FlexVPN Between a Router and an ASA with Next Generation Encryption Configuration Example

Document ID: 116008

Contributed by Graham Bartlett, Cisco TAC Engineer.
Mar 26, 2013

Contents

Introduction

This document describes how to configure a VPN between a router with FlexVPN and an Adaptive Security Appliance (ASA) that supports the Cisco Next Generation Encryption (NGE) algorithms.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FlexVPN
- Internet Key Exchange version 2 (IKEv2)
- IPSec
- ASA
- Next Generation Cryptography

Components Used

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

- **Hardware:** IOS Generation 2 (G2) Router that runs the security license.
- **Software:** Cisco IOS® Software Release Version 15.2−3.T2. Any release of M or T for releases later than Cisco IOS® Software Release Version 15.1.2T can be used because this is included with the

introduction of Galois Counter Mode (GCM).
- **Hardware:** ASA that supports NGE.

  Note: Only multi−core platforms support Advanced Encryption Standard (AES) GCM.
- **Software:** ASA Software Release 9.0 or later that supports NGE.
- OpenSSL.

For details, refer to Cisco 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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Dynamically Create IPSec Security Associations

The recommended IPSec interface on IOS is a Virtual Tunnel Interface (VTI), which creates a generic routing encapsulation (GRE) interface that is protected by IPsec. For a VTI, the Traffic Selector (what traffic should be protected by the IPSec security associations (SA)), consists of GRE traffic from the tunnel source to the tunnel destination. Because the ASA does not implement GRE interfaces, but instead creates IPSec SAs based on traffic defined in an access control list (ACL), we must enable a method that allows the router to respond to the IKEv2 initiation with a mirror of the proposed traffic selectors. The use of Dynamic Virtual Tunnel Interface (DVTI) on the FlexVPN router allows this device to respond to the presented Traffic Selector with a mirror of the Traffic Selector that was presented.

This example encrypts traffic between both internal networks. When the ASA presents the traffic selectors of the ASA internal network to the IOS internal network, `192.168.1.0/24` to `172.16.10.0/24`, the DVTI interface responds with a mirror of the traffic selectors, which is `172.16.10.0/24` to `192.168.1.0/24`.

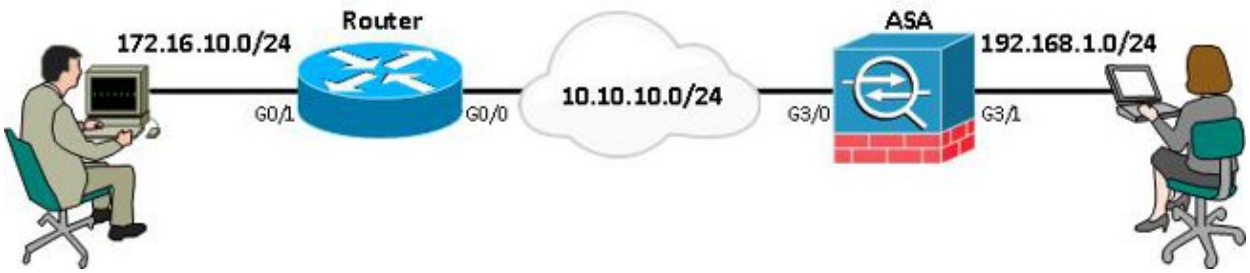
Certificate Authority

Currently, IOS and ASA do not support a local Certificate Authority (CA) server with Elliptic Curve Digital Signature Algorithm (ECDSA) certificates, which is required for Suite−B. So a third−party CA Server must be implemented. For example, use OpenSSL to act as a CA.

Configuration

Network Topology

This guide is based on the topology shown in this diagram. You should amend IP addresses to suit.



Note: The setup includes a direct connection of the router and ASA. These could be separated by many hops. If so make sure that there is a route to get to the peer IP address. The following configuration only details the encryption used.

Steps Required to Enable the Router to use the ECDSA

Certificate Authority

1. Create an **elliptic curve keypair.**

```
openssl ecparam −out ca.key −name secp256r1 −genkey
```

2. Create an **elliptic curve self−signed certificate**.

```
openssl req −x509 −new −key ca.key −out ca.pem −outform PEM −days 3650
```

FlexVPN

1. Create **domain−name** and **hostname**, which are prerequisites in order to create an elliptic curve (EC) keypair.

```
ip domain−name cisco.com
hostname Router1
crypto key generate ec keysize 256 label router1.cisco.com
```

2. Create a local **trustpoint** in order to gain a certificate from the CA.

```
crypto pki trustpoint ec_ca
 enrollment terminal
 subject−name cn=router1.cisco.com
 revocation−check none
 eckeypair router1.cisco.com
 hash sha256
```

   Note: Because the CA is offline, revocation checking is disabled; revocation checking should be enabled for maximum security in a production environment.

3. Authenticate the **trustpoint**. This obtains a copy of the CA s certificate, which contains the public key.

```
crypto pki authenticate ec_ca
```

4. You are then prompted to enter the base 64 encoded certificate of the CA. This is the file ca.pem, which was created with OpenSSL. In order to view this file, open it in an editor or with the OpenSSL command **openssl x509 −in ca.pem**. Enter **quit** when you paste this. Then type **yes** to accept.
5. Enroll the router into the Public Key Infrastructure (PKI) on the CA.

```
crypto pki enrol ec_ca
```

6. The output that you receive needs to be used in order to submit a certificate request to the CA. This can be saved as a text file (flex.csr) and signed with the OpenSSL command.

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

7. Import the certificate, which is contained within the file flex.pem, generated from the CA, into the router after you enter this command. Then, enter **quit** when completed.

```
crypto pki import ec_ca certificate
```

ASA

1. Create **domain−name** and **hostname**, which are prerequisites in order to create an EC keypair.

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

2. Create a local **trustpoint** in order to obtain a certificate from the CA.

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

   Note: Because the CA is offline, revocation checking is disabled; revocation checking should be enabled for maximum security in a production environment.

3. Authenticate the **trustpoint**. This obtains a copy of the CA s certificate, which contains the public key.

```
crypto ca authenticate ec_ca
```

4. You are then prompted to enter the base 64 encoded certificate of the CA. This is the file ca.pem, which was created with OpenSSL. In order to view this file, open it in an editor or with the OpenSSL command **openssl x509 −in ca.pem**. Enter **quit** when you paste this file, and then type **yes** to accept.
5. Enrol the ASA into the PKI on the CA.

```
crypto ca enrol ec_ca
```

6. The output that you receive must be used in order to submit a certificate request to the CA. This can be saved as a text file (asa.csr) and then signed with the OpenSSL command.

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

7. Import the certificate, which is contained within the file as a.pem, generated from the CA into the router after this command is entered. Then **enter** quit when completed.

```
crypto ca import ec_ca certificate
```

Configuration

FlexVPN

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

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

Enter these commands for IKEv2 Proposal for Suite−B configuration:

Note: For maximum security, configure with the **aes−cbc−256 with sha512 hash** command.

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

Match the IKEv2 profile to the certificate map and use ECDSA with the **trustpoint** previously defined.

```
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
```

Configure IPSec transform set to use Galois Counter Mode (GCM).

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

Configure the IPSec profile with the parameters previously configured.

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

Configure the tunnel interface:

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

Here is the interface configuration:

```
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

Use this interface configuration:

```
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
```

Enter this access list command in order to define the traffic to be encrypted:

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

Enter this IPSec proposal command with NGE:

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

Cryptography map commands:

```
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
```

This command configures the IKEv2 policy with NGE:

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

Tunnel group configured for peer commands:

```
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
```

Connection Verification

Verify that the ECDSA keys have been successfully generated.

```
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...>
```

Verify that the certificate has successfully been imported and that ECDSA is used.

```
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...>
```

Verify that the IKEv2 SA is successfully created and uses the configured NGE algorithms.

```
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
```

Verify that the IPSec SA is successfully created and uses the configured NGE algorithms.

Note: FlexVPN can terminate IPSec connections from non-IOS clients that support both the IKEv2 and IPSec protocols.

```
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, }
```

For further information on Cisco s implementation of Suite−B, refer to the Next Generation Encryption White Paper.

Refer to the Next Generation Encryption Solution page to learn more about Cisco s implementation of Next Generation Encryption.

Related Information

- **Next Generation Encryption White Paper**
- **Next Generation Encryption Solution Page**
- **Secure Shell (SSH)**
- **IPSec Negotiation/IKE Protocols**
- **ASA IKEv2 Debugs for Site−to−Site VPN with PSKs TechNote**
- **ASA IPSec and IKE debugs (IKEv1 Main Mode) Troubleshooting TechNote**
- **IOS IPSec and IKE debugs − IKEv1 Main Mode Troubleshooting TechNote**
- **ASA IPSec and IKE debugs − IKEv1 Aggressive Mode TechNote**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 26, 2013 Document ID: 116008