Switch mit SXP und IBNS 2.0 für identitätsbasierte Netzwerke konfigurieren

Inhalt

Einleitung

In diesem Dokument werden Verfahren zur Konfiguration von Cisco Switches mit SXP und IBNS 2.0 für identitätsbasierte Netzwerke beschrieben.

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine (ISE) Version 3.3 Patch 4
- Cisco Catalyst Switch 3850

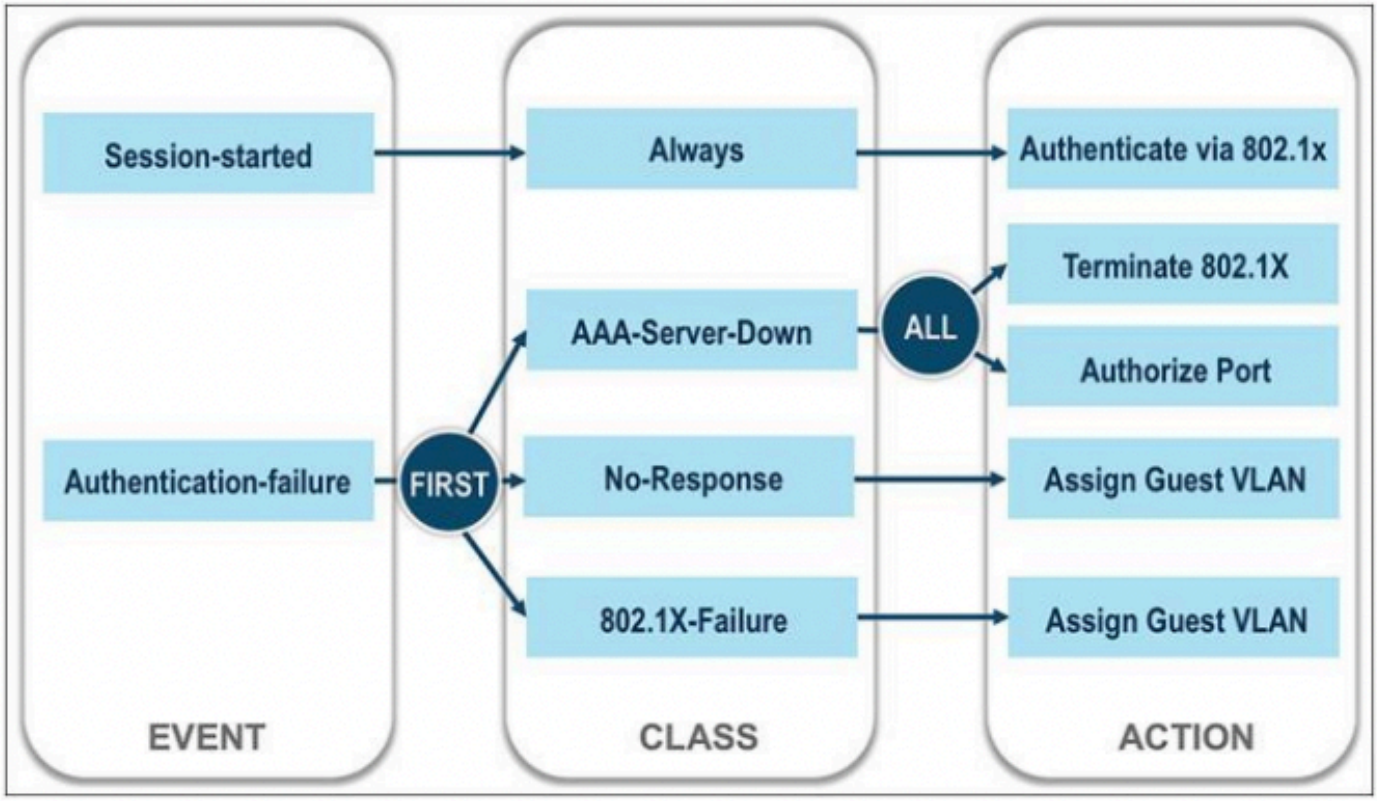
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

Identitätssteuerungsrichtlinien definieren die Aktionen, die der Access Session Manager als Reaktion auf bestimmte Bedingungen und Endpunktereignisse ausführt. Mithilfe einer konsistenten Richtliniensprache können verschiedene Systemaktionen, Bedingungen und Ereignisse zu diesen Richtlinien kombiniert werden.

Steuerungsrichtlinien werden auf Schnittstellen angewendet und sind in erster Linie für das Management der Endgeräteauthentifizierung und die Aktivierung von Services in Sitzungen zuständig. Jede Kontrollrichtlinie besteht aus einer oder mehreren Regeln und einer Entscheidungsstrategie, die festlegt, wie diese Regeln bewertet werden.

Eine Regel für eine Steuerelementrichtlinie enthält eine Steuerelementklasse (eine flexible Bedingungsanweisung), ein Ereignis, das die Bedingungsauswertung auslöst, und eine oder mehrere Aktionen. Administratoren legen fest, welche Aktionen von bestimmten Ereignissen ausgelöst werden. Für einige Ereignisse sind jedoch Standardaktionen vordefiniert.



Identitätssteuerungsrichtlinie

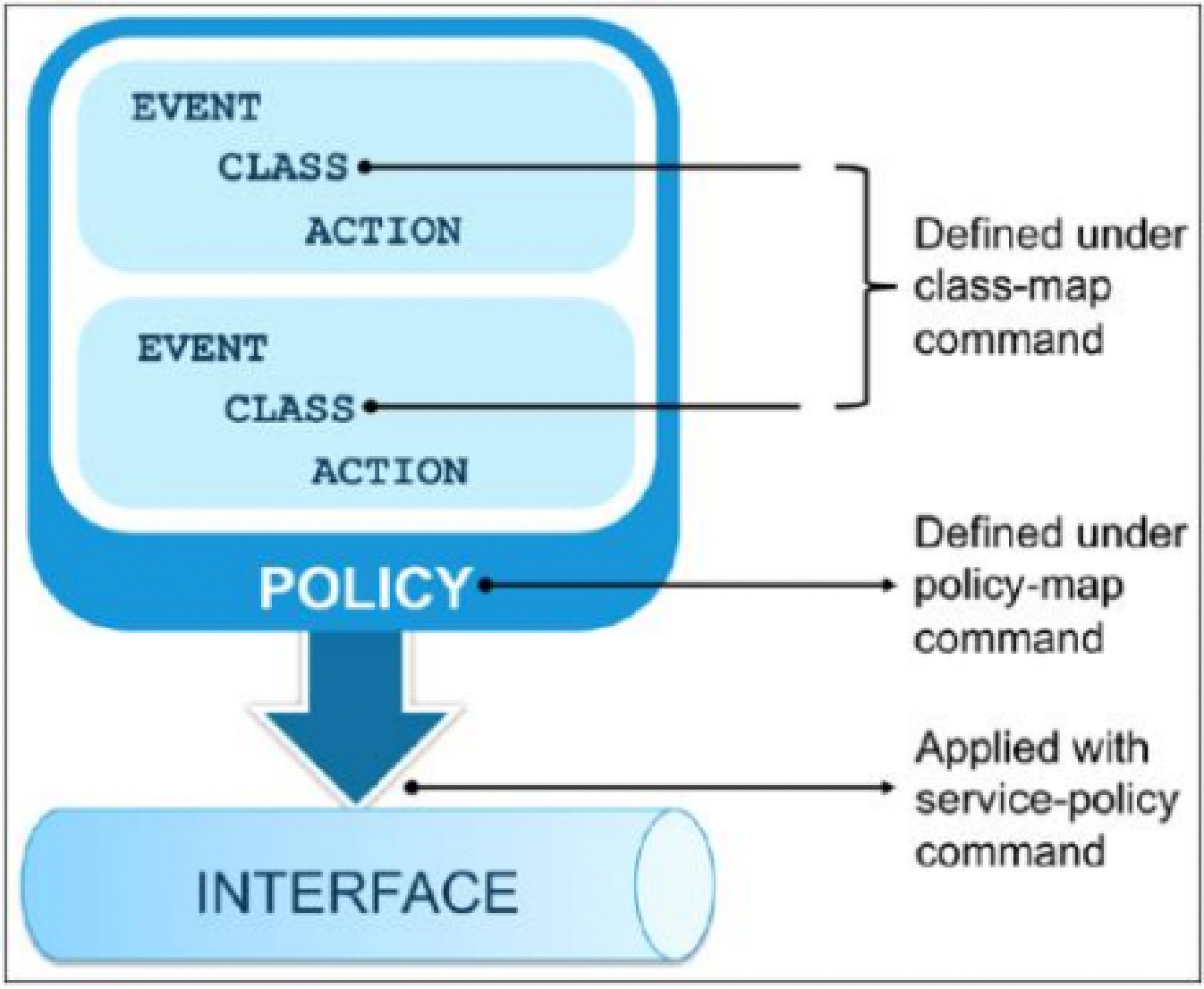
Übersicht über die Konfiguration der Identitätssteuerungsrichtlinie

Kontrollrichtlinien definieren das Systemverhalten anhand eines Ereignisses, einer Bedingung und einer Aktion. Die Konfiguration einer Kontrollrichtlinie umfasst drei Hauptschritte:

1. Erstellen von Steuerelementklassen:
   Eine Steuerelementklasse definiert die Bedingungen, die zum Aktivieren einer Steuerelementrichtlinie erforderlich sind. Jede Klasse kann mehrere Bedingungen haben, die als true oder false ausgewertet werden. Sie können festlegen, ob alle, alle oder keine der Bedingungen wahr sein müssen, damit die Klasse als wahr angesehen wird. Alternativ

können Administratoren eine Standardklasse verwenden, die über keine Bedingungen verfügt und immer als true ausgewertet wird.

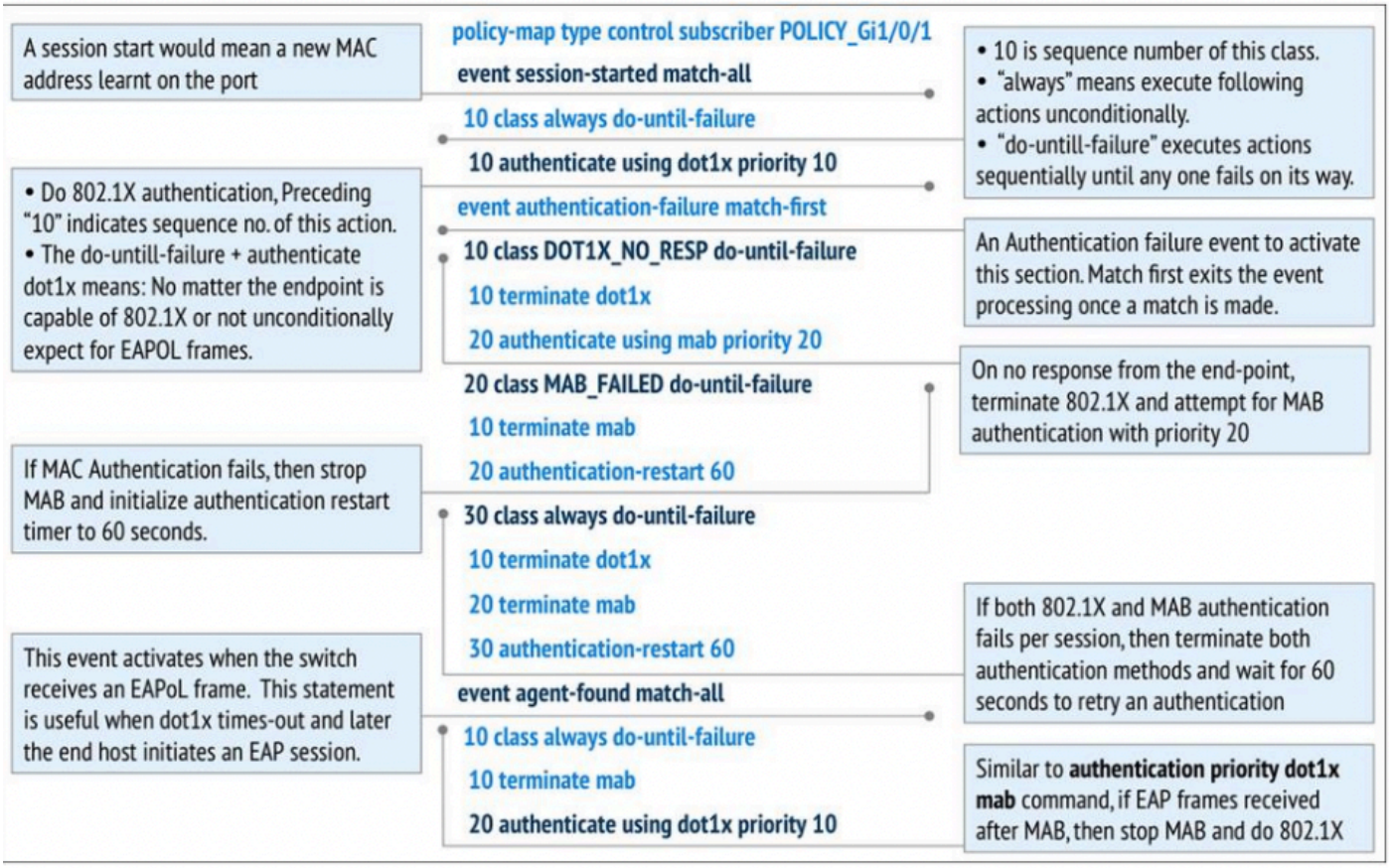
2. Erstellen Sie die Kontrollrichtlinie:
   Eine Kontrollrichtlinie enthält eine oder mehrere Regeln. Jede Regel enthält eine Steuerelementklasse, ein Ereignis, das die Bedingungsprüfung auslöst, und eine oder mehrere Aktionen. Aktionen werden nummeriert und der Reihe nach ausgeführt.
3. Kontrollrichtlinie anwenden:
   Wenden Sie abschließend die Kontrollrichtlinie auf eine Schnittstelle an, um sie zu aktivieren.



Konfiguration der Identitätssteuerungsrichtlinie

Der Befehl authentication display new-style konvertiert die vorhandenen Konfigurationen in einen neuen Stil.

switch#authentication neue Formatvorlage anzeigen



Interpretieren der Identitätssteuerungsrichtlinie

Konfigurieren

Switch-Konfiguration

WS-C3850-48F-E#show run aaa

!

aaa authentication dot1x Standardgruppenradius lokal

aaa, Autorisierungsnetzwerk, Standardgruppenradius lokal

Benutzername admin Kennwort 0 xxxxxx

!

!

!

!

Radius-Server ISE1

address ipv4 10,127.197,xxx auth-port 1812 acct-port 1813

PAK-Schlüssel xxxx@123

!

!

aaa Gruppenserver-Radius ISE2

Servername ISE1

!

!

!

!

aaa neues Modell

aaa, Sitzungs-ID gemeinsam

!

aaa server radius dynamic-author

client 10.127.197.xxx server-key xxxx@123

dot1x System-Authentifizierungssteuerung

!

WS-C3850-48F-E#show run | in POLICY_Gi1/0/45

policy-map type control participant POLICY_Gi1/0/45

service-policy type control-Teilnehmer POLICY_Gi1/0/45

WS-C3850-48F-E#show run | s POLICY_Gi1/0/45

policy-map type control participant POLICY_Gi1/0/45

Ereignis Sitzung gestartet Match-all

  10-Klasse immer bis zum Ausfall

   10 Authentifizierung mit dot1x-Priorität 10

Ereignis-Authentifizierungs-Fehler-Übereinstimmung zuerst

  5 class DOT1X_FAILED do-until-failure

   10 Punkt 1x terminieren

20 authentication-restart 60

10 class DOT1X_NO_RESP do-until-failure

10 Punkt 1x terminieren

20 mit MAB-Priorität authentifizieren 20

20 class MAB_FAILED do-until-failure

10 terminierte MAB

20 authentication-restart 60

40-Klasse immer bis zum Ausfall

10 Punkt 1x terminieren

20 terminierte MAB

30 authentication-restart 60

Ereignis-Agent gefunden - allen

10-Klasse immer bis zum Ausfall

10 terminierte MAB

20 Authentifizierung mit dot1x-Priorität 10

Ereignis-Authentifizierung-Erfolg-Abgleich-Alle

10-Klasse immer bis zum Ausfall

10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE

service-policy type control-Teilnehmer POLICY_Gi1/0/45

WS-C3850-48F-E#show run interface gig1/0/45

Konfiguration wird erstellt...

Aktuelle Konfiguration: 303 Byte

!

interface GigabitEthernet1/0/45

switchport access vlan 503

switchport mode access

access-session host-mode single-host

Zugriffssitzung geschlossen

Zugriffssitzungs-Portsteuerung (Auto)

Mab

keine CTS-rollenbasierte Durchsetzung

dot1x-Seiten-Authentifizierer

service-policy type control-Teilnehmer POLICY_Gi1/0/45

end

WS-C3850-48F-E#show run cts

!

cts Autorisierungsliste ISE2

cts sxp enable

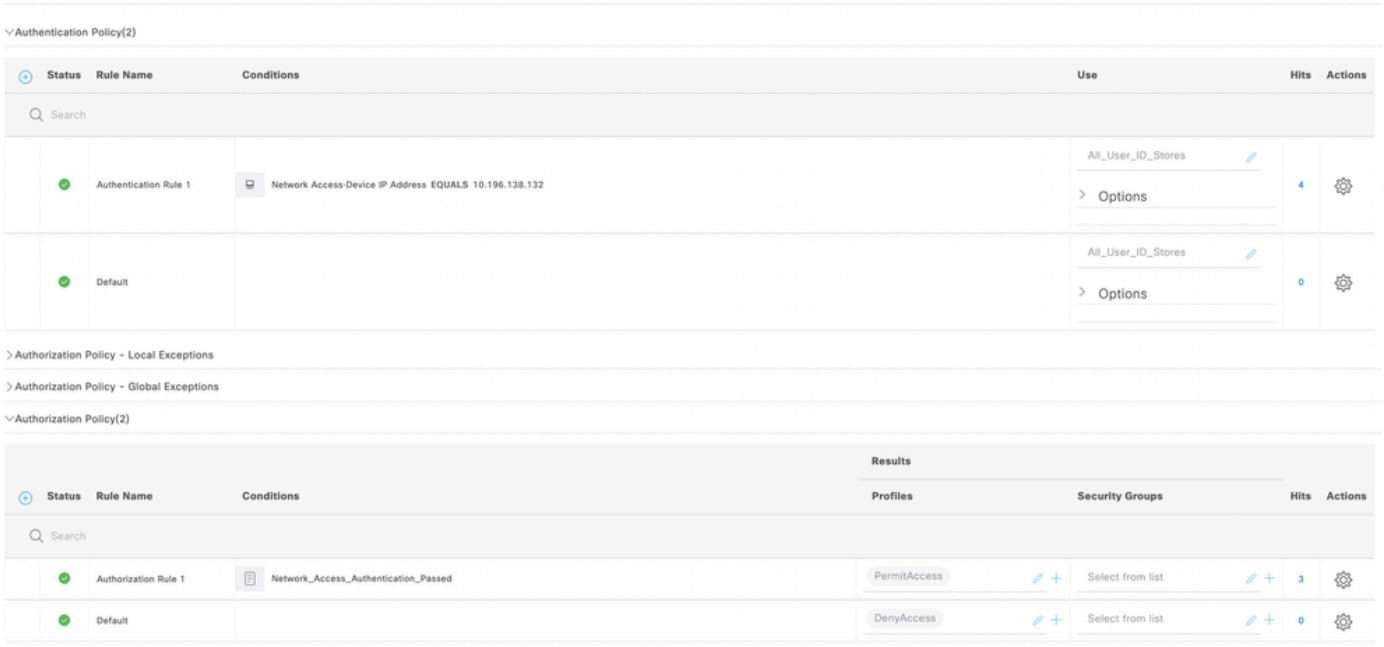
cts sxp connection 10.127.197.xxx kennwort none mode pro lautsprecher hold-time 0 0

cts sxp default source-ip 10.196.138.yyy

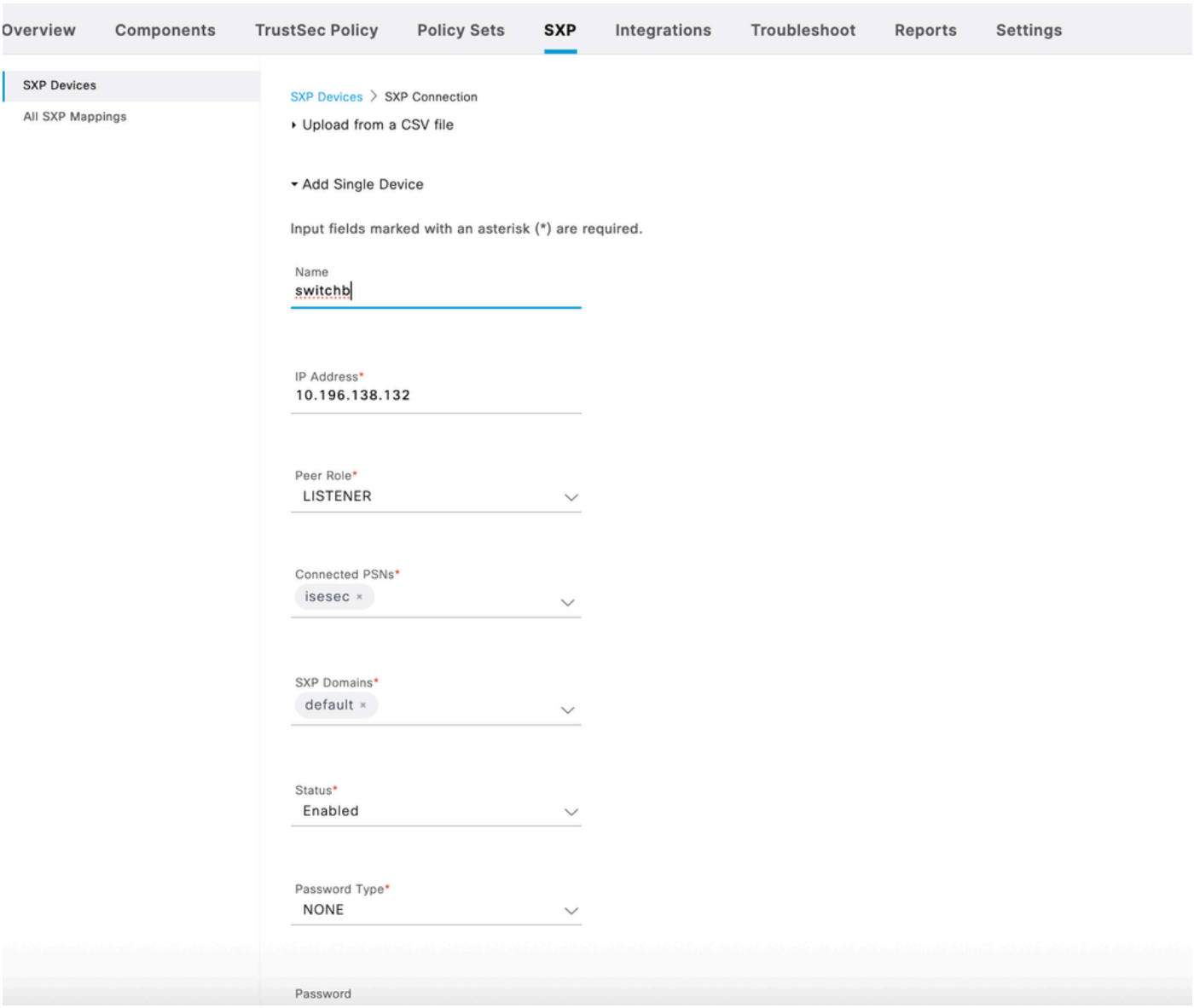
cts sxp default password xxxx@123

ISE-Konfiguration

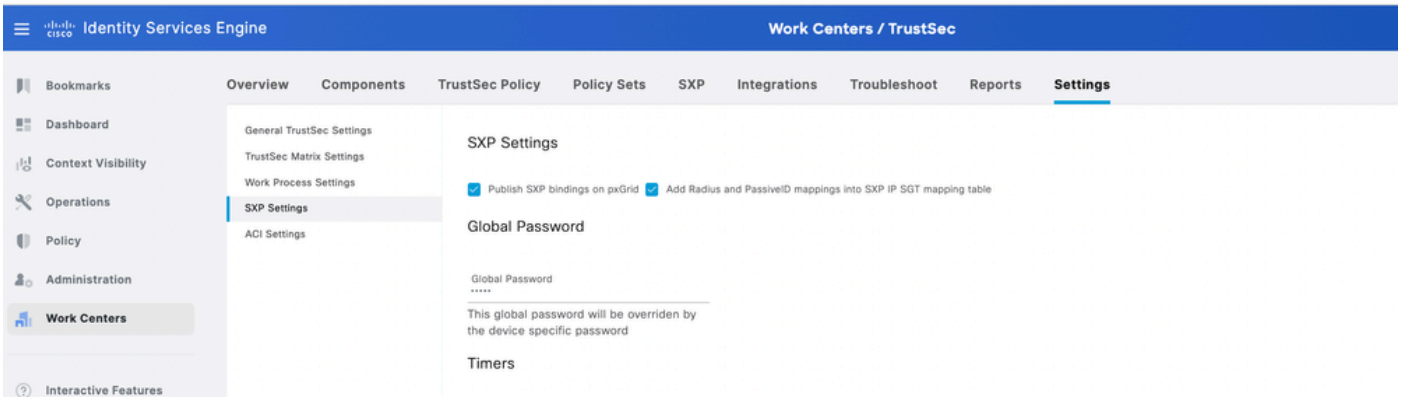
Schritt 1: Erstellen von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE



Phase 2: Konfigurieren eines SXP-Geräts auf der ISE



Schritt 3: Globales Kennwort unter SXP-Einstellungen konfigurieren



Überprüfung

```
WS-C3850-48F-E#show access-session interface gig1/0/45 details
            Schnittstelle:  Gigabit-Ethernet1/0/45
              IIF-ID:  0 x 1 A 146 F 96
           MAC-Adresse:  b496.9126.decc
          IPv6-Adresse:  Unbekannt
          IPv4-Adresse:  Unbekannt
            Benutzername:  Divya123
              Status:  Autorisiert
              Domäne:  DATEN
        Oper-Host-Modus:  Single-Host
      Ober Kontrollverzeichnis:  beide
       Sitzungs-Timeout:  –
     Gemeinsame Sitzungs-ID:  000000000000000B95163D98
       Kontositzungs-ID:  Unbekannt
              Handle:  0x6f000001
        Aktuelle Richtlinie:  POLICY_Gi1/0/45
Lokale Richtlinien:
         Servicevorlage: DEFAULT_LINKSEC_POLICY_MUST_SECURE (Priorität 150)
       Sicherheitsrichtlinie:  Sichern müssen
       Sicherheitsstatus:  Ungesicherter Link
Serverrichtlinien:
Methodenstatusliste:
        Status der Methode
         dot1x Authentifizierung erfolgreich
WS-C3850-48F-E#
WS-C3850-48F-E(config)#do show cts sxp conn
SXP : Aktiviert
```

Unterstützte Version: 4

Standardkennwort: Festlegen

Standard-Schlüsselbund: Nicht festgelegt

Standard-Schlüsselbundname: Nicht zutreffend

Standard-Quell-IP: 10.196.138.yyy

Offener Zeitraum für Verbindungsversuch: 120 s

Abstimmungszeitraum: 120 s

Zeitgeber zum erneuten Öffnen wird ausgeführt

Peer-Sequenz-Durchlauflimit für Export: Nicht festgelegt

Grenzwert für Peer-Sequenz-Durchläufe für den Import: Nicht festgelegt

---

Peer-IP: 10.127.197.xxx

Quell-IP: 10.196.138.yyy

Verbindungsstatus : On

Konvertierung : 4

Verbindungsfähigkeit: IPv4-IPv6-Subnetz

Zeit für Verbindungshaltezeit: 120 Sekunden

Lokaler Modus : SXP-Listener

Verbindungs-INST#: 1

TCP-Verbindung fd : 1

Passwort für TCP-Verbindung: none

Haltezeit läuft

Dauer seit letzter Statusänderung: 0:00:00:22 (TT:H:MM:S)

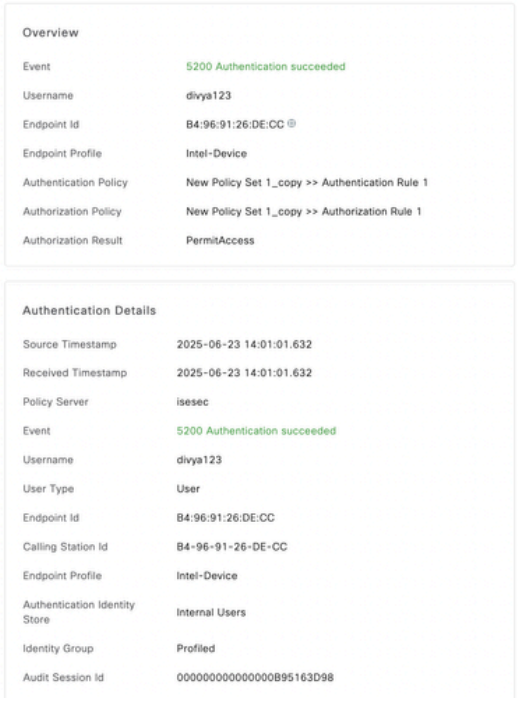
Gesamtzahl der SXP-Verbindungen = 1

0xFF8CBFC090 VRF:, fd: 1, Peer-IP: 10.127.197.xxx

cdbp:0xFF8CBFC090 <10.127.197.145, 10.196.138.yyy> tableid:0x0

WS-C3850-48F-E(config)#

Im Live-Protokollbericht wird der angewendete SGT-Tag Guest angezeigt:

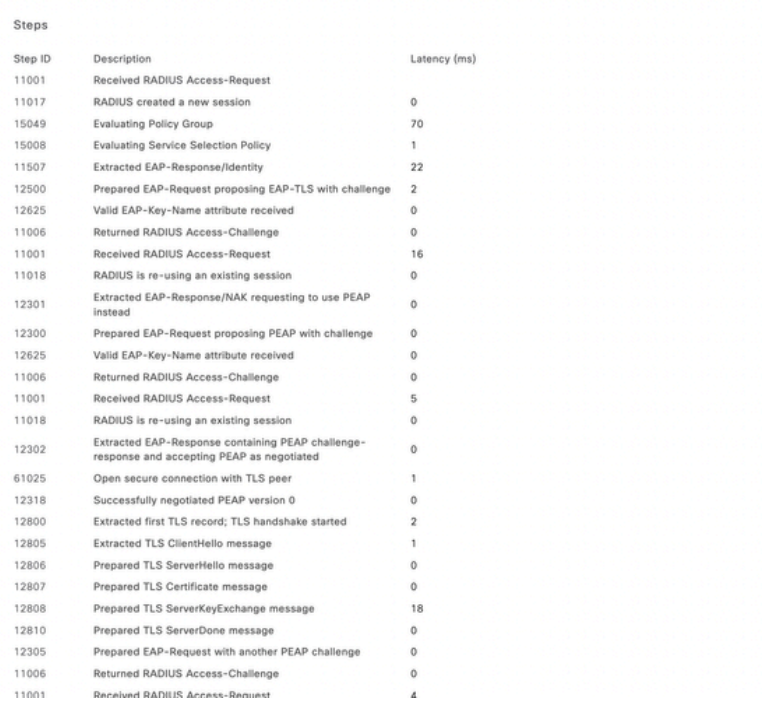


Overview

Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

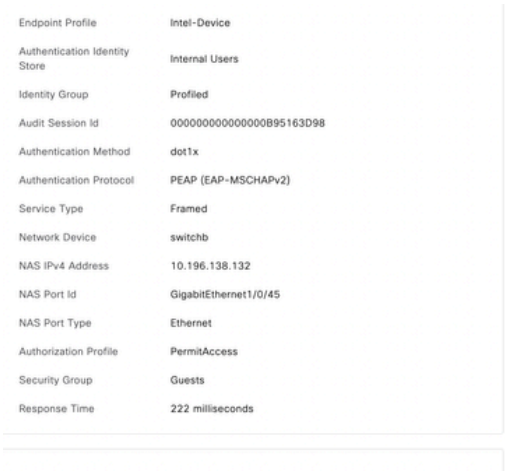
Authentication Details

Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isesec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98

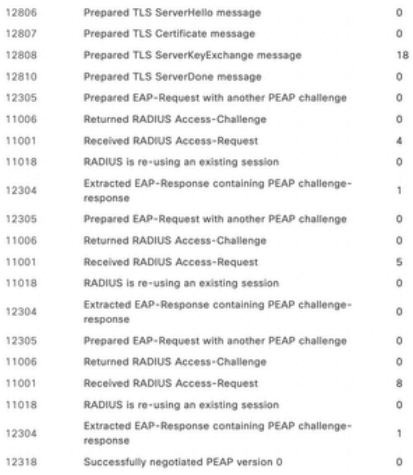


Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
15049	Evaluating Policy Group	70
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	22
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	16
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	2
12805	Extracted TLS ClientHello message	1
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4



Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Security Group	Guests
Response Time	222 milliseconds



12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12318	Successfully negotiated PEAP version 0	0

Fehlerbehebung

Aktivieren Sie dieses Debugging auf dem Switch, um dot1x-Probleme zu beheben:

- debug dot1x all

Protokollerklärung

dot1x-packet:EAPOL pak rx - Ver: 0x1-Typ: 0x1 **>>>>>** EAPoL-Paket empfangen vom Switch dot1x-Paket: länge: 0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45] Client erkannt, Senden des Sitzungsstartereignisses für b496.9126.decc **>>>>** dot1x Client erkannt

dot1x-ev:[b496.9126.decc, Gig1/0/45] Dot1x-Authentifizierung gestartet für 0x26000007

(b496.9126.decc)**>>>>** dot1x gestartet

%AUTHMGR-5-START: 'dot1x' für Client wird gestartet (b496.9126.decc) an Schnittstelle Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm:[b496.9126.decc, Gig1/0/45] Veröffentlichen von !EAP_RESTART auf Client 0x26000007 /**>>>>** Anfordern des Clients zum Neustart des EAP-Prozesses

dot1x-sm:[b496.9126.decc, Gig1/0/45] Veröffentlichen von RX_REQ auf Client 0x26000007 **>>>>>** Warten auf das EAPoL-Paket vom Client

dot1x-sm:[b496.9126.decc, Gig1/0/45] Veröffentlichen von AUTH_START für 0x26000007 **>>>>>** Starten des Authentifizierungsprozesses

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOL-Paket senden **>>>>>** Identitätsanforderung
dot1x-packet:EAPOL Paket Tx - Ver: 0x3-Typ: 0x0
dot1x-Paket: länge: 0x0005
dot1x-packet:EAP-Code: 0x1-ID: 0x1 Länge: 0x0005
dot1x-Paket: typ: 0 x 1
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL-Paket gesendet an Client 0x26000007

dot1x-ev:[Gig1/0/45] Received pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e 0100 000a
dot1x-packet:EAPOL pak rx - Ver: 0x1-Typ: 0x0 // Identitätsantwort
dot1x-Paket: länge: 0 x 000 A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Veröffentlichen von EAPOL_EAP für 0x26000007 **>>>>>** EAPoL-Paket (EAP-Antwort) empfangen, Vorbereiten der Serveranfrage

dot1x-sm:[b496.9126.decc, Gig1/0/45] EAP_REQ wird für 0x26000007 veröffentlicht **>>>>>>** Serverantwort erhalten, EAP-Anforderung wird vorbereitet

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOL-Paket wird gesendet
dot1x-packet:EAPOL Paket Tx - Ver: 0x3-Typ: 0x0
dot1x-Paket: länge: 0x0006
dot1x-packet:EAP-Code: 0x1-ID: 0xE5-Länge: 0x0006
dot1x-Paket: typ: 0 x T
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL-Paket gesendet an Client 0x26000007 **>>>>>** EAP-Anfrage gesendet

dot1x-ev:[Gig1/0/45] Received pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP-Antwort empfangen
dot1x-packet:EAPOL pak rx - Ver: 0x1-Typ: 0x0
dot1x-Paket: länge: 0x0006
||
||
||
|| Hier treten viele EAPOL-EAP- und EAP_REQ-Ereignisse auf, da viele Informationen zwischen

dem Switch und dem Client ausgetauscht werden.
|| Wenn die Ereignisse danach nicht mehr folgen, müssen die Timer und die bisher gesendeten Informationen überprüft werden.
||
||
||
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAP-Erfolg empfangen **>>>>** EAP-Erfolg vom Server empfangen

dot1x-sm:[b496.9126.decc, Gig1/0/45] Veröffentlichen von EAP_SUCCESS für 0x26000007 **>>>>** Veröffentlichen des EAP Success-Ereignisses

dot1x-sm:[b496.9126.decc,Gig1/0/45] Veröffentlichen von AUTH_SUCCESS auf Client 0x26000007 **>>>>>** Veröffentlichen der Authentifizierung erfolgreich

%DOT1X-5-ERFOLG: Authentifizierung erfolgreich für Client (b496.9126.decc) an Schnittstelle Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] EAP-Schlüsseldaten erkannt Hinzufügen zur Attributliste **>>>>>** Weitere Schlüsseldaten erkannt, gesendet vom Server

%AUTHMGR-5-ERFOLG: Die Autorisierung für den Client (b496.9126.decc) auf der Schnittstelle Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3 war erfolgreich.

dot1x-ev:[b496.9126.decc, Gig1/0/45] Erhaltener Autorisierungserfolg für den Client 0x26000007 (b496.9126.decc) **>>>>** Autorisierungserfolg

dot1x-ev:[b496.9126.decc, Gig1/0/45] EAPOL-Paket senden **>>>>>** EAP-Erfolg an den Client senden
dot1x-packet:EAPOL Paket Tx - Ver: 0x3-Typ: 0x0
dot1x-Paket: länge: 0x0004
dot1x-packet:EAP-Code: 0x3-ID: 0xED-Länge: 0x0004
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL-Paket gesendet an Client 0x26000007

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.