Configurazione della protezione da attacchi sul router VPN RV132W o RV134W

Obiettivo

La protezione dagli attacchi consente di proteggere la rete da tipi di attacchi comuni, ad esempio rilevamenti, allagamenti e tempeste di eco. Mentre per impostazione predefinita la protezione da attacchi è abilitata sul router, è possibile regolare i parametri per rendere la rete più sensibile e più reattiva agli attacchi rilevati.

Lo scopo di questo articolo è quello di mostrare come configurare la protezione dagli attacchi sull'RV132W e sul RV134W VPN Router.

Dispositivi interessati

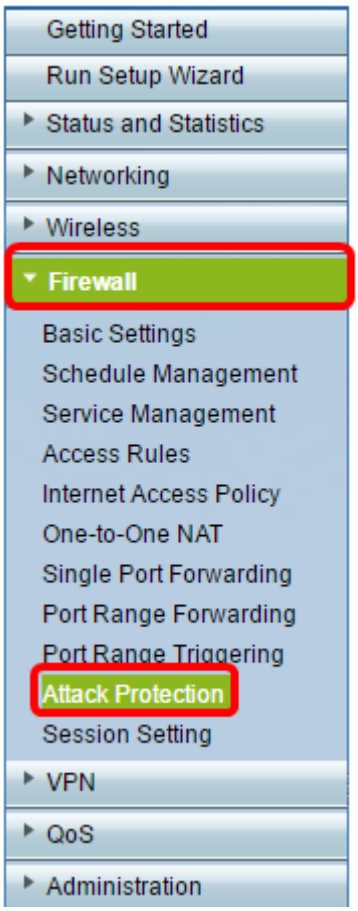
- RV 132 W
- RV134W

Versione del software

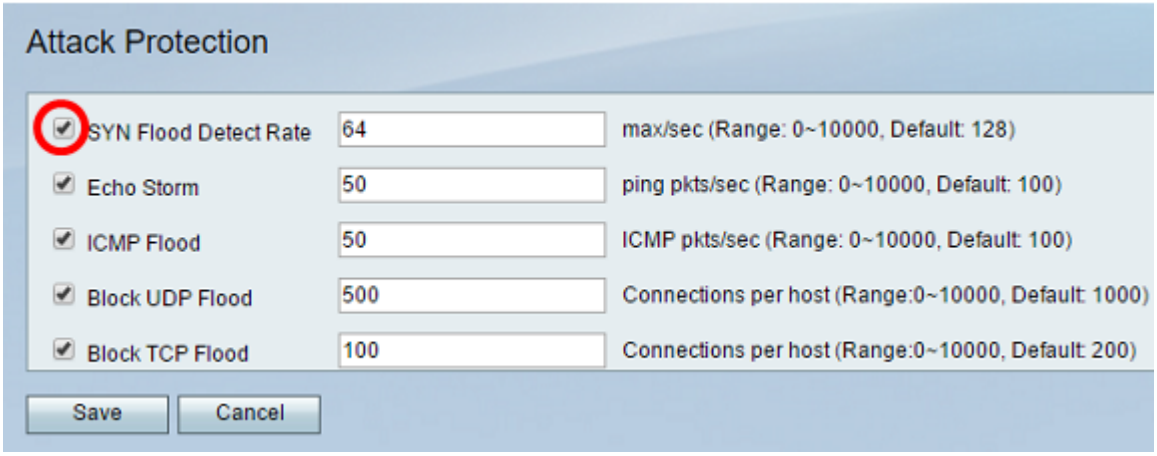
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

Configura protezione da attacchi

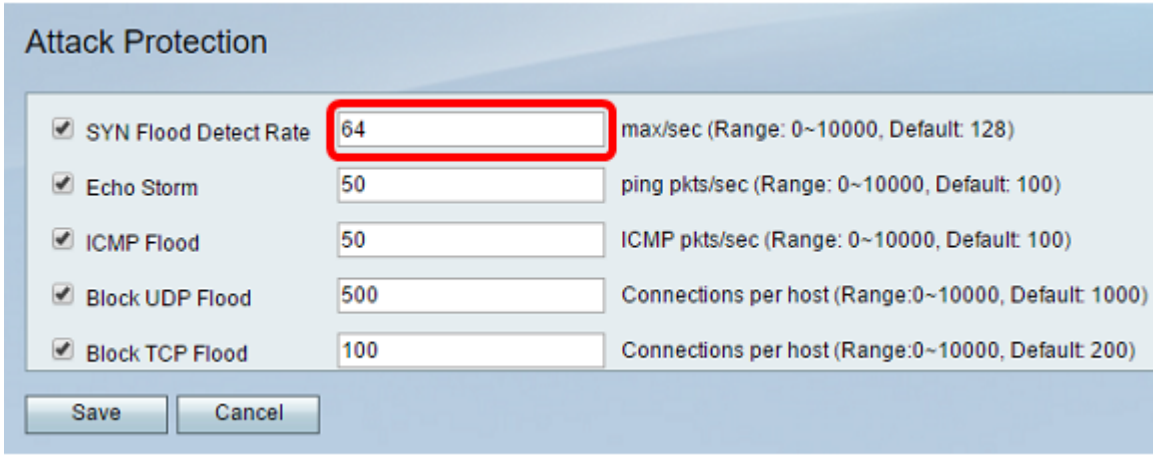
Passaggio 1. Accedere all'utility basata sul Web e scegliere **Firewall > Protezione da attacchi** .



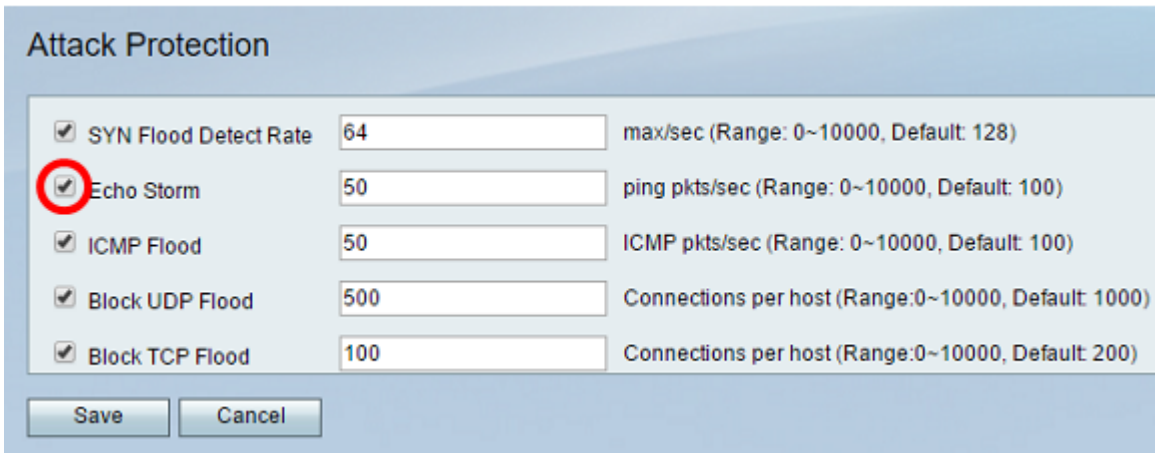
Passaggio 2. Verificate che la casella di controllo SYN Flood Detect Rate sia selezionata per garantire che la feature sia attiva. Questa opzione è selezionata per impostazione predefinita.



Passaggio 3. Immettere un valore nel campo *SYN Flood Detect Rate*. Il valore predefinito è 128 pacchetti SYN al secondo. È possibile immettere un valore compreso tra 0 e 10000. Il numero di pacchetti SYN al secondo che causano l'individuazione di un'intrusione SYN da parte dell'appliance di sicurezza. Il valore zero indica che la funzione SYN Flood Detection è disabilitata. In questo esempio, il valore immesso è 64. Significa che l'appliance rileva un'intrusione SYN a soli 64 pacchetti SYN al secondo, rendendolo più sensibile della configurazione predefinita.

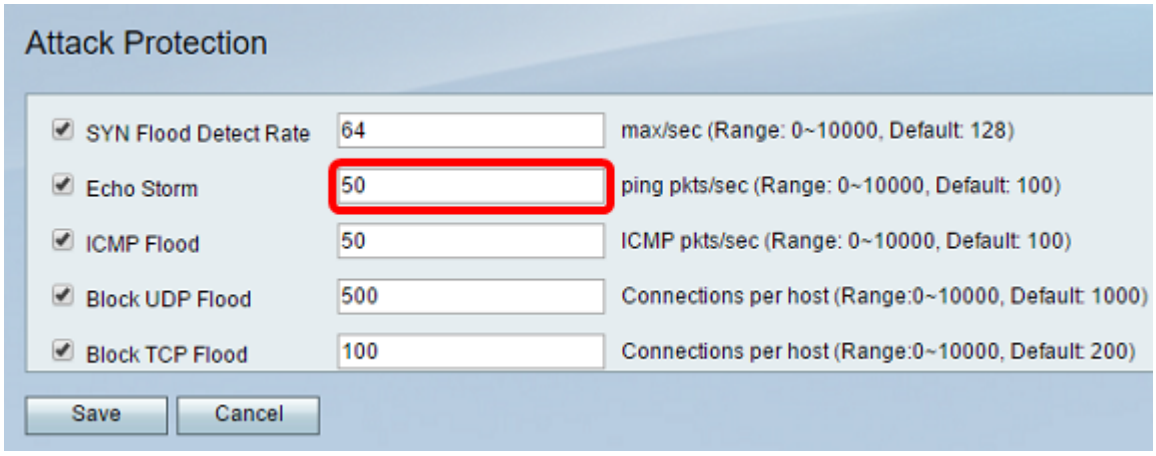


Passaggio 4. Verificate che la casella di controllo Tempesta di eco (Echo Storm) sia selezionata per garantire che la feature sia attiva. Questa opzione è selezionata per impostazione predefinita.

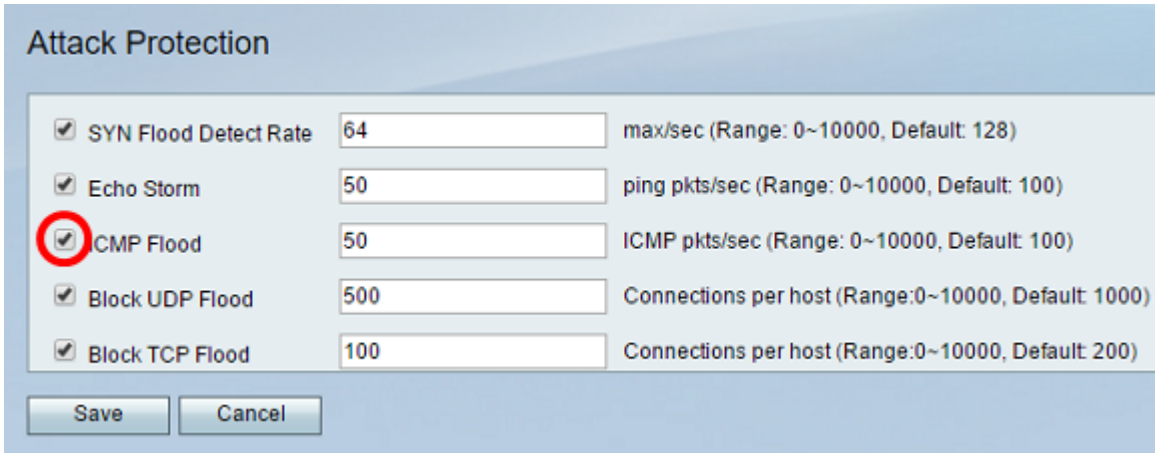


Passaggio 5. Immettere un valore nel campo *Tempesta di eco*. Il valore predefinito è 100 ping al secondo. È possibile immettere un valore compreso tra 0 e 10000. Il numero di ping al secondo che causano la rilevazione da parte dell'appliance di sicurezza di un evento di intrusione echo storm. Il valore zero indica che la funzione Tempesta di eco è disattivata.

Nota: nell'esempio, l'accessorio rileva un evento Echo Storm a soli 50 ping al secondo.

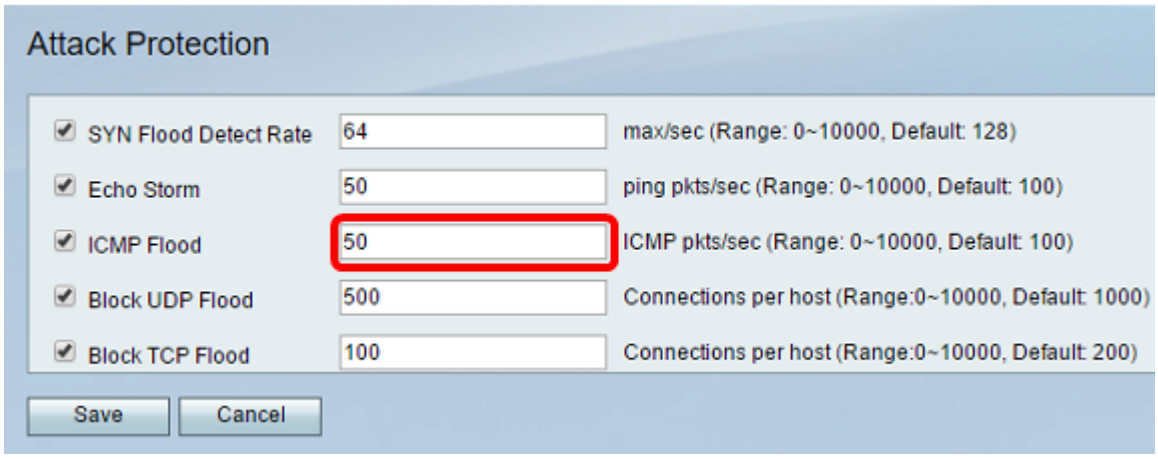


Passaggio 6. Verificare che la casella di controllo Inondazione ICMP (Internet Control Message Protocol) sia selezionata per assicurarsi che la funzionalità sia attiva. Questa funzione è selezionata per default.

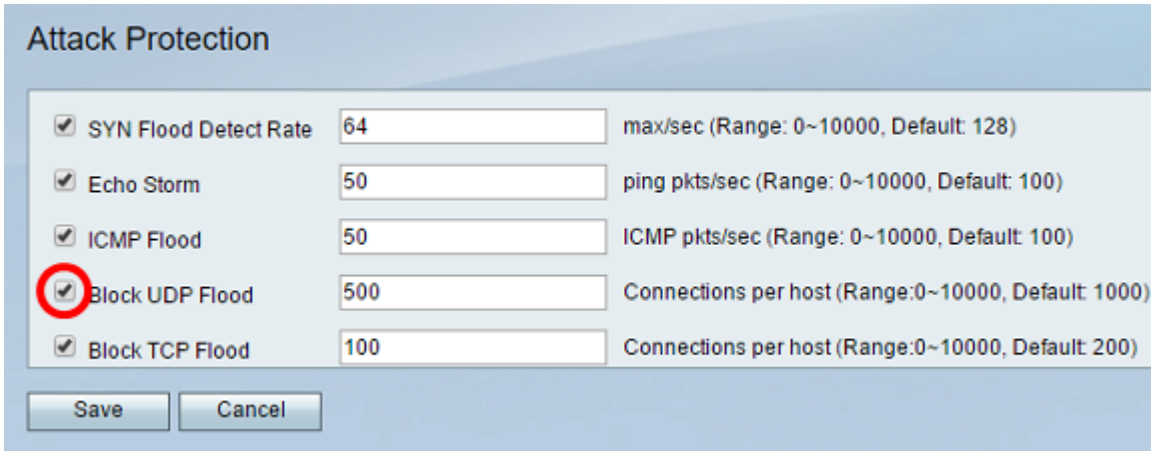


Passaggio 7. Immettere un valore numerico nel campo *ICMP Flood*. Il valore predefinito è 100 pacchetti ICMP al secondo. È possibile immettere un valore compreso tra 0 e 10000. Il numero di pacchetti ICMP al secondo che determina il rilevamento da parte dell'appliance di sicurezza di un evento di intrusione all'inondazione ICMP. Il valore zero indica che la funzione ICMP Flood è disabilitata.

Nota: nell'esempio, il valore immesso è 50, quindi è più sensibile al flooding ICMP rispetto all'impostazione predefinita.

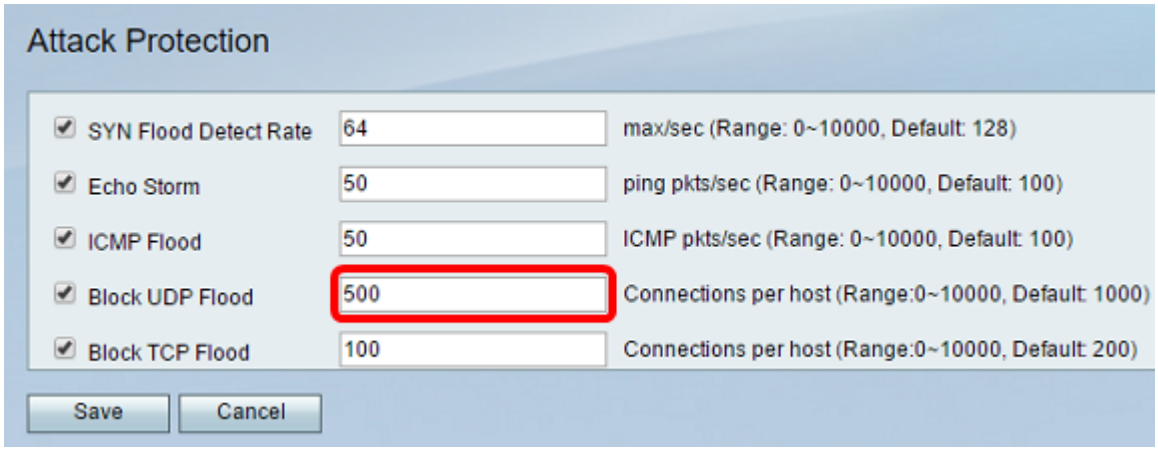


Passaggio 8. Verificare che la casella di controllo Blocca allagamento UDP sia selezionata per verificare che la funzionalità sia attiva e per impedire che l'appliance di sicurezza accetti più di 150 connessioni UDP (User Datagram Protocol) attive simultanee al secondo da un singolo computer della LAN. Questa opzione è selezionata per default.

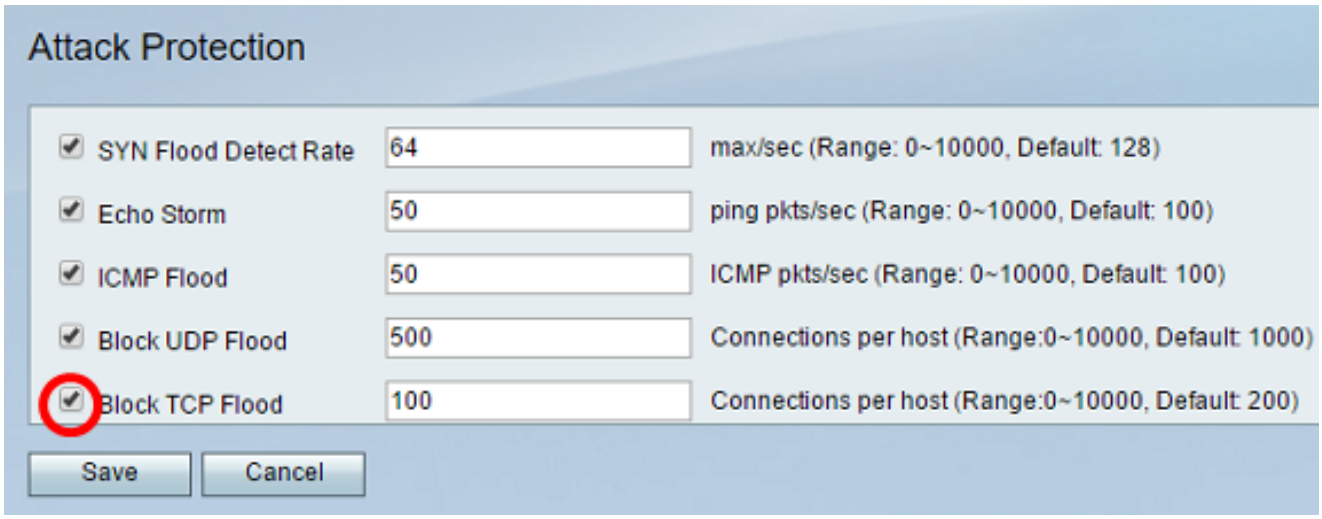


Passaggio 9. Immettere un valore compreso tra 0 e 10000 nel campo *Blocca flusso UDP*. Il valore predefinito è 1000. In questo esempio, il valore immesso è 500, che lo rende più

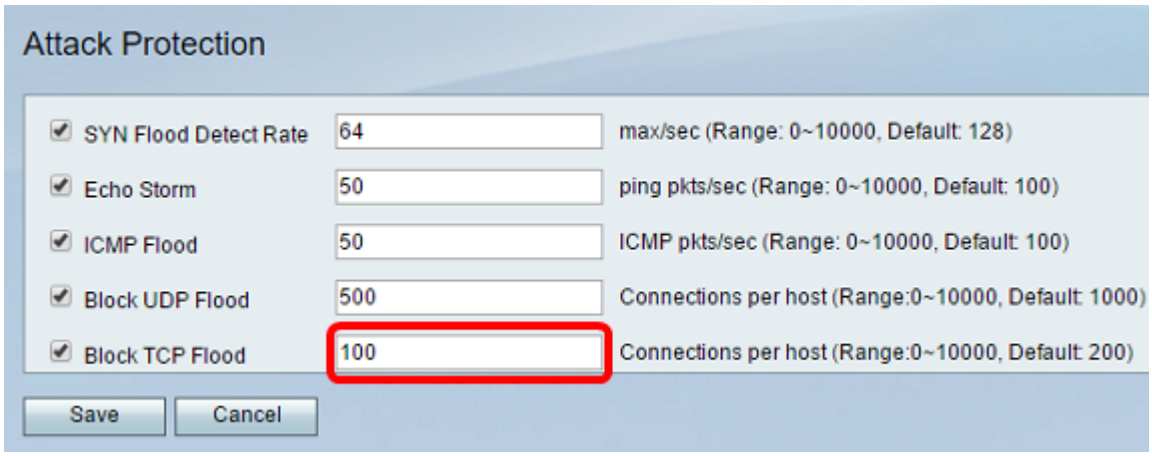
sensibile.



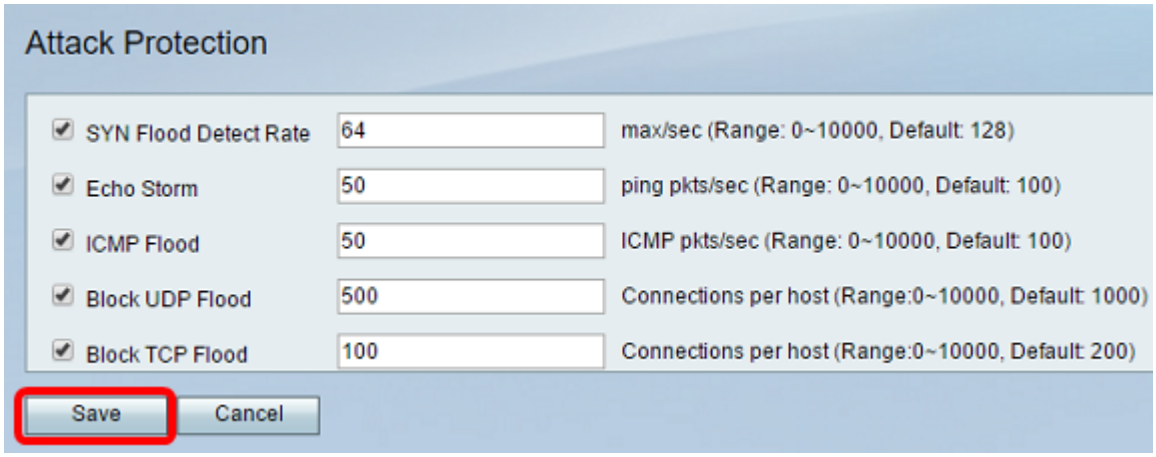
Passaggio 10. Verificare che la casella di controllo Blocca flusso TCP sia selezionata per eliminare tutti i pacchetti TCP (Transmission Control Protocol) non validi. Questa opzione è selezionata per default.



Passaggio 11. Immettere un valore compreso tra 0 e 10000 nel campo *Blocca TCP Flood* per proteggere la rete da un attacco di tipo SYN Flood. Il valore predefinito è 200. Nell'esempio, viene immesso 100, che lo rende più sensibile.



Passaggio 12. Fare clic su **Salva**.



A questo punto, è necessario configurare la protezione dagli attacchi sul router RV132W o RV134W.

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).