VMware SD-WAN Edge by VeloCloud Firewall Functionality

velocloud™
Now part of VMware

The purpose of this document is to describe the functionality of the firewall implemented in the VMware SD-WAN Edge by VeloCloud.

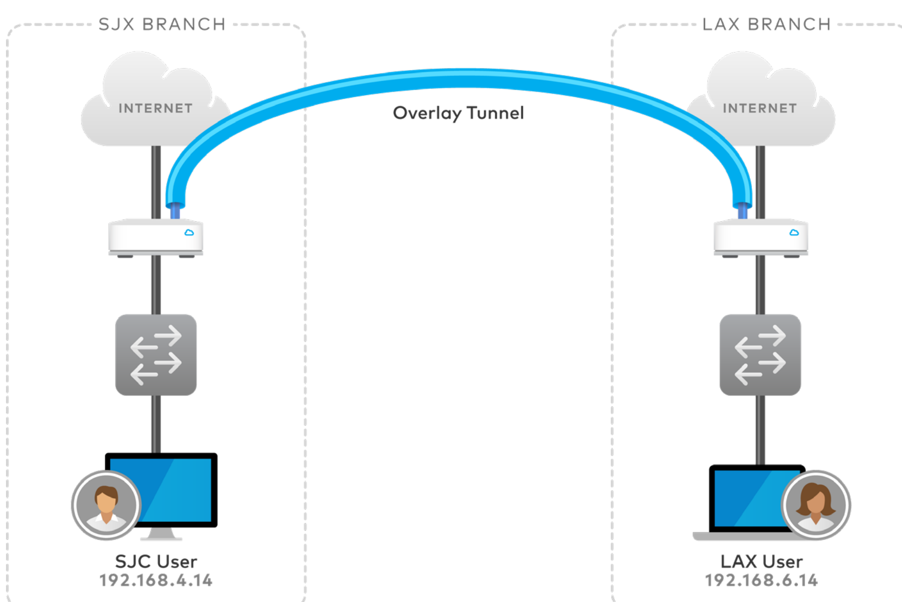
Firewall Capabilities on VMware SD-WAN Edge

On the VMware SD-WAN Edge, the firewall rules can be configured only on the outbound side. The rules are used to determine which traffic is allowed out from LAN to the Internet, overlay, and between LAN segments.

Examples

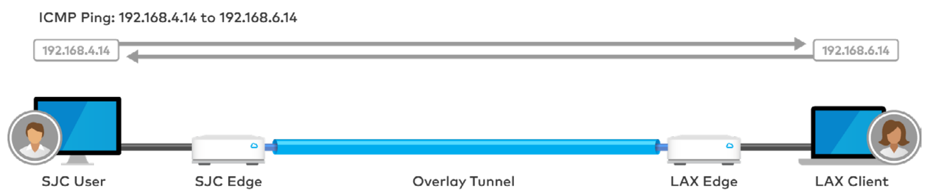
Examples of how this is performed will better explain this description.

Example 1: The enterprise network is powered by VMware SD-WAN.



Scenario 1

Ping from SIC user to LAX user.



The firewall has an "allow all" policy, so all the packets will go through. There is not much firewalling in this scenario.

Scenario 2

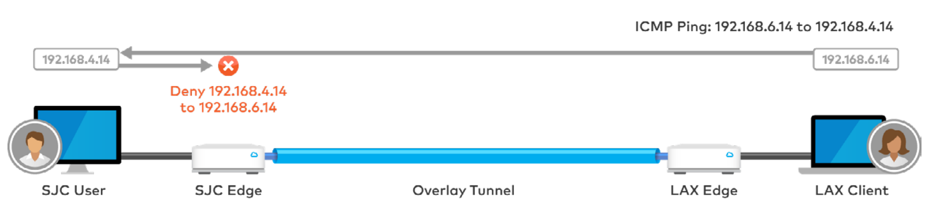
Configuration of an outbound firewall rule on the VMware SD-WAN Edge in the SJC branch location. The firewall rule will deny any traffic originating from 192.168.4.14 and going to 192.168.6.14 on any/all ports. As expected, when the SJC-user initiates ping traffic to LAX-user at 192.168.6.14, the firewall blocks the communication due the configured "deny" rule.

Scenario 3

Block the communication originating from LAX-user (192.168.6.14) to the SJC-user (192.168.4.14). There are two ways to configure this:

1. A rule on the LAX edge denying traffic from 192.168.6.14 to 192.168.4.14

2. A rule on the SJC VMware SD-WAN Edge denying traffic from 192.168.4.14 to 192.168.6.14. The ICMP reply gets blocked with this rule.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com