ASA 8.4 コードでの IKEv1 から IKEv2 への L2L トンネル設定のすばやい移行

内容

概要

このドキュメントでは、IKEv2 に関する情報と、IKEv1 からの移行プロセスについて説明します。

前提条件

要件

IKEv1 事前共有キー（PSK）認証方式を使用して IPsec を実行する Cisco ASA セキュリティ アプライアンスがあり、IPsec トンネルが作動可能状態になっていることを確認してください。

IKEv1 PSK 認証方式を使用して IPsec を実行する Cisco ASA セキュリティ アプライアンスの設定例については、『PIX/ASA 7.x 以降：PIX-to-PIX VPN トンネルの設定例』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- バージョン 8.4.x 以降で実行される Cisco ASA 5510 シリーズ セキュリティ アプライアンス。

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。

表記法

ドキュメントの表記法の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

IKEv2 に移行する理由

- IKEv2 では、ネットワーク攻撃に対する復元性が向上しています。IKEv2 は、IPsec 発信側の検証時にネットワークでの DoS 攻撃を軽減できます。DoS 脆弱性の悪用を困難にするために、応答側は、これが通常の接続であることを応答側に保証する必要がある発信側に Cookie を求めることができます。IKEv2 では、応答側の Cookie により DoS 攻撃が軽減されるため、発信側が応答側によって送信された Cookie を返さない限り、応答側は IKE 発信側の状態を維持しないか、D-H 操作を実行しません。応答側は、最小限の CPU を使用し、発信側を完全に検証できるまで状態をセキュリティ アソシエーション（SA）にコミットしません。
- IKEv2 は、さまざまな VPN 製品間での IPsec 確立の複雑さを軽減します。相互運用性を向上させ、さらに従来の認証方式に標準の方法を使用できます。IKEv2 は、デッド ピア検知（DPD）、NAT トラバーサル（NAT-T）、または Initial Contact などの組み込みテクノロジーを提供するため、ベンダー間のシームレスな IPsec の相互運用性を実現します。
- IKEv2 ではオーバーヘッドが少なくなっています。オーバーヘッドの減少によって、SA 設定の遅延が改善します。中継では複数の要求が許可されます（複数の子 SA を並行して設定する場合など）。
- IKEv2 では SA の遅延が短縮されています。IKEv1 では、パケット ボリュームが増幅すると、SA 作成の遅延は増幅します。IKEv2 は、パケット ボリュームが増幅しても同じ平均遅延を維持します。パケット ボリュームが増幅すると、パケット ヘッダーを暗号化して処理する時間も増えます。新しい SA 確立を作成する場合、より長い時間が必要です。IKEv2によって生成されるSAは、IKEv1によって生成されるSAよりも小さくなります。増幅されたパケットサイズでは、SAの作成に要する時間はほぼ一定です。
- IKEv2 ではキー再生成時間が短縮されています。IKEv1では、IKEv2よりもSAのキー再生成に時間がかかります。SAのIKEv2キー再生成では、セキュリティパフォーマンスが向上し、移行中に失われるパケットの数が減少します。IKEv1の特定のメカニズム（ToSペイロード、SAライフタイムの選択、SPIの一意性など）のIKEv2での再定義により、IKEv2で失われるパケットと複製されるパケットが減少します。そのため、SAのキー再生成は不要です。

注：ネットワークセキュリティは最も弱いリンクと同じ強度しか持つことができないため、IKEv2はIKEv1と相互運用できません。

移行の概要

IKEv1 または場合によっては SSL の設定がすでに存在する場合、ASA では移行プロセスが簡単になります。コマンド ラインで、**migrate** コマンドを入力します。

```
migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
```
注意する点：

- キーワード定義：**l2l**：これによって、現在の IKEv1 l2l トンネルが IKEv2 に変換されます。**remote access：これによって、リモート アクセス設定が変換されます。**IKEv1 または SSL のいずれかのトンネル グループを IKEv2 に変換できます。**overwrite**：上書きする IKEv2 の設定がある場合、このキーワードによって、現在の IKEv1 の設定が変換され、不要な IKEv2 の設定は削除されます。
- IKEv2 では、対称キーと非対称キーの両方を PSK 認証に使用できることに留意することが重要です。**migration** コマンドを ASA で入力すると、ASA は、自動的に対称 PSK で IKEv2 VPN を作成します。
- コマンドの入力後に現在の IKEv1 の設定は削除されません。代わりに、IKEv1 と IKEv2 の両方の設定が並行して同じクリプト マップで実行されます。これは、手動で行うこともできます。IKEv1 と IKEv2 の両方を並行して実行する場合、接続の試行が失敗する可能性がある IKEv2 のプロトコルまたは設定の問題が存在すると、これによって IPsec VPN の発信側が IKEv2 から IKEv1 にフォールバックします。IKEv1 と IKEv2 の両方を並行して実行する場合、ロールバック メカニズムも提供され、移行が簡単になります。
- IKEv1 と IKEv2 の両方を並行して実行する場合、ASA は、発信側で共通のトンネル マネージャまたは IKE というモジュールを使用して、接続に使用するクリプト マップと IKE プロトコル バージョンを決定します。ASA では常に IKEv2 の開始が優先されますが、これが可能ではない場合は IKEv1 にフォールバックします。
- 冗長性に使用される複数のピアは ASA 上の IKEv2 ではサポートされません。IKEv1 では、冗長性のために、**set peer** コマンドを入力すると、同じクリプト マップで複数のピアを持つことができます。最初のピアがプライマリになり、障害が発生した場合は 2 番目のピアが動作します。Cisco Bug ID CSCud22276（登録ユーザ専用）、『ENH：IKEv2 での複数ピアのサポート』を参照してください。

移行プロセス

コンフィギュレーション

この例では、事前共有キー（PSK）認証を使用する IKEv1 VPN が ASA 上に存在します。

注：ここで示す設定は、VPNトンネルにのみ関連しています。

現在の IKEv1 VPN（移行前）を使用した ASA の設定

```
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
```

```
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3
```

ASA IKEv2 の設定（移行後）

注：太字の斜体でマークされた変更。

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac

crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp integrity sha-
1
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset

crypto map vpn 12 set IKEv2 ipsec-proposal goset
crypto map vpn interface outside
crypto isakmp disconnect-notify

crypto IKEv2 policy 1 encryption 3des integrity sha group 5 prf sha lifetime seconds 86400
crypto IKEv2 enable outside
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3

IKEv2 remote-authentication pre-shared-key ***** IKEv2 local-authentication pre-shared-key *****
```

IKEv2 トンネルの確立の確認

```
ASA1# sh cry IKEv2 sa detail

IKEv2 SAs:
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id   Local                Remote     Status        Role
102061223 192.168.1.1/500  192.168.2.2/500  READY    INITIATOR
     Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
     Life/Active Time: 86400/100 sec
     Status Description: Negotiation done
     Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
     Local id: 192.168.1.1
     Remote id: 192.168.2.2
      DPD configured for 10 seconds, retry 3
     NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
         remote selector 10.20.20.0/0 - 10.20.20.255/65535
         ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
interface: outside
   Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
     access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
     10.20.20.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
     current_peer: 192.168.2.2
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

移行後の PSK の確認

PSK を確認するには、グローバル コンフィギュレーション モードで次のコマンドを実行できます。

```
more system: running-config | beg tunnel-group
```

IKEv2 とトンネル マネージャ プロセス

前述したとおり、ASA は、発信側で共通のトンネル マネージャまたは IKE というモジュールを使用して、接続に使用するクリプト マップと IKE プロトコル バージョンを決定します。モジュールをモニタするには、次のコマンドを入力します。

```
debug crypto ike-common <level>
```

IKEv2 トンネルを開始するためにトラフィックが渡されたときに、debug、logging、show コマンドが収集されました。明確にするために、一部の出力は省略されています。

```
ASA1(config)# logging enable
ASA1(config)# logging list IKEv2 message 750000-752999
ASA1(config)# logging console IKEv2
ASA1(config)# exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5

%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown
Received request to establish an IPsec tunnel; local traffic selector = Address Range:
10.10.10.11-10.10.10.11 Protocol: 0
Port Range: 0-65535; remote traffic selector = Address Range:
10.20.20.21-10.20.20.21 Protocol: 0 Port Range: 0-65535
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
```

```
message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12.
IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
    26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA UP. Reason: New Connection Established
43%ASA-5-752016: IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
IKEv2-PROTO-3: (12): Insert SA
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
IKEv2-PLAT-3:
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
IKEv2-PROTO-3: (12): Checking for duplicate SA
Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry.
Map Tag = vpn.  Map Sequence Number = 12.
```

IKEv2 から IKEv1 へのフォールバック メカニズム

IKEv1とIKEv2の両方が並行している場合、ASAは常にIKEv2を開始することを優先します。ASAが開始できない場合は、IKEv1にフォールバックします。Tunnel manager/IKE共通モジュールがこのプロセスを管理します。発信側でのこの例では、フォールバック メカニズムを示すために、IKEv2 SA がクリアされ、IKEv2 が故意に誤って設定されています (IKEv2 の提案は削除されます) 。

```
ASA1# clear  crypto  IKEv2 sa

%ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-4-752010: IKEv2 Doesn't have a proposal specified
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
%ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn.
```

```
Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 sa
IKEv1 SAs:
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1   IKE Peer: 192.168.2.2
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE
```

IKEv2 の強化

IKEv2 の使用時に追加のセキュリティを提供するために、次のオプション コマンドを使用することを強くお勧めします。

- **Crypto IKEv2 cookie-challenge**：ASA は、ハーフオープン SA が開始したパケットへの応答で Cookie チャレンジをピア デバイスに送信できます。
- **Crypto IKEv2 limit max-sa**：ASA での IKEv2 接続の数を制限します。デフォルトでは、許可される最大の IKEv2 接続は、ASA ライセンスで指定された接続の最大数と等しくなっています。
- **Crypto IKEv2 limit max-in-negotiation-sa**：ASA で IKEv2 のネゴシエーション中の（オープンな）SA の数を制限します。**crypto IKEv2 cookie-challenge** コマンドとともに使用する場合は、cookie-challenge しきい値がこの制限より低くなるようにしてください。
- 非対称キーを使用します。移行後に、非対称キーを使用するよう設定を変更できます（以下参照）。

```
ASA-2(config)# more system:running-config
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key cisco1234
 IKEv2 remote-authentication pre-shared-key cisco1234
 IKEv2 local-authentication pre-shared-key cisco123
```

IKEv2 事前共有キーの他のピアに設定をミラーリングする必要があることを十分に理解することが重要です。設定を選択して、ある側から他の側に貼り付けても機能しません。

注：これらのコマンドはデフォルトで無効になっています。

関連情報

- テクニカル サポートとドキュメント