ONUG Software-Defined WAN Use Case

A white paper from the
ONUG SD-WAN Working Group

October, 2014

Definition of Open Networking

Open networking is a suite of interoperable software and/or hardware that delivers choice and design options to IT business leaders, service and cloud providers. At its core, open networking is the separation or decoupling of specialized network hardware and software - all in an effort to give IT architects options in the way in which they choose to design, provision, and manage their networks. These technologies must be based on industry standards. The standards can be de-facto as adopted by a large consortium of the vendor community, open in the sense that they are community based, or defined as standards by the prevailing standards bodies. Open networking hopes to deliver on two promises:

1) Decoupling of network hardware and software which mitigates vendor lock-in and shifts network architecture structure options to users
2) Significant reduction of the total cost of ownership model, especially operational expense

Scope

The scope of this document is to provide a set of tactical and strategic requirements that may help guide enterprises in their selection of Software Defined – Wide Area Network (SD-WAN) vendor solutions. The current set of WAN problems are highlighted and SD-WAN implications to be considered within enterprise wide area networks as designed and operated by in-house teams and/or managed service providers.

While the impacts discussed are commensurate with an ITIL service delivery model, enterprises can leverage the information for an RFI and adapt to scale and suit their current or planned organizational support delivery and maturity capabilities.

Executive Summary

This document is comprised of four major focus areas surrounding Enterprise SD-WANs.

I. The problem statement as experienced in today's enterprise wide area networks.
II. The WAN architectural models prevalent within most enterprises.
III. The desired SD-WAN enterprise product features and functionality.
IV. SD-WAN implications to service management support tools and delivery processes.

The expected outcome for SD-WAN enterprise adoption and usage can be summarized, but is not limited to, meeting this set of 10 business requirements:

1. Ability for remote site/branch to leverage public and private WANs in an active-active fashion for business applications.
2. Ability to deploy CPE in a physical or virtual form factor on commodity hardware.
3. A secure hybrid WAN architecture that allows for dynamic traffic engineering capability across private and public WAN paths as specified by application policy, prevailing network WAN availability and/or degradation at transport or application layer performance.
4. Visibility, prioritization and steering of business critical and real-time applications as per security and corporate governance and compliance policies.
5. A highly available and resilient hybrid WAN environment for optimal client and application experience.
6. Layer 2 and 3 interoperability with directly connected switch and/or router.
7. Site, Application and VPN performance level dashboard reporting.
8. Open north-bound API for controller access and management, ability to forward specific log events to network event co-relation manager and/or Security Incident & Event Manager (SIEM).
9. Capability to effect zero touch deployment at branch site with minimal to no configuration changes on directly connected infrastructure, ensuring agility in provisioning and deployment.
10. FIPS 140-2 validation certification for cryptography modules/encryption with automated certificate life cycle management and reporting.

SD WAN WORKING GROUP
2014
Open Networking
USER GROUP

Open Networking User Group (ONUG)

ONUG is one of the largest industry user groups in the networking and storage sectors. Its board is made up exclusively of IT business leaders, with representation from Fidelity Investments, FedEx, Bank of America, UBS, Cigna, Pfizer, JPMorgan Chase, Citigroup, Credit Suisse, Gap, Inc., and Symantec. The ONUG mission is to guide and accelerate the adoption of open networking solutions that meet user requirements as defined through use cases, proof of concepts, hackathons, and deployment examples to ensure open networking promises are kept.

The ONUG community is led by IT business leaders and aims to drive industry dialogue to set the technology direction and agenda with vendors. To that end, ONUG hosts two major conferences per year where use cases are defined and members vote to establish a prioritized list of early adopter, open networking projects that communicate propensity to buy and budget development. The vendor community stages proof of concepts based upon ONUG Use Cases, while standards and open source organizations prioritize their initiatives and investments based upon them. ONUG also hosts user summits and smaller, regional user-focused Fireside Chat Meet-Ups through the year.

ONUG defines six architectural areas that will open the networking industry and deliver choice and design options. To enable an open networking ecosystem, a common multivendor approach is necessary for the following six architecture components:

1) Device discovery, provisioning, and asset registration for physical and virtual devices
2) Automated "no hands on keyboards" configuration and change management tools that align DevOps and NetOps
3) A common controller and control protocol for both physical and virtual devices
4) A baseline policy manager that communicates to the common controller for enforcement
5) A mechanism for sharing (communicating or consuming) network state and a unified network state database that collects, at a minimum, MAC and IP address forwarding tables automatically
6) Integrated monitoring of overlays and underlays

I. The Problem Statement

On a year-over-year basis, enterprise wide area networks have become increasingly complex and costly to manage and maintain. At the same time, businesses require 24 x 7 network uptime, so enterprise network teams are faced with shrinking change windows, often competing for the same time window set aside for application delivery and support teams. Production and efficiency at remote business sites/branches is adversely impacted by a number of traditional design and operational factors within the WAN that is called out here, but not necessarily limited to the following:

i) Significant delays and cost in provisioning cycles of remote sites.

Delays in carrier access layer provisioning at remote sites can take weeks to months. Provisioning of a T1 MPLS circuit can take anywhere from 30 to 90 days, despite in many cases where expedited fees are paid by the customer. Provisioning of higher speed, higher cost MPLS circuits (DS3 and above) take even longer, stretching to a time frame of six months or longer, primarily driven in most cases by absence of fiber to/at a remote site. In many such instances that play out across enterprise customer networks, internet links at the same remote sites may be provided via terrestrial cable/DSL access as well as via 4G LTE wireless access and have reasonably shorter provisioning cycles.

Businesses have an immediate need to start up operations at these remote sites without incurring prolonged delays, and the availability of these internet access links present a viable transport alternative to delay prone legacy T1/n x T1 (bundled T1) MPLS links. Yet, enterprise IT is challenged with the complexity of configuration and security at the remote site/branch router via these T1/n X T1, internet links. An MSP or a carrier-managed MPLS network not only requires additional levels of co-ordination across in-house and carrier/MSP resources, it also requires linkages to enterprise service support and delivery processes, which of course, come at an additional cost and effort. Bottom line: efforts on a site-by-site basis are time consuming and costly, and, being manually intensive, are prone to error.

ii) Operational and management complexities, resulting in provisioning and remediation inefficiencies.

Varying bandwidth via multiple access links and multiple providers providing connectivity into the remote site/branch give rise to a complex router/s configuration in order to accommodate features, such as link bundling (via MLPPP), Quality of Service, Multicast, VPN and avoidance of asymmetric routing besides others. This complexity not only impacts site turn up implementation of remote sites/branches, but also posts implementation operations monitoring and management of wide area networks.

Let's take the case of bundled T1 links via a MLPPP layer 2 configuration. It facilitates remote site/branch router Tx/Rx load balancing plus allows for a single IP address across the n x T1 links, alleviating additional PE IP level configuration for MSPs/carriers and reducing the number of IP addresses to be tracked and monitored via the enterprise/carrier/MSP NOC. However, since BGP operating at layer 3 has no visibility into the underlying layer 2 MLPPP protocol, failing/error degraded T1 circuits within a bundle go undetected unless monitored on a per-port basis. There are some industry proposals and very limited implementations available, where running BFD on components links can potentially detect the faulty component links

but does not necessarily address the problem completely. In an enterprise with several thousand sites/branches, this port-level monitoring of remote bundled circuits can be a daunting task for any NOC. Since the NOC is left monitoring a single IP address, these individual link/s failures, which at times are silent, within a bundle cause severe transport degradation, bringing application access to a crawl.

Traffic Symmetry and Inefficient WAN Bandwidth Utilization

In the current enterprise architectures, especially the environments with multiple WAN connectivity options, routing is set up in such a way that one path is chosen as primary, and the other is configured as secondary to ensure traffic symmetry so that infrastructure elements, such as firewalls and/or WAN optimization solutions, can still work effectively. In this scenario, the secondary path becomes active only upon primary path failure. Such an active-backup routing setup not only requires complex routing, redistribution and loop avoidance policies, but it is obviously sub-optimal and does not allow efficient use of all the available WAN bandwidth.

The problem gets even worse in partial failure scenarios with MLPPP. For example, in cases where there is a second private WAN or internet link, a situation arises wherein the second path or internet link has a higher bandwidth than the lone working T1 remaining in the MLPPP bundle. However, alternate path, with plenty of bandwidth, cannot be used since primary path from routing point of view is still valid. Similarly, any hard or soft failure within service provider network may not be immediately visible to the enterprise edge device to react quickly. The situation can become even more challenging in brown-out situations where the enterprise edge device has no knowledge, whatsoever, of failures within the service provider network if traditional routing protocols fail to detect and communicate the state of failures. A considerable amount of time, effort and resources, from both the in-house team and the carrier/MSP, is wasted in protracted cycles of finger pointing to troubleshoot the problem. More than often, after such painful and exhaustive exercise of finding the root cause of the problem, the mitigation options resort to manual re-configuration of site/branch routers to selectively prioritize and re-route corporate and cloud applications traffic across the alternative link. This situation may well be compounded by the fact that the best effort internet link may have better round-trip delay characteristics than the carrier provided MPLS circuits.

Bottom line: with the current network architecture and the existing tools and device capabilities at hand, network teams are continuously trying to optimize the network efficiency and are spending far more time trying to put out fires and restore site/branch link connectivity as opposed to having meaningful dialogue with their business partners on real-time trending and reporting of application level network consumption and/or insight into new applications and devices rolled out.

iii) The proliferation of required network and security services has resulted in a 1:1 ratio mapping of multi-vendor appliances not optimal for remote sites.

The intermediate between a LAN and a WAN at remote sites/branches is no longer a firewall and Ethernet cable connects. Providing optimally secure corporate and cloud application access from these sites has spawned a number of purpose built appliances that straddle the connection between the LAN and the WAN. Besides the LAN switches, WAN router and firewalls, today's remote site/branch may include an internet cable/DSL router, wide area network optimization appliances, application visibility and packet capture and analysis appliances, IPS/IDS appliances, content caching engines/appliances and Wi-Fi controllers amongst others. All of these appliances require an element of configuration, together with continuous lifecycle management. Enabling a chain of functions in certain order required for a specific service or application while each appliance performs corresponding functions on transitory traffic independently is quite challenging and, in some cases, not feasible. It is obvious that more appliances at remote sites/branches not only adds to the capex but also makes the management and orchestration of all such appliances to work together coherently for specific service/application delivery complex, while increasing operational costs.

iv) Complexity and inefficiency for managing security and compliance controls.

Enterprise information security policies in line with PCI regulatory compliance mandate usage of firewalls and encryption of data sent through the internet. In the absence of application level encryption, network layer IPSec encryption is normally deployed between the remote site/branch router and the head end corporate data center router.

There are several operational and security challenges with this traditional mode of IPSec deployment. Inadequacies with scaling, efficiencies, resiliency and security compliance are experienced in large enterprises.

As demand for bandwidth increases at remote sites/branches, wide area network routers/interface cards and/or crypto engines performing the IPSec crypto function need to keep up with the performance requirements, coupled with a cost multiplier factor relative to the number of remote site/branches to match this demand. Besides this, while traditional VPN solutions leveraging IPSec have facilitated site-to-site connectivity to some extent, elastic and on-demand expansion of head end/hub resources, scaling of routing protocols and optimization of routing updates remain a challenge. In addition, application inefficiencies in the form of reduced throughput can result from packet fragmentation specially due to nested and/or chained IPSec tunnels. One fundamental issue in the traditional VPN networks is that the routing engine does not talk to the encryption engine and vice-versa. So, any routing failures can result in black holing/dropping of traffic, which, in most cases, is overcome to a degree by duality of crypto engines and routers, adding to the operational cost and complexity.

Typical enterprise implementations of IPSec use symmetric encryption. With symmetric encryption, both sites use a shared secret key. Given the potential overhead of manual key management across thousands of sites, large enterprises normally use the same pre-shared keys across all sites/branches, which means that if any site/branch is compromised, the network is as well. Furthermore, most implementations resort to utilizing the same secret key indefinitely (with mitigating controls around router/crypto-engine access/authentication) since changing the keys at regular intervals can be manually intensive, hence, operationally prohibitive, business disruptive and furthermore, prone to human error.

Application Visibility and Traffic Control

With the evolution of network infrastructure and the operating model, the variety of applications and compliance requirements as well as how enterprises consume the applications is also changing. With the availability of broadband internet access to remote sites, enterprises potentially can consume SaaS and other hybrid applications seamlessly in the data center and/or virtualized data center/public cloud infrastructures. Traditional WAN architectures and routing protocols, however, do not natively provide application aware networking, allowing granular control of how and what type of application traffic flows across different paths in compliance business policies or resources needed for best application performance and user experience. Trying to implement policies to engineer the traffic for granular control, even in a small scale environment, only further complicates the management and maintenance of the infrastructure.

v) High cost and low control of the wide area network.

Enterprise wide area networks have evolved over the years, from a mix of point-to-point leased line circuits in a mesh model to SMDS to frame relay to ATM to current deployments of point-to-cloud carrier MPLS based service. Enterprise IT operating model has also evolved to a managed service model where a service provider maintains and operates the WAN infrastructure for the Enterprise. Through all of these enterprise production deployments, reliance on the carrier has increased as have the capex and opex costs to build, support and run these large networks. While MPLS promised and delivered on the separation of data forwarding and control plane, the increased usage of enterprise feature sets at remote sites/branches, such as Quality of Service, Multicast, encryption, come at additional cost and complexity.

While complexity is a given, the one-time-per-WAN-device/appliance charges coupled with the additional monthly recurring cost (maintenance, monitoring) to run these feature sets, not including volume-based carrier/MSP charges for soft/hard MACs, the costs have simply stacked up. So enterprises are totally reliant on the carriers and/or MSPs for every little change in the context of their wide area network.

At the same time, business internet access to remote sites on a global basis has become increasingly viable due to its ease of availability, shorter provisioning cycles, and most importantly lower cost at much higher levels of bandwidth. In an aggregated format, both cable and DSL connections lower the capex and opex operating networking model when compared to carrier-based MPLS networks. This, together with the above control and cost issues, have compelled enterprises to review SD-WAN as a means of securely incorporating the internet into their corporate network while taking back control through centralized policy management and gaining application level visibility through a reasonably automated and appropriate SD-WAN solution aligned with their WAN architecture.

II. WAN Architecture Models

The below WAN architecture models are typical in today's enterprise networks. Today, almost all businesses expect 24 x 7 WAN availability. Together with high availability, ensuring a best-case customer experience, regardless of application or end user device at remote sites/branches, requires consistent and deterministic levels of network performance metrics, e.g., jitter, packet delay/loss and quality of service amongst others. Direct internet access is also increasingly becoming a staple for remote sites/branches, as a means of providing direct access to e-commerce and cloud-based applications without the long haul transit to and from the data center. These shifting traffic flow patterns mandate a robust routing schema together with an adaptive security model. While there may be variations in the number of access circuits and WAN transport providers for MPLS/Cable/DSL/4G LTE WAN, understanding the SD-WAN product feature set applicability and its linkages with underlying service delivery and management processes will be key for enterprises, regardless of whether or not they have an in-house support model or an MSP support structure.

It is expected that the SD-WAN product be capable and/or evolve and mature to support any of these production WAN implementations. The enterprise customer base will want to understand the application, networking and security feature sets supported across their own and/or intended WAN implementation.

Many of the real-world issues pertinent to today's WAN implementations are discussed within the problem statement. Empowering enterprise customers to take back control of their network while allowing the carrier/MSP to accommodate their needs will make for an appropriate SD-WAN migration and implementation.

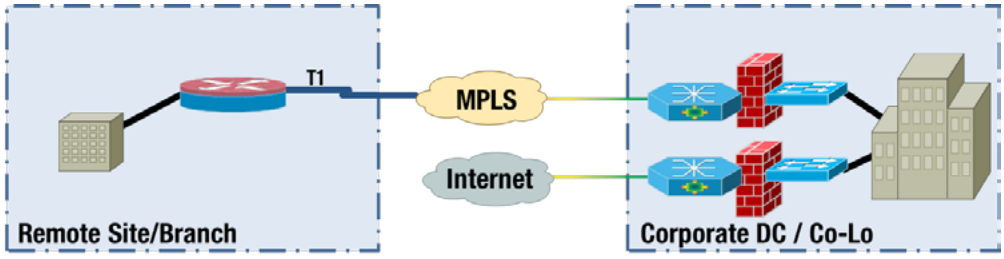

Figure 1. WAN Model 1 – Traditional MPLS WAN with Internet Back Haul to DC/Regional DC/Co-lo Facilities

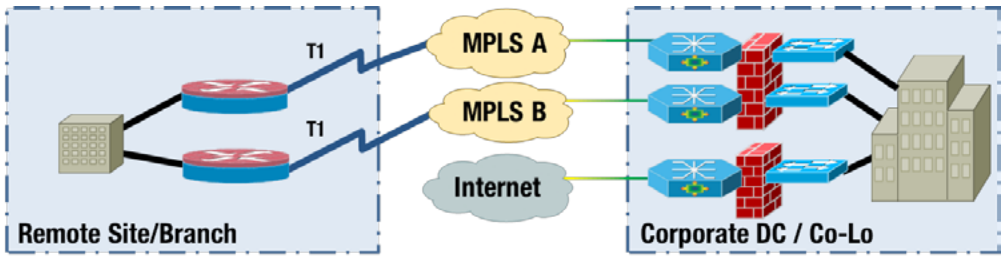

Figure 2. WAN Model 2 – Dual MPLS Carrier WAN with Internet Back Haul to DC/Regional DC/Co-lo Facilities

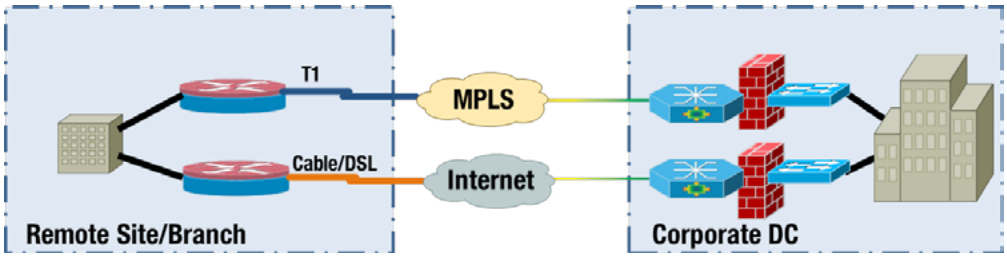

Figure 3. WAN Model 3 – Traditional MPLS with Direct Internet Access/ Secondary WAN

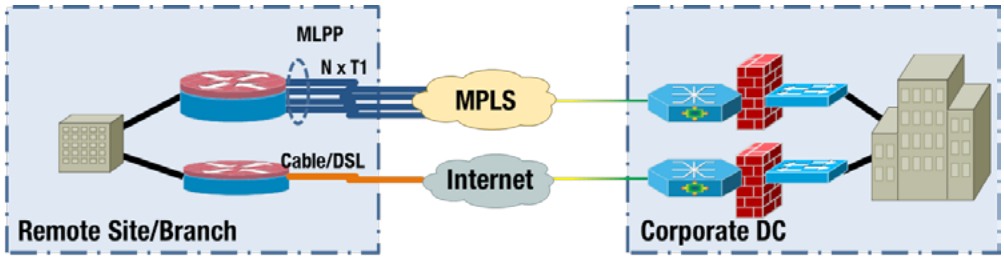

Figure 4. WAN Model 4 – High Bandwidth (N X T1) MPLS with Direct Internet Access/Secondary WAN

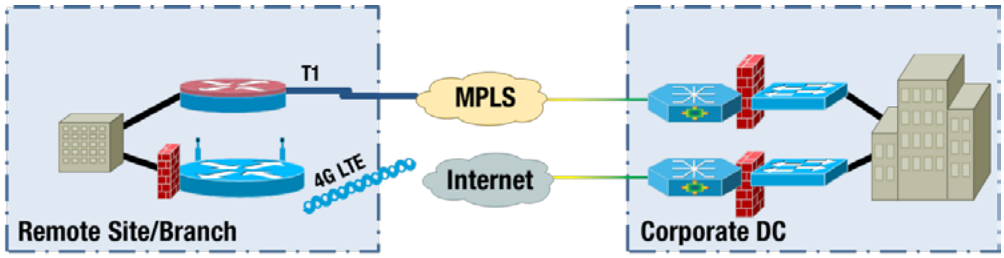

Figure 5. WAN Model 5 – Cellular Direct Internet Access/Secondary WAN

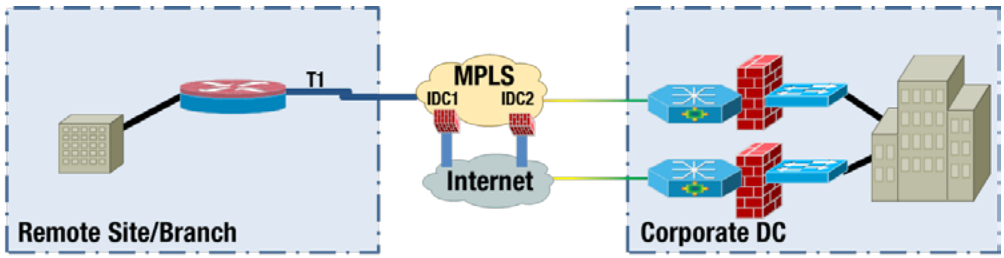

Figure 6. WAN Model 6 – MPLS with Direct Internet Access WAN

III. SD-WAN Solution and Architecture Requirements

Taking into account the different WAN models, the size and scale of the network notwithstanding, enterprise customers will want to know the below product and component architecture and feature sets supported relative to the SD-WAN product and pertinent to their current WAN model and/or future WAN implementation. While the below list is, by no means, exhaustive, it is meant to cover critical areas of an enterprise SD-WAN solution while overcoming the issues listed earlier within the problem statement and widely encountered in today's wide area networks.

Scalability

1. Are Single/Dual and/or Clustered and/or Virtual Machine Controller configurations supported within a single DC, across dual and/or multiple DCs?
2. Is the remote device/appliance platform horizontally scalable providing elastic growth capability?
3. Given the limitations around speed of light and subsequent variable response times in a global geography, what configuration may be considered optimal for an enterprise customer that may have sites in multiple continents, where access to the cloud/internet is just as critical as access to the corporate data center?
4. What are the disaster recovery options for the above, if any, and as applicable?
5. Controller and Remote Site Device/Appliance – What are appliance hardware options? Is it based on proprietary or commodity hardware? Does it provide options for virtual as well as physical form factors?
6. Controller and Remote Site Device/Appliance number and types of virtual/logical interfaces supported?
7. What is the maximum number of remote sites/branches supported without any loss or degradation in efficiency, reliability and security (0-1K, 1K-5K, 5K-10K, 10K+)?
8. Is the SD-WAN solution IPv6 ready and capable? Provide details and operating changes required to run both IP versions simultaneously.

Efficiency

1. List all L2 and L3 protocols supported for the SD-WAN solution (list both, physically local and across the WAN between remote end and controller).
2. Proprietary L2, L3, other protocols, if any, introduced by the SD-WAN?
3. Are there predefined templates for bandwidth allocation based on ToS/DSCP or any other application base-lining/profiling, and/or is it customizable based on business applications and usage?
4. Is bandwidth allocation and prioritization automatically affected based on centralized policy engine configuration and real-time characteristics of WAN access links?
5. What feature sets currently provided via external appliances in line with the WAN will be supported initially out of the box versus over the SD-WAN solution life cycle? Appliances such as wide area network optimizers, packet capture & decode tools, firewalls/UTMs…?
6. Will current routing between CE-PE change, and will there be an opportunity to simplify routing within the branch and across the wide area, given the overlay model with centralized control and distributed forwarding intelligence?
7. What are the areas where cost savings can be achieved on a one-time as well as a continuous-run-time operating model basis, and by how much?
8. Describe how complexity of traditional networking is reduced.
9. Describe how potential capex and opex savings are achieved with the SD-WAN solution.
10. Describe how operational efficiency is increased with the SD-WAN solution.
11. Does the solution provide end-end application aware networking?
12. Is the overlay able to operate in an any-to-any architecture (not only traditional hub and spoke architectures)?

Reliability

1. For the WAN models, inclusive of the different types of access networks, how is the overall resiliency of the solution achieved? List any and all dependencies on: remote site/branch device, hosted/corporate data center head end device, local device adjacencies and LAN/WAN protocol interfacing.
2. Describe HA and resiliency options for the SD-WAN solution components.

3. Describe the operation of remote device upon loss of communication to controller.
4. Can the solution intelligently overcome asymmetric routing to/from remote sites/branches?
5. It is assumed that the SD-WAN solution is an overlay design and that existing customer and/or carrier-owned WAN routers (CE)/access routers may remain on premises for some period of time into the future; all the same, how can enterprises leverage the inherent traffic and application visibility and control within SD-WAN to deliver business meaningful SLAs on site turn up and operations that go beyond the existing ones – i.e. per-site business application and end user level consumption trend and reporting?

Seamless Integration

1. Given any of the WAN models, can the SD-WAN solution work in a transparent pilot mode, whereby routing, application level traffic flow and security intelligence is gleaned, allowing networking teams time to familiarize themselves and iron out any issues before effecting actual production?
2. Describe how SD-WAN solution can integrate seamlessly with the existing infrastructure.

Security

1. How is AAA (Authentication, Authorization and Accounting) affected for the SD-WAN solution?
2. Describe any level of integration with TACACS/+, RADIUS, LDAP, or AD.
3. Describe any cryptography options available for the control and forwarding plane – symmetric and/or asymmetric encryption.
4. For each type of encryption, list the cryptographic algorithms, key length supported, frequency of key change supported via automation and any disruptive impacts to network operations
5. In the case of a PKI implementation, explain the CA, CA hierarchy and process for key generation, distribution, backup, recovery, revocation and overall key management.
6. How are security threats, such as spoofing, session hijacking, session playback, electronic eavesdropping/ packet sniffing and man-in-the-middle attacks, prevented?
7. Describe if and how the solution can provide real-time visibility and alert reporting into any extraneous routes and end points that would be foreign to a customer address space.
8. Describe if and how the solution can provide secure logical separation for internal corporate traffic, cloud/internet traffic and business partner traffic.
9. Describe if and how the solution can provide detection and mitigation capabilities for DoS/DDoS type of attacks experienced internally or through the cloud/internet.
10. Does the solution have auto application level identifying capabilities beyond just the port/protocol level to assist with policy management and compliance?
11. Can the solution through the remote site/branch appliance also provide stateful firewalling, eliminating the need for remote site/branch firewalls?
12. Redundancy/Contingency plan: How does product/service work if compromised?
13. Any capability of RBAC/Tiered access with multitenancy?
14. Multi-tenant enforcement and protection?

Manageability

1. Centralized provisioning, policy management, security management and automation?
2. Real-time visibility into cloud/internet, network and application centric management, linkages and/or dependencies, if any, to existing enterprise management tool/platforms?

IV. Service Management Considerations

Product feature sets and capabilities will significantly influence existing service management processes within an enterprise. Furthermore, the process linkages and dependencies listed in this section will vary widely, based on the current enterprise support model (in-house network team, fully managed service provider/carrier) as well as the tools and platforms situated in house versus MSP provided and supported. Based on prevailing WAN support model and organizational service management maturity, enterprises will need to understand, upfront, all of the linkages and dependencies so that a process unwind and/or a migratory path can be pursued; one that is not business disruptive and that facilitates the adoption and production implementation of SD-WAN.

i) **Provisioning & Quality Management**

- Request for Service/Service Request Process
- Business Performance Management
- Benchmarking
- Vendor Management

ii) **Systems Management**

- Change Management
- Monitoring
- Configuration Management
- Release Management

iii) **Service Support**

- SLA Management
- Help Desk
- Incident & Problem Management
- Patch Management

iv) **Operations Management & Security**

- Capacity Planning & Management
- Financial Management
- Infrastructure Performance Engineering
- Information Protection & Security
- Business Continuity & Disaster Recovery
- Compliance & Controls

ONUG SD-WAN Working Group

Conrad Menezes, Chairman	Jeff Gray	Rameshbabu Prabagaran
Pablo Espinosa, Co-Chairman	Joe Houle	Ryan Pena
Aryo Kresnadi, Co-Chairman	Brian Hedstrom	Srini Seetharaman
Andrew Kulawiak, Co-Chairman	Ron Howell	Mukhtair Shaikh
Vijay Balasubramanian	Bryan Larish	Nelson Tai
Matthew Clark	David Laundre	Howard Wang
David Crosbie	Ray Ng	Sean Wang
Mike Elmore	Jem Pagan	

SD WAN WORKING GROUP 2014 Open Networking USER GROUP