具有本地AAA属性列表的FlexVPN动态配置

目录

简介

此配置示例演示如何使用本地身份验证、授权和记帐(AAA)属性列表，以便无需使用外部远程身份验证拨入用户服务(RADIUS)服务器即可执行动态和潜在的高级配置。

在某些场景中，特别是在需要快速部署或测试时，这是必要的。此类部署通常是概念验证实验、新部署测试或故障排除。

动态配置在集中器/集线器端非常重要，在该端，应按用户、客户、会话应用不同的策略或属性。

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（但不限于）这些软件和硬件版本。此列表不列出最低要求，而是反映设备在此功能测试阶段的状态。

Hardware

- 聚合服务路由器(ASR)- ASR 1001 — 称为“bsns-asr1001-4”
- 第2代集成多业务路由器(ISR G2)- 3925e — 称为“bsns-3925e-1”
- 第2代集成多业务路由器(ISR G2)- 3945e — 称为“bsns-3945e-1”

软件

- 思科IOS XE版本3.8 - 15.3(1)S
- 思科IOS®软件版本15.2(4)M1和15.2(4)M2

许可证

- ASR路由器启用adventerprise和ipsec功能许可证。
- ISR G2路由器已启用ipbasek9、securityk9和hseck9功能许可证。

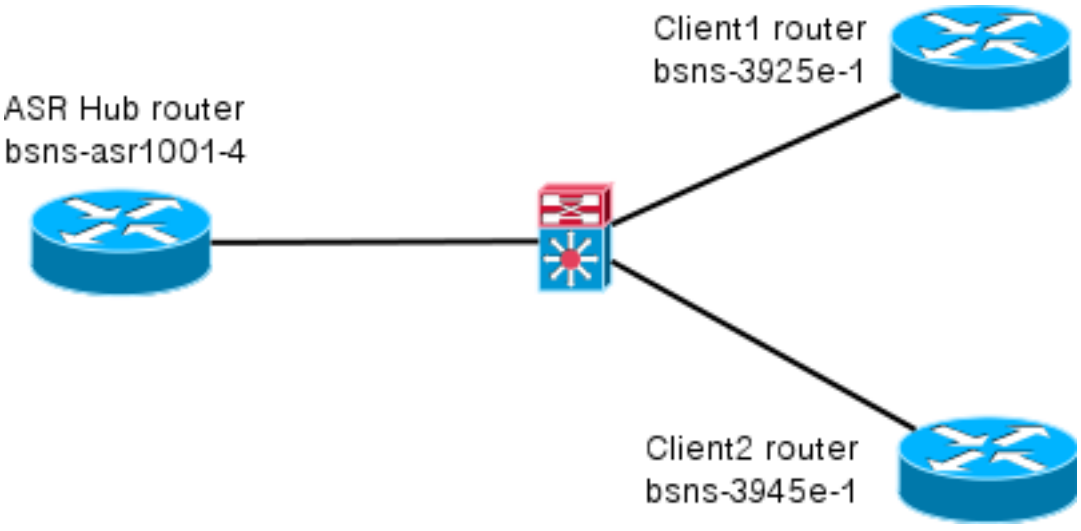
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

拓扑

本练习中使用的拓扑是基本的。使用一个中心路由器(ASR)和两个分支路由器(ISR)来模拟客户端。



配置

本文档中的配置旨在显示基本设置，尽可能使用智能默认值。有关思科对加密的建议，请访问cisco.com上的下一代加密页。

分支配置

如前所述，本文档中的大多数操作都在集线器上执行。辐条配置在此供参考。在此配置中，请注意，只有Client1和Client2之间的身份变更（以粗体显示）。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 identity local email Client1@cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

中心配置

集线器配置分为两部分：

1. **基本连接配**置，概述基本连接所需的配置。
2. **扩展配**置，其中概述了管理员如何使用AAA属性列表执行每用户或每会话配置更改所需的配置更改。

基本连通性配置

此配置仅供参考，并不是最佳配置，而是只能发挥作用。

此配置的最大限制是使用预共享密钥(PSK)作为身份验证方法。思科建议在适用时使用证书。

```
aaa new-model
aaa authorization network default local

aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
 route set interface

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
 peer Client1
 identity email Client1@cisco.com
 pre-shared-key cisco
 !!
 peer Client2
 identity email Client2@cisco.com
 pre-shared-key cisco

crypto ikev2 profile Flex_IKEv2
 match fvrf any
 match identity remote address 0.0.0.0
 match identity remote email domain cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

no crypto ikev2 http-url cert

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Virtual-Template1 type tunnel
 vrf forwarding IVRF
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel vrf INTERNET
 tunnel protection ipsec profile default
```

扩展配置

为特定会话分配AAA属性需要做几件事。此示例显示了client1的完整工作；然后显示如何添加其他客户端/用户。

客户端1的扩展集线器配置

1. 定义AAA属性列表。

```
aaa attribute list Client1
 attribute type interface-config "ip mtu 1300" protocol ip
 attribute type interface-config "service-policy output TEST" protocol ip
```

注意：请记住，通过属性分配的实体必须在本地存在。在这种情况下，**策略映**射之前已配置。

```
policy-map TEST
 class class-default
 shape average 60000
```

2. 将AAA属性列表分配给授**权策略。**

```
crypto ikev2 authorization policy Client1
 pool FlexSpokes
 aaa attribute list Client1
 route set interface
```

3. 确保连接的客户端使用此新策略。在这种情况下，提取客户端发送的身份的**用户名**部分。客户端应使用ClientX@cisco.com（X为1或2，取决于客户端）的电子邮件地址。 mangler将电子邮件地址拆分为用户名和域部分，并且仅使用其中一个（本例中为用户名）来选择授权策略的名称。

```
crypto ikev2 name-mangler GET_NAME
 email username

crypto ikev2 profile Flex_IKEv2
 aaa authorization group psk list default name-mangler GET_NAME
```

当client1运行时，可以相对轻松地添加client2。

客户端2的扩展集线器配置

确保存在策略和单独的属性集（如果需要）。

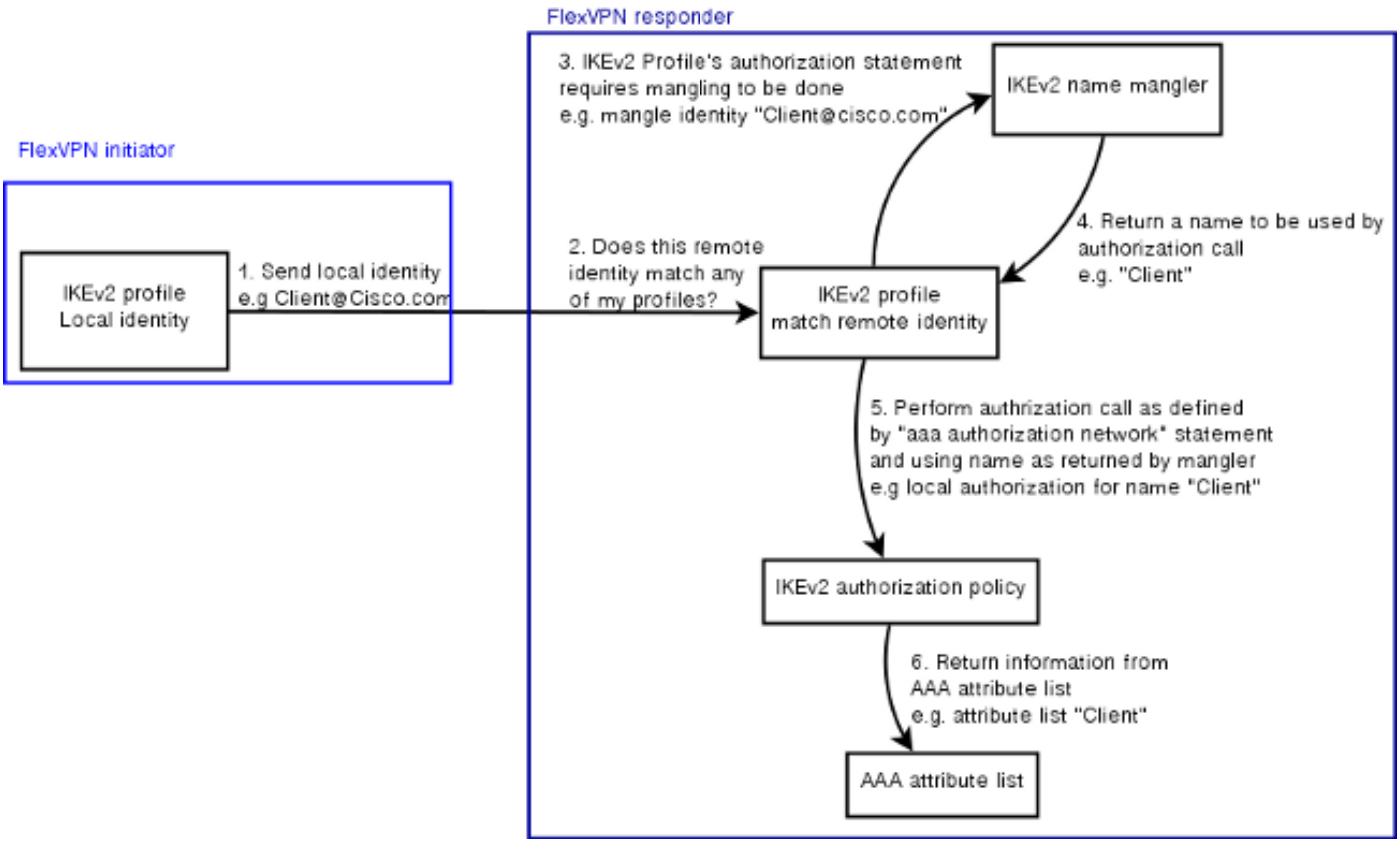
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

crypto ikev2 authorization policy Client2
 pool FlexSpokes
 aaa attribute list Client2
 route set interface
```

在本示例中，应用了更新的最大段大小(MSS)设置和为此客户端运行的入站访问列表。可以轻松选择其他设置。典型的设置是为不同的客户端分配不同的虚拟路由和转发(VRF)。如前所述，分配给属性列表的任何实体（如本场景中的access-list 133）必须已存在于配置中。

流程概述

此图概述了通过Internet密钥交换版本2(IKEv2)配置文件处理AAA授权时的操作顺序，并包含特定于此配置示例的信息。



确认

本节介绍如何验证之前分配的设置是否已应用到客户端。

客户端1

以下命令用于验证最大传输单位(MTU)设置以及服务策略已应用。

```
bsns-asr1001-4#show cef int virtual-access 1
(...)
 Hardware idb is Virtual-Access1
 Fast switching type 14, interface type 21
 IP CEF switching enabled
 IP CEF switching turbo vector
 IP Null turbo vector
 VPN Forwarding table "IVRF"
 IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
 Tunnel VPN Forwarding table "INTERNET" (tableid 2)
 Input fast flags 0x0, Output fast flags 0x4000
 ifindex 16(16)
 Slot unknown (4294967295) Slot unit 1 VC -1
 IP MTU 1300
 Real output interface is GigabitEthernet0/0/0

bsns-asr1001-4#show policy-map interface virtual-access1
 Virtual-Access1

Service-policy output: TEST

Class-map: class-default (match-any)
 5 packets, 620 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
```

```
 Match: any
 Queueing
 queue limit 64 packets
 (queue depth/total drops/no-buffer drops) 0/0/0
 (pkts output/bytes output) 5/910
 shape (average) cir 60000, bc 240, be 240
 target shape rate 60000
```

客户端2

以下命令用于验证MSS设置已推送，且访问列表133也已作为入站过滤器应用于等效虚拟访问接口。

```
bsns-asr1001-4#show cef int virtual-access 2
Virtual-Access2 is up (if_number 18)
 Corresponding hwidb fast_if_number 18
 Corresponding hwidb firstsw->if_number 18
 Internet address is 0.0.0.0/0
 Unnumbered interface. Using address of Loopback100 (192.168.1.1)
 ICMP redirects are never sent
 Per packet load-sharing is disabled
 IP unicast RPF check is disabled
 Input features: Access List, TCP Adjust MSS
 (...)

bsns-asr1001-4#show ip interface virtual-access2
Virtual-Access2 is up, line protocol is up
 Interface is unnumbered. Using address of Loopback100 (192.168.1.1)
 Broadcast address is 255.255.255.255
 MTU is 1400 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is 133, default is not set
(...)
```

调试

调试有两个主要块。当您需要打开TAC案例并更快地按顺序进行处理时，此功能非常有用。

调试IKEv2

从以下主要调试命令开始：

```
debug crypto ikev2 [internal|packet]
```

然后输入以下命令：

```
show crypto ikev2 sa
show crypto ipsec sa peer a.b.c.d
```

调试AAA属性分配

如果要调试属性的AAA分配，这些调试可能会有所帮助。

```
debug aaa authorization
debug aaa attr
debug aaa proto local
```

结论

本文档演示如何使用AAA属性列表，以便在RADIUS服务器可能不可用或不需要的FlexVPN部署中增加灵活性。如果需要，AAA属性列表会按会话、按组提供添加的配置选项。

相关信息

- FlexVPN和互联网密钥交换第2版配置指南，思科IOS版本15M&T
- 远程身份验证拨入用户服务(RADIUS)
- 请求注解 (RFC)
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems