Configurer l'accès Telnet ou SSH au périphérique avec des VRF

Table des matières

Introduction

Ce document décrit la configuration de l'accès au périphérique avec Telnet ou Secure Shell (SSH) à travers une table de routage et de transfert virtuel (VRF).

Informations générales

Dans un réseau d'ordinateurs basé sur le protocole d'adressage IP, le VRF est une technologie qui permet la coexistence de multiples tables de routage dans un même routeur. Les instances de routage étant indépendantes, les mêmes adresses IP ou qui se chevauchent peuvent être utilisées sans conflit. La fonctionnalité du réseau est améliorée, car les chemins de réseau peuvent être segmentés sans devoir utiliser plusieurs routeurs.

Le VRF peut être mis en oeuvre dans un périphérique réseau par des tables de routage distinctes appelées FIB (Forwarding Information Bases), une par instance de routage. Un périphérique réseau peut également être en mesure de configurer différents routeurs virtuels, chacun d'entre eux possédant sa propre FIB qui n'est accessible à aucune autre instance de routeur virtuel sur le même périphérique.

Telnet est un protocole de couche application utilisé sur Internet ou sur les réseaux locaux (LAN) pour fournir une fonction de communication bidirectionnelle, interactive et textuelle qui utilise une connexion de terminal virtuel. Les données de l'utilisateur sont disséminées en mode intrabande avec l'information de contrôle Telnet codée dans une connexion de données de type octets de 8 bits à l'aide du protocole TCP (Transmission Control Protocol).

SSH est un protocole de réseau cryptographique permettant d'exploiter des services réseau en toute sécurité sur un réseau non sécurisé. L'exemple d'application le plus connu est la connexion

à distance aux systèmes informatiques par des utilisateurs.

Souvent, lorsque ces technologies sont utilisées ensemble, elles créent de la confusion. En particulier lorsque vous tentez d'accéder à distance à un périphérique via une interface qui appartient à une instance VRF de routage non globale.

Ce guide de configuration utilise Telnet comme une forme d’accès à la gestion à des fins explicatives. Le concept peut aussi être étendu aux accès SSH.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

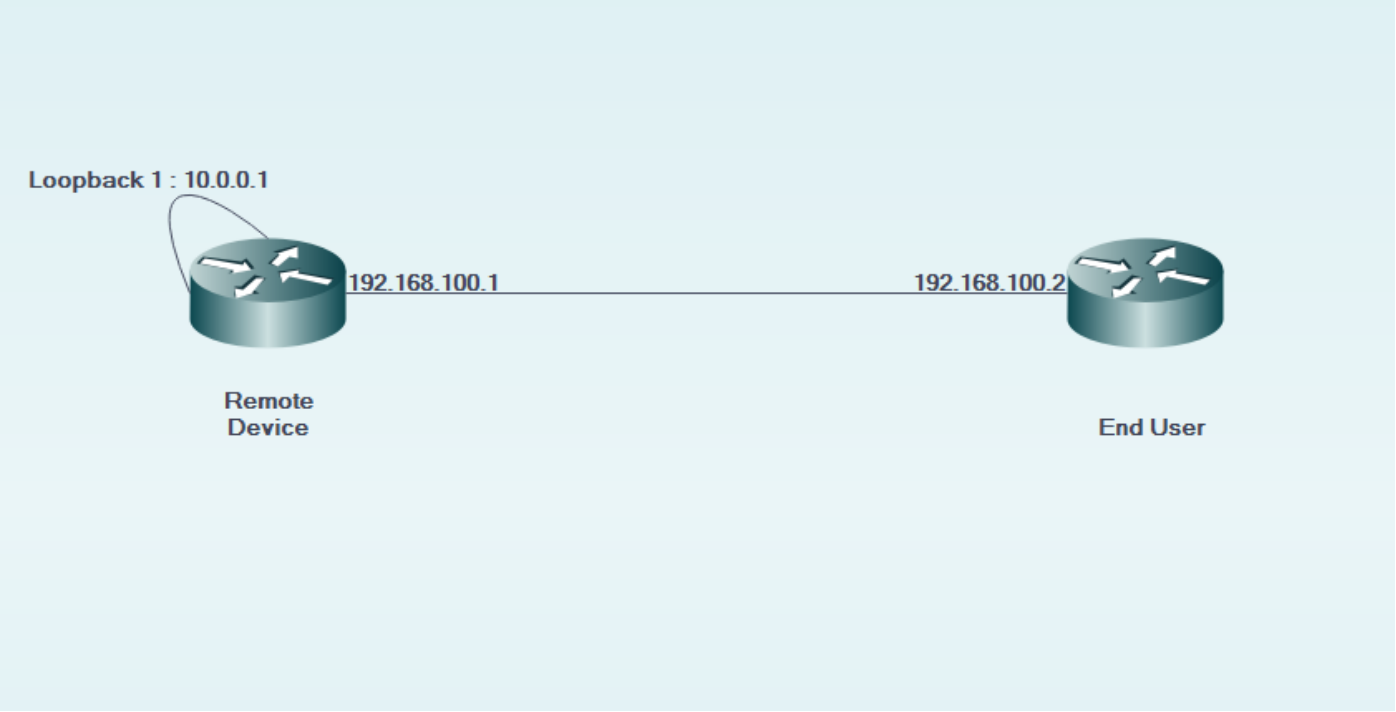
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Remarque : compréhension de base des VRF et de Telnet. Une connaissance de ACL est également recommandée. La configuration des VRF doit être prise en charge sur le périphérique et la plate-forme. Ce document s'applique à tous les routeurs Cisco qui exécutent Cisco IOS® et où les VRF et les ACL sont pris en charge.

Configurer

Diagramme du réseau



Configuration

Sur le périphérique distant :

```
!
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
!
```

Sur le périphérique de l'utilisateur 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
!
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Avant la vrf-also est utilisé dans la configuration access-class de la ligne vty 0 15 du périphérique distant :

```
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
```

Le flux de paquets augmente au niveau du périphérique à distance, tout comme le ACE correspondant.

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

Toutefois, après la vrf-also est ajouté dans la classe access de la ligne vty 0 15, l’accès telnet est autorisé.

Selon le comportement défini, les périphériques Cisco IOS acceptent toutes les connexions VTY par défaut. Cependant, si une access-class est utilisée, il est convenu que les connexions doivent parvenir seulement de l’instance IP globale. Toutefois, si vous devez et souhaitez autoriser les connexions à partir d'instances VRF, utilisez la vrf-also , ainsi que l'instruction access-class correspondante sur le
configuration de la ligne.

```
!
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>
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Un dépannage basé sur VRF peut parfois être nécessaire. Assurez-vous que les interfaces concernées sont toutes dans le même VRF et assurez-vous de leur accessibilité à l’intérieur du même VRF.

En outre, un dépannage SSH et Telnet approprié peut être nécessaire.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.