FlexVPN with Next−Generation Encryption Configuration Example

Document ID: 115730

Contributed by Graham Bartlett and Atri Basu, Cisco TAC Engineers.
Jan 08, 2015

Contents

Introduction

This document describes how to configure a FlexVPN between two routers that support the Cisco Next−Generation Encryption (NGE) set of algorithms.

Next−Generation Encryption

Cisco NGE cryptography secures information that travels over networks that use four configurable, well−established, and public−domain cryptographic algorithms:

- Encryption based on the Advanced Encryption Standard (AES), which uses 128−bit or 256−bit keys
- Digital signatures with the Elliptic Curve Digital Signature Algorithm (ECDSA) that use curves with 256−bit and 384−bit prime moduli
- Key exchange that uses the Elliptic Curve Diffie−Hellman (ECDH) method
- Hashing (digital fingerprints) based on the Secure Hash Algorithm 2 (SHA−2)

The National Security Agency (NSA) states that these four algorithms in combination provide adequate information assurance for classified information. NSA Suite B cryptography for IPsec has been published as a standard in RFC 6379 and has gained acceptance in the industry.

Suite Suite−B−GCM−128

As per RFC 6379, these algorithms are required for suite Suite−B−GCM−128.

This suite provides Encapsulating Security Payload (ESP) integrity protection and confidentiality with 128−bit AES−GCM (see RFC4106). This suite should be used when ESP integrity protection and encryption

are both needed.

ESP
Encryption AES with 128−bit keys and 16−octet Integrity Check Value (ICV) in Galois/Counter Mode (GCM) (RFC4106)
Integrity NULL

IKEv2
Encryption AES with 128−bit keys in Cipher Block Chaining (CBC) mode (RFC3602)
Pseudo−random function HMAC−SHA−256 (RFC4868)
Integrity HMAC−SHA−256−128 (RFC4868)
Diffie−Hellman group 256−bit random ECP group (RFC5903)

More information on Suite B and NGE can be found at Next−Generation Encryption.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FlexVPN
- Internet Key Exchange version 2 (IKEv2)
- IPsec

Components Used

The information in this document is based on these software and hardware versions:

- Hardware: Integrated Services Routers (ISR) Generation 2 (G2) that run the security license.
- Software: Cisco IOS® Software Release 15.2.3T2. Any release of Cisco IOS Software Release M or 15.1.2T or later can be used since this is when GCM was introduced.

For details, refer to the Feature Navigator.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

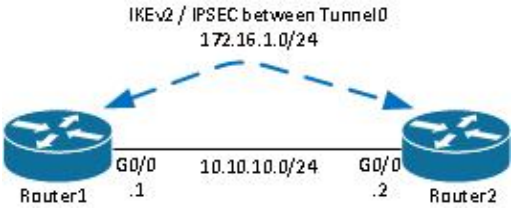
Certificate Authority

Currently, Cisco IOS software does not support a local Certificate Authority (CA) server that runs ECDH, which is required for Suite B. A third party CA server must be implemented. This example uses a Microsoft CA based on Suite B PKI

Configure

Network Topology

This guide is based on this illustrated topology. IP addresses should be amended to suit your requirements.



Notes:

The setup consists of two routers directly connected, which might be separated by many hops. If so, ensure that there is a route to get to the peer IP address. This configuration only details the encryption used. IKEv2 routing or a routing protocol should be implemented over the IPSec VPN.

Steps Required to Enable the Router to use the Elliptic Curve Digital Signature Algorithm

1. Create the domain name and hostname, which are prerequisites to create an EC keypair.

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

   Note: Unless you run a version with the fix for Cisco bug ID CSCue59994, the router will not allow you to enroll a certificate with a keysize less than 768.
2. Create a local trustpoint in order to gain a certificate from the CA.

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

   Note: Since the CA was offline, revocation checks were disabled. Revocation checks should be enabled for maximum security in a production environment.

3. Authenticate the trustpoint (this obtains a copy of the CA's certificate that contains the public key).

   ```
   crypto pki authenticate ecdh
   ```

4. Enter the base 64 encoded certificate of the CA at the prompt. Enter ***quit*** and then enter ***yes*** to accept.

5. Enroll the router into the PKI on the CA.

   ```
   crypto pki enrol ecdh
   ```

6. The output displayed is used in order to submit a certificate request to the CA. For the Microsoft CA, connect to the web interface of the CA and select ***Submit a certificate request***.

7. Import the certificate received from the CA into the router. Enter ***quit*** once the certificate is imported.

```
crypto pki import ecdh certificate
```

Configuration

The configuration provided here is for Router1. Router2 requires a mirror of the configuration where only the IP addresses on the tunnel interface are unique.

1. Create a certificate map to match the certificate of the peer device.

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

2. Configure the IKEv2 proposal for Suite B.

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

Note: IKEv2 Smart Defaults implements a number of preconfigured algorithms within the default IKEv2 proposal. Since aes−cbc−128 and sha256 are required for suite Suite−B−GCM−128, you must remove aes−cbc−256, sha384, and sha512 within these algorithms. The reason for this is that IKEv2 chooses the strongest algorithm when presented with a choice. For maximum security, use aes−cbc−256 and sha512. However, this is not required for Suite−B−GCM−128. In order to view the configured IKEv2 proposal, enter the ***show crypto ikev2 proposal*** command.

3. Configure the IKEv2 profile to match the certificate map and use ECDSA with the trustpoint defined earlier.

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

4. Configure the IPSec transform to use GCM.

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

5. Configure the IPSec profile with the parameters configured earlier.

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

6. Configure the tunnel interface.

```
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
```

Verify Connection

Use this section in order to confirm that your configuration works properly.

1. Verify that the ECDSA keys were successfully generated.

```
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. Verify that the certificate was successfully imported and that ECDH is used.

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

3. Verify that the IKEv2 SA was successfully created and uses the Suite B algorithms.

```
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. Verify that the IKEv2 SA was successfully created and uses the Suite B algorithms.

```
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)
```

Note: In this output, unlike in Internet Key Exchange version 1 (IKEv1), the perfect forward secrecy (PFS) Diffie−Hellman (DH) group value shows as ***PFS (Y/N): N, DH group: none*** during the first tunnel negotiation, but after a rekey occurs, the right values show. This is not a bug even though the behavior is described in Cisco bug ID CSCug67056. The difference between IKEv1 and IKEv2 is that, in the latter, the Child Security Associations (SAs) are created as part of the AUTH exchange itself. The DH Group configured under the crypto map is used only during the rekey. Hence, you see ***PFS (Y/N): N, DH group: none*** until the first rekey. But with IKEv1, you see a different behavior because the Child SA creation happens during Quick Mode and the CREATE_CHILD_SA message has a provision for carrying the Key Exchange payload that specifies the DH parameters to derive a new shared secret.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Conclusion

The efficient and strong cryptographic algorithms defined in NGE provide long−term assurance that data confidentially and integrity is provided and maintained at a low cost to process. NGE can easily be implemented with FlexVPN, which provides Suite B standard cryptography.

Further information on Cisco's implementation of Suite B can be found at Next−Generation Encryption.

Updated: Jan 08, 2015 Document ID: 115730