Configura prima autenticazione nel percorso più breve aperto

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione OSPF (Open Shortest Path First) e consentire la flessibilità necessaria per autenticare i router adiacenti OSPF.

Prerequisiti

Requisiti

I lettori di questo documento devono conoscere i concetti base del protocollo di routing OSPF. Fare riferimento alle informazioni o sul protocollo di routing OSPF.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Cisco 2503 router
- Software Cisco IOS® versione 12.2(27)

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

In questo documento vengono illustrate alcune configurazioni di esempio per l'autenticazione OSPF (Open Shortest Path First), che offre la flessibilità necessaria per autenticare i router adiacenti OSPF. È possibile abilitare l'autenticazione in OSPF per scambiare informazioni di aggiornamento del routing in modo sicuro. L'autenticazione OSPF può essere none (o null), simple o MD5. Il metodo di autenticazione "none" indica che non viene utilizzata alcuna autenticazione per OSPF ed è il metodo predefinito. Con l'autenticazione semplice, la password passa in chiaro attraverso la rete. Con l'autenticazione MD5, la password non passa attraverso la rete. MD5 è un algoritmo message-digest specificato nella RFC 1321. MD5 è considerato la modalità di autenticazione OSPF più sicura. Quando si configura l'autenticazione, è necessario configurare un'intera area con lo stesso tipo di autenticazione. Con il software Cisco IOS® versione 12.0(8), l'autenticazione è supportata per singola interfaccia. Questa condizione viene menzionata anche nella RFC 2328, Appendice D. Questa funzionalità è stata aggiunta in 'Cisco bug ID CSCdk33792'.

> **Nota:** Solo i client Cisco registrati possono accedere a questi siti e strumenti.

Si tratta dei tre diversi tipi di autenticazione supportati da OSPF.

- **Autenticazione Null**: questo tipo di autenticazione viene anche denominato Tipo 0 e significa che nell'intestazione del pacchetto non sono incluse informazioni di autenticazione. È l'impostazione predefinita.
- **Autenticazione testo normale**: questo tipo di autenticazione è denominato anche Type 1 e utilizza semplici password non crittografate.
- **Autenticazione MD5**: viene chiamata anche Tipo 2 e utilizza password crittografiche MD5.

Non è necessario impostare l'autenticazione. Tuttavia, se impostato, tutti i router peer sullo stesso segmento devono avere la stessa password e lo stesso metodo di autenticazione. Gli esempi riportati in questo documento illustrano le configurazioni per l'autenticazione sia in testo normale che MD5.

Configurazione

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

Esempio di rete

Nel documento viene usata questa impostazione di rete.

Esempio di rete

Configurazioni per l'autenticazione solo testo

L'autenticazione in testo normale viene utilizzata quando i dispositivi di un'area non supportano l'autenticazione MD5 più sicura. L'autenticazione in testo normale rende l'internetwork vulnerabile a un "attacco di sniffer", in cui i pacchetti vengono acquisiti da un analizzatore di protocolli e le password possono essere lette. Tuttavia, è utile quando si esegue la riconfigurazione OSPF, piuttosto che per motivi di sicurezza. Ad esempio, è possibile utilizzare password separate sui router OSPF più vecchi e più recenti che condividono una rete di trasmissione comune per impedire la comunicazione tra i router. Le password di autenticazione in testo normale non devono essere necessariamente le stesse in tutta l'area, ma devono essere le stesse tra i router adiacenti.

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 10.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.168.64.10 255.255.255.0
  ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network. ! route
10 log-adjacency-changes network 10.70.0.70 0.255.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0
0 authentication !--- Plain text authentication is enabled for !--- all interfaces in Area 0.
```

R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network. ! route
10 network 172.16.0.0 0.0.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0 area 0 authentication !
Plain text authentication is enabled !--- for all interfaces in Area 0.
```

Nota: Il comando area authentication nella configurazione abilita le autenticazioni per tutte le interfacce del router in una determinata area. Per configurare l'autenticazione testo normale per l'interfaccia, è possibile anche utilizzare il comando **ip ospf authentication** nell'interfaccia. Questo comando può essere utilizzato se nell'area a cui appartiene l'interfaccia è configurato un metodo di autenticazione diverso o nessun metodo di autenticazione. Ignora il metodo di autenticazione configurato per l'area. Questa opzione è utile se diverse interfacce appartenenti alla stessa area devono utilizzare metodi di autenticazione diversi

Configurazioni per l'autenticazione MD5

L'autenticazione MD5 offre una protezione maggiore rispetto all'autenticazione di solo testo. Questo metodo utilizza l'algoritmo MD5 per calcolare un valore hash dal contenuto del pacchetto OSPF e una password (o chiave). Questo valore hash viene trasmesso nel pacchetto, insieme a un ID chiave e un numero di sequenza non decrescente. Il destinatario, che conosce la stessa password, calcola il proprio valore hash. Se nel messaggio non viene modificato nulla, il valore hash del destinatario deve corrispondere al valore hash del mittente trasmesso con il messaggio.

L'ID chiave consente ai router di fare riferimento a più password. In questo modo la migrazione delle password diventa più semplice e sicura. Ad esempio, per eseguire la migrazione da una password all'altra, configurare una password con un ID chiave diverso e rimuovere la prima chiave. Il numero di sequenza previene gli attacchi di tipo replay, in cui i pacchetti OSPF vengono acquisiti, modificati e ritrasmessi a un router. Come per l'autenticazione di testo normale, le password di autenticazione MD5 non devono essere necessariamente le stesse in tutta l'area. Tuttavia, devono essere uguali tra vicini.

Nota: Cisco consiglia di configurare il comando service password-encryption su tutti i router. In questo modo, il router crittografa le password in qualsiasi visualizzazione del file di configurazione e protegge la copia di testo della configurazione del router dall'osservazione.

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 10.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.168.64.10 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key value (password) is set as "c1$c0 ". ! router ospf 10
network 192.168.10.10 0.0.0.255 area 0 network 10.70.0.70 0.255.255.255 area 0 area 0 authentication me
digest !--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key (password) value is set as "c1$c0 ". ! router ospf 10
network 172.16.0.0 0.0.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0 area 0 authentication mess
digest !--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

Nota: Il comando area authentication message-digest in questa configurazione abilita l'autenticazione di tutte le interfacce del router in una determinata area. È inoltre possibile utilizzare il comando ip ospf authentication message-digest nell'interfaccia per configurare l'autenticazione MD5 per l'interfaccia specifica. Questo comando può essere utilizzato se nell'area a cui appartiene l'interfaccia è configurato un metodo di autenticazione diverso o nessun metodo di autenticazione. Ignora il metodo di autenticazione configurato per l'area. Ciò è utile se diverse interfacce che appartengono alla stessa area devono utilizzare metodi di autenticazione diversi.

Verifica

Le sezioni seguenti forniscono informazioni che consentono di verificare il corretto funzionamento delle configurazioni.

Verifica autenticazione testo normale

Utilizzare il comando **show ip ospf interface** per visualizzare il tipo di autenticazione configurato per un'interfaccia, come mostrato nell'output. In questo caso, l'interfaccia Serial 0 è configurata per l'autenticazione di testo normale.

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.168.0.10/24, Area 0
  Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled
```

Il comando **show ip ospf neighbors** visualizza la tabella dei nodi adiacenti costituita dai dettagli dei nodi adiacenti, come mostrato nell'output.

```
R1-2503#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.70.70.70       1   FULL/  -        00:00:31    192.168.64.10     Serial0
```

Il comando **show ip route** visualizza la tabella di routing, come mostrato nell'output.

```
R1-2503#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     10.70.0.70/32 is subnetted, 1 subnets
O       10.70.70.70 [110/65] via 192.168.64.10, 00:03:28, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.168.10.10/24 is directly connected, Serial0
```

Verifica autenticazione MD5

Utilizzare il comando **show ip ospf interface** per visualizzare il tipo di autenticazione configurato per un'interfaccia, come mostrato nell'output. In questo caso, l'interfaccia Serial 0 è stata configurata per l'autenticazione MD5 con ID chiave "1".

```
R1-2503#show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.168.0.10/24, Area 0
  Process ID 10, Router ID  172.16.10.36 , Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.70.70.70
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Il comando **show ip ospf neighbors** visualizza la tabella dei nodi adiacenti costituita dai dettagli dei nodi adiacenti, come mostrato nell'output.

```
R1-2503#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.70.70.70       1   FULL/  -        00:00:34    192.168.64.10     Serial0
R1-2503#
```

Il comando **show ip route** visualizza la tabella di routing, come mostrato nell'output.

```
R1-2503#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

     10.70.0.70/32 is subnetted, 1 subnets
O       10.70.70.70 [110/65] via 192.168.64.10, 00:01:23, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.168.10.10/24 is directly connected, Serial0
```

Risoluzione dei problemi

Nelle sezioni seguenti vengono fornite informazioni utili per la risoluzione dei problemi relativi alle configurazioni. Usare il comando **debug ip ospf adj** per acquisire il processo di autenticazione. Questo comando **debug** deve essere eseguito prima di stabilire la relazione con il router adiacente.

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

Risoluzione dei problemi di autenticazione testo normale

L'output **deb ip ospf adj** per R1-2503 mostra quando l'autenticazione in testo normale ha esito positivo.

```
R1-2503#debug ip ospf adj
00:50:57: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:50:57: OSPF: Interface Serial0 going Down
00:50:57: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead,
  state DOWN
00:50:57: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead,
  state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
  FULL to DOWN, Neighbor Down: Interface down or detached
00:50:58: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x80000009
00:50:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to down
00:51:03: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:51:03: OSPF: Interface Serial0 going Up
00:51:04: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000A
00:51:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to up
00:51:13: OSPF: 2 Way Communication to 10.70.70.70 on Serial0,
  state 2WAY
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x19A4 opt 0x42
  flag 0x7 len 32 mtu 1500 state EXSTART
00:51:13: OSPF: First DBD and we are not SLAVE
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x2 len 72 mtu 1500 state EXSTART
00:51:13: OSPF: NBR Negotiation Done. We are the MASTER
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x3 len 72
00:51:13: OSPF: Database request to 10.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.168.64.10, length 12
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 10.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 10.70.70.70 on Serial0, state FULL

!--- Indicates the neighbor adjacency is established. 00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr
10.70.70.70 on Serial0 from LOADING to FULL, Loading Done 00:51:14: OSPF: Build router LSA for
area 0, router ID 172.16.10.36, seq 0x8000000B R1-2503#
```

Questo è l'output del comando **debug ip ospf adj** quando il tipo di autenticazione configurato sui router non corrisponde. In questo output viene mostrato che il router R1-2503 utilizza l'autenticazione di tipo 1, mentre il router R2-2503 è configurato per l'autenticazione di tipo 0. Ciò significa che il router R1-2503 è configurato per l'autenticazione in testo normale (Tipo 1), mentre il router R2-2503 è configurato per l'autenticazione null (Tipo 0).

```
R1-2503#debug ip ospf adj
00:51:23: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication type.

!--- Input packet specified type 0, you use type 1.
```

Questo è l'output del comando **debug ip ospf adj** quando i valori della chiave di autenticazione (password) non corrispondono. In questo caso, entrambi i router sono configurati per l'autenticazione con testo normale (tipo 1), ma i valori della chiave (password) non corrispondono.

```
R1-2503#debug ip ospf adj
00:51:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - Clear Text
```

Risoluzione dei problemi di autenticazione MD5

Questo è l'output del comando **debug ip ospf adj** per R1-2503 quando l'autenticazione MD5 ha esito positivo.

```
R1-2503#debug ip ospf adj
00:59:03: OSPF: Send with youngest Key 1

00:59:13: OSPF: Send with youngest Key 1
00:59:17: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:59:17: OSPF: Interface Serial0 going Down
00:59:17: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead,
  state DOWN
00:59:17: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead,
  state DOWN
00:59:17: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
  FULL to DOWN, Neighbor Down: Interface down or detached
00:59:17: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000E
00:59:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to down
00:59:32: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:59:32: OSPF: Interface Serial0 going Up
00:59:32: OSPF: Send with youngest Key 1
00:59:33: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000F
00:59:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to up

00:59:42: OSPF: Send with youngest Key 1
00:59:42: OSPF: 2 Way Communication to 10.70.70.70 on Serial0,
  state 2WAY

!--- Both neighbors configured for Message !--- digest authentication with Key ID "1". 00:59:42:
OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x7len 32 00:59:42: OSPF: Send
with youngest Key 1 00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x11F3 opt 0x42 flag
0x7 len 32 mtu 1500 state EXSTART 00:59:42: OSPF: First DBD and we are not SLAVE 00:59:42: OSPF:
Rcv DBD from 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x2 len 72 mtu 1500 state EXSTART
00:59:42: OSPF: NBR Negotiation Done. We are the MASTER 00:59:42: OSPF: Send DBD to 10.70.70.70
on Serial0 seq 0x2126 opt 0x42 flag 0x3 len 72 00:59:42: OSPF: Send with youngest Key 1
00:59:42: OSPF: Send with youngest Key 1 00:59:42: OSPF: Database request to 10.70.70.70
00:59:42: OSPF: sent LS REQ packet to 192.168.64.10, length 12 00:59:42: OSPF: Rcv DBD from
10.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x1len 32 00:59:42: OSPF: Send
with youngest Key 1 00:59:42: OSPF: Send with youngest Key 1 00:59:42: OSPF: Rcv DBD from
```

```
10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Exchange Done with 10.70.70.70 on Serial0 00:59:42: OSPF: Synchronized with 10.70.70.70 on
Serial0, state FULL 00:59:42: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
LOADING to FULL, Loading Done 00:59:43: OSPF: Build router LSA for area 0, router ID
172.16.10.36, seq 0x80000010 00:59:43: OSPF: Send with youngest Key 1 00:59:45: OSPF: Send with
youngest Key 1 R1-2503#
```

Questo è l'output del comando **debug ip ospf adj** quando il tipo di autenticazione configurato sui router non corrisponde. In questo output viene mostrato che il router R1-2503 utilizza l'autenticazione di tipo 2 (MD5), mentre il router R2-2503 utilizza l'autenticazione di tipo 1 (autenticazione in testo normale).

```
R1-2503#debug ip ospf adj
00:59:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication type.

!--- Input packet specified type 1, you use type 2.
```

Questo è l'output del comando **debug ip ospf adj** quando gli ID delle chiavi usati per l'autenticazione non corrispondono. Questo output mostra che il router R1-2503 utilizza l'autenticazione MD5 con ID chiave 1, mentre il router R2-2503 utilizza l'autenticazione MD5 con ID chiave 2.

```
R1-2503#debug ip ospf adj
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - No message digest key 2 on interface
```

Questo output del comando **debug ip ospf adj** per R1-2503 mostra quando vengono configurate sia la chiave 1 che la chiave 2 per l'autenticazione MD5 come parte della migrazione.

```
R1-2503#debug ip ospf adj

00:59:43: OSPF: Send with youngest Key 1
00:59:53: OSPF: Send with youngest Key 2

!--- Informs that this router is also configured !--- for Key 2 and both routers now use Key 2.
01:00:53: OSPF: 2 Way Communication to 10.70.70.70 on Serial0, state 2WAY R1-2503#
```

Informazioni correlate

- Configurazione dell'autenticazione OSPF su un collegamento virtuale
- Perché il comando show ip ospf neighbors rivela i vicini nello stato Init?
- Comandi OSPF
- Esempi di configurazione OSPF
- Pagina di supporto per il routing IP
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).