VRF당 IOS RADIUS 문제 해결

목차

소개

RADIUS는 네트워크 액세스를 위해 사용자를 인증하기 위해 인증 프로토콜로 많이 사용됩니다.더 많은 관리자가 VPN 라우팅 및 포워딩(VRF)을 사용하여 관리 트래픽을 분리하고 있습니다. 기본적으로 IOS®의 AAA(Authentication, Authorization, and Accounting)는 패킷을 전송하기 위해 기본 라우팅 테이블을 사용합니다.이 설명서에서는 RADIUS 서버가 VRF에 있을 때 RADIUS를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS
- VRF
- AAA

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

기능 정보

기본적으로 VRF는 디바이스의 가상 라우팅 테이블입니다.IOS에서 라우팅 결정을 내릴 때 기능 또는 인터페이스에서 VRF를 사용하는 경우 해당 VRF 라우팅 테이블에 대해 라우팅 결정이 수행됩니다.그렇지 않으면 이 피쳐는 전역 라우팅 테이블을 사용합니다.이 점을 염두에 두고 VRF를 사용하도록 RADIUS를 구성하는 방법은 다음과 같습니다.

```
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
```

보시다시피, 전역적으로 정의된 RADIUS 서버가 없습니다.서버를 VRF로 마이그레이션하는 경우 전역으로 구성된 RADIUS 서버를 안전하게 제거할 수 있습니다.

문제 해결 방법론

다음 단계를 완료하십시오.

1. AAA 그룹 서버 및 RADIUS 트래픽에 대한 소스 인터페이스에 적절한 IPVRF 포워딩 정의가 있는지 확인합니다.
2. VRF 라우팅 테이블을 확인하고 RADIUS 서버에 대한 경로가 있는지 확인합니다.위의 예를 사용하여 VRF 라우팅 테이블을 표시하겠습니다.

```
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. RADIUS 서버를 ping할 수 있습니까?VRF에 따라 달라야 합니다.

```
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. **test aaa** 명령을 사용하여 연결을 확인할 수 있습니다(맨 끝에서 new-code 옵션을 사용해야 합니다.레거시 기능 없음:

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

USER ATTRIBUTES

username             "cisco"
```

경로가 제자리에 있고 RADIUS 서버에 적중 사항이 없는 경우 ACL에서 udp 포트 1645/1646 또는 udp 포트 1812/1813이 라우터 또는 스위치에서 서버에 연결되도록 허용하는지 확인하십시오.인증 오류가 발생하면 RADIUS를 정상적으로 트러블슈팅합니다.VRF 기능은 패킷의 라우팅에만 사용됩니다.

데이터 분석

모든 것이 올바른 경우 **aaa** 및 **radius debug** 명령을 활성화하여 문제를 해결할 수 있습니다.다음 **debug** 명령으로 시작합니다.

- **디버그 반경**
- **디버그 aaa 인증**

다음은 **디버그**의 예로서 올바르게 구성되지 않은 **예입니다**. 예를 들면 다음과 같습니다.

- RADIUS 소스 인터페이스 누락
- 소스 인터페이스 또는 AAA 그룹 서버 아래에 IP VRF 포워딩 명령이 없습니다.
- VRF 라우팅 테이블에 RADIUS 서버에 대한 경로가 없습니다.

```
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
```

그러나 RADIUS에서는 시간 초과와 누락된 경로 간에 차이가 없습니다.

다음은 성공적인 인증의 예입니다.

```
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.
```

일반적인 문제

- 가장 일반적인 문제는 구성의 문제입니다.관리자가 aaa 그룹 서버에 배치하지만 서버 그룹을 가리키도록 aaa 라인을 업데이트하지 않는 경우가 많습니다.대신
  ```
  aaa authentication login default group management local
  aaa authorization exec default group management if-authenticated
  aaa accounting exec default start-stop group management
  ```
  관리자가 다음을 입력했습니다.
  ```
  aaa authentication login default grout radius local
  aaa authorization exec default group radius if-authenticated
  aaa accounting exec default start-stop group radius
  ```
  올바른 서버 그룹으로 구성을 업데이트하기만 하면 됩니다.
- 두 번째 일반적인 문제는 서버 그룹 아래에 IP VRF 포워딩을 추가하려고 할 때 이 오류가 표시된다는 것입니다.
  ```
  % Unknown command or computer name, or unable to find computer address
  ```
  즉, 명령을 찾을 수 없습니다.이 오류가 표시되면 IOS 버전이 VRF RADIUS당 지원되는지 확인합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems