SD-WAN APPLIANCES AND UCAAS

A BASIC GUIDE TO UNDERSTANDING EQUIPMENT SELECTION: PROS AND CONS

SD-WAN and UCaaS are the 'in' thing in today's networking marketplace. Unfortunately, they don't always work well together. This document will discuss considerations that should be made when planning an SD-WAN deployment that will work properly with the RingCentral UCaaS services.

TYPES OF SD-WAN

SD-WAN has become a catch-all marketing phrase used to identify many various types of equipment. Everyone that could do so stretched the definition of SD-WAN so that their equipment fit into their definition for marketing reasons.

In the SD-WAN world, there are three major categories of SD-WAN appliances and an almost infinite array of subcategories. Note that we use the generic term *appliances* instead of *devices* as many of these offerings are available in both hardware and virtualized forms.

1. ***Stand-alone appliances*** switch outbound traffic between WAN ports based upon customer defined rules and link availability. This appliance simply practices rule-based failover between WAN links. S-NAT is applied to outbound traffic on each WAN link resulting in a source address (return address) of the WAN link being used for the current data transmission.

2. ***Book-ended mesh appliances*** switch outbound traffic flows between appliances at different customer sites or gateway sites using a network of meshed VPN tunnels. No NAT is applied until the traffic is directed out through a gateway which may or may not be part of the SD-WAN mesh. Traffic retains its original source address until S-NAT is applied as it egresses the customer network, hopefully through a very high quality and stable connection.

   Customer rules may allow non-critical traffic to egress via the local WAN links.

   These appliances are usually advanced and may offer additional services. Actual laboratory testing at RingCentral using FEC and Packet Duplication features on the tunnel mesh showed that many of these appliances will maintain toll quality calls even with all the WAN links suffering 15% random packet loss simultaneously. This is a huge advantage when deploying to sites that have poor Internet service. This feature can frequently be applied to a site with a single WAN link to improve UCaaS performance.

3. ***Network vendor meshed appliances*** switch outbound traffic flows between appliances using a vendor-maintained network. The traffic may egress via vendor supplied gateways on the vendor network, via the local WAN links, or via site appliances specially configured to act as service gateways. Otherwise, all the points mentioned in the 'Book-ended mesh appliances' discussion pertain to them.

1) STAND-ALONE APPLIANCES

Stand-alone SD-WAN Appliances monitor multiple WAN links and direct outbound traffic through them based upon a set of user-defined rules. In the event of a failure or degradation of one link, traffic on a failing WAN link that has been identified by user-defined rules as critical is redirected through a different WAN link. Traffic flow is returned to the original link upon recovery. This wreaks havoc with UCaaS systems because the NAT source address of the traffic changes with each link redirection, resulting in active phone calls going silent / dropping and phones losing registration, timing out, and having to reregister.

This category of SD-WAN appliances should not be used for UCaaS traffic unless you are certain that your WAN links are *extremely* reliable and you are willing to accept the issue when it occurs.

Pros:

- Inexpensive
- Quick to implement
- Quickly responds to WAN link failure

Cons:

- All TCP/SSL/RTP connections must timeout and be reestablished when the connection moves between WAN links
- Active calls go silent and must timeout when the connection moves between WAN links
- Phones lose registration and must timeout/reregister when the connection moves between WAN links (this may take over 5 minutes, though some few appliances will shorten the timeout period by sending a TCP RST signal to active connection endpoints)

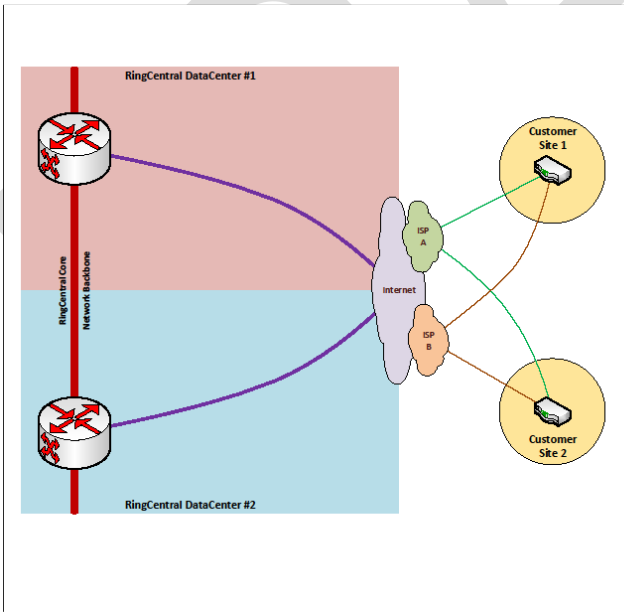

Figure 1 - Standalone SD-Wan Appliance

2) BOOK-ENDED MESH APPLIANCES

Book-ended Mesh SD-WAN Appliances establish a full mesh of tunnels interconnecting all a customer's sites using multiple WAN links. Tunnels are preestablished over all WAN links to each site. Complex algorithms monitor and control the flow of traffic between sites. Failure or degradation of a tunnel's underlying WAN link is detected, and the appliances quickly shift traffic away from that tunnel to a different tunnel preestablished on another WAN link.

Some of the appliances support FEC or Packet Duplication and can compensate for degraded links. Testing in the RingCentral Custom Engineering lab showed that these appliances can usually compensate for over 15% random packet loss on all WAN links simultaneously while maintaining toll quality voice. *{Please note that while this mechanism maintains high quality communications, it may mask a failing circuit from a customer. Care must be taken to ensure that a mechanism is present to warn the customer of degraded circuits!}*

Service Gateways may be set up to provide access for specific external service providers such as RingCentral, AWS, Azure, etc. Use of a Service Gateway site assures continuity of service during a local WAN issue because the NAT source address does not change as local site traffic dynamically shifts between WAN links. Alternatively, one of the customer sites with known good Internet service can be used to gateway traffic to the external service providers.

Pros:

- Quickly responds to WAN link failure or degradation
- Properly architected, voice traffic remains stable during local WAN issues
- Customer traffic remains on customer owned equipment for security

Cons:

- Expensive
- Extensive rollout effort for customers with large numbers of sites
- Customers with large numbers of sites result in huge numbers of tunnels with associated overhead
- Moderately complex configuration

Examples:

- Silver Peak
- Talari
- CloudGenix
- FatPipe
- Versa
- Viptella
- Citrix

CORPORATE SERVICE GATEWAYS

Service Gateways may be operated in central Corporate locations or data centers where there are very high-quality Internet connections as shown below in Figure 2. This is a common architecture and is preferred by many corporate security groups to force the flow of all traffic through several centralized locations for security vetting and IDS functionality.

It should be noted that many of these SD-WAN appliances implement advanced, localized, distributed IDS and firewall controls with centralized control and configuration. This allows the implementation of centrally configured/maintained security without the cost in bandwidth and latency of centralized traffic routing.

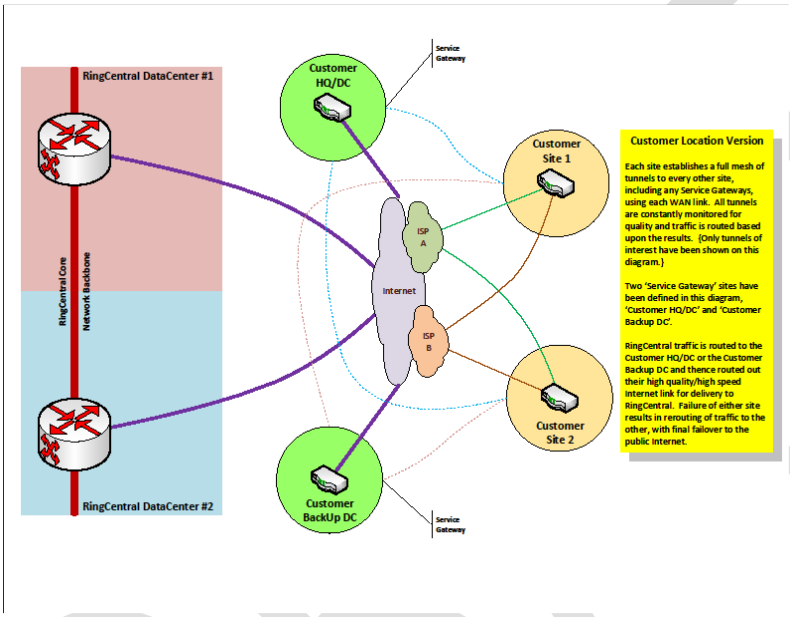

Figure 2 - Book-end Corporate Variant

AWS SERVICE GATEWAYS

Service Gateways may be operated in as virtual appliances in the AWS infrastructure as shown below in Figure 4. RingCentral is directly connected to the AWS cloud and most of the AWS visualization sites are co-resident in the same campuses as RingCentral. Latency between AWS and RingCentral is usually less than 5ms. DSCP markings are not guaranteed to be maintained across the AWS ⇔ RingCentral data pathway.

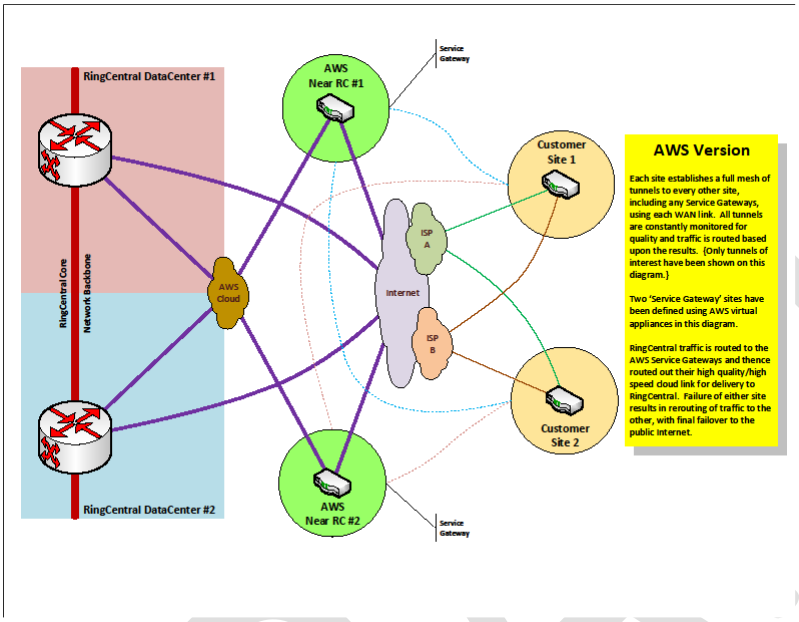

Figure 3 - Book-end AWS Variant

EQUINIX NETWORK EDGE SERVICE GATEWAYS

Service Gateways may be operated as virtual appliances in the Equinix Network Edge infrastructure as shown below in Figure 5. RingCentral is easily accessible using an ECX cross-connect. Latency between Network Edge and RingCentral is generally less than 1ms. The ECX link is a direct layer-2 interconnect and all DSCP/QoS information is maintained across the link. This architecture requires advance planning and purchase of a RingCentral CloudConnect option for each data center in which it is implemented. The appliance is set up as a BGP peer with the RingCentral Customer Edge Router. This BGP peering relationship is monitored by the RingCentral NOC and generates alarms on failure.

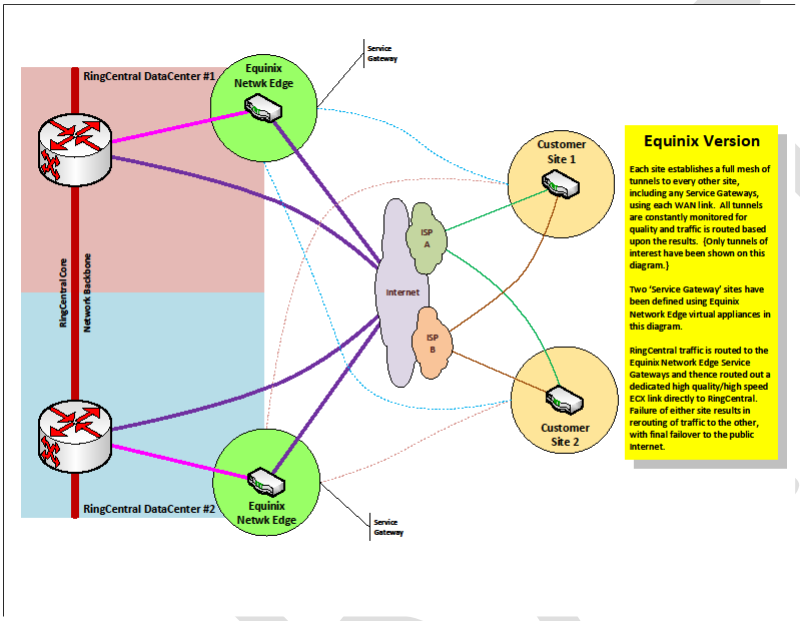

Figure 4 - Book-end Equinix Variant

3) NETWORK VENDOR MESHED APPLIANCES

Network Vendor Meshed SD-WAN Appliances are similar to Book-ended Mesh SD-WAN Appliances, but they establish a full mesh with nodes in a network vendor's network. The vendor's network routes traffic between the Customer's sites and to/from Service Gateways. (Some vendors may also provide for inter-site links directly between selected site appliances for optimization of specific traffic.) Some vendors have implemented Service Gateways to peer directly with various Service Providers such as RingCentral.

Pros:

- Quickly responds to WAN link failure or degradation
- **Very** fast rollout
- Properly architected, voice traffic remains stable during local WAN issues
- Vendor is responsible for Service Gateway ⇔ RingCentral stability and quality

Cons:

- Ongoing recurring charges
- Customer traffic traverses the vendors' network equipment

Examples:

- Velocloud
- GTT (Velocloud based, peers with RingCentral)
- CATO
- Aryaka
- Citrix

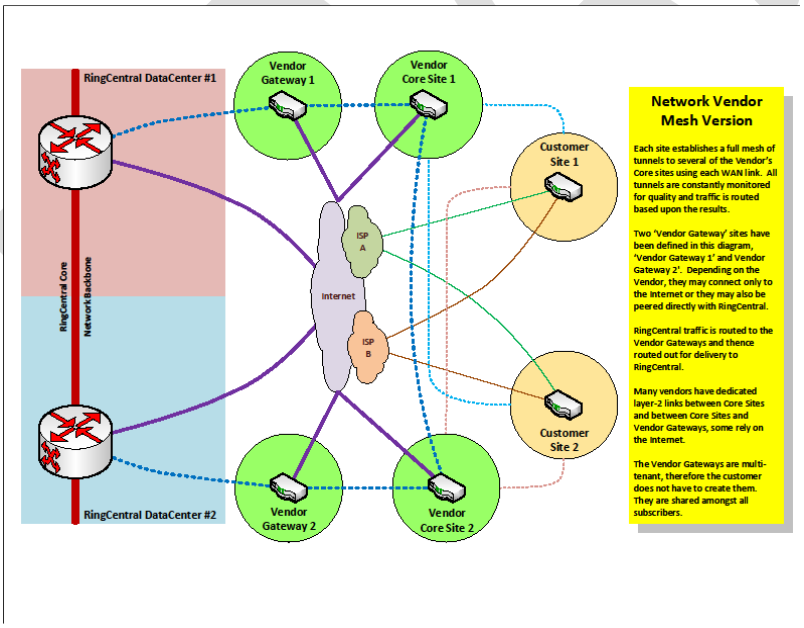

Figure 5 - Vendor Network Mesh