与本地AAA属性列表的FlexVPN动态配置

目录

简介

此配置示例展示如何使用本地认证，授权和核算(AAA)属性列表为了执行动态和潜在高级配置，不用使用外部远程验证拨入用户服务(RADIUS)服务器。

特别是当迅速部署或测验要求时，在某些情况下这希望。这样部署是典型地proof-of-concept实验室、新建的部署测试或者故障排除。

动态配置是重要在根据一个每用户，每个用户，每会话基本类型应该应用不同的策略或属性的集中器/集线器端。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据，但是没有被限制对，这些软件和硬件版本。此列表不略述最低要求，然而反射设备的状态在测试阶段此功能期间。

硬件

- 聚合服务路由器(ASR) - ASR 1001 -呼叫的"bsns-asr1001-4"
- 集成服务路由器生成2 (ISR G2) - 3925e -呼叫的"bsns-3925e-1"
- 集成服务路由器生成2 (ISR G2) - 3945e -呼叫的"bsns-3945e-1"

软件

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

许可证

- ASR路由器安排**adventerprise**和**ipsec**功能许可证启用。
- ISR G2路由器安排**ipbasek9**、**securityk9**和**hseck9**功能许可证启用。

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

用于此练习的拓扑基本。使用中心路由器(ASR)和两分支路由器(ISR)，模拟客户端。

配置

在本文的配置打算尽量表示一个基本设置，以聪明的默认。对于在加密算法的Cisco推荐，请访问在cisco.com的下一代加密页。

分支配置

如被提及以前，大多在此文档的操作在集线器进行。辐条配置在这里供参考。在此配置中，请注意仅更改是在Client1和Client2之间的标识(显示在粗体)。

```
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

集线器上配置分开成两部分：

1. **基本连通性配置**，略述配置为基本连通性需要。
2. **延长的配置**，概述配置更改需要为了展示管理员如何能使用AAA属性列表进行每用户或每会话配置更改。

基本连通性配置

此配置是供仅参考和没有被认为是最佳的，仅功能。

此配置的最巨大的限制是使用情况预先共享密钥(PSK)作为认证方法。思科推荐使用证书，每当可适用。

```
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
```

延长的配置

有一些工作必要的分配AAA属性给特定的会话。此示例显示完整为client1工作;然后它如何显示添加另一个客户端/用户。

Client1的延长的集线器上配置

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：** 切记通过属性分配的实体必须存在本地。在这种情况下，**策略映射**以前配置。`policy-map TEST`
   `class class-default`
   `shape average 60000`
2. 分配AAA属性列表到**授权策略。**`crypto ikev2 authorization policy` **`Client1`** `pool FlexSpokes`
   `aaa attribute list Client1 route set interface`
3. 保证这连接的客户端使用的新建的策略。在这种情况下，请解压缩客户端发送的标识的**用户名**部分。客户端应该使用ClientX@cisco.com电子邮件地址(X是1或2，从属的于客户端)。**mangler**只拆分电子邮件地址到用户名和域部分并且使用他们中的一个(用户名在这种情况下)选择授权策略名称。`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是可操作的时，client2可以是被添加的相对容易。

Client2的延长的集线器上配置

保证一项策略，并且另二套属性，若需要，存在。

```
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
```

在本例中，一更新最大分段尺寸(MSS)设置和进入访问控制列表为此客户端运行应用。其他设置可以容易地选择。典型的设置是分配另外虚拟路由和转发(VRF)不同的客户端的。如前面提到，所有实体分配到属性列表，例如access-list 133在此方案，必须在配置里已经存在。

进程概述

此图概述运算顺序，当AAA授权通过互联网密钥交换版本2 (IKEv2)时配置文件处理并且包含信息特定对此配置示例。

验证

此部分显示如何验证以前分配的设置应用给客户端。

Client1

这是验证的命令最大传输传声单位(MTU)设置，以及服务策略应用。

```
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
```

Client2

这是验证的命令MSS设置推送，并且access-list 133也应用作为在等同的虚拟访问接口的一个Inbound过滤器。

```
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

有调试的两主要块。当您需要开TAC案例和获得在跟踪的事更加快速时，这是有用的。

调试IKEv2

用此主要debug命令开始：

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

然后请输入这些命令：

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

Debug aaa属性分配

如果会想要对debug aaa属性的分配，这些调试可以是有用。

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

结论

本文展示如何使用AAA属性列表为了允许在RADIUS服务器也许不取得到的FlexVPN部署的已添加灵活性或没有希望。如果要求， AAA属性列表提供在每会话的已添加配置选项，基于组。

相关信息

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