# Introduction to Cloud Network Domains and VLANs

**Description**

Provides an overview of the variations of Cloud Network Domains, network services that come with them, and VLAN's.

- Cloud Network Domains
- Attached and Detached VLANs
- Routing and Network Domain Static Routes
- Firewall Rules and Allowed IP Traffic
- Network Address Translation (NAT)
- Virtual Listener (VIP and Port Translation)
- Server Anti-Affinity

## Content / Solution:

# Cloud Network Domains

Cloud Network Domains represent a "Virtual Private Data Center" within the Cloud infrastructure. Each Cloud Network Domain is isolated from each other from a network standpoint and uses its own universe of IPv4 address space. This allows you to deploy multiple Cloud Network Domains with overlapping IPv4 address ranges without having to worry about IP collisions. Within this environment, you can deploy VLANs with user-defined private IPv4 address space and a system-defined IPv6 space on which you can attach the NICs of Cloud servers. Cloud Servers can then be attached to one or more of the VLANs.

There are three levels of Cloud Network Domain with different capabilities. The current list of capabilities included with each level:

| Feature | Essentials | Advanced | Enterprise |
|---|---|---|---|
| Attached VLANs | YES | YES | YES |
| Detached VLANs | NO | NO | YES |
| Client Network Domain Static Routes | NO | NO | YES |
| Firewall Rules | YES | YES | YES |
| NAT | YES | YES | YES |
| Virtual Listeners | NO | YES | YES |
| Server Anti-Affinity | NO | YES | YES |

Each network domain incurs a different usage element which may affect pricing. For details on the usage differences, see Introduction to Usage Reporting.

### Cloud Network Domain Maximums

Cloud Network Domains have some constraints that clients need to be aware of. Some are hard limits and others are practical limits.

- Clients may deploy a maximum of 30 VLANs per Network Domain.
- Cloud Network Domains are limited to a total of 1,000 Firewall Rules, including the default rules applied to all network Domains.
- There is also a limit of 64 Firewall rules with a port range.
- Cloud Network Domains have a minimum guarantee of 140 Mbps throughput, burstable to 7 Gbps (subject to availability).
- Each Primary Administrator or Sub-Administrator account is limited to 2 simultaneous Client-to-Site VPN connections.
- VIPs in MCP 2.0 have the following limits - for details on these items, see Introduction to Virtual Listeners / VIPs in MCP 2.0
  - Maximum 100 Virtual Listeners can be created per Network Domain.
  - Maximum 100 Pools per Network Domain.
  - Maximum 100 Pool Members per Pool.

### Creating and Managing Cloud Network Domains

For details on creating, managing Network Domains, see:

- How to Deploy a MCP 1.0 Cloud Network or a MCP 2.0 Network Domain
- Navigating the Network Domain Dashboard in a MCP 2.0 Data Center
- How to View and Manage a Network Domain in a MCP 2.0 Data Center

More details on the functionality and links to related articles are included in the sections below.

# Attached and Detached VLANs

All Cloud Network Domains include the ability to add VLANs. There are two types of VLANs that are supported:

- **Attached VLANs** are the default VLAN type. They are "attached" to the Network Domain's routing capabilities and are therefore able to communicate with other attached VLANs on the same Network Domain as well as the Public Internet and the optional Customer Private Network Connection (CPNC) service. All such traffic is subject to the Network Domain's firewall rules
- **Detached VLANs** are a new VLAN type introduced in the November 2018 release. A Detached VLAN is disconnected from the Network Domain's routing capabilities and exists solely as a "standalone" VLAN. *Traffic from a Cloud Server NIC connected to a Detached VLAN can only communicate with other NICs on the same VLAN*. It cannot communicate directly with other VLANs, the Public Internet, or CPNC. However, you can deploy a server or appliance that accepts traffic from a NIC connected to a Detached VLAN and routes the traffic out to an Attached VLAN that does have such capabilities. The main use case for this function is to allow users to deploy their own firewall, network inspection, or other virtual devices as part of their network infrastructure and to deploy Servers "behind" these devices on Detached VLANs so that all traffic passes through those devices.

Attached VLANs can be deployed on any Network Domain type (Essentials/Advanced/Enterprise), however Detached VLANs can only be deployed on an Enterprise Network Domain. Users can switch between Attached and Detached VLANs so long as the VLAN meets the requirements of the type of VLAN to which the switch is being made.

With both types of VLAN's, Users define the IPv4 address range for each VLAN, which can be either RFC 1918 or non-RFC 1918. The acceptable size of the range varies based on the type of VLAN as described below. The system will ensure that you do not assign the same IPv4 address space to different VLANs within the same Cloud Network Domain. The system will also automatically assign a /64 IPv6 address block for the VLAN regardless of the type of VLAN.

For details on deploying and managing VLANs, see the following articles:

- Introduction to IP Addressing in MCP 2.0
- How to Deploy a VLAN on a Network Domain
- How to View, Edit, Detach, Attach or Delete a VLAN on a Cloud Network Domain
- How to Expand a VLAN on a Network Domain in a MCP 2.0 Data Center

More details about the specifics of **Attached** and **Detached VLANs** are included in the sections below.

## Attached VLAN Details

There are three types of Attached VLANs: Small Size, Low Gateway Addressed, and High Gateway Address. The differences are summarized in the following table:

| | Small Size | Low Gateway | High Gateway |
|---|---|---|---|
| User-Defined IPv4 Address Range | /28 (16) to /16 (64K) | /24 (256) to /16 (64K) | /24 (256) to /16 (64K) |
| IPv4 Gateway Addressing | Low (First .1 in range) | Low (First .1 in range) | High (Last .254 in range) |
| Ability to Expand Size of IPv4 range | Yes | Yes | No |
| Reserved IPv4 addresses within IPv4 range<br>*(in addition to Broadcast/Network at the start/end of the range)* | First 3 IP addresses | First 5 IP addresses<br>(.1 through .5 at start) | Last 3 IP addresses<br>(.252 through .254 at end) |

### Detached VLAN Details

Since Detached VLANs are isolated from all other VLANs on the Network Domain, the rules surrounding them are looser. In addition, users must define the "IP Gateway" tracked within CloudControl. *Note that no IP gateway is actually provided by the system since the VLAN is not routed.* Instead, this value is tracked and used as the default setting for a Primary NIC of a Server being deployed onto the Detached VLAN via Guest OS Customization as described in How to Deploy a Cloud Server from a Guest OS Customization Image. The normal use case here is that users will deploy an appliance or server with a NIC that answers to this IP gateway address and routes the traffic to the Internet or CPNC through another NIC connected to an Attached VLAN.

For high-level examples on how to user the Detached VLAN function, see Introduction to Detached VLAN Use Cases.

There is only one type of Detached VLAN, in comparison to the Attached VLAN types listed above:

| | Detached VLAN |
|---|---|
| User-Defined IPv4 Address Range | /30 (4) to /16 (64K) |
| IPv4 Gateway Addressing | No gateway is provided as VLAN is not routed.<br>User-Defined value is inserted into Servers deployed via Guest OS Customization |
| Ability to Expand Size of IPv4 range | Yes |
| Reserved IPv4 addresses within IPv4 range<br>*(in addition to Broadcast/Network at the start/end of the range)* | None |

# Routing and Network Domain Static Routes

When deployed, all Network Domains are set up to automatically route traffic between different Attached VLANs on the same Network Domain as well as having the ability to route traffic to the Public Internet and any CPNC connections. The routing is controlled by Network Domain Static Routes. All Network Domain types - Essentials/Advanced/Enterprise come with a standard set of "system" routes, however Enterprise Network Domains allow you to create your own "client" static routes. For more details, see:

- Introduction to Routing, Network Domain Static Routes, and SNAT in MCP 2.0 Locations.

# Firewall Rules and Allowed IP Traffic

All Cloud Network Domains include Firewall Rule capabilities that allow you to regulate both IPv4 and IPv6 traffic in and out of the Network Domain as well as to traffic between Attached VLAN's within the Network Domain. Note the Firewall Rules do not apply to traffic within a VLAN itself. As a general rule, outbound traffic from an Attached VLAN to the Public Internet is allowed, but any other traffic will require a firewall rule in place to allow it.

For more details on default IP traffic behavior and how firewall rules apply to it, see Introduction to Firewall Rules for Cloud Network Domains in MCP 2.0.

For details on creating and managing firewall rules, see:

- How to Create a Firewall Rule on a Network Domain
- How to View and Manage Firewall Rules and Statistics on a Network Domain

# Network Address Translation (NAT)

All Network Domains allow you to create NATs to Public IPv4 addresses and to other "external" IPv4 addresses that are not associated with an Attached VLAN on the same Network Domain. The latter allows you NAT to external networks connected via a CPNC (Cloud Private Network Connection). Once established, all IP traffic directed to the external IPv4 address will be routed to the internal IPv4 address. In addition, using a NAT may affect the source address from which IP traffic originating from the internal IP address will appear. For more information on this aspect of behavior in MCP 2.0, see Introduction to Routing, Network Domain Static Routes, and SNAT in MCP 2.0 Locations.

# Virtual Listener (VIP and Port Translation)

With Advanced and Enterprise Network domains, the **Virtual Listener** functions allow you to perform both load balancing and port translation functions. Virtual Listeners support the entire IP address universe supported by the Network Domain and thus can be configured to "listen" to both external addresses (i.e. public IP addresses) or internal ones (i.e. NICs on Cloud Servers within the Network Domain). The VIP functionality is made up of a series of different elements. At a high level, the important elements are:

- **The Virtual Listener** represents the IPv4 address on the Network Domain on which the traffic will be received and then redirected to the "pool" (see below).
- The **Pool** represents the recipient of the traffic received by the Virtual Listener. The Pool is made up of one or more "nodes" (see below) that represent the IPv4 or IPv6 addresses to which the traffic will be directed. The Pool uses **Health Monitors** to identify whether those nodes are available to accept traffic.
- **Nodes** represent the IP addresses that will receive traffic as part of a pool. In most cases, the IP addresses will be associated with a NIC on a Cloud Server to which you want to direct traffic. However, nodes can also be private IPv4 or IPv6 addresses routed to a CPNC connection. This allows you to direct traffic to infrastructure outside the VLANs on the Network Domain.

These are just definitions of the basic terms. The VIP functions in MCP 2.0 offer a lot of flexibility and configuration options. For more details, see:

- Introduction to Virtual Listeners / VIPs in MCP 2.0

# Server Anti-Affinity

With Advanced and Enterprise Network domains, the system allows you to define Server Anti-Affinity Rules. Such rules allow you to prevent two Cloud Servers from operating on the same physical host on the CaaS infrastructure. This allows a load-balanced or clustered pair of servers to avoid being affected by the failure of a physical "host" server on the infrastructure.

When you establish an Anti-Affinity relationship between two servers, the system will ensure that the CPU and RAM associated with the two Cloud Servers are running on different physical hosts. Therefore, if a physical host fails, only one of the two Cloud Servers will be affected.

For more details, see:

- Introduction to Server Anti-Affinity

## Related Articles

- Introduction to MCP 2.0 Data Center Locations
- Introduction to Cloud Network Domains and VLANs

- Navigating the Data Center Dashboard
- Understanding MCP 1.0 vs. MCP 2.0 Data Center Locations
- Introduction to Multiple Data Center Locations in the same Geographic Region