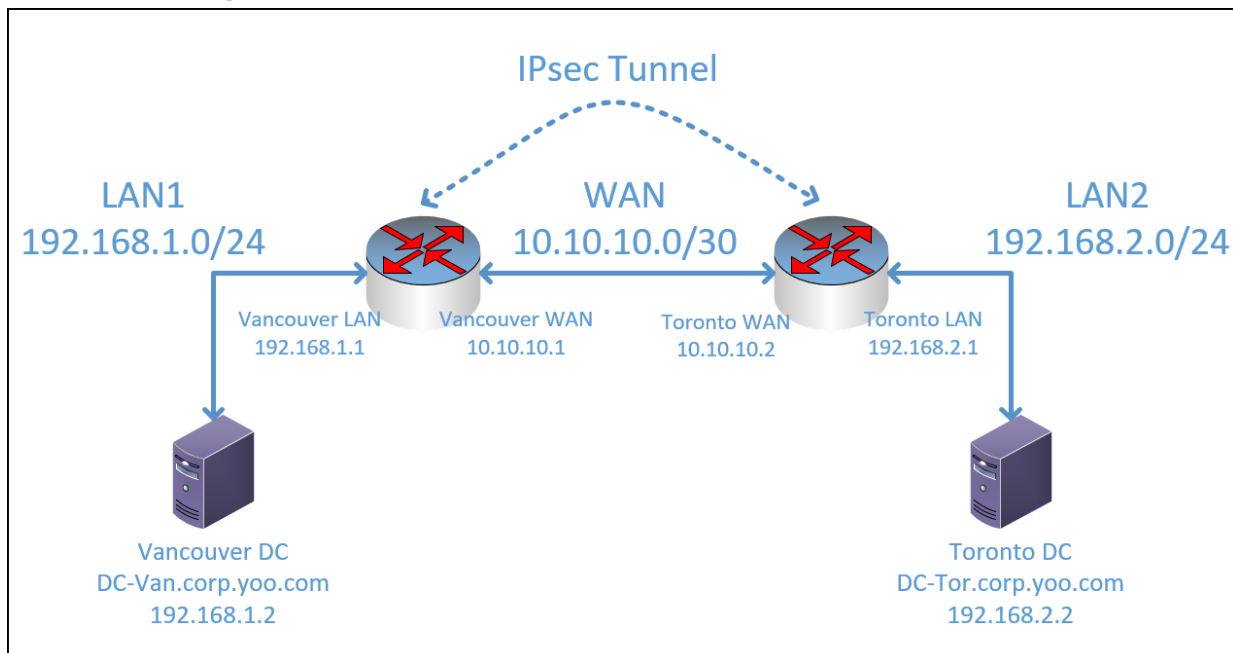


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Contents

Network Diagram	1
Activity 1: Create the Virtual Switches.....	2
Activity 2: Configure the External Devices.....	3
Activity 3: Configure IPsec VPN tunnel	4
Activity 4: Configure the Internal Devices	13
Activity 5: Connect the Vancouver Office to the Toronto Office Through IPsec Tunneling	14
Activity 6: Create the Domain Controllers.....	15
Activity 7: Create/Configure Sites and Services within Active Directory.....	16
Creating a new site through Active Directory Sites and Services	16
Creating Subnets.....	17
Creating Site Links.....	18
Move the Domain Controllers to Their Newly Created Sites.....	19
Test Replication.....	20
References	24

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.)

<p>Name:</p> <p>LAN1</p> <p>Notes:</p> <p>Vancouver 192.168.1.0/24 Default Gateway: 192.168.1.1</p> <p>Connection type</p> <p>What do you want to connect this virtual switch to?</p> <p><input type="radio"/> External network:</p> <p>Intel(R) Wi-Fi 6 AX201 160MHz</p> <p><input checked="" type="checkbox"/> Allow management operating system to share</p> <p><input type="radio"/> Internal network</p> <p><input checked="" type="radio"/> Private network</p>	<p>Name:</p> <p>LAN2</p> <p>Notes:</p> <p>Toronto 192.168.2.0/24 Default Gateway: 192.168.2.1</p> <p>Connection type</p> <p>What do you want to connect this virtual switch to?</p> <p><input type="radio"/> External network:</p> <p>Intel(R) Wi-Fi 6 AX201 160MHz</p> <p><input checked="" type="checkbox"/> Allow management operating system to share</p> <p><input type="radio"/> Internal network</p> <p><input checked="" type="radio"/> Private network</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Name:</p> <p>WAN</p> <p>Notes:</p> <p>Vancouver: 10.10.10.1/30 Toronto: 10.10.10.2/30 subnet mask: 255.255.255.252</p> <p>Connection type</p> <p>What do you want to connect this virtual switch to?</p> <p><input type="radio"/> External network:</p> <p>Intel(R) Wi-Fi 6 AX201 160MHz</p> <p><input checked="" type="checkbox"/> Allow management operating system to share</p> <p><input type="radio"/> Internal network</p> <p><input checked="" type="radio"/> Private network</p>

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

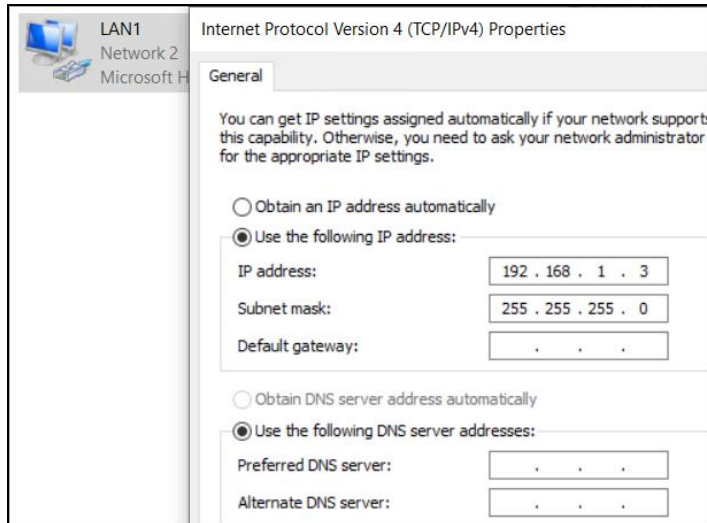
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable 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.



LAN1
Network 2
Microsoft H

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 3

Subnet mask: 255 . 255 . 255 . 0

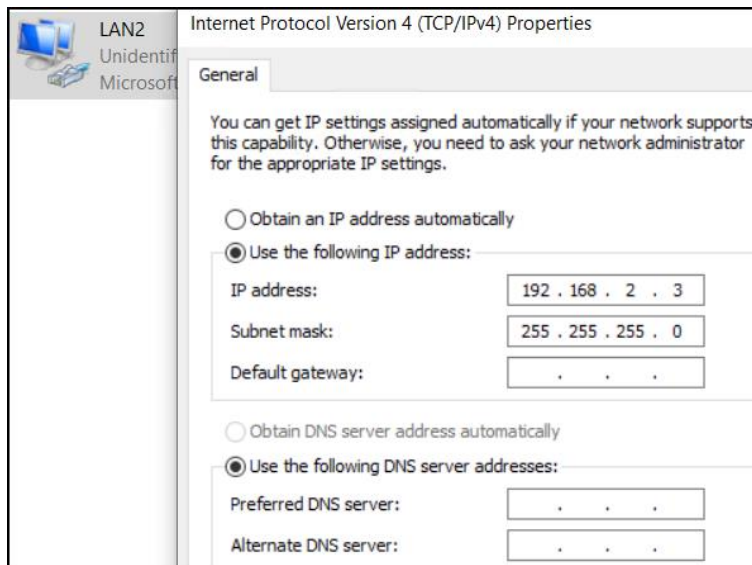
Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .



LAN2
Unidentif
Microsoft

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 2 . 3

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

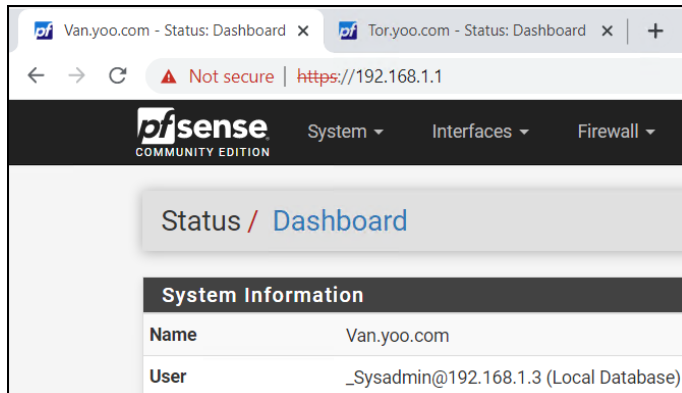
☒ Use the following DNS server addresses:

Preferred DNS server: . . .

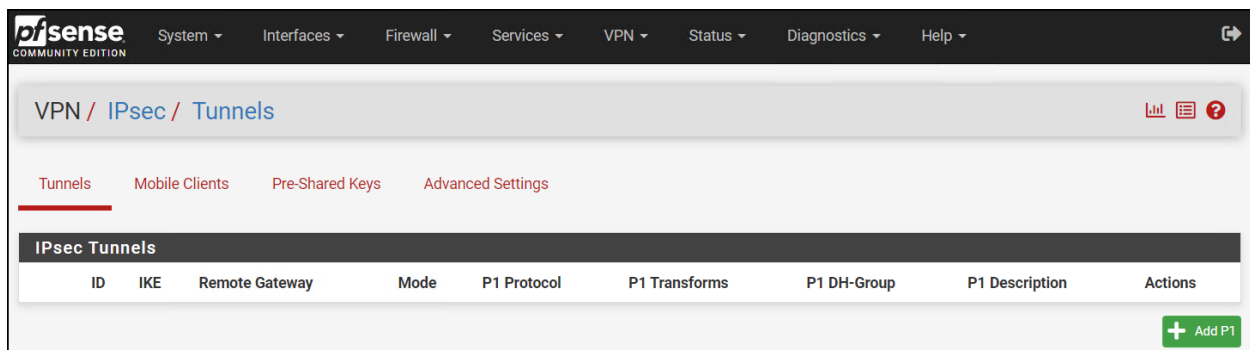
Alternate DNS server: . . .

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.

Tunnels	Mobile Clients	Pre-Shared Keys	Advanced Settings
---------	----------------	-----------------	-------------------

General Information

Description	IPsec to Toronto
A description may be entered here for administrative reference (not parsed).	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version	IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.	
Internet Protocol	IPv4
Select the Internet Protocol family.	
Interface	WAN
Select the interface for the local endpoint of this phase1 entry.	
Remote Gateway	10.10.10.2
Enter the public IP address or host name of the remote gateway.	

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)

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK
Must match the setting chosen on the remote side.	
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	13d168006c87e43c19f99e685cc2373264f31d00378fdab098b9c577
Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.	
Generate new Pre-Shared Key	

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.

Phase 1 Proposal (Encryption Algorithm)				
<u>Encryption Algorithm</u>	<div>AES</div>	<div>256 bits</div>	<div>SHA256</div>	<div>14 (2048 bit)</div>
	Algorithm	Key length	Hash	DH Group
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.				
Add Algorithm	<div>+ Add Algorithm</div>			

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

Expiration and Replacement	
Life Time	<div>28800</div>
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 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**.

Advanced Options	
Child SA Start Action	<div>Default</div> <div>Set this option to force specific initiation/responder behavior for child SA (P2) entries</div>
Child SA Close Action	<div>Restart/Reconnect</div> <div>Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)</div>
NAT Traversal	<div>Auto</div> <div>Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.</div>
MOBIKE	<div>Disable</div> <div>Set this option to control the use of MOBIKE</div>
Gateway duplicates	<input type="checkbox"/> Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	<div>Remote IKE Port</div> <div>Remote NAT-T Port</div> <div>UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).</div> <div>UDP port for NAT-T on the remote gateway.</div>
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	<div>10</div> <div>Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.</div>
Max failures	<div>5</div> <div>Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.</div>

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

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

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 10.10.10.2		AES (256 bits)	SHA256	14 (2048 bit)	IPsec to Toronto	

ID

Mode

Local Subnet

Remote Subnet

P2 Protocol

P2 Transforms

P2 Auth Methods

Description

P2 actions

Add P2

Add P1

Delete P1s

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

General Information

Description

IPsec to Toronto

A description may be entered here for administrative reference (not parsed).

Disabled

☐ Disable this phase 2 entry without removing it from the list.

Mode

Tunnel IPv4

Phase 1

IPsec to Toronto (IKE ID 1)

Networks

Local Network

LAN subnet

Type

Address

Local network component of this IPsec security association.

NAT/BINAT translation

None

Type

Address

If NAT/BINAT is required on this network specify the address to be translated

Remote Network

Network

Type

Address

Remote network component of this IPsec security association.

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.

Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP <small>Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.</small>
Encryption Algorithms	<div><input type="checkbox"/> AES 128 bits</div> <div><input type="checkbox"/> AES128-GCM 128 bits</div> <div><input type="checkbox"/> AES192-GCM Auto</div> <div><input checked="" type="checkbox"/> AES256-GCM 128 bits</div> <div><input type="checkbox"/> Blowfish Auto</div> <div><input type="checkbox"/> 3DES</div> <div><input type="checkbox"/> CAST128</div> <div><small>Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.</small></div>
Hash Algorithms	<div><input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC</div> <div><small>Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.</small></div>
PFS key group	14 (2048 bit) <small>Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</small>

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

Expiration and Replacement	
Life Time	3600 <small>Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.</small>
Rekey Time	3240 <small>Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.</small>
Rand Time	360 <small>A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.</small>

The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.

✓ 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.






Firewall / Rules / IPsec

Floating WAN LAN IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------------------------	--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

 Add  Add  Delete  Save  Separator

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol





Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

Destination

Destination ☐ Invert match /


Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.2.0/24	*	LAN net	*	*	none	allow traffic from the network at Toronto Site	   

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.

Description

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

Remote Gateway	<input type="text" value="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	<input type="text" value="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	<input type="text" value="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	<input type="text" value="None (Responder Only)"/>
Set this option to force specific initiation/responder behavior for child SA (P2) entries	
Child SA Close Action	<input type="text" value="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	<input type="text" value="Network"/>	<input type="text" value="192.168.1.0"/>	<input type="text" value="24"/>
	Type	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.

Expiration and Replacement	
Life Time	<input type="text" value="5400"/>
<small>Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.</small>	

Create a firewall rule for IPsec interface.

Firewall / Rules / Edit	
Edit Firewall Rule	
Action	<div>Pass</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>IPsec</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>Network</div> <div>192.168.1.0 / 24</div>
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>LAN net</div> <div>Destination Address /</div>

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.)

Status / IPsec / Overview

Overview

Leases

SADs

SPDs

IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	IPsec to Toronto	ID: 10.10.10.1 Host: 10.10.10.1	ID: 10.10.10.2 Host: 10.10.10.2				Disconnected <div><div></div>Connect P1 and P2s</div> <div><div></div>Connect P1</div>

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

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

Overview Leases SADs SPDs							
IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #13	IPsec to Toronto	ID: 10.10.10.1 Host: 10.10.10.1:500 SPI: b496d844dcaab917	ID: 10.10.10.2 Host: 10.10.10.2:500 SPI: f989d311910ac55c	IKEV2 Initiator	Rekey: 23169s (06:26:09) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 253 seconds (00:04:13) ago Disconnect P1
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #14	IPsec to Toronto	192.168.1.0/24	Local: c2747d9d Remote: c1142bac	192.168.2.0/24	Rekey: 2762s (00:46:02) Life: 3347s (00:55:47) Install: 253s (00:04:13)	AES_GCM_16 (256) IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0 Installed Disconnect P2

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.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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.

Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

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 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

Root domain name:

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

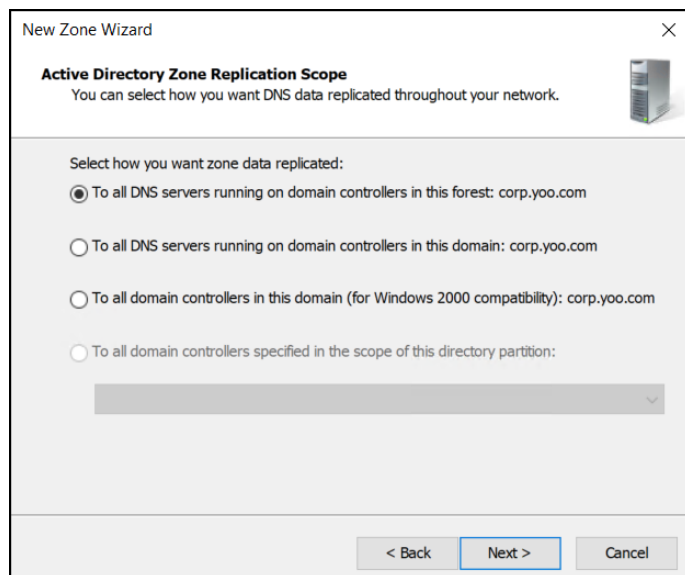
Type the Directory Services Restore Mode (DSRM) password

Password:

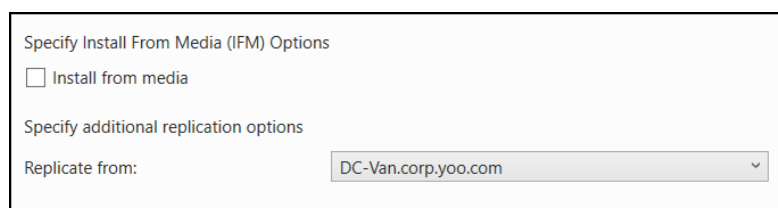
Confirm password:

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

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



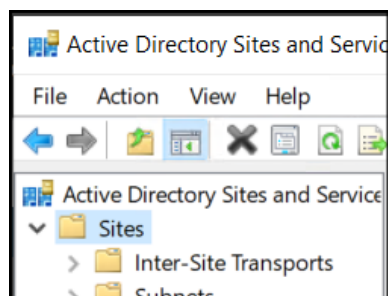
After making **DC-Van** a domain controller, add **DC-Tor** to existing domain. Set preferred DNS server on **DC-Tor** as the IP address of **DC-Van** before starting to install the ADDS role. Choose **Replicate from** the Vancouver domain controller.



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

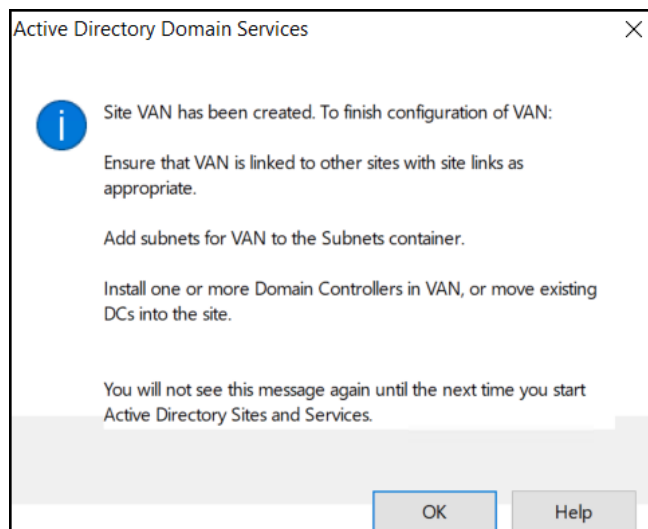
Creating a new site through Active Directory Sites and Services

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



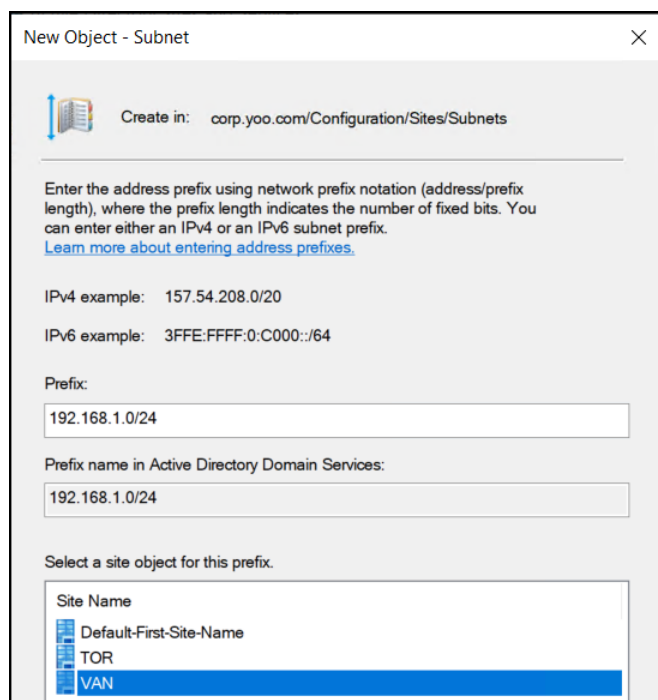
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

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



Creating Subnets

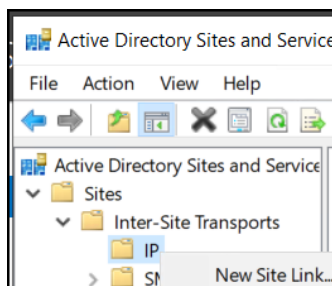
Back to Active Directory Sites and Services MMC, right-click **Subnet** and select **New Subnet**. Read the example to assign **Prefix** of the Vancouver subnet and select Vancouver site you created. Click **OK**. Repeat steps for Toronto. DCs and clients use the subnets you define to determine what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



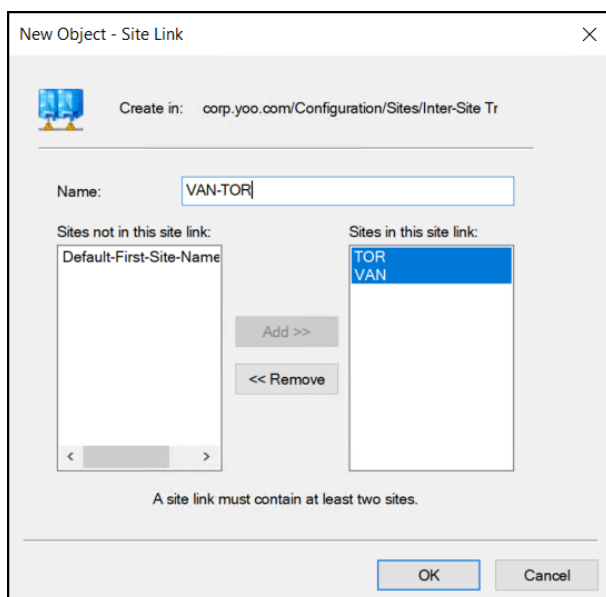
GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

Creating Site Links

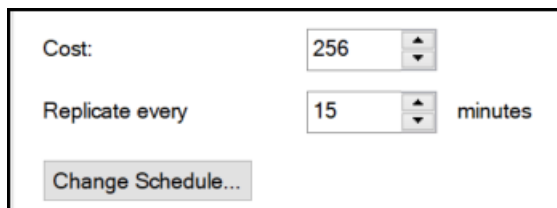
In the Active Directory Sites and Services MMC, click **Inter-Site Transports**, right-click **IP**, and click **New Site Link**.



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>)

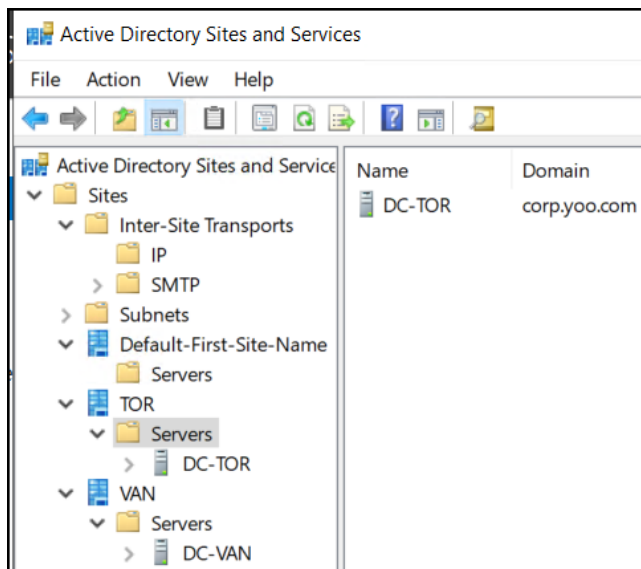


GROUP PROJECT – CREATE A REPLICATING MULTI-SITE DOMAIN USING AN IPSEC VPN TUNNEL

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.

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the Vancouver server. The 'General' tab is selected. The 'Obtain an IP address automatically' radio button is unselected, and the 'Use the following IP address:' radio button is selected. The IP address is 192.168.1.2, the subnet mask is 255.255.255.0, and the default gateway is 192.168.1.1. The 'Obtain DNS server address automatically' radio button is unselected, and the 'Use the following DNS server addresses:' radio button is selected. The preferred DNS server is 192.168.1.2 and the alternate DNS server is 192.168.2.2. The 'Validate settings upon exit' checkbox is unselected. The 'Advanced...' button is visible. The 'OK' and 'Cancel' buttons are at the bottom.

Vancouver

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box for the Toronto server. The 'General' tab is selected. The 'Obtain an IP address automatically' radio button is unselected, and the 'Use the following IP address:' radio button is selected. The IP address is 192.168.2.2, the subnet mask is 255.255.255.0, and the default gateway is 192.168.2.1. The 'Obtain DNS server address automatically' radio button is unselected, and the 'Use the following DNS server addresses:' radio button is selected. The preferred DNS server is 192.168.2.2 and the alternate DNS server is 192.168.1.2. The 'Validate settings upon exit' checkbox is unselected. The 'Advanced...' button is visible. The 'OK' and 'Cancel' buttons are at the bottom.

Toronto

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

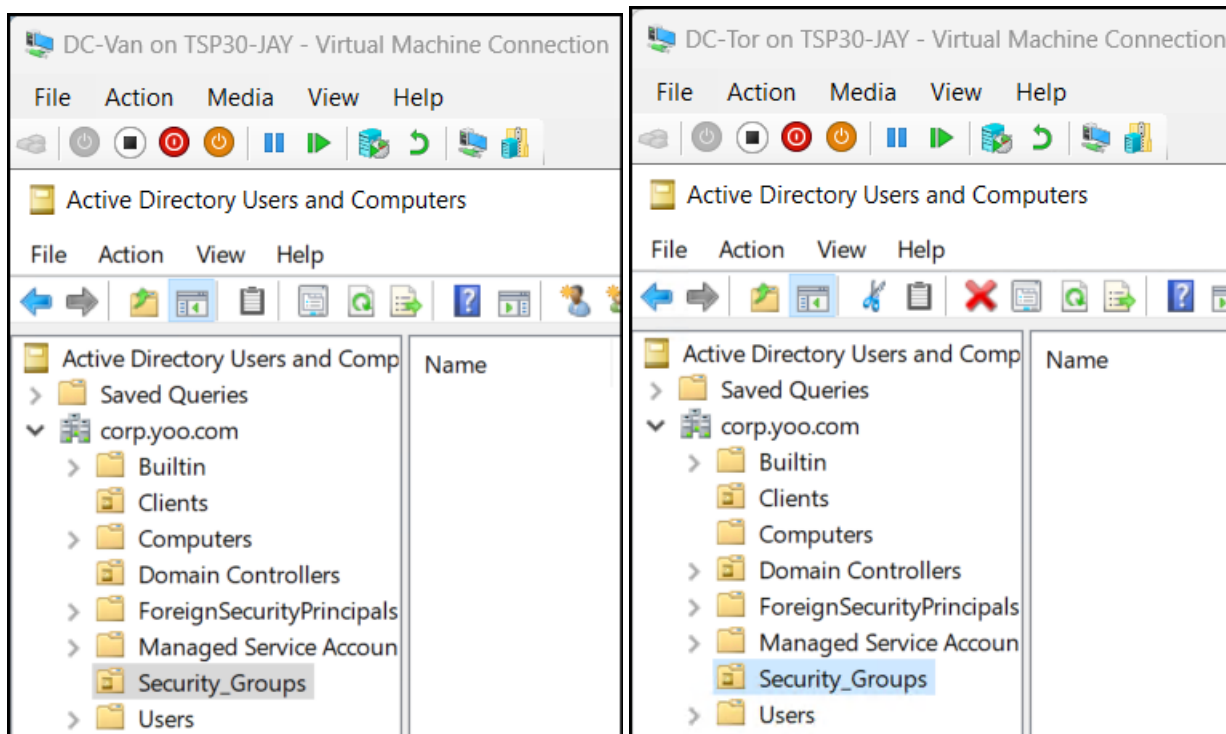
Create an object in the Vancouver DCs ADUC and see if that object is replicated to the Toronto DC. Run this command on Vancouver DC to force-replicate from Vancouver to Toronto.

```
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.

DC-Van on TSP30-JAY - Virtual Machine Connection

File Action Media View Help

DNS Manager

File Action View Help

DNS

- DC-VAN
 - Forward Lookup Zones
 - _msdcs.corp.yoo.com
 - corp.yoo.com
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[75], dc-van.corp.yoo.com,
(same as parent folder)	Name Server (NS)	dc-tor.corp.yoo.com.
(same as parent folder)	Name Server (NS)	dc-van.corp.yoo.com.
(same as parent folder)	Host (A)	192.168.1.2
(same as parent folder)	Host (A)	192.168.2.2
DC-Tor	Host (A)	192.168.2.2
dc-van	Host (A)	192.168.1.2
test	Host (A)	192.168.1.21
test2	Host (A)	192.168.2.21
Tor	Host (A)	192.168.2.1
Van	Host (A)	192.168.1.1

DC-Tor on TSP30-JAY - Virtual Machine Connection

File Action Media View Help

DNS Manager

File Action View Help

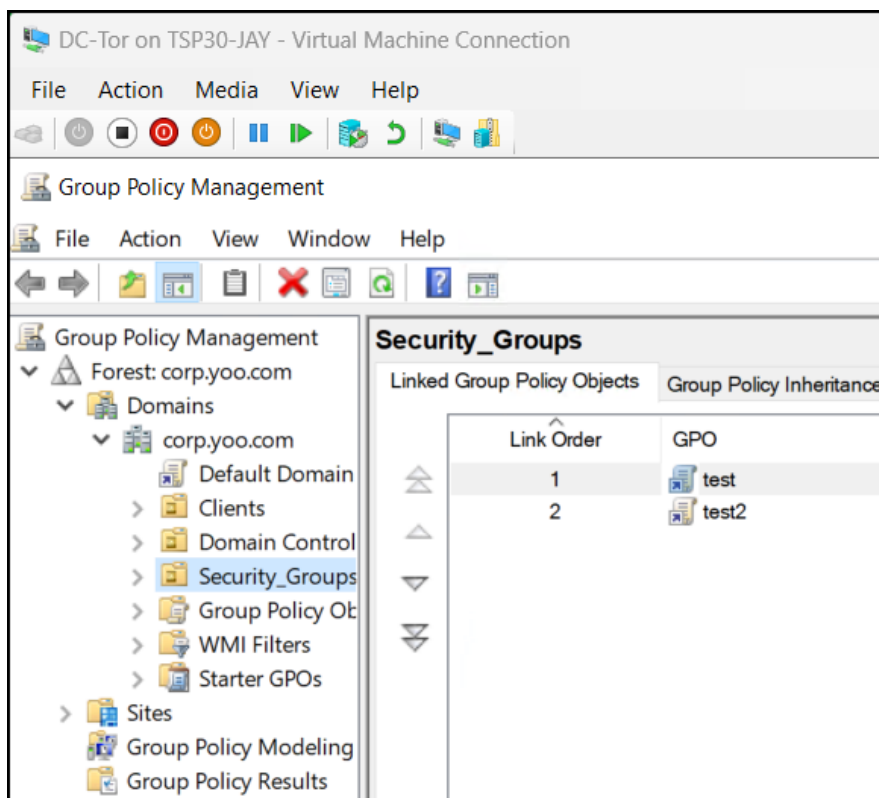
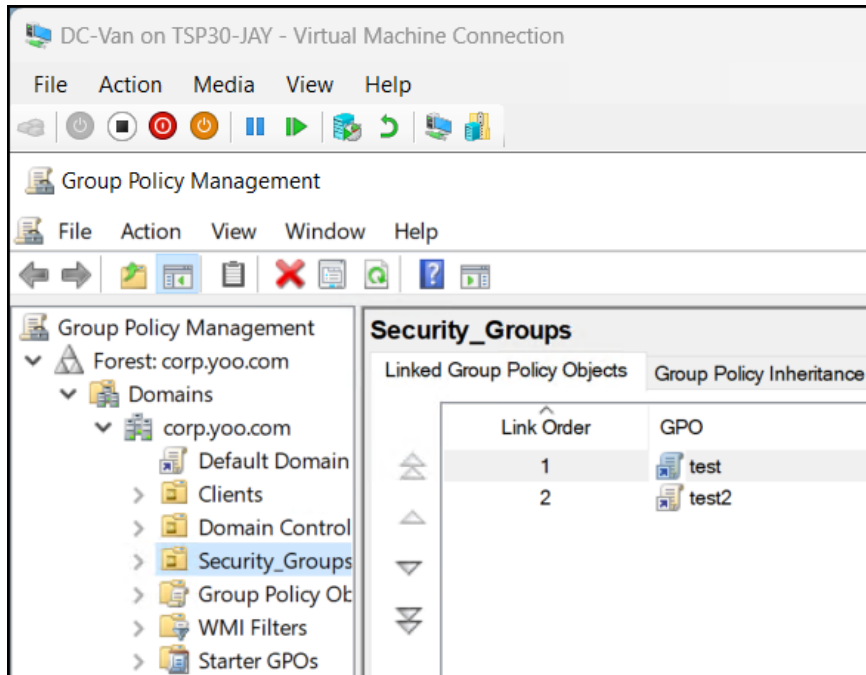
DNS

- DC-TOR
 - Forward Lookup Zones
 - _msdcs.corp.yoo.com
 - corp.yoo.com
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[75], dc-tor.corp.yoo.com, h
(same as parent folder)	Name Server (NS)	dc-van.corp.yoo.com.
(same as parent folder)	Name Server (NS)	dc-tor.corp.yoo.com.
(same as parent folder)	Host (A)	192.168.2.2
(same as parent folder)	Host (A)	192.168.1.2
dc-tor	Host (A)	192.168.2.2
dc-van	Host (A)	192.168.1.2
test	Host (A)	192.168.1.21
test2	Host (A)	192.168.2.21
Tor	Host (A)	192.168.2.1
Van	Host (A)	192.168.1.1

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>