Configurar el acceso de Telnet o SSH al dispositivo con VRF

Contenido

Introducción

Este documento describe la configuración de acceso de los dispositivos con Telnet o Shell seguro (SSH) a través de un routing y reenvío virtual (VRF).

Antecedentes

En las redes de computadoras basadas en IP, el VRF es una tecnología que permite que coexistan varias instancias de una tabla de routing en el mismo router, al mismo tiempo. Debido a que las instancias de routing son independientes, pueden utilizarse direcciones IP iguales o que se superpongan sin ningún conflicto entre sí. Hay una mejora en la funcionalidad de la red, porque se pueden segmentar las rutas de red sin necesidad de que haya muchos routers.

VRF puede implementarse en un dispositivo de red mediante diferentes tablas de routing conocidas como bases de información de reenvío (FIB), una por cada instancia de routing. Como alternativa, un dispositivo de red puede tener la capacidad de configurar diferentes routers virtuales, donde cada uno tiene su propia FIB, a la que no puede acceder ninguna otra instancia de router virtual en el mismo dispositivo.

Telnet es un protocolo de capa de aplicaciones utilizado en Internet o en redes de área local (LAN) para proporcionar una instalación de comunicación bidireccional interactiva orientada al texto mediante una conexión de terminal virtual. Los datos de usuario se intercalan dentro de la banda con la información de control de Telnet en una conexión de datos orientada a bytes de 8 bits en el Protocolo de control de transmisión (TCP).

SSH es un protocolo de red cifrado para que los servicios de red funcionen de forma segura en una red no segura. La aplicación de ejemplo más conocida es el inicio de sesión remoto en los sistemas de computación por parte de los usuarios.

A menudo, cuando estas tecnologías se usan en conjunto, crean confusión, especialmente al

intentar acceder de forma remota a un dispositivo a través de una interfaz que pertenece a una instancia VRF de routing no global.

Estas guías de configuración utilizan Telnet como una forma de acceso a la administración solamente para brindar un ejemplo. El concepto también se puede ampliar para el acceso SSH.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

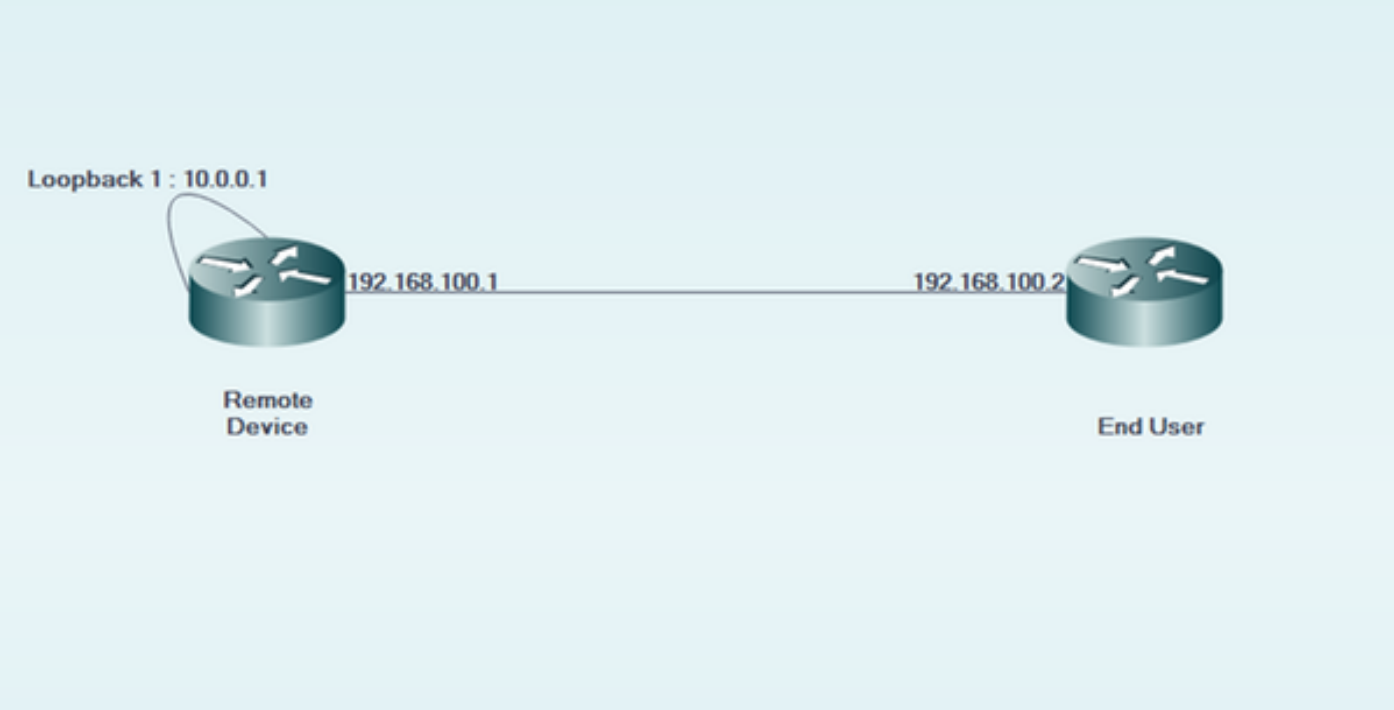
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

> Nota: Conocimientos básicos de VRF y Telnet. También se recomienda tener conocimientos de ACL. La configuración de VRF debe ser compatible con el dispositivo y la plataforma. Este documento es válido para todos los routers de Cisco que ejecutan CISCO IOS y que son compatibles con VRF y 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 se trata de una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

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 de usar la palabra clave vrf-also en la clase de acceso de las líneas vty de 0 a 15, configuración 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
```

Las llegadas del paquete al dispositivo remoto aumentan a medida que aumenta el recuento ACE correspondiente.

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

Sin embargo, después de agregar la palabra clave vrf-also en la clase de acceso de las líneas vty de 0 a 15, el acceso a telnet está permitido.

Según el comportamiento definido, los dispositivos de CISCO IOS aceptan todas las conexiones VTY de forma predeterminada. Sin embargo, si se utiliza una clase de acceso, se supone que las conexiones deben llegar solo desde la instancia IP global. Pero si hay un requisito y se desea permitir las conexiones de las instancias de VRF, utilice la palabra clave vrf-also junto con la instrucción de clase de acceso correspondiente en la configuración de la 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 brinda información que puede utilizar para la solución de problemas en su configuración.

A veces puede necesitarse la solución de problemas basada en VRF. Asegúrese de que las interfaces afectadas estén todas en el mismo VRF y que tengan disponibilidad dentro del mismo VRF.

Además, puede necesitarse la solución de problemas en relación con Telnet y el SSH relevante.