Configuration de la propagation TrustSec SGT SXP dans SD-WAN

Table des matières

Introduction

Ce document décrit la configuration de la méthode de propagation SXP (Security Group Tag Exchange Protocol) dans les réseaux étendus définis par logiciel (SD-WAN).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco Catalyst
- Fabric d'accès défini par logiciel (SD-Access)
- Cisco Identity Service Engine (ISE)

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco IOS® XE Catalyst SD-WAN Edge version 17.9.5a
- Cisco Catalyst SD-WAN Manager version 20.12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Intégration de Cisco TrustSec

La propagation SGT avec l'intégration Cisco TrustSec est prise en charge par Cisco IOS® XE Catalyst SD-WAN version 17.3.1a et ultérieures. Cette fonctionnalité permet aux périphériques de périphérie SD-WAN Cisco IOS® XE Catalyst de propager les balises SGT (Security Group Tag) en ligne générées par les commutateurs Cisco TrustSec dans les filiales vers d'autres périphériques de périphérie du réseau SD-WAN Cisco Catalyst.

Concepts de base de Cisco TrustSec :

- Liaisons SGT : Association entre IP et SGT, toutes les liaisons ont la configuration la plus courante et apprennent directement de Cisco ISE.
- Propagation SGT : Les méthodes de propagation sont utilisées pour propager ces balises SGT entre les sauts de réseau.
- Politiques des SGTACL : Ensemble de règles qui spécifient les privilèges d'une source de trafic au sein d'un réseau approuvé.
- Application SGT : Lorsque les politiques sont appliquées, en fonction de la politique SGT.

Méthodes de propagation SGT

Les méthodes de propagation SGT sont les suivantes :

- Propagation SGT Étiquetage en ligne
- Propagation SGT SXP

Propagation SGT avec SXP

Pour la propagation de l'étiquetage en ligne, les filiales doivent être équipées de commutateurs compatibles Cisco TrustSec capables de gérer l'étiquetage en ligne SGT (périphériques Cisco TrustSec). Si le matériel ne prend pas en charge l'étiquetage en ligne, la propagation SGT utilise le protocole SXP (Security Group Tag Exchange Protocol) pour propager les balises SGT sur les périphériques réseau.

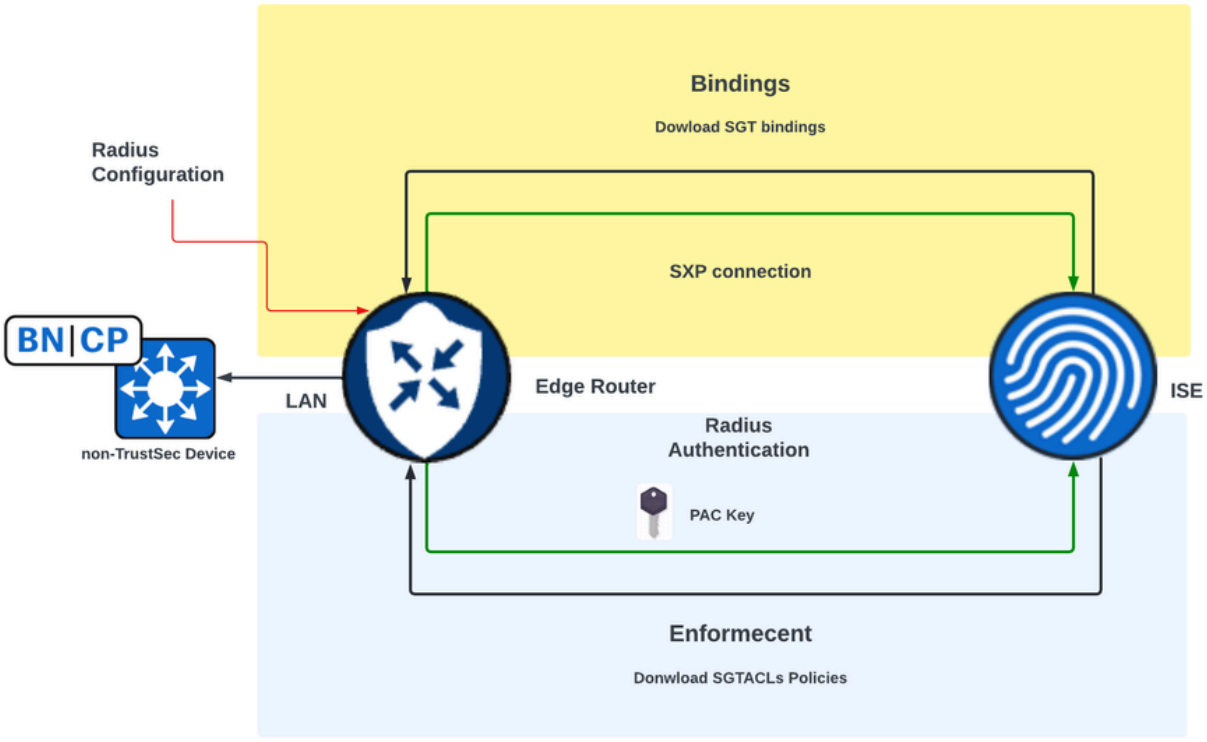
Cisco ISE permet de créer une liaison IP-SGT (Dynamic IP-SGT), puis de télécharger la liaison IP-SGT à l'aide de SXP sur un périphérique Cisco IOS® XE Catalyst SD-WAN pour la propagation de la liaison SGT sur le réseau Cisco Catalyst SD-WAN. En outre, les politiques pour le trafic SGT en sortie SD-WAN sont appliquées en téléchargeant les politiques SGACL depuis ISE.

Exemple :

- Le commutateur Cisco (noeud Périphérie) ne prend pas en charge l'étiquetage en ligne

(périphérique non TrustSec).

- Cisco ISE permet de télécharger la liaison IP-SGT via une connexion SXP vers un périphérique Cisco IOS® XE Catalyst SD-WAN (routeur de périphérie).
- Cisco ISE permet de télécharger les stratégies SGACL via l'intégration Radius et la clé PAC pour un Périphérique SD-WAN Cisco IOS® XE Catalyst (routeur de périphérie).



Configuration requise pour activer la propagation SXP et télécharger les stratégies SGACL sur les périphériques de périphérie SD-WAN

Remarque : Les stratégies SGACL ne sont pas appliquées au trafic entrant, mais uniquement au trafic sortant dans un réseau Cisco Catalyst SD-WAN.

Remarque : la fonctionnalité Cisco TrustSec n'est pas prise en charge pour plus de 24 000 stratégies SGT en mode contrôleur.

Activer la propagation SGT SXP et télécharger les stratégies SGACL

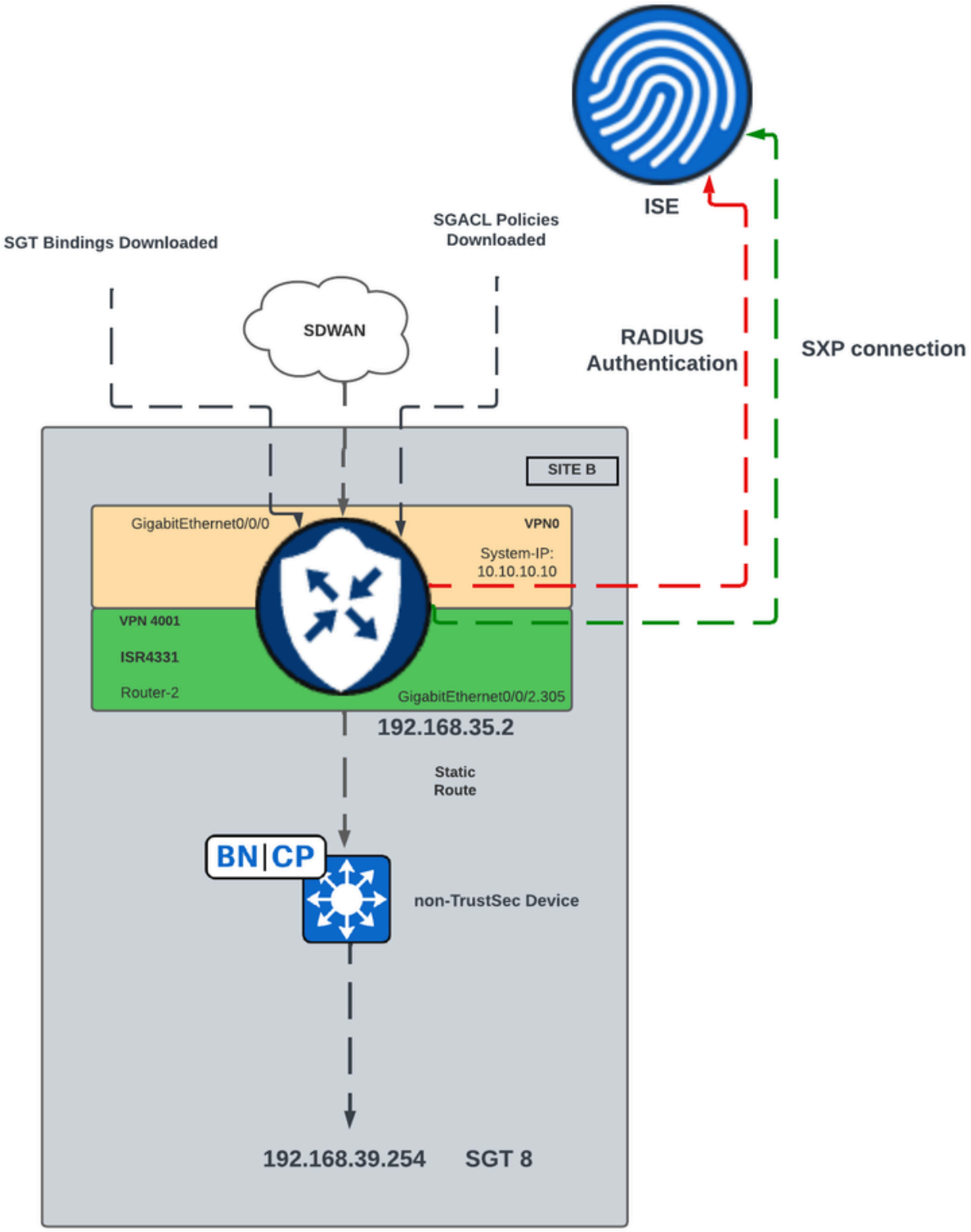


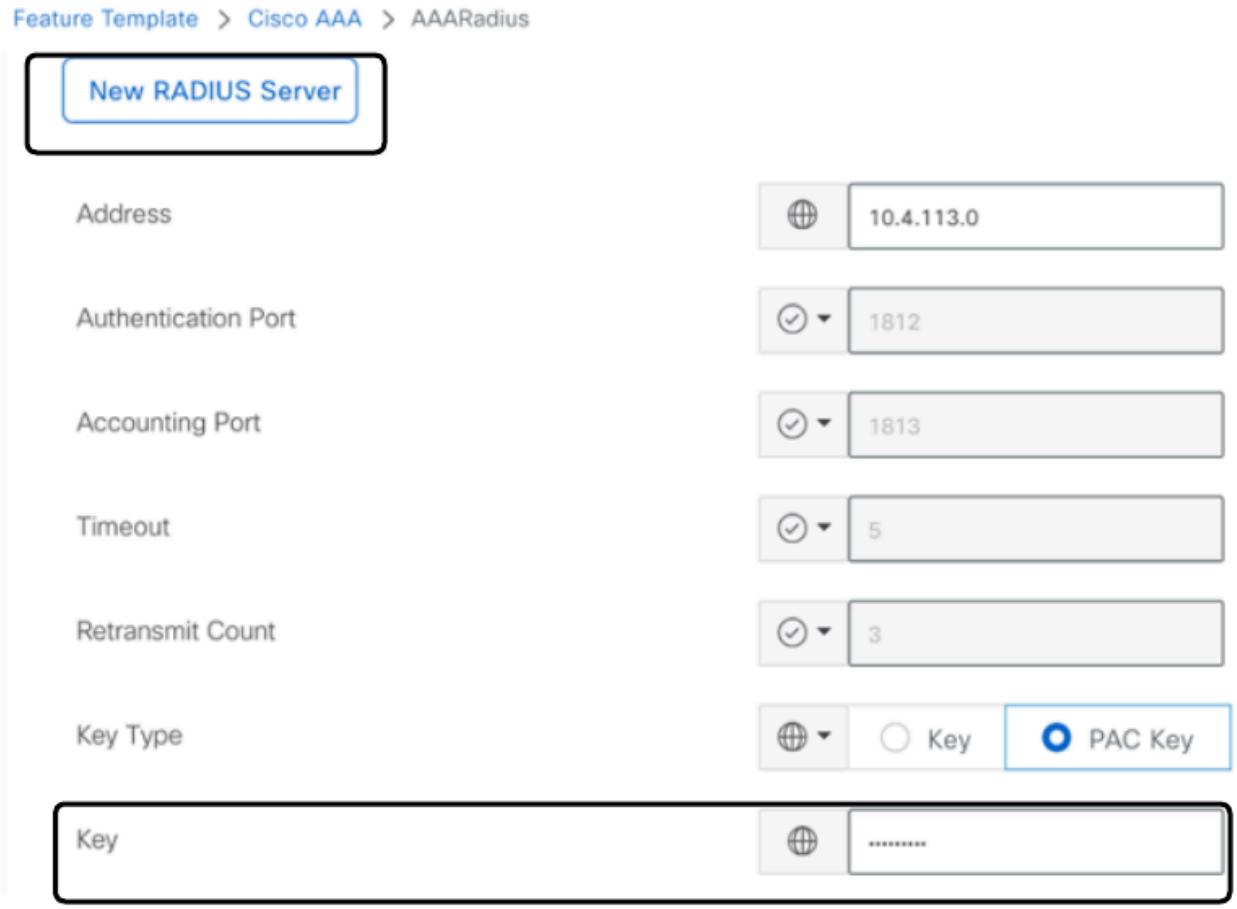
Schéma de réseau pour la propagation SGT SXP dans SD-WAN

Étape 1 : configuration des paramètres Radius

- Connectez-vous à l'interface utilisateur graphique de Cisco Catalyst SD-WAN Manager.
- Accédez à Configuration > Templates > Feature Template > Cisco AAA. Cliquez sur

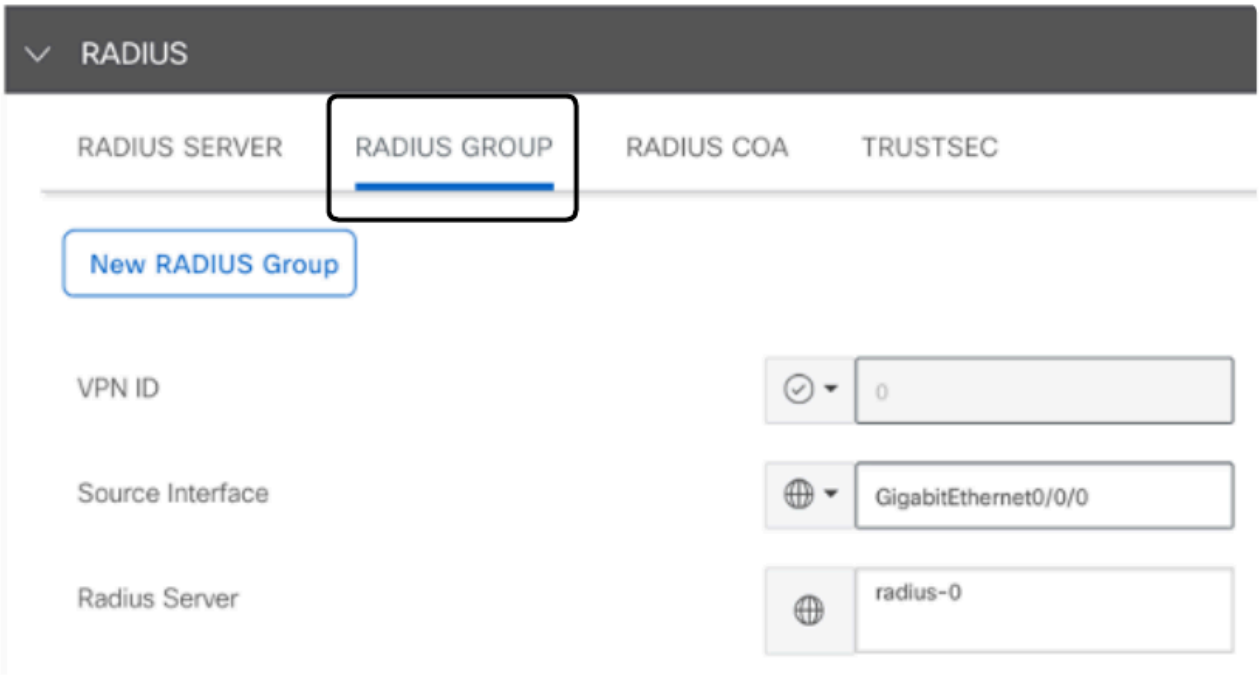
RADIUS SERVER.

- Configurez les paramètres et la clé du SERVEUR RADIUS.



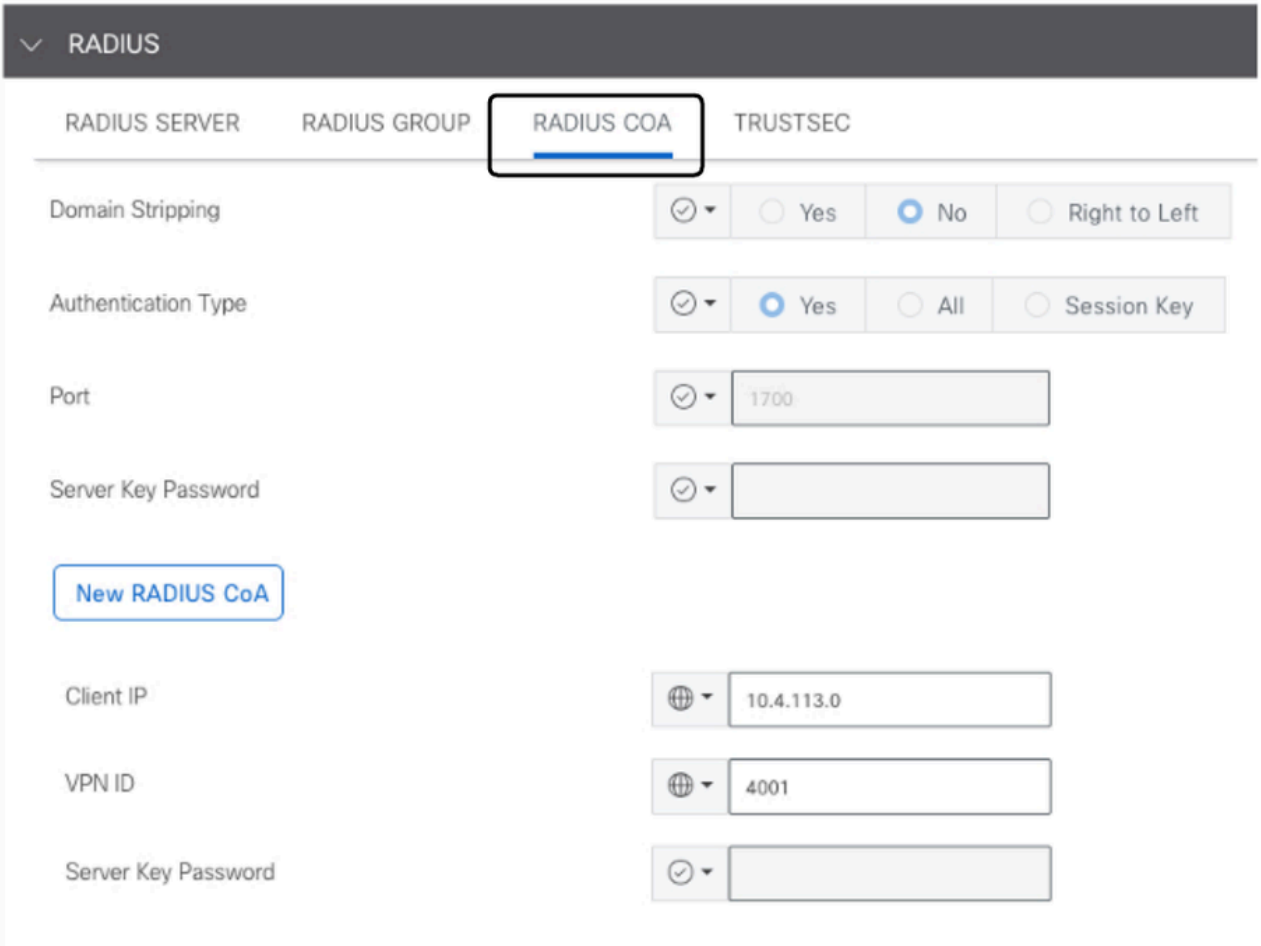
Configuration du serveur RADIUS

- Entrez les valeurs pour configurer les paramètres du groupe de rayons.



Configuration du groupe RADIUS

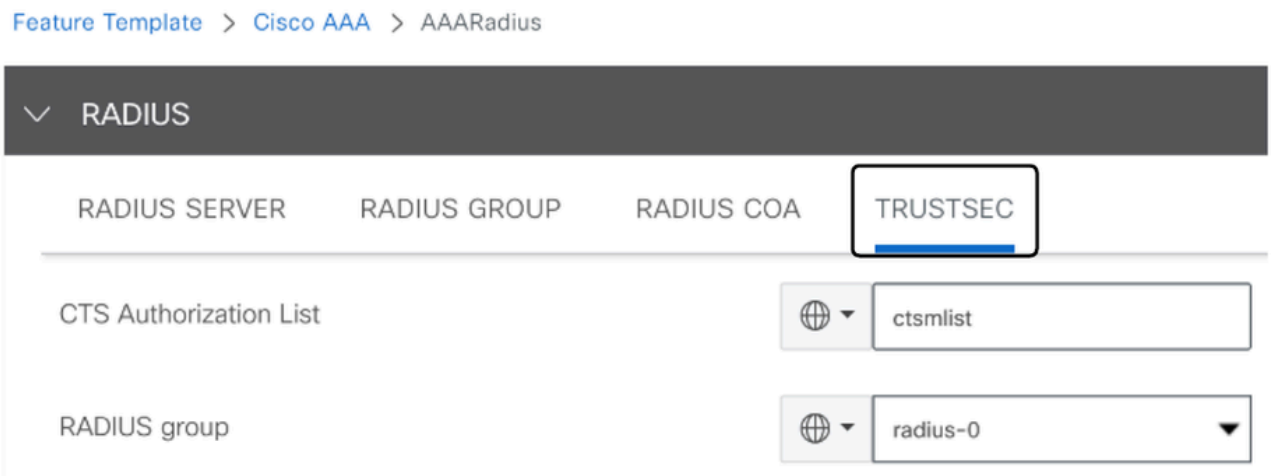
- Entrez les valeurs pour configurer les paramètres Radius COA.



Configuration du certificat RADIUS

Remarque : Si Radius COA n'est pas configuré, le routeur SD-WAN ne peut pas télécharger automatiquement les stratégies SGACL. Après avoir créé ou modifié une stratégie SGACL à partir d'ISE, la commande cts refresh policy est utilisée pour télécharger les stratégies.

- Accédez à la section TRUSTSEC et entrez les valeurs.

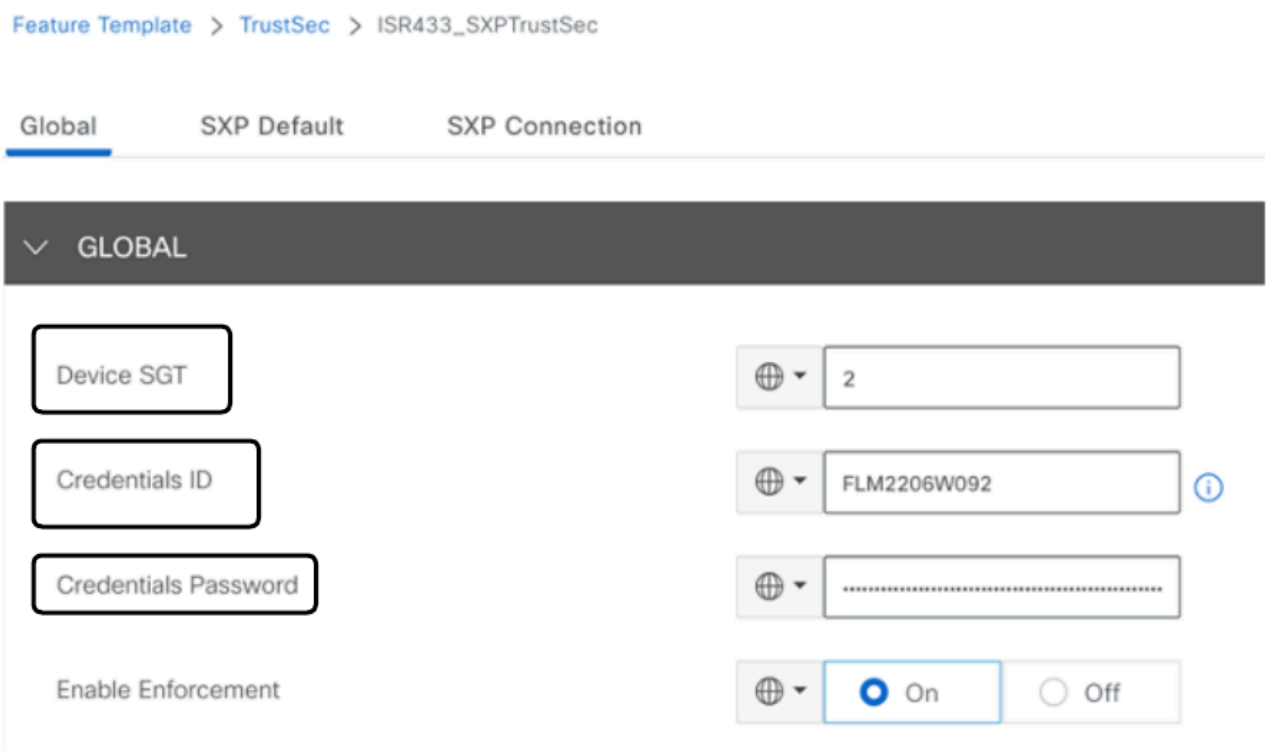


Configuration TRUSTSEC

- Associez le modèle de fonctionnalité Cisco AAA au modèle de périphérique.

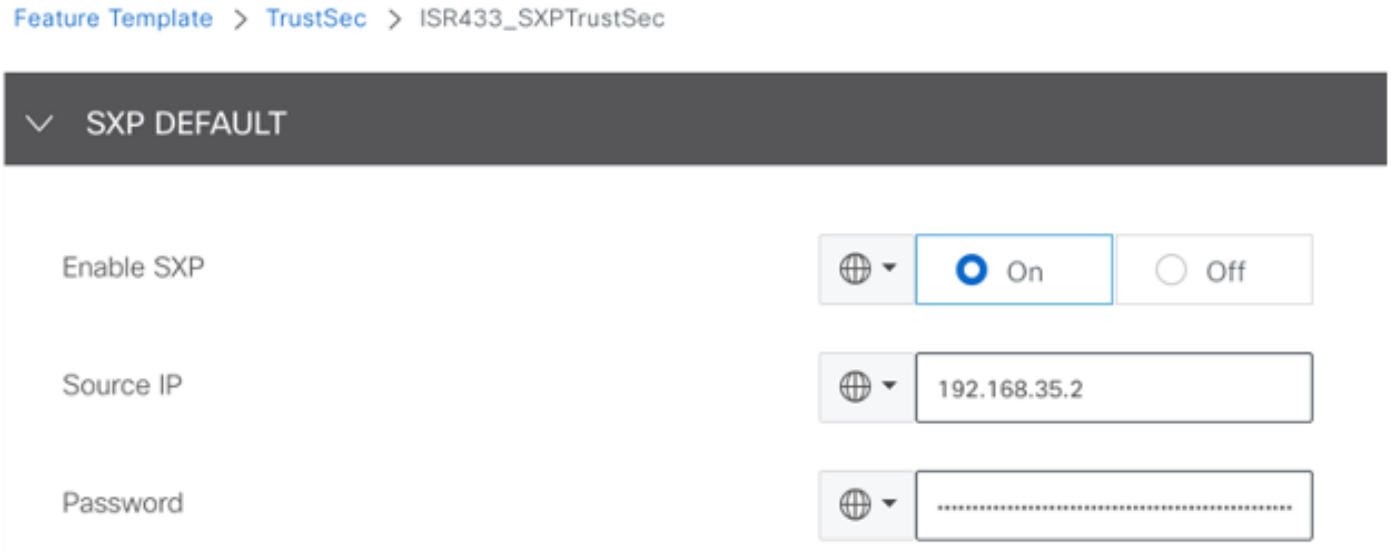
Étape 2 : configuration des paramètres SXP

- Accédez à Configuration > Templates > Feature Template > TrustSec.
- Configurez les informations d'identification CTS et attribuez une liaison SGT aux interfaces de périphériques.



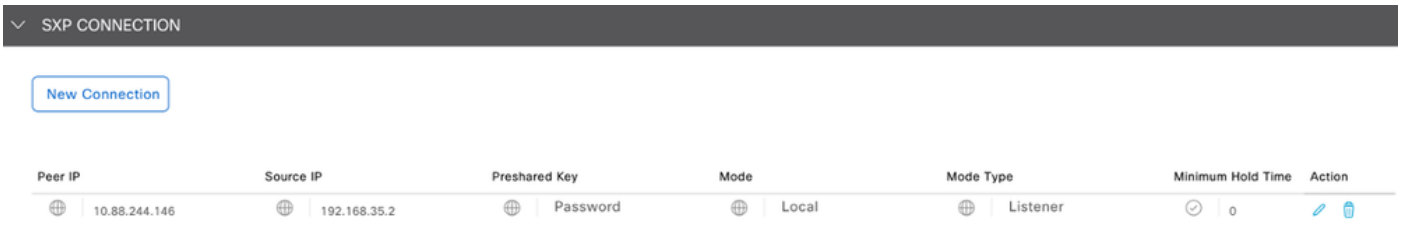
Modèle de fonctionnalité TrustSec

- Accédez à la section SXP Default et entrez les valeurs pour configurer les paramètres SXP Default.



Configuration SXP par défaut

- Accédez à SXP Connection et configurez les paramètres SXP Connection, puis cliquez sur Save.

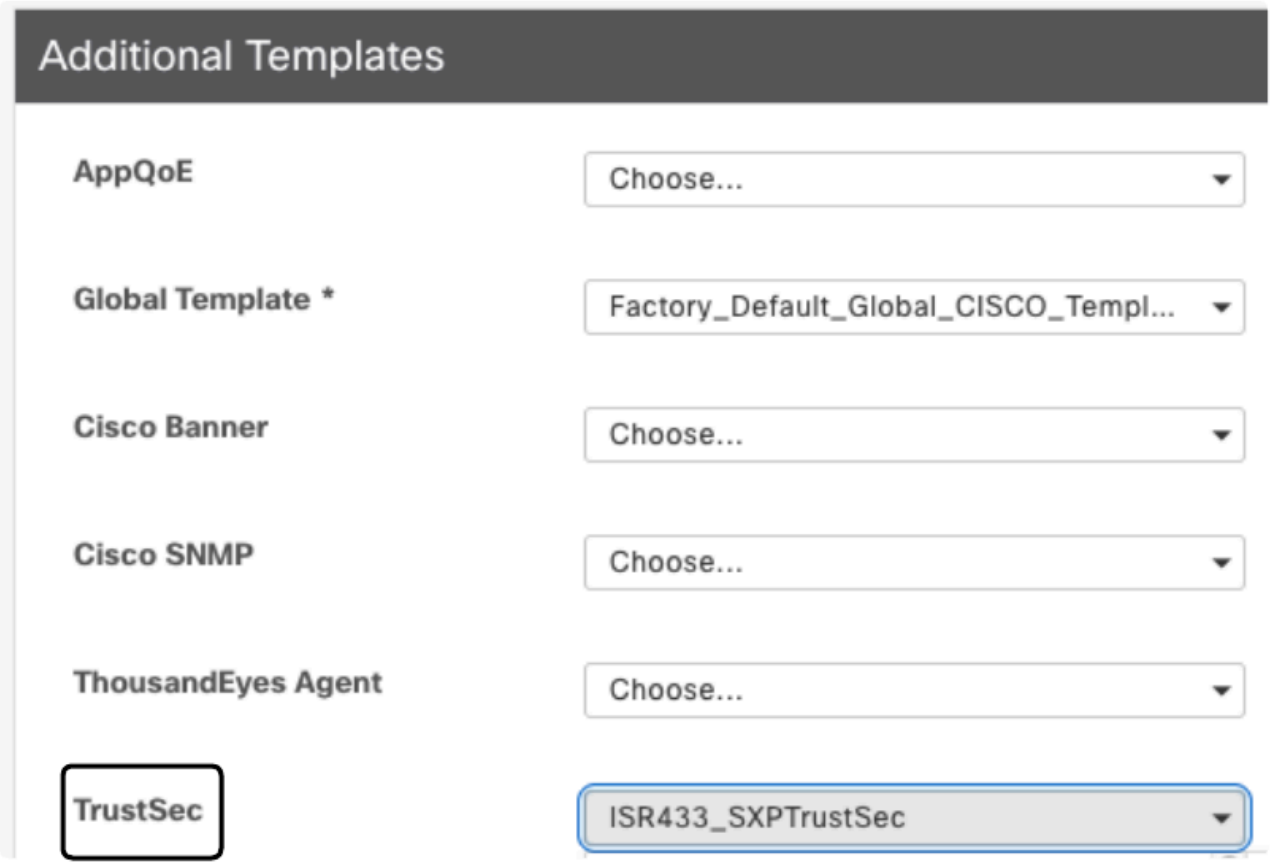


Configuration de la connexion SXP

Remarque : Cisco ISE limite le nombre de sessions SXP qu'il peut gérer. Par conséquent, comme alternative, un réflecteur SXP pour l'échelle horizontale du réseau pourrait être utilisé.

Remarque : Il est recommandé d'utiliser un réflecteur SXP pour établir un homologue SXP avec des périphériques Cisco IOS® XE Catalyst SD-WAN.

- Accédez à Configuration > Templates > Device Template > Additional Templates > TrustSec.
- Sélectionnez le modèle de fonctionnalité TrustSec précédemment créé, cliquez sur Enregistrer.



Section Modèles supplémentaires

Vérifier

Exécutez la commandeshow cts sxp connections vrf (service vrf)pour afficher les informations de connexion Cisco TrustSec SXP.

<#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

Exécutez la commande **show cts role-based sgt-map** tPour afficher le mappage global des balises SGT Cisco TrustSec entre les liaisons d'adresse IP et de balises SGT.

```
<#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
```

Exécutez la commande **show cts environment-data** pour afficher les données globales de l'environnement Cisco TrustSec.

```
<#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
```

Exécutez la commande`show cts pacs`pour afficher le PAC Cisco TrustSec provisionné.

```
<#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: 000200B80003000100040010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8
```

Exécutez la commande`show cts role-based permissions t`Pour afficher les stratégies SGACL.

```
<#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
```

Exécutez la commandeshow cts rbacl (SGACLName)pour afficher la configuration de la liste de contrôle d'accès (SGACL).

<#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

Informations connexes

- Guide de configuration de la sécurité SD-WAN de Cisco Catalyst

- Guide de configuration de Cisco TrustSec

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.