Adventures in SDWAN Customer Prem Deployments

Brian Knight, Sr Network Engineer
Nitel
Who we are - Nitel

• U.S.-based wireline ISP
  • Internet, MPLS, Layer 2 Ethernet
  • Focused on business customers
  • 7 POPs around the country
  • Managed hardware – routers, VoIP gateways, firewalls, and now SDWAN
What is SDWAN to us?

- Easy MPLS VPN replacement
- Ability to steer and load-balance customer traffic across multiple circuits
- Provide security services on-box – L4 firewall / NG firewall / UTM
- Multi-tenant portal
- Do all of this on commodity x86 hardware
What did SDWAN become?

• We found customers also wanted Internet load-balancing without the hassle of getting a /24 + ASN + BGP from carriers
• The ability to load-balance traffic flows became less important
2 Vendor solutions

• Vendor Q
  • Newer company, newer offering
  • Wrote their own software stack
  • Provides the multi-tenant web portal
  • Centralized analytics on detail logs (firewall / NAT logs) and aggregate logs (Netflow-like data)

• A core stack of servers resides on the Nitel network
  • Management console
  • Virtualized route reflector
  • Log gathering / log database
2 Vendor solutions

• Vendor Z
  • Older, more established company
  • Adapted a firewall product to do SDWAN
  • Centralized configuration
  • But logs are kept on the firewall at the premises
• A single management console server is required
• Report generation servers can be added
  • These servers reach out to the CPE firewalls, gather their logs, and generate reports
  • No logs are stored on these systems
SDWAN Go-Live

• Went live June 2017 with Vendor Q
• Vendor Z go-live Feb 2018
• Over 250 units shipped to ~35 customers (Sept 2018)
Challenges - 1

• Sourcing white label hardware for Vendor Q can be difficult
  • Hardware is not stocked, so manufacturers must do production runs
  • Lead times ~12wks
  • Vendor Q is helping to reduce these intervals

• Software-defined instability
  • Vendors are in a rush to capitalize on the market
  • So code quality can be a struggle, especially for newer players

• Learning curve for newer vendors can be higher
Challenges - 2

• Customer readiness
  • Integrating our stuff with existing customer LAN networks gets much more difficult the further up the stack one goes
    • Routing – relatively easy
    • L4 Firewall – harder, must know about customer policies
    • NG Firewall – even harder, must know about customer policies + IDS/IPS settings + AV + ...
    • SDWAN – must know about all of above + how customer wants to route traffic
Challenges - 3

• Customer readiness
  • Integrating third party MPLS was unexpectedly difficult
    • Vendor Q requires reachability to the core stack for operation
    • Leads to failure modes that are difficult to describe
  • Third party MSPs tend to increase this difficulty - but not always

• Metered Internet connections have been a challenge
  • Overages occur on account of ping probes among different nodes
  • Hub & Spoke topology was required for these customers
Questions?

Thank you