Konfigurieren des 802.11w Management Frame Protection auf dem WLC

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Management MIC Information Element (MMIE) Änderungen an RSN IE Vorteile des 802.11w Management Frame Protection Voraussetzungen für 802.11w Konfigurieren GUI CLI Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument werden Details zum IEEE 802.11w Management Frame Protection und seiner Konfiguration auf dem Cisco Wireless LAN Controller (WLC) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco WLC mit Code 7.6 oder höher verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf WLC 5508, der Code 7.6 ausführt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der 802.11w-Standard soll Kontroll- und Management-Frames sowie eine Reihe robuster Management-Frames vor Fälschungs- und Replay-Angriffen schützen. Zu den geschützten Frametypen gehören Frames zur Aufhebung der Zuordnung, zur Deauthentifizierung und zur robusten Aktion, z. B.:

- Spektrum-Management
- Quality of Service (QoS)

- Bestätigung blockieren
- Funkmessung
- Fast Basic Service Set (BSS)-Umstellung

802.11w verschlüsselt die Frames nicht, schützt jedoch die Management-Frames. Es stellt sicher, dass die Nachrichten aus legitimen Quellen stammen. Dazu müssen Sie ein MIC-Element (Message Integrity Check) hinzufügen. 802.11w hat einen neuen Schlüssel eingeführt, den Integrity Group Temporal Key (IGTK), der für den Schutz robuster Broadcast-/Multicast-Management-Frames verwendet wird. Dies wird als Teil des Vier-Wege-Handshake-Prozesses abgeleitet, der mit Wireless Protected Access (WPA) verwendet wird. Daher ist der dot1x/Pre-Shared Key (PSK) eine Voraussetzung für die Verwendung von 802.11w. Es kann nicht mit einem offenen/webauthentischen Service Set Identifier (SSID) verwendet werden.

Wenn der Management Frame Protection ausgehandelt wird, verschlüsselt der Access Point (AP) die GTKund IGTK-Werte im EAPOL-Key-Frame, der in Meldung 3 des 4-Wege-Handshakes übermittelt wird. Wenn der WAP später den GTK ändert, sendet er den neuen GTK und IGTK unter Verwendung des Group Key Handshake an den Client. Es fügt ein MIC hinzu, das mithilfe des IGTK-Schlüssels berechnet wird.

Management MIC Information Element (MMIE)

In 802.11w wird ein neues Informationselement eingeführt, das Management MIC-Informationselement. Es hat das Header-Format, wie im Bild gezeigt.

1	1	2	6	8
Element ID	Length	KeylD	IPN	MIC

Die wichtigsten Problemfelder sind hierbei die **Element-ID** und das **MIC**. Die Element-ID für MMIE ist 0x4c und dient als nützliche Identifizierung, wenn Sie die Wireless-Aufnahmen analysieren.

Hinweis: MIC: Dieser enthält den Integritätscode der Nachricht, der über den Management-Frame berechnet wird. Beachten Sie, dass dies am Access Point hinzugefügt wird. Der Ziel-Client berechnet dann das MIC für den Frame neu und vergleicht es mit den Daten, die vom Access Point gesendet wurden. Wenn sich die Werte unterscheiden, wird dies als ungültiger Frame zurückgewiesen.

Änderungen an RSN IE

Robust Security Network Information Element (RSN IE) legt die vom WAP unterstützten Sicherheitsparameter fest. Mit 802.11w wird RSN IE ein Group Management Cipher Suite-Selektor hinzugefügt, der den vom Access Point verwendeten Cipher Suite-Selektor zum Schutz robuster Broadcast-/Multicast-Management-Frames enthält. Dies ist die beste Methode, um zu erfahren, ob ein AP 802.11w unterstützt. Dies kann auch überprüft werden, wie im Bild gezeigt.

<u>File Edit View Go Capture Analyze</u>	Statistics Telephony Tools Interna	ls <u>H</u> elp				
0 0 💉 🔳 🔬 🗁 🗶 🤁	। ् 🗢 🔿 🖗 🛃 🗐 🗍		2 🗸 🗹 🥵 💥 🛛			
Filter: wlan_mgt.ssid == "PMF"	💌 Eq	pression Clear Ap	ply Save			
802.11 Channel: 💌 Channel Offset: 💌 FCS	Filter: All Frames Vone	▪ Wireless Settings	Decryption Keys			
No. Time Source	Destination D	SCP Protocol VLAN	I Length Info			
43 0.97510900 cisco_21:c9:7	4 IntelCor_20:52:b8	802.11	285 Probe Response,	SN=127, FN=0, Flags-	•R, BI=102	, SSID=PMF[Ma
68 1.20985500 c1sco_21:c9:7	4 IntelCor_20:52:b8	802.11	285 Probe Response,	SN=132, FN=0, Flags-	R, BI=102	, SSID=PMF[Ma
108 2.07189800 C1sco_21:c9:7	4 Broadcast	802.11	291 Beacon frame, St	N=3969, FN=0, Flags=.	BI=102,	SSID=PMF[Mal
122 2 15696900 C1sc0_21:C9:7	b IntelCor_20:52:68	802.11	201 Beacon frame St	SN=74, FN=0, Flags=.	R, BI=102, 87-102	SSID=PMF[Ma]
217 5.98307800 C1sco_21:09:7	4 IntelCor 20:52:68	802.11	285 Probe Response.	SN=137, EN=0, Flags=.	BT=102,	SSTD#PMF [Mar
241 6.19374400 c1sco_21:c9:7	4 IntelCor_20:52:b8	802.11	285 Probe Response.	SN=142, FN=0, Flags-	BI=102	. SSID=PMF[Ma
271 8.00264200 Cisco_21:c9:7	4 IntelCor_20:52:b8	802.11	285 Probe Response,	SN=166, FN=0, Flags-	R, BI=102	, SSID=PMF[Ma
272 8 00658300 cisco 21:c9:7	4 TotelCor 20:52:b8	802 11	285 Prohe Resnonse	SN=167 EN=0 Elaos-	R RT=102	SSTD=PMC Ma
B Tag: HT Capabilities (80) Tag: RSN Information Tag Number: RSN Information Tag Number: RSN Information RSN Version: 1 B Group Cipher Suite: 00- Pairwise Cipher Suite: 00- Pairwise Cipher Suite: 00- Pairwise Cipher Suite: 00- Auth Key Management (A) B Auth Key Management (A) RSN Capabilities: 0x000 0. 0. 0. 	<pre>2.11n D1.10) ation (48) -Of-ac (Ieee8021) AES (CCM) Dount: 1 fist 00-Of-ac (Ieee8021) AES (M) Suite Count: 1 (M) List 00-Of-ac (Ieee8021) 28 = RSN Pre-Auth capabilities = RSN No Pairwise capabilit = RSN GTKSA Replay Counter = Management Frame Protecti = Management Frame Protecti = PeerKey Enabled: False = Suite: 00-Of-ac (Ieee8021 peer Suite out: 00-Of-ac (Ieee8021) </pre>	S (CCM)) WPA (SHA256) : Transmitter (ies: Transmitt capabilities: 4 capabilities: 4 on Required: Tr on Capable: Tru 0 BIP ee8021)	does not support pre-aut er can support WEP defau i replay counters per Pl i replay counters per Pl ue ue	thentication ult key 0 simultaneou TKSA/GTKSA/STAKeySA (TKSA/GTKSA/STAKeySA (isly with Pairwise 0x0002) 0x0002)	key
Group Management Cipi Tag: Extended Supported P	ter Suite type: BIP (6) Rates 24, 36, 48, 54, [Mbit,	/sec]				

Hier finden Sie das Feld Group Management Cipher Suite, das anzeigt, dass 802.11w verwendet wird.

Auch bei den RSN-Funktionen wurden Änderungen vorgenommen. Die Bits 6 und 7 werden jetzt verwendet, um verschiedene Parameter für 802.11w anzugeben.

- Bit 6: Management Frame Protection Required (MFPR) Ein STA setzt dieses Bit auf 1, um anzukündigen, dass der Schutz von robusten Management-Frames obligatorisch ist.
- Bit 7: Management Frame Protection Capable (MFPC) Ein STA setzt dieses Bit auf 1, um anzukündigen, dass der Schutz von robusten Management-Frames aktiviert ist. Wenn der Access Point diese Einstellung festlegt, informiert er, dass er den Management-Frame-Schutz unterstützt.

Wenn Sie den Management-Frame-Schutz gemäß den Konfigurationsoptionen festlegen, werden sowohl Bit 6 als auch Bit 7 festgelegt. Dies ist im folgenden Bild der Paketerfassung dargestellt.

Filter	wlan_mg	gt.ssid == "PMF"				Expression Clear	r Apply Sa	ive						
802.11	Channel:	- Channel Offset:	FCS Filter: A	All Frames	- None	▼ Wireless Set	tings Deci	ryption Keys						
No.	Time	Source		Destination		DSCP Protocol	VLAN Lengt	th Info						
	43 0.97	510900 Cisco_	21:c9:74	IntelCor.	_20:52:b8	802.11	2	85 Probe	Response,	SN=127,	, FN=0,	Flags=.	R	., BI
	68 1.20	985500 cisco_	21:c9:74	IntelCor,	_20:52:b8	802.11	2	85 Probe	Response,	SN=132,	, FN=0,	Flags=,	R	., BI
1	.08 2.07	189800 cisco_	21:c9:74	Broadcas	t	802.11	2	91 Beacon	frame, s	N=3969,	FN=0,	Flags=		, BI=
1	17 2.14	027800 Cisco_	21:c9:7b	IntelCor	_20:52:b8	802.11	2	85 Probe	Response,	SN=74,	FN=0,	Flags=	R	, BI=
1	.22 2.15	696900 C1sco_	21:c9:7b	Broadcas	t	802.11	2	91 Beacon	frame, s	N=3185,	FN=0,	Flags=		, BI=
2	17 5.98	307800 Cisco_	21:c9:74	IntelCor.	_20:52:b8	802.11	2	85 Probe	Response,	SN=137,	, FN=0,	Flags=.	R	., BI
2	41 6.19	374400 C1sco_	21:c9:74	IntelCor.	_20:52:68	802.11	2	85 Probe	Response,	SN=142,	, FN=0,	Flags=.	R	., BI
	71 8.00	264200 C1sco_	21:c9:74	IntelCor.	_20:52:b8	802.11	2	85 Probe	Response,	SN=166,	, FN=0,	Flags=.	R	., BI
4	77 8 00	658300 01500	21 • 29 • 74	IntelCor	20-52-68	802 11	- 7	85 Prohe	Resnonse	SN=167	EN=0	Flags	P	BI
		LIN												
	Tag:	HT Capabiliti	les (802.11n	p1.10)										
	E Tag:	RSN Informati	ion											
	Тар	Number: RSN	Information	(48)										
	Tag	length: 26												
	RSN	Version: 1												
	🖃 Gro	up Cipher Sui	te: 00-0f-ad	c (Ieee802	1) AES (CO	:M)								
	G	roup cipher s	uite OUI: OC	0-0f-ac (I	eee8021)									
	G	roup cipher s	Suite type: /	AES (CCM)	(4)									
	Pai	rwise cipher	Suite Count:	: 1										
	🖃 Pai	rwise Cipher	Suite List (00-0f-ac (Ieee8021)	AES (CCM)								
	🖻 P	airwise Ciphe	er Suite: 00-	-Of-ac (Ie	ee8021) AE	ES (CCM)								
		Pairwise Cip	oher Suite Ol	JI: 00-0f-	ac (Ieee80	021)								
		Pairwise Cip	wher Suite ty	/pe: AES (CCM) (4)									
	Aut	h Key Manager	ient (AKM) SL	uite Count	: 1									
	Aut	n Key Managem	lent (AKM) L1	1st 00-0f-	ac (Ieee80)21) WPA (SHA2	56)							
	RSN	Capab111t1es	: 0x00e8						_					
			0 = RSN	Pre-Auth	capabi lit:	les: Transmitt	er does r	not suppor	rt pre-au	thentica	tion	1		
			= RSN	NO Pairwi	se capabi	Intres: Transm	itter car	1 support	WEP dera	uit key	0 simu	Itaneous	siy with	Pairs
			10 = RSN	PIKSA Rep	Tay Counte	er capabilitie	s: 4 rep	lay counte	ers per P	TKSA/GTK	SA/STA	Keysa (U	JX0002)	
	· · ·	10	/ = KSN	GIKSA KEP	ay counte	er capabilitie	з. ч гер	ay counte	ers per P	INSA/GTR	SA/STA	READA (O	00002)	
		1	= Mana	agement Fr	ame Protec	tion Canable:	True	1						
				Key Enabl	and Frotes	cron capable:	nue	1						
	•		= Peer	ney chabi	ees raise									

Wenn Sie diese Einstellung jedoch auf "optional" setzen, wird nur das Bit 7 gesetzt, wie im Bild gezeigt.

File Edit View Go Capture Analyze Statistics 7	Telephony Tools Internals Help			
◎ ◎ ∡ ■ ∡ 🖻 🖺 ೫ 😂 ९, ♦	🗢 🥥 🐺 👱 🗐 🗐 🔍 Q Q 🛛] 🏭 🗹 🥵 🖗 💢		
Filter: wlan_mgt.ssid == "PMF"	Expression Clear App	ly Save		
802.11 Channel: 👻 Channel Offset: 💌 FCS Filter: All Fra	ames 👻 None 💌 Wireless Settings	Decryption Keys		
No. Time Source Des	stination DSCP Protocol VLAN	Length Info		
35 2.00590100 Cisco_21:c9:7b In	itelCor_20:52:b8 802.11	279 Probe Response, SN=4	59, FN=0, Flags=R, BI	=102, SSID=PMF[Ma
36 2.00630400 C1sco_21:c9:7b Br	oadcast 802.11	285 Beacon frame, SN=230	6, FN=0, Flags= BI=	102, SSID=PMF[Mal
130 5.47209300 C15C0_21:C9:74 BF	0adcast 802.11	285 Beacon Trame, SN=257	, FN=0, Flags=, BI=1	-102, SSID=PMF[Mair]
161 5 89994000 Cisco 21:09:74 8r	roadcast 802.11	279 Probe Response, SN=0 285 Reacon frame SN=777	EN=0 Elans=	02 SSTD=DME[Ma]f
186 6,51628200 Cisco_21:c9:74 Br	oadcast 802.11	285 Beacon frame, SN=306	, FN=0, Flags= BI=1	02, SSID=PMF[Ma]f
<				
m rau, councily intermactor, councily	CODE 03. ENVILOPMENT ANY			
⊞ Tag: QBSS Load Element 802.11e CC	A Version			
■ Tag: HT Capabilities (802.11n D1.)	.10)			
— Tag: RSN Information				
Tag Number: RSN Information (48	3)			
Tag length: 20				
RSN Version: 1				
Group Cipher Suite: 00-0F-ac (I	(eees021) AES (CCM)			
Pairwise Cipher Suite Count: 1	AF 25 (10000000) AFE (654)			
Muth Key Management (AVM) Suite	n-ac (reeebuzz) AES (CCM)			
E Auth Key Management (AKM) List	00-Of-ac (Ieee8021) WPA			
RSN Capabilities: 0x00a8	to an at (receiver) with			
0 = RSN Pre	-Auth capabilities: Transmitter do	pes not support pre-authent	cation	
	Pairwise capabilities: Transmitter	can support WEP default ke	ey 0 simultaneously with Pair	wise key
10 = RSN PTK	(SA Replay Counter capabilities: 4	replay counters per PTKSA/0	STKSA/STAKEYSA (0x0002)	
= RSN GTK	(SA Replay Counter capabilities: 4	replay counters per PTKSA/G	STKSA/STAKeySA (0x0002)	
0 = Managem	ient Frame Protection Required: Fal	ise		
1 = Managem	ient Frame Protection Capable: True	2		
0 = Peerkey	/ Enabled: False			
H Tag: HT Information (802.11n D1.1	10)			
I TAG: CISCO COXE CREP + DEVICE NAM	le			

Hinweis: Der WLC fügt diese modifizierte RSN IE den Zuordnungs-/Neuzuordnungs-Antworten hinzu, und der AP fügt diese modifizierte RSN IE den Beacons und den Test-Antworten hinzu.

Vorteile des 802.11w Management Frame Protection

• Client-Schutz

Dies wird durch die Hinzufügung von kryptographischem Schutz zu Deauthentifizierungs- und Dissoziationsframes erreicht. Auf diese Weise wird verhindert, dass ein nicht autorisierter Benutzer einen Denial of Service (DOS)-Angriff starten kann, indem er die MAC-Adresse legitimer Benutzer manipuliert und die Frames zur Deaktivierung/Aufhebung der Zuordnung sendet.

• AP-Schutz

Der infrastrukturseitige Schutz wird durch einen Abbruchschutz der Security Association (SA) ergänzt, der aus einer Association Comeback Time und einer SA-Query-Prozedur besteht. Wenn ein WAP vor 802.11w entweder eine Assoziations- oder eine Authentifizierungsanforderung von einem bereits verknüpften Client empfangen hat, beendet er die aktuelle Verbindung und startet dann eine neue Verbindung. Wenn Sie 802.11w MFP verwenden und der STA zugeordnet ist und über einen Management Frame Protection verhandelt hat, lehnt der AP die Zuordnungsanfrage mit dem Rückgabestatuscode 30 ab. Association request rejected temporarily; Try again later an den Client gesendet.

In der Antwort auf die Zuordnung ist ein Informationselement für die Comeback-Zeit der Zuordnung enthalten, das eine Comeback-Zeit angibt, zu der der WAP bereit ist, eine Zuordnung zu diesem STA zu akzeptieren. Auf diese Weise können Sie sicherstellen, dass legitime Clients nicht aufgrund einer gefälschten Zuordnungsanforderung getrennt werden.

Hinweis: Der WLC (AireOS oder 9800) ignoriert die Trennung bzw. Aufhebung der Authentifizierung von Frames, die von den Clients gesendet werden, wenn diese keine 802.11w-PMF verwenden. Der Client-Eintrag wird beim Empfang eines solchen Frames erst dann gelöscht, wenn der Client PMF verwendet. Auf diese Weise soll ein Denial of Service durch bösartige Geräte vermieden werden, da diese Frames ohne PMF keine Sicherheit bieten.

Voraussetzungen für 802.11w

- Für 802.11w muss die SSID mit dot1x oder PSK konfiguriert werden.
- 802.11w wird von allen 802.11n-fähigen Zugangspunkten unterstützt. Das bedeutet, dass AP 1130 und 1240 802.11w nicht unterstützen.
- In Version 7.4 wird 802.11w auf Flexconnect AP und 7510 WLC nicht unterstützt. Unterstützung wurde seit Version 7.5 hinzugefügt.

Konfigurieren

GUI

Schritt 1: Sie müssen den geschützten Management-Frame unter der mit 802.1x/PSK konfigurierten SSID aktivieren. Sie haben drei Optionen, wie im Bild dargestellt.

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'PMF'
WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 1 WPA+WPA2 MAC Filtering 2 Fast Transition Fast Transition Protected Management Frame PMF WPA+WPA2 Parameters WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption AES TKIP Authentication Key Management 802.1X Enable CCKM Enable PSK Enable

'Erforderlich' gibt an, dass ein Client, der 802.11w nicht unterstützt, keine Verbindung herstellen darf. 'Optional' gibt an, dass selbst Clients, die 802.11w nicht unterstützen, eine Verbindung herstellen dürfen.

Schritt 2: Anschließend müssen Sie den Comeback-Timer und den SA-Abfragetimeout angeben. Der Comeback-Timer gibt die Zeit an, die ein verbundener Client warten muss, bevor die Zuordnung erneut versucht werden kann, wenn er zum ersten Mal mit einem Statuscode 30 abgelehnt wird. Der SA-Abfragetimeout gibt an, wie lange der WLC auf eine Antwort des Clients für den Abfrageprozess wartet. Wenn der Client nicht antwortet, wird seine Zuordnung vom Controller gelöscht. Dies geschieht wie im Bild gezeigt.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK						
WLANs	WLANs > Edit 'PMF'						
VLANS	General Security QoS Advanced						
Advanced	Layer 2 Layer 3 AAA Servers						
	Layer 2 Security 🙍 WPA+WPA2 🔻						
	MAC Filtering?						
	Fast Transition Fast Transition						
	Protected Management Frame						
	PMF Required *						
	Comeback timer(1- 20msec) 1						
	SA Query Timeout(100- 500msec) 200						
	WPA+WPA2 Parameters						
	WPA Policy						
	WPA2 Policy						
	WPA2 Encryption RAES TKIP						
	Authentication Key Management						

Schritt 3: Sie müssen 'PMF 802.1x' aktivieren, wenn Sie 802.1x als Methode zur Verwaltung von Authentifizierungsschlüsseln verwenden. Wenn Sie PSK verwenden, müssen Sie das Kontrollkästchen **PMF PSK** aktivieren, wie im Bild gezeigt.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'PMF'
VLANS	General Security QoS Advanced
▶ Advanced	Layer 2 Layer 3 AAA Servers Sht Query Timeout[100- Soumsec) 200 WPA+WPA2 Parameters WPA2 Policy Image: Constraint of the second sec
	FT PSK Enable PMF 802.1X Enable PMF PSK Enable
	WPA gtk-randomize Disable Disable

CLI

• Führen Sie den folgenden Befehl aus, um die 11w-Funktion zu aktivieren oder zu deaktivieren:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

• Führen Sie den folgenden Befehl aus, um geschützte Management-Frames zu aktivieren oder zu deaktivieren:

config wlan security pmf optional/required/disable

• Zeiteinstellungen für das Comeback der Zuordnung:

config wlan security pmf 11w-association-comeback

• Timeout-Einstellungen für SA-Abfragewiederholung:

config wlan security pmf saquery-retry-time

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die 802.11w-Konfiguration kann überprüft werden. Überprüfen Sie die WLAN-Konfiguration:

(wlc)>show wlan 1	
Wi-Fi Protected Access (WPA/WPA2)	Enabled
<snip></snip>	
802.1x Enable	ed
PSK Disabl	.ed
CCKM Disabl	.ed
FT-1X(802.11r) Disabl	.ed
FT-PSK(802.11r) Disabl	.ed
PMF-1X(802.11w) Enable	ed
PMF-PSK(802.11w) Disabl	.ed
FT Reassociation Timeout 20	
FT Over-The-DS mode Ena	bled
GTK Randomization Dis	abled
<snip></snip>	
PMF	Required
PMF Association Comeback Time	1
PMF SA Query RetryTimeout	200

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Die folgenden Debug-Befehle sind zur Behebung von 802.11w-Problemen auf dem WLC verfügbar:

- debug 11w-pmf events enable/disable
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.