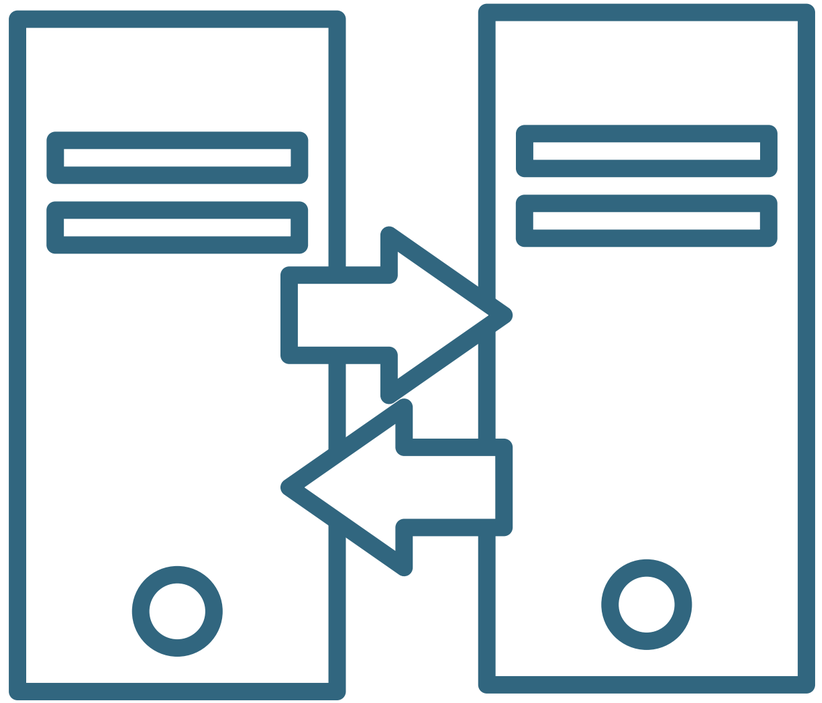
GNS3 FORTIGATE

OUTLINE

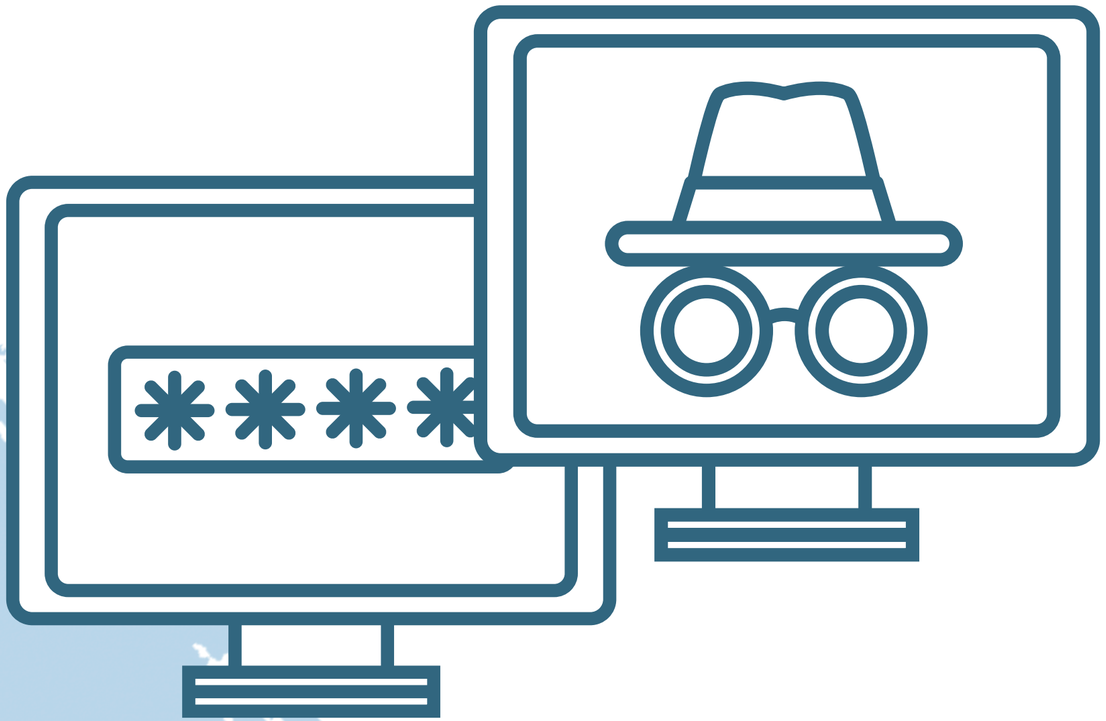
1. Project Overview
2. Project flow
3. Network Topology
4. VLAN Setup
5. FortiGate Integration
6. NAT
7. Firewall Policies
8. Testing

1. PROJECT OVERVIEW

- The goal was to build a secure segmented network for HR and IT.
- Tools used: GNS3, FortiGate, L3 Switch, Router, Endpoints



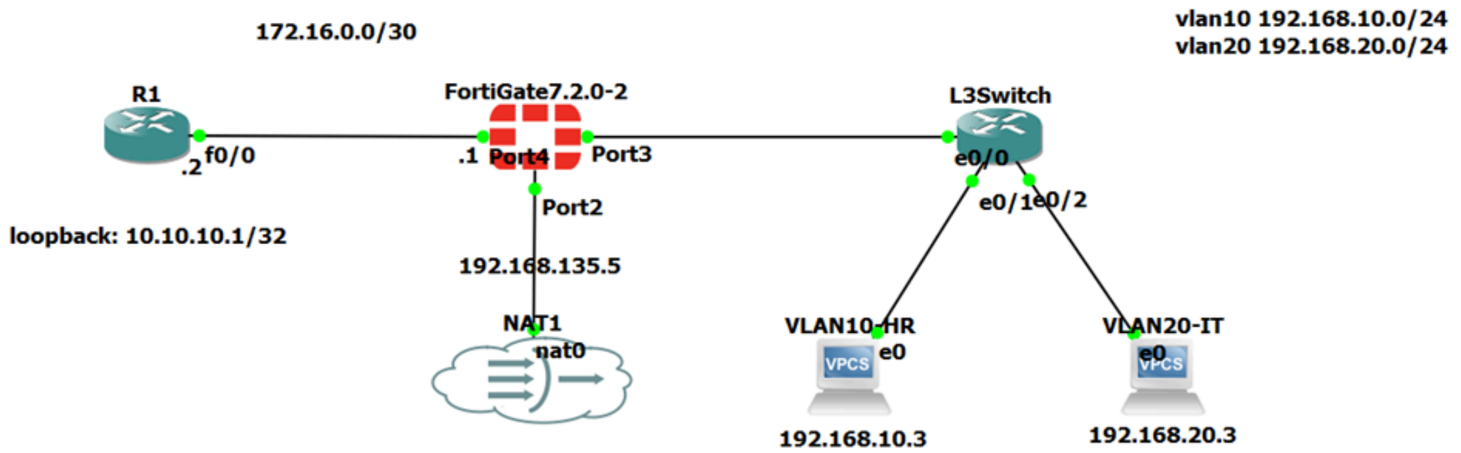
2. PROJECT FLOW



- Image installation
- Topology
- VLAN Setup
- FortiGate
- Policies
- Testing

3. NETWORK TOPOLOGY

- FortiGate as firewall
- L3 switch for VLANs
- Router branch link
- Endpoints (HR, IT)



4. VLAN SETUP

- Create VLANs HR and IT
- Assign Ports
- Set Trunk between switch and FortiGate
- DHCP Setup for vlans on switch

VLAN TEST

DHCP CONFIGURATION

```
L3Switch(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.2
L3Switch(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.2
L3Switch(config)#ip dhcp pool HR
L3Switch(dhcp-config)#network 192.168.10.0 255.255.255.0
L3Switch(dhcp-config)#default-router 192.168.10.1
L3Switch(dhcp-config)#dns-server 8.8.8.8
L3Switch(dhcp-config)#
L3Switch(dhcp-config)#ip dhcp pool IT
L3Switch(dhcp-config)#network 192.168.20.0 255.255.255.0
L3Switch(dhcp-config)#default-router 192.168.20.1
L3Switch(dhcp-config)#dns-server 8.8.8.8
L3Switch(dhcp-config)#
L3Switch(dhcp-config)#end
```

IP ASSIGNMENT

```
VLAN10-HR> dhcp
DDORA IP 192.168.10.3/24 GW 192.168.10.1
```

```
VLAN20-IT> dhcp
DDORA IP 192.168.20.3/24 GW 192.168.20.1
```

5. FORTIGATE INTEGRATION

- Trunk on port3
- Sub-interfaces
- Address and Addresses Groups
- Router Link on port4 (other branch)
- WAN on port2

FORTIGATE CONT.

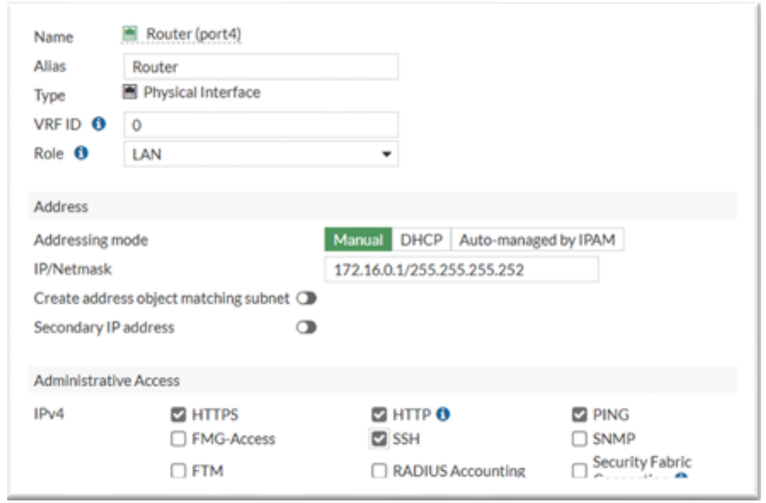
R1	R1-Loopback R1-IP
VLANs	VLAN10-HR address VLAN20-IT address

ADDRESSES GROUPS

LAN Trunk (port3)	Physical Interface		0.0.0.0/0.0.0.0	PING
VLAN10-HR	VLAN		192.168.10.1/255.255.255.0	PING HTTPS SSH
VLAN20-IT	VLAN		192.168.20.1/255.255.255.0	PING HTTPS SSH

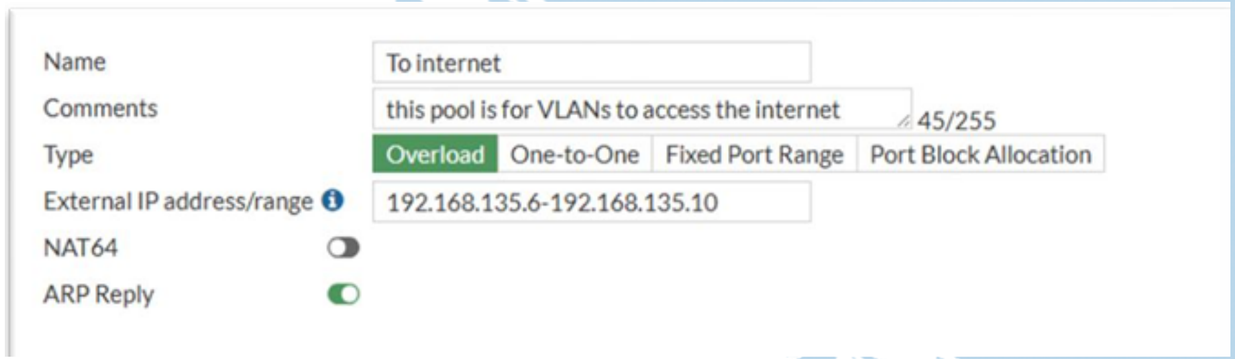
} PORT3 (WITH VLANS AS SUBINTERFACES)

PORT4 (THE OTHER BRANCH) {



6. NETWORK ADDRESS TRANSLATION (NAT)

a NAT IP Pool was created to support outbound traffic from internal VLANs toward the external router.



7. FIREWALL POLICIES

- Internal to Internal
- Internal to External

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
HR to IT (Ping)	VLAN10-HR	VLAN20-IT	VLAN10-HR address	VLAN20-IT address	always	ALL_ICMP PING	DENY			All
IT to HR (ping)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (SSH)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	SSH TELNET PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (RDP)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	RDP PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (SNMP)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	SNMP PING	ACCEPT	Disabled	no-inspection	UTM
HR to WAN	VLAN10-HR	port2	VLAN10-HR address	all	always	DNS HTTPS	ACCEPT	To Internet	certificate-inspection	UTM
IT to WAN	VLAN20-IT	port2	VLAN20-IT address	all	always	ALL	ACCEPT	To Internet	certificate-inspection	UTM
VLANs to WAN (NTP)	VLAN20-IT VLAN10-HR	port2	VLANs	all	always	NTP	ACCEPT	To Internet	certificate-inspection	UTM
VLANs to Router	VLAN10-HR VLAN20-IT	Router (port4)	VLANs	R1-Loopback	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM
R1-IP to VLANs	Router (port4)	VLAN10-HR VLAN20-IT	R1-IP	VLANs	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

INTERNAL TO INTERNAL

Source	Destination	Service	Action
HR	IT	ICMP	Deny
IT	HR	ICMP	Accept
IT	HR	SSH	Accept
IT	HR	RDP	Accept
IT	HR	SNMP	Accept
Both Vlans (IT and HR)	RI (2nd Branch)	ICMP	Accept
RI (2nd Branch)	Both Vlans (IT and HR)	ICMP	Accept

INTERNAL TO EXTERNAL

Source	Destination	Service	Action
HR	All	HTTPS, DNS	Accept
IT	All	ALL	Accept
Both Vlan (HR and IT)	All	NTP	Accept

8. TESTING

VLANs to their Gateways on FortiGate

```
VLAN10-HR> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=2.932 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=1.879 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=2.003 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=1.496 ms
```

```
VLAN20-IT> ping 192.168.20.1
84 bytes from 192.168.20.1 icmp_seq=1 ttl=255 time=3.834 ms
84 bytes from 192.168.20.1 icmp_seq=2 ttl=255 time=2.767 ms
84 bytes from 192.168.20.1 icmp_seq=3 ttl=255 time=3.470 ms
84 bytes from 192.168.20.1 icmp_seq=4 ttl=255 time=2.229 ms
```

VLAN to VLAN

```
VLAN10-HR> ping 192.168.20.3
192.168.20.3 icmp_seq=1 timeout
192.168.20.3 icmp_seq=2 timeout
192.168.20.3 icmp_seq=3 timeout
192.168.20.3 icmp_seq=4 timeout
```

```
VLAN20-IT> ping 192.168.10.3
192.168.10.3 icmp_seq=1 timeout
192.168.10.3 icmp_seq=2 timeout
84 bytes from 192.168.10.3 icmp_seq=3 ttl=63 time=4.383 ms
84 bytes from 192.168.10.3 icmp_seq=4 ttl=63 time=1.903 ms
84 bytes from 192.168.10.3 icmp_seq=5 ttl=63 time=2.535 ms
```

VLANs to the Other Branch RI

```
VLAN10-HR> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=254 time=16.647 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=254 time=17.478 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=254 time=20.085 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=254 time=17.300 ms
```

```
VLAN20-IT> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=254 time=49.602 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=254 time=16.975 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=254 time=17.504 ms
```

VLANs to WAN

```
VLAN20-IT> ping 192.168.135.5
84 bytes from 192.168.135.5 icmp_seq=1 ttl=255 time=3.458 ms
84 bytes from 192.168.135.5 icmp_seq=2 ttl=255 time=2.120 ms
84 bytes from 192.168.135.5 icmp_seq=3 ttl=255 time=2.181 ms
```

THANKS