二重 ISP シナリオの ASA 仮想 な トンネルインターフェイスを設定して下さい

目次

概要

この資料に IKEv2 （ Internet Key Exchange （ IKE ） 2 つのブランチの使用で 2 ASA 間の VTI （ 仮想 な トンネル Intrfaces ）を（ 適応型セキュリティ アプライアンス（ ASA ））間のセキュア接続を提供する 2 ）バージョン プロトコル設定する方法を記述されています。 ブランチの両方に高い availablility およびロード バランシング目的への 2 つの ISP リンクがあります。 Border Gateway Protocol （ BGP ）隣接性はトンネルに内部 ルーティング情報を交換するために確立されます。 この機能は ASA バージョン 9.8(1)で導入されます。 ASA VTI 実装は IOSルータで利用可能 な VTI 実装と互換性があります。

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。

- BGP プロトコル

使用するコンポーネント

この文書に記載されている情報は 9.8(1)6 ソフトウェア バージョンを実行する ASAv ファイアウォールに基づいています。

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、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。

VTI とクリプト マップの違い

- クリプト マップはインターフェイスの出力 機能です。 クリプト マップを通してトラフィックを送信 することはトンネルを基づかせていました、トラフィックはインターフェイスに（ 従来 outside インターフェイスと呼ばれる ）直面するインターネットにルーティングされるを必要とし、暗号 ACL と一致する必要があります。 一方では、VTI は論理インターフェイスです。 各 VPN ピアへのトンネルは異なる VTI によって表されます。 ルーティングが VTI の方に指す場合、パケットは対応した ピアに暗号化され、送信 されます。

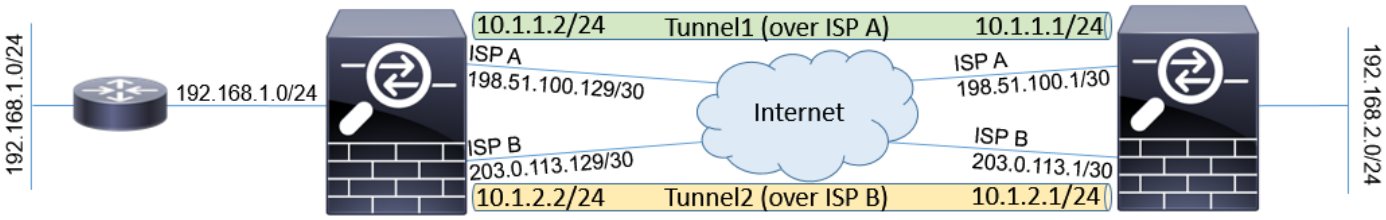
- VTI は暗号 アクセス リストおよびネットワーク アドレス変換（ NAT ）免除ルールを使用する必要を省きます。

- クリプト マップ Access Control List （ ACL ）はオーバーラップ エントリを可能にしません。 VTI は解決するために設定およびプロセスを簡素化するルートによって基づく VPN であり、規則的なルーティング ルールは VPN トラフィックに適用されます。

- クリプト マップは自動的にトンネルがダウンしている場合クリアテキストで送信 されるべきサイト間のトラフィックを防ぎます。 VTI はそれから自動的に保護しません。 ヌル ルートは等しい機能性を確認するために追加される必要があります。

設定

ネットワーク図



設定

注: この例は ASA は independed 自律システムのメンバー、ISP ネットワークの BGP ピアリングがあるシナリオのために適していません。 それは ASA に異なる自律システムからのパブリックアドレスとの 2 つの独立 した ISP リンクがあるトポロジーをカバーします。 そのようなケースでは、受け取り パケットは別の ISP に属するパブリック IP から送信されないかどうか確認する ISP はアンチスプーフィング保護を展開するかもしれません。 この設定ではこれを防ぐ、適切な手段は奪取 されます。

1. よくある暗号化および認証パラメータ。 推奨される暗号パラメータについての情報はで見つけることができます: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

両方の ASA:

```
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 24
prf sha256
lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal PROP
protocol esp encryption aes-256
protocol esp integrity sha-256
```

2. IPSec プロファイルを設定して下さい。 側の 1 つは発信側でなければなり、1 は IKEv2 ネゴシエーションの応答側である必要があります:

残っている ASA:

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
responder-only
```

ASA 権限:

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
```

3. 両方の ISP インターフェイスのイネーブル IKEv2 プロトコル。

両方の ASA:

```
crypto ikev2 enable ispa
crypto ikev2 enable ispb
```

4. 相互に ASA を認証するために事前共有キーを設定して下さい:

残っている ASA:

```
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

ASA 権限:

```
tunnel-group 198.51.100.129 type ipsec-l2l
tunnel-group 198.51.100.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.129 type ipsec-l2l
tunnel-group 203.0.113.129 ipsec-attributes
```

```
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

5. ISP インターフェイスを設定して下さい:

   残っている ASA:
   ```
   interface GigabitEthernet0/1
   nameif ispa
   security-level 0
   ip address 198.51.100.129 255.255.255.252
   !
   interface GigabitEthernet0/2
   nameif ispb
   security-level 0
   ip address 203.0.113.129 255.255.255.252
   !
   ```
   ASA 権限:
   ```
   interface GigabitEthernet0/1
   nameif ispa
   security-level 0
   ip address 198.51.100.1 255.255.255.252
   !
   interface GigabitEthernet0/2
   nameif ispb
   security-level 0
   ip address 203.0.113.1 255.255.255.252
   !
   ```
6. プライマリ リンクは ISP A インターフェイスです。 ISP B はセカンダリです。 プライマリ リンク アベイラビリティは PING 宛先としてこの例のインターネットのホストへの ICMP Ping 要求の使用と、ASA 使用互い ISP A インターフェイス トラッキングされます:

   残っている ASA:
   ```
   sla monitor 1
   type echo protocol ipIcmpEcho 198.51.100.1 interface ispa
   !
   sla monitor schedule 1 life forever start-time now
   !
   track 1 rtr 1 reachability
   !
   route ispa 0.0.0.0 0.0.0.0 198.51.100.130 1 track 1
   route ispb 0.0.0.0 0.0.0.0 203.0.113.130 10
   ```
   ASA 権限:
   ```
   sla monitor 1
   type echo protocol ipIcmpEcho 198.51.100.129 interface ispa
   !
   sla monitor schedule 1 life forever start-time now
   !
   track 1 rtr 1 reachability
   !
   route ispa 0.0.0.0 0.0.0.0 198.51.100.2 1 track 1
   route ispb 0.0.0.0 0.0.0.0 203.0.113.2 10
   ```
7. プライマリ VTI はトンネル宛先の方のスタティック・ルートによってが必要である ISP B. Static に ISP A. Secondary VTI に確立されます常に確立されます。 これは ISP アンチスプーフィング ドロップを回避するために暗号化されたパケットが正しい物理インターフェイスから去るようにします:

   残っている ASA:

```
route ispa 198.51.100.1 255.255.255.255 198.51.100.130 1
route ispb 203.0.113.1 255.255.255.255 203.0.113.130 1
```

ASA 権限:

```
route ispa 198.51.100.129 255.255.255.255 198.51.100.2 1
route ispb 203.0.113.129 255.255.255.255 203.0.113.2 1
```

8. VTI 設定:

残っている ASA:

```
interface Tunnel1
nameif tuna
ip address 10.1.1.2 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.2 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

ASA 権限:

```
interface Tunnel1
nameif tuna
ip address 10.1.1.1 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.1 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

9. BGP設定。 ISP A と関連付けられるトンネルはプライマリです。 より少なくルーティングテーブルによって好まれるそれらを作る ISP B に形成されるトンネルにアドバタイズされるプレフィックスにより低いローカルprefernce があります:

残っている ASA:

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.1 remote-as 65000
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.1 remote-as 65000
neighbor 10.1.2.1 activate
neighbor 10.1.2.1 next-hop-self
neighbor 10.1.2.1 route-map BACKUP out
network 192.168.1.0
```

```
no auto-summary
no synchronization
exit-address-family
```

ASA 権限:

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.2 remote-as 65000
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 next-hop-self
neighbor 10.1.2.2 remote-as 65000
neighbor 10.1.2.2 activate
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.2.2 route-map BACKUP out
network 192.168.2.0
no auto-summary
no synchronization
exit-address-family
```

10. （オプションの）それに直接接続されない左 ASA の後ろの追加ネットワークをアドバタイズするために、スタティック ルート 再配布は設定することができます:

    残っている ASA:

    ```
    route inside 192.168.10.0 255.255.255.0 192.168.1.100 1
    !
    prefix-list REDISTRIBUTE_LOCAL seq 10 permit 192.168.10.0/24
    !
    route-map REDISTRIBUTE_LOCAL permit 10
    match ip address prefix-list REDISTRIBUTE_LOCAL
    !
    router bgp 65000
    address-family ipv4 unicast
    redistribute static route-map REDISTRIBUTE_LOCAL
    ```

11. （オプションの）トラフィックはパケット の 宛先に基づいてトンネルの間でバランスをとられるロードである場合もあります。 この例では、192.168.10.0/24 ネットワークの方のルートはバックアップ トンネル（ISP B トンネル）に好まれます

    残っている ASA:

    ```
    route-map BACKUP permit 5
    match ip address prefix-list REDISTRIBUTE_LOCAL
    set local-preference 200
    !
    route-map BACKUP permit 10
    set local-preference 80
    ```

12. トンネルならダウンしているサイト間のトラフィックがインターネットにクリアテキストで、ヌル ルートは追加される必要があります送信 されることを防ぐために。 すべての RFC1918 アドレスは簡単にするために追加されました:

    両方の ASA:

    ```
    route Null0 10.0.0.0 255.0.0.0 250
    route Null0 172.16.0.0 255.240.0.0 250
    route Null0 192.168.0.0 255.255.0.0 250
    ```

13. （オプションの）デフォルトで、ASA BGPプロセスは 1 60 秒あたりのキープアライブを一度

送信します。 キープアライブ応答が 180 秒のピアから届かない場合、完全に宣言されます。 検出 neigbor 失敗を高速化するために、BGP タイマーを設定できます。 この例では、キープアライブは 10 秒毎に送信され、ネイバーは 30 秒後に宣言されます。

```
router bgp 65000
address-family ipv4 unicast
neighbor 10.1.1.2 timers 10 30
neighbor 10.1.2.2 timers 10 30
exit-address-family
```

確認

IKEv2 トンネルが稼働しているかどうか確認して下さい:

```
ASA-right(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:32538, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
836052177 198.51.100.1/500 198.51.100.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/7 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xc6623962/0x5c4a3bce

IKEv2 SAs:

Session-id:1711, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
832833529 203.0.113.1/500 203.0.113.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/29 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x2e3715af/0xc20e22b4
```

BGP 隣接性ステータスを確認して下さい:

```
ASA-right(config)# show bgp summary
BGP router identifier 203.0.113.1, local AS number 65000
BGP table version is 29, main routing table version 29
3 network entries using 600 bytes of memory
5 path entries using 400 bytes of memory
5/3 BGP path/bestpath attribute entries using 1040 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2040 total bytes of memory
BGP activity 25/22 prefixes, 69/64 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.2 4 65000 6 5 29 0 0 00:00:51 2
10.1.2.2 4 65000 7 6 29 0 0 00:01:20 2
```

BGP から届くルーティングを確認して下さい。 で「マークされるルーティングはルーティングテーブルに >」インストールされています:

```
ASA-right(config)# show bgp

BGP table version is 29, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i192.168.1.0 10.1.1.2 0 100 0 i
* i 10.1.2.2 0 80 0 i
*> 192.168.2.0 0.0.0.0 0 32768 i
* i192.168.10.0 10.1.1.2 0 100 0 ?
*>i 10.1.2.2 0 200 0 ?

Verify routing table:

ASA-right(config)# show route

Codes: L - local, C - connected, S - static, 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, V - VPN
i - IS-IS, su - IS-IS summary, 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, + - replicated route
Gateway of last resort is 198.51.100.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.2, ispa
S 10.0.0.0 255.0.0.0 is directly connected, Null0
C 10.1.1.0 255.255.255.0 is directly connected, tuna
L 10.1.1.1 255.255.255.255 is directly connected, tuna
C 10.1.2.0 255.255.255.0 is directly connected, tunb
L 10.1.2.1 255.255.255.255 is directly connected, tunb
S 172.16.0.0 255.240.0.0 is directly connected, Null0
S 192.168.0.0 255.255.0.0 is directly connected, Null0
B 192.168.1.0 255.255.255.0 [200/0] via 10.1.1.2, 00:02:06
C 192.168.2.0 255.255.255.0 is directly connected, inside
L 192.168.2.1 255.255.255.255 is directly connected, inside
B 192.168.10.0 255.255.255.0 [200/0] via 10.1.2.2, 00:02:35
C 198.51.100.0 255.255.255.252 is directly connected, ispa
L 198.51.100.1 255.255.255.255 is directly connected, ispa
S 198.51.100.129 255.255.255.255 [1/0] via 198.51.100.2, ispa
C 203.0.113.0 255.255.255.252 is directly connected, ispb
L 203.0.113.1 255.255.255.255 is directly connected, ispb
S 203.0.113.129 255.255.255.255 [1/0] via 203.0.113.2, ispb
```

トラブルシューティング

IKEv2 プロトコルのトラブルシューティングを実行するのに使用されるデバッグ:

debug crypto ikev2 プロトコル 4
debug crypto ikev2 プラットフォーム 4

IKEv2 プロトコルのトラブルシューティングに関する詳細については:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

BGP プロトコルのトラブルシューティングに関する詳細については:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

関連情報

- **BGPルート 選択規則:**
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- **ASA BGP設定 ガイド:**
  https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- テクニカルサポートとドキュメント - Cisco Systems