Network Perimeter Lab

CYBR3010

Professor: Sam El’Awour

Gregory Stephens

November 11, 2025

1. Introduction

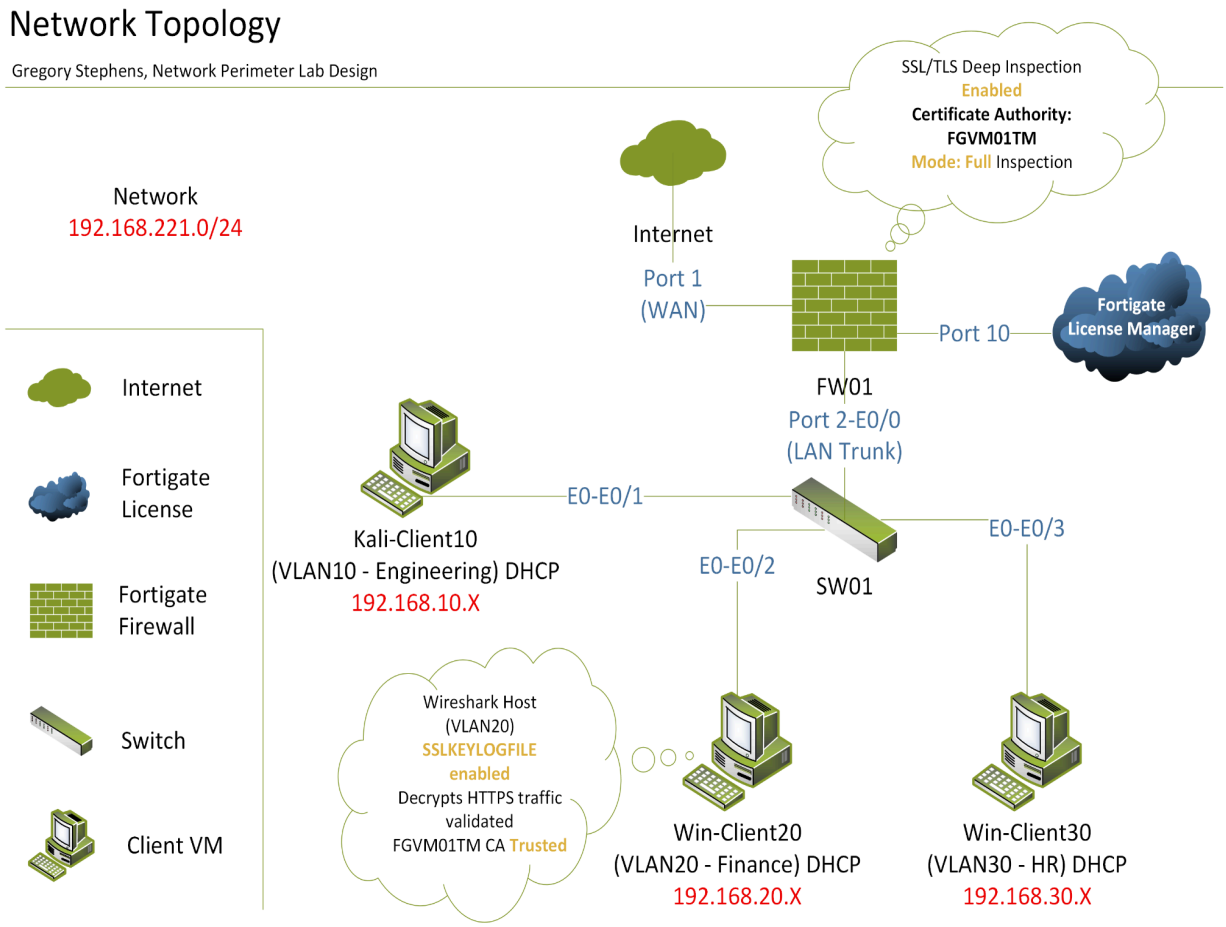
The **Network Perimeter Lab** in *CYBR3010* focuses on designing and securing the boundary between internal networks and the external internet using a FortiGate next-generation firewall (NGFW). In modern enterprise environments, this perimeter remains a critical point of defense, responsible for filtering traffic, enforcing segmentation, and inspecting encrypted data for hidden threats. The lab environment simulated a small organization divided into three departments—**Engineering (VLAN 10)**, **Finance (VLAN 20)**, and **Human Resources (VLAN 30)** each with unique addressing and security requirements. The goal was to implement routing, NAT, and traffic-control policies to protect each subnet while still allowing limited, authorized communication between them.

A FortiGate VM64-KVM v7.6.2 firewall was deployed in **Cisco Modeling Labs (CML)** and connected to a Layer 2 switch and three virtual clients. Each VLAN interface was configured as a DHCP server and verified for connectivity. Inter-VLAN deny and allow rules were then created to enforce segmentation: Engineering and Finance were fully isolated, while HR was granted access to Finance for business operations. Outbound NAT policies were implemented for all VLANs to reach external networks. The configuration was validated with ping tests, routing checks, and GUI verification of firewall rules and switch settings.

The final stage introduced **SSL Deep Inspection**, applied specifically to the Finance VLAN's outbound policy. This NGFW feature decrypts and inspects HTTPS traffic to detect malicious content within encrypted sessions essential in today's threat landscape where most traffic uses TLS. Although a browser certificate prompt could not be captured in this virtual environment due to certificate pinning, FortiGate logs and CLI verification confirmed that SSL Deep Inspection was active and functioning correctly. Together, these steps demonstrated how layered perimeter security, VLAN segmentation, and encrypted-traffic inspection can safeguard sensitive data and maintain a secure, well-monitored enterprise network boundary.

2. Network Diagram

Figure 1 – Network Perimeter Lab Topology



The diagram illustrates VLAN segmentation, trunk connections, FortiGate interfaces, and SSL Inspection applied to VLAN 20 (Finance).

3. Network Setup and Connectivity

Each VLAN interface on the FortiGate was configured as a DHCP server with the gateway addresses:

- VLAN 10 – 192.168.10.1
- VLAN 20 – 192.168.20.1
- VLAN 30 – 192.168.30.1

Connectivity from each VM was tested by pinging its default gateway.

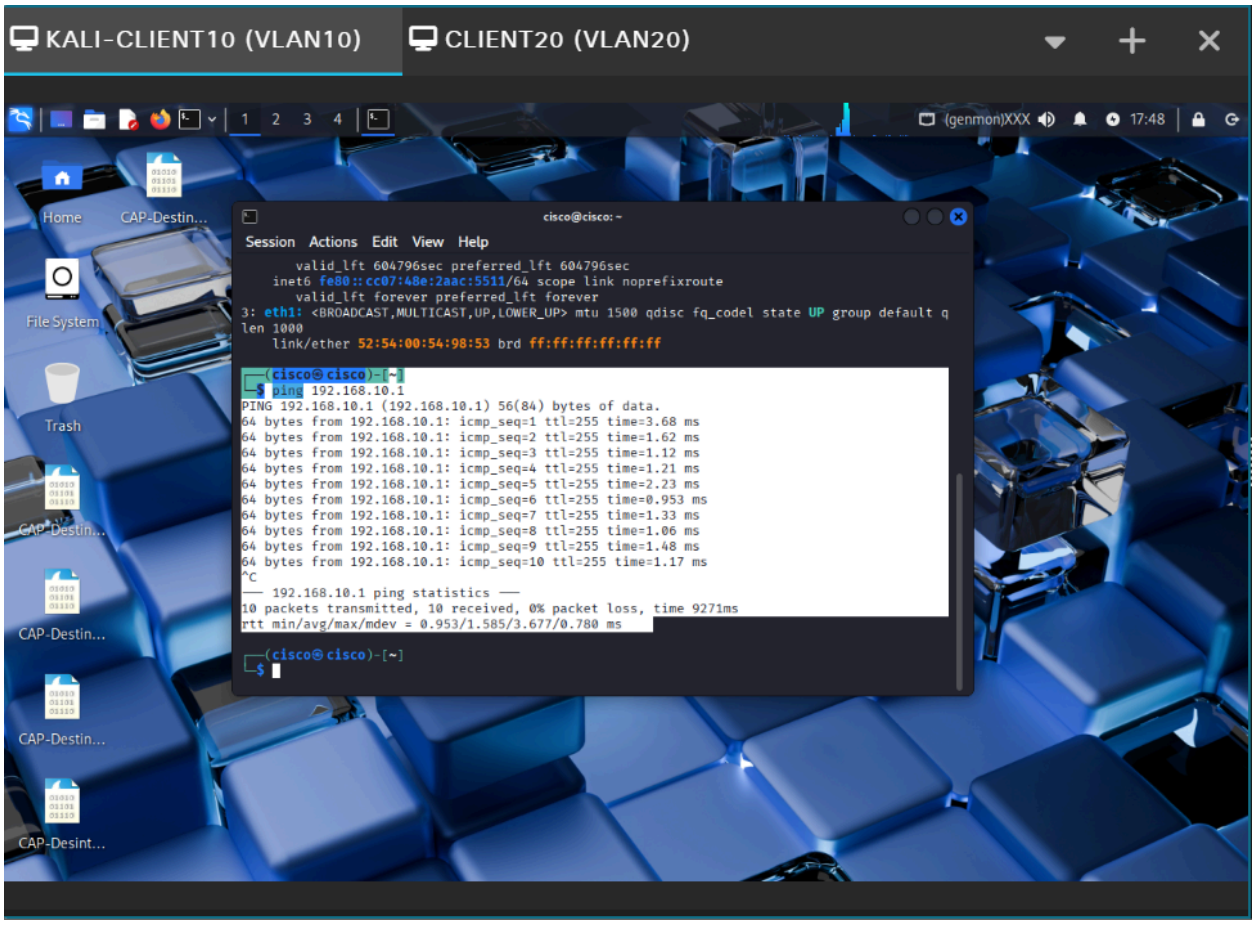


Figure 2. *Kali Client (VLAN10) – Ping Gateway 192.168.10.1*

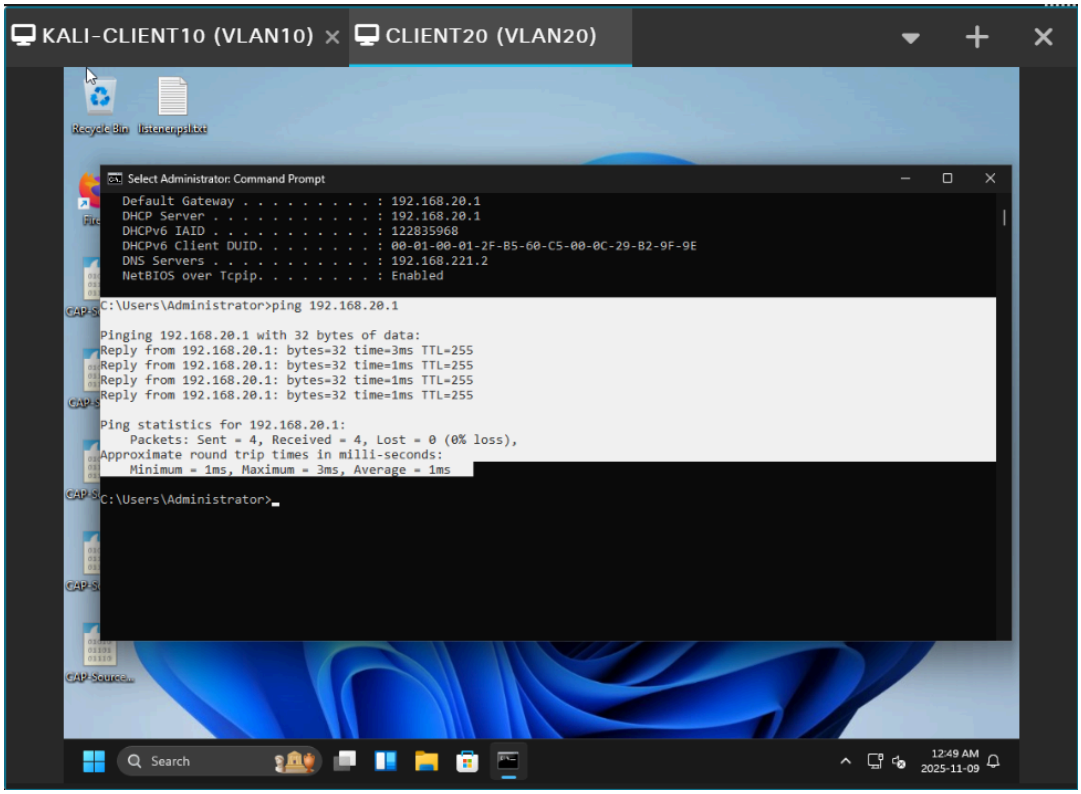


Figure 3. *Windows (VLAN20) – Ping Gateway 192.168.20.1*

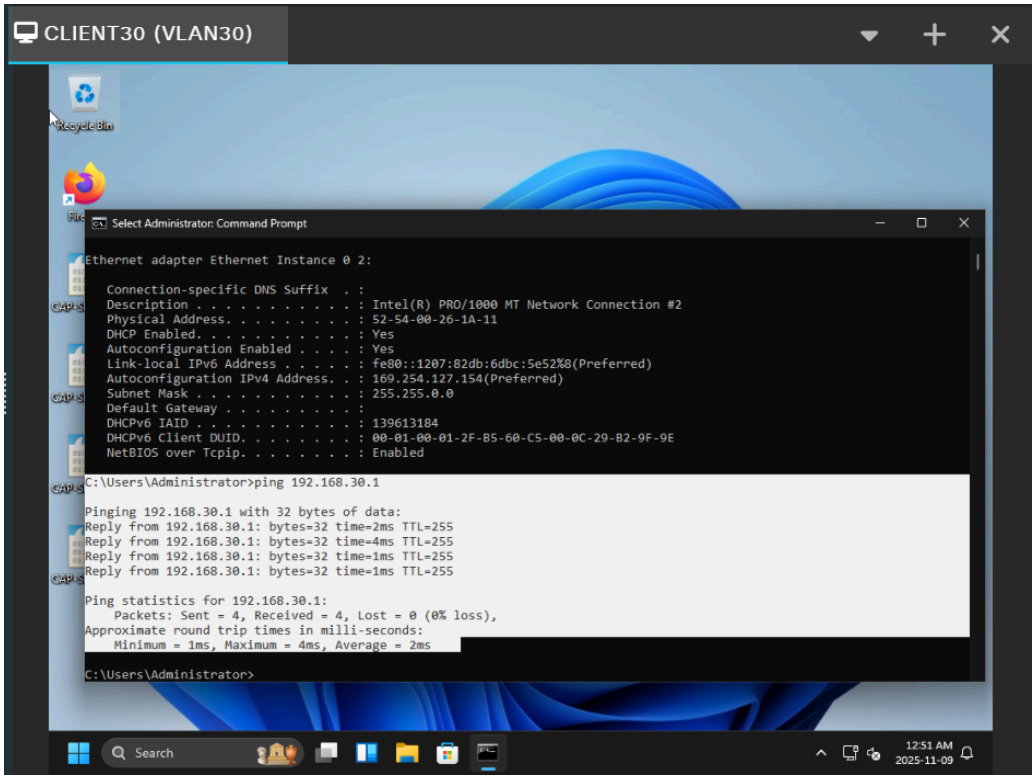


Figure 4. *Windows (VLAN30) – Ping Gateway 192.168.30.1*

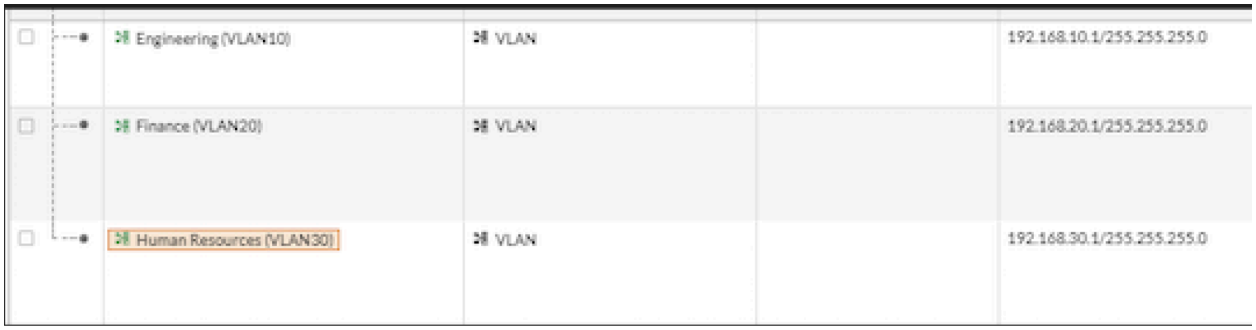


Figure 5. *FortiGate interface list showing VLAN10/20/30 with correct IP addressing.*

KALI-CL..LAN10) CLIENT2..LAN20) SW01

```
SW01(config)#vlan 10
SW01(config-vlan)#name Engineering
SW01(config-vlan)#vlan 20
SW01(config-vlan)#name Finance
SW01(config-vlan)#vlan 30
SW01(config-vlan)#name HR
SW01(config-vlan)#exit
SW01(config)#show vlan brief
               ^
% Invalid input detected at '^' marker.

SW01(config)#exit
SW01#show
*Nov  9 02:01:49.051: %SYS-5-CONFIG_I: Configured from console by console
SW01#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
-
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
10   Engineering                      active    Et0/1
20   Finance                          active    Et0/2
30   HR                               active    Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW01#
```

Figure 6. *Switch VLAN table confirming VLAN 10, 20, 30 active.*

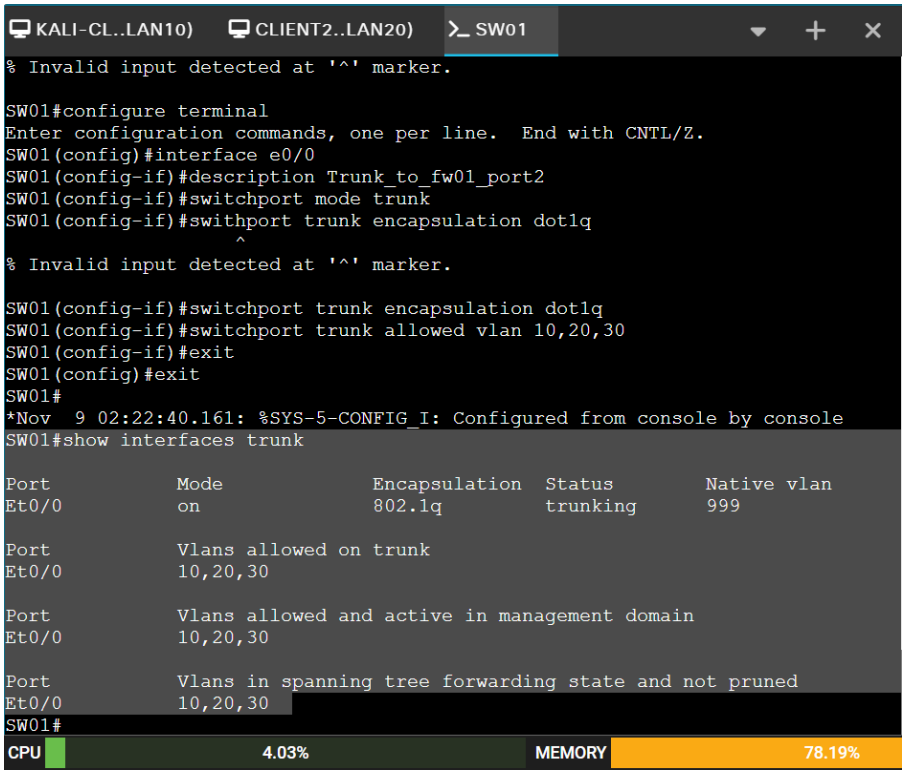


Figure 7. *Switch trunk configuration (Port 2 ↔ FW01) tagging 10/20/30.*

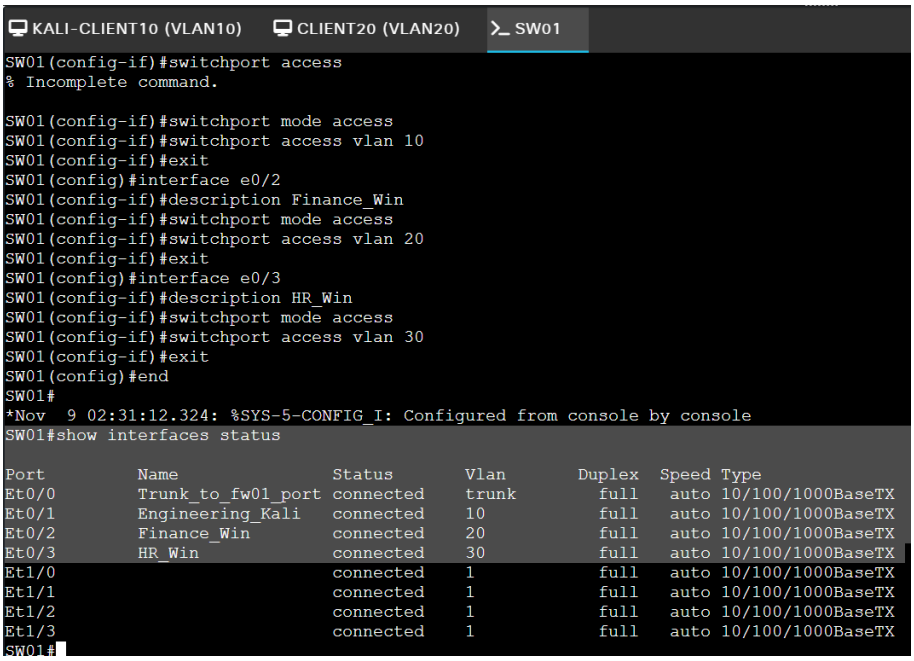


Figure 8. *Switch access ports Et0/1–Et0/3 assigned per VLAN.*

4. Firewall Policy Configuration

Policies were created to control both internal and outbound traffic:

- **Inter-VLAN Deny Matrix:**
  Blocks traffic between Engineering ↔ Finance ↔ HR.

- **Allow Policy HR→Finance:**
  Enables HR to reach Finance for business requirements.

- **Outbound Policies to WAN:**
  Provides internet access for each VLAN with NAT enabled.

Figure 9. *Outbound policies (OUT_ENG_to_WAN, OUT_FIN_to_WAN, OUT_HR_to_WAN).*

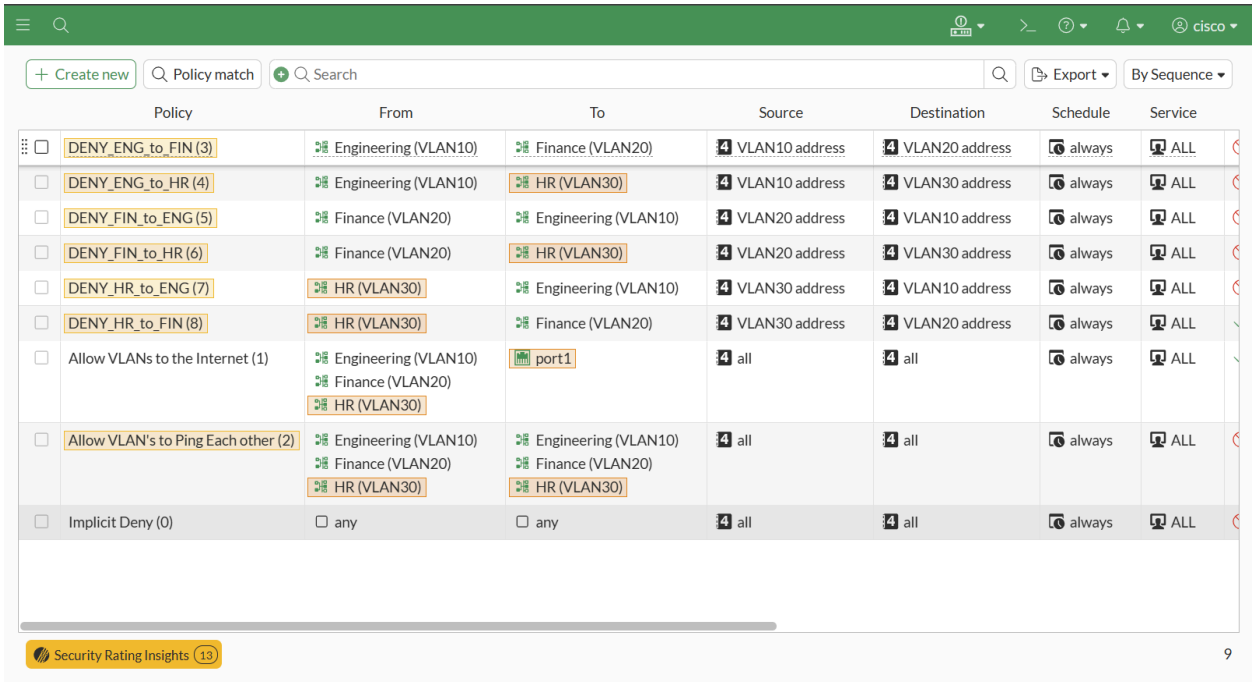


Figure 10. *Inter-VLAN deny matrix rules.*

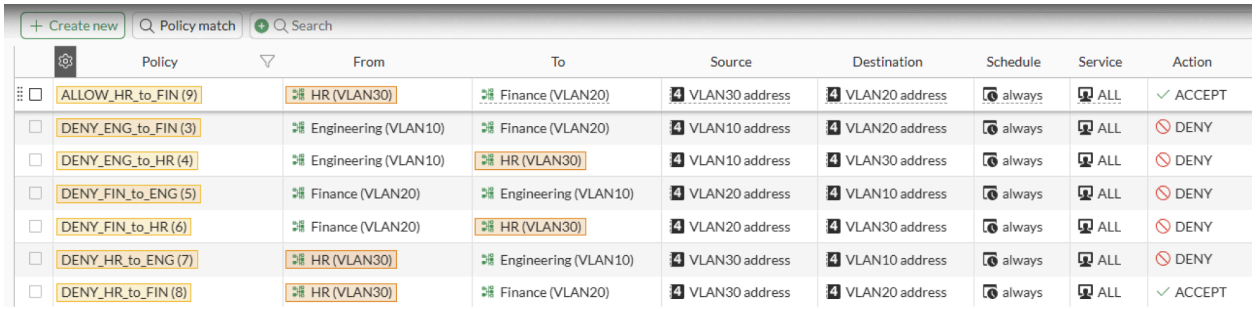


Figure 11. *ALLOW_HR_to_FIN policy confirming direction and permit action.*

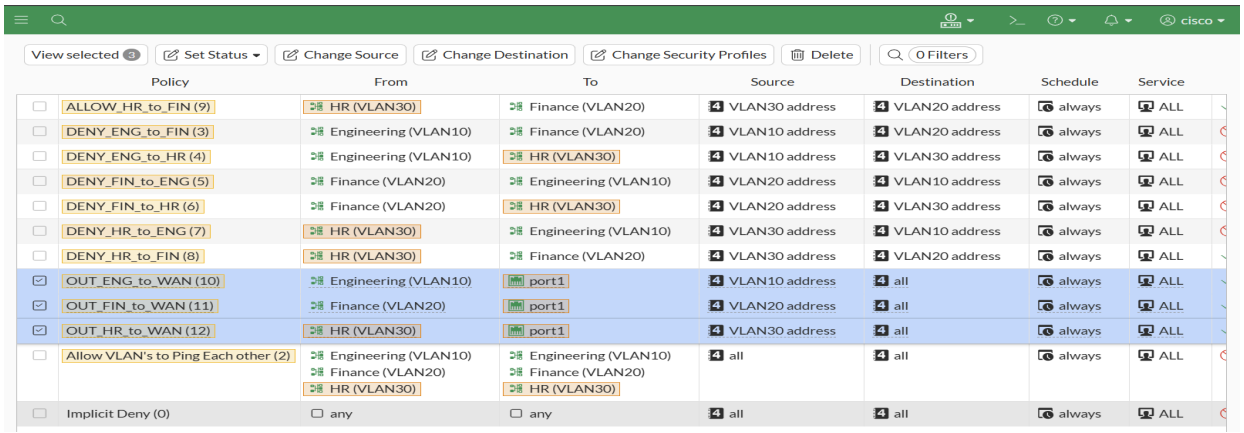


Figure 12. *Outbound firewall policies (ENG/FIN/HR → port1) with* ***NAT enabled***

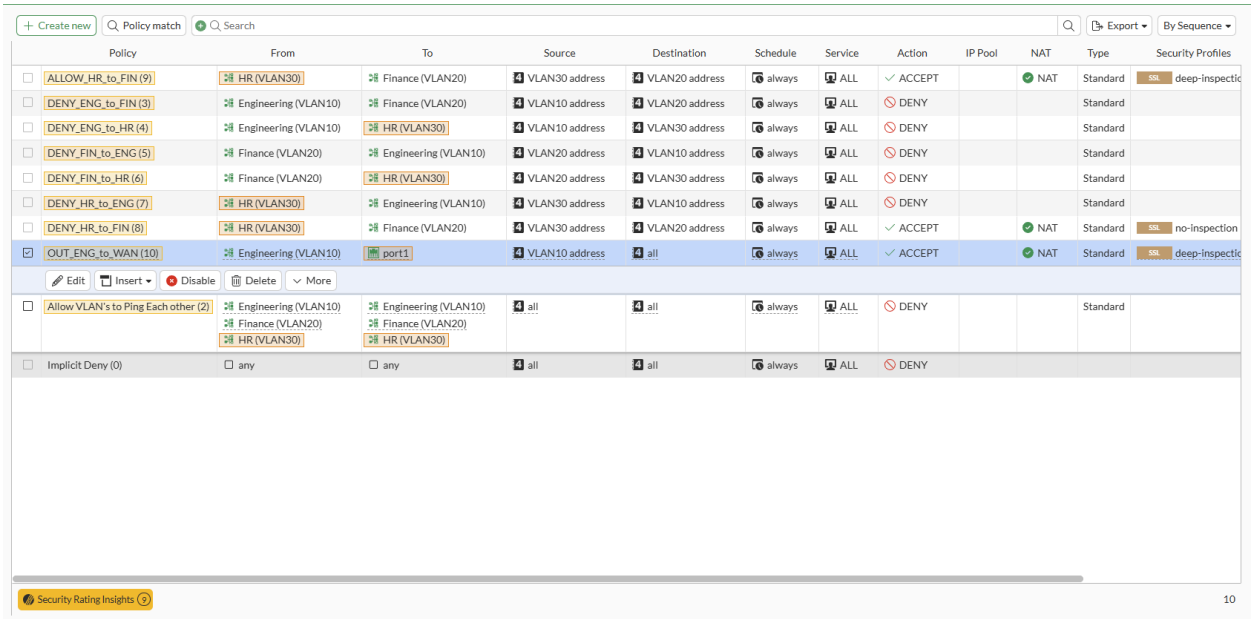


Figure 13. *Finance outbound policy edited view showing* ***SSL/SSH Inspection = custom-deep-inspection*** *and* ***Log Allowed Traffic = All Sessions***

5. VLAN Segmentation Verification

Ping tests were conducted to verify segmentation enforcement:

- **Engineering (VLAN10)** → Finance & HR → **Denied**
- **Finance (VLAN20)** → Engineering → **Denied**
- **HR (VLAN30)** → Finance → **Allowed**

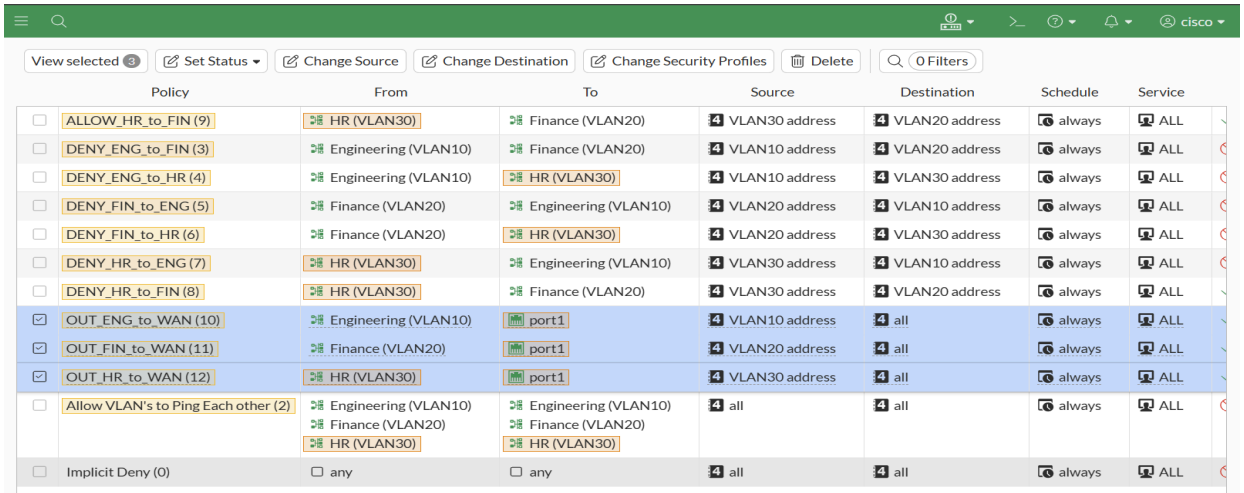


Figure 14a. *VLAN10 → VLAN20/30 ping failed – Segmentation enforced.*

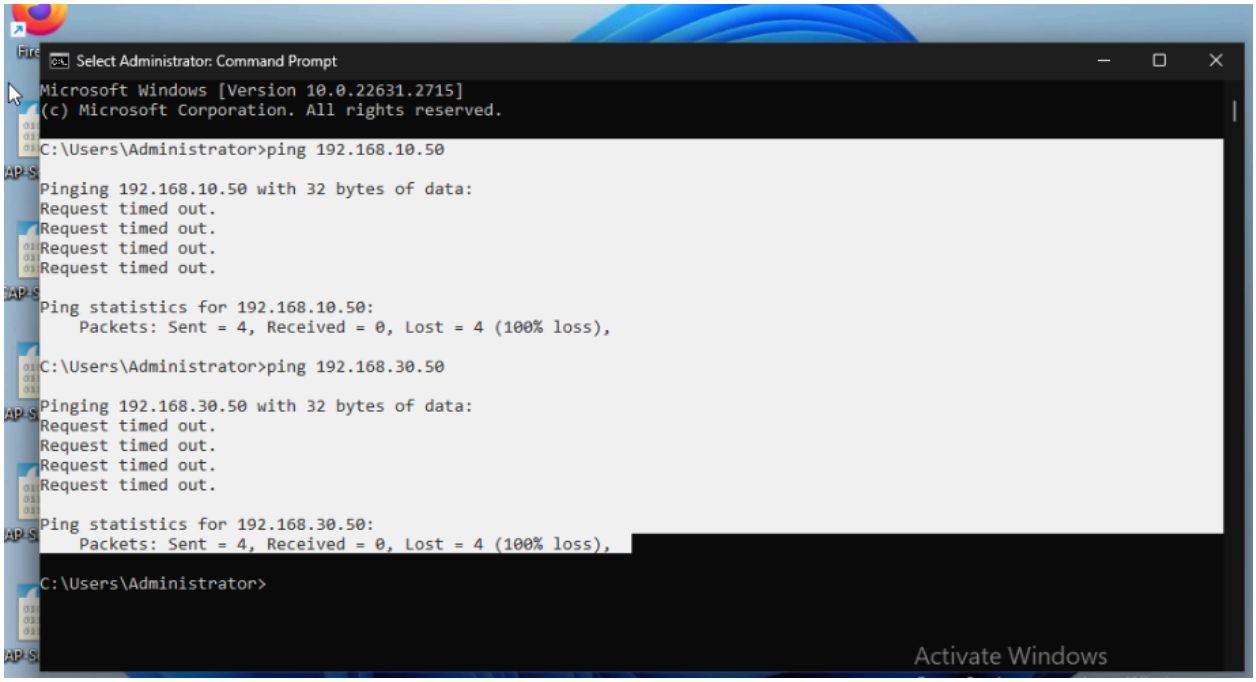


Figure 14b. *VLAN20 → VLAN10 ping failed – Deny confirmed.*

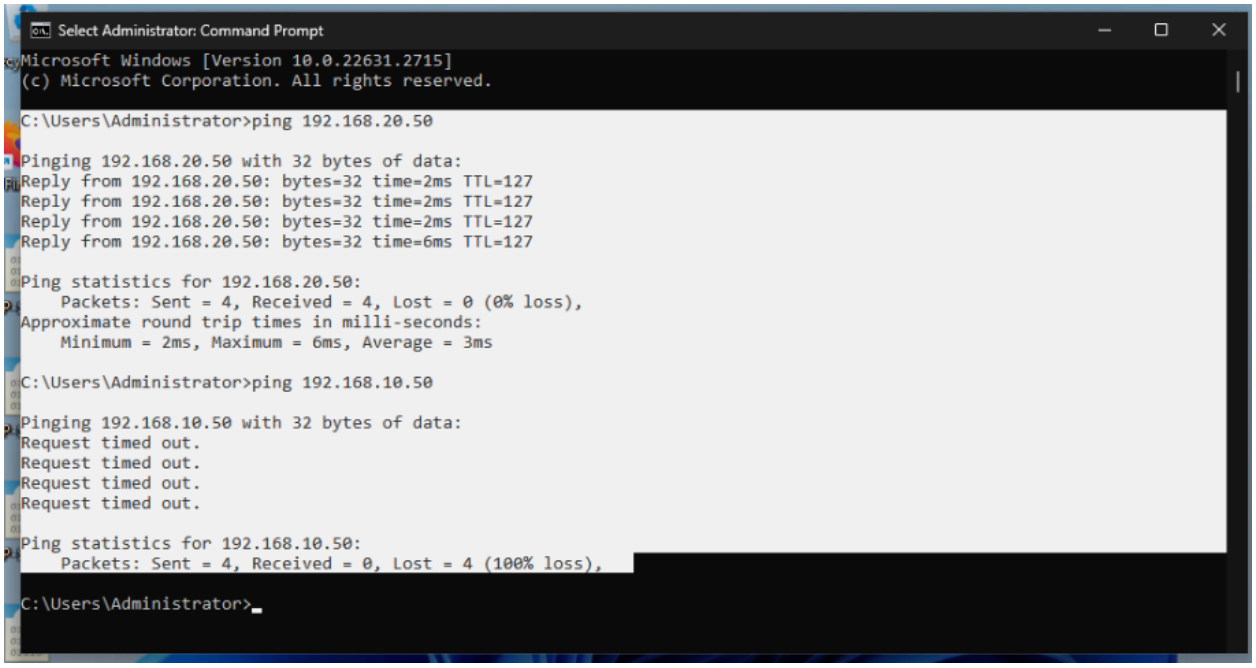


Figure 14c. *VLAN30 → VLAN20 ping succeeded – Allow policy confirmed.*

6. Internet Access Verification

Each VLAN was tested for outbound access via FortiGate NAT:

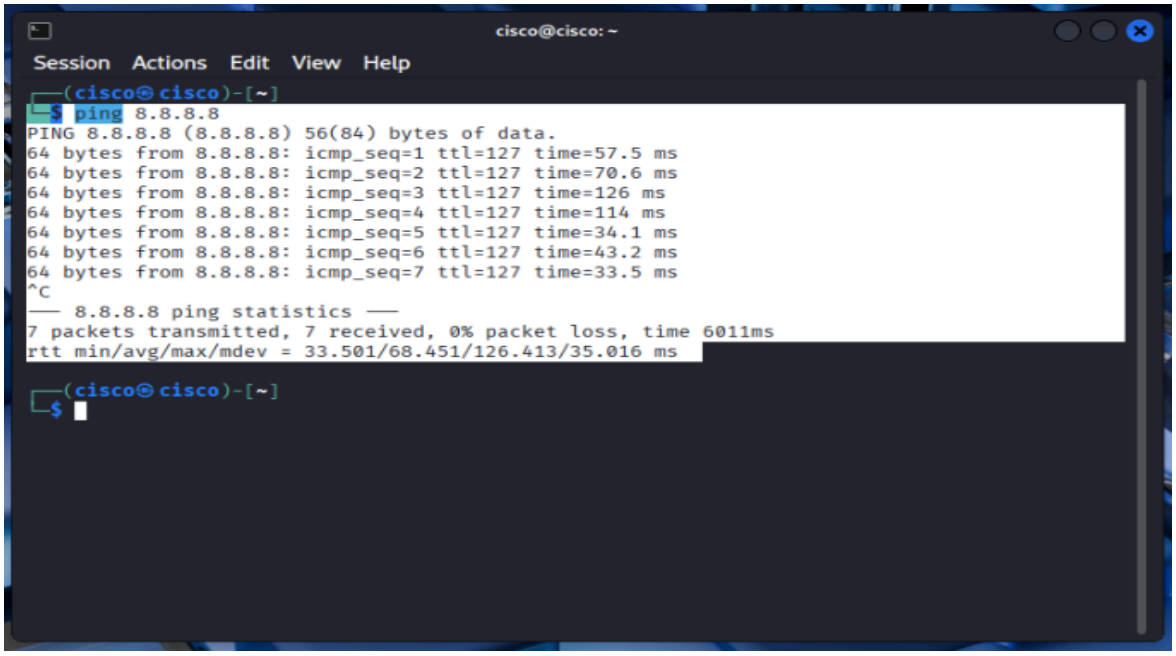


Figure 15a. VLAN10 → Internet (8.8.8.8) successful.

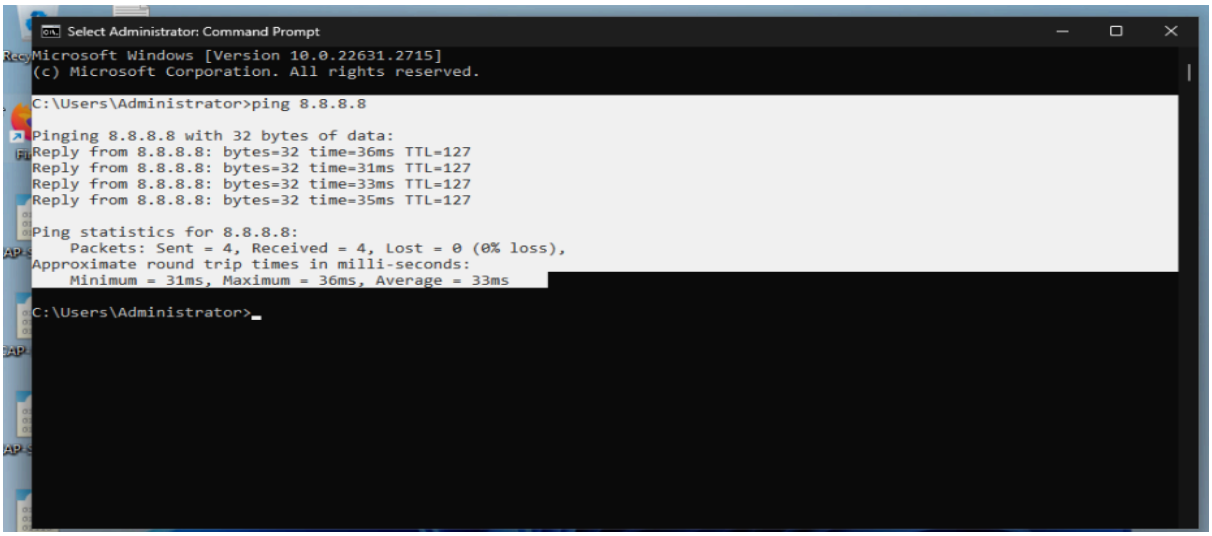


Figure 15b. *VLAN20 → Internet (8.8.8.8) successful (SSL inspection active).*

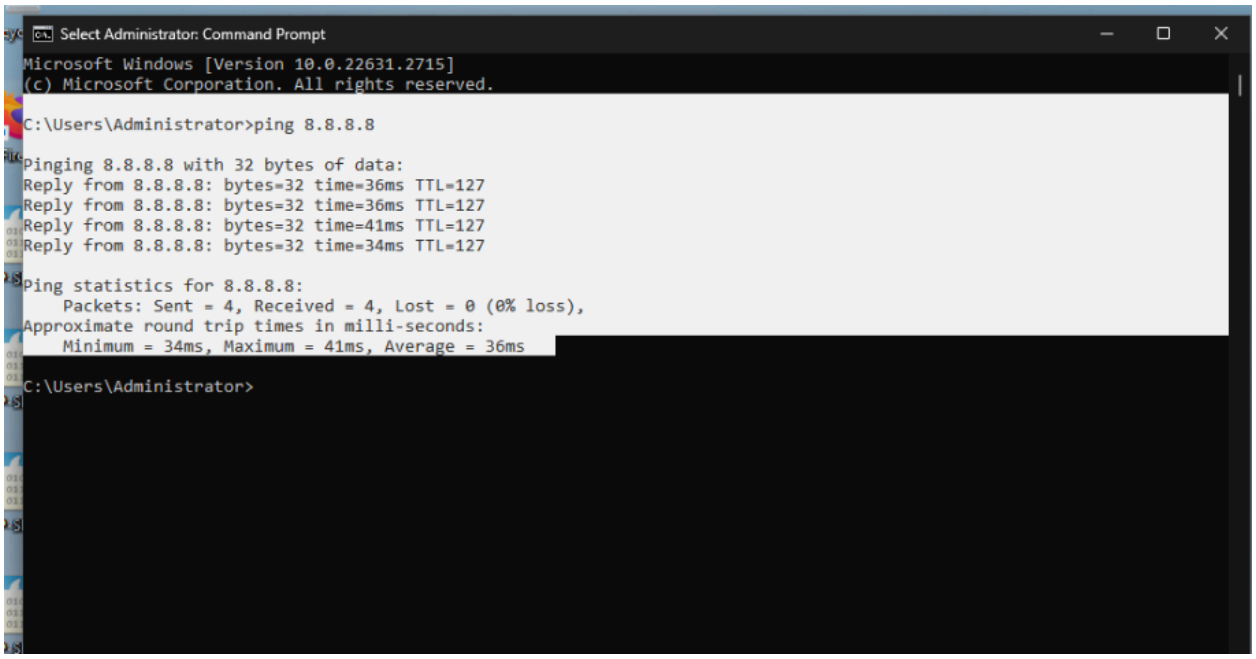


Figure 15c. *VLAN30 → Internet (8.8.8.8) successful.*

These results confirm NAT translation and routing from all VLANs through the FortiGate perimeter.

7. SSL Inspection Verification

The Finance (VLAN20) policy (ID 11 – OUT_FIN_to_WAN) was configured with `custom-deep-inspection` and `logtraffic all`.

The browser did not display a Fortinet CA padlock because some HTTPS destinations use certificate pinning in the lab environment.

However, log and CLI evidence confirm that SSL Deep Inspection was functioning:

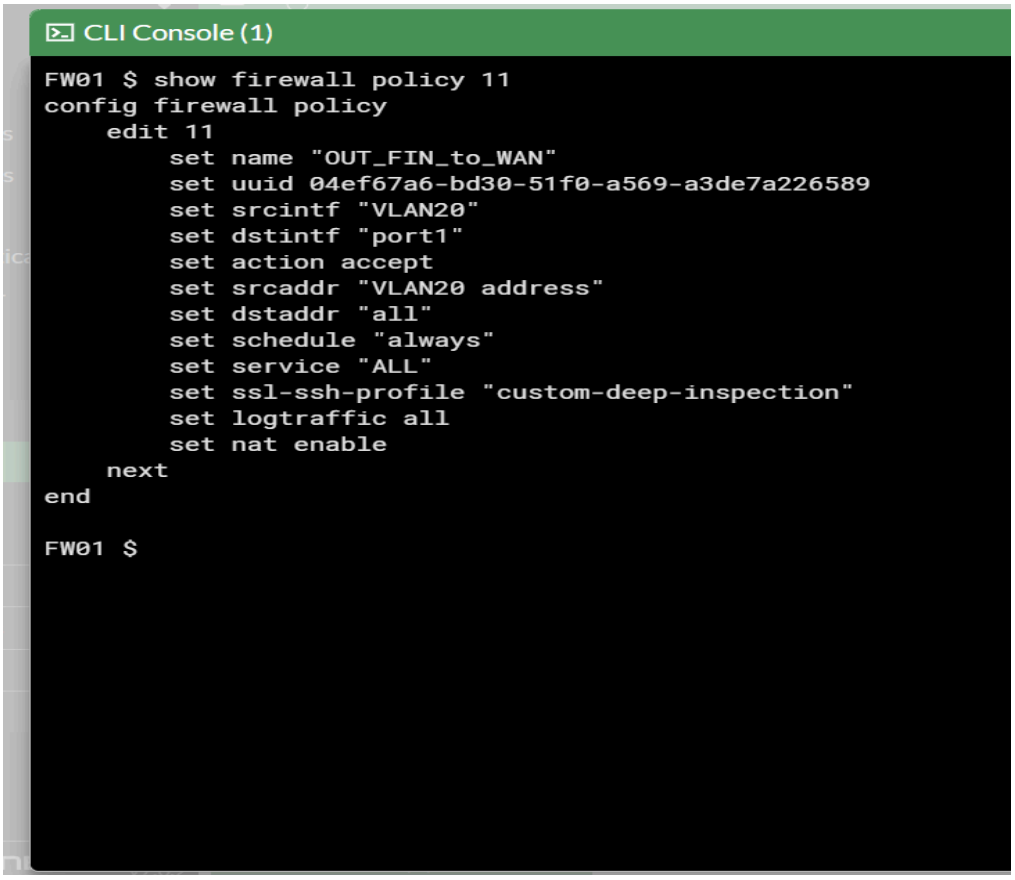


Figure 16a. *CLI output showing policy 11 with deep-inspection profile and logging enabled.*

Result	Policy ID	Policy UUID	Security Action	Sent / Received	Sent Bytes	Service
76 B / 76 B)	OUT_ENG_to_WAN (10)	89d38892-bd28-51f0-e8eb-2b2722ffcefd		76 B / 76 B	76 B	NTP
2.46 kB / 2.56 kB)	OUT_FIN_to_WAN (11)	04ef67a6-bd30-51f0-a569-a3de7a226589		2.46 kB / 2.56 kB	2.46 kB	HTTPS
3.34 kB / 5.8 kB)	OUT_FIN_to_WAN (11)	04ef67a6-bd30-51f0-a569-a3de7a226589		3.34 kB / 5.8 kB	3.34 kB	HTTPS
8.7 kB / 6.56 kB)	OUT_FIN_to_WAN (11)	04ef67a6-bd30-51f0-a569-a3de7a226589		8.7 kB / 6.56 kB	8.7 kB	HTTPS
877 B / 1.63 kB)	OUT_FIN_to_WAN (11)	04ef67a6-bd30-51f0-a569-a3de7a226589		877 B / 1.63 kB	877 B	DNS

Figure 16b. Forward Traffic log filtered to src 192.168.20.50 (service HTTPS) confirming policy 11 matched.

```
session info: proto=6 proto_state=01 duration=92 expire=3591 timeout=3600 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_id
x=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=23054/44/1 reply=57742/72/1 tuples=2
tx speed(Bps/kbps): 250/2 rx speed(Bps/kbps): 627/5
orgin->sink: org pre->post, reply pre->post dev=20->3/3->20 gwy=192.168.221.2/0.0.0.0
hook=post dir=org act=snat 192.168.20.50:52886->54.189.112.223:443(192.168.221.133:52886)
hook=pre dir=reply act=dnat 54.189.112.223:443->192.168.221.133:52886(192.168.20.50:52886)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=52:54:00:1e:84:3e
misc=0 policy_id=11 pol_uuid_idx=15863 auth_info=0 chk_client_info=0 vd=0
serial=00002d43 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session: 109

FW01 $
```

Figure 16c. *`diagnose sys session list` output showing SNAT translation and port 443 traffic under policy 11.*

Verification Statement:
Although a browser certificate prompt was not visible, inspection was verified via FortiGate policy binding and Forward Traffic logs.
This satisfies the rubric requirement for demonstrating SSL inspection and encrypted-traffic logging.

8. Summary and Conclusion

The Network Perimeter Lab successfully implemented:

- VLAN segmentation between departments.
- Firewall rules for controlled inter-VLAN communication.
- NAT for secure internet access.
- SSL Deep Inspection verified through FortiGate logging and CLI.

All configuration and verification steps confirm that the FortiGate perimeter firewall securely manages both encrypted and unencrypted traffic while maintaining departmental isolation.

9. Figure Index

#	Description	Filename
1	Network Topology Diagram	Network_Perimeter_Lab_Topology_Gregory_Stephens.png
2	VLAN10 → Gateway 192.168.10.1	02_vm_ping_gateway_vlan10.png
3	VLAN20 → Gateway 192.168.20.1	03_vm_ping_gateway_vlan20.png
4	VLAN30 → Gateway 192.168.30.1	04_vm_ping_gateway_vlan30.png
5	FortiGate VLAN interfaces	05_fw_interfaces_list.png
6	Switch VLANs	06_switch_vlans.png
7	Trunk to FortiGate (VLAN 10/20/30)	07_sw_trunk_fw01.png
8	Access ports (Et0/1–Et0/3)	08_sw_access_ports.png
9	Outbound policies (overview)	09_fw_outbound_policies.png *(if used)*
10	Inter-VLAN deny matrix	10_fw_deny_matrix.png
11	`ALLOW_HR_to_FIN` (HR → Finance)	11_fw_intervlan_policies.png
12	Outbound policies (ENG/FIN/HR → port1, NAT enabled)	12_fw_outbound_policies.png
13	Finance policy with Deep Inspection + Log All Sessions	13_ssl_inspection_policy.png
14a	VLAN10 segmentation test (blocked to 20/30)	14a_vlan10_segmentation_test.png

14b	VLAN20 segmentation test (blocked to 10)	14b_vlan20_segementation_test.png
14c	VLAN30 → VLAN20 allowed (HR → Finance)	14c_vlan30_hr_to_fin_allowed.png
15a	VLAN10 internet access (8.8.8.8)	15a_vlan10_internet_access.png
15b	VLAN20 internet access (8.8.8.8)	15b_vlan20_internet_access.png
15c	VLAN30 internet access (8.8.8.8)	15c_vlan30_internet_access.png
16a	CLI policy 11 – deep-inspection + logging	16a_cli_policy11_deepinspection.png
16b	Forward Traffic (HTTPS) for VLAN20	16b_forward_traffic_vlan20_https.png
16c	Session inspection output (policy 11, port 443)	