

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Схема сети](#)

[Трафик](#)

[Конфигурации](#)

[Коммутатор 3850-1](#)

[Коммутатор 3850-2](#)

[ISE](#)

[Проверка](#)

[Ссылки](#)

[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает, как настроить и устранить неполадки функции, что платформа Cisco Identity Services Engine (ISE) версия 2.0 поддерживает протокол обмена TrustSec SGT (SXP) в режиме Листера и Докладчика.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Конфигурация коммутатора Cisco Catalyst
- Платформа Identity Services Engine (ISE) и сервисы TrustSec

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Cisco Catalyst 3850 коммутаторов с программным обеспечением IOS-XE 3.7.2 и позже
- Cisco ISE, Выпуск 2.0 и позже

Настройка

Схема сети



Трафик

- 3850-2 средство проверки подлинности 802.1x для 10.0.0.100 - тег группы безопасности (SGT) возврата ISE 16 (IT) для успешной аутентификации
- 3850-2 коммутатора изучают IP-адрес соискателя (IP отслеживание устройства) и передают данные сопоставления (SGT IP) к ISE с помощью протокола SXP
- 3850-1 средство проверки подлинности 802.1x для 10.0.0.1 - ISE, возвращая SGT помечает 9 (Маркетинг) для успешной аутентификации
- 3850-1 получает данные сопоставления SXP от ISE (10.0.0.100, SGT 16), загружает политику от ISE
- Трафик, передаваемый от 10.0.0.100 до 10.0.0.1, передан 3850-2 (никакая определенная загруженная политика) к 3850-1, который является средством обеспечения выполнения, поражающим политику IT (16)-> Маркетинг (9)

Обратите внимание, что ссылка между коммутаторами не является ссылкой cts - таким образом, все удаленные сопоставления на коммутаторах установлены по протоколу SXP.

Примечание: Не все коммутаторы имеют аппаратные средства, позволяющие быть запрограммированными через политику, полученную от ISE на основе полученных сопоставлений SXP. Поскольку проверка всегда обращается к последней Матрице совместимости TrustSec или Cisco Systems контакта.

Конфигурации

Для получения дополнительной информации относительно основной конфигурации TrustSec, обратитесь к статьям в Ссылочном разделе.

Коммутатор 3850-1

Коммутатор завершает сеанс 802.1x с присвоением SGT и также как динамик SXP к 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
```

Коммутатор 3850-2

Коммутатор завершает сеанс 802.1x с присвоением SGT и также как слушатель SXP, собирающийся сопоставляющий от 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

Шаг 1. Устройства доступа к сети

Перейдите, чтобы **Работать Центры> Администрирование устройств> Сетевые ресурсы**, добавить оба коммутатора с Cisco общего секретного ключа и паролем Krakow123 TrustSec.



Шаг 2. Группы безопасности

Для добавления SGT для IT и Маркетинга, перейдите для **Работы Центров**> **TrustSec**> **Группы**> **Security Компонентов**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Guest Access'. The left sidebar contains 'TrustSec' and 'Device Administration'. The main content area is titled 'Security Groups' and includes a sub-header 'For Policy Export go to Administration > System > Backup &'. Below this are action buttons: 'Edit', 'Add', 'Import', 'Export', and 'Delete'. A table lists the following Security Groups:

	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

Шаг 3. ACL групп безопасности

Для добавления ACL Группы безопасности перейдите для **Работы Центров**> **TrustSec**> **ACL Группы**> **Security Компонентов**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Security Group ACLs. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Admin'. The left sidebar contains 'TrustSec' and 'Device Administration'. The main content area is titled 'Security Groups ACLs List > ICMP' and 'Security Group ACLs'. The configuration form includes the following fields:

- * Name:
- Description:
- IP Version: IPv4 IPv6 Agnostic
- * Security Group ACL content:

Позвольте только трафик ICMP.

Политика Шаг 4. TrustSec

Чтобы добавить, что политика, управляющая трафиком от IT до Маркетинга, перешла для Работы Центров> TrustSec> Компоненты> Выходная политика> Матрица.

The screenshot displays the Egress Policy Matrix in the Cisco ISE console. The matrix is organized with Source SGTs on the vertical axis and Destination SGTs on the horizontal axis. The Source SGTs listed are SGT_BYOD (15/000F), SGT_Guest (6/0006), and SGT_IT (16/0010). The Destination SGTs listed are SGT_BYOD (15/000F), SGT_Guest (6/0006), SGT_IT (16/0010), and SGT_Marketing (8/0008). The cells in the matrix represent the policy applied to traffic between these SGTs. A blue cell in the bottom-right corner indicates a policy of 'ICMP, Deny IP' for traffic from SGT_BYOD to SGT_Marketing.

Установите выгоду записи по умолчанию все правило запретить весь трафик.

Шаг 5. Устройства SXP

Для настройки слушателя SXP и докладчика для соответствующих коммутаторов, перейдите для Работы Центров> TrustSec> Устройства SXP.

The screenshot shows the SXP Devices configuration page in the Cisco ISE console. The page includes a table of SXP devices with the following columns: Name, IP Address, Status, Role(s), Password Type, Negotiated Version, Ver., Connected To, Duration, and VPN. Two devices are listed:

Name	IP Address	Status	Role(s)	Password Type	Negotiated Version	Ver.	Connected To	Duration [dd:hh:mm:ss]	VPN
KSEC-3850-1-...	10.62.148.108	ON	LISTENER	CUSTOM	V4	V4	ise20	00:00:01:38	default
KSEC-3850-2-...	10.62.148.109	ON	SPEAKER	CUSTOM	V4	V4	ise20	00:00:00:23	default

Используйте пароль cisco (или любой другой настроенный для sxp на коммутаторе).

Шаг 6. Политика авторизации

Гарантируйте, что политика авторизации возвращает корректные метки SGT для каждого пользователя, перейдите к Политике> Авторизация.

The screenshot shows the Authorization Policy configuration page in the Cisco ISE console. The page includes a table of authorization rules with the following columns: Status, Rule Name, Conditions, and Permissions. Two rules are listed:

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

Проверка

Шаг 1. ISE присоединения коммутатора для cts

От каждого коммутатора предоставляют учетные данные TrustSec (настроенный в ISE/Step1) для получения 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.

Гарантируйте, что загружен 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
```

И экологическая политика обновлена.

```
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
```

Повторите тот же процесс для 3850-1

Шаг 2. Сеансы 802.1x

После того, как пользователь IT аутентифицируется, корректная метка назначена.

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

Сопоставление установлено в локальной таблице IP SGT.

KSEC-3850-2#show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

Table with 3 columns: IP Address, SGT, Source. Row 1: 10.0.0.100, 16, LOCAL

Шаг 3. Динамик SXP

3850-2 передает сопоставление с ISE, отладки коммутатора для 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>

Отчёты о ISE (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
```

И представьте все сопоставления через GUI (включая сопоставление для 10.0.0.100 полученных от 3850-2), как показано в этом образе.

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation menu includes 'TrustSec' and 'Device Administration'. Under 'Device Administration', 'Overview', 'Authentication Policy', 'Authorization Policy', 'Components', 'Policy', 'SXP', 'Reports', and 'Settings' are visible. The 'SXP' tab is active, displaying 'All SXP Mappings'. A 'Refresh' button is present above a table with the following data:

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

192.168.77.2 идентификатор соединения SXP на 3850-2 (самый высокий определенный IP-адрес).

```
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
```

Шаг 4. Слушатель SXP

Затем ISE повторно передает то сопоставление с 3850-1, отладки коммутатора.

```
*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>

```

Захват пакета, взятый от ISE для трафика к 3850-1, подтверждает, что передаются сопоставления SXP.

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 использует стандартный декодер SMPP. Проверять информационное наполнение:

10 (SGT = 16) для "c0 a8 01 сбар" (192.168.1.203)

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

3850-1 установка все сопоставления получена от 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
```

Шаг 5. Загрузка политики и осуществление

Загрузите корректную политику от ISE. (Матричная строка с 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
```

Трафик ICMP от 10.0.0.100 (SGT IT) к 10.0.0.1 (Маркетинг SGT) разрешен, увеличение счетчиков.

```
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
```

При попытке использовать свои соединения TELNET, увеличение счетчиков сбросов.

```
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
```

Обратите внимание, что нет никакой определенной политики по 3850-2, весь трафик **позволен**.

```
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
```

После изменения ACL SG на ISE, добавляя tcp разрешения и политику обновления cts по 3850-1 - тогда принят трафик Telnet.

Его возможно также для использования Гибкого Netflow (запускающийся с XE IOS 3.7.2 это - знающий SGT), локальный кэш для подтверждения поведения.

```
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
```

Результаты показывают трафик, полученный от 3850-2. Источник, который SGT 0, потому что принимаемый трафик не имеет никакого SGT (никакая ссылка cts), но метка группы назначения, автоматически заменен на основе локальной таблицы соответствий.

```
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 TAG	SRC FLOW	ADDR CTS	IPV4 DST GROUP	ADDR TAG	TRNS IP	SRC PROT	PORT	TRNS pkts	DST long	PORT	FLOW DIRN	FLOW CTS	SRC GROUP
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					

Локальный кэш netflow может использоваться для подтверждения принимаемого трафика. Если тот трафик принят или отброшен, который подтвержден счетчиками cts, представленными прежде.

ISE также позволяет генерировать привязку SXP и отчёты о соединении, как показано в

этом образе.

The screenshot shows the Cisco Identity Services Engine (ISE) Reports interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, there are tabs for 'RADIUS LiveLog', 'TACACS LiveLog', and 'Reports'. The 'Reports' section is active, showing a 'Report Selector' on the left and a table of 'SXP Connection' logs on the right.

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 (selected)

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	

Ссылки

- [Положение VPN версии ASA 9.2.1 с примером конфигурации ISE](#)
- [ASA и Catalyst коммутатор серии 3750X пример конфигурации TrustSec и руководство устранения неполадок](#)
- [Руководство конфигурации коммутатора Cisco TrustSec: понимание Cisco TrustSec](#)
- [Развертывания Cisco TrustSec и RoadMap](#)
- [Cisco Catalyst 3850 руководств по конфигурации TrustSec](#)
- [Матрица совместимости Cisco TrustSec](#)
- [Cisco Systems – техническая поддержка и документация](#)