由於VPN客戶端斷開連線時出現流量環路，ASA的CPU使用率較高

目錄

簡介

本文檔介紹當VPN客戶端與作為遠端訪問VPN頭端運行的Cisco Adaptive Security Appliance(ASA)斷開連線時出現的常見問題。本文檔還介紹了當VPN使用者從ASA防火牆斷開連線時發生流量環路的情況。本文檔不介紹如何配置或設定對VPN的遠端訪問，僅介紹由某些常見路由配置引起的特定情況。

必要條件

需求

思科建議您瞭解以下主題：

- ASA上的遠端訪問VPN配置
- 基本的第3層路由概念

採用元件

本文檔中的資訊基於運行ASA代碼版本9.1(1)的ASA型號5520。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下硬體和軟體版本：

- 任何ASA型號
- 任何ASA代碼版本

背景資訊

當使用者作為遠端訪問VPN集中器連線到ASA時，ASA會在ASA路由表中安裝基於主機的路由，該路由會將流量從外部介面（通往網際網路）路由到該VPN客戶端。 當該使用者斷開連線時，該路由將從表中刪除，並且內部網路上的資料包（發往該斷開的VPN使用者）可能會在ASA和內部路由裝置之間環路。

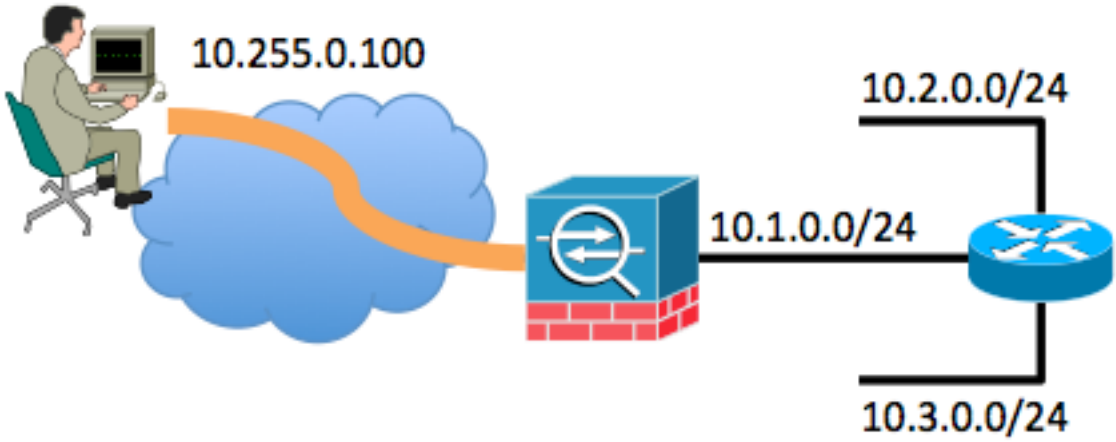
另一個問題是，定向（網路）廣播資料包（通過刪除VPN客戶端而生成）可能由ASA作為單播幀轉發到內部網路。這可能會將其轉回ASA，這將導致資料包在生存時間(TTL)到期之前循環。

本檔案將說明這些問題，並顯示可使用哪些組態技術防止發生問題。

問題：發往內部網路中斷開連線的VPN客戶端環路的資料包

當遠端訪問VPN使用者從ASA防火牆斷開連線時，資料包仍然存在於內部網路中（發往斷開連線的使用者），並且分配的IP VPN地址可能在內部網路中循環。這些資料包環路可能會導致ASA上的CPU使用率增加，直到環路停止為止，原因是IP資料包報頭中的IP TTL值減小為0，或者使用者重新連線並將IP地址重新分配給VPN客戶端。

為了更好地理解此情境，請考慮以下拓撲：



在本示例中，為遠端訪問客戶端分配了IP地址10.255.0.100。本示例中的ASA與路由器一起連線到同一個內部網段。路由器有兩個附加的第3層網段與其相連。示例中顯示了ASA和路由器的相關介面（路由）和VPN配置。

ASA配置亮點如下例所示：

```
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
```

路由器配置要點如以下示例所示：

```
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
```

連線到ASA內部的路由器的路由表只有一個指向ASA內部介面10.1.0.1的預設路由。

當使用者通過VPN連線到ASA時，ASA路由表顯示如下：

```
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
```

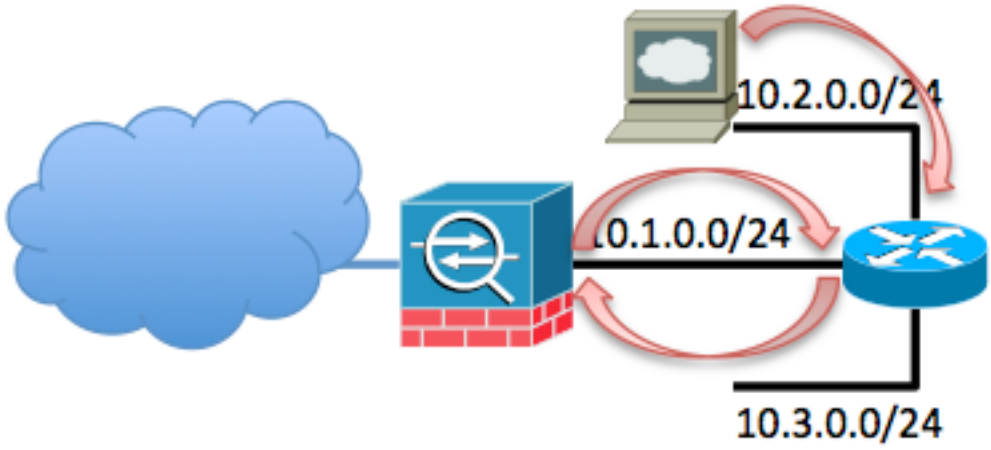
當遠端訪問VPN使用者從VPN斷開連線時會出現此問題。此時，從ASA路由表中刪除基於主機的路由。如果網路內的主機嘗試向VPN客戶端傳送流量，路由器會將該流量路由到ASA內部介面。發生以下系列步驟：

1. 目的地為10.255.0.100的資料包會到達ASA的內部介面。
2. 會執行標準型ACL檢查。
3. 檢查ASA路由表以確定此流量的輸出介面。
4. 封包的目的地與從內部介面往迴路由器的10.0.0.0/8寬路由相符。
5. ASA驗證是否允許髮夾流量 — 它搜尋**相同安全允許介面內**並發現允許該流量。

6. 與內部介面建立連線，並將資料包作為下一跳傳送迴路由器。

7. 路由器在面向ASA的介面上收到發往10.255.0.100的資料包。路由器會檢查其路由表以查詢合適的下一跳。路由器發現下一跳將是ASA內部介面，並將資料包傳送到ASA。
8. 返回步驟1。

以下提供範例：



此循環一直發生，直到此資料包的TTL遞減為0。注意，ASA防火牆在處理資料包時不會預設遞減TTL值**值**。路由器在路由封包時遞減TTL。這會無限期地防止出現此環路，但此環路確實會增加ASA上的流量負載，並導致CPU使用率激增。

問題：由VPN客戶端生成的定向（網路）廣播資料包在內網中循環

此問題與第一個問題類似。如果VPN客戶端生成指向其分配的IP子網（在上例中為10.255.0.255）的定向廣播資料包，則該資料包可能由ASA作為單播幀轉發到內部路由器。然後，內部路由器可能會將其轉發回ASA，這會導致資料包在TTL到期之前循環。

發生以下系列事件：

1. VPN客戶端電腦生成一個目的地為網路廣播地址10.255.0.255的資料包，該資料包到達ASA。
2. ASA將此資料包視為單播幀（由於路由表的原因）並將其轉發到內部路由器。

3. 內部路由器（它也將該資料包視為單播幀）會降低資料包的TTL並將其轉發回ASA。

4. 此程式會重複，直到封包的TTL降低到0為止。

問題的解決方案

這個問題有幾種潛在的解決辦法。根據網路拓撲和具體情況，一個解決方案可能比另一個解決方案更易於實施。

解決方案1 - Null0介面（ASA 9.2.1及更高版本）的靜態路由

將流量傳送到**Null0**介面時，會導致目的地為指定網路的封包遭捨棄。在配置邊界網關協定(BGP)的遠端觸發黑洞(RTBH)時，此功能非常有用。在這種情況下，如果為遠端訪問客戶端子網配置到

Null0的路由，則在沒有更具體的路由（由反向路由注入提供）時，它強制ASA丟棄該子網中主機的流量。

```
route Null0 10.255.0.0 255.255.255.0
```

解決方案2 — 為VPN客戶端使用不同的IP池

此解決方案是為遠端VPN使用者分配一個不與任何內部網路子網重疊的IP地址。如果VPN使用者未連線，這將阻止ASA將發往該VPN子網的包轉發回內部路由器。

解決方案3 — 使ASA路由表更特定於內部路由

此解決方案旨在確保ASA的路由表不包含任何與VPN IP池重疊的非常廣泛的路由。在此特定網路示例中，從ASA刪除10.0.0.0/8路由，並為內部介面以外的子網配置更具體的靜態路由。根據子網數量和網路拓撲的不同，這可能需要大量靜態路由，並且可能是不可能的。

解決方案4 — 為VPN子網從外部介面新增更具體的路由

此解決方案比本文檔中介紹的其他解決方案更複雜。思科建議您先嘗試使用其他解決方案，這由本節後面的說明中所述的情況決定。此解決方案是防止ASA將源自VPN IP子網的IP資料包轉發回內部路由器；如果在外部介面之外為VPN子網新增更具體的路由，則可以執行此操作。由於此IP子網是為外部VPN使用者保留的，因此具有來自此VPN IP子網的源IP地址的資料包永遠不能到達ASA內部介面的入站方向。最簡單的方法是從外部介面為遠端訪問VPN IP池新增路由，該路由具有上游ISP路由器的下一跳IP地址。

在此網路拓撲示例中，該路由如下所示：

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

除了此路由之外，請新增**ip verify reverse-path inside**命令，以使ASA丟棄在源自VPN IP子網的內部介面上收到的任何入站資料包，因為外部介面上存在更優先的路由：

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

實施這些命令後，當使用者連線時，ASA路由表看起來與以下內容類似：

```
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
```

連線VPN客戶端時，通往該VPN IP地址的主機路由在表中存在，並且是首選路由。當VPN客戶端斷開連線時，源自VPN客戶端IP地址的到達內部介面的流量會根據路由表進行檢查，並由於**ip verify reverse-path inside**命令而被丟棄。

如果VPN客戶端生成到VPN IP子網的定向網路廣播，則將該資料包轉發到內部路由器，並由路由器轉發回ASA，由於**ip verify reverse-path inside**命令而丟棄該資料包。

> **附註**：實施此解決方案後，如果配置中存在**same-security permit intra-interface**命令，且訪問策略允許該命令，則源自VPN使用者的流量可能會以明文方式路由回外部介面，該流量源自VPN使用者，且目的地為未連線的使用者的VPN IP池中的IP地址。這種情況非常罕見，可以在VPN策略中使用vpn過濾器來緩解這種情況。僅當ASA配置中存在**same-security permit intra-interface**命令時，才會出現這種情況。
>
> 同樣，如果內部主機生成發往VPN池中的IP地址的流量，並且該IP地址未分配給遠端VPN使用者，則該流量可能會以明文形式輸出到ASA外部。