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 9.20(2) 的新功能

发布日期：**2018** 年 **7** 月 **2** 日

功能	说明
许可证功能	
Smart Transport 是默认的智能许可传输	智能许可现在使用 Smart Transport 作为默认传输。如有必要，可以选择启用前一种类型 Smart Call Home 。 新增/修改的命令：**transport proxy**、**transport type**、**transport url** 同样适用于 *9.22(1)*。
管理、监控和故障排除功能	
SSH X.509 证书身份验证	现在，您可以使用 X.509v3 证书对 SSH 用户进行身份验证 (RFC 6187)。 **注释** Firepower 4100/9300 上的容器实例不支持此功能。 **注释** 捆绑版本的 ASDM 7.20(4) 不包括对此功能的支持。从 Cisco.com 下载并安装 ASDM 7.20(4) 以获得功能支持。如果要覆盖捆绑版本，请务必将映像名称更改为 asdm.bin。 新增/修改的命令：**aaa authorization exec ssh-x509**、**ssh authentication method**、**ssh trustpoint sign**、**ssh username-from-certificate**、**validation-usage ssh-client**
AES-256-GCM SSH 密码	ASA 支持用于 SSH 的 AES-256-GCM 密码。默认情况下，此功能对 **所有** 加密级别和 **高** 加密级别启用。 新增/修改的命令：**ssh cipher encryption**

ASA 9.20(3) 的新功能

发布日期：**2024** 年 **7** 月 **31** 日

功能	说明
平台功能	

功能	说明
ASA Virtual AWS IMDSv2 支持	ASA Virtual 现在支持 AWS 实例元数据服务版本 2 (IMDSv2) API，允许检索和验证实例元数据。IMDSv2 针对以实例元数据服务为目标的漏洞提供额外的安全保护。在 AWS 上部署 ASA Virtual 时，您现在可以为 ASA Virtual 配置元数据版本，如下所示： • ASA Virtual 9.20(3) 及更高版本仅支持 IMDSv2（需要令牌）- 设置“仅 V2（需要令牌）”以启用 IMDSv2。 • 较早的 ASA Virtual 版本仅通过 IMDS 选项支持 IMDSv1 API -“IMDSv1 或 IMDSv2（令牌可选）”- 设置“V1 和 V2（令牌可选）。 如果您有现有的 ASA Virtual 部署，则可以在升级到 9.20(3) 及更高版本后迁移到“需要 IMDSv2”模式。请参阅 AWS 文档：https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html 有关详细信息，请参阅《Cisco Secure Firewall ASA Virtual 入门指南，9.20》。
防火墙功能	
适用于 VPN 服务的威胁检测	您可以为 VPN 服务配置威胁检测，以防止来自 IPv4 地址的以下类型的 VPN 攻击： • 远程访问 VPN 验证尝试失败过多，例如用户名/密码暴力扫描。 • 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。 • 尝试访问无效的 VPN 服务，即仅供内部使用的服务。 这些攻击即使未能成功获取访问权，也会消耗计算资源，有时甚至会导致拒绝服务。 引入或更改了以下命令：**clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service**。
VPN 功能	
webvpn配置和隧道组中的多个IdP证书	现在可以在 webvpn 配置中配置特定于隧道组的 IdP 证书和多个 IdP 证书。此功能可让您信任旧证书和新证书，从而更容易迁移到新证书。 新增/修改的命令： **saml idp-trustpoint**、**trustpoint idp**
预身份验证 SSL 连接的速率限制	ASA Virtual 可以限制预身份验证 SSL 连接的速率。此限制按设备 VPN 连接限制的三倍计算。超过此限制后，将不允许新的 SSL 连接。只有当预身份验证的 SSL 连接计数为零时，设备才允许新的 SSL 连接。但这一限制不适用于管理连接。 新增/修改的命令：**show counters**

ASA 9.20(2) 的新功能

发布日期：**2023** 年 **12** 月 **13** 日

功能	说明
平台功能	
支持 100GB 网络模块的 Cisco Secure Firewall 3100	您现在可以使用支持 100GB 网络模块的 Cisco Secure Firewall 3100。Cisco Secure Firewall 4200 也支持此模块。
增加了 Cisco Secure Firewall 4200 的连接限制	已增加连接限制： • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
OCI 上的 ASAv：其他实例	OCI 上的 ASA Virtual 实例现在支持其他形状，以实现最高性能和吞吐量级别。
高可用性和扩展性功能	
Azure 上的 ASAv：使用网关负载均衡的集群	我们现在支持使用 Azure 资源管理器 (ARM) 模板在 Azure 上部署 ASA Virtual 集群，然后将 ASA Virtual 配置为使用网关负载均衡器 (GWLB) 来实现网络流量负载均衡。 新增/修改的命令：
AWS 上的 ASAv：采用网关负载均衡的集群恢复能力	您可以在 AWS 的目标组服务中配置目标故障转移选项，这有助于 GWLB 在发生虚拟实例故障转移时将现有流转发到正常运行的目标。在 ASAv 集群中，每个实例都与一个目标组关联，其中目标故障转移选项已启用。它可帮助 GWLB 识别运行状况不佳的目标，并将网络流量重定向或转发到在目标组中识别或注册为目标节点的正常运行的实例。
机箱心跳故障后重新加入集群的可配置延迟 (Firepower 4100/9300)	默认情况下，如果机箱心跳失败然后恢复，则节点会立即重新加入集群。但是，如果配置 **health-check chassis-heartbeat-delay-rejoin** 命令，则它将根据 **health-check system auto-rejoin** 命令的设置重新加入。 新增/修改的命令：**health-check chassis-heartbeat-delay-rejoin**
show failover statistics 包含客户端统计信息	故障转移客户端数据包统计信息现在已得到增强，以提高可调试性。 **show failover statistics** 命令已增强，可显示 **np-clients**（数据路径客户端）和 **cp-clients**（控制平面客户端）信息。 修改的命令： **show failover statistics cp-clients**、 **show failover statistics np-clients** 同样适用于 *9.18(4)*。

功能	说明
show failover statistics events 包括新事件	**show failover statistics events** 命令现已增强，可识别应用代理通知的本地故障：故障转移链路正常运行时间、管理引擎心跳故障和磁盘已满问题。 修改的命令： **show failover statistics events** 同样适用于 *9.18(4)*。

ASA 9.20(1)的新功能

发布日期：**2023** 年 **9** 月 **7** 日

注释 此版本仅在 Cisco Secure Firewall 4200 上支持。

功能	说明
平台功能	
Cisco Secure Firewall 4200	我们为 Cisco Secure Firewall 4215、4225 和 4245 引入了 ASA。Cisco Secure Firewall 4200 支持最多 8 个单位的跨区以太网通道集群。您可以在防火墙通电时热插拔相同类型的网络模块，而无需重新启动；进行其他模块更改需要重新启动。Cisco Secure Firewall 4200 25 Gbps 和更高接口支持基于安装的 SFP 的前向纠错和速度检测。SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，则它们会组成软件 RAID。有两个管理接口。
防火墙功能	
ASP 规则引擎编译已卸载到数据平面。	默认情况下，当任何基于规则的策略（例如 ACL、NAT、VPN）具有超过 100 个规则更新时，ASP 规则引擎编译会分流到数据平面（而不是控制平面）。分流为控制平面留出更多时间来执行其他任务。 添加或修改了以下命令：**asp rule-engine compile-offload**、**show asp rule-engine**。
数据平面快速重新加载	如果数据平面需要重新启动，您现在可以重新加载数据平面进程，而无需重新启动设备。在启用数据平面快速重新加载后，它会重新启动数据平面和其他进程。 新增/修改的命令：**data-plane quick-reload**、**show data-plane quick-reload status**。
高可用性和扩展性功能	
减少了 ASA 高可用性的错误故障转移。	现在我们在 ASA 高可用性的数据平面中引入了额外的心跳模块。该心跳模块有助于避免由于控制平面上的流量拥塞或CPU过载而可能发生的错误故障转移或裂脑情况。 同样适用于 *9.18(4)*。

功能	说明
流状态的可配置集群保持连接间隔	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
路由功能	
EIGRPv6	现在，您可以为 IPv6 配置 EIGRP 并单独管理它们。在每个接口上配置 EIGRP 时，必须明确启用 IPv6。 新增/修改的命令：以下是引入的新命令： **ipv6 eigrp**、 **ipv6 hello-interval eigrp**、 **ipv6 hold-time eigrp**、 **ipv6 split-horizon eigrp**、 **show ipv6 eigrp interface** 、 **show ipv6 eigrp traffic**、 **show ipv6 eigrp neighbors** 、 **show ipv6 eigrp interface**、 **ipv6 summary-address eigrp**、 **show ipv6 eigrp topology**、 **show ipv6 eigrp events** 、 **show ipv6 eigrp timers**、 **clear ipv6 eigrp** 和 **clear ipv6 router eigrp** 修改了以下命令以支持 IPv6： **default-metric**、 **distribute-list prefix-list**、 **passive-interface**、 **eigrp log-neighbor-warnings**、 **eigrp log-neighbor-changes**、 **eigrp router-id**和 **eigrp stub**
接口功能	
VXLAN VTEP IPv6 支持	现在，您可以为 VXLAN VTEP 接口指定 IPv6 地址。 ASA Virtual 集群控制链路或 Geneve 封装不支持 IPv6。 新增/修改的命令：**default-mcast-group**、**mcast-group**、**peer ip**
环回接口支持 DNS、HTTP、ICMP 和 IPsec 分流	您现在可以添加环回接口并用于： • DNS • HTTP • ICMP • IPsec 流分流
许可证功能	
用于智能许可和 Smart Call Home 等云服务的 IPv6	ASA 现在支持用于智能许可和 Smart Call Home 等云服务的 IPv6。
证书功能	
用于 OCSP 和 CRL 的 IPv6 PKI	ASA 现在支持 IPv4 和 IPv6 OCSP 和 CRL URL。在 URL 中使用 IPv6 时，必须用方括号将其括起来。 新增/修改的命令：**crypto ca trustpointcrl**、**cdp url**、**ocsp url**

功能	说明
管理、监控和故障排除功能	
SNMP 系统日志的速率限制	如果未设置系统范围的速率限制，那么您现在可以为发送到SNMP服务器的系统日志单独配置速率限制。 新增/修改的命令：**logging history rate-limit**
交换机的数据包捕获	您现在可以配置以捕获交换机的出口和进口流量数据包。此选项仅适用于Cisco Secure Firewall 4200 型号的设备。 新增/修改的命令： **capture** *capture_name* **switch interface** *interface_name* [**direction** { **both** | **egress** | **ingress** }]
VPN 功能	
加密调试增强功能	以下是加密调试的增强功能： • 加密存档现在有两种格式：文本和二进制格式。 • 额外 SSL 计数器。 • 停滞加密规则可从 ASP 表中删除，而无需重新启动设备。 新增/修改的命令： • **show counters**
IKEv2 的多密钥交换	ASA 支持 IKEv2 中的多密钥交换，以保护 IPsec 通信免受量子计算机攻击。 新增/修改的命令：**additional-key-exchange**

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。