Firewall Rules for Tanzu Kubernetes Grid on VMware Cloud on AWS

VMware App Modernization

Table of contents

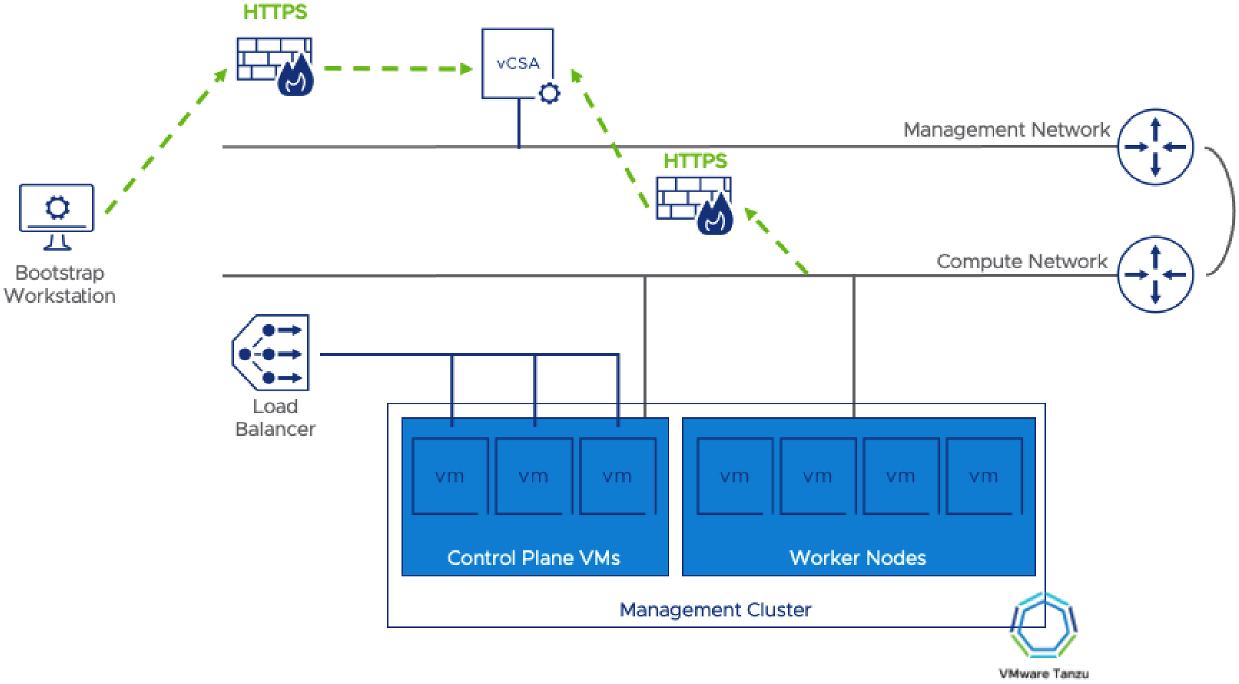
Firewall Rules for Tanzu Kubernetes Grid on VMware Cloud on AWS

Tanzu Kubernetes Grid Firewall Rules for VMware Cloud on AWS

To deploy Tanzu Kubernetes Grid (TKG) into a VMware Cloud on AWS environment, specific firewall rules must be created to allow proper communication between components. Please review the sections below that layout the firewall rules needed to properly deploy TKG management clusters and Tanzu Kubernetes clusters into VMware Cloud on AWS.

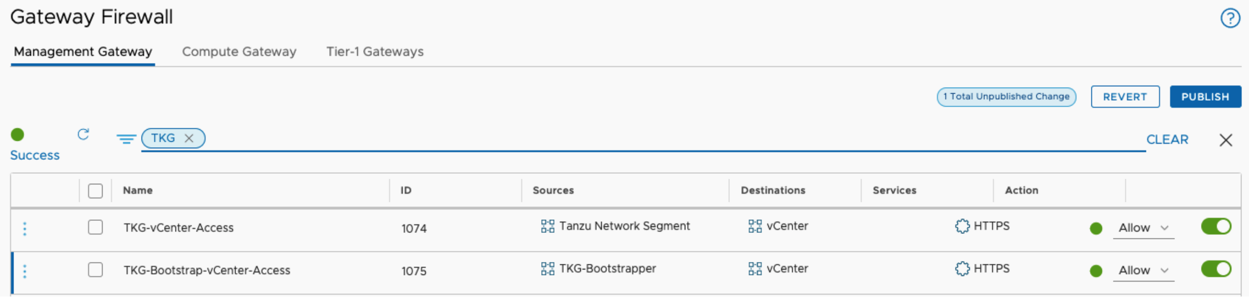
As a reminder, VMware Cloud on AWS uses a management gateway and a compute gateway. These gateways will need firewall rules created to allow traffic for Tanzu Kubernetes Grid deployments, and the sections below break the firewall rules down by gateway.

Management Gateway Firewall Rules



The management gateway needs a couple of rules to allow the Tanzu Management Cluster to be provisioned. The first is the bootstrap machine access. The bootstrap machine is usually a workstation or orchestrator where the Tanzu CLI runs to stand up the management cluster. This machine could be in a datacenter accessing VMware Cloud on AWS over a VPN/Direct Connect, or it could be a jump host in the VMware Cloud on AWS environment. Wherever it’s located, this machine needs to access vCenter to issue commands to deploy new virtual machines. Likewise, the Kubernetes cluster itself needs to communicate with the vCenter for provisioning additional clusters, so the network segment where the TKG clusters will run should also have access to vCenter.

Source	Destination	Port/Service
Bootstrap Machine	vCenter	HTTPS
Tanzu Network Segment	vCenter	HTTPS



Gateway Firewall

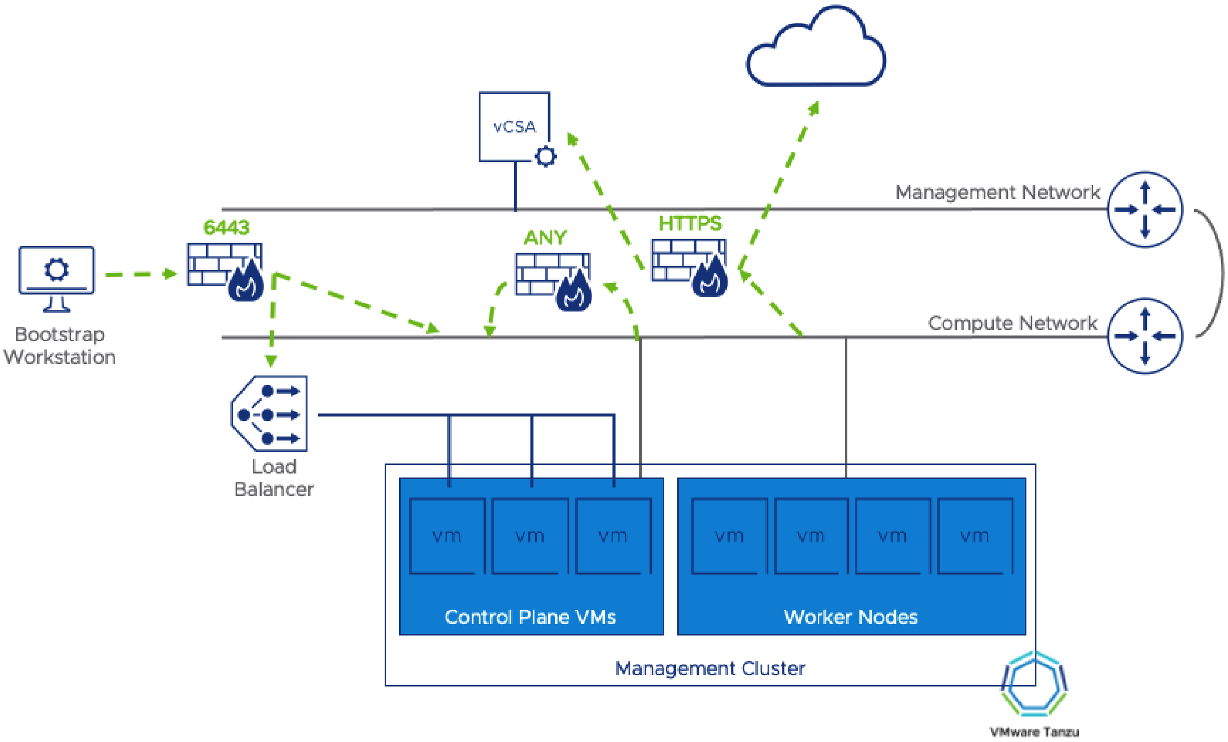
Management Gateway | Compute Gateway | Tier-1 Gateways

1 Total Unpublished Change | REVERT | PUBLISH

Success | TKG | CLEAR

	□	Name	ID	Sources	Destinations	Services	Action	
⋮	□	TKG-vCenter-Access	1074	Tanzu Network Segment	vCenter	HTTPS	● Allow	●
⋮	□	TKG-Bootstrap-vCenter-Access	1075	TKG-Bootstrapper	vCenter	HTTPS	● Allow	●

Compute Gateway Firewall Rules



The compute gateway firewall rules will allow access into the Tanzu Kubernetes Grid components being built. First, begin by ensuring that the Bootstrap machine can access the Tanzu cluster endpoint for the management cluster. This cluster endpoint is typically a load balancer address created by Kube-vip or the NSX-T Advanced load balancer. Regardless of your deployment model, the bootstrap machine uses this endpoint on port 6443 to communicate with the cluster. It should be noted that this load-balanced address could live in a different VMware Cloud on AWS network segment. If it does, make sure that that network segment also has access to the Tanzu Cluster Network resources.

If you plan on enabling “Machine Health Checks,” you’ll also need to have port 6443 open to all nodes of the cluster. Enabling health checks is an optional configuration step but recommended.

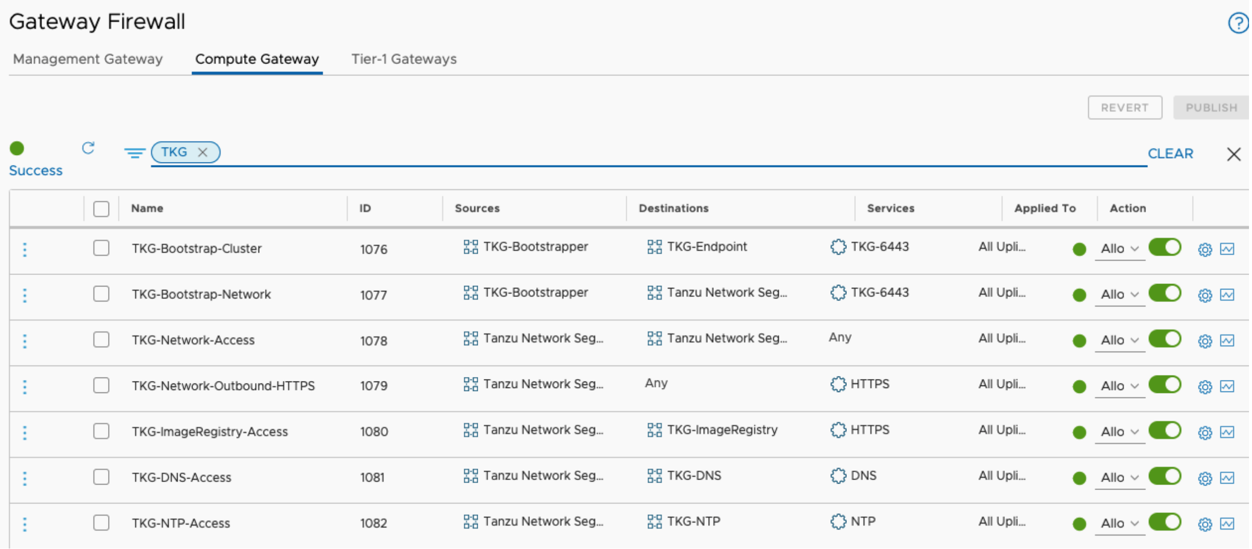
The Tanzu nodes should be able to communicate with each other. For this reason, it is assumed that the Tanzu Network Segment that will house the Kubernetes nodes will have access to any other nodes running on the same segment.

As mentioned previously, the Kubernetes clusters need access to vCenter for the creation of new nodes and requesting persistent volumes, etc. For this reason, the segment housing the Kubernetes nodes must have access to vCenter.

For the clusters to pull down the appropriate containers, access must be allowed for the Tanzu cluster nodes to retrieve them. By default, allowing HTTPS access to the Internet will enable the clusters to pull the images needed to build and operate the cluster. If you are in an environment that does not allow access to the Internet, then this should be your internal image registry with the appropriate images loaded.

And as with most environments, you should have firewall rules that allow the nodes to access the Network Time Protocol and DNS services.

Source	Destination	Port/Service
Bootstrap Machine	`Cluster Endpoint`	TCP 6443
Bootstrap Machine	`Tanzu Network Segment`	TCP 6443
Tanzu Network Segment	`Tanzu Network Segment`	ANY
Tanzu Network Segment	`vCenter`	HTTPS
Tanzu Network Segment	`Internet or Image Registry`	HTTPS
Tanzu Network Segment	`DNS Server`	TCP/UDP 53
Tanzu Network Segment	`NTP Server`	UDP 123


Gateway Firewall

	☐	Name	ID	Sources	Destinations	Services	Applied To	Action	
⋮	☐	TKG-Bootstrap-Cluster	1076	TKG-Bootstrapper	TKG-Endpoint	TKG-6443	All Upli...	● Allo	⚙
⋮	☐	TKG-Bootstrap-Network	1077	TKG-Bootstrapper	Tanzu Network Seg...	TKG-6443	All Upli...	● Allo	⚙
⋮	☐	TKG-Network-Access	1078	Tanzu Network Seg...	Tanzu Network Seg...	Any	All Upli...	● Allo	⚙
⋮	☐	TKG-Network-Outbound-HTTPS	1079	Tanzu Network Seg...	Any	HTTPS	All Upli...	● Allo	⚙
⋮	☐	TKG-ImageRegistry-Access	1080	Tanzu Network Seg...	TKG-ImageRegistry	HTTPS	All Upli...	● Allo	⚙
⋮	☐	TKG-DNS-Access	1081	Tanzu Network Seg...	TKG-DNS	DNS	All Upli...	● Allo	⚙
⋮	☐	TKG-NTP-Access	1082	Tanzu Network Seg...	TKG-NTP	NTP	All Upli...	● Allo	⚙

Additional Firewall Configurations

Depending on your desired configuration, you may need to add additional firewall rules to your Compute Gateway configuration. The table below outlines some of the common configurations used when deploying Tanzu Kubernetes Grid clusters on VMware Cloud on AWS.

Source	Destination	Port/Service	Purpose
Tanzu Network Segment	`Internet`	HTTPS	Tanzu Mission Control Integration
ANY	`Cluster Endpoint`	TCP 3124, 30167	LDAP / OIDC Integration with Dex/Pinniped
Tanzu Network Segment	`LDAPS Server`	TCP 636	LDAP Authentication to Active Directory (Secure)
Tanzu Network Segment	`OIDC Server`	HTTPS	OIDC Authentication
ANY	`Tanzu Network Segment`	HTTP/HTTPS or other	Access to cluster ingress for app access
Tanzu Network Segment	`Harbor`	HTTPS	Access to image registry

It’s worth noting that workload clusters should be able to be deployed using this configuration as long as they are also in the Tanzu Network Segment. Suppose you are to place Tanzu Kubernetes Clusters (TKCs) in a different network segment. In that case, additional firewall rules will need to be created to allow the management cluster to access those clusters.

Infrastructure as Code

If you would like to quickly deploy these rules in your own VMware Cloud on AWS environment, check out this PowerShell script to deploy these rules.

Summary and Additional Resources

This post walked through the required firewall rules needed to deploy Tanzu Kubernetes Grid on VMware Cloud on AWS. After reading, you should be able to setup the VMware Cloud on AWS environment either manually, or through the provided PowerShell script and are ready to being a TKG deployment.

Additional Resources

Deploy Tanzu Kubernetes Grid on VMware Cloud on AWS

Changelog

The following updates were made to this guide.

Date	Description of Changes
2021-06-1	Initial publication

About the Author and Contributors

Eric Shanks has spent two decades working with VMware and cloud technologies focusing on hybrid cloud and automation. Eric has obtained some of the industry's highest distinctions including two VMware Certified Design Expert (VCDX #195) certifications and many others across a variety of solutions including Microsoft, Cisco, and Amazon Web Services.

Eric's acted as a community contributor through work as a Chicago VMUG Users Group leader, blogger at theITHollow.com and Tech Field Day delegate.

- Eric Shanks, Sr. Technical Marketing Architect, Cloud Services Business Unit, VMware