次世代の暗号化を使用した FlexVPN の設定例

目次

[概要](#)
[次世代の暗号化](#)
[スイート Suite-B-GCM-128](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[認証機関](#)
[設定](#)
[ネットワーク トポロジ](#)
[ルータが楕円曲線デジタル署名アルゴリズムを使用できるようにするための手順](#)
[設定](#)
[接続の確認](#)
[トラブルシューティング](#)
[結論](#)

概要

このドキュメントでは、アルゴリズムの Cisco 次世代の暗号化（NGE）セットをサポートする 2 つのルータの間の FlexVPN を設定する方法について説明します。

次世代の暗号化

Cisco NGE 暗号化は、安定した 4 つの設定可能なパブリック ドメイン暗号化アルゴリズムを使用するネットワークを移動する情報を保護します。

- 128 ビットまたは 256 ビット キーを使用した Advanced Encryption Standard（AES）に基づく暗号化
- 256 ビットおよび 384 ビットプライムモジュールの曲線を使用する楕円曲線デジタル署名アルゴリズム（ECDSA）を備えたデジタル署名
- 楕円曲線 Diffie-Hellman（ECDH）メソッドを使用するキー交換
- セキュア ハッシュ アルゴリズム（SHA-2）に基づくハッシュ（デジタル フィンガープリント）

国家安全保障局（NSA）は、これら 4 つのアルゴリズムを組み合わせることで、分類された情報の十分な情報の保証が得られると述べています。 IPsec の NSA Suite B 暗号化は、RFC 6379 の標準規格として公開され、業界で受け入れられています。

スイート Suite-B-GCM-128

RFC 6379 では、これらのアルゴリズムは、スイート Suite-B-GCM-128 で必要です。

このスイートは、128 ビット AES-GCM によって Encapsulating Security Payload（ESP）整合性の保護と信頼性を提供します（ RFC4106を参照）。 ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。

ESP
暗号化　Galois/Counter Mode（GCM）での 128 ビット キーおよび 16 オクテット整合性チェック値（ICV）を使用した AES（RFC4106）
整合性　NULL

IKEv2
暗号化　暗号ブロック連鎖（CBC）モードでの 128 ビット キーを使用した AES（RFC3602）
擬似乱数関数　HMAC-SHA-256（RFC4868）
整合性　HMAC-SHA-256-128（RFC4868）
Diffie-Hellman グループ　256 ビット ランダム ECP グループ（RFC5903）

Suite B および NGE の詳細は、『次世代暗号化』を参照してください。

前提条件

要件

次の項目に関する知識が推奨されます。

- FlexVPN
- インターネット キー交換バージョン 2（IKEv2）
- IPSec

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くものです。

- ハードウェア： セキュリティ ライセンスを実行するサービス統合型ルータ（ISR）世代 2（G2）
- ソフトウェア： Cisco IOS® ソフトウェア リリース 15.2.3T2。 GCM が導入された、Cisco IOS ソフトウェア リリース M または 15.1.2T 以降のリリースを使用できます。

詳細については、Feature Navigator を参照してください。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

認証局

現在、Cisco IOS ソフトウェアは、Suite B で必要な ECDH を実行するローカル認証機関（CA）サーバをサポートしていません。 サード パーティ CA サーバを実装する必要があります。 この例では、Suite B PKI に基づく Microsoft CA を使用します。

設定

ネットワーク トポロジ

このガイドは、次の図に示すこのトポロジに基づいています。 要件に合わせて IP アドレスを変更する必要があります。

注：

セットアップは、直接接続された 2 つのルータで構成されており、複数のホップで区切られている可能性があります。 その場合、ピア IP アドレスへのルートが必要です。 この設定では、使用されている暗号化の詳細のみが含まれています。 IKEv2 ルーティングまたはルーティング プロトコルを IPSec VPN で実装する必要があります。

ルータが楕円曲線デジタル署名アルゴリズムを使用できるようにするための手順

1. EC キーペアを作成するために必要なドメイン名とホスト名を作成します。

```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label Router1.cisco.com
```

注: Cisco Bug ID CSCue59994 のフィックスでバージョンを実行しない場合、ルータで 768 より小さいキー サイズで証明書を登録できません。

2. CA から証明書を取得するために、ローカル トラストポイントを作成します。

```
crypto pki trustpoint ecdh
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

注: CA がオフラインだったため、失効の確認が無効になりました。 実稼働環境で最大限のセキュリティを確保するために失効の確認を有効にする必要があります。

3. トラストポイントを認証します（これにより公開キーを含む CA の証明書のコピーを取得できます）。

```
crypto pki authenticate ecdh
```

4. プロンプトで CA の Base64 エンコード証明書を入力します。 **quit** と入力してから、**yes** と

入力して承認します。

5. ルータを CA の PKI に登録します。

```
crypto pki enrol ecdh
```

6. 表示される出力は、証明書要求を CA に送信するために使用されます。 Microsoft CA の場合、CA の Web インターフェイスに接続し、[Submit a certificate request] を選択します。

7. CA から受信した証明書をルータにインポートします。 証明書をインポートした後、**quit** と入力します。

```
crypto pki import ecdh certificate
```

設定

ここでは、Router1 の設定が提供されています。 Router2 には、トンネル インターフェイスの IP アドレスのみが固有である構成のミラーが必要です。

1. ピア デバイスの証明書と一致する証明書マップを作成します。

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. Suite B の IKEv2 プロポーザルを設定します。

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

注: IKEv2 スマートのデフォルトは、デフォルトの IKEv2 プロポーザル内に事前設定されたいくつかのアルゴリズムを実装します。 aes-cbc-128 および sha256 はスイート Suite-B-GCM-128 で必要であるため、これらのアルゴリズム内の aes-cbc-256、sha384、および sha512 を削除する必要があります。 これは、選択肢が提示されるときに IKEv2 は最も強力なアルゴリズムを選択するからです。 最大限のセキュリティを確保するために、aes-cbc-256 と sha512 を使用します。 しかし、これは Suite-B-GCM-128 では必要ありません。 設定された IKEv2 プロポーザルを表示するには、**show crypto ikev2 proposal** コマンドを入力します。

3. 証明書マップと一致し、以前に定義したトラストポイントで ECDSA を使用するよう IKEv2 プロファイルを設定します。

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
```

```
 pki trustpoint ecdh
```

4. GCM を使用するよう IPSec トランスフォームを設定します。

```
crypto ipsec transform-set ESP_GCM esp-gcm
 mode transport
```

5. 事前に設定したパラメータで IPSec プロファイルを設定します。

```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

6. トンネル インターフェイスを設定します。

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

接続の確認

このセクションでは、設定が正常に機能していることを確認します。

1. ECDSA キーが正常に生成されていることを確認します。

```
Router1#show crypto key mypubkey ec
% Key pair was generated at: 04:05:07 JST Jul 6 2012
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
 30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E
(...omitted...)
```

2. 証明書が正常にインポートされ、ECDH が使用されていることを確認します。

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. IKEv2 SA が正常に作成され、Suite B アルゴリズムを使用していることを確認します。

```
Router1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
     Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify:
ECDSA
     Life/Active Time: 86400/20 sec
```

4. IKEv2 SA が正常に作成され、Suite B アルゴリズムを使用していることを確認します。

```
Router1#show crypto ipsec sa

interface: Tunnel0
   Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xAC5845E1(2891466209)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xAEF7FD9C(2935487900)
       transform: esp-gcm ,
       in use settings ={Transport, }
       conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4341883/3471)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
```

注: インターネット キー エクスチェンジ バージョン 1（IKEv1）の場合と異なり、この出力では、最初のトンネル ネゴシエーション時に Perfect Forwarding Secrecy（PFS）の Diffie-Hellman（DH）グループ値が **PFS (Y/N): N, DH group: none** と表示されますが、キー再作成が行われた後は正しい値が表示されます。 これは、動作が Cisco Bug ID CSCug67056 で説明されていますが、バグではありません。 IKEv1 と IKEv2 の違いは、後者では子の Security Associations（SA）が AUTH 交換の一部として作成される点です。 暗号マップに設定された DH グループは、キー再生成時にのみ使用されます。 したがって、最初のキー再生成が行われるまで **PFS (Y/N): N, DH group: none** が表示されます。 しかし、IKEv1 では、クイック モード時に子 SA が作成され、CREATE_CHILD_SA メッセージにキー交換ペイロードを伝送するためのプロビジョニングがあり、これによって新しい共有秘密を取得する DH パラメータが指定されるため、動作が異なります。

トラブルシューティング

現在のところ、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。

結論

NGE で定義された効率的で強力な暗号化アルゴリズムは、そのデータの機密性と整合性が確保され、データの処理が低コストで行われることを長期的に保証します。 NGE は FlexVPN で簡単に実装できます。これは Suite B の標準の暗号化を提供します。

Cisco の Suite B の実装の詳細は、『次世代暗号化』を参照してください。