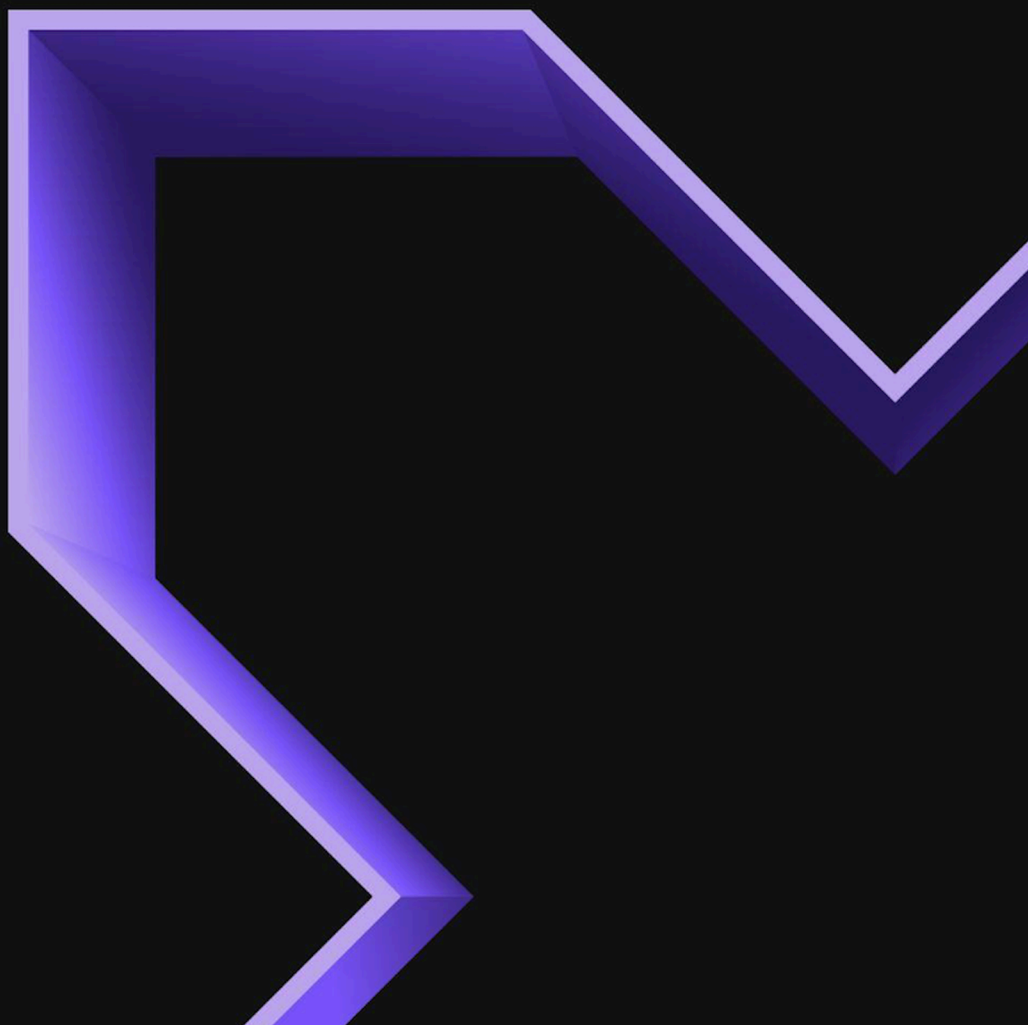
Flow Virtual Networking Guide

Flow Virtual Networking pc.2024.1

May 16, 2024



NUTANIX

Contents

PURPOSE

This *Flow Virtual Networking* Guide describes how to enable and deploy Nutanix Flow Virtual Networking on Prism Central.

RELATED DOCUMENTATION

Links to Nutanix Support Portal software and documentation.

The Nutanix Support Portal provides software download pages, documentation, compatibility, and other information.

Documentation	Description
Release Notes | Flow Virtual Networking	Flow Virtual Networking Release Notes
Port And Protocols	Port Reference: See this page for details of ports that must be open in the firewalls to enable Flow Virtual Networking to function.
Nutanix Security Guide	Prism Element and Prism Central security, cluster hardening, and authentication.
Flow Network Security Next Gen	Flow Network Security Next-Gen is the next-generation Nutanix microsegmentation solution with an enhanced policy model, advance policy operation, and enterprise readiness features. FNG
AOS guides and release notes	Covers AOS Administration, Hyper-V Administration for Acropolis, Command Reference, Powershell Cmdlets Reference, AOS Family Release Notes, and AOS release-specific Release Notes
AHV guides and release notes	Administration and release information about AHV.
Prism Central and Web Console guides and release notes	Administration and release information about Prism Central and Prism Element.

FLOW VIRTUAL NETWORKING OVERVIEW

Flow Virtual Networking, powered by the network controller, drives network virtualization to offer a seamless network experience with enhanced security. It is enabled by default.

It is a software-defined networking solution that provides multi-tenant isolation, self-service provisioning, and IP address preservation using VPCs, subnets, and other virtual components that are separate from the physical network, for the AHV clusters. It integrates tools to deploy networking features like Virtual LANs, Virtual Private Cloud (VPC), Virtual Private Network (VPN), Layer 2 Virtual Network Extension using VPN or Virtual Tunnel End Point (VTEP), Border Gateway Protocol sessions to support flexible app-driven networking that focuses on VMs and applications.

Flow Virtual Networking deploys the following components to manage software-defined network virtualization:

Network Controller

The network controller is defined as networking component of Prism Central that manages and controls configuration, monitoring and optimization of network resources for Flow Virtual Networking VPCs and VLAN subnets. It provides programmability, automation, and centralized control for configuring and managing network flows.

The network controller is necessary to use centralized VLAN management, Flow Virtual Networking and .Flow Network Security Next Generation.

Network Gateway

The network gateway appliance is available along with the network controller when you install or upgrade Prism Central. Network gateway VMs are used to create VPN, VTEP, or BGP gateways to connect subnets using VPN connections, Layer 2 subnet extensions over VPN or VTEP, or BGP sessions.

The network controller delivers the following:

- **Centralized Agile Management**

  Prism Central helps you enable the network controller that provides the application-driven network virtualization feature called Flow Virtual Networking as well as centralized VLAN management. Flow Virtual Networking leverages the network controller and any necessary network gateway appliances to help you manage network configuration changes with speed and agility. It delivers a centralized network management solution with multi-tenant networking, self-service network provisioning, and a multi-cluster network control plane.

  Prism Central provides the centralized network management plane that helps you manage the control plane provided by the network controller. The network controller as the control plane, deploys network virtualization. The Open vSwitch (OVS) infrastructure on the AHV hosts provide the data plane. For more information about the architecture of Flow Virtual Networking, see Flow Virtual Networking Architecture on page 9.

- **Programmability with Context and Visibility**

  Flow Virtual Networking helps you directly program network features and configure network resources quickly and easily through automated services on Prism Central. The network controller allows you to design and configure self-service networks using the Prism Central user interface and REST APIs. Flow Virtual Networking enables you to manage networks and network lifecycles easily, to accommodate the increasing demand for network services, without impacting the overall network.

  You can view the networks, connection endpoints, and the traffic parameters. This helps you easily redirect the traffic to improve service delivery, reduce service disruptions for your customers and increase network responsiveness, thus helping you deliver a seamless customer experience.

- **Secure Multi-tenancy Solution**

  The Flow Virtual Networking allows per-tenant isolation using VPC-based network segmentation and namespace isolation. These isolated virtual networks provide security by default.

  You can apply policy based routing using the network controller to improve the security of the networks by redirecting traffic through security VMs within the VPC. Flow Virtual Networking, with the network controller and network gateway, allows you to manage cloud networking by abstracting and unifying cloud resources effectively. The network controller uses Virtual Private Cloud (VPC) networks that are abstracts of the underlying network to unify multi-cluster based resources (managed by the Prism Central) into isolated network spaces (VPCs). Secure egress of traffic to the underlying VLAN network is managed using SNAT, Floating IP addresses, or routing with support for static and BGP advertisement.

- **Interoperable Secure Connectivity Solution**

  With Flow Virtual Networking you can use VPN, VTEP or BGP gateway-based configurations for multiple sites, with automated network gateway appliance upgrades. You can also extend subnets across sites using Layer 2 virtual subnet extensions (VPN or VTEP based) for connectivity without using physical gateways, in a vendor-neutral environment.

- **NAT-based Secure Egress**

  The network controller allows you to configure NAT based traffic egress routes to external networks, with IP address retention and policy-based routing. You can also use a no-NAT, or the routed, option for external networks. For more information about NAT, see Essential Concepts on page 12.

- **Enhanced Networking for Disaster Recovery**

  The network controller supports Nutanix Disaster Recovery solutions.

  > **Note:** Disaster Recovery of Prism Central (PC DR) supports Flow Virtual Networking. For more information, see Prism Central Disaster Recovery documentation.

Deployment Workflow

On an x-Large Prism Central deployment, Prism Central enables Flow Virtual Networking and the network controller when you upgrade Prism Central to pc.2023.3 or later versions. On Small or Large Prism Central deployments, manually enable the network controller. For steps to enable the network controller, see Enabling the Network Controller on page 26.

When Flow Virtual Networking is enabled, the network controller and the network gateway appliance are installed. The network controller is a collection of containerized services that run directly in the Prism Central VM(s). The network controller orchestrates all the virtual networking operations.

- You can deploy Flow Virtual Networking in a dark site (a site that does not have Internet access) environment. For more information, see Deploying the Network Controller at a Dark Site on page 35.
- You can upgrade the Flow Virtual Networking network controller. Nutanix releases an upgrade for the Flow Virtual Networking network controller with AOS and Prism Central releases. For more information, see Upgrading the Network Controller on page 34.
- Flow Virtual Networking allows you to create and manage virtual private clouds (VPCs) and overlay subnets to leverage the underlying physical networks that connect clusters and datacenters. For more information, see Virtual Private Cloud on page 82.
- You can upgrade the network gateway version. The network gateway is used to create VPN, VTEP, or BGP gateways to connect subnets using VPN connections, Layer 2 subnet extensions over VPN or VTEP, or over BGP sessions.

Flow Virtual Networking Architecture

Flow Virtual Networking lets you create integrated software-defined networks and virtual private cloud capabilities and provides software-defined networking with multi-tenant isolation, self-service provisioning, and IP address preservation. The Flow Virtual Networking architecture uses a three-plane approach to simplify network virtualization.

Flow Virtual Networking provides a software-defined networking (SDN) solution with the three-plane architecture that SDN is built with. Flow Virtual Networking as SDN follows the following three-plane architecture:

- **The Management Plane**

  The Management Plane provides the interface between you and the configuration and management interfaces. Primarily, it allows you to configure, manage, and monitor the virtual network resources such as IP addresses, subnets, routes and protocols.

  Prism Central provides the Management Plane for Flow Virtual Networking. The **Network & Security** entity provides the Flow Virtual Networking components like **Subnets**, **Virtual Private Clouds**, **Floating IPs**, and **Connectivity** (which encompasses network gateways, connections like VPN or VTEP or BGP sessions.) Prism Central also allows you to control access to these virtual networking components on Prism Central using Role-based access control (RBAC).

- **The Control Plane**:

  This plane is defined by the SDN controller. This plane is essentially decoupled from the data plane. In other words, the appliance that houses the SDN controller is a different and separate entity from the one that houses the data transport network or the Data Plane.

  In Flow Virtual Networking, the Control Plane is defined by the network controller. Prism Central enables the Microservices Infrastructure when you deploy Prism Central. The network controller is enabled on the Prism Central as containerized services using Microservices Infrastructure.

  The network controller that allows you to create a virtual overlay network as an abstraction of the complex underlay network infrastructure. The network controller manages the network services and direct packet traffic throughout the network. The network controller, with the network gateway appliance, helps you manage the networks, connections (such as VPN and VTEP connections, and BGP sessions) and devices with ease.

  In x-Large Prism Central, the network controller is automatically enabled when Prism Central is deployed. In Small and Large Prism Central deployments, you must enable the network controller manually. See Enabling the Network Controller on page 26.

- **The Data Plane**

  The Open vSwitch (OVS) deploys a collection of bridges within the AHV hosts. The traffic flows through these bridges between the AHV hosts. To configure and manage these bridges, AHV allows you to deploy virtual switches. AHV deploys a default virtual switch vs0 during the installation process. The default virtual switch manages the bridges br0 on all the AHV hosts in the cluster. For more information about the virtual switches, see About Virtual Switch.

  This OVS infrastructure on the AHV hosts provides the Data Plane for Flow Virtual Networking. See About Open vSwitch.

This architecture provides a foundation for Flow Virtual Networking as depicted in the following chart.

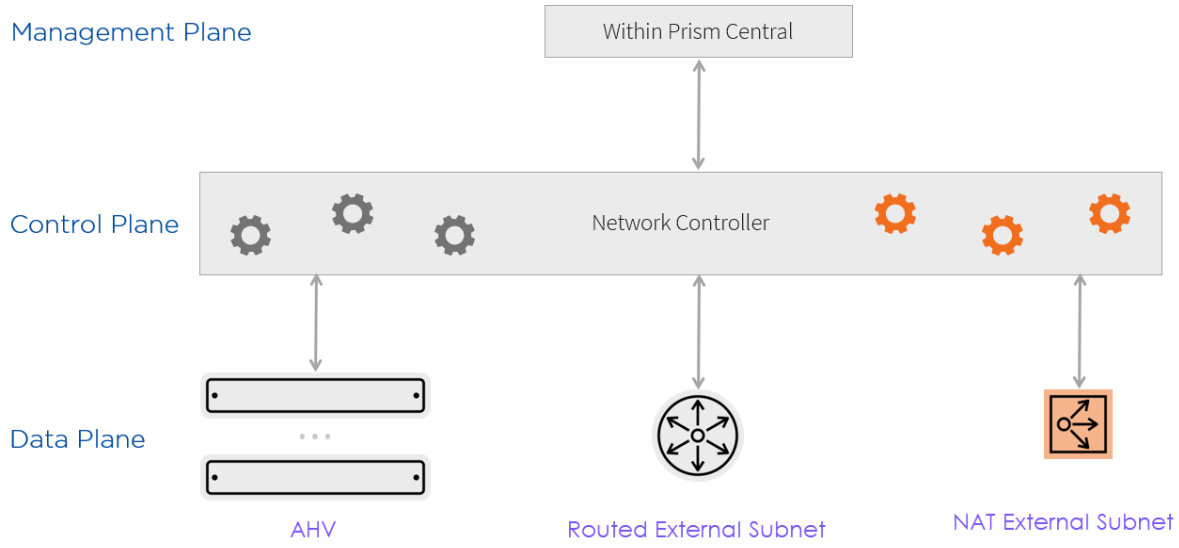


Figure 1: Flow Virtual Networking Architecture

Implementation Constructs of Flow Virtual Networking

Flow Virtual Networking provides the following virtual constructs to provide a complete networking solution:

- Virtual Private Clouds or VPCs:
- Subnets as VLAN or Overlay Subnets
- Routes
- Policies for routing.
- External Networks such as:
  - NAT based external networks
  - Routed (or NoNAT) external networks
  - Multiple networks or a set of networks with both NAT and NoNAT external networks
- Network gateways such as:
  - Layer 3 Virtual Private Network or VPN
  - Layer 2 Network Extensions with VxLAN or Virtual Tunnel End Point (VTEP)
  - Border Gateway Protocol based gateways and sessions.

For more information about these constructs, see Essential Concepts on page 12.

Flow Virtual Networking Operation

Each VPC, as an isolated network namespace with a virtual router instance, connects all of the subnets inside the VPC. The VPCs are created in Prism Central that manages all the nodes and clusters that the VPCs span across.

Each VPC can have one or more subnets and all the subnets are connected to the same VPC virtual router. A VPC uses Geneve encapsulation to tunnel traffic between the AHV hosts. When two VMs in a VPC on two different hosts send traffic to each other, the packets are encapsulated in GENEVE on the first host, sent to the other host where the packets are decapsulated, and sent to the destination VM.

When you select a NIC for a VM, place that NIC in an overlay subnet, or a VLAN Basic Subnet (VLAN on AHV networking stack). When you choose an overlay subnet, you are also choosing the VPC that the subnet is a part of. Each VM can be placed inside only a single VPC. You can't connect a VM to both a VPC and a VLAN Basic Network at the same time, or to two different VPCs at the same time.

Every VPC contains a single virtual router and different types of routes like External networks, direct connections, remote connections. The virtual router acts as a control point for traffic inside a VPC. An External Network is the primary way traffic enters and exits a VPC. External Networks are created in Prism Central and exist on only a single Prism Element cluster. This network defines the VLAN, the default gateway, the IP address pool, and the NAT type for all the VPCs using it. One External Network can be used by many VPCs.

Direct and remote connections can be established using network gateways in one-to-one (VPN, VTEP or BGP) or one-to-many (VTEP) connections. All connections require network gateways. For example, a VPN connection requires a local gateway and a remote gateway. While the VPN and VTEP gateways are a part of the data plane, BGP gateways are part of the control plane.

You can apply simple stateless policies here, and the traffic that flows through the router is evaluated by the policies. Policies do not apply to traffic from one VM to another VM inside the same subnet. Inside a VPC, policies are evaluated in priority order from highest (1,000) to lowest (10). Once traffic is matched a policy can take one of the following actions:

- Permit
- Deny
- Reroute including Redirect traffic to another /32 IPv4 address in another subnet.

Stateless policies require separate rules defined in both the forward and reverse direction if a Permit rule is overriding a Drop rule. Otherwise, return traffic would be denied by the Drop rule. Use similar priorities to group these matching forward and reverse entries.

Thus, Flow Virtual Networking allows you to create completely isolated virtual networks that are separated from the physical network. These isolated virtual networks provide security by default.

Deployment Scale

Flow Virtual Networking supports the scale provided in the Nutanix Configuration Maximums page.

> **Note:** For information about the algorithms supported by Flow Virtual Networking (network controller and network gateway) APIs, see Nutanix Networking Versioned APIs (4.0.1-alpha-1).

Supported Third Party Appliances

Nutanix has validated that the following the network gateway appliances work in Flow Virtual Networking VPCs:

- AWS
- CheckPoint
- Cisco ASA
- Fortinet
- Juniper SRX
- PaloAlto
- SonicWall NSv
- VyOS

Essential Concepts

Network Controller

The Network Controller is defined as networking component of Prism Central that manages and controls configuration, monitoring and optimization of network resources for Flow Virtual Networking. It provides programmability, automation, and centralized control for configuring and managing network flows.

Network Controller is necessary to use centralized VLAN management, Flow Virtual Networking and Flow Network Security Next-Gen.

VPC

A Virtual Private Cloud (VPC) is an independent and isolated IP address space that functions as a logically isolated virtual network. A VPC could be made up of one or more subnets that are connected through a logical or virtual router. VPCs allow you to manage the isolated and secure virtual network with enhanced automation and scaling. The isolation is done using network namespace techniques like IP-based subnets or VLAN based networking.

The IP addresses within a VPC must be unique. However, IP addresses may overlap across VPCs, in other words, the IP addresses inside of one VPC to overlap with any other VPC, or even with the physical network. As VPCs are provisioned on top of another IP-based infrastructure (connecting AHV nodes), they are often referred to as the overlay networks. Tenants may spin up VMs and connect them to one or more subnets within a VPC. Virtual Private Cloud (VPC) is a virtualized network of resources that are specifically isolated from the rest of the resource pool. A VPC can expand to include any cluster managed by the same Prism Central. A VPC might exist within a single AHV cluster, or within clusters in the same availability zone.

The default VPC type that is referred to as *VPC* in this documentation is the one you create to isolate selected subnets of connected VMs. This VPC is also called as user VPC or guest VPC, but generally referred to as VPC.

The other VPC type that Flow Virtual Networking supports is *transit VPC*. See the *Transit VPC* section below for more information. You need a minimum Prism Central version of pc.2024.1 to deploy transit VPCs.

Shared VPC Connections

Shared VPC connections involve connecting VPCs such that you can route traffic between them using private IP addresses. The VPCs can, then, communicate as if they are in the same network. You can connect a VPC to another VPC either directly or through a transit VPC to achieve shared connections. For information about transit VPCs, see the *Transit VPC* section below.

VPC Subnets

You can use IP address-based subnets to network virtual machines within a VPC. A VPC may use multiple subnets. VPC subnets use private IP address ranges. IP addresses within a single VPC must be unique, in other words, IP addresses inside the same VPC cannot be repeated. However, IP addresses can overlap across multiple VPCs. The following figure shows two VPCs named Blue and Green. Each VPC has two subnets, 192.168.1.0/24 and 192.168.2.0/24, that are connected by a logical router. Each subnet has a VM with an IP address assigned. The subnets and VM IP addresses overlap between the two VPCs.

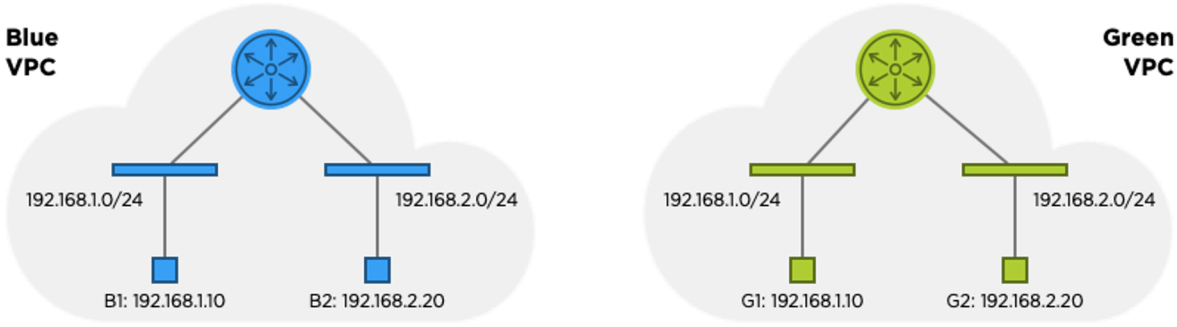


Figure 2: VPC Subnet

The communication between VMs in the same subnets or different subnets in the same VPC (also called East-West communication) is enabled using GEneric NEtwork Virtualization Encapsulation (GENEVE). If a Prism Central manages multiple clusters, then the VMs that belong to the same VPC could be deployed across different clusters. The virtual switch on the AHV nodes provide distributed virtual switching and distributed virtual routing for all VPCs.

The communication from a VM in a VPC to an endpoint outside the VPC (called external communication or North-South communication) is enabled by an external network connection. Such a connection may be secured using VPN. The following figure shows the logical connectivity of the VPCs to the external network, and subsequently to the Internet.

> **Note:** You must configure the default route (0.0.0.0/0) to the external subnet as the next hop for connectivity outside the cluster (north-south connectivity).

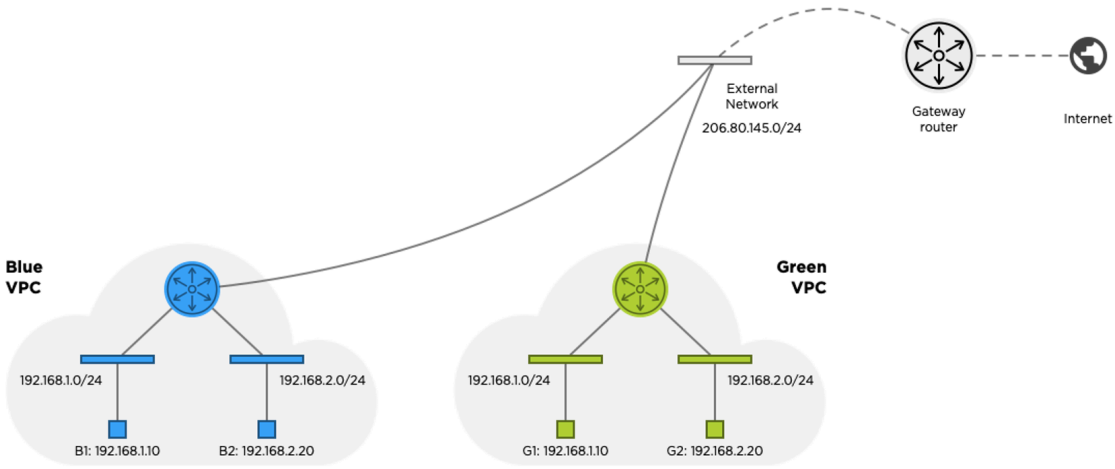


Figure 3: External Communication

Transit VPC

For external connectivity, connect a user VPC to a transit VPC or an Overlay External Subnet with external connectivity. You could use a maximum of one NAT and one No-NAT external network for a given VPC.

Transit VPC use a hub-and-spoke architecture. Transit VPCs are useful in the following cases.

- Transit VPCs simplify and scale routing configuration (for North-South traffic) for large number of VPCs by introducing a hub VPC in the path. This minimizes the need for dynamic routing advertisement to infrastructure routers or configuring infrastructure router statically.
- Transit VPCs enable you to route traffic between user VPCs using private IPv4 addresses (using Externally Routable Prefix or ERP routes),thus allowing user VPCs to access resources you have in one of your regular VPCs. An added advantage is that traffic does not need to be routed on the physical infrastructure.
- Transit VPCs enable hosting shared services among VPCs (by hosting these services on overlay subnets under a transit VPC).
- Transit VPCs allow a logical separation between provider (transit VPC) and tenant (user VPC) network in a multi-tiered model. Multi-tiered models allow for layers of access control where each tenant controls their own routing and security policies, whereas transit VPCs allow the administrators to control the routing and security policies in the layer above the tenant layer.
- Transit VPCs allow for routing and policy control over cross-tenant communication without touching the physical infrastructure.

Conditions applicable to transit VPCs:

- Use VLAN subnets with external connectivity for North-bound connections of a transit VPC.
- Use Overlay subnets with external connectivity (Overlay external subnet) for South-bound connections from a transit VPC to non-transit or user VPCs. Overlay subnets with external connectivity can only connect to transit VPCs
- Use the Overlay subnet without external connectivity to connect a transit VPC with entities such as VMs.
- Configure Externally Routable Prefixes (ERPs) on the VPCs to ensure that the transit VPC has a route to the Overlay subnets for the VPCs.
- When you connect a transit VPC to a VLAN backed No-NAT external network, deploy a Border Gateway Protocol (BGP) gateway to advertise the networks that connect through the transit VPC. Scale out the No-NAT gateways to provide maximum connectivity. For more information on scaling out No-NAT gateways, see *No-NAT Gateways* section in the following pages.
- Floating IP addresses supported for Recovery Plans in Disaster Recovery do not work if the floating IP addresses are configured for transit VPCs.

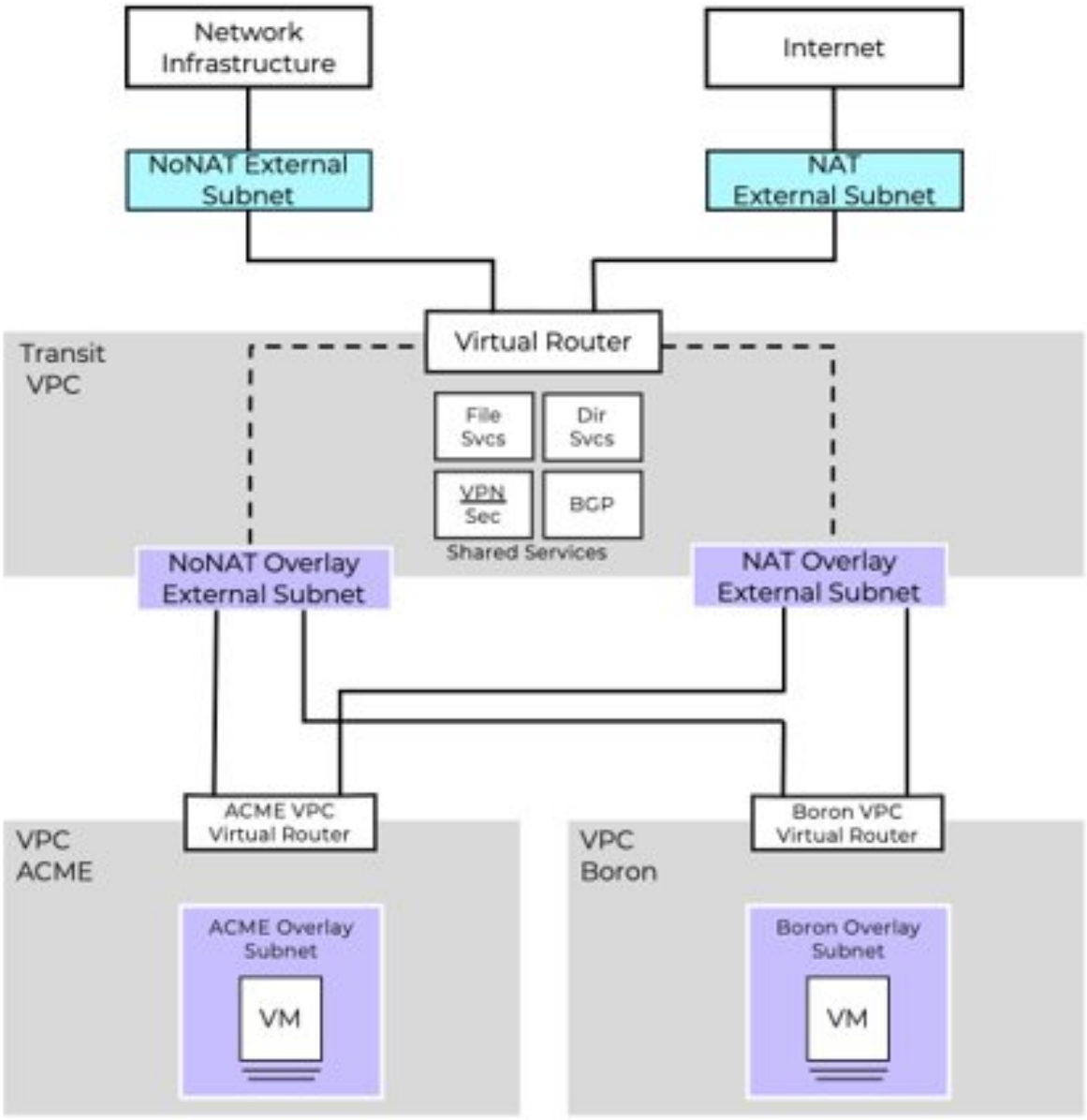


Figure 4: Transit VPC in a network

External Subnets

Subnets that provide external connectivity to a VPC are external subnets. External subnets may be subnets within the deployment but not included in a specific VPC. External subnets may also be subnets that connect to the endpoints outside the deployment such as another deployment or site.

External subnets can be deployed with NAT or without NAT. You can add a maximum of two external subnets - one external subnet with NAT and one external subnet without NAT to a VPC. Both external subnets cannot be of the same type. For example, you cannot add two external subnets, both with NAT.

You can deploy VLAN subnets (Network Controller based VLANs) or Overlay subnets as external subnets. However, an Overlay subnet deployed as an external subnet (Overlay external subnet) can be attached to only a transit VPC. You cannot attach an Overlay External subnet to a regular, non-transit VPC.

Primary and Secondary IP Addresses for VMs

See VM IP Address Management on page 83.

SNAT and Floating IP Address

SNAT and Floating IP addresses are used only when you use NAT for an external subnet.

In Source Network Address Translation (SNAT), the NAT router modifies the IP address of the sender in IP packets. SNAT is commonly used to enable hosts with private addresses to communicate with servers on the public Internet.

For VMs within the VPC to communicate with the rest of the deployment, the VPC must be associated with an external network. In such a case, the VPC is assigned a unique IP address, called the SNAT IP, from the subnet prefix of the external network. When the traffic from a VM needs to be transmitted outside the VPC, the source IP address of the VM, which is a private IP address, is translated to the SNAT IP address. The reverse translation from SNAT IP to private IP address occurs for the return traffic. Since the SNAT IP is shared by multiple VMs within a VPC, only the VMs within the VPC can initiate connections to endpoints outside the VPC. The NAT gateway allows the return traffic for these connections only. Endpoints outside the VPC cannot initiate connections to VMs within a VPC.

In addition to the SNAT IP address, you can also request a Floating IP address — an IP from the external subnet prefix that is assigned to a VM via the VPC that manages the network of the VM. Unless the floating IP address is assigned to the private IP address (primary or secondary IP address) of the VM, the floating IP address is not reachable. When the VM transmits packets outside the VPC, the private IP of the VM is modified to the Floating IP. The reverse translation occurs on the return traffic. As the VM uses the Floating IP address, an endpoint outside the VPC can also initiate a connection to the VM with the floating IP address.

The translation of the private IP addresses to Floating IP or SNAT IP address, and vice versa, is performed in the hypervisor virtual switch. Therefore, the VM is not aware of this translation. Floating IP translation may be performed on the hypervisor that hosts the VM to which the floating IP is assigned to. However, SNAT translation is typically performed in a centralized manner on a specific host.

Network Address Translation

Network Address Translation (NAT) provides a method to map the IP addresses of an internal or private subnet to a public IP address that can communicate with the internet or other subnets. It is a process for modifying the source or destination addresses in the headers of an IP packet when the packet is put in transit. In general, the sender and receiver applications are not aware that the IP packets are being manipulated.

For example, consider the following scenario:

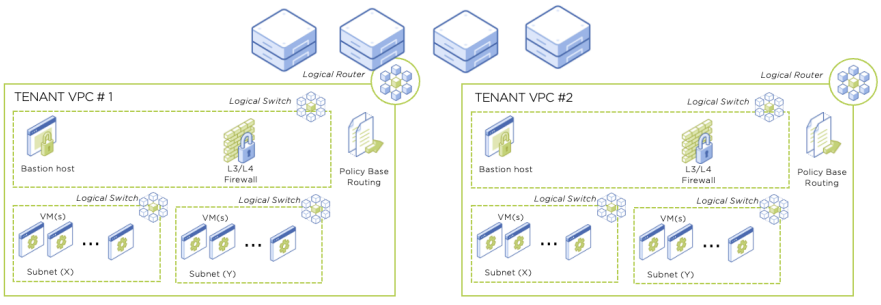


Figure 5: NAT

When VPC#1 and VPC #2 need access to a common segment of the overall organization's network, there would be conflicts with overlapping IP addresses in the common segment, VPC#1, and VPC#2

subnets. Using a NAT external subnet in this scenario eliminates the conflicts and connectivity issues. When the two VPCs (#1 and #2) communicate with each other as well, conflicting IP address would lead to connectivity issues. Especially while connecting to unknown subnets or the Internet, NAT provides security and masking.

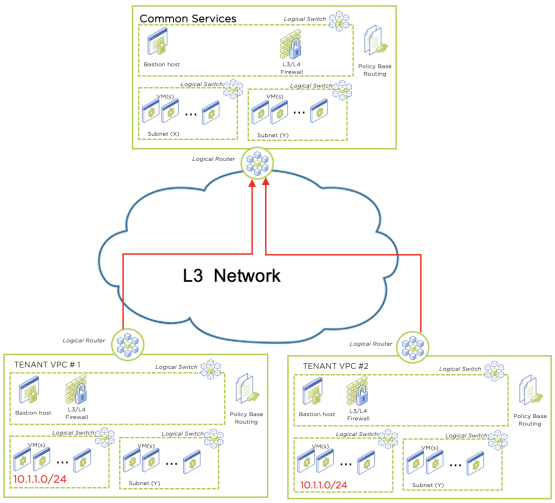


Figure 6: NAT Access to Common Segment

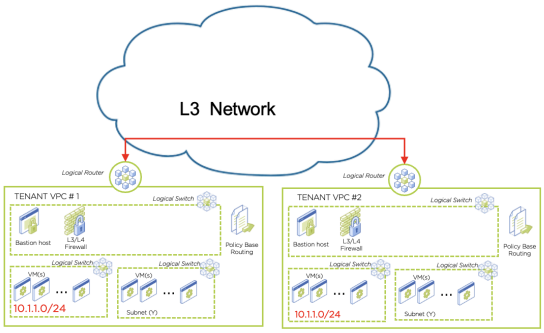


Figure 7: NAT Access between VPCs

NAT Gateways are used only when you use Network Address Translation (NAT) for an external subnet.

NAT Gateway

A NAT Gateway service provides the entities inside an internal network with connectivity to the Internet without exposing the internal network and its entities. It performs the process of Network Address Translation as a service.

A NAT Gateway service works as follows:

- A NAT Gateway service is deployed as an AHV host. You need an AHV host to implement a NAT Gateway service because NAT gateway services involve and require operations like load balancing and routing that are automatically performed by Flow Virtual Networking. One of the AHV hosts in a cluster (that also hosts the Prism Central AZ) is deployed as the NAT Gateway..

- A NAT Gateway service is connected to the internal network with an internal subnet IP address and to the external network with an externally-routable IP address.

  The externally-routable IP address is an IP address selected from IP address pool of the external subnet configured for the VPC.

No-NAT Gateway

Like the NAT Gateway service, the No-NAT gateway service also provide external connectivity. However, it does not perform Network Address Translation.

The No-NAT gateway service selects an AHV host or node from the Prism Element cluster to act as the gateway and route the external traffic. You can deploy scale-out gateway services with up to four AHV hosts acting as gateways, when you create a VPC with a VLAN subnet providing external connectivity. The external (North South) traffic for the VPC is distributed across the number of AHV hosts or nodes selected for the VPC.

See *External Connectivity* in the table in Creating Virtual Private Cloud on page 102.

The following considerations apply to No-NAT scale-out gateway services providing up to four No-NAT gateways:

- You can deploy a scale-out No-NAT gateway only if you attach a No-NAT VLAN external subnet (not an Overlay external subnet).
- The externally-routable IP address may be an IP address from a private IP address space or a private network (RFC1918) address.
- The No-NAT gateway IP address can be manually selected or chosen dynamically from the IP pool of the external subnet.

Static IP Address

A static IP address is a fixed IP address that is manually assigned to an interface in a network. Static IP addresses provide stable routes that do not have to be updated frequently in the routing table since the static routes generated using static IP addresses do not need to be updated.

Usually in a large IP-based network (a network that uses IP addresses), a Dynamic Host Configuration Protocol or DHCP server assigns IP addresses to interfaces of an entity (using DHCP client service on the entity). However, some entities may require a static IP address that can be reached (manual remote access or via VPN) quickly. A static IP address can be reached quickly because the IP address is fixed, assigned manually and is stored in the routing table for a long duration. For example, a printer in an internal network would need a static IP address so that it can be connected reliably. Static IP addresses can be used to generate static routes which remain unchanged in routing tables, thus providing stable long-term connectivity to the entity that has the static IP address assigned.

Virtual IP Address

Any IP address in a VPC subnet, that is assigned, manually or otherwise, to an entity like a VM may be termed as a virtual IP address.

Do not confuse this virtual IP address with the virtual IP addresses assigned to Prism Central or Prism Element cluster.

Static Route

Static routes are fixed routes that are created manually by the network administrator. Static routes are more suited for small networks or subnets. Irrespective of the size of a network, static routes may be required in a variety of cases. For example, in VPCs where you use virtual private networks (VPNs) or Virtual Tunnel End Point (VTEP) over VxLAN transport connections to manage secure connections, you could use static routes for specific connections such as site-to-site connections for disaster recovery. In such a case it is necessary to have a known reliable route over which the disaster recovery operations can be performed smoothly. Static routes are primarily used for:

- Facilitating the easy maintenance of the routing table in small networks that are not expected to grow.
- Routing to and from other internal route or stub networks. A stub network or an internal route network is a network accessed using a single route and the router has only one neighbor.
- Use as a default or backup route. Such a route is not expected to specifically match any other route in the routing table.

In a network that is not constantly changing, static routes can provide faster and more reliable services by avoiding the network overheads like route advertisement and routing table updates for specific routes.

Reroute Policy with No Action Fallback

When you want to persist the IP address assigned to an entity like a VM to ensure that traffic is sent to that IP address irrespective of the entity it is assigned to, create a Reroute policy with the **No action** option. See Creating a Policy on page 113.

Consider a high availability (HA) entity like a HA firewall VM. When the HA VM fails and the standby VM becomes active, the virtual IP (VIP) is attached to the standby VM. In such a case, the traffic must be routed to the standby VM using the VIP. Configure a Reroute policy with the **No action** option on the VIP assigned to the HA firewall VM to ensure that the traffic is rerouted to the standby VM when the primary VM fails.

When you need to route traffic to an IP address irrespective of the entity that the IP address is assigned to, you can create a traffic routing policy with **Reroute** option and **No action**.

VLAN Basic Subnets (or Basic VLANs)

VLAN Basic Subnets refer to the AHV networking based VLANs that Acropolis creates while creating the AHV clusters (VLAN0 - default VLAN that is used to network the CVMs and AHV hosts) or the VLANs that you create to network the guest VMs using the **Network Configuration** page in Prism Element Web Console.

These traditional AHV VLAN with or without IP management (VLAN Basic Subnets networks with or without IPAM) are managed by Acropolis. Therefore, you can create or manage these VLAN Basic Subnets in the Prism Element Web Console and in Prism Central.

For information about VLAN Basic Subnets, see AHV Administration Guide.

VLAN Subnets (or VLANs)

You create or manage the Network Controller VLANs (or just VLANs) using the network controller. You can only create or manage these VLANs in Prism Central. You cannot use Prism Element Web Console to create or manage these VLANs. The Network controller does not drop unicast traffic when it is specifically supported in VLAN Subnets (Network Controller based VLAN).

If you need to use Network Controller VLANs (VLANs) to the latest networking and network security features such as Flow Network Security Next-Gen.

You cannot migrate the VLANs to Basic VLANs (see Migration of VLAN Basic Subnets on page 97).

For requirements and limitations of VLANs, see Network Types on page 41.

Overlay subnets

You can create an IP-based Overlay subnet for a VPC. An Overlay subnet is a virtualized network that is configured on top of an underlying virtual or physical network. A peer-to-peer network or a VPN are examples of Overlay subnets. An important assumption for the underlying network is connected such that the set of AHV hosts using the same VPCs must have layer 3 connectivity.

There are two types of Overlay subnets and their conditions are:

- Overlay subnets without external connectivity or regular Overlay subnets:
  - Overlay subnets are regular IP-based subnets *without* external connectivity.
  - You can attach an Overlay subnet to regular VPCs or transit VPCs to connect the VPC or transit VPC to VMs or workload entities.
- Overlay subnets with external connectivity or Overlay external networks:
  - You can attach an Overlay external network **only** to a transit VPC.
  - You can connect only VPCs to an Overlay external network. You cannot connect VMs or workload entities to an Overlay external network.
  - You can configure an Overlay external network of either the NAT or the No-NAT type. The No-NAT Overlay external subnet does not support No-NAT gateway scale-out. For information on No-NAT gateway scale-out, see **No-NAT Gateway** in this section.

Traffic Behavior

Broadcast Traffic

Flow Virtual Networking forwards the broadcast traffic to all the guest VMs in the same subnet, irrespective of which AHV hosts these VMs are running on.

Unicast Traffic

Flow Virtual Networking transmits unicast traffic based on the configured networking policies.

Unknown Unicast Traffic

Flow Virtual Networking drops unknown unicast traffic. It is not transmitted to any guest VM within or outside the source AHV host.

Multicast Traffic

Inside a Flow Virtual Networking VPC, multicast traffic is forwarded only within a subnet and to all VMs in that subnet. Currently there is no IGMP snooping within VPCs.

PREREQUISITES FOR FLOW VIRTUAL NETWORKING

Make sure you meet these prerequisites before you enable Flow Virtual Networking on Prism Central.

Requirements

You must have the following fulfilled to enable Flow Virtual Networking:

- Ensure that you log on to Prism Central as a local account user with Prism Admin role, to use Flow Virtual Networking. If you log on to Prism Central as a non-local account (IDP-based) user or without Prism Admin role privileges, then Prism Central does not allow you to enable or use Flow Virtual Networking. The task is reported as **Failed** with a `User Denied Access` message.
- Nutanix deploys a number of ports and protocols in its software. These ports must be open in the firewalls to enable Flow Virtual Networking to function. To see the ports and protocols used Flow Virtual Networking, see Ports and Protocols.
- Ensure that the Prism Central running Flow Virtual Networking is hosted on an AOS cluster running AHV.

  The Network Controller has a dependency only on the AHV version. Ensure that the nodes in all the clusters managed by the same Prism Central are running the same compatible AHV version. See the Release Notes for compatible AHV version.

  When you deploy Prism Central with Network Controller, the prechecks that are run include a check of the AOS and AHV versions. An incompatible version of AHV, Prism Central creates the Network Controller but issues an alert (`Failed to configure host for Atlas networking`) during Network Controller enablement. For more information about the alert, see Prism Central Alerts and Events Reference Guide.

  Upgrade the AOS and AHV versions, as applicable, to the compatible versions.
- Flow Virtual Networking requires reliable connectivity between Prism Central and registered AHV clusters. Ensure that all AHV clusters reside at the same site or datacenter as their registered Prism Central instance. Do not register AHV clusters to a Prism Central at a remote site when using Flow Virtual Networking VPCs. Each site requires a local Prism Central when using Flow Virtual Networking. You can exclude specific AHV clusters from Flow Virtual Networking using CLI configurations.
- Microservices Infrastructure is enabled by default on a Prism Central that is running a minimum Prism Central version of pc.2022.9. For more information, see Prism Central Infrastructure Guide.
- Small, Large and x-Large Prism Central deployments support Flow Virtual Networking.

  Before you enable the Network Controller on a Small or Large Prism Central, ensure that the Prism Central instance is hosted by and registered to the same Prism Element cluster.

  When you enable Flow Virtual Networking on small or large Prism Central deployments, the deployment draws additional resources per PC VM. These additional resources are drawn in addition to the normal resources drawn when a small or large PC is deployed without enabling Flow Virtual Networking

  - For Flow Virtual Networking on a small PC: Every PC VM requires additional 3GB memory and 2 vCPUs.
  - For Flow Virtual Networking on a large PC: Every PC VM requires additional 4GB memory and 3 vCPUs.

  If the additional resources are not available on the hosting nodes, then Flow Virtual Networking is not enabled.

- Although Flow Virtual Networking may be enabled on a single-node PC, Nutanix strongly recommends that you deploy a three-node scale-out Prism Central for production deployments. The availability of Flow Virtual Networking service in Prism Central is critical for performing operations on VMs that are connected to overlay networks. A three-node scale-out Prism Central ensures that Flow Virtual Networking continues to run even if one of the nodes with a PCVM fails.
- Prism Central VM registration. You cannot unregister the Prism Element cluster that is hosting the Prism Central deployment where you have enabled Flow Virtual Networking. You can unregister other clusters being managed by this Prism Central deployment.
- Ensure that you have created a virtual IP address (VIP) for Prism Central. Once set, do not change this address.
- Ensure connectivity:
  - Between Prism Central and its managed Prism Element clusters.
  - To the Internet for connectivity (not required for dark site) to:
    - ECR for Docker images
    - S3 storage for LCM portal

    Note: For dark site deployments, Nutanix provides a dark site bundle, which has the Docker images (normally hosted on ECR) and the Network Controller package (normally hosted on LCM portal). These dark site bundles can be downloaded using an internet-connected system outside the dark site.
- Nutanix recommends increasing the MTU to 9000 bytes on the virtual switch vs0 and ensure that the physical networking infrastructure supports higher MTU values (jumbo frame support). Nutanix recommends configuring the MTU value in the range of 1500 ~ 9000 bytes.

  Note:

  If you try to configure, on the default virtual switch vs0, an MTU value that does not fall within the range of 1500 ~ 9000 bytes, Prism displays an error and fails to apply the configuration.

  Nutanix Controller VMs use the standard Ethernet MTU (maximum transmission unit) of 1,500 bytes for all the network interfaces by default. The system advertises the MTU of 1442 bytes to guest VMs using DHCP to account for the extra 58 bytes used by Generic Network Virtualization Encapsulation (Geneve). However, some VMs ignore the MTU advertisements in the DHCP response. Therefore, to

ensure that Flow Virtual Networking functions properly with such VMs, enable jumbo frame support on the physical network and the default virtual switch vs0.

If you cannot increase the MTU of the physical network, decrease the MTU of every VM in a VPC to 1442 bytes in the guest VM console.

> **Note:** Do not change the MTU of the CVM.

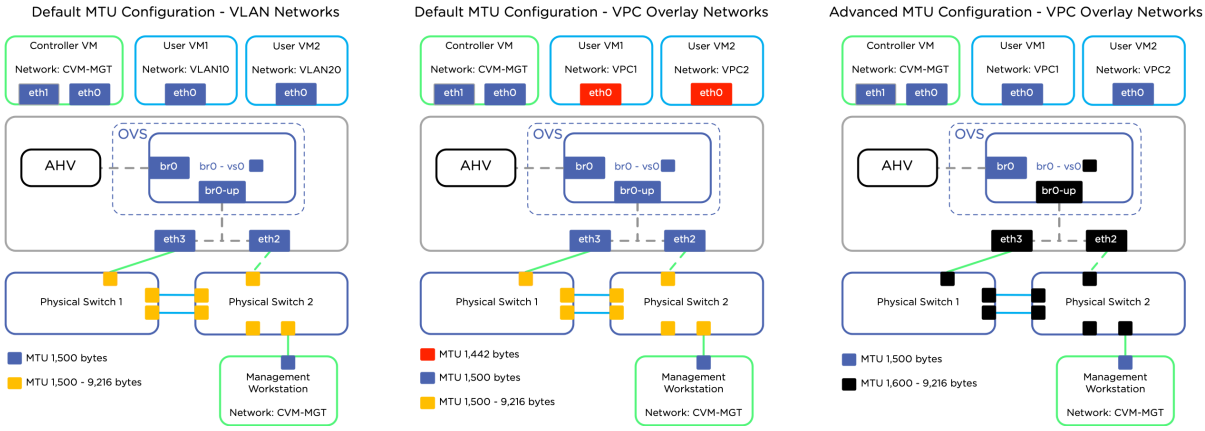


Figure 8: Sample Configurations with and without Higher MTU - VS0, CVM and UVMs

Table 1: Flow Virtual Networking MTUs

Feature	MTU (Overhead Calculation)
VPC	Regular GENEVE = 1442 (1500 - 58 bytes GENEVE)
VPC + Subnet Extension	GENEVE + VXLAN = 1392 (1500 - 58 bytes GENEVE - 50 bytes VXLAN)
VPC + VPN	GENEVE + IPSec = 1356 (1500 - 58 bytes GENEVE - 86 bytes IPsec)
VPC + VTEP + VPN	GENEVE + VXLAN VTEP + IPSec = 1306 (1500 - 58 bytes GENEVE - 86 bytes IPSec - 50 bytes VXLAN)

Requirements for Upgrades

The following applies to upgrades of Network Controller (**Advanced Networking** in **Prism Central Settings**):

- **Compatible AHV Versions**

  Ensure that the AHV hosts in the Prism Element clusters managed by a Prism Central that has Network Controller enabled are running an AHV version compatible with the Network Controller **upgrade**

version. The Network Controller is upgraded but not enabled, if any of the AHV hosts is running an incompatible version.

> **Important:** Before you upgrade the Prism Central version to upgrade the Network Controller, upgrade the AHV version on the hosts with incompatible AHV versions using LCM to the AHV version compatible with the Network Controller upgrade version.

See the Release Notes for compatible AHV version. For information on Prism Central, AHV and AOS version compatibility, see the Compatibility Matrix.

> **Note:** When the Network Controller is deployed with a compatible Prism Central deployment package but with incompatible AHV package, the Network Controller is deployed with Prism Central, but not enabled.

- Ensure that all the AHV hosts in the AOS cluster are running the version compatible with the Network Controller upgrade version.

Limitations

Limitations for Flow Virtual Networking are as follows.

- Flow Virtual Networking is supported only on AHV clusters. It is not supported on ESXi or Hyper-V clusters.
- Flow Virtual Networking is not supported in clusters with Compute-only nodes.
- Flow Virtual Networking is not enabled by default on the new Prism Element cluster registered with the Flow Virtual Networking-enabled Prism Central if the Prism Element cluster has nodes with incompatible AHV versions.
- Flow Virtual Networking does not support updating a VLAN Basic Subnet as an external subnet.

  You cannot enable the external connectivity option in the **Update Subnet** dialog box. Therefore, you cannot modify an existing VLAN-backed subnet to add external connectivity.

  VLAN Basic Subnets for external connectivity are managed by the Flow Virtual Networking control plane. Traditional AHV VLAN IPAM networks are managed by Acropolis.

  > **Note:** Do not configure the same VLAN as both a Flow Virtual Networking external network and an AHV IPAM network, as this can lead to IP address conflicts.

- Flow Virtual Networking cannot be disabled if any external subnets and VPCs are in use. Delete the external subnets and VPCs and then disable Flow Virtual Networking.

FLOW VIRTUAL NETWORKING CONFIGURATIONS

Flow Virtual Networking Network Controller is auto enabled when you install or upgrade an x-Large Prism Central to version PC.2023.3 or later. On Small and Large Prism Central instances, you need to enable the Network Controller.

> **Note:** Auto enabling of Flow Virtual Networking Network Controller occurs only on an x-Large Prism Central.

When you select **Subnets** (see step 2 in Subnets Summary View on page 51) for the first time, the following page indicating that Flow Virtual Networking is *auto enabled*, is displayed:

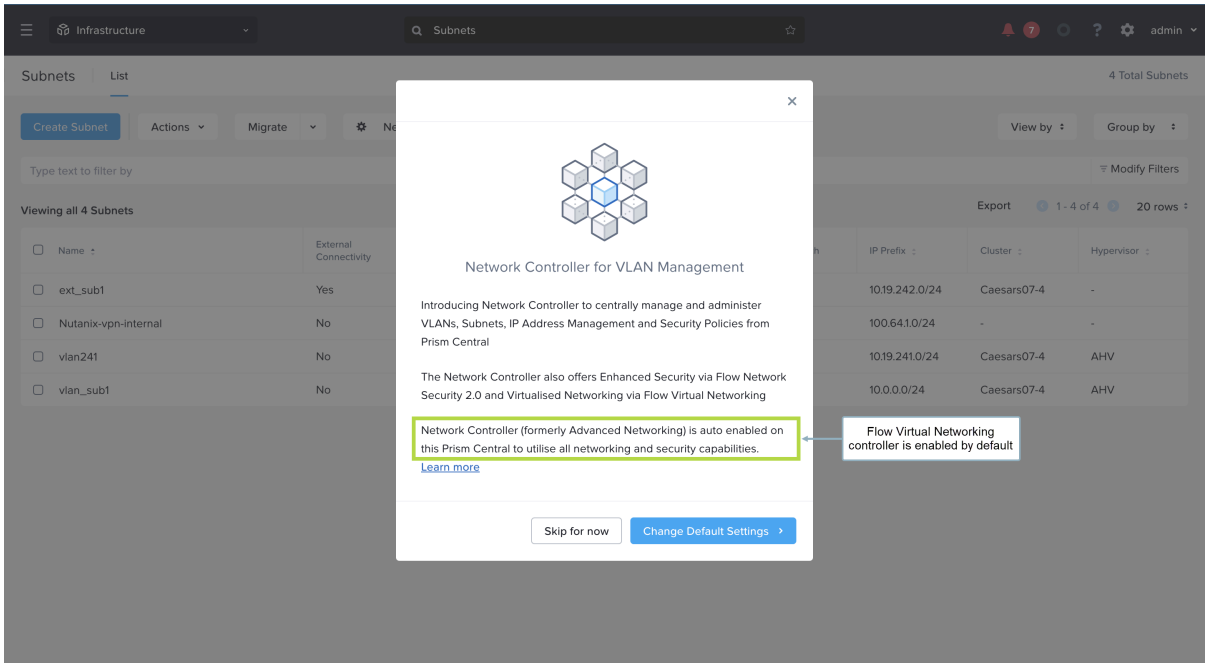


Figure 9: Flow Virtual Networking - Auto Enabled Status Message

Network Controller Settings View

- Log in to Prism Central.
- Click **Prism Central Settings** from the **Navigation Bar** of the **Infrastructure** application.
- On the **Prism Central Settings** page, click **Network Controller**.

  The **Network Controller (formerly Advance Networking)** page opens.

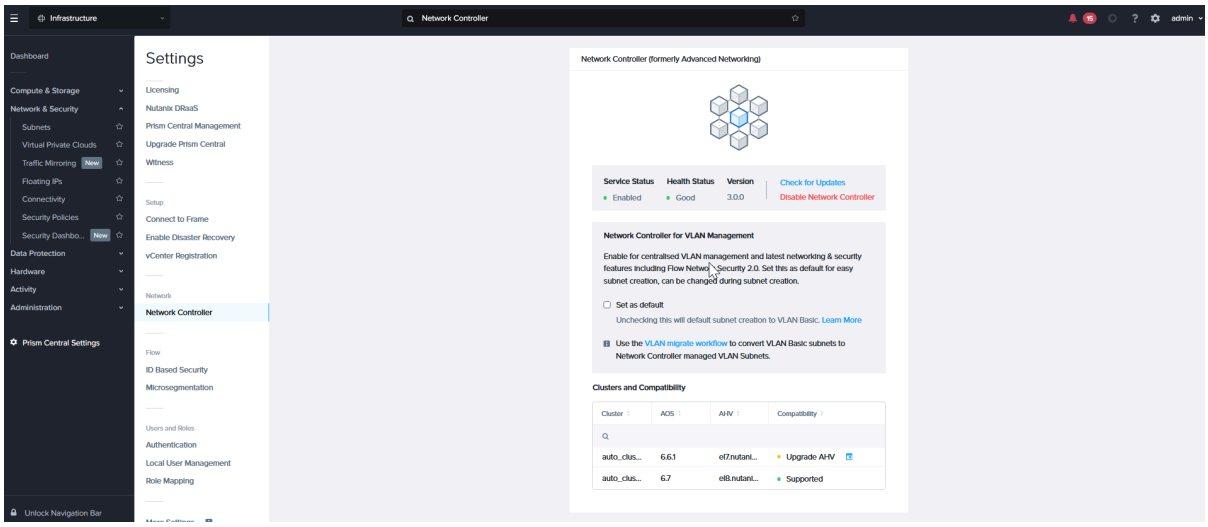


Figure 10: Network Controller (formerly Advance Networking)

On the **Network Controller (formerly Advanced Networking)**, the **Set as default** check box is clear by default to ensure that VLAN Basic (AHV based VLANs) is the default VLAN type. Select the **Set as default** check box to make VLAN Subnets (Network Controller based VLANs) the default VLAN type.

For information about the types of networks that Flow Virtual Networking creates and manages, see Network Types on page 41.

For information about migrating VMs from AHV based VLANs or VLAN Basic Subnets to Overlay networks, see Migration of VMs between VLAN Basic Subnet and VPC Subnets on page 88.

If you need to convert the AHV-based VLANs or VLAN Basic Subnets to Network Controller based VLANs or VLAN Subnets, see Migration of VLAN Basic Subnets on page 97.

Enabling the Network Controller

About this task

If you have a Small or Large Prism Central deployment, you need to manually enable the Network Controller.

Before you proceed to enable the Network Controller by clicking the **Network Controller** option on the **Prism Central Settings** page, see Prerequisites for Flow Virtual Networking on page 21.

Perform the following steps to enable Flow Virtual Networking.

Procedure

- Log in to Prism Central.
- Click **Prism Central Settings** from the **Navigation Bar** of the **Infrastructure** application. The **Prism Central Settings** page opens.
- Click **Network Controller**.

- In the **Network Controller (formerly Advanced Networking)** pane, click **Enable**.
  Ensure that the prerequisites specified on the pane are fulfilled.

Network Controller (formerly Advanced Networking)

Network Controller is a component of Prism Central that manages and controls configuration, monitoring and optimization of Network resources. It provides programmability, automation, and centralized control for configuring and managing network flows.

Network Controller is necessary to use centralized VLAN management, Flow Network Security Next-Gen or Flow Virtual Networking.

Requirements

Network Controller requires 2 vCPUs and 3GB RAM for small Prism Central VMs and 3 vCPUs and 4GB RAM for large Prism Central VMs. The VMs will be resized automatically upon enabling Network Controller.

To enable Network Controller ensure that

1. Prism Central can access download.nutanix.com
2. Prism Central has Microservice Infrastructure configured.

After enabling,

- Network Controller will be available for all AHV Clusters running AOS 6.1 or higher.
- The default configuration when creating new subnets will be VLAN Basic. You can change the subnet type during creation under the Advanced Configuration option or change the default to set Network Controller managed subnet.
- VLAN Basic subnets can be migrated to Network Controller managed VLAN subnets.

Enable

Figure 11: Enabling Network Controller

Prism Central displays the deployment in-progress.

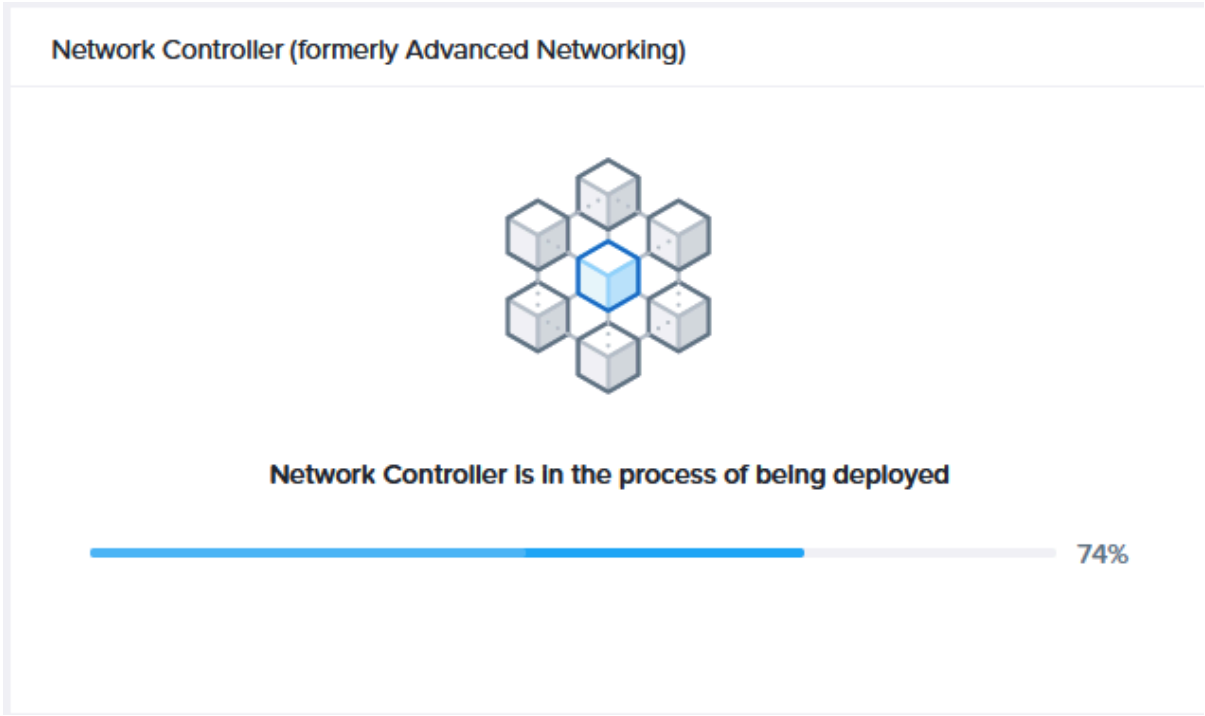


Figure 12: Deployment Progress

- Flow virtual networking is enabled.

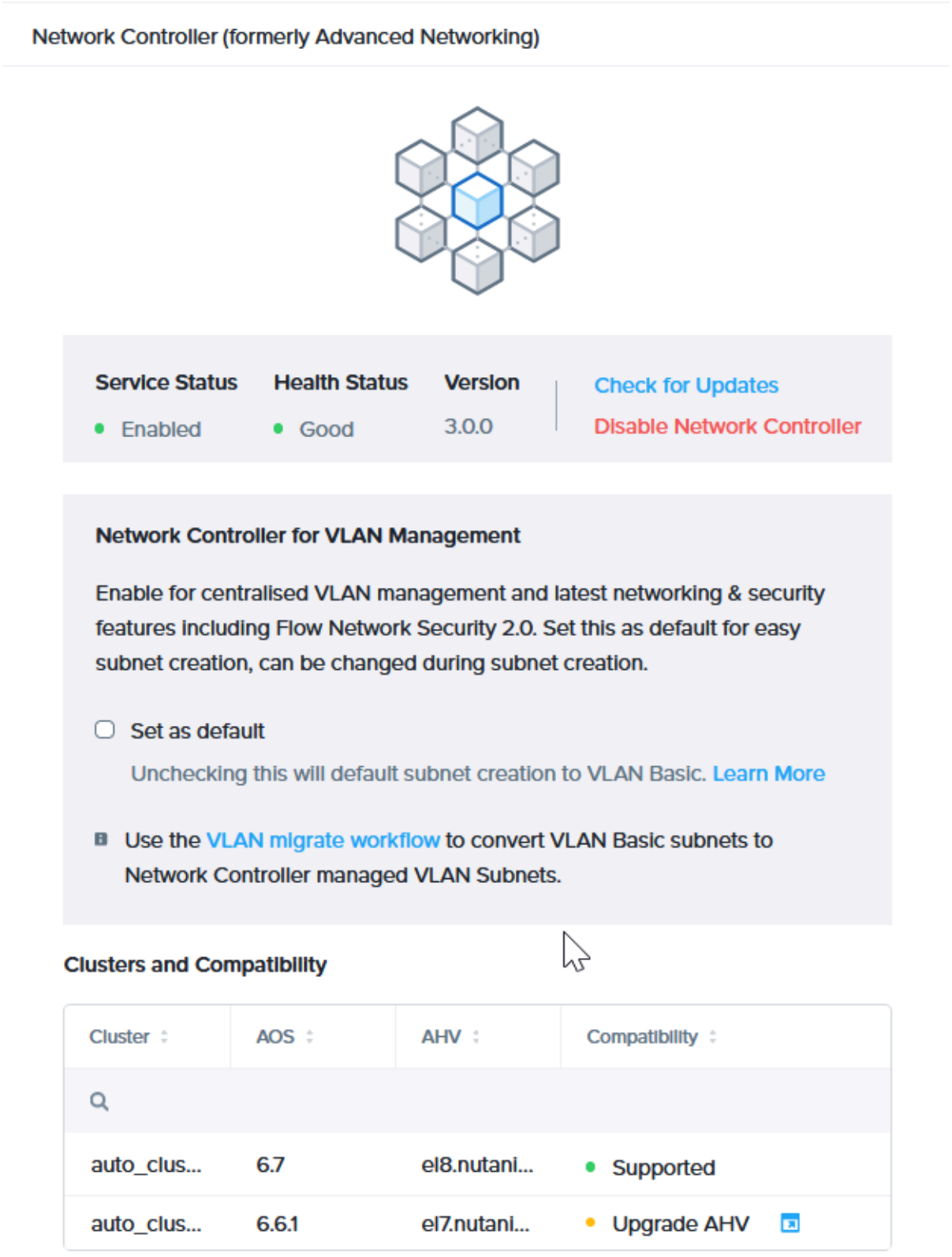


Figure 13: Flow Virtual Networking Status

Disabling the Network Controller

About this task

You can disable the Flow Virtual Networking Network Controller.

> **Note:**
> You cannot disable the if any external subnets and VPCs are in use. Delete the external subnets and VPCs and then disable Flow Virtual Networking.

To disable Flow virtual networking, do the following.

Procedure

1. Log in to Prism Central.
2. Click **Prism Central Settings** from the **Navigation Bar** of the **Infrastructure** application.
   The **Prism Central Settings** page opens.
3. Click **Network Controller**.
4. On the **Network Controller (formerly Advance Networking)** page, click **Disable Network Controller**.

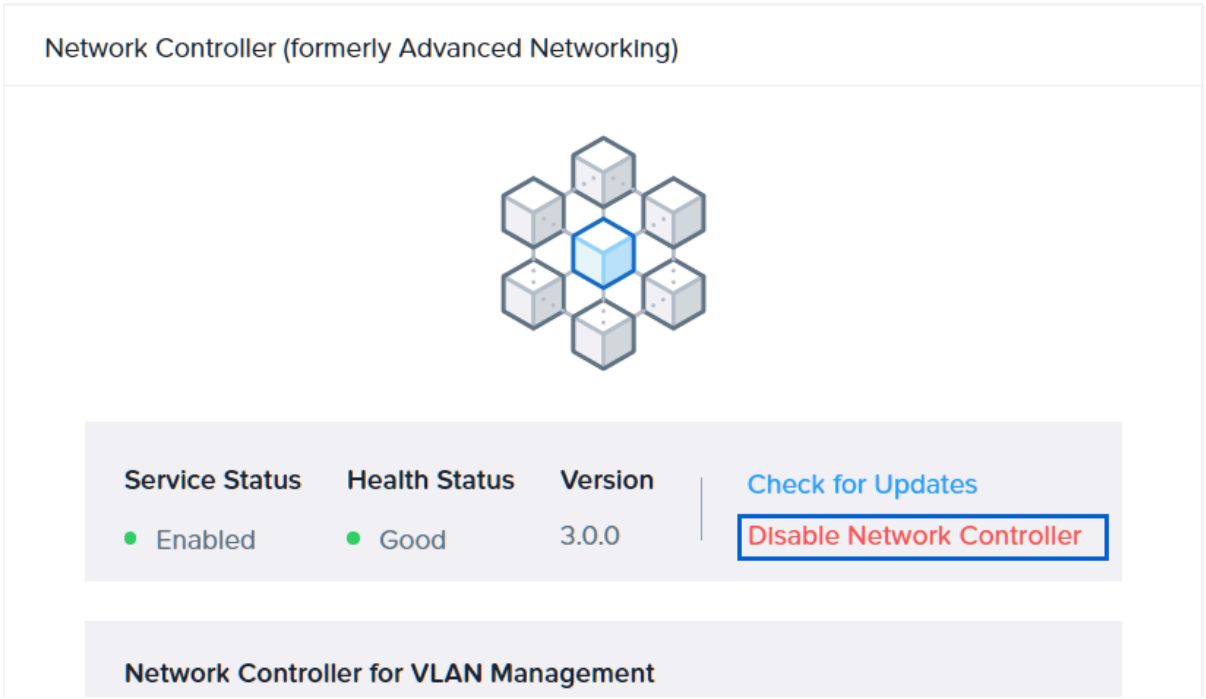


Figure 14: Disable the Network Controller

5. On the confirmation message box, click **Confirm** to confirm disablement.

   To exit without disabling the **Network Controller**, click **Cancel**.

Unregistering a PE from the PC

Before unregistering a Prism Central from the Prism Element cluster, disable Flow Virtual Networking on that Prism Element using network controller CLI (or atlas_cli).

About this task

When Flow Virtual Networking is enabled on a Prism Central, it propagates the capability to participate in VPC networking to all the registered Prism Elements that are running the required AHV version.

In cases where there are VMs on the Prism Element attached to the VPC network, or if the Prism Element is used to host one or more of the external VLAN networks attached to a VPC, Prism Central alerts you with a prompt. When being alerted about the aforementioned conditions, close the CLI and make adequate configuration to resolve the condition (for example, select a different cluster for the external VLAN network and delete the VMs attached to the VPC network running on the Prism Element). After making such configurations, execute the network controller CLI to disable Flow Virtual Networking. If the command goes through successfully, it is safe to unregister the Prism Element.

For example, in a deployment of three Prism Elements - PE1, PE2 and PE3 - registered to the Flow Virtual Networking-enabled PC, you want to unregister PE3 from the PC. You must first disable Flow Virtual Networking using the steps in Disabling the Network Controller on page 32 or the following steps:

Procedure

1. SSH to PE3.
2. Run the `ncli cluster info` or `ncli cluster get-params` command to get the cluster parameters.

   Copy the cluster UUID (For example: 017457d3-1012-465c-9c54-aa145f2da7d9) from the displayed cluster parameters.
3. SSH to the Prism Central VM.
4. Open the network controller console by executing the `atlas_cli` command.

   ```
   nutanix@cvm$ atlas_cli
   ```

   ```
   <atlas>
   ```
5. Execute the `config.add_to_excluded_clusters <cluster uuid>` command, providing the cluster UUID that you copied earlier.

   An example of the PC alert, for the condition that PE3 VM is attached to an external network, is as follows:

   ```
   <atlas> config.add_to_excluded_clusters 0005bf8d-2a7f-3b2e-0310-d8e34995511e
   Cluster 0005bf8d-2a7f-3b2e-0310-d8e34995511e has 1 external subnet,
   which will lose connectivity. Are you sure? (yes/no)
   ```

   > **Note:** To enable Flow Virtual Networking on the cluster, execute the `config.remove_from_excluded_clusters <cluster uuid>` command, providing the cluster UUID.

What to do next

To verify if Flow Virtual Networking is disabled, SSH to PE3 and run the `acli atlas_config.get` command.

The output displays the `enable_atlas_networking` parameter as `False` if Flow Virtual Networking is disabled and as `True` if Flow Virtual Networking is enabled on the Prism Element.

```
nutanix@cvm$ acli atlas_config.get
config {
  anc_domain_name_server_list: “10.10.10.10”
  enable_atlas_networking: False
  logical_timestamp: 19
  minimum_ahv_version: “20190916.101588"
  ovn_cacert_path: “/home/certs/OvnController/ca.pem”
  ovn_certificate_path: “/home/certs/OvnController/OvnController.crt”
```

```
  ovn_privkey_path: “/home/certs/OvnController/OvnController.key”
  ovn_remote_address: “ssl:anc-ovn-external.default.anc.aj.domain:6652"
}
```

You can now unregister the PC from the PE cluster. For steps to unregister a Prism Central from a Prism Element cluster, see Unregistering a cluster from Prism Central

Upgrading the Network Controller

You can upgrade the Flow Virtual Networking controller (*Advanced Networking Controller* in *Prism Central Settings*) using Life Cycle Manager (LCM) on Prism Central.

Before you begin

See Prerequisites for Flow Virtual Networking on page 21.

In case of upgrading the Flow Virtual Networking controller in a dark site, ensure that LCM is configured to reach the local web server that hosts the dark site upgrade bundles.

> **Note:**
>
> The network controller upgrade fails to start after the pre-check if one or more clusters have Flow Virtual Networking enabled and are running an AHV version incompatible with the new network controller upgrade version.

About this task

To upgrade the network controller using LCM, do the following.

Procedure

1. Log in to Prism Central.
2. Select the **Admin Center** application from the Application Switcher Function, and click **LCM** from the **Navigation Bar**.
   The **LCM** page opens displaying the **Best Practices** tab.
3. Click the **Inventory** tab.
4. Click **Perform Inventory**.

   When you click **Perform Inventory**, the system scans the registered Prism Central cluster for software versions that are running currently. Then it checks for any available upgrades and displays the information on the LCM page under the **Updates** tab.
5. Click the **Updates** tab.
   The **Updates** page opens displaying the available software updates.
6. Select the check box associated with **Networking Controller** and click **View Upgrade Plan**.
   The **Review Update Plan** window opens.
7. Click **Apply 1 Updates**.

Dark Site Installation and Upgrade

Dark sites are primarily on-premises installations which do not have access to the internet. Such sites are disconnected from the internet for a range of reasons including security. To install or upgrade the Network Controller at such dark sites, you need to deploy the Network Controller bundle at the site.

This dark site deployment procedures include downloading and deploying the LCM dark site server bundles, downloading and deploying the Nutanix Compatibility bundle to ensure that the latest product meta data is available, and the network controller bundles.

See Prerequisites for Flow Virtual Networking on page 21.

Prerequisite steps

You need access to the Nutanix Portal from an Internet-connected device to complete these steps.

> **Note:** For dark site deployments, Nutanix provides a dark site bundle, which has the Docker images (normally hosted on ECR) and the Network Controller package (normally hosted on LCM portal). These dark site bundles can be downloaded using an internet-connected system outside the dark site.

Do the following before you install or upgrade the Network Controller:

- Update the LCM Framework. See Updating the LCM Framework Using a Web Server in the *Life Cycle Manager Dark Site Guide*.
- Install and prepare the LCM Dark Site server. See Setting up a Local Web Server in the *Life Cycle Manager Dark Site Guide*.

  Take note of the FQDN or IP address of the LCM Dark Site server (Local Web Server). For example, in this documentation, `<LCM-web-server-ip>` is used to indicate the IP address of the LCM Dark Site server and `~/release` is the path of the dark site server folder.
- Ensure that you have configured the **Dark Site (Local Web Server)** settings on the **LCM** > **Settings** page.
- Update the firmware specific to the installed platform hardware (including the Nutanix Compatibility bundle). See Fetching the Firmware Update Bundle Using a Web Server.

  > **Note:** After you have downloaded the Nutanix Compatibility bundle tar.gz file, verify if the contents match the following output.

  ```
  [root@<LCM-web-server-ip> ~]$ tar -tvf
   nutanix_compatibility_bundle.tar.gz

  -rw-r--r-- jenkins/jenkins nutanix_compatibility.tgz

  -rw-r--r-- jenkins/jenkins nutanix_compatibility.tgz.sign

  -rw-rw-r-- jenkins/jenkins nutanix_compatibility.tgz.v2.sign

  -rw-rw-r-- jenkins/jenkins lcm_cert_v2.crt

  -rw-rw-r-- jenkins/jenkins lcm_intermediate_v2.crt

  nutanix@cvm$
  ```

- On the Flow Virtual Networking Downloads page, ensure that **ANC** is selected in the component selection dropdown menu. Download the Network Controller bundle: Copy the **Md5** value for the bundle.

Deploying the Network Controller at a Dark Site

Before you begin

See the prerequisites provided in Prerequisites for Flow Virtual Networking on page 21.

Complete the *Prerequisite steps* provided in Dark Site Installation and Upgrade on page 34.

About this task

When you deploy Prism Central in a dark site, the Network Controller bundle needs to be separately downloaded for deployment by Prism Central.

In x-Large Prism Central deployments, the Network Controller is automatically enabled.

In small and large Prism Central deployments, you must manually enable the Network Controller. See Enabling the Network Controller on page 26.

To upgrade the installed Network Controller, see Upgrading the Network Controller at a Dark Site on page 37.

Procedure

1. Log on to the LCM Dark Site server (Local Web Server) with root privileges.
2. Verify that the contents of the Network Controller bundle is similar to the following sample output for the Network Controller 3.0.0 bundle:

   ```
   [root@<LCM-web-server-ip> ~]$ tar -tzf 3.0.0.tar.gz
   ```

   ```
   builds/
   builds/atlas-controller/
   builds/atlas-controller/3.0.0/
   builds/atlas-controller/3.0.0/atlas_network_controller.tar.gz
   builds/atlas-controller/3.0.0/metadata.sign
   builds/atlas-controller/3.0.0/metadata.json
   ```

3. Extract the Network Controller bundle to `~/release`

   The following is a sample of the command to extract the Network Controller bundle.

   ```
   [root@<LCM-web-server-ip> ~]$ sudo tar -zxvf 3.0.0.tar.gz -C ~/release/
   ```

4. Run the following command after unpacking to ensure that the file permissions are not disrupted during the unpacking:

   ```
   chmod -R +r builds
   ```

5. In Prism Central, navigate to **Admin Center** > **LCM** > **Settings**.

   - Select **Source** > **Dark Site (Local Web Server)**
   - Enter the `http://<LCM-web-server-ip>/release` in **URL**.

6. SSH into the Prism Central VM as an admin user and run the following commands.

   ```
   admin@pcvm$ mspctl controller airgap enable --url=http://<LCM-web-server-ip>/release
   ```

   ```
   admin@pcvm$ mspctl controller airgap get
   ```

7. Verify that the source for deployment is configured as the dark site server.

   Log on to the Prism Central VM through an SSH session as a `nutanix` user, and run the following command.

   ```
   nutanix@pcvm$ configure_lcm --print | grep -i "msp\|atlas\|dark"
   ```

   The following sample output shows that `is_darksite` is `True`.

   ```
   msp: {"url": "BASE_URL/msp-builds/", "flags": [], "component": "msp", "tags": []}

   atlas_controller: {"url": "BASE_URL/atlas-controller/", "flags": [], "component":
    "atlas_controller", "tags": []}
   ```

```
is_darksite: True

enable_https_darksite: False

nutanix@NTNX-10-19-57-54-A-PCVM:~$
```

Where `BASE_URL` is the source location for the bundles. This should match `http://<LCM-web-server-ip>/release`.

8. Enable **Network Controller**. For more information, see Enabling the Network Controller on page 26.

Upgrading the Network Controller at a Dark Site

This procedure lets you upgrade the Network Controller in a dark site.

About this task

The procedure to upgrade the Network controller in a dark site consists of all the steps in the Deploying the Network Controller at a Dark Site on page 35 procedure up to the step that verifies that the source for upgrades is configured as the dark site server.

After the verification step, perform the following steps.

Procedure

1. In Prism Central, navigate to **Admin Center** > **LCM** > **Inventory** and click **Perform Inventory**.
   The **LCM** > **Updates** tab displays the **Networking Controller** upgrade version bundle.
2. Select the **Networking Controller** component.
3. Run **Pre-Upgrade** > **Upgrade Prechecks**.
   a. On the **Initiate Precheck?** window, click **Continue**.
      LCM runs the prechecks for upgrade.
   b. When the **Precheck successful!** message is displayed, click **Return to Updates** to return to the **Updates** page.
4. Upgrade **Networking Controller**.
   a. Click **View Upgrade Plan**.
   b. On the **Review Upgrade Plan** page, click **Apply _ Updates**.
   c. Click **Return to Updates** after the upgrade is complete.

Control User Access in Flow Virtual Networking (RBAC)

Flow Virtual Networking supports role-based access control (RBAC) that you can configure to provide customized access permissions for users based on their assigned roles. The roles dashboard allows you to view information about all defined roles and the users and groups assigned to those roles.

For more information about configuring RBAC for Flow Virtual Networking, see Controlling User Access (RBAC) in the *Nutanix Security Guide*.

Flow Virtual Networking Roles and Permissions

Flow Virtual Networking provides certain pre-configured roles and permissions with those roles.

Prism Central provides two roles for Flow Virtual Networking management:

- **VPC Admin** which has 41 permissions pre-configured to manage Overlay or VPC networking including create,update, and delete networks.
- **Network Infra Admin** which has 24 permissions pre-configured to manage the network infrastructure (underlay) on the AHV network stack.

The table provides the list of permissions that are pre-configured for the two roles.

Entity	Permissions	VPC Admin	Network Infra Admin
Virtual Switch (DVS)	View, Create, Update and Delete	View Only	View Only
	Migrate	No	Yes
VLAN Subnets	View, Create, Update, Delete, Migrate and IP Reservation	No	Yes
IPFix	View, Create, Update and Delete	Super Admin role can only perform this operation.	
VLAN External Subnets	View	Yes	Yes
	Create, Update and Delete	No	Yes
Advanced Network Controller deployment	Super Admin and Prism Admin Roles have permissions to perform this operation. The permissions for this operation are not provided on the **Roles** page.		
VPC	View and View_NS_stats	Yes	No
	Create	Yes	No
	Update	Yes	No
	Delete	Yes	No
Overlay Subnets	View, Create, Update and Delete	Yes	No
Overlay External Subnets	View	Yes	No
	Create, Update and Delete	No	No
Floating IP Addresses	View, Create, Update and Delete	Yes	No
Policy Based Routing (PBR)	View, Create, Update, Delete and Clear Containers	Yes	No
Routes	View, Update	Yes	No
Network Gateways (VPN, VTEP and BGP)	View, Create, Update and Delete	Yes	Yes
VPN Connections	View, Create, Update, Delete and Configuration Download	Yes	Yes
Layer 2 Stretch	View, Create, Update and Delete	Yes	Yes

Entity	Permissions	VPC Admin	Network Infra Admin
BGP Sessions	View, Create, Update and Delete	Yes	No
VM (Not networking objects)	View	Yes	Yes
	Create, Update and Delete	No	No
Cluster (Not networking objects)	View	No	Yes
Cluster Networking capabilities	View	Yes	Yes
Uplink Bonds	View	No	Yes
Status of schedulable Nodes	View	Yes	Yes
VPC Virtual Switch mappings	View and Update	Yes	No
Layer 2 Stretch related entities	View	Yes	Yes
Availability Zones (AZs)	View	Yes	No

Flow Virtual Networking Operational Authorizations

Flow Virtual Networking requires you to have certain permissions or authorizations to complete certain tasks.

The table provides the list of permissions you need to perform various operations. Ensure that the necessary permissions are set for your role, to perform the necessary operations.

> **Note:** This table provides a sample list of operations and necessary authorizations for Flow Virtual Networking. This list may not be a complete or extensive list.

Operations	Authorizations You need
Enable or deploy the Network Controller	• Permission to **Create** Network Controller. • Permission to **View** the **VLAN Subnet** on which the Network Controller is deployed.
Create Virtual Switch	• Permission to **Create** virtual switch • Permission to **View** the **Host** on which the virtual switch is instantiated.
Create VLAN Subnet	Permission to **Full Access** for the **VLAN Subnet** entity

Operations	Authorizations You need
Create vNIC on a VLAN Subnet or Overlay Subnet	• Necessary permissions for VM operations. Set these for the **VM** entity, including **View Overlay Subnet** and **View Subnet** • **View** permission for **VLAN Subnet** or **Overlay** subnet.
Create or Update a VPC Attach the VPC to an external subnet	• **Create VPC**, **Update VPC** • **View External Subnet**
Create Overlay Subnet, PBR or Route Update Route table	• **Create Overlay Subnet**, **Create Routing Policy** for PBR or **Update VPC Route Table** • **View VPC** to view the VPC to which the Overlay subnet, PBR or route table is attached
Create Network Gateway on VPC	• **Create Network Gateway** or **Update Network Gateway** • **View VPC** to view the VPC
Create Network Gateway on a VLAN subnet	• **Create Network Gateway** or **Update Network Gateway** • **View Subnet** to view the VLAN subnet
Create or Update BGP Gateway on VPC (Optionally with serviced VPC specified).	• **Create** and **Update** permissions for BGP Gateways. • **View VPC** to view the VPC subnet • **View** permissions for the serviced VPC if specified.
Create or Update BGP on VLAN (Optionally with serviced VPC specified).	• **Create** or **Update** BGP gateway. • **View Subnet** • **View VPC** to view the serviced VPC only if serviced VPC is specified. • **View Network Gateway** to view the local and remote network gateways
Create VPN Connection	• **Create VPN Connection** or **Update VPN Connection** • **View Subnet** to view the VLAN subnet
Create a Direct Connect on a VPC (For Nutanix Cloud Cluster on AWS)	• **Create** permission for Direct Connect. • **View** permission for the VPC.

Operations	Authorizations You need
Create Direct Connect Virtual Interfaces (VIFs)	• **Create** permission for Direct Connect. • **View** permission to view the Direct Connect VIF entities.
Create or Update Floating IP Address on an external subnet	• **Create Floating IP** or **Update Floating IP** • **View External Subnet** to view the external subnet
Attach Floating IP to vNIC of a VM	• **Update Floating IP** • **View VM** to view the vNIC of the VM
Attach Floating IP to Private IP of a VPC	• **Update Floating IP** • **View VPC** to view the VPC properties
Create a Layer 2 Network Extension on a subnet through a VPN connection	• **Create** permission for Layer 2 Network Extension • **View** permissions for the subnet that needs to be extended. • **View** permission for the VPN connection to be used for the extension.
Create a Layer 2 Network Extension on a subnet through a VTEP connection	• **Create** permission for Layer 2 Network Extension • **View** permissions for the subnet that needs to be extended. • **View** permission for the VTEP gateways to be used for the extension.
Create BGP Session	• **Create BGP Session** • **View** Network Gateway permissions for local and remote gateways.

Network Types

Flow Virtual Networking Network Controller supports Overlay and VLAN type networks.

Overlay networks

You can create an IP-based Overlay subnet for a VPC. An Overlay network is a virtualized network that is configured on top of an underlying virtual or physical network. Examples of Overlay networks are:

- You can create an Overlay subnet with external connectivity (Overlay external subnet) to connect a transit VPC to other regular VPCs.
- You can create a special purpose multicast network as an Overlay network within an existing network.

- A peer-to-peer network or a VPN.

An important assumption for an Overlay network is that the underlying network is fully connected. Nutanix provides the capability to create Overlay network-based VPCs.

For more information, see *Overlay networks* in Essential Concepts on page 12.

VLAN networks

Starting with Prism Central pc.2023.3 with AOS 6.7 and AHV 20230302.198, Network Controller 3.0.0 and later versions support the creation of VLANs (VLAN Subnets) on the Flow Virtual Networking Network Controller. The Network Controller also supports migration of VLAN Basic Subnets to VLAN Subnets subject to support and limitations information provided in the *VLAN Subnets Support* section.

For information about migration of VLAN networks, see VM and Network Migration on page 88.

VLAN Basic Subnets (or Basic VLANs)

VLAN Basic subnets are not managed by the network controller in Prism Central, and are instead managed by the Acropolis leader of their Prism Element cluster. VLAN Basic Subnets refer to the AHV networking based VLANs that Acropolis creates while creating the AHV clusters (VLAN0 - default VLAN that is used to network the CVMs and AHV hosts) or the VLANs that you create to network the guest VMs using the **Network Configuration** page in Prism Element Web Console.

These traditional AHV VLAN with or without IP management (VLAN Basic Subnets networks with or without IPAM) are managed by Acropolis. Therefore, you can create or manage these VLAN Basic Subnets in the Prism Element Web Console and in Prism Central.

You can only use Prism Central to migrate these VLAN Basic Subnets to Network Controller-based VLANs that you can manage in Prism Central (see Migration of VLAN Basic Subnets on page 97).

VLAN Subnets (VLANs)

Create or manage the VLAN Subnets (VLANs) or Network Controller managed VLANs using the Flow Virtual Networking Network Controller. You can only create or manage these VLAN Subnets in Prism Central. You cannot use Prism Element Web Console to create or manage these VLAN Subnets.

> **Note:** Clusters with CO nodes do not support the creation of VLAN Subnets.

For more information, see *VLANs (or VLAN Subnets)* in Essential Concepts on page 12.

VLAN Subnets (VLANs) Support

VLAN Subnets (VLANs) supports the following:

- **IGMP Snooping**

  For more information about IGMP snooping in Nutanix networks, see the IGMP Snooping documentation.

- **vNIC creation with Access VLAN mode**

  Network Controller VLAN Subnets support only access mode, and do not support VLAN trunk mode.

- **DHCP options on managed VLAN Subnets**

  VLAN subnets that are managed networks (networks which use IPAM managed IP addresses) support DHCP options.

- **Traffic Mirroring**

  VLAN Subnets support Traffic Mirroring. For information about Traffic Mirroring, see Traffic Mirroring on AHV Hosts in *AHV Administration Guide* and Traffic Mirroring in *Prism Central Infrastructure Guide*.

- **Unknown Unicast Traffic**

  VLAN Subnets support unknown unicast

- **vNIC Scale**

  The Network Controller only supports VMs with vNIC associated with either the AHV networking stack or the Network Controller stack.

- **IPFIX Exporter**

  VLAN Subnets support IPFIX Exporter.

- **TFTP Server IP Address**

  If you need to configure a TFTP server for a managed network, use the IP address of the TFTP server instead of the FQDN.

VLAN Subnet (VLAN) does not support the following:

1. Nutanix Files
2. Trunk mode
3. Virtual NICs in kDirect mode
4. You cannot update a vNIC on a VLAN Subnet that was created by migrating a VLAN Basic Subnet. Delete the vNIC that needs to be updated and create a new vNIC with the updated parameters.
5. Unknown unicast flooding and disabling port security. Any VMs or workloads that depend on unknown unicast traffic are impacted during the subnet migration workflow. When the VMs are migrated to the Flow Virtual Networking network controller, port security is enabled and unknown unicast stops working.
6. Service chaining (see *Service Chain* in Essential Concepts on page 12.
7. Remote Office Branch Office (ROBO) deployments
8. Clusters with Compute-only nodes

Changing the Default VLAN Type

With a minimum Prism Central version of PC.2023.3 that deploys Network Controller 3.0.0, you can change the default VLAN creation from VLAN Subnet (VLAN) type to VLAN Basic Subnet type and vice versa.

About this task

To change the default VLAN type created using the Creating a Subnet workflow, do the following:

Procedure

1. Log on to Prism Central.
2. Select the **Infrastructure** application from the Application Switcher function.

3. To change the default VLAN type in **Prism Central Settings**, do the following.

   a. Click **Prism Central Settings** from the **Navigation Bar** of the **Infrastructure** application.

      For more information about the **Navigation Bar** of Prism Central applications, see Application-specific Navigation Bar in the Prism Central Infrastructure Guide).

      The Prism Central Settings page opens.

   b. Click **Network Controller**.

   c. On the **Network Controller (formerly Advanced Networking)** page, under

      » Clear the **Set as default** check box to set the default VLAN type as VLAN Basic Networking. The **Set as default** is cleared by default ensuring that the VLAN Basic Networking is the default VLAN type when you deploy or upgrade Prism Central.

      » Select the **Set as default** check box to set the default VLAN type as VLAN Subnets (or Network Controller VLANs).

4. To change the default VLAN type when you navigate to **Network & Security** > **Subnets** for the first time after the Prism Central is deployed or upgraded.

   The **Network Controller for VLAN Management** page opens.

   a. On the **Network Controller for VLAN Management**, click **Change Default Settings**.

      The **Network Controller (formerly Advanced Networking)** page in **Prism Central Settings** opens.

   b. On the **Network Controller (formerly Advanced Networking)** page, under

      » Clear the **Set as default** check box to set the default VLAN type as VLAN Basic Networking. The **Set as default** is cleared by default ensuring that the VLAN Basic Networking is the default VLAN type when you deploy or upgrade Prism Central.

      » Select the **Set as default** check box to set the default VLAN type as VLAN Subnets (or Network Controller VLANs).

5. To change the default VLAN type to VLAN Basic Subnet while Creating a Subnet on page 106, do the following.

   a. Navigate to **Network & Security** > **Subnets**

   b. Click **Create Subnet** to create a VLAN network.

      Provide the necessary configuration details for the VLAN Basic Subnet.

   c. Under **Advanced Configuration**, select the **Advanced Configuration** check box under **VLAN Basic Networking**.

   For more information about creating a subnet, see Creating a Subnet on page 106.

Troubleshooting Tips

This section provides information to assist troubleshooting of Flow Virtual Networking deployments. This is in addition to the information that the *Prism Central Infrasturcture Guide* provides.

Audit Logs

Prism Central generates audit logs for all the flow networking activities like it does for other activities on Prism Central. For more information, see Audit Summary View in the *Prism Central Infrasturcture Guide*.

Support Bundle Collection

To support troubleshooting for Flow Virtual Networking, you can collect logs.

To collect the logs, run the following commands on the Prism Central VM console:

```
nutanix@cvm$ logbay collect -t msp,anc
```

An example of the command is as follows:

```
nutanix@cvm$ logbay collect -t msp,anc -O
 msp_pod=true,msp_systemd=true,kubectl_cmds=true,persistent=true --
duration=-48h0m0s
```

Where:

- `-t` flag indicates the tags to collect
  - *`msp`* tag will collect logs from the services running on MSP pods and persistent log volumes (application-level logs)
  - *`anc`* tag will collect the support bundle, which includes database dumps and OVN state
- `-O` flag adds tag-level options
  - `msp_pod=true` collects logs from MSP service pods

    On the PC, these logs can be found under `/var/log/containers`.
  - `persistent=true` collects persistent log volumes (application-level logs for ANC)

    On the PC, these can be found under /var/log/ctrlog
  - `kubectl_cmds=true` runs `kubectl` commands to get the Kubernetes resource state
- `--duration` sets the duration from the present to collect

The command run generates a zip file at a location, for example: `/home/nutanix/data/logbay/bundles/<filename>.zip`

Unzip the bundle and you'll find the *`anc`* logs under a directory specific to your MSP cluster, the worker VM where the pod is running, and the logging persistent volume of that pod. For example:

`./msp/f9684be8-b4e8-4524-74b4-076ed53ca1fd/10.48.128.185__worker_master_etcd/persistent/default/ovn/anc-ovn_StatefulSet/`

For more information about the task run, see the text file that the command generates at a location, for example:`/home/nutanix/data/logbay/taskdata/<taskID>/collection_result.txt`

For more information about the `logbay collect` command, see the *Logbay Log Collection (Command Line)* topic in the *Nutanix Cluster Check Guide* (NCC Guide).

Layer 2 Virtual Subnet Extension Alert

The `L2StretchLocalIfConflict` alert (Alert with Check ID - 801109) may occur while performing Layer 2 virtual subnet extensions. See KB-10395 for more information about its resolution.

NETWORK GATEWAY UPGRADES

Nutanix deployment can detect and install upgrades for the on-premises Network Gateways. Network Gateways may be deployed for Virtual Private Networks (VPNs) connections, Virtual Tunnel End Point (VTEP) connections and Border Gateway Protocol (BGP) sessions.

For information about identifying the current Nutanix Gateway version, see Identifying the Gateway Version on page 46.

For on-premises Network Gateways, the upgrades must detected and installed on the respective Prism Central on which each Network Gateway is installed. For more information, see Detecting Upgrades for Gateways on page 47.

When Prism Central detects the upgrades, it displays a banner on the **Gateways** tab of the **Connectivity** page. The banner notifies you that a Gateway upgrade is available after you have run LCM inventory. The table on the **Gateways** tab also displays an alert (exclamation mark) icon for the network gateways that the upgrade applies to. The hover message for the icon informs you that an upgrade is available for that Gateway.

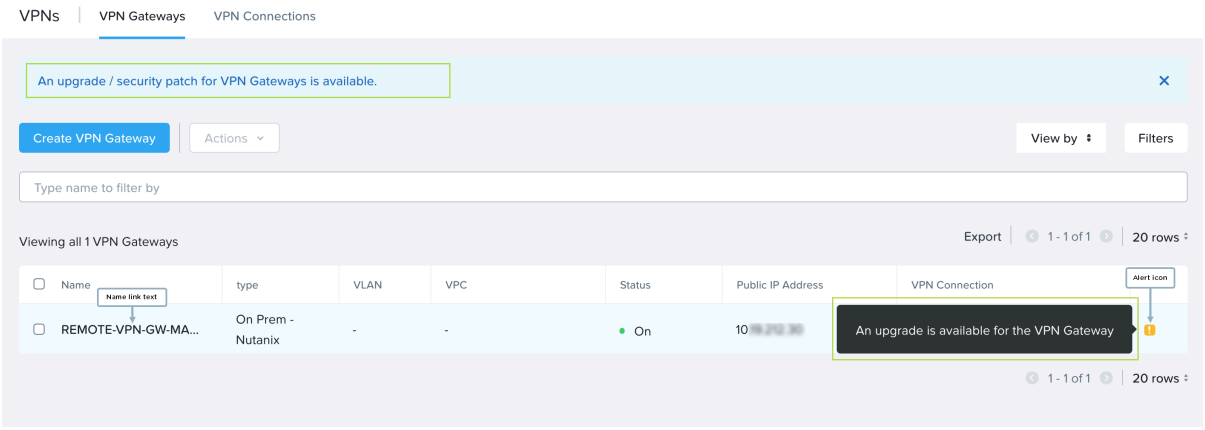


Figure 15: Upgrade Banner

For more information about the upgrade procedure, see Upgrading the Network Gateway on page 47.

Identifying the Gateway Version

About this task

To identify the current Nutanix Gateway version, do the following:

Procedure

- Log in to Prism Central.
- Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
  The **Connectivity** page opens displaying the **Gateways** tab.

- Click the Gateway name link text to open the Gateway details page.

  In the Gateway table, the Gateway name is a clickable link text.

  The **Gateway Version** is listed in the **Properties** widget.

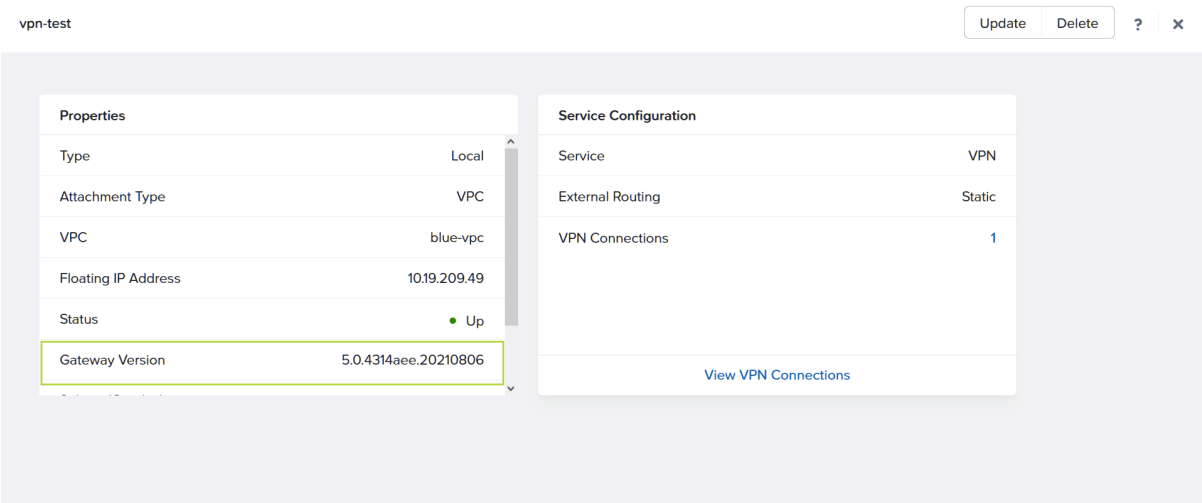


Figure 16: Gateway Version

Detecting Upgrades for Gateways

About this task

Prism Central can detect whether new Gateway upgrades are available, or not, for Nutanix Gateways using LCM. You can then install the upgrade.

Procedure

- Log in to Prism Central.
- Select the **Admin Center** application from the Application Switcher Function, and click **LCM** from the **Navigation Bar**.
  The **LCM** page opens displaying the **Best Practices** tab.
- Click the **Inventory** tab.
- Click **Perform Inventory**.

  Note:

  Nutanix recommends that you select **Enable LCM Auto Inventory** in the **LCM** page in Prism Central to continuously detect new Gateway upgrades as soon as they are available.

  The upgrade notification banner is displayed on the **Gateways** page.

Upgrading the Network Gateway

About this task

Perform upgrades of the Network Gateway using the respective Prism Central on which the Gateway is deployed.

To upgrade the Network Gateway, perform the following steps.

Procedure

1. Log in to Prism Central as an admin user.
2. Select the **Admin Center** application from the Application Switcher Function, and click **LCM** from the **Navigation Bar**.
   The **LCM** page opens displaying the **Best Practices** tab.
3. Click the **Inventory** tab.
4. Click **Perform Inventory**.
   The **Perform Inventory** window opens.
5. Click **Proceed**.

   When you click **Proceed**, the system scans the registered Prism Central cluster for software versions that are running currently. Then it checks for any available upgrades and displays the information on the **LCM** page under **Software**.

   > **Note:** Skip this step if you have enabled auto-inventory in the **LCM** page in Prism Central.

6. Click the **Updates** tab.
   The **Updates** page opens displaying the available software updates.
7. Select the checkbox associated with the Gateway version you want to upgrade and click **View Upgrade Plan**.
   The **Review Upgrade Plan** window opens.
8. Click **Apply 1 Updates**.

   LCM upgrades the gateway version. This process takes sometime.

Installing or Upgrading the Network Gateway in a Dark Site

Dark sites are primarily on-premises installations which do not have access to the internet. Such sites are disconnected from the internet for a range of reasons including security.

Before you begin

The Network Gateway is deployed for three types of connections:

- Virtual Private Networks as VPN Gateways
- Virtual Tunnel End Points as VTEP Gateways
- Border gateway Protocol sessions as BGP Gateways

Ensure that you complete the following tasks before you upgrade the Network Gateway in a dark site.

- Upgrade the LCM framework.
- Ensure that you have installed and prepared the LCM Dark Site server. See Setting up a Local Web Server in the *Life Cycle Manager Dark Site Guide*.
- Ensure that you have configured the **Dark Site (Local Web Server)** settings on the **LCM** > **Settings** page.
- See the *Release Notes* for the Network Gateway version compatible with the Network Controller and Prism Central version. To access the complete set of documentation, including the *Release Notes*, log on to Flow Virtual Networking.

- On the Flow Virtual Networking Downloads page, select **Network Gateway** in the component selection dropdown menu. Download the compatible Network Gateway bundle that you ascertained in the preceding task.

  Copy the **SHA256** value for the bundle.

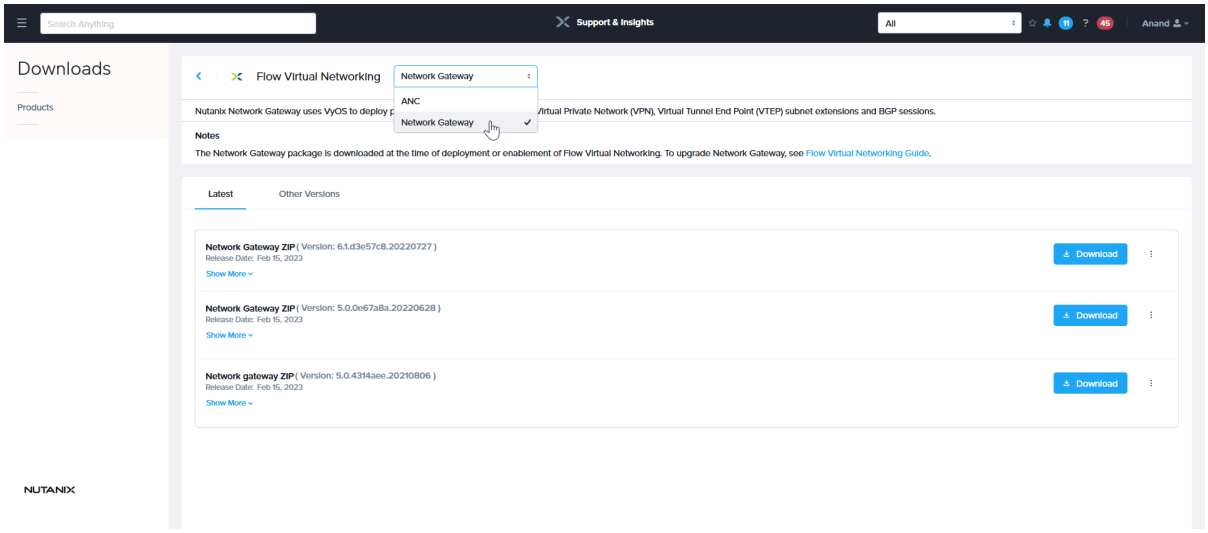


Figure 17: Flow Virtual Networking Download Portal - Network Gateway

- Place the extracted `vyos_<version>.qcow2` image and `vyos_<version>.cksum.txt` checksum files in the LCM Dark Site server. (See Setting up a Local Web Server in the *Life Cycle Manager Dark Site Guide*.)
- **Perform Inventory** on the **LCM** page in Prism Central **Admin Center** application.

  Tip:

  To go to the **LCM** page, select the **Admin Center** application from the Application Switcher Function, and click **LCM** from the **Navigation Bar**.

  In the **Updates** tab of the **LCM** page, **Network Gateway** now appears as an available update.

  See the Life Cycle Manager Dark Site Guide for more information about **Perform Inventory** and the **Updates** tab.

About this task

To install or upgrade the Network Gateway at such dark sites, you need to deploy the Network Gateway bundle at the site.

Procedure

- See KB-12393 and contact Nutanix Support to complete the Network Gateway version upgrade in the dark site.

NETWORK AND SECURITY ENTITIES

You can access the following networking and security entity items from the **Network and Security** entity of the **Infrastructure** application. For information about how to access the entity items available in **Network and Security** entity, see Application-specific Navigation Bar in the *Prism Central Infrastructure Guide*.

- **Subnets**: This page displays the subnets and the operations you can perform on subnets. For more information, see Subnets on page 50.
- **Virtual Private Clouds**: This page displays the VPCs and the operations you can perform on VPCs. For more information, see Virtual Private Clouds Summary View on page 55.
- **Floating IPs**: This page displays a list of floating IP addresses that you are using in the network. It allows you to request for floating IP addresses from the free pool of I addresses available to the clusters managed by the Prism Central instance. For more information, see Floating IPs Summary View on page 61.
- **Connectivity**: This page allows you to manage the following networking capabilities. For more information, see Connectivity on page 63.
  - **Gateways**: This page provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways. For more information, see Gateways Summary View on page 63.
  - **VPN Connections**: This page provides a list of VPN connections you have created and configured, and the operations you can perform on the VPN connections. For more information, see VPN Connections Summary View on page 66.
  - **Subnet Extensions**: This page provides a list of subnets that you have extended at the Layer 2 level using VPN (point-to-point over Nutanix VPN) or VTEP (point-to-multi-point including third party). For more information, see Subnet Extensions Summary View on page 72.
  - **BGP Sessions**: This page provides a list of BGP sessions you have created and configured, and the operations you can perform on the BGP sessions. For more information, see BGP Sessions Summary View on page 76.
- **Security Policies**: This page provides a list of security policies you configured using Flow Segmentation. For more information, see Security Policies on page 80.
- **Security Dashboard**: This page provides dynamic summary of the security posture across all registered clusters. For more information, see Security Dashboard on page 81.

For information about how to configure network connections, see Network Configuration.

Subnets (Overlay IP subnets), Virtual private clouds, floating IPs, and Connectivity are Flow virtual networking features. These features support flexible app-driven networking that focuses on VMs and applications instead of virtual LANs and network addresses. Flow virtual networking powers network virtualization to offer a seamless network experience with enhanced security. It is disabled by default. It is a software-defined network virtualization solution providing overlay capabilities for the on-premise AHV clusters.

Security policies drives the Flow Segmentation features for secure communications. For more information, see Flow Microsegmentation Guide.

Subnets

You can perform the following actions to manage a subnet from Prism Central.

- Creating a Subnet
- Updating a Subnet
- Deleting a subnet
- Creating a subnet extension
- Assigning a category value to a subnet
- Migrating VMs between VLAN and VPC networks

Subnets Summary View

The **Subnets** page displays the list of subnets across all the registered clusters.

To access the **Subnets** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   The **Subnets** page opens displaying the **List** tab. This tab provides information about all the subnets configured for the registered clusters.

The following table describes the fields that appear in the **Subnets** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable.

Table 2: Subnets – Field Description

Field	Description	Values
Name	Displays the subnet name.	(subnet name)
External Connectivity	Displays whether or not the subnet has external connectivity configured.	(Yes/No)
Type	Displays the subnet type.	VLAN or VLAN`Basic` or Overlay
VLAN ID	Displays the VLAN identification number.	(ID number)
VPC	Displays the name of the VPC in which the subnet is used.	(Name of VPC)
Virtual Switch	Displays the virtual switch that is configured for the VLAN you selected. The default value is the default virtual switch *`vs0`*. **Note:** The virtual switch name is displayed only if you add a VLAN ID in the VLAN ID field.	(virtual switch name)
IP Prefix	Displays the IPv4 address of the network with the prefix.	(IPv4 Address/Prefix)
Cluster	Displays the name of the cluster for which this subnet is configured.	(cluster name)

Field	Description	Values
Hypervisor	Displays the hypervisor that the subnet is hosted on.	(Hypervisor)

You can perform the following actions from the **Subnets** page:

- Click the name of a subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 53.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet on page 106 .
- Migrate VMs between VLAN network and VPC network by clicking **Migrate**. For more information, see Migration of VMs between VLAN Basic Subnet and VPC Subnets on page 88.
- Configure network connections for a cluster by clicking **Network Config**. For more information, see Network Configuration in the *Prism Central Infrastructure Guide*.
- Filter the subnets list based on a variety of parameter values using the **Filters** pane. For more information, see Filters Pane - Subnets page.
- Perform the following subnet-specific actions on a single or multiple subnets using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnets are selected.

Table 3: Subnet Actions

Action	Description
Update	Click this action to update the subnet. For more information, see Updating a Subnet on page 120.
Extend	Click this action to create a subnet extension. For more information, see Layer 2 Network Extension Over VPN on page 144.
Manage Categories	Click this action to associate the subnet with a category or change the categories that the subnet is associated with. For more information, see Assigning a Category in the *Prism Central Infrastructure Guide*.
Delete	Click this action to delete the subnet. For more information, see Deleting Subnets, Policies or Routes on page 122.

Filters Pane - Subnets page

You can filter the information in the **Subnets** page based on the following fields that are available in the **Filters** pane.

Table 4: Filter Pane Field Description - Subnets page

Field	Description	Values
Name	Filters based on the subnet name. It returns a list of subnets that satisfy the name condition/string.	(Subnet name string)
External Connectivity	Filters based on whether the subnet has external connectivity configured or not.	(Yes/No)

Field	Description	Values
Type	Filters based on the subnet type.	(VLAN/VLAN (External)/ Overlay
VLAN ID	Filters based on VLAN identification number.	(ID number)
VPC	Filters based on the name of the VPC in which the subnet is used.	(Name of VPC)
Cluster	Filters based on the name of the cluster for which this subnet is configured.	(cluster name)
Hypervisor	Filters based on the hypervisor that the subnet is hosted on.	ESXi/AHV/Hyper-V/XenServer/Mixed Hypervisor/Null Hypervisor

Subnet Details View

The Subnet details page consists of a dashboard that provides the detailed information about the subnet.

The details page has the **Summary**, and **Throughput** tabs.

To access the details page of an individual subnet:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   Prism Central displays the **Subnets** page that contains information about all the subnets configured for the registered clusters.
3. Click a subnet to open the details page of the subnet.

   The **Summary** tab opens displaying the detailed information about the subnet in widgets.

Summary Tab

The **Summary** tab provides detailed information about the subnet in widgets. A dash (-) is displayed in a field when a value is not available or applicable.

The **Summary** tab has the following widgets:

Widget Name	Information provided
Properties	Provides the following: • Type — Displays the type of network like VLAN or Overlay. • VLAN ID — Displays the VLAN ID. This parameter is displayed only for VLAN networks. • VPC — Displays the VPC name. This parameter is displayed only for Overlay networks. • Cluster — Displays the cluster that the VLAN network is configured on. This parameter is displayed only for VLAN networks. • IP Address Prefix — Displays the IP address prefix configured for the network. This parameter is displayed for both VLAN and Overlay networks.

Widget Name	Information provided
IP Address Pools	Provides the following: • The IP address Pool Range assigned to the network. • The total number of used and available IPs in the cluster. • Used IPs in Subnet — Displays the number of used IPs in the subnet. • Used IPs in Pools — Displays the number of used IPs in the pool. • Free IPs in Pools — Displays the number of free IPs in the pool. • Free IPs in Subnet — Displays the number of free IPs in the subnet.
Domain Settings	Provides the following DHCP settings configured for a VM in a subnet: • Domain Name Servers — Displays the total number of DNS IP addresses. • Domain Search — Displays the VLAN domain name. • Domain Name — Displays the domain name. • TFTP Server Name — Displays the name of the TFTP server where you host the host boot file. • Boot File Name — Displays the name of the boot file that the VMs need to download from the TFTP host server.

The **Summary** tab provides the following options, at the top of the page. For more information, see the *Subnet Actions* table in Subnets Summary View on page 51.

- **Update**
- **Extend**
- **Manage Categories**
- **Delete**

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet.

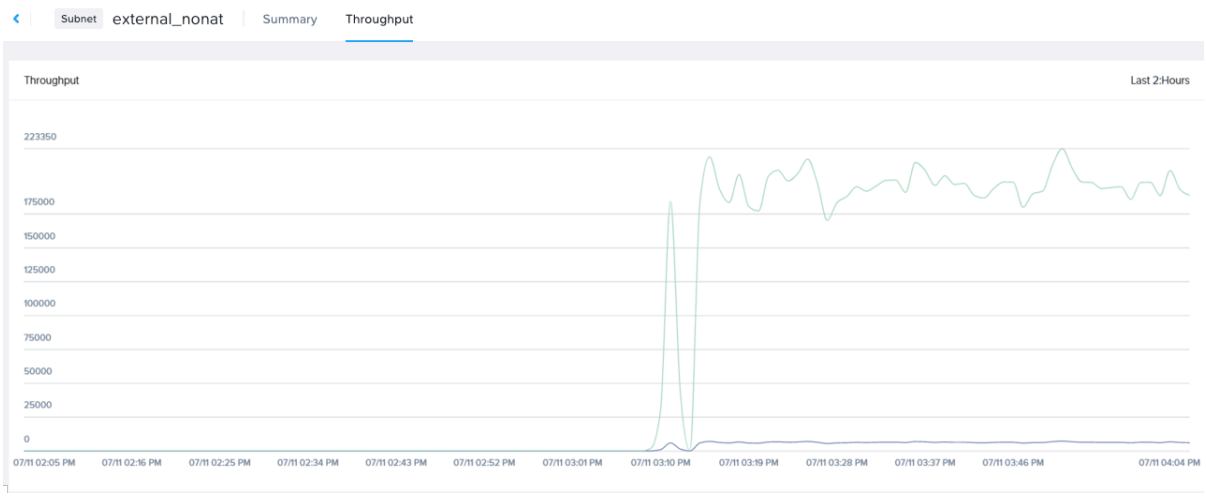


Figure 18: Subnet Details View - Throughput tab sample

Virtual Private Clouds

You can manage the virtual private clouds (VPCs) you have created and configured, from the **Virtual Private Clouds** page.

Virtual Private Clouds Summary View

The **Virtual Private Clouds** page displays the list of virtual private clouds (VPCs) across all the registered clusters.

To access the **Virtual Private Clouds** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   The **Virtual Private Clouds** page opens displaying the **List** tab. This tab provides a list of virtual private clouds you have created and configured, and the operations you can perform on them.

The following table describes the fields that appear in the **Virtual Private Clouds** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable.

Table 5: Virtual Private Clouds – Field Description

Field	Description
Name	Displays the name of the VPC. The **Name** of a VPC is suffixed with `Transit VPC` when you configure the VPC as a transit VPC.
Associated External Subnets	Displays the external subnet that the VPC is assigned to.
Categories	Displays the number of categories associated with the VPC.
Externally Routable IP Addresses	Displays the externally routable IP address.

Field	Description
Hypervisor	Displays the hypervisor that the VPC is hosted on.
Inter VN Traffic	Displays the traffic flowing between the virtual networks or VPCs.
Internet Traffic	Displays the traffic flowing to and from the Internet.
IPv4 Gateway	Displays the IPv4 gateway IP address.
IPv4/Subnet	Displays the IPv4 network IP with subnet prefix. For example, 10.20.30.0/24.
On-Prem Traffic	Displays the traffic flowing in the on-premises network.
VLAN ID	Displays the VLAN identification number. VLAN ID is a parameter used for Transit VPC networking in Nutanix Cloud Cluster with Microsoft Azure.

You can perform the following actions for the VPCs from the **Virtual Private Clouds** page:

- Click the name of a VPC to open the VPC details page, which displays the detailed information about the VPC. For more information, see Virtual Private Cloud Details View on page 56.
- Create a VPC by clicking **Create VPC**. For more information, see Creating Virtual Private Cloud on page 102.
- Update or delete an existing VPC using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPCs are selected. For more information, see Updating Virtual Private Cloud on page 118 or Deleting a Virtual Private Cloud on page 121.
- Filter the VPC list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Virtual Private Clouds Page.

Filters Pane - Virtual Private Clouds Page

You can filter the information in the **Virtual Private Clouds** page based on the following fields that are available in the **Filters** pane.

Table 6: Filter Pane Field Description - Virtual Private Clouds page

Field	Description	Values
Name	Filters based on the VPC name. It returns a list of IP addresses that satisfy the name condition/string.	(Virtual private cloud name string)
Associated External Subnets	Filters based on the external subnet that the VPC is assigned to.	(External Subnet)

Virtual Private Cloud Details View

The Virtual Private Cloud (VPC) details page consists of a dashboard that provides the detailed information about the VPC.

The details page has the **Summary**, **Subnets**, **Policies**, **Routes**, and **Metrics** tabs.

To access the details page of an individual VPC:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   Prism Central displays the **Virtual Private Clouds** page that contains information about all the VPCs configured for the registered clusters.
3. Click a VPC to open the details page of the VPC.

   The **Summary** tab opens displaying the detailed information about the VPC in widgets.

Summary Tab

The **Summary** tab provides detailed information about the VPC in widgets.

The **Summary** tab has the following widgets:

Widget Name	Information provided
External Connectivity	Provides the following: • Associated External Subnets — Displays the number of external subnets associated with the VPC. • Externally Routable IP Addresses — Displays the external routable IP addresses associated with the VPC.
Transit VPC	Displays **Yes** if the VPC is a Transit VPC. Displays **No** if the VPC is not a Transit VPC.
Domain Name Servers (DNS)	Displays the IP address or the FQDN of the DNS servers used by the VPC.
Associations	Provides the following: • Subnets (Overlay) — Displays the number of subnets associated with the VPC. • Policies — Displays the number of policies associated with the VPC. • Routes — Displays the number of routes associated with the VPC.
Floating IP Addresses	Provides the following: • Assigned Floating IPs — Displays the floating IP addresses assigned to the VPC. • Available Floating IPs — Displays the available floating IP addresses that can be assigned to the VPC.

Subnets Tab

The **Subnets** tab displays the list of subnets added to the VPC.

The following table describes the fields that appear in the **Subnets** tab.

Table 7: Subnets Tab – Field Description

Field	Description
Name	Displays the subnet name.
IP Range	Displays the IP address range configured for the subnet.

Field	Description
DHCP IP Pool	Displays the IP address pool range assigned to the subnet.
Default Gateway IP	Displays the IP address used as the default gateway by the entities in the subnet.
Actions	Action link for editing or deleting the subnet.

You can perform the following actions for a subnet from the **Subnets** tab:

- Click the name of the subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 53.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet on page 106.
- Update an existing subnet using the **Delete** option associated with the subnet. For more information, see Updating a Subnet on page 120.
- Delete an existing subnet using the **Delete** option associated with the subnet. For more information, see Deleting Subnets, Policies or Routes on page 122.

Policies Tab

The **Policies** tab displays information about the security-based traffic shaping policies you configured.

The following table describes the fields that appear in the **Policies** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable.

Table 8: Policies Tab – Field Description

Field	Description
Description	Displays the user-provided description of the policy.
Action	Displays the appropriate action for the implementation of the policy. • Permit: Permits traffic and services based on the parameters set. • Deny: Denies traffic and service based on the parameters set. • Re-route: Sends matching traffic to the next-hop IP address specified by the Reroute IP.
Priority	Displays the traffic priority.
Rule	Displays the **Permit** or **Deny** rule set for the priority.
Rule Type	Displays whether the rule is system generated or user defined.
Traffic	Displays the traffic type that the priority and rule should be applied to.
Virtual Network	Displays the ID of the subnet.
Source	Displays the source IP or subnet for which you want to manage traffic.

Field	Description
Destination	Displays the destination IP or subnet for which you want to set the priority.
Source Subnet	Displays the subnet IP and prefix designated as the source for the policy.
Destination Subnet	Displays the subnet IP and prefix designated as the destination for the policy.
Reroute Address	Displays the IP address to which the traffic is re-routed.
Bidirectional Policy	Displays whether the policy is bidirectional or not.
Protocol	Displays the type of protocol for which the policy is configured.
Protocol Number	Displays the protocol number for which the policy is configured.
ICMP Type	Displays the type of ICMP message associated with the policy.
ICMP Code	Displays the ICMP code of the policy.
Byte Count	Displays the total number of traffic bytes that matches the given policy. The count is updated periodically.
Packet Count	Displays the total number of traffic packets that matches the given policy. The count is updated periodically.

You can perform the following actions for a policy from the **Policies** tab:

- Create a policy by clicking **Create Policy**. For more information, see Creating a Policy on page 113.
- Perform the following actions using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more policies are selected.
  - **Update**: Update the policy. For more information, see Updating a Subnet on page 120.
  - **Delete**: Delete the policy. For more information, see Deleting Subnets, Policies or Routes on page 122.
  - **Clear Counters**: Reset the counters for the selected policy.
  - **Clear All Counters**: Reset the counters for all the policies.

Routes Tab

The **Routes** tab displays the list of static routes added to the VPC.

The following table describes the fields that appear in the **Routes** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable.

Table 9: Routes Tab – Field Description

Field	Description
Destination Prefix	Displays the IP address and prefix of the destination.

Field	Description
Next Hop	Displays the next hop network or subnet for the traffic exiting the VPC.
Priority	Displays the traffic priority.
Type	Displays the type of route, local or static.
Status	Displays the status of the route, whether it is active or not

You can perform the following actions for a route from the **Routes** tab:

- View routes based on pre-defined criteria or create a custom view.
- Perform the following actions using the **Manage Static Routes** option:
  - **Add Static Route**: Create a static route. For more information, see Creating Static Routes on page 117.
  - Update an existing static route. For more information, see Updating Static Routes on page 121.
  - Delete a static route. For more information, see Deleting Subnets, Policies or Routes on page 122.

Metrics Tab

The **Metrics** tab displays detailed information about the VPC metrics.

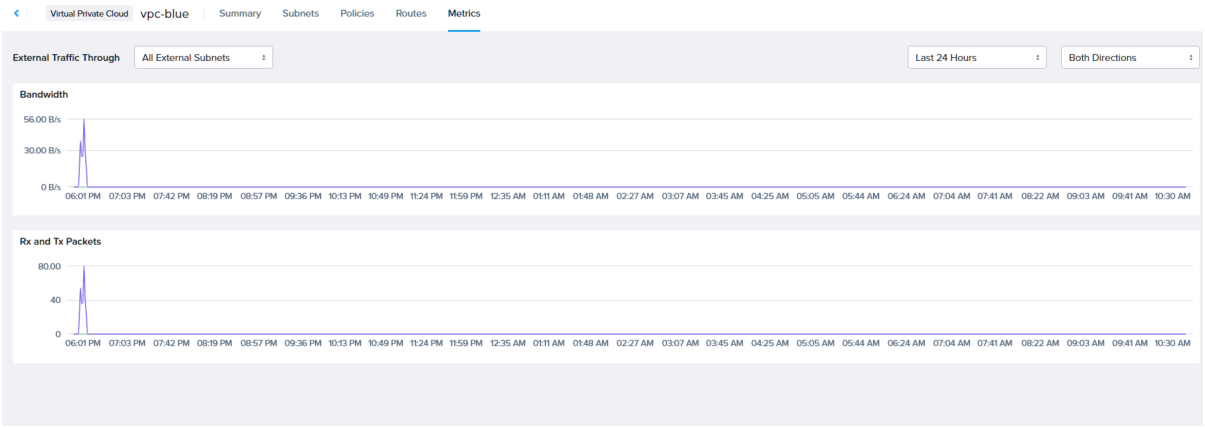


Figure 19: Metrics Tab

The following table describes the fields that appear in the **Metrics** tab.

Table 10: Metrics Tab – Field Description

Field	Description
External Traffic Through	Select **All External Networks** (default) or **(name_of_external_network_associated_with_the_VPC)** from the dropdown menu. The page displays the metrics based on your selection.

Field	Description
Last (time_period)	Select the period for which you want to display the metrics. The dropdown menu provides the following options: • **Last 24 Hours (default)** • **Last One Hour** • **Last Week**
Direction of traffic	Select the direction of traffic for which you want to display the metrics. The dropdown menu provides the following options: • **Both directions** (default) — Includes both directions, Ingress and Egress. • **Ingress** — Traffic entering the externally connected subnet. • **Egress** — Traffic leaving the externally connected subnet.
Bandwidth	Displays graphically the bandwidth utilization of the VPC on a timeline as set in the **Last (time_period)** parameter.
Rx and Tx Packets	Displays graphically the received and transmitted packet volume on a timeline as set in the **Last (time_period)** parameter.

Floating IPs

You can access the floating IP addresses you have created and configured, from the **Floating IPs** page.

For information about floating IP addresses and their role in flow virtual networking, see the *SNAT and Floating IP Address* section in Essential Concepts on page 12.

> **Note:** Floating IP addresses are not reachable (Pings fail) unless you associate them to primary or secondary IP addresses of VMs. For more information, see Assigning Secondary IP Addresses to Floating IPs on page 88.

Floating IPs Summary View

The **Floating IPs** page displays the list of floating IP addresses across all the registered clusters.

To access the **Floating IPs** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Floating IPs** from the **Navigation Bar**.

   The **Floating IPs** page opens displaying the **List** tab. This tab provides a list of floating IPs you have created and configured, and the operations you can perform on the IPs.

The following table describes the fields that appear in the **Floating IPs** page.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable.

Table 11: Floating IPs – Field Description

Parameter	Description	Values
Floating IP Address	Displays the floating IP address assigned.	(IP address)
External Subnet	Displays the name of the external subnet that the IP address is assigned to.	(Name of the assigned subnet)
Association Status	Displays the status of association between the IP address and the external subnet and VPC.	Associated
VPC	Displays the name of the VPC associated with the IP address.	(Name of the associated VPC)
VM Name	Displays the name of the VM associated with the IP address.	(Name of the assigned VM)
Private IP	Displays the private IP address assigned to the same VM. This private IP address is assigned from the internal private subnet that the network controller creates when you crate a network gateway.	(IP address)

You can perform the following actions for the floating IP addresses from the **Floating IPs** page:

- Request a floating IP address by clicking **Request Floating IP**. For more information, see Requesting Floating IPs on page 104.
- Update or delete an existing floating IP address using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more addresses are selected.
  - **Update**: Assign or change the assignment of the floating IP address. You can assign the floating IP address to a IP address such as a private IP address in a VPC or the primary IP address of a VM or a secondary IP address created on a VM.
  - **Delete**: Delete the floating IP address. The deleted IP address returns to the IP address pool as unused. Before you delete a floating IP address, ensure that it is not assigned to a private IP address or a VM. Change the assignment to `None` if it is already assigned, using the **Update** option.
- Filter the floating IP addresses list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Floating IPs Page.

Filters Pane - Floating IPs Page

You can filter the information in the **Floating IPs** page based on the following fields that are available in the **Filters** pane.

Table 12: Filter Pane Field Description - Floating IPs page

Field	Description	Values
Floating IP Address	Filters based on the floating IP address assigned. It returns a list of IP addresses that satisfy the string.	(Floating IP address)
External Subnet	Filters based on the external subnet that the IP address is assigned to.	(External Subnet)

Connectivity

You can access network gateways, VPN connections, subnet extensions, and BGP sessions from the `Connectivity` page.

To access the **Connectivity** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Connectivity** page opens displaying the **Gateways** tab. This tab provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways.

- To view the VPN connections, click the **VPN Connections** tab.
- To view the subnets extended across the clusters, click the **Subnet Extensions** tab.
- To view the BGP sessions created for the clusters, click the **BGP Sessions** tab.

Gateways Summary View

The **Gateways** page displays a list of gateways created for the clusters managed by Prism Central.

To access the **Gateways** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

The following table describes the fields that appear in the **Gateways** page.

Table 13: Gateway – Field Description

Parameter	Description	Values
Name	Displays the name of the gateway.	(Name of gateway)
Type	Displays the gateway type.	(Local or Remote)
Service	Displays the service that the gateway uses.	(VPN or VTEP)
Service IP	Displays the IP address used by the service.	(IP address)
Status	Displays the operational status of the gateway.	(Up or Down)
Attachment Type/Vendor	Displays the type of subnet associated with the gateway.	(VLAN or Overlay-VPC name)
Connections	Displays the number of service connections (such as VPN connections) configured and operational on the gateway.	(Number)

You can perform the following actions for a gateway from the **Gateways** page:

- Click the name of a gateway to open the gateway details page, which displays the detailed information about the gateway. For more information, see Gateway Details View on page 64.

- Create a local or remote gateway with VPN or VTEP service by clicking the **Create Gateway** dropdown menu. For more information, see Creating a Network Gateway on page 123.
- Update or delete an existing gateway using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more gateways are selected. For more information, see Updating a Network Gateway on page 133 or Deleting a Network Gateway on page 133.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Gateways Page.

Filters Pane - Gateways Page

You can filter the information in the **Gateways** page based on the following fields that are available in the **Filters** pane.

Table 14: Filter Pane Field Description - Gateways page

Field	Description	Values
Name	Filters based on the gateway name. It returns a list of gateways that satisfy the name condition/string.	(Gateway name string)
Service IP	Filters based on IP address used by the service.	(IP address)
Status	Filters based on the operational status of the gateway.	(Up or Down)

Gateway Details View

The **Summary** page of an individual gateway consists of a dashboard that provides the detailed information about the gateway.

To access the **Summary** page of an individual gateway:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways that you have created and configured.
3. Click a gateway to view the **Summary** page of the gateway.

The gateway **Summary** page has the following widgets:

Table 15: Gateway Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the gateway type.	(Local or Remote)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)

Parameter	Description	Values
Vendor (Applicable only if you select remote gateway)	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of Vendor)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address)
External IP (Applicable only if you select remote gateway)	Displays the IP address assigned to the remote gateway.	(IP Address that you assigned to the remote gateway.)
Status	Displays the operational status of the gateway.	(Up or Down)
Gateway Version	Displays the version of the Nutanix gateway appliance deployed.	(Version)
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Service Configuration widget		
Service	Displays the service used by the gateway.	(VPN or VTEP or BGP)
VPN Service Configuration		
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
VPN Connections	Displays the total number of VPN connections associated with the gateway.	(Number - actionable link. Click the link to open the VPN connection details page for the associated VPN connection.)
View VPN Connections	Click this link to open the VPN Connections tab.	-
VTEP Service Configuration		
VXLAN (UDP) Port	Displays the VXLAN (UDP) Port for the gateway.	(Number)
Subnet Extensions	Displays the total number of subnet extensions associated with the gateway.	(Number - actionable link. Click the link to open the subnet extensions details page for the associated subnet extension.)
View Subnet Extensions	Click this link to open the **Subnet Extensions** tab.	-
BGP Service Configuration		
ASN	Displays the ASN of the EBGP route.	(Number)

Parameter	Description	Values
BGP Sessions	Displays the total number of BGP sessions associated with the gateway.	(Number - actionable link. Click the link to open the BGP sessions details page for the associated BGP session.)
Serviced VPC	Displays VPC service used by the gateway.	(Name of VPC)
View BGP Sessions	Click this link to open the **BGP Sessions** tab.	-

You can perform the following actions for a gateway from the **Summary** tab:

- Update an existing gateway by clicking **Update**. For more information, see Updating a Network Gateway on page 133.
- Delete the gateway by clicking **Delete**. For more information, see Deleting a Network Gateway on page 133.

VPN Connections Summary View

The **VPN Connections** page displays a list of VPN connections created for the clusters managed by Prism Central.

A VPN connection represents the VPN IPSec tunnel established between local gateway and remote gateway. When you create a VPN connection, you must select two gateways between which you want to create the VPN connection.

To access the **VPN Connections** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.

The following table describes the fields that appear in the **VPN Connections** page.

Table 16: VPN Connections – Field Description

Parameter	Description	Values
Name	Displays the name of the connection.	(gateway name)
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)
Local Gateway	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Remote Gateway	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)

Parameter	Description	Values
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Nutanix Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)

You can perform the following actions for a VPN connection from the **VPN Connections** page:

- Click the name of a VPN connection to open the VPN connection details page, which displays the detailed information about the connection. For more information, see VPN Connection Details View on page 67.
- Create a VPN connection by clicking **Create VPN Connection**. For more information, see Creating a VPN Connection on page 137.
- Update or delete an existing VPN connection using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPN connections are selected. For more information, see Updating VPN Connection on page 139 or Deleting a VPN Connection on page 139.
- Filter the VPN connection list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - VPN Connections Page.

Filters Pane - VPN Connections Page

You can filter the information in the **VPN Connections** page based on the following fields that are available in the **Filters** pane.

Table 17: Filter Pane Field Description - VPN Connections page

Field	Description	Values
Name	Filters based on the VPN connection name. It returns a list of VPN connections that satisfy the name condition/string.	(VPN connection name string)
EBGP Status	Filters based on the status of the EBGP gateway connection.	(Established or Not Established)
IPSEC Status	Filters based on the connection status of IPSec tunnel.	(Connected or Disconnected)

VPN Connection Details View

The VPN Connection details page provides detailed information about a VPN connection.

The details page has the **Summary**, **Throughput**, **IPSec Logging**, and **Routing Protocol Logging** tabs.

To access the details page of an individual VPN connection:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Click the name of a VPN connection to open the details page of the connection.

   The **Summary** tab opens displaying the detailed information about the VPN connection in widgets.

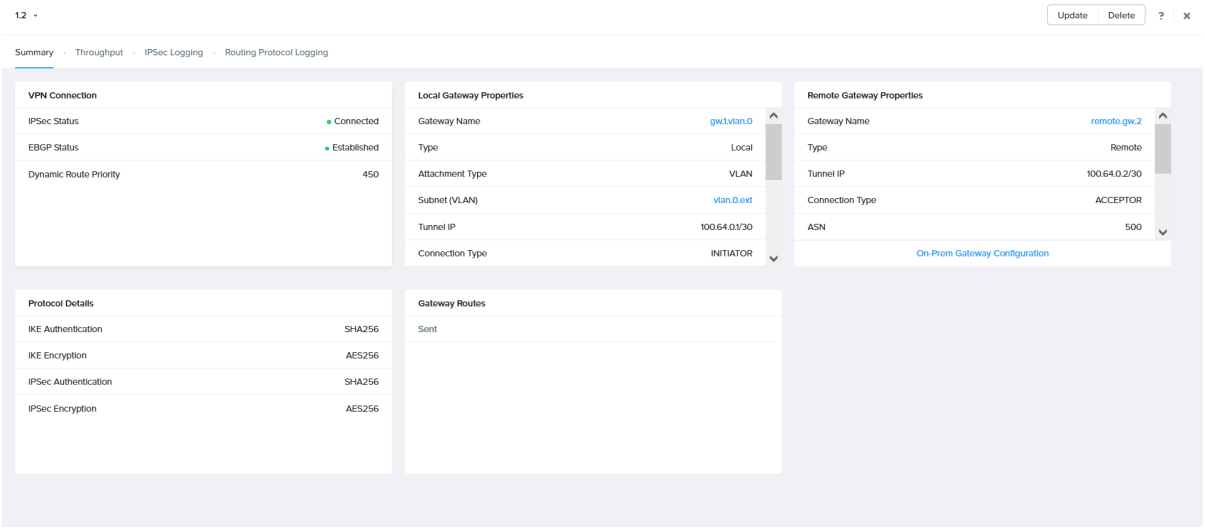


Figure 20: VPN Connection Details

Summary Tab

The **Summary** tab provides detailed information about a VPN connection in widgets.

The following table describes the fields that appear in the **Summary** tab.

Table 18: VPN Connection Summary Tab - Field Description

Parameter	Description	Values
VPN Connection widget		
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)

Parameter	Description	Values
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)
Local Gateway Properties widget		
Gateway Name	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Type	Displays the type of gateway.	(Local)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)
Tunnel IP	Displays the Tunnel IP address of the local gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address that you assigned to the local gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	(Up or Down)
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Remote Gateway Properties widget		
Gateway Name	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)

Parameter	Description	Values
Type	Displays the type of gateway.	(Remote)
Tunnel IP	Displays the Tunnel IP address of the remote gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
ASN	Displays the ASN of the EBGP route. This information is only displayed if you configured EBGP as the External Routing protocol.	(Number)
Vendor	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of vendor of gateway appliance)
External IP	Displays the IP address assigned to remote the gateway.	(IP Address that you assigned to the remote gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	-
Protocol Details widget		
Service	Displays the service used by the gateway.	(VPN or VTEP)
Gateway Routes widget	Displays the status of the routes used by the gateways.	(Sent)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a VPN connection. For the list of available parameters, see the *VPN Connection Summary Tab* table above.
- Update an existing VPN connection by clicking **Update**. For more information, see Updating VPN Connection on page 139.
- Delete an existing VPN connection by clicking **Delete**. For more information, see Deleting a VPN Connection on page 139.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the VPN connection.

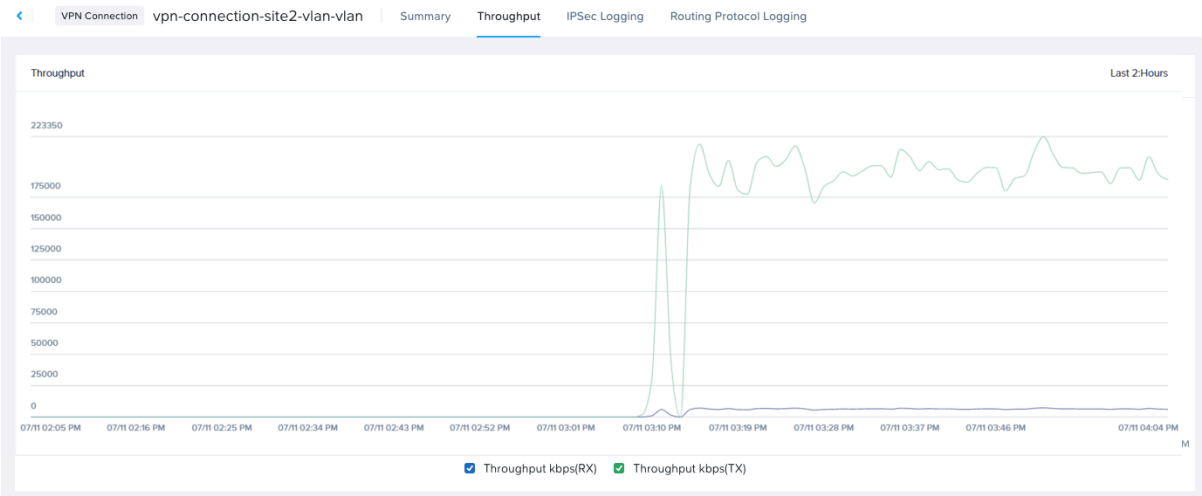


Figure 21: VPN Connections Details View - Throughput tab sample

IPSec Logging

The **IPSec Logging** tab provides logs for the IPSec tunnel.

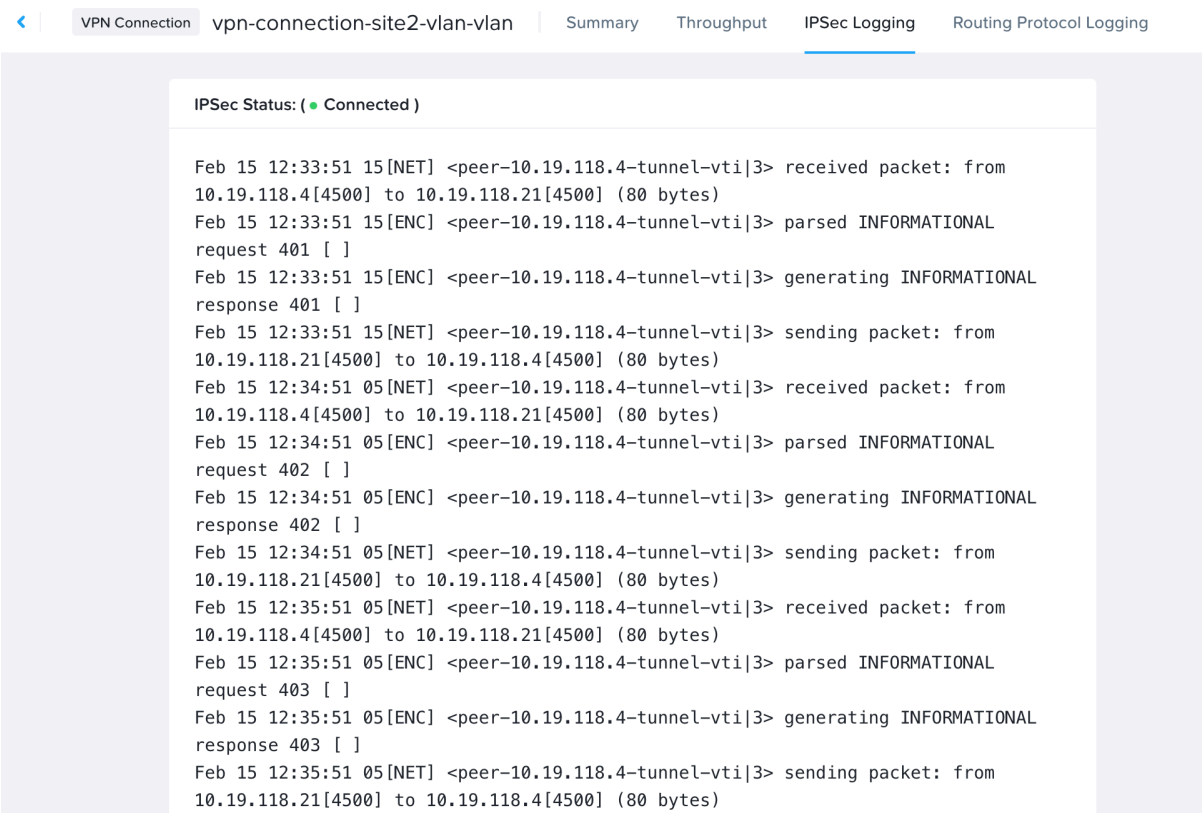


Figure 22: IPSec Logs tab sample for a VPN

Routing Protocol Logging

The **Routing Protocol Logging** tab provides logs for the routing protocol used in the VPN connection.

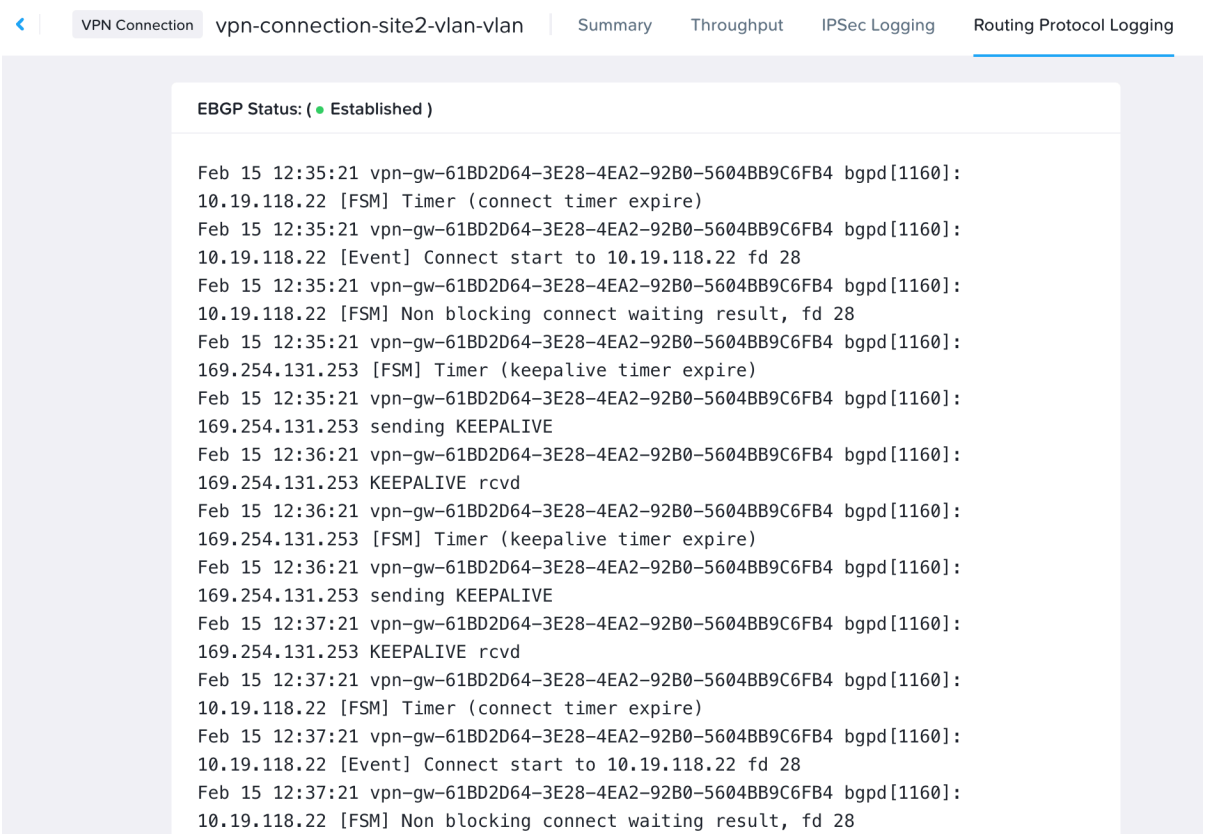


Figure 23: Routing Protocol Logs tab sample for a VPN

Subnet Extensions Summary View

The **Subnet Extensions** page displays a list of subnet extensions created for the clusters managed by Prism Central.

To access the **Subnet Extensions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

The following table describes the fields that appear in the **Subnet Extensions** page.

Table 19: Subnet Extensions – Field Description

Parameter	Description	Values
Name	Displays the name of the subnet extension.	(Name of subnet extension)
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)

Parameter	Description	Values
Extension Over	Displays the service that the subnet extension uses.	(VPN or VTEP)
Extension Uses	Displays the name of the local network gateway that the subnet extension uses.	(Name of local network gateway)
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Remote Site	Displays the name of the remote network gateway that the subnet extension uses.	(Name of remote network gateway)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Note: Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)

You can perform the following actions for a subnet extension from the **Subnet Extensions** page:

- Click the name of a subnet extension to open the subnet extension details page, which displays the detailed information about the extension. For more information, see Subnet Extension Details View on page 74.
- Extend a subnet **Across Availability Zones** or **To a Third Party Data Center** by clicking the **Create Subnet Extension** dropdown menu. You can extend a subnet using **VPN** or **VTEP** service. For more information, see Layer 2 Network Extension on page 141.
- Update or delete existing subnet extension using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnet extensions are selected. For more information, see Updating an Extended Subnet on page 161 or Removing an Extended Subnet on page 162.
- Filter the subnet extension list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Subnet Extensions Page.

Filters Pane - Subnet Extensions Page

You can filter the information in the **Subnet Extensions** page based on the following fields that are available in the **Filters** pane.

Table 20: Filter Pane Field Description - VPN Connections page

Field	Description	Values
Name	Filters based on the subnet extension name. It returns a list of subnet extensions that satisfy the name condition/string.	(Subnet extension name string)
Connection Status	Filters based on the status of the connection that is created by the subnet extension.	(Connected or Disconnected)

Field	Description	Values
Interface Status	Filters based on the status of the interface that is used by the subnet extension.	(Connected or Not Available)

Subnet Extension Details View

The Subnet Extension details page provides detailed information about a subnet extension.

The details page has the **Summary**, **Address Table**, and **Throughput** tabs.

To access the details page of an individual subnet extension:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.
3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.
4. Click a subnet extension to open the details page of the extension.

   The **Summary** tab opens displaying the detailed information about the extension in widgets.

Summary Tab

The **Summary** tab provides detailed information about the subnet extension in widgets.

The subnet extension **Summary** tab has the following widgets:

Table 21: Subnet Extension Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the subnet type.	(VLAN or Overlay)
VLAN ID	(For VLAN subnets only) Displays the VLAN ID of the VLAN subnet that is extended.	(VLAN ID number)
VPC	(For Overlay subnets only) Displays the name of the VPC subnet that is extended.	(Name of VPC)
Cluster	(For VLAN subnets only) Displays the cluster that the VLAN subnet belongs to.	(Name of cluster)
IP Address Prefix	Displays the network IP address with prefix, of the VLAN subnet that is extended.	(IP Address with prefix)
Virtual Switch	(For VLAN subnets only) Displays the virtual switch on which the VLAN subnet is configured.	(Virtual Switch name such as vs0 or vs1)
IP Address Pools widget		
Pool Range	Displays the range of IP addresses in the pool configured in the subnet that is extended.	(IP address range)

Parameter	Description	Values
(Interactive Graphic Pie Chart)	Displays a dynamic pie chart that displays the statistic you hover on. Displays the following IP address statistics outside the pie chart, that you can hover on: • Total number of IP addresses available. • Used IP addresses in the subnets • Used IP addresses in the IP address pools • Free IP addresses in the subnets • Free IP addresses in the IP address pools	(IP Address statistics)
Subnet Extension widget		
Subnet Extension (properties) - Common		
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Local IP Address	Displays the IP address that you entered in the **Local IP Address** field while creating the subnet extension.	(IP Address)
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Subnet Extension (properties) - (Only for **Across Availability Zones** type)		
Local Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the local AZ that is hosting the subnet that is extended.	(Name of the local Availability Zone)
Remote Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the remote AZ that the subnet is extended to.	(Name of the remote Availability Zone)
Remote Subnet	(Only for **Across Availability Zones** type) Displays the name of the remote subnet that the subnet extension connects to.	(Name of remote subnet)
Remote IP Address	(Only for **Across Availability Zones** type) Displays the IP address that you entered in the **Remote IP Address** field while creating the subnet extension.	(IP Address)
Subnet Extension (properties) - (Only for **To a Third Party Data Center** type)		

Parameter	Description	Values
Local Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the local gateway used for the subnet extension.	(Name of local gateway)
Remote Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the remote gateway used for the subnet extension.	(Name of remote gateway)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a subnet extension. For the list of available parameters, see the *Subnet Extension Details - Summary Tab Fields* table above.
- Update an existing subnet extension by clicking **Update**. For more information, see Updating an Extended Subnet on page 161.
- Delete an existing subnet extension by clicking **Delete**. For more information, see Removing an Extended Subnet on page 162.

Address Table Tab

The **Address Table** tab provides MAC Address information only when the subnet extension uses VTEP service. The tab provides the following information:

- **MAC Address**: This provides the MAC addresses of devices connected to the remote VTEP endpoint in the subnet extension.
- **Remote VTEP Endpoint**: This provides the IP address of the remote VTEP endpoint in the subnet extension.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet extension.

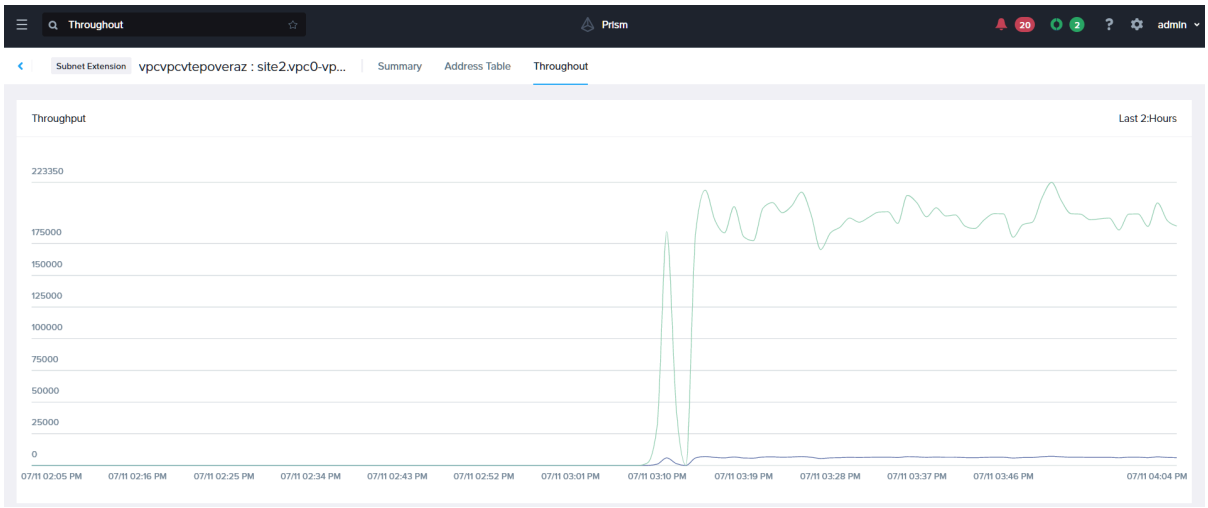


Figure 24: Subnet Extension Details View - Throughput tab sample for VTEP Extension

BGP Sessions Summary View

The **BGP Sessions** page displays a list of BGP sessions created for the clusters managed by Prism Central.

To access the **BGP Sessions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

The following table describes the fields that appear in the **BGP Sessions** page.

Table 22: BGP Sessions – Field Description

Parameter	Description	Values
Name	Displays the name of the BGP session.	(Name of BGP session)
Serviced VPC	Displays the name of the VPC that the BGP session services.	(Name of VPC)
Local Gateway	Displays the name of the local BGP gateway that the BGP session uses.	(Name of local BGP gateway)
Remote Gateway	Displays the name of the remote BGP gateway that the BGP session uses.	(Name of remote BGP gateway)
Session Status	Displays the status of the eBGP session. • Displays **Established** if the session is **Up**. • Displays **Active** when the network controller is attempting to establish the session.	**Established** or **Active**
Route Priority	Displays an integer number that denotes the route priority. When the route priority is assigned dynamically, then the network controller assigns integer numbers (usually between 600 and 800 starting with 700) in descending order with steps of 5. For example, the first session is assigned 700 as route priority and then when you create the second session, the controller assigns it a route priority of 695 and a third session is assigned 690. Greater the number, greater is the route priority. With dynamically assigned priority, the priority is assigned in the order of reducing priority to the order of BGP sessions created. The BGP session created first gets the highest priority 700, the second session get the second highest priority 695 and so on. You can manually assign a route priority as well by assigning any number between 300 and 900.	(Integer Number)

You can perform the following actions for a gateway from the **BGP Sessions** page:

- Click the name of a BGP session to open the details page, which displays the detailed information about the BGP session. For more information, see BGP Session Details View on page 78.
- Create a BGP session by clicking **Create BGP Session**. For more information, see Creating a BGP session on page 164.
- Update or delete an existing BGP session using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more BGP sessions are selected. For more information, see Updating a BGP session on page 167 or Deleting a BGP session on page 168.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - BGP Sessions Page.

Filters Pane - BGP Sessions Page

You can filter the information in the **BGP Sessions** page based on the following fields that are available in the **Filters** pane.

Table 23: Filter Pane Field Description - BGP Sessions page

Field	Description	Values
Name	Filters based on the BGP session name. It returns a list of BGP sessions that satisfy the name condition/ string.	(BGP session name string)
Session Status	Filters based on the status of the eBGP session.	(Established or Down)

BGP Session Details View

The BGP Session details page provides detailed information about a BGP session.

The details page has the **Summary**, **Routes**, and **BGP Logs** tabs.

To access the details page of an individual BGP session:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.
3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.
4. Click the name of a BGP session to open the details page of the session.

   The **Summary** tab opens displaying the detailed information about the BGP session in widgets.

Summary Tab

The **Summary** tab provides detailed information about the BGP session in widgets.

The BGP session **Summary** tab has the following widgets:

Table 24: BGP Session Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Session Status	Displays the overall status of the BGP session.	(Up or Down)
eBGP Status	Displays the eBGP status of the BGP session.	**Established** or **Active**
Route Priority	Displays an integer number that denotes the route priority. For more information about Route Priority, see BGP Sessions Summary View on page 76.	(Integer Number)
Local Gateway widget		
Local Gateway	Displays the name of the local BGP gateway.	(Name)
eBGP ASN	Displays the ASN of the local BGP gateway used by the session. It would be an integer number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)
Remote Gateway widget		
Remote Gateway	Displays the name of the remote BGP gateway.	(Name)
eBGP ASN	Displays the ASN of the remote BGP gateway used by the session. It would be an integer number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a BGP session. For the list of available parameters, see the *BGP Session Details - Summary Tab Fields* table above.
- Update an existing BGP session by clicking **Update**. For more information, see Updating a BGP session on page 167.
- Delete an existing BGP session by clicking **Delete**. For more information, see Deleting a BGP session on page 168.

Routes Tab

The **Routes** tab provides a list of the routes used by the BGP session with the corresponding **Next Hop** details. It has the following lists:

- **Advertised** (default): The **Routes** tab opens in the **Advertised** list. The **Advertised** list provides a list of the advertised routes with the corresponding **Next Hop** details.
- **Received**: This list provides list of the routes received from remote with the corresponding **Next Hop** details.

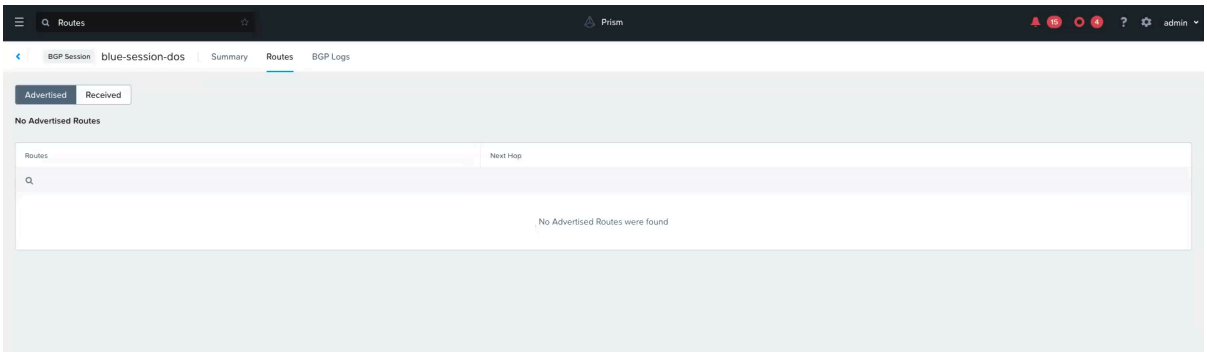


Figure 25: BGP Session Details View - Routes Advertised tab sample for a BGP session

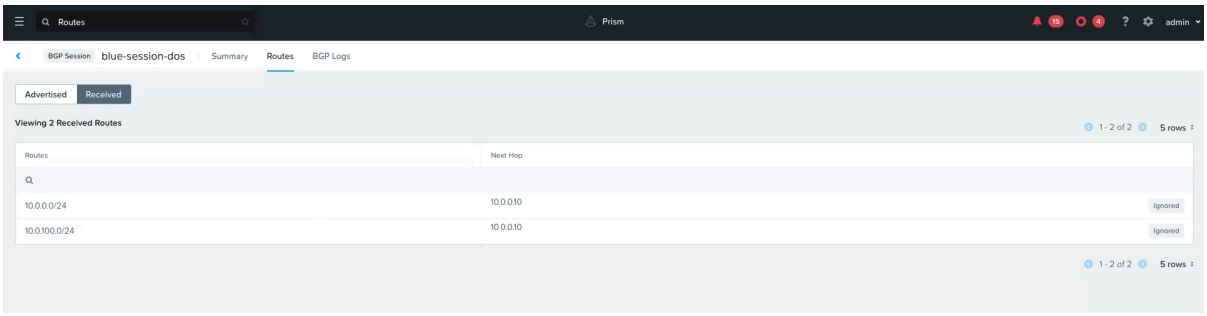


Figure 26: BGP Session Details View - Routes Received tab sample for a BGP session

BGP Logs Tab

The **BGP Logs** tab provides detailed live logs for the BGP session. This information can be very useful in monitoring and debugging a BGP session.

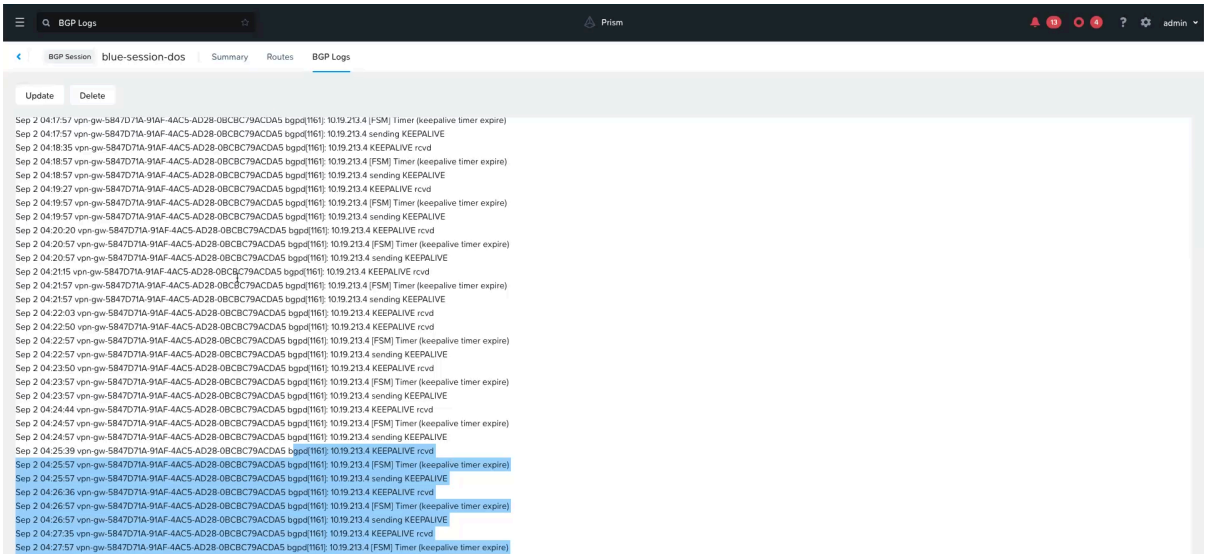


Figure 27: BGP Session Details View - BGP Logs tab sample for a BGP session

Security Policies

Security policies are defined using Nutanix Flow that provides a policy-driven security framework to inspect traffic within the data center.

For information about how to create and apply security policies, see Flow Microsegmentation Guide.

For information about how to view security policies in Prism Central, see Security Policies Summary View or Security Policy Details View.

Security Dashboard

The Security Dashboard provides dynamic summary of the security posture across all registered clusters. The Security Dashboard allows you to view the most critical security parameters like cluster-based issue summary, STIG policy compliance, security hardening, and identified vulnerabilities. For more information, see Security Dashboard in the *Nutanix Security Guide*.

VIRTUAL PRIVATE CLOUD

A Virtual Private Cloud (VPC) is an independent and isolated IP address space that functions as a logically isolated virtual network. A VPC could be made up of one or more subnets that are connected through a logical or virtual router. The IP addresses within a VPC must be unique. However, IP addresses may overlap across VPCs. As VPCs are provisioned on top of another IP-based infrastructure (connecting AHV nodes), they are often referred to as the overlay networks. Tenants may spin up VMs and connect them to one or more subnets within a VPC.

Virtual Private Cloud (VPC) is a virtualized network of resources that are specifically isolated from the rest of the resource pool. VPC allows you to manage the isolated and secure virtual network with enhanced automation and scaling. The isolation is done using network namespace techniques like IP-based subnets or VLAN based networking.

AHV provides the framework to deploy VPC on on-premises clusters using the following.

- Advanced Networking subnets and DHCP management
- Multiple uplink and bridge management via virtual switch (VS)
- Virtual Private Network (VPN) gateways and connections

Flow Virtual Networking simplifies the deployment and configuration of overlay-based VPCs. It allows you to quickly:

- Create, update and delete VPCs.
- Create, update and delete subnets within VPCs.

  Note: Create subnets as necessary when you create VPCs.

- Add network security policies and services.
- Configure hybrid cloud connectivity with VPNs.

This section covers the concepts and procedures necessary to implement VPCs in the network.

VPC Workflow

You can deploy the following types virtual private clouds (VPCs) on a Nutanix cluster infrastructure to manage the internal and external networking requirements using Flow Virtual Networking.

- *VPCs*: These are the VPCs that you create to isolate the groups of entities using overlay networks or subnets. This is the default VPC type. See *VPC* in Essential Concepts on page 12.
- *Transit VPC*: This is a *hub* VPC that VPCs connect to using one or two (NAT or No-NAT) external networks as spokes, in a a hub-and-spoke architecture to simplify the North-South connectivity. See *Transit VPC* in Essential Concepts on page 12.

The workflow to create a complete network based on VPC is described below.

1. Create a VPC or a transit VPC: See Creating Virtual Private Cloud on page 102.
2. Update an existing VPC or transit VPC: See Updating Virtual Private Cloud on page 118.
3. Add subnets to the VPC: See Creating a Subnet on page 106 to create a Subnet.
4. Update an existing subnet: See Updating a Subnet on page 120 to update a subnet.
5. Attach the subnet to VMs to VPCs: See Attaching a Subnet to a Virtual Machine on page 112.

VM IP Address Management

Primary Address

The primary IP address is assigned to a VM during initialization when the cluster provides any virtual NIC (NIC) to a VM.

- Select `Assign Static IP` as the **Assignment Type** to add a static IP address as primary IP address of the VM, when you attach a subnet to a VM.
- Select `Assign with DHCP` as the **Assignment Type** to allow DHCP to dynamically assign an IP address to the VM.
- Select `No Private IP` as the **Assignment Type** if you do not want to assign an IP address to the vNIC of the VM.

For more information about attaching a subnet to a VM, see Creating a VM through Prism Central (AHV) in the *Prism Central Infrastructure Guide*.

Secondary IP Addresses (Overlay Networks only)

For your deployment, you may need to configure multiple (static) IP addresses to a single NIC. These IP addresses (other than the primary IP address) are secondary IP addresses. A secondary IP address can be permanently associated with a specific NIC or be changed to any other NIC. The NIC ownership of a secondary IP address is important for security routing policies.

> **Note:** You can configure secondary IP addresses only for VMs in an Overlay network.

You can configure secondary IP addresses to a NIC when you want to:

- Associate multiple floating IP addresses with one VM without creating multiple NICs (each with one primary IP address) for the VM. You can assign one floating IP address to one secondary IP address that you create for the single NIC. For information, see Requesting Floating IPs on page 104.
- Run appliances, such as load balancers, that have multiple IP addresses on each interface.
- Host applications in a High Availability (HA) configuration where the ownership of IP address moves from the active entity to the standby entity when the active entity goes down.
- Host applications in a clustered configuration where the ownership of IP address follows the leader.
- Host Nutanix Files service in a VPC as a case of clustered application.

> **Note:**
>
> In applications that use secondary IP addresses as virtual IP addresses and the NIC ownership of the secondary IP address changes dynamically from one NIC to another, configure the application to incorporate the ownership change in its settings or configuration. If the applications do not incorporate these ownership changes, the VPCs configured for such applications fail.

For information about configuring secondary IP addresses, see Creating Secondary IP Addresses on page 84.

IP Address Information

You can view the IP addresses configured on a VM by clicking the **See More** link in the `IP Address` column in the VM details view to open the **IP Address Information** box.

> **Note:** The **See More** link in the `IP Address` column in the VM details view and the **IP Address Information** box are available only if the VM has any secondary IP addresses configured.

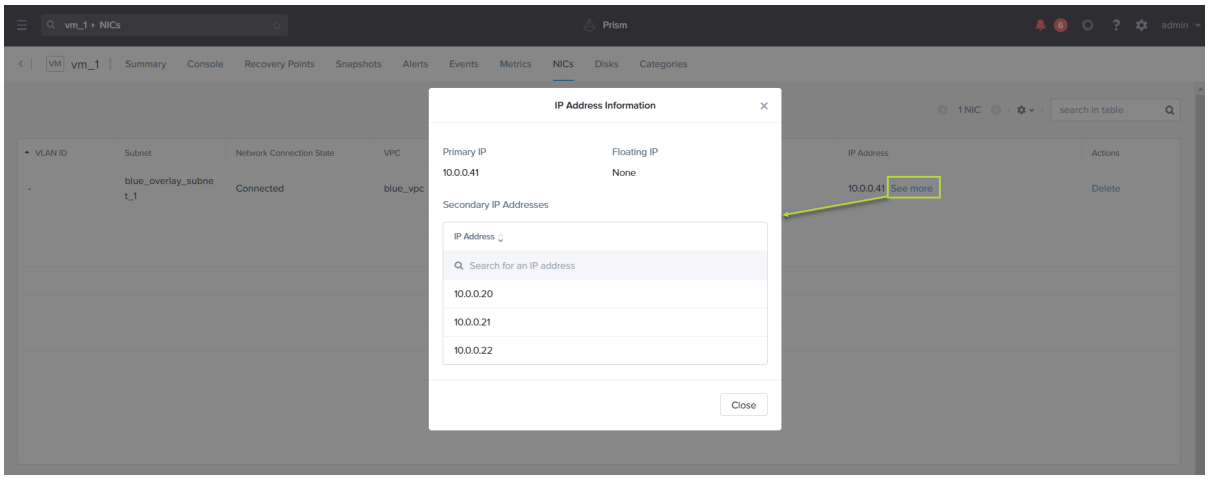


Figure 28: IP Address Information

Creating Secondary IP Addresses

You can assign multiple secondary IP addresses to a single vNIC.

About this task

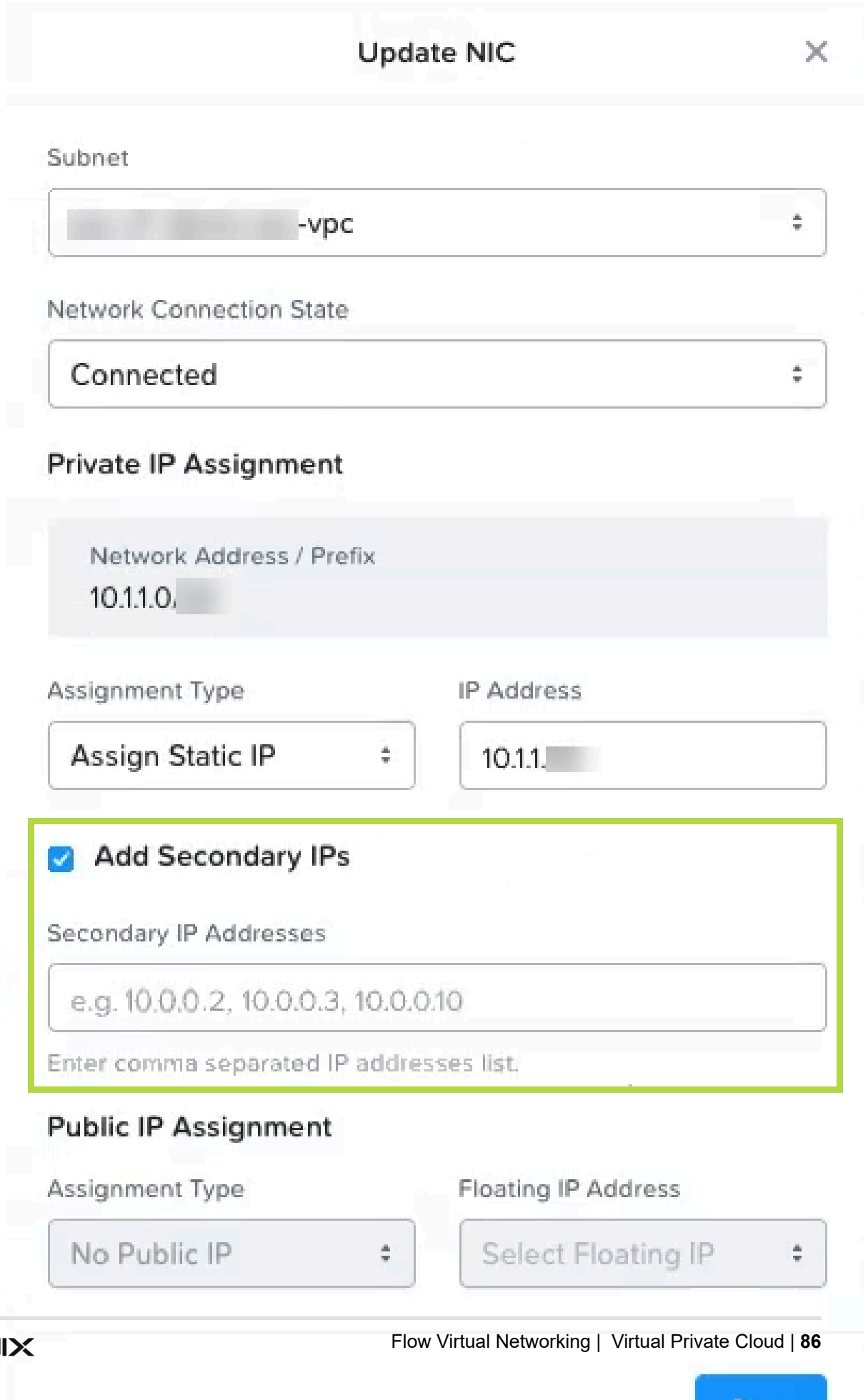
You can add multiple secondary IP addresses to the vNIC configured on a VM. Add the secondary IP addresses to the vNIC in the **Create VM** or the **Update VM** page.

Perform the following steps to assign a secondary IP address to a vNIC configured on a VM.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**.
   The **VMs** page opens displaying the **List** tab.
3. Select the checkbox associated with the VM that contains the vNIC for which you want to add a secondary IP address.
4. Click **Update** from the **Actions** dropdown menu.
   The **Update VM** page opens displaying the **Configuration** tab.
5. Click **Next**.
   The **Resources** tab opens.
6. Go to the **Networks** section.
7. Click the **Edit** icon for the subnet that you want to add the secondary IP addresses from.
   The **Update NIC** window opens.

8. Check the **Add Secondary IPs** checkbox in the **Update NIC** window.


Update NIC
Subnet
-vpc
Network Connection State
Connected
Private IP Assignment
Network Address / Prefix
10.1.1.0/
Assignment Type
Assign Static IP
IP Address
10.1.1.
Add Secondary IPs
Secondary IP Addresses
e.g. 10.0.0.2, 10.0.0.3, 10.0.0.10
Enter comma separated IP addresses list.
Public IP Assignment
Assignment Type
No Public IP
Floating IP Address
Select Floating IP

9. Add a comma-separated list of the secondary IP addresses that you want to add to the vNIC of the VM.

   Note:

   Ensure that the secondary IP addresses are within the same subnet that the primary IP address of the NIC is from. The subnets are displayed in the **Private IP Assignment** section in the **Update NIC** window.

   Ensure that the secondary IP address is not the same as the IP address provided in the **Private IP Assignment** field.

10. Click **Save**.

11. Click **Next** on the **Resources** and the **Management** tabs of the **Update VM** page.

    If you need to make any other changes on the **Resources** and the **Management** tabs for any configurations other than adding secondary IP addresses, make the changes and then click **Next** on these tabs.

12. Click **Launch VM** on the **Review** tab after you review.

What to do next

You can view the secondary IP addresses configured on the VM in the **IP Address Information** box.

Assigning Secondary IP Addresses to Interfaces

Assign the secondary IP addresses to interfaces or subinterfaces on the VM.

About this task

Perform the following steps to assign the secondary IP addresses to virtual interfaces on the VM.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**.
   The **VMs** page opens displaying the **List** tab.

3. Click the target VM for which you want to assign a secondary IP address.
   The VM details page opens displaying the **Summary** tab.

4. Click the **Console** tab.

5. Log in as a root user.

6. Run the `ifconfig` command as follows:

   ```
   root@host$ ifconfig <interface> <secondary ip address> <network mask>
   ```

   Provide the following in the command:

Parameter	Description
<interface>	The interface of the VM such as eth0. You can provide subinterfaces such as eth0:1 and eth0:2.

Parameter	Description
<secondary IP address>	The secondary IP address that you created and want to associate with the interface.
<network mask>	The network mask that is an expansion of the network prefix of the network that the secondary IP address belongs to. For example, if the secondary IP address belongs to 10.0.0.0/24 then the network mask is 255.255.255.0.

7. Repeat the aforementioned steps for all the secondary IP addresses you want to associate with interfaces on the VM.
8. Exit from the Console.

Assigning Secondary IP Addresses to Floating IPs

Assign the secondary IP addresses to floating IP addresses on the VM.

About this task

After you assign secondary IP addresses to interfaces or subinterfaces on the VM, you can assign the secondary IP addresses to floating IP addresses that may be used for external connectivity.

Perform the following steps to assign a secondary IP address to floating IPs.

Procedure

- Log in to Prism Central.
- Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Floating IPs** from the **Navigation Bar**.
  The **Floating IPs** page opens displaying the **List** tab.
- Perform either of the following:
  - » Click **Request Floating IP**. In the **Assign Floating IPs** section of the **Request Floating IP** window, assign floating IP addresses.

    To assign floating IP addresses while requesting for them, you must have the secondary IP addresses configured and ready when you are requesting the floating IP addresses.
  - » In the **Floating IPs** page, select the checkbox associated with the floating IP address you want to assign. Click the **Update** option in the **Actions** dropdown menu.

    Assign the secondary IP addresses you configured to the floating IP addresses you have.

VM and Network Migration

Flow Virtual Networking supports the following types of migrations:

- Migration of VMs between VLAN Basic Subnet and VPC Subnets on page 88
- Migration of VLAN Basic Subnets on page 97

Migration of VMs between VLAN Basic Subnet and VPC Subnets

You can migrate VMs networked in VLAN Basic Subnets to Flow Virtual Networking VPCs. The VMs networked using VLAN Basic Subnets are associated with categories. When you migrate the VLAN Basic Subnets to VPC subnets, the category associations are persisted.

Note: Flow Virtual Networking supports migration of VMs protected by protection policies from VLAN Basic networks to VPC subnets.

Migration Types

There are two types of migrations that you can select in the migration workflow.

- **Cold Migration**. For this type of migration, the incoming and outgoing connection configurations are not preserved. External connectivity for the subnet is irrelevant since the connections are preserved.

  If the source subnet is a managed subnet, the network ID and gateway is automatically populated based on the cluster and subnet selection.

  If the source subnet is not a managed subnet, specify the network ID and the gateway.

  In both the above cases, the network ID and gateway of both the source and target networks must be the same. For example, if the network ID and gateway of the source are `10.10.10.0/32` and `10.10.10.1/32` then the target subnet must have `10.10.10.0/32` and `10.10.10.1/32` as the network ID and gateway. If the network ID and gateway are not the same then Prism central displays an error.

- **Live Migration without incoming connections**. For this type of migration, only outgoing connection configurations for the migrating VMs are preserved. Other considerations for this type of migration are:

  - You need subnet extension with Layer 2 connectivity during and after migration. This subnet extension is required to be established between the two subnets that you are migrating from and to.

    For more information about virtually extending a subnet at layer 2, see Layer 2 Network Extension on page 141.

  - The external connection for the VPC must have NAT.

  - The network ID and gateway of both the source and target networks must be the same. For example, if the network ID and gateway of the source are `10.10.10.0/32` and `10.10.10.1/32` then the target subnet must have `10.10.10.0/32` and `10.10.10.1/32` as the network ID and gateway. If the network ID and gateway are not the same then Prism central displays an error.

Conditions for Migration

You will be unable to select some VMs for migration in the migration workflow because the selection button for those VMs are unavailable. When you hover on the selection button of such a VM, the pop-up message provides the reason for the unavailability of the VM for migration.

- You cannot migrate a VM with multiple vNIC. This is because a VM with vNICs in Acropolis and Flow Virtual Networking at the same time are not supported for migration. Therefore, ensure that the VM you want to migrate between VLANs and VPCs do not have multiple vNIC.
- You cannot migrate a VM which has a single vNIC but the vNIC has multiple IP addresses. Therefore, ensure that the VM you want to migrate between VLANs and VPCs has a single vNIC with a single IP address.
- You cannot perform cross-cluster live migration of VMs which are attached to Flow Network Security policies.
- Ensure that the IP addresses of the migrating VMs does not conflict with the IP addresses used by the VMs existing in the destination subnet. If you migrate a VM with conflicting IP address (in other words, an IP address that already belongs to another VM in the destination subnet) then an error is displayed and the migration fails for that VM.

Migrating VMs from VLAN Basic Subnets

About this task

You must have a **Super Admin** or **Prism Admin** access to migrate VMs from VLAN backed subnets to VPCs. If you are a user without **Super Admin** or **Prism Admin** level permissions, the **Migrate** button on the **Subnets** is unavailable.

You can migrate VLAN backed subnets on the **Subnets** page. Go to the **Subnets** page by clicking **Network & Security** > **Subnets**.

To migrate VLAN backed subnets to Flow Virtual Networking, on the **Subnets** dashboard, do the following.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   The **Subnets** page opens displaying the *List* tab.
3. Select the VLAN subnet that you want to migrate. Click **Migrate**.
4. On the **Migrate** page, do the following.
   a. Select `VLAN Basic Subnet` in the **Migrate From** field.
   b. Select `Overlay Subnet` in the **Migrate To** field.
   c. Click **Proceed**.

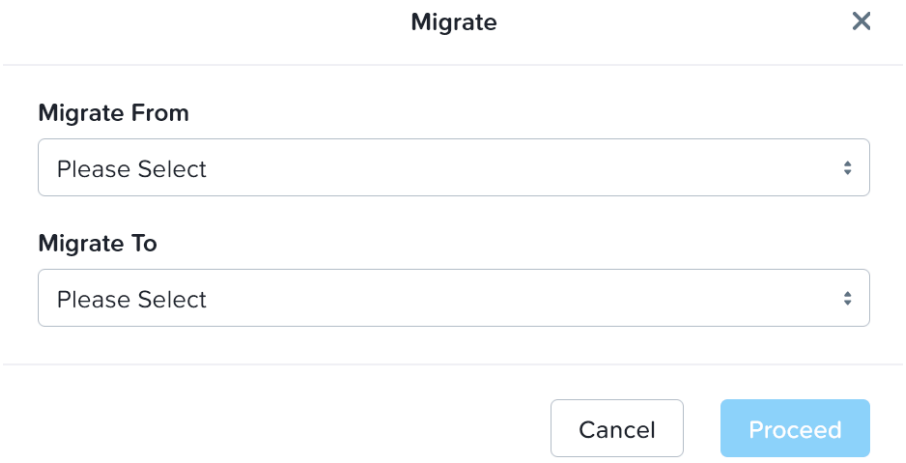


Figure 30:

5. On the **Migrate VMs between VLAN Network and VPC Network** page, select the **Migration Type** from the drop-down list.

   You can select one of the following migration types:

   - **Cold Migration**. For this type of migration, the incoming and outgoing connection configurations are not preserved.
   - **Live Migration without incoming connections**. For this type of migration, only outgoing connection configurations for the migrating VMs are preserved.

   For more information, see Migration of VMs between VLAN Basic Subnet and VPC Subnets on page 88.

6. To migrate VMs from VLAN to VPC, complete the configurations provided in the table and click **Next**.

   You can also migrate VMs from VPC to VLAN.

   Note: Click **Swap Source and Destination** link to toggle between **Migrate VMs from VLAN to VPC** and **Migrate VMs from VPC to VLAN**.

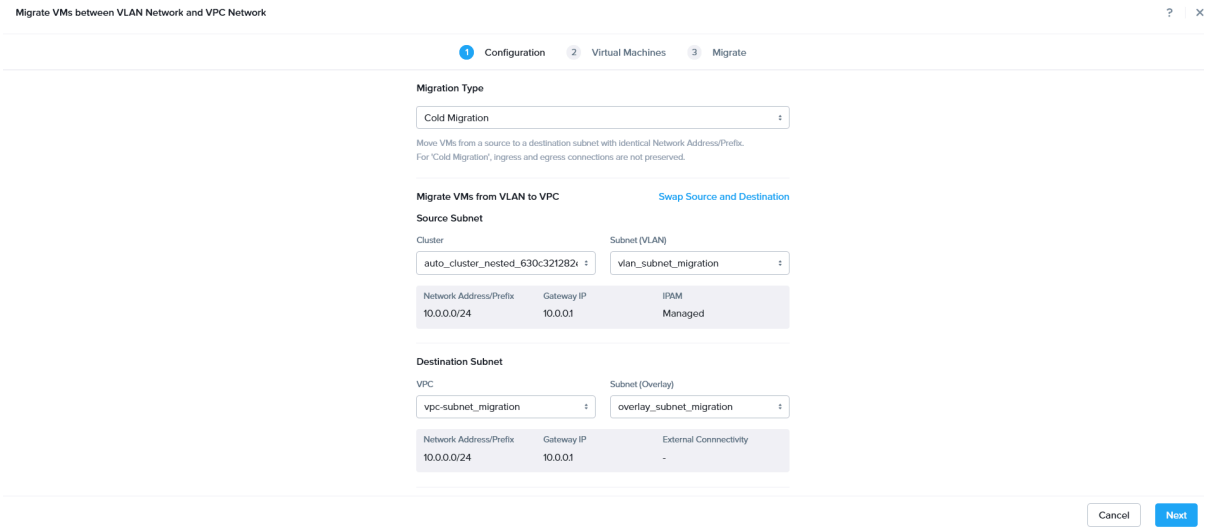


Figure 31: Migrate VMs from VLAN Network to VPC Network - Configuration

Table 25: Parameters for Migrate VMs from VLAN to VPC

Parameters	Action	Description and Value
Source Subnet		
Cluster	Select the source cluster where the VM is located.	Name of the source cluster. (String)
Subnet (VLAN)	Select the source VLAN that networks the VM to be migrated.	Name of the source VLAN subnet. (String)
Network Address/Prefix	Enter (for unmanaged networks) the network IP address with prefix in CIDR notation. When you select a managed subnet in **Subnet (VLAN)** the **Network Address/ Prefix**	IP address of the source subnet. Use CIDR notation. For example, `10.10.10.0/32`.

Parameters	Action	Description and Value
Gateway IP	Enter (for unmanaged networks) the Gateway IP address with prefix in CIDR notation. When you select a managed subnet in **Subnet (VLAN)** the **Gateway IP** value is automatically populated.	Gateway IP address of the source subnet. Use CIDR notation. For example, `10.10.10.1/32`.
IPAM (Display only)	The IPAM status is displayed when you select a managed subnet in the **Subnet (VLAN)** parameter.	Displays **Managed**
Destination Subnet		
VPC	Select the VPC that you want to migrate the VM to.	VPC name (String)
Subnet (Overlay)	Select the Overlay subnet in the selected VPC that you want to migrate the VM to.	Name of the Overlay subnet
Network Address/Prefix	Enter (for unmanaged networks) the network IP address with prefix in CIDR notation. When you select a managed subnet in **Subnet (VLAN)** the **Network Address/ Prefix**	IP address of the source subnet. Use CIDR notation. For example, `10.10.10.0/32`.
Gateway IP	Enter (for unmanaged networks) the Gateway IP address with prefix in CIDR notation. When you select a managed subnet in **Subnet (VLAN)** the **Gateway IP** value is automatically populated.	Gateway IP address of the source subnet. Use CIDR notation. For example, `10.10.10.1/32`.
IPAM (Display only)	The IPAM status is displayed when you select a managed subnet in the **Subnet (VLAN)** parameter.	Displays **Managed**

For **Migrate VMs from VPC to VLAN** the configurations provided in the table in with the following differences.

- For **Source Subnet**, provide the VPC parameters which is the source.

- For **Destination Subnet**, provide the VLAN parameters which is the source.

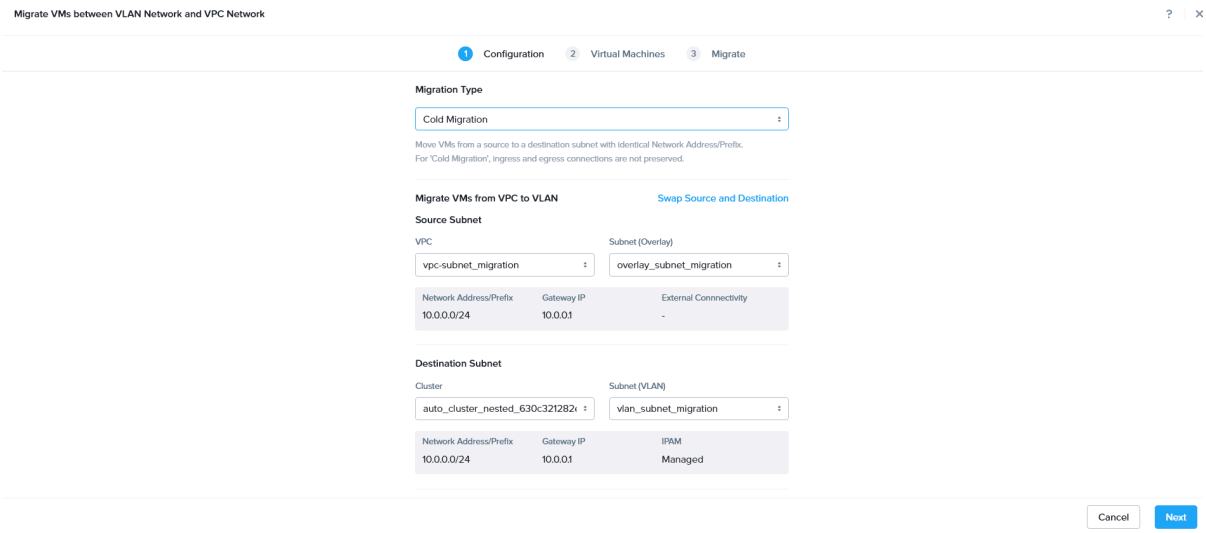


Figure 32: Migrate VMs from VPC Network to VLAN - Configuration

7. In the **Virtual Machines** tab, select the VMs you want to migrate in the **Source** side of the tab and click **Add**.

   Select as many subnets as required before you click **Add**.

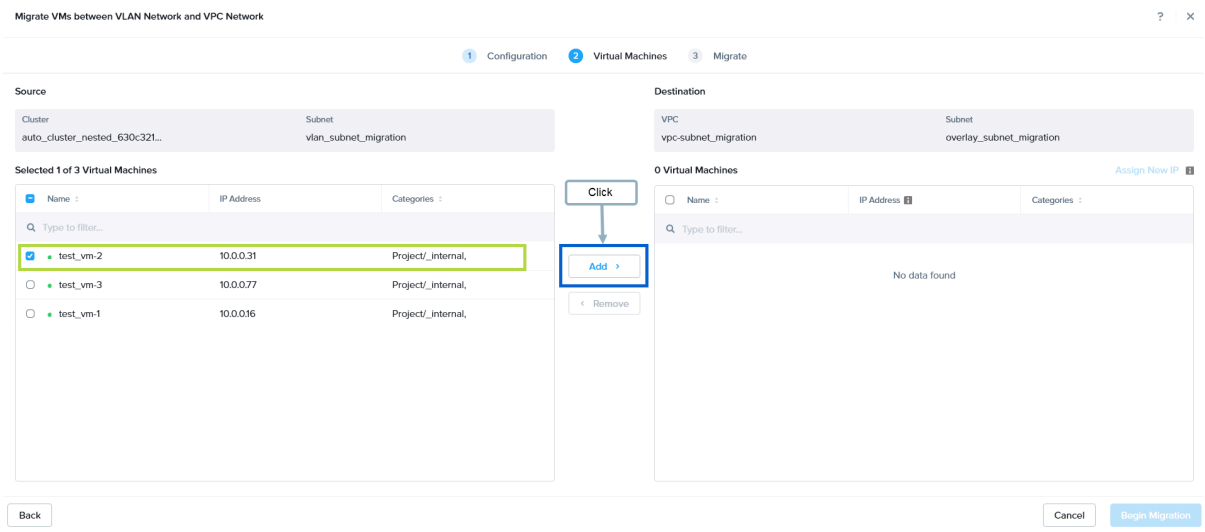


Figure 33: Migrate VMs from VLAN to VPC - Virtual Machines

For **Migrate VMs from VPC to VLAN**, the **Source** and destination subnets are reversed.

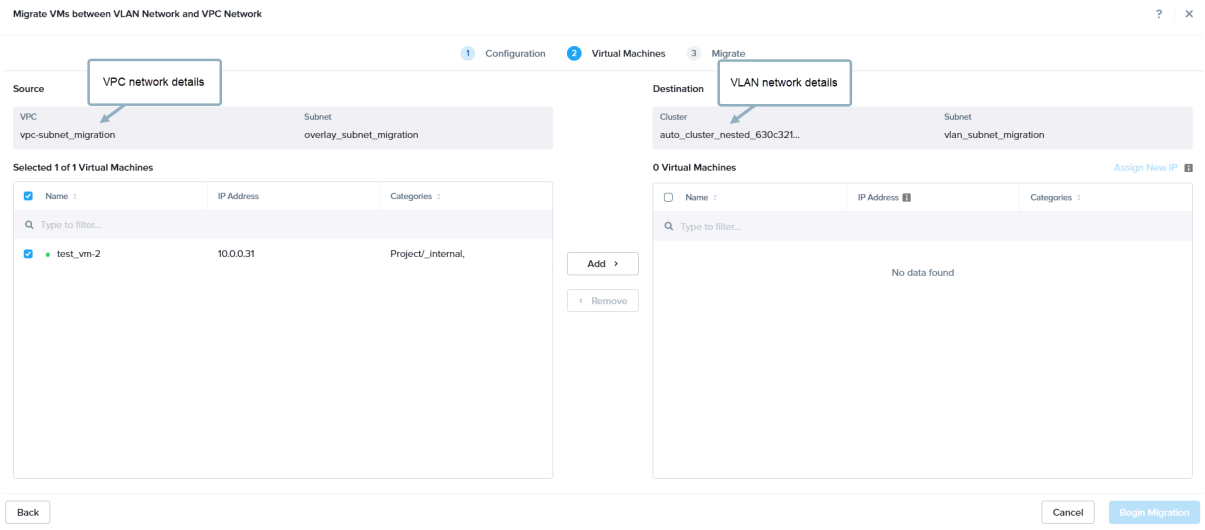


Figure 34: Migrate VMs from VPC to VLAN - Virtual Machines

The selected VM or VMs are displayed on the **Destination** side of the tab.

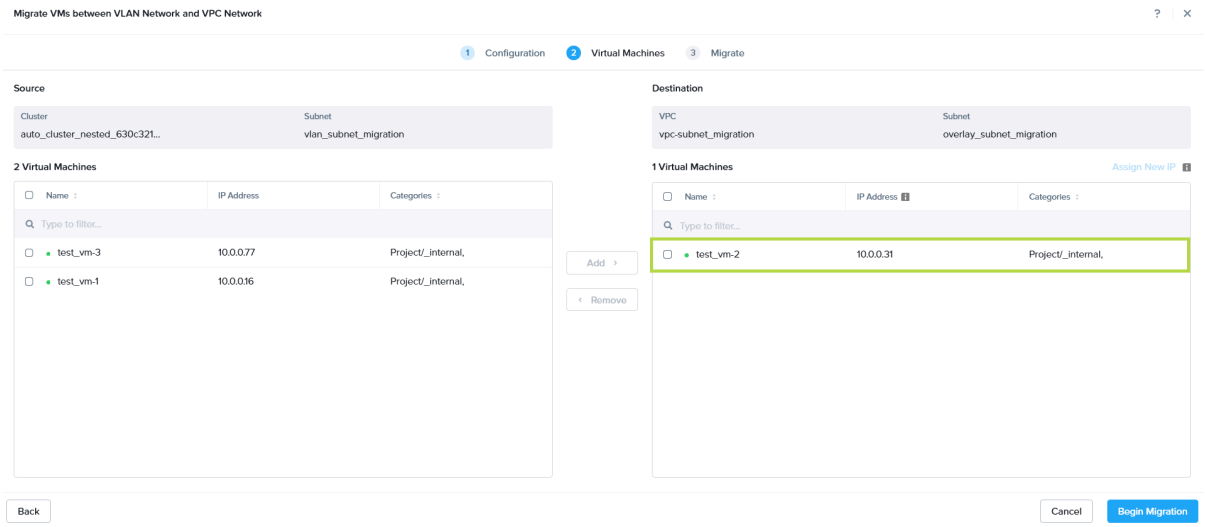


Figure 35: Migrate VMs from VLAN Network to VPC - Virtual Machines

You can select the migrating VM (**Add**ed on the **Destination** side) and click **Assign New IP** to assign a new IP address to the migrating VM after migration.

> **Note:** The IP address of the migrating VM is persisted after migration if the existing IP address is available in the destination subnet. If you migrate a VM with conflicting IP address (in other words, an IP

address that already belongs to another VM in the destination subnet) then an error is displayed on the **Migrate** tab.

- Click **Back** on the **Migrate** tab.
- On the **Virtual Machines** tab:
  - Select the migrating VM with conflicting IP address.
  - Click **Assign New IP**.

This ensures that a new IP address is assigned to the migrating VM after migration.

Click **Begin Migration** to start the migration process.

The **Migration** tab displays the progress of the migration.

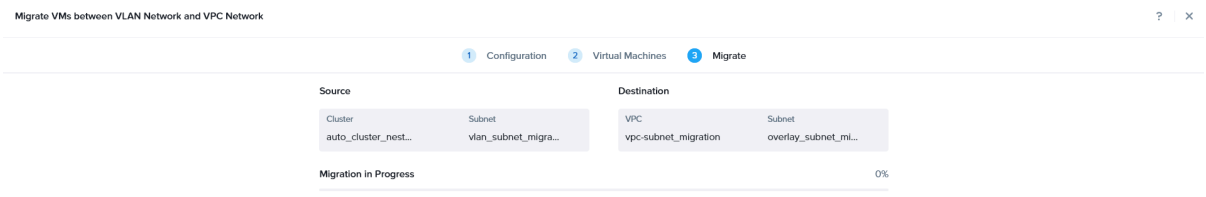


Figure 36: Migrate VMs from VLAN Network to VPC - Migration

When the migration process is complete, the **Migration** tab displays the status of the migration. It displays any errors that may have occurred during migration, the reason for failure of any VM migration.

You can filter the **Migration Summary of VM** by status using the status drop-down. There are three states: Completed, Failed and Pending. Usually, the **Migration Summary of VM** does not appear when the migration state of any migrating VM is **Pending**. Therefore, you may not find any VM listed with **Pending** state in the summary. A VM migration with pending state is displayed in **Tasks**.

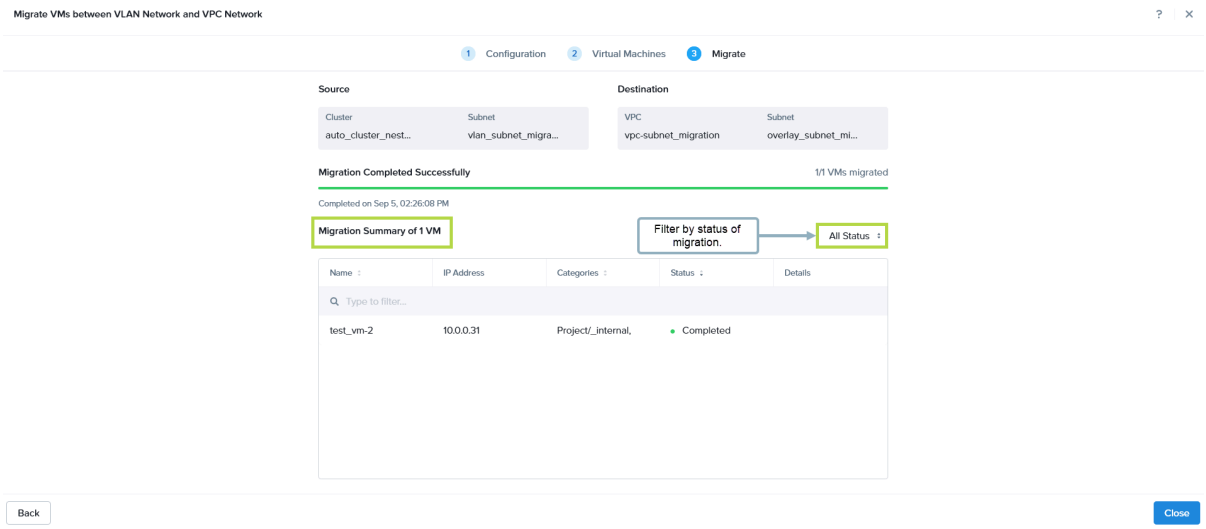


Figure 37: Migrate VMs from VLAN Network to VPC - Migration status

8. Click **Close** to close the **Migrate VMs between VLAN Network and VPC Network** window after migration is complete and successful.

What to do next

You can view the migration history on the **Subnets** dashboard by clicking **Migrate** > **View Migration History**.

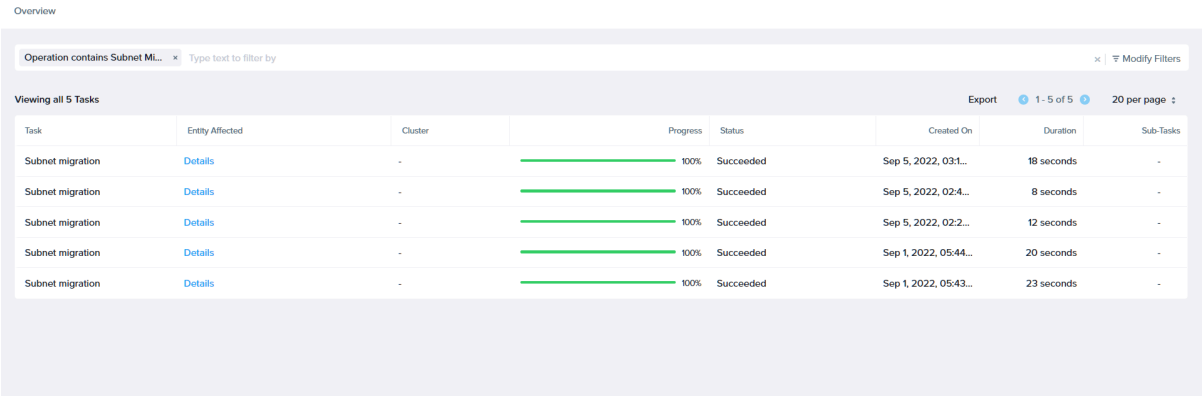


Figure 38: Migration History

Migration of VLAN Basic Subnets

For information about VLAN Basic Subnet, and VLAN Subnets, also see Network Types on page 41, Changing the Default VLAN Type on page 43, and Creating a Subnet on page 106.

With a minimum Prism Central version of PC.2023.3 that deploys Network Controller 3.0.0 on a minimum AOS version of 6.7:

- Flow Virtual Networking supports migration of VLAN Basic Subnets (see Essential Concepts on page 12 and Network Types on page 41) to VLAN Subnets (managed by the Flow Virtual Networking controller, see Essential Concepts on page 12 and Network Types on page 41).

  In the **Subnets** page that has the list of subnets, the Network Controller VLAN (VLAN or VLAN Subnet) does not have a suffix in the **Type** field. The VLAN Basic Subnet is suffixed with the word **Basic**.

- When you create VLANs using the Creating a Subnet workflow, Prism Central creates a VLAN of the type set as default.

You can change the default VLAN type that is created while you are Creating a Subnet, from VLAN Subnet type to VLAN Basic Subnet type and vice versa. For information about changing the default VLAN type, see Changing the Default VLAN Type on page 43.

Migration Process

The migration process involves migrating one subnet at a time. It locks the VLAN Basic subnet on AHV and creates a corresponding VLAN Subnet on Prism Central with the same UUID and properties or attributes as the VLAN Basic Subnet. Next, the migration process updates and migrates all the vNICs to the VLAN Subnet. After all the vNICs are migrated to the VLAN Subnet, the VLAN Basic Subnet on AHV is deleted.

Since the migration process retains the UUID of the VLAN Basic Subnet, any automations that use UUIDs are protected from impact. The MAC addresses of the vNICs are also preserved after migration, thus reducing any impact to configurations and automations that use these MAC addresses.

The Prism Central VM vNICs must always remain on a VLAN Basic Subnet. Therefore, when you migrate a VLAN Basic Subnet that hosts Guests VMs and Prism Central VMs, the Prism Central VMs vNICs are migrated to a newly created VLAN Basic Subnet on AHV host. The Prism Central VM is not migrated even if it is configured in the VLAN Basic Subnet that is marked for migration.

Note: Migration is irreversible. You must create a VLAN Basic subnet and move the vNICs to that Subnet if you want to use a VLAN Basic Subnet for vNICs that were previously migrated to a VLAN Subnet.

The migration process includes a pre-check that ascertains if all the necessary conditions for migration are met.

Migration Pre-check Conditions

You must have a **Super Admin** or **Prism Admin** access to migrate a VLAN Basic Subnet to VLAN subnet. If you are a user without **Super Admin** or **Prism Admin** level permissions, the **Migrate** button on the **Subnets** is unavailable.

The migration process includes a pre-check that ascertains if the necessary conditions for migration are met. The migration process checks whether:

- The Network Controller is enabled.
- Flow Network Security is enabled. If enabled, initiate the migration process from the Policy page.
- The number of vNICs or subnets included in the migration is within the scale numbers specified in *vNIC Scale* in Network Types on page 41.
- If you want to migrate a VLAN Basic Subnet, it must be associated with a Virtual Switch. VLAN Basic Subnets that do not have a Virtual Switch reference cannot be migrated.

  For more information about virtual switches and how to change the virtual switch that the VLAN Basic Subnet is attached to, see Virtual Switch Management in the *AHV Administration Guide*.
- Any of the VLAN Basic Subnets have kDirect vNICs or vNICs in Trunk mode. Migration of VLAN Basic Subnets with kDirect vNICs or vNICs in Trunk mode are not supported.
- The VLAN Basic Subnets are not associated with any Nutanix Files VMs. Migration of VLAN Basic Subnets associated with Nutanix Files VMs is not supported.
- The VLAN Basic Subnets are not associated with any SSP projects. Migration of VLAN Basic Subnets associated with Nutanix Self Service (formerly Calm) projects is not supported.
- The VLAN Basic Subnets are not associated with any Protection Domains for disaster recovery (see Data Protection and Recovery with Prism Element). Migration of VLAN Basic Subnets associated with Protection Domains for disaster recovery is not supported.
- Any of the VLAN Basic Subnets are not managed subnets hosting the vNICs of Prism Central VMs. Migration of (managed) VLAN Basic Subnets that host Prism Central VM vNICs is not supported.
- Any of the VLAN Basic Subnets are not used by Microservices Infrastructure. Migration of VLAN Basic Subnets that are used by Microservices Infrastructure is not supported.
- Any of the VMs in any of the VLAN Basic subnets that need to be migrated, have vNICs in multiple VLAN Basic Subnets but not all those subnets are being migrated. Such VLAN Basic Subnets that have VMs that do not have all the vNICs in the migrating Basic VLANs, cannot be migrated.

Migrating a VLAN Basic Subnet to VLAN Subnet

Before you begin

Ensure that Flow Virtual Networking is enabled.

About this task

Perform this task to migrate a VLAN Basic Subnet (AHV Networking based VLAN) and all the virtual NICs configured in that subnet to a newly create VLAN Subnet (Network Controller based VLAN). The target

VLAN Subnet is automatically created during the procedure of migration. The outcome of this task is that the VLAN Basic Subnet configuration is fully migrated to a VLAN Subnet.

You can migrate a VLAN Basic Subnet to VLAN subnet on the **Subnets** page. Go to the **Subnets** page by clicking **Network & Security** > **Subnets**.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   The **Subnets** page opens displaying the *List* tab.
3. Click **Migrate**.
4. To migrate VLAN Basic Subnet to VLAN Subnet, do the following.
   a. Select `VLAN Basic Subnet` in the **Migrate From** field.
   b. Select `VLAN Subnet` in the **Migrate To** field.
   c. Click **Next**.

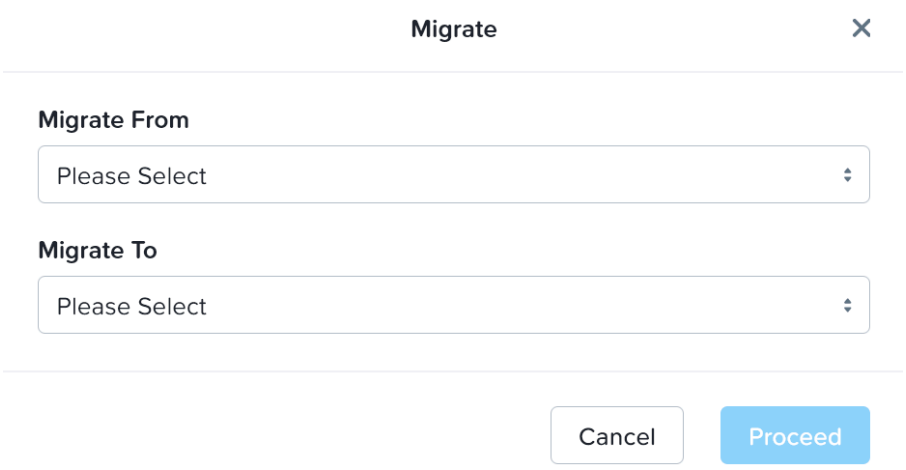


Figure 39:

5. On the **VLAN Basic to VLAN Migration** page, click **Add** to add the VLAN Basic subnets that you need to migrate.
6. On the **Add Subnets to migration** page, from the list of subnets, select the check boxes for the VLAN Basic Subnets that you need to migrate.
   Click **Add**.

7. On the **VLAN Basic to VLAN Migration** page, click **Begin Migration** to start the migration process. The **Migrate (x) VLAN Subnet(s)?** tab displays a message about the temporary downtime, that migration cannot be aborted or paused and that migration of other subnets cannot begin until this migration process is completed.

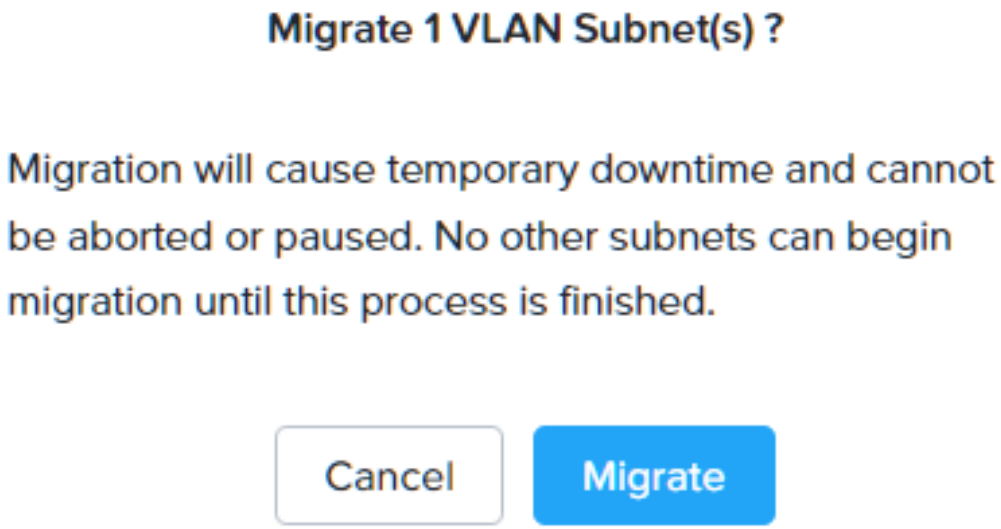


Figure 40:

Click **Migrate**.

8. On the **Migrating (x) Subnets** tab displays the progress of the migration.

   When the migration process is complete, the **Migrating (x) Subnets** tab displays the status of the migration. It displays any errors that may have occurred during migration, the reason for failure of any VM migration.

   You can filter the list of migrated VLANs using the drop-downs and filters in the table of migrated VLANs.

9. Click **Close** to close the **VLAN Basic to VLAN Migration** window after migration is complete and successful.

What to do next

You can view the migration history on the **Subnets** dashboard by clicking **Migrate** > **View Migration History**. If you see that the migration of any of the VLAN Basic Subnets has failed, initiate the migration for those VLAN Basic Subnets again by following all the above steps in this procedure.

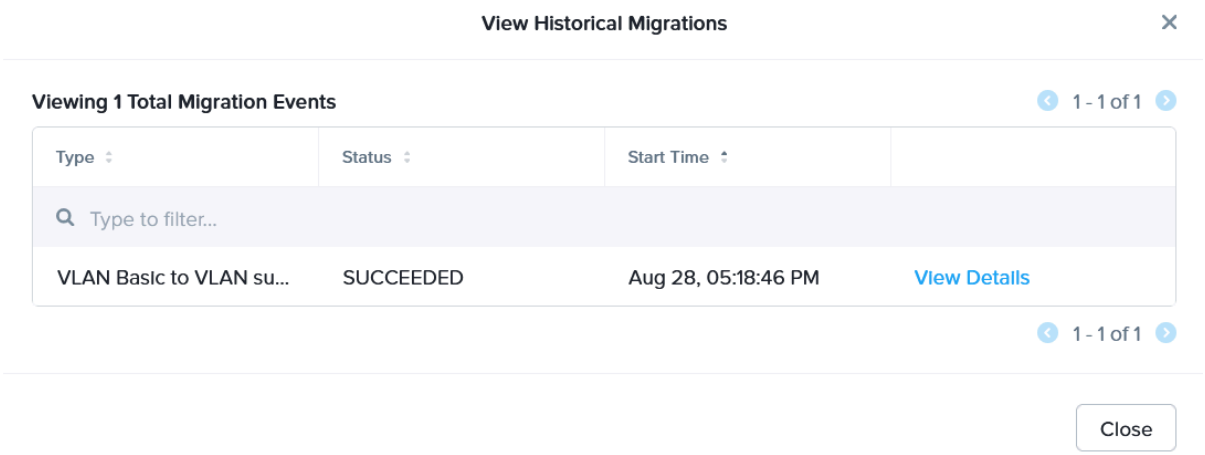


Figure 41: Migration History

VPC Management

This section provides information and procedures that you need to manage virtual private clouds (VPCs), subnets, routing policies, and static routes using Flow Virtual Networking.

A Virtual Private Cloud (VPC) is an independent and isolated IP address space that functions as a logically isolated virtual network. A VPC could be made up of one or more subnets that are connected through a logical or virtual router. VPCs allow you to manage the isolated and secure virtual network with enhanced automation and scaling. The isolation is done using network namespace techniques like IP-based subnets or VLAN based networking.

Flow Virtual Networking supports the following two types of VPCs.

VPC

The default VPC type that is referred to as *VPC* in this documentation is the one you create to isolate selected subnets of connected VMs. This is also called as User VPC or Guest VPC, specifically referred to as VPC.

The other VPC type is transit VPC, specifically referred to as *transit VPC* in this documentation.

Transit VPC

Overlay External Subnet for Transit VPCs

- You can only use a VLAN based network for the uplink (external connectivity) for a transit VPC. In other words, a transit VPC cannot be connected to another transit VPC.
- You can configure an Overlay subnet with external connectivity in transit VPC. When you create an Overlay external subnet, the workflow provides only transit VPCs in the **VPC** dropdown menu.
- You can configure an Overlay subnet with external connectivity (Overlay external subnet) with options such as NAT or NONAT (NAT being default) and necessary gateways for the NAT or No-NAT option.
- You can connect only regular VPCs to transit VPC using an Overlay external subnet.

  You cannot attach any VMs to an Overlay external subnet. You cannot connect, for example, two regular VPCs to each other using an Overlay external subnet.

- This is in line with the behavior for the VLAN backed external subnets. The external overlay subnets are how a regular VPC will connect to a transit VPC. Two transit VPCs will not be allowed to be connected using this.

For information on VPCs, see Essential Concepts on page 12.

Creating Virtual Private Cloud

You can create VPCs and transit VPCs on the **Virtual Private Clouds** page.

About this task

Perform the following steps to create a VPC.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click **Create VPC**.
   The **Create VPC** window opens.

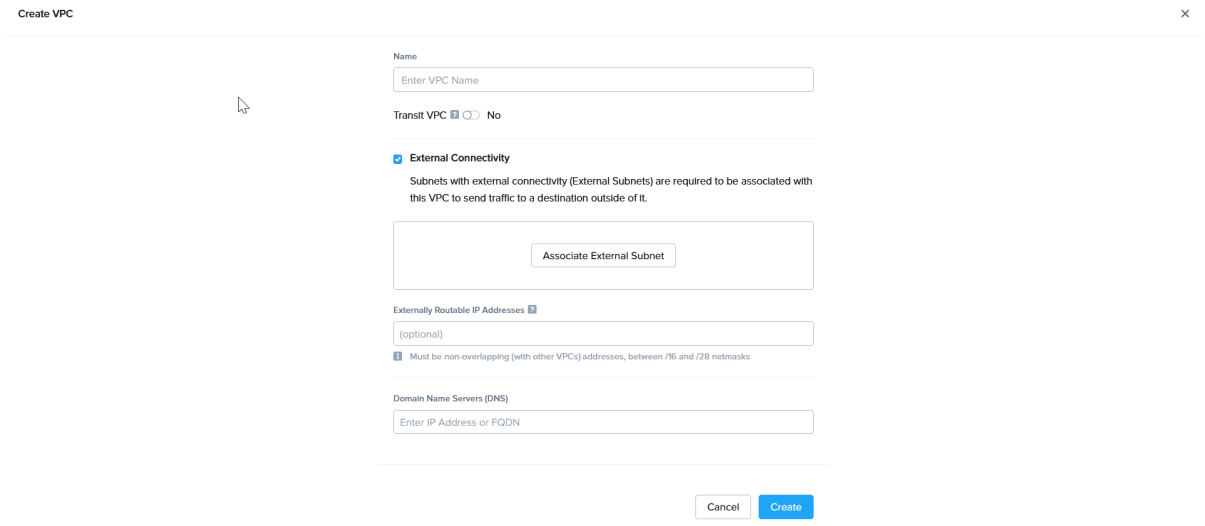


Figure 42: Create VPC

4. Provide the necessary values in respective fields.

Parameters	Description and Values
Name	Provide a name for the VPC.
Transit VPC toggle switch	Toggle the Transit VPC toggle switch to `Yes`if you want to create a transit VPC instead of a regular VPC. See Virtual Private Cloud on page 82 for information about the difference between a VPC and a transit VPC.

Parameters	Description and Values
External Connectivity	This section lets you **Associate External Subnet**s for the VPC. A subnet with external connectivity (External Subnet) is required if the VPC needs to send traffic to a destination outside of the VPC. **Note:** You can add a maximum of two external subnets - one external subnet with NAT and one external subnet without NAT to a VPC. Both external subnets cannot be of the same type. For example, you cannot add two external subnets, both with NAT. You can update an existing VPC similarly. Network address translation (NAT) Gateways perform the required IP address translations required for external routing. You can also have external connectivity without NAT (No-NAT).
External Connectivity > External Subnet	Displays the name of the external subnet that is associated with the VPC.
External Connectivity > Destination Prefixes	Displays the prefixes for which this external subnet is used as the next hop. The selection is based on the longest prefix match.
External Connectivity > SNAT IP / Router IP	Displays the SNAT IP or Router IP addresses that the IPs assigned to the VPC router in the external subnet. It is used as SNAT IP in case of NAT external subnet. These addresses would be used by the physical network router as the next hop for all the networks reachable inside the VPC using a No-NAT external subnet. **Note:** You can specify a custom SNAT or Router IP selected from the IP address pool of the
External Connectivity > Actions	Displays the actions (as icons) that you can perform on the external subnet. The actions listed are: Edit and Delete
Associate External Subnet button	Click the **Associate External Subnet** button to display the **Associate External Subnet** window which allows you to configure the external subnet parameters.
Associate External Subnet window details	
Associate External Subnet > Subnet Type	Select the type of subnet that you have configured as the external subnet. The types you can select from are **VLAN** being the VLAN subnet and **Overlay** subnets
Associate External Subnet > External Subnet	Select an external subnet from the drop down list. By associating the VPC with the external subnet you can provide external connectivity to the VPC. When you select the external subnet, the details of the subnet like **Network Address/Prefix**, **NAT-ed** (which displays the NAT status of the subnet as **Yes** or **No**, and (for only **VLAN** type subnet) **VLAN** ID of the VLAN External Subnet are displayed in a table below the **External Subnet** dropdown list field.
Static Routes	Configure the static routes that specify the list of prefixes for which the selected external subnet is the next hop. Also, configure the routes on the router for the return traffic to reach the VPC. For more information, see *External Connectivity* in Virtual Private Cloud Details View on page 56.

Parameters	Description and Values
SNAT IP/Router IP	Select the appropriate option from **Auto Assigned** or **Custom Defined**. The SNAT or Router IP address is the next hop for the physical routing infrastructure. If you select the **Auto Assigned**, the Network Controller assigns an IP address from the IP address pool of the external subnet as SNAT or Router IP address. When you select the **Custom Defined** option, a table with details of available IP address pool is displayed. This table displays **IP Pool Range**, **Used IPs in Pool**, and **Free IPs in Pool** information for the pool. Enter an IP address selected from the **Free IPs in Pool** that you want to be assigned as SNAT or Router IP address, in the **Custom SNAT IP / Router IP** field.
External Gateway Configuration > Number of Active Hosts	Displayed only when you select a No-NAT VLAN external subnet from the **Associate External Subnet** > **External Subnet** dropdown menu) Select the **Number of Active Hosts**, in other words, the number of No-NAT gateways you need. You can select up to **4** gateways. If you do not select the number of gateways or active hosts, the number is pre-selected as **2**, the default number of gateways or active hosts. No-NAT gateways are deployed as AHV hosts. See *No-NAT Gateway* in Essential Concepts on page 12.
Other details on the **Create VPC** page	
Externally Routable IP Addresses	(Optional) Add externally routable IP addresses or subnets with external connectivity without NAT. These are used by BGP Gateways to advertise routes. Ensure that the externally routable IP addresses that you provide, do not overlap with those provided for other VPCs.
Domain Name Servers (DNS)	(Optional) DNS is advertised to Guest VMs via DHCP. This can be overridden in the subnet configuration. Click **+ Server IP** to add DNS server IPs under **IP Address** and click the check mark. You can **Edit** or **Delete** an IP address you added using the options under **Actions**.

5. Click **Create**.

Requesting Floating IPs

About this task

User VMs or VPN gateways or many such entities require Floating IP addresses. To provide floating IP to an entity, you can request Floating IPs and assign them to VMs.

Perform the following steps to request a floating IP.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Floating IPs** from the **Navigation Bar**.
   The **Floating IPs** page opens displaying the **List** tab.
3. Click **Request Floating IP**.
   The **Request Floating IP(s)** window opens.
4. Enter the information in the respective fields.

> **Note:** Clear the **Assign Floating IPs** checkbox if you want to assign the requested IP addresses after you receive it. For more information, see Floating IPs Summary View on page 61.

Fields	Description and Values
External Subnet	Select a subnet that you configured with external connectivity. When you select an external subnet, a box displays the IP pool information for the selected external subnet. The following IP pool details are displayed. • **IP Pool Ranges**: Displays the range of IP addresses with th starting IP address and ending IP address of the range. • **Used IPs in the Pool**: Displays the number of IP addresses already used from the pool. • **Free IPs in the Pool**: Displays the number of unused IP addresses in the pool.
Number of Floating IPs	Enter the number of Floating IPs you want to request. You can request a maximum of 50 floating IP addresses.
Define Custom Floating IPs	Select this check box if you want to select specific IP addresses from the IP address pool range of the external subnet. When you select the check box, the **Enter Floating IPs to be requested** field is displayed below the check box text. Enter the specific IP addresses that you want to request as Floating IPs in this field.
Assign Floating IPs	Select this check box if you want to assign the Floating IPs to specific VMs in the table. Based on the number you entered in the **Number of Floating IPs** field, the system provides an equivalent number of rows of `Search VMs` and `IP Address` in the table. Under **Search VMs**, select the VM to which you want to assign a floating IP address. Under **IP Address**, select the IP address on the VM (primary or secondary IP address) to which you want to assign the floating IP. You can assign multiple floating IP addresses to multiple secondary IP addresses that you can create on the NIC of the VM. For information about configuring secondary IP addresses, see Creating Secondary IP Addresses on page 84.

> **Note:**

5. Click **Save**.

What to do next

When you receive the floating IP address you requested, you can see it, assign it (if not already assigned while requesting) or delete it in the **Floating IPs** view.

Creating a Subnet

About this task

Perform the following steps to create a subnet.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   The **Subnets** page opens displaying the **List** tab.

3. Click **Create Subnet**.
   The **Create Subnet** window opens. The following figure displays the Create Subnet window with all the options. These options are displayed based on the values you select in the **Type** field.

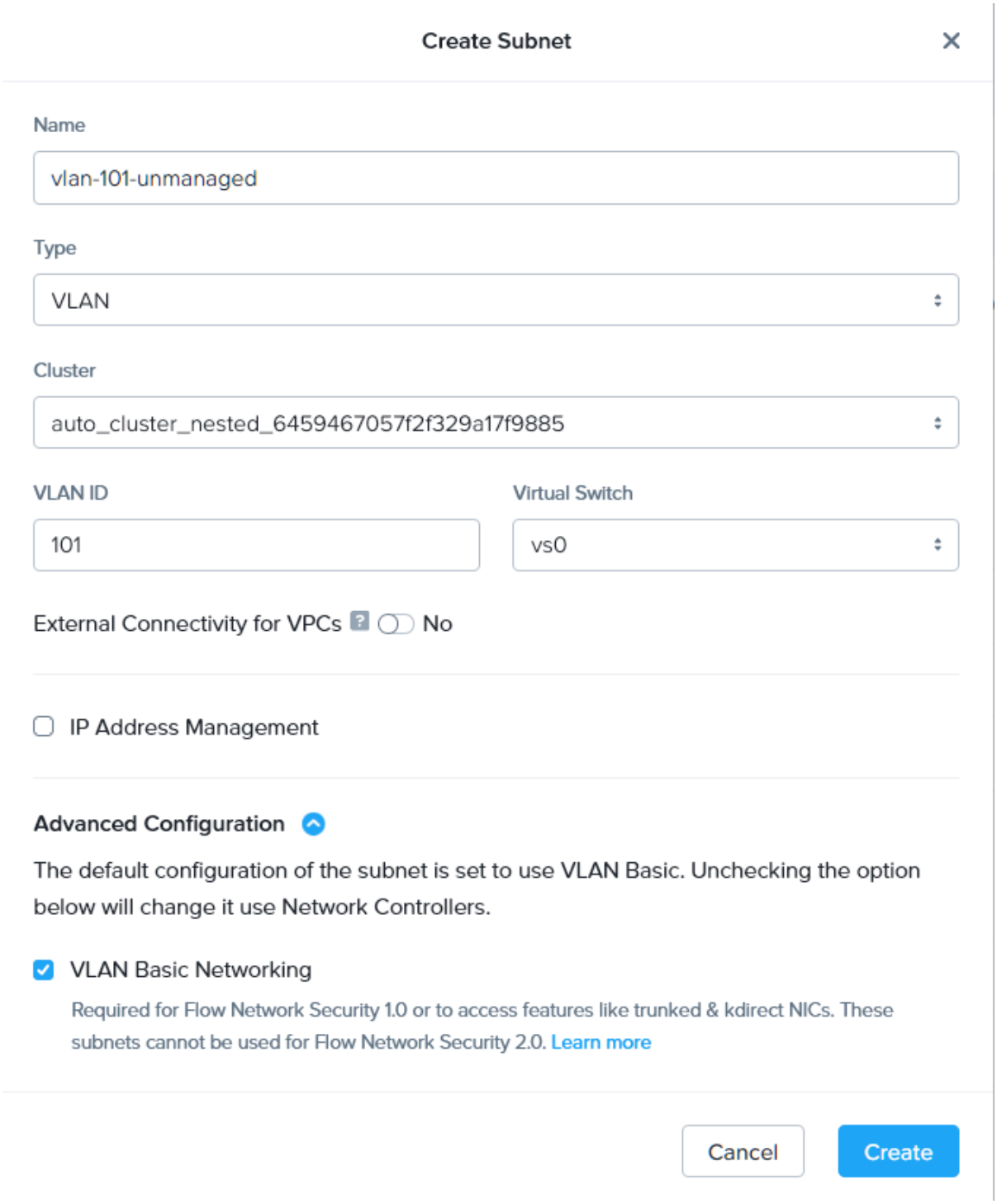


Figure 43: Create Subnet (With External Connectivity Disabled)

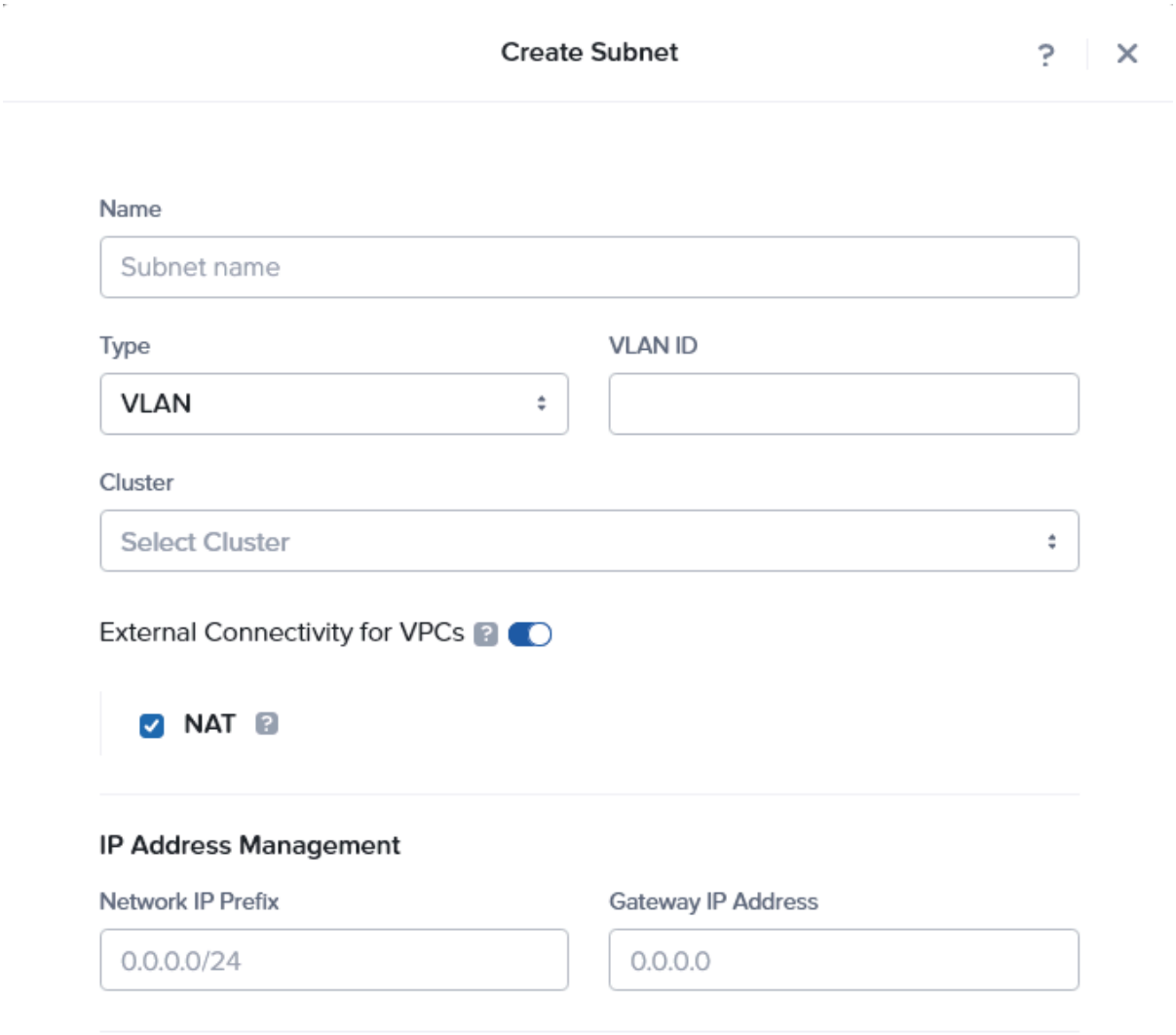


Figure 44: Create Subnet (With External Connectivity Enabled)

Fields	Description and Values
Name	Provide a name for the subnet.
Type	Select the type of subnet you want to create. You can create a `VLAN` subnet or an `Overlay` subnet.
VLAN ID	(VLAN subnet only) Enter the number of the `VLAN`. Enter just the number in this field, for example 1 or 27. Enter 0 for the native VLAN. The value is displayed as vlan.1 or vlan.27 in the View pages. **Note:** Provision any single VLAN ID either in the AHV network stack or in the Flow Virtual Networking (brAtlas) networking stack. Do not use the same VLAN ID in both the stacks.

Fields	Description and Values
IP Address management	(Mandatory for Overlay type subnets) This section provides the *Network IP Prefix* and *Gateway IP* fields for the subnet. (Optional for VLAN type subnet) Select this checkbox to display the *Network IP Prefix* and *Gateway IP* fields and configure the IP address details. Clearing this checkbox hides these fields. In this case, it is assumed that this virtual LAN is managed outside the cluster. **Note:** The **DHCP Settings** option is only available for VLAN subnets if you select this option.
DHCP Settings	(Optional for both VLAN and Overlay subnets) Select this checkbox to display fields for defining a domain. Selecting this checkbox displays fields to specify DNS servers and domains. Clearing this checkbox hides those fields. For more information, see Setting the DHCP Options on page 110.
Cluster (VLAN subnet only)	(VLAN subnet only) This option is available only for `VLAN` subnet configuration. Select the cluster that you want to assign to the subnet.
External Connectivity	Turn on this toggle switch if you want use this (`VLAN` or `Overlay`) subnet for external connectivity. The **External Connectivity** toggle switch is displayed as an option for an `Overlay` subnet, only if you associate the subnet with a transit VPC (selected in the **VPC** drop down menu that is displayed only when you select `Overlay` in the **Type** drop down menu). **Note:** • Ensure that the externally routable IP addresses (subnets with external connectivity without NAT) for different VPCs do not overlap. • Configure the routes for the external connectivity subnets with next hop as the Router or SNAT IP address. Also configure the routes on the router for the return traffic to reach the VPC. For more information, see *External Connectivity* in Virtual Private Cloud Details View on page 56.
NAT	(Option under **External Connectivity**) If you turn on the **External Connectivity** toggle switch, you can choose whether to connect to external networks with or without enabling NAT. Select the **NAT** checkbox to enable NAT for external connectivity for VPCs.
Virtual Switch	(VLAN subnet only) Select the virtual switch that is configured for the VLAN you selected. The default value is the default virtual switch vs0. This option is displayed only if you add a VLAN ID in the VLAN ID field.

Fields	Description and Values
VPC	(Overlay subnet only) Select the `Virtual Private Cloud (VPC)` that you want to assign to the subnet from the drop down list. You can create VPCs and assign them to `Overlay` subnets.
IP Address Pool	Defines a range of addresses for automatic assignment to virtual NICs. This field is optional for both `VLAN` and `Overlay`. For `VLAN`, this field is displayed only if you select the **IP Address Management** option. **Note:** Configure this field for `VLAN` or `Overlay` to complete the creation of the VPC, if you do not need external connectivity for this subnet. You must configure this field only if you need external connectivity for this subnet. Click the **Create Pool** button and enter the following in the **Add IP Pool** page: • Enter the starting IP address of the range in the **Start Address** field. • Enter the ending IP address of the range in the **End Address** field. • Under **Actions**, click the check mark to submit the starting and ending IP addresses you entered. Click the X mark to remove the entries.
Override DHCP Server	(VLAN subnet only) To configure a DHCP server, select the **Override DHCP Server** checkbox and enter an IP address in the **DHCP Server IP Address** field. For more information, see *Override DHCP Server (VLAN Only)* in Setting the DHCP Options on page 110.
Advanced Configuration —VLAN Basic Networking	(VLAN subnet only) Select the **VLAN Basic Networking** checkbox to create the Basic VLAN on AHV networking (see Basic VLANs or VLAN Basic Subnet in Essential Concepts on page 12 and Network Types on page 41).

4. Click **Create**.

Setting the DHCP Options

About this task

Selecting the **DHCP Settings** checkbox in **Create Subnet** or **Update Subnet** allows you to configure the DHCP options for the VMs within the subnet. When DHCP settings are configured for a VM in a subnet and the VM is powered on, Flow Virtual Networking configures these options on the VM automatically. If you do not configure the DHCP settings, then these options are not available on the VM automatically when you power it on.

You can enable **DHCP Settings** when you create a subnet and configure the **DHCP Settings** for the new subnet. You could also update the DHCP Settings for an existing subnet.

DHCP Settings is common to and is available on both the **Create Subnet** and the **Update Subnet** dialog boxes. To configure the **DHCP Settings**, do the following:

Procedure

- Provide the information in the **DHCP Settings** fields.

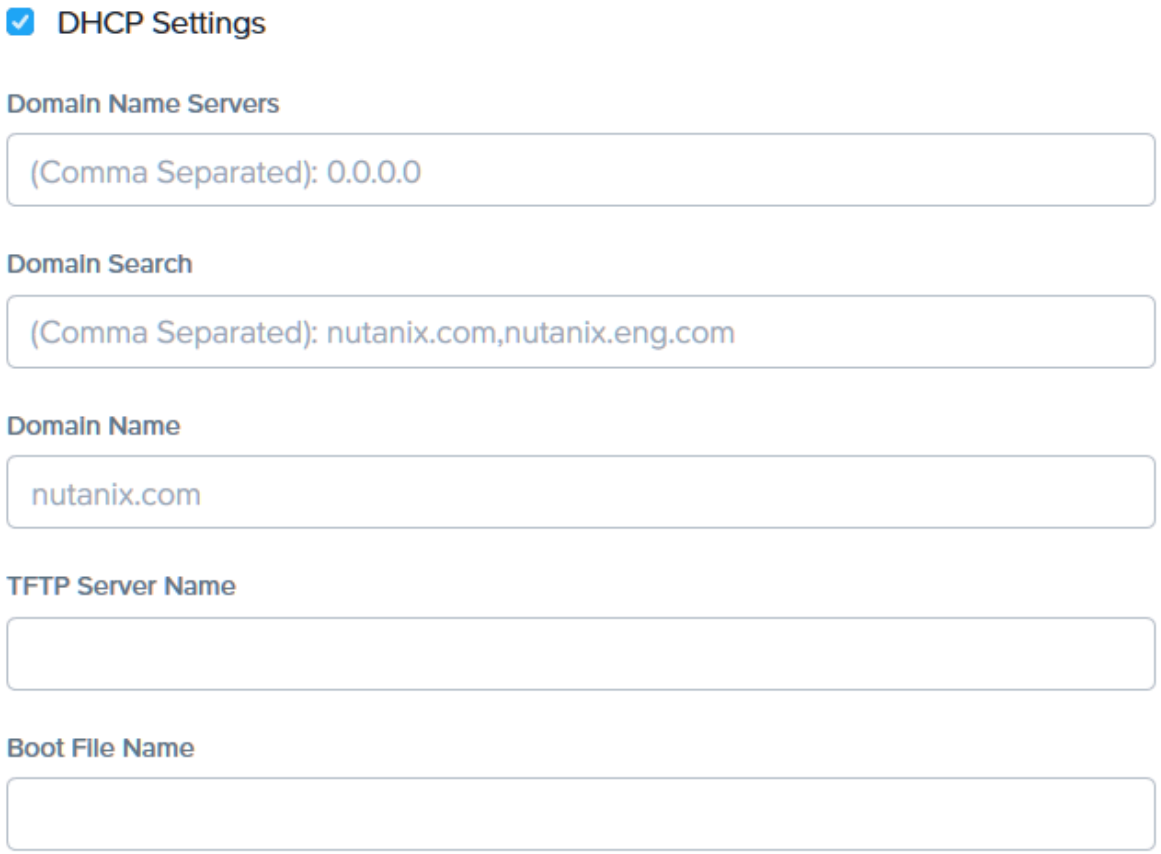


Figure 45: DHCP Settings

Fields	Description and Values
Domain Name Servers	Provide a comma-separated list of DNS IP addresses. Example: 8.8.8.8, 9.9.9.9
Domain Search	Enter the VLAN domain name. Use only the domain name format. Example: nutanix.com
TFTP Server Name	Enter a valid TFTP host server name of the TFTP server where you host the host boot file. The IP address of the TFTP server must be accessible to the virtual machines to download a boot file. Example: tftp_vlan103
Boot File Name	The name of the boot file that the VMs need to download from the TFTP host server. Example: boot_ahv2020xx

- (Optional and for VLAN networks only) Check the **Override DHCP Server** dialog box and enter an IP address in the **DHCP Server IP Address** field.

  You can configure a DHCP server using the **Override DHCP Server** option only in case of VLAN networks.

  The DHCP Server IP address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If this box is not checked, the DHCP Server IP Address field is not displayed and the DHCP server IP address is generated automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.

  Usually the default DHCP server IP is configured as the last usable IP in the subnet (For eg., its 10.0.0.254 for 10.0.0.0/24 subnet). If you want to use a different IP address in the subnet as the DHCP server IP, use the override option.

Attaching a Subnet to a Virtual Machine

About this task

Perform the following steps to attach a subnet to a VM.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**.
   The **VMs** page opens displaying the **List** tab.
3. Select the VM you want to attach a subnet to, and click **Update** from the **Actions** dropdown menu.
   The **Update VM** page opens displaying the **Configuration** tab.
4. Click **Next**.
   The **Resources** tab opens.
5. Click **Attach to Subnet**.
   The **Attach to Subnet** window opens.
6. Provide the necessary information in the indicated fields.
   a. Select the **Subnet Name** from the dropdown menu.
   b. Select the **Network Connection State** as `Connected` or `Disconnected`.

      The **Network Connection State** selection defines the state of the connection after the NIC configuration is implemented.
   c. Select the **Assignment Type**.

      You can select `Assign with DHCP` to assign a DHCP based IP address to the VM.

      You can select `Assign Static IP` to assign a static IP address to the VM to reach the VM quickly from any endpoint in the network such as a laptop.
7. Click **Save**.

Creating a Policy

About this task

For Policy-based routing you need to create policies that route the traffic in the network.

When you create a VPC, there is one default policy that Flow Virtual Networking creates for the VPC. This policy is pre-configured with the Priority 1 and other default values to Deny traffic flow and service (see the table of field descriptions and values for this dialog box).

> **Note:** You cannot update or delete the default policy.

- Policies control the traffic flowing between subnets (inter-subnet traffic).
- Policies control the traffic flowing in and out of the VPC.
- Policies do not control the traffic within a subnet (intra-subnet traffic).

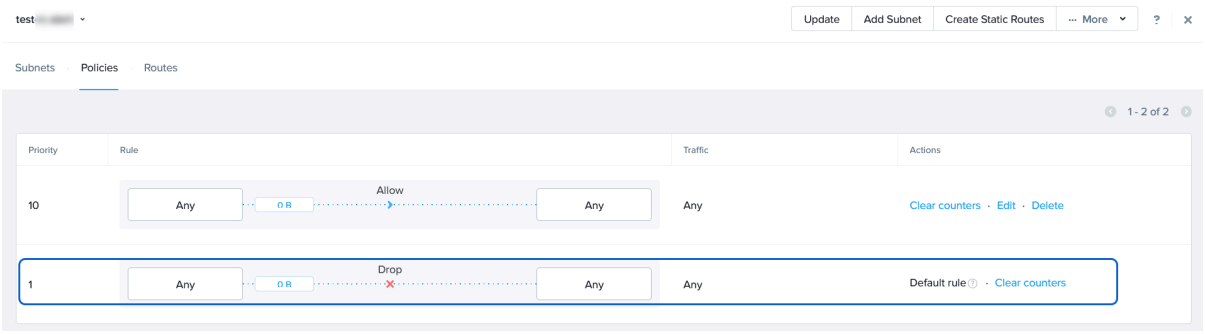


Figure 46: Policy Tab

Perform the following steps to create a policy.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click the name of the VPC for which you want to create a policy.
   The **Summary** tab opens displaying the detailed information about the VPC in widgets.
4. Click the **Policies** tab.
5. Click **Create Policy**.
   The **Create Policy** window opens.

6. Provide the necessary values in the respective fields.

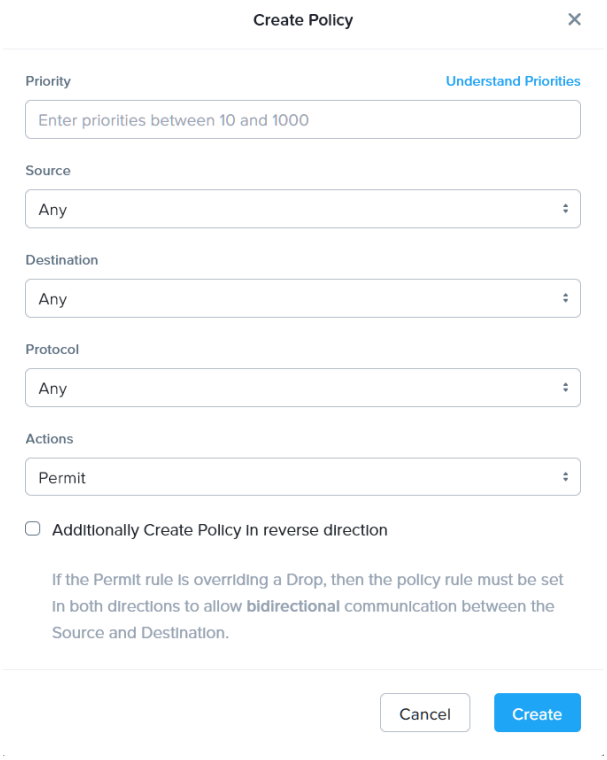


Figure 47:

The following table describes the fields that appear in the **Create Policy** window.

Fields	Description and Values	Value in Default Policy
Priority	The priority of the access list (ACL) determines which ACL is processed first. Priority is indicated by an integer number. A higher priority number indicates a higher priority. For example, if two ACLs have priority numbers 100 and 70 respectively, the ACL with priority 100 takes precedence over the ACl with priority 70. **Note:** • Click the `Understand Priorities` link to see the `Understand Priorities` information box (see the image of this box below this table).	1

Fields	Description and Values	Value in Default Policy
Source	The source indicates the source IP or subnet for which you want to manage traffic. Source can be: • `Any`: Indicates any IP address. • `External`: Indicates an IP address that is outside the subnets configured for the VPC. • `Custom`: You can provide a specific **Source Subnet IP** with prefix.	Any
Source Subnet IP	Only required if you selected the **Source** as `Custom`. Provide the subnet IP and prefix that you want to designate as the source for the policy. Use the CIDR notation format to provide the subnet IP. For example, 10.10.10.0/24.	None
Destination	The destination is the destination IP or subnet for which you want to set the priority. Destination can be: • `Any`: Indicates any IP address. • `External`: Indicates an IP address that is outside the subnets configured for the VPC. • `Custom`: You can provide a specific **Destination Subnet IP** with prefix.	Any
Destination Subnet IP	Only required if you selected the **Destination** as `Custom`.	None
Protocol	You can also set the priority configure policy for certain protocols. You can select one of the following options: • `Any`: Indicates any IP address. • `Protocol Number`: Provide an integer number that indicates the protocol you want to prioritize. Provide the appropriate value in the **Protocol Number** field. • `TCP` • `UDP` • `ICMP`	Any
Protocol Number	This field is displayed only if you select **Protocol Number** as the value in the **Protocol** field. The number you provide must be the IANA designated number that indicates respective protocol. See IANA Protocol Numbers.	None

Fields	Description and Values	Value in Default Policy
Actions	Assign the appropriate action for implementation of the policy. • `Permit`: Permits traffic and services based on the parameters set. If the Permit rule is set to override a Drop rule, then the Permit rule must be set in both the directions to allow bidirectional communication between the **Source** and **Destination**. • `Deny`: Denies traffic and service based on the parameters set. • `Reroute`: Sends matching traffic to the next-hop IP address specified by the `Reroute IP`. You can also persist traffic to a specified IP address that may be assigned or re-assigned to any entity. Configure **No Action** as the **Fallback Action** to persist traffic to the specified IP address. • Provide an IP address that the traffic needs to be re-routed to, in the `Reroute IP` field. • Select a **Fallback Action**. To persist traffic to the virtual IP address you added in the `Reroute IP` field, select `No Action`. See *Reroute Policy with No Action Fallback* in Essential Concepts on page 12. • `Forward`: Forwards matching traffic to the external next-hop IP address specified by the `Forward IP`. Provide an IP address that the traffic needs to be forwarded to, in the `Forward IP` field.	`Permit`

Fields	Description and Values	Value in Default Policy
Additionally Create Policy in reverse direction	Select this checkbox to set a policy rule in the reverse direction if you need to setup bidirectional communication between the **Source** and **Destination**.	Select or clear

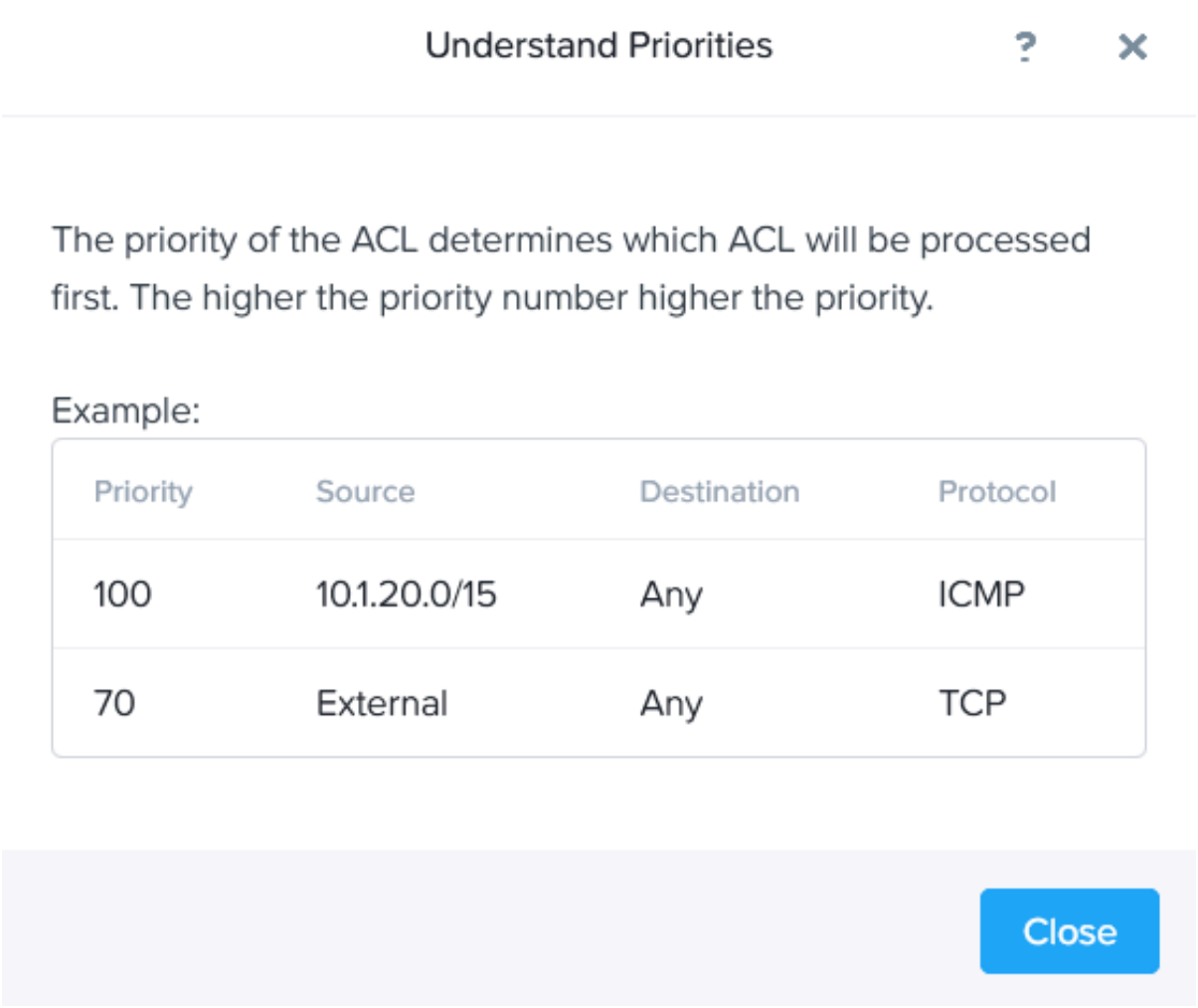


Figure 48: Understanding Priorities

7. Click **Create**.

Creating Static Routes

About this task

Perform the following steps to create static routes.

To create static route, do the following in the **Create Static Routes** dialog box:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click the name of the VPC for which you want to create a static route.
   The **Summary** tab opens displaying the detailed information about the VPC in widgets.
4. Click the **Routes** tab.
5. Click **Manage Static Routes**.
   The **Manage Static Routes** window opens.
6. Click **Add Static Route**.
7. Provide the necessary values in the respective fields.
   The following table describes the fields that appear in the **Manage Static Routes** window.

Fields	Description and Values
Destination Prefix	Provide the IP address with prefix of the destination subnet.
Next Hop Link	Select the next hop link from the drop down list. The next hop link is the IP address that the traffic must be sent for the static route you are configuring.
Add Static Route	You can create multiple static routes using this option. Click this link to add another set of **Destination Prefix** and **Next Hop Link** to configure another static route.

8. Click **Save**.

Updating Virtual Private Cloud

About this task

Perform the following steps to update a VPC or a transit VPC.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Select the checkbox associated with the VPC you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update VPC** window opens.

4. Update the necessary values in the respective fields.

   The fields in the **Update VPC** window is identical to the fields in the **Create VPC** window. For more information, see Creating Virtual Private Cloud on page 102.

   > **Note:** You cannot update the **Associate External Subnet** > **Number of Active Hosts**, in other words, the number of No-NAT gateways selected for the VPC.

   To update the **Number of Active Hosts** for the already selected external, No-NAT VLAN network, do the following.

   a. Delete the associated external, No-NAT VLAN network.

   b. Select **Update** to save the deletion.

   c. Select **Associate External Subnet** and add the previously associated external, No-NAT VLAN network.

   d. Select the necessary number of **Number of Active Hosts** after appropriately configuring other parameters in the **Associate External Subnet** window.

   e. Select **Update** to save the association.

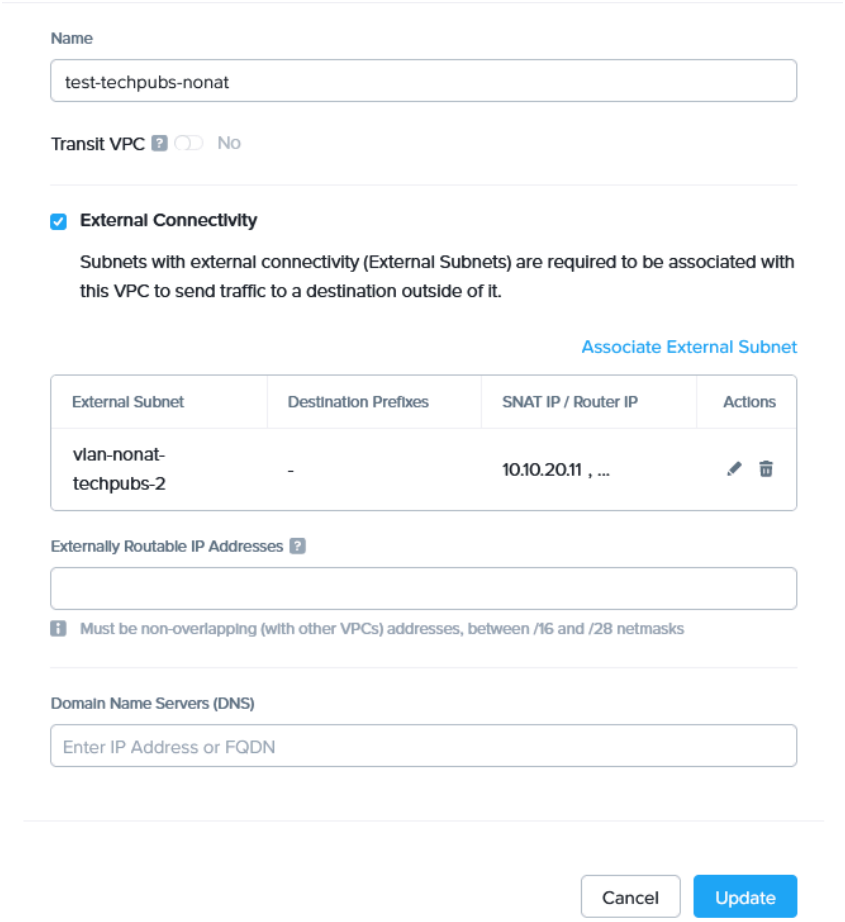


Figure 49: Update VPC

5. Select **Update** on the **Update VPC** page.

Updating a Subnet

About this task

Perform the following steps to update a subnet.

> **Important:** You cannot edit or update the subnet type. For example, if the subnet type is already configured as *VLAN*, you cannot modify it to an *Overlay* type subnet.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   The **Subnets** page opens displaying the **List** tab.
3. Select the checkbox associated with the subnet you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update Subnet** window opens.
4. Update the necessary values in the respective fields.

   The fields in the **Update Subnet** window is identical to the fields in the **Create Subnet** window. For more information, see Creating a Subnet on page 106.
5. Click **Update** to ensure that the updates are saved in the configuration.

Category Management

A category is a key-value pair that groups similar entities. Associating a policy with a category ensures that the policy applies to all the entities in the group regardless of how the group scales with time. For example, you can associate a group of VMs with the Department: Marketing category, where Department is a category that includes a value Marketing along with other values such as Engineering and Sales.

Currently, you can associate only VMs with a category. Categories are implemented in the same way on on-premises Prism Central instances and in Xi Cloud Services. For information about configuring categories, see the *Prism Central Infrastructure Guide*.

Updating a Policy

About this task

Perform the following steps to update a policy.

> **Note:** You cannot update or delete the default policy.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click the name of the VPC for which you want to update the policy.
   The **Summary** tab opens displaying the detailed information about the VPC in widgets.
4. Click the **Policies** tab.

5. Select the checkbox associated with the policy you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update Policy** window opens.
6. Update the necessary values in the respective fields.

   The fields in the **Update Policy** window is identical to the fields in the **Create Policy** window. For more information, see Creating a Policy on page 113.
7. Click **Update**.

Updating Static Routes

About this task

Perform the following steps to update a static route.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click the name of the VPC for which you want to update a static route.
   The **Summary** tab opens displaying the detailed information about the VPC in widgets.
4. Click the **Routes** tab.
5. Click **Manage Static Routes**.
   The **Manage Static Routes** window opens.
6. Update the necessary values in the respective fields.

   Note: You must configure the default route (0.0.0.0/0) to the external subnet as the next hop for connectivity outside the cluster (north-south connectivity).

   For details about the fields that you can update, see Creating Static Routes on page 117.
7. Click **Save**.

Deleting a Virtual Private Cloud

About this task

Perform the following steps to delete a VPC.

Important: Prism Central does not allow you to delete a VPC if the VPC is associated with any subnets and/or VPNs. You can delete the VPC after you remove all the subnets or VPN associations from the VPC.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.

3. Select the checkbox associated with the VPC you want to delete, and click **Delete** from the **Actions** dropdown menu.
4. In the confirmation dialog box, click **Delete** to delete the VPC.
   Click **Cancel** to exit without deleting the VPC.

Deleting Subnets, Policies or Routes

You can delete VPC entities such as subnets, policies or routes from the VPC details page.

About this task

Perform the following steps to delete VPC entities such as subnets, policies or routes.

> **Note:** You cannot update or delete the default policy.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.
   The **Virtual Private Clouds** page opens displaying the **List** tab.
3. Click the name of the VPC for which you want to delete an entity.
   The **Summary** tab opens displaying the detailed information about the VPC in widgets.
4. Navigate to the respective tab like **Subnets**, **Policies** or **Routes**.
5. Select the checkbox associated with the entity you want to delete, and click **Delete** from the **Actions** dropdown menu.
6. In the confirmation dialog box, click **Delete** to delete the entity.
   Click **Cancel** to exit without deleting the entity.

CONNECTIONS MANAGEMENT

This section covers the management of network gateways, VPN connections and subnet extensions including operations like create, update and delete network gateways and VPN connections, and extending subnets.

> **Note:**
>
> You can enable network segmentation on a Layer 2 Network Extension (or extended subnet) that does not have a gateway. For more information about Layer 2 Network Extensions, see Layer 2 Network Extension on page 141. For more information, see *Segmenting a Stretched L2 Network for Disaster Recovery* in the Securing Traffic through Network Segmentation topic of the *Nutanix Security Guide*.
>
> The Layer 2 Network Extension is also known as Layer 2 Stretch.

- For information about network gateways and their management, see Network Gateway Management on page 123.
- For information about virtual private network connections, see Virtual Private Network Connections on page 134.
- For information about Layer 2 Network Extensions, see Layer 2 Network Extension on page 141.
- For information about Border Gateway Protocol (BGP) sessions, see Border Gateway Protocol Sessions on page 163.

Network Gateway Management

You can create, update or delete network gateways that use VPN, VTEP or BGP service for connections.

Creating a Network Gateway

About this task

A network gateway connects two networks together, and can be used in both VLAN and VPC networks on AHV. In other words, you can extend the routing domain of a VLAN network or that of a VPC using a connection between two gateways, one local and one remote. A network gateway pair (local and remote) may host one service such as VPN, VXLAN or BGP service that provides connectivity between the local and remote networks.

> **Note:** You can create one network gateway with only one service such as VPN, VXLAN or BGP. The same network gateway cannot host two services at the same time. Once you create a network gateway with one service, you cannot change the service. For example, if you create a network gateway with BGP service, you cannot change it to VPN service after the network gateway is created.

You can create multiple network gateways for a VPC. Since a VPC is configured only on a Prism Central, the VPC is available to all the clusters registered to that Prism Central.

> **Note:**
>
> A best practice is to configure the remote gateway before you configure the local gateway especially when the gateway configuration involves entering unique parameters like eBGP ASNs in the local and remote gateways.

There are two parts in configuring a gateway (local or remote):

- (Local only) Gateway VM which the network gateway appliance deploys when you create the local network gateway.
- Service Configuration where you configure the service that you want the (local and remote) gateway to use, like **VPN** service, **VTEP** (VXLAN) service or **BGP** service.

Perform the following steps to create a VPN, VTEP or BGP service gateway.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Select **Local** or **Remote** in the **Create Gateway** dropdown menu.
   If you select **Local** in the dropdown menu, the **Create Local Gateway** window opens. If you select **Remote** in the dropdown menu, the **Create Remote Gateway** window opens.

4. Provide the necessary values in the respective fields as described in the table.
   For example, if you select **Local** in the dropdown menu, then the **Create Local Gateway** window opens. Provide the necessary values in the respective fields as described in the table.

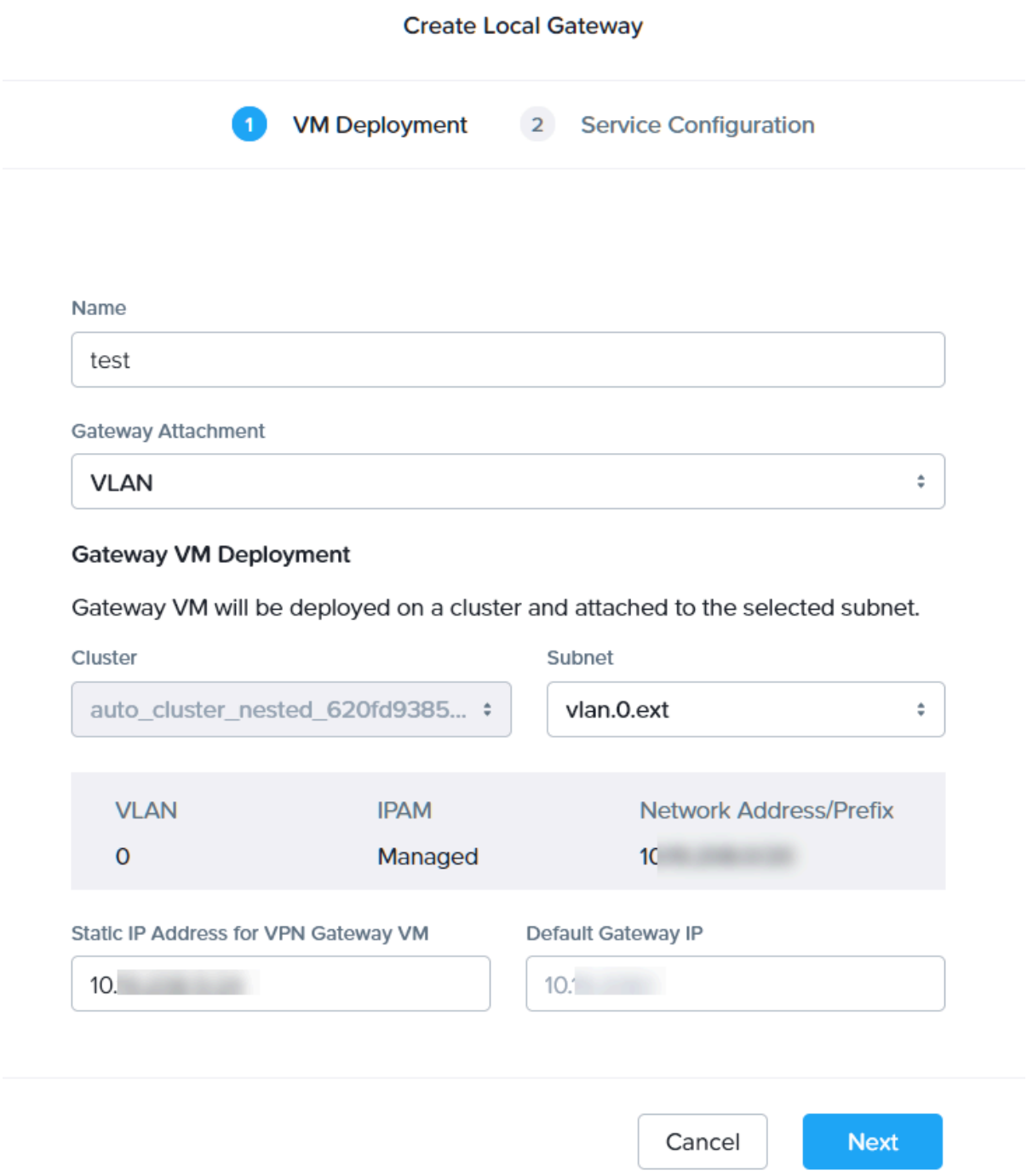


Figure 50: Sample Create Local Gateway - VM Deployment

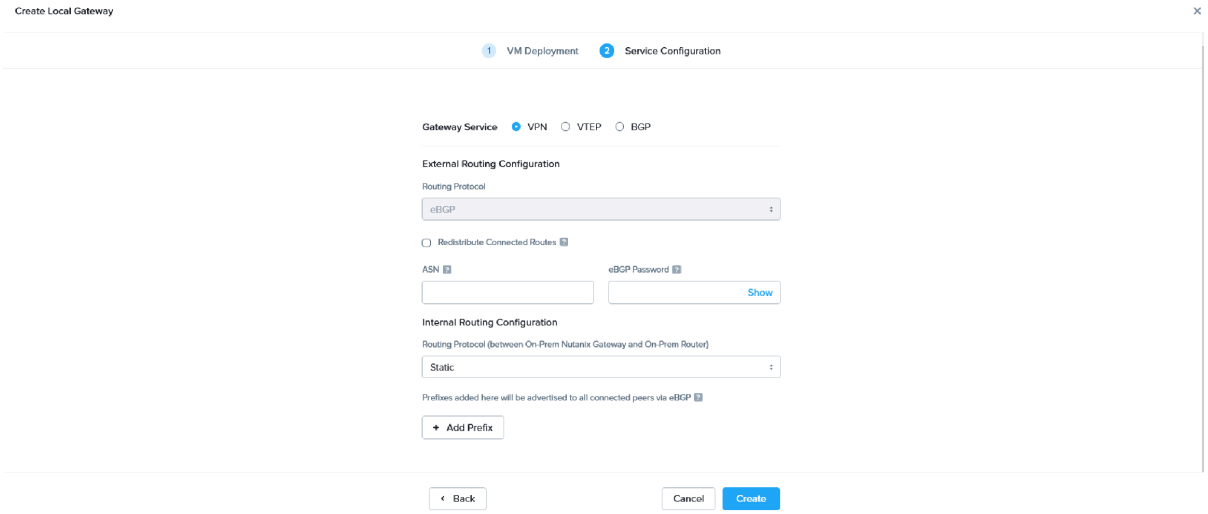


Figure 51: Sample Create Local Gateway - VPN Service Configuration

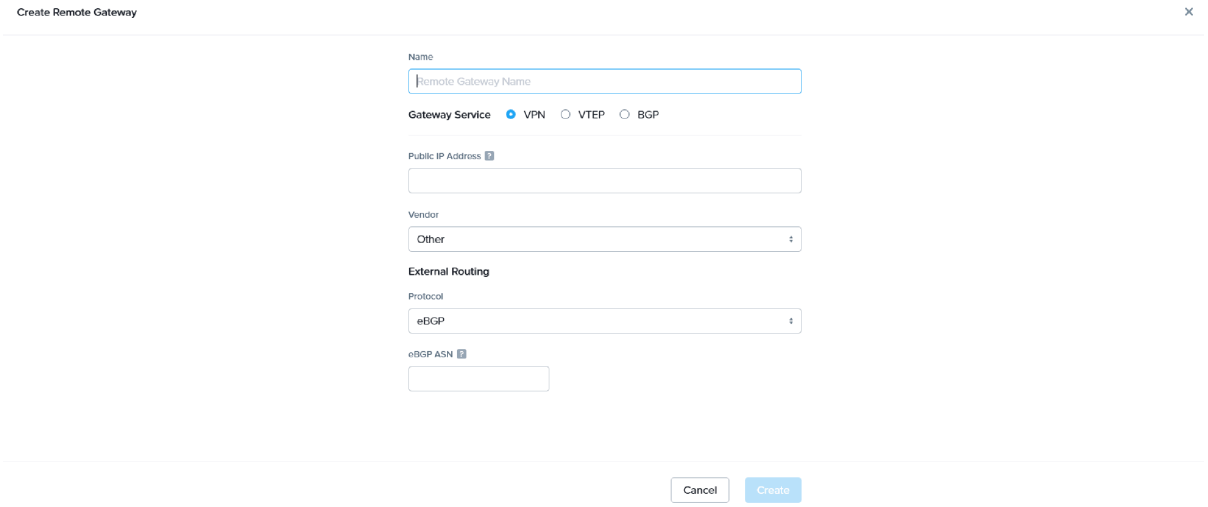


Figure 52: Sample Create Remote Gateway - VPN Gateway Service

Table 26: Local Gateway Configuration

Fields	Description	Values
VM Deployment		
Name	Enter a name for the network gateway.	(Name)

Fields	Description	Values
Gateway Attachments	(for Local gateway type only) Select the gateway attachment as `VPC` or `VLAN`. The VPN VM is deployed on a VPC VM or a cluster that has the selected VLAN respectively. **1.** If you select `VPC`, then *`VPC Attachment`* is displayed. `VPC` is the default value for the *`Gateway Attachments`* field. The Gateway VM is deployed on the cluster and associated with the VPC selected in the *`VPC Attachment`* section. *`VPC attachment`* mode provides the options of eBGP and Static routing methods for external routing (configured in the **External Routing Configuration** section). **2.** If you select `VLAN`, then the *`VLAN Attachment`* is displayed. The Gateway VM is deployed on the cluster that has the VLAN and the subnet specified in the *`VLAN Attachment`* section. *`VLAN attachment`* mode provides only the eBGP routing method for external routing.	(VLAN or VPC)
Gateway VM Deployment - VPC Attachment		
Cluster	Select the cluster on which you want to deploy the Gateway VM on.	(Name of the cluster)
VPC (If Gateway Attachment type is VPC)	Select the VPC configured on the selected cluster that you want to use for the Gateway VM deployment.	(Name of the VPC selected)
Floating IP (Optional)	Select a floating IP for the network gateway configuration. If you do not select a floating IP address then Prism Central allocates a floating IP automatically. This allocated floating IP is deleted when you delete the gateway. To request floating IPs and allocate them to subnets, see Requesting Floating IPs on page 104	(IP address)
Gateway VM Deployment - VLAN Attachment		
Cluster	Select the Cluster, from the drop down list, on which you want to deploy the Gateway VM on. **Note:** Only clusters with VLANs are available in the list.	(Name of the cluster)

Fields	Description	Values
Subnet	Select the subnet you want to attach the Gateway VM to, from the drop down list. **Note:** The list includes all the subnets you created on the selected cluster. After you select the subnet, the details of the subnet are displayed in a box below the **Subnet**field. The details include: VLAN ID, IPAM type being Managed or Unmanaged, and Network Address with Prefix.	(Name of the VLAN subnet)
Static IP Address for VPN Gateway VM	Enter the static IP address that the Gateway VM needs to use.	(IP Address with Prefix)
Default Gateway IP	Enter the default gateway IP of the subnet for the Gateway VM.	(IP Address)
Service Configuration		
Gateway Service	Select the gateway service you want to use for the gateway.	(VPN or VTEP)
VPN Service Configuration - External Routing Configuration (This section is available for VLAN and VPC attachment types)		
Routing Protocol	1. For `VPC` gateway attachments: Select `Static` for static routing. **Note:** You need to create static routes for external routing and attach the route to the VPC selected in this configuration. For more information, see Creating Static Routes on page 117. 2. Select `eBGP` for eBGP based external routing. 3. For `VLAN` gateway attachments: External routing protocol is pre-set to `eBGP`. You cannot change the routing protocol.	(Static or eBGP)
Redistribute Connected Routes (Applicable only if VLAN type gateway attachment is selected)	(`VLAN` only) Select this checkbox to enable the redistribution of connected routes into the eBGP.	(Check mark or blank)
ASN (Only available if eBGP routing protocol is selected)	(For `eBGP` only) Enter the ASN for your on-premises gateway. If you do not have a BGP environment in your on-premises site, you can choose any number. For example, you can choose a number in the 65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs. ASN must be distinct in case of eBGP.	(Number)

Fields	Description	Values

eBGP Password	(For `eBGP` in `Local` gateway type only) Enter the eBGP password for the eBGP route.	Password: The password must be between 1 and 80 characters.
		• Characters allowed for Pre-Shared Key for IPSec
		  • a-z
		  • A-Z
		  • 0-9
		  • ~ ! @ # % ^ & * ( ) _ - + = : ; { } [ ] | < > , . / ? $
		  • Password length: Minimum 1 and maximum 64 characters.
		• Characters allowed for BGP passwords
		  • a-z
		  • A-Z
		  • 0-9
		  • ~ ! @ # % ^ & * ( ) _ - + = : ; { } [ ] | < > , . / ? $
		  • Password length: Minimum 1 and maximum 80 characters.

VPN Service Configuration - Internal Routing Configuration (This section is available for VLAN attachment type only.)		

Fields	Description	Values
Routing Protocol (Between On-prem Gateway and On-prem Router)	Select the **Routing Protocol** to be used between on-premises Nutanix gateway and on-premises router. You can select: • `Static`: Select this protocol to provide a static route configuration for the VLAN gateway. • `OSPF`: Select this protocol to provide an OSPF routing configuration for the VLAN gateway. • `iBGP`: Select this protocol to provide a iBGP route configuration for the VLAN gateway. **Note:** For iBGP, the ASN must be the same between the Gateway appliance and the peer iBGP, when iBGP is selected as the internal routing protocol.	(Static or OSPF or iBGP)
+Add Prefix (Applicable to Static routing)	(For `Static` routing selected in **Routing Protocol**) Click this to enter a `Local Prefix` and click the check mark under **Actions** to add the prefix. If you click the X mark under **Actions**, the local prefix you entered is not added. The prefixes you add are advertised to all the connected peers via eBGP. The prefix must be a valid IP address with the host bits not set. You can add multiple local prefix IP addresses.	(prefix like /24)
Area ID (Applicable to OSPF protocol)	(OSPF only) Enter the OSPF area ID in the IPv4 address format.	(IPv4 address format)
Password Type	(OSPF only) Select the password type you want to set for the OSPF route. The options are: 1. `MD5`: Select this option to encrypt the packets with MD5 hash that can be decrypted with the MD5 password at the destination. 2. `Plain Text`: Select this option to set a clear-text password. 3. `None`: Select this if you do to set an open route without password protection	(Password)

Fields	Description	Values
Password	(OSPF only) Enter a password for the MD5 or Plain Text password type you select in the *Password Type* field. • For MD5: The password must be 1-16 characters long. Characters allowed for OSPF passwords (MD5) • a-z • A-Z • 0-9 • For Plain Text: The password must be 1-8 characters long. Characters allowed for OSPF passwords (Plain text): a-z.	
Peer IP (for iBGP)	Enter the IP Address of the On-prem router used to exchange routes with the network gateway.	(IP Address)
Password	Enter a password with 1-80 characters.	(Password)
VTEP Service Configurations		
VxLAN (UDP) Port	The default value provided is 4789. Do not change this.	(Number. Default value is 4789)
BGP Service Configurations		
Serviced VPC	Select the VPC that you want to connect using the local BGP gateway.	VPC
eBGP ASN	Enter the ASN for your local gateway. You can choose any number. For example, you can choose a number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other local or remote BGP ASNs. Once you enter the ASN, you cannot change the ASN using the **Update Gateway** page.	(Number)

Table 27: Remote Gateway Configuration

Fields	Description	Values
Name	Enter a name for the network gateway.	(Name)
Gateway Service	Select the gateway service you want to use for the gateway.	(VPN or VTEP)
VPN Service Configurations		

Fields	Description	Values
Public IP Address	Enter the public IP address of the remote endpoint. If a Floating IP is not selected, a new Floating IP is automatically allocated for the Gateway. These allocated IP addresses are deleted when the network gateway is deleted.	(IP Address)
Vendor	Select the vendor of the third party gateway appliance.	(Name of Vendor)
External Routing Protocol	**1.** Select `Static` for static routing. **Note:** You need to create static routes for external routing and attach the route to the VPC selected in this configuration. For more information, see Creating Static Routes on page 117. **2.** Select `eBGP` for eBGP based external routing.	(Static or eBGP)
eBGP ASN (Only available if eBGP routing protocol is selected)	(For `eBGP` only) Enter the ASN for your on-premises gateway. If you do not have a BGP environment in your on-premises site, you can choose any number. For example, you can choose a number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs. ASN must be distinct in case of eBGP.	(Number)
VTEP Service Configurations		
VTEP IP Address	Enter VTEP IP Addresses of the remote endpoints that you want to create the gateway for. You can add IP addresses of multiple endpoints in one remote gateway.	(Comma separated list of IP Addresses)
VxLAN (UDP) Port	The default value provided is 4789. Do not change this.	(Number. Default value is 4789)
BGP Service Configurations		
Service IP Address	Enter the IP Address of the remote endpoints that you want to create the gateway for.	(IP address)
eBGP ASN	Enter the ASN for the remote gateway. You can choose any number. For example, you can choose a number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs. You can modify the ASN using the **Update Gateway** page.	(Number)

5. Click **Create**.
   The gateways you create are displayed in the **Gateways** page.

Updating a Network Gateway

You can update a network gateway using the **Update Gateway** window.

About this task

Perform the following steps to update a gateway.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Select the checkbox associated with the gateway you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update Gateway** window opens.
4. Update the necessary values in the respective fields.
   The fields in the **Update Gateway** window is identical to the fields in the **Create Gateway** window. For more information, see Creating a Network Gateway on page 123.

   > **Note:** You cannot modify some parameters. Such parameters are greyed and in-actionable. If you need to modify such parameters, consider creating a new gateway with the appropriate parameters and deleting the current gateway.

5. Click **Save**.

Deleting a Network Gateway

About this task

Perform the following steps to delete a gateway.

> **Important:** You must first delete all the VPN or VTEP connections, BGP sessions or subnet extensions associated with the gateway to be able to delete a network gateway.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Select the checkbox associated with the gateway you want to delete, and click **Delete** from the **Actions** dropdown menu.
4. In the confirmation dialog box, click **Delete** to delete the gateway.
   Click **Cancel** to exit without deleting the gateway.

Virtual Private Network Connections

Virtual Private Network

You can use the Nutanix VPN solution to set up VPN between your on-premises clusters, which exist in distinct routing domains that are not directly connected. These distinct routing domains could either be VPCs within the same cluster or remote clusters or sites.

If you need to connect one Nutanix deployment in one site to another deployment in a different site, you can create a VPN endpoint in each of the sites. A VPN endpoint consists of a local VPN gateway, remote VPN gateway and VPN connection. Local VPN gateway can be instantiated in a VPC context or a legacy VLAN context. Launching the VPN gateway within a VPC allows stretching of the VPC. For example, in the figure, the Blue VPC is stretched between two sites with a VPN.

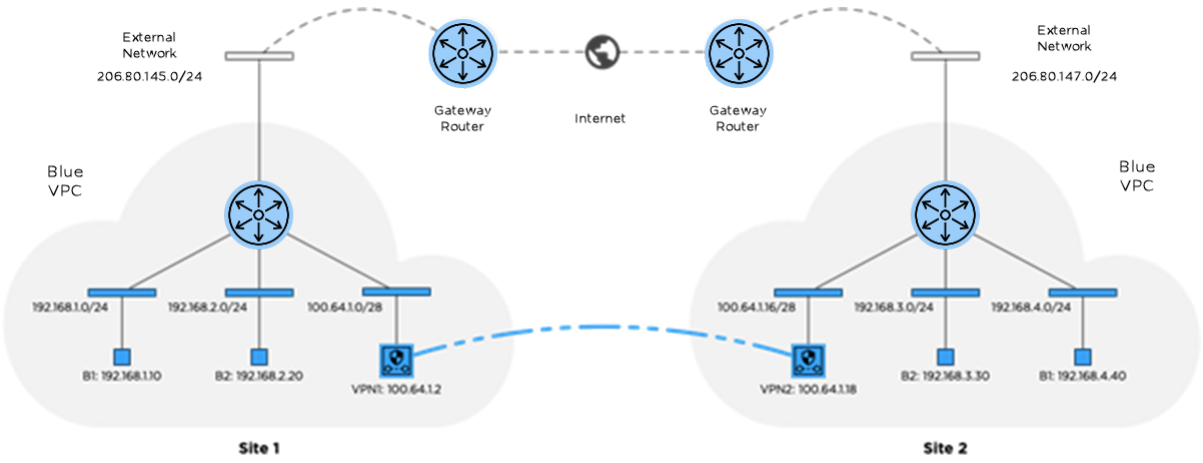


Figure 53: VPN Working

VPN connections are useful in connecting two points. You can connect two VPCs in the same cluster using a VPN or VPCs in different clusters in the same site. However, VPN connection can connect only one endpoint to another endpoint. Flow virtual networking based VPN service allows you to only connect two endpoints that use Nutanix VPN based gateway service.

Virtual Tunnel End Points Based Network Extensions

To connect one endpoint to multiple endpoints or third party (non Nutanix) networks, use VXLAN (Virtual Extensible LAN) based Virtual Tunnel End Point (VTEP) service based subnet extensions. For more information, see Layer 2 Network Extension Over VTEP on page 149.

Virtual Network Connection Using BGP

Border Gateway Protocol (BGP) works in Layer 4 (application layer). It works on top of TCP at layer 2. Flow Virtual Networking allows you to create and use BGP gateways and connections at layer 3 to connect two clusters for purposes including disaster recovery.

VPN Workflow

If you need to connect one Nutanix deployment in one site to another deployment in a different site, you can create a VPN endpoint in each of the sites. A VPN endpoint consists of a local VPN gateway, remote VPN gateway and VPN connection. You can configure multiple VPN endpoints for a site.

Each endpoint must have configurations for a local VPN gateway, remote VPN gateway (pointer information for the peer local VPN in the remote site endpoint) and a VPN connection (connecting the two endpoints). Then, based on the VPN connection configuration as initiator or acceptor, one endpoint initiates

a tunnel and the endpoint at the other end accepts the tunnel connection and, thus, establishes the VPN tunnel.

1. Gateways: Every VPN endpoint for each site consists of two VPN gateway configurations - Local and Remote.

   Local gateway is a VM that runs the VPN protocols (IKEv2, IPSec) and routing (BGP and OSPF). Remote gateway is a pointer - database entry - that provides information about the peer remote VPN endpoint. One of the key information contained in the remote gateway is the source IP of the remote VPN endpoint. For security reasons, the local VPN gateway will accept IKEv2 packets originating only from this Source IP.

   VPN gateways are of the following types:

   - On premises Nutanix VPN Gateway: Represents the VPN gateway appliance at your on-premises local or remote site if you are using the Nutanix VPN solution.
   - On premises Third Party Gateway: Represents the VPN gateway appliance at your on-premises site if you are using your own VPN solution (provided by a third-party vendor).

     To configure third party VPN Gateways, see the relevant third party documentation.
2. VPN Connection: Represents the VPN IPSec tunnel established between local gateway and remote gateway. When you create a VPN connection, you need to select two gateways between which you want to create the VPN connection.

VPN appliances perform the following:

1. Implementation of IKEv2 and IPSec protocols.
2. Routing: Between remote sites, Flow virtual networking advertises prefixes using eBGP. Optionally it uses Static routing. Within a site, Flow virtual networking uses iBGP or OSPF to share prefixes between the Nutanix VPN appliance and the edge router.

Prerequisites for VPN Configurations

General Requirements

- Ensure that you have enabled Flow virtual networking with microservices Infrastructure.
- Ensure that you have floating IP addresses when you create VPN gateways.

  Flow virtual networking automatically allocates a floating IP to a VPN gateway if you do not provide one during the VPN gateway creation. To provide floating IP during the VPN gateway creation, you can request floating IPs. For more information, see Requesting Floating IPs on page 104.
- Ensure that you have one of the following, depending on whether you are using iBGP or OSPF:
  - Peer IP (for iBGP): The IP address of the router to exchange routes with the VPN gateway VM.
  - Area ID (for OSPF): The OSPF area ID for the VPN gateway in the IP address format.
- Nutanix recommends setting the guest VM NIC MTU to 1,356 bytes for all VMs inside a VPC that send traffic over Nutanix VPN connections. This prevents fragmentation and accounts for the encapsulation overhead for VPN connections in a VPC. See the Flow Virtual Networking MTUs table.

  Accounting for the 1356 byte MTU: Assuming a 1,500 byte network MTU, subtract 58 bytes for Geneve VPC encapsulation and 86 bytes for IPsec encapsulation, leaving 1,356 bytes for guest VM frames.

- Ensure that you have the following details for the deployment of the VPN gateway VM:
  - Public IP address of the VPN Gateway Device: A public WAN IP address that you want the on-premises gateway to use to communicate with the Xi VPN gateway appliance.
  - Static IP Address: A static IP address that you want to allocate to the VPN gateway VM. Use a floating IP address requested as the static IP address.
  - IP Prefix Length: The subnet mask in CIDR format of the subnet on which you want to install the VPN gateway VM. You can use an overlay subnet used for a VPC and assigned to the VM that you are using for the VPN gateway.
  - Default Gateway IP: The gateway IP address for the on-premise VPN gateway appliance.
  - Gateway ASN: ASN must not be the same as any of your on-premises BGP ASNs. If you already have a BGP environment in your on-premises site, the customer gateway is the ASN for your organization. If you do not have a BGP environment in your on-premises site, you can choose any number. For example, you can choose a number in the 65000 range.

Ports and Protocols

Nutanix deploys a number of ports and protocols in its software. These ports must be open in the firewalls to enable Flow Virtual Networking to function. To see the ports and protocols used Flow Virtual Networking, see Ports and Protocols.

Endpoints and Terminations

The following endpoints and terminations occur in the course of Flow virtual networking based connections. For information about creating, updating or deleting VPN connections, see Connections Management on page 123.

> **Note:** In a VPN connection do not configure both the gateways (local gateway and remote gateway) in an endpoint as Initiators or as Acceptors. If you configure the local gateway as Initiator then configure the remote gateway as Acceptor in one endpoint and vice-versa in the (other) remote endpoint.

VPN Endpoint Behind a Network Address Translation or Firewall Device

In this scenario, the IPSec tunnel terminates behind a network address translation (NAT) or firewall device. For NAT to work, open UDP ports 500 and 4500 in both directions.

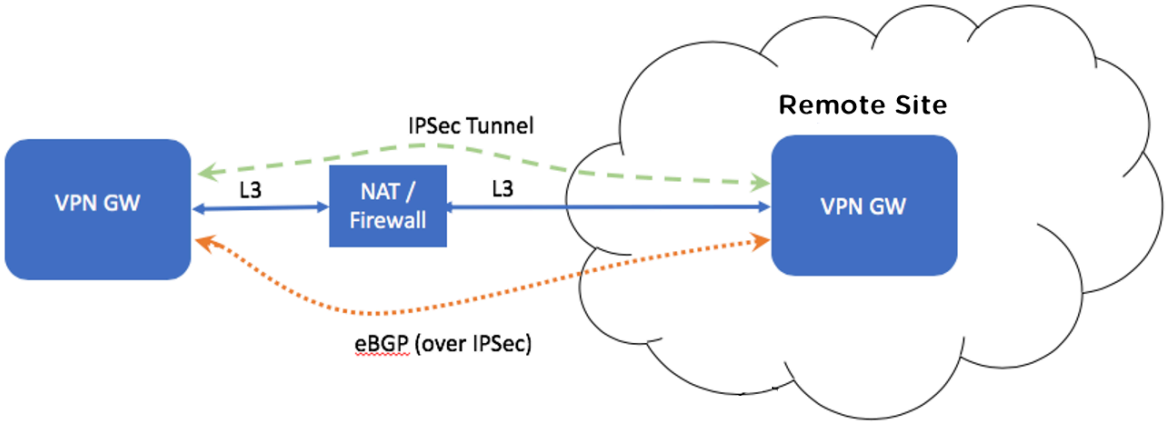


Figure 54: VPN Endpoint Behind NAT or Firewall

Things to do in NAT	Things to do in on-premises VPN GW
Open UDP ports 500 and 4500 on both directions	Enable the business application policies to `Allow` the commonly-used business application ports.

IPSec Terminates on the Firewall Device

In this scenario, you do not need to open the ports for NAT (500 and 4500).

However, enable the on-premises VPN gateway to allow the traffic from the PC subnet to the advertised load balancer route where the Source port is any and the Destination port may be in the range of 1024-1034.

The PC subnet refers to the subnet where your Prism Central is running.

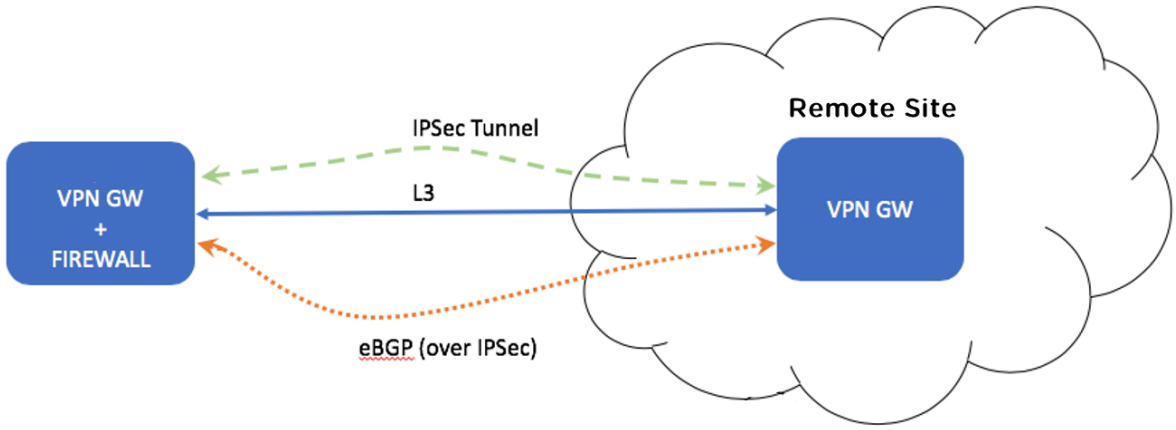


Figure 55: Tunnel Terminates on NAT or Firewall

Creating a VPN Connection

About this task

Create a VPN connection to establish a VPN IPSec tunnel between VPN gateways in your on-premises site. Select the gateways between which you want to create the VPN connection.

Perform the following steps to create a VPN connection.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **VPN Connections** tab.
   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Click the **Create VPN Connection**.

5. In the **Create VPN Connection** window, provide the values in the respective fields.

Fields	Description and Values
Name	Enter a name for the connection.
VPN Connection	
IPSec Secret	Enter a secret password for the IPSec connection. To see the password, click **Show**. To hide the password, click **Hide**.
Local Gateway	Select the connection parameters on the local gateway as Initiator or Acceptor of VPN Tunnel connections.
VPN Gateway	Select the appropriate VPN Gateway as the local gateway for the VPN connection
VTI Prefix - Local Gateway	Enter a IPv4 Address with /<prefix>. Example: 10.25.25.2/30. This is the *VPN Tunnel Interface* IP address with prefix for the local gateway. The subnet for this IP address must be a /30 subnet with two usable IP addresses. One of the IP addresses is used for Local Gateway. Use the other IP address for the Remote Gateway.
Connection Handshake	This defines the type of handshake that the connection must use. There are two types of connection handshakes: 1. `Initiator`: The local VPN gateway acts as the initiator of the connection and thus initializes the VPN tunnel. 2. `Acceptor`: The local VPN gateway accepts or rejects incoming connection requests from other gateways. **Note:** In a VPN connection do not configure both the gateways (local gateway and remote gateway) in an endpoint as Initiators or as Acceptors. If you configure the local gateway as Initiator then configure the remote gateway as Acceptor in one endpoint and vice-versa in the (other) remote endpoint.
Remote Gateway	For a specific VPN connection, set the remote gateway as Initiator or Acceptor when you configure the VPN connection on the Remote Gateway.
VPN Gateway	Select the appropriate VPN Gateway as the remote gateway for the VPN connection.
VTI Prefix - Remote Gateway	The VPN Tunnel Interface IP address with prefix for the local gateway. Provide a IPv4 Address with /<prefix>. Example: 10.25.25.2/30. This is the *VPN Tunnel Interface* IP address with prefix for the local gateway. The subnet for this IP address must be a /30 subnet with two usable IP addresses. One of the IP addresses is used for Local Gateway. Use the other IP address for the Remote Gateway.
Advanced Settings	Set the traffic route priority for the VPN connection. The route priority uses Dynamic route priority because the priority is dependent on the routing protocol configured in the VPN gateway.
Route Priority - Dynamic Route Priority	Set the route priority as an integer number. The greater the number, higher is the priority.

6. Click **Save**.
   The VPN connection you create is displayed in the **VPN Connections** page.

What to do next

The VPN connection you create is displayed in the **VPN Connections** page. Optionally, create static routes from the VPCs to the VPN connection. See *What to do next* section in VPN Connection within Same Prism Central on page 140 for information.

Updating VPN Connection

About this task

Perform the following steps to update a VPN connection.

You can open the **Update VPN Connection** dialog box. The parameters in the **Update VPN Connection**dialog box are the same as those in the **Create VPN Connection** dialog box.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **VPN Connections** tab.
   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Select the VPN Connection you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update VPN Connection** window opens.
5. Update the necessary values in the respective fields.

   The fields in the **Update VPN Connection** window is identical to the fields in the **Create VPN Connection** window. For more information, see Creating a VPN Connection on page 137.
6. Click **Save**.

Deleting a VPN Connection

About this task

Perform the following steps to delete a VPN connection.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **VPN Connections** tab.
   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Select the VPN Connection you want to delete, and click **Delete** from the **Actions** dropdown menu.
5. In the confirmation dialog box, click **Delete** to delete the VPN connection.
   Click **Cancel** to exit without deleting the connection.

VPN Connection within Same Prism Central

You can connect two VPCs within the same Prism Central availability zone using a VPN connection.

About this task

Assume that you have created two VPCs named **vpc-a** and **vpc-b** with overlay subnets named **subnet-a** and **subnet-b**.

To connect the two VPCs within the same Prism Central using a VPN connection, do the following.

Procedure

1. Do the following for local gateways:
   a. Create a local VPN gateway with dynamically assigned address for **vpc-a**, for example, named **local-vpn-a**. Note or write down the assigned IP address.
   b. Create a local VPN gateway with dynamically assigned address for **vpc-b**, for example, named **local-vpn-b**. Note or write down the assigned IP address.

   For more information about creating a VPN gateway, see Creating a Network Gateway on page 123.
2. Do the following for remote gateways:
   a. Create a remote VPN gateway with the IP address noted in 1.a on page 140 for **vpc-a**, for example, named **remote-vpn-a**.
   b. create a local VPN gateway with the IP address noted in 1.b on page 140 for **vpc-b**, for example, named **remote-vpn-b**.

   For more information about creating a VPN gateway, see Creating a Network Gateway on page 123.
3. Create a VPN connection between **vpc-a** and **vpc-b** named, for example, **vpn-conn-a-to-b**.
   Ensure that the VTI IP addresses for the local and remote gateways is unique with /30 prefix.

   > **Note:** The *VPN Tunnel Interface* IP address with prefix for the local gateway. The subnet for this IP address must be a /30 subnet with two usable IP addresses. One of the IP addresses is used for Local Gateway. Use the other IP address for the Remote Gateway.

   Ensure that you select **local-vpn-a** as the local gateway with **Connection Handshake** set as **Acceptor**.

   Ensure that you select **remote-vpn-b** as the remote gateway.
4. Create a VPN connection between **vpc-b** and **vpc-a** named, for example, **vpn-conn-b-to-a**.
   Ensure that the VTI IP addresses with /30 prefix for local and remote gateways are the reverse (vice versa) of what you configured for the VPN connection in previous step. For example, if in previous step you configured the VTI IP addresses as 10.20.20.5/30 for local and 10.20.20.6/30 for remote then for VPN connection in this step, configure 10.20.20.6/30 for local gateway and 10.20.20.5/30 for remote gateway respectively. These IP addresses do not need to be reachable anywhere else in the network. However, ensure that these IP addresses do not overlap with any other IP addresses assigned in the network.

   Ensure that you select **local-vpn-b** as the local gateway with **Connection Handshake** set as **Initiator**.

   Ensure that you select **remote-vpn-a** as the remote gateway.

What to do next

Optionally, create static routes for the subnets in the two VPCs to the VPN connections. The static routes ensure that the subnets communicate with the VPN connection.

For example,

- Create static routes in **vpc-a** with **Destination Prefix**: **subnet-b** (in **vpc-b**), **Next Hop**: **vpn-conn-a-to-b**
- Create static routes in **vpc-b** with **Destination Prefix**: **subnet-a** (in **vpc-a**), **Next Hop**: **vpn-conn-a-to-b**

For information about creating or updating static routes, see Updating Static Routes on page 121.

Layer 2 Network Extension

You can extend a subnet between on-premises local and remote clusters or sites (Availability Zones or AZs) to support seamless application migration between these clusters or sites.

> **Note:** One or more on-premises cluster or sites managed by one Prism Central instance is defined as an Availability Zone or AZ. In this section, Availability Zone or AZ refers to and must be understood as one or more on-premises clusters or sites managed by one Prism Central. Local AZ refers to local on-premises clusters or sites managed by a Prism Central instance and remote AZ refers to another on-premises cluster or site managed by another Prism Central instance.

With Layer 2 Network Extension, you can migrate a set of applications to the remote AZ while retaining their network bindings such as IP address, MAC address, and default gateway. Since the subnet extension mechanism allows VMs to communicate over the same broadcast domain, it eliminates the need to re-architect the network topology, which could otherwise result in downtime.

Layer 2 Network Extension assumes that there are underlying existing layer 3 connectivity already available between the Availability Zones. You can extend a subnet from a remote AZ to the primary (Local) AZ (and other remote AZs in case of VTEP-based subnet extensions)

- You can extend a Layer 2 subnet across two Nutanix AZs over either VPN or Virtual tunnel End Point (VTEP). For more information, see Layer 2 Network Extension Over VPN on page 144.
- You can extend a Layer 2 subnet between a Nutanix AZ and one or more non-Nutanix datacenters only over VTEP. For more information, see Layer 2 Network Extension Over VTEP on page 149.

You can extend subnets for the following configurations.

- **IPAM Type.** Managed and unmanaged networks.
- **Subnet Type.** On-prem VLAN subnets and VPC subnets.
- **Traffic Type.** IPv4 unicast traffic and ARP.

- **On-prem Hypervisor.** AHV and ESXi

> **Note:** If your cluster is ESXi, use vCenter Server to manually configure the port group attached to the subnet you want to extend. Set the security settings, **Promiscuous mode** and **Forged transmits** to **Accept** on the vSwitch as shown in the following image.

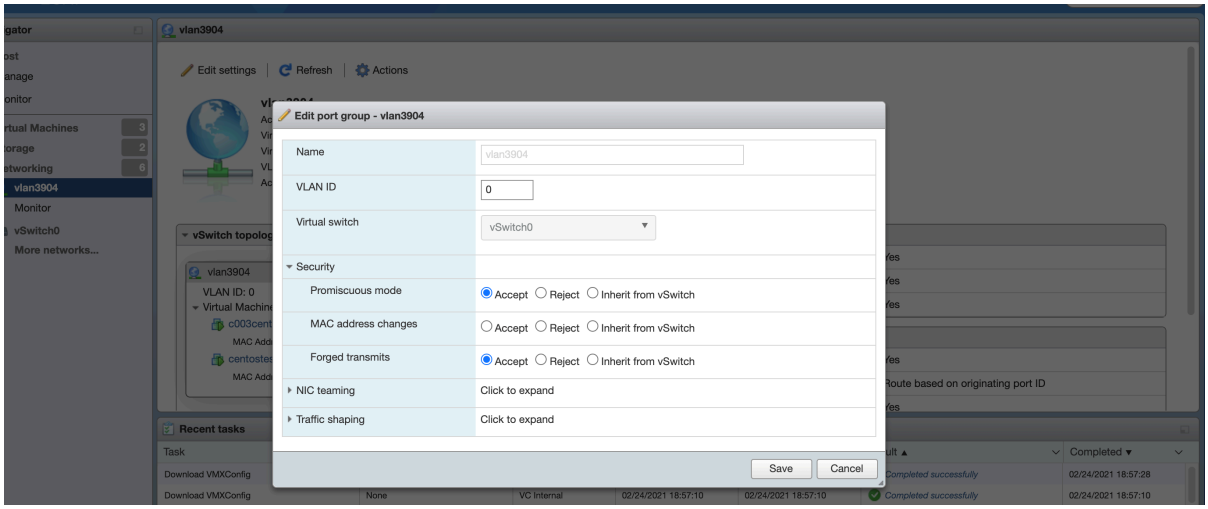


Figure 56: ESXi Host Port Group Configuration

Prerequisites for Setting Up Subnet Extension

Ensure the following before you configure Layer 2 Network Extension between your on-prem AZs.

- Ensure that the Prism Central version supports Layer 2 Network Extension. See *Features in Flow Virtual Networking* in Release Notes | Flow Virtual Networking as applicable.

  For instructions about how to upgrade a Prism Central instance through the Prism Central web console, see Prism Central Upgrade and Installation in *Prism Central Infrastructure Guide*.

- Ensure that you pair the Prism Central at the local AZ with the Prism Central at the remote AZ to use **Create Subnet Extension** wizard to extend a subnet across the AZs and facilitate bidirectional communication between these clusters or sites. Using paired availability zones it is possible to configure both VXLAN over VPN and VTEP based subnet extension. You can also extend subnets using the manual gateway and connection workflows instead of pairing the AZs.

  For instructions about how to pair the local and remote AZs, see Pairing Availability Zones on page 145.

- Ensure that you set up a default static route with `0.0.0.0/0` prefix and the External Network next hop for the VPC you use for any subnet extension. This allows NTP and DNS access for the Network Gateway appliance.

Best Practices for Subnet Extension

Nutanix recommends the following configurations to allow IP address retention for VMs on extended subnets.

- When using Nutanix IPAM ensure the address ranges in the paired subnets are unique to avoid conflict between VM IP addresses across extended subnets.

- If the source and target sites use third-party IPAM, ensure that there are no conflicting IP address assignments across the two sites.

  > **Note:** If the source and target sites use Nutanix IPAM, the Prism Central web console displays a message that indicates an IP address conflict if one exists.

- If connectivity between sites already provides encryption, consider using VTEP only subnet extension to reduce encryption overhead.
- Use the **Subnet Extension to a Third Party Data-Center** workflow in the following scenarios
  - To extend a subnet to more than one other AZ. This is also known as point to multi-point.
  - To extend subnets between clusters managed by the same Prism Central.
- To avoid tromboning or hair-pinning of traffic, provide valid gateway IP address for the local and remote sides of the subnet extension. If you want to route the traffic only from one side (local or remote, thus causing traffic tromboning or hair-pinning to that side) of the subnet extension, then provide a valid gateway IP address only on that side. See for more information.

Subnet Extension Workflow

You can manage Layer 2 Network Extension on the **Subnet Extensions** tab of the **Connectivity** page. To do this:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

- You can create point-to-point Layer 2 Network Extensions between two AZs over VPN or VTEP by opening the **Create Subnet Extension Across Availability Zones** window. See Extending a Layer 2 Subnet Over VPN on page 146 for VPN-based extensions. See Extending a Layer 2 Subnet Across Availability Zones Over VTEP on page 150 for VTEP-based extensions.
- You can create point-to-point or point-to-multipoint Layer 2 Network Extensions to third party datacenters over VTEP by opening the **Create Subnet Extension To A Third Party Data-Center** window. For more information, see Extending a Subnet to Third Party Datacenters Over VTEP on page 154.
- You can update a subnet extension that extends across AZs using the **Update Subnet Extension Across Availability Zones** window. The **Update Subnet Extension Across Availability Zones** has the same parameters and fields as the **Create Subnet Extension Across Availability Zones** window. You can open the **Update Subnet Extension Across Availability Zones** window by:
  - Selecting the subnet extended across AZs in the **Subnet Extensions** and clicking the **Update** button.
  - Clicking the subnet extended across AZs in the **Subnet Extensions** and clicking the **Update** button on the **Summary** tab.

You can update a subnet extension that extends to multiple AZs or third party datacenters using the **Update Subnet Extension To A Third Party Data-Center** window. **Update Subnet Extension To A Third Party Data-Center** window has the same parameters and fields as the **Create Subnet Extension To A Third Party Data-Center** window. You can open the **Update Subnet Extension To A Third Party Data-Center** window by:

- Selecting the subnet extended to third datacenters in the **Subnet Extensions** and clicking the **Update** button.
- Clicking the subnet extended to third datacenters in the **Subnet Extensions** and clicking the **Update** button on the **Summary** tab.

See Updating an Extended Subnet on page 161.

Layer 2 Network Extension Over VPN

Subnet extension using VPN allows seamless, secure migration to a new datacenter or for disaster recovery. VPN based Layer 2 Network Extension provides secure point to point connection to migrate workloads between Availability Zones. Consider VTEP-only subnet extension without VPN when encryption is not required.

Layer 2 Network Extension using VPN is useful:

- When the two Availability Zones (where the subnets to be extended belong) do not have any underlying secure connectivity. For example, when connecting over the Internet, VPN (IPSec) provides the necessary connectivity and encryption (security).
- Sometimes when you need to move (lift-and-shift) workloads from a VLAN subnet to a VPC subnet retaining the same VM IP addresses . You need connectivity from other subnets to workloads that have already migrated to VPC. In such cases, VPN provides the Layer 3 connectivity and encryption between the VPC segment of extended subnet to other VLAN subnets.

Prerequisites for Setting Up Subnet Extension Over VPN

- For general prerequisites to extend subnets, see Layer 2 Network Extension on page 141.
- Set up VPN gateway services and a VPN connection between local AZ and the remote AZ. The subnet extension feature supports only the Nutanix VPN solution (not a third-party VPN solution) at the both the local and remote AZs. For instructions about how to upgrade the VPN gateway VM at the local and remote clusters or sites, see Virtual Private Network Connections on page 134.

  > **Note:** Ensure that the VPN gateway version is 5.0 or higher. For instructions about how to upgrade the network gateway at the local and remote sites, see Updating a Network Gateway.

- Configure subnets with the same IP CIDR prefix at the source and target sites. For example, if the IP prefix at one site is 30.0.0.0/24, the IP prefix at the other site must also be 30.0.0.0/24. The network and mask must match at both AZs.
- Configure distinct DHCP pools for the source and target sites with no IP address overlap. Separate DHCP pools ensure no IP address conflicts occur for dynamically assigned IP addresses between the two AZs.
- Procure two free IP addresses, one from each subnet, for the Network Gateway in the subnets to be extended. These IP addresses are configured as local IP address and remote IP address for the subnet extension in the **Subnet Extension** wizard. These two free IP addresses are the externally accessible IP addresses for the local gateway, and the remote gateway. Those two usable IP addresses are already contained inside the VPN connection and must not conflict with the following:
  - DHCP pools on any of the Availability Zones.
  - Gateway IP address on any of the Availability Zones.
  - IP addresses allocated to existing user VMs on any of the Availability Zones.
  - IP addresses used by Network Gateway Management NIC subnet (IP pool 100.64.1.0/24)

Limitation

To use subnet extension over a VPN, both sites must use the VPN service of the Nutanix Network Gateway. Consider VTEP-only subnet extension to connect to non-Nutanix third party sites.

Pairing Availability Zones

About this task

> **Note:** For DRaaS, pair the on-premises AZ (Prism Central instance) only to Nutanix Cloud AZ. For reverse synchronization, you need not pair again from Nutanix Cloud AZ; Nutanix Cloud AZ captures the paring configuration from the on-premises AZ that pairs Nutanix Cloud AZ.

To pair an AZ with another AZ or Nutanix Cloud AZ, perform the following procedure at:

- Either of the on-premises AZs for DR solution between on-premises AZs
- Either the on-premises AZ or Nutanix Cloud availability zone AZ for DR solution between on-premises AZ and Nutanix Cloud availability zone.
- Either the on-premises AZ or NC2 AZ for DR solution between on-premises AZ and NC2 AZ.
- Either of the NC2 AZs for DR solution between NC2 AZs

For more information on Prism Central-based DR solution types, see Prism Central-Based Disaster Recovery Solution.

Procedure

1. Perform one of the following based on the Prism Central-based DR solution type you plan to deploy:
   - » *On-prem to on-prem AZ or on-prem AZ to NC2 AZ* – Log in to the Prism Central web console.
   - » *Nutanix Cloud AZ to on-prem AZ (DRaaS)* – Log in to the Nutanix Cloud Services portal.
   - » *NC2 AZ to NC2 AZ* – Log in to the Prism Central web console in the NC2 cluster.
2. Perform one of the following based on your choice in Step 1:
   - » *On-prem to on-prem AZ, on-prem AZ to NC2 AZ, or NC2 AZ to NC2 AZ* – Select the **Infrastructure** application from Application Switcher Function, and go to **Administration** > **Availability Zones** from the **Navigation Bar**.
   - » *Nutanix Cloud AZ to on-prem AZ (DRaaS)* – Click the Navigation icon to access the **Navigation Bar**, and go to **Administration** > **Availability Zones**.

   The **Availability Zones** page opens, displaying the paired AZs.

3. Click **Connect to Availability Zone**.
   Specify the following information in the **Connect to Availability Zone** window.

   a. Perform one of the following:

      » *(On-prem to on-prem AZ, on-prem AZ to NC2 AZ, or NC2 AZ to NC2 AZ)* **Availability Zone Type**: Select **Physical Location** from the dropdown menu.

      » *(Nutanix Cloud AZ to on-prem AZ (DRaaS))* **Availability Zone Type**: Select **XI** from the dropdown menu.

   b. *(On-prem to on-prem AZ, on-prem AZ to NC2 AZ, or NC2 AZ to NC2 AZ)* **IP Address for Remote PC**: Enter the IP address of Prism Central running on the recovery AZ.

   c. Perform one of the following:

      » *(On-prem to on-prem AZ, on-prem AZ to NC2 AZ, or NC2 AZ to NC2 AZ)* **Username**: Enter the username of Prism Central running on the recovery AZ.

      » *(Nutanix Cloud AZ to on-prem AZ (DRaaS))* **Username**: Enter the username of your Nutanix Cloud Services account.

   d. Perform one of the following:

      » *(On-prem to on-prem AZ, on-prem AZ to NC2 AZ, or NC2 AZ to NC2 AZ)* **Password**: Enter the password of Prism Central running on the recovery AZ.

      » *(Nutanix Cloud AZ to on-prem AZ (DRaaS))* **Password**: Enter the password of your Nutanix Cloud Services account.

4. Click **Connect**.
   Both AZs are paired with each other.

   When a paired AZ is unreachable due to service interruption, missing connection, or the expired access tokens on that AZ, the **Connectivity Status** of that AZ shows `Not Reachable` (see Availability Zones View) and the following alert is generated in **Alerts**.

   ```
   Availability Zone Connection Failure: The remote availability zone AZ_URL is
    unreachable.
   ```

   The disaster recovery operations might fail due to the unreachability. To make the paired AZ reachable, unpair the primary AZ with the recovery AZ and then pair it with with the recovery AZ again.

Extending a Layer 2 Subnet Over VPN

The Layer 2 Network Extension allows VMs to communicate over the same broadcast domain to a remote site or Availability Zone (AZ).

Before you begin

For information on prerequisites and best practices for extending a Layer 2 subnet, see Layer 2 Network Extension on page 141 and Layer 2 Network Extension Over VPN on page 144.

About this task

Perform the following steps to extend a subnet from the on-premises site.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **Subnet Extensions** tab.
   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.
4. Select **Create Subnet Extension** > **Across Availability Zones** .

5. In the **Create Subnet Extension Across Availability Zones** window, enter the necessary details as described in the following table.

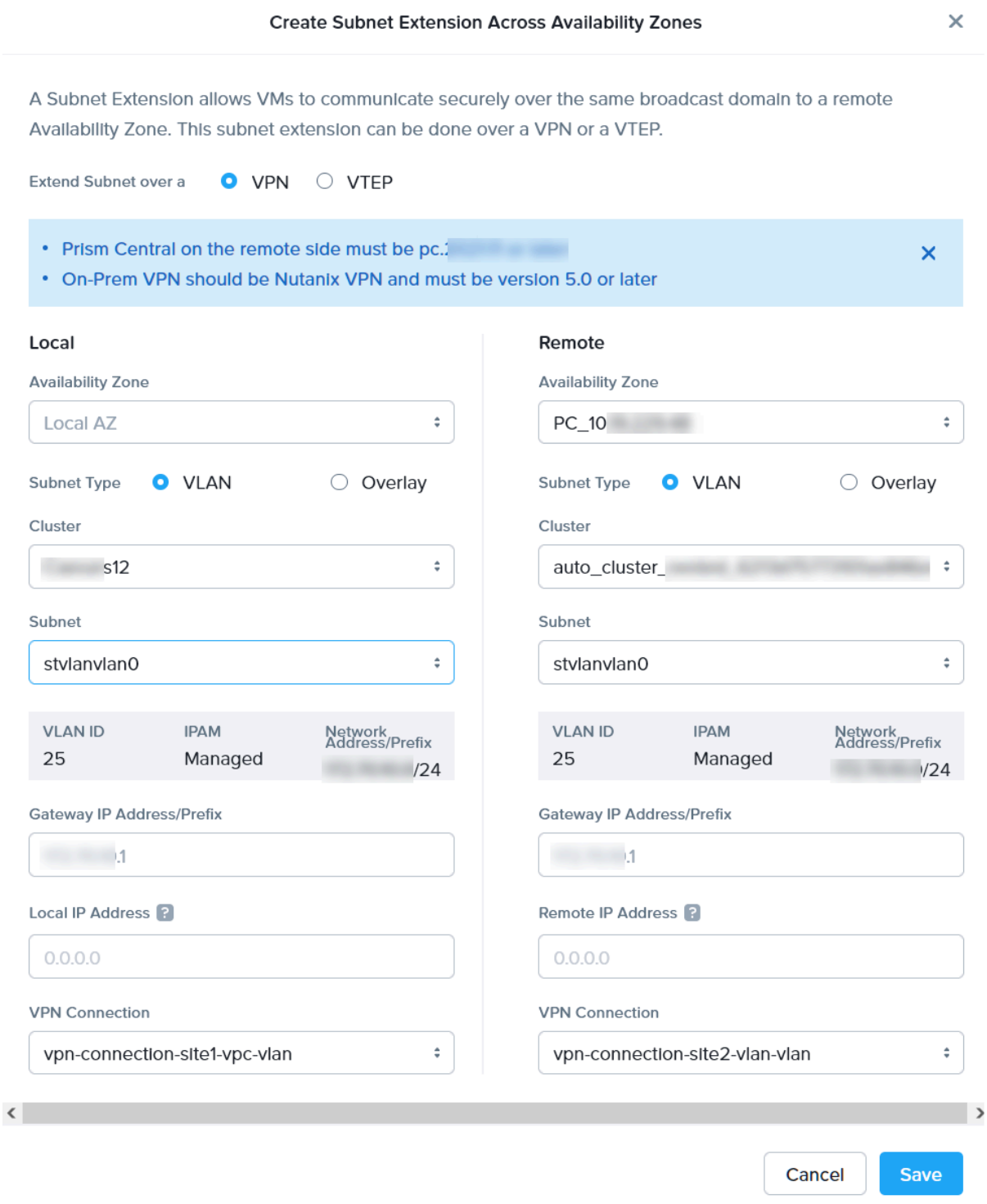


Figure 57: Create Subnet Extension Across Availability Zones

Fields	Description	Values
Extend Subnet over a	Select the gateway service you want to use for the subnet extension.	(VPN or VTEP)
Note: Configure the following fields for the **Local** and the **Remote** sides of the dialog box.		
Availability Zone	(For Local) Local AZ is pre-selected default. (For Remote) Select the appropriate AZ from the drop-down list of AZs.	(Local: Local AZ) (Remote: Dropdown list of AZs.)
Subnet Type	Select the type of subnet that you want to extend.	(VLAN or Overlay)
Cluster	Displayed if your selected VLAN subnet. Select the cluster from the dropdown list of clusters.	(Name of cluster selected from dropdown list)
VPC	Displayed if your selected Overlay subnet. Select the appropriate VPC from the dropdown list of VPCs.	(Name of VPC selected from dropdown list)
Subnet	Select the subnet that needs to be extended.	(Name of subnet selected from dropdown list)
(Network Information frame)	Displays the details of the VLAN or Overlay network that you selected in the preceding fields.	(Network information)
Gateway IP Address/Prefix	Displays the gateway IP address for the subnet. This field is already populated based on the subnet selected. For more information, see Gateway Configurations in Subnet Extensions on page 157.	(IP Address)
(Local or Remote) IP Address	Enter a unique and available IP address that are externally accessible IP addresses in **Local IP Address** and **Remote IP Address**.	(IP Address)
VPN Connection	Select the appropriate VPN Connection from the dropdown list that Flow virtual networking must use for the subnet extension. For instructions to create VPN connection, see Creating a VPN Connection on page 137.	(Name of VPN connection selected from the dropdown list)

6. Click **Save**.

   A successful subnet extension is listed on the **Subnet Extension** page.

Layer 2 Network Extension Over VTEP

Layer 2 Network Extension using Virtual tunnel End Point (VTEP) allows seamless migration to new datacenters or for disaster recovery. VTEP based Layer 2 Network Extension provides point-to-multipoint connections to migrate workloads from one Availability Zone (AZ) to multiple Availability Zones without encryption. If you need security and encryption, consider using Subnet Extension over VPN.

Subnet extension using VTEP is useful:

- When both subnets that need to be stretched are Nutanix subnets (managed or unmanaged). VTEP provides an optimized workflow to stretch the two subnets.
- When both subnets are connected over an existing private and secure link that does not need additional encryption.
- When one Nutanix subnet needs to be stretched across one or more non-Nutanix networks, sites, or datacenters. Subnet Extension with third-party VTEPs provides point-to-multipoint connectivity to third party datacenters assuming that there is underlying layer 3 connectivity between these VTEPs.

VTEP-based Layer 2 Network Extension provides the following advantages:

- Layer 2 Network Extension from one AZ to multiple AZs.
- Layer 2 Network Extension between Nutanix AZs and non-Nutanix third party VTEP-based AZs.
- The Remote VTEP Gateway is a set of endpoint IP addresses. You can add endpoint IP addresses to an existing operational Remote VTEP Gateway without stopping the subnet extension services. This on-the-fly addition enables you to extend the subnets to more AZs than originally planned, or perform maintenance, without disrupting the running services or configuring new remote VTEP gateways.

Prerequisite for Setting Up Subnet Extension Over VTEP

- For general prerequisites to extend subnets, see Layer 2 Network Extension on page 141 .
- Set up VTEP local and remote gateway services on local and remote AZs. In case of point-to-multipoint extension, ensure that you create local and remote VTEP gateways on all the remote AZs that the subnet needs to be extended to.
- For each extended subnet within the same Network Gateway appliance ensure that you have unique VxLAN Network Identifiers (VNIs) that you can use for the VTEP subnet extensions. VNI may be any number between 0 and 16777215.

Extending a Layer 2 Subnet Across Availability Zones Over VTEP

The Layer 2 Network Extension over VTEP allows VMs to communicate two Availability Zones (AZ) without a VPN connection.

Before you begin

For information on prerequisites and best practices for extending a Layer 2 subnet, see Layer 2 Network Extension on page 141 and Layer 2 Network Extension Over VPN on page 144.

About this task

Perform the following steps to extend a subnet over VTEP across two availability zones (AZs).

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **Subnet Extensions** tab.
   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

4. Select **Create Subnet Extension** > **Across Availability Zones**.

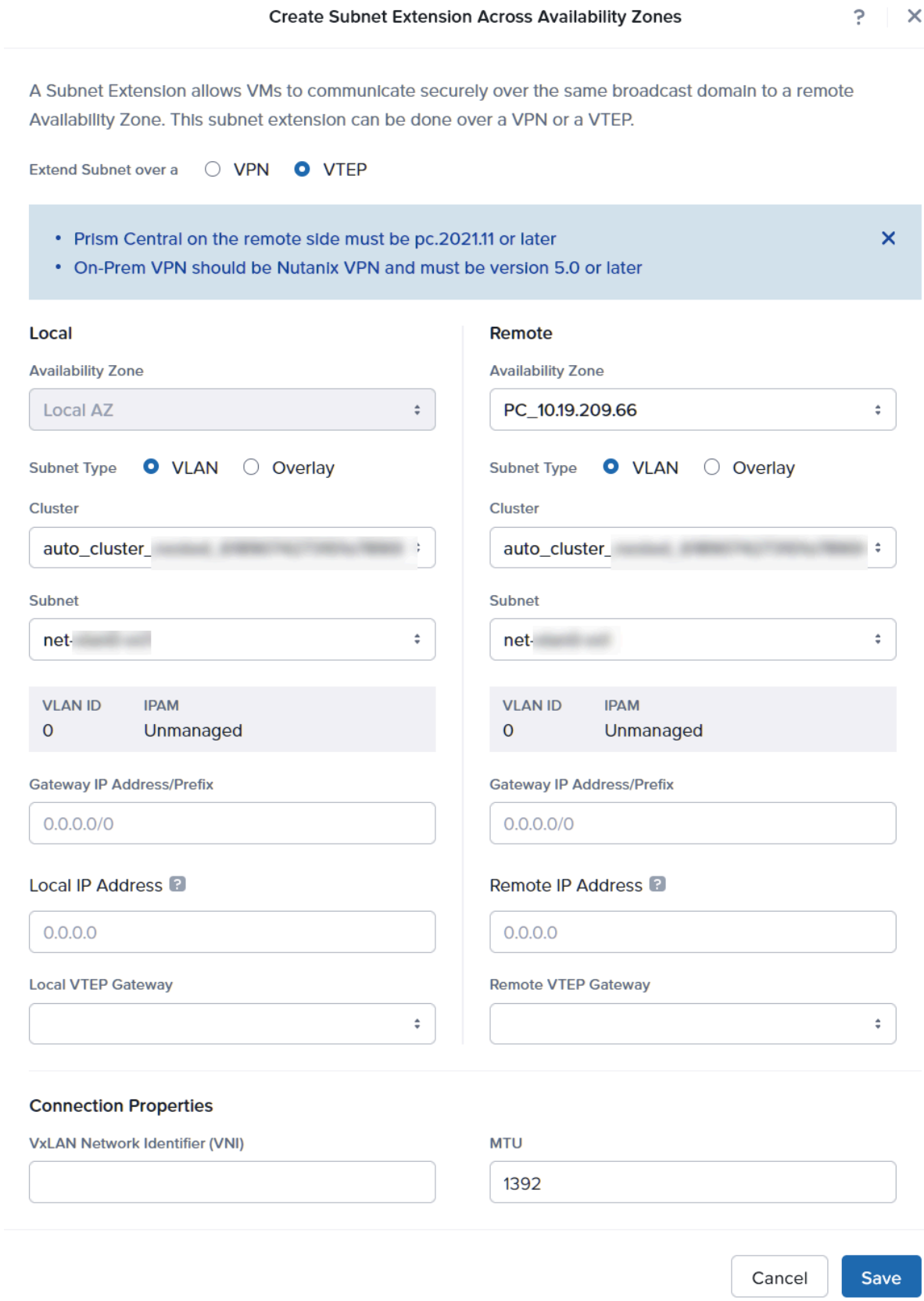


Figure 58: Example of Create VTEP Extension Across AZs with VLAN Subnet

5. For **Extend Subnet over a**, select VTEP.

6. Enter or select the necessary values for the parameters in the **Local** and **Remote** (AZ) sections as described in the table.

Parameters	Description and Value
Availability Zone	Displays the name of the paired availability zone at the local AZ.
Subnet Type	Select the type of the subnet - VLAN or Overlay that you are extending.
Cluster	Select the name of the cluster in the local AZ that the subnet is configured for.
Subnet	Select the name of the subnet at the local AZ for network. The VLAN ID and the IPAM - managed or unmanaged are displayed in the box below the **Subnet** field.
Gateway IP Address.	Enter the gateway IP address of the subnet you want to extend. Ensure that you provide the IP address in <IP-address/network-prefix> format. for example the gateway IP is 10.20.20.1 in a /24 subnet then provide the gateway IP address as `10.20.20.1/24`. **Note:** For an unmanaged network, enter the gateway IP address of the created subnet. For more information, see Gateway Configurations in Subnet Extensions on page 157.
Local IP Address	Enter a unique and available (unused) IP address from the subnet provided in **Subnet** for the Network Gateway appliance.
Remote IP Address	Enter a unique and available (unused) IP address from the subnet provided in **Subnet** for the remote Network Gateway appliance.
Local VTEP Gateway	Select the local VTEP gateway you created on the local AZ. For more information about creating VTEP gateways, see Creating a Network Gateway on page 123.
Remote VTEP Gateway	Select the VTEP gateway you created on the remote AZ. For more information about creating VTEP gateways, see Creating a Network Gateway on page 123.
Connection Properties	
VxLAN Network Identifier (VNI)	Enter a unique number from the range 0-16777215 as VNI. Ensure that this number is not reused anywhere in the local or remote VTEP Gateways.
MTU	The default MTU is 1392 to account for 108 bytes of overhead and the standard physical MTU of 1500 bytes. VPC Geneve encapsulation requires 58 bytes and VXLAN encapsulation requires 50. However, you can enter any valid MTU value for the network, taking this overhead into account. For example, if the physical network MTU and vs0 MTU are 1600 bytes, the Network Gateway MTU can be set to 1492 to account for 108 bytes of overhead. Ensure that the MTU value does not exceed the MTU of the AHV Host interface and all the network interfaces between the local and remote AZs.

7. Click **Save**.
   After the subnet is extended, the extension appears in the **Subnet Extensions** page.

Extending a Subnet to Third Party Datacenters Over VTEP

The Layer 2 Network Extension over VTEP allows VMs to communicate with multiple remote sites or Availability Zones (AZ) that may be third party (non-Nutanix) networks, or datacenters. It also provides the flexibility of adding more remote AZs to the same VTEP-based extended Layer 2 subnet. Examples of compatible VTEP gateways are switches from Cisco, Juniper, Arista, and others that support plain VXLAN VTEP termination.

About this task

Perform the following steps to extend a subnet over VTEP across multiple availability zones (AZs) or third party datacenters.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **Subnet Extensions** tab.
   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

4. Select **Create Subnet Extension** > **To A Third Party Data-Center**.

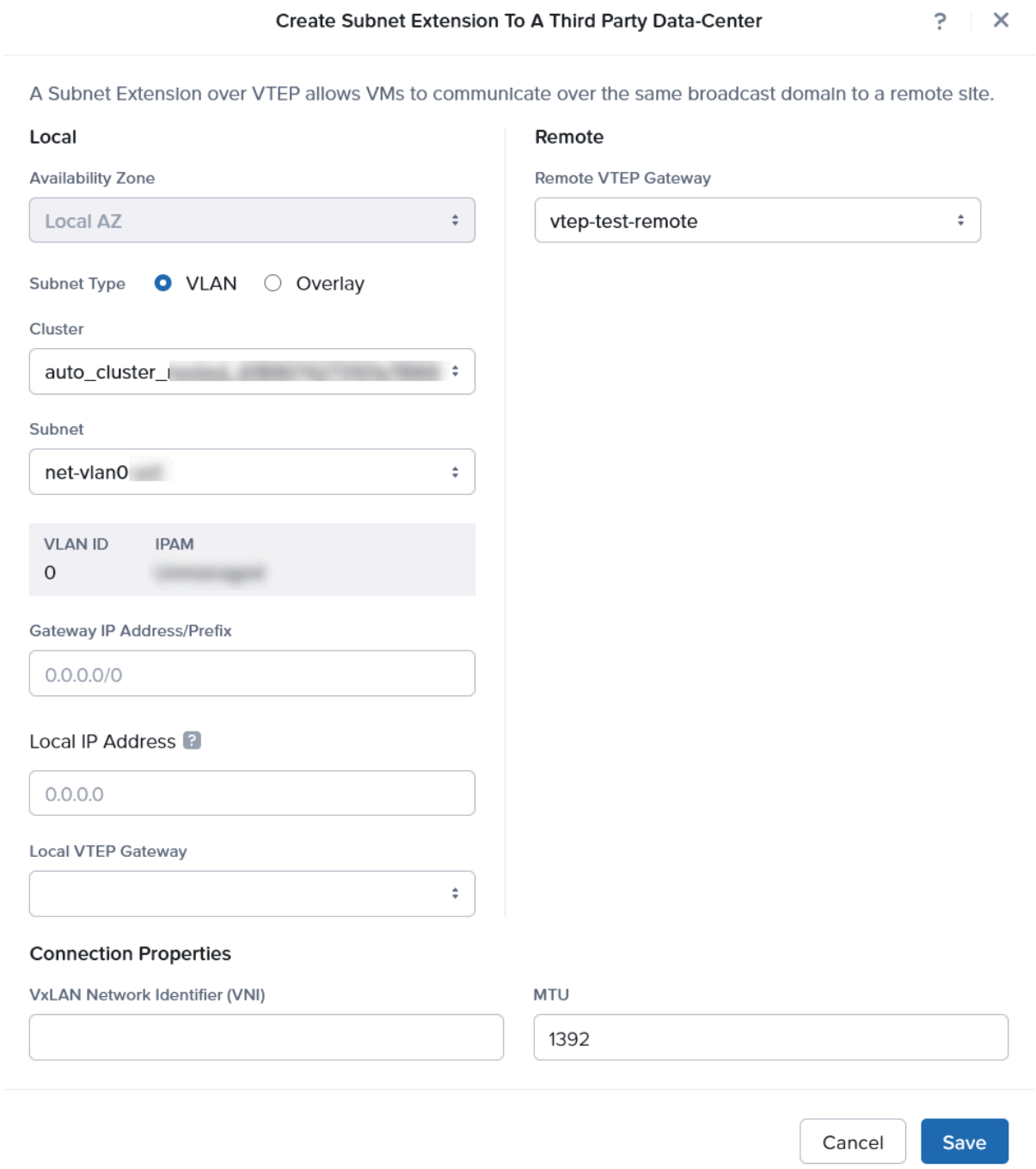


Figure 59: Example of Create VTEP Extension To A Third Party Data-Center with VLAN Subnet

5. Enter or select the necessary values for the parameters in the **Local**, **Remote** (AZ), and **Connection Properties** sections as described in the table.

Parameters	Description and Value
Local	

Parameters	Description and Value
Availability Zone	Displays the name of the paired availability zone at the local AZ.
Subnet Type	Select the type of the subnet - VLAN or Overlay that you are extending.
Cluster	Select the name of the cluster in the local AZ that the subnet is configured for.
Subnet	Select the name of the subnet at the local AZ for network. The VLAN ID and the IPAM - managed or unmanaged are displayed in the box below the **Subnet** field.
Gateway IP Address	Enter the gateway IP address of the subnet you want to extend. Ensure that you provide the IP address in <IP-address/network-prefix> format. For example the gateway IP is 10.20.20.1 in a /24 subnet then provide the gateway IP address as `10.20.20.1/24`. **Note:** For unmanaged network, enter the gateway IP address of the created subnet. For more information, see Gateway Configurations in Subnet Extensions on page 157.
Local IP Address	Enter a unique and available (unused) IP address from the subnet provided in **Subnet**.
Local VTEP Gateway	Select the local VTEP gateway you created on the local AZ. For more information about creating a remote VTEP gateway, see Creating a Network Gateway on page 123.
Remote	
Remote VTEP Gateway	Select the remote VTEP gateway you created on the local AZ. For more information about creating a remote VTEP gateway, see Creating a Network Gateway on page 123.
Connection Properties	
VxLAN Network Identifier (VNI)	Enter a unique number from the range 0-16777215 as VNI. Ensure that this number is not reused anywhere in the networks that the Prism Central and Cluster are a part of.
MTU	The default MTU is 1392 to account for 108 bytes of overhead and the standard physical MTU of 1500 bytes. VPC GENEVE encapsulation requires 58 bytes and VXLAN encapsulation requires 50. However, you can enter any valid MTU value for the network, taking this overhead into account. For example, if the physical network MTU and vs0 MTU are 1600 bytes, the Network Gateway MTU can be set to 1492 to account for 108 bytes of overhead. Ensure that the MTU value does not exceed the MTU of the AHV Host interface and all the network interfaces between the local and remote AZs.

6. Click **Save**.
   After the subnet is extended, the extension appears in the **Subnet Extensions** page.

Gateway Configurations in Subnet Extensions

This topic provides information about two gateway IP address configurations for traffic egress from an extended subnet.

In a usual subnet extension workflow using either VPN or VTEP, on the **Create Subnet Extension** or **Update Subnet Extension** page, you must provide a **Gateway IP Address/Prefix** for each side (primary or local and remote) of the subnet extension. Depending on how you want the traffic to egress the extended subnet, you can configure gateways for the subnets on each side accordingly.

Traffic Egressing the Sites from the Respective Gateways Without Tromboning

The gateway IP address is the IP address of the gateway that is created for the subnet on each side - Local Gateway and Remote Gateway respectively. This gateway of the subnet on each side allows the traffic to egress separately from the respective sides.

This means that the subnet on the local side must have a valid gateway configured to allow traffic to egress from the local subnet while the subnet on the remote side must have its own valid gateway configured to allow the traffic to egress from the remote subnet.

Example for Gateways without Traffic Tromboning

For example, you can create a subnet extension across the local and remote sides using the `subnet-local` and `subnet-remote` subnets on the local and remote sides respectively, such that the traffic egresses from each the side via the gateway configured in subnet on that side. Create subnets `subnet-local` on the primary or local side and `subnet-remote` on the remote side with the following parameters.

- For `subnet-local`
  - Network ID/Prefix: 192.168.1.0/24
  - Gateway IP Address/Prefix: 192.168.1.1/24

    This gateway provides external connection to `subnet-local`.
- For `subnet-remote`
  - Network ID/Prefix: 192.168.1.0/24
  - Gateway IP Address/Prefix: 192.168.1.1/24

    This gateway provides external connection to `subnet-remote`.

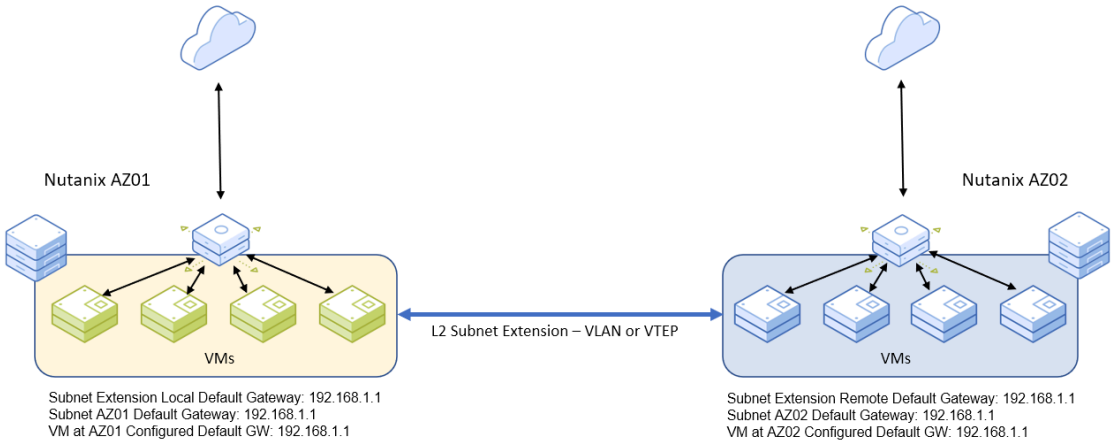


Figure 60: Gateways without Traffic Tromboning

When you configure a subnet extension, provide these gateway IP addresses for each subnet in the **Create Subnet Extension** page. This ensures that the traffic egresses each subnet via the gateway configured on that subnet.

This configuration prevents traffic tromboning or hair-pinning by ensuring that traffic egresses the subnets separately avoiding multiple hops. The VMs on `subnet-local` and `subnet-remote` use the gateways on their respective sides.

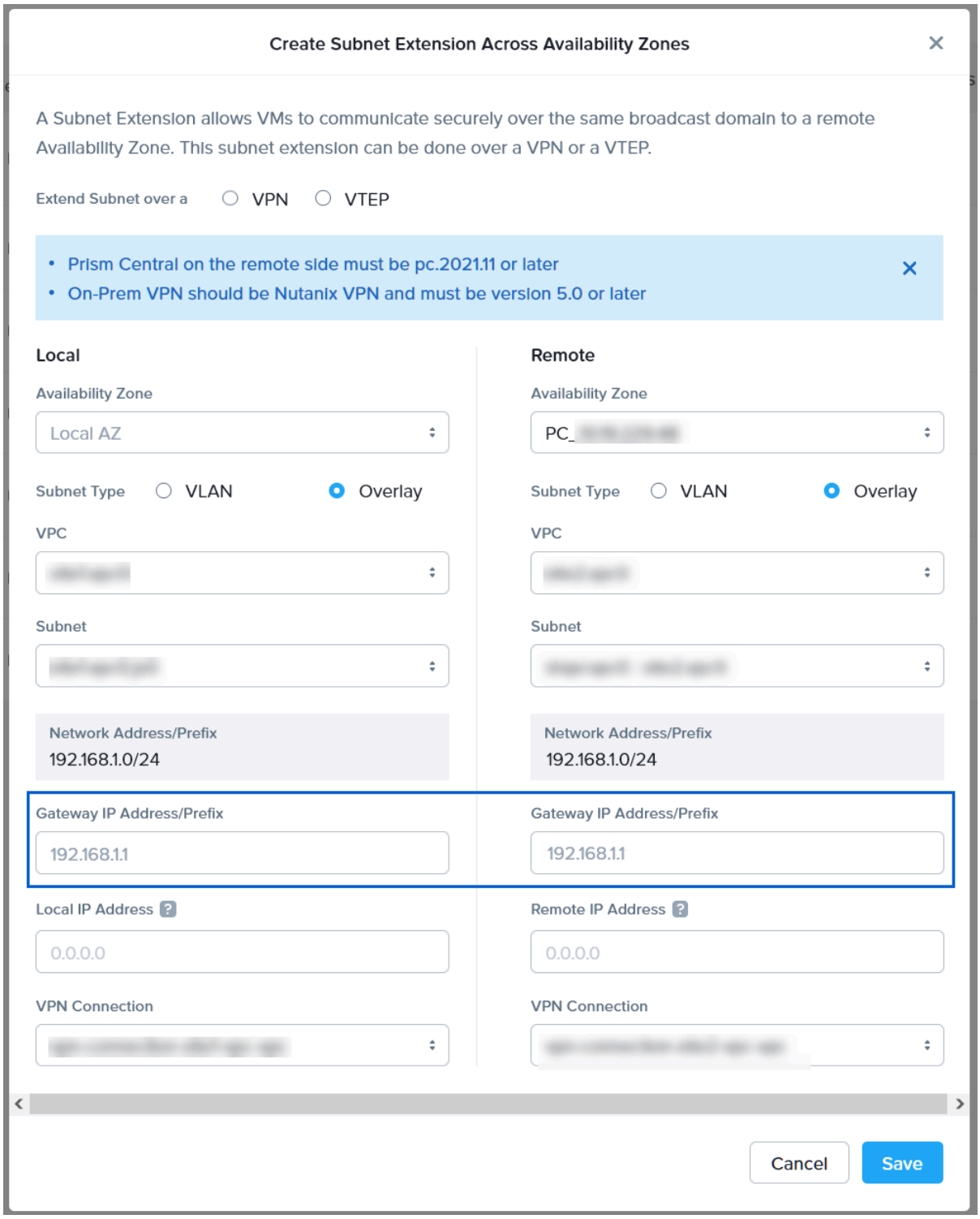


Figure 61: Creating a Subnet Extension - Gateways without Traffic Tromboning

Traffic Egressing the Sites from a Single Gateway With Tromboning

You can configure the subnets such that after extension, the subnets on both sides of the extension use only one gateway (that is configured for the subnet on any one side, either the local (primary) side or the remote side).

This means that, for the traffic from both the subnets of either side of an extended subnet to egress from only one gateway, the subnet on only one side, local side or remote side, must have a valid gateway configured and the IP address of this valid gateway is provided in the **Create Subnet Extension** page while configuring the subnet extension.

The gateway IP address specified in the **Create Subnet Extension** for the other side is an unassigned IP address.

Example for Single Gateway with Traffic Tromboning

For example, you can create a subnet extension across the local and remote sides using the `subnet-local` and `subnet-remote` subnets on the local and remote sides respectively, such that the traffic from both the sides egresses from the gateway configured in subnet `subnet-local` on the primary or local side. Create subnets `subnet-local` on the primary or local side and `subnet-remote` on the remote side with the following parameters.

- For `subnet-local`
  - **Network ID/Prefix**: 192.168.1.0/24
  - **Gateway IP Address/Prefix**: 192.168.1.1/24

    This gateway provides external connection to `subnet-local`.
- For `subnet-remote`
  - **Network ID/Prefix**: 192.168.1.0/24
  - **Gateway IP Address/Prefix**: 192.168.1.1/24

    This gateway provides an external connection to `subnet-remote`.
  - Ensure that you configure the static IP address 192.168.1.1/24 as the gateway for all the VMs on `subnet-remote`, using static routing or static IP configuration.

When you configure a subnet extension, provide these gateway IP addresses for each subnet in the **Create Subnet Extension** page as follows:

- For `subnet-local`
  - **Network ID/Prefix**: 192.168.1.0/24
  - **Gateway IP Address/Prefix**: 192.168.1.1/24

    This gateway provides external connection for `subnet-local` and `subnet-remote`.

- For `subnet-remote`
  - **Network ID/Prefix**: 192.168.1.0/24
  - **Gateway IP Address/Prefix**: 192.168.1.129/24. Ensure that, while creating `subnet-remote`, 192.168.1.129 is not configured as the gateway for `subnet-remote`.

> **Note:** Ensure that this IP address is not configured for any entity and is not eligible to be automatically assigned as a floating IP address.

> **Tip:**
>
> Since the IP address 192.168.1.129/24 does not represent a valid gateway for `subnet-remote`, this IP address (192.168.1.129/24) cannot allow egress of traffic from `subnet-remote`. Therefore, after subnet extension is created with 192.168.1.129/24 as **Gateway IP Address/Prefix** for `subnet-remote`, the traffic egressing from `subnet-remote` trombones or hairpins to `subnet-local` and egresses from **Gateway IP Address/Prefix** configured for `subnet-remote`.

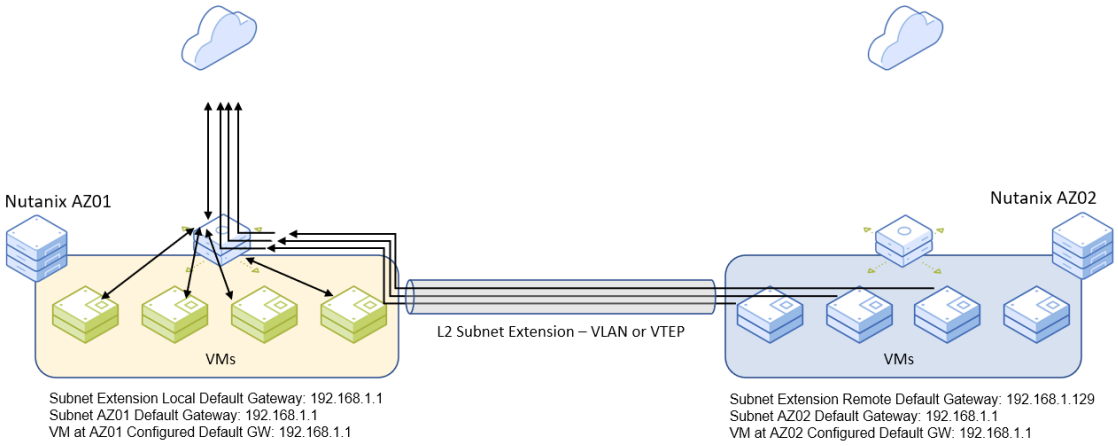


Figure 62: Gateways with Traffic Tromboning

> **Note:**
>
> This configuration creates traffic tromboning or hair-pinning by ensuring that traffic egresses the subnets from the gateway on only one side of the subnet extension, thereby adding multiple hops to the traffic egress route for the subnet that does not have a valid gateway for the extended subnet.

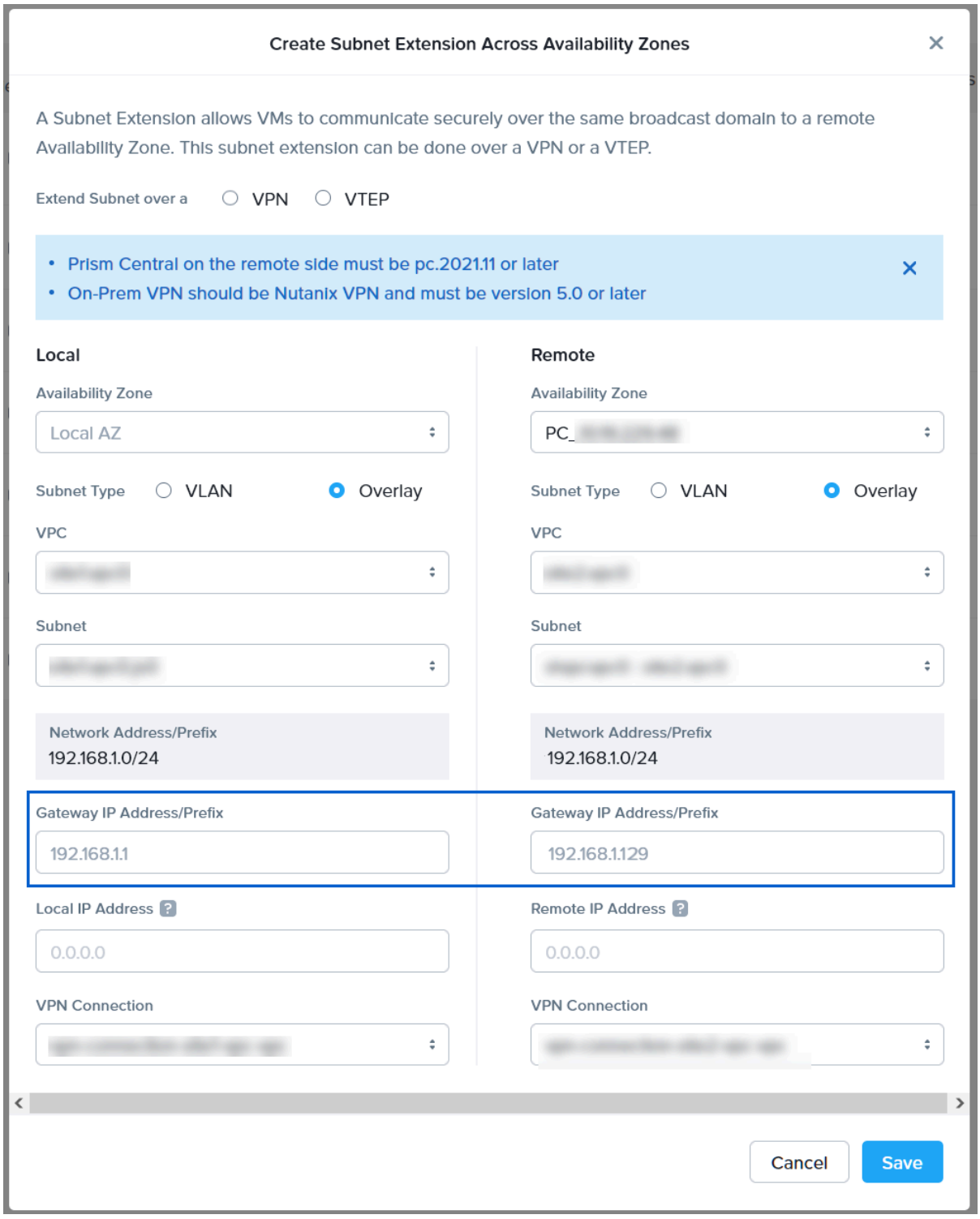


Figure 63: Creating a Subnet Extension - Gateways with Traffic Tromboning

Updating an Extended Subnet

The *Update Subnet Extension Across Availability Zones* window has the same parameters and fields as the *Create Subnet Extension Across Availability Zones* window.

About this task

You can update a subnet extension that extends across AZs using the **Update Subnet Extension Across Availability Zones** or the **Update Subnet Extension To A Third Party data center** window. The **Update Subnet Extension Across Availability Zones** or the **Update Subnet Extension To A Third Party data center** window has the same parameters and fields as the **Create Subnet Extension Across Availability Zones** or the **Create Subnet Extension To A Third Party data center** window, respectively.

Based on the type of the subnet extension that you want to modify, refer to the following:

Procedure

- Extending a Layer 2 Subnet Over VPN on page 146
- Extending a Layer 2 Subnet Across Availability Zones Over VTEP on page 150
- Extending a Subnet to Third Party Datacenters Over VTEP on page 154

Removing an Extended Subnet

Perform this procedure to remove the subnet extension.

About this task

This procedure deletes the extended subnet between the two Availability Zones (AZs) or between one Nutanix AZ and one or more third party subnets. Deleting the subnet extension does not automatically remove the network gateways or VPN connections that may have automatically been created by the Subnet Extension wizard. You need to separately delete these entities created automatically when the subnet was extended.

> **Note:** Removing an extended subnet from a cluster or AZ (either source or target AZs) automatically deletes the extended subnet from the corresponding source or target AZs.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

3. Click the **Subnet Extensions** tab.
   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

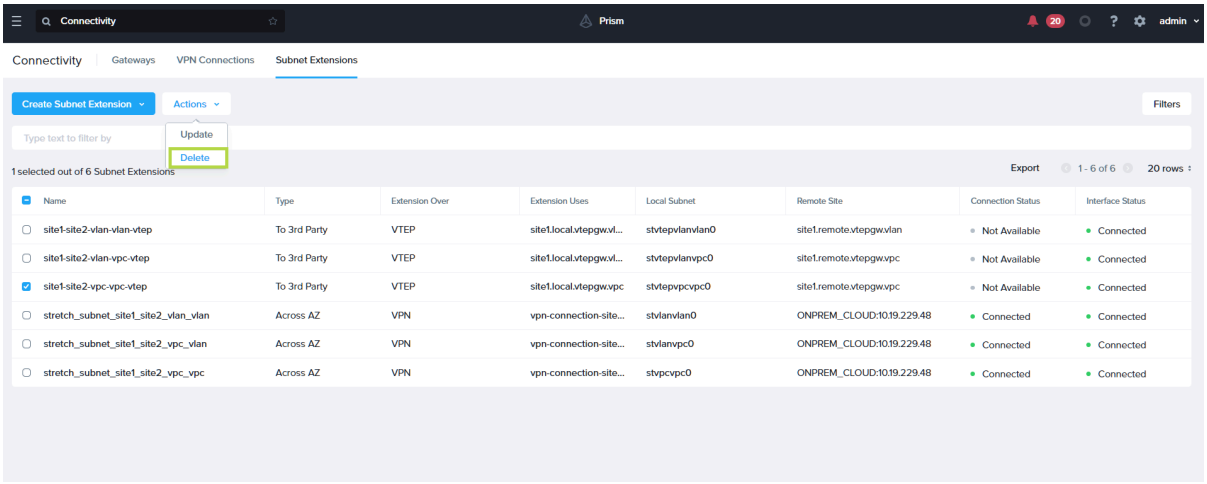


Figure 64: Sample Subnet Extensions dashboard

4. Select the checkbox associated with the subnet extension you want to remove, and click **Delete** from the **Actions** dropdown menu.

5. In the confirmation dialog box, click **Remove** to remove the extension.
   Click **Cancel** to exit without removing the subnet extension.

What to do next

Check the list in the **Subnet Extensions** tab to confirm that the subnet extension is removed.

Border Gateway Protocol Sessions

VPC networking supports No-NAT connectivity. For more information about NAT and No-NAT external connectivity configurations, see Creating a Subnet on page 106.

You can configure No-NAT external connectivity for VPC subnets using IP addresses with externally routable IP address/prefix that are reachable directly (without SNAT) from the underlying infrastructure. Underlay networks can directly communicate with endpoints in VPCs using such externally routable IP address/prefix. You need to configure routes in the underlay routers to route traffic to externally routable IP address/prefix via the virtual router of the VPC. In the reverse direction, you need to configure the virtual router of the VPC to route traffic to specific infrastructure subnets via an infrastructure router. Manually configuring these routes to and from externally routable IP address/prefix in infrastructure routers is a labor-intensive and error-prone process.

Border Gateway Protocol (BGP) gateways automate the exchange of externally routable IP address/prefix (ERP), routes, and IP address/prefix sets of infrastructure routers. **BGP Sessions** configurable in **Connectivity** supports eBGP and peering with up to 5 infrastructure routers.

Other conditions applicable to BGP sessions are:

1. You can create only one BGP session for one local and remote network gateway pair.

   In other words, a local BGP gateway and a remote BGP gateway can only host a maximum of one BGP session.
2. You need to have access permissions of the *VPC Admin* or *Nutanix Infra Admin* roles to create, update or delete BGP sessions.

   For more information, see Control User Access in Flow Virtual Networking (RBAC) on page 37.

3. Advertising all the externally routable IP address/prefix (ERP) of the VPC.
4. Without an externally routable IP address/prefix, BGP session creation fails.
5. The BGP appliance can learn and install up to 250 routes.
6. The BGP session advertises a single next hop for each Externally-routable prefix (ERP) of a VPC.

   A Network Gateway with a BGP Service is always associated with (servicing) exactly one VPC. A BGP session created on such gateway automatically advertises all the ERPs of the VPC.

   > **Note:** The BGP session ignores (or does not advertise) the received routes if the VPC is not associated with a routable (i.e. no-NAT) external subnet.

7. All received routes are added to the VPC routing table on FIFO (First In First Out) basis. Route installation priority is not dependent on destination IP address prefix length.
8. All received routes are added to the VPC routing table only if:

   - The routes added are less than or equal to 250 routes.
   - The routes to remote subnets use an IP address that is configured on a no-NAT network.

   If the VPC is not associated with a no-NAT network, the BG session ignores the received routes and does not add them to the routing table.
9. You can assign a route priority between 300 and 900. If you do not assign a route priority to a BGP session, the BGP session assigns the route priority dynamically between 600 and 800 with reducing steps of 5 starting with 700.

   For example, if you added one route without a priority, the BGP session assigns the route a priority of 700. When you add another route later without a priority, the BGP session assigns the new route a priority of 695.
10. Latest log messages are provided on Prism Central in the **BGP Logs** tab for easy troubleshooting.
11. The BGP session details include lists of all advertised and received routes.
12. The BGP session has a minimum 10-minute graceful restart period. If a BGP session fails for any reason, it attempts to restart over a period of 10 minutes or more. The routes of the session are preserved if the BGP session successfully restarts.

    The BGP session fails when it is unable to restart after the graceful restart attempt. The route of the failed session is removed from the routing table of the VPC after session failure.

Creating a BGP session

You can create a BGP session between a local BGP gateway and a remote BGP gateway also know as BGP peer.

Before you begin

You must create a local BGP gateway for the local VLAN or VPC network to connect *from*. The BGP gateway may be created in the same VLAN or VPCC or on a different VLAN.

Similarly for the remote network, ensure that you have a remote BGP gateway configured for the VLAN or VPC to connect *to*.

For information about creating, updating or deleting network gateways with BGP service, see Network Gateway Management on page 123.

About this task

Perform the following steps to create a BGP session.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

3. Click the **BGP Sessions** tab.
   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

4. Click **Create BGP Session**.

5. In the **Create BGP Session** window that opens, provide the necessary values in the respective fields as described in the table.

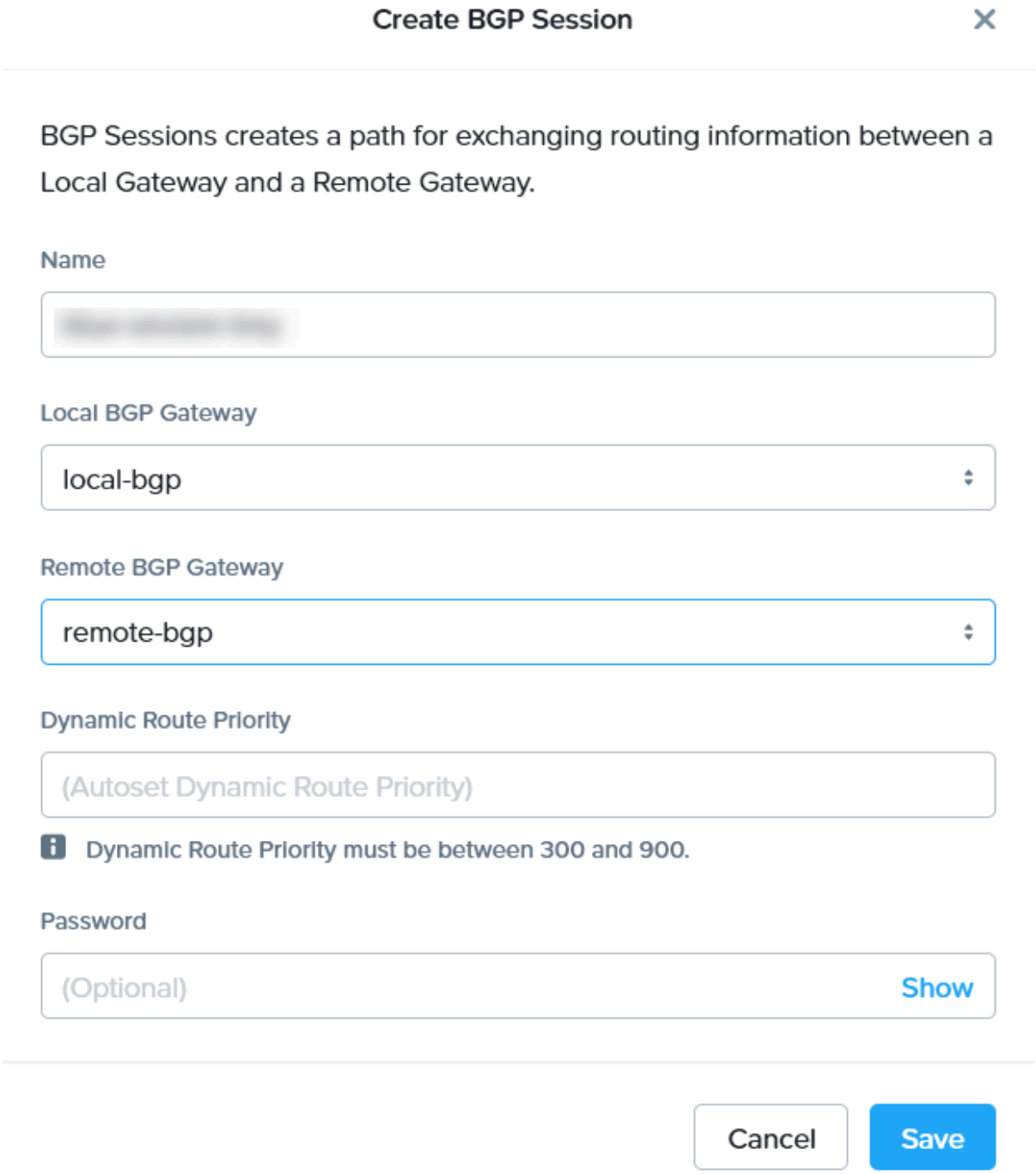


Figure 65: Create BGP Session

Parameters	Description
Name	Enter a name for the BGP session.

Parameters	Description
Local BGP Gateway	Select a local BGP gateway that you want to use for the BGP session.
Remote BGP Gateway	Select a remote BGP gateway that you want to use for the BGP session.
Dynamic Route Priority	(Optional) Enter a number between 300 and 900 as priority for the route. If you do not enter a number, Flow Virtual Networking assigns a number between 600-800. The greater the number, higher is the route priority of the session. The first automatically assigned number is 700. After that, subsequent routes requiring automatic or dynamic assignment are assigned numbers that reduce by five (5) from the previously assigned number.
Password	(Optional) Enter a password for the session. Characters allowed for BGP passwords • a-z • A-Z • 0-9 • ~ ! @ # % ^ & * ( ) _ - + = : ; { } [ ] | < > , . / ? $ • Password length: Minimum 1 and maximum 80 characters. Click **Show** to make the password visible.

6. Click **Save**.

Updating a BGP session

You can update an existing BGP session. You cannot modify some parameters of the BGP. Such parameters are greyed and in-actionable. If you need to modify such information, consider creating a new gateway with the updated parameters and deleting the current gateway.

About this task

Perform the following steps to update a BGP session.

> **Note:** You can only update the **Name**, **Dynamic Route Priority**, and **Password**. **Local BGP Gateway**, and **Remote BGP Gateway** are unavailable for update. If you need to modify such information, consider creating a new BGP session with the appropriate parameters and deleting the current BGP session.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.
3. Click the **BGP Sessions** tab.
   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

4. Select the checkbox associated with the BGP session that you want to update, and click **Update** from the **Actions** dropdown menu.
   The **Update BGP Session** window opens.

5. Update the necessary values in the respective fields.
   The fields in the **Update BGP Session** window is identical to the fields in the **Create BGP Session** window. For more information, see Creating a BGP session on page 164.

Deleting a BGP session

You can delete an existing BGP session. If you delete a BGP session, all the routes associated with the BGP session are irretrievably deleted.

About this task

Perform the following steps to delete a BGP session.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.
   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

3. Click the **BGP Sessions** tab.
   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

4. Select the checkbox associated with the BGP session that you want to delete, and click **Delete** from the **Actions** dropdown menu.
   Prism Central displays the **Delete BGP Session <bgp_session_name>** window with a checkbox for the message that warns you that all the active routes associated with the BGP session to be removed, causing a drop in traffic. Further, it asks you to confirm if you want to continue to delete the BGP session.

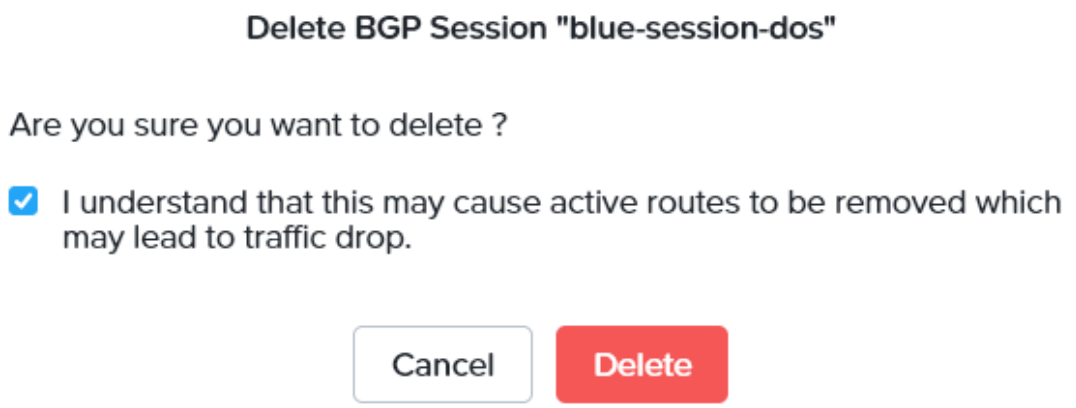


Figure 66: Delete Confirmation

5. Select the checkbox in the warning message to make the **Delete** button available.

6. Click **Delete** to delete the BGP session.
   Click **Cancel** to cancel the deletion.
   The status of the **Delete** operation is displayed as a task on the **Tasks** page.

COPYRIGHT