FlexVPN和Anyconnect IKEv2客户端配置示例

目录

简介

本文描述如何配置Cisco AnyConnect安全移动客户端使用远程验证拨入用户服务(RADIUS)和本地授权属性为了验证Microsoft Active Directory。

> **注意**：目前，使用验证的本地用户数据库在Cisco IOS设备不作用。这是因为Cisco IOS不功能作为EAP验证器。增强请求CSCui07025是被归档的添加支持。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS版本15.2(T)或以上

- Cisco AnyConnect安全移动客户端版本3.0或以上
- Microsoft Active Directory

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档中所述功能的信息。

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。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- 中心配置
- Microsoft Active Directory服务器配置
- 客户端配置

中心配置

1. 配置仅验证的RADIUS并且定义本地授权。

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
aaa authentication login FlexVPN-AuthC-List-1 group
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

list命令的AAA认证登录是指定义了RADIUS服务器)的验证、授权和统计(AAA)组(。本地定义用户/组的**AAA授权网络list命令**状态将使用。必须更改在RADIUS服务器的配置允许从此设备的认证请求。

2. 配置本地授权策略。

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
```

```
def-domain example.com
```

ip local pool命令用于定义分配到客户端的IP地址。授权策略定义与*FlexVPN-Local-Policy-1*用户名，并且客户端的(DNS服务器属性，网络屏蔽、已分解列表，域名，等等)配置此处。

3. 保证服务器使用证书(rsa-sig)为了验证。

   Cisco AnyConnect安全移动客户端需要服务器验证使用证书(rsa-sig)。路由器必须有一*Web服务器*证书(即与'服务器验证的'一证书在延长的密钥用法分机内)从委托Certificate Authority (CA)。

   在ASA 8.x的参考的步骤1至4手工安装第三方供应商证书为了用在WebVPN配置示例上，并且更改*crypto加州*所有实例对*crypto pki*。

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. 配置此连接的设置。
```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1
FlexVPN-Local-Policy-1
virtual-template 10
```
   大多**crypto ikev2 profilec** ontains此连接的相关设置： **匹配标识远程key-id** -是指客户端使用的IKE标识。此字符串值在AnyConnect XML配置文件内配置。**标识本地dn** -定义了FlexVPN集线器使用的IKE标识。此值使用值从使用的证书的内部。**验证远程**-阐明，应该用于EAP客户端验证。**验证本地状态**应该用于证书本地验证。**AAA认证eap** -使用AAA认证登录列表的状态FlexVPN-AuthC-List-1，当EAP使用验证。**AAA授权组eap列表**-使用AAA授权网络列表的状态FlexVPN-AuthZ-List-1以*FlexVPN-Local-Policy-1*用户名授权属性。**虚拟模板10** -定义了使用的哪个模板，当虚拟访问接口被克隆。

5. 配置回到IKEv2配置文件的链路在步骤4.定义的IPSec简档。
```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```
   注意：Cisco IOS使用聪明的默认。结果，转换集不需要明确地定义。

6. 配置虚拟访问接口被克隆的虚拟模板：
   ip unnumbered -不编号从*内部接口*，因此IPv4路由的接口在接口可以启用。**隧道模式ipsec ipv4 -**定义了接口是VTI类型通道。
```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. 对SHA-1限制协商。（可选）

   由于欠缺CSCud96246 (仅限注册用户)，AnyConnect客户端也许不能正确地验证FlexVPN集线器证书。此问题归结于协商伪随机功能的(PRF)的IKEv2一个SHA-2功能使用SHA-1，而FlexVPN HUB证书签了字。配置下面的限额对SHA-1的协商：

```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrf any
proposal SHA1-only
```

Microsoft Active Directory服务器配置

1. 在Windows服务器管理器，请展开**角色>网络策略和接入服务器> NMP (本地) > RADIUS客户端和服务器**，并且点击**RADIUS客户端**。

   新的RADIUS客户端对话框出现。

2. 在新的RADIUS客户端对话框中，请添加Cisco IOS路由器作为RADIUS客户端：
   点击**Enable (event)此RADIUS客户端**复选框。在友好名称字段输入一名称。此示例使用FlexVPN *HUB*。在地址字段输入路由器的IP地址。在共享秘密区域中，请点击**手工的**单选按钮，并且输入在共享机密的共享机密并且确认共享秘密字段。**注意：** 共享机密必须匹配在路由器配置的共享机密。单击 **Ok**。

3. 在服务器管理器接口，请展开**策略**，并且选择**网络策略**。

   新的网络策略对话框出现。

4. 在新的网络策略对话框中，请添加一个新的网络策略：

   输入在Policy Name字段的一名称。此示例使用*FlexVPN*。点击**网络类型接入服务器**单选按钮，并且从下拉列表选择**未指定**。单击 **Next**。在新的网络策略对话框中，请单击**添加**添加一个新的情况。在挑选情况对话框中，请选择**NAS IPv4地址**情况，并且单击**添加**。

   NAS IPv4地址对话框出现。

   在NAS IPv4地址对话框中，请输入网络接入服务器的IPv4地址为了对起源于此Cisco IOS路由器的仅请求限制网络策略。

   单击 **Ok**。

在新的网络策略对话框中，请点击**访问授权的**单选按钮为了允许对网络的访客接入(如果用户提供的凭证有效)，并且**其次**单击。

保证仅Microsoft ：安全口令(EAP-MSCHAP v2)在EAP标准地区出现为了允许作为在Cisco IOS设备和活动目录之间的通信方法将使用的EAP-MSCHAPv2，并且**其次**单击。

注意：留给所有'较不安全认证方法的选项被不选定。

通过向导继续并且应用任何另外的限制条件或设置如定义由您的组织安全策略。另外，请保证如此镜像所显示，策略首先在处理顺序列出：

客户端配置

1. 创建在文本编辑内的一XML配置文件，并且命名它*flexvpn.xml*。

   此示例使用此XML配置文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true
</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true
</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false
</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true
</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false
</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
```

```
</AutoReconnect>
<AutoUpdate UserControllable="true">false</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false">
</PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="true">true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<hostname>是在客户端出现的文本字符串。**<HostAddress>**是FlexVPN集线器的完全合格的域名(FQDN)。**<PrimaryProtocol>**配置连接使用IKEv2/IPsec而不是SSL (默认在AnyConnect)。**<AuthMethodDuringIKENegotiation>**配置连接使用在EAP内的MSCHAPv2。此值为Microsoft Active Directory的验证要求。**<IKEIdentity>**定义了匹配客户端对在集线器的特定IKEv2配置文件的字符串值(请参阅以上的步骤4)。
注意：客户端配置文件是客户端只使用的事。推荐管理员使用Anyconnect配置文件编辑器为了创建客户端配置文件。

2. 保存flexvpn.xml文件对适当的目录如在此表列出：

3. Close和重新启动AnyConnect客户端。

4. 在Cisco AnyConnect安全移动客户端对话框中，请选择**FlexVPN集线器**，并且点击**连接**。

思科AnyConnect|FlexVPN集线器对话框出现。

5. 输入用户名和密码，并且点击OK键。

验证

为了验证连接，请使用**显示crypto会话详细信息远程客户端IP地址**命令。refer to显示crypto会话关于此命令的更多信息。

> **注意**：命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

为了排除故障连接，从客户端收集和分析箭日志和使用这些调试on命令路由器： **debug crypto ikev2内部的数据包**和的**debug crypto ikev2**。

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- 技术支持和文档 - Cisco Systems