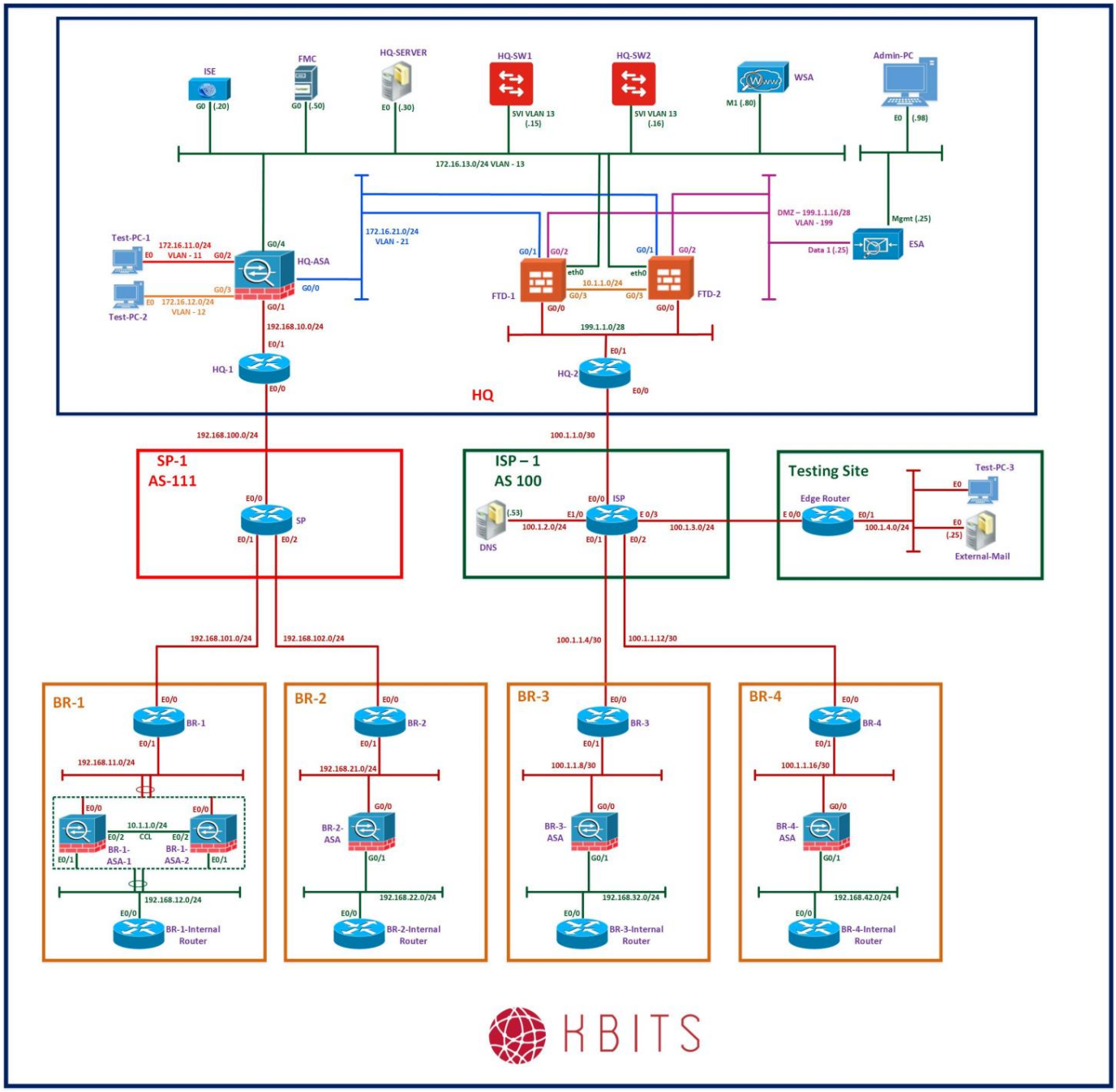
# CCIE Security v6 – Super Lab

**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

## Section 1

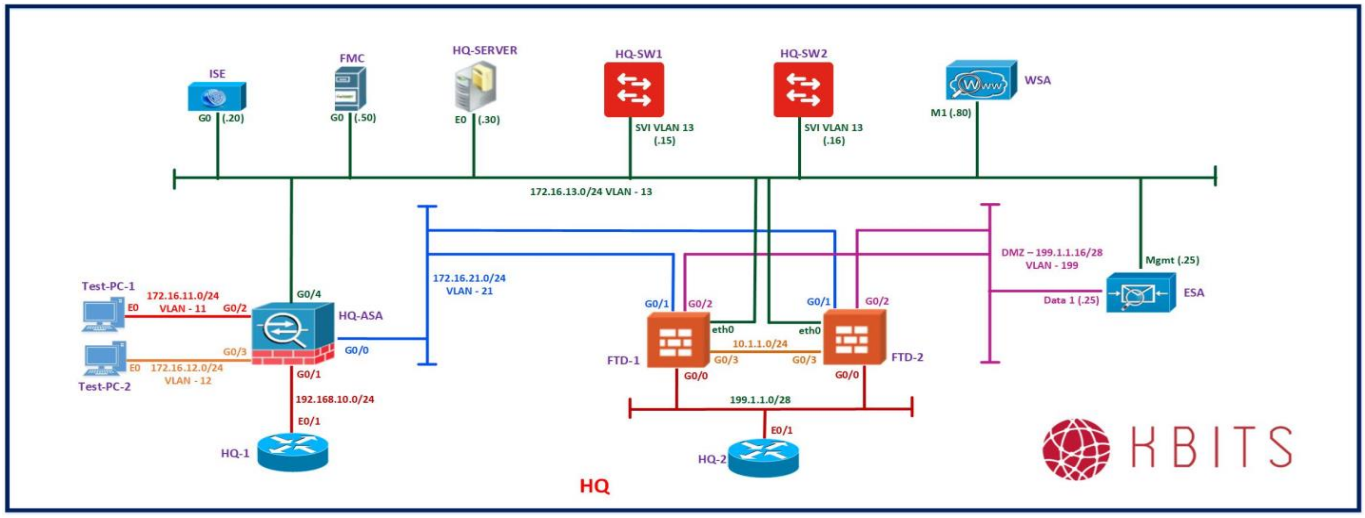
## Firewalls – ASA

# Full Logical Topology

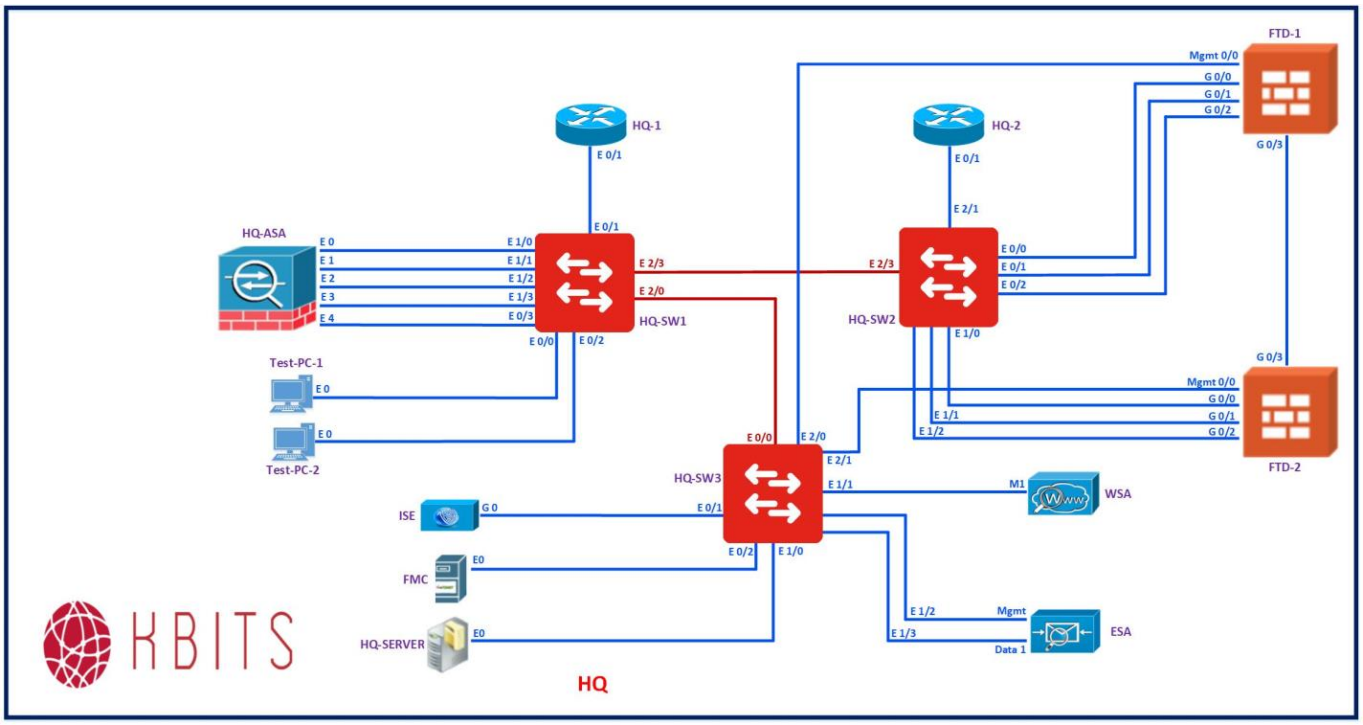


# Lab 1 – Configuring the HQ ASA Firewall

## HQ - Logical




## HQ – Layer 2 (Physical)



## Interface Configuration (Pre-Configured)

### HQ-1

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.100.1 | 255.255.255.0 |
| E 0/1 | 192.168.10.1 | 255.255.255.252 |
| Loopback10 | 172.25.1.1 | 255.255.255.255 |

### HQ-2

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 100.1.1.2 | 255.255.255.252 |
| E 0/1 | 199.1.1.1 | 255.255.255.240 |
| Loopback10 | 172.25.1.2 | 255.255.255.255 |

### HQ-SW1

| Interface | IP Address | Subnet Mask |
|---|---|---|
| SVI VLAN 13 | 172.16.13.15 | 255.255.255.0 |
| Loopback10 | 172.25.1.3 | 255.255.255.255 |

### HQ-SW2

| Interface | IP Address | Subnet Mask |
|---|---|---|
| SVI VLAN 13 | 172.16.13.16 | 255.255.255.0 |
| Loopback10 | 172.25.1.4 | 255.255.255.255 |

## Task 1 – Configure the HQ-ASA interfaces based on the following:

### HQ-ASA

| Interface | IP Address | Name | Security Level |
|---|---|---|---|
| E 0 | 172.16.21.10/24 | Outside | 0 |
| E 1 | 192.168.10.10/24 | PRIVATE-WAN | 25 |
| E 2 | 172.16.11.10/24 | Inside-Emp | 100 |
| E 3 | 172.16.12.10/24 | Inside-Cons | 75 |
| E 4 | 172.16.13.10/24 | MGMT-SERVER | 50 |

## Task 2 – Configure the DHCP Scopes on the HQ-SW1

- Configure the following scopes on the HQ-SW1:
  - Name: Employees
    - Range:172.16.11.51-172.16.11.200
    - Subnet Mask: /24
    - Default-Gateway: 172.16.11.10
    - DNS Server: 172.16.13.30
  - Name: Consultants
    - Range:172.16.12.51-172.16.12.200
    - Subnet Mask: /24
    - Default-Gateway: 172.16.12.10
    - DNS Server: 172.16.13.30

## Task 3 – Configure HQ-ASA as a DHCP Relay Agent

- Configure HQ-ASA to forward the DHCP Requests coming from clients on VLAN 11 & VLAN 12 to be forwarded towards the DHCP Server (172.16.13.15)

## Task 4 – Verification

- Verify that you can ping the HQ-Server from HQ-ASA
- Verify that you can ping ISE from HQ-ASA
- Verify that you can ping the switches (HQ-SW1 & HQ-SW2) from HQ-ASA.
- Verify that the Test-PCs are receiving appropriate addresses and they can ping their Default Gateway addresses.

## Task 5 – Configure OSPF on the HQ-ASA

- Configure HQ-ASA to run OSPF as the routing protocol.
- Configure it in Process ID 1.
- Enable the following networks in area 0 for OSPF Process 1:
  - 172.16.21.0/24
  - 172.16.11.0/24
  - 172.16.12.0/24
  - 172.16.13.0/24
  - 192.168.10.0/24
- Configure a default route on the Outside interface towards 172.16.21.3.

## Task 6 – Control Pinging the ASA Firewall

- The following should be the only IP addresses allowed to Ping the Outside Interface of HQ-ASA.
  - FTD-1 – Gig0/1 (172.16.21.3)
- HQ-ASA should be able to ping devices on the Outside interface and receive a response.

## Task 7 – Controlling Access to FMC

- The Employees and Consultants Subnets should not be able to connect to the FMC device. They should have all other access.

## Task 8 – Controlling Access to ISE & DNS

- Allow HQ-2 access to ISE for RADIUS (UDP/1812 & 1813) & TACACS+ (TCP/49).
- DNS Server is installed on the HQ-SERVER. It should be fully accessible to all users from Outside.

## Task 9 – Controlling Access to a Web Server

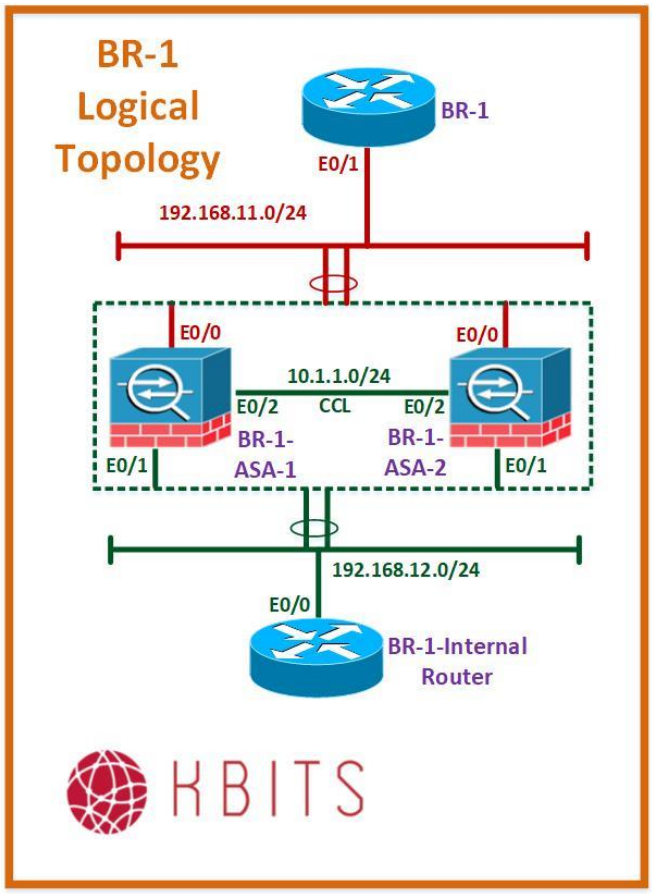
- HQ-SERVER is also acting as a Web Server. Allow HTTP & HTTPS access to it from the Outside.

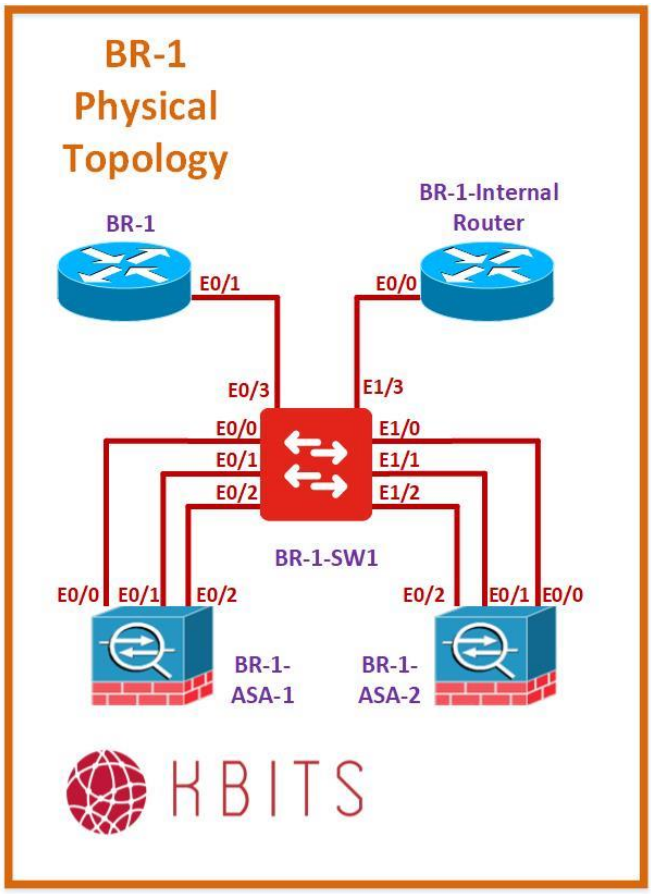
## Task 10 – Controlling ICMP

- ICMP Traffic that is allowed to pass-thru the firewall should be able to receive a response successfully. Do not create an ACL for this task.

# Lab 2 – Configuring the BR-1 ASA Firewall

## BR-1



## Interface Configuration (Pre-Configured)

### BR-1

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.101.11 | 255.255.255.0 |
| E 0/1 | 192.168.11.11 | 255.255.255.0 |
| Loopback10 | 172.25.1.11 | 255.255.255.255 |

### BR-1-Internal

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.12.12 | 255.255.255.0 |
| Loopback0 | 172.20.11.1 | 255.255.255.0 |
| Loopback1 | 172.20.12.1 | 255.255.255.0 |
| Loopback10 | 172.25.1.12 | 255.255.255.255 |

### Task 1 – Configure a Cluster between the 2 ASA Firewalls

- BR-1-ASA-1 & BR-2-ASA-2 will be configured in a Cluster. BR-1-ASA-1 will be the Master Firewall and BR-2-ASA-2 will be the Backup Firewall. Use the following parameters for the Failover configurations:
  - Cluster Interface Mode: Spanned
  - Cluster Group Name: CCIEv6
  - Cluster Interface: E2
  - Cluster Interfac IP Address – Master: 10.1.1.1/24
  - Cluster Interfac IP Address – Slave: 10.1.1.2/24
  - Cluster Key: cisco123

### Task 2 – Configure Cluster Interfaces as Port Channels

- Configure Cluster ASA Ports and the correcponding switch ports in a Port-channel based on the following table.

| Interface | Port-Channel # | Protocol | VLAN |
|---|---|---|---|
| E0 | 11 | LACP | 11 |
| E1 | 12 | LACP | 12 |

- Assign the BR-1 & BR-1-Internal router switch ports in the appropriate VLANs

## Task 3 – Configuring the Port Channel Interfaces

- Configure the Port-channel Interfaces based on the following table:

### BR-1 ASA Cluster

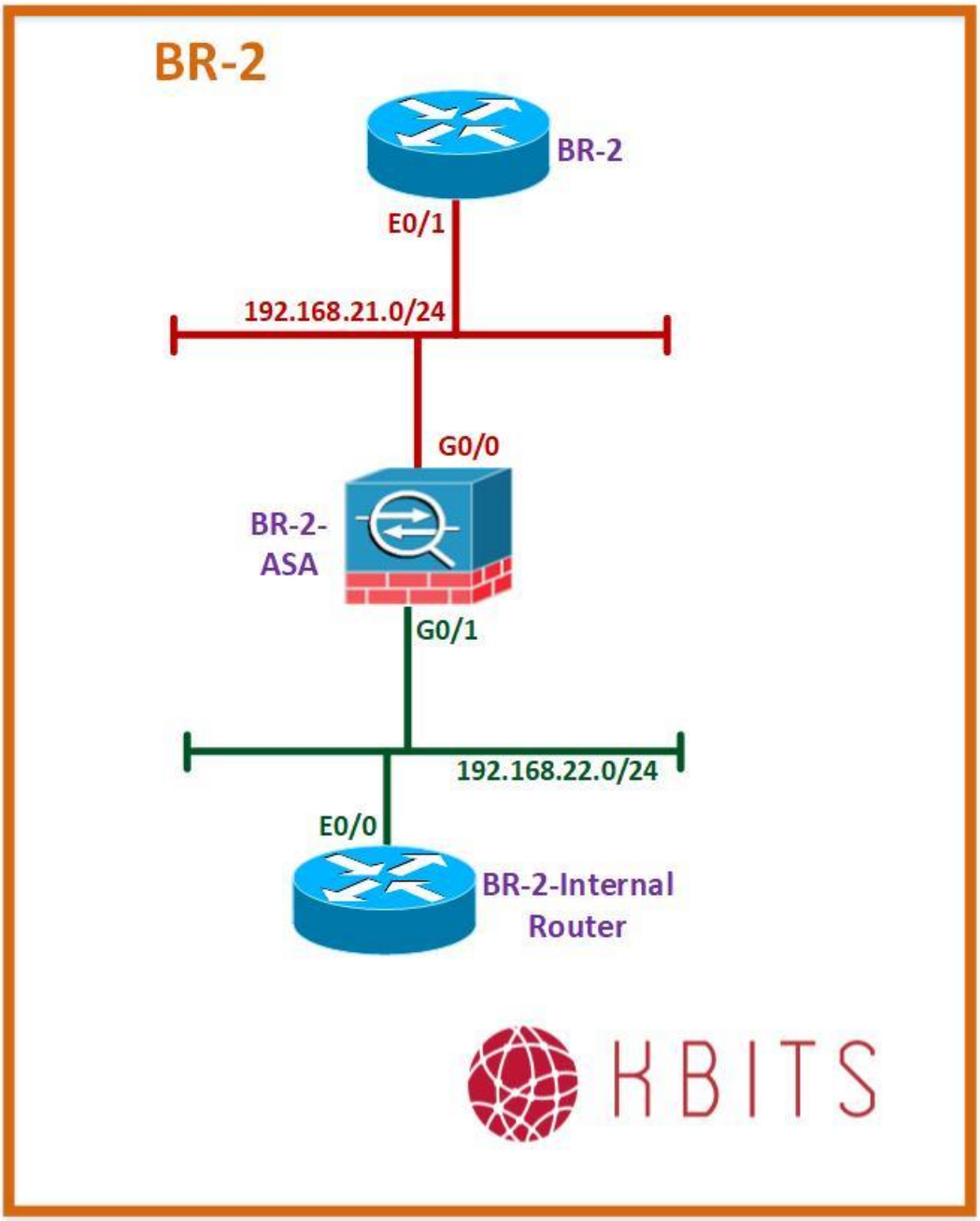
| Interface | IP Address | Name | Security Level | Mac Address |
|---|---|---|---|---|
| Po11(E0) | 192.168.11.10/24 | Outside | 0 | 0001.1111.0011 |
| Po12(E1) | 192.168.12.10/24 | Inside | 100 | 0001.1111.0012 |

## Task 4 – Configure Routing

- Configure OSPF on BR-1 ASA Cluster on the Outside & Inside Interfaces.
- Configure OSPF on BR-1 Internal router to route all interfaces.
- BR-1 ASA Cluster and BR-1 Internal router should be in Area 0.

# Lab 3 – Configuring the BR-2 ASA Firewall

**BR-2**



## Interface Configuration (Pre-Configured)

### BR-2

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.102.21 | 255.255.255.0 |
| E 0/1 | 192.168.21.21 | 255.255.255.0 |
| Loopback10 | 172.25.1.21 | 255.255.255.255 |

### BR-2-Internal

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.22.22 | 255.255.255.0 |
| Loopback0 | 172.20.21.1 | 255.255.255.0 |
| Loopback1 | 172.20.22.1 | 255.255.255.0 |
| Loopback10 | 172.25.1.22 | 255.255.255.255 |

### Task 1 – Configure the BR-2-ASA interfaces based on the following:

### BR-2-ASA

| Interface | IP Address | Name | Security Level |
|---|---|---|---|
| G 0/0 | 192.168.21.10/24 | Outside | 0 |
| G 0/1 | 192.168.22.10/24 | Inside | 100 |

### Task 2 – Configure Routing

- Configure OSPF on BR-2 ASA on the Outside & Inside Interfaces.
- Configure OSPF on BR-2 Internal router to route all interfaces.
- BR-2 ASA and BR-2 Internal router should be in Area 0.

### Task 3 – Configuring Access thru BR-2-ASA Firewall

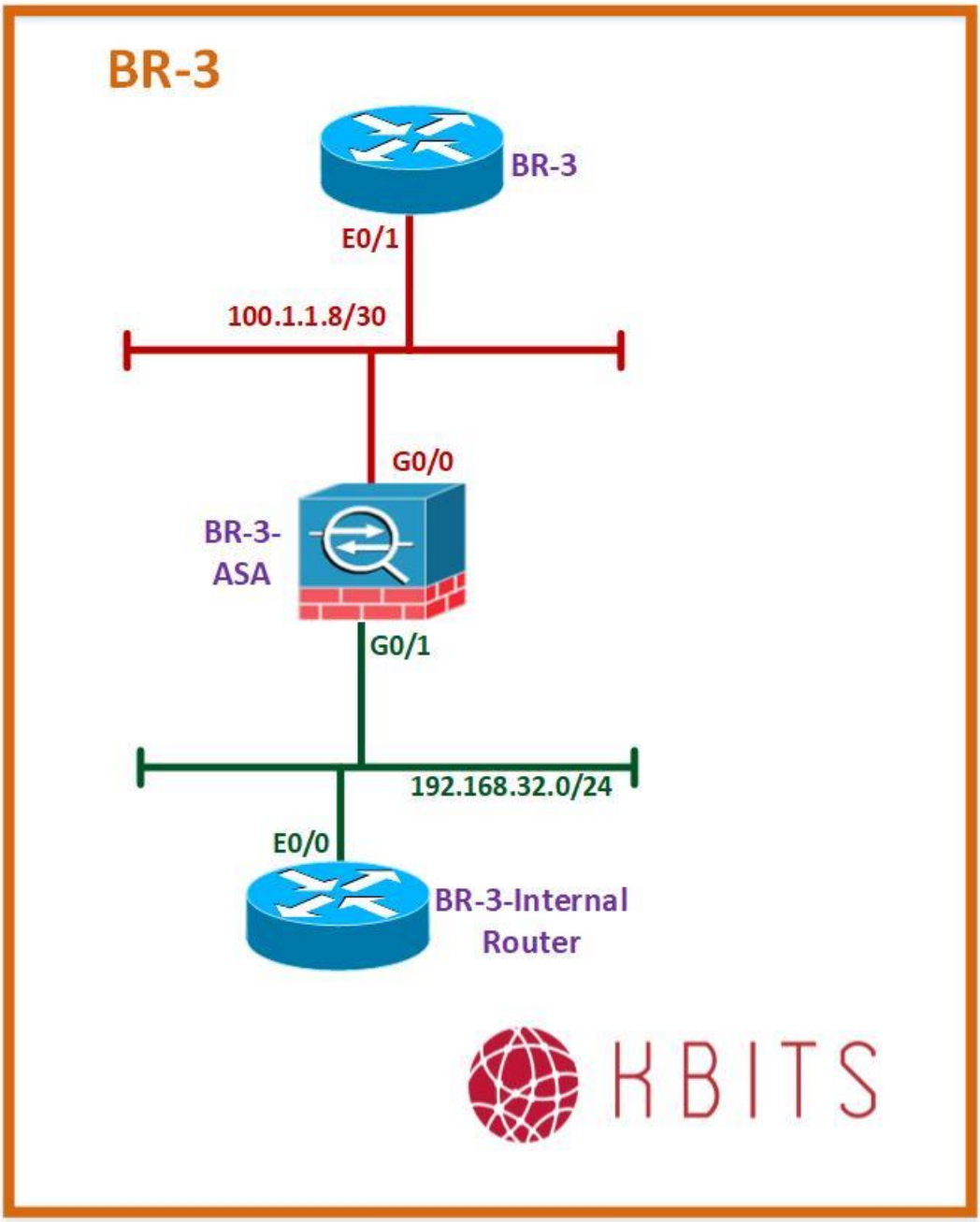
- The internal users should be able to ping the outside networks.
- Don't enable any type of inspection.

### Task 4 – Configure Management of Firewall

- Allow the 172.16.13.0/24 network SSH access to the firewall.
- Configure a username admin1 with a password of C1SCO123. It should be assigned a privilege of 15.
- This user should be used for Management access.

# Lab 4 – Configuring the BR-3 ASA Firewall

**BR-3**



## Interface Configuration (Pre-Configured)

### BR-3

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 100.1.1.6 | 255.255.255.252 |
| E 0/1 | 100.1.1.9 | 255.255.255.252 |
| Loopback10 | 172.25.1.31 | 255.255.255.255 |

### BR-3-Internal

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.32.32 | 255.255.255.0 |
| Loopback0 | 172.20.31.1 | 255.255.255.0 |
| Loopback1 | 172.20.32.1 | 255.255.255.0 |
| Loopback10 | 172.25.1.32 | 255.255.255.255 |

### Task 1 – Configure the BR-3-ASA interfaces based on the following:

### BR-3-ASA

| Interface | IP Address | Name | Security Level |
|---|---|---|---|
| G 0/0 | 100.1.1.10/30 | Outside | 0 |
| G 0/1 | 192.168.32.10/24 | Inside | 100 |

### Task 2 – Configure Routing

- Configure OSPF in Process ID 1 on the BR-3-ASA Firewall. Enable the Inside Interface in OSPF.
- Configure a default route on the Outside interface towards BR-3 Edge Router.

### Task 3 – Configuring NAT

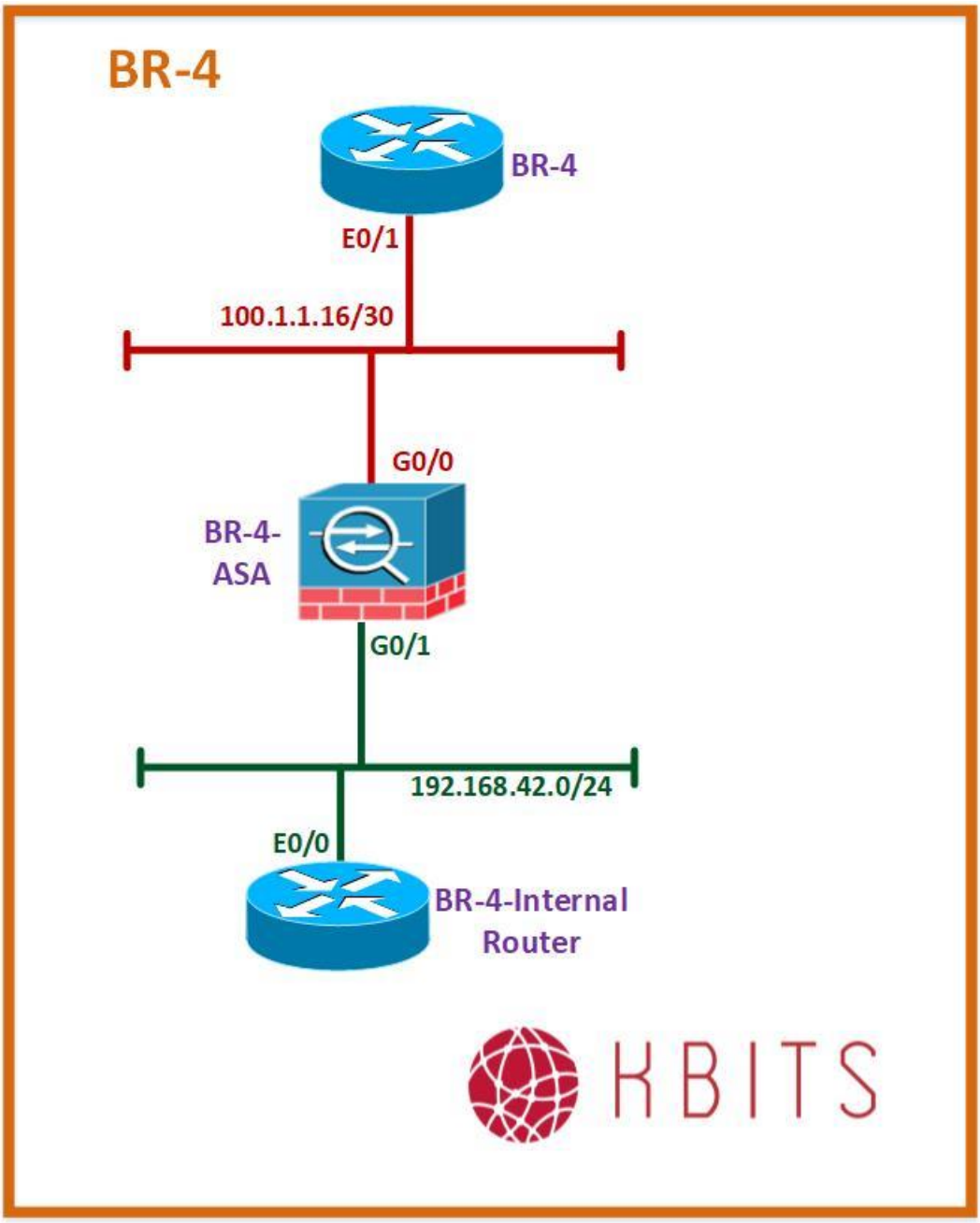
- The BR-3-Internal loopback networks (172.20.0.0/16) should be translated to the Outside Interface of the BR-3-ASA Firewall.

### Task 4 – Configuring Access thru the Firewall

- Allow the Internal Networks to go out for HTTP, HTTPS, Telnet, SSH & ICMP only.
- The Internal networks should be able to ping outside networks.

# Lab 5 – Configuring the BR-4 ASA Firewall

**BR-4**



## Interface Configuration (Pre-Configured)

### BR-4

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 100.1.1.14 | 255.255.255.252 |
| E 0/1 | 100.1.1.17 | 255.255.255.252 |
| Loopback10 | 172.25.1.41 | 255.255.255.255 |

### BR-4-Internal

| Interface | IP Address | Subnet Mask |
|---|---|---|
| E 0/0 | 192.168.42.42 | 255.255.255.0 |
| Loopback0 | 172.20.41.1 | 255.255.255.0 |
| Loopback1 | 172.20.42.1 | 255.255.255.0 |
| Loopback10 | 172.25.1.42 | 255.255.255.255 |

### Task 1 – Configure the BR-4-ASA interfaces based on the following:

### BR-4-ASA

| Interface | IP Address | Name | Security Level |
|---|---|---|---|
| G 0/0 | 100.1.1.18/30 | Outside | 0 |
| G 0/1 | 192.168.42.10/24 | Inside | 100 |

### Task 2 – Configure Routing

- Configure OSPF in Process ID 1 on the BR-4-ASA Firewall. Enable the Inside Interface in OSPF.
- Configure a default route on the Outside interface towards BR-4 Edge Router.

### Task 3 – Configuring NAT

- The internal users should be translated to the Outside Interface of the BR-4-ASA Firewall.

## Task 4 – Configuring Access thru the Firewall

- Allow the Internal Networks to go out for HTTP, HTTPS, Telnet, SSH & ICMP only.
- The Internal networks should be able to ping outside.

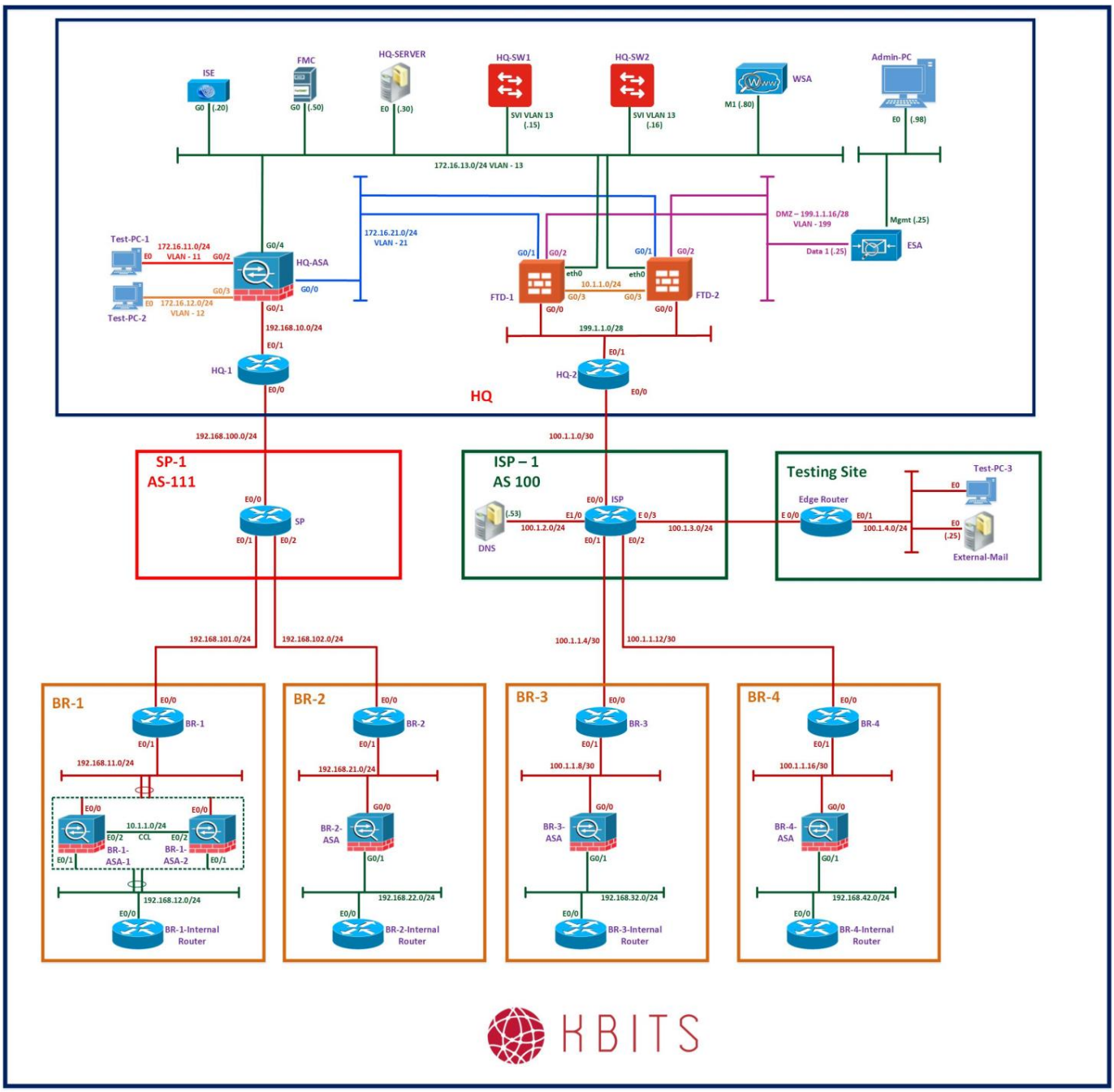
# CCIE Security v6 – Super Lab

**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

## Section 2

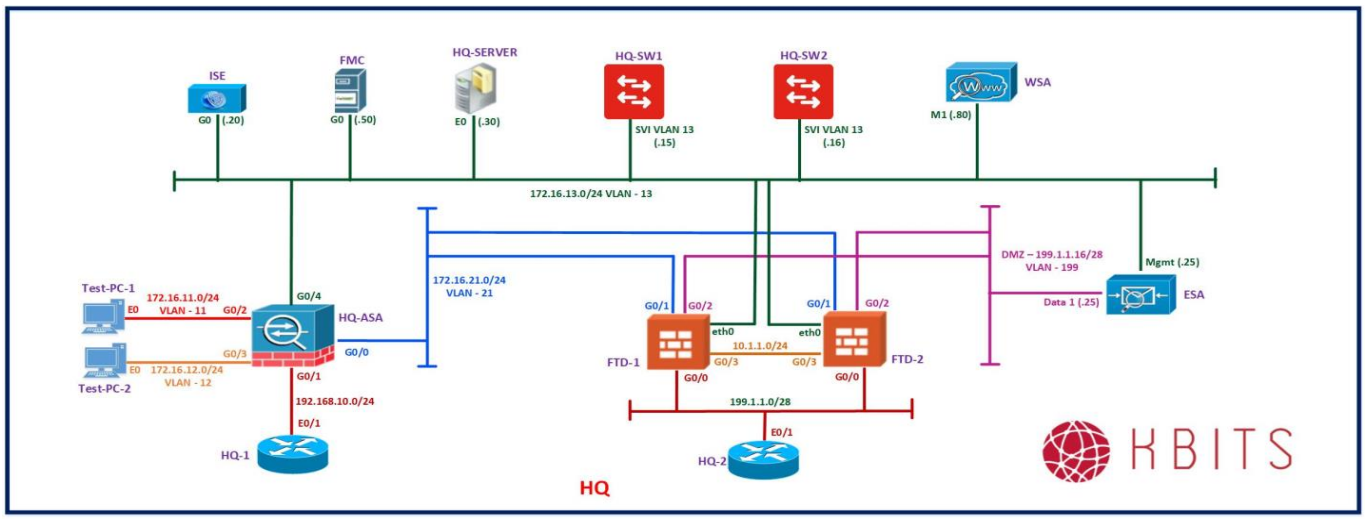
## Firewalls – FTD

# Full Logical Topology

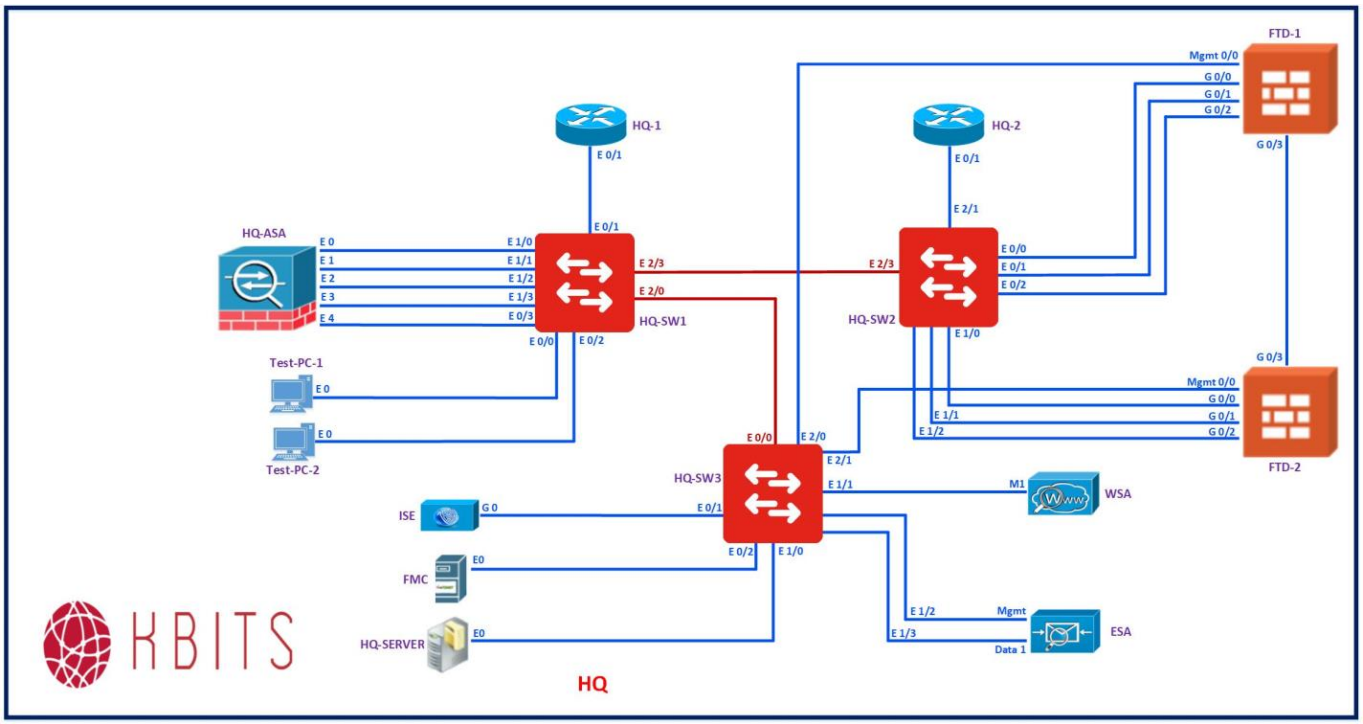


# Lab 1 – Configure the relationship between FMC & FTD

## HQ - Logical




## HQ – Layer 2 (Physical)



## Task 1 – Initialize FTDs (Pre-Configured)

- Initialize FTD-1 from the CLI based on the following
  - Username/Password: admin/Admin123
  - Network Configuration:
    - Interface IP:172.16.13.51
    - Subnet Mask: /24
    - Default-Gateway: 172.16.13.10
    - DNS Server: 172.16.13.30
  - Mode: Routed
  - FMC/Manager: 172.16.13.50
  - Secret Key: cisco123
- Initialize FTD-2 from the CLI based on the following
  - Username/Password: admin/Admin123
  - Network Configuration:
    - Interface IP:172.16.13.52
    - Subnet Mask: /24
    - Default-Gateway: 172.16.13.10
    - DNS Server: 172.16.13.30
  - Mode: Routed
  - FMC/Manager: 172.16.13.50
  - Secret Key: cisco123

## Task 2 – Configure the relationship between FMC & FTD by adding FTDs in FMC (Pre-Configured)

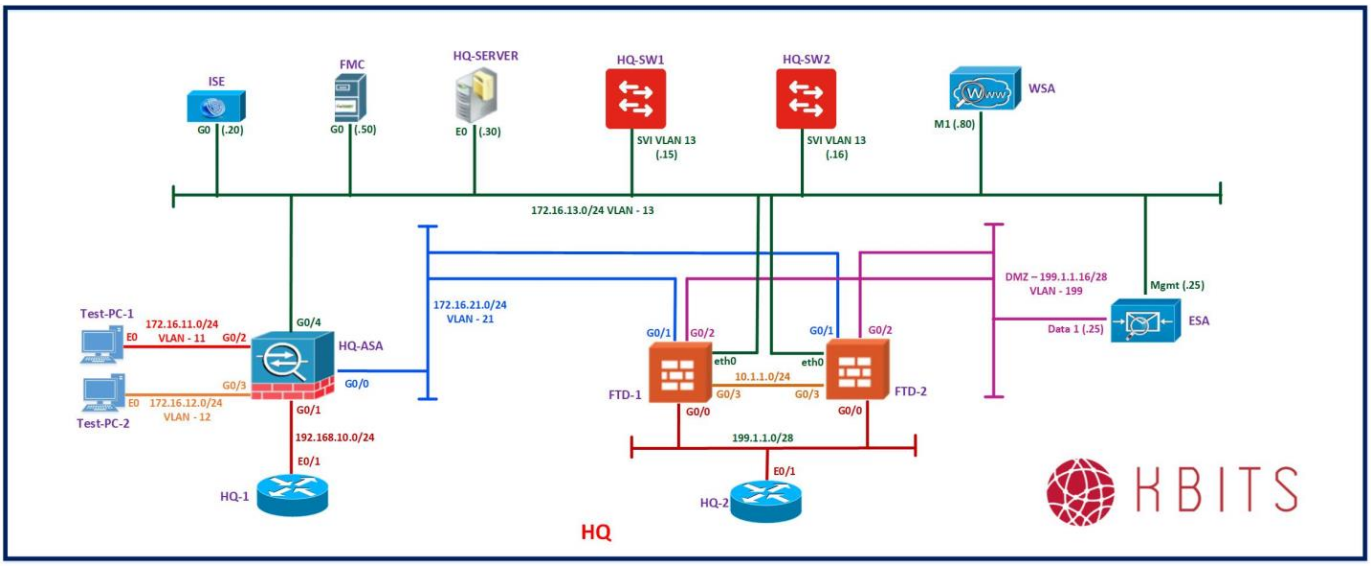
- Add FTD-1 to FMC using the following:
  - Host: 172.16.13.51
  - Name: FTD-1
  - Registration Key: Cisco123
  - Configure the Default Policy using a Name of FTD-ACP-POLICY with Block All
  - Enable all the Licenses and Add the Device
- Add FTD-2 to FMC using the following:
  - Host: 172.16.13.52
  - Name: FTD-2
  - Registration Key: Cisco123
  - Configure the Default Policy with Block All
  - Enable all the Licenses and Add the Device

## Task 3 – Create a management group and add FTD's

- Create a management group called Perimeter-FW
- Add FTD-1 & FTD-2 to the new group

# Lab 2 – Configure Failover between FTD1 & FTD2

## HQ

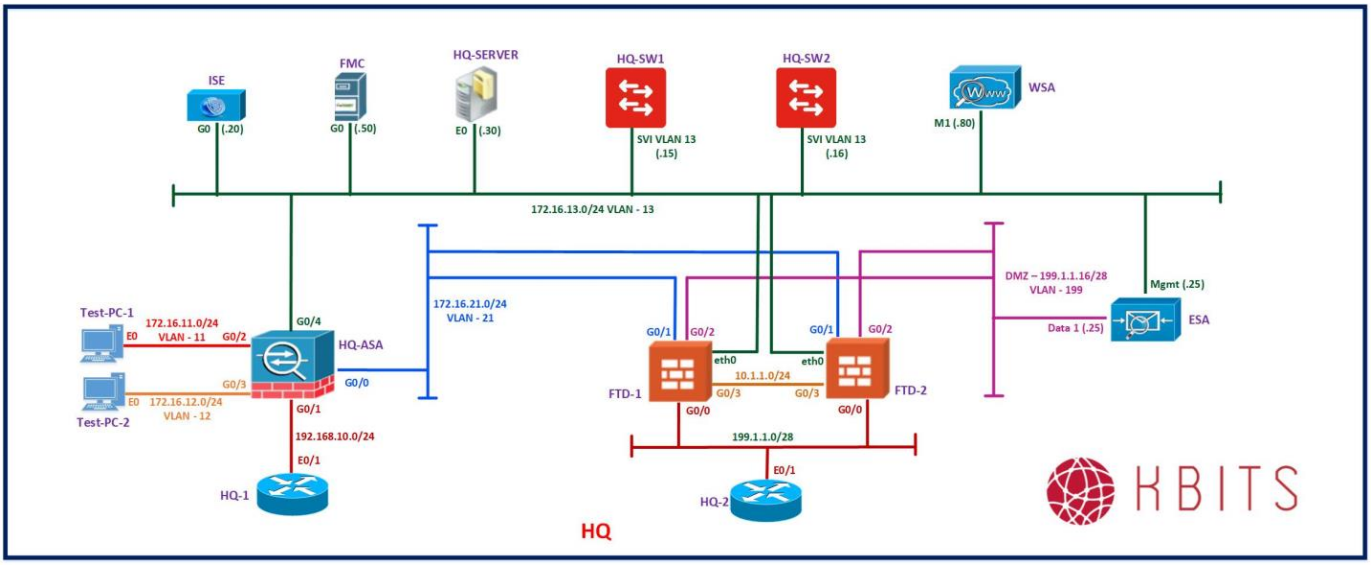



### Task 1 – Configure High Availability & Add FTDs

- Configure High Availability between FTD-1 & FTD-2 in a High Availability group called FTD-HA
- Configure FTD-1 as the Primary Device & FTD-2 as the Secondary Device
- Use the following High Availability parameters:
  - High Availability Link: Gig0/3
  - Stateful Link: Gig0/3 (Same link as High Availability Link)
  - Name: Failover
  - Primary IP: 10.1.1.1
  - Secondary IP: 10.1.1.2
  - Subnet Mask: 255.255.255.0
  - IPSec Encryption Enabled
  - Key: cisco123

# Lab 3 – Configure Interface IP's & Routing

## HQ




**Task 1 – Configure the FTD-HA interfaces based on the following:**

## Interface Parameters

### FTD-HA

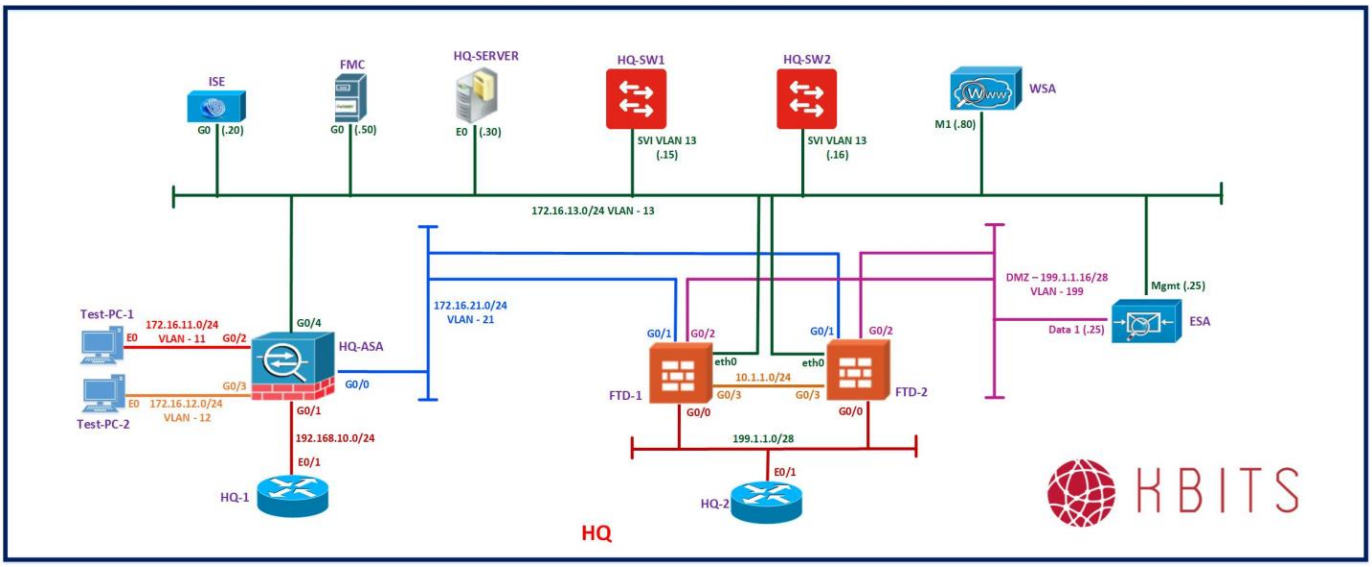
| Interface | IP Address(A) | IP Address (S) | Name | Zone |
|---|---|---|---|---|
| Gig0/0 | 199.1.1.11/28 | 199.1.1.12/28 | Outside | OUTSIDE |
| Gig0/1 | 172.16.21.3/24 | 172.16.21.4/24 | Inside | INSIDE |
| Gig0/2 | 199.1.1.30/28 | 199.1.1.29/28 | DMZ | DMZ |

**Task 2 – Configure Routing on the FTD-HA Device**

- Configure OSPF in Process ID 1 to communicate on the Outside, Inside and DMZ interfaces.
- Configure FTD-HA with a Default Route pointing towards HQ-2.
- Configure a Static Routes on the HQ-2 for the 199.1.1.16/28 & 192.168.10.1/32 networks via FTD-HA (199.1.1.11).

# Lab 4 – Configure NAT

## HQ




### Task 1 – Configuring NAT for Internal Users

- Configure FTD to translate all traffic coming from Inside Subnets towards the Outside to be translated to 199.1.1.5.

### Task 2 – Configuring NAT for ISE

- ISE should not get translated when it communicates to HQ-2.

### Task 3 – Configuring NAT for HQ-SERVER

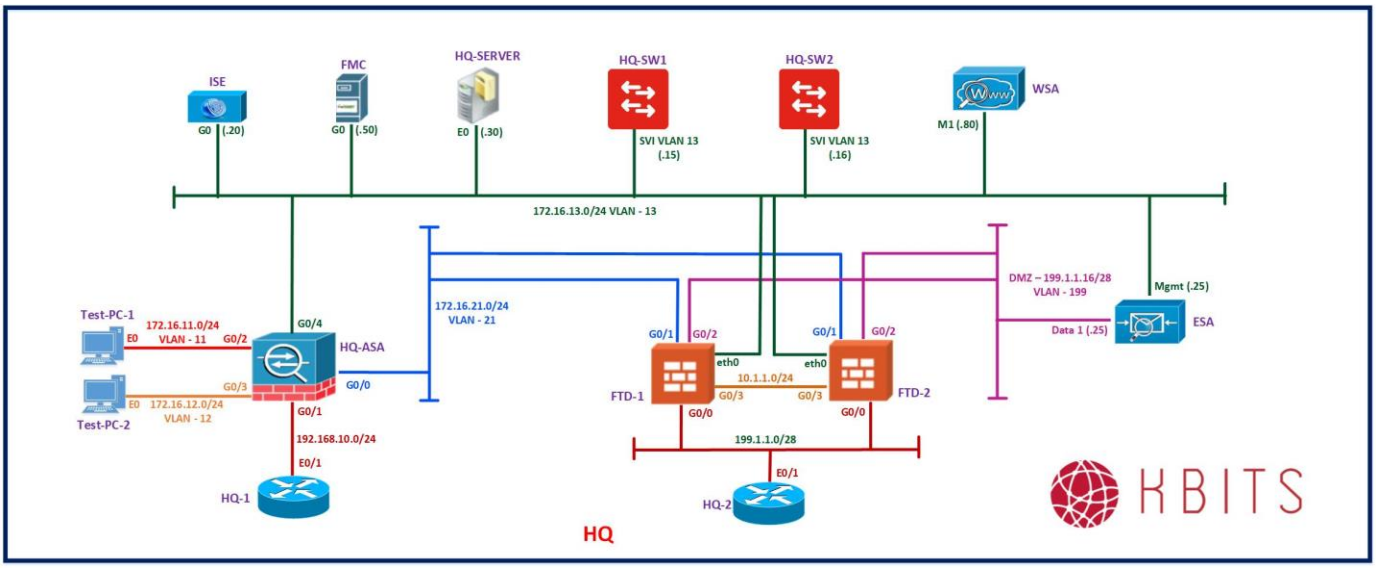
- HQ-SERVER should get translated to 199.1.1.6 on the Outside.

### Task 4 – Configuring NAT for WebServer

- There is a Web Server located at 172.16.13.35. Translate it to 199.1.1.7.

# Lab 5 – Configure Access Control Policies

## HQ




### Task 1 – Configure Access Policies for the Inside Network.

- All Inside networks should be able to access the access all the Interfaces.
- Allow HQ-2 RADIUS & TACACS+ access to ISE.
- Allow HTTP & HTTPS access to the Web Server located behind HQ-ASA (172.16.13.35) from the Outside.
- The first rule should be in the default policy. The of the policies should be in the Mandatory Policy.

### Task 2 – Configure AVC

- Configure the ACP to block Inside users from Accessing Facebook Video Chats and Facetime.

### Task 3 – Configure an IPS Policy

- Re-configue the Web Server ACP Entries to check against the IPS Engine before allowing access.
- Use the Default IPS “Balanced Security and Connectivity” rule.

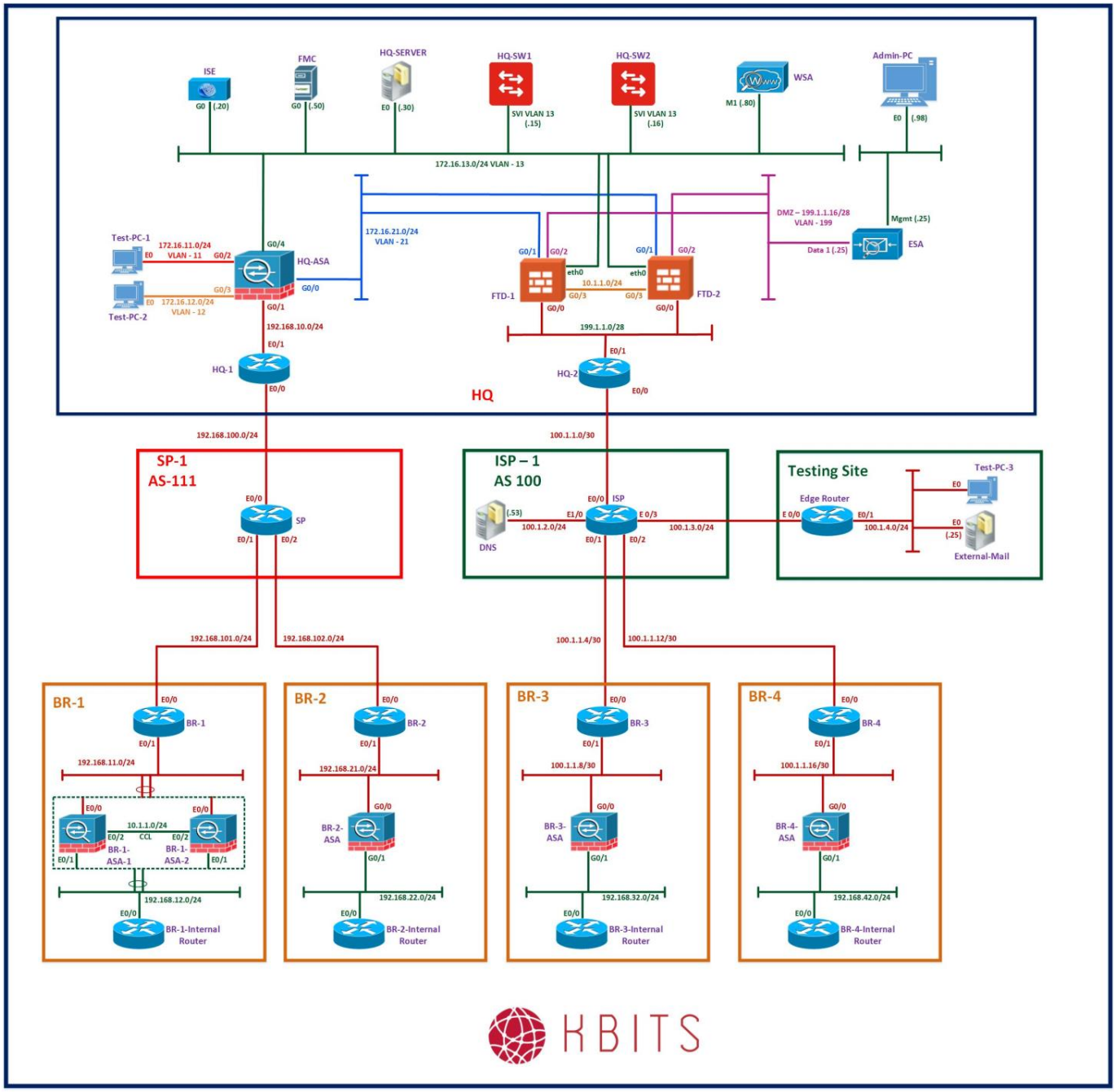
# CCIE Security v6 – Super Lab

**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

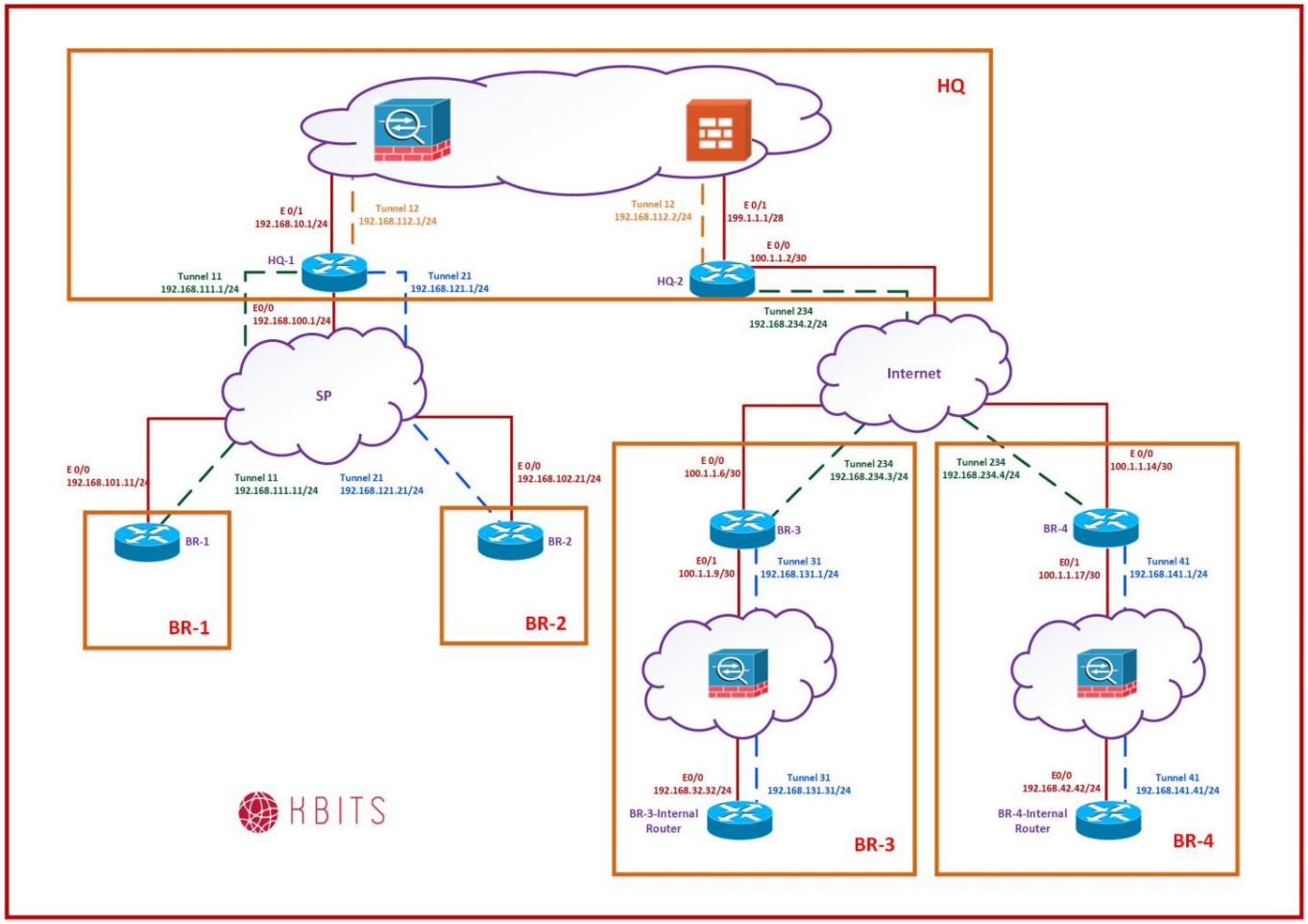
## Section 3

## Virtual Private Networks (VPNs)

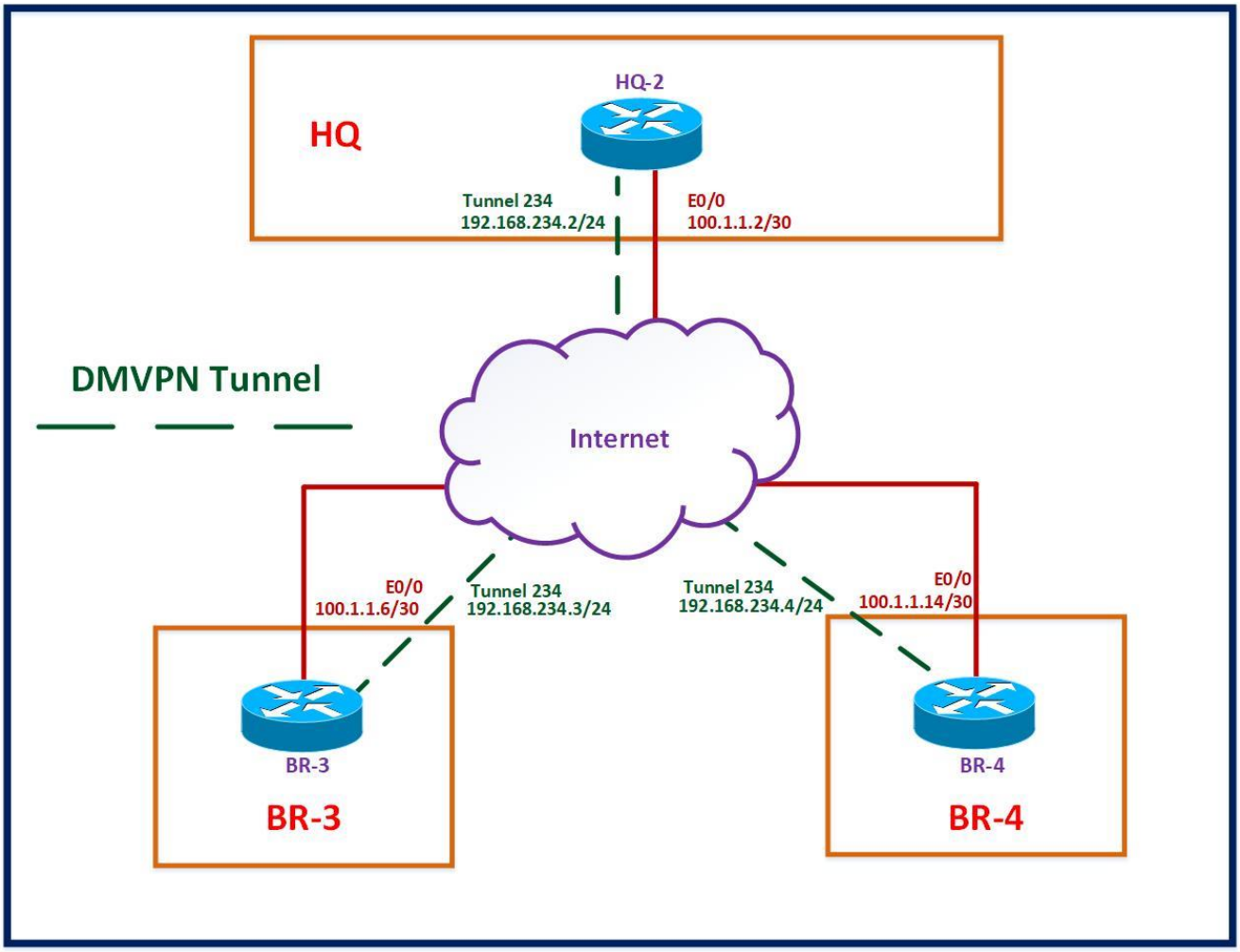
# Full Logical Topology



# Full VPN Topology



# Lab 1 – Configuring DMVPN



## Task 1 – Configure a DMVPN between HQ-2, BR-3 & BR-4

- Configure HQ-2 as NHS for a DMVPN tunnel to connect HQ-2, BR-3 and BR-4 Sites.
- Run EIGRP 12353 as the Routing Protocol in the Tunnel.
- Use the following parameters for the DMVPN Setup:
  - NHRP Network-ID: 234
  - NHRP Authenticatino: Kbits@123
  - Tunnel Network: 192.168.234.0/24

## Task 2 – Configure the tunnel for DMVPN Phase III

- Configure DMVPN Phase III to allow direct spoke to spoke communications.

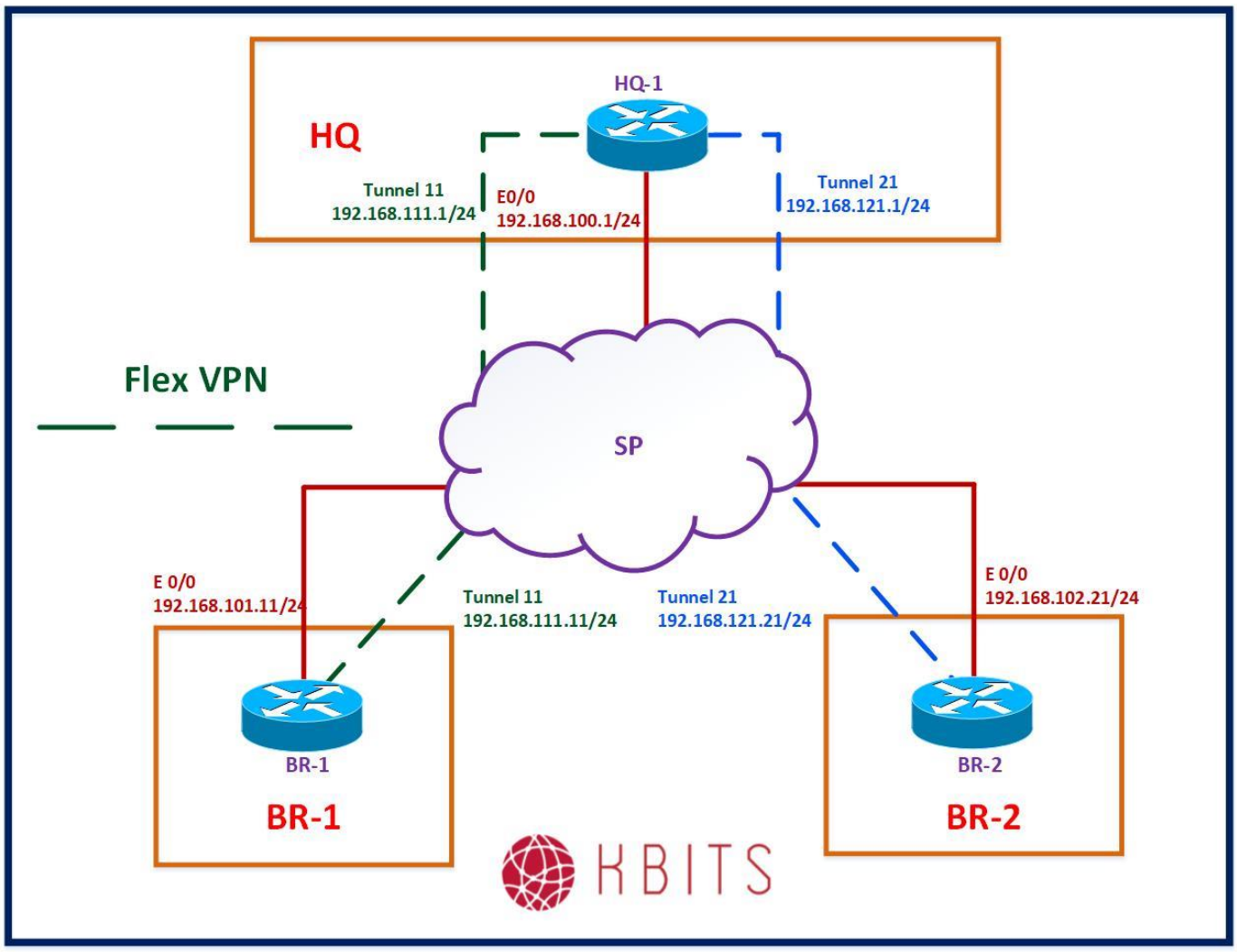
## Task 3 – Configure HQ-2 as a CA Server

- Configure HQ-2 as a CA Server using the following parameters:
  - RSA Key Label: KBITS-CA
  - Size: 1024
  - Grant: Auto
  - Issuer Information:
    - Name: KBITS CA Server
    - Location: Dubai
    - Country: AE

## Task 4 – Configure IPSec to Encrypt the Tunnel

- Configure IPSec based on the parameters below to encrypt the traffic on the DMVPN Tunnel
  - IKEv1: RSA-Sig, Group-2, Hash-MD5, Encryption–3DES
  - Pre-shared-key: Kbits@123
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Optimize the IPSec Header by eliminating any duplication in the header.
  - Interesting Traffic: All Traffic on the Tunnel

# Lab 2 – Configure a Flex VPN Tunnel Using D-VTI / S-VTI



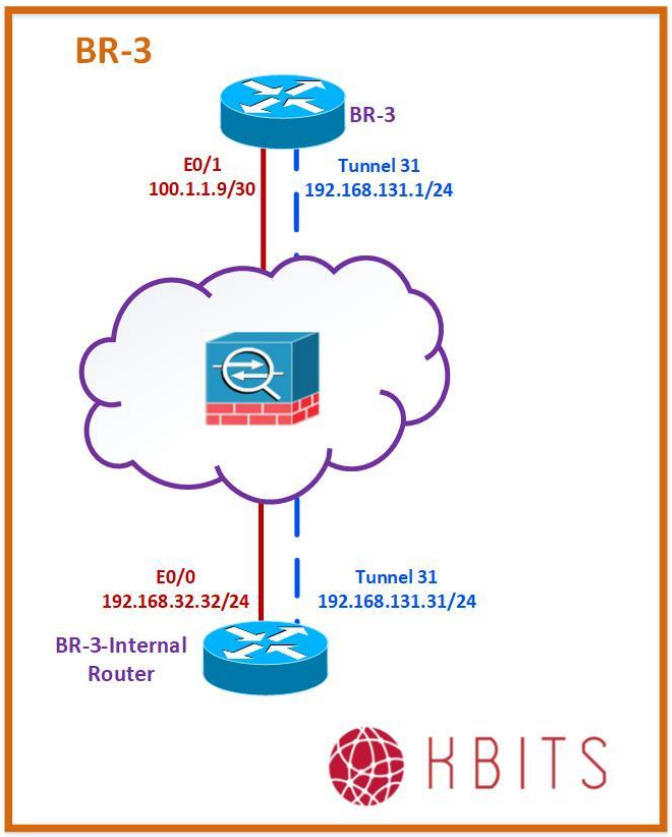
## Task 1 – Configure a Flex VPN tunnel between HQ-1 & BR-2

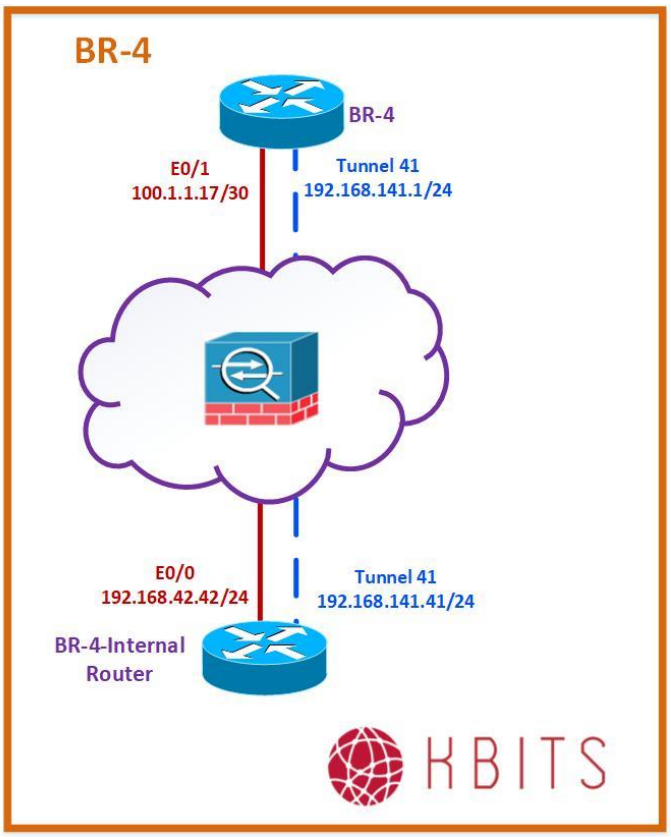
- Configure a tunnel interface to connect HQ-1 & BR-2.
- Configure IPSec based on the parameters below to encrypt the traffic between the 2 VPN Routers:
  - IKEv2 Profile: Group-2, Hash-SHA-256, Encryption–3DES
  - IKEv2 Key: Kbit@123
  - IKEv2 Profile: Authentication – Pre-Shared
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Tunnel Source: E 0/0
  - Interesting Traffic: All Traffic on the Tunnel
  - Tunnel IP's
    - HQ-1 – 192.168.121.1/24
    - BR-1 – 192.168.121.21/24
- Run EIGRP 12353 as the Routing Protocol in the Tunnel.

## Task 2 – Configure a Flex VPN tunnel between HQ-1 & BR-1

- Configure a tunnel interface to connect HQ-1 & BR-1.
- HQ-1 cannot configure an IP Address to point to BR-1.
- Configure IPSec based on the parameters below to encrypt the traffic between the 2 VPN Routers:
  - IKEv2 Profile: Group-2, Hash-SHA-256, Encryption–3DES
  - IKEv2 Key: Kbit@123
  - IKEv2 Profile: Authentication – Pre-Shared
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Tunnel Source: E 0/0
  - Interesting Traffic: All Traffic on the Tunnel
  - Tunnel IP's
    - HQ-1 – 192.168.111.1/24
    - BR-1 – 192.168.111.11/24
- Run EIGRP 12353 as the Routing Protocol in the Tunnel.

# Lab 3 – Configure a S-VTI Tunnel thru an ASA Firewall



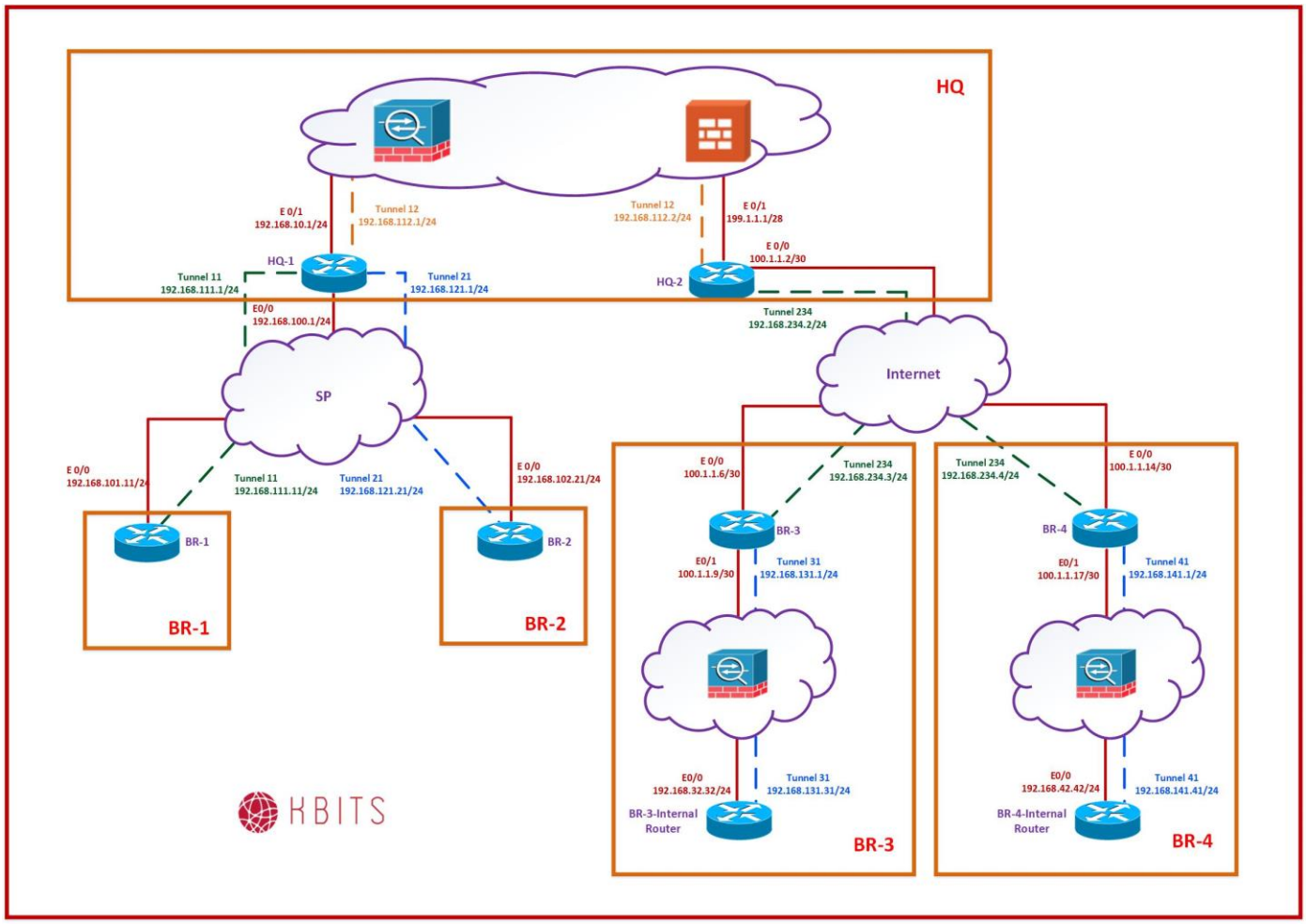
## Task 1 – Configure a Native IPSec VPN tunnel between BR-3 & BR-3-Internal Routers

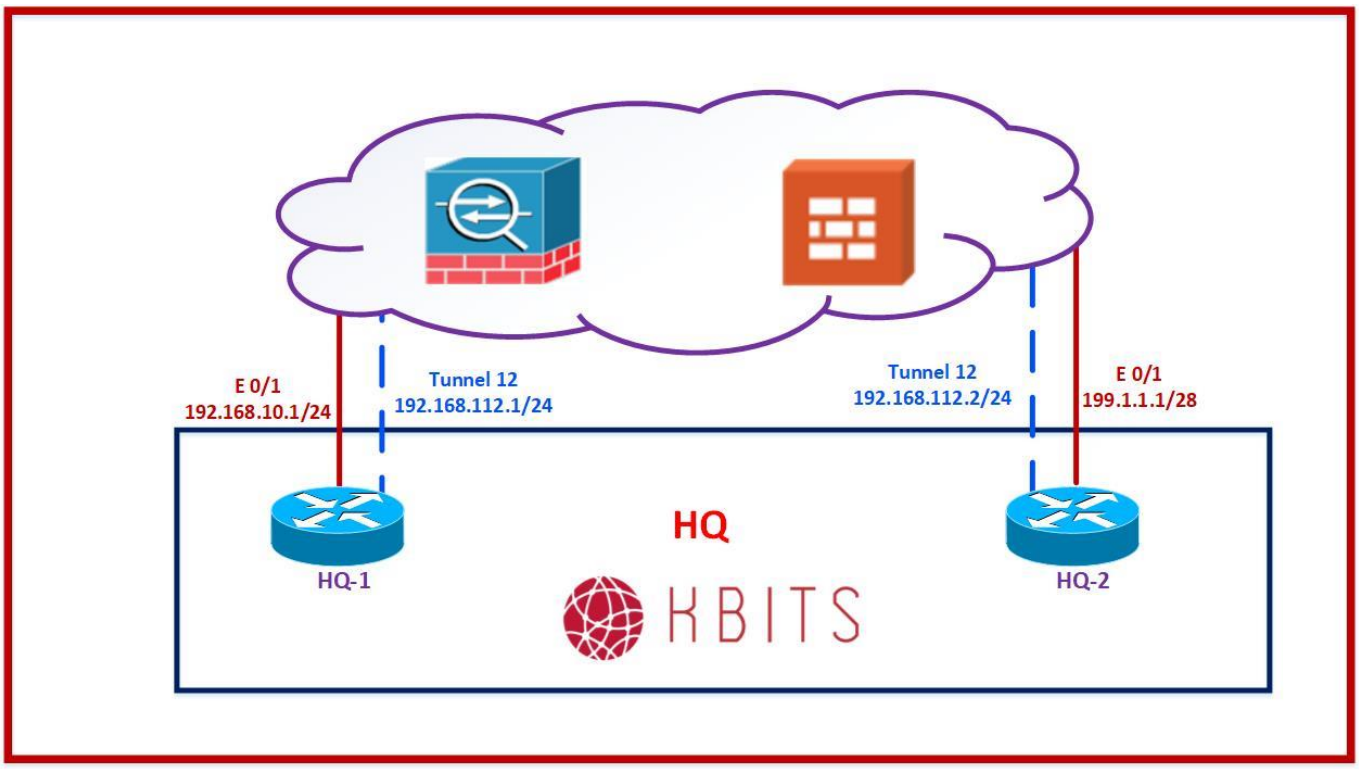
- Configure a tunnel interface to connect BR-3 to BR-3-Internal Routers using a Native IPSec Tunnel Interface.
- Configure IPSec based on the parameters below to encrypt the traffic between the 2 VPN Routers:
  - ISAKMP Parameters: Group-2, Hash-SHA, Encryption–3DES
  - ISAKMP Key: Kbit@123
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Tunnel Source: Based on the appropriate outgoing interface.
  - Interesting Traffic: All Traffic on the Tunnel
  - Routing Protocol:
    - EIGRP 12353
    - Enable the Tunnel Interface and Loopbacks on BR-3-Internal Router in EIGRP.
- Configure the ASA Firewall to allow the tunnel to form.
- You are allowed to create static routes for this task.

## Task 2 – Configure a Native IPSec VPN tunnel between BR-4 & BR-4-Internal Routers

- Configure a tunnel interface to connect BR-4 to BR-4-Internal Routers using a Native IPSec Tunnel Interface.
- Configure IPSec based on the parameters below to encrypt the traffic between the 2 VPN Routers:
  - ISAKMP Parameters: Group-2, Hash-SHA, Encryption–3DES
  - ISAKMP Key: Kbit@123
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Tunnel Source: Based on the appropriate outgoing interface.
  - Interesting Traffic: All Traffic on the Tunnel
  - Routing Protocol:
    - EIGRP 12353
    - Enable the Tunnel Interface and Loopbacks on BR-4-Internal Router in EIGRP.
- Configure the ASA Firewall to allow the tunnel to form.
- You are allowed to create static routes for this task.

# Lab 4 – Configure a VPN to connect all Sites to each other





## Task 1 – Configure a GRE Over IPSec VPN tunnel between HQ-1 & HQ-2 Routers

- Configure a tunnel interface to connect HQ-1 to HQ-2 Routers using a GRE Tunnel Interface.
- Configure IPSec to encrypt all traffic traversing the Tunnel Interface based on the parameters below:
  - ISAKMP Parameters: Group-2, Hash-SHA, Encryption–3DES
  - ISAKMP Key: Kbit@123
  - IPSec Parameters: ESP-3DES, ESP-SHA-HMAC
  - Tunnel Source: Based on the appropriate outgoing interface.
  - Interesting Traffic: All Traffic on the Tunnel
  - Routing Protocol:
    - EIGRP 12353
    - Enable the Tunnel Interfaces.
- Configure the ASA & FTD Firewalls to allow the tunnel to form.

## Task 2 – Configure Route Redistribution on HQ-1

- Configure Route Redistribution on HQ-1 to redistribute EIGRP routes into OSPF.
- Configure Route Redistribution on HQ-1 to redistribute OSPF routes into EIGRP.
- Only redistribute the 172.25.0.0/16 routes between EIGRP & OSPF.

## Task 3 – Verification

- Verify reachability between BR-1, BR-2, BR-3 & BR-4 by using the 172.25.X.X networks.

# CCIE Security v6 – Super Lab

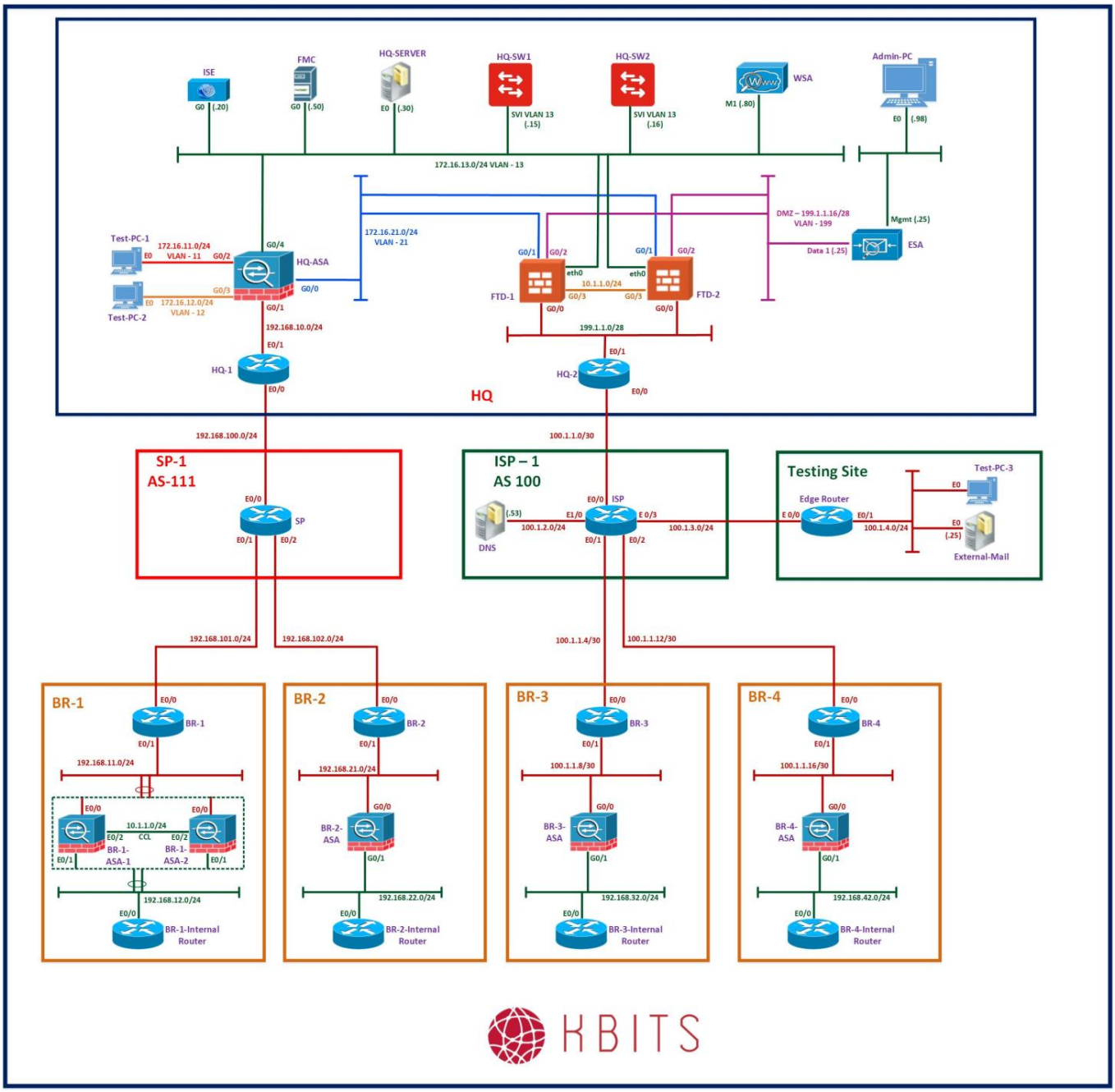
**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

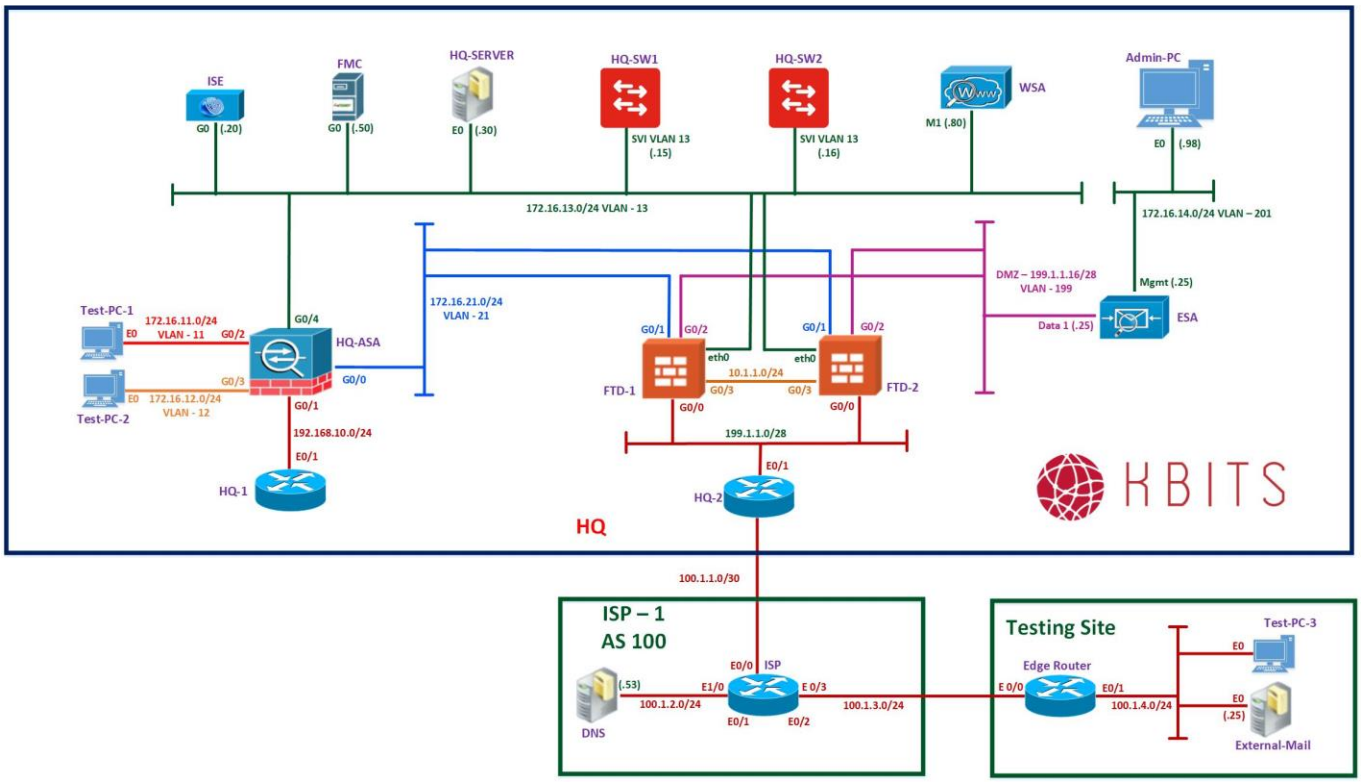
## Section 4

## Content Filtering – WSA – ESA

# Lab 1 – Configuring ESA for E-Mail Forwarding

## Full Logical Topology





## Task 1 – Initialize the ESA – CLI

Initialize the ESA from the CLI using the following parameters:

- Management Interface configuration:
  - Name: **MgmtData**
  - IP Address: **172.16.14.25/24**
  - Hostname: **MGMT.KBITS.LIVE**
  - Protocols: **SSH, FTP, HTTP & HTTPS**
- Rest of the Parameters: **Default**

## Task 2 – Initialize the ESA – GUI

Configure the ESA Networking with the following Parameters:

- System Configuration:
  - System Name: **ESA.Kbits.live**
  - Alert E-Mail: **kb@kbits.live**
  - Administrator Passphrase: **Kbits@123**

- Network Integration:
  - IPv4 Default Gatway: **199.1.1.30**
  - DNS Server: **100.1.2.53**

- Interface Configuration – Data 1:
  - Data1: **Enabled**
  - Name: **Internet**
  - IP Address: **199.1.1.25/28**
  - Hostname: **esa.Kbits.live**
  - Accept Incoming E-Mail: **Checked**
    - Domain: **Kbits.live**
    - Destination: **172.16.13.30**

### Task 3 – Configure Mail Flow Policy

Configure a Mail Flow Policy for Relaying messages on the ESA using the following parameters:

- Mail Flow Policy
  - Policy Name: **RELAYED**
  - Connection behavior: **Relay**
  - Remaing Parameters: **Use Default**

### Task 4 – Configure a Sender Group

Configure a Sender Group to use the Mail Flow Policy created in the previous task for the Mail Server for Kbits.live:

- HAT
  - Policy Name: **RELAY LIST**
  - Order: **1**
  - Policy: **RELAYED**
  - Send Group: **172.16.13.30**

### Task 5 – Configure access to the ESA

Allow SMTP Access to ESA from Outside. ESA should be able to communicate to any device outside the FTD.

### Task 6 – Configure access to the E-Mail Server

Allow SMTP access to the HQ-SERVER from the ESA thru the HQ-ASA.

## Task 7 – Verifying E-mail Access

2 Accounts for each domain are configured on the Thunderbird Client on the Mail Servers – kbits.live (HQ-Server) & Abc.com (External-Mail). We will use these accounts to send and receive Messages. **(Info Only).**

- Name: **Kbits One**
- Account: kbits1@kbits.live
- Password: Kbits@123
- Mail & SMTP Servers: mail.kbits.live

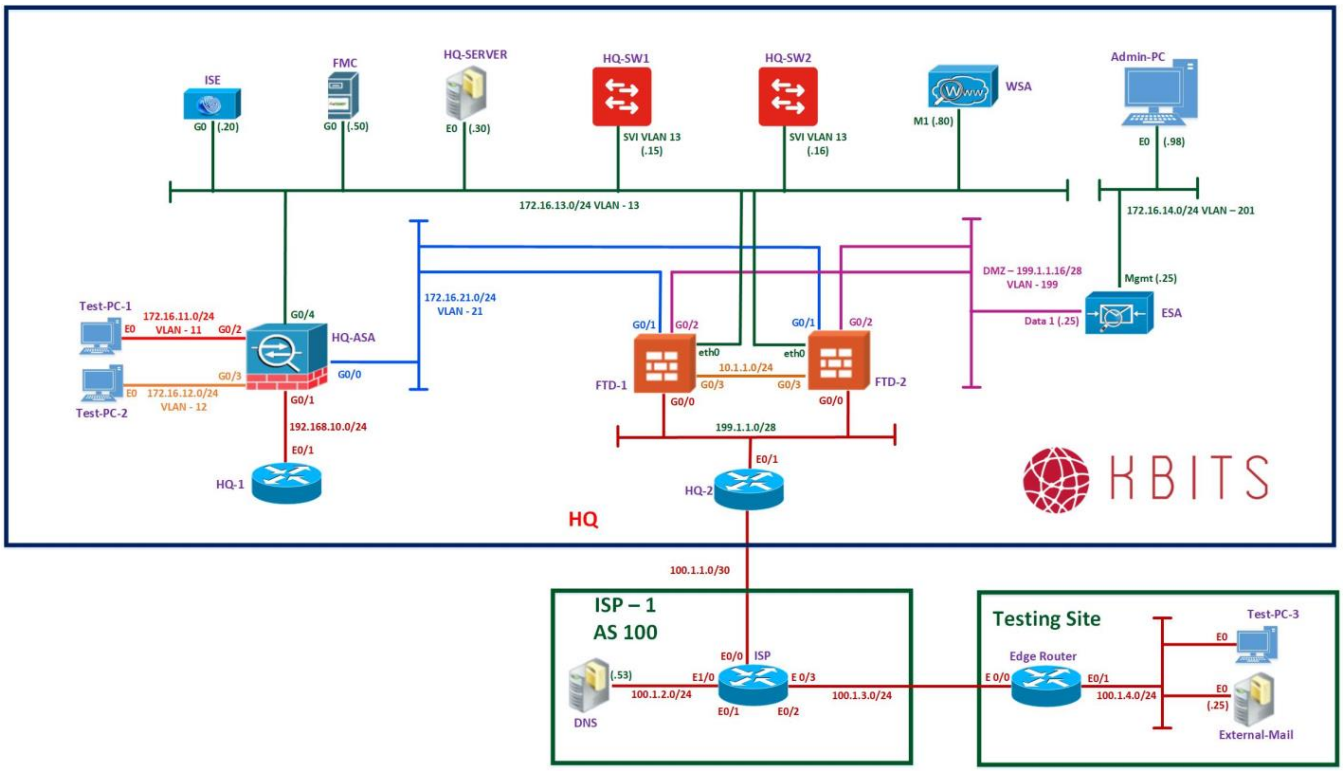
- Name: **Kbits Two**
- Account: kbits2@kbits.live
- Password: Kbits@123
- Mail & SMTP Servers: mail.kbits.live

- Name: **Abc One**
- Account: abc1@abc.com
- Password: Kbits@123
- Mail & SMTP Servers: mail.abc.com

- Name: **Abc Two**
- Account: abc2@abc.com
- Password: Kbits@123
- Mail & SMTP Servers: mail.abc.com

Verify the E-mail configuration by sending and receiving E-mail between the Users on the 2 domains using the ESA.

# Lab 2 – Configuring Content Filtering for Incoming Mail using ESA



## Task 1 – Configuring Incoming Content Filters

Configure an Incoming Content Filter that filter E-Mails based on the following parameters:

- Incoming Content Filter Name: **IC-BOMB**
  - Condition:
    - Message Body containg "**BOMB**"
  - Action:
    - **Drop**

## Task 2 – Configure an Incoming Mail Policy

Configure Incoming Mail Policies that uses the Filters created in the previous task to filter All E-Mails.

- Incoming Mail Policy Name: **IC-Mail-Policy**
  - Users:
    - Sender: **Any**
    - Recipient: **Any**
  - Content Filters:
    - **IC-BOMB**

## Task 3 – Verify the Incoming Filters

Verify the IC-BOMB filter by sending an e-mail from Abc1@abc.com to kbits1@kbits.live using the following:

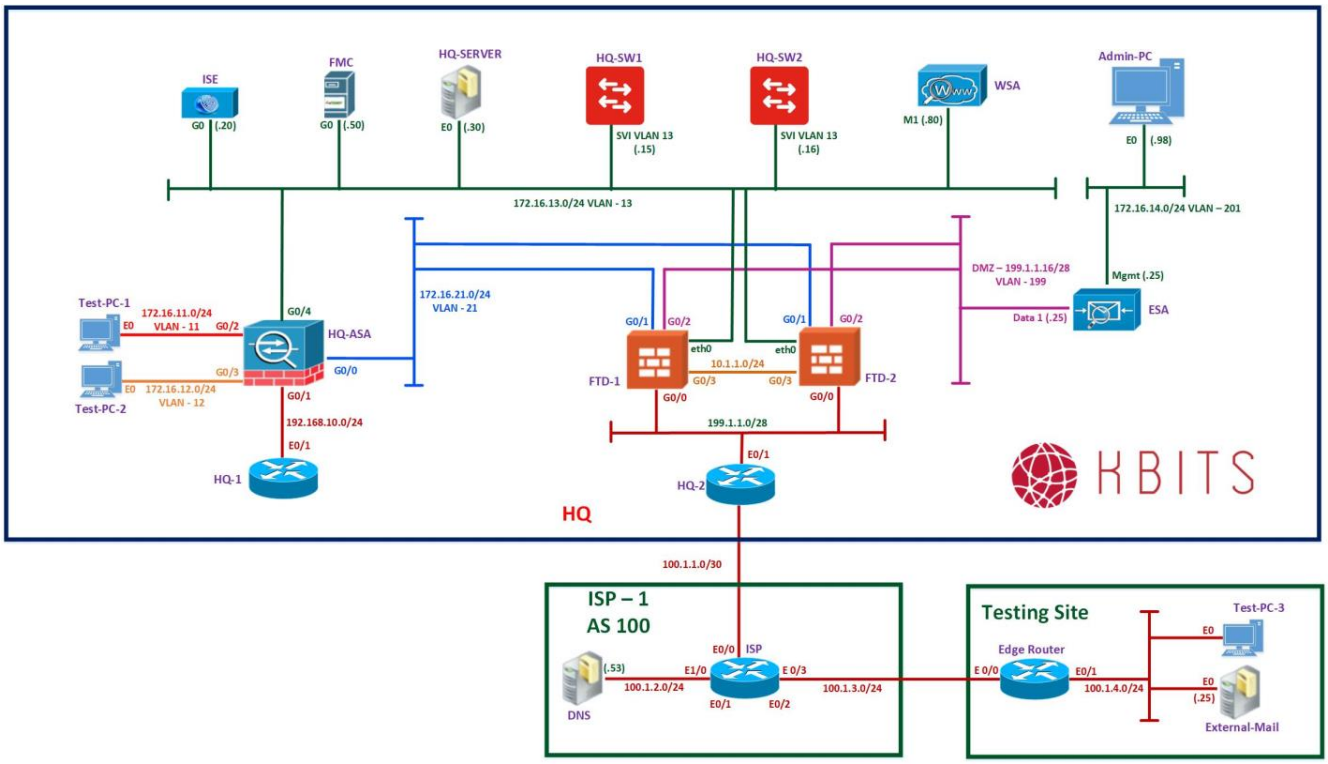
- From: **Abc1@abc.com**
- To: **kbits1@kbits.live**
- Subject: **BOOOOOOOOOOOOMB**
- Message Body:

  Hello Kbits One,

  BOMB is diffused.

  Regards
  ABC One

# Lab 3 – Configuring Content Filtering for Outgoing Filter using ESA



### Task 1 – Configuring Custom Notifications

Configure a Custom Text Notification based on the following:

- Text Resource Name: **SSN-Notification**
- Type: **Notification Template**
- Text: "**SSN should not be sent in an e-mail**"

### Task 2 – Configuring Outgoing Content Filters

Configure an Outgoing Content Filter that blocks E-Mails based on the following parameters:

- Outgoing Content Filter Name: **OG-SSN**
  - Condition:
    - Message Body contains "**Contains smart identifier**": "**SSN**"
  - Action:
    - **Notify:** Report the Message to the "**Sender**" with the "**SSN-Notifcation**" text message created in the previous task.
    - **Drop**

### Task 3 – Configure an Outgoing Mail Policy

Configure an Outgoing Mail Policy that uses the Filter created in the previous task to filter All E-Mails.

- Outgoing Mail Policy Name: **OG-Mail-Policy**
  - Users:
    - Sender: **Any**
    - Recipient: **Any**
  - Content Filters:
    - **OG-SSN**

## Task 4 – Verify the Outgoing Filters

Verify the OG-SSN filter by sending an e-mail from kbits2@kbits.live to Abc2@abc.com using the following:

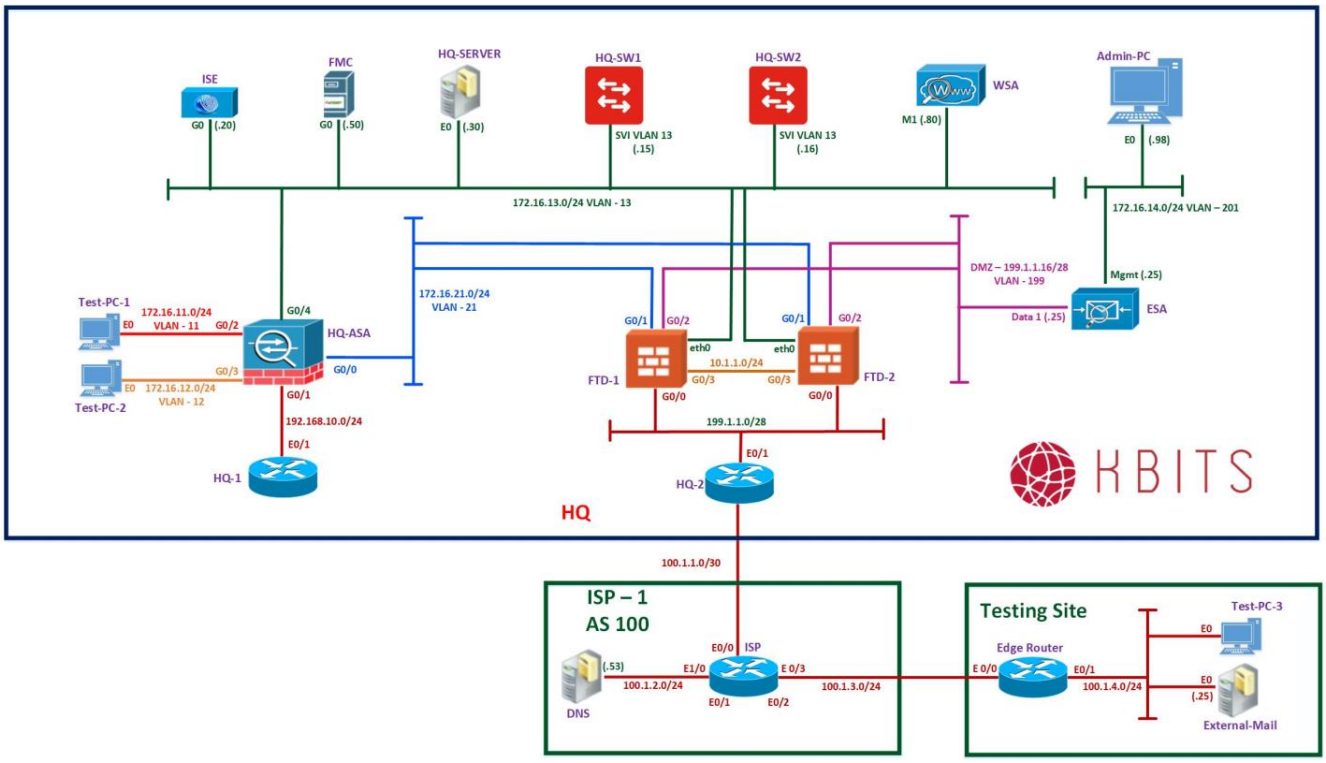
- From: **kbits2@kbits.live**
- To: **Abc2@abc.com**
- Subject: **Application Processing**
- Message Body:
-

  Hi Abc Two,

  My SSN is: 615-56-1234. Please process the application.

  Kbits Two

# Lab 4 – Configuring WSA for Web Proxy & Filtering



## Task 1 – Initializing the WSA – CLI

Initialize the WSA from the CLI using the following parameters:

- Management Interface configuration:
  - IP Address: **172.16.13.80**
  - Default Gateway: **172.16.13.10**
  - Hostname: **WSA.KBITS.LIVE**
  - Protocols: **SSH, HTTP & HTTPS**

- Rest of the Parameters: **Default**

## Task 2 – Configure the WSA from the GUI

Run the System Wizard to finalize the initial setup. Verify/Re-configure the WSA Networking with the following Parameters:

- System Configuration:
  - System Name: **WSA.Kbits.live**
  - DNS Server: **172.16.13.30**
  - NTP Server: **Delete and leave it blank**

- Network Content:
  - Proxy Server: **No**

- Network Interfaces & Wiring:
  - M1 IP: **172.16.13.80/24**
  - M1 Hostname: **wsa.kbits.live**

- L4 Traffic Monitor:
  - **Take the default**

- IPv4 Routes for Management:
  - Default Gateway: **172.16.13.10**

- Transparent Connection Settings:
  - **Take the default**

- Administrative Settings:
  - Admin Password: **Kbits@123**

- System Alerts E-mail: Khawarb@kbits.live
- SMTP Server: **199.1.1.25**

- Security Settings:
  - **Take the defaults**

### Task 3 – Configure WCCP between the HQ-ASA & WSA

Configure WCCP Transparent Redirection on the WSA based on the following parameters:

- Service Profile Name: **HQ-ASA**
- Dynamic Service ID: **55**
- Port Numbers: **80**
- Router IP Address: **172.16.13.10**
- Password: **cisco**

### Task 4 – Configure WSA on the HQ-ASA

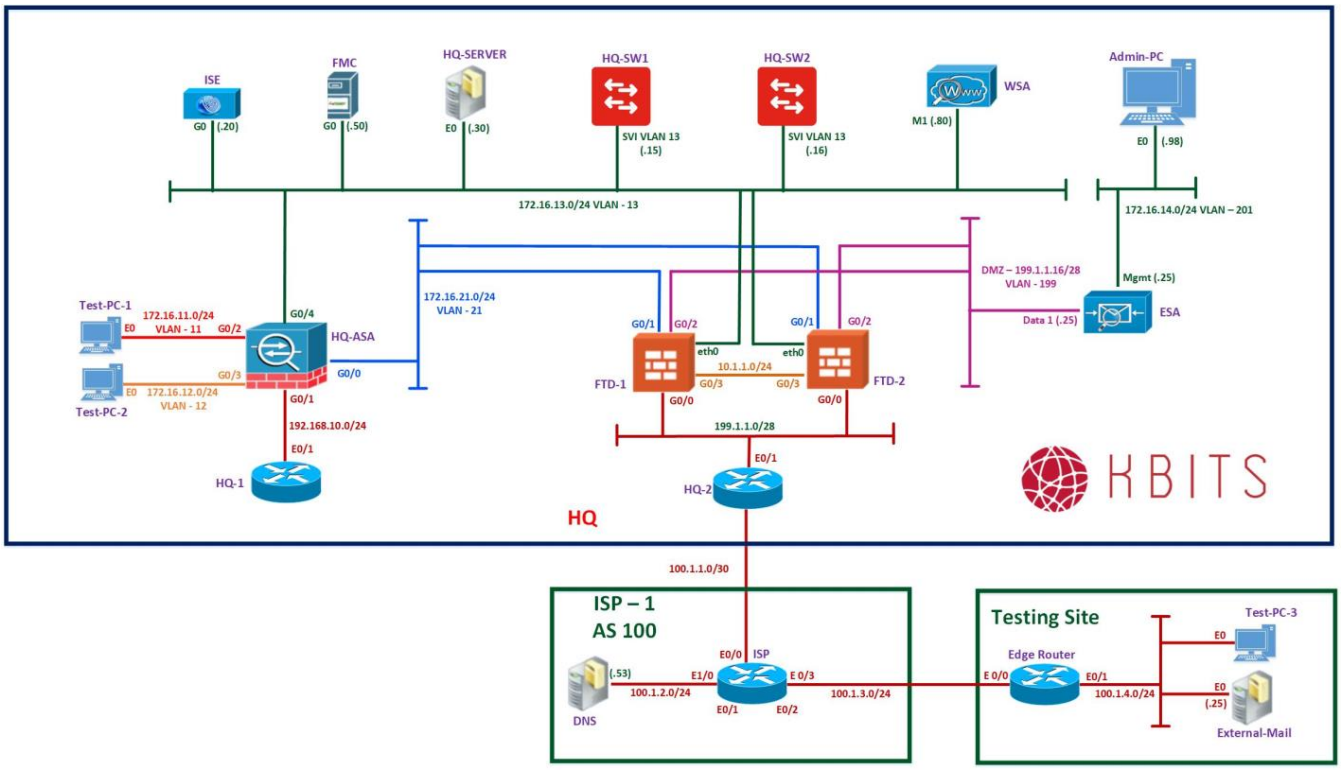
Configure WCCP on HQ-ASA based on the following parameters:

- WSA IP Address: **172.16.13.80**
- Traffic flow ACL: permit tcp any any eq 80
- Dynamic Service ID: **55**
- Password: **cisco**
- Redirection Interfaces: **G 0/4 & G 0/3**

### Task 5 – Verify the WSA & HQ-ASA Redirection

Verify you can browse to www.cnn.com or www.espn.com from the HQ-Server

# Lab 5 – Configuring URL Filtering on the WSA



### Task 1 – Configure Identities

Configure the following Identities on the WSA:

- Name: **Employees**
- Subnet: **172.16.11.0/24 & 172.16.13.0/24**

### Task 2 – Create an Access Policy

Configure an Access Policy called **EMP Policy** to Block the following websites categories:

- Adult
- Gambling
- Pornography
- Social Networking
- Sports & recreation

### Task 3 – Configure Custom URLs

Configure Custom URLs based on the following:

- Name: **Allow List**
  - URLs: www.espn.com, .espn.com
- Name: **Deny List**
  - URLs: www.cnn.com, .cnn.com

### Task 4 – Configure Custom URLs

Configure **EMP Policy** access policy to include the 2 Custom Categories in the policy. The Action for the **Allow List** should be to **Allow** and for the **Deny List** should be to **block**.

### Task 5 – Configure Custom URLs

Verify you can browse to www.espn.com from both of the PC's. Verify you cannot browse to www.cnn.com from the either of the PC's.

# CCIE Security v6 – Super Lab

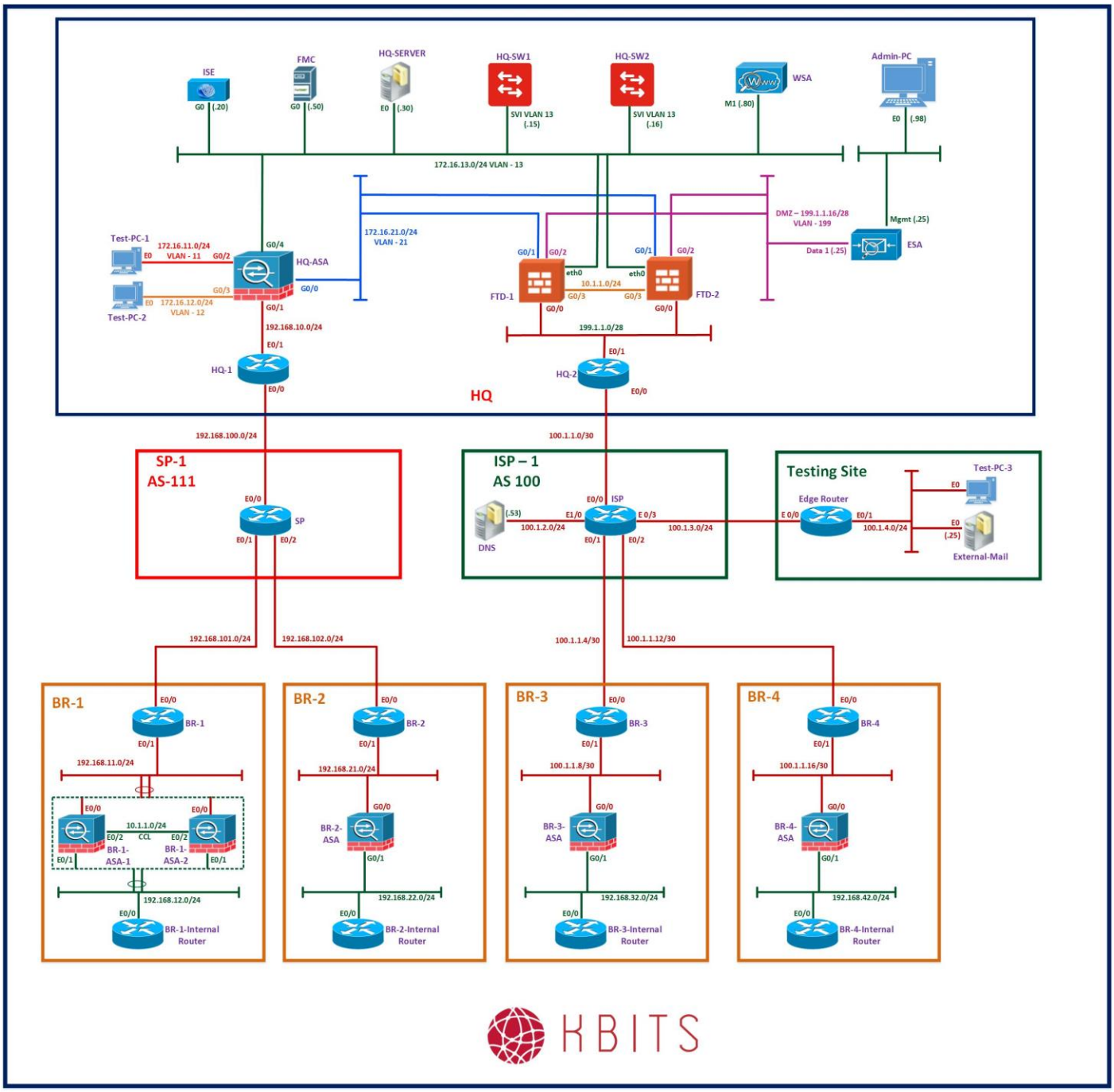
**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

## Section 5

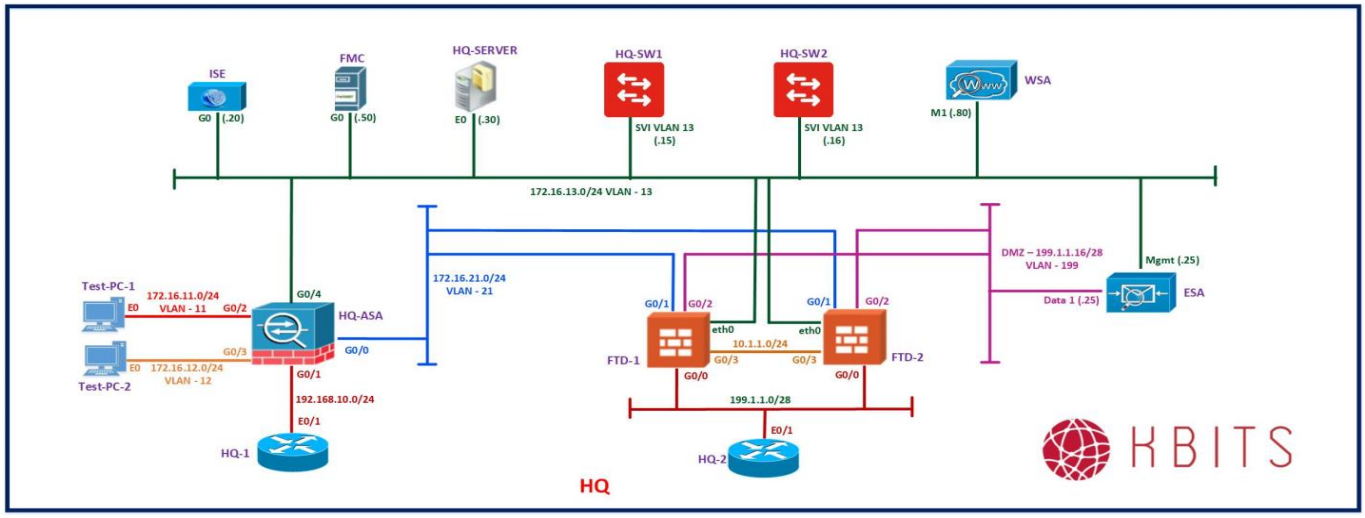
## Router & Switch Security

# Lab 1 – Configuring Layer 2 Security

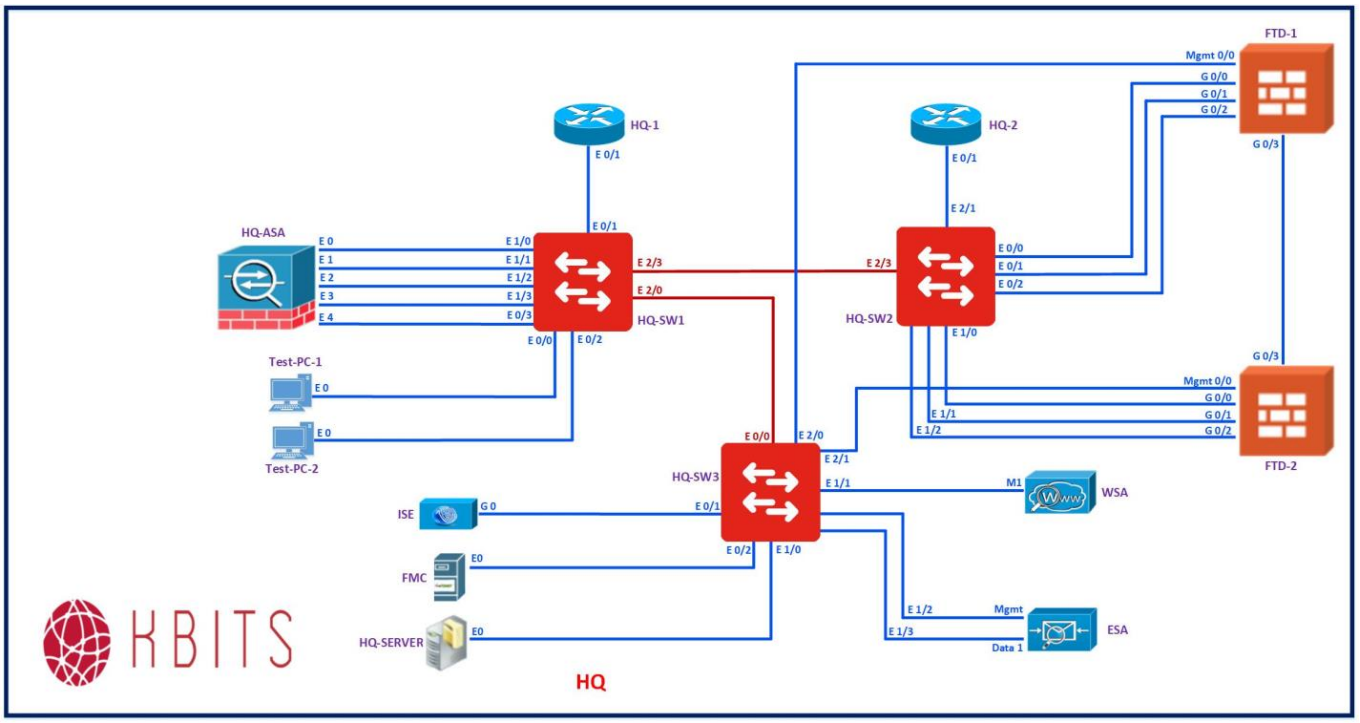
## Full Logical Topology



## HQ - Logical




## HQ – Layer 2 (Physical)



### Task 1 – Configure DHCP Snooping for VLAN 13

The DHCP server resides on HQ-Server. It is connected on port **E 1/0** on **HQ-SW3**. It is Make sure that VLAN 13 receives IP Configuration only from this DHCP Server.

### Task 2 – Configure MAC-To-Port Bindings – Static

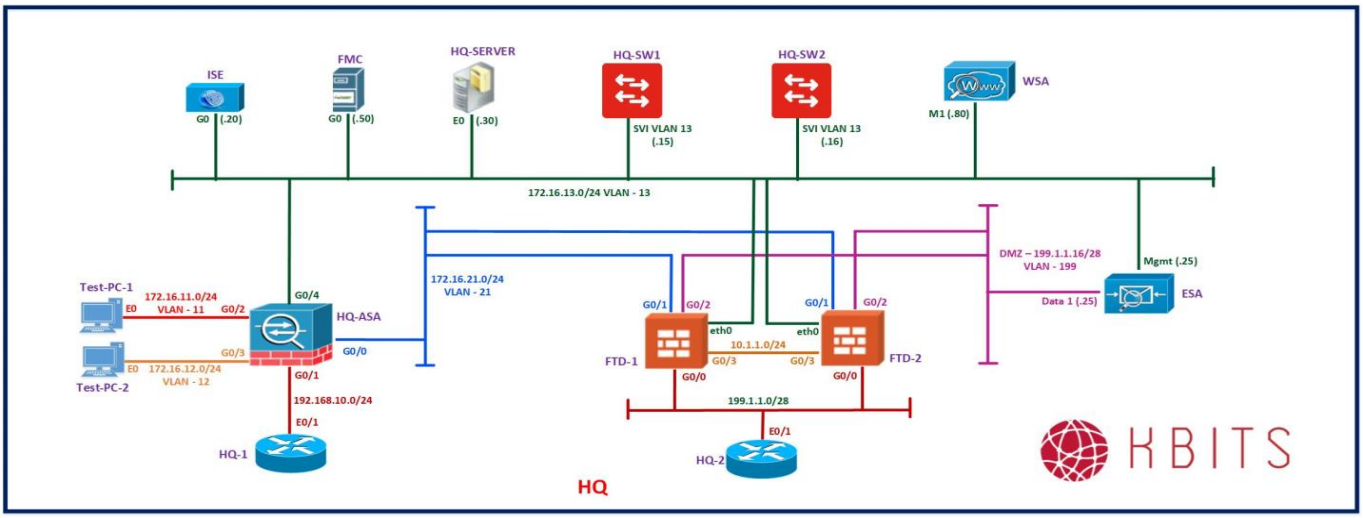
Make sure that only HQ-Server's MAC is allowed to connect on port **E 1/0** on **HQ-SW3**. This needs to be done statically.

### Task 3 – Configure MAC-To-Port Bindings – Dynamic

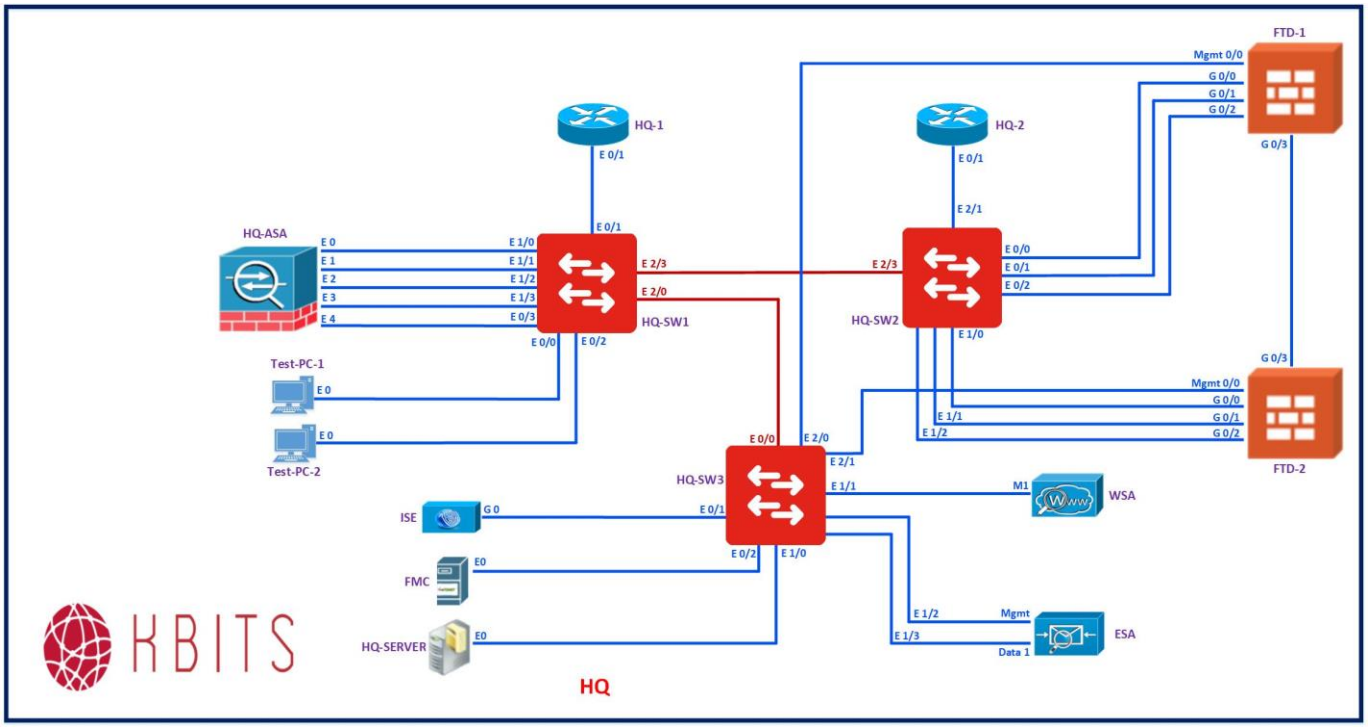
Make sure that only ISE's MAC is allowed to connect on port **E 0/1** on **HQ-SW3**. This needs to be done dynamically. The MAC address should show up in the Running Config.

# Lab 2 – Configuring Security Features on Routers

## HQ - Logical




## HQ – Layer 2 (Physical)



### Task 1 – Configure Anti-Spoofing ACL on HQ-2

Block any RFC 1918 address coming into HQ-2 from the Internet.

### Task 2 – Configure uRPF on HQ-2

Use Strict RPF to prevent IP spoofing using network addresses from the internal networks. The route could use the default gateway to check for the source address. Also make sure all packets that are failing the RPF check get logged.

# CCIE Security v6 – Super Lab

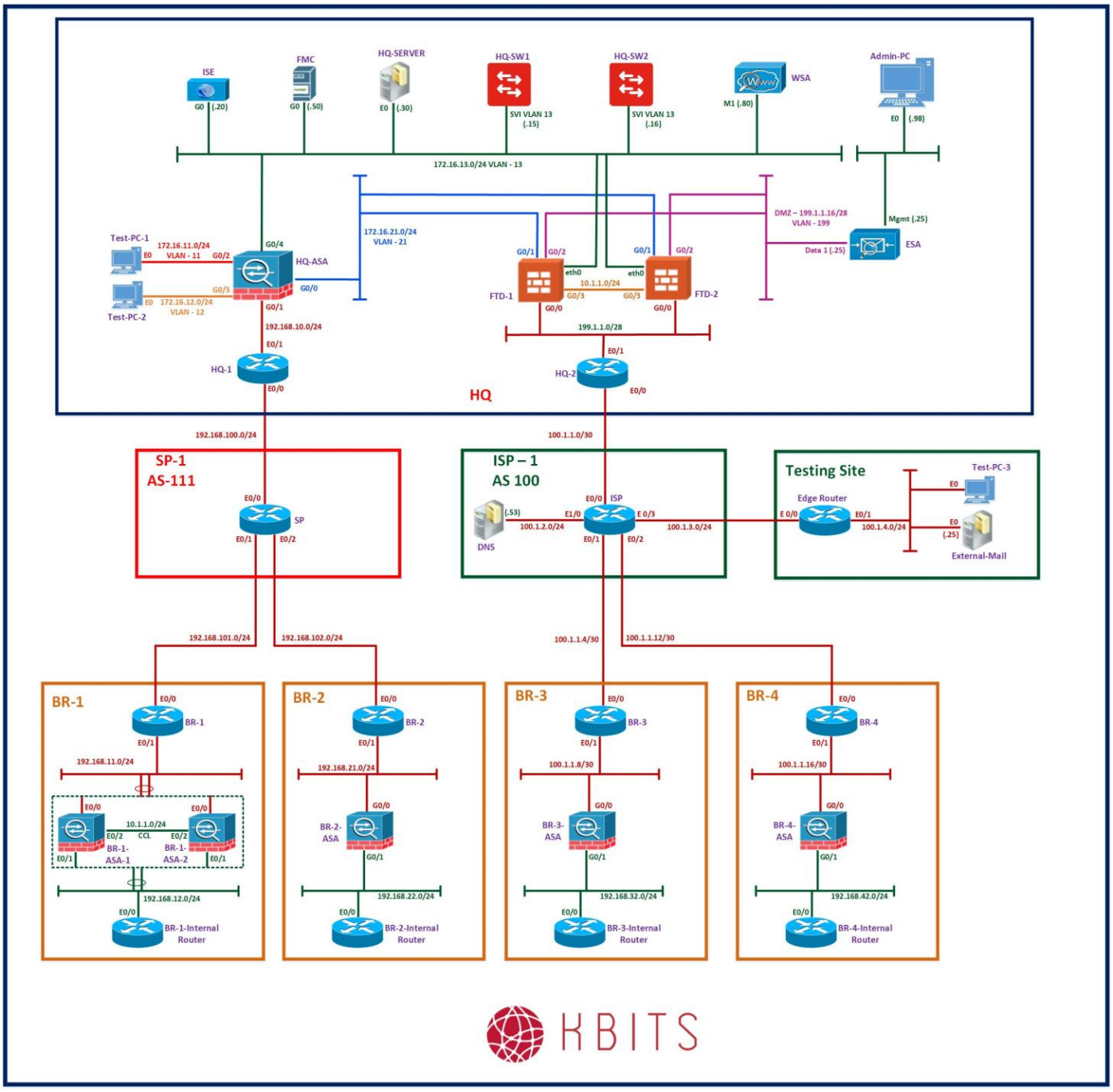
**Khawar Butt**
**CCIE # 12353**
**Hepta CCIE#12353**
**CCDE # 20110020**

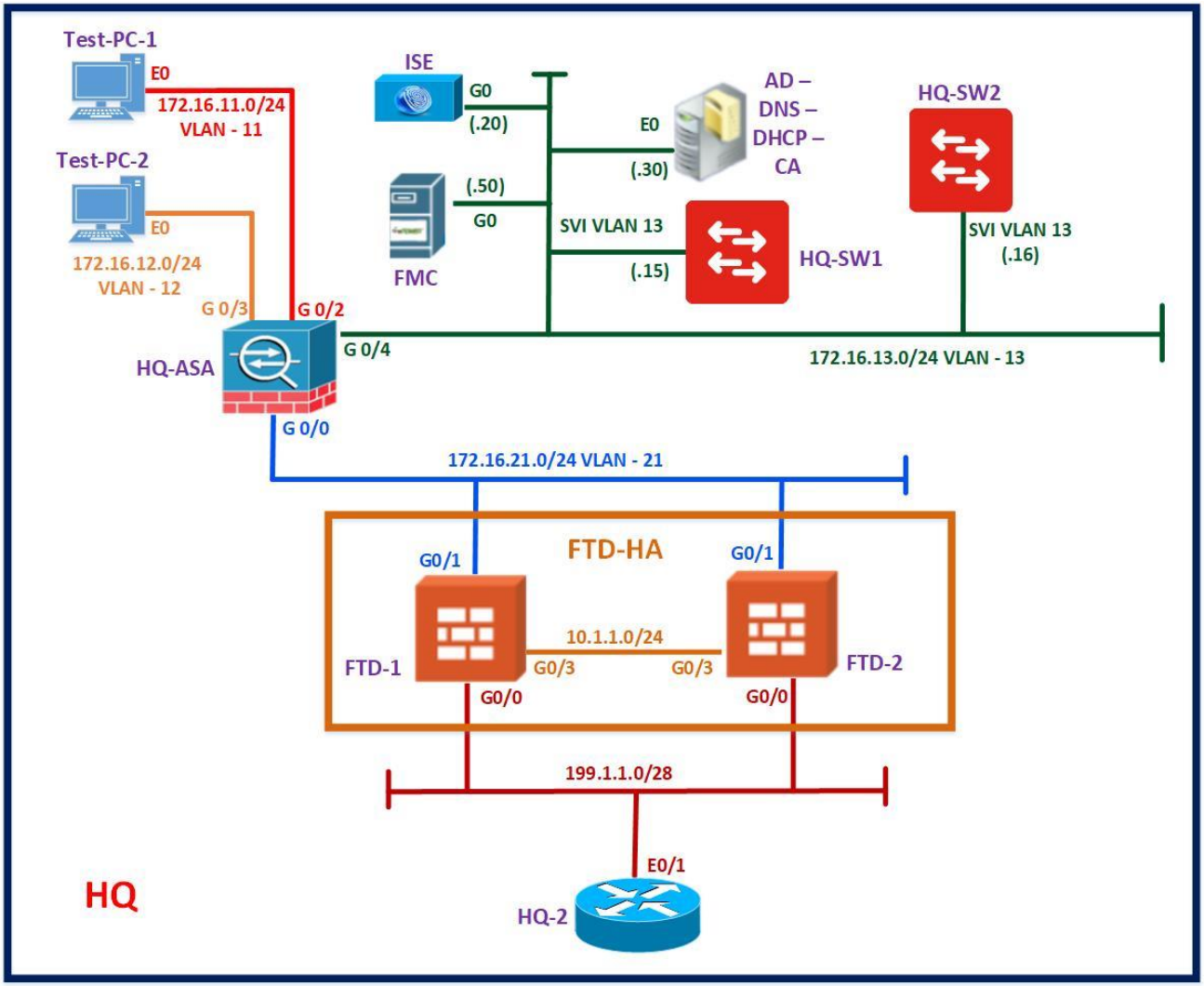
## Section 6

## Identity Services Engine (ISE)

# Lab 1 – Initializing ISE and Adding Network Devices

## Full Logical Topology





## Task 1 – Configuring RADIUS Settings

- Configure ISE RADIUS setting to allow repeated Failures & suppress failied atempts. This is done to see the logs as we are testing configurations.
- Configure ISE RADIUS to display all Successful authentications in the log even if they are repeated. This is done to see the logs as we are testing configurations.

## Task 2 – Enabling Services

- Configure ISE to run the Device Administration services.
- We will be using TACACS+ for Device Administration in a later section.

## Task 3 – Trust the CA Server Certificate

- Configure ISE to trust the Enterprise CA Certificate

## Task 4 – Configure Network Device Groups on ISE

- Configure Network Device Groups for Switches, Routers and Firewalls based on the following:

  - Name: **Switches**
  - Parent: All Device Types

  - Name: **Routers**
  - Parent: All Device Types

## Task 5 – Configure the Switches

- Configure the Switches based on the following parameters:

  - Name: **HQ-SW1**
  - IP Address: **172.16.13.15/32**
  - Device Type: **Switches**
  - RADIUS: **Checked**
  - RADIUS Secret Password: **Kbits@123**
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Kbits@123**

  - Name: **HQ-SW2**
  - IP Address: **172.16.13.16/32**
  - Device Type: **Switches**

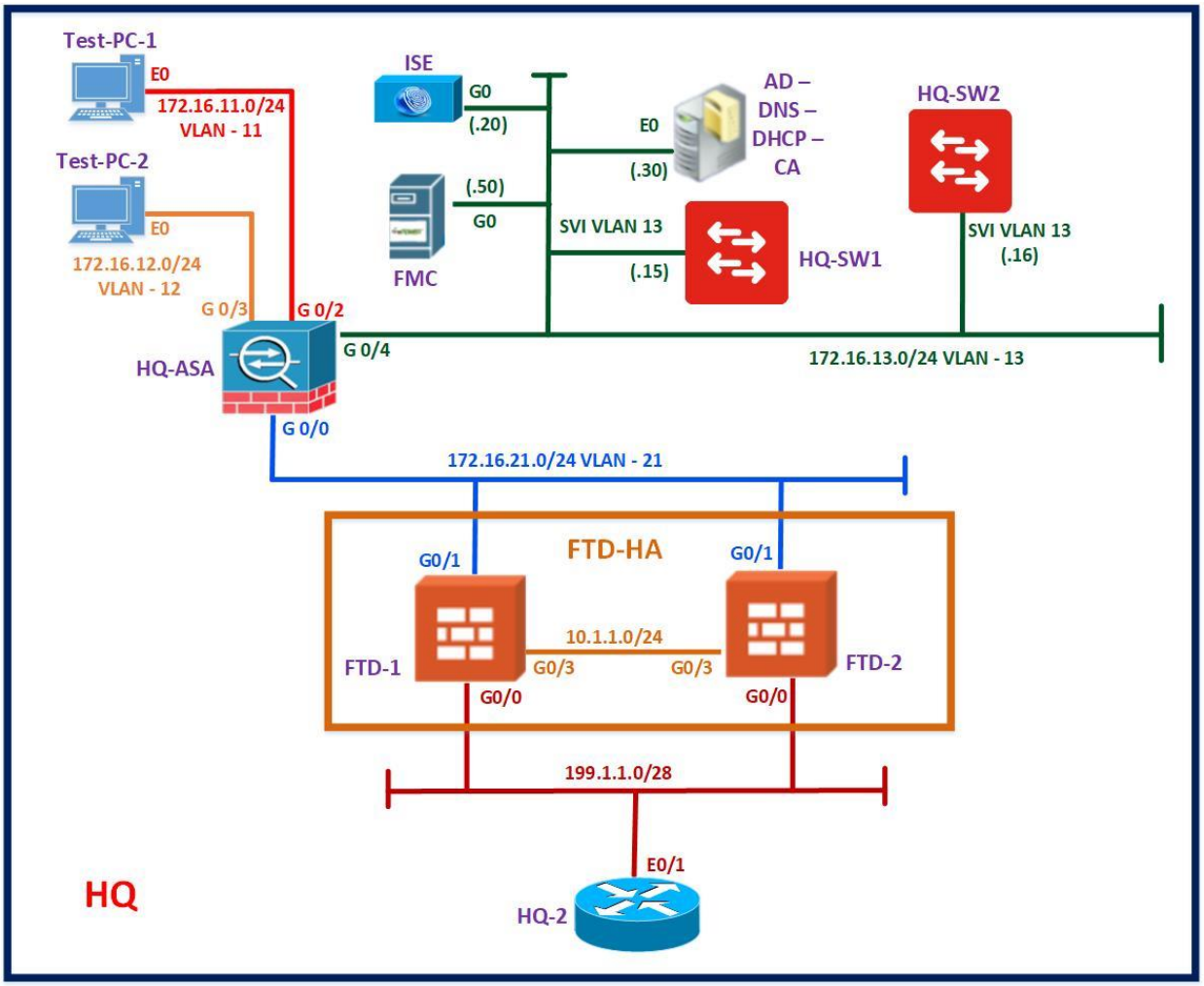
- RADIUS: **Checked**
- RADIUS Secret Password: **Kbits@123**
- TACACS+: **Checked**
- TACACS+ Secret Password: **Kbits@123**

## Task 6 – Configure the Routers

- Configure the Routers based on the following parameters:

  - Name: **HQ-2**
  - IP Address: **199.1.1.1/32**
  - Device Type: **Routers**
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Kbits@123**

# Lab 2 – Configuring Groups & Users in ISE



## Task 1 – Configure User Identity Groups in ISE

- Configure the following Groups on ISE. They will be used for grouping local Identities.

  ➔ Name: **ISE-Employees**

  ➔ Name: **ISE-Consultants**

  ➔ Name: **SuperAdmins**

  ➔ Name: **RP-Admins**

  ➔ Name: **Switching-Admins**

## Task 2 – Configure Users on ISE & Assign them to the appropriate Groups

- Configure the Users & Assign them to the groups created in the previous task based on the following. They will be used for Local ISE-based authentications.

  ➔ Name: **ISE-1**
  ➔ Password: **Kbits@123**
  ➔ Group: **ISE-Employees**

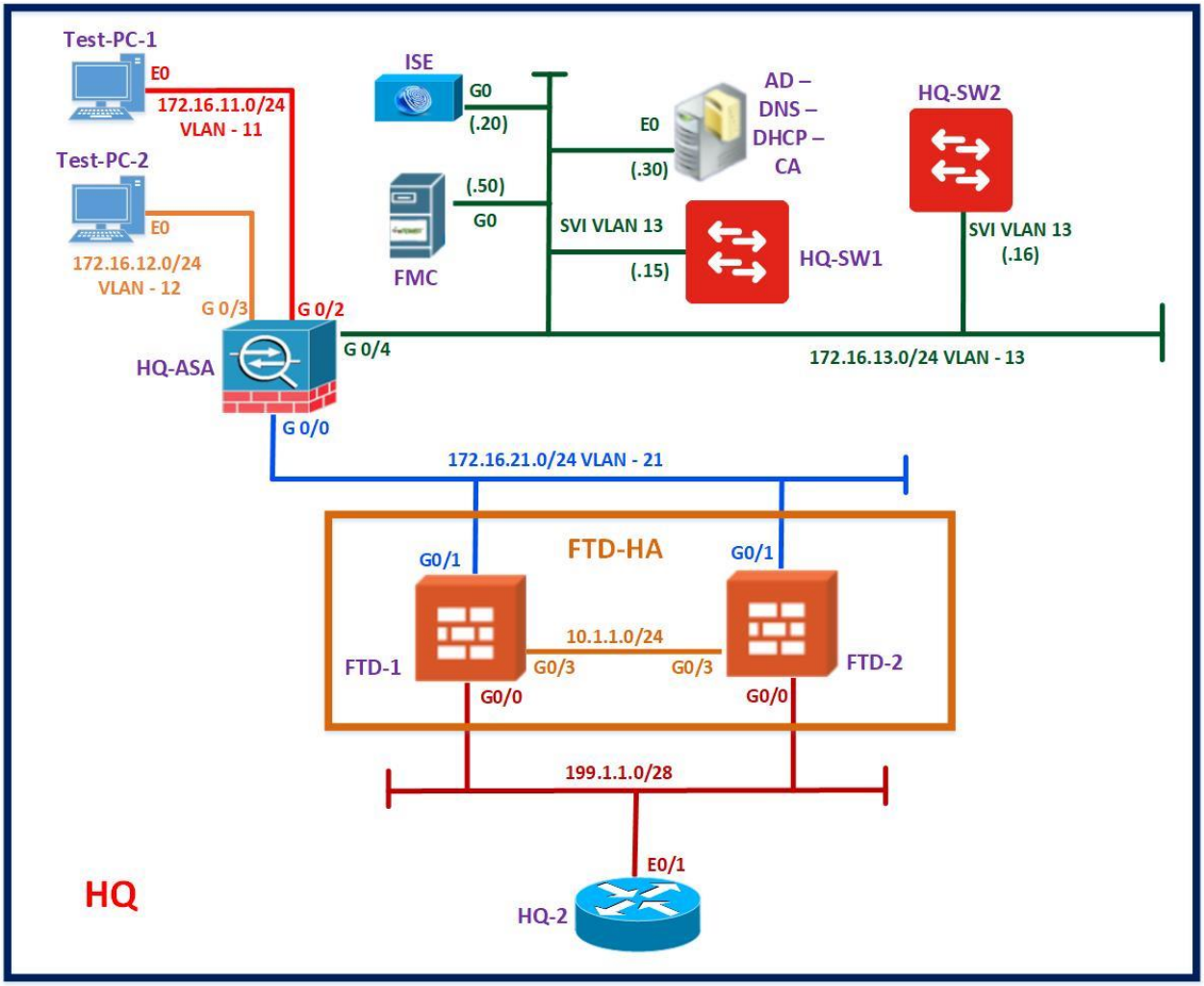
  ➔ Name: **ISE-2**
  ➔ Password: **Kbits@123**
  ➔ Group: **ISE-Consultants**

  ➔ Name: **Admin1**
  ➔ Password: **Kbits@123**
  ➔ Group: **SuperAdmins**

  ➔ Name: **Admin2**
  ➔ Password: **Kbits@123**
  ➔ Group: **RP-Admins**

  ➔ Name: **Admin3**
  ➔ Password: **Kbits@123**
  ➔ Group: **Switching-Admins**

# Lab 3 – Configuring Dot1x Authentication with VLAN & DACL Assignment



## Task 1 – Configure HQ-ASA for Telnet

- Configure HQ-ASA for Telnet using a Password of **Kbits@123**.
- Allow Telnet Access from the Inside-Emp & Inside-Cons interfaces.
- Ping & Telnet to HQ-ASA from the Inside PCs. You should be successful.

## Task 2 – Configure a Downloadable ACL (DACL) on ISE

- Configure a DACL on ISE with the following entries:
  - Deny icmp any any
  - Permit ip any any

## Task 3 – Configure Authorization Profiles

- Configure 2 Authorization Profiles to assign Users to appropriate VLANs & DACLs (If required) based on the following:

  Name: ISE-EMP-PROFILE
  VLAN: 11
  DACL: ISE-EMP-DACL

  Name: ISE-CON-PROFILE
  VLAN: 12
  DACL: None

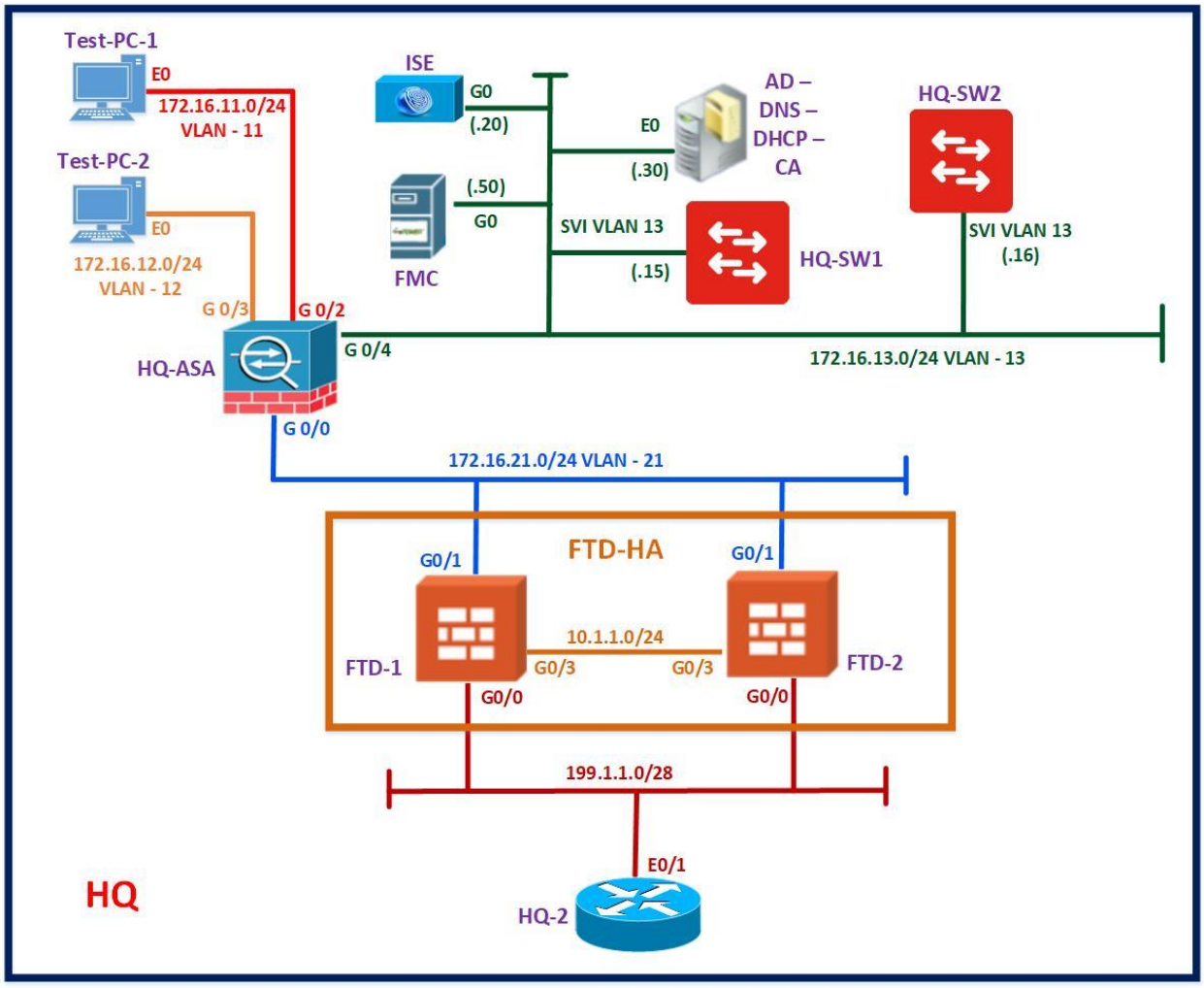
## Task 4 – Configure Authorization Policy

- Configure 2 Authorization Policies based on the following:

  - Name: **ISE-EMP-POLICY**
  - Conditions:
    - Identity Group Name: ISE-Employees
    - Wired_802.1x
  - Profile: **ISE-EMP-PROFILE**

  - Name: **ISE-CONS-POLICY**
  - Conditions:
    - Identity Group Name: ISE-Consultants
    - Wired_802.1x
  - Profile: **ISE-CON-PROFILE**

# Lab 4 – Configuring HQ-SW1 for Dot1x Authentication & Verify using Windows



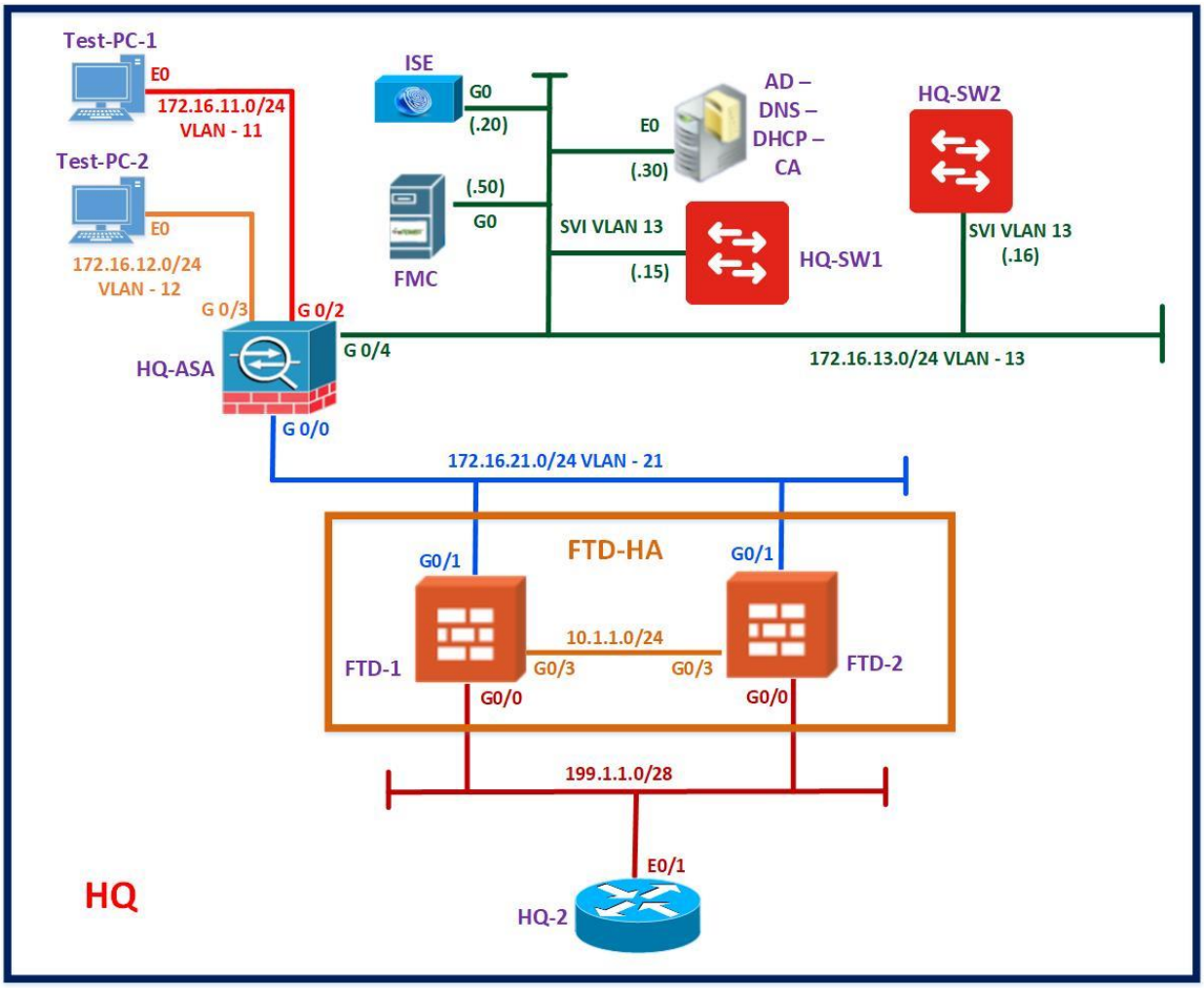
## Task 1 – Configure HQ-SW1 to use ISE for Dot1x Authentication

- Configure the HQ-SW1 with the following to support Dot1x Authenticatoin:
  - Local Username/Password with Privilege 15: admin/admin
  - RADIUS Server
    - Name: ISE1
    - Address/Key: 172.16.13.20/Kbits@123
  - Enable appropriate Authentication, Authorization & Accounting Lists.
  - Enable Dot1x on the ports connected towards the Client PCs in VLANs 11 & 12.

## Task 2 – Configure the Windows Supplicant

- Enable the WiredAutoConfig Services
- Enable the Dot1x services on the Network Adapter.
- Login using ISE-1 and verify that the DACL is working.
- Login using ISE-2 and verify that the User has full Access.

# Lab 5 – Integrating ISE with Microsoft Active Directory (AD)



## Task 1 – Configure the relationship between ISE & AD

- Configure the relationship based on the parameters below:
  - Join Point Name: KBITS
  - Active Directory Domain: kbits.live
  - Administrator Username & Password: Administrator/Cisco@123

## Task 2 – Pull down User and Computer Groups from AD

- Pull down the groups listed below from AD to ISE
  - Kbits.live/users/Employees
  - Kbits.live/users/Consultants
  - Kbits.live/users/Domain Users
  - Kbits.live/users/Domain Computers

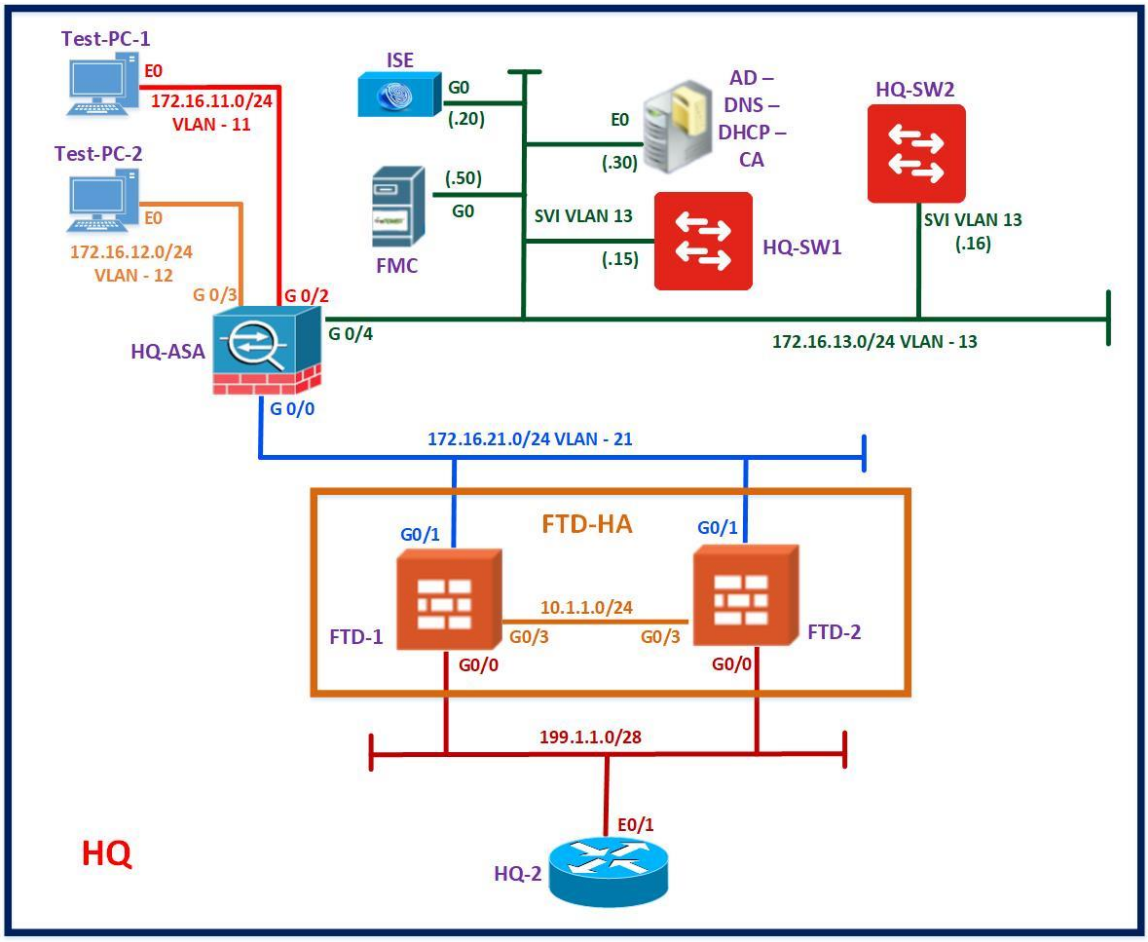
## Task 3 – Add the KBITS Identity in the Identity Source Sequence

- Configure the Active Directory Join Point KBITS within the Identity Source Sequences.
- Place it at #2 in the Sequence after “Internal Users”.

## Task 4 – Adding Certificate Support from AD.

- Allow the Active Directory Join Point KBITS in the Certificate Authentication Profile.

# Lab 6 – Authenticating Users using AD - Username/Password



## Task 1 – Configure Authorization Profiles for AD Users

- Configure 2 Authorization Profiles to assign AD Users to appropriate VLANs based on the following:

  Name: AD-EMP-PROFILE
  VLAN: 11

  Name: AD-CON-PROFILE
  VLAN: 12

## Task 2 – Configure Authorization Policy

- Configure 2 new Authorization Policies at the top based on the following:

  - Name: **AD-EMP-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: kbits.live/Users/Employees
    - Wired_802.1x
    - Device:DeviceType: Switches
  - Profile: **AD-EMP-PROFILE**

  - Name: **AD-CON-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: kbits.live/Users/Consultants
    - Wired_802.1x
    - Device:DeviceType: Switches
  - Profile: **AD-CON-PROFILE**

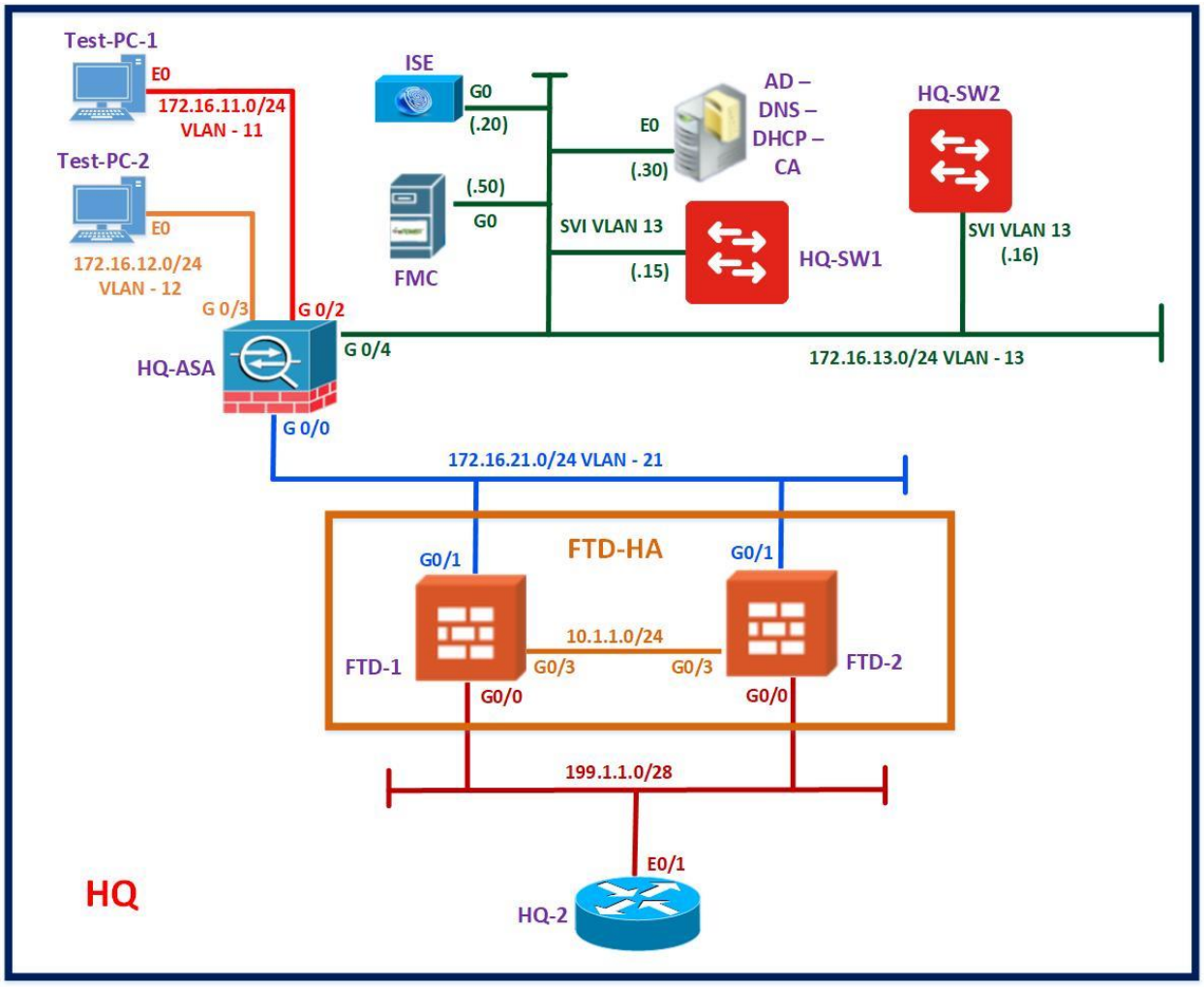
## Task 3 – Re-login to verify the Policy

- **Disable** and **re-enable** the Network Adapter under **Network & Sharing Center** on **PC2**.

- Replace the credentials to **EMP-1/Cisco@123** on the Authentication -> Additional Settings Page and verify the IP Address and RADIUS Log in ISE.

- Replace the credentials to **CONS-1/Cisco@123** on the Authentication -> Additional Settings Page and verify the IP Address and RADIUS Log in ISE.

# Lab 7 – Configuring Device Administration for Routers/Switches



### Task 1 – Configure HQ-SW1, HQ-SW2 & HQ-2 to point towards ISE

- Configure HQ-SW1, HQ-SW2 & HQ-R2 to point towards ISE using TACACS+ as the protocol.
- Use ISE-T as the server's name and ISE-TAC as the Group Name.
- Configure the Secret Password as **Kbits@123**

### Task 2 – Configure HQ-SW1, HQ-SW2 & HQ-2 to use ISE for Telnet and SSH authentication.

- Configure HQ-SW1, HQ-SW2 & HQ-R2 to use ISE for Telnet & SSH Authenticaiton using the TACACS+ server.
- Use a Named-list of your choice.

### Task 3 – Configure HQ-SW1, HQ-SW2 & HQ-R2 to use ISE for Telnet and SSH Exec & command Authorization

- Configure HQ-SW1, HQ-SW2 & HQ-R2 to use ISE for Telnet & SSH Exec and Command Authorization using the previously configured TACACS+ server.
- Comand Authorization should be done for Level 15 commands only.
- Use a Named-list.

### Task 4 – Configure HQ-SW1, HQ-SW2, HQ-2 to use ISE for TACACS+ Accounting

- Configure HQ-SW1, HQ-SW2 & HQ-2 to use ISE for Exec Accounting (Login/Logouts).
- Configure HQ-SW1, HQ-SW2 & HQ-2 to use ISE for Command Level 15 Accounting (Command Accounting).
- Use a Named-list.

### Task 5 – Configure a TACACS+ Exec Authorization Profile

- Configure a TACACS+ Exec Authorization Profile to set the Exec Level to 15.
- Name the Authorization Profile **PRIV_15**.

### Task 6 – Configure TACACS+ Command Set Profile

- Configure TACACS+ Commad Sets based on the following parameters:
    - Name: **Full-Access**

- Commands: All

- Name: **Routing-Protocol-CMDS**
- Commands:
  - Configure terminal
  - Router (All Protocols)
  - Network
  - Version
  - Router-id
  - Distribute-list
  - Redistribute
  - Access-list

- Name: **Switching-CMDS**
- Commands:
  - Configure terminal
  - VLAN
  - Interface
  - Switchport
  - Spanning-tree
  - Ip routing

## Task 7 – Configure the Device Admin Policy Sets

- Configure TACACS+ Device Admin Policies based on the following:

  - Name: **SuperAdmins-Policy**
    Conditions:
  - Identity Group Name: **SuperAdmins**
  - Device Types: **Routers or Switches Only**
    Results
  - Exec Profile: **PRIV_15**
  - Commands Set: **Full-Access**

  - Name: **RP-Admins-Policy**
    Conditions:
  - Identity Group Name: **RP-Admins**
  - Device Types: **Routers**
    Results
  - Exec Profile: **PRIV_15**
  - Commands Set: **Routing-Protocol-CMDS**

  - Name: **SwitchingAdmins-Policy**
    Conditions:
  - Identity Group Name: **Switching-Admins**

- Device Types: **Switches**
  Results
- Exec Profile: **PRIV_15**
- Commands Set: **Switching-CMDS**

## Task 8 – Telnet or SSH into HQ-2 & HQ-SW1 to verify the Device Configuration

- Telnet into HQ-2 from HQ-SW1 using admin1/Kbits@123 username/password combination.
- Verify that the Authorization is working.

- Telnet into HQ-SW1 from HQ-SW2 using admin/Kbits@123 username/password combination.
- Verify that the Authorization is working.

- Telnet into HQ-SW2 from HQ-SW1 using admin3/Cisco@123 username/password combination.
- Verify that the Authorization is working.

## Task 9 – Verify Accounting by verifying the TACACS+ Logs on ISE

- Verify that the Command and Logins are being recorded on ISE.