Configure MD5 Authentication Between BGP Peers

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configurations
- Understand Debugs

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure Message Digest5 (MD5) authentication on a TCP connection between two BGP peers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document is based on command outputs from the 3600 Series Routers that run 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

You can configure MD5 authentication between two BGP peers, and that means each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them cannot be made. When you configure MD5 authentication it causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

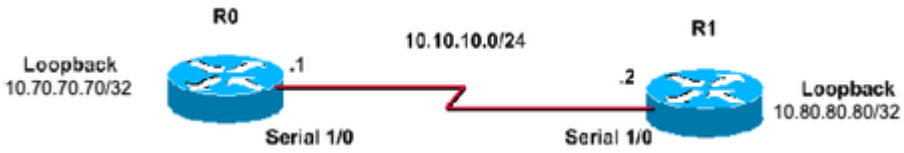
Configure

In this section is the information to configure the features described in this document.

Note: Use the Cisco CLI Analyzer to obtain more information on the commands used in this section. Only registered Cisco user have access to Cisco internal tools and information.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

Router 0 Configurations
<#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.
```

Router 1 Configurations

```
<#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.
```

Understand Debugs

<#root>

RO#

clear ip bgp *

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

<#root>

RO#

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 respondi
*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 respondi
*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-fami
*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-fami
*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
```

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as this is displayed while the routers attempt to establish a BGP session between them:

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

Similarly, if the two routers have different passwords configured, a message such as this is displayed:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:1
```

Verify

Use this section to confirm that your configuration works properly.

- **show ip bgp neighbors | include 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
```

Troubleshoot

There is currently no troubleshooting information for this configuration.

Related Information

- Cisco IOS IP Routing: BGP Command Reference
- IP Routing Support Page
- Cisco Technical Support & Downloads