Содержание

Введение

TACACS + в большой степени используется в качестве протокола аутентификации для аутентификации пользователей на сетевых устройствах. Все больше администраторов выделяет свой трафик управления с помощью VPN Routing и Forwarding (VRF). По умолчанию AAA на IOS использует таблицу маршрутизации по умолчанию для передавания пакеты. Этот документ описывает, как настроить и устранить неполадки TACACS +, когда сервер находится в VRF.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- TACACS +
- VRF

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Информация о функциональной возможности

По существу VRF является таблицей виртуальной маршрутизации на устройстве. Когда IOS

делает решение о маршрутизации, если функция или интерфейс используют VRF, решения о маршрутизации сделаны против той таблицы маршрутизации VRF. В противном случае функция использует таблицу глобальной маршрутизации. С этим в памяти, вот то, как вы настраиваете TACACS + для использования VRF (соответствующая конфигурация полужирным):

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Как вы можете видеть нет никаких глобально определенных TACACS + серверы. При миграции серверов на VRF можно безопасно удалить глобально настроенный TACACS + серверы.

Методика устранения проблем

1. Удостоверьтесь, что у вас есть надлежащее определение ip vrf forwarding под вашим aaa group server, а также исходным интерфейсом для TACACS + трафик.
2. Проверьте свою таблицу маршрутизации VRF и удостоверьтесь, что существует маршрут к вашему TACACS + сервер. Приведенный выше пример используется для отображения таблицы маршрутизации VRF:`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all`
3. Можно ли пропинговать TACACS + сервер? Помните, что это должно быть VRF, определенным также:`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all`
4. Можно использовать **команду test aaa** для проверки подключения (необходимо использовать опцию нового кода в конце, наследство не работает):`version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0
0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Если маршруты существуют, и вы не видите соответствий на своем TACACS + сервер, удостоверьтесь, что ACL позволяют порту TCP 49 достигать сервера от маршрутизатора или коммутатора. Если вы получаете TACACS устранения неполадок ошибки проверки подлинности + как обычный, функция VRF только для маршрутизации пакета.

Анализ данных

Если всему выше корректных взглядов, aaa и отладки tacacs можно позволить решить проблему. Запустите с этих отладок:

- debug tacacs
- debug aaa authentication

Вот пример отладки, где что-то не настроено должным образом, такой как, но не ограничено:

- Недостающий TACACS + исходный интерфейс
- Недостающие команды ip vrf forwarding под исходным интерфейсом или под aaa group server
- Никакой маршрут к TACACS + сервер в таблице маршрутизации VRF

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Вот успешное подключение:

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime
msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line
aux 0line vty 0 4 transport input all
```

Типичные неполадки

Самая обычная проблема является конфигурацией. Много раз admin вставляет aaa group

server, но не обновляет линии aaa для обращения к группе серверов. Вместо:

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Admin вставит:

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Просто обновите конфигурацию с корректной группой серверов.

Вторая типичная проблема является пользователем, получает эту ошибку при попытке добавить ip vrf forwarding под группой серверов:

```
version 15.2service configservice timestamps debug datetime msecservice timestamps log datetime msecno service password-encryption!hostname vrfAAA!boot-start-markerboot-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 localaaa 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 lookupip 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 serverno ip http secure-server!ip route vrf blue 0.0.0.0 0.0.0.0 203.0.113.1!line con 0line aux 0line vty 0 4 transport input all
```

Это означает, что не была найдена команда. Если это происходит, удостоверяются, что версия IOS поддерживает TACACS на VRF +. Вот некоторые общие минимальные номера версии:

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

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация