的 ARP 检测和 MAC 地址表

本章介绍如何自定义 MAC 地址表以及为网桥组配置 ARP 检测。

关于 ARP 检测和 MAC 地址表

对于网桥组中的接口，ARP检测可防止“中间人”攻击。您还可以自定义其他ARP设置。您可以自定义网桥组的 MAC 地址表，包括添加静态 ARP 条目来防范 MAC 欺骗。

网桥组流量的 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP检测可防止恶意用户模拟其他主机或路由器（称为ARP欺骗）。ARP欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，ASA 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 ASA 会丢弃数据包。

- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 ASA 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用管理接口也绝不会以泛洪方式传输数据包。

MAC 地址表

当你使用网桥组时，ASA 以与一般网桥或交换机相似的方式获悉和构建 MAC 地址表：当某个设备通过网桥组发送数据包时，ASA 将在其表中添加 MAC 地址。此表将 MAC 地址与源接口相关联，以便ASA可了解如何将要发送到设备的任何数据包从正确的接口发出。由于网桥组成员之间的流量须遵守 ASA 安全策略，因此如果数据包的目标 MAC 地址不在此表中，则 ASA 不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - ASA 将生成针对目标 IP 地址的 ARP 请求，以使它能了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - ASA将生成一个针对目标 IP 地址的 ping，以使它能了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

对于路由模式，可以选择在所有接口上启用非 IP 数据包泛洪。

默认设置

- 如果启用 ARP 检测，则默认情况下会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 ASA 会将对应的条目添加到 MAC 地址表中。

注释 Secure Firewall ASA 生成重置数据包以重置状态检测引擎拒绝的连接。在这里，数据包的目标MAC地址不是根据ARP表查找确定的，而是直接从被拒绝的数据包（连接）中获取的。

ARP 检测和 MAC 地址表准则

- ARP 检测仅支持网桥组。
- MAC 地址表配置仅支持网桥组。

配置 ARP 检测和其他 ARP 参数

对于网桥组，可以启用 ARP 检测。您还可以为网桥组和路由模式接口配置其他 ARP 参数。

过程

步骤 1 根据添加静态 ARP 条目并自定义其他 ARP 参数，第 3 页中所述添加静态 ARP 条目。ARP 检测会将 ARP 数据包与 ARP 表中的静态 ARP 条目作比较，因此该功能需要静态 ARP 条目。您还可以配置其他 ARP 参数。

步骤 2 根据启用 ARP 检测，第 4 页启用 ARP 检测。

添加静态 ARP 条目并自定义其他 ARP 参数

对于桥接组，默认情况下，桥接组成员接口之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。ARP 检测会对比 ARP 数据包与 ARP 表中的静态 ARP 条目。

对于路由接口，可以输入静态 ARP 条目，但通常动态条目就足够了。对于路由接口，使用 ARP 表向直连主机交付数据包。虽然发件人可根据 IP 地址识别数据包目标，但在以太网上实际交付数据包依赖于以太网 MAC 地址。当路由器或主机希望在直连网络上交付数据包时，它会发送 ARP 请求来寻求与该 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器可保留 ARP 表，所以不必对需要交付的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果某个条目错误（例如给定 IP 地址的 MAC 地址改变），该条目需要超时后，才能为其更新新信息。

对于透明模式，ASA 仅对进出 ASA 的流量（例如管理流量）使用 ARP 表中的动态 ARP 条目。

此外，还可以设置 ARP 超时和其他 ARP 行为。

过程

步骤 1 添加静态 ARP 条目：

arp *interface_name ip_address mac_address* [**alias**]

示例：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

本示例在外部接口上允许来自地址 10.1.1.1、MAC 地址 0009.7cbe.2100 的路由器的 ARP 响应。

在路由模式下，指定 **alias** 可为此映射启用代理 ARP。如果 ASA 收到指定 IP 地址的 ARP 请求，则会使用 ASA MAC 地址做出响应。例如，此关键字在您有不执行 ARP 的设备时非常有用。在透明防火墙模式下，此关键字将被忽略；ASA 不执行代理 ARP。

步骤 2 设置动态 ARP 条目的 ARP 超时：

arp timeout 秒

示例：

```
ciscoasa(config)# arp timeout 5000
```

此字段设置 ASA 在重建 ARP 表前允许的时长，范围介于 60 到 4294967 秒之间。默认值为 14400 秒。重建 ARP 表会自动更新新的主机信息并删除旧的主机信息。由于主机信息频繁更改，因此可能要减少超时。

步骤 3 允许未连接的子网：

arp permit-nonconnected

ASA ARP 缓存默认仅包含来自直连子网的条目。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。

步骤 4 设置 ARP 速率限制以控制每秒的 ARP 数据包数：

arp rate-limit 秒

示例：

```
ciscoasa(config)# arp rate-limit 1000
```

输入 10 到 32768 之间的值。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。

启用 ARP 检测

本节介绍如何为网桥组启用 ARP 检测。

过程

启用 ARP 检测：

arp-inspection *interface_name* **enable** [**flood** |**no-flood**]

示例：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood 关键字将不匹配的 ARP 数据包转发出所有接口，**no-flood** 则会丢弃不匹配的数据包。

默认设置是以泛洪方式传输不匹配的数据包。要通过 ASA 将 ARP 限制为仅静态条目，请将此命令设置为 **no-flood**。

自定义网桥组的 MAC 地址表

本部分介绍如何为网桥组自定义 MAC 地址表.

为网桥组添加静态 MAC 地址

通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。可以向 MAC 地址表中添加静态 MAC 地址。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向不匹配静态条目的接口发送流量，ASA 将会丢弃流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目并自定义其他 ARP 参数，第 3 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

要向 MAC 地址表中添加静态 MAC 地址，请执行以下步骤。

过程

添加静态 MAC 地址条目：

mac-address-table static *interface_name mac_address*

示例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

interface_name 是源接口。

设置 MAC 地址超时

动态MAC地址表条目的默认超时值为5分钟，但您可以更改超时。要更改超时，请执行以下步骤：

过程

设置 MAC 地址条目超时：

mac-address-table aging-time *timeout_value*

示例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

timeout_value（以分钟为单位）介于 5 到 720（12 小时）之间。默认值为 5 分钟。

配置 MAC 地址学习

默认情况下，每个接口都会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加至 MAC 地址表。如果需要，您可以禁用 MAC 地址获悉，不过除非您将 MAC 地址静态添加至此表中，否则没有流量可以通过 ASA。在路由模式下，可以在所有接口上启用非 IP 数据包泛洪。

要配置 MAC 地址学习，请执行以下步骤：

过程

步骤 1 禁用 MAC 地址获悉：

mac-learn *interface_name* **disable**

示例：

```
ciscoasa(config)# mac-learn inside disable
```

此命令的 **no** 形式会重新启用 MAC 地址获悉。

clear configure mac-learn 命令会在所有接口上重新启用 MAC 地址获悉。

步骤 2 （仅限路由模式）启用非 IP 数据包的泛洪。

mac-learn 泛洪

示例：

```
ciscoasa(config)# mac-learn flood
```

监控 ARP 检测和 MAC 地址表

- **show arp-inspection**

  监控 ARP 检测。显示所有接口上的 ARP 检测的当前设置。

- **show mac-address-table [*interface_name*]**

  监控 MAC 地址表。可以查看整个 MAC 地址表（包括两个接口的静态和动态条目），也可以查看某个接口的 MAC 地址表。

以下是 **show mac-address-table** 命令（用于显示整个 MAC 地址表）的样本输出：

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside      0010.7cbe.6101       static    -
inside      0009.7cbe.5101       dynamic    10
```

以下是 **show mac-address-table** 命令（用于显示内部接口的 MAC 地址表）的样本输出：

```
ciscoasa# show mac-address-table inside
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside      0010.7cbe.6101       static    -
inside      0009.7cbe.5101       dynamic    10
```

以下是 **show mac-address-table** 命令（用于静态和动态网桥组条目的总数）的样本输出：

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/16384
Dynamic    mac-address bridges (curr/max): 0/16384
```

ARP 检测和 MAC 地址表历史记录

功能名称	平台版本	功能信息
ARP 检测	7.0(1)	ARP 检测会将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目作比较。此功能适用于透明防火墙模式，而且自 9.7(1) 起，还适用于透明模式和路由模式下桥接组中的接口。 引入了以下命令：**arp**、**arp-inspection** 和 **show arp-inspection**。
MAC 地址表	7.0(1)	您可能希望为透明防火墙模式自定义 MAC 地址表，而且自 9.7(1) 起，还为透明模式和路由模式下桥接组中的接口进行自定义。 引入了以下命令：**mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable** 和 **show mac-address-table**。

功能名称	平台版本	功能信息
针对未连接的子网添加 ARP 缓存	8.4(5)/9.1(2)	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**。
可自定义的 ARP 速率限制	9.6(2)	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**
集成的路由与桥接	9.7(1)	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**

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。