

Configure a Replicating Multi-Site Domain using an IPsec VPN Tunnel

DOCUMENTATION

STEVEN FONSECA

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Contents

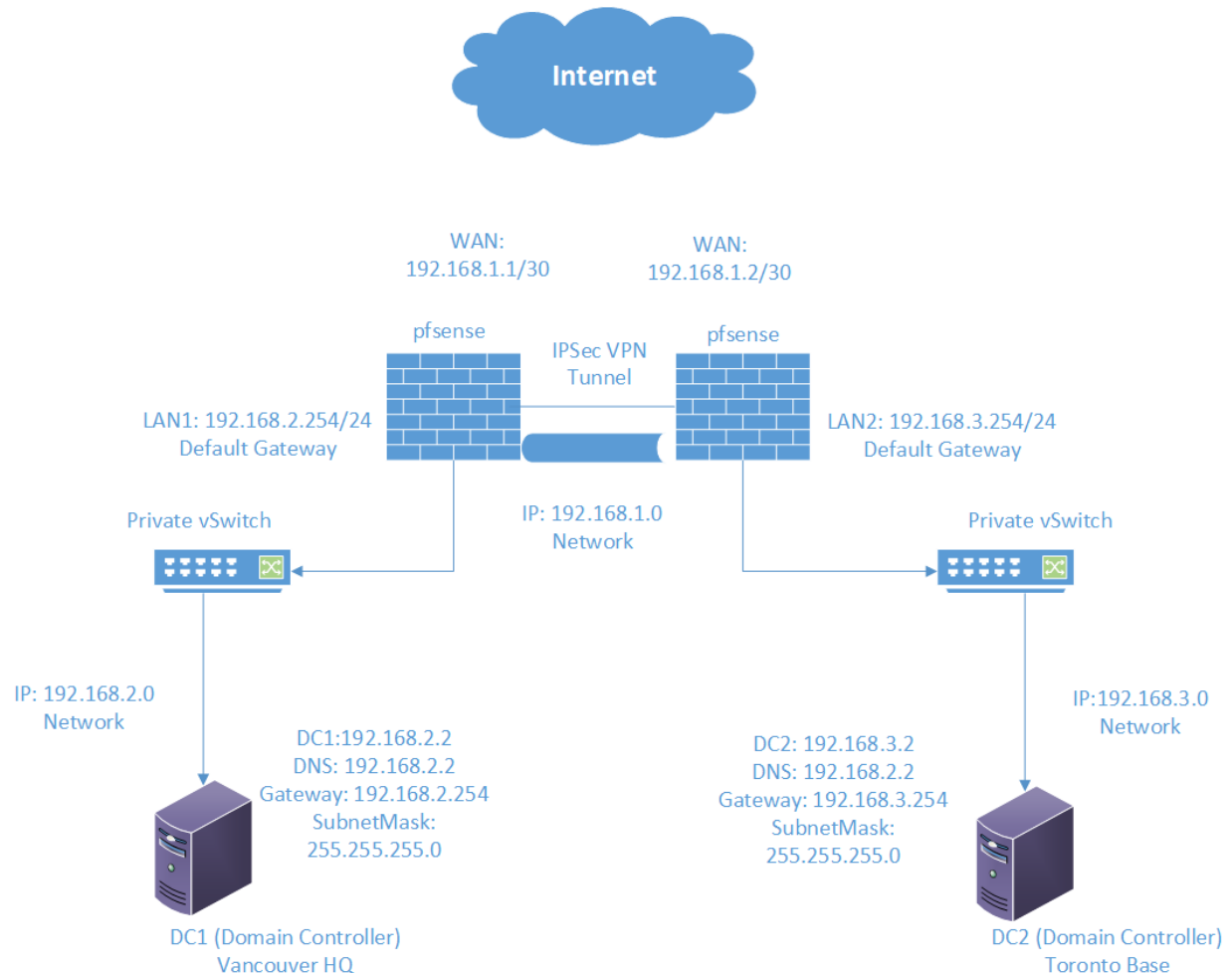
Network Diagram:.....	3
What is IPsec?.....	3
Create the Virtual Switches:	4
WAN IP Configuration Settings:	4
Configure the External Device:	5
VanRouter & TorRouter Configurations:.....	5
Update pfSense:.....	5
Remove the Default Switch / Attach the Private vSwitches:.....	5
Assign Static IPs:	6
Configure the WAN:.....	6
VanRouter:.....	6
TorRouter:.....	7
Configure the LAN:.....	8
VanRouter:.....	8
TorRouter:.....	9
Test Connectivity:	10
Firewall rules on pfSense for DC1 & DC2:	10
Ping WAN:.....	12
Ping LAN.....	13
Configure IPsec VPN Tunnel:.....	13
Phase 1 on DC1: Set up the VPN Endpoints:	13
Phase 2 on DC1: Set up the Tunnel Networks:.....	14
Phase 1 on DC2: Set up the VPN Endpoints:	15
Phase 2 on DC2: Set up the Tunnel Networks:.....	16
Post-Configuration:.....	17
Configure the Internal Devices:	18
DC1 > Vancouver:.....	18
DC2 > Toronto:.....	18
Connect the Vancouver Office to the Toronto Office Through IPsec Tunneling:	19
Create the Domain Controllers:	20

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Installation Steps for the First Domain Controller (DC1):.....	20
Create Secondary Disk for DC1:	20
Bring Disk Online DC1:	21
Promote to Domain Controller:	21
Installation Steps for the First Domain Controller (DC2):.....	22
Create Secondary Disk for DC2:	23
Bring Disk Online DC2:	23
Promote to Domain Controller:	23
Configure DNS:.....	27
Create Reverse Lookup Zone:	27
Create PTR Record:	30
Create/Configure Sites and Services within Active Directory:.....	31
Creating a new site through Active Directory Sites and Services:	31
Creating Subnets:.....	33
Creating Site Links:.....	35
Move the Domain Controllers to their newly created sites:	37
Test Replication:	39
Create an Object in the Vancouver DCs ADUC and see if that object is replicated to the Toronto DC:	40
Create an object in the Toronto DCs ADUC and see if that object is replicated to the Vancouver DC:	41
Create an A record in the Toronto's DC and see if it replicates to Vancouver's DC:	42
Create an A record in the Vancouver's DC and see if it replicates to Toronto's DC:	45
Create a new group policy (no settings need to be defined) in the Vancouver's DC and see if it replicates to Toronto's DC:	45
Create a new group policy (no settings need to be defined) in the Toronto's DC and see if it replicates to Vancouver's DC:.....	47
References:	48

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Network Diagram:



What is IPsec?

- What is IPsec and what is the purpose of using it to establish a VPN Tunnel?
 - o **IPsec**, which stands for **Internet Protocol Security**, is a suite of protocols designed to ensure the integrity, confidentiality, and authentication of data communications over an Internet Protocol (IP) network
 - o The primary purpose of using IPsec to establish a VPN tunnel is to create a secure and encrypted connection over a less secure network, like the internet
- Key Components:
 - o **Authentication**: Data is sent and received by the intended parties and not intercepted by an attacker
 - **Authentication Header (AH)** is one of the protocols used for this purpose
 - o **Encryption**: It encrypts data being transmitted, ensuring data cannot be read by unauthorized entities if intercepted

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- **Encapsulating Security Payload (ESP)** is the protocol used for encrypting data
- **Data Integrity**: Ensures data is not altered during transit
 - Both **AH** and **ESP** provide integrity checks
- **Secure Key Exchange**: IPsec uses **Internet Key Exchange (IKE)** to safely exchange cryptographic keys between the sender and receiver

Create the Virtual Switches:

- For this lab configuration, we will be utilizing a **Private vSwitch**
 - It allows VMs on a single Hyper-V host to communicate with each other but isolates them from the external network, which can be useful for testing network configurations and firewall rules
- Open Hyper-V Manager on Host Workstation
 - Access **Virtual Switch Manager**
 - Create **3** new *vSwitches*
 - Select "**Private**" > "**Create Virtual Switch**" for all 3
- **WAN vSwitch**: A vSwitch for the **192.168.1.0/30** network to establish a WAN link between both routing devices
- **LAN1 vSwitch**: A vSwitch for the **192.168.2.0/24** network. DC1 and the LAN interface of the first pfSense VM would connect to this vSwitch
- **LAN2 vSwitch**: A vSwitch for the **192.168.3.0/24** network. DC2 and the LAN interface of the second pfSense VM would connect to this vSwitch

WAN IP Configuration Settings:

- WAN facing subnet must only have two usable host IPs
- To create a subnet with only two usable host IPs:
 - We need a subnet that contains exactly four addresses in total, because in every subnet, one address is used for the **network address**, and one is reserved for the **broadcast address**. The remaining two addresses can be used for **hosts**. This configuration requires a **/30 subnet mask (255.255.255.252)**, which divides an IP address space into smaller subnets with four addresses each
- For our lab environment we will utilize the following static IPs for the WAN on both sites:
 - Network Address: **192.168.1.0**
 - Usable Host IPs: **192.168.1.1/30** and **192.168.1.2/30**
 - Subnet Mask: **255.255.255.252**

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Configure the External Device:

- Install two standalone pfSense Machines in Hyper-V, version 2.7.0
 - o **VanRouter**
 - o **TorRouter**

VanRouter & TorRouter Configurations:

- Use the pre-configured "**Default Switch**" to allow VM's to share the hosts network connection by using NAT (Network Address Translation)
 - o This switch can be used to temporarily provide internet access to a VM for updates or package installation before configuring the network according to the static IP setup

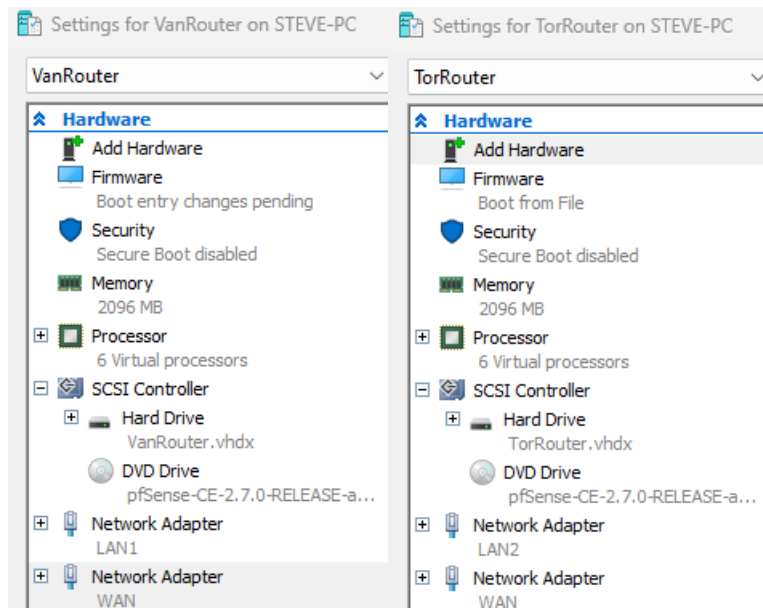
Update pfSense:

- o 1. *Run option 14 (sshd):*
 - **enable**
- o 2. *Run option 8 (shell):*
 - **opens command line interface**
- o 3. *Reinstall package database:*
 - **pkg-static bootstrap -f**
 - Ignore mismatch and select Y to continue
- o 3. *Update Package Repository Configuration:*
 - **cat /usr/local/etc/pkg/repos/pfSense.conf**
- o 4. *Fix Corrupted Package Database:*
 - **pkg-static clean -ay**
 - **pkg-static install -f pkg**
- o 5. *Check for Updates:*
 - **pfSense-upgrade**

Remove the Default Switch / Attach the Private vSwitches:

- After completing the updates, shut down both pfSense VMs (**VanRouter**) and (**TorRouter**)
- Go back to Hyper-V Manager and to the **Settings**
- Remove the "**Default Switch**" from the network adapter
- Attach the new private WAN/LAN1 vSwitch to VanRouter
- Attach the new private WAN/LAN2 vSwitch to TorRouter

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



Assign Static IPs:

- Start the pfSense VMs

Configure the WAN:

VanRouter:

- Access the pfSense console for **VanRouter** and configure the WAN interface with a static IP address (**192.168.1.1/30**)
 - o Option 2 > 1 for WAN

```
Enter an option: 2

Available interfaces:

1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) █
```

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

```
Enter the new WAN IPv4 address. Press <ENTER> for none:  
> 192.168.1.1  
  
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
     255.255.0.0   = 16  
     255.0.0.0     = 8  
  
Enter the new WAN IPv4 subnet bit count (1 to 32):  
> 30
```

- For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:
 - o Press Enter
- Configure IPv6 address WAN interface via DHCP6? (y/n)
 - o N
- Enter the new WAN IPv6 address. Press <ENTER> for none:
 - o Press Enter
- Do you want to enable the DHCP server on WAN? (y/n)
 - o N

```
The IPv4 WAN address has been set to 192.168.1.1/30  
You can now access the webConfigurator by opening the following URL in your web browser:  
  
http://192.168.1.1/  
  
Press <ENTER> to continue.
```

TorRouter:

- Access the pfSense console for **TorRouter** and ensure the WAN interface is also connected to the same "**WAN Private vSwitch**" and configure it with the other static IP (**192.168.1.2/30**)

```
Enter an option: 2  
  
Available interfaces:  
  
1 - WAN (hn0 - dhcp, dhcp6)  
2 - LAN (hn1 - static)  
  
Enter the number of the interface you wish to configure: 1  
  
Configure IPv4 address WAN interface via DHCP? (y/n)
```


CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 30
```

- For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:
 - o Press Enter
- Configure IPv6 address WAN interface via DHCP6? (y/n)
 - o N
- Enter the new WAN IPv6 address. Press <ENTER> for none:
 - o Press Enter
- Do you want to enable the DHCP server on WAN? (y/n)
 - o N

```
The IPv4 WAN address has been set to 192.168.1.2/30
You can now access the webConfigurator by opening the following URL in your web browser:

http://192.168.1.2/

Press <ENTER> to continue.
```

Configure the LAN:

VanRouter:

- Access the pfSense console for **VanRouter** and configure the LAN interface with a static IP address (**192.168.2.254/24**)
 - o Option 2 > 2 for LAN

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

- For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:
 - o Press Enter

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Configure IPv6 address WAN interface via DHCP6? (y/n)
 - o N
- Enter the new WAN IPv6 address. Press <ENTER> for none:
 - o Press Enter
- Do you want to enable the DHCP server on WAN? (y/n)
 - o N

```
The IPv4 LAN address has been set to 192.168.2.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
      http://192.168.2.254/
Press <ENTER> to continue.
```

TorRouter:

- Access the pfSense console for **TorRouter** and configure the LAN interface with a static IP address (**192.168.3.254/24**)
 - o Option 2 > 2 for LAN

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.3.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

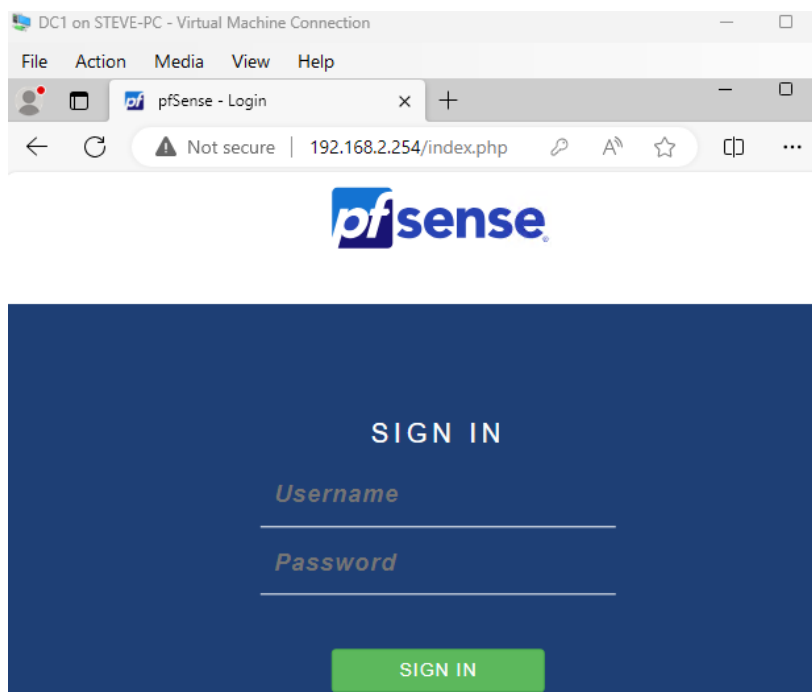
- For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none:
 - o Press Enter
- Configure IPv6 address WAN interface via DHCP6? (y/n)
 - o N
- Enter the new WAN IPv6 address. Press <ENTER> for none:
 - o Press Enter
- Do you want to enable the DHCP server on WAN? (y/n)
 - o N

```
The IPv4 LAN address has been set to 192.168.3.254/24
You can now access the webConfigurator by opening the following URL in your web browser:
      http://192.168.3.254/
Press <ENTER> to continue.
```

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Test Connectivity:

- Verify that the two pfSense VMs can communicate with each other over the WAN interfaces by using the ping command from the pfSense console
- To do this we must allow PING on pfSense WAN via the Firewall rule setting on both Routers
- Navigate to Edge browser on **DC1** > We can access the pfSense Dashboard GUI by entering the Default Gateway on **LAN1** which is **192.168.2.254**

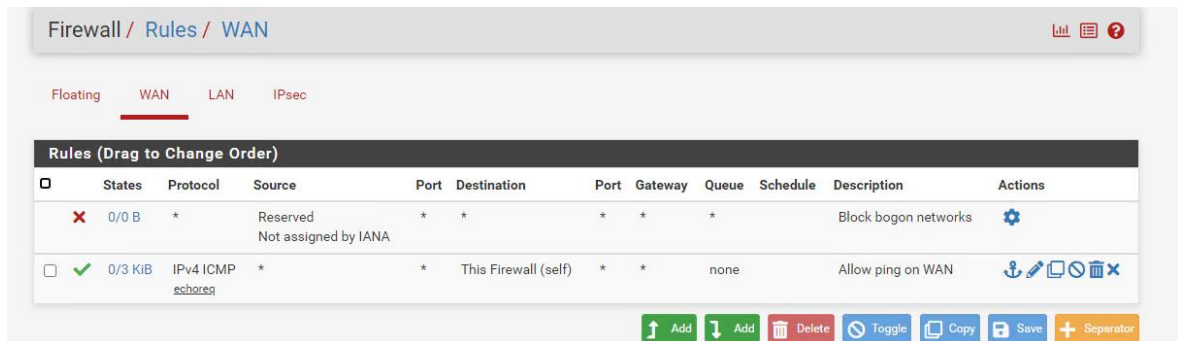


- Sign in using the default username and password:
 - o **admin/pfsense**

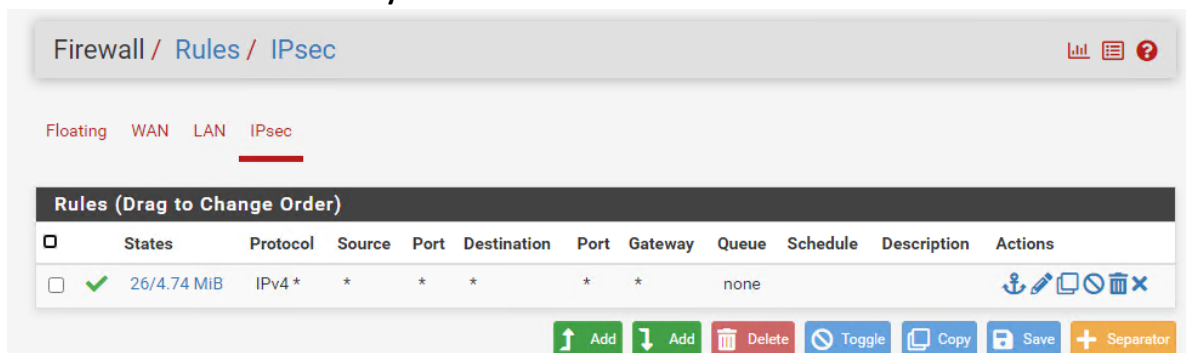
Firewall rules on pfSense for DC1 & DC2:

- Go to > **Firewall** > **Rules** > **WAN** (To allow PING from WAN to WAN)
 - o Create a new rule by clicking Add
 - Action: **Pass**
 - Protocol: **ICMP**
 - ICMP subtypes: **Echo Request**
 - Source: **any**
 - Destination: **This Firewall**
 - Description: **Allow ping on WAN**
 - Save > **Apply**

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- Go to > **Firewall** > **Rules** > **IPsec** (To allow IPv4 traffic to pass from site 1 to site 2)
 - Action: **Pass**
 - Interface: **IPsec**
 - Address Family: **IPv4**
 - Protocol: **Any**
 - Source: **Any**
 - Destination: **Any**



- Navigate to Edge browser on **DC2** > We can access the pfSense Dashboard GUI by entering the Default Gateway on **LAN2** which is **192.168.3.254**
- Go to > **Firewall** > **Rules WAN**
 - Create a new rule by clicking **Add**
 - Action: **Pass**
 - Protocol: **ICMP**
 - ICMP subtypes: **Echo Request**
 - Source: **any**
 - Destination: **This Firewall**
 - Description: **Allow ping on WAN**

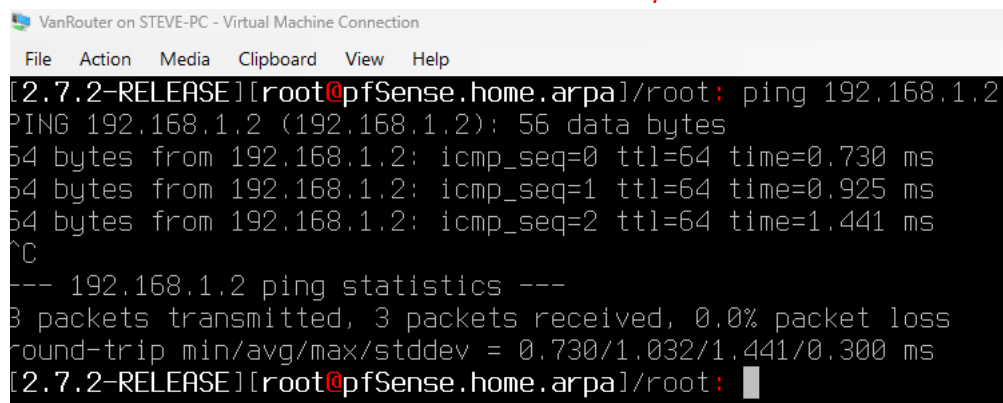
CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Save > **Apply**
- Go to > **Firewall > Rules > IPsec** (To allow IPv4 traffic to pass from site 2 to site 1)
 - Action: **Pass**
 - Interface: **IPsec**
 - Address Family: **IPv4**
 - Protocol: **Any**
 - Source: **Any**
 - Destination: **Any**

Ping WAN:

1. VanRouter: **192.168.1.1/30**

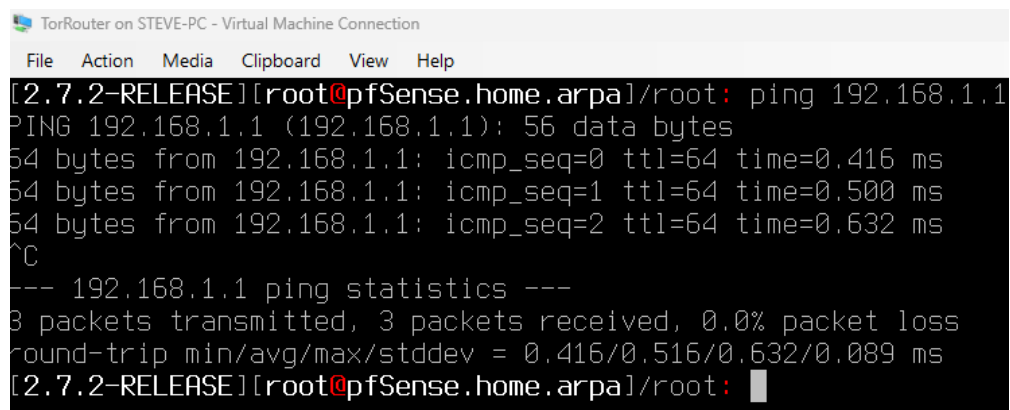
- **PING WAN on TorRouter: 192.168.1.2/30**



```
VanRouter on STEVE-PC - Virtual Machine Connection
File Action Media Clipboard View Help
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.730 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.925 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.441 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.730/1.032/1.441/0.300 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: █
```

2. TorRouter: **192.168.1.2/30**

- **PING WAN on VanRouter: 192.168.1.1/30**

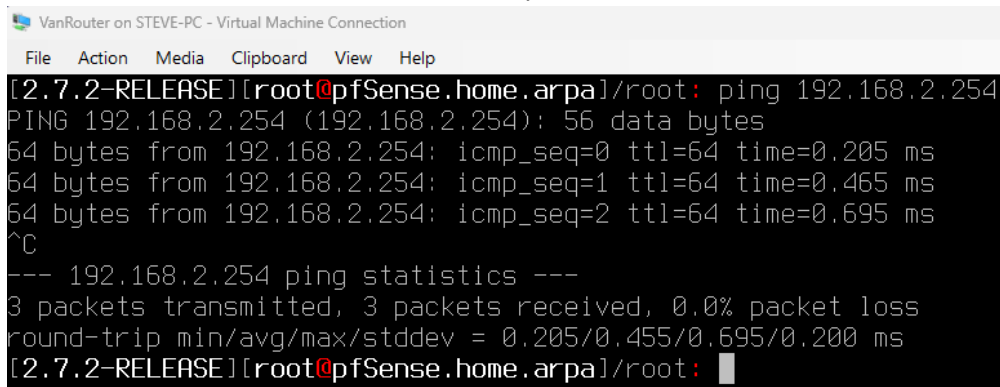


```
TorRouter on STEVE-PC - Virtual Machine Connection
File Action Media Clipboard View Help
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=0.416 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.500 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.632 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.416/0.516/0.632/0.089 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: █
```

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

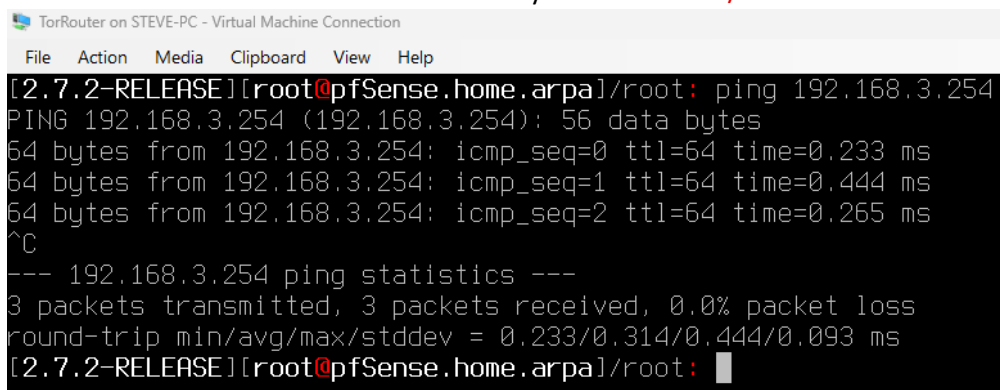
Ping LAN

1. VanRouter: **192.168.1.1/30**
 - PING **LAN1** Default Gateway: **192.168.2.254/24**



```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254): 56 data bytes
64 bytes from 192.168.2.254: icmp_seq=0 ttl=64 time=0.205 ms
64 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=0.465 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=0.695 ms
^C
--- 192.168.2.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.205/0.455/0.695/0.200 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: █
```

2. TorRouter: **192.168.1.2/30**
 - PING **LAN2** Default Gateway: **192.168.3.254/24**



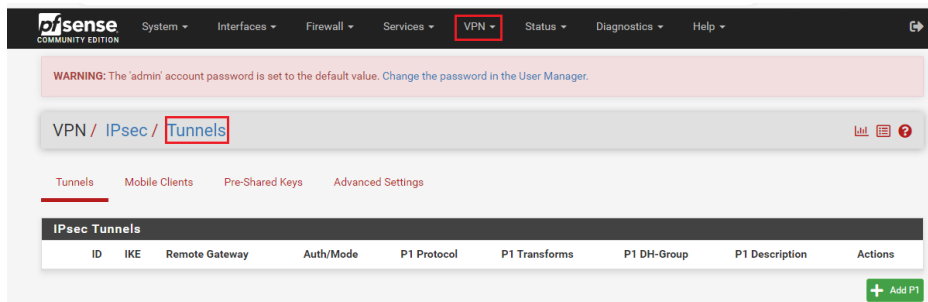
```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping 192.168.3.254
PING 192.168.3.254 (192.168.3.254): 56 data bytes
64 bytes from 192.168.3.254: icmp_seq=0 ttl=64 time=0.233 ms
64 bytes from 192.168.3.254: icmp_seq=1 ttl=64 time=0.444 ms
64 bytes from 192.168.3.254: icmp_seq=2 ttl=64 time=0.265 ms
^C
--- 192.168.3.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.233/0.314/0.444/0.093 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: █
```

Configure Ipsec VPN Tunnel:

Phase 1 on DC1: Set up the VPN Endpoints:

- Login to pfSense Firewall (Site 1):
 - o Access the pfSense web interface on the first site (**192.168.2.254**)
- Navigate to VPN Configuration:
 - o Go to **VPN > IPsec** and click on the **'Tunnels'** tab

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- Create Phase 1:
 - o General Information
 - Click on '**Add P1**' to create a new **Phase 1** entry
 - o IKE Endpoint Configuration
 - Key Exchange version: **IKEv2**
 - Internet Protocol: **IPv4**
 - Interface: **WAN**
 - Remote Gateway: **192.168.1.2** (WAN IP of second pfSense Firewall)
 - o Phase 1 Proposal (Authentication)
 - Authentication Method: **Mutual PSK**
 - My identifier: **My IP address**
 - Peer identifier: **Peer IP address**
 - Pre-Shared Key:
a2bb37eeaf2a955e72869a1c4b85bb51f56ba860e204c3e25c8f875e
 - o Phase 1 Proposal (Encryption Algorithm)
 - Encryption Algorithm: **AES > 256 bits > SHA256 > 20 (nist ecp384)**
 - o Expiration and Replacement
 - Life Time: **28800**
 - Rekey: **25920**
 - Reauth Time: **0**
 - Rand Time: **2880**
 - o Advanced Options
 - Child SA Start Action: **Default**
 - Child SA Close Action: **Restart/Reconnect**
 - NAT Traversal: **Auto**
 - MOBIKE: **Disable**

Phase 2 on DC1: Set up the Tunnel Networks:

- Create Phase 2:
 - o On the same page, click on '**Show Phase 2 Entries**' and add a new Phase 2 entry

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	1	V2	WAN 192.168.1.2	Mutual PSK -	AES (256 bits)	SHA256	20 (nist ecp384)	Site-To-Site VPN to Site 2	
+ Show Phase 2 Entries (1)									
+ Add P1 Delete P1s									

- General Information
 - Mode: **Tunnel IPv4**
- Networks
 - Local Network: **LAN subnet**
 - NAT/BINAT translation: **None**
 - Remote Network: **Network > 192.168.3.0/24**
- Phase 2 Proposal (SA/Key Exchange)
 - Protocol: **ESP**
 - Encryption Algorithm: **AES > 256 bits**
 - Hash Algorithm: **SHA256**
 - PFS key group: **20 (nist ecp384)**
- Expiration and Replacement
 - Life Time: **3600**
 - Rekey Time: **3240**
 - Rand Time: **360**
 - Save > **Apply**

VPN / IPsec / Tunnels																													
Tunnels Mobile Clients Pre-Shared Keys Advanced Settings																													
IPsec Tunnels																													
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions																				
<input type="checkbox"/> Disable	1	V2	WAN 192.168.1.2	Mutual PSK -	AES (256 bits)	SHA256	20 (nist ecp384)	Site-To-Site VPN to Site 2																					
<div><div></div><table><tr><th></th><th>ID</th><th>Mode</th><th>Local Subnet</th><th>Remote Subnet</th><th>P2 Protocol</th><th>P2 Transforms</th><th>P2 Auth Methods</th><th>Description</th><th>P2 actions</th></tr><tr><td><input type="checkbox"/> Disable</td><td>1</td><td>tunnel</td><td>LAN</td><td>192.168.3.0/24</td><td>ESP</td><td>AES (256 bits)</td><td>SHA256</td><td></td><td> </td></tr></table>+ Add P2</div>											ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions	<input type="checkbox"/> Disable	1	tunnel	LAN	192.168.3.0/24	ESP	AES (256 bits)	SHA256		
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions																				
<input type="checkbox"/> Disable	1	tunnel	LAN	192.168.3.0/24	ESP	AES (256 bits)	SHA256																						
+ Add P1 Delete P1s																													

Phase 1 on DC2: Set up the VPN Endpoints:

- Login to pfSense Firewall (Site 2):
 - Access the pfSense web interface on the first site (**192.168.3.254**)
- Navigate to VPN Configuration:

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Go to **VPN > IPSec** and click on the '**Tunnels**' tab
- Create Phase 1:
 - General Information
 - Click on '**Add P1**' to create a new Phase 1 entry
 - IKE Endpoint Configuration
 - Key Exchange version: **IKEv2**
 - Internet Protocol: **IPv4**
 - Interface: **WAN**
 - Remote Gateway: **192.168.1.1** (WAN IP of first pfSense Firewall)
 - Phase 1 Proposal (Authentication)
 - Authentication Method: **Mutual PSK**
 - My identifier: **My IP address**
 - Peer identifier: **Peer IP address**
 - Pre-Shared Key:
a2bb37eeaf2a955e72869a1c4b85bb51f56ba860e204c3e25c8f875e (copy the generated shared key from DC1)
 - Phase 1 Proposal (Encryption Algorithm)
 - Encryption Algorithm: **AES > 256 bits > SHA256 > 20 (nist ecp384)**
 - Expiration and Replacement
 - Life Time: **31860**
 - Rekey: **28674**
 - Reauth Time: **0**
 - Rand Time: **3186**
 - Advanced Options
 - Child SA Start Action: **None (Responder Only)**
 - Child SA Close Action: **Close connection and clear SA**
 - NAT Traversal: **Auto**
 - MOBIKE: **Disable**

Phase 2 on DC2: Set up the Tunnel Networks:

- Create Phase 2:
 - On the same page, click on '**Show Phase 2 Entries**' and add a new Phase 2 entry

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.1.1	Mutual PSK -	AES (256 bits)	SHA256	20 (nist ecp384)	Site-To-Site VPN to Site 1	
<div> Show Phase 2 Entries (1)</div>									
<div> Add P1 Delete P1s</div>									

- General Information
 - Mode: **Tunnel IPv4**
 - Networks
 - Local Network: **LAN subnet**
 - NAT/BINAT translation: **None**
 - Remote Network: **Network > 192.168.2.0/24**
 - Phase 2 Proposal (SA/Key Exchange)
 - Protocol: **ESP**
 - Encryption Algorithm: **AES > 256 bits**
 - Hash Algorithm: **SHA256**
 - PFS key group: **20 (nist ecp384)**
 - Expiration and Replacement
 - Life Time: **5400**
 - Rekey Time: **4860**
 - Rand Time: **540**
- Save > Apply

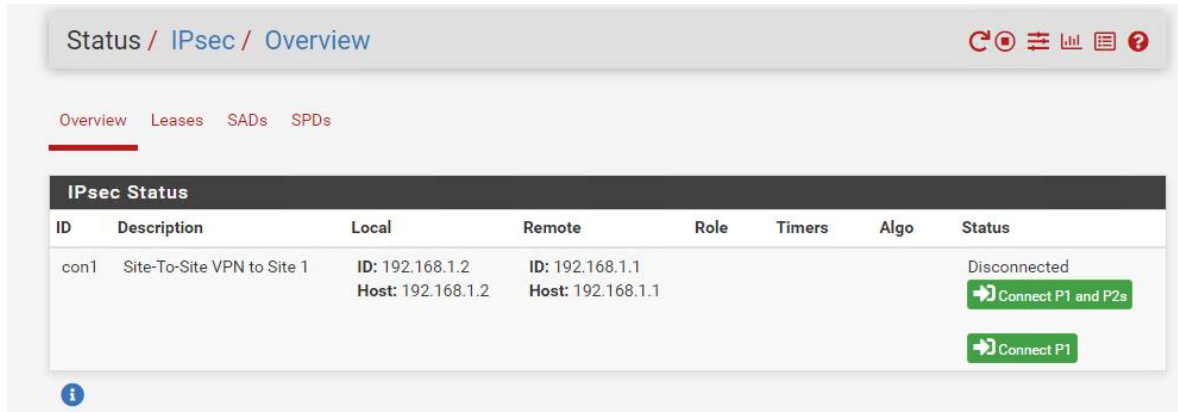
VPN / IPsec / Tunnels									
Tunnels Mobile Clients Pre-Shared Keys Advanced Settings									
IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.1.1	Mutual PSK -	AES (256 bits)	SHA256	20 (nist ecp384)	Site-To-Site VPN to Site 1	
<div> Add P2</div>									
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/>	1	tunnel	LAN	192.168.2.0/24	ESP	AES (256 bits)	SHA256		
<div> Add P1 Delete P1s</div>									

Post-Configuration:

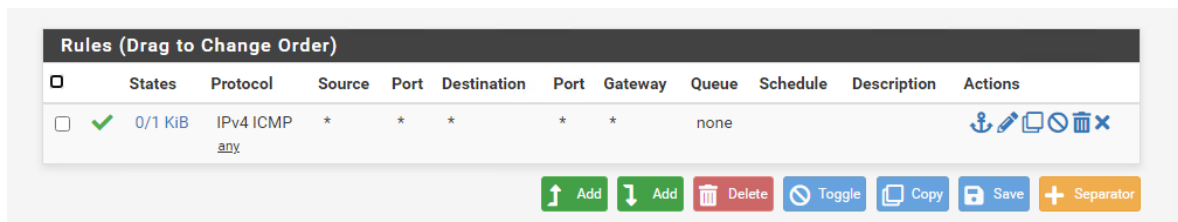
- Start the IPsec Service:

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- On both firewalls, navigate to **Status > IPsec**, and click on '**Start Service**' if it's not running
- Establish the Tunnel:
 - Click on '**Connect VPN**' for the newly created IPsec connection



- Firewall Rules:
 - Adjust firewall rules to allow traffic to pass through the tunnel. This is done in the **Firewall > Rules > IPsec** section



- Use the **Status > IPsec** page to view the status of the IPsec tunnels

Configure the Internal Devices:

DC1 > Vancouver:

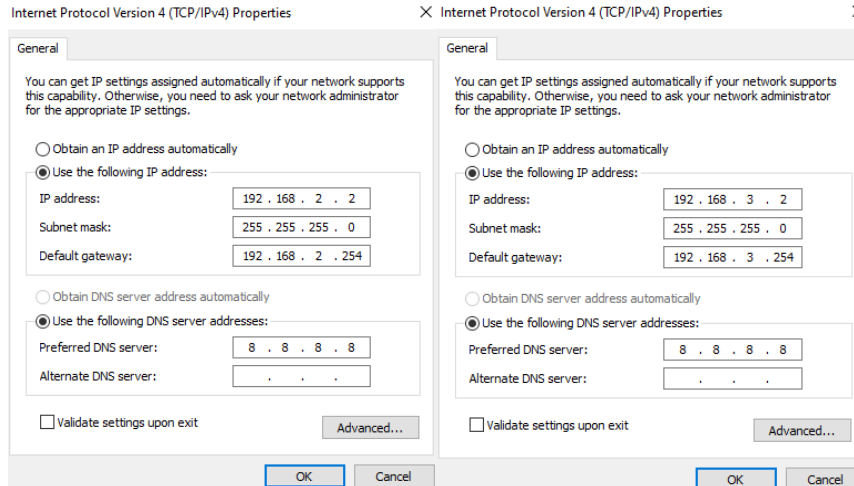
- Configure Networking: **DC1 > Server Manager > Local Server > LAN1 > Properties > TCP/IPv4**
 - Set Static IP:
 - IP Address: **192.168.2.2**
 - Subnet mask: **255.255.255.0**
 - Default Gateway: **192.168.2.254**
 - DNS (Before DC Promotion): **8.8.8.8**

DC2 > Toronto:

- Configure Networking: **DC2 > Server Manager > Local Server > LAN2 > Properties > TCP/IPv4**
 - Set Static IP:
 - IP Address: **192.168.3.2**
 - Subnet mask: **255.255.255.0**

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Default Gateway: **192.168.3.254**
- DNS (Before DC Promotion): **8.8.8.8**



Connect the Vancouver Office to the Toronto Office Through IPsec Tunneling:

- Test Connectivity:
 - o Ping **192.168.3.2 DC2** (Toronto) from DC1 (Vancouver)

```
DC1 on STEVE-PC - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
PS C:\Users\Administrator>
```

- o Ping **192.168.2.2 DC1** (Vancouver) from DC2 (Toronto)

```
DC2 on STEVE-PC - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=3ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

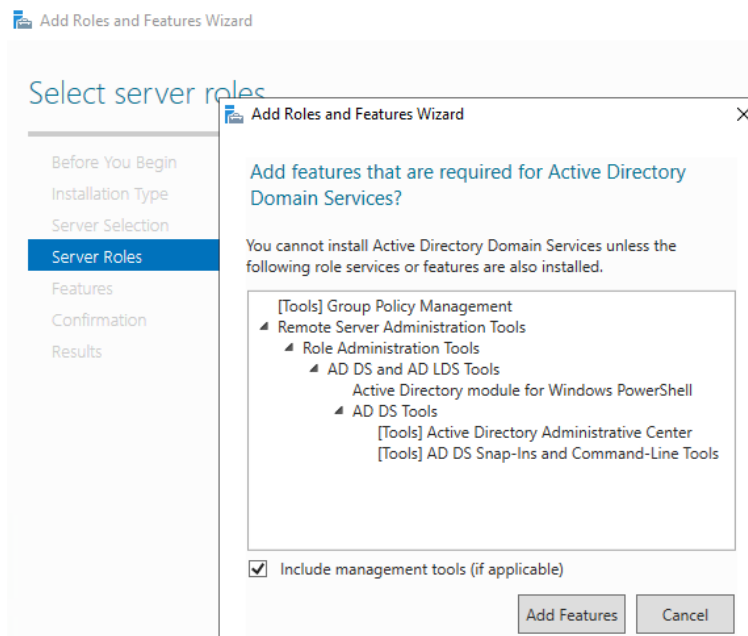
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
PS C:\Users\Administrator>
```

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Create the Domain Controllers:

Installation Steps for the First Domain Controller (DC1):

- DC1 Running on Windows Server 2022
- Static IP configuration:
 - o IP Address: **192.168.2.2/24**
 - o Gateway: **192.168.2.254**
- Install Active Directory Domain Services (AD DS):
 - o Open **Server Manager**
 - o Click on '**Add roles and features**'



- Proceed to the '**Roles**' section and check '**Active Directory Domain Services**'
- Add features that are required for Active Directory Domain Services and click '**Next**'
- Install

Create Secondary Disk for DC1:

- We will create a secondary storage disk to hold all Database files
 - o Run script on Host using PowerShell ISE Administrator
- `$VHDXname = Read-Host -Prompt 'Input VHDX name'`
- `$SizeInGB = Read-Host -Prompt 'Input the size in GB. Ex 5, 10'`
- `$VMName = Read-Host -Prompt 'Input target VM name'`
- `$VHDPATH = "V:\VMs\VHDX\" + $VHDXname + ".vhdx"`

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

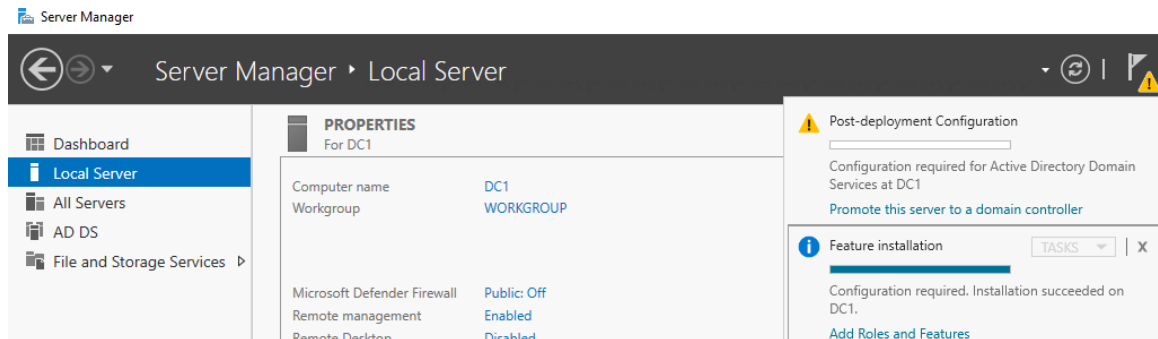
- `$SizeBytes = ($SizeInGB/1 * 1073741824)`
- `$alreadyExists = Test-Path -Path $VHDPATH`
- `if ($alreadyExists) {`
- `Write-Error "Error. The VHDX already exists"`
- `return`
- `}`
- `New-VHD -Path $VHDPATH -Dynamic -SizeBytes $SizeBytes | Mount-VHD -Passthru | Initialize-Disk -Passthru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -Confirm:$false -Force`
- `Dismount-VHD -Path $VHDPATH`
- `# Optimize-VHD -Path $VHDPATH -Mode Full`
- `Add-VMHardDiskDrive -VMName $VMName -Path $VHDPATH`

Bring Disk Online DC1:

- **Server Manager > File and Storage Services > Volumes > Disks > Right click > Bring Online**
- The Volume is designated as D:\

Promote to Domain Controller:

- After installation, click on the notification flag and select '**Promote this server to a domain controller**'



- Choose '**Add a new forest**' and type your Root domain name

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

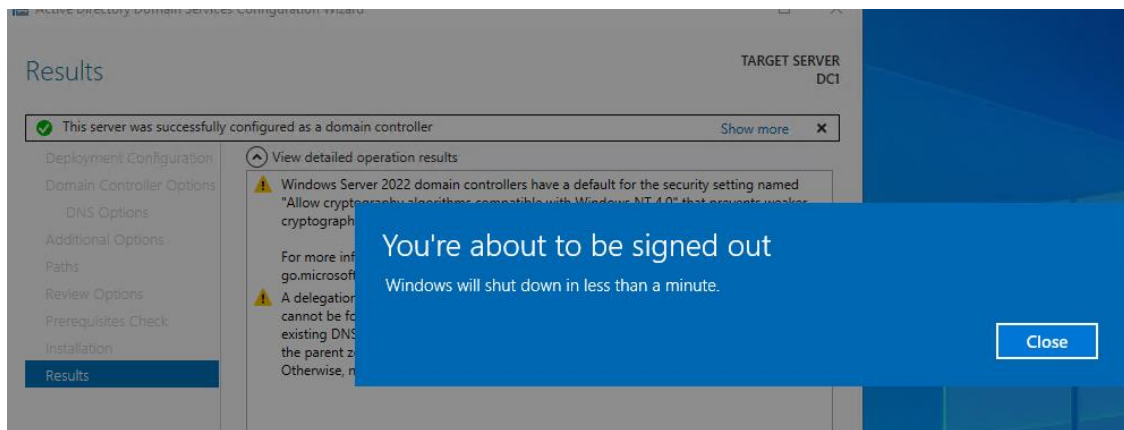
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes standard window controls. The main window has a left-hand navigation pane with the following items: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Deployment Configuration' and has a 'TARGET SERVER DC1' label in the top right corner. It contains two sections: 'Select the deployment operation' with three radio buttons ('Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' - which is selected), and 'Specify the domain information for this operation' with a text box for 'Root domain name:' containing the value 'corp.tsp.ca'.

- **tsp.ca – external domain**
 - **corp.tsp.ca – root domain**
- **Set the Directory Services Restore Mode (DSRM) password**
 - **Pa\$\$w0rd**
- Follow the wizard to configure additional options like **DNS**, and **GC (Global Catalog)**
 - Click the checkbox for **DNS** and **GC**
- Click '**Next**' through the wizard, then click '**Install**'

- **Paths:**

The screenshot shows the 'Paths' step of the wizard. The left-hand navigation pane has 'Paths' highlighted in blue. The main content area is titled 'Specify the location of the AD DS database, log files, and SYSVOL'. It contains three rows of configuration: 'Database folder:' with a text box containing 'D:\NTDS' and a browse button (...); 'Log files folder:' with a text box containing 'D:\NTDS' and a browse button (...); and 'SYSVOL folder:' with a text box containing 'D:\SYSVOL' and a browse button (...).

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- The server will automatically reboot and become the first Domain Controller

Installation Steps for the First Domain Controller (DC2):

- DC1 Running on Windows Server 2022
- Static IP configuration:
 - o IP Address: **192.168.3.2/24**
 - o Gateway: **192.168.3.254**
- Install Active Directory Domain Services (AD DS):
 - o Open **Server Manager**
 - o Click on '**Add roles and features**'
- Proceed to the '**Roles**' section and check '**Active Directory Domain Services**'
- Add features that are required for Active Directory Domain Services and click '**Next**'
- Install

Create Secondary Disk for DC2:

- We will create a secondary storage disk to hold all Database files
 - o Run script on Host using PowerShell ISE Administrator
- `$VHDXname = Read-Host -Prompt 'Input VHDX name'`
- `$SizeInGB = Read-Host -Prompt 'Input the size in GB. Ex 5, 10'`
- `$VMName = Read-Host -Prompt 'Input target VM name'`
- `$VHDXPath = "V:\VMs\VHDX\" + $VHDXname + ".vhdx"`
- `$SizeBytes = ($SizeInGB/1 * 1073741824)`
- `$alreadyExists = Test-Path -Path $VHDXPath`
- `if ($alreadyExists) {`
- `Write-Error "Error. The VHDX already exists"`
- `return`

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- }
- `New-VHD -Path $VHDPATH -Dynamic -SizeBytes $SizeBytes | Mount-VHD -Passthru | Initialize-Disk -Passthru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -Confirm:$false -Force`
- `Dismount-VHD -Path $VHDPATH`
- `# Optimize-VHD -Path $VHDPATH -Mode Full`
- `Add-VMHardDiskDrive -VMName $VMName -Path $VHDPATH`

Bring Disk Online DC2:

- **Server Manager > File and Storage Services > Volumes > Disks > Right click > Bring Online**
- The Volume is designated as D:\

Promote to Domain Controller:

- After installation, click on the notification flag > **'Promote this server to a domain controller'**
- Select **"Add a domain controller to an existing domain"** in the deployment configuration wizard
- In the **"Specify the domain information for this operation"** field type **corp.tsp.ca** which is the **Fully Qualified Domain Name (FQDN)** of the existing domain

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER DC2

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☒ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☐ Add a new forest

Specify the domain information for this operation

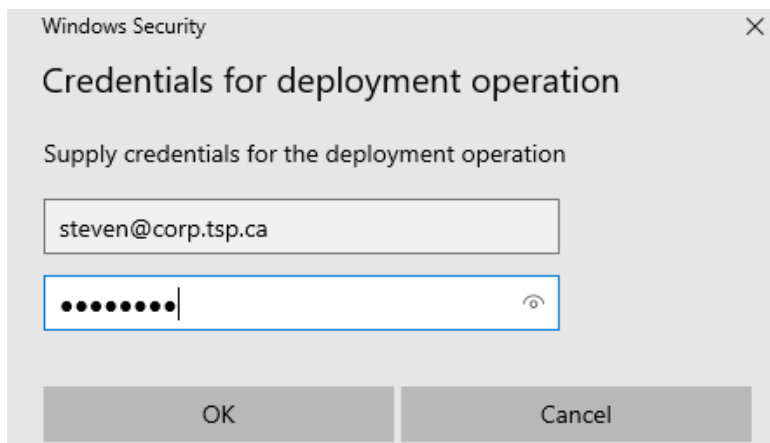
Domain: corp.tsp.ca Select...

Supply the credentials to perform this operation

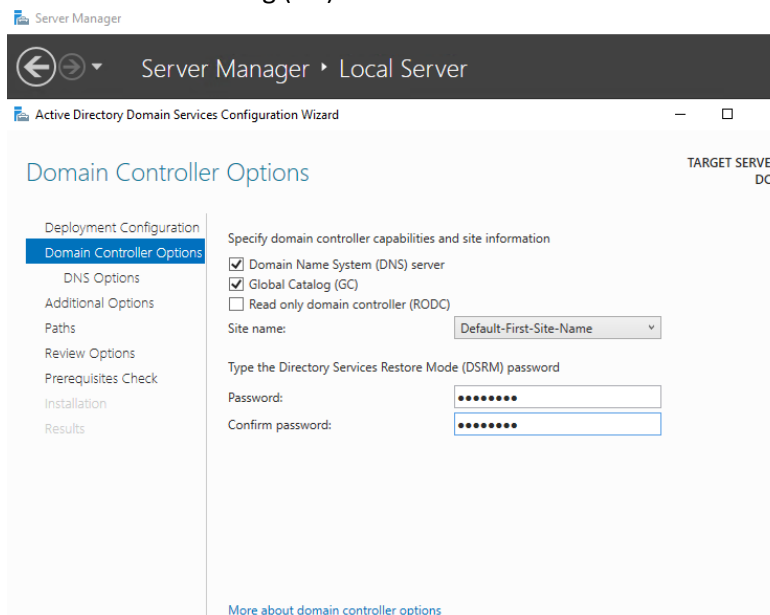
<No credentials provided> Change...

- Click **"Select"** to browse for the domain
- You will be prompted to provide credentials
 - o Click **"Change"** to enter the *username* and *password* of an account with permissions to add a domain controller to the domain

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

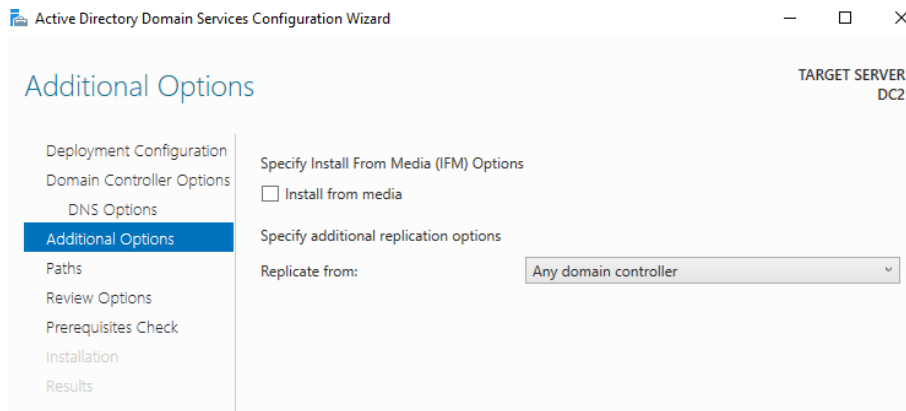


- Domain Controller Options:
 - o Domain Name System (DNS)
 - o Global Catalog (GC)

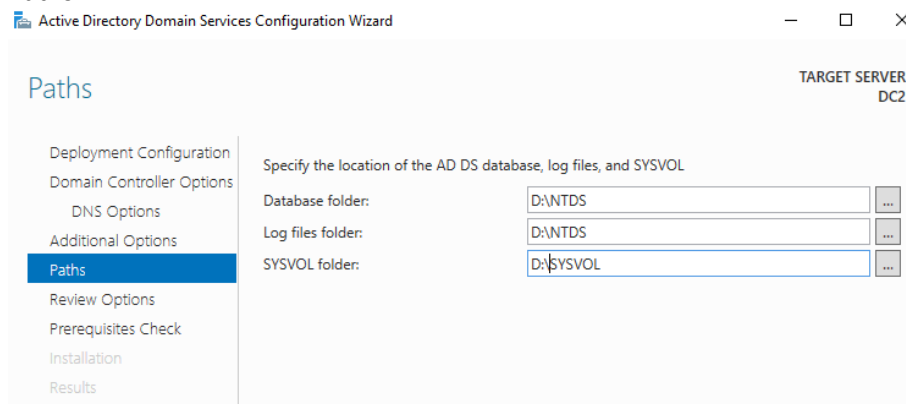


- DNS Options:
 - o Click **"Next"**
- Additional Options:

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

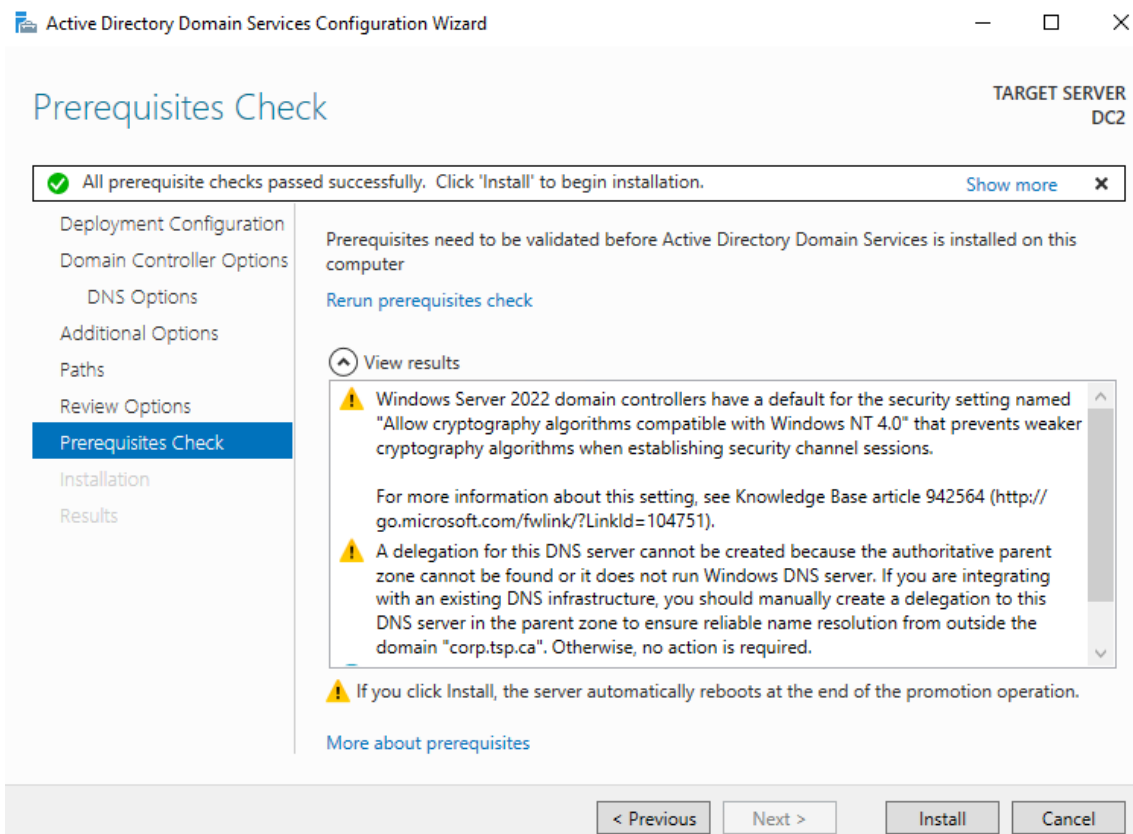


- Paths:

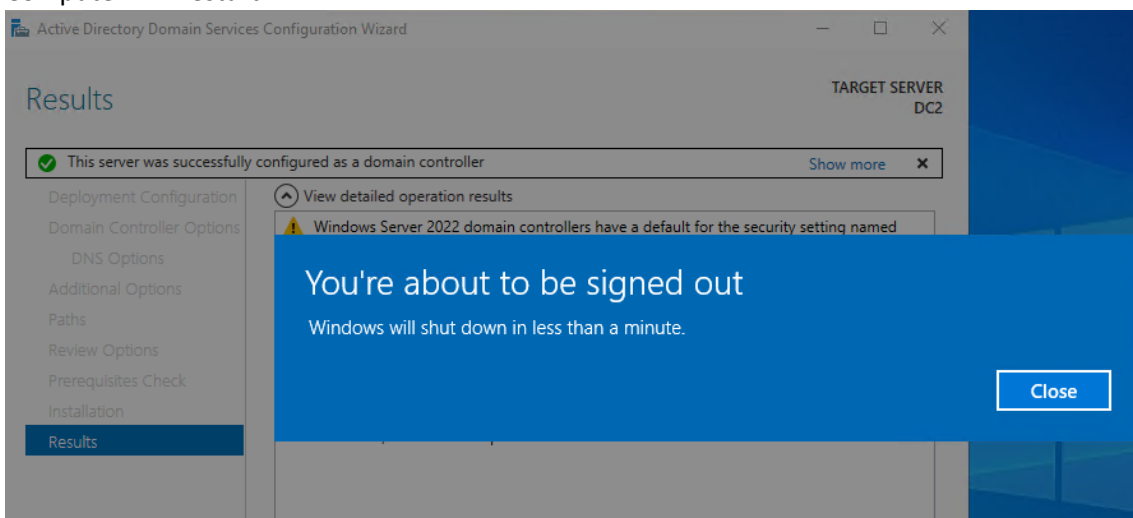


- After configuring these settings, you will proceed to the prerequisites check

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- The wizard will verify that the server meets all the requirements to become a domain controller
- Once all checks are passed - proceed with the installation
- Computer will restart:

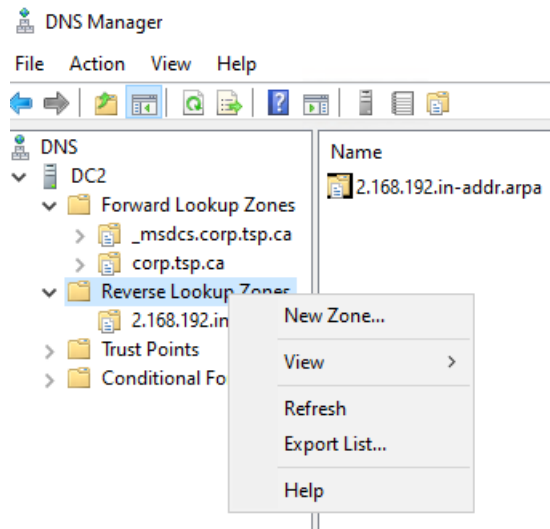


CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

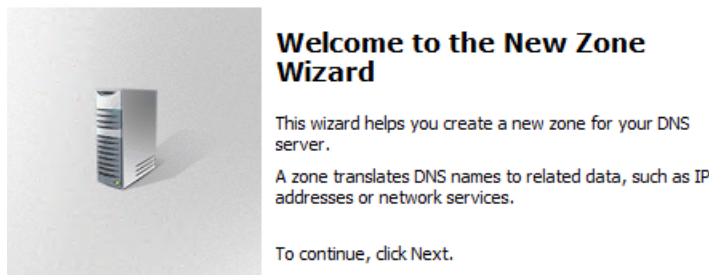
Configure DNS:

Create Reverse Lookup Zone:

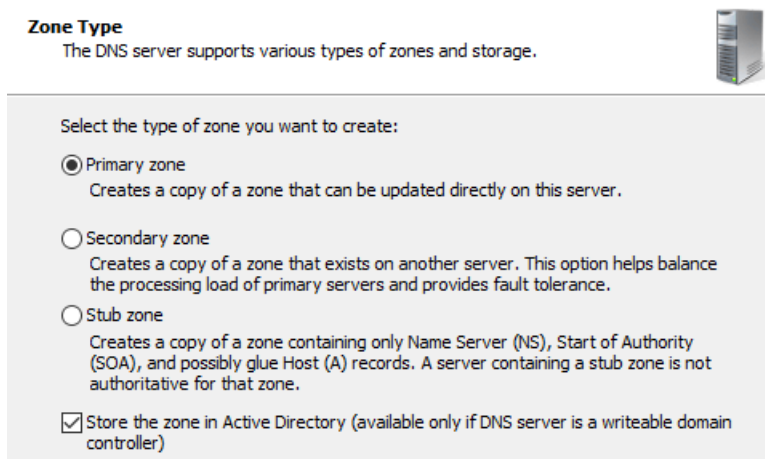
DC2 > Server Manager > Tools > DNS



- Click Next
New Zone Wizard



- Click Next
New Zone Wizard



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Click Next

New Zone Wizard ✕

Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

☐ To all DNS servers running on domain controllers in this forest: corp.tsp.ca

☒ To all DNS servers running on domain controllers in this domain: corp.tsp.ca

☐ To all domain controllers in this domain (for Windows 2000 compatibility): corp.tsp.ca

☐ To all domain controllers specified in the scope of this directory partition:

- Click Next

New Zone Wizard ✕

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone

☐ IPv6 Reverse Lookup Zone

- Click Next

New Zone Wizard ✕

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:

- Click Next

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Dynamic Update


You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.



Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

☒ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back

Next >

Cancel

- Click Finish

New Zone Wizard



Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name:	2.168.192.in-addr.arpa
Type:	Active Directory-Integrated Primary
Lookup type:	Reverse

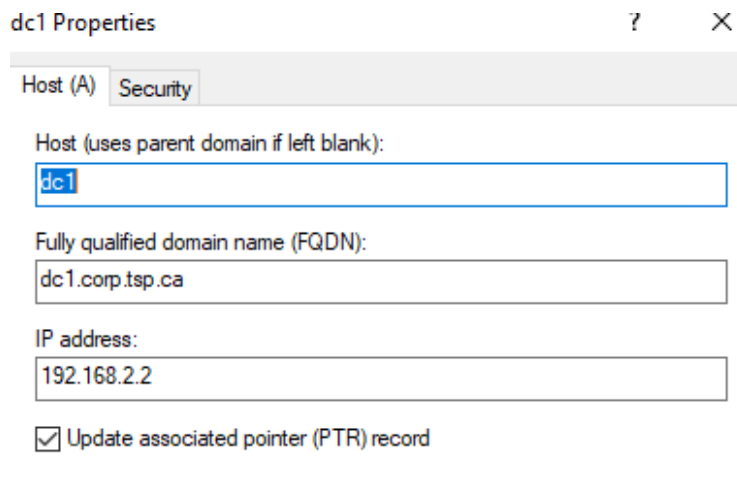
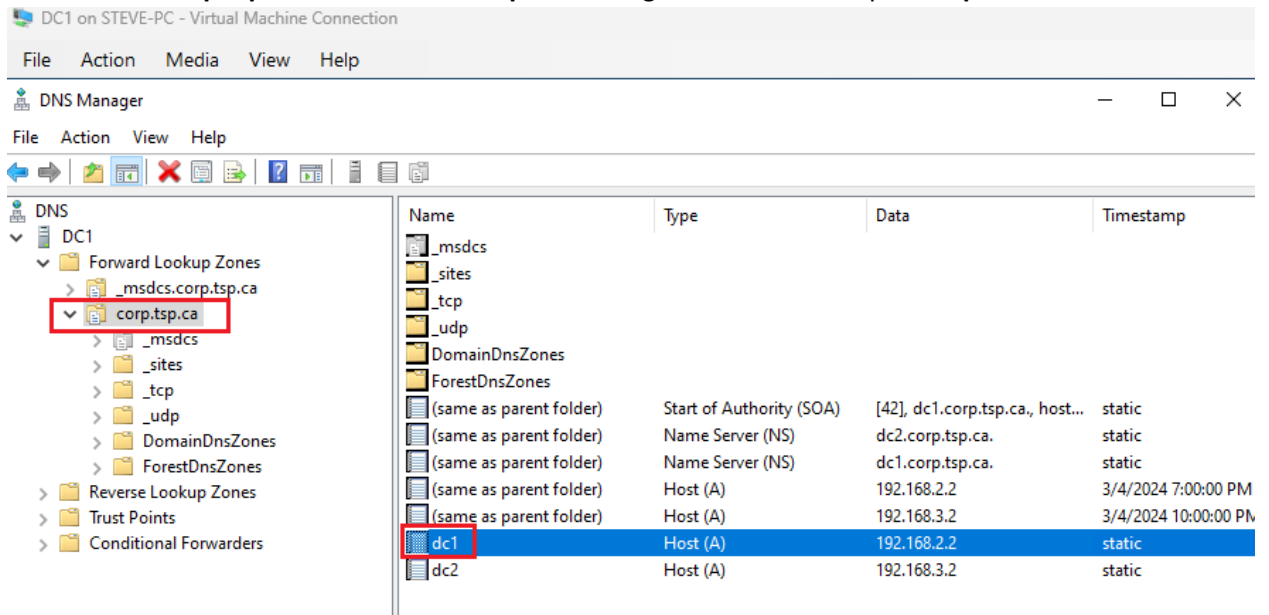
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Create PTR Record:

- **DC1**
 - o Click **corp.tsp.ca** > **Forward Lookup Zone** > Right click **DC1** and open **Properties**

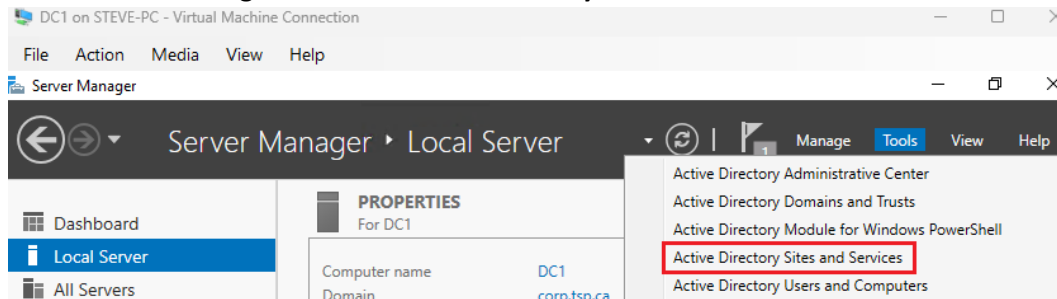


CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

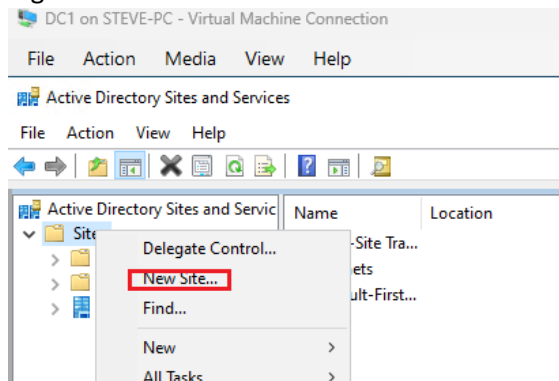
Create/Configure Sites and Services within Active Directory:

Creating a new site through Active Directory Sites and Services:

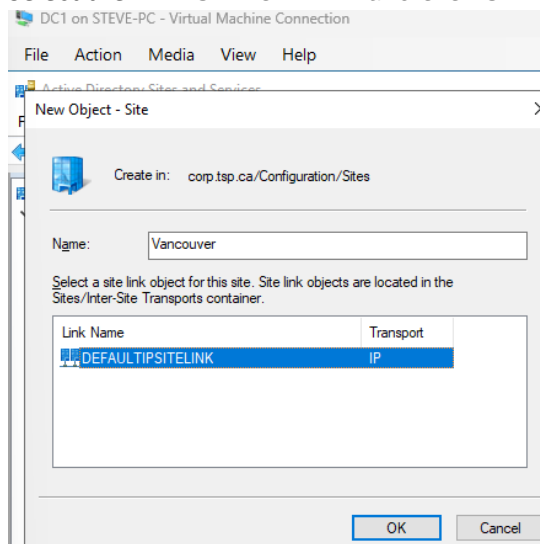
- **DC1 > Server Manager > Tools > Active Directory Sites and Services**



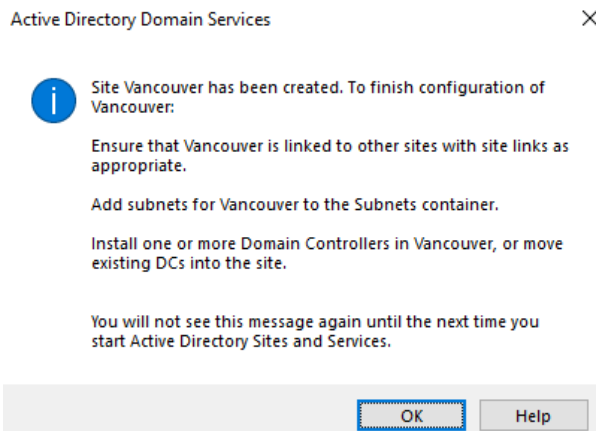
- Right click 'Sites' > 'New Site'



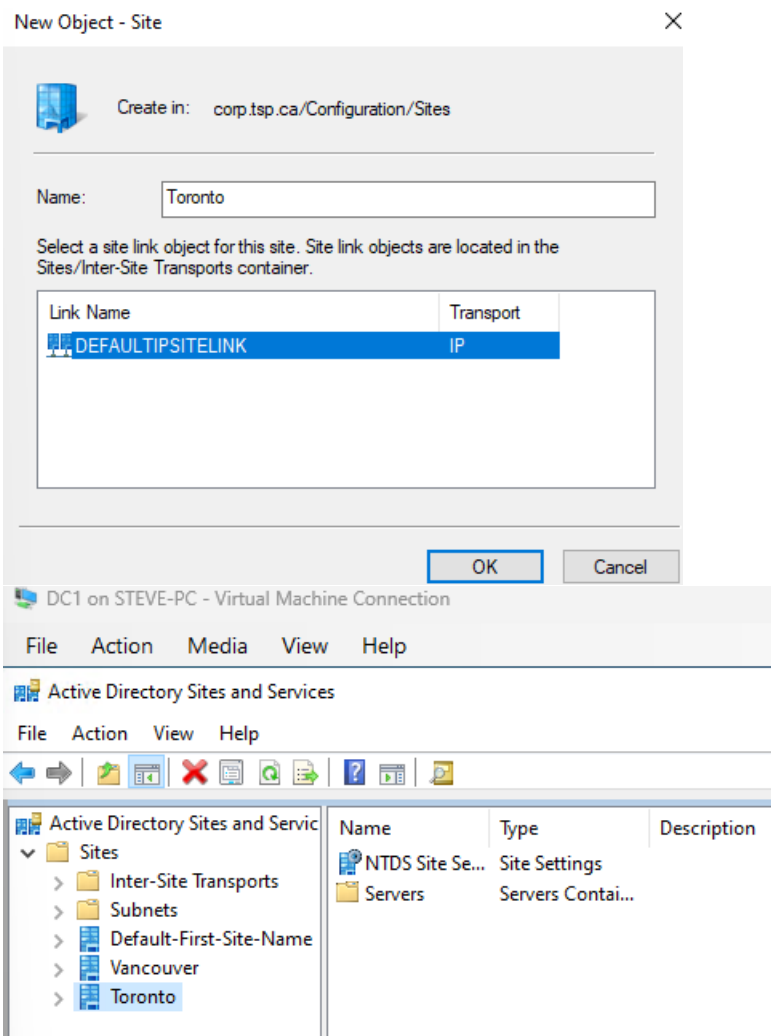
- Enter Site Name:
 - o **Vancouver**
- Select the **DEFAULTIPSITELINK** and click OK



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



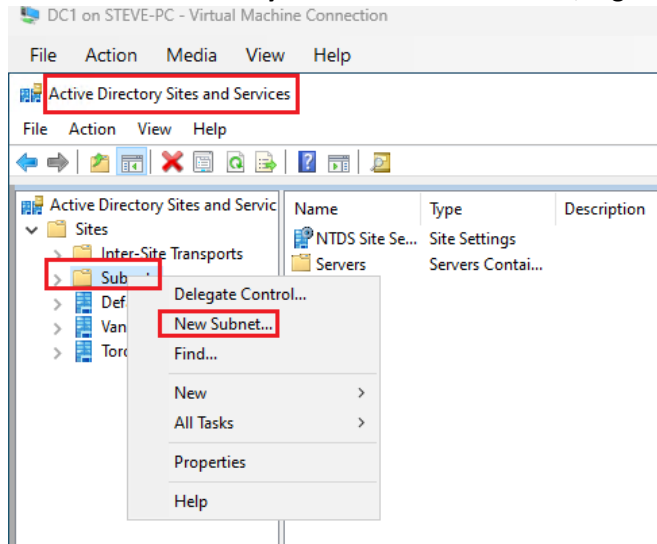
- Repeat the steps to create the second site – **Toronto**
- Select the **DEFAULTIPSITELINK** and click **OK**



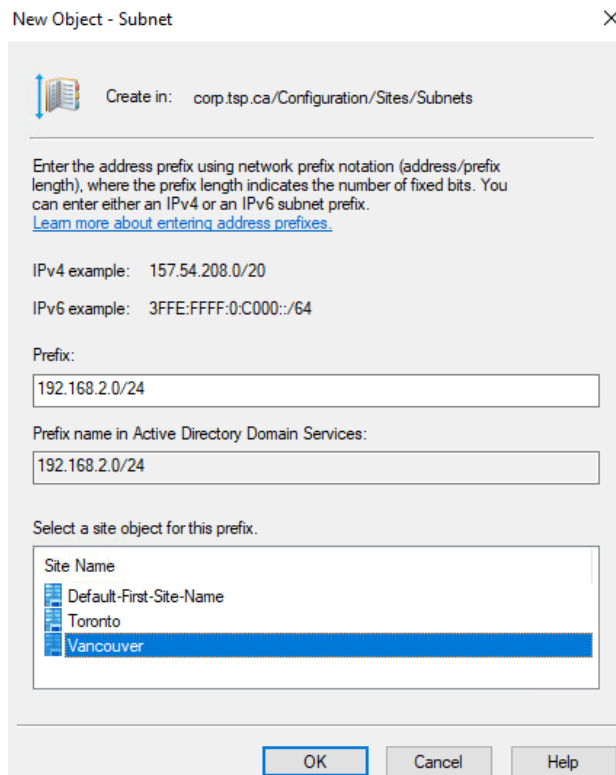
CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Creating Subnets:

- In the **Active Directory Sites and Services** MMC, Right click 'Subnets' and select 'New Subnet'



- Enter the prefix **192.168.2.0/24** as the prefix and select the **Vancouver** site object to associate with this prefix



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- Repeat steps and use the IP assigned to the Toronto subnet

- 192.168.3.0/24

New Object - Subnet

Create in: corp.tsp.ca/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix. [Learn more about entering address prefixes.](#)

IPv4 example: 157.54.208.0/20
IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix:

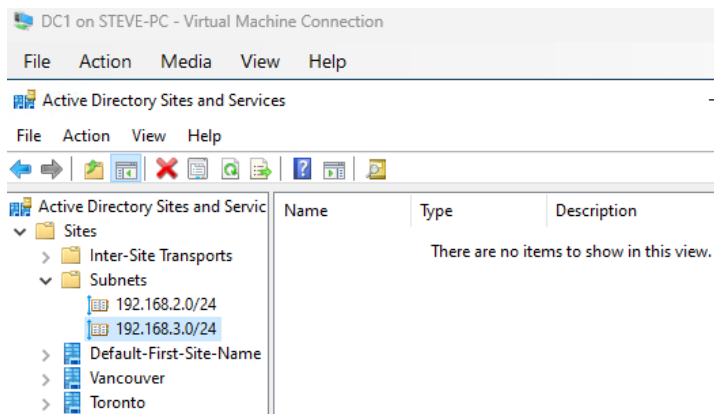
Prefix name in Active Directory Domain Services:

Select a site object for this prefix.

Site Name

- Default-First-Site-Name
- Toronto**
- Vancouver

OK Cancel Help



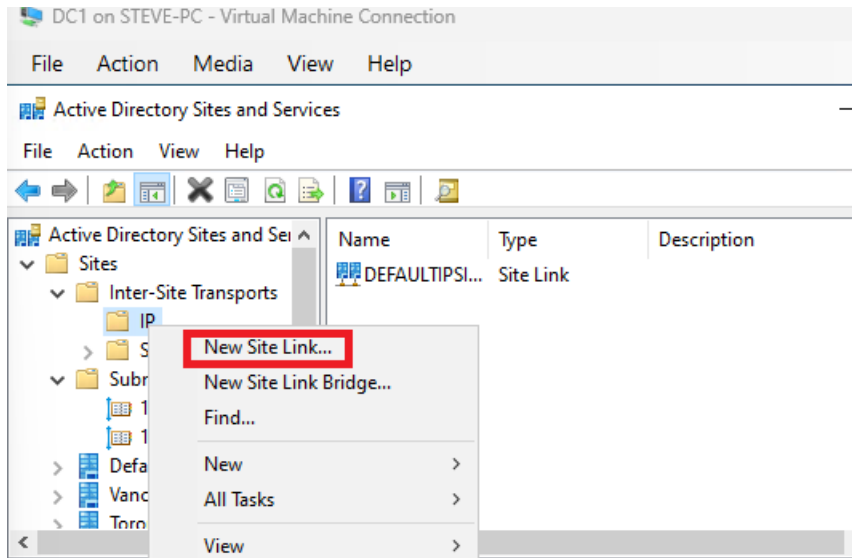
- **Why is it important to configure site subnets?**
 - Configuring site subnets in Active Directory is crucial for directing users to the nearest domain controller, ensuring efficient network traffic flow, and minimizing WAN usage. It optimizes replication traffic between domain controllers by aligning it with the actual network topology, reducing overhead on network resources
 - Properly assigned subnets also enable the application of site-specific policies and settings, enhancing the overall network performance and user experience. Additionally,

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

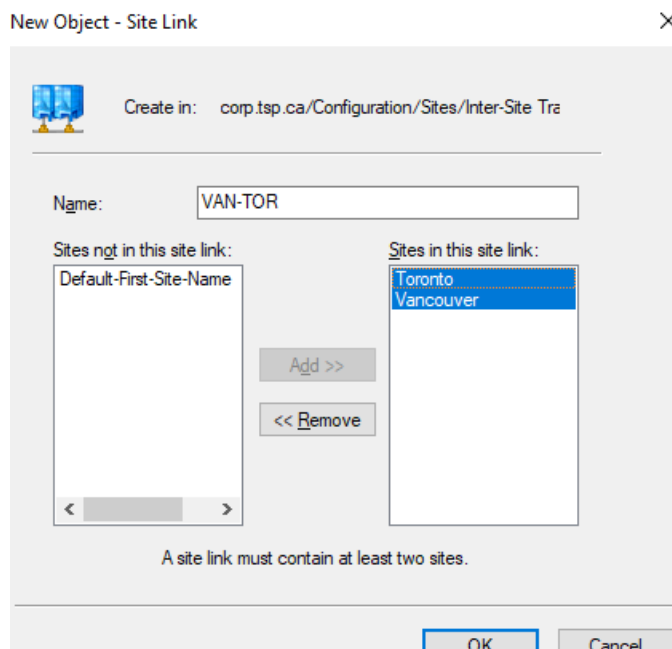
they play a key role in disaster recovery by facilitating the redirection of users to alternative sites when necessary

Creating Site Links:

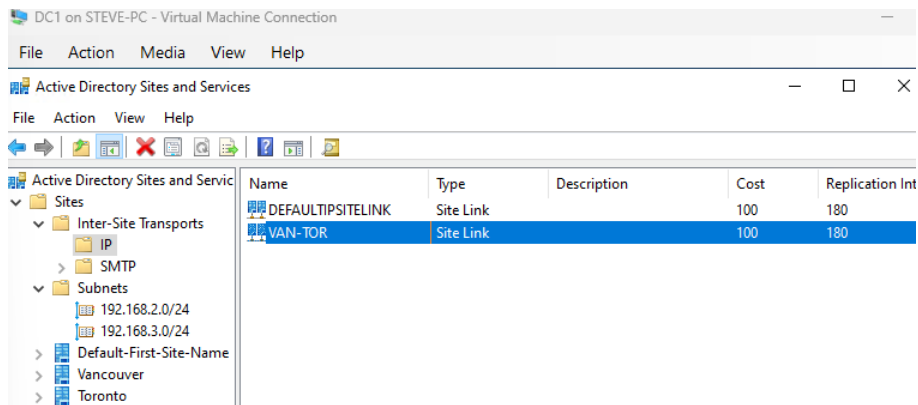
- **DC1 > Active Directory Sites and Services > Expand Inter-Site Transports > Right click IP > New Site Link**



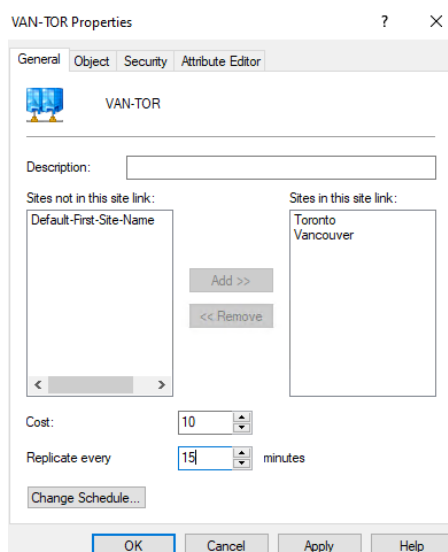
- In the 'New Object' Window – Name the Site Link: **VAN-TOR**
- Select both Sites and click 'Add'



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



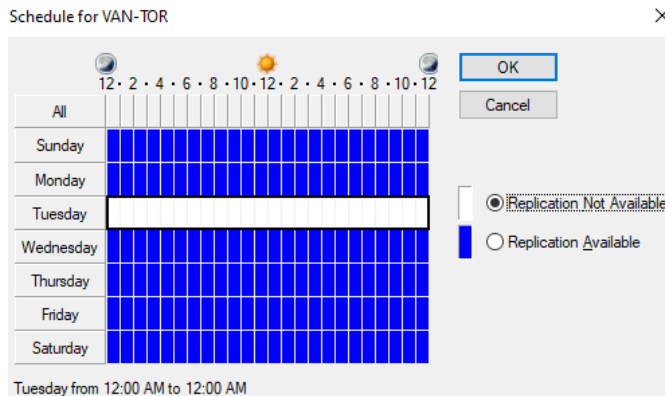
- Change the replication cost number
 - o Right click **VAN-TOR** > **Properties**
 - o Change Cost to 10
 - o Set Replicate Ever to 15 Minutes
- **Cost:** This is a numerical value that represents the relative cost of replication traffic over this site link. Active Directory uses this cost to determine the most efficient replication route; **lower costs are preferred over higher ones**. If there are multiple possible routes, AD will use the route with the lowest cumulative cost
- **Replicate every:** This value specifies the **frequency with which replication occurs** over this site link. The replication frequency helps balance the need for up-to-date information against the utilization of network resources



- Click Change Schedule

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

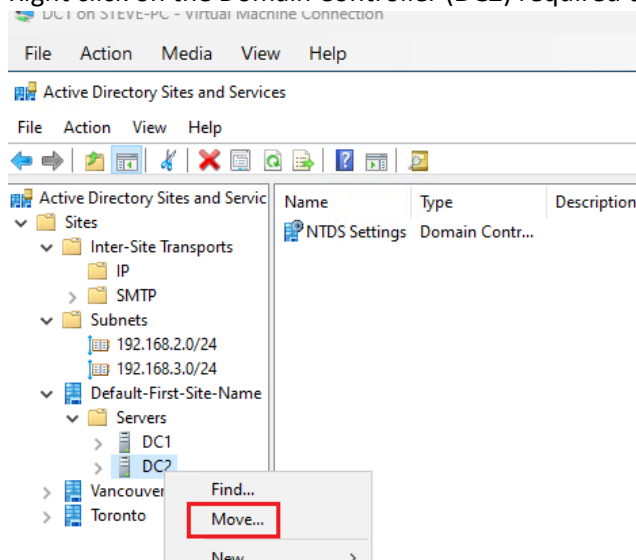
- Set replication schedule
 - o In this case, for the entirety of Tuesday, replication will not be available
- Click OK



- Apply > OK
- What is the purpose of a site link?
 - o A site link in Active Directory defines the replication topology between AD sites by indicating a path through which domain controllers in different sites can replicate data. It allows administrators to control replication traffic by setting a cost, frequency, and available schedule to optimize the use of network resources

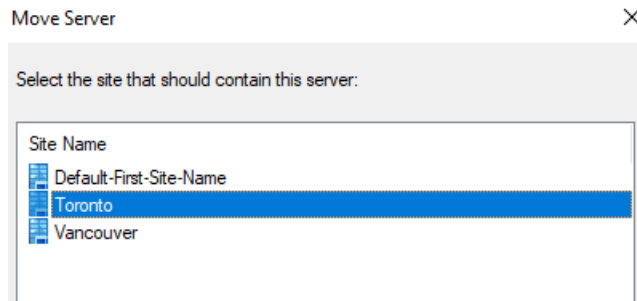
Move the Domain Controllers to their newly created sites:

- **DC1 > AD Site and Services > Default-First-Site-Name > Servers**
- Right click on the Domain Controller (DC2) required to move and select 'Move'

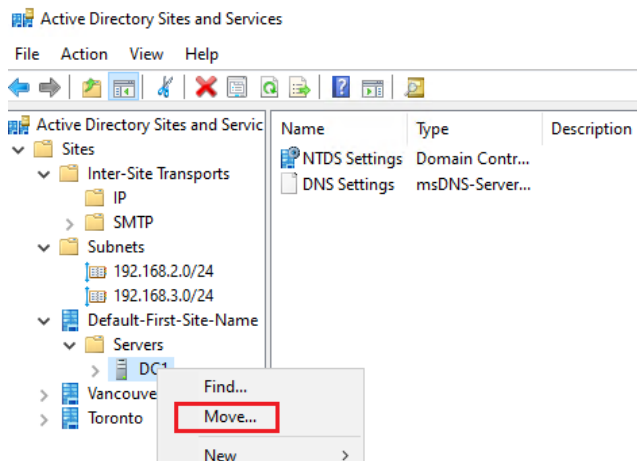


CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

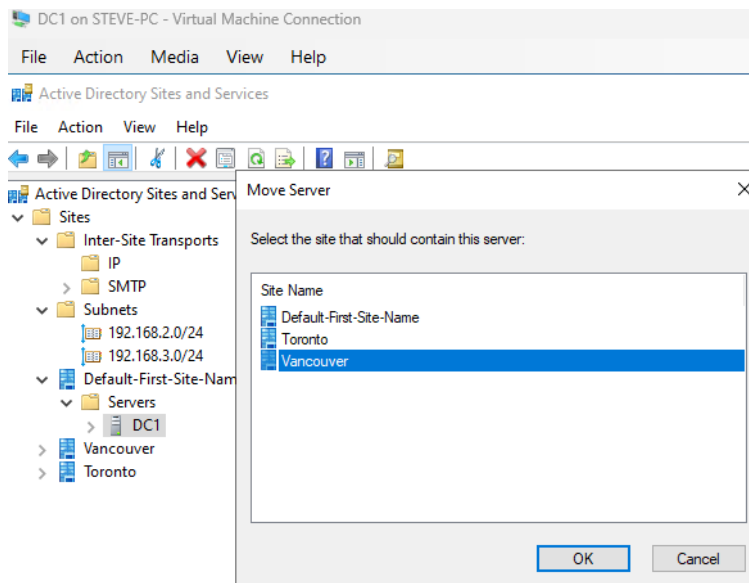
- In the '**Move Server**' Window select Toronto and click OK, as **DC2** is associated to Toronto



- Right Click **DC1** and click '**Move**'

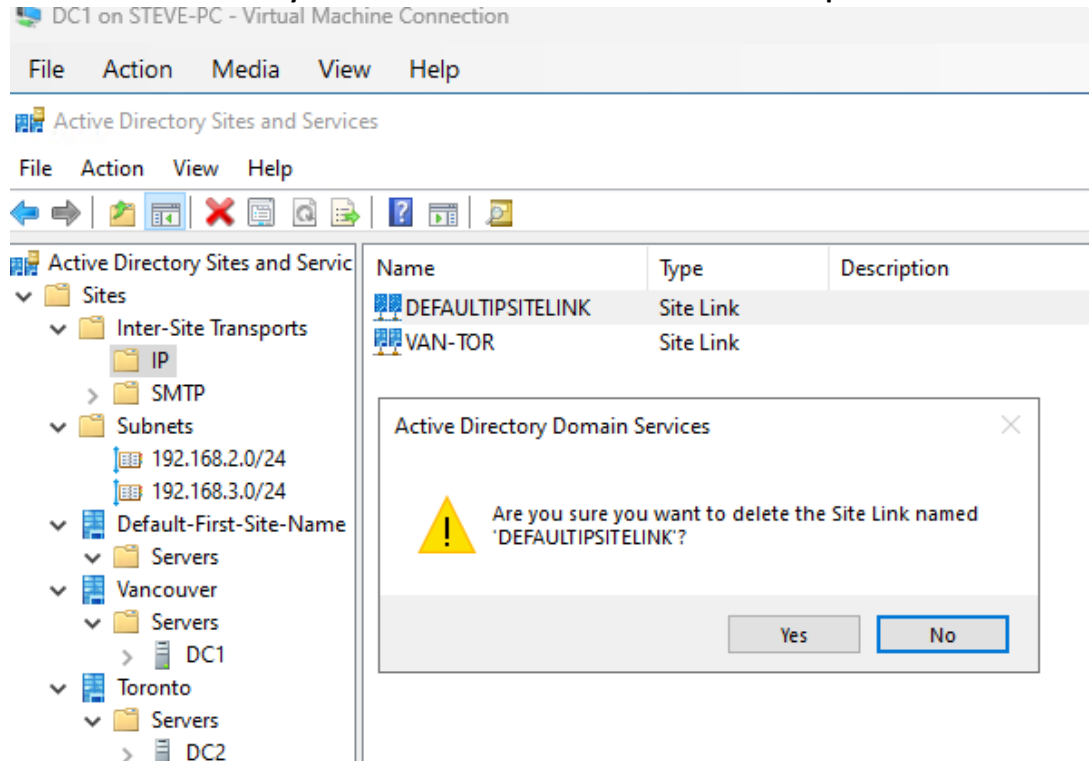


- Select '**Vancouver**'



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- After the DCs are moved there is no need for the DEFAULTIPSITELINK. Delete it
 - o **Active Directory Sites and Services > Sites > Inter-Site Transports > IP**



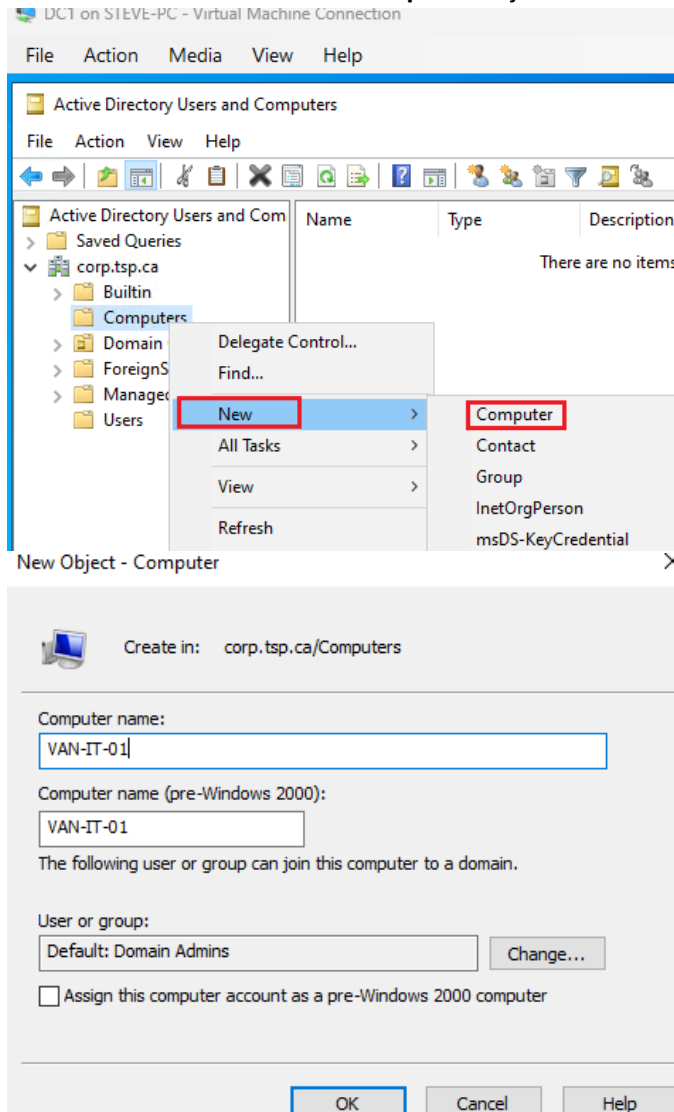
Test Replication:

- What are the commands to force replication?
 - o To force replication between domain controllers in Active Directory, you can use the following commands:
 - Using repadmin:
 - **repadmin /syncall**: This command synchronizes a specified domain controller with all replication partners
 - **repadmin /syncall /AeP**: This command includes all partitions and attempts to push changes outward from the specified DC.
 - o Using PowerShell:
 - **Sync-ADObject**: This cmdlet is used to replicate a single object between any two domain controllers that have partitions in common.

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Create an Object in the Vancouver DCs ADUC and see if that object is replicated to the Toronto DC:

- **DC1 > ADUC > Create a New Computer object in the Computers container**

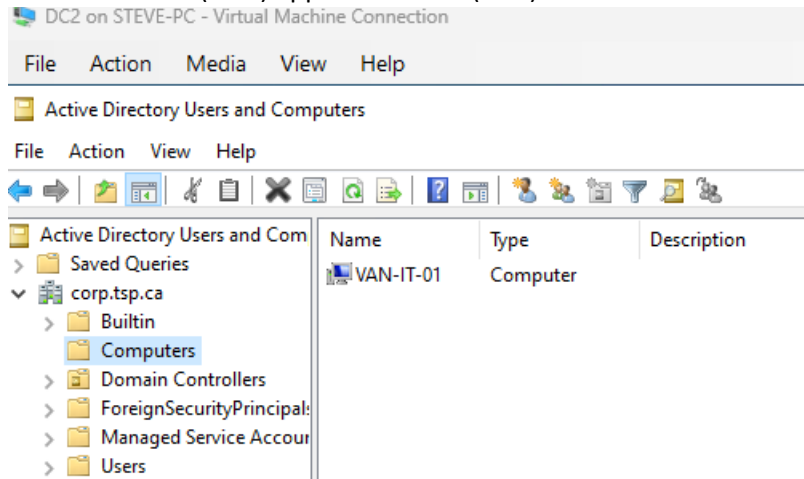


- On DC2, open ADUC to see if VAN-IT-01 appears in the Computers container

```
PS C:\Windows\system32> repadmin /syncall /AeP
Syncing all NC's held on DC1.
Syncing partition: DC=ForestDnsZones,DC=corp,DC=tsp,DC=ca
CALLBACK MESSAGE: The following replication is in progress:
  From: 8d3395d1-11f3-4b34-984b-c52bff5bb45c._msdcs.corp.tsp.ca
  To : dd54606f-b7da-46fa-9652-392f2d625b2b._msdcs.corp.tsp.ca
CALLBACK MESSAGE: The following replication completed successfully:
  From: 8d3395d1-11f3-4b34-984b-c52bff5bb45c._msdcs.corp.tsp.ca
  To : dd54606f-b7da-46fa-9652-392f2d625b2b._msdcs.corp.tsp.ca
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

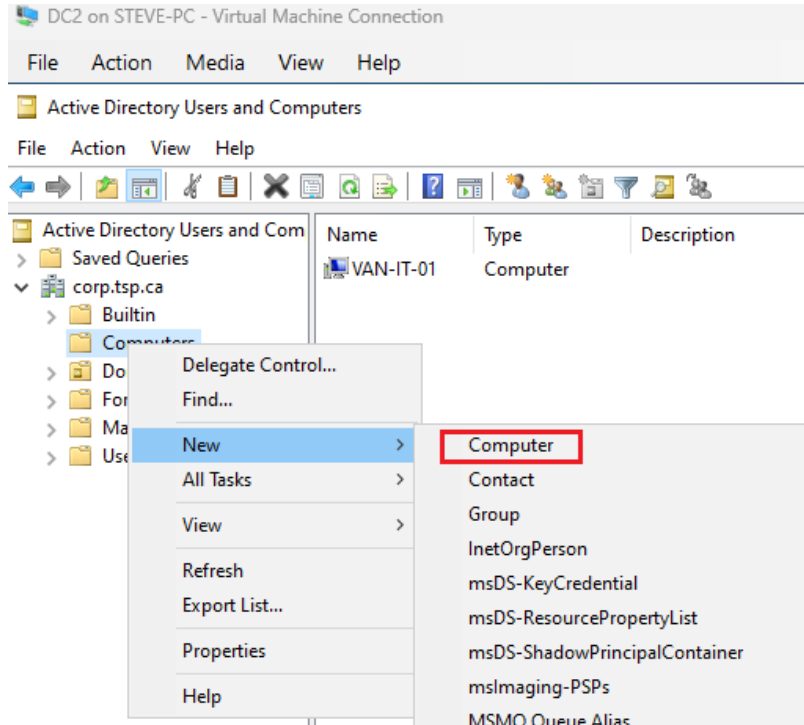
CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- After forcing replication using the command **repadmin /syncall /AeP** the computer object created on **DC1 (VAN)** appears on **DC2 (TOR)**

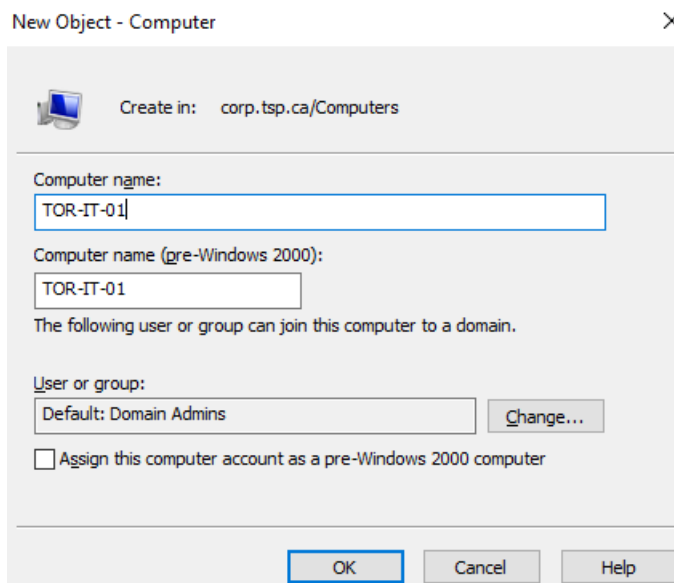


Create an object in the Toronto DCs ADUC and see if that object is replicated to the Vancouver DC:

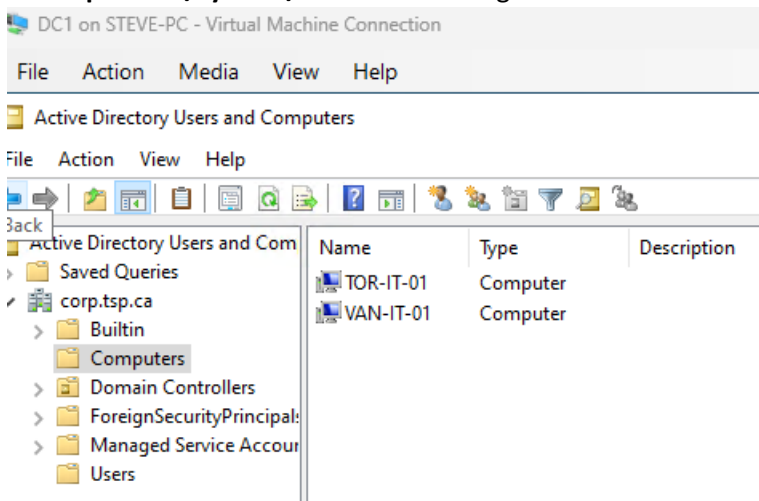
- **DC2 > ADUC > Create a New Computer object in the Computers container**



CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- On DC1, open ADUC to see if TOR-IT-01 appears in the Computers container
- Run **repadmin /syncall /AeP** on **DC2** using PowerShell as Administrator

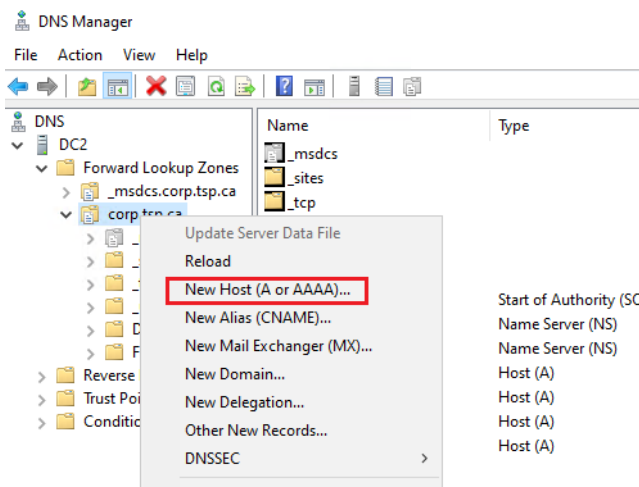


- The computer object created on **DC2** (TOR) appears on **DC1** (VAN)

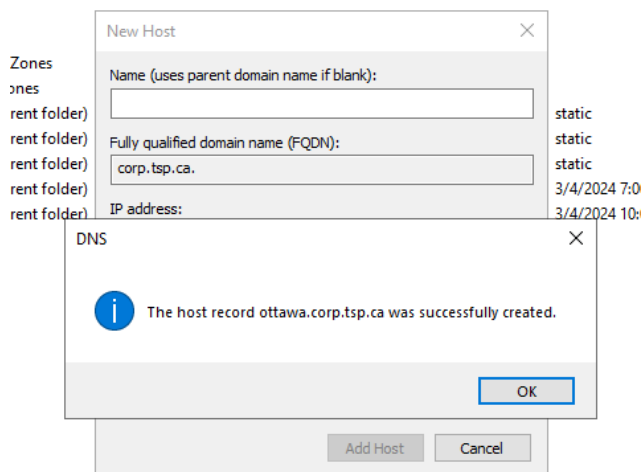
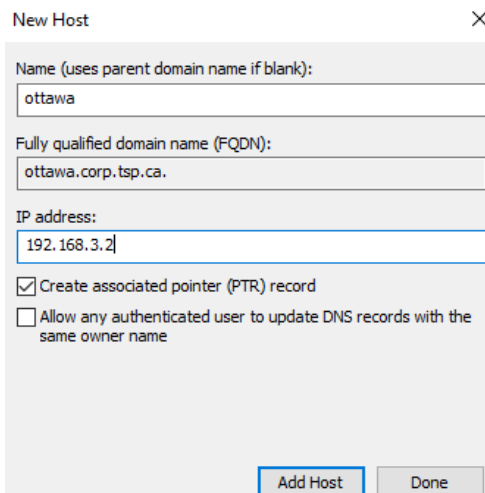
Create an A record in the Toronto's DC and see if it replicates to Vancouver's DC:

- On DC2, open **DNS Manager**. Create a new **A record** in the corp.tsp.ca forward lookup zone

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



- Enter 'ottawa' as the name and 192.168.3.2 as the IP. Click Add Host



- Note: If the process is refused, restart the DNS Server
 - o DC2 > Server Manager > Tools > DNS > Right click DC2 > All Tasks > Restart

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

- On **DC1**, open DNS Manager to verify '**ottawa**' A record entry
- If refreshing doesn't force it appear you can force the entry to arrive by running the command '**repadmin /syncall /AeD**' in PowerShell followed by '**dnscmd /zoneupdatefromds corp.tsp.ca**'

```
DC1 on STEVE-PC - Virtual Machine Connection
File Action Media View Help

Administrator: Windows PowerShell

PS C:\Windows\system32> repadmin /syncall /AeD
Syncing all NC's held on DC1.
Syncing partition: DC=ForestDnsZones,DC=corp,DC=tsp,DC=ca
CALLBACK MESSAGE: The following replication is in progress:
  From: dd54606f-b7da-46fa-9652-392f2d625b2b._msdcs.corp.tsp.ca
  To   : 8d3395d1-11f3-4b34-984b-c52bff5bb45c._msdcs.corp.tsp.ca
CALLBACK MESSAGE: The following replication completed successfully:
  From: dd54606f-b7da-46fa-9652-392f2d625b2b._msdcs.corp.tsp.ca
  To   : 8d3395d1-11f3-4b34-984b-c52bff5bb45c._msdcs.corp.tsp.ca
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

PS C:\Windows\system32> dnscmd /zoneupdatefromds corp.tsp.ca

DNS Server . update zone corp.tsp.ca
  Status = 0 (0x00000000)
Command completed successfully.

PS C:\Windows\system32> _
```

- Now check:

DC1 on STEVE-PC - Virtual Machine Connection

File Action Media View Help

DNS Manager

File Action View Help

Name	Type	Data	Tim
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[85], dc1.corp.tsp.ca, host...	stat
(same as parent folder)	Name Server (NS)	dc2.corp.tsp.ca.	stat
(same as parent folder)	Name Server (NS)	dc1.corp.tsp.ca.	stat
(same as parent folder)	Host (A)	192.168.2.2	3/4,
(same as parent folder)	Host (A)	192.168.3.2	3/4,
dc1	Host (A)	192.168.2.2	stat
dc2	Host (A)	192.168.3.2	stat
Ottawa	Host (A)	192.168.3.2	stat

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Create an A record in the Vancouver's DC and see if it replicates to Toronto's DC:

- Enter 'surrey' as the name and 192.168.2.2 as the IP. Click Add Host

DNS

×



The host record surrey.corp.tsp.ca was successfully created.

OK

- On DC2 (Toronto) - force the entry to arrive by running the command 'repadmin /syncall /AeD' in PowerShell followed by 'dnscmd /zoneupdatefromds corp.tsp.ca'

DC2 on STEVE-PC - Virtual Machine Connection

File Action Media View Help

DNS Manager

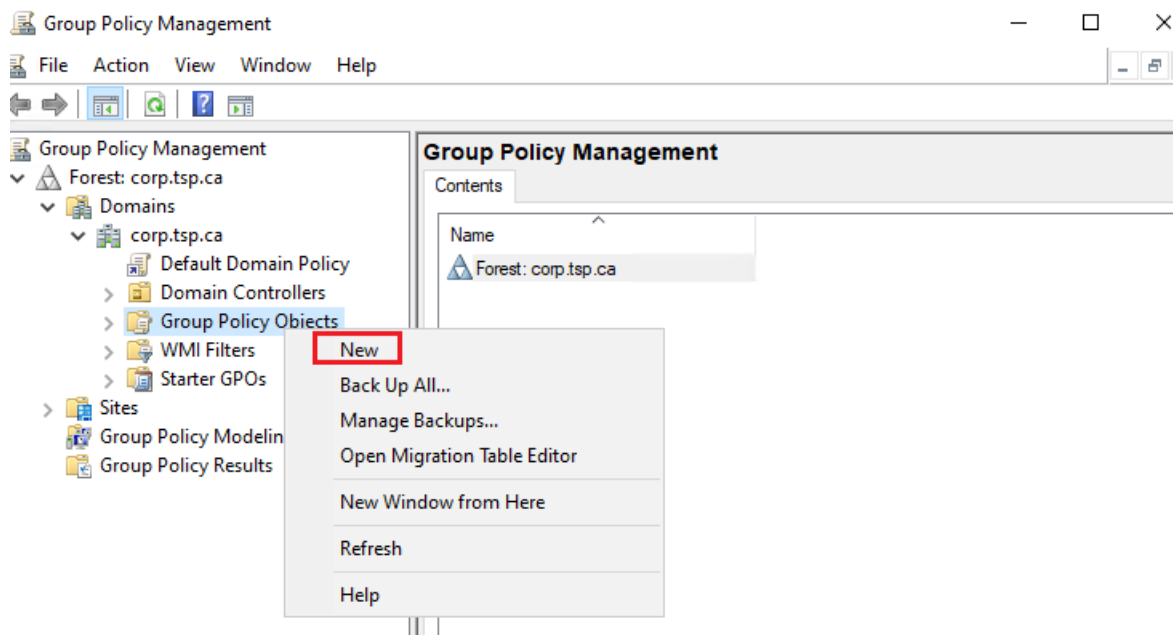
File Action View Help

DNS	Name	Type	Data	Timestamp
DC2				
Forward Lookup Zones				
_msdcs.corp.tsp.ca				
corp.tsp.ca				
_msdcs	_msdcs			
_sites	_sites			
_tcp	_tcp			
_udp	_udp			
DomainDnsZones	DomainDnsZones			
ForestDnsZones	ForestDnsZones			
(same as parent folder)	(same as parent folder)	Start of Authority (SOA)	[86], dc2.corp.tsp.ca., host...	static
(same as parent folder)	(same as parent folder)	Name Server (NS)	dc1.corp.tsp.ca.	static
(same as parent folder)	(same as parent folder)	Name Server (NS)	dc2.corp.tsp.ca.	static
(same as parent folder)	(same as parent folder)	Host (A)	192.168.2.2	3/4/2024 7:00:00 PM
(same as parent folder)	(same as parent folder)	Host (A)	192.168.3.2	3/4/2024 10:00:00 PM
dc1	dc1	Host (A)	192.168.2.2	static
dc2	dc2	Host (A)	192.168.3.2	static
Ottawa	Ottawa	Host (A)	192.168.3.2	static
surrey	surrey	Host (A)	192.168.2.2	static
Reverse Lookup Zones				
Trust Points				
Conditional Forwarders				

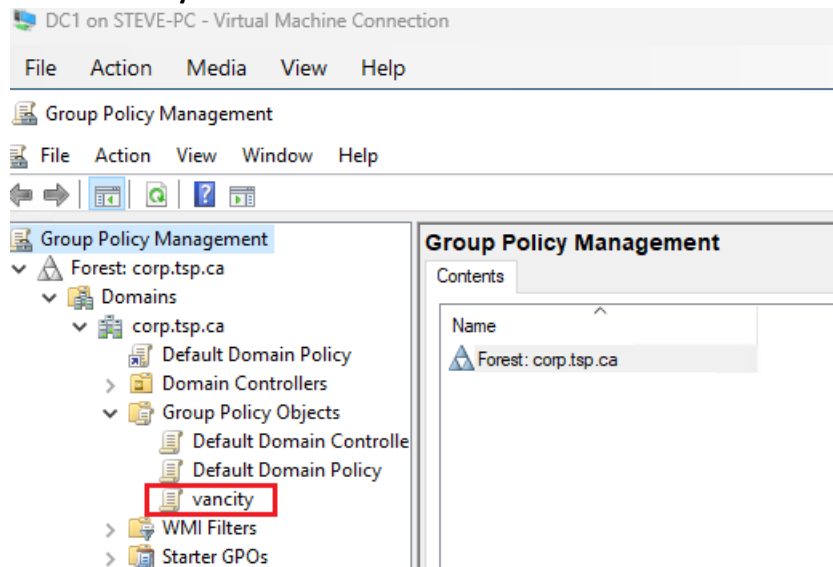
Create a new group policy (no settings need to be defined) in the Vancouver's DC and see if it replicates to Toronto's DC:

- **DC1 > Server Manager > Tools > Group Policy Management**
 - o Expand Forest > Domains > corp.tsp.ca > Right click **Group Policy Objects > New**

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

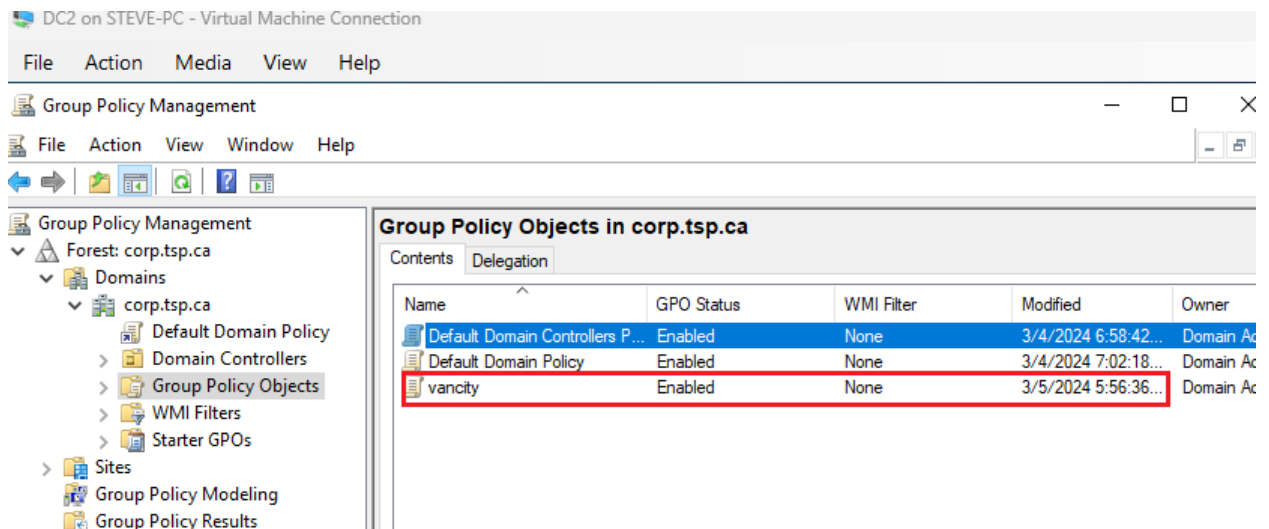


- Name: '**vancity**'



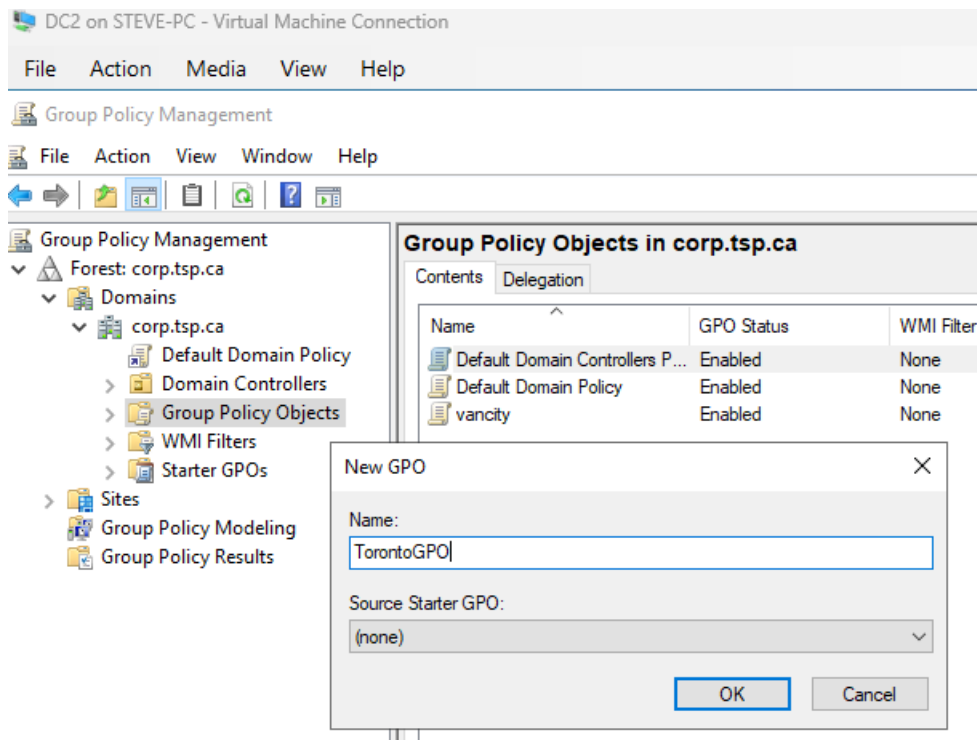
- Navigate over to **DC2**, open Group Policy Management – Expand Forest > Domains > corp.tsp.ca > click **Group Policy Objects**

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



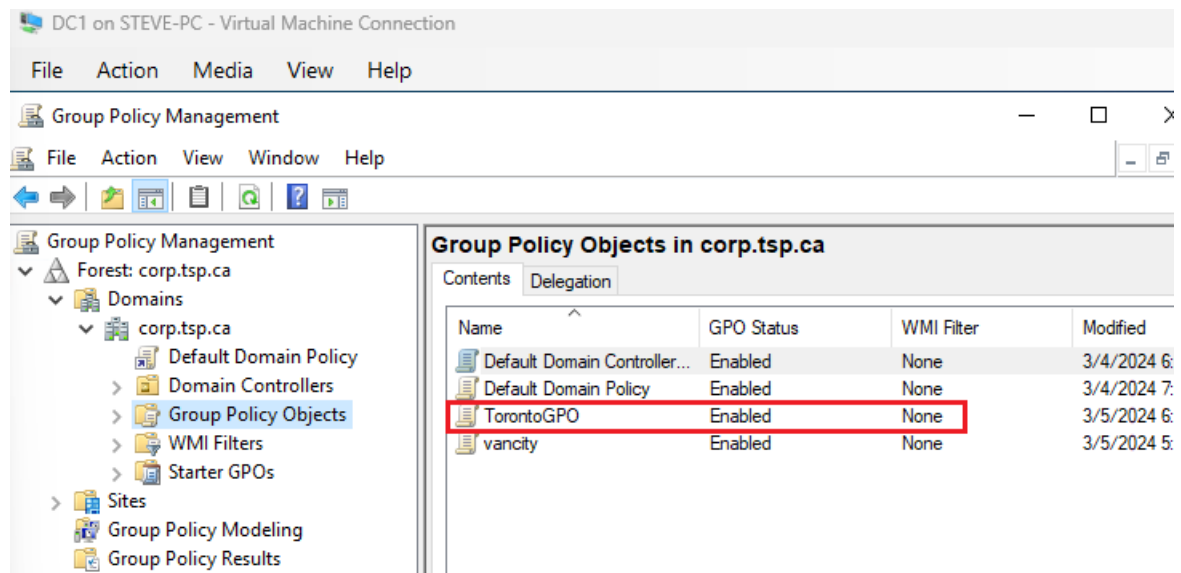
Create a new group policy (no settings need to be defined) in the Toronto's DC and see if it replicates to Vancouver's DC:

- On **DC2**:



- On **DC1**: Verify Replication:

CONFIGURE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL



References:

- <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/#:~:text=IPsec%20tunnel%20mode%20is%20used,addition%20to%20the%20packet%20payload.>
- <https://www.tp-link.com/ca/support/faq/2136/>
- <https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html>
- <https://www.provya.com/blog/pfsense-configuring-a-site-to-site-ipsec-vpn/>
- <https://www.ceos3c.com/pfsense/pfsense-site-to-site-vpn/>
- <https://geekistheway.com/2020/08/01/how-to-allow-ping-on-pfsense-wan/>
- <https://serverfault.com/questions/419658/how-to-speed-up-ad-integrated-dns-zone-replication-server-2008-r2>
- https://kifarunix.com/setup-ipsec-site-to-site-vpn-tunnel-on-pfsense/?expand_article=1