



思科 ASA v 简介

思科自适应安全虚拟设备 (ASA v) 可为虚拟环境提供完整的防火墙功能，从而确保数据中心流量和多租户环境的安全。

您可以使用 ASDM 或 CLI 来管理和监控 ASA v。其他管理选项也可能可用。

- [虚拟机监控程序支持，第 1 页](#)
- [ASA v 的许可，第 1 页](#)
- [准则和限制，第 6 页](#)
- [ASA v 接口和虚拟 NIC，第 9 页](#)
- [ASA v 和 SR-IOV 接口调配，第 11 页](#)

虚拟机监控程序支持

有关虚拟机监控程序支持的信息，请参阅[思科 ASA 兼容性](#)。

ASA v 的许可

ASA v 使用思科智能软件许可。有关完整信息，请参阅[智能软件许可 \(ASA v, ASA on Firepower\)](#)。



注释

您必须在 ASA v 上安装智能许可证。在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。需要安装智能许可证才能正常运行。

从 9.13(1) 开始，现在可在任何受支持的 ASA v vCPU/内存配置中使用任何 ASA v 许可证。这可以让您在各种各样的 VM 资源上部署 ASA v。AnyConnect 和 TLS 代理的会话限制由安装的 ASA v 平台授权确定，而不是与型号相关的平台限制。

有关支持的私有和公共部署目标的 ASA v 许可授权和资源规格，请参阅以下各节。

关于智能许可证授权

可在任何受支持的 ASA v CPU/内存配置中使用任何 ASA v 许可证。这可以让您在各种各样的 VM 资源上运行 ASA v。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 ASA v VM 时，支持的最大数量 Vcpu 为 16 (ASA v100)；支持的最大内存为 64GB RAM。



重要事项

部署后无法更改 ASA v 实例的资源配置（内存、CPU、磁盘空间）。如果出于任何原因需要增加资源配置，例如将许可的授权从 ASA v30/2Gbps 更改为 ASA v50/10Gbps，则需要使用必要的资源创建新实例。

- vCPUs — ASA v 支持 1 至 16 个 vCPU。
- Memory — the ASA v 支持 2 GB 到 64 GB 的 RAM。
- 磁盘存储 - 默认情况下，ASA v 支持最大 8 GB 的虚拟磁盘。磁盘大小不能超过 8 GB。在调配 VM 资源时，请记住这一点。



重要事项

ASA v 的最低内存要求为 2GB。如果当前 ASA v 的内存少于 2GB，您将无法在不增加 ASA v VM 内存的情况下，从早期版本升级到 9.13(1) 或更高版本。您也可以使用最新版本重新部署新的 ASA v VM。

部署具有超过 1 个 vCPU 的 ASA v 时，ASA v 的最低内存要求是 4GB。

许可功能的会话限制

AnyConnect 和 TLS 代理的会话限制由安装的 ASA v 平台授权确定，并通过速率限制器强制执行。下表总结了基于授权层和速率限制器的会话限制。

表 1: ASA v 会话限制（按授权）

授权	AnyConnect 高级版对等体数	TLS 代理会话总数	速度限制器
标准层, 100M	50	500	150 Mbps
标准层, 1G	250	500	1 Gbps
标准层, 2G	750	1000	2 Gbps
标准层, 10G	10,000	10,000	10 Gbps
标准层, 20G	2 万	2 万	20 Gbps

权限授予的会话限制（如上表所示）不能超过平台的会话限制。平台会话限制基于为 ASA v 调配的内存量。最大 ASA v VM 维度是 8 vCPU 和 64 GB 内存。

表 2: ASA 会话限制 (按内存要求)

调配的内存	AnyConnect 高级版对等体数	TLS 代理会话总数
2 GB 至 7.9 GB	250	500
8 GB 至 15.9 GB	750	1000
16 GB - 31.9 GB	10,000	10,000
32 GB 至 64 GB	2 万	2 万

平台限制

并行防火墙连接数和 VLAN 是基于 ASA 内存的平台限制。



注释 当 ASA 处于“未许可”状态时，防火墙连接数限制为 100。获得任何授权的许可后，连接数将遵循平台限制。ASA 的最低内存要求为 2GB。

表 3: 平台限制

ASA 内存	并发防火墙连接数	VLAN
2 GB 至 7.9 GB	100,000	50
8 GB 至 15.9 GB	500,000	200
16 GB 至 31.9	2,000,000	1024
32 GB 至 64 GB	4,000,000	1024

ASA 私有云授权 (VMware、KVM、Hyper-v)

由于任何 ASA 许可证均可用于任何受支持的 ASA vCPU/内存配置，因此在私有云环境 (VMware、KVM、Hyper-v) 中部署 ASA 时具有更大的灵活性。



注释 HyperV 上不支持 ASA50 和 ASA100。

AnyConnect 和 TLS 代理的会话限制由安装的 ASA 平台授权确定，并通过速率限制器强制执行。下表根据部署到私有云环境的 ASA 的授权层 (具有强制速率限制器) 总结了会话限制。



注释 ASA 会话限制基于为 ASA 调配的内存量；请参阅表 2: ASA 会话限制 (按内存要求)，第 3 页。

表 4: ASA on VMware/KVM/HyperV Private Cloud - 基于授权的许可功能限制

随机存取存储器(GB)		权限支持*				
		标准层, 100M	标准层, 1G	标准层, 2G	标准层, 10G	标准层, 20G
最小值	最大值					
2	7.9	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
8	159	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
16	319	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

*每个权限/实例的 AnyConnect 会话数/TLS 代理会话数/速率限制器。

ASA 公有云授权 (AWS)

由于任何 ASA 许可证均可用于任何支持的 ASA vCPU/内存配置，因此您可以在各种不同的 AWS 实例类型上部署 ASA。AnyConnect 和 TLS 代理的会话限制由安装的 ASA 平台授权确定，并通过速率限制器强制执行。

下表总结了基于 AWS 实例类型的授权层的速率限制器和会话限制。有关受支持实例的 AWS VM 维度（vCPU 和内存）细分信息，请参阅“关于 AWS 云上的 ASA 部署”。

表 5: 基于授权的 ASA on AWS 许可功能限制

实例	BYOL 授权支持*				PAYG**
	标准层, 100M	标准层, 1G	标准层, 2G	标准层, 10G	
c5.xlarge	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000
c5.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K
c4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
c3.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
m4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500

实例	BYOL 授权支持*				PAYG**
	标准层, 100M	标准层, 1G	标准层, 2G	标准层, 10G	
m4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	10K/10K
m4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K

*每个权限/实例的 AnyConnect 会话数/TLS 代理会话数/速率限制器。
 ** AnyConnect 会话/TLS 代理会话。在 PAYG 模式下未采用速率限制器。

即付即用 (PAYG) 模式

下表总结了每一层的智能许可授权，以用于基于分配的内存的小时计费 (PAYG) 模式。

表 6: AWS 上的 ASA v - PAYG 的智能许可证授权

随机存取存储器(GB)	每小时计费模式授权
2 GB 至 < 8 GB	标准层, 1G
8 GB 至 < 16 GB	标准层, 2G
16 GB-64 GB	标准层, 10G

ASA v 公有云授权 (Azure)

由于任何 ASA v 许可证均可用于任何支持的 ASA v vCPU/内存配置，因此您可以在各种不同的 Azure 实例类型上部署 ASA v。AnyConnect 和 TLS 代理的会话限制由安装的 ASA v 平台授权确定，并通过速率限制器强制执行。

下表总结了基于 Azure 实例类型的授权层的速率限制器和会话限制。有关受支持实例的 Azure VM 维度 (vCPU 和内存) 细分信息，请参阅“关于 Microsoft Azure Cloud 上的 ASA v 部署”。



注释 Azure 上的 ASA v 目前不支持“即付即用” (PAYG) 模式。

表 7: 基于授权的 Azure 许可功能限制的 ASA v

实例	BYOL 授权支持*				
	标准层, 100M	标准层, 1G	标准层, 2G	标准层, 10G	标准层, 20G
D1, D1_v2DS1, DS1_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
D2, D2_v2, DS2, DS2_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G

实例	BYOL 授权支持*				
	标准层, 100M	标准层, 1G	标准层, 2G	标准层, 10G	标准层, 20G
D3, D3_v2, DS3, DS3_v2	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4, D4_v2, DS4, DS4_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D5, D5_v2, DS5, DS5_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
D2_v3	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D8_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
F4, F4s	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
F8, F8s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
F16, F16s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G

*每个权限/实例的 AnyConnect 会话数/TLS 代理会话数/速率限制器。

准则和限制

ASA v 防火墙功能与思科 ASA 硬件防火墙非常相似，但存在以下准则和限制。

ASA v（所有权限）准则和限制

智能许可准则

- Vcpu 支持的最大数量为 8；支持的最大内存为 64GB RAM。可在任何受支持的 ASA v vCPU/内存配置中使用任何 ASA v 许可证。
- 许可功能和未许可平台功能的会话限制根据 VM 内存量设置。
- AnyConnect 和 TLS 代理的会话限制取决于 ASA v 平台授权；会话限制不再与 ASA v 型号类型 (ASA v5/10/30/50/100) 关联。
- 会话限制有最低内存要求；如果 VM 内存低于最低要求，会话限制将设置为内存量支持的最大数。
- 现有授权没有任何变化；授权 SKU 和显示名称将继续包括型号 (ASA v5/10/30/50/100)。
- 授权通过速度限制器设置最大吞吐量。

- 客户订购过程没有变化。

磁盘存储

默认情况下，ASA 支持最大 8 GB 的虚拟磁盘。磁盘大小不能超过 8 GB。在调配 VM 资源时，请记住这一点。

情景模式准则

仅支持单情景模式。不支持多情景模式。

通过故障切换实现高可用性准则

对于故障切换部署，请确保备用设备具有相同的许可证权限；例如，两台设备均应具备 2Gbps 权限。



重要事项

使用 ASA 创建高可用性对时，需要按相同顺序将数据接口添加到每个 ASA。如果将完全相同的接口添加到每个 ASA，但顺序不同，ASA 控制台上可能会显示错误。故障切换功能可能也会受到影响。

不支持的 ASA 功能

ASA 不支持以下 ASA 功能：

- 可调整
- 集群
- 多情景型号
- 主用/主用故障切换
- EtherChannel
- 共享 AnyConnect 高级许可证

限制

- ASA 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）

1 GB 权限的准则和限制

性能准则

- 在配置了 9 个或更多 e1000 接口的 1 GB 平台上，巨帧预留可能会导致设备重新加载。如果启用巨帧预留，请将接口数量减到 8 个或更少。接口的确切数量取决于已配置的其他功能正常工作所需的内存，可以少于 8 个。

10 GB 权限的准则和限制

性能准则

- 支持 10Gbps 的汇聚流量。
- 支持通过以下实践提高 ASA v 性能：
 - Numa 节点
 - 多个 RX 队列
 - SR-IOV 调配
 - 有关详细信息，请参阅[ASA v on VMware 的性能调整](#)和[ASA v on KVM 的性能调整](#)。
- 建议通过 CPU 固定来实现完整的吞吐量速率；请参阅[提高 ESXi 配置的性能](#)和[提高 KVM 配置的性能](#)。
- 混合使用 e1000 和 i40e-vf 接口的巨帧预留可能会导致 i40e-vf 接口保持关闭。如果启用巨帧预留，请不要混合使用 e1000 和 i40e-vf 驱动程序的接口类型。

限制

- 不支持透明模式。
- ASA v 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）
- 不受 Hyper-v 支持。

20 GB 权限的准则和限制

性能准则

- 支持 20Gbps 的汇聚流量。
- 支持通过以下实践提高 ASA v 性能：
 - Numa 节点
 - 多个 RX 队列
 - SR-IOV 调配
 - 有关详细信息，请参阅[ASA v on VMware 的性能调整](#)和[ASA v on KVM 的性能调整](#)。
- 建议通过 CPU 固定来实现完整的吞吐量速率；请参阅[提高 ESXi 配置的性能](#)和[提高 KVM 配置的性能](#)。

限制

- ASA v 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）
- 不支持透明模式。
- 不支持 Amazon Web 服务 (AWS) 和 Hyper-V。

ASA v 接口和虚拟 NIC

作为虚拟化平台上的访客，ASA v 使用底层物理平台的网络接口。每个 ASA v 接口映射到一个虚拟 NIC (vNIC)。

- ASA v 接口
- 支持的 vNIC

ASA v 接口

ASA v 包括以下千兆以太网接口：

- Management 0/0
对于 AWS 和 Azure，Management 0/0 可以是传输流量的“外部”接口。
- GigabitEthernet 0/0 到 0/8。请注意，如果将 ASA v 部署为故障切换对的成员，则 GigabitEthernet 0/8 将用于故障切换链路。



注 释 为了进行简单的配置迁移，十个千兆以太网接口（如 VMXNET3 驱动程序上可用的接口）已被标记为千兆以太网。这对实际接口速度没有影响，仅作为外观显示。

ASA v 将使用 E1000 驱动程序的 GigabitEthernet 接口定义为 1Gbps 链路。请注意，VMware 不再建议使用 E1000 驱动程序。

- Hyper-V 最多支持八个接口。Management 0/0 和 GigabitEthernet 0/0 至 0/6。您可以将 GigabitEthernet 0/6 用作故障切换链路。

支持的 vNIC

ASA v 支持以下 vNIC。不支持在同一 ASA v 上混合 vNIC，例如 e1000 和 vmxnet3。

表 8: 支持的 vNIC

vNIC 类型	虚拟机监控程序支持		ASA 版本	备注
	VMware	KVM		
vmxnet3	支持	不支持	9.9(2) 及更高版本	VMware 默认值 如果使用 vmxnet3, 则需要禁用 Large Receive Offload (LRO), 以免 TCP 性能不佳。请参阅 禁用 VMware 和 VMXNET3 的 LRO , 第 10 页。
e1000	是	是	9.2(1) 及更高版本	不建议使用 VMware。
virtio	不支持	支持	9.3(2.200) 及更高版本	KVM 默认值
ixgbe-vf	是	是	9.8(1) 及更高版本	AWS 默认值; 支持 SR-IOV 的 ESXi 和 KVM。
i40e-vf	不支持	支持	9.10(1) 及更高版本	对 SR-IOV 的 KVM 支持。

禁用 VMware 和 VMXNET3 的 LRO

Large Receive Offload (LRO) 技术通过减少 CPU 开销增加高带宽网络连接的入站吞吐量。它的工作方式是, 将从单一流传入的多个数据包聚合到更大的缓冲区, 然后向网络堆栈上方传递, 从而减少必须处理的数据包数量。不过, LRO 可能会导致 TCP 性能问题, 即网络数据包传送可能不会一致流动, 而是在拥挤的网络中“突发”。



重要事项

VMware 默认启用 LRO, 以增加整体吞吐量。因此, 此平台要求在 ASA 部署中禁用 LRO。

您可以在 ASA 虚拟机上直接禁用 LRO。在进行任何配置更改之前, 请关闭虚拟机。

- 在 vSphere Web Client 清单中查找 ASA 虚拟机。
 - 要查找虚拟机, 请选择一个数据中心、文件夹、集群、资源池或主机。
 - 单击**相关对象 (Related Objects)** 选项卡, 然后单击**虚拟机 (Virtual Machines)**。
- 右键单击虚拟机, 然后选择**编辑设置 (Edit Settings)**。
- 单击**VM 选项 (VM Options)**。
- 展开**高级**。

5. 在“配置参数”(Configuration Parameters)下，单击**编辑配置 (Edit Configuration)**按钮。
6. 单击**添加参数 (Add Parameter)** 并输入 LRO 参数的名称和值：
 - Net.VmxnetSwLROSL | 0
 - Net.Vmxnet3SwLRO | 0
 - Net.Vmxnet3HwLRO | 0
 - Net.Vmxnet2SwLRO | 0
 - Net.Vmxnet2HwLRO | 0



注 (可选) 如果存在 LRO 参数，您可以检查这些值并在需要时进行更改。如果参数等于 1，则 LRO 已启用。如果等于 0，则 LRO 已禁用。

7. 单击**确定 (OK)** 以保存您的更改并退出**配置参数 (Configuration Parameters)** 对话框。
8. 单击**保存 (Save)**。

有关详细信息，请参阅以下 VMware 支持文章：

- VMware KB [1027511](#)
- VMware KB [2055140](#)

ASA 和 SR-IOV 接口调配

单一根 I/O 虚拟化 (SR-IOV) 允许运行各种访客操作系统的多个 VM 共享主机服务器内的单个 PCIe 网络适配器。SR-IOV 允许 VM 在网络适配器中绕过虚拟机监控程序而直接移入或移出数据，从而提高网络吞吐量及降低服务器 CPU 负担。最新的 x86 服务器处理器包括芯片组增强功能（例如 Intel VT-d 技术），它们可促进 SR-IOV 所需的直接内存传输及其他操作。

SR-IOV 规范定义了两种设备类型：

- 物理功能 (PF) - 实质上属于静态 NIC，PF 是完整的 PCIe 设备，包括 SR-IOV 功能。PF 按正常 PCIe 设备的方式进行发现、管理和配置。使用单个 PF 可为一组虚拟功能 (VF) 提供管理和配置。
- 虚拟功能 (VF) - 类似于动态 vNIC，VF 是完整或轻型虚拟 PCIe 设备，至少提供必要的移动数据资源。VF 并非直接进行管理，而是通过 PF 进行获取和管理。可以为一台 VM 分配一个或多个 VF。

SR-IOV 由外围组件互联专业组 (PCI SIG) 定义和维护，该行业组织负责开发和管理 PCI 标准。有关 SR-IOV 的详细信息，请参阅《[PCI-SIG SR-IOV 入门：SR-IOV 技术简介](#)》。

要在 ASA 上调配 SR-IOV 接口，需要从适当的操作系统级别、硬件和 CPU、适配器类型及适配器设置等开始进行一些规划。

SR-IOV 接口准则和限制

根据规模和使用要求，用于 ASA 部署的具体硬件可能不尽相同。[ASA 的许可](#)，第 1 页说明了与不同 ASA 平台的许可证授权相匹配的合规资源方案。此外，SR-IOV 虚拟功能还需要特定的系统资源。

主机操作系统和虚拟机监控程序支持

SR-IOV 支持和 VF 驱动程序可用于：

- Linux 2.6.30 内核或更高版本

以下虚拟机管理程序目前支持带 SR-IOV 接口的 ASA：

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

硬件平台支持



注释

您应该在能够运行支持的虚拟化平台的任何服务器类 x86 CPU 设备上部署 ASA。

本节介绍 SR-IOV 接口的硬件准则。尽管这些只是准则而不是要求，但使用不符合这些准则的硬件可能会导致功能问题或性能不佳。

需要一台支持 SR-IOV 并配备了支持 SR-IOV 的 PCIe 适配器的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。



注释

请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。

- 对于启用 VT-d 的芯片组、主板和 CPU，可以从“[支持虚拟化功能的 IOMMU 支持硬件](#)”页面中查找相关信息。VT-d 是 SR-IOV 系统所需的 BIOS 设置。
- 对于 VMware，可以搜索[兼容性指南](#)以启用 SR-IOV 支持。

- 对于 KVM，可以验证 [CPU 兼容性](#)。请注意，对于 KVM 上的 ASA v，我们仅支持 x86 硬件。



注 我们使用思科 UCS C 系列机架服务器对 ASA v 进行了测试。请
释 注意，思科 UCS-B 服务器不支持 ixgbe-vf vNIC。

SR-IOV 支持的 NIC

- [Intel 以太网服务器适配器 X710](#)



注 ASA v 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或
意 更新版本的驱动程序将正常工作。（仅适用于 VMware）

- [Intel 以太网服务器适配器 X520 - DA2](#)

CPU

- X86_64 多核 CPU

Intel 沙桥或更高版本（推荐）



注 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率
释 对 ASA v 进行了测试。

- 核心
 - 每个 CPU 插槽至少 8 个物理核心
 - 8 个核心必须位于一个插槽中。



注 建议使用 CPU 固定实现 ASA v50 和 ASA v100 上的完整吞吐量
释 速率；请参阅[提高 ESXi 配置的性能](#)和[提高 KVM 配置的性能](#)。

BIOS 设置

SR-IOV 需要 BIOS 以及硬件上运行的操作系统实例或虚拟机监控程序方面的支持。检查系统 BIOS 中的以下设置：

- 已启用 SR-IOV
- 已启用 VT-x（虚拟化技术）

- 已启用 VT-d
- (可选) 已禁用超线程

我们建议您通过供应商文档验证该过程，因为不同的系统使用不同的方法来访问和更改 BIOS 设置。

限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 ASA 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障切换通过从主用设备向备用设备传送 IP 地址的方式运行。
- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。