128 TECHNOLOGY

Deploying Microsoft Azure Virtual WAN with 128Technology Router

Abstract

A description of the steps necessary to use a 128T router in an Azure Virtual WAN as described on Microsoft Azure. The primary goal of the Azure Virtual WAN solution is to automate provisioning of branch site access to Azure-based resources, including private VNet-based hosts and global Microsoft backbone routing. The goal of 128 Technology is to become a preferred provider device that enables simplified integration and provisioning of 128T node Azure connectivity.

18 March 2020

Contents

Overview

Overview

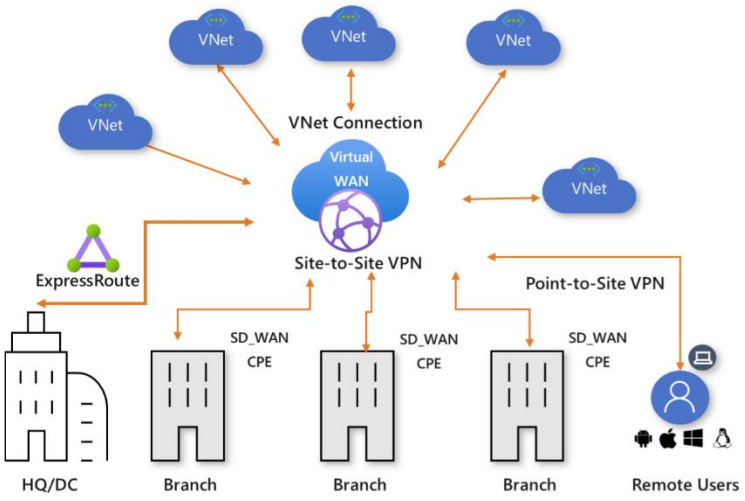
Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You can leverage the Azure backbone also to connect branches and enjoy branch-to-VNet connectivity. Microsoft has a list of partners such as 128Technology that support connectivity automation with Azure Virtual WAN VPN. For more information, see the Virtual WAN partners and locations article.

Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, User VPN (point-to-site), and ExpressRoute into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections. It enables global transit network architecture based on a classic hub-and-spoke connectivity model where the cloud-hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of spokes.

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (128Technology), you can connect to a VPN Gateway, ExpressRoute circuits, and even connect mobile users via a Point-to-site gateway to the virtual hub. The hub is the core of your network in a region. There can only be one hub per Azure region.

A hub gateway is not the same as a virtual network gateway that you use for ExpressRoute and VPN Gateway. For example, when using Virtual WAN, you don't create a site-to-site connection from your on-premises site directly to your VNet. Instead, you create a site-to-site connection to the hub. The traffic always goes through the hub gateway. This means that your VNets do not need their own virtual network gateway. Virtual WAN lets your VNets take advantage of scaling efficiently through the virtual hub and the virtual hub gateway.

A typical Microsoft Virtual WAN architecture is shown in the diagram below



The high-level steps for deploying the Azure Virtual WAN with a 128Technology Router as are as follows

- Create a Azure Virtual WAN
- Create a Hub
- Create a Site-to-Site
- Create a VPN site to hub
- Connect the VNet to the hub
- Download VPN configuration
- Configure the 128T Router to connect to the Azure Virtual WAN

Step 1: Azure Virtual WAN

Task 1: Creating a Azure Virtual WAN:

Step	Action
1.	Refer to the steps for deploying the Azure Virtual WAN
2.	Once completed, continue on with step 2

Step 2: Create a hub

Task 1: Creating a Azure Virtual WAN HUB.

Step	Action
1.	Refer to the steps for creating the Azure Virtual WAN Hub
2.	Once completed, continue on with step 3 for creating a site.

Step 3: Create a site

With the Azure Virtual WAN Hub created the next step is to establish a site-to-site connection from the Azure HUB to a 128Technology on-premises router.

Task 1: Create a site to the hub

Step	Action
1.	Refer to the steps for creating the Azure Virtual site to the WAN Hub
2.	Once completed, continue on with step 4 for connecting the VNet to the hub.

Step 4: Connect the VNet to the hub

With the Azure Virtual WAN Site created the next step is to establish vNet connectivity to the Azure HUB.

Task 1: Connect the VNet a site to the hub

Step	Action
1.	Refer to the steps for connecting the VNet to the hub
2.	Once completed, continue with step 5 for downloading the VPN configuration

Step 5: Download VPN configuration

Task 1: To establish connectivity to Azure Virtual WAN from a 128T router, the VPN configuration file needs to be downloaded, and the PSK copied for later use.

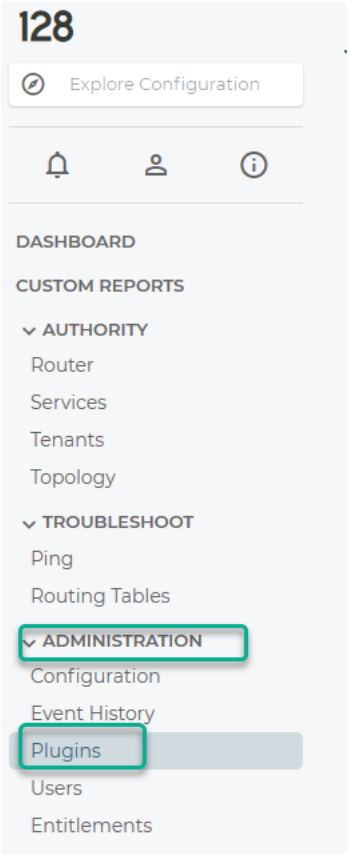
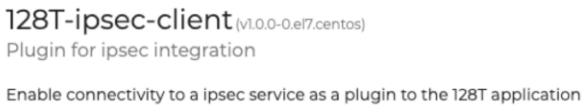
Step	Action
1.	Refer to the steps for downloading the VPN configuration needed for the 128T router.
2.	With the VPN file downloaded, **open** the file in **Notepad**. *Example Config*: [{"configurationVersion":{"LastUpdatedTime":"2020-01-28T18:31:48.0055512Z","Version":"c250e6d3-b263-42e3-bb0d-8d822af3db26"},"vpnSiteConfiguration":{"Name":"128TRtrHOU","IPAddress":"X.X.X.X","LinkName":"Fiber_R1P1"},"vpnSiteConnections":[{"hubConfiguration":{"AddressSpace":"172.30.2.0/24","Region":"East US 2"},"gatewayConfiguration":{"IpAddresses":{"***Instance0":"X.X.X.X","Instance1":"X.X.X.X***"}},"connectionConfiguration":{"IsBgpEnabled":false***,"PSK":"ABCDEFG123***","IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}}}]}]
3.	Keep this file open to leverage later on during the 128T IPSec configuration.
4.	Once completed, continue on with step 6 deploying the 128T plugin for Azure Virtual WAN

Step 6: Deploying the Azure Virtual WAN 128T Conductor plugin

In this step the plugin for the Azure Virtual WAN will be deployed via the 128T Conductor. It is implied that a 128T Conductor and Router are already deployed.

Task 1: Configure basic settings

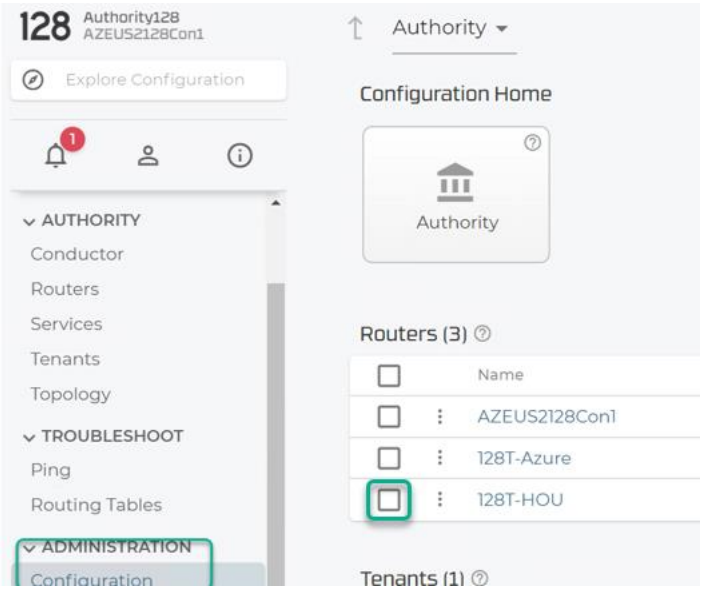
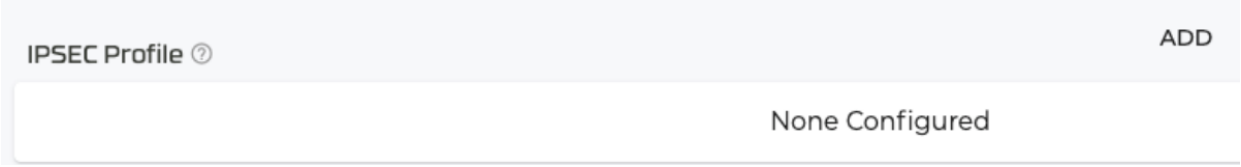
Step	Action
1.	Connect via using the supported list of browsers such Microsoft Edge Chromium, Google Chrome, Firefox, or Safari on Mac to the 128T Conductor portal. This is the IP address or FQDN for the VM or physical appliance. *Note: Using older Microsoft Edge browser or Interne Explorer may not dispay some items in the web UI correctly. Please use only the suported list above for administration.* Login with the username **Admin** and password created during the deployment. Click **Sign In** 

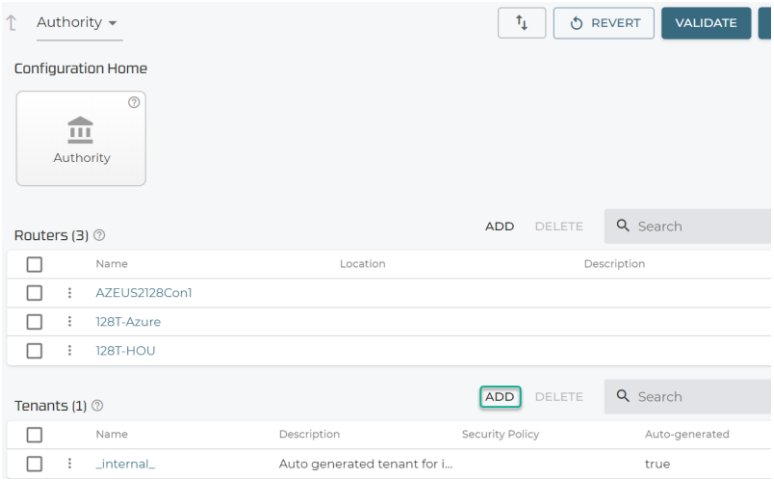
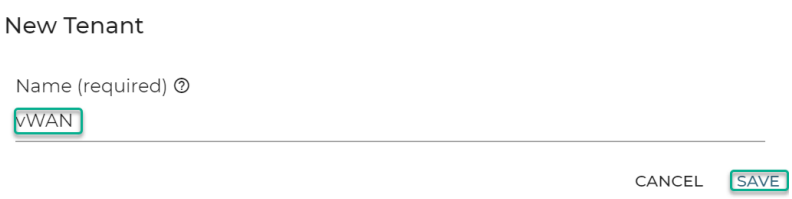
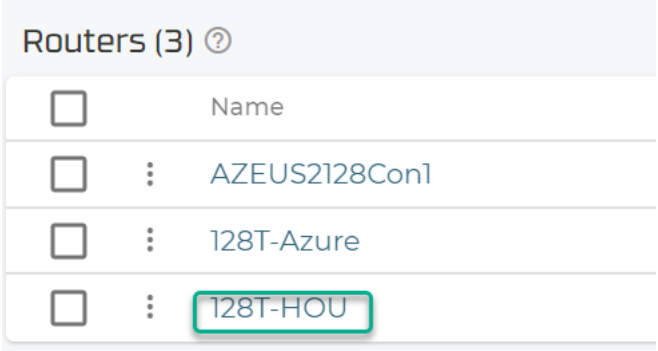
Step	Action
2.	Navigate to **Administation→ Plugins**. 
3.	Click in **Available**. In the available tab select the **128T-ipsec-client** plugin then click **Install** 
4.	After a few minutes the plugin will be installed

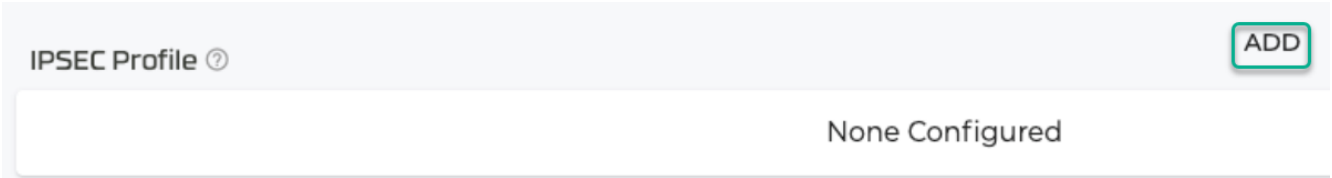
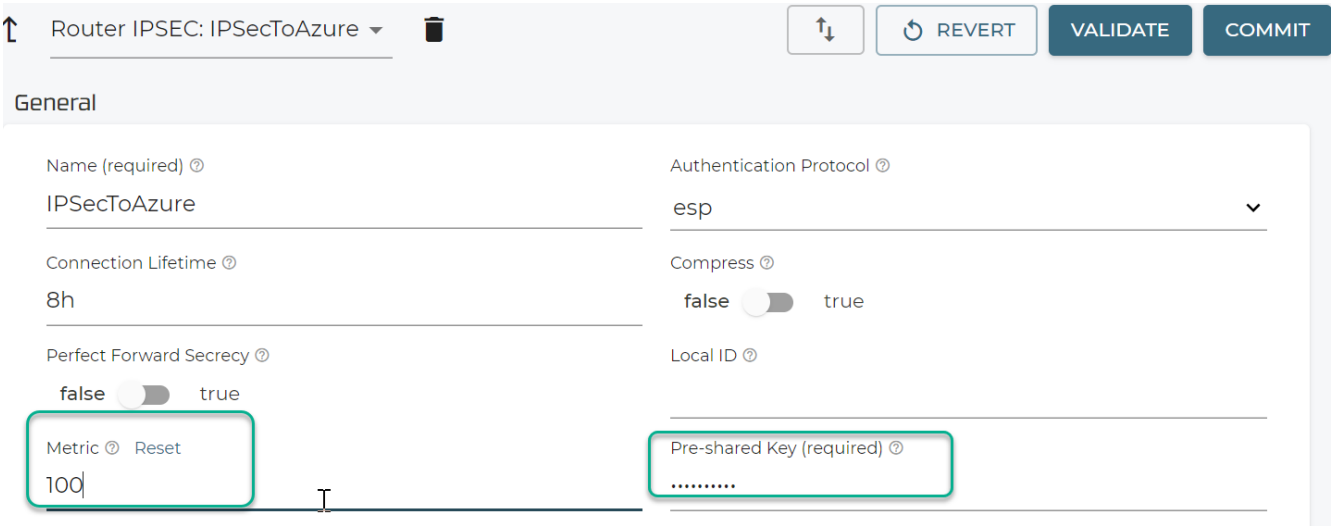
Step 7: Configuring the 128T Router for Azure Virtual WAN

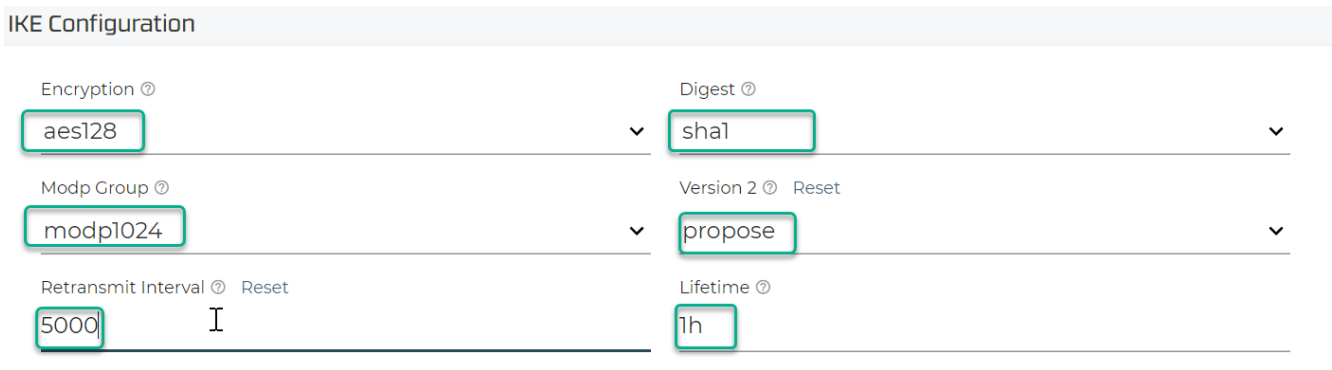
With the Azure Virtual WAN Hub created the next step is to establish a site-to-site connection from the Azure HUB to a 128Technology onsite router.

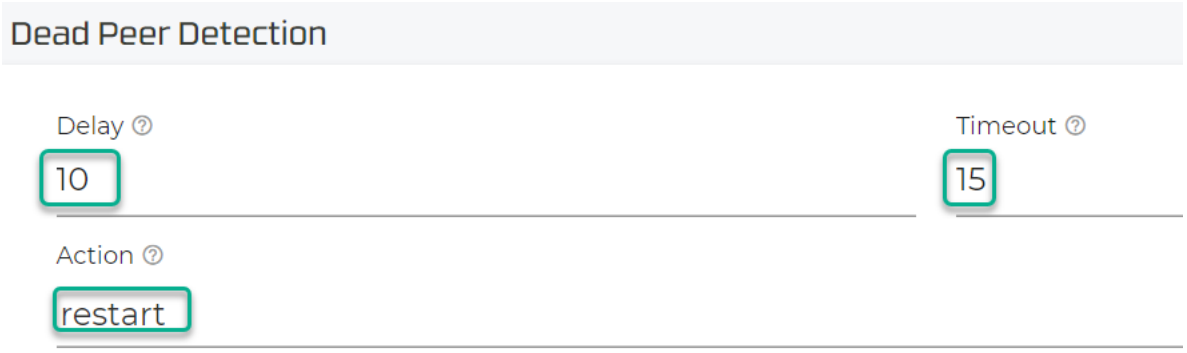
Task 1: Configuring the 128T Tenant

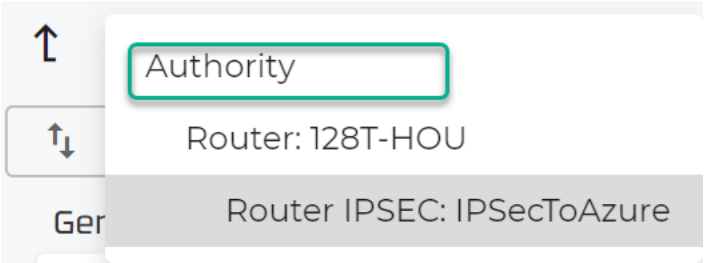
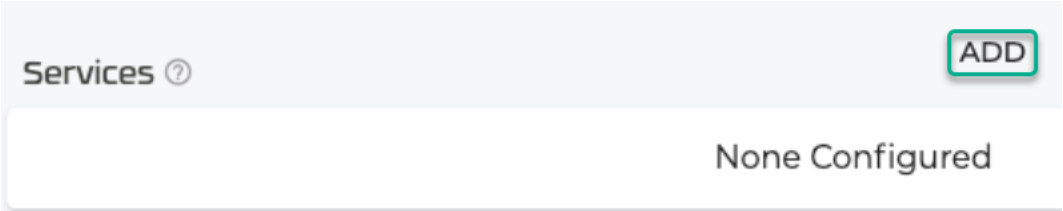
Step	Action
1.	In the 128T portal go to **Administration—>Configuration** click on the 128T router that will be used for the connection to Azure Virtual WAN. In this example 128T-HOU is a on-premises router that running the 128T software. 
2.	Scroll down to end of the page to verigy that IPSEC profile appears. There is no configuration required at this point as this just to ensure that it was properly installed from the previous step. 

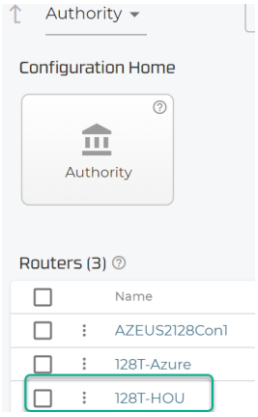
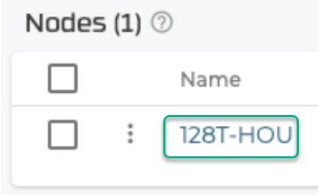
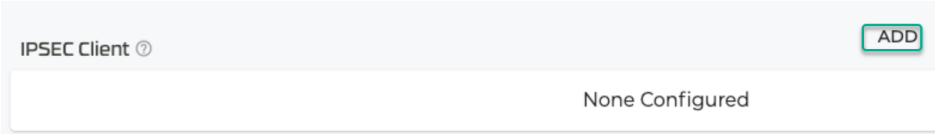
Step	Action
3.	Scroll back up to the top of the page and under Authority should be **Tenants**. Click **Add.** 
4.	Give the Tenant a name such **vWAN.** Then click **Save.** 
5.	From the **Configuration** section navigate to **Routers.** Click on the **Router** that will be used for the IPSec connection 

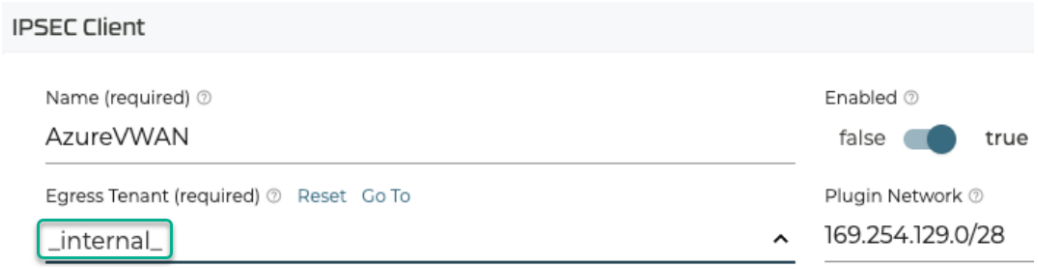
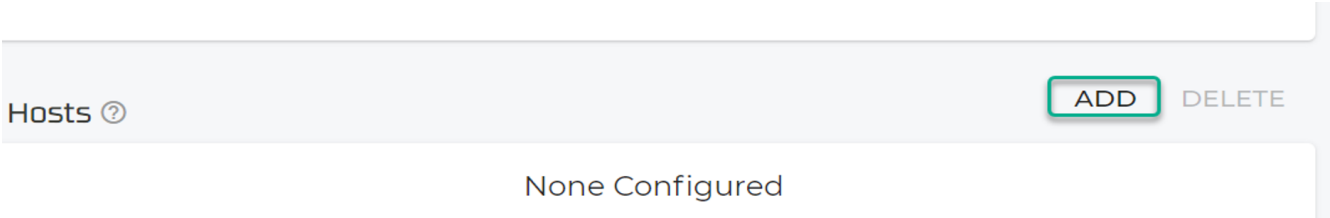
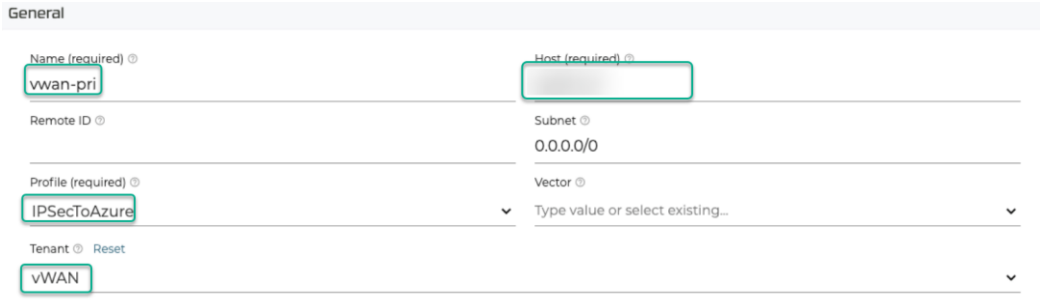
Step	Action
6.	Scroll down to the **IPSec** Profile section click **Add**  Give the profile a name such as **IPSectoAzure**.Click **Save**.
7.	In the previous step 5 task 1, the VPN config file was created. Open the config file and then **copy** the PSK value and other information that needs to match. Enter the PSK value into the **Pre-shared Key field** and change the Metric to **100** 

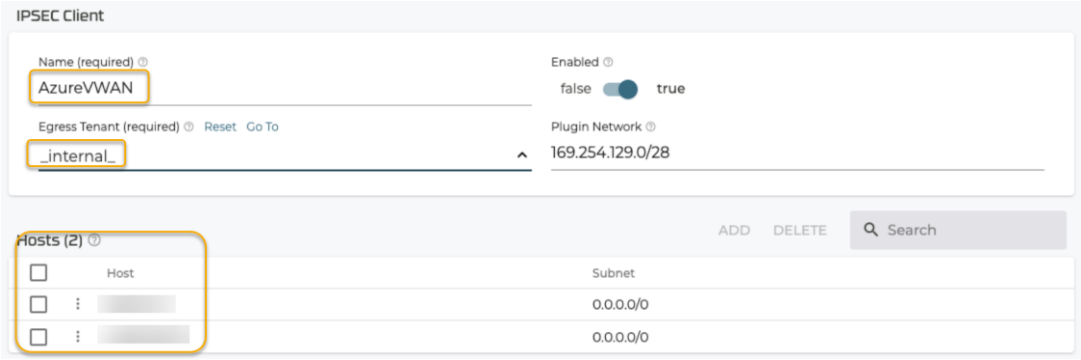
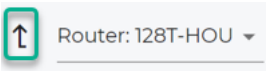
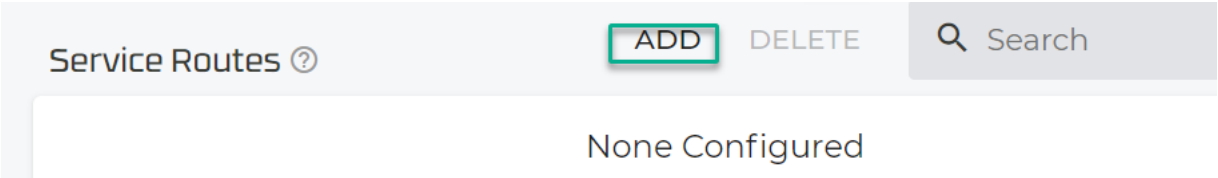
Step	Action
8.	Scroll down to the **IKE configration** section and ensure the following fields are set: Encryption: **aes128** Digest: **sha1** Modp Group: **modp1024** Version 2: **propose** Restransmit interval: **5000** Lifetime: **1h** 
9.	Scroll down to the **Phase two** section and ensure the following fields are set: Encryption: **aes128** Digest: **sha1** Modp: **modp1024** 

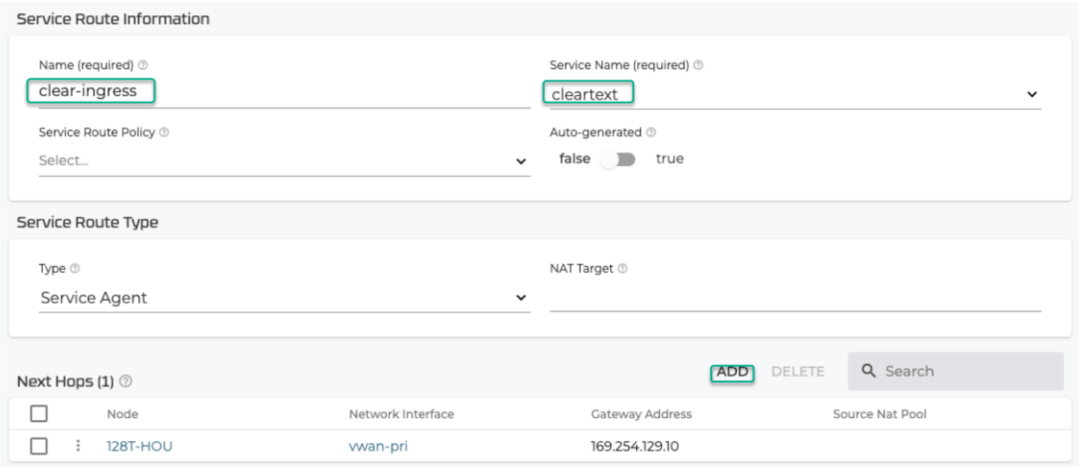
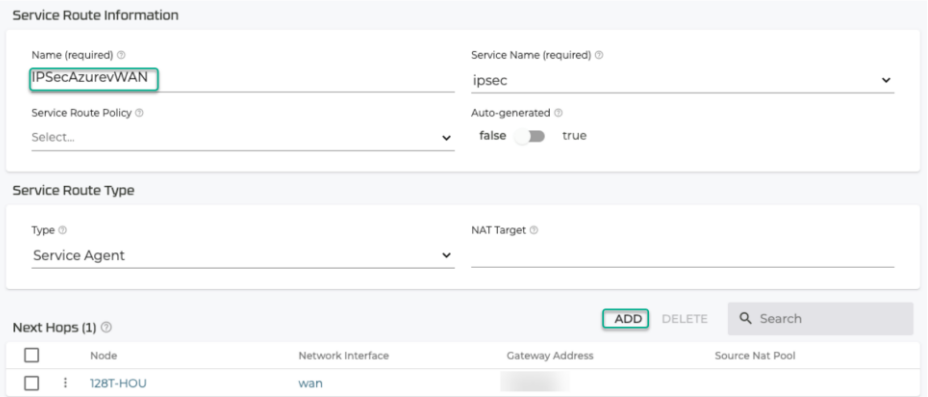
Step	Action
10.	Scroll down to **Dead Peer Detection** and ensure the following fields are set: Delay:**10** Timeout:**15** Action:**restart** 

Step	Action
11.	Scroll up to In the hiearchy tree then click on the **Authority** then scroll down to **Services**. Then click **Add**. In service click the **IPSec** service created earlier.  In the Service Address click **Add**.  Enter in the name **ipsec** then click **Save.** In the services addresses click **Add. Enter 0.0.0.0/0. Click Save. Click** back up in the hiearchy to **Authority.** 
12.	In the **Authority** scroll down to **Services** to create a second service. Click **Add**. In name enter **cleartext** the click **save**. In the services addresses click **Add. Enter the LAN address 0.0.0.0/0. Click Save. Click** back up in the hiearchy to **Authority.** 

Step	Action
13.	In the **Authority** select the **Router.**  **Click** on the **Node**  Scroll down to the bottom of the page and select the **IPSEC Client. Click Add**  **Name** the client **AzureVWAN. Click Save.** 

Step	Action
14.	In the IPSEC Client change the following fields: Egress Tenant: **_internal_** 
15.	In the **Hosts** section click **Add.**  Name (Required): **vwan-pri** Host (required): Enter in the **IP address** of the Azure Virtual WAN Gateways. *Note: The Public IP addresses can be found in the config file in the Gateway configuration for **Instance 0** and **Instance 1**.* Profile: **IPSecToAzure** Tenant: **vwan** 

Step	Action
16.	Click the **Up arrow.**  Repeat the process from step 15 for adding the second host with the second public IP address for the Azure vWAN host in the config file. The final configuration should look like below: 
17.	Click **Validate**. 
18.	Click the **up arrow** and navigate to **Router→Service Routes.** Click **Add**  

Step	Action
19.	In the New Service Route enter a name like **clear-ingress**. Click **Save.** In the **clear-ingress** service routes enter: Name: **clear-ingress** Service Name: **cleartext** Service Route Type: **Service Agent** In the **Next Hops** section click **Add** **Select node 128T-HOU and network interface vwan-pri** 
20.	Create a second Service Route enter a name like **IPSecAzurevWAN**. Click **Save.** In the **IPSecAzurevWAN** service routes enter: Name: **IPSecAzurevWAN** Service Name: **ipsec** Service Route Type: **Service Agent** In the **Next Hops** section click **Add** **Select node 128T-HOU and network interface vwan-pri** 

Step	Action
21.	Click **Validate** and **Commit** 
22.	After a short time the connectivity between the 128T router and the Azure VWAN Hub is established.

Authors

The following authors contributed to the creation of this deliverable.

Tony Sanchez	TSanchez@128Technology.com
Francisco Mendez	fmendez@128technology.com

Revision History

Revision	Change Description	Updated By	Date
1.02	Minor Updates	Tony Sanchez	March 2020