

ISE 2.0 TrustSec SXP Luistener en Luidspreker configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[verkeersstroom](#)

[Configuraties](#)

[Switch 3850-1](#)

[Switch 3850-2](#)

[ISE](#)

[Verifiëren](#)

[Referenties](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit document beschrijft hoe u de functie kunt configureren en oplossen die Cisco Identity Services Engine (ISE) versie 2.0 ondersteunt TrustSec SGT Exchange Protocol (SXP) in een Lozer- en Luidsprekermodus.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst-switchconfiguratie
- Identity Services Engine (ISE) en TrustSec-services

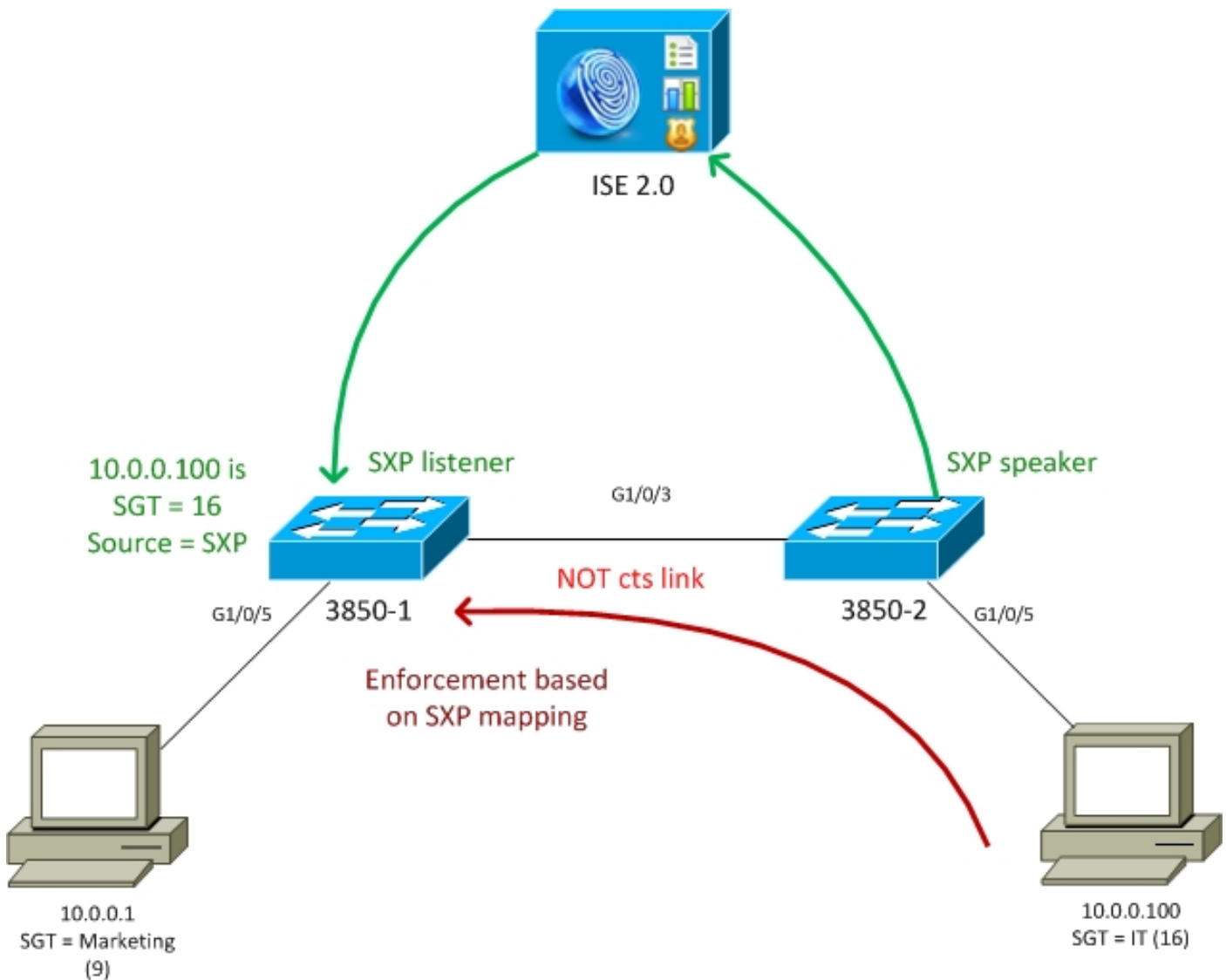
Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Catalyst 3850-switch met software IOS-XE 3.7.2 en hoger
- Cisco ISE, release 2.0 en hoger

Configureren

Netwerkdigram



verkeersstroom

- 3850-2 is 802.1x authenticator voor 10.0.100 - ISE Terugkeren Security Group Tag (SGT) 16 (IT) voor succesvolle authenticatie
- De schakelaar 3850-2 leert flexibel IP adres (ip apparaat tracking) en stuurt kartelinformatie (IP-SGT) naar ISE met behulp van SXP-protocol
- 3850-1 is 802.1x authenticator voor 10.0.0.1 - ISE Terugkerend SGT tag 9 (Marketing) voor succesvolle authenticatie
- 3850-1 ontvangt SXP-kaartinformatie van ISE (10.0.100 is SGT 16), downloads het beleid van ISE
- Verkeer dat van 10.0.100 naar 10.0.1 wordt verzonden, wordt vóór 3850-2 (geen specifiek beleid gedownload) naar 3850-1 verzonden, wat beleid IT (16) -> Marketing (9) afdwingt

Let op dat het verband tussen de switches geen link is - dus alle afstandsbediening van de switches is via SXP protocol geïnstalleerd.

Opmerking: Niet alle switches hebben de hardware die geprogrammeerd kan worden via beleid dat van ISE is ontvangen, op basis van ontvangen SXP-mappings. Raadpleeg voor verificatie altijd de nieuwste TrustSec-compatibiliteitsmatrix of neem contact op met Cisco-

systemen.

Configuraties

Raadpleeg de artikelen in de sectie Verwijzingen voor meer informatie over de basisconfiguratie van TrustSec.

Switch 3850-1

Switch beëindigt 802.1x sessie met SGT toewijzing en ook als SXP spreker naar 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

Switch eindigen 802.1x sessie met SGT toewijzing en ook als SXP luisteraar mapping van 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
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

Stap 1. Netwerkttoegangsapparaten

Navigeer aan **Werkcentra > Apparaatbeheer > Netwerkbronnen**, voeg beide switches toe met gedeeld geheim cisco en TrustSec-wachtwoord Krakau123.

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: KSEC-3850-1
Description: []

* IP Address: 10.62.148.108 / 32

* Device Profile: Cisco [+]
Model Name: []
Software Version: []

* Network Device Group

Location: All Locations [Set To Default]
Device Type: All Device Types [Set To Default]

- RADIUS Authentication Settings
- TACACS+ Authentication Settings
- SNMP Settings
- Advanced TrustSec Settings

Stap 2. Beveiligingsgroepen

Om SGT voor IT en marketing toe te voegen, navigeer naar **Workcenters > TrustSec > Componenten > Security Group**.

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

Stap 3. Security groepen ACL

Als u Security Group ACL's wilt toevoegen, navigeer dan naar **werkcentra > TrustSec > Componenten > Security Group ACL's**.

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

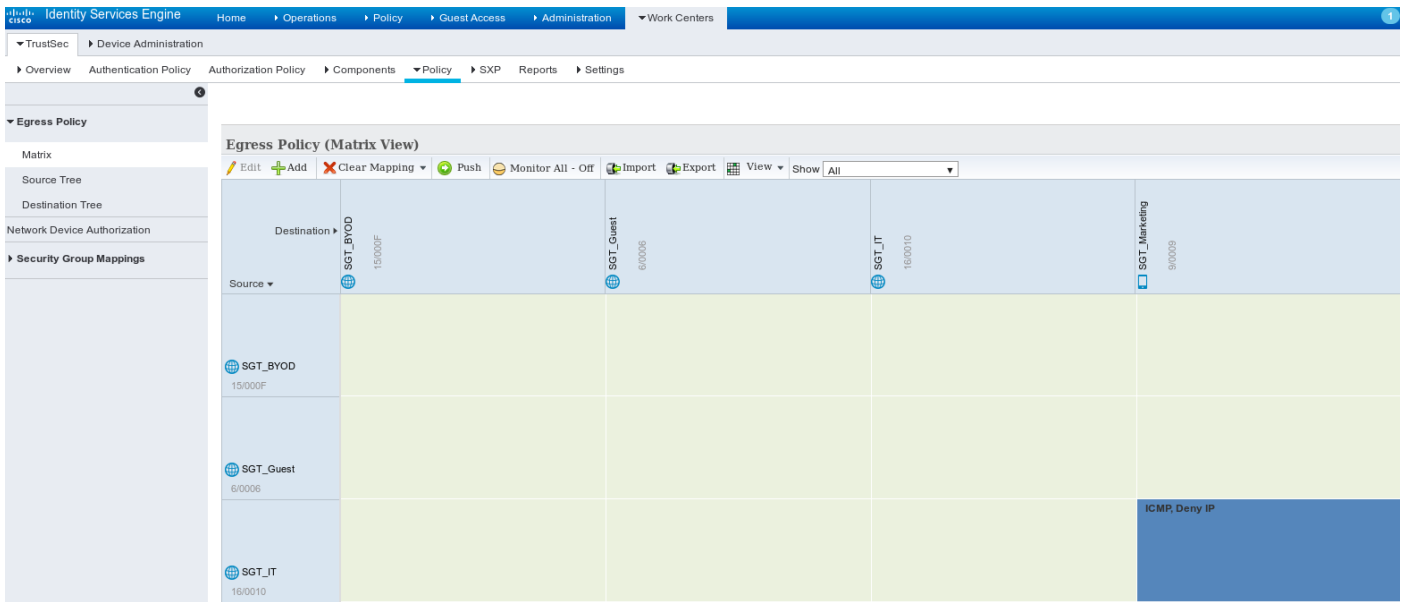
IP Version IPv4 IPv6 Agnostic

* Security Group ACL content

Alleen ICMP-verkeer toestaan.

Stap 4. VertrouwenSec-beleid

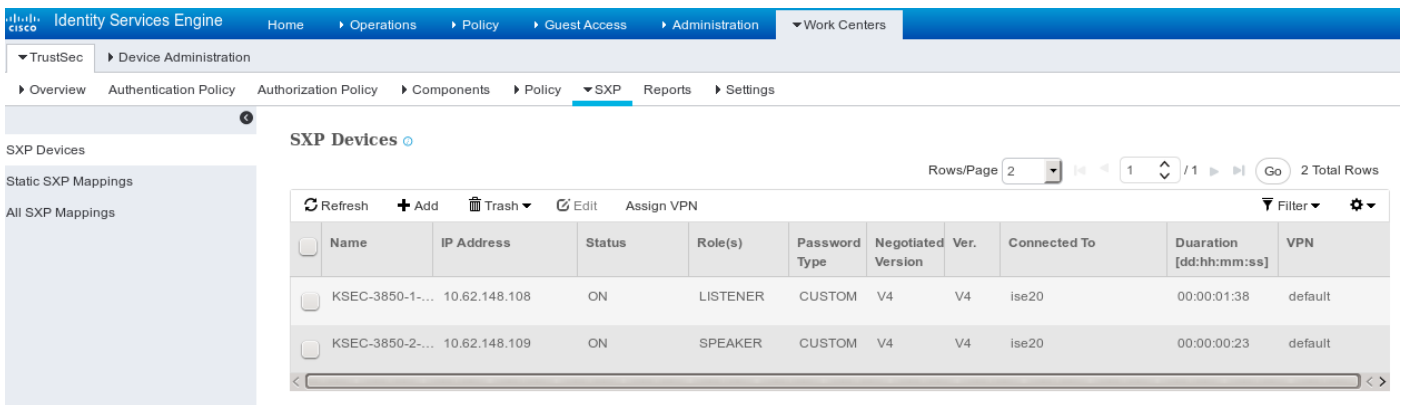
Om beleid toe te voegen dat het verkeer van IT naar marketing regelt, navigeer naar **Work Centers > TrustSec > Componenten > Egress Policy > Matrix**.



Stel de standaard invoerregel in om al het verkeer te ontkenen.

Stap 5. SXP-apparaten

Om SXP te configureren stuurt u een luisteraar en spreker voor de corresponderende switches door te navigeren naar **Work Centers > TrustSec > SXP Devices**.



Gebruik wachtwoordcisco (of een andere die voor sxp in de schakelaar is ingesteld).

Stap 6. Goedkeuringsbeleid

Zorg ervoor dat het autorisatiebeleid correcte SGT tags voor elke gebruiker retourneert, navigeer naar **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

Verifiëren

Stap 1. Schakelt via ISE voor TS

Van elke schakelaar geef TrustSec-referenties (ingesteld in ISE/Stap 1) aan om de PAC te krijgen.

```
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.

Zorg ervoor dat PAC wordt gedownload.

```
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
```

En het milieubeleid is nieuw leven ingeblazen.

```
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

Herhaal hetzelfde proces voor de 3850-1

Stap 2. 802.1x-sessies

Nadat de IT-gebruiker is geauthentificeerd, wordt de juiste tag toegewezen.

```
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
```

De afbeelding is geïnstalleerd in de lokale SGT-IP-tabel.

```
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
------------	----	-------

Stap 3: SXP-luidspreker

3850-2 stuurt de mapping naar ISE, switch debugs voor 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_recv 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-rapporten (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

```

En alle afbeeldingen weergeven via GUI (inclusief mapping voor 10.0.100, ontvangen van 3850-2), zoals in deze afbeelding.

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation menu includes 'TrustSec' and 'Device Administration'. The main content area displays 'All SXP Mappings' with a table containing two entries. The first entry shows IP Address 10.0.0.100/32, SGT SGT_IT(16/0010), Learned From 192.168.77.2, and Learned By SXP. The second entry shows IP Address 192.168.1.203/32, SGT SGT_IT(16/0010), Learned From 10.48.17.235,10.48.67.250, and Learned By Session.

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 is de identificator van SXP-verbinding op 3850-2 (hoogste IP-adres gedefinieerd).

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

Stap 4. SXP-luisteraar

Dan weergeeft ISE die mapping aan 3850-1, switch debugs.

```
*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_rcv 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>
```

De pakketvastlegging van ISE voor verkeer naar 3850-1 bevestigt dat SXP in kaart wordt gebracht.

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 gebruikt standaard SMP-decoder. Zo controleert u de lading:

10 (SGT = 16) voor "c0 a8 01 cb" (192.168.1.2003)

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

3850-1 installeert alle afbeeldingen die van ISE zijn ontvangen.

```

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
```

Stap 5: Beleidstoepassingen en handhaving

Download het juiste beleid van ISE (Matrixrij met 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
```

Het ICMP-verkeer van 10.0.100 (SGT IT) naar 10.0.0.1 (SGT Marketing) is toegestaan, tellers stijgen.

```
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

Wanneer het proberen om telnet verbinding te gebruiken mislukt, daalt tellers stijgen.

```
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

Er is geen specifiek beleid voor 3850-2, al het verkeer is toegestaan.

```
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
```

Na het wijzigen van SG ACL op ISE, het toevoegen van vergunning tcp, en cts verfrissen beleid op 3850-1 - dan wordt het telnet verkeer aanvaard.

Het is ook mogelijk om Flexibel NetFlow (beginnend bij IOS-XE 3.7.2 het is SGT bewust) lokaal cache te gebruiken om gedrag te bevestigen.

```
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

```

De resultaten tonen verkeer dat van 3850-2 is ontvangen. Bron SGT is 0 omdat ontvangen verkeer geen SGT (geen cts link) heeft, maar de tag van de doelgroep wordt automatisch vervangen op basis van de lokale mapping tabel.

```

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	

NetFlow Local cache kan worden gebruikt om ontvangen verkeer te bevestigen. Als dat verkeer wordt geaccepteerd of afgezet, wordt dat bevestigd door de voordien gepresenteerde loketten.

Met ISE kunnen ook SXP-verbindings- en -verbindingsrapporten worden gegenereerd, zoals in deze afbeelding wordt getoond.

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

Filters

* 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	

Referenties

- [ASA versie 9.2.1 VPN-post met ISE Configuration Voorbeeld](#)
- [ASA en Catalyst 3750X Series switchstack-SEC Configuratievoorbeeld en probleemoplossing](#)
- [Cisco TrustSec-switchconfiguratie-gids: De betekenis van Cisco TrustSec](#)
- [Cisco TrustSec-implementatie en RoadMap](#)
- [Cisco Catalyst 3850 Tech-configuratiehandleiding](#)
- [Cisco-compatibiliteitsmatrix voor TechSEC](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)