Securing Networks: A Practical Approach

By Abdelrhman Sobhy Hanafy abdelhamid

ABSTRACT

This report explores key concepts and skills gained from cybersecurity certifications such as CCNA and NSE4, along with an introduction to ethical hacking. It covers essential networking topics like routing, switching, NAT, VLANs, and security protocols, while also discussing the role of ethical hackers in identifying and mitigating vulnerabilities. Additionally, it examines the practical application of these concepts through real-world network configurations and security measures. The report highlights how these certifications and ethical hacking practices contribute to building robust network security frameworks.

Securing Networks: A Practical Approach

CCNA Routing and Switching

CCNA (Cisco Certified Network Associate) Routing and Switching certification validates your skills in networking fundamentals, routing and switching technologies, and security. Below are key concepts in CCNA:

Some Concepts which I gained from this certificate

Network Fundamentals: Understanding IP addressing, subnetting, and the OSI model.

Routing: Configuring routing protocols like OSPF, RIP, static routes.

Switching; VLANs, and Inter-VLAN routing.

Network Security: Basic security concepts such as configuring ACLs, NAT/PAT, and hardening network devices.

WAN Technologies: Understanding and configuring WAN protocols like PPP and HDLC.

IP Services: Configuring DHCP, DNS, and NTP for network services.

Troubleshooting: Using diagnostic tools to resolve network issues across layers.

Hands-on Experience: Practical skills gained through simulators like Cisco Packet Tracer and EVE-EN.

Network Management: You learn to configure and manage network devices, ensuring optimal performance and availability. This includes configuring network devices for monitoring, applying QoS (Quality of Service), and implementing SNMP (Simple Network Management Protocol) for tracking device health and performance.

Concept's Implementation

Used Topology:

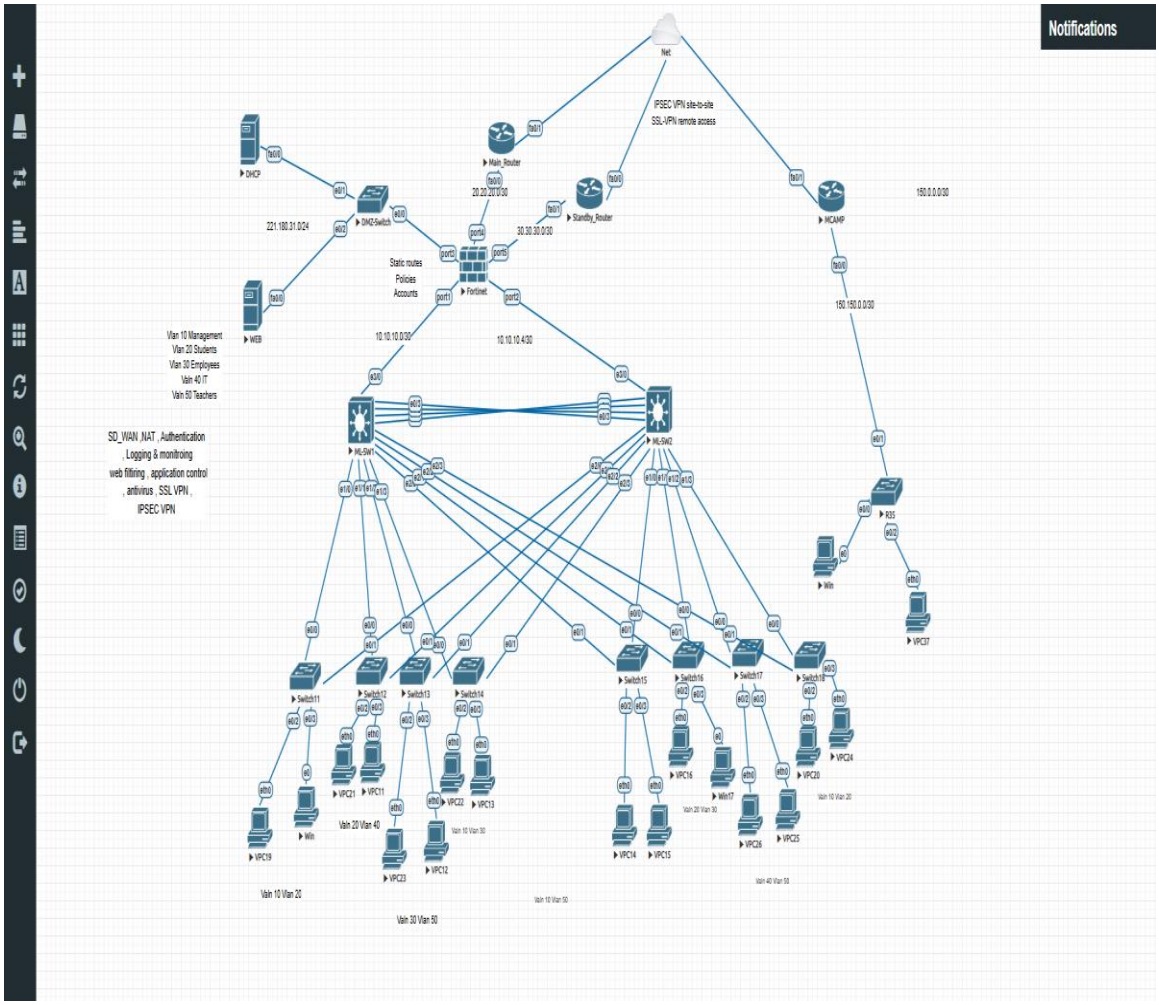
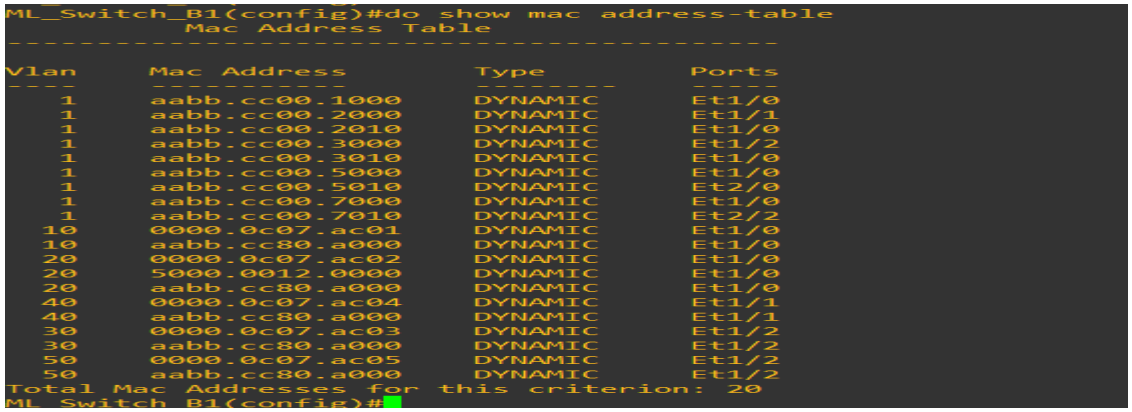


Figure1.1

Switching and Connectivity:

Switching: A Layer 2 device that forwards Ethernet frames based on MAC addresses. It is responsible for creating and maintaining a MAC address table to determine the destination of each frame. The primary purpose is to reduce network traffic and increase performance.

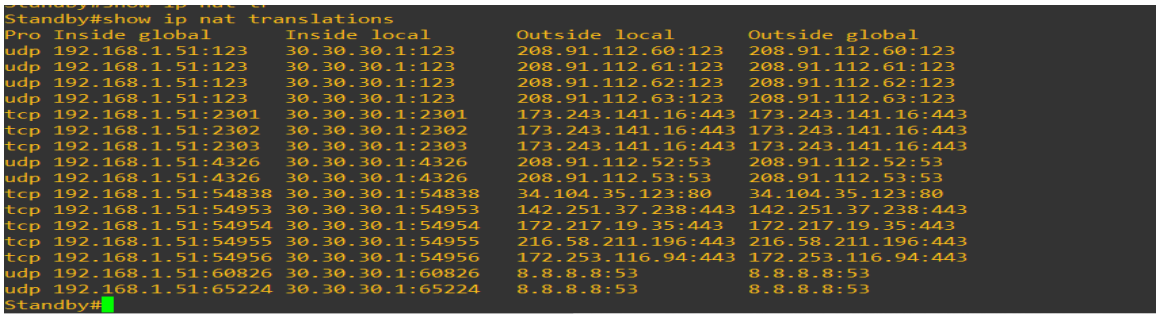


```
ML_Switch_B1(config)#do show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address          Type          Ports
----    -----------          --------      -----
   1    aabb.cc00.1000       DYNAMIC       Et1/0
   1    aabb.cc00.2000       DYNAMIC       Et1/1
   1    aabb.cc00.2010       DYNAMIC       Et1/0
   1    aabb.cc00.3000       DYNAMIC       Et1/2
   1    aabb.cc00.3010       DYNAMIC       Et1/0
   1    aabb.cc00.5000       DYNAMIC       Et1/0
   1    aabb.cc00.5010       DYNAMIC       Et2/0
   1    aabb.cc00.7000       DYNAMIC       Et1/0
   1    aabb.cc00.7010       DYNAMIC       Et2/2
  10    0000.0c07.ac01       DYNAMIC       Et1/0
  10    aabb.cc80.a000       DYNAMIC       Et1/0
  20    0000.0c07.ac02       DYNAMIC       Et1/0
  20    5000.0012.0000       DYNAMIC       Et1/0
  20    aabb.cc80.a000       DYNAMIC       Et1/0
  40    0000.0c07.ac04       DYNAMIC       Et1/1
  40    aabb.cc80.a000       DYNAMIC       Et1/1
  30    0000.0c07.ac03       DYNAMIC       Et1/2
  30    aabb.cc80.a000       DYNAMIC       Et1/2
  50    0000.0c07.ac05       DYNAMIC       Et1/2
  50    aabb.cc80.a000       DYNAMIC       Et1/2
Total Mac Addresses for this criterion: 20
ML_Switch_B1(config)#
```

Figure1.2

NAT (Network Address Translation): This technique modifies the source or destination IP address in the packet header as it passes through a router or firewall. This is essential for allowing devices on a private network to communicate with devices on the public internet using a shared public IP.



```
Standby#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 192.168.1.51:123   30.30.30.1:123     208.91.112.60:123  208.91.112.60:123
udp 192.168.1.51:123   30.30.30.1:123     208.91.112.61:123  208.91.112.61:123
udp 192.168.1.51:123   30.30.30.1:123     208.91.112.62:123  208.91.112.62:123
udp 192.168.1.51:123   30.30.30.1:123     208.91.112.63:123  208.91.112.63:123
tcp 192.168.1.51:2301  30.30.30.1:2301    173.243.141.16:443 173.243.141.16:443
tcp 192.168.1.51:2302  30.30.30.1:2302    173.243.141.16:443 173.243.141.16:443
tcp 192.168.1.51:2303  30.30.30.1:2303    173.243.141.16:443 173.243.141.16:443
udp 192.168.1.51:4326  30.30.30.1:4326    208.91.112.52:53   208.91.112.52:53
udp 192.168.1.51:4326  30.30.30.1:4326    208.91.112.53:53   208.91.112.53:53
tcp 192.168.1.51:54838 30.30.30.1:54838   34.104.35.123:80   34.104.35.123:80
tcp 192.168.1.51:54953 30.30.30.1:54953   142.251.37.238:443 142.251.37.238:443
tcp 192.168.1.51:54954 30.30.30.1:54954   172.217.19.35:443  172.217.19.35:443
tcp 192.168.1.51:54955 30.30.30.1:54955   216.58.211.196:443 216.58.211.196:443
tcp 192.168.1.51:54956 30.30.30.1:54956   172.253.116.94:443 172.253.116.94:443
udp 192.168.1.51:60826 30.30.30.1:60826   8.8.8.8:53         8.8.8.8:53
udp 192.168.1.51:65224 30.30.30.1:65224   8.8.8.8:53         8.8.8.8:53
Standby#
```

Figure 1.3

HSRP (Hot Standby Router Protocol): A redundancy protocol that provides failover between two or more routers, ensuring the availability of a default gateway even if one router fails.

```
ML_Switch_B1(config)#do show stan
ML_Switch_B1(config)#do show standby
Vlan10 - Group 1
  State is Standby
    1 state change, last state change 04:18:04
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.376 secs
  Preemption enabled
  Active router is 192.168.10.2, priority 110 (expires in 9.248 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-1" (default)
Vlan20 - Group 2
  State is Standby
    1 state change, last state change 04:18:04
  Virtual IP address is 192.168.20.254
  Active virtual MAC address is 0000.0c07.ac02 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.304 secs
  Preemption enabled
  Active router is 192.168.20.2, priority 110 (expires in 8.528 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl20-2" (default)
Vlan30 - Group 3
  State is Standby
    1 state change, last state change 04:18:05
  Virtual IP address is 192.168.30.254
  Active virtual MAC address is 0000.0c07.ac03 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.480 secs
  Preemption enabled
  Active router is 192.168.30.2, priority 110 (expires in 9.776 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl30-3" (default)
Vlan40 - Group 4
  State is Standby
    1 state change, last state change 04:18:03
  Virtual IP address is 192.168.40.254
  Active virtual MAC address is 0000.0c07.ac04 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac04 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.144 secs
  Preemption enabled
```

Figure1.4

VLANs (Virtual Local Area Networks): A VLAN is a logical grouping of network devices that can communicate as if they are on the same physical LAN, even if they are not. VLANs reduce broadcast domains and improve network performance.

```
ML_Switch_B1(config)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et3/1, Et3/2, Et3/3, Po1
10   Management                       active
20   Students                         active
30   Employees                        active
40   IT                               active
50   Teachers                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure1.5

Routing between VLANs (Inter-VLAN Routing): This process allows communication between devices in different VLANs, typically done using a Layer 3 device like a router or a multilayer switch.

```
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.10.10.1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.10.10.0/30 is directly connected, Ethernet3/0
L        10.10.10.2/32 is directly connected, Ethernet3/0
O        10.10.10.4/30 [110/11] via 192.168.50.2, 04:20:54, Vlan50
                       [110/11] via 192.168.30.2, 04:20:44, Vlan30
                       [110/11] via 192.168.20.2, 04:20:44, Vlan20
                       [110/11] via 192.168.10.2, 04:20:44, Vlan10
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.1/32 is directly connected, Vlan30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, Vlan40
L        192.168.40.1/32 is directly connected, Vlan40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, Vlan50
L        192.168.50.1/32 is directly connected, Vlan50
```

Figure1.6

EtherChannel: A method of combining multiple physical Ethernet links into a single logical link, enhancing bandwidth and providing redundancy. It is particularly useful in high-traffic environments.

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)    Et0/2(P)
                                 Et0/3(P)
```

Figure1.7

SSH (Secure Shell):

A protocol used for securely accessing remote devices over the network. It ensures encrypted communication between the client and the server

Routing

Dynamic → OSPF (Open Shortest Path First):

OSPF is a dynamic routing protocol used to share routing information in large networks. OSPF is more efficient than other protocols like RIP, as it calculates the shortest path using Dijkstra's algorithm. It supports hierarchical networks with areas to reduce overhead.

Static Routing:

This involves manually configuring the route information in the router's routing table. It is ideal for small networks or when a network administrator wants full control over routing decisions.

```
ML_Switch_B1(config)#do show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.10.10.1
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.10.10.0/30 is directly connected, Ethernet3/0
L        10.10.10.2/32 is directly connected, Ethernet3/0
O        10.10.10.4/30 [110/11] via 192.168.50.2, 03:53:06, Vlan50
                       [110/11] via 192.168.30.2, 03:52:56, Vlan30
                       [110/11] via 192.168.20.2, 03:52:56, Vlan20
                       [110/11] via 192.168.10.2, 03:52:56, Vlan10
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.1/32 is directly connected, Vlan30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, Vlan40
L        192.168.40.1/32 is directly connected, Vlan40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, Vlan50
L        192.168.50.1/32 is directly connected, Vlan50
ML_Switch_B1(config)#
```

Figure1.8

NSE4 (FortiGate Security)

NSE4 focuses on securing and configuring FortiGate devices, covering both foundational security concepts and advanced features. Here are key topics:

1.Policies: Policies define the security rules for traffic flow between interfaces. A policy specifies which traffic is allowed or blocked based on factors like source, destination, application, and user identity. Policies can also be used to enforce security measures like deep packet inspection and SSL inspection.

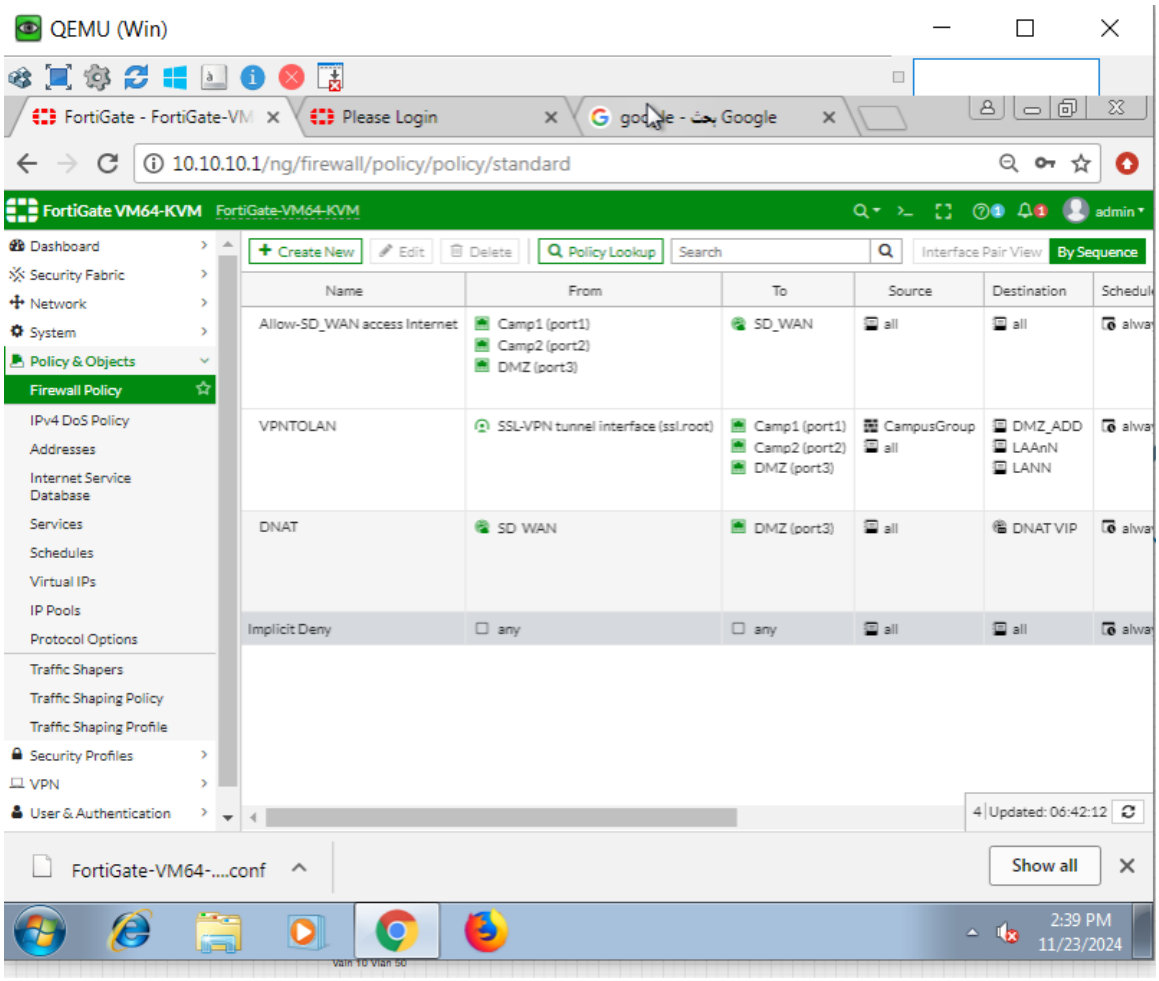


Figure2.1

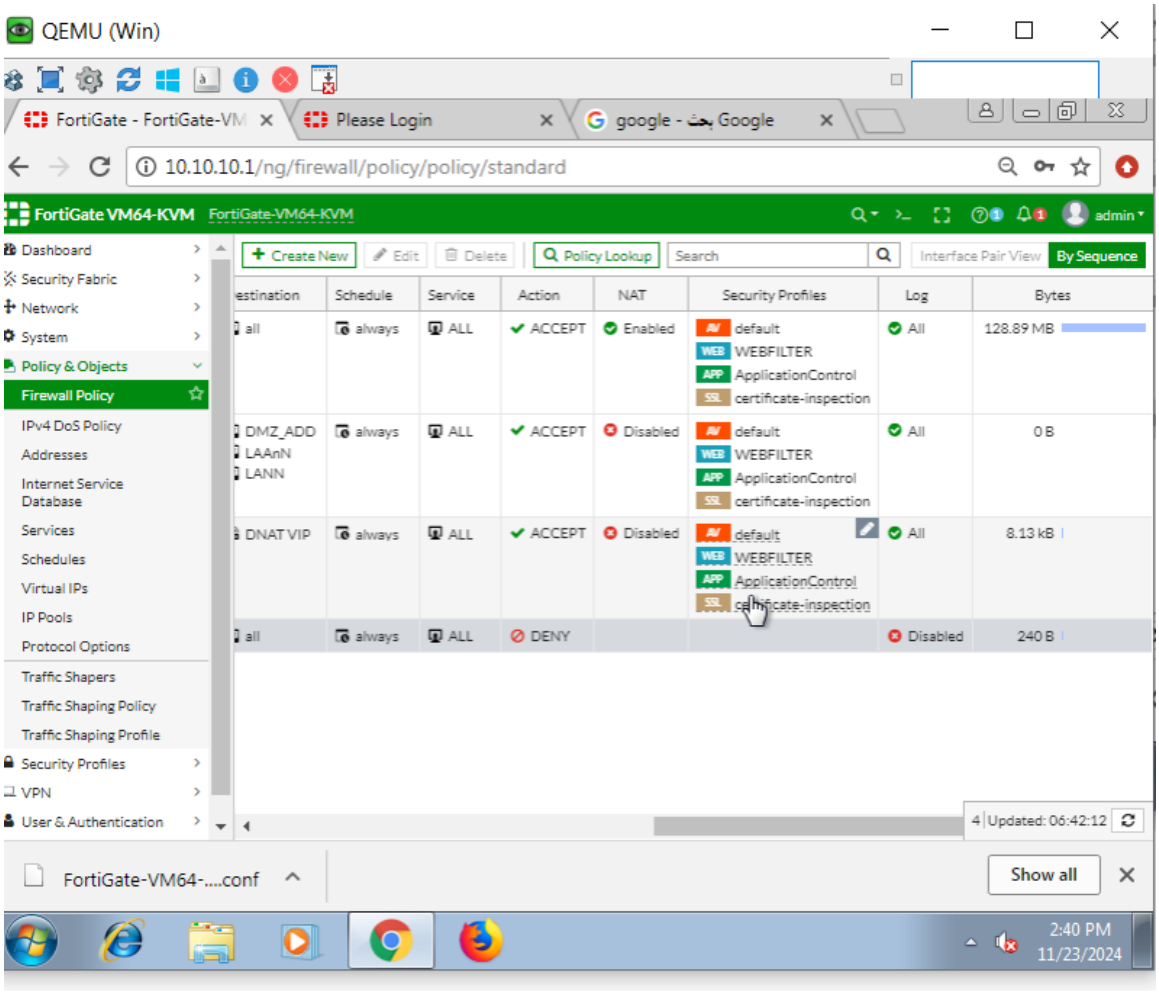


Figure2.2

2.Authentication: Authentication is the process of validating the identity of users before granting access. FortiGate supports a wide range of authentication methods including local user accounts, LDAP, RADIUS, and two-factor authentication.

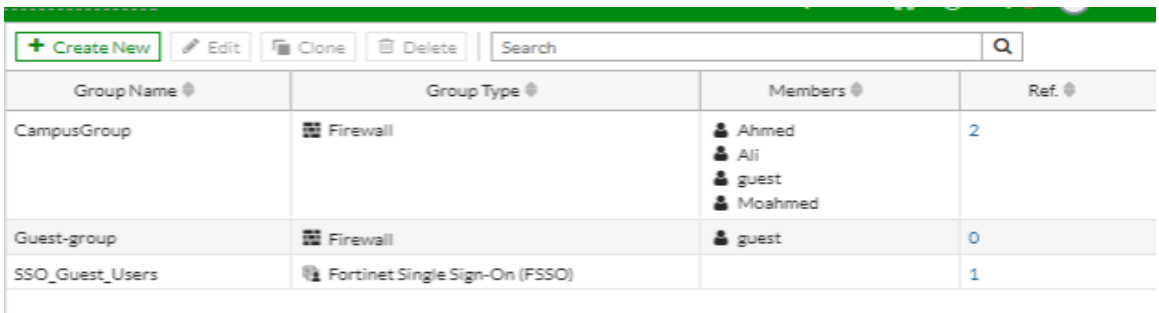


Figure2.3

3. **Admins**: Proper user and admin management is essential to maintaining secure access to network resources. FortiGate allows administrators to configure roles and permissions for different users and admins, ensuring that each user has access only to the resources they need.

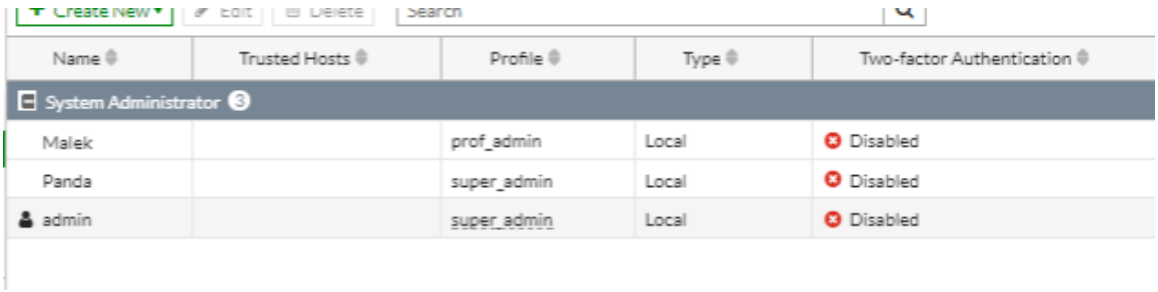


Figure2.4

4. **SD-WAN**: Software-Defined WAN (SD-WAN) optimizes the use of multiple network connections (MPLS, broadband, LTE) by dynamically directing traffic based on real-time conditions. This technology enhances application performance, improves bandwidth utilization, and provides a more cost-effective alternative to traditional WAN links.

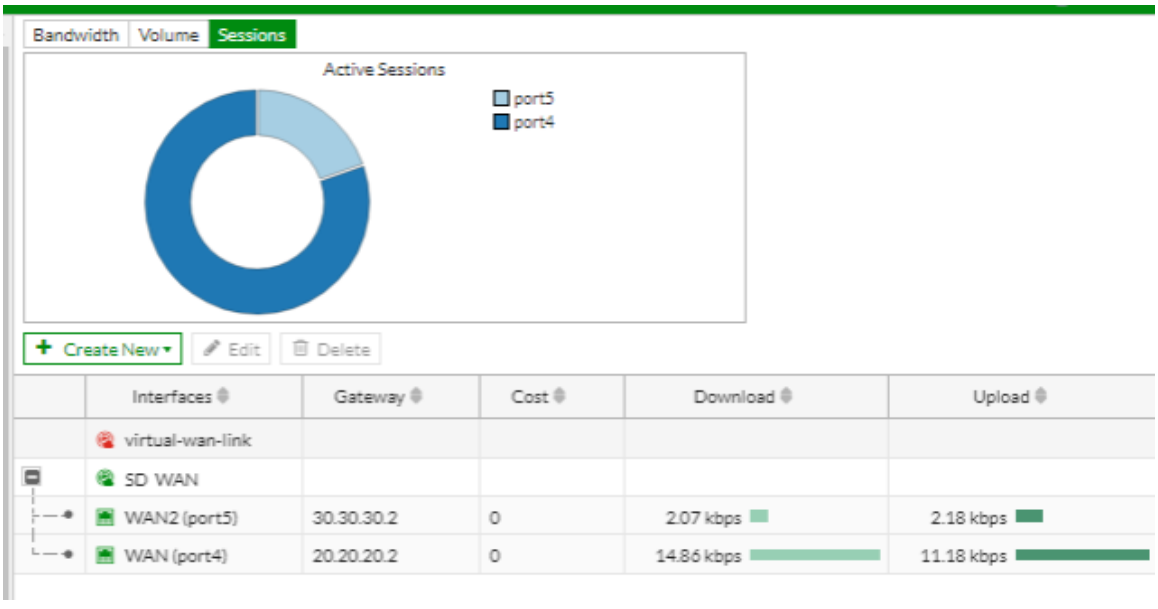


Figure2.5

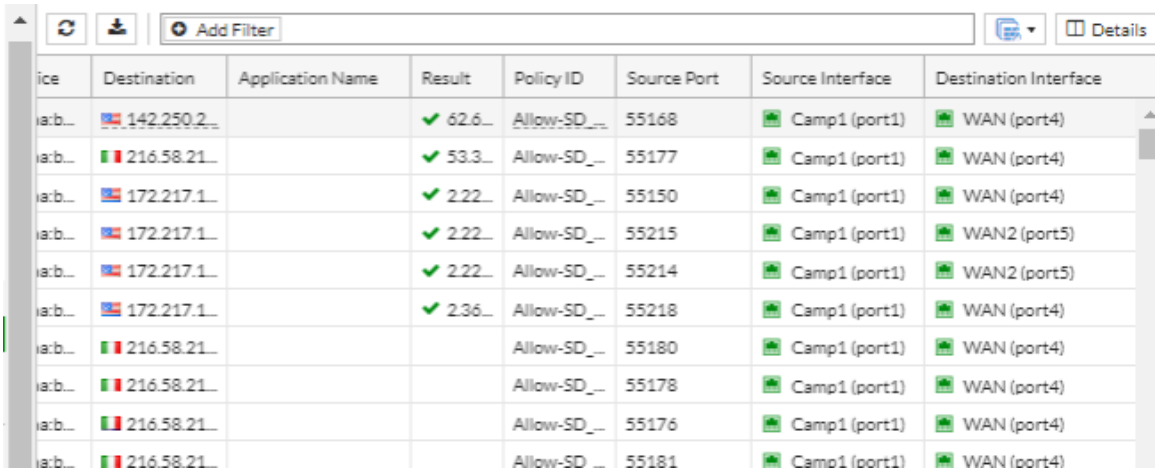


Figure2.6

5. **DNAT (Destination NAT):** This type of NAT translates the destination IP address of incoming packets. DNAT is typically used for port forwarding, allowing external users to access internal servers.

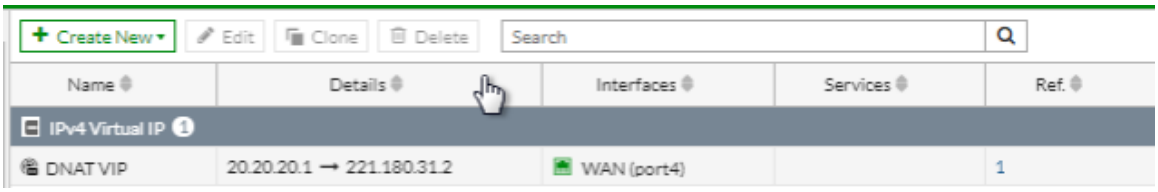


Figure2.7

6. **Application Control**: This feature allows organizations to control the applications that can run on their network. It includes the ability to block or allow specific applications and apply deep packet inspection to detect and block malicious traffic.

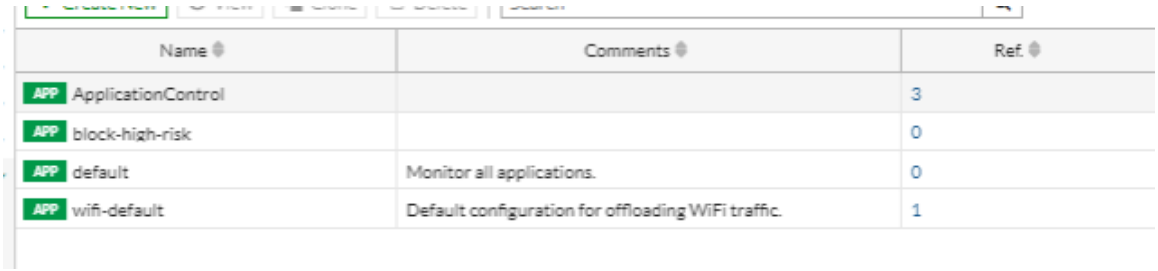


Figure2.8

7. **Antivirus**: Antivirus features on FortiGate devices scan network traffic for malware and viruses. By scanning files and traffic before it reaches the internal network, it prevents the spread of harmful content.

8. **Web Filtering**: Web filtering enables administrators to control web access based on categories, URLs, and other criteria. This helps prevent users from accessing harmful or non-productive websites.

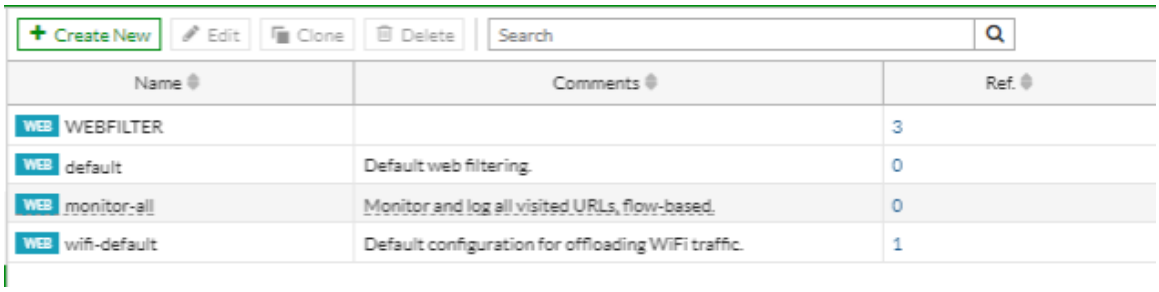


Figure2.9

9. **SSL VPN Remote Access**: SSL VPN provides secure, encrypted access to a network for remote users. It is often used in conjunction with two-factor authentication to ensure secure access from any device.

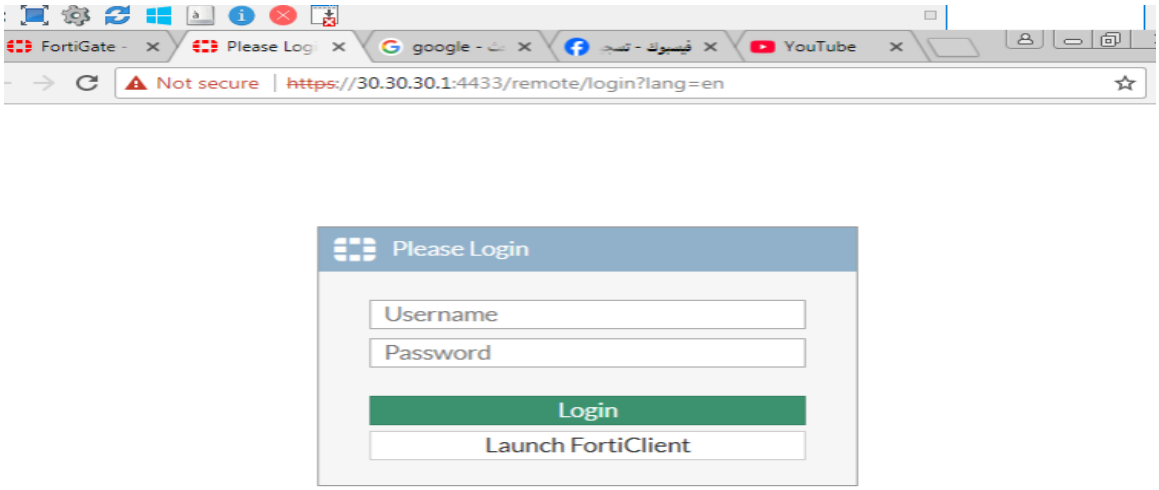


Figure2.10

10. Static Routes: Static routing is the process of manually configuring routing tables. It is useful for ensuring that specific traffic follows a predefined path.

Destination	Gateway IP	Interface	Status	Comments
IPv4 4				
0.0.0.0/0		SD-WAN	Enabled	
192.168.0.0/16	10.10.10.2	Camp1 (port1)	Enabled	
192.168.0.0/16	10.10.10.6	Camp2 (port2)	Enabled	
150.150.0.0/24	0.0.0.0	SSL-VPN tunnel interface (ssl.root)	Enabled	

Figure2.11

11. Backup: Backup of FortiGate configurations is crucial for disaster recovery. Regular backups ensure that administrators can restore settings in case of hardware failure or misconfiguration.

Some of attacks & its mitigations

1. DHCP Spoofing:

-Description: In a DHCP spoofing attack, an attacker masquerades as a legitimate DHCP server, providing clients with incorrect network configuration, such as the wrong default gateway or DNS server.

-Mitigation: Enable DHCP Snooping to only allow trusted DHCP servers on the network. Also, configure **Dynamic ARP Inspection** to prevent ARP spoofing attacks.

2. MAC Address Poisoning:

- Description: This attack involves sending fake MAC addresses onto the network to manipulate the network's MAC table. This could cause traffic to be forwarded to an attacker's device.

- Mitigation: Enable Port Security on switches to limit the number of MAC addresses allowed on a port. Use **Dynamic ARP Inspection** to ensure the correct mapping of IP addresses and MAC addresses.

3. Security Port Vulnerabilities:

-Description: Attackers exploit open or unused ports to gain unauthorized access to the network or launch attacks such as DoS (Denial of Service).

- Mitigation: Use Access Control Lists (ACLs)** to restrict access to ports.

Setup Servers

DHCP Sever

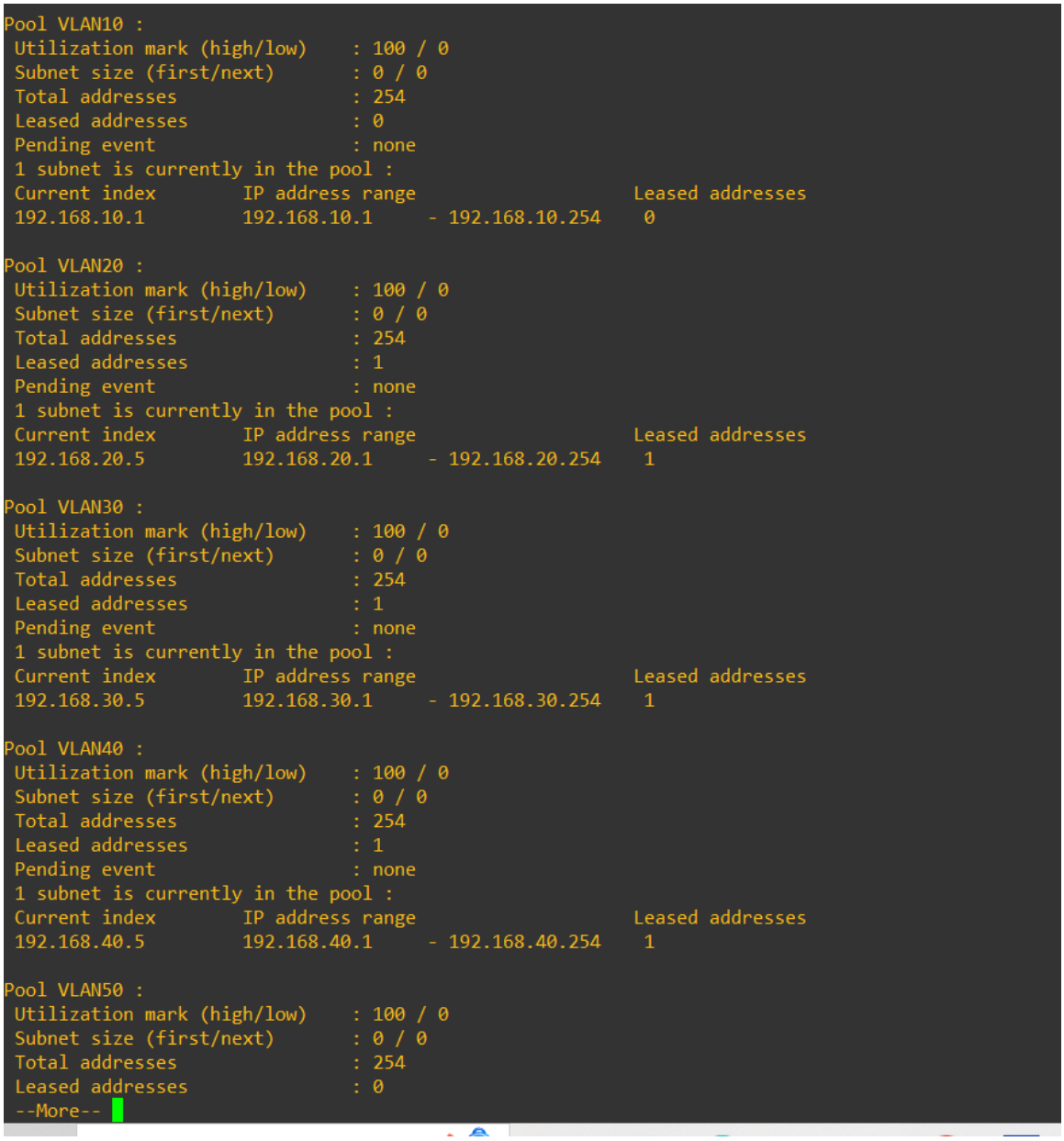


Figure2.12

WEBSERVER

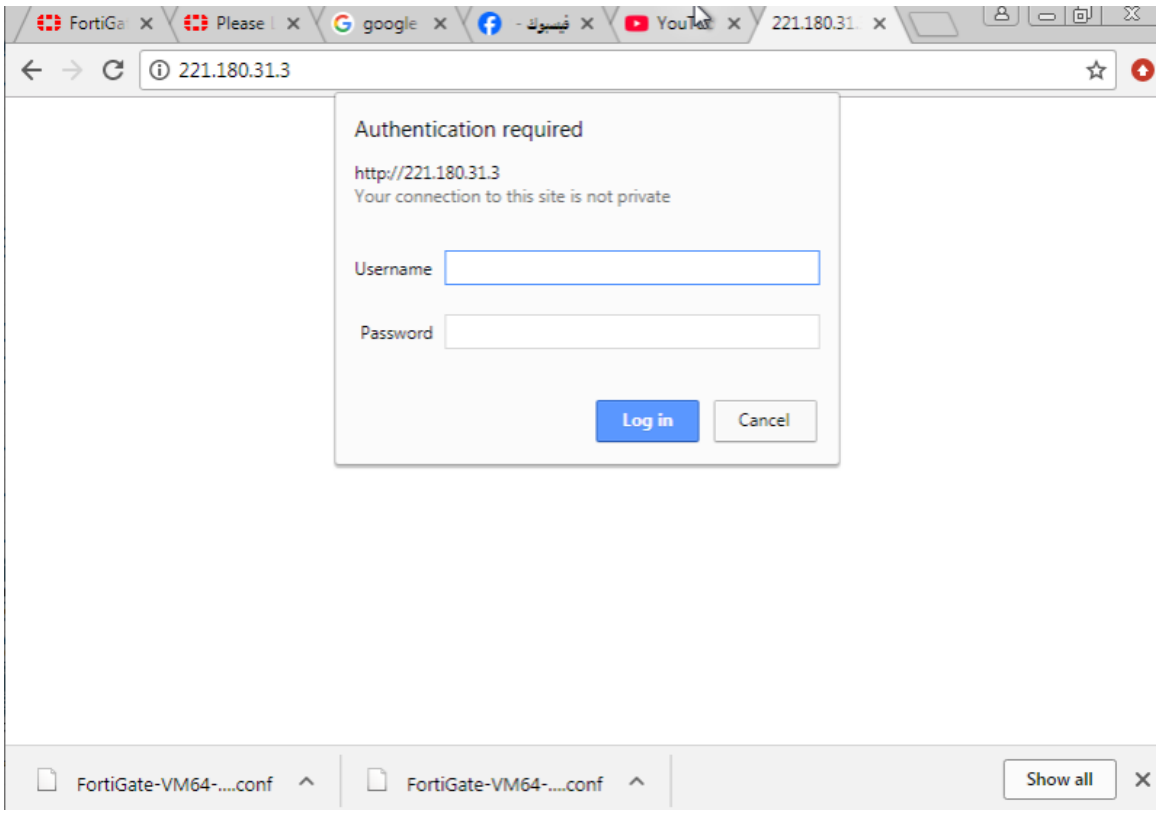


Figure2.13

Palo Alto Networks Overview

Palo Alto Networks is a leading cybersecurity company known for its **next-generation firewalls** (NGFW), cloud-based security services, and network security solutions. The company provides robust protection for enterprises by enabling threat prevention, application visibility, and secure access.

Key Features of Palo Alto Networks:

1. **Next-Generation Firewalls (NGFW)**: Palo Alto firewalls go beyond traditional firewalls by offering features such as application awareness, user identity-based policies, and advanced threat detection.
2. **Threat Intelligence**: The platform integrates advanced threat intelligence to block known and unknown threats, using techniques like signature-based detection and behavior analysis.
3. **URL Filtering**: It helps prevent access to malicious or inappropriate websites by filtering based on categories or specific URLs.
4. **SSL Decryption**: It decrypts SSL traffic to inspect encrypted communications for potential threats.
5. **WildFire**: A cloud-based malware analysis service that detects and prevents advanced threats by analyzing suspicious files in real-time.

Ethical Hacking Overview

Ethical hacking, also known as **white-hat hacking**, refers to the practice of legally probing systems, networks, and applications for vulnerabilities to help organizations strengthen their security. Ethical hackers use the same tools and techniques as malicious hackers but with permission to identify weaknesses before they can be exploited by cybercriminals.

Key Aspects of Ethical Hacking:

1. **Reconnaissance**: Information gathering about the target, including public details and network infrastructure.
2. **Scanning**: Using tools to identify open ports, services, and vulnerabilities in systems.
3. **Gaining Access**: Attempting to exploit vulnerabilities to gain unauthorized access to a system.
4. **Maintaining Access**: Creating backdoors or persistent access to the system for later exploitation.
5. **Analysis and Reporting**: Documenting findings and providing recommendations for fixing vulnerabilities.

Ethical hackers are typically hired by organizations to perform **penetration testing** and **vulnerability assessments** to identify and mitigate potential security risks. Ethical hacking is an essential part of proactive cybersecurity, aiming to reduce the chance of data breaches and system compromises.