思科 ASA 简介

思科 ASA 在一台设备以及带附加模块的集成服务中提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。

硬件和软件兼容性

有关受支持硬件和软件的完整列表，请参阅《思科 ASA 兼容性》。

VPN 兼容性

请参阅受支持的 VPN 平台（思科 ASA 系列）。

新增功能

本部分列出了每个版本的新功能。

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。

ASA 9.16(2) 中的新增功能

发布日期：2021 年 8 月 18 日

此版本中无新增功能。

ASA 9.16(1)

发布日期：2021 年 5 月 26 日

特性	说明
防火墙功能	
新增的系统定义的 NAT 规则的第 0 部分。	向 NAT 规则表添加了新的第 0 部分。此部分专门供系统使用。系统正常运行所需的任何 NAT 规则都添加到此部分，这些规则优先于您创建的任何规则。以前，系统定义的规则添加到第 1 部分，用户定义的规则可能会干扰系统的正常运行。您无法添加、编辑或删除第 0 部分中的规则，但您会在 **show nat detail** 命令输出中看到这些规则。
默认 SIP 检测策略映射会丢弃非 SIP 流量。	对于 SIP 检查的流量，现在默认为丢弃非 SIP 流量。以前的默认设置是允许在检查 SIP 的端口上允许非 SIP 流量。 我们更改了默认 SIP 策略映射以包含 **no traffic-non-sip** 命令。
能够指定要在 GTP 检测中丢弃的 IMSI 前缀。	通过 GTP 检测，您可以配置 IMSI 前缀过滤，以识别允许的移动国家/地区代码/移动网络代码 (MCC/MNC) 组合。现在，您可以对要丢弃的 MCC/MNC 组合执行 IMSI 过滤。这样，您可以列出不需要的组合，并默认允许所有其他组合。 添加了以下命令：**drop mcc**。
配置初期连接的最大分段大小 (MSS)	您可以配置服务策略，以在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)。这对于还设置初期连接最大值的服务策略非常重要。 新增/修改的命令：**set connection syn-cookie-mss**。
改进了多对一和一对多连接的 CPU 使用率和性能。	系统在创建连接时，不再创建本地主机对象并锁定它们，但涉及动态 NAT/PAT 和扫描威胁检测和主机统计信息的连接除外。在许多连接将连接到同一服务器（例如负载平衡器或 Web 服务器）或一个终端与许多远程主机建立连接的情况下，这会提高性能和 CPU 使用率。 我们更改了以下命令：**clear local-host** （已弃用）、**show local-host**
平台功能	

特性	说明
ASAv 支持 VMware ESXi 7.0	ASAv 虚拟平台支持在 VMware ESXi 7.0 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 7.0 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 上的 Intel QuickAssist 技术 (QAT)	对于使用 Intel QuickAssist (QAT) 8970 PCI 适配器的 ASAv 部署，ASAv 支持硬件加密加速。仅在 VMware ESXi 和 KVM 上支持使用 QAT 的 ASAv 的硬件加密加速。 未修改任何命令。 未修改任何菜单项。
OpenStack 上的 ASAv	ASAv 虚拟平台增加了对 OpenStack 的支持。 未修改任何命令。 未修改任何菜单项。
高可用性和扩展性功能	
群集成员限制	如果您明确知道集群中的设备数少于最大设备数（即 16 台），建议您设置实际计划的设备数。设置最大单位可让群集更好地管理资源。例如，如果您使用端口地址翻译 (PAT)，则控制设备可以将端口块分配给计划的成员数，并且不必为您不打算使用的额外设备预留端口。 新增/修改的命令：**cluster-member-limit**
show cluster history 命令改进	我们为 **show cluster history** 命令添加了其他输出。 新增/修改的命令：**show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
Firepower 1140 最大情景数从 5 增加到 10	Firepower 1140 现在最多支持 10 个情景。
证书功能	
用于认证的安全传输注册 (EST)	ASA 支持使用 Enrollment over Secure Transport (EST) 进行证书注册。但是，您可以配置为仅对 RSA 和 ECDSA 密钥使用 EST 注册。对于为 EST 注册配置的信任点，不能使用 EdDSA 密钥对。 新增/修改的命令：**enrollment protocol**、**crypto ca authenticate** 和 **crypto ca enroll**。
支持新的 EdDSA 密钥	新的密钥选项 EdDSA 已添加到现有 RSA 和 ECDSA 选项中。 新增/修改的命令：**crypto key generate**、**crypto key zeroize**、**show crypto key mypubkey**

特性	说明
覆盖证书密钥限制的命令	不再支持使用 SHA1 和 RSA 加密算法进行认证，并且不再支持 RSA 密钥大小小于 2048 的证书。您可以使用 **crypto ca permit-weak-crypto** 命令覆盖这些限制。 新增/修改的命令：**crypto ca permit-weak-crypto**
管理和故障排除功能	
SSH 安全性改进	SSH 现在支持以下安全性改进： • 主机密钥格式 - **crypto key generate** {**eddsa** | **ecdsa**}. 除了 RSA，我们还增加了对 EdDSA 和 ECDSA 主机密钥的支持。如果密钥存在，ASA 会尝试按以下顺序使用：EdDSA、ECDSA，然后是 RSA。如果使用 **ssh key-exchange hostkey rsa** 命令将 ASA 显式配置为使用 RSA 密钥，则必须生成 2048 位或更高位的密钥。为了实现升级兼容性，仅当使用默认主机密钥设置时，ASA才会使用较小的RSA主机密钥。RSA支持将在更高版本中删除。 • 密钥交换算法 - **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 加密算法 - **ssh cipher encryption** {**chacha20-poly1305@openssh.com** | **aes128-gcm@openssh.com**} • 不再支持 SSH 版本 1 - 已删除 **ssh version** 命令。 新增/修改的命令：**crypto key generate eddsa**、**crypto key zeroize eddsa** 、**show crypto key mypubkey**、**ssh cipher encryption** {**chacha20-poly1305@openssh.com** | **aes128-gcm@openssh.com**}、**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}、**ssh key-exchange hostkey**、**ssh version**
监控功能	
SNMPv3 身份验证	您现在可以使用 SHA-224 和 SHA-384 进行用户身份验证。您不能再使用 MD5 进行用户身份验证。 您不能再使用 DES 进行加密。 新增/修改的命令：**snmp-server user**
VPN 功能	
在静态 VTI 上支持 IPv6	ASA 在虚拟隧道接口 (VTI) 配置中支持 IPv6 地址。 VTI 隧道源接口可以具有 IPv6 地址，您可以将其配置为用作隧道终端。如果隧道源接口有多个 IPv6 地址，您可以指定要使用的地址，否则默认使用列表中的第一个 IPv6 全局地址。 隧道模式可以是 IPv4 或 IPv6，但必须与 VTI 上配置的 IP 地址类型相同，隧道才能处于活动状态。IPv6 地址可以分配给 VTI 中的隧道源或隧道目标接口。 新增/修改的命令：**tunnel source interface**、**tunnel destination**、**tunnel mode**

特性	说明
支持每个设备 1024 个 VTI 接口	要在设备上配置的最大VTI数量已从 100 增加到 1024。 即使平台支持超过 1024 个接口，VTI 计数也限于该平台上可配置的 VLAN 数量。例如，ASA 5510 支持 100 个VLAN，隧道计数为 100 减去配置的物理接口数。 新增/修改的命令：无
在 SSL 中支持 DH 组 15	已为 DH 组 15 添加了对 SSL 加密的支持。 新增/修改的命令：**ssl dh-group group15**
支持 DH 组 31 进行 IPsec 加密	已添加对 DH 组 31 的 IPsec 加密支持。 新增/修改的命令：**set pfs**
支持限制 IKEv2 队列中的 SA	增加了支持以限制 SA-INIT 数据包中的队列数量。 新增/修改的命令：**crypto ikev2 limit queue sa_init**
用于清除 IPsec 统计信息的选项	引入了 CLI 以清除和重置 IPsec 统计信息。 新增/修改的命令：**clear crypto ipsec stats** 和 **clear ipsec stats** 。

防火墙功能概述

防火墙可防止外部网络上的用户在未经授权的情况下访问内部网络。防火墙同时可以为不同的内部网络提供保护，例如将人力资源网络与用户网络分开。如果需要向外部用户提供某些网络资源（例如 Web 服务器或 FTP 服务器），可以将这些资源放置在防火墙后面单独的网络上（这种网络称为隔离区 (DMZ)）。防火墙允许有限访问 DMZ，但由于 DMZ 只包括公共服务器，因此发生在这个位置的攻击只会影响到服务器，而不会影响其他内部网络。还可以通过以下手段来控制内部用户何时可以访问外部网络（例如，访问互联网）：仅允许访问某些地址，要求身份验证或授权，配合使用外部 URL 过滤服务器。

讨论连接到防火墙的网络时，外部网络位于防火墙之前，内部网络可以得到保护，位于防火墙之后，*DMZ* 虽然位于防火墙之后，却可以限制外部用户的访问权限。由于 ASA 允许您配置许多安全策略不同的接口，包括许多内部接口、许多 DMZ 甚至许多外部接口（如果需要），则仅按照常规含义使用这些术语。

安全策略概述

安全策略确定哪些流量可通过防火墙来访问其他网络。默认情况下，ASA 允许流量从内部网络（较高安全性级别）自由流向外部网络（较低安全性级别）。可以将操作应用于流量，以自定义安全策略。

通过访问规则允许或拒绝流量

您可以应用访问规则，以限制从内部到外部的流量，或者允许从外部到内部的流量。对于网桥组接口，还可以应用 EtherType 访问规则来允许非 IP 流量。

应用 NAT

NAT 的一些优势如下：

- 可以在内部网络上使用专用地址。专用地址不能在互联网上进行路由。
- NAT 可隐藏其他网络的本地地址，使攻击者无法获悉主机的真实地址。
- NAT 可通过支持重叠 IP 地址来解决 IP 路由问题。

保护 IP 片段

ASA 提供 IP 片段保护。此功能对所有 ICMP 错误消息执行完全重组，并对通过 ASA 路由的剩余 IP 片段执行虚拟重组。系统会丢弃并记录未能通过安全检查的片段。不能禁用虚拟重组。

应用 HTTP、HTTPS 或 FTP 过滤

虽然可以使用访问列表来防止对于特定网站或 FTP 服务器的出站访问，但由于互联网的规模和动态性质，以这种方式配置和管理网络使用并不切合实际。

可以在 ASA 上配置云网络安全，或者安装提供 URL 和其他过滤服务的 ASA 模块（例如 ASA CX 或 ASA FirePOWER）。您还可以将 ASA 与思科网络安全设备 (WSA) 等外部产品结合使用。

应用应用检测

针对在用户数据包内嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议要求 ASA 执行深度数据包检测。

将流量发送到支持的硬件或软件模块

某些ASA型号允许配置软件模块或者将硬件模块装入到机箱中，以提供高级服务。这些模块提供其他流量检测，并可根据配置的策略来阻止流量。可以将流量发送到这些模块，以利用这些高级服务。

应用 QoS 策略

某些网络流量（例如声音和流传输视频）不允许出现长时间延迟。QoS 是一种网络功能，使您可以向此类流量赋予优先级。QoS 是指一种可以向所选网络流量提供更好服务的网络功能。

应用连接限制和 TCP 规范化

可以限制TCP连接、UDP连接和半开连接。限制连接和半开连接的数量可防止遭受DoS攻击。ASA 通过限制初期连接的数量来触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。半开连接是源与目标之间尚未完成必要握手的连接请求。

TCP 规范化是指一种包含高级 TCP 连接设置的功能，用以丢弃有异常迹象的数据包。

启用威胁检测

可以配置扫描威胁检测和基本威胁检测，还可以配置如何使用统计信息来分析威胁。

基本威胁检测会检测可能与攻击（例如 DoS 攻击）相关的活动，并自动发送系统日志消息。

典型的扫描攻击包含测试子网中每个 IP 地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。ASA 扫描威胁检测功能与基于流量签名的 IPS 扫描检测不同，前者维护着一个广泛的数据库，其中包含可用来分析扫描活动的主机统计信息。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机 IPID 等易受攻击的 TCP 行为以及更多行为）。

您可以将 ASA 配置为发送有关攻击者的系统日志消息，也可以自动避开主机。

防火墙模式概览

ASA 在两种不同的防火墙模式下运行：

- 路由
- 透明

在路由模式下，ASA 被视为网络中的一个路由器跃点。

在透明模式下，ASA 如同是“线缆中的块”或“隐蔽的防火墙”，不被视为路由器跃点。ASA 在“网桥组”中连接至其内部和外部接口上的同一子网。

您可以使用透明防火墙简化网络配置。如果希望防火墙对攻击者不可见，透明模式同样有用。还可以针对在路由模式中会以其他方式被阻止的流量使用透明防火墙。例如，透明防火墙可通过 EtherType 访问列表允许组播数据流。

路由模式支持集成路由和桥接，因此也可以在路由模式下配置网桥组，并在网桥组和普通接口之间路由。在路由模式下，您可以复制透明模式功能；如果您不需要多情景模式或集群，可以考虑改用路由模式。

状态监测概览

系统使用自适应安全算法检测通过 ASA 的所有流量，要么允许通过，要么将其丢弃。简单的数据包过滤器可以检查源地址、目标地址和端口是否正确，但不会检查数据包序列或标记是否正确。过滤器还可以根据过滤器本身检查每个数据包，但这个过程可能比较慢。

注释 TCP 状态绕行功能使您可以自定义数据包流量。

但 ASA 等状态防火墙会考虑数据包的状态：

- 这是新连接吗？

如果是新连接，ASA 必须对照访问列表检查数据包，并执行其他任务以确定允许还是拒绝数据包。为了执行此检查，会话的第一个数据包将通过“会话管理路径”，根据流量类型，它还可能通过“控制平面路径”。

会话管理路径负责执行以下任务：

- 执行访问列表检查
- 执行路由查找
- 分配 NAT 转换 (xlate)
- 在“快速路径”中建立会话

ASA 会在快速路径中为 TCP 流量创建转发和反向流；ASA 还会为无连接协议（例如 UDP、ICMP）创建连接状态信息（启用 ICMP 检测时），以便它们也可以使用快速路径。

注释 对于其他 IP 协议，例如 SCTP，ASA 不会创建反向流路径。因此，涉及这些连接的 ICMP 错误数据包将被丢弃。

需要第 7 层检测的某些数据包（必须检测或改变数据包负载）会传递到控制平面路径。具有两个或多个信道（一个使用已知端口号的数据信道，一个对每个会话使用不同端口号的控制信道，）的协议需要第 7 层检测引擎。这些协议包括 FTP、H.323 和 SNMP。

- 这是已建立的连接吗？

  如果连接已建立，则ASA不需要重新检查数据包；多数匹配的数据包都可以双向通过“快速”路径。快速路径负责执行以下任务：

  - IP 校验和验证
  - 会话查找
  - TCP 序列号检查
  - 基于现有会话的 NAT 转换
  - 第 3 层和第 4 层报头调整

  需要第 7 层检测的协议的数据包也可以通过快速路径。

  某些建立的会话数据包必须继续通过会话管理路径或控制平面路径。通过会话管理路径的数据包包括需要检测或内容过滤的 HTTP 数据包。通过控制平面路径的数据包包括需要第 7 层检测的协议的控制数据包。

VPN 功能概述

VPN 是一个跨 TCP/IP 网络（例如互联网）的安全连接，显示为私有连接。这种安全连接被称为隧道。ASA 使用隧道传输协议协商安全参数，创建和管理隧道，封装数据包，通过隧道收发数据包，

然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。ASA 可调用各种标准协议来完成这些功能。

ASA 可执行以下功能：

- 建立隧道
- 协商隧道参数
- 对用户进行身份验证
- 分配用户地址
- 数据加密和解密
- 管理安全密钥
- 管理隧道范围内的数据传输
- 按隧道终端或路由器方式管理入站和出站数据传输

ASA 可调用各种标准协议来完成这些功能。

安全情景概述

您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个 context 都是一台独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。多情景模式支持很多功能，包括路由表、防火墙功能、IPS 和管理；但是，某些功能不受支持。有关详细信息，请参阅相关功能章节。

在多情景模式中，ASA 包括用于每个情景的配置，其中确定安全策略、接口以及可以在独立设备中配置的几乎所有选项。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，是启动配置。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景类似于任何其他情景，唯一不同之处在于，当用户登录管理情景时，该用户拥有系统管理员权限并能访问系统和所有其他情景。

ASA 集群概述

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。

只能在控制设备上执行所有配置（引导程序配置除外）；然后配置将被复制到成员设备中。

特殊服务和传统服务

对于某些服务，可以在主配置指南和在线帮助以外找到相关文档。

特殊服务指南

特殊服务使 ASA 可以与其他思科产品实现互操作；例如，为电话服务提供安全代理（统一通信），同时提供僵尸网络流量过滤和思科更新服务器上的动态数据库，或者为思科网络安全设备提供 WCCP 服务。某些特殊服务在单独的指南中进行介绍：

- 思科 ASA 僵尸网络流量过滤器指南
- 思科 ASA NetFlow 实施指南
- 思科 ASA 统一通信指南
- 思科 ASA WCCP 流量重定向指南
- SNMP 版本 3 工具实施指南

传统服务指南

ASA 仍支持传统服务，但可能还有更好的替代服务可供使用。传统服务在单独的指南中进行介绍：

思科 ASA 传统功能指南

本指南包含以下章节：

- 配置 RIP
- 适用于网络接入的 AAA 规则
- 使用保护工具，其中包括防止 IP 欺骗 (**ip verify reverse-path**)、配置分段大小 (**fragment**)、阻止不需要的连接 (**shun**)、配置 TCP 选项（适用于 ASDM）以及为基本 IPS 支持配置 IP 审核 (**ip audit**)。
- 配置过滤服务