Networking Infrastructure on AWS

Leveraging ISV AWS Marketplace Solutions

November 2016

Table of Contents

Introduction

According to a recent Equinix report on the enterprise of the future, the #1 Enterprise IT strategy for delivering corporate revenue growth is to deploy interconnected (hybrid) infrastructures in support of new product offerings . As they make their transition to the cloud, many companies will want to continue to keep on-premises systems running as part of hybrid architectures for the next 2-3 years to get the most out of their existing capital investments. The AWS Marketplace Network Infrastructure Category is comprised of offerings that help organizations establish hybrid enterprise infrastructures using best-of-breed routers and security appliances in order to meet business demands leveraging a combination of AWS and on-premises investments in people, skills, and equipment.

Sellers in the Marketplace Network Infrastructure Category supplement, and in some cases build on, existing AWS Networking Services such as Amazon Virtual Private Cloud, AWS Direct Connect, Elastic Load Balancing, and Amazon Route 53, allowing Enterprise IT to integrate on-premises environments with AWS. While AWS offers a very broad and deep set of networking services, ISVs in AWS Marketplace bring additional feature and operational consistency to on-premises and AWSworkloads. This enterprise-grade control, visibility, and policy consistency increases the security and performance of applications hosted on AWS and delivered to corporate locations. This solution overview document will look at some of the most common reasons that customers adopt networking infrastructure solutions from AWS Marketplace, and popular products that have been supporting specific use cases.

Use Application Delivery Controllers for L4-L7 control across AWS and on-premises

If you're ready to start leveraging AWS, chances are you'd like to continue using many of the same tools and processes you use on-premises while still deriving the security, scalability, and cost-effectiveness benefits that the cloud is known for. With AWS Marketplace, you can access a wide variety of networking infrastructure solutions to extend your L4-L7 Network Stack to AWS.

One of the most common ways to accomplish this is to use an Application Delivery Controller (ADC), which are devices placed between an organization's firewall and application/web servers to offload common tasks from the servers themselves. ADCs offer functionality including load balancing, SSL offload, web application firewalling, and more to help you improve the availability and performance of your applications across your AWS and on-premises environments. Several ADCs are available from the AWS Marketplace as virtual appliances.

Brocade Virtual Traffic Manager is a commonly deployed ADC from AWS Marketplace. It's a software-based layer 7 ADC that inspects and processes application traffic with full payload inspection and streaming. To reduces the strain placed on your EC2 instances, Virtual Traffic Manager uses network-level buffering, protocol optimizations, and application-specific measures such as dynamic compression and caching. The result is reduced latency, increased capacity, improved availability, and optimized service levels for each end user. It also allows you to create and configure your own load-balancing templates to help simplify the deployment of applications on AWS.

Equinix: The Enterprise of the Future: Unleashing the Interconnected Enterprise, October 2015 http://www.equinix.com/ss/Satellite?blobcol=urldata&blobheader=application/pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1308113355064&ssbinary=true

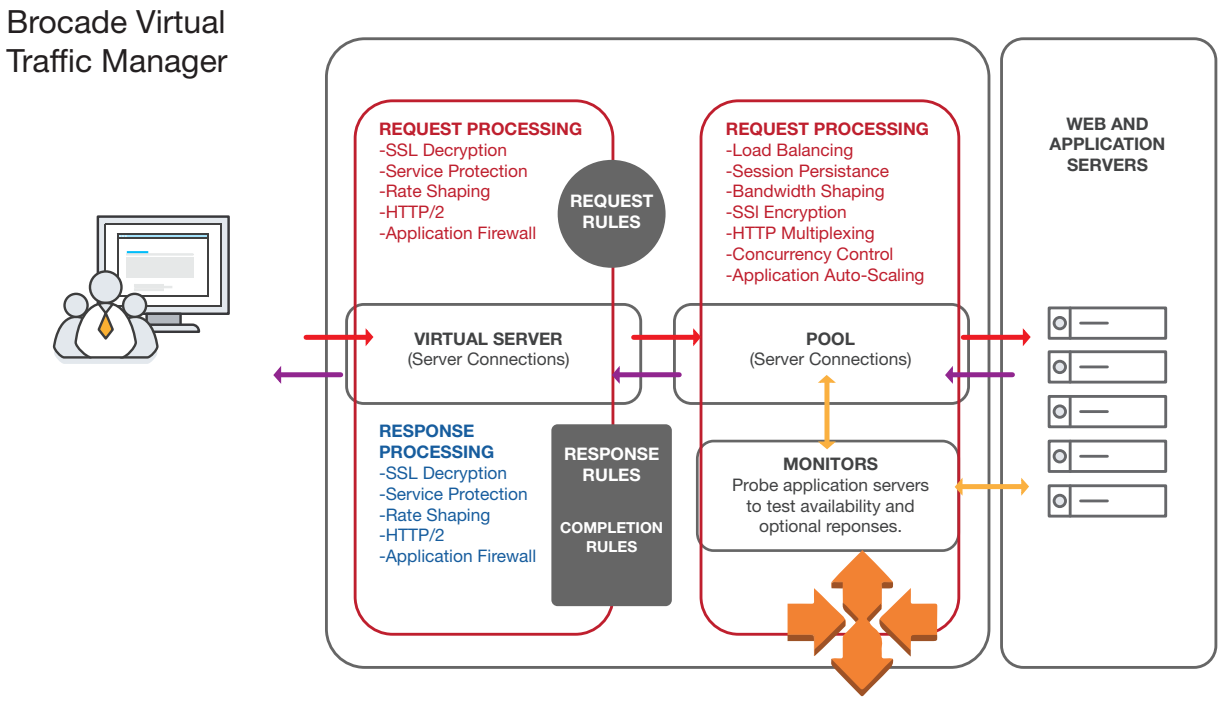

Fig. 1. The advanced capabilities in Brocade Virtual Traffic Manager can be enhanced using TrafficScript or Java extensions

Another popular ADC deployed from AWS Marketplace is Citrix NetScaler. NetScaler offers a complete portfolio of ADCs, offered both as hardware and as virtual appliances. Many customers who are used to using these products on-premises deploy them on AWS to achieve similar functionality while also benefitting from the cost-effectiveness and scalability that AWS is known for. One particular strength of NetScaler is its integration with Cisco's networking solutions, including Nexus switches and Application Centric Infrastructure. In addition, Citrix is one of the ADC vendors that provides database load balancing for Microsoft SQL Server Tabular Data Stream (TDS) and MySQL.

F5 Big IP is also very popular among AWS customers. It can help consolidate multiple security, remote access, performance and application delivery functionalities into a single platform, making it a particularly strong choice for complex deployments. F5 also offers a broad range of functionality to support software-defined networking (SDN) and network functions virtualization (NFV).

Using an ADC makes it much simpler to manage application traffic between on-premises resources and the AWS cloud, helping you with security, availability, and efficiency initiatives. The experience is very similar to running an ADC on-premises, and hourly, monthly, and yearly payment models enable you to optimize efficiency and architectural flexibility without incurring any down time or upfront costs.

Application performance for branch offices

Most AWS deployments utilize several Virtual Private Clouds (VPCs) across multiple AWS Availability Zones, and require that users have access to the applications and data residing in those VPCs from branch offices across the world. As additional VPCs are added, the complexity of the environment grows, and backhauling becomes increasingly complex. Naturally, many organizations begin adding more IPsec Tunnels that connect branches to the nearest VPC in a partial mesh topology. This unnecessarily complicates network management and impacts the user experience due to network congestion. With solutions found in AWS Marketplace, you can quickly and easily find virtual appliances that allow you to improve the connectivity between all of your data centers, branch offices, and your VPCs in the AWS cloud to address these challenges.

Citrix has a long-standing reputation for their enterprise-grade networking solutions, and they have extended that experience to AWS by making Citrix NetScaler SD-WAN (formerly CloudBridge) available in AWS Marketplace. NetScaler SD-WAN can optimize the secure tunnel between your data center, branch offices, and AWS for a wide variety of applications and protocols. It automatically applies the right mix of WAN acceleration techniques based on network conditions, data flows and application mix, and dynamically tunes the system as these variables change, ensuring optimal WAN performance. With Citrix NetScaler SD-WAN, you get LAN-like performance for applications, even when delivered to branch offices.

Another popular solution for connecting remote locations to AWS is Cisco's Cloud Services Router (CSR) 1000v, also available immediately and with pay-as-you-go pricing from the AWS Marketplace. CSR 1000v offers a rich set of features that are built on Cisco's long-standing reputation as a leader in enterprise networking solutions, including routing, VPN, firewall, Network Address Translation (NAT), quality of service (QoS), application visibility, failover and WAN optimization. Using Cisco CSR1000v (Cisco IOS-XE), you can extend your enterprise network to AWS using secure tunnels (DMVPN, FlexVPN, S2SVPN) to build scalable enterprise VPNs that support distributed applications across different points of your network worldwide. Cisco's Cloud Services Router provides centralized and secure networking access for all of your applications residing on AWS. If you already use CSR 1000v, you can bring your existing license and migrate it to the CSR BYOL AMI or you can access CSR via the marketplace for a simple, pay-as-you-go hourly rate.

Secure inter-VPC connectivity

It is very common for enterprises to establish a peering connection between multiple VPCs within their AWS environment. There are too many cases where this makes sense to list them all, but we will cover a few examples. One typical use case is a large enterprise that stores the data for each of its departments in separate VPCs, requires that those departments can see each other's data. A car manufacturer, for example, may store all of the data for its manufacturing department in one VPC, and all of the data for its marketing department in another. If the marketing department wants to analyze data coming out of its manufacturing facilities to run a series of ads that describe their commitment to green manufacturing, it needs to be able to access the data that resides inside the manufacturing department's VPC. Or, customers will use interconnected VPCs spread across multiple regions as a data recovery solution that is resilient to natural disasters and other rare events that could cause physical datacenters in one region to be wiped out. Another use case would be an organization deploying an Active Directory in a VPC, which needs to communicate with applications that are running in VPCs in other AWS Regions.

These are only a few of the reasons that you may want to connect multiple VPCs together—the list goes on and on. From the AWS Marketplace, you can find several third-party solutions that enable secure, low-latency inter-VPC connectivity quickly and cost-effectively.

Aviatrix Cloud Gateway makes it easy to set up encrypted IPSEC peering between VPCs. It is comprised of two components—Aviatrix Gateway and Aviatrix Controller. Aviatrix Gateway is a scale-out VPC peering solution that enables encrypted peering across AWS Regions. It is integrated with a host of AWS services, including Elastic Load Balancing, Amazon S3, Amazon Simple Queue Service, Amazon Simple Notification Service, Amazon Route 53, and AWS CloudTrail. Aviatrix Controller is used to orchestrate Aviatrix Gateways and apply configuration and access policies, while providing a central dashboard with visibility into the VPC network to simplify administration. One of the most common reason that customers choose Aviatrix for this use case is to encrypt data that is moving between multiple EC2 instances in order to maintain PCI compliance.

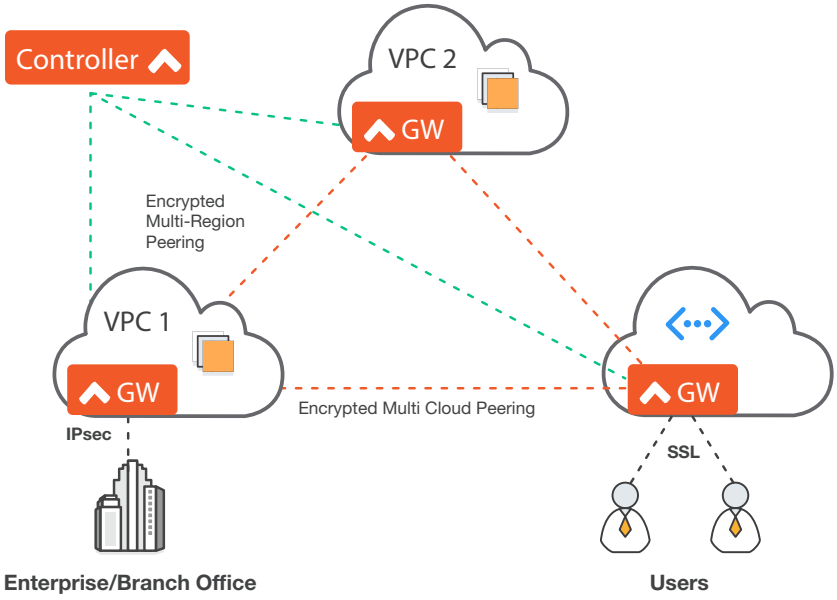

Fig. 2. Peering with Aviatrix Gateway and Aviatrix Controller

Ciphergraph Network's Cloud VPN can also be used to enable interconnectivity between your VPCs, as well as enterprise class encryption and role-based access control for your entire AWS Deployment. Direct integration into Active Directory and LDAP make this product easy to roll out across your user base. You can also have several simultaneous options for authentication to allow access to partners and customers, again subject to the security rules you specify based on identity or role.

Complement infrastructure security with application firewalls

Security threats at the application layer are more common than they've ever been. When hackers are able to gain access to organization's application, that application and the data inside it are not the only assets at risk. In a worst-case scenario, hackers can use unprotected applications as an entry point into the organization's entire IT infrastructure, where they can do damage that extends far beyond a single application.

SQL Injections are common application-based exploit in which attackers insert malicious SQL queries into the input forms of a web application with the goal of downloading or making changes to the underlying database. Injection attacks are typically enabled by cross-site scripting vulnerabilities, which allow attackers to inject malicious client-side scripts into web pages viewed by other users. This can allow them to acquire access-privileges to sensitive content, to session cookies, and to a variety of other information maintained by the browser on behalf of the user. Applications vulnerabilities are also frequently exploited by attackers to carry out DDoS attacks.

While most network security initiatives focus on protection of the underlying infrastructure, web application firewalls can add an additional layer of security to complement infrastructure security. AWS Marketplace makes it easy to deploy a web application firewall from popular software vendors to protect your AWS environment from malicious attacks that are initiated at the application layer.

Barracuda Web Application Firewall monitors all inbound web traffic to detect and block threats arising from attacks against your web applications, and guards against data loss prevention (DLP) by inspecting the HTTP responses from your back-end servers. The integrated access control engine enables administrators to create granular access control policies for Authentication, Authorization & Accounting (AAA), giving organizations strong authentication and user control. It also allows you to use CloudFormation templates for Auto Scaling, allowing you to automatically bootstrap and cluster additional instances as needed, for higher throughput and easy deployment. It also can be integrated with Elastic Load Balancing, Amazon CloudWatch, and other AWS services to enable an integrated WAF solution.

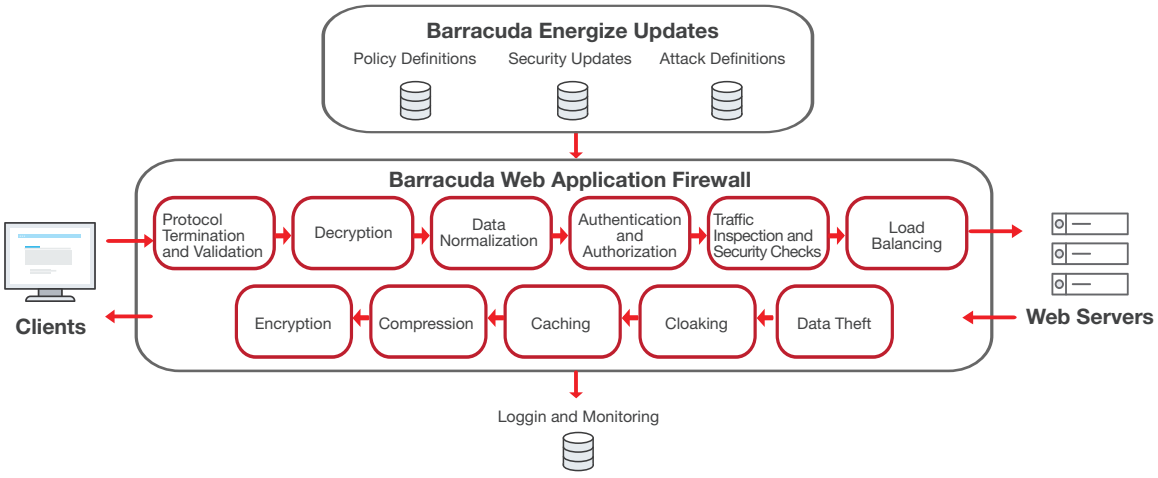

Fig. 3. Barracuda Web Application Firewall Architecture

Palo Alto's VM-Series Next-Generation Firewall Bundle analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These business relevant elements are then used as integral components of your security policy, resulting in an improved security posture and a reduction in incident response time. Traffic flowing into, and across your AWS deployment is identified and secured based on the application identity, while sophisticated cyber threats detected within the application flows are prevented and web activity are strictly controlled with URL filtering.

Conclusion

An organization's ability to capitalize on all of the performance, scalability, and agility benefits that the cloud promises is largely dependent on their networking capabilities. If an organization struggles to move data into and out of AWS quickly and securely, they aren't taking full advantage of its capabilities. By leveraging networking infrastructure solutions from popular vendors in AWS Marketplace, you can take full advantage of existing investments in on-premises systems and the cloud to meet your unique business challenges.

Learn more about Network Infrastructure Solutions from AWS Marketplace at **https://aws.amazon.com/mp/networking/**