Configura tunnel VPN da sito a sito basato su route su FTD Gestito da FMC

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Limitazioni e restrizioni
Procedura di configurazione in FMC
Verifica
Dalla GUI FMC
Da CLI FTD

Introduzione

In questo documento viene descritto come configurare un tunnel VPN da sito a sito basato su route statica su Firepower Threat Defense gestito da Firepower Management Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza base del funzionamento di un tunnel VPN.
- Comprendere come spostarsi all'interno del CCP.

Componenti usati

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

- Cisco Firepower Management Center (FMC) versione 6.7.0
- Cisco Firepower Threat Defense (FTD) versione 6.7.0

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.

Premesse

La VPN basata su route consente di determinare il traffico interessante da crittografare o inviare tramite tunnel VPN e di utilizzare il routing del traffico anziché policy/elenchi degli accessi, come nella VPN basata su policy o su crypto-map. Il dominio di crittografia è impostato per consentire tutto il traffico in entrata nel tunnel IPsec. I selettori di traffico locale e remoto IPsec sono impostati su 0.0.0.0/0.0.0.0. Ciò significa che tutto il traffico indirizzato nel tunnel IPsec viene crittografato, a prescindere dalla subnet di origine/destinazione.

Nel documento si fa riferimento alla configurazione SVTI (Static Virtual Tunnel Interface). Per la configurazione di Dynamic Virtual Tunnel Interface (DVTI) su Secure Firewall, fare riferimento a questo <u>documento</u>.

Limitazioni e restrizioni

Di seguito sono riportati i limiti e le restrizioni noti per i tunnel basati su route su FTD:

- Supporta solo IPsec. GRE non supportato.
- Supporta solo interfacce IPv4, IPv4, reti protette o payload VPN (nessun supporto per IPv6).
- Il routing statico e solo il protocollo BGP Dynamic Routing è supportato per le interfacce VTI che classificano il traffico per la VPN (nessun supporto per altri protocolli come OSPF, RIP e così via).
- Sono supportate solo 100 VTI per interfaccia.
- VTI non è supportato in un cluster FTD.
- VTI non è supportato in questi criteri:

QoS NAT · Impostazioni piattaforma

Questi algoritmi non sono più supportati in FMC/FTD versione 6.7.0 per i nuovi tunnel VPN (FMC supporta tutte le cifrature rimosse per gestire FTD < 6.7):

- Crittografia 3DES, DES e NULL non supportata nei criteri IKE.
- I gruppi DH 1, 2 e 24 non sono supportati nei criteri IKE e nelle proposte IPSec.

- Integrità MD5 non supportata nei criteri IKE.
- PRF MD5 non è supportato nei criteri IKE.
- Gli algoritmi di crittografia DES, 3DES, AES-GMAC, AES-GMAC-192 e AES-GMAC-256 non sono supportati nella proposta IPsec.

Nota: ciò vale sia per i tunnel VPN basati su route da sito a sito che per quelli basati su criteri. Per aggiornare un FTD precedente alla versione 6.7 da FMC, viene attivato un controllo di pre-convalida che avvisa l'utente delle modifiche relative alle cifrature rimosse che bloccano l'aggiornamento.

FTD 6.7 gestito tramite FMC 6.7	Configurazione disponibile	Tunnel VPN da sito a sito		
Nuova installazione	Sono disponibili cifrari deboli, ma non possono essere utilizzati per configurare il dispositivo FTD 6.7.	Sono disponibili cifrari deboli, ma non possono essere utilizzati per configurare il dispositivo FTD 6.7.		
Aggiornamento: FTD configurato solo con cifratura debole	Aggiornamento da FMC 6.7 UI, un controllo di pre-convalida visualizza un errore. L'aggiornamento è bloccato fino alla riconfigurazione.	Dopo l'aggiornamento FTD e presupponendo che il peer non abbia modificato le proprie impostazioni, il tunnel viene terminato.		
Aggiornamento: FTD configurato solo con alcune cifrature deboli e alcune cifrature forti	Aggiornamento da FMC 6.7 UI, un controllo di pre-convalida visualizza un errore. L'aggiornamento è bloccato fino alla riconfigurazione.	Dopo l'aggiornamento del FTD e presupponendo che il peer disponga di cifrature efficaci, il tunnel viene ristabilito.		
Aggiornamento: paese di classe C (non si dispone di una licenza di crittografia efficace)	Consenti DES è consentito	Consenti DES è consentito		



Nota: non sono necessarie licenze aggiuntive. La VPN basata su route può essere configurata in modalità Licensed e Evaluation. Senza la conformità alla crittografia (funzionalità di esportazione controllate abilitate), solo DES può essere utilizzato come algoritmo di crittografia.

Procedura di configurazione in FMC

Passaggio 1. Passare a Dispositivi > VPN > Sito-sito.

Overview Analysis	Policies	Devic	es Obj	jects	AMP Inte	lligence		
Device Management	NAT	VPN 🔻	QoS	Pla	form Settings	FlexConfig	Certificates	
		Site To	Site					
View By : Group	-	Remote Trouble	Access shooting	D)	Warning (0)	Offline (0) N	ormal (1) Depl	loymer

Passaggio 2. Fare clic su Add VPN (Aggiungi VPN), quindi selezionare Firepower Threat Defense Device, come mostrato nell'immagine.

S	Deploy	System	Help 🔻	admin 🔻
			A (2)	dd VPN 👻
	Fire	epower Dev	ice	
<i>i</i>	Fire	epower Thre	eat Defense	e Device

Passaggio 3. Fornire un nome di topologia e selezionare il tipo di VPN come VTI (Route Based). Scegliere la versione IKE.

Ai fini della presente dimostrazione:

Nome topologia: VTI-ASA

Versione IKE: IKEv2

○ Policy Based (Crypto Map) ● Route Based (VTI) Network Topology: ➡ Point to Point ★ Hub and Spoke ◆ Full Mest	Topology Name:*	VTI-ASA		
Network Topology: Point to Point & Hub and Spoke Full Mesi		O Policy Based (Cryp	oto Map) 💿 Route Ba	ased (VTI)
	Network Topology:	↔ Point to Point	* Hub and Spoke	💠 Full Mesh
IKE Version:*	IKE Version:*	🗌 IKEv1 🗹 IKEv2		

Passaggio 4. Selezionare il dispositivo su cui configurare il tunnel, scegliere di aggiungere una nuova interfaccia di modello virtuale (fare clic sull'icona +) oppure selezionarne una dall'elenco esistente.

ndpoints	IKE	IPsec	Advanced			
	Node A			Node B		
Device:				Device:*		
FTD		*		Empty	*	
Virtual 1	funnel Interface:*	1		Virtual Tunnel Interface:*	~	0
Tunne	I Source IP is Private	Edit VI		Tunnel Source IP is Private	Edit VTI	~
Connect	ion Type:*			Connection Type:*		
Bidirecti	onal	*		Bidirectional	*	
Tunnel I Tunnel S Tunnel S	IP Address Source Interface Source Interface IP	:		Tunnel IP Address : Tunnel Source Interface : Tunnel Source Interface IP :		

Passaggio 5. Definire i parametri della nuova interfaccia del tunnel virtuale. Fare clic su OK.

Ai fini della presente dimostrazione:

Nome: VTI-ASA

Descrizione (Facoltativa): tunnel VTI con ASA Extranet

Area di sicurezza: VTI-Zone

ID tunnel: 1

Indirizzo IP: 192.168.100.1/30

Origine tunnel: Gigabit Ethernet0/0 (esterna)

Add Virtual Tunnel	Interface	?
General		
Name *:	VTI-ASA	nabled
Description:	VTI Tunnel with Extranet ASA	
Security Zone:	VTI-Zone	
Tunnel ID *:	1 Ran	ge: 0 - 10413
IP Address *:	192.168.100.1/30	
Tunnel Source *:	GigabitEthernet0/0 (Outside)	
	_	
		OK Cancel

Passaggio 6. Fare clic su OK nel popup per indicare che la nuova VTI è stata creata.



Passaggio 7. Selezionare la VTI appena creata o una VTI esistente in Virtual Tunnel Interface. Fornire le informazioni per il nodo B (che è il dispositivo peer).

Ai fini della presente dimostrazione:

Dispositivo: Extranet

Nome dispositivo: ASA-Peer

Indirizzo IP endpoint: 10.106.67.252

81	Create New VPN Topo	logy					? ×
	Topology Name:*	VTI-ASA					
l		O Policy Based (C	rypto Map) 💿 Rout	e Based (V	(IT)		
l	Network Topology:	++ Point to Poir	Hub and Spo	oke 💠 Fi	ull Mesh		
l	IKE Version:*	🗆 IKEv1 🗹 IKEv	2				
l							
	Endpoints IKE	IPsec	Advar	nced			
	No Device:* FTD	de A	×		Node B Device:* Extranet	¥	
	Virtual Tunnel Inte VTI-ASA	rface:*	Contraction Contraction		Device Name*: ASA-Peer		
l	Connection Type:* Bidirectional		¥		10.106.67.252		
	Tunnel IP Address Tunnel Source Inte Tunnel Source Inte	: 192.1 erface : Outsi erface IP : 10.19	l68.100.1 de 97.224.90				
	Additional Configure Route traffic to the Permit VPN traffic	ration (1) 2 VTI : <u>Routi</u> : <u>AC P</u>	<u>ng Policy</u> blicy				
						Save	Cancel

Passaggio 8. Passare alla scheda IKE. È possibile scegliere di utilizzare un criterio predefinito oppure fare clic sul pulsante + accanto alla scheda Criterio per crearne uno nuovo.

IKEv2 Settings	_	
Policy:*	AES-GCM-NULL-SHA-LATEST	0
Authentication Type:	Pre-shared Automatic Key	_
Pre-shared Key Length:*	24 Characters (Range 1-127)	

Passaggio 9. (Facoltativo, se si crea un nuovo criterio IKEv2.) Fornire un nome per il criterio e selezionare gli algoritmi da utilizzare nel criterio. Fare clic su Save (Salva).

Ai fini della presente dimostrazione:

Nome: ASA-IKEv2-Policy

Algoritmi di integrità: SHA-512

Algoritmi di crittografia: AES-256

Algoritmi PRF: SHA-512

Gruppo Diffie-Hellman: 21

ew IKEv2 Policy			?
Name:*	ASA-IKEv2-Policy		
Description:			
Priority:	1	(1-65535)	
Lifetime:	86400	seconds (120-2147483647)	
Integrity Algorithms	Available Algorithms	Selected Algorithms	
Encryption Algorithms PRF Algorithms Diffie-Hellman Group	MD5 SHA SHA SHA512 SHA256 SHA384 SHA384 NULL	Add	
		Save	Cancel

Passaggio 10. Scegliere il nuovo criterio o il criterio esistente. Selezionare il tipo di autenticazione. Se si utilizza una chiave manuale già condivisa, specificare la chiave nelle caselle Chiave e Conferma chiave.

Ai fini della presente dimostrazione:

Criterio: ASA-IKEv2-Policy

Tipo di autenticazione: chiave manuale già condivisa

Chiave: cisco123

Chiave di conferma: cisco123

indpoints IKE		IPsec	Advanced	
KEv1 Settings				
Policy:*	nechana	d cha acc256 db1	4.2	
Folicy.	presnare	u_sna_aeszbo_uni	*_3	<u> </u>
Authentication Type:	Pre-share	ed Automatic Key	1	·
Pre-shared Key Length:*	24	Characters	(Range 1-127	')
Policy:*	ASA-IKE	/2-Policy		• •
Authentication Type:	Pre-share	ed Manual Key	1	*
Key:*	•••••			
Confirm Key:*	•••••			
	Enforc	e hex-based pre-sh	ared key only	

Nota: se entrambi gli endpoint sono registrati sullo stesso FMC, è possibile utilizzare anche l'opzione di chiave automatica precondivisa.

Passaggio 11. Passare alla scheda IPSec. È possibile scegliere di utilizzare una proposta IPSec IKEv2 predefinita o crearne una nuova. Fare clic sul pulsante Modifica accanto alla scheda Proposta IPSec IKEv2.

Crypto Map Type:	Static Opynamic						
IKEv2 Mode:	Tunnel	-					
Transform Sets:	IKEv1 IPsec Proposals 🥜		IKEv2 IPsec Proposals* 🥜				
	tunnel_aes256_sha		AES-GCM				
Enable Security Association (SA) Strength Enforcement							

Passaggio 12. (Facoltativo, se si crea una nuova proposta IPSec IKEv2.) Fornire un nome per la proposta e selezionare gli algoritmi da utilizzare nella proposta. Fare clic su Save (Salva).

Ai fini della presente dimostrazione:

Nome: ASA-IPSec-Policy

Hash ESP: SHA-512

Crittografia ESP: AES-256

Name:* ASA-IPSec-Policy Description: ESP Hash ESP Encryption Available Algorithms Selected Algorithms AES-256 AES-256 AES-256 AES-92 Add AES Sign AES-GCM AES	New IKEv2 IPsec P	roposal		?
ESP Hash ESP Encryption Available Algorithms AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES-GCM AES DES AES-GMAC-256	Name:*	ASA-IPSec-Policy		
ESP Encryption	ESP Hash	Available Algorithms	Selected Algorithms	
AES-256 AES-GCM-192 AES-192 AES-GCM AES AES AES Add Add	ESP Encryption	AES-GCM-256	AES-256	0
AES-GCM-192 AES-192 AES-GCM AES-GCM AES Add Add Add Add Add Add Add Ad				
AES-GCM AES AES AES Add Add Add Add Add Add Add Ad		@ AES-GCM-192		
AES Constraints of the second		AES-GCM	Add	
DES AES-GMAC-256		AES		
DES AES-GMAC-256		ig 3DES		
AES-GMAC-256		🔅 DES		
		AES-GMAC-256		
			Save	Cancel

Passaggio 13. Scegliere la proposta o la proposta appena creata dall'elenco delle proposte disponibili. Fare clic su OK.

on:*	IKEv2 IPsec Proposal			? ×
ł	Available Transform Sets C		Selected Transform Sets	
D Tr	 AES-GCM AES-SHA 	Ĺ		
e.	ASA-IPSec-Policy			
26	@ DES_SHA-1	Add		
Sec				
Perl				
s G				
ura:			ок	Cancel
CG1.				

Passaggio 14. (Facoltativo) Scegliere le impostazioni Perfect Forward Secrecy. Configurare Durata IPSec e Dimensione durata.

Ai fini della presente dimostrazione:

Perfect Forward Secrecy: Gruppo di moduli 21

Durata: 28800 (predefinita)

Dimensione durata: 4608000 (predefinita)

Ļ	Enable Security Ass	sociation (SA) Stre	ength Enforce	ement
L	Enable Perfect Forv	vard Secrecy		
L	Modulus Group:	21	~	
L	Lifetime Duration*:	28800		Seconds (Range 120-2147483647)
L	Lifetime Size:	4608000		Kbytes (Range 10-2147483647)
ľ	- ESPv3 Settings	1		

Passaggio 15. Controllare le impostazioni configurate. Fare clic su Save (Salva), come mostrato nell'immagine.

Topology Name:*	VTI-ASA					
		Based (Crypto Ma	p) 🖲 Route Based (VTI)			
Network Topology	/: ← Poir	t to Point 😤	Hub and Spoke 💠 Full Mesh			
IKE Version:*	IKEv1	IKEv2				
Endpoints	IKE	IPsec	Advanced			
Crypto Map Type:	Static O Dy	namic				
IKEv2 Mode:	Tunnel	×				
Transform Sets:	IKEv1 IPsec Prop	oosals 🥜	IKEv2 IPsec Proposals* 🥜			
	tunnel_aes256_	sha	ASA-IPSec-Policy			
Enable Security	Association (SA) Str	ength Enforceme	nt			
Enable Perfect F	orward Secrecy					
Modulus Group	21	*				
Lifetime Duration*	28800	Se	econds (Range 120-2147483647	7)		
Lifetime Size:	4608000	KI	oytes (Range 10-2147483647)			
— ▼ ESPv3 Settir	ngs					
					Save	Cancel

Passaggio 16. Configurare i criteri di controllo di accesso. Passare a Policy > Controllo accesso > Controllo accesso. Modificare il criterio applicato all'FTD.

Nota: il protocollo allow-vpn della connessione syspot non funziona con tunnel VPN basati su route. Le regole di controllo d'accesso devono essere configurate sia per le zone IN-> OUT che per le zone OUT -> IN.

Specificare le zone di origine e di destinazione nella scheda Zone.

Specificare le reti di origine e di destinazione nella scheda Reti. Fare clic su Add.

Ai fini della presente dimostrazione:

Zone di origine: zona interna e zona esterna

Zone di destinazione: zona esterna e zona interna

Reti di origine: in rete e rete remota

Reti di destinazione: rete remota e in rete

Add Rule					? ×
Name VTI-Traffic		Enabled	Insert into Mand	atory	~
Action Allow	V 00.8	rh.F			
Time Range None					
Zones Networks VLAN Tags 🛆 Users	Applications	Ports URLs SGT/	SF Attributes	Inspection Loggi	ng Comments
Available Zones C		Source Zones (2)		Destination Zones (2)	
Search by name		In-Zone	8	In-Zone	5
In-Zone		Out-Zone	9	Out-Zone	9
Out-Zone	L	2			
VTI-Zone	Add to Source				
	Add to				
	Destination				
Add Rule					? X
Name VTI-Traffic		Enabled	Insert into Mand	atory	~
Action		eka 📑			
Time Range None					
Zones Networks VLAN Tags 🔺 User	s Applications	Ports URLs SGT/	ISE Attributes	Inspection Logo	ing Comments
Available Networks C		Source Networks (2)		Destination Networks (2)	
]	Source	Original Client	📰 In-Netwrk	
Networks Geolocation		📻 In-Netwrk	8	Remote-Network	8
IPv4-Private-172.16.0.0-12		Remote-Network	6		
Pv4-Private-192.168.0.0-16	Add To Source				
Private-All-RFC1918	Networks				
IPv6-IPv4-Mapped	Add to Destination				
IPvo-unk-Local IPvo-unk-Local-Addresses					
IPv6-to-IPv4-Relay-Anvcast					
Remote-Network					
VTI-ASA-Tunnel		Enter an IP address	Add	Enter an IP address	Add
				Add	Cancel

Passaggio 17. Aggiungere il routing sul tunnel VTI. Selezionare Dispositivi > Gestione dispositivi. Modificare il dispositivo su cui è configurato il tunnel VTI.

Passare a Instradamento statico nella scheda Instradamento. Fare clic su Aggiungi instradamento.

Fornire l'interfaccia, scegliere la rete, fornire il gateway. Fare clic su OK.

Ai fini della presente dimostrazione:

Interfaccia: VTI-ASA

Rete: rete remota

Gateway: tunnel VTI-ASA

Add Static Ro	ute Configuratio	n			? ×
Type: Interface*	IPv4 O IPv6 VTI-ASA (Interface starting wi	ith this icon 👩	▼ signifies it is a	vailable for rout	e leak)
Available Net	thmark-Tests Local cast ite-10.0.0.0-8 ite-172.16.0.0-12 ite-192.168.0.0-1 ite-All-RFC1918	Add	Selected	Network te-Network	
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel	fault Route)	 (1 - 254) (254))	
			(ок	Cancel

Passaggio 18. Passare a Distribuisci > Distribuzione. Selezionare l'FTD in cui distribuire la configurazione e fare clic su Distribuisci.

Push della configurazione nella CLI FTD dopo la corretta distribuzione:

<#root>
crypto ikev2 policy 1
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400

```
crypto ikev2 enable Outside
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2
tunnel-group 10.106.67.252 type ipsec-121
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4
```

tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

Verifica

Dalla GUI FMC

Fare clic sull'opzione Check Status (Verifica stato) per monitorare lo stato del tunnel VPN dalla GUI stessa



Ciò include questi comandi presi dalla CLI FTD:

- show crypto ipsec sa peer <Indirizzo IP peer>
- show vpn-sessiondb detail I2I filter ipaddress <Indirizzo IP peer>

😑 extranet : ASA-Peer 🛛 🖓		• FTD/VTI-ASA
> show crypto ipsec sa peer	T	> show crypto ipsec sa peer 10.106.67.252
Not applicable for extranet peer		<pre>peer address: 10 106 67 252 Crypto map tag:vti-crypto-map-4-0-1, seq num: 65280, local addr: 10.197.224.90 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.106.67.252 #pkts encaps: 100, #pkts decrypt: 100, #pkts digest: 100 #pkts compressed: 0, #pkts decrypt: 100, #pkts verify: 100 #pkts compressed: 0, #pkts decrypt: 0, #pkts verify: 100 #pkts compressed: 0, #pkts decrypt: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.224.90/500, remote crypto endpt.: 10.106.67.252/500</pre>
show vpn-sessiondb detail l2l filter ipaddress	Ĩ	> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252
Not applicable for extranet peer		Session Type: LAN-to-LAN Detailed Connection : 10.106.67.252 Index : 44 IP Addr : 10.106.67.252 Protocol : IKEV2 IPsec Encryption : IKEV2: (1)AES256 IPsec: (1)AES256 Hashing : IKEV2: (1)SHA512 IPsec: (1)SHA512 Bytes Tx : 10000 Login Time : 03:54:57 UTC Thu Nov 12 2020 Duration : 0h:02m:12s Tunnel Zone : 0 IKEV2 Tunnels: 1 IPsec Tunnels: 1 IKEV2: Tunnel TD : 44.1
		UNDE STC Port : 500 Rem Auth Mode: preSharedKeys Loc Auth Mode: preSharedKeys Encryption : AES256 Rekey Int (T): 86400 Seconds PRF : SHA512 D/H Group : 21 Refresh Close

Da CLI FTD

Questi comandi possono essere usati dalla CLI di FTD per visualizzare la configurazione e lo stato dei tunnel VPN.

show running-config crypto
show running-config nat

show running-config route show crypto ikev1 sa detailed show crypto ikev2 sa detailed show crypto ipsec sa detailed show vpn-sessiondb detail 121

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).