

Azure Virtual WAN - VPN site-to-site - Check Point with BGP.



About this guide

This guide will describe the full setup configuration of a Azure Virtual WAN in two Regions South / West establishing a full resilience site-to-site VPN .

The scope is based on site-to-site VPN between Azure Virtual WAN and a TWO on premises Check Point clusters.

Introduction

The Azure hub-and-spoke connectivity model has been adopted by thousands of our customers to leverage the default transitive routing behavior of Azure Networking in order to build simple and scalable cloud networks. Azure Virtual WAN builds on these concepts and introduces new capabilities that allow global connectivity topologies, not only between on-premises locations and Azure, but also allowing customers to leverage the scale of the Microsoft network to augment their existing global networks.

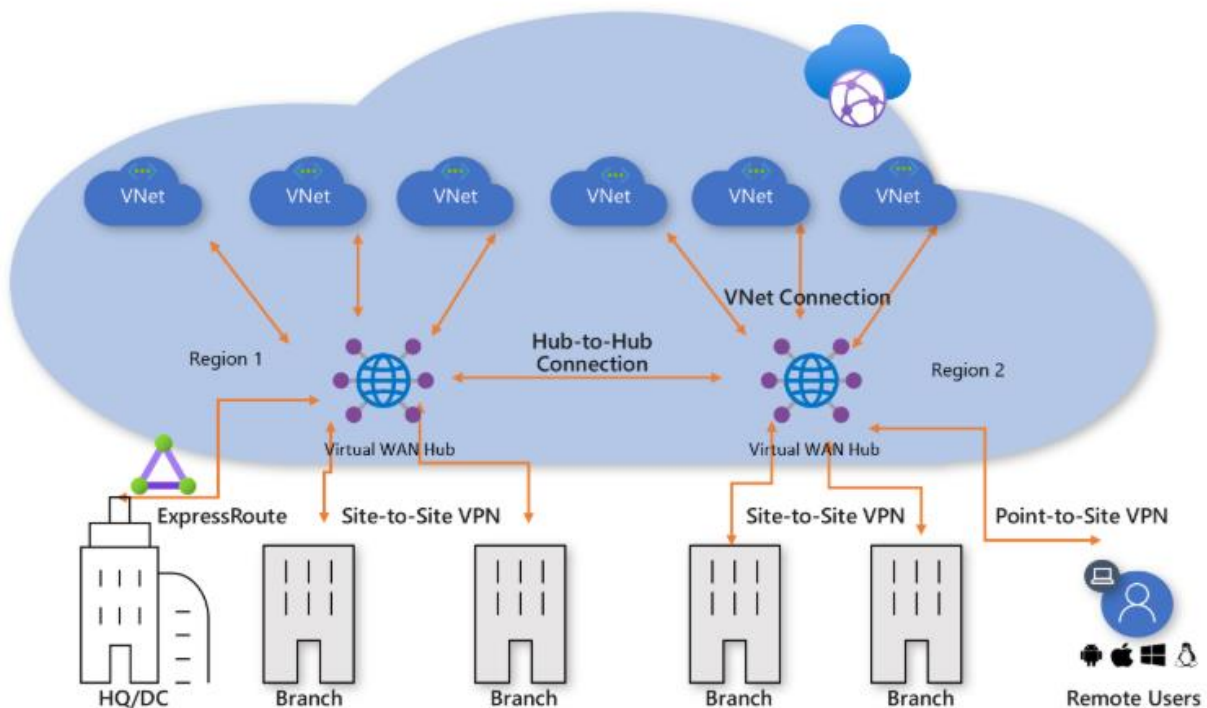
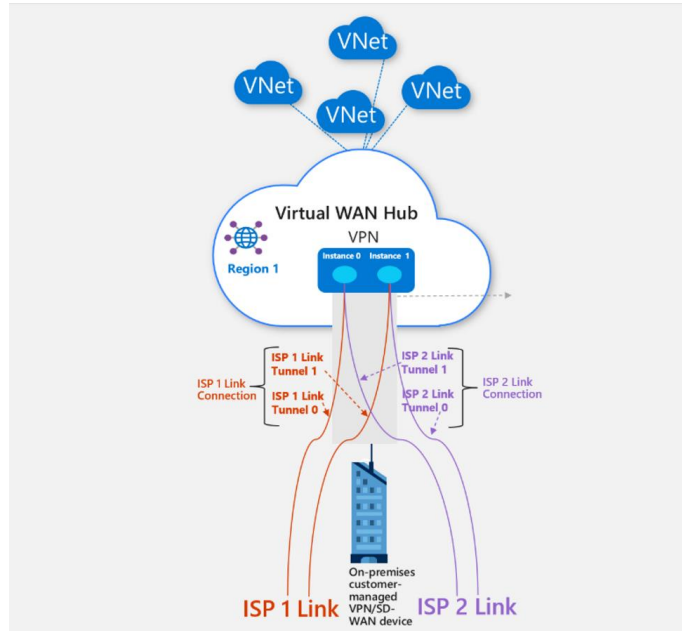


Table of Contents

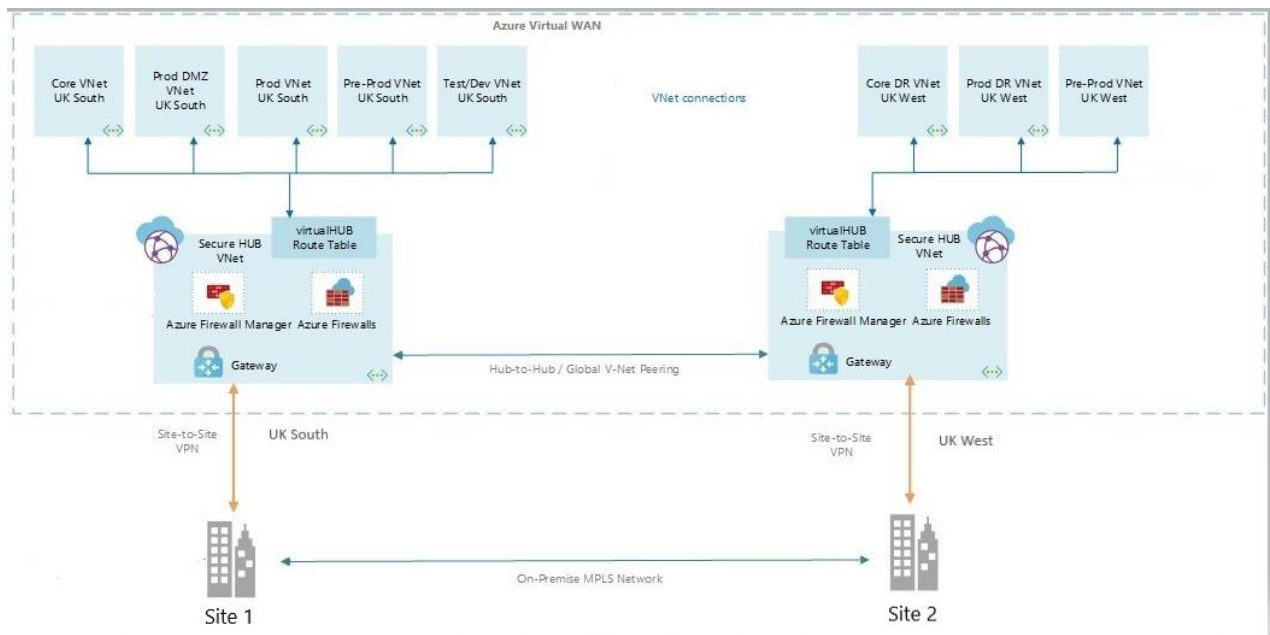
1.	Overview	3
2.	General configuration	4
3.	Azure Virtual WAN configuration.....	5
3.1.	Hub creation for UK-South	5
3.2.	Attach VNET(s) to hub	6
3.3.	VPN configuration in hub	7
3.4.	VPN site-to-site	8
3.5.	Link configuration.....	9
3.6.	Hub creation for UK-West	10
3.7.	Download the VPN configuration	11
3.8.	Logical VPN schema	12
4.	Check Point VPN configuration	13
4.1.	The Interface configuration on the Check Point cluster site 1	13
4.2.	The Interface configuration on the Check Point cluster site 2	13
4.3.	Interoperable devices	13
4.4.	Pre-shared key	14
4.5.	Wire mode.....	14
5.	BGP configuration	15
5.1.	BGP peering from Site 1	15
5.1.1.	BGP peering to South	15
5.1.2.	BGP peering to West	15
5.2.	BGP peering from Site 2	16
5.2.1.	BGP peering to South	16
5.2.2.	BGP peering to West	16
5.3.	Routemaps	17
5.3.1.	Routemap to import Azure routes	17
5.3.2.	Routemap to export on-premises routes to Azure	18
5.3.3.	Routemap redistribute Azure routes into on-premises OSPF backbone	19

1. Overview

The scope is based on providing a full resilience through multiple VPN site-to-site from on-premises to Azure Virtual WAN. In our setup Azure Virtual Wan is based in two geographic regions, "UK South" and "UK West"; We will make use of two hubs, one in each region and each hub does contain two instances.

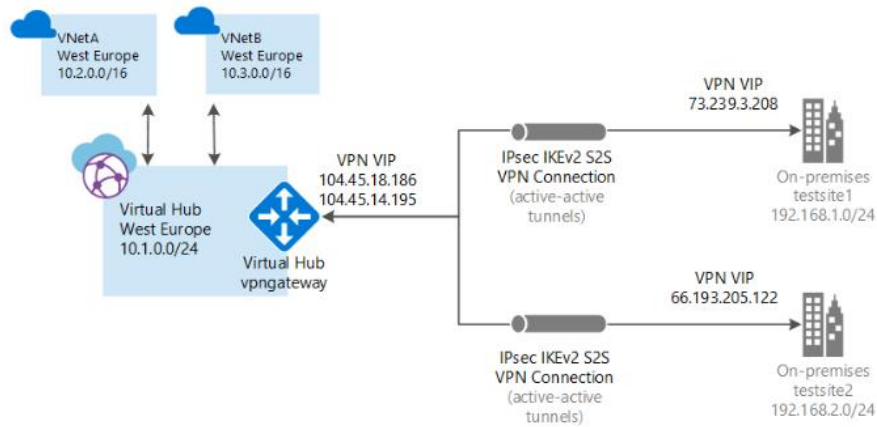


We have two datacenters with Check Point firewall clusters. Each cluster will have VPN connectivity to each region "UK South" and "UK West" to provide resiliency.



Both Datacenter interconnect via an internal MPLS backbone and runs as dynamic protocol OSPF inside their flat network.

We will use BGP inside our VPN tunnels in order to exchange routes between on-premises and Azure Vnets.

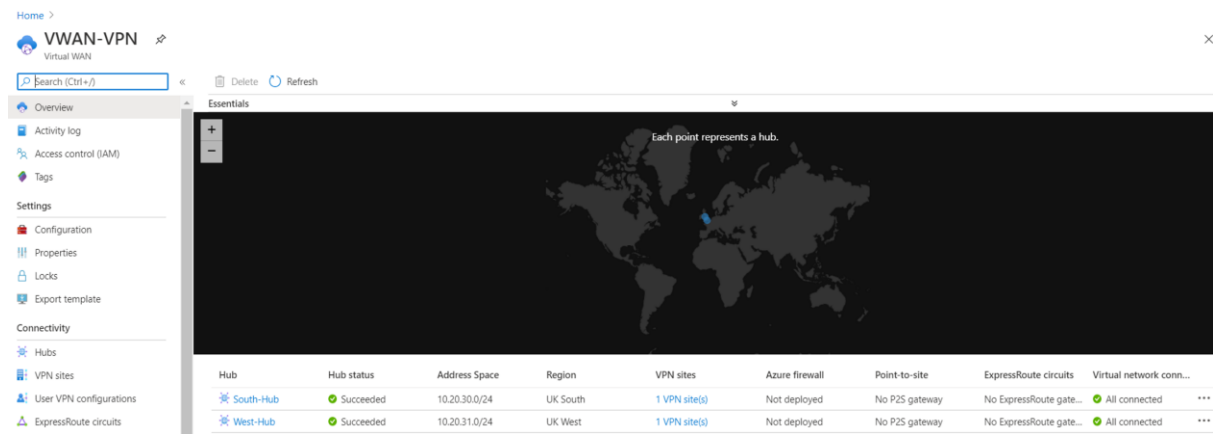


2. General configuration

- Azure Virtual WAN in two regions “UK South” and “UK West”.
- The Check Point Firewall are running R80.30 build 200 on-premises.
- OSPF is running inside the datacenters.
- BGP will be used to exchange routes from Azure Vnet and subnets and on-premises network.

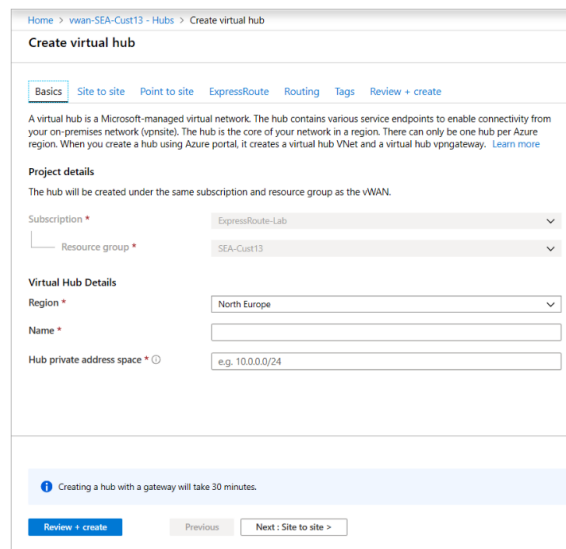
3. Azure Virtual WAN configuration

The Azure Virtual WAN configuration will be deployed in EMEA. To provide High availability we used two regions and therefore we made two hubs, “UK South” and “UK West”. The two small dots in the screenshot located the Virtual Wan regions.



3.1. Hub creation for UK-South

A hub is a virtual network that can contain gateways for site-to-site, ExpressRoute, or point-to-site functionality. It takes 30 minutes to create the site-to-site VPN gateway in the virtual hub.

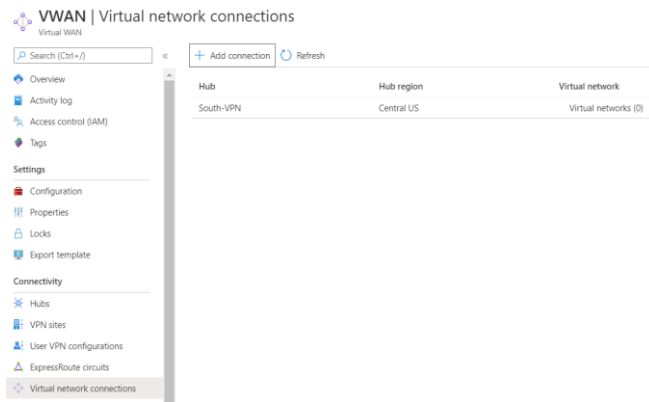


I created a new resource-group “RG-South” and use for the **Region** = UK South, Hub Private space = 10.20.30.0/24. And another resource-group “RG-West” and use for the **Region** = UK West, Hub Private space = 10.20.31.0/24.

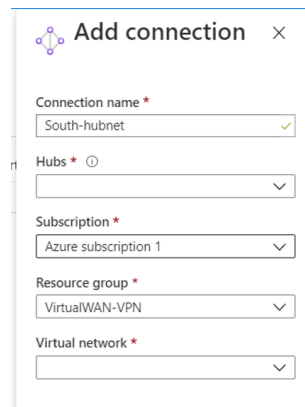
NOTE: Hub private address space. The minimum address space is /24 to create a hub, which implies anything range from /25 to /32 will produce an error during creation.

3.2. Attach VNET(s) to hub

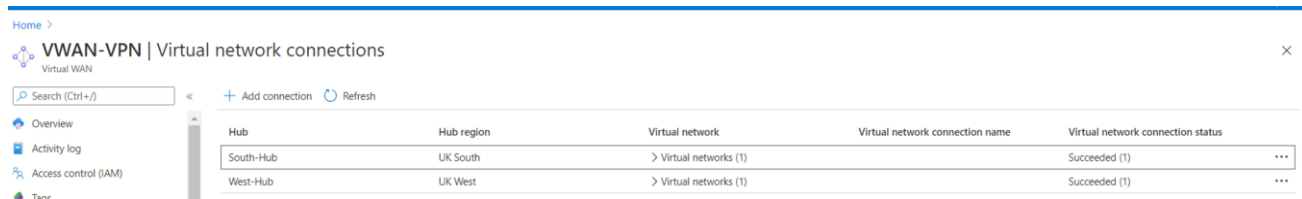
Go to your Virtual WAN configuration



Select "Virtual network connections"



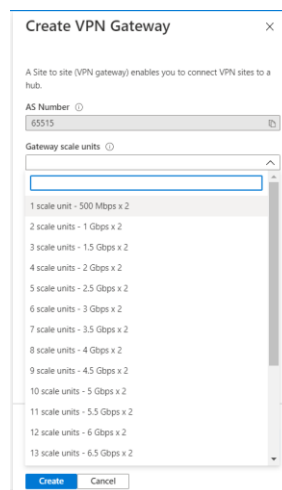
Select your resource group and attach it to your VNET.



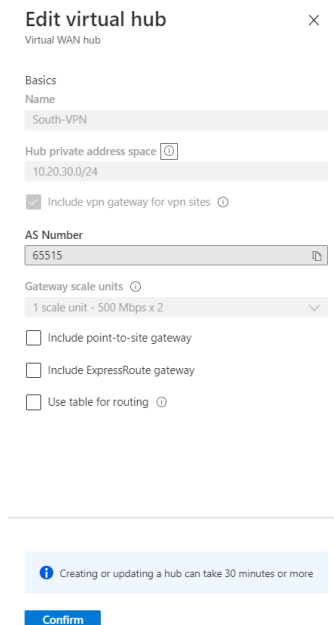
3.3. VPN configuration in hub

Select the hub where you would attach the VPN connections. You can create up to 1000 sites per Virtual Hub in a Virtual WAN. If you had multiple hubs, you can create 1000 per each of those hubs.

First we have to create a VPN Gateway for the VPN site-to-site connections, the BGP AS number on Azure Virtual WAN is per default “65515” and the scale units give you a broad choice of throughput.

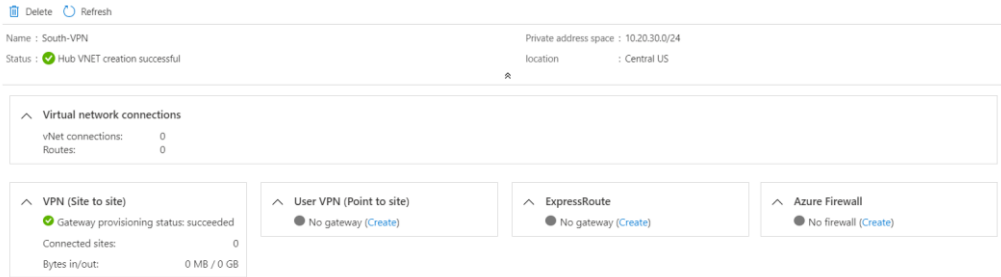


When the VPN gateway is created, you add also other connectivity such as Express route, Point-to-site or routing.

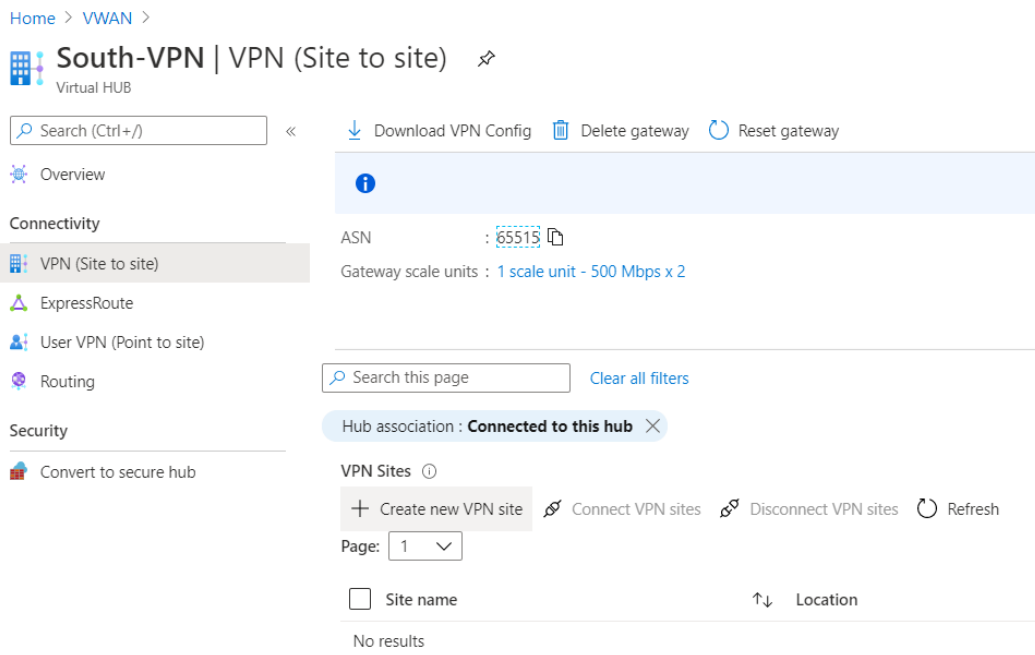


3.4. VPN site-to-site

You will have in the general view, the Hub is created successful and the VPN Gateway provisioned.



From here you select the VPN site you want to add to the hub.

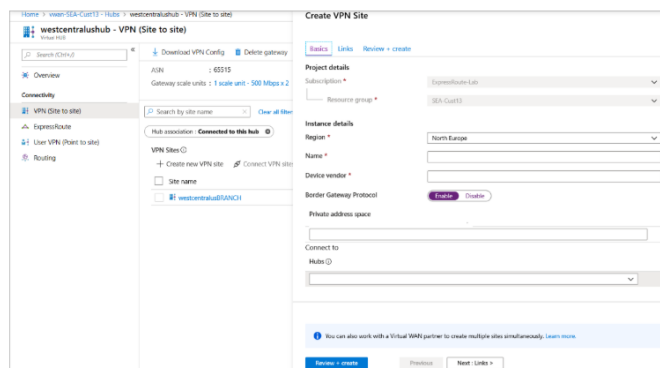


Select "Create new VPN site"

Fill in the following fields,

The inputs are **Region** = Uk South, **Device Vendor** = Check Point, **BGP** = enabled and select **Hub** = UK-South.

Private address space - The IP address space that is located on your on-premises site. Traffic destined for this address space is routed to your local site. This is required when BGP is not enabled for the site.



3.5. Link configuration

The “Links” we will create TWO links, one for Site1 and one for Site2.

Create VPN site

Link name * Provider name *

Speed * IP address *

BGP address * ASN *

Link name * Provider name *

Speed * IP address *

BGP address * ASN *

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

IP Address= Public IP address of the on-premises firewall using this link. Optionally, you can provide the private IP address of your on-premises VPN device that is behind ExpressRoute. If you add multiple Links you **can't use the same Public IP address for different links into the same VPN configuration.**

The BGP address for site 1 VTI interface will be “100.64.100.1” and ASN = 65530
 The BGP address for site 2 VTI interface will be “100.64.110.1” and ASN 65530.
 We use same BGP ASN on both Datacenters because it’s a stretched flat network.

For the “South-VPN” hub we have created following links, first link to Site1 with official IP 35.176.190.117, BGP peering IP address “100.64.100.1” and ASN 65530 and the second link to Site2 with official 3.10.11.219, BGP peering IP address “100.64.110.1 and ASN 65530.

In our example we choose 100Mb throughput.

Connected Hubs						
Hub name	Location			Connectivity status		
South-Hub	UK South			Connected		

Links						
Link name	Provider name	Speed	IP address	BGP address	ASN	
toGW1	Checkpoint	100 Mbps	35.176.190.117	100.64.100.1	65530	
toGW2	Checkpoint	100 Mbps	3.10.11.219	100.64.110.1	65530	

3.6. Hub creation for UK-West

The configuration is similar to the South-hub, except the BGP IP peer addresses changes.

Connected Hubs						
Hub name	Location			Connectivity status		
West-Hub	UK West			Not connected		

Links						
Link name	Provider name	Speed	IP address	BGP address	ASN	
toGW1	Checkpoint	100 Mbps	35.176.190.117	100.64.200.1	65530	
toGW2	Checkpoint	100 Mbps	3.10.11.219	100.64.210.1	65530	

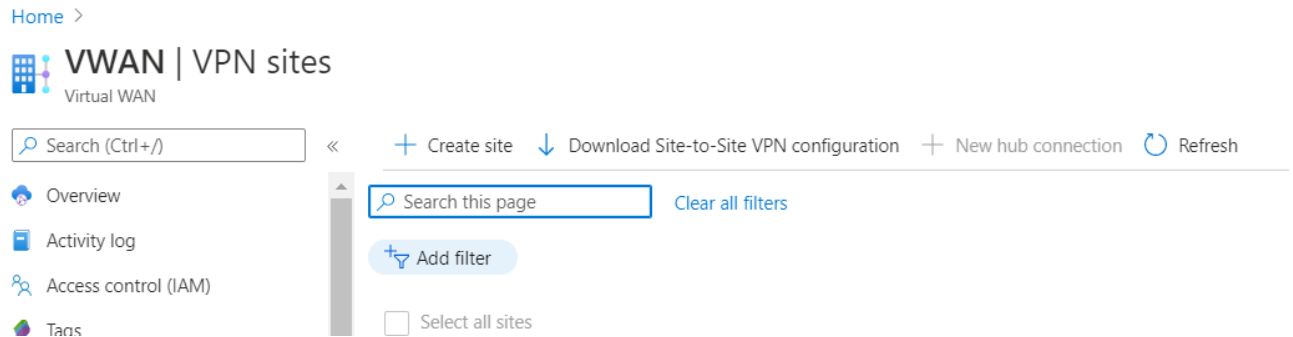
The BGP peering IP address is the IP address you will assign to your VTI interface in the Check Point firewall. The easiest way to add VTI is via the GAIA web portal. You can verify the VTI tunnel interfaces configuration through the clish.

```

gw-3bad44> show vpn tunnels
Interface: vpnt1
  Local IP: 100.64.100.1
  Peer Name: AZure-South_0
  Remote IP: 10.20.30.12
  Interface type: numbered
Interface: vpnt2
  Local IP: 100.64.200.1
  Peer Name: AZure-west_0
  Remote IP: 10.20.31.12
  Interface type: numbered
  
```

3.7. Download the VPN configuration

On the Azure portal of the hub, select “Download Site-to-Site VPN configuration”.



The output of the config file will give all the needed info about the local but also remote connectivity settings to complete into the Check Point on-premises firewalls.

Hereunder a sample of the output.

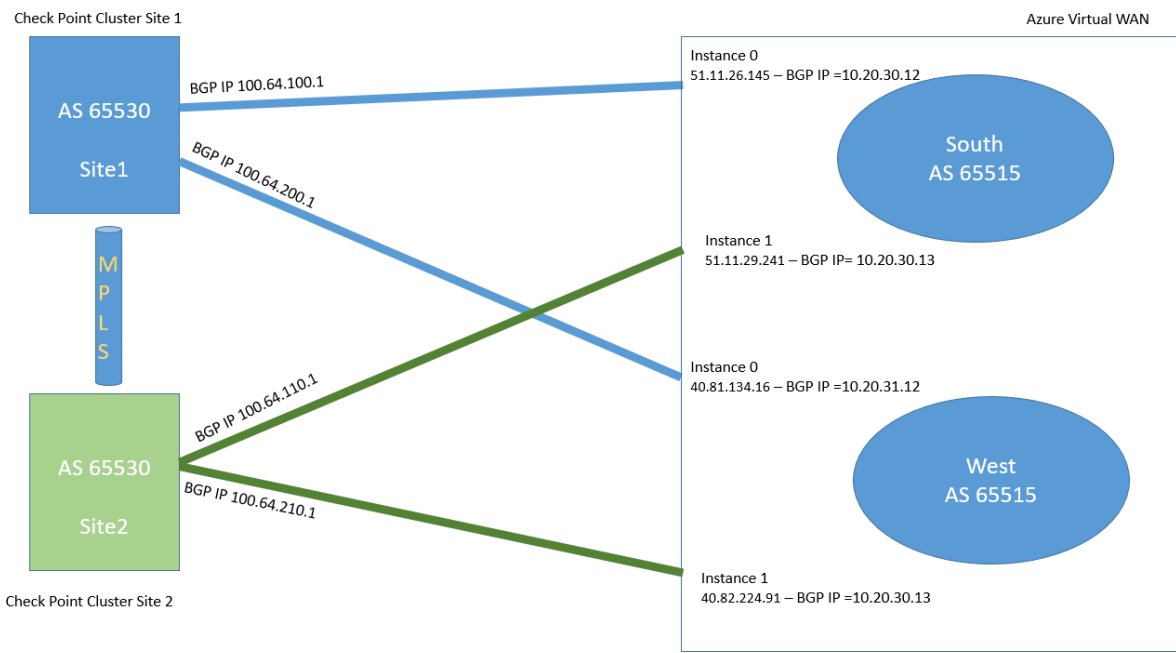
```
"configurationVersion": {
  "LastUpdatedTime": "2020-06-15T12:13:41.5925179Z",
  "Version": "e07b8b12-291a-4aef-af24-bf50ca6706e9"
},
"vpnSiteConfiguration": {
  "Name": "South-hub",
  "IPAddress": "65.25.223.2", IP address of Check Point cluster – Site1
  "BgpSetting": {
    "Asn": 65530, AS number – Site1
    "BgpPeeringAddress":
    "BgpPeeringAddresses": "100.64.100.1" BGP Peer 1, "100.64.110.1", BGP Peer 2
    "PeerWeight": 32768
  },
  "LinkName": "siteLink01"
},
"vpnSiteConnections": [
  {
    "hubConfiguration": {
      "AddressSpace": "10.20.30.0/24",
      "Region": "UK South",
      "ConnectedSubnets": [
        ]
      }
    }
  ]
}
```

```

},
"gatewayConfiguration": {
  "IpAddresses": {
    "Instance0": "52.16.26.145", Azure VWAN Official IP1
    "Instance1": "54.17.29.241" Azure VWAN Official IP2
  },
  "BgpSetting": {
    "Asn": 65515,
    "BgpPeeringAddresses": {
      "Instance0": "10.20.30.12", Azure VWAN BGP peer IP1
      "Instance1": "10.20.30.13" Azure VWAN BGP peer IP2
    },
    "PeerWeight": 0
  }
},
"connectionConfiguration": {
  "IsBgpEnabled": true,
  "PSK": " the preshared key between Azure South and Site1/site2 - VPN tunnel",
  "IPsecParameters": {
    "SADataSizeInKilobytes": 102400000,
    "SALifeTimeInSeconds": 3600
  }
}

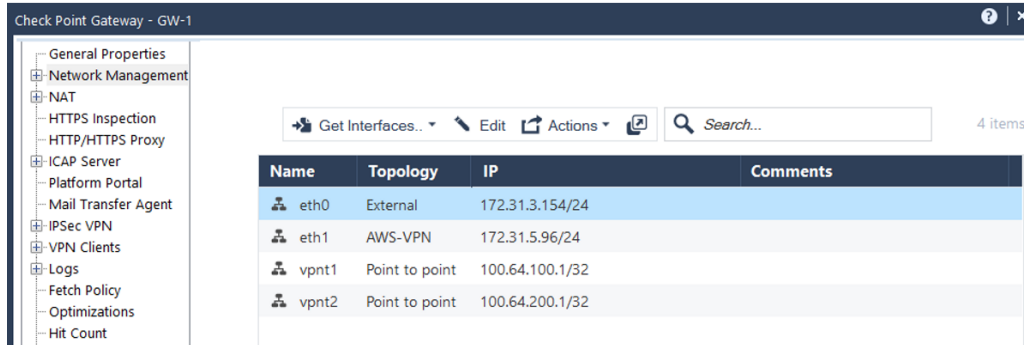
```

3.8. Logical VPN schema



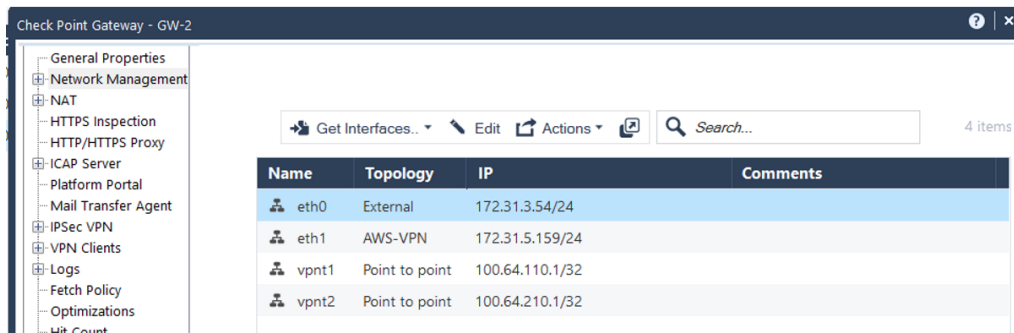
4. Check Point VPN configuration

4.1. The Interface configuration on the Check Point cluster site 1



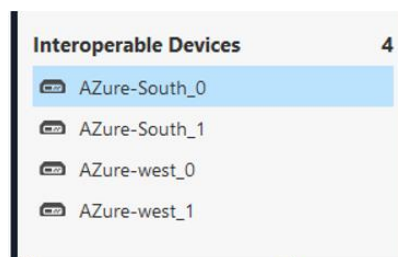
During the VPN tunnel interface creation, it's important to assign the right "interoperable device" name that will connect with that VPN tunnel.

4.2. The Interface configuration on the Check Point cluster site 2



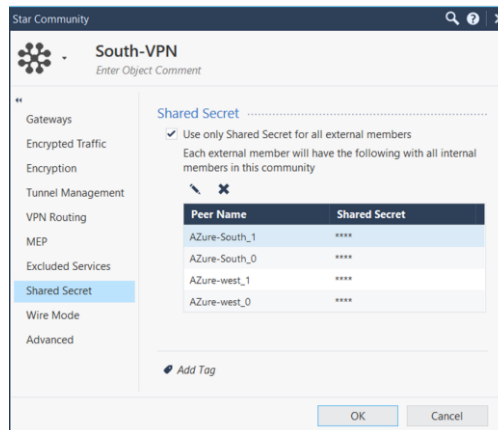
4.3. Interoperable devices

I created 4 interoperable devices, with the IP address information and Pre-shared key in the configuration output downloaded from the Azure Vwan hub and VPN sites.



4.4. Pre-shared key

As with the IP addresses settings, you can find the Azure generated pre-shared key in vpn config file.

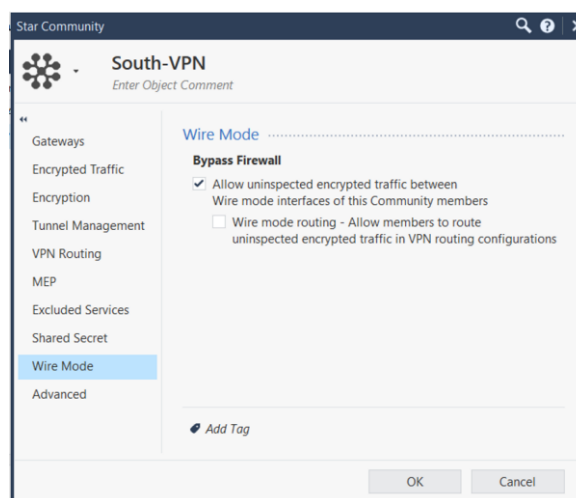


4.5. Wire mode

Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Statefull Inspection. Since Statefull Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

Wire Mode highlights include the following:

- **Improves performance**
- **Reduces downtime**
- **Supports dynamic-routing protocols** Maintains a private and secure VPN session, without employing Stateful Inspection



5. BGP configuration

First part of the process is to verify we have a peering establish between Check Point firewall and Azure Virtual Wan via the IPSEC tunnel interface.

5.1. BGP peering from Site 1

5.1.1. BGP peering to South

We will configure this through “clish” into the firewall of Site 1

```
> set as 65530
> set router-id "0.119.0.5"
> set bgp external remote-as 65515 on
> set bgp external remote-as 65515 peer 172.30.0.12 on
> set bgp external remote-as 65515 peer 172.30.0.12 graceful-restart on
> set bgp external remote-as 65515 peer 172.30.0.12 ip-reachability-detection on
> set bgp external remote-as 65515 peer 172.30.0.12 ip-reachability-detection check-control-plane-failure on
```

5.1.2. BGP peering to West

```
> set as 65530
> set router-id "0.119.0.5"
> set bgp external remote-as 65515 on
> set bgp external remote-as 65515 peer 172.30.1.12 on
> set bgp external remote-as 65515 peer 172.30.1.12 graceful-restart on
> set bgp external remote-as 65515 peer 172.30.1.12 ip-reachability-detection on
> set bgp external remote-as 65515 peer 172.30.1.12 ip-reachability-detection check-control-plane-failure on
```

```
gw-3bad44> show bgp peers
```

Flags: R - Peer restarted, W - Waiting for End-Of-RIB from Peer

PeerID	AS	Routes	ActRts	State	InUpds	OutUpds	Uptime
10.20.30.12	65515	6	1	Established	6	0	01:05:47
10.20.31.12	65515	6	1	Established	8	0	01:21:34

5.2. BGP peering from Site 2

5.2.1. BGP peering to South

We will configure this through “clish” into the firewall of Site 2

```
> set as 65530
> set router-id "0.119.0.35"
> set bgp external remote-as 65515 on
> set bgp external remote-as 65515 peer 172.30.0.13 on
> set bgp external remote-as 65515 peer 172.30.0.13 graceful-restart on
> set bgp external remote-as 65515 peer 172.30.0.13 ip-reachability-detection on
> set bgp external remote-as 65515 peer 172.30.0.13 ip-reachability-detection check-control-plane-failure on
```

5.2.2. BGP peering to West

```
> set as 65530
> set router-id "0.119.0.35"
> set bgp external remote-as 65515 on
> set bgp external remote-as 65515 peer 172.30.1.13 on
> set bgp external remote-as 65515 peer 172.30.1.13 graceful-restart on
> set bgp external remote-as 65515 peer 172.30.1.13 ip-reachability-detection on
> set bgp external remote-as 65515 peer 172.30.1.13 ip-reachability-detection check-control-plane-failure on
```

```
gw-23fe1e> show bgp peers
```

Flags: R - Peer restarted, W - Waiting for End-Of-RIB from Peer

PeerID	AS	Routes	ActRts	State	InUpds	OutUpds	Uptime
10.20.30.13	65515	6	1	Established	8	0	01:04:57
10.20.31.13	65515	6	1	Established	13	0	01:27:11

5.3. Routemaps

5.3.1. Routemap to import Azure routes

We will import the Azure Vnet 172.30.0.0/16 routes.

```
>set routemap im_azure id 10 on
```

```
>set routemap im_azure id 10 match network 172.30.0.0/16 all
```

Apply the routemap to your BGP configuration

- For Site 1

```
>set bgp external remote-as 65515 peer 10.20.30.12 import-routemap im_azure preference 10 on
```

```
>set bgp external remote-as 65515 peer 10.20.31.12 import-routemap im_azure preference 10 on
```

- For Site 2

```
>set bgp external remote-as 65515 peer 10.20.30.13 import-routemap im_azure preference 10 on
```

```
>set bgp external remote-as 65515 peer 10.20.31.13 import-routemap im_azure preference 10 on
```

This is an example of how the result in your routing table should resemble.

```
FW-2> show route bgp
Codes: C - Connected, S - Static, R - RIP, B - BGP (D - Default),
O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA),
A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed,
U - Unreachable, i - Inactive
B          172.30.1.0/24          via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.8.0/21         via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.16.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.24.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.32.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.40.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.48.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.56.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.64.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
B          172.30.72.0/21        via 172.30.1.12, vpnt3, cost None, age 424036
FW-2> █
```

5.3.2. Routemap to export on-premises routes to Azure

We will export OSPF network “158.119.0.0/16” towards Azure.

```
set routemap ex_azure id 10 on
set routemap ex_azure id 10 allow
set routemap ex_azure id 10 match protocol ospf2
set routemap ex_azure id 10 match network 158.119.0.0/16
```

To export “EX2_ospf” routes we did add this routemap

```
set routemap ex_azure id 20 on
set routemap ex_azure id 20 allow
set routemap ex_azure id 20 match protocol ospf2ase
set routemap ex_azure id 20 match network 158.119.0.0/16 all
```

Apply the routemap to your BGP configuration

- For Site 1

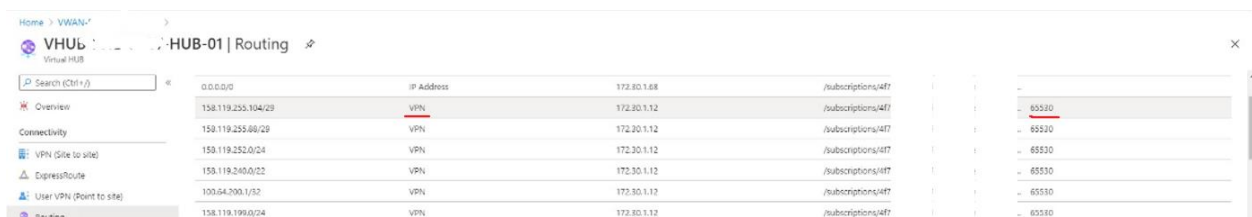
```
>set bgp external remote-as 65515 peer 10.20.30.12 export-routemap ex_azure preference 10 on
>set bgp external remote-as 65515 peer 10.20.31.12 export-routemap ex_azure preference 10 on
```

- For Site 2

```
>set bgp external remote-as 65515 peer 10.20.30.13 export-routemap ex_azure preference 10 on
>set bgp external remote-as 65515 peer 10.20.31.13 export-routemap ex_azure preference 10 on
```

When you check on South-hub or West-hub in the Routing tab, go to the Tab “effective routes”.

You will find the exported routes that are announced and routed through the “VPN” in Virtual Wan and remote AS 65530.



0.0.0.0/0	IP Address	172.80.1.68	/subscriptions/4f7			
158.119.255.104/29	VPN	172.80.1.12	/subscriptions/4f7			65530
150.119.255.88/29	VPN	172.30.1.12	/subscriptions/4f7			65530
150.119.252.0/24	VPN	172.30.1.12	/subscriptions/4f7			65530
150.119.240.0/22	VPN	172.30.1.12	/subscriptions/4f7			65530
100.64.200.1/32	VPN	172.30.1.12	/subscriptions/4f7			65530
158.119.198.0/24	VPN	172.80.1.12	/subscriptions/4f7			65530

5.3.3. Routemap redistribute Azure routes into on-premises OSPF backbone

We will import Azure routes learned from BGP into the OSPF backbone with a Metric Value “100”

On site 1

```
set routemap ex_ospf id 10 on
set routemap ex_ospf id 10 match network 172.30.0.0/16 all
set routemap ex_ospf id 10 match protocol bgp
set routemap ex_ospf id 10 action metric value 100
set ospf export-routemap 0.119.0.5 ex_ospf preference 10 on
```

On site 2

```
set routemap ex_ospf id 10 on
set routemap ex_ospf id 10 match network 172.30.0.0/16 all
set routemap ex_ospf id 10 match protocol bgp
set routemap ex_ospf id 10 action metric value 200
set ospf export-routemap 0.119.0.35 ex_ospf preference 10 on
```

On site 2 we increased the metric to “200” as the Site 1 is the Active site, so the routes to Azure will go through Site 1 as the metric is “100” and has precedence.

#####