

配置ISE 2.0 TrustSec SXP監聽器和揚聲器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[流量](#)

[組態](#)

[交換機3850-1](#)

[交換機3850-2](#)

[ISE](#)

[驗證](#)

[參考資料](#)

[相關思科支援社群討論](#)

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)版本2.0在清單和揚聲器模式下支援TrustSec SGT交換協定(SXP)的功能並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst交換器組態
- 身分識別服務引擎(ISE)和TrustSec服務

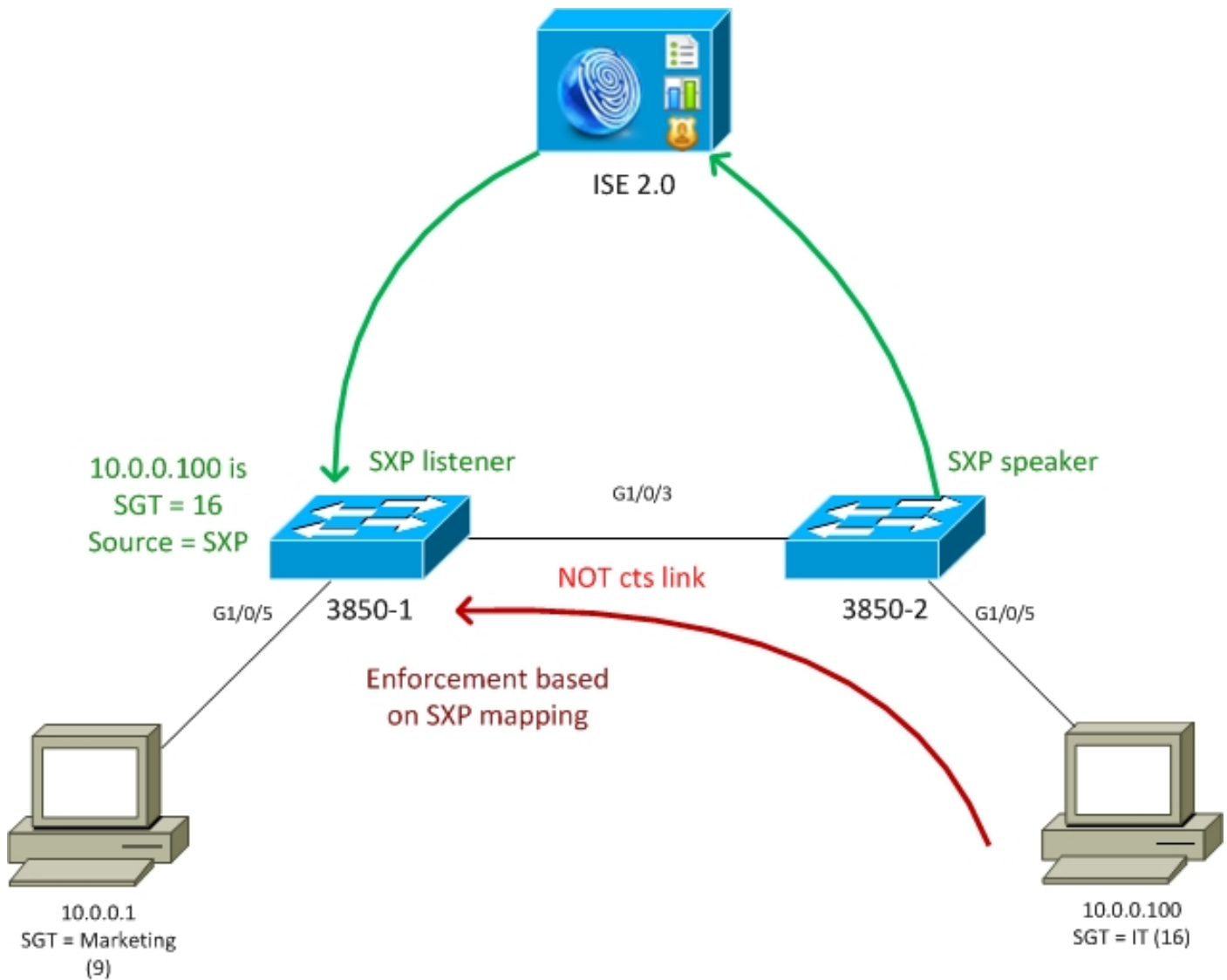
採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Catalyst 3850交換器 (含軟體IOS-XE 3.7.2及更新版本)
- Cisco ISE 2.0版及更高版本

設定

網路圖表



流量

- 3850-2是10.0.0.100的802.1x身份驗證器 — ISE返回安全組標籤(SGT)16(IT)以成功進行身份驗證
- 3850-2交換機學習請求方ip地址 (ip裝置跟蹤)，並使用SXP協定將對映資訊(IP-SGT)傳送到ISE
- 3850-1是10.0.0.1的802.1x身份驗證器 — ISE返回SGT標籤9 (行銷) 以成功進行身份驗證
- 3850-1從ISE接收SXP對映資訊 (10.0.0.100是SGT 16)，從ISE下載策略
- 從10.0.0.100傳送到10.0.0.1的流量由3850-2 (未下載具體策略) 轉發到3850-1，該策略的執行者將執行策略IT(16)->行銷(9)

請注意，交換機之間的鏈路不是cts link — 因此交換機上的所有遠端對映都是通過SXP協定安裝的。

附註：並非所有交換機都有允許根據收到的SXP對映通過ISE接收的策略進程式設計的硬體。有關驗證，請始終參閱最新的TrustSec相容性表或與Cisco Systems聯絡。

組態

有關基本TrustSec配置的詳細資訊，請參閱參考部分中的文章。

交換機3850-1

交換機通過SGT分配終止802.1x會話，並作為SXP揚聲器向ISE傳送。

```
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
```

交換機3850-2

交換機通過SGT分配終止802.1x會話，同時作為SXP偵聽器從ISE獲取對映。

```
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
```

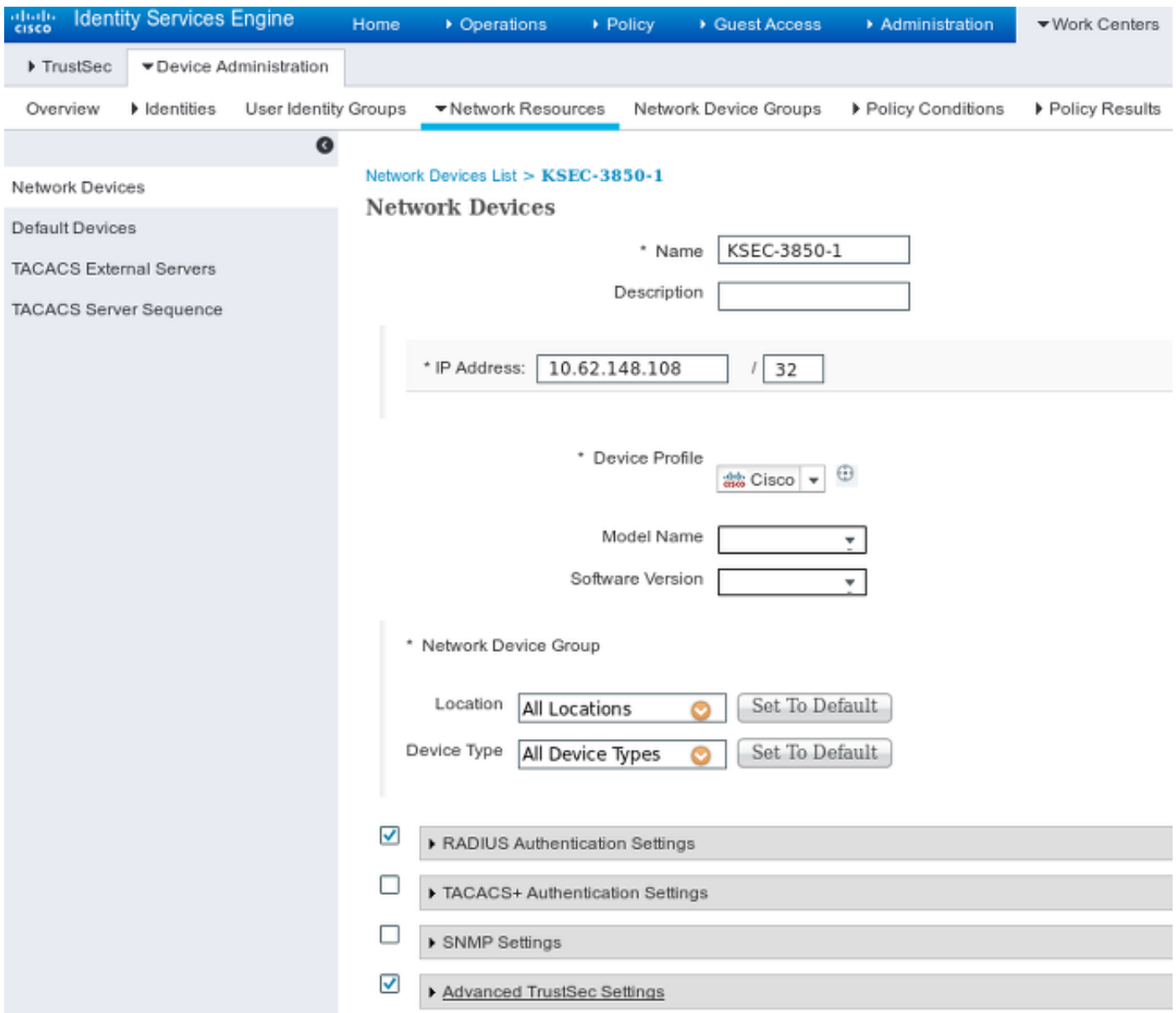
```
description mgarcarz
switchport access vlan 100
switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
```

```
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

步驟1. 網路存取裝置

導航至工作中心(Work Centers)>裝置管理(Device Administration)>網路資源(Network Resources)，新增兩台具有共用金鑰cisco和TrustSec密碼Krakow123的交換機。



The screenshot displays the Cisco Identity Services Engine (ISE) web interface for configuring a network device. The breadcrumb navigation shows: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Device Administration. The main navigation bar includes: Overview, Identities, User Identity Groups, Network Resources (selected), Network Device Groups, Policy Conditions, and Policy Results. The left sidebar lists: Network Devices (selected), Default Devices, TACACS External Servers, and TACACS Server Sequence. The main content area is titled 'Network Devices List > KSEC-3850-1' and 'Network Devices'. The configuration form includes the following fields and options:

- * Name:
- Description:
- * IP Address: /
- * Device Profile: (with a plus icon)
- Model Name:
- Software Version:
- * Network Device Group:
- Location: (with a dropdown arrow) and a 'Set To Default' button.
- Device Type: (with a dropdown arrow) and a 'Set To Default' button.

At the bottom, there are four expandable sections with checkboxes:

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

步驟2.安全組

若要新增面向IT和市場行銷的SGT，請導航至**工作中心> TrustSec >元件>安全組**。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > TrustSec > Device Administration > Components > Policy > SXP. The left sidebar contains: Security Groups (selected), Security Group ACLs, Network Devices, and Trustsec AAA Servers. The main content area is titled "Security Groups" and includes a sub-header "For Policy Export go to Administration > System > Backup &". Below this is a table with columns "Name" and "SGT (Dec / Hex)". The table contains five rows: SGT_BYOD (15/000F), SGT_Guest (6/0006), SGT_IT (16/0010), SGT_Marketing (9/0009), and Unknown (0/0000). Above the table are buttons for Edit, Add, Import, Export, and 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

步驟3. 安全組ACL

要新增安全組ACL，請導航到**工作中心> TrustSec >元件>安全組ACL**。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Security Group ACL. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Admin > TrustSec > Device Administration > Components > Policy > SXP > Reports. The left sidebar contains: Security Groups, Security Group ACLs (selected), Network Devices, and Trustsec AAA Servers. The main content area is titled "Security Groups ACLs List > ICMP" and "Security Group ACLs". It features a form with the following fields: "Name" (ICMP), "Description" (empty), "IP Version" (radio buttons for IPv4, IPv6, and Agnostic, with IPv4 selected), and "Security Group ACL content" (permit icmp).

* Name

Description

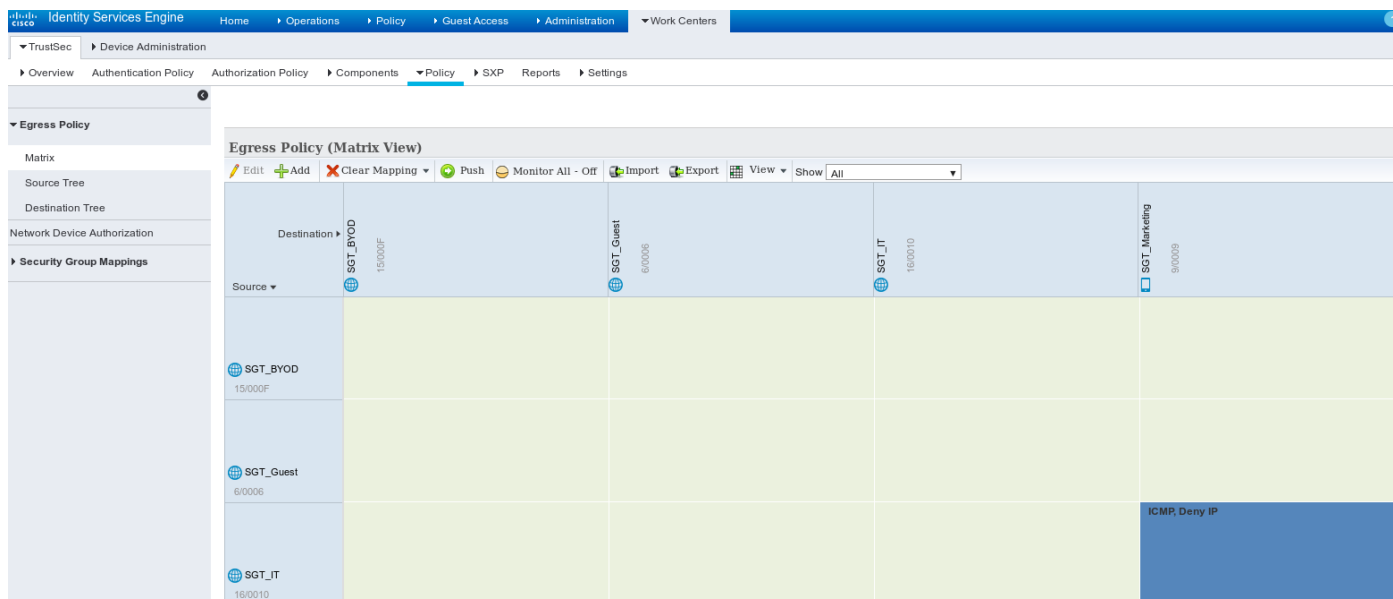
IP Version IPv4 IPv6 Agnostic

* Security Group ACL content

僅允許ICMP流量。

步驟4. TrustSec策略

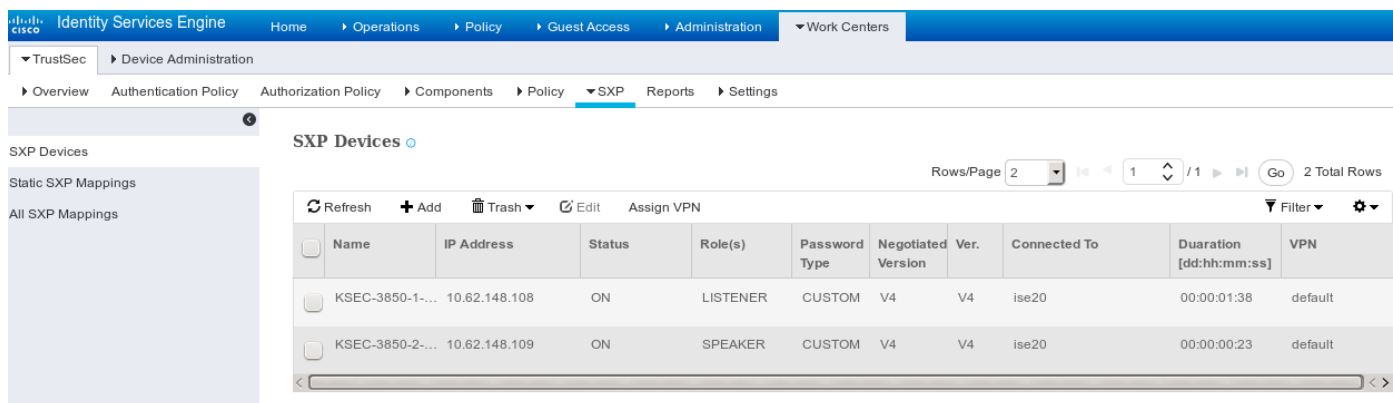
若要新增控制從IT到Marketing的流量的策略，請導航到Work Centers > TrustSec > Components > Egress Policy > Matrix。



設定預設條目 catch all 規則以拒絕所有流量。

步驟5. SXP裝置

要為相應的交換機配置SXP監聽器和揚聲器，請導航至工作中心> TrustSec > SXP裝置。



使用指令 cisco (或在交換機上為sxp配置的任何其它指令)。

步驟6. 授權策略

確保授權策略為每個使用者返回正確的SGT標籤，導航至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

驗證

步驟1.交換機加入CTS的ISE

從每台交換機提供TrustSec憑證 (在ISE/Step1中配置) 以獲取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.

確保已下載PAC。

```
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
```

並刷新環境策略。

```
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
對3850-1重複相同的過程

步驟2. 802.1x會話

IT使用者通過身份驗證後，將分配正確的標籤。

```
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
```

對映將安裝在本地SGT-IP表中。

```
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

步驟3. SXP揚聲器

3850-2將對映傳送到ISE，交換機調試用於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報告(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
並通過GUI顯示所有對映 ( 包括從3850-2接收的10.0.0.100的對映 ) , 如下圖所示。

```

All SXP Mappings

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是3850-2上SXP連線的識別符號 (定義的最高ip地址) 。

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

步驟4. SXP偵聽程式

然後ISE將該對映重新傳送到3850-1，交換機調試。

```
*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>
```

從ISE獲取的資料包捕獲流量指向3850-1確認正在傳送SXP對映。

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 0b  .....0. ....
0060 05 20 c0 a8 01 cb 10 10 08 0a 30 11 eb c0 a8 4d  . . . . .0...M
0070 02 10 11 02 00 10 10 0b 05 20 0a 00 00 64  . . . . .d
  
```

Wireshark使用標準SMPP解碼器。檢查負載：

「c0 a8 01 cb」(192.168.1.203)為10(SGT = 16)

10(SGT = 16)表示「0a 00 00 64」(10.0.0.100)

3850-1安裝從ISE接收的所有對映。

```

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
```

步驟5.政策下載和執行

從ISE下載正確的策略。(使用SGT 16的矩陣行)

```
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
```

允許從10.0.0.100(SGT IT)到10.0.0.1(SGT Marketing)的ICMP流量，計數器增加。

```
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
```

當嘗試使用telnet連線失敗時，丟棄計數器增加。

```
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
```

請注意，3850-2沒有特定策略，允許所有流量。

```
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
```

在ISE上修改SG ACL後，在3850-1上新增permit tcp和cts刷新策略 — 然後接受telnet流量。

也可以使用Flexible Netflow (從IOS-XE 3.7.2開始，它具有SGT感知)本地快取來確認行為。

```
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

```

結果顯示從3850-2接收的流量。源SGT為0，因為接收的流量沒有任何SGT（無cts連結），但根據本地對映表自動替換目標組標籤。

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 TAG FLOW CTS	IPV4 DST ADDR DST GROUP TAG	TRNS SRC PORT IP PROT	TRNS DST PORT pkts long	FLOW DIRN	FLOW CTS SRC GROUP
150.1.1.7.1 0	224.0.0.10 0	88	0 57	Output	
10.62.148.1 0	224.0.0.13 0	103	0 8192	Output	
7.7.4.1 0	224.0.0.10 0	88	0 56	Output	
10.0.0.1 0	10.0.0.100 0	1	0 1388	Output	
150.1.1.7.105 0	224.0.0.5 0	89	0 24	Output	
150.1.1.7.1 0	224.0.0.5 0	89	0 24	Output	
10.0.0.100 0	10.0.0.1 9	1	0 1388	Input	2048

Netflow本地快取可用於確認收到的流量。如果流量被接受或丟棄，則這一點由之前出現的cts計數器確認。

ISE還允許生成SXP繫結和連線報告，如下圖所示。

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	

參考資料

- [採用ISE的ASA 9.2.1版VPN安全評估配置示例](#)
- [ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南](#)
- [Cisco TrustSec交換機配置指南：瞭解Cisco TrustSec](#)
- [Cisco TrustSec部署和路線圖](#)
- [Cisco Catalyst 3850 TrustSec配置指南](#)
- [Cisco TrustSec相容性矩陣](#)
- [技術支援與文件 - Cisco Systems](#)