Esempio di configurazione per l'autenticazione in RIPv2

Sommario

Introduzione

In questo documento vengono mostrati alcuni esempi di configurazione per autenticare il processo di scambio delle informazioni di routing quando si usa il protocollo RIPv2 (Routing Information Protocol version 2).

L'implementazione Cisco di RIPv2 supporta due modalità di autenticazione: autenticazione di testo normale e autenticazione MD5 (Message Digest 5). Quando l'autenticazione è abilitata, la modalità di autenticazione testo normale è l'impostazione predefinita in ogni pacchetto RIPv2. L'autenticazione in testo normale non deve essere utilizzata quando la sicurezza è un problema, perché la password di autenticazione non crittografata viene inviata in ogni pacchetto RIPv2.

Nota: RIP versione 1 (RIPv1) non supporta l'autenticazione. Se si inviano e ricevono pacchetti RIPv2, è possibile abilitare l'autenticazione RIP su un'interfaccia.

Prerequisiti

Requisiti

I lettori di questo documento devono avere le seguenti conoscenze di base:

- RIPv1 e RIPv2

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. A partire dal software Cisco IOS® versione 11.1, RIPv2 è supportato e quindi tutti i comandi specificati nella configurazione sono supportati nel software Cisco IOS® versione 11.1 e successive.

La configurazione nel documento viene testata e aggiornata utilizzando le seguenti versioni software e hardware:

- Router Cisco serie 2500
- Software Cisco IOS versione 12.3(3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Oggi la sicurezza è una delle principali preoccupazioni dei progettisti di reti. La protezione di una rete include la protezione dello scambio di informazioni di routing tra router, ad esempio la garanzia che le informazioni immesse nella tabella di routing siano valide e non vengano originate o manomesse da utenti che tentano di interrompere la rete. Un utente non autorizzato potrebbe tentare di introdurre aggiornamenti non validi per indurre il router a inviare i dati alla destinazione errata o per ridurre notevolmente le prestazioni della rete. Inoltre, gli aggiornamenti dei percorsi non validi potrebbero finire nella tabella di routing a causa di una configurazione errata (ad esempio, il mancato utilizzo del comando **passive interface** sui limiti della rete) o di un router non funzionante. Per questo motivo, è prudente autenticare il processo di aggiornamento del routing in esecuzione su un router.

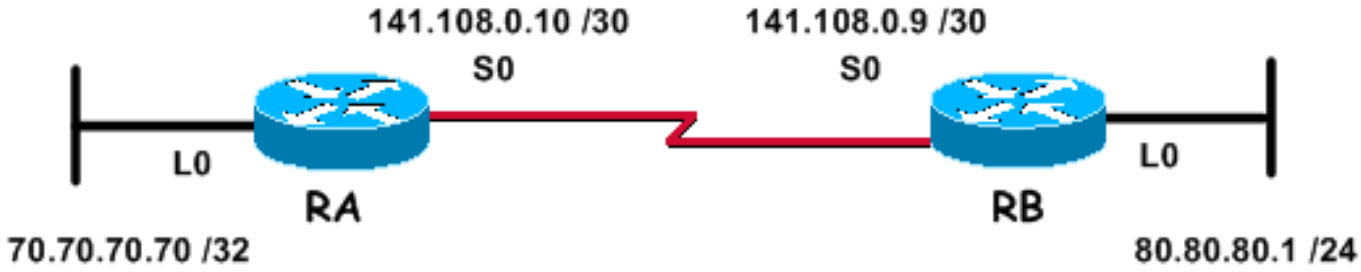
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



La rete sopra descritta, utilizzata per gli esempi di configurazione riportati di seguito, è costituita da due router: router RA e router RB, entrambi eseguono RIP e si scambiano periodicamente aggiornamenti del routing. Lo scambio di informazioni di routing tramite il collegamento seriale deve essere autenticato.

Configurazioni

Eseguire la procedura seguente per configurare l'autenticazione in RIPv2:

1. Definire una catena di chiavi con un nome.**Nota:** la catena di chiavi determina l'insieme di chiavi che è possibile utilizzare nell'interfaccia. Se non è configurata una catena di chiavi, l'interfaccia non verrà autenticata.
2. Definire la chiave o le chiavi sulla catena di chiavi.
3. Specificare la password o la stringa da utilizzare nella chiave.Stringa di autenticazione da inviare e ricevere nei pacchetti che utilizzano il protocollo di routing da autenticare. Nell'esempio seguente, il valore della stringa è 234.
4. Abilitare l'autenticazione su un'interfaccia e specificare la catena di chiavi da utilizzare.Poiché l'autenticazione è abilitata per interfaccia, un router che esegue RIPv2 può essere configurato per l'autenticazione su determinate interfacce e può funzionare senza autenticazione su altre interfacce.
5. Specificare se l'interfaccia utilizzerà l'autenticazione di testo normale o MD5.L'autenticazione predefinita utilizzata in RIPv2 è l'autenticazione in testo normale, quando l'autenticazione è abilitata nel passaggio precedente. Pertanto, se si utilizza l'autenticazione di testo normale, questo passaggio non è necessario.
6. Configurare la gestione delle chiavi (questo passaggio è facoltativo).La gestione delle chiavi è un metodo di controllo delle chiavi di autenticazione. Utilizzato per eseguire la migrazione da una chiave di autenticazione a un'altra. Per ulteriori informazioni, fare riferimento alla sezione "Manage Authentication Keys" nel documento sulla configurazione delle funzionalità indipendenti dal protocollo di routing IP.

Configurazione dell'autenticazione solo testo

Uno dei due modi in cui è possibile autenticare gli aggiornamenti RIP è l'autenticazione in testo normale. È possibile configurare questa opzione come illustrato nelle tabelle seguenti.

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
```

Per informazioni dettagliate sui comandi, consultare la guida di riferimento dei comandi di Cisco IOS IP.

Configurazione dell'autenticazione MD5

L'autenticazione MD5 è una modalità di autenticazione opzionale aggiunta da Cisco all'autenticazione in testo normale definita da RFC 1723 originale. La configurazione è identica a quella dell'autenticazione di testo normale, ad eccezione dell'uso del comando aggiuntivo **ip rip**

authentication mode md5. Gli utenti devono configurare le interfacce del router su entrambi i lati del collegamento per il metodo di autenticazione MD5, assicurandosi che il numero di chiave e la stringa di chiave corrispondano su entrambi i lati.

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
```

Per informazioni dettagliate sui comandi, consultare la guida di riferimento dei comandi di Cisco IOS.

Verifica

Verifica dell'autenticazione solo testo

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Configurando i router come mostrato sopra, tutti gli scambi di aggiornamenti del routing verranno autenticati prima di essere accettati. È possibile verificare questa condizione osservando l'output ottenuto dai comandi debug ip rip e show ip route.

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

```
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
```

L'utilizzo dell'autenticazione di testo normale migliora la progettazione della rete impedendo l'aggiunta di aggiornamenti di routing originati da router non destinati a partecipare al processo di scambio del routing locale. Questo tipo di autenticazione non è tuttavia sicuro. La password (234 in questo esempio) viene scambiata in testo normale. Può essere acquisito facilmente e quindi sfruttato. Come accennato in precedenza, quando la sicurezza è un problema, l'autenticazione

MD5 deve essere preferita all'autenticazione in testo normale.

Verifica dell'autenticazione MD5

Configurando i router RA e RB come mostrato sopra, tutti gli scambi di aggiornamenti del routing verranno autenticati prima di essere accettati. È possibile verificare questa condizione osservando l'output ottenuto dai comandi debug ip rip e show ip route.

```
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
```

L'autenticazione MD5 utilizza l'algoritmo hash MD5 unidirezionale, riconosciuto come un algoritmo hash avanzato. In questa modalità di autenticazione, l'aggiornamento del routing non dispone della password per effettuare l'autenticazione. Al contrario, un messaggio a 128 bit, generato eseguendo l'algoritmo MD5 sulla password, e il messaggio vengono inviati per l'autenticazione. Pertanto, si consiglia di utilizzare l'autenticazione MD5 anziché l'autenticazione di testo normale, poiché è più sicura.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Il comando debug ip rip può essere usato per risolvere i problemi relativi all'autenticazione RIPv2.

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Nota: di seguito è riportato un esempio dell'output del comando debug ip rip , quando uno dei parametri relativi all'autenticazione che devono essere identici tra i router adiacenti non corrisponde. Di conseguenza, uno o entrambi i router non installano le route ricevute nella relativa tabella di routing.

```
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)
```

L'output seguente del comando show ip route mostra che il router non sta imparando alcuna route tramite RIP:

```
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#
```

Nota 1: Quando si utilizza la modalità di autenticazione solo testo, verificare che i parametri seguenti corrispondano ai router adiacenti per la riuscita dell'autenticazione.

- Stringa-chiave
- Modalità di autenticazione

Nota 2: Quando si utilizza la modalità di autenticazione MD5, per una corretta autenticazione

assicurarsi che i parametri seguenti corrispondano ai router adiacenti.

- Stringa-chiave
- Numero chiave
- Modalità di autenticazione

Informazioni correlate

- Introduzione al protocollo RIP (Routing Information Protocol)
- Configurazione di RIP
- Configurazione delle funzioni indipendenti dai protocolli di routing IP
- Comandi RIP
- Guida di riferimento ai comandi di Cisco IOS IP, volume 2 di 4: Protocolli di routing, release 12.3
- Pagina di supporto per la tecnologia RIP
- Pagina di supporto per la tecnologia dei protocolli di routing IP
- Supporto tecnico – Cisco Systems