ASA ：对NAT地址的入站访问在升级以后失效对8.4(3)

目录

简介

本文提供关于在升级可适应安全工具以后失效的NAT讨论的信息(ASA)对版本8.4(3)。本文也提供一解决方法给此问题。

先决条件

要求

本文读者应该有这些主题知识。

- 地址解析服务(ARP)和代理ARP的概念的基本的了解

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系列可适应安全工具
- 可适应安全工具版本8.4(3)或以上

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

开始与ASA版本8.4(3)， ASA不回答在一个接口接收的ARP请求，不是该接口的IP子网的部分的IP地址的。在版本8.4(3)前， ASA将回答不在ASA的接口的IP子网的ARP请求。

此更改能在升级ASA之后表明自己到版本8.4(3)。有时，互联网用户不能连接到一个翻译的服务器的全局地址通过ASA。

此消息显示，如果此情况被遇到，并且'debug arp'在ASA的CLI启用：

```
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。请参阅下面信息得知更多潜在的原因和解决方案到问题。

情况/环境

为了遇到此情况， ASA必须收到匹配在一个已配置的NAT转换的一个全局地址的IP地址的一个ARP请求。全局IP地址必须位于是与在ASA的接口配置的IP子网不同的IP子网。

原因/问题说明

为了了解此问题的全双工分枝，获得完整了解对此问题如何能出现是重要的和最佳方法减轻问题。

这些是此情况可以被遇到的一些实例：

上行设备有IP路由配置没有下一跳IP地址

这很可能是此情况的多数常见原因。它归结于一个上行设备的一非最优配置。更喜欢配置IP路由这样Ip route的下一跳是在相同子网的一个IP地址作为该接口的地址：

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

然而，网络管理员有时配置接口而不是IP地址作为下一跳：

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

这导致路由器路由流量被注定对10.1.2.0/24网络对FastEthernet0/1接口，并且发送目的IP地址的一个ARP请求在IP数据包。假设，一些设备将回答ARP请求，并且路由器然后转发数据包对解决归结于ARP进程的MAC地址。这类配置的好处是配置和管理是非常容易的。管理员不明确地必须配置路由的一个下一跳IP地址，并且他们假设，邻接设备proxy-arp启用，并且请回答ARP请求是否有能力在路由上数据包对目的IP地址。

然而，有与此种Ip route配置的严重问题：

- 通过发送ARP请求确定IP数据流的下一跳，路由器显示在也许不正确地回答该ARP请求的其它设备引起的问题。结果是流量可以黑洞，当发送对一个不正确设备。
- 路由将促成设备发送每唯一目的地址的一个ARP请求在匹配路由的数据包。这能导致在子网的很多ARP流量和负影响性能以及要求的存储器空间保持可能增大的相当数量ARP条目。
- 由于ARP表空间是内存限制资源，过量的条目能负面影响路由器性能和stabilty。

所以，最佳实践是配置有明确IP下个跳段地址的所有路由和不使用单独有识别一的接口名称流出接口的路由。如果接口是需要的附加路由到故障切换的出口接口，请输入两个出口接口名称和下一跳在静态路由。

给一些Cisco用户的管理暗示，打开增强请求为了使新的安全行为成为可配置：Cisco Bug ID

CSCty95468 (仅限注册用户) (ENH ：Add命令允许从未连接的子网的ARP缓存条目)。

在邻接设备的不匹配的IP子网掩码

在ASA的接口和邻接设备的接口配置的不匹配的IP子网掩码能导致一个相似的情况。如果邻接设备有是超网的一个子网掩码(255.255.240.0) ASA的接口IP子网掩码(255.255.255.0)，邻接设备不在ASA接口IP子网的IP地址的ARP。保证子网掩码正确。

透明模式暗示

此更改另一个副作用是了解从非直接连接的子网的MAC地址的无法在透明模式。这在这些情况下影响通信：

- 透明ASA没有配置的一个管理IP地址或配置不正确。
- 透明ASA使用在同一分段的二级子网。

除降级之外，没有此问题的应急方案在透明模式。然而，打开此增强请求为了做ASA与在透明模式的二级子网兼容：Cisco Bug ID CSCty49855 (仅限注册用户) (ENH ：在MAC发现机制的支持非直接地连接的主机)。

解决方法

对此问题的解决方案(在案件有问题的IP地址不在第3层子网和ASA的接口IP一样)将使更改必要在ASA路由流量附近保证设备直接地到ASA的接口IP地址作为下一跳设备，而不是取决于在设备到proxy-arp代表IP地址。

相关信息

- 技术支持和文档 - Cisco Systems