Introduction to the Cisco ASAv

The Cisco Adaptive Security Virtual Appliance (ASAv) brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments.

You can manage and monitor the ASAv using ASDM, REST API, or CLI. Other management options may be available.

Prerequisites for the ASAv

For hypervisor support, see Cisco ASA Compatibility.

Guidelines for the ASAv (all models)

Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

Failover Guidelines

For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

Unsupported ASA Features

The ASAv does not support the following ASA features:

- Clustering
- Multiple context mode
- Active/Active failover
- EtherChannels
- Shared AnyConnect Premium Licenses

Guidelines for the ASAv5

Guidelines, Features, and Limitations for the ASAv5

- Jumbo frames are not supported.

- Beginning with 9.5(1.200), the memory requirement for the AVAv5 was reduced to 1GB. Downgrading the available memory on an ASAv5 from 2GB to 1GB is not supported. To run with 1 GB of memory, the ASAv5 VM must be redeployed with version 9.5(1.200) or later.
- In some situations, the ASAv5 may experience memory exhaustion. This can occur during certain resource heavy applications, such as enabling AnyConnect or downloading files. Console messages related to spontaneous reboots or critical syslogs related to memory usage are symptoms of memory exhaustion. In these cases, you can enable the ASAv5 to be deployed in a VM with 1.5 GB of memory. To change from 1GB to 1.5 GB, power down your VM, modify the memory, and power the VM back on.
- The ASAv5 will begin to drop packets soon after the threshold of 100 Mbps is reached (there is some headroom so that you get the full 100 Mbps). The ASAv5 is intended for users who require a small memory footprint and small throughput, so that you can deploy larger numbers of ASAv5s without using unnecessary memory.
- Supports 8000 connections per second, 25 maximum VLANs, 50,000 concurrent session, and 50 VPN sessions.
- Not supported on AWS.

Guidelines for the ASAv50

Guidelines, Features, and Limitations for the ASAv50

- Supported only on ESXi and KVM.
- Introduces support for the ixgbe-vf vNIC for SR-IOV interfaces; see ASAv and SR-IOV Interface Provisioning, page 9.
- The ASAv50 supports 10Gbps of aggregated traffic.
- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations, page 30 and Increasing Performance on KVM Configurations, page 42.
- Automatic ASP load balancing can be enabled; see Automatic Load Balancing on the ASAv, page 79.
- Transparent mode is not supported.
- Amazon Web Services (AWS), Microsoft Azure, and Hyper-V are not supported.
- The ixgbe NIC is not supported for the ASAv50 in this release.

System Requirements

The specific hardware used for ASAv deployment can vary, depending on size and usage requirements. Table 1 on page 6 shows the compliant resources scenarios that match license entitlement for the different ASAv platforms. In addition, SR-IOV Virtual Functions require specific system resources.

Host Operating System and Hypervisor Support

SR-IOV support and VF drivers are available for:

- Linux 2.6.30 kernel or later

The ASAv with SR-IOV interfaces is currently supported on the following hypervisors:

- VMware vSphere/ESXi 5.5 and 6.0
- QEMU/KVM
- AWS

Hardware Platform Support

This section describes hardware guidelines for SR-IOV support. Although these are guidelines, not requirements, using hardware that does not meet these guidelines may result in functionality problems or poor performance.

A server that supports SR-IOV is required in addition to an SR-IOV capable PCIe adapter. You must be aware of the following hardware considerations:

- The capabilities of SR-IOV NICs, including the number of VFs available, differ across vendors and devices.
- Not all PCIe slots support SR-IOV.
- SR-IOV-capable PCIe slots may have different capabilities.

You should consult your manufacturer's documentation for SR-IOV support on your system.

- For VT-d enabled chipsets, motherboards, and CPUs, you can find information from this page of virtualization-capable IOMMU supporting hardware. VT-d is a required BIOS setting for SR-IOV systems.
- For VMware, you can search their online Compatibility Guide for SR-IOV support.
- For KVM, you can verify CPU compatibility. Note that for the ASAv on KVM we only support x86 hardware.

  Note: We tested the ASAv with the Cisco UCS C-Series Rack Server. Note that the Cisco UCS-B server does not support the ixgbe-vf vNIC.

Supported NICs for SR-IOV

- Intel Ethernet Server Adapter X520 - DA2
- Intel Ethernet Server Adapter X540

CPUs

- x86_64 multicore CPU
  - Intel Sandy Bridge or later (Recommended)

  Note: We tested the ASAv on Intel's Broadwell CPU (E5-2699-v4) at 2.3GHz.
- Cores
  - Minimum of 8 physical cores per CPU socket
  - The 8 cores must be on a single socket.

  Note: CPU pinning is recommended to achieve full throughput rates on the ASAv50; see Increasing Performance on ESXi Configurations, page 30 and Increasing Performance on KVM Configurations, page 42.

BIOS Settings

SR-IOV requires support in the BIOS as well as in the operating system instance or hypervisor that is running on the hardware. Check your system BIOS for the following settings:

- SR-IOV is enabled
- VT-x (Virtualization Technology) is enabled
- VT-d is enabled
- (optional) Hyperthreading is disabled

We recommend that you verify the process with the vendor documentation because different systems have different methods to access and change BIOS settings.

Guidelines, Features, and Limitations for ixgbe-vf Interfaces

- The guest VM is not allowed to set the VF to promiscuous mode. Because of this, transparent mode is not supported when using ixgbe-vf.

- The guest VM is not allowed to set the MAC address on the VF. Because of this, the MAC address is not transferred during HA like it is done on other ASA platforms and with other interface types. HA failover works by transferring the IP address from active to standby.
- The Cisco UCS-B server does not support the ixgbe-vf vNIC.

Smart Software Licensing for the ASAv

Cisco Smart Software Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAs without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance.

Note: The ASAv product identifier (PID) is "ASAv". When you deploy the ASAv, it's important that you use a unique hostname to identify your ASAv. A hostname cannot be the same as the PID when using Smart Software Licensing.

For complete information about Smart Software Licensing for the ASAv, see the "Guidelines for Smart Software Licensing" and "Defaults for Smart Software Licensing" sections of the Cisco ASA Series General Operations Configuration Guide.

See the following tables for information about ASAv licensing entitlements, resources, and model specifications:

- **Smart License Entitlements**—Table 1 on page 6 shows the compliant resources scenarios that match license entitlement for the ASAv platforms.

  Note: The ASAv uses Cisco Smart Software Licensing. A smart license is required for regular operation. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. For more information, see Smart Software Licensing for the ASAv.

- **ASAv Licensing States**—Table 2 on page 7 shows the ASAv states and messages connected to resources and entitlement for the ASAvs.
- **ASAv Model Descriptions and Specifications**—Table 3 on page 8 shows the ASAv models and associated specifications, resource requirements, and limitations.

Table 1 Smart License Entitlements

License Entitlement	vCPU/RAM	Throughput	Rate Limiter Enforced
Lab Edition Mode (no license)	All Platforms	100Kbps	Yes
ASAv5 (100M)	1vCPU/1 GB to 1.5 GB	100Mbps	Yes
ASAv10 (1 GB)	1vCPU/2 GB	1Gbps	Yes
ASAv30 (2 GB)	4vCPU/8 GB	2Gbps	Yes
ASAv50 (10 GB)	8vCPU/16 GB	10Gbps	Yes

Table 2 ASAv Licensing States

State	Resources vs. Entitlement	Actions and Messages
Compliant	Resource = Entitlement limits (vCPU, GB of RAM)	Appliances optimally resourced ASAv5 (1vCPU,1G), ASAv10 (1vCPU,2G), ASAv30 (4vCPU,8G), ASAv50 (8vCPU, 16G) No actions, no messages
	Resources < Entitlement limits Under-provisioned	No actions while Warning messages are logged that ASAv cannot run at licensed throughput.
Non-compliant	Resources > Entitlement limits Over-provisioned	ASAv rate limiter engages to limit performance and log Warnings on the console.
		ASAv10, ASAv30, and ASAv50 reboot after logging Error messages on the console.

Table 3 ASAv Model Descriptions and Specifications

Model	License Requirement
ASAv5	Smart license See the following specifications: ■ 100 Mbps throughput ■ 1 vCPU ■ 1 GB RAM (adjustable to 1.5 GB) ■ 50,000 concurrent firewall connections ■ Does not support AWS ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv10	Smart license See the following specifications: ■ 1 Gbps throughput ■ 1 vCPU ■ 2 GB RAM ■ 100,000 concurrent firewall connections ■ Supports AWS on c3.large, c4.large, and m4.large instances ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv30	Smart license See the following specifications: ■ 2 Gbps throughput ■ 4 vCPUs ■ 8 GB RAM ■ 500,000 concurrent firewall connections ■ Supports AWS on c3.xlarge, c4.xlarge, and m4.xlarge instances ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv50	Smart license See the following specifications: ■ 10 Gbps throughput ■ 8 vCPUs Minimum of 8 physical cores per CPU socket required (cannot be provisioned across multiple CPU sockets) ■ 16 GB RAM ■ 2,000,000 concurrent firewall connections ■ Does not support AWS, Microsoft Azure, or Hyper-V

ASAv Interfaces and Virtual NICs

As a guest on a virtualized platform, the ASAv utilizes the network interfaces of the underlying physical platform. Each ASAv interface maps to a virtual NIC (vNIC).

ASAv Interfaces

The ASAv includes the following Gigabit Ethernet interfaces:

- Management 0/0

  For AWS and Azure, Management 0/0 can be a traffic-carrying “outside” interface.
- GigabitEthernet 0/0 through 0/8. Note that the GigabitEthernet 0/8 is used for the failover link when you deploy the ASAv as part of a failover pair.
- TenGigabitEthernet 0/0 through 0/8 on the ASAv50. Note that the TenGigabitEthernet 0/8 is used for the failover link when you deploy the ASAv50 as part of a failover pair.
- Hyper-V supports up to eight interfaces. Management 0/0 and GigabitEthernet 0/0 through 0/6. You can use GigabitEthernet as a failover link.

Supported vNICs

The ASAv supports the following vNICs:

vNIC Type	Hypervisor Support		ASAv Version	Notes
	VMware	KVM		
VMXNET3	**Yes**	No	9.9(2) and later	When using VMXNET3, you need to disable Large Receive Offload (LRO) to avoid poor TCP performance. See the following VMware support articles: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	**Yes**	**Yes**	9.2(1) and later	VMware default.
Virtio	No	**Yes**	9.3(2.200) and later	KVM default.
ixgbe-vf	**Yes**	**Yes**	9.8(1) and later	AWS default; ESXi and KVM for SR-IOV support.

ASAv and SR-IOV Interface Provisioning

Single Root I/O Virtualization (SR-IOV) allows multiple VMs running a variety of guest operating systems to share a single PCIe network adapter within a host server. SR-IOV allows a VM to move data directly to and from the network adapter, bypassing the hypervisor for increased network throughput and lower server CPU burden. Recent x86 server processors include chipset enhancements, such as Intel VT-d technology, that facilitate direct memory transfers and other operations required by SR-IOV.

The SR-IOV specification defines two device types:

- Physical Function (PF)—Essentially a static NIC, a PF is a full PCIe device that includes SR-IOV capabilities. PFs are discovered, managed, and configured as normal PCIe devices. A single PF can provide management and configuration for a set of virtual functions (VFs).
- Virtual Function (VF)—Similar to a dynamic vNIC, a VF is a full or lightweight virtual PCIe device that provides at least the necessary resources for data movements. A VF is not managed directly but is derived from and managed through a PF. One or more VFs can be assigned to a VM.

SR-IOV is defined and maintained by the Peripheral Component Interconnect Special Interest Group (PCI SIG), an industry organization that is chartered to develop and manage the PCI standard. For more information about SR-IOV, see the PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology.

Provisioning SR-IOV interfaces on the ASAv requires some planning, which starts with the appropriate operating system level, hardware and CPU, adapter types, and adapter settings.