FlexVPN dynamische configuratie met lokale AAA-kenmerken

Inhoud

Inleiding

Dit configuratievoorbeeld toont aan hoe u de lijst met lokale verificatie, autorisatie en accounting (AAA) kunt gebruiken om dynamische en mogelijk geavanceerde configuratie uit te voeren zonder het gebruik van externe Remote Authentication Dial-In User Service (RADIUS) server.

Dit is in bepaalde scenario's gewenst, vooral wanneer een snelle inzet of test vereist is. Zulke implementaties zijn typisch test-of-concept labs, nieuwe implementatietests of probleemoplossing.

Dynamische configuratie is belangrijk voor de concentrator/hub-zijde, waar verschillende beleidslijnen of eigenschappen moeten worden toegepast per gebruiker, per klant, per sessie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op, maar niet beperkt tot, deze software- en hardwareversies. In deze lijst worden de minimumvereisten niet aangegeven, maar wordt de stand van de voorziening gedurende de testfase van deze functie weergegeven.

Hardware

- Aggregation Services Routers (ASR) - ASR 1001 - genaamd "bsns-asr1001-4"
- Generation 2 (ISR G2) - 3925e - met de naam "bsns-3925e-1" voor geïntegreerde services routers
- Generation 2 (ISR G2) - 3945e - met de naam "bsns-3945e-1" voor geïntegreerde services routers

in Cisco IOS®-software

- Cisco IOS XE release 3.8 - 15.3(1)S
- Cisco IOS®-softwarerelease 15.2(4)M1 en 15.2(4)M2

Licenties

- ASR-routers hebben de licenties voor **geavanceerde** en **IPsec**-functies ingeschakeld.
- ISR G2-routers hebben de licenties voor eigenschappen **ipbasek9**, **security9** en seck9 ingeschakeld.

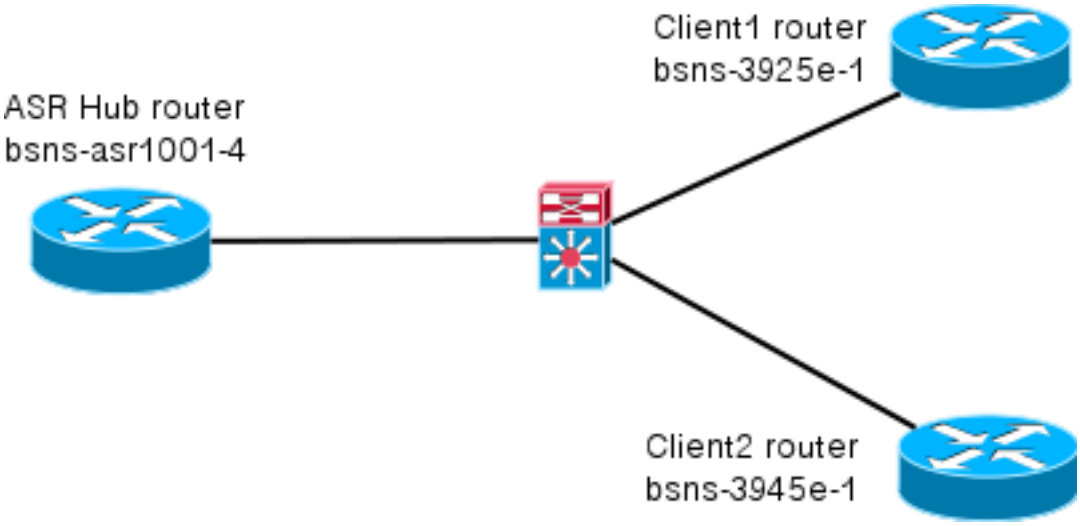
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Topologie

De topologie die in deze oefening wordt gebruikt is van fundamenteel belang. Er wordt een hub router (ASR) en twee SPD-routers (ISR) gebruikt, die klanten simuleren.



Configuraties

De configuraties in dit document zijn bedoeld om een basisinstellingen weer te geven, met zo veel mogelijk slimme standaardinstellingen. Ga voor Cisco-aanbevelingen over cryptografie naar de pagina Encryptie van de volgende generatie op cisco.com.

Spoelconfiguratie

Zoals eerder vermeld, worden de meeste acties in deze documentatie uitgevoerd op de hub. De woordconfiguratie is hier ter referentie. Merk in deze configuratie op dat alleen verandering de identiteit is tussen Client1 en Client2 (vet weergegeven).

```
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
```

Hub-configuratie

De configuratie van de hub is verdeeld in twee delen:

1. **Basisconfiguratie**, die de configuratie beschrijft die nodig is voor basisconnectiviteit.
2. **Uitgebreide configuratie**, die de configuratieveranderingen weergeeft die nodig zijn om aan te tonen hoe een beheerder de AAA-attributenlijst kan gebruiken om configuratiewijzigingen per gebruiker of per sessie uit te voeren.

Configuratie van basisverbindingen

Deze configuratie is uitsluitend bedoeld voor referentie en is niet bedoeld als optimaal, maar slechts functioneel.

De grootste beperking van deze configuratie is het gebruik van vooraf gedeelde sleutel (PSK) als de authenticatiemethode. Cisco raadt het gebruik van certificaten aan wanneer van toepassing.

```
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
```

Uitgebreide configuratie

Er zijn een paar dingen nodig om AAA-eigenschappen aan een bepaalde sessie toe te wijzen. Dit voorbeeld toont volledig werk voor cliënt1; dan toont het hoe een andere client/gebruiker toe te voegen.

Extended Hub Configuration voor Client1

1. Defineert een lijst van AAA-kenmerken.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Opmerking: Onthoud dat de entiteit die via eigenschappen wordt toegewezen lokaal moet bestaan. In dit geval werd **de beleidsmatige kaart** eerder geconfigureerd.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Toewijzen van een lijst van kenmerken van de AAA aan een **vergunningbeleid.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Zorg ervoor dat dit nieuwe beleid wordt gebruikt door de klanten die verbinding maken. In dit geval, haal het **gebruikersnaam** deel van de identiteit dat door de cliënten wordt verstuurd. De klanten zouden een e-mailadres van ClientX@cisco.com (X is 1 of 2, afhankelijk van de cliënt) moeten gebruiken. De **manager** splitst het e-mailadres in een gebruikersnaam- en domeingedeelte en gebruikt er slechts één (in dit geval een gebruikersnaam) om de naam van het vergunningsbeleid te kiezen.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username

   crypto ikev2 profile Flex_IKEv2
   ```

```
aaa authorization group psk list default name-mangler GET_NAME
```

Wanneer client1 operationeel is, kan client2 relatief gemakkelijk worden toegevoegd.

Extended Hub Configuration voor Client2

Zorg ervoor dat er een beleid en indien nodig een aparte reeks eigenschappen bestaan.

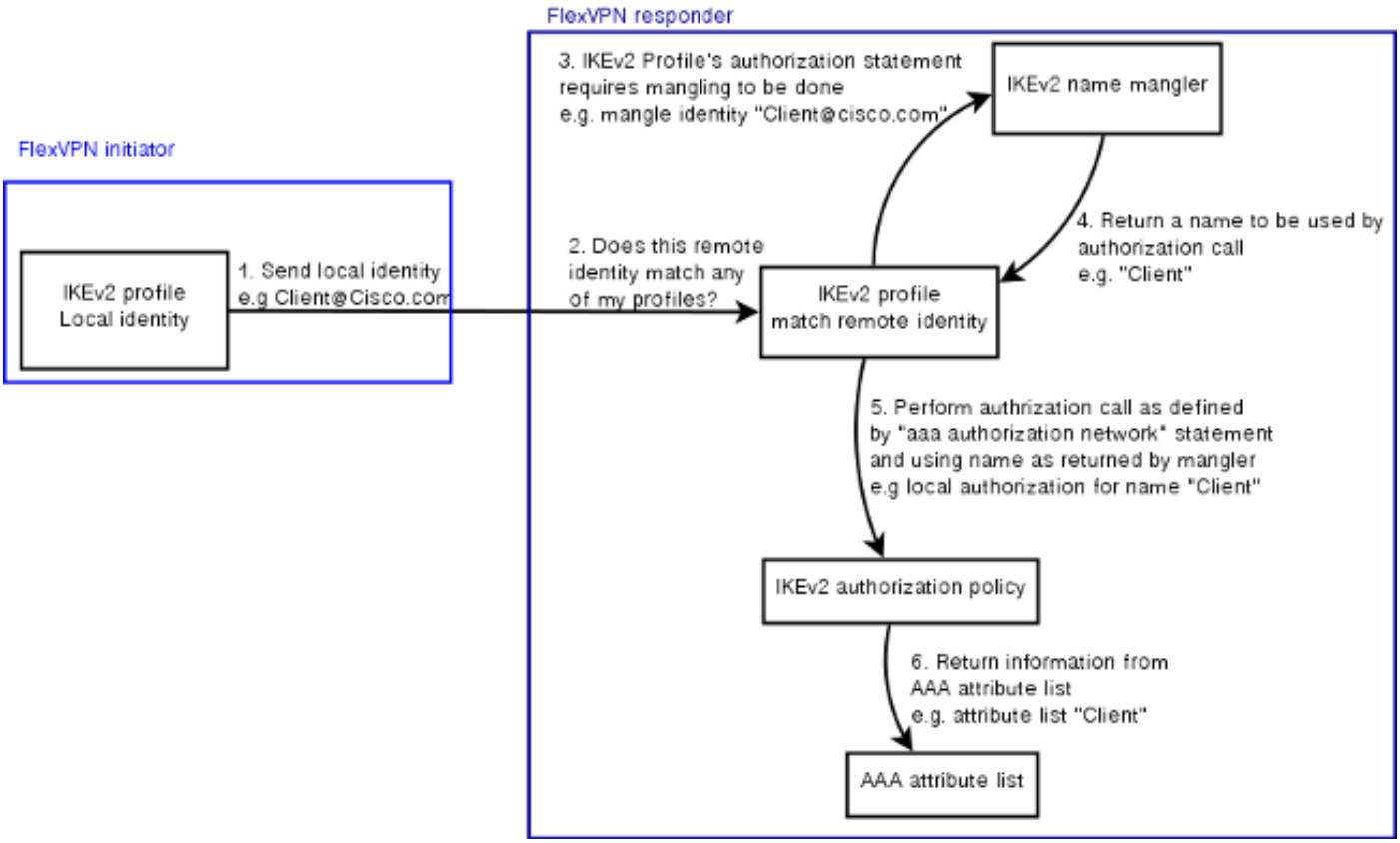
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

In dit voorbeeld wordt een bijgewerkte maximum segmentgrootte (MSS) instelling en een inkomende toegangslijst om voor deze client te opereren toegepast. Andere instellingen kunnen eenvoudig worden gekozen. Een standaardinstelling is om verschillende virtuele routing en Forwarding (VRF) aan verschillende klanten toe te wijzen. Zoals eerder vermeld, moet elke aan de lijst van eigenschappen toegewezen entiteit, zoals toegangslijst 133 in dit scenario, reeds in de configuratie bestaan.

Overzicht van processen

Dit cijfer schetst de volgorde waarin de AAA-vergunning wordt verwerkt via het IKEv2-profiel (Internet Key Exchange, versie 2) en bevat informatie die specifiek is voor dit configuratievoorbeeld.



Verificatie

Deze paragraaf laat zien hoe te verifiëren dat de eerder toegewezen instellingen op de cliënten zijn toegepast.

Clientclient1

Hier zijn de opdrachten die controleren of de maximale instellingen voor transmissie-eenheden (MTU's) en het dienstverleningsbeleid zijn toegepast.

```
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
```

Cliënt2

Hier zijn de opdrachten die controleren of de MSS-instellingen zijn geduwd en dat de toegangslijst 133 ook is toegepast als een inkomende filter in de equivalente virtuele toegangsinterface.

```
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
(...)
```

Debuggen

Er zijn twee belangrijke blokken om te zuiveren. Dit is handig als u een TAC-case wilt openen en de zaken sneller op schema wilt krijgen.

Debug IKEv2

Begin met deze belangrijke debug opdracht:

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

Voer vervolgens deze opdrachten in:

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

Toewijzing van AAA-kenmerken debug

Als u AAA-toewijzing van eigenschappen wilt debug, kunnen deze debugs behulpzaam zijn.

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

Conclusie

Dit document toont aan hoe de AAA-attributenlijst te gebruiken om extra flexibiliteit in FlexVPN-implementaties toe te staan waar de RADIUS-server mogelijk niet beschikbaar of niet gewenst is. De AAA-attributenlijst biedt indien nodig toegevoegde configuratieopties per sessie, per groep.

Gerelateerde informatie

- Configuratie-gids voor FlexVPN en Internet Key Exchange, versie 2, Cisco IOS release 15M&T
- Inbel-in-gebruikersservices (RADIUS)
- Verzoeken om opmerkingen (RFC's)

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems