로컬 AAA 특성 목록이 있는 FlexVPN 동적 구성

목차

소개

이 컨피그레이션 예에서는 외부 RADIUS(Remote Authentication Dial-In User Service) 서버를 사용하지 않고 동적 및 잠재적으로 고급 컨피그레이션을 수행하기 위해 로컬 AAA(Authentication, Authorization, and Accounting) 특성 목록을 사용하는 방법을 보여 줍니다.

이는 특정 시나리오에서 특히 신속한 구축 또는 테스트가 필요한 경우에 필요합니다. 이러한 구축은 일반적으로 개념 증명 랩, 새로운 구축 테스트 또는 문제 해결입니다.

동적 구성은 사용자별, 고객별, 세션별로 서로 다른 정책 또는 특성을 적용해야 하는 Concentrator/Hub 측면에서 중요합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 하며 이에 국한되지 않습니다. 이 목록은 최소 요구 사항을 요약하지는 않지만 이 기능의 테스트 단계 전반에 걸쳐 디바이스의 상태를 반영합니다.

하드웨어

- ASR(Aggregation Services Router) - ASR 1001 - "bsns-asr1001-4"라고 함
- ISR G2(Integrated Services Router Generation 2) - 3925e - "bsns-3925e-1"이라고 함
- ISR G2(Integrated Services Router Generation 2) - 3945e - "bsns-3945e-1"이라고 함

소프트웨어

- Cisco IOS XE 릴리스 3.8 - 15.3(1)S
- Cisco IOS® 소프트웨어 릴리스 15.2(4)M1 및 15.2(4)M2

라이센스

- ASR 라우터에는 **adventerprise** 및 **ipsec** 기능 라이센스가 활성화되어 있습니다.
- ISR G2 라우터에는 ipbasek **9**, **securityk9** 및 hseck9 기능 라이센스가 활성화되어 있습니다.

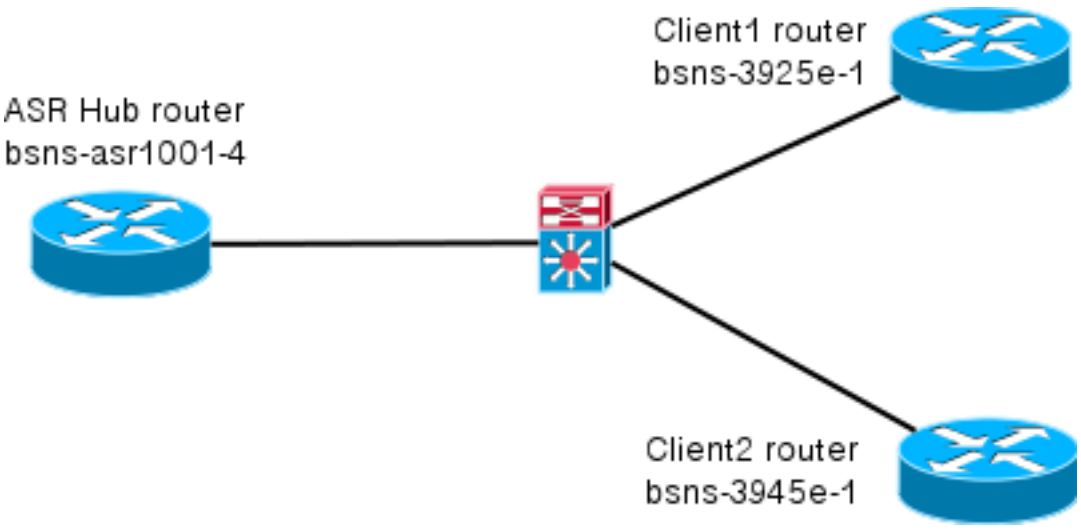
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

토폴로지

이 연습에서 사용되는 토폴로지는 기본입니다. 클라이언트를 시뮬레이션하는 허브 라우터(ASR) 및 ISR(스포크 라우터) 2개가 사용됩니다.



구성

이 문서의 컨피그레이션은 스마트 기본값과 함께 가능한 한 기본 설정을 표시하기 위한 것입니다. 암호화에 대한 Cisco 권장 사항은 cisco.com의 Next Generation Encryption 페이지를 참조하십시오 .

스포크 구성

앞서 언급한 대로 이 설명서의 대부분의 작업은 허브에서 수행됩니다. 스포크 컨피그레이션은 참조용으로 여기에 있습니다. 이 컨피그레이션에서는 Client1과 Client2 사이의 ID만 변경된다는 점에 유의하십시오(굵게 표시됨).

```
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
```

허브 구성

허브 컨피그레이션은 다음 두 부분으로 구성됩니다.

1. **기본 연결 구성** - 기본 연결에 필요한 구성을 간략하게 설명합니다.
2. **확장 구성** - 관리자가 AAA 특성 목록을 사용하여 사용자별 또는 세션별 컨피그레이션 변경을 수행하는 방법을 보여 주는 데 필요한 컨피그레이션 변경 사항을 간략하게 설명합니다.

기본 연결 구성

이 컨피그레이션은 참조용으로만 사용되며 최적화되어 있지 않고 기능만 가능합니다.

이 컨피그레이션의 가장 큰 제한은 인증 방법으로 PSK(pre-shared key)를 사용하는 것입니다. Cisco는 해당되는 경우 언제든지 인증서 사용을 권장합니다.

```
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
```

확장 구성

특정 세션에 AAA 특성을 할당하는 데 필요한 몇 가지 사항이 있습니다. 이 예에서는 client1에 대한 전체 작업을 보여 줍니다. 다른 클라이언트/사용자를 추가하는 방법을 보여 줍니다.

클라이언트1에 대한 확장 허브 구성

1. AAA 특성 목록을 정의합니다.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   참고: 속성을 통해 지정된 엔티티는 로컬에 있어야 합니다. 이 경우 **정책 맵이** 이전에 구성되었습니다.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. **권한 부여 정책**에 AAA 특성 목록을 **할당합니다.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. 연결하는 클라이언트에서 이 새 정책을 사용해야 합니다. 이 경우 클라이언트에서 보낸 ID의 **사용자 이름** 부분을 추출합니다. 클라이언트는 ClientX@cisco.com의 이메일 주소를 사용해야 합니다(X는 클라이언트에 따라 1 또는 2). 관리자는 이메일 주소를 사용자 이름 및 도메인 부분으로 분할하고 그중 하나만(이 경우 사용자 이름)사용하여 권한 부여 정책의 이름을 선택합니다.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username

   crypto ikev2 profile Flex_IKEv2
    aaa authorization group psk list default name-mangler GET_NAME
   ```
   client1이 작동하면 client2를 비교적 쉽게 추가할 수 있습니다.

클라이언트2의 확장 허브 구성

필요한 경우 정책과 별도의 특성 집합이 있어야 합니다.

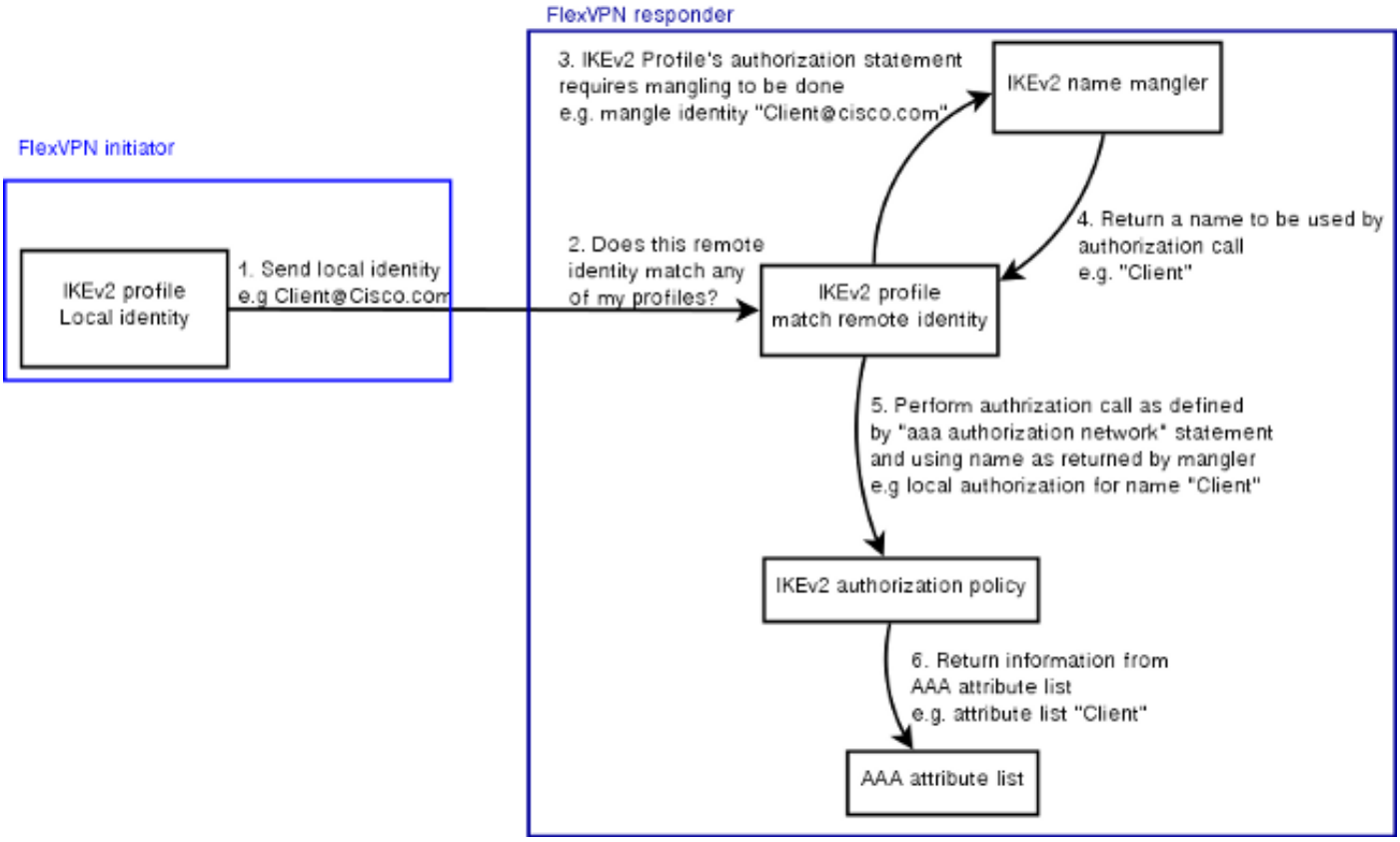
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

이 예에서는 이 클라이언트에 대해 작동할 업데이트된 MSS(Maximum Segment Size) 설정과 인바운드 액세스 목록이 적용됩니다. 다른 설정은 쉽게 선택할 수 있습니다. 일반적인 설정은 여러 클라이언트에 대해 서로 다른 VRF(가상 라우팅 및 전달)를 할당하는 것입니다. 앞에서 설명한 것처럼 이 시나리오의 access-list 133과 같이 특성 목록에 할당된 모든 엔터티가 컨피그레이션에 이미 있어야 합니다.

프로세스 개요

이 그림은 IKEv2(Internet Key Exchange version 2) 프로파일을 통해 AAA 권한 부여가 처리되는 경우의 작동 순서를 간략하게 설명하고 이 구성 예와 관련된 정보를 포함합니다.



확인

이 섹션에서는 이전에 할당된 설정이 클라이언트에 적용되었는지 확인하는 방법을 보여줍니다.

클라이언트1

다음은 MTU(Maximum Transmission Unit) 설정과 서비스 정책이 적용되었는지 확인하는 명령입니다.

```
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
```

클라이언트2

다음은 MSS 설정이 푸시되었고 access-list 133이 동일한 가상 액세스 인터페이스에서 인바운드 필터로 적용되었는지 확인하는 명령입니다.

```
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
(...)
```

디버그

디버깅할 주요 블록은 두 가지입니다. 이 기능은 TAC 케이스를 열고 더 신속하게 업무를 진행해야 하는 경우에 유용합니다.

디버그 IKEv2

다음 주 debug 명령으로 시작합니다.

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

그런 다음 다음 명령을 입력합니다.

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

디버그 AAA 특성 할당

특성의 AAA 할당을 디버깅하려는 경우 이러한 디버그가 유용할 수 있습니다.

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

결론

이 문서에서는 RADIUS 서버를 사용할 수 없거나 원하지 않는 FlexVPN 구축에서 유연성을 추가하기 위해 AAA 특성 목록을 사용하는 방법을 보여 줍니다. AAA 특성 목록은 필요한 경우 세션별로 그룹별로 추가 구성 옵션을 제공합니다.

관련 정보

- FlexVPN 및 Internet Key Exchange 버전 2 컨피그레이션 가이드, Cisco IOS 릴리스 15M&T
- 원격 인증 전화 접속 사용자 서비스(RADIUS)
- RFC(Request for Comments)
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems