デュアルISPシナリオでのASA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、IKEv2(Internet Key Exchange（IKE；インターネットキーエクスチェンジ）バージョン2)プロトコルを使用して2つのASA（適応型セキュリティアプライアンス）間のVTI（仮想トンネルインターフェイス）を設定し、2つのブランチ間のセキュアな接続を提供する方法について説明します。両方のブランチには、ハイアベイラビリティとロードバランシングを目的とした2つのISPリンクがあります。内部ルーティング情報を交換するために、トンネルを介してボーダーゲートウェイプロトコル(BGP)ネイバーシップが確立されます。
この機能は、ASAバージョン9.8(1)で導入されました。ASA VTI実装は、IOSルータで使用可能な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

このドキュメントの情報は、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。

VTIとクリプトマップの違い

- 暗号マップは、インターフェイスの出力機能です。暗号マップベースのトンネルを通じてトラフィックを送信するには、トラフィックをインターネット側のインターフェイス（従来は外部インターフェイス）にルーティングし、暗号ACLと照合する必要があります。一方、VTIは論理インターフェイスです。すべての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を指している場合、パケットは暗号化され、対応するピアに送信されます。

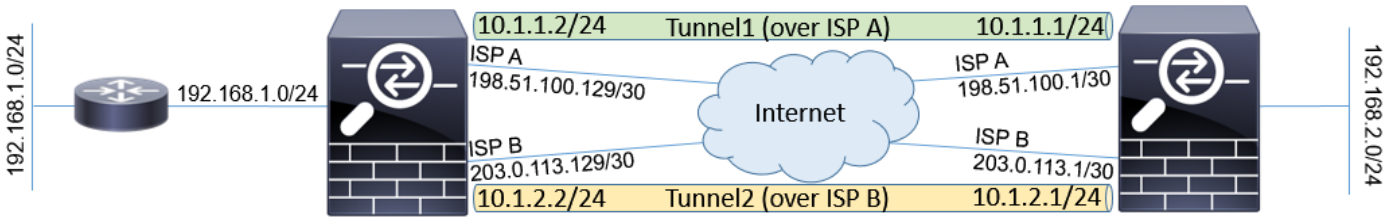
- VTIでは、暗号アクセスリストとネットワークアドレス変換(NAT)免除ルールを使用する必要がなくなります。

- 暗号マップアクセスコントロールリスト(ACL)では、エントリの重複は許可されません。VTIはルートベースのVPNであり、VPNトラフィックには通常のルーティングルールが適用されるため、設定とトラブルシューティングのプロセスが簡素化されます。

- クリプトマップは、トンネルがダウンしている場合、サイト間のトラフィックがクリアテキストで送信されるのを自動的に防止します。VTIは自動的に保護しません。同じ機能を確保するには、ヌルルートを追加する必要があります。

設定

ネットワーク図



設定

注：この例は、ASAが依存しない自律システムのメンバーであり、ISPネットワークとのBGPピアリングを持つシナリオには適していません。ASAに、異なる自律システムからのパブリックアドレスを持つ2つの独立したISPリンクがあるトポロジをカバーします。このような場合、ISPは、受信したパケットが別のISPに属するパブリックIPから送信されていないかどうかを確認するアンチスプーフィング保護を導入できます。この設定では、これを防ぐために適切な対策を講じます。

1. 共通の暗号化および認証パラメータ。推奨される暗号化パラメータについては、次を参照してください。
   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ます。一方の側が発信側であり、もう一方がIKEv2ネゴシエーションの応答側である必要があります。

ASA左：

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

ASA右：

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

3. 両方のISPインターフェイスでIKEv2プロトコルを有効にします。

両方のASA:

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

4. ASAを相互認証するように事前共有キーを設定します。

ASA左：

```
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右：

```
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ます。

ASA左：

```
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右：

```
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。プライマリリンクの可用性は、インターネット上のホストへのICMP ping要求を使用して追跡されます。この例では、ASAは互いにISP Aインターフェイスをpingの宛先として使用します。

ASA左：

```
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右：

```
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は常にISP A上で確立されます。セカンダリVTIはISP B上で確立されます。トンネルの宛先へのスタティックルートが必要です。これにより、ISPのアンチスプーフィングの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確実に残ります。

ASA左：

```
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右：

```
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の設定：

ASA左：

```
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右：

```
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の設定。ISP Aに関連付けられたトンネルはプライマリです。ISP B上で形成されたトンネルを介してアドバタイズされたプレフィックスのローカル優先順位が低いため、ルーティングテーブルでは優先順位が低くなります。

ASA左：

```
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右：

```
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）直接接続されていない追加のネットワークを左側のASAの背後にアドバタイズするには、スタティックルート再配布を設定できます。

    ASA左：

    ```
    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）トラフィックは、パケットの宛先に基づいてトンネル間でロードバランシングできます。この例では、バックアップトンネル（ISP Bトンネル）よりも192.168.10.0/24ネットワークへのルートが優先されます

    ASA左：

    ```
    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. トンネルがダウンした場合に、サイト間のトラフィックがクリアテキストでインターネットに送信されないようにするには、ヌルルートを追加する必要があります。簡単にするために、すべてのRFC1918アドレスが追加されました。

    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）デフォルトでは、ASA BGPプロセスは60秒ごとに1回キープアライブを送信します。キープアライブ応答がピアから180秒間受信されない場合は、deadと宣言されます。検出ネイバー障害を高速化するには、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秒ごとに送信され、ネイバーは30秒後にダウンとして宣言されます。

```
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を確認します。

```
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ネイバーシップステータスを確認します。

```
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から受信したルートを確認します。「>」とマークされたルートがルーティングテーブルにインストールされます。

```
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
```

トラブルシュート

IKEv2プロトコルのトラブルシューティングに使用されるデバッグ：

debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4

IKEv2プロトコルのトラブルシューティングの詳細については、次を参照してください。
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の詳細については、次を参照してください。
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ルート選択ルール：
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- ASA BGPコンフィギュレーションガイド：
  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