Konfigurieren der TrustSec SGT SXP-Propagierung im SD-WAN

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

- Cisco TrustSec-Integration
- SGT-Propagierungsmethoden
- SGT-Propagierung mit SXP

SGT-SXP-Propagierung aktivieren und SGACL-Richtlinien herunterladen

- Schritt 1: Konfigurieren der Radius-Parameter
- Schritt 2: Konfigurieren der SXP-Parameter

Überprüfung

Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration der SXP-Propagierungsmethode (Security Group Tag Exchange Protocol) in SD-WAN (Software-Defined Wide-Area Networks) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Software-Defined Access (SD-Access) Fabric
- Cisco Identity Service Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Cisco IOS® XE Catalyst SD-WAN-Edges Version 17.9.5a
- Cisco Catalyst SD-WAN Manager Version 20.12.4

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.

Hintergrundinformationen

Cisco TrustSec-Integration

Die SGT-Propagierung mit Cisco TrustSec-Integration wird von Cisco IOS® XE Catalyst SD-WAN Version 17.3.1a und höher unterstützt. Mit dieser Funktion können Cisco IOS® XE Catalyst SD-WAN-Edge-Geräte von Cisco TrustSec-fähigen Switches in den Zweigstellen generierte Security Group Tag (SGT)-Inline-Tags an andere Edge-Geräte im Cisco Catalyst SD-WAN-Netzwerk weitergeben.

Grundlegendes zu Cisco TrustSec:

- SGT-Bindungen: Zuordnung zwischen IP und SGT, alle Bindungen haben die gängigste Konfiguration und lernen direkt von der Cisco ISE.
- SGT-Verbreitung: Die Propagierungsmethoden dienen zur Propagierung dieser SGTs zwischen Netzwerk-Hops.
- SGTACLs-Richtlinien: Ein Regelsatz, der die Berechtigungen einer Datenverkehrsquelle in einem vertrauenswürdigen Netzwerk festlegt.
- SGT-Durchsetzung: Wo die Richtlinien basierend auf der SGT-Richtlinie durchgesetzt werden.

SGT-Propagierungsmethoden

Die SGT-Propagierungsmethoden sind:

- SGT-Propagierung Inline-Tagging
- SGT SXP-Propagierung

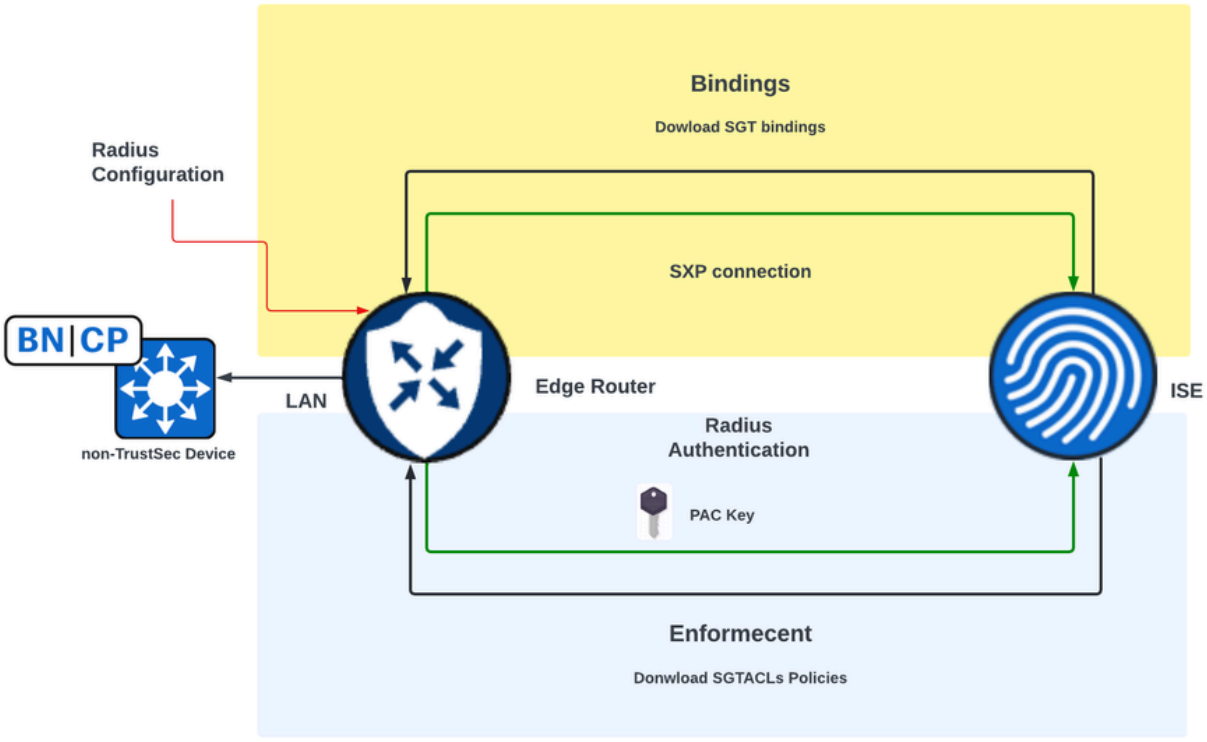
SGT-Propagierung mit SXP

Für die Inline-Tagging-Propagierung müssen die Außenstellen mit Cisco TrustSec-fähigen Switches ausgestattet sein, die SGT Inline-Tagging (Cisco TrustSec-Geräte) verarbeiten können. Wenn die Hardware kein Inline-Tagging unterstützt, verwendet die SGT-Propagierung das Security Group Tag Exchange Protocol (SXP), um SGTs über Netzwerkgeräte zu verbreiten.

Die Cisco ISE ermöglicht das Erstellen einer IP-to-SGT-Bindung (Dynamic IP-SGT) und das anschließende Herunterladen der IP-SGT-Bindung mithilfe von SXP auf ein Cisco IOS® XE Catalyst SD-WAN-Gerät zur Übertragung des SGT über das Cisco Catalyst SD-WAN-Netzwerk. Außerdem werden die Richtlinien für den SGT-Datenverkehr am SD-WAN-Ausgang durch Herunterladen der SGACL-Richtlinien von der ISE durchgesetzt.

Beispiel:

- Der Cisco Switch (Border Node) unterstützt kein Inline Tagging (kein TrustSec-Gerät).
- Die Cisco ISE ermöglicht das Herunterladen der IP-SGT-Bindung über eine SXP-Verbindung auf ein Cisco IOS® XE Catalyst SD-WAN-Gerät (Edge-Router).
- Mit der Cisco ISE können SGACL-Richtlinien über den Radius-Integrations- und PAC-Schlüssel auf eine Cisco IOS® XE Catalyst SD-WAN-Gerät (Edge-Router).

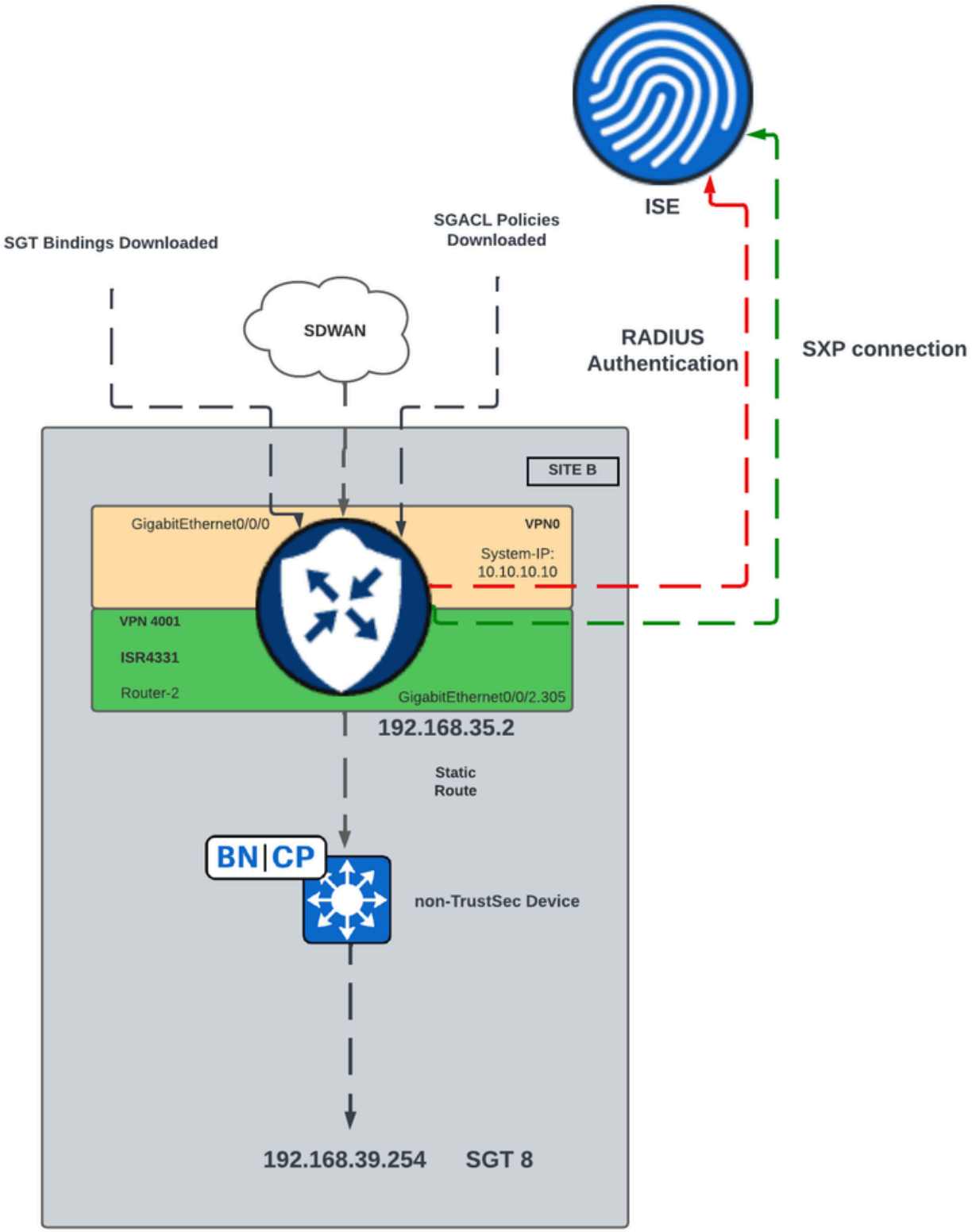


Anforderungen zum Aktivieren der SXP-Propagierung und Herunterladen von SGACL-Richtlinien auf SD-WAN-Edge-Geräten

Anmerkung: SGACL-Richtlinien werden nicht für den eingehenden Datenverkehr, sondern nur für den ausgehenden Datenverkehr in einem Cisco Catalyst SD-WAN-Netzwerk durchgesetzt.

Hinweis: Die Cisco TrustSec-Funktion wird für mehr als 24.000 SGT-Richtlinien im Controller-Modus nicht unterstützt.

SGT-SXP-Propagierung aktivieren und SGACL-Richtlinien herunterladen



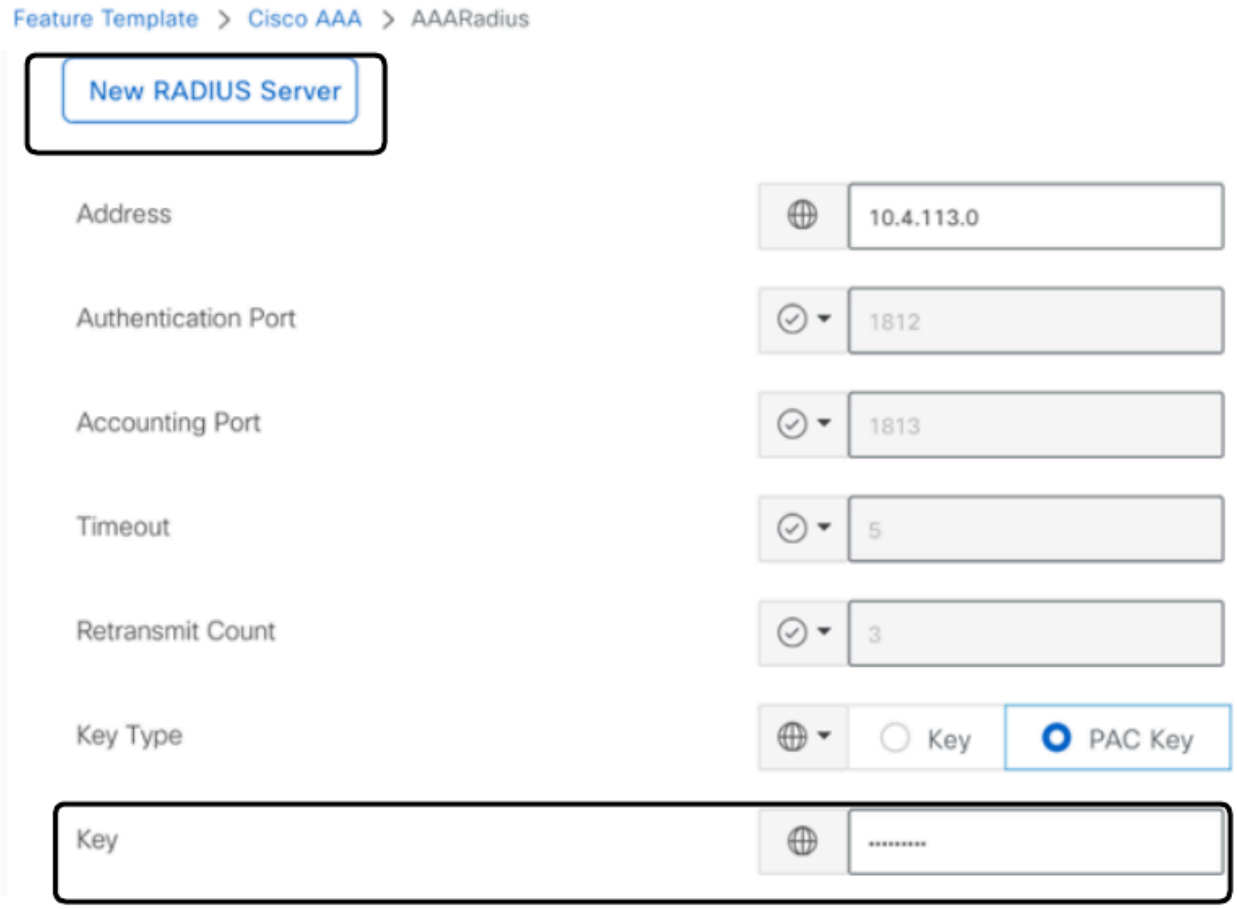
Netzwerkdiagramm für die SGT SXP-Propagierung im SD-WAN

Schritt 1: Konfigurieren der Radius-Parameter

- Melden Sie sich bei der Cisco Catalyst SD-WAN Manager-GUI an.
- Navigieren Sie zu Konfiguration > Vorlagen > Funktionsvorlage > Cisco AAA. Klicken Sie auf

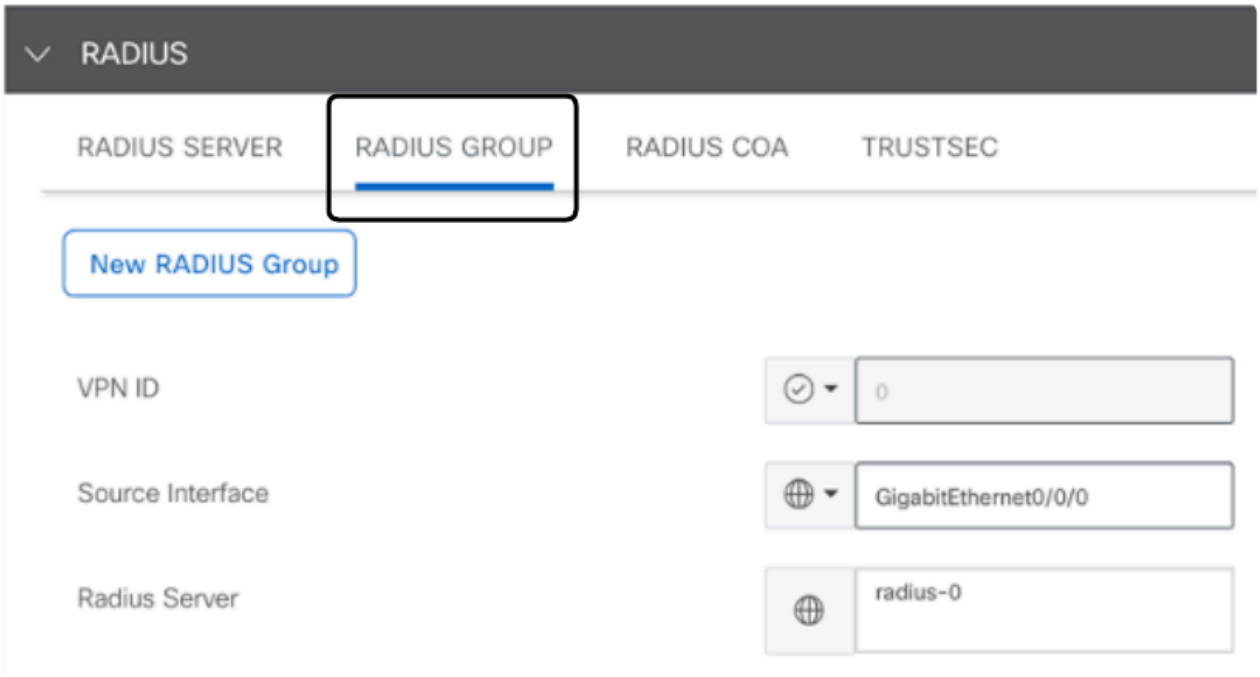
RADIUS SERVER.

- Konfigurieren Sie die RADIUS SERVER-Parameter und den Schlüssel.



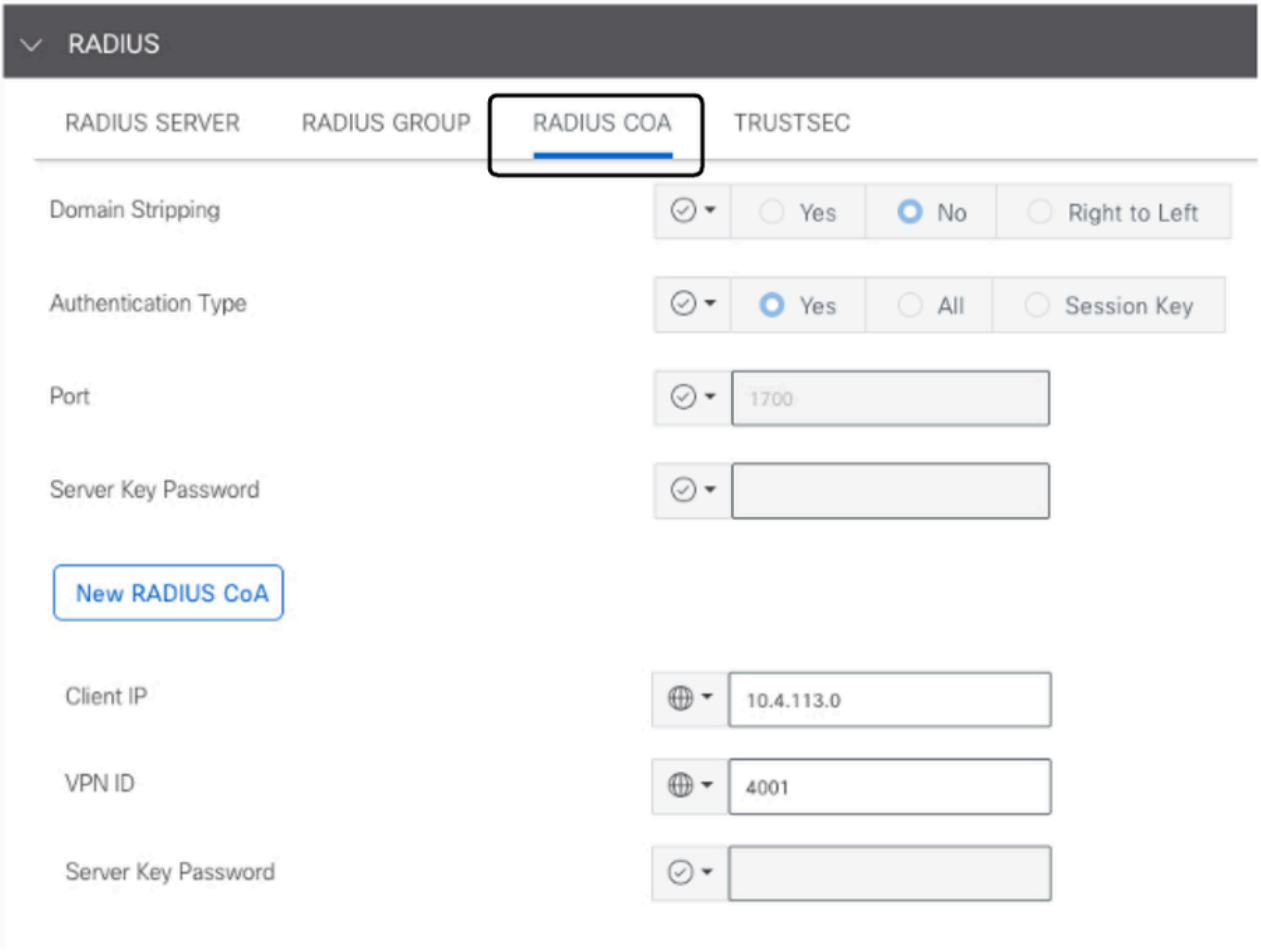
Konfiguration des RADIUS-Servers

- Geben Sie die Werte zum Konfigurieren der Parameter für die Radius-Gruppe ein.



Konfiguration der RADIUS-Gruppe

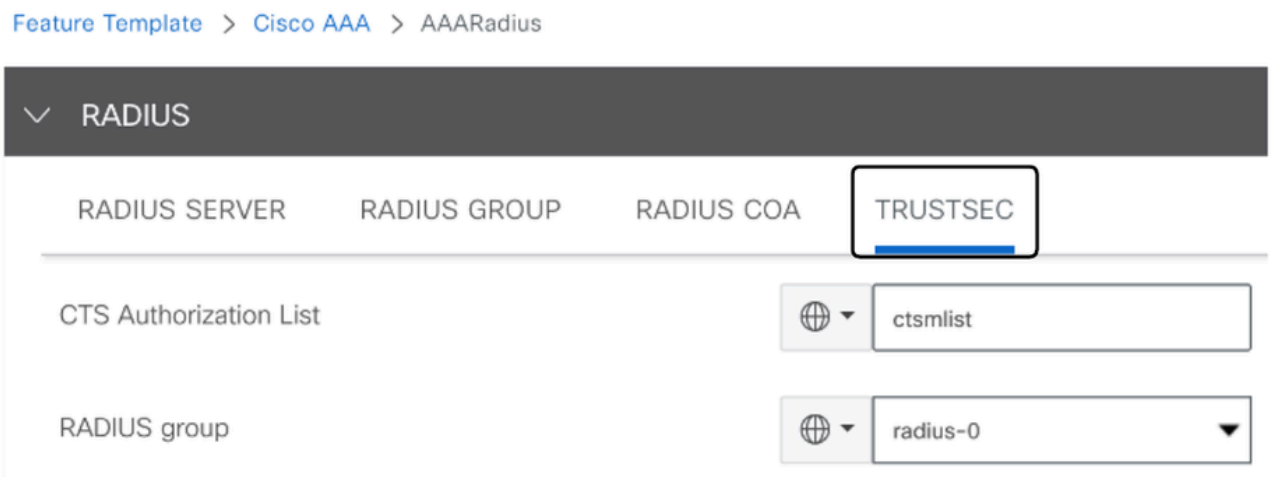
- Geben Sie die Werte zum Konfigurieren der Radius-COA-Parameter ein.



RADIUS-COA-Konfiguration

Anmerkung: Wenn Radius COA nicht konfiguriert ist, kann der SD-WAN-Router die SGACL-Richtlinien nicht automatisch herunterladen. Nach dem Erstellen oder Ändern einer SGACL-Richtlinie von der ISE wird der Befehl cts refresh policy zum Herunterladen der Richtlinien verwendet.

- Navigieren Sie zum Abschnitt TRUSTSEC, und geben Sie die Werte ein.

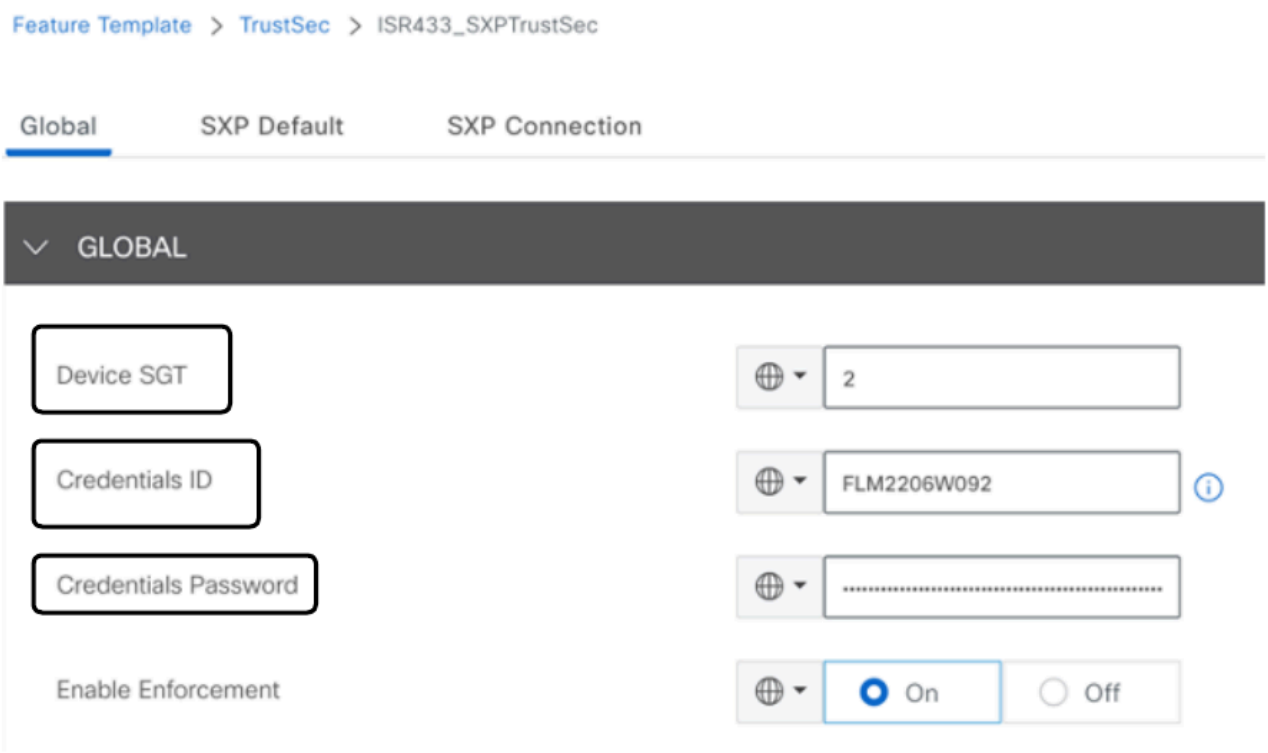


TRUSTSEC-Konfiguration

- Verknüpfen Sie die Cisco AAA-Funktionsvorlage mit der Gerätevorlage.

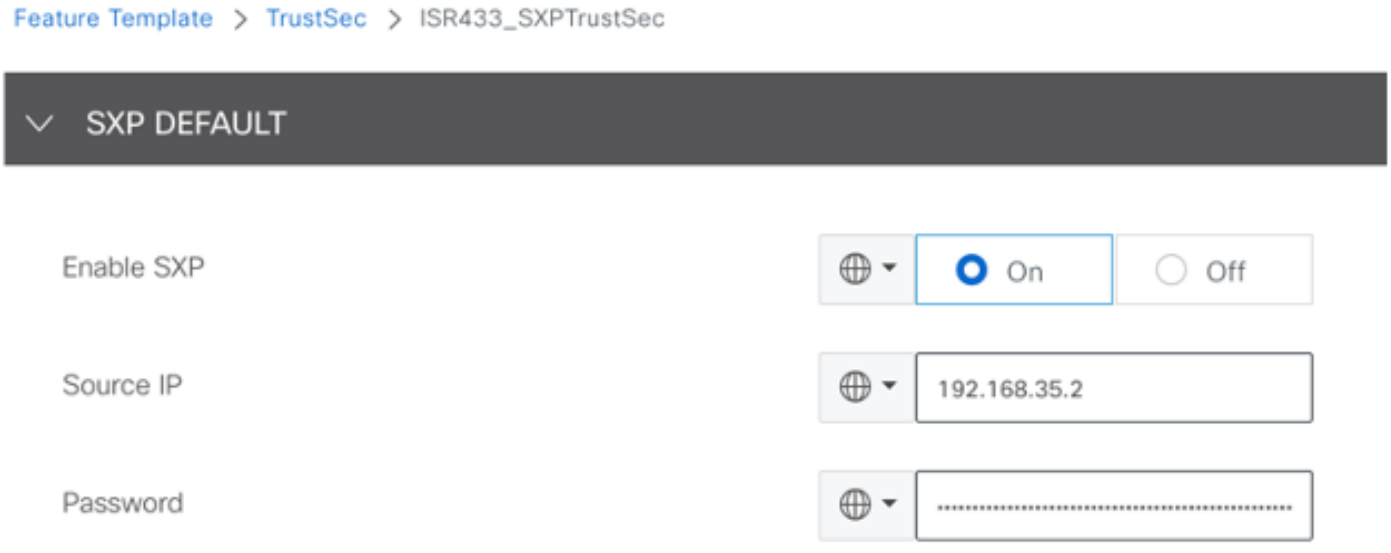
Schritt 2: Konfigurieren der SXP-Parameter

- Navigieren Sie zu Konfiguration > Vorlagen > Funktionsvorlage > TrustSec.
- Konfigurieren Sie die CTS-Anmeldeinformationen, und weisen Sie den Geräteschnittstellen eine SGT-Bindung zu.



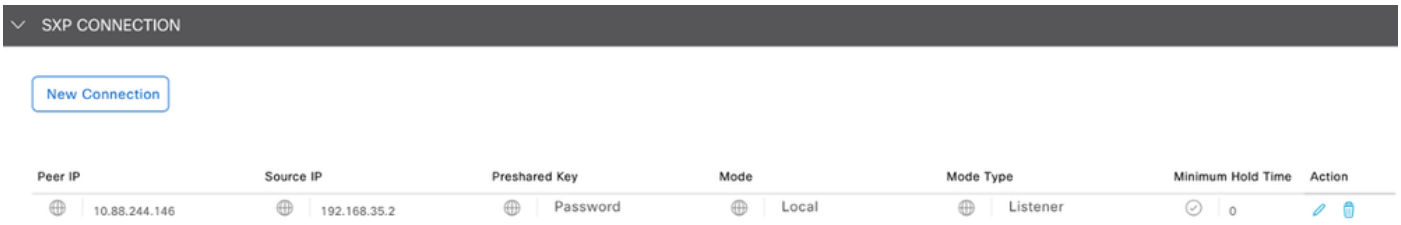
TrustSec-Funktionsvorlage

- Navigieren Sie zum Abschnitt SXP-Standard, und geben Sie die Werte ein, um die SXP-Standard-Parameter zu konfigurieren.



SXP-Standardkonfiguration

- Navigieren Sie zu SXP Connection, und konfigurieren Sie die SXP-Verbindungsparameter, und klicken Sie dann auf Save.

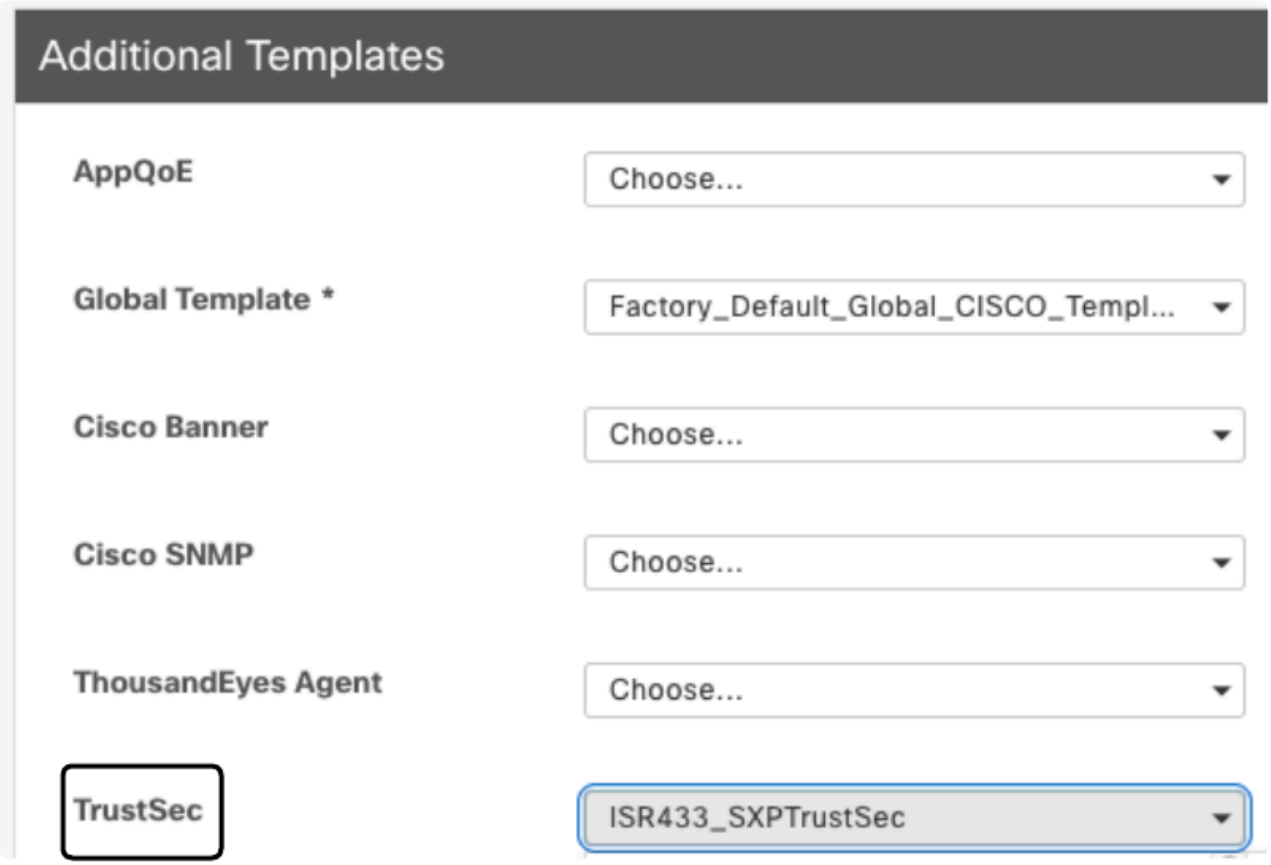


SXP-Verbindungskonfiguration

Anmerkung: Die Anzahl der SXP-Sitzungen, die von der Cisco ISE verarbeitet werden können, ist begrenzt. Als Alternative könnte daher ein SXP-Reflektor für skalierbare Netzwerk-Horizontale verwendet werden.

Anmerkung: Es wird empfohlen, einen SXP-Reflektor zu verwenden, um einen SXP-Peer mit Cisco IOS® XE Catalyst SD-WAN-Geräten einzurichten.

- Navigieren Sie zu Konfiguration > Vorlagen > Gerätevorlage > Zusätzliche Vorlagen > TrustSec.
- Wählen Sie die zuvor erstellte TrustSec-Funktionsvorlage aus, und klicken Sie auf Speichern.



Abschnitt "Zusätzliche Vorlagen"

Überprüfung

Führen Sie den Befehl aus,show cts sxp connections vrf (service vrf)um die Cisco TrustSec SXP-Verbindungsinformationen anzuzeigen.

<#root>

#show

cts

sxp

connections

vrf

4001

SXP : Enabled

Highest Version Supported: 5
Default Password : Set
Default Key-Chain: Not Set
Default Key-Chain Name: Not Applicable
Default Source IP: 192.168.35.2
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

Peer IP : 10.88.244.146

Source IP : 192.168.35.2

Conn status : On

Conn version : 4
Conn capability : IPv4-IPv6-Subnet
Conn hold time : 120 seconds
Local mode : SXP Listener
Connection inst# : 1
TCP conn fd : 1
TCP conn password: default SXP password
Hold timer is running

Total num of SXP Connections = 1

Führen Sie den Befehl **show cts role-based sgt-map** to zeigt die globale Cisco TrustSec SGT-Zuordnung zwischen IP-Adresse und SGT-Bindungen an.

```
<#root>

#

show

cts

 role-based

sgt

-map

vrf

 4001 all


Active IPv4-SGT Bindings Information
IP Address              SGT     Source
============================================
192.168.1.2             2       INTERNAL
192.168.35.2            2       INTERNAL

192.168.39.254          8       SXP       <<< Bindings learned trough SXP for the host connected in the


IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 0

Total number of SXP      bindings = 1


Total number of INTERNAL bindings = 2
Total number of active   bindings = 3
```

Führen Sie den Befehl aus, **show cts environment-data** um die globalen Daten der Cisco TrustSec-Umgebung anzuzeigen.

```
<#root>

#show

cts

 environment-data


CTS Environment Data
====================

Current state = COMPLETE


Last status = Successful
```

```
Service Info Table:
Local Device SGT:
  SGT tag = 2-01:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 1 server(s):
 Server: 10.88.244.146, port 1812, A-ID B546BF54CA5778A0734C8925EECE2215
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

Security Group Name Table:

0-00:Unknown

2-01:TrustSec_Devices

3-00:Network_Services

4-00:Employees

5-00:Contractors

6-00:Guests

7-00:Production_Users

8-02:Developers

<<<<< Security Group assigned to the host connected in the LAN side (SGT 8)

9-00:Auditors

10-00:Point_of_Sale_Systems

11-00:Production_Servers

12-00:Development_Servers

13-00:Test_Servers

14-00:PCI_Servers

```
    15-01:BYOD

Environment Data Lifetime = 86400 secs
```

Führen Sie den Befehlshow cts pacsaus, um die bereitgestellte Cisco TrustSec-PAC anzuzeigen.

```
<#root>
#show cts pacs


AID: B546BF54CA5778A0734C8925EECE2215

PAC-Info:

  PAC-type = Cisco Trustsec

  AID: B546BF54CA5778A0734C8925EECE2215

  I-ID: FLM2206W092



A-ID-Info: Identity Services Engine

  Credential Lifetime: 22:24:54 UTC Tue Dec 17 2024

PAC-Opaque: 000200B800030001000400010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8
```

Führen Sie den Befehlshow cts role-based permissions to Anzeigen der SGACL-Richtlinien

```
<#root>
#show

cts

 role-based permissions


IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group 2:TrustSec_Devices:
        Deny IP-00

IPv4 Role-based permissions from group 5:Contractors to group 8:Developers:



DNATELNET-00
```

```
IPv4 Role-based permissions from group 5:Contractors to group 15:BYOD:
        Deny IP-00
```

show cts rbacl (SGACLName)Führen Sie den Befehl aus, um die Konfiguration der Zugriffskontrollliste (SGACL) anzuzeigen.

<#root>

#show

cts

rbacl

DNATELNET

```
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =
```

DNATELNET-00

```
  IP protocol version = IPV4, IPV6
  refcnt = 2
  flag   = 0xC1000000
  stale  = FALSE
```

RBACL ACEs:

deny

tcp

dst

eq 23 log

<<<<< SGACL action

permit

ip

Zugehörige Informationen

- Cisco Catalyst SD-WAN - Sicherheitskonfigurationsleitfaden

- Cisco TrustSec Konfigurationsleitfaden

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.