

DEPI Final Project

Fortinet Cybersecurity Engineer

Agenda



1 – what is VPN



2- site to site VPN



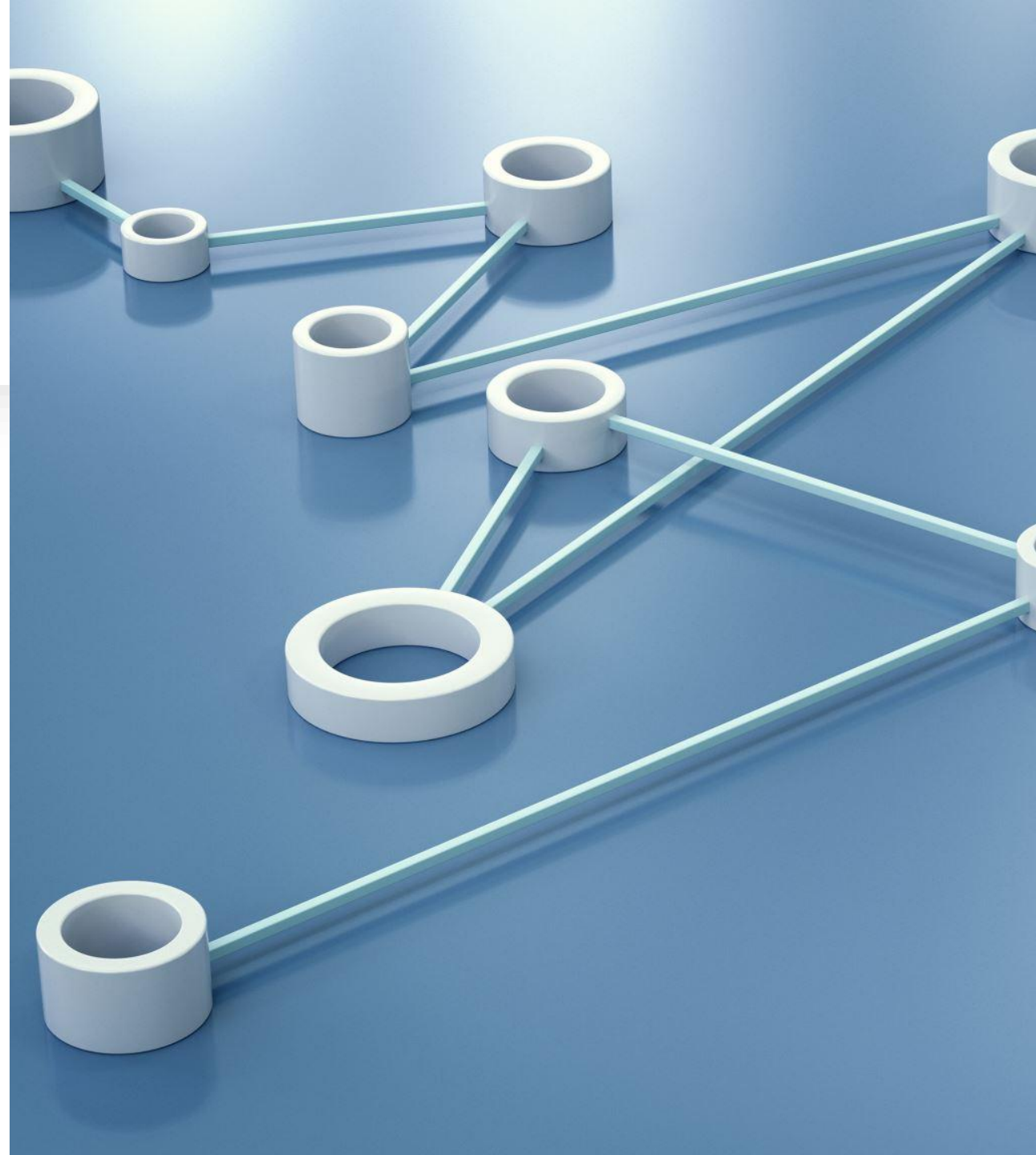
3 – ipsec VPN



4 – implementation and
simple topology

What is VPN ?

- A **VPN (Virtual Private Network)**:
- is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. VPNs are used to enhance privacy, protect sensitive data, and enable secure communication. They work by encrypting your data and routing it through a remote server, hiding your IP address and online activities.



Type of VPN:

- **1. Remote Access VPN**
 - **Purpose:** Enables users to securely connect to a private network (e.g., an office network) from a remote location.
- **2. Site-to-Site VPN**
 - **Purpose:** Connects entire networks (e.g., two office branches) over the internet securely.
- **3. Client-to-Site VPN**
 - **Purpose:** Similar to remote access but more tailored to individual users needing direct access to a corporate network.



Type of VPN:

- **4. SSL VPN (Secure Sockets Layer VPN)**
 - **Purpose:** Provides secure remote access without requiring specialized software.
- **5. MPLS VPN (Multiprotocol Label Switching VPN)**
 - **Purpose:** Uses MPLS technology to connect different locations over a service provider's private network.
- **6. Mobile VPN**
 - **Purpose:** Designed for users on mobile devices who frequently switch between networks or maintain active sessions.



Type of VPN:

- **7. Cloud VPN**
 - **Purpose:** Extends secure connections to cloud environments.
- **8. Peer-to-Peer (P2P) VPN**
 - **Purpose:** Used for secure file sharing or decentralized network setups.



A glowing green padlock is centered on a dark blue background with a complex circuit board pattern. The padlock is illuminated with a bright green light, creating a shimmering effect. The circuit lines are thin and white, with some small white dots scattered throughout.

VPN Protocols

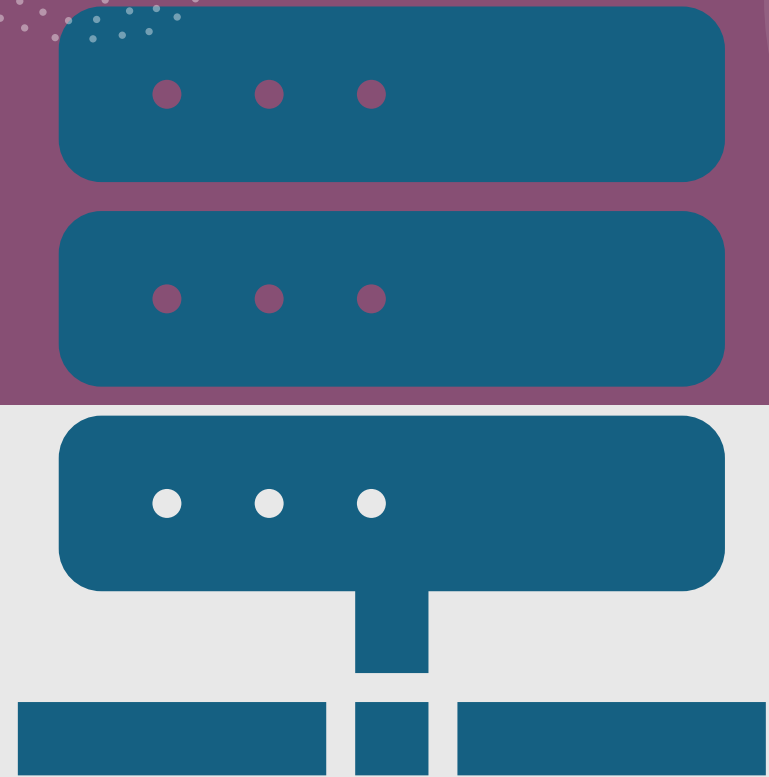
- VPNs can also be categorized based on the protocols they use:
1. **OpenVPN:** Open-source, highly secure, and flexible.
 2. **IKEv2/IPsec:** Secure and stable, especially for mobile devices.
 3. **L2TP/IPsec:** A combination of Layer 2 Tunneling Protocol and IPsec encryption.
 4. **PPTP:** Fast but outdated and less secure.
 5. **WireGuard:** Modern, lightweight, and efficient.

Site To Site VPN:

- **Purpose:** Connects entire networks (e.g., two office branches) over the internet securely.
- **Use Case:** Large organizations that need to interconnect geographically separated networks.
 - **How It Works:**
 - Establishes a secure tunnel between routers or gateways of two networks.
 - **Subtypes:**
 - **Intranet-based Site-to-Site VPN:** Connects different branches of the same organization.
 - **Extranet-based Site-to-Site VPN:** Connects an organization's network with that of a partner organization.

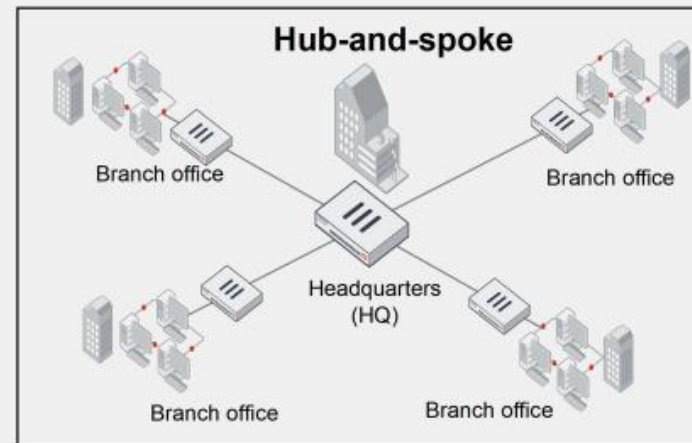
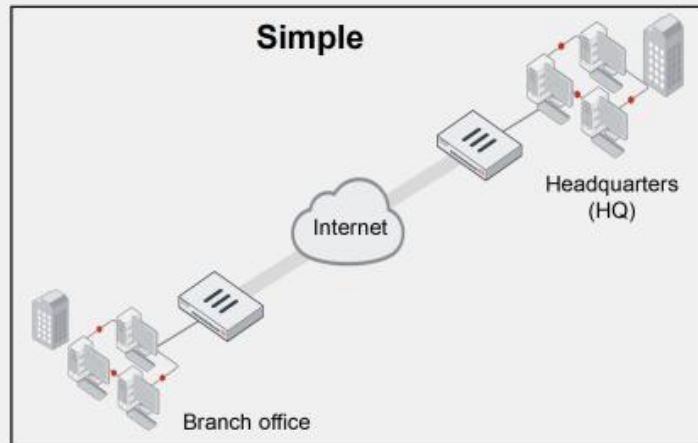
IPsec VPN Site TO Site:

- What is IPsec? When should you use it?
 - IPsec is a vendor-neutral set of standard protocols that is used to join two physically distinct LANs. The LANs are joined as if they were a single logical network, despite being separated by the internet.



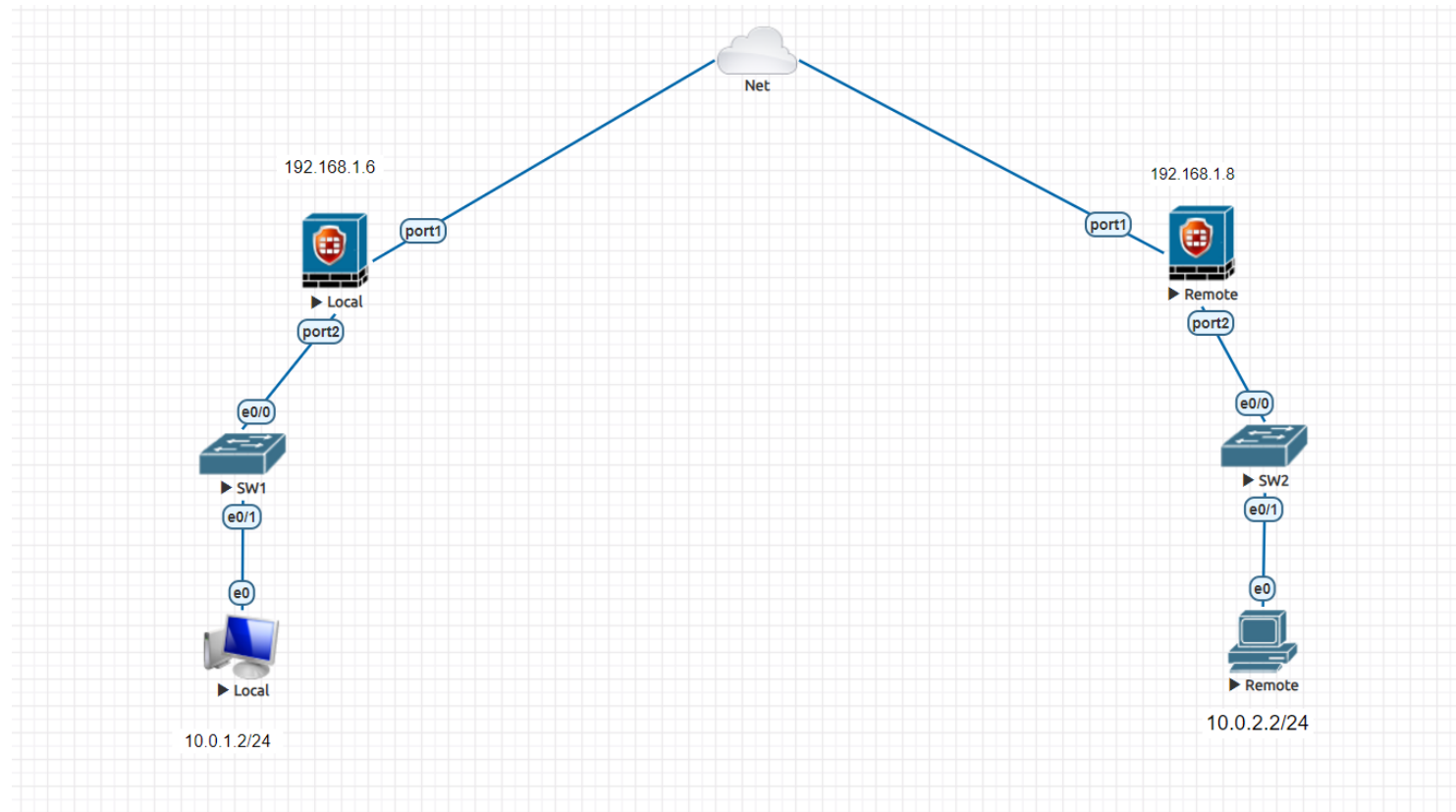
Site To Site Topologys:

VPN Topologies—Site-to-Site



Simple Topology and implementation on EVE Environment

Topology Will Work on



Methods to make ipsec Tunnel

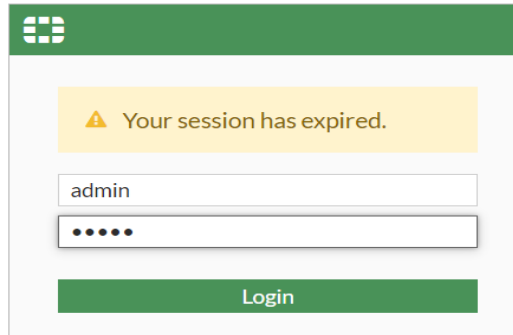
1 – Manually


2 – using Wizerd

So For simplicity
we will use
ipsec wizerd

Ipssec using ipsec wizard in Fortigate:

- Local Fortigate:
 - Login:

A screenshot of the Fortigate web interface login page. At the top, there is a green header bar with the Fortigate logo. Below the header, a yellow warning box contains a triangle icon and the text "Your session has expired.". Underneath the warning box, there are two input fields: the first contains the username "admin", and the second contains masked characters (dots). At the bottom of the login area, there is a green button labeled "Login".

 Your session has expired.

admin

••••

Login

Go to vpn tab:

- 1 – select ipsec wizard
 - Then fill the information about the Remote site

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Name: TO Remote

Template type: Site to Site | Hub-and-Spoke | Remote Access | Custom

NAT configuration: No NAT between sites | This site is behind NAT | The remote site is behind NAT

Remote device type: FortiGate | Cisco

Site to Site - FortiGate

The diagram illustrates a Site to Site - FortiGate configuration. It shows two FortiGate devices, one labeled 'This FortiGate' and the other 'Remote FortiGate', connected via the Internet. The 'This FortiGate' device is highlighted with a green box.

< Back Next > Cancel

Make the Authentication configuration

VPN Creation Wizard

✓ VPN Setup > ② Authentication > ③ Policy & Routing > ④ Review Settings

Remote device

IP Address Dynamic DNS

Remote IP address

192.168.1.8

Outgoing Interface

WAN (port1)

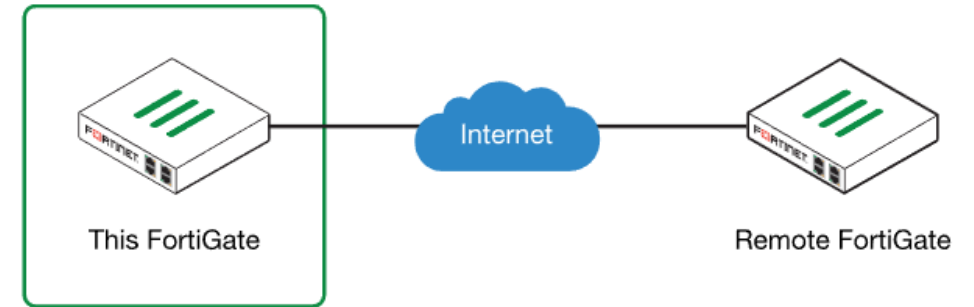
Authentication method

Pre-shared Key Signature

Pre-shared key

123456

Site to Site - FortiGate



< Back

Next >

Cancel

Make routing policy for forward the traffic

VPN Creation Wizard

✓ VPN Setup

✓ Authentication

3 Policy & Routing

4 Review Settings

Local interface

LAN (port2) ✕

+

Local subnets

10.0.1.0/24

+

Remote Subnets

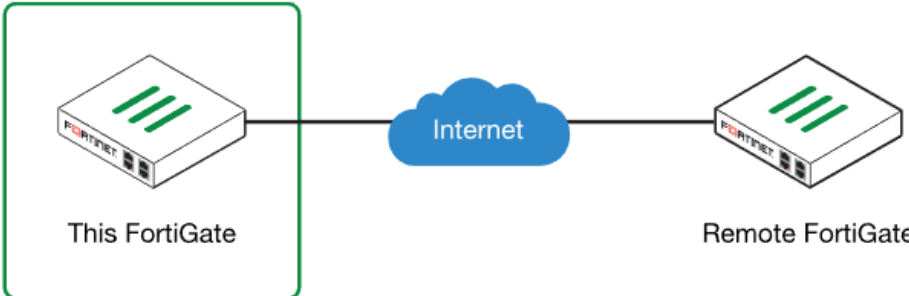
10.0.2.0/24

+

Internet Access i

None Share Local Use Remote

Site to Site - FortiGate



```
graph LR; FG1[This FortiGate] --- Internet((Internet)); Internet --- FG2[Remote FortiGate];
```

< Back

Next >

Cancel

Finally review your configuration:

VPN Creation Wizard

✓ VPN Setup

✓ Authentication

✓ Policy & Routing

4 Review Settings

The following settings should be reviewed prior to creating the VPN.

Object Summary

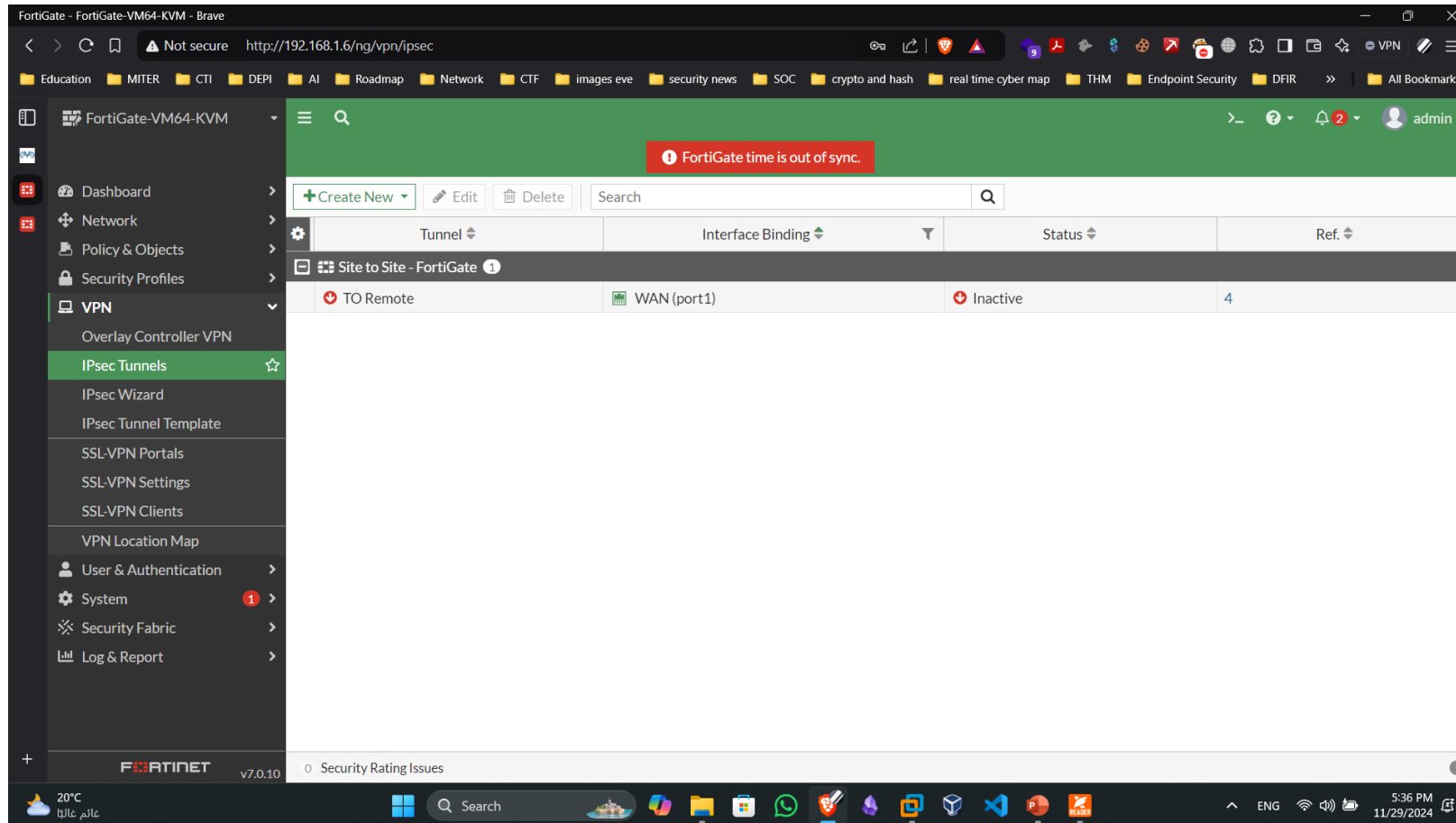
Phase 1 interface	TO Remote
Local address group	TO Remote_local
Remote address group	TO Remote_remote
Phase 2 interface	TO Remote
Static route	static
Blackhole route	static
Local to remote policies	vpn_TO Remote_local
Remote to local policies	vpn_TO Remote_remote

< Back

Create

Cancel

The First VPN site ready:



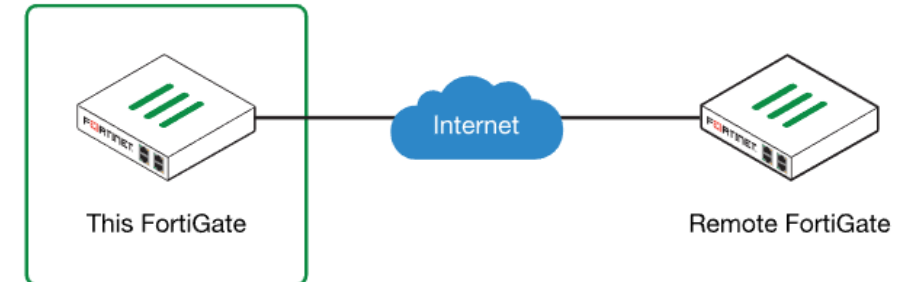
Go to the remote side the make the same conf

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Name	<input type="text" value="TO local"/>
Template type	Site to Site Hub-and-Spoke Remote Access Custom
NAT configuration	No NAT between sites This site is behind NAT The remote site is behind NAT
Remote device type	FortiGate Cisco

Site to Site - FortiGate



< Back

Next >

Cancel


Choose your Remote IP and the interface

VPN Creation Wizard


✓ VPN Setup > ② Authentication > ③ Policy & Routing > ④ Review Settings

Remote device IP Address Dynamic DNS

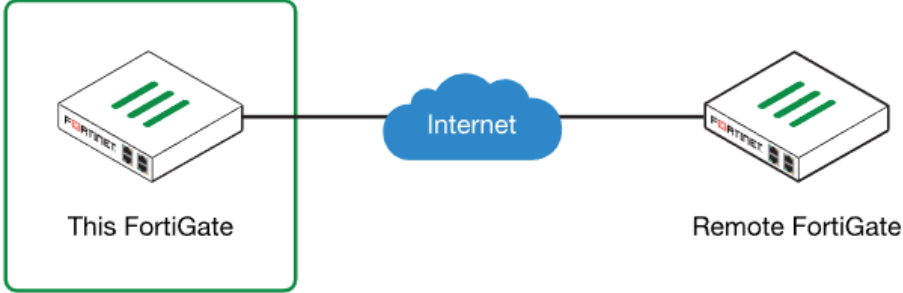
Remote IP address

Outgoing Interface  WAN (port1) ▼

Authentication method Pre-shared Key Signature

Pre-shared key 

Site to Site - FortiGate



< Back Next > Cancel

Choose what is the local and remote subnets:

VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > **3 Policy & Routing** > 4 Review Settings

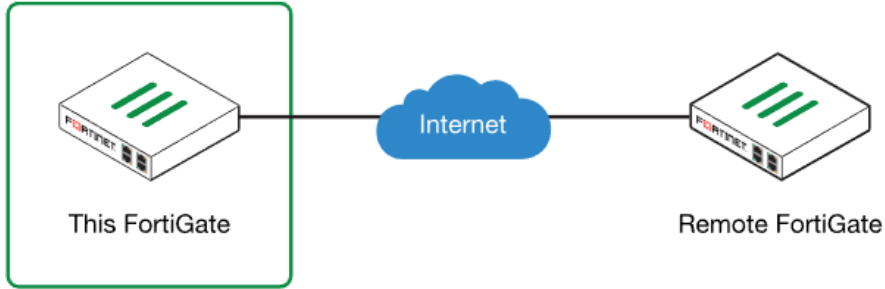
Local interface: LAN (port2) ✕

Local subnets: 10.0.2.0/24 +

Remote Subnets: 10.0.1.0/24 +

Internet Access ⓘ **None** Share Local Use Remote

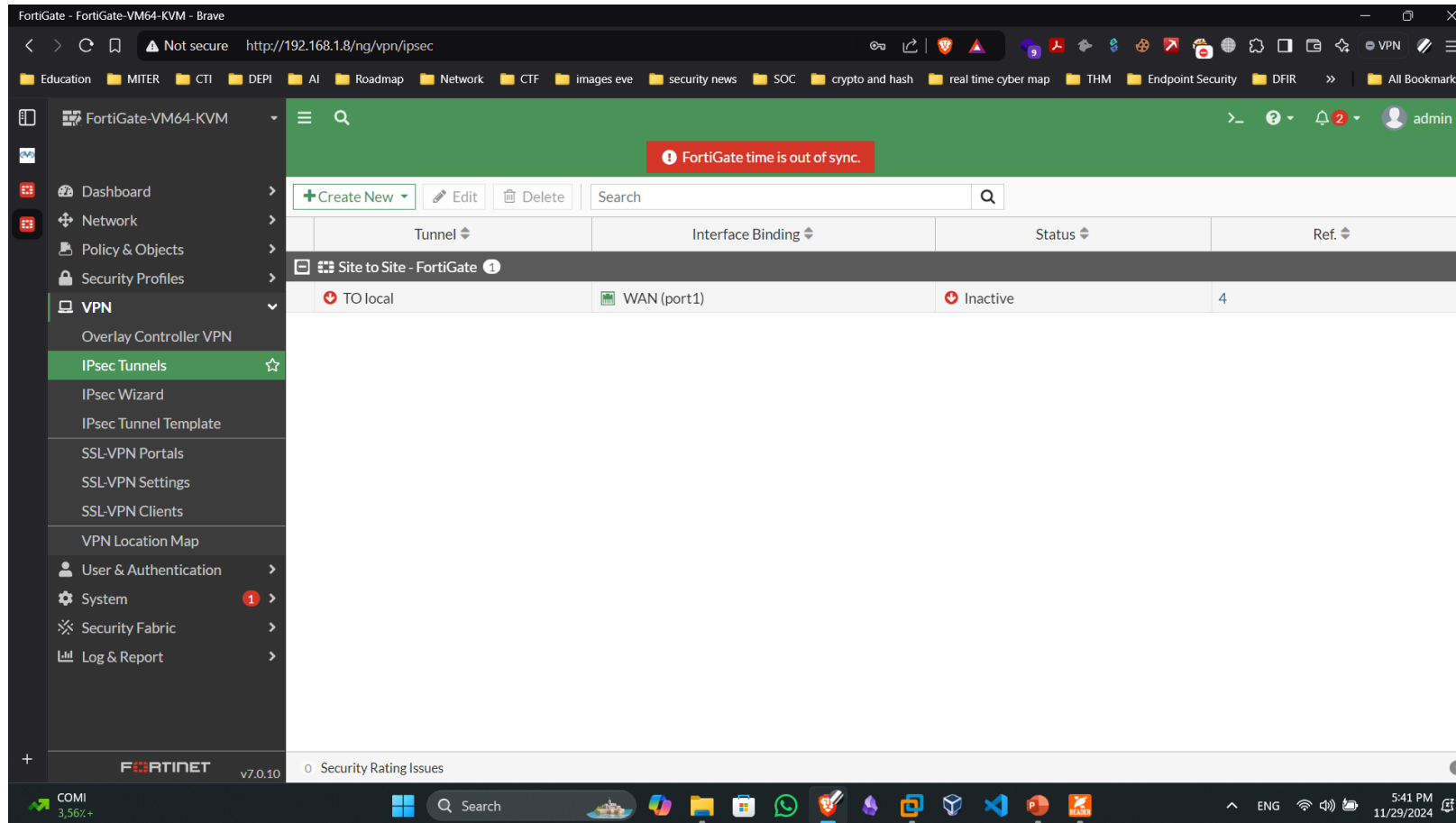
Site to Site - FortiGate



The diagram illustrates a Site-to-Site VPN configuration. On the left, a FortiGate device is labeled 'This FortiGate' and is enclosed in a green rectangular box. A line connects this device to a blue cloud icon labeled 'Internet'. Another line connects the 'Internet' cloud to a second FortiGate device on the right, labeled 'Remote FortiGate'.

< Back Next > Cancel

The Second site now ready:



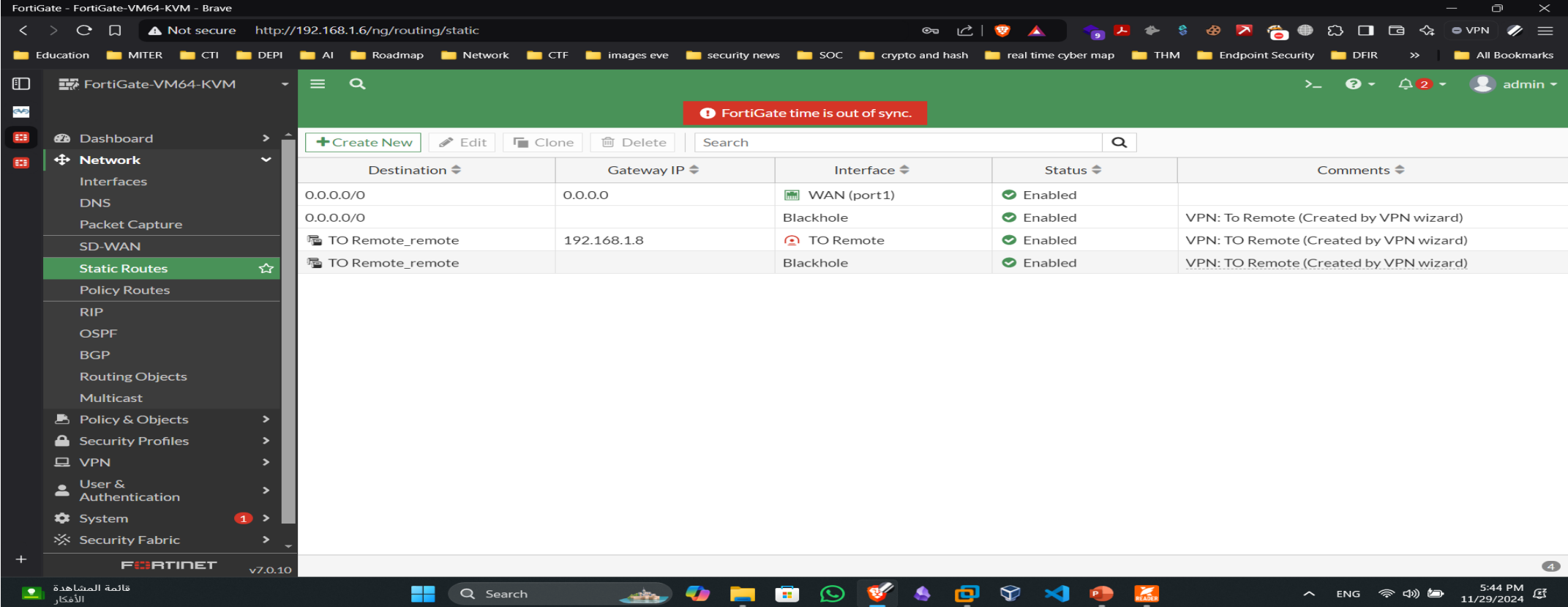
Back to the first site and show:

Because We use the wizard we just choose the configuration and don't make any custome configuration

So let set the configuration that done automatically with using the wizard

From the first side:

- Static routes adds automatic:



The screenshot displays the FortiGate VM64-KVM web interface. The left sidebar menu is expanded, showing the 'Static Routes' option under the 'Network' section. The main content area shows a table of static routes. A red banner at the top of the main content area indicates 'FortiGate time is out of sync.'.









Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	0.0.0.0	WAN (port1)	Enabled	
0.0.0.0/0		Blackhole	Enabled	VPN: To Remote (Created by VPN wizard)
TO Remote_remote	192.168.1.8	TO Remote	Enabled	VPN: TO Remote (Created by VPN wizard)
TO Remote_remote		Blackhole	Enabled	VPN: TO Remote (Created by VPN wizard)

The policy created automatic:

<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Policy Lookup</div><div>Search</div><div>Q</div><div>Export</div><div>Interface Pair View</div><div>By Sequence</div></div>										
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log		B
LAN (port2) → TO Remote 1										
vpn_TO Remote_local_0	TO Remote_local	TO Remote_remote	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM		0
TO Remote → LAN (port2) 1										
vpn_TO Remote_remote_0	TO Remote_remote	TO Remote_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM		0
Implicit 1										
Implicit Deny	all	all	always	ALL	DENY			Disabled		22.99 k

The secode or the remote site:

- Static routes :

<div><div>+ Create New</div><div>Edit</div><div>Clone</div><div>Delete</div><div>Search</div><div>Q</div></div>				
Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	0.0.0.0	 WAN (port1)	 Enabled	
0.0.0.0/0		Blackhole	 Enabled	
 TO local_remote	192.168.1.6	 TO local	 Enabled	VPN: TO local (Created by VPN wizard)
 TO local_remote		Blackhole	 Enabled	VPN: TO local (Created by VPN wizard)

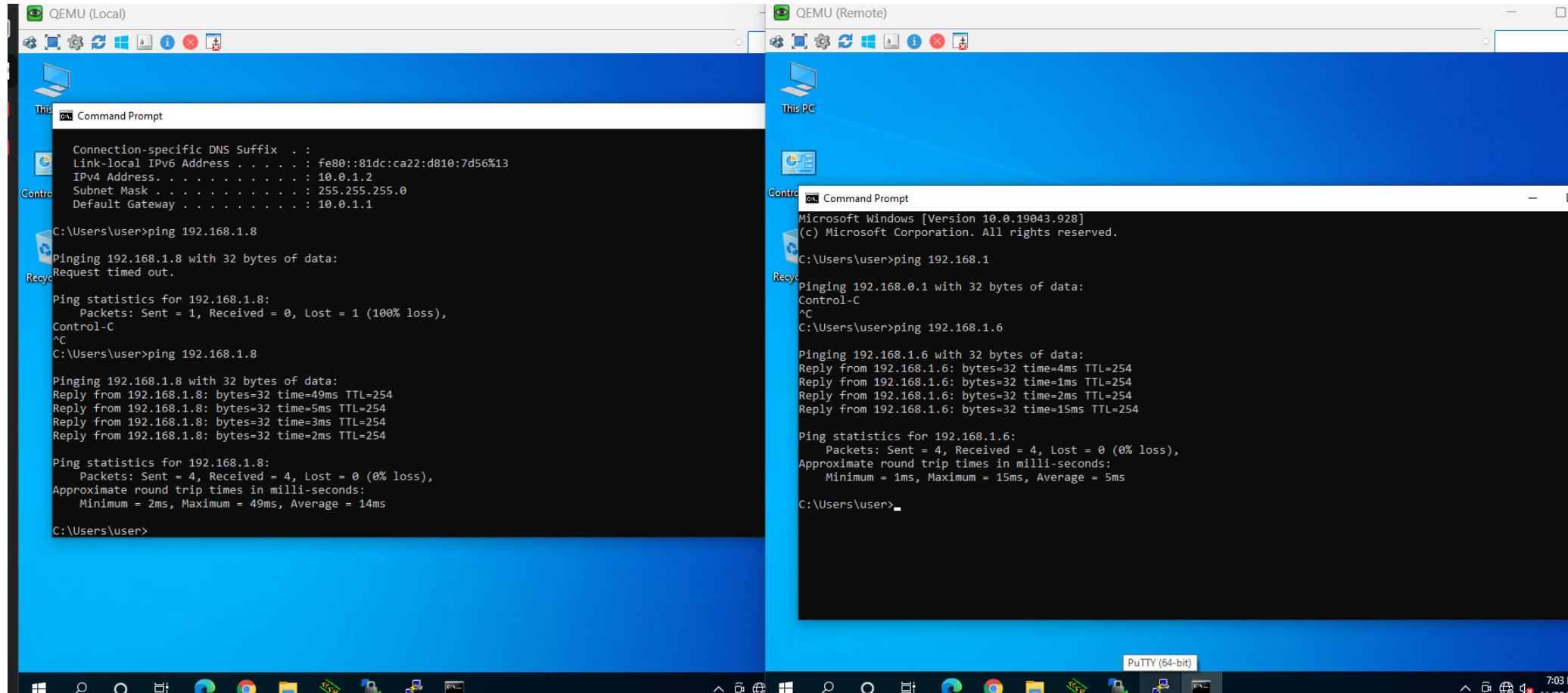
The policy created automatic:

[illegible]

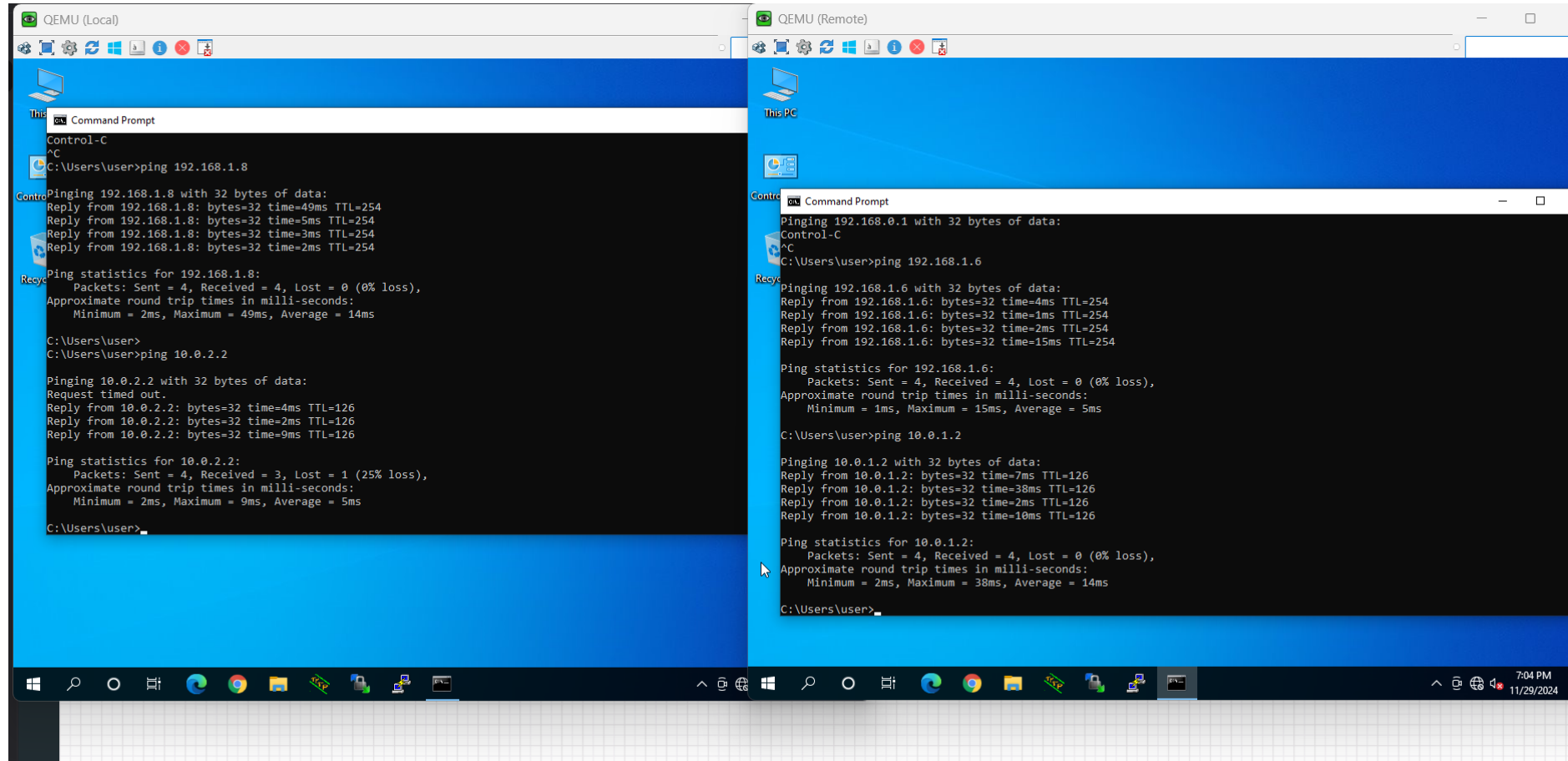


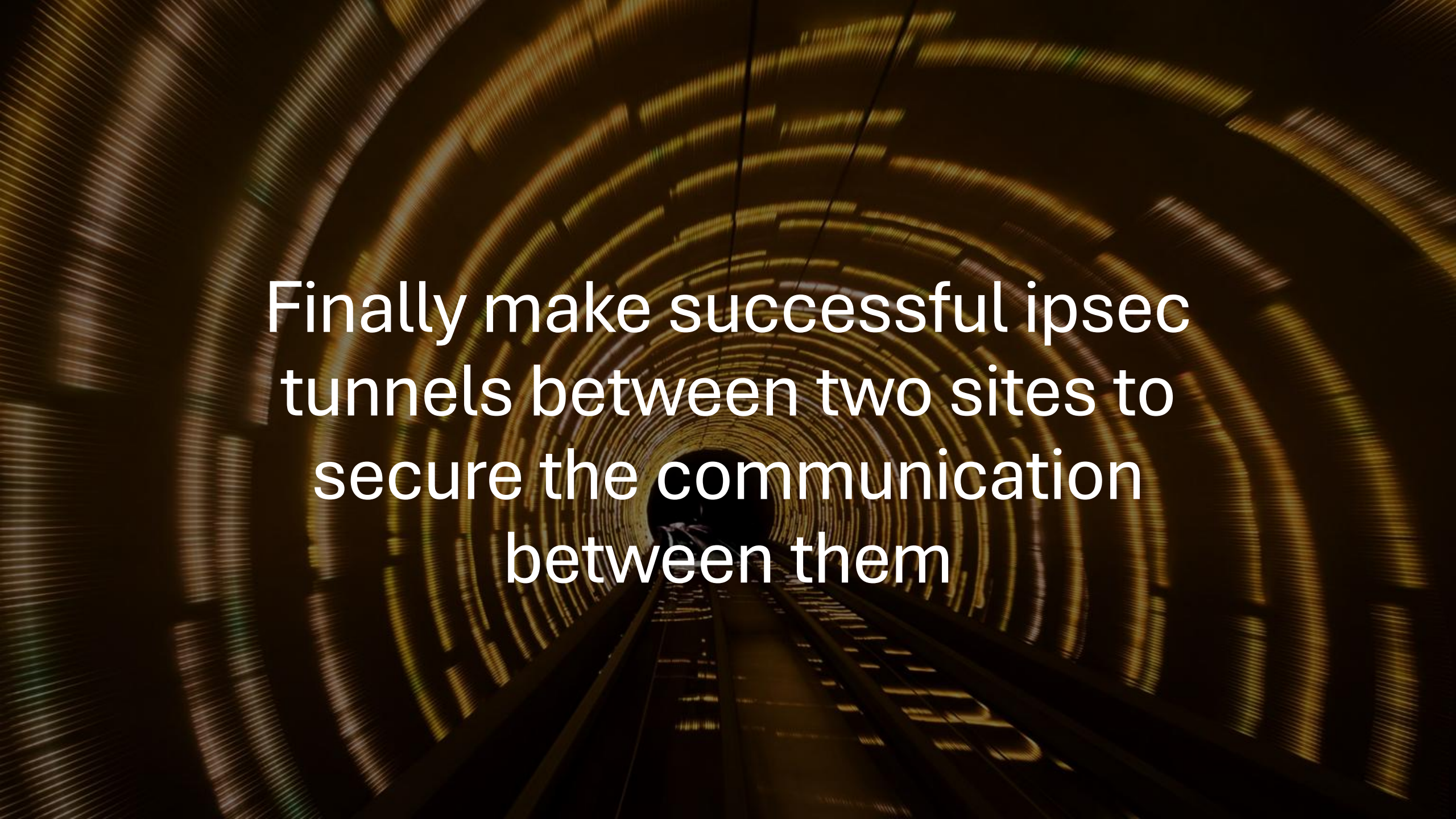
Now Lets Test Connectivity

Test Gateways:



Test connectivity between hosts





Finally make successful ipsec
tunnels between two sites to
secure the communication
between them



Q&A

LinkedIn: www.linkedin.com/in/momen-ameer-7b3032233

mail: momenameer2003@gmail.com



Thank you