IOS Per VRF TACACS+ 트러블슈팅

목차

소개

TACACS+는 사용자를 네트워크 디바이스에 인증하는 인증 프로토콜로 많이 사용됩니다.점점 더 많은 관리자가 VPN 라우팅 및 포워딩(VRF)을 사용하여 관리 트래픽을 분리하고 있습니다. 기본적으로 IOS의 AAA는 기본 라우팅 테이블을 사용하여 패킷을 전송합니다.이 문서에서는 서버가 VRF에 있을 때 TACACS+를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- TACACS+
- VRF

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

기능 정보

기본적으로 VRF는 디바이스의 가상 라우팅 테이블입니다.기능 또는 인터페이스에서 VRF를 사용

하는 경우 IOS에서 라우팅 결정을 내릴 때 해당 VRF 라우팅 테이블에 대해 라우팅 결정이 수행됩니다.그렇지 않으면 이 피쳐는 전역 라우팅 테이블을 사용합니다.이 점을 염두에 두고 VRF를 사용하도록 TACACS+를 구성하는 방법은 다음과 같습니다(굵게 표시된 관련 컨피그레이션).

```
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 tacacs+ management
 server-private 192.0.2.4 key cisco
 server-private 192.0.2.5 key cisco
 ip vrf forwarding blue
 ip tacacs 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 전체적으로 정의된 TACACS+ 서버는 없습니다.서버를 VRF로 마이그레이션하는 경우 전역으로 구성된 TACACS+ 서버를 안전하게 제거할 수 있습니다.

문제 해결 방법론

1. TACACS+ 트래픽에 대한 소스 인터페이스와 aaa 그룹 서버 아래에 올바른 ip vrf 포워딩 정의가 있는지 확인합니다.
2. vrf 라우팅 테이블을 확인하고 TACACS+ 서버에 대한 경로가 있는지 확인합니다.위의 예는 vrf 라우팅 테이블을 표시하는 데 사용됩니다.

```
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
      203.0.0.0/24 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. TACACS+ 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 102.0.2.4, 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(마지막에 new-code 옵션을 사용해야 하며, 레거시가 작동하지 않음).

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

USER ATTRIBUTES

username             "cisco"
reply-message        "password: "
```

경로가 제자리에 있고 TACACS+ 서버에 적중 횟수가 표시되지 않는 경우 ACL에서 TCP 포트 49가 라우터 또는 스위치에서 서버에 연결되도록 허용하는지 확인하십시오.TACACS+를 정상적으로 트러블슈팅하는 데 인증 오류가 발생하는 경우 VRF 기능은 패킷의 라우팅에만 사용됩니다.

데이터 분석

위의 모든 내용이 올바르게 표시되면 aaa 및 tacacs 디버그를 사용하여 문제를 해결할 수 있습니다.다음 디버그로 시작:

- 디버그 tacacs
- 디버그 aaa 인증

다음 예는 올바르게 구성되지 않은 디버그(예: 그러나 다음으로 제한되지 않음)의 예입니다.

- TACACS+ 소스 인터페이스 누락
- 소스 인터페이스 또는 aaa 그룹 서버 아래에 ip vrf forwarding 명령이 없습니다.

- VRF 라우팅 테이블에서 TACACS+ 서버에 대한 경로가 없습니다.

```
Jul 30 20:23:16.399: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:23:16.399: TPLUS: processing authentication start request id 0
Jul 30 20:23:16.399: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:23:16.399: TPLUS: Using server 192.0.2.4
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
Jul 30 20:23:16.399: TPLUS: Choosing next server 192.0.2.5
Jul 30 20:23:16.399: TPLUS(00000000)/0: Connect Error No route to host
```

성공적인 연결은 다음과 같습니다.

```
Jul 30 20:54:29.091: AAA/AUTHEN/LOGIN (00000000): Pick method list 'default'
Jul 30 20:54:29.091: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.091: TPLUS: processing authentication start request id 0
Jul 30 20:54:29.091: TPLUS: Authentication start packet created for 0(cisco)
Jul 30 20:54:29.091: TPLUS: Using server 192.0.2.4
Jul 30 20:54:29.091: TPLUS(00000000)/0/NB_WAIT/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: socket event 2
Jul 30 20:54:29.095: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.095: TPLUS(00000000)/0/READ: Would block while reading
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.099: TPLUS(00000000)/0/READ: read entire 28 bytes response
Jul 30 20:54:29.099: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.099: TPLUS: Received authen response status GET_PASSWORD (8)
Jul 30 20:54:29.099: TPLUS: Queuing AAA Authentication request 0 for processing
Jul 30 20:54:29.099: TPLUS: processing authentication continue request id 0
Jul 30 20:54:29.099: TPLUS: Authentication continue packet generated for 0
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE/2B2DC1AC: Started 5 sec timeout
Jul 30 20:54:29.099: TPLUS(00000000)/0/WRITE: wrote entire 25 bytes request
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: socket event 1
Jul 30 20:54:29.103: TPLUS(00000000)/0/READ: read entire 18 bytes response
Jul 30 20:54:29.103: TPLUS(00000000)/0/2B2DC1AC: Processing the reply packet
Jul 30 20:54:29.103: TPLUS: Received authen response status PASS (2)
```

일반적인 문제

가장 일반적인 문제는 컨피그레이션입니다.관리자가 aaa group server에 배치하지만 서버 그룹을 가리키도록 aaa 라인을 업데이트하지 않습니다.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 tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```

올바른 서버 그룹으로 구성을 업데이트하기만 하면 됩니다.

두 번째 일반적인 문제는 서버 그룹 아래에 ip vrf 포워딩을 추가하려고 할 때 이 오류가 발생하는 것

입니다.

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

즉, 명령을 찾을 수 없습니다.이 경우 IOS 버전이 VRF TACACS+당 지원하는지 확인합니다.다음은 몇 가지 일반적인 최소 버전입니다.

- 12.3(7)T
- 12.2(33)SRA1
- 12.2(33)SXI
- 12.2(33)SXH4
- 12.2(54)SG

관련 정보

- 기술 지원 및 문서 – Cisco Systems