Acceso del telnet/SSH de la configuración al dispositivo con los VRF

Contenido

Introducción

Este documento describe la configuración del acceso del dispositivo con Telnet o del Secure Shell (SSH) a través de un ruteo virtual y de una expedición (VRF).

Antecedentes

En las redes informáticas basadas en IP, el VRF es una tecnología que permite que las instancias múltiples de una tabla de ruteo coexistan dentro del mismo router al mismo tiempo. Porque los casos de la encaminamiento son independientes, el mismo o los IP Addresses que solapan se puede utilizar sin ningún conflicto con uno a. Se mejora la funcionalidad de la red porque los trayectos de red se pueden dividir en segmentos sin el requisito de los routeres múltiples.

El VRF se pudo implementar en un dispositivo de red por las tablas de ruteo distintas conocidas como bases de información de reenvío (FIB), uno por el caso de la encaminamiento. Alternativamente, un dispositivo de red puede tener la capacidad de configurar a diversos routeres virtuales, donde cada uno tiene su propia BOLA que no sea accesible a ningún otro caso del router virtual en el mismo dispositivo.

Telnet es un Application Layer Protocol usado en Internet o las redes de área local (LAN) para proporcionar una instalación de comunicación centrada en el texto interactiva bidireccional usando una conexión de terminal virtual. Los datos del usuario son en-banda entremezclada con la información de control de Telnet en una conexión de datos orientada byte de 8 bits sobre el Transmission Control Protocol (TCP).

SSH es un Network Protocol criptográfico para los servicios de red de funcionamiento con seguridad sobre una red insegura. La aplicación de ejemplo más conocida está para el registro remoto a los sistemas informáticos de los usuarios.

A menudo cuando estas Tecnologías se utilizan juntas, crean la confusión, especialmente cuando

usted intenta acceder remotamente un dispositivo a través de una interfaz que pertenezca a un caso no global VRF que rutea.

Este las guías de configuración utilizan Telnet como forma de Acceso de administración apenas para los propósitos ejemplares. El concepto puede ser extendido para el acceso de SSH también.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

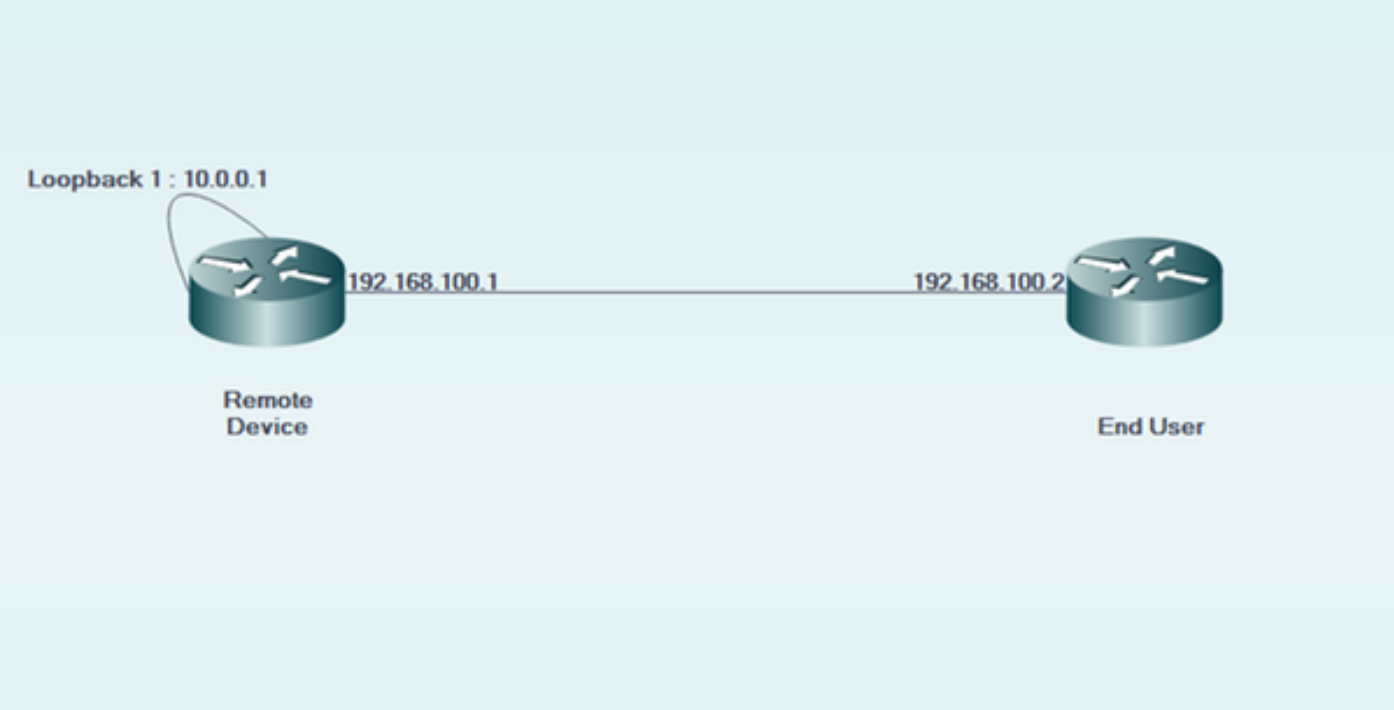
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

> **Note**: Comprensión básica de los VRF y de Telnet. El conocimiento del ACL también se recomienda. La configuración de los VRF se debe soportar en el dispositivo y la plataforma. Este documento se aplica a todos los routeres Cisco que funcionen con el Cisco IOS y a donde se soportan los VRF y los ACL.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está viva, aseegurese que usted entiende el impacto potencial del comando any.

Configurar

Diagrama de la red



Configuración

En el dispositivo remoto:

```
!
interface GigabitEthernet0/0
 description LINK TO END USER
 ip vrf forwarding MGMT
 ip address 192.168.100.1 255.255.255.252
 duplex auto
 speed auto
!


!
interface Loopback1
description LOOPBACK TO TELNET INTO FOR MANAGEMENT ACCESS ip vrf forwarding MGMT ip address
10.0.0.1 255.255.255.255 !

!
line vty 0 4
 access-class 8 in
 password cisco
 login
 transport input all
line vty 5 15
 access-class 8 in
 password cisco
 login
 transport input all
!
```

En el usuario final:

```
!
interface GigabitEthernet0/0
 description LINK TO REMOTE SITE
 ip vrf forwarding MGMT
 ip address 192.168.100.2 255.255.255.252
 duplex auto
 speed auto
!
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Antes del VRF-también la palabra clave se utiliza en la acceso-clase de configuración del line vty 0 15 del dispositivo remoto:

```
EndUser#ping vrf MGMT ip 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
EndUser#telnet 10.0.0.1 /vrf MGMT
Trying 10.0.0.1 ...
% Connection refused by remote host
```

Los golpes del paquete en el aumento del dispositivo remoto como ACE cuentan que corresponde los aumentos.

```
RemoteSite#show ip access-lists 8
Standard IP access list 8
    10 permit 192.168.100.2 log (3 matches)
```

Sin embargo, después de que la palabra clave VRF-también se agregue en la acceso-clase del line vty 0 15, se permite el acceso telnet.

Según el comportamiento definido, los dispositivos Cisco IOS validan todas las conexiones del VTY por abandono. Sin embargo, si se utiliza una acceso-clase, la suposición es que las conexiones deben llegar solamente del caso del IP global. Sin embargo, si hay un requisito y desea de permitir las conexiones de los casos VRF, utiliza la palabra clave VRF-también junto con la declaración correspondiente de la acceso-clase sobre configuración de línea.

```
!
line vty 0 4
 access-class 8 in vrf-also
 password cisco
 login
 transport input all
line vty 5 15
```

```
 access-class 8 in vrf-also
 password cisco
 login
 transport input all
!
```

```
EndUser#ping vrf MGMT ip 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
EndUser#telnet 10.0.0.1 /vrf MGMT
Trying 10.0.0.1 ... Open

User Access Verification

Password:
RemoteSite>
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

El troubleshooting basado VRF se pudo necesitar a veces. Asegúrese de que las interfaces afectadas sean todas en el mismo VRF y ellas tienen accesibilidad dentro del mismo VRF.

También, SSH relevante y el troubleshooting relacionado Telnet pudieron ser necesarios.