Private Networking (AHV)

Customers using Nutanix AHV infrastructure can create a Frame account using Customer-managed networking, Private Networking so users must access the Frame workload VMs using the private IP addresses of the Frame workload VMs. Since the Frame workload VMs have no public IP addresses, the customer must provide a network path between the end user and the private Frame workload VMs. Customers will also need to ensure these workload VMs and Cloud Connector Appliances (CCAs) can communicate to the Frame control plane on the Internet.

If a customer requires an outbound proxy server for any communication to the Internet, the outbound proxy server must support both HTTPS and Secure WebSocket (WSS) in order for the Frame Guest Agent (FGA) and CCAs to establish HTTPS and WSS connections to Frame Platform.

To ensure proper network communication to the Frame Platform there are two Backends available depending on which one should be used for the connection for services and VMs please refer to the corresponding networking requirements:

USE (located in the United states- Location AWS Datacenter Virginia)

DEU (located in European Union - Location AWS Datacenter Frankfurt)

FRP8 Networking

FRP8 is a udp-based protocol for all communication between the end user and the Frame workload VMs.

Nutanix AHV - Private Networking (FRP8)

Nutanix AHV - Private Networking (FRP8)

The following table describes the required protocols and ports for Frame accounts using Private Networking and FRP8.

Dizzion is in the process of migrating from *.nutanix.com to *.difr.com domain. For the

time being, the additional difr.com domains will need to be whitelisted in addition to the existing nutanix.com domains. At a later time, once Dizzion has confirmed there is no dependencies on the nutanix.com domains, we will send out a communication notifying customers that all nutanix.com domains can be safely removed from your whitelist configurations.

IMPORTANT: For IMG Domains, Customers can whitelist new IMG difr domains but should NOT change SAML 2 configurations to use new difr.com domains. SAML 2 configurations should continue to use img.console.nutanix.com and img.frame.nutanix.com until further direction from Dizzion

USE: Nutanix AHV - Private Networking

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
Cloud Connector Appliance (CCA) to Frame Platform	Public IP address	• use.difr.com • api.use.difr.com • console.nutanix.com • cpanel-backend.console.nutanix.com • gateway-external-api.console.nutanix.com	tcp/443 (HTTPS)
Cloud Connector Appliance (CCA) to Frame Platform	Public IP address	• hub.use.difr.com • cch.console.nutanix.com	tcp/443 (HTTPS, WSS)
Prism Central to Frame Platform	Public IP address	• downloads.difr.com • downloads.console.nutanix.com	tcp/443 (HTTPS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
CCA to Prism Central	Private IP address	• Prism Central IP address	tcp/443 (HTTPS)
CCA to Prism Element	Private IP address	• Prism Element IP address	tcp/443 (HTTPS)
Workload VMs to Frame Platform	Public IP address	• api.use.difr.com • hub.deu.difr.com • logging.use.difr.com • downloads.difr.com • download.visualstudio.microsoft.com • gateway-external-api-prod.frame.nutanix.com • downloads.console.nutanix.com • logging.console.nutanix.com • cch.console.nutanix.com • download.visualstudio.microsoft.com	tcp/443 (HTTPS)
Workload VMs to Frame Platform	Public IP address	• hub.use.difr.com • logging.use.difr.com • api.use.difr.com • cch.console.nutanix.com	tcp/443 (HTTPS, WSS)
End user to Frame Platform	Public IP address	• use.difr.com • api.use.difr.com • img.use.difr.com • assets.use.difr.com • login.use.difr.com • logging.use.difr.com • downloads.difr.com • console.nutanix.com • img.frame.nutanix.com • img.console.nutanix.com • cpanel-backend.console.nutanix.com • terminal-prod.frame.nutanix.com • logging.console.nutanix.com • login.console.nutanix.com (for Frame IdP, if used)	tcp/443 (HTTPS)
End user to Frame Platform	Public IP address	api.use.difr.com	tcp/443 (HTTPS, WSS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
End user to Workload VM	Private IP address	Workload’s dynamic private IP address within VPC/VNET	udp/4503-4509, tcp /4503-4509 (optional)

FRP8 Networking

The following table describes the required protocols and ports for Frame accounts using Private Networking and FRP8, , specifically for organizations electing to use Dizzion's EU control plane.

DEU: Nutanix AHV - Private Networking

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
Cloud Connector Appliance (CCA) to Frame Platform	Public IP address	• deu.difr.com • api.use.difr.com	tcp/443 (HTTPS)
Cloud Connector Appliance (CCA) to Frame Platform	Public IP address	• hub.deu.difr.com	tcp/443 (HTTPS, WSS)
Prism Central to Frame Platform	Public IP address	• downloads.difr.com	tcp/443 (HTTPS)
Workload VMs to Frame Platform	Public IP address	• api.deu.difr.com • hub.deu.difr.com • logging.deu.difr.com • downloads.difr.com • download.visualstudio.microsoft.com	tcp/443 (HTTPS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
Workload VMs to Frame Platform	Public IP address	• hub.deu.difr.com • logging.deu.difr.com • api.deu.difr.com	tcp/443 (HTTPS, WSS)
End user to Frame Platform	Public IP address	• deu.difr.com • api.deu.difr.com • img.deu.difr.com • assets.deu.difr.com • login.deu.difr.com • logging.deu.difr.com • downloads.difr.com	tcp/443 (HTTPS)
End user to Frame Platform	Public IP address	• api.deu.difr.com	tcp/443 (HTTPS, WSS)
End user to Workload VM	Private IP address	Workload’s dynamic private IP address within VPC/VNET	udp/4503-4509, tcp/4503-4509 (optional)

Revision #13
Created 1 October 2025 04:47:15
Updated 9 January 2026 11:15:53 by Dragan Mladenovic