Well-Architected Design: Gateway Firewalls Use Cases and Scope

Table of contents

Well-Architected Design: Gateway Firewalls Use Cases and Scope

Introduction

VMware Cloud SDDC includes vCenter Server, NSX software-defined networking, and vSAN software-defined storage. These products are delivered as a cloud service to accelerate cloud adoption and simplify the cloud operating model.

While VMware Cloud SDDC simplifies the consumption of advanced networking capabilities using NSX, it is critical for customers to understand the networking and security model of VMware Cloud SDDC. This design will help them adapt to a modern security architecture with consistent protection across the on-premises and cloud environments.

Scope of the Document

Within a VMware Cloud SDDC, two layers of firewalling provide intrinsic network security: the NSX Gateway Firewall and the NSX Distributed Firewall (DFW). The NSX Gateway Firewall, when used in conjunction with the NSX Distributed Firewall, extends the capabilities to provide defense-in-depth protection across the entire VMware Cloud SDDC infrastructure. This document will cover the NSX Gateway firewall use cases and scope in the VMware Cloud SDDC.

Summary and Considerations

Use Case	
Pre-requisites	
General Considerations/Recommendations	
Performance Considerations	VMware Configuration Maximums
Network Considerations/Recommendations	
Cost Implications	https://www.vmware.com/products/aria-operations-for-logs.html https://www.vmware.com/products/aria-operations-for-networks.html
Document Reference	For NSX recommended limits, use the VMware Configuration Maximums tool.
Last Updated	April 2023

NSX Gateway Firewall Architecture and Scope

The NSX Firewall design includes two types or layers of firewalls, Gateway Firewalls and the Distributed Firewall. Gateway Firewalls are North-South Firewalls that are designed to protect the SDDC's perimeters or boundaries, whereas Distributed Firewalls are East-West Firewalls that protect workloads at the vNIC level.

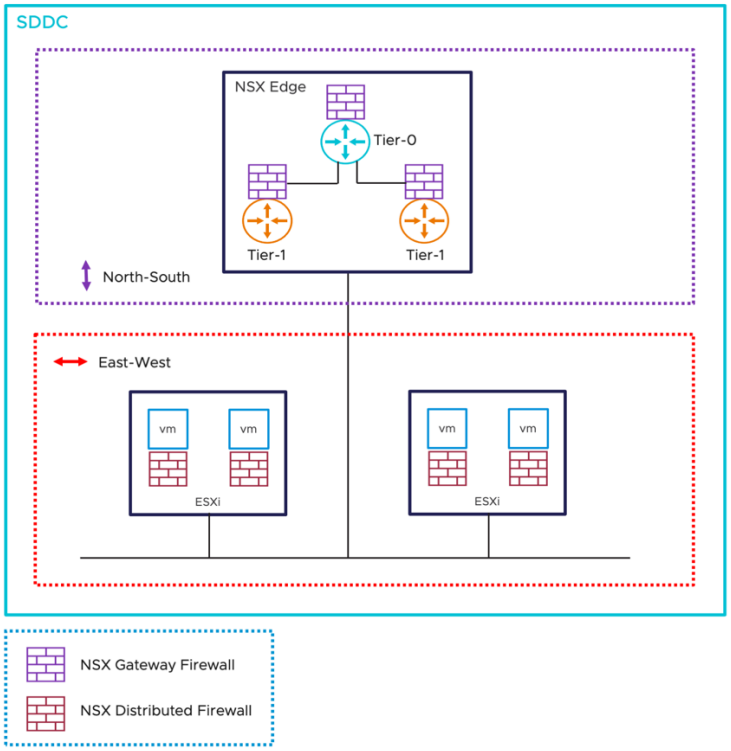

Figure 1 - SDDC Firewall Types

The VMware Cloud SDDC network has two logical tiers.

- NSX Tier-0 Gateway handles traffic from North-South (traffic leaving or entering the SDDC, or between the Tier-1 Gateways). Each SDDC is configured with a single NSX Tier-0 Gateway by default.
- Tier-1 Gateways connect to a Tier-0 Gateway and provide network segments with a North-South connectivity for the workloads. Additional Tier-1 Gateways can be created to provide dedicated Tier-1 Gateway Firewalls to use as inter-tenant or inter-zone connections. Each SDDC includes a default Tier-1 Gateway to provide protection for SDDC management components (vCenter, NSX Manager) and initial workload segments created by customers.

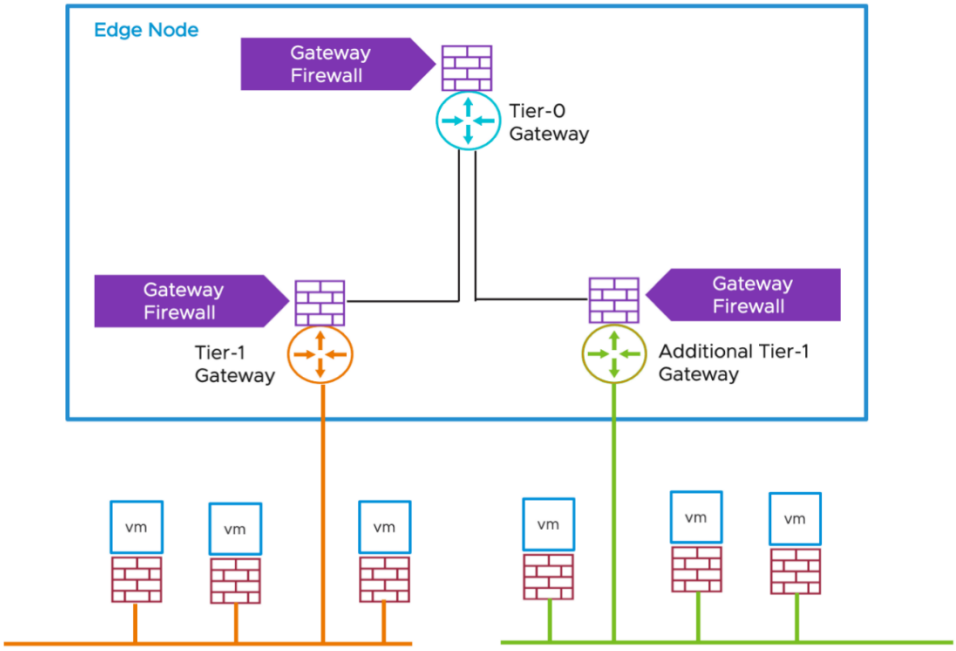

Figure 2 - Gateway Firewall Logical Topology

NSX Edge Nodes

The default NSX Edge is a pair of VMs that operate in high availability mode. This NSX Edge pair serves as the platform for the default Tier-0 and Tier-1 Gateways, providing security services for North-South traffic, as well as IPsec VPN connections and BGP routing mechanisms.

The NSX Edge can contain multiple Gateway Firewalls as shown in Figure 2. These Gateway Firewalls have their own firewall or security rule table while being centrally managed by NSX. NSX Edge can initiate Gateway Firewall on Tier-0 or Tier-1 Gateway to provide firewalling services in VMware Cloud SDDC at boundaries or perimeters and provides NAT, DHCP, and VPN services to the workload network segments.

Default Tier-0 Gateway

The default Tier-0 Gateway handles all North-South traffic. To prevent transmitting East-West traffic through the NSX Edges, a Tier-1 router component handles routing for SDDC destinations operates on each ESXi host. The NSX Edge can contains a Firewall on Tier-0 or Tier-1 Gateway.

The SDDC Network Topology can vary based on the VMware Cloud provider. The Gateway Firewall runs on Default Tier-0 or Tier-1 based on an optimized integration with the respective VMware Cloud provider's infrastructure. For example, Figure 3 depicts the SDDC Network Topology used with VMware Cloud on AWS or Alibaba Cloud VMware Service (ACVS). They provide a default Tier-0 with Gateway Firewalling service to protect the network traffic for workload VMs connected to routed compute network segments behind the default Tier-1 Gateway, also known as Compute Gateway (CGW). Compute Gateway Firewall rules, along with NAT rules, run on Tier-0. In the default configuration, these rules block all traffic to and from compute network segments until the customer adds Compute Gateway firewall rules to allow traffic as needed.

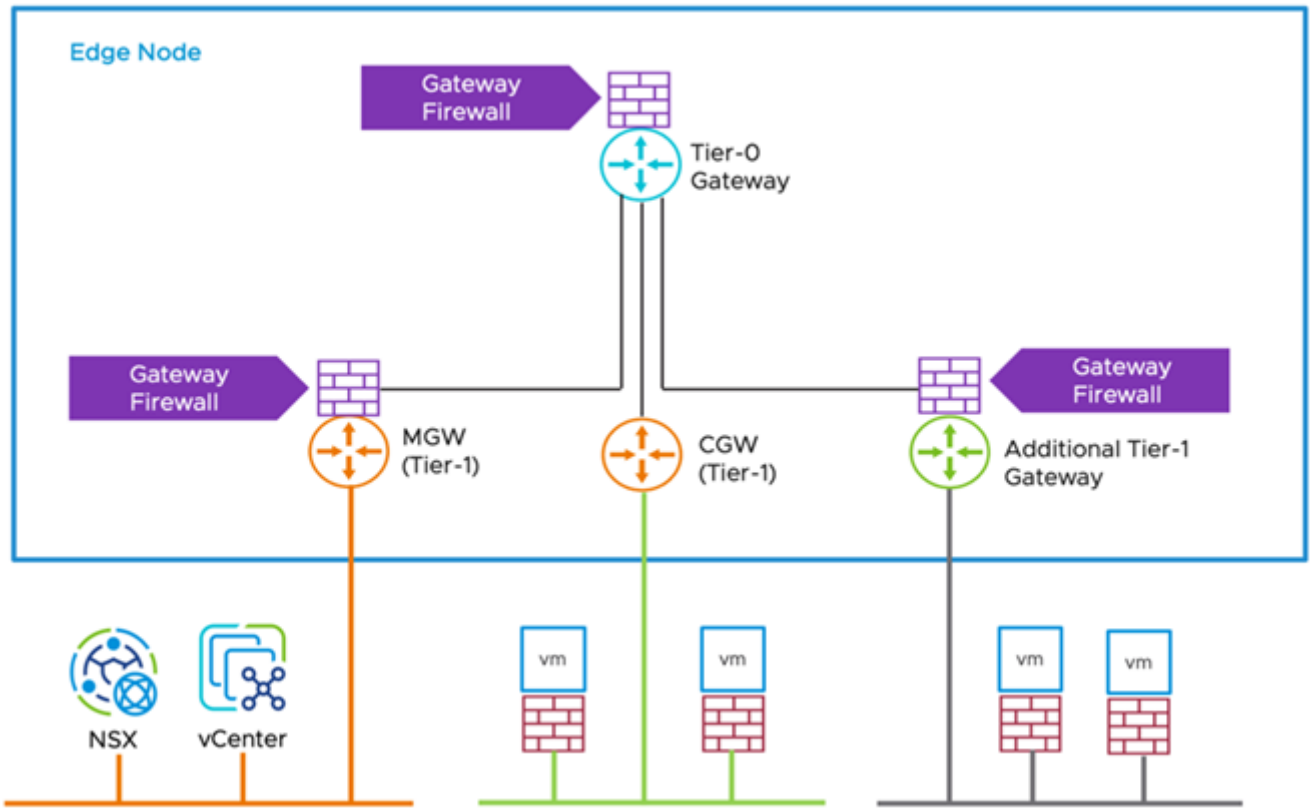

Figure 3 –SDDC Network Topology in VMware Cloud on AWS

Default Tier-1 Gateway Firewall

The Default Tier-1 Gateway also runs on the NSX Edge Nodes and handles network traffic for workload VMs connected to the routed compute network segments.

As mentioned, the SDDC Network Topology in VMware Cloud on AWS or Alibaba Cloud VMware Service (ACVS) provides default Tier-1 Gateway, also known as Compute Gateway (CGW). In Addition to the CGW, there is also a Management Gateway (MGW). This is a Tier-1 Gateway that handles routing and firewalling for vCenter Server and other management appliances running in the SDDC. The Management Gateway Firewall runs on the MGW to protect management VMs for north-south security and from compute networks within the SDDC. Since keeping the SDDC management infrastructure safe and secure is critical, the management gateway, by default, blocks traffic to all management network destinations from all sources until the customer creates a Management Gateway Firewall rule allowing access from a trusted source.

Additional Tier-1 Gateway Firewalls

Additional Tier-1 Gateways can be created by the customer. Tier-1 Gateways enable an SDDC network administrator to dedicate workload network capacity within a VMware Cloud SDDC to specific projects, tenants, or other administrative units. Each Tier-1 gateway protects the traffic between the SDDC Tier-0 Gateway and any number of compute network segments.

Deployment Scenarios

Deployment Scenario	Description	Recommendations
Greenfield SDDC deployment on VMware Cloud	For greenfield deployments, Gateway Firewall security is needed for applications and workloads.	Start building the security posture from day one for Gateway Firewall capabilities with Zone firewalling or multi-tenancy deployments
On-premises data-center extension to VMware Cloud	After an SDDC is built in VMware Cloud, you can apply the same posture for your workload VMs as in on-premises for security using Gateway Firewall. When using NSX in your on-premises environment, use similar security constructs within the Cloud SDDC as you have used on-premises with NSX.	Start building the security posture from day one for Gateway Firewall capabilities with Zone firewalling or multi-tenancy deployments. Explore APIs (Application Programmable Interfaces) to provision the similar policies for Gateway Firewall rules across on-premises and VMware Cloud environments.
On-premises data center evacuation to VMware Cloud	You may consider evacuating your complete on-premises data center to VMware Cloud to satisfy various business requirements. You can deliver an equivalent or increased level of protection using VMware Cloud.	Take a backup of your on-premises security configuration and start designing Gateway Firewall capabilities in pre-migration phase. Start your VMware Cloud journey by applying a combination of Gateway Firewall and DFW Firewall using your existing backup configuration as reference.
Disaster Recovery VMware Cloud SDDC	A Disaster Recovery SDDC contains mission critical VMs. Plan Gateway Firewall security design for disaster recovery VMs prior to a disaster.	In a disaster scenario, you may not be in a place to implement new security policies. Plan and implement Gateway Firewall policies and rules from day 0 for VMs within the recovery SDDC.

Resiliency and Availability

The NSX Gateway Firewall is a software-only, layer 4 firewall that incorporates platform capabilities for high availability provided by a pair of NSX Edge nodes. Stretched Cluster for VMware Cloud SDDC provides a higher level of resiliency and higher protection by stretching the SDDC management components across two availability zones within the same region.

Scalability

A VMware Cloud SDDC can contain medium or large SDDC appliance configurations. By default, a new SDDC is created with medium-sized NSX Edge and vCenter Server appliances. Large-sized appliances are recommended for large-scale deployments or in any other situation where management cluster resources might be oversubscribed. An SDDC created with a medium appliance configuration can be upsized to a large configuration.

Performance

The firewall performance and resource requirements of the NSX Gateway Firewall should be considered as part of the entire SDDC deployment, together with the number of hosts or VMs and management cluster resources. Default medium sized NSX Edges are designed for typical SDDC workloads. For large-scale SDDC implementations, large-sized NSX Edge appliances are generally recommended. For more information on resource allocation to Large SDDC, please visit the VMware Configuration Maximum page.

Integrations

Additional Tier-1 Gateway features include integration with Customer managed appliances (CMA) such as a North/South perimeter or security zone firewall, a Load Balancer configured for in-line mode, and a VPN or remote access endpoint.

Operations Overview

Security

While VMware Cloud SDDC simplifies the use of advanced NSX capabilities, customers must still implement strong identity governance for NSX service roles access with multi-factor authentication, monitor NSX audit logs for network changes, enable NSX firewall logs for visibility and troubleshooting, and archive NSX logs for security compliance. Customers are responsible for configuring the Gateway Firewall and ensuring the least privileged access model is followed by Gateway Firewall policies.

Monitoring and Alerting

VMware Aria Operations for Logs integrates with VMware Cloud SDDC to provide administrators with powerful insights into NSX firewall rules with audit details. This allows auditing, monitoring, and alerting on the behavior of configured rules in the VMware Cloud environment.

Logging

VMware Aria Operations for Logs integrates with VMware Cloud SDDC to provide administrators with centralized log management, deep operational visibility and intelligent analytics for NSX Gateway Firewall logs. This facilitates troubleshooting, auditing, security monitoring and application monitoring.

Capacity Management

Use the VMware Configuration Maximums tool to evaluate limits on the number of Gateway Firewall rules to stay within the recommended capacity.

Cost

There are no extra costs for using the Gateway Firewall included with a VMware Cloud SDDC subscription. Traffic egressing the VMware Cloud SDDC to External Services or the Internet may result in network egress charges. The additional services such as VMware Aria Operations for Logs and VMware Aria Operations for Networks are sold separately.

NSX Gateway Firewall Use Cases

Gateway Firewall Overview

The NSX Gateway Firewall is enabled per gateway and provides protection at both the Tier-0 and Tier-1 levels. The Gateway Firewall provides firewalling services at perimeters or boundaries. The Gateway Firewall also offers NAT, DHCP, and VPN services. The Gateway Firewall is implemented in the NSX Edge nodes. The Gateway Firewall operates independently of the NSX DFW regarding policy configuration and enforcement, however objects from the DFW can be shared with Gateway Firewall policies.

Key differentiating capabilities of Gateway Firewall

The Gateway Firewall is similar in function to a traditional firewall, but there are differences to consider so that an optimal configuration can be designed.

Traditional Firewalls	NSX Gateway Firewalls
Physical appliance firewalls have network topology dependencies, so firewalling can be done only at the network boundary and for north-south traffic.	Virtual firewalls are network agnostic and expand your firewalling capacity with no need for specialized hardware.
Network segmentation without having the option to do granular application and micro-segmentation, which is needed to protect organizations from east-west lateral movement	Native support for multi-tenancy to easily operationalize multi-tenant deployments. A capable partner to Distributed Firewall (DFW) which enables Granular application and Micro-segmentation. When the NSX Gateway Firewall is deployed in conjunction with the NSX Distributed Firewall, it is easy to extend consistent layer 2-7 security controls across all applications and workloads
Static policy based on IP or gateway interface	The dynamic context-based policy enables security groups and policies to be dynamically created and automatically updated based on attributes to include elements such as VM names and tags. The NSX Gateway Firewall shares the same unified management console as the NSX Distributed Firewall. This makes it simple to enforce consistent policies at the perimeter, between zones and inside the organizational network.
Cannot secure endpoints on the same VLAN, unless they are deployed in Layer 2 mode	NSX Gateway Firewall is a software-only, layer 4 firewall with native zone firewall capabilities that provide unified North-South and East-West security with stateful firewalling between multiple security zones at the boundaries. When deployed together with the NSX Distributed Firewall, the Distributed Firewall extends the capabilities to provide defense-in-depth granular micro-segmentation policies for the Zero Trust security model that enables consistent network security coverage for all workloads.
Legacy firewalls are built around IP address constructs	Policies in NSX with Gateway Firewall can be defined using IP addresses, but this is not required. Grouping logic can be implemented using operating system name, a substring of the VM name, tags, etc. For container environments, labels can be leveraged for the grouping.
Runs on specific dedicated hardware/server	Runs on every hypervisor in VMware Cloud that expands your firewalling capacity with no need for specialized hardware.
Centralized, network dependent	Decentralized, distributed and network agnostic.
Hair-pinning if workloads are hosted on the same host	No hair-pinning when deployed together with the NSX Distributed Firewall. The NSX Distributed Firewall is purpose-built to extend the capabilities of the NSX Gateway Firewall across all workloads in VMware Cloud SDDC.
Fixed architecture	Scale-out architecture

Edge Firewall Use Cases

NSX Edge provides firewalling services that enforce consistent policies extending to the cloud edge and various external uplinks. The Gateway Firewall is a centralized firewall implemented on NSX Tier-0 gateway uplinks and Tier-1 gateway links. This is implemented on a Tier-0 and Tier-1 component which is hosted on NSX Edge. Gateway Firewall uses a similar model as DFW for defining policy, and NSX grouping constructs can be used as well. Gateway firewall policy rules are organized using one or more policy sections in the firewall table for Gateway Firewall.

The SDDC's NSX Edge provides numerous interfaces for various uplinks. It is critical to understand the SDDC's multiple uplinks and the traffic traversing them. This knowledge is valuable not only for understanding SDDC interconnectivity but also for understanding how traffic exits the SDDC (and potentially incurs bandwidth charges).

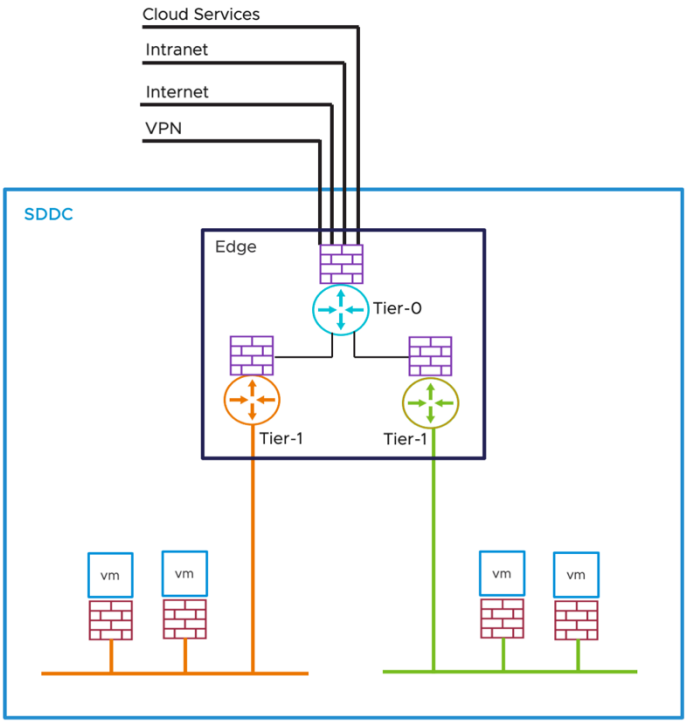

Figure 3 - NSX Edge Uplink Types

- The internet uplink connects the SDDC to the internet via the Internet Gateway. The SDDC Edge has a default route that points to the Internet Gateway as a next hop, consequently, any unknown destination networks will use this uplink. This uplink's traffic is chargeable per egress bandwidth pricing, and the charges will be passed through as part of the SDDC's billing.
- The intranet interface routes traffic over a dedicated high-bandwidth low-latency network connection. The SDDC Edge will use the intranet uplink for any network prefixes received through BGP over this uplink. Because this is a resource managed by the customer's public cloud account, all bandwidth charges incurred for this uplink will be invoiced to the customer's public cloud account.
- The Cloud Services interface connects the SDDC Edge to the customer-owned public cloud account's cloud services. This uplink is only non-billable for cloud resources that are in the same Availability Zone as the SDDC. Traffic to resources in different Availability Zones is billable, and charges will be billed to the customer's public cloud account.
- The VPN Tunnel Interface routes traffic over the Route-Based IPSec VPN. The VPN Tunnel Interface is classified as a virtual interface and not an uplink. The egress charges for the VPN traffic apply to the Internet or intranet uplink where the VPN tunnel is running over and established.

Tier-1 Gateway Firewall Overview

The default Tier-1 Gateway is preconfigured in your SDDC. In a new SDDC, the default firewall rule blocks traffic to all uplinks in NSX Gateway Firewall. New SDDCs are created without a default network segment, so customer must create at least one compute segment for your workload VMs and add Gateway Firewall rules to allow traffic as needed.

The default Tier-1 Gateway provides firewalling service to protect North-South network traffic for workload VMs. It also provides

VPN, NAT, and DHCP services.

The Tier-1 Gateway Firewall provides firewalling services at the border or perimeter of workload network segments to secure North-South traffic leaving or entering the Gateway Firewall. VMware Cloud SDDC adds another layer of firewalling to secure East-West traffic within network segments or SDDCs with NSX Distributed Firewall (DFW). Distributed Firewall rules apply at the VM (vNIC) level and protect East-West traffic within the SDDC.

VPN service

NSX Gateway Firewall provides secure connectivity services with support for IPsec Virtual Private Network (IPsec VPN) and Layer 2 VPN (L2 VPN) services which enables secure low-latency connectivity across geographically diverse sites. With L2 VPN, you can extend the network in order to provide a single broadcast domain spanning your on-premises network and the SDDC workload network. L2 VPN capability enables virtual machines to keep their network connectivity across geographical boundaries using the same IP address.

NAT service

NSX Gateway Firewall provides a Network address translation (NAT) service which maps internal IP addresses on your workload network to addresses exposed on the public Internet. NAT rules are configured on the SDDC network's Internet interface since that is where you're the workload VMs' public addresses are exposed. Firewall rules, which examine packet sources and destinations, run on the Gateway Firewall, and process traffic after it has been transformed by any applicable NAT rules.

DHCP service

NSX Gateway Firewall provides DHCP service on each segment regardless of whether the segment is connected to a gateway. NSX Gateway Firewall supports the following types of DHCP configuration on a segment:

- Segment DHCP server (earlier known as Local DHCP server)
- Gateway DHCP server (supported only for IPv4 subnets in a segment)
- DHCP Relay

DHCP configuration is a per-segment property. In the default configuration, the Gateway DHCP server handles DHCP requests from VMs on all routed segments. To use another DHCP server for your workload networks, you can configure the segment to use DHCP relay. You can also configure a segment to use its own local DHCP Server.

DNS Forwarding service

NSX Gateway Firewall provides DNS forwarding service which enables workload VMs in the zone to resolve fully qualified domain names to IP addresses. SDDC includes a default DNS Forwarder and allows you to configure your own DNS Server IPs.

Tier-1 Gateway Firewall Use Cases

Customers can create additional Tier-1 Gateways and manage the life cycle for those Tier-1 Gateways in VMware Cloud SDDC. Each Tier-1 Gateway provides North-South protection between the SDDC Tier-0 Gateway and the network segments for workload VMs.

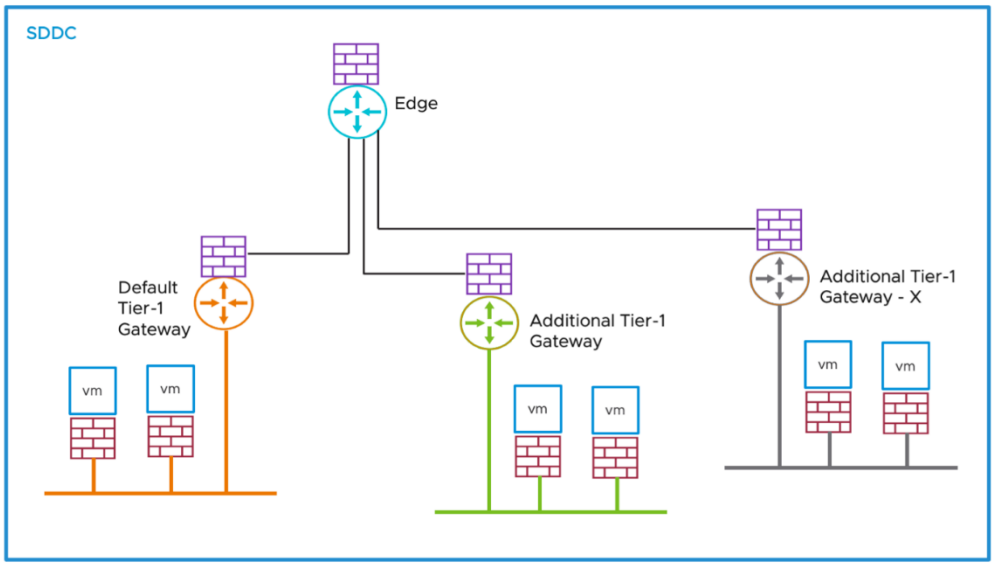

Figure 4 - Additional Tier 1 Gateways

Each additional Tier-1 Gateway has its own Gateway Firewall that is scoped to the specific gateway, and the security policy is enforced at the individual Gateway Firewall level for all traffic entering and exiting the corresponding zones.

Additional Tier-1 Gateway Firewalls are ideal for establishing zones or tenants because they are designed to operate at boundaries or perimeters protecting North-South traffic. Customers can use the additional Tier-1 Gateways as inter-tenant or zone firewalls from the North-South perspective within the SDDC.

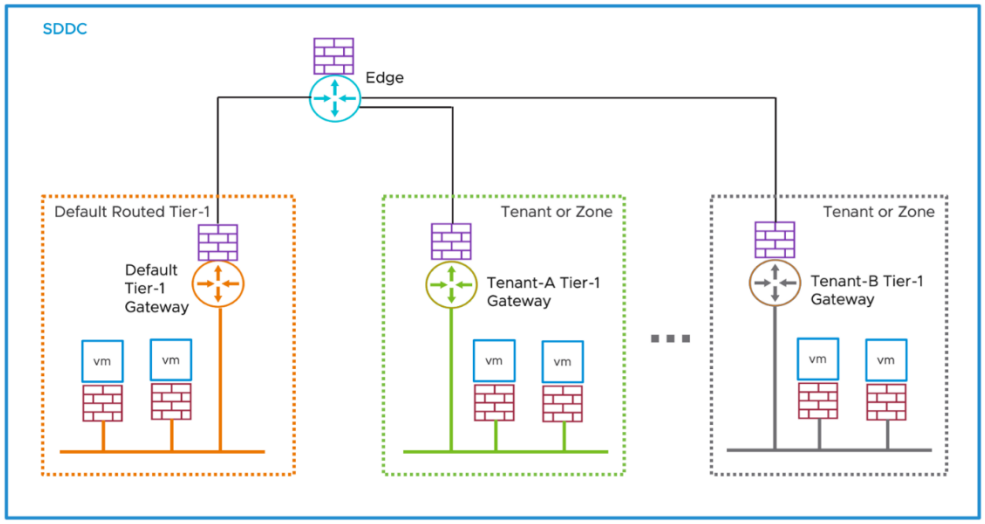

Figure 5 - Tier-1 Tenant Gateways

The Tier-1 Gateway capabilities provide customers with new use cases by delivering dedicated Gateway Firewalling services, VPN and NAT services to workload VMs.

- Multi-Tenancy use case to easily operationalize multi-tenant deployments.
- Implementing Zone Firewalling use case such as Prod and Non-Prod, sensitive security zones
- Workload portability use case with overlapping IPv4 address space across Tenants or Zones to simplify application migration across on-premises and cloud environments.
- Isolated Zones use case for Disaster Recovery (DR) testing or “Sandbox” environments.

Customers have the option to choose different Tier-1 Gateway types to enable particular use cases inside VMware Cloud SDDC. These gateway types include Routed, NAT'ed, or Isolated, and each comes with additional features such as static routes, local DHCP servers, DNS forwarding, and Traceflow.