Remediate Legacy Spoke to Network

Overview

This article is a set of instructions for converting existing ‘legacy’ spoke to networks to connect to the new Core Network controlled by the Azure Firewall.

Instructions

Step One: Delete Peering for Legacy Spoke

⚠️ Note this will disconnect the spoke from the BHP network, ensure you do this during a scheduled change window.

1. Locate the target spoke VNet in the Azure Portal. This can be done by looking up VNets and narrowing the scope to the target subscription.
2. Click on the ‘Peerings’ blade.
3. Delete the existing peer (confirm you want to delete at both ends).

Step Two: Re-Calculate Route Summaries

Firstly, identify the current spoke VNet CIDR range. This can be done via the Azure portal by looking up VNets and narrowing the scope to the target subscription.

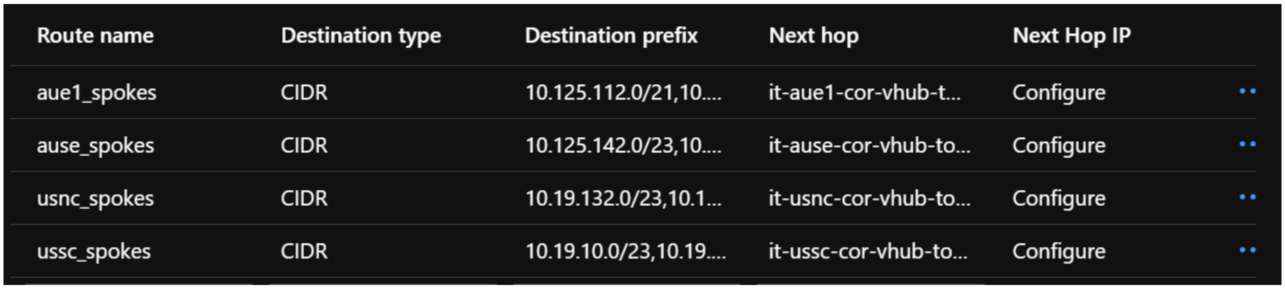
Next, you will need to re-calculate the route summaries advertised by the vWAN hub so that they include the range for the target legacy spoke. Once calculated, make sure to update the table below with the new values.

Current Advertised Ranges

AU East	AU Southeast	US South Central	US North Central
10.125.7.0/24	10.125.135.0/24	10.19.8.0/22	10.19.132.0/23
10.125.8.0/24	10.125.136.0/24	10.19.13.0/24	10.19.134.0/24
10.125.15.0/24	10.125.142.0/23	10.19.14.0/23	10.19.136.0/21
10.125.16.0/24	10.125.146.0/23	10.19.16.0/20	10.19.144.0/20
10.125.18.0/23	10.125.166.0/23	10.19.32.0/19	10.19.160.0/19
10.125.25.0/24	10.125.168.0/21	10.19.64.0/19	10.19.192.0/19
10.125.31.0/24	10.125.176.0/20	10.19.96.0/20	10.19.224.0/20
10.125.46.0/23	10.125.192.0/23	10.19.120.0/22	10.19.240.0/21
10.125.48.0/20	10.125.224.0/20		10.19.248.0/22
10.125.64.0/19	10.125.240.0/21		
10.125.96.0/20	10.125.248.0/22		
10.125.112.0/21			
10.125.120.0/22			

Step Three: Update Routes on vWAN Hubs

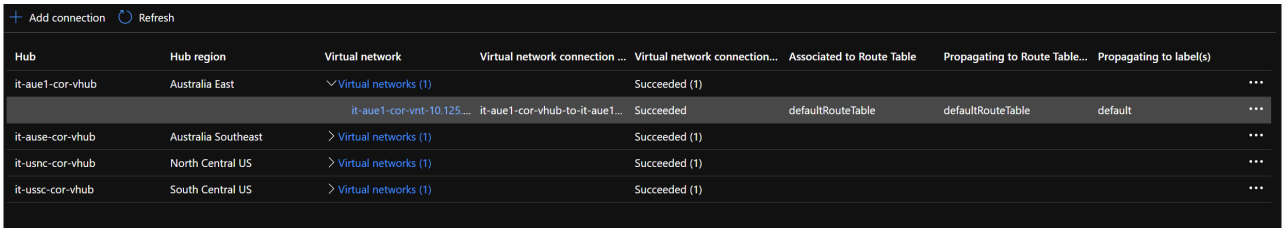
1. Connect to the Azure Portal, look up the Virtual WAN (the one you are looking for is called ‘it-aue1-cor-vwan’ which sits in the ‘BHP-Shared-Services’ subscription.
2. Then click on ‘Hubs’.
3. Click on the first one (AU East - Sydney) and go to the ‘Routing’ option.
4. Click on ‘Default’ to display the routes
   a.



Route name	Destination type	Destination prefix	Next hop	Next Hop IP
aue1_spokes	CIDR	10.125.112.0/21,10....	it-aue1-cor-vhub-t...	Configure
ause_spokes	CIDR	10.125.142.0/23,10....	it-ause-cor-vhub-to...	Configure
usnc_spokes	CIDR	10.19.132.0/23,10.1...	it-usnc-cor-vhub-to...	Configure
ussc_spokes	CIDR	10.19.10.0/23,10.19....	it-ussc-cor-vhub-to...	Configure

5. Next take your new route summaries and paste them in the ‘Destination Prefix’ boxes for each region (only regions where you have updated routes to advertise. If you are doing a single region update just update that entry.)
6. Click on the ‘Review + Create’ button at the bottom of the table. Wait until this finishes saving before moving on.
7. Repeat Steps 3 through 6 for the other 3 vWAN Hubs (Au Southeast, US North Central and US South Central) so that all hubs have the new routes. **It is important that all four hubs have the same static routes for all four sets of spoke networks**.

Step Four: Update Regional VNet Connection Routes

1. Open up the Virtual WAN screen in the portal again.
2. Click on the ‘Virtual Network Connections’ blade.
3. Now expand the Network(s) from the regions you are updating
   a. 

Hub	Hub region	Virtual network	Virtual network connection ...	Virtual network connection...	Associated to Route Table	Propagating to Route Table...	Propagating to label(s)
it-aue1-cor-vhub	Australia East	Virtual networks (1)		Succeeded (1)			
		it-aue1-cor-vnt-10.125....	it-aue1-cor-vhub-to-it-aue1...	Succeeded	defaultRouteTable	defaultRouteTable	default
it-ause-cor-vhub	Australia Southeast	Virtual networks (1)		Succeeded (1)			
it-usnc-cor-vhub	North Central US	Virtual networks (1)		Succeeded (1)			
it-ussc-cor-vhub	South Central US	Virtual networks (1)		Succeeded (1)			

4. Click on the ‘…' at the end of the row and choose 'Edit'
5. Update the ‘Destination Prefix’ column with your new routes and press ‘Confirm’.
6. Repeat this for each Virtual Network with new routes. If you are only updating routes in one region this will only require one update.

Step Five: Create New Route Table

1. Open up the Route Tables in the target spoke subscription.
2. Click ‘Add New’.
3. Follow the naming convention and create a new table.
4. Add two routes to the table as per the table below and save.

Region	Name	Route Prefix	Destination (Virtual Appliance)
AU East	it-aue1-<env>-afw-rte	10.0.0.0/8	10.125.45.4
	it-aue1-<env>-cpfw-rte	0.0.0.0/0	10.125.127.196
AU Southeast	it-ause-<env>-afw-rte	0.0.0.0/0	10.125.165.4
	it-ause-<env>-cpfw-rte	10.0.0.0/8	10.125.255.196
US South Central	it-ussc-<env>-afw-rte	0.0.0.0/0	10.19.12.4
	it-ussc-<env>-cpfw-rte	10.0.0.0/8	10.19.127.196
US North Central	it-usnc-<env>-afw-rte	0.0.0.0/0	10.19.135.4
	it-usnc-<env>-cpfw-rte	10.0.0.0/8	10.19.255.196

Note: Where <env> denotes target environment (e.g. npe for Non-Prod and prd for Prod).

Step Six: Associate Route Table to Spoke Network

1. Locate the target spoke VNet in the Azure Portal. This can be done by looking up VNets and narrowing the scope to the target subscription.
2. Click on Subnets.
3. Open each subnet and change the route table to the new one you created in Step Five.

Step Seven: Create New Peering to Core Network

1. Keep the portal screen on the target VNet and click on the ‘Peerings’ blade.
2. Click on ‘Add’.
3. Peering Link name should be <name of the source VNet>-<Name of target peer VNet>, name for the peer on the other side should be the inverse. Make sure to enable ‘Allow forwarding traffic’ for the legacy spoke from the core network. The target VNet for the peer should be the Shared Services core networking VNet from the appropriate region (See table below). Confirm the change when finished.

Australia East	it-aue1-cor-vnt-10.125.126.0
Australia Southeast	it-ause-cor-vnt-10.125.254.0
US South Central	it-ussc-cor-vnt-10.19.126.0
US North Central	it-usnc-cor-vnt-10.19.254.0

Step Eight: Create Firewall Rules

Firewall rules should be worked out in conjunction with the application team owning the legacy spoke. The following sets of rules should be identified:

- Integrations with on-prem or other Azure networks (e.g. database access, APIs, file transfers, etc)
- Remote Admin (find out which jump box / Citrix ranges are used for remote access of servers)
- Non-HTTP based access to the servers from end users

Once you have collated a list of rules (Source, Destination, Port, Protocol, Action), these should be added to the Terraform application ruleset and deployed to the Firewalls.

⚠ **DO NOT ADD THE RULES THROUGH THE AZURE PORTAL, THEY WILL BE REMOVED THE NEXT TIME TERRAFORM DEPLOYS RULES.**

Step Nine: Add Internal WAF Policies

If your spoke contains web applications they will now be required to go via the internal WAF (Azure Application Gateway with WAF enabled). These policies are also deployed only through Terraform. In order to create the policy you will require a copy of the application certificate(s) in a .PFX format. These should be uploaded to the central Shared Service Key Vault (Vault Name: it-akv-001 in BHP-Shared-Services subscription).

Once the certificate is uploaded create the appropriate Listener, Backend and Rule on the App Gateway using Terraform.

⚠ **DO NOT ADD THE POLICY THROUGH THE AZURE PORTAL, IT WILL BE REMOVED THE NEXT TIME TERRAFORM DEPLOYS ADDITIONAL POLICIES.**

Step Ten: Test Connectivity

Test the following connections once remediation is complete:

- Remote Access from Jump host
- Ensure your VMs have internet access via the CheckPoint
- Check basic service connectivity for Active Directory, DNS, etc
- Test each integration
- Test WAF and Firewall policies