VPN クライアント切断時にトラフィック ループによって ASA で CPU 使用率が高くなる

目次

概要

このドキュメントでは、リモート アクセス VPN ヘッドエンドとして稼働する適応型セキュリティ アプライアンス（ASA）から VPN クライアントが切断された場合に発生する一般的な問題について説明します。 また、VPN ユーザが ASA ファイアウォールから切断されたときにトラフィック ループが発生する状況についても説明します。 このドキュメントでは、VPN へのリモート アクセスを設定またはセットアップする方法ではなく、ある一般的なルーティング設定から発生する特定の状況について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA でのリモート アクセス VPN の設定
- 基本レイヤ 3 ルーティングの概念

使用するコンポーネント

このドキュメントの情報は、ASA コード バージョン 9.1(1) が稼働する ASA モデル 5520 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアに使用できます。

- ASA モデル
- ASA コード バージョン

背景説明

ユーザがリモート アクセス VPN コンセントレータとして ASA に接続する場合、ASA はトラフィックを外部インターフェイスから VPN クライアントに（インターネットに向けて）ルーティングする ASA ルーティング テーブルにホストベースのルートをインストールします。 そのユーザが切断されると、ルートはがテーブルから削除され、ネットワーク内部のパケット（切断された VPN ユーザ宛）は ASA と内部ルーティング デバイス間でループする場合があります。

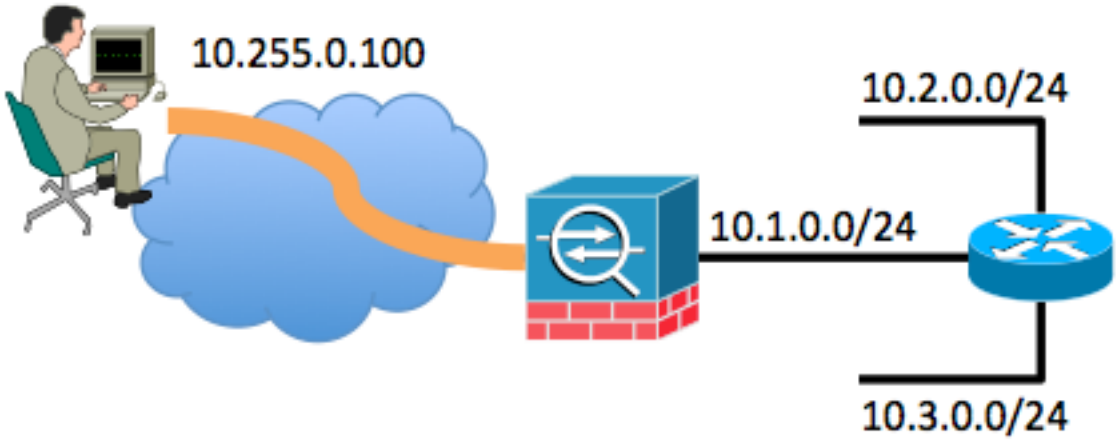
もう一つの問題として、送信（ネットワーク）ブロードキャスト パケット（VPN クライアントの削除によって生成された）が、内部ネットワークへのユニキャスト フレームとして ASA によって転送される場合があります。 これは転送して ASA に戻される可能性があり、これによってパケットの存続可能時間（TTL）が期限切れになるまでループします。

このドキュメントでは、これらの問題を説明して問題を防止するために使用する設定手法を示します。

問題： 内部ネットワーク内の切断された VPN クライアント ループ宛のパケット

VPN ユーザが ASA ファイアウォールから切断されても、（これらの切断されたユーザ宛）パケットは内部ネットワークに存在し続け、割り当てられた IP VPN アドレスが内部ネットワーク内でループする場合があります。 これらのパケット ループによって、IP パケット ヘッダー内の IP TTL 値が 0 に減少するか、ユーザが再接続して IP アドレスが VPN クライアントに再度割り当てられることで、ループが停止するまで、ASA の CPU 使用率が増加する場合があります。

このシナリオをより詳しく理解するには、次のトポロジを検討してください。



この例では、リモート アクセス クライアントには 10.255.0.100 の IP アドレスが割り当てられています。 この例の ASA は、ルータと同じ内部ネットワーク セグメントに接続されています。 ルータには、追加のレイヤ 3 ネットワーク セグメントが接続されています。 関連するインターフェイス (ルーティング) と ASA およびルータの VPN 設定を例に示します。

ASA 設定の特徴を次の例に示します。

```
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
```

ルータ設定の特徴を次の例に示します。

```
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
```

ASA の内部に接続されているルータのルーティング テーブルには ASA 内部インターフェイス 10.1.0.1 宛のデフォルト ルートがあります。

ユーザが ASA に VPN 経由で接続している間の ASA ルーティング テーブルは次のとおりです。

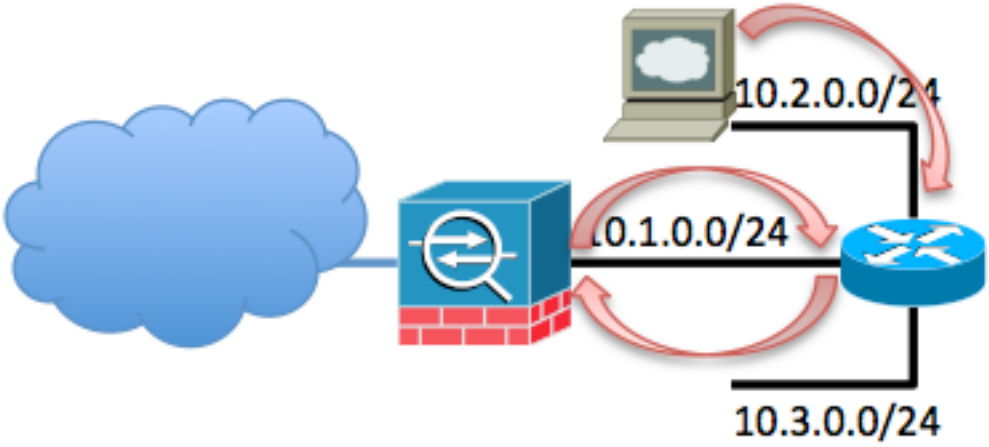
```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
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
```

問題は、リモート アクセス VPN ユーザが VPN から切断するときに発生します。 この時点で、ホストベースのルートは ASA ルーティング テーブルから削除されます。 ネットワーク内のホストが VPN クライアントにトラフィックを送信しようとすると、そのトラフィックがルータによって ASA 内部インターフェイスにルーティングされます。 次の一連の手順が発生します。

1. 10.255.0.100 宛のパケットが、ASA の内部インターフェイスに到達します。
2. 標準 ACL チェックが実行されます。
3. このトラフィックの出力インターフェイスを決定するために、ASA ルーティング テーブルを確認します。
4. パケットの宛先と、内部インターフェイスからルータを指すブロード 10.0.0.0/8 ルートが一致しています。
5. ASA がヘアピン トラフィックが許可されているかどうかの確認で、**same-security permit intra-interface** を検索すると許可されていることがわかります。
6. 内部インターフェイスへの接続が確立され、パケットがネクスト ホップとしてルータに戻されます。
7. ルータは、ASA に接続するインターフェイス上の 10.255.0.100 宛のパケットを受信します。 ルータは合致するネクスト ホップのルーティング テーブルを確認します。 ルータは、ネクスト ホップが ASA 内部インターフェイスであることを見つけ、パケットが ASA に送信されます。
8. ステップ 1 に戻ります。

次に例を示します。



このループは、このパケットの TTL が 0 に減少するまで発生します。 ASA ファイアウォールがパケットを処理するときに、デフォルトで TTL 値を減じることは**ない**ということに注意してください。 ルータがパケットをルーティングすると、TTL が減じられます。 これにより、無限ループの発生は抑止されますが、それでも、このループによって ASA でトラフィック負荷は増大し、CPU 使用率が急激に上昇します。

問題： VPN クライアントによって生成された送信（ネットワーク）ブロードキャスト パケットがネットワーク内部でループする

この問題は、最初の問題に似ています。 VPN クライアントが、割り当てられた IP サブネット（上記の例では 10.255.0.255）に送信されたブロードキャスト パケットを生成すると、そのパケットは、ASA によってユニキャスト フレームとして内部ルータに転送される場合があります。 それから内部ルータがそれを ASA に転送して戻すことで、TTL が期限切れになるまでパケットがループします。

この一連のイベントは、以下の場合に発生します。

1. VPNクライアント マシンは、ネットワーク ブロードキャスト アドレス 10.255.0.255 宛のパケットを生成し、パケットが ASA に到達します。
2. ASA はこのパケットをユニキャスト フレームとして扱い（ルーティング テーブルによって）、これを内部ルータに転送します。

3. 内部ルータもこのパケットをユニキャスト フレームとして扱い、パケットの TTL を削減して ASA に転送して戻します。

4. このプロセスは、パケットの TTL が 0 に減じられるまで繰り返されます。

問題の解決策

この問題の根本的な解決策は、いくつか考えられます。 ネットワーク トポロジおよび特定の状況によって、一方のソリューションが他方のソリューションより容易に実装可能である場合があります。

ソリューション 1：Null0 インターフェイスのスタティック ルート（ASA バージョ

ン 9.2.1 以降)

トラフィックを Null0 インターフェイスに送信するときに、指定したネットワーク宛のパケットをドロップします。 この機能は、Border Gateway Protocol (BGP) の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 この場合、リモート アクセス クライアント サブネットの Null0 へのルートを設定するときに、より詳細に指定されたルート (リバース ルート インジェクションによって提供される) が存在しない場合は、ASA がサブネット内のホスト宛のトラフィックを強制的にドロップします。

```
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
```

ソリューション2：VPN クライアント用に別の IP プールを使用する

このソリューションは、リモート VPN ユーザに内部ネットワークのサブネットと重複しない IP アドレスを割り当てるものです。 これにより、VPN ユーザが接続されていない場合に ASA が内部ルータに戻る VPN サブネット宛のパケットを転送しないようにします。

ソリューション 3：ソリューション 3：ASA ルーティング テーブルを内部ルートについてより詳細に指定する

このソリューションは、ASA のルーティング テーブルに VPN IP プールと重複する非常に広範なルートがないようにします。 この特定のネットワークの例では、10.0.0.0/8 ルートを ASA から削除し、内部インターフェイスに存在するサブネットに、より詳細に指定されたスタティック ルートを設定します。 サブネットの数およびネットワーク トポロジによっては、スタティック ルートの数が多数となることがあり、これは可能ではない場合があります。

ソリューション 4：外部インターフェイスから VPN サブネットに戻る、より詳細に指定されたルートを追加する

このドキュメントに記載されているその他のソリューションより、このソリューションはより複雑です。 この項の注で後ほど説明する状況のため、シスコは最初に他のソリューションを試すことを推奨します。 このソリューションは、ASA が VPN IP サブネットから送信される IP パケットを内部ルータに転送しないようにします。 外部インターフェイスから VPN サブネットへのより詳細に指定されたルートを追加することでこれを実行できます。 この IP サブネットは外部 VPN ユーザ用に予約されているため、この VPN IP サブネットからのソース IP アドレスを持つパケットは、ASA 内部インターフェイスにインバウンドで到達することはありません。 これを実現する最も簡単な方法は、アップストリーム ISP ルータのネクスト ホップ IP アドレスを持つ外部インターフェイスからリモート アクセス VPN の IP プールのルートを追加することです。

このネットワーク トポロジの例では、そのルートは次のようになります。

```
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
```

このルートに加えて、外部インターフェイスに優先ルートが存在することから、ASA が VPN IP サブネットから送信され内部インターフェイス上のインバウンドで受信したパケットをドロップするために、ip verify reverse-path inside コマンドを追加します。

```
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
```

これらのコマンドを実装すると、ユーザが接続しているときの ASA ルーティング テーブルは、次のようになります。

```
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
```

VPN クライアントが接続されると、VPN IP アドレスへのホストベースのルートがテーブルに存在し、優先されます。 ip verify reverse-path inside コマンドのため、VPN クライアントが切断されると、クライアント IP アドレスから送信され内部インターフェイスに着信するトラフィックがルーティング テーブルに照らして確認され、ドロップされます。

VPN クライアントが VPN IP サブネットへの送信ネットワーク ブロードキャストを生成すると、そのパケットは内部ルータに転送され、ルータによって転送され ASA に戻されます。ここで ip

verify reverse-path inside のためドロップされます。

> **注:** このソリューションが実装されると、same-security permit intra-interface コマンドが構成に存在していて、アクセス ポリシーによってこれが許可される場合、接続していないユーザ向けの VPN IP プール内の IP アドレス宛に VPN ユーザから送信されるトラフィックは、クリア テキストで外部インターフェイスからルーティングされ戻される可能性があります。 これはまれな状況であり、VPN ポリシー内で vpn-filter を使用することで発生を抑えることができます。 この状況が発生するのは、same-security permit intra-interface コマンドが ASA の構成に存在する場合のみです。
>
> 同様に、内部ホストが VPN プール内の IP アドレス宛のトラフィックを生成し、その IP アドレスがリモート VPN ユーザに割り当てられていない場合、トラフィックはクリア テキストで ASA の外部に出力される場合があります。