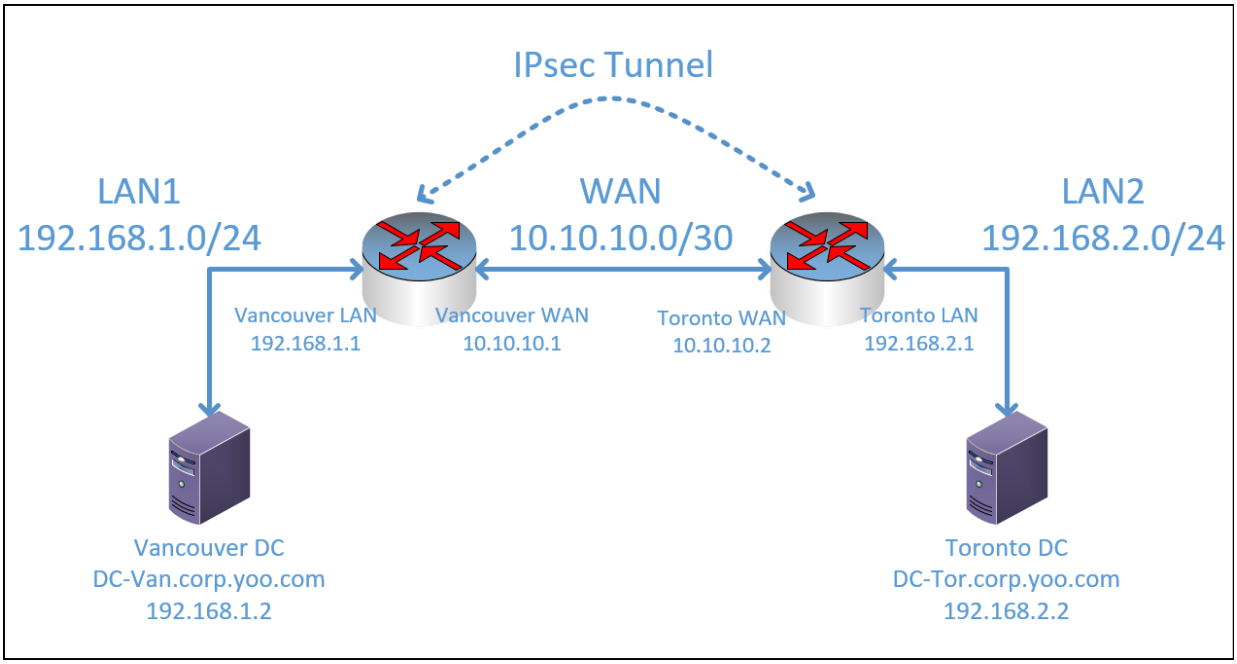
JAY YOO
2/16/23

GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Contents

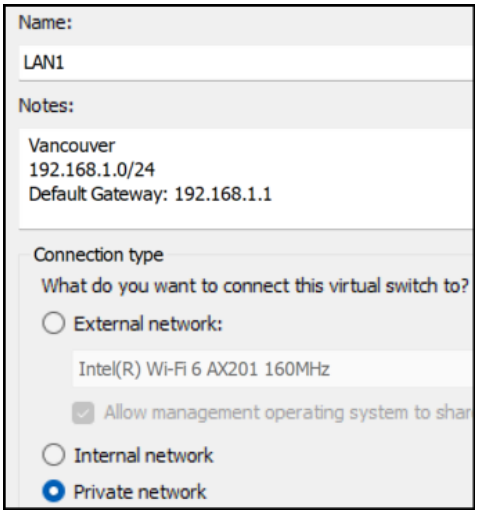
Network Diagram

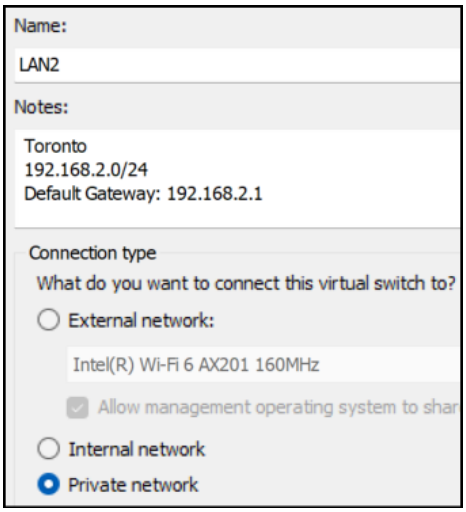


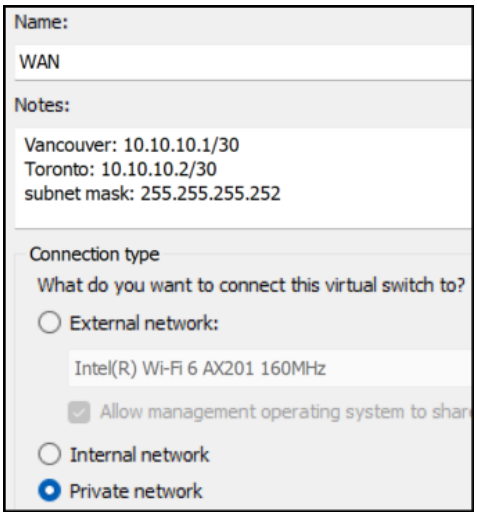
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Activity 1: Create the Virtual Switches

Create all required **private** vSwitches. (WAN facing subnet must only have two usable host IPs.)







GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Activity 2: Configure the External Devices

Create a **pfSense** routers that will route the two networks together so communication between sites can be made. Set static IPs on the pfSense routers' interfaces (Both Vancouver and Toronto). You can set interface IP addresses by selecting **Option 2**. Do not use DHCP assignment for IP addresses.

```
Hyper-V Virtual Machine - Netgate Device ID: 0b1c2121631297f85d2c

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on Van ***

 WAN (wan)       -> hn0        -> v4: 10.10.10.1/30
 LAN (lan)       -> hn1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Vancouver

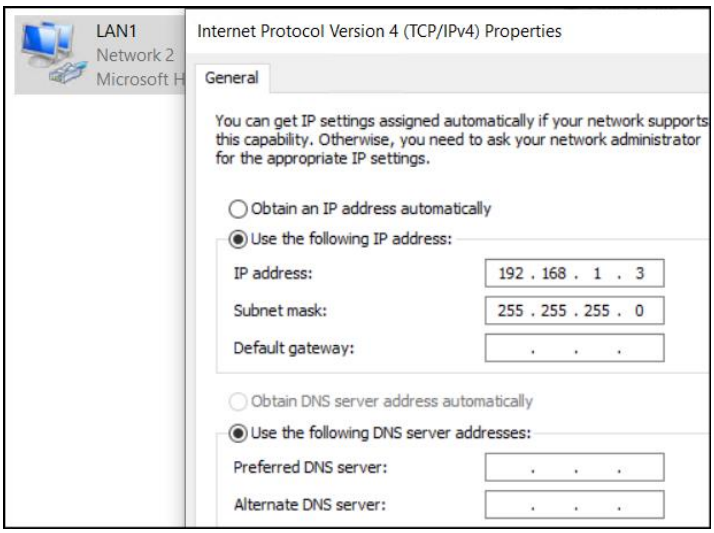
```
Hyper-V Virtual Machine - Netgate Device ID: 9de5fa9533dc51c4944e

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on Tor ***

 WAN (wan)       -> hn0        -> v4: 10.10.10.2/30
 LAN (lan)       -> hn1        -> v4: 192.168.2.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```

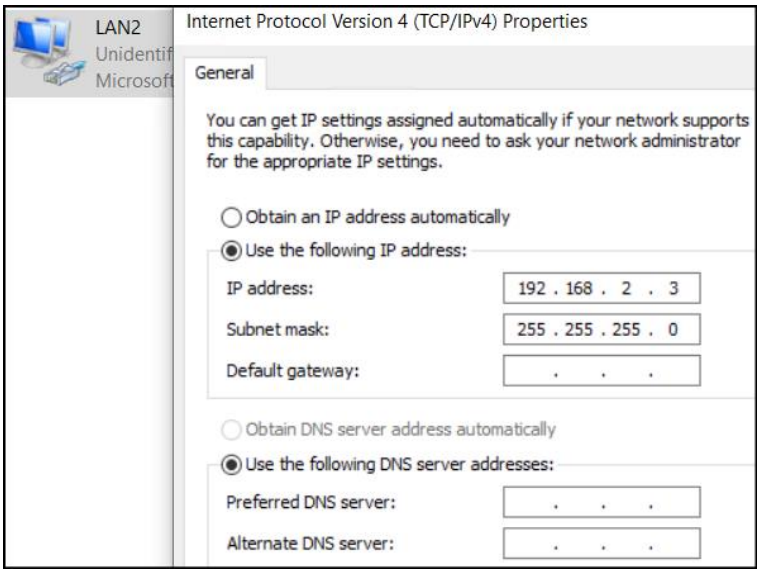
Toronto

GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Activity 3: Configure IPsec VPN tunnel

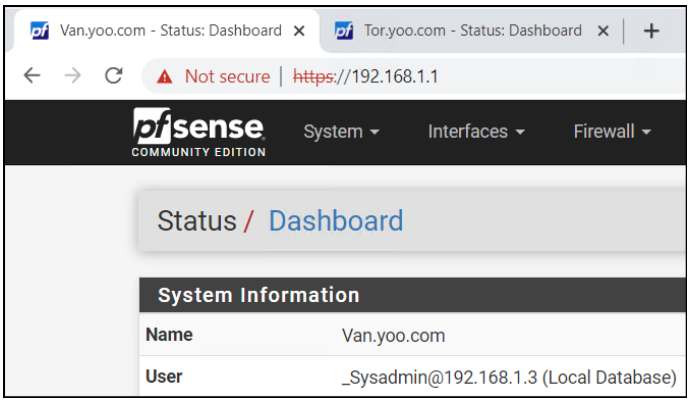
To access webConfigurator of pfSense, you need connection to **LANs**. In advance, you can create two servers which will become Domain Controllers of each site so that each server can be used to configure its respective pfSense router. Also, you can set up one VM with two NICs instead to access two pfSense routers.



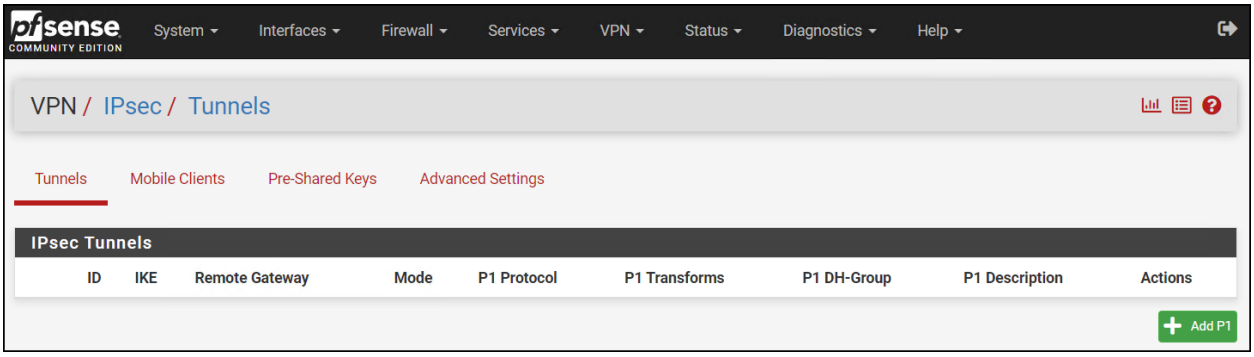


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Access webConfigurator router at Vancouver site. Default administrative account has a username **admin** and a password **pfsense**. Adjust clock on pfSense.



Click **VPN -> IPsec**. To add a new IPsec phase 1, click **Add P1**.



There are two phases of negotiation for an IPsec tunnel. During **phase 1** the two endpoints of a tunnel setup a secure channel between using ISAKMP to negotiate the IKE SA entries and exchange keys. This also includes authentication, checking identifiers, and checking the pre-shared keys (PSK) or certificates. When phase 1 is complete the two ends can exchange information securely, but they have not yet decided which traffic will traverse the tunnel or its encryption.

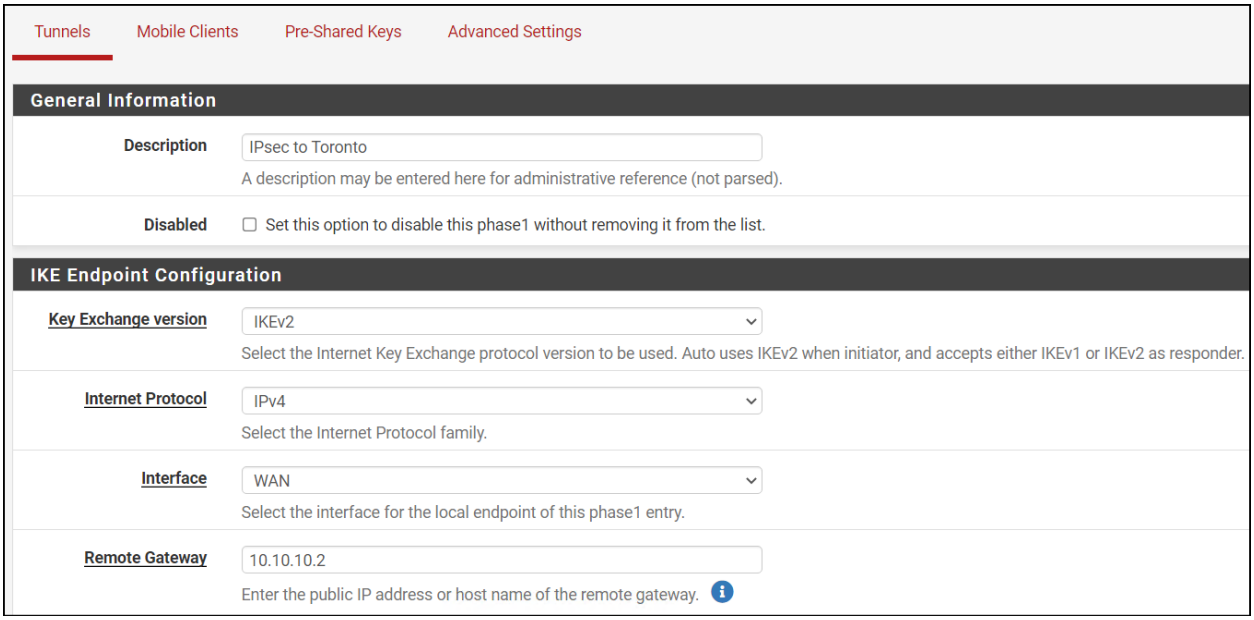
In **phase 2** the two endpoints negotiate how to encrypt and send the data for the private hosts based on security policies. This part builds an entry referred to as a "Child SA". This forms the connection used to transfer data between the endpoints and clients whose traffic is handled by those endpoints. If the policies on both side agree and a phase 2 child SA is successfully established the tunnel will be up and ready for use. (https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/terms.html)

GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

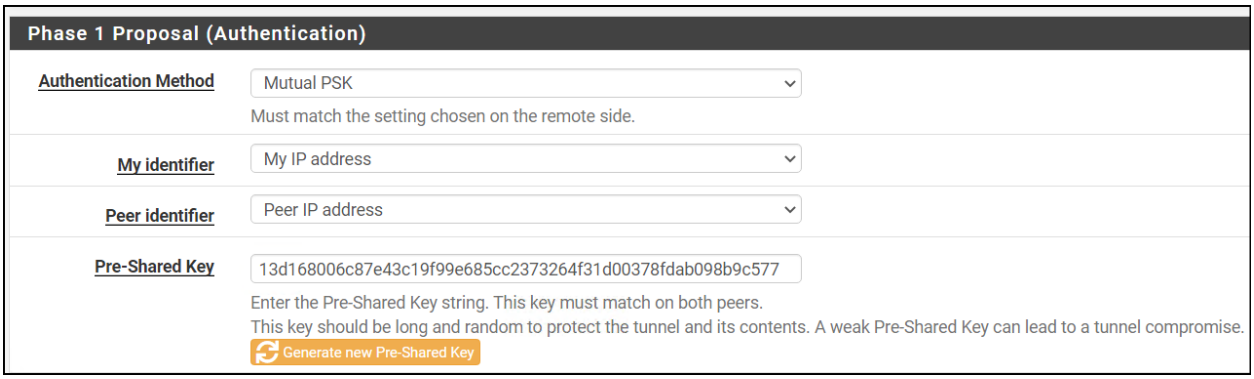
For general guides of IPsec site-to-site VPN configuration with pfSense, follow this link:

- https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html

Put **Description** regarding this tunnel. **Remote Gateway** is the WAN address of Toronto Site.

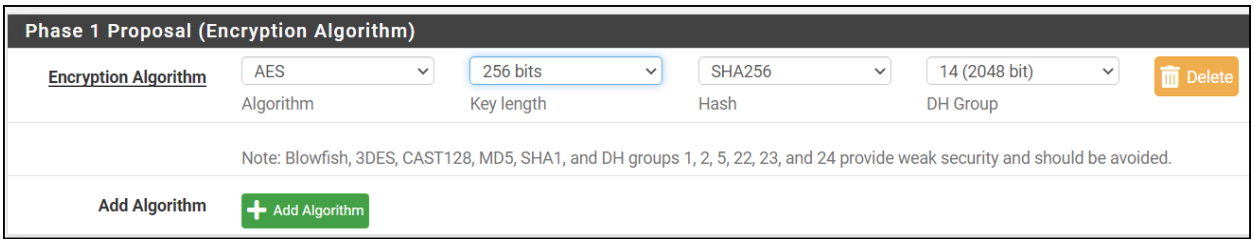


Create **Pre-Shared Key** for authentication. For our test purposes, you can use any key (ex. Pa$$w0rd), but I clicked **Generate new Pre-Shared Key** for strong security. The exact same key must be entered into the tunnel configuration for Toronto Site later, so copy and paste it elsewhere. (13d168006c87e43c19f99e685cc2373264f31d00378fdab098b9c577)

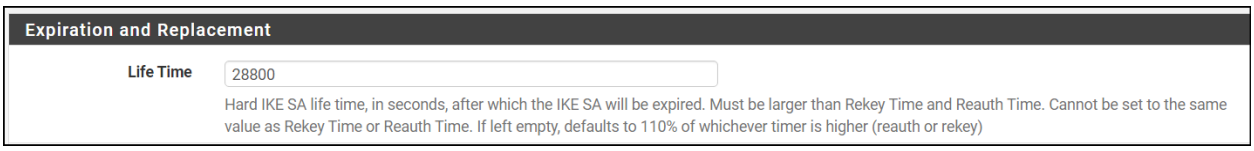


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

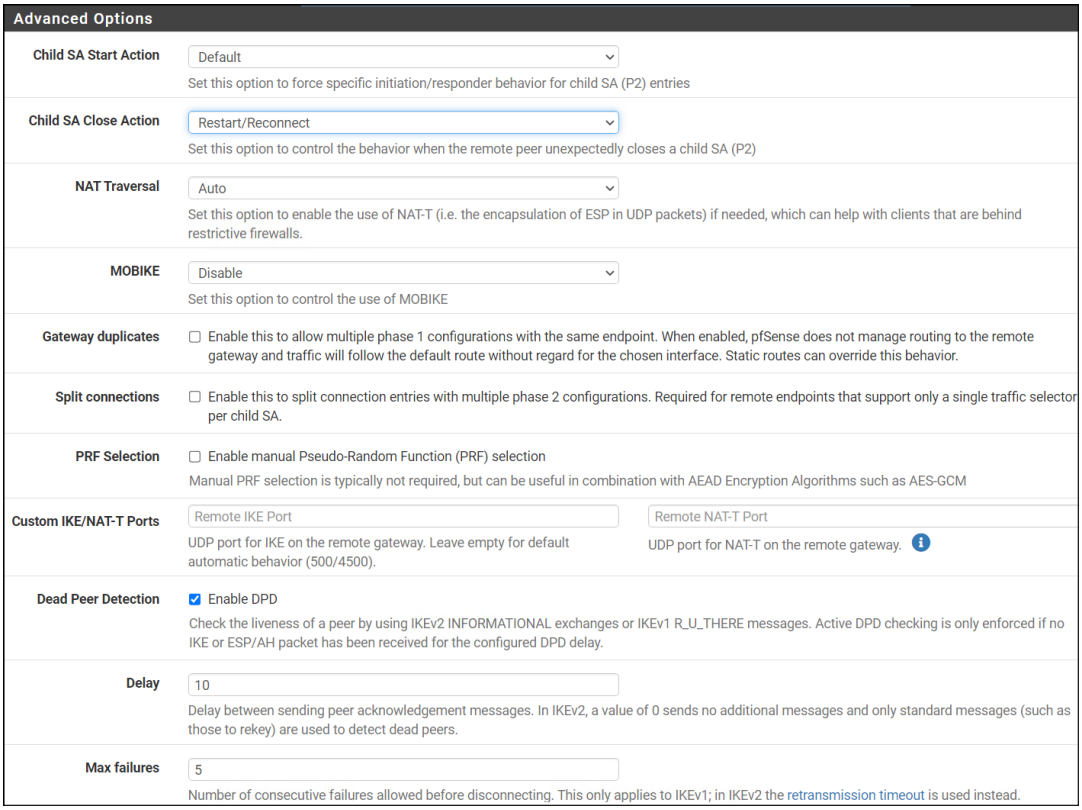
Change **Key length** to 256 bits. Use SHA256 if both sides support it, otherwise use the strongest **Hash** supported by both endpoints.



Notice that **Life Time** is set to 28800.

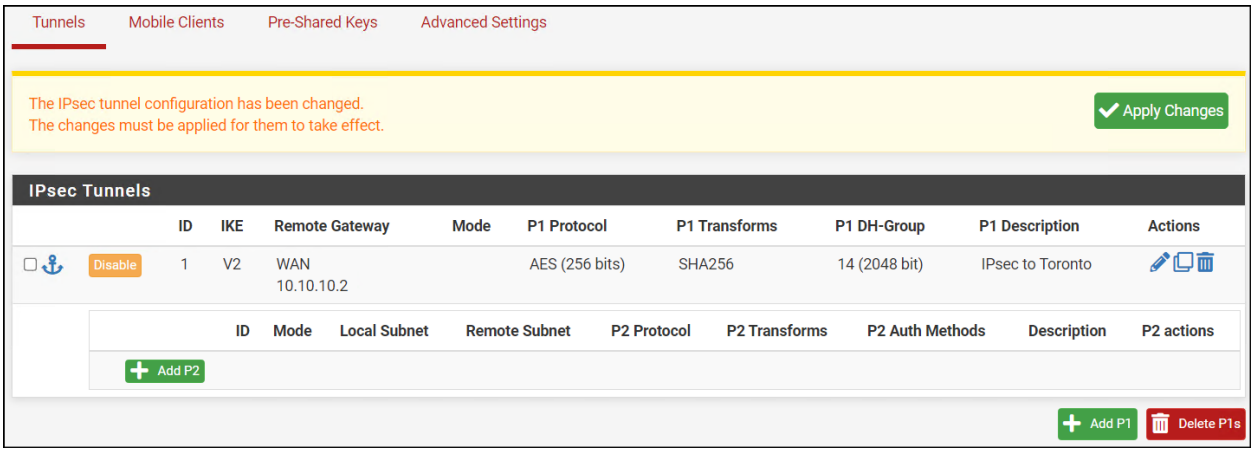


Set **Child SA Close Action** to Restart/Reconnect so that the phase 2 entries will be reconnected if they get disconnected. Check that **Dead Peer Detection** is marked. Click **Save**.

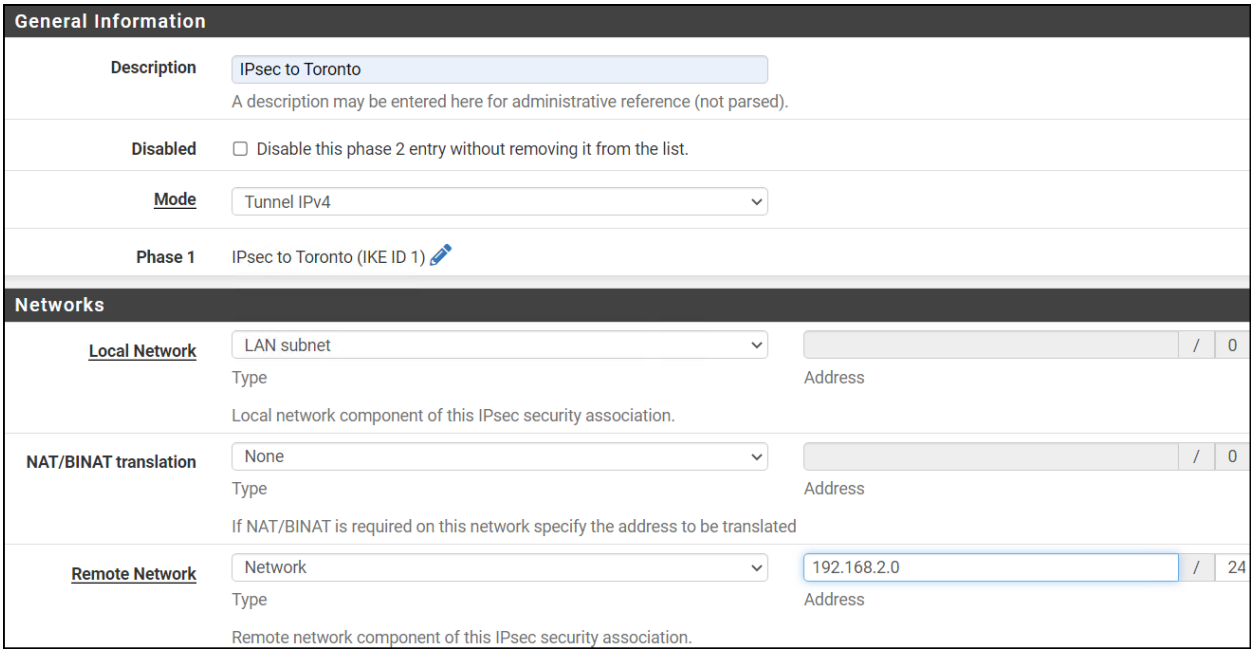


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Click **Show Phase 2 Entries -> Add P2**.

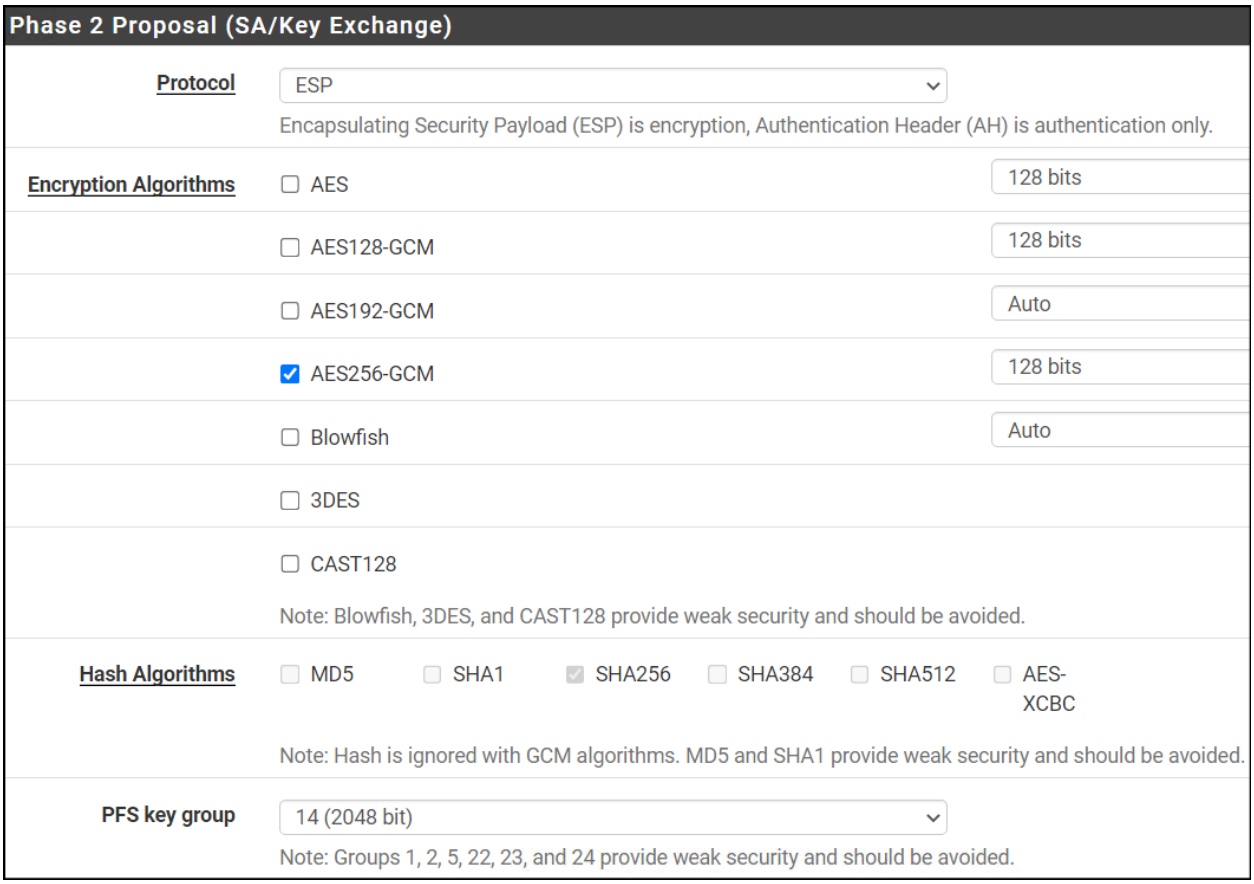


Put **Description**. Set **Remote Network** as the internal network of Toronto Site.

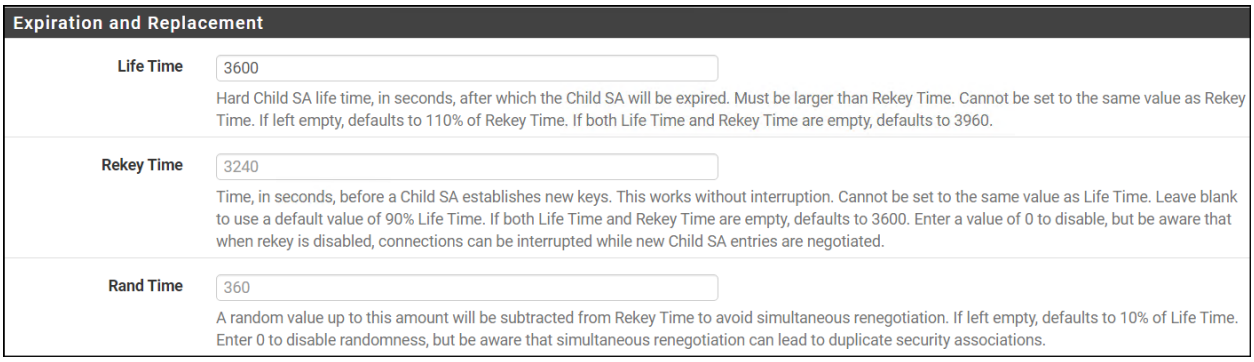


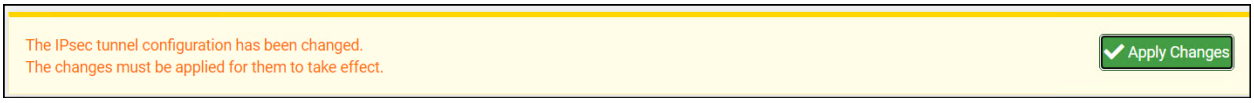
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Use AES256-GCM with a 128-bit key length for **Encryption Algorithms**. AES-GCM must be supported by both endpoints to be used.



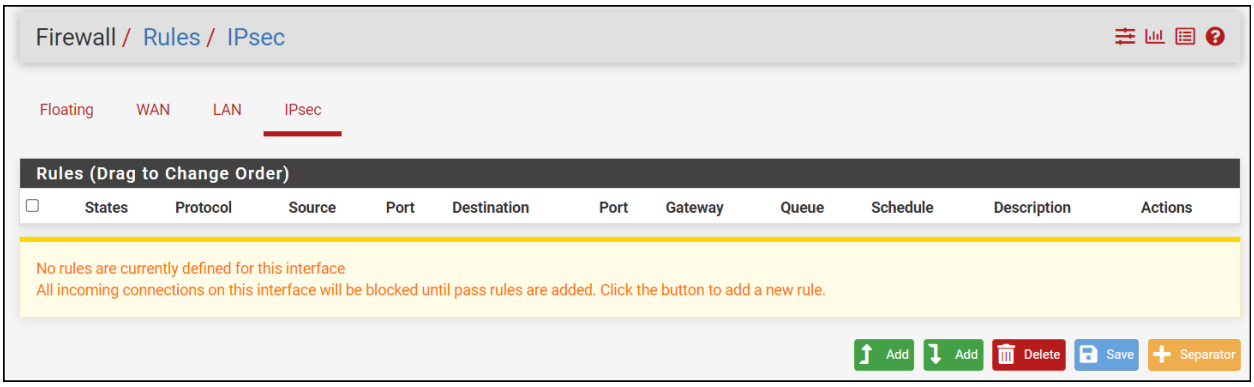
Use default 3600 for **Life Time**. Click **Save -> Apply Changes**.

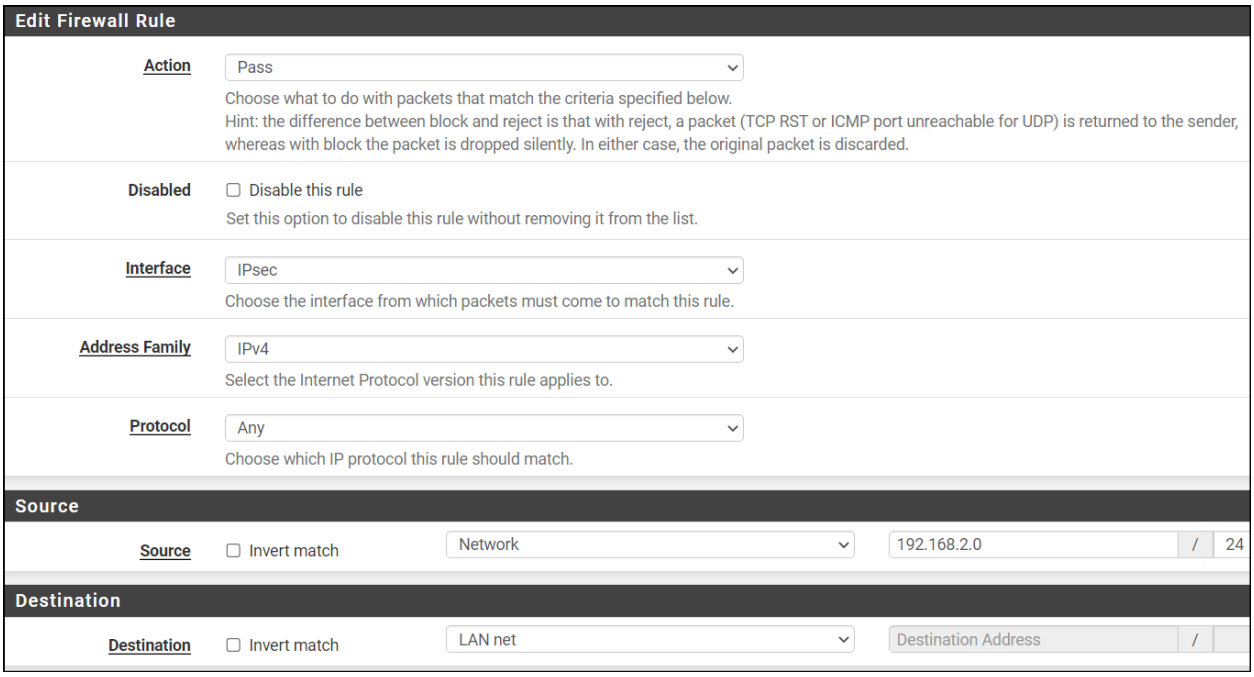


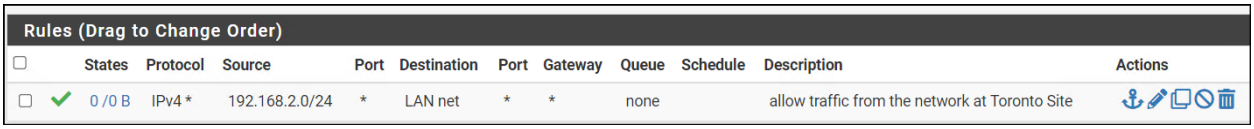


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Navigate **to Firewall -> Rules** on the **IPsec** tab and add rules there to pass traffic from the remote side of the VPN.

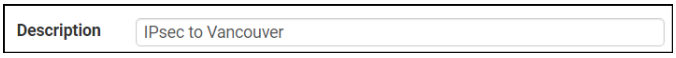






Now we need to configure Toronto Site as well for IPsec tunneling. Repeat general configuration process for Vancouver Site with a few differences.

Put adequate **Description**. **Remote Gateway** must be set to WAN address of Vancouver Site.



GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Remote Gateway	10.10.10.1 Enter the public IP address or host name of the remote gateway.

Make sure to use same **Pre-Shared Key**.

Pre-Shared Key	13d168006c87e43c19f99e685cc2373264f31d00378fdab098b9c577

Set **Life Time** 10% higher than Vancouver Site's. With Toronto Site's Life Time set higher, Vancouver Site will primarily manage IKE SA renegotiation, reducing the chance of conflicts. (https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec-duplicate-sa.html)

Life Time	31680 Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Set **Child SA Start Action** to **None (Responder Only)** so that this endpoint will not initiate on its own but will wait for Vancouver Site to initiate. Set this endpoint to **Close connection and clear SA** so that the phase 2 will not automatically reconnect, since Vancouver Site will be managing that. Click **Save**.

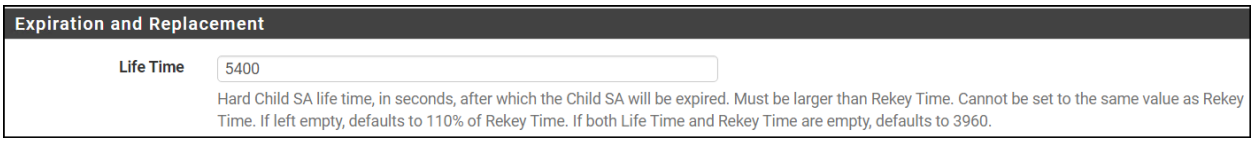
Advanced Options	
Child SA Start Action	None (Responder Only) Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action	Close connection and clear SA Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)

At the phase 2 configuration stage, put adequate **Description**. Set **Remote Network** as internal network for Vancouver Site.

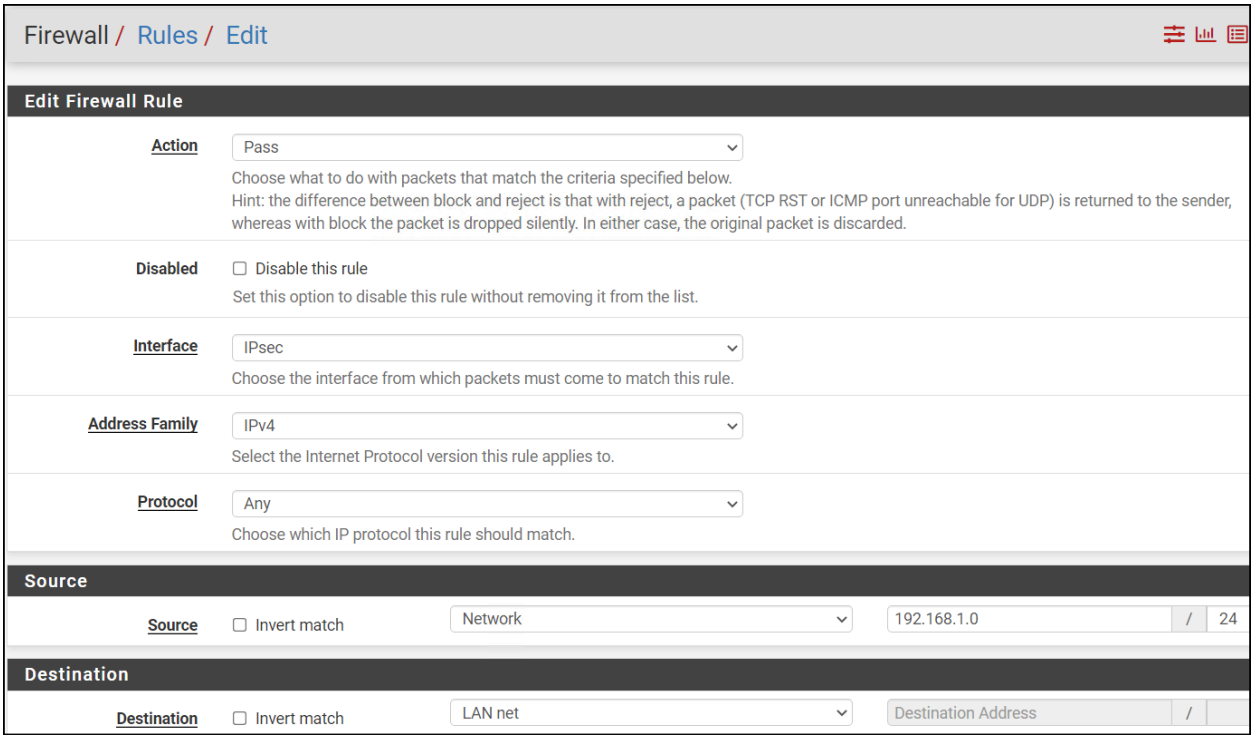
Remote Network	Network Type	192.168.1.0 / 24 Address	
	Remote network component of this IPsec security association.		

GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

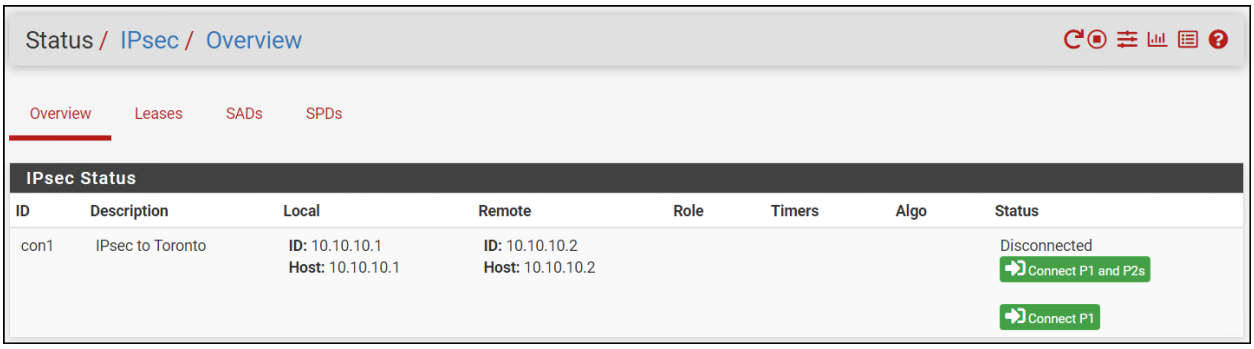
Set **Life Time** as 5400.



Create a firewall rule for IPsec interface.

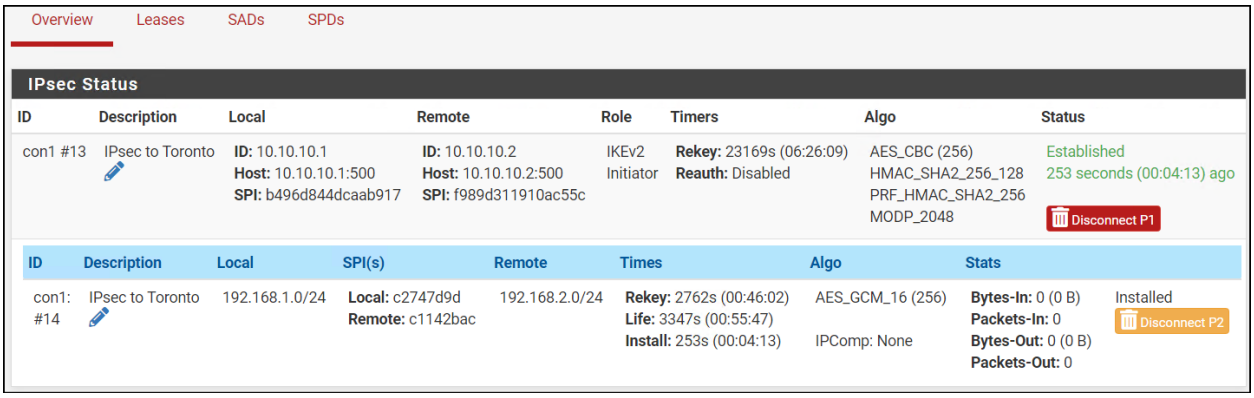


Click **Status -> IPsec -> Connect P1 and P2s** from pfSense on Vancouver Site because it is set up as initiator. (Toronto Site's pfSense is responder.)



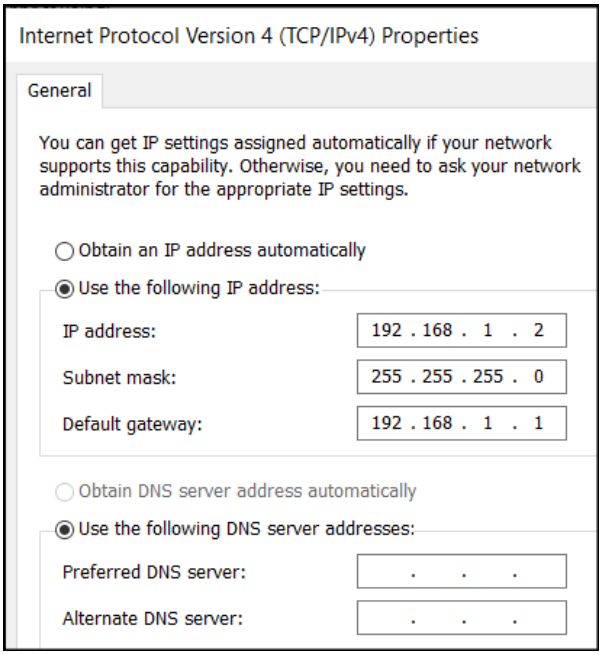
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

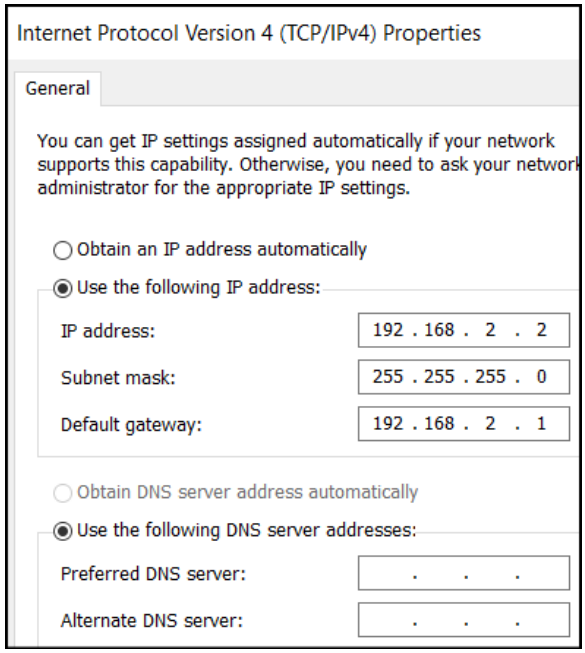
If you configured everything right, the connection should be established.



Activity 4: Configure the Internal Devices

Create two server VMs. Do post-installation tasks on both VMs (Do not create the domain yet). Assign each VM a static IP from the Vancouver Site's and Toronto Site's internal network respectively.





GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Activity 5: Connect the Vancouver Office to the Toronto Office Through IPsec Tunneling

To test connectivity, we need to allow incoming ping requests on both servers first. Open PowerShell on both servers as administrator and type **netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow** to enable ping.

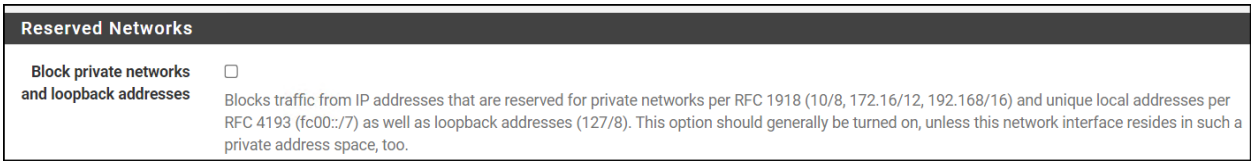
Try pinging from one server to the other. Requests timed out. Try pinging the router on different site too. It timed out as well. (Same result from other site)

```
C:\Users\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

```
C:\Users\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Since ping requests did not return the message “host unreachable” and IPsec tunneling was established, I went back to webConfigurator for pfSense to check other firewall rules.

Click **Interfaces -> WAN** and scroll down to the bottom. Since we are using private IP range for WAN connections, you must disable **Block private networks and loopback addresses** on both pfSense.



GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

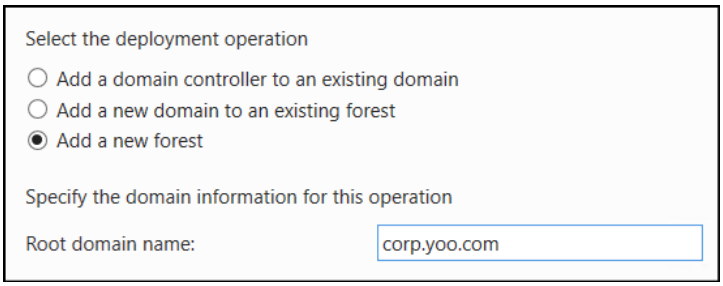
Test connectivity again from both directions. The connectivity is established.

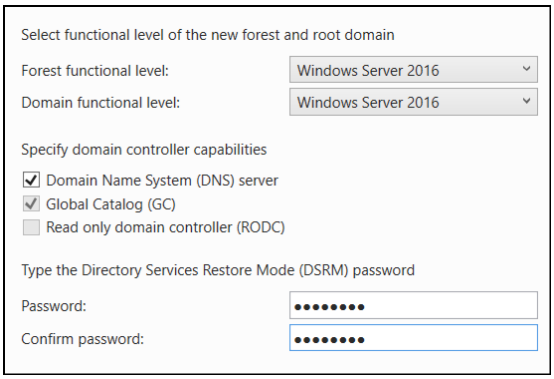
```
C:\Users\Administrator>ping 192.168.2.2

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=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\Users\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

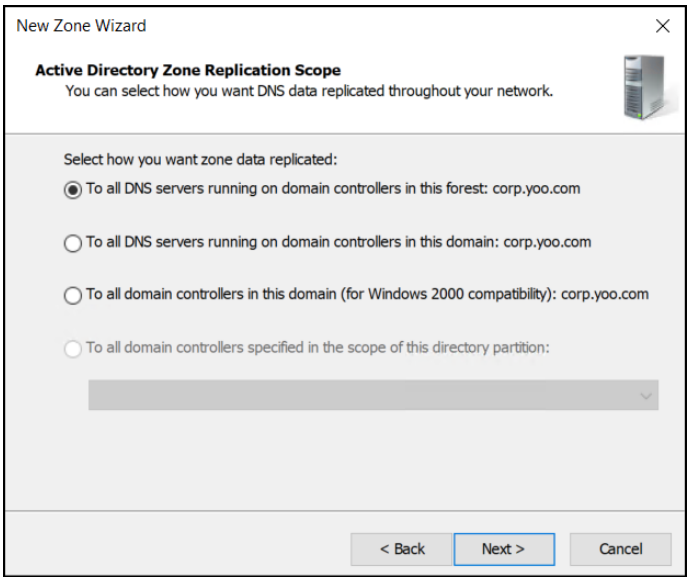
Activity 6: Create the Domain Controllers

First, create a domain controller on Vancouver DC.

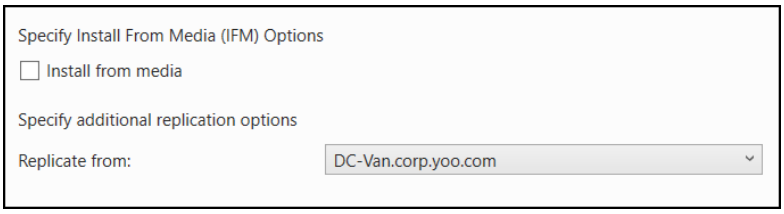




Select **To all DNS servers running on domain controllers in this forest**. Finish installation and configuration.



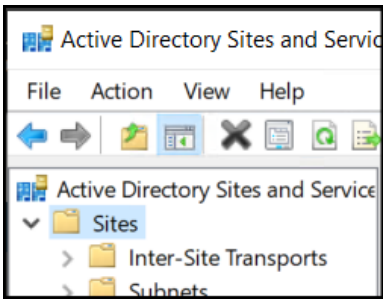
After making **DC-Van** a domain controller, add **DC-Tor** to existing domain. Set preferred DNS server on **DC-Tor** as the IP address of **DC-Van** before starting to install the ADDS role. Choose **Replicate from** the Vancouver domain controller.



Activity 7: Create/Configure Sites and Services within Active Directory

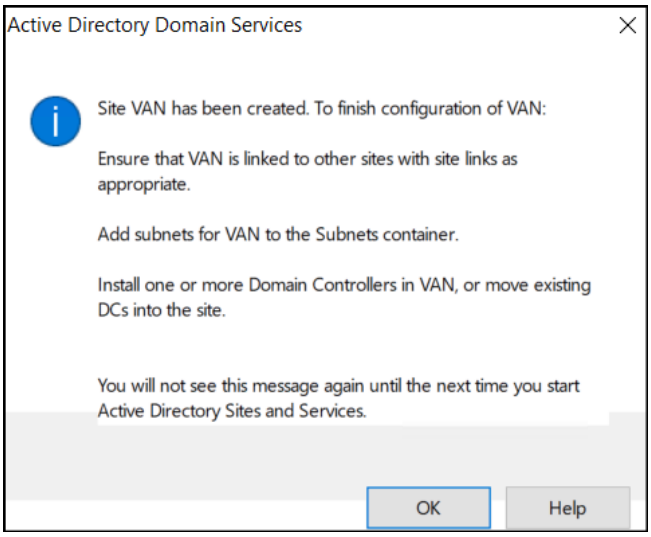
Creating a new site through Active Directory Sites and Services

Open **Active Directory Sites and Services**. Right-click **Sites** and choose **New Site**.



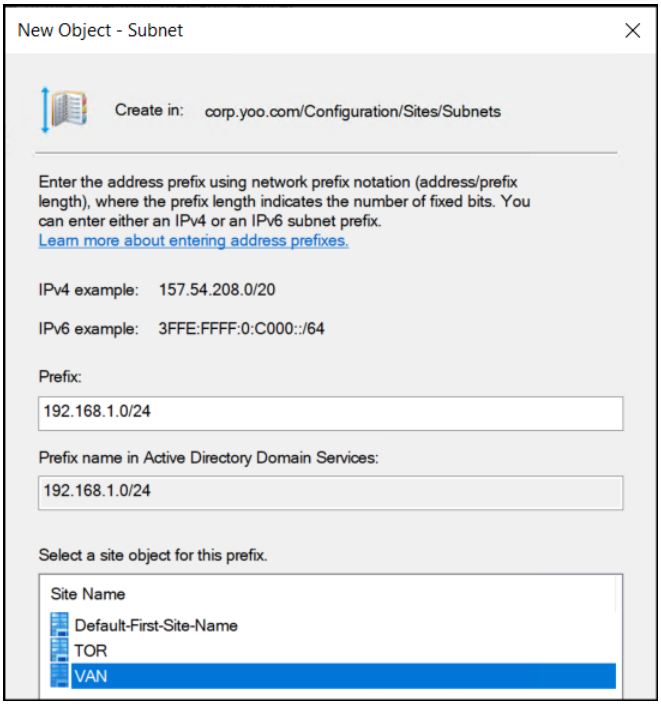
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Enter the site **Name** for Vancouver, select the **DEFAULTIPSITELINK**, and click **OK**. Repeat the steps for Toronto Site.



Creating Subnets

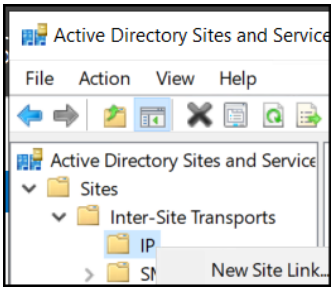
Back to Active Directory Sites and Services MMC, right-click **Subnet** and select **New Subnet**. Read the example to assign **Prefix** of the Vancouver subnet and select Vancouver site you created. Click **OK**. Repeat steps for Toronto. DCs and clients use the subnets you define to determine what site they are in.



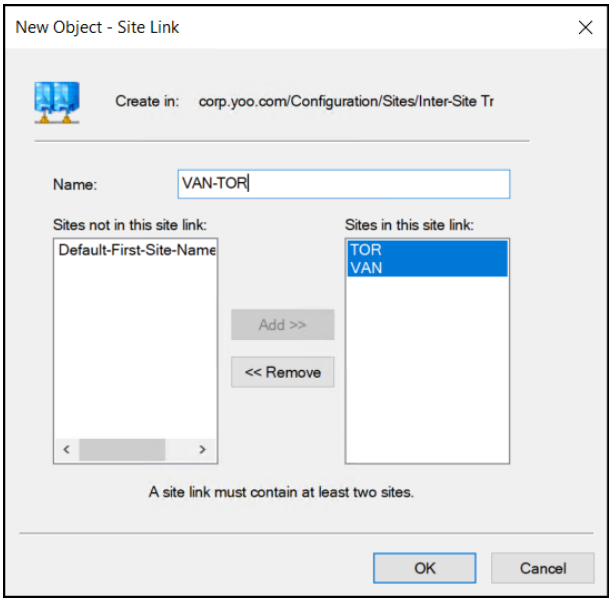
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Creating Site Links

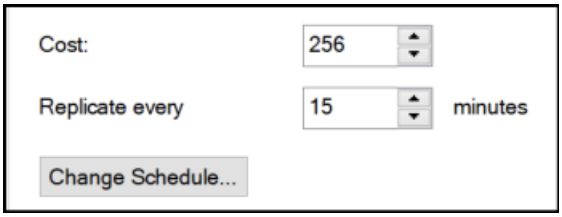
In the Active Directory Sites and Services MMC, click **Inter-Site Transports**, right-click **IP,** and click **New Site Link**.



Enter a desired name for the link, select both Sites, and click **Add**. Click OK to continue.



Right-click the newly created link and choose **Properties**. Change **Cost**, **Replication** interval, and **Schedule**. To determine the cost, visit this link. (https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/determining-the-cost)

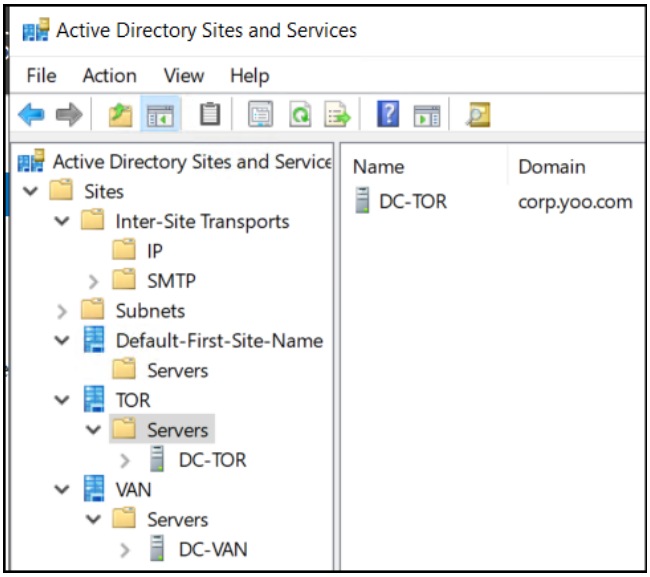


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Create a site link design to connect your sites with site links. Site links reflect the inter-site connectivity and method used to transfer replication traffic. You must connect sites with site links so that domain controllers at each site can replicate Active Directory changes.

Move the Domain Controllers to Their Newly Created Sites

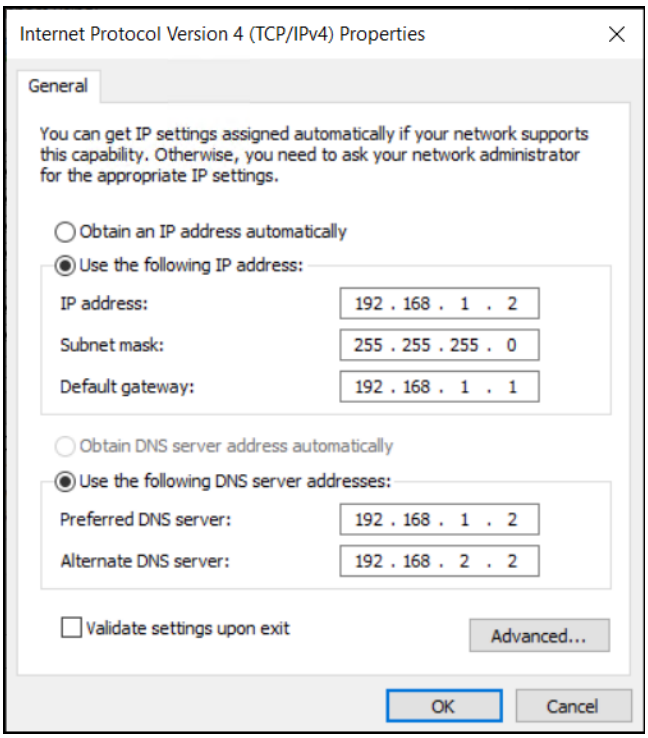
In the Active Directory Sites and Services MMC, navigate to **Default-First-Site-Name -> Servers**. Right-click on the Domain controller required to move and select **Move**. In the **Move Server** window, select the site which will be site the Domain Controller will be moving to and click **OK**. Repeat steps to move the other DC to its site. After the DCs are moved, there is no need for the **DEFAULTIPSITELINK**. Delete it.



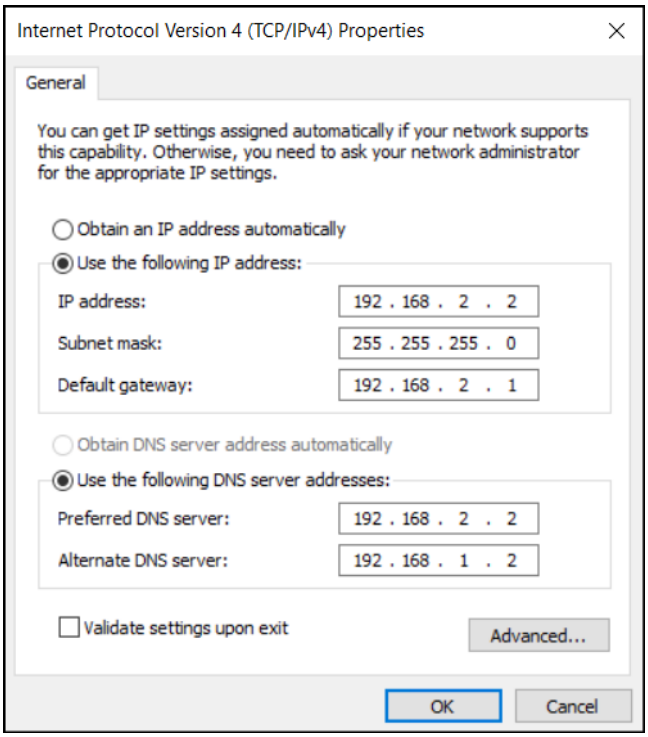
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Test Replication

Check the network configurations on both DCs.



Vancouver



Toronto

GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

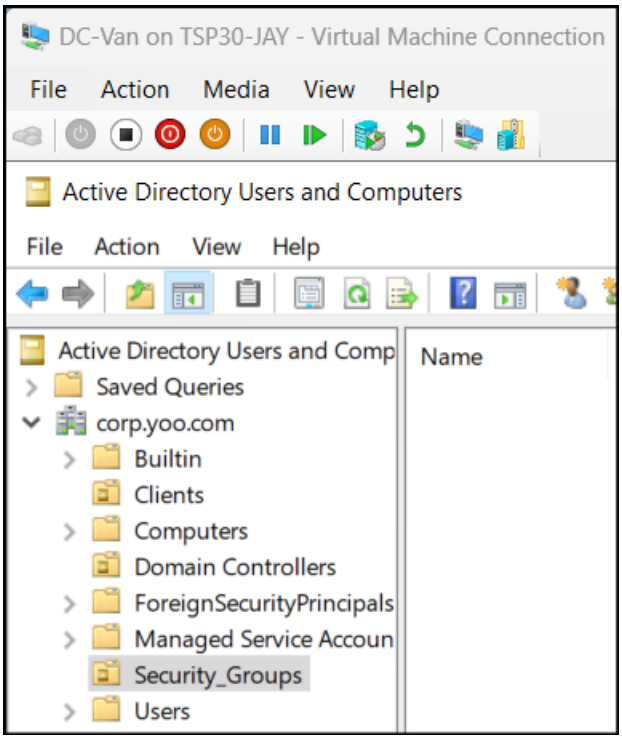
Create an object in the Vancouver DCs ADUC and see if that object is replicated to the Toronto DC. Run this command on Vancouver DC to force-replicate from Vancouver to Toronto.

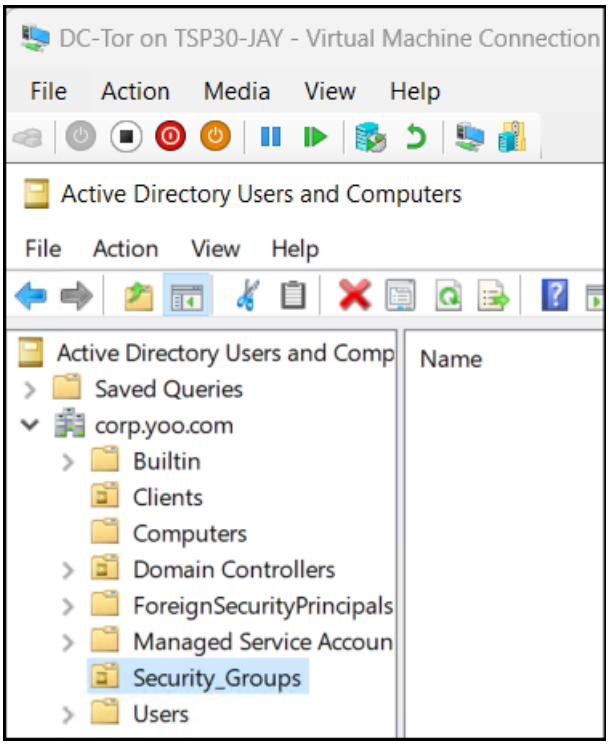
```
PS C:\Windows\system32> repadmin /replicate DC-Tor DC-Van dc=corp,dc=yoo,dc=com
Sync from DC-Van to DC-Tor completed successfully.
```

- **repadmin /replicate <DC Name to Replicate To> <DC Name to Replicate From> <NamingContextDN>**

Create an object in the Toronto DC as well and check replication.

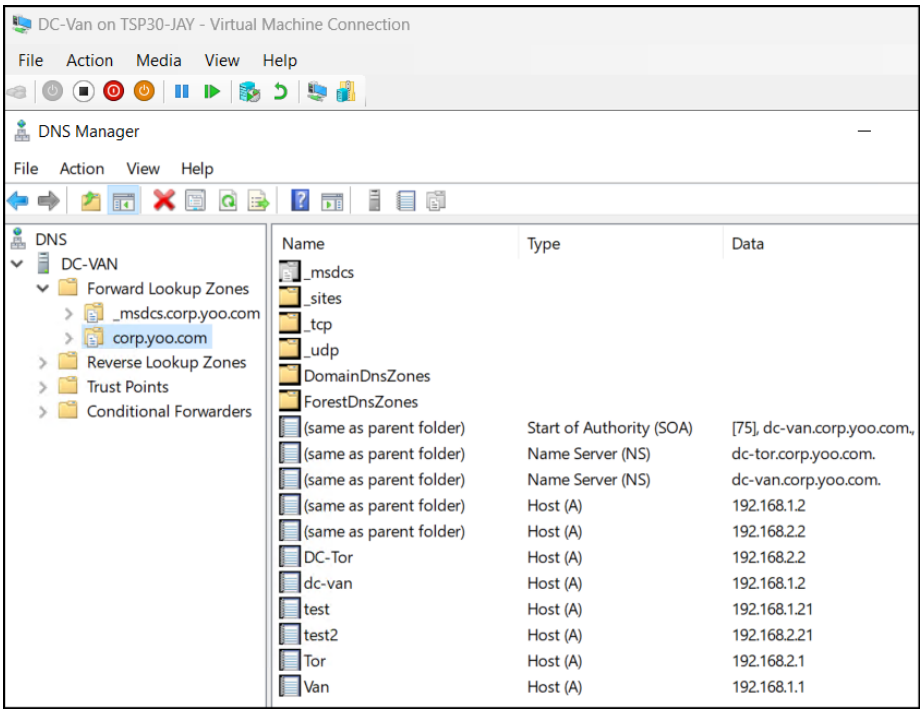
```
PS C:\Windows\system32> repadmin /replicate DC-Van DC-Tor dc=corp,dc=yoo,dc=com
Sync from DC-Tor to DC-Van completed successfully.
```

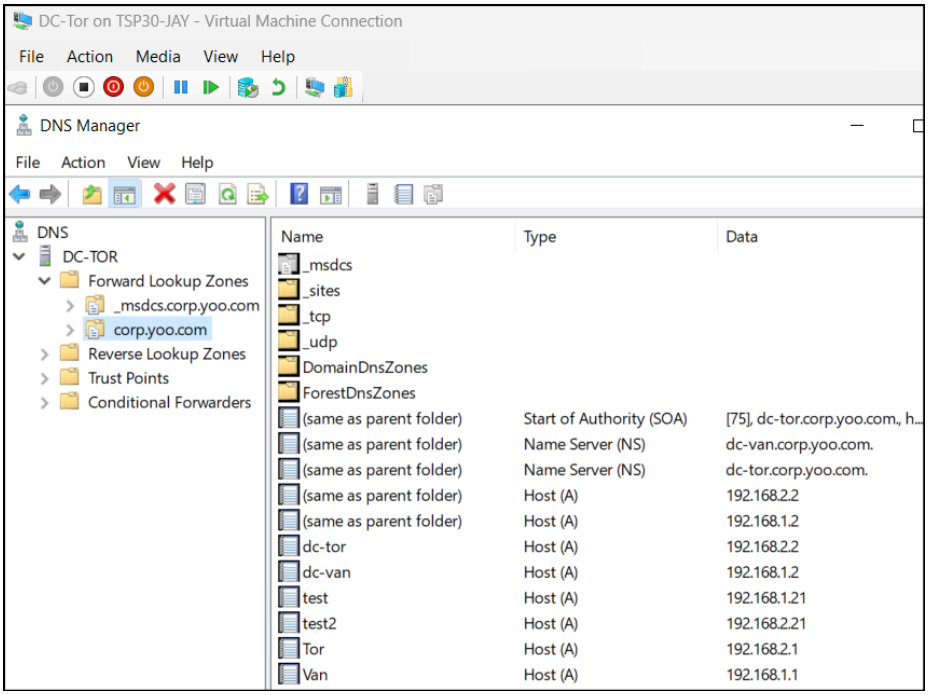




GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

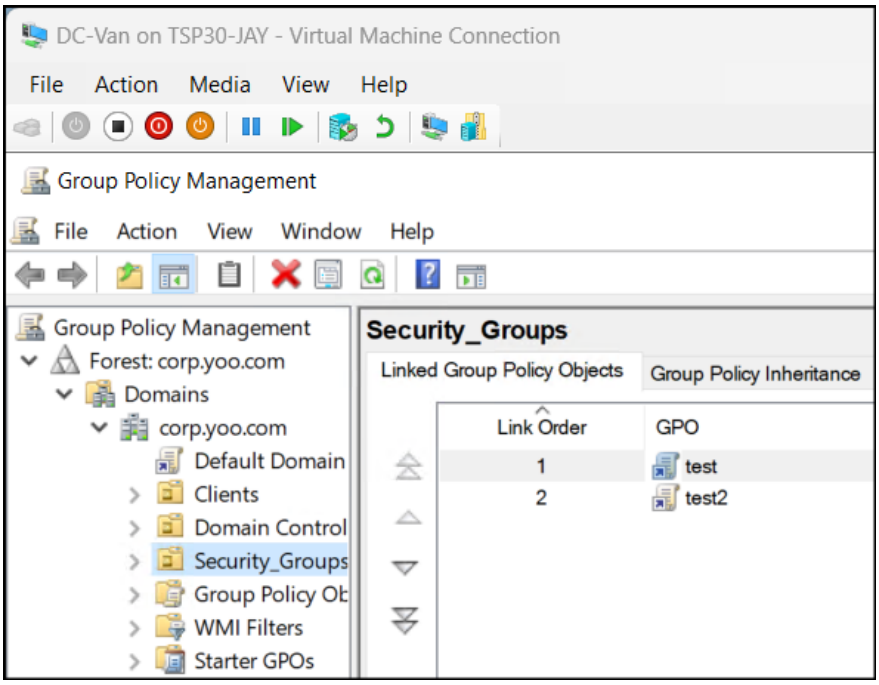
Create an A record in the Toronto's DC and see if it replicates to Vancouver's DC. Do the same Vancouver's DC as well. In the case of DNS records, the above command did not force-replication (nor did the replication method on GUI). Our group had to wait about 15 minutes (our set replication interval) to check the replication.

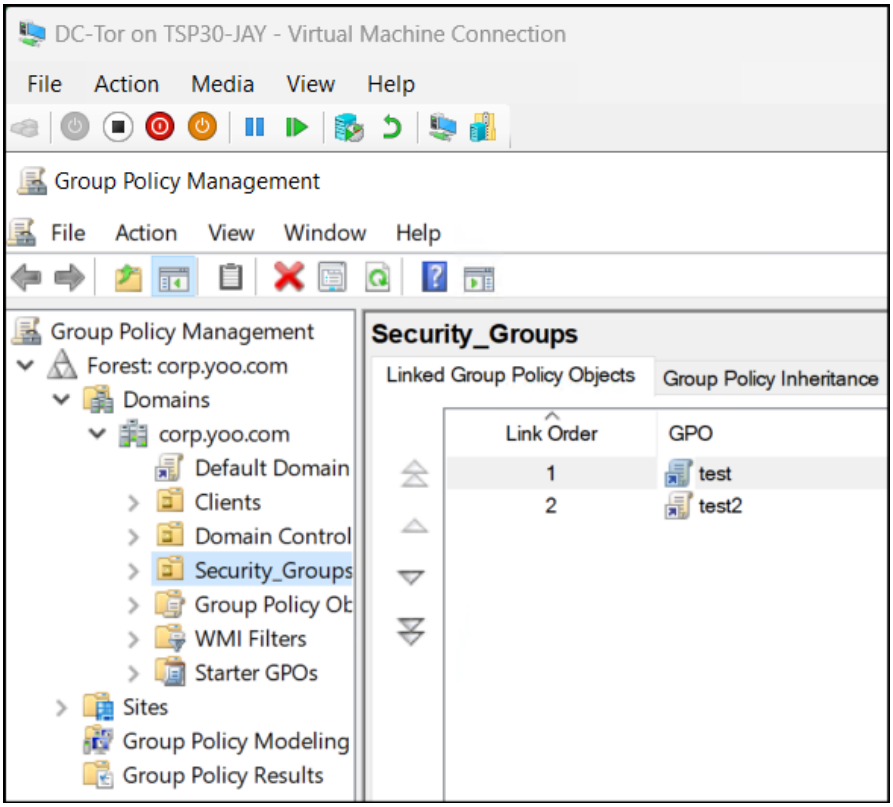




GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

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. Do the same from Toronto's DC.





GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

References

IPsec Terminology: https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/terms.html

IPsec Site-to-Site VPN Example with Pre-Shared Keys:
https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html

Troubleshooting Duplicate IPsec SA Entries:
https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec-duplicate-sa.html

Determining the Cost: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/determining-the-cost

Forcing Replication from One Domain Controller to Another:
https://www.oreilly.com/library/view/active-directory-cookbook/0596004648/ch12s05.html