Networking

Requirements, Public Networking, Private Networking, Streaming Gateway, VPN Configurations

Networking

Decide on the following before creating your Frame account:

1. How will your users reach their workload VMs? From the Internet or from a private network?
2. Do you want Frame Control Plane to provision and manage the network where the workload VMs reside ("Frame-managed Networking") or whether you wish to manage the network yourself ("Customer-managed Networking")?
3. Will the workload VMs run in a public cloud or on-premises on a Nutanix AHV cluster?

This guide outlines the differences and tradeoffs between Frame-managed versus customer-managed networking and summarizes the network requirements based on the above choices for Frame and network administrators.

Management Responsibility

Note

Considerations

1. Frame-managed networking is only available when a Frame account is provisioned on public cloud infrastructure.
2. Customer-managed networking is required for Frame accounts provisioned on Nutanix AHV infrastructure.
3. Customer-managed networking is an option for Frame accounts provisioned on customer-managed public cloud infrastructure.
4. Customer-managed networking is not available when using Frame-provided public cloud infrastructure.

Frame-managed Networking

When Frame-managed networking is selected during Frame account creation in public cloud, Frame will provision all **public cloud** networking elements required for the operation of the

platform:

- VPC/VNET
- Subnets
- Routes
- Security groups/firewall rules
- NAT gateway
- DNS
- DHCP
- Load balancer (if required for SGA high availability).

When a Frame account is terminated, Frame control plane will deprovision all network elements it previously provisioned.

> If you attach network elements to the Frame-managed VNET or VPC after the Frame account is provisioned, Frame Control Plane will return an error and not deprovision the network elements when you terminate the Frame account.

Customer-managed Networking

When customer-managed networking is selected during Frame account creation in public cloud or on AHV clusters, the customer is responsible for provisioning and managing all **public cloud** or **AHV** networking elements required for the operation of Frame:

- VPC/VNET
- Subnets
- Routes
- Security groups/firewall rules
- NAT gateway
- DNS
- DHCP
- Load balancer (if required for SGA high availability).

The Frame account creation process requires the following information, which can be obtained from the console of your infrastructure provider. This information dictates where Frame control plane will provision the workload VMs.

Infrastructure	Configuration Parameters
AWS	VPC name and CIDR Subnet name and CIDR Security Group

Infrastructure	Configuration Parameters
Azure	Resource group name VNET name Subnet name and CIDR
AHV	VLAN name
GCP	VPC name Subnet name

Frame will only provision and deprovision virtual machines, volumes, and snapshots.

Requirements

Frame DaaS requires the Frame workload virtual machines (Sandbox, production, test, and Utility server) to be able to communicate with Frame control plane. It also requires end users to be able to communicate with the Frame control plane and the Frame workload VMs. Additionally, for Frame-managed workloads on Nutanix AHV clusters, the Frame Platform must be able to communicate with Prism Element and Prism Central via one or more Frame Cloud Connector Appliances (CCAs), a Frame-provided appliance you deploy in your AHV cluster(s).

Based on your overall configuration (user access, network responsibility, and infrastructure), choose and implement one of the deployment models in Network Requirements.

> If you choose **customer-managed networking**, you must ensure that your networking (CIDR, routes, security group/firewall rules) meets the [network requirements](/platform/networking/requirements) for the deployment model you wish to use **before** you attempt to create a Frame account.

WARNING

FQDN vs. IP Address

Frame protects its control plane from DDoS and external threats using a global content distribution network (CDN) and web application firewall. The public IP addresses associated with the Frame Fully-Qualified Domain Names (FQDNs) may change without notice and vary globally due to this CDN service.

Customers who deploy Frame into a private network (in public cloud or on-premises with AHV) may need to configure their network security appliances to allow Frame workload VMs (and Frame Streaming Gateway Appliances and Cloud Connector Appliances, if required) in their network to communicate with the Frame control plane. These customers are **strongly recommended** to use the Frame Fully-Qualified Domain Names (FQDNs) instead of public IP addresses. Alternatively, they may use an outbound proxy supporting HTTP/HTTPS and Secure WebSocket (WSS) in conjunction with their firewall.

If a customer chooses to use public IP addresses within their security appliances (instead of the Frame FQDNs), customers will need to monitor these Frame control plane DNS records and update their security appliances with the new Frame public IP addresses, if they change.

Requirements

Deployment Models

When deploying Frame workloads, customers can choose from five primary deployment models—**three for public cloud environments** and **two for Nutanix AHV clusters**. The choice of deployment model depends on your organization's specific use case(s) and security policies. Whether your workloads require public or private networking, or need to leverage static IP addresses or DHCP for dynamic assignment, each Frame account can be tailored to meet these requirements.

For further details on each deployment model and the networking requirements, select the specific hyperlink in the table below.

> **Considerations**
> Customers provisioning Frame accounts in their own network (**customer-managed networking**) in public cloud should select either *Private Networking* or *Private Networking with SGA* deployment models.

Deployment Type	Deployment Model	Description
Public Cloud	Public Networking	All workload VMs (Sandbox, Test, Production, and Utility Server VMs) hosted in a public cloud infrastructure have public IP addresses and are directly accessed by users from the Internet.
	Private Networking	All workload VMs (Sandbox, Test, Production, and Utility Server VMs) hosted in a public cloud infrastructure only have private IP addresses. Users must access the workload VMs through a private network connection.

Deployment Type	Deployment Model	Description
Private Networking with SGA	All workload VMs (Sandbox, Test, Production, and Utility Server VMs) hosted in a public cloud infrastructure have private IP addresses. However, users can access the workload VMs through a Streaming Gateway Appliance (SGA) from the Internet.	
AHV	Private Networking	All workload VMs (Sandbox, Test, Production, and Utility Server VMs) hosted on a Nutanix AHV cluster only have private IP addresses. Users must access the workload VMs through a private network connection.
	Private Networking with SGA	All workload VMs (Sandbox, Test, Production, and Utility Server VMs) hosted on a Nutanix AHV cluster have private IP addresses. However, users can access the workload VMs through a Streaming Gateway Appliance (SGA) from the Internet.

Dynamic vs. Static IP Addresses

All Frame-managed workload VMs require access to a DHCP service to obtain a dynamic IP address when they are created. The SGA and CCA Frame appliances, however, can be assigned static IP addresses.

Workload Type	IP Address Assignment
Sandbox	**DHCP (Dynamic IP)**
Utility Server	
Persistent Desktops	
Test/Production VMs	
Streaming Gateway Appliance (SGA)	**Static IP**

Workload Type	IP Address Assignment
Cloud Connector Appliance (AHV only)	

Public Networking (Public Cloud)

Customers using public cloud infrastructure can create a Frame account using Frame-managed networking, Public Networking so users on the Internet can directly access the Frame workload VMs using the public IP addresses of the Frame workload VMs. For egress to the Internet, these workload VMs communicate directly to the Internet for publicly-accessible resources.

If users must access network resources on-premises or in a private network, a private network connection (e.g., VPN, direct connection, SD-WAN, VPC/VNET peering) with the appropriate routing must be implemented.

> 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 us-east-1Virginia)
>
> DEU (located in European Union - Location AWS eu-central-1 Frankfurt)

FRP8 Networking

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

Public IaaS - Public Networking (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: Public IaaS - Public Networking (FRP8)

The following table lists the required protocols and ports for Frame accounts using Public Networking and FRP8.

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
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	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 • logging.console.nutanix.com • messaging.console.nutanix.com	tcp/443 (HTTPS, WSS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
Workload VMs to Frame Platform	Public IP address	• stun.use.difr.com	udp/3478
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 • messaging.console.nutanix.com	tcp/443 (HTTPS, WSS)
End user to Workload VM	Public IP address	• Workload’s dynamic private IP address within VPC/VNET	udp/4503-4509, tcp/4503-4509 (optional)

DEU: Public IaaS - Public Networking (FRP8

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

DEU: Public Networking (Public Cloud)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port

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)
Workload VMs to Frame Platform	Public IP address	• hub.deu.difr.com • logging.deu.difr.com • api.deu.difr.com	tcp/443 (HTTPS, WSS)
Workload VMs to Frame Platform	Public IP address	• stun.deu.difr.com	udp/3478
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	Public IP address	• Workload’s dynamic private IP address within VPC/VNET	udp/4503-4509, tcp/4503-4509 (optional)

FRP7 Networking End of Life

Warning

FRP7 reached end-of-life (EOL) effective June 30, 2024. Refer to the EOL Announcement of December 18, 2023 for further details.

Private Networking (Public Cloud)

Customers using public cloud infrastructure can create a Frame account using Frame-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. For egress to the Internet, these workload VMs communicate directly to the Internet through a NAT gateway in the public cloud infrastructure.

> Customers who choose to create a Frame account in their own managed network where all users access the Frame workload VMs within their private network must follow the networking requirements defined below.

If users must access network resources on-premises or in a private network, a private network connection (e.g., VPN, direct connection, SD-WAN, VPC/VNET peering) with the appropriate routing must be implemented.

> 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.

Public IaaS - Private Networking (FRP8)

Public IaaS - 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: Private Networking (Public Cloud)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port

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	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 • logging.console.nutanix.com • messaging.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 • messaging.console.nutanix.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)

FRP8 Networking - EU

The following table lists 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: Private Networking (Public Cloud)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
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)
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)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
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)

FRP7 Networking

Warning

FRP7 reached end-of-life (EOL) as of June 30, 2024. Refer to the EOL Announcement of December 18, 2023 for further details.

Private Networking with SGA (Public Cloud)

Customers using public cloud infrastructure can create a Frame account using Frame-managed networking, Private Networking with Streaming Gateway Appliance (SGA) so users can access the Frame workload VMs through the SGA. The Internet-accessible SGA serves as a reverse proxy for Frame sessions between the end users and their Frame workload VMs in the private network. The Frame workload VMs only have private IP addresses. For egress from the workload VMs to the Internet, these workload VMs are configured to communicate directly to the Internet through a NAT gateway in the public cloud infrastructure.

If users must access network resources on-premises or in a private network, a private network connection (e.g., VPN, direct connection, SD-WAN, VPC/VNET peering) with the appropriate routing must be implemented.

> Customers who choose to create a Frame account in their own managed network where users will access the Frame workload VMs from the Internet through an SGA must follow the networking requirements defined below.

> 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 (SGA 4)

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

Public IaaS - Private Networking with SGA 4 (FRP8)

Public IaaS - Private Networking with SGA 4 (FRP8)

The following table describes the required protocols and ports for Frame accounts using Private Networking with SGA 4 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: Private Networking (Public Cloud) - Streaming Gateway 4

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port

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- • downloads.console.nutanix.com • logging.console.nutanix.com • cch.console.nutanix.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 • logging.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 • messaging.console.nutanix.com	tcp/443 (HTTPS, WSS)
SGA VMs to Frame Platform	Public IP address	• hub.use.difr.com • ntp.ubuntu.com • api.snapcraft.io • cch.console.nutanix.com	tcp/443 (HTTPS, WSS)
End user to SGA VM	Public IP address	• SGA VM-specific public IP address	udp/3478 and tcp/3478

SGA VM to End user	Public IP address	• End user-specific public IP address	udp/49152–65535
SGA VM to Workload VM	Private IP address	• Dynamic private IP address within VPC/VNET	udp/4503–4509
Workload VM to SGA VM	Private IP address	• SGA VM-specific private IP address	udp/49152–65535

FRP8 Networking (SGA 4)

The following table lists the required protocols and ports for Frame accounts using Private Networking with SGA 4 and FRP8, specifically for organizations electing to use Dizzion's EU control plane.

DEU: Private Networking (Public Cloud) - Streaming Gateway 4

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
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)
Workload VMs to Frame Platform	Public IP address	• hub.deu.difr.com • logging.deu.difr.com • api.deu.difr.com	tcp/443 (HTTPS, WSS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/port
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)
SGA VMs to Frame Platform	Public IP address	• hub.deu.difr.com • ntp.ubuntu.com • api.snapcraft.io	tcp/443 (HTTPS, WSS)
End user to SGA VM	Public IP address	• SGA VM-specific public IP address	udp/3478 and tcp/3478
SGA VM to End user	Public IP address	• End user-specific public IP address	udp/49152–65535
SGA VM to Workload VM	Private IP address	• Dynamic private IP address within VPC/VNET	udp/4503–4509
Workload VM to SGA VM	Private IP address	• SGA VM-specific private IP address	udp/49152–65535

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)

Private Networking with SGA (AHV)

Customers using Nutanix AHV infrastructure can create a Frame account using Customer-managed networking, Private Networking with Streaming Gateway Appliance (SGA) so users can access the Frame workload VMs through the public IP address of the SGA VM. The Internet-accessible SGA VM serves as a reverse proxy for Frame sessions between the end users and their Frame workload VMs in the private network. The Frame workload VMs only have private IP addresses. Customers will also need to ensure these workload VMs, Cloud Connector Appliances (CCAs), and Streaming Gateway Appliances (SGAs) 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), CCAs, and SGAs 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 us-east-1Virginia)

DEU (located in European Union - Location AWS eu-central-1 Frankfurt)

FRP8 Networking (SGA 4)

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

Nutanix AHV - Private Networking with SGA (FRP8)

Nutanix AHV - Private Networking with SGA (FRP8)

The following table describes the required protocols and ports for Frame accounts using Private Networking with SGA 4 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 with Streaming Gateway 4

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)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/ port
Prism Central to Frame Platform	• Public IP address	• downloads.difr.com • downloads.console.nutanix.com	tcp/443 (HTTPS)
CCA to Prism Central	Private IP address	• Prism Central 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 • logging.console.nutanix.com • messaging.console.nutanix.com	tcp/443 (HTTPS, WSS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol/ port
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 • messaging.console.nutanix.com	tcp/443 (HTTPS, WSS)
SGA VMs to Frame Platform	Public IP address	• hub.use.difr.com • cch.console.nutanix.com • ntp.ubuntu.com • api.snapcraft.io (Canonical Snapcraft)	tcp/443 (HTTPS, WSS)
End user to SGA VM	Public IP address	• SGA VM-specific public IP address	udp/3478 and tcp/3478
SGA VM to End user	Public IP address	• End user-specific public IP address	udp/49152–65535
SGA VM to Workload VM	Private IP address	• Dynamic private IP address within VPC/VNET	udp/4503–4509
Workload VM to SGA VM	Private IP address	• SGA VM-specific private IP address	udp/49152–65535

FRP8 Networking (SGA 4)

The following table lists the required protocols and ports for Frame accounts using Private Networking with SGA 4 and FRP8, specifically for organizations electing to use Dizzion's EU control plane.

DEU: Nutanix AHV - Private Networking with Streaming Gateway 4

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.deu.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 (not required starting with PC 2023.4)	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)
Workload VMs to Frame Platform	Public IP address	• hub.deu.difr.com • logging.deu.difr.com • api.deu.difr.com	tcp/443 (HTTPS, WSS)

Source to Destination	Source IP address	Destination FQDN(s)	Protocol /port
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)
SGA VMs to Frame Platform	Public IP address	• hub.use.difr.com • ntp.ubuntu.com • api.snapcraft.io (Canonical Snapcraft)	tcp/443 (HTTPS, WSS)
End user to SGA VM	Public IP address	• SGA VM-specific public IP address	udp/3478 and tcp/3478
SGA VM to End user	Public IP address	• End user-specific public IP address	udp/49152–65535
SGA VM to Workload VM	Private IP address	• Dynamic private IP address within VPC/VNET	udp/4503–4509
Workload VM to SGA VM	Private IP address	• SGA VM-specific private IP address	udp/49152–65535

VPN Configurations

Some customers need to integrate Frame into a network where VPNs are used. This guide discusses the use of VPNs for common Frame solution architectures.

End User Access to Frame Workloads

Customers who have end users on the Internet who need to access Frame workloads in a private network can use a point-to-site VPN between the end user and the workloads or Streaming Gateway Appliance (SGA). If the customer requires a point-to-site VPN, the client VPN software can be configured for split-tunnel or full-tunnel, provided that the client's endpoint can still resolve Frame-related public fully-qualified domain names (FQDNs).

Frame Workload Access to Private Networks

Customers who need their users to access an existing private network (usually on-premises) from Frame workloads in public cloud need a secure way to connect to the private network. Once this connection is established, users running on Frame can securely access resources from the network such as file servers or license servers. Customers can chose from a number of different options, based on the desired end user experience, security, cost, and performance.

Software VPN Client

Installing a software VPN client within the Frame workload VMs will allow you to quickly publish a VPN client to all of your users. Simply install the VPN client software in the Sandbox and test the connection before publishing to your production instances.

When setting up your VPN client, you must use a **split-tunnel configuration** to ensure:

1. Frame workload VMs can continue communicate to the Frame Control Plane
2. The Frame Remoting Protocol traffic between end user and their Frame workload VM can continue to flow. If the Frame Remoting Protocol traffic is unable to route back from the workload VM to the end user's endpoint after the software VPN client starts up its VPN connection, the end user will be abruptly disconnected from their Frame session.

> It is also possible to automatically prompt users to login via VPN when they start a session on Frame by using [pre-session scripts](/books/platform-administrators-guide/page/scripting).

Frame works with Cisco AnyConnect, GlobalProtect, OpenVPN, and SonicWall services. Any other VPN clients that support split-tunnel configurations should work as well.

Site-to-Site VPN

For customers who deploy Frame workloads in public cloud and require end users to access network services in their private, on-premises network, customers can design and implement a site-to-site Virtual Private Network (VPN) using their public cloud provider's VPN Gateway solution. Use of a site-to-site VPN eliminates the need for end users to authenticate to a VPN Gateway while in a Frame session.

To learn more about VPN gateways, review the documentation below for each of the supported public cloud infrastructures:

- AWS
- Azure
- GCP
- IBM

Other Private Inter-Networking Solutions

Customers can use other private inter-networking solutions:

- VPC/VNET peering, if the Frame workloads in one VPC/VNET need to communicate with resources in a different VPC/VNET on the same public cloud infrastructure
- AWS Direct Connect, Azure ExpressRoute, or Google Cloud Interconnect
- SD-WAN

The design, deployment, and management of these inter-networking solutions are the responsibility of the customer.