使用本地AAA屬性清單的FlexVPN動態配置

目錄

簡介

此組態範例示範了如何使用本機驗證、授權和記帳(AAA)屬性清單在不使用外部遠端驗證撥入使用者服務(RADIUS)伺服器的情況下執行動態和潛在的進階組態。

在某些情況下需要這樣做，尤其是當需要快速部署或測試時。此類部署通常是概念驗證實驗、新部署測試或故障排除。

在集中器/集線器端，動態配置非常重要，因為不同的策略或屬性應針對每個使用者、每個客戶、每個會話應用。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據（但不限於）這些軟體和硬體版本。此清單不概述最低要求，但反映此功能整個測試階段的裝置狀態。

硬體

- 聚合服務路由器(ASR)- ASR 1001 — 稱為「bsns-asr1001-4」
- 第二代整合多業務路由器(ISR G2)- 3925e — 稱為「bsns-3925e-1」
- 第二代整合多業務路由器(ISR G2)- 3945e — 稱為「bsns-3945e-1」

軟體

- Cisco IOS XE版本3.8 - 15.3(1)S
- Cisco IOS®軟體版本15.2(4)M1和15.2(4)M2

授權

- ASR路由器啟用了**adventerprise**和**ipsec**功能許可證。
- ISR G2路由器啟用了**ipbasek9**、**securityk9**和**hseck9**功能許可證。

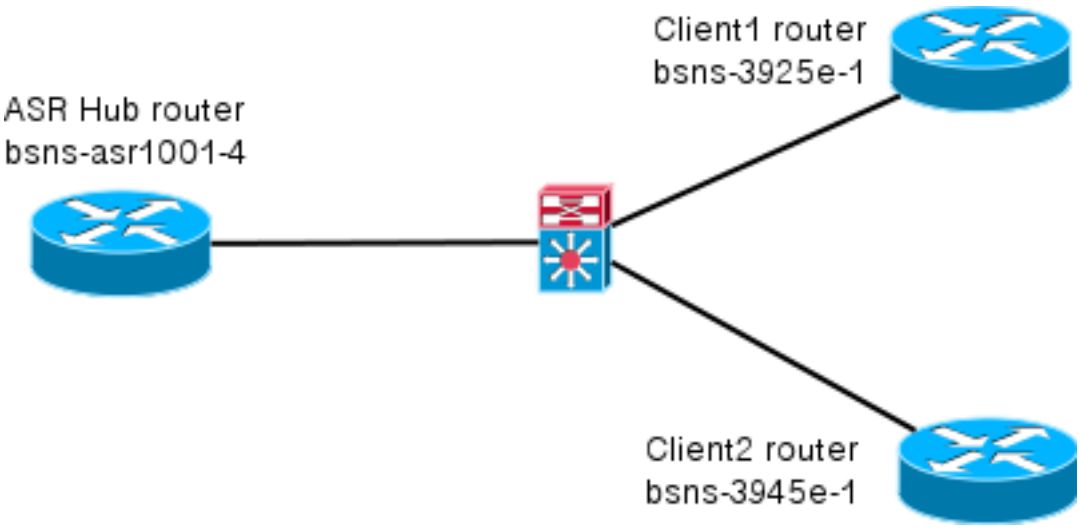
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

拓撲

本練習中使用的拓撲是基本的。使用一台中心路由器(ASR)和兩個分支路由器(ISR)，它們模擬客戶端。



組態

本文中的設定旨在顯示基本設定，並儘可能使用智慧型預設值。有關思科密碼學的建議，請訪問cisco.com上的下一代加密頁面。

分支配置

如前所述，本文檔中的大多數操作都是在中心上執行的。分支配置供參考。請注意，在此配置中，只有在Client1和Client2之間更改identity（以粗體顯示）。

```
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
```

集線器配置

集線器配置分為兩部分：

1. **基本連線配**置，其中概述了基本連線所需的配置。
2. **擴展配**置，它概述了管理員如何使用AAA屬性清單執行每個使用者或每個會話的配置更改所需的配置更改。

基本連線配置

此配置僅供參考，不是最佳配置，只是功能配置。

此組態的最大限制是使用預共用金鑰(PSK)作為驗證方法。思科建議在適用時使用憑證。

```
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
```

擴展配置

為特定會話分配AAA屬性需要做幾件事。此範例顯示client1的完整工作；然後顯示如何新增另一個

使用者端/使用者。

Client1的擴展集線器配置

1. 定義AAA屬性清單。
   ```
   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：請記住，通過屬性分配的實體必須存在於本地。在本例中，先前配置了**policy-map**。
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. 將AAA屬性清單分配給授**權策略。**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. 請確保連線的客戶端使用此新策略。在這種情況下，提取客戶端傳送的身份的**username**部分。使用者端應使用ClientX@cisco.com的電子郵件地址（X為1或2，視使用者端而定）。 **管理員**將電子郵件地址拆分為使用者名稱和域部分，並且僅使用其中一個（本例中為使用者名稱）來選擇授權策略的名稱。
   ```
   crypto ikev2 name-mangler GET_NAME
    email username

   crypto ikev2 profile Flex_IKEv2
    aaa authorization group psk list default name-mangler GET_NAME
   ```
   當client1正常運行時，可以相對輕鬆地新增client2。

Client2的擴展集線器配置

如果需要，請確儲存在策略和單獨的屬性集。

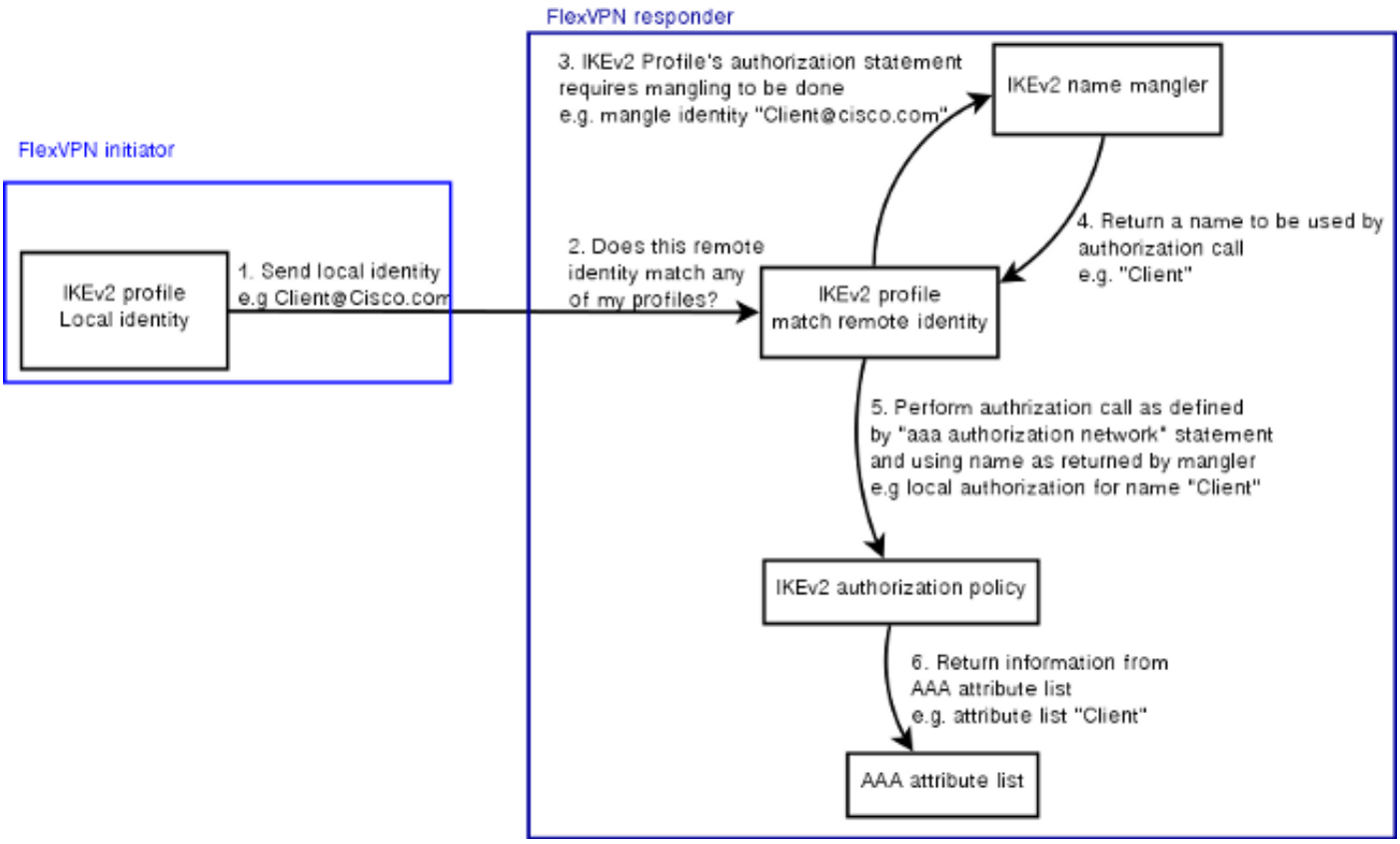
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

在此範例中，會套用已更新的最大區段大小(MSS)設定和傳入存取清單，以便為此使用者端操作。可以輕鬆選擇其他設定。典型的設定是為不同的客戶端分配不同的虛擬路由和轉發(VRF)。如前所述，配置中必須已經存在分配給屬性清單的任何實體，如本場景中的訪問清單133。

流程概述

下圖概述了通過網際網路金鑰交換版本2(IKEv2)配置檔案處理AAA授權時的操作順序，並包含特定於此配置示例的資訊。



驗證

本節介紹如何驗證以前分配的設定是否已應用到客戶端。

客戶端1

以下是用於驗證是否已應用最大傳輸單位(MTU)設定的命令，以及服務策略。

```
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
```

客戶端2

以下是用於驗證是否已推送MSS設定以及存取清單133是否也作為傳入過濾器應用於等同虛擬存取介面的命令。

```
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
(...)
```

調試

有兩個主要區塊需要調試。這在您需要建立TAC案例並更快地使事情步入正軌時非常有用。

調試IKEv2

從以下主要偵錯指令開始：

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

然後輸入以下命令：

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

調試AAA屬性分配

如果要調試AAA屬性分配，這些調試可能會很有用。

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

結論

本文檔演示了如何使用AAA屬性清單，以便在RADIUS伺服器可能不可用或不需要的FlexVPN部署中增加靈活性。如果需要的話，AAA屬性清單將以每個會話、每個組為單位提供新增的配置選項。

相關資訊

- FlexVPN和Internet金鑰交換版本2配置指南，Cisco IOS版本15M&T
- 遠端驗證撥入使用者服務(RADIUS)
- 要求建議 (RFC)
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems