Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Traffic Flow](#)
[Configurations](#)
[Switch 3850-1](#)
[Switch 3850-2](#)
[ISE](#)
[Verify](#)
[References](#)
[Related Cisco Support Community Discussions](#)

Introduction

This document describes how to configure and troubleshoot the feature that Cisco Identity Services Engine (ISE) version 2.0 supports TrustSec SGT Exchange Protocol (SXP) in a Lister and Speaker mode.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst Switch Configuration
- Identity Services Engine (ISE) and TrustSec services

Components Used

The information in this document is based on these software versions:

- Cisco Catalyst 3850 switch with software IOS-XE 3.7.2 and later
- Cisco ISE, Release 2.0 and later

Configure

Network Diagram

Traffic Flow

- 3850-2 is 802.1x authenticator for 10.0.0.100 - ISE returning Security Group Tag (SGT) 16 (IT) for successful authentication
- 3850-2 switch learns supplicant ip address (ip device tracking) and sends mapping information (IP-SGT) to ISE using SXP protocol
- 3850-1 is 802.1x authenticator for 10.0.0.1 - ISE returning SGT tag 9 (Marketing) for successful authentication
- 3850-1 receives SXP mapping information from ISE (10.0.0.100 is SGT 16), downloads the policy from ISE
- Traffic sent from 10.0.0.100 to 10.0.0.1 is forwarded by 3850-2 (no specific policies downloaded) to 3850-1 which is enforcer hitting policy IT (16) -> Marketing (9)

Please note the link between the switches is not cts link - so all remote mappings on the switches are installed via SXP protocol.

> **Note**: Not all the switches have the hardware allowing to be programmed via policy received from ISE based on received SXP mappings. For verification please always refer to the latest TrustSec Compatibility Matrix or contact Cisco Systems.

Configurations

For details regarding basic TrustSec configuration, refer to the articles in References section.

Switch 3850-1

Switch terminates 802.1x session with SGT assignment and also as SXP speaker towards 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

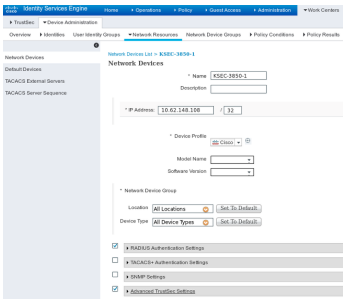
Switch terminates 802.1x session with SGT assignment and also as SXP listener getting mapping from ISE.

```
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

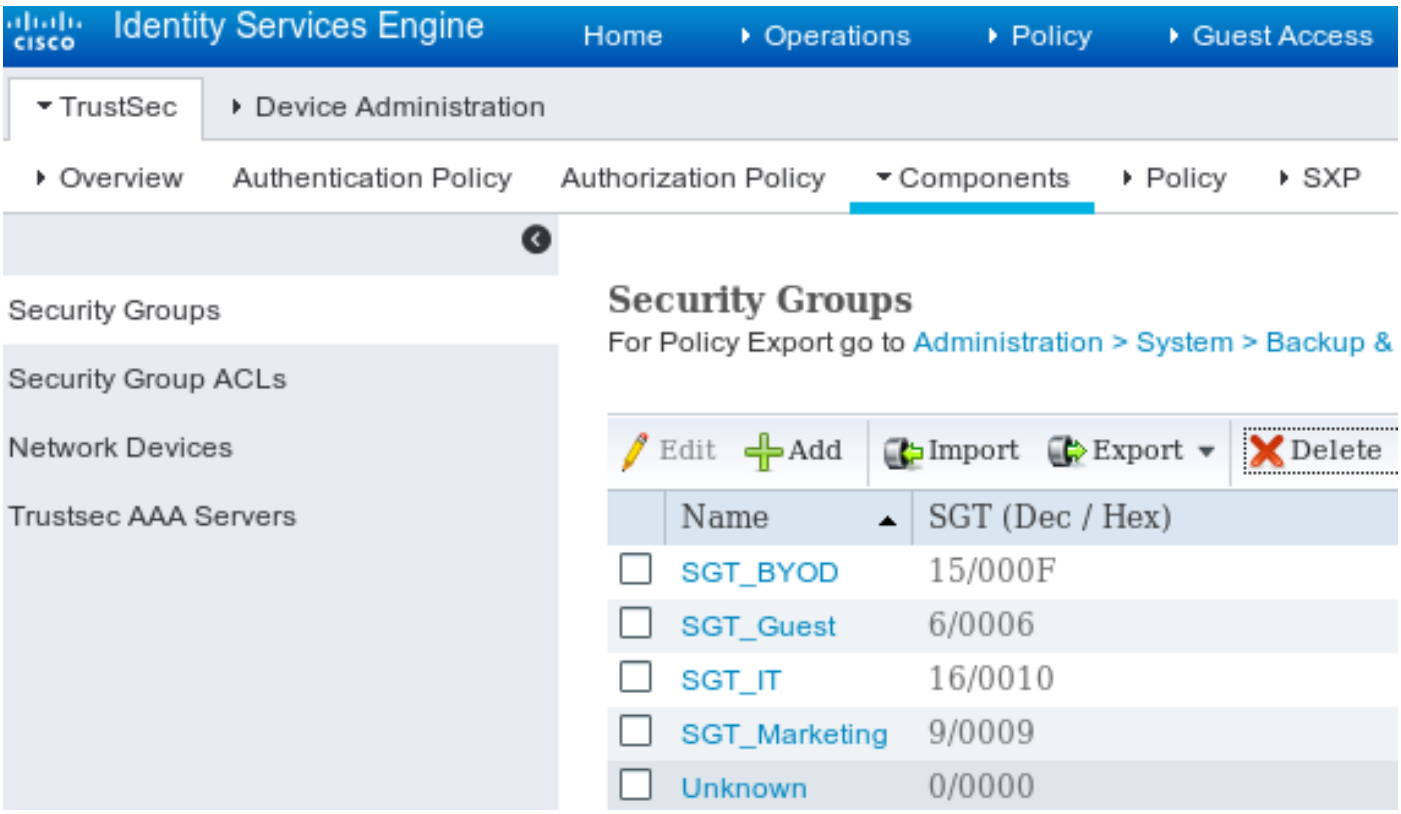
Step 1. Network Access Devices

Navigate to **Work Centers > Device Administration > Network Resources,** add both switches with shared secret cisco and TrustSec password Krakow123.



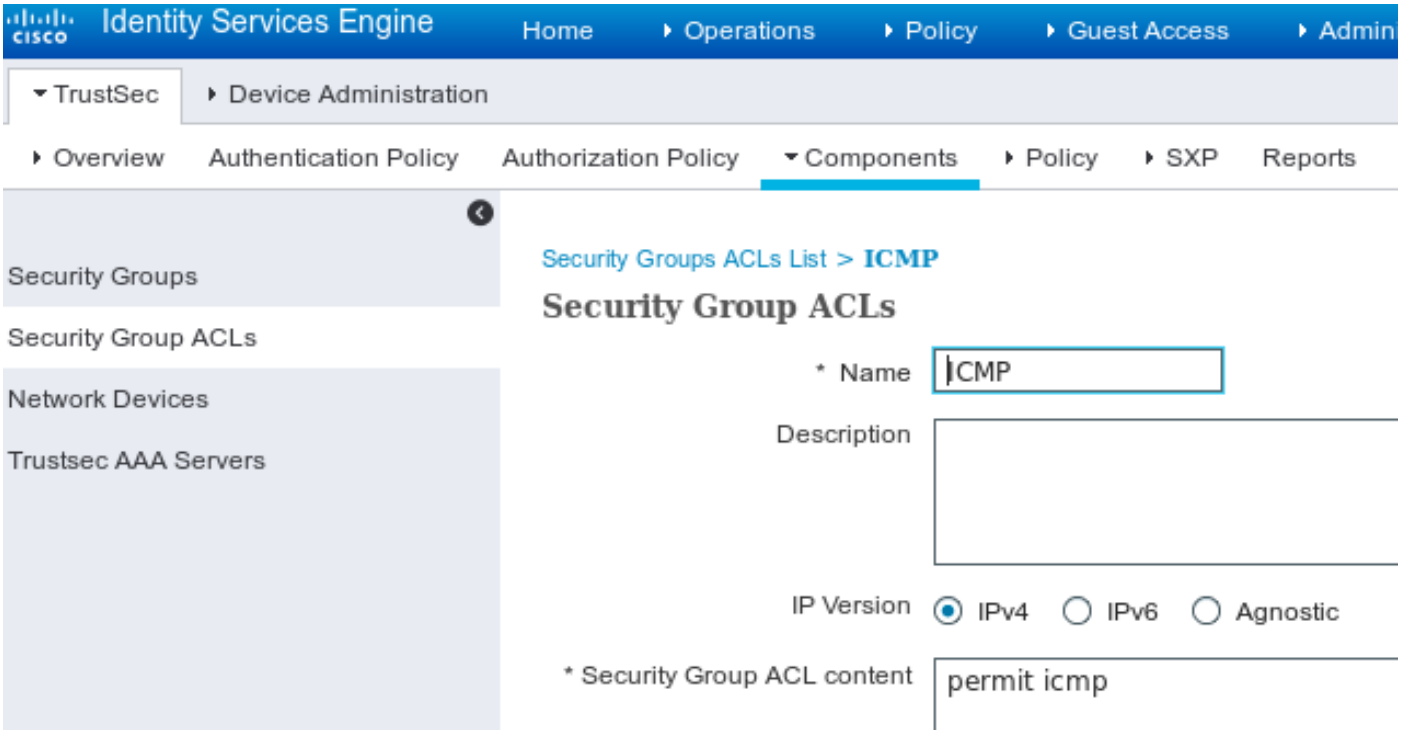
Step 2. Security Groups

In order to add SGT for IT and Marketing, navigate to **Work Centers > TrustSec > Components > Security Groups.**



Step 3. Security Groups ACL

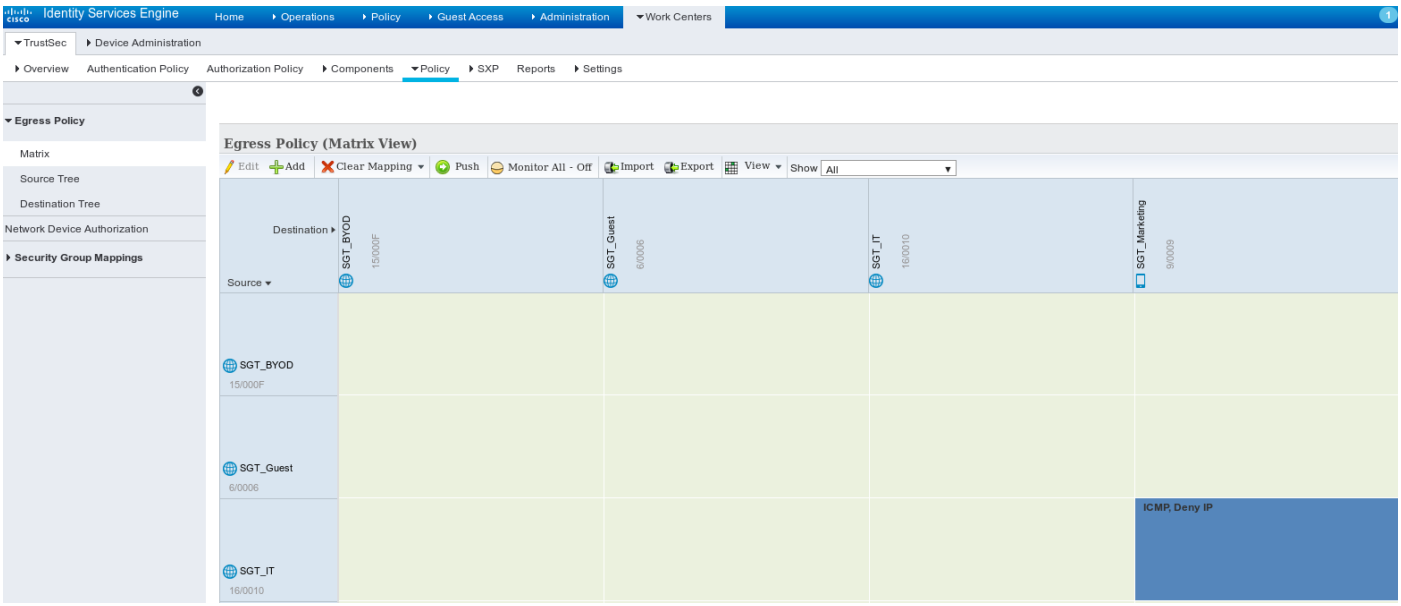
In order to add Security Group ACL, navigate to **Work Centers > TrustSec > Components > Security Group ACLs.**



Allow only ICMP traffic.

Step 4. TrustSec Policy

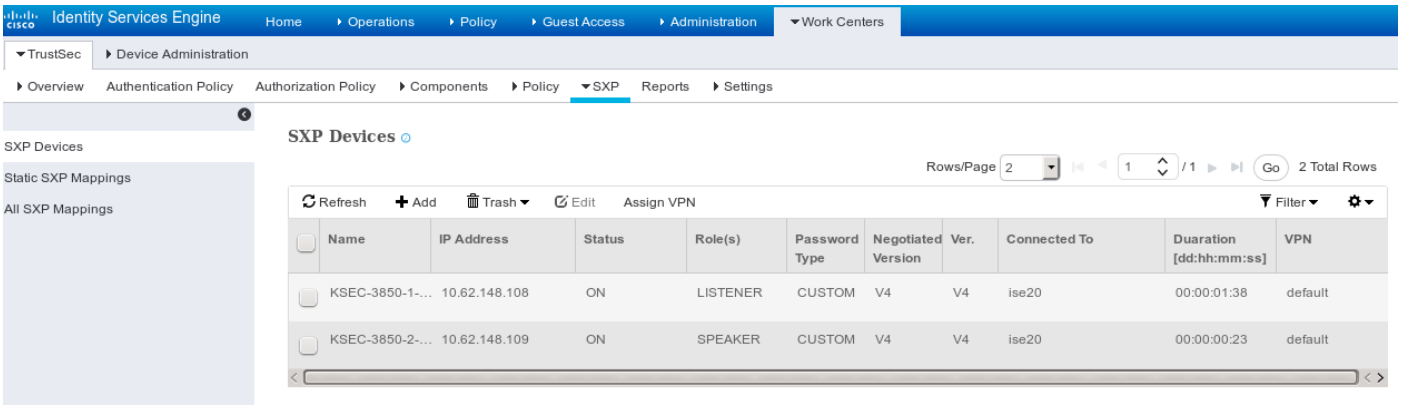
In order to add policy controlling the traffic from IT to Marketing, navigate to **Work Centers > TrustSec > Components > Egress Policy > Matrix.**



Set the default entry catch all rule to deny all traffic.

Step 5. SXP Devices

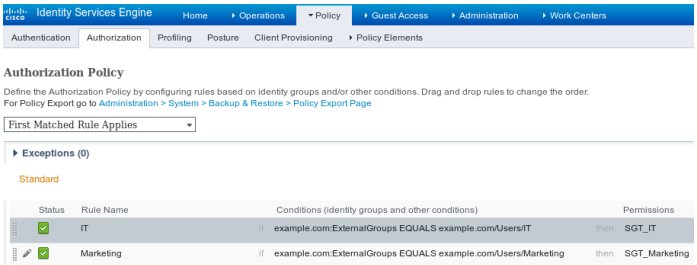
In order to configure SXP listener and speaker for the corresponding switches, navigate to **Work Centers > TrustSec > SXP Devices.**



Use password cisco (or any other configured for sxp on the switch).

Step 6. Authorization Policy

Ensure that authorization policy returns correct SGT tags for each user, navigate to **Policy > Authorization.**



Verify

Step 1. Switch joining ISE for cts

From every switch provide TrustSec credentials (configured in ISE/Step1) to get the PAC.

```
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.
```

Ensure that PAC is downloaded.

```
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:
000200B800030001000400 1065D55BAF222BBC73362A7810A04A005B0006009C00030100B26D8DDC125B6595067D64F9
17DA624C0000001355CB2E1C00093A800E567155E0DE76419D2F3B97D890F34F109C4C42F586B29050CEC7B441E0CA60
FC6684D4F6E8263FA2623A6E450927815A140CD3B9D68988E95D8C1E65544E222E187C647B9F7F3F230F6DB4F80F3C20
1ACD623B309077E27688EDF7704740A1CD3F18CE8485788054C19909083ED303BB49A6975AC0395D41E1227B
 Refresh timer is set for 12w4d
```

And environment policy is refreshed.

```
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
```

Repeat the same process for 3850-1

Step 2. 802.1x sessions

After IT user is authenticated, the correct tag is assigned.

```
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
```

The mapping is installed in local SGT-IP table.

```
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
```

Step 3. SXP speaker

3850-2 sends the mapping to ISE, switch debugs for 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>
```

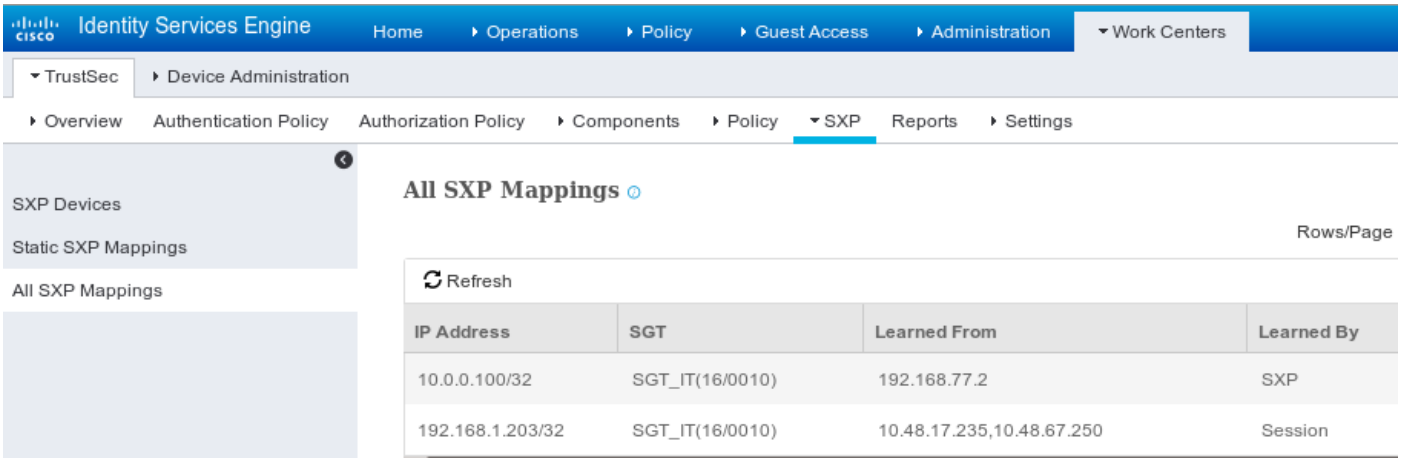
```
*Aug 16 12:48:30.278: CTS-SXP-MSG:trp_socket_read <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.278: CTS-SXP-MSG:RCVD peer 10.48.17.235 readlen:32, datalen:0 remain:4096 bufp
=
*Aug 16 12:48:30.278: CTS-SXP-MSG:sxp_handle_rx_msg_v2 <1>, <10.48.17.235, 10.62.148.109>
*Aug 16 12:48:30.279: CTS-SXP-MSG:imu_sxp_conn_cr <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 reports (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
```

And present all mappings via GUI (including mapping for 10.0.0.100 received from 3850-2), as shown in this image.



192.168.77.2 is the identifier of SXP connection on 3850-2 (highest ip address defined).

```
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
```

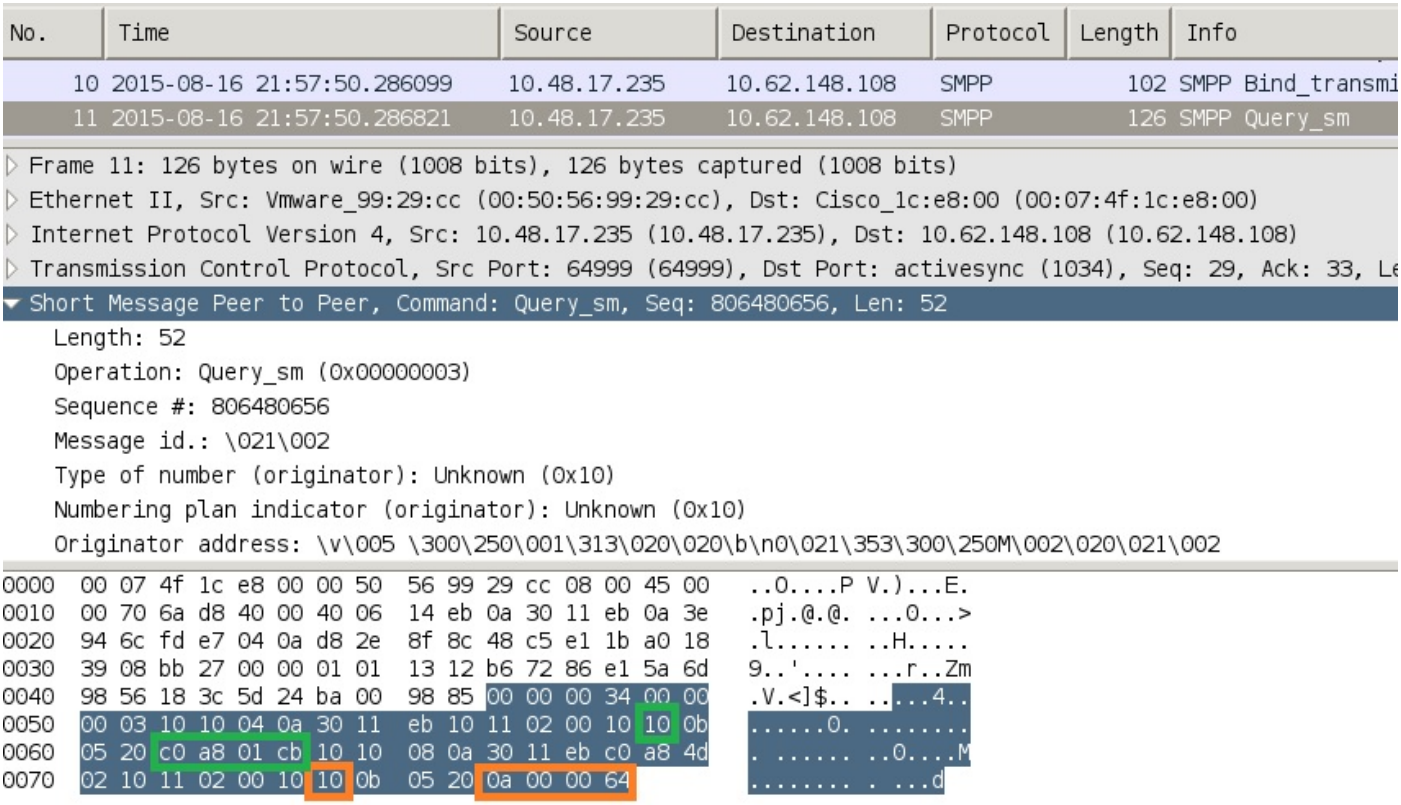
Step 4. SXP listener

Then ISE resends that mapping to 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_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_recv_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>
```

Packet capture taken from ISE for traffic towards 3850-1 confirms SXP mappings are being sent.



Wireshark uses standard SMPP decoder. To check the payload:

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

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

3850-1 installs all the mappings received from ISE.

```
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
```

Step 5. Policy download and enforcement

Download the correct policy from ISE. (Matrix row with 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 traffic from 10.0.0.100 (SGT IT) to 10.0.0.1 (SGT Marketing) is allowed, counters increase.

```
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
```

When trying to use telnet connection fails, drop counters increase.

```
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
```

Please note there is no specific policy on 3850-2, all traffic is allowed.

```
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
```

After modifying SG ACL on ISE, adding permit tcp, and cts refresh policy on 3850-1 - then telnet traffic is accepted.

Its possible also to use Flexible Netflow (starting from IOS-XE 3.7.2 it's SGT aware) local cache to confirm behavior.

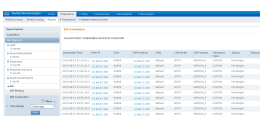
```
KSEC-3850-2#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

The results shows traffic received from 3850-2. Source SGT is 0 because received traffic does not have any SGT (no cts link), but destination group tag is automatically replaced based on the local mapping table.

```
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 can be used to confirm received traffic. If that traffic is accepted or dropped, that is confirmed by cts counters presented before.

ISE also allows to generate SXP binding and connection reports, as shown in this image.



References

- ASA Version 9.2.1 VPN Posture with ISE Configuration Example
- ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide
- Cisco TrustSec Switch Configuration Guide: Understanding Cisco TrustSec
- Cisco TrustSec Deployment and RoadMap
- Cisco Catalyst 3850 TrustSec configuration Guide
- Cisco TrustSec Compatibility Matrix
- Technical Support & Documentation - Cisco Systems