



VMware Cloud Director 10.4.1

External Networks

Avnish Kumar Tripathi
Staff Multi-Cloud Solutions Architect
February 2023

vmware®

Confidential | ©2023 VMware, Inc.

New Features in Cloud Director 10.4.1 External Networks

- An external network is a network that is outside of the VCD infrastructure, such as a physical network or a virtual network. External networks are used to connect virtual machines in VCD with the external world, allowing them to communicate with the Internet or with other networks that are not part of the VCD infrastructure.
 - With the release of Cloud Director 10.4.1, External networks that are NSX-T Segment backed (VLAN or overlay) can now be connected directly to Org VDC Edge and are not required to be routed through the Tier-0 or VRF that the Org VDC Gateway is connected to.
 - This connection is done via the service interface on the service node of the Tier-1 router that is backing the Org VDC Edge Gateway.
 - The Org VDC Edge Gateway still needs a parent Tier-0/VRF, but it can be disconnected from the T1 serving as the Org VCD Edge Gateway.

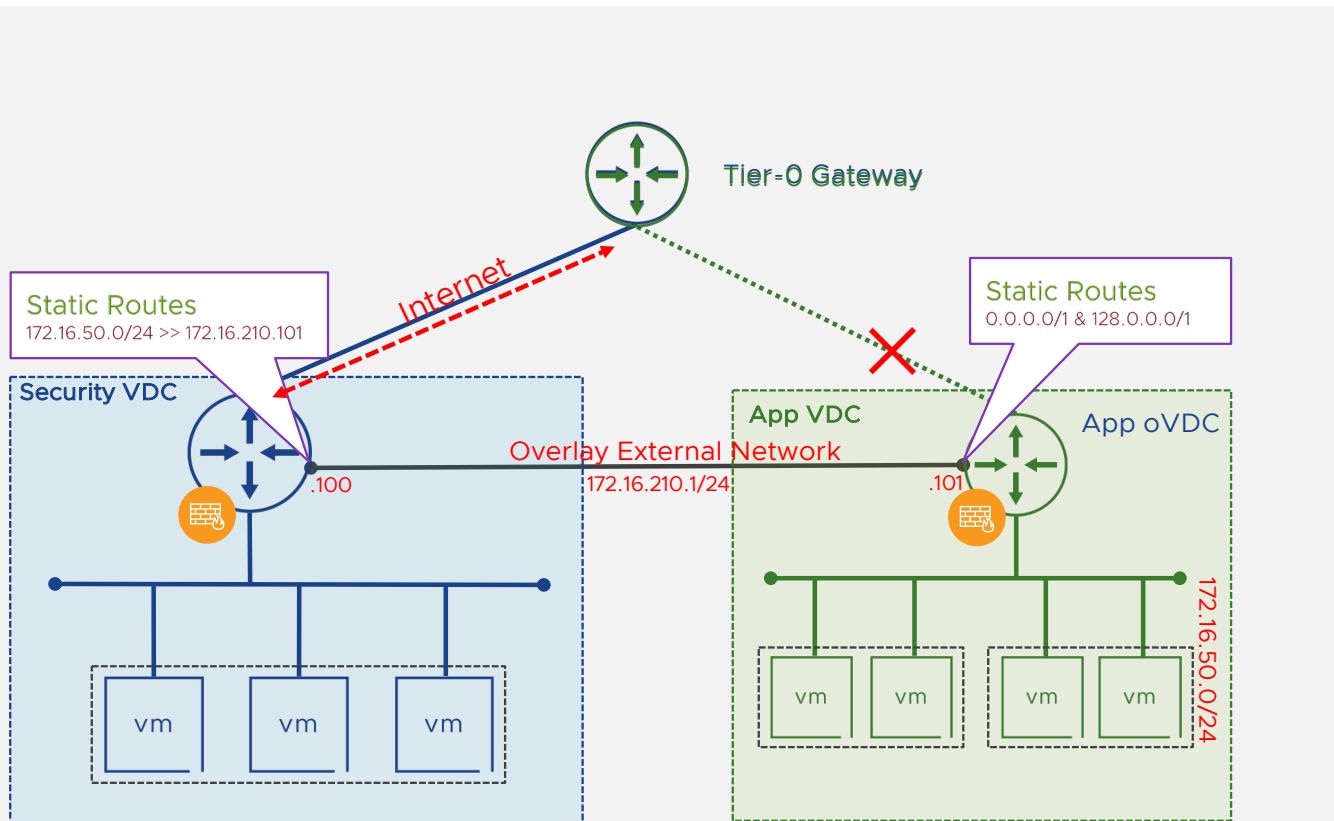
New Features in Cloud Director 10.4.1 External Networks

Use cases

1. Routed connectivity via dedicated VLAN to tenant's co-location physical servers
2. Transit connectivity across multiple Org VDC Edge Gateways to route between different Org VDCs
3. Connectivity with Partner Service Networks
4. MPLS connectivity to direct connect while Internet connectivity is available via shared provider gateway (T0)

Security VDC Architecture Using External Networks

Transit Connectivity Across Two Org VDC Edge Gateways - Overlay



This is using Overlay (GENEVE) backed external network

This Overlay network must be prepared by provider in NSX as well as in Cloud Director

NSX Tier-1 GW does not provide any dynamic routing capabilities, so routing to such network can be configured only via static routes

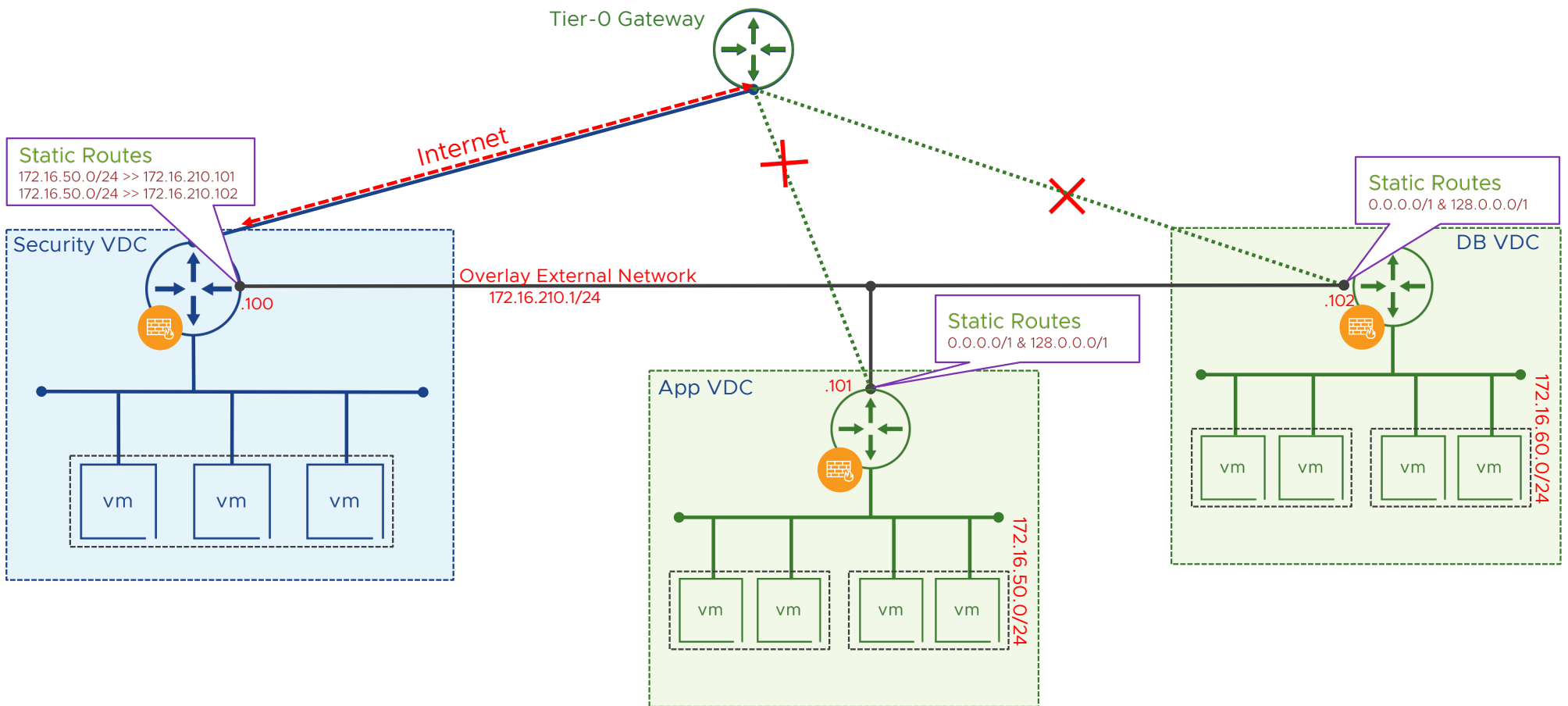
Tier-1 GW has default route (0.0.0.0/0) always pointing towards its parent Tier-0/VRF GW

Set default route to the segment backed external network you need to use two more specific routes. For example:

- 0.0.0.0/1 next hop <IP> scope <network>
- 128.0.0.0/1 next hop <IP> scope <network>

Security VDC Architecture Using External Networks

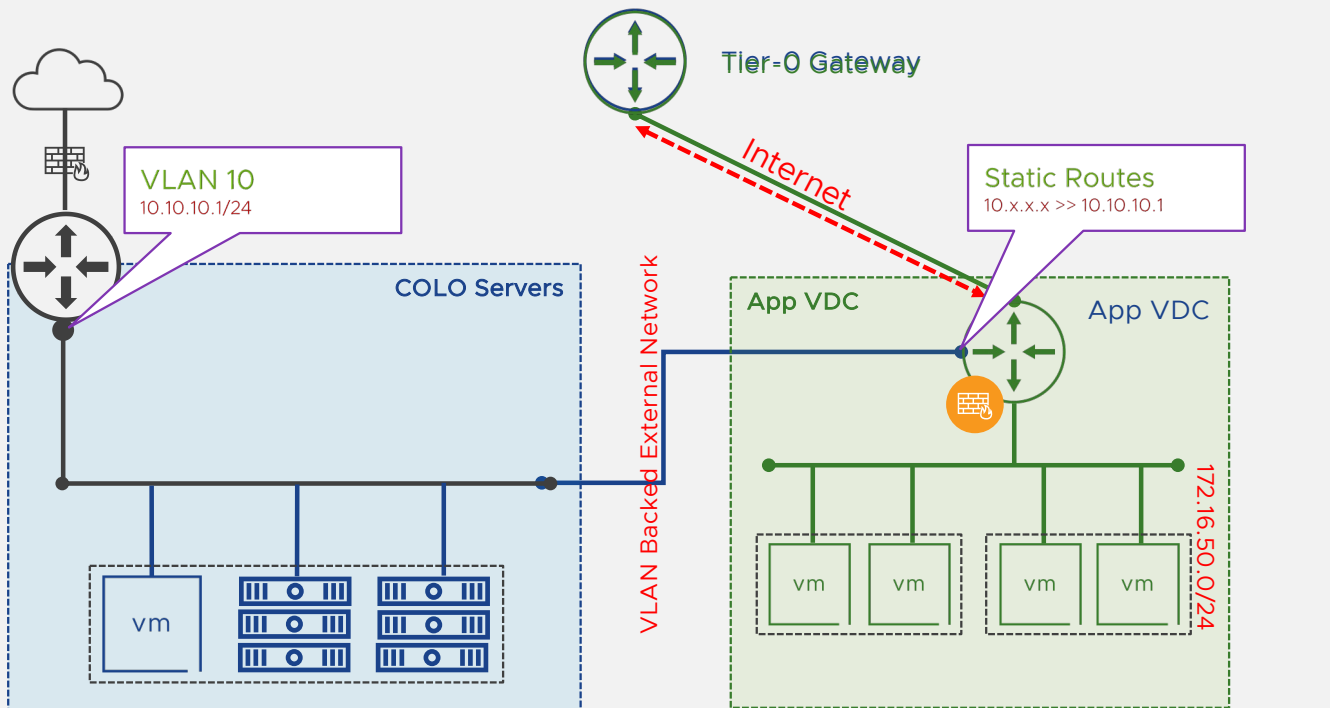
Transit Connectivity Across Multiple Org VDC Edge Gateways - Overlay



NOTE - This is applicable from Cloud Director 10.4.1 onwards

Architecture for VDC Connectivity to Colocation/MPLS

Routed connectivity via dedicated VLAN to tenant's co-location physical servers or MPLS



This is using VLAN backed external network

This VLAN backed network must be prepared by provider in NSX as well as in Cloud Director

NSX Tier-1 GW does not provide any dynamic routing capabilities, so routing to such network can be configured only via static routes

One VLAN segment, it can be connected to only one Org VDC Edge GW

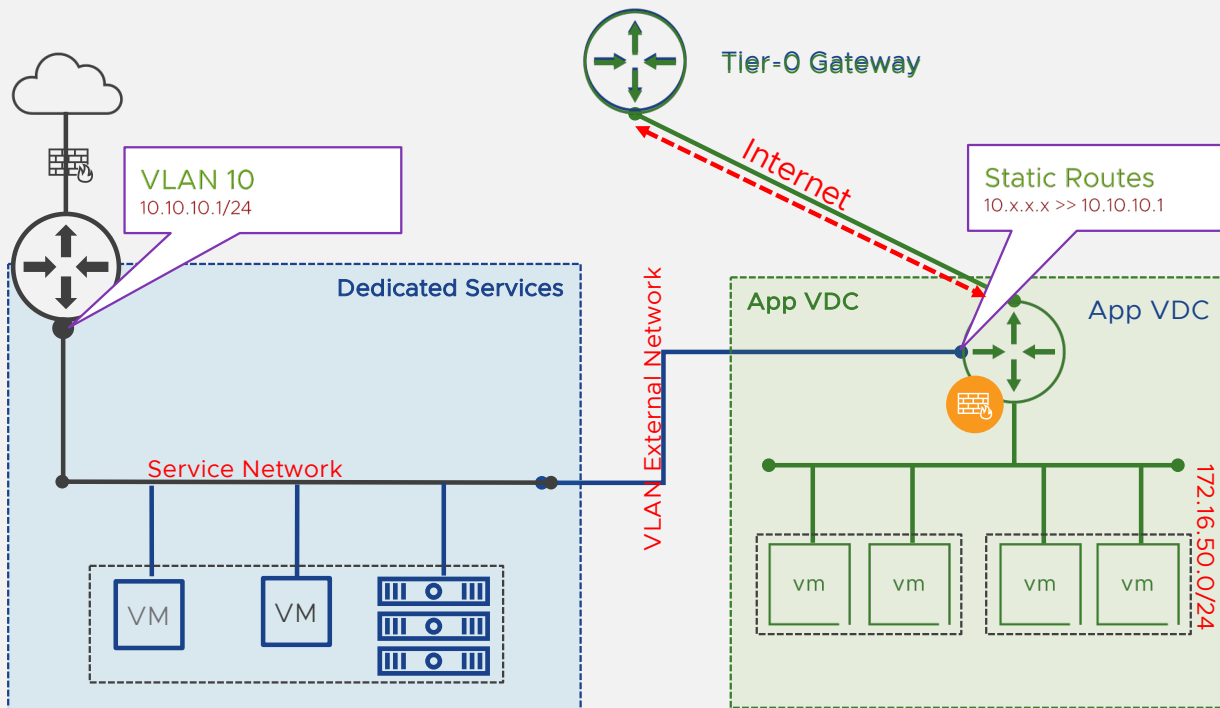
Tier-1 GW has default route (0.0.0.0/0) always pointing towards its parent Tier-0/VRF GW

Set default route to the segment backed external network. For example:

- 172.16.50.0/24 next hop <router IP> scope <external network>

Architecture for VDC Connectivity to Provider Service Networks

Connectivity towards Partner Service Networks



This is using VLAN backed external network

This VLAN backed network must be prepared by provider in NSX as well as in Cloud Director

NSX Tier-1 GW does not provide any dynamic routing capabilities, so routing to such network can be configured only via static routes

One VLAN segment, it can be connected to only one Org VDC Edge GW

Tier-1 GW has default route (0.0.0.0/0) always pointing towards its parent Tier-0/VRF GW

Set static route to the segment backed external network you need to use two more specific routes. For example:

> <Service Network> next hop <Service Network Router IP> scope <External Network>



Thank You