TrustSec SGT SXP-doorgifte in SD-WAN configureren

Inhoud

Inleiding

In dit document wordt de configuratie beschreven van de voortplantingsmethode van Security Group Tag Exchange Protocol (SXP) in softwaregedefinieerde Wide Area Networks (SD-WAN).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst softwaregedefinieerde Wide Area Network (SD-WAN)
- Softwaregedefinieerde access (SD-Access) fabric
- Cisco Identify Service Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco IOS® XE Catalyst SD-WAN Edge versie 17.9.5a
- Cisco Catalyst SD-WAN Manager versie 20.12.4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

CISCO TRUSTsec-INTEGRATIE

SGT-doorgifte met Cisco TrustSec Integration wordt ondersteund door Cisco IOS® XE Catalyst SD-WAN release 17.3.1a en hoger. Deze eigenschap laat Cisco IOS® XE Catalyst SD-WAN randapparaten toe om inline tags van de Security Group Tag (SGT) te verspreiden die door Cisco TrustSec-enabled switches in de takken worden gegenereerd naar andere randapparaten in het Cisco Catalyst SD-WAN netwerk.

Basisconcepten van Cisco TrustSec:

- SGT-bindingen: Koppeling tussen IP en SGT, alle bindingen hebben de meest gebruikelijke configuratie en leren direct van Cisco ISE.
- SGT-doorgifte: De voortplantingsmethodes worden gebruikt om deze SGTs tussen netwerkhop te verspreiden.
- SGTACL-beleid: Reeks regels die de rechten van een verkeersbron binnen een vertrouwd netwerk specificeren.
- Handhaving van SGT: Waar het beleid wordt uitgevoerd, op basis van het SGT-beleid.

SGT-voortplantingsmethoden

De SGT-voortplantingsmethoden zijn:

- SGT-doorgifte - inline tagging
- SGT SXP-doorgifte

SGT-doorgifte met SXP

Voor Inline Tagging Propagation moeten de vestigingen worden uitgerust met Cisco TrustSec-enabled switches die SGT Inline Tagging (Cisco TrustSec Devices) kunnen verwerken. Als de hardware inline-tagging niet ondersteunt, maakt SGT-doorgifte gebruik van Security Group Tag Exchange Protocol (SXP) om SGT's over netwerkapparaten te verspreiden.

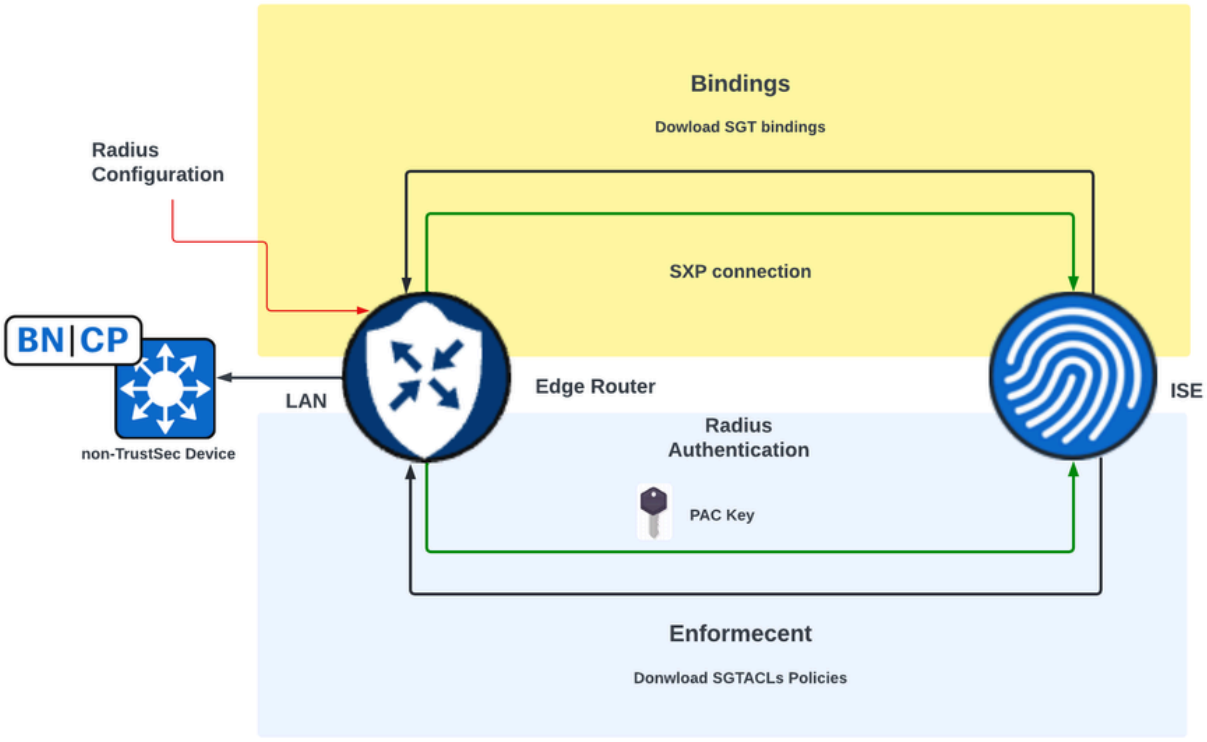
Cisco ISE maakt het mogelijk een IP-naar-SGT binding (Dynamic IP-SGT) te maken en downloadt vervolgens IP-SGT binding met SXP naar een Cisco IOS® XE Catalyst SD-WAN apparaat voor doorgifte van SGT via het Cisco Catalyst SD-WAN-netwerk. Ook worden de beleidsregels voor het SGT-verkeer op SD-WAN-uitgang afgedwongen door SGACL-beleid van ISE te downloaden.

Voorbeeld:

- De Cisco Switch (Border knooppunt) ondersteunt geen inline tagging (non-TrustSec-

apparaat).

- Cisco ISE maakt het mogelijk IP-SGT Binding te downloaden via SXP-verbinding met een Cisco IOS® XE Catalyst SD-WAN apparaat (Edge-router).
- Cisco ISE maakt het mogelijk om SGACL-beleid te downloaden via de Radius-integratie en PAC-toets naar een Cisco IOS® XE Catalyst SD-WAN apparaat (Edge-router).

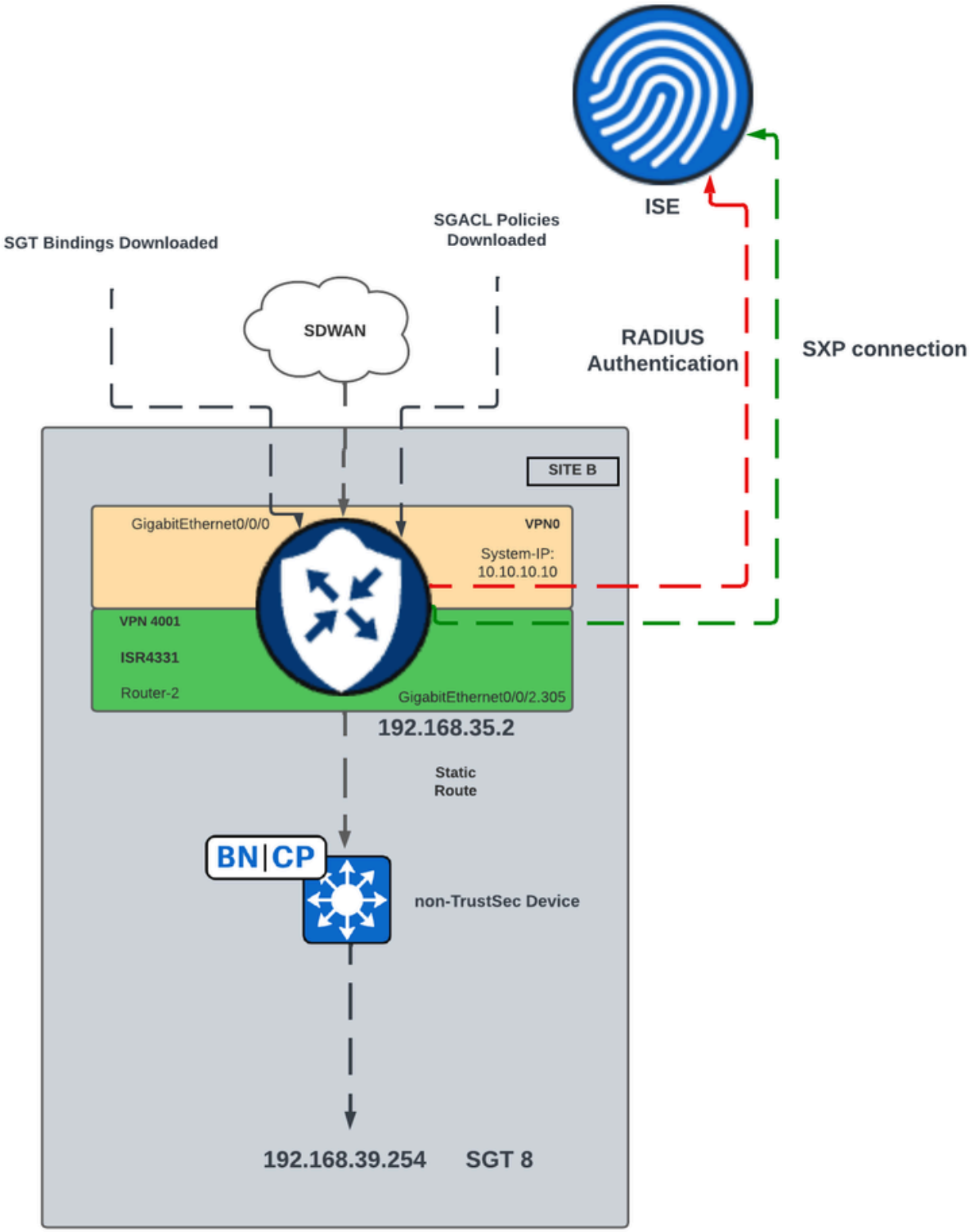


Vereisten om de SXP-doorgifte en het downloaden van SGACL-beleid op SD-WAN Edge-apparaten mogelijk te maken

Opmerking: SGACL-beleid wordt niet afgedwongen op het toegangsverkeer, alleen op uitgaand verkeer in een Cisco Catalyst SD-WAN-netwerk.

Opmerking: Cisco TrustSec-functie wordt niet ondersteund voor meer dan 24K SGT-beleid in controllermodus.

SGT SXP-doorgifte en -beleid voor downloaden van SGACL inschakelen



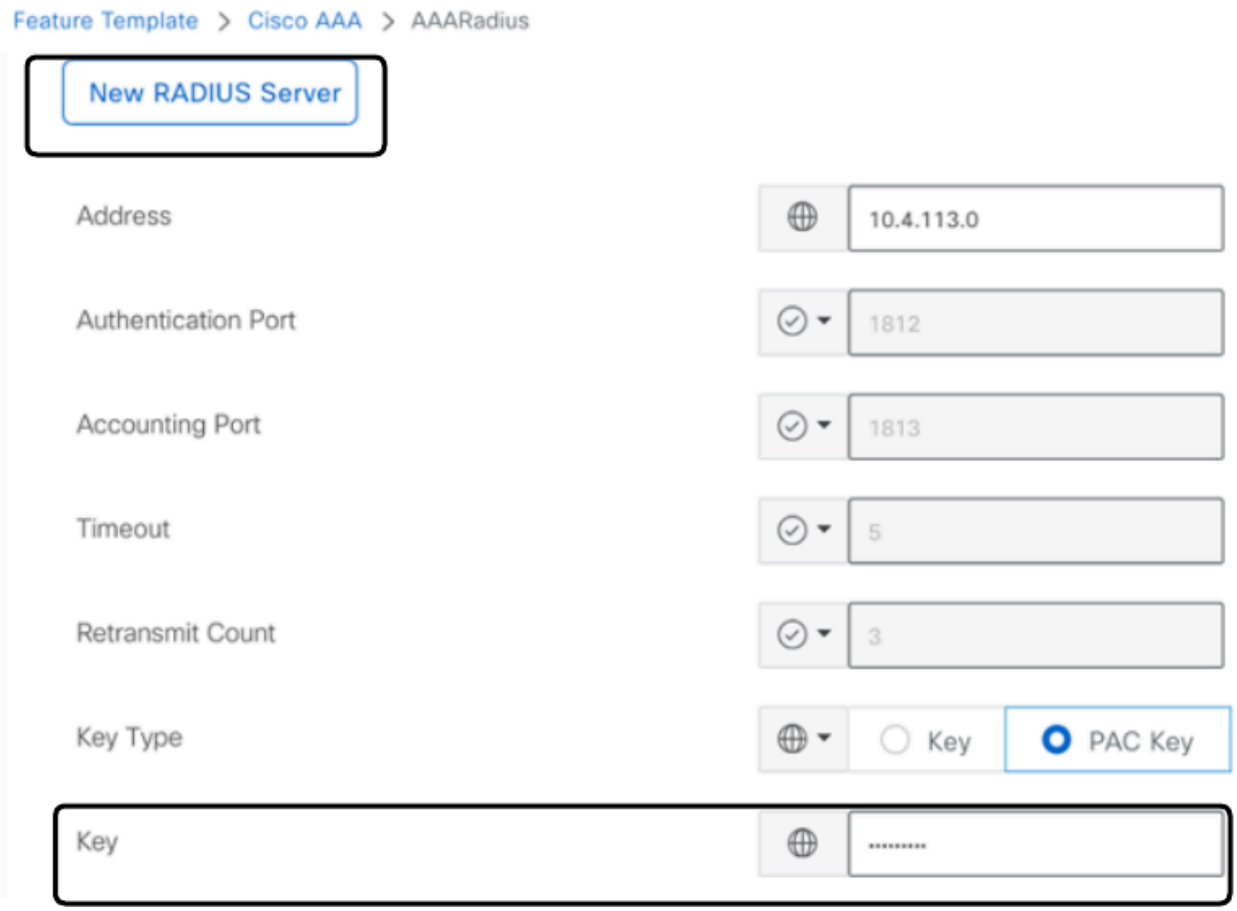
Netwerkdiagram voor SGT SXP-doorgifte in SD-WAN

Stap 1. Configureer de RADIUS-parameters

- Log in op Cisco Catalyst SD-WAN Manager GUI.
- Ga naar Configuration > Templates > Feature Template > Cisco AAA. Klik op RADIUS

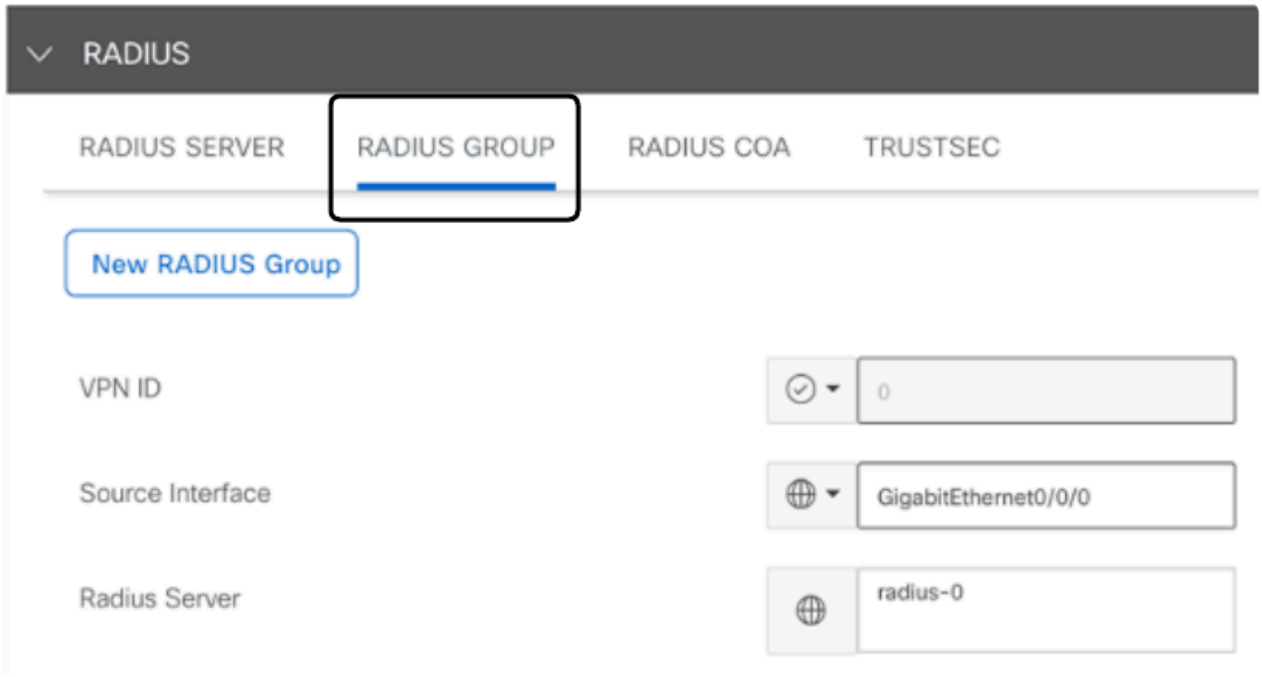
SERVER.

- Configureer de parameters en de sleutel van de RADIUS-SERVER.



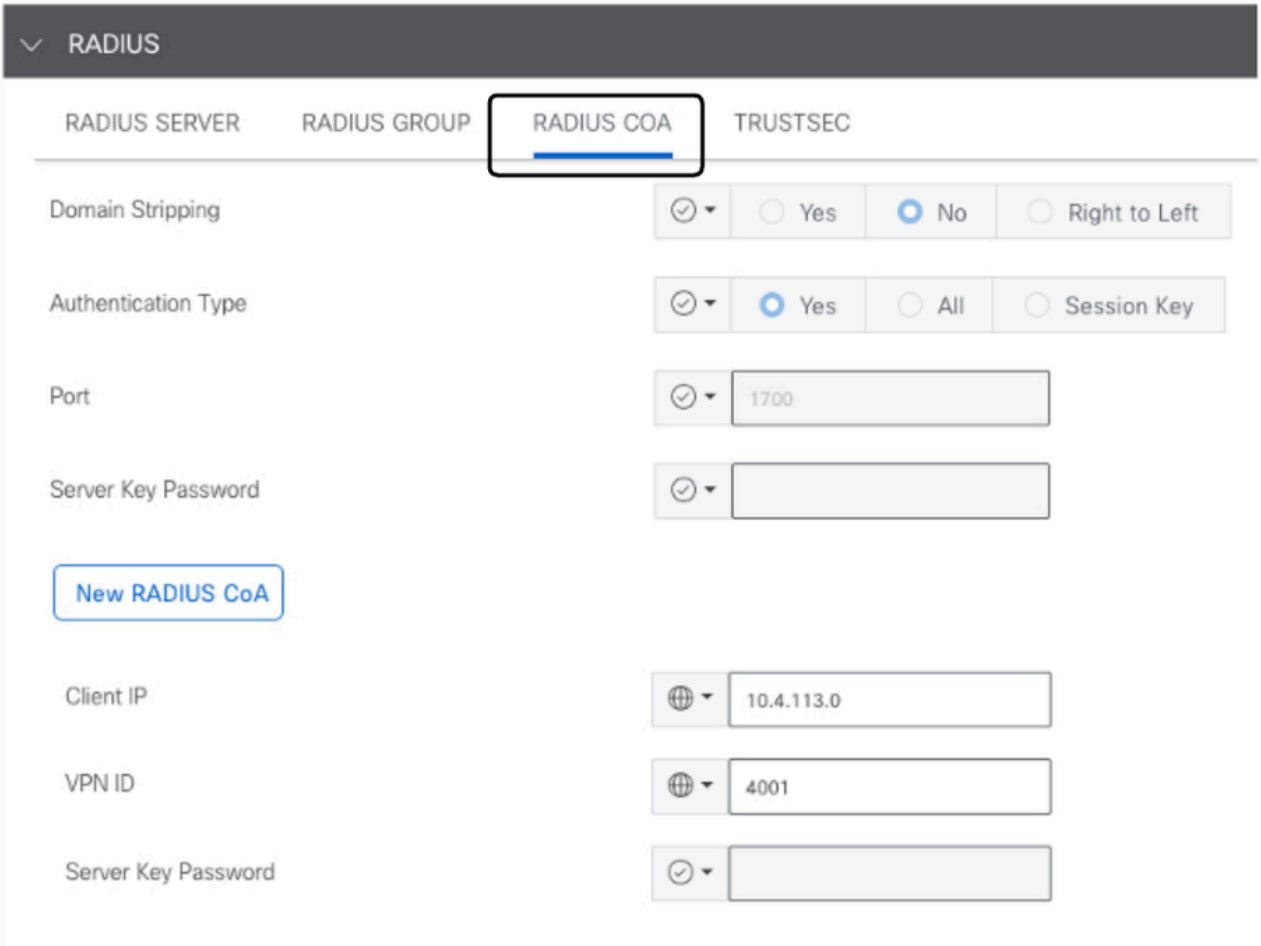
RADIUS-serverconfiguratie

- Voer de waarden in om de parameters van de RADIUS-groep te configureren.



Configuratie RADIUS-groep

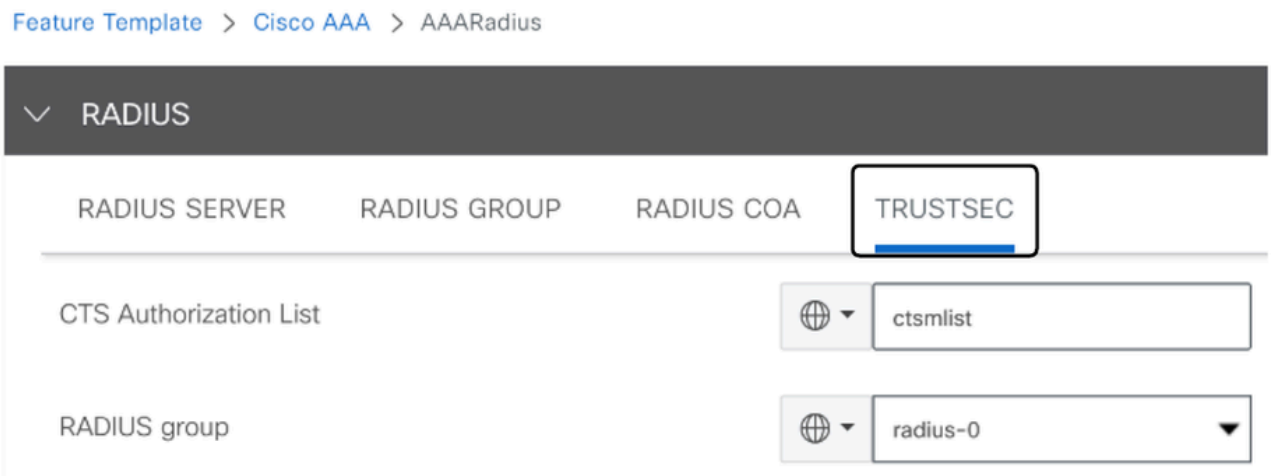
- Voer de waarden in om de RADIUS COA-parameters te configureren.



RADIUS-COA-configuratie

Opmerking: Als Radius COA niet is geconfigureerd, kan SD-WAN router het SGACL-beleid niet automatisch downloaden. Nadat u een SGACL-beleid van ISE hebt gemaakt of gewijzigd, wordt het commando cts refresh-beleid gebruikt om het beleid te downloaden.

- Navigeer naar TRUSTSEC en voer de waarden in.

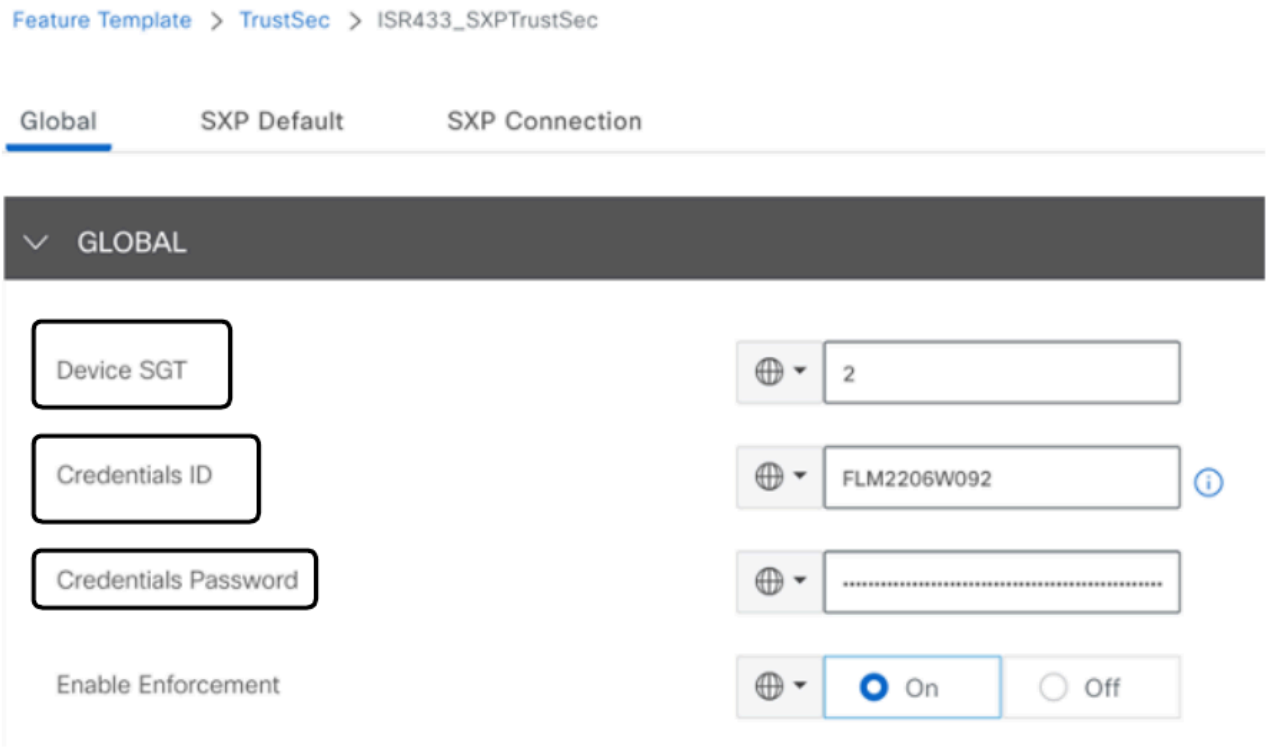


TRUSTSEC-configuratie

- Hang de Cisco AAA-functiesjabloon aan de apparaatsjabloon.

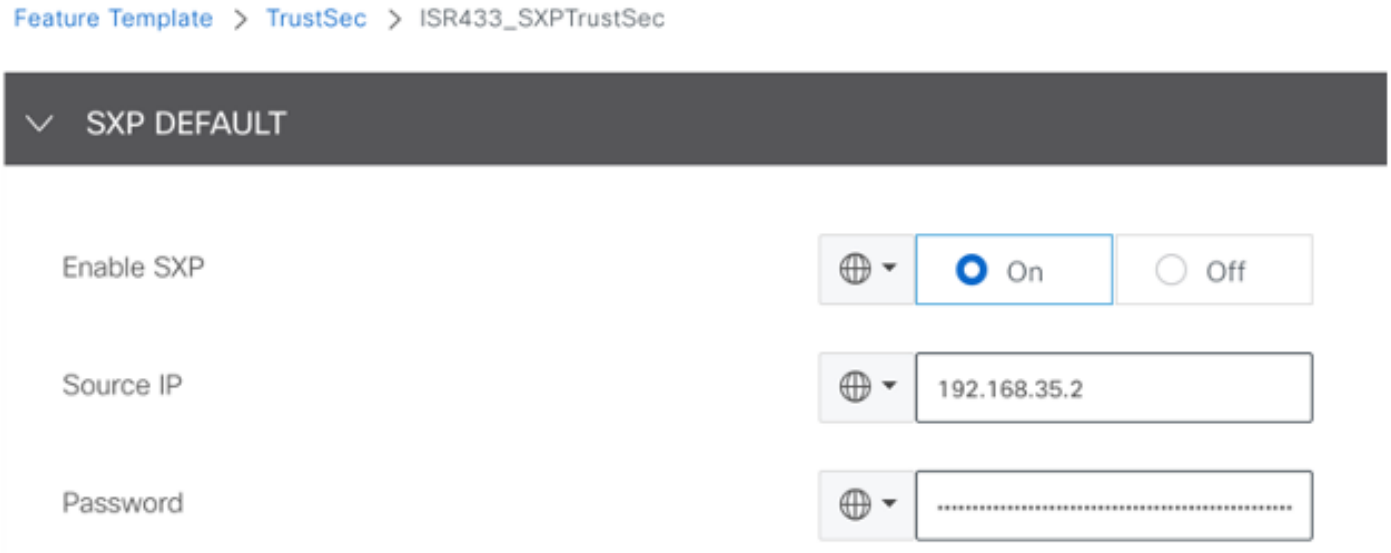
Stap 2. Configureer de SXP-parameters

- Navigeer naar Configuration > Templates > Feature Template > TrustSec.
- Configureer de CTS-referenties en wijs een SGT-binding aan apparaatinterfaces toe.



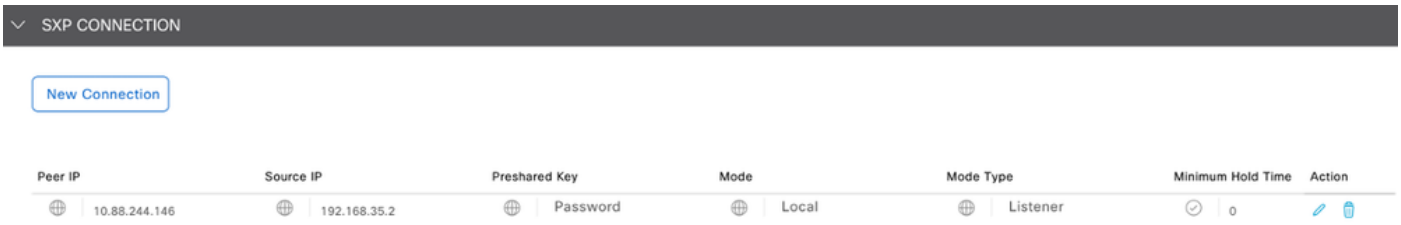
TrustSec-functiesjabloon

- Navigeer naar het gedeelte SXP Default en voer de waarden in om de parameters voor SXP Default te configureren.



SXP - standaardconfiguratie

- Navigeer naar SXP Connection en configureer de SXP Connection-parameters en klik vervolgens op Save.

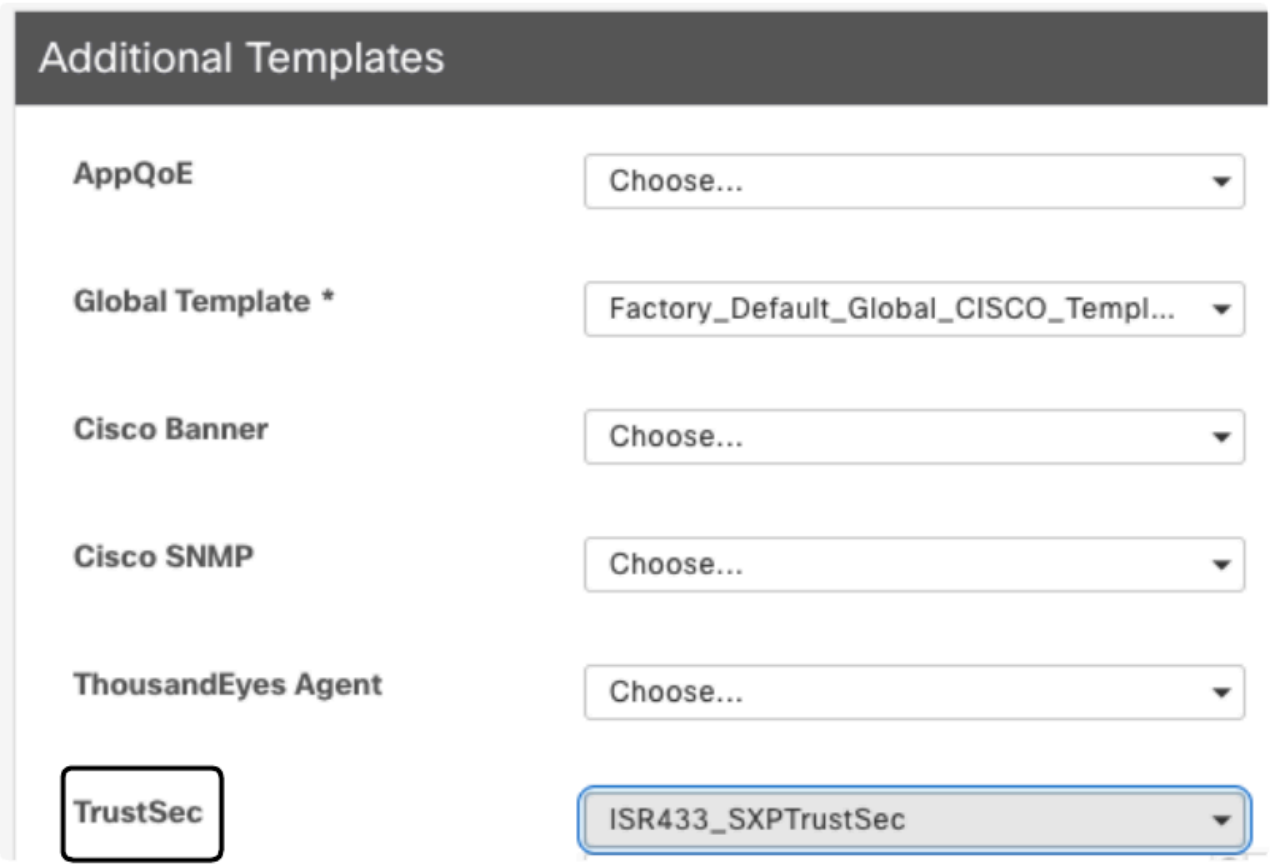


SXP-verbindingsconfiguratie

Opmerking: Cisco ISE heeft een limiet op het aantal SXP-sessies dat de klant kan verwerken. Daarom kan als alternatief een SXP Reflector voor schaal netwerk horizontaal worden gebruikt.

Opmerking: Het wordt aanbevolen om een SXP-reflector te gebruiken om een SXP-peer te maken met Cisco IOS® XE Catalyst SD-WAN apparaten.

- Navigeer naar Configuratie > Sjablonen > Apparaatsjabloon > Aanvullende sjablonen > TrustSec.
- Selecteer de TrustSec functiesjabloon die eerder gemaakt is, klik op Opslaan.



Sectie Aanvullende sjablonen

Verifiëren

Voer de opdracht uitshow cts sxp connections vrf (service vrf)om de informatie over de Cisco TrustSec SXP-verbindingen weer te geven.

<#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

Start de opdracht **show cts role-based sgt-map** tDe wereldwijde Cisco TrustSec SGT-kaart tussen IP-adres en SGT-banden weergeven.

```
<#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
```

Voer de opdracht uit **show cts environment-data** om de wereldwijde Cisco TrustSec Environment Data weer te geven.

```
<#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
```

Start de opdrachtshow cts pacsom de geleverde Cisco TrustSec PAC weer te geven.

<#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

Voer de opdrachtshow cts role-based permissions t uitHet SGACL-beleid weergeven.

<#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

Start de opdrachtshow cts rbacl (SGACLName)om de configuratie van de toegangscontrolelijst (SGACL) weer te geven.

<#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

Gerelateerde informatie

- Configuratiehandleiding voor Cisco Catalyst SD-WAN security
- Configuratiehandleiding voor Cisco TrustSec

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.