AnyConnect to IOS Headend Over IPsec with IKEv2 and Certificates Configuration Example

TAC **Document ID: 115014**

Contributed by Marcin Latosiewicz and Atri Basu, Cisco TAC Engineers.
Jan 18, 2013

Contents

Introduction

This document provides information on how to achieve an IPsec−protected connection from a device that runs AnyConnect client to a Cisco IOS® router with only certificate authentication by utilizing FlexVPN framework.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FlexVPN
- AnyConnect

Components Used

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

Headend

Cisco IOS router can be any router capable of running IKEv2, running at least 15.2 M&T release. However, you should use a newer release (see the known caveats section), if available.

Client

AnyConnect 3.x release

Certificate authority

In this example, certificate authority (CA) will be running 15.2(3)T release.

It is crucial that one of the newer releases is used because of the need to support Extended Key Usage (EKU).

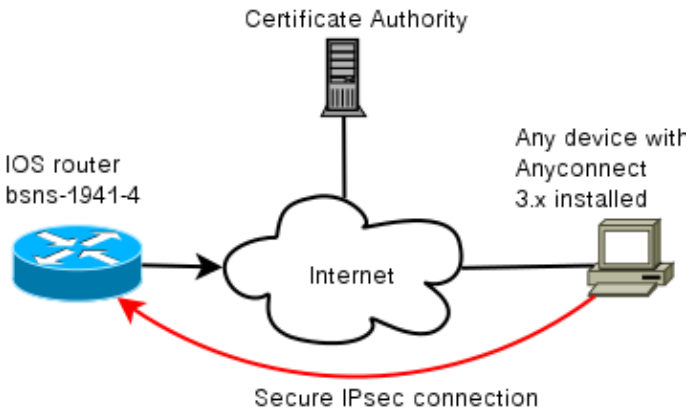
In this deployment, the IOS router is used as CA. However, any standards−based CA application capable of using EKU should be fine.

Conventions

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

Configuration

Network Topology



Certificate authority (optional)

If you choose to use it, your IOS router can act as a CA.

IOS CA configuration

You need to remember that the CA server must put the correct EKU on the client and server certificates. In this case server−auth and client−auth EKU were set for all certificates.

```
bsns−1941−3#show run | s crypto pki
crypto pki server CISCO
 database level complete
 database archive pem password 7 00071A1507545A545C
 issuer−name cn=bsns−1941−3.cisco.com,ou=TAC,o=cisco
 grant auto rollover ca−cert
 grant auto
```

```
 auto-rollover
 eku server-auth client-auth
```

How to verify if correct EKU was set on certificate

Note that bsns-1941-3 is the CA server while bsns-1941-4 is the IPsec headend. Parts of output omitted for brevity.

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
  Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
    X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
    Authority Info Access:
    Extended Key Usage:
        Client Auth
        Server Auth
  Associated Trustpoints: CISCO2
  Storage: nvram:bsns-1941-3c#5.cer
  Key Label: BSNS-1941-4.cisco.com
  Key storage device: private config

CA Certificate
(...omitted...)
```

Headend configuration

Headend configuration is comprised of two parts: the PKI part and actual flex/IKEv2.

PKI configuration

You will notice that CN of bsns-1941-4.cisco.com is used. This needs to match a proper DNS entry and needs to be included in the AnyConnect profile under <Hostname>.

```
crypto pki trustpoint CISCO2
 enrollment url http://10.48.66.14:80
 serial-number
 ip-address 10.48.66.15
 subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
 revocation-check none

crypto pki certificate map CMAP 10
 subject-name co cisco
```

Crypto/IPsec configuration

Note that your PRF/integrity setting in proposal ***NEEDS*** to match what your certificate supports. This is typically SHA-1.

```
crypto ikev2 authorization policy AC
pool AC
```

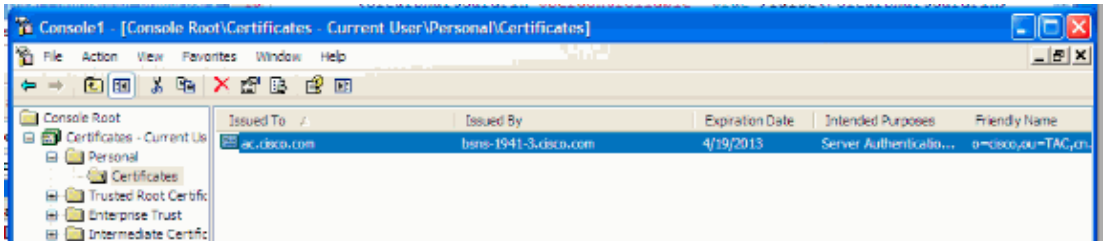
```
crypto ikev2 proposal PRO
  encryption 3des aes-cbc-128
  integrity sha1
  group 5 2

crypto ikev2 policy POL
  match fvrf any
  proposal PRO

crypto ikev2 profile PRO
  match certificate CMAP
  identity local dn
  authentication remote rsa-sig
  authentication local rsa-sig
  pki trustpoint CISCO2
  aaa authorization group cert list default AC
  virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
  set transform-set TRA
  set ikev2-profile PRO

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

Client

Client configuration for a successful AnyConnect connection with IKEv2 and certificates consists of two parts.

Certificate enrollment

When the certificate is properly enrolled, you can verify that it is present either in machine or personal store. Remember that client certificates also need to have EKU.



AnyConnect profile

The AnyConnect profile is lengthy and very basic.

The relevant part is to define:

1. Host you are connecting to
2. Type of protocol
3. Authentication to be used when connected to that host

What is used:

```
<ServerList>
        <HostEntry>
            <HostName>bsns-1941-4.cisco.com</HostName>
            <PrimaryProtocol>IPsec
                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>
                     IKE-RSA
                    </AuthMethodDuringIKENegotiation>
                </StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
    </ServerList>
```

In the connection field of AnyConnect you need to provide the full FQDN, which is the value seen in `<HostName>`.

Connection verification

Some information is omitted for brevity.

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2  SA
 Tunnel-id Local          Remote          fvrf/ivrf          Status
2    10.48.66.15/4500    10.55.193.212/65311   none/none    READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5,
              Auth sign: RSA, Auth verify: RSA
      Life/Active Time: 86400/180 sec


IPv6 Crypto IKEv2  SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0)
   current_peer 10.55.193.212 port 65311
     PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
    #pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26

     local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x5C171095(1545015445)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8283D0F0(2189676784)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040,
                 crypto map: Virtual-Access1-head-0
        sa timing: remaining key lifetime (k/sec): (4215478/3412)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound esp sas:
      spi: 0x5C171095(1545015445)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
```

```
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040,
         crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215482/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

Next generation cryptography

The above configuration is provided for reference to show a minimal working configuration. Cisco recommends using next generation cryptography (NGC) where possible.

Current recommendations for migration can be found here:
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

When choosing NGC configuration, make sure that both client software and headend hardware support it. ISR generation 2 and ASR 1000 routers are recommended as headends because of their hardware support for NGC.

On the AnyConnect side, as of the AnyConnect 3.1 version, NSA's Suite B algorithm suite is supported.

Known caveats and issues

- Remember to have this line configured on your IOS headend: ***no crypto ikev2 http-url cert***. The error produced by IOS and AnyConnect when this is not configured is quite misleading.
- Early IOS 15.2M&T software with IKEv2 session might not come up for RSA-SIG authentication. This can be related to Cisco bug ID CSCtx31294 (registered customers only) . Make sure to run the latest 15.2M or 15.2T software.
- In certain scenarios IOS might not be able to pick the correct trustpoint to authenticate. Cisco is aware of the issue, and it is fixed as of 15.2(3)T1 and 15.2(4)M1 releases.
- If AnyConnect is reporting a message similar to this:

```
The client certificate's cryptographic service provider(CSP)
    does not support the sha512 algorithm
```

Then, you need to make sure that the integrity/PRF setting in your IKEv2 proposals match what your certificates can handle. In the configuration example above, SHA-1 is used.

Related Information

- ***Technical Support & Documentation - Cisco Systems***

Updated: Jan 18, 2013 Document ID: 115014