RIPv2 での認証のための設定例

内容

概要

このドキュメントでは、Routing Information Protocol バージョン 2 (RIPv2) のルーティング情報交換プロセスを認証するための設定例を示します。

RIPv2 の Cisco 実装では、2 種類の認証モードがサポートされます。平文認証と Message Digest 5 (MD5) 認証平文認証モードは、認証が有効な場合、すべての RIPv2 パケットのデフォルト設定です。平文認証は、暗号化されていない認証パスワードが RIPv2 パケットごとに送信されるため、セキュリティが問題になる場合には使用しないでください。

注：RIPバージョン1 (RIPv1)は認証をサポートしていません。RIPv2 パケットを送受信する場合は、インターフェイスで RIP 認証を有効にできます。

前提条件

要件

このドキュメントの読者は次の項目に関する基本知識が必要です。

- RIPv1 と RIPv2

使用するコンポーネント

このドキュメントの内容は、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。Cisco IOS® ソフトウェア バージョン 11.1 以降では RIPv2 がサポートされているため、この設定で指定されるすべてのコマンドが Cisco IOS® ソフトウェア バージョン 11.1 以降でサポートされます。

このドキュメントの設定は、次のソフトウェアとハードウェアのバージョンを使用してテストされ、更新されます。

- Cisco 2500 シリーズ ルータ
- Cisco IOS ソフトウェア バージョン 12.3(3)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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

今日のネットワーク設計者にとって、セキュリティは最も重要な関心事の 1 つになっています。ネットワークのセキュリティには、ルータ間でのルーティング情報の交換に関するセキュリティも含まれます。たとえば、ルーティング テーブルに書き込まれる情報が有効なものであること、これがネットワークの妨害を意図するような発信者から送られたり、改ざんされたりしたものではないことの確認などです。攻撃者は、不正な更新情報を持ち込んでルータが誤った宛先にデータを送るようにしたり、ネットワークのパフォーマンスを著しく低下させようとします。さらに、不正なルート更新によってルーティング テーブルの内容が破壊されることもありますが、これは設定がよくないこと（ネットワークの境界に対して passive interface コマンドが使用されていないなど）、あるいはルータの動作不良が原因で発生します。このため、ルータ上で実行されるルーティング更新プロセスの認証は慎重に行われます。

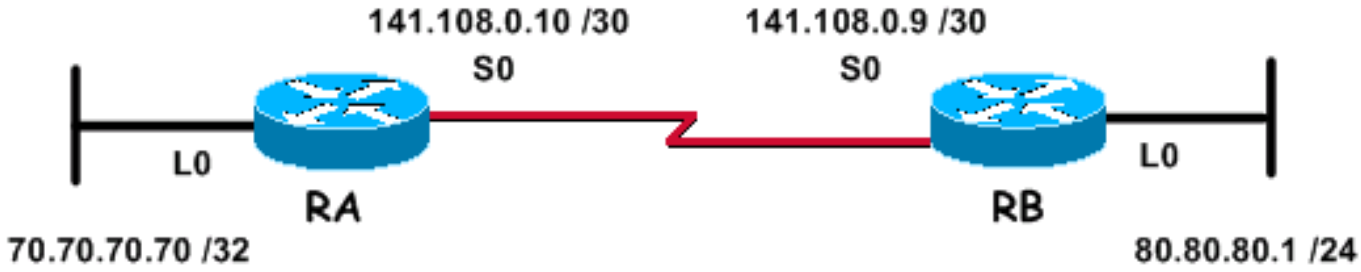
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは次の図に示すネットワーク構成を使用しています。



次の設定例で使用される上記のネットワークは、2 台のルータ、ルータ RA およびルータ RB で構成され、どちらも RIP を実行し、定期的にルーティング更新の交換を実行しています。このシリアル リンクを経由するルーティング情報の交換は、認証を受ける必要があります。

設定

RIPv2 で認証を設定するには、次の手順を実行します。

1. 名前の付いたキー チェーンを定義します。**注：キーチェーン**は、インターフェイスで使用できるキーのセットを決定します。キーチェーンが設定されていない場合、そのインターフェイスで認証は実行されません。
2. キー チェーンに 1 つ以上のキーを定義します。
3. キーで使用するパスワードまたはキー ストリングを指定します。これは、認証されるルーティング プロトコルを使用するパケットで送受信される必要がある認証文字列です（次の例では、文字列の値は 234 です）。
4. インターフェイスの認証を有効にして、使用するキー チェーンを指定します。認証はインターフェイス単位で有効にするため、RIPv2 を実行しているルータは、特定のインターフェイスで認証の設定ができ、他のインターフェイスでは認証なしで動作できます。
5. インターフェイスで平文を使用するか、MD5 認証を使用するかを指定します。前の手順で認証を有効にしている場合、RIPv2 で使用されるデフォルトの認証は、平文認証です。したがって平文認証を使用している場合、この手順は必要ありません。
6. キー管理を設定します（この手順は任意選択です）。キー管理は認証キーを制御する方法です。これは、ある認証キーから別の認証キーへの移行に使用されます。詳細については、『IP ルーティングのプロトコル独立型機能の設定』の「認証キーの管理」の項を参照してください。

平文認証の設定

RIP 更新を認証する 2 種類の方法のうちの 1 つは、平文認証を使用する方法です。この方法は、次の表に示すように設定します。

RA
key chain kal *!--- Name a key chain. A key chain may contain more than one key for added security. !--- It need not be identical on the remote router.* **key 1** *!--- This is the Identification number of an authentication key on a key chain. !--- It need not be identical on the remote router.* **key-string 234**

```
!--- The actual password or key-string. !--- It needs to
be identical to the key-string on the remote router. !
interface Loopback0 ip address 70.70.70.70
255.255.255.255 ! interface Serial0 ip address
141.108.0.10 255.255.255.252 ip rip authentication key-
chain kal
!--- Enables authentication on the interface and
configures !--- the key chain that will be used. !
router rip version 2 network 141.108.0.0 network
70.0.0.0
```

RB

```
key chain kal

key 1
key-string 234


!

interface Loopback0

 ip address 80.80.80.1 255.255.255.0

!

interface Serial0

 ip address 141.108.0.9 255.255.255.252

 ip rip authentication key-chain kal

 clockrate 64000

!

router rip

 version 2

 network 141.108.0.0

 network 80.0.0.0
```

コマンドの詳細については、『Cisco IOS IP コマンド リファレンス』を参照してください。

MD5 認証の設定

MD5認証は、元のRFC 1723で定義された平文認証にシスコが追加したオプションの認証モードです 。設定は平文認証の場合と同じですが、ip rip authentication mode md5 コマンドを追加する点が異なっています。MD5 認証方式では、ユーザがのリンクの両側のルータ インターフェイスを設定する必要があり、両側のキー番号とキー ストリングが一致しなければなりません。

RA

```

```

```
key chain kal

!--- Need not be identical on the remote router. key 1

!--- Needs to be identical on remote router. key-string
234

!--- Needs to be identical to the key-string on the
remote router. ! interface Loopback0 ip address
70.70.70.70 255.255.255.255 ! interface Serial0 ip
address 141.108.0.10 255.255.255.252 ip rip
authentication mode md5
!--- Specifies the type of authentication used !--- in
RIPv2 packets. !--- Needs to be identical on remote
router. !-- To restore clear text authentication, use
the no form of this command. ip rip authentication key-
chain kal

 !

 router rip

  version 2

  network 141.108.0.0

  network 70.0.0.0
```

RB

```
key chain kal

key 1

key-string 234

!

interface Loopback0

 ip address 80.80.80.1 255.255.255.0

!

interface Serial0

 ip address 141.108.0.9 255.255.255.252

 ip rip authentication mode md5

 ip rip authentication key-chain kal

 clockrate 64000

!

router rip

 version 2

 network 141.108.0.0
```

```
 network 80.0.0.0
```

コマンドの詳細については、『Cisco IOS コマンド リファレンス』を参照してください。

確認

平文認証の確認

このセクションでは、設定が正常に動作しているかどうかを確認するための情報について説明します。

上記のようにルータを設定することで、すべてのルーティング更新の交換が、許可される前に認証されるようになります。このことは、debug ip rip コマンドおよび show ip route コマンドから得られる出力を調べることによって確認できます。

注：debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。

```
RB#debug ip rip

 RIP protocol debugging is on

*Mar  3 02:11:39.207: RIP: received packet with text authentication 234

*Mar  3 02:11:39.211: RIP: received v2 update from 141.108.0.10 on Serial0

*Mar  3 02:11:39.211: RIP: 70.0.0.0/8 via 0.0.0.0 in 1 hops

RB#show ip route

R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:25, Serial0

     80.0.0.0/24 is subnetted, 1 subnets

C       80.80.80.0 is directly connected, Loopback0

     141.108.0.0/30 is subnetted, 1 subnets

C       141.108.0.8 is directly connected, Serial0
```

平文認証を使用することで、ローカルのルーティング交換プロセスには参加し得ないルータからのルーティング更新を排除でき、ネットワーク設計が向上します。しかし、この認証方式は万全ではありません。平文認証では、パスワード (この例では 234) が交換されます。これは簡単に捕捉され、利用されてしまう可能性があります。先に述べたように、セキュリティが問題になる場合には、平文認証よりも MD5 認証の方を使用してください。

MD5 認証の確認

上記のように RA ルータと RB ルータを設定することで、すべてのルーティング更新の交換が、受け入れの前に認証されるようになります。このことは、debug ip rip コマンドおよび show ip route コマンドから得られる出力を調べることによって確認できます。

```
RB#debug ip rip

 RIP protocol debugging is on

*Mar  3 20:48:37.046: RIP: received packet with MD5 authentication

*Mar  3 20:48:37.046: RIP: received v2 update from 141.108.0.10 on Serial0

*Mar  3 20:48:37.050:  70.0.0.0/8 via 0.0.0.0 in 1 hops


RB#show ip route

R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:03, Serial0

     80.0.0.0/24 is subnetted, 1 subnets

C       80.80.80.0 is directly connected, Loopback0

     141.108.0.0/30 is subnetted, 1 subnets

C       141.108.0.8 is directly connected, Serial0
```

MD5 認証では、強力なハッシング アルゴリズムとして知られている単方向の MD5 ハッシュ アルゴリズムを使用しています。このモードの認証では、ルーティング更新によって認証の目的でパスワードが搬送されることはありません。その代わり、MD5 アルゴリズムによって 128 ビットのメッセージがパスワードの目的で作成され、このメッセージが認証用に送信されます。したがって、MD5 の方がより安全な方法であるため、平文認証よりも MD5 認証を使うことを推奨します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

debug ip ripコマンドは、RIPv2認証関連の問題のトラブルシューティングに使用できます。

注：debugコマンドを発行する前に、「debugコマンドの重要な情報」を参照してください。

注：隣接ルータ間で同一である必要がある認証関連パラメータが一致しない場合の**debug ip ripコマンドの出力の例を次に示しま**す。この結果、いずれかのルータまたは両方のルータが、ルーティング テーブルに受信したルートをインストールしない可能性があります。

```
RA#debug ip rip

   RIP protocol debugging is on
```

```
*Mar 1 06:47:42.422: RIP: received packet with text authentication 234

*Mar 1 06:47:42.426: RIP: ignored v2 packet from 141.108.0.9 (invalid authentication)


RB#debug ip rip

RIP protocol debugging is on



*Mar 1 06:48:58.478: RIP: received packet with text authentication 235

*Mar 1 06:48:58.482: RIP: ignored v2 packet from 141.108.0.10 (invalid authentication)
```

show ip route コマンドの次の出力は、RIP を介してルートがルータを学習していないことを示しています。

```
RB#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

80.0.0.0/24 is subnetted, 1 subnets

   C 80.80.80.0 is directly connected, Loopback0

   141.108.0.0/30 is subnetted, 1 subnets

   C 141.108.0.8 is directly connected, Serial0

   RB#
```

注 1：平文認証モードを使用する場合、認証が正常に終了するためには、次のパラメータが隣接ルータで一致していることを確認してください。

- キー ストリング
- 認証モード

注 2：MD5 認証モードを使用する場合、認証が正常に終了するためには、次のパラメータが隣接ルータで一致していることを確認してください。

- キー ストリング
- キー番号
- 認証モード

関連情報

- ルーティング情報プロトコル（RIP）の概要

- RIP の設定
- IP ルーティングのプロトコル独立型機能の設定
- RIP コマンド
- Cisco IOS IP コマンド リファレンス、2/4 部：ルーティング プロトコル、リリース 12.3
- RIP テクノロジーに関するサポート ページ
- IP ルーティング プロトコルのテクノロジーに関するサポート ページ
- テクニカルサポート - Cisco Systems