IPsec VTI でのセキュア eBGP セッションの設定

内容

概要

このドキュメントでは、データ プレーン トラフィック用の物理インターフェイス（非トンネル）とともに IPsec 仮想トンネル インターフェイス（VTI）を使用して、外部ボーダー ゲートウェイ プロトコル（eBGP）ネイバー関係を保護する方法について説明します。この構成には、次のような利点があります。

- データの機密性、アンチリプレイ、認証、整合性を伴う BGP ネイバー セッションのプライバシーを実現します。
- データ プレーン トラフィックには、トンネル インターフェイスの最大伝送単位（MTU）オーバーヘッドの制限がありません。お客様は、パフォーマンスへの影響やフラグメンテーションなしで標準 MTU パケット（1500 バイト）を送信できます。
- セキュリティ ポリシー インデックス（SPI）の暗号化および復号化が BGP コントロール プレーン トラフィックに制限されるため、エンド ポイント ルータのオーバーヘッドが小さくなります。

この設定のメリットは、データ プレーンがトンネル インターフェイスの制限に拘束されないことです。設計上、データ プレーン トラフィックは IPSec 保護ではありません。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- eBGP の設定と検証の基本
- ルート マップを使用する BGP ポリシー アカウンティング（PA）操作
- 基本の Internet Security Association and Key Management Protocol（ISAKMP）および Ipsec ポリシー機能

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®ソフトウェアリリース15.3(1.3)Tに基づいていますが、他のサポートされているバージョンでも動作します。IPsec 設定は暗号化機能であるため、ご使用のコードのバージョンにこの機能セットが含まれていることを確認します。

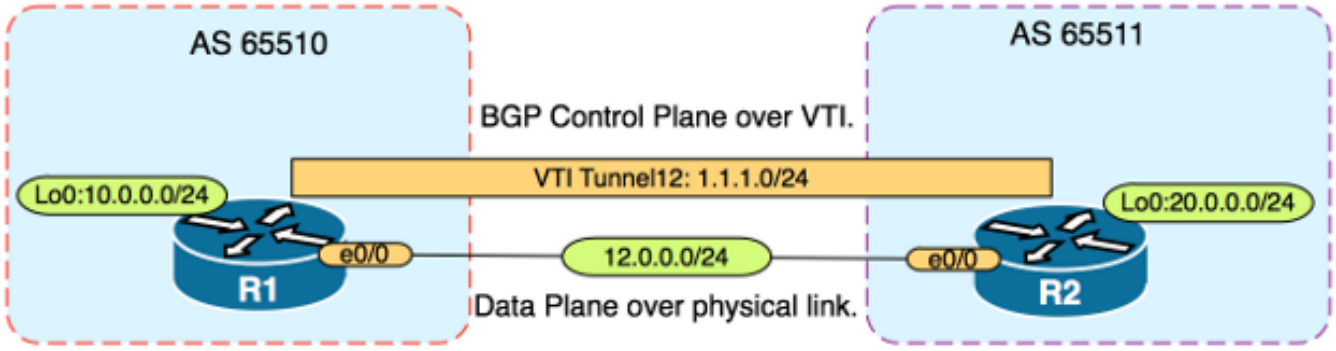
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

> **注意**：このドキュメントの設定例では、無難な暗号化アルゴリズムを使用しており、お客様の環境に適している場合も、適さない場合もあります。さまざまな暗号スイートとキー サイズの相対的なセキュリティの詳細については、次世代暗号化に関するホワイト ペーパーを参照してください。

設定

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



設定

次のステップを実行します。

1. R1 の事前共有キーを使用して、R1 と R2 のインターネット キー エクスチェンジ（IKE）フェーズ 1 パラメータを設定します。 **注**：不良と判断されるため、DH グループ番号の 1、2、5 を使用しないでください。可能であれば、グループ19、20、24などの楕円曲線暗号(ECC)を持つDHグループを使用してください。高度暗号化規格(AES)およびセキュアハッシュアルゴリズム256(SHA256)は、データ暗号規格(DES)/3DESおよびメッセージ5(MD)それぞれMD5)/SHA1です。実稼働環境では「cisco」というパスワードを使用しないでください。**R1 の設定**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
```

```
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
R1(config-isakmp)exit

R1(config)#crypto isakmp key CISCO address 12.0.0.2
```

R2 の設定

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```

2. R1とR2のNVRAMの事前共有キーにレベル6パスワード暗号化を設定します。これにより、プレーンテキストで保存された事前共有キーが、ルータが侵害された場合に読み取られる可能性が減ります。

```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```

注：レベル 6 パスワード暗号化を有効にすると、次のように、アクティブな設定で事前共有キーのプレーン テキスト バージョンが表示されなくなります。

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. R1 と R2 の IKE フェーズ 2 パラメータを設定します。 **R1 の設定**

```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```

R2 の設定

```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```

注：Perfect Forward Secrecy（PFS）の設定はオプションですが、IKE フェーズ 2 SA の確立時に新しい対称キーの生成を強制するため、VPN 強度を向上させます。

4. R1 と R2 のトンネル インターフェイスを設定し、IPsec プロファイルで保護します。 **R1 の設定**

```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0
```

```
R1(config-if)#tunnel mode ipsec ipv4

R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```

R2 の設定

```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. R1 と R2 の BGP を設定し、loopback0 ネットワークを BGP にアドバタイズします。 **R1 の設定**

```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```

R2 の設定

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```

6. 手動でネクスト ホップの IP アドレスを変更するために、R1 と R2 のルート マップを設定し、トンネルではなく、物理インターフェイスを指すようにします。このルート マップをインバウンド方向に適用する必要があります。 **R1 の設定**

```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```

R2 の設定

```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end
```

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

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。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

IKE フェーズ 1 と IKE フェーズ 2 の両方が完了したことを検証します。 仮想トンネル インターフェイス (VTI) の回線プロトコルは IKE フェーズ 2 が完了するまで「up」に変更されることはありません。

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

ルート マップの適用の前に、ネクストホップ IP アドレスが次のようにトンネル インターフェイスである BGP ネイバーの IP アドレスを指していることに注意してください。

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

トラフィックがトンネルを使用する場合、MTU はトンネル MTU に制限されます。

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)
```

```
R1#show interfaces tunnel 12 | inc transport|line

Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

ルート マップを適用すると、IP アドレスはトンネルではなく、R2 の物理インターフェイスに変更されます。

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

トンネルが標準サイズの MTU を許可するのとは対照的に、物理的なネクスト ホップを使用するために、データ プレーンを変更します。

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。