ASA ：升级到8.4(3)后，NAT地址的入站访问失败

目录

简介

本文档提供有关在将自适应安全设备(ASA)升级到版本8.4(3)后失败的NAT地址的信息。 本文档还提供了此问题的解决方案。

先决条件

要求

本文档的读者应了解这些主题。

- 基本了解地址解析协议(ARP)和代理ARP的概念

使用的组件

本文档中的信息基于这些硬件与软件版本。

- 任何Cisco ASA 5500系列自适应安全设备
- 自适应安全设备8.4(3)版或更高版本

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

症状

从ASA版本8.4(3)开始，ASA不响应接口上收到的ARP请求，请求的IP地址不属于该接口的IP子网。在版本8.4(3)之前，ASA将响应不在ASA接口IP子网中的ARP请求。

将ASA升级到版本8.4(3)后，此更改可立即显现。 在某些情况下，Internet用户无法通过ASA连接到已转换服务器的全局地址。

如果遇到此情况，并且在ASA的CLI上启用了“debug arp”，则显示此消息：

```
arp-in: Arp packet received from 192.168.10.1 which is in different subnet
than the connected interface 192.168.11.1/255.255.255.0
```

此问题的根本原因不是Bug。请参阅以下信息，了解有关潜在原因和问题解决方案的详细信息。

条件/环境

为了遇到这种情况，ASA必须收到ARP请求，请求的IP地址与配置的NAT转换中的全局地址匹配。全局IP地址必须位于与ASA接口上配置的IP子网不同的IP子网中。

原因/问题描述

要了解此问题的全部后果，必须全面了解此问题的出现方式以及缓解此问题的最佳方式。

以下是可能遇到此情况的一些实例：

上游设备的IP路由没有配置下一跳IP地址

这可能是造成这种情况的最常见原因。这是由于上游设备的配置非最佳。首选配置IP路由，使IP路由的下一跳是与该接口地址位于同一子网中的IP地址：

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

但是，有时网络管理员会将接口而不是IP地址配置为下一跳：

```
ip route 10.1.2.0 255.255.255.0 FastEthernet0/1
```

这会导致路由器将发往10.1.2.0/24网络的流量路由到FastEthernet0/1接口，并发送ARP请求以获取IP数据包中的目的IP地址。假设某些设备将响应ARP请求，然后路由器将数据包转发到因ARP过程而解析的MAC地址。这种配置的优点是配置和管理非常容易。管理员不必为路由明确配置下一跳IP地址，他们假设邻接设备将启用代理ARP，并且如果能够将数据包路由到目的IP地址，将响应ARP请求。

但是，此类IP路由配置存在严重问题：

- 通过发送ARP请求来确定IP流量的下一跳，路由器会面临其他设备可能错误地响应该ARP请求而引起的问题。结果是，当流量发送到不正确的设备时，可能会黑洞。
- 该路由将导致设备发送ARP请求，查找与路由匹配的数据包中的每个唯一目的地址。这可能导致子网上出现大量ARP流量，并对性能和存储大量ARP条目所需的内存空间产生负面影响。
- 由于ARP表空间是内存绑定资源，因此过多的条目可能会对路由器的性能和稳定性产生负面影响。

因此，最佳做法是使用显式IP下一跳地址配置所有路由，而不使用自身具有接口名称的路由来标识

传出接口。如果需要接口将路由与出口接口关联以进行故障转移，请在静态路由中输入出口接口名称和下一跳。

鉴于对某些思科客户的管理影响，我们已提出增强请求，以便可配置新的安全行为：Cisco Bug ID CSCty95468(仅注册客户)(增强版：添加命令以允许来自未连接子网的ARP缓存条目)。

相邻设备上的IP子网掩码不匹配

在ASA接口和相邻设备接口上配置的不匹配的IP子网掩码也可能导致类似情况。如果相邻设备的子网掩码是ASA接口IP子网掩码(255.255.240.0)的超网(255.255.255.0)，则相邻设备将对不在ASA接口IP子网中的IP地址执行ARP。确保子网掩码正确。

透明模式含义

此更改的另一个副作用是无法在透明模式下从非直接连接的子网获取MAC地址。这会影响以下场景中的通信：

- 透明ASA未配置管理IP地址或配置不正确。
- 透明ASA使用同一网段上的辅助子网。

在透明模式下，除降级外，没有解决此问题的解决方法。但是，此增强请求已打开，以便ASA在透明模式下与辅助子网互操作：Cisco Bug ID CSCty49855(仅注册客户)(增强版：在MAC发现机制中支持非直连主机)。

分辨率

此问题的解决方案（如果所讨论的IP地址与ASA的接口IP不在同一第3层子网中）是进行必要的更改，以确保与ASA相邻的设备将流量直接路由到ASA的接口IP地址作为下一跳设备，而不是依赖设备代表IP地址代理ARP。

相关信息

- 技术支持和文档 - Cisco Systems