ISE SXP-Update-Protokolle und Catalyst Debug-Protokolle verstehen

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration und das Verständnis der SXP-Verbindung (Security Group Exchange Protocol) zwischen ISE und Catalyst 9300-Switch beschrieben.

Hintergrundinformationen

SXP ist das von TrustSec verwendete SGT (Security Group Tag)-Austauschprotokoll, mit dem IP-zu-SGT-Zuordnungen an TrustSec-Geräte weitergegeben werden.

SXP wurde entwickelt, damit Netzwerke wie Drittanbietergeräte oder ältere Cisco Geräte, die kein

SGT-Inline-Tagging unterstützen, über TrustSec-Funktionen verfügen.

SXP ist ein Peering-Protokoll, bei dem ein Gerät als Lautsprecher und das andere als Listener fungieren kann.

Der SXP-Sprecher ist für das Senden der IP-SGT-Bindungen verantwortlich, und der Listener ist für das Sammeln dieser Bindungen verantwortlich.

Die SXP-Verbindung verwendet den TCP-Port 64999 als zugrunde liegendes Transportprotokoll und MD5 für die Integrität/Authentizität der Nachricht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit der Konfiguration des SXP-Protokolls und der Identity Services Engine (ISE) vertraut sind.

Verwendete Komponenten

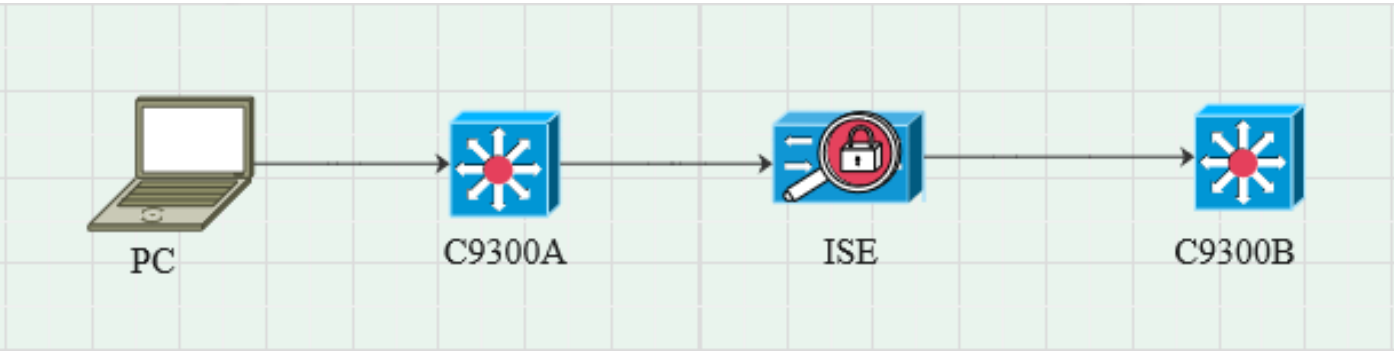
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switch der Serie 9300 mit der Software Cisco IOS® XE 17.6.5 und höher Cisco ISE, Version 3.1 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

Netzwerkdiagramm



Datenverkehrsfluss

Der PC wird mit C9300A authentifiziert, und die ISE weist SGT dynamisch über Richtliniensätze zu.
Wenn die Authentifizierung erfolgreich war, werden Bindungen mit einer IP erstellt, die dem RADIUS-Attribut der Framed-IP-Adresse und dem in der Richtlinie konfigurierten SGT entspricht.
Die Bindungen werden in "Alle SXP-Bindungen" unter der Standarddomäne propagiert.
Der C9300B empfängt die SXP-Zuordnungsinformationen von der ISE über das SXP-Protokoll.

Switch konfigurieren

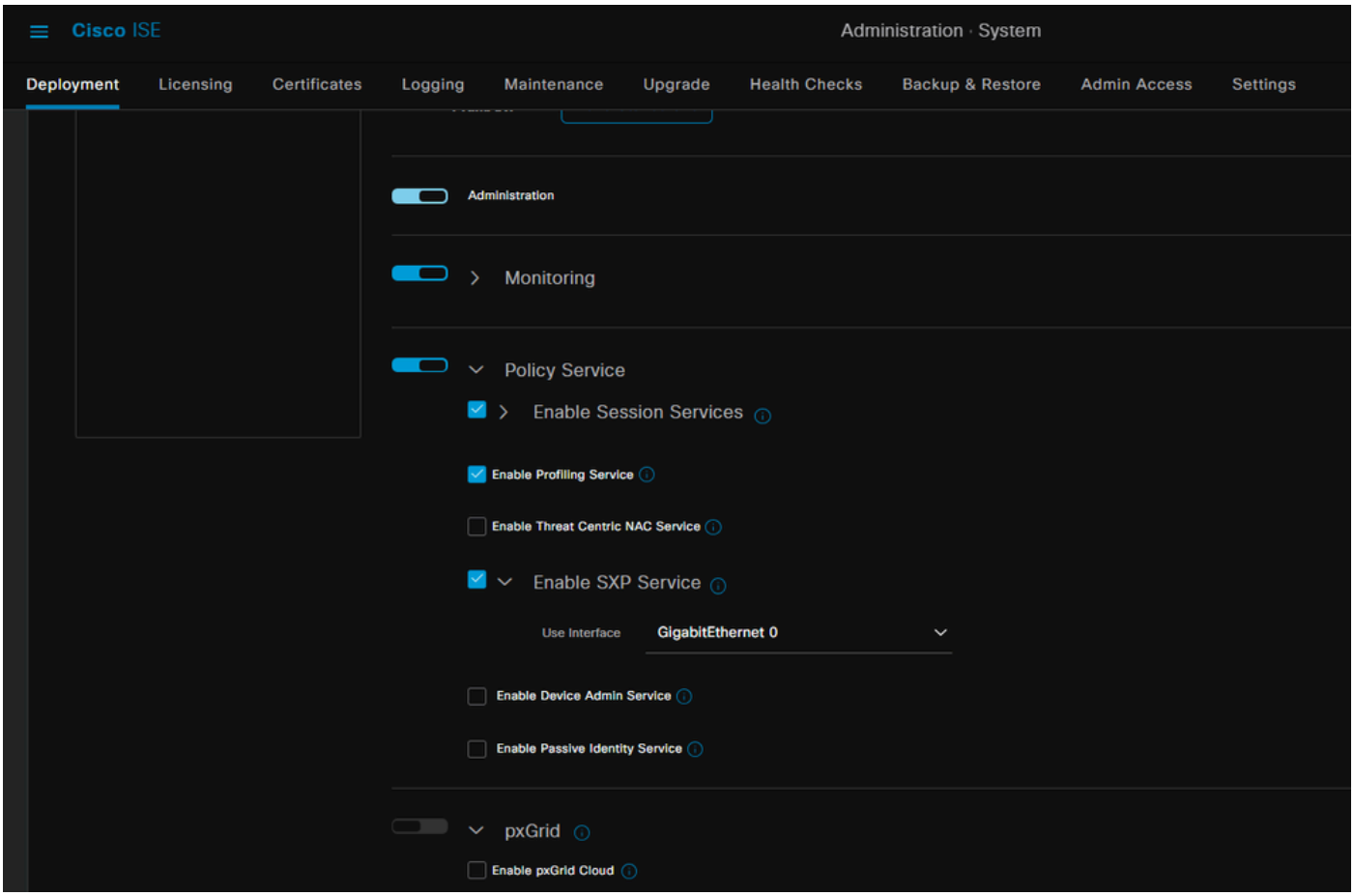
Konfigurieren Sie den Switch als SXP-Listener, um die IP-SGT-Zuordnungen von der ISE abzurufen.

```
cts sxp enable
cts sxp default kennwort cisco
cts sxp default source-ip 10.127.213.27
cts sxp connection peer 10.127.197.53 Kennwort Standardmodus Peer-Lautsprecher Haltezeit 0
0 vrf Mgmt-vrf
```

Konfigurieren der ISE

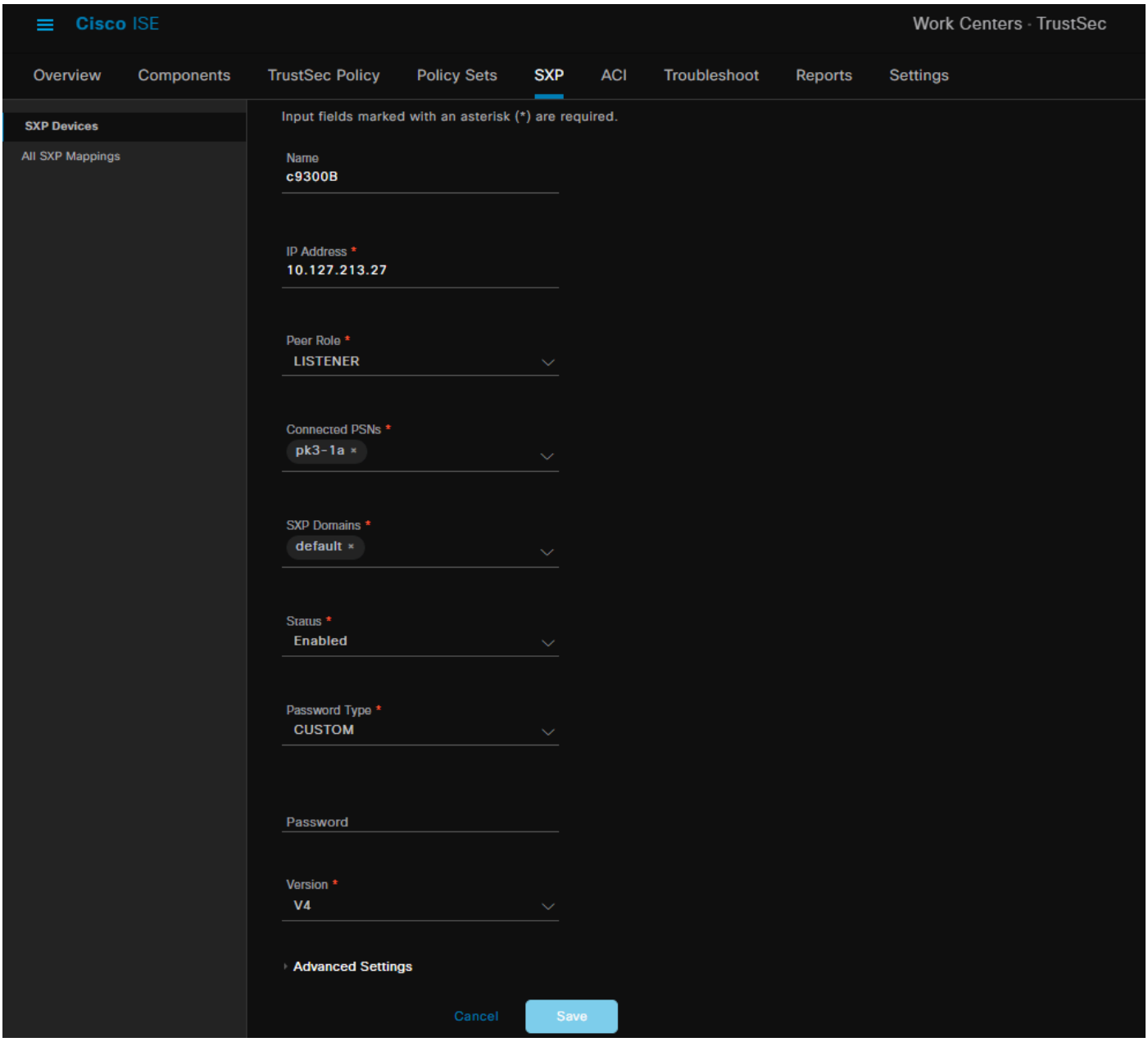
Schritt 1: SXP-Dienst auf der ISE aktivieren

Navigieren Sie zu Administration > System > Deployment > Edit the node, und wählen Sie unter Policy Service die Option Enable SXP Service aus.



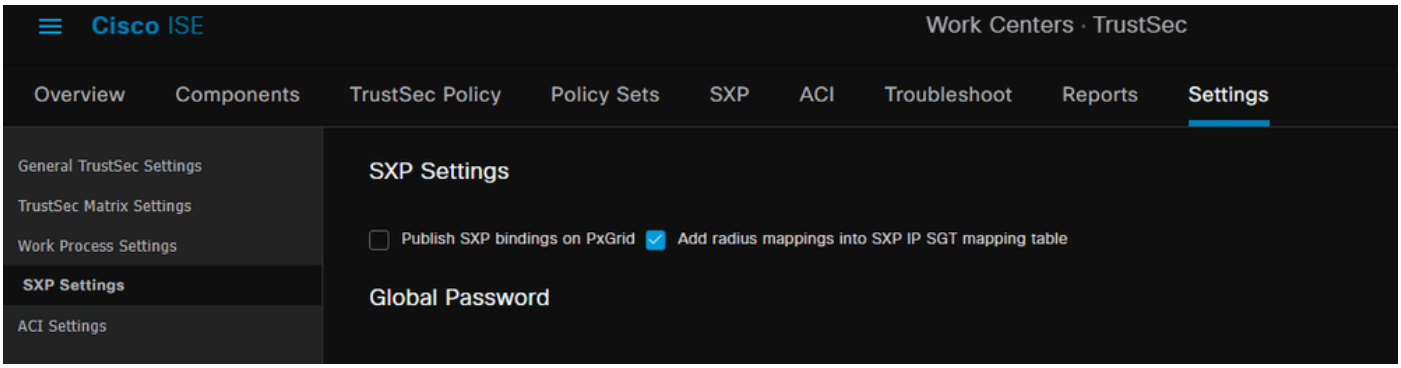
Schritt 2: Hinzufügen von SXP-Geräten

Um den SXP-Listener und -Lautsprecher für die entsprechenden Switches zu konfigurieren, navigieren Sie zu Workcenters > TrustSec > SXP > SXP Devices.
Fügen Sie den Switch mit der Peer-Rolle als Listener hinzu, und weisen Sie ihn der Standarddomäne zu.



Schritt 3: SXP-Einstellungen

Stellen Sie sicher, dass die Option "Add radius mappings into SXP IP SGT mapping table" aktiviert ist, damit die ISE dynamische IP-SGT-Zuordnungen über Radius-Authentifizierungen erlernt.



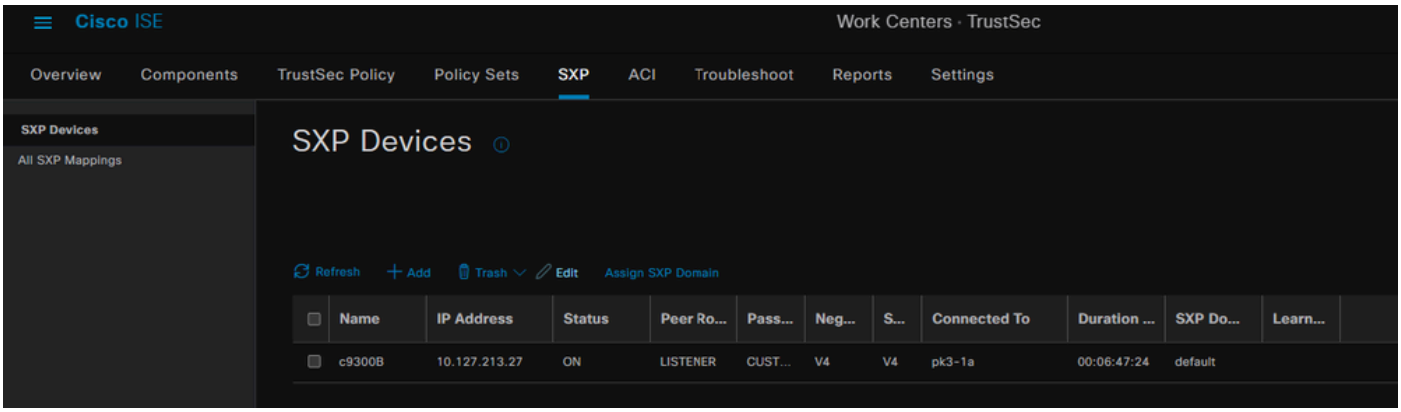
Überprüfung

Schritt 1: SXP-Verbindung auf Switch

```
C9300B#show cts sxp verbindungen vrf mgmt-vrf
SXP: Aktiviert
Unterstützte Version: 4
Standardkennwort: Festlegen
Standard-Schlüsselbund: Nicht festgelegt
Standard-Schlüsselbundname: Nicht zutreffend
Standard-Quell-IP: 10.127.213.27
Verbindungsversuch: 120 s
Abstimmungszeitraum: 120 s
Der Zeitgeber zum erneuten Öffnen wird nicht ausgeführt
Grenzwert für Peer-Sequenz-Traverse für Export: Nicht festgelegt
Grenzwert für Peer-Sequenz-Durchlauf für Import: Nicht festgelegt
----------------------------------------------
Peer-IP: 10.127.197.53
Quell-IP: 10.127.213.27
Verbindungsstatus: Ein
Konvertierung: 4
Verbindungsfähigkeit: IPv4-IPv6-Subnetz
Wartezeit: 120 Sekunden
Lokaler Modus: SXP Listener
Verbindungsinstanz: 1
TCP-Verbindung fd: 1
TCP-Verbindungskennwort: Standard-SXP-Kennwort
Haltezeit läuft
Dauer seit letzter Zustandsänderung: 0:00:23:36 (TT:Std:MM:Sek.)


Gesamtzahl der SXP-Verbindungen = 1

0x7F128DF555E0 VRF:Mgmt-vrf, fd: 1, Peer-IP: 10.127.197.53
cdbp:0x7F128DF555E0 Mgmt-vrf <10.127.197.53, 10.127.213.27> tableid:0x1
```

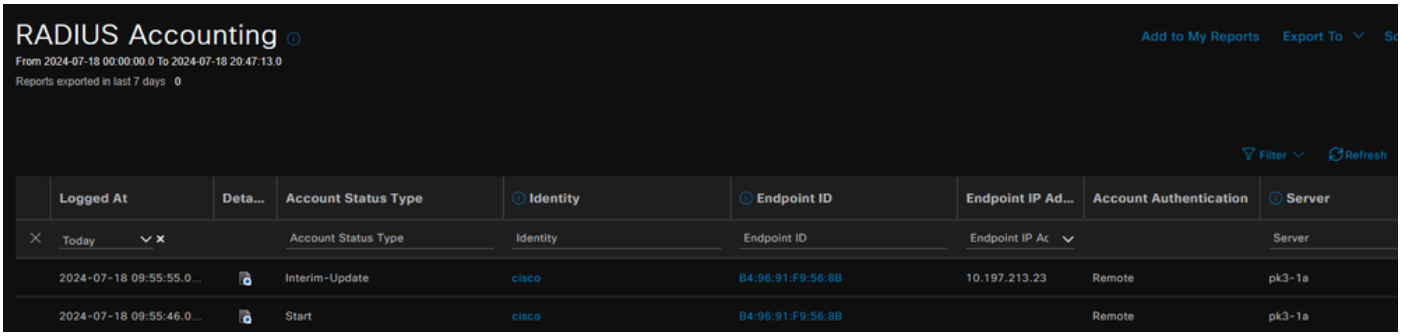
Schritt 2: ISE SXP-Verifizierung

Vergewissern Sie sich, dass der SXP-Status für den Switch unter Workcenters > TrustSec > SXP > SXP Devices (Workcenter > TrustSec > SXP > SXP-Geräte) ON lautet.



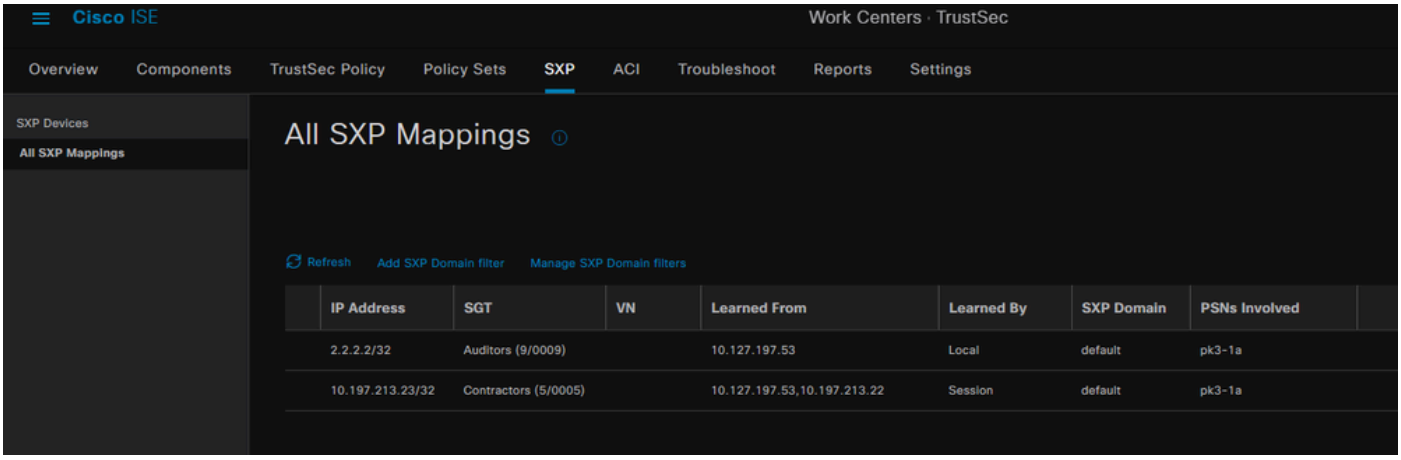
Schritt 3: RADIUS-Abrechnung

Vergewissern Sie sich, dass die ISE nach der erfolgreichen Authentifizierung das RADIUS-Attribut für die Framed-IP-Adresse vom Radius-Accounting-Paket erhalten hat.

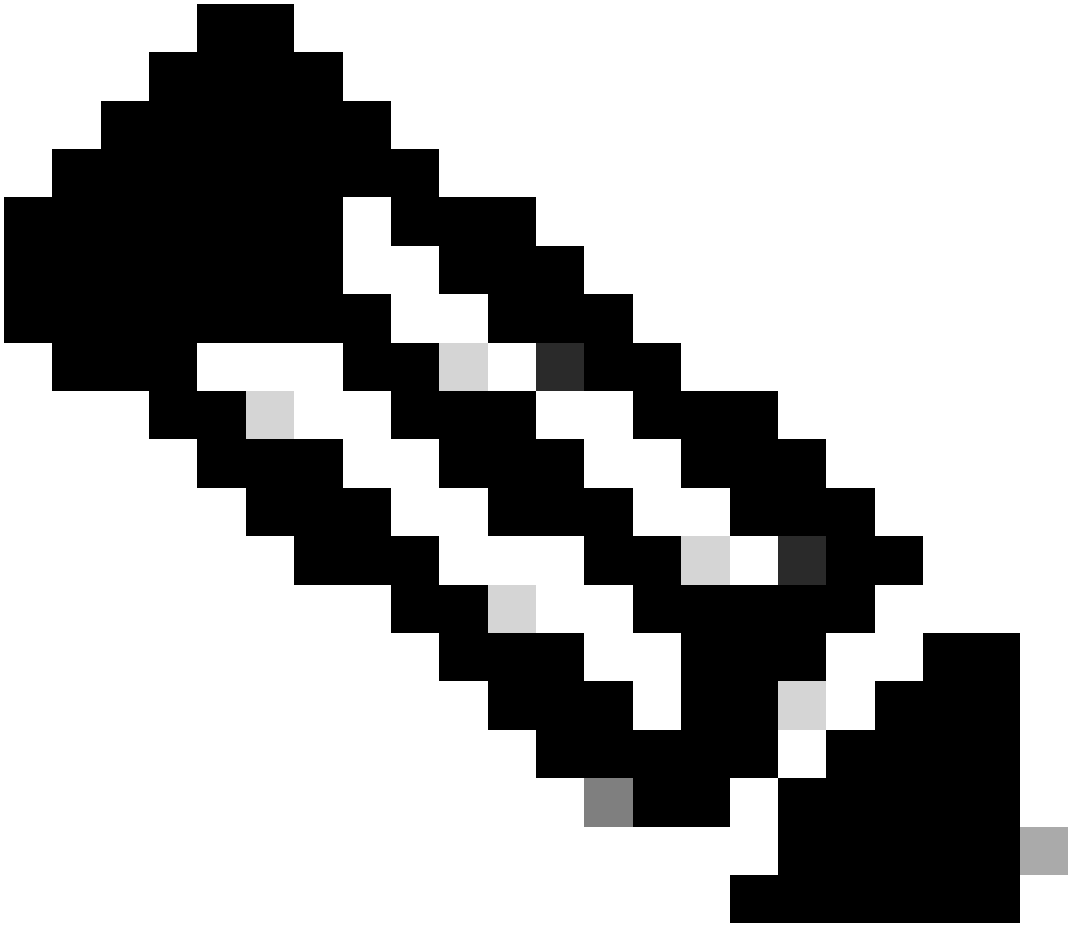


Schritt 4: ISE SXP-Zuordnungen

Navigieren Sie zu Workcenters > TrustSec > SXP > All SXP Mappings, um die dynamisch abgefragten IP-SGT-Zuordnungen aus der Radius-Sitzung anzuzeigen.



Gelernt von
Lokal - Statisch zugewiesene IP-SGT-Bindungen auf der ISE.
Sitzung - Dynamisch empfangene IP-SGT-Bindungen aus einer Radius-Sitzung.



Hinweis: Die ISE kann IP-SGT-Bindungen von einem anderen Gerät empfangen. Diese Bindungen können als Gelernt von SXP unter Alle SXP-Zuordnungen angezeigt werden.

Schritt 5: SXP-Zuordnungen auf Switch

Der Switch hat IP-SGT-Zuordnungen über das SXP-Protokoll von der ISE erhalten.

```
C9300B#show cts sxp sgt-map vrf mgmt-vrf brief
SXP-Knoten-ID(generiert):0x03030303(3.3.3.3)
IP-SGT-Zuordnungen:
IPv4, SGT: <2.2.2.2, 9>
IPv4, SGT: <10.197.213.23 , 5>
Gesamtzahl der IP-SGT-Zuordnungen: 2
conn in der sxp_bnd_exp_conn_list (gesamt:0):
C9300B#
```

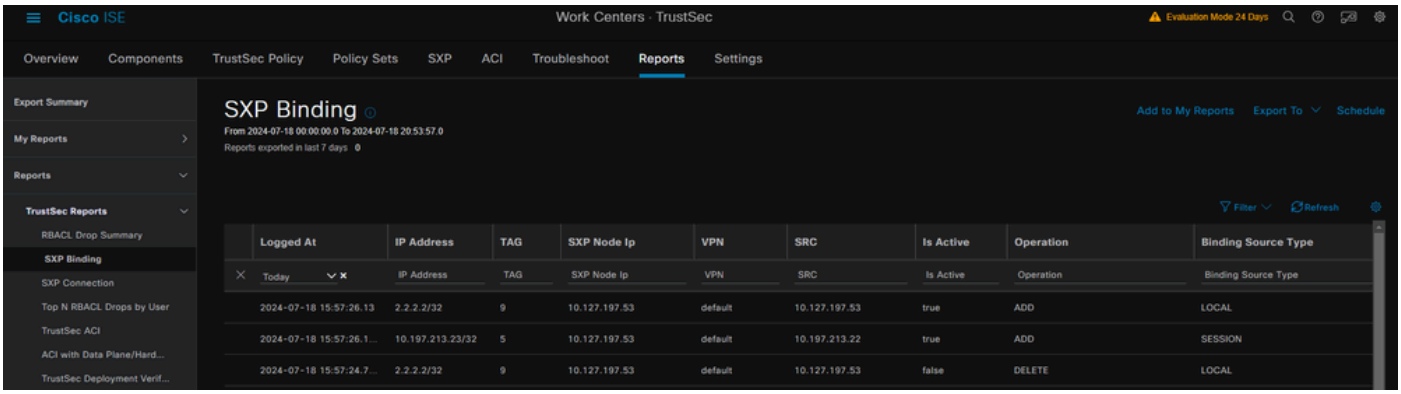
```
C9300B#show cts, rollenbasiertes SGT-Map-VRF, Mgmt-VRF, alle
Informationen zu aktiven IPv4-SGT-Bindungen

IP-Adresse SGT-Quelle
============================================
2.2.2.2 9 SXP
10.197.213.23 5 SXP

Zusammenfassung der aktiven IP-SGT-Bindungen
============================================
Gesamtanzahl der SXP-Bindungen = 2
Gesamtzahl aktiver Bindungen = 2
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

ISE-Bericht

Die ISE ermöglicht auch das Generieren von SXP-Bindungs- und Verbindungsberichten, wie in diesem Bild gezeigt.



Debuggen auf der ISE

Sammeln Sie das ISE-Supportpaket mit den folgenden Attributen, die auf Debugebene festgelegt werden sollen:

- SXP
- SGTbindung
- NSF
- NSF-Sitzung
- TrustSec

Wenn ein Benutzer vom ISE-Server authentifiziert wird, weist die ISE dem Accept Response-Paket einen SGT zu. Sobald der Benutzer die IP-Adresse erhält, sendet der Switch die Frame-IP-Adresse im Radius-Accounting-Paket.

show logging-Anwendung localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 HINWEIS Radius-Accounting: RADIUS Accounting watchdog update, ConfigVersionId=129, Geräte-IP-Adresse=10.197.213.22, UserName=cisco, NetworkDeviceName=pk, User-Name=cisco, NAS-IP-Adresse=10.197.213.22, NAS-Port=50124, Framed-IP-Adresse=10.197.2 13.23, Class=CACS:16D5C50A00000017C425E3C6:pk3-1a/510648097/25, Called-Station-ID=C4-B2-39-ED-AB-18, Calling-Station-ID=B4-96-91-F9 -56-8B, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=413, Acct-Output-Octets=0, Acct-Session-Id=00000007, Acct-Authentic=Remote, Acct-Input-Packets=4, Acct-Output-Packets=0, Event-Timestamp=1721277745, NAS-Port-Type=Ethernet, NAS-Port-Id=TenGigabitEthernet1/0/24, cisco-av-pair=audit-session-id=16D5C50A00000017C425E3C6, cisco-av-pair=method=dot1x, cisco-av-pair=cts:security-group-tag=0 0005-00, AcsSessionID=pk3-1a/510648097/28, SelectedAccessService=Default Network Access, RequestLatency=6, Step=11004, Step=11017, Step=15049, Step=15008, Step=22085, NetworkDeviceGroups=IPSEC#Is IPSEC Device#No, NetworkDeviceGroups=Location#All Locations , NetworkDeviceGroups=Gerätetyp#Alle Gerätetypen, CPMSessionID=16D5C50A1100500000017 C425E3C6, TotalAuthenticationLatency=6, ClientLatency=0, Network Device Profile=Cisco, Location=Location#Alle Standorte, Gerätetyp=Gerätetyp#Alle Gerätetypen, IPSEC=IPSEC#Is IPSEC Device#No und
```

show logging application ise-psc.log:

```
2024-07-18 09:55:55,054 DEBUG [SxpSessionNotifierThread][] ise.sxp.sessionbinding.util.SxpBindingUtil -:::-
Protokollieren der von PrrtCpmBridge empfangenen Sitzungswerte:
Vorgangstyp ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==> ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nas IP ==> 10.197.213.22null, vn ==> null
```

Der SXP-Knoten speichert die IP + SGT-Zuordnung in seiner H2DB-Tabelle und der spätere PAN-Knoten sammelt diese IP SGT-Zuordnung und spiegelt sie in Alle SXP-Zuordnungen in der ISE-GUI wider (Workcenter ->TrustSec -> SXP->Alle SXP-Zuordnungen).

show logging-Anwendung sxp_appserver/sxp.log:

```
2024-07-18 10:01:01,312 INFO [sxpservice-http-96441] cisco.ise.sxp.rest.SxpGlueRestAPI:147 - SXP-PEERF Hinzufügen von Sitzungsbindungen Batchgröße: 1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread] cpm.sxp.engine.services.NotificationSerializerImpl:202 - processing task [add=true, notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32, nasIp=10.197.213.22, sessionId=16D5C50A00000017C425E3C6, peerSequence=null,
```

```
sxpBindingOpType=null, sessionExpiryTime InMillis=0, apic=false, routable=true, vns=[])]

2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1543 - [VPN: 'default'] Neue Bindung hinzufügen:
MasterBindingIdentity [ip p=10.197.213.23/32, peerSequence=10.127.197.53,10.197.213.22,
tag=5, isLocal=true, sessionId=16D5C50A00000017C425E3C6, vn=STANDARD_VN]
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1581 - Adding 1 binding(s)
18.07.2024 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener:251 - Aufgabe wird an H2 Handler zum Hinzufügen von
Bindungen gesendet, Anzahl der Bindungen: 1
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
MasterDbListener Processing onAdded - BindingsCount: 1
```

Der SXP-Knoten aktualisiert den Peer-Switch mit den neuesten IP-SGT-Bindungen.

```
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:93 -
SXP_PERF:SEND_UPDATE_BUFFER_SIZE=32
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:116 - SENT_UPDATE to [ISE:10.127.197.53]
[10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:137 - SENT_UPDATE SUCCESSFUL to
[ISE:10.127.197 1.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

Debuggen auf Switch

Aktivieren Sie diese Fehlerbehebungen auf dem Switch, um SXP-Verbindungen und -Updates zu beheben.

debug cts sxp conn

debug cts sxp error

debug cts sxp mdb

debug cts sxp nachricht

Switch hat die SGT-IP-Zuordnungen vom SXP-Lautsprecher "ISE" erhalten.

Aktivieren Sie **Protokoll anzeigen**, um diese Protokolle anzuzeigen:

```
18.07.04:23:04.324: CTS-SXP-MSG:sxp_recv_update_v4 <1> Peer-IP: 10.127.197.53
18. Juli 04:23:04.324: CTS-SXP-MDB:IMU Bindung hinzufügen:- <conn_index = 1> von Peer
```

10.127.197.53
18.07.04:23:04.324: CTS-SXP-MDB:mdb_send_msg <IMU_ADD_IPSGT_DEVID>

18.07.04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Start
18. Juli 04:23:04.324: CTS-SXP-MDB:sxp_mdb_notify_rbm tableid:0x1 sense:1 sgt:5 peer:10.127.197.53
18.07.04:23:04.324: CTS-SXP-MDB:SXP MDB: Entry added ip 10.197.213.23 sgt 0x0005
18.07.04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Fertig

Zugehörige Informationen

ISE 3.1 Administratorhandbuch-Segmentierung

Catalyst Konfigurationsleitfaden TrustSec - Überblick

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.