ポリシーベースのVPNトンネル内のクリプトACLカウンタについて

内容

はじめに

このドキュメントでは、ポリシーベースのVPNトンネル内での暗号アクセスコントロールリスト(ACL)カウンタの動作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。

- Cisco IOS®/Cisco IOS® XEプラットフォームでのポリシーベースのサイト間VPN
- Cisco IOS/Cisco IOS XEプラットフォームのアクセスコントロールリスト

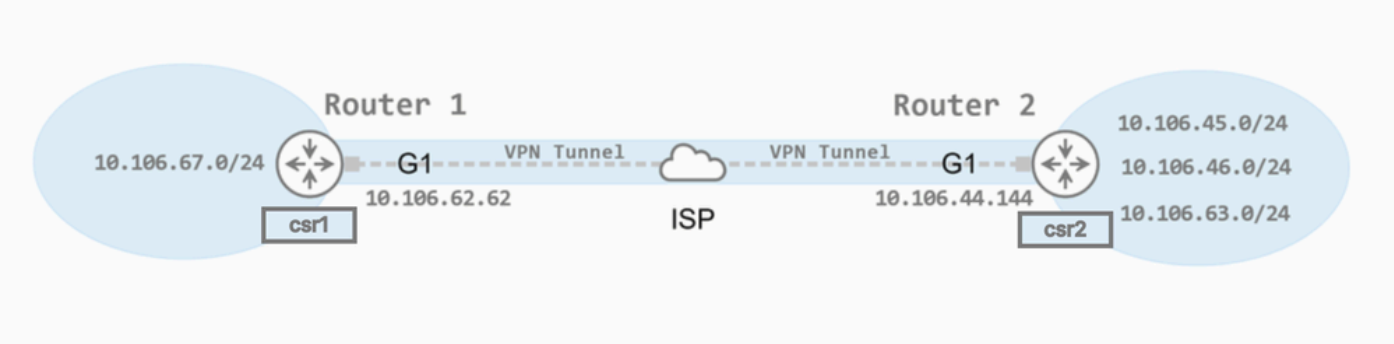
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco C8kv、バージョン17.12.04(MD)

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ



トポロジ

シナリオ

2つの異なるシナリオを調べることにより、異なるピアからトラフィックが開始された場合とトンネルがリセットされた場合に、ACLヒットカウントがどのように影響を受けるのかを理解することを目的としています。

1. シナリオ1:VPNトンネルが非アクティブな間にRouter1から開始されたトラフィック

   このシナリオでは、VPNトンネルが最初にダウンし、Router1からトラフィックが開始されるときに、ACLヒットカウントの変化が分析されます。この分析は、初期設定と、最初のトラフィックフローの試行に対するクリプトACLカウンタの反応を理解するのに役立ちます。

2. シナリオ2:VPNトンネルがアクティブな状態でRouter2から開始されるトラフィック

   このシナリオでは、VPNトンネルはすでに確立されており、Router2からトラフィックが開始されます。このシナリオでは、トンネルがアクティブで、トラフィックが別のピアから送信された場合のACLカウンタの動作について詳しく説明します。

これらのシナリオを比較することで、さまざまな条件下でのVPNトンネル内のACLカウンタのダイナミクスを包括的に理解できます。

コンフィギュレーション

ピアとして指定された2台のCisco C8kvルータ間に、ポリシーベースのサイト間VPNトンネルを

設定しました。ルータ1の名前は「csr1」、ルータ2の名前は「csr2」です。

Router1の暗号設定

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Router2での暗号設定

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

VPNトンネル内の暗号アクセスコントロールリストカウンタの動作分析

最初は、両方のデバイスのそれぞれのクリプトアクセスリストで、ACLヒット数が0になっています。

両方のピアデバイスのそれぞれの暗号化アクセスリストでのアクセスコントロールリストヒットカウントが0である。

シナリオ1:VPNトンネルが非アクティブな間にRouter1から開始されたトラフィック

初期状態：

Router1(IP:10.106.67.27)とRouter2(IP:10.106.45.145)を接続するVPNトンネルは、現在非アクテ

ィブです。

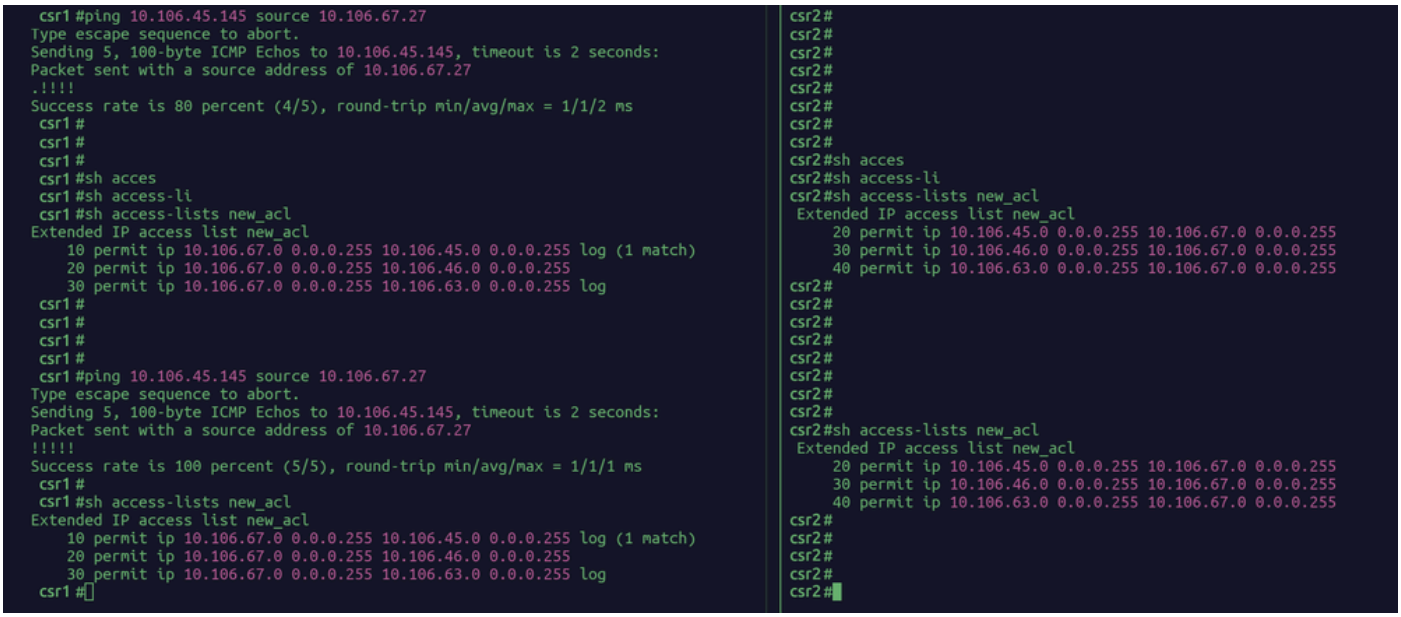
アクション実施済み:

トラフィックは、ルータ2との通信を確立することを目的として、ルータ1から開始されます。

観察:

1. ACLカウンタの動作：
   a. Router1からトラフィックを開始すると、Router1のアクセスコントロールリスト(ACL)カウンタが顕著に増加します。この増加は、トンネルの確立が試行された時点で1回だけ発生します。
   b. ACLカウンタの上昇は、発信側のルータ（このシナリオではRouter1）でのみ観察されます。この段階では、ルータ2はACLカウンタの変更を反映しません。
2. トンネルの確立:
   a.トラフィックの開始に対応する最初の増分の後、最初のルータとRouter2の間のトンネルが正常に確立されます。
   b.トンネルが確立されると、Router1のACLカウンタが安定してそれ以上の増加は示されなくなります。これは、ACLルールが一致し、確立されたトンネルを通じてトラフィックが継続的に許可されていることを示します。
3. トンネルの再始動：
   Router1のACLカウンタに対する追加の増分が発生するのは、トンネルがドロップして再確立が必要になった場合だけです。これは、トンネルがアクティブになった後の継続的なデータ転送ではなく、トンネルの確立を試行する最初のトラフィック開始によってACLルールがトリガーされることを示唆します。

要約すると、このシナリオでは、Router1のACLカウンタがトンネル作成の最初のトラフィック試行の影響を受けるものの、VPNトンネルがアップ状態で動作可能になった後はスタティックのままであることを示しています。



シナリオ1

シナリオ2:VPNトンネルがアクティブな状態でRouter2から開始されるトラフィッ

ク

初期状態：

Router1(IP:10.106.67.27)とRouter2(IP:10.106.45.145)を接続するVPNトンネルは、現在アクティブで稼働しています。

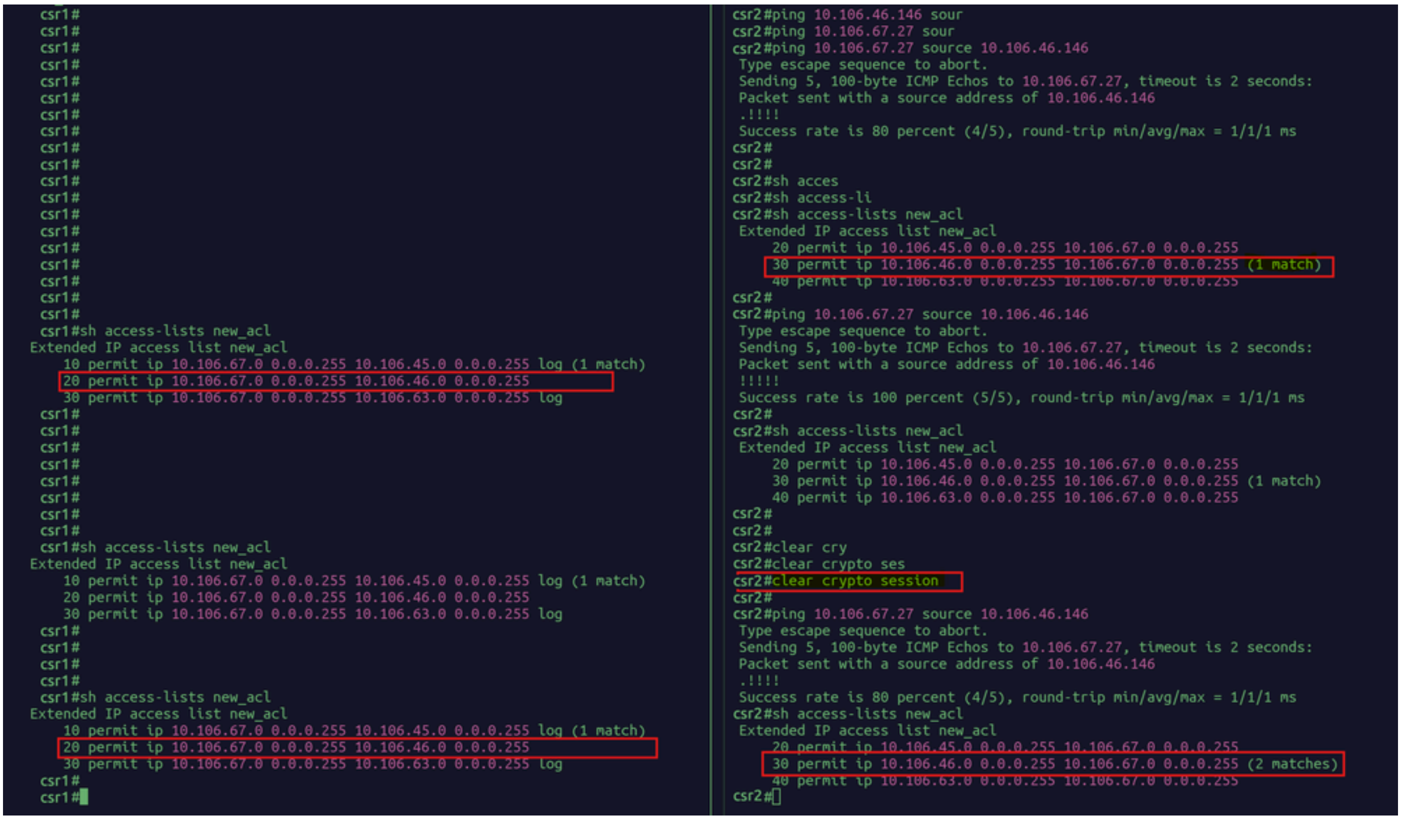
アクション実施済み:

1. トンネルがアップ状態の間、トラフィックはRouter2からRouter1に向けて開始されます。
2. その後、トンネルは意図的にクリア（またはリセット）されます。
3. トンネルがクリアされた後、Router2は接続を再確立するために再度トラフィックを開始します。

観察:

1. 最初のトラフィック開始：
   a.トンネルがすでに確立されている状態で、トラフィックが最初にRouter2から開始された場合、Access Control List（ACL；アクセスコントロールリスト）のカウンタは即座には変更されません。
   b.これは、すでに確立されたトンネル内の進行中のトラフィックによってACLカウンタの増分がトリガーされないことを示します。
2. トンネルのクリアと再始動：
   a.トンネルをクリアすると、最初のルータとRouter2の間に確立されている接続が一時的に中断されます。これにより、後続のトラフィックの再確立プロセスが必要になります。
   b.トンネルがクリアされた後にRouter2からトラフィックが再始動すると、Router2のACLカウンタが著しく増加します。この増加は、トンネルの作成を容易にするためにACLルールが再度使用されていることを示します。
3. ACLカウンタの特殊性：
   ACLカウンタの増分は、トラフィックを開始した側（この場合はRouter2）だけで発生します。この動作により、発信側でのトラフィック開始プロセスの監視と制御におけるACLの役割が明らかになります。このフェーズでは、Router1のACLカウンタは影響を受けません。

要約すると、このシナリオでは、Router2のACLカウンタが、VPNトンネルの再確立時にトラフィックの開始に応答することを示しています。カウンタは、アクティブなトンネル内の通常のトラフィックフローでは増加しませんが、トンネルの再確立の必要性に反応し、トンネル開始イベントの正確なトラッキングを確保します。



シナリオ 2

結論：

クリプトACLカウンタの動作から、VPNトンネルの開始フェーズでだけヒットカウントが登録されることがわかります。

イニシエータ固有の増分：トンネルがRouter1から開始されると、ヒットカウントの増加はRouter1だけで観察されます。同様に、ルータ2から開始した場合、ヒットカウントはルータ2でのみ上昇します。これは、送信元でトラフィック開始プロセスを監視する際のACLの役割を示しています。

確立後の安定性：トンネルが正常に確立されると、両方のピアのACLカウンタは変化せず、それ以上のヒットはないことを示します。この安定性は、トンネルがクリアまたはリセットされ、トラフィックの開始が再試行されるまで維持されます。
この動作は、トンネル作成の初期フェーズを追跡および制御するAccess Control List（ACL；アクセスコントロールリスト）の機能を明確に示しており、確立済みのトンネル内での後続のデータフローがヒット数に影響を与えないようにします。

主なポイント

ACLカウンタの動作：ACLカウンタレジスタは、トンネルの開始プロセス中にイニシエータ側だけで増加します。これは、トンネルの確立をトリガーする最初のトラフィックをモニタするようにカウンタが設計されていることを示します。

確立後のスタティックカウンタ：トンネルがアクティブで確立されると、ACLカウンタは変更されずに残ります。トンネルがリセットされて再始動の必要が生じない限り、これらはそれ以上の

アクティビティを反映しないため、最初のトラフィックイベントに重点が置かれていることが強調されます。

トラフィック開始指定：ACLヒットカウントはトンネルを開始しているピアに固有です。この特異性により、どちらの側がVPN接続を開始するかを正確に追跡でき、正確な監視と制御が可能になります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。