

# Tectorial - Firepower SDWAN

## (Firepower SD-WAN) Tectorial from Zero to Hero

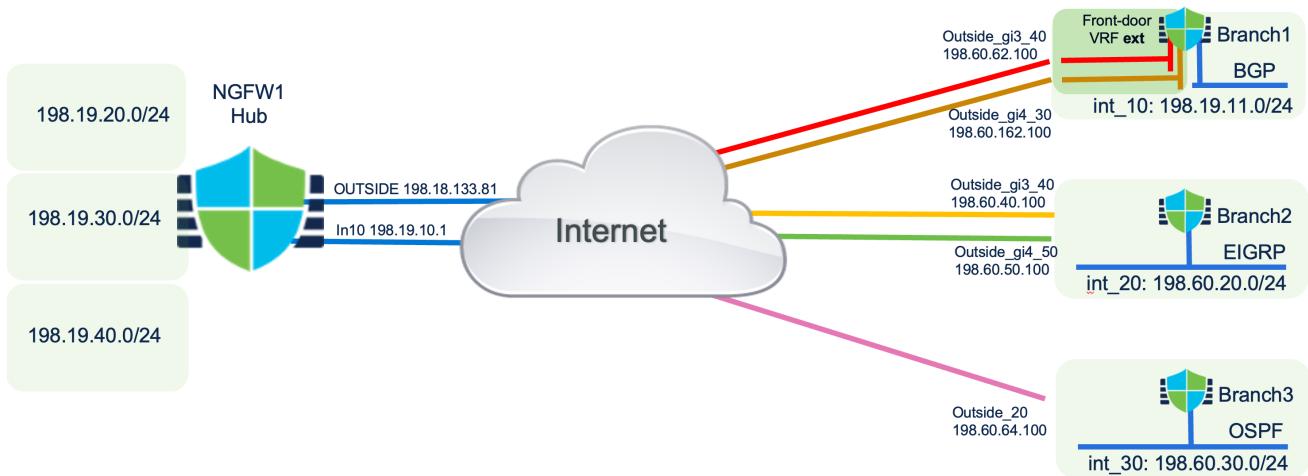
Note	This is not a Firepower training, it expects people to know how to configure the basics including, but not limited to: interfaces, static routing, dynamic routing, rules and NAT
------	---

## Agenda

- Lab Topologies
- Overall configuration
- Interface configuration
- Routing and ECMP configuration
- Direct Internet Access (DIA) configuration
- SDWAN configuration
- SDWAN and WAN status/summary

## Lab Topologies

# Lab Logical Topology

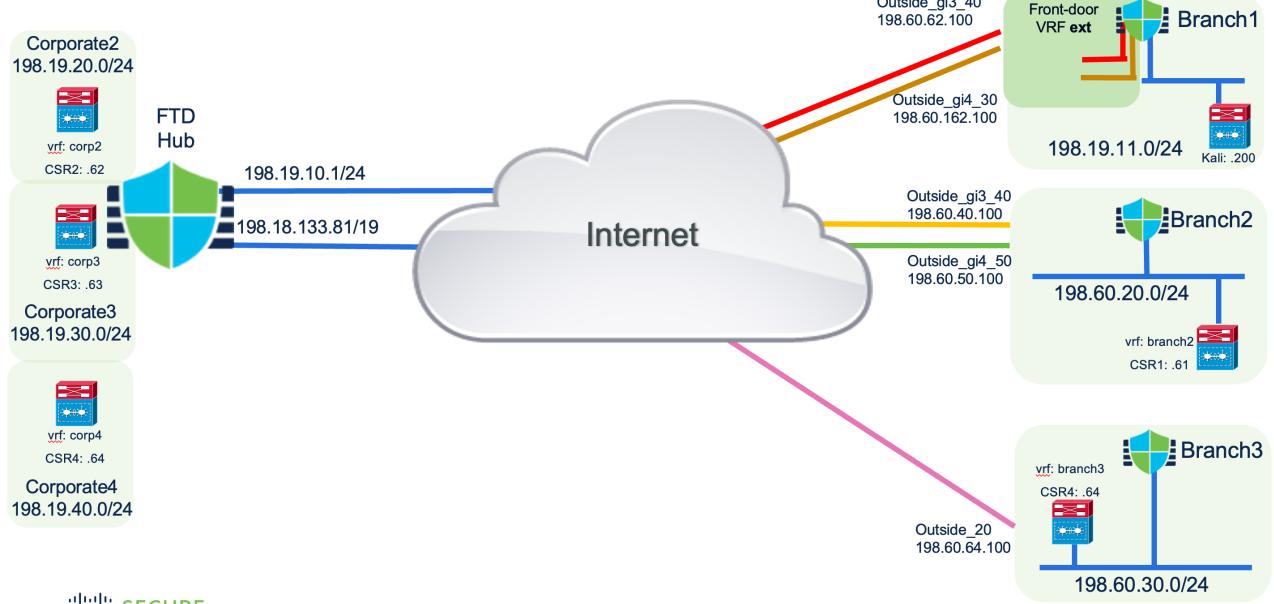


cisco SECURE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

8

## Lab Logical Topology - detailed

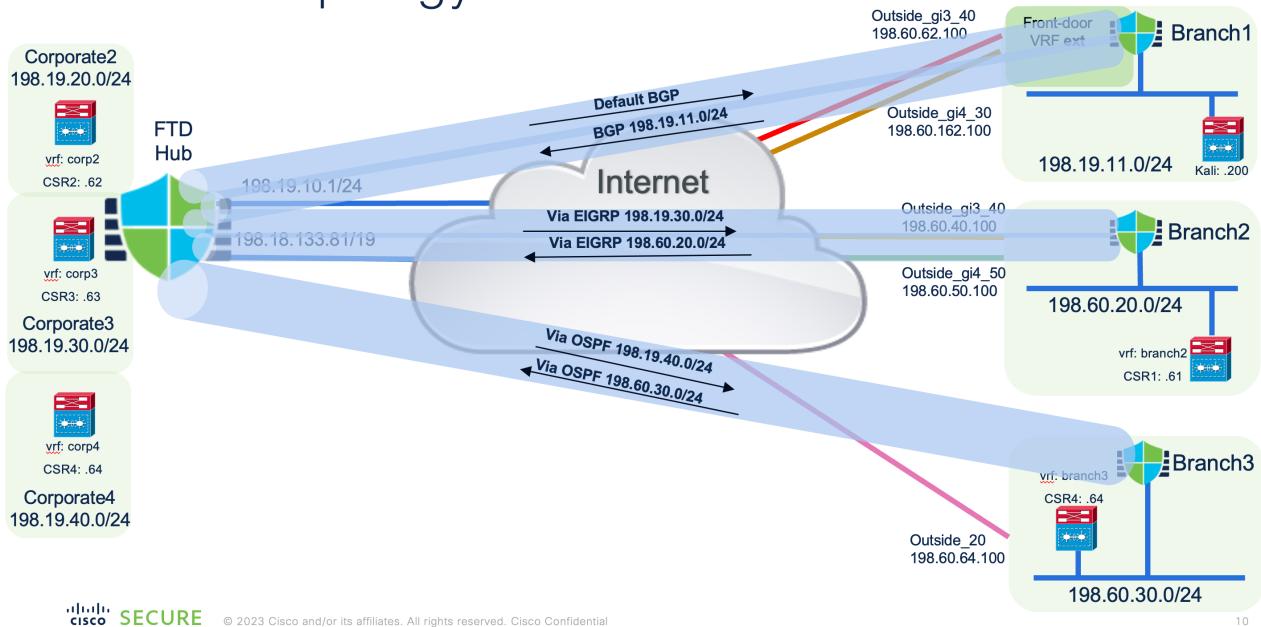


cisco SECURE

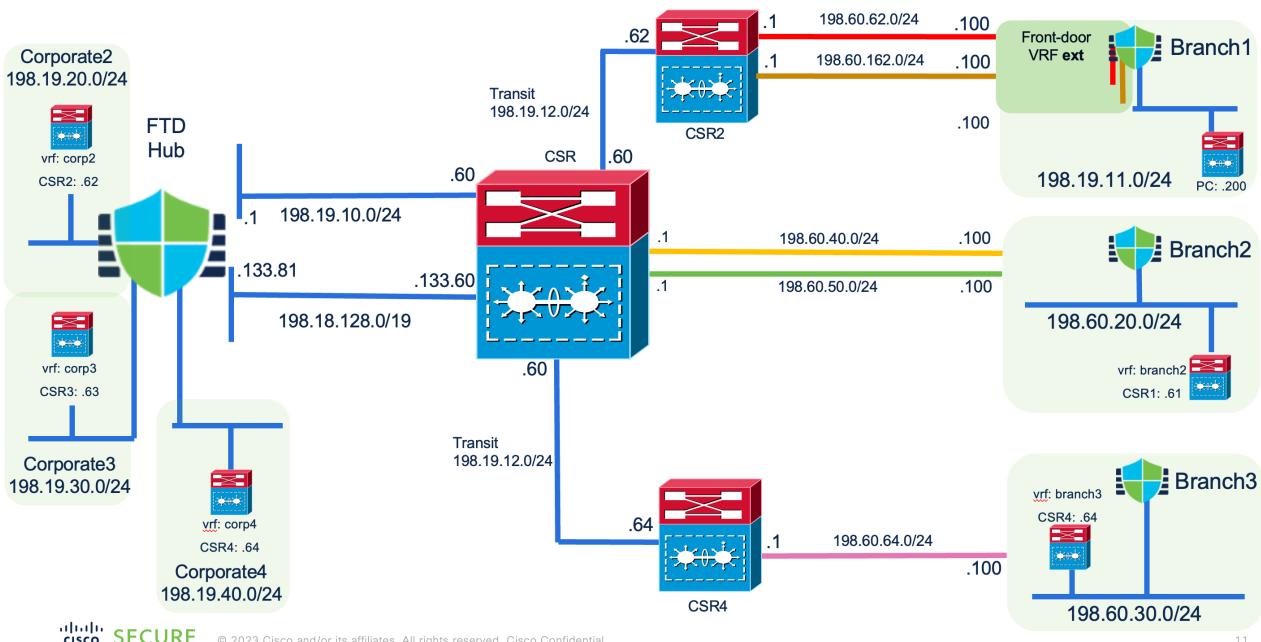
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

9

# SDWAN Topology



# Lab Physical Topology



# Overall configuration

The following screenshots will guide you how to configure the interfaces, static routings and ECMP alongside with the topology drawings.

Firewalls that will be using during this lab

Branch1 Snort 3 198.18.133.42 - Routed	FTDv for VMware	7.4.1	N/A	Essentials, IPS (2 more...)	Branch Access Control	
Branch2 Snort 3 198.19.10.82 - Routed	FTDv for VMware	7.4.1	N/A	Essentials, IPS (2 more...)	Branch2	
Branch3 Snort 3 198.19.10.83 - Routed	FTDv for VMware	7.4.1	N/A	Essentials, IPS (2 more...)	Branch Access Control	
NGFW1 Snort 3 198.19.10.81 - Routed	FTDv for VMware	7.4.1	N/A	Essentials, IPS (4 more...)	NGFW1	

# HUB - NGFW1

## 1. Interfaces

Cisco Firepower Threat Defense for VMWare								
Device	Routing	Interfaces	Inline Sets	DHCP	VTEP		Save	Cancel
All Interfaces		Virtual Tunnels						
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	
GigabitEthernet0/0	outside	Physical	OutZone	198.18.133.81/18(Static)		Disabled	Global	
GigabitEthernet0/1	in10	Physical	InZone1	198.18.10.1/24(Static)		Disabled	Global	
GigabitEthernet0/2	in20	Physical	InZone2	198.18.20.1/24(Static)		Disabled	Global	
GigabitEthernet0/3	in30	Physical	InZone3	172.30.30.1/24(Static)		Disabled	Global	
GigabitEthernet0/4.100	in_dummy_1	Subinterface	InZone4			Disabled	Global	
GigabitEthernet0/3.110	out_dummy_1	Subinterface	out_dummy_5Z			Disabled	Global	
GigabitEthernet0/4	in40	Physical	InZone4	198.18.40.1/24(Static)		Disabled	Global	
GigabitEthernet0/4.200	in_dummy_2	Subinterface	InZone5			Disabled	Global	
GigabitEthernet0/4.220	out_dummy_2	Subinterface	out_dummy_5Z			Disabled	Global	

## 2. Static Route - HUB has a default route to internet and static routes to PE router to reach branches external IPs

IPv4 Routes						
branch1_net30,branch1_net40,branch2_net30,branch2_net40,branch3_net40	in10	Global	198.19.10.60	false	1	
branch3_net40,branch1_net40,branch2_net30,branch2_net40,branch1_net30	outside	Global	198.18.133.60	false	1	
InsideLoop	in10	Global	198.19.10.200	false	1	
any-ipv4	outside	Global	198.18.128.1	false	1	

## 3. ECMP to reach spokes, since HUB has 2 links Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP_VPN	outside, in10

# Branch1

## 1. Interfaces

Cisco Firepower Threat Defense for VMWare								
Device	Routing	Interfaces	Inline Sets	DHCP	VTEP		Save	Cancel
All Interfaces		Virtual Tunnels						
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1	inside	Physical	InZone	198.19.11.4/255.255.255.0(Static)		Disabled	Global	
GigabitEthernet0/2		Physical				Disabled		
GigabitEthernet0/3	outside_gi3_40	Physical	OutZone	198.60.62.100/24(Static)		Disabled	ext	
GigabitEthernet0/4	outside_gi4_30	Physical	OutZone	198.60.162.100/24(Static)		Disabled	ext	

## 2. Static route (vrf ext)

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
IPv4 Routes					
any-ipv4	outside_gi4_30		198.60.162.1	false	1
any-ipv4	outside_gi3_40		198.60.62.1	false	1

### 3. ECMP (vrf ext)

#### Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ext_vrf	outside_gi3_40, outside_gi4_30

## Branch2

### 1. Interfaces

branch2						
Cisco Firepower Threat Defense for VMware						
Device	Routing	Interfaces	Inline Sets	DHCP	VTEP	
<a href="#">All Interfaces</a> <a href="#">Virtual Tunnels</a>						
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	
Management0/0	management	Physical				
GigabitEthernet0/0		Physical				
GigabitEthernet0/1		Physical				
GigabitEthernet0/2	in20	Physical	InZone1		198.60.20.100/24(Static)	
GigabitEthernet0/3	outside_gi3_40	Physical	OutZone		198.60.40.100/24(Static)	
GigabitEthernet0/4	outside_gi4_50	Physical	OutZone		198.60.50.100/24(Static)	

### 2. Static route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
any-ipv4	outside_gi4_50	Global	198.60.50.1	false	1
any-ipv4	outside_gi3_40	Global	198.60.40.1	false	1

### 3. ECMP

#### Equal-Cost Multipath Routing (ECMP)

Name	Interfaces
ECMP-ext	outside_gi3_40, outside_gi4_50

## Branch3

### 1. Interfaces

branch3						
Cisco Firepower Threat Defense for VMware						
Device	Routing	Interfaces	Inline Sets	DHCP	VTEP	
<a href="#">All Interfaces</a> <a href="#">Virtual Tunnels</a>						
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	
Management0/0	management	Physical				
GigabitEthernet0/0		Physical				
GigabitEthernet0/1		Physical				
GigabitEthernet0/2	outside_20	Physical	OutZone		198.60.64.100/24(Static)	
GigabitEthernet0/3	int_30	Physical	InZone1		198.60.30.1/24(Static)	
GigabitEthernet0/4		Physical				

## 2. Static route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
any-ipv4	outside_20	Global	198.60.64.1	false	1

3. ECMP - N/A because Branch3 has only 1 WAN interface

## Interface configuration

### Hub (NGFW1) - Configuring two DVTI interfaces to use with two WAN links

**Note:** HUB will contain two loopback interfaces, one per topology. SDWAN topology is, in simple words, created per WAN links at the HUB. It can also be created for other reasons

Hub will have two loopbacks because it has 2 links. They will be addressed as CIDR /29 to accommodate 1 hub and 3 spokes inside the same network. Their addresses will be:

- Loop10: 169.254.100.0/29 where the HUB is the first valid IP inside the block
- Loop11: 169.254.100.8/29 where the HUB is the first valid IP inside the block

## Connecting to the lab

1. Open **jumpbox** by clicking on WEB\_RDP link inside the section **How to Connect to the Lab Environment**



2. You will be presented with the **Quick Launch** page as soon as you are logged in. In case you are not presented with this page or you accidentally

close during your lab, go to **Desktop** and double-click on this icon



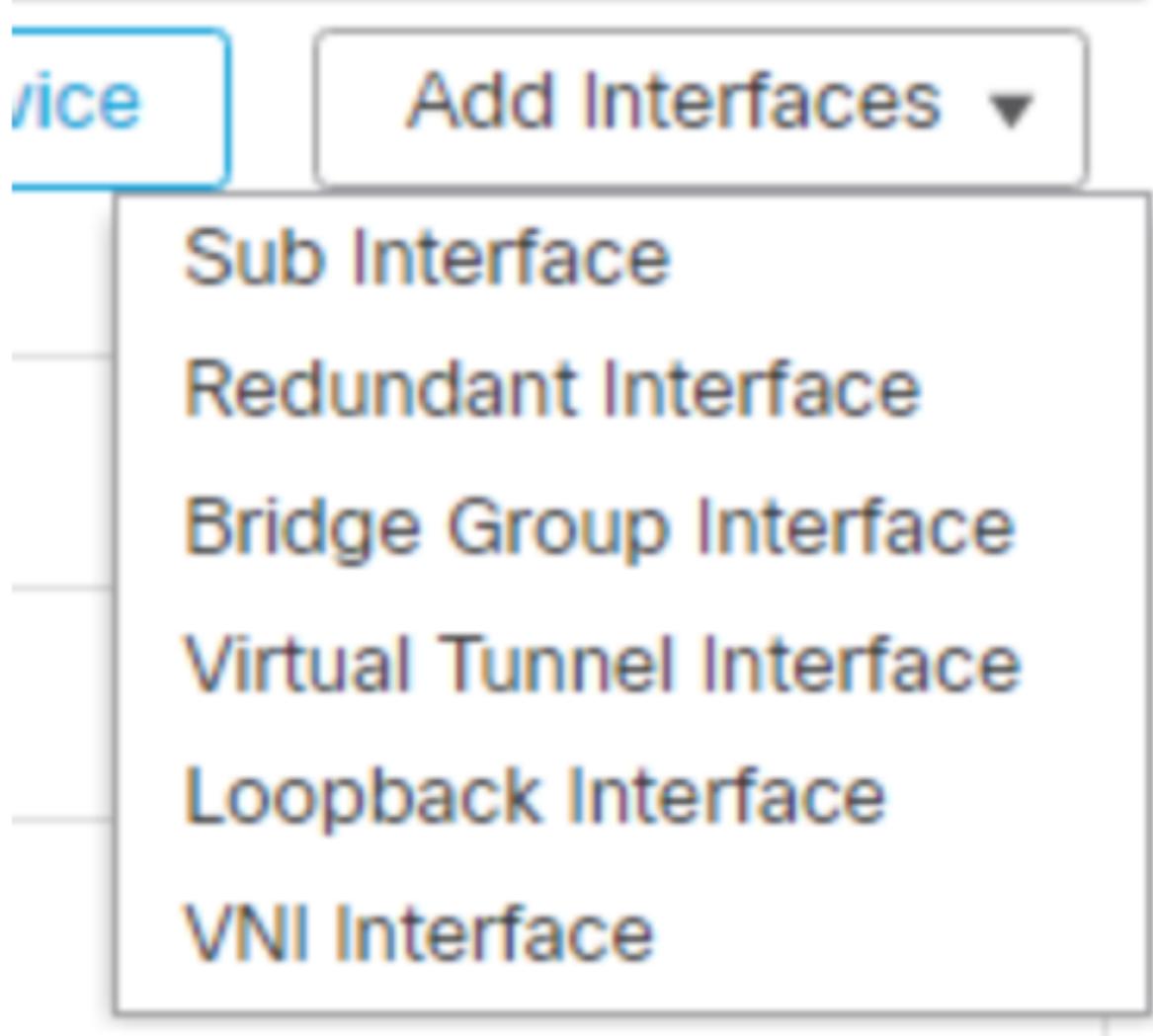
3. You will be presented with the following page that contains most of the access you will need to complete this lab



## VPN1 - Interface outside - using Loop10 169.254.100.0/29.

1. Go to **Devices > Device Management**. Find **NGFW1** and click on the pencil to **edit** it

2. Inside Interfaces tab, click on Add Interfaces > Loopback Interface



3. Fill out name and Loopback ID as per image under **General** tab.

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop10

Enabled

Loopback ID:\*

10

(1-1024)

Description

4. Go to **IPv4** tab and fill out IP Address. Click **Ok** to finish.

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

169.254.100.1/29

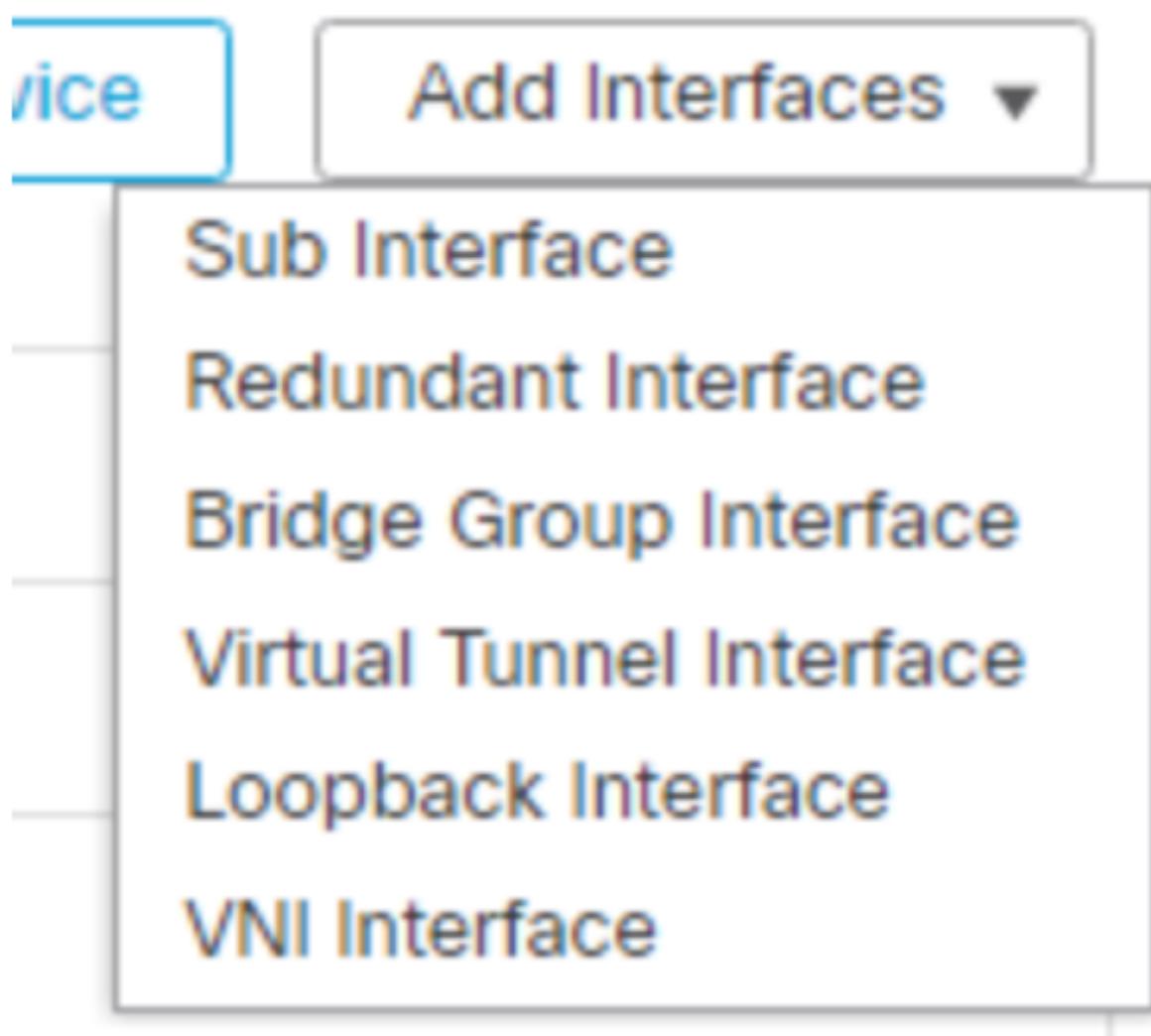
e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

5. Create a **Dynamic** Virtual Tunnel Interface (DVTI) using Loop10 IP address we just created.

- Create a separate Security Zone for Static/Dynamic VTIs. We will be using Zone **VTI** here. If you don't have it, you need to create under this page
- Tunnel source was left unchecked because it will be chosen when creating the SDWAN topology, so no need to do this here
- Use meaningful names so you know which physical and which loopback you are using on your DVTIs or SVTIs

6. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**

---



7. There are some fields to fill out:

1. Tunnel Type: **Dynamic**. This is the default when configuring the HUB. Branches will be of Static type
2. Name: **DVTI\_outside\_Loop10**
3. Security Zone: **VTI**.
4. Template ID: select a number to represent this DVTI. We will use **10** to match our loopback number

5. Tunnel Source: leave it blank, we will select the source while creating the topology
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop10** we created before

## Add Virtual Tunnel Interface

General      Path Monitoring

Tunnel Type

Static       Dynamic

Name:\*

DVTI\_outside\_Loop10

Enabled

Note: If you do not have VTI Security Zone, you can create it from here

Security Zone:

None

InZone

InZone1

InZone2

InZone3

InZone4

OutZone

VTI

in\_dummy\_SZ

out\_dummy\_SZ

New...

Note: If you do not have VTI Security Zone, you can create it from here

## New Security Zone

Enter a name...

Security Zone:



Priority:

---

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tu

Template ID:\*

Tunnel Source:

Select Interface	▼	Empty	▼
------------------	---	-------	---

---

*IPsec Tunnel Details*

*IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.*

IPsec Tunnel Mode:\*

- IPv4     IPv6

IP Address:\*

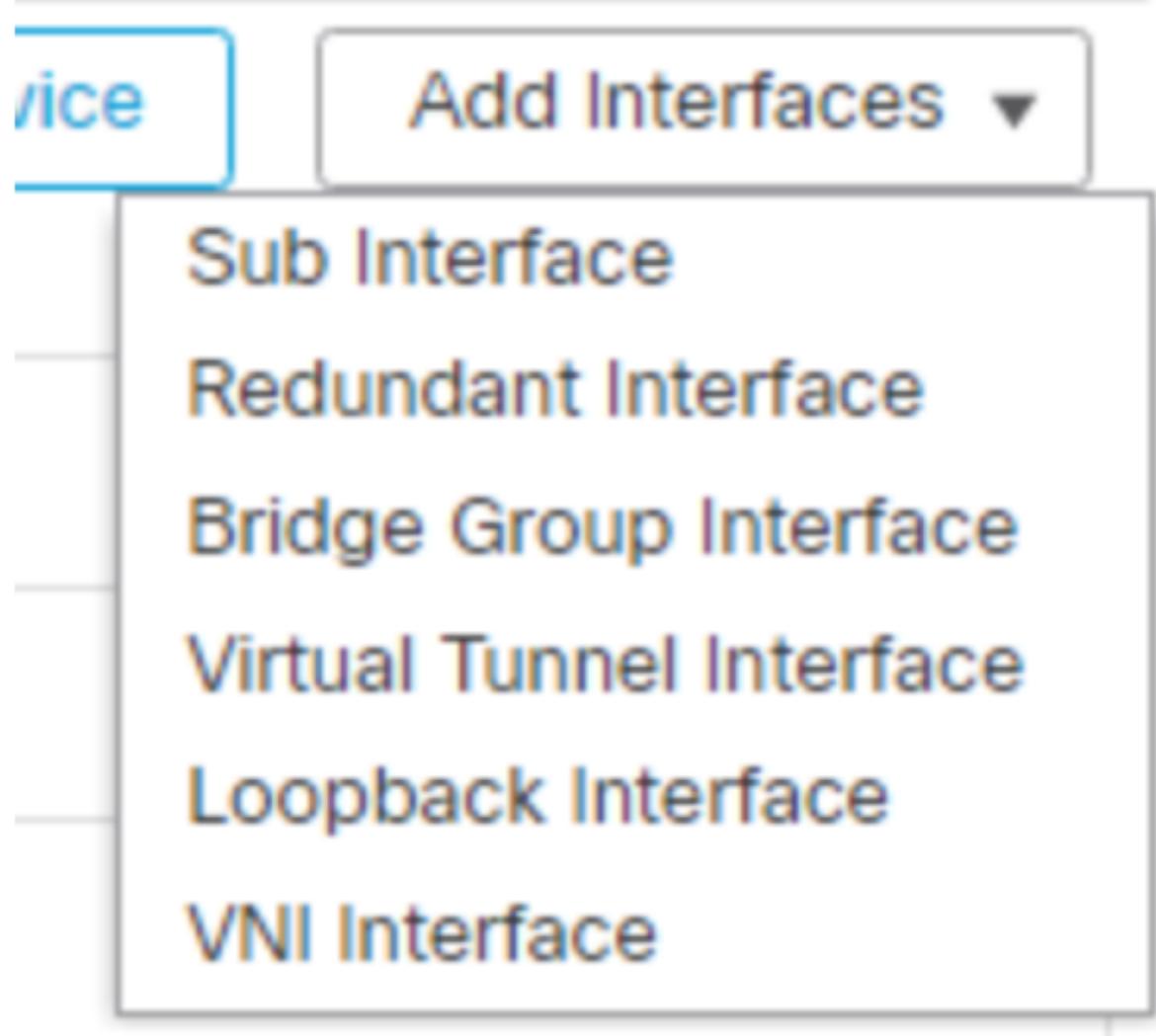
<input type="radio"/> Configure IP	<Valid IPv4 address>/<Mask>	i
<input checked="" type="radio"/> Borrow IP (IP unnumbered)	Loopback10 (Loop10)	▼ +

8. Click **Ok** to create the DVTI interface

## VPN2 - Interface in10 - using Loop11 169.254.100.8/29.

1. Go to **Devices > Device Management**. Find **NGFW1** and click on the pencil to **edit** it

2. Inside Interfaces tab, click on Add Interfaces > Loopback Interface



3. Fill out name and Loopback ID as per image under **General** tab.

## Add Loopback Interface

**General**

IPv4

IPv6

Name:

Loop11

Enabled

Loopback ID:\*

11

(1-1024)

Description

4. Go to **IPv4** tab and fill out IP Address. Click **Ok** to finish.

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

169.254.100.9/29

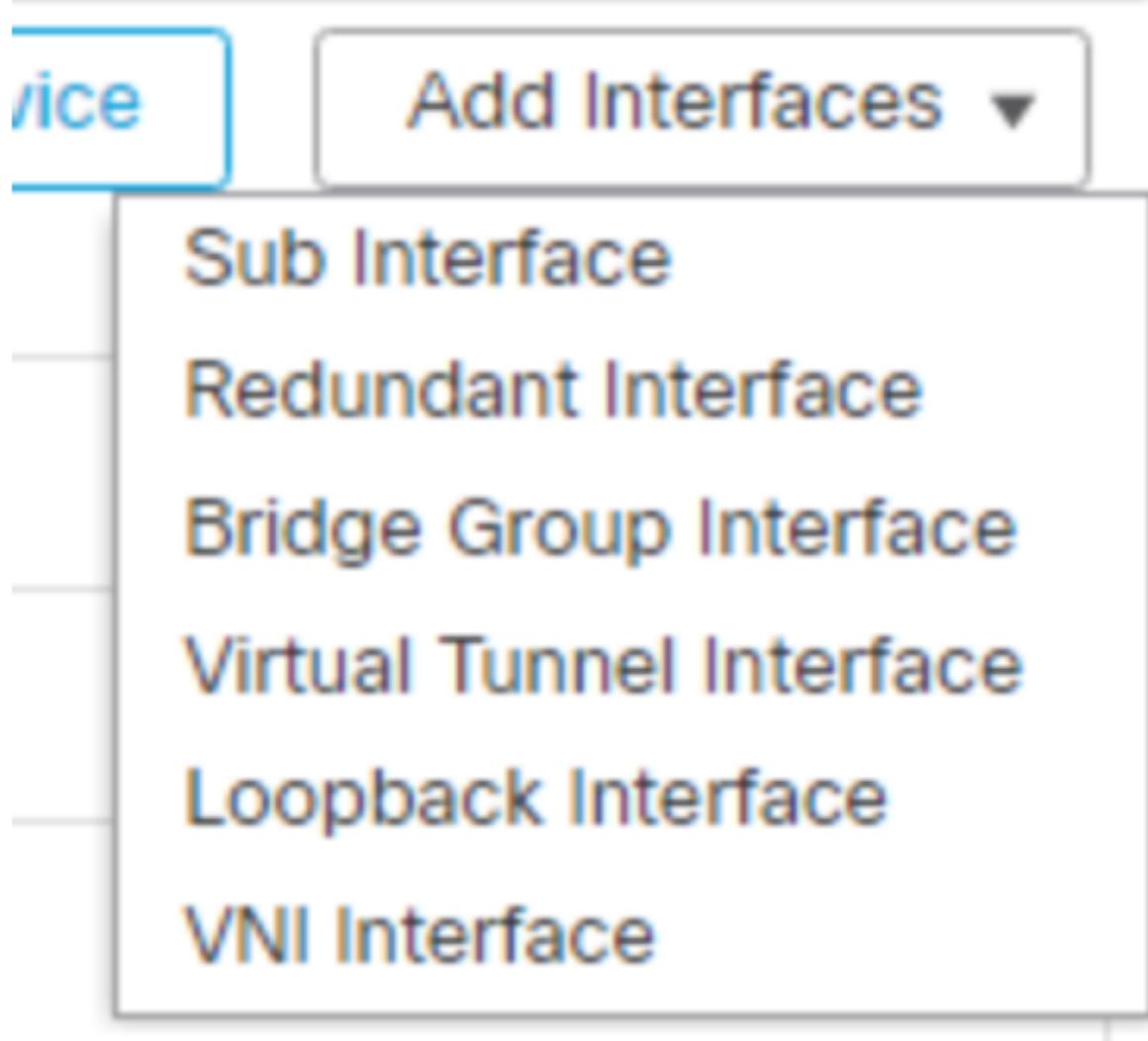
e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

5. Create a **Dynamic** Virtual Tunnel Interface (DVTI) using Loop11 IP address we just created.

- Since we have already created the **VTI** Security Zone before, then we will be using it.
- Tunnel source was left unchecked because it will be chosen when creating the SDWAN topology, so no need to do this here
- Use meaningful names so you know which physical and which loopback you are using on your DVTIs or SVTIs

6. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**

---



7. There are some fields to fill out:

1. Tunnel Type: **Dynamic**. This is the default when configuring the HUB.  
Branches will be of Static type
2. Name: **DVTI\_in10\_Loop11**
3. Security Zone: **VTI**.
4. Template ID: select a number to represent this DVTI. We will use **11** to match our loopback number
5. Tunnel Source: leave it blank, we will select the source while creating the topology
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop11** we created before

## Add Virtual Tunnel Interface

General

Path Monitoring

### Tunnel Type

Static       Dynamic

Name:\*

DVTI\_in10\_Loop11

Enabled

Security Zone:

VTI



Priority:

0

---

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tu

Template ID:\*

11

Tunnel Source:

Select Interface	▼	Empty	▼
------------------	---	-------	---

#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

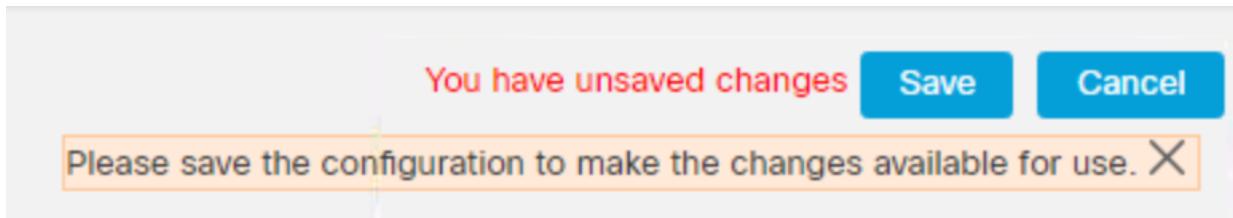
IPv4     IPv6

IP Address:\*

<input type="radio"/> Configure IP	<Valid IPv4 address>/<Mask>	
<input checked="" type="radio"/> Borrow IP (IP unnumbered)	Loopback11 (Loop11)	▼
		+

8. Click **Ok** to create the DVTI interface

9. Click **Save**



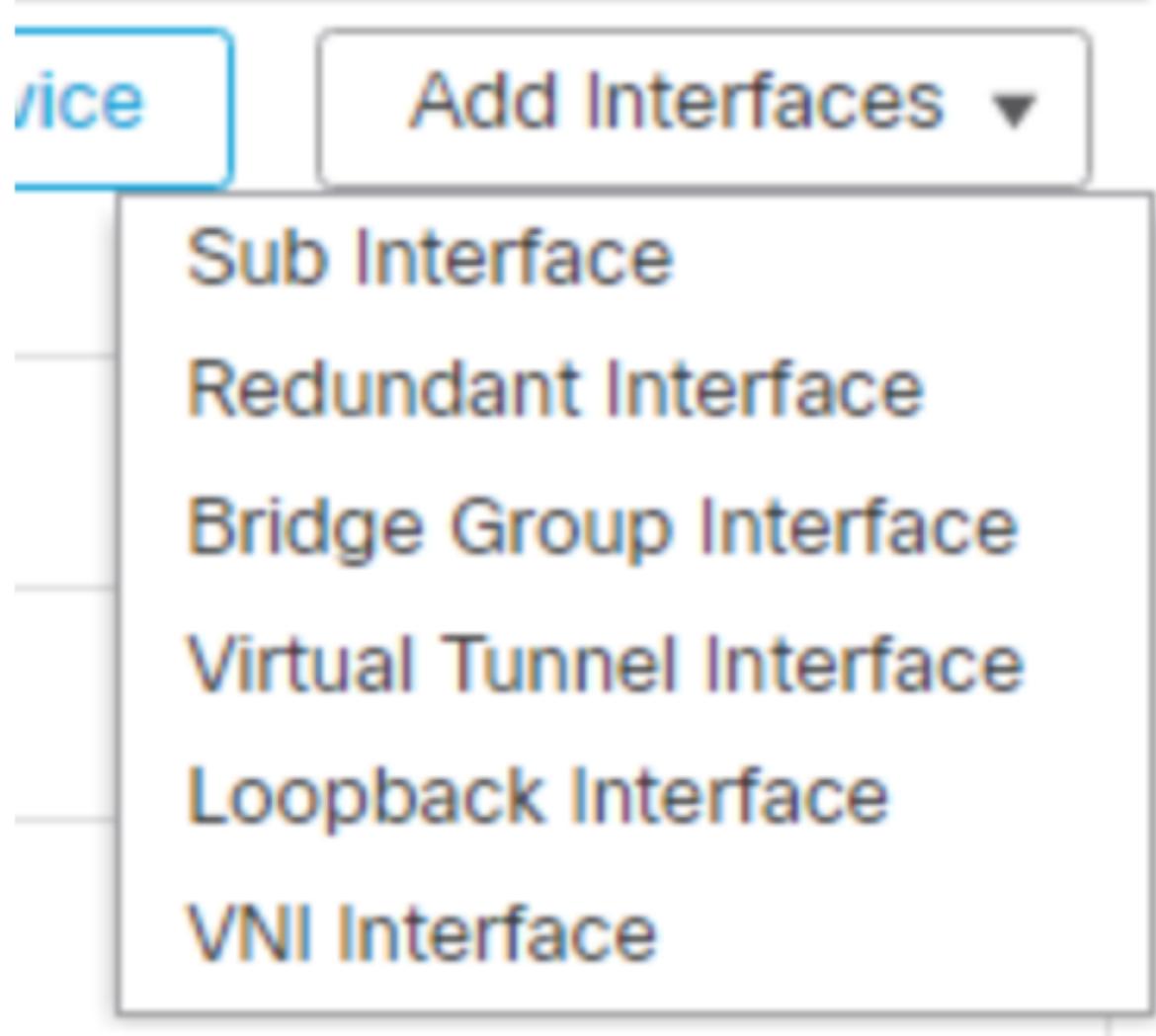
Interfaces overview:

Virtual-Template10	DVTI_outside_Loop10	VTI	VTI
Virtual-Template11	DVTI_in10_Loop11	VTI	VTI
Loopback10	Loop10	Loopback	169.254.100.1/29(Static)
Loopback11	Loop11	Loopback	169.254.100.9/29(Static)

## Branch3 - Configuring two SVTI interfaces to connect with the two HUB links

1. Go to **Devices > Device Management**. Find **Branch3** and click on the pencil to **edit** it

2. Inside Interfaces tab, click on Add Interfaces > Loopback Interface



3. Fill out name and Loopback ID as per image under **General** tab.

## Add Loopback Interface

**General**

IPv4

IPv6

Name:

Loop10

Enabled

Loopback ID:\*

10

(1-1024)

4. Go to **IPv4** tab and fill out IP Address. Click **Ok** to finish.

## Add Loopback Interface

General

**IPv4**

IPv6

IP Type:

Use Static IP

IP Address:

169.254.100.3/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

5. Create the second Loopback interface, use the same steps as before

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop11

Enabled

Loopback ID:\*

11

(1-1024)

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

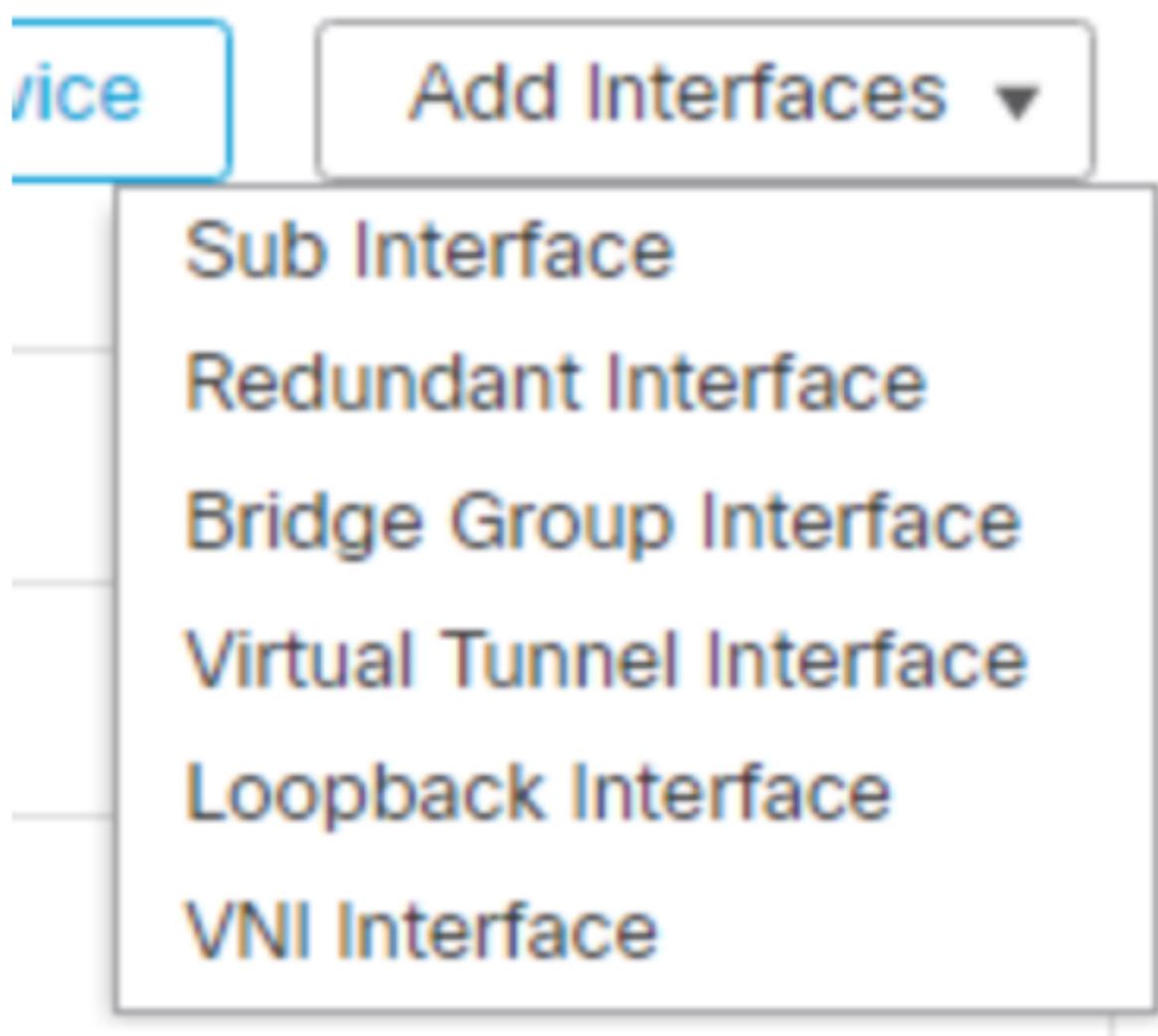
169.254.100.11/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

6. Create a **Static** Virtual Tunnel Interface (SVTI) using Loop10 IP address we just created.

- Since we have already created the **VTI** Security Zone before, then we don't need to create again.
- Use meaningful names so you know which physical and which loopback you are using on your DVTIs or SVTIs

7. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**



8. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside20\_Loop10**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **10** to match our loopback number
5. Tunnel Source: select the outside interface as it will be the only one reach out to HUB. Branch3 has only one WAN interface, which is **outside\_20**
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop10** we created before

## Add Virtual Tunnel Interface

General

Path Monitoring

### Tunnel Type

Static       Dynamic

Name:\*

SVTI\_outside20\_Loop10

Enabled

Description:

Security Zone:

VTI



Tunnel ID:\*

(0 - 10413)

Tunnel Source:\*

---

#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4     IPv6

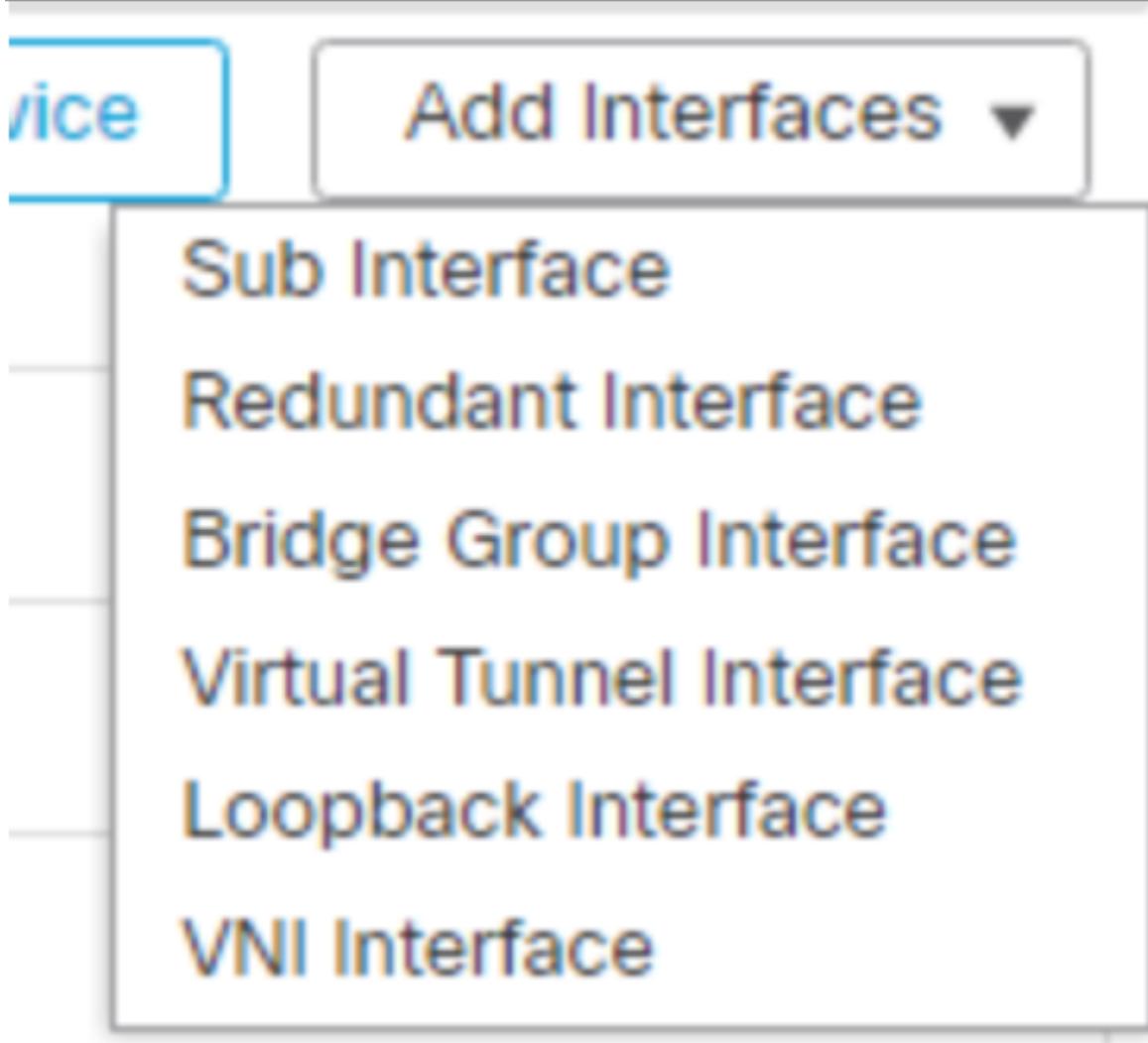
IP Address:\*

Configure IP <Valid IPv4 address>/<Mask> i

Borrow IP (IP unnumbered) Loopback10 (Loop10) ▾ +

9. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**

---



10. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside20\_Loop11**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **11** to match our loopback number
5. Tunnel Source: select the outside interface as it will be the only one reach out to HUB. Branch3 has only one WAN interface, which is **outside\_20**
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop11** we created before

## Add Virtual Tunnel Interface

**General**      **Path Monitoring**

---

**Tunnel Type**

**Static**     **Dynamic**

**Name:**\*

**SVTI\_outside20\_Loop11**

**Enabled**

**Description:**

**Security Zone:**

**VTI** ▾

Tunnel ID:\*

(0 - 10413)

Tunnel Source:\*

 ▾

#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4     IPv6

IP Address:\*

Configure IP

<Valid IPv4 address>/<Mask>



Borrow IP (IP unnumbered)

Loopback11 (Loop11) ▾



11. Click **Ok** and then Save the configuration

You have unsaved changes

**Save**

**Cancel**

Please save the configuration to make the changes available for use.

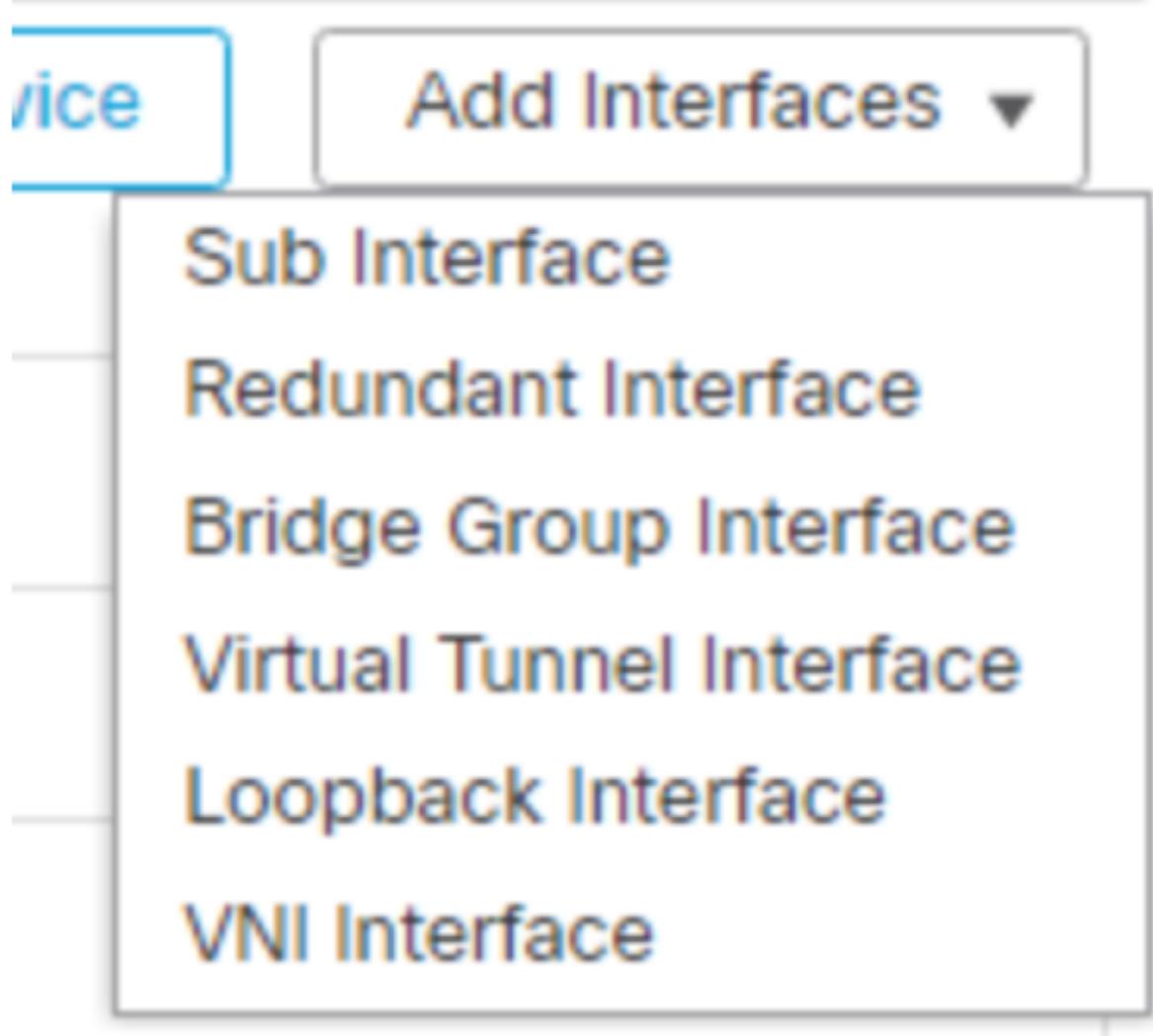
Interfaces overview:

GigabitEthernet0/2	outside_20	Physical	OutZone	198.60.64.100/24(Static)
Tunnel10	SVTI_outside20_Loop10	VTI	VTI	
Tunnel11	SVTI_outside20_Loop11	VTI	VTI	
GigabitEthernet0/3	int_30	Physical	InZone1	198.60.30.1/24(Static)
GigabitEthernet0/4		Physical		
Loopback10	Loop10	Loopback		169.254.100.3/29(Static)
Loopback11	Loop11	Loopback		169.254.100.11/29(Static)

## Branch2 - Configuring two SVTI interfaces to connect with the two HUB links

1. Go to **Devices > Device Management**. Find **Branch2** and click on the pencil to **edit** it

2. Inside Interfaces tab, click on Add Interfaces > Loopback Interface



3. Fill out name and Loopback ID as per image under **General** tab.

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop10

Enabled

Loopback ID:\*

10

(1-1024)

4. Go to **IPv4** tab and fill out IP Address. Click **Ok** to finish.

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

169.254.100.2/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

5. Create the second Loopback interface, use the same steps as before

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop11

Enabled

Loopback ID:\*

11

(1-1024)

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

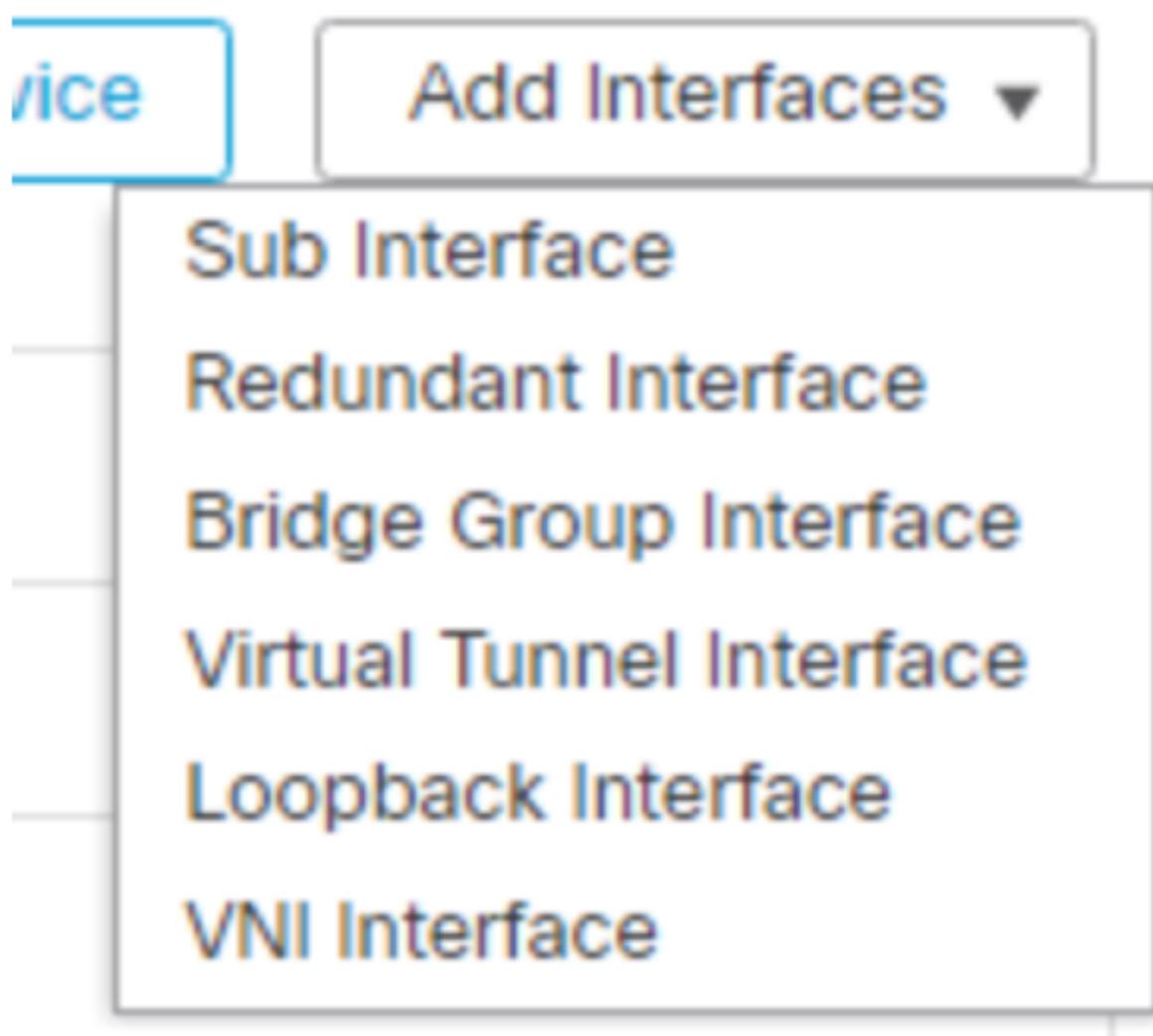
169.254.100.10/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

6. Create a **Static** Virtual Tunnel Interface (SVTI) using Loop10 IP address we just created.

- Since we have already created the **VTI** Security Zone before, then we will be using it.
- Use meaningful names so you know which physical and which loopback you are using on your DVTIs or SVTIs

7. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**



8. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside\_gi3\_40\_Loop10**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **10** to match our loopback number
5. Tunnel Source: select Gi0/3 (**outside\_gi3\_40**) as it will be the first interface we will be using to reach out to HUB. Branch2 has two WAN interfaces, we will create one SVTI per WAN interface in this lab.
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop10** we created before

## Add Virtual Tunnel Interface

General

Path Monitoring

### Tunnel Type

Static       Dynamic

Name:\*

SVTI\_outside\_gi3\_40\_Loop10

Enabled

Description:

Security Zone:

VTI

Tunnel ID:\*

(0 - 10413)

Tunnel Source:\*

▼

#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

- IPv4     IPv6

IP Address:\*

- Configure IP

<Valid IPv4 address>/<Mask>

?

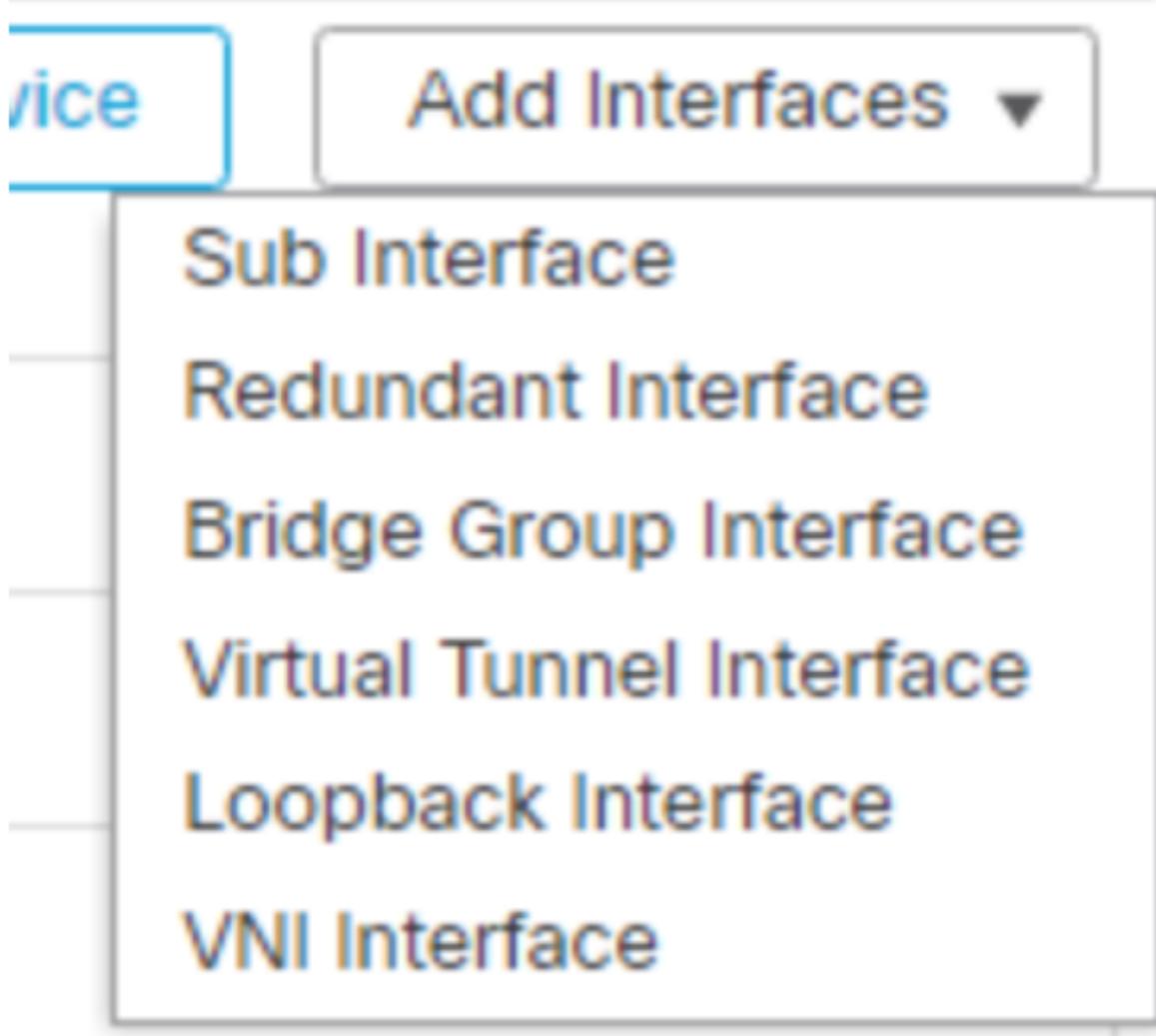
- Borrow IP (IP unnumbered)

Loopback10 (Loop10)

▼

+

9. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**



10. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside\_gi4\_50\_Loop11**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **11** to match our loopback number
5. Tunnel Source: select Gi0/4 (**outside\_gi4\_50**) as it will be the second interface we will be using to reach out to HUB. Branch2 has two WAN interfaces, we will create one SVTI per WAN interface in this lab.
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop11** we created before

## Add Virtual Tunnel Interface

**General**      **Path Monitoring**

---

**Tunnel Type**

Static       Dynamic

**Name:**\*

SVTI\_outside\_gi4\_50\_Loop11

Enabled

**Description:**

**Security Zone:**

VTI ▾

Tunnel ID:\*

11

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/4 (outside\_gi4\_5)

198.60.50.100



#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4     IPv6

IP Address:\*

Configure IP

<Valid IPv4 address>/<Mask>



Borrow IP (IP unnumbered)

Loopback11 (Loop11)



11. Click **Ok** and then Save the configuration

You have unsaved changes

Save

Cancel

Please save the configuration to make the changes available for use.

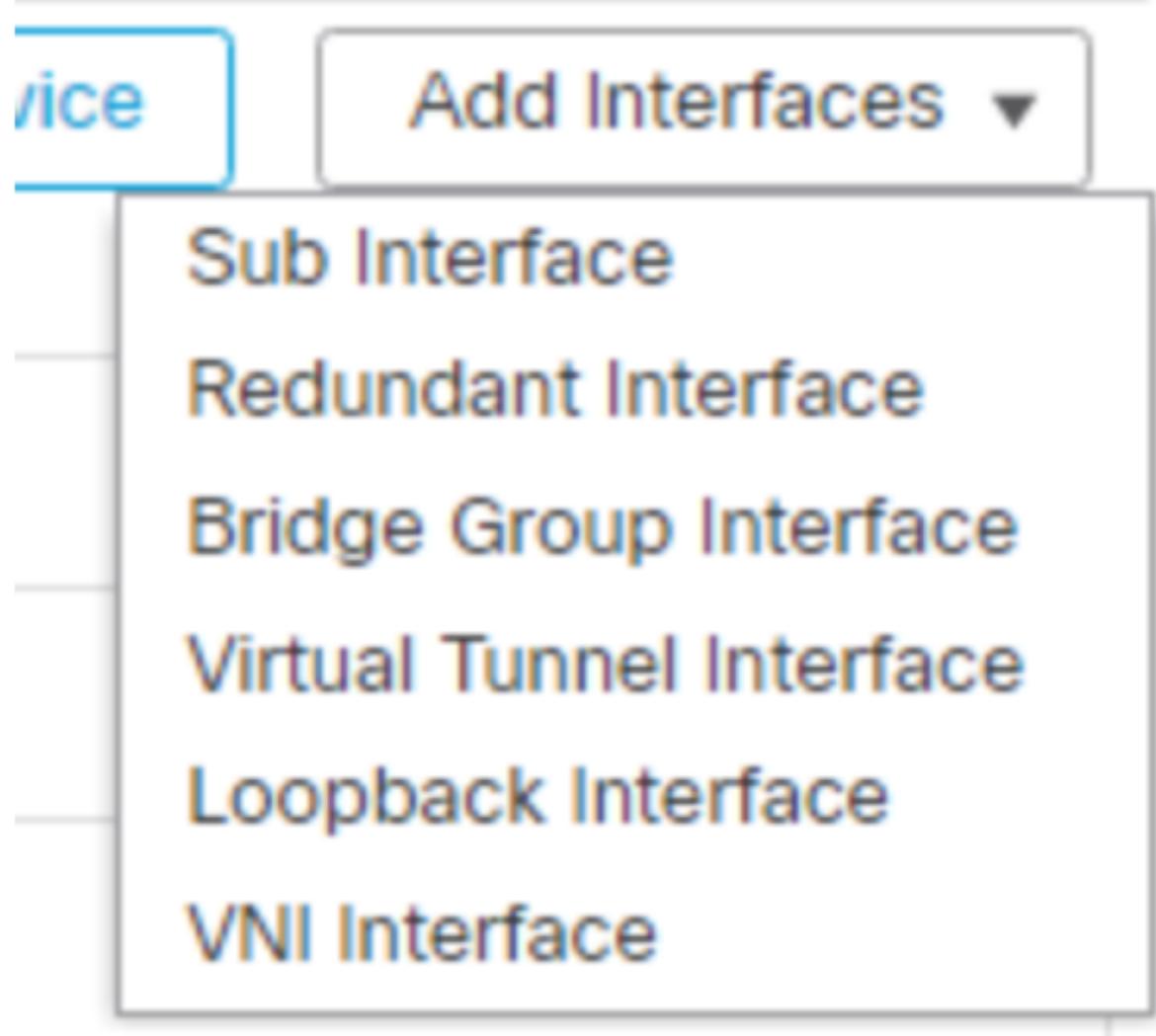
Interfaces overview:

● GigabitEthernet0/3	outside_gi3_40	Physical	OutZone	198.60.40.100/24(Static)
Tunnel10	SVTI_outside_gi3_40_Loop10	VTI	VTI	
● GigabitEthernet0/4	outside_gi4_50	Physical	OutZone	198.60.50.100/24(Static)
Tunnel11	SVTI_outside_gi4_50_Loop11	VTI	VTI	
Loopback10	Loop10	Loopback		169.254.100.2/29(Static)
Loopback11	Loop11	Loopback		169.254.100.10/29(Static)

## Branch1 - Configuring two SVTI interfaces to connect with the two HUB links

1. Go to **Devices > Device Management**. Find **Branch1** and click on the pencil to **edit** it

2. Inside Interfaces tab, click on Add Interfaces > Loopback Interface



3. Fill out name and Loopback ID as per image under **General** tab.

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop10

Enabled

Loopback ID:\*

10

(1-1024)

4. Go to **IPv4** tab and fill out IP Address. Click **Ok** to finish.

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP



IP Address:

169.254.100.6/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

5. Create the second Loopback interface, use the same steps as before

## Add Loopback Interface

General

IPv4

IPv6

Name:

Loop11

Enabled

Loopback ID:\*

11

(1-1024)

## Add Loopback Interface

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

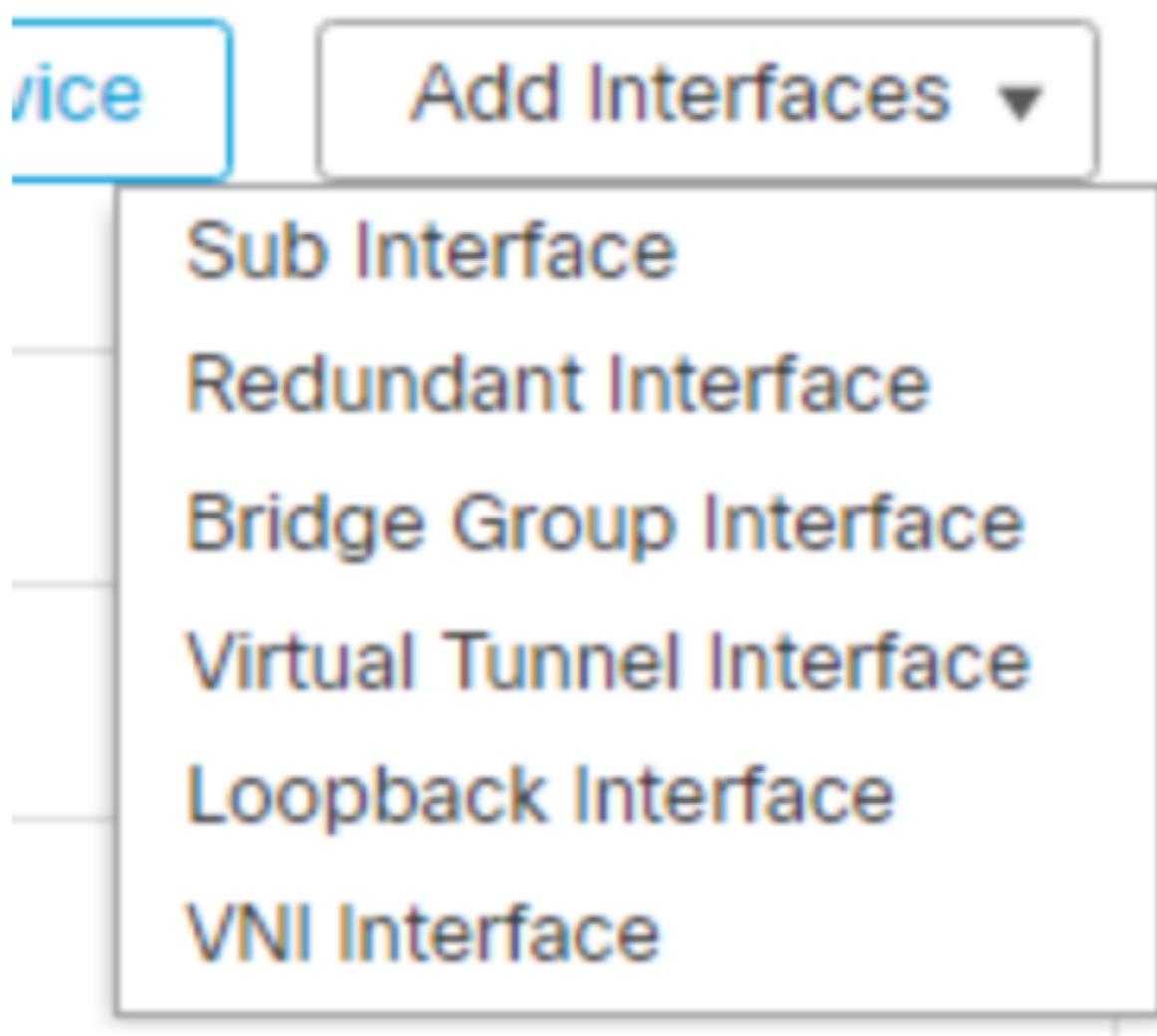
169.254.100.14/29

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

6. Create a **Static** Virtual Tunnel Interface (SVTI) using Loop10 IP address we just created.

- Since we have already created the **VTI** Security Zone before, then we will be using it.
- Use meaningful names so you know which physical and which loopback you are using on your DVTIs or SVTIs

7. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**



8. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside\_gi3\_40\_Loop10**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **10** to match our loopback number
5. Tunnel Source: select Gi0/3 (**outside\_gi3\_40**) as it will be the first interface we will be using to reach out to HUB. Branch1 has two WAN interfaces, we will create one SVTI per WAN interface in this lab.
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop10** we created before

## Add Virtual Tunnel Interface

General

Path Monitoring

### Tunnel Type

Static       Dynamic

Name:\*

SVTI\_outside\_gi3\_40\_Loop10

Enabled

Description:

Security Zone:

VTI

Tunnel ID:\*

(0 - 10413)

Tunnel Source:\*



#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

- IPv4     IPv6

IP Address:\*

- Configure IP

<Valid IPv4 address>/<Mask>



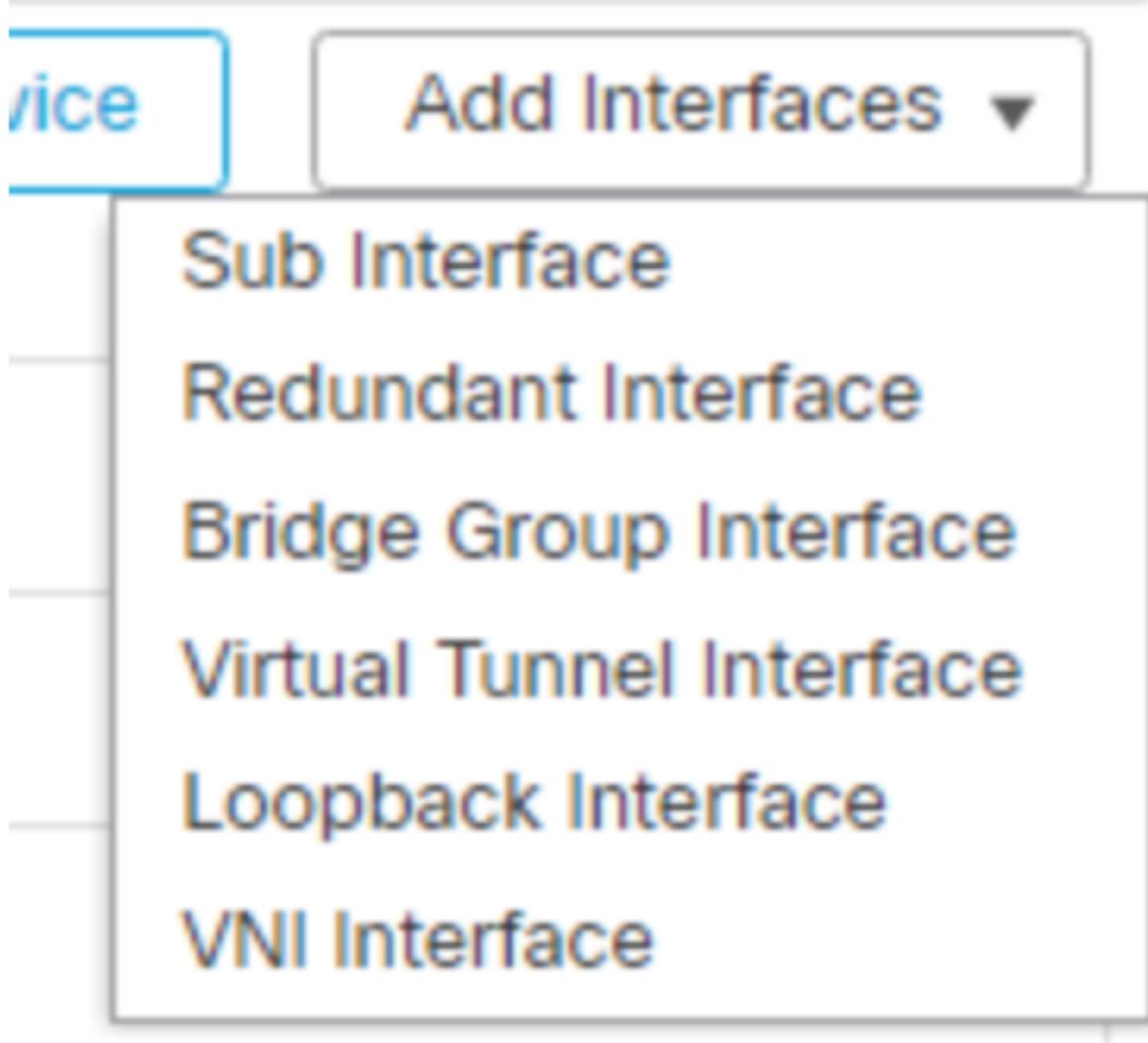
- Borrow IP (IP unnumbered)

Loopback10 (Loop10)



9. Go to **Add Interfaces** again and select **Virtual Tunnel Interface**

---



10. There are some fields to fill out:

1. Tunnel Type: **Static**. This is the default when configuring the Branches.
2. Name: **SVTI\_outside\_gi4\_30\_Loop11**
3. Security Zone: **VTI**
4. Tunnel ID: select a number to represent this SVTI. We will use **11** to match our loopback number
5. Tunnel Source: select Gi0/4 (**outside\_gi4\_30**) as it will be the second interface we will be using to reach out to HUB. Branch1 has two WAN interfaces, we will create one SVTI per WAN interface in this lab.
6. IP address: we will use **IP unnumbered** with the IP of the Loopback **Loop11** we created before

## Add Virtual Tunnel Interface

General

Path Monitoring

Tunnel Type

Static       Dynamic

Name:\*

SVTI\_outside\_gi4\_30\_Loop11

Enabled

Description:

Security Zone:

VTI ▼

Tunnel ID:\*

(0 - 10413)

Tunnel Source:\*

#### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4     IPv6

IP Address:\*

Configure IP

<Valid IPv4 address>/<Mask>



Borrow IP (IP unnumbered)

Loopback11 (Loop11)



11. Click **Ok**

12. Click **Ok** and then Save the configuration

You have unsaved changes

**Save**

**Cancel**

Please save the configuration to make the changes available for use.

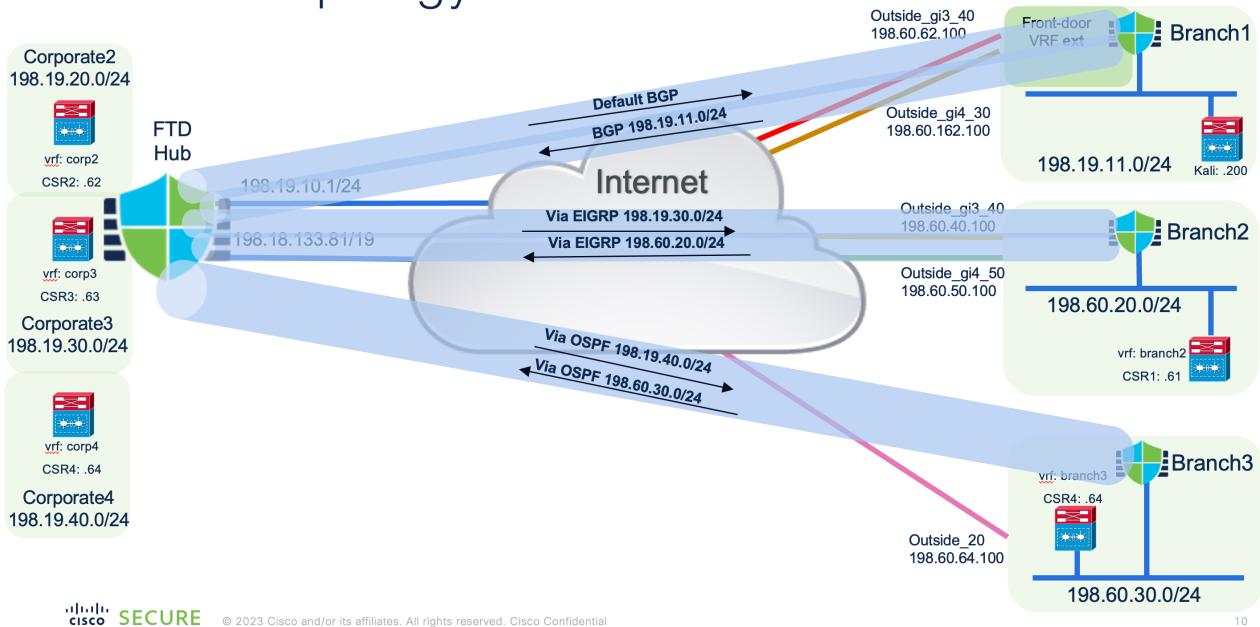
Interfaces overview:

GigabitEthernet0/3	outside_gi3_40	Physical	OutZone	198.60.62.100/24(Static)
Tunnel10	SVTI_outside_gi3_40_Loop10	VTI	VTI	
GigabitEthernet0/4	outside_gi4_30	Physical	OutZone	198.60.162.100/24(Static)
Tunnel11	SVTI_outside_gi4_30_Loop11	VTI	VTI	
Loopback10	Loop10	Loopback		169.254.100.6/29(Static)
Loopback11	Loop11	Loopback		169.254.100.14/29(Static)

## Routing and ECMP configuration

Based on the following topology, configure the routing protocols on the HUB and Branches.

# SDWAN Topology



## HUB and Branch3 - OSPF

This will be a basic OSPF configuration where HUB will announce the network **Corporate4** (198.19.40.0/24) and Branch3 will announce **198.60.30.0/24**

## HUB (NGFW1) configuration

1. Go to **Devices > Device Management**. Find **NGFW1** and click on the pencil to **edit it**

2. Click on **Routing** tab and then click on **OSPF** option

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, it displays "NGFW1" and "Cisco Firepower Threat Defense for". Below this, there is a navigation bar with three tabs: "Device", "Routing" (which is highlighted with a blue underline), and "Interface". The main content area is titled "Manage Virtual Routers". A dropdown menu labeled "Global" is open. Below the dropdown, a list of routing protocols is displayed: ECMP, BFD, OSPF, OSPFv3, EIGRP, and RIP. The "OSPF" option is highlighted with a dark grey background.

3. We need to enable OSPF process, click on **Process 1**

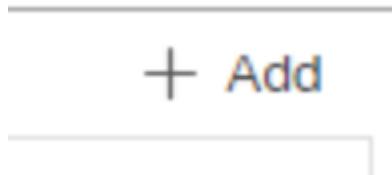
---

Process 1      ID: 1

OSPF Role:

Internal Router      Enter Description here      Advanced

4. Under **Area** tab, click **Add** to add a new Area



5. When configuring the area, we will choose **Area ID 100**

## Add Area

Area Range Virtual Link

OSPF Process:

1

Area ID:\*

100

Area Type:

Normal

Summary Stub    Redistribute  

6. Now we will select the networks that are part of OSPF. Since we do not have the objects yet, we will create them as follows: **Corporate4** (198.19.40.0/24) and **net\_Loop10** (169.254.100.0/29) and **net\_Loop11** (169.254.100.8/29). Click on the + (plus) sign to create the new objects.
- Click Save and then click on the + (plus) sign again to create other objects



## New Network Object

Name

Description

Network

- Host
- Range
- Network
- FQDN

Allow Overrides

## New Network Object

Name

Description

Network

- Host     Range     Network     FQDN

Allow Overrides

## New Network Object

Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

7. After creating the objects, they can be searched in the **Available Network** field. Search for **Corporate4**, **net\_Loop10**, and **net\_Loop11**. Then click **Add** to add them to **Selected Network**. Click **Ok** to finish.

Available Network	Selected Network
<input type="text" value="Loop10"/> <b>net_Loop10</b>	<input type="text" value="net_Loop10"/>

Available Network + C  
Selected Network  
Add

Available Network	Selected Network
<input type="text" value="net_Loop"/> <b>net_Loop10</b> <b>net_Loop11</b>	<input type="text" value="net_Loop10"/> <b>net_Loop11</b>

Available Network + C  
Selected Network  
Add

The screenshot shows a user interface for managing networks. On the left, under 'Available Network', there is a search bar containing 'Corporate4' with an 'X' button to clear it. Below the search bar is a list box containing 'Corporate4', which is highlighted with a blue background. To the right of the list box is a light blue 'Add' button. On the right, under 'Selected Network', there is a list box containing three items: 'net\_Loop10', 'net\_Loop11', and 'Corporate4'. Each item has a small trash can icon to its right.

8. Click Ok and then Save

A confirmation dialog box is displayed. It contains the text 'You have unsaved changes' in red. To the right are two blue buttons: 'Save' and 'Cancel'.

## Branch3 configuration

9. Let's jump to **Branch3** and do the same.

10. Go to **Devices > Device Management**. Find **Branch3** and click on the pencil to **edit** it

11. Click on **Routing** tab and then click on **OSPF** option

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, there is a header with the device name "branch3" and the text "Cisco Firepower Threat Defense for". Below the header, there is a navigation bar with three tabs: "Device", "Routing", and "Interface". The "Routing" tab is currently selected, indicated by a blue underline. Below the navigation bar, the main content area has a title "Manage Virtual Routers". Underneath the title, there is a dropdown menu set to "Global". A vertical list of options is displayed, with "OSPF" highlighted in orange, indicating it is the selected process.

- Global ▾
- Virtual Router Properties
- ECMP
- BFD
- OSPF
- OSPFv3

12. We need to enable OSPF process, click on **Process 1**

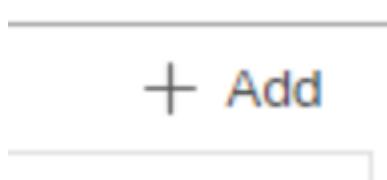
The screenshot shows the configuration page for an OSPF process. At the top, there is a checkbox labeled "Process 1" which is checked, and an "ID:" field containing the value "1". Below this, there is a section for "OSPF Role" with a dropdown menu set to "Internal Router". To the right of the role selection, there is a "Enter Description here" input field and a "Advanced" button.

Process 1      ID: 1

OSPF Role:

Internal Router      Enter Description here      Advanced

13. Under **Area** tab, click **Add** to add a new Area



14. When configuring the area, we will choose **Area ID 100**

---

## Add Area

Area	Range	Virtual Link
<b>OSPF Process:</b> 1		
<b>Area ID:*</b> 100		
<b>Area Type:</b> Normal		
<input type="checkbox"/> Summary Stub	<input type="checkbox"/> Redistribute	<input type="checkbox"/>

15. Now we will select the networks that are part of OSPF. Since we do not have the object for Branch3 network yet, we will create it as follows: **net\_Branch3** (198.60.30.0/24). Click on the + (plus) sign to create a new object.

- Click Save to create the object



## New Network Object

Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

16. After creating the object, they can be searched in the **Available Network** field. Search for **net\_Branch3**, **net\_Loop10**, and **net\_Loop11**. Then click **Add** to add them to **Selected Network**. Click **Ok** to finish.

Available Network	Selected Network
<input type="text" value="Loop10"/> <b>net_Loop10</b>	<input type="text" value="net_Loop10"/>

Available Network	Selected Network
<input type="text" value="net_Loop"/> <b>net_Loop10</b> <b>net_Loop11</b>	<input type="text" value="net_Loop10"/> <b>net_Loop11</b>

The screenshot shows two panels. The left panel, titled 'Available Network', contains a search bar with 'net\_branch3' and a list with one item: 'net\_Branch3'. A blue button labeled 'Add' is located to the right of the search bar. The right panel, titled 'Selected Network', lists three items: 'net\_Loop10', 'net\_Loop11', and 'net\_Branch3'. Each listed item has a small trash can icon to its right.

17. Click Ok

18. Still under **Routing** tab, click on **ECMP** menu

The screenshot shows a 'Manage Virtual Routers' interface. At the top, there are tabs: 'Device', 'Routing' (which is highlighted in blue), and 'Interface'. Below the tabs, a dropdown menu is open, showing 'Global' and a downward arrow. At the bottom of the interface, there are two buttons: 'Virtual Router Properties' and 'ECMP' (which is also highlighted in blue).

19. Click **Add** to add a new ECMP zone.

20. Name the zone **ECMP-VTI**, select both SVTI and add them.

Add ECMP

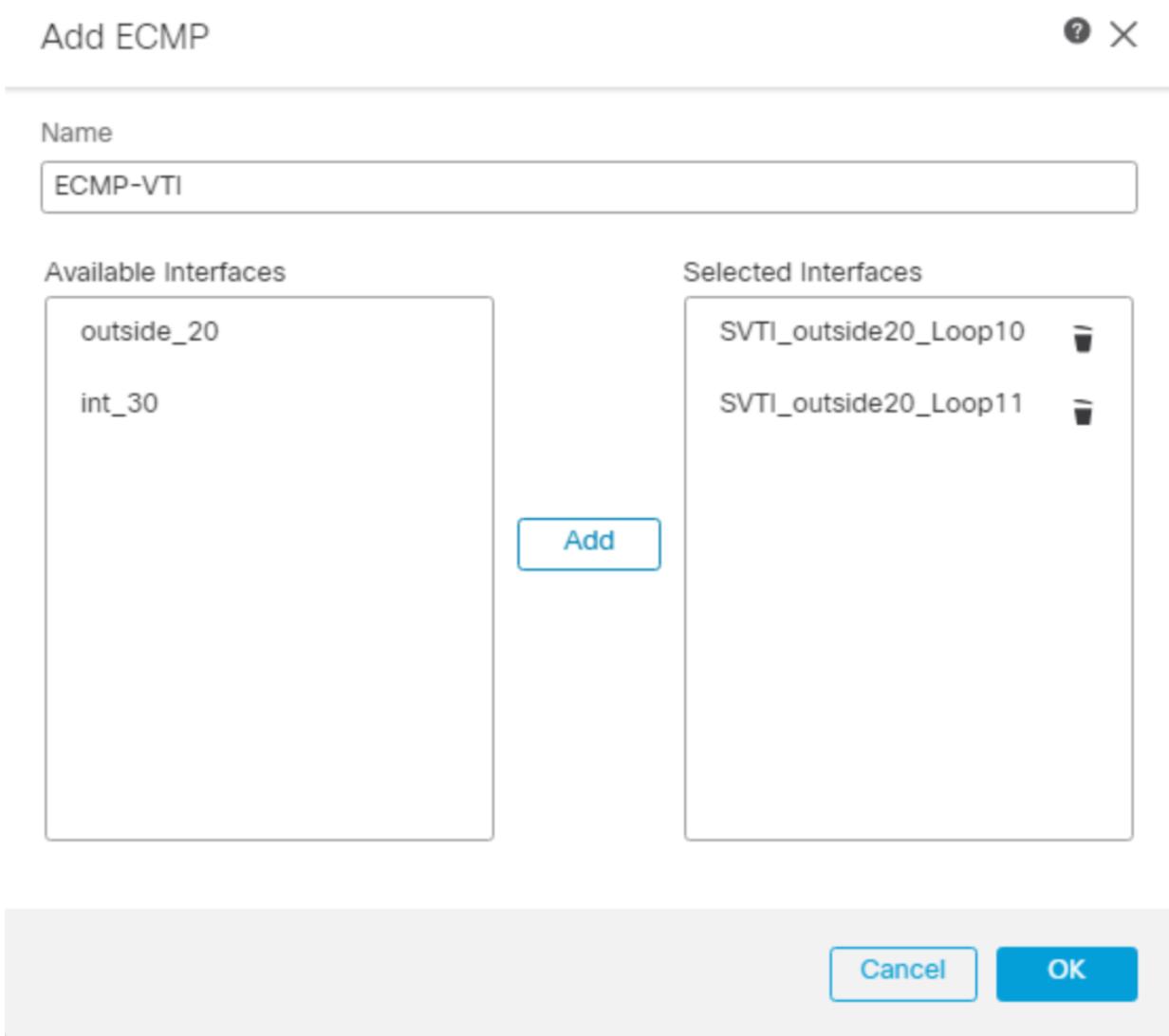
Name  
ECMP-VTI

Available Interfaces  
outside\_20  
int\_30

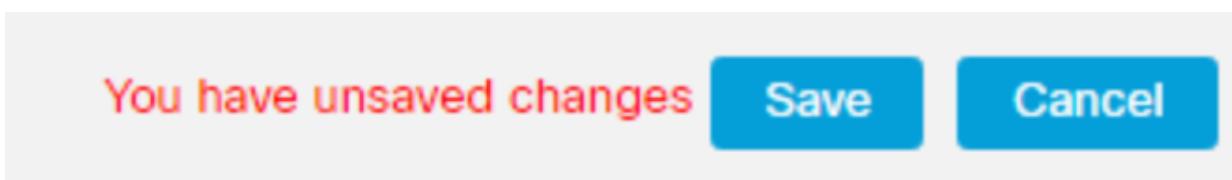
Selected Interfaces  
SVTI\_outside20\_Loop10  
SVTI\_outside20\_Loop11

Add

Cancel OK



21. Click Ok and then Save



## HUB and Branch2 - EIGRP

### HUB (NGFW1) configuration

1. Go to **Devices > Device Management**. Find **NGFW1** and click on the pencil to edit it

2. Click on **Routing** tab and then click on **EIGRP** option

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, the device name "NGFW1" is displayed. Below it, the word "Cisco Firepower Threat Defense for" is partially visible. A navigation bar at the top has three tabs: "Device", "Routing", and "Interface". The "Routing" tab is currently selected, indicated by a blue underline. Below the navigation bar, the title "Manage Virtual Routers" is shown. Underneath this, there is a dropdown menu set to "Global". A vertical list of routing protocols is provided: ECMP, BFD, OSPF, OSPFv3, and EIGRP. The "EIGRP" option is highlighted with a dark grey background.

3. We need to enable EIGRP process, click on **Enable** and pick an AS Number.  
We will use AS Number **10**

The screenshot shows the configuration page for the EIGRP process. It features two main input fields: a checkbox labeled "Enable EIGRP" which is checked, and a text input field labeled "AS Number\*" containing the value "10". To the right of the AS number input field, the range "(1-65535)" is indicated.

4. Now we will select the networks that are part of EIGRP. Since we do not have the object yet, we will create them as follows: **Corporate3**

(198.19.30.0/24). For Loop10 and Loop11 we have already created the objects in the previous task, when we configured OSPF. Click on the + (plus) sign to create the new objects.

- Click Save



## New Network Object

Name

Description

Network

- Host
- Range
- Network
- FQDN

- Allow Overrides

5. After creating the objects, they can be searched in the **Available Network** field. Search for **Corporate3**, **net\_Loop10**, and **net\_Loop11**. Then click **Add**

to add them to **Selected Network**. Click **Ok** to finish.

### Selected Networks/Hosts (3)

net\_Loop10



net\_Loop11



Corporate3



6. Click Ok and then Save

You have unsaved changes

**Save**

**Cancel**

## Branch2 configuration

7. Let's jump to **Branch2** and do the same.
8. Go to **Devices > Device Management**. Find **Branch2** and click on the pencil to **edit** it

9. Click on **Routing** tab and then click on **EIGRP** option

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, there is a header with the text "branch2" and "Cisco Firepower Threat Defense for V". Below the header, there are three tabs: "Device", "Routing" (which is highlighted with a blue underline), and "Interfaces". A large central panel titled "Manage Virtual Routers" contains a dropdown menu set to "Global". Below the dropdown, there is a list of routing protocols: ECMP, BFD, OSPF, OSPFv3, and EIGRP. The "EIGRP" option is highlighted with a dark grey background.

10. We need to enable EIGRP process, click on **Enable** and pick an AS Number.  
We will use AS Number **10**

The screenshot shows the configuration page for the EIGRP process. It features two main input fields: a checkbox labeled "Enable EIGRP" which is checked, and a text input field labeled "AS Number\*" containing the value "10". To the right of the AS number input, there is a note in parentheses: "(1-65535)".

11. Now we will select the networks that are part of EIGRP. Since we do not have the Branch2 object yet, we will create it as follows: **net\_Branch2**

(198.60.20/24). The objects for Loop10 and Loop11 have been already created in the previous task, when we configured OSPF. Click on the + (plus) sign to create the new object.

- Click Save



## New Network Object

Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

12. After creating the object, they can be searched in the **Available Network** field. Search for **net\_Branch2**, **net\_Loop10**, and **net\_Loop11**. Then click

Add to add them to **Selected Network**. Click **Ok** to finish.

### Selected Networks/Hosts (3)

net_Branch2	
net_Loop11	
net_Loop10	

13. Click Ok

14. Still under **Routing** tab, click on **ECMP** menu

The screenshot shows the Cisco Firepower Threat Defense interface for a device named "branch2". The top navigation bar includes tabs for Device, Routing (which is selected), and Interfaces. Below the navigation bar is a section titled "Manage Virtual Routers" with a dropdown menu set to "Global". Underneath this is a "Virtual Router Properties" section. At the bottom of the screen, there is a prominent grey bar containing the text "ECMP".

15. Click **Add** to add a new ECMP zone.

16. Name the zone **ECMP-VTI**, select both SVTI and add them.

Add ECMP

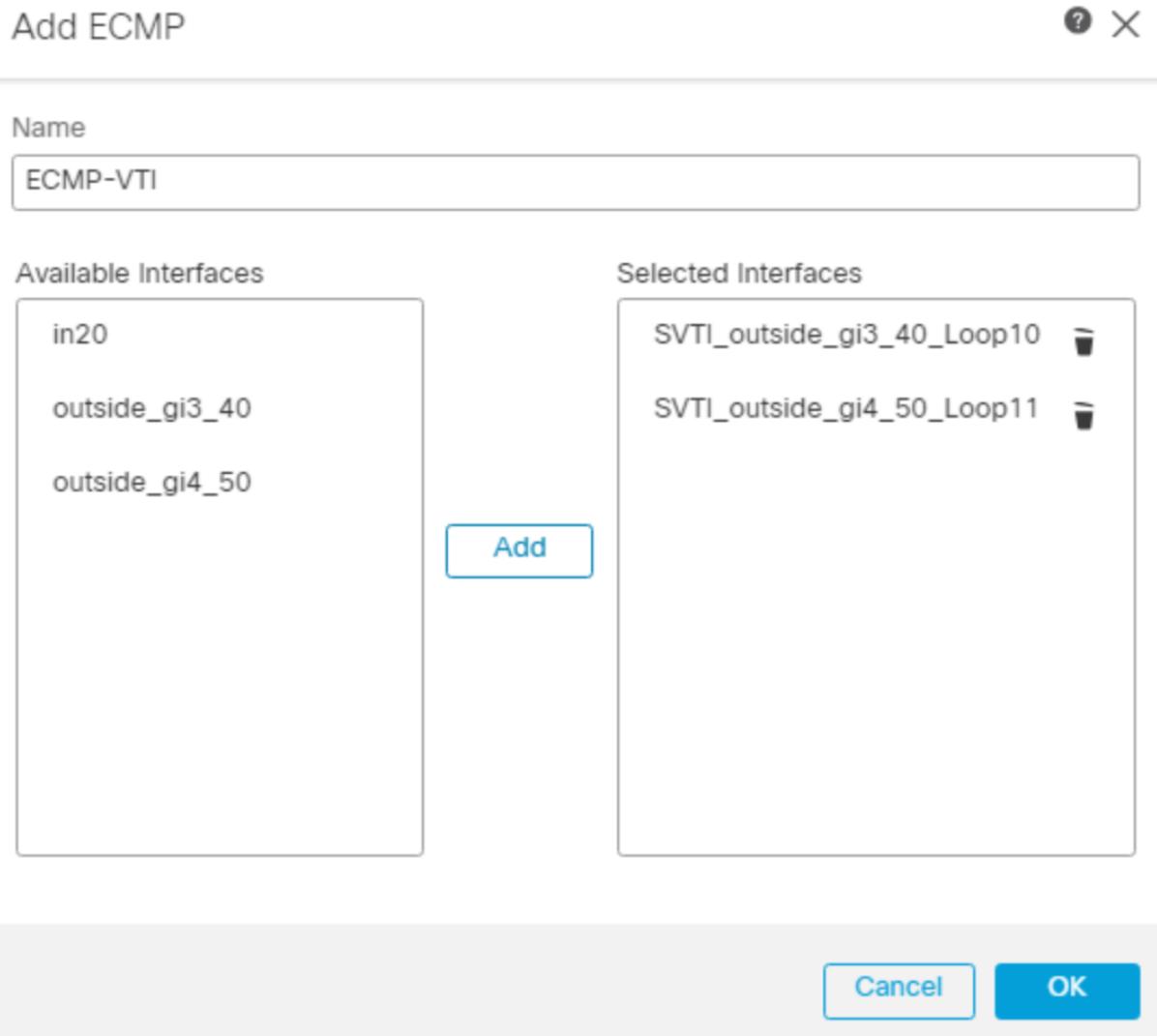
Name  
ECMP-VTI

Available Interfaces  
in20  
outside\_gi3\_40  
outside\_gi4\_50

Selected Interfaces  
SVTI\_outside\_gi3\_40\_Loop10  
SVTI\_outside\_gi4\_50\_Loop11

Add

Cancel OK



17. Click Ok and then Save

You have unsaved changes **Save** **Cancel**

## HUB and Branch1 - BGP

Branch1 will be able to receive a default route from BGP because it has been configured with a **front-door VRF**. You can check this configuration under

## Routing tab

The screenshot shows the 'branch1' device configuration. The 'Virtual Routers' section lists two entries: 'Global' and 'ext'. The 'Global' entry includes several interfaces: Loop10, Loop11, SVTI\_outside\_gi3\_40\_Loop10, management, and SVTI\_outside\_gi4\_30\_Loop11. The 'ext' entry includes the interfaces outside\_gi3\_40 and outside\_gi4\_30.

The VRF is called **ext** and it has the two WAN links. When we select the VRF, we can see the two default routes going to the local ISP

The screenshot shows the 'branch1' device configuration with the 'ext' VRF selected. The 'IPv4 Routes' table shows two entries:

Network	Interface	Leaked from Virtual Router	Gateway
any-ipv4	outside_gi4_30		198.60.162.1
any-ipv4	outside_gi3_40		198.60.62.1

So, in order to avoid routing problem where Firepower has default routes to ISPs and also receives default routes via BGP, we need to create a front-door VRF. Gladly, Firepower doesn't require you to know how to leak routes, it does everything for you.

## HUB (NGFW1) configuration

1. Go to **Devices > Device Management**. Find **NGFW1** and click on the pencil to **edit** it
2. Click on **Routing** tab, click on **BGP** under General Settings at the bottom of the right hand side.

# NGFW1

Cisco Firepower Threat Defense for

Device

Routing

Interface

## Manage Virtual Routers

Global



Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

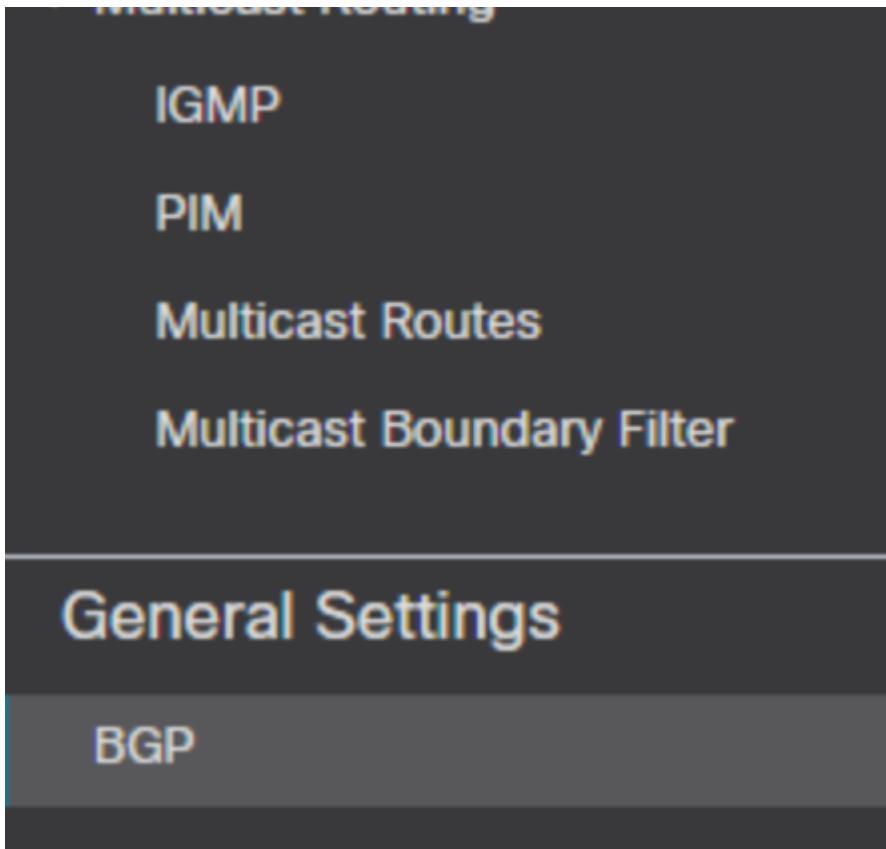
▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing



3. Click on **Enable BGP** checkbox and type the AS Number. Private AS starts at 65000, so this will be our choice

Enable BGP:

AS Number\*

65000

4. Click on **BGP > IPv4** on the left hand side

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, the device name "NGFW1" is displayed in large blue letters, followed by the text "Cisco Firepower Threat Defense for". Below the device name, there are three tabs: "Device", "Routing", and "Interface". The "Routing" tab is currently selected, indicated by a blue underline and a blue bar underneath it. In the main content area, the title "Manage Virtual Routers" is shown in large white text. Below this, a dropdown menu is open, showing the option "Global" with a downward arrow icon. A vertical list of routing protocols is displayed, each with a small orange icon to its left: ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4, and IPv6. The "BGP" item has a small downward arrow icon to its left, indicating it is a collapsed section. The "IPv4" item is highlighted with a dark grey background.

5. Click on **Enable IPv4** option

Enable IPv4:

AS Number 65000

6. Under **General** tab, edit the options below

1. Forward Packets Over Multiple Paths
  - Number of Paths: 2
  - iBGP number of paths: 2

### Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

2

[Cancel](#)

[OK](#)

7. Under **Neighbor** tab, click **Add** to add a new neighbor

[+](#) [Add](#)

8. We will add two neighbors, one per Branch1 WAN interface. Since each WAN will have a SVTI, we can become neighbor in each interface. We will fill out the following fields
1. IP Address: 169.254.100.6 (Branch1 SVTI over gi3)
  2. Remote AS: 65000 (same for both)
  3. Check the option **Enable address**
  4. Under **Routes** tab, check the option **Generate default routes**
  5. Under **Advanced** tab, check the option **Use itself as next hop for this neighbor**

## 6. Click Ok

### Add Neighbor

IP Address\*

 Enabled address

Remote AS\*

 Shutdown administratively

(1-4294967295 or 1.0-65535.65535)

 Configure graceful restart Graceful restart(failover/spanned mode)

Filtering Routes

Routes

Til

### Advertisement Interval

(0-600)

Remove private AS numbers from

Generate default routes

### Route Map

Enable Authentication

#### Enable Encryption

0



#### Password

#### Confirm Password

Send Community attribute to this neighbor

Use itself as next hop for this neighbor

9. Now we will do the same steps again for the other SVTI to Branch1.

1. IP Address: 169.254.100.14 (Branch1 SVTI over gi4)
2. Remote AS: 65000 (same for both)
3. Check the option **Enable address**
4. Under **Routes** tab, check the option **Generate default routes**
5. Under **Advanced** tab, check the option **Use itself as next hop for this neighbor**
6. Click **Ok**

#### Add Neighbor

IP Address\*

169.254.100.14

Enabled address

Shutdown administratively

Remote AS\*

65000

Configure graceful restart

(1-4294967295 or 1.0-65535.65535)

Graceful restart(failover/s)

Filtering Routes

Routes

Advertisement Interval

(0-600)

Remove private AS numbers from advertisements

Generate default routes

- - -

Filtering Routes

Routes

Timers

Advanced

Enable Authentication

Enable Encryption

0

▼

Password

Confirm Password

Send Community attribute to this neighbor

Use itself as next hop for this neighbor

10. Click Ok and then Save

You have unsaved changes

Save

Cancel

**Branch1 configuration**

1. Go to **Devices > Device Management**. Find **Branch1** and click on the pencil to **edit** it
2. Click on **Routing** tab, click on **BGP** under General Settings at the bottom of the right hand side. Make sure you are NOT in the VRF but in the **Global** table. You can easily spot this looking at under **Manage Virtual Routers**

where it says "Global"

# branch1

Cisco Firepower Threat Defense for

Device

Routing

Interface

## Manage Virtual Routers

Global



Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

## ▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

## General Settings

BGP

3. Click on **Enable BGP** checkbox and type the AS Number. Private AS starts at 65000, so this will be our choice

Enable BGP:

AS Number\*

65000

4. Click on **BGP > IPv4** on the left hand side

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, the device name "branch1" is displayed. Below it, the navigation bar includes tabs for "Device", "Routing" (which is underlined in blue), and "Interface". A large central panel titled "Manage Virtual Routers" contains a dropdown menu set to "Global". Below this, a list of routing protocols is shown: ECMP, BFD, OSPF, OSPFv3, EIGRP, and RIP. A "Policy Based Routing" section follows. At the bottom of the list, "BGP" is expanded, revealing its sub-option "IPv4".

5. Click on **Enable IPv4** option

Enable IPv4:

AS Number 65000

6. Under **General** tab, edit the options below

1. Forward Packets Over Multiple Paths
  - Number of Paths: 2
  - iBGP number of paths: 2

### Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

2

[Cancel](#)

[OK](#)

7. Under **Neighbor** tab, click **Add** to add a new neighbor

[+](#) [Add](#)

8. We will add two neighbors, one per HUB WAN interface. Since each Branch1 WAN has a SVTI, we can become neighbor in each interface. We will fill out the following fields

1. IP Address: 169.254.100.1 (HUB DVTI over outside interface)
2. Remote AS: 65000 (same for both)
3. Check the option **Enable address**
4. Click **Ok**

## Add Neighbor

IP Address*	<input type="text" value="169.254.100.1"/>	<input checked="" type="checkbox"/> Enabled address
Remote AS*	<input type="text" value="65000"/> (1-4294967295 or 1.0-65535.65535)	<input type="checkbox"/> Shutdown administratively
		<input type="checkbox"/> Configure graceful restart
		<input type="checkbox"/> Graceful restart(failover)

9. Now we will do the same steps again for the other SVTI to HUB.

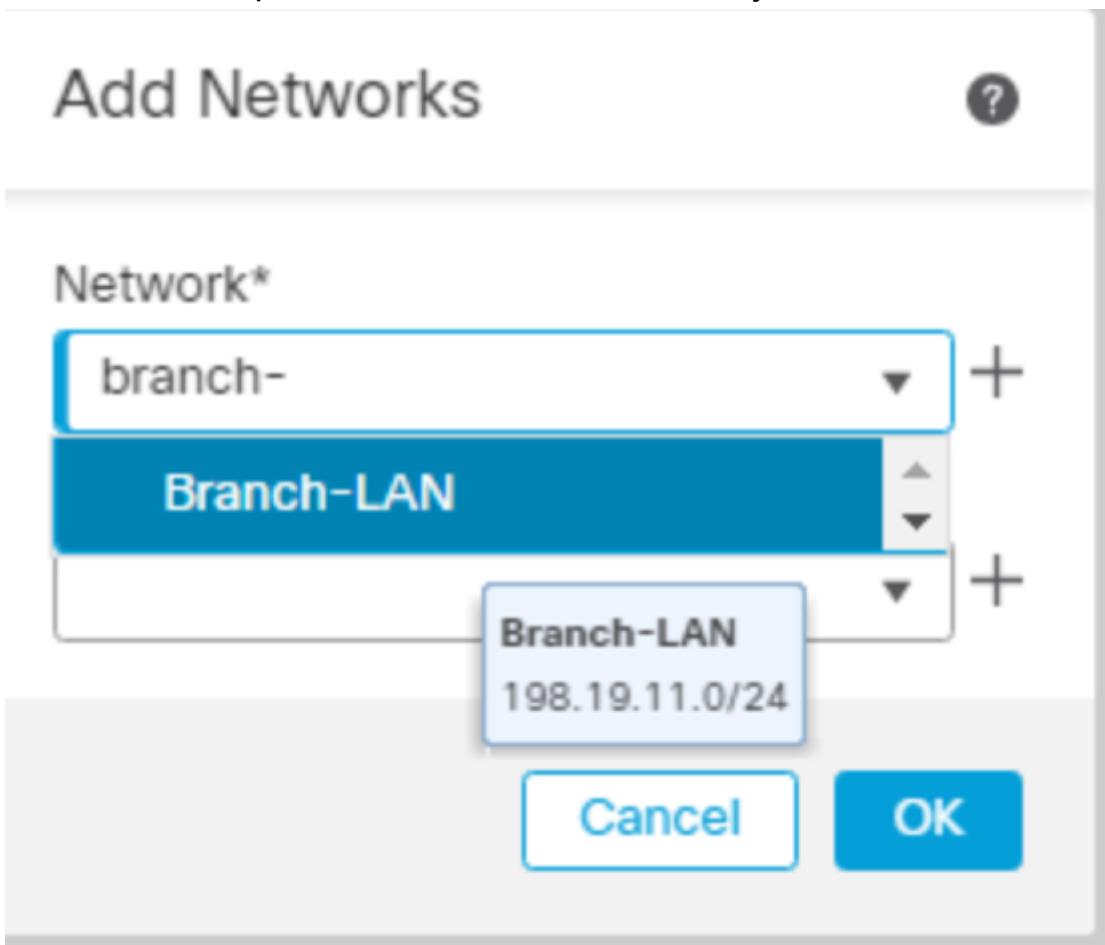
1. IP Address: 169.254.100.9 (HUB DVTI over in10)
2. Remote AS: 65000 (same for both)
3. Check the option **Enable address**
4. Click **Ok**

## Add Neighbor

IP Address*	<input type="text" value="169.254.100.9"/>	<input checked="" type="checkbox"/> Enabled address
Remote AS*	<input type="text" value="65000"/> (1-4294967295 or 1.0-65535.65535)	<input type="checkbox"/> Shutdown administratively
		<input type="checkbox"/> Configure graceful restart
		<input type="checkbox"/> Graceful restart(failover/sp)

10. Under **Networks** tab, click the + (plus) sign to add a network to be advertised

11. Click on the drop down menu and select the object **Branch-LAN**



12. Click Ok

13. Still under **Routing** tab, click on **ECMP** menu

The screenshot shows the Cisco Firepower Threat Defense interface for a device named "branch1". The top navigation bar has tabs for "Device", "Routing" (which is highlighted in blue), and "Interface". Below the navigation bar, the main content area is titled "Manage Virtual Routers". A dropdown menu is open, showing options: "Global" (which is selected and highlighted in white) and "Virtual Router Properties". Further down, there is a link labeled "ECMP".

14. Click **Add** to add a new ECMP zone.

15. Name the zone **ECMP-VTI**, select both SVTI and add them.

Add ECMP

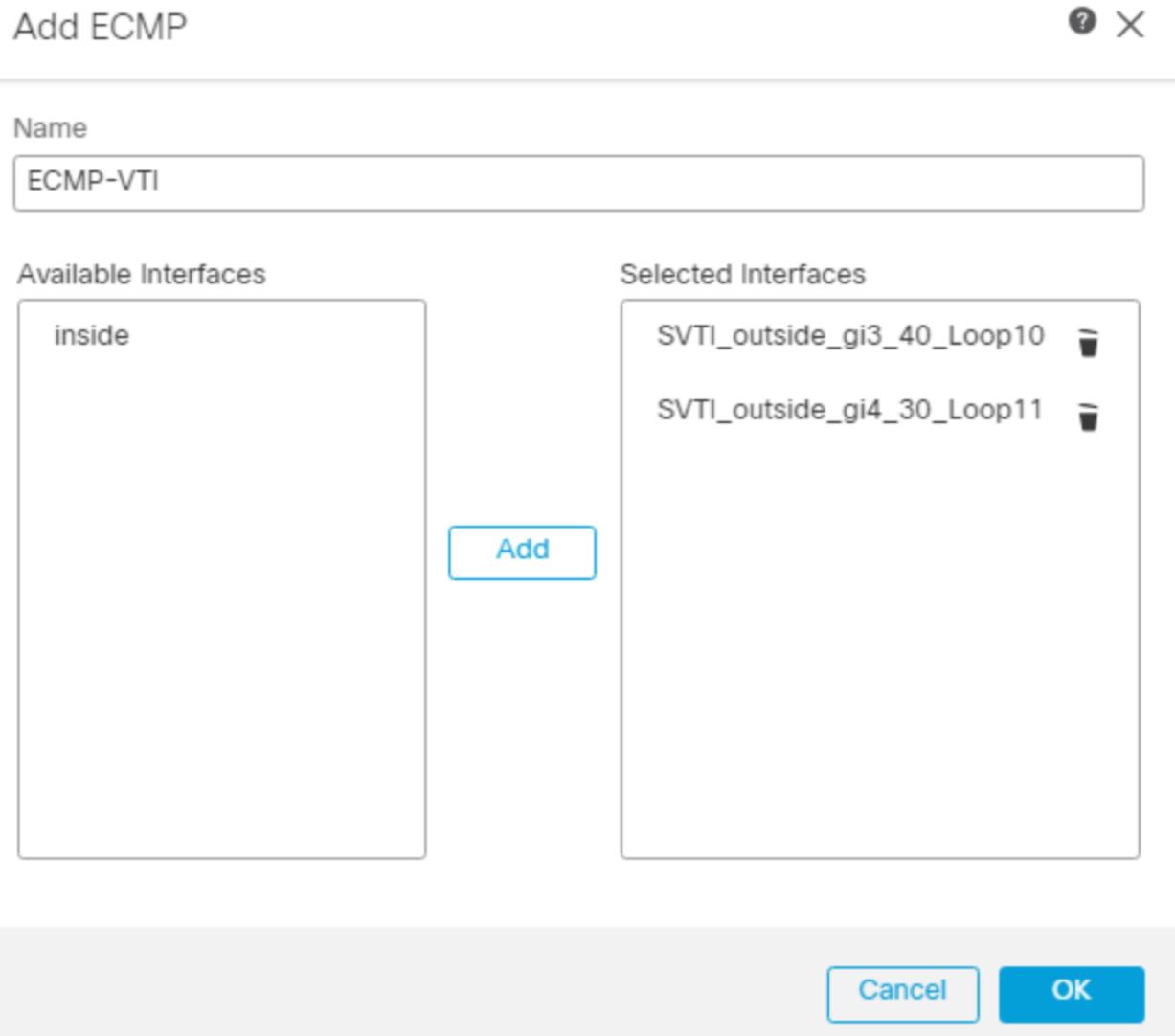
Name  
ECMP-VTI

Available Interfaces  
inside

Selected Interfaces  
SVTI\_outside\_gi3\_40\_Loop10  
SVTI\_outside\_gi4\_30\_Loop11

Add

Cancel OK



16. Click Ok and then Save

You have unsaved changes **Save** **Cancel**

## Direct Internet Access (DIA) configuration

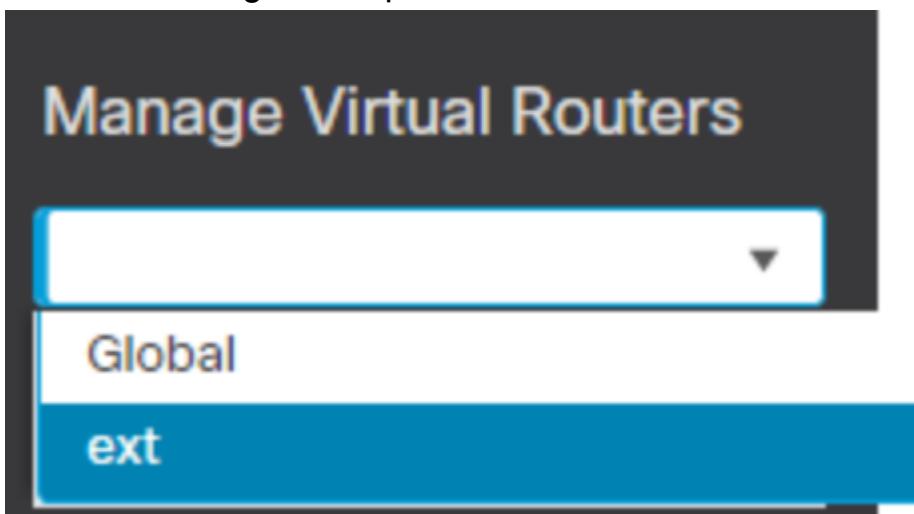
- DIA is a feature that gives the branch local internet access without going to HUB for internet or SaaS services.
- Branch2 and Branch3 only receive specific routes from HUB via their respective dynamic routing protocols. With that, the default route prevails and they already send internet traffic to their local ISP.
- Branch1 by the other hand, it receives and default route via BGP, meaning, it will send everything to HUB. In this case we can leverage DIA to send some applications to exit via local ISPs, balanced by their dual ISP approach.

### Branch1 - Default routes to WAN providers - VRF ext

## 1. Under Routing tab, click on Manage Virtual Routers

The screenshot shows the 'branch1' device configuration. The 'Routing' tab is selected. On the left, a sidebar lists 'Manage Virtual Routers', 'Virtual Router Properties', 'ECMP', 'BFD', 'OSPF', 'BGP', 'IPv4', 'IPv6', and 'Static Route'. The 'Static Route' option is highlighted. The main panel displays 'Virtual Routers' with two entries: 'Global' and 'ext'. The 'ext' entry is expanded, showing interfaces 'Loop10', 'Loop11', 'SVI1\_outside\_gi3\_40\_Loop10', 'management', and 'SVI1\_outside\_gi4\_30\_Loop11...'. A search bar at the top right is labeled 'Search Virtual Router or Interface'.

2. Select **ext** using the drop down menu.



3. VRF is called **ext**. Click on **Static route** to see Branch1 two default route to local ISPs.

The screenshot shows the 'branch1' device configuration. The 'Routing' tab is selected. The 'Static Route' option in the sidebar is selected. The main panel displays a table titled 'Network' with columns for 'Network', 'Interface', 'Leaked from Virtual Router', and 'Gateway'. Two rows are listed: one for 'any-ipv4' pointing to 'outside\_gi4\_30' with gateway '198.60.162.1' and another for 'any-ipv4' pointing to 'outside\_gi3\_40' with gateway '198.60.62.1'. The table has sections for 'IPv4 Routes' and 'IPv6 Routes'.

Network	Interface	Leaked from Virtual Router	Gateway
any-ipv4	outside_gi4_30		198.60.162.1
any-ipv4	outside_gi3_40		198.60.62.1

4. Click on **ECMP** to see the load-balancing on these two links

The screenshot shows the 'branch1' device configuration. The 'ECMP' option in the sidebar is selected. The main panel displays a table titled 'Equal-Cost Multipath Routing (ECMP)' with columns for 'Name' and 'Interfaces'. One row is listed: 'ECMP\_ext' with interfaces 'outside\_gi3\_40, outside\_gi4\_30'.

Name	Interfaces
ECMP_ext	outside_gi3_40, outside_gi4_30

**Branch1 - Static route - Global table**

As we mentioned, Branch1 will receive a default route via BGP when tunnel is up. This default route will be installed in the global routing table which will not conflict with ISP routes installed at VRF ext

1. Click on **Manage Virtual Routes** again and now select Global

The screenshot shows the Cisco Firepower Threat Defense interface. At the top, it displays "branch1" and "Cisco Firepower Threat Defense for VM". Below this, there are three tabs: "Device", "Routing" (which is highlighted in blue), and "Interfaces". A large central panel is titled "Manage Virtual Routers". Within this panel, there is a search bar containing a single character and a dropdown arrow. Below the search bar is a blue header bar with the word "Global" in white. The main content area is currently empty, showing only a small portion of the interface.

2. Now click on **Static Route**. Notice that there aren't any routes configured since it will receive via BGP

Network	Interface	Leaked from Virtual Router	Gateway	T
▼ IPv4 Routes				

## Enabling Path Monitoring

Path monitoring, when configured on interfaces, derive metrics such as round trip time (RTT), jitter, mean opinion score (MOS), and packet loss per interface. These metrics are used to determine the best path for routing PBR traffic.

### ICMP-based Path Monitoring

- The metrics on the interfaces are collected dynamically using ICMP probe messages to the interface's default gateway or a specified remote peer.

### HTTP-based Path Monitoring

- Path monitoring computes flexible metrics for multiple remote peers per interface. To monitor and determine best path for multiple applications through a policy on a branch firewall, HTTP is preferred over ICMP for the following reasons:
  - HTTP-ping can derive the performance metrics of the path up to the application layer of the server, where the application is hosted.
  - The need to change the firewall configuration whenever the application server IP address is changed is removed as the application domain is tracked instead of the IP address.

1. Edit Branch1, under **Interfaces** tab, we will select both WAN interfaces to enable Path Monitoring.
2. Select Gi0/3 and click on the pencil to edit it
3. Click on **Path Monitoring** to enable the metrics over ICMP and HTTP. We will enable both in this lab
4. Click **Ok**

### Edit Physical Interface

The screenshot shows the 'Edit Physical Interface' dialog with the 'Path Monitoring' tab selected. The tabs at the top are General, IPv4, IPv6, Path Monitoring (which is highlighted with a blue underline), and Hardware Configuration.

**Enable IP based Monitoring:** A checked checkbox labeled "Enable IP based Monitoring". Below it is a note: "Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface."

**Monitoring Type:** A dropdown menu set to "Next-hop of default route out of interface (Auto)". Below the dropdown is a note: "System monitors the next hop of the interface. Tries IPv4 and then IPv6. If the peer is unavailable, monitoring is not done."

**Enable HTTP based Application Monitoring:** A checked checkbox labeled "Enable HTTP based Application Monitoring". Below it is a note: "By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically."

**Applications:** A table with one row labeled "Applications" and one row below it stating "No records to display".

5. Select Gi0/4 and click on the pencil to edit it
6. Click on **Path Monitoring** to enable the metrics over ICMP and HTTP. We will enable both in this lab

## Edit Physical Interface

The screenshot shows a configuration interface for a physical interface. At the top, there are tabs for General, IPv4, IPv6, Path Monitoring (which is highlighted in blue), and Hardware Configuration. Under the Path Monitoring tab, there is a section titled "Enable IP based Monitoring" with a checked checkbox. Below it, a note says "Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface." A "Monitoring Type:" dropdown is set to "Next-hop of default route out of interface (Auto)". A note below explains the monitoring type. Another section titled "Enable HTTP based Application Monitoring" has a checked checkbox, with a note explaining its function. A "Applications" table below shows no records.

Applications
No records to display

## Enabling PBR

### PBR and Path Monitoring

- Typically, in PBR, traffic is forwarded through egress interfaces based on the priority value (interface cost) configured on them. From management center version 7.2, PBR uses IP-based path monitoring to collect the performance metrics (RTT, jitter, packet-lost, and MOS) of the egress interfaces. PBR uses the metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR about the monitored interface whose metric got changed. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path.

## PBR and HTTP-based Path Monitoring

- From management center version 7.4, PBR can be configured to use HTTP-based path monitoring to collect the performance metrics of the application domains and not just one destination IP address. Path monitoring does not commence monitoring immediately after HTTP-based application monitoring is configured. It starts monitoring only when a DNS entry is snooped for a domain. With the information on the resolved IP for the domain, it sends and receives the HTTP request and response respectively. When DNS resolves multiple IP addresses for a single domain, the first resolved IP address will be used for probing and monitoring the application. It continues to monitor till the IP address changes or the HTTP-based path monitoring is disabled.

1. Now, under **Routing** tab, inside Global routing table, select **Policy Based Routing**

# branch1

Cisco Firepower Threat Defense fo

Device

Routing

Interface

## Manage Virtual Routers

Global

**Virtual Router Properties**

ECMP

BFD

OSPF

OSPFv3

EIGRP

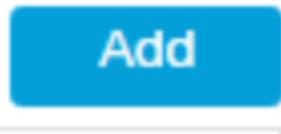
RIP

**Policy Based Routing**

POP

2. Click **Configure Interface Priority** to specify if there is any preferred interface over the other. Set both WAN interfaces with priority **10** so they can load-balance between them.
3. Click Save.

4. Create a new PBR policy by clicking on Add button



5. Select which interface the users will be coming from. In our case, interface inside

Add Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface\*

inside x

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel Save

6. Click Add again

7. In this page, we will configure the following

1. **Match ACL:** this is the applications we want to enable DIA. Create an ACL called **Social-Networking** and add social network applications such as LinkedIn, Facebook and Instagram
2. **Send to:** which interface you want to send this traffic that matches the ACL. This can be either an IP or Egress interface. Select **Egress Interfaces**
3. **Interface Ordering:** how we are going to choose which interface to send the traffic to. Select **Interface Priority**. Just for documentation purpose, here are the options:
  - By Interface Priority—The traffic is forwarded based on the priority of the interfaces. Traffic is routed to the interface with the least priority value first. When the interface is not available, the traffic is then forwarded to the interface with the next lowest priority value

- By Order—The traffic is forwarded based on the sequence of the interfaces specified here
- By Minimal Jitter—The traffic is forwarded to the interface that has the lowest jitter value
- By Maximum Mean Opinion Score—The traffic is forwarded to the interface that has the maximum mean opinion score (MOS)
- By Minimal Round Trip Time—The traffic is forwarded to the interface that has the minimal round trip time (RTT)
- By Minimal Packet Loss—The traffic is forwarded to the interface that has the minimal packet loss. You need to enable Path Monitoring on the interfaces for PBR to obtain the packet loss values.

8. To create an ACL, click on the + (plus) sign next to Match ACL field.

9. Give it a name and click Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

10. Keep the defaults. Under **Application** tab, select the applications we mentioned above.

11. Click **Add** then click **Save**

Network	Port	<b>Application</b>	Users	Security Group Tag				
Application Filters <input type="button" value="Clear All Filters"/> Available Applications (2) <input type="button" value="Clear All"/> <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <input type="text" value="Search by name"/> <div style="list-style-type: none; padding-left: 0;"> <ul style="list-style-type: none"> <li><input type="checkbox"/> Very Low</li> <li><input type="checkbox"/> Low</li> <li><input type="checkbox"/> Medium</li> <li><input type="checkbox"/> High</li> <li><input type="checkbox"/> Very High</li> </ul> </div> </div> <div style="flex: 1;"> <input type="text" value="Search by name"/> <div style="list-style-type: none; padding-left: 0;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Instagram</li> <li><input type="checkbox"/> Instagram Media</li> </ul> </div> </div> <div style="flex: 1; text-align: right;"> <input type="button" value="Add to Rule"/> </div> </div>								
Selected Applications and Filters (3) <table border="1"> <thead> <tr> <th>Applications</th> </tr> </thead> <tbody> <tr> <td>Facebook</td> </tr> <tr> <td>Instagram</td> </tr> <tr> <td>LinkedIn</td> </tr> </tbody> </table>					Applications	Facebook	Instagram	LinkedIn
Applications								
Facebook								
Instagram								
LinkedIn								

Entries (1)									<a href="#">Add</a>
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Facebook Instagram LinkedIn	Any		

## 12. Click **Save** again

Add Forwarding Actions

?

Match ACL:  Social-Networking																	
Send To:  Egress Interfaces																	
Interface Ordering:  Interface Priority																	
<table border="1"> <tr> <td colspan="2">Available Interfaces</td> </tr> <tr> <td colspan="2"> <input type="text" value="Search by interface name"/> </td> </tr> <tr> <td>Priority</td> <td>Interface</td> </tr> <tr> <td>0</td> <td>inside</td> </tr> <tr> <td>0</td> <td>Loop10</td> </tr> <tr> <td>0</td> <td>Loop11</td> </tr> <tr> <td>0</td> <td>SVTI_outside_gi3_40_Loop10</td> </tr> <tr> <td>0</td> <td>SVTI_outside_gi4_30_Loop11</td> </tr> </table>		Available Interfaces		<input type="text" value="Search by interface name"/>		Priority	Interface	0	inside	0	Loop10	0	Loop11	0	SVTI_outside_gi3_40_Loop10	0	SVTI_outside_gi4_30_Loop11
Available Interfaces																	
<input type="text" value="Search by interface name"/>																	
Priority	Interface																
0	inside																
0	Loop10																
0	Loop11																
0	SVTI_outside_gi3_40_Loop10																
0	SVTI_outside_gi4_30_Loop11																
<table border="1"> <tr> <td colspan="2">Selected Egress Interfaces*</td> </tr> <tr> <td>Priority</td> <td>Interface</td> </tr> <tr> <td>10</td> <td>outside_gi3_40</td> </tr> <tr> <td>10</td> <td>outside_gi4_30</td> </tr> </table>		Selected Egress Interfaces*		Priority	Interface	10	outside_gi3_40	10	outside_gi4_30								
Selected Egress Interfaces*																	
Priority	Interface																
10	outside_gi3_40																
10	outside_gi4_30																
<a href="#">Cancel</a> <a href="#">Save</a>																	

## 13. Click **Save** to finish the process

Add Policy Based Route

?

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface\*

inside	
--------	--

Match Criteria and Egress Interface

[Add](#)

Specify forward action for chosen match criteria.

Match ACL	Forwarding Action	<a href="#">Add</a>
Social-Networking	Send and load balance it through #10 outside_gi3_40 #10 outside_gi4_30	

<a href="#">Cancel</a>	<a href="#">Save</a>
------------------------	----------------------

14. Click **Save** to save the policy

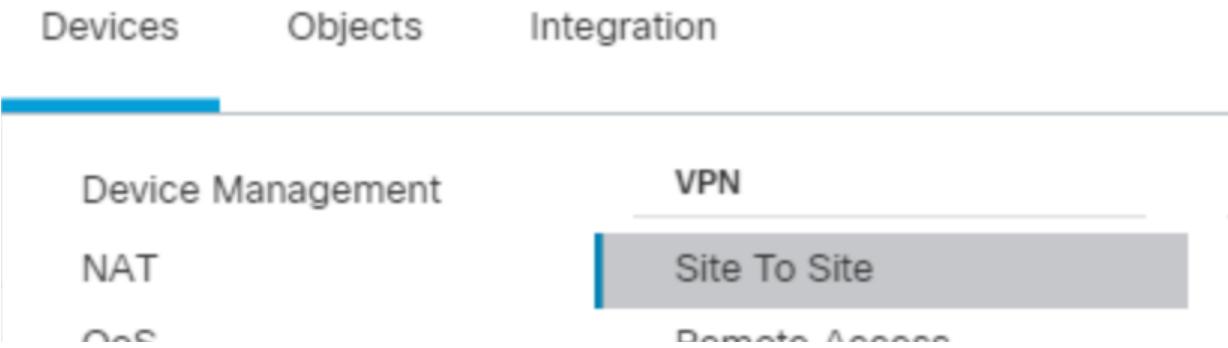
You have unsaved changes **Save** **Cancel**

**Note:** We can monitor the behavior by debugging the decisions using the CLI command `debug policy-route`

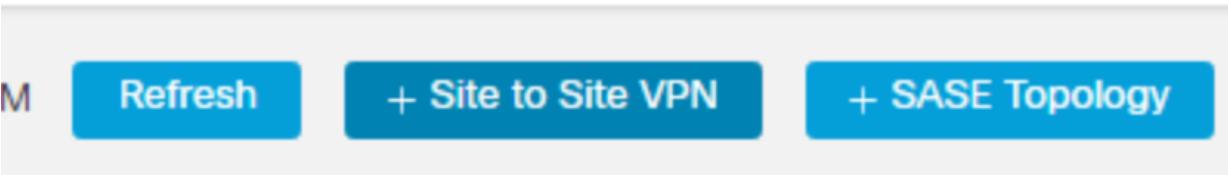
## SDWAN configuration

With all the previous steps having been completed, we are ready to configure SDWAN topologies.

1. Go to **Devices > Site to Site** menu



2. Click on **Site to Site VPN** button



## SDWAN Topology 1

1. Type a **topology name**, select **Route Based VTI** and then select **Hub and Spoke** network topology
2. The topology name is important to remind us which Topology we are working with, in this case, the HUB DVTI will be using **outside** interface and **Loop10**

## Create New VPN Topology

Topology Name:\*

SDWAN1-DVTI-outside-Loop10

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

Point to Point

**Hub and Spoke**

Full Mesh

IKE Version:\*

IKEv1  IKEv2

3. Under **Endpoints** tab, click the + (plus) sign to add **Hub nodes**
4. Now select the following:
  1. Device: **NGFW1**
  2. Dynamic Virtual Tunnel Interface (DVTI): **DVTI\_outside\_Loop10**
  3. Tunnel Source: **Giga0/0 (outside)**
  4. IP address: 198.18.133.81
  5. Click **Advanced Settings**
    - Check the option **Send Virtual Tunnel Interface IP to the peers**

6. Click **Ok**

## Add Endpoint



Device:\*

NGFW1



Dynamic Virtual Tunnel Interface

DVTI\_outside\_Loop10



Tunnel Source:\*

GigabitEthernet0/0 (outside)



198.18.133.81



Tunnel Source IP is Private

[Edit VTI](#)

Additional  
Configuration



Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

[▼ Advanced Settings](#)

Send Virtual Tunnel Interface IP to the peers

5. Click on the + (plus) sign to add **Spoke Nodes**

6. Select the following:

1. Device: **branch1**

2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside\_gi3\_40\_Loop10**

3. Click **Ok**

## Add Endpoint



Device:\*

branch1



Static Virtual Tunnel Interface

SVTI\_outside\_gi3\_40\_Loop10



Tunnel Source: outside\_gi3\_40 (IP: 198.60.62.100) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

7. Click on the + (plus) sign again to add **Spoke Nodes**

8. Select the following:

1. Device: **branch2**

2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside\_gi3\_40\_Loop10**

3. Click **Ok**

## Add Endpoint



Device:\*

branch2



Static Virtual Tunnel Interface

SVTI\_outside\_gi3\_40\_Loop10



Tunnel Source: outside\_gi3\_40 (IP: 198.60.40.100) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

9. Click on the + (plus) sign again to add **Spoke Nodes**

10. Select the following:

1. Device: **branch3**

2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside20\_Loop10**

### 3. Click Ok

## Add Endpoint



Device:\*

branch3



Static Virtual Tunnel Interface

SVTI\_outside20\_Loop10



Tunnel Source: outside\_20 (IP: 198.60.64.100)

[Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

### 11. Under IKE tab, change Authentication Type to Pre-shared Manual Key

- Type and confirm the key: C1sco12345

### 12. Click Save

## SDWAN1 - Overall configuration

[Edit VPN Topology](#)



Topology Name:\*

SDWAN1-DVTI-outside-Loop10

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

[Point to Point](#) [Hub and Spoke](#) [Full Mesh](#)

IKE Version:\*

IKEv1  IKEv2

[Endpoints](#) [IKE](#) [IPsec](#) [Advanced](#)

Hub Nodes:



Device Name	VPN Interface	Traffic Match Criteria	
FTD NGFW1	DVTI_outside_Loop10 (169.254.100.1)	Routing Policy	

Spoke Nodes:



Device Name	VPN Interface	Traffic Match Criteria	
FTD branch1	SVTI_outside_gi3_4... (169.254.100.6)	Routing Policy	
FTD branch2	SVTI_outside_gi3_4... (169.254.100.2)	Routing Policy	
FTD branch3	SVTI_outside20_Loo... (169.254.100.3)	Routing Policy	

## SDWAN Topology 2

1. Type a **topology name**, select **Route Based VTI** and then select **Hub and Spoke** network topology
2. The topology name is important to remind us which Topology we are working with, in this case, the HUB DVTI will be using **in10** interface and **Loop11**

## Create New VPN Topology

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*

IKEv1  IKEv2

3. Under **Endpoints** tab, click the + (plus) sign to add **Hub nodes**
4. Now select the following:
  1. Device: **NGFW1**
  2. Dynamic Virtual Tunnel Interface (DVTI): **DVTI\_in10\_Loop11**
  3. Tunnel Source: **Giga0/1 (in10)**
  4. IP address: 198.19.10.1
  5. Click **Advanced Settings**
    - Check the option **Send Virtual Tunnel Interface IP to the peers**

6. Click **Ok**

## Add Endpoint



Device:\*

NGFW1



Dynamic Virtual Tunnel Interface

DVTI\_in10\_Loop11



Tunnel Source:\*

GigabitEthernet0/1 (in10)



198.19.10.1



Tunnel Source IP is Private

[Edit VTI](#)

Additional Configuration i

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

▼ Advanced Settings

Send Virtual Tunnel Interface IP to the peers

5. Click on the + (plus) sign to add **Spoke Nodes**

6. Select the following:

1. Device: **branch1**

2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside\_gi4\_30\_Loop11**

3. Click **Ok**

## Add Endpoint



Device:\*

branch1



Static Virtual Tunnel Interface

SVTI\_outside\_gi4\_30\_Loop11



Tunnel Source: outside\_gi4\_30 (IP:  
198.60.162.100)

[Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

7. Click on the + (plus) sign again to add **Spoke Nodes**

8. Select the following:

1. Device: **branch2**

2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside\_gi4\_50\_Loop11**

3. Click **Ok**

## Add Endpoint



Device:\*

branch2



Static Virtual Tunnel Interface

SVTI\_outside\_gi4\_50\_Loop11



Tunnel Source: outside\_gi4\_50 (IP: 198.60.50.100) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

9. Click on the + (plus) sign again to add **Spoke Nodes**

10. Select the following:

1. Device: **branch3**
2. Static Virtual Tunnel Interface (SVTI): **SVTI\_outside20\_Loop11**
3. Click **Ok**

## Add Endpoint



Device:\*

branch3



Static Virtual Tunnel Interface

SVTI\_outside20\_Loop11 (IP: 169.254.1.1) +

Tunnel Source: outside\_20 (IP: 198.60.64.100)

Edit VTI

Tunnel Source IP is Private

Send Local Identity to Peers

11. Under **IKE** tab, change **Authentication Type** to **Pre-shared Manual Key**

- Type and confirm the key: C1sco12345

12. Click **Save**

## SDWAN2 - Overall configuration

Edit VPN Topology

Topology Name:\*

Policy Based (Crypto Map)    Route Based (VTI)

Network Topology:

Point to Point   **Hub and Spoke**   Full Mesh

IKE Version:\*

IKEv1    IKEv2

Endpoints   IKE   IPsec   Advanced

Hub Nodes: +

Device Name	VPN Interface	Traffic Match Criteria	
FTD NGFW1	DVTI_in10_Loop11 (169.254.100.9)	Routing Policy	

Spoke Nodes: +

Device Name	VPN Interface	Traffic Match Criteria	
FTD branch1	SVTI_outside_gi4_... (169.254.100.14)	Routing Policy	
FTD branch2	SVTI_outside_gi4_... (169.254.100.10)	Routing Policy	
FTD branch3	SVTI_outside20_Lo... (169.254.100.11)	Routing Policy	

## Deploy and Validation

### Deploy

1. Deploy the configuration to all devices
2. Click **Deploy** at the top right hand side

Deploy



3. Click **Ignore Warnings** and click **Deploy All**



Advanced Deploy

Ignore warnings

**Deploy All**

<input type="checkbox"/> branch1	Ready for Deployment
<input type="checkbox"/> branch2	Ready for Deployment
<input type="checkbox"/> branch3	Ready for Deployment
<input type="checkbox"/> NGFW1	Ready for Deployment

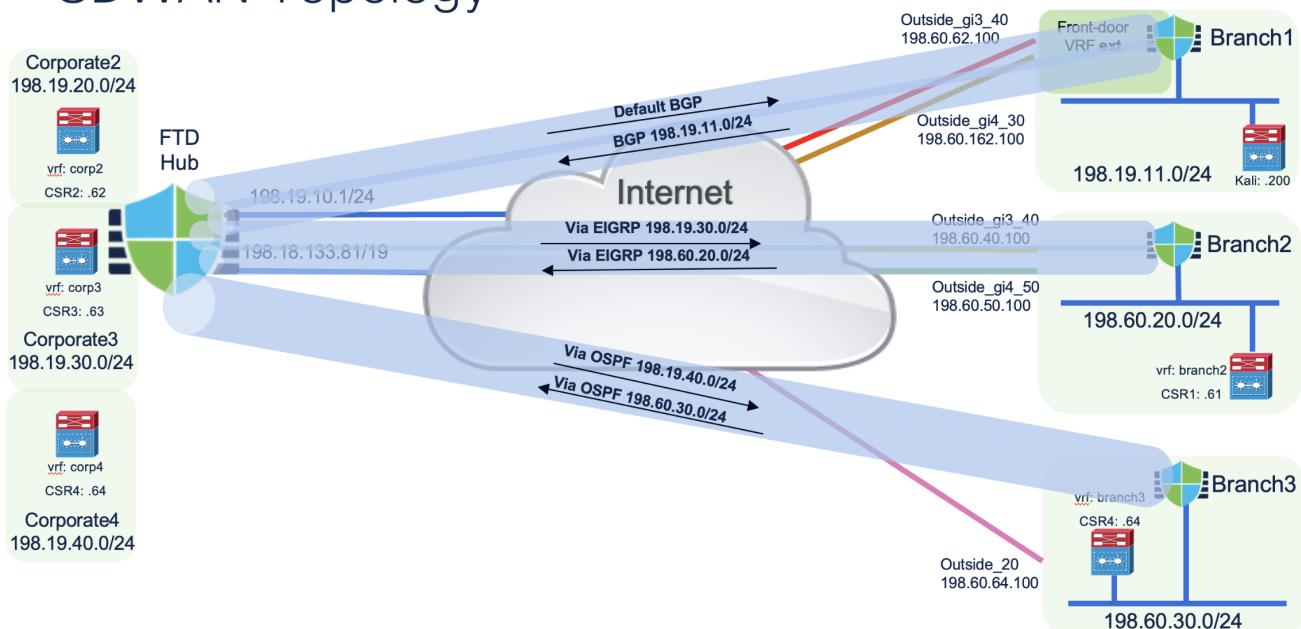
#### 4. Wait to see whether the deploy was completed

	Advanced Deploy	<input checked="" type="checkbox"/> Ignore warnings	Deploy All
branch1		Completed	
branch2		Completed	
branch3		Completed	
NGFW1		Completed	

## Validation

Tests are based on this topology

SDWAN Topology



### 1. Open Putty and SSH to the following IPs

1. HUB (NGFW1): 198.19.10.81
  - username: admin / password: C1sco12345
2. Branch1: 198.18.133.42
  - username: admin / password: C1sco12345
3. Branch2: 198.19.10.82
  - username: admin / password: C1sco12345
4. Branch3: 198.19.10.83
  - username: admin / password: C1sco12345

## Validating Branch3 connections

1. Inside HUB (NGFW1) and Branch3, type the command `show route ospf` to see which routes have been advertised

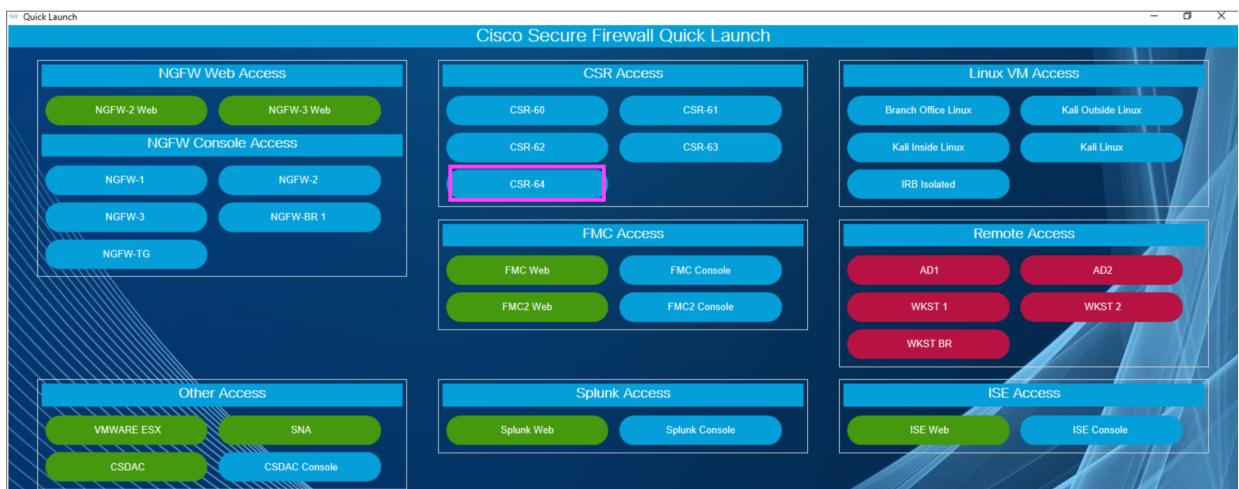
## 2. HUB (NGFW1)

```
o      198.60.30.0 255.255.255.0 [110/1572] via 169.254.100.11, 01:07:00  
|          [110/1572] via 169.254.100.3, 01:06:47, DVTI_in10_Loop11_va49
```

## 3. Branch3

```
o      169.254.100.1 255.255.255.255  
|          [110/1563] via 169.254.100.9, 01:04:53, SVTI_outside20_Loop11  
|          [110/1563] via 169.254.100.9, 01:04:53, SVTI_outside20_Loop10  
o      198.19.40.0 255.255.255.0  
|          [110/1572] via 169.254.100.9, 00:00:00, SVTI_outside20_Loop11  
|          [110/1572] via 169.254.100.9, 00:00:00, SVTI_outside20_Loop10
```

## 4. Open Quick Launch and click CSR-64 (topology reference as CSR4)



5. Type the command `debug ip icmp` to see the ICMP messages

6. Now type the command `ping vrf branch3 198.19.40.64` to test connectivity from Branch3 to Corporate4. Follow output from ping from 198.60.30.64 to 198.19.40.64

```
csr64#  
*Apr  3 03:50:18.679: ICMP: echo reply rcvd, src 198.19.40.64, dst 198.60.30.64,  
topology BASE, dscp 0 topoid 1  
*Apr  3 03:50:18.683: ICMP: echo reply rcvd, src 198.19.40.64, dst 198.60.30.64,  
topology BASE, dscp 0 topoid 1  
*Apr  3 03:50:18.702: ICMP: echo reply rcvd, src 198.19.40.64, dst 198.60.30.64,  
topology BASE, dscp 0 topoid 1  
*Apr  3 03:50:18.729: ICMP: echo reply rcvd, src 198.19.40.64, dst 198.60.30.64,  
topology BASE, dscp 0 topoid 1  
*Apr  3 03:50:18.756: ICMP: echo reply rcvd, src 198.19.40.64, dst 198.60.30.64,  
topology BASE, dscp 0 topoid 1
```

## Validating Branch2 connections

Inside HUB (NGFW1) and Branch2, type the command `show route ospf` to see which routes have been advertised

## 2. HUB (NGFW1)

```
D      198.60.20.0 255.255.255.0  
|          [90/28416] via 169.254.100.2, 00:14:36, DVTI_outside_Loop10_va47
```

### 3. Branch2

```
D      198.19.30.0 255.255.255.0
      [90/28416] via 169.254.100.9, 00:00:03, SVTI_outside_gi4_50_Loop11
      [90/28416] via 169.254.100.1, 00:00:03, SVTI_outside_gi3_40_Loop10
```

### 4. Open Quick Launch and click CSR-61 (topology references as CSR1)



5. Type the command **debug ip icmp** to see the ICMP messages

6. Now type the command **ping vrf branch2 198.19.30.63** to test connectivity from Branch2 to Corporate3. Follow the output of ping from 198.60.20.61 to 198.19.30.63

```
*Apr  3 03:56:18.823: ICMP: echo reply rcvd, src 198.19.30.63, dst 198.60.20.61,
 topology BASE, dscp 0 topoid 1
*Apr  3 03:56:18.827: ICMP: echo reply rcvd, src 198.19.30.63, dst 198.60.20.61,
 topology BASE, dscp 0 topoid 1
*Apr  3 03:56:18.838: ICMP: echo reply rcvd, src 198.19.30.63, dst 198.60.20.61,
 topology BASE, dscp 0 topoid 1
*Apr  3 03:56:18.868: ICMP: echo reply rcvd, src 198.19.30.63, dst 198.60.20.61,
 topology BASE, dscp 0 topoid 1
*Apr  3 03:56:18.896: ICMP: echo reply rcvd, src 198.19.30.63, dst 198.60.20.61,
 topology BASE, dscp 0 topoid 1
```

## Validating Branch1 connections

Inside HUB (NGFW1) and Branch1, type the command **show route bgp** to see which routes have been advertised

### 2. HUB (NGFW1)

```
B      198.19.11.0 255.255.255.0 [200/0] via 169.254.100.14, 01:17:32
      [200/0] via 169.254.100.6, 01:17:32
```

### 3. Branch1

```
B*      0.0.0.0 0.0.0.0 [200/0] via 169.254.100.9, 01:17:56
      [200/0] via 169.254.100.1, 01:17:56
```

### 4. Open Quick Launch and click Kali Inside Linux (topology references as Kali)



- Now type the command **ping 198.19.20.62** to test connectivity from Branch1 to Corporate2. Follow the output of ping from 198.19.11.200 to 198.19.20.62

```
[root@branch ~]# ping 198.19.20.62
PING 198.19.20.62 (198.19.20.62) 56(84) bytes of data.
64 bytes from 198.19.20.62: icmp_seq=1 ttl=255 time=5.25 ms
64 bytes from 198.19.20.62: icmp_seq=2 ttl=255 time=4.37 ms
^C
```

- SSH into branch1 (198.18.133.42 / admin / C1sco12345), type the command **debug policy-route** to see the PBR being hit and steering the traffic to the local exit ISP.
- Testing Path Monitoring, DIA and PBR by pinging one or all of the following domains from **Branch Office Linux**.

```
ping facebook.com
ping instagram.com
ping linkedin.com
```

- Output from Branch Office Linux after a ping

```
[root@branch ~]# ping facebook.com
PING facebook.com (31.13.80.36) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-yyz1.facebook.com
(31.13.80.36): icmp_seq=1
```

- Output from branch1 debug command

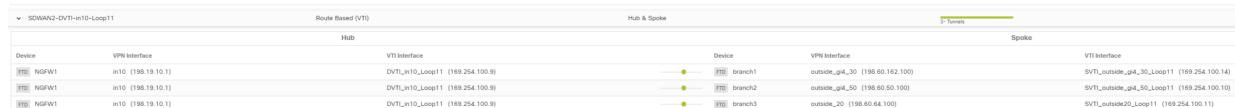
```
pbr: route map FMC_GENERATED_PBR_1711935212670, sequence 5, permit; proceed with
    policy routing
pbr : PBR Using Default DP Table for forwarding for dest addr 31.13.80.36
pbr: Ingress ifc inside, PBR adaptive traffic forward for dest 31.13.80.36, egress
    ifc outside_gi4_30 nh 198.60.162.1
pbr: policy based routing applied; egress_ifc = outside_gi4_30 : next_hop = 198.
    60.162.1
```

# SDWAN and WAN status/summary

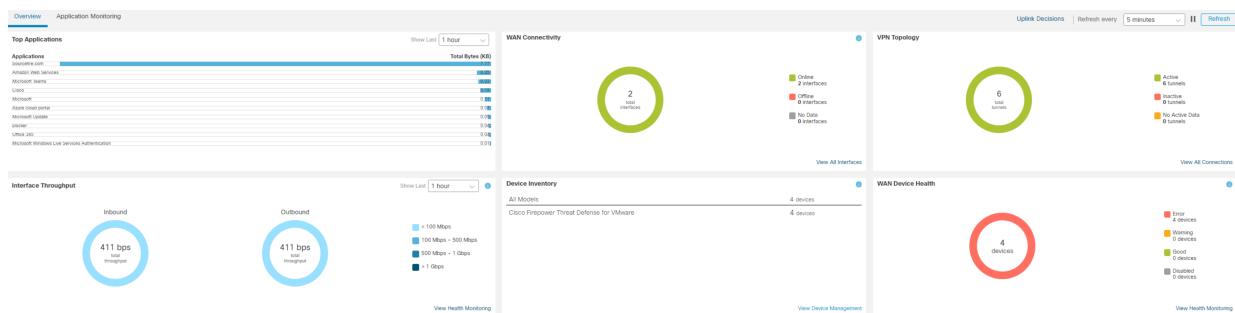
1. Go to **Devices > Site to Site VPN** and expand the two SDWANs topology we created earlier. They should be green with 3 tunnels UP
2. SDWAN1 using HUB DVTI Loop10



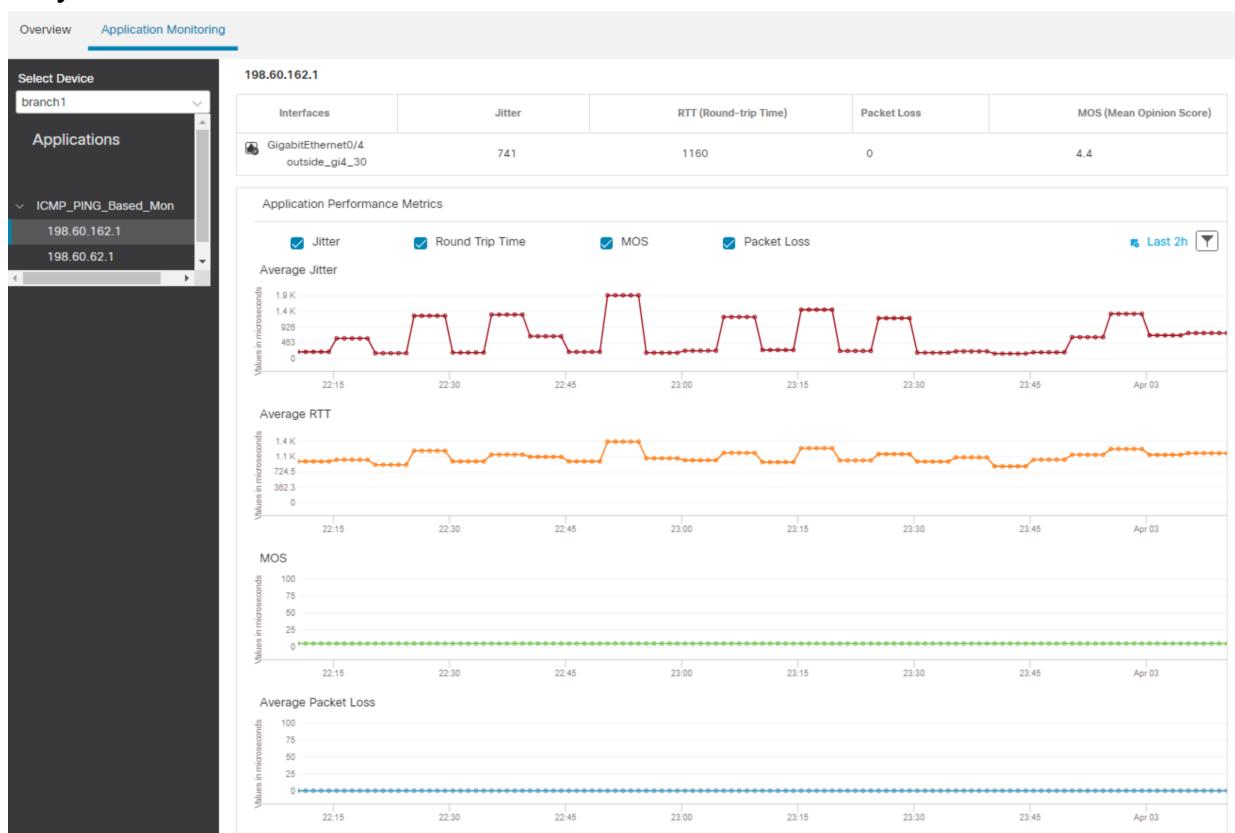
3. SDWAN2 using HUB DVTI Loop11



4. Go to **Overview > SD-WAN Summary**. Overview tab will show some stats about SDWAN health



5. Also at the SD-WAN Summary, click on **Application Monitoring** tab. It will show you the stats of the interfaces we enabled **Path Monitoring** which was only on branch1



## 6. Go to Overview > Site to Site VPN

Tunnel Summary	Node A	Node B	Topology	Status	Last Updated
 100% Active 6 connections	NGFW1 (VPN IP: 198.18.133.81)	branch1 (VPN IP: 198.60.62.100)	SDWAN1-DVTI-outside-Loop10	<span>Active</span>	2024-04-02 22:27:32
	NGFW1 (VPN IP: 198.18.10.1)	branch1 (VPN IP: 198.60.62.100)	SDWAN2-DVTI-in10-Loop11	<span>Active</span>	2024-04-02 22:27:45
	NGFW1 (VPN IP: 198.18.133.81)	branch2 (VPN IP: 198.60.64.100)	SDWAN1-DVTI-outside-Loop10	<span>Active</span>	2024-04-02 22:41:36
	NGFW1 (VPN IP: 198.18.10.1)	branch3 (VPN IP: 198.60.64.100)	SDWAN2-DVTI-in10-Loop11	<span>Active</span>	2024-04-02 22:41:36
	NGFW1 (VPN IP: 198.18.133.81)	branch2 (VPN IP: 198.60.40.100)	SDWAN1-DVTI-outside-Loop10	<span>Active</span>	2024-04-02 22:55:59
	NGFW1 (VPN IP: 198.18.10.1)	branch2 (VPN IP: 198.60.50.100)	SDWAN2-DVTI-in10-Loop11	<span>Active</span>	2024-04-02 22:55:59