Solution Overview: Cisco Adaptive Security Virtual Appliance Comes to Amazon Web Services
Now you can get the benefits of the industry-leading Cisco® Adaptive Security Virtual Appliance in the Amazon Web Services (AWS) cloud. The virtual appliance brings both firewall and VPN features and use cases.

Solutions for integrating Amazon AWS with your existing network become simpler when your Cisco cloud virtual firewall runs the same features and policies as your on-premises physical Adaptive Security Appliance or hypervisor-based virtual appliance. The security team needs no additional training to extend the on-premises security policies into the cloud firewall. The virtual appliance provides the familiar user interface, so your team can take advantage of the existing network management tools and processes. In addition to the software command line, a representational state transfer (REST) application programming interface (API) has been added to all Adaptive Security Appliance platforms to allow programmable configuration and monitoring (see Figure 1).

Cisco on the AWS Marketplace offers:

- Full Adaptive Security Appliance feature set
- Easy licensing for dynamic virtual environments
- Compatibility with existing configuration and management tools
- Cisco AnyConnect® and clientless remote-access VPN and site-to-site VPN
- Elastic scalability
- Cloud automation using RESTful API

### How the Amazon Virtual Private Cloud Works

The Amazon Virtual Private Cloud (VPC) is a virtual network dedicated to your AWS account. It lets you provision a network that is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources such as Amazon EC2 instances into your VPC. You have complete control over your virtual networking environment, which includes an IP address range, selected subnets, a configuration of route tables, network gateways, and security policy. You can build a VPN connection between your corporate data center and your VPC and use the AWS cloud as an extension of the data center.

Amazon VPC is designed to provide a customized network configuration. For example, you can place web servers in public-facing networks that have access to the Internet and place your backend servers such as databases or application servers in a private subnet with no Internet access. You can provision multiple layers of security to provide controlled access to Amazon EC2 instances in each subnet.

### Use Cases in Amazon AWS

#### Extending the Data Center

Amazon VPC is an extension of your corporate network. It gives you the flexibility of scaling resources at a low optional and managerial cost. You can deploy the virtual appliance to provide highly secure connectivity using an IPsec tunnel between your corporate firewall and the appliance. The VPN tunnel is created over the public Internet and encrypted using a number of advanced algorithms to provide confidentiality of the data transmitted between the Amazon VPC and your corporate data center (see Figure 2).

Users located in the corporate network can access applications hosted in AWS (subnet1 and subnet2) by means of a site-to-site tunnel.
Solution Overview: Cisco Adaptive Security Virtual Appliance Comes to Amazon Web Services

Figure 2. Data Center Extension Using a Site-to-Site Tunnel

VPC-Edge Firewall

Adding Amazon VPC to your operations is similar to adding a new network. The Cisco virtual appliance is a complete cloud security platform, offering a scalable stateful firewall, VPN, routing, and application inspection. You can deploy the appliance at the edge of Amazon VPC (see Figure 3) and provide security to internal servers. You have use of private IP addresses on servers hosted in AWS and can translate addresses on the virtual appliance so that users can access those servers through the Internet.

Figure 3. VPC-Edge Stateful Firewall

VM-to-VM security

In Amazon VPC most of the applications have a multitier design. Example: Web servers are located in public-facing networks with access to the Internet, while the database and applications are located in another network with no Internet access. The Adaptive Security Virtual Appliance can be deployed to protect communication between tiers in a multitier application environment (see Figure 4).

One must take following points into consideration while designing security for communications between virtual machines:

- AWS security groups applied to the virtual machine and the Cisco appliance interfaces must allow needed communication.
- AWS source and destination checks on all involved network interfaces must be disengaged.
Today AWS is making the VPC model even more flexible. You now have the ability to create a VPC peering connection, a networking connection between two VPCs. Instances in either VPC can communicate with each other. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.

The Adaptive Security Virtual Appliance can be deployed at both ends to provide highly secure connections using an IPsec site-to-site tunnel (see Figure 5).

**VPC Peering**

**Highly Secure Connectivity for Remote Users**

Enterprises across the globe are continually working toward increasing employee productivity and flexibility. Mobility has moved up the priority list of many IT executives, who are expanding mobility initiatives throughout the organization. The Cisco virtual appliance can be deployed as VPN gateway to provide highly secure connectivity to remote users. It supports a wide variety of remote-access VPN technologies such as AnyConnect®, clientless VPN, IPsec (Internet Key Exchange Versions 1 and 2, known as IKEv1 and IKEv2) and third-party client support with IKEv2.

The Cisco VPN configuration makes it easy for your IT staff to quickly provision remote-access VPN for mobile users and employees using their own devices (see Figure 6).

Users can access applications on AWS using their personal devices even when they are remote.
How to Deploy the Adaptive Security Virtual Appliance in Amazon AWS

The Cisco Adaptive Security Virtual Appliance is available in the Amazon AWS Marketplace by searching on “Cisco ASAv” or “Cisco.”

From the AWS Marketplace page, you can deploy the appliance in the bring-your-own-license (BYOL) mode.

For configuration assistance, please refer to the documentation on the Cisco Adaptive Security Virtual Appliance webpage.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

For more information, please visit the following pages:

- Cisco Adaptive Security Virtual Appliance “Bring Your Own License” product page on Amazon Marketplace
- Cisco seller page on Amazon Marketplace
- Product webpage