次世代暗号化によるルータと ASA 間の FlexVPN の設定例

内容

概要

このドキュメントでは、FlexVPN を使用したルータと Cisco Next Generation Encryption（NGE）アルゴリズムをサポートする適応型セキュリティ アプライアンス（ASA）間で VPN を設定する方法について説明します。

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。

- FlexVPN
- インターネット キー交換バージョン 2（IKEv2）
- IPSec
- ASA
- 次世代暗号化

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。

- **Hardware:**セキュリティ ライセンスを実行する IOS Generation 2（G2）ルータ。
- **ソフトウェア**：Cisco IOS®ソフトウェアリリースバージョン15.2-3.T2。Cisco IOS®ソフトウェアリリースバージョン15.1.2T以降のリリースでは、MまたはTのすべてのリリースを使用できます。これは、Galois Counter Mode(GCM)の導入に含まれています。
- **Hardware:**NGE をサポートする ASA。**注：マルチコア**・プラットフォームのみが高度暗号化規格(AES)GCMをサポートしています。
- **ソフトウェア**：NGE をサポートする ASA ソフトウェア リリース 9.0 以降。
- OpenSSL。

詳細については、「Cisco Feature Navigator」を参照してください。

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

ドキュメント表記の詳細は、『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。

IPSec セキュリティ アソシエーションの動的な作成

IOS での推奨 IPSec インターフェイスは、IPsec により保護される総称ルーティング カプセル化（GRE）インターフェイスを作成する、仮想トンネル インターフェイス（VTI）です。VTI では、トラフィック セレクタ（IPSec セキュリティ アソシエーション（SA）により保護されるトラフィック）は、トンネルの発信元から送信先への GRE トラフィックで構成されます。ASA は GRE インターフェイスを実装せず、アクセス コントロール リスト（ACL）で定義されるトラフィックに基づいて IPSec SA を作成するので、ルータが推奨トラフィック セレクタのミラーを使用して IKEv2 開始に応答できる方式をイネーブルにする必要があります。FlexVPN ルータで Dynamic Virtual Tunnel Interface（DVTI）を使用すると、デバイスは、提供されたトラフィック セレクタにそのミラーを使用して応答できます。

この例では、両方の内部ネットワーク間でトラフィックを暗号化します。ASA が ASA 内部ネットワークのトラフィック セレクタ（192.168.1.0/24 から 172.16.10.0/24）を IOS 内部ネットワークに提供する場合、DVTI インターフェイスは、トラフィック セレクタのミラー（172.16.10.0/24 から 192.168.1.0/24）を使用して応答します。

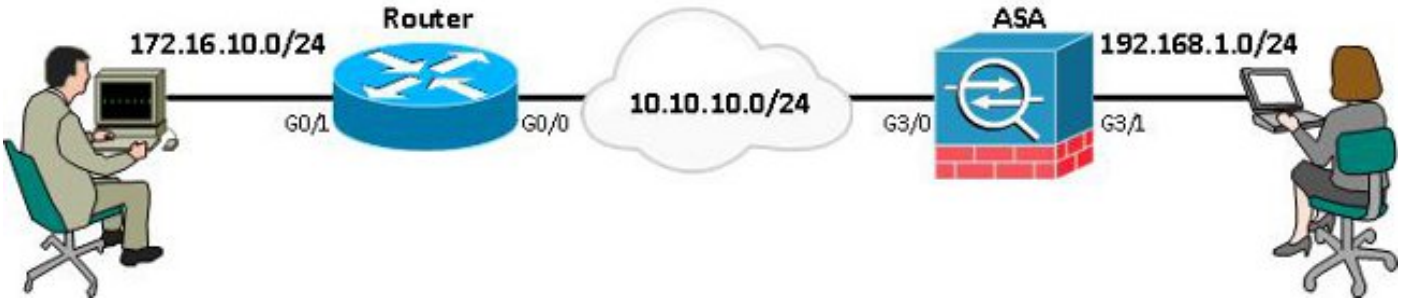
認証局

現在、IOS および ASA は、Suite-B で必要な楕円曲線デジタル署名アルゴリズム（ECDSA）を使用するローカル認証局（CA）サーバをサポートしません。そのため、サードパーティ CA サーバを実装する必要があります。たとえば、CA として機能する OpenSSL を使用します。

コンフィギュレーション

Network Topology

このガイドは、次の図に示すトポロジに基づいています。そのため、必要に応じて IP アドレスを修正する必要があります。



注：設定には、ルータとASAの直接接続が含まれています。これらは、多くのホップで分割できます。その場合、ピア IP アドレスへのルートが必要です。次の設定では、使用されている暗号化について詳しく説明します。

ルータが ECDSA を使用できるようにするための手順

認証局

1. **elliptic curve keypair を作成します。**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. **elliptic curve self-signed certificate** を作成します。
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. 楕円曲線（EC）キーペアを作成するために必要な **domain-name** および **hostname** を作成します。
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
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 ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   注：CAがオフラインであるため、失効確認は無効です。実稼働環境ではセキュリティを最大にするために失効確認をイネーブル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します。
   ```
   crypto pki authenticate ec_ca
   ```
4. 次に base 64 エンコードされた CA の証明書を入力するように指示されます。これは OpenSSL で作成済みの ca.pem ファイルです。このファイルを表示するには、エディタで開くか、OpenSSL コマンド **openssl x509 -in ca.pem** を使用します。ペーストするときに **quit** を入力します。次に、**yes** を入力して適用します。
5. ルータを CA の公開キー インフラストラクチャ（PKI）に登録します。
   ```
   crypto pki enrol ec_ca
   ```
6. 出力は、証明書要求を CA に送信するときに使用する必要があります。これは、テキスト ファイル（flex.csr）として保存し、OpenSSL コマンドを使用して署名できます。

```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```

7. 次のコマンドの入力後、CA により生成されるファイル flex.pem 内に含まれる証明書をルータにインポートします。完了したら、**quit** を入力します。

```
crypto pki import ec_ca certificate
```

ASA

1. EC キー ペアを作成するために必要な **domain-name** および **hostname** を作成します。

```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```

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 ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```

注：CAがオフラインであるため、失効確認は無効です。実稼働環境ではセキュリティを最大にするために失効確認をイネーブル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します。

```
crypto ca authenticate ec_ca
```

4. 次に base 64 エンコードされた CA の証明書を入力するように指示されます。これは OpenSSL で作成済みの ca.pem ファイルです。このファイルを表示するには、エディタで開くか、OpenSSL コマンド **openssl x509 -in ca.pem** を使用します。このファイルをペーストしたら **quit** を入力し、**yes** を入力して適用します。
5. ASA を CA の PKI に登録します。

```
crypto ca enrol ec_ca
```

6. 出力は、証明書要求を CA に送信するときに使用する必要があります。これは、テキスト ファイル (asa.csr) として保存し、OpenSSL コマンドを使用して署名できます。

```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
```

7. 次のコマンドの入力後、CA により生成されるファイル a.pem 内に含まれる証明書をルータにインポートします。完了したら、**quit** を入力します。

```
crypto ca import ec_ca certificate
```

コンフィギュレーション

FlexVPN

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
```

Suite-B 設定で IKEv2 プロポーザルに次のコマンドを入力します。

注：セキュリティを最大限に高めるには、**aes-cbc-256 with sha512 hashコマンドを使用して設定**します。

```
crypto ikev2 proposal default
 encryption aes-cbc-128
```

```
 integrity sha256
 group 19
```

IKEv2 プロファイルと証明書マップをマッチングし、事前に定義した**トラストポイント**で ECDSA を使用します。

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ec_ca
 virtual-template 1
```

IPSec トランスフォーム セットを設定し、Galois Counter Mode（GCM）を使用します。

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

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
```

トンネル インターフェイスを設定します。

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

次に、インターフェイス設定を示します。

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
```

ASA

次のインターフェイス設定を使用します。

```
interface GigabitEthernet3/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet3/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

次のアクセス リスト コマンドを入力して、暗号化するトラフィックを定義します。

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```

NGE で次の IPSec プロポーザル コマンドを入力します。

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```

暗号化マップ コマンド：

```
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 10.10.10.1
crypto map mymap 10 set ikev2 ipsec-proposal prop1
crypto map mymap 10 set trustpoint ec_ca
crypto map mymap interface outside
```

このコマンドは、NGE で IKEv2 ポリシーを設定します。

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

ピア コマンドに設定されるトンネル グループ：

```
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 peer-id-validate cert
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate ec_ca
```

接続の確認

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 router1.cisco.com
% Key pair was generated at: 21:28:26 UTC Feb 19 2013
Key name: router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
<...omitted...>

ASA-1(config)#show crypto key mypubkey ecdsa
Key pair was generated at: 21:11:24 UTC Feb 19 2013
Key name: asa1.cisco.com
 Usage: General Purpose Key
 EC Size (bits): 256
 Key Data&colon;
<...omitted...>
```

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

```
Router1#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0137
  Certificate Usage: General Purpose
  Issuer:
<...omitted...>
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    EC Public Key:  (256 bit)
  Signature Algorithm: SHA256 with ECDSA


ASA-1(config)#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 00a293f1fe4bd49189
  Certificate Usage: General Purpose
  Public Key Type: ECDSA (256 bits)
  Signature Algorithm: SHA256 with ECDSA Encryption
 <...omitted...>
```

IKEv2 SA が正常に作成され、設定された NGE アルゴリズムが使用されていることを確認します。

```
Router1#show crypto ikev2 sa  detailed
 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: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      Life/Active Time: 86400/94 sec


ASA-1#show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status         Role
268364957        10.10.10.2/500        10.10.10.1/500      READY    INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      <...omitted...>
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xe847d8/0x12bce4d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec SA が正常に作成され、設定された NGE アルゴリズムが使用されていることを確認します。

注：FlexVPNは、IKEv2プロトコルとIPSecプロトコルの両方をサポートする非IOSクライアントからのIPSec接続を終了できます。

```
Router1#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
<...omitted...>

     inbound esp sas:
      spi: 0x12BCE4D(19648077)
        transform: esp-gcm ,
        in use settings ={Tunnel, }

ASA-1#show crypto ipsec sa detail
interface: outside
    Crypto map tag: mymap, seq num: 10, local addr: 10.10.10.2

      access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0
        255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
      current_peer: 10.10.10.1
<...omitted...>


    inbound esp sas:
      spi: 0x00E847D8 (15222744)
         transform: esp-aes-gcm esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
```

Cisco の Suite-B の実装の詳細については、『次世代暗号化に関するホワイト ペーパー』を参照してください。

Cisco の次世代暗号化の実装の詳細については、『次世代暗号化に関するソリューション ページ』を参照してください。

関連情報

- 次世代暗号化に関するホワイト ペーパー
- 次世代暗号化に関するソリューション ページ
- セキュア シェル (SSH)
- IPSec ネゴシエーション/IKE プロトコル
- PSK によるサイト間 VPN の ASA IKEv2 デバッグ テクニカルノート
- ASA IPsec および IKE のデバッグ (IKEv1 メイン モード) のトラブルシューティング テクニカル ノート
- IOS IPSec および IKE のデバッグ (IKEv1 メイン モード) のトラブルシューティング テクニカルノート
- ASA IPSec および IKE デバッグ：IKEv1 アグレッシブ モード テクニカルノート
- テクニカル サポートとドキュメント – Cisco Systems