

BGP ピア間の MD5 認証の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[デバッグについて](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、2 つの BGP ピア間の TCP 接続での Message Digest5 (MD5) 認証の設定方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントに掲載されているコマンド出力は、IOS® バージョン 12.4(15)T14 が稼働する 3660 シリーズ ルータから取得したものです。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

2つのBGPピア間にMD5認証を設定できますが、これはピア間のTCP接続上で送信された各セグメントが検証されることを意味します。MD5認証は、両方のBGPピアで同じパスワードを設定する必要があります。そうしないと、接続を確立できません。MD5認証の設定により、TCP接続上で送信された各セグメントのMD5ダイジェストに対する、Cisco IOSソフトウェアによる生成とチェックが行われます。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは、次の設定を使用します。

ルータ0の設定

```
R0#! interface Loopback70 ip address 70.70.70.70
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 80.80.80.80 remote-as 400 !--- iBGP
Configuration using Loopback Address neighbor
80.80.80.80 password cisco !--- Invoke MD5
authentication on a TCP connection to a BGP peer
neighbor 80.80.80.80 update-source Loopback70 no auto-
summary ! ip route 80.80.80.80 255.255.255.255
10.10.10.2 !--- This static route ensures that the
remote peer address used for peering !--- is reachable.
. . .
```

ルータ1コンフィギュレーション

```
R1#! interface Loopback80 ip address 80.80.80.80
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 70.70.70.70 remote-as 400 !--- iBGP
Configuration using Loopback Address neighbor
70.70.70.70 password cisco !--- Invoke MD5
authentication on a TCP connection to a BGP peer
neighbor 70.70.70.70 update-source Loopback80 no auto-
summary ! ip route 70.70.70.70 255.255.255.255
10.10.10.1 !--- This static route ensures that the
remote peer address used for peering !--- is reachable.
. . .
```

デバッグについて

```
R0#clear ip bgp * R0#
```

```
*Mar 1 01:02:17.523: %BGP-5-ADJCHANGE: neighbor 80.80.80.80 Down User reset
```

```
R0#debug ip bgp
BGP debugging is on for address family: IPv4 Unicast
*Mar 1 01:03:58.159: BGP: 80.80.80.80 open failed: Connection timed out;
  remote host not responding, open active delayed 1782ms (2000ms max, 28%
  jitter)
*Mar 1 01:03:58.415: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 01:03:59.943: BGP: 80.80.80.80 open active, local address 70.70.70.70
*Mar 1 01:04:00.039: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:00.807: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(33358)
  to 70.70.70.70(179)
*Mar 1 01:04:01.991: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:01.995: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:05.995: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:06.015: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 80.80.80.80(179) to
  70.70.70.70(64444)
*Mar 1 01:04:29.947: BGP: 80.80.80.80 open failed: Connection timed out;
  remote host not responding, open active delayed 3932ms (4000ms max, 28%
  jitter)
*Mar 1 01:04:33.879: BGP: 80.80.80.80 open active, local address 70.70.70.70
*Mar 1 01:04:33.983: BGP: 80.80.80.80 went from Active to OpenSent
*Mar 1 01:04:33.983: BGP: 80.80.80.80 sending OPEN, version 4, my as: 400,
  hold time 180 seconds
*Mar 1 01:04:33.987: BGP: 80.80.80.80 send message type 1, length (incl.
  header ) 45
*Mar 1 01:04:34.091: BGP: 80.80.80.80 rcv message type 1, length (excl.
  header) 26
*Mar 1 01:04:34.091: BGP: 80.80.80.80 rcv OPEN, version 4, holdtime 180 seconds
*Mar 1 01:04:34.091: BGP: 80.80.80.80 rcv OPEN w/ OPTION parameter len: 16
*Mar 1 01:04:34.095: BGP: 80.80.80.80 rcvd OPEN w/ optional parameter type 2
  (Capability) len 6
*Mar 1 01:04:34.095: BGP: 80.80.80.80 OPEN has CAPABILITY code: 1, length 4
*Mar 1 01:04:34.095: BGP: 80.80.80.80 OPEN has MP_EXT CAP for afi/safi: 1/1
*Mar 1 01:04:34.095: BGP: 80.80.80.80 rcvd OPEN w/ optional parameter type 2
  (Capability) len 2
*Mar 1 01:04:34.095: BGP: 80.80.80.80 OPEN has CAPABILITY code: 128, length 0
*Mar 1 01:04:34.099: BGP: 80.80.80.80 OPEN has ROUTE-REFRESH capability(old)
  for all address-families
*Mar 1 01:04:34.099: BGP: 80.80.80.80 rcvd OPEN w/ optional parameter type 2
  (Capability) len 2
*Mar 1 01:04:34.099: BGP: 80.80.80.80 OPEN has CAPABILITY code: 2, length 0
*Mar 1 01:04:34.099: BGP: 80.80.80.80 OPEN has ROUTE-REFRESH capability(new)
  for all address-families
BGP: 80.80.80.80 rcvd OPEN w/ remote AS 400
*Mar 1 01:04:34.103: BGP: 80.80.80.80 went from OpenSent to OpenConfirm
*Mar 1 01:04:34.103: BGP: 80.80.80.80 went from OpenConfirm to Established
*Mar 1 01:04:34.103: %BGP-5-ADJCHANGE: neighbor 80.80.80.80 Up
```

ルータがネイバーに対してパスワードを設定しているものの、ネイバーのルータがパスワードを設定していない場合は、ルータが BGP セッションの確立を試行する間に次のようなメッセージが表示されます。

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

同様に、2つのルータに異なるパスワードが設定されている場合は、次のようなメッセージが表示されます。

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

確認

ここでは、設定が正常に動作していることを確認します。

- [R0#show ip bgp neighbors | include BGP](#) BGP neighbor is 80.80.80.80, remote AS 400, internal link

```
BGP version 4, remote router ID 80.80.80.80
BGP state = Established, up for 00:08:26
BGP table version 1, neighbor version 1/0
```

- [R0#show ip bgp summary](#) BGP router identifier 70.70.70.70, 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
80.80.80.80	4	400	75	75	1	0	0	00:08:52	0

- [R1#show IP bgp 要約](#) BGP router identifier 80.80.80.80, 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
70.70.70.70	4	400	76	76	1	0	0	00:09:27	0

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco IOS IP ルーティング : BGP コマンド リファレンス](#)
- [IP ルーティングに関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)