..|...|.. cisco

Prescriptive Deployment Guide Cisco Public

# Cisco Cloud onRamp for IAAS using Azure

Prescriptive Deployment Guide

November, 2020

## Contents

Introduction	3
Define - Cisco Cloud onRamp for laaS Introduction	4
Design - Cisco Cloud onRamp for laaS Use Case and Feature Overview	9
Prerequisites - Cisco Cloud onRamp for laaS using Azure	23
Deploy - Cisco Cloud onRamp for laaS using Azure	48
Operate - Cisco Cloud onRamp for laaS Monitoring	67
Appendix A: New in this Guide	81
Appendix B: Hardware and Software Used for Validation	81
Appendix C: Transit VNet Cisco WAN Edge Device and Feature Templates	82
Example Branch Configuration	88
Appendix D: Glossary	100
Feedback	101

## Introduction

## **About the Guide**

This document discusses the design and deployment of Cisco SD-WAN Cloud onRamp for laaS using Azure. The guide focuses on the deployment of secure network connectivity from private network data center and branch locations to one or more Azure VNets using Cisco Cloud onRamp for laaS. The guide explains at length the platforms deployed within the transit VNet and in the on-premise branches/ datacenter, it highlights the best practices and assists with the successful configuration and deployment of the Cisco Cloud onRamp for laaS feature. However, the document is not meant to exhaustively cover all options.

This document assumes that the Cisco SD-WAN controllers are already deployed and integrated into vManage NMS, the WAN Edge devices are deployed, and the Cisco SD-WAN overlay network is successfully established. For the device models and software versions used for this deployment, refer to Appendix B and for the device/feature templates, refer to Appendix C.

This document contains four major sections:

- The **Define** section introduces the Cisco Cloud onRamp for laaS feature and explains the overall solution, along with the benefits of deploying it.
- The **Design** section includes the two use cases covered in the guide, along with the design components and considerations for successful SD-WAN Azure integration.
- The **Deploy** section is divided into two parts. The first part includes the Azure cloud and vManage prerequisites to deploy the Cisco Cloud onRamp for IaaS feature. The second part discusses the automated deployment of the Azure transit VNet to support the two use cases presented within the design section.
- The **Operate** section explains some of the common monitoring and troubleshooting capabilities available within the Cisco vManage for the Cloud onRamp for IaaS feature.



#### Figure 1. Implementation Flow

## Audience

The audience for this document includes network design engineers, network operations personnel, and security operations personnel who wish to implement Cisco SD-WAN secure virtual private network (VPN) connectivity from their private networks to one or more Azure virtual networks (VNets).

## Define – Cisco Cloud on Ramp for IaaS Introduction

## Challenges

Network engineers in today's multicloud world are beginning to understand the benefits of cloud computing services such as Infrastructure as a Service (IaaS), a set of computing resources such as storage and networking components that can be used to host and deliver enterprise applications over the Internet. With IaaS, the on-premise physical data center infrastructure is moved off-premise or extended to a virtualized environment where computing resources are hosted by a public cloud provider such as Amazon Web Services (AWS) or Microsoft Azure. This enables organizations to instantly provision and manage compute infrastructure over the Internet, eliminating the need to procure, install and manage physical hardware appliances.

However, connecting an enterprise network to a cloud provider infrastructure can be challenging since each cloud provider has different models for connectivity. Within the cloud infrastructure, instances or virtual machines are deployed within Azure Virtual Networks (VNets) or Amazon Virtual Private Clouds (VPCs), and connectivity is established via various cloud connectivity models.

The rest of this guide explains the some of the possible design options for Cisco SD-WAN Azure interconnection, with focus on Cisco Cloud onRamp for IaaS design. For details regarding Cisco SD-WAN AWS interconnection refer to the <u>Cisco Cloud OnRamp for IaaS using AWS</u> guide.

## **Cisco SD-WAN Interconnection with Azure**

Within the Azure public cloud, virtual machines or containers are hosted in the cloud infrastructure to extend and interconnect cloud services with the enterprise WAN architecture.

Within the Azure Cloud the following Azure services are used to interconnect with the on-premise Cisco SD-WAN network.

Azure Terminology	Definition
Azure Resource Groups	Azure resource groups are a logical collection of resources that include virtual machines, storage accounts, virtual networks, web apps, databases, and/or database servers.
Azure Virtual Network (VNet)	Azure Virtual Networks (VNets) are the fundamental building block for a private network in Azure that contain Azure resources such as Azure Virtual Machines (VM), to securely communicate with each other, the Internet, and to on-premises networks. Note, a VNet is similar to a traditional network that you operate in your own data center, but it brings along it's additional benefits of Azure's cloud infrastructure such as scale, availability, and isolation.
Azure Instances	Virtual Machines (VMs) or Azure Instances are used to host applications within Azure VNets, they also allow you to deploy Cisco SD-WAN virtual instances within VNets.
Transit VNet	A transit VNet is an Azure VNet used as a transit point for data flows between Azure host VNets as well as between Cisco SD-WAN campus and branch sites and Azure host VNets. The transit VNet is built using a configuration wizard in the vManage NMS. The wizard automates the bring-up of the transit VNet within the Azure public cloud account and the connections between public-cloud applications and the users of those applications in the branches in the overlay network. This VNet contains a pair of WAN Edge virtual devices placed in an availability set for isolating the VMs from each other. These availability sets run across multiple physical servers, compute racks, storage units and network

Azure Terminology	Definition
	switches. Therefore, when a software or hardware failure occurs only a subset of VM's fail. Each WAN Edge device is automatically provisioned with the necessary public and private IP addresses, and Network Security Groups. Within the NSGs, rules can be manually configured to block or allow IP traffic flow.
	The bring up and deployment of transit VNet is explained in depth in the design and deployment section of this guide.
Host VNet	A host VNet is a customer owned virtual network in the Azure cloud, that is manually deployed prior to provisioning the transit VNet. When a transit VNet connects to an application or application provider, it is simply connecting to a host VNet. Each host VNet mapped to the transit VNet, contains a Virtual Network Gateway (VNG) associated to the host VNet's gateway subnet. Note, while host VNet itself is manually deployed by the user, its associated VNG is automatically provisioned during the cloud onRamp workflow.
Virtual Hub	A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity.
Virtual WAN (vWAN)	The Virtual WAN resource represents a virtual overlay of the customer's Azure network and is a collection of multiple resources. It contains links to all your virtual hubs that you would like to have within the virtual WAN.
Azure Subscription	Azure Subscription lists out all the subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. Each subscription is associated with a subscription ID, a unique alphanumeric string.
Azure Active Directory (Azure AD)	Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps employees sign in and access resources such as applications within the corporate network and Intranet, along with access to any cloud-based applications developed by the organization. However, remember Azure AD is not similar to an AD on-premise that provides authentication directory policies and other services. Azure AD has only two major services which are identity and access management.
Azure AD Application and Service Principal	Within the Azure AD new applications and service principals are created, that are used with the role-based access control.
	When you have applications, hosted services, or automated tools that needs to access or modify resources, you can create an identity for the application. This identity is known as a service principal. Roles are assigned to the service principal to maintain control over access to resources.
Application ID	When an application is registered through the Azure portal, an application object, along with the service principal are automatically created in your Azure home directory or tenant. For programmatic sign in access from vManage to your Azure subscription, you pass the directory ID or tenant ID with your authentication request, along with the application ID and secret key. The Application ID or client ID is an identity of the application that Azure AD
	recognizes.
Tenant ID	The Tenant ID or Directory ID is the identity of the Azure AD in which you have created the Cloud onRamp applications.
Client Secret Key	A client secret key is the secret string that the application uses to prove its

Azure Terminology	Definition
	identity when requesting a token.
Subscription ID	The subscription ID uniquely identifies the subscription to use Azure services. The Subscription ID, along with the application ID, tenant ID and secret key are required for programmatic sign-in access during the cloud onramp workflow.

Note, all the Azure ID's needed for the programmatic sign-in access are explained in depth in the prerequisites section, along with the steps to retrieve these values.

Using the services available in Azure, the following are some of the common Cisco SD-WAN Azure integration.

## Cisco SD-WAN Interconnection: Using Azure Virtual WAN (vWAN/ vHub)

In this design, Azure Virtual WAN and virtual WAN hub(s) serve as a central connection point for host VNets and SD-WAN routers.

There are two possible scenarios for connecting SD-WAN to Azure Virtual WAN:

Born-on-Prem SD-WAN to Azure Virtual WAN: In the first scenario, on-prem physical WAN Edge devices located in branch or data center locations establish IKE-based IPsec tunnel to Azure Virtual Hub (vHub), run BGP and exchange routing information between the cloud infrastructure and the SD-WAN network using BGP-OMP redistribution.

Born-in-Cloud SD-WAN to Azure Virtual WAN: In the second scenario, virtual WAN Edge device hosted in Azure VNets establishes IKE-based IPsec tunnels to Azure Virtual Hub (vHub), run BGP and exchange routing information between the cloud infrastructure and the SD-WAN network using BGP-OMP redistribution.





For the steps to deploy this design option, refer to the following guide:

## Interconnection Cisco SD-WAN and Azure Virtual WAN Guide (vWAN)

Currently, automation within the Cloud onRamp for laaS feature is only available for connecting Azure host VNets to the Cisco SD-WAN through a transit VNet, and not for Azure Virtual WAN.

#### Cisco SD-WAN Interconnection: using Cloud onRamp for IaaS

One of the most popular and widely used options is the Cisco Cloud onRamp for IaaS feature. The key differentiator for Cloud onRamp for IaaS is automation. The entire solution is completely automated – the end user simply needs to enter his Azure subscription ID, along with the tenant ID, application ID and secret key in the related vManage section, discover Azure hosted virtual networks and workloads, and define two routers for interconnection. Cisco Cloud onRamp for IaaS brings up a fully deployed Azure hosted transit VNet containing a pair of Cisco WAN Edge routers, extends the fabric of the Cisco SD-WAN overlay network into the public cloud via the transit VNet, and allows Cisco SD-WAN branches to connect directly to public-cloud application providers.



#### Figure 3. Cloud onRamp for laaS using Azure

The rest of this solution focuses on the SD-WAN Azure Integration using Cloud onRamp for IaaS.

## About the Cloud onRamp for laaS using Azure Solution

Using Cisco SD-WAN Cloud onRamp for laaS, you can automatically spin up virtual WAN Edge router instances via Cisco vManage in a specific region of the public cloud. These virtual instances become part of the SD-WAN overlay and establish data plane connectivity to the WAN Edge routers located in the branch and/or the datacenter. As a result, secure end-to-end connectivity is established between the workloads in the cloud, physical branches and data centers.

In this design, cloud hosted virtual networks connect via IPsec VPN connections to a redundant pair of virtual WAN Edge devices within a transit VNet. The transit VNet is in turn part of the SD-WAN Secure Extensible Network (SEN), which provides direct VPN connectivity to branch and Data Center (DC) sites within the private network.

#### Benefits of deploying Cisco Cloud onRamp for laaS transit VNet Design

Some of the key benefits of deploying the Cloud onRamp feature includes the following,

Automated Infrastructure in Public Cloud	The entire solution is automated. The deployment of the
	transit VNet, bring-up procedure of WAN Edge virtual





## Design – Cisco Cloud on Ramp for IaaS Use Case and Feature Overview

The design section is organized in the following order:

- Use Case #1 Full Connectivity
- Use Case #2 Segmentation to the Cloud Provider
- Design Components and Consideration
  - Supported Platform and Software
  - Azure Design Considerations
  - Mapping of a Host VNet to Transit VNet
  - Firewall Port Considerations
  - Cisco Cloud onRamp for laaS Workflow

## **Use Case #1 - Full Connectivity**

In this use case, all entities within an organization have full connectivity to the public cloud resources deployed by the organization.

This design has the host VNets mapped to a single VRF or service-side VPN. In the example figure, all traffic from service-side VPN 1 of the WAN Edge devices deployed in both the datacenter and branch are routed over to the applications (virtual machines) in the Azure host VNets, along with communication between the VMs in the Host VNets.

#### Figure 4. Full Connectivity



Note: Cisco SD-WAN branches are deployed within the Azure cloud only for testing purposes. If you plan on deploying virtual SD-WAN branch networks within the Azure platform, these WAN Edge devices can run any Cisco SD-WAN image available in the Azure Marketplace. You can alternatively also download a Cisco SD-WAN image from CCO and upload this to Storage Service within Azure and use this image to deploy WAN Edge devices within the Host VNets.

Regarding size of the Virtual images that can be hosted within Azure branch VNets, refer to products page in Microsoft Azure and select the Cisco WAN Edge.

Link: <u>https://azuremarketplace.microsoft.com/en-</u> us/marketplace/apps/cisco.cisco\_cloud\_vedge\_17\_2\_4?tab=PlansAndPrice

## Use Case #2 - Segmentation to the Cloud Provider

In this use case, different entities within an organization have connectivity to specific public cloud resources deployed by the organization.

This design leverages Cisco SD-WAN segmentation, therefore isolating traffic between different host VNets. In this example design, one of the host VNet is mapped to VRF 1 or service-side VPN 1; and the other host VNet is mapped to VRF 2 or service-side VPN 2. As traffic across the SD-WAN overlay carries the VRF or VPN label, LAN traffic from the datacenter can be configured to communicate only with VRF 1, while branch traffic communicates with VRF 2.

This use case helps provide traffic isolation.

#### Figure 5. Segmentation to the Cloud Provider



Note: The Azure branches are there only for testing purposes.

## **Design Components and Consideration**

The rest of the design section focuses on the platforms, software, and features to be considered while deploying the SD-WAN Azure cloud integration using Cisco SD-WAN Cloud onRamp for laaS feature.

#### Supported Platforms and Software

Cloud onRamp for laaS using Azure is supported on vManage from version 18.2 onwards. Refer to the table below to understand the platforms that support the feature. Note, this list does not account for any product development changes made since the release of code version 20.1.

Platform	Azure Transit VNet	On-premise DC/Branch
Cisco - ISR4k	Ν	Υ
Cisco - ISR1k	Ν	Y
Cisco - ASR1k	Ν	Υ
Cisco - ENCS (ISRv)	Ν	Υ
Cisco - CSR1k	Ν	Υ
Cisco - vEdge Cloud	Υ	Y

Table 1. Supported Platforms

#### **Azure Design Considerations**

Before extending the on-premise network to Azure using the Cloud onRamp for laaS feature ensure to configure, setup and gather details required to complete the onRamp process from the Azure public cloud. The rest of this section shares all necessary details associated with the Azure cloud account.

#### Design a Transit VNet

Using the Cloud OnRamp for laaS feature available in vManage, a transit VNet is automatically provisioned in the Azure public cloud containing pair of WAN Edge virtual devices.

The transit VNet design can be split into two parts:

- Preparation of WAN Edge Devices: To use the Cloud onRamp feature you must have at least two unused WAN Edge cloud devices available in the vManage devices list, with device templates attached to them. When the transit VNet is deployed these two devices will be hosted within it.
- Automated bring up of Transit VNet: The second part includes the automated creation of the transit VNet, along with the provisioning of a pair of WAN Edge cloud devices to this new VNet.

#### **Preparation of WAN Edge Devices**

Design device templates comprising of all the required feature templates to be associated with the WAN Edge cloud devices in the transit VNet. These templates are attached to the two valid unused WAN Edge cloud devices.

The following are the feature templates attached to the WAN Edge cloud devices:

System Template: This feature template includes configurations like system-IP, site-id, hostname, IP addresses, and so on, defined as editable variables in the template. It is important to note that, while designing the system template for a pair of WAN Edge devices in a transit VNet, the system-IPs are different but the site-IDs are configured the same.

For instance, a transit VNet containing two devices - WAN Edge device 1 and WAN Edge device 2 are configured with the same site, such as 115001.

#### Figure 6. Site ID - System IP for a pair of WAN Edge Devices



Also, within the system template, by default, gateway tracking is enabled to determine whether the next hop for the static route is reachable before adding that route to the device's route table. It is

recommended to disable "track-default-gateway" in the system template. Keeping this feature enabled may not affect the provisioning process, but the overall configuration of the routers may be incorrect.

- NTP Template: The NTP server used in this deployment is time.nist.gov. With Cisco Cloud onRamp, the Cisco WAN Edge Cloud routers within the Azure transit VNet are automatically configured such that interface ge0/0 is part of VPN 0 and gets its IP address via DHCP (ip dhcp-client). The Azure DHCP server which allocates the IP address to ge0/0 will also provide the DNS server IP address. Therefore, a hostname can be configured and translated to an IP address by the Azure DNS server. For this deployment guide the NTP server time.nist.gov was used.
- AAA Template: This feature template is crucial and must be configured within the WAN Edge routers, in
  order to understand the username/password required to access the devices via SSH once the WAN Edge
  cloud routers are built and configured within the Transit VNet.
- BFD Template: This template is used to specify the BFD app-route multiplier and poll interval and specify the hello and BFD multiplier for each transport. In this deployment, the only color used is of Biz-Internet, since Cisco Cloud onRamp only provisions physical Internet connections to the transit VNet (VPN 0, interface ge0/0). The BFD hello interval has been made a variable. For this deployment guide, the BFD hello interval was set to 10,000 milliseconds with a multiplier of 3. You should select the appropriate BFD hello interval to balance the requirement for fast convergence against the cost of additional data transfer charges in your deployment.
- VPN Template: This feature template is created to separate VPN feature templates for each VPN. For the WAN Edge devices in transit VNet, a separate feature template is created for VPN 0, VPN 512 and service side-VPN (For ex. VPN 1 and VPN 2). To enable Cloud onRamp for IaaS feature only a minimum of one service VPN template is required. If you like to segment traffic to service-side VPN 1 and service-side VPN 2, attach separate service-VPN templates for each service side VPN within the device template. Within this template, enable IPv4 routing, ECMP keying etc. Within OMP, both BGP and connected routes are advertised within OMP so that the IP addresses of the Loopback interfaces, which are a part of VPN 1/ VPN 2, are also visible across the network.

#### Technical Tip

The cloud onRamp workflow configures a default static route to null 0 on the WAN Edge cloud router to be advertised by BGP. Advertising the null0 route via OMP to other WAN Edge devices in your network can be disruptive. However, if for any reason you have additional static routes defined within the Cisco SD-WAN Edge routers, requiring the redistribution of static routes into OMP within the transit VNet, then you may need to look at filtering out the static default route through policies applied to the SD-WAN network.

 VPN Interface Template: This feature template is created to configure interface parameters for the WAN Edge cloud routers. Separate VPN Interface templates are configured for interfaces under VPN 0, VPN 512 and service-side VPNs (VPN 1, VPN 2 among others).

With Cisco Cloud onRamp for IaaS, the Cisco WAN Edge cloud routers within the Azure transit VNet are automatically configured such that interface ge0/0 is in VPN 0 and interface eth0 is in VPN 512 and both of them get their IP addresses via DHCP (ip dhcp-client).

Although, no physical interfaces are attached to a service-side VPN, within the service side VPN template, BGP routes are advertised within OMP.

**Technical Tip** 

The templates associated within vManage NMS attached to the Cisco SD-WAN Edge devices are not updated with the additional configuration resulting from the loopback, IPsec connections and BGP routing to the host VNets. Instead, the configurations of the Cisco SD-WAN Edge devices within the transit VNet are dynamically modified by Cisco Cloud onRamp for IaaS. Because of this, you must exercise some caution if you wish to modify the configuration of the Cisco SD-WAN Edge routers within a transit VNet after you have mapped host VNets to it.

For example, if you add a BGP feature template to a service interface within the device template for the Cisco SD-WAN Edge router, you have to use BGP ASN 64600 in the feature template. This is the BGP ASN that Cisco Cloud onRamp for IaaS uses for the transit VNet when mapping host VNet to the transit VNet. Network devices can only be part of a single BGP ASN at one time.

#### Automated Bring-up of Transit VNet

At the time of configuring the cloud onRamp feature via the vManage GUI you must the region, choose the image, VM size and the appropriate chassis UUID to be associated with the virtual WAN Edge device to be provisioned within the new transit VNet.

 Software Image: In a vManage NMS running Cisco SD-WAN code 19.2/ 20.1, a virtual device within transit VNet can be automatically deployed running either of these Cisco SD-WAN code versions - 19.1, 18.4, 18.3, 18.2.

## Technical Tip

Cloud onRamp for laaS with Azure does not support the CSR1k. As of 19.2/20.1 vManage only vEdge Cloud devices can be successfully provisioned within the transit VNet.

• Size of WAN Edge Device: The size of a Virtual Machine (VM) within your transit VNet is selected at the time of deploying Cloud onRamp for laaS feature. Choose the size based on the overall workload that you want to support. The size that you choose then determines factors such as processing power, memory, and storage capacity. Azure offers a wide variety of sizes to support many types of uses. Azure charges an hourly price based on the VM's size and operating system.

vManage NMS running version 19.2.2, lets you choose between either of the following sizes for your WAN Edge device pairs hosted in your transit VNet. Both the sizes provide a high memory-to-core ratio.

#### Table 2. WAN Edge Virtual Device Sizes

Size	RAM	Core
Standard F8 (8 vCPU)	16GiB	8
Standard F4 (4 vCPU)	8GiB	4

For per size pricing details, refer to the Azure pricing chart.

Note: For this guide throughput has not been tested.

• Transit VNet CIDR: Within the Cisco Cloud onRamp workflow, specify an IPv4 CIDR block range for the transit VNet. The IPv4 CIDR range you configure is automatically sub-netted to create the necessary subnets within the transit VNet. Cisco Cloud onRamp automatically creates the Azure logical components such as the transit VNet, its associated subnets, network interfaces and publicly routable IP addresses.

By default, Azure proposes the CIDR - 10.0.0/16 to be used for the new transit VNet. It is best to avoid using such a large address block and rather divide this network into smaller chucks for each VNet. For this deployment, the CIDR for transit VNet is set to 10.0.1.0/24.

#### Mapping of a Host VNet to Transit VNet

For successful mapping of host VNet to the transit VNet, make sure to choose the appropriate service-side VPN label, a valid IPsec CIDR address, Azure acceptable BGP AS Numbers and host VNet gateway subnet.

 Choosing the Service-Side VPN: Mapping of a host VNet to a transit VNet is done per service-side VPN. You can either place all host VNets in the same VPN or leverage segmentation by placing host VNets in separate VPNs. As traffic across the SD-WAN overlay carries the VRF or VPN label details, LAN traffic from Data Centers (DCs) and branches can be configured to either communication only all VPNs or to a single VPN.

#### Technical Tip

When a host VNet is selected to be mapped to a transit VNet, it is mapped to only one service-side VPN within the Cisco SD-WAN WAN Edge device. However, a single service-side VPN can be mapped to multiple host VNets. The number of Host VNets supported per Cisco SD-WAN Edge virtual device pair depends on the overall throughput requirements.

IPsec Tunnel CIDR: Each Cisco WAN Edge virtual router in the transit VNet builds two site-to-site IPsec tunnels for redundancy to the Azure virtual network gateway (VNG) in the host VNet. Since there are two Cisco WAN Edge routers in the transit VNet, the total number of IPsec tunnels in the transit VNet is four. The IPsec tunnels that connect the WAN Edge routers in the transit VNet to the host VNet run IKE for secure connection. For Azure, the IPsec tunnels run IKE version 2.

The IPsec IP addresses must be network addresses in the /30 subnet, unique across the overlay network, and not a part of the host VNet CIDR. If they are part of the host VNet CIDR, Azure will return an error while attempting to create VPN connections to the transit VNet.

~	Y 😵 Failure System F		Failed to map gateway vpc/vnet	23 Sep 2020 2:24:05 PM PDT			
	[23-Sep-2020 14:40:25 PDT] Successfully created a Virtual Network Gateway						
	[23-Sep-2020 14:40:25 PDT] Creating Vpn conne [23-Sep-2020 14:40:26 PDT] Creating vpn conne	ctions ction for local network gateway : COR_COR_Spok	e_2_LNG_vedge1	1			
	[23-Sep-2020 14:40:27 PDT] Error with Creating VPN Connections : Azure Error: GatewayConnectionHasOverlappingAddressSpaces						
	Message: Virtual Network Gateway connection /subscriptions/5f70cd2b-baee-4c43-889a-71bb1e8a0efc/resourceGroups/AZ-IAAS/providers/Microsoft.Network/connections/C						
				^ ¥			

At this stage, you must also enter a /32 loopback address, which is used later during BGP peering. Ensure this IP address is unique.

 BGP ASN: Over secure IPsec tunnels, Cisco SD-WAN Edge routers establish BGP connectivity to the Host VNets Virtual Network Gateway (VNG) and exchanges BGP (Border Gateway Protocol) routes. WAN Edge virtual routers learn host VNet networks over BGP and redistribute routes into Overlay Management Protocol (OMP). By default, the BGP ASN number configured within the WAN Edge virtual devices is 64600. The BGP ASN you enter within the Cloud onRamp for laaS workflow is the BGP ASN assigned to the Virtual Network Gateway (VNG) associated with the host VNet. This ASN number can be any number acceptable within Azure cloud. To note the acceptable Azure BGP ASN number refer to the document - <a href="https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview">https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview</a>.

 Host VNet Gateway: The Host VNet Gateway Subnet is defined based on the overall subnet associated with the Azure host VNet. For example, if the host VNet subnet is defined as 10.25.2.0/24, then, the Host VNet Gateway Subnet is a subset of that such as 10.25.2.128/25. If the configured gateway subnet is invalid, Azure will return an error.

>	Status	Device IP	Message	Start Time	
~	🙁 Failure	System	Failed to map gateway vpc/vnet	23 Sep 2020 2:17:10 PM PDT	
	[23-Sep-2020 14:17:12 PDT] Mapping to host vm. [23-Sep-2020 14:17:12 PDT] Creating Gateway SN [23-Sep-2020 14:17:13 PDT] Could not create G Message: Subnet 'GatewaySubnet' is not valid [23-Sep-2020 14:17:13 PDT] Stopping mapping p [23-Sep-2020 14:17:13 PDT] Failed to map Host [23-Sep-2020 14:17:13 PDT] Failed to map gateway [23-Sep-2020 14:17:13 PDT] Failed to map gateway	et : AZ-Host-VNET-2 ubnet in AZ-Host-VNET-2 ateway Subnet : Was not able to create a gatew in virtual network 'AZ-Host-VNET-2'. rocess WNet : AZ-Host-VNET-2 way vpc/vnet	ay subnet in AZ-Host-VNET-2 :Azure Error: Net	fgInvalidSubnet	
				~ ~	

Once all the details are entered, the mapping process is initiated. A new gateway subnet is created in the host VNet, followed by a new Local Network Gateway (LNG) in Azure. Note, the LNG simply represents the WAN Edge virtual device in the network. A new Virtual Network Gateway (VNG) is created within the host VNet and this VNG is associated with the Host VNet's gateway subnet. Therefore, each VNG (associated with the host VNet) contains two public IP addresses for site-to-site VPN connection, private IP addresses, and a BGP ASN number for BGP peering.

In the transit VNets WAN Edge devices, logical IPsec tunnel interfaces are built within the chosen service-side VPN (E.g. VPN 1). The IPsec tunnel source is set to the VPN 0 Ge0/0 private IP address and the tunnel destination is set to the Virtual Network Gateway's (VNG's) public IP address. Within these devices two static routes are configured within the service-side VPN (For. E.g. VPN 1/ VPN 2), to route traffic to the Virtual Network Gateway (VNG) (10.25.2.133 and10.25.2.132) via the IPsec interfaces and establish BGP peering over the IPsec tunnel using the source of the WAN Edge device's loopback addresses.

In the example figure, segmentation is leveraged and the IPsec tunnel CIDR is configured in the range 192.168.x.x/30. For each of the WAN Edge device, tunnels sourced from the VPN0 Ge0/0 IP address (10.0.1.36) and VPN0 Ge0/0 IP address (10.0.1.37), with the destination set as VNG's public IP addresss (52.246.248.146 and 51.144.25.10).

Static routes are configured in both the WAN Edge device's service-side VPN, for reachability to the VNG's IP addresses (10.25.2.132 and 10.25.2.133), via the IPsec tunnel interfaces. Each WAN Edge device forms BGP neighbors with these VNG IP addresses (10.25.2.132 and 10.25.2.133) via loopback interface (1.1.1.1 and 2.2.2.2) configured during the mapping process.

Therefore, each WAN Edge router, neighbors with both the IP addresses of the Virtual Network Gateway.

- One BGP peering between the WAN Edge devices loopback IP and the IP address 1 (10.25.2.132) of Virtual Network Gateway.
- Another BGP peering between the WAN Edge devices loopback IP and the IP address 2 (10.25.2.133) of Virtual Network Gateway.

#### Figure 7. VPN Connections and BGP Peering



So, each mapped host VNet has a total of four BGP peers – two BGP peers configured on one Cisco SD-WAN Edge router, and two BGP peers configured on the other Cisco SD-WAN Edge router. Hence, there are four potential paths from the transit VNet to the host VNet.

These BGP routes are then re-distributed into OMP within the WAN Edge devices, which then advertises the OMP routes to the vSmart controllers in the domain. vSmart controllers act as a route reflector and sends the OMP routes as route updates to other WAN Edge devices part of the Cisco SD-WAN overlay. Therefore, establishing data plane communication between them and connectivity between the branch/ Datacenter to the Host VNet in Azure cloud.



Figure 8. BGP to OMP redistribution

Note, redistribution of OMP routes into BGP is not necessarily needed, as the WAN Edge devices advertise network 0.0.0.0/0 to the Virtual Network Gateway (VNG) within the host VNet.

#### **Technical Tip**

Cloud onRamp for laaS does not cover scenarios where the customer wants to include Security NVAs in their Cloud environment, and consequently, for such deployment's customers will need to build all laaS components and SD-WAN Edge routers manually (or via scripting using AWS CLI or Azure PowerShell).

Once the mapping process completes successfully, you still need to open all necessary ports within the Azure Network Security Groups (NSGs) associated with the WAN Edge virtual devices NIC modules hosted in the Azure transit VNet.

#### **Firewall Port Considerations**

Firewall ports are opened within the on-premise gateway firewall and within the Network Security Group (NSG) associated with the Azure WAN Edge devices to allow for the formation of secure sessions between the WAN Edge routers and the controllers.

Within the cloud onRamp workflow Azure Network Security Groups (NSGs) are automatically created and associated with the transit VNets network interface and they contain security rules that filter the network traffic to and from the device. These rules are classified as inbound security rules and outbound security rules. The inbound security rule allows or denies inbound network traffic to other resources, while the outbound security rule allows or denies outbound network traffic from other resources. For each rule, you can specify source and destination, port, and protocol.

Note, all NSGs have a set of default rules. These default rules cannot be deleted, but since they have the lowest possible priority, they can be overridden by the rules that you create. Note, by default no incoming or outgoing ports are open, you need to manually open these ports.

At a minimum the following UDP ports must be opened to establish control plane and data plane connections.

Source Device	Security Rules
WAN Edge (DTLS)	UDP 12346+n, 12366+n, 12386+n, 12406+n, and 12426+n, where n=0-19 and represents the configured offset

Table 3. UDP ports for SD-WAN device connections

For more details regarding firewall port considerations, please refer to the Cisco SD-WAN Design Guide.

#### Cisco Cloud onRamp for laaS Workflow

The order of workflow for the Cloud onRamp for laaS feature is explained below, along with concurrent real time audit logs collected from the vManage GUI.

Template Built: Within the Cloud onRamp for laaS workflow, feature and device templates are built and the WAN Edge serial numbers are validated.

Basic Information		Transport & Management VPN		Service VPN  Service VPN						
	System *	System_Template_Transit	•	VPN 0 *	Azure_Transit_VPN0_Template		VPN	Azure_Transit_VPN1_Template	•	
	Logging*	Logging_Template	•	VDN Interface	Anne Tree is UDIO Interfere		VPN Interface	VPN1_Lo0		Sub-Templates 👻
	NTP	NTP_Template	- 0	VENIMENACE	Azure_Iransit_VPNU_Interface					
-										
	AAA *	AAA	•				-			
	BFD *	Azure_Transit_BFD_Template	•	VPN 512 *	Azure_Transit_VPN512_Template					
	OMP *	OMP_Template	•	VPN Interface	Azure_Transit_VPN512_Interface		VPN	Azure, Transit, VPN2, Template	•	
	Security *	Security_Template	•							

When WAN Edge serial numbers are validated the device serial list is pushed and processed into vBond, vManage, vSmart.



Template Push: The device template is attached to the WAN Edge virtual devices and the device template is pushed into the devices. During this step the following occurs,

• Device Validation: During device validation, the vManage checks if the WAN Edge device scheduled for template push is active. In the following example, the WAN Edge devices are validated.

WAN Edge Device 1: Chassis-ID - bc6827c6-041a-4afa-806d-433efcd2ed7f

```
WAN Edge Device 2: Chassis-ID - e6bad40d-afec-4ce7-87d2-c23a08bafcd4
```

```
Starting Checks.
Validating if device scheduled for template push are active
DeviceIP: -, uuid: bc6827c6-041a-4afa-806d-433efcd2ed7f is not connected to vManage
DeviceIP: -, uuid: e6bad40d-afec-4ce7-87d2-c23a08bafcd4 is not connected to vManage
Sending message to vmanage:172.27.0.14
Published messages to vmanage(s)
Checks completed.
```

• The device template is attached to the device. Since the WAN Edge devices are yet to be configured and deployed using the Cloud onRamp for laaS workflow, the devices are currently offline and unreachable.

```
Configuring device with feature template: OnRamp_Transit_WAN_edge_Template
Generating configuration from template
Checking and creating device in vManage
Device is offline
Updating device configuration in vManage
Configuration template OnRamp_Transit_WAN_edge_Template scheduled to be attached when
device comes online. To check the synced state, click Configuration > Devices > Device
Options
```

Bootstrap Configuration File: At this stage a minimum cloud–INIT bootstrap configuration file is also generated from the vManage for the WAN Edge virtual devices. This bootstrap configuration file consists of a one-time password (OTP) token needed for the WAN Edge device authentication and validation. In the following example, bootstrap configuration files are generated for the vEdge cloud devices with Chassis-ID - bc6827c6-041a-4afa-806d-433efcd2ed7f and Chassis-ID - e6bad40d-afec-4ce7-87d2-c23a08bafcd4.

Bootstrap config generated for vEdge cloud-ead1954a-087e-4571-b747-0665fb330406 Bootstrap config generated for vEdge cloud-0d777876-18a4-4elf-ba0d-2297ba6d5185

Note, at this stage the devices are still not up and running, with the required configuration and certificates.

vManage Azure API Access: For programmatic access from the vManage NMS to the Azure account, the Tenant ID, Client ID, Secret Key and Subscription ID associated with your Azure account are entered.

Note, these credentials are saved for API access into the Azure account.

Successfully saved credentials for accountId:5f70cd2b-baee-4c43-889a-71bb1e8a0efc

Creation of Gateway VNet Process: vManage NMS builds Azure constructs through API calls:

 At first a new resource group is provisioned. Within the resource group, the transit VNet is deployed in the selected Azure location and associated to the same account ID/ subscription ID entered for access from vManage to Azure.

```
Creating transit VPC/VNet: COR_TransitVNet
Creating Transit Vnet in westus2 under subscription 5f70cd2b-baee-4c43-889a-
71bble8a0efc
Resource Group Name: COR TransitVNet
```

· Resources deployed within the resource group include,

```
    An availability set in which the WAN Edge virtual devices are to be provisioned
```

```
Creating Resources - This can take up to 10 minutes
Created resource : COR TransitVNet AvailabilitySet
```

- Network Security Groups (NSG) where ports and IP addresses are either allowed or denied access
   Created resource : COR TransitVNet NSG
- Subnet, IP addresses and virtual network modules for VPN 512 and VPN 0 network interfacesare deployed.

Within transport VPN 0, an interface is configured with both public and private IPs Within management VPN 512, an interface is configured with both public and private IPs.

At this point no logical IPsec interfaces are configured within the service-side VPN.

```
Created resource : GatewayVedge1 management ip
Created resource : GatewayVedge1 transport ip
Created resource : GatewayVedge2 management ip
Created resource : GatewayVedge2 transport ip
Created resource : COR TransitVNet
Created resource : GatewayVedge1
Created resource : GatewayVedge2
Created resource : GatewayVedge1 management nic
Created resource : GatewayVedge1 service nic
Created resource : GatewayVedge1 transport2 nic
Created resource : GatewayVedge1 transport nic
Created resource : GatewayVedge2 management nic
Created resource : GatewayVedge2 service nic
Created resource : GatewayVedge2 transport2 nic
Created resource : GatewayVedge2 transport nic
Created resource : GatewayVedge2 osdisk
Created resource : GatewayVedge1 osdisk
Gateway VNet creation process finished successfully : COR TransitVNet
```

Mapping Host VNet to Transit VNet: Within the Cloud onRamp for IaaS workflow, at first you map a single host VNet to the transit VNet.

Cisco Cloud onRamp for laaS uses Azure APIs to automatically create a gateway subnet within the Azure host VNet, followed by the creation of Local Network Gateway (LNG). Note, each LNG in the functions as a WAN Edge virtual router.

A Virtual Network Gateway (VNG) is deployed in the host VNet and a redundant pair of site-to-site VPN connections are established between the Local Network Gateway (LNG) and the Virtual Network Gateway (VNG). Each Azure Site-to-Site VPN connection consists of a pair of IPsec tunnels established to the same Local Network Gateway (LNG). Therefore, a total of four IPsec tunnels is established from each host VNet to the transit VNet.



Figure 9. Local Network Gateway and Virtual Network Gateway

The Azure Site-to-Site VPN Connections are mapped to the WAN Edge routers in the transit VNet, through the service-side VPN of the WAN Edge routers.

IPsec protected logical tunnel interfaces are automatically configured in the service VPN between the Cisco SD-WAN Edge routers and the IPsec endpoints of the Azure Site-to-Site VPN Connections associated with the Azure Virtual Network Gateway (VNG) at the host VNet.

Static routes and BGP AS number 64600 are configured in the service-side VPN in the WAN Edge virtual routers placed in the transit VNet, along with network 0.0.0/0 (static null 0) advertised to the BGP neighbor definitions corresponding to the endpoints of the Azure Site-to-Site VPN Connections in the Azure Virtual Network Gateway (VPN GW) at the host VNet. These BGP routes are redistributed into OMP.

The Audit Logs that correspond to this workflow is as given below. Here the transit VNet is mapped to the host VNet COR\_Spoke\_1.

```
Mapping Host VNet in 5f70cd2b-baee-4c43-889a-71bble8a0efc to Transit VNet in 5f70cd2b-
baee-4c43-889a-71bble8a0efc
Location : westus2
Mapping to host vnet : COR_Spoke_1
Creating Gateway Subnet in COR_Spoke_1
Creating local network gateways
Creating COR_COR_Spoke_1_LNG_vedge1
Created local network gateway : COR_COR_Spoke_1_LNG_vedge1
Creating COR_ COR_Spoke_1_LNG_vedge2
Created local network gateway : COR_ COR_Spoke_1_LNG_vedge2
Creating Virtual Network Gateway. This could take up to 45 minutes
Successfully created a Virtual Network Gateway
Creating vpn connections
Creating vpn connection for local network gateway : COR_COR_Spoke_1_LNG_vedge1
Created VPN Connection COR_COR_Spoke_1_vpnConnection_vedge1_vng
```

```
Creating vpn connection for local network gateway : COR_COR_Spoke_1_LNG_vedge2
Created VPN Connection COR_COR_Spoke_1_vpnConnection_vedge2_vng
Finished mapping Host VNet COR Spoke 1
```

Device Validation: Device validation occurs again and vManage checks if the WAN Edge devices scheduled for template push is active.

WAN Edge Device 1: Chassis-ID - bc6827c6-041a-4afa-806d-433efcd2ed7f

WAN Edge Device 2: Chassis-ID - e6bad40d-afec-4ce7-87d2-c23a08bafcd4

```
Starting Checks.
Validating if device scheduled for template push are active
DeviceIP: -, uuid: bc6827c6-041a-4afa-806d-433efcd2ed7f is not connected to vmanage
DeviceIP: -, uuid: e6bad40d-afec-4ce7-87d2-c23a08bafcd4 is not connected to vmanage
Sending message to vmanage:172.27.0.14
Published messages to vmanage(s)
Checks completed.
```

Note, the logs show that the devices are not connected to vManage yet, as all the necessary UDP/ TCP ports must be opened within the,

- Azure Network Security Group (NSG) associated to the NIC of each WAN Edge device
- On-premise gateway firewall for device authentication.

vManage as CA: Once the firewall ports are open and return routes are configured, the WAN Edge devices use the cloud-init file generated by the vManage during the bootstrap process to authenticate itself to vBond and form control connections with vManage and vSmart. During this process, the following processes occur.

Cisco vManage acts as a certificate authority (CA), handing the Cisco SD-WAN Edge device a certificate.
 vManage generates CSR for both the WAN Edge devices.

```
CSR generated for WAN edge
UUID: e6bad40d-afec-4ce7-87d2-c23a08bafcd4
Device IP: 10.1.0.137
```

• The generated CSR is signed by vManage for the WAN Edge devices.

```
CSR Signed by vManage-b8a4fa09-bf86-4b1a-bb9e-9eb80f365226for vEdge cloud-e6bad40d-afec-4ce7-87d2-c23a08bafcd4
```

 Then root cert chain file is transferred and installed into both the vEdge cloud devices from vManage NMS.

```
Transferred root cert chain file to vEdge
UUID: e6bad40d-afec-4ce7-87d2-c23a08bafcd4
Device IP: 10.1.0.137
Installed root cert chain on vEdge
UUID: e6bad40d-afec-4ce7-87d2-c23a08bafcd4
Device IP: 10.1.0.137
```

• Certificate installation is completed on the WAN Edge device.

```
Certificate Installation successful for vEdge cloud by vManage-b8a4fa09-bf86-4b1a-bb9e-
9eb80f365226
```

```
UUID: e6bad40d-afec-4ce7-87d2-c23a08bafcd4
```

```
Device IP: 10.1.0.137
Certificate signed by vManage: b8a4fa09-bf86-4b1a-bb9e-9eb80f365226
```

The Cisco SD-WAN Edge device then uses this certificate to re-authenticate to vBond and establish
permanent control connections to vManage and vSmart. Once the control connections are established,
vSmart updates the Cisco SD-WAN Edge device with policy information, OMP routing information and
IPsec keys for establishing connections to other Cisco SD-WAN Edge devices, etc. This ends the cloud
onRamp for laaS workflow.

#### **Mapping Additional Host VNets to Transit VNet**

Once the Cloud onRamp for IaaS workflow is complete, you can optionally map additional host VNets to the transit VNet. This provides connectivity between the host VNets. Alternatively, individual host VNets can be mapped to separate SD-WAN service VPNs at the transit VNet - if network segmentation is required.

Here's the overall illustration of a scenario in which two host VNets are mapped to the same transit VNet.



## Prerequisites - Cisco Cloud onRamp for IaaS using Azure

The processes explained in the prerequisites section are as given below:

Process 1: Azure Prerequisites

Process 2: vManage NMS and Transit VNet Prerequisites

## **Process 1: Azure Prerequisites**

#### **Procedure 1: Check Resource Usage limits**

Check the Azure limits associated with your account (by going to your subscription in the portal to ensure that the following resources can be created in your account:

- 1 VNet, which is required for creating the transit VNet
- 1 Availability set, required for Virtual Machine distribution in the transit VNet
- 6 Static Public IP addresses associated with the transit vEdge Cloud routers
- 1 Azure Virtual Network Transit and 2 Static Public IP Addresses for each host VNet
- 4 VPN connections for mapping each host VNet

#### Step 1. Log into the Azure portal.

#### Step 2. Navigate to Subscriptions and select Usage + quotas.

Home > Subscriptions > Microsoft Azure Enter	Microsoft Azure En	ternrise      sage + quotas				×
	Subscription					~
+ Add	✓ Search (Cmd+/) «	Զ Request Quota Increase 🜔 Refresh	1			
View list of subscriptions for which you have role-based access control (RBAC) permissions	Security	You can use each Microsoft Azure resource increase via Help + Support. Learn more	e up to its quota. Each subscription has se	parate quotas and usage is tracked per subs	cription. If you reach a quota cap, you can request an	Request Increase
subscriptions for which you have billing	Cost Management	All service quotas	All providers	All locations	Show only ite	ms with usage
Showing subscriptions in Cisco-ENB-SDWAN	🗞 Cost analysis	Filter items				
directory. Don't see a subscription? Switch directories	Cost alerts					
My role  Status	③ Budgets	Quota Tu	Provider	↑↓ Location	h↓ Usage	¢↓
8 selected V 3 selected V	Advisor recommendations	Standard Sku Public IP Addresses	Microsoft.Network	East US 2	0 %	5 3 of 1000
Apply	Billing	Standard Sku Public IP Addresses	Microsoft.Network	UK South	0 %	5 3 of 1000
Showing 1 of 1 subscriptions Slobal Show only subscriptions selected in the	80. Bastass information	Static Public IP Addresses	Microsoft.Network	UK South	0 %	5 3 of 1000
subscriptions filter ①	X Partier information	Virtual Networks	Microsoft.Network	East US 2	0 %	5 3 of 1000
Schereleting and As	Settings	Virtual Networks	Microsoft.Network	France Central	0 %	5 3 of 1000
Subscription name TU	Programmatic deployment	Virtual Networks	Microsoft.Network	Southeast Asia	0 %	5 3 of 1000
Microsoft Azure Enterprise ••••	<ul> <li>Resource groups</li> </ul>	Virtual Networks	Microsoft.Network	UK South	0 %	5 3 of 1000
	Resources	Standard Av2 Family vCPUs	Microsoft.Compute	Southeast Asia	0 %	5 1 of 350
	🗮 Usage + quotas	Total Regional vCPUs	Microsoft.Compute	Central India	0 %	5 2 of 768
	Policies	Network Security Groups	Microsoft.Network	East US 2	0 %	5 13 of 5000
	🐖 Management certificates	Network Security Groups	Microsoft.Network	Central US	0 %	5 11 of 5000
	A My permissions	Network Security Groups	Microsoft.Network	East US	0 %	5 11 of 5000
	S Resource providers	Public IP Addresses	Microsoft.Network	West Central US	0 %	5 2 of 1000
	Deployments	Standard Sku Public IP Addresses	Microsoft.Network	West US	0 %	6 2 of 1000
	Properties	Static Public IP Addresses	Microsoft.Network	West Central US	0 %	6 2 of 1000
	A Resource locks	Virtual Networks	Microsoft.Network	Central India	0 %	5 2 of 1000
	Automation	Virtual Machines	Microsoft.Compute	West US 2	0 %	5 45 of 25000
	🗲 Events	Network Interfaces	Microsoft.Network	West US 2	0 %	5 109 of 65536

#### **Procedure 2: Deploy Resource Groups on Azure**

The resource group is a container that includes all the resources for the solution, or only those resources that you want to manage as a group. This resource group contains the Host VNet, any associated Network Security Groups (NSGs), subnets among others.

In this deployment Resource Group AZ-IAAS is deployed in West US 2.

Step 1. Navigate to **Home > Resource groups**.

Step 2. Within the resource group, create a new resource group. Here, set the **Subscription** type, enter a name for the new **Resource Group** and enter the **Region** under resource details. Click on **Review + Create**.

Home > Resource groups >		
Create a resource grou	IP	×
Basics Tags Review + create		
Resource group - A container that holds re resources for the solution, or only those re allocate resources to resource groups base	elated resources for an Azure solution. The resource group can include all the sources that you want to manage as a group. You decide how you want to do not not not not not not not not not no	
Project details		
Subscription *	Microsoft Azure Enterprise 🗸 🗸	
Resource group * ()	AZ-IAAS	
Resource details		
Region * ()		
Review + create < Previous	Next: Tags >	

#### **Procedure 3: Deploy Host VNets within the Resource Group**

A host VNet is a customer-owned virtual network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. Each host VNet you create has its own CIDR block and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap.

Step 1. Navigate to **Home > Virtual Networks**.

Step 2. Under the section **Basics**, choose your Azure **Subscription** and the newly created **Resource Group**. Next, Enter Instance details, such as the instance **Name** and choose the location/ **Region** in which the instance will be deployed. The new VNet COR\_Spoke\_1 is deployed within this Resource Group

Step 3. Select **Next: IP Addresses >** to specify the virtual networks address space.

Home > Virtual networks >		
Create virtual network		×
Basics IP Addresses Security	Tags Review + create	
Azure Virtual Network (VNet) is the funda Azure resources, such as Azure Virtual Ma networks. VNet is similar to a traditional n benefits of Azure's infrastructure such as	mental building block for your private network in Azure. VNet enables many types of chines (VM), to securely communicate with each other, the internet, and on-premises tework that your do operate in your own data center, but brings with it additional scale, availability, and isolation. Learn more about virtual network	
Project details		
Subscription * ①	Microsoft Azure Enterprise	
Resource group * ①	AZ-IAAS V	
	Create new	
Instance details		
Name *	COR_Spoke_1	
Region *	(US) West US 2 V	
Review + create	< Previous Next : IP Addresses > Download a template for automation	

Generally, Azure proposes use 10.0.0.0/16 as the CIDR. Try to avoid using this and divide the subnet into smaller chucks. In this guide, host VNet CIDR address space is set as 10.25.2.0/24 and subnet within this CIDR is defined as 10.25.2.0/25.

Step 4. Under the **IP Addresses** section, enter your host VNet CIDR address space under **IPv4 address** space.

Step 5. Click on the + Add subnet to add the new Subnet name and Subnet address range. Then, click Add.

Step 6. Review all the changes made and click Next: Security >.

Home > Virtual networks >	Add subnet ×
Create virtual network	
Basics IP Addresses Security Tags Review + create The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24). IPV4 address space 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Subnet name * Workload Subnet Subnet address range *  1025.20/25 10.25.2.0 - 10.25.2.127 (123 + 5 Azure reserved addresses) SERVICE ENDPOINTS Create service endpoint policies to allow traffic to
Add IPv6 address space ①         The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.         2 + Add subnet ③ Remove subnet	Create service endpoint pointes to allow value. to specific azure resources from your virtual network over service endpoints. Learn more Services ① 10 selected Filter services
Subnet name Subnet address range	Select all
This virtual network doesn't have any subnets.	Microsoft.AzureActiveDirectory
This virtual network doesn't have any subnets.	<ul> <li>Microsoft AzureCosmosDB</li> <li>Microsoft CognitiveServices</li> <li>Microsoft ContainerRegistry</li> <li>Microsoft LeventHub</li> <li>Microsoft LeventHub</li> <li>Microsoft ServiceBus</li> <li>Microsoft ServiceBus</li> <li>Microsoft Storage</li> <li>Microsoft Hveb</li> </ul>
Review + create         Vext : Security >         Download a template for automation         5	Add Cancel

You can also enable **Security** features such as DDoS Protection, Firewall etc. and associate **Tags** to the VNet based on your network. In this deployment, these features were kept default.

Step 7. Review all the changes made and click **Create**.

Home > Virtual networks >		
Create virtual net	twork	×
Validation passed		
Basics IP Addresses Se	ecurity Tags Review + create	
Basics		
Subscription	Microsoft Azure Enterprise	
Resource group	AZ-IAAS	
Name	COR_Spoke_1	
Region	West US 2	
IP addresses		
Address space	10.25.2.0/24	
Subnet	Workload_Subnet (10.25.2.0/25)	
<b>T</b> =		
Tags		
psayinat	Test-bed	
Convolta.		
Security		
BastionHost	Disabled	
DDoS protection plan	Basic Distribut	
riiewali	nanist	
Create	< Previous Next > Download a template for automation	

Note: The Virtual Network Gateways are automatically added once Cisco Cloud onRamp for laaS feature is enabled. You need not deploy it using Azure services.

#### Procedure 4: Deploy Virtual Machines hosted within the host VNets on Azure

Any Azure Instance (s) can be deployed within the Host VNet.

Step 1. Launch the Microsoft Azure portal.

Step 2. Navigate to Home > Virtual Machine and create a VM in the host VNet COR\_Spoke\_1.

Home > Virtual machines >		
Create a virtual machir	ne	$\times$
Basics Disks Networking Ma	anagement Advanced Tags Review + create	
Create a virtual machine that runs Linux o image. Complete the Basics tab then Revi for full customization. Learn more 🗗	or Windows. Select an image from Azure marketplace or use your own customized iew + create to provision a virtual machine with default parameters or review each tab	
Project details		
Select the subscription to manage deploy your resources.	yed resources and costs. Use resource groups like folders to organize and manage all	
Subscription *	Microsoft Azure Enterprise	
Resource group * ①	AZ-IAAS V	
	Create new	
Instance details		
Virtual machine name * 🕕	Workload	
Region * ①	(US) West US 2 V	
Availability options	No infrastructure redundancy required	
Image * 🕕	Ubuntu Server 18.04 LTS V	
	Browse all public and private images	
Azure Spot instance ①	Ves  No	
Size * 🕕	Standard_F8 - 8 vcpus, 16 GiB memory (US\$290.54/month)	
	Select size	
Administrator account		
Authentication type	SSH public key  Password	
Review + create < Prev	vious Next : Disks >	

During this process you can create a new subnet or choose the subnet created earlier, also create new public IPs and associate new Network Security Groups (NSG) to the devices virtual Network Interface Cards (NIC) within the Networking tab.

Home > Virtual machines >	
Create a virtual machin	ne
Basics Disks Networking Ma	anagement Advanced Tags Review + create
Define network connectivity for your virtu ports, inbound and outbound connectivit Learn more	ual machine by configuring network interface card (NC) settings. You can control y with security group rules, or place behind an existing load balancing solution.
Network interface	
When creating a virtual machine, a netwo	rk interface will be created for you.
Virtual network * ①	COR_Spoke_1 V Create new
Subnet * 🕕	Workload Subnet (10.252.0/25) V
	Manage subnet configuration
Public IP ①	(new)kokada1-ip
NIC network security group ①	None     Basic <ul> <li>Advanced</li> </ul>
Configure network security group *	(new) Workload1-nsg V
	Create new
Accelerated networking ①	
Load balancing	
You can place this virtual machine in the	backend pool of an existing Azure load balancing solution. Learn more
Place this virtual machine behind an existing load balancing solution?	🔿 Yes 💿 No
Review + create < Pre	vious Next : Management >

#### **Procedure 5: Gather Subscription ID**

One of the four IDs needed to provide the vManage with programmatic access to your Azure Subscription is the Subscription ID.

Note, the Subscription ID is a GUID that uniquely identifies your **subscription** to use **Azure** services.

Step 1. Navigate to Subscriptions service and click on the three dots located on the right side of the page (...)

All services > Subscriptions					
Subscriptions					Documentation ♂ ☆ ×
+ Add					
Showing subscriptions in Don't see a s	ubscription? Switch directories				
My role 🗊		Status 🕕			
8 selected		✓ 3 selected			$\sim$
Apply					
Showing 1 of 1 subscriptions Show only subscriptions	selected in the global subscriptions filter ①				
Subscription name	U Subscription ID	↑↓ My role	↑↓ Current cost	Status	↑↓
Microsoft Azure Enterprise	5f70cd2b-baee-4c43-889a-71bb1e8a0efc	Contributor	1000	Active	

Step 2. Copy the **Subscription ID** to a notepad.

All services > Subscriptions > Microsoft Azure Enter	rprise		
Subscriptions « × Cisco-ENB-SDWAN	Microsoft Azure Enterpris	se	\$ X
+ Add		${egin{array}{c} & \\ & \\ & \\ & \\ & \\ & \\ & \\ & \\ & \\ & $	
Showing subscriptions in Cisco-ENB-SDWAN, Don't see a subscription? Switch directories My role O Status O 8 selected V 3 selected V Apply Showing 1 of 1 subscriptions global	Overview     Activity log     Activity log     Access control (IAM)     Tags     Diagnose and solve problems	Subscription ID : \$770cd2b-base-4c43-889a-71bb1e8a0efc       Subscription name       : Microsoft Azure Enterprise         Directory       :       Current billing period       : \$1/2020-5/31/2020         My role       : Contributor       Currency       : USD         Offer       : Enterprise Agreement       Status       : Active	
Show only subscriptions selected in the subscriptions filter ○ Subscriptions filter ○ Subscription na ↑↓ Subscription ID ↑. Microsoft Azure Ente 5f70cd2b-baee-4c4:	<ul> <li>Security</li> <li>Events</li> <li>Cost Management</li> <li>Cost analysis</li> <li>Budgets</li> <li>Advisor recommendations</li> <li>Billing</li> <li>Pag, Partner information</li> </ul>	Costs by resource	
	Settings	Spending rate and forecast	

 Table 4.
 Gathered 1 out of 4 values needed during the Cloud onRamp Workflow

Section	Value
Tenant ID	
Subscription ID	5f70cd2b-XXXX- XXXX - XXXX - XXXX XXXX XXXX
Client ID	
Secret Key	

#### **Procedure 6: Application Registration**

In Azure, application objects describe the application to the Azure AD, allowing the service to know how to issue tokens to the application based on its settings. These objects can be created in multiple ways, the chosen method here is that of Application Registrations in Azure portal.

#### Sub-Procedure 1: Check Azure AD Permissions

You must have sufficient permissions to register an application with your Azure AD tenant, and to assign the application a role in your Azure subscription.

Step 1. Select Azure Active Directory, and note your role. Only roles with admin privileges can register applications in your Azure AD tenant.

For details on Azure roles refer to the Azure roles and privileges guide.

Home >	Overview		
Overview	≪ Switch tenant ॥ Delete tenant + Cre	eate a tenant 📝 What's new 🛛 🐱 Preview	features 🛛 🛇 Got feedback?
🖋 Getting started	<ul> <li>Azure Active Directory can help you enable rei</li> </ul>	mote work for your employees and partners. Learn m	ore
<ul> <li>Preview hub</li> <li>Diagnose and solve problems</li> </ul>	Cisco-ENB-SDWAN		
Manage			
<ul> <li>Users</li> <li>Groups</li> </ul>	Tenant information	Second Azure AD Connect	
External Identities	Your role	Status	
Administrative units	License	Last sync	
<ul> <li>Enterprise applications</li> <li>Devices</li> </ul>	Tenant ID f95/d3f42_fe02_4r16_8f7/d_4f126	Sync has never run	
App registrations	Primary domain		
<ul> <li>Identity Governance</li> <li>Application proxy</li> </ul>			
🔓 Licenses	Sign-Ins		
Azure AD Connect			
두 Custom domain names			Only global administrators, security administrators, security
Mobility (MDM and MAM)			readers, and report readers can view sign-ins. More info to
Password reset			Tour role Application developer
Company branding			

#### **Technical Tip**

If you assigned User role, you must make sure that non-administrators can register applications.

If it is set to User role, then select User settings and check the **App registrations** setting. This value can only be set by an administrator. If set to **Yes**, any user in the Azure AD tenant can register an app. If the app registrations setting is set to No, only users with an administrator role may register these types of applications. See <u>available roles</u> and <u>role permissions</u> to learn about available administrator roles and the specific permissions in Azure AD that are given to each role.

Also, If your account is assigned the User role, but the app registration setting is limited to admin users, ask your administrator to either assign you one of the administrator roles that can create and manage all aspects of app registrations,

or to enable users to register apps.				
Home >				
Azure Active Directory	V User settings			
Administrative units	뒶 Save X Discard			
Enterprise applications	Enterprise applications			
Devices	Manage how end users launch and view their applications			
App registrations				
Identity Governance	App registrations			
Application proxy	Users can register applications ①			
Licenses				
Azure AD Connect	Administration portal			
Custom domain names	Restrict access to Azure AD administration portal			
Mobility (MDM and MAM)     Passward reset	Ves No			
Company branding				
83 User settings	LinkedIn account connections			
Properties	Allow Users to connect them who of knowledge used with the second of the second with the second s			
Security	Ves Selected group No			
Monitoring				
Sign-ins	External users			
Audit logs	manufactore construction of the data			
Provisioning logs (Preview)	User feature previews			
🤗 Logs	Manage user feature preview settings			
Diagnostic settings				
Workbooks				
📫 Usage & insights				
Troubleshooting + Support				
🕎 Virtual assistant (Preview)				
New support request				

#### Sub-Procedure 2: Check Subscription Permissions

As explained previously, when you have applications that needs to access or modify resources, you create an identity for the application. This identity is known as a service principal. Access to resources are restricted by the roles assigned to your service principal, giving you control over which resources can be accessed.

Therefore, after having verified your role and privileges associated with the Azure AD, also make sure your Azure subscription account has Microsoft.Authorization/\*/Write access to assign a role to an Azure AD application. This action is associated only with the Owner role or User Access Administrator role. If your account is assigned the Contributor role, you do not have adequate permission. You will receive an error when attempting to assign the service principal a role.

Step 1. Select the **subscription** you want to create the service principal in and select **My permissions**. Then, select **Click here to view complete access details for this subscription**.



Step 2. Select **View my access** to view your assigned roles, and determine if you have adequate permissions to assign a role to an AD app. If not, ask your subscription administrator to add you to **User Access Administrator** role. In the following image, the user is assigned the **User Access Assignment** role, which means that user has adequate permissions.

Home > Microsoft Azure Enterprise			@cisco.co	om assignments	- Microsoft Azure	e Enterprise	×
A Microsoft Azure Enterprise   Access control (IAM)		Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope					
O Search (Cend : 0	Add	Defrech					
Search (Cmd+/)	Add 🔮 Download role assignments == Edit columns 🔿 r	kerresn   🔨 kerno	pearch by assignment name or	description			
Overview	My access		Role assignments (2) ①				
Activity log	View my level of access to this resource.	Grant access to	Role	Description	Scope	Group assignment	
Access control (IAM)	View my access	Grant access to res	Contributor	Grants full access to mana	ge all This resource		
Tags	Check access		User Access Administrator	Lets you manage user acco	ess to This resource	**	
Diagnose and solve problems	Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more B		Denv assignments (0)				
Security	Find ①	Add role assig	Deny assignments (0)				
Cost Management	User, group, or service principal		Classic administrators (0) ①				
🗞 Cost analysis	Search by name or email address	View access to					
Cost alerts		View the role assig other resources.					
③ Budgets							
Advisor recommendations							
Billing		View					
<sup>9</sup> A Partner information		View deny assi					
Settings		View the role assig					
Programmatic deployment		access to specific a					
Resource groups							
Resources		View					
🖽 Usage + quotas							
Policies		Create a custo					
Management certificates		Create a custom ro					
A My permissions		organization.					
≆ Resource providers							
Deployments		Add					
Properties							

Sub-Procedure 3: Register an Application with Azure AD and Create a Service Principal Step 1. To create an application ID, select Azure Active Directory and in the sub-menu, click App registrations.

#### Step 2. Click New registration.

Home > Cisco-ENB-SDWAN   App registrations							
Cisco-ENB-SDWAN   App	o registrations			× \$\$			
Source directory	+ New registration	ng 🛇 Got feedback?					
>> search (Cmd+/)							
0 Overview	We come to the new and improved App registrations (now Generally Available), see what's new and learn more on now it's changed. →						
🚀 Getting started	All applications Owned applications						
X Diagnose and solve problems	P Start typing a name or Application ID to filter these results						
Manage	Display name	Application (client) ID	Created on	Certificates & secrets			
🚨 Users							
A Groups							
Organizational relationships							
& Roles and administrators							
Administrative units (Preview)							
Enterprise applications							
Devices							
App registrations							
Identity Governance							
Application proxy							
🛔 Licenses							
Azure AD Connect							
🐖 Custom domain names							
Ø Mobility (MDM and MAM)							
📍 Password reset							
Company branding							
Ø User settings							
Properties							
Security							

Step 3. In the Name field, enter a descriptive name such as **CloudonRamplAASGuide**. The rest of the tabs can be left as default. After setting the values, select Register.

Home > Cisco-ENB-SDWAN   App registrations > Register an application					
Register an application					
* Name					
The user-facing display name for this application (this can be changed later).					
CloudOnRampIAASGuide					
Supported account types					
Who can use this application or access this API?					
Accounts in this organizational directory only (Cisco-ENB-SDWAN only - Single tenant)					
Accounts in any organizational directory (Any Azure AD directory - Multitenant)					
O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)					
Help me choose					
Redirect URI (optional)					
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.					
Web     V       https://cloudonrampazure     V					
By proceeding, you agree to the Microsoft Platform Policies 👩					
Banister					

You've created your Azure AD application and service principal.

#### Sub-Procedure 4: Assign Contributor role to the Application

To access resources in your subscription, you must assign a role to the application. You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of scope.

vManage NMS uses the values gathered to access Azure via REST API, and to enable this we need to set up appropriate permissions or access privileges. The Owner, Contributor, Reader and User Access Administrator are the four fundamental built-in roles. For example, adding an application to the **Contributor** role means granting it full access to manage all resources, but this does not allow you to assign roles in Azure RBAC.

The built-in role Contributor is used here that lets you access and manage everything except granting access to resources.

Step 1. In the Azure portal, select the level of scope you wish to assign the application to. Therefore, navigate to **All services > Subscriptions > Microsoft Azure Enterprise | Access Control (IAM)** 

Step 2. To retrieve Azure credentials, you must create an **App Registration** in Azure with **Contributor** privileges. To do so, click on **Access control (IAM)** from the left side and click on the **+ Add** to select **Add role assignment**.

All services > Subscriptions > Microsoft Azure Enterprise   Access control (IAM)						
Subscriptions « ×	Microsoft Azure Enterpris	e   Access control (IAM)	$\times$			
+ Add		+ Add == Edit columns 🖒 Refresh   X Remove   🛇 Got feedback?				
Showing subscriptions in Cisco-ENB-SDWAN. Don't see a subscription? Switch directories My role ① Status ①	Overview     Activity log	Add role assignment Its Deny assignments Classic administrators Roles				
8 selected V 3 selected V Apply	Access control (IAM)     Tags	Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more et				
Showing 1 of 1 subscriptions global Show only subscriptions selected in the subscriptions filter ①	<ul> <li>Diagnose and solve problems</li> <li>Security</li> </ul>	Find ①     Grant access to resource at this scope by assigning a role to a user, group, service principal       Azure AD user, group, or service principal     v				
Search to filter items	Events	Image: Contract of the second seco				
Subscription na 75 Subscription ID 7. Microsoft Azure Ente 5f70cd2b-baee-4c4:	Cost Management	cloud_onramp.jaas				
	<ul> <li>Budgets</li> <li>Advisor recommendations</li> </ul>	Cloudomamp-test View the users, groups, service principals and managed identities that have role assignments granting them access at this				
	Billing	CloudOnRampIAASGuide View Learn more 🖉				
	Settings	View denv assignments				
	<ul> <li>Programmatic deployment</li> <li>Resource groups</li> </ul>	View the users, groups, service principals and managed identities that have been				
	<ul> <li>Resources</li> <li>Usage + quotas</li> </ul>	dened access to specific actions at this scope.				
	Policies	View Learn more 2*				
	A My permissions	Create a custom role Create a custom role for Azure resources				
	E Resource providers	with your own set of permissions to meet the specific needs of your oraanization.				

Step 3. From the **Role** drop-down menu, select **Contributor**.

Step 4. From the **Assign access to** drop-down, select the default value **Azure AD user, group, or service principle**.

Step 5. In the **Select** tab, enter the name of the Application you had initially created. Your application will populate below.

Step 6. Select the application and click **Save**.



Access to service principal is set up.

Cisco Cloud onRamp uses API calls to create the Azure transit VNet with two Cisco vEdge Cloud router instances, and to map existing Azure host VNets to the transit VNet. The next section shows how to get the values needed to sign in programmatically from vManage.

#### Procedure 7: Get Tenant ID and Application ID for Signing In

For the programmatic sign in access from vManage NMS, you need to pass both the tenant ID with your authentication request and the application ID. You also need either a certificate or an authentication key. In this example, an authentication (secret) key is created. To get these values, follow the steps below:

Step 7. When a user signs up for a Microsoft cloud service subscription such as Microsoft Azure, a dedicated instance of Azure AD (Active Directory) is created for the user's organization. This Azure AD instance is partitioned into separate tenants. Each tenant is a dedicated, isolated instance of the Azure Active Directory service, owned and managed by an organization.

From the Azure AD service, you can get the Tenant ID or Directory ID, which is the identity of the Azure AD in which you have created the Cloud onRamp applications and the Application ID or Client ID which is an identity of the application that Azure AD recognizes.

Copy the Directory (tenant) ID and Application (client) ID to a notepad. You will use those IDs later in your vManage to connect to your Azure Application.



Table 5.

Gathered 3 out of 4 values needed for the Cloud onRamp Workflow

Section	Value
Tenant ID	f95d3f42-fe02-4c16-8f7d-4f126df87754
Subscription ID	5f70cd2b-XXXX- XXXX - XXXX - XXXX XXXX XXXX
Client ID	0c33f63d-ebde-4d2f-915e-69871bbf00ae
Secret Key	

#### Procedure 8: Authentication - Create a new Secret key for the Cisco Cloud onRamp Application

Gather the Cloud onRamp secret key that the 'CloudonRamplaaSGuide' application can use to authenticate itself to AD.

- Step 1. In the summary screen of App registrations, click Certificates & Secret.
- Step 2. In the screen, click on + New client secret.
| Home > Cisco-ENB-SDWAN   App registra | tions > CloudOnRampIAASGuide   Certificates & secrets       |   |   |                    |     |
|---------------------------------------|---|---|---|--------------------|-----|
| CloudOnRampIAASGuide                  | e   Certificates & secrets                                  |   |   |                    | × × |
| C. Sansk (Card - 0                    | Copy the new client secret value. You won't be able to p    | etrieve it after vou perform another op | eration or leave this blade.                              |                    |     |
| > Search (Cmd+/) «                    | Condentials applies the identify the model as to            | the authentication convice when rea     | aiving takang at a wab addressable location (using an UTT | 'DE scheme). Ees e |     |
| Overview                              | higher level of assurance, we recommend using a certific    | ate (instead of a client secret) as a c | redential.  | rs scheme), ror a  |     |
| Quickstart                            |   |   |   |                    |     |
| Manage                                | Certificates  |   |   |                    |     |
| 🔤 Branding                            | Certificates can be used as secrets to prove the applicati  | on's identity when requesting a toke    | n. Also can be referred to as public keys.                |                    |     |
| Authentication                        | T Upload certificate  |   |   |                    |     |
| 📍 Certificates & secrets 🛛 1          | Thumbprint  | Start date                              | Expires   |                    |     |
| Token configuration                   | No certificates have been added for this application.       |   |   |                    |     |
| API permissions                       |   |   |   |                    |     |
| Expose an API                         |   |   |   |                    |     |
| Owners                                | Client secrets  |   |   |                    |     |
| Roles and administrators (Previ       | A secret string that the application uses to prove its iden | tity when requesting a token. Also c    | an be referred to as application password.                |                    |     |
| 0 Manifest                            | 2 + New client secret                                       | <b>.</b> .                              |   |                    |     |
| Support + Troubleshooting             | Description   | Expires                                 | value   | ~ ~                |     |
| P Troubleshooting                     | cloudonrampsecretkey  | 5/7/2021                                | Mp4x_jkhTR1T5Ket02yRsrj-LAXBHa                            |                    |     |
| New support request                   |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |
|                                       |   |   |   |                    |     |

Step 3. Enter a **Description** and **Expiry** time period. Click, **Add**.

Home > Cisco-ENB-SDWAN   App registra	tions > CloudOnRampIAASGuide   Certificates & secrets		1
🔶 CloudOnRampIAASGuide	e   Certificates & secrets	\$ ×	
	Add a client secret		
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Description         1           Cloudonrampsecretkey		
Manage	Expires		
🔤 Branding			
Authentication	O in zvers 2		
📍 Certificates & secrets			
Token configuration	3 Add Cancel		-
API permissions			
Expose an API	Cirent sectors		1
Owners	+ New client serrer		
Roles and administrators (Previ	Description Expires Value		
🔟 Manifest			
Support + Troubleshooting	No client secrets have been created for this application.		
Troubleshooting			
New support request			
			_

Step 4. Click on the copy button [] to copy the value of secret key to a notepad. This value is used later in vManage.

Home > Cisco-ENB-SDWAN   App registra	ations > CloudOnRampIAASGuide   Certificates & secrets	i			
🔶 CloudOnRampIAASGuide	e   Certificates & secrets				× ×
Search (Cmd+/) «	Copy the new client secret value. You won't be able	to retrieve it after you perform another opera	tion or leave this blade.		
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Credentials enable applications to identify themselve higher level of assurance, we recommend using a cer	s to the authentication service when receiv tificate (instead of a client secret) as a cred	ing tokens at a web addressable location (using ential.	) an HTTPS scheme). For a	
Manage	Certificates				
Branding	Certificates can be used as secrets to prove the appli	cation's identity when requesting a token.	Also can be referred to as public keys.		
Authentication	→ Upload certificate				
📍 Certificates & secrets	Thumbprint	Start date	Expires		
Token configuration	No certificates have been added for this application.				
API permissions					
Expose an API					
Owners	Client secrets				
Roles and administrators (Previ	A secret string that the application uses to prove its i	dentity when requesting a token. Also can	be referred to as application password.		
Manifest	+ New client secret				
Support + Troubleshooting	Description	Expires	Value		
Troubleshooting	cloudonrampsecretkey	5/7/2021	Mp4x_jkhTR1T5Ket02yRsrj-LAXBHa		
New support request					

Table 6. Gathered 4 out of 4 values needed during the Cloud onRamp Workflow

Section	Value
Tenant ID	f95d3f42-fe02-4c16-8f7d-4f126df87754
Subscription ID	5f70cd2b-XXXX- XXXX - XXXX - XXXX XXXX XXXX
Client ID	0c33f63d-ebde-4d2f-915e-69871bbf00ae
Secret Key	1IIPm_JKlih_C~-TK_8h3-Ugws4cmDly4

#### Procedure 7: Firewall Ports are opened in both Azure and in the on-premise gateway firewall

Lastly, remember to open firewall ports to establish DTLS connection with the on-premise controllers and to establish control plane connections with the vSmart controller. For details on the ports opened, refer to the design section of this document.

#### **Process 2: vManage NMS and Transit VNet Prerequisites**

Before you can configure Cloud onRamp for laaS, you must properly provision the vManage NMS.

#### Procedure 1: Verify Internet Access from vManage

Step 1. Make sure that your vManage server has access to the Internet and that it has a DNS server configured so that it can reach Azure Cloud. To enable DNS server configuration, you can do this either within the VPN feature template associated with your vManage device template or do it via CLI.

Option 1: If your vManage is configured using the vManage device templates, then a DNS server config is added in the VPN feature template. To configure a DNS server in vManage VPN 0, enter the IP address of a DNS server, and then save the edited feature template.

	dealer -					
≡	cisco vManage		•	Ê	<b>≜</b>	admin 🔻
5	CONFIGURATION   TEMPLATES					
	Device Feature					
	Feature Template > Add Template > VPN					
\$	Basic Configuration DNS IPv4 Route	IPv6 Route				
٩						
â	BASIC CONFIGURATION					
	VDN	2				
<b>`</b> `	VPN	VPN 0				
	Name	⊕				
	DNS					
	Primary DNS Address	⊕ - 208.67.222.222				
	Secondary DNS Address	⊕ ▼ 208.67.220.220				
	New Host Mapping					
	Optional Hostname				Ac	ion
		Save Cancel				

Option 2: If your vManage is configured manually via CLI, then login to vManage GUI and navigate to **Tools** > **SSH Terminal**. Click on the vManage server from the device group and enter the following commands:

vManage# conf t	
Entering configuration	mode terminal
vManage(config)# vpn 0	
<pre>vManage(config-vpn-0)#</pre>	dns 208.67.222.222 primary
<pre>vManage(config-vpn-0)#</pre>	dns 208.67.220.220 secondary
<pre>vManage(config-vpn-0)#</pre>	commit

#### Procedure 2: Verify you have two unused Cisco vEdge Cloud routers in vManage

Step 1. Ensure that two vEdge Cloud routers that are to be used to bring up the Cisco Cloud onRamp for laaS are added to the vManage NMS. These two routers are later deployed in Azure public cloud in their own VNet, and together they form the transit VNet, which is the bridge between the Cisco SD-WAN overlay network and Azure cloud applications.

	alulu e					-			
[≡_	cisco Cisco vManag	3e				8	¢.	0	admin 🔻
-	Dashboard >	CONFIGURATION   CERTIFICATES							
	Monitor >	WAN Edge List Controllers							
		Send to Controllers							
٠	Configuration 🗸							•	00
	Devices							Q	ge
	0	Q	Search Options 🗸					Total	Rows: 84
	Certificates		Validate	Enterprise Cert Serial No					
	Network Design	48190c94	Invalid   Staging   Valid	NA	NA				
	Templates		Invalid   Staging   Valid	NA	NA				
		5a310409	Invalid   Staging   Valid	NA	NA				
	Policies		Invalid   Staging   Valid	NA	NA				
	Security	₽80341d	Invalid   Staging   Valid	NA	NA				
		'df8a055	Invalid   Staging   Valid	NA	NA				
	Cloud onRamp for Saas		Invalid   Staging   Valid	NA	NA				•••
	Cloud onRamp for laaS		Invalid   Staging   Valid	NA	NA				
	Cloud OnRomn for	c85b960	Invalid   Staging   Valid	NA	NA				•••
	Colocation		Invalid   Staging   Valid	NA	NA				•••
3		9c467ab6	Invalid   Staging   Valid	NA	NA				
	10015	2039f37	Invalid   Staging   Valid	NA	NA				
÷	Maintenance >	65eb1e9	Invalid   Staging   Valid	NA	NA				

⊨	cisco Cisco vManag	ge					•	Ê	<u>۽</u>	0	admin 👻
::	Dashboard >	¢ co	DNFIGURATION   DEVIC	ES							
□	Monitor >	WAN	I Edge List Controller	'S							
\$	Configuration 🗸	[] (	Change Mode 👻 单 U	pload WAN Edge List 🛛 Export Bootst	rap Configuration 🛛 S	ync Smart Account				٩	00
	Devices	Q		Search Options 🗸						Tota	l Rows: 84
		Stat	te Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No		Enterpris	e Cert Expir	ration Date	
	Certificates	<b>X</b>	vEdge 1000	110G403180462	100070F6	NA		NA			•••
	Network Design	6	vEdge Cloud	0d777876-18a4-4e1f-ba0d-2297ba6d5	Token - 4ae3884a1054	NA		NA			
	Hetholic beolgi	<b>O</b>	vEdge Cloud	4d67b056-0e1c-4acc-840e-da1a9a2fb7	17C09195	NA		NA			
	Templates	٢	vEdge Cloud	d82af1c6-cd58-42fa-b1fa-a20e0941196f	Token - 38049872d93f	NA		NA			
	Deligios	Ø	vEdge 5000	193A1104180040	1AFAA920	NA		NA			
	Folicies	(8)	vEdge Cloud	46bc4c1a-8f21-4478-8b8d-771752777	Token - 05abfa9fb62ee	NA		NA			
	Security	٢	vEdge Cloud	847a408c-ffde-4920-a6ec-b0fac65dfcbb	Token - 090a1c43a67c	NA		NA			
	Cloud on Pamp for SaaS	Ø	vEdge 1000	110G408180011	10006E32	NA		NA			
	cloud onkamp for Saas	Ø	vEdge 100 B	1920B448161432	10004C17	NA		NA			
	Cloud onRamp for laaS	(8)	vEdge Cloud	2923298d-5e05-4efe-bc99-cf95f9db0ef5	Token - 4dccfcdb4787f	NA		NA			
	Cloud OnDomn for	Ø	vEdge 5000	193A1104180039	0D611768	NA		NA			
	Colocation	٢	vEdge Cloud	c68a08b8-c7a2-4339-8c2b-8e4526329	Token - bbc233797725	NA		NA			
<b></b>		(3)	vEdge Cloud	f1eabfac-a29d-4cd2-bc40-4b3dee76e395	Token - 193f09c002302	NA		NA			
		(8)	vEdge Cloud	bc6827c6-041a-4afa-806d-433efcd2ed7f	Token - 700f0707150ea	NA		NA			
÷	Maintenance >	0		10000440161414	10004040	NIA		NI A			

#### **Technical Tip**

If you do not have 2 unused Cisco vEdge Cloud routers within the WAN Edge list, login to Cisco Plug and Play portal. Under the Devices tab, click Add Software Device to add the devices to the portal. To add a vEdge Cloud device, enter Base ID as VEDGE-CLOUD-DNA and Quantity as 2 or more, and select your Controller Profile from the drop-down option. Click Save and then Submit.

Identify Device		×	
* Base PID	VEDGE-CLOUD-DNA		
Quantity	15		
Controller Profile	ENTERPRISE-VBOND	•	
Description	Enter short optional description for this device.	G	
		Cancel	

Step 2. Ensure that the vManage NMS is synchronized to the current time. To check the current time, click the Help (?) icon in the top bar of any vManage screen.

	cisco <sup>®</sup> Cisco vManage	• · · · · · · · · · · · · · · · · · · ·			
	Dashboard >	CONFIGURATION   TEMPLATES	Templates Hel	,	
	Monitor >	Device Feature			
\$	Configuration 🗸	Add Template	About		90
	Devices	Template Type Non-D Cisco vManage X		Total Ro	ws: 129
		Name Descrip hed L			
	Certificates	BR_VPN1 BR VPN Platform Version: 19.2.2	admin	08 Jun 2020 6:51:	
	Network Design	Logging_T Loggini Application Version: 19.2R-vbamboo-13-Mar- 2020 14:07:10 PDT	admin	25 Sep 2019 6:26:.	
		OMP_Te OMP Te CISCO Server: vmanage a	admin	04 Jun 2020 12:1	
	Templates	DC_VPN0 DC Tran Copyright (c) 2020, Cisco. All rights reserved.	admin	23 Jul 2019 11:58.	
	Policies	BR_WAN Branch CISCO VManage Timestamp: 2020-07-15 16:59:19	admin	29 Jan 2019 4:56:.	
		ISR43211n ISR432 Time zone: America/Los_Angeles a	admin	19 Nov 2018 8:58:.	
	Security	BR_INT2 Branch a	admin	11 Dec 2018 12:3	
	Cloud onRamp for SaaS	BR_INET Branch a	admin	24 Jul 2019 4:07:	
		vEdgeIntT vEdgeIn	admin	01 Nov 2018 1:53:.	
	Cloud onRamp for laaS	BFD_Tem BFD Template BFD ISR4331 ISR4451-X I 14 9 a	admin	23 Jul 2019 11:48.	
	Cloud OnRamp for	DC_VPN1 DC VPN1 BGP Template BGP C1111-4PLTEEA (ISR4 1 2 a	admin	23 Jul 2019 11:56.	
	Colocation	BR_VPN1 Branch VPN1 Base configu WAN Edg C1111-4PLTEEA C11 10 5 a	admin	23 Jul 2019 4:21:	
4	Tools >	System_T System Template with Tran WAN Edg ISR4331 ISRv CSR10 0 0 a	admin	09 Jan 2019 1:40:.	
÷	Maintenance >	vBondVP test WAN Edg vEdge Cloud 0 0 a	admin	06 Aug 2018 2:09:.	

Step 3. The Timestamp field shows the current time. If the time mentioned is incorrect, configure the vManage server's time to point to an NTP time server, such as the Google NTP server. To do this either an NTP feature template can be associated within the vManage device template or you can configure it manually via CLI.

Option 1: To configure or update the vManage NTP feature template, enter the Hostname/ IP Address of an NTP server, and then attach the new or updated feature template within the vManage device template.

=	Cisco vManag	e	۵	Ê		<b>@</b> a	ıdmin 👻
::	Dashboard >	CONFIGURATION   TEMPLATES					
□	Monitor >	Device Feature					
۵	Configuration 🗸	Feature Template > NTP					
	Devices	Authentication					
	Certificates				/lark as Optic	onal Row 🔒	
	Network Design	Hostname/IP Address		_		-	
	Templates						
	Policies	Authentication Key					
	Security	VPN ID					
	Cloud onRamp for SaaS	Version 🖉 👻 4					
	Cloud onRamp for laaS	Source Interface 🖉 🗸					
	Cloud OnRamp for	Prefer On Off					
ع	Tools >				Add	Cancel	
ŵ	Maintenance >	Update Cancel	]				

Option 2: To configure NTP server via CLI, login to vManage GUI and navigate to Tools > SSH Terminal. Click on the vManage server from the device group and enter the following commands:

```
vManage(config)# sys
vManage(config-system)# ntp
vManage(config-ntp)# server time.nist.gov
vManage(config-server-time.nist.gov)# version 4
vManage(config-server-time.nist.gov)# com
Commit complete.
```

#### Procedure 3: Configure a device template for the Cisco vEdge Cloud routers

You must have a device template assigned within Cisco vManage NMS to the two Cisco vEdge Cloud routers that Cisco Cloud onRamp for laaS provisions within the transit VNet. Apart from configurations in VPN 0, you need at least one service-side VPN and the Management VPN 512 configured within the device template.

Step 1. Build a device template with feature templates similar to the figure below. For drill-down details of the feature templates used in this deployment refer to the Appendix C.

System *	System_Template_Transit	
Logging*	Logging_Template	
NTP	NTP_Template	
4AA *	AAA	
BFD *	Azure_Transit_BFD_Template	
OMP *	OMP_Template	
Security *	Security_Template	
Transport & Mana	gement VPN	
VPN 0 *	Azure_Transit_VPN0_Template	
VPN Interface	Azure_Transit_VPN0_Interface	•
VPN 512 *	Azure_Transit_VPN512_Template	

Service VPN Service VPN	▼
VPN	Azure_Transit_VPN1_Template
VPN Interface	VPN1_Lo0    Sub-Templates
VPN	Azure_Transit_VPN2_Template

Step 2. Next, go to **Configuration** > **Templates** and select the **Device** tab.

Step 3. Find the desired device template (**Onramp\_Transit\_WAN\_edge\_Template**).

Step 4. Select the ... to the right of the template, and from the drop-down menu select **Attach Devices**.

An example is shown in the following figure.

≡	Cisco vManage	:			•	ê	۹	0	admin 🔻
		MPLATES							
	Device 3 Feature								
*	Configuration 1								
ચ	Devices	Sea	rch Options 🗸					Tota	al Rows: 20
			Description	Туре	Device Model	Feature Tem	plates	Device	es At
<b>±</b>	Certificates	nt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LAN-side OSPF w	Feature	vEdge 1000	20		0	
*	Network Design	S_DIA	Direct Internet Access in hybrid transport branch with TLOC extension	Feature	ISR4461	20		1	
_	Templates	nt_OSPF	Branch Dual vEdge Hybrid TLOC SubInts with INET and LAN-side OSPF w	Feature	C1111X-8P	13		1	
<sup>100</sup>	2		Device Template to push configurations into the edge devices hosted in $\ldots$	Feature	vEdge Cloud	8		2	
	Policies	_Template	Device Template to push configurations into the edge devices hosted in $\ldots$	Feature	vEdge Cloud	13		0	4 •••
	Security	_DCA	Branch A with OSPF on the LAN side with MPLS and Internet transport w	Feature	ISR4431	20		1	
			vSmart	Feature	vSmart	9		0	
	Cloud onRamp for SaaS	et_LAN_OSPF	Branch Dual WAN Edge router with Dual Internet transport with DIA	Feature	ISR4351	11		0	
	Cloud onRamp for IaaS	SPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	17		1	
		_VRRP	Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-side Access w	Feature	ISR4331	20		0	
	Cloud OnRamp for Cloud_WAN_Edge_2_Template		Device Template to push configurations into vEdge Cloud device 2 hoste	Feature	vEdge Cloud	17		1	
		SPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	17		0	
	Branch_C_MPLS_CE_LAN_	OSPF	Branch with Dual WAN with Hybrid transport and DIA exit	Feature	ISR4331	20		1	
	Branch_A_Hybrid_Transpo	rt_Compliance	Branch A with OSPF on the LAN side with MPLS and Internet transport w	Feature	ISR4431	20		0	

A pop-up window listing the available devices to be attached to this configuration will appear. The list of available devices contains either the hostname and IP address of a device if it is known through vManage; or it contains the chassis serial number of the devices that have not yet come up on the network and are unknown by

vManage. Cisco WAN Edge Cloud routers are assigned a chassis serial number although there is no physical chassis.

Step 5. Select the devices you want to apply the configuration template to and select the arrow to move the device from the **Available Devices** box to the **Selected Devices** box.

	cisco Cisco vN	Manage										
-		Attach Devices						_		×		
므	Device Feat	Attach device from t	the list below						0 Items Se	lected		
\$	Create Tem	Available Devices		Select A	I	Selected Devices						© =
ع	Q	All	• Q	~		All	Q			~	To	otal Rows: 20
Ĺ	Name	Name	Dev	ce IP		Name	Devic	e IP			Devi	ces At
-	Branch_A_INET_	6c07c04f-5ace-ae	7c-592f-36b47908b1ed								0	
*	Branch_C_INET_	2923298d-5e05-4e	efe-bc99-cf95f9db0ef5								1	
	Branch_B_INET_	0d777876-18a4-4e	e1f-ba0d-2297ba6d518	5							1	
	test	ead1954a-087e-45	571-b747-0665fb33040	6	~						2	
	Onramp_Transit,	0bb1fbcf-30ce-412	26-b6fa-f5fa491c828c		4						0	••••
	Branch_A_Hybrid	e6bad40d-afec-4c	e7-87d2-c23a08bafcd4		$\mathbf{\nabla}$						1	•••
	vSmart	bc6827c6-041a-4a	afa-806d-433efcd2ed7f								0	
	Branch_D_Bronz	46bc4c1a-8f21-44	78-8b8d-7717527774c	а							0	•••
	Branch_H_MPLS										1	
	Branch_F_MPLS										0	
	Branch C MDI S							_			0	
	Branch C MPLS							Attach	Can	cel	1	
	Branch A Hybrid	Transport Compliance	A	Branch A with OSPE on the LA	I side with M	PLS and Internet transpo	rt w Feature IS	R4431	20		0	
	Dranon_A_Hybrid			Dianon A with OSPP on the LA	* Side With W	in Lo and internet transpo		114401	20		0	

You can select multiple devices at one time by simply clicking each desired device.

Step 6. Click the **Attach** button.

A new screen will appear, listing the devices that you have selected.

- onRamp-vEdge-Cloud1: bc6827c6-041a-4afa-806d-433efcd2ed7f
- onRamp-vEdge-Cloud2: e6bad40d-afec-4ce7-b7d2-c23a08bafcd4

≡	cisco VM	anage						•	Ê	<u>۽</u>	0	admin 🔻
==	CONFIGURAT	Attach Devices								×		
▫	O Create Tem	Attach device from the list	st below						2 Items Sele	ected		00
\$	Create rem	Available Devices		Select All		Selected Devices			Selec	et All	т	
عر	Q	All 👻	۹.	*		All	• Q			~		Dial Rows. 20
÷	Name Branch_C_INET_T	Name	Device IP			Name	De	vice IP		_		es Att
	Branch_B_INET_T	ef7e4537-5183-4319-a	114-7919a5d8ed9d			bc6827c6-041a-4a	fa-806d-433efcd2ed7	f			1	
	Corramo Transit	e9c4ba23-f1ed-4090-8	533-9251859a111d			ebbad40d-atec-4ce	e7-87d2-c23aU8batcd	4			2	
•	Branch_A_Hybrid	2fbf39ee-2ebb-4fa7-b0	)d5-8f625b0f93f7		$(\rightarrow)$						1	
	vSmart	34f4a954-307e-4f67-84	40b-98801236f749		$\left( \leftarrow \right)$						0	
	Branch_D_Bronze	84981447-dd9c-46fe-9	114e-c1c454949715		0						0	
	Branch_H_MPLS_	f1eabfac-a29d-4cd2-bc 8f810857-5263-4076-8	c40-4b3dee76e395 381c-f1ee4ffc4601								1	
	OnRamp_IAAS_A:										1	
	Branch_G_MPLS_										0	
	Branch_C_MPLS_									-	1	
	Branch_A_Hybrid	N Edge Lemplate	Device Lemn	iate to push contigura	tions into t	he edge devices host	ied in Feature V	Attach	Canc	ei	0	
	Rranch E INET TLO		Branch Dual	vEdge Hybrid TLOC wi	th INET an	d I AN-side Access pr	orte wi Eastura I	CD/1221	10		0	

6. Find the first Cisco vEdge Cloud router, select ... to the far right of it, and from the drop-down menu select **Edit Device Template**.

For this deployment guide the first Cisco vEdge Cloud router has a chassis serial number of **6bad40d-afec-4ce7-87d2-c23a08bafcd4**. An example is shown in the following figure

≡	alta cisc	Cisco vManage						•	Ê	Ļ	?	admin 👻
::	\$	CONFIGURATION   TEMPLATES										
	Dev	rice Template   Onramp_Tra	ansit_WAN_	edge_Templa	e							
*												00
a	Q	l.		Search Optic	ns 🗸							Total Rows: 2
	S	Chassis Number		System IP	Hostname		Interface Name(vpn2_lan_int1_gex x_or_ gex x.VLAN)		IP	v4 Addres	s(vpn2_lan_i	nt1_ip_
2	C	bc6827c6-041a-4afa-806d-433ef	cd2ed7f	•	-							
*		e6bad40d-afec-4ce7-87d2-c23a0	8bafcd4	-	-						Edit Device	Template
•										L		
							-					
						Next	Cancel					

A pop-up screen will appear with a list of variables and empty text boxes. There may also be variables with check boxes to check/uncheck for on/off values.

Step 7. Fill in the values of the variables in the text boxes.

This deployment guide uses a custom device template onRamp\_Transit\_WAN\_Edge\_Template for Cisco vEdge Cloud routers deployed by using Cisco Cloud onRamp within the Azure transit VNet.

The following template is deployed on the	Chassis Number -	bc6827c6-041a-4afa-	806d-433efcd2ed7f
---	------------------	---------------------	-------------------

Variables	Value
Hostname (system_host_name)	onRamp_vEdge-Cloud1
System IP (system_system_ip)	10.1.0.136
Site ID (system_site_id)	115001
IPv4 Address(vpn1_lo0_int_ip_addr_maskbits)	10.1.0.136/32
Interface Name(vpn512_mgt_int_mgmt0_or_gex)	eth0
Interface Name(vpn0_inet_int_gex)	ge0/0
Shutdown(vpn1_lan_int1_shutdown)	
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream (vpn0_inet_int_bandwidth_ down)	1000000
Timezone (UTC -7)	America/Los_Angeles
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-97.335
Device Groups(system_device_groups)	Azure
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	
Hello Interval (milliseconds)(bfd_internet_bfd_hello_interval)	10000
Address(vpn0_inet_next_hop_ip_addr)	10.0.1.33

The following template is deployed on Chassis Number - e6bad40d-afec-4ce7-b7d2-c23a08bafcd4

Variables	Value
Hostname (system_host_name)	onRamp_vEdge-Cloud2
System IP (system_system_ip)	10.1.0.137
Site ID (system_site_id)	115001
IPv4 Address(vpn1_lo0_int_ip_addr_maskbits)	10.1.0.137/32
Interface Name(vpn512_mgt_int_mgmt0_or_gex)	eth0
Interface Name(vpn0_inet_int_gex)	ge0/0

Shutdown(vpn1_lan_int1_shutdown)	
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream (vpn0_inet_int_bandwidth_ down)	1000000
Timezone (UTC -7)	America/Los_Angeles
Latitude(system_latitude)	37.3541
Longitude(system_longitude)	-121.9552
Device Groups(system_device_groups)	Azure
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	
Hello Interval (milliseconds)(bfd_internet_bfd_hello_interval)	10000
Address(vpn0_inet_next_hop_ip_addr)	10.0.1.33

# Deploy - Cisco Cloud onRamp for IaaS using Azure

This section covers the steps to deploy Cisco Cloud onRamp feature using laaS.

## **Configuration Workflow**

- Make sure the prerequisites explained previously are added.
- The Cloud onRamp for laaS feature uses APIs to automate the following process:
  - Configure and deploy Azure transit VNets with all necessary subnets, network interface, network security groups, public IP addresses etc. This process also includes the instantiation of a pair of redundant Cisco WAN Edge Virtual routers within the transit VNet.
  - Discover and map host VNets to the transit VNet via Azure site-to-site connections. Note, one Host VNet must be mapped to the transit VNet within the workflow that creates the transit VNet. Any remaining host VNets can be added later.

## Process 1: Deploy a Transit VNet using Cisco Cloud onRamp for IaaS

This section discusses the procedures for deploying a transit VNet using Cisco Cloud onRamp for IaaS.

#### Procedure 1: Login to vManage and navigate to Cisco Cloud onRamp for IaaS

Step 1. Login to the vManage web console.

Login to the vManage web console using the IP address or fully qualified domain name of your vManage instance. For example:

https://vManage ip addr or FQDN:8443/

ululu Cisco vManage						白	AB 0	admin 🔻	
ASHBOARD   MAIN DASHBOARD							÷- v		
vSmart - 1 WAI	<b>16 ↑</b> N Edge - 16	•	<b>1 ↑</b> vBond - 1	t ⊗ the second s	e - 1 Last 24 hrs	2	Warning Invalid	0	
Control Status (Total 15)		Site Health (Total 12)			Transport Interface Distrib	oution			
Control Up	15	S Full WAN Connect	ivity	10 sites	< 10 Mbps 10 Mbps - 100 Mbps			57	
Control Down	0	<ul> <li>Partial WAN Conn</li> <li>No WAN Connecti</li> </ul>	ectivity vity	2 sites 0 sites	100 Mbps - 500 Mbps > 500 Mbps			0	
				V	iew Percent Utili	zation			
WAN Edge Inventory		WAN Edge Health (Total	16)	-	Transport Health	Type: By Loss	yLoss ♦ \Xi 🖸		
Total Authorized	83 24	(16) 0		0	50 %				
Deployed	16				30 %				
Staging	0	Normal	Warning	Error	0	•••••	• • • • • • • •		
Top Applications	ΨD	Application-Aware Routin	ng				Type: By	Loss 🖨 🖸	
		Tunnel Endpoints		Avg. Latency (ms)	Avg. Loss (%)	Avg.	Jitter (ms)		
		Nouter:mpls-BR2-WA	N-Edge2:mpls	0	3.099	0			
No data to display		BR2-WAN-Edge2:mp DC1-WAN-Edge1:mp	ls-Router:mpis ils-BR2-WAN-Edge2:mpis	0	2.341	0			

Step 2. In the navigation panel on the left side of the screen, select **Configuration > Cloud onRamp for IaaS**. If this is the first time you're configuring the Cloud onRamp for IaaS feature, then no Azure or AWS cloud instances will appear, and the initial screen should look similar to the figure below.



able unable to proceed with the deployment of this feature.

At least 2 unused WAN Edge devices with templates attached should be available in vManage to proceed with this step.

#### Procedure 2: Select the Cloud Provider and Configure Access Credentials

Step 1. Click the Add New Cloud Instance button in the bottom center of the screen.

This will begin the workflow for you to add a new cloud instance.

≡	Cisco vManage				•	Ê	<b>≜</b> 60	Ø	admin 👻
	CONFIGURATION   CLOUD ONRAMP FOR IAAS								
묘									
\$									
3									
÷									
÷		Add Cloud Instance - Log In to	a cloud server	×					
•		• • • • • • • • • • • • • • • • • • •	O H Microsoft Azure						
			Login	Cancel					
		Ad	ld New Cloud Instance						

Step 2. Click on the radio button next to **Microsoft Azure** cloud provider and enter the **Tenant ID**, **Subscription ID**, **Client ID** and the **Secret Key** gathered from the steps in the Azure prerequisites.

_	de de				 				
	cisco vManage				•	Ê	<b>£</b> 63	0	admin 🔻
<b></b>	CONFIGURATION   CLOUD ONRAMP FOR IAAS								
▣	-			_					
¢		Add Cloud Instance -	Log In to a cloud server	×					
3		O 👘 amaz web ser	xon vices Microsoft Azure 1						
2				- 1					
		Login to AZURE							
		Tenant ID	f95d3f42-fe02-4c16-8f7d-4f126df87754	2					
		Subscription ID	5f70cd2b-baee-4c43-889a-71bb1e8a0efc	3					
		Client ID	0c33f63d-ebde-4d2f-915e-69871bbf00ae	4					
		Secret Key		5					
			6 Login Cance						

## **Procedure 3: Select a Location and Create Transit VNets**

After you have entered the Azure IDs and secret key, the cloud instance configuration wizard opens. This wizard consists of three screens that you use to **Create Transit VNets**, **Discover Host VNet**, and **Map Host VNets to Transit VNets**.

A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

Step 1. Choose the **location** where you want to deploy your SD-WAN Transit VNet.

≡	Cisco vManage									Û	,®	Ø	admin 👻
::	CONFIGURATION   CLOU	D ONRAMP FOR IAAS	Dashboard > Add Transit	it VNet									
□		0	Select a Location and Create Transit VNets		O Discover H	Host VNet	— O Map Tr	Host VNets ansit VNets	s to				
<b>ث</b> عر	Transit Account ID: configure paramete	5f70cd2b-baee-4c43 ers	889a-71bb1e8a0efc   Choos	ose a Locati	ion, create a trans	sit VNet and							
۵	Choose Location	Select a Location											
*		westcentralus											
618		westeurope									Но		
_		westindia						VI	Net	VNet	VN		
		westus											
	[	westus2											
									Ì	$\Delta\Delta$	1		
										ZAN			
									R				
									v	Edge Devices			
									Tra	insit VNet			

Step 2. Next, enter a name for your new Transit VNet, followed by the Device Information.

Device Information:

Software Version of WAN Edge devices: In a vManage NMS running Cisco SD-WAN code 19.2/ 20.1, a virtual device within transit VNet can be automatically deployed running either of these Cisco SD-WAN code versions - 19.1, 18.4, 18.3, 18.2.

Choose the WAN Edge Version from the drop-down menu. The cloud routers in the transit VNet will be deployed running the chosen SD-WAN software version.

- Size of VM: At this point you also select the size of Virtual Machine (VM) within your transit VNet. Choose the size based on the overall workload that you want to support. vManage NMS running version 19.2.2, lets you choose between either size.
  - Standard F8 (8 vCPU)
  - Standard F4 (4 vCPU)

For pricing details refer to the Azure pricing chart.

Choose the Size of Transit WAN Edge from the drop-down menu. The WAN Edge cloud routers will be deployed with the chosen size. Standard F8 (8vCPU) is the chosen size in this deployment. Before choosing the size, refer to Azure f-series cost vs memory.

 The Device Pair 1# lists the two WAN Edge cloud devices, that were logically attached to a device template.

1		
Transit VNet Name COR_TransitVNet	0	Host Host Host VNet VNet VNet
Device Information		
WAN Edge Version vedge-cisco_vedge_azurecloud_19_1_0   2		
Size of Transit WAN Edge Standard F8 (8 vCPU)	0	
Max. Host VNets per Device Pair		
	0	vEdge Devices
onRamp_vEdge-Cloud1 : bc6827c6-041a-4afa-806c × 4 Device Pair 1#		Transit VNet
onRamp_vEdge-Cloud2 : e6bad40d-afec-4ce7-87d2 X 5		

Step 3. Within the Cisco Cloud onRamp workflow, you specify an IPv4 CIDR block range when creating the transit VNet. This IPv4 CIDR range you configure is automatically sub-netted to create the necessary subnets for the network interfaces associated with the WAN Edge devices deployed in the Transit VNet.

The suggested CIDR is 10.0.0/16 for our new Transit VNet. Try to avoid using up an entire address space and divide the network in smaller chucks.

Select the **Advanced** tab, to enter the **Transit VNet CIDR**. This is a Classless Interdomain Routing value, which in our case is defined as 10.0.1.0/24.

Next, click **Proceed to Discovery and Mapping** to map host VNets to the transit VNet.

≡	cisco Cisc	co vMa	anage				•	É) 🖡	0	admin 👻
	CONFIG	URATIO	ON   CLOUD ONRAMP FOR I	AAS Dashboard > Add Transit VNet						
_				· ·						
•			Size of Transit WAN Edge	Standard F8 (8 vCPU)	•		Host Ho VNet VI	ost Net	Host VNet	
<b>4</b>			Max. Host VNets per Device Pair						/	
*			Device Pair 1#	onRamp_vEdge-Cloud1 : bc6827c6-041a-4afa-806c X		0		X/		
•				onkanp_rcugeolouuz.eouau4uralec-4ce7-0702		0	vEdge D	Pevices		
		/	Advanced 🖂 1							
		[	Transit VNet CIDR 2	10.0.1.0/24						
				Save and Finish Proceed to Disc	overy and Mapping 3	Cancel				

## **Procedure 3: Discover Host VNet**

Host VNets part of the same Account ID or Subscription ID can be discovered and later mapped to the transit VNet.

Step 1. Click on the drop-down menu on the tab next to **Select an account to discover**. The drop down lists out the Subscription ID.

≡	cisco Cis	co vManage				•	â	<b>"</b> @	0	admin 🔫
::	CONFIG	GURATION   CLOUD ONRAMP FOR	RIAAS Dashboard > Discover Host VN	let						
□		Select an account to								
*		discover	Select one account	Ø Discover Host VNets	ſ	 				
عر			5f70cd2b-baee-4c43-889a- 71bb1e8a0efc			Host VNet	Host VNet	Hos VNo	t et	
÷					l	•				
*										
•										
			New Account				vEdge Devices			
						Ti	ansit VNet			
	Back			NEXT	ancel					

Step 2. Once the subscription ID is selected, click **Discover Host VNets**.

≡	cisco Cis	sco vManage					•	ê	<b>.</b>	0	admin 🔻
	CONFIC	GURATION   CLOUD ONRA	MP FOR IAAS Dashboard > Discover Host VNe	et							
= □ <b>◇</b>		Select an account to discover	5f70cd2b-baee-4c43-889a-71bb1e8a0efc ×	Discover Host VNets		•	Host VNet	Host	Host VNe	t	
							Т	vEdge Devices ransit VNet			
	Back			NEXT	Cancel						

Step 3. Click on the drop-down arrow, to **Select a** host **VNet**. With this step, discovery of Host VNet is complete.

Click Next to map the selected host VNet to the transit VNet.

≡	cisco Cis	co vManage					•	Ê	<b>¢</b> 200	0	admin 🔫
	CONFIG	URATION   CLOUD ONRAM	P FOR IAAS Dashboard > Discover Host VNet	1							
		Select an account to discover	5f70cd2b-baee-4c43-889a-71bb1e8a0efc ×	Discover Host VNets	5						
ع م		Select a VNet	AZ-IAAS   COR_Spoke_1	•	1	0	Host VNet	Host VNet	Ho VN	st let	
						0					
						L					
								vEdge Devices			
							Ti	ansit VNet			
	Back			2 NEXT	Cancel						

## **Procedure 4: Map Host VNets to Transit VNets**

Each discovered Host VNet is mapped to the transit VNet. During this mapping process, Cloud onRamp for IaaS automatically provisions a Virtual Network Gateway in the host VNet which is associated to the VNet's gateway subnet. The Virtual Network Gateway contains two public IP addresses for site-to-site connection, private IP addresses and a BGP ASN number for BGP peering. While public IP addresses are automatically added by Azure, the IPv4 CIDR address block for the private IP address is decided by the user during the host VNet to transit VNet mapping process.

Step 1. Click on **Map VNets** to map the discovered Host VNet to the Transit VNet *COR\_TransitVNet*.

≡	cisco Cisc	o vM	anage							•	Ê	<b>¢</b> <sup>66</sup>	)	•	admin 🔻
::	CONFIGU	JRATI	ON   CLOUD ONRAMP FOR	IAAS	Dashboard > N	Apping Configuration	on								
▣					Select a Locatio Create Transit \	on and /Nets		Discover Host VNet	Map Host V Transit V	/Nets to /Nets					
٠															
٩		1 Rov	vs Selected 🗘 Map VI	Nets	🕅 UnMap VNet	s		0 🗐							
÷		Q				Search Options $\checkmark$		Total Rows: 1							
*			Host VNets	Мар	bing Status	Transit VNet		VPN Segment							
678			COR_Spoke_1					-		Host	Host		Host		
<b>—</b>										VNet	VNet		VNet		
											<u> </u>	- /	<u>//</u>	_	
											$\Delta$				
											V/ N	V			
											Š.				
									$\mathbf{v}$		vEdge Devices				
										1	Fransit VNet				

#### Technical Tip

If you try to click Save and Complete without mapping host VNet and transit VNet, an error message will pop-up - "Please create mapping in order to proceed".

Step 2. A pop-up screen appears that lets you associate the mapping to a service-side VPN. Click on the drop-down menu and choose a **VPN**.

	cisco vManage				• Ê	<b>A</b> 360	0	admin 🔻
55	CONFIGURATION   CLOUD ONRAMP FOR IAAS	Dashboard > Mapping Config	guration					
▫	Ø	Select a Location and Create Transit VNets	Oiscover Host VNet	Map Host VNets to Transit VNets	0			
\$								
4	1 Rows Selected 🗘 Map VNets	없 UnMap VNets	68					
÷	Q	Map Host VNets		× .				
	Host VNets Ma	OnRamping multiple \	/Nets with overlapping subnets will cause r	network routing issues.				
_	COR_Spoke_1 -				Host	Has		
		Transit VNet	COR_TransitVNet	×	t VNet	VNe	t	
		VPN	Select VPN			/		
			1					
			2					
						V		
					vEdge Devices			
					Transit VNet			

Step 3. On selecting a VPN, you will be navigated over to the following screen. Here, you define the IPsec site-to-site tunnel IP addresses under the **IPsec Tunnel CIDR** and the **Loopback IP addresses**.

≡	cisco vManage						•		)	•	admin 🔻
55	CONFIGURATION   CLOUD ONRAMP FOR IAAS Dashbo	ard > Mapping Co	onfiguration								
	Map Host VNets							×			
¢	OnRamping multipl	e VNets with overla	opping subnets will o	cause netwo	rk routing issues.						
<b>∢</b> ₫	1 Rows Selecter Q Transit VNet	COR_TransitV	Net					×			
	Host VNI VPN	1						$\times$			
	COR_Spc IPsec Tunnel CIDR		,	IPSec T	unnel		Loopback IP			Host VNet	
	46bc4c1a-8f21-4478-8b	8d-7717527774ca	192.168.0.0	/30	192.168.0.4	/30	1.1.1.1			2	
	5274c506-0980-4dcd-9	'e8-07c4cbfb883e	192.168.0.8	/30	192.168.0.12	/30	1.1.1.2				
	Azure Information										
	BGP ASN	Enter a BGP A	SN value						1		
	Host VNet Gateway Subr CIDR: 10.25.2.0/24	et Host VNet Su	bnet						<b>Z</b> Y		
								Transit VN	et		

Step 4. The **BGP ASN** is used to build BGP sessions between the Host VNet and the Transit VNet. Under **Azure Information**, enter a **BGP ASN**. Also, based on the subnet you had defined in your Host VNet, define a **Host VNet Gateway Subnet**. Next, click on **Map VNets**. Note, choose a subset of the subnet already assigned to your host VNet as the gateway subnet. To decide on the BGP ASN number refer to the <u>Azure BGP guide</u>.

The subnet defined within the Host VNet COR-Spoke-1 is 10.25.2.0/25. Therefore, the Host VNet Gateway Subnet defined here is 10.25.2.128/25. Two IP's from this block will be used to establish BGP Peering with the WAN Edge device's loopback IP over IPsec VPN tunnels.

≡	Cisco vManage								•	Ê	<b>≜</b> 360	0	admin 👻
	CONFIGURATION   CLOUD O	NRAMP FOR IAAS Dashboard	Mapping Cor	nfiguration									
□		OnRamping multiple VI	Nets with overlap	oping subnets will o	ause netwo	rk routing issues.							
\$		Transit VNet	COR_TransitVN	let					×				
۹,	1 Rows Selected	VPN	1						×				
÷	Q	IPsec Tunnel CIDR											
<b>.</b>	Host VNd				10.0		100						
•		46bc4c1a-8t21-44/8-8b8d-	//1/52///4ca	192.168.0.0	/30	192.168.0.4	/30	1.1.1.1			Ho: VN	st let	
		52/4c506-0980-4dcd-9/e8-	0/c4cbfb883e	192.168.0.8	/30	192.168.0.12	/30	1.1.1.2			/		
		Azure Information											
		1 BGP ASN	65534										
		2 Host VNet Gateway Subnet CIDR: 10.25.2.0/24	10.25.2.128/25	5							1		
							3	/lap VNets	Cancel				
		_		_	-	_			Transi	t VNet			

Step 5. Finally, click **Save and Complete** to initiate the Cloud onRamp for laaS workflow.

=	altalla Cise	o vMa	anage						自	<b>1</b> 30	0	admin 🔻
		URATIO	ON   CLOUD ONRAMP FOF	IAAS Dashboard > M	apping Configuration					<b>~</b> ~	•	
		ζ			Search Options 🗸	Total Rows	5. 1					
-			Host VNets	Mapping Status	Transit VNet	VPN Segment						
۵			COR_Spoke_1	<b>Ø</b>	COR_TransitVNet	1		Hest	Hast	Had		
عر								VNet	VNet	VNe	:t	
÷									Ā	_/		
*												
1.									$\sum$			
										<b>X</b>		
									vEdge Devices			
								Т	ransit VNet			
	Back				[	Save and Complete	Cancel					

The configuration process takes about 15 to 20 minutes. Post completion, your Transit VNets will be provisioned on Azure with a pair of WAN Edge cloud routers configured based on the templates attached. The mapping of Host VNet and Transit VNet will also be complete.

≡	cisco	Cisco vManage				• É	1 🔎	Ø	admin 👻
::	Ê TA	ASK VIEW							
	Map h	host to transit VPC/VNet				I	nitiated By: admir	From: 1	00.119.42.246
~	Total	Task: 1   Success : 1							
* 3									08
Å	Q		Search Options 🗸						Total Rows: 1
	1.0	Status	Device IP		Message		Start Time		
*	~	Success	System		Finished mapping Host VNet COR_Spo	oke_1	23 Jul 2020 1	2:04:30 PI	M PDT
		<pre>[23-Jul-2020 12:24:11 PDT] Creating vy [23-Jul-2020 12:24:11 PDT] Creating vy [23-Jul-2020 12:24:24 PDT] Creating vy [23-Jul-2020 12:24:24 PDT] Creating vy [23-Jul-2020 12:24:35 PDT] Created VP [23-Jul-2020 12:25:00 PDT] Finished mmi</pre>	y clatca a vitat later later on connection for local net V Connection COR_COR_Spoke_1 on connection for local net V Connection COR_COR_Spoke_1 apping Host VNet COR_Spoke_1	work gateway : COR_COR_Spok 1_vpnConnection_vedge1_vng work gateway : COR_COR_Spok 1_vpnConnection_vedge2_vng 1	e_1_LNG_vedge1 e_1_LNG_vedge2				^ ×

## Procedure 3: Use Case #1 - Full Connectivity

Optionally, you can associate additional host VNets with the transit VNet. For the this use case, both host VNets, **COR-Spoke-1** and **COR-Spoke-2** are mapped to same VPN on the transit VNet.

The main Cloud onRamp page has two tabs - Mapped Host VNets and Transit VNets.

Step 1. To map additional Host VNets, select the Mapped Host VNets Connections.

≡	diada cisco	Cisco vMana	ge					•	â	<u>,</u>	20	9	9 0	9 🕜	9 (9	<b>9</b> 🕑 a	🦻 🕜 adn	🦻 🕜 admin	🤌 👔 admin '	🦻 🕜 admin	🦻 🕜 admin	🦻 🕜 admin י	🦻 🕜 admin	🦻 👩 admin 🖥	🦻 🌍 admin	🦻 🍞 admin	🦻 🕜 admin	🤌 👩 admin	🦻 👩 admin	🦻 🕜 admin	🤌 🕜 admin	🦻 🕜 admir	🦻 🕜 admir	🦻 🕜 admii	🦻 🕜 admi	🦻 👩 admi	🤌 🕜 admi	🦻 🕜 adm	🤌 🕜 adm	🦻 🕜 adm	🦻 📀 adr	🦻 🕜 adr	🦻 🕜 ad	🦻 🕜 ad	🦻 🕜 ad	) 🕜 ac	) 🕜 a	<b>) ()</b> a	<b>) ()</b> a	<b>) ()</b> a	<b>9</b> 🛛 a	<b>) ()</b> e	<b>) ()</b> a	<b>) ()</b> (	9 🕜 🕯	9 📀 🕴	9 (9	9 9	9 😧	9 🕜	9	9 😧	9 📀	9	9 9	• •	9	9	. 0	. 0	• •	• •	9 🚱	•	20	0	0	0	0	20	1	1	1			ľ	ļ																																						
	🌣 co	NFIGURATION	CLOUD ONRAMP FOR	R IAAS																																																																																																																									
	•	Add New Cloud	Instance																																																																																																																										
						Transit Vie	Host View																																																																																																																						
•																																																																																																																													
		🌣 Microsof	t Azure Enterpri	se   Mapped A	ccounts : 1																																																																																																																								
		westus2																																																																																																																											
1.			Mapped Host V	Nets (Total: 1)	Transit VNet	s (Total: 1)																																																																																																																							
		Microsoft Azure	<b>↑1</b>	↓0	<u>↑</u> 2	↓0																																																																																																																							
			Connect	tions	Device	es																																																																																																																							

Step 2. You will be navigated to a page containing the **Mapped Host VNets**.

≡	Cisco vManage					•	Ê	<b>≜</b> ®	0	admin 🔻
::	CONFIGURATION   CLO	UD ONRAMP FOR IAAS Dashboard >	AZURE : westus2   5f7	0cd2b-baee-4c43-889a-71bb1e8a0e	fc					
묘				Host VNets Transit VNets						
\$	Mapped Host VNets	Un-Mapped Host VNets								
ح 11 11	0 Rows Selected ⋈ U	In-Map VNets Search	Options 🗸						Tot	al Rows: 1
Ĩ.	Host VNets	Host VNet Account Name	Resource Group	Mapped Transit VNet	Host VNet State	Transit VN	et State	VPN	Segment	
•	COR_Spoke_1	Microsoft Azure Enterprise	AZ-IAAS	COR_TransitVNet	$\uparrow$	$\uparrow$		1		

Step 3. Click on the **Un-Mapped Host VNets** tab. Within this **Select an account to discover**, choose your Subscription ID from the drop-down menu. Then click on **Discover Host VNets**. This will populate all the available VNets associated to the Subscription ID.

≡	Cisco vManage		•	Ê	<b>4</b> 929	0	admin 🔫
::		UD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc					
□		Host VNets Transit VNets					
٠	Mapped Host VNets	Un-Mapped Host VNets 1					
ع •	Select an account to dis	cover 5f70cd2b-base-4c43-889a-71bb1e8a0efc × Discover Host VNets 2					
	Select a VNet	Select VNet *					-
m	Ø Map VNet						
<b>–</b>							

Step 4. Click on the drop-down menu located next to **Select a VNet** to choose the VNet you want to map. Once the VNet is selected, click **Map VNet**.

∣≡	Cisco vManage						•	Ê	<b>4</b> 22	0	admin 🔫
::		OUD ONRAMI	P FOR IAAS Dashboard >	AZURE : westus2   5f	70cd2b-baee-4c43	3-889a-71bb1e8a0efc					
▫					Host VNets	Transit VNets					
\$	Mapped Host VNets	Un-Map	ped Host VNets								
م ≞	Select an account to dis	scover	5f70cd2b-baee-4c43-889a	-71bb1e8a0efc ×	¢ Disc	over Host VNets					1
	Select a VNet	AZ-IAAS	COR_Spoke_2								-
	Ø Map VNet 2										_

Step 5. Within pop-up screen, choose the VPN ID. The VPN ID is set to VPN 1.

≡	cisco vManage			•	Ê	<b>Å</b> 381	0	admin 👻
	CONFIGURATION   CLOUD ONRAMP FOR IAAS	Dashboard > AZURE : westus	2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc					
▫			Host VNets Transit VNets					
\$	Mapped Host VNets Un-Mapped Host V	Nets						
*	Select an account to discover 5f70cd2 Select a VNet AZ-IAAS   COR_Spok	Map Host VNets  OnRamping multiple V Transit VNet	X Nets with overlapping subnets will cause network routing issues. COR. Transit/Net X	1				¥
		VDN	Falset //IN					
		VEIN	1					
			2					

Step 6. Define the **IPsec tunnel CIDR** details and **BGP ASN** used to build BGP sessions between the Host VNet and the Transit VNet. Also, define a **Host VNet Gateway Subnet** and click on **Map VNets**.

⊨	cisco VManage								•		<b>.</b> ®	
8		ONRAMP FOR IAAS Dashboard	> AZURE : westu	us2   5f70cd2b-baee-4	1c43-889	a-71bb1e8a0efc						
□		OnRamping multiple V	Nets with overlap	ping subnets will cau	ise netwo	rk routing issues.				ų		
	Mapped Host VNets	Transit VNet	COR_TransitVN	et					×			
3	Select an account to discov	VPN	1						×			
•	Select a VNet A	1 IPsec Tunnel CIDR		1	IPSec I	Details						•
*	Ф Map VNet	bc6827c6-041a-4afa-806d-	433efcd2ed7f	192.168.0.16	/30	192.168.0.20	/30	1.1.1.2				
		e6bad40d-afec-4ce7-87d2-	c23a08bafcd4	192.168.0.24	/30	192.168.0.28	/30	1.1.1.1				
		Azure Information										
		2 BGP ASN	65534									
		3 Host VNet Gateway Subnet CIDR: 10.22.0.0/16	10.22.10.0/28									
										-1		
							4	Map VNets	Cancel			

Note, mapping of Host VNet to Transit VNet can take up to 45 minutes.

=	ahah	" Cisco vManage		▲ 自		
	Ê T/	ASK VIEW				×
-	Map I	host to transit VPC/VNet		In	iitiated By: admin	From: 100.119.42.246
	Total	Task: 1   Success : 1				
\$						
٩						
÷	Q	Se	arch Options 😽			Total Rows: 1
_	8	Status	Device IP	Message		
÷	~	Success	System	Finished mapping Host VNet COR_Spoke_2	23 Jul 2020	1:10:46 PM PDT
		[23-Jul-2020 13:28:47 PDT] Creating vpn conne [23-Jul-2020 13:28:47 PDT] Creating vpn conne [23-Jul-2020 13:29:10 PDT] Created VPN Connee [23-Jul-2020 13:29:10 PDT] Created VPN Connee [23-Jul-2020 13:29:23 PDT] Created VPN Connee [23-Jul-2020 13:29:47 PDT] Finished mapping H	ections ection for local network gateway : COR_COR_Spo tion COR_COR_Spoke_2_vpnConnection_vedge1_vng ection for local network gateway : COR_COR_Spo ction COR_COR_Spoke_2_vpnConnection_vedge2_vng Host VNet COR_Spoke_2	ke_2_LNG_vedge1 ke_2_LNG_vedge2		

## Procedure 4: Use Case #2 - Segmentation

For the second use case, the first host VNet **COR-Spoke-1** is mapped to VPN 1 on the transit VNet. The second and new host VNet **COR-Spoke-2** is mapped to VPN 2.

The main Cloud onRamp page has two tabs, Mapped Host VNets and Transit VNets.

Step 1. To map additional Host VNets, select the Mapped Host VNets Connections.

∎	alialia cisco	Cisco vMana	ge			
::	🌣 co	NFIGURATION	CLOUD ONRAMP FO	RIAAS		
	€	Add New Cloud	Instance			
۵						Transit Vi
عر						
÷		🌣 Microsof	t Azure Enterpri	ise   Mapped A	ccounts : 1	
*		westus2				
			Mapped Host V	/Nets (Total: 1)	Transit VNe	ts (Total: 1)
		Microsoft	1		<b>小</b> 2	
		Azure		• 0		• 0
			Connec	tions	Devic	es

≡	dialia cisco C	lisco vManage					▲ Ê	<b>1</b> 80 (b)	admin ·
	CONF	IGURATION   CLOUD	ONRAMP FOR IAAS Dashboard >	AZURE : westus2   5f70c	d2b-baee-4c43-889a-71bb1e8a0	lefc			
▫				-	Host VNets Transit VNets				
٠	Марр	ed Host VNets	Jn-Mapped Host VNets						
∢ ≇	0 Rov	vs Selected 🕺 Un-M	Map VNets Search (	Options 🗸				Total	C)
*		Host VNets	Host VNet Account Name	Resource Group	Mapped Transit VNet	Host VNet State	Transit VNet State	VPN Segment	
		COR_Spoke_1	Microsoft Azure Enterprise	AZ-IAAS	COR_TransitVNet	$\uparrow$	$\uparrow$	1	

Step 2. You will be navigated to a page containing the Mapped Host VNets.

Step 3. Click on the **Un-Mapped Host VNets** tab. Within **Select an account to discover**, choose your Subscription ID from the drop-down menu. Then click on **Discover Host VNets**. This will populate all the available VNets associated to the Subscription ID

⊨	Cisco vManage							•	Ê	<b>≜</b> 373	0	admin 🔻
::		OUD ONRAMP	PFOR IAAS Das	hboard > AZURE : westus2	5f70cd2b-baee-4c4	l3-889a-71bb1e8a0e	fc					
ㅁ					Host VNets	Transit VNets						
۵	Mapped Host VNets	Un-Mapp	oed Host VNets	1								
ج 1	Select an account to dis	scover	5f70cd2b-baee-	4c43-889a-71bb1e8a0efc ×	🗘 Disc	cover Host VNets	2					
	Select a VNet	Select VNe	et *									-
	🗘 Map VNet											

Step 4. Click on the drop-down menu located next to **Select a VNet** to choose the VNet you want to map. Once the VNet is selected, click **Map VNet**.

≡	Cisco vManage								•	Ê	<b>"</b> 22	Ø	admin 🔻
::		OUD ONRAMF	PFOR IAAS Dash	board > AZURE : w	vestus2   5f70co	d2b-baee-4c43	3-889a-71bb1e	8a0efc					
▣						Host VNets	Transit VNets						
٠	Mapped Host VNets	Un-Mapp	oed Host VNets										
ج 1	Select an account to dis	scover	5f70cd2b-baee-4	c43-889a-71bb1e8a0e	efc ×	Ø Disc	over Host VN	ets					1
••	Select a VNet	AZ-IAAS   0	COR_Spoke_2										-
	Ø Map VNet 2												_

Step 5. Within pop-up screen, choose the VPN ID. The VPN ID is set to VPN 2.

≡	cisco vManage				<b>A</b>	
55	CONFIGURATION   CLOUD ONRAMP FOR IAA	S Dashboard > AZURE : wes	us2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc			
			Host VNets Transit VNets			
\$	Mapped Host VNets Un-Mapped Host	VNets				
<u>م</u>	Select an account to discover 5f70cd2	Map Host VNets	×			
	Select a VNet AZ-IAAS   COR_Spok	OnRamping multiple	e VNets with overlapping subnets will cause network routing issues.			*
		Transit VNet	COR_TransitVNet X			
		VPN	Select VPN			
			1			
			2			
			·			
		and the second				

Step 6. Define the **IPsec tunnel CIDR** details, **loopback IP** and **BGP ASN** used to build BGP sessions between the Host VNet and the Transit VNet. Also, define a **Host VNet Gateway Subnet** and click on **Map VNets**.

	de de											
	cisco <sup>®</sup> Cisco vManage							•	Ê	A381	0	admin 🔻
==		ONRAMP FOR IAAS Dashboar	d > AZURE : we	stus2   5f70cd2b-bae	e-4c43-889a-71bb1e8	a0efc						
□		OnRamping multiple	VNets with overla	apping subnets will ca	ause network routing i	SSUES.						
<b>ب</b>	Mapped Host VNets	Transit VNet	COR_TransitVI	Net				×				
3	Select an account to disco	VPN	2					×				
÷	Select a VNet	1 IPsec Tunnel CIDR			IPSec Details		Loopbac	k IP				-
	🗘 Map VNet	bc6827c6-041a-4afa-806d	l-433efcd2ed7f	192.168.0.16	/30 192.168.0	.20 /30	1.1.1.3					
		e6bad40d-afec-4ce7-87d2	-c23a08bafcd4	192.168.0.24	/30 192.168.0	.28 /30	1.1.1.4					
		Azure Information										
		2 BGP ASN	65534									
		3 Host VNet Gateway Subnet	10.26.2.128/2	25								
		GIDA. 10.20.2.0/24										
						4	Map VNets	Cancel				
						4						
=	Cisco vManage	_			_			•	Ê	<u>"@</u>	0	admin 👻
=	Gisco VManage			-				•	â	<b>*</b> ®	0	admin 👻
= = _	Cisco vManage Cisco TASK VIEW Map host to transit VPC/VNet	-		-	-			٠	) Initiated	A By: admin	Prom: 100	admin ◄
= :: 	Cisco vManage         TASK VIEW         Map host to transit VPC/VNet         Total Task: 1   Success : 1							•	Ê Initiated	پی By: admin	Prom: 100	admin ▼ ).119.42.246
≡ ∷ ♀	Cisco vManage         TASK VIEW         Map host to transit VPC/VNet         Total Task: 1   Success : 1							•	E Initiated	پی By: admin	<b>2</b> From: 100	admin ▼ 0.119.42.246
= = □ ☆ ∢ ∢	Cisco vManage	Searcl	h Options 🗸					•	Ê Initiated	<b>▲</b> <sup>®</sup> By: admin	<b>2</b> From: 100	admin ▼ 0.119.42.246
= □ \$ \$	Cisco vManage         Image: Cisco vManage <t< th=""><th>Searc</th><th>h Options Y Device IP</th><th></th><th></th><th>Message</th><th></th><th>•</th><th>E Initiated</th><th><b>▲</b>(1) By: admin</th><th><b>2</b> From: 100</th><th>admin 👻</th></t<>	Searc	h Options Y Device IP			Message		•	E Initiated	<b>▲</b> (1) By: admin	<b>2</b> From: 100	admin 👻
≡ ≡ □ ⇔ √ ⇔ ∷	Cisco vManage  TASK VIEW  Map host to transit VPC/VNet  Total Task: 1   Success : 1	Search	h Options 💙 Device IP System		1	Message Finished mapping F	iost VNet COR_S	poke_2	E Initiated	€ By: admin 3 Jul 2020	From: 100 Transition 1:10:46 PM	admin 🗸
	Cisco vManage         Cisco vManage         Map host to transit VPC/VNet         Total Task: 1   Success : 1         V         Status         ✓         Status         ✓         Success         (23-Jul-2020 13:28:4 (23-Jul-2020 13:28:4 (23-Jul-2020 13:28:4 (23-Jul-2020 13:28:4 (23-Jul-2020 13:28:1 (23-Jul-2020 13:29:1 (23-Jul-2020 13:29:1 (23-Jul-2020 13:29:1	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 0 PDT] Creating vpn connect 0 PDT] Created VPN Connect 3 PDT] Created VPN Connect 7 PDT] Finished mapping Hos	h Options Y Device IP System d a Virtual Ne tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp st VNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	f F F COR_COR_Spoke_2 ion_vedge1_vng : COR_COR_Spoke_2 ion_vedge2_vng	Message Finished mapping H _LNG_vedge1 _LNG_vedge2	fost VNet COR_S	poke_2		eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	From: 100 Tr 1:10:46 PM	admin V admin V adm
	Cisco vManage         Cisco vManage         Map host to transit VPC/VNet         Total Task: 1   Success : 1         Q         Status         V< Success         [23-Jul-2020 13:28:4         [23-Jul-2020 13:29:4	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 8 PDT] Created VPN Connecti 9 PDT] Created VPN Connecti 7 PDT] Finished mapping Hos	h Options ✓ Device IP System d a Virtual Ne tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp t VNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	f F F : COR_COR_Spoke_2. i. COR_COR_Spoke_2. i. COR_COR_Spoke_2. on_vedge2_vng	Vessage Inished mapping H _LNG_vedge1 _LNG_vedge2	lost VNet COR_S	poke_2	E Initiated	▲ By: admin 3 Jul 2020	From: 100 T: 10:46 PM	admin V 1.119.42.246 () () () () tal Rows: 1 I PDT () (
	Cisco vManage           Cisco vManage           Task VIEW           Map host to transit VPC/VNet           Total Task: 1   Success : 1           Q           Status           (23-Jul-2020 13:28:4           (23-Jul-2020 13:29:1           (23-Jul-2020 13:29:2           (23-Jul-2020 13:29:4           Jul-2020 13:29:4	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 9 PDT] Created VPN Connecti 8 PDT] Created VPN Connecti 3 PDT] Created VPN Connecti 7 PDT] Finished mapping Hos	h Options V Device IP System d a Virtual Ne tions tion for local ion COR_COR_Sp tion for Local ion COR_COR_Sp t Whet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	: COR_COR_Spoke_2 : COR_COR_Spoke_2 : con_vedge1_vng : COR_COR_Spoke_2 : on_vedge2_vng	Message Finished mapping P _LNG_vedge1 _LNG_vedge2	fost VNet COR_S	poke_2	E Initiated	<b>№</b> By: admin	From: 100 Tr 1:10:46 PM	admin
	Cisco vManage           Cisco vManage           Application           Map host to transit VPC/VNet           Total Task: 1   Success : 1           Q           Status           Status <th>7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 0 PDT] Creating vpn connect 0 PDT] Created VPN Connect 3 PDT] Created VPN Connect 7 PDT] Finished mapping Hos</th> <th>h Options Y Device IP System d a Virtual Ne tions tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp st VNet COR_Sp</th> <th>twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2</th> <th>: COR_COR_Spoke_2 : COR_COR_Spoke_2 : COR_COR_Spoke_2, on_vedge2_vng</th> <th>Vessage Finished mapping H _LING_vedge1 _LING_vedge2</th> <th>lost VNet COR_S</th> <th>poke_2</th> <th>E Initiated</th> <th>▲ By: admin 13 Jul 2020 :</th> <th>From: 100 T:</th> <th>admin V 0.119.42.246</th>	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 0 PDT] Creating vpn connect 0 PDT] Created VPN Connect 3 PDT] Created VPN Connect 7 PDT] Finished mapping Hos	h Options Y Device IP System d a Virtual Ne tions tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp st VNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	: COR_COR_Spoke_2 : COR_COR_Spoke_2 : COR_COR_Spoke_2, on_vedge2_vng	Vessage Finished mapping H _LING_vedge1 _LING_vedge2	lost VNet COR_S	poke_2	E Initiated	▲ By: admin 13 Jul 2020 :	From: 100 T:	admin V 0.119.42.246
	Cisco vManage         Image: Cisco vManage         Map host to transit VPC/VNet         Total Task: 1   Success : 1         V         Status         V         Success         (23-Jut-2020 13:28:4         (23-Jut-2020 13:28:4         (23-Jut-2020 13:28:4         (23-Jut-2020 13:28:4         (23-Jut-2020 13:28:4         (23-Jut-2020 13:29:1         (23-Jut-2020 13:29:1         (23-Jut-2020 13:29:1         (23-Jut-2020 13:29:4	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 9 PDT] Created VPN Connecti 8 PDT] Created VPN Connect 3 PDT] Created VPN Connect 7 PDT] Finished mapping Hos	h Options V Device IP System d a Virtual Ne tions tion for local tion COR_COR_Sp tion for Local tion COR_COR_Sp st WNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	: COR_COR_Spoke_2 : COR_COR_Spoke_2 : COR_COR_Spoke_2 : COR_COR_Spoke_2 oon_vedge2_vng	Message Finished mapping F _LNG_vedge1 _LNG_vedge2	iost VNet COR_S	poke_2	initiated 2	Ry: admin	From: 100 Transition of the second	admin
	Cisco vManage         Image         Map host to transit VPC/VNet         Total Task: 1   Success : 1         Image         Status         Image         Status         Image         Status         Image         Image <t< th=""><th>7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 8 PDT] Creating vpn connect 9 PDT] Created VPN Connect 7 PDT] Created VPN Connect 7 PDT] Finished mapping Hos</th><th>h Options ✓ Device IP System d a Virtual Ne tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp st VNet COR_Sp</th><th>twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2</th><th>: COR_COR_Spoke_2 : COR_COR_Spoke_2 : con_vedge2_vng</th><th>Message Finished mapping H _LNG_vedge1 _LNG_vedge2</th><th>lost VNet COR_S</th><th>poke_2</th><th>E Initiated</th><th>★ By: admin :3 Jul 2020</th><th>From: 100 Ti 1:10:46 PM</th><th>admin V 0.119.42.246</th></t<>	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 8 PDT] Creating vpn connect 9 PDT] Created VPN Connect 7 PDT] Created VPN Connect 7 PDT] Finished mapping Hos	h Options ✓ Device IP System d a Virtual Ne tion for local ion COR_COR_Sp tion for local ion COR_COR_Sp st VNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	: COR_COR_Spoke_2 : COR_COR_Spoke_2 : con_vedge2_vng	Message Finished mapping H _LNG_vedge1 _LNG_vedge2	lost VNet COR_S	poke_2	E Initiated	★ By: admin :3 Jul 2020	From: 100 Ti 1:10:46 PM	admin V 0.119.42.246
	Cisco vManage           Cisco vManage           Ask VIEW           Map host to transit VPC/VNet           Total Task: 1   Success : 1           Q           Status           Sourcess           [23-Jul-2020 13:28:4           [23-Jul-2020 13:28:4           [23-Jul-2020 13:28:4           [23-Jul-2020 13:28:4           [23-Jul-2020 13:28:4           [23-Jul-2020 13:29:1           [23-Jul-2020 13:29:2           [23-Jul-2020 13:29:4	7 PDT] Successfully created 7 PDT] Creating vpn connect 7 PDT] Creating vpn connect 0 PDT] Created VPN Connecti 0 PDT] Created VPN Connect 3 PDT] Created VPN Connect 7 PDT] Finished mapping Hos	h Options ✓ Device IP System d a Virtual Ne tions tion for local ion COR_COR_Sp ion COR_COR_Sp st WNet COR_Sp	twork Gateway network gateway oke_2_vpnConnecti network gateway oke_2_vpnConnecti oke_2	f F F COR_COR_Spoke_2. on_vedge1_vng : COR_COR_Spoke_2. ion_vedge2_vng	Message Finished mapping F _LNG_vedge1 _LNG_vedge2	iost VNet COR_S	poke_2	initiated	★ By: admin 33 Jul 2020	From: 100 Tr 1:10:46 PM	admin V 0.119.42.246 Colla Rows: 1 IPDT

Step 7. The Cloud onRamp main page will appear similar to the figure below.

cisco <sup>°</sup> Cisco vMan	age					•	Ê	<b>A</b>	0	adn
CONFIGURATION	CLOUD ONRAMP F	OR IAAS								
Add New Cloud	Instance									
				Transit V	ew Host View					
🌣 Microso	ft Azure Enterp	rise   Mapped /	Accounts : 1							
westus2										
	Mapped Host	VNets (Total: 2)	Transit VN	ets (Total: 1)						
Microsoft Azure	<u>↑</u> 2	↓0	<u>^2</u>	↓0						
	Conne	ections	Devi	ices						

# Operate - Cisco Cloud on Ramp for IaaS Monitoring

Using the vManage GUI, you can monitor, troubleshoot, and manage the Cisco SD-WAN Cloud onRamp for laaS using Azure deployment. The 3 main ways to troubleshoot the deployment are as follows:

vManage Cloud onRamp for IaaS Dashboard: From the vManage Cloud onRamp for IaaS dashboard you can monitor the connectivity state of each host VNet, the state of the transit VNet, and detailed traffic statistics for IPsec VPN connections between the transit VNet and the host VNets.

vManage Monitor Dashboard: From the vManage Monitor dashboard, you can view and gather error logs and interface details for the WAN Edge cloud routers deployed in the transit VNet

vManage SSH Server Dashboard: The vManage SSH server dashboard provides the option to manage and monitor the WAN Edge device via CLI.

At the end this section, you will find some of the common deployment mistakes.

## Process 1: vManage Cisco Cloud onRamp for laaS Dashboard

#### Procedure 1: View the connectivity state of each transit VNet

Step 1. Select the **cloud** icon at the top of the vManage GUI.

Step 2. From the drop-down menu select **Cloud onRamp for laaS**.

Alternatively, to get to this page, you can select **Configuration** > **Cloud onRamp for laaS** in the left-hand column of vManage.

You will be navigated to the following page.

	cisco	Cisco vMana	age			
	🌣 co	NFIGURATION	CLOUD ONRAMP F	OR IAAS		
	Đ	Add New Cloud	Instance			
1						
						Transit Vie
		C Microsof	ft Azure Enterp	rise   Mapped	Accounts : 1	
		westus2				
			Mapped Host	VNets (Total: 2)	Transit VNe	ets (Total: 1)
		Microsoft	<b>∧</b> 2		<b>∧</b> 2	
		Azure	Ϋ́	VU		VU
			Connec	ctions	Devie	ces

The aggregate number of host VNets which are reachable is indicated with a green "up" arrow under **Mapped Host VNets**. Likewise, the aggregate number of host VNets which are unreachable is indicated with a red "down" arrow. The color-coded "up" and "down" arrows indicate whether the IPsec VPN tunnels connecting the host VNets with the transit VNets are up or down.

The aggregate number of Cisco vEdge Cloud routers which are reachable is indicated with a green "up" arrow under **Transit VNets**. Likewise, the aggregate number of Cisco vEdge Cloud routers which are unreachable is indicated with a red "down" arrow. In the case of the transit VNet, the color-coded "up" and "down" arrows indicate whether the logical Cisco vEdge Cloud router is reachable or not. Generally, reachability indicates whether the Cisco vEdge Cloud router is running or not. Since there are two Cisco vEdge Cloud routers per transit VNet, the number of devices shown here should be twice the number of transit VNets.

Step 3. Click on **Host View** tab to gather additional details about the Azure account Name, hosted cloud region, VPN segmentation details per VNet, along with the reachability state of each transit VNet and host VNet.

≡	cisco Cisc	co vManage						•	3	<b>*</b>	0	admin 👻
::	CONFIG	URATION   CLOUD ONRA	MP FOR IAAS									
▫	• Add 1	New Cloud Instance										
٠					Transit View	Host View						
عر											0	)
ŝ	Q			Search Options ${\color{red} }$							Total Rows:	2
	~	Host VPC Account Na	Cloud Type	Cloud Region	Host VPCs	Mapped Transit VPC	VPN Segment				Transit VPC	s
	~	Microsoft Azure Ente	AZURE									
				westus2	COR_Spoke_2	COR_Transit/Net	2				<b>↑</b>	
				westus2	COR_Spoke_1	COR_TransitVNet	1				1	
		(e										

≡	cisco	Cisco vManag	e					•	Ê	<b>4</b>	0	admin 🔻
	🌣 co	NFIGURATION   C	LOUD ONRAMP FOR I	AAS								
▫	0	Add New Cloud In	stance									
٠						Transit View	Host View					
عر											0	•
÷		Q			Search Options $\checkmark$						Total Rows:	2
		∼ je	Cloud Region	Host VPCs	Mapped Transit VP	С	VPN Segment	Transit VPC	State	Host VF	C State	
•••		~	westus2 westus2	COR_Spoke_2 COR_Spoke_1	COR_TransitVNet COR_TransitVNet		2	个 个		↑ ↑		
			_					 	_	_	_	

Step 4. When you click on the cloud instance, by default you are taken to a screen which displays the state of each host VNet within that cloud instance. An example is shown in the following figure.

≡	cisco Cisco vMar	nage				•	Ê	<b>_</b>	0	admin 🔫
=		I   CLOUD ONRAMP FOR IAAS								
▣	Add New Clou	d Instance								
٠				Transit Vie	w Host View					
عر										
÷	🌣 Micros	oft Azure Enterprise   Mapp	ed Accounts : 1							
*	westus2									
		Mapped Host VNets (Total: 2	Transit VNet	s (Total: 1)						
	Microsoft Azure	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	↑2	↓0						
		Connections	Device	2S						

You can see specific details regarding whether individual host VNets are up or down, as well as their associated transit VNet. You can also see which service VNet the host VNet is mapped to at the transit VNet.

≡	cisco C	Cisco vManage						•	Ê	<b>A</b>	9	admin 🔻
::	CONF	FIGURATION   CLO	UD ONRAMP FOR IAAS Dash	ooard > AZURE:w	vestus2   5f70	0cd2b-baee-4c43-889a-71b	bb1e8a0efc					
▫						Host VNets Transit VNe	ets					
٠	Марр	ed Host VNets	Un-Mapped Host VNets									
ع •	0 Rov	ws Selected 🔯 U	Jn-Map VNets									0
	Q			Search Options 🗸							Tota	al Rows: 2
*		Host VNets	Host VNet Account Nat	ne Resour	ce Group	Mapped Transit VNe	t Host VNet Sta	ite Transit V	Net State	VPI	N Segment	
•		COR_Spoke_2	Microsoft Azure Enterp	rise AZ-IAA	S	COR_TransitVNet	$\uparrow$	$\uparrow$		2		
		COR_Spoke_1	Microsoft Azure Enterp	rise AZ-IAA	S	COR_TransitVNet	$\uparrow$	$\uparrow$		1		

Step 5. Click on the **Transit VNets** tab to view the details of each transit VNet within the cloud instance.

	cisco	Cisco vManage					▲ Ê 4	💯 😗 admin
	¢ co	NFIGURATION   CLOUD	ONRAMP FOR IAAS Dash	board > AZURE : westus2	5f70cd2b-baee-4c43-889a-71	bb1e8a0efc		
⊐					Host VNets Transit VN	lets		
•	G	Add Transit VNet						08
	Q			Search Options 🗸				Total Rows: 1
,	~	Transit VNet Name	Transit VNet Id	Size of Transit VNet	Transit VNet CIDR	Device Pair Id	WAN edge Serial Number/ OTP	Hostname
-	~	COR_TransitVNet	/subscriptions/5f70cd2	Standard F8 (8 vCPU)	10.0.1.0/24			***
						bc6827c6-041a	bc6827c6-041a-4afa-806d-433efcd2ed7f e6bad40d-afec-4ce7-87d2-c23a08bafcd4	onRamp_vEdge-Clou onRamp_vEdge-Clou
ech	nnica	l Tip						
יווכ	can	re-arrange the	columns by dr	aqqinq-and-dr	opping them so t	hat the colu	mns with the most relev	ant information

You can re-arrange the columns by dragging-and-dropping them so that the columns with the most relevant information come first, as shown in the figure above. The state of each of the Cisco vEdge Cloud routers within each transit VNet is displayed with a green "up" arrow or a red "down" arrow.

Q		Search Options	learch Options 🗸						
~	Transit VNet Name	Transit VNet Id	Host VPCs	Interface	WAN edge State	Size of Transit VNet	Device Pair Id	WAN edge Serial Number/ OTP	
Ý	COR_TransitVNet	/subscriptions/5f70cd2				Standard F8 (8 vCPU)			•••
			2	~~	$\wedge$		bc6827c6-041a	bc6827c6-041a-4afa-806d-433efcd2ed	
					·			e6bad40d-afec-4ce7-87d2-c23a08bafc	

Step 6. Click on under **Host VPCs** (VNets) column to view the state of the host VNets.

cisi	co C	isco vManage						<b>●</b> É	i 🍂	0	admin 🔻
\$	CONF	IGURATION   CLO	OUD ONRAMP FOR IAAS Dashb	oard > A	ZURE : westus2   5f70cd2	b-baee-4c43-889a-71bb1	e8a0efc				
					Hos	st VNets Transit VNets					
	🕈 A	dd Transit VNet									
	Q			Search Opt	ions 🗸					Tota	I Rows: 1
	~	Device Pair Id	WAN edge Serial Number/ OTP		Hostname	System IP	Instance Id	WAN edge State	Interface	Host VPCs	
	Ý										•••
		bc6827c6-041a	bc6827c6-041a-4afa-806d-433e e6bad40d-afec-4ce7-87d2-c23a	fcd2ed7f 08bafcd4	onRamp_vEdge-Cloud1 onRamp_vEdge-Cloud2	10.1.0.136 10.1.0.137	/subscriptions/5f70c /subscriptions/5f70c	$\uparrow$	~*	2	
			Cisco vManage	CONFIGURATION   CLOUD ONRAMP FOR IAAS Dashb	Cisco vManage         CONFIGURATION   CLOUD ONRAMP FOR IAAS       Dashboard > A         Add Transit VNet       Q       Search Opt         V       Device Pair Id       WAN edge Serial Number/ OTP         V       Device Pair Id       bc6827c6-041a-4afa-806d-433efcd2ed7f         bc6827c6-041a       bc6827c6-041a-4afa-806d-433efcd2ed7f         e6bad40d-afec-4ce7-87d2-c23a08bafcd4	CONFIGURATION   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f7ocd2	Cisco vManage         CONFIGURATION   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD ONRAMP FOR IAAS Dashboard > AZURE : westus2   5f70cd2b-base-4c43-889a-71bb1         Image: Configuration   CLOUD	Cisco VManage         CONFIGURATION   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   5f70cd2b-baee-4c43-889a-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options ~         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options ~         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options ~         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options ~         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options / Sf70c         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options / Sf70c         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options / Sf70c         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options / Sf70c         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options / Sf70c	Clsco vManage       Image:	Cisco vManage           CONFIGURATION   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   St70cd2b-base-4c43-8899-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   St70cd2b-base-4c43-8899-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   St70cd2b-base-4c43-8899-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   St70cd2b-base-4c43-8899-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Dashboard > AZURE : westus2   St70cd2b-base-4c43-8899-71bb1e8a0efc         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOUD ONRAMP FOR IAAS       Bearch Options *         Image: Configuration   CLOU	Cisco vManage     ConFiguration   cloud onRAMP FOR IAAS     Dehica Pair Id     MAN edge Secial Number/ OTP     Host Weis     Image     Obelse27ce-041a     Cobes27ce-041a     Cobes27ce-041a

≡	cisco vManage					•	ê 🔎	0	admin 🔻
::	CONFIGURATION   CLOUD ONRAMP FO	RIAAS Dashboard > AZURE : we	estus2   5f70cd2b-baee-4c43-88	9a-71bb1e8a0efc					
		Mapped Host Vpcs for this Dev	ice Pair		×				
-					6				~~
¥	Add Transit VNet	0	Sea	rch Ontions 🗸	Total Rows: 2				Qe
3	Q	Ч.						Tot	al Rows: 1
÷	V Device Pair Id WAN edge Seria	COR_Spoke_2				State		Host VPCs	
	×	COR_Spoke_1	1						•••
	bc6827c6-041a bc6827c6-041a e6bad40d-afec-4						~	2	
					Close				
				_			_		•

# Procedure 2: View detailed traffic statistics for the IPsec VPN connections between the transit VNet and each host VNet

Although the more detailed information discussed in the previous procedure is useful in determining if a given Cisco vEdge Cloud router is up or down, it doesn't provide any information regarding the traffic between the transit VNet and each host VNet.
Step 1. Click on the graph icon for one of the Cisco WAN Edge Cloud routers under the Interface Stats column shown in the figure.

≡	altalta cisco	Cisco vManage						•	ê 🍂	0	admin 👻
::	CON	IFIGURATION   CL	OUD ONRAMP FOR IAAS Dashb	ooard > AZ	URE : westus2   5f70cd2	b-baee-4c43-889a-71bb1	e8a0efc				
▣					Hos	st VNets Transit VNets					
٠	O	Add Transit VNet									0
عر	Q			Search Optio	ons 🗸					Tota	al Rows: 1
÷	$\sim$	Device Pair Id	WAN edge Serial Number/ OTP		Hostname	System IP	Instance Id	WAN edge State	Interface	Host VPCs	
*	Ŷ										•••
•		bc6827c6-041a	bc6827c6-041a-4afa-806d-433e e6bad40d-afec-4ce7-87d2-c23a	efcd2ed7f 08bafcd4	onRamp_vEdge-Cloud1 onRamp_vEdge-Cloud2	10.1.0.136 10.1.0.137	/subscriptions/5f70c /subscriptions/5f70c	$\uparrow$	~	2	

A pop-up screen displaying statistics for the IPsec VPN connections between the Cisco Cloud onRamp for IaaS transit VNet router and the host VNets is displayed.

	cisco Cis	co vM	lanage							•		<u>¢</u>		
55		IPSEC	C Interfa	ce Statistics									×	
		🖪 CI	hart Opt	ions 🔻 IP	v4 & IPv6 🔻				🔻 Real Tim	ie 1h 3h 6h 12	h <mark>24h</mark> 7days	Custom 👻	·	
ш.		2	kbps							Legend				
\$	🕀 Ado	sd								ipsec13				
3	0	4X 71	kbps							ipsec14				Total Rows: 1
	~	_	0		• • • • • • • • • • • • • • • • • • • •	•				ipsec15			- 18	
÷	×	2	kbps							ipsec16			PO	)s
	Ť	sdc											- 18	•••
		ΎΕ	kbps										- 18	
			0		• •	•	•	•					2	
				Jul	23, 14:00			Jul 23, 1	6:00				- 10	
			4 Pov	vs Selected										
			4 100	vs Selected							<b>U</b>		- 18	
			Q			Search Op	ptions 🗸				Total Ro	ows: 4	- 18	
			Oper 🕹	(0) Oper 🛧 (4	) Admin 샂 (0) Admin 🛧 (4)								- 18	
				Interface↑ <sub>3</sub>	Interface Description		IP Address	IPv6 Address	VPN↑ <sub>2</sub>	Admin Status	Oper Statu	ıs∳ <sub>1</sub>		
				ipsec13	-		192.168.0.1/30	-	1	$\uparrow$	$\uparrow$			
			✓	ipsec14	-		192.168.0.5/30		1	$\mathbf{\uparrow}$	$\uparrow$			
				ipsec15	-		192.168.0.17/30	-	2	$\uparrow$	$\uparrow$			
				ipsec16	-		192.168.0.21/30		2	$\uparrow$	$\uparrow$			

Step 2. From the drop-down menu under Chart Options, you can select the information displayed within the graph over each collection interval. The options are as follows:

Kbps - Traffic rate in kilobits per second for each collection interval

Packets - Packets seen over each collection interval

- Octets Bytes seen over each collection interval
- Errors Number of errors over each collection interval
- Drops Number of dropped packets over each collection interval

Pps - Rate in packets per second over each collection interval



Step 3. You can also select one of the Legends to list details specific to that.

≡	cisco Cis	co vManag	e						•	Ê	<b>A</b>	admin
sa		IPSEC Interf	ace Statistics								×	
		🔝 Chart Opt	tions 👻 IP	v4 & IPv6 ▼				🔻 Real Tim	e 1h 3h 6h 12h	24h 7days	Custom 👻	
-		500							Legend			
۵	🕈 Ado	ckets		• •	•	•	•		• ipsec13			
L	Q	RX Pa							ipsec14			Total Rows: 1
<u> </u>	~	0							ipsec15			'PCs
•	~	500 S		••					ipsec ro			
*		Packet										
		TX I										2
	_	0 Jul 23, 1	.3:30 Jul 23	3, 14:00 Jul 23, 14:30	Jul 23, 1	5:00 Jul 23, 15	:30 Jul 23, 16	:00 Jul 23,	16			
										-	-	-
		4 Ro	ws Selected							(¢)	₿	
		Q			Search O	ptions 🗸				Total Row	/s: 4	
		Oper 🤸	(0) Oper 🛧 (4	) Admin 샂 (0) Admin 🛧 (4)								
			Interface↑ <sub>3</sub>	Interface Description		IP Address	IPv6 Address	VPN↑ <sub>2</sub>	Admin Status	Oper Status	<b>₽</b> 1	
			ipsec13	-		192.168.0.1/30	-	1	<b>^</b>	$\uparrow$		
		<b>~</b>	ipsec14			192.168.0.5/30		1	$\uparrow$	$\uparrow$		
			ipsec15	-		192.168.0.17/30	-	2	1	Υ		
			ipsec16	-		192.168.0.21/30	-	2	$\uparrow$	$\uparrow$		

Step 4. The collection interval displayed within the graph varies based upon overall length of time displayed within the graph. This is selected in the upper right corner of the pop-up window. The time interval named Custom allows you to select a custom start date & time and end date & time. The collection interval depends on the start and end dates and times.



The collection interval is important because traffic rates may appear differently depending upon the interval over which they are averaged. Likewise, packet or byte counts will appear smaller over smaller collection intervals.

Statistics are displayed in both the transmit and receive direction – from the perspective of the Cisco WAN Edge Cloud router logical IPsec interfaces configured within the transit VPN. By default, statistics are displayed for all IPsec interfaces. You can remove an interface from the graph by un-selecting it in the panel below the graph.

#### Process 2: vManage Monitor Dashboard

#### Procedure 1: Monitor SD-WAN devices via Monitor tab

Step 1. To monitor both your controllers and WAN Edge devices within the Transit VNet, Navigate to **Monitor** > **Events**.



Step 2. To view more details for the error logs, you can also monitor your device by navigating to **Monitor** > **Audit Log** and click on the three dots (...) located on the right. Click on **Audit Log Details** to view the more details for the selected log message.

	de de la compañía de									
∣≡	cisco Cisco vi	/lanag	e				● Ê	<u> </u>	) (	admin 🤊
::	Dashboard	>	MONITOR   AUDIT LOG							
	Monitor		〒 Filter ▼				1h 3h	6h 12h <mark>24h</mark> 7da	ays Cust	om 👻
<u> </u>	MONITO	1							6	
	Geography									
	Network		Q		Search Options 🗸				Total Rov	vs: 256
	Network		Timestamp	User	User IP	Message	Module	Feature	Device	
	Alarms		23 Jul 2020 11:57:50 AM PDT	admin	100.119.42.246	Device Validation Template device config - Valid	template	template-device	. Valida	•••
	Events		23 Jul 2020 11:57:50 AM PDT	system	172.27.0.14	Completed unmapping task for host $vnet(s)$ : $[u'$	device	cloud-on-ramp	Systen	•••
_		_	23 Jul 2020 11:48:38 AM PDT	admin	100.119.42.246	Template Onramp_Transit_WAN_edge_Template	template	template-device	10.1.0	••••
	Audit Log	2	23 Jul 2020 11:48:37 AM PDT	admin	100.119.42.246	Completed template push to device.	template	template-device	vedge-	
	ACL Log		23 Jul 2020 11:48:36 AM PDT	admin	100.119.42.246	Template Onramp_Transit_WAN_edge_Template	template	template-device	10.1.0	•••
			23 Jul 2020 11:48:35 AM PDT	admin	100.119.42.246	Completed template push to device.	template	template-device	vedge-	•••
\$	Configuration	>	23 Jul 2020 11:48:17 AM PDT	admin	100.119.42.246	Device Validation Template device config - Valid	template	template-device	Valida	
a	Tools	>	23 Jul 2020 11:48:17 AM PDT	system	172.27.0.14	Completed unmapping task for host vnet(s) : [u'	device	cloud-on-ramp	Systen	••• 3
		Ť	23 Jul 2020 11:46:16 AM PDT	admin	100.119.42.246	Successfully saved credentials for accountId:5f	device	cloud-o Audit L	.og Detai	ils 🔺
_ ≏	Maintenance	>	23 Jul 2020 11:45:40 AM PDT	admin	100.119.42.246	Device became unreachable. Configuration tem	template	template-uevice	. JZ/40	•••
	Administration	>	23 Jul 2020 11:45:39 AM PDT	admin	100.119.42.246	Device became unreachable. Configuration tem	template	template-device	46bc4	•••
		,	23 Jul 2020 11:45:31 AM PDT	admin	100.119.42.246	Device Validation Template device config - Valid	template	template-device	. Valida	
	vAnalytics	>	23 Jul 2020 11:45:21 AM PDT	admin	100.119.42.246	Template Onramp_Transit_WAN_Edge_Template	template	device		•••
			23 Jul 2020 11:42:08 AM PDT	admin	100.119.42.246	Successfully saved credentials for accountId:5f	device	cloud-on-ramp	-	
			23 Jul 2020 11:39:09 AM PDT	admin	100.119.42.246	Authentication succeeded for admin, source IP:1	user	user	172.27	

≡	cisco Cisco vM	lanag	çe					▲ Ê	¢ <sup>20</sup> Ø	ć	admin 🤜
5											
		\$	· 〒 Filter ▼					1h 3h	6h 12h <mark>24h</mark> 7day	ys Custo	om 👻
_		<i>.</i>							(	6) <b>E</b>	
			Q		Search Options 🗸				1	Total Row	vs: 256
			Timestamp				~			Device	
			23 Jul 2020 11:57:50 AM P	idit Log Details			x ig - Valid	template	template-device	Valida <sup>.</sup>	•••
			23 Jul 2020 11:57:50 AM F	[23-Jul-2020 11:41:18 PDT	] Unmapping host from	n transit VPC/VNet	et(s) : [u'	device	cloud-on-ramp	Systen	
			23 Jul 2020 11:48:38 AM F	[23-Jul-2020 11:41:19 PDT 71bb1e8a0efc	] Un-Mapping Host VN	let in 5f70cd2b-baee-4c43-889a-	Template.	. template	template-device	10.1.0	•••
	Audit Log		23 Jul 2020 11:48:37 AM F	[23-Jul-2020 11:41:19 PDT	] Location : westus2	t-VNFT-1		template	template-device	vedge-	•••
			23 Jul 2020 11:48:36 AM F	[23-Jul-2020 11:41:20 PDT	Checking for Cloud O	n Ramp Vpn Connections	Template.	. template	template-device	10.1.0	••••
			23 Jul 2020 11:48:35 AM F	successfully deleted	] COR_AZ-HOST-VNE I-	I_vpnConnection_vedge1_vng was		template	template-device	vedge-	•••
\$			23 Jul 2020 11:48:17 AM F		-		fig - Valid	template	template-device	Valida	•••
a			23 Jul 2020 11:48:17 AM F			01	et(s) : [u'	device	cloud-on-ramp	Systen	•••
			23 Jul 2020 11:46:16 AM F			Close	puntld:5f	device	cloud-on-ramp		•••
۵			23 Jul 2020 11:45:40 AM PDT	admin	100.119.42.246	Device became unreachable. Con	figuration tem	template	template-device	5274c	•••
			23 Jul 2020 11:45:39 AM PDT	admin	100.119.42.246	Device became unreachable. Con	figuration tem	template	template-device	46bc4	•••
			23 Jul 2020 11:45:31 AM PDT	admin	100.119.42.246	Device Validation Template devic	e config - Valid	template	template-device	Valida <sup>.</sup>	•••
			23 Jul 2020 11:45:21 AM PDT	admin	100.119.42.246	Template Onramp_Transit_WAN_	Edge_Template.	. template	device		•••
			23 Jul 2020 11:42:08 AM PDT	admin	100.119.42.246	Successfully saved credentials for	r accountId:5f	device	cloud-on-ramp		
			23 Jul 2020 11:39:09 AM PDT	admin	100.119.42.246	Authentication succeeded for adr	min,source IP:1	. user	user	172.27	

Step 3. To view interface and its associated traffic statistics, navigate to **Monitor** > **Network**, and select the device.



Step 4. You can alternatively view error logs specific to the WAN Edge device by clicking on the **Events** tab.



## Process 3: vManage SSH Server Dashboard

Procedure 1: To monitor the WAN Edge routers hosted on transit VNet via vManage CLI, navigate to **Tools** > **SSH** and log into the one of the transit VNet vEdge routers.

Step 1. To view the BGP route details, from the CLI, issue the following commands "show bgp <neighbor/ routes/ summary>" and "show ip route bgp <detail>".

≡	cisco	' Cisco vMa	nage									•	Ê	<b>≜</b> <sup>429</sup>	0	admin 👻
::	🔧 т	OOLS   SSH TER	MINAL													
ᅟᅟ	>	10.1.0.137 ×														
	onR	amp_vEdge-Clo	ud2#sh	ow bgp sum	mary											
±	e vpn															
<b>*</b>	evi bgb	-router-ident	ifier	10.1.0.13	37											
5	- 1oc	al-as		64600												
	rib	-entries		784												
~	tot	al-peers		2												
2	pee	er-memory		9632												
	Loc	al-soo		So0:0:115	5001											
*	ign	ore-soo														
				MSG	MSG	OUT		PREFIX	PREFIX	PREFIX						
11.	NEI	GHBOR	AS	RCVD	SENT	Q 	UPTIME	RCVD	VALID	INSTALLED	STATE					
	10.	25.2.132	65534	11216	9838		0:11:11:05				established					
	10.	25.2.133	65534	11190	9836		0:11:10:49				established					
	vpn			2												
	bgp	-router-ident	ifier	10.1.0.13	37											
	loc	al-as		64600												
	rib	-entries														
	rib	-memory		784												
	tot	al-peers		2												
	pee	er-memory		9632	0.01											
	ign	a1-500		SOU:0:11:	5001											
	- gr	010 000		MSG	MSG	OUT		PREFIX	PREFIX	PREFIX						
	NEI	GHBOR	AS	RCVD	SENT	Q	UPTIME	RCVD	VALID	INSTALLED	STATE					
	10.	26.2.132	65534	11006	9645	0	0:10:41:57	4	4	4	established					
	10.	26.2.133	65534	10990	9650		0:10:41:45				established					

≡	il c	Cisco vManage								•	Ê	<b>4</b> 22	0	admin 👻
::	٩	TOOLS   SSH TERMINAL												
	>	10.1.0.137 ×												
* * *	Device List	onRamp_vEdge-Cloud2# show Codes Proto-sub-type: IA -> ospf-intra-area, El -> ospf-externall, H Nl -> ospf-nssa-externa e -> bgp-external, i -> Codes Status flags: F -> fib, S -> selected B -> blackhole, R -> re	<pre>v ip routes bgp IE -&gt; ospf-inter- 22 -&gt; ospf-externa 111, N2 -&gt; ospf-as &gt; bgp-internal i, I -&gt; inactive, scursive</pre>	area, 12, sa-externa]	.2,									
				PROTOCOL	NEXTHOP	NEXTHOP	NEXTHOP							
		VPN PREFIX ENCAP STATUS	PROTOCOL	SUB TYPE	IF NAME	ADDR	VPN	TLOC IP	COLOR					
		1 1.1.1.2/32	bgp			10.25.2.132								
		- F,S,R 1 10.25.2.0/24	bgp			10.25.2.132								
		- F,S,R 1 192.168.0.1/32	bgp			10.25.2.132								
		- F,S,R 1 192.168.0.5/32	bgp			10.25.2.132								
		2 1.1.1.4/32	bgp			10.26.2.132								
		2 10.26.2.0/24	bgp			10.26.2.132								
		2 192.168.0.17/32	bgp			10.26.2.132								
		- F,S,R 2 192.168.0.21/32	pdb	i	-	10.26.2.132	-	-	-					

Step 2. To view IPsec active sessions via CLI issue the "show IPsec ike sessions | tab" command.

≡	ار ci	isco vManage							•	ê	<b>42</b>	0	admin 🔻
	٩	TOOLS   SSH TERMINAL											
	>	10.1.0.137 🗙											
	List	onRamp_vEdge-Cloud2#											
\$	evice	onRamp_vEdge-Cloud2# onRamp_vEdge-Cloud2#											
-	ă	onRamp_vEdge-Cloud2#											
4		onRamp_vEdge-Cloud2#											
		onRamp_vEdge-Cloud2#											
Ê		onRamp_vEdge-Cloud2# onRamp_vEdge-Cloud2# show ipsec i	ke sessions   tab										
••			COURCE	DRCM									
			TUNNEL	0631									
		VPN IF NAME VERSION SOURCE IP	PORT DEST IP	PORT	INITIATOR SPI	RESPONDER SPI	CIPHER SUITE	DH GR					
-		OUP STATE UPTIME	UPTIME										
		1 ipsec13 2 10.0.1.37	4500 20.191.64.244	4500	62674824bf4184e7	0f5860836c84321f	aes128-cbc-sha1	2 (MO					
		DP-1024) IKE_UP_IPSEC_UP 0:03:3	7:02 0:11:13:19										
		1 ipsec14 2 10.0.1.37	4500 52.158.247.205	4500	b964ccc9bc9c0fb6	a3c65500c1b99c2c	aes128-cbc-shal	2 (MO					
		DP-1024) IKE_UP_IPSEC_UP 0:04:0	5:47 1:02:48:43	4500	6			2 (110					
		2 1psec15 2 10.0.1.37	4500 52.1/5.251.1/ 9.08 1.02.48.43	4500	ICC/3C2F0D0a108a	C6490434063eb109	aes128-CDC-Shal	2 (MO					
		2 ipsec16 2 10.0.1.37	4500 52.175.251.108	4500	456eaf65ba8a307f	e5784106e787dc6c	aes128-cbc-sha1	2 (MO					
		DP-1024) IKE_UP_IPSEC_UP 0:04:2	9:26 1:02:48:43										
		<b>D</b>											
		onRamp_vEdge=Cloud2#											
		onRamp vEdge-Cloud2#											
		onRamp_vEdge-Cloud2#											
		onRamp_vEdge-Cloud2#											
		onRamp_vEdge-Cloud2#											
		onRamp_vEdge-Cloud2#											

# **Some Common Deployment Mistakes**

#### Note 1: Entering an Incorrect Host Gateway Subnet

During the mapping process, make sure to enter a Host Gateway subnet that is valid for the CIDR configured within the host VNet.

≡	ahah cisco	' Cisco vManage			▲ Ê	<b>*</b> @	🕑 admin 🗸
::	Ê TA	ASK VIEW					
	Map h	host to transit VPC/VNet			In	nitiated By: admin	n From: 100.119.42.88
*	Total	Task: 1   Failure : 1					
							08
	Q		Search Options 🗸				Total Rows: 1
-	>	Status	Device IP	Message		Start Time	
*	~	😣 Failure	System	Failed to map gateway vpc/vnet		23 Sep 2020 2	2:17:10 PM PDT
		<pre>[23-sep-2020 14:17:12 PDT] reating Gateway [23-sep-2020 14:17:13 PDT] Could not creat Message: Subnet 'GatewaySubnet' is not val [23-sep-2020 14:17:13 PDT] Stopping mappin [23-sep-2020 14:17:13 PDT] Failed to map f [23-sep-2020 14:17:13 PDT] Failed to map f</pre>	Vnet : A2-Hosi y Subnet in AZ- e Gateway Subne id in virtual r g process ost VNet : AZ-H ateway vpc/vnet	-WRET-2 Host-VNET-2 t : Was not able to create a gateway subnet in AZ-Host-VNET-2 :Azu etwork 'AZ-Host-VNET-2'. ost-VNET-2	ıre Error: Net	cfgInvalidSub	net

#### Note 2: Entering an Incorrect IPsec IP address CIDR Gateway Subnet

During the mapping process, make sure to enter an IPsec addresses that does not overlap with the host VNet subnet or address space.

≡	cisco	Cisco vManage		▲ Ê	<b>*</b> ® (	admin 🕶
::	Ê T/	ASK VIEW				
	Map	host to transit VPC/VNet		In	nitiated By: admin	From: 100.119.42.88
	Total	Task: 1   Failure : 1				
<b>*</b>						00
3	0					Total Rows: 1
÷	Q		Search Options V			Total Nows. 1
*		Status	Device IP	Message	Start Time	
_	-	[23-Sep-2020 14:40:25 PDT] Successfully c	reated a Virtual Network Gateway	Palled to map gateway vpc/ viet	23 Sep 2020 2.24	.05 PM PD1
		[23-Sep-2020 14:40:25 PDT] Creating vpn c [23-Sep-2020 14:40:26 PDT] Creating vpn c [23-Sep-2020 14:40:27 PDT] Error with Cre Message: Virtual Network Gateway connecti [23-Sep-2020 14:40:27 PDT] Could not creating [23-Sep-2020 14:40:27 PDT] Could not creating [23-Sep-2020 14:40:27 PDT] Could no	onnections onnection for local network gateway : COR_COR_ ating VPN Connections : Azure Error: GatewayCo on /subscriptions/5f70cd2b-baee-4c43-889a-71bb te VPN connections	Spoke_2_LNG_vedge1 nmectionHasOverlappingAddressSpaces le8a0efc/resourceGroups/AZ-IAAS/providers/Microsc	oft.Network/conne	ctions/C
						^ ¥

# Appendix A: New in this Guide

This guide is new and is not updated from a previous version.

# Appendix B: Hardware and Software Used for Validation

This guide was validated using the following hardware and software.

Table 7.System Feature Template Settings

Functional Area	Product	Software Version
Cloud	Cisco vManage NMS	19.2.2
Cloud	Cisco vBond Controller	19.2.2
Cloud	Cisco vSmart Controller	19.2.2
Data center	Cisco vEdge 5000 Series Routers	19.2.2
Branch office (cloud)	Cisco vEdge	19.2.2
Transit VNet (cloud)	Cisco vEdge	19.1.0

Note: 19.1.0 was chosen to validate and deploy the cloud onRamp solution as it is the latest version available the vManage GUI running version 19.2.2/20.1 code.

# Appendix C: Transit VNet Cisco WAN Edge Device and Feature Templates

This section includes the device and feature templates specific to the Cisco vEdge Cloud router attached to the Transit VNet device template. For templates specific to Data Center and Branch, refer to the <u>Cisco SD-WAN</u> <u>End-to-End Deployment Guide</u>.

#### Feature Template

Within this section, the configured lists, the main security policy template and its container template is listed.

#### Cisco vEdge feature templates

The following feature templates are common across Cisco vEdge and vEdge Cloud routers within the SD-WAN for this deployment guide. In other words, they apply not only to the Cisco vEdge Cloud routers within the transit VNet, but also to other physical and/or logical Cisco vEdge routers within the branch locations.

#### Technical Tip

The configuration of the physical and/or logical Cisco SD-WAN Edge routers within the branch locations are not discussed within this deployment guide.

#### vEdge System feature template

Devices:	All Cisco vEdge
Template:	Basic Information / System
Template Name:	vEdge_System_Template
Description:	vEdge System Template

Table 8. vEdge System feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_host_name
	Device Groups	Device Specific	system_device_groups
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset
	track-default-gateway	Global	Disable

Devices: All Cisco vEdge

Template:	Basic Information / NTP
Template Name:	vEdge_NTP_Template
Description:	vEdge NTP Template

Table 9. vEdge NTP feature template settings

Section	Parameter	Туре	Variable/Value
Server	Hostname/IP Address	Global	time.nist.gov

#### vEdge AAA feature template

Devices:	All Cisco vEdge
Template:	Basic Information / AAA
Template Name:	vEdge_AAA_Template
Description:	vEdge AAA Template

#### Table 10. vEdge AAA feature template settings

Section	Parameter	Туре	Variable/Value
Authentication	Authentication Order	Drop-down	local
Local	Password	Global	<your admin="" password=""></your>

#### vEdge BFD feature template

Devices:	vEdge Cloud
Template:	Basic Information / BFD_Template
Template Name:	vEdge_Azure_Transit_BFD_Template
Description:	vEdge BFD Template for Azure Transit VNet vEdge Cloud Routers

Table 11. vEdge BFD feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	Poll Interval	Global	120000
Color (Biz Internet)	Color	Drop-down	Biz Internet
	Hello Interval (milliseconds)	Device Specific	biz_internet_bfd_hello_interval
	Path MTU	Global	Off

#### feature template

Devices:	All Cisco vEdge

Template: Basic Information / OMP

vEdge OMP

Template Name:	vEdge_0	DMP_	Template
----------------	---------	------	----------

Description: vEdge OMP Template

Table 12. vEdge OMP feature template settings

Section	Parameter	Туре	Variable/Value
Basic configuration	Number of Paths Advertised per Prefix	Global	16
	ECMP Limit	Global	16
Advertise	Connected	Global	Off
	Static	Global	Off

# vEdge Security feature template Devices: All Cisco vEdge

Devices.	All Olsco VLage
Template:	Basic Information / Security
Template Name:	vEdge_Security_Template
Description:	vEdge Security Template

Table 13. vEdge Security feature template settings

Section	Parameter	Туре	Variable/Value
Basic configuration	Replay window	Global / drop-down	4096

# vEdge VPN 0 feature template Devices: vEdge Cloud Template: VPN / VPN Template Name: vEdge\_Azure\_Transit\_VPN0\_Template Description: vEdge VPN0 Transport Template for Azure Transit VNet vEdge Cloud Routers

Table 14. vEdge VPN0 feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	VPN	Global	0
	Name	Global	Transport VPN

vEdge VPN 0 Interface Ethernet feature template Devices: vEdge Cloud Template: VPN / VPN Interface Ethernet

Template Name: vEdge\_Azure\_Transit\_VPN0\_Interface

Description: vEdge VPN 0 Transport Interface for Azure Transit VNet vEdge Cloud Routers

 Table 15.
 vEdge VPN0 Interface Ethernet feature template settings (Internet)

Section	Parameter	Туре	Variable/Value
Basic Configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex x
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio Button	Dynamic
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
	Allow Service>NTP	Global	On
Tunnel>Advanced Options>Encapsulation	IPsec Preference	Device Specific	vpn0_inet_tunnel_IPsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

vEdge VPN 512 feature template			
Devices:	vEdge Cloud		
Template:	VPN / VPN		
Template Name:	vEdge_Azure_Transit_VPN512_Template		
Description:	vEdge VPN 512 Out-of-Band Management for Azure Transit VNet vEdge Cloud Routers		

Table 16.vEdge VPN512 feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	VPN	Global	512
	Name	Global	Management VPN

#### vEdge VPN 512 Interface Ethernet feature template

Devices:	vEdge Cloud
Template:	VPN / VPN Interface Ethernet
Template Name:	vEdge_Azure_Transit_VPN512_Interface
Description:	vEdge VPN 512 Management Interface for Azure Transit vEdge Cloud Routers

Table 17. vEdge VPN512 Interface Ethernet feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgmt_int
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio Button	Dynamic

#### vEdge VPN 1 feature template

Devices:	vEdge Cloud
Template:	VPN / VPN
Template Name:	vEdge_Azure_Transit_VPN1_Template
Description:	vEdge VPN1 Service Template for Azure Transit VNet vEdge Cloud Routers

Table 18. vEdge VPN1 feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	VPN	Global	1
	Name	Global	Service VPN 1
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP (IPv4)	Global	On
	Connected (IPv4)	Global	On

BGP routes are advertised within OMP for service VPN 1. Connected routes are also advertised within OMP so that the IP addresses of the Loopback0 interfaces, which are part of VPN 1, are visible across the network.

#### vEdge VPN 1 Interface Ethernet Loopback0

Devices:	All Cisco vEdge
Template:	VPN / VPN Interface Ethernet
Template Name:	vEdge_VPN1_Lo0
Description:	vEdge Service VPN 1 Interface Loopback 0

Table 19.	vEdge VPN 1	Interface Ether	net Loopback0	feature t	template	settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	loopback0
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn1_lo0_int_ip_addr maskbits

vEdge VPN 2 featur	e template
Devices:	vEdge Cloud
Template:	VPN / VPN
Template Name:	vEdge_Azure_Transit_VPN2_Template
Description:	vEdge VPN2 Service Template for Azure Transit VNet vEdge Cloud Routers
Table 20	VDNO facture toreslate actions

#### Table 20. VPN2 feature template settings

Section	Parameter	Туре	Variable/Value
Basic Configuration	VPN	Global	2
	Name	Global	Service VPN 2
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP (IPv4)	Global	On

BGP routes are advertised within OMP for service VPN 2.

# **Transit VNet Device Template**

## Azure Transit VNet vEdge Device Template

The following table summarizes the device template for the Cisco vEdge Cloud routers deployed within the Azure transit VNet.

Device Model:	vEdge Cloud
Template Name:	onRamp_Transit_WAN_Edge_Template
Description:	vEdge Template for Cloud onRamp for IaaS Routers in a Transit VNet

Table 21. Transit VNet device template: (	Onramp_Transit_WAN_edge_Template
---	----------------------------------

Template Type	Template Sub-Type	Template Name
System		vEdge_System_Template
	NTP	vEdge_NTP_Template

	AAA	vEdge_AAA_Template
BFD		vEdge_Azure_Transit_BFD_Template
OMP		vEdge_OMP_Template
Security		vEdge_Security_Template
VPN0		vEdge_Azure_Transit_VPN0_Template
	VPN Interface	vEdge_Azure_Transit_VPN0_Interface
VPN512		vEdge_Azure_Transit_VPN512_Template
	VPN Interface	vEdge_Azure_Transit_VPN512_Interface
VPN1		vEdge_Azure_Transit_VPN1_Template
	VPN Interface	vEdge_VPN1_Lo0
VPN2		vEdge_Azure_Transit_VPN2_Template

# Example Branch Configuration

The following section lists out an example transit VNet configuration.

#### onRamp\_vEdge-Cloud1

```
system

host-name onRamp_vEdge-Cloud1

gps-location latitude 37.3541

gps-location longitude -121.9552

device-groups Azure

system-ip 10.1.0.136
```

```
115001
 site-id
 port-offset
                         1
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name
                        "ENB-Solutions - 21615"
                       "ENB-Solutions - 21615"
 organization-name
 no track-default-gateway
 clock timezone America/Los Angeles
 vbond 52.156.128.118
 aaa
 auth-order local radius tacacs
 usergroup basic
  task system read write
  task interface read write
  !
  usergroup netadmin
  !
 usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
  !
 user admin
  password $6$V8EKzg==$ulijOEP9FwPzfA3kwsTW6nRb9xxjDH38mp.ePVxVz17tNtLdJQdW58b9K
3eVQX7CIma3JD042IpjA5aWLWulv0
  !
 !
logging
 disk
  enable
 !
 !
ntp
 server time.nist.gov
 version 4
 exit
 !
1
bfd color biz-internet
hello-interval 10000
multiplier
              3
!
bfd app-route poll-interval 120000
omp
no shutdown
```

```
send-path-limit 16
             16
ecmp-limit
graceful-restart
1
security
IPsec
 replay-window
                     4096
 authentication-type shal-hmac ah-shal-hmac
 !
!
vpn 0
name "Transport VPN"
interface ge0/0
 description
                     "Internet Interface"
 ip dhcp-client
  tunnel-interface
  encapsulation IPsec
  color biz-internet
  allow-service all
  allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  !
  clear-dont-fragment
  tcp-mss-adjust
                   1350
 no shutdown
 bandwidth-upstream 1000000
 bandwidth-downstream 1000000
 L
 ip route 0.0.0.0/0 10.0.1.33
ip route 52.156.128.118/32 10.0.1.33
ip route 52.233.80.195/32 10.0.1.33
ip route 52.233.90.51/32 10.0.1.33
ip route 173.36.197.111/32 10.0.1.33
ip route 173.36.197.112/32 10.0.1.33
!
vpn 1
name "Service VPN 1"
ecmp-hash-key layer4
router
```

```
bgp 64600
  timers
   holdtime 30
   1
  address-family ipv4-unicast
   network 0.0.0/0
   !
  neighbor 10.25.2.132
   no shutdown
   remote-as 65534
   update-source loopback1000001
   ebgp-multihop 2
   !
  neighbor 10.25.2.133
   no shutdown
   remote-as 65534
   update-source loopback1000001
   ebgp-multihop 2
   !
  !
 !
interface IPsec21
 ip address 192.168.0.1/30
  tunnel-source 10.0.1.36
  tunnel-destination 52.250.11.112
 ike
  version
              2
  rekey
              28800
  cipher-suite aes128-cbc-shal
  group
               2
  authentication-type
   pre-shared-key
    pre-shared-secret "$8$UalW0IM0z/ulqbs6Zrt2IHEdSd+tE2CElhfW4UItGlou0+k9TJj4nb
wb/Q4pmuybHVwbDc27\nFBH6cswinsQowQ=="
   !
   !
  !
 IPsec
                          3600
  rekey
  replay-window
                          512
  cipher-suite
                          aes256-cbc-shal
  perfect-forward-secrecy none
  !
 no shutdown
 1
 interface IPsec22
  ip address 192.168.0.5/30
```

```
tunnel-source 10.0.1.36
  tunnel-destination 52.250.11.161
  ike
  version
              2
  rekey
              28800
  cipher-suite aes128-cbc-shal
  group
               2
  authentication-type
   pre-shared-key
    pre-shared-secret "$8$Vj6+q7rWu16lNdWdRCnU/xPPQ0QvSume53ZT5Lvz0th6H8XbhW9TlP
TGBZU/7p4TVbk3+C93\n9WAphM6CxvVOcQ=="
   !
   !
  !
 IPsec
                          3600
  rekey
  replay-window
                          512
  cipher-suite
                         aes256-cbc-shal
  perfect-forward-secrecy none
  !
 no shutdown
 !
interface loopback0
 ip address 10.1.0.136/32
 no shutdown
 !
interface loopback1000001
 ip address 2.2.2.3/32
 no shutdown
 !
ip route 0.0.0.0/0 null0
ip route 10.25.2.132/32 192.168.0.2
ip route 10.25.2.133/32 192.168.0.6
omp
 advertise bgp
 advertise connected
!
!
vpn 2
name "Service VPN 2"
ecmp-hash-key layer4
router
 bgp 64600
  timers
   holdtime 30
  !
```

```
address-family ipv4-unicast
```

```
network 0.0.0.0/0
   I.
  neighbor 10.26.2.132
   no shutdown
   remote-as 65534
   update-source loopback1000002
   ebgp-multihop 2
   !
  neighbor 10.26.2.133
   no shutdown
   remote-as 65534
   update-source loopback1000002
   ebgp-multihop 2
  !
  !
 T.
 interface IPsec19
 ip address 192.168.0.17/30
  tunnel-source 10.0.1.36
  tunnel-destination 51.143.15.221
  ike
  version
              2
  rekey
             28800
  cipher-suite aes128-cbc-shal
               2
  group
  authentication-type
   pre-shared-key
    pre-shared-secret "$8$ale0MalRZ4mz1vGsuW/j5FJCvWxoOKjlMuFsW48sXMgTRWGLyxZd/0
YBQTukcJRi4lYiF1Rh\nbA1iCUFJmdeEGg=="
   !
  !
  !
 IPsec
                         3600
  rekey
  replay-window
                         512
                        aes256-cbc-shal
  cipher-suite
  perfect-forward-secrecy none
  !
 no shutdown
 1
interface IPsec20
 ip address 192.168.0.21/30
  tunnel-source 10.0.1.36
  tunnel-destination 52.250.119.9
 ike
  version
              2
  rekey
             28800
```

```
cipher-suite aes128-cbc-shal
  group
                2
  authentication-type
   pre-shared-key
    pre-shared-secret "$8$ttuF8nHUq2Ne3UDTTBaUvsuAONJTmIEr+WcIYprYBkrBMq/bsFKwi0
L7fZnUfinHFReHZaeN\nX9s8iavTJyr9zg=="
    !
   !
  !
 IPsec
  rekey
                         3600
  replay-window
                         512
  cipher-suite
                          aes256-cbc-shal
  perfect-forward-secrecy none
  !
  no shutdown
 !
interface loopback1000002
 ip address 1.1.1.4/32
 no shutdown
 1
ip route 0.0.0.0/0 null0
ip route 10.26.2.132/32 192.168.0.18
ip route 10.26.2.133/32 192.168.0.22
omp
 advertise bgp
 advertise connected
!
!
vpn 512
name "Management VPN"
interface eth0
 description "Management Interface"
 ip dhcp-client
 no shutdown
 !
!
onRamp vEdge-Cloud2
system
host-name
                        onRamp vEdge-Cloud2
gps-location latitude 37.3541
gps-location longitude -121.9552
device-groups
                       Azure
system-ip
                       10.1.0.137
                        115001
site-id
```

```
1
port-offset
admin-tech-on-failure
no route-consistency-check
sp-organization-name
                         "ENB-Solutions - 21615"
                     "ENB-Solutions - 21615"
organization-name
no track-default-gateway
clock timezone America/Los_Angeles
vbond 52.156.128.118
aaa
 auth-order local radius tacacs
 usergroup basic
  task system read write
  task interface read write
  !
  usergroup netadmin
  !
 usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
  !
 user admin
  password
$6$V8EKzg==$ulij0EP9FwPzfA3kwsTW6nRb9xxjDH38mp.ePVxVz17tNtLdJQdW58b9K3eVQX7CIma3JD042Ip
jA5aWLWulv0
  !
 !
logging
 disk
  enable
  !
 !
ntp
 server time.nist.gov
  version 4
 exit
!
L
bfd color biz-internet
hello-interval 10000
no pmtu-discovery
!
bfd app-route poll-interval 120000
omp
no shutdown
send-path-limit 16
```

```
ecmp-limit
                16
graceful-restart
L
security
IPsec
 replay-window
                      4096
 authentication-type shal-hmac ah-shal-hmac
 !
I.
vpn 0
name "Transport VPN"
interface ge0/0
 description
                       "Internet Interface"
 ip dhcp-client
  tunnel-interface
  encapsulation IPsec
  color biz-internet
  allow-service all
  allow-service bqp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  !
  clear-dont-fragment
  tcp-mss-adjust
                       1350
  no shutdown
 bandwidth-upstream
                      1000000
 bandwidth-downstream 1000000
 !
 ip route 0.0.0.0/0 10.0.1.33
 ip route 52.156.128.118/32 10.0.1.33
ip route 52.233.80.195/32 10.0.1.33
ip route 52.233.90.51/32 10.0.1.33
ip route 173.36.197.111/32 10.0.1.33
ip route 173.36.197.112/32 10.0.1.33
!
vpn 1
name "Service VPN 1"
ecmp-hash-key layer4
router
```

```
bgp 64600
  timers
   holdtime 30
   1
  address-family ipv4-unicast
   network 0.0.0/0
  1
  neighbor 10.25.2.132
   no shutdown
   remote-as 65534
   update-source loopback1000001
   ebgp-multihop 2
   !
  neighbor 10.25.2.133
   no shutdown
   remote-as 65534
   update-source loopback1000001
   ebgp-multihop 2
   !
 !
 !
interface IPsec13
 ip address 192.168.0.9/30
 tunnel-source 10.0.1.37
 tunnel-destination 20.191.64.244
 ike
  version
              2
  rekey
              28800
  cipher-suite aes128-cbc-shal
  group
               2
  authentication-type
   pre-shared-key
    pre-shared-secret
"$8$kzM/CIMpHYv0z8t51pNILnUDUNUUUqrKzra3PbO1sGUrIm+1wmaijpxknx+G7lsLsfx1X9pW\nNrYhMlhRM
z4D2w=="
   !
  !
 !
 IPsec
                          3600
  rekey
  replay-window
                         512
  cipher-suite
                         aes256-cbc-shal
  perfect-forward-secrecy none
 !
 no shutdown
 !
interface IPsec14
 ip address 192.168.0.13/30
```

```
tunnel-source 10.0.1.37
  tunnel-destination 52.158.247.205
  ike
  version
               2
  rekey
               28800
  cipher-suite aes128-cbc-shal
  group
                2
  authentication-type
   pre-shared-key
    pre-shared-secret
"$8$jhSJlxN2vlwPwkaGoLXmkMnO1CuxwJLd1XqpBPvooaKtA9jUOJ2XUglZq/uOrFPlFU/fWKae\nmGZCE53dp
N58Yg=="
   !
   !
  !
 IPsec
  rekey
                           3600
                          512
  replay-window
  cipher-suite
                          aes256-cbc-shal
  perfect-forward-secrecy none
  !
 no shutdown
 !
 interface loopback0
 ip address 10.1.0.137/32
 no shutdown
 1
 interface loopback1000001
 ip address 1.1.1.1/32
 no shutdown
 !
ip route 0.0.0.0/0 null0
ip route 10.25.2.132/32 192.168.0.10
ip route 10.25.2.133/32 192.168.0.14
omp
 advertise bgp
 advertise connected
 !
!
vpn 2
name "Service VPN 2"
ecmp-hash-key layer4
router
 bgp 64600
  timers
   holdtime 30
   !
  address-family ipv4-unicast
```

```
network 0.0.0.0/0
   I.
  neighbor 10.26.2.132
   no shutdown
   remote-as 65534
   update-source loopback1000002
   ebgp-multihop 2
   !
  neighbor 10.26.2.133
   no shutdown
   remote-as 65534
   update-source loopback1000002
   ebgp-multihop 2
   !
 !
 T.
interface IPsec15
 ip address 192.168.0.25/30
 tunnel-source 10.0.1.37
 tunnel-destination 52.175.251.17
 ike
  version
               2
  rekey
              28800
  cipher-suite aes128-cbc-shal
               2
  group
  authentication-type
   pre-shared-key
    pre-shared-secret
"$8$j8wRp13y9AdVBkQsJH0L5SOO/+b9v00IqWAp/Bdy1zQ2ybY1DP10cyLptjKzv9DYg0FmEq01\nuezJ24xNE
lNe/0=="
   !
  !
 !
 IPsec
                          3600
  rekey
  replay-window
                          512
  cipher-suite
                          aes256-cbc-shal
  perfect-forward-secrecy none
 1
 no shutdown
 !
interface IPsec16
 ip address 192.168.0.29/30
 tunnel-source 10.0.1.37
 tunnel-destination 52.175.251.108
 ike
  version
              2
  rekey
               28800
```

```
cipher-suite aes128-cbc-shal
  group
                2
  authentication-type
   pre-shared-key
    pre-shared-secret
"$8$elffP+KjzYpn3j0G/Ckg8JhPKDcbBUclPpJNJsnc4z4G8ztgEB/Q9PhsK+TnOvU8CjDmcoz/\nsuXo7oXwS
6jaeA=="
    !
   !
  !
  IPsec
  rekey
                          3600
                         512
  replay-window
  cipher-suite
                          aes256-cbc-shal
  perfect-forward-secrecy none
  !
 no shutdown
 !
 interface loopback1000002
 ip address 1.1.1.3/32
 no shutdown
 !
ip route 0.0.0.0/0 null0
 ip route 10.26.2.132/32 192.168.0.26
ip route 10.26.2.133/32 192.168.0.30
omp
 advertise bgp
 advertise connected
 !
!
vpn 512
name "Management VPN"
interface eth0
 description "Management Interface"
 ip dhcp-client
 no shutdown
 !
!
```

# Appendix D: Glossary

- VPN Virtual Private Network
- NAT Network Address Translation
- LAN Local Area Network
- WAN Wide Area Network

- DNS Domain Name Server
- VNET Virtual Network
- VPN Virtual Private Network
- GW Gateway
- NSG Network Security Group
- VM Virtual Machine
- LNG Local Network Gateway

# Feedback

For comments and suggestions about this guide and related guides, join the discussion on <u>Cisco Community</u> at <u>https://cs.co/en-cvds</u>.