当VPN客户端断开连接时，由于流量环路，ASA的CPU使用率较高

目录

简介

本文档介绍当VPN客户端从作为远程访问VPN前端运行的思科自适应安全设备(ASA)断开连接时发生的常见问题。本文档还介绍当VPN用户从ASA防火墙断开连接时发生流量环路的情况。本文档不介绍如何配置或设置对VPN的远程访问，而只介绍某些常见路由配置产生的特定情况。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA上的远程访问VPN配置
- 第3层路由的基本概念

使用的组件

本文档中的信息基于运行ASA代码版本9.1(1)的ASA型号5520。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文档可与以下硬件和软件版本配合使用：

- 任何ASA型号
- 任何ASA代码版本

背景信息

当用户作为远程访问VPN集中器连接到ASA时，ASA在ASA路由表中安装基于主机的路由，该路由将流量从外部接口（指向互联网）路由到该VPN客户端。 当该用户断开连接时，该路由将从表中删除，并且内部网络（发往该断开的VPN用户）上的数据包可能会在ASA和内部路由设备之间环路。

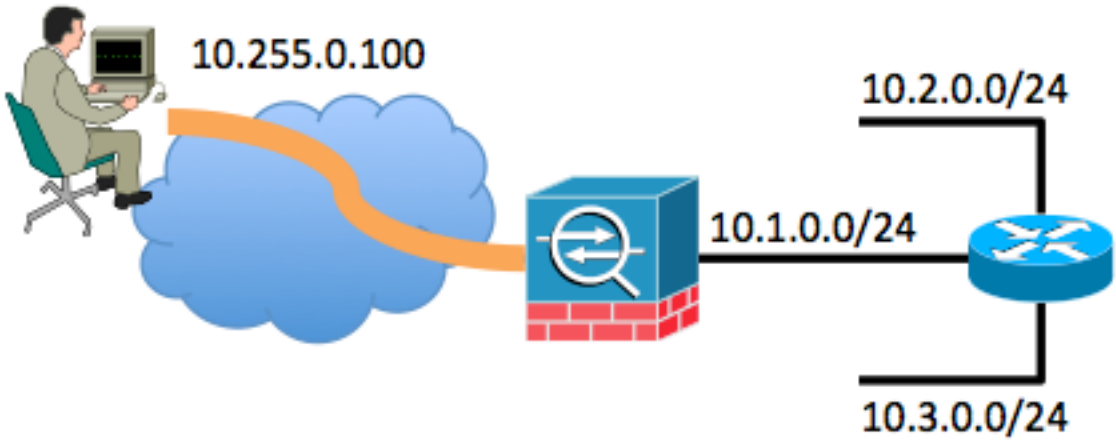
另一个问题是，定向（网络）广播数据包（通过删除VPN客户端而生成）可能由ASA作为单播帧转发到内部网络。这可能会将其转发回ASA，导致数据包在生存时间(TTL)到期前循环。

本文档将介绍这些问题，并展示可使用哪些配置技术来防止问题。

问题：发往内部网络内断开的VPN客户端环路的数据包

当远程访问VPN用户从ASA防火墙断开连接时，数据包仍然存在于内部网络（发往那些断开连接的用户）中，且分配的IP VPN地址可能会在内部网络中环路。这些数据包环路可能导致ASA上的CPU使用率增加，直到环路停止，或者由于IP数据包报头中的IP TTL值减为0，或者用户重新连接并将IP地址重新分配给VPN客户端。

为了更好地理解此场景，请考虑以下拓扑：



在本例中，远程访问客户端已分配IP地址10.255.0.100。本例中的ASA与路由器连接到同一内部网段。路由器还连接了两个额外的第3层网段。ASA和路由器的相关接口（路由）和VPN配置如示例所示。

ASA配置要点如本示例所示：

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
```

```
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

路由器配置要点如本例所示：

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

连接到ASA内部的路由器的路由表中只有一条指向ASA内部接口10.1.0.1的默认路由。

当用户通过VPN连接到ASA时，ASA路由表显示如下：

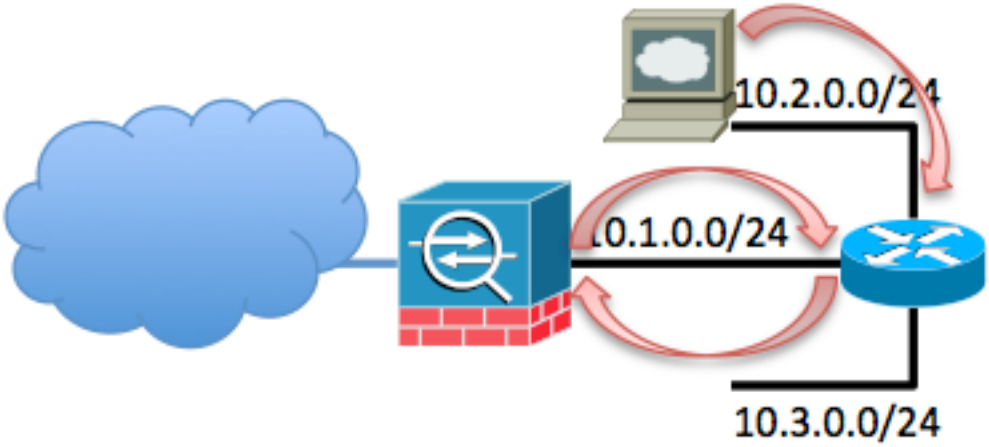
```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

当远程访问VPN用户断开与VPN的连接时，会出现问题。此时，基于主机的路由将从ASA路由表中删除。如果网络内部的主机尝试将流量发送到VPN客户端，则该流量将由路由器路由到ASA内部接口。此系列步骤发生：

1. 发往10.255.0.100的数据包到达ASA的内部接口。
2. 执行标准ACL检查。
3. 检查ASA路由表以确定此流量的出口接口。
4. 数据包的目的地与从内部接口指向路由器的广10.0.0.0/8路由匹配。
5. ASA验证是否允许发夹流量 — 它搜索**相同安全许可的接口内**部，并发现允许它。
6. 从内部接口建立连接，然后将数据包作为下一跳发回路由器。

7. 路由器在面向ASA的接口上收到发往10.255.0.100的数据包。路由器会检查其路由表以查找合适的下一跳。路由器发现下一跳将是ASA内部接口，并且数据包将发送到ASA。
8. 返回到第 1 步。

示例如下所示：



此循环发生，直到此数据包的TTL递减到0。请注意，ASA防火墙在处**理数**据包时不会默认递减TTL值。路由器在路由数据包时递减TTL。这可以无限期地防止此环路的出现，但此环路确实会增加ASA上的流量负载并导致CPU使用率激增。

问题：由VPN客户端生成的定向（网络）广播数据包在内部网络上循环

此问题与第一个问题类似。如果VPN客户端生成定向广播数据包到其分配的IP子网（上例中为10.255.0.255），则该数据包可能作为单播帧由ASA转发到内部路由器。然后，内部路由器可能会将其转发回ASA，这会导致数据包循环，直到TTL过期。

发生以下一系列事件：

1. VPN客户端计算机生成一个发往网络广播地址10.255.0.255的数据包，该数据包到达ASA。
2. ASA将此数据包视为单播帧（由于路由表），并将其转发到内部路由器。
3. 内部路由器也将数据包视为单播帧，它会递减数据包的TTL并将其转发回ASA。
4. 该过程会重复，直到数据包的TTL减小为0。

问题解决方案

此问题有几种可能的解决方案。根据网络拓扑和具体情况，一个解决方案可能比另一个解决方案更容易实施。

解决方案1 - Null0接口的静态路由（ASA 9.2.1及更高版本）

当您将流量发送到**Null0接**口时，它会导致发往指定网络的数据包被丢弃。当您为边界网关协议(BGP)配置远程触发黑洞(RTBH)时，此功能非常有用。在这种情况下，如果为远程访问客户端子网

配置到Null0的路由，它会强制ASA在没有更具体路由（反向路由注入提供）时丢弃发往该子网中主机的流量。

```
route Null0 10.255.0.0 255.255.255.0
```

解决方案2 — 为VPN客户端使用不同的IP池

此解决方案是为远程VPN用户分配一个不与任何内部网络子网重叠的IP地址。如果VPN用户未连接，这将阻止ASA将发往该VPN子网的数据包转发回内部路由器。

解决方案3 — 使ASA路由表更具体地用于内部路由

此解决方案是确保ASA的路由表没有与VPN IP池重叠的任何非常广泛的路由。对于此特定网络示例，从ASA中删除10.0.0.0/8路由，并为位于内部接口之外的子网配置更具体的静态路由。根据子网数量和网络拓扑，这可能是大量静态路由，可能不可能。

解决方案4 — 为从外部接口返回的VPN子网添加更具体的路由

此解决方案比本文档中介绍的其他解决方案更为复杂。思科建议您首先尝试使用其他解决方案，原因是本部分后面的“注释”中描述了这种情况。此解决方案是防止ASA将源自VPN IP子网的IP数据包转发回内部路由器；如果为外部接口之外的VPN子网添加更具体的路由，则可以执行此操作。由于此IP子网为外部VPN用户保留，因此来自此VPN IP子网的具有源IP地址的数据包永远不应到达ASA内部接口的入站方向。实现此目的的最简单方法是使用上游ISP路由器的下一跳IP地址从外部接口添加远程访问VPN IP池的路由。

在此网络拓扑示例中，该路由如下所示：

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

除此路由外，添加**ip verify reverse-path inside** 命令，以使ASA丢弃从VPN IP子网接收的来自内部接口的入站数据包，因为外部接口上存在更优先的路由：

```
ip verify reverse-path inside
```

在实施这些命令后，当用户连接时，ASA路由表的外观与下面类似：

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

当VPN客户端连接时，表中会显示指向该VPN IP地址的基于主机的路由，并且是首选路由。当VPN客户端断开连接时，来自该客户端IP地址到达内部接口的流量会根据路由表进行检查，并因为使用**ip verify reverse-path inside命令而被**丢弃。

如果VPN客户端生成指向VPN IP子网的定向网络广播，则该数据包将转发到内部路由器并由路由器转发回ASA，在ASA中，由于使用**ip verify reverse-path inside命令，该数据包将被丢弃。**

> **注意**：实施此解决方案后，如果配置中存在**same-security permit intra-interface**命令，且访问策略允许该命令，则来自VPN用户的流量将以明文形式从外部接口路由回VPN IP池中的IP地址。这种情况非常罕见，在VPN策略中使用vpn过滤器可以缓解这种情况。仅当ASA配置中**存在same-security permit intra-interface**命令时，才会发生这种情况。
>
> 同样，如果内部主机生成发往VPN池中IP地址的流量，且该IP地址未分配给远程VPN用户，则该流量可能以明文形式流出ASA外部。