Manuals+ — User Manuals Simplified.

CISCO ASAv5 Adaptive Security Virtual Appliance User Guide

Contents

CISCO ASAv5 Adaptive Security Virtual Appliance
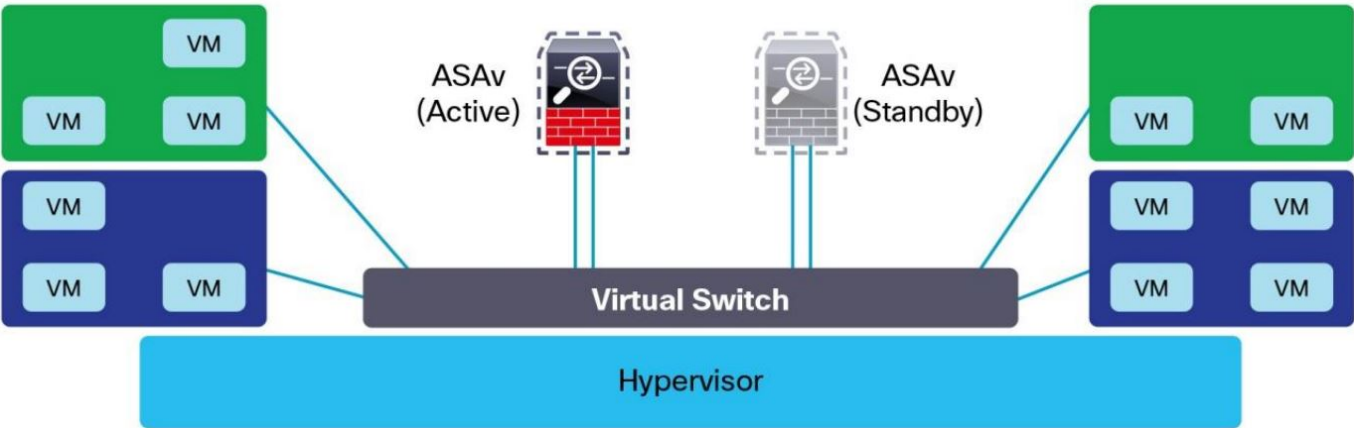
Specifications

- **Model:** ASAv
- **Firewall Functionality:** Full firewall functionality
- **Supported Environments:** Virtualized environments, data center traffic, multitenant environments
- **Management Options:** ASDM, CLI
- **Hypervisor Support:** Refer to Cisco ASA Compatibility
- **Licensing:** Cisco Smart Software Licensing
- **Smart License Requirement:** Yes, a smart license is required for regular operation
- **Throughput Limitation:** Until a license is installed, throughput is limited to 100 Kbps for preliminary connectivity tests

Usage Instructions

Installing a Smart License

To use the ASAv with regular operation and remove the throughput limitation, you need to install a smart license. Follow the steps below to install a smart license on the ASAv:

1. Obtain a valid smart license from Cisco.
2. Access the ASAv management interface using ASDM or CLI.
3. Navigate to the licensing section.
4. Select the option to install a new license.
5. Enter the license key provided by Cisco.
6. Follow the on-screen instructions to complete the license installation process.

Resource Specifications

The following table provides resource specifications for the supported private and public deployment targets:

Model	vCPU/RAM	Throughput	Rate Limiter Enforced
ASAv5 (100M)	1vCPU/1 GB to 1.5 GB	100Mbps (2 GB recommended)	Yes
ASAv10 (1 GB)	1vCPU/2 GB	1Gbps	Yes
ASAv30 (2 GB)	4vCPU/8 GB	2Gbps	Yes

FAQ

- **Q:** Is a smart license required for the ASAv?
- **A:** Yes, a smart license is required for the regular operation of the ASAv. Until a license is installed, the throughput is limited to 100 Kbps for preliminary connectivity tests.
- **Q:** How can I install a smart license on the ASAv?
- **A:** To install a smart license on the ASAv, follow the steps provided in the "Installing a Smart License" section of the user manual.
- **Q:** What are the resource specifications for different ASAv models?
- **A:** The resource specifications for different ASAv models are listed in the "Resource Specifications" section of

the user manual.

- **Q:** What management options are available for the ASAv?
- **A:** The ASAv can be managed using ASDM (Adaptive Security Device Manager) or CLI (Command Line Interface).

Introduction to the ASAv

- The Adaptive Security Virtual Appliance (ASAv) brings full firewall functionality to virtualized environments to secure data centre traffic and multitenant environments.
- You can manage and monitor the ASAv using ASDM or CLI. Other management options may be available.

Hypervisor Support

- For hypervisor support, see Cisco ASA Compatibility.

Licensing for the ASAv

The ASAv uses Cisco Smart Software Licensing. For complete information, see Smart Software Licensing.
You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.
Note
See the following sections for information about ASAv licensing entitlements and resource specifications for the supported private and public deployment targets.

Licensing for the ASAv

- See the following tables for information about ASAv licensing entitlements, licensing states, required resources, and model specifications:
- Table 1: ASAv Smart License Entitlements—This shows the compliant resource scenarios that match license entitlement for the ASAv platform.

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.

• Table 2: ASAv Licensing States—Shows the ASAv states and messages connected to resources and entitlement for the ASAvs.
• Table 3: ASAv Model Descriptions and Specifications—Shows the ASAv models and associated specifications, resource requirements, and limitations.

Smart License Entitlements

The ASAv uses Cisco Smart Software Licensing. For detailed information, see Smart Software Licensing for the ASAv and ASA.

Note: You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.

Table 1: ASAv 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 (2 GB recommended)	100Mbps	Yes
ASAv10 (1 GB)	1vCPU/2 GB	1Gbps	Yes
ASAv30 (2 GB)	4vCPU/8 GB	2Gbps	Yes

Licensing States

Table 2: ASAv Licensing States

State	Resources vs. Entitlement	Actions and Messages
Compliant	Resource = Entitlement limits (vCPU, GB of RAM)	Appliances optimally resourced No actions, no messages
	Resources < Entitlement limits Under-provisioned	No actions while Warning messages are logged that ASAv cannot run at licensed throughput.

State	Resources vs. Entitlement	Actions and Messages
Non-compliant	Resources > Entitlement limits Over-provisioned	ASAv rate limiter engages to limit performance and log Warnings on the console.

Model Descriptions and Specifications

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) **Note** For optimum performance we recommend 2 GB of memory for the ASAv5. • 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

Model	License Requirement
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

Guidelines and Limitations

• The ASAv firewall functionality is very similar to the ASA hardware firewalls but with the following guidelines

and limitations.

Guidelines and Limitations for the ASAv (all models)

Disk Storage

- The ASAv supports a maximum virtual disk of 8 GB by default. You cannot increase the disk size beyond 8 GB. Keep this in mind when you provision your VM resources.

Context Mode Guidelines

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

Failover for High Availability Guidelines

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

Important: When creating a high availability pair using ASAv, it is necessary to add the data interfaces to each ASAv in the same order. If the same interfaces are added to each ASAv, but in different order, errors may be presented at the ASAv console. Failover functionality may also be affected.

Unsupported ASA Features

The ASAv does not support the following ASA features:

- Clustering (for all entitlements, except KVM and VMware)
- Multiple context mode
- Active/Active failover
- EtherChannels
- Shared AnyConnect Premium Licenses

Limitations

- The ASAv is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. (VMware only)

Guidelines and Limitations for the ASAv5

Performance Guidelines

- Supports 8000 connections per second, 25 maximum VLANs, 50,000 concurrent sessions, and 50 VPN sessions.
- 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.
- Beginning with 9.5(1.200), the memory requirement for the AVAv5 was reduced to 1GB. Downgrading the

available memory on an ASAv5 from 2 GB to 1 GB is not supported. To run with 1 GB of memory, the ASAv5 VM must be redeployed with version 9.5(1.200) or later. Similarly, if you try to downgrade to a version earlier than 9.5(1.200), you must increase the memory to 2 GB.

Note: For optimum performance, we recommend 2 GB of memory for the ASAv5.

- 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.
- You can display a summary of the maximum memory and current free memory available to the system using the show memory command from the CLI.
- 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).

Limitations

- ASAv5 is not compatible with AnyConnect HostScan 4.8, which requires 2 GB of RAM.
- ASAv5 is not supported on Amazon Web Services (AWS).
- Jumbo frames are not supported.

ASAv Interfaces and Virtual NICs

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

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.
- Hyper-V supports up to eight interfaces. Management 0/0 and GigabitEthernet 0/0 through 0/6. You can use GigabitEthernet 0/6 as a failover link.

Supported vNICs
The ASAv supports the following vNICs.
Table 4: Supported vNics
Table 5: Supported vNics

| vNIC Type | Hypervisor Support | | ASAv Version | Notes |
	VMware	KVM		
e1000	Yes	Yes	9.2(1) and later	VMware default
virtio	No	Yes	9.3(2.200) and later	KVM default

Disable LRO for VMware and VMXNET3

Large Receive Offload (LRO) is a technique for increasing the inbound throughput of high-bandwidth network connections by reducing CPU overhead. It works by aggregating multiple incoming packets from a single stream into a larger buffer before they are passed higher up the networking stack, thus reducing the number of packets that have to be processed. However, LRO can lead to TCP performance problems where network packet delivery may not flow consistently and could be "bursty" in congested networks.

Important: VMware enables LRO by default to increase overall throughput. It is therefore a requirement to disable LRO for ASAv deployments on this platform.

You can disable LRO directly on the ASAv machine. Power off the virtual machine before you make any configuration changes.

1. Find the ASAv machine in the vSphere Web Client inventory.
    -   To find a virtual machine, select a data centre, folder, cluster, resource pool, or host.
    -   Click the Related Objects tab and click Virtual Machines.
2. Right-click the virtual machine and select Edit Settings.
3. Click VM Options.
4. Expand Advanced.
5. Under Configuration Parameters, click the Edit Configuration button.
6. Click Add Parameter and enter a name and value for the LRO parameters:
    -   Net.VmxnetSwLROSL | 0
    -   Net.Vmxnet3SwLRO | 0
    -   Net.Vmxnet3HwLRO | 0
    -   Net.Vmxnet2SwLRO | 0
    -   Net.Vmxnet2HwLRO | 0

        Optionally, if the LRO parameters exist, you can examine the values and change them if needed. If a parameter is equal to 1, LRO is enabled. If equal to 0, LRO is disabled.

        Note
7. Click OK to save your changes and exit the Configuration Parameters dialogue box.
8. Click Save.

See the following VMware support articles for more information:

-   VMware KB 1027511
-   VMware KB 2055140

Documents / Resources

	[CISCO ASAv5 Adaptive Security Virtual Appliance](#) [pdf] User Guide ASAv5, ASAv10, ASAv30, ASAv5 Adaptive Security Virtual Appliance, Adaptive Security Virtual Appliance, Virtual Appliance

References

- **VMware Knowledge Base**
- **VMware Knowledge Base**
- **CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4 - Licenses: Smart Software Licensing (ASAv, ASA on Firepower) [Cisco ASA 5500-X Series Firewalls] - Cisco**
- **Cisco Secure Firewall ASA Compatibility - Cisco**
- **User Manual**