Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab Review

SD-WAN Integration with Amazon Web Services – Versa Networks

Date: November 2017 **Authors:** Tony Palmer, Senior Validation Analyst; and Alex Arcilla, Validation Consultant

Abstract

This ESG Lab Review documents hands-on testing of the Versa Networks solution and how it integrates with AWS.

Introduction

The goal of this review is to educate customers on the capabilities that Versa Networks provides when working with Amazon Web Services (AWS). ESG describes Versa Networks' solution and highlights the business value it can deliver to customers via its integration with AWS. ESG completed this summary as part of an AWS-commissioned report to review nine SD-WAN vendors. Readers should use this review as a starting point when investigating how they can leverage the combination of AWS and Versa Networks for business advantage.

Background

Software-defined wide-area networking (SD-WAN) is built on the same principles as software-defined networking (SDN): It abstracts the wide-area network to a set of capabilities that is independent of how those capabilities are provided. SD-WAN connects organizations' data centers, branch offices, and cloud environments. As a network architecture, SD-WAN disaggregates the control of the network from the data flow while simultaneously aggregating multiple physical and/or virtual devices into a single logical network. The control plane should be agile to enable dynamic adjustment of network-wide traffic flows to meet changing needs, and all devices should be centrally manageable.

The SD-WAN solutions offered by various vendors provide some combination of WAN functions. First, they may offer virtual overlay networks, which aggregate an organization's disparate networks—including classic multiprotocol label switching (MPLS) networks, carrier Ethernet, T3, and public Internet—into a single logical network. Another SD-WAN function is path selection to route packets properly when using multiple connections to a branch office. SD-WAN solutions may also offer simultaneous load balancing and cost optimization of the data transport, and service insertions such as firewalls, VPNs, load balancers, or other services relevant to branch offices or cloud environments. Finally, they often supply the network automation to make it all work together.

Cloud computing has become a transformative force in the IT world. ESG research conducted earlier this year on cloud computing reported that 78% of the 641 respondents are actively using public cloud services for varying combinations of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), or platform-as-a-service (PaaS).[1] In another survey, ESG asked respondents to identify the ways public cloud computing services have affected their organization's networking strategy, and the most reported impact, selected by 38% of respondents, was that organizations have integrated data center and WAN links to create a seamless network that connects on-premises and off-premises resources.[2]

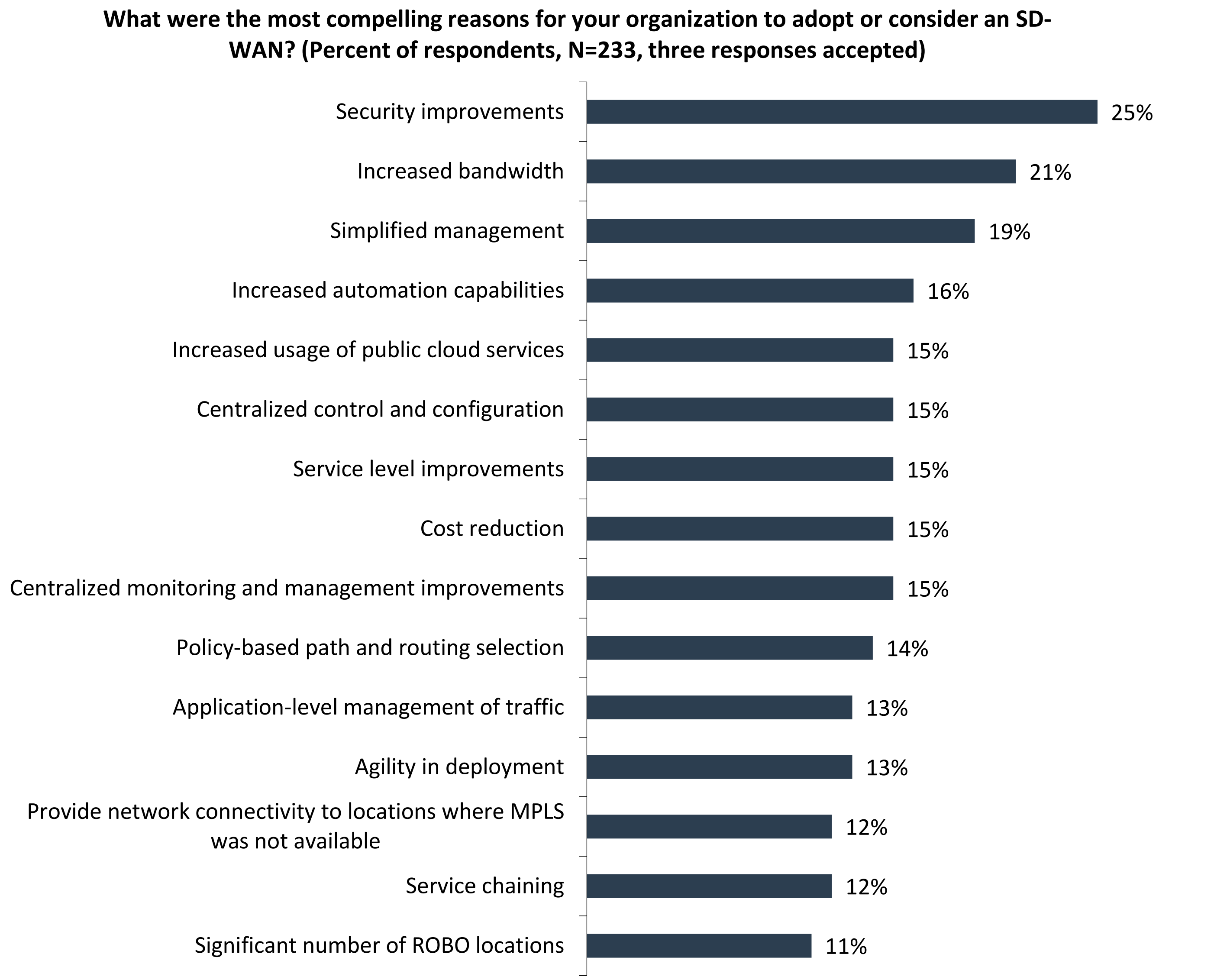
Given that most organizations using cloud services still have on-premises resources, it makes sense that organizations would strive to ensure ubiquitous connectivity and create a seamless experience for employees and customers. As a result, many organizations are considering SD-WAN to help consolidate their networking visibility and management of cloud and on-premises usage. In fact, when organizations were asked to identify the most compelling reasons to adopt or consider SD-

[1] Source: ESG Research Report, *2017 Public Cloud Computing Trends*, April 2017.

[2] Source: ESG Survey, *Network Modernization Trends*, July 2017.

WAN, simplified management, automation, and increasing public cloud utilization, along with centralized control/configuration, and management/monitoring, were all among the top ten most-cited responses.[3]

Figure 1. Most Compelling Reasons to Adopt or Consider SD-WAN



Source: Enterprise Strategy Group, 2017

One of the choices in the move toward deploying solutions "as-a-service" is how something as fundamental as network services will be delivered. Unlike software, it's obvious that some equipment is necessary at all locations, but with virtual customer premises equipment (vCPE), it's possible to have much of the intelligence pushed out to the central office or to the cloud as virtualized services.

SD-WAN is one of the areas where the two worlds of on-premises and cloud intersect, as the ability to run network services in the cloud enables an end-to-end solution where a variety of services are offered to SD-WAN customers. Many of these network services, such as load balancers, application delivery controllers, or firewalls, are already offered by either cloud service providers or as virtual network functions from network or security vendors.

[3] Source: Ibid.

Testing Methodology

ESG and AWS created a test plan in two sections: a questionnaire to assess SD-WAN features and capabilities,[4] and test scenarios for assessing SD-WAN tunnel performance (throughput) and availability (failover and convergence time between SD-WAN instances). Versa Networks agreed to assess its solution's capabilities and levels of integration with AWS. ESG met with Versa Networks, conducted interviews, and investigated test scenarios onsite at its facility.

Amazon Web Services provided cloud resources for the test environment, while Versa Networks provided software licenses and facilities (e.g., broadband connections and devices). Versa Networks could choose not to answer specific questions or conduct certain tests; in those cases, participation was at AWS's discretion.

Test Scenarios:

- Demonstrate the ease of implementation and installation of Amazon Machine Images (AMIs) and virtual private network (VPN) creation. This is important to reduce the amount of time it takes to procure and then configure SD-WAN solutions for AWS customers.

- Demonstrate multiple Availability Zones (AZs) support. This is important because it is a best practice for all customer deployments to be multi-AZs, which implies that SD-WAN products will support this.

- Demonstrate that the solution supports a high-availability deployment on AWS. Measure failover/convergence times for traffic between customer premises and AWS as well as for traffic between instances inside AWS. This is important because network availability is both business- and mission-critical in modern environments with highly distributed resources and workforces.

- Demonstrate the performance throughput of the solution. This is important because consistently high-performance networks are essential for modern enterprise computing. Every aspect of business is impacted by network health and functionality, as employees and customers access data and applications from multiple locations, on multiple devices.

- Demonstrate the management, visibility, and monitoring capabilities of the system, including statistics, monitoring, and AWS visibility (Amazon Virtual Private Cloud [VPC], subnet, Amazon CloudWatch metrics, and flow logs). This is important because today's dynamic IT environments demand the ability to quickly and easily monitor and manage services to meet the demands of the business. Organizations need flexible, easy-to-use tools that enable efficient monitoring and management of cloud environments with minimal effort.

For the test scenarios, ESG Lab stresses that any performance and failover time measurements should not be used as a sole basis for comparison. Although ESG and AWS defined the testing topology and scenarios, test conditions and instance types differed, which led to different results across all SD-WAN vendors for the same test. For example, when measuring throughput between on-premises instances and instances in Amazon VPCs in different regions, other traffic present on the vendor's Internet connection, which is not under the vendor's control, can affect the result.

ESG Lab did note some consistent responses across all vendors, including:

- All SD-WAN vendors support some type of bootstrapping. Differences emerged in the type of files or processes used by each vendor.

- All SD-WAN vendors supported encryption over all supported link types.

[4] A complete list of questions can be found in the Appendix.

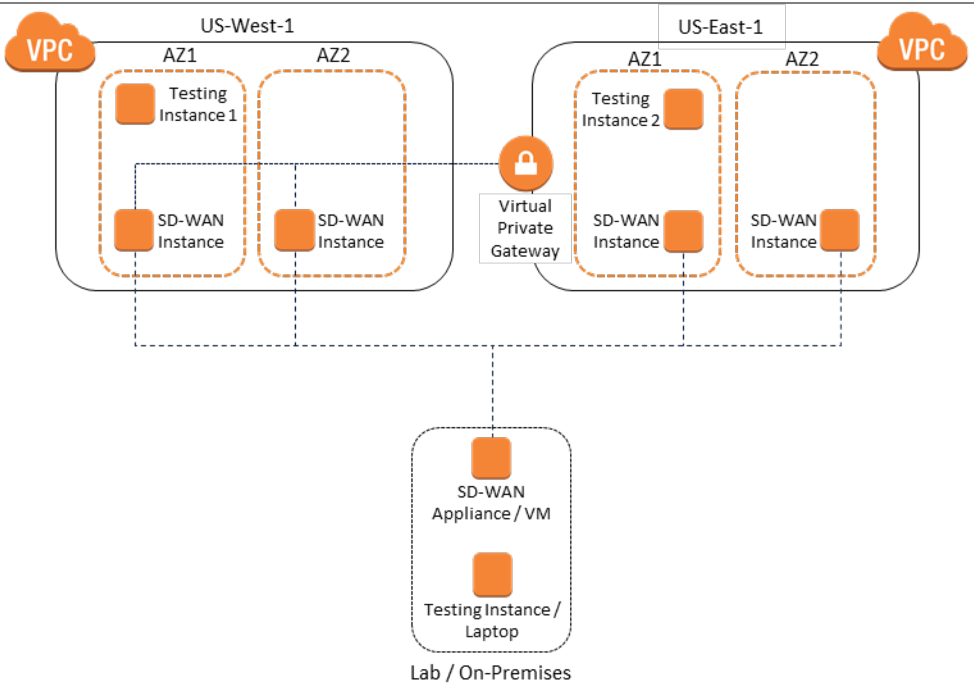
- All SD-WAN vendors supported AES 256 as their default encryption mode.
- All SD-WAN vendors performed some level of traffic throttling or shaping via QoS metrics.
- All SD-WAN vendors supported IAM roles to secure access to the solution's controller/orchestrator. Some vendors also supported access keys.

Versa Networks was given the option to generate traffic using iPerf (for Linux), NTttcp (for Windows), or a dedicated traffic generation tool (such as Ixia) to generate test traffic and measure connection throughput and availability. The test traffic originated from testing instances located behind the Amazon VPC and SD-WAN instances. ESG allowed Versa Networks to choose packet size and number of streams generated by the testing instances and reported those parameters for each vendor.

The test topology shown in Figure 2 was used as the template for Versa Networks' test environment. This topology was designed to enable assessment of the performance and availability of connections between on-premises and cloud SD-WAN instances and between cloud regions. While ESG suggested a set of instance types[5] to be used for testing, Versa Networks may not have supported those specific instances. ESG noted the specific instance used during each test. Versa Networks deployed an SD-WAN instance or device in its lab, which represented a branch office. Versa Networks set up a tunnel between the "branch" and SD-WAN instances deployed in two Amazon VPCs deployed in AWS US-East and US-West Regions. These connections represented a typical SD-WAN customer network—a mix of broadband Internet, mobile internet, and private MPLS connections between on-premises and cloud environments.

Within both regions, Versa Networks created redundant instances. Versa Networks placed the primary and redundant instances in different AZs within the US-East and US-West Regions. Versa Networks connected both the primary and redundant instances of each region to each other in a full mesh and connected the redundant instances in the US-East Region to a virtual private gateway on AWS.

Figure 2. Testing Topology



Source: Enterprise Strategy Group, 2017

[5] The list of instance types can be found in the Appendix.

The following sections discuss the highlights of ESG Lab's onsite testing with Versa Networks. The goal of this vendor summary is to highlight the solution and the unique problems it focuses on solving, and to describe its integration with AWS.

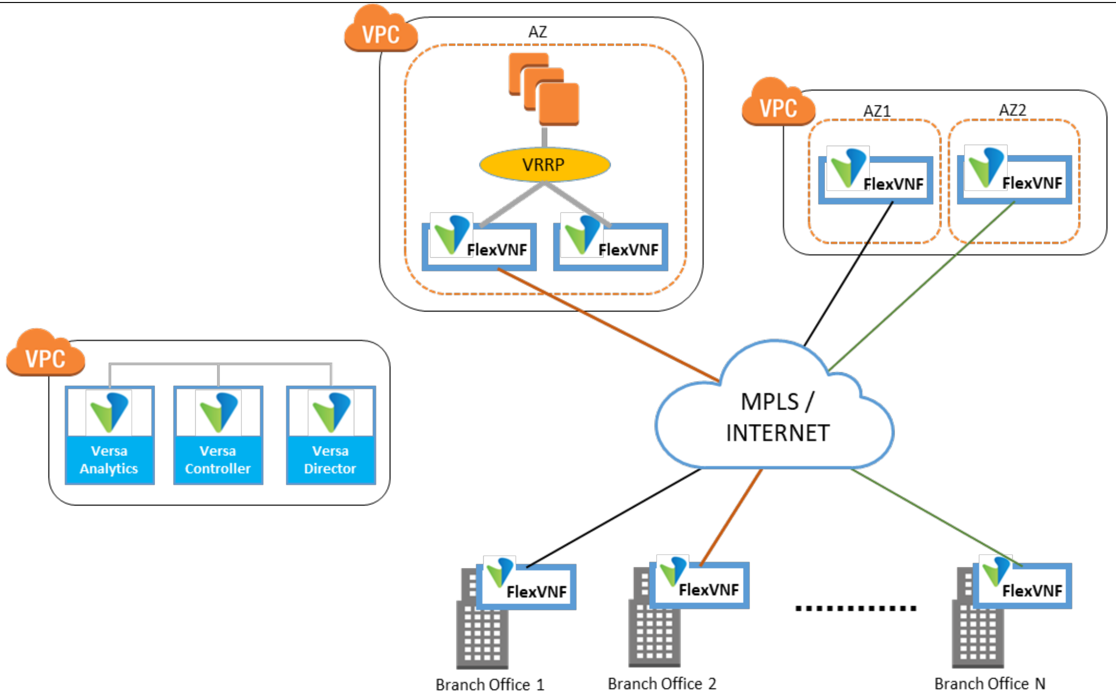
Versa Networks FlexVNF

Versa FlexVNF is a multitenant software platform that integrates multiple network services within its architecture, such as routing functionality, next-generation firewall (NGFW), and unified threat management (UTM). FlexVNF supports service chaining, which allows organizations to integrate third-party physical and virtual appliances. The platform leverages an integrated KVM hypervisor that enables the service chaining. Versa Networks streamlines packet-processing for routing, SD-WAN, and security with native support for all services, thus reducing latency by minimizing the inspection points for each packet in the flow. In traditional deployments, packets passing through separate appliances (virtual or physical) add latency because each hop is required to process packets at both the ingress and egress.

Multitenancy allows one FlexVNF to serve multiple customers without the need to create multiple individual instances. The multitenancy makes the solution ideal for service providers that want to offer managed SD-WAN services at larger scale while reducing costs for additional infrastructure. Large enterprises that require complex routing integration with their existing branch networks can also use FlexVNF.

The solution's head-end consists of the Director, Controller, and Analytics cluster. The Director makes the API calls, enabling the network professional to automate, configure, deploy, and manage the FlexVNF branches. IKE-based IPSec tunnels connect the branches to the Controller. Based on the open source Cassandra database, the Analytics platform provides the network professional with several metrics and statistics, particularly related to routing, to support monitoring and troubleshooting. The head-end resides in a private subnet. Figure 3 highlights the components of the Versa SD-WAN solution and how they are integrated with AWS.

Figure 3. Versa Integration with AWS



Source: Enterprise Strategy Group, 2017

ESG Lab Highlights

ESG validated the integration of the Versa Networks' solution with AWS and explored additional capabilities. Features include:

- Versa Networks delivers its SD-WAN solution either virtually (on VMware, KVM, or AWS) or physically via bare metal servers or appliances. Multitenancy is a native part of the Versa solution regardless of the deployment mode.
- FlexVNF is currently available only as a private AMI. The solution runs on a minimum c3.xlarge instance, to provide three interfaces and four virtual central processing units (vCPUs).
- FlexVNF supports single root I/O virtualization (SR-IOV), which allows higher I/O performance on network interfaces with lower central processing unit (CPU) utilization. Thus, the SD-WAN instance can deliver faster performance, and higher bandwidth speeds and performance, decreasing latencies between SR-IOV-enabled instances. FlexVNF supports SR-IOV on instances larger than or equal to c3.xlarge.
- Versa Networks employs AWS CloudFormation templates for automated configuration. Administrators can create branch deployments and VPNs via the Director, with the option to create a mesh or hub-and-spoke model between deployed instances.
- Versa Networks has added a routing capability, Virtual Router Redundancy Protocol (VRRP), that is not native to AWS. In a traditional WAN, this capability allows a network administrator to assign a virtual IP to a group of routers, with one designated as the master router and the others as backup routers. When the master router fails, a backup will continue to forward traffic. On AWS, organizations can spin up master and backup branches in an AZ. Versa Networks developed this capability to help customers ease the transition to AWS by maintaining capabilities that they were already leveraging.
- ESG measured link performance between instances deployed in two Amazon VPCs in the US-West Region. Using c4.4xlarge instances, we used iPerf3 with the default MSS of 1,460 bytes to generate traffic over the link. ESG observed that the maximum bidirectional encrypted throughput between the instances was 2.45 Gb/sec—1.22 8Gb/sec in each direction. We also noted that the instance CPU utilization was less than 40% while RAM utilization was less than 4%. Low instance utilization translates into additional processing resources to support multiple user traffic streams. A Versa customer can decrease network complexity, thus lowering management and cloud-related costs.
- FlexVNF supports routing between Amazon VPCs both natively and via support for the transit VPC on AWS. The native functionality is automated with FlexVNF. Organizations can use the available AWS CloudFormation template to implement the transit VPC.
- The Director Dashboard allows the user to create policies to enable application steering over available WAN links. For example, an administrator can set up a Service Level Agreement (SLA) profile that monitors link latency and initiates a failover to another link if a threshold is reached. These policies can also be created to react to other triggers such as link failures or static policies.

Why This Matters

Deploying SD-WAN for multiple users can become costly and harder to manage. Scaling the underlying network means purchasing more and disparate hardware components and their related management systems. Network administrators must also consider inserting other network services, specifically security, into the network. The downside is that large, complex networks add latency, thus decreasing network performance. To address both scalability and performance, SD-WAN solutions enable support for multiple users via virtualization while integrating routing and network services to expedite secure packet forwarding.

ESG confirmed that Versa FlexVNF integrates with AWS and allows the creation of a high-performance SD-WAN while minimizing CPU and RAM utilization. Conserving compute resources allows the support of multiple users on the same FlexVNF instance via virtualization.

awsmarketplace AWS Marketplace Homepage

VERSA NETWORKS

Direct sales contact: Gaurav Prashad – Director, Enterprise Sales, gprashad@versa-networks.com, (925) 348-1533

The Bigger Truth

SD-WAN implementations generically offer some combination of multiple WAN functions, including: virtual overlay networks, which aggregate all of an organization's disparate networks into a single logical network; path selection, to route packets properly when using multiple connections to a branch office; the ability to combine multiple physical networks—including classic MPLS networks, carrier Ethernet, T3, and public Internet—into one virtual network, enabling simultaneous load balancing and cost optimization of the data transport; service insertion, such as firewalls, VPNs, load balancers, or other services relevant to branch offices or cloud environments; and network automation to make it all work together.

Cloud computing has become a transformative force in the IT world. Recent ESG research found that 78% of respondents are actively using public clouds for varying combinations of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), or platform-as-a-service (PaaS).[6] In a different survey, ESG asked respondents to identify the ways public cloud computing services have affected their organization's networking strategy, and the most commonly reported impact, selected by 38% of respondents, was that organizations have integrated data center and WAN links to create a seamless network that connects on-premises and off-premises resources.[7]

Recognizing the need for simplicity in network resource integration and management, AWS is in the process of building a network competency to certify that networking vendors can integrate with AWS in a consistent, centrally manageable, highly available manner.

ESG Lab has validated that Versa Networks provides a cloud-native solution with the required baseline level of integration with AWS—bootstrapping options for deployment, AES 256 encryption over all link types, traffic shaping controls, and IAM role-based access for security. Versa Networks supported additional features and functionality that are above and beyond this baseline of support, based on their target market and use cases.

ESG Lab recommends that organizations that need to provide seamless access and connectivity, for their users or customers, to applications or geographically dispersed locations—whether on-premises or in the cloud—should seriously consider SD-WAN to integrate their networks and provide universal access. The data collected in this report can be used to better understand how the Versa Networks solution integrates with AWS and determine if it will serve an organization's individual business needs and use cases.

[6] Source: ESG Research Report, *Public Cloud Computing Trends*, April 2017.

[7] Source: ESG Survey, *Network Modernization Trends*, July 2017.

Appendix

Questionnaire Sent to SD-WAN vendors

- Bootstrapping—Can the instance take in and process EC2 user-data? (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html). Any testing should demonstrate all types of data supported by the SD-WAN vendor, e.g., shell scripts and/or cloud-init directives. Other options: plain text, as a file (useful for launching instances via the command line tools), or as base64-encoded text (for API calls).
- Enhanced networking support using single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. A performance comparison can be made between an instance running SR-IOV and an identical instance running a traditional virtualized interface. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html
- ENA Driver support - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networkingena.html
- Encryption:
  - Is encryption supported? (Y/N)?
  - Encryption of traffic supported over all link types (Y/N)?
- AWS EC2 API Support / Command line tools support (Y/N)? http://docs.aws.amazon.com/general/latest/gr/GetTheTools.html
- Does the instance support roles, access keys, or both?
- For deployment, are there CloudFormation or other automation tools available?
- Does the instance support overlapping IP addresses? (VGW Transit VPC support)
  - Is there automation available for the Transit VPC topology? https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/
- Is the solution on AWS Marketplace or a private AMI?
- Does the system monitor these conditions to handle failover?
  - Packet loss
  - Blackholed traffic
  - BGP/neighbor changes
  - Link flapping
  - Latency
- Can the instance policy-route traffic over Direct Connect versus VPN?
  - Can the instance route certain types of traffic over different links, e.g., voice over Direct Connect, SSL over the Internet, etc.
  - Can the instance create a VPN backup for Direct Connect?

- Does the instance do Quality of Service or preferential traffic throttling/shaping?
- Does the instance do any WAN acceleration for high latencies?
- Can the instance be placed behind Elastic Load Balancing (ELB/ALB)?
- Can the instance load-balance traffic over multiple VPNs?
- What APIs or level of APIs are available with the solution?
- What automation tools have support and/or example code?
    - AWS CloudFormation, Terraform, Puppet, Chef, Ansible, SaltStack, others?

Test Plan Sent to SD-WAN Vendors

- Demonstrate ease of implementation and installation of AMIs and VPN creation
- Multiple Availability Zone support
    - Demonstrate the ability to support and leverage multiple availability zones.
- Auto Scaling support – can the product scale out and scale in on AWS? https://aws.amazon.com/autoscaling/
- Compatibility with the Virtual Private Gateway (VGW)
    - Configure a VPN to the VGW, test that it works.
        - This can be optionally removed if the vendor prefers direct VPN to their instances.
    - Support for BGP with the VGW
- High Availability – does the SD-WAN product support a high-availability deployment on AWS?
    - Inside to outside – route shifting or ENI shifting
        - Measure the failover time for these failure modes
            - Measurement can use ping or any other availability check between the test instances. The traffic must be initiated by the us-east-1 testing instance.
            - The primary SD-WAN instance for a region is shut down, and connectivity is tested from us-east-1 to the lab.
            - Network ACL is applied to deny all traffic to the primary subnet, and connectivity is tested from us-east-1 to the lab.
    - Outside to inside
        - Measure the failover time for these failure modes
            - When the primary SD-WAN instance is shut down from the lab to the test instance in us-east-1.
            - When the VPN or BGP session is deleted for the primary instance.
- Performance – Throughput performance testing

    - All SD-WAN vendors will execute tests in the same manner and with the same parameters using common tools (iPerf3 for Linux, NTttcp for Windows).
    - Performance will be tested in these scenarios for both m4.xlarge, m4.16xlarge, and c4.8xlarge instance types (if supported, otherwise performance tests can be conducted against supported instance types).
        - The branch instance to us-east-1 testing instance
        - The branch instance to us-west-1 testing instance
        - The us-east-1 testing instance to the us-west-1 testing instance
    - Note: The m4.xlarge and c4.8xlarge support the ixgbevf driver (Intel 82599) and the m4.16xl supports the Elastic Network Adapter (ENA) driver.
- Visibility and Monitoring
    - What statistics are available?
    - What level of monitoring is available?
    - What type of AWS visibility is available?
        - VPC
        - Subnet
        - CloudWatch metrics
        - Flow Logs

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.