Configuration de l'authentification MD5 entre homologues BGP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Diagramme du réseau
- Configurations
- Comprendre les débogages

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit comment configurer l'authentification du message Digest5 (MD5) sur une connexion TCP entre deux pairs BGP.

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.

Les informations contenues dans ce document sont basées sur les résultats des commandes des routeurs de la gamme 3600 qui exécutent Cisco IOS® version 12.4(15)T14.

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.

Informations générales

Vous pouvez configurer l'authentification MD5 entre deux homologues BGP, ce qui signifie que chaque segment envoyé sur la connexion TCP entre les homologues est vérifié. L'authentification MD5 doit être configurée avec le même mot de passe sur les deux homologues BGP ; sinon, le lien entre elles ne peut pas être établi. Lorsque vous configurez l'authentification MD5, le logiciel Cisco IOS génère et vérifie l'empreinte MD5 de chaque segment envoyé sur la connexion TCP.

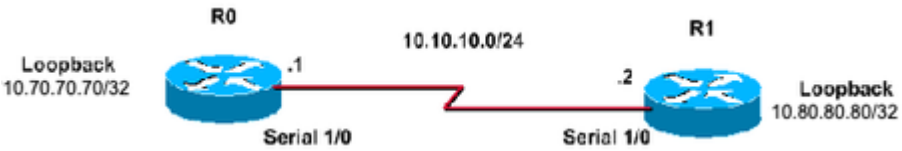
Configurer

Cette section contient les informations permettant de configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l'analyseur CLI Cisco pour obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés ont accès aux outils et informations internes de Cisco.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise ces configurations :

Configurations du routeur 0

<#root>

```
R0#

!
interface Loopback70
 ip address 10.70.70.70 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.1 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.80.80.80 remote-as 400



!--- iBGP Configuration using Loopback Address


 neighbor 10.80.80.80 password cisco



!--- Invoke MD5 authentication on a TCP connection to a BGP peer


 neighbor 10.80.80.80 update-source Loopback70
 no auto-summary
!
ip route 10.80.80.80 255.255.255.255 10.10.10.2


!--- This static route ensures that the remote peer address used for peering is reachable.
```

Configurations du routeur 1

<#root>

```
R1#

!
interface Loopback80
 ip address 10.80.80.80 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.2 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
```

```
 neighbor 10.70.70.70 remote-as 400

!--- iBGP Configuration using Loopback Address

 neighbor 10.70.70.70 password cisco

!--- Invoke MD5 authentication on a TCP connection to a BGP peer

 neighbor 10.70.70.70 update-source Loopback80
 no auto-summary
!
ip route 10.70.70.70 255.255.255.255 10.10.10.1

!--- This static route ensures that the remote peer address used for peering is reachable.
```

Comprendre les débogages

<#root>

```
R0#

clear ip bgp *
*Mar 1 01:02:17.523: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Down User reset
```

<#root>

```
R0#

debug ip bgp

BGP debugging is on for address family: IPv4 Unicast
*Mar  1 01:03:58.159: BGP: 10.80.80.80 open failed: Connection timed out; remote host not responding, o
*Mar  1 01:03:58.415: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 01:03:59.943: BGP: 10.80.80.80 open active, local address 10.70.70.70
*Mar  1 01:04:00.039: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:00.807: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(33358) to 10.70.70.70(179)
*Mar  1 01:04:01.991: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:01.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:05.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:06.015: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to 10.70.70.70(64444)
*Mar  1 01:04:29.947: BGP: 10.80.80.80 open failed: Connection timed out; remote host not responding, o
*Mar  1 01:04:33.879: BGP: 10.80.80.80 open active, local address 10.70.70.70
*Mar  1 01:04:33.983: BGP: 10.80.80.80 went from Active to OpenSent
```

```
*Mar  1 01:04:33.983: BGP: 10.80.80.80 sending OPEN, version 4, my as: 400, hold time 180 seconds
*Mar  1 01:04:33.987: BGP: 10.80.80.80 send message type 1, length (incl. header ) 45
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv message type 1, length (excl. header) 26
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN, version 4, holdtime 180 seconds
*Mar  1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN w/ OPTION parameter len: 16
*Mar  1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 6
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 1, length 4
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has MP_EXT CAP for afi/safi: 1/1
*Mar  1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
*Mar  1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 128, length 0
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(old) for all address-families
*Mar  1 01:04:34.099: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has CAPABILITY code: 2, length 0
*Mar  1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(new) for all address-families
*Mar  1 01:04:34.103: BGP: 10.80.80.80 went from OpenSent to OpenConfirm
*Mar  1 01:04:34.103: BGP: 10.80.80.80 went from OpenConfirm to Established
*Mar  1 01:04:34.103: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Up
```

Si un routeur a un mot de passe configuré pour un voisin, mais que le routeur voisin n'en a pas, un message tel que celui-ci s'affiche pendant que les routeurs tentent d'établir une session BGP entre eux :

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179
```

De même, si les deux routeurs ont des mots de passe différents configurés, un message tel que celui-ci s'affiche :

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- show ip bgp neighbors | inclure BGP

  <#root>

  R0#

  show ip bgp neighbors| include BGP

  BGP neighbor is 10.80.80.80

  ,

remote AS 400

, internal link
  BGP version 4, remote router ID 10.80.80.80

BGP state = Established

,

up for 00:08:26

  BGP table version 1, neighbor version 1/0

- show ip bgp summary

<#root>

R0#

show ip bgp summary

BGP router identifier 10.70.70.70, local AS number 400
BGP table version is 1, main routing table version 1

Neighbor   V   AS MsgRcvd MsgSent   TblVer InQ OutQ Up/Down State/PfxRcd

10.80.80.80 4 400 75 75 1 0 0 00:08:52 0

- show ip bgp summary

<#root>

R1#

show ip bgp summary

BGP router identifier 10.80.80.80, local AS number 400
BGP table version is 1, main routing table version 1

Neighbor   V   AS MsgRcvd MsgSent   TblVer InQ OutQ Up/Down State/PfxRcd

10.70.70.70 4 400 76 76 1 0 0 00:09:27 0

Dépannage

Il n'existe actuellement aucune information de dépannage pour cette configuration.

Informations connexes

- Routage IP Cisco IOS : Référence des commandes BGP
- Page IP Routing Support
- Assistance technique de Cisco et téléchargements

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.