

Introduction to the Secure Firewall ASA Virtual

The Adaptive Security Appliance Virtual (ASA Virtual) brings full firewall functionality to virtualized environments to secure data center traffic and multitenant environments.

You can manage and monitor the ASA Virtual using ASDM or CLI. Other management options may be available.

- Hypervisor Support, on page 1
- Licensing for the ASA Virtual, on page 1
- Guidelines and Limitations, on page 5
- ASA Virtual Interfaces and Virtual NICs, on page 9
- ASA Virtual and SR-IOV Interface Provisioning, on page 11

Hypervisor Support

For hypervisor support, see Cisco Secure Firewall ASA Compatibility.

Licensing for the ASA Virtual

The ASA Virtual uses Cisco Smart Software Licensing. For complete information, see Smart Software Licensing.

Note You must install a smart license on the ASA Virtual. 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.

Beginning with 9.13(1), any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration. This allows you to deploy an ASA Virtual on a wide variety of VM resource footprints. Session limits for Secure Client and TLS Proxy are determined by the ASA Virtual platform entitlement installed rather than a platform limit tied to a model type.

See the following sections for information about ASA Virtual licensing entitlements and resource specifications for the supported private and public deployment targets.

About Smart License Entitlements

Any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration. This allows you to run the ASA Virtual on a wide variety of VM resource footprints. This also increases the number of supported AWS and Azure instances types. When configuring the ASA Virtual machine, the maximum supported number of vCPUs is 16 (ASAv100); and the maximum supported memory is 64GB for ASA virtual deployed on all platforms other than AWS and OCI. For ASA virtual deployed on AWS and OCI, the maximum supported memory is 128GB.

When configuring the ASA Virtual machine, the maximum supported number of vCPUs is 16 (ASAv100 license) for ASA virtual deployed on all platforms other than VMware and KVM. For ASA virtual deployed on VMware and KVM, the maximum supported number of vCPUs is 32 when you use the ASAvU license. For ASA virtual deployed on AWS, the maximum supported number of vCPUs is 64 when you use the ASAvU license. The ASAvU license is available on VMware, KVM, and AWS deployments. The maximum supported memory is 32GB for ASA virtual deployed on Azure, Rackspace, and Hyper-V. For ASA virtual deployed on AWS, OCI, VMware, and KVM, the maximum supported memory is 128GB.

Note ASAvU is the only license option for VMware and KVM deployments with 32 vCPUs. If you upgrade from a 16 vCPU deployment to a 32 vCPU deployment with an ASAv100 license, the VM will enter an unlicensed state.

Important It is not possible to change the resource allocation (memory, CPUs, disk space) of an ASA Virtual instance once it is deployed. If you need to increase your resource allocations for any reason, for example to change your licensed entitlement from the ASAv30/2Gbps to the ASAv50/10Gbps, you need to create a new instance with the necessary resources.

- vCPUs: The ASA Virtual supports 1 to 16 vCPUs on all platforms other than VMware, KVM, and AWS.

  The ASA Virtual supports 1 to 32 vCPUs on VMware and KVM, and 1 to 64 vCPUs on AWS.
- Memory: The ASA Virtual supports 2GB to 64GB of RAM for ASA virtual deployed on all platforms other than AWS and OCI. For ASA virtual deployed on AWS and OCI, the maximum supported memory is 128GB.

  The ASA Virtual supports 2GB to 64GB of RAM for ASA virtual deployed on Azure, Rackspace, and Hyper-V. For ASA virtual deployed on AWS, OCI, VMware, and KVM, the maximum supported memory is 128GB.
- Disk storage: The ASA Virtual supports a minimum virtual disk of 8GB by default. Depending on the type of platform, the virtual disk support varies between 8GB to 10GB. Keep this in mind when you provision your VM resources.

Important The minimum memory requirement for deploying ASA Virtual with more than 1 vCPU is 4 GB.

To upgrade ASA Virtual from version 9.14 or later to a newer version, the ASA virtual machine requires a minimum memory of 4 GB and 2 vCPUs.

Session Limits for Licensed Features

Session limits for Secure Client and TLS Proxy are determined by the installed ASA Virtual platform entitlement tier, and enforced via a rate limiter. The following table summarizes the session limits based on the entitlement tier and rate limiter.

Table 1: ASA Virtual Session Limits by Entitlement

Entitlement	Secure Client Premium Peers	Total TLS Proxy Sessions	Rate Limiter
Standard Tier, 100M	50	500	150 Mbps
Standard Tier, 1G	250	500	1 Gbps
Standard Tier, 2G	750	1000	2 Gbps
Standard Tier, 10G	10,000	10,000	10 Gbps
Standard Tier, 20G	20,000	20,000	20 Gbps

The session limits granted by an entitlement, as shown in the previous table, cannot exceed the session limits for the platform. The platform session limits are based on the amount of memory provisioned for the ASA Virtual.

Table 2: ASA Virtual Session Limits by Memory Requirement

Provisioned Memory	Secure Client Premium Peers	Total TLS Proxy Sessions
2 GB to 7.9 GB	250	500
8 GB to 15.9 GB	750	1000
16 GB - 31.9 GB	10,000	10,000
32 GB to 64 GB	20,000	20,000
64 GB to 128 GB	20,000	20,000

Platform Limits

Firewall connections, concurrent and VLANs are platform limits based on the ASA Virtual memory.

Note We limit the firewall connections to 100 when the ASA Virtual is in an unlicensed state. Once licensed with any entitlement, the connections go to the platform limit. The minimum memory requirement for the ASA Virtual is 2GB.

Table 3: Platform Limits

ASA Virtual Memory	Firewall Conns, Concurrent	VLANs
2 GB to 7.9 GB	100,000	50

ASA Virtual Memory	Firewall Conns, Concurrent	VLANs
8 GB to 15.9 GB	500,000	200
16 GB to 31.9	2,000,000	1024
32 GB to 64 GB	4,000,000	1024

Note A known issue in ASA Virtual version 9.22.2.14 may cause interface instability and performance issues due to incomplete interface initialization. It is recommended to use a later maintenance release where this issue is resolved before deploying ASA Virtual in production environments.

ASA Virtual Private Cloud Entitlements (VMware, KVM, Hyper-V)

Because any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration, you have greater flexibility when you deploy the ASA Virtual in a private cloud environment (VMware, KVM, Hyper-V).

Session limits for Secure Client and TLS Proxy are determined by the installed ASA Virtual platform entitlement tier, and enforced via a rate limiter. The following table summarizes the session limits based on the entitlement tier for the ASA Virtual deployed to a private cloud environment, with the enforced rate limiter.

Note ASA Virtual session limits are based on the amount of memory provisioned for the ASA Virtual; see Table 2: ASA Virtual Session Limits by Memory Requirement, on page 3.

Table 4: ASA Virtual on VMware/KVM/HyperV Private Cloud - Licensed Feature Limits Based on Entitlement

RAM (GB)		Entitlement Support*				
Min	Max	Standard Tier, 100M	Standard Tier, 1G	Standard Tier, 2G	Standard Tier, 10G	Standard Tier, 20G
2	7.9	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
8	15.9	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
16	31.9	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
32	64	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	20K/20K/20G
*Secure Client Sessions / TLS Proxy Sessions / Rate Limiter per entitlement/instance.						

ASA Virtual Public Cloud Entitlements (AWS)

Because any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration, you can deploy the ASA Virtual on a wide variety AWS instances types. Session limits for Secure Client and

TLS Proxy are determined by the installed ASA Virtual platform entitlement tier, and enforced via a rate limiter.

Pay-As-You-Go (PAYG) Mode

The following table summarizes the Smart Licensing entitlements for each tier for the hourly billing (PAYG) mode, which is based on the allocated memory.

Table 5: ASA Virtual on AWS - Smart License Entitlements for PAYG

RAM (GB)	Hourly Billing Mode Entitlement
< 2 GB	Standard Tier, 100M (ASAv5)
2 GB to < 8 GB	Standard Tier, 1G (ASAv10)
8 GB to < 16 GB	Standard Tier, 2G (ASAv30)
16 GB to < 32 GB	Standard Tier, 10G (ASAv50)
30 GB and higher	Standard Tier, 20G (ASAv100)
64 GB	Unlimited Tier (ASAvU)
128 GB	Unlimited Tier (ASAvU)

ASA Virtual Public Cloud Entitlements (Azure)

Because any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration, you can deploy the ASA Virtual on a wide variety Azure instances types. Session limits for Secure Client and TLS Proxy are determined by the installed ASA Virtual platform entitlement tier, and enforced via a rate limiter.

Guidelines and Limitations

The ASA Virtual firewall functionality is very similar to the ASA hardware firewalls, but with the following guidelines and limitations.

Guidelines and Limitations for the ASA Virtual (all entitlements)

Smart Licensing Guidelines

- The maximum supported number of vCPUs is 16. The maximum supported memory is 64GB for ASA virtual deployed on all platforms other than AWS and OCI. For ASA virtual deployed on AWS and OCI, the maximum supported memory is 128GB. Any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration.
- Session limits for licensed features and unlicensed platform capabilities are set based on the amount of VM memory.

- Session limits for Secure Client and TLS Proxy are determined by the ASA Virtual platform entitlement; session limits are no longer associated with an ASA Virtual model type (ASAv5/10/30/50/100/ASAvU).
- Session limits have a minimum memory requirement; in cases where the VM memory is below the minimum requirement, the session limits will be set for the maximum number supported by the amount of memory.
- There are no changes to existing entitlements; the entitlement SKU and display name will continue to include the model number (ASAv5/10/30/50/100/ASAvU).
- The entitlement sets the maximum throughput via a rate limiter.
- The rate limiter is removed when you use the ASAvU entitlement.
- There is no change to customer ordering process.

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 license entitlement; for example, both units should have the 2Gbps entitlement.



Important

- When creating a High Availability (HA) pair using ASA Virtual, it is necessary to add the data interfaces to each ASA Virtual in the same order. If the exact same interfaces are added to each ASA Virtual, but in different order, errors may be presented at the ASA Virtual console. Failover functionality may also be affected.
- HA can be configured between two ASA virtual instances even if there is a resource mismatch (Example: One instance with 8GB RAM and another with 16GB RAM). This configuration is supported to facilitate hitless upgrades. However, it is not recommended running HA with resource disparities beyond the necessary duration until the resource allocation changes is complete.
- In ASA Virtual Primary–Standby with Secondary-Active configuration, reloading the standby node can result in 3–4 ping timeouts on the Secondary-Active outside interface. This is expected behavior. During reload, the standby node briefly assumes interface configuration before HA state synchronization completes, causing MAC and active IP renegotiation with the upstream switch and a temporary traffic interruption.

Unsupported ASA Features

The ASA Virtual does not support the following ASA features:

- Clustering (for all entitlements, except AWS, KVM and VMware)
- Multiple context mode
- Active/Active failover
- EtherChannels

- Shared AnyConnect Premium Licenses

Limitations

- The ASA Virtual 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 1 GB Entitlement

Performance Guidelines

- Jumbo frame reservation on the 1 GB platform with 9 or more configured e1000 interfaces may cause the device to reload. If **jumbo-frame reservation** is enabled, reduce the number of interfaces to 8 or less. The exact number of interfaces will depend on how much memory is needed for the operation of other features configured, and could be less than 8.

Guidelines and Limitations for the 10 GB Entitlement

Performance Guidelines

- Supports 10Gbps of aggregated traffic.
- Supports the following practices to improve ASA Virtual performance:
  - Numa nodes
  - Multiple RX queues
  - SR-IOV provisioning
  - See Performance Tuning and Performance Tuning for more information.
- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations and Increasing Performance on KVM Configurations.
- Jumbo frame reservation with a mix of e1000 and i40e-vf interfaces may cause the i40e-vf interfaces to remain down. If **jumbo-frame reservation** is enabled, do not mix interface types that use e1000 and i40e-vf drivers.

Limitations

- Transparent mode is not supported.
- The ASA Virtual 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 20 GB Entitlement

Performance Guidelines

- Supports 20Gbps of aggregated traffic.
- Supports the following practices to improve ASA Virtual performance:
  - Numa nodes
  - Multiple RX queues
  - SR-IOV provisioning
  - See Performance Tuning and Performance Tuning for more information.
- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations and Increasing Performance on KVM Configurations.

Limitations

- The ASA Virtual is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. (VMware only)
- Transparent mode is not supported.
- Not supported on Amazon Web Services (AWS) and Hyper-V.

Guidelines and Limitations for the ASA Virtual Unlimited Entitlement

Performance Guidelines

- Rate limiter is removed.
- Supported on VMware, KVM, and AWS.
- Supports High Availability
- Supports clustering for a maximum of 16 nodes in individual mode and spanned mode
- For optimal performance, we recommend using the Intel E810 ethernet network adapter series or similar ethernet network adaptors that support a high number of queues. On the Intel X710 ethernet network adapter series, queue to core mapping issues result in reduced performance levels.
- For practices to improve ASA virtual performance on KVM and VMware, see Performance Tuning on KVM and Performance Tuning on VMware.
- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations and Increasing Performance on KVM Configurations.

ASA Virtual Interfaces and Virtual NICs

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

- ASA Virtual Interfaces
- Supported vNICs

Note Hyperthreading is not recommended for ASA Virtual deployments.

ASA Virtual Interfaces

The ASA Virtual 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 ASA Virtual as part of a failover pair.

Note To simply configuration migration, Ten GigabitEthernet interfaces, like those available on the VMXNET3 driver, are labeled GigabitEthernet. This has no impact on the actual interface speed and is cosmetic only.

The ASA Virtual defines GigabitEthernet interfaces using the E1000 driver as 1Gbps links. Note that VMware no longer recommends using the E1000 driver.

- 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 ASA Virtual supports the following vNICs. Mixing vNICs, such as e1000 and vmxnet3, on the same ASA Virtual is not supported.

Table 6: Supported vNics

vNIC Type	Hypervisor Support		ASA Virtual Version	Notes
	VMware	KVM		
vmxnet3	Yes	No	9.9(2) and later	VMware default When using vmxnet3, you need to disable Large Receive Offload (LRO) to avoid poor TCP performance. See Disable LRO for VMware and VMXNET3, on page 10.
e1000	Yes	Yes	9.2(1) and later	Not recommended by VMware.
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.
i40e-vf	No	Yes	9.10(1) and later	KVM for SR-IOV support.

Disable LRO for VMware and VMXNET3

Large Receive Offload (LRO) is a technique for increasing 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 perfomance 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 ASA Virtual deployments on this platform.

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

1. Find the ASA Virtual machine in the vSphere Web Client inventory.
   a. To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b. 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



Note 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.

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

See the following VMware support articles for more information:

- VMware KB 1027511
- VMware KB 2055140

ASA Virtual 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 PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology.

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

Guidelines and Limitations for SR-IOV Interfaces

The specific hardware used for ASA Virtual deployment can vary, depending on size and usage requirements. Licensing for the ASA Virtual, on page 1 explains the compliant resource scenarios that match license entitlement for the different ASA Virtual 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 ASA Virtual with SR-IOV interfaces is currently supported on the following hypervisors:

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

Hardware Platform Support

Note You should deploy the ASA Virtual on any *server class* x86 CPU device capable of running the supported virtualization platforms.

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

A server that supports SR-IOV and that is equipped with an SR-IOV-capable PCIe adapter is required. 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.

Note 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 ASA Virtual on KVM we only support x86 hardware.

Note We tested the ASA Virtual 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 Network Adapter X710

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

- Intel Ethernet Server Adapter X520 - DA2

CPUs

- x86_64 multicore CPU

  Intel Sandy Bridge or later (Recommended)

Note We tested the ASA Virtual 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 and ASAv100; see Increasing Performance on ESXi Configurations and Increasing Performance on KVM Configurations.

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.

Limitations

Be aware of the following limitations when using 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.

Note This limitation is applicable to the i40e-vf interfaces too.

- The Cisco UCS-B server does not support the ixgbe-vf vNIC.
- In a failover setup, when a paired ASA Virtual (primary unit) fails, the standby ASA Virtual unit takes over as the primary unit role and its interface IP address is updated with a new MAC address of the standby ASA Virtual unit. Thereafter, the ASA Virtual sends a gratuitous Address Resolution Protocol (ARP) update to announce the change in MAC address of the interface IP address to other devices on the same network. However, due to incompatibility with these types of interfaces, the gratuitous ARP update is not sent to the global IP address that is defined in the NAT or PAT statements for translating the interface IP address to global IP addresses.