Risoluzione dei problemi relativi al proxy su Cisco Secure Firewall Management Center (FMC)

Sommario

Introduzione

In questo documento viene descritta la configurazione di un proxy in FMC per consentire agli utenti di connettersi a Internet tramite un server intermedio, migliorando la protezione e talvolta migliorando le prestazioni. In questo articolo viene descritto come configurare un proxy in FMC e vengono forniti suggerimenti per la risoluzione dei problemi più comuni.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)

- Proxy

Componenti usati

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

- FMC 7.4.x

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.

Configurazione

Configurare Network http-proxy sull'interfaccia utente di FMC:

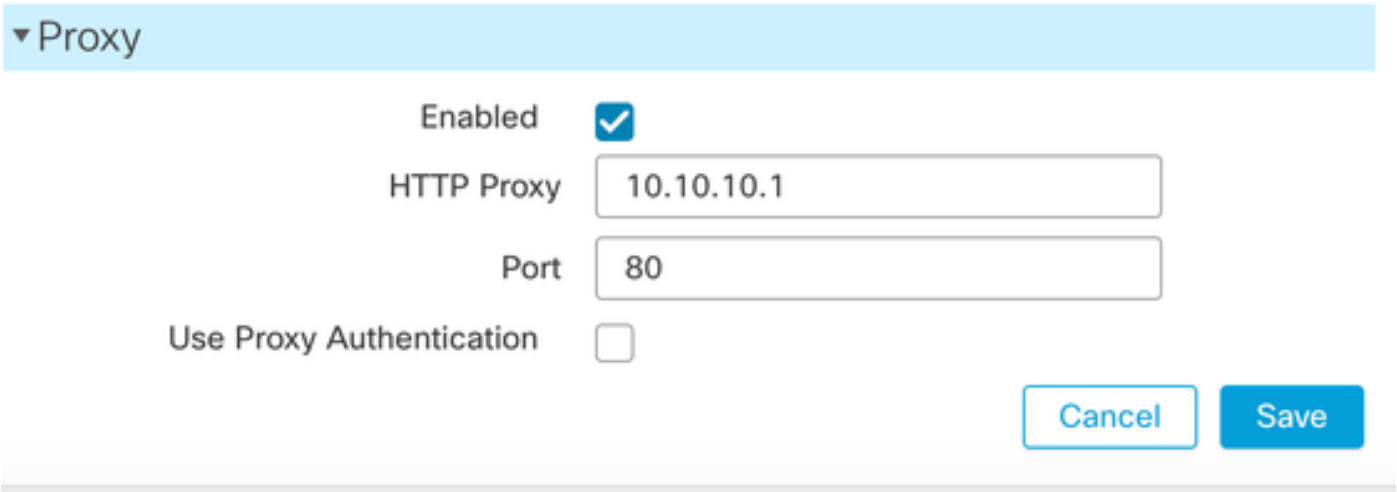
Login FMC GUI > Scegliere Sistema > Configurazione, quindi scegliere Interfacce di gestione.

Nota: I proxy che utilizzano l'autenticazione NTLM (NT LAN Manager) non sono supportati. Se si utilizza Smart Licensing, l'FQDN proxy non può contenere più di 64 caratteri.

Nell'area Proxy configurare le impostazioni del proxy HTTP.

Il centro di gestione è configurato per la connessione diretta a Internet sulle porte TCP/443 (HTTPS) e TCP/80 (HTTP). È possibile utilizzare un server proxy, al quale è possibile eseguire l'autenticazione tramite HTTP Digest.

- Selezionare la casella di controllo Attivato.
- Nel campo Proxy HTTP, immettere l'indirizzo IP o il nome di dominio completo del server proxy.
- Nel campo Porta, immettere un numero di porta.
- Fornire le credenziali di autenticazione scegliendoUsa autenticazione proxy, quindi fornire un nome utente e una password.
- Fare clic su Save (Salva).



Nota: Per la password proxy è possibile utilizzare A-Z, a-z e 0-9 e caratteri speciali.

Risoluzione dei problemi

Accedere alla CLI di FMC e alla modalità Expert, quindi verificare che iprep_proxy.conf garantisca la correttezza delle impostazioni proxy:

<#root>

```
admin@fmc:~$
cat /etc/sf/iprep_proxy.conf

iprep_proxy {
PROXY_HOST 10.10.10.1;
PROXY_PORT 80;
}
```

Controllare le connessioni attive per verificare la connessione proxy attiva:

<#root>

```
admin@fmc:~$
netstat -na | grep 10.10.10.1

tcp 0 0 10.40.40.1:40220 10.10.10.1:80
ESTABLISHED
```

Utilizzando il comando curl, verificare i dettagli della richiesta e la risposta dal proxy. Se si riceve la risposta: HTTP/1.1 200 Connessione stabilita, significa che il FMC ha inviato e ricevuto correttamente il traffico tramite il proxy.

<#root>

```
admin@fmc:~$
```

curl -x http://10.10.10.1:80 -I https://tools.cisco.com

HTTP/1.1 200 Connection established

Se sono stati configurati il nome utente e la password per il proxy, verificare l'autenticazione e la risposta del proxy:

```
curl -u proxyuser:proxypass --proxy http://proxy.example.com:80 https://example.com
```

Verifica

Connessione stabilita tramite proxy

Quando si esegue un comando curl con un proxy, ad esempio curl -x http://proxy:80 -I https://tools.cisco.com, si verifica una serie di interazioni di rete previste, che possono essere osservate tramite packet capture (tcpdump). Questa è una panoramica di alto livello del processo, arricchita da output tcpdump reali:

Avvio handshake TCP:
Il client (FMC) avvia una connessione TCP al server proxy sulla porta 80 inviando un pacchetto SYN. Il proxy risponde con un SYN-ACK e il client completa l'handshake con un ACK. In questo modo viene stabilita la sessione TCP su cui procede la comunicazione HTTP.

Output tcpdump di esempio:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Richiesta di connessione HTTP:
Una volta stabilita la connessione TCP, il client invia una richiesta HTTP CONNECT al proxy,

richiedendo di creare un tunnel per il server HTTPS di destinazione (tools.cisco.com:443). Questa richiesta consente al client di negoziare una sessione TLS end-to-end tramite il proxy.

Esempio di tcpdump (HTTP decodificato):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Conferma creazione connessione:
Il proxy risponde con una risposta HTTP/1.1 200 Connection stabilita, indicando che il tunnel verso il server di destinazione è stato creato correttamente. Questo significa che il proxy ora funge da inoltro, inoltrando il traffico crittografato tra il client e tools.cisco.com.

Esempio di tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

Comunicazione HTTPS tramite tunnel:
Dopo la risposta CONNECT, il client avvia l'handshake SSL/TLS direttamente con tools.cisco.com sul tunnel stabilito. Poiché questo traffico è crittografato, i contenuti non sono visibili nel dump del tcp, ma è possibile osservare la lunghezza e gli intervalli dei pacchetti, inclusi i pacchetti TLS Client Hello e Server Hello.

Esempio di tcpdump:

```
10:20:59.123456 IP client.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > client.54321: Flags [P.], length 1514 (Server Hello)
```

Gestione del reindirizzamento HTTP (302 trovato):
Nell'ambito della comunicazione HTTPS, il client richiede la risorsa all'indirizzo tools.cisco.com. Il server risponde con un reindirizzamento HTTP/1.1 302 Found a un altro URL (https://tools.cisco.com/healthcheck), che il client può seguire a seconda dei parametri e dello

scopo della richiesta. Sebbene questo reindirizzamento si verifichi all'interno della sessione TLS crittografata e non sia direttamente visibile, si tratta di un comportamento previsto che può essere osservato se il traffico TLS viene decrittografato.

Il traffico di reindirizzamento crittografato sarebbe simile al seguente:

```
10:21:00.123000 IP client.54321 > proxy.80: Flags [P.], length 517 (Encrypted Application Data)
10:21:00.123045 IP proxy.80 > client.54321: Flags [P.], length 317 (Encrypted Application Data)
```

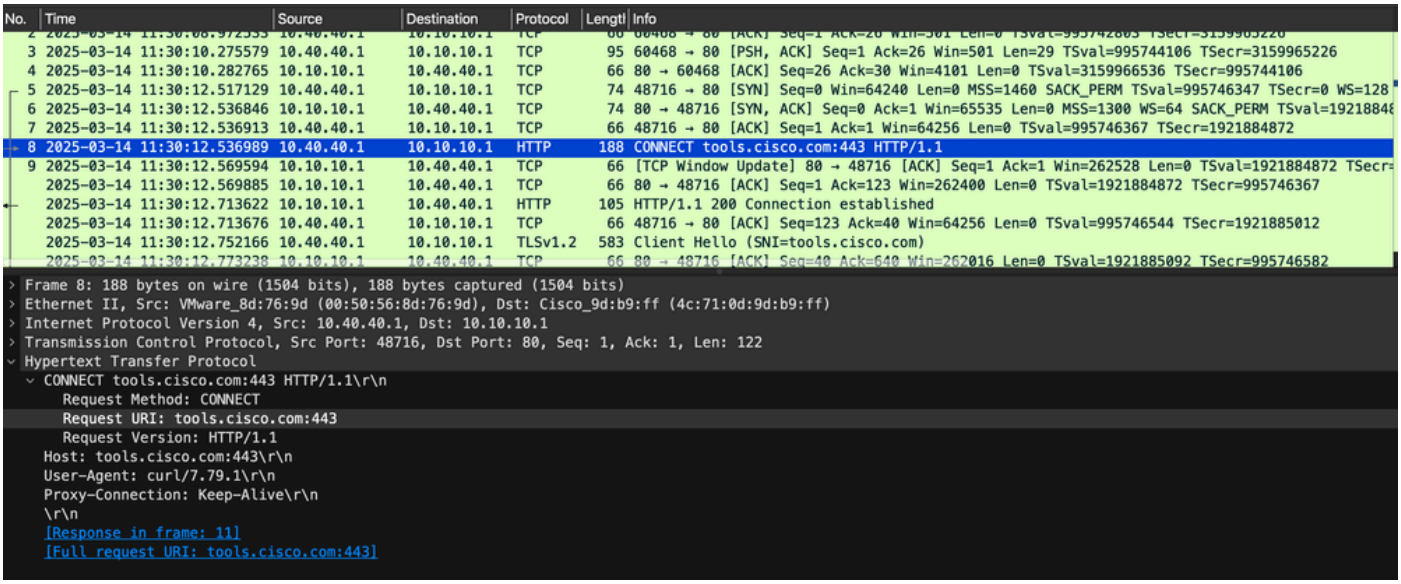
Interruzione connessione:
Una volta completato lo scambio, sia il client che il proxy chiudono normalmente la connessione TCP scambiando i pacchetti FIN e ACK, assicurando la corretta terminazione della sessione.

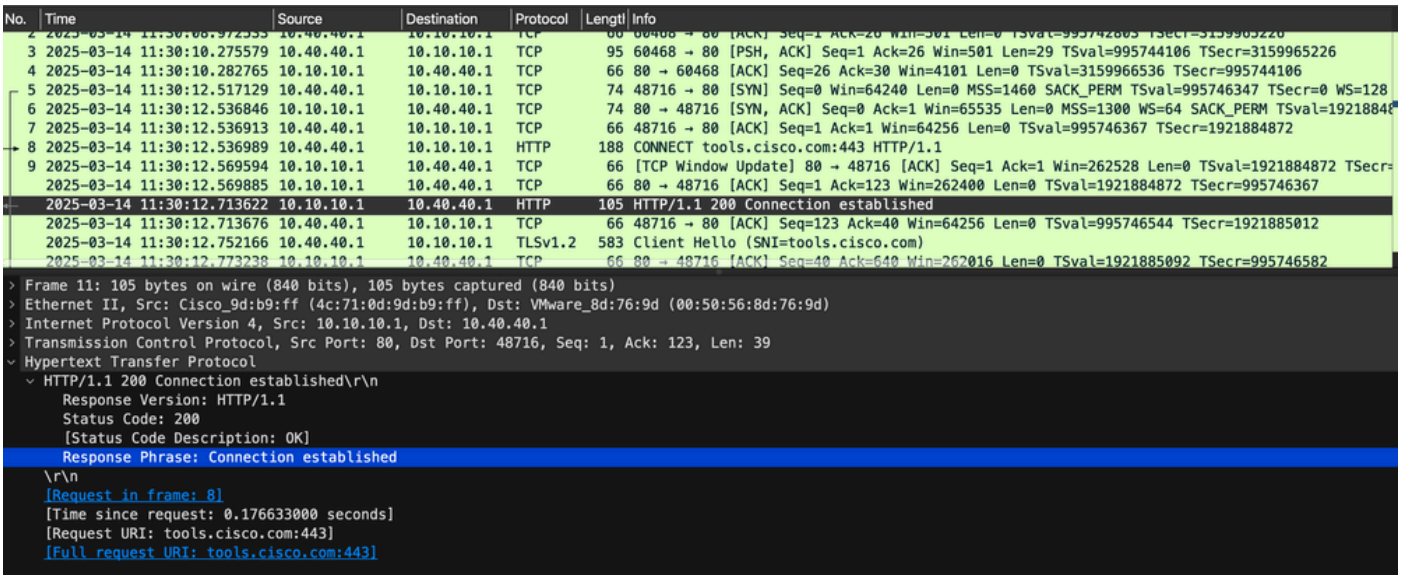
Output tcpdump di esempio:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

Suggerimento: Analizzando l'output tcpdump, è possibile verificare che la richiesta HTTPS tramite il proxy esplicito segua il flusso previsto: handshake TCP, richiesta CONNECT, definizione del tunnel, handshake TLS, comunicazione crittografata (inclusi eventuali reindirizzamenti) e chiusura regolare della connessione. Ciò conferma che l'interazione tra il proxy e il client funziona come previsto e aiuta a identificare eventuali problemi nel flusso, ad esempio errori nel tunneling o nella negoziazione SSL.

La FMC (10.40.40.1) stabilisce un handshake TCP riuscito con il proxy (10.10.10.1) sulla porta 80, seguito da una connessione HTTP al server (72.163.4.161) sulla porta 443. Il server risponde con un messaggio HTTP 200 Connection stabilito. L'handshake TLS viene completato e i dati vengono trasferiti correttamente. Infine, la connessione TCP termina normalmente (FIN).





Problemi noti

Restrizioni ACL proxy

Se esiste un problema di autorizzazioni (come un elenco degli accessi sul proxy), si può notare che attraverso l'acquisizione del pacchetto (tcpdump). Questa è una spiegazione dettagliata dello scenario di errore e degli output di esempio di tcpdump:

Avvio handshake TCP:
Il client (Firepower) si avvia stabilendo una connessione TCP al proxy sulla porta 80. L'handshake TCP (SYN, SYN-ACK, ACK) viene completato correttamente, ossia il proxy è raggiungibile.

Output tcpdump di esempio:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
```

```
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Richiesta di connessione HTTP:
Una volta connesso, il client invia una richiesta HTTP CONNECT al proxy, chiedendogli di creare un tunnel a tools.cisco.com:443.

Esempio di tcpdump (HTTP decodificato):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Risposta di errore dal proxy:

Anziché consentire il tunnel, il proxy nega la richiesta, probabilmente a causa di un elenco di accesso (ACL) che non consente questo traffico. Il proxy risponde con un errore come 403 Non consentito o 502 Gateway non valido.

Esempio di output tcpdump che mostra l'errore:

<#root>

```
HTTP/1.1
```

403

```
 Forbidden
Content-Type: text/html
Content-Length: 123
Connection: close
```

Interruzione connessione:
Dopo aver inviato il messaggio di errore, il proxy chiude la connessione ed entrambi i dispositivi scambiano i pacchetti FIN/ACK.

Output tcpdump di esempio:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

Suggerimento: Dalla pagina tcpdump è possibile notare che, anche se la connessione TCP e la richiesta HTTP CONNECT hanno avuto esito positivo, il proxy ha negato la configurazione del tunnel. Ciò in genere indica che il proxy ha un ACL o una restrizione di autorizzazione che impedisce il passaggio del traffico.

Download del proxy non riuscito (timeout/trasferimento incompleto)

In questo scenario, FMC si connette al proxy e avvia il download del file, ma il trasferimento si interrompe o non viene completato. Ciò è in genere dovuto all'ispezione del proxy, a timeout o a limiti di dimensioni dei file sul proxy.

Avvio handshake TCP
FMC avvia una connessione TCP al proxy sulla porta 80 e l'handshake viene completato correttamente.
Output tcpdump di esempio:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Richiesta di connessione HTTP
FMC invia una richiesta HTTP CONNECT al proxy per raggiungere la destinazione esterna.
Esempio di tcpdump (HTTP decodificato):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

Tunnel Establishment e TLS Handshake
Il proxy risponde con la connessione HTTP/1.1 200 stabilita, consentendo l'avvio dell'handshake TLS.

Output tcpdump di esempio:

<#root>

```
HTTP/1.1
```

```
200

 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Timeout o download incompleto
Dopo l'avvio del trasferimento dei file, il download si interrompe o non viene completato, determinando un timeout. La connessione rimane inattiva.
Le possibili cause includono:

- Ritardi nell'ispezione dei proxy o filtraggio.
- Timeout proxy per trasferimenti lunghi.
- Limiti delle dimensioni dei file imposti dal proxy.

Esempio di tcpdump che mostra inattività:

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440

# FMC sending data


# No response from proxy, connection goes idle...


# After a while, FMC may close the connection or retry.
```

Suggerimento: FMC avvia il download ma non riesce a completarlo a causa di timeout o trasferimenti incompleti, spesso causati da filtri proxy o restrizioni alle dimensioni dei file.

Il download del file Proxy non riesce (problema MTU)

In questo caso, FMC si connette al proxy e inizia a scaricare i file, ma la sessione ha esito negativo a causa di problemi di MTU. Questi problemi causano la frammentazione o la perdita di pacchetti, in particolare con file di grandi dimensioni o handshake SSL/TLS.

Avvio handshake TCP
FMC avvia l'handshake TCP con il proxy, operazione che riesce.
Output tcpdump di esempio:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
```

```
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Richiesta CONNECT HTTP e definizione tunnel
La console centrale del servizio invia una richiesta di connessione HTTP e il proxy risponde, consentendo la creazione del tunnel.
Esempio di tcpdump (HTTP decodificato):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

Inizio handshake TLS
FMC e tools.cisco.com avviano la negoziazione di SSL/TLS e vengono scambiati i pacchetti iniziali.
Output tcpdump di esempio:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Frammentazione o eliminazione dei pacchetti a causa dell'MTU
Quando il FMC o il server tentano di inviare pacchetti di grandi dimensioni, i problemi MTU causano la frammentazione o la perdita dei pacchetti, con conseguenti errori di trasferimento file o di negoziazione TLS.
Questo si verifica in genere quando l'MTU tra FMC e il proxy (o tra il proxy e Internet) è impostata in modo errato o è troppo piccola.
Esempio di tcpdump che mostra il tentativo di frammentazione:

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440
```

 # Large packet

```
10:21:00.456123 IP proxy.80 > fmc.54321: Flags [R], seq X, win 0, length 0
# Proxy resets connection due to MTU issue
```

Suggerimento: Il problema dell'MTU determina pacchetti scartati o frammentati che interrompono l'handshake TLS o impediscono il download dei file. Questa condizione si verifica in genere quando l'ispezione SSL o la frammentazione del pacchetto viene effettuata a causa di impostazioni MTU non corrette.

In uno scenario di errore, FMC ottiene CONNECT senza HTTP 200, con ritrasmissioni e FIN che confermano l'assenza di scambio TLS/dati, probabilmente a causa di problemi MTU o di problemi proxy/upstream.

Quando si utilizza l'URL, è possibile che vengano visualizzati vari codici di risposta HTTP che indicano problemi sul lato server o errori di autenticazione. Di seguito sono elencati i codici di errore più comuni e il relativo significato:

Codice HTTP	Significato	Causa
400	Richiesta non valida	Sintassi richiesta non corretta
401	Non autorizzato	Credenziali mancanti o non corrette
403	Non consentito	Accesso negato
404	Non trovato	Risorsa non trovata
500	Errore interno	Errore del server
502	Gateway non valido	Errata comunicazione del server
503	Servizio non disponibile	Sovraccarico o manutenzione del server
504	Timeout gateway	Timeout tra i server

Riferimenti

Note sulla versione di Cisco Secure Firewall Threat Defense, versione 7.4.x

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).