DEPI Final Project

Fortinet Cybersecurity Engineer

Agenda

1 – what is VPN

2- site to site VPN

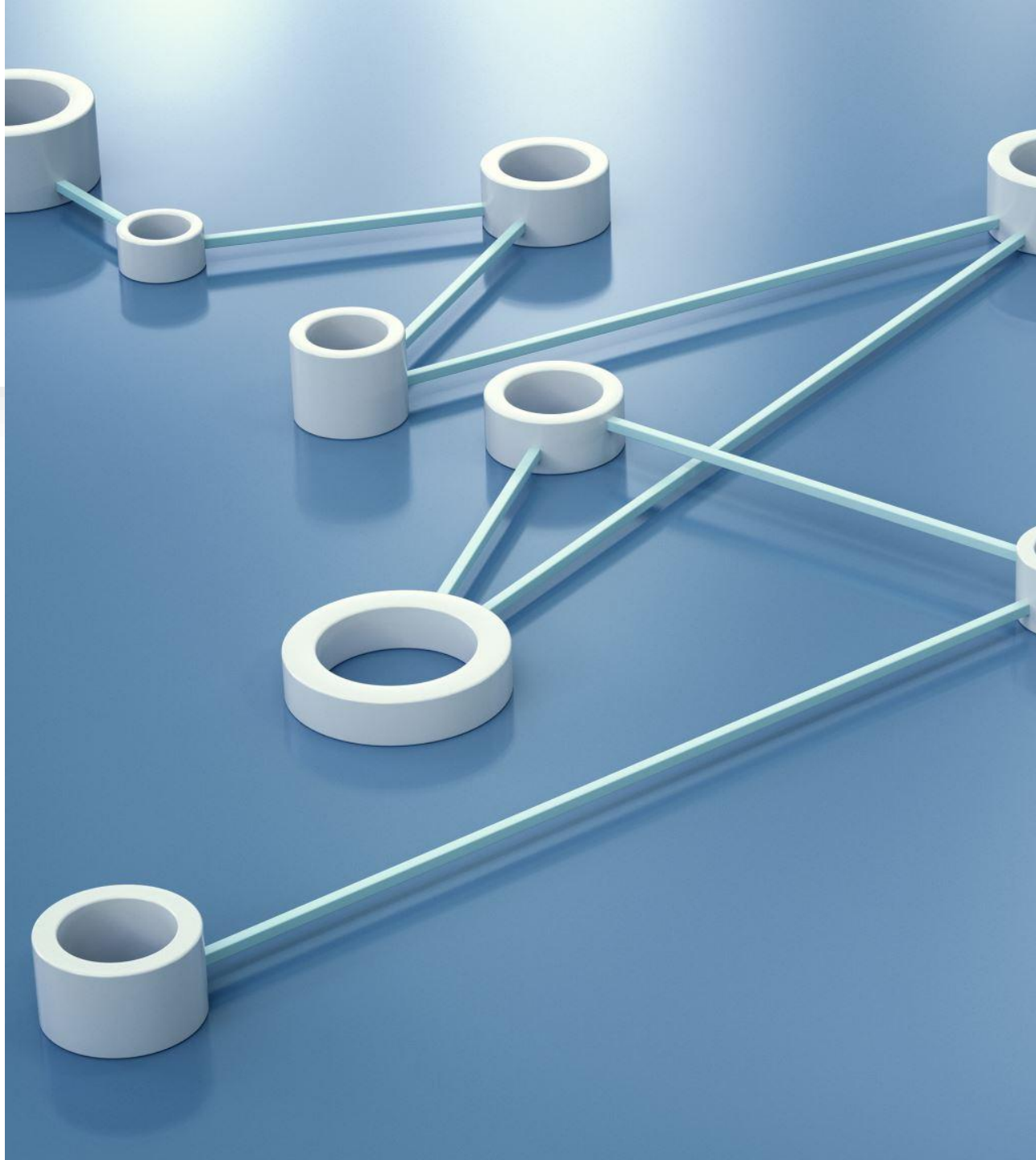
3 – ipsec VPN

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.

VPN Protocols

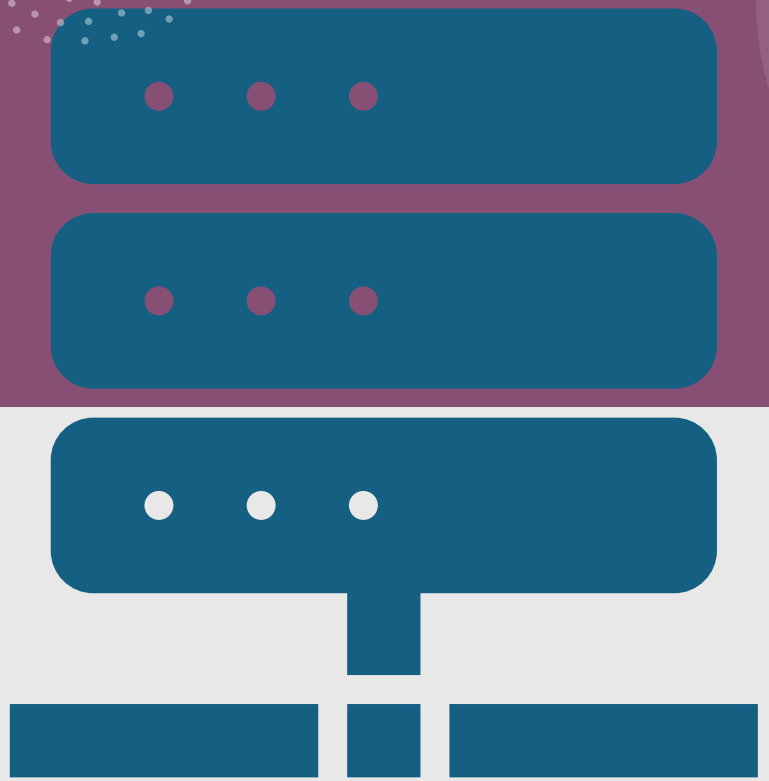
- VPNs can also be categorized based on the protocols they use:

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 **PPTP**: Fast but outdated and less secure.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:

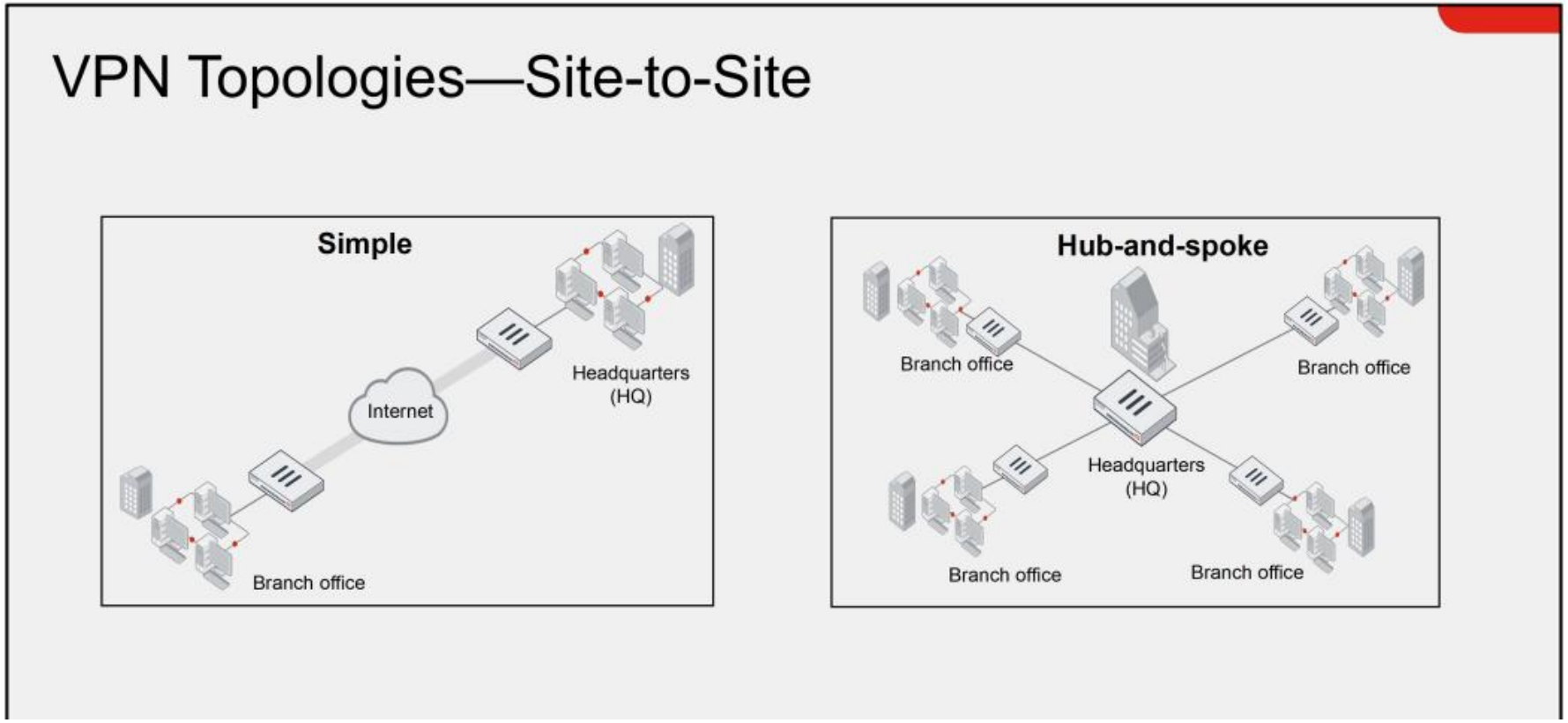
- **Purpose**: Connects entire networks (e.g., two office branches) over the internet securely.
- **Use Case**: Large organizations that need to interconnect geographically separated networks.
    - **How It Works**:
- Establishes a secure tunnel between routers or gateways of two networks.
- Subtypes:
    - **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:



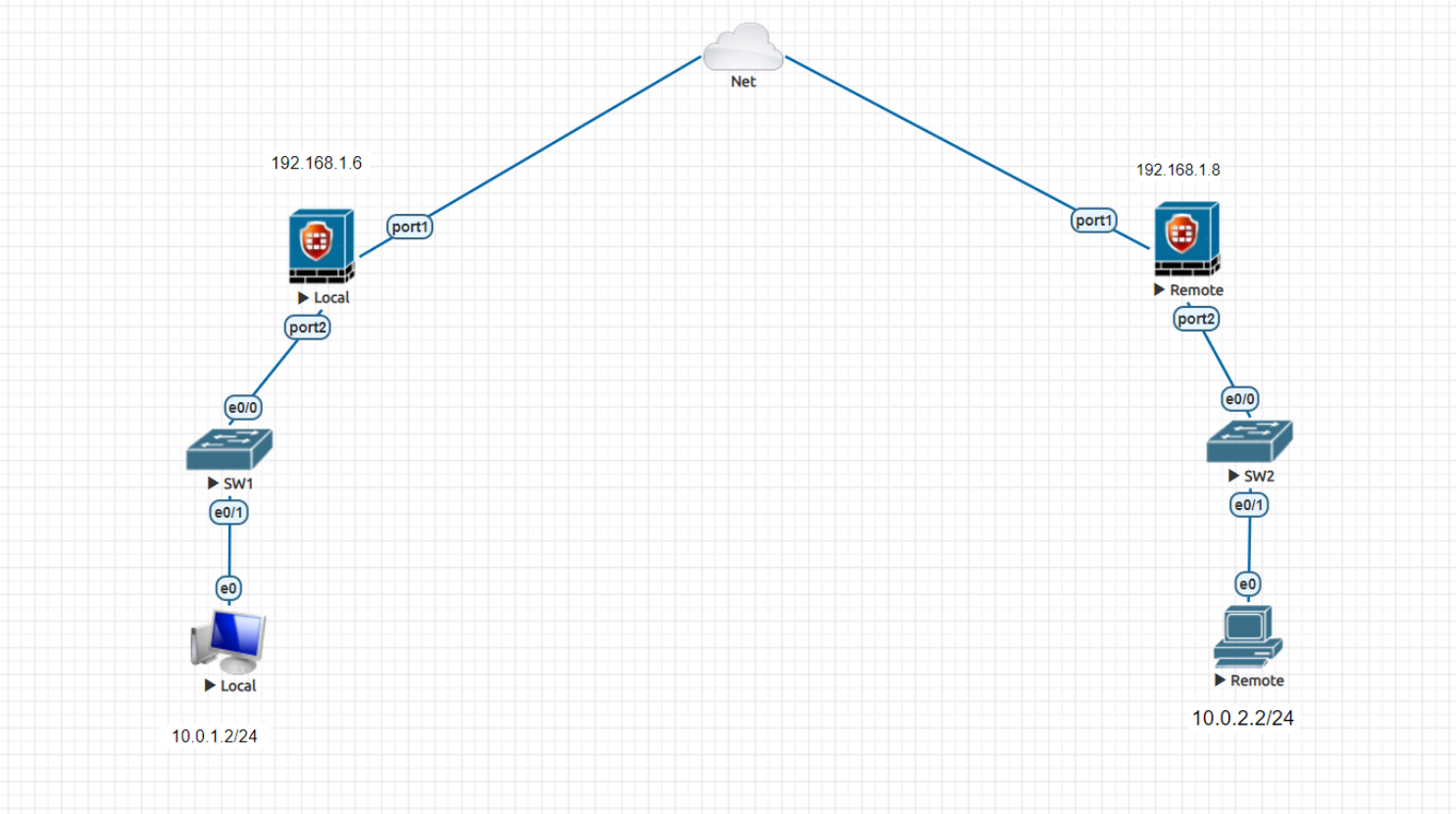
- What is IPsec? When should you use it?
  - IPsec is a vendor-neutral set of standard protocols that is used to join two physically distinct LANs. The LANs are joined as if they were a single logical network, despite being separated by the internet.

Site To Site Topologys:



Simple Topology and implementation on EVE Environment

Toplogy Will Work on



Methods to make ipsec Tunnle

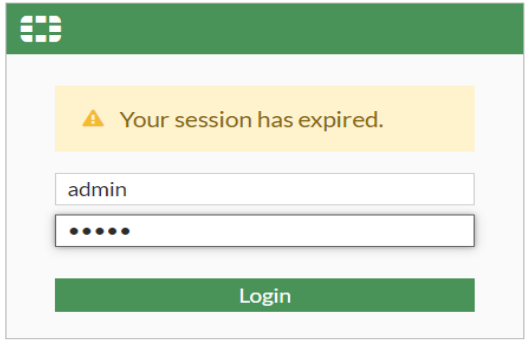
1 – Manually

2 – using Wizerd

So For simplicity we will use ipsec wizerd

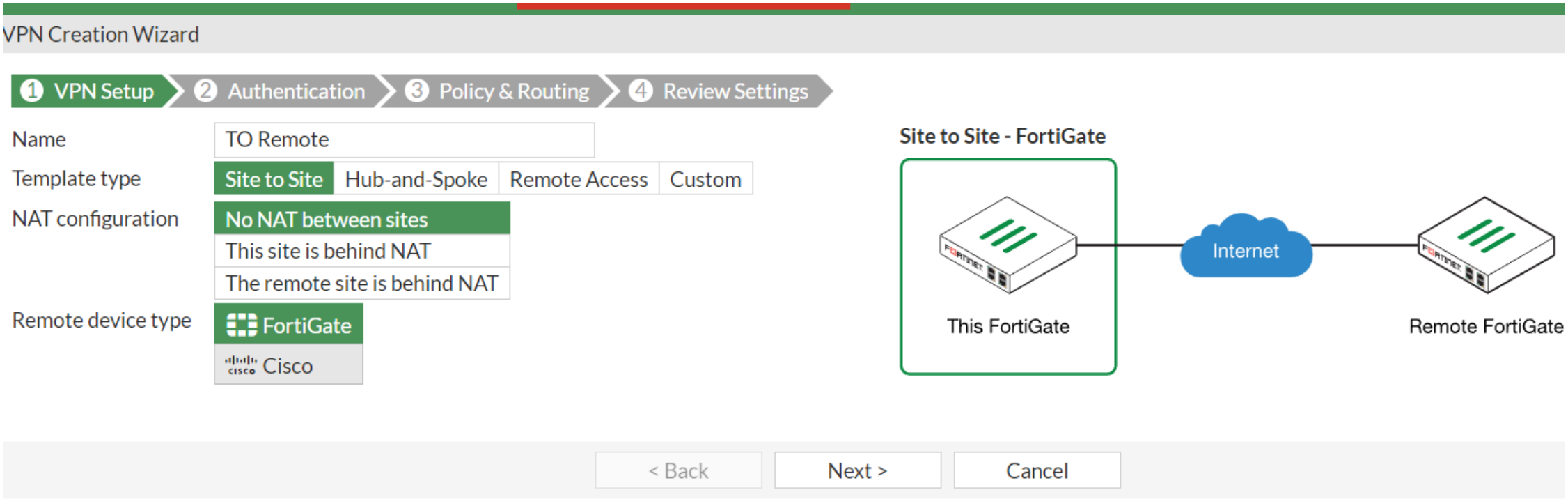
Ipsec using ipsec wizard in Fortigate:

- Local Fortigate:
  - Login:

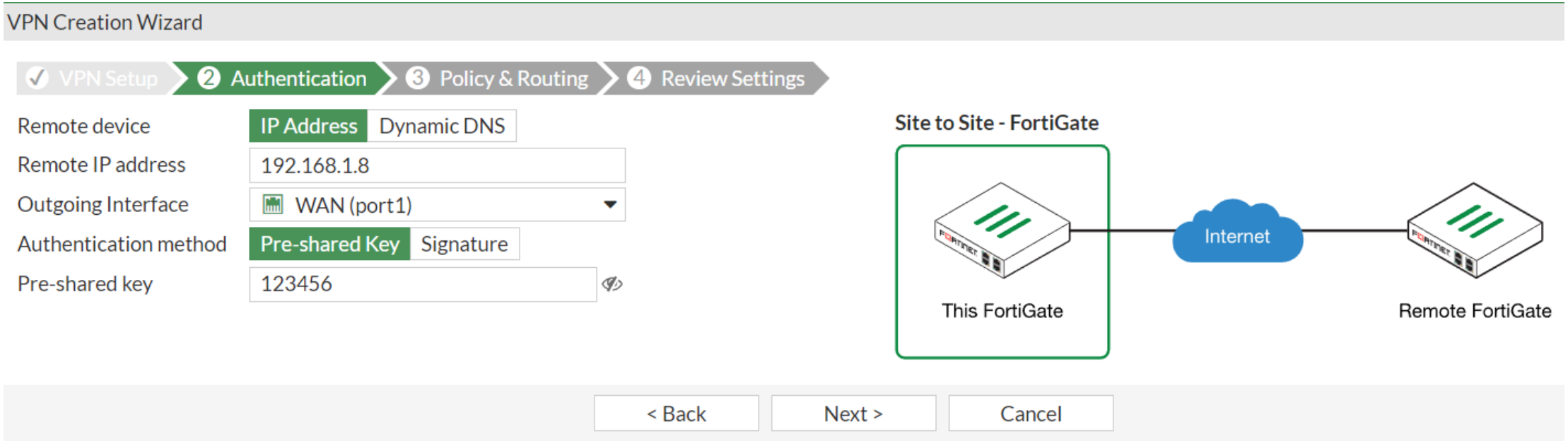


Go to vpn tab:

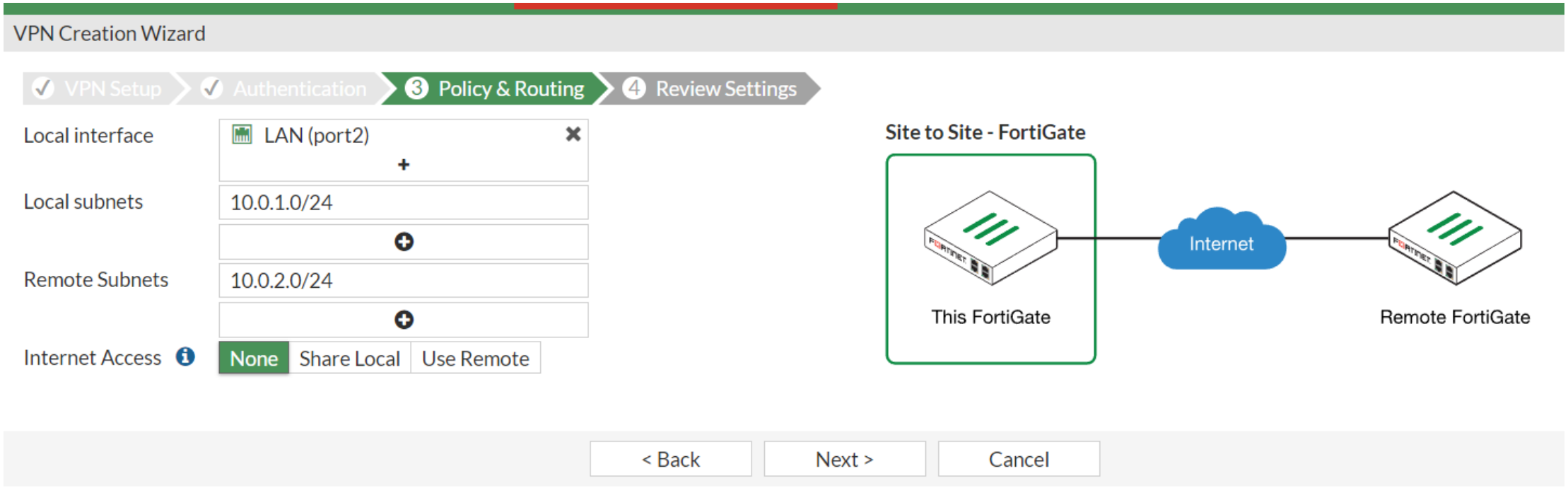
- 1 – select ipsec wizard
  - Then fill the information about the Remote site



Make the Authentication configuration



Make routing policy for forward the traffic



Finally review your configuration:

VPN Creation Wizard

✓ VPN Setup ✓ Authentication ✓ Policy & Routing 4 Review Settings

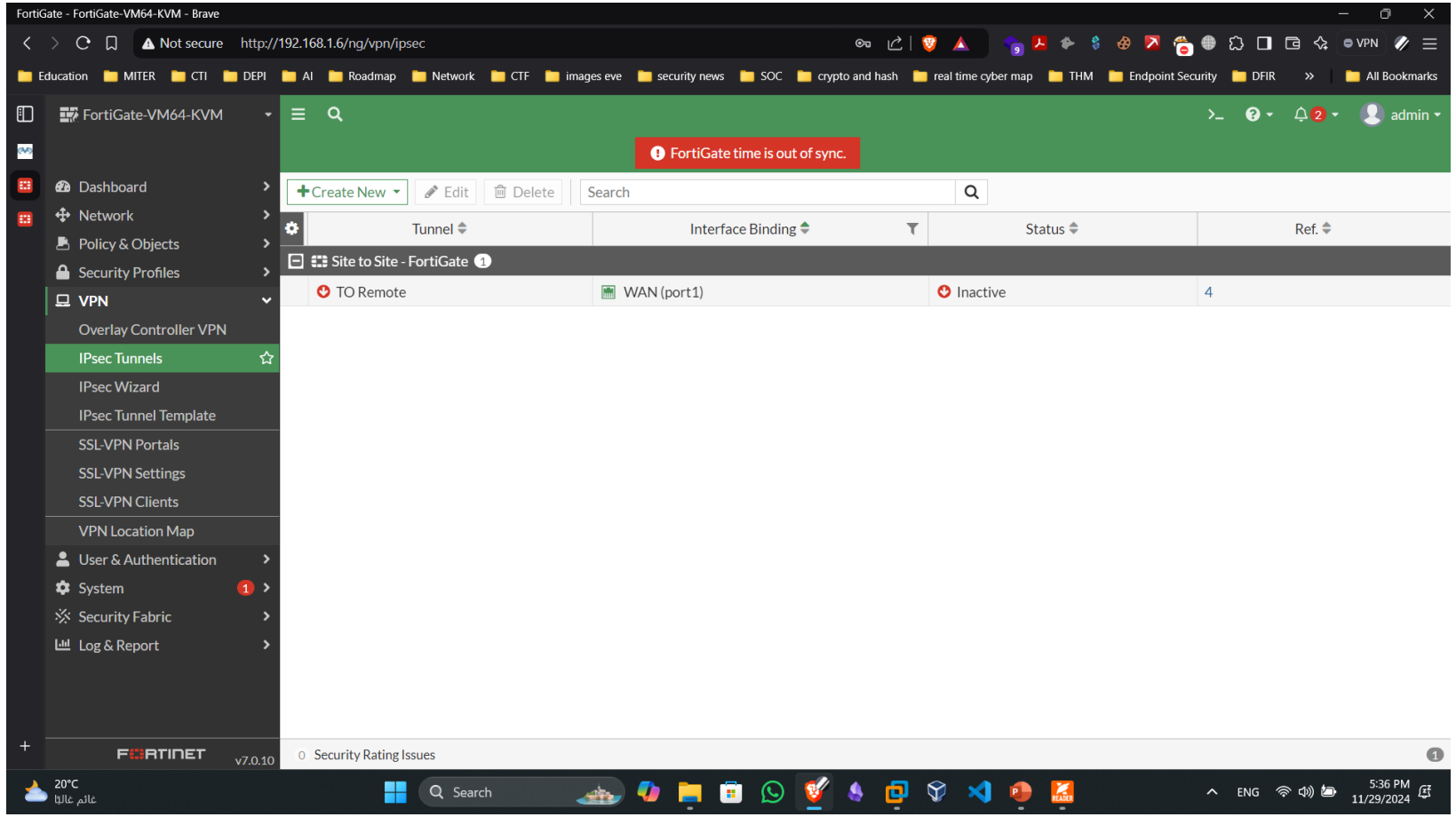
The following settings should be reviewed prior to creating the VPN.

Object Summary

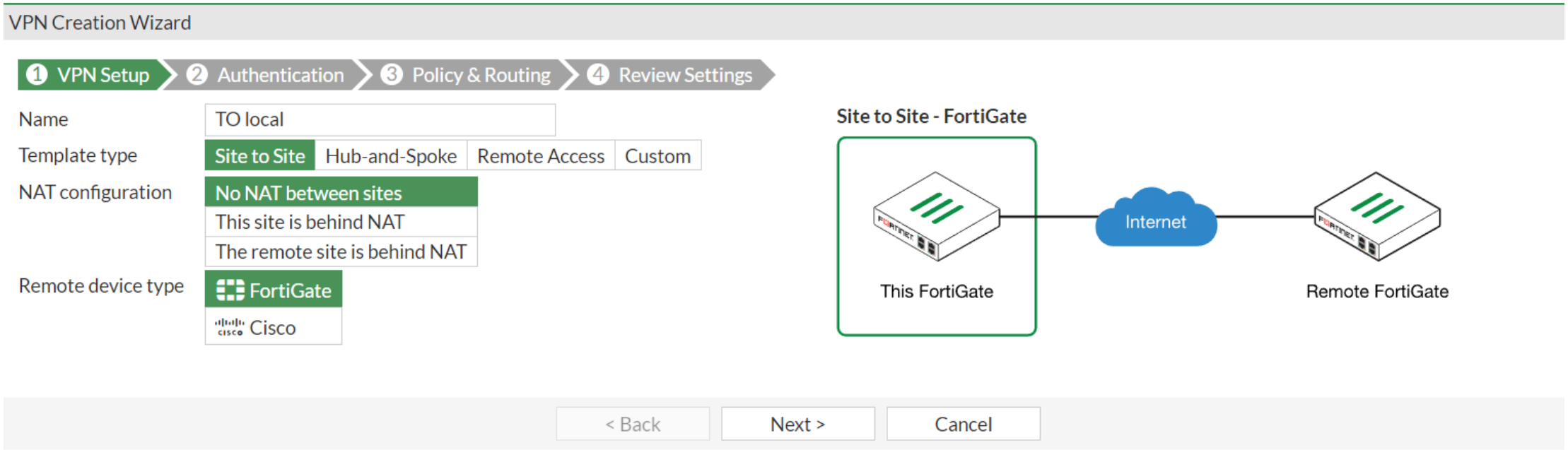
Phase 1 interface	TO Remote
Local address group	TO Remote_local
Remote address group	TO Remote_remote
Phase 2 interface	TO Remote
Static route	static
Blackhole route	static
Local to remote policies	vpn_TO Remote_local
Remote to local policies	vpn_TO Remote_remote

< Back | Create | Cancel

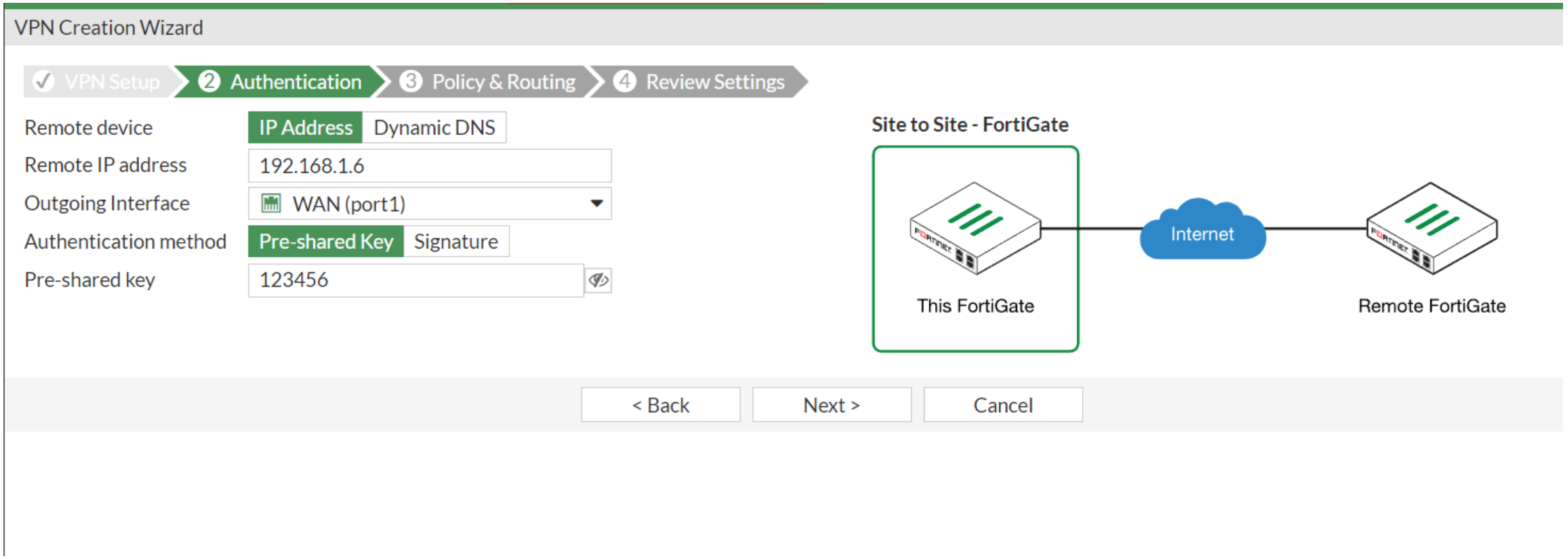
The First VPN site ready:



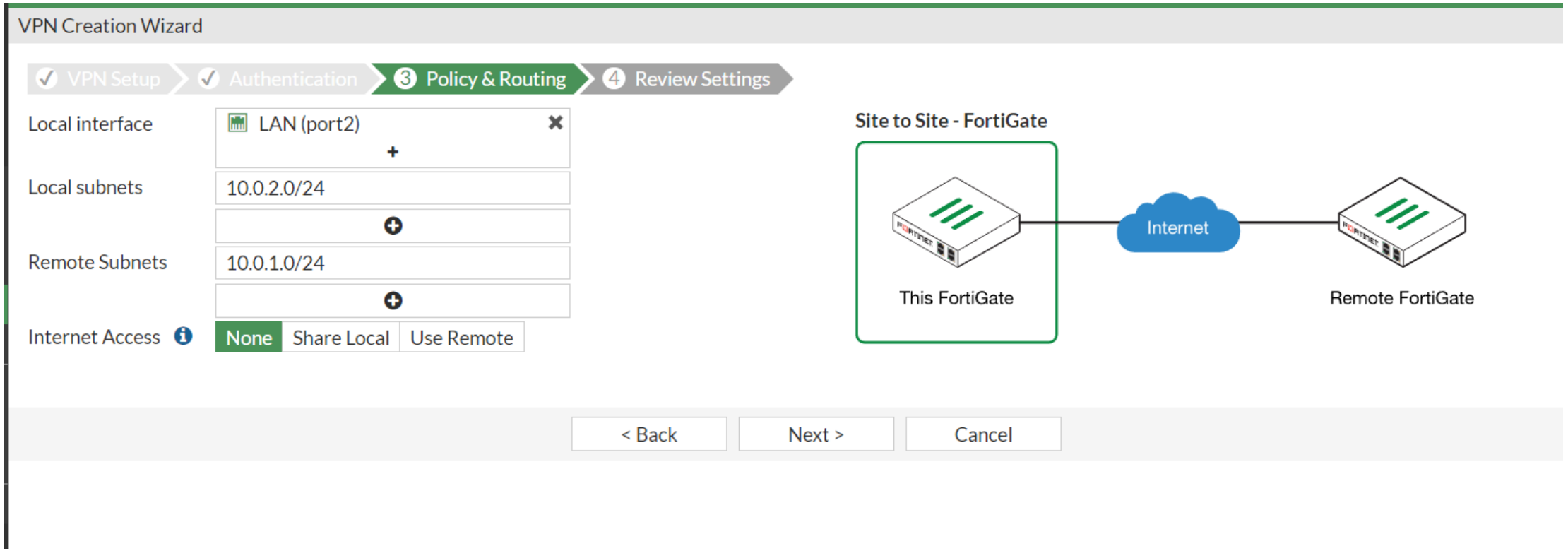
Go to the remote side the make the same conf



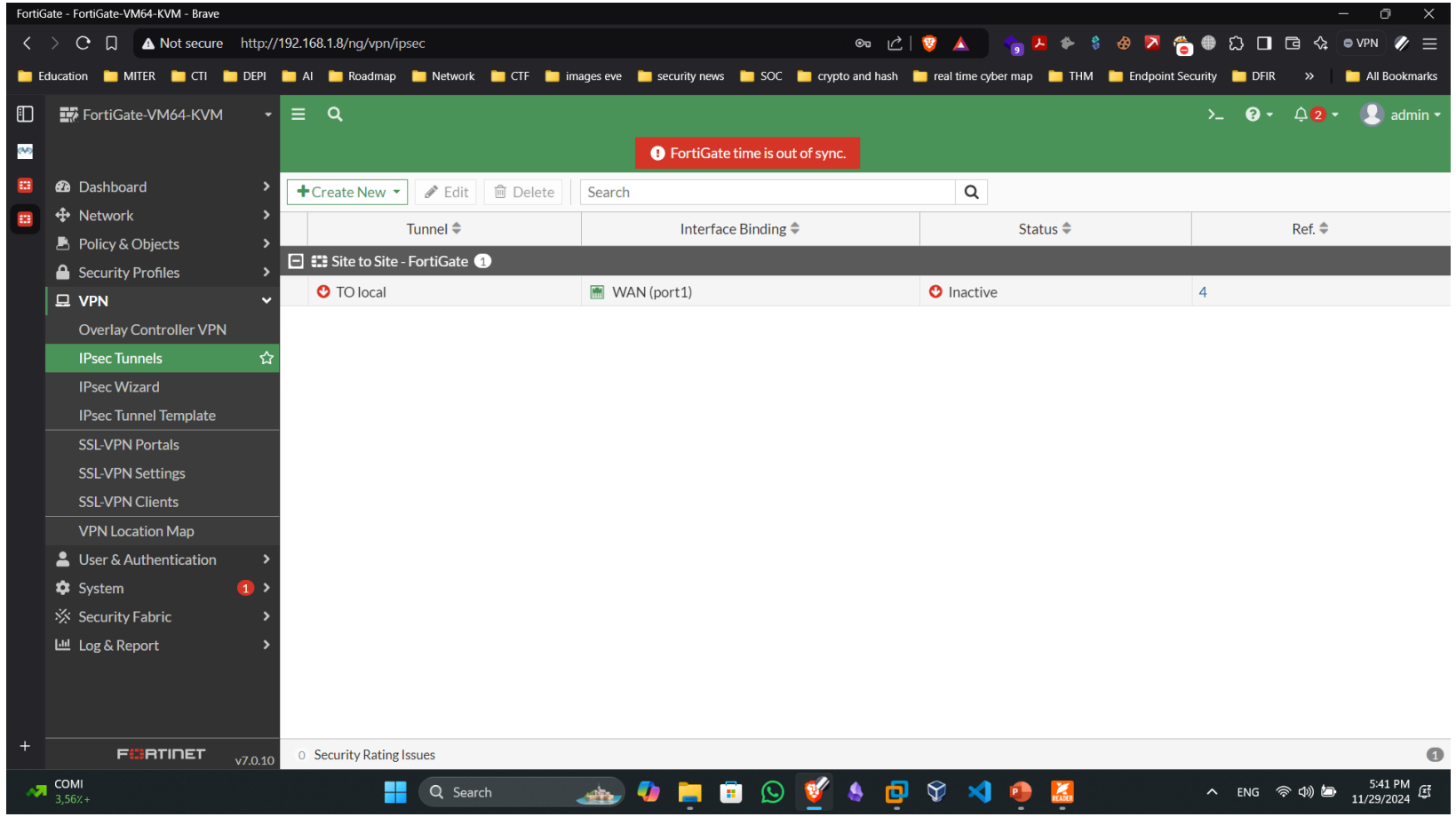
Choose your Remote IP and the interface



Choose what is the local and remote subnets:



The Second site now ready:



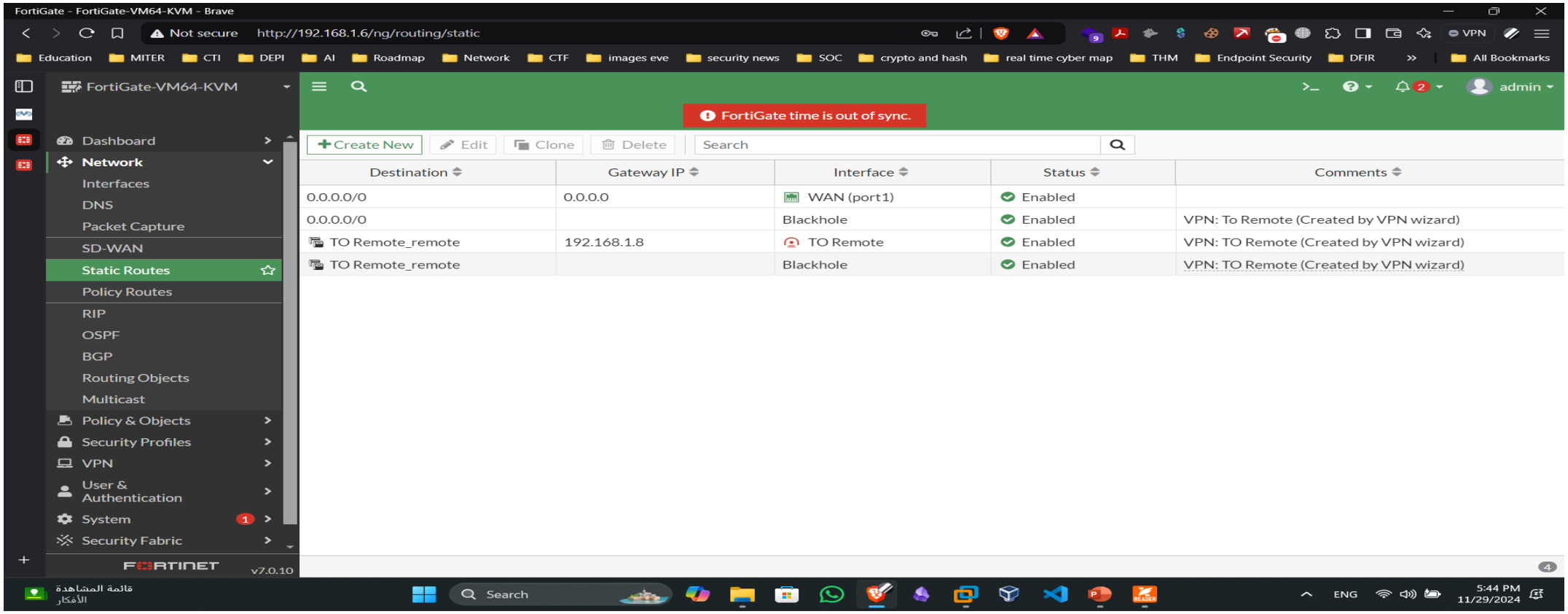
Back to the first site and show:

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

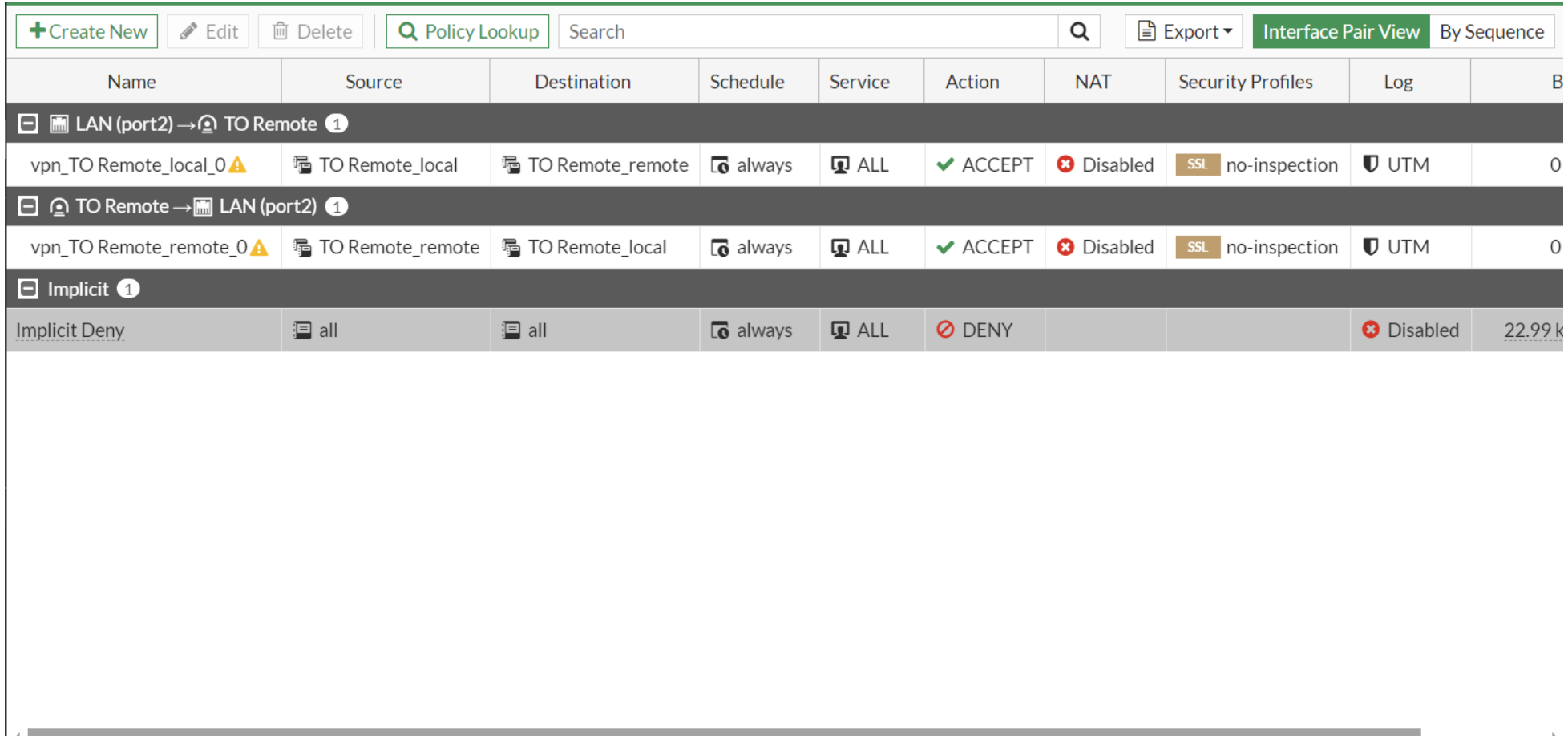
So let set the configuration that done automatically with using the wizard

From the first side:

- Static routes addes automatic:



The policy created automatic:



Create New | Edit | Delete | Policy Lookup | Search | Export | Interface Pair View | By Sequence

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

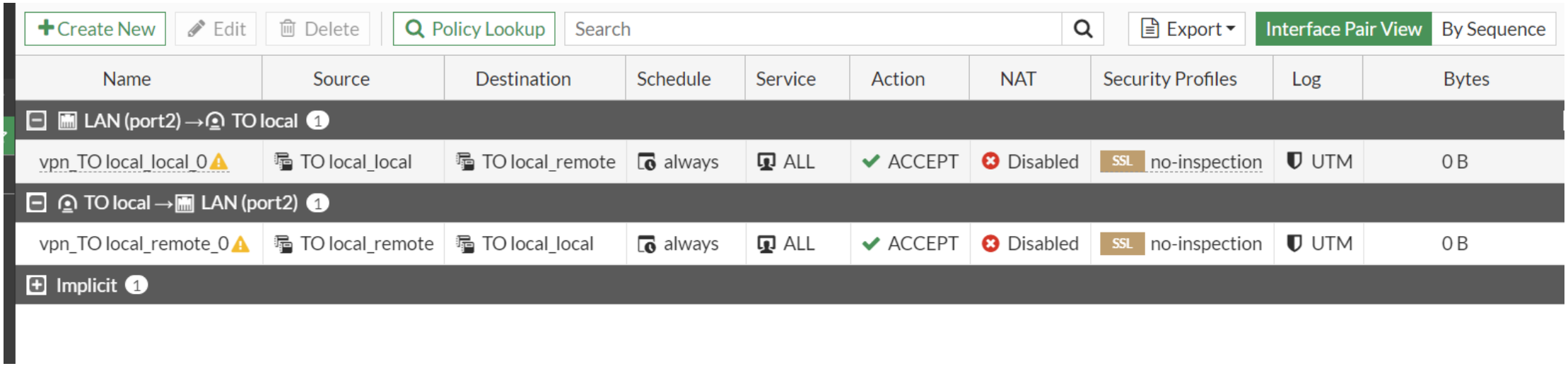
The secode or the remote site:

- Static routes :

Create New | Edit | Clone | Delete | Search

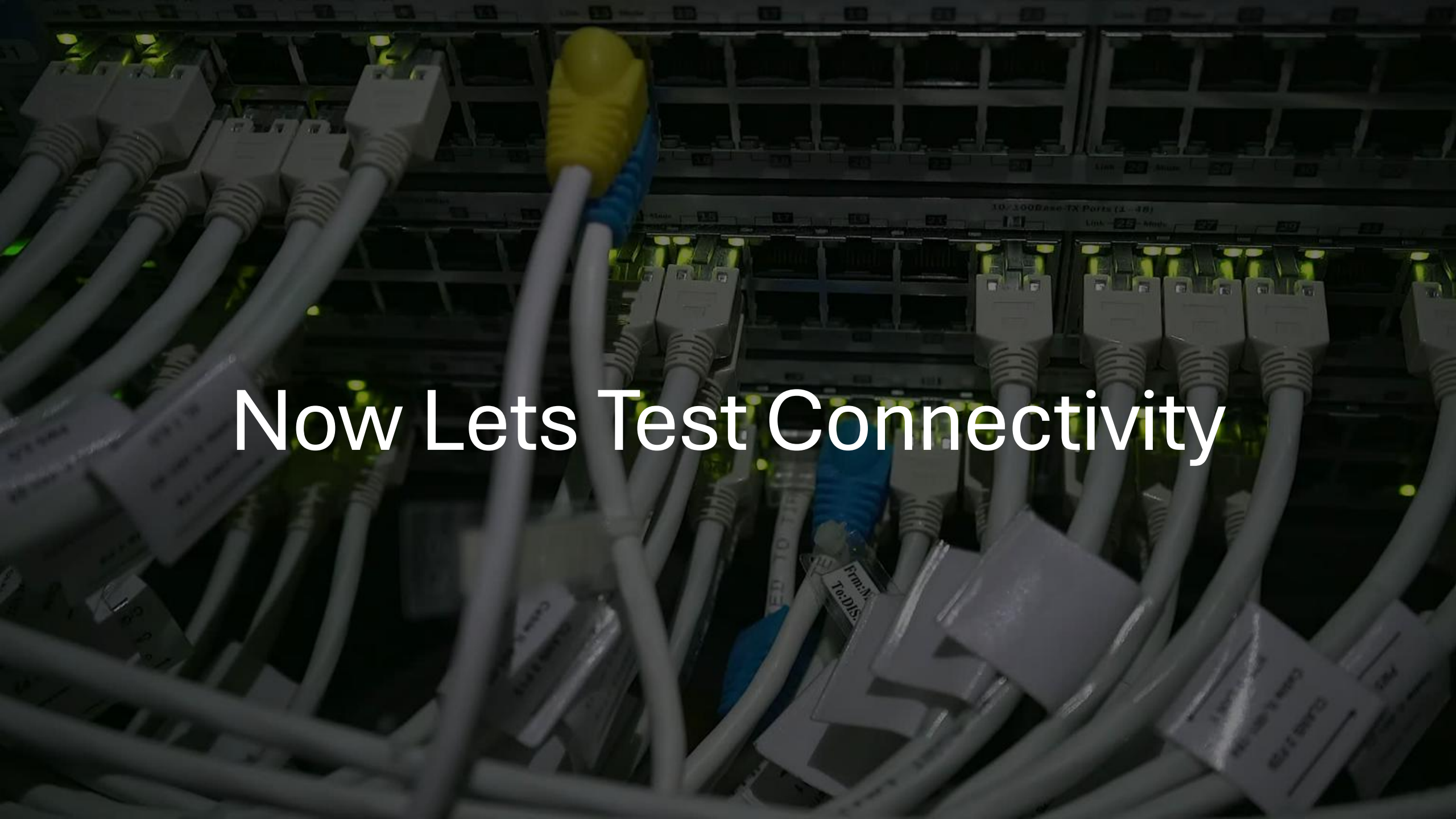
Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	0.0.0.0	WAN (port1)	Enabled	
0.0.0.0/0		Blackhole	Enabled	
TO local_remote	192.168.1.6	TO local	Enabled	VPN: TO local (Created by VPN wizard)
TO local_remote		Blackhole	Enabled	VPN: TO local (Created by VPN wizard)

The policy created automatic:



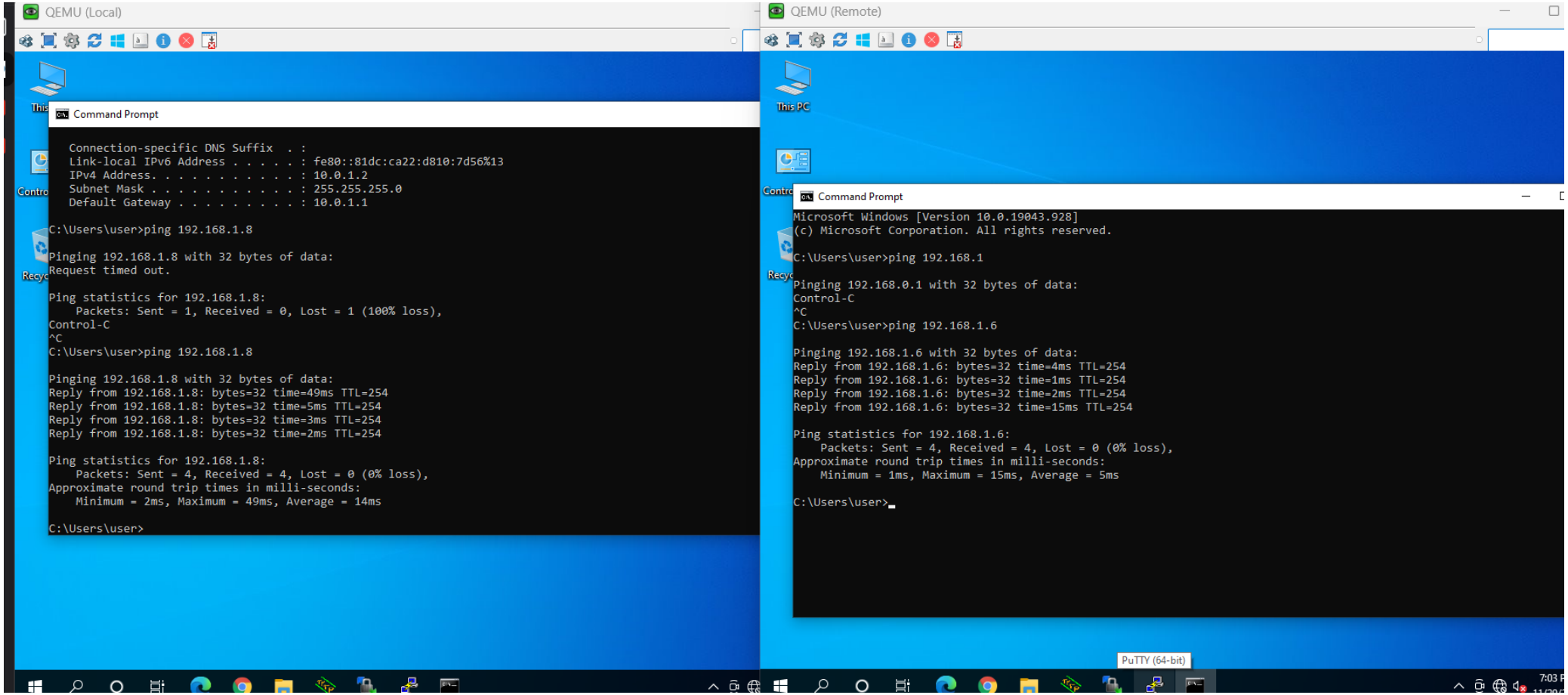
+Create New | Edit | Delete | Policy Lookup | Search | Export | Interface Pair View | By Sequence

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
LAN (port2) → TO local 1									
vpn_TO local_local_0	TO local_local	TO local_remote	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
TO local → LAN (port2) 1									
vpn_TO local_remote_0	TO local_remote	TO local_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit 1									

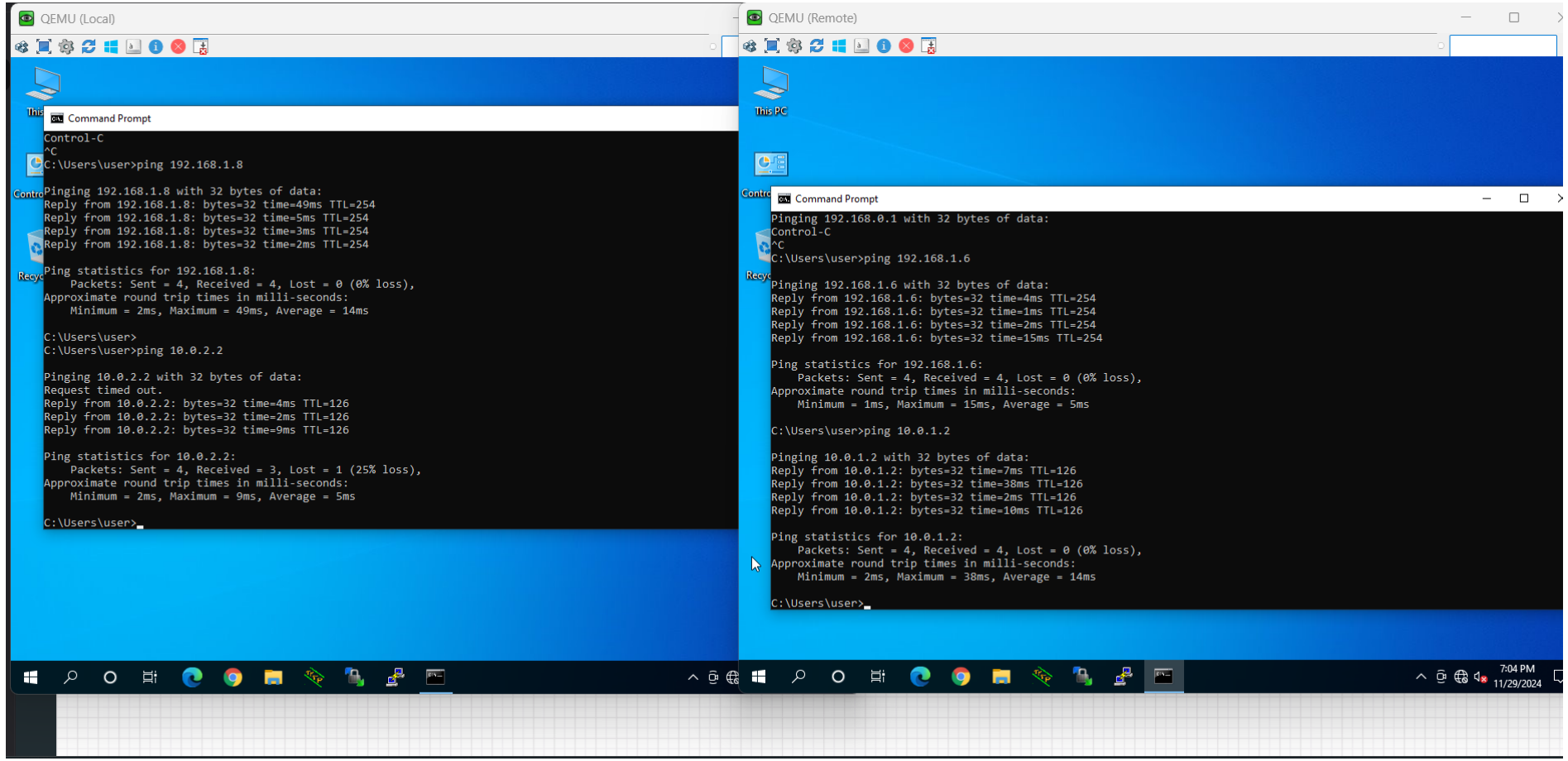


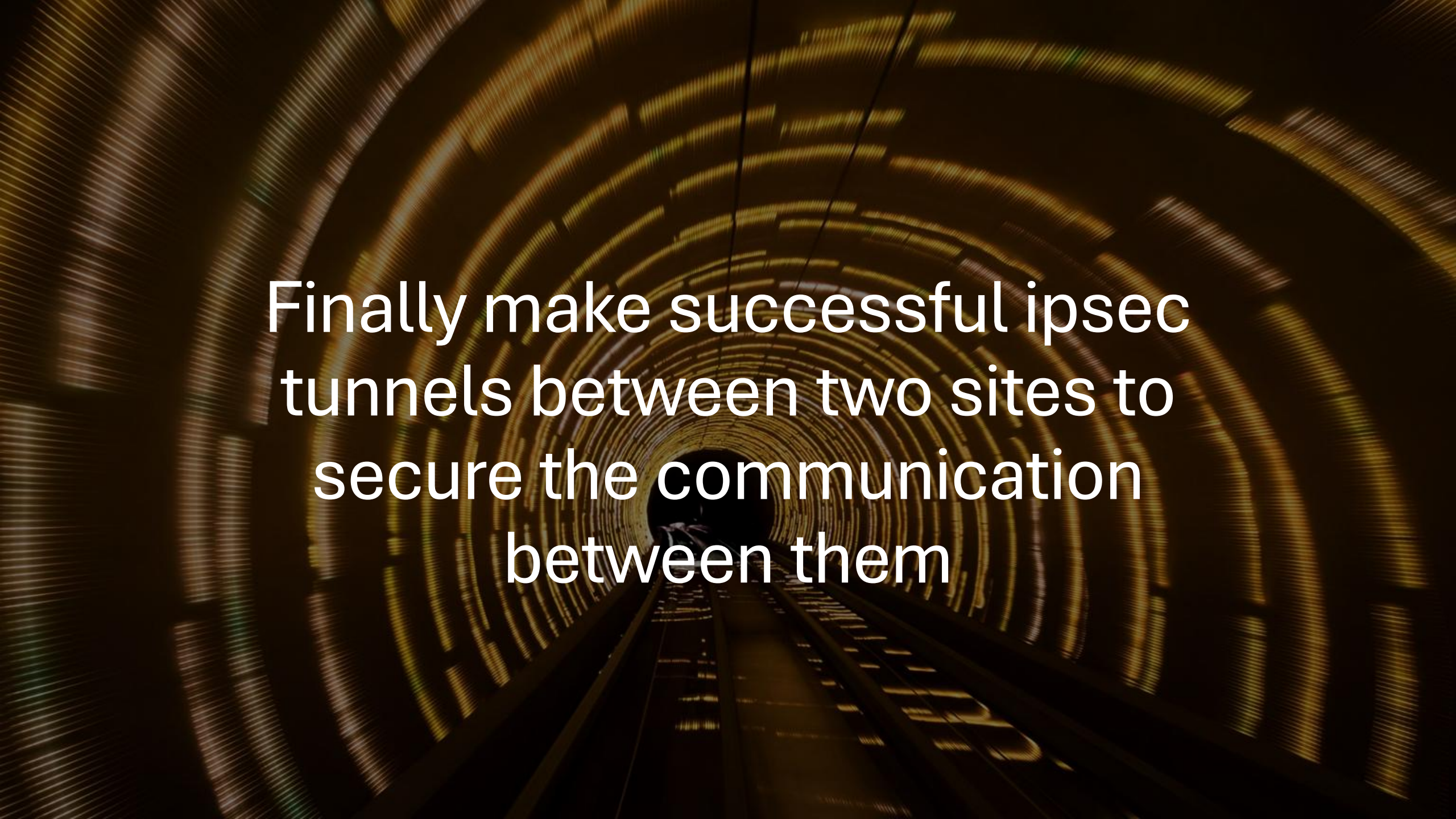
Now Lets Test Connectivity

Test Gatways:



Test connectivity between hosts



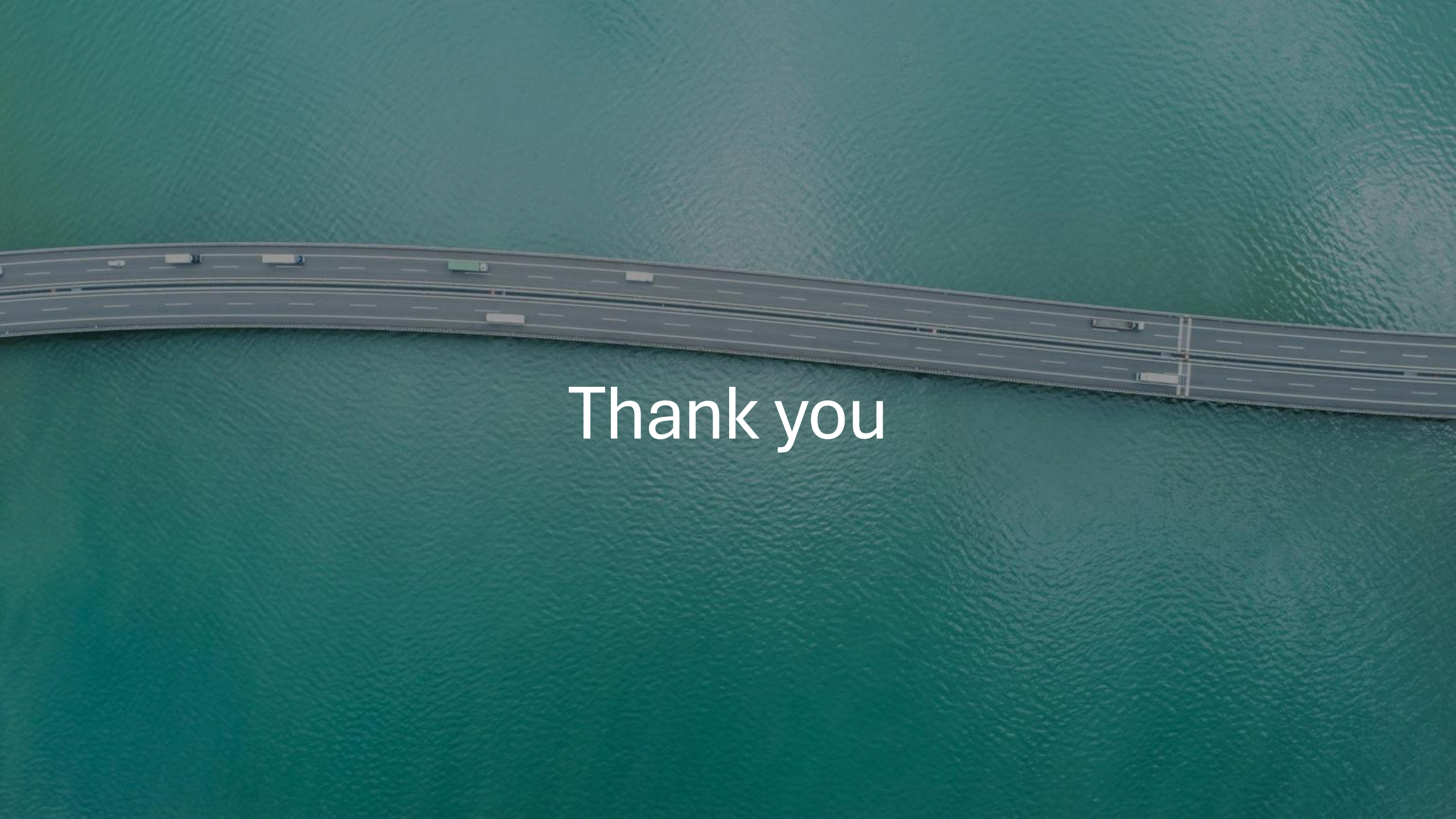


Finally make successful ipsec tunnels between two sites to secure the communication between them

Q&A

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

mail: momenameer2003@gmail.com



Thank you