Cisco Secure Firewall ASA 简介

Cisco Secure Firewall ASA 在一台设备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 9.23(1) 的新功能

发布日期：**2025** 年 **3** 月 **5** 日

功能	说明
平台功能	
Cisco Secure Firewall 1230/1240/1250	Cisco Secure Firewall 1230/1240/1250 是一款 1RU 机架式防火墙。
增加了 Cisco Secure Firewall 4200 的连接限制	已增加连接限制： • 4225: 80M → **90M** • 4245: 80M → **180M**
防火墙功能	
支持 RADIUS Message-Authenticator 属性。	Message-Authenticator 属性用于防御 Blast-RADIUS 攻击。如果已升级 RADIUS 服务器使其支持消息身份验证器，则可以启用此选项来帮助防御这些攻击。启用后，所有请求和响应都必须有消息身份验证器，否则身份验证将失败。 添加了以下命令：**message-authenticator-required**。
新的 Umbrella API。	您现在可以使用 Umbrella 开放 API 来配置 Umbrella，该 API 使用带密钥的 API 密钥。 添加了以下命令：**token-request-credential**
Cisco Secure Firewall 3100/4200 默认启用流量分流	流量分流现已默认启用。 添加/修改的命令：**flow-offload enable**。
高可用性和扩展性功能	
为所有 Cisco Secure Firewall 1200 型号提供多情景支持	我们增加了对 Cisco Secure Firewall 1210/1220 的多情景模式支持： • Cisco Secure Firewall 1210CE - 5 个情景。 • Cisco Secure Firewall 1210CP - 5 个情景。 • Cisco Secure Firewall 1220CX - 10 个情景。 多情景模式中不支持交换机端口，您必须先将所有接口转换为路由器接口，然后才能转换为多情景模式。 在其初始版本中，Cisco Secure Firewall 1230/1240/1250 还支持多情景模式： • Cisco Secure Firewall 1230- 25 个情景。 • Cisco Secure Firewall 1240- 25 个情景。 • Cisco Secure Firewall 1250- 25 个情景。

功能	说明
集群重定向：支持 Cisco Secure Firewall 4200 不对称集群流量的流分流	对于不对称流，集群重定向允许转发节点将流量分流到硬件上。默认情况下启用此功能。 当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。 添加/修改的命令：**flow-offload cluster-redirect**、**show conn**、**show flow-offload flow**、**show flow-offload flow protocol**、**show flow-offload info**。
改进了故障转移期间的角色切换时间	发生故障转移时，新的活动设备会为每个 MAC 地址条目生成组播数据包，并将其发送到所有网桥组接口，从而促使上游交换机更新路由表。生成组播数据包并将其发送到网桥接口的任务现在可以在数据平面中异步运行，从而使控制平面中的关键故障转移任务能够无延迟地进行。 此增强功能可缩短故障转移期间的角色切换时间，并减少停机时间。
集群节点加入时的 MTU ping 测试	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。
接口功能	
Cisco Secure Firewall 1210CP IEEE 802.3bt 支持（PoE++ 和 Hi-PoE）	请参阅以下与 IEEE 802.3bt 支持相关的改进： • PoE++ 和 Hi-PoE - 每个端口最高 90W。 • 单签名和双签名受电设备 (PD)。 • 电源预算遵循先到先得的原则。 • 功率预算字段已被添加到 **show power inline**。 新增/修改的命令： **power inline**、**show power inline**
许可证功能	
ASA Virtual 的灵活永久许可证预留	对于 ASA Virtual，您可以将任何特定型号的许可证配置为永久许可证预留，而与 RAM 和 vCPU 无关。您可以在永久许可证预留许可证之间切换，而不考虑分配给 ASA Virtual 的内存。您也可以更改分配给 ASA Virtual 的内存和 vCPU，而无需更改型号许可证。 如果将 ASA Virtual 降级到 9.23.1 之前的版本，许可证状态将变为未注册。建议您不要降级具有灵活永久许可证预留的 ASA Virtual。 添加了以下命令：**license smart flex-model**
管理、监控和故障排除功能	

功能	说明
用于 TLS 设备证书的自动化证书管理环境 (ACME)协议	您可以为 ASA 信任点配置自动证书管理环境 (ACME) 协议，以管理 TLS 设备证书。ACME 使ASA 能够通过自动续订、域验证以及轻松注册和撤销证书来简化证书管理。您可以选择使用 Let's Encrypt CA 服务器或使用任何其他 ACME 服务器进行身份验证。ACME 使用 http01 方法进行身份验证。 未修改任何命令。 **crypto ca trustpoint enrollment protocol crypto ca authenticate**
VPN 功能	
通过 Cisco Secure Firewall 4200 上的集群支持分布式站点间 VPN	Cisco Secure Firewall 4200 上的 ASA 集群在分布式模式下支持站点间 VPN。使用分布式模式能够在 ASA 集群的成员之间分布多个站点间 IPsec IKEv2 VPN 连接，而不仅分布在控制节点上（如集中模式一样）。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。 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 conn detail**、**show crypto ikev2 stats**
在分布式站点间 VPN 模式下，对 Cisco Secure Firewall 4200 上的集群控制链路上的流量进行 IPsec 流分流	对于分布式站点间 VPN 模式中的不对称流量，IPsec 流分流现在可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，启用 IPsec 流分流后始终可用。 添加/修改的命令：**flow-offload-ipsec**、**show crypto ipsec sa detail**。

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。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。

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。

防火墙模式概述

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。

状态监测概述

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

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。