Beispielkonfiguration für die Authentifizierung in RIPv2

Inhalt

Einführung

Dieses Dokument enthält Beispielkonfigurationen für die Authentifizierung des Austauschprozesses von Routing-Informationen für Routing Information Protocol Version 2 (RIPv2).

Die Cisco Implementierung von RIPv2 unterstützt zwei Authentifizierungsmodi: Nur-Text-Authentifizierung und MD5-Authentifizierung (Message Digest 5). Bei Aktivierung der Authentifizierung ist in jedem RIPv2-Paket der Standardmodus für die einfache Textauthentifizierung festgelegt. Bei Sicherheitslücken sollte keine Klartext-Authentifizierung verwendet werden, da das unverschlüsselte Authentifizierungskennwort in jedem RIPv2-Paket gesendet wird.

Hinweis: RIP Version 1 (RIPv1) unterstützt keine Authentifizierung. Wenn Sie RIPv2-Pakete senden und empfangen, können Sie die RIP-Authentifizierung auf einer Schnittstelle aktivieren.

Voraussetzungen

Anforderungen

Leser dieses Dokuments sollten folgende Grundkenntnisse haben:

- RIPv1 und RIPv2

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Ab der Cisco IOS® Software Version 11.1 wird RIPv2 unterstützt. Daher werden alle in der Konfiguration angegebenen Befehle von der Cisco IOS® Software Version 11.1 und höher unterstützt.

Die Konfiguration im Dokument wird mit den folgenden Software- und Hardwareversionen getestet und aktualisiert:

- Cisco Router der Serie 2500
- Cisco IOS Software Version 12.3(3)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

Sicherheit ist heutzutage eines der Hauptanliegen von Netzwerkdesignern. Der Schutz eines Netzwerks umfasst die Sicherung des Austauschs von Routing-Informationen zwischen Routern, z. B. die Sicherstellung, dass die in die Routing-Tabelle eingegebenen Informationen gültig sind und nicht von jemandem generiert oder manipuliert werden, der versucht, das Netzwerk zu stören. Ein Angreifer könnte versuchen, ungültige Updates einzuführen, um den Router dazu zu verleiten, Daten an das falsche Ziel zu senden, oder um die Netzwerkleistung ernsthaft zu beeinträchtigen. Darüber hinaus können ungültige Routen-Updates aufgrund einer schlechten Konfiguration (z. B. aufgrund der Nichtverwendung des Befehls **passive Schnittstelle** an der Netzwerkgrenze) oder aufgrund eines defekten Routers in der Routing-Tabelle landen. Aus diesem Grund ist es ratsam, den Routing-Update-Prozess auf einem Router zu authentifizieren.

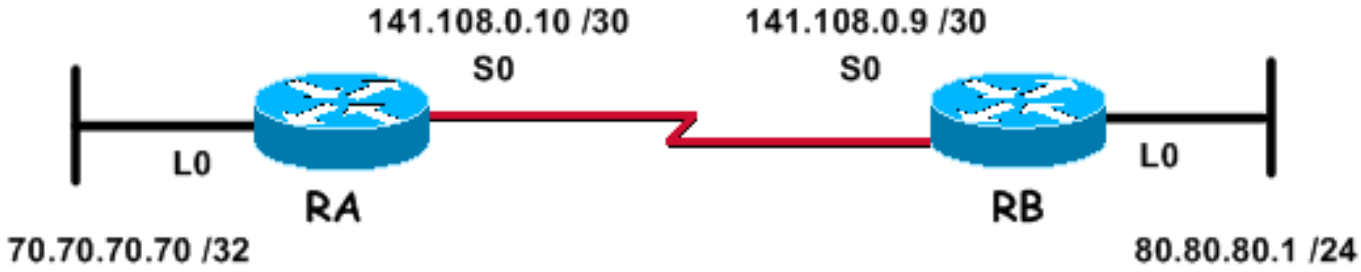
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Das oben angegebene Netzwerk, das für die folgenden Konfigurationsbeispiele verwendet wird, besteht aus zwei Routern. Router RA und Router RB, die beide RIP ausführen und regelmäßig Routing-Updates austauschen. Dieser Austausch von Routing-Informationen über die serielle Verbindung muss authentifiziert werden.

Konfigurationen

Führen Sie folgende Schritte aus, um die Authentifizierung in RIPv2 zu konfigurieren:

1. Definieren Sie eine Schlüsselkette mit einem Namen.**Hinweis:** Die Schlüsselkette bestimmt den Satz von Schlüsseln, die auf der Schnittstelle verwendet werden können. Wenn keine Schlüsselkette konfiguriert ist, wird für diese Schnittstelle keine Authentifizierung durchgeführt.
2. Definieren Sie den oder die Schlüssel in der Schlüsselkette.
3. Geben Sie das Kennwort oder die Schlüsselzeichenfolge für den Schlüssel an.Hierbei handelt es sich um die Authentifizierungszeichenfolge, die in den Paketen mit dem authentifizierten Routing-Protokoll gesendet und empfangen werden muss. (Im Beispiel unten lautet der Wert der Zeichenfolge 234.)
4. Aktivieren Sie die Authentifizierung auf einer Schnittstelle, und geben Sie die zu verwendende Schlüsselkette an.Da die Authentifizierung auf Schnittstellenbasis aktiviert ist, kann ein Router mit RIPv2 für die Authentifizierung an bestimmten Schnittstellen konfiguriert werden und ohne Authentifizierung an anderen Schnittstellen betrieben werden.
5. Geben Sie an, ob die Schnittstelle Nur-Text- oder MD5-Authentifizierung verwendet.Die in RIPv2 verwendete Standardauthentifizierung ist die Nur-Text-Authentifizierung, wenn im vorherigen Schritt die Authentifizierung aktiviert wurde. Wenn Sie also eine Nur-Text-Authentifizierung verwenden, ist dieser Schritt nicht erforderlich.
6. Konfigurieren Sie die Schlüsselverwaltung (dieser Schritt ist optional).Schlüsselverwaltung ist eine Methode zur Steuerung von Authentifizierungsschlüsseln. Diese wird verwendet, um von einem Authentifizierungsschlüssel zu einem anderen zu migrieren. Weitere Informationen finden Sie im Abschnitt "Authentifizierungsschlüssel verwalten" unter Konfigurieren von protokollunabhängigen Funktionen für das IP-Routing.

Konfigurieren der einfachen Textauthentifizierung

Eine der beiden Möglichkeiten, RIP-Aktualisierungen zu authentifizieren, besteht in der einfachen Textauthentifizierung. Dies kann wie in der nachfolgenden Tabelle dargestellt konfiguriert werden.

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
```

Detaillierte Informationen zu den Befehlen finden Sie in der Befehlsreferenz zu Cisco IOS IP.

Konfigurieren der MD5-Authentifizierung

Die MD5-Authentifizierung ist ein optionaler Authentifizierungsmodus, der von Cisco der

ursprünglichen RFC 1723-definierten Nur-Text-Authentifizierung hinzugefügt wurde. Die Konfiguration ist identisch mit der für die Nur-Text-Authentifizierung, mit Ausnahme der Verwendung des zusätzlichen Befehls **ip rip authentication mode md5**. Die Benutzer müssen die Router-Schnittstellen auf beiden Seiten der Verbindung für die MD5-Authentifizierungsmethode konfigurieren, wobei sicherzustellen ist, dass die Schlüsselnummer und die Schlüsselzeichenfolge auf beiden Seiten übereinstimmen.

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
```

Detaillierte Informationen zu den Befehlen finden Sie in der Cisco IOS-Befehlsreferenz.

Überprüfen

Überprüfen der Nur-Text-Authentifizierung

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn die Router wie oben gezeigt konfiguriert werden, werden alle Routing-Update-Austauschvorgänge authentifiziert, bevor sie akzeptiert werden. Dies kann überprüft werden, indem die Ausgabe der **Befehle** debug ip rip und show ip route **überwacht wird**.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

```
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
```

Die Verwendung der Nur-Text-Authentifizierung verbessert das Netzwerkdesign, indem verhindert wird, dass Routing-Updates hinzugefügt werden, die von Routern erstellt wurden, die nicht am

lokalen Routing-Austauschprozess teilnehmen sollen. Diese Art der Authentifizierung ist jedoch nicht sicher. Das Passwort (in diesem Beispiel 234) wird im Klartext ausgetauscht. Sie kann leicht erfasst und somit ausgenutzt werden. Wie bereits erwähnt, muss die MD5-Authentifizierung gegenüber der Nur-Text-Authentifizierung bevorzugt werden, wenn die Sicherheit ein Problem darstellt.

Überprüfen der MD5-Authentifizierung

Wenn die RA- und RB-Router wie oben gezeigt konfiguriert werden, werden alle Routing-Update-Austauschvorgänge authentifiziert, bevor sie akzeptiert werden. Dies kann überprüft werden, indem die Ausgabe der **Befehle debug** ip rip und show ip route überwacht wird.

```
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
```

Die MD5-Authentifizierung verwendet den unidirektionalen MD5-Hash-Algorithmus, der als starker Hash-Algorithmus anerkannt wird. In diesem Authentifizierungsmodus enthält die Routing-Aktualisierung kein Kennwort für die Authentifizierung. Stattdessen wird eine 128-Bit-Nachricht, die durch Ausführen des MD5-Algorithmus im Kennwort generiert wird, und die Nachricht zur Authentifizierung gesendet. Daher wird empfohlen, die MD5-Authentifizierung über die Nur-Text-Authentifizierung zu verwenden, da diese sicherer ist.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Der Befehl debug ip rip kann zur Behebung von Problemen im Zusammenhang mit der RIPv2-Authentifizierung verwendet werden.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debugbefehle.

Hinweis: Das nachfolgende Beispiel zeigt die Ausgabe des Befehls **debug ip rip**, wenn einer der authentifizierungsbezogenen Parameter, die zwischen den benachbarten Routern identisch sein müssen, nicht übereinstimmt. Dies kann dazu führen, dass entweder ein oder beide Router die empfangenen Routen nicht in ihrer Routing-Tabelle installieren.

```
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)
```

Die folgende Ausgabe des **Befehls** **show ip route** zeigt, dass der Router keine Routen über RIP lernt:

```
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#
```

Hinweis 1: Wenn Sie den Nur-Text-Authentifizierungsmodus verwenden, stellen Sie sicher, dass die folgenden Parameter auf benachbarten Routern übereinstimmen, um eine erfolgreiche Authentifizierung zu gewährleisten.

- Schlüsselzeichenfolge
- Authentifizierungsmodus

Hinweis 2: Wenn Sie den MD5-Authentifizierungsmodus verwenden, stellen Sie für eine erfolgreiche Authentifizierung sicher, dass die folgenden Parameter auf benachbarten Routern übereinstimmen.

- Schlüsselzeichenfolge
- Schlüsselnummer
- Authentifizierungsmodus

Zugehörige Informationen

- Einführung in das Routing Information Protocol (RIP)
- Konfigurieren von RIP
- Konfiguration von IP-Routing-Protokollen - unabhängige Funktionen
- RIP-Befehle
- Cisco IOS IP-Befehlsreferenz, Band 2 von 4: Routing-Protokolle, Version 12.3
- Support-Seite für RIP Technology
- Technologieunterstützung für IP Routing Protocols
- Technischer Support - Cisco Systems