VRF TACACS+ ごとの IOS のトラブルシューティング

内容

概要

TACACS+は、ネットワークデバイスに対してユーザを認証するための認証プロトコルとして頻繁に使用されます。VPN Routing and Forwarding(VRF)を使用して管理トラフィックを分離する管理者が増えています。 デフォルトでは、IOSのAAAはパケットを送信するためにデフォルトのルーティングテーブルを使用します。このドキュメントでは、サーバがVRF内にある場合のTACACS+の設定とトラブルシューティングの方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- TACACS+
- VRF

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

機能情報

基本的に、VRFはデバイスの仮想ルーティングテーブルです。機能またはインターフェイスがVRFを使用している場合、IOSがルーティングを決定すると、そのVRFルーティングテーブルに対してルーティングの決定が行われます。これ以外の場合、機能はグローバル ルーティング テーブルを使用します。これを念頭に置いて、VRFを使用するようにTACACS+を設定する方法を次に示します（関連する設定は太字で示しています）。

```
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
```

このように、グローバルに定義されたTACACS+サーバはありません。サーバをVRFに移行する場合は、グローバルに設定されたTACACS+サーバを安全に削除できます。

トラブルシューティング手法

1. aaaグループサーバの下に、TACACS+トラフィックの送信元インターフェイスだけでなく、適切なip vrf転送定義があることを確認します。
2. vrfルーティングテーブルを確認し、TACACS+サーバへのルートがあることを確認します。上記の例は、vrfルーティングテーブルを表示するために使用されます。

```
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+サーバにpingを実行できますか。VRF固有である必要があります。

```
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 aa**aコマンドを使用して接続を確認できます（最後にnew-codeオプションを使用する必要があります。レガシーは機能しません）。

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

USER ATTRIBUTES

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

ルートが設定されていて、TACACS+サーバにヒットがない場合は、ACLがルータまたはスイッチからサーバに到達するためにTCPポート49を許可していることを確認します。認証障害が発生した場合は、通常どおりTACACS+をトラブルシューティングします。VRF機能は、パケットのルーティングのためのものです。

データ分析

上記のすべてが正しく表示される場合は、aaaおよびtacacsのデバッグをイネーブルにして、問題をトラブルシューティングできます。次のデバッグから開始します。

- debug tacacs
- aaa 認証のデバッグ

次に示すのは、何かが正しく設定されていない場合のデバッグの例です。たとえば、次のような場合です。

- TACACS+送信元インターフェイスがない
- 送信元インターフェイスまたは AAA グループ サーバに IP VRF 転送コマンドがない
- VRFルーティングテーブルにTACACS+サーバへのルートがない

```
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
```

正常な接続を次に示します。

```
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)
```

一般的な問題

最も一般的な問題は、設定です。多くの場合、管理者はaaaグループサーバを設定しますが、aaa回線がサーバグループをポイントするように更新しません。代わりに：

```
aaa authentication login default group management local
aaa authorization exec default group management if-authenticated
aaa accounting exec default start-stop group management
```

管理者は次のように入力します。

```
aaa authentication login default grout tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
```
正しいサーバ グループで設定を更新するだけです。

2つ目の一般的な問題は、サーバグループでip vrf forwardingを追加しようとすると、次のエラーが発生することです。

```
% Unknown command or computer name, or unable to find computer address
```
これはコマンドが見つからなかったことを意味します。この場合、IOSのバージョンがVRFごとのTACACS+をサポートしていることを確認します。次に、一般的な最小バージョンをいくつか示します。

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

関連情報

- テクニカル サポートとドキュメント – Cisco Systems