高级接口配置

本章介绍如何为接口配置 MAC 地址，如何设置最大传输单元 (MTU)，如何设置最大 TCP 分片大小 (TCP MSS)，以及如何允许相同安全级别通信。设置正确的 MTU 和最大 TCP 分片大小是实现最佳网络性能的关键。

关于高级接口配置

本节介绍高级接口设置。

关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。对于多情景模式，您可以自动生成唯一的 MAC 地址（适用于分配给情景的所有接口）和单情景模式（适用于子接口）。.

注释 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。

- VLAN 接口 (Firepower 1010) - 路由防火墙模式：所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置手动 MAC 地址、MTU 和 TCP MSS，第 6 页。

  透明防火墙模式：各 VLAN 接口均有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置手动 MAC 地址、MTU 和 TCP MSS，第 6 页。

- EtherChannels（Firepower 型号） - 对于 EtherChannel，属于通道组的所有接口均共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

- EtherChannel（ASA 型号）- 端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口配置 MAC 地址。我们建议在组通道接口成员身份更改时，配置唯一的 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。

- 子接口- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

自动 MAC 地址

在多情景模式下，自动生成会为分配给情景的所有接口分配唯一的 MAC 地址。

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址（如果已启用）。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。

由于自动生成的地址（使用前缀时）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

ASA 使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中，*xx.yy* 是用户定义的前缀或根据接口 MAC 地址的最后两个字节自动生成的前缀，*zz.zzzz* 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与 ASA 的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

注释 没有前缀的MAC地址格式是旧式版本。有关传统格式的详细信息，请参阅命令参考中的**mac-address auto** 命令。

关于 MTU

MTU 指定 ASA 在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

对于 VXLAN 或 Geneve，帧中会封装整个以太网数据报，因此新的 IP 数据包更大，需要更大的 MTU：您应该将 ASA VTEP 源接口 MTU 设置为网络 MTU + 54 字节 (对于 VXLAN) 或 + 306 字节 (Geneve)。

路径 MTU 发现

ASA 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。该值不包括 18-22 字节的以太网报头、VLAN 标记和其他开销。

如果在 VTEP 接口上启用 VXLAN，当 MTU 小于 1554 字节时，ASA 会自动将 MTU 提高到 1554 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。一般来说，应将 ASA 源接口 MTU 设置为网络 MTU + 54 字节。

MTU 和分段

对于IPv4，如果传出IP数据包大于指定MTU，则该数据包将分为2帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 TCP 数据包，终端通常使用它们的 MTU 来确定 TCP 最大报文段长度（例如，MTU-40）。如果之后添加额外的 TCP 报头，例如对于站点间的 VPN 隧道，则 TCP MSS 可能需要由隧道传输实体向下调整。请参阅关于 TCP MSS，第 4 页。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，ASA 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的MTU相匹配 - 我们建议将所有ASA接口以及流量路径的其他设备接口上的MTU设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 在启用巨型帧时，MTU 可设置为 9000 字节或更高。最大值取决于型号。

关于 TCP MSS

TCP 最大报文段长度 (MSS) 是 TCP 负载在添加任何 TCP 和 IP 报头前的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

您可以使用 FlexConfig中的 Sysopt_Basic 对象在 ASA威胁防御 FlexConfig 策略#unique_955；默认情况下，最大 TCP MSS 设置为 1380 字节。当 ASA 需要增加数据包长度以执行 IPsec VPN 封装时，此设置非常有用。不过，对于非 IPsec 终端，应在 ASA 上禁用最大 TCP MSS。

如果设置了 TCP MSS 的最大值，当连接的任一终端请求的 TCP MSS 大于 ASA 中设定的值时，ASA 会使用 ASA 最大值覆盖请求数据包中的 TCP MSS。如果主机或服务器没有请求 TCP MSS，ASA 会假定采用 RFC 793 的默认值 536 字节 (IPv4) 或 1220 字节 (IPv6)，但不会修改数据包。例如，可以将默认 MTU 保留为 1500 字节。如果主机请求的 MSS 为 1500 减去 TCP 和 IP 报头长度，这会将 MSS 设置为 1460。如果 ASA 上的最大 TCP MSS 为 1380（默认值），ASA 会将 TCP 请求数据包中的 MSS 值改为 1380。然后，服务器会发送 1380 字节负载的数据包。然后，ASA 可向数据包中增加最多 120 字节的报头，并且仍然符合 1500 的 MTU 大小。

您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

对于流向设备的流量，包括用于 SSL VPN 连接的流量，此设置不适用。ASA 使用 MTU 来推导 TCP MSS：MTU - 40 (IPv4) 或 MTU - 60 (IPv6)。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可达到 120 字节）；此值在默认 MTU（1500 字节）范围内。

建议的最大 TCP MSS 设置

默认 TCP MSS 假定 ASA作为 IPv4 IPsec VPN 终端，并且 MTU 为 1500。当 ASA用作 IPv4 IPsec VPN 终端时，它需要为 TCP 和 IP 报头容纳最多 120 个字节。

如果您要更改 MTU 值、使用 IPv6，或者不使用 ASA作为 IPsec VPN 终端，则应更改 TCP MSS 设置（。

请参阅以下准则：

- 正常流量 - 禁用TCP MSS限制，并接受在连接终端之间建立的值。由于连接终端一般是从MTU获得 TCP MSS，因此非 IPsec 数据包通常符合此 TCP MSS。
- IPv4 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨帧并将 MTU 设置为 9000，则需要将 TCP MSS 设置为 8880，以利用新 MTU。
- IPv6 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 140。

接口间通信

允许同一安全级别的接口之间相互通信具有以下优势：

- 您可以配置超过 101 个通信接口。

  如果您为每个接口使用不同级别，而且不将任何接口分配到同一安全等级，则仅可以为每个级别（0 到 100）配置一个接口。

- 您希望流量能够在同一安全级别的各接口之间自由流动而无需 ACL。

如果启用同一安全级别接口通信，则仍可以照常配置不同安全级别的接口。

接口内通信（路由防火墙模式）

接口间通信可能对从某一接口流入、却从同一接口流出的 VPN 流量有用。这种情况下，VPN 流量可能未加密，也可能被重新加密以用于另一个 VPN 连接。例如，如果您有一个中心和辐射 VPN 网络，其中 ASA 是中心，远程 VPN 网络是辐射，一个辐射与另一个辐射进行通信，则流量必须流入 ASA，然后再流出，进入另一个辐射。

注释 此功能允许的所有流量仍将受到防火墙规则的制约。务必要小心，不要造成不对称的路由情景，否则可能会导致流量不会流经 ASA。

分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。对于多情景模式，此功能将向所有已分配至情景的接口类型分配唯一 MAC 地址。 对于单模式，此功能将向 VLAN 子接口分配唯一 MAC 地址。

开始之前

- 为接口配置名称时，会立即生成新MAC地址。如果在配置接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的MAC地址与网络中的另一个专用MAC地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。
- 对于多情景模式，请在系统执行空间中完成本程序。如果您尚未进入系统配置模式，请在 **Configuration** > **Device List** 窗格中双击主用设备 IP 地址下的 **System**。

过程

步骤 1 对于多情景模式: 在系统中完成以下步骤。

a) 依次选择**配置** > **情景管理** > **安全情景**。
b) 选中**自动 Mac 地址**。
c) （可选） 选中**前缀**复选框，并在字段中输入一个介于 0 和 65535 之间的十进制值。

此前缀会转换为一个四位数的十六进制数字，并用作MAC地址的一部分。如果未输入前缀，则 ASA 将根据接口 MAC 地址的最后两个字节自动生成前缀。

步骤 2 对于单情景模式：完成以下步骤。

a) 依次选择**配置** > **设备设置** > **接口设置** > **接口**。
b) 在页面底部，选中**为子接口启用自动生成 MAC 地址**复选框。
c) （可选） 在**前缀**字段中，输入一个介于 0 和 65535 之间的十进制值。

此前缀会转换为一个四位数的十六进制数字，并用作MAC地址的一部分。如果未输入前缀，则 ASA 将根据接口 MAC 地址的最后两个字节自动生成前缀。

步骤 3 点击**应用**。

配置手动 MAC 地址、MTU 和 TCP MSS

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统更改为情景配置，请在“配置 > 设备列表”窗格中双击主用设备 IP 地址下的情景名称。

过程

步骤 1 依次选择**配置** > **设备设置** > **接口设置** > **接口**。

步骤 2 选择接口行，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框，其中 **General** 选项卡已选定。

步骤 3 点击**高级 (Advanced)** 选项卡。

步骤 4 要设置 MTU 或启用巨型帧支持（仅限支持的型号），请在 **MTU** 字段输入数值。最小值和最大值取决于您的平台。

默认值为 1500 字节。

注释 为端口通道接口设置 MTU 时，ASA 将设置应用于所有成员接口。

- 对于在单情景模式下支持句型帧的型号 - 如果为任何接口输入的值大于 1500，则您将自动为所有接口启用巨型帧支持。如将所有接口的 MTU 值均设置回小于 1500 的值，则将禁用巨型帧支持。
- 对于在多情景模式下支持句型帧的型号 - 如果为任何接口输入的值大于 1500，则在模型要求的情况下务必在系统配置中启用巨型帧支持。请参阅 启用巨帧支持（ASA Virtual、ISA 3000）。

注释　　对于某些型号，启用或禁用巨型帧支持需要重新加载 ASA。

步骤 5　要手动向该接口分配 MAC 地址，请在 **Active Mac Address** 字段中以 H.H.H 格式输入 MAC 地址，其中，H 是 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

步骤 6　如果使用故障转移，请在 **Standby Mac Address** 字段输入备用 MAC 地址。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 7　要设置 TCP MSS，请依次选择**配置** > **防火墙** > **高级** > **TCP 选项**。设置以下选项：

- Send reset reply for denied outside TCP packets - 使 ASA 能够为尝试传输 ASA 且被 ASA 根据访问列表或 AAA 设置拒绝的所有出站 TCP 会话发送重置应答。
- Force Maximum Segment Size for TCP - 将最大 TCP 分片大小设置为介于 48 和任何最大数值之间的字节数。默认值为 1380 字节。您可以禁用此功能，只需将字节数设置为 0。
- Force Minimum Segment Size for TCP - 覆盖最大分片大小，使其不小于已设置的字节数，介于 48 和任何最大数值之间。默认情况下，此功能已禁用（设置为 0）。
- TCP Maximum unprocessed segment - 选中此复选框并指定未处理的 TCP 分段的最大数量。默认值为 6。范围为 6 到 24。

步骤 8　对于 **Secure Group Tagging** 设置，请参阅防火墙配置指南。

步骤 9　(Secure Firewall 3100) 点击**自动协商 (Auto-negotiate)**，协商 1 千兆及更高接口的链路状态和流量控制。

步骤 10　对于 **ASA Cluster** 设置，请参阅（推荐；在多情景模式下为必需）在控制节点上配置接口。

允许同一安全级别的通信

默认情况下，同一个安全级别的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

过程

步骤 1　要启用相同安全级别的接口之间的通信，请在**配置** > **接口**窗格中选中**启用两个或更多个配置相同安全级别的接口之间的流量**。

步骤 2　要启用连接到同一接口的主机之间的通信，请选中 **Enable traffic between two or more hosts connected to the same interface**。

监控 ARP 和 MAC 地址表

- **Monitoring > Interfaces > ARP Table**

  显示 ARP 表，包括静态和动态条目。ARP 表包含将给定接口的 MAC 地址映射到 IP 地址的条目。

- **Monitoring > Interfaces > MAC Address Table**

  显示静态和动态 MAC 地址条目。

高级接口配置历史记录

表 *1:* 高级接口配置历史记录

功能名称	版本	功能信息
最大 MTU 现为 9198 字节	9.1(6)、9.2(1)	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。 修改了以下屏幕：**配置 > 设备设置 > 接口设置 > 接口 > 编辑接口 > 高级**
增加了 Firepower 4100/9300 机箱 上 ASA 的 MTU 大小	9.6(2)	可以在 Firepower 4100 和 9300 上将最大 MTU 设置为 9184 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。 修改了以下菜单项：**配置 > 设备设置 > 接口设置 > 接口 > 高级**
单情景模式下的唯一 MAC 地址生成	9.8(3), 9.8(4), 9.9(2)	现在，您可以在单情景模式下启用 VLAN 子接口的唯一 MAC 地址生成。正常情况下，子接口与主接口共享同一 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此，此功能将允许唯一的 IPv6 链路本地地址。 新增或修改的命令：**mac-address auto** 无 ASDM 支持。

功能名称	版本	功能信息
ASDM 支持为单一情景模式生成唯一的 MAC 地址	ASDM 7.15(1)	现在，您可以在 ASDM 中的单情景模式下启用 VLAN 子接口的唯一 MAC 地址生成。正常情况下，子接口与主接口共享同一 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此，此功能将允许唯一的 IPv6 链路本地地址。 新增或修改的菜单项：**配置** > **设备设置** > **接口设置** > **接口**
可以为 1Gigabit 及更高版本的接口启用或禁用安全防火墙 3100 自动协商。	9.17(1)	可以为 1Gigabit 及更高版本的接口启用或禁用安全防火墙 3100 自动协商。对于其他型号的 SFP 端口， **no speed nonegotiate** 选项将速度设置为 1000 Mbps；新命令意味着您可以独立设置自动协商和速度。 新增/修改的屏幕： **配置** > **设备设置** > **接口设置** > **接口** > **高级**

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。