IOS per VRF-probleemoplossing

Inhoud

Inleiding

RADIUS wordt sterk gebruikt als het authenticatieprotocol om gebruikers voor netwerktoegang te authentiseren. Meer beheerders segregeren hun beheerverkeer met VPN Routing en Forwarding (VRF). Door standaard gebruikt Verificatie, autorisatie en accounting (AAA) op IOS de standaard routingtabel om pakketten te verzenden. Deze handleiding beschrijft hoe u RADIUS kunt configureren en problemen oplossen wanneer de RADIUS-server in een VRF staat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- RADIUS
- VRF
- AAA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Functieinformatie

In wezen is een VRF een virtuele routingtabel op het apparaat. Wanneer IOS een routebesluit neemt, als de eigenschap of de interface een VRF gebruikt, worden de routeringsbesluiten genomen tegen die VRF-routingtabel. Anders gebruikt de functie de globale routingtabel. In deze geest, is hier hoe u RADIUS configureren om een VRF te gebruiken:

```
version 15.2
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vrfAAA
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa group server radius management
 server-private 192.0.2.4 key cisco
 server-private 192.0.2.5 key cisco
 ip vrf forwarding blue
 ip radius source-interface GigabitEthernet0/0
!
aaa authentication login default group management local
aaa authorization exec default group management if-authenticated
aaa accounting exec default start-stop group management
!
aaa session-id common
!
no ipv6 cef
!
ip vrf blue
!
no ip domain lookup
ip cef
!
interface GigabitEthernet0/0
 ip vrf forwarding blue
 ip address 203.0.113.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
```

```
ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1
!
line con 0
line aux 0
line vty 0 4
 transport input all
```

Zoals u kunt zien, zijn er geen wereldwijd gedefinieerde RADIUS-servers. Als u de servers naar een VRF migreert, kunt u de wereldwijd geconfigureerd RADIUS-servers veilig verwijderen.

Methode voor probleemoplossing

Voer de volgende stappen uit:

1. Zorg ervoor dat u de juiste IPVRF-verzenddefinitie onder uw AAA groepsserver evenals de broninterface voor het RADIUS-verkeer hebt.
2. Controleer uw VRF-routingtabel en controleer of er een route naar uw RADIUS-server is. We zullen het bovenstaande voorbeeld gebruiken om de VRF-routingtabel weer te geven:

```
vrfAAA#show ip route vrf blue

Routing Table: blue
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      203.0.113.0/8 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet0/0
L        203.0.113.2/32 is directly connected, GigabitEthernet0/0
```

3. Kunt u uw RADIUS-server pingelen? Bedenk dat dit ook VRF-specifiek moet zijn:

```
vrfAAA#ping vrf blue 192.0.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

4. U kunt de opdracht **Test Aa** gebruiken om de connectiviteit te verifiëren (u moet de nieuwe-code optie aan het eind gebruiken; " de erfenis zal niet werken " :

```
vrfAAA#test aaa group management cisco Cisco123 new-code
User successfully authenticated

USER ATTRIBUTES

username             "cisco"
```

Als de routes zijn opgezet en u geen hits op uw RADIUS-server ziet, zorg er dan voor dat ACL's udp-poort 1645/1646 of udp-poort 1812/1813 mogelijk maken om de server vanaf de router of switch te bereiken. Als u een authenticatiefout hebt, geeft u RADIUS als normaal problemen op. De optie VRF is alleen bestemd voor de routing van het pakket.

Gegevensanalyse

Als alles correct lijkt, kunnen **a** en **Straal debug** opdrachten worden ingeschakeld om het probleem op te lossen. Start met deze **debug-**opdrachten:

- **straal deken**
- **debug van verificatie**

Hier is een voorbeeld van een **debug** waar iets niet goed is ingesteld, zoals maar niet beperkt tot:

- Ontbrekende RADIUS-broninterface
- Ontbrekende IP VRF-verzendopdrachten onder de broninterface of onder de AAA-groepsserver
- Geen route naar de RADIUS-server in de VRF-routingtabel

```
Aug  1 13:39:28.571: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'
Aug  1 13:39:28.571: RADIUS/ENCODE(00000000):Orig. component type = Invalid
Aug  1 13:39:28.571: RADIUS/ENCODE(00000000): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
Aug  1 13:39:28.571: RADIUS(00000000): Config NAS IP: 203.0.113.2
Aug  1 13:39:28.571: RADIUS(00000000): Config NAS IPv6: ::
Aug  1 13:39:28.571: RADIUS(00000000): sending
Aug  1 13:39:28.575: RADIUS(00000000): Send Access-Request to 192.0.2.4:1645
   id 1645/2, len 51
Aug  1 13:39:28.575: RADIUS:  authenticator 12 C8 65 2A C5 48 B8 1F -
   33 FA 38 59 9C 5F D3 3A
Aug  1 13:39:28.575: RADIUS:  User-Password       [2]   18  *
Aug  1 13:39:28.575: RADIUS:  User-Name           [1]   7   "cisco"
Aug  1 13:39:28.575: RADIUS:  NAS-IP-Address      [4]   6   203.0.113.2
Aug  1 13:39:28.575: RADIUS(00000000): Sending a IPv4 Radius Packet
Aug  1 13:39:28.575: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:32.959: RADIUS(00000000): Request timed out
Aug  1 13:39:32.959: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:32.959: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:37.823: RADIUS(00000000): Request timed out
Aug  1 13:39:37.823: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:37.823: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:42.199: RADIUS(00000000): Request timed out
Aug  1 13:39:42.199: RADIUS: Retransmit to (192.0.2.4:1645,1646) for id 1645/2
Aug  1 13:39:42.199: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:47.127: RADIUS(00000000): Request timed out
Aug  1 13:39:47.127: RADIUS: Fail-over to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:47.127: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:51.927: RADIUS(00000000): Request timed out
Aug  1 13:39:51.927: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:51.927: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:39:56.663: RADIUS(00000000): Request timed out
Aug  1 13:39:56.663: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:39:56.663: RADIUS(00000000): Started 5 sec timeout
Aug  1 13:40:01.527: RADIUS(00000000): Request timed out
Aug  1 13:40:01.527: RADIUS: Retransmit to (192.0.2.5:1645,1646) for id 1645/2
Aug  1 13:40:01.527: RADIUS(00000000): Started 5 sec timeoutUser rejected
```

Helaas, met RADIUS is er geen onderscheid tussen een timeout en een ontbrekende route.

Hier is een voorbeeld van een succesvolle authenticatie:

```
Aug  1 13:35:51.791: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'

Aug  1 13:35:51.791: RADIUS/ENCODE(00000000):Orig. component type = Invalid
```

```
Aug  1 13:35:51.791: RADIUS/ENCODE(00000000): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off

Aug  1 13:35:51.791: RADIUS(00000000): Config NAS IP: 203.0.113.2

Aug  1 13:35:51.791: RADIUS(00000000): Config NAS IPv6: ::

Aug  1 13:35:51.791: RADIUS(00000000): sending

Aug  1 13:35:51.791: RADIUS(00000000): Send Access-Request to 192.0.2.4:1645 id
   1645/1, len 51

Aug  1 13:35:51.791: RADIUS:  authenticator F4 E3 00 93 3F B7 79 A9 -
   2B DC 89 18 8D B9 FF 16

Aug  1 13:35:51.791: RADIUS:  User-Password       [2]   18  *

Aug  1 13:35:51.791: RADIUS:  User-Name           [1]   7   "cisco"

Aug  1 13:35:51.791: RADIUS:  NAS-IP-Address      [4]   6   203.0.113.2

Aug  1 13:35:51.791: RADIUS(00000000): Sending a IPv4 Radius Packet

Aug  1 13:35:51.791: RADIUS(00000000): Started 5 sec timeout

Aug  1 13:35:51.799: RADIUS: Received from id 1645/1 14.36.142.31:1645,
   Access-Accept, len 62

Aug  1 13:35:51.799: RADIUS:  authenticator B0 0B AA FF B1 27 17 BD -
   3F AD 22 30 C6 03 5C 2D

Aug  1 13:35:51.799: RADIUS:  User-Name           [1]   7   "cisco"

Aug  1 13:35:51.799: RADIUS:  Class               [25]  35

Aug  1 13:35:51.799: RADIUS:   43 41 43 53 3A 6A 65 64 75 62 6F 69 73 2D 61 63
   [CACS:ACS1]

Aug  1 13:35:51.799: RADIUS:   73 2D 35 33 2F 31 33 32 34 35 33 37 33 35 2F 33
   [s-53/132453735/3]

Aug  1 13:35:51.799: RADIUS:   38                 [ 8]

Aug  1 13:35:51.799: RADIUS(00000000): Received from id 1645/1.
```

Vaak voorkomende problemen

- Het meest voorkomende probleem is dat van de configuratie. Vaak wordt de admin in de aaa groepsserver geplaatst maar werkt niet de aaa lijnen bij om naar de servergroep te wijzen. In plaats daarvan:
  ```
  aaa authentication login default group management local
  aaa authorization exec default group management if-authenticated
  aaa accounting exec default start-stop group management
  ```
  De admin heeft dit gedaan:
  ```
  aaa authentication login default grout radius local
  aaa authorization exec default group radius if-authenticated
  aaa accounting exec default start-stop group radius
  ```
  update de configuratie eenvoudig met de juiste servergroep.
- Een tweede algemeen probleem is dat een gebruiker deze fout ziet wanneer hij IP VRF wil toevoegen dat onder de servergroep wordt verzonden:

```
% Unknown command or computer name, or unable to find computer address
```

Dit betekent dat de opdracht niet gevonden is. Als u deze fout ziet, zorg dan dat de versie van IOS-ondersteuning per VRF-RADIUS verloopt.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems