思科 ASA 各版本的新功能

思科 ASA 新功能

本文档列出每个版本的新功能。

注释 系统日志消息指南中列出了新增的、更改的和已弃用的系统日志消息。

版本 9.10 的新功能

ASA 9.10(1)/ASDM 7.10(1) 的新功能

发布日期：**2018** 年 **10** 月 **25** 日

功能	描述
平台功能	
适用于 Azure 的 ASAv VHD 自定义图像	您现在可以使用思科提供的压缩的 VHD 映像，在 Azure 上创建自定义 ASAv 映像。要使用 VHD 映像进行部署，您需要将 VHD 映像上传到您的 Azure 存储帐户。然后，您可以使用上传的磁盘映像和 Azure 资源管理器模板创建托管映像。Azure 模板是包含资源说明和参数定义的 JSON 文件。
ISA 3000 支持 FirePOWER 模块版本 6.3	以前支持的版本为 FirePOWER 5.4。
防火墙功能	
思科 Umbrella 支持	您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的企业安全策略应用于用户连接。您可以允许或阻止基于 FQDN 的连接，或者，对于可疑的 FQDN，您可以将用户重定向至思科 Umbrella 智能代理，该代理可以执行 URL 筛选。Umbrella 配置是 DNS 检测策略的一部分。 新增/修改的命令：**umbrella**、**umbrella-global**、**token**、**public-key**、**timeout edns**、**dnscrypt** 和 **show service-policy inspect dns detail**。 新增/修改的菜单项： **配置 > 防火墙 > 对象 > Umbrella**、**配置 > 防火墙 > 对象 > 检测映射 > DNS**

功能	描述
MSISDN 的 GTP 检测增强功能和选择模式筛选、防重放以及用户防欺骗	您现在可以配置 GTP 检测基于移动站点国际用户目录编号 (MSISDN) 或选择模式丢弃创建 PDP 情景消息。您还可以实施防重放和用户防欺骗。 新增/修改的命令：**anti-replay**、**gtp-u-header-check**、**match msisdn** 和 **match selection-mode**。 新增/修改的菜单项： **配置** > **防火墙** > **对象** > **检测映射** > **GTP** > **添加/编辑**对话框
TCP 状态绕行的默认空闲超时	TCP 状态绕行连接的默认空闲超时现在为 2 分钟，而不是 1 小时。
支持从直接转发代理登录页面删除注销按钮。	如果您配置直接转发代理获取用户身份信息（AAA 身份验证侦听器），您现在可以从页面中删除注销按钮。这在用户从 NAT 设备后面连接并且无法按 IP 地址进行区分的情况下非常有用。当一个用户注销时，它会注销该 IP 地址的所有用户。 新增/修改的命令：**aaa authentication listener no-logout-button** 无 ASDM 支持。 同样适用于 *9.8(3)*。
Trustsec SXP 连接可配置删除抑制计时器	默认 SXP 连接抑制计时器为 120 秒。现在，您可以配置此计时器，范围介于 120 到 64000 秒之间。 新增/修改的命令：**cts sxp delete-hold-down period**、**show cts sxp connection brief** 和 **show cts sxp connections**。 无 ASDM 支持。 同样适用于 *9.8(3)*。
支持在透明模式下卸载经过 NAT 的数据流。	如果您使用了数据流分流（**flow-offload enable** 和 **set connection advanced-options flow-offload** 命令），分流的数据流现在可以包括在透明模式下需要 NAT 的数据流。
Firepower 4100/9300 ASA 逻辑设备透明模式部署	在 Firepower 4100/9300 上部署 ASA 时，您现在可以指定透明模式或路由模式。 新增/修改的 FXOS 命令：**enter bootstrap-key FIREWALL_MODE**、**set value routed** 和 **set value transparent** 新增/修改的 Firepower 机箱管理器菜单项： **逻辑设备** > **添加设备** > **设置** 新增/修改的选项：**防火墙模式**下拉列表
VPN 功能	

功能	描述
支持传统 SAML 身份验证	如果您部署的 ASA 包含对 CSCvg65072 的修复，则默认的 SAML 行为是使用嵌入式浏览器，而这在 AnyConnect 4.4 或 4.5 上不受支持。因此，要继续使用 AnyConnect 4.4 或 4.5，您必须启用传统外部浏览器 SAML 身份验证方法。由于安全限制，只能将此选项用作迁移至 AnyConnect 4.6（或更高版本）的临时计划的一部分。此选项在近期将会弃用。 新增/修改的命令：**saml external-browser** 新增/修改的菜单项： **配置 > 远程接访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件**页面 **> 连接配置文件**区域 **> 添加**按钮 **> 添加 AnyConnect 连接配置文件**对话框 **配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 连接配置文件** > 页面 **> 连接配置文件**区域 **> 添加**按钮 **> 添加无客户端 SSL VPN 连接配置文件**对话框 新增/修改的选项：**SAML 外部浏览器**复选框 同样适用于 *9.8(3)*。
DTLS 1.2 支持 AnyConnect VPN 远程访问连接。	除了当前支持的 DTLS 1.0（版本号 1.1 未用于 DTLS）之外，DTLS 1.2（如 RFC- 6347 中定义）现在也支持 AnyConnect 远程访问。这适用于除 5506 以外的所有 ASA 型号；并且仅当 ASA 用作服务器而不是客户端时适用。DTLS 1.2 支持其他密码，以及所有最新的 TLS/DTLS 密码和更大的 cookie。 新增/修改的命令：**show run ssl**、**show vpn-sessiondb detail anyconnectssl cipher**、**ssl server-version** 新增/修改的菜单项：**配置 > 远程访问 VPN > 高级 > SSL 设置**
高可用性和扩展性功能	
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id.slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的 FXOS 命令：**set cluster-control-link network** 新增/修改的 Firepower 机箱管理器菜单项： **逻辑设备 > 添加设备 > 集群信息** 新增/修改的选项：**CCL 子网 IP** 字段

功能	描述
按 Firepower 9300 机箱并行加入集群设备	对于 Firepower 9300，此功能可确保机箱中的安全模块同时加入集群，以便在模块之间均匀分配流量。如果某个模块先于其他模块很早加入，它可能会收到超过所需的流量，因为其他模块还无法分担负载。 新增/修改的命令：**unit parallel-join** 新增/修改的菜单项： **配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群** 新增/修改的选项：**按机箱并行加入设备**区域
集群接口防反跳时间现在应用于从故障状态更改为正常运行状态的接口	在发生接口状态更新时，ASA 会等待 **health-check monitor-interface debounce-time** 命令或 ASDM **配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**菜单项中指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。此功能现在应用于从故障状态更改为正常运行状态的接口。例如，对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群上的接口仅仅因为另一个集群设备在绑定端口时的速度更快便显示为故障状态。 未修改任何命令。 未修改任何菜单项。
Microsoft Azure 管理云中 ASAv 的主用/备用高可用性	Azure 管理云现在支持无状态主用/备用解决方案，可允许主用 ASAv 故障触发系统自动执行故障切换到 Microsoft Azure 公共云中的备用 ASAv。 新增或修改的命令：**failover cloud** 新增或修改的菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **故障切换** **监控** > **属性** > **故障切换** > **状态** **监控** > **属性** > **故障切换** > **历史记录**
接口功能	
show interface ip brief 和 **show ipv6 interface** 输出增强为可显示 Firepower 2100/4100/9300 的管理引擎关联	对于 Firepower 2100/4100/9300，命令输出增强为指示接口的管理引擎关联状态。 新增/修改的命令：**show interface ip brief**、**show ipv6 interface**
Firepower 2100 上的 **set lacp-mode** 命令已更改为 **set port-channel-mode**	为了与 Firepower 4100/9300 中的命令用法保持一致，**set lacp-mode** 命令已更改为 **set port-channel-mode**。 新增/修改的 FXOS 命令：**set port-channel-mode**
管理和故障排除功能	

功能	描述
在 Firepower 2100 上支持 NTP 身份验证	现在，您可以在 FXOS 中配置 SHA1 NTP 服务器身份验证。 新增/修改的 FXOS 命令：**enable ntp-authentication**、**set ntp-sha1-key-id**、**set ntp-sha1-key-string** 新增/修改的 Firepower 机箱管理器菜单项： **平台设置** > **NTP** 新增/修改的选项：**NTP 服务器身份验证**：**启用**复选框、**身份验证密钥**字段、**身份验证值**字段
无需使用 ACL 便可匹配 IPv6 流量的数据包捕获支持	如果您在 **capture** 命令中使用 **match** 关键字，则 **any** 关键字仅匹配 IPv4 流量。现在，您可以指定 **any4** 和 **any6** 关键字，以捕获 IPv4 或 IPv6 流量。**any** 关键字仍旧仅匹配 IPv4 流量。 新增/修改的命令：**capture match** 无 ASDM 支持。
Firepower 2100 上支持将公共密钥身份验证用于到 FXOS 的 SSH 连接	您可以设置 SSH 密钥，以便改为使用公共密钥身份验证/同时使用密码身份验证。 新增/修改的 FXOS 命令：**set sshkey** 不支持 Firepower 机箱管理器。
支持 GRE 和 IPinIP 封装	当您在内部接口上执行包捕获时，命令输出现已得到增强，可以显示 ICMP、UDP、TCP 和其他连接中的 GRE 和 IPinIP 封装。 新增/修改的命令：**show capture**
支持启用内存阈值来限制应用缓存分配	您可以将应用缓存分配限制在特定内存阈值范围内，以便预留充足的内存来保持设备稳定运行且可以管理。 新增/修改的命令：**memory threshold enable**、**show run memory threshold**、**clear conf memory threshold**
支持 RFC 5424 日志记录时间戳	您可以启用 RFC 5424 格式的日志记录时间戳。 新增/修改的命令：**logging timestamp**
支持显示 TCB-IPS 的内存使用情况	您可以显示用于 TCB-IPS 的应用级内存缓存 新增/修改的命令：**show memory app-cache**

版本 9.9 的新功能

ASDM 7.9(2.152) 的新功能

发布日期：**2018** 年 **5** 月 **9** 日

功能	描述
VPN 功能	
对传统 SAML 身份验证的支持	如果您部署的 ASA 包含对 CSCvg65072 的修复，则默认的 SAML 行为是使用嵌入式浏览器，而这在 AnyConnect 4.4 或 4.5 上不受支持。因此，要继续使用 AnyConnect 4.4 或 4.5，您必须启用传统外部浏览器 SAML 身份验证方法。由于安全限制，只能将此选项用作迁移至 AnyConnect 4.6 的临时计划的一部分。此选项在近期将会弃用。 新建/修改的菜单项： **配置** > **远程接入 VPN** > **网络（客户端）接入** > **AnyConnect 连接配置文件**页面 > **连接配置文件**区域 > **添加**按钮 > **添加 AnyConnect 连接配置文件**对话框 **配置** > **远程接入 VPN** > **无客户端 SSL VPN 接入** > **连接配置文件** > 页面 > **连接配置文件**区域 > **添加**按钮 > **添加无客户端 SSL VPN 连接配置文件**对话框 新增/修改的选项：**SAML 外部浏览器**复选框

ASA 9.9(2)/ASDM 7.9(2) 的新功能

发布日期：**2018** 年 **3** 月 **26** 日

功能	描述
平台功能	
ASAv 支持 VMware ESXi 6.5	ASAv 虚拟平台支持在 VMware ESXi 6.5 上运行的主机。新的 VMware 硬件版本已添加到 *vi.ovf* 和 *esxi.ovf* 文件，使 ESXi 6.5 上的 ASAv 能够实现最佳的性能和可用性。 未修改任何命令。 未修改任何菜单项。
ASAv 支持 VMXNET3 接口	ASAv 虚拟平台支持 VMware 虚拟机监控程序上的 VMXNET3 接口。 未修改任何命令。 未修改任何菜单项。

功能	描述
ASAv 在首次启动时支持虚拟串行控制台	现在，您可以配置 ASAv 在首次启动时使用虚拟串行控制台，而不是虚拟 VGA 控制台来访问和配置 ASAv。 新增或修改的命令：**console serial**
ASAv 支持更新多个 Azure 订用中用户定义的路由，从而在 Microsoft Azure 上实现高可用性	现在，您可以在 Azure 高可用性配置中配置 ASAv，以更新多个 Azure 订用中用户定义的路由。 新增或修改的命令：**failover cloud route-table** 新增或修改的菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 路由表**
VPN 功能	
远程访问 VPN 多情景支持已扩展至 IKEv2 协议	支持配置 ASA，以允许 Anyconnect 和基于标准的第三方 IPSec IKEv2 VPN 客户端建立远程访问 VPN 会话，连接到以多情景模式运行的 ASA。
与 Radius 服务器的 IPv6 连接	ASA 9.9.2 现在支持到外部 AAA Radius 服务器的 IPv6 连接。
实现 BVI 支持的 Easy VPN 增强功能	Easy VPN 经过增强，可支持使用网桥虚拟接口作为其内部安全接口，并且现在允许管理员直接使用新的 **vpnclient secure interface** [*interface-name*] 命令来配置内部安全接口。 可以将物理接口或网桥虚拟接口分配为内部安全接口。如果管理员未设置此选项，Easy VPN 将会使用与以前一样的安全级别选择其内部安全接口，而不论此接口是独立的物理接口还是 BVI。 此外，现在如果在 BVI 上启用了管理访问，则可以在其上面配置 **telnet**、**http** 和 **ssh** 等管理服务。 新增或修改的命令：**vpnclient secure interface** [*interface-name*]、**https**、**telnet**、**ssh**、**management-access**
分布式 VPN 会话的改进	• 改善了用于均衡分布式站点间 VPN 主用和备份会话的主用会话重新分发逻辑。此外，可针对由管理员输入的单一 **cluster redistribute vpn-sessiondb** 命令，在后台重复执行均衡进程多达八次。 • 改善了跨集群动态反向路由注入 (RRI) 的处理。
高可用性和扩展性功能	
内部故障后自动重新加入集群	过去，许多错误条件导致集群设备从集群中移除，并且在解决问题后需要手动重新加入集群。现在，设备默认将尝试以下列时间间隔自动重新加入群集：5 分钟、10 分钟以及 20 分钟。这些值是可配置的。内部故障包括：应用程序同步超时、不一致的应用程序状态等。 新增或修改的命令：**health-check system auto-rejoin**、**show cluster info auto-join** 新增或修改的菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群 > 自动重新加入**

功能	描述
ASA 5000-X 系列可配置防反跳时间，以将接口标记为发生故障	您现在可以在 ASA 5500-X 系列上配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。此功能可以加快接口故障检测的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。默认的防反跳时间是 500 毫秒，该时间的范围是 300 毫秒至 9 秒。此功能之前在 Firepower 4100/9300 上可用。 新增或修改的命令：**health-check monitor-interface debounce-time** 新增或修改的菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**
显示集群可靠传输协议消息的传输相关统计信息	现在，您可以查看每台设备的集群可靠传输缓冲区使用情况，因此您可以确定在控制平面的缓冲区已满时发生的丢包问题。 新增或修改的命令：**show cluster info transport cp detail**
显示对等设备的故障切换历史记录	现在，您可以使用 **details** 关键字查看对等设备的故障切换历史记录。这包括故障切换状态更改和发生状态更改的原因。 新增或修改的命令：**show failover**
管理功能	
RSA 密钥对支持 3072 位密钥	您现在可以将模数长度设为 3072。 新增或修改的命令：**crypto key generate rsa modulus** 新增或修改的菜单项：**配置** > **设备管理** > **证书管理** > **身份证书**
FXOS 引导程序配置现在会设置启用密码	在 Firepower 4100/9300 上部署 ASA 时，引导程序配置中的密码设置现在会设置启用密码，以及管理员用户密码。需要 FXOS 版本 2.3.1。
监控和故障排除功能	
SNMP IPv6 支持	ASA 现在支持基于 IPv6 的 SNMP，包括通过 IPv6 与 SNMP 服务器通信，允许通过 IPv6 执行查询和陷阱，以及支持现有 MIB 使用 IPv6 地址。我们添加了以下新的 SNMP IPv6 MIB 对象，如 RFC 8096 中所述。 • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30) - 包含每个接口 IPv6 特定的信息。 • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32) - 包含由此实体获知的所有前缀。 • ipAddressTable (OID: 1.3.6.1.2.1.4.34) - 包含与实体接口相关的寻址信息。 • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35) - 包含从 IP 地址到物理地址的映射。 新增或修改的命令：**snmp-server host** 注释 **snmp-server host-group** 命令不支持 IPv6。 新增或修改的菜单项：**配置** > **设备管理** > **管理访问** > **SNMP**

功能	描述
利用条件调试来排除单一用户会话故障	条件调试功能现在可帮助您根据设置的筛选器条件来验证特定 ASA VPN 会话的日志。针对 IPv4 和 IPv6 子网提供“any, any”支持。

ASDM 7.9(1.151) 的新功能

发布日期：**2018** 年 **2** 月 **14** 日

此版本中无新增功能。

ASA 9.9(1)/ASDM 7.9(1) 的新功能

发布时间：**2017** 年 **12** 月 **4** 日

功能	说明
防火墙功能	
Ethertype 访问控制列表更改	EtherType 访问控制列表现在支持以太网 II IPX (EII IPX)。此外，在 DSAP 关键字中增加了新关键字，以支持通用 DSAP 值：BPDU (0x42)、IPX (0xE0)、Raw IPX (0xFF) 和 ISIS (0xFE)。因此，现有的使用 BPDU 或 ISIS 关键字的 EtherType 访问控制条目将被自动转换为使用 DSAP 规范，并且 IPX 的规则将被转换为 3 条规则（DSAP IPX、DSAP Raw IPX 和 EII IPX）。此外，使用 IPX 作为 EtherType 值的数据包捕获已被弃用，因为 IPX 对应于 3 个单独的 EtherType。 新增或修改的命令：**access-list ethertype** 添加了新的关键字 **eii-ipx** 和 **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}；**capture ethernet-type** 不再支持关键字 **ipx**。 新增或修改的菜单项：**配置** > **防火墙** > **Ethertype 规则**。
VPN 功能	

功能	说明
通过 Firepower 9300 上的集群支持分布式站点到站点 VPN	Firepower 9300 上的 ASA 集群在分布式模式下支持站点到站点 VPN。通过分布式模式，可以实现跨 ASA 集群成员分布的许多站点间 IPSec IKEv2 VPN 连接，而不只是在主设备上实现（在集中式模式下）。这将在集中式 VPN 功能的基础上大幅扩展 VPN 支持，并提供高可用性。分布式站点间 VPN 在最多由两个机箱组成的集群上运行，每个机箱最多包含三个模块（集群成员总共包含六个），每个模块最多支持 6K 个活动会话（总共 12K 个），最多支持大约 36K 个活动会话（总共 72K 个）。 新增或修改的命令：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2** 新增或修改的菜单项： **监控 > ASA 集群 > ASA 集群 > VPN 集群摘要** **监控 > VPN > VPN 统计信息 > 会话 > 从属** **配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群** **向导 > 站点到站点** **监控 > VPN > VPN 统计信息 > 会话** **监控 > ASA 集群 > ASA 集群 > VPN 集群摘要** **监控 > ASA 集群 > ASA 集群 > 系统资源图 > CPU/内存** **监控 > 日志记录 > 实时日志查看器**
高可用性和扩展性功能	
Microsoft Azure 中 ASAv 的主用/备份高可用性	无状态主用/备份解决方案，允许主用 ASAv 故障触发系统自动执行故障切换到 Microsoft Azure 公共云中的备份 ASAv。 新增或修改的命令：**failover cloud** 新增或修改的菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换** **监控 > 属性 > 故障切换 > 状态** **监控 > 属性 > 故障切换 > 历史记录** 同样适用于 *9.8(1.200)* 中。
改进了 Firepower 机箱运行状况检查故障检测	现在，您可以为机箱运行状况检查配置较低的保持时间：100 毫秒。以前的最小值为 300 毫秒。 新增或修改的命令：**app-agent heartbeat interval** 无 ASDM 支持。

功能	说明
站点间集群冗余	站点间冗余可确保流量的备份所有者将始终位于不同于该所有者的另一站点。此功能可防范站点发生故障。 新增或修改的命令：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag** 新增或修改的菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**
监控和故障排除功能	
增强了数据包跟踪器和数据包捕获功能	数据包跟踪器通过以下功能得到增强： • 在集群设备之间传递数据包时跟踪该数据包。 • 允许模拟数据包传出 ASA。 • 绕过对模拟数据包的安全检查。 • 将模拟数据包视为 IPSec/SSL 解密数据包。 数据包捕获通过以下功能得到增强： • 在解密后捕获数据包。 • 捕获跟踪并将其保留在永久列表中。 新增或修改的命令：**cluster exec capture test trace include-decrypted**、**cluster exec capture test trace persist**、**cluster exec clear packet-tracer**、**cluster exec show packet-tracer id**、**cluster exec show packet-tracer origin**、**packet-tracer persist**、**packet-tracer transmit**、**packet-tracer decrypted**、**packet-tracer bypass-checks** 新增或修改的菜单项： **工具** > **数据包跟踪器** 添加了**集群捕获**字段以支持以下选项：**解密**、**保持**、**绕行检查**、**传输** 在**所有会话**下拉列表下面的**筛选依据**视图中添加了两个新选项：**来源**和**来源 ID** **监控** > **VPN** > **VPN 统计信息** > **数据包跟踪器和捕获** 在“数据包捕获向导”菜单项中添加了 **ICMP 捕获**字段：**向导** > **数据包捕获向导** 添加了两个选项**包括已解密**和**保持**，以支持 ICMP 捕获。

版本 9.8 的新功能

ASA 9.8(3)/ASDM 7.9(2.152) 的新功能

发布日期：**2018** 年 **7** 月 **2** 日

功能	说明
平台功能	
现在，Firepower 2100 主用 LED 在备用模式下点亮琥珀色指示灯	以前，主用指示灯在备用模式下处于未点亮状态。
防火墙功能	
支持从直接转发代理登录页面删除注销按钮。	如果您配置直接转发代理获取用户身份信息（AAA 身份验证侦听器），您现在可以从页面中删除注销按钮。这在用户从 NAT 设备后面连接并且无法按 IP 地址进行区分的情况下非常有用。当一个用户注销时，它会注销该 IP 地址的所有用户。 新增/修改的命令：**aaa authentication listener no-logout-button**。 无 ASDM 支持。
Trustsec SXP 连接可配置删除抑制计时器	默认 SXP 连接抑制计时器为 120 秒。现在，您可以配置此计时器，范围介于 120 到 64000 秒之间。 新增/修改的命令：**cts sxp delete-hold-down period**、**show cts sxp connection brief** 和 **show cts sxp connections**。 无 ASDM 支持。
VPN 功能	
支持传统 SAML 身份验证	如果您部署的 ASA 包含对 CSCvg65072 的修复，则默认的 SAML 行为是使用嵌入式浏览器，而这在 AnyConnect 4.4 或 4.5 上不受支持。因此，要继续使用 AnyConnect 4.4 或 4.5，您必须启用传统外部浏览器 SAML 身份验证方法。由于安全限制，只能将此选项用作迁移至 AnyConnect 4.6 的临时计划的一部分。此选项在近期将会弃用。 新增/修改的命令：**saml external-browser** 新建/修改的菜单项： **配置** > **远程访问 VPN** > **网络（客户端）访问** > **AnyConnect 连接配置文件**页面 > **连接配置文件**区域 > **添加**按钮 > **添加 AnyConnect 连接配置文件**对话框 **配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **连接配置文件** > 页面 > **连接配置文件**区域 > **添加**按钮 > **添加无客户端 SSL VPN 连接配置文件**对话框 新增/修改的选项：**SAML 外部浏览器**复选框

ASDM 7.8(2.151) 的新功能

发布时间：**2017** 年 **10** 月 **12** 日

功能	说明
防火墙功能	
Ethertype 访问控制列表更改	EtherType 访问控制列表现在支持以太网 II IPX (EII IPX)。此外，在 DSAP 关键字中增加了新关键字，以支持通用 DSAP 值：BPDU (0x42)、IPX (0xE0)、Raw IPX (0xFF) 和 ISIS (0xFE)。因此，现有的使用 BPDU 或 ISIS 关键字的 EtherType 访问控制条目将被自动转换为使用 DSAP 规范，并且 IPX 的规则将被转换为 3 条规则（DSAP IPX、DSAP Raw IPX 和 EII IPX）。此外，使用 IPX 作为 EtherType 值的数据包捕获已被弃用，因为 IPX 对应于 3 个单独的 EtherType。 9.8(2.9) 和其他临时版本中支持此功能。有关详细信息，请参阅 CSCvf57908。 修改了以下命令：**access-list ethertype** 添加了新的关键字 **eii-ipx** 和 **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}；**capture ethernet-type** 不再支持关键字 **ipx**。 修改了以下菜单项：**配置** > **防火墙** > **Ethertype 规则**。

ASA 9.8(2)/ASDM 7.8(2) 的新功能

发布日期：**2017** 年 **8** 月 **28** 日

功能	说明
平台功能	
适用于 Firepower 2100 系列的 ASA	引入了适用于 Firepower 2110、2120、2130 和 2140 的 ASA。与 Firepower 4100 和 9300 类似，Firepower 2100 运行基本 FXOS 操作系统，然后作为一项应用运行 ASA 操作系统。与 Firepower 4100 和 9300 相比，Firepower 2100 实施可以将 FXOS 更紧密地与 ASA 结合起来（精简了 FXOS 功能、单个设备映像捆绑包、对 ASA 和 FXOS 的简易管理访问）。 FXOS 拥有适用于接口的配置硬件设置，包括创建 EtherChannel 以及 NTP 服务、硬件监控和其他基本功能。您可以使用 Firepower 机箱管理器或 FXOS CLI 进行此配置。ASA 拥有其他所有功能，包括智能许可（不同于 Firepower 4100 和 9300）。ASA 和 FXOS 在管理1/1 接口上都有自己的 IP 地址，您可以从任何数据接口配置 ASA 和 FXOS 实例的管理。 引入了以下命令：**connect fxos**、**fxos https**、**fxos snmp**、**fxos ssh**、**ip-client** 引入了以下菜单项： **配置** > **设备管理** > **管理访问** > **FXOS 远程管理**

功能	说明
美国国防部统一功能批准的产品列表	更新了 ASA，以满足统一功能批准的产品列表 (UC APL) 要求。在此版本中，输入 **fips enable** 命令时，ASA 将重新加载。在启用故障切换之前，两个故障切换对必须处于相同的 FIPS 模式下。 修改了以下命令：**fips enable**
ASAv 对 Amazon Web Services M4 实例的支持	现在，可以将 ASAv 作为 M4 实例部署。 未修改任何命令。 未修改任何菜单项。
ASAv5 1.5 GB RAM 功能	从版本 9.7(1) 开始，ASAv5 可能会遇到内存耗尽的情况，这样，某些功能（如启用 AnyConnect 或将文件下载到 ASAv）会失败。现在，您可以将 1.5 GB（从 1 GB 开始增加）的 RAM 分配给 ASAv5。 未修改任何命令。 未修改任何菜单项。
VPN 功能	
HTTP 严格传输安全 (HSTS) 信头支持	HSTS 可保护网站免受协议降级攻击和无客户端 SSL VPN 上的 cookie 劫持。它允许 Web 服务器声明网络浏览器（或其他随附的用户代理）只应使用安全的 HTTPS 连接与它进行交互，而不能通过不安全的 HTTP 协议。HSTS 是 IETF 标准跟踪协议，在 RFC 6797 中指定。 引入了以下命令：**hsts enable, hsts max-age** *age_in_seconds* 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 代理**
接口功能	
ASAv50 对 VLAN 的支持	现在，ASAv50 在 SR-IOV 接口的 ixgbe-vf vNIC 上支持 VLAN。 未修改任何命令。 未修改任何菜单项。

ASA 9.8(1.200) 的新功能

发布日期：2017 年 7 月 30 日

注释 此版本仅在 Microsoft Azure 的 ASAv 上受支持。这些功能在版本 9.8(2) 中不受支持。

功能	说明
高可用性和扩展性功能	
Microsoft Azure 中 ASAv 的主用/备份高可用性	无状态主用/备份解决方案，允许主用 ASAv 故障触发系统自动执行故障切换到 Microsoft Azure 公共云中的备份 ASAv。 引入了以下命令：**failover cloud** 无 ASDM 支持。

ASDM 7.8(1.150) 的新功能

发布日期：**2017** 年 **6** 月 **20** 日

此版本中无新增功能。

ASA 9.8(1)/ASDM 7.8(1) 的新功能

发布日期：2017 年 5 月 15 日

功能	说明
平台功能	
ASAv50 平台	ASAv 虚拟平台添加了高端性能 ASAv50 平台，该平板台提供了 10 Gbps 防火墙吞吐量级别。ASAv50 需要仅在 Vmware 和 KVM 上受支持的 ixgbe-vf vNIC。
ASAv 平台上的 SR-IOV	ASAv 虚拟平台支持单个根 I/O 虚拟化 (SR-IOV) 接口，允许多个虚拟机共享主机内的一个 PCIe 网络适配器。ASAv SR-IOV 支持仅在 VMware、KVM 和 AWS 上提供。
ASAv 现在支持自动 ASP 负载均衡	过去只能手动启用和禁用 ASP 负载均衡。 修改了以下命令：**asp load-balance per-packet auto** 修改了以下菜单项：**配置 > 设备管理 > 高级 > ASP 负载均衡**
防火墙功能	
支持设置 TLS 代理服务器 SSL 密码套件	现在可在 ASA 作为 TLS 代理服务器时设置 SSL 密码套件。过去，您只能在**配置** > **设备管理** > **高级** > **SSL 设置** > **加密**页面中使用 **ssl cipher** 命令为 ASA 设置全局设置。 引入了以下命令：**server cipher-suite** 修改了以下菜单项：**配置** > **防火墙** > **统一通信** > **TLS 代理**、“添加/编辑”对话框、**服务器配置**页面。

功能	说明
ICMP 的全局超时错误	现在可以设置 ASA 在 接收 ICMP echo-reply 数据包后后、删除 ICMP 连接之前的空闲时间。如果禁用了此超时（默认），并且启用了 ICMP 检查，则 ASA 将在接收 echo-reply 后立即删除 ICMP 连接；因此将丢弃为该连接（现已关闭）生成的任何 ICMP 错误。此超时可以延迟删除 ICMP 连接，使您能够接收重要的 ICMP 错误。 添加了以下命令：**timeout icmp-error** 修改了以下菜单项：**配置** > **防火墙** > **高级** > **全局超时**。
高可用性和扩展性功能	
改进了集群设备运行状态检查故障检测	现在可为设备运行状态检查配置更短的保持时间：最小值为 0.3 秒。过去的最小值为 0.8 秒。此功能可将设备运行状态检查消息传递方案从控制平面中的 *keepalives* 更改为数据平面中的 *heartbeats*。使用心跳设置可改进集群的可靠性和响应能力，使其不易受控制平面 CPU 占用和调度延迟所影响。请注意，配置较低的保持时间值会增加集群控制链路消息活动。我们建议您在配置低保持时间值之前先分析网络状况；例如，确保在保持时间/3 范围内通过集群控制链路返回从一台设备到另一台设备的 ping，因为在一个保持时间间隔内有三次心跳消息。如果在将保持时间设置为 0.3 - 0.7 后对 ASA 软件降级，则此设置将恢复为默认的 3 秒，因为新设置不受支持。 修改了以下命令：**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details** 修改了以下菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**
Firepower 4100/9300 机箱可配置防反跳时间，以将接口标记为发生故障	您现在可以配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。此功能可以加快接口故障检测的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。默认的防反跳时间是 500 毫秒，该时间的范围是 300 毫秒至 9 秒。 新增或修改的命令：**health-check monitor-interface debounce-time** 新增或修改的菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**
VPN 功能	
VTI 中支持 IKEv2、基于证书的身份验证和 ACL	虚拟隧道接口 (VTI) 现在支持 BGP（静态 VTI）。现在可在独立和高可用性模式下使用 IKEv2。可以通过在 IPsec 配置文件中设置信任点来使用基于证书的身份验证。还可以使用 access-group 命令，将 VTI 上的访问列表应用于过滤入口流量。 在 IPsec 配置文件配置模式下引入了以下命令：**set trustpoint**。 在以下屏幕中引入了几个选项，用于为基于证书的身份验证选择信任点： **配置** > **站点到站点 VPN** > **高级** > **IPSec 协议（转换集）** > **IPSec 配置文件** > **添加**

功能	说明
默认情况下，将启用移动 IKEv2 (MobIKE)	作为远程访问客户端运行的移动设备在移动时需要透明 IP 地址更改。ASA 上支持 MobIKE 可以不必删除当前的安全关联 (SA) 即可更新当前的 IKE SA。MobIKE 为“始终开启”。 引入了以下命令：**ikev2 mobike-rrc**。用于启用/禁用返回路由能力检查。
SAML 2.0 SSO 更新	SAML 请求中签名的默认签名方法从 SHA1 更改为 SHA2，并且可以配置首选哪种签名方法：rsa-sha1、rsa-sha256、rsa-sha384 或 rsa-sha512。 更改了 webvpn 模式下的以下命令：可以使用值来配置 **saml idp signature**。默认设置仍为“禁用”。 我们对以下菜单项进行了更改：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 单点登录服务器 > 添加**。
tunnelgroup webvpn-attributes 的更改	将 pre-fill-username 和 secondary-pre-fill-username 值从 *clientless* 更改为了 *client*。 我们在 webvpn 模式下更改了以下命令：**pre-fill-username** 和 **secondary-pre-fill-username** 可以使用 *client* 值配置。
AAA 功能	
登录历史	默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多 365 天。仅当为一种或多种管理方法（SSH、ASDM、Telnet 等）启用本地 AAA 身份验证时，此功能才适用于本地数据库中的用户名。 引入了以下命令：**aaa authentication login-history**、**show aaa login-history** 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 登录历史记录**
禁止重复使用密码以及禁止使用与某一用户名匹配的密码的密码策略实施	现在，可以禁止重复使用过去的密码（最多 7 代），还可以禁止使用与某一用户名匹配的密码。 引入了以下命令：**password-history**、**password-policy reuse-interval**、**password-policy username-check** 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 密码策略**

功能	说明
对使用 SSH 公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必明确启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。 未修改任何菜单项。 同样适用于 *9.6(3)* 版本。
监控和故障排除功能	
在 ASA 崩溃时保存当前运行的数据包捕获	过去，如果 ASA 崩溃，则活动数据包捕获将丢失。现在，在崩溃时会使用文件名 [*context_name*.]*capture_name*.**pcap** 将数据包捕获保存到磁盘 0。 未修改任何命令。 未修改任何菜单项。

版本 9.7 的新功能

ASDM 7.7(1.151) 的新功能

发布日期：2017 年 4 月 28 日

注释 由于错误 CSCvd90344，已从 Cisco.com 中删除 ASDM 7.7(1.150)。

功能	说明
管理功能	
ASDM 升级工具的新后台服务	ASDM 为**工具 > 检查 ASA/ASDM 升级**使用新后台服务。未来，思科会终止 ASDM 早期版本使用的旧版服务。

ASA 9.7(1.4)/ASDM 7.7(1) 中的新功能

发布日期：2017 年 4 月 4 日

注释 由于错误 CSCvd78303，已从 Cisco.com 删除了版本 9.7(1)。

功能	说明
平台功能	
使用集成路由和桥接的 ASA 5506-X 系列的新默认配置	ASA 5506-X 系列 将使用一种新默认配置。集成桥接和路由功能为使用外部第 2 层交换机提供了一种替代方法。对于替换 ASA 5505（其中包含硬件交换机）的用户，无需使用其他硬件即可借助此功能将 ASA 5505 替换为 ASA 5506-X 或其他 ASA 型号。 新默认配置包括： • 千兆以太网 1/1 上的外部接口、来自 DHCP 的 IP 地址 • 内部网桥组 BVI 1，包含 GigabitEthernet ½ (inside1) 至 1/8 (inside7)，IP地址 192.168.1.1 • 内部 --> 外部流量 • 内部 ---> 内部流量（成员接口） • (ASA 5506W-X) 千兆以太网 1/9 上的 wifi 接口、IP 地址 192.168.10.1 • (ASA 5506W-X) WiFi <--> 内部，WiFi --> 外部流量 • 内部和 wifi 上的客户端的 DHCP 接入点本身及其所有客户端均使用 ASA 作为 DHCP 服务器。 • Management 1/1 接口启用，但未进行其他配置。ASA FirePOWER 模块随后可以使用此接口接入 ASA 内部网络，并将内部接口用作通向互联网的网关。 • ASDM 接入 - 允许内部和 wifi 主机。 • NAT - 从内部、wifi 和管理到外部的所有流量的接口 PAT。 若要升级，您可以使用 **configure factory-default** 命令清除配置并应用默认值，也可以手动配置BVI和网桥组来满足需求。请注意，要使网桥组内能够轻松地进行通信，您需要启用 **same-security-traffic permit inter-interface** 命令（对于 ASA 5506W-X 默认配置，此命令已存在）。

功能	说明
ISA 3000 上支持报警端口	ISA 3000 支持两个报警输入接口和一个报警输出接口。外部传感器（如门禁传感器）可以连接到报警输入。可以将蜂音器等外部设备连接到报警输出接口。触发的报警通过两个 LED、系统日志、SNMP 陷阱以及连接到报警输出接口的设备传达。您可以配置外部报警说明。另外，也可以指定外部和内部报警的严重性和触发器。可为中继、监控和日志记录配置各种报警。 引入了以下命令：**alarm contact description**、**alarm contact severity**、**alarm contact trigger**、**alarm facility input-alarm**、**alarm facility power-supply rps**、**alarm facility temperature**、**alarm facility temperature high**、**alarm facility temperature low**、**clear configure alarm**、**clear facility-alarm output**、**show alarm settings**、**show environment alarm-contact**。 引入了以下菜单项： **配置 > 设备管理 > 警报端口 > 报警触点** **配置 > 设备管理 > 警报端口 > 冗余电源** **配置 > 设备管理 > 警报端口 > 温度** **监控 > 属性 > 警报 > 警报设置** **监控 > 属性 > 警报 > 报警触点** **监控 > 属性 > 警报 > 设施警报状态**
ASAv10 上的 Microsoft Azure 安全中心支持	Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。Microsoft Azure 安全中心是在 Azure 之上的 Microsoft 协调和管理层，可以简化高度安全的公共云基础设施的部署。通过将 ASAv 集成到 Azure 安全中心，系统可以作为防火墙选项来提供 ASAv 以保护 Azure 环境。

ISA 3000 的精确时间协议 (PTP)	ISA 3000 支持 PTP，它是用于某一网络中分布的各个节点的时间同步协议。由于该协议具有硬件时间戳功能，因此它可以提供比其他时间同步协议（如 NTP）更高的精确度。ISA 3000 支持 PTP 转发模式，以及单步、端到端透明时钟。我们向默认配置添加了以下命令，以确保不会将 PTP 流量发送到 ASA FirePOWER 模块进行检查。如果您有现有部署，则需手动添加这些命令：
	
	`object-group service bypass_sfr_inspect`
	`  service-object udp destination range 319 320`
	`access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any`
	
	引入了以下命令：**debug ptp**、**ptp domain**、**ptp mode e2etransparent**、**ptp enable**、**show ptp clock**、**show ptp internal-info**、**show ptp port**
	
	引入了以下菜单项：
	
	配置 > 设备管理 > PTP
	
	监控 > 属性 > PTP

功能	说明
ISA 3000 的自动备份和自动恢复	可以使用 pre-set parameters in the backup 和 restore 命令中的预设参数来启用自动备份和/或自动恢复功能。这些功能的使用情形包括从外部介质的初始配置；设备更换；回滚到某一可操作状态。 引入了以下命令：**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary** 无 ASDM 支持。
防火墙功能	
支持 SCTP 多流重新排序、重组和分段。支持 SCTP 多宿主，其中 SCTP 终端具有一个以上的 IP 地址。	现在，系统完全支持 SCTP 多流重新排序、重组和分段，由此改善了 SCTP 流量的 Diameter 和 M3UA 检测效果。该系统还支持 SCTP 多宿主，其中每个 SCTP 终端都有一个以上的 IP 地址。对于多宿主，该系统可以打开辅助地址的针孔，使您无需编写访问规则即可允许它们访问。必须将每个 SCTP 终端限制为 3 个 IP 地址。 修改了以下命令的输出：**show sctp detail**。 未修改任何菜单项。
改进了 M3UA 检查。	M3UA 检查现在支持状态化故障切换、半分布式集群和多宿主。另外，您还可以配置严格应用服务器进程 (ASP) 状态验证和各种消息验证。对于状态故障切换和集群，需要使用严格 ASP 状态验证。 添加或修改了以下命令：**clear service-policy inspect m3ua session** [**assocID** *id*]、**match port sctp**、**message-tag-validation**、**show service-policy inspect m3ua drop**、**show service-policy inspect m3ua endpoint**、**show service-policy inspect m3ua session**、**show service-policy inspect m3ua table**、**strict-asp-state**、**timeout session**。 修改了以下菜单项：**配置** > **防火墙** > **对象** > **检测映射** > **M3UA**“添加/编辑”对话框。
TLS 代理和思科统一通信管理器 10.5.2 中支持 TLSv1.2。	现在，您可以将包含 TLS 代理的 TLSv1.2 与思科 Unified Communications Manager 10.5.2 一起用于加密 SIP 或 SCCP 检查。TLS 代理支持作为 **client cipher-suite** 命令的一部分添加的附加 TLSv1.2 密码套件。 修改了以下命令：**client cipher-suite** 未修改任何菜单项。

功能	说明
集成路由和桥接	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指ASA桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn** 修改了以下菜单项： **配置** > **设备设置** > **接口设置** > **接口** **配置** > **设备设置** > **路由** > **静态路由** **配置** > **设备管理** > **DHCP** > **DHCP 服务器** **配置** > **防火墙** > **访问规则** **配置** > **防火墙** > **EtherType 规则**
VM 属性	您可以根据与 VMware vCenter 管理的 VMware ESXi 环境中的一个或多个虚拟机 (VM) 相关联的属性来定义网络对象，以筛选流量。您可以定义访问控制列表 (ACL)，以便将策略分配给来自共享一项或多项属性的 VM 组的流量。 添加了以下命令：**show attribute**。 添加了以下菜单项： **配置** > **防火墙** > **VM 属性代理**
内部网关协议的过时路由超时	现在您可以配置超时，用于删除内部网关协议（如 OSPF）的陈旧路由。 添加了以下命令：**timeout igp stale-route**。 修改了以下菜单项：**配置** > **防火墙** > **高级** > **全局超时**。

功能	说明
对象组搜索的网络对象限制。	您可以使用 **object-group-search access-control** 命令来进行对象组搜索，以减少搜索访问规则所需的内存。已启用的对象组搜索不会展开网络或服务对象，而是根据这些组定义搜索匹配的访问规则。 从此版本开始，设备将添加以下限制：对于每个连接，源和目标IP地址将根据网络对象进行匹配。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过10,000，则丢弃连接。 此检查是为了防止性能降低。配置规则以防止过多的匹配项。
路由功能	
31 位子网掩码	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障切换链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。网桥组或组播路由的 BVI 不支持此功能。 修改了以下命令：**ip address**、**http**、**logging host**、**snmp-server host**、**ssh** 修改了以下菜单项： **配置** > **设备设置** > **接口设置** > **接口** > **添加接口** > **通用**
高可用性和扩展性功能	
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱 配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 修改了以下命令：**site-id** 修改了以下菜单项：**配置** > **设备管理** > **高可用性和扩展性** > **ASA 集群** > **集群配置**
导向器本地化：数据中心的站点间集群改进	为了提高性能和将流量保存在数据中心站点间集群的某个站点内，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。 引入或修改了以下命令：**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail** 修改了以下菜单项：**配置** > **设备管理** > **高可用性和扩展性** > **ASA 集群** > **集群配置**

功能	说明
现在，可为故障切换配置接口链路状态监控轮询以加快检测速度	默认情况下，故障切换对中的每个 ASA 都会每隔 500 毫秒检查一次其接口的链接状态。现在，您可以在 300 毫秒和 799 毫秒之间配置轮询间隔；例如，如果将轮询时间设置为 300 毫秒，ASA 则可以更快地检测接口故障并触发故障切换。 引入了以下命令：**failover polltime link-state** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 标准**
Firepower 9300 和 4100 上支持使用双向转发检测 (BFD) 进行主用/备用故障切换运行状况监控	您可以针对 Firepower 9300 和 4100 上主用/备用对两台设备之间的故障切换运行状况检查启用双向转发检测 (BFD)。将 BFD 用于运行状况检查比默认健康检查方法更可靠，并且 CPU 占用更少。 引入了以下命令：**failover health-check bfd** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 设置**
VPN 功能	
用于 IKEv2 静态加密映射的动态 RRI	如果为 **crypto map** 指定 **dynamic**，在成功建立 IPSec 安全关联 (SA) 后将发生动态反向路由注入。根据商定的选择器信息添加路由。在删除 IPSec SA 后，这些路由会被删除。仅在基于静态加密映射的 IKEv2 上支持动态 RRI。 修改了以下命令：**crypto map set reverse-route**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 加密映射 > 添加/编辑 > 隧道策略（加密映射）- 高级**
ASA VPN 模块支持虚拟隧道接口 (VTI)	使用新的逻辑接口（称为“虚拟隧道接口 (VTI)”）可增强 ASA VPN 模块，该接口用于向对等体表示 VPN 隧道。这可通过将 IPSec 配置文件连接到隧道的每一端，为基于 VPN 的路由提供支持。使用 VTI 将不再需要配置静态加密映射访问列表并将其映射到接口。 引入了以下命令：**crypto ipsec profile**、**interface tunnel**、**responder-only**、**set ikev1 transform-set**、**set pfs**、**set security-association lifetime**、**tunnel destination**、**tunnel mode ipsec**、**tunnel protection ipsec profile**、**tunnel source interface**。 引入了以下菜单项： **配置 > 站点到站点 VPN > 高级 > IPSec 协议（转换集） > IPSec 配置文件** **配置 > 站点到站点 VPN > 高级 > IPSec 协议（转换集） > IPSec 配置文件 > 添加 > 添加 IPSec 配置文件** **配置 > 设备设置 > 接口设置 > 接口 > 添加 > VTI 接口** **配置 > 设备设置 > 接口设置 > 接口 > 添加 > VTI 接口 > 通用** **配置 > 设备设置 > 接口设置 > 接口 > 添加 > VTI 接口 > 高级**

功能	说明
用于 AnyConnect 的基于 SAML 2.0 的 SSO	在专用网络中支持基于 SAML 2.0 的服务提供商 IdP。使用 ASA 作为用户与服务之间的网关，可利用受限的匿名 webvpn 会话来处理 IdP 上的身份验证，并转换 IdP 与用户之间的所有流量。 添加了以下命令：**saml idp** 修改了以下命令：**debug webvpn saml**、**show saml metadata** 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 单点登录服务器 > 添加 SSO 服务器**。
CMPv2	为了在无线 LET 网络中担当安全网关设备，ASA 现在支持使用证书管理协议 (CMPv2) 的某些管理功能。 修改了以下命令：**enrollment url**、**keypair**、**auto-update**、**crypto-ca-trustpoint**、**show crypto ca server certificates**、**show crypto key**、**show tech-support** 修改了以下菜单项：**配置 > 远程访问 VPN > 证书管理 > 身份证书 > 添加身份证书**
多证书身份验证	现在，您可以使用 AnyConnect SSL 和 IKEv2 客户端协议验证每个会话的多重证书。我们对汇聚身份验证协议进行了扩展，以便定义用于多证书身份验证的协议交换并将此功能用于两种会话类型。 修改了以下命令：**authentication {[aaa] [certificate | multiple-certificate] | saml}** 修改了以下菜单项： **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 编辑 AnyConnect 连接配置文件** **配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件 > 编辑 AnyConnect 连接配置文件**
增加隧道拆分路由限制	AC-SSL 和 AC-IKEv2 的隧道拆分路由限制从 200 增至 1200。IKEv1 限值仍为 200。
Chrome 上的智能隧道支持	现已创建了一种新方法，用于 Mac 和 Windows 设备上的 Chrome 浏览器中的智能隧道支持。Chrome 智能隧道扩展 (Chrome Smart Tunnel Extension) 取代了 Chrome 中不再支持的 Netscape 插件应用程序编程接口 (NPAPI)。如果您在没有安装该扩展的情况下点击了 Chrome 中启用了智能隧道的书签，则系统会将您重定向到 Chrome 网上应用店以获取该扩展。新的 Chrome 安装会将用户定向到 Chrome 网上应用店以下载该扩展。该扩展将从 ASA 下载运行智能隧道所需的二进制文件。除安装新扩展的进程之外，使用智能隧道时，常规书签和应用程序配置均不会改变。
无客户端 SSL VPN：所有 Web 界面的会话信息	现在，所有 Web 界面都会显示当前会话的详情，包括用于登录的用户名，以及当前分配的用户权限。这让用户可以了解当前用户会话，还可提高用户的安全性。
无客户端 SSL VPN：Web 应用会话的所有 cookie 的验证	现在，所有 Web 应用都将仅在验证所有与安全相关的 cookie 后才会授予访问权限。在每次请求中，都会在向用户会话授予访问权限之前验证每个具有身份验证令牌或会话 ID 的 cookie。如果同一个请求中有多个会话 cookie，将导致该连接被丢弃。验证失败的 cookie 将被视为无效，并会将该事件添加到审核日志。

功能	说明
AnyConnect：现在，AnyConnect VPN 客户端连接的组策略中支持最大连接时间警告间隔。	警告间隔是达到最大连接时间之前的时间间隔，系统会向用户显示一条消息，提示他们连接将被终止。有效的时间间隔为 1-30 分钟。默认值为 30 分钟。以前无客户端和站点间 VPN 连接支持此功能。 现在，以下命令可以用于 AnyConnect 连接：**vpn-session-timeout alert-interval** 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑 > 通用 > 更多选项**，添加了**最大连接时间警报间隔**字段
AAA 功能	
用于 AAA 的 LDAP 和 TACACS+ 服务器支持 IPv6 地址	现在，您可以将 IPv4 或 IPv6 地址用于 LDAP 和 TACACS+ 服务器（用于 AAA）。 修改了以下命令：**aaa-server host**、**test aaa-server** 修改了以下菜单项：**配置 > 设备管理 > 用户/AAA > AAA 服务器组 > 添加 AAA 服务器组**
管理功能	
对所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列算法	配置中存储的所有长度的本地 **username** 和 **enable** 密码都将使用 PBKDF2 (基于密码的密钥派生函数 2) 散列算法。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于MD5的哈希值，但您输入的新密码除外。如需下载指南，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下命令：**enable password**、**username** 修改了以下菜单项： **配置 > 设备设置 > 设备名称/密码 > 启用密码** **配置 > 设备管理 > 用户/AAA > 用户账户 > 添加/编辑用户账户 > 身份**
许可功能	
Firepower 4100/9300 机箱 上的故障切换对的许可变化	只有主用单元能够请求许可权利。过去，两种设备都需请求许可证授权。支持 FXOS 2.1.1。
监控和故障排除功能	
traceroute 支持 IPv6 地址	**traceroute** 命令已修改为接受 IPv6 地址。 修改了以下命令：**traceroute** 修改了以下菜单项：**工具 > Traceroute**
对于网桥组成员接口，支持使用 Packet Tracer	现在，对于网桥组成员接口可以使用 Packet Tracer。 我们为 **packet-tracer** 命令添加了两个新选项：**vlan-id** 和 **dmac** 在 packet-tracer 菜单项“**工具 > 数据包跟踪器**”中添加了 **VLAN ID** 和**目标 MAC 地址**字段

功能	说明
系统日志服务器支持 IPv6 地址	现在，您可以使用 IPv6 地址来配置系统日志服务器，以便通过 TCP 和 UDP 记录和发送系统日志。 修改了以下命令：**logging host**、**show running config**、**show logging** 修改了以下菜单项：**配置** > **设备管理** > **日志记录** > **系统日志服务器** > **添加系统日志服务器**
SNMP OID 和 MIB	作为 ISA 3000 的精确时间协议 (PTP) 的组成部分，ASA 现在支持对应于端到端透明时钟模式的 SNMP MIB 对象支持以下SNMP MIB 对象： • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable
手动停止和启动数据包捕获	您现在可以手动停止和开始捕获。 添加/修改的命令：**capture stop** 添加/修改的菜单项：**向导** > **数据包捕获向导** > **运行捕获** 添加/修改的选项：**开始**按钮、**停止**按钮

版本 9.6 的新功能

ASA 9.6(4)/ASDM 7.9(1) 的新功能

发布时间：**2017** 年 **12** 月 **13** 日

此版本中无新增功能。

ASA 9.6(3.1)/ASDM 7.7(1) 的新功能

发布日期：**2017** 年 **4** 月 **3** 日

注释 由于错误 CSCvd78303，已从 Cisco.com 删除了版本 9.6(3)。

功能	说明
AAA 功能	

功能	说明
对使用 SSH 公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必明确启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。 未修改任何菜单项。 同样适用于 *9.8(1)* 版本。

ASDM 7.6(2.150) 的新功能

发布时间：2016 年 10 月 12 日

此版本中无新增功能。

ASA 9.6(2)/ASDM 7.6(2) 的新功能

发布日期：2016 年 8 月 24 日

功能	说明
平台功能	
用于 Firepower 4150 的 ASA	我们引入了用于 Firepower 4150 的 ASA。 需要 FXOS 2.0.1。 未添加或修改任何命令。 未修改任何菜单项。
ASAv 上的热插接口	当系统处于活动状态时，您可以在 ASAv 上添加和删除 Virtio 虚拟接口。当您将新接口添加到 ASAv 时，虚拟机会检测和调配该接口。当您删除现有接口时，虚拟机会释放与该接口关联的所有资源。热插接口仅限于在基于内核的虚拟机 (KVM) 虚拟机监控程序上的 Virtio 虚拟接口。

功能	说明
ASAv10 上提供 Microsoft Azure 支持	Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。ASAv 在 Hyper V 虚拟机监控程序的 Microsoft Azure 环境中充当访客。Microsoft Azure 上的 ASAv 支持一个实例类型，即标准 D3。标准 D3 可支持 4 个 vCPU、14 GB 内存和 4 个接口。 同样适用于 *9.5(2.200)*。
ASAv 的管理 0/0 接口上提供通过流量支持	现在，您可以在 ASAv 的管理 0/0 接口上允许通过流量。过去，仅 Microsoft Azure 上的 ASAv 支持通过流量；现在所有 ASAv 都支持通过流量。您可以选择将此接口配置为仅管理接口，但默认情况下，没有进行此配置。 修改了以下命令：**management-only**

通用标准认证	更新了 ASA，以满足通用标准要求。请参阅下表中的各行，了解下列为 UCR 2013 认证添加的功能：
	• ASDM 的 ASA SSL 服务器模式匹配
	• SSL 客户端 RFC 6125 支持：
	  • 安全系统日志服务器连接和智能许可连接的参考身份
	  • ASA 客户端会检查服务器证书中的“Extended Key Usage”
	  • 当 ASA 作为 TLS1.1 和 1.2 的 TLS 客户端时，进行相互身份验证
	• PKI 调试消息
	• 加密密钥归零验证
	• 对 IKEv2 的 IPSec/ESP 传输模式支持
	• 新的系统日志消息

防火墙功能	
DNS over TCP 检测	您现在可以检测 DNS over TCP 流量 (TCP/53)。 添加了以下命令：**tcp-inspection** 修改了以下页面：**配置** > **防火墙** > **对象** > **检查映射** > **DNS** 添加/编辑对话框

功能	说明
MTP3 用户适应性 (M3UA) 检测	现在，您可以检测M3UA流量，并根据点代码、服务指示器以及消息类和类型应用操作。 添加或修改了以下命令：**clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint** *IP_address*}、**ss7 variant** 和 **timeout endpoint** 对于服务策略规则，添加或修改了以下页面：**配置** > **防火墙** > **对象** > **检查映射** > **M3UA**；**规则行为** > **协议检查**选项卡
NAT (STUN) 检测的会话遍历实用程序	现在，您可以检测 WebRTC 应用程序的 STUN 流量，包括思科 Spark。检测会打开返回流量所需的针孔。 添加或修改了以下命令：**inspect stun**、**show conn detail** 和 **show service-policy inspect stun**。 向“添加/编辑服务策略”对话框的“规则行为”>“协议检查”选项卡添加了一个选项
思科云 Web 安全的应用层运行状况检查	现在，您可以配置思科云 Web 安全以在确定服务器是否正常时检查云 Web 安全应用的运行状况。通过检查应用运行状况，系统可以在主服务器响应TCP三向握手但无法处理请求时，故障切换到备用服务器。这可确保系统更加可靠。 添加了以下命令：**health-check application url** 和 **health-check application timeout**。 修改了以下菜单项：**配置** > **设备管理** > **云 Web 安全**
路由汇聚的连接抑制超时。	现在，您可以配置在连接使用的路由不再存在或不活动时，系统应保持连接的时间。如果路由在此抑制期间未变为活动状态，连接将被释放。您可以减小抑制计时器，使路由汇聚更快速地进行。但是，默认值 15 秒适合大多数网络，可以防止路由摆动。 添加了以下命令：**timeout conn-holddown** 修改了以下菜单项：**配置** > **防火墙** > **高级** > **全局超时** 同样适用于 *9.4(3)*。

功能	说明
TCP 选项处理的更改	现在，当配置 TCP 映射时，您可以在数据包的 TCP 报头中为 TCP MSS 和 MD5 选项指定操作。此外，对 MSS、timestamp、window-size 和 selective-ack 选项的默认处理已更改。以前，允许这些选项，即使报头中具有指定类型的多个选项也是如此。现在，默认情况下会丢弃包含指定类型的多个选项的数据包。例如，以前允许具有 2 个 timestamp 选项的数据包，而现在将丢弃该数据包。 您可以配置 TCP 映射，以针对 MD5、MSS、selective-ack、timestamp 和 window-size 允许同一类型的多个选项。对于 MD5 选项，以前的默认设置为清除该选项，而现在的默认设置是允许它。您还可以丢弃包含 MD5 选项的数据包。对于 MSS 选项，您可以在 TCP 映射中设置最大分段大小（每个流量类）。所有其他 TCP 选项的默认设置均保持不变：被清除。 修改了以下命令：**tcp-options** 修改了以下菜单项：**配置** > **防火墙** > **对象** > **TCP 映射**“添加/编辑”对话框
每个桥接组的透明模式最大接口数增加到 64	每个桥接组的最大接口数量已从 4 增加到 64。 未修改任何命令。 未修改任何菜单项。
透明模式下对组播连接的流量卸载支持。	现在，您可以卸载将在透明模式 Firepower 4100 和 9300 系列设备的网络接口卡中直接切换的组播连接。组播卸载仅适用于有且只有两个接口的网桥组。 对于此功能，没有新的命令或 ASDM 菜单项。
可自定义的 ARP 速率限制	您可以设置每秒允许的最大 ARP 数据包数。默认值取决于 ASA 型号。您可以自定义此值以防止 ARP 风暴攻击。 添加了以下命令：**arp rate-limit**、**show arp rate-limit** 修改了以下菜单项：**配置** > **设备管理** > **高级** > **ARP** > **ARP 静态表**
对于 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址的 Ethertype 规则支持。	现在，您可以为 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址编写 Ethertype 访问控制规则。添加此支持后，**bpdu** 关键字与预期流量不再匹配。我们重写了 **dsap 0x42** 的 **bpdu** 规则。 修改了以下命令：**access-list ethertype** 修改了以下菜单项：**配置** > **防火墙** > **EtherType 规则**。
远程访问功能	
多情景模式的 Pre-fill/Username-from-cert 功能	AnyConnect SSL 支持已扩展，允许 pre-fill/username-from-certificate 功能 CLI（以前其仅在单情景模式下可用）在多情景模式下也可启用。 未修改任何命令。 未修改任何菜单项。

功能	说明
使用闪存虚拟化实现远程访问 VPN	多情景模式下的远程访问 VPN 现在支持闪存虚拟化。每个情景都可以根据可用的总闪存拥有专用存储空间和共享存储位置： • 专用存储 - 仅存储与该用户关联且特定于您希望该用户具有的内容的文件。 • 共享存储 - 将文件上传到此空间，并且将其启用后，可供任何用户情景进行读/写访问。 引入了以下命令：**limit-resource storage**、**storage-url** 修改了以下菜单项：**配置 > 情景管理 > 资源类 > 添加资源类** **配置 > 情景管理 > 安全情景**
多情景模式下支持 AnyConnect 客户端配置文件	多情景模式下支持 AnyConnect 客户端配置文件。要使用 ASDM 添加新配置文件，您必须要有 AnyConnect 安全移动客户端版本 4.2.00748 或 4.3.03013 及更高版本。
多情景模式下 AnyConnect 连接的有状态故障切换	现在，多情景模式下 AnyConnect 连接支持有状态故障切换 未修改任何命令。 未修改任何菜单项。
多情景模式下支持远程访问 VPN 动态访问策略 (DAP)	现在，可以在多情景模式下按情景配置 DAP。 未修改任何命令。 未修改任何菜单项。
多情景模式下支持远程访问 VPN CoA（授权更改）	现在，可以在多情景模式下按情景配置 CoA。 未修改任何命令。 未修改任何菜单项。
多情景模式下支持远程访问 VPN 本地化	支持全局本地化。只有一组跨不同情景共享的本地化文件。 未修改任何命令。 未修改任何菜单项。
Umbrella 漫游安全模块支持	当没有 VPN 处于活动状态时，您可以选择配置 AnyConnect 安全移动客户端的 Umbrella 漫游安全模块，以获得额外的 DNS 层安全。 未修改任何命令。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 客户端配置文件**。

功能	说明
对 IKEv2 的 IPSec/ESP 传输模式支持	现在支持传输模式进行 ASA IKEv2 协商。它可用于替代隧道模式（默认设置）。隧道模式会封装整个 IP 数据包。传输模式只封装 IP 数据包的上层协议。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。 修改了以下命令：**crypto map set ikev2 mode** 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > IPSec 协议（转换集） > IKEv2 协议 > 添加/编辑**
IPsec 内部数据包的按数据包路由查找	默认情况下，按数据包邻接关系查找针对外部 ESP 数据包执行；不会对通过 IPsec 隧道发送的数据包执行查找。在某些网络拓扑中，路由更新更改了内部数据包的路径，但本地 IPsec 隧道仍正常运行时，通过隧道的数据包可能无法正确路由，且无法到达其目的地。要避免此情况，请使用新选项启用对 IPsec 内部数据包的按数据包路由查找功能。 添加了以下命令：**crypto ipsec inner-routing-lookup** 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 加密映射**添加**启用 IPSec 内部路由查找**复选框。
证书和安全连接功能	
ASA 客户端会检查服务器证书中的“Extended Key Usage”	系统日志与智能许可服务器证书必须在“Extended Key Usage”字段中包含“ServerAuth”。否则，连接会失败。
当 ASA 作为 TLS1.1 和 1.2 的 TLS 客户端时，进行相互身份验证	如果服务器从 ASA 请求客户端证书以进行身份验证，则 ASA 将发送为该接口配置的客户端身份证书。该证书通过 **ssl trust-point** 命令配置。
PKI 调试消息	ASA PKI 模块会与 CA 服务器建立连接，例如进行 SCEP 注册、使用 HTTP 进行撤销检查等。所有这些 ASA PKI 交换都将在 debug crypto ca message 5 下记录为调试跟踪。
ASDM 的 ASA SSL 服务器模式匹配	对于通过证书进行身份验证的 ASDM 用户，您现在可以要求证书与证书映射匹配。 修改了以下命令：**http authentication-certificate match** 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH**
安全系统日志服务器连接和智能许可连接的参考身份	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。身份验证将在 PKI 验证期间仅针对与系统日志服务器和智能许可服务器的 TLS 连接执行。如果所显示的身份无法与配置的参考身份匹配，则不会建立连接。 添加或修改了以下命令：**crypto ca reference-identity**、**logging host**、**call home profile destination address** 修改了以下菜单项： **配置 > 远程访问 VPN > 高级** **配置 > 设备管理 > 日志记录 > 系统日志服务器 > 添加/编辑** **配置 > 设备管理 > Smart Call Home**

功能	说明
加密密钥归零验证	ASA 加密系统已更新来符合新的密钥归零要求。密钥必须全部重写为零，然后必须读取数据以确认写入成功。
SSH 公钥身份验证改进	在更早的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下命令：**ssh authentication**、**username**。 修改了以下菜单项： **配置** > **设备管理** > **管理访问** > **ASDM/HTTPS/Telnet/SSH** **配置** > **设备管理** > **用户/AAA** > **用户账户** > **添加/编辑用户账户**
接口功能	
增加了 Firepower 4100/9300 机箱上 ASA 的 MTU 大小	可以在 Firepower 4100 和 9300 上将最大 MTU 设置为 9188 字节；以前，最大值为 9000 字节。FXOS 2.0.1.68 及更高版本中支持此 MTU。 修改了以下命令：**mtu** 修改了以下菜单项：**配置** > **设备设置** > **接口设置** > **接口** > **高级**
路由功能	
双向转发检测 (BFD) 支持	ASA 现在支持 BFD 路由协议。添加了对配置 BFD 模板、接口和映射的支持。还添加了对 BGP 路由协议使用 BFD 的支持。 添加或修改了以下命令：**authentication**、**bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd template**、**bfd-template**、**clear bfd counters**、**echo**、**debug bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary** 引入或修改了以下菜单项： **配置** > **设备设置** > **路由** > **BFD** > **模板** **配置** > **设备设置** > **路由** > **BFD** > **接口** **配置** > **设备设置** > **路由** > **BFD** > **映射** **配置** > **设备设置** > **路由** > **BGP** > **IPv6 系列** > **邻居**

功能	说明
IPv6 DHCP	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 引入或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address** 引入或修改了以下菜单项： **配置** > **设备设置** > **接口设置** > **接口** > **添加接口** > **IPv6** **配置** > **设备管理** > **DHCP** > **DHCP 池** **配置** > **设备设置** > **路由** > **BGP** > **IPv6 系列** > **网络** **监控** > **接口** > **DHCP**
高可用性和扩展性功能	
缩短了使用主用/备用故障切换时从 AnyConnect 进行动态 ACL 同步的时间	当您在故障切换对上使用 AnyConnect 时，将关联的动态 ACL (dACL) 同步到备用设备的时间现在已缩短。以前，对于大量dACL，同步时间可能需要几小时，在此期间，备用设备会一直忙于同步而不是提供高度可用的备份。 未修改任何命令。 未修改任何菜单项。
许可功能	

功能	说明
ASAv 永久许可证保留	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以请求提供 ASAv 永久许可证。在 9.6(2) 中，我们还为 Amazon Web 服务上的 ASAv 添加了对此功能的支持。Microsoft Azure 不支持此功能。 **注释** 并非所有帐户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。 引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** 无 ASDM 支持。 同样适用于 *9.5(2.200)*。
适用于 ASAv 短字符串增强的永久许可证保留	由于智能代理的更新（更新至 1.6.4），请求和授权代码现在使用更短的字符串。 未修改任何命令。 未修改任何菜单项。
适用于 Firepower 4100/9300 机箱上 ASAv 的永久许可证预留	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以为Firepower 9300 和 Firepower 4100 上的 ASA 请求永久许可证。所有可用许可证授权均包括在永久许可证中，包括标准层、强加密（如果符合条件）、安全情景和运营商许可证。需要 FXOS 2.0.1。 所有配置均在 Firepower 4100/9300 机箱 上执行；无需对 ASA 进行配置。
ASAv 的智能代理升级至 v1.6	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证保留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 **注释** 如果您从 9.5(2.200) 版本降级，ASAv 将不保留许可注册状态。您需要在**配置 > 设备管理 > 许可 > 智能许可**页面的**强制注册**选项中，使用 **license smart register idtoken** *id_token* **force** 命令重新注册，并从智能软件管理器获取 ID 令牌。 引入了以下命令：**show license status**、**show license summary**、**show license udi**、**show license usage** 修改了以下命令：**show license all**、**show tech-support license** 弃用了以下命令：**show license cert**、**show license entitlement**、**show license pool**、**show license registration** 未更改任何菜单项。 同样适用于 *9.5(2.200)*。
监控功能	

功能	说明
类型为 asp drop 的数据包捕获支持 ACL 和匹配过滤	当您创建类型为 asp drop 的数据包捕获时，现在还可以指定 ACL 或匹配选项来限制捕获范围。 修改了以下命令：**capture type asp-drop** 未修改任何菜单项。
调查分析增强功能	您可以创建在 ASA 运行的任何进程的核心转储。ASA 还可提取主要 ASA 进程的文本部分，您可以从 ASA 复制该文本部分以进行检查。 修改了以下命令：**copy system:text**、**verify system:text**、**crashinfo force dump process** 未修改任何菜单项。
根据每个连接通过 NetFlow 跟踪数据包计数	添加了两个计数器，它们使 Netflow 用户可以查看在连接的两个方向上发送的第 4 层数据包数。您可以使用这些计数器来确定平均数据包速率和大小，并且更好地预测流量类型、异常和事件。 未修改任何命令。 未修改任何菜单项。
用于故障切换的 SNMP engineID 同步	在故障切换对中，已配对 ASA 的 SNMP engineID 会在两个设备上同步。每个 ASA 都保存了 3 组 engineID：同步 engineID、本地 engineID 和远程 engineID。 SNMPv3 用户也可在创建配置文件以保留本地化 **snmp-server user** 身份验证和隐私选项时指定 ASA 的 engineID。如果用户不指定本地 engineID，**show running-config** 输出将显示每位用户的 2 个 engineID。 修改了以下命令：**snmp-server user** 无 ASDM 支持。 同样适用于 *9.4(3)*。

ASA 9.6(1)/ASDM 7.6(1) 新功能

发布日期：2016 年 3 月 21 日

注释 9.6(1) 中未提供 ASAv 9.5.2(200) 的功能，包括 Microsoft Azure 支持。 9.6(2) 中提供了这些功能。

功能	说明
平台功能	

功能	说明
适用于 Firepower 4100 系列 的 ASA	引入了适用于 Firepower 4110、4120 和 4140 的 ASA。 需要 FXOS 1.1.4。 未添加或修改任何命令。 未添加或修改任何菜单项。
ISA 3000 支持 SD 卡	现在，可以使用 SD 卡作为 ISA 3000 上的外部存储。该卡在 ASA 文件系统中显示为 disk3。请注意，即插即用支持需要硬件版本 2.1 和更高版本。可以使用 **show module** 命令检查硬件版本。 未添加或修改任何命令。 未添加或修改任何菜单项。
ISA 3000 支持双电源	对于 ISA 3000 中的双电源，可在 ASA OS 中将双电源建立为预期配置。如果其中一个电源发生故障，ASA 会发出报警。默认情况下，ASA 需要单一电源，只要其中有一个电源正常工作，它就不会发出报警。 引入了以下命令：**power-supply dual** 无 ASDM 支持。
防火墙功能	
Diameter 检查改进	现在，可以检查 TCP/TLS 上的 Diameter 流量，应用严格的协议一致性检查，并可检查集群模式下的 SCTP 上的 Diameter。 引入或修改了以下命令：**client clear-text**、**inspect diameter** 和 **strict-diameter**。 添加或修改了以下菜单项： **配置** > **防火墙** > **对象** > **检查映射** > **Diameter** **配置** > **防火墙** > **服务策略** 添加/编辑向导的**规则操作** > **协议检测**选项卡
集群模式下的 SCTP 状态检查	SCTP 状态检查现在可在集群模式下进行。还可以在集群模式下配置 SCTP 状态检查旁路。 未添加或修改任何命令。 未添加或修改任何菜单项。
H.323 检查支持在 H.225 SETUP 消息之前发出 H.255 FACILITY 消息，以兼容 H.460.18。	现在，当终端符合 H.460.18 的要求时，可将 H.323 检查策略映射配置为允许在 H.225 SETUP 消息之前发出 H.225 FACILITY 消息。 引入了以下命令：**early-message** 我们为 H.323 检查策略映射中的 Call Attributes 选项卡添加了一个选项。

功能	说明
安全交换协议 (SXP) 版本 3 支持思科 TrustSec。	ASA 上的思科 Trustsec 现在实施 SXPv3，它可使 SGT 与子网绑定，这种绑定比主机绑定更高效。 引入或修改了以下命令：**cts sxp mapping network-map** *maximum_hosts*、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map** 和 **show asp table cts sgt-map**。 修改了以下菜单项：**配置** > **防火墙** > **按 TrustSec 标识** 和 **SGT 映射设置**对话框。
Firepower 4100 系列 支持流卸载。	可以识别应从 ASA 中卸载并直接在 Firepower 4100 系列 的 NIC 中切换的流。 需要 FXOS 1.1.4。 未添加或修改任何命令。 未添加或修改任何菜单项。
远程访问功能	
IKEv2 分段、RFC-7383 支持	ASA 现在支持 IKEv2 数据包的此标准分段。这将实现与其他 IKEv2 实施（如 Apple、Strongswan 等）的互操作性。ASA 继续支持当前的专有 IKEv2 分段，以保持对不支持 RFC-7383 的思科产品（如 AnyConnect 客户端）的向后兼容性。 引入了以下命令： **crypto ikev2 fragmentation**、**show running-config crypto ikev2** 和 **show crypto ikev2 sa detail**
Firepower 9300 和 Firepower 4100 系列 上的 VPN 吞吐量性能增强	Firepower 9300 和 Firepower 4100 系列 上的 ASA 安全模块现在支持 **crypto engine accelerator-bias** 命令。此命令使您能将更多加密核心向 IPSec 或 SSL“偏差”。 修改了以下命令：**crypto engine accelerator-bias** 未添加或修改任何菜单项。
可配置 SSH 加密和 HMAC 算法。	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下命令：**ssh cipher encryption, ssh cipher integrity**。 引入了以下菜单项：**配置** > **设备管理** > **高级** > **SSH 密码** 同样适用于 *9.1(7)*、*9.4(3)* 和 *9.5(3)* 版本。
IPV6 支持 HTTP 重定向	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 向以下命令添加了功能：**http redirect** 向以下菜单项添加了功能：**配置** > **设备管理** > **HTTP 重定向** 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。

功能	说明
路由功能	
IS-IS 路由	ASA 现在支持中间系统到中间系统 (IS-IS) 路由协议。添加了对使用 IS-IS 路由协议进行路由数据、执行身份验证和重新分发及监控路由信息的支持。 引入了以下命令： **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear isis, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, route isis, set-attached-bit, set-overload-bit, show clns, show isis, show router isis, spf-interval, summary-address.** 引入了以下菜单项： **配置 > 设备设置 > 路由 > ISIS** **监控 > 路由 > ISIS**
高可用性和扩展性功能	
在路由、跨网络 EtherChannel 模式下支持站点特定的 IP 地址	对于使用跨网络 EtherChannel 的路由模式下的站点间集群，除了站点特定的 MAC 地址以外，现在还可配置站点特定的 IP 地址。添加站点 IP 地址后，允许您对重叠传输虚拟化 (OTV) 设备使用 ARP 检测来防止通过数据中心互联 (DCI) 传输的全局 MAC 地址的 ARP 响应（可能导致路由问题）。对于无法使用 VACL 来过滤 MAC 地址的某些交换机，需要使用 ARP 检测。 修改了以下命令：**mac-address**、**show interface** 修改了以下菜单项：**配置** > **设备设置** > **接口设置** > **接口** > **添加/编辑 EtherChannel 接口** > **高级**
管理功能	
本地 **username** 和 **enable** 密码支持更长的密码（最多 127 个字符）	您现在可以创建最多 127 个字符的本地 **username** 和 **enable** 密码（过去的限制为 32 个字符）。在创建长度超过 32 个字符的密码时，它将使用 PBKDF2（基于密码的密钥派生功能 2）散列存储在配置中。较短的密码将继续使用基于 MD5 的散列处理方法。 修改了以下命令：**enable**、**username** 修改了以下菜单项： **配置** > **设备设置** > **设备名称/密码** > **启用密码** **配置** > **设备管理** > **用户/AAA** > **用户账户** > **添加/编辑用户账户** > **身份**

功能	说明
支持 CISCO-ENHANCED-MEMPOOL-MIB 中的 cempMemPoolTable	现在支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，监控受管系统上所有物理实体的条目。 注释 CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持报告 RAM 超过 4GB 的平台上的内存。 未添加或修改任何命令。 未添加或修改任何菜单项。 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。
REST API 版本 1.3.1	增加了对 REST API 1.3.1 版本的支持。

版本 9.5 的新功能

ASA 9.5(3.9)/ASDM 7.6(2) 的新功能

发布日期：**2017** 年 **4** 月 **11** 日

注释 由于漏洞 CSCvd78303，已从 Cisco.com 中删除版本 9.5(3)。

功能	说明
远程访问功能	
可配置 SSH 加密和 HMAC 算法。	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下命令：**ssh cipher encryption, ssh cipher integrity**。 引入了以下菜单项：**配置** > **设备管理** > **高级** > **SSH 密码** 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。

ASAv 9.5(2.200)/ASDM 7.5(2.153) 新增功能

发布日期：**2016** 年 **1** 月 **28** 日

注释 此版本仅支持 ASAv。

功能	说明
平台功能	
ASAv10 上提供 Microsoft Azure 支持	Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。ASAv 在 Hyper V 虚拟机监控程序的 Microsoft Azure 环境中充当访客。Microsoft Azure 上的 ASAv 支持一个实例类型，即标准 D3。标准 D3 可支持 4 个 vCPU、14 GB 内存和 4 个接口。
许可功能	
ASAv 永久许可证保留	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以请求提供 ASAv 永久许可证。 注释 并非所有帐户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。 引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** 无 ASDM 支持。
智能代理升级至 v1.6	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证保留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 注释 如果您从 9.5(2.200) 版本降级，ASAv 将不保留许可注册状态。您需要在**配置 > 设备管理 > 许可 > 智能许可**页面的**强制注册**选项中，使用 **license smart register idtoken** *id_token* **force** 命令重新注册，并从智能软件管理器获取 ID 令牌。 引入了以下命令：**show license status**、**show license summary**、**show license udi**、**show license usage** 修改了以下命令：**show license all**、**show tech-support license** 弃用了以下命令：**show license cert**、**show license entitlement**、**show license pool**、**show license registration** 未修改任何菜单项。

ASA 9.5(2.1)/ASDM 7.5(2) 新增功能

发布时间：**2015** 年 **12** 月 **14** 日

注释　此版本仅支持 Firepower 9300 ASA。

功能	说明
平台功能	
Firepower 9300 上 ASA 的 VPN 支持	您可使用 FXOS 1.1.3 版本配置 VPN 功能。
防火墙功能	
Firepower 9300 上 ASA 的分流支持	您可以识别需从 ASA 中分流并直接在 NIC（位于 Firepower 9300 上）中切换的流量。此功能可提升数据中心中的大数据流性能。 还需要 FXOS 1.1.3。 添加或修改了以下命令：**clear flow-offload**、**flow-offload enable**、**set-connection advanced-options flow-offload**、**show conn detail** 和 **show flow-offload**。 在**配置** > **防火墙** > **安全策略规则**下添加或编辑规则时，添加或修改了以下菜单项：**配置** > **防火墙** > **高级** > **分流引擎**、**规则行为** > **连接设置**选项卡。
高可用性功能	
6 个模块的机箱间集群，以及 Firepower 9300 上 ASA 的站点间集群	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。在最多 6 个机箱中最多可以包含 6 个模块。 未修改任何命令。 未修改任何菜单项。
许可功能	
为 Firepower 9300 上的 ASA 自动应用的强加密 (3DES) 许可证	对于一般的思科智能软件管理器用户，当他们在 Firepower 9300 上应用注册令牌时，只要符合相应条件，系统会自动启用强加密许可证。 注释　如果您通过智能软件管理器卫星部署使用 ASDM 和其他强加密功能，您必须在部署 ASA 之后使用 ASA CLI 启用强加密 (3DES) 许可证。 此功能要求具有 FXOS 1.1.3 版本。 删除了以下非卫星配置中的命令：**feature strong-encryption** 修改了以下菜单项：**配置** > **设备管理** > **许可** > **智能许可**

ASA 9.5(2)/ASDM 7.5(2) 的新功能

发布时间：**2015** 年 **11** 月 **30** 日

功能	说明
平台功能	
提供思科 ISA 3000 支持	思科 ISA 3000 是一个装有 DIN 导轨的坚固型工业安全设备。它是一种低功耗、无风扇设备，并配有千兆以太网和专用管理端口。该型号设备中预装了 ASA Firepower 模块。该型号的特殊功能包括自定义的透明模式默认配置，以及允许流量在出现功率损耗时继续通过设备的硬件旁路功能。 引入了以下命令：**hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay** 修改了以下菜单项：**配置** > **设备管理** > **硬件绕过** 同样适用于 *9.4.(1.225)* 版本。
防火墙功能	
DCERPC 检测改进和 UUID 过滤	DCERPC 检测现在支持 OxidResolver ServerAlive2 opnum5 消息的 NAT。现在您可根据 DCERPC 消息通用唯一标识 (UUID) 进行过滤，以便重置或记录特定消息类型。新 DCERPC 检测类映射可用于 UUID 过滤。 引入了以下命令：**match [not] uuid**。修改了以下命令：**class-map type inspect**。 添加了以下菜单项：**配置** > **防火墙** > **对象** > **类映射** > **DCERPC**。 修改了以下菜单项：**配置** > **防火墙** > **对象** > **检测映射** > **DCERPC**。
Diameter 检测	现在您可以检测 Diameter 流量。Diameter 检测需要 Carrier 许可证。 引入或修改了以下命令：**class-map type inspect diameter**、**diameter**、**inspect diameter**、**match application-id**、**match avp**、**match command-code**、**policy-map type inspect diameter**、**show conn detail**、**show diameter**、**show service-policy inspect diameter** 和 **unsupported** 添加或修改了以下菜单项： **配置** > **防火墙** > **对象** > **检查映射** > **Diameter** 和 **Diameter AVP** **配置** > **防火墙** > **服务策略** 添加/编辑向导的**规则操作** > **协议检测**选项卡

功能	说明
SCTP 检测和访问控制	现在您可以在服务对象、访问控制列表 (ACL) 和访问规则中使用 SCTP 协议和端口规范，并检测 SCTP 流量。SCTP 检测需要 Carrier 许可证。 引入了以下命令：**access-list extended** 、**clear conn protocol sctp**、**inspect sctp**、**match ppid**、**nat static**（对象）、**policy-map type inspect sctp**、**service-object**、**service**、**set connection advanced-options sctp-state-bypass**、**show conn protocol sctp**、**show local-host connection sctp**、**show service-policy inspect sctp** 和 **timeout sctp** 添加或修改了以下菜单项： **配置** > **防火墙** > **访问规则**“添加/编辑”对话框 **配置** > **防火墙** > **高级** > **ACL 管理器**“添加/编辑”对话框 **配置** > **防火墙** > **高级** > **全局超时** **配置** > **防火墙** > **NAT**添加/编辑静态网络 NAT 规则、**高级 NAT 设置**对话框 **配置** > **防火墙** > **对象** > **服务对象/组** 添加/编辑对话框 **配置** > **防火墙** > **对象** > **检测映射** > **SCTP** **配置** > **防火墙** > **服务策略** 添加/编辑向导的**规则操作** > **协议检查**和**连接设置**选项卡
现在支持在故障切换和 ASA 集群中增强运营商级 NAT	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。现在支持在故障切换和 ASA 集群部署中使用此功能。 修改了以下命令：**show local-host** 未修改任何菜单项。
ASA FirePOWER 6.0 中使用强制网络门户的主动身份验证。	从 ASA FirePOWER 6.0 开始，要使用身份策略启用主动身份验证，需使用强制网络门户功能。 引入或修改了以下命令：**captive-portal**、**clear configure captive-portal** 和 **show running-config captive-portal**。
高可用性功能	

功能	说明
站点间流移动性的 LISP 检测	思科定位编号分离协议(LISP)架构将设备身份与设备位置分离开，并分隔到两个不同的编号空间，使服务器迁移对客户端透明化。ASA 可以通过检测 LISP 流量确定位置更改,并使用此信息进行无缝集群操作；ASA 集群成员检查第一跳路由器与出口隧道路由器 (ETR) 或入口隧道路由器 (ITR) 之间的 LISP 流量，然后将流所有者位置更改为新站点。 引入或修改了以下命令：**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key** 引入或修改了以下菜单项： 配置 > 设备管理 > 高可用性和可扩展性 > **ASA** 集群 > 集群配置 配置 > 防火墙 > 对象 > 检查映射 > **LISP** 配置 > 防火墙 > 服务策略规则 > 协议检查 配置 > 防火墙 > 服务策略规则 > 集群 监控 > 路由 > **LISP-EID** 表
ASA 5516-X 对集群的支持	ASA 5516-X 现在支持由 2 台设备组成的集群。默认情况下，基本许可证中启用 2 台设备的集群。 未修改任何命令。 未修改任何菜单项。
可配置级别集群跟踪条目	默认情况下，所有级别的集群事件都储存在跟踪缓冲区中，包括大量低级事件。要将跟踪事件级别限制为更高级别，您可以设置集群跟踪事件的最低级别。 引入了以下命令：**trace-level** 未修改任何菜单项。
接口功能	
支持将辅助 VLAN 映射到主 VLAN	现在，可以为子接口配置一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。 引入或修改了以下命令：**vlan secondary**、**show vlan mapping** 修改了以下菜单项：配置 > 设备设置 > 接口设置 > 接口 配置 > 设备设置 > 接口设置 > 接口 > 添加接口 > 通用
路由功能	

功能	说明
为组播路由提供 PIM 自举路由器 (BSR) 支持	目前，ASA 支持配置静态 RP，为不同的组路由组播流量。对于可能存在多个 RP 的大型复杂网络，ASA 现在支持使用 PIM BSR 选择动态 RP 来支持 RP 移动。 引入了以下命令：**clear pim group-map**、**debug pim bsr**、**pim bsr-border**、**pim bsr-candidate**、**show pim bsr-router**、**show pim group-map rp-timers** 引入了以下菜单项：**配置** > **设备设置** > **路由** > **组播** > **PIM** > **Bootstrap 路由器**
远程访问功能	
支持多情景模式下的远程接入 VPN	现在您可在多情景模式中使用以下远程接入功能： • AnyConnect 3.x 及更高版本（仅支持 SSL VPN；无 IKEv2 支持） • 集中式 AnyConnect 映像配置 • AnyConnect 映像升级 • 对 AnyConnect 连接进行情景资源管理 **注释** 多情景模式下需要 AnyConnect Apex 许可证；您无法使用默认或传统许可证。 引入了以下命令：**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect** 修改了以下菜单项：**配置** > **情景管理** > **资源类** > **添加资源类**
无客户端 SSL VPN 提供基于 SAML 2.0 的单点登录 (SSO) 功能	ASA 充当 SAML 服务提供商。
无客户端 SSL VPN 条件调试	您可以根据过滤条件集进行过滤，以达到调试日志的目的，也可以更好地对其进行分析。 向调试命令中引入了以下添加项： • [no] debug webvpn condition user <user name> • [no] debug webvpn condition group <group name> • [no] debug webvpn condition p-ipaddress <ipv4> [subnet<mask>] • [no] debug webvpn condition p-ipaddress <ipv6> [prefix<prefix>] • debug webvpn condition reset • show debug webvpn condition • show webvpn debug-condition

功能	说明

默认情况下，无客户端 SSL VPN 为禁用状态。	现在，无客户端 SSL VPN 缓存默认为禁用状态。禁用 SSL VPN 缓存可增强稳定性。若要启用缓存，您必须手动操作。
	
	`webvpn`
	`  cache`
	`  no disable`
	
	修改了以下命令：**cache**
	
	修改了以下菜单项：**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **高级** > **内容缓存**

许可功能	
如果服务器证书的颁发层次结构出现更改，思科智能报障服务 (Smart Call Home)/智能许可 (Smart Licensing) 证书需进行验证	智能许可使用 Smart Call Home 基础设施。当 ASA 首次在后台配置智能报障服务的匿名报告时，它会自动创建一个信任点，这个信任点包含颁发过智能报障服务证书的 CA 的证书。ASA 现在支持在服务器证书颁发层次结构出现变更时对证书进行验证；您可以按一定时间间隔定期启用 trustpool 捆绑的自动更新功能。 引入了以下命令：**auto-import** 修改了以下菜单项：**配置** > **远程访问 VPN** > **证书管理** > **可信任证书池** > **编辑策略**
新运营商许可证	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 Firepower 9300 上的 ASA，**feature mobile-sp** 命令将自动迁移到 **feature carrier** 命令。 引入或修改了以下命令：**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version** 修改了以下菜单项：**配置** > **设备管理** > **许可** > **智能许可**
监控功能	
SNMP engineID 同步	在一个 HA 对中，已配对 ASA 的 SNMP engineIDs 会在两个设备上同步。每个 ASA 都保存了 3 组 engineID：同步 engineID、本地 engineID 和远程 engineID。 SNMPv3 用户也可在创建配置文件以保留本地化 **snmp-server user** 身份验证和隐私选项时指定 ASA 的 engineID。如果用户不指定本地 engineID，**show running-config** 输出将显示每位用户的 2 个 engineID。 修改了以下命令：**snmp-server user**、**no snmp-server user** 未修改任何菜单项。 同样适用于 *9.4(3)* 版本。

功能	说明
show tech support 改进	**show tech support** 命令现在： • 包括 **dir all-filesystems** 输出 - 该输出可在以下情况中起作用： • SSL VPN 配置：检查所需资源是否在 ASA 上 • 故障：检查日期时间戳及是否存在故障文件 • 删除 **show kernel cgroup-controller detail** 输出 - 此命令输出将保留在 **show tech-support detail** 的输出中。 修改了以下命令：**show tech support** 未修改任何菜单项。 同样适用于 *9.1(7)* 和 *9.4(3)* 版本。
logging debug-trace 持久性	以前，当您启用 **logging debug-trace** 以将调试重定向到系统日志服务器时，如果 SSH 连接断开（由于网络连接或超时），调试将被删除。现在，只要 **logging** 命令有效，调试就会一直存在。 修改了以下命令：**logging debug-trace** 未修改任何菜单项。

ASA 9.5(1.5)/ASDM 7.5(1.112) 的新功能

发布时间：**2015** 年 **11** 月 **11** 日

功能	说明
平台功能	
支持 ASA FirePOWER 6.0	所有以前支持过的设备型号都支持 ASA FirePOWER 6.0 版本。
从 5512-X 到 5585-X 系列都支持通过 ASDM 管理 ASA FirePOWER 模块。	在模块上运行 6.0 版本时，您可以使用 ASDM 来管理 ASA FirePOWER 模块，而无需使用 Firepower 管理中心 (Firepower Management Center)（以前称为 FireSIGHT 管理中心 (FireSIGHT Management Center)）来进行管理。运行 6.0 版本时，您还可以使用 ASDM 来管理 5506-X、5506H-X、5506W-X、5508-X 和 5516-X 上的模块。 无新增菜单项或命令。

ASDM 7.5(1.90) 新增功能

发布时间：**2015** 年 **10** 月 **14** 日

功能	说明
远程访问功能	
支持 AnyConnect 4.2 版本	ASDM 可支持 AnyConnect 4.2 版本及网络可视性模块 (NVM)。NVM 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。NVM收集终端遥测数据，在系统日志中记录流数据和文件信誉,并导出流记录给收集器（第三方供应商），由其执行文件分析并提供 UI 接口。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 客户端配置文件**（一个名为**网络可视性服务配置文件**的配置新文件)

ASAv 9.5(1.200)/ASDM 7.5(1) 新增功能

发布日期：**2015** 年 **8** 月 **31** 日

注释 此版本仅支持 ASAv。

功能	说明
平台功能	
提供 Microsoft Hyper-V 管理引擎支持	扩展 ASAv 虚拟机监控程序配置文件。
支持 ASAv5 低内存	ASAv5 现在只需要 1 GB RAM 即可运行。而此前它需要 2 GB 的内存。对于已部署的 ASAv5s，您应将分配的内存减少至 1 GB，若不进行此操作，系统将显示错误消息提示您使用的内存已超出许可范围。

ASA 9.5(1)/ASDM 7.5(1) 新增功能

发布时间：**2015** 年 **8** 月 **12** 日

注释 此版本不支持 Firepower 9300 ASA 安全模块或 ISA 3000。

功能	说明
防火墙功能	
GTPv2 检测及对 GTPv0/1 检测的改进	GTP 检测现在可以处理 GTPv2。此外，所有版本的 GTP 检测现在均支持 IPv6 地址。 修改了以下命令：**clear service-policy inspect gtp statistics**、**clear service-policy inspect gtp pdpmcb**、**clear service-policy inspect gtp request**、**match message id**、**show service-policy inspect gtp pdpmcb**、**show service-policy inspect gtp request**、**show service-policy inspect gtp statistics**、**timeout endpoint** 弃用了以下命令：**timeout gsn** 修改了以下菜单项：**配置 > 防火墙 > 对象 > 检测图 > GTP**
对 IP 选项检测的改进	IP 选项检测现在支持所有可能的 IP 选项。您可以对检测进行调整以允许、清除或丢弃任何标准的或试验性选项，包括尚未定义的选项。还可以为 IP 选项检测图中尚未明确定义的选项设置默认行为。 引入了以下命令：**basic-security, commercial-security, default, exp-flow-control, exp-measure, extended-security, imi-traffic-description, quick-start, record-route, timestamp** 修改了以下菜单项：**配置 > 防火墙 > 对象 > 检测图 > IP 选项**
对运营商级 NAT 的改进	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。 引入了以下命令：**xlate block-allocation size**、**xlate block-allocation maximum-per-host**。我们已将关键字 **block-allocation** 添加到 **nat** 命令中。 引入了以下菜单项：**配置 > 防火墙 > 高级 > PAT 端口块分配**。添加了对象 NAT **启用端口块分配**并两次添加了 NAT 对话框。
高可用性功能	
为路由防火墙模式下的 Spanned EtherChannel 提供站点间集群支持	现在您可以在路由防火墙模式下对 Spanned EtherChannel 使用站点间集群。要避免 MAC 地址摆动，请为每个集群成员配置一个站点 ID，这样就可在站点的设备间共享每个接口的站点特定 MAC 地址。 我们引入或修改了以下命令：**site-id**、**mac-address site-id**、**show cluster info**、**show interface** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群 > 集群配置**
自定义接口或集群控制链路发生故障时的 ASA 集群自动重新加入行为	现在您可以自定义接口或集群控制链路发生故障时的自动重新加入行为。 引入了以下命令：**health-check auto-rejoin** 引入了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群 > 自动重新加入**

功能	说明
ASA 集群支持 GTPv1 和 GTPv2	ASA 集群现在支持 GTPv1 和 GTPv2 检测。 未修改任何命令。 未修改任何菜单项。
TCP 连接的集群复制延迟	该功能可以延迟导向器/备份流的创建，从而避免与短期流量相关的“不必要的工作”。 引入了以下命令：**cluster replication delay** 引入了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群复制** 同样适用于 *Firepower 9300 ASA* 安全模块 *9.4(1.152)* 版本。
禁用 ASA 集群中硬件模块的健康状况监控	默认情况下，当使用集群时，ASA 会监控已安装的硬件模块（例如 ASA FirePOWER 模块）的运行状况。如果您不希望硬件模块故障触发故障切换，则可以禁用模块监控。 修改了以下命令：**health-check monitor-interface service-module** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群 > 集群接口健康状况监控**
在 ASA 5506H 上启用管理 1/1 接口作为故障切换链路	现在您只能在 ASA 5506H 上将管理 1/1 接口配置为故障切换链路。此功能允许您使用设备上的所有其他接口作为数据接口。说明：如果您使用了此功能，便不能使用 ASA Firepower 模块，因为它要求管理 1/1 接口仍作为常规管理接口。 修改了以下命令：**failover lan interface**、**failover link** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 设置**
路由功能	
支持 IPv6 策略型路由	策略型路由现在支持 IPv6 地址。 引入了以下命令：**set ipv6 next-hop**、**set default ipv6-next hop**、**set ipv6 dscp** 修改了以下菜单项： **配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 基于策略的路由配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 匹配语句**
为策略型路由提供 VXLAN 支持	现在您可以在 VNI 接口中启用策略型路由。 未修改任何命令。 修改了以下菜单项：**配置 > 设备设置 > 接口设置 > 接口 > 添加/编辑接口 > 常规**
为身份防火墙和思科 TrustSec 提供策略型路由支持	您可以先配置身份防火墙和思科 TrustSec，然后再在策略型路由的路由图中使用身份防火墙和思科 TrustSec ACL。 未修改任何命令。 修改了以下菜单项：**配置 > 设备设置 > 路由 > 路由映射 > 添加路由映射 > 匹配语句**

功能	说明
仅用于管理的接口的独立路由表	为了使管理流量与数据流量分开并隔离，ASA 现在支持为仅管理接口使用独立路由表。 引入或修改了以下命令：**backup**、**clear ipv6 route management-only**、**clear route management-only**、**configure http**、**configure net**、**copy**、**enrollment source**、**name-server**、**restore**、**show asp table route-management-only**、**show ipv6 route management-only show route management-only** 未修改任何菜单项。
支持协议无关组播 - 源特定组播 (PIM-SSM) 直接通过	ASA 现允许 PIM-SSM 数据包在您启用组播路由后直接通过，但有一种情况除外：ASA 是最后一跳路由器时。此功能使得在选择组播组时更加灵活，同时也防止了多种攻击；主机只接收明确请求的数据源发来的流量。 未修改任何命令。 未修改任何菜单项。
远程访问功能	
IPv6 VLAN 映射	经改进后，ASA VPN 代码现已支持所有 IPv6 功能。管理员不需要更改配置。
提供无客户端 SSL VPN SharePoint 2013 支持	为此 SharePoint 新版本增加了支持和一个预定义的应用模板。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签 > 添加书签列表 > 选择书签类型 > 预定义应用模板**
无客户端 VPN 动态书签	我们将 CSCO_WEBVPN_DYNAMIC_URL 和 CSCO_WEBVPN_MACROLIST 添加到使用书签时的宏列表中。管理员可利用这些宏配置出可在无客户端用户的门户中生成多个书签链接的单个书签，并静态配置多个书签来利用 LDAP 属性地图提供的大小随机的列表。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签**
VPN 标志长度增加	登录后在 VPN 远程客户端门户上显示的整体标志长度已从 500 增至 4000。 修改了以下命令：**banner**（策略组）。 修改了以下菜单项：**配置 > 远程访问 VPN > .... 添加/编辑内部组策略 > 通用参数 > 标志**

功能	说明
ASA 5506-X、5506W-X、5506H-X 和 5508-X 上的思科 Easy VPN 客户端	此版本支持在 ASA 5506-X 系列和 ASA 5508-X 型号的设备上使用思科 Easy VPN。当连接到 VPN 头端时，ASA 会充当 VPN 硬件客户端。当一个 ASA 设备连接到 Easy VPN 端口，其下面连接的所有设备（计算机、打印机等）都可通过 VPN 进行通信；这些设备无需单独运行 VPN 客户端。请注意只有一个 ASA 接口可用作 Easy VPN 端口；要使多个设备连接到该端口，您需在该端口安置一个第二层交换机，再将您的设备连接至交换机。 引入了以下命令：**vpnclient enable**、**vpnclient server**、**vpnclient mode**、**vpnclient username**、**vpnclient ipsec-over-tcp**、**vpnclient management**、**vpnclient vpngroup**、**vpnclient trustpoint**、**vpnclient nem-st-autoconnect**、**vpnclient mac-exempt** 引入了以下菜单项：**配置 > VPN > Easy VPN Remote**
监控功能	
在系统日志消息中显示无效用户名	您现在可以在失败登录尝试的系统日志消息中显示无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。 引入了以下命令：**no logging hide username** 修改了以下菜单项：**配置 > 设备管理 > 日志记录 > 系统日志设置** 此功能同样适用于 *9.2(4)* 和 *9.3(3)* 版本。
REST API 功能	
REST API 1.21 版本	增加了对 REST API 1.2.1 版本的支持。

版本 9.4 的新功能

ASA 9.4(4.5)/ASDM 7.6(2) 的新功能

发布日期：2017 年 4 月 3 日

注释 由于漏洞 CSCvd78303，已从 Cisco.com 中删除版本 9.4(4)。

此版本中无新增功能。

ASA 9.4(3)/ASDM 7.6(1) 新增功能

发布时间：**2016** 年 **4** 月 **25** 日

功能	说明
防火墙功能	
路由融合的连接等待超时	现在，您可以配置系统在连接使用的路由不再存在或处于非活动状态时，应保持连接的时间。如果路由在此抑制期间未变为活动状态，连接将被释放。您可以减小抑制计时器，使路由汇聚更快速地进行。但是，默认值 15 秒适合大多数网络，可以防止路由摆动。 添加了以下命令：**timeout conn-holddown** 修改了以下菜单项：**配置** > **防火墙** > **高级** > **全局超时**
远程访问功能	
可配置 SSH 加密和 HMAC 算法。	用户可以在执行 SSH 加密管理时选择密码模式，并且可以为不同的密钥交换算法配置 HMAC 和加密。 引入了以下命令：**ssh cipher encryption, ssh cipher integrity**。 引入了以下菜单项：**配置** > **设备管理** > **高级** > **SSH 加密** 同样适用于 *9.1(7)* 版本。
对 IPv6 的 HTTP 重新定向支持	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 向以下命令添加了该功能：**http redirect** 为以下菜单项添加了功能：**配置** > **设备管理** > **HTTP 重定向** 同样适用于 *9.1(7)* 版本。
监控功能	
用于故障切换的 SNMP engineID 同步	在故障切换对中，已配对 ASA 的 SNMP engineID 会在两个设备上同步。每个 ASA 都保存了 3 组 engineID：同步 engineID、本地 engineID 和远程 engineID。 SNMPv3 用户也可在创建配置文件以保留本地化 **snmp-server user** 身份验证和隐私选项时指定 ASA 的 engineID。如果用户不指定本地 engineID，**show running-config** 输出将显示每位用户的 2 个 engineID。 修改了以下命令：**snmp-server user** 无 ASDM 支持。

功能	说明
show tech support 改进	**show tech support** 命令现在： • 包括 **dir all-filesystems** 输出 - 该输出可在以下情况中起作用： • SSL VPN 配置：检查所需资源是否在 ASA 上 • 故障：检查日期时间戳及是否存在故障文件 • 删除 **show kernel cgroup-controller detail** 输出 - 此命令输出将保留在 **show tech-support detail** 的输出中。 修改了以下命令：**show tech support** 未修改任何菜单项。 同样适用于 *9.1(7)* 版本。
CISCO-ENHANCED-MEMPOOL-MIB 中对 cempMemPoolTable 的支持	现在支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，监控受管系统上所有物理实体的条目。 **注释** CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持报告 RAM 超过 4GB 的平台上的内存。 未添加或修改任何命令。 未修改任何菜单项。 同样适用于 *9.1(7)* 版本。

ASA 9.4(2.145)/ASDM 7.5(1) 新增功能

发布日期：2015 年 11 月 13 日

此版本中无新增功能。

注释 此版本仅支持 Firepower 9300 ASA 安全模块。

ASA 9.4(2)/ASDM 7.5(1) 的新功能

发布时间：2015 年 9 月 24 日

此版本中无新增功能。

注释 此版本中不包含 ASAv 9.4(1.200) 功能。

注释 此版本不支持 ISA 3000。

ASA 9.4(1.225)/ASDM 7.5(1) 的新功能

发布日期：**2015** 年 **9** 月 **17** 日

注释 此版本仅支持思科 ISA 3000。

功能	说明
平台功能	
提供思科 ISA 3000 支持	思科 ISA 3000 是一个装有 DIN 导轨的坚固型工业安全设备。它是一种低功耗、无风扇设备，并配有千兆以太网和专用管理端口。该型号设备中预装了 ASA Firepower 模块。该型号的特殊功能包括自定义的透明模式默认配置，以及允许流量在出现功率损耗时继续通过设备的硬件旁路功能。 引入了以下命令：**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** 引入了以下菜单项：**配置** > **设备管理** > **硬件旁路** **hardware-bypass boot-delay** 命令不适用于 ASDM 7.5(1) 版本。 此功能不适用于 *9.5(1)* 版本。

ASA 9.4(1.152)/ASDM 7.4(3) 的新功能

发布日期：**2015** 年 **7** 月 **13** 日

注释 此版本仅支持 Firepower 9300 ASA。

功能	说明
平台功能	
Firepower 9300 ASA 安全模块	我们引入了 Firepower 9300 ASA 安全模块。 注释 Firepower 机箱管理器 1.1.1 对于 Firepower 9300 上的 ASA 安全模块不支持任何 VPN 功能（站点到站点访问或远程访问）。

功能	说明
高可用性功能	
Firepower 9300 的机箱内 ASA 集群	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 引入了以下命令：**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis** 引入了以下菜单项：**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群复制**
许可功能	
Firepower 9300 ASA 的思科智能软件许可	我们为 Firepower 9300 ASA 引入了智能软件许可。 引入了以下命令：**feature strong-encryption, feature mobile-sp, feature context** 修改了以下菜单项：**配置** > **设备管理** > **许可** > **智能许可**

ASAv 9.4(1.200)/ASDM 7.4(2) 的新功能

发布日期：**2015** 年 **5** 月 **12** 日

注释 此版本仅支持 ASAv。

功能	说明
平台功能	
VMware ASAv 不再需要 vCenter 支持	您现在可以使用 vSphere 客户端安装 VMware ASAv，而无需 vCenter，或使用 Day 0 配置安装 OVFTool。
亚马逊网络服务 (AWS) ASAv	您现在可以将 ASAv 与亚马逊网络服务 (AWS) 和 Day 0 配置结合使用。 **注释** 亚马逊网络服务仅支持 ASAv10 和 ASAv30 模式。

ASDM 7.4(2) 新功能

发布日期：**2015** 年 **5** 月 **6** 日

功能	说明
远程访问功能	

功能	说明
支持 AnyConnect 4.1 版本	ASDM 现在支持 AnyConnect 4.1 版本。 修改了以下菜单项：**配置 > 远程访问 VPN >网络（客户端）访问 > AnyConnect 客户端配置文件**（一个名为 **AMP 启用服务配置**的新配置文件）

ASA 9.4(1)/ASDM 7.4(1) 新功能

发布时间：**2015** 年 **3** 月 **30** 日

功能	说明
平台功能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X、ASA 5516-X	引入了以下型号：带有无线接入点的 ASA 5506W-X、强化型 ASA 5506H-X、ASA 5508-X 和 ASA 5516-X。 引入了以下命令：**hw-module module wlan recover image** 和 **hw-module module wlan recover image**。 未修改任何 ASDM 菜单项。
认证功能	
美国国防部统一功能要求 (UCR) 2013 认证	ASA 已更新，符合 DoD UCR 2013 要求。请参阅下表中的各行，了解下列为 UCR 2013 认证添加的功能： • 定期证书身份验证 • 证书到期警报 • 执行基本约束 CA 标记 • 从证书配置 ASDM 用户名 • ASDM 管理授权 • IKEv2 无效选择器通知配置 • IKEv2 十六进制预共享密钥

功能	说明
FIPS 140-2 认证合规更新	当在 ASA 上启用 FIPS 模式时，将会对 ASA 实施其他限制，以使其符合 FIPS 140-2。限制包括： • RSA 和 DH 密钥大小限制 - 仅允许使用大小为 2K（2048 位）或以上的 RSA 和 DH 密钥。对于 DH，这意味着不允许使用第 1 组（768 位）、第 2 组（1024 位）和第 5 组（1536 位）密钥。 注释　密钥大小限制禁止 IKEv1 与 FIPS 结合使用。 • 数字签名的散列算法限制 - 仅允许使用 SHA256 或更安全的算法。 • SSH 密码限制 - 允许的密码为：aes128-cbc 或 aes256-cbc。MAC：SHA1 要查看 ASA 的 FIPS 认证状态，请参阅： http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf 此 PDF 每周更新一次。 有关详细信息，请访问计算机安全部门的计算机安全资源中心网站： http://csrc.nist.gov/groups/STM/cmvp/inprocess.html 修改了以下命令：**fips enable**
防火墙功能	
改进了多核 ASA 上的 SIP 检查性能。	如果有多条 SIP 信令流通过多核 ASA，表明 SIP 检查性能已经改进。但是，如果您使用的是 TLS、电话或 IME 代理，则不会看到性能改进。 未修改任何命令。 未修改任何菜单项。
取消了对电话代理和 UC-IME 代理的 SIP 检查支持。	配置 SIP 检查后，将无法再使用电话代理或 UC-IME 代理。使用 TLS 代理检查加密流量。 删除了以下命令：**phone-proxy** 和 **uc-ime**。从 **inspect sip** 命令中删除了 **phone-proxy** 和 **uc-ime** 关键字。 从 **Select SIP Inspect Map** 服务策略对话框中删除了 Phone Proxy 和 UC-IME Proxy。
对 ISystemMapper UUID 消息 RemoteGetClassObject opnum3 的 DCERPC 检查支持。	ASA 从版本 8.3 开始支持非 EPM DCERPC 消息，支持 ISystemMapper UUID 消息 RemoteCreateInstance opnum4。此更改扩展了对 RemoteGetClassObject opnum3 消息的支持。 未修改任何命令。 未修改任何菜单项。

功能	说明
每个情景的 SNMP 服务器陷阱主机数没有限制	ASA 支持每个情景的 SNMP 服务器陷阱主机数不受限制。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 修改了以下命令：**show snmp-server host**。 未修改任何菜单项。
VXLAN 数据包检查	ASA 可检查 VXLAN 报头以强制遵守标准格式。 引入了以下命令：**inspect vxlan**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 > 规则行为 > 协议检查**
IPv6 的 DHCP 监控	您现在可以监控 IPv6 的 DHCP 统计信息和 DHCP 绑定。 引入了以下菜单项： **监控 > 接口 > DHCP > IPV6 DHCP 统计信息监控 > 接口 > DHCP > IPV6 DHCP 绑定**。
TLS 会话的默认行为中的 ESMTP 检查更改。	已将 ESMTP 检查的默认设置更改为允许 TLS 会话，这些会话不会被检查。不过，此默认设置适用于新的或重新映像的系统。如果您升级了包括 **no allow-tls** 的系统，则该命令不会更改。 还在以下早期版本中进行了此默认行为更改：8.4(7.25)、8.5(1.23)、8.6(1.16)、8.7(1.15)、9.0(4.28)、9.1(6.1)、9.2(3.2)、9.3(1.2)、9.3(2.2)。
高可用性功能	
阻止在备用 ASA 上生成系统日志	您现在可以阻止在备用设备上生成特定系统日志。 引入了以下命令：**no logging message** *syslog-id* **standby**。 未修改任何菜单项。
按接口启用和禁用 ASA 集群运行状况监控	您现在可以按接口启用或禁用运行状况监控。默认情况下，运行状况监控在所有端口通道冗余接口和单一物理接口上处于启用状态。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。 引入了以下命令：**health-check monitor-interface**。 引入了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群 > 集群接口运行状况监控**

功能	说明
DHCP 中继的 ASA 集群支持	现在可以在 ASA 集群上配置 DHCP 中继。通过使用客户端 MAC 地址散列，使客户端 DHCP 请求在集群成员中实现了负载均衡。仍然不支持 DHCP 客户端和服务器功能。 引入了以下命令：**debug cluster dhcp-relay** 未修改任何菜单项。
ASA 集群中的 SIP 检查支持	您现在可以在 ASA 集群上配置 SIP 检查。控制流可以在任何设备上创建（由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 引入了以下命令：**show cluster service-policy** 未修改任何菜单项。
路由功能	
基于策略的路由	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容，ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入了以下命令：**set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route** 和 **debug policy-route** 引入或修改了以下菜单项： **配置 > 设备设置 > 路由 > 路由映射 > 基于策略的路由配置 > 设备设置 > 路由 > 接口设置 > 接口**。
接口功能	
VXLAN 支持	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 引入了以下命令：**debug vxlan**、**default-mcast-group**、**encapsulation vxlan**、**inspect vxlan**、**interface vni**、**mcast-group**、**nve**、**nve-only**、**peer ip**、**segment-id**、**show arp vtep-mapping**、**show interface vni**、**show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、**source-interface**、**vtep-nve**、**vxlan port** 引入了以下菜单项： **配置 > 设备设置 > 接口设置 > 接口 > 添加 > VNI 接口配置 > 设备设置 > 接口设置 > VXLAN**
监控功能	

功能	说明
EEM 的内存跟踪	添加了一项新的调试功能来记录内存分配和内存使用情况，以响应内存日志记录封装事件。 引入或修改了以下命令：**memory logging**、**show memory logging**、**show memory logging include**、**event memory-logging-wrap** 修改了以下菜单项：**配置 > 设备管理 > 高级 > 嵌入式事件管理器 > 添加事件管理器 Applet > 添加事件管理器 Applet 事件**
对崩溃进行故障排除	**show tech-support** 命令输出和 **show crashinfo** 命令输出包含最新生成的 50 行系统日志。请注意，必须启用 **logging buffer** 命令才能出现这些结果。
远程访问功能	
支持 ECDHE-ECDSA 密码	TLSv1.2 增加了对以下密码的支持： • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 **注释** ECDSA 和 DHE 密码具有最高优先级。 引入了以下命令：**ssl ecdh-group**。 修改了以下菜单项：**配置 > 远程访问 VPN > 高级 > SSL 设置**。

功能	说明
无客户端 SSL VPN 会话 Cookie 访问限制	您现在可以防止第三方通过 JavaScript 等客户端侧脚本访问无客户端 SSL VPN 会话 Cookie。 **注释** 仅在思科 TAC 建议您使用此功能时再使用。启用此功能会引发安全风险，因为系统在以下无客户端 SSL VPN 功能不运行时不提供任何警告。 • Java 插件 • Java 重写工具 • 端口转发 • 文件浏览器 • 需要桌面应用（例如 MS Office 应用）的 Sharepoint 功能 • AnyConnect 网络启动 • Citrix Receiver、XenDesktop 和 Xenon • 其他不基于浏览器和浏览器插件的应用 引入了以下命令：**http-only-cookie**。 引入了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > HTTP Cookie**。 *9.2(3)* 中也包含此功能。
使用安全组标记的虚拟桌面访问控制	ASA 现在支持基于安全组标记的策略控制，从而可对内部应用和网站进行无客户端 SSL 远程访问。此功能将 Citrix 的虚拟桌面基础架构 (VDI) 与 XenDesktop 配合使用，将其用作交付控制器和 ASA 的内容转换引擎。 有关详细信息，请参阅以下 Citrix 产品文档： • 用于 XenDesktop 和 XenApp 的策略：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • 管理 XenDesktop 7 中的策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • 将组策略编辑器用于 XenDesktop 7 策略：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

功能	说明
为无客户端 SSL VPN 添加了 OWA 2013 功能支持	无客户端 SSL VPN 支持 OWA 2013 中除以下功能外的新功能： • 支持平板电脑和智能手机 • 离线模式 • Active Directory 联合身份验证服务 (AD FS) 2.0。ASA 和 AD FS 2.0 无法协商加密协议。 未修改任何命令。 未修改任何菜单项。
为无客户端 SSL VPN 添加了 Citrix XenDesktop 7.5 和 StoreFront 2.5 支持	无客户端 SSL VPN 支持访问 XenDesktop 7.5 和 StoreFront 2.5。 有关 XenDesktop 7.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html。 有关 StoreFront 2.5 功能的完整列表以及详细信息，请参阅 http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html。 未修改任何命令。 未修改任何菜单项。
定期证书身份验证	启用定期证书身份验证时，ASA 将存储从 VPN 客户端接收的证书链，并定期对它们进行身份验证。 引入或修改了以下命令：**periodic-authentication certificate**、**revocation-check** 和 **show vpn-sessiondb** 修改了以下菜单项： **配置 > 设备管理 > 证书管理 > 身份证书配置 > 设备管理 > 证书管理 > CA 证书**
证书到期警报	ASA 每 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。可以配置提醒和重现间隔。默认情况下，提醒将在到期之前 60 天启动，每 7 天重现一次。 引入或修改了以下命令：**crypto ca alerts expiration** 修改了以下菜单项： **配置 > 设备管理 > 证书管理 > 身份证书配置> 设备管理 > 证书管理 > CA 证书**
执行基本约束 CA 标记	默认情况下，不带 CA 标志的证书现在不能作为 CA 证书安装在 ASA 上。基本约束扩展标可确定证书的主题是否为 CA，及包含此证书的有效证书路径的最大深度。如果需要，可将 ASA 配置为允许安装这些证书。 引入了以下命令：**ca-check** 修改了以下菜单项：**配置 > 设备管理 > 证书管理 > CA 证书**

功能	说明
IKEv2 无效选择器通知配置	目前，如果 ASA 在 SA 上接收到入站数据包，并且数据包的报头字段与 SA 的选择器不一致，则ASA 会丢弃该数据包。您现在可以启用或禁用向对等方发送IKEv2通知。默认情况下会禁用发送此通知。 注释 AnyConnect 3.1.06060 和更高版本中支持此功能。 引入了以下命令：**crypto ikev2 notify invalid-selectors**
IKEv2 十六进制预共享密钥	您现在可以配置十六进制形式的 IKEv2 预共享密钥。 引入了以下命令：**ikev2 local-authentication pre-shared-key hex** 和 **ikev2 remote-authentication pre-shared-key hex**
管理功能	
ASDM 管理授权	现在可以单独为 HTTP 访问与 Telnet 和 SSH 访问配置管理授权。 引入了以下命令：**aaa authorization http console** 修改了以下菜单项：**配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权**
从证书配置 ASDM 用户名	当启用 ASDM 证书身份验证 (**http authentication-certificate**) 时，可以配置 ASDM 从证书提取用户名的方式；还可以在出现登录提示时启用用户名预填充功能。 引入了以下命令：**http username-from-certificate** 引入了以下菜单项：**配置 > 设备管理 > 管理访问 > HTTP 证书规则**。
terminal interactive 命令用于在 CLI 中输入 **?** 时启用或禁用帮助	通常，在 ASA CLI 中输入 **?** 时，会显示命令帮助。要能输入 **?** 作为命令中的文本（例如，将 ? 加入 URL 中），可以使用 **no terminal interactive** 命令禁用交互式帮助。 引入了以下命令：terminal interactive
REST API 功能	
REST API 版本 1.1	添加了对 REST API 1.1 版的支持。
对基于令牌的授权的支持（除了现有的基本授权之外）	客户端可以将登录请求发送到特定URL；如果发送成功，则会返回令牌（在响应报头中）。之后，客户端会将此令牌（在特殊请求报头中）用于发送其他 API 调用。在明确失效或到达空闲/会话超时之前，令牌一直有效。
有限的多情景支持	REST API 代理现在可以在多情景模式下启用；CLI 命令仅可以在系统情景模式下发出（与单情景模式的命令相同）。 直通 CLI API 命令可以用于配置任何情景，如下所示。 `https://<asa_admin_context_ip>/api/cli?context=<context_name>` 如果 **context** 参数不存在，则假设该请求会被定向到 **admin** 情景。

功能	说明
高级（精细）检测	支持对以下协议进行精细检查： • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP Options • NetBIOS Name Server over IP • SQL*Net

版本 9.3 的新功能

ASA 9.3(3)/ASDM 7.4(1) 的新功能

发布日期：**2015** 年 **4** 月 **22** 日

功能	说明
平台功能	
在系统日志消息中显示无效用户名	您现在可以在失败登录尝试的系统日志消息中显示无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。 引入了以下命令：**no logging hide username** ASDM 中不支持此功能。 此功能在版本 *9.4(1)* 中不可用。

ASA 9.3(2)/ASDM 7.3(3) 的新功能

发布日期：**2015** 年 **2** 月 **2** 日

功能	说明
平台功能	
ASA 5506-X 的 ASA FirePOWER 软件模块	在 ASA 5506-X 上，可以使用 ASDM 配置 ASA FirePOWER；无需单独的 FireSIGHT 管理中心，虽然可以用一个管理中心来代替 ASDM。 引入了以下菜单项： **主页 > ASA FirePOWER 控制面板** **主页 > ASA FirePOWER 报告** **配置 > ASA FirePOWER 配置** **监控 > ASA FirePOWER 监控**

ASA 9.3(2.200)/ASDM 7.3(2) 的新功能

发布日期：**2014** 年 **12** 月 **18** 日

注释 此版本仅支持 ASAv。

功能	说明
平台功能	
使用 KVM 和 Virtio 部署 ASAv	您可以使用基于内核的虚拟机 (KVM) 和 Virtio 虚拟接口驱动程序部署 ASAv。

ASA 9.3(2)/ASDM 7.3(2) 的新功能

发布日期：**2014** 年 **12** 月 **18** 日

功能	说明
平台功能	

功能	说明
ASA 5506-X	引入了 ASA 5506-X。 引入或修改了以下命令：**service sw-reset-button**、**upgrade rommon**、**show environment temperature accelerator**
ASA 5506-X 的 ASA FirePOWER 软件模块	在 ASA 5506-X 上，可以使用 ASDM 配置 ASA FirePOWER；无需单独的 FireSIGHT 管理中心，虽然可以用一个管理中心来代替 ASDM。**注意**：此功能要求具有 ASA 7.3(3)。 引入了以下菜单项： **主页 > ASA FirePOWER 控制面板** **主页 > ASA FirePOWER 报告** **配置 > ASA FirePOWER 配置** **监控 > ASA FirePOWER 监控**
使用流量重定向接口的 ASA FirePOWER 被动仅监控模式	现在可以将流量转发接口配置为向模块发送流量，以代替使用服务策略。在这种模块下，模块和 ASA 都不会影响流量。 完全支持以下命令：**traffic-forward sfr monitor-only**。仅可在 CLI 中进行此配置。
ASA 5585-X 中的混合级别 SSP	现在，您可以在 ASA 5585-X 中使用以下混合级别 SSP： • ASA SSP-10/ASA FirePOWER SSP-40 • ASA SSP-20/ASA FirePOWER SSP-60 要求：ASA SSP 在插槽 0 中，ASA FirePOWER SSP 在插槽 1 中
ASA REST API 1.0.1	增加了 REST API 来支持 ASA 的配置和管理主要功能。 引入或修改了以下命令：**rest-api image**、**rest-api agent**、**show rest-api agent**、**debug rest-api**、**show version**

功能	说明
支持 ASA 映像签名和验证	现在，ASA 映像使用数字签名进行签名。启动 ASA 后，系统将对数字签名进行验证。 引入了以下命令：**copy /noverify**、**verify /image-signature**、**show software authenticity keys**、**show software authenticity file**、**show software authenticity running**、**show software authenticity development**、**software authenticity development**、**software authenticity key add special**、**software authenticity key revoke special** ASDM 中不支持此功能。
加速安全路径负载均衡	加速安全路径 (ASP) 负载均衡机制允许 CPU 的多个核心接收并独立处理来自接口接收环的数据包，从而降低丢包率并提高吞吐量。 引入了以下命令：**asp load-balance per-packet-auto** 引入了以下菜单项：**配置 > 设备管理 > 高级 > ASP 负载均衡**
防火墙功能	
用于编辑 ACL 和对象的配置会话。 向前引用访问规则中的对象和 ACL。	现在，可以在单独的配置会话中编辑 ACL 和对象。还可以向前引用对象和 ACL，也就是说，可以为尚未存在的对象或 ACL 配置规则和访问组。 引入了以下命令：**clear configuration session**、**clear session**、**configure session**、**forward-reference**、**show configuration session** ASDM 中不支持此功能。
适用于信任验证服务、NAT66、CUCM 10.5(1) 和 8831 型号电话的 SIP 支持。	现在，可以在 SIP 检测中配置信任验证服务服务器。还可以使用 NAT66。使用 CUCM 10.5(1) 对 SIP 检测进行了测试。 引入了以下命令：**trust-verification-server**。 引入了以下菜单项：**配置 > 防火墙 > 对象 > 检查映射 > SIP > 添加/编辑 SIP 检查映射 > 细节 > TVS 服务器**
对 CUCM 10.5(1) 的统一通信支持	使用思科统一通信管理器 10.5(1) 测试和验证了 SIP 和 SCCP 检验。
远程访问功能	

功能	说明
Citrix VDI 的浏览器支持	现在，您可以使用基于 HTML 5 的浏览器解决方案访问 Citrix VDI，而无需在桌面设备上安装 Citrix Receiver 客户端。
用于 Mac OSX 10.9 的无客户端 SSL VPN	现在，我们在 Mac OSX 10.9 支持的所有浏览器上支持无客户端 SSL VPN 功能（例如重写程序、智能隧道和插件）。
与基于标准的第三方之间的互操作性，IKEv2 远程访问客户端	现在，我们通过基于标准的第三方 IKEv2 远程访问客户端（不仅仅是 AnyConnect）支持 VPN 连接。身份验证支持包括预共享密钥、证书以及通过可扩展身份验证协议 (EAP) 进行的用户身份验证。 引入或修改了以下命令：**ikev2 remote-authentication**、**ikev2 local-authentication**、**clear vpn-sessiondb**、**show vpn-sessiondb**、**vpn-sessiondb logoff** 引入或修改了以下菜单项： **向导 > IPSec IKEv2 远程访问向导**。 **配置 > 远程访问 VPN > 网络（客户端）访问 > IPSec (IKEv2) 连接配置文件** **配置 > 远程访问 VPN > 网络（客户端）访问 > IPSec (IKEv2) 连接配置文件 > 添加/编辑 > 高级 > IPSec** **监控 > VPN > VPN 统计信息 > 会话**
传输层安全 (TLS) 1.2 支持	现在，我们支持使用 TLS 版本 1.2 进行 ASDM、无客户端 SSVPN 和 AnyConnect VPN 的安全消息传送。 引入或修改了以下命令：**ssl client-version**、**ssl server-version**、**ssl cipher**、**ssl trust-point**、**ssl dh-group**、**show ssl**、**show ssl cipher**、**show vpn-sessiondb** 弃用了以下命令：**ssl encryption** 修改了以下菜单项： **配置 > 设备管理 > 高级 > SSL 设置** **配置 > 远程访问 VPN > 高级 > SSL 设置**

功能	说明
AnyConnect 4.0 支持 TLS 版本 1.2	现在，AnyConnect 4.0 支持 TLS 版本 1.2，增加了以下四种密码套件：DHE-RSA-AES256-SHA256、DHE-RSA-AES128-SHA256、AES256-SHA256 和 AES128-SHA256。
许可功能	
适用于 ASAv 的思科智能软件许可	通过智能软件许可，您可以购买和管理许可证池。与 PAK 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASA，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。 引入了以下命令：**clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level** 引入或修改了以下菜单项： **配置 > 设备管理 > 许可 > 智能许可** **配置 > 设备管理 > Smart Call-Home** **监控 > 属性 > 智能许可证**
高可用性功能	
锁定故障切换对中的备用设备或备用情景上的配置更改	现在可以锁定备用设备（主用/备用故障切换）或备用情景（主用/主用故障切换）上的配置更改，因此，除了正常的配置同步之外，将无法在备用设备上做出更改。 引入了以下命令：**failover standby config-lock** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 设置**

功能	说明
通过在内部网络之间设置 ASA 集群防火墙进行透明模式的 ASA 集群站点间部署	您现在可以在每个站点上的内部网络和网关路由器之间部署透明模式的集群（AKA 东西插入），并在站点之间扩展内部 VLAN。建议使用重叠传输虚拟化 (OTV)，但您可以使用任何可确保网关路由器的重叠 MAC 地址和 IP 地址在站点之间不泄漏的方法。使用 HSRP 等第一跃点冗余协议 (FHRP) 为网关路由器提供相同的虚拟 MAC 和 IP 地址。
接口功能	
流量区域	您可以将接口集合到一个流量区域以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的非对称路由。 **注释** 您不能将安全策略应用于已命名的区域；安全策略是基于接口的策略。当区域中的接口配置了相同的访问规则、NAT 和服务策略时，负载均衡和非对称路由将能够正常工作。 引入或修改了以下命令：**zone**、**zone-member**、**show running-config zone**、**clear configure zone**、**show zone**、**show asp table zone**、**show nameif zone**、**show conn long**、**show local-host zone**、**show route zone**、**show asp table routing**、**clear conn zone**、**clear local-host zone** 引入或修改了以下菜单项： **配置 > 设备设置 > 接口参数 > 区域** **配置 > 设备设置 > 接口参数 > 接口**
路由功能	
IPv6 的 BGP 支持	我们添加了对 IPv6 的支持。 引入或修改了以下命令：**address-family ipv6**、**bgp router-id**、**ipv6 prefix-list**、**ipv6 prefix-list description**、**ipv6 prefix-list sequence-number**、**match ipv6 next-hop**、**match ipv6 route-source**、**match ipv6- address prefix-list**、**set ipv6-address prefix -list**、**set ipv6 next-hop**、**set ipv6 next-hop peer-address** 引入了以下菜单项：**配置 > 设备设置 > 路由 > BGP > IPv6 系列**

功能	说明
监控功能	
SNMP MIB 和陷阱	CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 均已更新，以支持新的 ASA 5506-X。 ASA 5506-X 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 中。 ASA 现在支持 CISCO-CONFIG-MAN-MIB，它使您能够执行以下操作： • 了解已为特定配置输入的命令。 • 在运行配置发生更改后通知 NMS。 • 跟踪与上一次更改或保存运行配置相关的时间戳。 • 跟踪命令的其他更改，例如，终端详细信息和命令源。 修改了以下命令：**snmp-server enable traps** 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > SNMP > 配置陷阱 > SNMP 陷阱配置**
显示用于故障排除的路由摘要信息	**show tech-support detail** 命令中增加了 **show route-summary** 命令输出。
管理功能	
系统备份和恢复	现在，我们支持使用 CLI 进行完整的系统备份和恢复。 引入了以下命令：**backup**、**restore** 未修改任何菜单项。此功能已在 ASDM 中提供。

ASA 9.3(1)/ASDM 7.3(1) 的新功能

发布日期：**2014** 年 **7** 月 **24** 日

注释 ASA 5505 在此版本或更高版本中不受支持。ASA 9.2 版本是适用于 ASA 5505 的最终版本。

功能	说明
防火墙功能	
对 IPv6 的 SIP、SCCP 和 TLS 代理支持	现在使用 SIP、SCCP 和 TLS 代理（使用 SIP 或 SCCP）时可检查 IPv6 流量。 未修改任何命令。 未修改任何 ASDM 菜单项。
支持思科统一通信管理器 8.6	ASA 现在可与思科统一通信管理器 8.6 版本互操作（包括 SCCPv21 支持）。 未修改任何命令。 未修改任何 ASDM 菜单项。
适用于访问组和 NAT 的基于规则引擎的事务提交模型	一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。 引入了以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit** 引入了以下菜单项：**配置 > 设备管理 > 高级 > 规则引擎**
远程访问功能	
支持将 XenDesktop 7 用于无客户端 SSL VPN	我们添加了对 XenDesktop 7 的支持，可将其用于无客户端 SSL VPN。在自动登录状态下创建书签时，您现在可以指定登录页面 URL 或控制 ID。 未修改任何命令。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签**

功能	说明
AnyConnect 自定义属性增强功能	自定义属性用于定义和配置 ASA 中未包含的 AnyConnect 功能，例如延迟升级。自定义属性配置已得到增强，以允许多个值和更长的值，而且现在需要其类型、名称和值的规格。这些属性现在可以添加到动态访问策略和组策略。升级到 9.3.x 后，以前定义的自定义属性将更新至此增强配置格式。 引入或修改了以下命令：**anyconnect-custom-attr**、**anyconnect-custom-data** 和 **anyconnect-custom** 引入或修改了以下菜单项： **配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > AnyConnect 自定义属性** **配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > AnyConnect 自定义属性名称** **配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑 > 高级 > AnyConnect 客户端 > 自定义属性** **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加/编辑 > AnyConnect 自定义属性**
适用于桌面平台的 AnyConnect Identity Extensions (ACIDex)	ACIDex 是指 AnyConnect 终端属性（也称为移动终端安全评估），AnyConnect VPN 客户端会使用这些属性与 ASA 进行终端安全评估信息通信。动态访问策略使用这些终端属性向用户进行授权。 现在，AnyConnect VPN 客户端可为桌面操作系统（Windows、Mac OS X 和 Linux）提供平台识别，并支持可供 DAP 使用的 MAC 地址池。 未修改任何命令。 修改了以下菜单项：配置 > 远程访问 VPN > 动态访问策略 > 添加/编辑 > 添加/编辑（终端属性），选择 **AnyConnect** 作为**终端属性类型**。此外，**平台**下拉列表中添加了更多操作系统，“MAC 地址”也已改为 **MAC 地址池**。

功能	说明
针对 VPN 的 TrustSec SGT 分配	现在，当远程用户连接到设备时，系统会向 ASA 上的 SGT-IP 表添加 TrustSec 安全组标记 (SGT)。 引入了以下新命令：**security-group-tag value** 引入或修改了以下菜单项： **配置 > 远程访问 VPN > AAA/本地用户 > 本地用户 > 编辑用户 > VPN 策略** **配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加策略**
高可用性功能	
增强了对集群中模块运行状况监控的支持	我们增强了对集群中模块运行状况监控的支持。 修改了以下命令：**show cluster info health** 未修改任何 ASDM 菜单项。
禁用硬件模块的运行状况监控	默认情况下，ASA 会监控 ASA FirePOWER 模块等已安装硬件模块的运行状况。如果您不希望硬件模块故障触发故障切换，则可以禁用模块监控。 修改了以下命令：**monitor-interface service-module** 修改了以下菜单项：**配置 > 设备管理 > 高可用性和可扩展性 > 故障切换 > 接口**
平台功能	

功能	说明
ASP 负载均衡	**asp load-balance per-packet** 命令中新增的 **auto** 选项使 ASA 能够以自适应方式在每个接口接收环上开启和关闭每数据包 ASP 负载均衡。这一自动机制可检测是否引入了不对称的流量，有助于避免以下问题： • 因偶发的流量高峰而造成溢出 • 因大量流量过度订用特定接口接收环而造成溢出 • 因相对严重过载的接口接收环而造成溢出（这种情况下，一个核心无法维持负载） 引入或修改了以下命令：**asp load-balance per-packet auto**、**show asp load-balance per-packet**、**show asp load-balance per-packet history** 和 **clear asp load-balance history** 未修改任何 ASDM 菜单项。
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB 现在支持 ASASM。
接口功能	
透明模式的网桥组最大数量增加到 250	网桥组最大数量从 8 个增加到 250 个网桥组。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 修改了以下命令：**interface bvi**、**bridge-group** 修改了以下菜单项： **配置 > 设备设置 > 接口** **配置 > 设备设置 > 接口 > 添加/编辑桥接组接口** **配置 > 设备设置 > 接口 > 添加/编辑接口**
路由功能	
BGP 对 ASA 集群的支持	增加了对 BGP 用于 ASA 集群的支持。 引入了以下新命令：bgp router-id clusterpool 修改了以下菜单项：**配置 > 设备设置 > 路由 > BGP > IPv4 系列 > 通用**

功能	说明
不间断转发的 BGP 支持	添加了对 BGP 不间断转发的支持。 引入了以下新命令：bgp graceful-restart、neighbor ha-mode graceful-restart 修改了以下菜单项： **配置 > 设备设置 > 路由 > BGP > 通用** **配置 > 设备设置 > 路由 > BGP > IPv4 系列 > 邻居** **监控 > 路由 > BGP 邻居**
通告映射的 BGP 支持	添加了对 BGPv4 通告映射的支持。 引入了以下新命令：neighbor advertise-map 修改了以下菜单项：**配置 > 设备设置 > 路由 > BGP > IPv4 系列 > 邻居 > 添加 BGP 邻居 > 路由**
OSPF 支持不间断转发 (NSF)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 添加了以下命令：capability、nsf cisco、nsf cisco helper、nsf ietf、nsf ietf helper、nsf ietf helper strict-lsa-checking、graceful-restart、graceful-restart helper、graceful-restart helper strict-lsa-checking 添加了以下菜单项： **配置 > 设备设置 > 路由 > OSPF > 设置 > NSF 属性** **配置 > 设备设置 > 路由 > OSPFv3 > 设置 > NSF 属性**
AAA 功能	

功能	说明
第 2 层安全组标记实施	现在，可以使用结合了以太网标记的安全组标记来实施策略。SGT 加以太网标记，也称为第 2 层 SGT 强制，使 ASA 能够使用思科专有以太网帧 (Ether Type 0x8909) 在千兆以太网接口上发送和接收安全组标记，从而将源安全组标记插入纯文本以太网帧。 引入或修改了以下命令：**cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、**clear configure all** 和 **write memory** 修改了以下菜单项： **配置 > 设备设置 > 接口 > 添加接口 > 高级** **配置 > 设备设置 > 接口 > 添加冗余接口 > 高级** **配置 > 设备设置 > 添加以太网接口 > 高级** **向导 > 数据包捕获向导** **工具 > 数据包跟踪器**
删除 AAA Windows NT 域身份验证	取消了对远程访问 VPN 用户的 NTLM 支持。 弃用了以下命令：aaa-server protocol nt 修改了以下菜单项：**配置 > 远程访问 VPN > AAA/本地用户 > AAA 服务器组 > 添加 AAA 服务器组**
ASDM 身份证书向导	使用当前 Java 版本时，ASDM 启动程序需要可信任证书。满足证书要求的一个简单方法就是安装自签身份证书。ASDM 身份证书向导可简化创建自签名身份证书的过程。首次启动 ASDM 且没有可信任证书时，系统会提示通过 Java Web Start 启动 ASDM。这时，这个新向导会自动启动。创建身份证书后，您需要将其注册至 Java 控制面板。有关说明，请参阅 https://www.cisco.com/go/asdm-certificate。 添加了以下菜单项：**向导 > ASDM 身份证书向导**
监控功能	
监控物理接口的汇聚流量	**show traffic** 命令输出经过更新，现在包括物理接口汇聚流量信息。要启用此功能，必须先输入 **sysopt traffic detailed-statistics** 命令。

功能	说明
show tech support 改进	**show tech support** 命令现在包括 **show resource usage count all 1** 输出，包括有关转换、连接、检查、系统日志等的信息。这些信息有助于诊断性能问题。 修改了以下命令：**show tech support** 未修改任何菜单项。
ASDM 可以将僵尸网络流量过滤器报告保存为 HTML 而不是 PDF	ASDM 不能再将僵尸网络流量过滤器报告保存为 PDF 文件；可以改为将其保存为 HTML。 修改了以下菜单项：**监控 > 僵尸网络流量过滤器**

版本 9.2 的新功能

ASA 9.2(4)/ASDM 7.4(3) 的新功能

发布日期：**2015** 年 **6** 月 **16** 日

功能	说明
平台功能	
在系统日志消息中显示无效用户名	您现在可以在失败登录尝试的系统日志消息中显示无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。 引入了以下命令：**no logging hide username** 修改了以下菜单项：**配置 > 设备管理 > 日志 > 系统日志设置**
DHCP 功能	
DHCP 中继服务器会验证用于应答的 DHCP 服务器标识符	如果 ASA DHCP 中继服务器收到来自错误的 DHCP 服务器的应答，现在它会验证该应答是否来自正确的服务器，然后对应答做出反应。
监控功能	

功能	说明
NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 将允许 Xlate count 轮询。	添加对 NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 的支持以支持 SNMP xlate_count 和 max_xlate_count。 此数据等同于 **show xlate count** 命令。 未修改任何 ASDM 菜单项。 同样适用于 *8.4(5)* 和 *9.1(5)* 版本。

ASA 9.2(3)/ASDM 7.3(1.101) 的新功能

发布日期：**2014** 年 **12** 月 **15** 日

功能	说明
远程访问功能	
无客户端 SSL VPN 会话 Cookie 访问限制	您现在可以防止第三方通过 JavaScript 等客户端侧脚本访问无客户端 SSL VPN 会话 Cookie。 **注释** 仅在思科 TAC 建议您使用此功能时再使用。启用此功能会引发安全风险，因为系统在以下无客户端 SSL VPN 功能不运行时不提供任何警告。 • Java 插件 • Java 重写工具 • 端口转发 • 文件浏览器 • 需要桌面应用（例如 MS Office 应用）的 Sharepoint 功能 • AnyConnect 网络启动 • Citrix Receiver、XenDesktop 和 Xenon • 其他不基于浏览器和浏览器插件的应用 引入了以下命令：**http-only-cookie** 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > HTTP Cookie**

ASA 9.2(2.4)/ASDM 7.2(2) 的新功能

发布日期：2014 年 8 月 12 日

注释 由于内部版本问题，从 Cisco.com 中删除了版本 9.2(2)；请升级到版本 9.2(2.4) 或更高版本。

功能	说明
平台功能	
ASA 5585-X（所有型号）支持匹配的 ASA FirePOWER SSP 硬件模块。 ASA 5512-X 到 ASA 5555-X 支持 ASA FirePOWER 软件模块。	ASA FirePOWER 模块提供下一代防火墙服务，包括下一代 IPS (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤及高级恶意软件保护 (AMP)。您可以在单情景或多情景模式以及路由或透明模式下使用该模块。 引入或修改了以下命令：**capture interface asa_dataplane**、**debug sfr**、**hw-module module 1 reload**、**hw-module module 1 reset**、**hw-module module 1 shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**session sfr**、**sfr**、**show asp table classify domain sfr**、**show capture**、**show conn**、**show module sfr**、**show service-policy** 和 **sw-module sfr**。 引入了以下菜单项： **主页 > ASA FirePOWER 状态** **导向 > 启动导向 > ASA FirePOWER 基本配置** **配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 > 规则行为 > ASA FirePOWER 检查**
远程访问功能	
面向无客户端 SSL VPN 提供 Windows 8.1 和 Windows 7 对 Internet Explorer 11 浏览器的支持	面向无客户端 SSL VPN 增加了 Windows 8.1 和 Windows 7 对 Internet Explorer 11 浏览器的支持。 未修改任何命令。 未修改任何菜单项。

ASA 9.2(1)/ASDM 7.2(1) 的新功能

发布日期：**2014** 年 **4** 月 **24** 日

注释 ASA 5510、ASA 5520、ASA 5540、ASA 5550 和 ASA 5580 在此版本或更高版本中不受支持。ASA 9.1 版本是适用于这些型号的最终版本。

功能	说明
平台功能	
思科自适应安全虚拟设备 (ASAv) 已作为一个新平台添加到 ASA 系列中。	ASAv 可为虚拟环境带来完整的防火墙功能，从而确保数据中心流量和多租户环境的安全。ASAv 在 VMware vSphere 上运行。您可以使用 ASDM 或 CLI 管理和监控 ASAv。
路由功能	

功能	说明
BGP 支持	

功能	说明
	我们现在支持边界网关协议 (BGP)。BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。 引入了以下命令：**router bgp**、**bgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、**show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、**network**。 修改了以下命令：**show route**、**show route summary**、**show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。 引入了以下菜单项： **配置 > 设备设置 > 路由 > BGP** **监控 > 路由 > BGP 邻居**、**监控 > 路由 > BGP 路由** 修改了以下菜单项： **配置 > 设备设置 > 路由 > 静态路由 > 添加 > 添加静态路由**

功能	说明
	配置 > 设备设置 > 路由 > 路由器映射 > 添加 > 添加路由映射
Null0 接口的静态路由	向 Null0 接口发送流量会导致丢弃发往指定网络的数据包。此功能有助于为 BGP 配置远程触发黑洞 (RTBH)。 修改了以下命令：**route**。 修改了以下菜单项：配置 > 设备设置 > 路由 > 静态路由 > 添加 > 添加静态路由
OSPF 支持快速呼叫	OSPF 支持快速呼叫数据包功能，从而产生在 OSPF 网络中导致更快收敛的配置。 修改了以下命令：**ospf dead-interval** 修改了以下菜单项：配置 > 设备设置 > 路由 > OSPF > 接口 > 编辑 OSPF 接口高级属性
新的 OSPF 计时器	添加了新 OSPF 计时器；弃用了旧 OSPF 计时器。 引入了以下命令：**timers lsa arrival**、**timers pacing**、**timers throttle**。 删除了以下命令：**timers spf**、**timers lsa-grouping-pacing** 修改了以下菜单项：**配置 > 设备设置 > 路由 > OSPF > 设置 > 编辑 OSPF 进程高级属性**
使用 ACL 进行 OSPF 路由过滤	现在支持使用 ACL 筛选路由。 引入了以下命令：**distribute-list** 引入了以下菜单项：配置 > 设备设置 > 路由 > OSPF > 过滤规则 > 添加过滤规则
OSPF 监控增强功能	添加了其他 OSPF 监控信息。 修改了以下命令：**show ospf events**、**show ospf rib**、**show ospf statistics**、**show ospf border-routers [detail]**、**show ospf interface brief**
OSPF 重新分发 BGP	添加了 OSPF 重新分发功能。 添加了以下命令：**redistribute bgp** 添加了以下菜单项：配置 > 设备设置 > 路由 > OSPF > 重新分发

功能	说明
EIGRP 自动摘要	默认情况下，现已针对 EIGRP 禁用 Auto-Summary 字段。 修改了以下菜单项：配置 > 设备设置 > 路由 > EIGRP > 设置 > 编辑 EIGRP 进程高级属性
高可用性功能	
对透明模式支持集群成员位于不同的地理位置（站点间）	在透明防火墙模式下使用跨网络 EtherChannel 模式时，集群成员现在可位于不同的地理位置。不支持在路由防火墙模式下使用跨网络 EtherChannel 的站点间集群。 未修改任何命令。 未修改任何 ASDM 菜单项。
对集群的静态 LACP 端口优先级支持	有些交换机不支持 LACP 动态端口优先级（活动链路和备用链路）。您现在可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。您还应遵循以下准则： • 集群控制链路路径上的网络要素不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。 • 端口通道绑定中断时间不得超过配置的 keepalive 间隔。 引入了以下命令：**clacp static-port-priority**。 修改了以下菜单项：配置 > 设备管理 > 高可用性和扩展性 > ASA 集群

功能	说明
支持跨网络 EtherChannel 中有 32 条活动链路，以实现集群	ASA EtherChannel 现在最多可支持 16 条活动链路。借助跨网络 EtherChannel，此功能已扩展为在使用 vPC 中的两台交换机且禁用动态端口优先级时，最多可在整个集群中支持 32 条活动链路。交换机必须支持有 16 条活动链路的 EtherChannel；例如，带 F2 系列 10 千兆以太网模块的思科 Nexus 7000。 对于 VSS 或 vPC 中支持 8 条活动链路的交换机，您现在可以在跨网络 EtherChannel 中配置 16 条活动链路（每台交换机各连接 8 条）。以前，即便使用 VSS/vPC，跨网络 EtherChannel 也只支持 8 条活动链路和 8 条备用链路。 **注释** 如果您要在跨网络 EtherChannel 中使用 8 条以上的活动链路，则无法同时使用备用链路；要支持 9 至 32 条活动链路，需要您禁用允许使用备用链路的 cLACP 动态端口优先级。 引入了以下命令：**clacp static-port-priority**。 修改了以下菜单项：配置 > 设备管理 > 高可用性和扩展性 > ASA 集群
对 ASA 5585-X 支持 16 个集群成员	ASA 5585-X 现在支持由 16 台设备组成的集群。 未修改任何命令。 未修改任何 ASDM 菜单项。
支持与思科 Nexus 9300 的集群	ASA 支持在连接到思科 Nexus 9300 时的集群。
远程访问功能	

功能	说明
ISE 授权更改	ISE 授权变更 (CoA) 功能提供一种机制，以在建立身份验证、授权和记帐 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，可以将 CoA 数据包从 ISE 直接发送到 ASA，以重新初始化身份验证并应用新策略。不再需要内联安全状态实施点 (IPEP) 来为与 ASA 建立的每个 VPN 会话应用访问控制列表 (ACL)。 当终端用户请求 VPN 连接时，ASA 将会面向 ISE 对该用户进行身份验证，并会收到一个提供对网络的有限访问的用户 ACL。系统向 ISE 发送记帐启动消息以注册会话。直接在 NAC 代理和 ISE 之间进行终端安全评估。此过程对 ASA 透明。ISE 通过 CoA“policy push”向 ASA 发送策略更新。这样可以识别提供更多网络访问权限的新用户 ACL。在连接的生存期内，可能会通过后续 CoA 更新进行对于 ASA 而言透明的其他策略评估。 引入了以下命令：**dynamic-authorization**、**authorize-only**、**debug radius dynamic-authorization**。 修改了以下命令：**without-csd** [**anyconnect**]、**interim-accounting-update** [**periodic** [*interval*]]。 删除了以下命令：**nac-policy**、**eou**、**nac-settings**。 修改了以下菜单项：配置 > 远程访问 VPN > AAA/本地用户 > AAA 服务器组 > 添加/编辑 AAA 服务器组
改进了无客户端重写器 HTTP 1.1 压缩处理	重写器已更改，以便在客户端支持压缩内容，并且内容不会被重写时，它将从服务器接受压缩内容。如果内容必须重写，并且被确定为正被压缩，则内容将被解压，重写，并且如果客户端支持，还会重新进行压缩。 未引入或修改任何命令。 未引入或修改任何 ASDM 菜单项。

功能	说明
OpenSSL 升级	ASA 上的 OpenSSL 版本将更新为版本 1.0.1e。 **注释** 我们禁用了心跳选项，因此 ASA 不容易受到 Heartbleed Bug 的攻击。 未引入或修改任何命令。 未引入或修改任何 ASDM 菜单项。
接口功能	
一个 EtherChannel 中支持 16 个主用链路	现在，一个 EtherChannel 中最多可以配置 16 个主用链路。以前，可以有 8 个主用链路和 8 个备用链路。确保您的交换机可以支持 16 个主用链路（例如，可使用带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。 **注释** 如果从早期 ASA 版本进行升级，则为了实现兼容，可将最大主用接口数设置为 8（**lacp max-bundle** 命令）。 修改了以下命令：**lacp max-bundle** 和 **port-channel min-bundle**。 修改了以下菜单项：配置 > 设备设置 > 接口 > 添加/编辑 EtherChannel 接口 > 高级。
最大 MTU 现为 9198 字节	ASA 可使用的最大 MTU 为 9198 字节（通过 CLI 帮助可检查型号的确切限制）。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。如果您的 MTU 设置为高于 9198 的值，则升级后 MTU 会自动降低。在某些情况下，这种 MTU 变化可能导致 MTU 不匹配；请务必将连接的所有设备设置为使用新的 MTU 值。 修改了以下命令：**mtu** 修改了以下菜单项：**配置 > 设备设置 > 接口设置 > 接口 > 编辑接口 > 高级** 同样适用于 *9.1.(6)* 版本。
监控功能	

功能	说明
嵌入式事件管理器 (EEM)	EEM 功能使您可以调试问题并提供用于故障排除的通用日志记录。EEM 通过执行操作对 EEM 系统中的事件作出响应。其中涉及两个组件：EEM 触发的事件；用于定义操作的事件管理器小应用程序。您可以为每个事件管理器小应用程序添加多个事件，从而触发小应用程序调用配置的操作。 引入或修改了以下命令：**event manager applet**、**description**、**event syslog id**、**event none**、**event timer**、**event crashinfo**、**action cli command**、**output**、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem**。 引入了以下菜单项：配置 > 设备管理 > 高级 > 嵌入式事件管理器、监控 > 属性 > EEM Applets。
SNMP 主机、主机组和用户列表	最多可以添加 4000 台主机。支持的活动轮询目标数量为 128。您可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。 引入或修改了以下命令：**snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server**。 修改了以下菜单项：配置 > 设备管理 > 管理访问 > SNMP。
SNMP 消息大小	SNMP 发送的消息大小限制已增大为 1472 字节。
SNMP OID 和 MIB	ASA 现在支持 cpmCPUTotal5minRev OID。 ASAv 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 中。 CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 均已更新，以支持新的 ASAv 平台。
管理功能	

功能	说明
改进的一次性密码身份验证	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。**aaa authorization exec** 命令中添加了 **auto-enable** 选项。 修改了以下命令：**aaa authorization exec**。 修改了以下菜单项：配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权。
自动更新服务器证书验证默认已启用	现在，默认情况下会启用自动更新服务器证书验证；对于新的配置，必须明确禁用证书验证。如果您是从较早版本升级且未启用证书验证，则不会启用证书验证，并会显示以下警告： `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 系统将自动迁移配置，以明确配置无验证： **auto-update server no-verification** 修改了以下命令：**auto-update server** [**verify-certificatee** | **no-verification**]。 修改了以下菜单项：配置 > 设备管理 > 系统/映像配置 > 自动更新 > 添加自动更新服务器。

版本 9.1 的新功能

ASA 9.1(7.4)/ASDM 7.5(2.153) 的新功能

发布日期：**2016** 年 **2** 月 **19** 日

注释 由于内部版本问题，从 Cisco.com 中删除了版本 9.1(7)；请升级到版本 9.1(7.4) 或更高版本。

功能	说明
远程访问功能	

功能	说明
无客户端 SSL VPN 会话 Cookie 访问限制	您现在可以防止第三方通过 JavaScript 等客户端侧脚本访问无客户端 SSL VPN 会话 Cookie。 注释 仅在思科 TAC 建议您使用此功能时再使用。启用此功能会引发安全风险，因为系统在以下无客户端 SSL VPN 功能不运行时不提供任何警告。 • Java 插件 • Java 重写工具 • 端口转发 • 文件浏览器 • 需要桌面应用（例如 MS Office 应用）的 Sharepoint 功能 • AnyConnect 网络启动 • Citrix Receiver、XenDesktop 和 Xenon • 其他不基于浏览器和浏览器插件的应用 引入了以下命令：**http-only-cookie**。 引入了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > HTTP Cookie**。 此功能同样适用于 *9.2(3)* 和 *9.4(1)* 版本。
可配置 SSH 加密和 HMAC 算法	用户可以在执行SSH加密管理时选择密码模式，并且可以为不同的密钥交换算法配置HMAC和加密。 引入了以下命令：**ssh cipher encryption** 和 **ssh cipher integrity**。 无 ASDM 支持。

功能	说明

默认情况下，无客户端 SSL VPN 为禁用状态。	现在，无客户端 SSL VPN 缓存默认为禁用状态。禁用 SSL VPN 缓存可增强稳定性。若要启用缓存，您必须手动操作。
	
	`webvpn`
	`cache`
	`no disable`
	
	修改了以下命令：**cache**
	
	修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 内容缓存**
	
	同样适用于 *9.5(2)* 版本。

IPV6 支持 HTTP 重定向	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 为以下命令添加了功能：**http redirect** 为以下菜单项添加了功能：**配置 > 设备管理 > HTTP 重定向**
管理功能	

show tech support 改进	**show tech support** 命令现在：
	
	• 包括 **dir all-filesystems** 输出 - 该输出可在以下情况中起作用：
	  • SSL VPN 配置：检查所需资源是否在 ASA 上
	  • 故障：检查日期时间戳及是否存在故障文件
	
	• 包括 **show resource usage count all 1** 输出 - 包括有关转换、连接、检查、系统日志等的信息。这些信息有助于诊断性能问题。
	
	• 删除 **show kernel cgroup-controller detail** 输出 - 该命令输出依然存在于 **show tech-support detail** 的输出中。
	
	修改了以下命令：**show tech support**
	
	未修改任何菜单项。

功能	说明
支持 CISCO-ENHANCED-MEMPOOL-MIB 中的 cempMemPoolTable	现在支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，监控受管系统上所有物理实体的条目。 注释 CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持报告 RAM 超过 4GB 的平台上的内存。 未添加或修改任何命令。 未添加或修改任何菜单项。

ASA 9.1(6)/ASDM 7.1(7) 的新功能

发布日期：**2015** 年 **3** 月 **2** 日

功能	说明
接口功能	
最大 MTU 现为 9198 字节	ASA 可使用的最大 MTU 为 9198 字节（通过 CLI 帮助可检查型号的确切限制）。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。如果您的 MTU 设置为高于 9198 的值，则升级后 MTU 会自动降低。在某些情况下，这种 MTU 变化可能导致 MTU 不匹配；请务必将连接的所有设备设置为使用新的 MTU 值。 修改了以下命令：**mtu** 修改了以下菜单项：**配置 > 设备设置 > 接口设置 > 接口 > 编辑接口 > 高级**

ASA 9.1(5)/ASDM 7.1(6) 的新功能

发布日期：**2014** 年 **3** 月 **31** 日

功能	说明
管理功能	

功能	说明
安全复制客户端	ASA 现在支持安全复制 (SCP) 客户端与 SCP 服务器进行双向文件传输。 引入了以下命令：**ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash** 和 **ssh stricthostkeycheck**。 修改了以下命令：**copy scp**。 修改了以下菜单项： 工具 > 文件管理 > 文件传输 > 在远程服务器与 Flash 配置之间> 设备管理 > 管理访问 > 文件访问 > 源复制 (SCP) 服务器
改进的一次性密码身份验证	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。**aaa authorization exec** 命令中添加了 **auto-enable** 选项。 修改了以下命令：**aaa authorization exec**。 修改了以下菜单项：配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权。
防火墙功能	
访问组的规则引擎事务提交模型	一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。 引入了以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**. 引入了以下菜单项：配置 > 设备管理 > 高级 > 规则引擎。
监控功能	

功能	说明
SNMP 主机、主机组和用户列表	最多可以添加 4000 台主机。支持的活动轮询目标数量为 128。您可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。 引入或修改了以下命令：**snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > SNMP**。
NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 将允许 Xlate count 轮询。	添加对 NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 的支持以支持 SNMP xlate_count 和 max_xlate_count。 此数据等同于 **show xlate count** 命令。 未修改任何 ASDM 菜单项。 同样适用于 *8.4(5)* 版本。
远程访问功能	
AnyConnect DTLS 单会话性能改进	当通过 AnyConnect DTLS 连接发送大量丢弃的数据包时，UDP 流量（如流媒体）会受到影响。例如，这可能导致流式视频播放不佳或完全停止流。之所以会这样，是流控制队列相对较小。 我们增加了 DTLS 流控制队列的大小，并通过减少管理加密队列大小来消除这一点。对于 TLS 会话，加密命令的优先级已增加到“高”至已对此更改予以弥补。现在，对于 DTLS 和 TLS 会话，即使丢弃了数据包，该会话仍将继续。这样可以防止媒体流关闭，并确保丢弃的数据包的数量可与其他连接方法相媲美。 未修改任何命令。 未修改任何 ASDM 菜单项。

功能	说明
Webtype ACL 增强功能	引入了 URL 规范化。URL 规范化是包括路径规范化、大小写规范化和方案规范化在内的一项额外安全功能。系统在比较 URL 之前，会先对在 ACE 和门户地址栏中指定的 URL 进行规范化；在过滤 webvpn 流量时，会以规范化 URL 比较结果为依据。 例如，如果您有一个 https://calo.cisco.com/checkout/Devices 书签，则 Web 类型 acl 下的 https://calo.cisco.com/checkout/Devices/* 似乎是匹配的。但是，由于引入了 URL 规范化，因此在进行比较之前，书签 URL 和 Web 类型的 ACL 都将被规范化。在本例中，https://calo.cisco.com/checkout/Devices 被规范化为 https://calo.cisco.com/checkout/Devices，https://calo.cisco.com/checkout/Devices/* 保持不变，因此两者不匹配。 您必须配置以下内容才能满足要求： • 要允许书签 URL (https://calo.cisco.com/checkout/Devices)，请将 ACL 配置为允许该 URL • 要允许“设备”文件夹中的URL，请将 ACL 配置为允许 https://calo.cisco.com/checkout/Devices/* 未修改任何命令。 未修改任何 ASDM 菜单项。

ASA 9.1(4)/ASDM 7.1(5) 的新功能

发布日期：**2013** 年 **12** 月 **9** 日

功能	说明
远程访问功能	

功能	说明
HTML5 WebSocket 代理	HTML5 WebSocket 提供客户端与服务器之间的持久连接。在建立无客户端 SSL VPN 连接期间，握手将作为 HTTP 升级请求出现在服务器上。现在，ASA 会将此请求通过代理发送到后端，并在握手完成后提供中继。网关模式当前不受支持。 未修改任何命令。 未修改任何 ASDM 菜单项。
适用于 IKEv2 的内部 IPv6	IPv6 流量现在可以通过 IPSec/IKEv2 隧道进行隧道传送。这样，ASA 至 AnyConnect VPN 的连接完全兼容 IPv6。当 IPv4 和 IPv6 流量都在隧道中并且客户端和前端都支持 GRE 时，使用 GRE。对于单一的流量类型，或者当客户端或前端不支持 GRE 时，我们直接使用 IPSec。 注释 此功能需要 AnyConnect 客户端版本 3.1.05 或更高版本。 **show ipsec sa** 和 **show vpn-sessiondb detail anyconnect** 命令的输出已更新来反映分配的 IPv6 地址且指出执行 IKEv2 双流量时的 GRE 传输模式安全关联。 **vpn-filter** 命令现在必须用于 IPv4 和 IPv6 ACL。如果使用我们不推荐的 **ipv6-vpn-filter** 命令来配置 IPv6 ACL，连接将终止。 未修改任何 ASDM 菜单项。
运行 Citrix Server Mobile 的移动设备具有附加连接选项	对通过 ASA 连接到 Citrix 服务器的移动设备的支持现在包括选择隧道组以及用于授权的 RSA Securid。通过允许移动用户选择不同的隧道组，管理员可以使用不同的身份验证方法。 我们引入了 **application-type** 命令，以在 Citrix 接收器用户未选择隧道组时为 VDI 连接配置默认隧道组。**Vdi** 命令中添加了 **none** 操作以面向特定组策略或用户禁用 VDI 配置。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > VDI 访问**。

功能	说明
拆分隧道支持排除了 ACL	VPN流量的拆分隧道功能已经过增强，既支持排除 ACL，也支持包括 ACL。之前忽略了排除 ACL。 注释 此功能需要 AnyConnect 客户端版本 3.1.03103 或更高版本。 未修改任何命令。 未修改任何 ASDM 菜单项。
高可用性和可扩展性功能	
ASA 5500-X 对集群的支持	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 现在支持由 2 台设备组成的集群。默认情况下，在基础许可证中支持两台设备的集群；对于 ASA 5512-X，您需要增强型安全许可证。 未修改任何命令。 未修改任何 ASDM 菜单项。
提高了 VSS 和 vPC 对运行状况检查监控的支持	如果将集群控制链路配置为 EtherChannel（推荐）且它连接到 VSS 或 vPC 对，则您现在可提高运行状况检查监控的稳定性。对某些交换机（例如，Nexus 5000）而言，当 VSS/vPC 中的一台设备正在关闭或启动时，连接到这些交换机的 EtherChannel 成员接口可能看似对 ASA 打开，但在交换机端却并未传输流量。如果您将 ASA 保持时间超时设置为一个较低值（如 0.8 秒），则可将 ASA 从集群中匿名删除，ASA 会将 keepalive 消息发送到这些 EtherChannel 接口之一。当您启用 VSS/vPC 运行状况检查功能时，ASA 将在集群控制链路中的所有 EtherChannel 接口上泛洪 keepalive 消息，以确保至少有一台交换机可以收到这些消息。 修改了以下命令：**health-check** [**vss-enabled**] 修改了以下菜单项：配置 > 设备管理 > 高可用性和扩展性 > ASA 集群

功能	说明
支持集群成员位于不同的地理位置（站点间）；仅限独立接口模式	使用独立接口模式时，集群成员现在可位于不同的地理位置。有关站点间指南，请参阅配置指南。 未修改任何命令。 未修改任何 ASDM 菜单项。
支持与思科 Nexus 5000 和思科 Catalyst 3750-X 的集群	ASA 支持在连接到思科 Nexus 5000 和思科 Catalyst 3750-X 时的集群。 修改了以下命令：**health-check** [**vss-enabled**] 修改了以下菜单项：配置 > 设备管理 > 高可用性和扩展性 > ASA 集群
基本操作功能	
DHCP 重新绑定功能	在 DHCP 重新绑定阶段，客户端会尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不会重新绑定到备用服务器。 引入了以下命令：**show ip address dhcp lease proxy**、**show ip address dhcp lease summary** 和 **show ip address dhcp lease server**。 引入了以下菜单项：**监控 > 接口 > DHCP > DHCP 租用信息**。
故障排除功能	
Crashinfo 转储包括 AK47 框架信息	现在，应用内核层 4 到 7 (AK47) 框架相关的信息在 crashinfo 转储中提供。**debug menu** 命令中添加了一个新的选项 **ak47**，用于帮助调试 AK47 框架问题。crashinfo 转储中与框架相关的信息包括以下内容： • 创建 AK47 实例。 • 销毁 AK47 实例。 • 使用内存管理器帧生成 crashinfo。 • 在光纤堆栈溢出后生成 crashinfo。 • 在局部变量溢出后生成 crashinfo。 • 在发生异常后生成 crashinfo。

ASA 9.1(3)/ASDM 7.1(4) 的新功能

发布日期：**2013** 年 **9** 月 **18** 日

功能	说明
模块功能	
在多情景模式下支持 ASA CX 模块	您现在可以在 ASA 上按情景配置 ASA CX 服务策略。 **注释** 虽然您可以配置每情景 ASA 服务策略，但是，ASA CX 模块自身（在 PRSM 中配置）是一台单一情景模式设备；来自 ASA 的情景特定流量将根据通用 ASA CX 策略来检查。 需要 ASA CX 9.2(1) 或更高版本。 未修改任何命令。 未修改任何 ASDM 菜单项。
ASA CX SSP-40 和 -60 支持带 SSP-40 和 -60 的 ASA 5585-X	ASA CX SSP-40 和 -60 模块可以与匹配级别带 SSP-40 和 -60 的 ASA 5585-X 一起使用。 需要 ASA CX 9.2(1) 或更高版本。 未修改任何命令。 未修改任何菜单项。
过滤在 ASA CX 背板上捕获的数据包	您现在可以使用关键字 **match** 或 **access-list** 与 **capture interface asa_dataplane** 命令来过滤在 ASA CX 背板上捕获的数据包。ASA CX 模块的特定控制流量不受访问列表或匹配过滤的影响；ASA 可以捕获所有控制流量。在多情景模式下，按情景配置数据包捕获。请注意，在多情景模式下的所有控制流量仅流向系统执行空间。由于只有控制流量无法使用访问列表或匹配来过滤，因此这些选项在系统执行空间中不可用。 需要 ASA CX 9.2(1) 或更高版本。 修改了以下命令：**capture interface asa_dataplane**。 一个新的选项“使用背板通道”添加到了数据包捕获向导中的“进口流量选择器”屏幕和“出口选择器”屏幕中，以启用对在 ASA CX 背板上捕获的数据包进行过滤。

功能	说明
监控功能	
能够查看前 10 个内存用户	现在，您可以查看已分配的排名靠前的容器大小以及每个已分配容器大小的前 10 台 PC。以前，您必须输入多个命令才能查看这些信息（**show memory detail** 命令和 **show memory binsize** 命令）；新命令提供了更快分析内存问题的方式。 引入了以下命令：**show memory top-usage**。 未修改任何 ASDM 菜单项。 同样适用于 *8.4(6)* 版本。
Smart Call Home	添加了新的 Smart Call Home 消息类型，以支持 ASA 集群。 仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群主装置时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出 修改了以下命令：**show call-home**、**show running-config call-home**。 未修改任何 ASDM 菜单项。 同样适用于 *9.0(3)* 版本。
远程访问功能	
Show 命令现在对 **user-storage value** 命令密码进行了加密	现在，输入 **show running-config** 时会对 **user-storage value** 命令中的密码进行加密。 修改了以下命令：**user-storage value**。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 更多选项 > 会话设置**。 同样适用于 *8.4(6)* 版本。

ASA 9.1(2)/ASDM 7.1(3) 的新功能

发布日期：**2013** 年 **5** 月 **14** 日

注释 除非下表中明确列出，否则 9.1(2) 中不包括 8.4(6) 中添加的功能。

功能	说明
认证功能	
FIPS 和通用标准认证	FIPS 140-2 非专有安全策略在对思科 ASA 系列的级别 2 FIPS 140-2 验证中进行了更新，其中包括思科 ASA 5505、ASA 5510、ASA 5520、ASA 5540、ASA 5550、ASA 5580、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X 和 ASA 服务模块。 更新了通用标准评估保障层 4 (EAL4)，该标准是思科 ASA 和 VPN 平台解决方案特定评估目标 (TOE) 的基础。
加密功能	
支持 IPSec LAN 到 LAN 隧道加密故障切换和状态链路通信。	现在可以将 IPSec LAN 到 LAN 隧道用于故障切换和状态链路加密，而不是对故障切换密钥使用专有加密（**failover key** 命令）。 注释 故障切换 LAN 到 LAN 隧道不计入 IPSec（其他 VPN）许可证。 引入或修改了以下命令：**failover ipsec pre-shared-key**、**show vpn-sessiondb**。 修改了以下菜单项：**配置 > 设备管理 > 高可用性 > 故障切换 > 设置**。

功能	说明

适用于 SSL 加密的其他短暂 Diffie-Hellman 密码	ASA 现在支持以下短暂的 Diffie-Hellman (DHE) SSL 密码套件：
	• DHE-AES128-SHA1
	• DHE-AES256-SHA1
	这些密码套件在 RFC 3268“适用于传输层安全 *(TLS)* 的高级加密标准 *(AES)* 密码套件”中指定。
	当客户端支持 DHE 时，DHE 将是首选密码，因为它提供完全前向保密 (Perfect Forward Secrecy)。请参阅以下限制：
	• SSL 3.0 连接中不支持 DHE，所以请务必同时对 SSL 服务器启用 TLS 1.0。
	`!! set server version`
	`ciscoasa(config)# ssl server-version tlsv1 sslv3`
	`!! set client version`
	`ciscoasa(config) # ssl client-version any`
	• 有些常见应用不支持DHE，所以请至少包括一种其他SSL加密方法，以确保可以使用对SSL 客户端和服务器通用的密码套件。
	• 有些客户端可能不支持 DHE，包括 AnyConnect 2.5 和 3.0、思科安全桌面和 Internet Explorer 9.0。
	修改了以下命令：**ssl encryption**。
	修改了以下菜单项：**配置 > 设备管理 > 高级 > SSL 设置**。
	同样适用于 *8.4(4.1)* 版本。

管理功能	

功能	说明
使用本地数据库时，支持管理员密码策略。	使用本地数据库配置用于CLI或ASDM访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 引入了以下命令：**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**。 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 密码策略**。 同样适用于 *8.4(4.1)* 版本。
对 SSH 公钥身份验证的支持	对于与 ASA 的 SSH 连接，您现在可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下命令：**ssh authentication**。 引入了以下菜单项： **配置 > 设备管理 > 用户/AAA > 用户账户 > 编辑用户账户 > 公钥身份验证**和**配置 > 设备管理 > 用户/AAA > 用户账户 > 编辑用户账户 > 使用 PKF 的公钥**。 在 *8.4(4.1)* 中也可用；*PKF* 密钥格式支持仅在 *9.1(2)* 中提供。
SSH 的 AES-CTR 加密	ASA 中的 SSH 服务器实施现在支持 AES-CTR 模式加密。
改进的 SSH 重新生成密钥间隔	在连接时间达到 60 分钟后或数据流量达到 1 GB 后，SSH 连接重新生成密钥。 引入了以下命令：**show ssh sessions detail**。

功能	说明
支持用于 SSH 密钥交换的 Diffie-Hellman 群 14	已添加支持 Diffie-Hellman 组 14 进行 SSH 密钥交换。以前，只支持组 1。 引入了以下命令：**ssh key-exchange**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH**。 同样适用于 *8.4(4.1)* 版本。
支持管理会话最大数量	您可以设置并发 ASDM、SSH 和 Telnet 会话的最大数量。 引入了以下命令：**quota management-session**、**show running-config quota management-session**、**show quota management-session**。 引入了以下菜单项：**配置 > 设备管理 > 管理访问 > 管理会话配额**。 同样适用于 *8.4(4.1)* 版本。
支持 ASDM 中的预登录横幅	管理员可以定义在用户登录到 ASDM 以进行管理访问之前显示的消息。这种可自定义的内容称为预登录横幅，可以将特殊要求或重要信息通知用户。
删除默认 Telnet 密码	为了提高 ASA 管理访问的安全性，已删除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。**注意**：仅当未配置 Telnet 用户身份验证时，才会使用登录密码（**aaa authentication telnet console** 命令）。 过去，当清除了密码时，ASA 会恢复默认设置“cisco”。现在，当清除密码时，密码也被删除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 修改了以下命令：**passwd**。 未修改任何 ASDM 菜单项。 同样适用于 *9.0(2)* 版本。
平台功能	

功能	说明
支持开机自检 (POST)	ASA 在启动时会运行开机自检，即使为在 FIPS 140-2 兼容的模式下运行亦是如此。 在 POST 中添加了附加的测试，以处理 AES-GCM/GMAC 算法、ECDSA 算法、PRNG 和确定性随机位生成器验证系统 (DRBGVS) 中的变化。
改进的伪随机数生成 (PRNG)	X9.31 实施已升级为使用 AES-256 加密而不是 3DES 加密，以符合单核 ASA 中的网络设备保护配置文件 (NDPP)。
支持映像验证	添加了对 SHA-512 映像完整性检查的支持。 修改了以下命令：**verify**。 未修改任何 ASDM 菜单项。 同样适用于 *8.4(4.1)* 版本。
支持 ASA 服务模块上的专用 VLAN	可以将专用 VLAN 与 ASASM 配合使用。将主 VLAN 分配给 ASASM；ASASM 会自动处理辅助 VLAN 流量。对于此功能，不需要在 ASASM 上进行任何配置；有关详细信息，请参阅交换机配置指南。
CPU 配置文件增强	**cpu profile activate** 命令现在支持以下操作： • 分析器在触发前的延迟启动（全局或特定线程 CPU%） • 抽样单个线程 修改了以下命令：**cpu profile activate** [*n-samples*] [**sample-process** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]。 未修改任何 ASDM 菜单项。 同样适用于 *8.4(6)* 版本。
DHCP 功能	

功能	说明
每个接口的 DHCP 中继服务器（仅限 IPv4）	现在可以配置单个接口的 DHCP 中继服务器，因此仅将进入指定接口的请求中继给为该接口指定的服务器。每接口 DHCP 中继不支持 IPv6。 引入或修改了以下命令：**dhcprelay server**（接口配置模式）、**clear configure dhcprelay**、**show running-config dhcprelay**。 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 中继**。
DHCP 受信任接口	现可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 引入或修改了以下命令：**dhcprelay information trusted**、**dhcprelay informarion trust-all**、**show running-config dhcprelay**。 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 中继**。
模块功能	
ASA 5585-X 对网络模块的支持	ASA 5585-X 的插槽 1 中现在支持网络模块上的其他接口。您可以安装下面一个或两个可选网络模块： • ASA 4-端口 10G 网络模块 • ASA 8-端口 10G 网络模块 • ASA 20-端口 1G 网络模块 同样适用于 *8.4(4.1)* 版本。
ASA 5585-X DC 电源支持	添加了对 ASA 5585-X 直流电源的支持。 同样适用于 *8.4(5)* 版本。

功能	说明
支持采用 ASA CX 仅监控模式用于演示目的	如果只是为了演示，您可以为服务策略启用仅监控模式，将流量副本转发到 ASA CX 模块，而原有流量不会受到影响。 在进行演示时，您也可以配置流量转发接口，而不配置仅监控模式下的服务策略。流量转发接口绕过 ASA，将所有流量直接发送到 ASA CX 模块。 修改或引入了以下命令：**cxsc** {**fail-close** | **fail-open**} **monitor-only**、**traffic-forward cxsc monitor-only**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 > 规则操作 > ASA CX 检查**。 仅 CLI 支持流量转发功能。
支持 ASA CX 模块和 NAT 64	现在，您可以同时使用 NAT 64 和 ASA CX 模块。 未修改任何命令。 未修改任何 ASDM 菜单项。
NetFlow 功能	
支持 NetFlow 流更新事件和扩展的 NetFlow 模板集	除了添加流更新事件之外，现在还有 NetFlow 模板，允许您跟踪使用 NAT 对其 IP 版本进行更改的流程，以及在 NAT 之后保留为 IPv6 的 IPv6 流。 添加了两个新字段以支持 Ipv6 转换。 多个 NetFlow 字段 ID 被更改为其 IPFIX 等效项。 有关详细信息，请参阅*适用于 NetFlow 收集器的思科 ASA 实施说明*。
防火墙功能	
对于 IS-IS 流量支持 EtherType ACL（透明防火墙模式）	在透明防火墙模式下，ASA 现在可使用 EtherType ACL 传输 IS-IS 流量。 修改了以下命令：**access-list ethertype** {**permit** | **deny**} **is-is**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > EtherType 规则**。 同样适用于 *8.4(5)* 版本。

功能	说明
半闭超时最小值减小至 30 秒	全局超时和连接超时的半闭超时最小值从 5 分钟缩短至 30 秒，以提供更好的 DoS 保护。 修改了以下命令：**set connection timeout half-closed**、**timeout half-closed**。 修改了以下菜单项： **配置 > 防火墙 > 服务策略规则 > 连接设置** **配置 > 防火墙 > 高级 > 全局超时**。
远程访问功能	
IKE 安全和性能改进	IPSec-IKE 安全关联 (SA) 的数量现在可以面向 IKE v1 以及 IKE v2 进行限制。 修改了以下命令：**crypto ikev1 limit**。 修改了以下菜单项：**配置 > 站点到站点 VPN > 高级 > IKE 参数**。
	IKE v2 的临时大小已增加到 64 字节。 未修改任何 ASDM 菜单项或 CLI 命令。
	对于基于站点到站点的 IKE v2，可以采用一种新算法来确保子 IPSec SA 使用的加密算法的强度不高于父 IKE。较高强度的算法将被降级到 IKE 级别。 默认情况下，此新算法处于启用状态。我们建议您不要禁用此功能。 引入了以下命令：**crypto ipsec ikev2 sa-strength-enforcement**。 未修改任何 ASDM 菜单项。
	对于站点到站点，可以禁用基于 IPSec 数据的密钥更新。 修改了以下命令：**crypto ipsec security-association**。 修改了以下菜单项：**配置 > 站点到站点 > IKE 参数**。

功能	说明
改进了 Host Scan 和 ASA 互操作性	Host Scan 和 ASA 使用改良的过程从客户端向 ASA 传送安全评估属性。这使得 ASA 有更多时间与客户端建立VPN连接和应用动态范围策略。 同样适用于 *8.4(5)* 版本。
无客户端 SSL VPN： Windows 8 支持	此版本添加了对 Windows 8 x86（32 位）和 Windows 8 x64（64 位）操作系统的支持。 在 Windows 8 中支持以下浏览器： • Internet Explorer 10（仅限桌面） • Firefox（所有支持的 Windows 8 版本） • Chrome（所有支持的 Windows 8 版本） 请参阅以下限制： • Internet Explorer 10： • 不支持 Modern (AKA Metro) 浏览器。 • 如果启用增强保护模式，我们建议您将 ASA 添加到受信任区。 • 如果启用增强保护模式，则不支持智能隧道和端口转发程序。 • 不支持连接到 Windows 8 PC 的 Java 远程桌面协议 (RDP) 插件。 同样适用于 *9.0(2)* 版本。
思科安全桌面： Windows 8 支持	CSD 3.6.6215 更新为在“预登录策略”操作系统检查中支持 Windows 8 选项。 请参阅以下限制： • 对于 Windows 8 不支持安全桌面 (Vault)。 同样适用于 *9.0(2)* 版本。
动态访问策略： Windows 8 支持	ASDM 更新为在“DAP 操作系统”属性中支持 Windows 8 选项。 同样适用于 *9.0(2)* 版本。
监控功能	

功能	说明
NSEL	引入了 Flow-update 事件，以便定期提供数据流流量的字节计数器。您可以更改系统向 NetFlow 收集器发送 flow-update 事件的时间间隔。您可以对 flow-update 记录被发送到的收集器进行过滤。 引入或修改了以下命令：**flow-export active refresh-interval**、**flow-export event-type**。 修改了以下菜单项： **配置 > 设备管理 > 日志记录 > NetFlow**。 **配置 > 防火墙 > 服务策略规则 > 添加服务策略规则向导 - 规则操作 > NetFlow > 添加流事件** 同样适用于 *8.4(5)* 版本。

ASA 9.1(1)/ASDM 7.1(1) 的新功能

发布日期：**2012** 年 **12** 月 **3** 日

注释 除非 9.0(1) 功能表中列出，否则 9.1(1) 中不包括 8.4(4.x)、8.4(5)、8.4(6) 和 9.0(2) 中添加的功能。

功能	说明
模块功能	
对适用于 ASA 5512-X 至 ASA 5555-X 的 ASA CX SSP 的支持	为 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 引入了 ASA CX SSP 软件模块支持。ASA CX 软件模块需要在 ASA 上安装思科固态驱动器 (SSD)。有关 SSD 的详细信息，请参阅《ASA 5500-X 硬件指南》。 修改了以下命令：**session cxsc**、**show module cxsc**、**sw-module cxsc**。 未修改任何菜单项。

版本 9.0 的新功能

ASA 9.0(4)/ASDM 7.1(4) 的新功能

ASA 9.0(4)/ASDM 7.1(4) 中无新增功能。

ASA 9.0(3)/ASDM 7.1(3) 的新功能

发布日期：**2013** 年 **7** 月 **22** 日

注释 除非 9.0(1) 功能表中列出，否则 9.0(3) 中不包括 8.4(4.x)、8.4(5) 和 8.4(6) 中添加的功能。

功能	说明
监控功能	
Smart Call Home	添加了新的 Smart Call Home 消息类型，以支持 ASA 集群。 仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群主装置时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群主装置运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

ASA 9.0(2)/ASDM 7.1(2) 的新功能

发布日期：**2013** 年 **2** 月 **25** 日

注释 除非 9.0(1) 功能表中列出，否则 9.0(2) 中不包括 8.4(4.x)、8.4(5) 和 8.4(6) 中添加的功能。

功能	说明
远程访问功能	

功能	说明
无客户端 SSL VPN： Windows 8 支持	此版本添加了对 Windows 8 x86（32 位）和 Windows 8 x64（64 位）操作系统的支持。 在 Windows 8 中支持以下浏览器： • Internet Explorer 10（仅限桌面） • Firefox（所有支持的 Windows 8 版本） • Chrome（所有支持的 Windows 8 版本） 请参阅以下限制： • Internet Explorer 10： • 不支持 Modern (AKA Metro) 浏览器。 • 如果启用增强保护模式，我们建议您将 ASA 添加到受信任区。 • 如果启用增强保护模式，则不支持智能隧道和端口转发程序。 • 不支持连接到 Windows 8 PC 的 Java 远程桌面协议 (RDP) 插件。
管理功能	
删除默认 Telnet 密码	为了提高 ASA 管理访问的安全性，已删除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。**注意**：仅当未配置 Telnet 用户身份验证时，才会使用登录密码（**aaa authentication telnet console** 命令）。 过去，当清除了密码时，ASA 会恢复默认设置“cisco”。现在，当清除密码时，密码也被删除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 修改了以下命令：**passwd**。 未修改任何 ASDM 菜单项。

ASA 9.0(1)/ASDM 7.0(1) 的新功能

发布日期：**2012** 年 **10** 月 **29** 日

注释 除非下表中明确列出，否则 9.0(1) 中不包括 8.4(4.x)、8.4(5) 和 8.4(6) 中添加的功能。

功能	说明
防火墙功能	

功能	说明
思科 TrustSec 集成	思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制解决方案，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 解决方案中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。 在此版本中，ASA 与思科 TrustSec 相集成以提供基于安全组的策略实施。思科 TrustSec 域中的访问策略不受拓扑影响，基于源和目标设备的角色，而非基于网络 IP 地址。 ASA 可对其他类型的基于安全组的策略（例如应用检测）使用思科 TrustSec，例如可配置包含基于安全组的访问策略的类映射。 引入或修改了以下命令：**access-list extended**、**cts sxp enable**、 **cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconcile period**、**cts sxp connection peer**、**cts import-pac**、**cts refresh environment-data**、**object-group security**、**security-group**、**show running-config cts**、**show running-config object-group**、**clear configure cts**、**clear configure object-group**、**show cts**、**show object-group**、**show conn security-group**、**clear cts** 和 **debug cts**。 引入了以下 MIB：CISCO-TRUSTSEC-SXP-MIB。 引入或修改了以下菜单项： **配置 > 防火墙 > 使用 TrustSec 配置身份** **配置 > 防火墙 > 对象 > 安全组对象组** **配置 > 防火墙 > 访问规则 > 添加访问规则** **监控 > 属性 > 使用 TrustSec 配置身份 > PAC** **监控 > 属性 > 使用 TrustSec 配置身份 > 环境数据** **监控 > 属性 > 使用 TrustSec 配置身份 > SXP 连接** **监控 > 属性 > 使用 TrustSec 配置身份 > IP 映射** **监控 > 属性 > 连接** **工具 > 数据包跟踪器**

功能	说明
思科云网络安全 (ScanSafe)	思科云网络安全为 Web 流量提供内容扫描及其他恶意软件保护服务。还能够根据用户身份重定向网络流量和提交相关报告。 注释 云网络安全不支持无客户端 SSL VPN；云网络安全的 ASA 服务策略不得包含任何无客户端 SSL VPN 流量。 引入了以下命令：**class-map type inspect scansafe**、**default user group**、**http**[**s**] (parameters)、**inspect scansafe**、**license**, **match user group**、**policy-map type inspect scansafe**、**retry-count**、**scansafe**、**scansafe general-options**、**server** {**primary** | **backup**}、**show conn scansafe**、**show scansafe server**、**show scansafe statistics**、**user-identity monitor**、**whitelist**。 引入或修改了以下菜单项： **配置 > 设备管理 > 云 Web 安全** **配置 > 防火墙 > 对象 > 类映射 > 云 Web 安全** **配置 > 防火墙 > 对象 > 类映射 > 云 Web 安全 > 添加/编辑** **配置 > 防火墙 > 对象 > 检查映射 > 云 Web 安全** **配置 > 防火墙 > 对象 > 检查映射 > 云 Web 安全 > 添加/编辑** **配置 > 防火墙 > 对象 > 检查映射 > 云 Web 安全 > 添加/编辑 > 管理云 Web 安全类映射** **配置 > 防火墙 > 身份选项配置 > 防火墙 > 服务策略规则** **监控 > 属性 > 云 Web 安全**
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	现在可以根据 ICMP 代码允许/拒绝 ICMP 流量。 引入或修改了以下命令：**access-list extended**、**service-object**、**service**。 引入或修改了以下菜单项： **配置 > 防火墙 > 对象 > 服务对象/组配置 > 防火墙 > 访问规则**
ASASM 上支持统一通信	ASASM 现在支持所有统一通信功能。

功能	说明
NAT 支持反向 DNS 查找	在为 NAT 规则启用了 DNS 检测的情况下使用 IPv4 NAT、IPv6 NAT 和 NAT64 时，NAT 现支持为反向 DNS 查找转换 DNS PTR 记录。
每会话 PAT	每会话 PAT 功能可改进 PAT 的扩展性，而且对于 ASA 集群，还允许每个成员设备拥有 PAT 连接；多会话 PAT 连接必须转发到主设备并归其所有。在每会话 PAT 会话结束时，ASA 将发送一条重置消息并立即删除转换。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。对于“命中并运行”的数据流，例如 HTTP 或HTTPS，每会话功能可以显著提高一个地址支持的连接速度。不使用每会话功能时，一个用于 IP 协议的地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 65535/*average-lifetime*。 默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT xlate。对于可受益于多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），可以创建每会话拒绝规则来禁用每会话 PAT。 引入了以下命令：**xlate per-session**、**clear configure xlate**、**show running-config xlate**。 引入了以下菜单项：**配置 > 防火墙 > 高级 > 每会话 NAT 规则**。

功能	说明
针对未连接的子网添加 ARP 缓存	在默认情况下，ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则不建议启用此功能。此功能可能有助于引发对 ASA 的拒绝服务 (DoS) 攻击；任意接口上的用户都可能发出许多 ARP 应答，并使 ASA ARP 表中的错误条目超载。 如果您使用以下对象，则可能要使用此功能： • 辅助子网。 • 用于流量转发的相邻路由上的代理 ARP。 引入了以下命令：**arp permit-nonconnected**。 修改了以下菜单项：配置 > 设备管理 > 高级 > ARP > ARP 静态表。 同样适用于 *8.4(5)* 版本。
SunRPC 从动态 ACL 更改为针孔机制	以前，Sun RPC 检测不支持出站访问列表，因为该检测引擎使用的是动态访问列表，而不是辅助连接。 在此版本中，当在 ASA 上配置动态访问列表时，仅在入口方向支持该检测，ASA 会丢弃传至目标端口的出口流量。因此，Sun RPC 检测会实施针孔机制来支持出口流量。Sun RPC 检测使用此针孔机制来支持出站动态访问列表。 同样适用于 *8.4(4.1)* 版本。

功能	说明
检测重置操作更改	以前，当 ASA 因检测引擎规则丢弃数据包时，ASA 仅向被丢弃数据包的源设备发送一个 RST。此行为可能会导致资源问题。 在此版本中，如果将检测引擎配置为使用重置操作，当数据包触发重置时，ASA 在以下条件下会发送一个 TCP 重置： • 当启用 **service resetoutbound** 命令时，ASA 向内部主机发送一个 TCP 重置。（默认情况下，启用 **service resetoutbound** 命令。） • 当启用 **service resetinbound** 命令时，ASA 向外部主机发送一个 TCP 重置。（默认情况下，禁用 **service resetinbound** 命令。） 有关详细信息，请参阅 ASA 命令参考中的 **service** 命令。 此行为可确保重置操作重置 ASA 和内部服务器上的连接；因此抵抗拒绝服务攻击。对于外部主机，ASA 默认不发送重置并且不会通过 TCP 重置显示信息。 同样适用于 *8.4(4.1)* 版本。
服务策略规则增加的最大连接数限制	服务策略规则的最大连接数从 65535 增加至 2000000。 修改了以下命令：**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 连接设置**。 同样适用于 *8.4(5)* 版本
高可用性和扩展性功能	

功能	说明
ASA 5580 和 5585-X 的 ASA 集群	

功能	说明
	通过 ASA 集群，您可以将多台 ASA 组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。ASA 5580 和 ASA 5585-X 支持 ASA 集群；集群中的所有设备必须为相同型号且硬件规格相同。有关启用集群时不支持的功能列表，请参阅配置指南。 引入或修改了以下命令：**channel-group**、**clacp system-mac**、**clear cluster info**、**clear configure cluster**、**cluster exec**、**cluster group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalance**、**console-replicate**、**cluster master unit**、**cluster remove unit**、**debug cluster**、**debug lacp cluster**、**enable**（集群组）、**health-check**、**ip address**、**ipv6 address**、**key**（集群组）、**local-unit**、**mac-address**（接口）、**mac-address pool**、**mtu cluster**、**port-channel span-cluster**、**priority**（集群组）、**prompt cluster-unit**、**show asp cluster counter**、**show asp table cluster chash-table**、**show cluster**、**show cluster info**、**show cluster user-identity**、**show lacp cluster**、**show running-config cluster**。 引入或修改了以下菜单项： 主页 > 设备控制面板 主页 > 集群控制面板主页 > 集群防火墙控制面板 **配置 > 设备管理 > 高级 > 地址池 > MAC 地址池** **配置 > 设备管理 > 高可用性和可扩展性 > ASA 集群** **配置 > 设备管理 > 日志记录 > 系统日志设置 > 高级** **配置 > 设备设置 > 接口 > 添加/编辑接口 > 高级** **配置 > 设备设置 > 接口 > 添加/编辑接口 > IPv6** **配置 > 设备设置 > 接口 > 添加/编辑 EtherChannel 接口 > 高级** **配置 > 防火墙 > 高级 > 每会话 NAT 规则** **监控 > ASA 集群监控 > 属性 > 系统资源图 > 集群控制链路** **工具 > 首选项 > 通用**

功能	说明
	工具 > 系统重新加载 **工具 > 从本地计算机升级软件** **向导 > 高可用性和可扩展性向导** **向导 > 数据包捕获向导** **向导 > 启动向导**
用于集群的 OSPF、EIGRP 和组播	对于 OSPFv2 和 OSPFv3，在集群环境中支持批量同步、路由同步和跨网络 EtherChannel。 对于EIGRP，在集群环境中支持批量同步、路由同步和跨网络 EtherChannel。 组播路由支持集群。 引入或修改了以下命令：**show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster**。
用于集群的数据包捕获	要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在主设备上启用捕获集群特定流量的功能，随后集群中的所有从属设备上将自动启用此功能。**cluster exec** 关键字是放在 **capture** 命令前面的新关键字，可启用集群范围的捕获。 修改了以下命令：**capture**、**show capture**。 修改了以下菜单项：向导 > **数据包捕获向导**。
用于集群的日志记录	集群中的每台设备将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同设备。 修改了以下命令：**logging device-id**。 修改了以下菜单项：**配置 > 日志记录 > 系统日志设置 > 高级 > 高级系统日志配置**。
对于思科 Nexus 7000 和思科 Catalyst 6500 支持集群	当连接到使用管理引擎 32、720 和 720-10GE 的思科 Nexus 7000 和思科 Catalyst 6500 时，ASA 支持集群。

功能	说明
配置批量同步期间的连接复制速率	现在，您可以配置 ASA 在使用状态故障切换时将连接复制到备用设备的速率。默认情况下，连接会在 15 秒内复制到备用设备。但是，当执行批量同步时（例如首次启用故障切换时），由于每秒最大连接数的限制，15 秒可能不足以同步大量连接。例如，ASA 的最大连接数为 800 万；在 15 秒内复制 800 万个连接意味着每秒创建 533,000 个连接。不过，每秒允许的最大连接数为 300,000 个。现在，您可以指定复制速率小于或等于每秒最大连接数，同步期间将会调整，直到所有连接均同步为止。 引入了以下命令：**failover replication rate** *rate*。 同样适用于 *8.4(4.1)* 和 *8.5(1.7)* 版本。
IPv6 的功能	
在 ASA 的外部接口上，VPN 功能支持 IPv6。	此版 ASA 为其使用 SSL 和 IKEv2/IPSec 协议的外部接口添加了 IPv6 VPN 连接支持。 此版 ASA 在其使用 SSL 协议的内部接口上，同过去一样继续支持 IPv6 VPN 流量。此版本在内部接口上不提供 IKEv2/IPSec 协议。
远程访问 VPN 支持 IPv6：IPv6 地址分配策略	通过在 ASA 上创建内部地址池，或者通过向 ASA 上的本地用户分配专用地址，您可以将 ASA 配置为向 AnyConnect 客户端分配 IPv4 地址和/或 IPv6 地址。 终端必须已在其操作系统中实现双栈协议，才有资格分配得到这两种地址。 SSL 协议支持向客户端分配 IPv6 地址。IKEv2/IPSec 协议不支持此功能。 引入了以下命令：**ipv6-vpn-addr-assign**、**vpn-framed-ipv6-address**。 修改了以下菜单项： **配置 > 远程访问 VPN > 网络（客户端）访问 > 地址分配 > 分配策略** **配置 > 远程访问 VPN > AAA/本地用户 > 本地用户 > (编辑本地用户帐户) > VPN 策略**

功能	说明
远程访问 VPN 支持 IPv6：您可以将使用 IPv6 地址的 DNS 服务器分配至组策略	在 ASA 的“网络（客户端）访问”内部组策略中可以定义DNS服务器。最多可以指定四个DNS服务器地址，最多包括两个IPv4地址和两个IPv6地址。 当 VPN 客户端配置为使用 SSL 协议时，可通过 VPN 客户端访问使用 IPv6 地址的 DNS 服务器。此功能不支持配置为使用 IKEv2/IPSec 协议的客户端。 修改了以下命令：**dns-server value**。 修改了以下菜单项：配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > (编辑组策略) > 服务器。
远程访问 VPN 支持 IPv6：拆分隧道	拆分隧道使您能够通过 VPN 隧道传输某些网络流量（已加密），并可传输 VPN 隧道外部的其他网络流量（未加密或“明文”形式）。现在，您可以通过定义指定统一访问控制规则的IPv6策略，对 IPv6 网络流量执行拆分隧道。 IPv6 拆分隧道报告带有 Smart Call Home 功能发送的遥测数据。如果启用了 IPv4 或 IPv6 拆分隧道，Smart Call Home 会将拆分隧道报告为“已启用”。对于遥测数据，VPN 会话数据库将显示通常使用会话管理报告的 IPv6 数据。 对于配置为使用 SSL 协议的 VPN 客户端，您可以从 VPN“隧道”中添加或排除 IPv6 流量。IKEv2/IPSec 协议不支持此功能。 引入了以下命令：**ipv6-split-tunnel-policy**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > (编辑组策略) > 高级 > 拆分隧道**。
远程访问 VPN 支持 IPv6：AnyConnect 客户端防火墙规则	客户端防火墙的访问控制规则支持 IPv4 和 IPv6 地址的访问列表条目。 可将包含IPv6地址的ACL应用于配置为使用SSL协议的客户端。IKEv2/IPSec协议不支持此功能。 修改了以下命令：**anyconnect firewall-rule**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > (编辑组策略) > 高级 > AnyConnect 客户端 > 客户端防火墙**。

功能	说明
远程访问 VPN 支持 IPv6：客户端协议旁路	通过客户端绕行协议功能，可以配置 ASA 在应该只有 IPv6 流量时如何管理 IPv4 流量，或者在应该只有 IPv4 流量时如何管理 IPv6 流量。 当 AnyConnect 客户端对 ASA 进行 VPN 连接时，ASA 可以为客户端分配一个 IPv4、IPv6 或 IPv4 和 IPv6 两个地址。如果 ASA 对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置客户端旁路协议以丢弃 ASA 尚未分配 IP 地址的网络流量，或允许该流量绕过 ASA 并从客户端以未加密或“明文形式”发送。 举例来说，假设 ASA 只分配一个 IPv4 地址到 AnyConnect 连接且终端被双堆叠。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。 配置为使用 SSL 或 IKEv2/IPSec 协议的客户端可以使用此功能。 引入了以下命令：**client-bypass-protocol**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > (组策略)高级 > AnyConnect 客户端 > 客户端旁路协议**。
远程访问 VPN 支持 IPv6：IPv6 接口 ID 和前缀	现在，您可以为本地 VPN 用户指定专用的 IPv6 地址。 此功能可为配置为使用 SSL 协议的用户带来好处。IKEv2/IPSec 协议不支持此功能。 引入了以下命令：**vpn-framed-ipv6-address**。 修改了以下菜单项：**配置 > 远程访问 VPN > AAA/本地用户 > 本地用户 > (编辑用户) > VPN 策略**。
远程访问 VPN 支持 IPv6：将 ASA FQDN 发送到 AnyConnect 客户端	您可以将 ASA 的 FQDN 返回到 AnyConnect 客户端，以便于负载均衡和会话漫游。 配置为使用 SSL 或 IKEv2/IPSec 协议的客户端可以使用此功能。 引入了以下命令：**gateway-fqdn**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > (编辑组策略) > 高级 > AnyConnect**。

功能	说明
远程访问 VPN 支持 IPv6：ASA VPN 负载均衡	使用 IPv6 地址的客户端可通过 ASA 的公开 IPv6 地址或GSS服务器进行AnyConnect连接。同样，使用 IPv6 地址的客户端可通过 ASA 的公开 IPv4 地址或 GSS 服务器进行 AnyConnect VPN 连接。任何一种连接类型都可以在 ASA 集群内进行负载均衡。 对于使用IPv6地址的客户端，要成功连接至ASA的公开 IPv4 地址，网络中需要有可执行从 IPv6 至 IPv4 的网络地址转换的设备。 配置为使用 SSL 或 IKEv2/IPSec 协议的客户端可以使用此功能。 修改了以下命令：**show run vpn load-balancing**。 修改了以下菜单项：**配置 > 远程访问 VPN > 负载均衡**。
远程访问VPN支持IPv6：动态访问策略支持IPv6属性	现在，将 ASA 9.0 或更高版本与 ASDM 6.8 或更高版本搭配使用时，您可以将这些属性指定为动态访问策略 (DAP) 的一部分： • IPv6 地址作为思科 AAA 属性 • IPv6 TCP 和 UDP 端口作为设备终端属性的一部分 • 网络 ACL 过滤器（客户端） 配置为使用 SSL 或 IKEv2/IPSec 协议的客户端可以使用此功能。 修改了以下菜单项： **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加 > 思科 AAA 属性** **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加 > 设备 > 添加终端属性** **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 网络 ACL 过滤器（客户端）** **配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > Webtype ACL 过滤器（无客户端）**

功能	说明
远程访问 VPN 支持 IPv6：会话管理	会话管理输出在 AnyConnect 连接、站点到站点 VPN 连接和无客户端 SSL VPN 连接的“公共/分配”地址字段中显示IPv6地址。您可以添加新的过滤器关键字来支持输出过滤，以仅显示 IPv6（外部或内部）连接。未对IPv6用户过滤器进行任何更改。 配置为使用SSL协议的客户端可以使用此功能。此功能不支持 IKEv2/IPSec 协议。 修改了以下命令：**show vpn-sessiondb**。 修改了以下菜单项：**监控 > VPN > VPN 统计信息 > 会话**。
NAT 支持 IPv6	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换 (NAT64)。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。 修改了以下命令：**nat**（在全局和对象网络配置模式下）、**show conn**、**show nat**、**show nat pool**、**show xlate**。 修改了以下菜单项： **配置 > 防火墙 > 对象 > 网络对象/组** **配置 > 防火墙 > NAT 规则**
DHCPv6 中继	IPv6 支持 DHCP 中继。 引入了以下命令：**ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics** 和 **clear ipv6 dhcprelay statistics**。 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 中继**。

功能	说明
OSPFv3	

功能	说明
	IPv6 支持 OSPFv3 路由。请注意以下适用于 OSPFv2 和 OSPFv3 的附加准则和限制： 集群 • OSPFv2 和 OSPFv3 支持集群。 • 当配置了集群时，不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。 • 使用个别接口时，请确保已作为 OSPFv2 或 OSPFv3 邻居建立主设备和从属设备。 • 使用个别接口时，只能在主设备共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在一个接口上仅允许一个邻居声明。 其他 • OSPFv2 和 OSPFv3 在接口上支持多个实例。 • OSPFv3 身份验证支持 ESP 和 AH 协议。 • OSPFv3 支持非负载加密。 引入或修改了以下命令：**ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf dead-interval**、**ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neighbor**、**ipv6 ospf network**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、**ipv6 ospf transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、**ipv6 router ospf distance**、**ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router ospf log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router ospf redistribute**、**ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area range**、**area virtual-link**、 **default**、**default-information originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes**、**redistribute**、**router-id**、**summary-prefix**、**timers lsa arrival**、**timers pacing flood**、**timers pacing lsa-group**、**timers pacing retransmission**、**show ipv6 ospf**、**show ipv6 ospf border-routers**、**show ipv6 ospf database-filter**、**show ipv6 ospf flood-list**、**show**

功能	说明
	ipv6 ospf interface、**show ipv6 ospf neighbor**、**show ipv6 ospf request-list**、**show ipv6 ospf retransmission-list**、**show ipv6 ospf summary-prefix**、**show ipv6 ospf virtual-links**、**show ospf**、**show run ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3**。 引入了以下菜单项： **配置 > 设备设置 > 路由 > OSPFv3 > 设置** **配置 > 设备设置 > 路由 > OSPFv3 > 接口** **配置 > 设备设置 > 路由 > OSPFv3 > 重新分配** **配置 > 设备设置 > 路由 > OSPFv3 > 摘要前缀** **配置 > 设备设置 > 路由 > OSPFv3 > 虚拟链路** **监控 > 路由 > OSPFv3 LSA** **监控 > 路由 > OSPFv3 邻居**
适用于 IPv4 和 IPv6 的统一 ACL	ACL 现支持 IPv4 和 IPv6 地址。您还可以为源和目标同时指定 IPv4 和 IPv6 地址。特定于 IPv6 的 ACL 已弃用。现有 IPv6 ACL 已迁移到扩展 ACL。 可将包含 IPv6 地址的 ACL 应用于配置为使用 SSL 协议的客户端。IKEv2/IPSec 协议不支持此功能。 修改了以下命令：**access-list extended**、**access-list webtype**。 删除了以下命令：**ipv6 access-list**、**ipv6 access-list webtype** 和 **ipv6-vpn-filter**。 修改了以下菜单项： **配置 > 防火墙 > 访问规则** **配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 通用 > 更多选项**
IPv4 和 IPv6 混合对象组	以前，网络对象组只能包含所有 IPv4 地址或所有 IPv6 地址。现在，网络对象组可以同时包含 IPv4 和 IPv6 地址。 **注释** 不能使用混合对象组进行 NAT。 修改了以下命令：**object-group network**。 修改了以下菜单项：**配置 > 防火墙 > 对象 > 网络对象/组**。

功能	说明
适用于网络对象的 IPv6 地址范围	现在，您可以为网络对象配置 IPv6 地址范围。 修改了以下命令：**range**。 修改了以下菜单项：**配置 > 防火墙 > 对象 > 网络对象/组**。
IPv6 和 NAT64 的检测支持	我们现在支持对 IPv6 流量执行 DNS 检测。 另外，对于以下检测还支持 IPv4 和 IPv6 之间的转换： • DNS • FTP • HTTP • ICMP 现在，您还可以配置服务策略，使其在不支持的检测接收和丢弃 IPv6 流量时生成系统日志消息 (767001)。 修改了以下命令：**service-policy fail-close**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 - 服务策略**。
远程访问功能	
无客户端 SSL VPN： 其他支持	添加了对以下浏览器、操作系统、Web 技术和应用的附加支持： **Internet 浏览器支持**：Microsoft Internet Explorer 9、Firefox 4、5、6、7 和 8 **操作系统支持**：Mac OS X 10.7 **Web 技术支持**：HTML 5 **应用支持**：Sharepoint 2010
无客户端 SSL VPN： 改进了重写程序引擎的质量	显著改进了无客户端 SSL VPN 重写程序引擎以提供更好的质量和效率。因此，您可以预计无客户端 SSL VPN 用户将获得更好的最终用户体验。 对于此功能，我们未添加或修改任何命令。 对于此功能，我们未添加或修改任何 ASDM 菜单项。 同样适用于 *8.4(4.1)* 版本。

功能	说明
无客户端 SSL VPN： Citrix Mobile Receiver	此功能使移动设备上运行的 Citrix Receiver 应用可通过 ASA 安全地远程访问 XenApp 和 XenDesktop VDI 服务器。 如果使用 ASA 作为 Citrix Receiver 访问 Citrix Server 的代理，当用户尝试连接到 Citrix 虚拟化资源时，用户只需输入 ASA 的 SSL VPN IP 地址和凭证，而不必提供 Citrix Server 地址和凭证。 修改了以下命令：**vdi**。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 编辑 > 更多选项 > VDI 访问 > 添加 VDI 服务器**。
无客户端 SSL VPN：增强了自动登录功能	此功能改进了对需要动态参数进行身份验证的 Web 应用的支持。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签**。
无客户端 SSL VPN：无客户端 Java 重写程序代理支持	当在客户端计算机的浏览器中配置代理时，此功能为无客户端 Java 插件提供代理支持。 对于此功能，我们未添加或修改任何命令。 对于此功能，我们未添加或修改任何 ASDM 菜单项。
无客户端 SSL VPN：Remote File Explorer	有了 Remote File Explorer，用户可以从其网络浏览器浏览企业网络。当用户点击思科 SSL VPN 门户页面上的“远程文件系统”图标时，用户系统上会启动一个小应用程序，在文件夹树视图中显示远程文件系统。 对于此功能，我们未添加或修改任何命令。 对于此功能，我们未添加或修改任何 ASDM 菜单项。
无客户端 SSL VPN：服务器证书验证	此功能增强了无客户端 SSL VPN 支持，使得可以根据受信任的 CA 证书列表对远程 HTTPS 站点执行 SSL 服务器证书验证。 修改了以下命令：ssl-server-check、crypto、crypto ca trustpool、crl、certificate、revocation-check。 修改了以下菜单项：**配置 > 远程访问 VPN > 证书管理 > 可信任证书池**。

功能	说明
AnyConnect 性能改进	此功能改进了多核平台中 AnyConnect TLS/DTLS 流量的吞吐量性能。它们可以加速 SSL VPN 数据路径，并在 AnyConnect、智能隧道和端口转发方面提供客户可见的性能提升。 修改了以下命令：**crypto engine accelerator-bias** 和 **show crypto accelerator**。 修改了以下菜单项：**配置 > 远程访问 VPN > 高级 > 加密引擎**。
自定义属性	自定义属性定义和配置尚未添加到 ASDM 中的 AnyConnect 功能。您可以向组策略中添加自定义属性，并为这些属性定义值。 对于 AnyConnect 3.1，可以使用自定义属性来支持 AnyConnect 延迟升级。 自定义属性可以为针对 IKEv2/IPSec 或 SSL 协议配置的 AnyConnect 客户端带来好处。 添加了以下命令：**anyconnect-custom-attr**。 添加了一个新菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > AnyConnect 自定义属性**。

功能	说明
下一代加密	

功能	说明
	国家标准协会 (NSA) 指定了一套加密算法，设备必须支持这套算法才能满足美国联邦的加密强度标准。RFC 6379 定义了 Suite B 加密套件。由于这套定义为 NIST Suite B 的算法集合正在成为标准，所以现在 AnyConnect IPSec VPN（仅 IKEv2）和公共密钥基础设施 (PKI) 子系统均支持它们。下一代加密 (NGE) 包括此集合的更大超集，添加了适用于 IPSec V3 VPN 的加密算法、适用于 IKEv2 的 Diffie-Hellman 组 14 和 24，以及适用于 DTLS 和 IKEv2 的 RSA 证书和 4096 位密钥。 ASA 中添加了以下功能以支持 Suite B 算法： • AES-GCM/GMAC 支持（128 位、192 位和 256 位密钥） • IKEv2 负载加密与身份验证 • ESP 数据包加密与身份验证 • 仅在多核平台上支持硬件 • SHA-2 支持（256 位、384 位和 512 位散列） • ESP 数据包身份验证 • 仅在多核平台上支持硬件和软件 • ECDH 支持（组 19、20 和 21） • IKEv2 密钥交换 • IKEv2 PFS • 仅单核或多核平台上支持软件 • ECDSA 支持（256 位、384 位和 521 位 Elliptic Curves） • IKEv2 用户身份验证 • PKI 认证登记 • PKI 认证生成和确认 • 仅单核或多核平台上支持软件 对 IPSecV3 添加了新的加密算法。 注释 Suite B 算法支持需要使用 AnyConnect 高级版许可证才能进行 IKEv2 远程访问

功能	说明
	连接，但对于其他连接或目的（例如 PKI）使用 Suite B 没有限制。IPSecV3 没有许可限制。 引入或修改了以下命令：**crypto ikev2 policy**、**crypto ipsec ikev2 ipsec-proposal**、**crypto key generate**、**crypto key zeroize**、**show crypto key mypubkey**、**show vpn-sessiondb**。 引入或修改了以下菜单项： **监控 > VPN > 会话** **监控 > VPN > 加密统计信息** **配置 > 站点到站点 VPN > 证书管理 > 身份证书** **配置 > 站点到站点 VPN > 高级 > 系统选项** **配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 加密映射**
ASASM 上支持 VPN	ASASM 现在支持所有 VPN 功能。
多情景模式功能	
多情景模式下的站点间 VPN	现在，在多情景模式下支持站点间 VPN 隧道。
用于站点间 VPN 隧道的新资源类型	系统创建了新的资源类型（即 vpn other 和 vpn burst other），用于设置每个情景中站点间 VPN 隧道的最大数量。 修改了以下命令：**limit-resource**, **show resource types**、**show resource usage**、**show resource allocation**。 修改了以下菜单项：**配置 > 情景管理 > 资源类 > 添加资源类**。
安全情景中的动态路由	现在，在多情景模式下支持 EIGRP 和 OSPFv2 动态路由协议。不支持 OSPFv3、RIP 和组播路由。
用于路由表条目的新资源类型	创建了一个新的资源类(routes)，以在每个情景中设置路由表条目的最大数量。 修改了以下命令：**limit-resource**, **show resource types**、**show resource usage**、**show resource allocation**。 修改了以下菜单项：**配置 > 情景管理 > 资源类 > 添加资源类**。

功能	说明
在多情景模式下支持混合防火墙模式	可以在多情景模式下为每个情景独立设置防火墙模式，因此某些情景可在透明模式下运行，而另一些情景则可在路由模式中运行。 修改了以下命令：**firewall transparent**。 不能在 ASDM 中设置防火墙模式；必须使用命令行界面进行设置。 同样适用于版本 *8.5.(1)*。
模块功能	
思科 7600 交换机支持 ASA 服务模块	Cisco 7600 系列现在支持 ASASM。有关具体的硬件和软件要求，请参阅：http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html。
ASA 5585-X 对 ASA CX SSP-10 和 -20 的支持	通过 ASA CX 模块，您可以根据某个情况的全部情景实施安全措施。此情景包括用户身份（身份）、用户要访问的应用或网站（事情）、访问的来源（地点）、访问的时间（时间）和用于访问的设备的属性（方式）。通过 ASA CX 模块，您可以提取流量的全部情景并执行精细策略，例如允许访问 Facebook，但不允许访问 Facebook 上的游戏，或允许财务人员访问敏感的企业数据库，但不允许其他员工进行同样的访问。 引入或修改了以下命令：**capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module**、**show service-policy**。 引入了以下菜单项： **主页 > ASA CX 状态** **向导 > 启动向导 > ASA CX 基本配置** **配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 > 规则行为 > ASA CX 检查** 同样适用于 *8.4(4.1)* 版本。

功能	说明
SSP-10 和 SSP-20 的 ASA 5585-X 双 SSP 支持（SSP-40 和 SSP-60 除外）；双 SSP 的 VPN 支持	ASA 5585-X 现在支持所有 SSP 型号使用双 SSP（在同一机箱中，您可以使用两个相同级别的 SSP）。使用双 SSP 时，现在支持 VPN。 未修改任何命令。 未修改任何菜单项。

版本 8.7 的新功能

ASA 8.7(1.1)/ASDM 6.7(1) 的新功能

发布日期：2012 年 10 月 16 日

注释 由于内部版本问题，从 Cisco.com 中删除了版本 8.7(1)；请升级到版本 8.7(1.1) 或更高版本。

功能	说明
平台功能	
支持 ASA 1000V	面向 Nexus 1000V 交换机引入了对 1000V 的支持。
克隆 ASA 1000V	您可以使用克隆虚拟机的方法将 ASA 1000V 的一个或多个实例添加到部署中。
管理功能	
ASDM 模式	您可以使用自适应安全设备管理器（ASDM，适用于 ASA 的单个基于 GUI 的设备管理器）配置、管理和监控 ASA 1000V。
VNMC 模式	您可以使用思科虚拟网络管理中心（VNMC，适用于多租户的基于 GUI 的多设备管理器）配置和管理 ASA 1000V。
XML API	您可以使用 XML API 配置和管理 ASA 1000V，XML API 是通过思科 VNMC 提供的应用编程接口。此功能仅在 VNMC 模式下可用。
防火墙功能	

功能	说明
思科 VNMC 访问和配置	创建安全配置文件需要进行思科VNMC访问和配置。您可以通过 ASDM 中的“配置”>“设备设置”>“接口”窗格来配置对思科 VNMC 的访问。输入登录用户名和密码、主机名和共享密钥以访问思科VNMC。然后，您可以配置安全配置文件和安全配置文件接口。在VNMC模式下，使用 CLI 配置安全配置文件。
安全配置文件和安全配置文件接口	安全配置文件是对应于已在思科VNMC中配置并在思科Nexus 1000V VSM中分配的边缘安全配置文件的接口。直通流量的策略将分配给这些接口和外部接口。您可以通过“配置”>“设备设置”>“接口”窗格添加安全配置文件。您可以通过添加安全配置文件的名称并选择服务接口来创建安全配置文件。然后，ASDM 将通过思科 VNMC 生成安全配置文件，分配安全配置文件 ID，并自动生成唯一的接口名称。接口名称将在安全策略配置中使用。 引入或修改了以下命令：**interface security-profile**、**security-profile**、**mtu**、**vpath path-mtu**、**clear interface security-profile**、**clear configure interface security-profile**、**show interface security-profile**、**show running-config interface security-profile**、**show interface ip brief**、**show running-config mtu**、**show vsn ip binding**、**show vsn security-profile**。 引入或修改了以下菜单项： **配置 > 设备设置 > 接口** **配置 > 设备设置 > 接口 > 添加安全配置文件** **监控 > 接口 > 安全配置文件**
服务接口	服务接口是与安全配置文件接口关联的以太网接口。您只能配置一个服务接口，该接口必须是内部接口。 引入了以下命令：**service-interface security-profile all**。 修改了以下菜单项：**配置 > 设备设置 > 接口**。

功能	说明
VNMC 策略代理	VNMC 策略代理通过 ASDM 和 VNMC 模式启用策略配置。它包括一个 Web 服务器，用于从基于 HTTPS 的思科 VNMC 接收基于 XML 的请求，并将其转换为 ASA 1000V 配置。 引入了以下命令：**vnmc policy-agent**、**login**、**shared-secret**、**registration host**、**vnmc org**、**show vnmc policy-agent**、**show running-config vnmc policy-agent**、**clear configure vnmc policy-agent**。 修改了以下菜单项：**配置 > 设备设置 > 接口**。

版本 8.6 的新功能

ASA 8.6(1)/ASDM 6.6(1) 的新功能

发布日期：**2012** 年 **2** 月 **28** 日

注释 此 ASA 软件版本仅在 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X。

版本 8.6(1) 包括 8.4(2) 中的所有功能，另外添加了下表中列出的功能。

除非下表中明确列出，否则 8.6(1) 中不包括 8.4(3) 中添加的功能。

功能	说明
硬件功能	
支持 ASA 5512-X 至 ASA 5555-X	我们引入了对 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 的支持。
IPS 功能	
对适用于 5512-X 至 ASA 5555-X 的 ASA IPS SSP 的支持	我们为 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 引入了对 ASA IPS SSP 软件模块的支持。 引入或修改了以下命令：**session**、**show module**、**sw-module**。 未修改任何菜单项。
远程访问功能	

功能	说明
无客户端 SSL VPN 浏览器支持	ASA 现在支持使用 Microsoft Internet Explorer 9 和 Firefox 4 的无客户端 SSL VPN。 同样适用于版本 *8.4(3)*。
DTLS 和 TLS 压缩	为了提高吞吐量，思科现在在 AnyConnect 3.0 或更高版本上支持 DTLS 和 TLS 压缩。每种隧道传输方法会单独配置压缩，而首选配置是将 SSL 和 DTLS 都配置为 LZS。此功能增强了从旧版 VPN 客户端的迁移操作。 **注释** 在传输高度压缩数据的高速远程接入连接上使用数据压缩，要求 ASA 具备强大的处理能力。对于 ASA 上的其他活动和流量，平台上可支持的会话数量会下降。 引入或修改了以下命令：**anyconnect dtls compression** [**lzs** | **none**] 和 **anyconnect ssl compression** [**deflate** | **lzs** | **none**]。 修改了以下菜单项：**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 组策略 > 编辑 > 编辑内部组策略 > 高级 > AnyConnect 客户端 > SSL 压缩**。 同样适用于版本 *8.4(3)*。
无客户端 SSL VPN 会话超时风险通告	允许您创建自定义消息以提醒用户由于不活动或会话超时，他们的 VPN 会话即将终止。 引入了以下命令：**vpn-session-timeout alert-interval**、**vpn-idle-timeout alert-interval**。 引入了以下菜单项： 远程接入 VPN > 配置 > 无客户端 SSL VPN 访问 > 门户 > 自定义 > 添加/编辑 > 超时警报 远程访问 VPN > 配置 > 无客户端 SSL VPN 访问 > 组策略 > 添加/编辑常规 同样适用于版本 *8.4(3)*。
多情景模式功能	

功能	说明
自动生成 MAC 地址前缀	在多情景模式下，ASA 现在支持将自动 MAC 地址生成配置转换为使用默认前缀。ASA 根据接口 MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。前缀生成方法提供许多好处，包括更好地保证 MAC 地址在网段上的唯一性。您可以通过输入 **show running-config mac-address** 命令查看自动生成的前缀。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的MAC 地址生成方法不再可用。 **注释** 为了保持故障切换对无中断升级，如果已启用故障切换，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。但是，我们强烈建议您手动更改为生成的前缀方法。升级后，要使用MAC 地址生成的前缀方法，请重新启用MAC 地址生成来使用前缀。 修改了以下命令：**mac-address auto**。 修改了以下菜单项：**配置 > 情景管理 > 安全情景**
AAA 功能	
每属性最大 LDAP 值数增加	ASA 针对单一属性可接收的最大值数从 1000（默认）增加到了 5000，允许的范围为 500 到 5000。如果收到的响应消息超出配置的限制，ASA 将拒绝执行身份验证。如果 ASA 检测到单一属性包含 1000 多个值，该 ASA 将生成信息级别的系统日志 109036。如果超过 5000 个属性，ASA 将生成错误级别的系统日志 109037。 引入了以下命令：**ldap-max-value-range** *number*（请在 aaa-server 主机配置模式下输入此命令）。 ASDM 不支持该命令，请使用命令行工具输入该命令。 同样适用于版本 *8.4(3)*。

功能	说明
支持子范围 LDAP 搜索结果	如果 LDAP 搜索产生包含大量值的属性，则根据服务器配置，它可能会返回值的子范围并期望 ASA 针对其余的值范围发起其他查询。现在，ASA 会对其余范围发起多个查询，并将响应合并成一个完整的属性值阵列。 同样适用于版本 *8.4(3)*。
故障排除功能	
show asp table classifier 和 **show asp table filter** 命令的正则表达式匹配	现在，您可以使用正则表达式输入 **show asp table classifier** 和 **show asp table filter** 命令来过滤输出。 修改了以下命令：**show asp table classifier match** *regex*、**show asp table filter match** *regex*。 ASDM 不支持该命令，请使用命令行工具输入该命令。 同样适用于版本 *8.4(3)*。

版本 8.5 的新功能

ASA 8.5(1.7)/ASDM 6.5(1.101) 的新功能

发布日期：**2012** 年 **3** 月 **5** 日

注释 我们建议您仅在 Cisco.com 发布的 ASA 临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们通常会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。

我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个 ASA 临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

表 *1: ASA* 临时版本 *8.5(1.7)/ASDM* 版本 *6.5(1.101)* 的新功能

功能	说明
硬件功能	

功能	说明
支持 Catalyst 6500 管理引擎 2T	ASA 现在可与 Catalyst 6500 管理引擎 2T 进行互操作。有关硬件和软件的兼容性，请参阅：http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html。 注释 您可能需要升级 ASA 上的 FPD 映像。请参阅版本说明中的升级过程。
多情景功能	
ASDM 支持自动生成 MAC 地址前缀	现在，如果您不指定前缀，ASDM 会显示一个自动生成的前缀。 修改了以下菜单项：**配置 > 情景管理 > 安全情境**
故障切换功能	
配置批量同步期间的连接复制速率	现在，您可以配置 ASA 在使用状态故障切换时将连接复制到备用设备的速率。默认情况下，连接会在 15 秒内复制到备用设备。但是，当执行批量同步时（例如首次启用故障切换时），由于每秒最大连接数的限制，15 秒可能不足以同步大量连接。例如，ASA 的最大连接数为 800 万；在 15 秒内复制 800 万个连接意味着每秒创建 533,000 个连接。但是，每秒的最大连接数是 300K。您现在可以指定复制速率小于或等于每秒最大连接数，同步期间将会调整，直到所有连接均同步为止。 引入了以下命令：**failover replication rate** *rate*。 修改了以下菜单项：**配置 > 设备管理 > 高可用性 > 故障切换**。

ASA 8.5(1.6)/ASDM 6.5(1) 的新功能

发布日期：2012 年 1 月 27 日

注释 我们建议您仅在 Cisco.com 发布的 ASA 临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们通常会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。

我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个 ASA 临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

表 *2: ASA* 临时版本 *8.5(1.6)/ASDM* 版本 *6.5(1)* 的新功能

功能	说明
多情景功能	
自动生成 MAC 地址前缀	在多情景模式下，ASA 现在支持将自动 MAC 地址生成配置转换为使用默认前缀。ASA 根据背板 MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。前缀生成方法提供许多好处，包括更好地保证 MAC 地址在网段上的唯一性。您可以通过输入 **show running-config mac-address** 命令查看自动生成的前缀。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的MAC 地址生成方法不再可用。 **注释** 为了保持故障切换对无命中地升级，如果已启用故障切换，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。但是，我们强烈建议您在使用故障切换时，手动将生成方法更改为前缀方法。如果没有前缀方法，安装在不同插槽编号的 ASASM 在故障切换时会遇到 MAC 地址变更，并可能会遇到流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址生成来使用前缀。 修改了以下命令：**mac-address auto**。 ASDM 没有变化。

ASA 8.5(1)/ASDM 6.5(1) 的新功能

发布日期：2011 年 7 月 8 日

此 ASA 和 ASDM 软件版本仅在 ASASM 上受支持。

版本 8.5(1) 包括 8.4(1) 中的所有功能，另外添加了下表中列出的功能。但是，以下功能在无负载加密软件中不受支持，此版本仅作为无负载加密版本提供：

- VPN
- 统一通信

除非下表中明确列出，否则 8.5(1) 中不包括 8.4(2) 中添加的功能。

表 *3: ASA* 版本 *8.5(1)/ASDM* 版本 *6.5(1)* 的新功能

功能	说明
硬件功能	
支持 ASA 服务模块	我们面向思科 Catalyst 6500 E 交换机引入了对 ASASM 的支持。
防火墙功能	
在多情景模式下支持混合防火墙模式	可以在多情景模式下为每个情景独立设置防火墙模式，因此某些情景可在透明模式下运行，而另一些情景则可在路由模式中运行。 修改了以下命令：**firewall transparent**。 不能在ASDM中设置防火墙模式；必须使用命令行界面进行设置。
接口功能	
在多情景模式下，自动 MAC 地址生成现在默认处于启用状态	在多情景模式下，自动 MAC 地址生成现在默认处于启用状态。 修改了以下命令：**mac address auto**。 修改了以下菜单项：系统 > 配置 > 情景管理 > 安全情景。
NAT 功能	

功能	说明
身份 NAT 可配置代理 ARP 和路由查找	在身份 NAT 的更早版本中，代理 ARP 被禁用，始终使用路由查找确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。 对于 8.3 之前版本的配置，NAT 免除规则（**nat 0 access-list** 命令）至 8.4(2) 及更高版本的迁移现包含以下关键字，以禁用代理 ARP 并使用路由查找：**no-proxy-arp** 和 **route-lookup**。用于迁移至 8.3(2) 和 8.4(1) 的 **unidirectional** 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置现包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字已删除。 修改了以下命令：**nat static** [**no-proxy-arp**] [**route-lookup**]（对象网络）和 **nat source static** [**no-proxy-arp**] [**route-lookup**]（全局）。 修改了以下菜单项： 配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象 > 高级 NAT 设置 配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则 同样适用于版本 *8.4(2)*。

功能	说明
PAT 池和轮询地址分配	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程更轻松。 **注释** 当前在 8.5(1) 中，不可将 PAT 池功能用作动态 NAT 或 PAT 的回退方法。只能将 PAT 池配置为动态 PAT 的主要方法 (CSCtq20634)。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（对象网络）和 **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（全局）。 修改了以下菜单项： 配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象 配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则 同样适用于版本 *8.4(2)*。
交换机集成功能	
自动状态	交换机管理引擎可向 ASASM 发送自动状态消息，说明与 ASA VLAN 关联的物理接口状态。例如，当与 VLAN 关联的所有物理接口关闭时，自动状态消息会告知 ASA VLAN 已关闭。此信息可让 ASA 宣告 VLAN 已关闭，避免像平常一样需要通过监测接口来确定链路故障端。自动状态消息大幅缩短了 ASA 检测链路故障的时间（只需要几毫秒，而没有自动状态支持时则需要长达 45 秒）。 **注释** 只有在机箱中安装单个 ASA，该交换机才支持自动状态消息。 请参阅以下思科 IOS 命令：**firewall autostate**。
虚拟交换系统	当 ASASM 在交换机上配置时支持 VSS。无需进行 ASA 配置。

版本 8.4 的新功能

ASA 8.4(7)/ASDM 7.1(3) 的新功能

发布日期：**2013** 年 **9** 月 **3** 日

ASA 8.4(7)/ASDM 7.1(3) 中无新增功能。

ASA 8.4(6)/ASDM 7.1(2.102) 的新功能

发布日期：**2013** 年 **4** 月 **29** 日

功能	说明
监控功能	
能够查看前 10 个内存用户	现在，您可以查看已分配的排名靠前的容器大小以及每个已分配容器大小的前 10 台 PC。以前，您必须输入多个命令才能查看这些信息（**show memory detail** 命令和 **show memory binsize** 命令）；新命令提供了更快分析内存问题的方式。 引入了以下命令：**show memory top-usage**。 未更改 ASDM。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。
CPU 配置文件增强	**cpu profile activate** 命令现在支持以下操作： • 分析器在触发前的延迟启动（全局或特定线程 CPU%） • 抽样单个线程 修改了以下命令：**cpu profile activate** [*n-samples*] [**sample-process** *process-name*] [**trigger cpu-usage** *cpu%* [*process-name*]。 未更改 ASDM。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。
远程访问功能	

功能	说明
Show 命令现在对 **user-storage value** 命令密码进行了加密	现在，输入 **show running-config** 时会对 **user-storage value** 命令中的密码进行加密。 修改了以下命令：**user-storage value**。 修改了以下菜单项：**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 组策略 > 更多选项 > 会话设置**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。

ASA 8.4(5)/ASDM 7.0(2) 的新功能

发布日期：2012 年 10 月 31 日

功能	说明
防火墙功能	
对于 IS-IS 流量支持 EtherType ACL（透明防火墙模式）	在透明防火墙模式下，ASA 现在可使用 EtherType ACL 传输 IS-IS 流量。 修改了以下命令：**access-list ethertype** {**permit** | **deny**} **is-is**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > EtherType 规则**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。

功能	说明
针对未连接的子网添加 ARP 缓存	在默认情况下，ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则不建议启用此功能。此功能可能有助于引发对 ASA 的拒绝服务 (DoS) 攻击；任意接口上的用户都可能发出许多 ARP 应答，并使 ASA ARP 表中的错误条目超载。 如果您使用以下对象，则可能要使用此功能： • 辅助子网。 • 用于流量转发的相邻路由上的代理 ARP。 引入了以下命令：**arp permit-nonconnected**。 修改了以下菜单项：**配置 > 设备管理 > 高级 > ARP > ARP 静态表**。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。
服务策略规则增加的最大连接数限制	服务策略规则的最大连接数从 65535 增加至 2000000。 修改了以下命令：**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 连接设置**。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。
远程访问功能	
改进了 Host Scan 和 ASA 互操作性	Host Scan 和 ASA 使用改良的过程从客户端向 ASA 传送安全评估属性。这使得 ASA 有更多时间与客户端建立 VPN 连接和应用动态范围策略。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。
思科安全桌面： Windows 8 支持	CSD 3.6.6215 更新为在“预登录策略”操作系统检查中支持 Windows 8 选项。 请参阅以下限制： • 对于 Windows 8 不支持安全桌面 (Vault)。

功能	说明
动态访问策略： Windows 8 支持	ASDM 更新为在“DAP 操作系统”属性中支持 Windows 8 选项。
监控功能	
NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 将允许 Xlate count 轮询。	添加对 NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 的支持以支持 SNMP xlate_count 和 max_xlate_count。 此数据等同于 **show xlate count** 命令。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。
NSEL	引入了 Flow-update 事件，以便定期提供数据流流量的字节计数器。您可以更改系统向 NetFlow 收集器发送 flow-update 事件的时间间隔。您可以对 flow-update 记录被发送到的收集器进行过滤。 引入了以下命令：**flow-export active refresh-interval**。 修改了以下命令：**flow-export event-type**。 修改了以下菜单项： **配置 > 设备管理 > 日志记录 > NetFlow**。 **配置 > 防火墙 > 服务策略规则 > 添加服务策略规则向导 - 规则操作 > NetFlow > 添加流事件** 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。
硬件功能	
ASA 5585-X DC 电源支持	添加了对 ASA 5585-X 直流电源的支持。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。

ASA 8.4(4.5)/ASDM 6.4(9.103) 的新功能

发布日期：2012 年 8 月 13 日

注释 由于内部版本问题，从 Cisco.com 中删除了版本 8.4(4.3)；请升级到版本 8.4(4.5) 或更高版本。

我们建议您仅在 Cisco.com 发布的临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。我们会在发布下一个维护或功能版本时记录临时版本的功能。 有关每个临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

功能	说明
防火墙功能	
针对未连接的子网添加 ARP 缓存	在默认情况下，ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则不建议启用此功能。此功能可能有助于引发对 ASA 的拒绝服务 (DoS) 攻击；任意接口上的用户都可能发出许多 ARP 应答，并使 ASA ARP 表中的错误条目超载。 如果您使用以下对象，则可能要使用此功能： • 辅助子网。 • 用于流量转发的相邻路由上的代理 ARP。 引入了以下命令：**arp permit-nonconnected**。 修改了以下菜单项：**配置 > 设备管理 > 高级 > ARP > ARP 静态表**。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。
监控功能	
NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 将允许 Xlate count 轮询。	添加对 NAT-MIB cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 的支持以支持 SNMP xlate_count 和 max_xlate_count。 此数据等同于 **show xlate count** 命令。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)* 或 *9.1(1)* 中不可用。

ASA 8.4(4.1)/ASDM 6.4(9) 的新功能

发布日期：2012 年 6 月 18 日

注释 由于内部版本问题，从 Cisco.com 中删除了版本 8.4(4)；请升级到版本 8.4(4.1) 或更高版本。

功能	说明
认证功能	
FIPS 和通用标准认证	FIPS 140-2 非专有安全策略在对思科 ASA 5500 系列的级别 2 FIPS 140-2 验证中进行了更新，其中包括思科 ASA 5505、ASA 5510、ASA 5520、ASA 5540、ASA 5550、ASA 5580 和 ASA 5585-X。 更新了通用标准评估保障层 4 (EAL4)，该标准是思科 ASA 和 VPN 平台解决方案特定评估目标 (TOE) 的基础。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。
使用本地数据库时，支持管理员密码策略。	使用本地数据库配置用于CLI或ASDM访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 引入或修改了以下命令： **change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**。 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 密码策略**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。

功能	说明
对 SSH 公钥身份验证的支持	对于与 ASA 的 SSH 连接，您现在可以使用最多 2048 位的 Base64 密钥基于每个用户启用公钥身份验证。 引入了以下命令：**ssh authentication**。 引入了以下菜单项：**配置 > 设备管理 > 用户/AAA > 用户帐户 > 编辑用户帐户 > 公钥身份验证** 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。
支持用于 SSH 密钥交换的 Diffie-Hellman 群 14	已添加支持 Diffie-Hellman 组 14 进行 SSH 密钥交换。以前，只支持组 1。 引入了以下命令：**ssh key-exchange**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > ASDM/HTTPS/Telnet/SSH**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。
支持管理会话最大数量	您可以设置并发 ASDM、SSH 和 Telnet 会话的最大数量。 引入了以下命令：**quota management-session**、**show running-config quota management-session**、**show quota management-session**。 引入了以下菜单项：**配置 > 设备管理 > 管理访问 > 管理会话配额**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。

功能	说明

适用于 SSL 加密的其他短暂 Diffie-Hellman 密码	ASA 现在支持以下短暂的 Diffie-Hellman (DHE) SSL 密码套件：
	• DHE-AES128-SHA1
	• DHE-AES256-SHA1
	这些密码套件在 RFC 3268“适用于传输层安全 *(TLS)* 的高级加密标准 *(AES)* 密码套件”中指定。
	当客户端支持 DHE 时，DHE 将是首选密码，因为它提供完全前向保密 (Perfect Forward Secrecy)。请参阅以下限制：
	• SSL 3.0 连接中不支持 DHE，所以请务必同时对 SSL 服务器启用 TLS 1.0。
	`!! set server version`
	`ciscoasa(config)# ssl server-version tlsv1 sslv3`
	`!! set client version`
	`ciscoasa(config) # ssl client-version any`
	• 有些常见应用不支持 DHE，所以请至少包括一种其他 SSL 加密方法，以确保可以使用对 SSL 客户端和服务器通用的密码套件。
	• 有些客户端可能不支持 DHE，包括 AnyConnect 2.5 和 3.0、思科安全桌面和 Internet Explorer 9.0。
	修改了以下命令：**ssl encryption**。
	修改了以下菜单项：**配置 > 设备管理 > 高级 > SSL 设置**。
	此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。

映像验证	添加了对 SHA-512 映像完整性检查的支持。 修改了以下命令：**verify**。 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。

功能	说明
改进的伪随机数生成	基于软件的随机数生成过程中添加了基于硬件的附加熵的噪声。这种变化使得伪随机数生成 (PRNG) 更加随机，更难让攻击者获得可重复的模式或猜测下一个要用于加密和解密操作的随机数。为改进 PRNG 进行了两项更改： • 将当前用于随机数据的基于硬件的 RNG 用作基于软件的 RNG 的参数之一。 • 如果基于硬件的 RNG 不可用，请为基于软件的 RNG 使用其他硬件噪声源。根据您的型号，使用以下硬件传感器： • ASA 5505 - 电压传感器。 • ASA 5510 和 5550 - 风扇速度传感器。 • ASA 5520、5540 和 5580 - 温度传感器。 • ASA 5585-X - 风扇速度传感器。 引入了以下命令：**show debug menu cts** [**128** | **129**] 此功能在 *8.5(1)*、*8.6(1)*、*8.7(1)*、*9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。
远程访问功能	
无客户端 SSL VPN： 改进了重写程序引擎的质量	显著改进了无客户端 SSL VPN 重写程序引擎以提供更好的质量和效率。因此，您可以预计无客户端 SSL VPN 用户将获得更好的最终用户体验。 对于此功能，我们未添加或修改任何命令。 对于此功能，我们未添加或修改任何 ASDM 菜单项。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。
故障切换功能	

功能	说明
配置批量同步期间的连接复制速率	现在，您可以配置 ASA 在使用状态故障切换时将连接复制到备用设备的速率。默认情况下，连接会在 15 秒内复制到备用设备。但是，当执行批量同步时（例如首次启用故障切换时），由于每秒最大连接数的限制，15 秒可能不足以同步大量连接。例如，ASA 的最大连接数为 800 万；在 15 秒内复制 800 万个连接意味着每秒创建 533,000 个连接。但是，每秒允许的最大连接数是 300 K。您现在可以指定复制速率小于或等于每秒最大连接数，同步期间将会调整，直到所有连接均同步为止。 引入了以下命令：**failover replication rate** *rate*。 此功能在 *8.6(1)* 或 *8.7(1)* 中不可用。*8.5(1.7)* 中也包含此功能。
应用检测功能	
SunRPC 从动态 ACL 更改为针孔机制	以前，Sun RPC 检测不支持出站访问列表，因为该检测引擎使用的是动态访问列表，而不是辅助连接。 在此版本中，当在 ASA 上配置动态访问列表时，仅在入口方向支持该检测，ASA 会丢弃传至目标端口的出口流量。因此，Sun RPC 检测会实施针孔机制来支持出口流量。Sun RPC 检测使用此针孔机制来支持出站动态访问列表。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。

功能	说明
检测重置操作更改	以前，当 ASA 因检测引擎规则丢弃数据包时，ASA 仅向被丢弃数据包的源设备发送一个 RST。此行为可能会导致资源问题。 在此版本中，如果将检测引擎配置为使用重置操作，当数据包触发重置时，ASA 在以下条件下会发送一个 TCP 重置： • 当启用 **service resetoutbound** 命令时，ASA 向内部主机发送一个 TCP 重置。（默认情况下，**service resetoutbound** 命令处于禁用状态。） • 当启用 **service resetinbound** 命令时，ASA 向外部主机发送一个 TCP 重置。（默认情况下，禁用 **service resetinbound** 命令。） 有关详细信息，请参阅 ASA 命令参考中的 **service** 命令。 此行为可确保重置操作重置 ASA 和内部服务器上的连接；因此抵抗拒绝服务攻击。对于外部主机，ASA 默认不发送重置并且不会通过 TCP 重置显示信息。 此功能在 *8.5(1)*、*8.6(1)* 或 *8.7(1)* 中不可用。
模块功能	

功能	说明
ASA 5585-X 对 ASA CX SSP-10 和 -20 的支持	通过 ASA CX 模块，您可以根据某个情况的全部情景实施安全措施。此情景包括用户身份（身份）、用户要访问的应用或网站（事情）、访问的来源（地点）、访问的时间（时间）和用于访问的设备的属性（方式）。通过 ASA CX 模块，您可以提取流量的全部情景并执行精细策略，例如允许访问 Facebook，但不允许访问 Facebook 上的游戏，或允许财务人员访问敏感的企业数据库，但不允许其他员工进行同样的访问。 引入或修改了以下命令：**capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**，**session do get-config**，**session do password-reset**，**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module** 和 **show service-policy**。 引入了以下菜单项： **主页 > ASA CX 状态向导 > 启动向导 > ASA CX 基本配置** **配置 > 防火墙 > 服务策略规则 > 添加服务策略规则 > 规则行为 > ASA CX 检查**
ASA 5585-X 对网络模块的支持	ASA 5585-X 的插槽 1 中现在支持网络模块上的其他接口。您可以安装下面一个或两个可选网络模块： • ASA 4-端口 10G 网络模块 • ASA 8-端口 10G 网络模块 • ASA 20-端口 1G 网络模块 此功能在 *9.0(1)*、*9.0(2)* 或 *9.1(1)* 中不可用。

ASA 8.4(3)/ASDM 6.4(7) 的新功能

发布日期：**2012** 年 **1** 月 **9** 日

功能	说明
NAT 功能	

功能	说明
轮询 PAT 池分配技术使用现有主机的相同 IP 地址	组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。 未修改任何命令。 未修改任何菜单项。 此功能在 *8.5(1)* 或*8.6(1)* 中不可用。
用于 PAT 池的不分段 PAT 端口范围	如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，1024 以下的端口只有一个小 PAT 池。 如果大量流量使用较小的端口范围，在使用 PAT 池时，现可指定使用以下不分段端口范围，代替三个分段大小不等的端口范围：1024 至 65535，或 1 至 65535。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]（对象网络配置模式）和 **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]（全局配置模式）。 修改了以下菜单项： **配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象** **配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则** 此功能在 *8.5(1)* 或*8.6(1)* 中不可用。

功能	说明
用于 PAT 池的扩展 PAT	每个 PAT IP 地址允许最多 65535 个端口。如果 65535 个端口不能提供足够的转换，则现可启用适合 PAT 池的扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**extended**]]（对象网络配置模式）和 **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]]（全局配置模式）。 修改了以下菜单项： **配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象** **配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则** 此功能在 *8.5(1)* 或*8.6(1)* 中不可用。
可配置 PAT 转换超时	如果 PAT 转换超时（默认为 30 秒后）且 ASA 使用该端口执行新的转换，因为以前的连接在上游设备中可能仍处于打开状态，有些上游路由器可能会拒绝该新连接。PAT 转换超时现在可配置为一个介于 30 秒到 5 分钟之间的值。 引入了以下命令：**timeout pat-xlate**。 修改了以下菜单项：**配置 > 防火墙 > 高级 > 全局超时**。 此功能在 *8.5(1)* 或*8.6(1)* 中不可用。

功能	说明
自动 NAT 规则，可将 VPN 对等体的本地 IP 地址转换回对等体的实际 IP 地址	在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 IP 地址。 可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。可使用 **show nat** 命令查看这些规则。 **注释** 由于路由问题，除非您确定自己需要此功能，否则我们不建议使用此功能。请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制： • 仅支持思科 IPSec 和 AnyConnect Client。 • 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。 • 不支持负载均衡（由于路由问题）。 • 不支持漫游（公共 IP 更改）。 引入了以下命令：**nat-assigned-to-public-ip** *interface*（tunnel-group general-attributes 配置模式）。 ASDM 不支持该命令，请使用命令行工具输入该命令。
远程访问功能	
无客户端 SSL VPN 浏览器支持	ASA 现在支持使用 Microsoft Internet Explorer 9 和 Firefox 4 的无客户端 SSL VPN。

功能	说明
DTLS 和 TLS 压缩	为了提高吞吐量，思科现在在 AnyConnect 3.0 或更高版本上支持 DTLS 和 TLS 压缩。每种隧道传输方法会单独配置压缩，而首选配置是将 SSL 和 DTLS 都配置为 LZS。此功能增强了从旧版 VPN 客户端的迁移操作。 注释 在传输高度压缩数据的高速远程访问连接上使用数据压缩，要求 ASA 具备强大的处理能力。对于 ASA 上的其他活动和流量，平台上可支持的会话数量会下降。 引入或修改了以下命令：**anyconnect dtls compression** [**lzs** | **none**] 和 **anyconnect ssl compression** [**deflate** | **lzs** | **none**]。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 编辑 > 编辑内部组策略 > 高级 > AnyConnect 客户端 > SSL 压缩**。
无客户端 SSL VPN 会话超时风险通告	允许您创建自定义消息以提醒用户由于不活动或会话超时，他们的 VPN 会话即将终止。 引入了以下命令：**vpn-session-timeout alert-interval**、**vpn-idle-timeout alert-interval**。 引入了以下菜单项： **远程访问 VPN > 配置 > 无客户端 SSL VPN 访问 > 门户 > 自定义 > 添加/编辑 > 超时通知** **远程访问 VPN > 配置 > 无客户端 SSL VPN 访问 > 组策略 > 添加/编辑通用**
AAA 功能	
每属性最大 LDAP 值数增加	ASA 针对单一属性可接收的最大值数从 1000（默认）增加到了 5000，允许的范围为 500 到 5000。如果收到的响应消息超出配置的限制，ASA 将拒绝执行身份验证。如果 ASA 检测到单一属性包含 1000 多个值，该 ASA 将生成信息级别的系统日志 109036。如果超过 5000 个属性，ASA 将生成错误级别的系统日志 109037。 引入了以下命令：**ldap-max-value-range** *number*（请在 aaa-server 主机配置模式下输入此命令）。 ASDM 不支持该命令，请使用命令行工具输入该命令。

功能	说明
支持子范围 LDAP 搜索结果	如果 LDAP 搜索产生包含大量值的属性，则根据服务器配置，它可能会返回值的子范围并期望 ASA 针对其余的值范围发起其他查询。现在，ASA 会对其余范围发起多个查询，并将响应合并成一个完整的属性值阵列。
在来自 ASA 的 RADIUS 访问请求和计费请求数据包中发送主要的供应商特有属性 (VSA)	四个新 VSA - 通过来自 ASA 的 RADIUS 访问请求数据包发送 Tunnel Group Name (146) 和 Client Type (150)。通过来自 ASA 的 RADIUS 记帐请求数据包发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记帐请求数据包（Start、Interim-Update 和 Stop）发送全部四个属性。RADIUS 服务器（例如 ACS 和 ISE）可以执行授权和策略属性，或者将这些属性用于记帐和收费。
故障排除功能	
show asp table classifier 和 **show asp table filter** 命令的正则表达式匹配	现在，您可以使用正则表达式输入 **show asp table classifier** 和 **show asp table filter** 命令来过滤输出。 修改了以下命令：**show asp table classifier match** *regex*、**show asp table filter match** *regex*。 ASDM不支持该命令，请使用命令行工具输入该命令。

ASA 8.4(2.8)/ASDM 6.4(5.106) 的新功能

发布日期：2011 年 8 月 31 日

注释 我们建议您仅在 Cisco.com 发布的 ASA 临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们通常会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。

我们会在发布下一个维护或功能版本时记录临时版本的功能。 有关每个 ASA 临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

功能	说明
远程访问功能	

功能	说明
无客户端 SSL VPN 浏览器支持	ASA 现在支持使用 Microsoft Internet Explorer 9 和 Firefox 4 的无客户端 SSL VPN。 同样适用于版本 *8.2(5.13)* 和 *8.3.2(25)*。
DTLS 和 TLS 压缩	为了提高吞吐量，思科现在在 AnyConnect 3.0 或更高版本上支持 DTLS 和 TLS 压缩。每种隧道传输方法会单独配置压缩，而首选配置是将 SSL 和 DTLS 都配置为 LZS。此功能增强了从旧版 VPN 客户端的迁移操作。 **注释** 在传输高度压缩数据的高速远程访问连接上使用数据压缩，要求 ASA 具备强大的处理能力。对于 ASA 上的其他活动和流量，平台上可支持的会话数量会下降。 引入或修改了以下命令：**anyconnect dtls compression** [**lzs** | **none**] 和 **anyconnect ssl compression** [**deflate** | **lzs** | **none**]。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 编辑 > 编辑内部组策略 > 高级 > AnyConnect 客户端 > SSL 压缩**。 同样适用于版本 *8.2(5.13)* 和 *8.3.2(25)*。
无客户端 SSL VPN 会话超时风险通告	允许您创建自定义消息以提醒用户由于不活动或会话超时，他们的 VPN 会话即将终止。 引入了以下命令：**vpn-session-timeout alert-interval**、**vpn-idle-timeout alert-interval**。 引入了以下菜单项： **远程访问 VPN > 配置 > 无客户端 SSL VPN 访问 > 门户 > 自定义 > 添加/编辑 > 超时通知** **远程访问 VPN > 配置 > 无客户端 SSL VPN 访问 > 组策略 > 添加/编辑通用**
AAA 功能	

功能	说明
每属性最大 LDAP 值数增加	ASA 针对单一属性可接收的最大值数从 1000（默认）增加到了 5000，允许的范围为 500 到 5000。如果收到的响应消息超出配置的限制，ASA 将拒绝执行身份验证。如果 ASA 检测到单一属性包含 1000 多个值，该 ASA 将生成信息级别的系统日志 109036。如果超过 5000 个属性，ASA 将生成错误级别的系统日志 109037。 引入了以下命令：**ldap-max-value-range** *number*（请在 aaa-server 主机配置模式下输入此命令）。 ASDM 不支持该命令，请使用命令行工具输入该命令。
支持子范围 LDAP 搜索结果	如果 LDAP 搜索产生包含大量值的属性，则根据服务器配置，它可能会返回值的子范围并期望 ASA 针对其余的值范围发起其他查询。现在，ASA 会对其余范围发起多个查询，并将响应合并成一个完整的属性值阵列。
故障排除功能	
show asp table classifier 和 **show asp table filter** 命令的正则表达式匹配	现在，您可以使用正则表达式输入 **show asp table classifier** 和 **show asp table filter** 命令来过滤输出。 修改了以下命令：**show asp table classifier match** *regex*、**show asp table filter match** *regex*。 ASDM 不支持该命令，请使用命令行工具输入该命令。 同样适用于版本 *8.2(5.13)* 和 *8.3.2(25)*。

ASA 8.4(2)/ASDM 6.4(5) 的新功能

发布日期：**2011** 年 **6** 月 **20** 日

功能	说明
防火墙功能	

功能	说明
身份防火墙	

功能	说明
	通常，防火墙不知道用户的身份，因此无法基于身份应用安全策略。 ASA 中的身份防火墙可基于用户身份提供更加精细的访问控制。您可以基于用户名和用户组名而不是通过源 IP 地址来配置访问规则和安全策略。ASA 会基于 IP 地址与 Windows Active Directory 登录信息的关联应用安全策略，并基于映射的用户名（而不是网络 IP 地址）报告事件。 身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Window Active Directory 相集成。ASA 使用 Windows Active Directory 作为源来检索特定 IP 地址的当前用户身份信息。 在企业中，一些用户通过使用其他身份验证机制登录网络，例如通过 Web 门户（直通代理）或 VPN 进行身份验证。您可以将身份防火墙配置为在与基于身份的访问策略的连接中允许这些类型的身份验证。 引入或修改了以下命令：**user-identity enable**、**user-identity default-domain**、**user-identity domain**、**user-identity logout-probe**、**user-identity inactive-user-timer**、**user-identity poll-import-user-group-timer**、**user-identity action netbios-response-fail**、**user-identity user-not-found**、**user-identity action ad-agent-down**、**user-identity action mac-address-mismatch**、**user-identity action domain-controller-down**、**user-identity ad-agent active-user-database**、**user-identity ad-agent hello-timer**、**user-identity ad-agent aaa-server**、**user-identity update import-user**、**user-identity static user**、**ad-agent-mode**、**dns domain-lookup**、**dns poll-timer**、**dns expire-entry-timer**、**object-group user**、**show user-identity**、**show dns**、**clear configure user-identity**、**clear dns**、**debug user-identity** 和 **test aaa-server ad-agent**. 引入了以下菜单项： 配置 > 防火墙 > 身份选项。配置 > 防火墙 > 对象 > 本地用户组 监控 > 属性 > 身份

功能	说明
	修改了以下菜单项： **配置 > 设备管理 > 用户/AAA > AAA 服务器组 > 添加/编辑服务器组**。
身份 NAT 可配置代理 ARP 和路由查找	在身份 NAT 的更早版本中，代理 ARP 被禁用，始终使用路由查找确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。 对于 8.3 之前版本的配置，NAT 免除规则（**nat 0 access-list** 命令）至 8.4(2) 及更高版本的迁移现包含以下关键字，以禁用代理 ARP 并使用路由查找：**no-proxy-arp** 和 **route-lookup**。用于迁移至 8.3(2) 和 8.4(1) 的 **unidirectional** 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置现包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字已删除。 修改了以下命令：**nat static** [**no-proxy-arp**] [**route-lookup**]（对象网络）和 **nat source static** [**no-proxy-arp**] [**route-lookup**]（全局）。 修改了以下菜单项： **配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象 > 高级 NAT 设置** **配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则**

功能	说明
PAT 池和轮询地址分配	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程更轻松。 注释 当前在 8.4(2) 中，不可将 PAT 池功能用作动态 NAT 或 PAT 的回退方法。只能将 PAT 池配置为动态 PAT 的主要方法 (CSCtq20634)。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（对象网络）和 **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（全局）。 修改了以下菜单项： **配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象** **配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则**

功能	说明
IPv6 检测	通过将服务策略配置为基于扩展信头选择性地阻止 IPv6 流量，可以配置 IPv6 流量。IPv6 数据包需要接受早期的安全检查。在阻止路由器信头并且没有下一个信头时，ASA 总是传递逐跳和目标选项类型的扩展信头。 您可以启用默认的 IPv6 检查或自定义 IPv6 检查。通过为 IPv6 检查定义策略映射，可以将 ASA 配置为基于 IPv6 数据包中随处可见的以下类型的扩展信头来选择性地丢弃 IPv6 数据包： • 逐跳选项 • 路由（类型 0） • 分段 • 目标选项 • 身份验证 • 封装安全负载 修改了以下命令：**policy-map type inspect ipv6**、**verify-header**、**match header**、**match header routing-type**、**match header routing-address count gt**、**match header count gt**。 引入了以下菜单项：**配置 > 防火墙 > 对象 > 检查映射 > IPv6**。
远程访问功能	
门户访问规则	此增强功能让客户可以配置全局无客户端 SSL VPN 访问策略，以根据 HTTP 报头中的数据允许或拒绝无客户端 SSL VPN 会话。如果访问遭到拒绝，系统会向客户端返回错误代码。由于此拒绝操作是在用户身份验证之前发生的，所以可以减少处理资源的使用。 修改了以下命令：**webvpn portal-access-rule**。 修改了以下菜单项：**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 门户 > 门户访问规则**。 同样适用于版本 *8.2(5)*。
对 Microsoft Outlook Web App 2010 的无客户端支持	ASA 8.4(2) 无客户端 SSL VPN 核心重写器现在支持 Microsoft Outlook Web App 2010。

功能	说明
安全哈希算法 SHA-2 支持 IPSec IKEv2 完整性和 PRF	此版本支持安全哈希算法 SHA-2，用于增强与 IPSec/IKEv2 AnyConnect 安全移动客户端与 ASA 的连接的加密哈希安全性。SHA-2 包括具有 256、384 或 512 位摘要的哈希函数，以满足美国政府的要求。 修改了以下命令：**integrity**、**prf, show crypto ikev2 sa detail** 和 **show vpn-sessiondb detail remote**。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > IKE 策略 > 添加/编辑 IKEv2 策略**（提议）。
安全哈希算法 SHA-2 支持基于 IPSec IKEv2 的数字签名	此版本支持使用 SHA-2 兼容的签名算法来对使用数字证书的 IPSec IKEv2 VPN 连接进行身份验证，其哈希大小为 SHA-256、SHA-384 和 SHA-512。 IPSec IKEv2 连接的 SHA-2 的数字签名受 AnyConnect 安全移动客户端版本 3.0.1 或更高版本的支持。
AnyConnect 的拆分隧道策略	此版本包括一个推送到 AnyConnect 安全移动客户端的新策略，用于解析通过拆分隧道的 DNS 地址。此策略适用于使用 SSL 或 IPSec/IKEv2 协议的 VPN 连接，并指示 AnyConnect 客户端解析通过 VPN 隧道的所有 DNS 地址。如果 DNS 解析失败，则地址将保持未解析状态，而且 AnyConnect 客户端不会尝试通过公共 DNS 服务器解析地址。 默认情况下，此功能处于禁用状态。客户端根据拆分隧道策略（隧道化所有网络、隧道化网络列表中指定的网络或排除网络列表中指定的网络）通过隧道发送 DNS 查询。 引入了以下命令：split-tunnel-all-dns。 修改了以下菜单项：**配置 > 远程接入 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑组策略 > 高级 > 拆分隧道**（请参阅“通过隧道发送所有 DNS 查找”复选框）。 同样适用于版本 *8.2.(5)*。

功能	说明
移动状况 （以前称为适用于移动设备检测的 AnyConnect 标识扩展）	现在，您可以将 ASA 配置为允许或拒绝到移动设备的 VPN 连接，在每个组的基础上启用或禁用移动设备访问，并根据移动设备的姿态数据收集有关已连接的移动设备的信息。支持此功能的移动平台如下：iPhone/iPad/iPod 版 AnyConnect 2.5.x 和 Android 版 AnyConnect 2.4.x。 许可要求 实施远程访问控制和从移动设备收集安全评估数据要求在 ASA 上安装一个 AnyConnect Mobile 许可证和一个 AnyConnect 基础版或 AnyConnect 高级版许可证。您将根据安装的许可证收到以下功能： • **AnyConnect 高级版许可证功能** 安装 AnyConnect 高级版许可证的企业将能够根据 DAP 属性和任何其他现有终端属性，在受支持的移动设备上实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。 • **AnyConnect 基础版许可证功能** 安装 AnyConnect 基础版许可证的企业将能够执行以下任务： • 逐个组启用或禁用移动设备访问，以及使用 ASDM 配置该功能。 • 通过 CLI 或 ASDM 显示有关已连接移动设备的信息，这些移动设备并不具有实施 DAP 策略或者拒绝或允许对其进行远程访问的能力。 修改了以下菜单项：**配置 > 远程接入 VPN > 网络（客户端）访问 > 动态访问策略 > 添加/编辑终端属性 > 终端属性类型: AnyConnect**。 同样适用于版本 *8.2.(5)*。

功能	说明
SSL SHA-2 数字签名	现在，您可以使用符合 SHA-2 规范的签名算法对使用数字证书的 SSL VPN 连接进行身份验证。针对 SHA-2 的支持包括所有三种散列大小：SHA-256、SHA-384 和 SHA-512。SHA-2 需要 AnyConnect 2.5(1) 或更高版本（建议为 2.5(2) 或更高版本）。此版本不支持对其他用途或产品使用 SHA-2。 注意：要支持 SHA-2 连接的故障切换，备用 ASA 必须运行相同的映像。 修改了以下命令：**show crypto ca certificate**（“签名算法”字段标识生成签名时使用的摘要式算法）。 未修改任何菜单项。 同样适用于版本 *8.2.(5)*。
对于 Microsoft Windows 7 和 Android 本机 VPN 客户端支持 SHA2 证书签名	使用 L2TP/IPSec 协议时，ASA 对于 Microsoft Windows 7 和 Android 本机 VPN 客户端支持 SHA2 证书签名。 未修改任何命令。 未修改任何菜单项。 同样适用于版本 *8.2.(5)*。
启用/禁用证书映射以覆盖“组 URL”属性	此功能在连接配置文件选择过程中会更改连接配置文件首选项。默认情况下，如果 ASA 将连接配置文件中指定的证书字段值与终端所用证书的字段值进行匹配，ASA 会将该配置文件分配到 VPN 连接。此可选功能会更改指定终端所请求的组 URL 的连接配置文件的首选项。通过该新选项，管理员可采用许多旧版 ASA 软件使用的组 URL 首选项。 引入了以下命令：**tunnel-group-preference** 修改了以下菜单项： **配置 > 远程访问 VPN > 无客户端 SSL VPN > 连接配置文件** **配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件** 同样适用于版本 *8.2.(5)*。
ASA 5585-X 功能	

功能	说明
对适用于 SSP-40 和 SSP-60 的双 SSP 的支持	对于 SSP-40 和 SSP-60，您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP（例如，不支持混用 SSP-40 和 SSP-60）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障切换对。 注释 当在机箱中使用两个 SSP 时不支持 VPN；但请注意，VPN 并没有被禁用。 修改了以下命令：**show module**、**show inventory**、**show environment**。 未修改任何菜单项。
支持 IPS SSP-10、-20、-40 和 -60	对于 ASA 5585-X，引入了 IPS SSP-10、-20、-40 和 -60 支持。只能安装具有匹配 SSP 级别的 IPS SSP，例如 SSP-10 和 IPS SSP-10。 同样适用于版本 *8.2.(5)*。
CSC SSM 功能	
CSC SSM 支持	对于 CSC SSM，添加了对以下功能的支持： • HTTPS 流量重定向：用于传入 HTTPS 连接的 URL 过滤和 WRS 查询。 • 为传入和传出 SMTP 和 POP3 邮件配置全局批准的白名单。 • 产品许可证续订的邮件通知。 未修改任何命令。 修改了以下菜单项： **配置 > Trend Micro 内容安全 > 邮件 > SMTP** **配置 > Trend Micro 内容安全 > 邮件 > POP3** **配置 > Trend Micro 内容安全 > 主机/通知设置** **配置 > Trend Micro 内容安全 > CSC 安装 > 主机配置**
监控功能	

功能	说明
Smart Call-Home Anonymous Reporting	客户现在可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 引入了以下命令：**call-home reporting anonymous**、**call-home test reporting anonymous**。 修改了以下菜单项：**配置 > 设备监控 > Smart Call-Home**。 同样适用于版本 *8.2.(5)*。
IF-MIB ifAlias OID 支持	ASA 现在支持 ifAlias OID。浏览 IF-MIB 时，ifAlias OID 将设置为已为接口说明设置的值。 同样适用于版本 *8.2.(5)*。
接口功能	
在千兆以太网接口上支持暂停帧以进行流量控制	现在，您可以在千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制；以前在 8.2(2) 中已对 10 千兆以太网接口添加该支持。 修改了以下命令：**flowcontrol**。 修改了以下菜单项： （单情景模式）**配置 > 设备设置 > 接口 > 添加/编辑接口 > 通用** （多情景模式、系统）**配置 > 接口 > 添加/编辑接口** 同样适用于版本 *8.2.(5)*。
管理功能	
提高了 SSH 安全性；不再支持 SSH 默认用户名	从 8.4(2) 开始，您无法再使用 **pix** 或 **asa** 用户名和登录密码通过 SSH 连接至 ASA。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或“配置 \> 设备管理 \> 用户/AAA \> AAA 访问 \> 身份验证 (ASDM)”来配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或依次选择“配置 \> 设备管理 \> 用户/AAA \> 用户帐户 (ASDM)”来定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。

功能	说明
统一通信功能	
ASA-Tandberg 与 H.323 检测的互操作性	H.323 检测现在对于双向视频会话支持单向信令。此增强功能允许对 Tandberg 视频电话支持的单向视频会议执行 H.323 检测。支持单向信令使 Tandberg 电话能够切换视频模式（关闭其 H.263 视频会话的一端，并使用 H.264（高清视频的压缩标准）重新打开会话）。 未修改任何命令。 未修改任何菜单项。 同样适用于版本 *8.2.(5)*。
路由功能	
使用备份静态路由的连接超时	当多个静态路由以不同的指标共存于一个网络时，ASA 将使用创建连接时指标最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。要利用此功能，请将超时更改为新值。 修改了以下命令：**timeout floating-conn**。 修改了以下菜单项：**配置 > 防火墙 > 高级 > 全局超时**。 同样适用于版本 *8.2.(5)*。
ASDM 功能	

功能	说明
迁移网络对象组成员	如果迁移到 8.3 或更高版本，ASA 会创建命名网络对象来替换某些功能中的内联 IP 地址。除命名对象以外，ASDM 还会为配置中使用的任何 IP 地址自动创建非命名对象。这些自动创建的对象仅通过 IP 地址进行识别，不具有名称，并且在平台配置中不是作为命名对象存在。 当 ASA 在迁移过程中创建命名对象时，匹配的非命名纯 ASDM 对象会替换为命名对象。唯一的例外是网络对象组中的非命名对象。当 ASA 为网络对象组中包含的 IP 地址创建命名对象时，ASDM 还会保留非命名对象，从而在 ASDM 中创建重复对象。若要合并这些对象，请选择**工具 > 迁移网络对象组成员**。 引入了以下菜单项：**工具 > 迁移网络对象组成员**。 有关详细信息，请参阅《思科 *ASA 5500* 到 *8.3* 版本及更高版本的迁移》。

ASA 8.4(1.11)/ASDM 6.4(2) 的新功能

发布日期：**2011** 年 **5** 月 **20** 日

注释 我们建议您仅在 Cisco.com 发布的临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。我们会在发布下一个维护或功能版本时记录临时版本的功能。 有关每个临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

功能	说明
防火墙功能	

功能	说明
PAT 池和轮询地址分配	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程更轻松。 注释 当前在 8.4(1.11) 中，不可将 PAT 池功能用作动态 NAT 或 PAT 的回退方法。只能将 PAT 池配置为动态 PAT 的主要方法 (CSCtq20634)。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（对象网络）和 **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]（全局）。 修改了以下菜单项： **配置 > 防火墙 > NAT 规则 > 添加/编辑网络对象** **配置 > 防火墙 > NAT 规则 > 添加/编辑 NAT 规则**

ASA 8.4(1)/ASDM 6.4(1) 的新功能

发布日期：**2011** 年 **1** 月 **31** 日

功能	说明
硬件功能	
支持 ASA 5585-X	引入了对使用安全服务处理器 (SSP)-10、-20、-40 和 -60 的 ASA 5585-X 的支持。 注释 以前在 8.2(3) 和 8.2(4) 中添加了该支持；8.3(x) 中不支持 ASA 5585-X。

功能	说明
用于出口的无负载加密硬件	您可以购买无负载加密的 ASA 5585-X。如要出口至某些国家/地区，则在思科 ASA 5500 系列上不能启用负载加密。ASA 软件可感知无负载加密型号，并会禁用以下功能： • 统一通信 • VPN 您仍然可以安装强加密 (3DES/AES) 许可证，以便用于管理连接。例如，可以使用 ASDM HTTPS/SSL、SSHv2、Telnet 和 SNMPv3。您还可以为僵尸网络流量过滤器下载动态数据库（使用 SSL）。
远程访问功能	
Android 平台上的 L2TP/IPSec 支持	现在使用 L2TP/IPSec 协议和本机 Android VPN 客户端时，在 Android 移动设备和 ASA 5500 系列设备之间支持 VPN 连接。移动设备必须使用 Android 2.1 或更高版本的操作系统。 同样适用于版本 *8.2.(5)*。
UTF-8 字符对 AnyConnect 密码的支持	与 ASA 8.4(1) 配合使用的 AnyConnect 3.0 在使用 RADIUS/MSCHAP 和 LDAP 协议发送的密码中支持 UTF-8 字符。

功能	说明
使用 IKEv2 进行 IPSec VPN 连接	互联网密钥交换版本 2 (IKEv2) 是用于建立和控制互联网协议安全 (IPSec) 隧道的最新密钥交换协议。现在，ASA 对用于所有客户端操作系统的 AnyConnect 安全移动客户端版本 3.0(1) 均支持使用 IKEv2 的 IPSec 隧道。 在 ASA 上，您可以在组策略中为用户启用 IPSec 连接。对于 AnyConnect 客户端，可以为客户端配置文件服务器列表中的每个 ASA 指定主协议（IPSec 或 SSL）。 向 AnyConnect 基础版和 AnyConnect 高级版许可证中添加了使用 IKEv2 的 IPSec 远程访问 VPN。 站点到站点会话添加到了 Other VPN 许可证（之前的 IPSec VPN）。其他 VPN 许可证包含在基础许可证中。 修改了以下命令：**vpn-tunnel-protocol**、**crypto ikev2 policy**、**crypto ikev2 enable**、**crypto ipsec ikev2**、**crypto dynamic-map** 和 **crypto map**。 修改了以下菜单项： **配置 > 站点到站点 VPN > 连接配置文件** **配置 > 远程访问 > 网络（客户端）访问 > AnyConnect 连接配置文件** **网络（客户端）访问 > 高级 > IPSec > IKE 参数 > IKE 策略** **网络（客户端）访问 > 高级 > IPSec > IKE 参数 > IKE 参数** **网络（客户端）访问 > 高级 > IPSec > IKE 参数 > IKE 建议**

功能	说明
SSL SHA-2 数字签名	此版本支持使用符合 SHA-2 规范的签名算法对使用数字证书的 SSL VPN 连接进行身份验证。针对 SHA-2 的支持包括所有三种散列大小：SHA-256、SHA-384 和 SHA-512。SHA-2 需要 AnyConnect 2.5.1 或更高版本（建议为 2.5.2 或更高版本）。此版本不支持对其他用途或产品使用 SHA-2。此功能不涉及配置更改。 **注意**：要支持 SHA-2 连接的故障切换，备用 ASA 必须运行相同的映像。为了支持此功能，我们在 **show crypto ca certificate command** 命令中添加了“签名算法”字段以标识生成签名时使用的摘要式算法。
SCEP 代理	SCEP 代理为 AnyConnect 安全移动客户端提供自动第三方证书注册支持。使用此功能，不必接触 AnyConnect 即可安全地部署设备证书来授权终端连接、实施阻止非企业资产访问的策略，以及跟踪企业资产。此功能需要 AnyConnect 高级版许可证，不能使用基础版许可证。 引入或修改了以下命令：**crypto ikev2 enable**、**scep-enrollment enable**、**scep-forwarding-url**、**debug crypto ca scep-proxy**、**secondary-username-from-certificate**、**secondary-pre-fill-username**。
Host Scan 软件包支持	此功能为 ASA 安装或升级 Host Scan 软件包及启用或禁用 Host Scan 提供必要的支持。此软件包可以是独立的 Host Scan 软件包，也可以是 ASA 从 AnyConnect 下一代软件包中提取的 Host Scan 软件包。 在以前的 AnyConnect 版本中，终端的安全评估由思科安全桌面 (CSD) 决定。Host Scan 是 CSD 中捆绑的众多功能之一。从 CSD 中拆分出 Host Scan，使 AnyConnect 管理员可以独立于 CSD 的其他功能，更加自由地更新和安装 Host Scan。 引入了以下命令：**csd hostscan image path**。

功能	说明
Kerberos 约束委派 (KCD)	此版本在 ASA 上实施 KCD 协议转换和约束委派扩展。KCD 使无客户端 SSL VPN（也称为 WebVPN）用户能够通过 SSO 访问受 Kerberos 保护的任何 Web 服务。这类服务或应用的示例包括 Outlook Web Access (OWA)、Sharepoint 和互联网信息服务器 (IIS)。 实施协议转换允许 ASA 代表远程访问用户获取 Kerberos 服务票证，而无需他们对 KDC 进行身份验证（通过 Kerberos）。相反，用户会使用任何支持的身份验证机制（包括数字证书和智能卡）对无客户端 SSL VPN（也称为 WebVPN）的 ASA 进行身份验证。当用户验证完成时，ASA 会请求和获取模拟票证，即 ASA 代表用户获取的 ASA 服务票证。然后，ASA 可以使用模拟票证为远程访问用户获取其他服务票证。 约束委派为域管理员提供了一种限制允许委派的服务（例如 ASA）可访问的网络资源的方法。通过将允许委派的服务的运行帐户配置为特定计算机上运行的某个服务的特定实例，可完成此任务。 修改了以下命令：**kcd-server**、**clear aaa**、**show aaa** 和 **test aaa-server authentication**。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > Microsoft KCD 服务器**。
无客户端 SSL VPN 浏览器支持	现在，ASA 支持使用 Apple Safari 5 的无客户端 SSL VPN。

功能	说明
无客户端 VPN 自动登录增强	现在，智能隧道在 Firefox 及 Internet Explorer 上支持基于 HTTP 进行自动登录。与使用 Internet Explorer 浏览器时类似，管理员决定 Firefox 浏览器自动向哪些主机发送凭证。对于某些身份验证方法，如果需要，管理员可在 ASA 上指定与 Web 应用匹配的领域字符串（在“添加智能隧道自动登录服务器”窗口中）。现在，您也可以使用带宏替换功能的书签通过智能隧道自动登录。 POST 插件现已过时。之前创建 POST 插件是为了使管理员可以指定带登录宏的书签和接收发布 POST 请求之前要加载的启动页面。POST 插件方法允许提前获取的要求存在 cookie 和其他报头项目的请求通过。现在，管理员可以在创建书签时指定预加载页，从而实现相同的功能。与 POST 插件相同，管理员指定预加载页 URL 和要将 POST 请求发送到的 URL。 现在，您可以将默认的预配置 SSL VPN 门户替换为自己的门户。管理员可通过将 URL 指定为外部门户来完成此任务。与组策略主页不同，外部门户支持带宏替换功能（用于自动登录）的 POST 请求以及预加载页。 引入或修改了以下命令：**smart-tunnel auto-signon**。 引入或修改了以下菜单项： **配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 自定义**。 **配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签 > 编辑 > 编辑书签**
扩展的智能隧道应用支持	智能隧道添加了对以下应用的支持： • Microsoft Outlook Exchange Server 2010（本机支持）。 现在，用户可以使用智能隧道将 Microsoft Office Outlook 连接到 Microsoft Exchange 服务器。 • Microsoft Sharepoint/Office 2010。 现在，用户可以通过智能隧道使用 Microsoft Office 2010 应用和 Microsoft Sharepoint 来执行远程文件编辑。

功能	说明
接口功能	
EtherChannel 支持（ASA 5510 及更高版本）	您可以为八个主用接口各配置多达 48 个 802.3ad EtherChannel。 注释 您无法将 4GE SSM（包括 ASA 5550 上插槽 1 中集成的 4GE SSM）上的接口用作 EtherChannel 的一部分。 引入了以下命令：**channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel**。 引入或修改了以下菜单项： **配置 > 设备设置 > 接口** **配置 > 设备设置 > 接口 > 添加/编辑 EtherChannel 接口** **配置 > 设备设置 > 接口 > 添加/编辑接口** **配置 > 设备设置 > EtherChannel**
透明模式的网桥组	如果您不希望产生安全情景开销，或者希望最大限度地利用安全情景，则可以将接口一起集合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量相互分隔。在单情景模式和多情景模式的每个情景中，最多可配置 8 个网桥组，每组最多 4 个接口。 注释 尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。 引入了以下命令：**interface bvi**、**bridge-group** 和 **show bridge-group**。 修改或引入了以下菜单项： 配置 > 设备设置 > 接口 配置 > 设备设置 > 接口 > 添加/编辑网桥组接口配置 > 设备设置 > 接口 > 添加/编辑接口
可扩展性功能	

功能	说明
增加了 ASA 5550、5580 和 5585-X 的情景数	对于带 SSP-10 的 ASA 5550 和 ASA 5585-X，最大情景数从 50 增加到 100。对于带 SSP-20 和更高版本的 ASA 5580 和 5585-X，最大数量从 50 增加到 250。
增加了 ASA 5580 和 5585-X 的 VLAN 数量	对于 ASA 5580 和 5585-X，最大 VLAN 数量从 250 增加到 1024。
其他平台支持	Google Chrome 被添加为 ASA 版本 8.4 的支持平台。Windows XP、Vista 和 7 以及 Mac OS X 版本 6.0 均支持 32 位和 64 位平台。
增加了 ASA 5580 和 5585-X 的连接数	提高了防火墙连接限制： • ASA 5580-20 - 1,000,000 至 2,000,000。 • ASA 5580-40 - 2,000,000 至 4,000,000。 • 带 SSP-10 的 ASA 5585-X：750,000 至 1,000,000。 • 带 SSP-20 的 ASA 5585-X：1,000,000 至 2,000,000。 • 带 SSP-40 的 ASA 5585-X：2,000,000 至 4,000,000。 • 带 SSP-60 的 ASA 5585-X：2,000,000 至 10,000,000。
增加了 ASA 5580 的 AnyConnect VPN 会话数	AnyConnect VPN 会话限制从 5,000 增加到 10,000。
增加了 ASA 5580 的其他 VPN 会话数	其他 VPN 会话限制从 5,000 增加到 10,000。
高可用性功能	

功能	说明
使用动态路由协议执行状态故障切换	现在，在备用设备的路由信息库 (RIB) 表中维护主用设备上通过动态路由协议获取的路由（例如 OSPF 和 EIGRP）。现在，发生故障切换事件时，辅助主用设备上的流量会通过，并尽可能地减少中断，因为路由是已知的。路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。 修改了以下命令：**show failover**、**show route**、**show route failover**。 未修改任何菜单项。
统一通信功能	
统一通信向导中添加了电话代理	统一通信向导可指导您完成配置过程，并自动配置电话代理所需的设置。该向导可自动创建必要的 TLS 代理，然后指导您创建电话代理实例、导入和安装所需的证书，最后自动为电话代理流量启用 SIP 和 SCCP 检测。 修改了以下菜单项： **向导 > 统一通信向导**。 **配置 > 防火墙 > 统一通信**。
UC 协议检测增强	增强了 SIP 检测和 SCCP 检测，以支持统一通信解决方案中的新功能；例如 SCCP v2.0 支持、SCCP 检测中对 GETPORT 消息的支持、使用 SIP 检测的 INVITE 消息中对 SDP 字段的支持，以及基于 SIP 执行 QSIG 隧道传输。此外，思科公司间媒体引擎还支持思科 RT Lite 电话和第三方视频终端（例如 Tandberg）。 未修改任何命令。 未修改任何菜单项。
检测功能	
增强 DCERPC	增强了 DCERPC 检测功能，以支持对 RemoteCreateInstance RPC 消息执行检测。 未修改任何命令。 未修改任何菜单项。
故障排除和监控功能	

功能	说明
SNMP 陷阱和 MIB	支持以下附加关键字：**connection-limit-reached**、**entity cpu-temperature**、**cpu threshold rising**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart**。 entPhysicalTable 报告传感器、风扇、电源和相关组件的条目。 支持以下附加 MIB：ENTITY-SENSOR-MIB、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、NAT-MIB、EVENT-MIB、EXPRESSION-MIB 支持以下附加陷阱：warmstart、cpmCPURisingThreshold、mteTriggerFired、cirResourceLimitReached、natPacketDiscard、ciscoEntSensorExtThresholdNotification。 引入或修改了以下命令：**snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps**。 修改了以下菜单项：**配置 > 设备管理 > 管理访问 > SNMP**。
TCP Ping 增强	TCP Ping 允许其 ICMP 回应请求被阻止的用户通过 TCP 检查连接状况。使用 TCP Ping 增强功能，您可以指定源 IP 地址和端口以及源接口，以便将 ping 发送到主机名或 IPv4 地址。 修改了以下命令：**ping tcp**。 修改了以下菜单项：**工具 > Ping**。

功能	说明
显示排名靠前的 CPU 进程	现在，您可以监控CPU上运行的进程，以获取任何指定进程使用的 CPU 百分比的相关信息。另外，您还可以查看有关日志时间前 5 分钟、1 分钟和5秒钟按进程细分的CPU负载信息。信息每 5 秒钟自动更新一次以提供实时统计信息；使用窗格中的刷新按钮可随时手动刷新数据。 引入了以下命令：**show process cpu-usage sorted** 引入了以下菜单项：**监控 > 属性 > CPU - 按进程**。
通用功能	
密码加密可见性	您可以在安全情景中显示密码加密。 修改了以下命令：**show password encryption**。 未修改任何菜单项。
ASDM 功能	
ASDM 升级增强	如果加载 ASDM 的设备使用的是不兼容的 ASA 软件版本，系统会显示一个对话框，通知用户可以从以下选项中选择： • 从 Cisco.com 升级映像版本。 • 从其本地驱动器升级映像版本。 • 继续使用不兼容的 ASDM/ASA 对（新选项）。 未修改任何菜单项。 此功能与所有 ASA 版本互操作。
在向导中实时 IKEv2	AnyConnect VPN 向导（前称为 SSL VPN 向导）、无客户端 SSL VPN 向导和站点到站点 IPSec VPN 向导（前称为 IPSec VPN 向导）中已实施了 IKEv2 支持，以遵守联邦和公共部门律令中规定的 IPSec 远程访问要求。随着安全性增强，新的支持还提供相同的最终用户体验，而不受 AnyConnect 客户端会话使用的隧道协议影响。IKEv2 还允许其他供应商的 VPN 客户端连接到 ASA。 修改了以下向导：站点到站点 IPSec VPN 向导、AnyConnect VPN 向导和无客户端 SSL VPN 向导。

功能	说明
“IPS 启动向导”增强	对于 ASA 5585-X 中的 IPS SSP，启动向导中添加了“IPS 基本配置”菜单项。“自动更新”菜单项中也添加了适用于 IPS SSP 的签名更新。添加了“时区和时钟配置”菜单项，以确保 ASA 上设置了时钟；IPS SSP 可从 ASA 获取其时钟。 引入或修改了以下菜单项：向导 > 启动向导 > IPS 基本配置向导 > 启动向导 > 自动更新向导 > 启动向导 > 时区和时钟配置

版本 8.3 的新功能

ASA 8.3(2.25)/ASDM 6.4(5.106) 的新功能

发布日期：2011 年 8 月 31 日

注释 我们建议您仅在 Cisco.com 发布的 ASA 临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们通常会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。

我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个ASA临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

功能	说明
远程访问功能	
无客户端 SSL VPN 浏览器支持	ASA 现在支持使用 Microsoft Internet Explorer 9 和 Firefox 4 的无客户端 SSL VPN。 同样适用于版本 *8.2(5.13)* 和 *8.4.2(8)*。

功能	说明
DTLS 和 TLS 压缩	为了提高吞吐量，思科现在在 AnyConnect 3.0 或更高版本上支持 DTLS 和 TLS 压缩。每种隧道传输方法会单独配置压缩，而首选配置是将 SSL 和 DTLS 都配置为 LZS。此功能增强了从旧版 VPN 客户端的迁移操作。 注释 在传输高度压缩数据的高速远程接入连接上使用数据压缩，要求 ASA 具备强大的处理能力。对于 ASA 上的其他活动和流量，平台上可支持的会话数量会下降。 引入或修改了以下命令：**anyconnect dtls compression** [**lzs** | **none**] 和 **anyconnect ssl compression** [**deflate** | **lzs** | **none**]。 修改了以下菜单项：**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 组策略 > 编辑 > 编辑内部组策略 > 高级 > AnyConnect 客户端 > SSL 压缩**。 同样适用于版本 *8.2(5.13)* 和 *8.4.2(8)*。
故障排除功能	
show asp table classifier 和 **show asp table filter** 命令的正则表达式匹配	现在，您可以使用正则表达式输入 **show asp table classifier** 和 **show asp table filter** 命令来过滤输出。 修改了以下命令：**show asp table classifier match** *regex*、**show asp table filter match** *regex*。 ASDM 不支持该命令，请使用命令行工具输入该命令。 同样适用于版本 *8.2(5.13)* 和 *8.4.2(8)*。

ASA 8.3(2)/ASDM 6.3(2) 的新功能

发布日期：**2010** 年 **8** 月 **2** 日

功能	说明
监控功能	

功能	说明
增强型日志记录和连接阻止	当您将系统日志服务器配置为使用TCP且系统日志服务器不可用时，ASA将阻止生成系统日志消息的新连接，直到该服务器重新变为可用状态（例如VPN、防火墙和直接转发代理连接）。此外，此功能已增强，也能在 ASA 上的日志记录队列已满时阻止新连接；连接将在日志记录队列被清除后恢复。 为符合通用标准 EAL4+ 而添加了此功能。除非专门要求，否则在系统日志消息无法发送时，建议允许新的连接。要允许新连接，请将系统日志服务器配置为使用 UDP 或使用 **logging permit-hostdown** 命令勾选“配置”>“设备管理”>“日志记录”>“系统日志服务器”窗格中的 **Allow user traffic to pass when TCP syslog server is down** 复选框。 修改了以下命令：**show logging**。 引入了以下系统日志消息：414005、414006、414007 和 414008 未修改任何 ASDM 菜单项。
系统日志消息过滤和排序	已为下列各项添加了支持： • 根据与各列对应的多个文本字符串过滤系统日志消息 • 创建自定义过滤器 • 对消息进行列排序。有关详细信息，请参阅 ASDM 配置指南。 修改了以下菜单项： **监控 > 日志记录 > 实时日志查看器 > 查看** **Monitoring > Logging > Log Buffer Viewer > View** 此功能与所有 *ASA* 版本互操作。
清除 CSC SSM 的系统日志消息	“最近的CSC安全事件”窗格中添加了对清除系统日志消息的支持。 修改了以下菜单项：**主页 > 内容安全**。 此功能与所有 *ASA* 版本互操作。
远程访问功能	

功能	说明
2048 位 RSA 证书和 Diffie-Hellman 组 5 (DH5) 性能改进	（仅限 ASA 5510、ASA 5520、ASA 5540 和 ASA 5550）对于 2048 位证书和 DH5 密钥等大型模数操作，我们强烈建议您启用硬件处理，而不是软件处理。如果您对于大型密钥继续使用软件处理，可能会由于 IPSec 和 SSL VPN 连接的会话建立缓慢而使性能大幅下降。我们建议您在使用量少或维护期间的最初启用硬件处理，以最大限度地降低从软件处理过渡到硬件处理时可能发生的临时丢包情况。 **注释** 对于使用 SSL VPN 的 ASA 5540 和 ASA 5550，在特定情况下可能要对大型密钥继续使用软件处理。如果添加 VPN 会话的速度非常慢，而且ASA满载运行，则对数据吞吐量造成的负面影响会大于建立会话的积极影响。 引入或修改了以下命令：**crypto engine large-mod-accel**、**clear configure crypto engine**、**show running-config crypto engine** 和 **show running-config crypto**。 在 ASDM 中，使用命令行界面工具输入 **crypto engine large-mod-accel** 命令。 同样适用于版本 *8.2(3)*。
Microsoft Internet Explorer 代理锁定控制	启用此功能将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡。禁用此功能将保持“连接”选项卡的显示不变；根据用户注册表设置，可以显示或隐藏该选项卡。 引入了以下命令：**msie-proxy lockdown**。 在ASDM中，使用命令行界面工具输入此命令。 同样适用于版本 *8.2.(3)*。

功能	说明
辅助密码增强功能	现在，您可以为所有身份验证配置对公用辅助密码的 SSL VPN 支持，或使用主密码作为辅助密码。 修改了以下命令：**secondary-pre-fill-username** [**use-primary-password** | **use-common-password**]] 修改了以下菜单项：**配置 > 远程接入 VPN > 无客户端 SSL 访问 > 连接配置文件 > 添加/编辑无客户端 SSL VPN 连接配置文件 > 高级 > 辅助身份验证**。
通用功能	

功能	说明

用于出口的无负载加密映像	如要出口至某些国家/地区，则在思科 ASA 5500 系列上不能启用负载加密。对于版本 8.3(2)，您现在可以在以下型号上安装无负载加密映像 (asa832-npe-k8.bin)：
	• ASA 5505
	• ASA 5510
	• ASA 5520
	• ASA 5540
	• ASA 5550
	在无负载加密映像中禁用的功能包括：
	• 统一通信。
	• VPN 的强加密（DES 加密仍可用于 VPN）。
	• VPN 负载均衡（请注意，CLI GUI 仍然存在；但该功能将无法正常工作）。
	• 下载僵尸网络流量过滤器的动态数据库（静态黑名单和白名单仍受支持。请注意，CLI GUI 仍然存在；但是该功能将无法正常工作。
	• 需要强加密的管理协议，包括 SSL、SSHv2 和 SNMPv3。但是，您可以通过基本加密 (DES) 来使用 SSL 或 SNMPv3。此外，SSHv1 以及 SNMPv1 和 v2 仍然可用。
	如果尝试安装强加密 (3DES/AES) 许可证，则会看到以下警告：
	`WARNING: Strong encryption types have been disabled in this image;`
	`the VPN-3DES-AES license option has been ignored.`

ASA 8.3(1)/ASDM 6.3(1) 的新功能

发布日期：**2010** 年 **3** 月 **8** 日

功能	说明
远程访问功能	

功能	说明
智能隧道的相关增强	注销增强-现在，当所有浏览器窗口已关闭时（父关联），可以注销智能隧道，也可以右键点击系统任务栏中的通知图标并确认注销。 隧道策略 - 管理员可以决定哪些连接通过 VPN 网关，哪些连接不通过。如果管理员进行相应选择，最终用户可通过智能隧道直接浏览互联网，同时可访问公司内部资源。 对隧道应用的简化配置 - 当需要智能隧道时，用户不再需要配置可以访问智能隧道并转而访问特定网页的进程列表。书签或独立应用的“启用智能隧道”复选框可实现更加简便的配置过程。 组策略主页 - 现在，使用 ASDM 中的一个复选框，管理员便可在组策略中指定他们的主页，以便通过智能隧道进行连接。 引入了以下命令：**smart-tunnel network**、**smart-tunnel tunnel-policy**。 修改了以下菜单项：**配置 > 远程访问 VPN > AAA/本地用户 > 本地用户 > 编辑 > VPN 策略 > 无客户端 SSL VPN**。

功能	说明
对基于浏览器的 VPN 新支持的平台	版本 8.3(1) 提供从以下新支持的平台进行基于浏览器（无客户端）的 VPN 访问的功能： • Windows 7 x86（32 位）和 x64（64 位），通过 Internet Explorer 8.x 和 Firefox 3.x • Windows Vista x64，通过 Internet Explorer 7.x/8.x 或 Firefox 3.x。 • Windows XP x64，通过 Internet Explorer 6.x/7.x/8.x 和 Firefox 3.x • Mac OS 10.6.x 32 位 和 64 位，通过 Safari 4.x 和 Firefox 3.x。 Firefox 2.x 很可能会起作用，尽管我们不再测试它。 版本 8.3(1) 为 Mac OS 10.5 上的 64 位应用引入了基于浏览器的支持。 现在，版本 8.3(1) 在支持用于基于浏览器的 VPN 访问的所有 32 位和 64 位 Windows 操作系统、仅在英特尔处理器上运行的 Mac OS 10.5 以及 Mac OS 10.6.x 上支持进行智能隧道访问。ASA 在 64 位操作系统上不支持端口转发。 基于浏览器的 VPN 访问在 Windows 7、Vista 和 Internet Explorer 8 上不支持 Web 文件夹。 对于 64 位浏览器，无法使用 RDP 插件的 ActiveX 版本。 **注释** Windows 2000 和 Mac OS X 10.4 不再支持基于浏览器的访问。

功能	说明
对 IKEv1 局域网到局域网 VPN 连接的 IPv6 支持	

功能	说明
	对于使用混合 IPv4 和 IPv6 寻址或全 IPv6 寻址的局域网到局域网连接，如果对等方均为思科 ASA 5500 系列 ASA，并且双方的内部网络具有匹配的寻址方案（全部为 IPv4 或 IPv6），则 ASA 支持 VPN 隧道。 尤其是，两个对等方均为思科 ASA 5500 系列 ASA 时，支持以下拓扑： • ASA 具有 IPv4 内部网络，外部网络为 IPv6（内部接口使用 IPv4 地址，外部接口使用 IPv6 地址）。 • ASA 具有 IPv6 内部网络，外部网络为 IPv4（内部接口使用 IPv6 地址，外部接口使用 IPv4 地址）。 • ASA 具有 IPv6 内部网络，外部网络为 IPv6（内部接口和外部接口都使用 IPv6 地址）。 注释 缺陷 CSCtd38078 目前会阻止思科 ASA 5500 系列连接到思科 IOS 设备作为局域网到局域网连接的对等设备。 修改或引入了以下命令：**isakmp enable**、**crypto map**、**crypto dynamic-map**、**tunnel-group**、**ipv6-vpn-filter**、**vpn-sessiondb**、**show crypto isakmp sa**、**show crypto ipsec sa**、**show crypto debug-condition**、**show debug crypto**、**show vpn-sessiondb**、**debug crypto condition**、**debug menu ike**。 修改或引入了以下菜单项： **向导 > IPSec VPN 向导**， **配置 > 站点到站点 VPN > 连接配置文件配置 > 站点到站点 VPN > 连接配置文件 > 基本 > 添加 IPSec 站点到站点连接配置文件** **配置 > 站点到站点 VPN > 组策略** **配置 > 站点到站点 VPN > 组策略 > 编辑内部组策略** **配置 > 站点到站点 VPN > 高级 > 加密映射** **配置 > 站点到站点 VPN > 高级 > 加密映射 > 添加 > 创建 IPSec 规则**

功能	说明
	配置 > 站点到站点 VPN > 高级 > ACL 管理器
AnyConnect 配置文件编辑器的插件	AnyConnect 配置文件编辑器是一种基于 GUI 的便捷配置工具，您可以使用它来配置 AnyConnect 2.5 或更高版本的客户端配置文件（这是一个包含控制客户端功能的设置的 XML 文件）。以前，您只能通过编辑配置文件中的 XML 标记来手动更改配置文件设置。AnyConnect 配置文件编辑器是一个名为 anyconnectprof.sgz 的插件二进制文件，它使用 ASDM 映像打包，安装在 ASA 上闪存的 disk0:/ 根目录中。此设计使您可以更新编辑器，使其与新的客户端版本中提供的新 AnyConnect 功能兼容。
SSL VPN 门户自定义编辑器	您可以使用 ASDM 中新的“编辑自定义对象”窗口来更名和自定义展示给无客户端 SSL VPN 用户的屏幕。您可以自定义登录、门户和注销屏幕，包括公司徽标、文本消息和常规布局。以前，自定义功能嵌入在 ASA 软件映像中。将其移动到 ASDM 可为该功能及将来的增强提供更高的可用性。 修改了以下菜单项：配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 门户 > 自定义。
针对远程接入 VPN 的可用性改进	ASDM 提供一个逐步操作指南，用于配置无客户端 SSL VPN、AnyConnect SSL VPN 远程接入或使用 ASDM 助手的 IPSec 远程接入。ASDM 助手比 VPN 向导更全面，后者只是为了让您能够实现正常运行。 修改了以下菜单项：**配置 > 远程接入 VPN > 简介 > ASDM 助手**。
防火墙功能	
接口独立的访问策略	现在可以配置全局应用的访问规则，以及应用于某个接口的访问规则。如果配置同时指定了全局访问策略和特定于接口的访问策略，则将在全局策略之前评估特定于接口的策略。 修改了以下命令：**access-group global**。 修改了以下菜单项：**配置 > 防火墙 > 访问规则**。

功能	说明
网络和服务对象	现在，您可以创建用于在配置中代替主机、子网或一组IP地址的已命名网络对象，以及用于在配置中代替协议和端口的已命名服务对象。然后，您可以在一个位置更改对象定义，而不必更改配置的任何其他部分。此版本介绍了以下功能中对网络和服务对象的支持： • NAT • 访问列表规则 • 网络对象组 注释 ASDM在以前版本的内部使用网络对象；此功能为网络对象引入了平台支持。 引入或修改了以下命令：**object network**、**object service**、**show running-config object**、**clear configure object**、**access-list extended**、**object-group network**。 修改或引入了以下菜单项： **配置 > 防火墙 > 对象 > 网络对象/组**， **配置 > 防火墙 > 对象 > 服务对象/组** **配置 > 防火墙 > NAT 规则**，**配置 > 防火墙 > 访问规则**
对象组扩展规则缩减	显著减少了网络对象组扩展，同时保持了数据包分类性能的满意程度。 修改了以下命令：**show object-group**、**clear object-group**、**show access-list**。 修改了以下菜单项：**配置 > 防火墙 > 访问规则 > 高级**。

功能	说明
NAT 简单化	NAT 配置已完全重新设计，以实现更大的灵活性和易用性。现在，在您将 NAT 配置为网络对象属性的一部分的情况下，可以使用自动 NAT 配置 NAT，而在配置更高级 NAT 选项的情况下，可以使用手动 NAT 进行配置。 引入或修改了以下命令：**nat**（在全局和对象网络配置模式下）、**show nat**、**show nat pool**、**show xlate**、**show running-config nat**。 删除了以下命令：**global**、**static**、**nat-control**、**alias**。 修改或引入了以下菜单项： **配置 > 防火墙 > 对象 > 网络对象/组 配置 > 防火墙 > NAT 规则**
在访问列表中使用真实 IP 地址而不是转换的地址	使用 NAT 时，对于许多功能，访问列表中不再需要映射的地址。配置这些功能时，您始终应使用未转换的真实地址。使用真实地址意味着，如果 NAT 配置更改，则您无需更改访问列表。 使用访问列表的以下命令和功能现在使用真实 IP 地址。除非另行说明，否则这些功能将在升级到 8.3 时自动迁移为使用真实 IP 地址。 • **access-group command** 访问规则 • 模块化策略框架 **match access-list** 命令服务策略规则 • 僵尸网络流量过滤器 **dynamic-filter enable classify-list** 命令 • AAA **aaa ... match** 命令规则 • WCCP **wccp redirect-list group-list** 命令重定向。 **注释** 升级到 8.3 时，WCCP 不会自动迁移。

功能	说明
威胁检测增强	现在，您可以自定义为其收集高级统计信息的速率间隔数。默认速率数已从 3 更改为 1。对于基本统计信息、高级统计信息和扫描威胁检测，内存使用率得到了提高。 修改了以下命令：**threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates**、**show threat-detection memory**。 修改了以下菜单项：**配置 > 防火墙 > 威胁检测**。
统一通信功能	
SCCP v19 支持	思科电话代理功能中的IP电话支持得到增强，以包括对支持的 IP 电话列表中的 SCCP 协议版本 19 的支持。
思科跨企业间媒体引擎代理	思科跨企业间媒体引擎 (UC-IME) 支持公司使用 VoIP 技术提供的高级功能按需通过互联网进行互联。通过利用 P2P、安全和 SIP 协议在不同企业之间创建动态 SIP 中继，思科公司间媒体引擎可在不同企业的思科Unified Communication Manager集群之间实现企业到企业联盟。许多企业彼此协作，就像一个大型企业一样运作 修改或引入了以下命令：**uc-ime**、**fallback hold-down**、**fallback monitoring**、**fallback sensitivity-file**、**mapping-service listening-interface**、**media-termination**、**ticket epoch**、**ucm address**、**clear configure uc-ime**、**debug uc-ime**、**show running-config uc-ime**、**inspect sip**。 修改或引入了以下菜单项： **向导 > 统一通信向导 > 思科企业间媒体引擎代理配置 > 防火墙 > 统一通信**，然后点击 **UC-IME 代理配置 > 防火墙 > 服务策略规则 > 添加/编辑服务策略规则 > 规则行为 > 选择 SIP 检测映射**

功能	说明
对 IME 的 SIP 检测支持	SIP 检测已得到加强，以支持新的思科跨企业间媒体引擎 (UC IME) 代理。 修改了以下命令：**inspect sip**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略规则 > 添加/编辑服务策略规则 > 规则行为 > 选择 SIP 检测映射**。
统一通信向导	统一通信向导将指导您完成整个配置，并为以下代理自动配置所需的方面：思科 Mobility Advantage Proxy、思科 Presence Federation Proxy、思科跨企业间媒体引擎代理。此外，统一通信向导还自动配置代理的其他必需方面。 修改或引入了以下菜单项： **向导 > 统一通信向导** **配置 > 防火墙 > 统一通信**
增强的统一通信功能导航	统一通信代理功能（如电话代理、TLS代理、CTL文件和CTL提供程序页）从左侧“导航”面板的“对象”类别下移动到了新的统一通信类别。此外，该新类别还包含新的统一通信向导和UC IME代理页面。 此功能与所有 *ASA* 版本互操作。
路由功能	
路由映射支持	ASDM 为静态和动态路由添加了增强的支持。 修改了以下菜单项：**配置 > 设备安装 > 路由 > 路由映射**。 此功能与所有 *ASA* 版本互操作。
监控功能	
访问列表命中次数的时间戳	显示指定访问列表的时间戳，以及哈希值和命中次数。 修改了以下命令：**show access-list**。 修改了以下菜单项：**配置 > 防火墙 > 访问规则**。（当您将鼠标悬停在“命中”列中的单元格上时，会显示时间戳。）

功能	说明
对 ASDM 的高性能监控	现在，您可以为 ASDM 启用高性能监控，以显示通过 ASA 连接的前 200 个主机。主机的每个条目都包含主机的 IP 地址和由主机启动的连接数，并且每 120 秒进行更新。 引入了以下命令：**hpm topn enable**、**clear configure hpm**、**show running-config hpm**。 引入了以下菜单项：**主页 > 防火墙控制面板 > 前 200 个主机**。
许可功能	
不相同的故障切换许可证	不再要求每个设备上的故障切换许可证相同。来自主设备和辅助设备的合并许可证是同时用于这两种设备的许可证。 **注释** 对于 ASA 5505 和 5510 ASA，两种设备都需要增强型安全许可证；基本许可证不支持故障切换，因此您无法对仅具有基本许可证的备用设备启用故障切换。 修改了以下命令：**show activation-key** 和 **show version**。 修改了以下菜单项：**配置 > 设备管理 > 许可 > 激活密钥**。
可堆叠的基于时间的许可证	基于时间的许可证现在可以堆叠。在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，许可证没有到期尤为重要。ASA 使您可以堆叠基于时间的许可证，让您不必担心许可证过期或由于及早安装新的许可证而丢失许可证的时间。对于具有数字层的许可证，仅支持对具有相同容量的许可证（例如，两个 1000 个会话级的 SSL VPN 许可证）进行堆叠。您可以使用以下位置的 show activation-key 命令查看许可证的状态：**配置 > 设备管理 > 许可 > 激活密钥**。
公司间媒体引擎许可证	引入了 IME 许可证。
基于时间的许可证以正常运行时间为基础	现在，基于时间的许可证根据 ASA 的总正常运行时间进行倒计时；系统时钟不会影响许可证。

功能	说明
多个基于时间的许可证同时处于活动状态	您现在可以安装多个基于时间的许可证，每个功能一次只能有一个许可证处于活动状态。 修改了以下命令：**show activation-key** 和 **show version**。 修改了以下菜单项：**配置 > 设备管理 > 许可 > 激活密钥**。
基于时间的许可证的独立激活和停用。	您现在可以使用一个命令来激活或停用基于时间的许可证。 修改了以下命令：**activation-key** [**activate** | **deactivate**]。 修改了以下菜单项：**配置 > 设备管理 > 许可 > 激活密钥**。
通用功能	
主口令	主口令功能使您可以以加密格式安全地存储纯文本密码。它提供一个主密钥，用于在不更改任何功能的情况下对所有密码全面进行加密或屏蔽。备份/恢复功能支持主口令。 引入了以下命令：**key config-key password-encryption**、**password encryption aes**。 引入了以下菜单项： **配置 > 设备管理 > 高级 > 主口令** **配置 > 设备管理 > 设备管理 > 主口令**
ASDM 功能	
通过 Cisco.com 向导升级软件	Cisco.com 向导中的升级软件已更改，以便您可以使 ASDM 和 ASA 自动升级到更新的版本。请注意，此功能仅在单模式、多情景模式以及系统执行空间中可用。它在单个情景中不可用。 修改了以下菜单项：**工具 > 检查 ASA/ASDM 更新**。 此功能与所有 *ASA* 版本互操作。

功能	说明
备份/恢复增强	“备份配置”窗格经过重新排序和重新分组，以便您可以更轻松地选择要备份的文件。添加了一个“备份进度”窗格，以便您可以直观地衡量备份的进度。在使用备份或还原时，您将看到显著的性能改进。 修改了以下菜单项：**工具 > 备份配置**或**工具 > 恢复配置**。 此功能与所有 *ASA* 版本互操作。

版本 8.2 的新功能

ASA 8.2(5.13)/ASDM 6.4(4.106) 的新功能

发布日期：2011 年 9 月 18 日

注释 我们建议您仅在 Cisco.com 发布的 ASA 临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们通常会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。

我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个ASA临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的临时版本说明。

功能	说明
远程访问功能	
无客户端 SSL VPN 浏览器支持	ASA 现在支持使用 Microsoft Internet Explorer 9 和 Firefox 4 的无客户端 SSL VPN。 同样适用于版本 *8.3(2.25)* 和 *8.4.2(8)*。

功能	说明
DTLS 和 TLS 压缩	为了提高吞吐量，思科现在在 AnyConnect 3.0 或更高版本上支持 DTLS 和 TLS 压缩。每种隧道传输方法会单独配置压缩，而首选配置是将 SSL 和 DTLS 都配置为 LZS。此功能增强了从旧版 VPN 客户端的迁移操作。 注释 在传输高度压缩数据的高速远程访问连接上使用数据压缩，要求 ASA 具备强大的处理能力。对于 ASA 上的其他活动和流量，平台上可支持的会话数量会下降。 引入或修改了以下命令：**anyconnect dtls compression** [**lzs** | **none**] 和 **anyconnect ssl compression** [**deflate** | **lzs** | **none**]。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 组策略 > 编辑 > 编辑内部组策略 > 高级 > AnyConnect 客户端 > SSL 压缩**。 同样适用于版本 *8.3(2.25)* 和 *8.4.2(8)*。
故障排除功能	
show asp table classifier 和 **show asp table filter** 命令的正则表达式匹配	现在，您可以使用正则表达式输入 **show asp table classifier** 和 **show asp table filter** 命令来过滤输出。 修改了以下命令：**show asp table classifier match** *regex*、**show asp table filter match** *regex*。 ASDM不支持该命令，请使用命令行工具输入该命令。 同样适用于版本 *8.3(2.25)* 和 *8.4.2(8)*。

ASA 8.2(5)/ASDM 6.4(3) 的新功能

发布日期：**2011** 年 **5** 月 **23** 日

功能	说明
监控功能	

功能	说明
Smart Call-Home Anonymous Reporting	客户现在可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 引入了以下命令：**call-home reporting anonymous**、**call-home test reporting anonymous**。 修改了以下菜单项：**配置 > 设备监控 > Smart Call-Home**。 同样适用于版本 *8.4(2)*。
IF-MIB ifAlias OID 支持	ASA 现在支持 ifAlias OID。浏览 IF-MIB 时，ifAlias OID 将设置为已为接口说明设置的值。 同样适用于版本 *8.4(2)*。
远程访问功能	
门户访问规则	此增强功能让客户可以配置全局无客户端 SSL VPN 访问策略，以根据 HTTP 报头中的数据允许或拒绝无客户端 SSL VPN 会话。如果访问遭到拒绝，系统会向客户端返回错误代码。由于此拒绝操作是在用户身份验证之前发生的，所以可以减少处理资源的使用。 修改了以下命令：**portal-access-rule**。 修改了以下菜单项：**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 门户访问规则**。 同样适用于版本 *8.4(2)*。

功能	说明
移动状况 （以前称为适用于移动设备检测的 AnyConnect 标识扩展）	现在，您可以将 ASA 配置为允许或拒绝到移动设备的 VPN 连接、基于组启用或禁用移动设备访问以及根据移动设备的安全评估数据收集有关已连接的移动设备的信息。支持此功能的移动平台如下：iPhone/iPad/iPod 版 AnyConnect 2.5.x 和 Android 版 AnyConnect 2.4.x。无需启用 CSD 即可在 ASDM 中配置这些属性。 许可要求 实施远程访问控制和从移动设备收集安全评估数据要求在 ASA 上安装一个 AnyConnect Mobile 许可证和一个 AnyConnect 基础版或 AnyConnect 高级版许可证。您将根据安装的许可证收到以下功能： • **AnyConnect 高级版许可证功能** 安装 AnyConnect 高级版许可证的企业将能够根据 DAP 属性和任何其他现有终端属性，在受支持的移动设备上实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。 • **AnyConnect 基础版许可证功能** 安装 AnyConnect 基础版许可证的企业将能够执行以下任务： • 逐个组启用或禁用移动设备访问，以及使用 ASDM 配置该功能。 • 通过 CLI 或 ASDM 显示有关已连接移动设备的信息，这些移动设备并不具有实施 DAP 策略或者拒绝或允许对其进行远程访问的能力。 修改了以下菜单项：**配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加/编辑终端属性 > 终端属性类型：AnyConnect**。 同样适用于版本 *8.4(2)*。

功能	说明
AnyConnect 的拆分隧道策略	此版本包括一个推送到 AnyConnect 安全移动客户端的新策略，用于解析通过拆分隧道的 DNS 地址。此策略适用于使用 SSL 或 IPSec/IKEv2 协议的 VPN 连接，并指示 AnyConnect 客户端解析通过 VPN 隧道的所有 DNS 地址。如果 DNS 解析失败，则地址将保持未解析状态，而且 AnyConnect 客户端不会尝试通过公共 DNS 服务器解析地址。 默认情况下，此功能处于禁用状态。客户端根据拆分隧道策略通过隧道发送 DNS 查询，这些策略包括隧道化所有网络、隧道化网络列表中指定的网络，以及排除网络列表中指定的网络。 引入了以下命令：**split-tunnel-all-dns**。 修改了以下菜单项：**配置 > 远程放 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑组策略 > 高级 > 拆分隧道**（请参阅“通过隧道发送所有 DNS 查找”复选框）。 同样适用于版本 *8.4(2)*。
SSL SHA-2 数字签名	现在，您可以使用符合 SHA-2 规范的签名算法对使用数字证书的 SSL VPN 连接进行身份验证。针对 SHA-2 的支持包括所有三种散列大小：SHA-256、SHA-384 和 SHA-512。SHA-2 需要 AnyConnect 2.5(1) 或更高版本（建议为 2.5(2) 或更高版本）。此版本不支持对其他用途或产品使用 SHA-2。 注意：要支持 SHA-2 连接的故障切换，备用 ASA 必须运行相同的映像。 修改了以下命令：**show crypto ca certificate**（“签名算法”字段标识生成签名时使用的摘要式算法）。 未修改任何菜单项。 同样适用于版本 *8.4(2)*。

功能	说明
L2TP/IPSec 支持 Android	现在使我们用 L2TP/IPSec 协议和本机 Android VPN 客户端时，在 Android 移动设备和 ASA 5500 系列设备之间支持 VPN 连接。移动设备必须使用 Android 2.1 或更高版本的操作系统。 未修改任何命令。 未修改任何菜单项。 同样适用于版本 *8.4(1)*。
对于 Microsoft Windows 7 和 Android 本机 VPN 客户端支持 SHA2 证书签名	使用 L2TP/IPSec 协议时，ASA 对于 Microsoft Windows 7 和 Android 本机 VPN 客户端支持 SHA2 证书签名。 未修改任何命令。 未修改任何菜单项。 同样适用于版本 *8.4(2)*。
启用/禁用证书映射以覆盖“组 URL”属性	此功能在连接配置文件选择过程中会更改连接配置文件首选项。默认情况下，如果 ASA 将连接配置文件中指定的证书字段值与终端所用证书的字段值进行匹配，ASA 会将该配置文件分配到 VPN 连接。此可选功能会更改指定终端所请求的组 URL 的连接配置文件的首选项。通过该新选项，管理员可采用许多旧版 ASA 软件使用的组 URL 首选项。 引入了以下命令：**tunnel-group-preference** 修改了以下菜单项： **配置 > 远程访问 VPN > 无客户端 SSL VPN > 连接配置文件** **配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件** 同样适用于版本 *8.4(2)*。
接口功能	

功能	说明
在 1 千兆以太网接口上支持暂停帧以进行流量控制	现在，您可以在 1 千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制；以前在 8.2(2) 中已对 10 千兆以太网接口添加该支持。 修改了以下命令：**flowcontrol**。 修改了以下菜单项： （单情景模式）配置 > 设备安装 > 接口 > 添加/编辑界面 > 常规（多情景模式、系统）配置 > 接口 > 添加/编辑界面 同样适用于版本 *8.4(2)*。
统一通信功能	
ASA-Tandberg 与 H.323 检测的互操作性	H.323 检测现在对于双向视频会话支持单向信令。此增强功能允许对 Tandberg 视频电话支持的单向视频会议执行 H.323 检测。支持单向信令使 Tandberg 电话能够切换视频模式（关闭其 H.263 视频会话的一端，并使用 H.264 [高清视频的压缩标准] 重新打开会话）。 未修改任何命令。 未修改任何菜单项。 同样适用于版本 *8.4(2)*。
路由功能	
使用备份静态路由的连接超时	当多个静态路由以不同的指标共存于一个网络时，ASA 将使用创建连接时指标最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。要利用此功能，请将超时更改为新值。 修改了以下命令：**timeout floating-conn**。 修改了以下菜单项：**配置 > 防火墙 > 高级 > 全局超时**。 同样适用于版本 *8.4(2)*。

ASA 8.2(4.4)/ASDM 6.3(5) 的新功能

发布日期：2011 年 3 月 4 日

注释 我们建议您仅在 Cisco.com 发布的临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的*思科 ASA 临时版本说明*。

功能	说明
硬件功能	
对适用于 5585-X 的 ASA IPS SSP-10、-20、-40 和 -60 的支持	对于 ASA 5585-X，引入了 IPS SSP-10、-20、-40 和 -60 支持。只能安装具有匹配 SSP 级别的 IPS SSP，例如 SSP-10 和 IPS SSP-10。
远程访问功能	
对 Outlook Web Access 2010 的无客户端 SSL VPN 支持	默认情况下，无客户端 SSL VPN 现在提供对 Outlook Web Access (OWA) 2010 流量的内容转换（重写）支持。 未修改任何命令。 未修改任何菜单项。

ASA 8.2(4.1)/ASDM 6.3(5) 的新功能

发布日期：2011 年 1 月 18 日

注释 我们建议您仅在 Cisco.com 发布的临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的思科 *ASA* 临时版本说明。

功能	说明
远程访问功能	

功能	说明
SSL SHA-2 数字签名	此版本支持使用符合 SHA-2 规范的签名算法对使用数字证书的 SSL VPN 连接进行身份验证。针对 SHA-2 的支持包括所有三种散列大小：SHA-256、SHA-384 和 SHA-512。SHA-2 需要 AnyConnect 2.5.1 或更高版本（建议为 2.5.2 或更高版本）。此版本不支持对其他用途或产品使用 SHA-2。此功能不涉及配置更改。注意：要支持 SHA-2 连接的故障切换，备用 ASA 必须运行相同的映像。为了支持此功能，我们在 **show crypto ca certificate** 命令中添加了“签名算法”字段以标识生成签名时使用的摘要式算法。

ASA 8.2(4)/ASDM 6.3(5) 的新功能

发布日期：**2010** 年 **12** 月 **15** 日

功能	说明
硬件功能	
对于 SSP-10 和 SSP-40 支持思科 ASA 5585-X	引入了对配有安全服务处理器 (SSP)-10 和 (SSP)-40 的 ASA 5585 x 的支持。 注释　8.3(x) 版本不支持 ASA 5585-X。

ASA 8.2(3.9)/ASDM 6.3(4) 的新功能

发布日期：**2010** 年 **11** 月 **2** 日

注释　我们建议您仅在 Cisco.com 发布的临时版本可解决您的具体问题时，再升级到相关临时版本。如果您决定在生产环境下运行临时版本，请注意我们仅对临时版本执行了有针对性的测试。思科 TAC 完全支持临时版本，而且在下一个维护版本发布之前，它们会一直保留在下载站点中。如果您选择运行临时版本，我们强烈建议您在有完全测试的维护或功能版本可用时升级到相应版本。我们会在发布下一个维护或功能版本时记录临时版本的功能。有关每个临时版本的已解决警告列表，请参阅 Cisco.com 软件下载站点中提供的思科 *ASA* 临时版本说明。

功能	说明
远程访问功能	

功能	说明
SSL SHA-2 数字签名	此版本支持使用符合 SHA-2 规范的签名算法对使用数字证书的 SSL VPN 连接进行身份验证。针对 SHA-2 的支持包括所有三种散列大小：SHA-256、SHA-384 和 SHA-512。SHA-2 需要 AnyConnect 2.5.1 或更高版本（建议为 2.5.2 或更高版本）。此版本不支持对其他用途或产品使用 SHA-2。此功能不涉及配置更改。注意：要支持 SHA-2 连接的故障切换，备用 ASA 必须运行相同的映像。为了支持此功能，我们在 **show crypto ca certificate** 命令中添加了“签名算法”字段以标识生成签名时使用的摘要式算法。

ASA 8.2(3)/ASDM 6.3(3) 和 6.3(4) 的新功能

发布日期：**2010** 年 **8** 月 **9** 日

注释 ASDM 6.3(4) 不包括任何新功能；它只包括支持 ASA 5585-X 所需的警告修补程序。

功能	说明
硬件功能	
对于 SSP-20 和 SSP-60 支持思科 ASA 5585-X	引入了对配有安全服务处理器 (SSP)-20 和 (SSP)-60 的 ASA 5585 x 的支持。 注释 8.3(x) 版本不支持 ASA 5585-X。 ASA 5585-X 需要 ASDM 6.3(4)。
远程访问功能	

功能	说明
2048 位 RSA 证书和 Diffie-Hellman 组 5 (DH5) 性能改进	（仅限 ASA 5510、ASA 5520、ASA 5540 和 ASA 5550）对于 2048 位证书和 DH5 密钥等大型模数操作，我们强烈建议您启用硬件处理，而不是软件处理。如果您对于大型密钥继续使用软件处理，可能会由于 IPSec 和 SSL VPN 连接的会话建立缓慢而使性能大幅下降。我们建议您在使用量少或维护期间的最初启用硬件处理，以最大限度地降低从软件处理过渡到硬件处理时可能发生的临时丢包情况。 **注释** 对于使用 SSL VPN 的 ASA 5540 和 ASA 5550，在特定情况下可能要对大型密钥继续使用软件处理。如果添加 VPN 会话的速度非常慢，而且ASA满载运行，则对数据吞吐量造成的负面影响会大于建立会话的积极影响。 ASA 5580/5585-X 平台已经集成此功能；因此，crypto engine 命令不适用于这些平台。 引入或修改了以下命令：**crypto engine large-mod-accel**、**clear configure crypto engine**、**show running-config crypto engine** 和 **show running-config crypto**。 在 ASDM 中，使用命令行界面工具输入 **crypto engine large-mod-accel** 命令。 同样适用于版本 *8.3(2)*。
Microsoft Internet Explorer 代理锁定控制	启用此功能将会在 AnyConnect VPN 会话期间隐藏 Microsoft Internet Explorer 中的“连接”选项卡。禁用此功能将保持 Connections 选项卡的显示不变；根据用户注册表设置，可以显示或隐藏该选项卡。 引入了以下命令：**msie-proxy lockdown**。 在 ASDM 中，使用命令行界面工具输入此命令。
可信网络检测暂停和恢复	此功能使 AnyConnect 客户端可以保留其会话信息和 cookie，以便在用户离开办公室后能够无缝地恢复连接，只要会话不超过空闲计时器设置即可。此功能需要一个支持 TND 暂停和恢复的 AnyConnect 版本。

ASA 8.2(2)/ASDM 6.2(5) 的新功能

发布日期：**2010** 年 **1** 月 **11** 日

功能	说明
远程访问功能	
等待恢复 (Waiting-to-Resume) VPN 会话的可扩展解决方案	管理员现在可跟踪处于活动状态的用户数量，也可以查看统计信息。处于非活动状态时间最长的会话会被标记为空闲（并自动注销），以便不会达到许可证容量限制，而且新用户可以登录。 修改了以下菜单项：**监控 > VPN > VPN 统计信息 > 会话**。 同样适用于版本 *8.0(5)*。
应用检测功能	
检查 IP 选项	现在，您可以控制应允许通过 ASA 的具有特定 IP 选项的 IP 数据包。您还可以从 IP 数据包中清除 IP 选项，然后允许它通过 ASA。以前，除部分特殊情况外，所有 IP 选项默认都是被拒绝的。 **注释** 默认情况下，此选项处于启用状态。默认的全局服务策略中添加了以下命令：**inspect ip-options**。因此，当 ASA 处于路由模式中时，ASA 允许包含带有 Router Alert（路由器告警）选项（选项 20）的数据包的 RSVP 流量通过。 引入了以下命令：**policy-map type inspect ip-options**、**inspect ip-options**、**eool**、**nop**。 引入了以下菜单项： **配置 > 防火墙 > 对象 > 检查映射 > IP 选项** **配置 > 防火墙 > 服务策略 > 添加/编辑服务策略规则 > 规则操作 > 协议检查**

功能	说明
在 H.323 终端之间启用调用设置	如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。ASA 包括基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息打开呼叫针孔的选项。 由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。 引入了以下命令：**ras-rcf-pinholes enable**（在 **policy-maptype inspect h323 > parameters** 命令之下）。 修改了以下菜单项：**配置 > 防火墙 > 对象 > 检查映射 > H.323 > 详细信息 > 状态检查**。 同样适用于版本 *8.0(5)*。
统一通信功能	
移动代理应用不再需要统一通信代理许可证	移动代理不再需要 UC 代理许可证。
接口功能	
在多情景模式下，自动生成的 MAC 地址现在使用用户可配置的前缀以及其他增强功能	MAC 地址格式更改为允许使用前缀，以便使用固定起始值(A2)，并在故障切换对中为主设备和辅助设备 MAC 地址使用不同方案。 现在，MAC地址在重新加载之后也会保持不变。 现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配MAC地址，则手动MAC地址不能以 A2 开头。 修改了以下命令：**mac-address auto prefix** *prefix*。 修改了以下菜单项：**配置 > 情景管理 > 安全情景**。 同样适用于版本 *8.0(5)*。
对 ASA 5580 10 千兆以太网接口上流量控制的暂停帧支持	您现在可以为流量控制启用暂停 (XOFF) 帧。 引入了以下命令：**flowcontrol**。 修改了以下菜单项： （单情景模式）**配置 > 设备设置 > 接口 > 添加/编辑接口 > 通用** （多情景模式、系统）**配置 > 接口 > 添加/编辑接口**

功能	说明
防火墙功能	
僵尸网络流量过滤器增强功能	现在，僵尸网络流量过滤器支持根据威胁级别自动拦截被列入黑名单的流量。您还可以在统计信息和报告中查看恶意软件站点的类别和威胁级别。报告功能已增强为显示受感染的主机。删除了顶部主机报告的 1 小时超时；现在没有超时。 引入或修改了以下命令： **dynamic-filter ambiguous-is-black**、**dynamic-filter drop blacklist**、**show dynamic-filter statistics**、**show dynamic-filter reports infected-hosts**, 和 **show dynamic-filter reports top**。 引入或修改了以下菜单项： **配置 > 防火墙 > 僵尸网络流量过滤器 > 流量设置** **监控 > 僵尸网络流量过滤器 > 感染的主机**
适用于所有协议的连接超时	空闲超时已被更改为应用于所有协议，而不仅是 TCP 协议。 修改了以下命令：**set connection timeout**。 修改了以下菜单项：**配置 > 防火墙 > 服务策略 > 规则操作 > 连接设置**。
路由功能	
兼容 DHCP RFC（rfc3011、rfc3527）以解决路由问题	此增强功能对于 DHCP RFCs 3011（IPv4 子网选择选项）和 3527（中继代理信息选项的链路选择子选项）引入了 ASA 支持。对于为 VPN 客户端配置的每个 DHCP 服务器，现在可以将 ASA 配置为发送“子网选择”选项或“链接选择”选项。 修改了以下命令：**dhcp-server [subnet-selection | link-selection]**。 修改了以下菜单项：**远程访问 VPN > 网络访问 > IPSec 连接配置文件 > 添加/编辑**。 同样适用于版本 *8.0(5)*。
高可用性功能	

功能	说明
故障切换配置中支持 IPv6	IPv6现在在故障切换配置中受支持。您可以将主用和备用IPv6地址分配给接口，并为故障切换和有状态的故障切换接口使用 IPv6 地址。 修改了以下命令：**failover interface ip**、**ipv6 address**。 修改了以下菜单项： **配置 > 设备管理 > 高可用性 > 故障切换 > 设置** **配置 > 设备管理 > 高可用性 > 故障切换 > 接口** **配置 > 设备管理 > 高可用性 > HA/可扩展性向导**
在切换事件期间启用或关闭接口时不发送通知	要在故障切换期间区分从链路连接过渡到链路断开正常操作期间的链路连接/断开过渡，在故障切换期间不发送链路连接/断开陷阱。另外，在故障切换期间不会针对断链路连接/断开过渡发送系统日志消息。 同样适用于版本 *8.0(5)*。
AAA 功能	
100 个 AAA 服务器组	现在，可以配置多达 100 个 AAA 服务器组；而以前最多配置 15 个服务器组。 修改了以下命令： **aaa-server**。 修改了以下菜单项：**配置 > 设备管理 > 用户/AAA > AAA 服务器组**。
监控功能	
Smart Call Home	Smart Call Home 用于在 ASA 上提供主动诊断和实时警报，并提供更高的网络可用性和运行效率。如果检测到问题，客户和TAC工程师可以快速获得解决问题所需的东西。 **注释** Smart Call Home 服务器版本 3.0(1) 对 ASA 提供有限支持。有关详细信息，请参阅“重要通知”： 引入了以下命令：**call-home**、**call-home send alert-group**、**call-home test**、**call-home send**、**service call-home**、**show call-home**、**show call-home registered-module status**。 引入了以下菜单项：**配置 > 设备管理 > Smart Call Home**。

ASA 8.2(1)/ASDM 6.2(1) 的新功能

发布日期：2009 年 5 月 6 日

您好

功能	说明
远程访问功能	
对 ASDM 身份验证的一次性密码支持	ASDM 现在支持使用 RSA SecurID (SDI) 支持的一次性密码 (OTP) 进行管理员身份验证。此功能解决了有关使用静态密码进行管理员身份验证的安全顾虑。 ASDM用户的新会话控件包括限制会话时间和空闲时间的功能。如果ASDM管理员使用的密码超时，ASDM 会提示管理员重新进行身份验证。 引入了以下命令：**http server idle-timeout** 和 **http server session-timeout**。**http server idle-timeout** 的默认值为 20 分钟，最多可增加到 1440 分钟。 在 ASDM 中，请参阅**配置 > 设备管理 > 管理访问 > ASDM/HTTPD/Telnet/SSH**。
自定义安全桌面	您可以使用ASDM自定义显示给远程用户的安全桌面窗口，包括安全桌面背景（锁图标）及其文本颜色，以及针对“桌面”、“缓存清理器”、“按键记录器”和“关闭安全桌面”窗口的对话框横幅。 在 ASDM 中，请参阅**配置 > CSD 管理器 > 安全桌面管理器**。

功能	说明
从证书预填充用户名	预填充用户名功能允许使用从证书提取的用户名进行用户名/密码身份验证。启用此功能后，登录屏幕上的用户名为“已预填充”，且系统仅提示用户输入密码。要使用此功能，必须在隧道组配置模式下同时配置 **pre-fill username** 和 **username-from-certificate** 命令。 双重身份验证功能与预填充用户名功能兼容，因为需要两个用户名时，预填充用户名功能支持从证书中提取主用户名和辅助用户名作为双重身份验证的用户名。为双重身份验证配置预填充用户名功能时，管理员使用以下新的隧道组常规属性配置模式命令： • **secondary-pre-fill-username** - 支持提取用户名用于无客户端或 AnyConnect 客户端连接。 • **secondary-username-from-certificate** - 允许从证书中提取一些标准 DN 字段以用作用户名。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 或无客户端 SSL VPN 连接配置文件 > 高级**。设置位于“身份验证”、“辅助身份验证”和“授权”窗格中。

功能	说明
双重身份验证	双重身份验证功能实现了对远程访问网络的双因素身份验证，符合支付卡行业标准委员会数据安全标准。此功能要求用户在登录页上输入两组单独的登录凭据。例如，主身份验证可能是一次性密码，而辅助身份验证可能是域(Active Directory)凭据。如果任一身份验证失败，则连接会被拒绝。 AnyConnect VPN 客户端和无客户端 SSL VPN 都支持双重身份验证。AnyConnect 客户端支持在 Windows 计算机（包括支持的 Windows 移动设备和在登录前启动）、Mac 计算机和 Linux 计算机上进行双重身份验证。IPSec VPN 客户端、SVC 客户端、直通代理身份验证、硬件客户端身份验证和管理身份验证不支持双重身份验证。 双重身份验证要求以下新的隧道组常规属性配置模式命令： • **secondary-authentication-server-group** - 指定辅助 AAA 服务器组（不可以是 SDI 服务器组）。 • **secondary-username-from-certificate** - 允许从证书中提取一些标准 DN 字段以用作用户名。 • **secondary-pre-fill-username** - 支持提取用户名用于无客户端或 AnyConnect 客户端连接。 • **authentication-attr-from-server** - 指定应用于连接的身份验证服务器授权属性。 • **authenticated-session-username** - 指定与会话关联的身份验证用户名。 **注释** RSA/SDI 身份验证服务器类型不能用作辅助用户名/密码凭据。它只能用于主身份验证。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问或无客户端 SSL VPN > AnyConnect 连接配置文件 > 添加/编辑 > 高级 > 辅助身份验证**。

功能	说明
AnyConnect 基础版	AnyConnect 基础版是单独许可的 SSL VPN 客户端，完全在 ASA 上配置，可提供完整的 AnyConnect 功能，但存在以下例外： • 没有 CSD（包括主机扫描/保管库/缓存清理器） • 未安装无客户端 SSL VPN • 可选的 Windows 移动支持 AnyConnect 基础版客户端为运行 Microsoft Windows Vista、Windows Mobile、Windows XP 或 Windows 2000、Linux 或 Macintosh OS X 的远程最终用户提供思科 SSL VPN 客户端的优点。 若要配置 AnyConnect 基础版，管理员可使用以下命令： **anyconnect-essentials**- 启用 AnyConnect 基础版功能。如果禁用此功能（使用此命令的 **no** 形式），则使用 SSL 高级许可证。默认情况下启用此功能。 **注释** 此许可证不能与共享 SSL VPN 高级许可证同时使用。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > AnyConnect 基础版许可证**。必须为 ASDM 安装 AnyConnect 基础版许可证才能显示此窗格。

功能	说明
按连接配置文件禁用思科安全桌面	启用后，思科安全桌面将自动在与 ASA 建立 SSL VPN 连接的所有计算机上运行。通过此新功能，您可以免除某些用户按连接配置文件运行思科安全桌面。它可以避免检测这些会话的终端属性，因此您可能需要调整动态访问策略 (DAP) 配置。 CLI：[**no**] **without-csd** 命令 注释 ASDM 中的“连接配置文件”在 CLI 中也称为“隧道组”。此外，此功能还需要 **group-url** 命令。如果 SSL VPN 会话使用连接别名，则此功能将不起作用。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 连接配置文件 > 添加或编辑 > 高级 > 无客户端 SSL VPN 配置**。 或 **配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件 > 添加或编辑 > 高级 > SSL VPN**。
按连接配置文件的证书身份验证	以前的版本支持对每个 ASA 接口进行证书身份验证，因此即使用户不需要证书，也会收到证书提示。使用此新功能，只有在连接配置文件配置需要证书时，用户才会收到证书提示。此功能是自动的；不再需要 **ssl certificate authentication** 命令，但 ASA 保留它以实现向后兼容性。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 连接配置文件 > 添加/编辑 > 基本**。 或 **配置 > 远程访问 VPN > 无客户端 SSL VPN > 连接配置文件 > 添加/编辑 > 基本**。

功能	说明
证书映射的 EKU 扩展	此功能添加了创建证书映射的功能，该功能可用于查看客户端证书的扩展密钥用法扩展，并使用这些值确定客户端应使用的连接配置文件。如果客户端与该配置文件不匹配，则使用默认组。然后，连接的结果将取决于证书是否有效以及连接配置文件的身份验证设置。 引入了以下命令：**extended-key-usage**。 在 ASDM 中，使用 **IPSec 证书到连接映射 > 规则**窗格，或**证书到 SSL VPN 连接配置文件映射**窗格。
对 Win 2007 服务器的 SSL VPN SharePoint 支持	无客户端 SSL VPN 会话现在支持 Microsoft Office SharePoint Server 2007。
SSL VPN 会话的共享许可证	您可以为大量 SSL VPN 会话购买一个共享许可证，以及通过将一个 ASA 配置为共享许可证服务器并将其余 ASA 作为客户端，从而根据需要在一组 ASA 之间共享会话。引入了以下命令：**license-server** 命令（各种）、**show shared license**。 **注释** 此许可证不能与 AnyConnect 基础版许可证同时使用。 在 ASDM 中，请参阅**配置 > 设备管理 > 许可 > 共享 SSL VPN 许可证**。另请参阅**监控 > VPN > 无客户端 SSL VPN > 共享许可证**。
已更新 VPN 向导	已更新了 VPN 向导（可通过选择“向导”>“IPSec VPN 向导”来访问）。选择 IPSec 加密和身份验证的步骤（以前的第 9 步，共 11 步）已被删除，因为向导现在会为这些设置生成默认值。此外，选择 IPSec 设置（可选）的步骤现在包含新字段，以启用完全前向保密 (PFS) 并设置 Diffie-Hellman 组。
防火墙功能	
TCP 状态绕行	如果已在上游路由器中配置非对称路由，且流量在两个 ASA 之间交替传送，则可以为特定流量配置 TCP 状态绕行。引入了以下命令：**set connection advanced tcp-state-bypass**。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 规则操作 > 连接设置**。

功能	说明
由电话代理使用的媒体终止实例的按接口 IP 地址	在版本 8.0(4) 中，您在 ASA 上配置了一个全局媒体终止地址 (MTA)。在版本 8.2 中，您现在可以为单个接口配置 MTA（至少有两个 MTA）。由于此增强，旧的 CLI 已被弃用。如果需要，您可以继续使用旧配置。但是，如果需要更改配置，则只接受新的配置方法；您以后无法恢复旧配置。 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > 加密流量检测 > 媒体终止地址**。
显示电话代理的 CTL 文件	思科电话代理功能包含 **show ctl-file** 命令，该命令可显示电话代理所使用的 CTL 文件的内容。使用 **show ctl-file** 命令在配置电话代理实例调试时非常有用。 ASDM 中不支持此命令。
从电话代理数据库中清除安全电话条目	思科电话代理功能包含 **clear phone-proxy secure-phones** 命令，该命令可清除电话代理数据库中的安全电话条目。由于安全 IP 电话在启动后始终需要 CTL 文件，因此电话代理会创建将 IP 电话标记为安全的数据库。在指定的配置超时（通过 **timeout secure-phones** 命令）过后，安全电话数据库中的条目会被移除。或者，您可以使用 **clear phone-proxy secure-phones** 命令清除电话代理数据库，无需等待配置的超时。 ASDM 中不支持此命令。
H.323 应用检测中的 H.239 消息支持	在此版本中，ASA 支持 H.239 标准作为 H.323 应用检测的一部分。H.239 是一项标准，使 H.300 系列终端能够在单个呼叫中打开另外一个视频信道。在呼叫中，终端（例如视频电话）会发送视频信道和数据演示信道。H.239 协商发生于 H.245 信道上。ASA 为附加媒体信道打开一个针孔。终端使用开放逻辑信道 (OLC) 消息来发出有关新信道创建的信息。消息扩展是 H.245 v13 的一部分。默认情况下，电话演示会话的解码和编码已启用。H.239 的编码和解码由 ASN.1 编码器执行。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 添加服务策略规则向导 > 规则操作 > 协议检测 > H.323 H.225**。点击**配置**，然后选择 **H.323 检查映射**。

功能	说明
在终端不发送 OLCAck 时处理 H.323 终端	H.323 应用检测已得到改进，以处理通用 H.323 终端。该增强功能将 extendedVideoCapability OLC 与 H.239 协议标识符配合使用来影响终端。即使 H.323 终端在收到来自对等方的 OLC 消息后不发送 OLCAck，ASA 也会将 OLC 媒体方案信息传播到媒体阵列中，并为媒体信道 (extendedVideoCapability) 打开一个针孔。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 添加服务策略规则向导 > 规则操作 > 协议检测 > H.323 H.225**。
透明防火墙模式下的 IPv6	透明防火墙模式现在参与 IPv6 路由。在此版本之前，ASA 无法在透明模式下传输 IPv6 流量。现在，您可以在透明模式下配置 IPv6 管理地址、创建 IPv6 访问列表以及配置其他 IPv6 功能，ASA 可识别和传输 IPv6 数据包。 除非特别指明，否则支持所有 IPv6 功能。 在 ASDM 中，请参阅**配置 > 设备管理 > 管理访问 > 管理 IP 地址**。
僵尸网络流量过滤器	恶意软件是安装在未知主机上的出于恶意目的而开发的软件。当恶意软件发起与已知不良 IP 地址的连接时，僵尸网络流量过滤器可以检测到尝试进行网络活动（例如发送密码、信用卡号、键盘输入或专有数据等私人数据）的恶意软件。僵尸网络流量过滤器根据已知的不良域名和 IP 地址的动态数据库检查传入和传出连接，然后记录任何可疑活动。您也可以通过在本地“黑名单”或“白名单”中输入 IP 地址或域名，来使用静态数据库补充动态数据库。 **注释** 此功能需要使用僵尸网络流量过滤器许可证。有以下许可文档： http://www.cisco.com/en/US/docs/security/asa/asa82 引入了以下命令：**dynamic-filter** 命令（各种）和 **inspect dns dynamic-filter-snoop** 关键字。 在 ASDM 中，请参阅**配置 > 防火墙 > 僵尸网络流量过滤器**。

功能	说明
ASA 5505 的 AIP SSC 卡	AIP SSC 为 ASA 5505 ASA 提供 IPS。请注意，AIP SSM 不支持虚拟传感器。引入了以下命令：**allow-ssc-mgmt**、**hw-module module ip** 和 **hw-module module allow-ip**。 在 ASDM 中，请参阅**配置 > 设备设置 > SSC 安装和配置 > IPS**。
对 IPS 的 IPv6 支持	现在，当您的流量类使用 **match any** 命令而策略映射指定 **ips** 命令时，您可以将 IPv6 流量发送到 AIP SSM 或 SSC。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则**。
管理功能	
SNMP 版本 3 和加密	此版本提供 DES、3DES 或 AES 加密，并且支持 SNMP 版本 3（这是受支持的安全模型的最安全形式）。此版本允许您使用基于用户的安全模型 (USM) 来配置身份验证特性。 引入了以下命令： • **show snmp engineid** • **show snmp group** • **show snmp-server group** • **show snmp-server user** • **snmp-server group** • **snmp-server user** 修改了以下命令： • **snmp-server host** 在 ASDM 中，请参阅**配置 > 设备管理 > 管理访问 > SNMP**。
NetFlow	此功能在 ASA 5580 8.1(1) 版中引入；该版本将此功能引入其他平台。新 NetFlow 功能会通过 NetFlow 协议记录基于流的事件，由此增强了 ASA 日志记录功能。 在 ASDM 中，请参阅**配置 > 设备管理 > 日志记录 > Netflow**。

功能	说明
路由功能	
组播 NAT	ASA 现在为组地址提供组播 NAT 支持。
故障排除功能	
核心转储功能	核心转储是程序异常终止时，对正在运行的程序的快照。核心转储用于诊断或调试错误，以及保存崩溃情况供以后或非现场进行分析。思科TAC可能要求用户启用核心转储功能，以对 ASA 上的应用或系统崩溃进行故障排除。 若要启用核心转储，请使用 **coredump enable** 命令。
ASDM 功能	
对 IPv6 的 ASDM 支持	除非特别指明，否则支持所有 IPv6 功能。
支持公共服务器配置	您可以使用ASDM配置公共服务器。这使您可以定义要向外部接口公开的服务器和服务。 在 ASDM 中，请参阅**配置 > 防火墙 > 公共服务器**。

版本 8.1 的新功能

ASA 8.1(2)/ASDM 6.1(5) 的新功能

发布日期：**2008** 年 **10** 月 **10** 日

功能	说明
远程访问功能	

功能	说明
适用于 IE 的智能隧道自动登录	通过此功能，您可以替换 WININET 连接的登录凭证。大多数 Microsoft 应用均使用 WININET，包括 Internet Explorer。Mozilla Firefox 不使用 WININET，所以此功能不支持 Mozilla Firefox。此外，该功能还支持基于 HTTP 的身份验证，因此基于表单的身份验证不适用于此功能。 从统计方面而言，凭证与目标主机（而不是服务）相关联，所以如果初始凭证错误，在运行期间则无法动态更正它们。另外，鉴于凭证与目标主机相关联，所以如果要拒绝访问启用自动登录的主机上的某些服务，则对于这些主机提供支持可能不妥。 要为智能隧道配置一组自动登录，可创建一个自动登录站点全局列表，然后将该列表分配到组策略或用户名。对于动态访问策略不支持此功能。 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > ACL 管理器**。
委托证书调配	ASDM 6.1.3（允许您管理运行版本 8.0x 和 8.1x 的安全设备）包含一个指向委托网站的链接，用于为您的 ASA 申请临时（测试）或折扣性的永久 SSL 身份证书。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 证书管理 > 身份凭证 > 以委托形式注册 SSL VPN 头端**。
扩展了用户基于 IKE 密钥更新重新进行身份验证的时间	可以对安全设备进行配置，以便为远程用户提供更多时间来在第 1 阶段 SA 密钥更新时输入其凭证。以前，如果为 IKE 隧道配置了密钥更新时重新进行身份验证 (reauthenticate-on-rekey)，当发生第 1 阶段密钥更新时，安全设备会提示用户进行身份验证并仅为用户提供约 2 分钟的时间来输入其凭证。如果用户在 2 分钟时段内未输入其凭证，隧道将被终止。启用此新功能后，用户现在有更多时间在隧道断开前输入凭证。当真正发生密钥更新时建立的新第 1 阶段 SA 与旧的第 1 阶段 SA 到期之间的差异在于时间段不同。对于设定的默认第 1 阶段密钥更新时间，差异约为 3 小时或约为密钥更新间隔的 15%。 在 ASDM 中，请参阅**配置 > 设备管理 > 证书管理 > 身份证书**。

功能	说明
持久通过 IPSec 隧道传输的流	启用持久通过 IPSec 隧道传输的流后，安全设备将在隧道断开后保留并恢复基于状态 (TCP) 通过隧道传输的流，然后再进行恢复。隧道丢弃时，所有其他流量都会被丢弃，并且必须在新隧道出现时重建。保留 TCP 流允许某些较早或敏感的应用度过短暂的隧道中断而继续运行。此功能支持来自硬件客户端的 IPSec LAN 到 LAN 隧道和网络扩展模式隧道。它不支持 IPSec 或 AnyConnect/SSL VPN 远程访问隧道。请参见 **sysopt connection preserve-vpn-flows** 命令。默认情况下该选项处于禁用状态。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 系统选项**。选中**当隧道由于网络扩展模式 (NEM) 中断时保留基于状态的 VPN 流**复选框，以启用持久通过 IPSec 隧道传输的流。
显示 Active Directory 组	添加了 CLI 命令 **show ad-groups**，以列出 Active Directory 组。ASDM 动态访问策略使用此命令为管理员提供可用来定义 VPN 策略的 MS AD 组列表。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 动态访问策略 > 添加/编辑 DAP > 添加/编辑 AAA 属性**。
Mac OS 上的智能隧道	智能隧道现在支持 Mac OS。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 智能隧道**。
防火墙功能	
NetFlow 过滤	您可以根据流量和事件类型过滤 NetFlow 事件，然后将记录发送到不同的收集器。例如，可以将所有流创建事件记录到一个收集器，而将流拒绝的事件记录到另一个收集器。请参阅 **flow-export event-type** 命令。 在 ASDM 中，请参阅**配置 > 防火墙 > 安全策略 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > NetFlow**。

功能	说明
NetFlow 延迟流创建事件	对于短暂的流，NetFlow 收集设备无需查看两个事件：流创建和损毁，只需处理单个事件即可，受益匪浅。现在，您可以在发送流创建事件之前配置延迟。如果流在计时器到期之前被损毁，则只发送流损毁事件。请参阅 **flow-export delay flow-create** 命令。 **注释** 损毁事件包括有关流的所有信息；信息不会丢失。 在 ASDM 中，请参阅**配置 > 设备管理 > 日志记录 > NetFlow**。
QoS 流量整形	如果您有高速传输数据包的设备，例如使用快速以太网的 ASA，但它连接到低速设备，例如电缆调制解调器，则电缆调制解调器是导致数据包被频繁丢弃的瓶颈。要管理具有不同线路速率的网络，可将安全设备配置为以较慢的固定速率传输数据包。请参阅 **shape** 命令。 另请参阅 **crypto ipsec security-association replay** 命令，该命令允许您配置 IPSec 防重放窗口大小。优先级排队的一个负面影响是数据包重新排序。对于 IPSec 数据包，未处于防重放窗口内的错序数据包，会生成警告系统日志消息。在进行优先级排队的情况下，这些警告会变成错误警报。此新命令可避免潜在的错误警报。 在 ASDM 中，请参阅**配置 > 防火墙 > 安全策略 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > QoS**。请注意，唯一支持流量整形的流量类为 class-default，该类与所有流量匹配。

功能	说明
TCP 规范化增强	现在，您可以为特定数据包类型配置TCP规范化操作。以前，针对这种数据包的默认操作是丢弃数据包。现在，您可以设置TCP规范器来允许数据包。 • TCP 无效 ACK 检查（**invalid-ack** 命令） • TCP 数据包序列通过窗口检查（**seq-past-window** 命令） • TCP SYN-ACK 及数据检查（**synack-data** 命令） 另外，您还可以设置TCP错序数据包缓冲区超时（**queue** 命令 **timeout** 关键字）。以前，该超时值为 4 秒。现在，您可以将超时设置为其他值。 针对超出 MSS 的数据包的默认操作从“丢弃”改为“允许”（**exceed-mss** 命令）。 对于这些数据包类型，以下不可配置的操作从“丢弃”改成了“清除”： • TCP 中的选项长度错误 • 非 SYN 上的 TCP 窗口扩展 • TCP 窗口扩展值错误 • 错误 TCP SACK ALLOW 选项 在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > TCP 映射**。
TCP 拦截统计信息	您可以使用 **threat-detection statistics tcp-intercept** 命令启用 TCP 拦截统计信息收集，并使用 **show threat-detection statistics** 命令查看具体信息。 在 ASDM 中，请参阅**配置 > 防火墙 > 威胁检测**。
威胁检测避开超时	现在，您可以使用 **threat-detection scanning-threat shun duration** 命令配置威胁检测避开超时。 在 ASDM 中，请参阅**配置 > 防火墙 > 威胁检测**。
威胁检测主机统计信息微调	现在，您可以通过使用 **threat-detection statistics host number-of-rate** 命令来减少收集的主机统计信息量，从而减少此功能对系统的影响。 在 ASDM 中，请参阅**配置 > 防火墙 > 威胁检测**。

功能	说明
平台功能	
增加了 VLAN 数量	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。
未命名接口的 SNMP 支持	以前，SNMP 只提供了有关使用 **nameif** 命令配置的接口的信息。例如，SNMP 仅为已命名的接口发送陷阱和对 IF MIB 和 IP MIB 执行的检测。SNMP 已经过增强，可以显示有关所有物理接口和逻辑接口的信息；使用 SNMP 显示接口不再需要 **nameif** 命令。

ASA 8.1(1)/ASDM 6.1(1) 的新功能

发布日期：2008 年 3 月 1 日

功能	说明
思科 ASA 5580 简介	思科 ASA 5580 有两个型号： • ASA 5580-20 提供每秒 5 千兆的 TCP 流量，并且 UDP 性能更优。系统中的许多功能都支持多核，可以实现这种高吞吐量。此外，系统每秒可提供超过 6 万个 TCP 连接，并支持多达百万个连接。 • ASA 5580-40 提供每秒 10 千兆的 TCP 流量，与 ASA 5580-20 类似，UDP 性能也是更优。系统每秒可提供超过 12 万个 TCP 连接，并总共支持多达二百万个连接。 在 ASDM 中，请参阅**主页 > 系统资源状态和主页 > 设备信息 > 环境状态**。
NetFlow	新 NetFlow 功能会通过 NetFlow 协议记录基于流的事件，由此增强了 ASA 日志记录功能。有关此功能和新 CLI 命令的详细信息，请参阅*思科 ASA 5580 自适应安全设备命令行配置指南*。 在 ASDM 中，请参阅**配置 > 设备管理 > 日志记录 > Netflow**。

功能	说明
支持巨帧	输入 **jumbo-frame reservation** 命令时，思科 ASA 5580 支持巨帧。巨帧是指大于标准最大字节数（1518 字节）的以太网数据包（包括第 2 层报头和 FCS），最大可达 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨帧支持。为巨帧分配较多内存可能会有碍于最大限度地利用其他功能（例如访问列表）。 在 ASDM 中，请参阅**配置 > 设备设置 > 接口 > 添加/编辑接口 > 高级**。
多核 ASA 的每包负载均衡	对于多核 ASA，默认行为是一次只允许一个核心从接口接收环接收数据包。**asp load-balance per-packet** 命令更改了此行为，以允许多个核心从接口接收环接收数据包并对数据包单独进行处理。针对在所有接口环统一接收数据包的情况优化默认行为。 引入了以下命令：**asp load-balance per-packet** 和 **show asp load-balance**。
SIP 临时媒体超时	现在，您可以使用 timeout sip-provisional-media 命令为 SIP 临时媒体配置超时。 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > 全局超时**。
有关激活密钥的详细信息	现在，您可以使用 **show activation key detail** 命令查看永久和临时激活密钥及其启用的功能，包括以前安装的所有临时密钥及其到期日期。 在单情景模式下的 ASDM 中，请参阅**配置 > 设备管理 > 系统映像/配置 > 激活密钥**。在多情景模式下的 ASDM 中，请参阅**系统 > 配置 > 设备管理 > 激活密钥**。
新的 ASDM 在线帮助引擎	ASDM 现在支持在线帮助的新外观。现在，在线帮助左侧是书签窗格，用户可从中选择主题，同时可以浏览右侧的窗格的主题。
ASDM CPU 核心使用图形	在单模式或多模式下，CPU 核心的使用图形可以从 ASDM 主页显示核心 CPU 利用率状态。
适用于 ASDM 的智能平台管理界面 (IPMI)	增加了对智能平台管理界面 (IPMI) 的支持，该界面可从 ASDM 主页为用户提供有关电源状态、冷却风扇以及处理器和机箱温度的信息。

功能	说明
ASDM 助手	现在，ASDM助手从**查看**菜单而不是**工具**菜单访问。GUI 已经过更改，简化了**搜索**机制。
ASDM 备份和恢复增强功能	通过备份和恢复增强功能，您可以将配置备份到本地计算机，然后在必要时将其恢复回到服务器。此外，此功能还可备份与SSL VPN相关的文件。此功能可通过**工具 > 备份配置**和**工具 > 恢复配置**访问。 同样适用于版本 *8.0*。
ASDM 日志查看器	日志查看器增强后可显示从系统日志消息中解析出的源和目标端口信息。此信息显示在**监控 > 日志记录 > 实时日志查看器**和**日志缓冲区**页面中。 同样适用于版本 *8.0*。
ASDM 中增强的 VPN 搜索	添加了一个基于 CLI 命令的搜索功能，当您在键入关键字或命令时，该功能可提供智能提示。此搜索增强功能仅存在于“用户帐户”、“连接配置文件”和“组策略”页面。 同样适用于版本 *8.0*。

版本 8.0 的新功能

ASA 8.0(5)/ASDM 6.2(3) 的新功能

发布日期：**2009** 年 **11** 月 **3** 日

注释 PIX 安全设备不支持版本 8.0(5)。

功能	说明
远程访问功能	

功能	说明
等待恢复 (Waiting-to-Resume) VPN 会话的可扩展解决方案	管理员现在可跟踪处于活动状态的用户数量，也可以查看统计信息。处于非活动状态时间最长的会话会被标记为空闲（并自动注销），这样就不会达到许可证容量限制，而且新用户也就可以登录。 修改了以下 ASDM 菜单项：**监控 > VPN > VPN 统计信息 > 会话**。 同样适用于版本 *8.2(2)*。
应用检测功能	
在 H.323 终端之间启用调用设置	如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。ASA 包括基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息打开呼叫针孔的选项。 由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且安全设备会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。 引入了以下命令：**ras-rcf-pinholes enable**。在创建 H.323 检查策略图时，在参数配置模式下使用此命令。 修改了以下 ASDM 菜单项：**配置 > 防火墙 > 对象 > 检查映射 > H.323 > 详细信息 > 状态检查**。 同样适用于版本 *8.2(2)*。
接口功能	
在多情景模式下，自动生成的 MAC 地址现在使用用户可配置的前缀以及其他增强功能	MAC 地址格式更改为允许使用前缀，以便使用固定起始值 (A2)，并在故障切换对中为主设备和辅助设备 MAC 地址使用不同方案。 现在，MAC 地址在重新加载之后也会保持不变。 现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。 修改了以下命令：**mac-address auto prefix** *prefix*。 修改了以下 ASDM 菜单项：**配置 > 情景管理 > 安全情景**。 同样适用于版本 *8.2(2)*。
高可用性功能	

功能	说明
在切换事件期间启用或关闭接口时不发送通知	要在故障切换期间区分从链路连接过渡到链路断开正常操作期间的链路连接/断开过渡，在故障切换期间不发送链路连接/断开陷阱。另外，在故障切换期间不会针对断链路连接/断开过渡发送系统日志消息。 同样适用于版本 *8.2(2)*。
路由功能	
兼容 DHCP RFC（rfc3011、rfc3527）以解决路由问题	此增强功能对于 DHCP RFCs 3011（IPv4 子网选择选项）和 3527（中继代理信息选项的链路选择子选项）引入了 ASA 支持。对于使用 **dhcp-server** 命令时配置的每个 DHCP 服务器，现在您可以将 ASA 配置为发送 **subnet-selection** 选项或 **link-selection** 选项，或是二者都不发送。 修改了以下 ASDM 菜单项： **远程接入 VPN > 网络接入 > IPSec 连接配置文件 > 添加/编辑**。 同样适用于版本 *8.2(2)*。
SSM 功能	
ASDM 中对 CSC 6.3 的支持	ASDM 在主页上的“增强型许可证”列表中显示 Web 声誉、用户组策略和用户 ID 设置。纳入了 CSC 6.3 安全事件增强功能，例如新的 Web 声誉事件以及用户和组标识。

ASA 8.0(4)/ASDM 6.1(3) 的新功能

发布日期：2008 年 8 月 11 日

功能	说明
统一通信功能脚注。	

功能	说明
电话代理	支持电话代理功能。ASA 电话代理提供与 Metreos 思科统一电话代理的功能类似的功能，并为 SIP 检测和增强的安全性提供额外的支持。ASA 电话代理具有以下主要功能： • 通过强制电话加密信号和媒体来保护远程 IP 电话 • 使用远程 IP 电话执行基于证书的身份验证 • 终止来自 IP 电话的 TLS 信号，并启动到思科 Unified Mobility Advantage 服务器的 TCP 和 TLS 信号 • 终止 SRTP 并启动到被叫方的 RTP/SRTP 信号 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > 加密流量检测 > 电话代理**。
移动代理	支持思科 Unified Mobility Advantage 客户端与服务器之间的安全连接（移动代理）。 思科 Unified Mobility Advantage 解决方案包括思科 Unified Mobile Communicator，这是一种易于使用的移动手持式设备软件应用，可将企业通信应用和服务扩展到移动电话和智能手机以及思科 Unified Mobility Advantage 服务器。移动解决方案简化了通信体验，支持在整个企业内进行实时协作。 该解决方案中的 ASA 提供对 MMP（以前称为 OLWP）协议的检测，该协议是思科 Unified Mobile Communicator 与思科 Unified Mobility Advantage 之间的专有协议。ASA 还充当 TLS 代理，用于在思科 Unified Mobile Communicator 与思科 Unified Mobility Advantage 之间终止和重新发出 TLS 信号。 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > 加密流量检测 > TLS 代理**。

功能	说明
状态联合代理	支持思科 Unified Presence 服务器与思科/Microsoft Presence 服务器之间的安全连接（状态联合代理）。通过 Presence 解决方案，企业可以将其思科 Unified Presence 客户端安全地连接回其企业网络，或在不同企业的 Presence 服务器之间共享 Presence 信息。 ASA 提供功能来支持 Presence 在互联网与企业内部之间进行通信。支持 SSL 的思科 Unified Presence 客户端可以与 Presence 服务器建立 SSL 连接。ASA 支持在服务器与服务器通信之间启用 SSL 连接，包括与思科 Unified Presence 服务器通信的第三方 Presence 服务器。企业共享 Presence 信息，并且可以使用 IM 应用。ASA 会检测服务器之间的 SIP 消息。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > 协议检测或配置 > 防火墙 > 高级 > 加密流量检测 > TLS 代理 > 添加 > 客户端配置**。
远程访问功能	
用于 IE1 的智能隧道自动登录 脚注。	通过此功能，您可以替换 WININET 连接的登录凭证。大多数 Microsoft 应用均使用 WININET，包括 Internet Explorer。Mozilla Firefox 不使用 WININET，所以此功能不支持 Mozilla Firefox。此外，该功能还支持基于 HTTP 的身份验证，因此基于表单的身份验证不适用于此功能。 从统计方面而言，凭证与目标主机（而不是服务）相关联，所以如果初始凭证错误，在运行期间则无法动态更正它们。另外，鉴于凭证与目标主机相关联，所以如果要拒绝访问启用自动登录的主机上的某些服务，则对于这些主机提供支持可能不妥。 要为智能隧道配置一组自动登录，可创建一个自动登录站点全局列表，然后将该列表分配到组策略或用户名。对于动态访问策略不支持此功能。 在 ASDM 中，请参阅**防火墙 > 高级 > ACL 管理器**。

功能	说明
委托证书调配 脚注。	ASDM 包含一个指向委托网站的链接，该网站用于为您的 ASA 申请临时（测试）或打折的永久 SSL 身份证书。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 证书管理 > 身份证书**。点击**通过委托注册 SSL VPN 前端**。
扩展了用户基于 IKE 密钥更新重新进行身份验证的时间	可以对安全设备进行配置，以便为远程用户提供更多时间来在第 1 阶段 SA 密钥更新时输入其凭证。以前，如果为 IKE 隧道配置了密钥更新时重新进行身份验证 (reauthenticate-on-rekey)，当发生第 1 阶段密钥更新时，安全设备会提示用户进行身份验证并仅为用户提供约 2 分钟的时间来输入其凭证。如果用户在 2 分钟时段内未输入其凭证，隧道将被终止。启用此新功能后，用户现在有更多时间在隧道断开前输入凭证。当真正发生密钥更新时建立的新第 1 阶段 SA 与旧的第 1 阶段 SA 到期之间的差异在于时间段不同。对于设定的默认第 1 阶段密钥更新时间，差异约为 3 小时或约为密钥更新间隔的 15%。 在 ASDM 中，请参阅**配置 > 设备管理 > 证书管理 > 身份证书**。
持久通过 IPSec 隧道传输的流	启用持久通过 IPSec 隧道传输的流后，安全设备将在隧道断开后保留并恢复基于状态 (TCP) 通过隧道传输的流，然后再进行恢复。隧道丢弃时，所有其他流量都会被丢弃，并且必须在新隧道出现时重建。保留 TCP 流允许某些较早或敏感的应用度过短暂的隧道中断而继续运行。此功能支持来自硬件客户端的 IPSec LAN 到 LAN 隧道和网络扩展模式隧道。它不支持 IPSec 或 AnyConnect/SSL VPN 远程访问隧道。请参阅 **[no] sysopt connection preserve-vpn-flows** 命令。默认情况下该选项处于禁用状态。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 系统选项**。选中**当隧道由于网络扩展模式 (NEM) 中断时保留基于状态的 VPN 流**复选框，以启用持久通过 IPSec 隧道传输的流。

功能	说明
显示 Active Directory 组	添加了 CLI 命令 **show ad-groups**，以列出 Active Directory 组。ASDM 动态访问策略使用此命令为管理员提供可用来定义 VPN 策略的 MS AD 组列表。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 动态访问策略 > 添加/编辑 DAP > 添加/编辑 AAA 属性**。
通过 Mac OS1 传输的智能隧道 脚注。	智能隧道现在支持 Mac OS。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 门户 > 智能隧道**。
本地地址池编辑	您可以编辑地址池，而不会影响所需的连接。如果不从池中删除正在使用的地址，则连接不受影响。不过，如果要从池中删除正在使用的地址，连接则会断开。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
防火墙功能	
QoS 流量整形	如果您有高速传输数据包的设备，例如使用快速以太网的 ASA，但它连接到低速设备，例如电缆调制解调器，则电缆调制解调器是导致数据包被频繁丢弃的瓶颈。要管理具有不同线路速率的网络，可将安全设备配置为以较慢的固定速率传输数据包。请参阅 **shape** 命令。另请参阅 **crypto ipsec security-association replay** 命令，该命令允许您配置 IPSec 防重放窗口大小。优先级排队的一个负面影响是数据包重新排序。对于 IPSec 数据包，未处于防重放窗口内的错序数据包，会生成警告系统日志消息。在进行优先级排队的情况下，这些警告会变成错误警报。此新命令可避免潜在的错误警报。 在 ASDM 中，请参阅**配置 > 防火墙 > 安全策略 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > QoS**。请注意，唯一支持流量整形的流量类为 class-default，该类与所有流量匹配。 同样适用于版本 *7.2(4)*。

功能	说明
TCP 规范化增强	现在，您可以为特定数据包类型配置TCP规范化操作。以前，针对这种数据包的默认操作是丢弃数据包。现在，您可以设置TCP规范器来允许数据包。 • TCP 无效 ACK 检查（**invalid-ack** 命令） • TCP 数据包序列通过窗口检查（**seq-past-window** 命令） • TCP SYN-ACK 及数据检查（**synack-data** 命令） 另外，您还可以设置TCP错序数据包缓冲区超时（**queue** 命令 **timeout** 关键字）。以前，该超时值为 4 秒。现在，您可以将超时设置为其他值。 针对超出 MSS 的数据包的默认操作从“丢弃”改为“允许”（**exceed-mss** 命令）。 对于这些数据包类型，以下不可配置的操作从“丢弃”改成了“清除”： • TCP 中的选项长度错误 • 非 SYN 上的 TCP 窗口扩展 • TCP 窗口扩展值错误 • 错误 TCP SACK ALLOW 选项 在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > TCP 映射**。 同样适用于版本 *7.2(4)*。
TCP 拦截统计信息	您可以使用 **threat-detection statistics tcp-intercept** 命令启用 TCP 拦截统计信息收集，并使用 **show threat-detection statistics** 命令查看具体信息。 在 ASDM 6.1(5) 及更高版本中，请参阅**配置 > 防火墙 > 威胁检测**。ASDM 6.1(3) 中不支持此命令。
威胁检测避开超时	现在，您可以使用 **threat-detection scanning-threat shun duration** 命令配置威胁检测避开超时。 在 ASDM 6.1(5) 及更高版本中，请参阅**配置 > 防火墙 > 威胁检测**。ASDM 6.1(3) 中不支持此命令。

功能	说明
SIP 临时媒体超时	现在，您可以使用 **timeout sip-provisional-media** 命令来配置 SIP 临时媒体的超时时间。 在 ASDM 中，请参阅**配置 > 防火墙 > 高级 > 全局超时**。 同样适用于版本 *7.2(4)*。
clear conn 命令	添加了 **clear conn** 命令，以删除连接。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
完全重组数据分段	通过 **reassembly full** 关键字改进了 **fragment** 命令，支持完全重组通过设备传输的数据分段。在设备处终止的数据分段始终会完全重组。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
Ethertype ACL MAC 增强	EtherType ACL 功能进行了增强，支持非标准的 MAC。现有的默认规则予以保留，但无需添加新规则。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
故障排除和监控功能	
capture 命令增强	**capture type asp-drop** *drop_code* 命令现在接受 **all** 作为 *drop_code*，所以您现在可以捕获 ASA 丢弃的所有数据包，包括由于安全检查而丢弃的数据包。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
show asp drop 命令增强	输出现在包括指示计数器上次清除时间的时间戳（请参阅 **clear asp drop** 命令）。输出还会在说明旁边显示丢弃原因关键字，以便您能够轻松使用具有该关键字的 **capture asp-drop** 命令。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
clear asp table 命令	添加了 **clear asp table** 命令，以清除“show asp table”命令输出的命中次数。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。

功能	说明
show asp table classify hits 命令增强	将 **hits** 选项添加到 **show asp table classify** 命令，用于显示指示上次何时清除 asp 表计数器的时间戳。该命令还会显示符合值不等于零的规则。借此，用户可以快速查看符合哪些规则，特别是 **show asp table classify** 命令中一个简单配置以数百个条目结尾的情况。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
MIB 增强	更加全面地实施 CISCO-REMOTE-ACCESS-MONITOR-MIB。 同样适用于 *8.0(4)* 版本。
show perfmon 命令	添加了以下输出：已建立 TCP 拦截连接、TCP 拦截尝试、TCP 初期连接超时和 TCP 拦截中的连接速率有效。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。

功能	说明
memory tracking 命令	此版本中引入了以下新命令： • **memory tracking enable** - 此命令支持跟踪堆内存请求。 • **no memory tracking enable** - 此命令禁止跟踪堆内存请求、清理当前收集的所有信息，并向系统返回工具本身使用的所有堆内存。 • **clear memory tracking** - 此命令会清除当前收集的所有信息，但会继续跟踪进一步的内存请求。 • **show memory tracking** - 此命令显示当前工具所跟踪的已分配内存，它们按最上方的调用方函数地址进行细分。 • **show memory tracking address** - 此命令显示当前按每一块内存细分的已分配内存。输出会列出当前工具跟踪的每个已分配内存块的大小、位置以及最上方的调用方函数。 • **show memory tracking dump** - 此命令显示指定内存地址的大小、位置、部分调用栈和内存转储。 • **show memory tracking detail** - 此命令显示探查工具内部行为时要使用的各种内部详细信息。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
路由功能	

功能	说明
IPv6 组播侦听程序发现协议 v2 支持	ASA 现在支持组播侦听程序发现协议 (MLD) 版本 2，以发现组播地址侦听程序在其直接连接的链路上的在线状态，并具体发现哪些组播地址与相邻节点相关。ASA 将成为组播地址侦听程序或主机（但不是组播路由器），并只响应组播侦听程序查询且仅发送组播侦听程序报告。 以下命令支持此功能： • **clear ipv6 mld traffic** - clear ipv6 mld traffic 命令使您可以重置所有组播侦听程序发现流量计数器。 • **show ipv6 mld traffic** - show ipv6 mld 命令使您可以显示所有组播侦听程序发现流量计数器。 • **debug ipv6 mld** - 对 debug ipv6 命令的增强，使用户可以显示 MLD 的调试消息，以查看 MLD 协议活动是否正常工作。 • **show debug ipv6 mld** - 对 show debug ipv6 命令的增强，使用户可以显示是启用还是禁用 debug ipv6 mld。 同样适用于版本 *7.2(4)*。
平台功能	
对 ASA 5505 的本地 VLAN 支持	现在，您可以通过 **switchport trunk native vlan** 命令在 ASA 5505 主干端口中包括本机 VLAN。 在 ASDM 中，请参阅**配置 > 设备安装 > 接口 > 交换机端口 > 编辑**对话框。 同样适用于版本 *7.2(4)*。
未命名接口的 SNMP 支持	以前，SNMP 仅提供有关使用 **nameif** 命令配置的接口的信息。例如，SNMP 仅为已命名的接口发送陷阱和对 IF MIB 和 IP MIB 执行的检测。由于 ASA 5505 配有未命名的交换机端口和命名的 VLAN 接口，因此增强了 SNMP 以显示有关所有物理接口和逻辑接口的信息；使用 SNMP 显示接口不再需要 **nameif** 命令。这些更改会影响所有型号，而不仅仅是 ASA 5505。
故障切换功能	

功能	说明
failover timeout 命令	**failover timeout** 命令用于静态指定功能时，不再需要故障切换许可证。 同样适用于版本 *7.0(8)* 和 *7.2(4)*。
ASDM 功能	
简化 DNS 面板	ASDM GUI 上的 DNS 面板已经过修改，以便于使用。请参阅**配置 > 设备管理 > DNS**。
重新设计“文件传输”对话框	可以在“文件传输”对话框中拖放文件。若要访问此对话框，请转到**工具 > 文件管理**，然后点击**文件传输**。
清除 ACL 命中计数器	添加了使用户能够清除ACL命中计数器的功能。请参阅**防火墙 > 高级 > ACL 管理器**面板。
重命名 ACL	添加了从 ASDM 重命名 ACL 的功能。 请参阅**防火墙 > 高级 > ACL 管理器**面板。
将 ASDM/HTTPS、SSH、Telnet 合并到一个面板中	ASDM 已将 ASDM、HTTPS、SSH、Telnet 组合在一个面板中。请参阅**监控 > 属性 > 设备访问 > ASDM/HTTPS/Telnet/SSH 会话**面板。
在 ACL 管理器中显示所有标准 ACL	添加了使用户能够在ACL管理器中显示所有标准ACL 的功能。 请参阅**防火墙 > 高级 > ACL 管理器**面板。

[1] (1) 此功能在 PIX 安全设备上不受支持。

ASA 8.0(3)/ASDM 6.0(3) 的新功能

发布日期：2007 年 11 月 7 日

功能	说明
VPN 功能	

功能	说明
AnyConnect RSA SoftID API 集成	支持 AnyConnect VPN 客户端直接与 RSA SoftID 进行通信以获取用户令牌代码。通过此集成，可以指定对连接配置文件（隧道组）的 SoftID 消息支持，并且可以在安全设备上配置与通过RADIUS代理接收的 SDI 消息匹配的 SDI 消息。此功能可确保向远程客户端用户显示的提示适用于身份验证期间需要执行的操作，并且 AnyConnect 客户端可以成功应对身份验证挑战。
IP 地址重用延迟	将 IP 地址返回到 IP 地址池后，延迟该地址的重用。增加延迟可防止IP地址返回地址池并快速重新分配时安全设备可能遇到的问题。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 地址分配 > 分配策略**。

无客户端 SSL VPN 缓存静态内容增强	无客户端 SSL VPN 缓存命令有两项变动：
	cache-compressed 命令被启用。
	新的 **cache-static-content** 命令将 ASA 配置为缓存所有静态内容，这意味着所有可缓存的 Web 对象都不受 SSL VPN 重写的干扰。其中包括映像和 PDF 文件等内容。
	该命令的语法是 **cache-static-content** {**enable** | **disable**}。默认情况下，禁用静态内容缓存。
	示例：
	`hostname (config) # webvpn`
	`hostname (config-webvpn) # cache`
	`hostname (config-webvpn-cache) #`
	`cache-static-content enable`
	hostname (config-webvpn-cache) #
	在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 内容缓存**。
	同样适用于版本 *7.2(3)*。

功能	说明
移除智能卡时断开连接	此功能使中心站点管理员可配置远程客户端策略，以便在移除智能卡时删除活动隧道。默认情况下，当用户移除用于身份验证的智能卡时，思科 VPN 远程访问软件客户端（IPSec 和 SSL）会清除现有的 VPN 隧道。以下 cli 命令在移除智能卡时会断开现有的 VPN 隧道：**smartcard-removal-disconnect** {**enable** | **disable**}。默认情况下，此选项已启用。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑内部/外部组策略 > 更多选项**。 同样适用于版本 *7.2(3)*。
WebVPN 负载均衡	自适应安全设备现在支持使用FQDN执行负载均衡。要使用 FQDN 执行 WebVPN 负载均衡，必须启用使用 FQDN 执行负载均衡，请输入 **redirect-fqdn enable** 命令。然后，对于每个自适应安全设备外部接口向 DNS 服务器中添加一个条目（如果尚不存在）。每个自适应安全设备外部 IP 地址都应该有一个与其关联的 DNS 条目用于查找。对于反向查找，也必须启用这些 DNS 条目。使用 **dns domain-lookup inside** 命令（或具有通向 DNS 服务器的路由的任一接口）在自适应安全设备上启用 DNS 查找。最后，必须在您的自适应安全设备上定义DNS服务器的IP地址。下面是与此增强相关的新 CLI：**redirect-fqdn** {**enable** | **disable**}。 在 ASDM 中，请参阅**配置 > VPN > 负载均衡**。 同样适用于版本 *7.2(3)*。
应用检测功能	

功能	说明
WAAS 和 ASA 互操作性	添加了 **inspect waas** 命令，以在策略映射类配置模式下启用 WAAS 检查。此 CLI 集成在模块化策略框架内，以便最大限度地灵活配置功能。可以在默认的检查类和自定义类映射下配置 [no] inspect waas 命令。默认情况下，此检测服务未启用。 **show service-policy inspect** 命令中添加了关键字选项 waas，以显示 WAAS 统计信息。 `show service-policy inspect waas` 在连接中检测到 WAAS 优化时，生成一条新的系统日志消息。在 WAAS 优化的连接中绕过包括 IPS 在内的所有 L7 检测服务。 系统日志编号和格式： %ASA-6-428001：从 in_interface:src_ip_addr/src_port 向 out_interface:dest_ip_addr/dest_port 确认的 WAAS，在此连接中绕过检测服务。 WAAS 连接中添加了新的连接标记“W”。**show conn detail** 命令已更新以反映新的标志。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > 协议检测**。 同样适用于版本 *7.2(3)*。
DNS Guard 增强	添加了启用或禁用 DNS Guard 的选项。启用时，此功能仅允许 DNS 请求返回一个 DNS 响应。 在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > 检查映射 > DNS**。 同样适用于版本 *7.2(3)*。

功能	说明

支持基于 TLS 的 ESMTP	此增强功能在 esmtp 策略映射中添加了配置参数 **allow-tls** [**action log**]。默认情况下，不启用此参数。启用此功能后，ESMTP 检查不会将来自服务器的 250-STARTTLS 回应和来自客户端的 STARTTLS 命令屏蔽。在服务器回应 220 个应答代码后，ESMTP 检测会自行关闭；不再检测该会话中的 ESMTP 流量。如果已配置 **allow-tls action log** 参数，则在 ESMTP 会话中启动 TLS 时会生成系统日志消息 ASA-6-108007。
	
	`policy-map type inspect esmtp esmtp_map`
	
	`parameters`
	
	`allow-tls [action log]`
	
	用于显示与 **allow-tls** 参数关联的计数器的新行已添加到 show service-policy inspect esmtp 命令中。仅在策略映射中已配置 **allow-tls** 时才会显示该行。默认情况下，不启用此参数。
	
	`show service-policy inspect esmtp`
	`allow-tls, count 0, log 0`
	
	此增强功能会为 **allow-tls** 参数添加一条新的系统日志消息。它指示在 esmtp 会话中，服务器已使用 220 应答代码响应客户端 STARTTLS 命令。ESMTP 检测引擎不再检测此连接中的流量。
	
	系统日志编号和格式：
	
	%ASA-6-108007：TLS 在客户端 <client-side interface-name>:<client IP address>/<client port> 与服务器 <server-side interface-name>:<server IP address>/<server port> 之间的 ESMTP 会话上启动
	
	在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > 检查映射 > ESMTP**。
	
	同样适用于版本 *7.2(3)*。

高可用性功能	

功能	说明
添加了数据平面保持连接机制	现在，您可以配置 ASA 以免在升级 AIP SSM 时发生故障切换。在以前版本中，如果在故障切换中配置两个具备 AIP SSM 的 ASA，在更新 AIP SSM 软件时，ASA 就会触发故障切换，因为 AIP SSM 需要重新引导或重启，才会使软件更新生效。 同样适用于版本 *7.0(7)* 和 *7.2(3)*
完全限定域名支持增强功能	在 **redirect-fqdn** 命令中添加了选项，以将完全限定域名 (FQDN) 或 IP 地址发送至 VPN 负载均衡集群中的客户端。 在 ASDM 中，请参阅**配置 > 设备管理 > 高可用性 > VPN 负载均衡**或**配置 > 远程访问 VPN > 负载均衡**。
DHCP 功能	
DHCP 客户端 ID 增强	如果使用 **ip address dhcp** 命令对接口启用 DHCP 客户端，某些 ISP 会将选项 61 作为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。使用此新命令可包含选项 61 的接口 MAC 地址。如果未配置此命令，客户端 ID 则如下所示： cisco-<MAC>-<interface>-<hostname>。 引入了以下命令：**dhcp-client client-id interface** *interface_name* 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 服务器**；然后点击**高级**。 同样适用于版本 *7.2(3)*。

功能	说明
DHCP 客户端广播标志	如果使用 **ip address dhcp** 命令为接口启用 DHCP 客户端，则当 DHCP 客户端发送发现请求 IP 地址时，便可使用此命令在 DHCP 数据包报头中将广播标志设置为 1。DHCP 服务器侦听此广播标志，并在标志设置为 1 时广播应答数据包。 如果输入 **no dhcp-client broadcast-flag** 命令，则广播标志设置为 0，并且 DHCP 服务器使用提供的 IP 地址将应答数据包单播到客户端。 DHCP 客户端可以从 DHCP 服务器接收广播和单播。 引入了以下命令：**dhcp-client broadcast-flag** 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 服务器**；然后点击**高级**。
平台功能	
ASA 5510 增强型安全许可证对于端口 0 和 1 支持千兆以太网	ASA 5510 ASA 现在配备增强型安全许可证，对于端口 0 和 1 支持 GE（千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部端口 Ethernet0/0 和 Ethernet0/1 的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。 同样适用于版本 *7.2(3)*。
ASA 5505 扩大了 VLAN 范围	ASA 5505 ASA 现在支持介于 1 到 4090 之间的 VLAN ID。最初仅支持介于 1 到 1001 之间的 VLAN ID。 同样适用于版本 *7.2(3)*。
故障排除功能	

功能	说明
Capture 命令增强	对 capture 命令的增强允许用户实时捕获和显示流量。此外，该命令还允许用户指定过滤流量的命令行选项，而不必配置单独的访问列表。此增强功能添加了 **real-time** 和 five-tupple **match** 选项。 **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] 同样适用于版本 *7.2(3)*。
ASDM 功能	
ASDM 横幅增强	自适应安全设备软件支持 ASDM 横幅。如果已配置横幅，在启动 ASDM 时，横幅文本会显示在对话框中，并提供继续或断开连接的选项。“继续”选项将删除横幅并照常完成登录，而“断开连接”选项将删除横幅并终止连接。此增强功能需要客户接受书面策略条款，才能进行连接。 下面是与此增强相关的新 CLI： **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** 在 ASDM 中，请参阅**配置 > 属性 > 设备管理 > 横幅**。 同样适用于版本 *7.2(3)*。
ASDM 中的本地化增强功能	ASDM 现在已得到增强，可以支持 AnyConnect 本地化。请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > AnyConnect 自定义**，或**配置 > 远程访问 > 网络访问 > AnyConnect 自定义和配置 > 远程访问 > 访问语言本地化 >“MST 转换”面板**。
基于时间的许可证增强功能	在主页上，“设备控制面板”选项卡上的“许可证”选项卡现在包括一个基于时间的许可证到期前的天数（如果适用）。

功能	说明
网络对象	现在，您可以添加可在防火墙规则中使用的真实网络对象。您可以为对象命名，并且当您编辑对象时，无论从何处使用该对象，更改都会从此处继承下来。此外，当您创建规则时，您在规则中指定的网络将自动添加到网络对象列表中，以便您可以在其他地方重新使用它们。您也可以命名和编辑这些自动条目。请参阅**配置 > 防火墙 > 对象 > 网络对象/组**。
客户端软件位置增强功能	“客户端软件位置”列表中添加了支持项目，允许从 Linux 或 Mac 系统更新客户端。请参阅**配置 > 远程访问 VPN > 语言本地化**。 同样适用于版本 *7.2(3)*。
CSC 事件和统计报告增强功能	通过思科内容安全和控制 (CSC) 6.2 软件，ASDM 可提供新损害清理服务 (DCS) 功能的事件和统计信息。DCS 将从客户端和服务器中删除恶意软件，并修复系统注册表和内存。

ASA 8.0(2)/ASDM 6.0(2) 的新功能

发布日期：2007 年 6 月 18 日

注释 没有 8.0(1)/6.0(1) 版本。

功能	说明
路由功能	
EIGRP 路由	ASA 支持 EIGRP 或 EIGRP 末节路由。
高可用性功能	
在故障切换对中远程执行命令	在故障切换对中，您可以在对等设备上执行命令，而无需直接连接至对等设备。此功能适用于主用/备用故障切换和主用/主用故障切换。
支持 CSM 配置回滚	故障切换配置中增加了对思科安全管理器配置回滚功能的支持。
故障切换对自动更新支持	您可以使用自动更新服务器更新故障切换对中的平台映像和配置。

功能	说明
SIP 信令的状态故障切换	SIP 媒体和信令连接将会复制到备用设备。
冗余接口	逻辑冗余接口将一个主用接口和一个备用物理接口进行配对。当主用接口发生故障时，备用接口将变为主用接口并开始传递流量。您可以配置冗余接口来提高 ASA 的可靠性。此功能独立于设备级故障切换，但如果需要，您可以配置冗余接口以及故障切换。您最多可以配置 8 个冗余接口对。
模块功能	
AIP SSM 运行虚拟 IPS 传感器	运行 IPS 软件版本 6.0 及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以将每个情景或单模式自适应安全设备分配给一个或多个虚拟传感器，也可以将多个安全情景分配给同一个虚拟传感器。请参阅 IPS 文档，了解有关虚拟传感器的详细信息，包括受支持的传感器最大数量。
密码重设	您可以在 SSM 硬件模块上重设密码。
VPN 身份验证功能脚注。	
同时使用证书和用户名/密码登录	管理员要想登录 SSL VPN 连接，除了证书，还需要用户名和密码。
内部域用户名/密码	此版本可为使用域用户名和密码以外的方式登录的用户提供用于访问内部资源的密码（例如一次性密码）。此密码不同于用户登录时输入的密码。
一般 LDAP 支持	此版本包括 OpenLDAP 和 Novell LDAP 支持，从而对可用于身份验证和授权的 LDAP 支持进行了扩展。
屏幕键盘	ASA 提供了一个屏幕键盘选项，可用于在登录页面中输入所需信息，并完成后续的内部资源身份验证请求。此功能需要用户使用鼠标点击屏幕键盘上的字符进行身份验证，而不是在物理键盘上输入字符，所以可针对基于软件的按键记录器提供额外的防护。

功能	说明
使用 RSA 访问管理器验证 SAML SSO	ASA 支持安全断言标记语言 (SAML) 协议，从而能够实现基于 RSA 访问管理器（Cleartrust 和联合身份管理器）的单点登录 (SSO)。
NTLMv2	版本 8.0(2) 中增加了对基于 Windows 的客户端进行 NTLMv2 身份验证的支持。
证书功能	
本地证书颁发机构	ASA 上提供了一个证书颁发机构，可用于 SSL VPN 连接（基于浏览器和基于客户端）。
OCSP CRL	此版本针对 SSL VPN 提供 OCSP 撤销检查。
思科安全桌面功能	
主机扫描	作为建立思科 AnyConnect 或无客户端 SSL VPN 连接的一个条件，远程计算机会对一系列规模大幅扩展的防病毒软件和反间谍软件应用、防火墙、操作系统以及相关更新进行扫描。它还会扫描您指定的所有注册表项、文件名和进程名称，它会将扫描结果发送至 ASA。ASA 使用用户登录凭证和计算机扫描结果来指定动态访问策略 (DAP)。 借助高级终端评估许可证，您可以进行相关配置，以尝试对不合规计算机进行更新（使其符合版本要求），从而增强主机扫描。 思科可通过独立于思科安全桌面的软件包，对主机扫描所支持的应用和版本的列表进行及时更新。
简化的预登录评估和定期检查	现在，思科安全桌面简化了要在远程 Microsoft Windows 计算机上执行的预登录和定期检查配置。通过思科安全桌面，您可以使用简化的图形化检查视图在终端检查标准中添加、修改、删除和放置条件。在使用此图形化视图配置检查顺序、将检查顺序链接到分支机构、拒绝登录，以及分配终端配置文件时，思科安全桌面管理器会将相关更改记录到一个 XML 文件中。您可以将 ASA 配置为将返回的结果与许多其他类型的数据（如连接类型和多个组设置）结合使用，以生成 DAP 并将其应用于会话。
VPN 访问策略功能	

功能	说明
动态访问策略 (DAP)	VPN 网关在动态环境下运行。许多可变因素都可能会影响各个 VPN 连接，例如，频繁更改内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。 利用 ASA 上的动态访问策略 (DAP)，您可以配置兼顾上述众多可变因素的授权方法。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。换言之，ASA 会根据您定义的策略，为特定用户授予特定会话的访问权限。它会在用户进行连接时，通过从一个或多个 DAP 记录选择和/或汇聚属性来生成 DAP。它会根据远程设备的终端安全信息，以及经过身份验证的用户的 AAA 授权信息，选择这些 DAP 记录。然后它会将 DAP 记录应用至用户隧道或会话。
管理员差异化	此功能允许您在同一数据库（RADIUS 或 LDAP）中区分常规远程访问用户和管理用户。您可以通过多种方法（例如 TELNET 和 SSH）来实现控制台访问，并限制为只有管理员可以进行此访问。此功能基于 IETF RADIUS 服务类型属性。
平台增强	
针对远程访问 VPN 连接提供 VLAN 支持	此版本支持在组或用户级别进行客户端流量映射（标记）。此功能与无客户端以及基于 IPSec 和 SSL 隧道的连接兼容。
面向 ASA 5510 的 VPN 负载均衡	此版本将负载均衡的支持范围扩展到具有增强型安全许可证的 ASA 5510 自适应安全设备。
加密条件调试	利用此功能，用户可以根据预定义的加密条件（如对等 IP 地址、加密引擎的连接 ID 和安全参数索引 [SPI]）来调试 IPSec 隧道。通过将调试消息限制到特定的 IPSec 操作并减少调试输出量，有助于更好地对具有大量隧道的 ASA 进行故障排除。
基于浏览器的 SSL VPN 功能	
增强的门户设计	版本 8.0(2) 的终端用户界面得到了增强，其外观更整洁、更有序、更直观。

功能	说明
可以定制	支持对所有用户可见的内容进行管理员定义的定制。
支持 FTP	除了使用 CIFS（基于 Windows），您还可以通过 FTP 实现文件访问。
插件小应用程序	版本 8.0(2) 中添加了一个框架，使用户无需预安装客户端应用，即可支持基于 TCP 的应用。用户可以从支持浏览器的 SSL VPN 门户访问各种 Java 小应用程序。此功能目前支持 TELNET、SSH、RDP 和 VNC。
智能隧道	智能隧道是应用与远程站点之间的连接，它使用与 ASA 建立的基于浏览器的 SSL VPN 会话作为通道。在版本 8.0(2) 中，您可以指定要向其授予智能隧道访问权限的应用、应用所使用的路径，以及授予访问权限之前需要执行的校验和检查的 SHA-1 散列算法。例如，您可以为 Lotus SameTime 和 Microsoft Outlook Express 等应用授予智能隧道访问权限。 源自智能隧道连接的远程主机必须运行 Microsoft Windows Vista、Windows XP 或 Windows 2000，并且浏览器必须使用 Java 和/或 Microsoft ActiveX 启用。
RSS 新闻馈送	管理员可以在无客户端门户中填入 RSS 新闻馈送信息，这样，公司新闻或其他信息即可显示在用户屏幕上。
支持使用个人书签	用户可以定义自己的书签。这些书签存储在文件服务器上。
转变	此功能通过无客户端连接增加了对多种复杂类型的网络内容的支持，包括 Adobe Flash 和 Java WebStart。
IPv6	允许通过公共 IPv4 连接访问 IPv6 资源。

功能	说明
Web 文件夹	通过此功能，基于浏览器且从 Windows 操作系统进行连接的 SSL VPN 用户可以浏览共享文件系统，并可以执行以下操作：查看文件夹、查看文件夹和文件属性、创建、移动、复制（从本地主机复制到远程主机、从远程主机复制到本地主机）和删除。Internet Explorer 会指明 Web 文件夹何时可以访问。访问此文件夹会启动另一个窗口，此时会出现一个共享文件夹视图，用户可以从中执行 Web 文件夹功能，不过前提是文件夹和文档的属性允许他们这样做。
Microsoft Sharepoint 增强功能	此功能扩展了对 Microsoft Sharepoint 的 Web 访问支持，从而将计算机上可用的 Microsoft Office 应用与浏览器集成，以查看、更改和保存服务器上共享的文档。版本 8.0(2) 支持在 Windows Server 2003 中使用 Windows Sharepoint Services 2.0。
HTTP/HTTPS 代理功能	
支持 PAC	此功能允许您指定要下载到浏览器的代理自动配置文件 (PAC) 的 URL。下载后，该 PAC 文件将使用 JavaScript 功能标识每个 URL 的代理。
代理排除列表	此功能允许您配置要从 ASA 可发送到外部代理服务器的 HTTP 请求中排除的 URL 列表。
VPN 网络访问控制功能	
支持 SSL VPN 隧道	ASA 可为建立 AnyConnect VPN 客户端会话的终端提供 NAC 安全评估验证。
支持审核服务	您可以将 ASA 配置为在客户端对安全评估验证请求无响应时将客户端的 IP 地址传送到可选的审核服务器。审核服务器会使用主机 IP 地址直接质询主机，以评估其运行状况。例如，它可能会质询主机来确定主机的病毒检查软件是否处于活动和最新状态。审核服务器完成与远程主机后的交互后，会向安全状态验证服务器传送标记，表明远程主机的运行状况。如果标记指明远程主机运行状态良好，那么安全评估验证服务器会向 ASA 发送网络访问策略，以将其应用于隧道中的流量。
应用检测功能	

功能	说明
模块化策略框架检查类映射	现在，流量可以仅匹配检查类映射中多个匹配命令中的一个；而在以前，流量必须与类映射中的所有匹配命令都匹配才能匹配该类映射。
支持为加密流和 AIC Arch 更改应用 AIC 检查	提供对 TLS 的 HTTP 检查，从而允许在 WebVPN HTTP 和 HTTPS 流中进行 AIC/MPF 检查。
为 SCCP 和 SIP 应用 TLS 代理脚注。	此功能支持对加密流量进行检查。实施包括 SSL 加密 VoIP 信令（即瘦客户端和 SIP）以及与思科 CallManager 的交互。
适用于 CCM 的 SIP 增强功能	此功能在信令针孔方面改进了与 CCM 5.0 和 6.x 之间的互操作性。
SIP 支持 IPv6	SIP 检查引擎支持 IPv6 地址。IPv6 地址可以在 URL、“通过标头”字段和“SDP”字段中使用。
支持全 RTSP PAT	此功能支持 TCP 数据分段重组（RTSP 上的一个可扩展解析例程），并提供可保护 RTSP 流量的安全增强功能。
访问列表功能	
改进的服务对象组	您配置的服务对象组可以包含 TCP 服务、UDP 服务、ICMP 类型的服务以及任何协议的混合内容，从而不再需要 ICMP 类型的特定对象组和协议对象组。改进的服务对象组还将指定源服务和目标服务。现在，访问列表 CLI 支持此行为。
能够重命名访问列表	允许您重命名访问列表。
实时访问列表命中次数	包括来自多个访问列表的 ACE 的命中次数。命中次数值表示流量命中特定访问规则的次数。
攻击预防功能	
此功能可为流向自适应安全设备的管理流量设置连接限制	对于 3/4 层管理类映射，您可以指定 **set connection** 命令。
威胁检测	您可以启用基本威胁检测和扫描威胁检测，以监控 DoS 攻击和扫描攻击等攻击。对于扫描攻击，您可以自动避开攻击主机。您还可以启用扫描威胁统计信息，以监控主机、端口、协议和访问列表的有效和无效流量。
NAT 功能	

功能	说明
支持透明防火墙 NAT	您可以为透明防火墙配置 NAT。
监控功能	
安全日志记录	您可以使用采用 TCP 的 SSL 或 TLS 以及加密的系统日志消息内容，启用到日志服务器的安全连接。PIX 系列自适应安全设备不支持此功能。
ASDM 功能	
重新设计的界面	此界面对信息进行了重整，为您的导航提供更大的逻辑一致性和简易性。
扩展的屏幕帮助	ASDM 可以介绍屏幕上的功能和配置选项，从而减少了咨询其他信息源的需要。
可视化策略编辑器	管理员可通过可视化策略编辑器配置访问控制策略和安全评估检查。
防火墙控制面板	现在，您可以从主页上通过监控超出速率限制的流量以及通过主机、访问列表、端口或协议允许和丢弃的流量来跟踪对网络的威胁。
无障碍功能	此功能增加了对键盘导航、图形替换文本以及改进的屏幕阅读器等功能的支持。
支持进行复杂的配置	您无需应用更改即可在窗格之间移动，从而可以先输入多窗格配置，然后再将此配置应用于设备。
设备列表	ASDM 维护了一个最近访问的设备的列表，允许您在设备和上下文之间切换。
SSL VPN 配置向导	新的 SSL VPN 配置向导就如何配置基本的 SSL VPN 连接提供了逐步指导。
启动向导增强功能	现在，您可以通过启动向导配置自适应 ASA，以将流量传递至已安装的 CSC SSM。
ASDM 助手增强功能	增加了一个配置安全语音的助手。
数据包捕获向导	数据包捕获向导可帮助您以 PCAP 格式获取和下载嗅探器跟踪。
服务策略规则向导	该向导经过更新后支持 IPS 虚拟化。
证书管理增强功能	证书管理 GUI 已经过重整和简化。

[2] (1) 无客户端 SSL VPN 功能在 PIX 安全设备上不受支持。
[3] (2) TLS 代理功能在 PIX 安全设备上不受支持。

版本 7.2 的新功能

ASA 7.2(5)/ASDM 5.2(5) 的新功能

发布日期：**2010** 年 **5** 月 **11** 日

ASA 7.2(5)/ASDM 5.2(5) 中无新增功能

ASA 7.2(4)/ASDM 5.2(4) 的新功能

发布日期：**2008** 年 **4** 月 **7** 日

功能	说明
远程访问功能	
本地地址池编辑	您可以编辑地址池，而不会影响所需的连接。如果不从池中删除正在使用的地址，则连接不受影响。不过，如果要从池中删除正在使用的地址，连接则会断开。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
路由功能	

功能	说明
IPv6 组播侦听程序发现协议 v2 支持	ASA 现在支持组播侦听程序发现协议 (MLD) 版本 2，以发现组播地址侦听程序在其直接连接的链路上的在线状态，并具体发现哪些组播地址与相邻节点相关。ASA 将成为组播地址侦听程序或主机（但不是组播路由器），并只响应组播侦听程序查询且仅发送组播侦听程序报告。 以下命令支持此功能： • **clear ipv6 mld traffic** clear ipv6 mld traffic 命令使您可以重置所有组播侦听程序发现流量计数器。 • **show ipv6 mld traffic** show ipv6 mld 命令使您可以显示所有组播侦听程序发现流量计数器。 • **debug ipv6 mld** 对 debug ipv6 命令的增强，使用户可以显示 MLD 的调试消息，以查看 MLD 协议活动是否正常工作。 • **show debug ipv6 mld** 对 show debug ipv6 命令的增强，使用户可以显示是启用还是禁用 debug ipv6 mld。 同样适用于版本 *8.0(4)*。
平台功能	
ASA 5505 中继端口上的本地 VLAN 支持	现在，您可以在中继端口上允许本地 VLAN（请参阅 **switchport trunk native vlan** 命令）。 在 ASDM 中，请参阅**配置 > 设备安装 > 接口 > 交换机端口 > 编辑**对话框。 同样适用于版本 *8.0(4)*。
连接功能	
clear conn 命令	添加了 **clear conn** 命令，以删除连接。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。

功能	说明
完全重组数据分段	通过 **reassembly full** 关键字增强了 **fragment** 命令，支持完全重组通过设备传输的数据分段。在设备处终止的数据分段始终会完全重组。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
QoS 流量整形	如果您有高速传输数据包的设备，例如使用快速以太网的ASA，但它连接到低速设备，例如电缆调制解调器，则电缆调制解调器是导致数据包被频繁丢弃的瓶颈。要管理具有不同线路速率的网络，可将安全设备配置为以较慢的固定速率传输数据包。请参阅 **shape** 命令。另请参阅 **crypto ipsec security-association replay** 命令，该命令允许您配置 IPSec 防重放窗口大小。 优先级排队的一个负面影响是数据包重新排序。对于 IPSec 数据包，未处于防重放窗口内的错序数据包，会生成警告系统日志消息。在进行优先级排队的情况下，这些警告会变成错误警报。此新功能可避免潜在的错误警报。 在 ASDM 中，请参阅**配置 > 防火墙 > 安全策略 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > QoS**。请注意，唯一支持流量整形的流量类为 class-default，该类与所有流量匹配。 同样适用于版本 *8.0(4)*。
防火墙功能	

功能	说明
TCP 规范化增强	现在，您可以为特定数据包类型配置TCP规范化操作。以前，针对这种数据包的默认操作是丢弃数据包。现在，您可以设置TCP规范器来允许数据包。 • TCP 无效 ACK 检查（**invalid-ack** 命令） • TCP 数据包序列通过窗口检查（**seq-past-window** 命令） • TCP SYN-ACK 及数据检查（**synack-data** 命令） 另外，您还可以设置TCP错序数据包缓冲区超时（**queue** 命令 **timeout** 关键字）。以前，该超时值为 4 秒。现在，您可以将超时设置为其他值。 针对超出 MSS 的数据包的默认操作从“丢弃”改为“允许”（**exceed-mss** 命令）。 对于这些数据包类型，以下不可配置的操作从“丢弃”改成了“清除”： • TCP 中的选项长度错误 • 非 SYN 上的 TCP 窗口扩展 • TCP 窗口扩展值错误 • TCP SACK ALLOW 选项错误 在 ASDM 中，请参阅**配置 > 全局对象 > TCP 映射**窗格。 同样适用于版本 *8.0(4)*。
SIP 临时媒体超时	现在，您可以使用 **timeout sip-provisional-media** 命令来配置 SIP 临时媒体的超时时间。 在 ASDM 中，请参阅**配置 > 属性 > 超时**窗格。 同样适用于版本 *8.0(4)*。
Ethertype ACL MAC 增强	EtherType ACL 功能进行了增强，支持非标准的 MAC。现有的默认规则予以保留，但无需添加新规则。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
故障排除和监控功能	

功能	说明
capture 命令增强	**capture type asp-drop** *drop_code* 命令现在接受 **all** 作为 *drop_code*，所以您现在可以捕获 ASA 丢弃的所有数据包，包括由于安全检查而丢弃的数据包。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
MIB 增强	更加全面地实施 CISCO-REMOTE-ACCESS-MONITOR-MIB。 同样适用于 *8.0(4)* 版本。
show asp drop 命令增强	输出现在包括指示计数器上次清除时间的时间戳（请参阅 **clear asp drop** 命令）。输出还会在说明旁边显示丢弃原因关键字，以便您能够轻松使用具有该关键字的 **capture asp-drop** 命令。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
clear asp table 命令	添加了 **clear asp table** 命令以清除 **show asp table** 命令的命中次数输出。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
show asp table classify hits 命令增强	将 hits 选项添加到 **show asp table classify** 命令，用于显示指示上次何时清除 asp 表计数器的时间戳。该命令还会显示符合值不等于零的规则。借此，用户可以快速查看符合哪些规则，特别是 **show asp table classify** 命令中一个简单配置以数百个条目结尾的情况。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
show perfmon 命令	添加了以下速率输出：已建立 TCP 拦截连接、TCP 拦截尝试、TCP 初期连接超时和 TCP 拦截中的有效连接速率。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。

功能	说明
memory tracking 命令	此版本中引入了以下新命令： • **memory tracking enable** - 此命令支持跟踪堆内存请求。 • **no memory tracking enable** - 此命令禁止跟踪堆内存请求、清理当前收集的所有信息，并向系统返回工具本身使用的所有堆内存。 • **clear memory tracking** - 此命令会清除当前收集的所有信息，但会继续跟踪进一步的内存请求。 • **show memory tracking** - 此命令显示当前工具所跟踪的已分配内存，它们按最上方的调用方函数地址进行细分。 • **show memory tracking address** - 此命令显示当前按每一块内存细分的已分配内存。输出会列出当前工具跟踪的每个已分配内存块的大小、位置以及最上方的调用方函数。 • **show memory tracking dump** - 此命令显示指定内存地址的大小、位置、部分调用栈和内存转储。 • **show memory tracking detail** - 此命令显示探查工具内部行为时要使用的各种内部详细信息。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
故障切换功能	
failover timeout 命令	**failover timeout** 命令用于静态指定功能时，不再需要故障切换许可证。 同样适用于版本 *7.0(8)* 和 *8.0(4)*。
ASDM 功能	

功能	说明
网络对象	现在，您可以添加可在防火墙规则中使用的真实网络对象。您可以为对象命名，并且当您编辑对象时，无论从何处使用该对象，更改都会从此处继承下来。此外，当您创建规则时，您在规则中指定的网络将自动添加到网络对象列表中，以便您可以在其他地方重新使用它们。您也可以命名和编辑这些自动添加的条目。请参阅“配置”>“对象”>“网络对象/组”。
增强的 ASDM 规则表	ASDM规则表已经过重新设计，以简化策略创建过程。

ASA 7.2(3)/ASDM 5.2(3) 的新功能

发布日期：**2007** 年 **8** 月 **15** 日

功能	说明
远程访问功能	
WebVPN 负载均衡	自适应安全设备现在支持使用FQDN执行负载均衡。要使用 FQDN 执行 WebVPN 负载均衡，必须启用使用 FQDN 执行负载均衡，请输入 **redirect-fqdn enable** 命令。然后，对于每个自适应安全设备外部接口向 DNS 服务器中添加一个条目（如果尚不存在）。每个自适应安全设备外部 IP 地址都应该有一个与其关联的 DNS 条目用于查找。对于反向查找，也必须启用这些 DNS 条目。使用 **dns domain-lookup inside** 命令（或具有通向 DNS 服务器的路由的任一接口）在自适应安全设备上启用 DNS 查找。最后，必须在您的自适应安全设备上定义DNS服务器的IP地址。下面是与此增强相关的新 CLI：**redirect-fqdn** {**enable** | **disable**}。 在 ASDM 中，请参阅**配置 > VPN > 负载均衡**。 同样适用于版本 *8.0(3)*。

功能	说明

无客户端 SSL VPN 缓存静态内容增强	无客户端 SSL VPN 缓存命令有两项变动：
	Cache-compressed 命令被启用。
	新的 **cache-static-content** 命令将 ASA 配置为缓存所有静态内容，这意味着所有可缓存的 Web 对象都不受 SSL VPN 重写的干扰。其中包括映像和 PDF 文件等内容。
	该命令的语法是 **cache-static-content** {**enable** | **disable**}。默认情况下，禁用静态内容缓存。
	示例：
	`hostname (config) # webvpn`
	`hostname (config-webvpn) # cache`
	`hostname (config-webvpn-cache) #`
	`cache-static-content enable`
	hostname (config-webvpn-cache) #
	在 ASDM 中，请参阅**配置 > 远程访问 VPN > 无客户端 SSL VPN 访问 > 高级 > 内容缓存**。
	同样适用于版本 *8.0(3)*。

移除智能卡时断开连接	此功能使中心站点管理员可配置远程客户端策略，以便在移除智能卡时删除活动隧道。默认情况下，当用户移除用于身份验证的智能卡时，思科 VPN 远程访问软件客户端（IPSec 和 SSL）会清除现有的 VPN 隧道。以下 cli 命令在移除智能卡时会断开现有的 VPN 隧道：**smartcard-removal-disconnect** {**enable** | **disable**}。默认情况下，此选项已启用。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑内部/外部组策略 > 更多选项**。 同样适用于版本 *8.0(3)*。
平台功能	

功能	说明
ASA 5510 增强型安全许可证对于端口 0 和 1 支持千兆以太网	ASA 5510 ASA 现在配备增强型安全许可证，对于端口 0 和 1 支持 GE（千兆以太网）。如果从基础许可证升级至增强型安全许可证，则外部端口 Ethernet0/0 和 Ethernet0/1 的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令可更改接口上的速度，使用 show interface 命令可查看为每个接口当前配置的速度。 同样适用于版本 *8.0(3)*。
ASA 5505 扩大了 VLAN 范围	ASA 5505 ASA 现在支持介于 1 到 4090 之间的 VLAN ID。最初仅支持介于 1 到 1001 之间的 VLAN ID。 同样适用于版本 *8.0(3)*。
故障排除功能	
Capture 命令增强	对 **capture** 命令的增强允许用户实时捕获和显示流量。此外，该命令还允许用户指定过滤流量的命令行选项，而不必配置单独的访问列表。此增强功能添加了 **real-time** 和 five-tupple **match** 选项。 **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] 同样适用于版本 *8.0(3)*。
应用检测功能	

功能	说明

支持基于 TLS 的 ESMTP	此增强功能在 esmtp 策略映射中添加了配置参数 **allow-tls** [**action log**]。默认情况下，不启用此参数。启用此功能后，ESMTP 检查不会将来自服务器的 250-STARTTLS 回应和来自客户端的 **STARTTLS** 命令屏蔽。在服务器回应 220 个应答代码后，ESMTP 检测会自行关闭；不再检测该会话中的 ESMTP 流量。如果已配置 **allow-tls action log** 参数，则在 ESMTP 会话中启动 TLS 时会生成系统日志消息 ASA-6-108007。
	
	`policy-map type inspect esmtp esmtp_map parameters`
	
	`allow-tls [action log]`
	
	用于显示与 **allow-tls** 参数关联的计数器的新行已添加到 **show service-policy inspect esmtp** 命令中。仅在策略映射中已配置 **allow-tls** 时才会显示该行。默认情况下，不启用此参数。
	
	`show service-policy inspect esmtp`
	`allow-tls, count 0, log 0`
	
	此增强功能会为 **allow-tls** 参数添加一条新的系统日志消息。它在 esmtp 会话中指示服务器已使用 220 应答代码响应客户端 **STARTTLS** 命令。ESMTP 检测引擎不再检测此连接中的流量。
	
	系统日志编号和格式：
	
	%ASA-6-108007：TLS 在客户端 *<client-side interface-name>:<client IP address>/<client port>* 与服务器 *<server-side interface-name>:<server IP address>/<server port>* 之间的 ESMTP 会话上启动
	
	在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > 检测映射 > ESMTP**。
	
	同样适用于版本 *8.0(3)*。

DNS Guard 增强	添加了启用或禁用 DNS Guard 的选项。启用时，此功能仅允许 DNS 请求返回一个 DNS 响应。 在 ASDM 中，请参阅**配置 > 防火墙 > 对象 > 检测映射 > DNS**。 同样适用于版本 *8.0(3)*。

功能	说明
WAAS 和 ASA 互操作性	添加了 **inspect waas** 命令，以在策略映射类配置模式下启用 WAAS 检查。此 CLI 集成在模块化策略框架内，以便最大限度地灵活配置功能。可以在默认的检查类和自定义类映射下配置 **[no] inspect waas** 命令。默认情况下，此检测服务未启用。 **show service-policy inspect** 命令中添加了关键字选项 waas，以显示 WAAS 统计信息。 `show service-policy inspect waas` 在连接中检测到 WAAS 优化时，生成一条新的系统日志消息。在 WAAS 优化的连接中绕过包括 IPS 在内的所有 L7 检测服务。 系统日志编号和格式： %ASA-6-428001：从 in_interface:src_ip_addr/src_port 向 out_interface:dest_ip_addr/dest_port 确认的 WAAS，在此连接中绕过检测服务。 WAAS 连接中添加了新的连接标记“W”。show conn detail 命令已更新以反映新的标志。 在 ASDM 中，请参阅**配置 > 防火墙 > 服务策略规则 > 添加/编辑服务策略规则 > 规则操作 > 协议检测**。 同样适用于版本 *8.0(3)*。
DHCP 功能	
DHCP 客户端 ID 增强	如果使用 **ip address dhcp** 命令对接口启用 DHCP 客户端，某些 ISP 会将选项 61 作为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。使用此新命令可包含选项 61 的接口 MAC 地址。如果未配置此命令，客户端 ID 则如下所示： cisco-<MAC>-<interface>-<hostname>。 引入了以下命令：**dhcp-client client-id interface** *interface_name* 修改了以下菜单项：**配置 > 设备管理 > DHCP > DHCP 服务器**；然后点击**高级**。 同样适用于版本 *8.0(3)*。

功能	说明
模块功能	
添加了数据平面保持连接机制	现在，您可以配置 ASA 以免在升级 AIP SSM 时发生故障切换。在以前版本中，如果在故障切换中配置两个具备 AIP SSM 的 ASA，在更新 AIP SSM 软件时，ASA 就会触发故障切换，因为 AIP SSM 需要重新引导或重启，才会使软件更新生效。 同样适用于版本 *7.0(7)* 和 *8.0(3)*
ASDM 功能	
ASDM 横幅增强	自适应安全设备软件支持 ASDM 横幅。如果已配置横幅，在启动 ASDM 时，横幅文本会显示在对话框中，并提供继续或断开连接的选项。“继续”选项将删除横幅并照常完成登录，而“断开连接”选项将删除横幅并终止连接。此增强功能需要客户接受书面策略条款，才能进行连接。 下面是与此增强相关的新 CLI： **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** 在 ASDM 中，请参阅**配置 > 属性 > 设备管理 > 横幅**。 同样适用于版本 *8.0(3)*。
思科内容安全和控制 (CSC) 损害清理服务 (DCS) 功能事件和统计信息	通过思科内容安全和控制 (CSC) 6.2 软件，ASDM 可提供新损害清理服务 (DCS) 功能的事件和统计信息。DCS 将从客户端和服务器中删除恶意软件，并修复系统注册表和内存。
客户端软件位置	“客户端软件位置”列表中添加了支持项目，允许从 Linux 或 Mac 系统更新客户端。 在 ASDM 中，请参阅**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPSec > 上传软件 > 客户端软件**。 同样适用于版本 *8.0(3)*。

ASA 7.2(2)/ASDM 5.2(2) 的新功能

发布日期：**2006** 年 **11** 月 **22** 日

功能	说明
模块功能	
在 SSM 上重置密码	您可以在用户的 AIP-SSM 和 CSC-SSM 上将用户“cisco”重置为默认值“cisco”。 添加了以下命令：**hw-module module password-reset**。
AAA 功能	

功能	说明
HTTP(S) 身份验证挑战灵活的配置	新的 **aaa authentication listener** 命令支持 ASA 对网页进行身份验证，并选择版本 7.2(1) 中当前使用的基于表单的重定向方法。 7.2(2) 重新引入在 7.2(1) 之前提供的基本 HTTP 身份验证的选择。基本 HTTP 和 HTTPS 身份验证会生成自定义登录窗口。在以下情况下，您可以使用基本的 HTTP 身份验证： • 您不希望自适应安全设备打开侦听端口 • 您在路由器上使用NAT，但不希望为自适应安全设备提供的网页创建转换规则 • 基本 HTTP 身份验证可以更好地适应您的网络。例如，非浏览器应用（例如，当将URL嵌入到邮件中时）可能更适合基本身份验证。 **注释** 默认情况下，**aaa authentication listener** 命令在配置中是不存在的，从而使版本 7.1 aaa 的行为就是 7.2(2) 的默认行为。但如果将版本 7.2(1) 配置升级到版本 7.2(2)，则系统会将相应的 **aaa authentication listener** 命令添加到配置中，以便升级后不会更改 **aaa** 行为。 为了支持基本 HTTP，系统恢复了 **virtual http** 命令。当您具有级联身份验证请求时，需要使用基本身份验证方法。 在版本 7.2(1) 中，基本身份验证将被基于表单的身份验证方法所取代，在基于表单的方法中，HTTP 和 HTTPS 连接被重定向到从 ASA 提供的身份验证页面。成功进行身份验证后，浏览器再次重定向到原计划要达到的URL。这样做是为了提供： • 更好地支持身份验证挑战处理 • 适用于 http 和 https 用户的相同身份验证体验 适用于网络用户的持久登录/注销 URL 此方法确实要求在启用了 **aaa authentication** 的每个接口上的 ASA 上打开侦听端口。

功能	说明
接口功能	
增加了 VLAN 的最大数量	ASA 5505 自适应安全设备上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障切换；1 个限用于备用接口）增加到 20 个全功能接口。此外，中继端口数量也从 1 增加到 8。现在有 20 个全功能接口，您不需要使用 **backup interface** 命令禁用备用 ISP 接口的功能；您可以为其使用全功能接口。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有所增加：ASA 5510 自适应安全设备（对于基础许可证，从 10 增加到 50；对于增强型安全许可证，从 25 增加到 100）、ASA 5520 自适应安全设备（从 100 增加到 150）和 ASA 5550 自适应安全设备（从 200 增加到 250）。
增加了 ASA 5510 基础许可证上的物理接口数	在 ASA 5510 中，可用的物理接口的最大数量已从 3+1 更改为无限制 (5)。
认证功能	
FIPS 140-2	7.2(2) 已提交进行 FIPS 140 级 2 验证。
ASDM 功能	
组播支持	添加了对以下多播命令的支持： • **mfib forwarding** • **multicast boundary** • **pim bidir-neighbor-filter** • **pim neighbor-filter** • **pim old-register-checksum**
本地演示模式	ASDM 在本地演示模式下连接到设备时有效。

ASA 7.2(1)/ASDM 5.2(1) 的新功能

发布日期：**2006** 年 **5** 月 **31** 日

功能	说明
平台功能	
ASA 5505 支持	此版本中引入了对 ASA 5505 的支持。ASA 5505 是一款适合小型办公室/家庭办公室、企业远程工作环境的新型设备，包括一个内置 8 端口快速以太网交换机，支持 Easy VPN、双 ISP，并具有许多其他功能 ASA 5505 具有以太网供电 (PoE) 交换机端口，可用于 IP 电话等 PoE 设备。但这些端口的用途不限于此。它们也可以用作以太网交换机端口。如果没有连接 PoE 设备，则不会向端口供电。
ASA 5550 支持	ASA 5550 在可靠的 1RU 外型中提供千兆位级安全服务，并可实现适合大型企业和运营商网络的主用/主用高可用性。ASA 5550 通过以太网接口和基于光纤的接口形式提供千兆位连接以及高密度VLAN集成，使企业能够将其网络细分为许多高性能区域，从而提高安全性。
Easy VPN 功能（仅限 ASA 5505）	
客户端模式（也称为“端口地址转换”）和网络扩展模式	• 客户端模式 - 隐藏 ASA 5505 专用网络上的设备 IP 地址，以使来自 ASA 5505 专用网络的所有流量都会到达具有指定单源IP地址的中心站点ASA的专用网络。从中心站点无法ping通或访问ASA 5505专用网络上的设备，但可以访问分配的 IP 地址。 • 网络扩展模式 (NEM) - 仅允许 ASA 所连接的设备通过隧道直接访问 ASA 5505 专用网络上的设备。您可以从中心站点ping通或访问 ASA 5505 网络上的设备。 ASA 5505 没有默认模式；您必须指定要使用的模式。
自动隧道启动	支持NEM，但不支持客户端模式。该功能使用配置中存储的组名、用户名和密码来启动隧道。

功能	说明
互联网密钥交换 (IKE) 和 IPSec 支持	ASA 5505 支持预共享的密钥和证书 (RSA-SIG)。ASA 对于预共享密钥使用 IKE 积极模式，对基于 RSA-SIG 的密钥交换使用 IKE 主模式。思科 ASA 5505 可以启动 IPSec 会话、基于 NAT-T 的 IPSec 会话和基于 cTCP 的 IPSec 会话。
安全设备身份验证 (SUA)	支持使用动态生成的身份验证凭证或隧道启动时输入的静态凭证执行 ASA 5505 身份验证。当 SUA 启用时，用户必须使用浏览器或交互式 CLI 手动触发 IKE 隧道。
个别用户身份验证 (IUA)	支持对内部网络上的单个客户端执行静态的一次性密码身份验证。IUA 和 SUA 相互独立，它们可以一起使用，也可以单独使用。
基于令牌的身份验证	支持安全动态 (SDI) SecurID 一次性密码。
通过 HTTP 重定向进行身份验证	如果未配置 SUA 或用户名和密码或者 IUA 被禁用，则将未通过身份验证的 HTTP 流量重定向到登录页面。
负载均衡	配置了双 ISP 备份的 ASA 5505 在互联网区域可用的两个以太网端口上支持基于集群的 VPN 负载均衡。负载均衡方案涉及“虚拟导向器”IP 地址，即传入客户端连接的目标。共享同一个虚拟导向器 IP 地址的服务器构成一个集群，其中有一个集群成员充当集群主设备。主设备接收发送到虚拟导向器的请求，并使用专有 IKE 通知消息将客户端重定向到集群中的最佳服务器。当前 ISAKMP 会话将会终止，并且系统会尝试与该最佳服务器建立新的会话。 如果连接到最佳服务器失败，客户端会重新连接到主服务器（使用集群的虚拟导向器 IP 地址）并重复执行负载均衡程序。如果连接到主服务器失败，客户端将回滚到下一个已配置的备份服务器（可能是另一个集群的主设备）。
故障切换（使用备份服务器列表）	除主服务器之外，您还可以配置一个包含 10 台备份服务器的列表。ASA 5505 会尝试与主服务器建立隧道。如果尝试失败，ASA 5505 将按顺序尝试与备份服务器列表中指定的其他服务器建立隧道。

功能	说明
设备直通	包括 IP 电话直通和 LEAP 直通功能。 某些设备（如打印机和思科IP电话）无法执行身份验证，因此无法参与IUA。启用设备直通功能后，ASA 5505 会在 IAU 启用时豁免相关设备的身份验证。 Easy VPN 远程功能根据配置的 MAC 地址列表标识要豁免的设备。但无线设备（例如无线接入点和无线节点）在这方面存在一个问题。这些设备需要执行 LEAP/PEAP 身份验证，才能允许无线节点参与网络。只有在完成 LEAP/PEAP 身份验证阶段后，无线节点才能执行 IUA。当设备直通功能启用时，ASA 5505 也会绕过 LEAP/PEAP 数据包，以使无线节点可以参与 IUA。
IKE 模式配置	您可以设置 ASA 5505 在完成 IKE 第 I 阶段和 XAUTH 后所需请求的属性值。中心站点上的设备会下载 VPN 策略，而 ASA 5505 会根据安全值动态配置功能。除SUA、清除保存密码和备份集中器列表之外，动态功能配置仅在隧道正常工作时才会有效。
远程管理	支持通过以下途径管理 ASA 5505：连接至配置了 NEM 的外部接口的隧道，以及连接至外部接口的安全连接。
对 Easy VPN 对等体名称执行 DNS 解析	ASA 5505 使用 DNS 服务器解析 Easy VPN 对等体名称。您可以在 CLI 中指定服务器/客户端的 DNS 名称。
拆分隧道	允许客户端决定要通过隧道发送的流量，具体取决于通过以隧道连接至中心站点可访问的网络配置列表。如果流量所发往的网络不在拆分隧道网络列表中，则流量的发送不受阻。列表长度为零表示没有拆分隧道，所有流量均通过隧道传输。
推送横幅	您可以配置一个长度为 491 字节的横幅消息，它将以 HTTP 表单形式显示给尝试使用 IUA 进行身份验证的单个用户。
应用检测功能	

功能	说明
增强的 ESMTP 检测功能	此功能可用于检测各种攻击，包括垃圾邮件、网络钓鱼、畸形消息攻击和缓冲区溢出/下溢攻击。这项检测还支持应用安全和协议符合性检查（即对 ESMTP 消息执行健全性检查），检测若干种攻击，阻止发件人/收件人，以及阻止邮件转发。
DCERPC 检测	此功能让您可以通过 DCERPC 检测映射来更改用于 DCERPC 应用检测的默认配置值。 DCERPC 是 Microsoft 分布式客户端和服务器应用采用的一种协议，允许软件客户端在服务器远程执行程序。 通常，客户端会查询名为终端映射器 (EPM) 的服务器（用于侦听已知端口号，以获取所需服务的动态分配网络信息），然后与提供服务的服务器实例建立辅助连接。安全设备允许相应的端口号以及网络地址，如有必要，还会为辅助连接应用 NAT 或 PAT。
增强的 NetBIOS 检测功能	此功能让您可以更改用于 NetBIOS 应用检测的默认配置值。 NetBIOS 应用检测为 NetBIOS 名称服务数据包和 NetBIOS 数据报服务数据包中的嵌入式 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制实现协议符合性。
改进了 H.323 检测功能	此功能让您可以更改用于 H.323 应用检测的默认配置值。 H.323 检测支持 RAS、H.225 和 H.245，这项检测功能会转换所有嵌入式 IP 地址和端口。H.323 检测执行状态跟踪和过滤，并且可以激活很多检测功能。H.323 检测支持电话号码筛选、动态 T.120 控制、H.245 隧道控制、协议状态跟踪、H.323 呼叫持续时间实施和音频/视频控制。
增强的 DNS 检测功能	此功能让您可以指定当消息不符合使用 DNS 检测策略映射的参数时所需执行的操作。DNS 应用检测支持 DNS 消息控制，以防范 DNS 欺骗和缓存投毒。用户可配置的规则允许基于 DNS 报头、域名和资源记录类型和类进行过滤。

功能	说明
增强的 FTP 检测功能	此功能让您可以更改用于FTP应用检测的默认配置值。 使用严格FTP检测可进行FTP命令过滤和安全检查，从而提高安全和加强控制。协议符合性包括数据包长度检查、分隔符和数据包格式检查、命令终止符检查以及命令验证。 此功能还支持根据用户值阻止 FTP，这样一来，FTP 站点可以发布可供下载的文件，但仅允许某些用户访问。可以根据文件类型、服务器名称及其他属性阻止FTP连接。如果进行检测后FTP连接被拒绝，将会生成系统消息日志。
增强的 HTTP 检测功能	此功能让您可以更改用于 HTTP 应用检测的默认配置值。 HTTP 应用会检测扫描 HTTP 报头和正文，并对数据执行各种检查。这些检查可防止各种 HTTP 构造、内容类型、隧道协议和消息传送协议通过安全设备。 HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达 Web 服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。
增强的瘦客户端控制协议 (SCCP) 检测	此功能让您可以更改用于 SCCP（瘦客户端控制协议）应用检测的默认配置值。 瘦客户端应用检测对数据包数据中的嵌入式IP地址和端口号执行转换，并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。
增强的 SIP 检测功能	此功能让您可以更改用于 SIP 应用检测的默认配置值。 SIP 是一种广泛用于网络会议、电话、事件通知和即时消息的协议。部分原因是 SIP 本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。 SIP 应用检测会在消息报头和正文中提供地址转换，动态打开端口，以及执行基本健全性检查。它还支持应用安全和协议符合性检测（此功能强制对 SIP 消息进行健全性检查，并检测基于 SIP 的攻击）。

功能	说明
即时消息 (IM) 检测	此功能允许您更改用于即时消息 (IM) 应用检测的默认配置值。 即时消息 (IM) 应用检测提供详细的访问控制机制来控制网络使用情况。它还有助于防止机密数据泄露和网络威胁传播。此功能会执行正则表达式数据库搜索，以展示要过滤的各种即时消息 (IM) 协议。如果无法识别流，则会生成一个系统日志。 该范围可以通过使用访问列表来指定要检查的任何业务流来限制。对于 UDP 消息，也可以配置相应的 UDP 端口号。Yahoo! 检测支持 Messenger 和 MSN Messenger 即时消息。
基于 MPF 的正则表达式分类映射	此功能允许您在模块化策略框架类映射中定义正则表达式，并匹配一组具有 **match-any** 属性的正则表达式。您可以使用正则表达式类映射来匹配特定流量的内容，例如，可以匹配 HTTP 数据包内的 URL 字符串。
RADIUS 记帐检测	此功能可用于在移动记帐基础设施中防范过度记帐攻击。此版本中引入了 **policy-map type inspect radius-accounting** 命令。
H.323 的 GKRCS 支持	ITU-T H.323 建议中描述了两种控制信令方法：网守路由控制信令 (GKRCS) 和直接呼叫信令 (DCS)。思科 IOS 网守支持 DCS。此功能增加了对网守路由控制信令 (GKRCS) 控制信令方法的支持。
瘦客户端控制协议视频支持	此功能添加了对 SCCP 版本 4.1.2 消息的支持，以便在启用 **debug skinny** 时输出由检测功能处理的消息名称。此功能也支持 CCM 4.0.1 消息。
SIP IP 地址隐私	此功能允许您保留所有事务（在代理和电话之间交换的 REGISTER 事务除外）的入站 SIP 数据包中嵌入的外部 IP 地址，以隐藏电话的实际 IP 地址。系统不会对 REGISTER 消息和 REGISTER 消息的响应执行此操作，因为此消息在电话和代理之间交换。 启用此功能时，系统将保留 SIP 报头中的外部 IP 地址和入站 SIP 数据包的 SDP 数据。使用 **ip-address-privacy** 命令可启用此功能。

功能	说明
RTP/RTCP 检测	此功能可对嵌入式IP地址执行NAT，并可为RTP和 RTCP 流量打开针孔。此功能可确保仅在检测SIP、瘦客户端控制协议和H.323打开的针孔上传送 RTP 数据包。为了防止恶意应用发送 UDP 流量来利用 ASA 上创建的针孔，此功能允许您监控 RTP 和 RTCP 流量及强制验证 RTP 和 RTCP 数据包的有效性。
远程访问和站点到站点 VPN 功能	

功能	说明
网络准入控制	

功能	说明
	网络准入控制(NAC)让您可以根据对等体的状态来验证对等体。这种方法称为安全评估验证(PV)。PV包括验证对等体运行的应用是否具有最新的补丁程序，并确保远程主机上运行的防病毒文件、个人防火墙规则或入侵防护软件是最新的。 在 ASA 上配置 NAC 之前，您必须先为网络准入控制配置访问控制服务器 (ACS)。 作为 NAC 身份验证设备，ASA 执行以下操作： • 根据建立的 IPSec 会话发起初始凭证交换，并在此后定期进行交换。 • 在对等体和ACS之间转发凭证请求和响应。 • 根据 ACS 服务器的结果对 IPSec 会话执行网络访问策略。 • 基于对等操作系统支持本地异常列表（还可选择支持 ACL）。 • （可选）对于无客户端主机，从ACS服务器请求访问策略。 作为 ACS 客户端，ASA 支持以下设置： • EAP/RADIUS • NAC 所需的 RADIUS 属性 ASA 上的 NAC 与思科 IOS 第 3 层设备（如路由器）上的 NAC 不同，就后者而言，路由器根据路由流量触发 PV。启用 NAC 的 ASA 使用 IPSec VPN 会话来触发 PV。配置 NAC 的思科 IOS 路由器根据发往特定网络的流量，使用拦截ACL来触发 PV。由于外部设备无法在不启动 VPN 会话的情况下访问 ASA 后面的网络，因此 ASA 不需要使用拦截 ACL 来触发 PV。在 PV 期间，来自对等体的所有 IPSec 流量都要接受为对等体组配置的默认 ACL 检测。 与思科 VPN 3000 集中器系列不同，ASA 上的 NAC 支持无状态故障切换、在隧道组中执行所有NAC会话初始化、重新验证隧道组中的所有NAC会话，并支持为每个隧道配置的安全评估验证豁免列表。ASA 上的 NAC 不支持非 VPN 流量、IPv6、安全情景和 WebVPN。

功能	说明
	默认情况下，会禁用NAC。您可以根据组策略启用 NAC。
基于 IPSec 的 L2TP	第2层隧道协议(L2TP)是允许远程客户端使用公共 IP 网络安全地与企业专用网络服务器通信的 VPN 隧道协议。L2TP 使用 PPP over UDP（端口 1701）来通过隧道传送数据。L2TP 基于客户端/服务器模式。此功能在 L2TP 网络服务器 (LNS) 和 L2TP 访问集中器 (LAC) 之间分配。LNS 通常在网络网关（如路由器）上运行，而LAC可以是拨号网络接入服务器 (NAS) 或有一个捆绑 L2TP 客户端（如 Microsoft Windows 2000）的 PC。 L2TP/IPSec可在单一平台上提供部署和管理L2TP VPN解决方案以及IPSec VPN和防火墙服务的功能。 在远程访问场景中，使用 IPSec 配置 L2TP 的主要优势在于远程用户可以通过公共 IP 网络访问 VPN，而无需使用网关或专用线路。这就意味着可以使用 POTS 从几乎任何位置执行远程访问。该模式的另一个优势在于，VPN访问在客户端方面的唯一要求是使用带Microsoft拨号网络(DUN)的 Windows 2000，而不需要使用思科 VPN 客户端软件等任何其他客户端软件。
OCSP 支持	联机证书状态协议 (OCSP) 提供了一种替代 CRL 来获取 X.509 数字证书吊销状态的方法。OCSP 无需客户端下载整个证书吊销列表（通常非常大），它会向证书颁发机构查询特定证书的状态，从而获得证书状态。
NAT 后面的多个基于 IPSec 的 L2TP 客户端	安全设备可成功与一个或多个 NAT 设备后的多个客户端建立基于IPSec的远程访问L2TP连接。这样可增强典型 SOHO/分支机构环境基于 IPSec 的 L2TP 连接的可靠性（在典型 SOHO/分支机构环境中，多个基于 IPSec 的 L2TP 客户端必须安全地与一个中央办公室进行通信）。
Nokia 移动身份验证支持	您可以使用手持Nokia 92xx Communicator系列蜂窝设备建立 VPN 来进行远程访问。这些设备使用的身份验证协议是IKE面向已验证加密密钥的质询/响应 (CRACK) 协议。

功能	说明
Zonelabs 完整性服务器	您可以在部署 Zone Labs 完整性系统的网络中将 ASA 配置为对远程 VPN 客户端实施安全策略。在这种情况下，ASA 是 Zone Labs 完整性服务器与远程客户端之间的边缘网关。Zone Labs 完整性服务器和远程客户端上的 Zone Labs 个人防火墙确保远程客户端符合集中管理的安全策略后，该客户端才能访问专用网络资源。您可以将 ASA 配置为在服务器和客户端之间传送安全策略信息以保持或关闭客户端连接，从而防止服务器连接故障；此外，您也可以选择要求对完整性服务器和 ASA 实施 SSL 证书身份验证。
混合 XAUTH	您可以配置混合身份验证来增强 ASA 与远程用户之间的IKE安全。在使用此功能的情况下，IKE第I阶段需要完成两个步骤。首先，ASA 使用标准公共密钥技术对远程VPN用户进行身份验证，并建立一个已经过单向身份验证的 IKE 安全关联。然后，XAUTH交换对远程VPN用户进行身份验证。此扩展身份验证可以使用任一受支持的身份验证方法。混合 XAUTH 允许您使用数字证书进行 ASA 身份验证，同时使用另一种方法执行远程VPN用户验证（例如RADIUS、TACACS+或 SecurID）。
IPSec 分段和重组统计信息	您可以监控其他 IPSec 分段和重组统计信息，以帮助调试与 IPSec 相关的分段和重组问题。更新后的统计信息可提供 IPSec 处理前后的分段和重组相关信息。
WebVPN 的检测 IPS、CSC 和 URL 过滤	此功能在无客户端模式和端口转发模式下添加了对 WebVPN 流量相关检测、IPS 和 Trend Micro 功能的支持。这些功能以前在SVC模式下可受支持。现在，所有模式下都可以触发 Trend Micro 和 IPS 引擎（如果已配置）。 此功能还添加了基于 WebSense 和 N2H2 支持的 URL/FTP/HTTPS/Java/Activex 过滤功能。对于 DNS 请求，此功能会触发 DNS 检测。 在端口转发模式下，此功能还添加了基于 WebSense 和 N2H2 支持的 HTTP、SMTP、FTP 和 DNS 检测功能及过滤机制。
路由功能	

功能	说明
主动的 RIP 支持	ASA 支持 RIP 版本 1 和 RIP 版本 2。在 ASA 中只能启用一个 RIP 路由进程。启用 RIP 路由进程后，所有接口上都会启用 RIP。默认情况下，安全设备会发送 RIP 版本 1 更新并接受 RIP 版本 1 和版本 2 更新。 要指定在接口上接受的 RIP 版本，请在接口配置模式下使用 **rip receive version** 命令。
备用 ISP 支持	如果主 ISP 链路失败，此功能允许您配置备用 ISP 链路。该功能使用静态路由和对象跟踪来确定主路由的可用性，并在主路由失败时激活辅助路由。
PPPoE 客户端	基于以太网的点对点协议 (PPPoE) 将以太网和 PPP 两个广泛接受的标准结合在一起，可提供将 IP 地址分配至客户端系统的身份验证方法。PPPoE 客户端通常是通过 DSL 或电缆服务等远程宽带连接来连接到 ISP 的个人计算机。ISP 部署 PPPoE 的原因在于，PPPoE 支持使用其现有远程访问基础设施进行高速宽带访问，同时也更加便于客户使用。
动态 DNS 支持	您可以创建动态 DNS (DDNS) 更新方法，并将它们配置为按您所需的任何频率在 DNS 服务器上更新资源记录 (RR)。 DDNS 与 DHCP 相互补充，DHCP 使用户能够透明地为客户端动态分配可重用的 IP 地址。然后，DDNS 提供动态更新和同步，将名称更新并同步到地址，再将地址更新并同步到 DNS 服务器上的名称映射。使用此版本，ASA 支持将 IETF 标准用于 DNS 记录更新。

功能	说明
静态路由跟踪	静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。 引入了以下命令：**clear configure sla**、**frequency**、**num-packets**、**request-data-size**、**show sla monitor**、**show running-config sla**、**sla monitor**、**sla monitor schedule**、**threshold**、**timeout**、**tos**、**track rtr** 引入或修改了以下菜单项： **配置 > 设备设置 > 路由 > 静态路由 > 添加静态路由 配置 > 设备设置 > 路由 > 静态路由 > 添加静态路由 > 路由监控选项**
组播路由增强功能	组播路由增强功能让您可以定义组播边界以免RP的IP地址相同的域相互泄露信息，允许您对PIM邻居执行过滤以便更好地控制PIM过程，并允许对PIM双向邻居执行过滤以支持混合双向和稀疏模式的网络。
扩展了 DNS 域名使用范围	在配置 AAA 服务器时，可以使用 DNS 域名（例如 www.example.com），也可以使用 **ping**、**traceroute** 和 **copy** 命令。
接口内通信流量畅通无阻	现在，您可以允许任何流量传入和传出同一接口，而不只是 VPN 流量。
针对 IPv6 地址实施 IPv6 安全机制	此功能允许您将安全设备配置为：要求直连主机的IPv6地址对地址的接口标识符部分使用修改后的 EUI-64 格式。
多情景模式功能	
多情景模式的专用和自动 MAC 地址分配及生成	您可以为每个接口分配一个专用的MAC地址（用于故障切换的主用和备用设备）。对于多情景模式，您可以为共享情景的接口自动生成唯一的 MAC 地址，这样可以使数据包的情景分类更加可靠。 新 **mac-address auto** 命令允许您为每个共享情景的接口自动分配专用 MAC 地址。

功能	说明
安全情景的资源管理	例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。
从系统中保存所有情景配置	现在，您可以使用 **write memory all** 命令从系统执行空间一次性保存所有情景配置。
高可用性功能	
次秒级故障切换	此功能让您可以通过配置故障切换来迅速检测和响应故障。
配置提示	使用此功能，用户可以查看安全设备的故障切换状态，而不必输入 **show failover** 命令及分析输出。此功能让用户可以查看故障切换设备的机箱插槽号。以前，该提示反映的只是主机名、安全情景和配置模式。prompt 命令支持此功能。
防火墙功能	
常规输入速率限制	此功能通过防火墙防止拒绝服务 (DoS) 对 ASA 或某些检测引擎发起攻击。7.0 版支持出口速率限制（监测）功能，而且此版本中的输入速率限制功能扩展了当前的出口监测功能。 对于此功能扩展了 **police** 命令。
针对通过流量和管理访问的身份验证支持 VPN 客户端之前支持的所有服务器	所有服务器类型均可使用防火墙身份验证，但以下情况例外：HTTP 表单协议仅支持对 WebVPN 用户进行单点登录身份验证，并且不支持使用 SDI 进行 HTTP 管理访问。
失效连接检测 (DCD)	此功能让自适应安全设备可以自动检测和终止失效连接。在以前的版本中，失效连接从不会超时，它们的超时设置为无限值。您需要进行手动干预，才能确保失效连接的数量不会让安全设备崩溃。使用此功能，系统会自动检测和终止失效连接，而不会干扰仍可处理流量的连接。set connection timeout 和 show service-policy 命令支持 DCD。
WCCP	Web 缓存通信协议 (WCCP) 功能允许您指定 WCCP 服务组及重定向 Web 缓存流量。该功能可透明地将选定类型的流量重定向到一组 Web 缓存引擎，从而优化资源使用率并缩短响应时间。

功能	说明
过滤功能	
Secure Computing (N2H2) 的 URL 过滤增强功能	此功能让您可以使用 Websense（当前供应商）和 N2H2（已被 Secure Computing 收购的一家供应商）启用长 URL、HTTPS 和 FTP 过滤。以前，代码仅支持使用供应商 Websense 来提供此类过滤。url-block、url-server 和 filter 命令支持此功能。
管理和故障排除功能	
自动更新	现在，安全设备不仅可以配置为“自动更新”客户端，还可以配置为“自动更新”服务器。原有的客户端更新命令（也用于更新 VPN 客户端）经过增强，现在可以支持新的自动更新服务器功能，并包括更新作为客户端配置的安全设备所需的新关键字和新参数。对于配置为“自动更新”客户端的安全设备，仍然使用 auto-update 命令来配置安全设备与“自动更新”服务器通信所需的参数。
模块化策略框架对管理流量的支持	现在，您可以为发送到安全设备的流量定义第 3/4 层类映射，以此对管理流量执行特殊操作。对于此版本，您可以检测 RADIUS 记帐流量。
Traceroute	**traceroute** 命令让您可以跟踪数据包传至其目标的路由。
数据包跟踪器	数据包跟踪器工具让您可以通过 ASA 跟踪数据包的生命周期来查看其行为是否符合预期。 **packet-tracer** 命令可提供有关数据包的详细信息，以及安全设备对数据包的处理方式。如果配置命令未导致数据包被丢弃，**packet-tracer** 命令将提供相关原因的具体信息。 借助 ASDM 中正在申请专利的新 Packet Tracer 工具，无论网络设计有多么复杂您都可以通过 ASA 在数据包动画流模型中轻松地跟踪数据包的生命周期，以查看其行为是否符合预期并简化故障排除。该工具以可视方式展示数据包的不同阶段和相关配置（点击一下即可访问），由此提供数据包的属性，例如源 IP 地址和目标 IP 地址。对于每个阶段，该工具都会显示是丢弃还是允许数据包。

功能	说明
ASDM 功能	
增强的 ASDM 规则表	ASDM规则表已经过重新设计，以简化策略创建过程。不仅简化的规则创建使得与 CLI 的映射更加紧密，而且规则表还支持大多数配置方案，包括超网和使用与多个接口关联的对象组。不再要求使用 ASDM 位置和 ASDM 组，以简化规则的创建。现在，您能够： • 在单个面板中创建对象、对象组和规则 • 对接口、源、目标或服务执行过滤 • 在规则表中执行策略查询，以使用多个条件执行高级过滤 • 在实时日志查看器中显示特定访问规则的日志 • 点击一下即可选择规则和数据包跟踪，而且系统会自动填充相应的数据包属性 • 支持轻松整理和上下移动表中条目，以更改访问列表条目的顺序 • 可展开并显示对象组中的元素 • 可通过工具提示查看组对象或组成员的属性
高可用性和可扩展性向导	高可用性和可扩展性向导可用于简化主用/主用、主用/备用故障切换及 VPN 负载均衡的配置。该向导还可以智能地配置对等设备。
系统日志增强功能	系统日志功能的增强包括： • 解析系统日志，以在不同列中显示源 IP、目标 IP、系统日志 ID、日期和时间 • 点击一下即可为每个系统日志集成系统日志参考及解释和建议操作 • 基于严重性级别设置系统日志颜色 • 在日志查看器中以工具提示形式简要说明系统日志
NAT 规则	简化了 NAT 规则的创建过程。

功能	说明
支持对象组	现在，ASDM 已完全支持网络、服务、协议和 ICMP 类型的对象组。
命名的 IP 地址	现在，您可以创建要与 IP 地址关联的名称。
ASDM 助手	新的 ASDM 助手可以就功能（例如 AAA 服务器、日志记录过滤器、SSL VPN 客户端及其他功能）的配置提供以任务为导向的指导。您也可以上传新的指导。
情景管理	情景管理功能经过改进，包括了情景缓存并提高了可扩展性。
检测映射	预定义的低、中和高安全设置，简化了检测映射的创建和管理。

版本 7.1 的新功能

ASA 7.1(2)/ASDM 5.1(2) 的新功能

发布日期：**2006** 年 **3** 月 **15** 日

ASA 7.1(2)/ASDM 5.1(2) 中无新增功能

ASA 7.1(1)/ASDM 5.1(1) 的新功能

发布日期：**2006** 年 **2** 月 **6** 日

功能	说明
平台功能	

功能	说明
支持内容安全和控制 (CSC) SSM	

功能	说明
	作为思科安防系列解决方案不可或缺的一部分，CSC SSM 提供行业领先的互联网边缘威胁防范与内容控制机制，包括全面的防病毒、反间谍软件、文件阻止、反垃圾邮件、反网络钓鱼、URL 阻止和过滤，以及内容过滤服务。CSC SSM 服务模块可帮助企业通过以下关键元素更加有效地保护其网络，并提高网络可用性和员工工作效率： • 防病毒 - Trend Micro 提供的市场领先的防病毒服务，可在基础设施最有效的位置（互联网网关）保护您的内部网络资源不受已知和未知的病毒攻击。该服务通过在外围清理邮件和 Web 流量，使您无需再对海量资源执行恶意软件感染清理，从而确保业务连续性。 • 反间谍软件 - 防止间谍软件通过 Web 流量（HTTP 和 FTP）和邮件流量进入您的网络。让 IT 支持资源不必再执行费时费力的间谍软件删除程序，并通过在网关阻止间谍软件提高员工工作效率。 • 反垃圾邮件 - 有效阻止垃圾邮件并保证极低的误报率，让邮件通信恢复应有的效率，从而确保与客户、供应商和合作伙伴的联系持续不间断。 • 反网络钓鱼 - 防范身份盗窃可抵御网络钓鱼攻击，从而防止员工无意中泄露公司或个人详细信息，以免蒙受财务损失。 • TrendLabs 提供的自动更新 - 该解决方案由业内最大的病毒、间谍软件和垃圾邮件专家团队之一提供支持，他们全天候工作，确保您的解决方案可自动提供最新的保护。 • 集中管理 - 通过支持远程访问的 Web 控制台和自动更新实现轻松、无忧的管理，从而降低 IT 支持成本。 • 为 Web 访问、邮件（SMTP 和 POP3）和 FTP（文件传输）提供实时保护 - 即使公司邮件已得到保护，还是会有很多员工使用公司 PC 或笔记本电脑访问自己的私人网络邮件，从而为互联网传播的威胁提供另一个入口点。同样，员工也可能会直接下载已感染类似威胁的文件程序。在互联网网关实时保护所有 Web 流量可大大减少这种常被忽视的漏洞

功能	说明
	点。 • 支持各种类别、日程安排和缓存的完整URL过滤功能 - URL 过滤可用于控制员工对互联网的使用，此功能不仅可以阻止员工访问不当或与工作无关的网站，以此提高员工工作效率，而且能降低员工因接触攻击性 Web 内容而受到法律制裁的风险。 • 邮件内容过滤 - 邮件过滤可最大限度地避免因通过邮件传输攻击性材料而承担法律责任，并可强制执行合规性措施，从而帮助组织满足GLB和“数据保护法”等法规要求。
常规 VPN 功能	

功能	说明
思科安全桌面	思科安全桌面 (CSD) 是一个可选 Windows 软件包，您可以将其安装在 ASA 上来验证请求访问 SSL VPN 的客户端计算机的安全性，确保它们在连接时一直安全，并在它们断开连接后删除所有会话痕迹。 在运行 Microsoft Windows 的远程 PC 连接到 ASA 之后，CSD 将自行安装并使用特定文件的 IP 地址和状态、注册表项和证书来识别连接 PC 的位置的类型。执行用户验证之后，CSD 将以可选标准作为授予访问权限的条件。这些标准包括 PC 上运行的操作系统、防病毒软件、反间谍软件和个人防火墙。 为了确保 PC 在连接至网络时是安全的，安全桌面（Microsoft Windows XP 和 Windows 2000 客户端上运行的 CSD 应用）会限制用户在会话期间可执行的操作。对于具有管理员权限的远程用户，安全桌面使用 168 位三重数据加密标准 (3DES) 对 SSL VPN 会话期间关联或下载的数据和文件进行加密。对于权限较低的远程用户，该应用使用 Rivest Cipher 4 (RC4) 加密算法。当会话关闭时，安全桌面将按照美国国防部 (DoD) 安全标准覆盖和删除远程 PC 中的所有数据，以便安全删除文件。这种清理方法可确保在远程用户注销或 SSL VPN 会话超时后，能够彻底删除 Cookie、浏览器历史记录、临时文件和下载的内容。此外，CSD 也会从客户端 PC 自行卸载。 缓存清理器可在会话结束时擦除客户端缓存（适用于 Windows XP、Windows 2000、Windows 9x、Linux 和 Apple Macintosh OS X 客户端）。

功能	说明
基于 CSD 主机检查的自定义访问控制	安装了思科安全桌面的自适应安全设备可以指定备选组策略。ASA 按如下方式使用此属性，以限制对远程 CSD 客户端的访问： • 当 VPN 功能策略设置为“使用失败组策略”时，始终使用此属性。 • 当 VPN 功能策略设置为“如果符合标准，则使用成功组策略”时，如果不符合标准，则使用此属性。 此属性可指定要应用的备选组策略的名称。您可以选择一个组策略，以使相关的访问权限与默认组策略关联的权限区分开来。默认值为 DfltGrpPolicy。 **注释** 将 VPN 功能策略设置为“始终使用成功组策略”时，ASA 不使用此属性。
SSL VPN 客户端	SSL VPN 客户端是一种 VPN 隧道技术，该技术无需网络管理员在远程计算机上安装和配置 IPSec VPN 客户端，即可为远程用户提供 IPSec VPN 客户端在连接上的优势。SVC 结合使用远程计算机上已有的 SSL 加密方法以及 ASA 的 WebVPN 登录和身份验证方法。 要建立 SVC 会话，远程用户需要在浏览器中输入 ASA 的 WebVPN 接口 IP 地址，浏览器将连接到该接口并显示 WebVPN 登录屏幕。如果用户认可这种登录和身份验证方法，而且 ASA 认为用户需要 SVC，则 ASA 会将 SVC 下载到远程计算机。如果 ASA 认为用户可选用 SVC，则 ASA 会将 SVC 下载到远程计算机，同时在用户屏幕上显示一个跳过 SVC 安装的链接。 下载后，SVC 会自行安装和配置；连接终止后，SVC 会保留在远程计算机中或自行卸载（具体取决于配置情况）。

功能	说明
WebVPN 功能和性能优化	此版本通过以下组件增强了 WebVPN 的性能和功能： • 灵活的内容转换/重写（包括复杂的 JavaScript、VBScript 和 Java 内容） • 服务器端缓存和浏览器缓存 • 压缩 • 代理绕行 • 支持应用配置文件自定义框架 • 应用保持连接和超时处理 • 支持逻辑 (VLAN) 接口
Citrix 对 WebVPN 的支持	现在，WebVPN 用户可以连接到 ASA 来访问 Citrix MetaFrame 服务。在此配置中，ASA 用作 Citrix 安全网关。因此，您必须将 Citrix Web Interface 软件配置为在不使用 Citrix 安全网关的模式下运行。将 SSL 证书安装到远程用户使用完全限定域名 (FQDN) 连接到的 ASA 接口上；如果将 IP 地址指定为 SSL 证书的公用名称 (CN)，则此功能不起作用。远程用户尝试使用 FQDN 与 ASA 进行通信。远程 PC 必须能够使用 DNS 或 System32\drivers\etc\hosts 文件中的条目来解析 FQDN。最后，使用 **functions** 命令来启用 Citrix。
PDN 对 WebVPN 的支持	您可以从 Pocket PC 2003 或 Windows Mobile X 访问 WebVPN。如果您是 PDA 用户，这样可以更方便地访问您的专用网络。此功能不需要进行配置。

功能	说明
WebVPN 支持 CIFS 文件的字符编码	现在，WebVPN 支持门户页面的可选字符编码，以确保按预期语言正确呈现通用互联网文件系统文件。字符编码支持以下网页上注明的字符集，包括日语 Shift-JIS 字符： http://www.iana.org/assignments/character-sets 使用 **character-encoding** 命令可指定在传给远程用户的 WebVPN 门户页面中要编码的字符集。默认情况下，远程浏览器上设置的编码类型将决定 WebVPN 门户页面的字符集。 默认情况下，字符编码属性是所有 WebVPN 入口页面都会继承的全局设置。不过，您可以使用 **file-encoding** 命令指定来自特定 CIFS 服务器的 WebVPN 门户页面的编码。这样，您就可以将不同的 file-encoding 值用于需要不同字符编码的 CIFS 服务器。 当文件名或目录路径以及页面无法正确呈现时，CIFS 服务器到适当字符编码的映射（在全局映射时使用 webvpn character-encoding 属性，在单独映射时使用 file-encoding 覆盖）可正确处理和显示 CIFS 页面。 **提示** 字符编码和文件编码值包括浏览器所使用的字体族。如果当前使用日语 Shift_JIS 字符编码，则需要在 webvpn 自定义命令模式下使用 **page style** 命令对上述值之一进行补充设置以替换字体系列；或者在 webvpn 自定义命令模式下输入 **no page style** 命令以删除字体系列。

功能	说明
WebVPN 和 SSL VPN 客户端连接的压缩	压缩可以减小传输数据包的大小并提高通信性能，此功能特别适合用于具有带宽限制的连接，例如使用拨号调制解调器和手持设备进行远程访问的情况。 默认情况下，压缩功能对 WebVPN 和 SVC 连接均启用。您可以使用 ASDM 或 CLI 命令来配置压缩。 在全局配置模式下，您可以使用 **compression** 命令对所有 WebVPN 或 SVC 连接禁用压缩。 您可以在组策略或用户名 webvpn 模式下，使用 http-comp 命令对特定组或用户禁用 WebVPN 连接压缩，或使用 **svc compression** 命令对特定组或用户禁用 SVC 连接压缩。
WebVPN 和 SVC 连接的主用/备用状态故障切换	在故障切换期间，系统将使用辅助的备用安全设备重新建立 WebVPN 和 SVC 连接以及 IPSec 连接，以便不间断地提供服务。主用/备用故障切换需要对每个连接进行一对一的主用/备用匹配。 配置用于故障切换的安全设备将与备用安全设备共享 WebVPN 用户的相关身份验证信息。因此，执行故障切换后，WebVPN 用户不需要重新进行身份验证。 对于 SVC 连接，执行故障切换后，SVC 将自动重新连接备用安全设备。
WebVPN 自定义	您可以自定义用户在连接到安全设备时看到的 WebVPN 页面，还可以按用户、组或隧道组自定义 WebVPN 主页。用户或组在通过安全设备的身份验证后，就会看到自定义的 WebVPN 主页。 您可以使用级联样式表 (CSS) 参数。为了实现轻松自定义，我们建议您使用 ASDM（它具有配置样式元素的便捷功能，包括色样和预览功能）。
自动下载小应用程序	要通过 WebVPN 运行远程应用，用户可在 WebVPN 主页上点击“启动应用访问”来下载并启动一个端口转发 Java 小应用程序。要简化应用访问并缩短启动时间，您现在可以将 WebVPN 配置为在用户首次登录到 WebVPN 时自动下载此端口转发小应用程序。
身份验证和授权 VPN 功能	

功能	说明
覆盖禁用的帐户	您可以将 ASA 配置为覆盖 AAA 服务器中的禁用帐户指示，并允许用户以任何方式登录。 引入了以下命令：**override account disabled**。
LDAP 支持	您可以对安全设备进行配置，使 IPSec VPN 用户、SSL VPN 客户端和 WebVPN 用户需要经过身份验证和授权才能访问 LDAP 目录服务器。在身份验证过程中，ASA 将充当 VPN 用户访问 LDAP 服务器的客户端代理，并以明文形式或使用简单身份验证和安全层 (SASL) 协议对访问 LDAP 服务器的用户执行身份验证。安全设备支持符合 LDAP V3 或 V2 规范的任何目录服务器。它仅在 Sun Microsystems Java 系统目录服务器和 Microsoft Active Directory 服务器上支持密码管理功能。
密码管理	您可以将 ASA 配置为在最终用户的密码即将到期时向他们发出警告。配置此功能后，ASA 将在远程用户登录时通知其当前密码即将到期或已到期。然后，ASA 为用户提供机会更改密码。如果当前密码尚未到期，用户仍可使用该密码登录。此命令适用于支持此类通知的 AAA 服务器，即 RADIUS、使用 NT 服务器的 RADIUS 以及 LDAP 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。 请注意，此命令不会更改密码过期前的天数，而是指定 ASA 会提前多少天开始警告用户密码即将过期。默认值为 14 天。 您仅可对 LDAP 服务器身份验证指定具体提前多少天开始警告用户密码即将过期。 引入了以下命令：**password management**。

功能	说明
单点登录 (SSO)	借助单点登录 (SSO) 支持，WebVPN 用户只需输入一次用户名和密码，即可访问多个受保护的服务和 Web 服务器。您可以选择以下方法来配置 SSO： • Computer Associates eTrust SiteMinder SSO 服务器（以前称为 Netegrity SiteMinder）- 如果您的网站安全基础设施中已引入 SiteMinder，通常可选择对 SiteMinder 实施 SSO。 • HTTP 表单 - 执行 SSO 身份验证的通用标准方法，也可用作 AAA 方法。此方法可以与其他 AAA 服务器（例如 RADIUS 或 LDAP 服务器）配合使用。 • 基于基本 HTTP 和 NTLM 身份验证的 SSO - 三种 SSO 方法中最简单的方法，可将用于身份验证的 WebVPN 登录凭证传送到使用基本 HTTP 或 NTLM 身份验证的内部服务器。此方法不需要外部 SSO 服务器。
隧道组和组策略 VPN 功能	
WebVPN 隧道组类型	此版本中添加了一个 WebVPN 隧道组，它允许您使用 WebVPN 特定的属性配置隧道组，这些属性包括要使用的身份验证方法、要应用到用户 GUI 的 WebVPN 自定义项、要使用的 DNS 组、备选组名称（别名）、组 URL、用于 CIFS 名称解析的 NBNS 服务器以及要应用于 CSD 用户以限制对远程 CSD 客户端的访问权限的备选组策略。
基于组的 WebVPN DNS 配置	您可以按组定义 DNS 服务器列表。用户可用的 DNS 服务器列表取决于该用户分配到了哪个组。您可以指定用于 WebVPN 隧道组的 DNS 服务器。默认值为 DefaultDNS。
面向 WebVPN 用户的新登录页面选项	您可以选择将 WebVPN 配置为显示一个用户登录页面，用户可在该页面中选择用于登录的隧道组。如果配置了此选项，登录页面将显示一个提供组下拉菜单的附加字段，供您从中进行选择。系统将根据所选的组对用户进行身份验证。

功能	说明
组别名和组 URL	您可以通过指定一个或多个组别名来创建一个或多个备选名称，供用户用于引用隧道组。此处指定的组别名显示在用户登录页面的下拉列表中。每个组可以有多个别名或没有别名。如果希望此列表中显示隧道组的实际名称，请将其指定为别名。此功能在同一个组具有多个常见名称（如“Devtest”和“QA”）时有用。 指定组URL后，用户在登录时无需再选择组。当用户登录时，ASA 会在隧道组策略 (tunnel-group-policy) 表中查找用户的传入URL。如果 ASA 找到 URL 且启用了此功能，则会自动选择适当的服务器，并且在登录窗口中仅向用户显示用户名和密码字段。如果该URL被禁用，则登录窗口中还会显示组下拉列表，且用户必须进行选择。 可以为一个组配置多个 URL，也可以不配置URL。您可以单独启用或禁用每个URL。您必须为每个 URL 单独进行指定（**group-url** 命令）。您必须指定完整的 URL（可以使用 HTTP 或者 HTTPS 协议）。 同一个 URL 不能与多个组关联。ASA 在接受隧道组的 URL 之前会验证该 URL 的唯一性。
ASDM 功能	

功能	说明
支持对 CSC SSM 进行管理和监控	ASDM 版本 5.1 提供行业领先的解决方案，该解决方案既具备 Trend Micro 基于 HTML 的配置面板的简洁性，又具备 ASDM 的独创性。这样有助于确保实施一致的策略，并简化调配、配置和监控 CSC SSM 提供的丰富而统一的威胁管理功能的整个过程。ASDM 提供包含新 CSC SSM 主页和新监控面板的补充性监控解决方案。安装 CSC SSM 后，主 ASDM 主页将自动更新为显示新的 CSC SSM 面板，在该面板中可查看威胁、邮件病毒、实时事件以及重要模块的历史统计信息，例如上次安装的软件/签名更新、系统资源等。 ASDM 的监控部分有一组丰富的分析工具，通过它们可详细查看威胁、软件更新、资源图等信息。“实时安全事件监控”是一款全新的故障排除和监控工具，它根据扫描或阻止的邮件消息、识别的病毒/蠕虫、检测到的攻击等提供实时更新。通过该工具，管理员可以选择基于正则表达式字符串匹配来过滤消息，由此关注并详细分析特定的攻击类型和消息。
系统日志与访问规则关联	此 ASDM 版本引入了一款全新的“系统日志与访问规则关联”工具，该工具可显著改善日常安全管理和故障排除活动。使用此动态工具，安全管理员可快速解决常见的配置问题以及大多数用户和网络连接问题。用户可以在“实时系统日志查看器”面板中选择系统日志消息，而且只需点击面板顶部的“创建”按钮即可调用该特定系统日志的访问控制选项。智能默认设置有助于确保配置过程简单易行，这样有利于提高业务关键功能的操作效率，缩短其响应时间。另外，通过“系统日志与访问规则关联”工具还可直观地查看用户配置的访问规则调用的系统日志消息。
自定义的系统日志颜色	ASDM 允许根据系统日志级别设置系统日志消息组的颜色，从而让您能够快速识别关键系统消息并方便地监控系统日志。用户可以选择默认颜色设置选项，也可以创建自己独特的系统日志颜色配置文件，以便轻松识别各种信息。
ASDM 和 WebVPN 接口	现在，ASDM 和 WebVPN 可以同时在同一接口上运行。
ASDM 演示模式	初始支持 ASDM 演示模式。

版本 7.0 的新功能

ASA 7.0(8)/ASDM 5.0(8) 和 ASDM 5.0(9) 的新功能

发布日期：2007 年 6 月 2 日

注释 ASDM 5.0(9) 不包括任何新功能；它只包含警告修补程序。

功能	说明
防火墙功能	
Ethertype ACL MAC 增强	EtherType ACL 功能进行了增强，支持非标准的 MAC。现有的默认规则予以保留，但无需添加新规则。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
远程访问功能	
本地地址池编辑	您可以编辑地址池，而不会影响所需的连接。如果不从池中删除正在使用的地址，则连接不受影响。不过，如果要从池中删除正在使用的地址，连接则会断开。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
连接功能	
clear conn 命令	添加了 **clear conn** 命令，以删除连接。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
完全重组数据分段	通过 **reassembly full** 关键字改进了 **fragment** 命令，支持完全重组通过设备传输的数据分段。在设备处终止的数据分段始终会完全重组。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
故障排除和监控功能	
capture 命令增强	**capture type asp-drop** *drop_code* 命令现在接受 **all** 作为 *drop_code*，所以您现在可以捕获 ASA 丢弃的所有数据包，包括由于安全检查而丢弃的数据包。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。

功能	说明
show asp drop 命令增强	输出现在包括指示计数器上次清除时间的时间戳（请参阅 **clear asp drop** 命令）。输出还会在说明旁边显示丢弃原因关键字，以便您能够轻松使用具有该关键字的 **capture asp-drop** 命令。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
clear asp table 命令	添加了 **clear asp table** 命令，以清除 **show asp table** 命令输出的命中次数。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
show asp table classify hits 命令增强	将 hits 选项添加到 **show asp table classify** 命令，用于显示指示上次何时清除 asp 表计数器的时间戳。该命令还会显示符合值不等于零的规则。借此，用户可以快速查看符合哪些规则，特别是 **show asp table classify** 命令中一个简单配置以数百个条目结尾的情况。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
show perfmon 命令	添加了以下速率输出：已建立 TCP 拦截连接、TCP 拦截尝试、TCP 初期连接超时和 TCP 拦截中的有效连接速率。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。

功能	说明
memory tracking 命令	此版本中引入了以下新命令： • **memory tracking enable** - 此命令支持跟踪堆内存请求。 • **no memory tracking enable** - 此命令禁止跟踪堆内存请求、清理当前收集的所有信息，并向系统返回工具本身使用的所有堆内存。 • **clear memory tracking** - 此命令会清除当前收集的所有信息，但会继续跟踪进一步的内存请求。 • **show memory tracking** - 此命令显示当前工具所跟踪的已分配内存，它们按最上方的调用方函数地址进行细分。 • **show memory tracking address** - 此命令显示当前按每一块内存细分的已分配内存。输出会列出当前工具跟踪的每个已分配内存块的大小、位置以及最上方的调用方函数。 • **show memory tracking dump** - 此命令显示指定内存地址的大小、位置、部分调用栈和内存转储。 • **show memory tracking detail** - 此命令显示探查工具内部行为时要使用的各种内部详细信息。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
故障切换功能	
failover timeout 命令	**failover timeout** 命令用于静态指定功能时，不再需要故障切换许可证。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
可用性功能	
show access-list 输出	扩展的访问列表输出是缩进的，以使其更易于阅读。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。

功能	说明
show arp 输出	在透明防火墙模式下，您可能需要知道ARP条目是静态配置的还是动态获悉的。如果已获悉动态ARP 条目，ARP 检查将从合法主机丢弃 ARP 应答。ARP 检查只适用于静态 ARP 条目。现在，如果条目是动态的，show arp 命令会显示每个条目及其显示时长，如果是静态的，则不显示显示时长。 请参阅**监控 > 接口 > ARP 表**。 同样适用于版本 *7.2(4)* 和 *8.0(4)*。
show conn 命令	该语法已简化为使用源和目标概念，而不是“本地”和“外部”。在新语法中，源地址是输入的第一个地址，目标地址是输入的第二个地址。旧语法使用诸如 foreign 和 port 之类的关键字来确定目标地址和端口。
ASDM 功能	
支持分段选项	ASDM现在支持使用片段选项来重组通过ASDM路由的数据包。 要配置此功能，请参阅**配置 > 属性 > 高级 > 分段**。

ASA 7.0(7)/ASDM 5.0(7) 的新功能

发布日期：**2007** 年 **7** 月 **9** 日

功能	说明
模块功能	
添加了数据平面保持连接机制	现在，您可以配置 ASA 以免在升级 AIP SSM 时发生故障切换。在以前版本中，如果在故障切换中配置两个具备 AIP SSM 的 ASA，在更新 AIP SSM 软件时，ASA 就会触发故障切换，因为 AIP SSM 需要重新引导或重启，才会使软件更新生效。 同样适用于版本 *7.2(3)* 和 *8.0(3)*

ASA 7.0(6)/ASDM 5.0(6) 的新功能

发布日期：**2006** 年 **8** 月 **22** 日

ASA 7.0(6)/ASDM 5.0(6) 中无新增功能

ASA 7.0(5)/ASDM 5.0(5) 的新功能

发布日期：**2006** 年 **4** 月 **14** 日

功能	说明
应用检测功能	
用于控制 DNS 保护的命令	现在，您可以控制DNS保护功能。在7.0(5)之前的版本中，无论如何配置 DNS 检查，DNS 保护功能始终处于启用状态： • 对 ID 匹配 DNS 请求的 DNS 响应进行状态跟踪 • 在所有待处理的请求都得到响应时断开DNS连接 此命令仅在禁用了 DNS 检查的接口上有效 (**no inspect dns**)。当 DNS 检查启用时，DNS 保护功能将始终处于工作状态。 引入了以下命令：**dns guard**。
增强的 IPSEC 检查功能	通过增强的 IPSec 检查功能，可以在存在 IKE 流时打开适用于ESP流的特定针孔。此功能可以在MPF基础设施中与其他检查功能一起配置。所产生的 ESP 流的空闲超时静态设置为 10 分钟。所能允许的 ESP 流的数量没有最大值限制。 引入了以下命令：**inspect ipsec-pass-thru**。
防火墙功能	

功能	说明
对被拒绝的 TCP 数据包禁用 RST 的命令	若 TCP 数据包在从高安全性接口转至低安全性接口时被拒绝，自适应安全设备始终会发送重置命令。**service resetinbound** 命令用于启用或禁用如下操作：如果 TCP 数据包在从低安全性接口转至高安全性接口时被拒绝，则发送重置命令。引入 **service resetinbound** 命令是为了避免在数据包从高安全性接口转至低安全性接口时被拒绝的情况下发送重置命令。现有的 **service resetinbound** 命令已经过增强，可以选择其他接口选项。 引入了以下命令：**service resetoutbound** 和 **service resetinbound**。
平台功能	
增加了连接数和 VLAN 数量	最大连接数和 VLAN 数增加至以下数值。 • ASA5510 基本许可证连接数 32000->> 50000；VLAN 数 0-> 10 • ASA5510 增强许可证连接数 64000->> 130000；VLAN 数 10-> 25 • ASA5520 连接数 130000->280000；VLAN 数 25->100 • ASA5540 连接数 280000->400000；VLAN 数 100->200
管理功能	
本地数据库中的密码长度增加	本地数据库中的用户名和启用密码长度限制从 16 增加到 32。

功能	说明

增强的 **show interface** 和 **show traffic** 命令	**show interface** 和 **show traffic** 命令中显示的流量统计信息现在支持使用 1 分钟的速率和 5 分钟的速率进行输入、输出和丢弃。最后两个采样点之间的差值即为计算出的速率值。对于 1 分钟速率和 5 分钟速率，系统会持续对这两个速率分别运行 1 分钟的计时器和 5 分钟的计时器。新的显示内容示例如下：
	
	`1 minute input rate 128 pkts/sec, 15600 bytes/sec`
	`1 minute output rate 118 pkts/sec, 13646 bytes/sec`
	`1 minute drop rate 12 pkts/sec`
	`5 minute input rate 112 pkts/sec, 13504 bytes/sec`
	`5 minute output rate 101 pkts/sec, 12104 bytes/sec`
	`5 minute drop rate 4 pkts/sec`

ASA 7.0(4)/ASDM 5.0(4) 的新功能

发布日期：2005 年 10 月 15 日

注释 没有 7.0(3)/5.0(3) 版本。

功能	说明
平台功能	
支持 4GE SSM	4GE 安全服务模块 (SSM) 是自适应安全设备的可选 I/O 卡。4GE SSM 扩展了安全设备上可用的端口总数，可提供四个附加端口进行以太网 (RJ-45) 或 SFP（光纤）连接。
VPN 功能	
WebVPN 捕获功能	WebVPN 捕获功能允许您记录无法通过 WebVPN 连接正常显示的网站的信息。您可以使用 capture 命令启用 WebVPN 捕获功能，但请注意，该功能对安全设备的性能有不利影响。因此，在捕获进行故障排除所需的信息之后，请务必禁用此功能。

功能	说明
通过 VPN 隧道进行自动更新	在此版本中，**auto-update server** 命令有一个新的 **source** 参数，该参数可用于指定接口，例如用于管理访问且由 **management-access** 命令指定的 VPN 隧道： **auto-update server** *url* [**source** *interface*] [*verify-certificate*]
HTTP 代理小应用程序	HTTP 代理是一个互联网代理，它支持 HTTP 和 HTTPS 连接。HTTP 代理代码可以动态修改浏览器代理配置，已将所有浏览器 HTTP/S 请求重定向到新的代理配置。这允许 Java 小应用程序可以接任浏览器的代理。 HTTP 代理可以与端口转发（应用访问）功能或与自身结合使用。 **注释** HTTP 代理功能仅在使用 Internet Explorer 浏览器时有效。 在运行 Windows XP 的某些较旧的计算机上，RunOnce Reg-Key 不可用，这会导致在尝试修改 Internet Explorer 上的代理设置时，端口转发 HTTP 代理功能失败。 您可以手动更改注册表。完成以下步骤以手动更改注册表： **1.** 点击**开始** | **运行**。 **2.** 在打开的文本框中键入 **regedit**，然后点击**确定**。 **3.** 打开此文件夹：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ **4.** 在“当前版本”内点击鼠标右键，然后选择**新建** | **密钥**。 **5.** 将新密钥命名为 **RunOnce**。 **6.** 点击**确定**。 要为该用户或组策略配置文件访问和文件浏览、MAPI 代理、HTTP 代理以及基于 WebVPN 的 URL 输入，请在 WebVPN 模式下使用 **functions** 命令。

功能	说明
IPSec VPN：添加对级联 ACL 的支持	*级联 ACL* 涉及插入 deny ACE 以绕过按照某个 ACL 进行的评估，而按照加密映射集中的后续 ACL 继续进行评估。由于您可以将每个加密映射与不同的 IPSec 设置关联，因此您可以使用 deny ACE 将特定流量从相应加密映射中的进一步评估中排除，并且将特定流量与另一个加密映射中的 permit 语句匹配以提供或要求提供不同的安全保护。分配给加密 ACL 的序号确定其在加密映射集内评估序列中的位置。
故障排除和监控功能	
Crashinfo 增强功能	**crashinfo** 命令的输出可能包含不适合连接至 ASA 的所有用户查看的敏感信息。新的 **crashinfo console disable** 命令可用来抑制输出显示在控制台上。
对系统日志消息的速率限制	日志记录速率限制使您可以限制生成系统日志消息的速率。您可以限制在指定的时间间隔内生成的系统消息的数量。 您可以限制所有消息、单个消息 ID、消息 ID 的范围或具有特定严重性级别的所有消息的消息生成率。若要限制生成系统日志消息的速率，请使用 **logging rate-limit** 命令。
防火墙功能	
使用模块化策略框架	新的 **set connection timeout** 命令允许您配置超时时段，该时段过后，空闲的 TCP 连接将会断开。
可下载 ACL 增强功能	此版本中添加了一个新功能，以确保发送到 RADIUS 服务器的可下载 ACL 请求通过 Message-Authenticator 属性来自有效的源。 在收到其用户名属性中包含可下载 ACL 名称的 RADIUS 身份验证请求时，思科安全 ACS 将通过检查 Message-Authenticator 属性对该请求进行身份验证。Message-Authenticator 属性的存在可以防止恶意使用可下载 ACL 名称来获取未经授权的网络访问。Message-Authenticator 属性及其用法在 RFC 2869（RADIUS 扩展）中定义，可从 http://www.ietf.org 获得。

功能	说明
在可下载 ACL 中将通配符转换为网络掩码	某些思科产品（如 VPN 3000 集中器和思科 IOS 路由器）要求您使用通配符（而不是网络掩码）配置可下载 ACL。而思科 ASA 5500 自适应安全设备要求您使用网络掩码配置可下载ACL。这一新功能允许ASA将通配符内部转换为子网掩码。通配符网络掩码表达的转换意味着为思科 VPN 3000 系列集中器编写的可下载 ACL 可由 ASA 使用，而无需更改 RADIUS 服务器上可下载 ACL 的配置。 您可以使用 **acl-netmask-convert** 命令（在 AAA 服务器配置模式下可用）在每台服务器上配置 ACL 子网掩码转换。
应用检测功能	
支持跨 GSN 的 GTP 负载平衡	当 ASA 执行 GTP 检测时，ASA 默认会丢弃来自 GSN 的 GTP 请求中未指定的 GTP 响应。如果在 GSN 池中使用负载平衡来实现 GPRS 的效率和可扩展性，将会出现这种情况。使用 **permit response** 命令，可以启用对 GSN 池的支持。此命令将 ASA 配置为允许来自任何指定的 GSN 组的响应，而不考虑 GTP 请求发送到哪个 GSN。

ASA 7.0(2)/ASDM 5.0(2) 的新功能

发布日期：**2005** 年 **7** 月 **22** 日

ASA 7.0(2)/ASDM 5.0(2) 中无新增功能

ASA 7.0(1)/ASDM 5.0(1) 的新功能

发布日期：**2005** 年 **5** 月 **31** 日

功能	说明
平台功能	
支持 ASA 5500 系列	引入了对 ASA 5500 系列的支持，包括对以下型号的支持：ASA 5510、ASA 5520 和 ASA 5540。
防火墙功能	

功能	说明
透明防火墙（第 2 层防火墙）	使用此功能，可以在安全桥接模式下以类似于第 2 层设备的方式部署 ASA，从而为受保护网络提供第 2 - 7 层的各种安全服务。这使企业能够在现有网络环境下部署此 ASA，而无需改写网络地址。虽然 ASA 可以对受保护网络两端的设备完全“隐身”，但管理员可以通过专用 IP 地址（可在独立接口上托管）对其进行管理。除标准 ACL 之外，管理员还可以指定使用非 IP (EtherType) ACL 对第 2 层设备和协议执行访问控制。 引入了以下命令：**arp-inspection**、**firewall**、**mac-address-table** 和 **mac-learn**。
安全情景（虚拟防火墙）	此功能引入了在单一设备中创建多个安全情景（虚拟防火墙）的功能，每个情景可有自己的一组安全策略、逻辑接口和管理域。这样，企业可以方便地将多个防火墙整合到单一物理设备中，同时保留独立管理其中每个虚拟实例的能力。这些功能仅适用于具备无限制 (UR) 或故障切换 (FO) 许可证的 ASA。这是一项许可功能，具有多层支持的安全情景（2、5、10、20 和 50 层）。 引入了以下命令：**admin-context**、**context**（以及 context 子命令）、**changeto** 和 **mode**。
出站 ACL 以及	此功能添加了对出站 ACL 和基于时间的 ACL 的支持（基于现有的入站 ACL 支持构建），使管理员可以更加灵活地定义访问控制策略。现在使用这些新功能，管理员可以在流量进出接口时应用访问控制。基于时间的访问控制列表使管理员可以定义特定 ACL 条目处于活动状态的时间，从而加强资源利用率控制。新命令允许管理员先定义时间范围，再将这些时间范围应用于特定的 ACL。
基于时间的 ACL	现有的通用 **access-list** 全局配置命令通过 **time-range** 命令进行了扩展，以指定使用 **time-range** 全局配置命令定义的基于时间的策略。此外，**access-group** 全局配置命令还支持使用 out 关键字来配置出站 ACL。
启用/禁用 ACL 条目	此功能提供了一种便利的故障排除工具，允许管理员测试和调整 ACL，而不必删除和替换 ACL 条目。

功能	说明
EtherType 访问控制	此功能为根据数据包的 EtherType 执行数据包过滤和日志记录提供强大的支持。当作为透明防火墙运行时，此功能可无比灵活地允许或拒绝非IP协议。
模块化策略框架	此功能引入了灵活性和扩展性极高的下一代模块化策略框架。它允许构建基于流的策略，以便根据管理员定义的条件识别特定流，然后再对该流应用一组服务（例如防火墙/检测策略、VPN 策略、QoS 策略等)。这样可显著改进对流量流以及针对它们所执行的服务的精细控制。另外，新框架还支持对检测引擎进行特定于流的设置（以前版本中是全局设置）。 引入了以下命令：**class-map**、**policy-map** 和 **service-policy**。
TCP 安全引擎	此功能引入了一些新的基础功能，以便帮助检测协议和应用层攻击。TCP 流重组可帮助检测扩散到一系列数据包中的攻击，其方法为将数据包重组为一个完整的数据包流，并执行流分析。TCP 流量规范化提供检测攻击的其他技术，包括高级标志和选项检查、检测重新传输的数据包中有无数据篡改、TCP 数据包校验和验证等。 您可以使用全局配置命令中的 **set connection advanced-options** 以及 **tcp-map** 全局配置命令来配置可扩展的 TCP 安全策略。
出站低延迟队列 (LLQ) 和策略	此功能通过支持低延迟队列 (LLQ) 和流量策略（支持使用端到端网络QoS策略的功能），支持具有严格服务质量 (QoS) 要求的应用。当此功能启用时，每个接口将维护两个出站流量队列：一列用于延迟敏感性流量（例如语音或市场数据），另一列用于延迟宽容性流量（例如文件传输）。通过一系列配置参数可优化队列性能。 QoS 功能使用以下命令进行管理：**police**、**priority**、**priority-queue**、**queue-limit** 和 **tx-ring-limit**。
应用检测功能	

功能	说明
高级 HTTP 检测引擎	此功能引入了 Web 流量深入分析功能，支持 HTTP会话精细控制，以便加强防御各种基于Web 的攻击。此外，新 HTTP 检测引擎允许对即时消息应用、点对点文件共享应用以及试图通过端口 80 或用于HTTP 事务的任何端口进行隧道传输的应用执行管理控制。提供的功能包括RFC 合规性实施、HTTP 命令授权和实施、响应验证、多用途互联网邮件扩展(MIME)类型验证和内容控制、统一资源标识符 (URI) 长度实施等。 用户可以使用 **http-map** 全局配置命令定义高级 HTTP 检测策略，再将其应用于 **inspect http** 配置模式命令（该命令已扩展为支持指定映射名称）。
FTP 检测引擎	此功能包括支持新命令过滤的FTP 检测引擎。版本 7.0 基于以前支持的 FTP 安全服务（例如协议异常检测、协议状态跟踪、NAT/PAT 支持和动态端口打开）构建，使管理员能够精细地控制 9 种不同 FTP 命令的使用，从而执行用户/组在 FTP 会话中可执行的操作。另外，版本 7.0 还引入了 FTP 服务器掩蔽功能，可对通过 ASA 访问 FTP 服务器的用户隐藏服务器的类型和版本。
ESMTP 检测引擎	此功能基于 SMTP (RFC 821) 功能构建，并添加了对 SMTP (ESMTP) 协议的支持，该协议包含 RFC 1869 中定义的各种命令。支持的命令包括 **AUTH**、**DATA**、**EHLO**、**ETRN**、**HELO**、**HELP**、**MAIL**、**NOOP**、**QUIT**、**RCPT**、**RSET**、**SAML**、**SEND**、**SOML** 和 **VRFY**（所有其他命令将会自动锁定，以提高安全性）。 **inspect esmtp** 全局配置命令为 SMTP 和 ESMTP 流量提供检测服务。
SunRPC/NIS+ 检测引擎	SunRPC 检测引擎为 NIS+ 和 SunRPC 服务提供更好的支持。具体增强功能包括支持所有三个版本的查找服务 - Portmapper v2 以及 RPCBind v3 和 v4。 使用 **inspect sunrpc** 和 **sunrpc-server** 全局配置命令可配置 SunRPC/NIS+ 检测引擎。

功能	说明
ICMP 检测引擎	此功能引入了 ICMP 检测引擎。此引擎通过提供 ICMP 连接状态跟踪，将回应请求与应答相匹配，从而实现 ICMP 的安全使用。对于 ICMP 错误消息还可运用其他控制，但它们仅适用于已建立的连接。此版本引入了对 ICMP 错误消息执行 NAT 的功能。 使用 **inspect icmp** 和 **inspect icmp error** 命令可配置 ICMP 检测引擎。
适用于移动无线环境的 GTP 检测引擎	此功能引入了一种新的检测引擎来保护使用 GPRS 隧道协议 (GTP) 提供数据包交换数据服务的 3G 移动无线环境。这些新的高级 GTP 检测服务允许移动服务提供商安全地与漫游合作伙伴进行交互，并为移动管理员提供基于 IMSI 前缀和 APN 值等 GTP 特定参数执行过滤的强大功能。这是一项许可功能。 版本 7.0 中引入的新功能是策略映射配置模式下的 **inspect gtp** 命令和 **gtp-map** 全局配置命令。有关 GTP 的详细信息以及配置 GTP 检测策略的详细说明，请参阅《CLI 配置指南》中的“管理 GTP 检测”一节。您可能需要使用 **activation-key** exec 命令来安装 GTP 激活密钥。
H.323 检测引擎	H.323 检测引擎添加了对 T.38 协议的支持，该协议是一项 ITU 标准，支持安全地传输 IP 传真 (FoIP)。支持实时传真和存储转发传真方法。除当前支持的直接呼叫信令 (DCS) 方法之外，H.323 检测引擎还支持网守路由呼叫信令 (GKRCS)。现在，基于 ITU 标准的 GKRCS 支持允许 ASA 处理 H.323 网守之间直接交换的呼叫信令消息。
H.323 版本 3 和 4 支持	此版本支持对 H.323 v3 和 v4 消息执行 NAT 和 PAT，特别是 H.323 v3 在一个呼叫信令通道上包括多个呼叫。
SIP 检测引擎	此功能添加了对基于会话初始协议 (SIP) 的即时消息客户端（例如 Microsoft Windows Messenger）的支持。增强功能包括支持 RFC 3428 和 RFC 3265 所描述的功能。
支持使用 SIP 的即时消息	现在，修复 SIP 仅支持 Windows XP 上使用 Windows Messenger RTC 客户端版本 4.7.0105 的即时消息 (IM) 聊天功能。

功能	说明
可配置的 SIP UDP 检测引擎	此功能提供了一种通过 CLI 解决非会话信息协议 (SIP) 数据包使用 SIP UDP 端口时可通过 ASA 而不被丢弃的方案。
MGCP 检测引擎	此功能包括 MGCP 检测引擎，该引擎支持对 MGCP 协议执行 NAT 和 PAT。这样可确保在作为 VoIP 协议包括 MGCP 版本 0.1 或 1.0 的分布式呼叫处理环境中实现无缝安全集成。 用户可在策略映射配置模式下使用 **inspect mgcp** 命令并使用 **mgcp-map** 全局配置命令来配置 MGCP 检测策略。
RTSP 检测引擎	此功能引入了对实时流协议 (RTSP) 的 NAT 支持，它允许流式应用（例如思科 IP/TV、Apple Quicktime 和 RealNetworks RealPlayer）跨 NAT 边界透明地运行。
SNMP 检测引擎	与其他新检测引擎类似，用户可在策略映射配置模式下使用 inspect snmp 命令并使用 snmp-map 全局配置命令来配置 SNMP 检测策略。
适用于 H.323 和 SIP 检测引擎的端口地址转换 (PAT)	此版本添加了对端口地址转换 (PAT) 的支持，由此增强了对现有 H.323 和 SIP 检测引擎的支持。添加对 H.323 和 SIP 执行 PAT 的支持功能后，我们的客户即可使用单个全局地址扩展其网络地址空间。
适用于瘦客户端的 PAT	此功能允许思科 IP 电话与 ASA 范围内配置 PAT 的思科 CallManager 进行通信。在 ASA 后面的瘦客户端 IP 电话通过 VPN 与企业站点中的 CallManager 通信的远程访问环境下，此功能显得尤其重要。
ILS 检测引擎	此功能提供互联网定位器服务 (ILS) 修复，以支持对 ILS 和轻量级目录访问协议 (LDAP) 执行 NAT。另外，通过添加此修复，ASA 还可支持 Microsoft NetMeeting 建立的 H.323 会话。Microsoft NetMeeting、SiteServer 和 Active Directory 产品均可利用 ILS 目录服务来提供终端注册和定位。ILS 支持 LDAP 协议且符合 LDAPv2 规范。

功能	说明
可配置的 RAS 检测引擎	此功能包括用于关闭 H.323 RAS（注册、准许和状态）修复的选项，并可在配置中显示此选项（设置时）。这使客户能够在以下情况下关闭 RAS 修复：没有任何 RAS 流量、不希望检测其 RAS 消息或具有使用 UDP 端口 1718 和 1719 的其他应用。
CTIQBE 检测引擎	此功能也称为 TAPI/JTAPI 修复，包含支持 NAT、PAT 和双向 NAT 的计算机电话接口快速缓冲区编码 (CTIQBE) 协议检测模块。借此，思科 IP SoftPhone 及其他思科 TAPI/JTAPI 应用可成功地与思科 CallManager 协同运行和通信，以便在 ASA 范围内建立呼叫及传送语音流量。 此版本支持 **inspect ctiqbe 2748** 命令。
MGCP 检测引擎	此版本添加了对媒体网关控制协议 (MGCP) 1.0 的支持，使呼叫代理和 VoIP 媒体网关之间的消息能够安全地通过 ASA。 请参阅 **inspect mgcp** 命令。
能够配置 TFTP 检测引擎	能够配置 TFTP 检测引擎来检查 TFTP 协议，并在必要时动态创建连接和转换以允许在 TFTP 客户端和服务器之间传输文件。具体来说，此修复可检测 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)。 **注释** 默认情况下，TFTP 修复处于启用状态。如果使用静态 PAT 来重定向 TFTP 流量，则必须启用 TFTP 修复。
过滤功能	
改进了 URL 过滤性能	此功能通过改进 ASA 和 Websense 服务器之间的通信通道，显著增加了可处理的并发 URL 数量。 现在，现有的 **url-server** 全局配置命令支持使用 **connections** 关键字来指定所用池中的 TCP 连接数。

功能	说明
URL 过滤增强	此版本支持对长达 1159 字节的 URL 执行 N2H2 URL 过滤服务。 对于 Websense，支持对长达 4096 字节的 URL 执行长 URL 过滤。 另外，此版本还提供了一个配置选项来缓冲来自 Web 服务器的响应（如果其响应速度比来自 N2H2 或 Websense 过滤服务服务器的响应速度快）。这样可防止 Web 服务器的响应被加载两次。
IPSec VPN 功能	
不完整的加密映射增强	每个静态加密映射必须定义一个访问列表和一个 IPSec 对等体。如果缺少其中任意一个，加密映射则被视为不完整，系统会显示一条警告消息。系统会跳过尚未与完整加密映射匹配的流量，并尝试下一项。不会对故障切换问候数据包执行不完整的加密映射检查。
Spoke-to-Spoke VPN 支持	此功能通过允许加密的流量进出同一接口，改进了对 Spoke-to-Spoke（以及客户端到客户端）VPN 通信的支持。而且，现在可以在 ASA 的外部接口上终止拆分隧道远程访问连接，由此允许从远程访问用户 VPN 隧道传至互联网的流量通过传入时使用的同一接口传出（应用防火墙规则后）。 **same-security-traffic** 命令搭配支持 Spoke-to-Spoke VPN 的 **intra-interface** 关键字使用时，允许流量进出同一接口。
基于 VPN 的 OSPF 动态路由	OSPF 支持已扩展到支持跨 IPSec VPN 隧道的邻居。这使得 ASA 能够支持跨 VPN 隧道到其他 OSPF 对等体的动态路由更新。OSPF 问候为单播加密形式，以便按符合 RFC 要求的方式沿隧道传输到识别的邻居。 接口配置模式下的 **ospf network point-to-point non-broadcast** 命令将全面的 OSPF 动态路由服务扩展至支持跨 IPSec VPN 隧道的邻居，从而提高了 VPN 连接网络的网络可靠性。

功能	说明
远程管理增强	此功能使管理员能够使用远程 ASA 的内部接口 IP 地址远程管理基于 VPN 隧道的防火墙。实际上，管理员可以为管理访问定义任何 ASA 接口。此功能支持需要动态 IP 地址的 ASDM、SSH、Telnet 和 SNMP 等。此功能明显可使宽带环境受益。
X.509 证书支持	ASA 中显著改进了对 X.509 证书的支持，添加了对 n 层证书链（适用于具有多级证书颁发机构层次结构的环境）、手动注册（适用于具有脱机证书颁发机构的环境）以及 4096 位 RSA 密钥的支持。另外，版本 7.0 还包括对思科 IOS 软件中引入的新证书颁发机构的支持，这是一个轻量级 X.509 证书颁发机构，旨在简化启用 PKI 的站点到站点 VPN 环境的发布。
Easy VPN 服务器	此版本支持思科 Easy VPN 服务器。思科 Easy VPN 服务器旨在实现与当前配置为支持思科 VPN 客户端的 VPN 头端的无缝协同运行，并通过将 VPN 配置集中到思科 Easy VPN 服务器中来最大限度降低客户端的管理开销。思科 Easy VPN 服务器产品的示例包括思科 VPN 客户端 v3.x 和更高版本以及思科 VPN 3002 硬件客户端。 **注释** ASA 已可用作中心站点 VPN 设备，并支持终止远程访问 VPN 客户端。
Easy VPN 服务器负载均衡支持	ASA 5500 ASA 可参与基于集群的集中器负载均衡。它支持 VPN 3000 系列集中器负载均衡，并可自动重定向到使用率最低的集中器。
动态下载备份 Easy VPN 服务器信息	支持下载头端上定义的备份集中器列表。 此功能支持 vpngroup group_name **backup-server** {{ip1 [*ip2... ip10*]} | **clear-client-cfg**} 命令。

功能	说明
Easy VPN 互联网访问策略	对于用于受保护网络中用户的互联网访问策略，ASA 可更改用作 Easy VPN 远程设备的 ASA 行为。在 Easy VPN 服务器上启用拆分隧道时会出现新行为。拆分隧道功能允许通过 ASA 连接的用户以明文会话形式访问互联网，而无需使用 VPN 隧道。 用作 Easy VPN 远程设备的 ASA 在首次连接到 Easy VPN 服务器时，会下载拆分隧道策略并将其保存到本地闪存中。如果该策略启用了拆分隧道，则连接到受 ASA 保护的网络的用户可以连接互联网，而不考虑连接 Easy VPN 服务器的 VPN 隧道的状态。
验证证书可分辨名称	此功能使充当站点到站点 VPN 对等体或远程访问部署中 Easy VPN 服务器的自适应安全设备能够验证证书是否与管理员指定的标准相匹配。
用于手动隧道控制用户验证和隧道状态的 Easy VPN Web 界面	通过引入用户级别身份验证和安全设备身份验证，ASA 能够提供使用新网页（当用户尝试通过 ASA 访问 VPN 隧道或未受保护的网络时对其提供）输入凭证、连接/断开隧道以及监控连接的功能。此功能仅适用于 Easy VPN 服务器功能。
用户级别身份验证	支持单独对 ASA 内部网络中的客户端进行身份验证（基于 IP 地址）。支持静态身份验证和一次性密码 (OTP) 身份验证机制。通过基于 Web 的界面完成身份验证。 此功能添加了对 **vpn-group-policy** 命令的支持。
安全设备身份验证	通过此功能，可以使用动态生成的身份验证凭证对 Easy VPN 远程（VPN 硬件客户端)）设备进行身份验证。
灵活的 Easy VPN 管理解决方案	使用外部接口管理 ASA 不需要流量流过 VPN 隧道。您可以灵活地选择要求所有 NMS 流量流过隧道或调整此策略。
VPN 客户端安全评估实施	此功能引入了在发起 VPN 连接时执行 VPN 客户端安全评估检查的功能。这些功能包括强制使用基于授权主机的安全产品（例如思科安全代理）以及验证其版本号、策略和状态（启用/禁用）。 要设置 IKE 隧道协商期间安全设备推送到 VPN 客户端的个人防火墙策略，请在组策略配置模式下使用 **client-firewall** 命令。

功能	说明
VPN 客户端更新	要配置和更改 **client update** 参数，请在隧道组 ipsec 属性配置模式下使用 client-update 命令。
根据操作系统和类型阻止 VPN 客户端	此功能添加了根据客户端类型、安装的操作系统版本和 VPN 客户端软件版本限制允许连接的不同VPN客户端类型（软件客户端、路由器、VPN 3002 和 PIX）的功能。当不符合要求的用户尝试连接时，系统可将它们定向到专门允许不符合要求的用户连接的组。 要通过 ASA 配置可通过 IPSec 连接的远程访问客户端类型和版本的限制规则，请在组策略配置模式下使用 **client-access-rule** 命令。
Movian VPN 客户端支持	此功能引入了对基于手持设备（PocketPC 和 Palm）的 Movian VPN 客户端的支持，从而将网络访问安全扩展到了移动员工和业务合作伙伴。 版本 7.0 中新添加了对使用 Diffie-Hellman 组 7 (ECC) 协商完美前向保密的支持。此选项旨在用于 MovianVPN 客户端，但也可用于支持 D-H 组 7 (ECC) 的其他客户端。
VPN NAT 透明度	此功能将对站点到站点 VPN 和基于远程访问 IPSec 的 VPN 的支持扩展到了实施 NAT 或 PAT 的网络环境，例如机场、酒店、无线热点和宽带环境。另外，版本7.0还添加了支持使用思科TCP和用户数据报协议(UDP)NAT遍历方法作为当前支持的 IETF UDP 封装机制补充方法的功能，以便安全地穿过 NAT/PAT 边界。 有关配置 NAT 遍历策略时的其他选项，请参阅 **isakmp** 全局配置命令。
IKE 系统日志支持	此功能引入了一项小的IKE系统日志记录增强功能，并引入了少量IKE事件跟踪功能以实现可扩展的 VPN 故障排除。添加这些增强功能是为了允许生成新的系统日志消息和改进ISAKMP命令控制。
Diffie-Hellman (DH) 组 5 支持	此版本支持已被赋予组5标识符的1536位MODP组。
高级加密标准 (AES)	此功能添加了对使用新国际加密标准安全连接站点到站点 VPN 及远程访问 VPN 的支持。此外，它还通过新的 VAC+ 卡对所有支持的 ASA 型号和硬件加速 AES 提供基于软件的 AES 支持。

功能	说明
使用地址池分配网络掩码的新功能	此功能引入了为每个地址池定义子网掩码及将这些信息传递到客户端的功能。
加密引擎已知应答测试 (KAT)	KAT 的功能是测试 ASA 加密引擎的实例化。每次 ASA 启动时，在从闪存中读取配置之前都会执行该测试。针对适用于 ASA 中当前许可证的加密算法运行 KAT。
自定义备份集中器超时	此功能会为 ASA 尝试连接 VPN 头端建立一个可配置的超时设置，由此控制滚动到列表中的下一个备份集中器所涉及的延迟。 此功能支持 **vpngroup** 命令。
WebVPN 功能	
通过网络浏览器进行远程访问 (WebVPN)	版本 7.0(1) 在单一路由模式下对 ASA 5500 系列安全设备支持 WebVPN。WebVPN 使用户能够通过网络浏览器与安全设备建立安全的远程访问 VPN 隧道。无需软件或硬件客户端。WebVPN 几乎支持从可连接 HTTPS 互联网站点的任何计算机轻松访问各种 Web 资源和启用 Web 的应用与传统应用。WebVPN 使用安全套接字层协议及其后继传输层安全性协议 (SSL/TLS1)，在远程用户与您在中心站点上配置的特定受支持内部资源之间提供安全连接。安全设备可识别需要代理的连接，并且 HTTP 服务器可与身份验证子系统交互以对用户进行身份验证。
CIFS	WebVPN 支持通用互联网文件系统，该协议允许远程用户浏览和访问中心站点上预先配置的 NT/Active Directory 文件服务器和共享。CIFS 基于 TCP/IP 运行，并使用 DNS 和 NetBIOS 进行名称解析。
端口转发	WebVPN 端口转发也称为应用访问，允许远程用户使用基于 SSL VPN 连接的 TCP 应用。

功能	说明
邮件	WebVPN 支持多种邮件使用方式，包括 IMAP4S、POP3S、SMTPS、MAPI 和网络邮件。 • IMAP4S、POP3S、SMTPS WebVPN 允许远程用户基于 SSL 连接使用 IMAP4、POP3 和 SMTP 邮件协议。 • MAPI 代理 WebVPN 支持 MAPI，即通过 MS Outlook Exchange 端口转发远程访问邮件。必须在远程计算机上安装 MS Outlook Exchange。 • 网络邮件 网络邮件是适用于 Exchange 2000、Exchange 5.5 和 Exchange 2003 的 MS Outlook Web Access。它需要在中心站点上安装 MS Outlook Exchange 服务器。
路由功能	
IPv6 检测、访问控制和管理	此功能引入了对 IP 版本 6 (IPv6) 检测、访问控制和管理的支持。在专用 IPv6 模式和双堆栈 IPv4/IPv6 模式下，对于通过设备的 IPv6 流量提供完全的状态检测。另外，也可以将 ASA 部署在纯 IPv6 环境下，以便对 SSHv2、Telnet、HTTP 和 ICMP 等协议支持 IPv6 传入管理流量。版本 7.0 中支持 IPv6 流量的检测引擎包括 HTTP、FTP、SMTP、UDP、TCP 和 ICMP。
DHCP 选项 66 和 150 支持	此功能在 ASA 内部接口上增强了 DHCP 服务器，以便向服务的 DHCP 客户端提供 TFTP 地址信息。此实施会用一个 TFTP 服务器对 DHCP 选项 66 查询做出响应，并且最多用两个服务器对 DHCP 选项 150 查询做出响应。 DHCP 选项 66 和 150 通过提供下载其余 IP 电话配置所需的思科 CallManager 联系信息，简化了思科 IP 电话和思科 SoftPhone 的远程部署。

功能	说明
多个接口上的 DHCP 服务器支持	此版本允许根据需要配置多个集成动态主机配置协议 (DHCP) 服务器，并可使用任何接口。DHCP 客户端只能在外部接口上配置，而 DHCP 中继代理可以在任何接口上配置。不过，不能在同一个 ASA 上同时配置 DHCP 服务器和 DHCP 中继代理，但可以同时配置 DHCP 客户端和 DHCP 中继代理。 修改了以下命令：**dhcpd address**。
组播支持	添加了 PIM 稀疏模式，以允许使用 PIM-SM 直接参与创建组播树。此功能扩展了当前对 IGMP 转发以及 D 类访问控制策略和 ACL 的组播支持。PIM-SM 为组播环境下的透明模式操作提供了一种备选方案。 除此功能中的 **show mrib** EXEC 命令之外，**pim** 命令和 **multicast-routing** 命令也添加了对该新功能的支持。
接口功能	
多个接口的通用安全级别	此功能使多个接口能够共享某个通用安全级别，从而扩展了安全级别策略结构。通过允许使用通用安全策略的接口（例如，连接到同一 DMZ 的两个端口或网络中的多个区域/部门）共享某个通用安全级别，可以简化策略部署。由每个接口上的 ACL 管理安全级别相同的接口之间的通信。 请参阅 **same-security-traffic** 命令和 **inter-interface** 关键字，以便在配置相同安全级别的接口之间启用流量。
show interface 命令	**show interface** 命令具有显示缓冲区计数器。
专用带外管理接口	在接口配置模式中引入了 **management-only** 配置命令，以使专用带外管理能够访问设备。
GE 硬件速度设置的修改	在 TBI 或 GMII 模式下，可通过硬件配置千兆位以太网卡。TBI 模式不支持半双工。GMII 模式支持半双工和全双工。系统为 TBI 配置了 ASA 中使用的所有 i8255x 控制器，因此它们无法支持半双工模式，故而删除了半双工设置。

功能	说明
基于 VLAN 的虚拟接口	802.1Q VLAN 支持可灵活地管理和调配 ASA。此功能允许分离 IP 接口与物理接口（使得可以不考虑安装的接口卡数来配置逻辑 IP 接口），并提供处理 IEEE 802.1Q 标记的适当方法。 引入了以下命令：**vlan**。
NAT 功能	
可选地址转换服务	此功能消除了先前允许网络流量传输需要地址转换策略的要求，从而简化了 ASA 部署。现在，只有需要地址转换的主机和网络才需要配置地址转换策略。此功能引入了一个新配置选项“nat-control”，允许以增量方式启用 NAT。 版本 7.0 引入了 **nat-control** 命令，并保留了客户当前从以前软件版本升级的行为。对于新安全设备或已清除配置的设备，默认情况下流量遍历安全设备不需要 NAT 策略。
高可用性功能	
支持非对称路由的主用/主用故障切换	此功能基于屡获殊荣的 ASA 高可用性架构构建，其中引入了对主用/主用故障切换的支持。这使得两个 UR 许可的 ASA 或一个 UR 许可的 ASA 与一个 FO-AA 许可的 ASA 可作为故障切换对，两者皆可主动传输流量，并支持非对称路由。主用/主用故障切换功能利用此软件版本的安全情景功能，其中故障转移对中的每个 ASA 皆在一个情景中为主用设备，而在另一个情景中为备用设备，呈反向对称对的形式。我们在版本 7.0 中解决的另一重大客户挑战是非对称路由支持。这使得采用高级路由拓扑（其中数据包从一个 ISP 传入，而通过另一个 ISP 传出）的客户能够部署 ASA 来保护这些环境（利用版本 7.0 中引入的非对称路由支持）。 为了支持主用/主用功能，**failover active** 命令通过 **group** 关键字进行了扩展，而且此软件版本引入了故障切换组配置模式。另外，接口配置模式下的 **asr-group** 命令将主用/主用解决方案扩展到了支持非对称路由的环境。

功能	说明
VPN 状态故障切换	此功能引入了对 VPN 连接执行状态故障切换的功能，从而为屡获殊荣的防火墙故障切换服务提供了补充。所有安全关联 (SA) 状态信息和重要材料可在故障切换对成员之间自动同步，从而提供高度灵活的 VPN 解决方案。 当设备在单路由模式下运行时，系统将隐式启用 VPN 状态故障切换。除 **show failover** EXEC 命令（包括 VPN 状态故障切换操作和统计信息的详细视图）之外，**show isakmp sa**、**show ipsec sa** 和 **show vpnd-sessiondb** 命令也包括有关主用和备用设备中隧道的信息。
故障切换增强	此功能增强了故障切换功能，以便可以将 ASA 故障转移对中的备用单元配置为使用虚拟 MAC 地址。这样就消除了连接到 ASA 故障切换对的设备可能出现“过时”ARP 条目的问题，而故障切换对中的两个 ASA 同时遇到故障，仅备用设备保持运行的情况不太可能出现。
show failover 命令	此新功能增强了 **show failover** 命令，以显示最后进行的故障切换。
对 HTTP 的故障切换支持	此功能支持 **failover replicate http** 和 **show failover** 命令，允许在状态故障切换环境下对 HTTP 会话执行状态复制： 当 HTTP 复制启用时，**show failover** 命令会显示 **failover replicate http** 命令。
不间断软件升级	此功能为客户引入了以下功能：可对故障切换对执行软件升级，而不会影响网络正常运行或流过设备的连接。版本 7.0 引入了在 ASA 故障转移对之间共享版本间状态的功能，使客户能够对维护版本执行软件升级（例如，从版本 7.0(1) 升级到 7.0(2)），而不会影响流过故障切换对的流量（在故障切换对未过度订用的主用/备用故障切换环境或主用/主用环境下，过度订用是指每个对成员的负载超过 50%）。

功能	说明
常规高可用性增强	此功能包括对故障切换操作和配置的许多重大增强，以便更快地完成故障切换过渡、提高可扩展性乃至增强故障切换操作。 该版本引入了以下新命令：**failover interface-policy**、**failover polltime** 和 **failover reload-standby**。
故障排除和监控功能	
改进了 SNMP 支持	此功能添加了对 SNMPv2c 的支持，提供包括 64 位计数器在内的新服务（有利于千兆位以太网接口上的数据包计数器）以及对批量 MIB 数据传输的支持。另外，版本 7.0 还包括 SNMPv2 MIB (RFC 1907) 和 IF-MIB（RFC 1573 和 2233）以及思科 IPSec 流监控 MIB，使您可以全面了解 VPN 流统计信息，包括隧道正常运行时间、传输的字节/数据包数等。
通过 SNMP 监控 CPU 使用率	此功能支持通过 SNMP 监控 ASA 的 CPU 使用率。在 ASA 中，通过 **show cpu** [**usage**] 命令仍可直接查看 CPU 使用信息，但 SNMP 可提供与其他网络管理软件的集成功能。
SNMP 增强	**SNMP mib-2.system.sysObjectID** 变量中添加了对特定于 ASA 平台的对象 ID 的支持。这使得 ASA 中能够支持 CiscoView。
闪存中的堆栈跟踪	此功能支持将堆栈跟踪存储在非易失性闪存中，以便日后进行调试/故障排除时可以检索到它们。
ICMP Ping 服务	此功能引入了几种 ping 附加服务（ICMP 回应），包括对 IPv6 地址的支持。另外，**ping** 命令还支持扩展的选项，包括 data pattern、df-bit、repeat count、datagram size、interval、verbose output 和 sweep range of sizes。 现有 **ping** EXEC 命令已通过各种关键字和参数进行了扩展，以帮助解决网络连接问题。另外，它还支持交互式操作模式。

功能	说明
系统运行状况监控和诊断服务	此功能改进了对系统操作的监控，并有助于隔离潜在的网络和 ASA 问题。**show resource** 和 **show counters** 命令提供有关设备和安全情景资源利用率的详细信息以及详细的统计信息。要监控CPU使用率，您可以使用新的 **show cpu** EXEC 命令以及 **show process cpu-hog** EXEC 命令。为了隔离潜在的软件缺陷，该软件引入了 **checkheaps** 命令和相关的 show EXEC 命令。最后，为了更好地了解块（数据包）的利用率，**show blocks** EXEC 命令提供有关系统中块队列和利用率的各种分析工具。
调试服务	**debug** 命令进行了改进，并针对各种调试支持添加了许多新功能。而且，现在对于所有虚拟终端均支持调试输出，没有任何限制。也就是说，当您对某个特定功能启用调试输出时，您将能够不受任何限制地查看输出。当然，输出仅限于启用它的会话。最后，用户可以使用 **logging** 命令通过系统日志发送调试输出（如果您的安全策略允许且您希望这样做）。
SSL 调试支持	**debug** 命令中添加了对安全套接字层 (SSL) 协议的支持。SSL 是用于对客户端和服务器（例如 ASDM 和 ASA）之间的通信进行身份验证和加密的协议。
数据包捕获	此版本支持数据包捕获。ASA 数据包捕获提供嗅探或“查看”ASA 接受或阻止的任何流量的功能。捕获数据包信息后，您可以选择以下操作：在控制台上查看信息、使用 TFTP 服务器通过网络将其传输到文件中或使用安全 HTTP 通过网络浏览器访问信息。不过，ASA 不会捕获同一网段中与自身无关的流量，而且此数据包捕获功能不支持文件系统、DNS 名称解析或混杂模式。 现在，用户可以指定使用 **capture** 命令将数据包捕获存储在循环缓冲区中。捕获将持续向缓冲区中写入数据包，直到被管理员停止。 ASA 引入了其他支持以改进用户诊断设备操作的能力，它支持捕获 ISAKMP 流量以及仅捕获新加速安全路径 (ASP) 丢弃的数据包的功能。 现有的 **capture** 命令通过新的 **type** 关键字和参数进行了扩展，以便捕获 ISAKMP、丢包和与指定原因字符串匹配的丢包。

功能	说明
show tech 命令	此功能增强了当前的 **show tech** 命令输出，以包含其他诊断信息。
管理功能	
在闪存中存储多个配置	此版本在ASA中推出了一个新的闪存文件系统，使管理员能够在安全设备上存储多个配置。这使您可以在配置错误的情况下执行配置回滚。引入了在此新文件系统中管理文件的命令。 注释 新的闪存文件系统不仅能够存储配置文件，而且还可以在闪存空间充足时存储多个系统映像和多个 PIX 映像。 **boot config** 全局配置命令提供指定启动时应使用哪个配置文件的功能。
安全资产恢复	此功能引入了在 ASAs 配置中没有 **service password recovery** 命令的情况下，阻止恢复配置数据、证书和重要材料的功能（但仍允许客户恢复资产）。此功能有利于物理安全可能不太理想的环境，并可防止恶意用户获取敏感配置数据的访问权限。
计划性系统重新加载（重新启动）	现在，管理员可以在特定时间或按与当前时间的一定偏差安排 ASA 系统重新加载，由此使得更易于安排网络停机时间及通知远程访问 VPN 用户即将进行重新启动。
命令行界面 (CLI) 可用性	此功能增强了 CLI“用户体验”，加入了许多常见的思科 IOS 软件命令行服务（例如命令完成、在线帮助及别名），从而改进了易用性和公共用户体验。
命令行界面 (CLI) 激活密钥管理	此功能让您可以通过 ASA 命令行界面 (CLI) 输入新的激活密钥，而无需使用系统监控模式并对新映像执行 TFTP。此外，当您输入 **show version** 命令时，ASA CLI 将显示当前运行的激活密钥。
show version 命令	现在，**show version** 命令输出包含两个与接口相关的行：最大物理接口数和最大接口数。最大接口数指物理接口和虚拟接口的总数。
AAA 功能	

功能	说明
AAA 集成	版本 7.0(1) 可与身份验证服务实现本机集成，其中包括 Kerberos、NT 域和 RSA SecurID（无需单独的 RADIUS/TACACS+ 服务器），以简化 VPN 用户身份验证。另外，此版本还引入了生成 TACACS+ AAA 会计记录的功能，以便跟踪 ASA 管理访问以及在管理会话期间进行的所有配置更改。
用于管理访问的 AAA 回退	此功能引入了对请求进行身份验证和授权请求回退到 ASA 本地用户数据库的功能。要求和设计将会考虑未来与思科 IOS 软件（例如对 ASA 的“方法列表”支持）兼容的因素，并添加了 LOCAL 回退方法。
AAA 集成增强	此功能推出了与身份验证服务的本机集成，包括 Kerberos、LDAP 和 RSA SecurID（无需单独的 RADIUS/TACACS+ 服务器），以简化用户和管理员身份验证。另外，此功能还引入了生成 TACACS+AAA 会计记录的功能，以便跟踪 ASA 管理访问以及在管理会话期间进行的所有配置更改。
安全超文本传输协议 (HTTPS) 身份验证代理	此功能扩展了 ASA 的功能以安全地执行 HTTP 会话身份验证，并添加了对 HTTPS 身份验证代理的支持。要配置 HTTP 会话的安全身份验证，请使用 **aaa authentication secure-http-client** 命令。要配置 HTTPS 会话的安全身份验证，请使用 **aaa authentication include https** 或 **aaa authentication include tcp/0** 命令。 在此版本中，包括 **aaa authentication include tcp/0** 命令的配置将继承 HTTPS 身份验证代理功能，通过代码升级到版本 6.3 或更高版本后将默认启用该功能。
可下载的访问控制列表 (ACL)	此功能支持从访问控制服务器 (ACS) 将 ACL 下载到 ASA。这样就可以在 AAA 服务器上配置每用户访问列表以提供每用户访问列表授权，然后即可通过 ACS 将其下载到 ASA。 此功能仅支持 RADIUS 服务器，不支持 TACACS+ 服务器。
用于 AAA 身份验证的新系统日志消息	此功能引入了新的 AAA 系统日志消息，可在用户使用服务端口之前提示其进行身份验证。

功能	说明
Per-user-override	此功能允许用户为 **access-group** 命令指定一个新关键字 per-user-override。当指定了此关键字时，允许与用户关联的每用户访问列表 (per-user access-list)（可通过 AAA 身份验证下载）中的允许/拒绝状态覆盖访问组访问列表 (access-group access-list) 中的允许/拒绝状态。
用于网络和 VPN 访问的本地用户身份验证数据库	此功能允许使用 ASA 本地用户名数据库（作为当前通过外部 AAA 服务器进行身份验证的替代方法）对直接转发流量和 VPN（使用 xauth）流量进行身份验证。 现在，server tag 变量接受值 LOCAL，以支持使用本地数据库进行直接转发代理身份验证。
ASDM 功能	
动态控制面板（ASDM 主页）	• 显示详细的设备和许可信息，以便快速识别可用的系统和资源。 • 显示实时系统和流量分析。
实时日志查看器	• 显示实时系统日志消息。 • 高级过滤功能，使您可以轻松地关注重要事件。
改进了基于 Java Web 的架构	• 通过优化的小应用程序缓存功能加速 ASDM 加载。 • 可随时随地访问所有管理和监控功能。
可下载的 ASDM 发射器（仅支持 Microsoft Windows 2000 或 XP 操作系统）	• 允许您在 PC 上本地下载和运行 ASDM。 • 通过 ASDM 发射器的多个实例，可从同一管理工作站同时对多个安全设备执行管理访问。 • 根据设备上安装的版本自动更新软件，从而在整个网络范围内实现一致的安全管理。
支持多种语言操作系统	支持英语和日语版本的 Microsoft Windows 操作系统。