ASAでのポリシーベースの暗号化トンネルからルートベースの暗号化トンネルへの移行

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[設定](#)

- [移行手順：](#)
- [コンフィギュレーション](#)
  - [既存のポリシーベーストンネル：](#)
  - [ポリシーベースのトンネルからルートベースのトンネルへの移行](#)

[確認](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、ポリシーベースのトンネルからASA上のルートベースのトンネルへの移行について説明します。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- IKEv2-IPSec VPNの概念に関する基本的な知識
- ASAでのIPSec VPNとその設定に関する知識。

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 ASA:ASAコードバージョン9.8(1)以降。

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。

設定

移行手順:

1. 既存のポリシーベースのVPN設定の削除
2. IPSecプロファイルの設定
3. 仮想トンネルインターフェイス(VTI)の設定
4. スタティックルーティングまたはダイナミックルーティングプロトコルの設定

コンフィギュレーション

既存のポリシーベーストンネル：

1. インターフェイス設定：

クリプトマップがバインドされている出力インターフェイス。

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. IKEv2ポリシー：

IPSecネゴシエーションプロセスのフェーズ1のパラメータを定義する

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. トンネルグループ：

VPN接続のパラメータを定義するトンネルグループは、サイト間VPNを設定するために不可欠です。トンネルグループには、ピア、認証方式、およびさまざまな接続パラメータに関する情報が含まれているためです。

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. クリプトACL:

暗号化してトンネル経由で送信する必要があるトラフィックを定義する

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. 暗号化IPSecプロポーザル：

IPSecネゴシエーションのフェーズ2の暗号化アルゴリズムと整合性アルゴリズムを指定する
IPSecプロポーザルを定義する

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. クリプトマップの設定：

暗号化されるトラフィック、ピア、以前に設定したipsec-proposalなど、IPsec VPN接続のポリシーを定義するまた、VPNトラフィックを処理するインターフェイスにもバインドされます。

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

ポリシーベースのトンネルからルートベースのトンネルへの移行

1. 既存のポリシーベースのVPN設定の削除：
   最初に、既存のポリシーベースのVPN設定を削除します。これには、そのピアのクリプトマップエントリ、ACL、および関連する設定が含まれます。

```
no crypto map outside_map 10 match address asa-vpn
no crypto map outside_map 10 set peer 10.20.20.20
no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
```

2. IPSecプロファイルの設定：
   既存のIKEv2 ipsec-proposalまたはtransform-setを使用してIPsecプロファイルを定義します。

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. 仮想トンネルインターフェイス(VTI)の設定：
   仮想トンネルインターフェイス(VTI)を作成し、それにIPsecプロファイルを適用します。

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. スタティックルーティングまたはダイナミックルーティングプロトコルを設定します。
   スタティックルートを追加するか、ダイナミックルーティングプロトコルを設定して、トンネルインターフェイス経由でトラフィックをルーティングします。このシナリオでは、スタティックルーティングを使用しています。

   スタティックルーティング:

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

確認

Cisco ASAで仮想トンネルインターフェイス(VTI)を使用してポリシーベースのVPNからルートベースのVPNに移行した後は、トンネルがアップ状態で正常に機能していることを確認することが

重要です。ステータスを確認し、必要に応じてトラブルシューティングを行うために使用できる手順とコマンドを次に示します。

1. トンネルインターフェイスの確認
トンネルインターフェイスのステータスをチェックして、アップになっていることを確認します。

<#root>

```
ciscoasa# show interface Tunnel1

Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up

Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is
10.1.1.2/24

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
Tunnel source 10.10.10.10, destination 10.20.20.20

Tunnel protocol/transport IPSEC/IP
Tunnel protection
IPsec profile PROPOSAL_IKEV2_TSET
```

このコマンドは、動作ステータス、IPアドレス、トンネルの送信元/宛先など、トンネルインターフェイスに関する詳細を提供します。次のインジケータを確認します。
・ インターフェイスのステータスはupです。
・ 回線プロトコルのステータスはupです。

2. IPSecセキュリティアソシエーション(SA)の確認

IPSec SAのステータスをチェックして、トンネルが正常にネゴシエートされたことを確認します。

<#root>

```
ciscoasa# show crypto ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:

10.10.10.10



local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer:

10.20.20.20



#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000



#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000


#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:

10.10.10.10

/500, remote crypto endpt.:

10.20.20.20

/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)


inbound esp sas:



spi: 0xC0A80102(3232235778)


transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE



outbound esp sas:



spi: 0xC0A80101(3232235777)
```

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

Status: ACTIVE

このコマンドは、カプセル化およびカプセル化解除されたパケットのカウンタを含む、IPSec SAのステータスを表示します。次の内容を確認してください。
・ トンネルにアクティブなSAがある。
・ カプセル化カウンタとカプセル化解除カウンタが増加しており、トラフィックフローが示されています。

詳細については、次の情報を参照してください。

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:
```

Session-id:2, Status:UP-ACTIVE

```
, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
```

10.10.10.10/500 10.20.20.20/500 READY INITIATOR

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

このコマンドは、IKEv2 SAのステータスを表示します。このステータスはREADY状態です。

3. ルーティングの確認
ルーティングテーブルをチェックして、ルートがトンネルインターフェイスを正しく通過していることを確認します。

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
```

```
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, 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, H - NHRP, l - LISP
+ - replicated route, % - next hop override

S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1



S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1
```

トンネルインターフェイス経由でルーティングされたルートを探します。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

1. ASAのルートベースのトンネル設定を確認します。

2. IKEv2トンネル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できます。

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. ASAでトラフィックの問題をトラブルシューティングするには、パケットキャプチャを実行して設定を確認します。

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。