ESG Lab Review

SD-WAN Integration with Amazon Web Services – Cisco

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 Cisco solution and how it integrates with AWS.

Introduction

The goal of this review is to educate customers on the capabilities that Cisco's SD-WAN solution provides when working with Amazon Web Services (AWS). ESG describes Cisco's 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 Cisco 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.

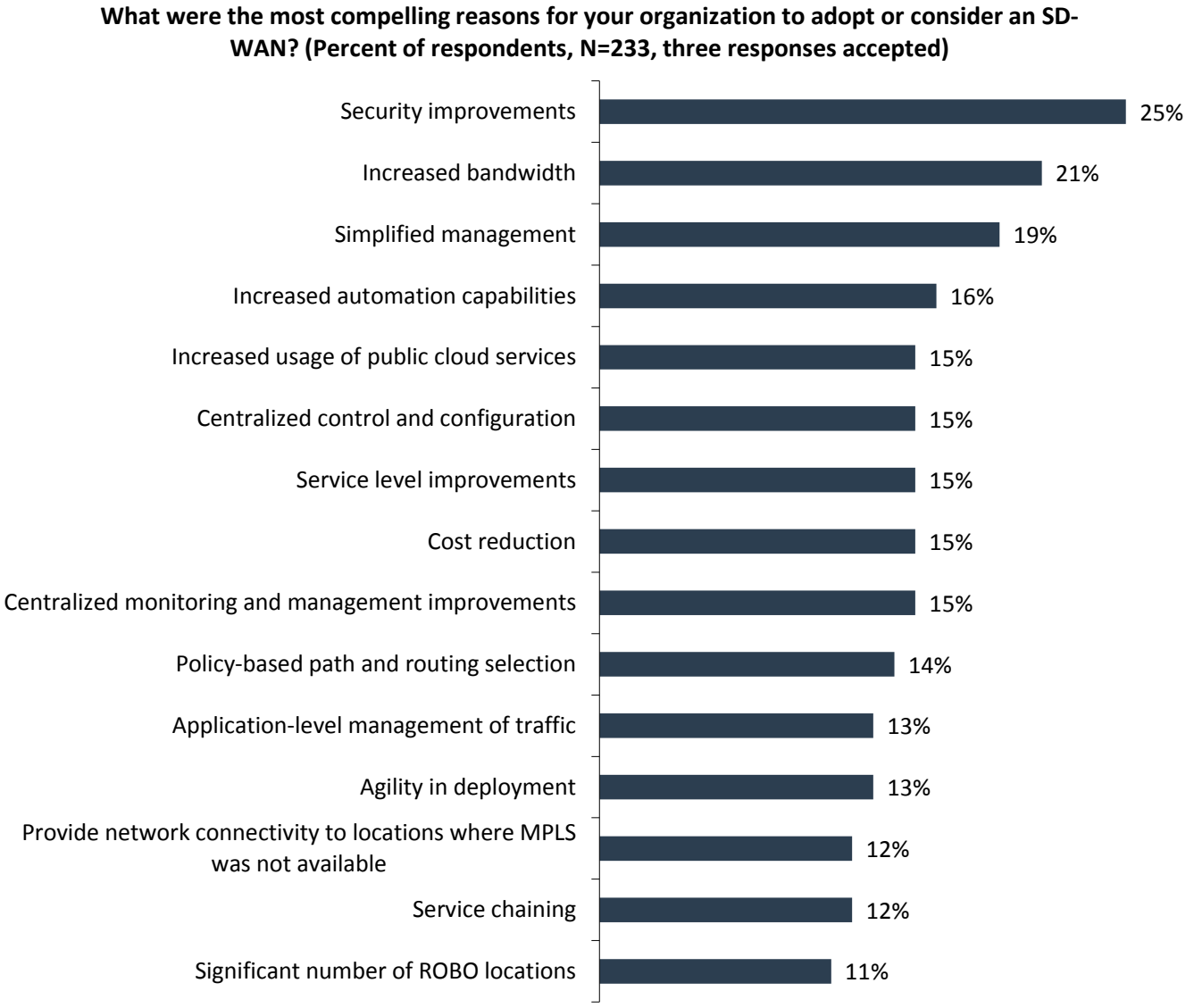
Cloud computing has become a transformative force in the IT world. ESG research conducted earlier this year on cloud computing reported that 78% of the 641 respondents are actively using public cloud services for varying combinations of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), 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). Cisco agreed to assess its solution's capabilities and levels of integration with AWS. ESG met with Cisco, conducted interviews, and investigated test scenarios onsite at its facility.

Amazon Web Services provided cloud resources for the test environment, while Cisco provided software licenses and facilities (e.g., broadband connections and devices). Cisco 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.

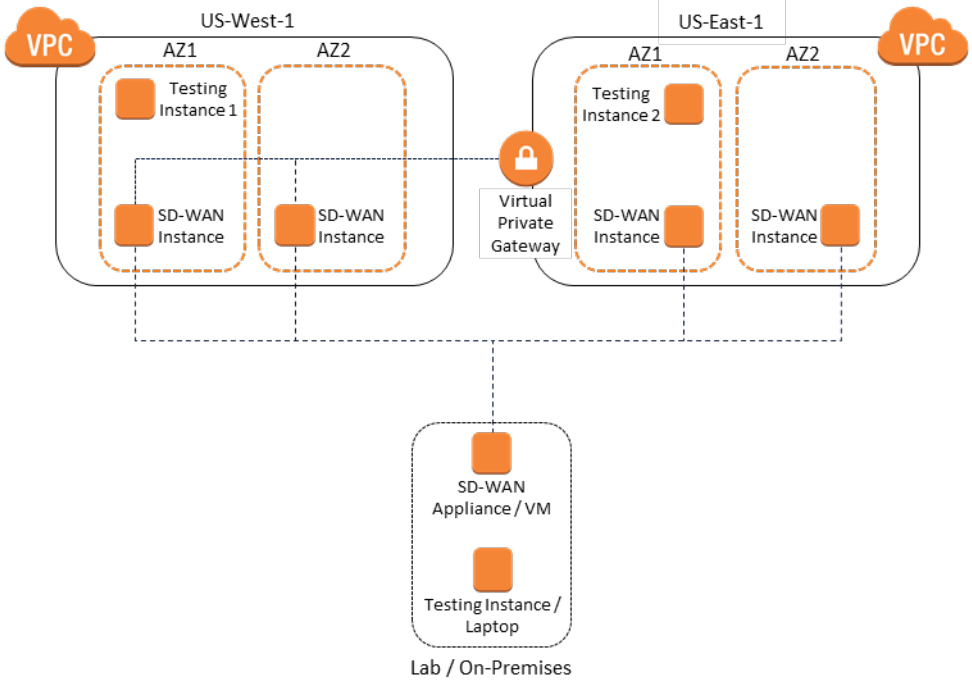
- All SD-WAN vendors supported AES 256 as their default encryption mode.
- All SD-WAN vendors performed some level of traffic throttling or shaping via QoS metrics.
- All SD-WAN vendors supported IAM roles to secure access to the solution's controller/orchestrator. Some vendors also supported access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

Cisco 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 Cisco 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 Cisco's 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, Cisco may not have supported those specific instances. ESG noted the specific instance used during each test. Cisco deployed an SD-WAN instance or device in its lab, which represented a branch office. Cisco 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, Cisco created redundant instances. Cisco placed the primary and redundant instances in different AZs within the US-East and US-West Regions. Cisco 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 Barracuda. 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.

Cisco SD-WAN Solution

The Cisco SD-WAN Solution (acquired from Viptela) focuses on providing organizations with a streamlined workflow to connect with deployed applications on AWS. The solution consists of three components: the vEdge Router, vSmart Controller, and vManage Network Management System (NMS).

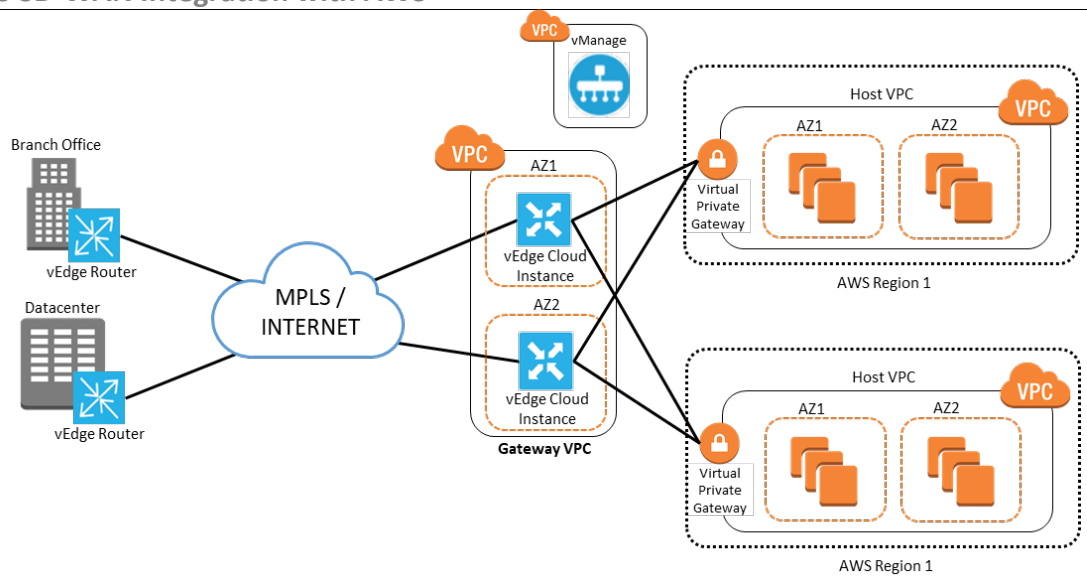
Organizations deploy the vEdge Router in a software or hardware form factor at their enterprise sites—branches, remote sites, and data centers. The vEdge router connects branches and application VPCs via a gateway VPC, a private VPC containing a pair of vEdge cloud instances. The gateway VPC enables the administrator to easily scale up the VPC environment, since this approach reduces the number of point-to-point tunnels between enterprise sites and host VPCs. Not only is WAN management simplified, but cloud-related costs and deployment time can decrease.

This gateway VPC can be used as a regional point of access, offering organizations two key benefits. First, this supports workload segmentation, especially when an enterprise deploys application VPCs across multiple regions. This can improve the ability to manage and monitor the AWS environment. Second, organizations can leverage the access point to contain potential security breaches, directing customer traffic via the gateway VPC away from the threat.

The vManage NMS helps customers orchestrate the WAN sites and Amazon VPCs so that connectivity is quick and easy to establish. Also, vManage provides full lifecycle management and network-wide visibility into the customer's SD-WAN. The Cisco SD-WAN Solution can particularly help enterprises whose application developers and DevOps engineers want to spin up and tear down development environments in the AWS Cloud easily.

To ensure cloud application performance, the Cisco SD-WAN Solution offers application-aware routing. This feature will choose the best path for delivering application packets over the available network transports. Organizations can benefit by setting up the appropriate environment to meet application service level agreements (SLAs). Figure 3 highlights the components of the Cisco SD-WAN Solution and how they are integrated with AWS.

Figure 3. Cisco SD-WAN Integration with AWS



Source: Enterprise Strategy Group, 2017

ESG Lab Highlights

ESG validated the Cisco SD-WAN Solution's integration with AWS and explored additional capabilities. Features include:

- For the gateway VPC, organizations can use c4.large, c4.xlarge and c4.2xlarge, c3.large, c3.xlarge, and c3.2xlarge instances, choosing the instance size during the workflow to deploy the solution. They purchase vEdge Routers through AWS Marketplace. Depending on the region in which customers deploy vEdge Routers, various instances can be supported (e.g., M3 and M4, and C3 and C4).
- Currently, the Cisco SD-WAN Solution does not support single root I/O virtualization (SR-IOV), which would allow higher I/O performance on network interfaces with lower central processing unit (CPU) utilization or Elastic Network Adapter.
- The Cisco SD-WAN Solution supports API keys that can be associated with roles. Cisco uses this approach to provide secure access whether the controller is deployed in the cloud or on-premises at a customer site.
- ESG Lab measured link performance between instances deployed in two Amazon VPCs. Cisco simulated bidirectional traffic by leveraging instances in three gateway VPCs, two in the US-East Region and one in the US-West Region. Each gateway VPC contained a pair of vEdge cloud instances deployed on c4.4xlarge instances. Cisco deployed Ubuntu virtual machines behind each of the gateway VPCs and measured bidirectional traffic on one Ubuntu server in US-East. Using iPerf3, we generated 10 traffic streams from this server to another server behind the second gateway VPC in US-East using the default iPerf MSS of 1,460 bytes. Simultaneously, we generated 10 traffic streams from the Ubuntu server in US-West to the server from which traffic was generated. After running the test for five minutes, we achieved a maximum total throughput of 500 Mb/sec. Cisco noted that they have achieved higher throughput in internal testing and connection segments that run over the Internet can present a bottleneck.
- ESG Lab also observed failover times between gateways deployed within the gateway VPC. We initiated traffic via iPerf3 from the on-premises instance to one gateway deployed in the second US-East Amazon VPC. We then shut down the gateway to initiate failover. Failover time was approximately nine seconds.
- vManage will monitor tunnel conditions—packet loss, latency, link flapping, BGP/neighbor changes, and black-holed traffic—and initiate failover when customer-defined conditions are met. Organizations can also set thresholds on a per-application basis to trigger failover. Cisco stated that vManage will also allow IT administrators to monitor application utilization from the network across an organization's hybrid WAN.
- Currently, the Cisco SD-WAN Solution does not support AWS Auto Scaling, Elastic Load Balancing, or transit VPC on AWS. The solution offers alternative native approaches to provide these types of functionality.

Why This Matters

Scaling out an AWS environment to extend your WAN can create manageability, cost, workload segmentation, and security challenges. Supporting multiple point-to-point tunnels between enterprise sites and Amazon VPCs can prevent application developers and DevOps from fully taking advantage of AWS.

ESG Lab confirmed that the Cisco SD-WAN Solution allows an enterprise to leverage Amazon VPCs in multiple regions via its gateway VPC implementation. Organizations can map multiple host VPCs to a gateway VPC, then leverage the gateway VPC to set up connections between the enterprise sites and the host VPCs. Using the gateway VPC allows the organization to scale up the number of host VPCs as needed while segmenting and isolating workloads for easier management, application quality monitoring, and security.

Cisco SD-WAN Listing on AWS Marketplace

Direct sales contact: sales@viptela.com

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 Cisco 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. Cisco 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 Cisco 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