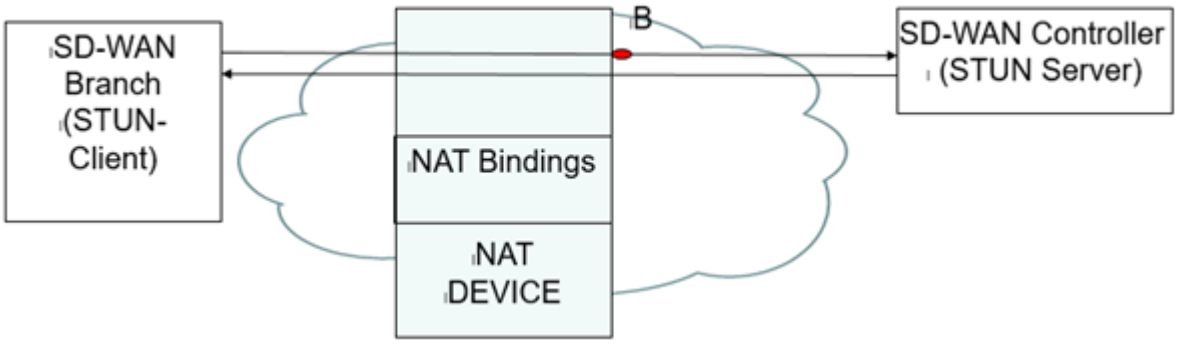
NAT Traversal

For supported software information, click here.

When some remote sites are outside the service provider footprint, the service provider may not have full control of the end-to-end path between remote SD-WAN branches within the same SD-WAN VPN instance (that is, NAT firewall instances along the path). The Versa SD-WAN NAT traversal solution provides a way to handle any NAT layer that exists between different SD-WAN remote branches.

NAT traversal is a key requirement when it comes to SD-WAN technology, as the main concept is about establishing tunnels over any network and it is likely that NAT and firewall functions exist along the path for establishing a tunnel path. For example, the NAT function is generally enabled on 4G PDN gateways. The Versa SD-WAN solution uses VXLAN generic protocol encapsulation (GPE) to provide NAT traversal capabilities for IPsec. VXLAN GPE addresses the problem of traffic exiting a NAT device, but it offers no solution for handling return traffic. To address NAT traversal and to make sure that Versa SD-WAN Versa Operating System™ (VOS™) devices (CPEs, gateways, and Controllers) can establish communication, the Versa SD-WAN solution uses the Session Traversal Utilities for NAT (STUN) protocol and VOS devices acting as hubs for traversing NAT endpoint-independent mapping (EIM) and NAT endpoint-dependent (ED) devices that may exist along the path.

The STUN protocol is used by branches to discover the NAT IP address seen by the Controller, where the branch is the STUN client and the Controller is the STUN server. The branch runs the STUN protocol on each local access circuit.



Supported Software Information

Releases 20.2 and later support all content described in this article.