

ISE 2.0 TrustSec SXP Listener und Lautsprecher konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Datenverkehrsfluss](#)

[Konfigurationen](#)

[Switch 3850-1](#)

[Switch 3850-2](#)

[ISE](#)

[Überprüfen](#)

[Referenzen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie die Funktion, die die Cisco Identity Services Engine (ISE) Version 2.0 das TrustSec SGT Exchange Protocol (SXP) im Listen- und Lautsprechermodus unterstützt, konfigurieren und Fehler beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Catalyst Switch-Konfiguration
- Identity Services Engine (ISE) und TrustSec-Services

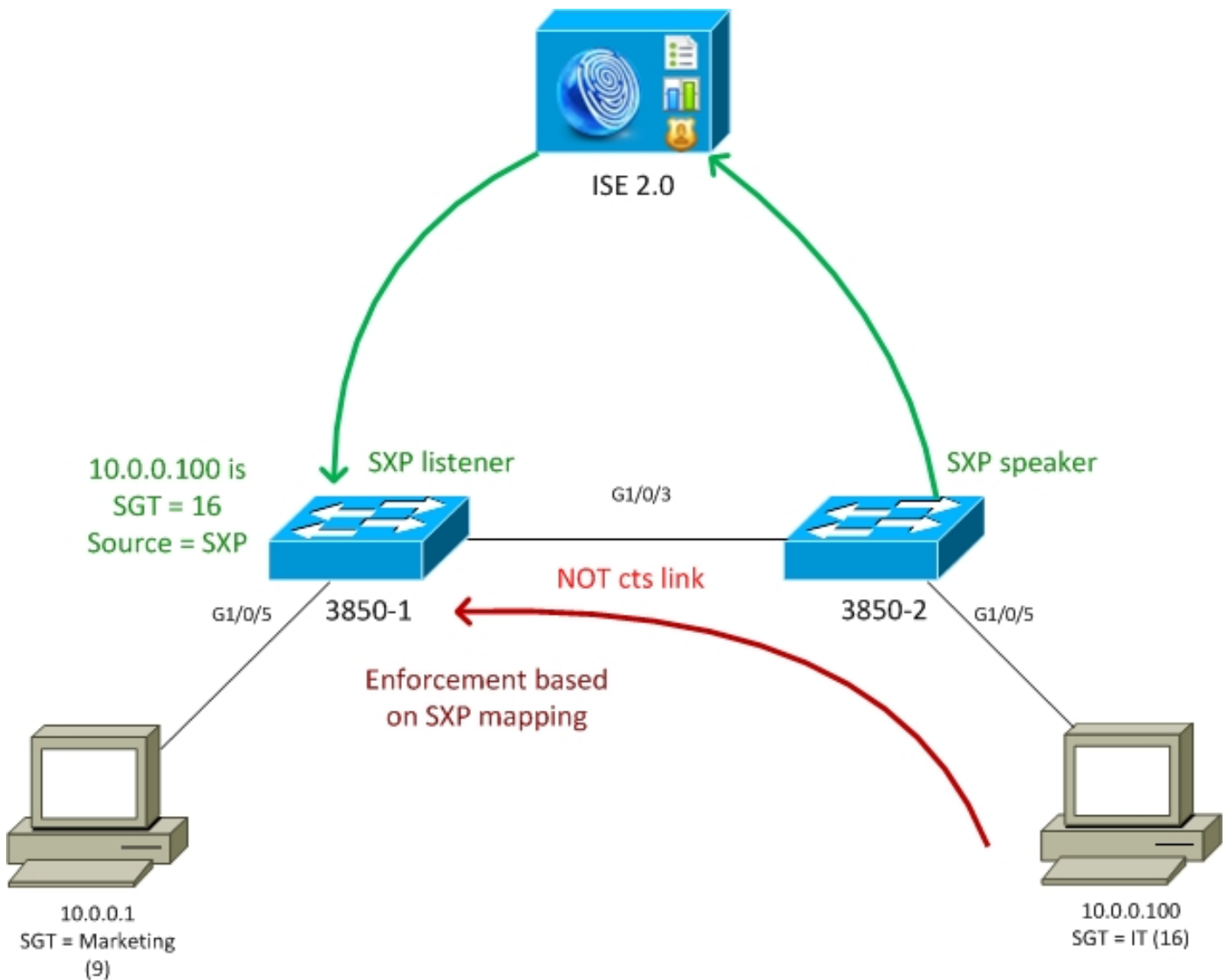
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Catalyst 3850 Switch mit Software IOS-XE 3.7.2 und höher
- Cisco ISE, Version 2.0 und höher

Konfigurieren

Netzwerkdiagramm



Datenverkehrsfluss

- 3850-2 ist 802.1x-Authentifizierer für 10.0.0.100 - ISE Return Security Group Tag (SGT) 16 (IT) für erfolgreiche Authentifizierung
- Der Switch 3850-2 erfährt die Supplicant IP-Adresse (IP Device Tracking) und sendet Zuordnungsinformationen (IP-SGT) mithilfe des SXP-Protokolls an die ISE.
- 3850-1 ist 802.1x-Authentifizierer für 10.0.0.1 - ISE-SGT-Tag 9 (Marketing) zur erfolgreichen Authentifizierung zurücksenden
- 3850-1 empfängt SXP-Zuordnungsinformationen von der ISE (10.0.0.100 ist SGT 16), lädt die Richtlinie von der ISE herunter
- Von 10.0.0.100 an 10.0.0.1 gesendeter Datenverkehr wird von 3850-2 (keine speziellen heruntergeladenen Richtlinien) an 3850-1 weitergeleitet, bei dem die Richtlinie IT (16) -> Marketing (9) befolgt wird

Bitte beachten Sie, dass der Link zwischen den Switches nicht cts-Link ist - daher werden alle Remote-Zuordnungen auf den Switches über das SXP-Protokoll installiert.

Hinweis: Nicht alle Switches verfügen über die Hardware, die das Programmieren über Richtlinien ermöglicht, die von der ISE basierend auf empfangenen SXP-Zuordnungen

empfangen werden. Bitte lesen Sie die aktuelle TrustSec-Kompatibilitätsmatrix, oder wenden Sie sich an Cisco Systems, um eine Überprüfung durchzuführen.

Konfigurationen

Einzelheiten zur grundlegenden TrustSec-Konfiguration finden Sie in den Artikeln im Abschnitt Referenzen.

Switch 3850-1

Der Switch beendet die 802.1x-Sitzung mit der SGT-Zuweisung sowie als SXP-Sprecher für die ISE.

```
aaa authentication dot1x default group ISE_mgarcarz
aaa authorization network default group ISE_mgarcarz
aaa authorization network ISE_mgarcarz group ISE_mgarcarz
aaa accounting dot1x default start-stop group ISE_mgarcarz
aaa accounting update newinfo

radius server ISE_mgarcarz
 address ipv4 10.48.17.235 auth-port 1645 acct-port 1646
 pac key cisco

aaa group server radius ISE_mgarcarz
 server name ISE_mgarcarz

interface GigabitEthernet1/0/3
 switchport mode trunk

interface GigabitEthernet1/0/5
 description mgarcarz
 switchport access vlan 100
 switchport mode access
 ip flow monitor F_MON input
 ip flow monitor F_MON output
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator

cts authorization list ISE_mgarcarz
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094
cts sxp enable
cts sxp default password cisco
cts sxp connection peer 10.48.17.235 password default mode local listener hold-time 0
```

Switch 3850-2

Der Switch beendet die 802.1x-Sitzung mit der SGT-Zuweisung und auch als SXP-Listener, der die Zuordnung von der ISE erhält.

```
aaa authentication dot1x default group ISE_mgarcarz
aaa authorization network default group ISE_mgarcarz
aaa authorization network ISE_mgarcarz group ISE_mgarcarz
```

```
aaa accounting dot1x default start-stop group ISE_mgarcarz
aaa accounting update newinfo

radius server ISE_mgarcarz
  address ipv4 10.48.17.235 auth-port 1645 acct-port 1646
  pac key cisco

aaa group server radius ISE_mgarcarz
  server name ISE_mgarcarz

interface GigabitEthernet1/0/3
  switchport mode trunk

interface GigabitEthernet1/0/5
  description mgarcarz
  switchport access vlan 100
  switchport mode access
  authentication order dot1x mab
  authentication priority dot1x mab
  authentication port-control auto
  mab
  dot1x pae authenticator

cts authorization list ISE_mgarcarz
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094
cts sxp enable
cts sxp default password cisco
cts sxp connection peer 10.48.17.235 password default mode local speaker hold-time 0
```

ISE

Schritt 1: Netzwerkzugriffsgeräte

Navigieren Sie zu **Work Centers > Device Administration > Network Resources**, fügen Sie beide Switches mit dem gemeinsamen geheimen cisco und TrustSec-Kennwort Krakow123 hinzu.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results

Network Devices

Default Devices
TACACS External Servers
TACACS Server Sequence

Network Devices List > KSEC-3850-1

Network Devices

* Name:
Description:

* IP Address: /

* Device Profile:

Model Name:
Software Version:

* Network Device Group

Location:

Device Type:

- [RADIUS Authentication Settings](#)
- [TACACS+ Authentication Settings](#)
- [SNMP Settings](#)
- [Advanced TrustSec Settings](#)

Schritt 2: Sicherheitsgruppen

Um SGT für IT und Marketing hinzuzufügen, navigieren Sie zu **Work Centers > TrustSec > Components > Security Groups**.

Identity Services Engine Home Operations Policy Guest Access

TrustSec Device Administration

Overview Authentication Policy Authorization Policy Components Policy SXP

Security Groups

Security Group ACLs

Network Devices

Trustsec AAA Servers

Security Groups

For Policy Export go to [Administration > System > Backup &](#)

Edit Add Import Export Delete

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	SGT_BYOD	15/000F
<input type="checkbox"/>	SGT_Guest	6/0006
<input type="checkbox"/>	SGT_IT	16/0010
<input type="checkbox"/>	SGT_Marketing	9/0009
<input type="checkbox"/>	Unknown	0/0000

Schritt 3: Sicherheitsgruppen ACL

Um Sicherheitsgruppen-ACL hinzuzufügen, navigieren Sie zu **Work Centers > TrustSec > Components > Security Group ACLs (Arbeitszentren > TrustSec > Komponenten > Sicherheitsgruppen-ACLs)**.

Identity Services Engine Home Operations Policy Guest Access Admin

TrustSec Device Administration

Overview Authentication Policy Authorization Policy Components Policy SXP Reports

Security Groups

Security Group ACLs

Network Devices

Trustsec AAA Servers

Security Groups ACLs List > ICMP

Security Group ACLs

* Name

Description

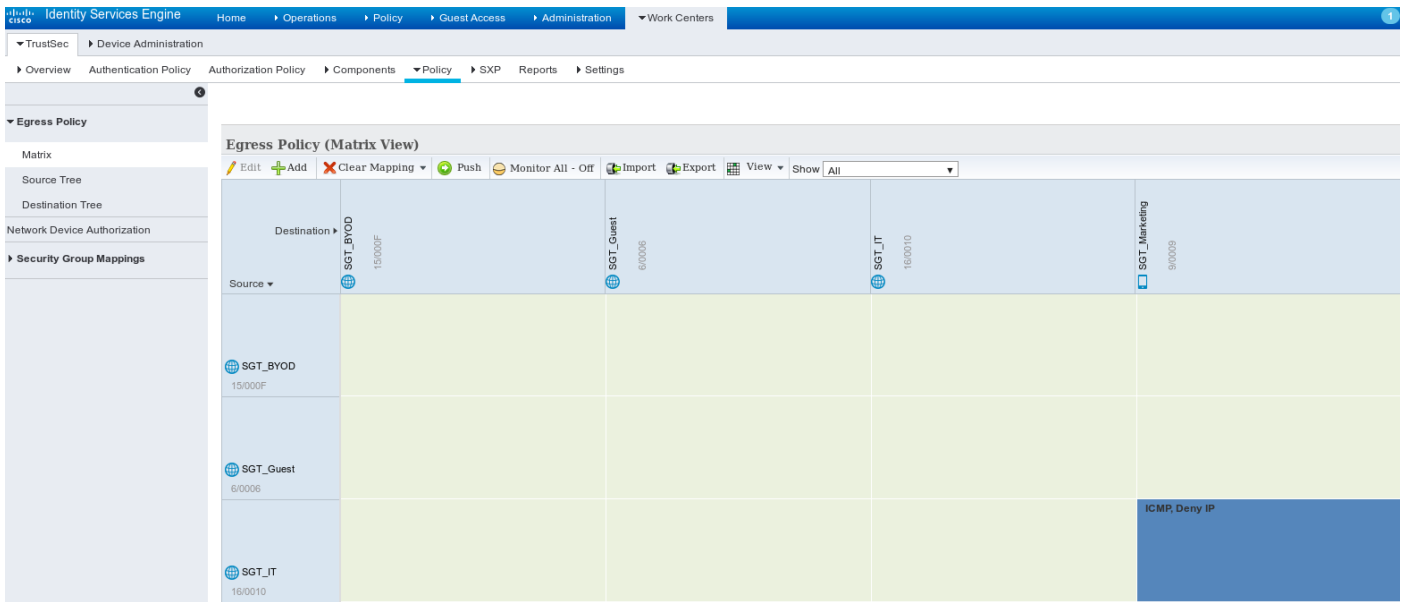
IP Version IPv4 IPv6 Agnostic

* Security Group ACL content

Nur ICMP-Datenverkehr zulassen.

Schritt 4: TrustSec-Richtlinie

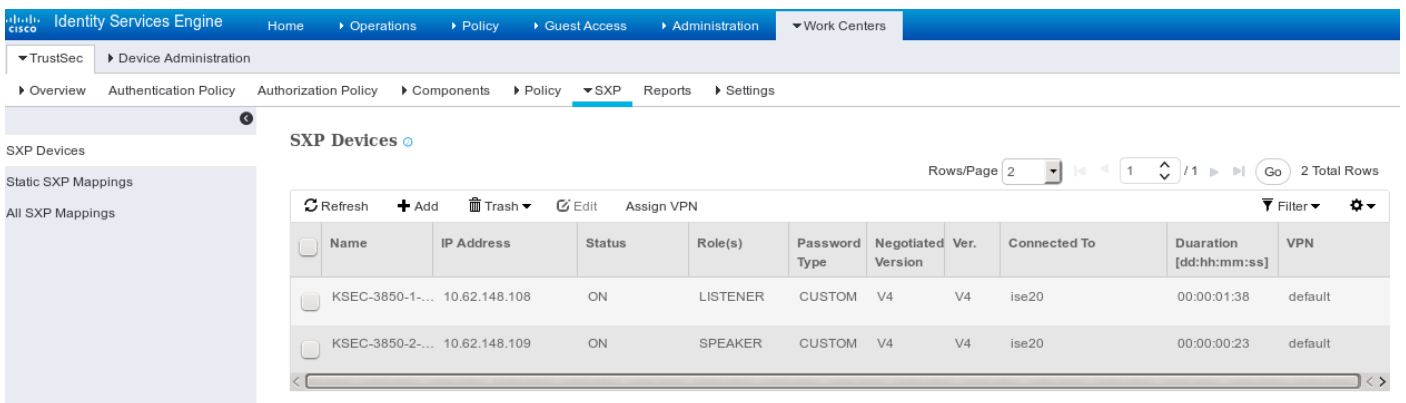
Um Richtlinien hinzuzufügen, die den Datenverkehr von der IT zur Marketingkommunikation steuern, navigieren Sie zu **Work Centers > TrustSec > Components > Egress Policy > Matrix**.



Legen Sie fest, dass der Standardeintrag "catch all" (Alle abfangen) die Regel lautet, den gesamten Datenverkehr abzulehnen.

Schritt 5: SXP-Geräte

Um SXP-Listener und -Lautsprecher für die entsprechenden Switches zu konfigurieren, navigieren Sie zu **Work Centers > TrustSec > SXP Devices**.



Verwenden Sie das Kennwort cisco (oder eine andere für sxp auf dem Switch konfigurierte Methode).

Schritt 6: Autorisierungsrichtlinie

Vergewissern Sie sich, dass die Autorisierungsrichtlinie die richtigen SGT-Tags für jeden Benutzer zurückgibt, und navigieren Sie zu **Policy > Authorization**.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies ▼

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	IT	if example.com:ExternalGroups EQUALS example.com/Users/IT	then SGT_IT
✔	Marketing	if example.com:ExternalGroups EQUALS example.com/Users/Marketing	then SGT_Marketing

Überprüfen

Schritt 1: Switch-Beitritt zur ISE für CTS

Geben Sie von jedem Switch TrustSec-Anmeldeinformationen ein (konfiguriert in ISE/Step1), um die PAC abzurufen.

```
KSEC-3850-2#cts credentials id KSEC-3850-2 password Krakow123
```

CTS device ID and password have been inserted in the local keystore. Please make sure that the same ID and password are configured in the server database.

Stellen Sie sicher, dass PAC heruntergeladen wird.

```
KSEC-3850-2#show cts pacs
```

```
AID: 65D55BAF222BBC73362A7810A04A005B
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 65D55BAF222BBC73362A7810A04A005B
  I-ID: KSEC-3850-2
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 20:42:37 UTC Nov 13 2015
PAC-Opaque:
000200B8000300010004001065D55BAF222BBC73362A7810A04A005B0006009C00030100B26D8DDC125B6595067D64F9
17DA624C0000001355CB2E1C00093A800E567155E0DE76419D2F3B97D890F34F109C4C42F586B29050CEC7B441E0CA60
FC6684D4F6E8263FA2623A6E450927815A140CD3B9D68988E95D8C1E65544E222E187C647B9F7F3F230F6DB4F80F3C20
1ACD623B309077E27688EDF7704740A1CD3F18CE8485788054C19909083ED303BB49A6975AC0395D41E1227B
Refresh timer is set for 12w4d
```

Die Umweltpolitik wird überarbeitet.

```
KSEC-3850-2#show cts environment-data
```

```
CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server: 10.48.17.235, port 1812, A-ID 65D55BAF222BBC73362A7810A04A005B
  Status = ALIVE
```



```

    auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
  0-00:Unknown
  6-00:SGT_Guest
  9-00:SGT_Marketing
  15-00:SGT_BYOD
  16-00:SGT_IT
  255-00:SGT_Quarantine
Environment Data Lifetime = 86400 secs
Last update time = 20:47:04 UTC Sat Aug 15 2015
Env-data expires in 0:08:09:13 (dd:hr:mm:sec)
Env-data refreshes in 0:08:09:13 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
Wiederholen Sie den gleichen Vorgang für 3850-1.

```

Schritt 2: 802.1x-Sitzungen

Nach der Authentifizierung des IT-Benutzers wird das richtige Tag zugewiesen.

```

KSEC-3850-2#show authentication sessions interface g1/0/5 details
    Interface: GigabitEthernet1/0/5
      IIF-ID: 0x107E700000000C4
    MAC Address: 0050.b611.ed31
    IPv6 Address: Unknown
    IPv4 Address: 10.0.0.100
    User-Name: cisco
      Status: Authorized
    Domain: DATA
    Oper host mode: single-host
    Oper control dir: both
    Session timeout: N/A
    Common Session ID: 0A3E946D00000FF214D18E36
    Acct Session ID: 0x00000FDC
      Handle: 0xA4000020
    Current Policy: POLICY_Gi1/0/5

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
  SGT Value: 16

```

```

Method status list:
  Method      State
  dot1x      Authc Success

```

Die Zuordnung wird in der lokalen SGT-IP-Tabelle installiert.

```

KSEC-3850-2#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address      SGT      Source
=====
10.0.0.100      16       LOCAL

```

Schritt 3: SXP-Lautsprecher

3850-2 sendet die Zuordnung an ISE, Switch-Debugging für cts sxp.

```
KSEC-3850-2(config)#do show debug
```

```
CTS:
  CTS SXP message debugging is on

*Aug 16 12:48:30.173: CTS-SXP-MSG:trp_send_msg <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.173: CTS-SXP-MSG:trp_socket_write fd<1>, cdbp->ph_sock_pending<1>,
<10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.226: CTS-SXP-MSG:trp_process_read_sock <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.226: CTS-SXP-MSG:trp_process_read_sock socket_rcv result:-1 errno:11;
<10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.226: CTS-SXP-MSG:trp_process_read_sock socket_conn is accepted; <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.226: CTS-SXP-MSG:trp_socket_write fd<1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.226: CTS-SXP-MSG:trp_socket_write freeing tx_msgq_entry, <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.227: CTS-SXP-MSG:after socket_send, wlen=28, slen=0, tot_len=28, <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.227: CTS-SXP-MSG:trp_socket_write freeing tx_buf, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.227: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.227: CTS-SXP-MSG:trp_socket_read readlen = -1; errno = 11, <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.278: CTS-SXP-MSG:trp_process_read_sock <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.278: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.278: CTS-SXP-MSG:RCVD peer 10.48.17.235 readlen:32, datalen:0 remain:4096 bufp
=
*Aug 16 12:48:30.278: CTS-SXP-MSG:sxp_handle_rx_msg_v2 <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:imu_sxp_conn_cr <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:wrt_sxp_opcode_info_v4 cdbp 0x3D541160
*Aug 16 12:48:30.279: CTS-SXP-MSG:trp_send_msg <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:trp_socket_write fd<1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:trp_socket_write freeing tx_msgq_entry, <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:after socket_send, wlen=28, slen=0, tot_len=28, <10.48.17.235,
10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:trp_socket_write freeing tx_buf, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.280: CTS-SXP-MSG:trp_socket_read readlen = 32; errno = 11, <10.48.17.235,
10.62.148.109>
```

ISE-Berichte (sxp_appserver/sxp.log)

```
2015-08-16 14:44:07,029 INFO [nioEventLoopGroup-2-3]
opendaylight.sxp.core.behavior.Strategy:473 -
[ISE:10.48.17.235][10.48.17.235:21121/10.62.148.109:64999][O|Lv4/Sv4 192.168.77.2] PURGEALL
processing
2015-08-16 14:44:07,029 WARN [nioEventLoopGroup-2-3]
opendaylight.sxp.core.handler.MessageDecoder:173 -
[ISE:10.48.17.235][10.48.17.235:21121/10.62.148.109:64999] Channel inactivation
2015-08-16 14:44:07,029 INFO [pool-3-thread-1] sxp.util.database.spi.MasterDatabaseProvider:721
- SXP_PERF:BINDINGS_PER_SXP_UPDATE_MESSAGE(CHUNK)=1, onlyChanged=true
2015-08-16 14:44:07,030 INFO [pool-3-thread-1] sxp.util.database.spi.MasterDatabaseProvider:725
- SXP_PERF:NUM_OF_CHUNKS=1, onlyChanged=true
2015-08-16 14:44:07,030 INFO [pool-3-thread-9]
opendaylight.sxp.core.service.UpdateExportTask:93 - SXP_PERF:SEND_UPDATE_BUFFER_SIZE=16
2015-08-16 14:44:07,030 INFO [pool-3-thread-9]
opendaylight.sxp.core.service.UpdateExportTask:119 - SENT_UPDATE to
[ISE:10.48.17.235][10.48.17.235:57719/10.62.148.108:64999][O|Sv4]
2015-08-16 14:44:07,030 INFO [pool-3-thread-9]
opendaylight.sxp.core.service.UpdateExportTask:140 - SENT_UPDATE SUCCESSFUL to
[ISE:10.48.17.235][10.48.17.235:57719/10.62.148.108:64999][O|Sv4]:false
```

```

2015-08-16 14:44:07,030 INFO [pool-3-thread-1]
opendaylight.sxp.core.service.BindingDispatcher:198 -
SXP_PERF:MDB_PARTITON_AND_SXP_DISPATCH:DURATION=1 milliseconds, NUM_CONNECTIONS=1
2015-08-16 14:44:07,031 INFO [pool-3-thread-1] sxp.util.database.spi.MasterDatabaseProvider:725
- SXP_PERF:NUM_OF_CHUNKS=0, onlyChanged=true
2015-08-16 14:44:12,534 INFO [nioEventLoopGroup-2-4]
opendaylight.sxp.core.behavior.Strategy:232 -
[ISE:10.48.17.235][10.48.17.235:64999/10.62.148.109:1035][X|Lv4/Sv4 192.168.77.2] received
Message Open
2015-08-16 14:44:12,535 INFO [nioEventLoopGroup-2-4]
opendaylight.sxp.core.behavior.Strategy:358 -
[ISE:10.48.17.235][10.48.17.235:64999/10.62.148.109:1035][O|Lv4/Sv4 192.168.77.2] Sent RESP 0 0
0 32 0 0 0 2 | 0 0 0 4 0 0 0 2 80 6 6 3 0 2 0 1 0 80 7 4 0 120 0 180
2015-08-16 14:44:12,585 INFO [nioEventLoopGroup-2-4]
opendaylight.sxp.core.behavior.Strategy:451 -
[ISE:10.48.17.235][10.48.17.235:64999/10.62.148.109:1035][O|Lv4/Sv4 192.168.77.2] received
Message Update
2015-08-16 14:44:12,586 INFO [pool-3-thread-2]
opendaylight.sxp.core.service.SimpleBindingHandler:663 - PERF_SXP_PROCESS_UPDATE from
[ISE:10.48.17.235][10.48.17.235:64999/10.62.148.109:1035][O|Lv4/Sv4 192.168.77.2]
2015-08-16 14:44:12,586 INFO [pool-3-thread-2]
opendaylight.sxp.core.service.SimpleBindingHandler:666 - PERF_SXP_PROCESS_UPDATE_DONE from
[ISE:10.48.17.235][10.48.17.235:64999/10.62.148.109:1035][O|Lv4/Sv4 192.168.77.2]
2015-08-16 14:44:12,586 INFO [pool-3-thread-1] sxp.util.database.spi.MasterDatabaseProvider:721
- SXP_PERF:BINDINGS_PER_SXP_UPDATE_MESSAGE(CHUNK)=1, onlyChanged=true
2015-08-16 14:44:12,587 INFO [pool-3-thread-1] sxp.util.database.spi.MasterDatabaseProvider:725
- SXP_PERF:NUM_OF_CHUNKS=1, onlyChanged=true
2015-08-16 14:44:12,587 INFO [pool-3-thread-11]
opendaylight.sxp.core.service.UpdateExportTask:93 - SXP_PERF:SEND_UPDATE_BUFFER_SIZE=32
2015-08-16 14:44:12,587 INFO [pool-3-thread-11]
opendaylight.sxp.core.service.UpdateExportTask:119 - SENT_UPDATE to
[ISE:10.48.17.235][10.48.17.235:57719/10.62.148.108:64999][O|Sv4]
2015-08-16 14:44:12,587 INFO [pool-3-thread-11]
opendaylight.sxp.core.service.UpdateExportTask:140 - SENT_UPDATE SUCCESSFUL to
[ISE:10.48.17.235][10.48.17.235:57719/10.62.148.108:64999][O|Sv4]:false
2015-08-16 14:44:12,587 INFO [pool-3-thread-1]
opendaylight.sxp.core.service.BindingDispatcher:198 -
SXP_PERF:MDB_PARTITON_AND_SXP_DISPATCH:DURATION=1 milliseconds, NUM_CONNECTIONS=1

```

Darstellen Sie alle Zuordnungen über GUI (einschließlich der Zuordnung für 10.0.0.100 aus 3850-2), wie in diesem Bild gezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation menu includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. Under Work Centers, there is a sub-menu for TrustSec, which includes Device Administration. The main content area is titled 'All SXP Mappings' and features a table with the following data:

IP Address	SGT	Learned From	Learned By
10.0.0.100/32	SGT_IT(16/0010)	192.168.77.2	SXP
192.168.1.203/32	SGT_IT(16/0010)	10.48.17.235,10.48.67.250	Session

192.168.77.2 ist die Kennung der SXP-Verbindung auf 3850-2 (höchste definierte IP-Adresse).

KSEC-3850-2#show ip interface brief

```

Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0      unassigned      YES unset  down            down

```

Vlan1	unassigned	YES NVRAM	administratively down	down
Vlan100	10.0.0.2	YES manual	up	up
Vlan480	10.62.148.109	YES NVRAM	up	up
Vlan613	unassigned	YES NVRAM	administratively down	down
Vlan666	192.168.66.2	YES NVRAM	down	down
Vlan777	192.168.77.2	YES NVRAM	down	down

Schritt 4: SXP-Listener

Anschließend sendet die ISE diese Zuordnung erneut an 3850-1 Switch-Debugging.

```
*Aug 16 05:42:54.199: CTS-SXP-MSG:trp_send_msg <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.199: CTS-SXP-MSG:trp_socket_write fd<1>, cdbp->ph_sock_pending<1>,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_process_read_sock <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_process_read_sock socket_recv result:-1 errno:11;
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_process_read_sock socket_conn is accepted; <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_socket_write fd<1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_socket_write freeing tx_msgq_entry, <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:after socket_send, wlen=32, slen=0, tot_len=32, <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.248: CTS-SXP-MSG:trp_socket_write freeing tx_buf, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.249: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.249: CTS-SXP-MSG:trp_socket_read readlen = -1; errno = 11, <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.300: CTS-SXP-MSG:trp_process_read_sock <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.300: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.300: CTS-SXP-MSG:RCVD peer 10.48.17.235 readlen:28, datalen:0 remain:4096 bufp
=
*Aug 16 05:42:54.301: CTS-SXP-MSG:sxp_handle_rx_msg_v2 <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.301: CTS-SXP-MSG:imu_sxp_conn_cr ci<1> cdbp->ph_conn_state<2>, <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.301: CTS-SXP-MSG:trp_socket_read readlen = 28; errno = 11, <10.48.17.235,
10.62.148.108>
*Aug 16 05:42:54.301: CTS-SXP-MSG:trp_process_read_sock <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:RCVD peer 10.48.17.235 readlen:52, datalen:0 remain:4096 bufp
=
*Aug 16 05:42:54.302: CTS-SXP-MSG:sxp_handle_rx_msg_v2 <1>, <10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:sxp_rcv_update_v4 <1> peer ip: 10.48.17.235
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:44, opc_ptr:0x3DFC7308,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:37, opc_ptr:0x3DFC730F,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:32, opc_ptr:0x3DFC7314,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:24, opc_ptr:0x3DFC731C,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:13, opc_ptr:0x3DFC7327,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.302: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:8, opc_ptr:0x3DFC732C,
<10.48.17.235, 10.62.148.108>
*Aug 16 05:42:54.303: CTS-SXP-MSG:1. msg type:3, total len:52, payl len:0, opc_ptr:0x3DFC7334,
<10.48.17.235, 10.62.148.108>
```

Die Paketerfassung aus der ISE für den Datenverkehr zum 3850-1 bestätigt, dass SXP-Zuordnungen gesendet werden.

No.	Time	Source	Destination	Protocol	Length	Info
10	2015-08-16 21:57:50.286099	10.48.17.235	10.62.148.108	SMPP	102	SMPP Bind_transmi
11	2015-08-16 21:57:50.286821	10.48.17.235	10.62.148.108	SMPP	126	SMPP Query_sm

> Frame 11: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
 > Ethernet II, Src: Vmware_99:29:cc (00:50:56:99:29:cc), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00)
 > Internet Protocol Version 4, Src: 10.48.17.235 (10.48.17.235), Dst: 10.62.148.108 (10.62.148.108)
 > Transmission Control Protocol, Src Port: 64999 (64999), Dst Port: activesync (1034), Seq: 29, Ack: 33, Len: 52
 > Short Message Peer to Peer, Command: Query_sm, Seq: 806480656, Len: 52

Length: 52
 Operation: Query_sm (0x00000003)
 Sequence #: 806480656
 Message id.: \021\002
 Type of number (originator): Unknown (0x10)
 Numbering plan indicator (originator): Unknown (0x10)
 Originator address: \v\005 \300\250\001\313\020\020\b\n0\021\353\300\250M\002\020\021\002

0000	00 07 4f 1c e8 00 00 50	56 99 29 cc 08 00 45 00	..0....P V.)...E.
0010	00 70 6a d8 40 00 40 06	14 eb 0a 30 11 eb 0a 3e	.pj.@.@. ...0...>
0020	94 6c fd e7 04 0a d8 2e	8f 8c 48 c5 e1 1b a0 18	.l..... ..H....
0030	39 08 bb 27 00 00 01 01	13 12 b6 72 86 e1 5a 6d	9..'.... ..r..Zm
0040	98 56 18 3c 5d 24 ba 00	98 85 00 00 00 34 00 00	.V.<]\$. ..4..
0050	00 03 10 10 04 0a 30 11	eb 10 11 02 00 10 10 0b0.
0060	05 20 c0 a8 01 cb 10 10	08 0a 30 11 eb c0 a8 4d0...M
0070	02 10 11 02 00 10 10 0b	05 20 0a 00 00 64d

Wireshark verwendet einen standardmäßigen SMPP-Decoder. So überprüfen Sie die Nutzlast:

10 (SGT = 16) für "c0 a8 01 cb" (192.168.1.203)

10 (SGT = 16) für "0a 00 00 64" (10.0.0.100)

3850-1 installiert alle von der ISE erhaltenen Zuordnungen.

```

KSEC-3850-1# show cts sxp sgt-map
SXP Node ID(generated):0xC0A84D01(192.168.77.1)
IP-SGT Mappings as follows:
IPv4,SGT: <10.0.0.100 , 16:SGT_IT>
source : SXP;
Peer IP : 10.48.17.235;
Ins Num : 2;
Status : Active;
Seq Num : 439
Peer Seq: 0A3011EB,C0A84D02,
IPv4,SGT: <192.168.1.203 , 16:SGT_IT>
source : SXP;
Peer IP : 10.48.17.235;
Ins Num : 6;
Status : Active;
Seq Num : 21
Peer Seq: 0A3011EB,
Total number of IP-SGT Mappings: 2

```

```

KSEC-3850-1# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

```

IP Address	SGT	Source
10.0.0.100	16	SXP
192.168.1.203	16	SXP

IP-SGT Active Bindings Summary

```
=====
Total number of CLI      bindings = 1
Total number of SXP      bindings = 2
Total number of active   bindings = 3
```

Schritt 5: Herunterladen und Durchsetzen von Richtlinien

Laden Sie die richtige Richtlinie von der ISE herunter. (Matrix-Zeile mit SGT 16)

```
KSEC-3850-1#show cts role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
IPv4 Role-based permissions from group 16:SGT_IT to group 9:SGT_Marketing:
```

```
ICMP-10
```

```
Deny IP-00
```

```
RBACL Monitor All for Dynamic Policies : FALSE
```

```
RBACL Monitor All for Configured Policies : FALSE
```

ICMP-Datenverkehr von 10.0.0.100 (SGT IT) bis 10.0.0.1 (SGT-Marketing) ist zulässig, Zähler steigen.

```
KSEC-3850-1#show cts role-based counters from 16
```

```
Role-based IPv4 counters
```

```
#Hardware counters are not available for specific SGT/DGT
```

```
#Use this command without arguments to see hardware counters
```

From	To	SW-Denied	SW-Permitted		
16	9	0	0	11	0

Wenn die Verwendung der Telnet-Verbindung fehlschlägt, erhöhen sich die Zähler der verworfenen Geräte.

```
KSEC-3850-1#show cts role-based counters from 16
```

```
Role-based IPv4 counters
```

```
#Hardware counters are not available for specific SGT/DGT
```

```
#Use this command without arguments to see hardware counters
```

From	To	SW-Denied	SW-Permitted		
16	9	3	0	11	0

Beachten Sie, dass für die 3850-2 keine speziellen Richtlinien gelten, der gesamte Datenverkehr zulässig ist.

```
KSEC-3850-2#show cts role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
RBACL Monitor All for Dynamic Policies : FALSE
```

```
RBACL Monitor All for Configured Policies : FALSE
```

Nach der Änderung der SG-ACL für ISE, dem Hinzufügen von permit tcp und der cts-Aktualisierungsrichtlinie für 3850-1 wird Telnet-Datenverkehr akzeptiert.

Es ist auch möglich, zur Verhaltensbestätigung den lokalen Cache Flexible NetFlow (ab IOS-XE 3.7.2 SGT-kompatibel) zu verwenden.

```
flow record cts-v4
match ipv4 protocol
match ipv4 source address
```

```

match ipv4 destination address
match transport source-port
match transport destination-port
match flow direction
match flow cts source group-tag
match flow cts destination group-tag
collect counter packets long

```

```

flow monitor F_MON
record cts-v4

```

```

interface GigabitEthernet1/0/3
ip flow monitor F_MON input
ip flow monitor F_MON output

```

Die Ergebnisse zeigen den Datenverkehr, der von 3850-2 empfangen wurde. Das Quell-SGT ist 0, da der empfangene Datenverkehr kein SGT (keine cts-Verbindung) hat, aber das Ziel-Gruppen-Tag wird basierend auf der lokalen Zuordnungstabelle automatisch ersetzt.

```
KSEC-3850-1#show flow monitor F_MON cache
```

```

Cache type:                Normal (Platform cache)
Cache size:                 Unknown
Current entries:           6

```

```

Flows added:                1978
Flows aged:                 1972
- Active timeout ( 1800 secs) 30
- Inactive timeout ( 15 secs) 1942

```

IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	FLOW DIRN	FLOW CTS SRC GROUP
TAG	FLOW CTS DST GROUP TAG	IP PROT	pkts long		
150.1.7.1	224.0.0.10	0	0	Output	
0	0	88	57		
10.62.148.1	224.0.0.13	0	8192	Output	
0	0	103	0		
7.7.4.1	224.0.0.10	0	0	Output	
0	0	88	56		
10.0.0.1	10.0.0.100	0	0	Output	
0	0	1	1388		
150.1.7.105	224.0.0.5	0	0	Output	
0	0	89	24		
150.1.7.1	224.0.0.5	0	0	Output	
0	0	89	24		
10.0.0.100	10.0.0.1	0	2048	Input	
0	9	1	1388		

Der lokale NetFlow-Cache kann zur Bestätigung des empfangenen Datenverkehrs verwendet werden. Wenn dieser Datenverkehr angenommen oder verworfen wird, wird dies durch zuvor vorgestellte CTS-Zähler bestätigt.

Die ISE ermöglicht auch das Generieren von SXP-Bindungs- und Verbindungsberichten, wie in diesem Bild gezeigt.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

RADIUS Livelog TACACS Livelog Reports Troubleshoot Adaptive Network Control

Report Selector

Favorites

ISE Reports

- Audit 10 reports
- Device Administration 4 reports
- Diagnostics 10 reports
- Endpoints and Users 15 reports
- Guest Access Reports 5 reports
- SXP**
 - SXP Binding
 - SXP Connection**

Time Range: Yesterday Run

SXP Connection

From 08/15/2015 12:00:00 AM to 08/15/2015 11:59:59 PM

Generated Time	Peer IP	Port	SXP Node Ip	VPN	SXP Mode	SXP Version	Password Type	Status	Reason
2015-08-15 07:13:41.1	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:11:41.1	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:09:41.0	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:07:40.7	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:05:40.4	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:03:40.4	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 07:01:40.2	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 06:59:39.9	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 06:57:39.5	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 06:55:39.3	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	
2015-08-15 06:53:38.9	10.48.67.250	64999	10.48.17.235	default	BOTH	VERSION_4	CUSTOM	PendingOn	

Referenzen

- [ASA Version 9.2.1 VPN-Status mit ISE-Konfigurationsbeispiel](#)
- [ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung](#)
- [Konfigurationsanleitung für Cisco TrustSec-Switches: Cisco TrustSec im Überblick](#)
- [Cisco TrustSec-Bereitstellung und Roadmap](#)
- [Konfigurationsleitfaden für Cisco Catalyst 3850 TrustSec](#)
- [Cisco TrustSec-Kompatibilitätsmatrix](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)