Cisco IOS XEルータでのマルチSA仮想トンネルインターフェイスの設定

内容

概要

このドキュメントでは、Cisco IOS® XEソフトウェアを使用するCiscoルータでマルチセキュリティアソシエーション(Multi-SA)仮想トンネルインターフェイス(VTI)を設定する方法について説明します。移行プロセスについても説明します。マルチSA VTIは、クリプトマップベース（ポリシーベース）のVPN設定に代わるものです。暗号マップベースおよびその他のポリシーベースの実装と下位互換性があります。この機能は、Cisco IOS XEリリース16.12以降でサポートされています。

前提条件

要件

Cisco IOS XEルータのIPsec VPN設定に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS XEリリース16.12.01aを搭載したサービス統合型ルータ(ISR)4351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、初期（デフォルト）設定の状態から起動しています。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。

背景説明

クリプトマップと比較したVTIの利点

暗号マップは、物理インターフェイスの出力機能です。異なるピアへのトンネルが同じクリプトマップで設定されている。クリプトマップのアクセスコントロールリスト(ACL)エントリは、特定のVPNピアに送信されるトラフィックを照合するために使用されます。このタイプの設定は、ポリシーベースVPNとも呼ばれます。

VTIの場合、各VPNトンネルは個別の論理トンネルインターフェイスで表されます。ルーティングテーブルは、トラフィックが送信されるVPNピアを決定します。このタイプの設定は、ルートベースVPNとも呼ばれます。

Cisco IOS XEリリース16.12より前のリリースでは、VTI設定はクリプトマップ設定と互換性がありませんでした。相互運用するには、トンネルの両端を同じタイプのVPNで設定する必要がありました。

Cisco IOS XEリリース16.12では、新しい設定オプションが追加されました。このオプションを使用すると、トンネルインターフェイスはプロトコルレベルでポリシーベースのVPNとして機能しますが、トンネルインターフェイスのすべてのプロパティを持つことができます。

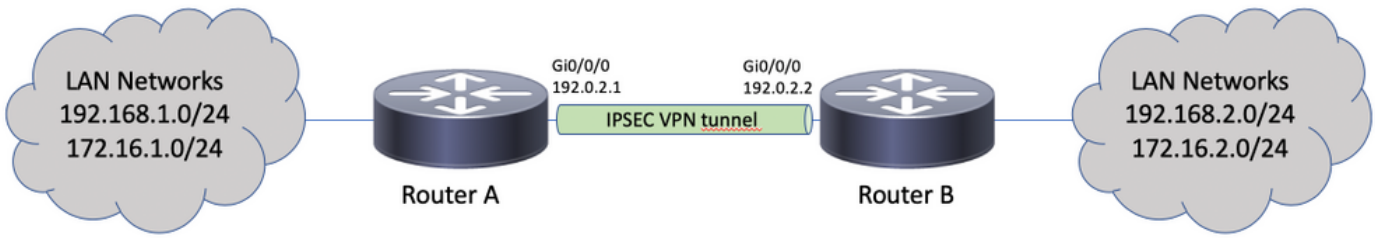
シスコは、Cisco IOS XEリリース17.6のCisco IPsecスタティック暗号マップおよびダイナミック暗号マップ機能のサポート終了日を発表しました。

暗号マップに対するVTIの利点は次のとおりです。

- トンネルのアップ/ダウンステータスを簡単に判別できます。
- トラブルシューティングが簡単です。
- Quality of Service(QoS)、ゾーンベースファイアウォール(ZBF)、ネットワークアドレス変換(NAT)、Netflowなどの機能をトンネル単位で適用できます。
- すべてのタイプのVPNトンネルに対する設定が合理化されています。

設定

ネットワーク図



ルーティングの考慮事項

管理者は、リモートネットワークのルーティングがトンネルインターフェイスを指していること

を確認する必要があります。「 **reverse-route** IPsecプロファイルの下のオプションを使用すると、クリプトACLで指定されたネットワークのスタティックルートを自動的に作成できます。このようなルートは手動で追加することもできます。以前に、より詳細なルートが設定されている場合、そのルートがトンネルインターフェイスではなく物理インターフェイスを指している場合は、これらを削除する必要があります。

設定例

クリプトマップベースのIKEv1トンネルのマルチSA sVTIへの移行

両方のルータには、Internet Key Exchange Version 1(IKEv1)クリプトマップベースのソリューションが事前設定されています。

ルータ A

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.2
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

ルータ B

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.1
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
match address CACL
!
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

ルータAをマルチSA VTI設定に移行するには、次の手順を実行します。ルータBは古い設定のままにすることも、同様に再設定することもできます。

1. インターフェイスからクリプトマップを削除します。
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. IPsecプロファイルを作成します。リバースルートは、リモートネットワークのスタティックルートが自動的にルーティングテーブルに追加されるようにオプションで設定されます。
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. トンネル インターフェイスを設定します。暗号化ACLは、IPsecポリシーとしてトンネル設定に適用されます。トンネルインターフェイスに設定されているIPアドレスは関係ありませんが、何らかの値を設定する必要があります。このIPアドレスは、 **ip unnumbered** コマンドにより、WLC CLI で明確に示されます。
   ```
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec policy ipv4 CACL
   tunnel protection ipsec profile PROF
   ```
4. その後、クリプトマップエントリを完全に削除できます。
   ```
   no crypto map CMAP 10
   ```

   最終的なルータAの設定

   ```
   crypto isakmp policy 10
   encryption aes
   hash sha256
   authentication pre-share
   group 14
   !
   crypto isakmp key cisco123 address 192.0.2.2
   !
   crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
   !
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   !
   ip access-list extended CACL
   permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
   permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
   !
   interface GigabitEthernet0/0/0
   ip address 192.0.2.1 255.255.255.0
   !
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec policy ipv4 CACL
   tunnel protection ipsec profile PROF
   ```

クリプトマップベースのIKEv2トンネルのマルチSA sVTIへの移行

両方のルータには、Internet Key Exchange Version 2(IKEv2)クリプトマップベースのソリューションが事前に設定されています。

ルータ A

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

ルータ B

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.1 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

ルータAをマルチSA VTI設定に移行するには、次の手順を実行します。ルータBは古い設定のままにすることも、同様に再設定することもできます。

1. インターフェイスからクリプトマップを削除します。
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. IPsecプロファイルを作成します。「 **reverse-route** コマンドは、リモートネットワークのスタティックルートが自動的にルーティングテーブルに追加されるようにオプションで設定されます。
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   ```

```
set ikev2-profile PROF
reverse-route
```

3. トンネル インターフェイスを設定します。暗号化ACLは、IPsecポリシーとしてトンネル設定に適用されます。トンネルインターフェイスに設定されているIPアドレスは関係ありませんが、何らかの値を設定する必要があります。このIPアドレスは、 **ip unnumbered** コマンドにより、WLC CLI で明確に示されます。

```
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

4. クリプトマップを完全に削除します。

```
no crypto map CMAP 10
```

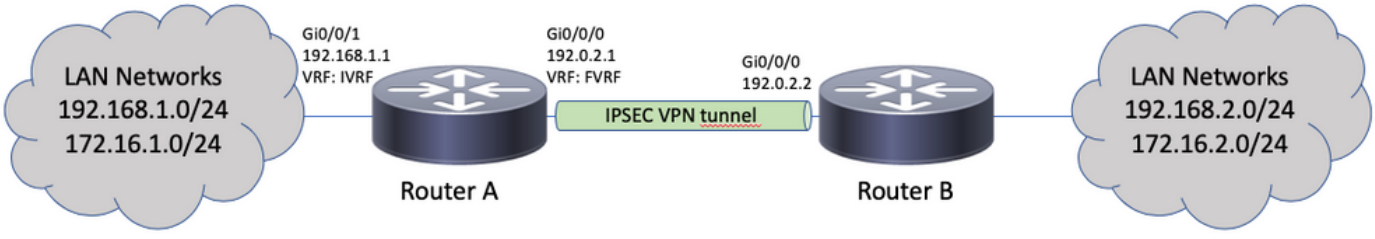
最終的なルータAの設定

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto ipsec profile PROF
set transform-set TSET
set ikev2-profile PROF
reverse-route
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
!
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

マルチSA VTIへのVRF対応クリプトマップの移行

この例では、VRF対応のクリプトマップ設定を移行する方法を示します。

トポロジ



暗号マップの設定

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
vrf ivrf
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set isakmp-profile PROF
match address CACL
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

マルチSA VTIへの移行に必要な手順は次のとおりです。

```
! vrf configuration under isakmp profile is only for crypto map based configuration
!
crypto isakmp profile PROF
no vrf ivrf
!
interface GigabitEthernet0/0/0
no crypto map
!
no crypto map CMAP 10
!
no ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
no ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
```

```
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

最終的なVRF対応の設定

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

Cisco CLI Analyzer(登録ユーザ専用)では、次の機能がサポートされています **show** コマンドを発

行します。Cisco CLIアナライザを使用して、 **show** コマンド出力.

トンネルが正常にネゴシエートされたかどうかを確認するには、トンネルインターフェイスのステータスを確認できます。最後の2列 – Status と Protocol – ステータスの表示 up トンネルが動作している場合：

```
RouterA#show ip interface brief | include Interface|Tunnel0
Interface IP-Address OK? Method Status Protocol
Tunnel0 192.0.2.1 YES TFTP up                    up
```

現在の暗号化セッションのステータスの詳細については、 **show crypto session** エラーが表示される場合があります。「 Session status （ UP-ACTIVE ikeセッションが正しくネゴシエートされたことを示します。

```
RouterA#show crypto session interface tunnel0
Crypto session current status

Interface: Tunnel0
Profile: PROF
Session status: UP-ACTIVE
Peer: 192.0.2.2 port 500
Session ID: 2
IKEv2 SA: local 192.0.2.1/500 remote 192.0.2.2/500 Active
IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 172.16.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

リモートネットワークへのルーティングが正しいトンネルインターフェイスを指していることを確認します。

```
RouterA#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Tunnel0
Route metric is 0, traffic share count is 1

RouterA#show ip cef 192.168.2.100
192.168.2.0/24
attached to Tunnel0
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

IKEプロトコルネゴシエーションをトラブルシューティングするには、次のデバッグを使用します。

> **注**：使用する前に、『debugコマンドの重要な情報』を参照してください **debug** コマンドを発行します。

```
! For IKEv1-based scenarios:
debug crypto isakmp
debug crypto ipsec
```

```
! For IKEv2-based scenarios:
debug crypto ikev2
debug crypto ipsec
```

よく寄せられる質問（FAQ）

トンネルは自動的に起動しますか。または、トンネルを起動するためにトラフィックが必要ですか。

暗号マップとは異なり、マルチSA VTIトンネルは、暗号ACLに一致するデータトラフィックがルータを通過するかどうかにかかわらず、自動的に確立されます。トンネルは、対象トラフィックがない場合でも、常にアップ状態になります。

トラフィックがVTI経由でルーティングされても、トラフィックの送信元または宛先がこのトンネルのIPsecポリシーとして設定されたクリプトACLと一致しない場合はどうなりますか。

このようなシナリオはサポートされていません。暗号化を目的としたトラフィックだけをトンネルインターフェイスにルーティングする必要があります。ポリシーベースルーティング(PBR)は、特定のトラフィックだけをVTIにルーティングするために使用できます。PBRはIPsecポリシーACLを使用して、VTIにルーティングされるトラフィックを照合できます。

各パケットは設定されたIPsecポリシーに照らしてチェックされ、暗号ACLと一致する必要があります。一致しない場合、暗号化されず、トンネル送信元インターフェイスからクリアテキストで送信されます。

同じ内部VRF(iVRF)とフロントVRF(fVRF)が使用されている場合(iVRF = fVRF)、ルーティングループが発生し、パケットが理由を付けてドロップされます **Ipv4RoutingErr**.このようなドロップの統計情報は、 **show platform hardware qfp active statistics drop** コマンドにより、WLC CLI で明確に示されます。

```
RouterA#show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

---------------------------------------------------------------------
Global Drop Stats Packets Octets
---------------------------------------------------------------------
Ipv4RoutingErr 5 500
```

iVRFがfVRFと異なり、iVRFでトンネルに入り、IPsecポリシーと一致しないパケットは、fVRFのトンネル送信元インターフェイスからクリアテキストで出力されます。VRF間にルーティングループが存在しないため、これらは廃棄されません。

マルチSA VTIでは、VRF、NAT、QoSなどの機能はサポートされていますか。

はい。これらの機能はすべて、通常のVTIトンネルと同じ方法でサポートされます。