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.

Revision #3
Created 1 October 2025 04:47:10
Updated 18 December 2025 12:05:37 by Dominik Conrad