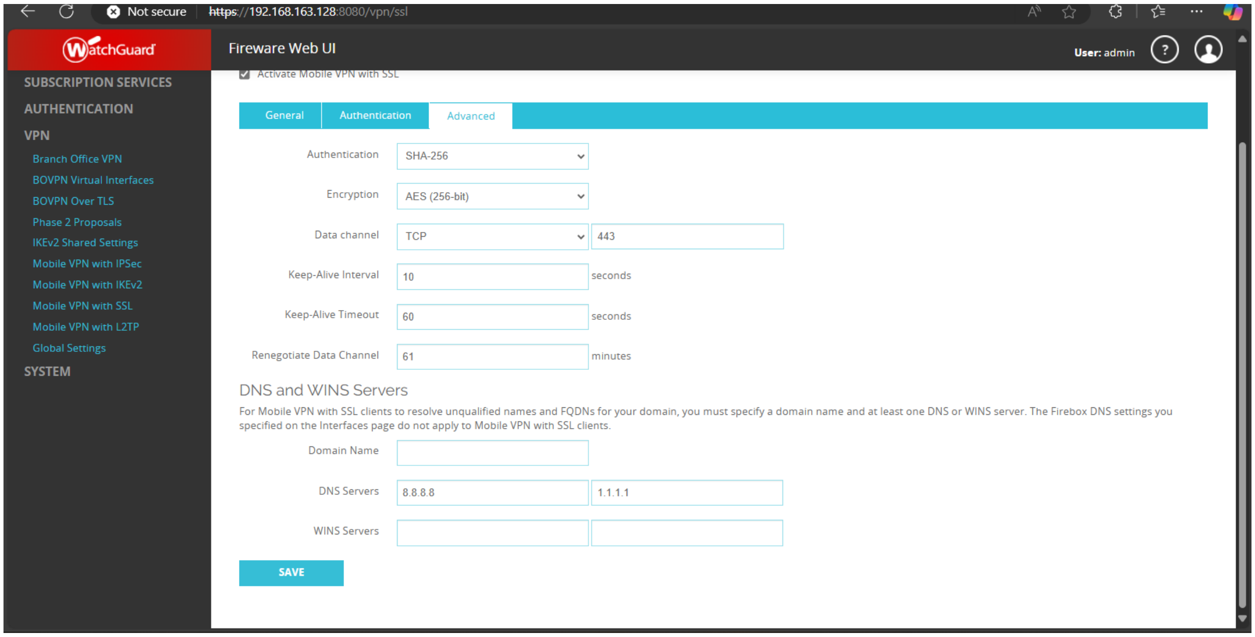
Virtual IP Address Pool

Enter a subnet to be used as virtual address pool. Your Firebox allows 5 Mobile VPN with SSL users.

192.168.113.0 / 24

Fig 2.2

SSL vpn authentication and encryption configuration



☑ Activate Mobile VPN with SSL

Authentication: SHA-256

Encryption: AES (256-bit)

Data channel: TCP 443

Keep-Alive Interval: 10 seconds

Keep-Alive Timeout: 60 seconds

Renegotiate Data Channel: 61 minutes

DNS and WINS Servers

For Mobile VPN with SSL clients to resolve unqualified names and FQDNs for your domain, you must specify a domain name and at least one DNS or WINS server. The Firebox DNS settings you specified on the Interfaces page do not apply to Mobile VPN with SSL clients.

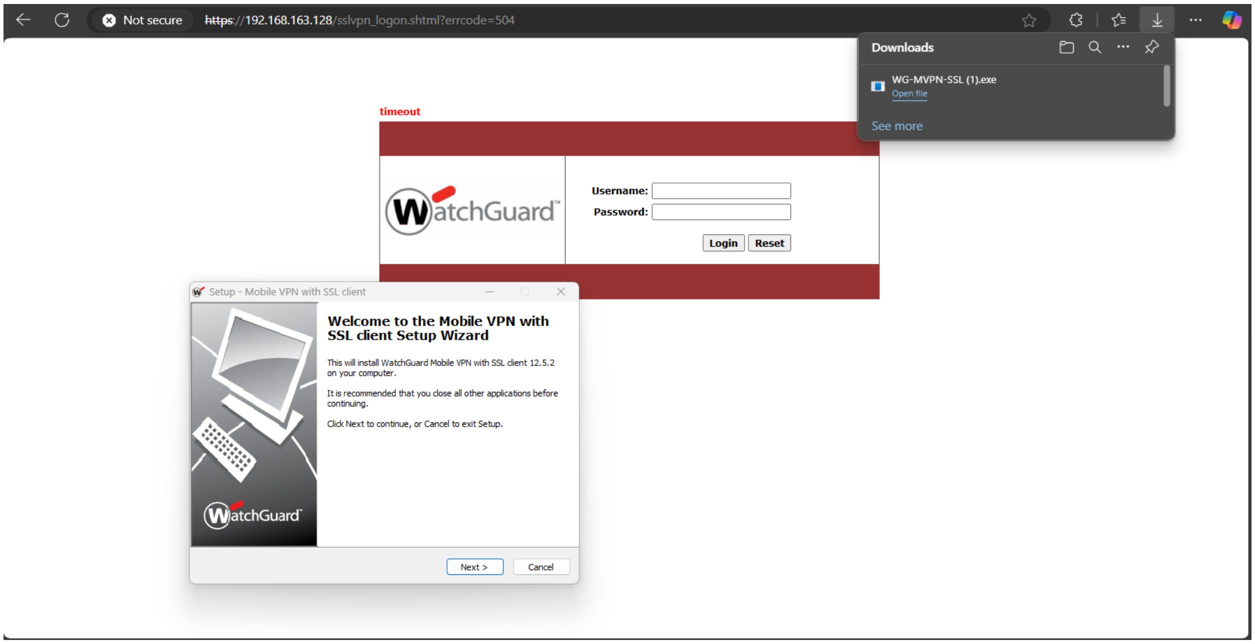
Domain Name:

DNS Servers: 8.8.8.8 1.1.1.1

WINS Servers:

Fig 2.3

SSL vpn user portal



Welcome to the Mobile VPN with SSL client Setup Wizard

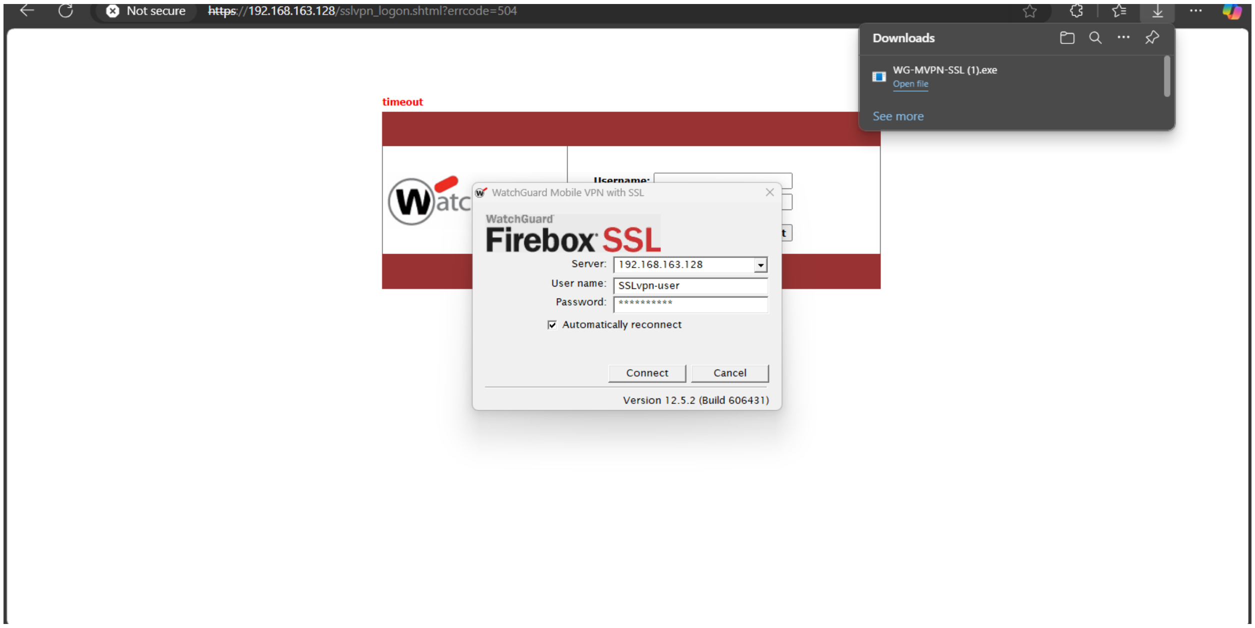
This will install WatchGuard Mobile VPN with SSL client 12.5.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Fig 2.4

SSL vpn connection establishment



https://192.168.163.128/sslvpn_logon.shtml?errcode=504

WG-MVPN-SSL (1).exe
Open file

Username:

Server: 192.168.163.128

User name: SSLvpn-user

Password: **********

☑ Automatically reconnect

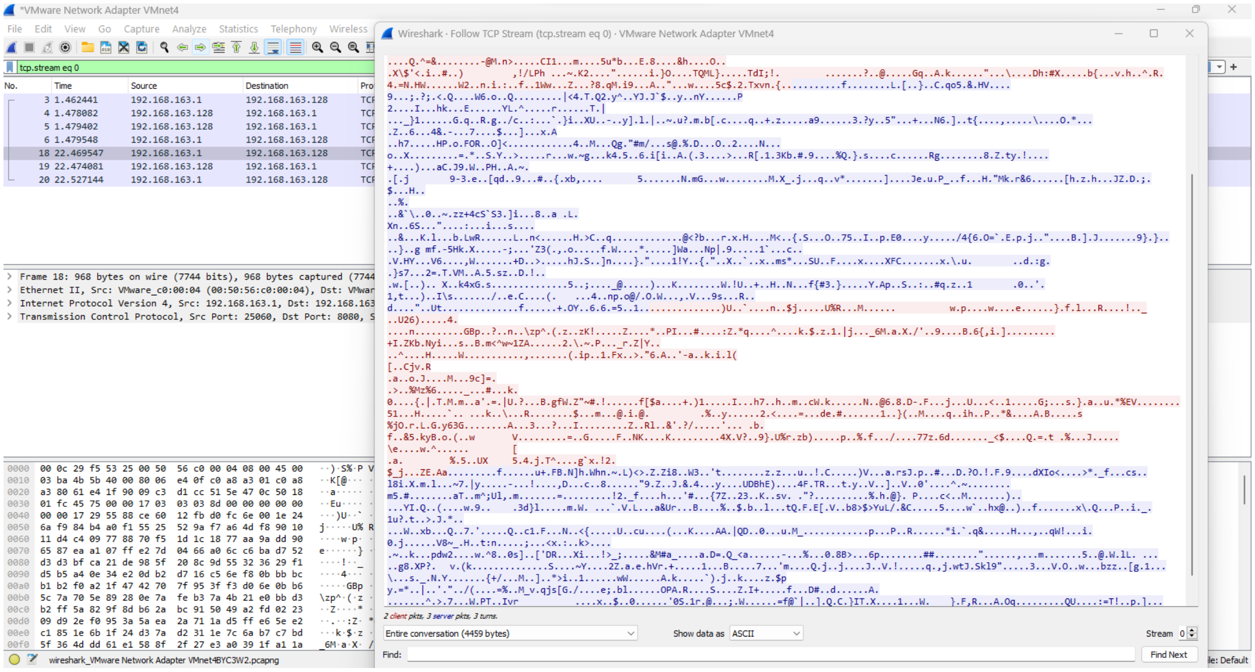
Version 12.5.2 (Build 606431)

Testing SSL vpn encryption

To test the remote access vpn we monitored the specific vpn traffic with wireshark to verify the encryption which showed that the traffic was encrypted .

Fig 2.5

SSLvpn encryption testing



*VMware Network Adapter VMnet4
File Edit View Go Capture Analyze Statistics Telephony Wireless

```
tcp.stream eq 0

No.   Time        Source            Destination       Pro
  3   1.462441    192.168.163.1     192.168.163.128   TC
  4   1.478082    192.168.163.128   192.168.163.1     TC
  5   1.479402    192.168.163.128   192.168.163.1     TC
  6   1.479548    192.168.163.1     192.168.163.128   TC
 18   22.469547   192.168.163.1     192.168.163.128   TC
 19   22.474081   192.168.163.128   192.168.163.1     TC
 20   22.527144   192.168.163.1     192.168.163.128   TC

> Frame 18: 968 bytes on wire (7744 bits), 968 bytes captured (7744
> Ethernet II, Src: VMware_c0:00:04 (00:50:56:c0:00:04), Dst: VMwar
> Internet Protocol Version 4, Src: 192.168.163.1, Dst: 192.168.163
> Transmission Control Protocol, Src Port: 25060, Dst Port: 8080, S

0000  00 0c 29 f5 53 25 00 50  56 c0 00 04 08 00 45 00   ··)·S%·P V
0010  03 ba 4b 5b 40 00 80 06  e4 0f c0 a8 a3 01 c0 a8   ··K[@···  ·
0020  a3 80 61 e4 1f 90 09 c3  d1 cc 51 5e 47 0c 50 18   ··a·····  ·
0030  01 fc 45 75 00 00 17 03  03 03 8d 00 00 00 00 00   ··Eu····  ·
0040  00 00 17 29 55 88 ce 60  12 fb d0 fc 6e 00 1e 24   ···)U··`  ·
0050  6a f9 84 b4 a0 f1 55 25  52 9a f7 a6 4d f8 90 10   j·····U% R
0060  11 d4 c4 09 77 88 70 f5  1d 1c 18 77 aa 9a dd 90   ····w·p·  ·
0070  65 87 ea a1 07 ff e2 7d  04 66 a0 6c c6 ba d7 52   e······}  ·
0080  d3 d3 bf ca 21 de 98 5f  20 8c 9d 55 32 36 29 f1   ····!··_
0090  d5 b5 a4 0e 34 e2 0d b2  d7 16 c5 6e f8 0b bb bc   ····4···  ·
00a0  b1 b2 f0 a2 1f 47 42 70  7f 95 3f f3 d0 6e 0b b6   ·····GBp  ·
00b0  5c 7a 70 5e 89 28 0e 7a  fe b3 7a 4b 21 e0 bb d3   \zp^·(·z  ·
00c0  b2 ff 5a 82 9f 8d b6 2a  bc 91 50 49 a2 fd 02 23   ··Z····*  ·
00d0  09 d9 2e f0 95 3a 5a ea  2a 71 1a d5 ff e6 5e e2   ··.··:Z·  *
00e0  c1 85 1e 6b 1f 24 d3 7a  d2 31 1e 7c 6a b7 c7 bd   ···k·$·z  ·
00f0  5f 36 4d dd 61 e1 58 8f  2f 27 e3 a0 39 1f a1 1a   _6M·a·X·  /

wireshark_VMware Network Adapter VMnet4BYC3W2.pcapng
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · VMware Network Adapter VMnet4

```
....Q.^=&........-@M.n>.....CI1...m....5u*b...E.8....&h....O..
.X\$'<.i..#..)        ,!/LPh ...~.K2....".....i.}O....TQML}.....TdI;!.        .......?..@.....Gq..A.k......"...\....Dh:#X.....b{...v.h..^.R.
4.=N.HW......W2..n.i.:..f..1Ww...Z...?8.qM.i9...A.."...w....5c$.2.Txvn.{..........f........L.[..}..C.qo5.&.HV....
9...;.?;.<.Q....W6.o..Q.........|<4.T.Q2.y^..YJ.J`$..y..nY......P
2....I...hk...E......YL.^.....r......T.|
..._}1......G.q..R.g../c..:...`.}i..XU..-..y].l.|..~.u?.m.b[.c....q..+.z.....a9......3.?y..5"...+...N6.]..t{....,.....\....O.*...
.Z..6...4&.-...7....$...]...x.A
..h7.....HP.o.FOR..O]<............4..M...Qg."#m/...s@.%.D...O..2....N...
o..X.........=.*..S.Y..>.....r...w.~g...k4.5..6.i[i..A.(.3....>...R[.1.3Kb.#.9....%Q.}.s....c......Rg........8.Z.ty.!....
+....)...aC.J9.W..PH..A.~.
.[.j        9-3.e..[qd..9...#..{.xb,....       5.......N.mG...w........M.X_.j...q..v*.......]....Je.u.P_..f...H."Mk.r&6......[h.z.h...JZ.D.;.
$...H..
..%.
..&`\..0..~.zz+4cS`S3.]i...8..a .L.
Xn..6S..."....:...i...s....
..&...K.l...b.LwR......L..n<......H.>C..q.............@<?b...r.x.H....M<..{.S...O..75..I..p.E0....y...../4{6.O=`.E.p.j.."....B.].J.......9}.}..
..}..g mf.-5Hk.X.....-;...'Z3(.,.o.....f.W....*.....]Wa...Np|.9.....1`...c..
.V.HY...V6....,W.......+D..>.....hJ.S..]n....}."....1!Y..{."..X..`..x..ms*...SU..F....x....XFC.......x.\.u.        ..d.:g.
.}s7...2=.T.VM..A.5.sz..D.!..
.w.[..).. X..k4xG.s..............5..;...._@.....)...K........W.!U..+..H..N...f{#3.}.....Y.Ap..S..:..#q.z..1        .0..'.
1,t...)..I\s......./..e.C....(.    ...4..np.o@/.O.W...,.V...9s...R..
d...."..Ut..............f......+.OY..6.6.=5..1...............)U..`....n..$j.....U%R...M......          w.p....w....e......}.f.l...R....!.._
..U26).....4.
....n.........GBp..?..n..\zp^.(.z..zK!.....Z....*..PI...#....:Z.*q....^....k.$.z.1.|j..._6M.a.X./'..9....B.6{,i.].........
+I.ZKb.Nyi...s..B.m<^w~1ZA......2.\.~.P..._r.Z|Y..
..^....H.....W..........,.......(.ip..1.Fx..>."6.A..'-a..k.i.l(
[..Cjv.R
.a..o.J....M...9c]=.
.>..%Mz%6....._...#...k.
0....{.|.T.M.m..a'.=.|U.?...B.gfW.Z"~#.!......f[$a....+.)1.....I...h7..h..m..cW.k......N..@6.8.D-.F...j...U...<..1.....G;...s.}.a..u.*%EV........
51...H.....`.. ...k..\...R........$...m...@.i.@.         .%..y......2.<....=...de.#.......1..}(..M....q..ih..P..*&....A.B.....s
%jO.r.L.G.y63G........A...3...?...I.........Z..Rl..&'.?/.....'... .b.
f..&5.kyB.o.(..w       V.........=..G.....F..NK....K.........4X.V?..9}.U%r.zb).....p..%.f.../....77z.6d......_<$....Q.=.t .%...J.....
\e....w.^......        [
.a.        %.5..UX    5.4.j.T^....g`x.!2.
$_j...ZE.Aa.........f......u+.FB.N]h.Whn.~.L)<>.Z.Zi8..W3..'t........z.z...u..!.C.....)V...a.rsJ.p..#...D.?O.!.F.9....dXIo<....>*._f...cs..
l8i.X.m.l...~7.|y.....-...!....,D...c..8......"9.Z..J.&.4...y....UDBhE)....4F.TR...t.y..V..]..V..0'....^.~........
m5.#........aT..m^;Ul,.m.......=.........!2._f....h...'#...{7Z..23..K..sv. ."?..........%.h.@}. P....c<..M.......)..
...YI.Q..(....w.9..    .3d}l.....m.W. ...`.V.L...a&Ur...B....%..$.b..l...tQ.F.E[.V..b8>$>YuL/.&C.....5....w`..hx@..)..f.......x\.Q...P..i._.
1u?.t..>.J.*..
...W..xb...Q..7.'.....Q..c1.F...N..<{.....U..cu....(...K....AA.|QD..0...u.M_............p...P..R......*i.`.q&.....H...,..qW!...i.
0.j......V8~_.H..t:n.....;...<x.:..k>....
.~..k...pdw2....w.^8..0s]..['DR...Xi...!>_;.....&M#a_....a.D=.Q_<a......-...%...0.8B>...6p........##........"......,...m.......5..@.W.lL. ...
..g8.XP?.  v.(k.............S....~Y....2Z.a.e.hVr.+.....1...B.....7...'m....Q.j..j....J..V.!.....q.,j.wtJ.Skl9".....3...V.O..w...bzz..[g.1...
\...s._.N.Y.......{+/...M..]..*>i..1......wW......A.k.....`).j..k....z.$p
y.=*..|..'."../(....=%..M_v.qjs[G./....e;.bl......OPA.R....S....Z.I+.....f...D#..d......A.
.......^.>.7...W.PT..Ivr         ....x..$..0......'0S.1r.@...;.W......=f@`|..].Q.C.}IT.X....1...W.    }.F,R...A.Oq.........QU....:=T!..p.]...

2 client pkts, 3 server pkts, 3 turns.
Entire conversation (4459 bytes)    Show data as ASCII    Stream 0
```

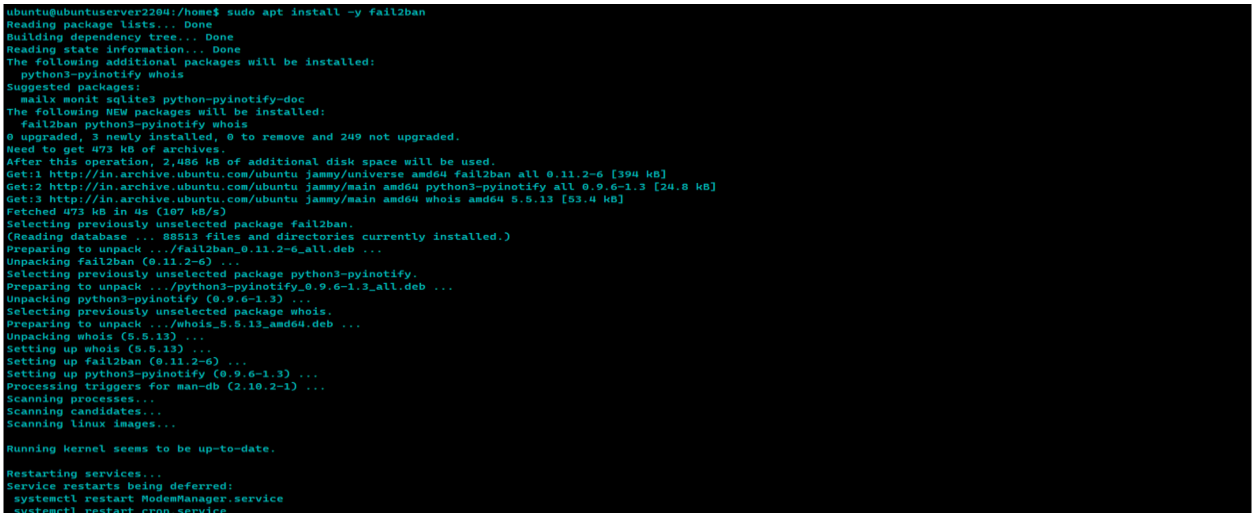
IDS Implementation

A Linux Ubuntu based DMZ server was deployed on virtual machines with content IDS system called Fail2ban IDS. A custom SSH intrusion rule was configured as follows:

```
[sshd]

enabled = true

port = ssh

logpath = /var/log/auth.log

bantime = 3600
```

Fig 2.6

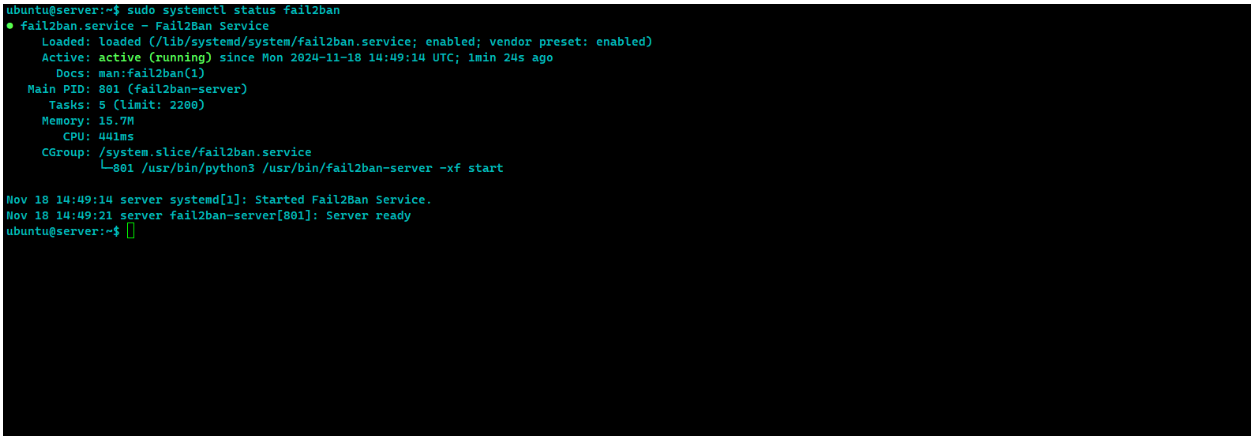
Installing Fail2ban IDS



```
ubuntu@ubuntuserver2204:/home$ sudo apt install -y fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 249 not upgraded.
Need to get 473 kB of archives.
After this operation, 2,486 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 fail2ban all 0.11.2-6 [394 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyinotify all 0.9.6-1.3 [24.8 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 whois amd64 5.5.13 [53.4 kB]
Fetched 473 kB in 4s (107 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 88513 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-6_all.deb ...
Unpacking fail2ban (0.11.2-6) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-1.3_all.deb ...
Unpacking python3-pyinotify (0.9.6-1.3) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.13_amd64.deb ...
Unpacking whois (5.5.13) ...
Setting up whois (5.5.13) ...
Setting up fail2ban (0.11.2-6) ...
Setting up python3-pyinotify (0.9.6-1.3) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
Service restarts being deferred:
 systemctl restart ModemManager.service
 systemctl restart cron.service
```

Fig 2.7

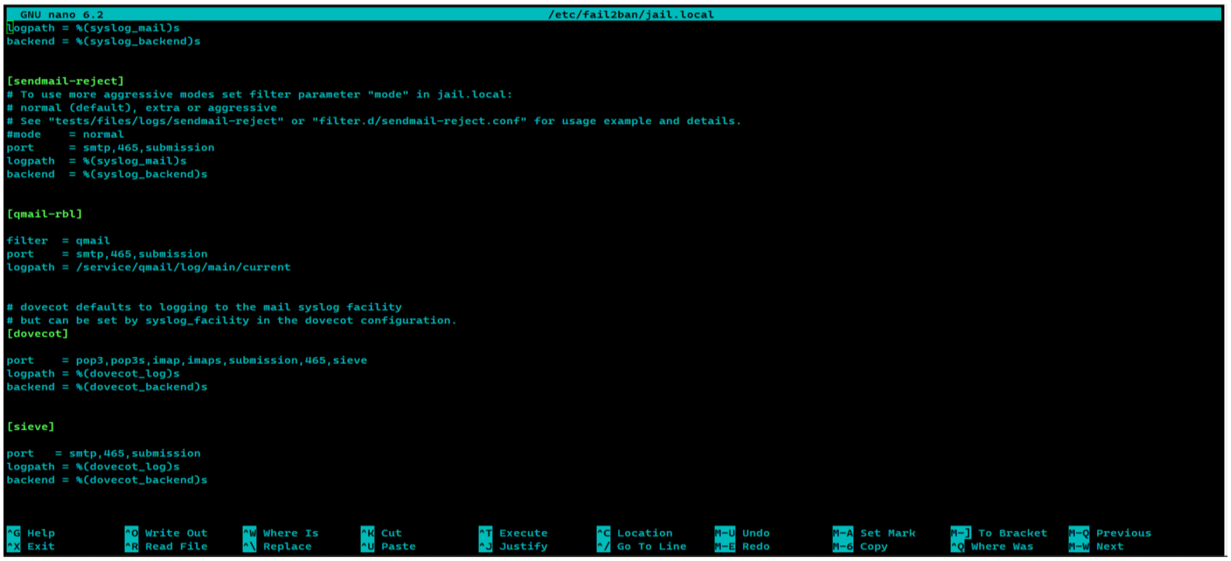
IDS status



```
ubuntu@server:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-11-18 14:49:14 UTC; 1min 24s ago
       Docs: man:fail2ban(1)
   Main PID: 801 (fail2ban-server)
      Tasks: 5 (limit: 2200)
     Memory: 15.7M
        CPU: 441ms
     CGroup: /system.slice/fail2ban.service
             └─801 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 18 14:49:14 server systemd[1]: Started Fail2Ban Service.
Nov 18 14:49:21 server fail2ban-server[801]: Server ready
ubuntu@server:~$ 
```

Fig 2.8

IDS configuration and adding custom rule



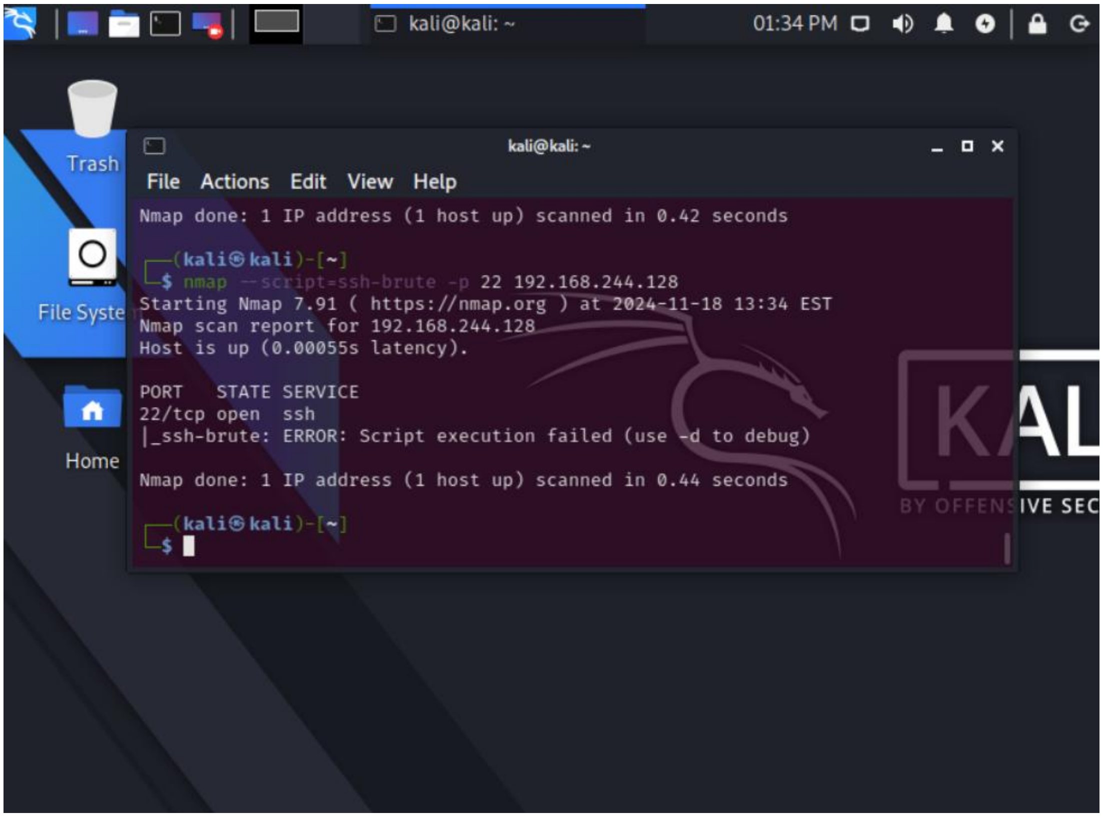
```
  GNU nano 6.2                                              /etc/fail2ban/jail.local
logpath = %(syslog_mail)s
backend = %(syslog_backend)s


[sendmail-reject]
# To use more aggressive modes set filter parameter "mode" in jail.local:
# normal (default), extra or aggressive
# See "tests/files/logs/sendmail-reject" or "filter.d/sendmail-reject.conf" for usage example and details.
#mode     = normal
port      = smtp,465,submission
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s


[qmail-rbl]

filter  = qmail
port    = smtp,465,submission
logpath = /service/qmail/log/main/current


# dovecot defaults to logging to the mail syslog facility
# but can be set by syslog_facility in the dovecot configuration.
[dovecot]

port    = pop3,pop3s,imap,imaps,submission,465,sieve
logpath = %(dovecot_log)s
backend = %(dovecot_backend)s


[sieve]

port   = smtp,465,submission
logpath = %(dovecot_log)s
backend = %(dovecot_backend)s


^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket M-Q Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was   M-W Next
```

IDS testing.

To verify that the IDS can detect anomalous traffic we simulated ssh bruteforce attack to ward the server and Fail2ban successfully detected the traffic.

Fig 2.9

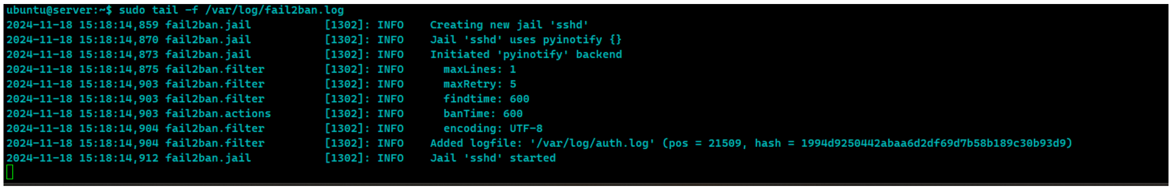
Testing IDS with simulated attack



```
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-brute -p 22 192.168.244.128
Starting Nmap 7.91 ( https://nmap.org ) at 2024-11-18 13:34 EST
Nmap scan report for 192.168.244.128
Host is up (0.00055s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_ssh-brute: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 3.0

IDS testing: log shows ssh bruteforce blocked



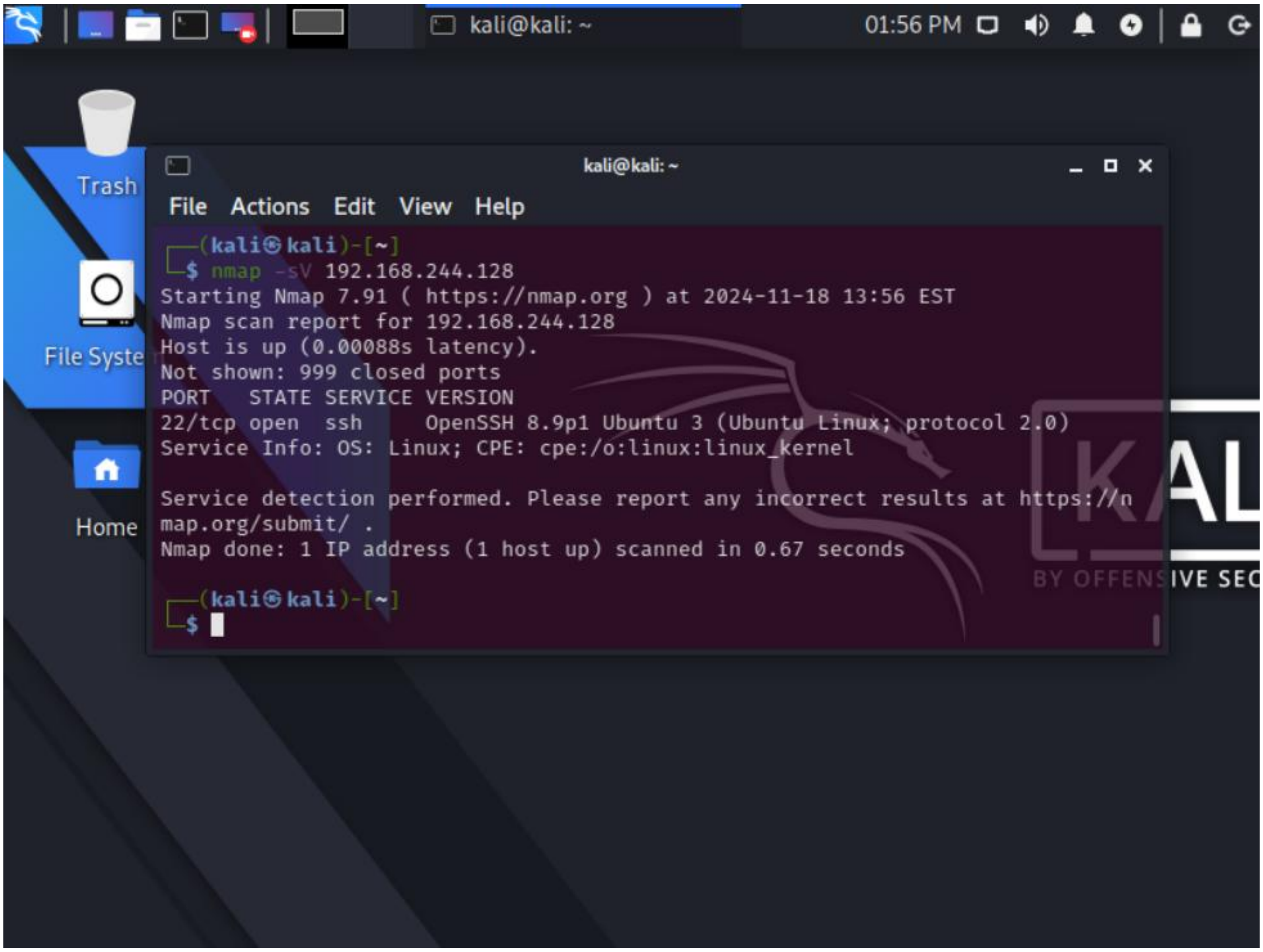
```
ubuntu@server:~$ sudo tail -f /var/log/fail2ban.log
2024-11-18 15:18:14,859 fail2ban.jail           [1302]: INFO    Creating new jail 'sshd'
2024-11-18 15:18:14,870 fail2ban.jail           [1302]: INFO    Jail 'sshd' uses pyinotify {}
2024-11-18 15:18:14,873 fail2ban.jail           [1302]: INFO    Initiated 'pyinotify' backend
2024-11-18 15:18:14,875 fail2ban.filter         [1302]: INFO      maxLines: 1
2024-11-18 15:18:14,903 fail2ban.filter         [1302]: INFO      maxRetry: 5
2024-11-18 15:18:14,903 fail2ban.filter         [1302]: INFO      findtime: 600
2024-11-18 15:18:14,903 fail2ban.actions        [1302]: INFO      banTime: 600
2024-11-18 15:18:14,904 fail2ban.filter         [1302]: INFO      encoding: UTF-8
2024-11-18 15:18:14,904 fail2ban.filter         [1302]: INFO    Added logfile: '/var/log/auth.log' (pos = 21509, hash = 1994d9250442abaa6d2df69d7b58b189c30b93d9)
2024-11-18 15:18:14,912 fail2ban.jail           [1302]: INFO    Jail 'sshd' started
```

Testing and Security Assessment

To test and verify the implemented security we used nmap to footprint the network and tried bruteforce attack to the firewall web UI which actually had positive results meaning it even went to an extent of the set policies recognizing the malicious traffic and dropping the attacking machine traffic.We used Nmap and hydra in this two cases.One of the weakness identified was that port 22 was exposed to the internet which can be a risk of being exploited by a zero day.

Fig 3.1

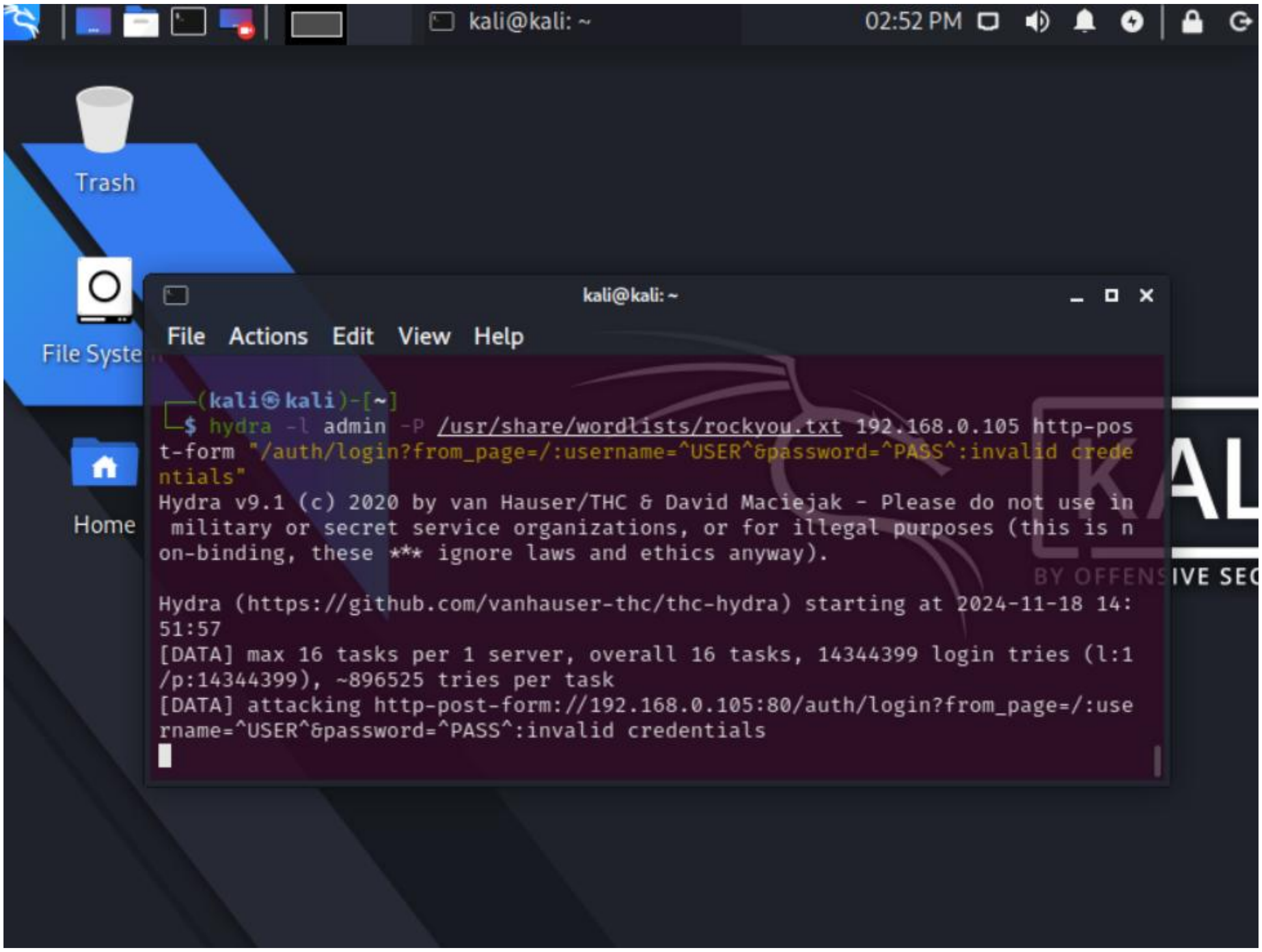
IDS testing: log shows ssh bruteforce blocked



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.244.128
Starting Nmap 7.91 ( https://nmap.org ) at 2024-11-18 13:56 EST
Nmap scan report for 192.168.244.128
Host is up (0.00088s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 3.2

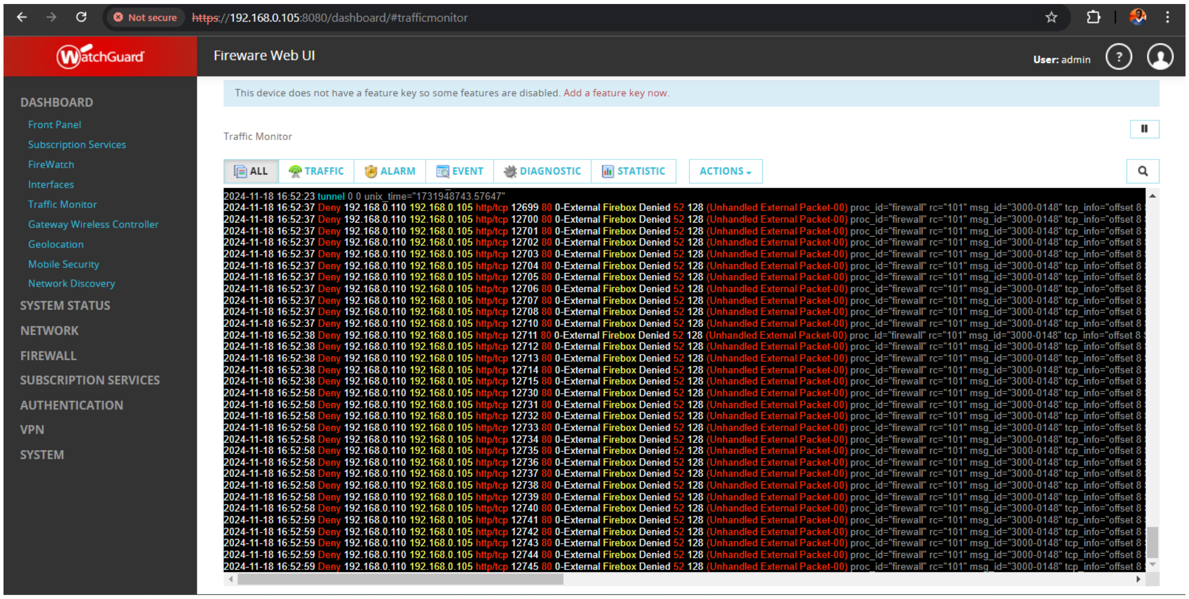
Attack vector II: firewall web UI login bruteforce.



```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.105 http-pos
t-form "/auth/login?from_page=/:username=^USER^&password=^PASS^:invalid crede
ntials"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-18 14:
51:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.0.105:80/auth/login?from_page=/:use
rname=^USER^&password=^PASS^:invalid credentials
█
```

Fig 3.3

Firewall blocked hydra bruteforce probes



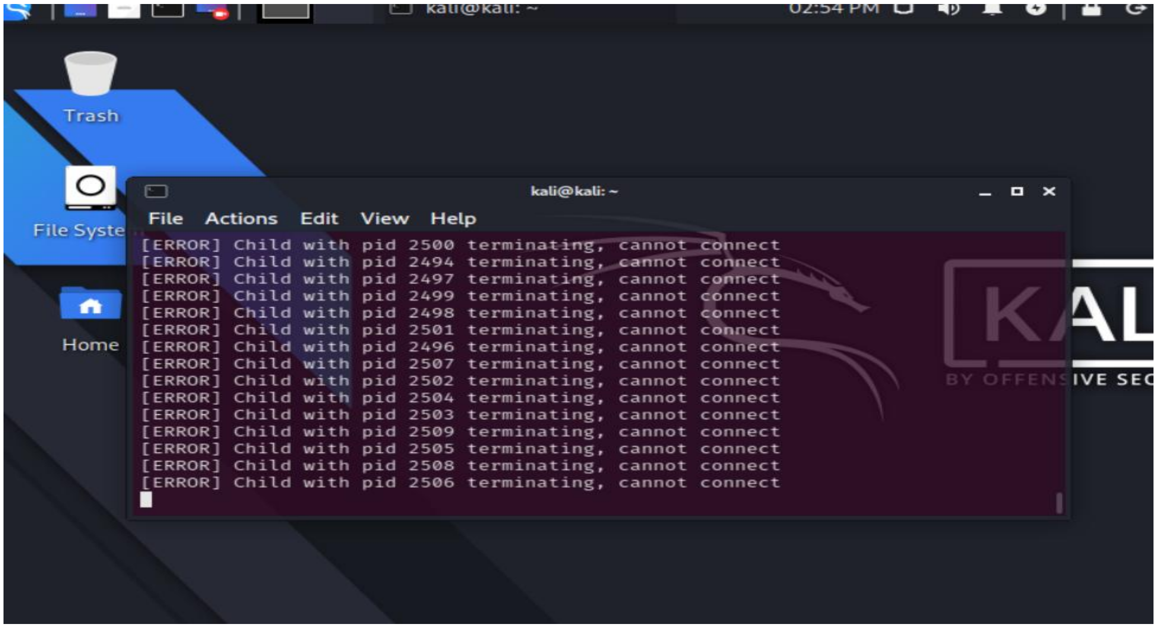
This device does not have a feature key so some features are disabled. Add a feature key now.

Traffic Monitor

```
2024-11-18 16:52:23 tunnel 0 0 unix_time="1731948743.57647"
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12699 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12700 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12701 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12702 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12703 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12704 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12705 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12706 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12707 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12708 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:37 Deny 192.168.0.110 192.168.0.105 http/tcp 12710 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:38 Deny 192.168.0.110 192.168.0.105 http/tcp 12711 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:38 Deny 192.168.0.110 192.168.0.105 http/tcp 12712 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:38 Deny 192.168.0.110 192.168.0.105 http/tcp 12713 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:38 Deny 192.168.0.110 192.168.0.105 http/tcp 12714 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:38 Deny 192.168.0.110 192.168.0.105 http/tcp 12715 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12730 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12731 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12732 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12733 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12734 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12735 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12736 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12737 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12738 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12739 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:58 Deny 192.168.0.110 192.168.0.105 http/tcp 12740 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:59 Deny 192.168.0.110 192.168.0.105 http/tcp 12741 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:59 Deny 192.168.0.110 192.168.0.105 http/tcp 12742 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:59 Deny 192.168.0.110 192.168.0.105 http/tcp 12743 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:59 Deny 192.168.0.110 192.168.0.105 http/tcp 12744 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
2024-11-18 16:52:59 Deny 192.168.0.110 192.168.0.105 http/tcp 12745 80 0-External Firebox Denied 52 128 (Unhandled External Packet-00) proc_id="firewall" rc="101" msg_id="3000-0148" tcp_info="offset 8
```

Fig 3.4

Firewallweb ui login bruteforce attack failed.



```
[ERROR] Child with pid 2500 terminating, cannot connect
[ERROR] Child with pid 2494 terminating, cannot connect
[ERROR] Child with pid 2497 terminating, cannot connect
[ERROR] Child with pid 2499 terminating, cannot connect
[ERROR] Child with pid 2498 terminating, cannot connect
[ERROR] Child with pid 2501 terminating, cannot connect
[ERROR] Child with pid 2496 terminating, cannot connect
[ERROR] Child with pid 2507 terminating, cannot connect
[ERROR] Child with pid 2502 terminating, cannot connect
[ERROR] Child with pid 2504 terminating, cannot connect
[ERROR] Child with pid 2503 terminating, cannot connect
[ERROR] Child with pid 2509 terminating, cannot connect
[ERROR] Child with pid 2505 terminating, cannot connect
[ERROR] Child with pid 2508 terminating, cannot connect
[ERROR] Child with pid 2506 terminating, cannot connect
```

Risk Assessment

The risks identified during the vulnerability assessment and exploitation in the network include expose of unsued ports like ssh.

Mitigation

Exposing only required/used ports and with different ports not well known ports