与Windows 7 IKEv2敏捷VPN客户端的在FlexVPN的IKEv2和证书验证

目录

简介

FlexVPN是新的互联网密钥交换版本2 (在Cisco IOS的IKEv2)-based VPN基础设施和被认为是一个统一的VPN解决方案。本文描述如何配置被构件到Windows 7为了连接与Certificate Authority (CA)的利用率的一Cisco IOS头端的IKEv2客户端。

> **注意**：可适应安全工具(ASA)自版本9.3(2)现在支持IKEv2与Windows 7镶入客户端的连接。

> **注意**：SUITE-B协议不工作，因为IOS头端不支持与IKEv1的SUITE-B，或者Windows 7 IKEv2敏捷VPN客户端当前不支持与IKEv2的SUITE-B。

先决条件

要求

Cisco 建议您了解以下主题：

- Windows 7镶入VPN客户端
- Cisco IOS软件版本15.2(2)T
- 认证机关- Openssl CA

使用的组件

本文档中的信息基于下列硬件和软件版本：

- Windows 7镶入VPN客户端
- Cisco IOS软件Release15.2(2)T
- 认证机关- Openssl CA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

配置

概述

有四个主要步骤在Windows 7内置的IKEv2客户端的配置方面为了连接与CA:的利用率的一Cisco IOS头端

1. 配置CA

   CA在证书应该允许您嵌入需要的延长的密钥用法(EKU)。例如，在IKEv2服务器，‘服务器验证EKU’要求，而客户端证书需要‘客户端验证EKU’。本地部署能利用：Cisco IOS CA服务器-自签名证书不可能使用由于bug CSCuc82575。Openssl CA服务器Microsoft CA服务器-一般来说，因为可以配置正确地签署证书如期望的一样，这是首选。

2. 配置Cisco IOS头端

   获取证书配置IKEv2

3. 配置Windows 7镶入客户端
4. 获取客户端证书

这些主要步骤中的每一个在随后部分详细解释。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置认证机关

本文不提供详细步骤关于怎样设置CA。然而，在此部分的步骤显示您如何配置CA，因此它能发行这种的证书部署。

Openssl

Openssl CA根据‘设置’文件。Openssl服务器的‘设置’文件应该有：

```
[ extCSR ]
keyUsage            = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage    = serverAuth, clientAuth
```

Cisco IOS CA服务器

如果使用一个Cisco IOS CA服务器，请确保您使用最最近的Cisco IOS软件版本，分配EKU。

```
IOS-CA# show run | section crypto pki
crypto pki server IOS-CA
 issuer-name cn=IOS-CA.cisco.com,ou=TAC,o=cisco
 grant auto
  eku server-auth client-auth
```

配置Cisco IOS头端

获取证书

证书必须有EKU字段设置为‘服务器验证’ Cisco IOS和‘客户端验证的’客户端的。一般，同样CA用于签署两客户端和服务器证书。在这种情况下，‘服务器验证’和‘客户端验证’在各自服务器证书和客户端证书被看到，是可接受。

如果在公钥加密标准(PKCS) #12的证书在IKEv2服务器给客户端和服务器格式化的CA问题，并且，如果证书撤销列表(CRL)不是可及的或可用的，必须配置：

```
IOS-CA# show run | section crypto pki
crypto pki server IOS-CA
 issuer-name cn=IOS-CA.cisco.com,ou=TAC,o=cisco
 grant auto
  eku server-auth client-auth
```

输入此命令为了导入PKCS-12证书：

```
copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash:/
crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password>
!! Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.
```

如果Cisco IOS CA服务器自动授权证书，必须配置如此示例所显示， IKEv2服务器以CA服务器URL为了接收证书：

```
copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash:/
crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password>
!! Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.
```

当信任点配置时，您需要：

1. 验证CA用此命令：

```
copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash:/
crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password>
!! Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.
```

2. 登记有CA的IKEv2服务器用此命令：


```
copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash:/
crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password>
!! Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.
```


为了看到证书是否包含所有所需的选项，请使用此**show命令**：

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption
 Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

 Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
 X509v3 extensions:
   X509v3 Key Usage: F0000000
      Digital Signature
     Non Repudiation
     Key Encipherment
     Data Encipherment
   X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
   X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
   Authority Info Access:
   Extended Key Usage:
        Client Auth
        Server Auth
 Associated Trustpoints: FlexRootCA
 Key Label: FlexRootCA
```

配置IKEv2

这是IKEv2配置示例：

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
```

```
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
Signature Algorithm: MD5 with RSA Encryption
Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
X509v3 extensions:
  X509v3 Key Usage: F0000000
     Digital Signature
    Non Repudiation
    Key Encipherment
    Data Encipherment
  X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
  X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
  Authority Info Access:
  Extended Key Usage:
       Client Auth
       Server Auth
Associated Trustpoints: FlexRootCA
Key Label: FlexRootCA
```

虚拟模板的Ip unnumbered应该是任何用于IPSec连接的exceptthe本地地址。 [If you use a hardware client， you would exchange routing information via IKEv2 configuration node and create a recursive routing issue on the hardware client.]

配置Windows 7镶入客户端

此步骤描述如何配置Windows 7镶入客户端。

1. 导航对**网络和共享中心**，并且单击**建立新连接或网络**。

2. 点击**使用我的互联网连接(VNP)**。这允许您设置在当前互联网连接协商的VPN连接。

3. 输入完全合格的域名(FQDN)或IKEv2服务器的IP地址，并且给予它目的地名称识别它本地。

   注意：FQDN必须匹配从路由器身份证书的共同名称(CN)。如果检测不匹配， Windows 7切与错误13801的连接。
   由于另外的参数需要设置，检查**当前不连接;设置它我能如此连接以后**，并且**其次**单击：

4. 请勿填写**用户名**、**密码**和**域(可选)**字段，因为将使用证书验证。单击**创建**。

   注意：关上产生的窗口。**请勿设法连接。**
5. 导航回到**网络和共享中心**，并且点击**崔凡吉莱适配器设置**。

6. 选择逻辑适配器FlexVPN IOS，是所有步骤结果采取对此点。点击其属性。这些是呼叫FlexVPN IOS的新建立的连接配置文件的属性：

   在安全选项卡， VPN种类应该是IKEv2。在Authentication部分，请选择**使用机器认证**。

   在您导入certifcate到机器认证存储后， FlexVPN IOS配置文件当前准备连接。

获取客户端证书

客户端证书要求这些要素：

- 客户端证书有'客户端验证' EKU。并且， CA给PKCS-12证书：

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption
 Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

 Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
 X509v3 extensions:
   X509v3 Key Usage: F0000000
      Digital Signature
     Non Repudiation
     Key Encipherment
     Data Encipherment
   X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
   X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
   Authority Info Access:
   Extended Key Usage:
        Client Auth
        Server Auth
 Associated Trustpoints: FlexRootCA
 Key Label: FlexRootCA
```

- CA证书：

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
   cn=ikev2.cisco.com
```

```
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption
 Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

 Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
 X509v3 extensions:
   X509v3 Key Usage: F0000000
      Digital Signature
     Non Repudiation
     Key Encipherment
     Data Encipherment
   X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
   X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
   Authority Info Access:
   Extended Key Usage:
        Client Auth
        Server Auth
 Associated Trustpoints: FlexRootCA
 Key Label: FlexRootCA
```

重要详细信息

- ‘IPSec应该使用IKE中间’ (OID = 1.3.6.1.5.5.8.2.2)作为EKU，如果这两个语句应用：

  IKEv2服务器是Windows 2008服务器。有超过一个服务器验证证书在使用中IKEv2连接的。如果这是真的，任一地方‘服务器验证’ EKU和‘在一证书的IPSec IKE半成品’ EKU或者分配这些在证书中的EKUs。确保至少一证书包含‘IPSec IKE中间’ EKU。

  参考排除故障IKEv2 VPN Connectionsfor更多信息。

- 在FlexVPN部署，请勿使用‘IPSec IKE中间’在EKU。如果， IKEv2客户端不拾起IKEv2服务器证书。结果，他们不能响应到从IOS的CERTREQ在IKE_SA_INIT响应消息和不因而能连接13806个错误ID。

- 当附属的替代方案名称(SAN)时没有要求，是可接受，如果证书有一。

- 在Windows 7客户端证书存储，请确保计算机委托根证明权限存储有可能的证书最少编号。如果它有超过50余， Cisco IOS也许不能读整个Cert_Req有效负载，包含所有已知CA证书特有名(DN)从Windows 7方框的。结果，协商发生故障，并且您看到在客户端的连接超时。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

```
ikev2#show crypto ikev2 session detail
IPv4 Crypto IKEv2 Session

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.3.1/4500 192.168.56.1/4500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/17 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: A40828A826160328 Remote spi: C004B7103936B430
Local id: ikev2.cisco.com
Remote id: ou=TAC,o=Cisco,c=BE,cn=Win7
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 1 DPD configured for 0 seconds,
retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled

ikev2#show crypto ipsec sa peer 192.168.56.1

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 10.0.3.1
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): (172.16.0.104/255.255.255.255/0/0)
current_peer 192.168.56.1 port 4500
PERMIT, flags={origin_is_acl,}
#pkts encaps:5, #pkts encaps:5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.3.1, remote crypto endpt.: 192.168.56.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x3C3D299(63165081)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xE461ED10(3831622928)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 7, flow_id: SW:7, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4257423/0)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x3C3D299(63165081)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 8, flow_id: SW:8, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4257431/0)
IV size: 16 bytes
replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 站点到站点VPN的ASA IKEv2调试与PSKs TechNote
- 主模式)排除故障TechNote的ASA IPsec和IKE调试(IKEv1
- IOS IPSec和IKE调试- IKEv1排除故障TechNote的主模式
- ASA IPSec和IKE调试- IKEv1积极模式TechNote
- Cisco ASA 5500 系列自适应安全设备
- Cisco ASA 5500系列自适应安全设备软件下载
- Cisco IOS 防火墙
- Cisco IOS 软件
- Secure Shell (ssh)
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems