ISE 2.0 TrustSec SXP 리스너 및 스피커 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine) 버전 2.0이 클러스터 및 스피커 모드에서 SXP(TrustSec SGT Exchange Protocol)를 지원하는 기능을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst 스위치 구성
- ISE(Identity Services Engine) 및 TrustSec 서비스

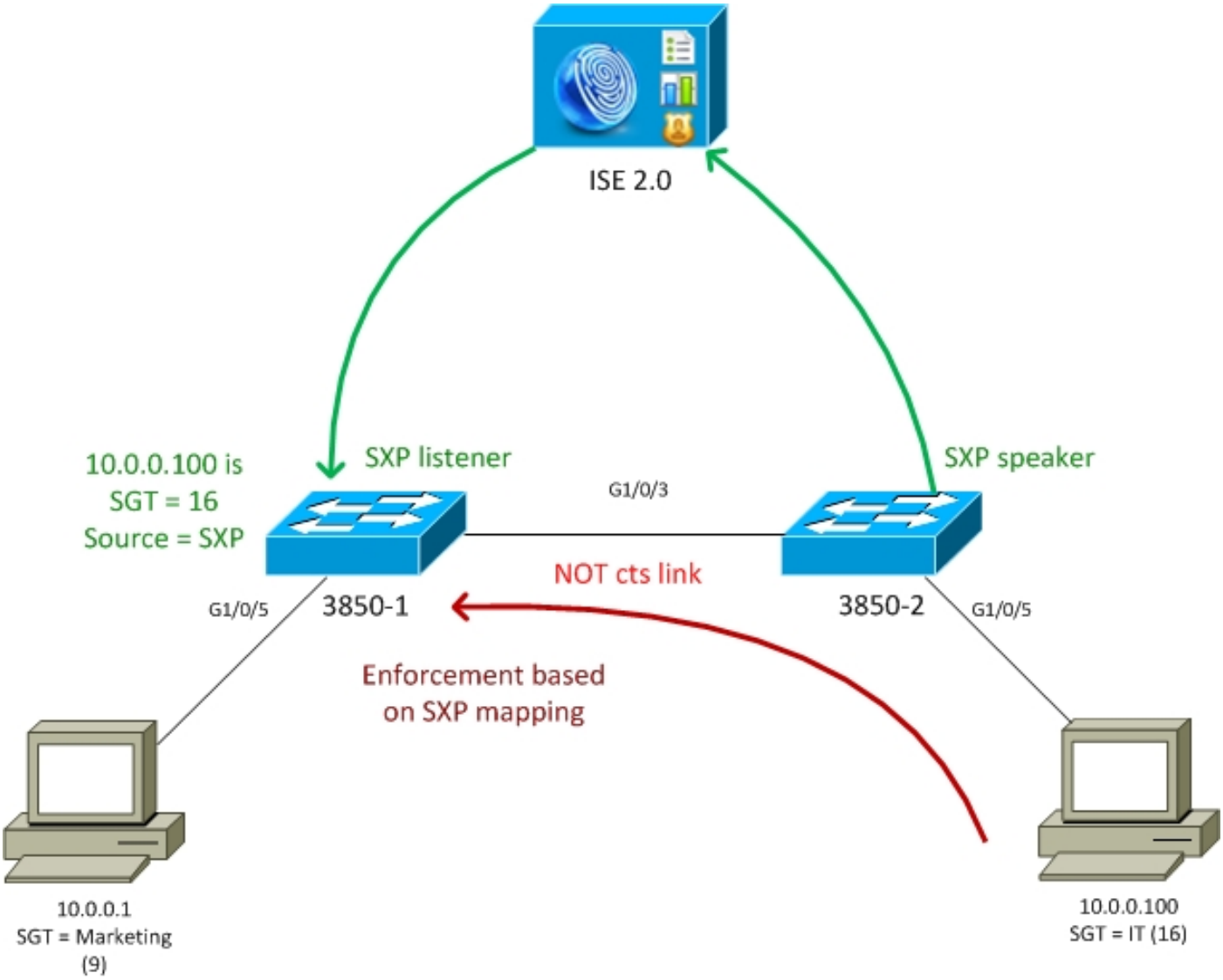
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- 소프트웨어 IOS-XE 3.7.2 이상이 포함된 Cisco Catalyst 3850 스위치
- Cisco ISE, 릴리스 2.0 이상

구성

네트워크 다이어그램



트래픽 흐름

- 3850-2는 10.0.0.100용 802.1x 인증자 - 성공적인 인증을 위해 ISE에서 SGT(Security Group Tag) 16(IT) 반환
- 3850-2 스위치는 SXP 프로토콜을 사용하여 신청자 IP 주소(ip 디바이스 추적)를 학습하고 ISE에 매핑 정보(IP-SGT)를 보냅니다.
- 3850-1은 10.0.0.1용 802.1x 인증자 - ISE에서 성공적인 인증을 위해 SGT 태그 9(마케팅)를 반환
- 3850-1은 ISE에서 SXP 매핑 정보(10.0.0.100은 SGT 16) 수신, ISE에서 정책 다운로드
- 10.0.0.100에서 10.0.0.1으로 전송된 트래픽은 3850-2(특정 정책은 다운로드되지 않음)에 의해 3850-1로 전달되며, 이는 정책 IT(16) -> 마케팅(9)을 적중하는 집행자입니다.

스위치 간 링크는 cts 링크가 아니므로 스위치의 모든 원격 매핑이 SXP 프로토콜을 통해 설치됩니다.

> **참고:**모든 스위치에는 수신된 SXP 매핑을 기반으로 ISE에서 받은 정책을 통해 프로그래밍할 수 있는 하드웨어가 없습니다.확인을 위해 항상 최신 TrustSec 호환성 매트릭스를 참조하거나 Cisco Systems에 문의하십시오.

구성

기본 TrustSec 구성에 대한 자세한 내용은 참조 섹션의 기사를 참조하십시오.

스위치 3850-1

스위치는 SGT를 할당하고 ISE를 위한 SXP 스피커로도 802.1x 세션을 종료합니다.

```
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
```

스위치 3850-2

스위치는 SGT 할당을 사용하는 802.1x 세션을 종료하고 ISE에서 매핑을 가져오는 SXP 리스너로도 종료합니다.

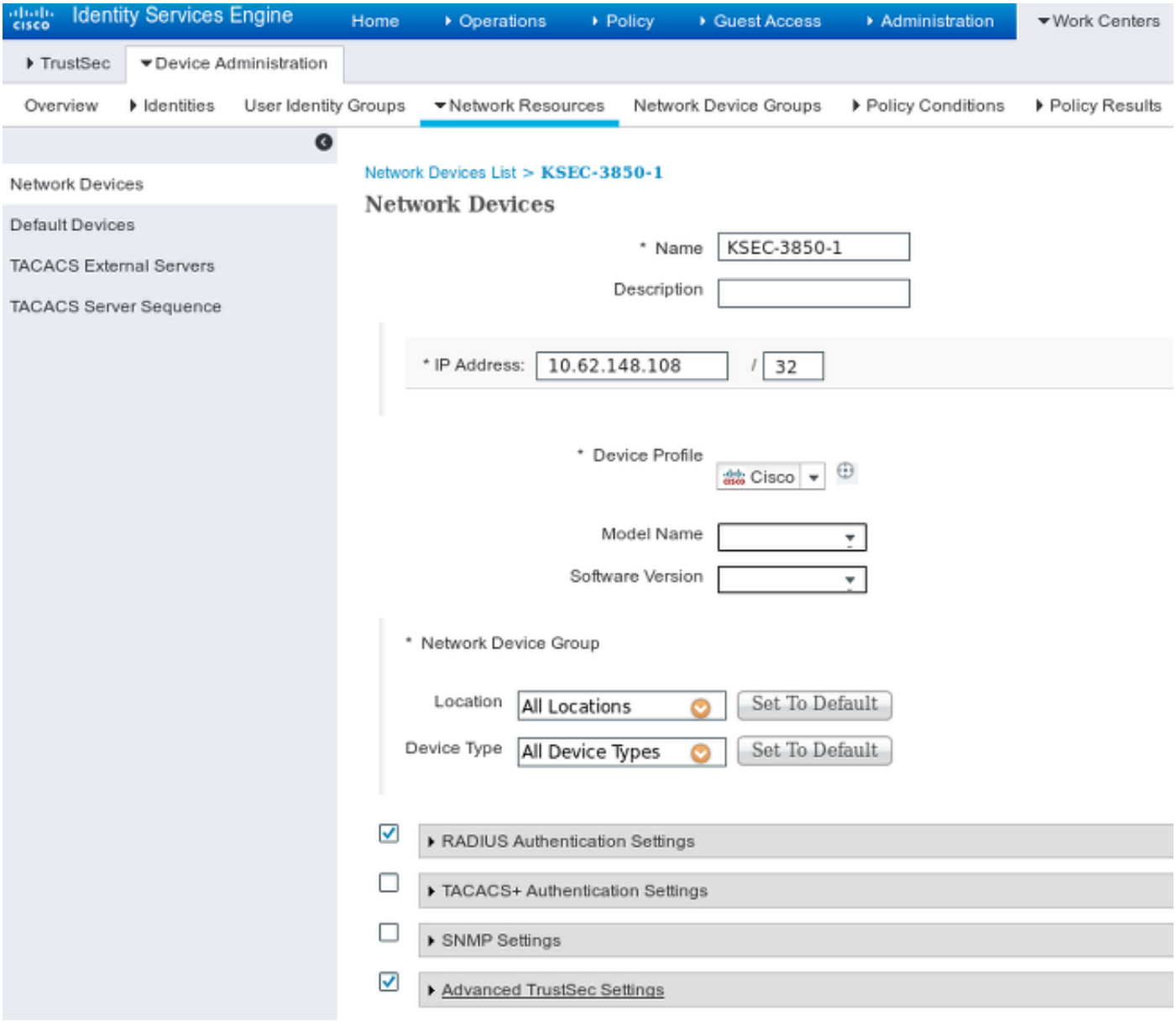
```
aaa authentication dot1x default group ISE_mgarcarz
aaa authorization network default group ISE_mgarcarz
aaa authorization network ISE_mgarcarz group ISE_mgarcarz
aaa accounting dot1x default start-stop group ISE_mgarcarz
aaa accounting update newinfo

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

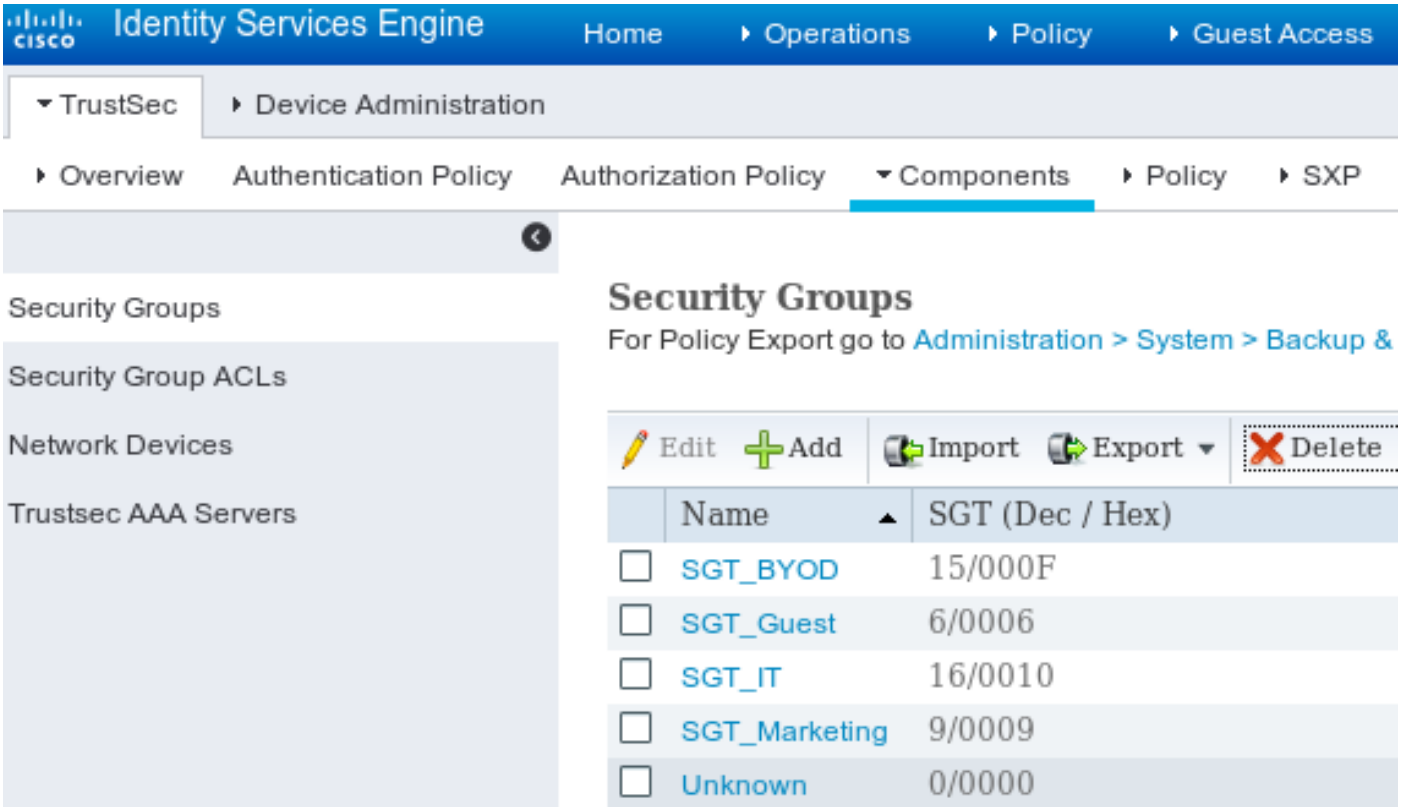
1단계. 네트워크 액세스 디바이스

Work Centers(작업 **센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스)로 이동하여** 공유 비밀 cisco 및 TrustSec 비밀번호 Krakow123과 함께 두 스위치를 추가합니다.



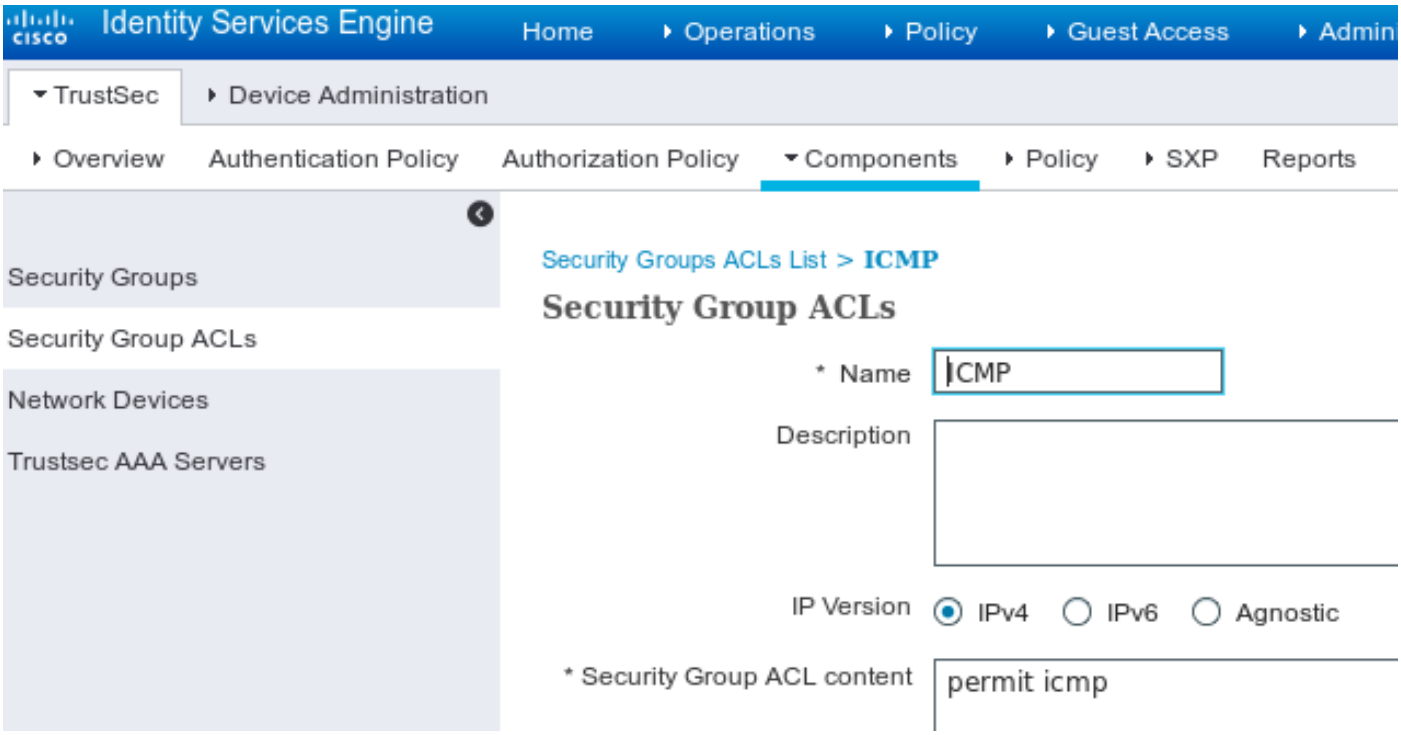
2단계. 보안 그룹

IT 및 마케팅용 SGT를 추가하려면 **Work Centers(작업 센터) > TrustSec > Components(구성 요소) > Security Groups(보안 그룹)**로 이동합니다.



3단계. 보안 그룹 ACL

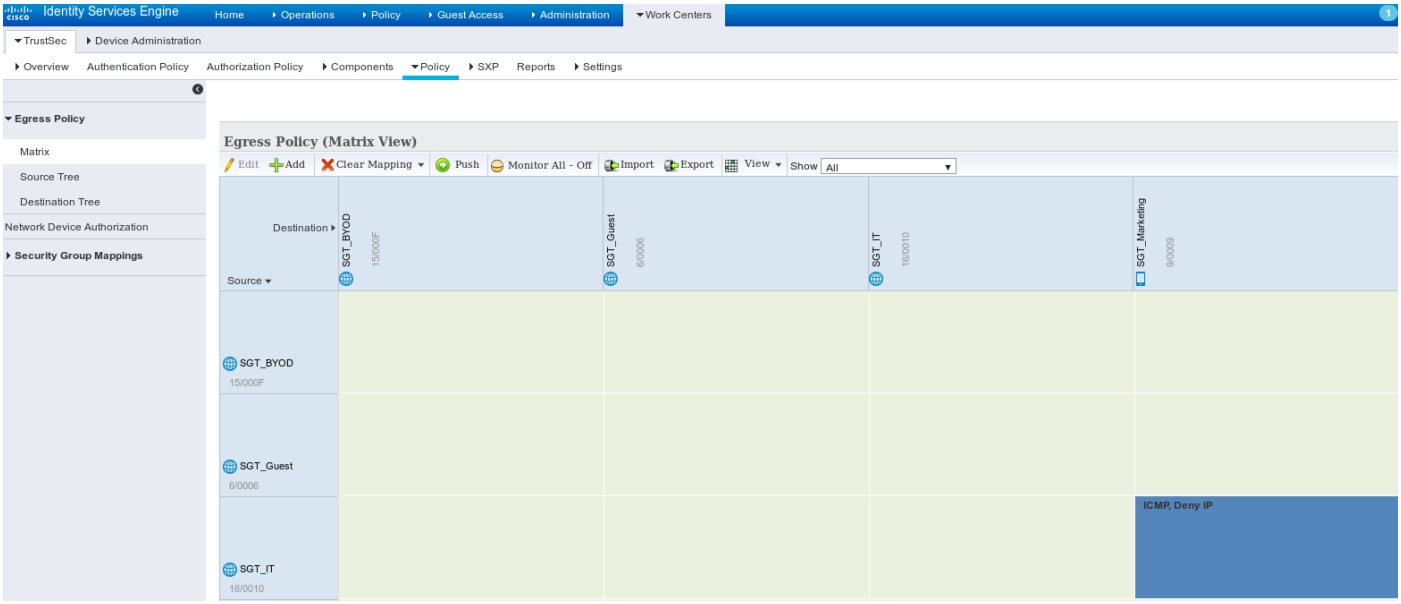
보안 그룹 ACL을 추가하려면 Work Centers(작업 센터) > **TrustSec > Components(구성 요소) > Security Group ACLs(보안 그룹 ACL)로 이동합니다.**



ICMP 트래픽만 허용합니다.

4단계. TrustSec 정책

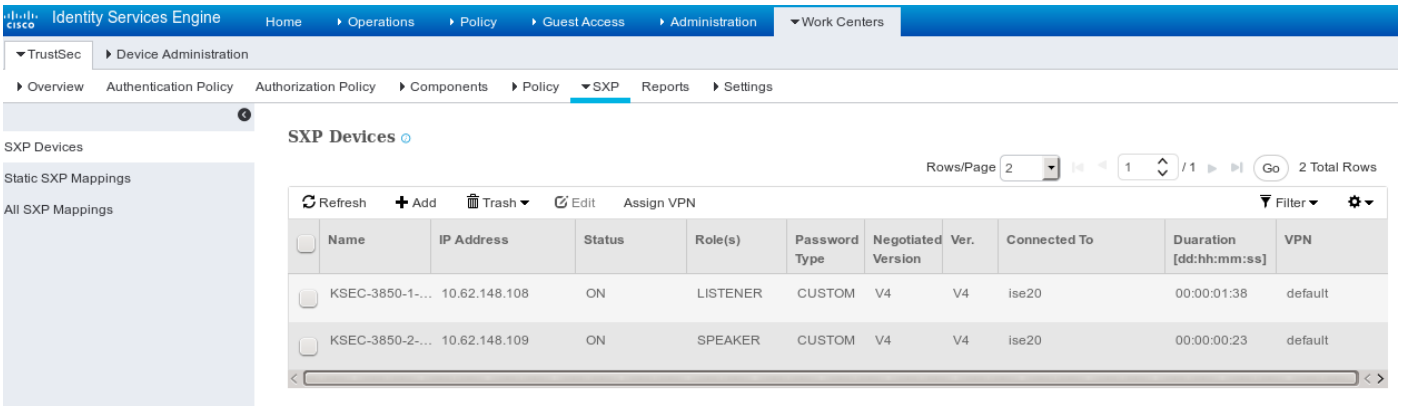
IT에서 마케팅으로 트래픽을 제어하는 정책을 추가하려면 **Work Centers(작업 센터) > TrustSec > Components(구성 요소) > Egress Policy(이그레스 정책) > Matrix(매트릭스)로 이동합니다.**



모든 트래픽을 거부하도록 기본 항목 catch all 규칙을 설정합니다.

5단계. SXP 디바이스

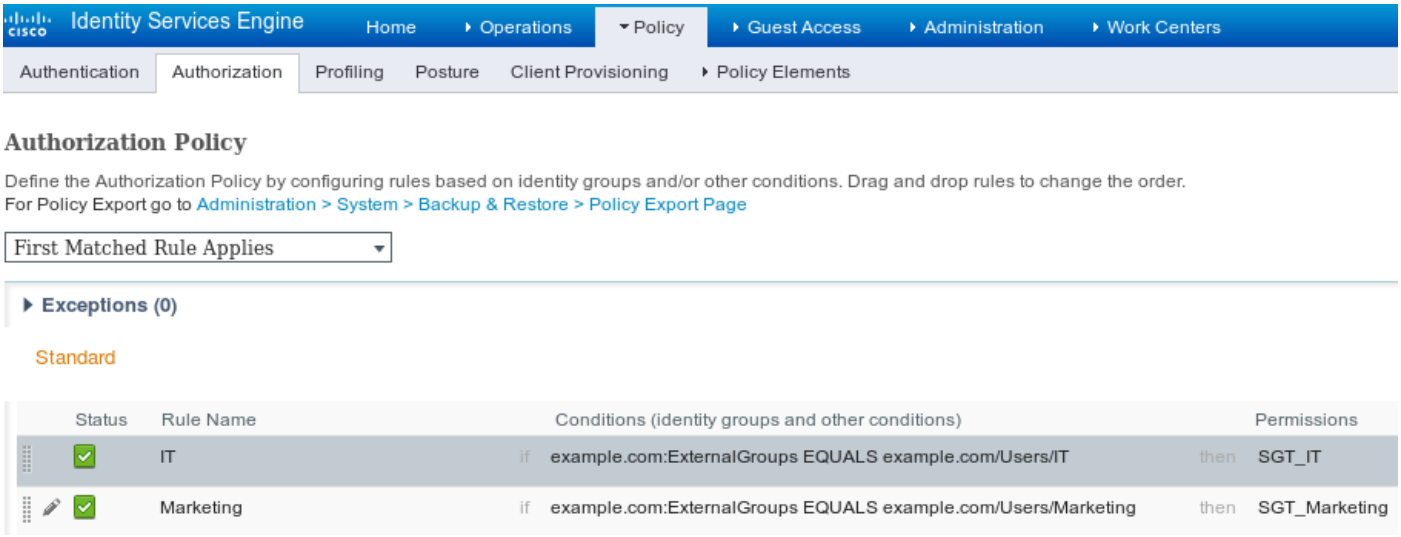
해당 스위치에 대한 SXP 리스너 및 스피커를 구성하려면 Work Centers(작업 센터) **> TrustSec > SXP Devices(SXP 디바이스)로 이동합니다.**



비밀번호 cisco(또는 스위치에서 sxp에 대해 구성된 다른 비밀번호)를 사용합니다.

6단계. 권한 부여 정책

권한 부여 정책이 각 사용자에 대해 올바른 SGT 태그를 반환하는지 확인하고 Policy(정책) **> Authorization(권한 부여)으로 이동합니다.**



다음을 확인합니다.

1단계. cts에 대해 ISE를 조인하는 전환

모든 스위치에서 TrustSec 자격 증명(ISE/Step1에서 구성)을 제공하여 PAC를 가져옵니다.

```
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.
```

PAC가 다운로드되었는지 확인합니다.

```
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:
000200B800030001000400101065D55BAF222BBC73362A7810A04A005B0006009C00030100B26D8DDC125B6595067D64F9
17DA624C0000001355CB2E1C00093A800E567155E0DE76419D2F3B97D890F34F109C4C42F586B29050CEC7B441E0CA60
FC6684D4F6E8263FA2623A6E450927815A140CD3B9D68988E95D8C1E65544E222E187C647B9F7F3F230F6DB4F80F3C20
1ACD623B309077E27688EDF7704740A1CD3F18CE8485788054C19909083ED303BB49A6975AC0395D41E1227B
 Refresh timer is set for 12w4d
```

환경 정책이 새로 고쳐집니다.

```
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
```

3850-1에 대해 동일한 프로세스 반복

2단계 802.1x 세션

IT 사용자가 인증되면 올바른 태그가 할당됩니다.

```
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
```

매핑은 로컬 SGT-IP 테이블에 설치됩니다.

```
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
```

3단계. SXP 스피커

3850-2는 ISE에 매핑을 전송하고, cts sxp에 대한 스위치 디버그를 전송합니다.

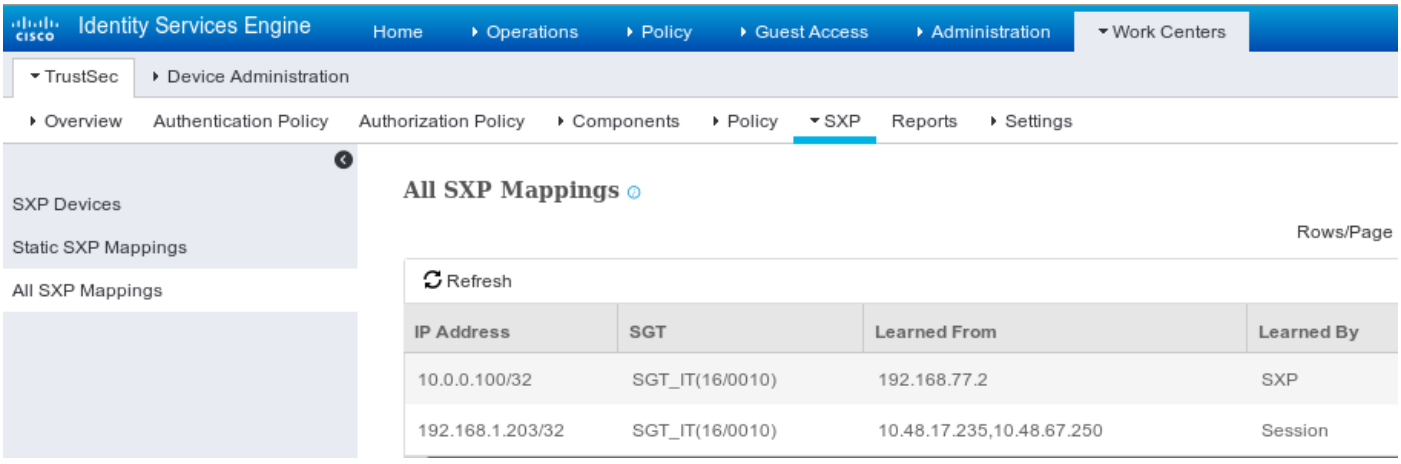
```
KSEC-3850-2(config)#do show debug
CTS:
 CTS SXP message debugging is on

*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 보고서(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
```

그리고 이 이미지에 표시된 대로 GUI를 통한 모든 매핑(3850-2에서 받은 10.0.0.100 매핑 포함)을 표시합니다.



192.168.77.2은 3850-2(가장 높은 ip 주소가 정의됨)에서 SXP 연결의 식별자입니다.

```
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
```

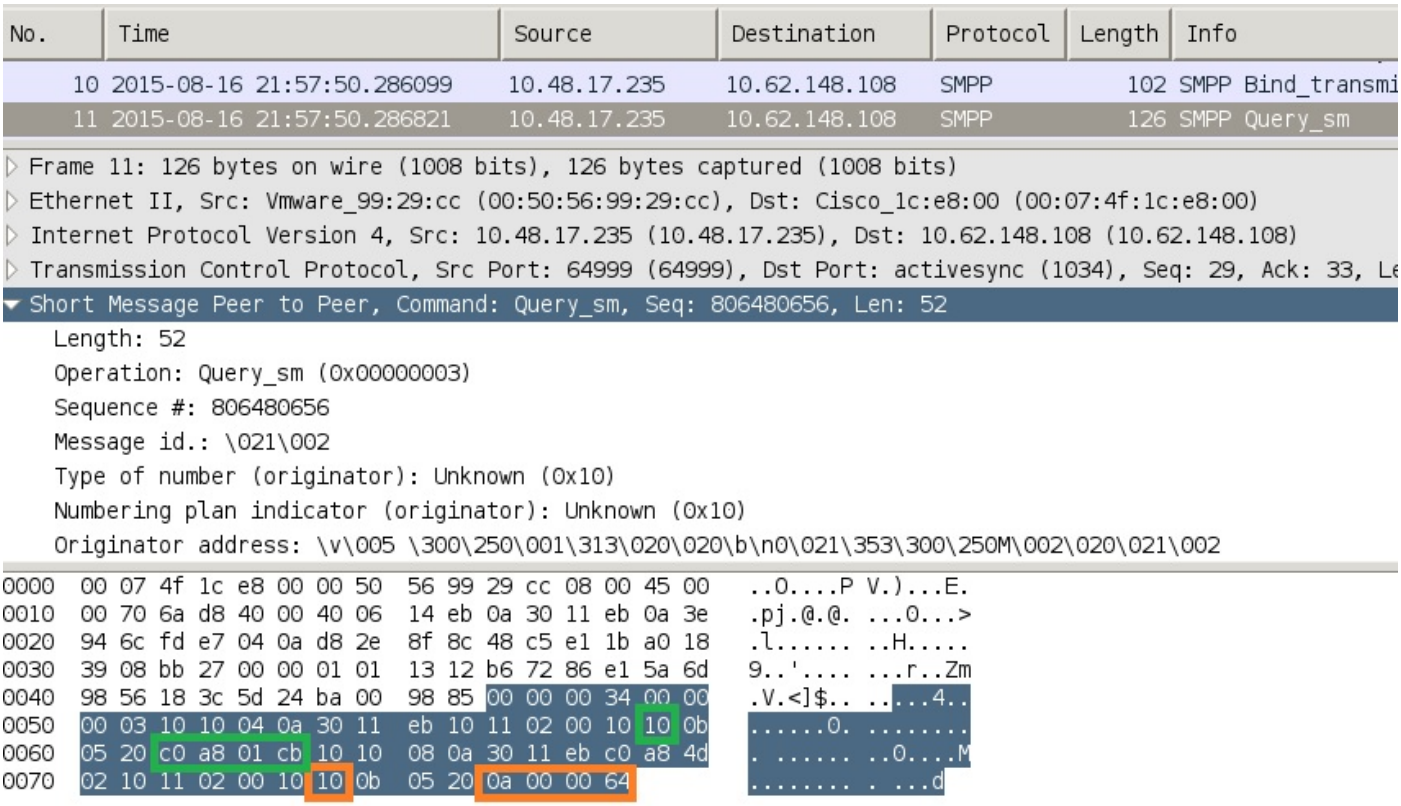
```
Vlan613                unassigned      YES NVRAM  administratively down down
Vlan666                192.168.66.2    YES NVRAM  down                  down
Vlan777                192.168.77.2    YES NVRAM  down                  down
```

4단계. SXP 리스너

그런 다음 ISE는 3850-1, 스위치 디버깅으로 매핑을 재전송합니다.

```
*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>
```

3850-1로 향하는 트래픽에 대해 ISE에서 가져온 패킷 캡처는 SXP 매핑이 전송되고 있음을 확인합니다.



Wireshark는 표준 SMPP 디코더를 사용합니다.페이로드를 확인하려면

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

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

3850-1은 ISE에서 받은 모든 매핑을 설치합니다.

```
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
```

5단계. 정책 다운로드 및 시행

ISE에서 올바른 정책을 다운로드합니다(SGT 16이 포함된 Matrix 행).

```
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
```

10.0.0.100(SGT IT)에서 10.0.0.1(SGT Marketing)까지의 ICMP 트래픽이 허용되고 카운터가 증가합니다.

```
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
```

텔넷 연결을 사용하려고 할 때 오류가 발생하면 드롭 카운터가 증가합니다.

```
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
```

3850-2에는 특정 정책이 없으며 모든 트래픽이 허용됩니다.

```
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
```

ISE에서 SG ACL을 수정하고, permit tcp를 추가하고, 3850-1에서 cts refresh 정책을 추가한 후, 텔넷 트래픽이 수락됩니다.

또한 Flexible Netflow(IOS-XE 3.7.2부터 SGT 인식) 로컬 캐시를 사용하여 동작을 확인할 수 있습니다.

```
flow record cts-v4
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
```

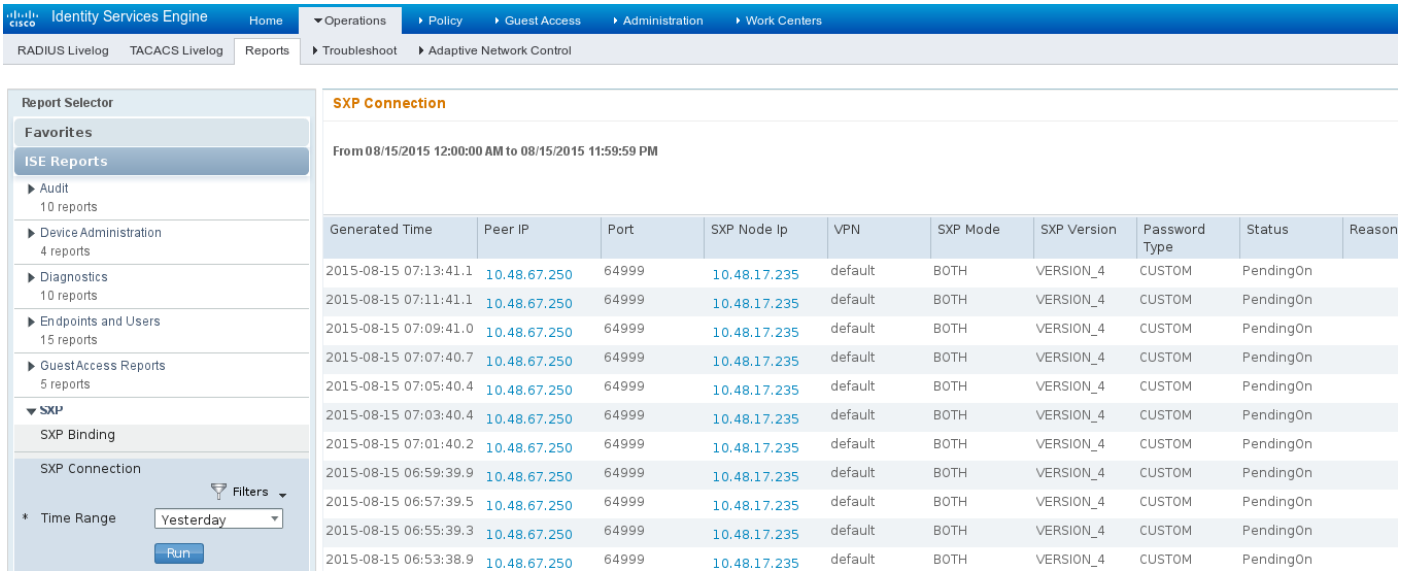
```
 match flow direction
 match flow cts source group-tag
 match flow cts destination group-tag
 collect counter packets long

flow monitor F_MON
 record cts-v4

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

결과는 3850-2에서 수신된 트래픽을 보여줍니다. 수신된 트래픽에 SGT(cts 링크 없음)가 없으므로 소스 SGT는 0이지만 로컬 매핑 테이블을 기반으로 대상 그룹 태그가 자동으로 교체됩니다.

```
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 로컬 캐시를 사용하여 수신된 트래픽을 확인할 수 있습니다.해당 트래픽이 허용 또는 삭제되면 전에 나타난 cts 카운터에서 확인합니다.

ISE는 이 이미지에 표시된 대로 SXP 바인딩 및 연결 보고서를 생성할 수도 있습니다.



참조

- ASA 버전 9.2.1 VPN Posture with ISE 컨피그레이션 예
- ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 문제 해결 가이드
- Cisco TrustSec 스위치 구성 가이드:Cisco TrustSec 이해
- Cisco TrustSec 구축 및 로드맵
- Cisco Catalyst 3850 TrustSec 컨피그레이션 가이드
- Cisco TrustSec 호환성 매트릭스
- 기술 지원 및 문서 – Cisco Systems