Configure a Virtual Network Connection for Azure Virtual WAN

Overview of Virtual WAN

If you use Azure cloud services, you can create a Virtual WAN (VWAN) to orchestrate and simplify network connectivity between your on-premises networks, branch offices, and remote users. You can integrate Multicloud Defense with Azure VWAN by orchestrating virtual network connections and route propagation between Service VNets and a virtual hub (vHub).

Typically, within a vHub, Multicloud Defense is not supported as a Network Virtual Appliance (NVA). Instead, you can use VWAN route orchestration to address this limitation. To use Multicloud Defense to protect your application on Azure, you can orchestrate the creation of a virtual network connection from a Service VNet to a vHub inside a VWAN. You can propagate routes between the vHub and Multicloud Defense. Multicloud Defense supports VWAN for egress mode only. Azure VWAN is supported only for Multicloud Defense gateways.

Guidelines for Virtual WAN Connections to Azure vHub

Prerequisites

- An Azure subscription with VWAN and vHub configured.
- Service VNet and spoke VNets set up in Azure.
- Multicloud Defense gateway deployed in the service VNet.
- Permissions to create and manage virtual network connections and route tables in Azure.
- Permissions to enable and disable vHub connections.

Limitations

- Multicloud Defense is not supported as an NVA within a vHub.
- CIDR selection is only available during the edit phase, not during VNet creation.
- Route propagation is dependent on the configuration of the egress or ingress gateway.

Create Service VPC with Virtual WAN Attachment

You can create a Service VPC with VWAN attachment using the **Easy Setup** wizard when you secure your account. For details, see Centralized Model: Add a VPC or VNet.

Use the following procedure to create a Service VPC and attach a VWAN.

Procedure

Step 1 From the Multicloud Defense Controller, navigate to **Infrastructure** > **Gateways** > **VPCs/VNets**.

Step 2 Click **Create Service VPC/VNet** to create a Service VPC.

Step 3 Provide a **Name**.

Step 4 From the **Region** drop-down list, choose a region.

Step 5 From the **CSP Account** drop-down list, choose an account.

Step 6 Provide details for **CIDR Block**.

Step 7 From the **Availability Zones** drop-down list, choose a zone.

Step 8 From the **Resource Group** drop-down list, choose a resource group.

Step 9 Check the **Use NAT Gateway** check box to direct traffic through the NAT gateway.

Step 10 In **vWAN Attachment**, set the toggle to **Enabled**.

Step 11 From the **vHub** drop-down list, choose a hub.

Step 12 In the **Associate Route Table** drop-down list, select a route table to associate.

Step 13 In the **Propagate Route Tables** drop-down list, select route tables to propagate.

Step 14 Click **Save**.

A Service VPC is created with a vHub connection to an Azure VWAN. You can also view the configuration changes made, on your Azure account.

Note
If you delete a Service VPC in Multicloud Defense, the vHub connection between the VWAN and the Azure Service VPC is also deleted.

Modify Service VPC with Virtual WAN Attachment

Procedure

Step 1 From the Multicloud Defense Controller, navigate to **Infrastructure** > **Gateways** > **VPCs/VNets**.

Step 2 Choose a Service VPC that you want to edit, from the list.

Step 3 Click **Edit**.

Step 4 In **vWAN Attachment**, set the toggle to **Enabled**.

Step 5 From the **vHub** drop-down list, choose a hub.

Step 6 In the **Associated Route Table** drop-down list, choose route tables to associate.

Step 7 In the **Propagate Route Tables** drop-down list, choose route tables to propagate.

Step 8 To propagate all spoke CIDRs to the vHub, set the toggle to **Always**.

Note
To add multiple spoke VPCs to the route tables, use the list builder to move the spoke VPCs from the **Available** section to the **Selected** section. Moving the VPC to the **Selected** section ensures that the VPC is added.

Step 9 Click **Save**.

The Service VPC connects to a VWAN containing a vHub and spoke VPCs in Azure. Any changes made to route tables are also updated in Azure.