Cisco Adaptive Security Virtual Appliance

As you transform more workloads and functions into virtualized assets, you need the same protections that are available for your physical assets. Cisco has developed a virtual security solution based on the best-selling Cisco® Adaptive Security Appliance (ASA). The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. Use Cisco ASAv to protect virtual and physical data center workloads that expand, contract, or shift their location over time. And use Cisco ASAv to deliver site-to-site, remote-access, and clientless VPN as a service in virtual domains or private cloud deployments.

Cisco ASAv Overview

Applications in data centers include private cloud and physical and virtual infrastructure. With the advent of big data applications such as Hadoop, more traffic is being exchanged between nodes in a data center than between nodes that straddle data center boundaries. Cisco ASAv is a virtual appliance that provides firewall services to protect data passing between nodes within data centers and cloud environments.

Cisco ASAv runs as a virtual machine (VM) on multiple hypervisors, including VMware ESXi and a kernel-based VM (KVM), and it interacts with virtual switches to process traffic. It works with multiple virtual switches, including the Cisco Nexus® 1000v and the VMware dvSwitch and vSwitch. Multiple cloud management solutions, including custom applications, can manage the Cisco ASAv through a rich API.

Cisco ASAv uses Cisco Smart Licensing. Features include:

• Simple purchase and activation
• Easy license management due to license pooling
• Automatic license activation upon provisioning
• Accurate and simple reporting of Cisco ASAv usage in one portal

The Cisco ASA physical and virtual product portfolio can be managed by security administrators as a pool of resources that scale on demand, provide programmable automation for deployment and management, and use a common policy-based operational model across physical and virtual environments. These features reduce cost and complexity. Cisco ASAv has a built-in lab-edition mode that can be enhanced with evaluation licenses from the Cisco Smart Licensing portal.

Benefits

• Provide uniform security across physical and virtual domains with one security policy for multiple hypervisors.

• Simplify management by using representational state transfer (REST) API to manage the device, to easily introduce Cisco ASAv into software-defined networking (SDN) environments, and to incorporate ASAv into custom policy-orchestration systems.

• Accelerate and simplify provisioning with predetermined configurations to quickly deploy security services to match the speed of application deployment.
Next Steps

## Cisco ASAv Features

Table 1 describes key features of the Cisco ASAv.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single policy domain</strong></td>
<td>Identity, Cisco TrustSec tag, network, and application policies can be used to protect traffic reaching virtual and physical servers. Since the physical Cisco ASA and Cisco ASAv support the same rich policy constructs, virtual and physical domains are coalesced into a single policy domain so the same policies can be applied to all Cisco ASAs, whether they are physical or virtual.</td>
</tr>
<tr>
<td><strong>API-based management</strong></td>
<td>Cisco ASAv offers the REST API, an HTTP-based interface that facilitates management of the appliance, including changing the security policy and monitoring the status. Using REST APIs, multiple cloud management solutions can be used to manage both physical and virtual instances of Cisco ASA. In addition, custom applications can be written by customers to manage Cisco ASA and Cisco ASAv.</td>
</tr>
<tr>
<td><strong>Agile provisioning</strong></td>
<td>Cisco ASAv supports fast instantiation and Smart Licensing. It can be provisioned within a matter of minutes with a chosen configuration to quickly deploy security services. With Smart Licensing, the entitlements are automatically obtained by Cisco ASAv upon boot up. Customers can maintain a single pool of licenses, each of which can be granted to or retracted from appliances in the customer’s premises.</td>
</tr>
<tr>
<td><strong>Cisco Application Centric Infrastructure (ACI) integration</strong></td>
<td>In traditional topology-oriented environments, administrators either push policy rules as a complete rule set or manually build custom rule sets for each network appliance. With Cisco ACI integration, the Cisco Application Policy Infrastructure Controller (APIC) ties Cisco ASAv into a single point of orchestration for network and security policy configuration, the provisioning of security as a service, and flow policy control. Cisco APIC makes monitoring available for a unified view of the infrastructure while allowing for contextual reuse of common security elements in an end-to-end policy design.</td>
</tr>
<tr>
<td><strong>VPN as a service</strong></td>
<td>Cisco ASAv offers the same features as a physical Cisco ASA, including VPN services that can be deployed in the virtual domain using Cisco ASAv. Site-to-site, remote-access, and clientless VPN services can be deployed quickly in a private cloud or over a virtual infrastructure in response to demand.</td>
</tr>
</tbody>
</table>