

# Full Network Project Configuration

## 1. Project Overview

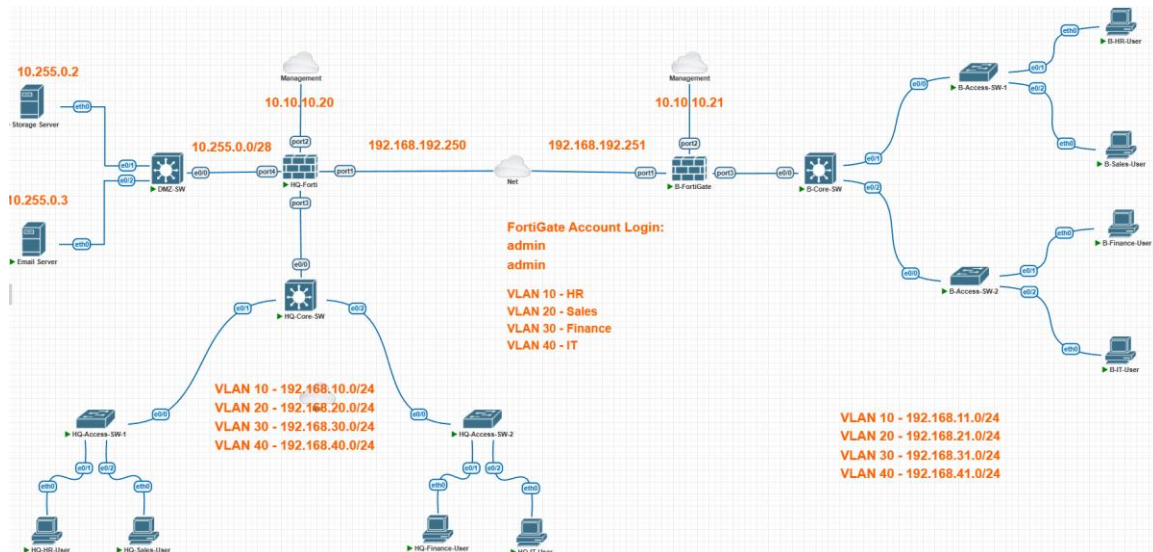
Project Name: Network Security Fundamentals and FortiGate Integration

Objective:

The purpose of this project is to design and implement Firewall policies and NAT configuration for port forwarding

## 2. Network Topology

Topology Diagram:



Logical Overview:

- Two FortiGate firewalls (HQ & Branch)
- 2 Core and 4 access switching with VLAN segmentation
- Static routing between firewalls
- NAT enabled on HQ & Branch firewall
- Inter-VLAN communication via core switch
- Simulated or bridged WAN connectivity
- VPN integration via IPsec

### 3. IP Addressing Scheme

VLANs & Subnets (HQ):

- VLAN 10: 192.168.10.0/24
- VLAN 20: 192.168.20.0/24
- VLAN 30: 192.168.30.0/24
- VLAN 40: 192.168.40.0/24

IP Range/Subnet					
B_VPN_local_subnet_1	10.255.0.0/28		Address	1	
B_VPN_local_subnet_2	192.168.10.0/24		Address	1	
B_VPN_local_subnet_3	192.168.20.0/24		Address	1	
B_VPN_local_subnet_4	192.168.30.0/24		Address	1	
B_VPN_remote_subnet_1	192.168.11.0/24		Address	3	
B_VPN_remote_subnet_2	192.168.21.0/24		Address	3	
B_VPN_remote_subnet_3	192.168.31.0/24		Address	3	
DMZ	10.255.0.0/28	DMZ (port4)	Address	2	
FABRIC_DEVICE	0.0.0.0/0		Address	0	
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0	
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	1	
all	0.0.0.0/0		Address	1	
none	0.0.0.0/32		Address	0	
Interface Subnet					
VLAN 10 address	192.168.10.0/24	HR (VLAN 10)	Address	3	
VLAN 20 address	192.168.20.0/24	Sales (VLAN 20)	Address	3	
VLAN 30 address	192.168.30.0/24	Finance (VLAN 30)	Address	3	
VLAN 40 address	192.168.40.0/24	IT (VLAN 40)	Address	2	

HQ FortiGate Interfaces:

- port1 (WAN): 192.168.192.250/24
- port2 (MGMT): 10.10.10.20/24
- port3 (Internal): Connected to core switch

802.3ad Aggregate						
fortilink	802.3ad Aggregate	Dedicated to FortiSwitch	PING Security Fabric Connection	10.255.1.2-10.255.1.254	2	
Physical Interface						
DMZ (port4)	Physical Interface	10.255.0.1/255.255.255.240	PING		3	
LAN (port3)	Physical Interface	0.0.0.0/0.0.0.0			4	
Management (port2)	Physical Interface	10.10.10.20/255.255.255.0	PING HTTPS HTTP		0	
WAN (port1)	Physical Interface	192.168.192.250/255.255.255.0	PING		4	
Tunnel Interface						
NAT interface (natroot)	Tunnel Interface	0.0.0.0/0.0.0.0			0	

## VLANs & Subnets (Branch):

- VLAN 10: 192.168.11.0/24
- VLAN 20: 192.168.21.0/24
- VLAN 30: 192.168.31.0/24
- VLAN 40: 192.168.41.0/24

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Byte
HQ_to_B_VLAN10	HQ_VPN	HR (VLAN 10)	HQ_VPN_remote_subnet_1	VLAN 10 address	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
B_to_HQ_VLAN10	HR (VLAN 10)	HQ_VPN	VLAN 10 address	HQ_VPN_remote_subnet_1	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
HQ_to_B_VLAN20	HQ_VPN	Sales (VLAN 20)	HQ_VPN_remote_subnet_2	VLAN 20 address	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
B_to_HQ_VLAN20	Sales (VLAN 20)	HQ_VPN	VLAN 20 address	HQ_VPN_remote_subnet_2	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
HQ_to_B_VLAN30	HQ_VPN	Finance (VLAN 30)	HQ_VPN_remote_subnet_3	VLAN 30 address	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
B_to_HQ_VLAN30	Finance (VLAN 30)	HQ_VPN	VLAN 30 address	HQ_VPN_remote_subnet_3	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
B_to_HQ_DMZ	HR (VLAN 10) Sales (VLAN 20) Finance (VLAN 30)	HQ_VPN	VLAN 10 address VLAN 20 address VLAN 30 address	HQ_VPN_remote_subnet_4	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
IT_TO_Internet	IT (VLAN 40)	WAN (port1)	VLAN 40 address	all	always	ALL	ACCEPT	internet_access	no-inspection	All	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

## Branch FortiGate Interfaces:

- port1 (WAN): 192.168.192.251/24
- port2 (MGMT): 10.10.10.21/24
- port3 (Internal): Connected to Branch core

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
802.3ad Aggregate	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface							
LAN (port3)	Physical Interface		0.0.0.0/0.0.0.0				4
Management (port2)	Physical Interface		10.10.10.21/255.255.255.0	PING HTTPS HTTP			0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (port1)	Physical Interface		192.168.192.251/255.255.255.0	PING			4
Tunnel Interface							
NAT interface (na.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

## 4. Routing Configuration

### Static Routes:

### HQ FortiGate:

- 0.0.0.0/0 → 192.168.192.2 (simulated ISP gateway) via port1
- Internal VLAN networks on branch reachable via IPSec tunnel

B_VPN_remote		B_VPN	Enabled	VPN: B_VPN (Created by VPN wizard)
B_VPN_remote		Blackhole	Enabled	VPN: B_VPN (Created by VPN wizard)
0.0.0.0/0	192.168.192.2	WAN (port1)	Enabled	

Branch FortiGate:

- 0.0.0.0/0 → 192.168.192.2 (Simulated ISP gateway) via port1

- Internal VLAN networks on branch reachable via IPSec tunnel

Destination ☯	Gateway IP ☯	Interface ☯	Status ☯	Comments ☯
0.0.0.0/0	192.168.192.2	WAN (port1)	Enabled	
HQ_VPN_remote		HQ_VPN	Enabled	VPN: HQ_VPN (Created by VPN wizard)
HQ_VPN_remote		Blackhole	Enabled	VPN: HQ_VPN (Created by VPN wizard)

## 5. Firewall Configuration

Policies:

HQ Firewall:

1. VLANs → WAN (NAT enabled for IT, allow similar vlans to communicate with each other)

- Dynamic IP NAT from an IP pool 192.168.192.100-192.168.192.150 for VLAN 40(IT)

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
HQ_to_B_VLAN10	HR (VLAN 10)	B_VPN	VLAN 10 address	B_VPN_remote_subnet_1	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
B_to_HQ_VLAN10	B_VPN	HR (VLAN 10)	B_VPN_remote_subnet_1	VLAN 10 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
HQ_to_B_VLAN20	Sales (VLAN 20)	B_VPN	VLAN 20 address	B_VPN_remote_subnet_2	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
B_to_HQ_VLAN20	B_VPN	Sales (VLAN 20)	B_VPN_remote_subnet_2	VLAN 20 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
HQ_to_B_VLAN30	Finance (VLAN 30)	B_VPN	VLAN 30 address	B_VPN_remote_subnet_3	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
B_to_HQ_VLAN30	B_VPN	Finance (VLAN 30)	B_VPN_remote_subnet_3	VLAN 30 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
B_to_HQ_DMZ	B_VPN	DMZ (port4)	B_VPN_remote	DMZ	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
Lan_to_DMZ	HR (VLAN 10) Sales (VLAN 20) Finance (VLAN 30) IT (VLAN 40)	DMZ (port4)	VLAN 10 address VLAN 20 address VLAN 30 address VLAN 40 address	DMZ	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM
IT_to_Internet	IT (VLAN 40)	WAN (port1)	VLAN 40 address	all	always	ALL	ACCEPT	Internet access	SSL no-inspection	UTM
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

Name ☯	External IP Range ☯	Type ☯	ARP Reply ☯	Ref. ☯
Internet access	192.168.192.100 - 192.168.192.150	Overload	Enabled	1

Branch Firewall:

1. VLANs → WAN (NAT enabled for IT, allow similar vlans to communicate with each other)

- Dynamic IP NAT from an IP pool 192.168.192.151-192.168.192.200 for VLAN 40(IT)

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Byte
HQ_to_B_VLAN10	HQ_VPN	HR (VLAN 10)	HQ_VPN_remote_subnet_1	VLAN 10 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
B_to_HQ_VLAN10	HR (VLAN 10)	HQ_VPN	VLAN 10 address	HQ_VPN_remote_subnet_1	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
HQ_to_B_VLAN20	HQ_VPN	Sales (VLAN 20)	HQ_VPN_remote_subnet_2	VLAN 20 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
B_to_HQ_VLAN20	Sales (VLAN 20)	HQ_VPN	VLAN 20 address	HQ_VPN_remote_subnet_2	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
HQ_to_B_VLAN30	HQ_VPN	Finance (VLAN 30)	HQ_VPN_remote_subnet_3	VLAN 30 address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
B_to_HQ_VLAN30	Finance (VLAN 30)	HQ_VPN	VLAN 30 address	HQ_VPN_remote_subnet_3	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
B_to_HQ_DMZ	HR (VLAN 10) Sales (VLAN 20) Finance (VLAN 30)	HQ_VPN	VLAN 10 address VLAN 20 address VLAN 30 address	HQ_VPN_remote_subnet_4	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0B
IT_TO_Internet	IT (VLAN 40)	WAN (port1)	VLAN 40 address	all	always	ALL	ACCEPT	Internet_access	SSL no-inspection	All	0B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0B

Name ☯	External IP Range ☯	Type ☯	ARP Reply ☯	Ref. ☯
Internet_access	192.168.192.151 - 192.168.192.200	Overload	Enabled	1

### VPN (Site-To-Site Using IPsec):

## 1-Transfer data across a secure tunnel using IPsec

## Branch-VPN

VPN Tunnel

Tunnel Template

Site to Site - FortiGate

Convert To Custom Tunnel

Name

HQ\_VPN

Comments

VPN: HQ\_VPN (Created by VPN wizard)

Network

IP Version

IPv4

IP Address

192.168.192.250

Outgoing Interface

WAN (port1)

Dead Peer Detection

Disable

On Idle

On Demand

DPD retry count

3

DPD retry interval

20

s

Forward Error Correction

Egress ☐

Ingress ☐

Advanced...

Authentication

Edit

Authentication Method : Pre-shared Key

Phase 2 Selectors

	Local Address	Remote Address	
HQ_VPN	HQ_VPN_local	HQ_VPN_remote	<div>Edit</div>

	Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate	HQ_VPN	WAN (port1)	Up	9

HQ-VPN

Edit VPN Tunnel

Tunnel Template

Site to Site - FortiGate

Convert To Custom Tunnel

Name

B\_VPN

Comments

VPN: B\_VPN (Created by VPN wizard)

Network

IP Version

IPv4

IP Address

192.168.192.251

Outgoing Interface

WAN (port1)

Dead Peer Detection

Disable

On Idle

On Demand

DPD retry count

3

DPD retry interval

20

s

Forward Error Correction

Egress

Ingress

Advanced...

Authentication

Authentication Method : Pre-shared Key

Edit

Phase 2 Selectors

Local Address

Remote Address

B\_VPN

B\_VPN\_local

B\_VPN\_remote

Q

admin

Create New

Edit

Delete

Search

Tunnel	Interface Binding	Status	Ref
Site to Site - FortiGate			
B_VPN	WAN (port1)	Up	9

7. Device Configurations

```
HQ-Access-SW-1#show vlan b
VLAN Name                               Status    Ports
----
1    default                               active    Et0/3
10   HR                                     active    Et0/1
20   Sales                                active    Et0/2
30   Finance                              active
40   IT                                    active
1002 fddi-default                           act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                      act/unsup
1005 trnet-default                       act/unsup
HQ-Access-SW-1#
```

#HQ-SW1

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname HQ-Access-SW-1

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

!

```
interface Ethernet0/1
  switchport access vlan 10
  switchport mode access
!
interface Ethernet0/2
  switchport access vlan 20
  switchport mode access
!
interface Ethernet0/3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
End
```

#HQ-SW2

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname HQ-Access-SW-2

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

```
!  
interface Ethernet0/1  
    switchport access vlan 30  
    switchport mode access  
!  
interface Ethernet0/2  
    switchport access vlan 40  
    switchport mode access  
!  
interface Ethernet0/3  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
control-plane  
!  
line con 0  
    logging synchronous  
line aux 0  
line vty 0 4  
    login  
!  
End
```

#HQ-CORE-SW

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname HQ-Access-SW-2

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

```
!  
interface Ethernet0/1  
    switchport access vlan 30  
    switchport mode access  
!  
interface Ethernet0/2  
    switchport access vlan 40  
    switchport mode access  
!  
interface Ethernet0/3  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
control-plane  
!  
line con 0  
    logging synchronous  
line aux 0  
line vty 0 4  
    login  
!  
End
```

#B-CORE-SW

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname B-Core-SW

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

```
!  
interface Ethernet0/1  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface Ethernet0/2  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface Ethernet0/3  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
control-plane  
!  
line con 0  
    logging synchronous  
line aux 0  
line vty 0 4  
    login  
!  
End
```

#B-ACCESS-SW

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname B-Access-SW-1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

!

```
interface Ethernet0/1
  switchport access vlan 10
  switchport mode access
!
interface Ethernet0/2
  switchport access vlan 20
  switchport mode access
!
interface Ethernet0/3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
End
```

## #B-ACCESS-SW2

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname B-Access-SW-1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

!

```
interface Ethernet0/1
  switchport access vlan 10
  switchport mode access
!
interface Ethernet0/2
  switchport access vlan 20
  switchport mode access
!
interface Ethernet0/3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
end
```

## 8. Testing & Verification

Connectivity Tests:

IT → ping google.com successful

HQ-HR → ping google.com unsuccessful

HQ-HR → ping B-HR successful

HQ-HR → ping HQ-IT unsuccessful

B-IT → ping google.com successful

All CLIENT → ping GATEWAY(192.168.192.2) successful