Configurare la propagazione TrustSec SGT SXP in SD-WAN

Sommario

Introduzione

In questo documento viene descritto come configurare il metodo di propagazione SXP (Security Group Tag Exchange Protocol) in SD-WAN (Software-Defined Wide-Area Network).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Software Cisco Catalyst Defined Wide Area Network (SD-WAN)
- Fabric ad accesso definito dal software (SD-Access)
- Cisco Identify Service Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano su:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Integrazione Cisco TrustSec

La propagazione SGT con integrazione Cisco TrustSec è supportata da Cisco IOS® XE Catalyst SD-WAN versione 17.3.1a e successive. Questa funzionalità consente a Cisco IOS® XE Catalyst SD-WAN Edge Device di propagare i tag in linea Security Group Tag (SGT) generati dagli switch Cisco TrustSec nelle filiali ad altri dispositivi periferici della rete Cisco Catalyst SD-WAN.

Concetti base di Cisco TrustSec:

- Binding SGT: Associazione tra IP e SGT, tutti i binding hanno la configurazione più comune e vengono appresi direttamente da Cisco ISE.
- Propagazione SGT: I metodi di propagazione vengono utilizzati per propagare questi SGT tra gli hop di rete.
- Criteri SGTACL: Set di regole che specificano i privilegi di un'origine traffico all'interno di una rete attendibile.
- Applicazione SGT: Dove vengono applicate le politiche, sulla base della politica SGT.

Metodi di propagazione SGT

I metodi di propagazione SGT sono i seguenti:

- Tagging in linea propagazione SGT
- Propagazione SGT SXP

Propagazione SGT con SXP

Per la propagazione dei tag in linea, le filiali devono essere dotate di switch abilitati a Cisco TrustSec in grado di gestire i tag in linea SGT (dispositivi Cisco TrustSec). Se l'hardware non supporta la codifica in linea, la propagazione SGT utilizza il protocollo SXP (Security Group Tag Exchange Protocol) per propagare le schede SGT sui dispositivi di rete.

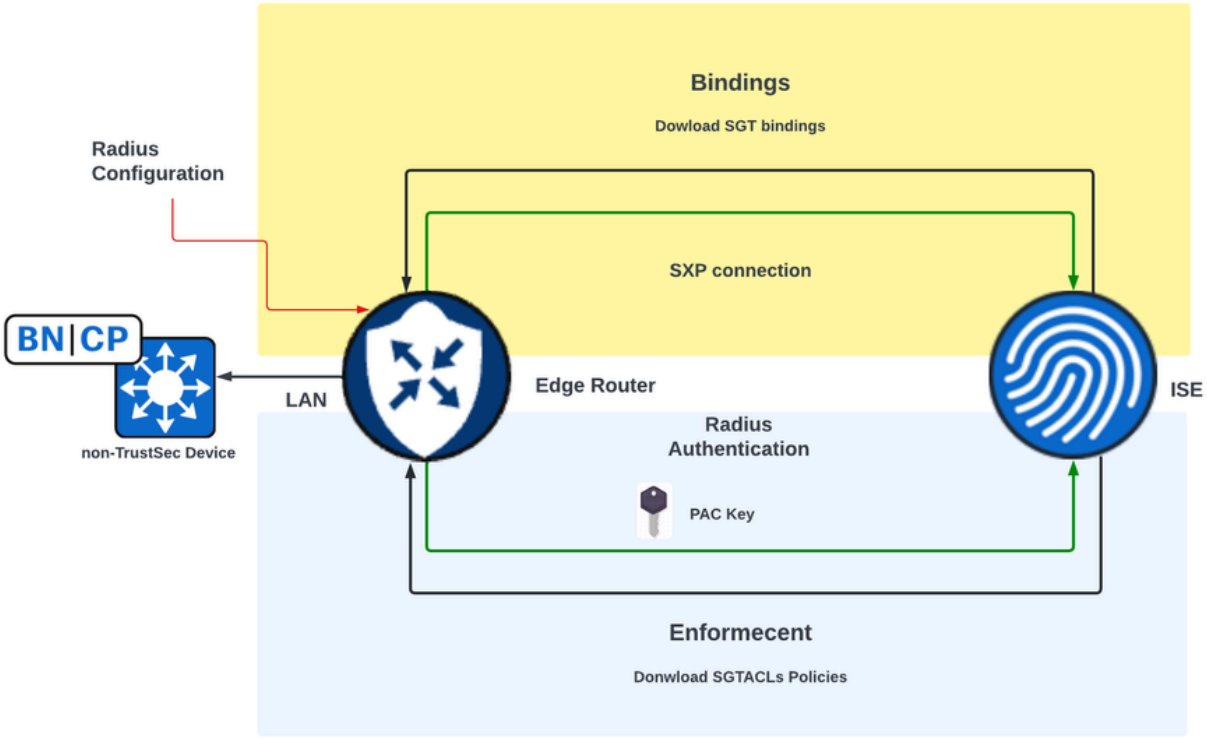
Cisco ISE consente di creare un binding IP-to-SGT (Dynamic IP-SGT) e quindi di scaricare il binding IP-SGT utilizzando SXP su un dispositivo SD-WAN Cisco IOS® XE Catalyst per la propagazione del SGT sulla rete Cisco Catalyst SD-WAN. Inoltre, i criteri per il traffico SGT su SD-WAN in uscita vengono imposti scaricando i criteri SGACL da ISE.

Esempio:

- Lo switch Cisco (nodo Border) non supporta i tag in linea (dispositivo diverso da TrustSec).
- Cisco ISE consente di scaricare il binding IP-SGT tramite una connessione SXP a un

dispositivo Cisco IOS® XE Catalyst SD-WAN (Edge Router).

- Cisco ISE consente di scaricare le policy SGACL tramite l'integrazione Radius e la chiave PAC su Dispositivo Cisco IOS® XE Catalyst SD-WAN (Edge Router).

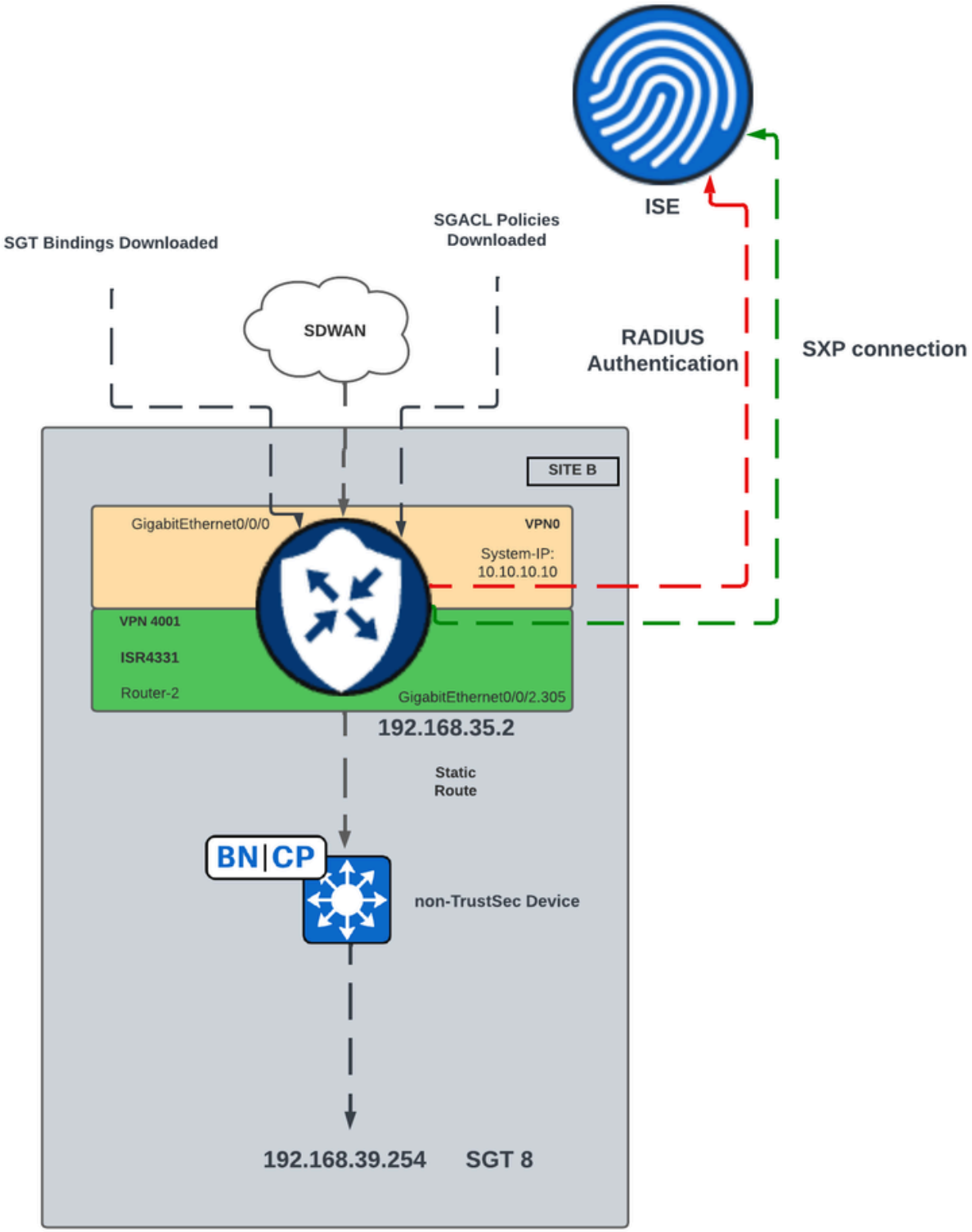


Requisiti per abilitare la propagazione SXP e scaricare i criteri SGACL sui dispositivi edge SD-WAN

Nota: Le policy SGACL non vengono applicate al traffico in entrata, ma solo al traffico in uscita su una rete Cisco Catalyst SD-WAN.

Nota: la funzionalità Cisco TrustSec non è supportata per più di 24.000 criteri SGT in modalità controller.

Abilita propagazione SGT SXP e scarica criteri SGACL



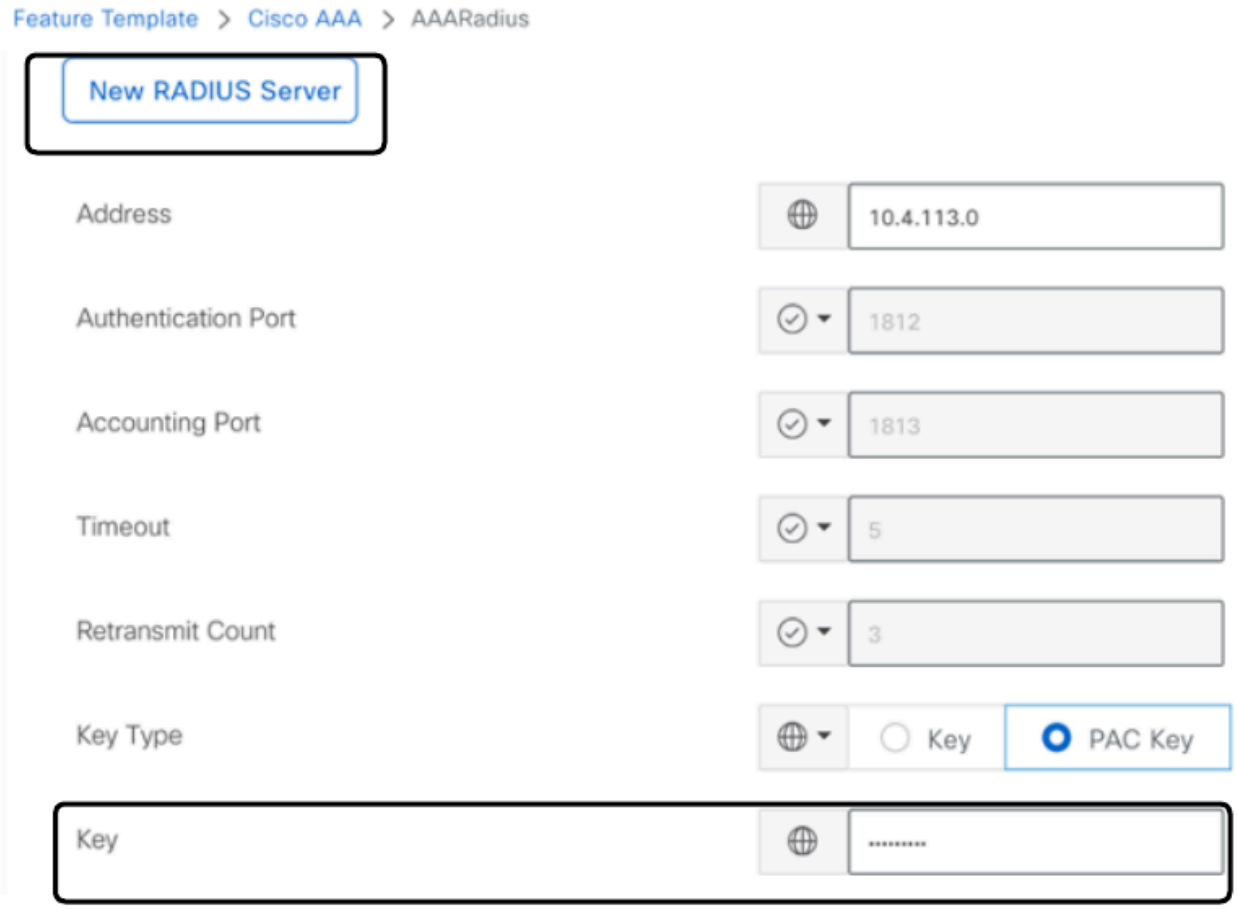
Esempio di rete per la propagazione SGT SXP in SD-WAN

Passaggio 1. Configurazione dei parametri Radius

- Accedere all'interfaccia utente di Cisco Catalyst SD-WAN Manager.
- Selezionare Configurazione > Modelli > Modello funzione > Cisco AAA. Fare clic su

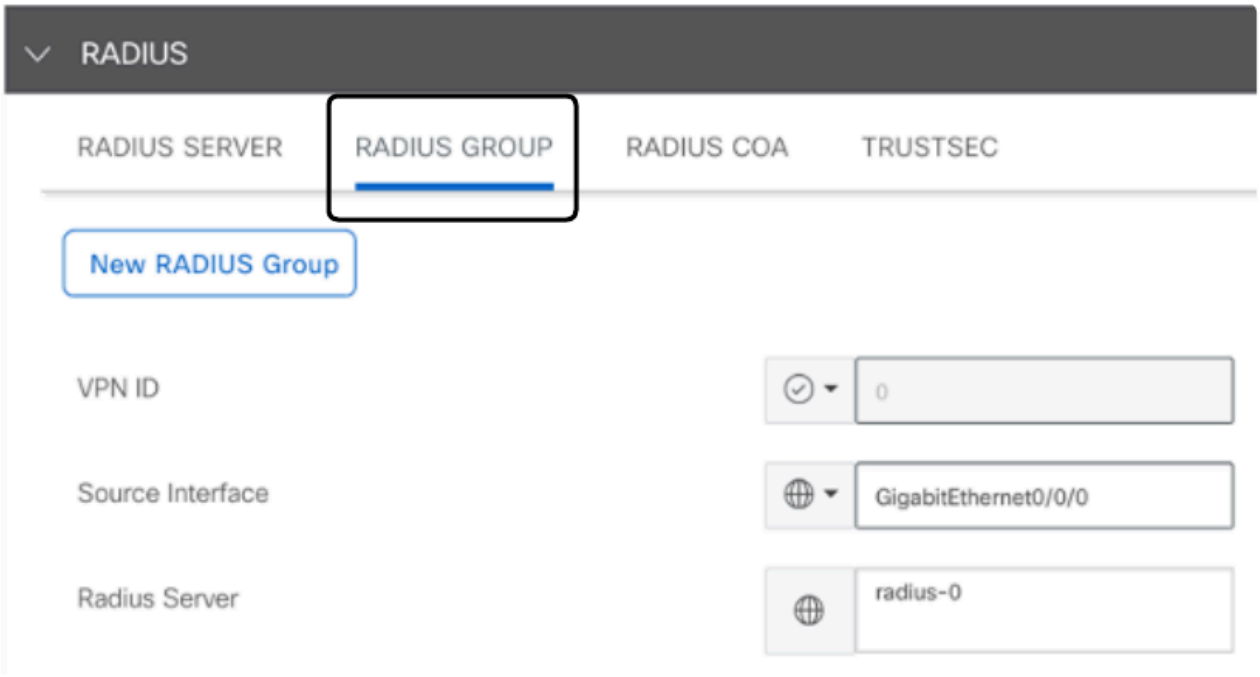
SERVER RADIUS.

- Configurare i parametri e la chiave DEL SERVER RADIUS.



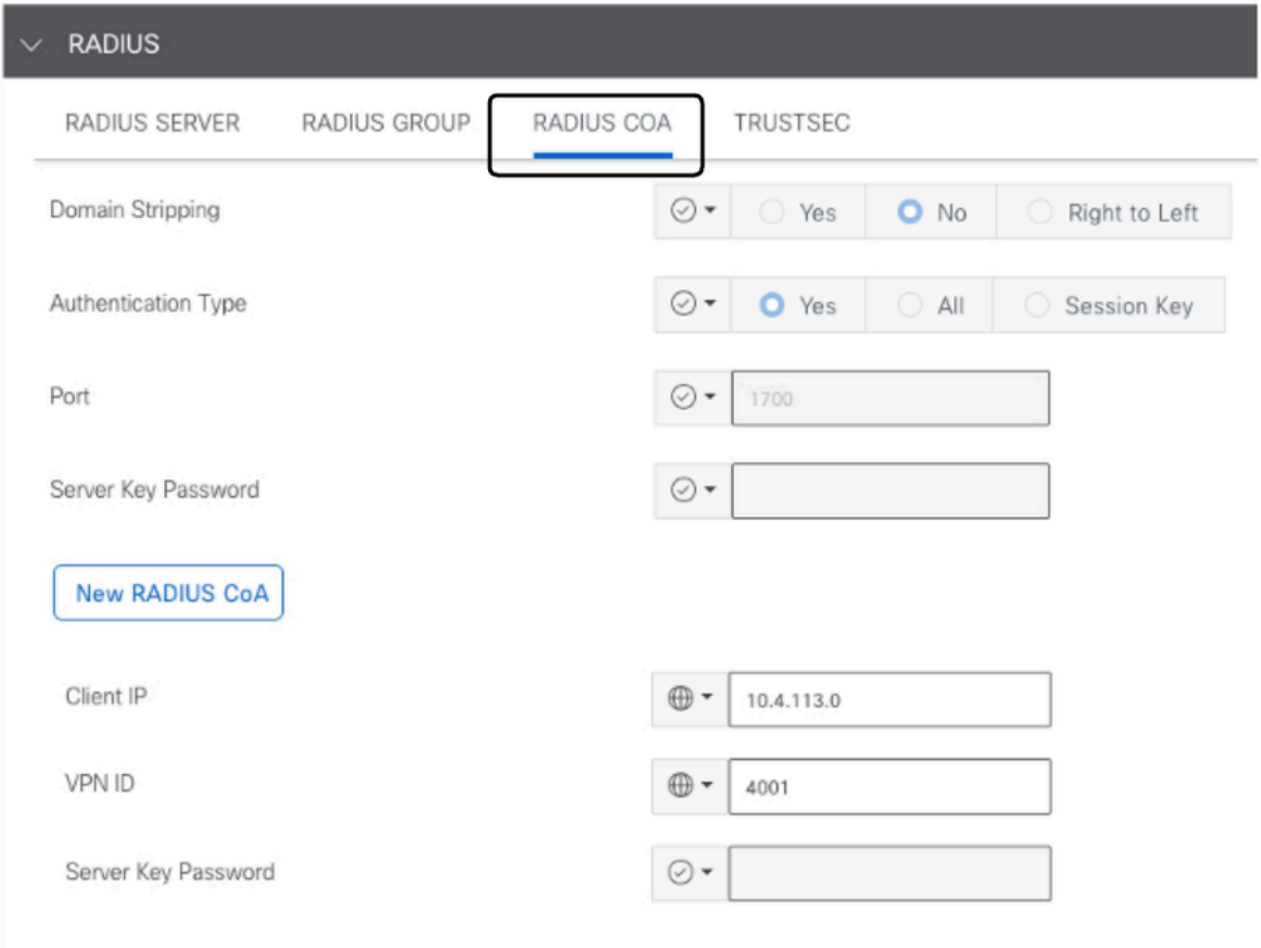
Configurazione server RADIUS

- Immettete i valori per configurare i parametri Gruppo raggio (Radius Group).



Configurazione gruppo RADIUS

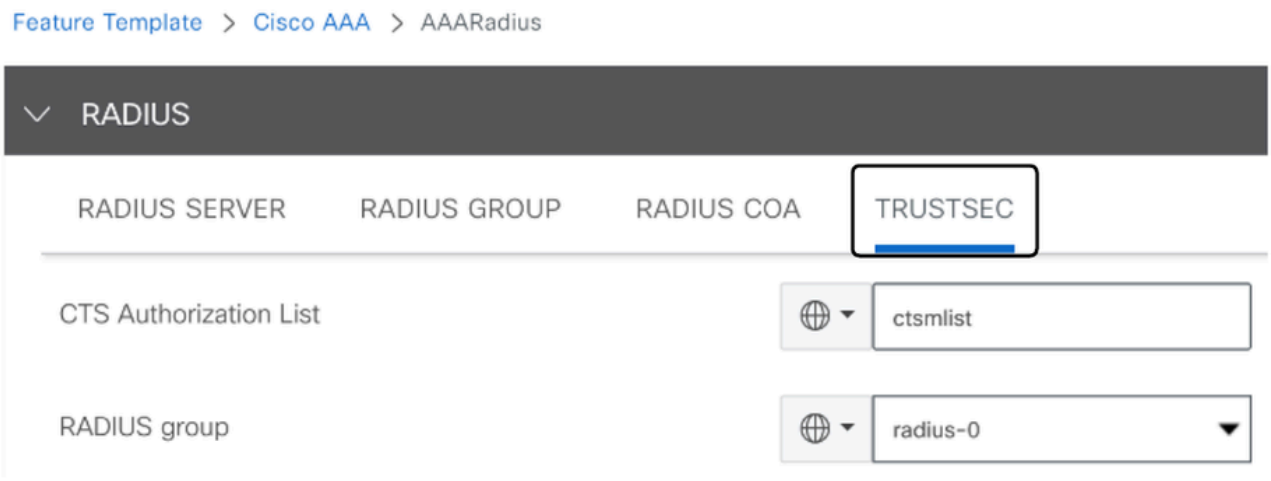
- Immettere i valori per configurare i parametri Radius COA.



Configurazione COA RADIUS

Nota: Se Radius COA non è configurato, il router SD-WAN non è in grado di scaricare automaticamente i criteri SGACL. Dopo aver creato o modificato un criterio SGACL da ISE, il comando cts refresh policy viene utilizzato per scaricare i criteri.

- Passare alla sezione TRUSTSEC e immettere i valori.

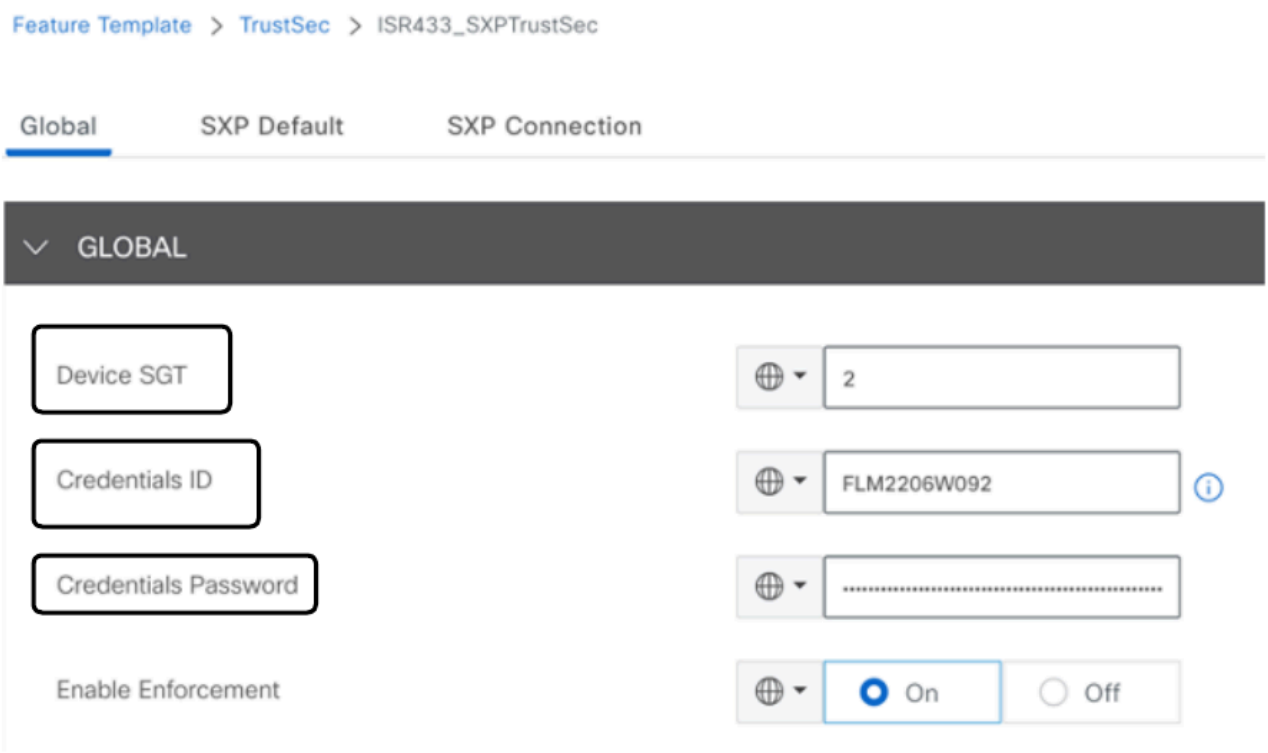


Configurazione TRUSTSEC

- Collegare il modello della funzione Cisco AAA al modello del dispositivo.

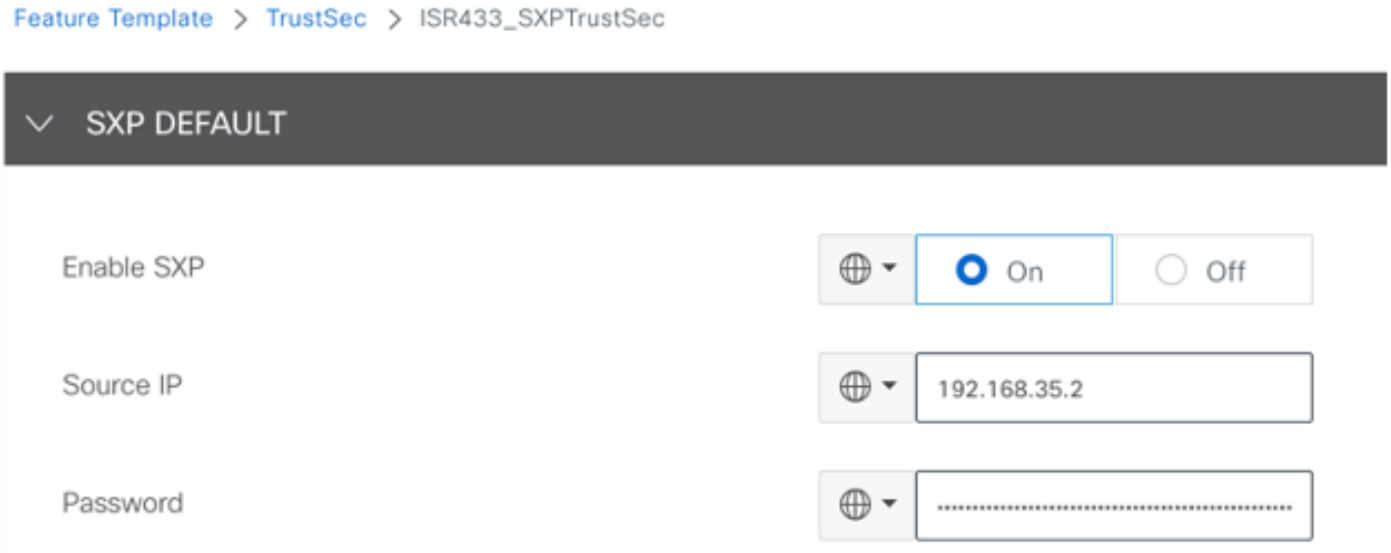
Passaggio 2. Configurare i parametri SXP

- Selezionare Configurazione > Modelli > Modello funzionalità > TrustSec.
- Configurare le credenziali CTS e assegnare un'associazione SGT alle interfacce dispositivo.



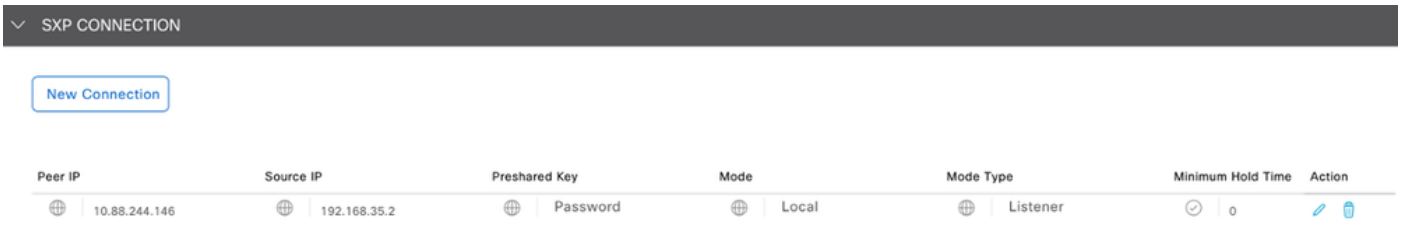
Modello funzionalità TrustSec

- Passare alla sezione SXP Default e immettere i valori per configurare i parametri SXP Default.



Configurazione predefinita SXP

- Passare a SXP Connection e configurare i parametri SXP Connection, quindi fare clic su Save (Salva).

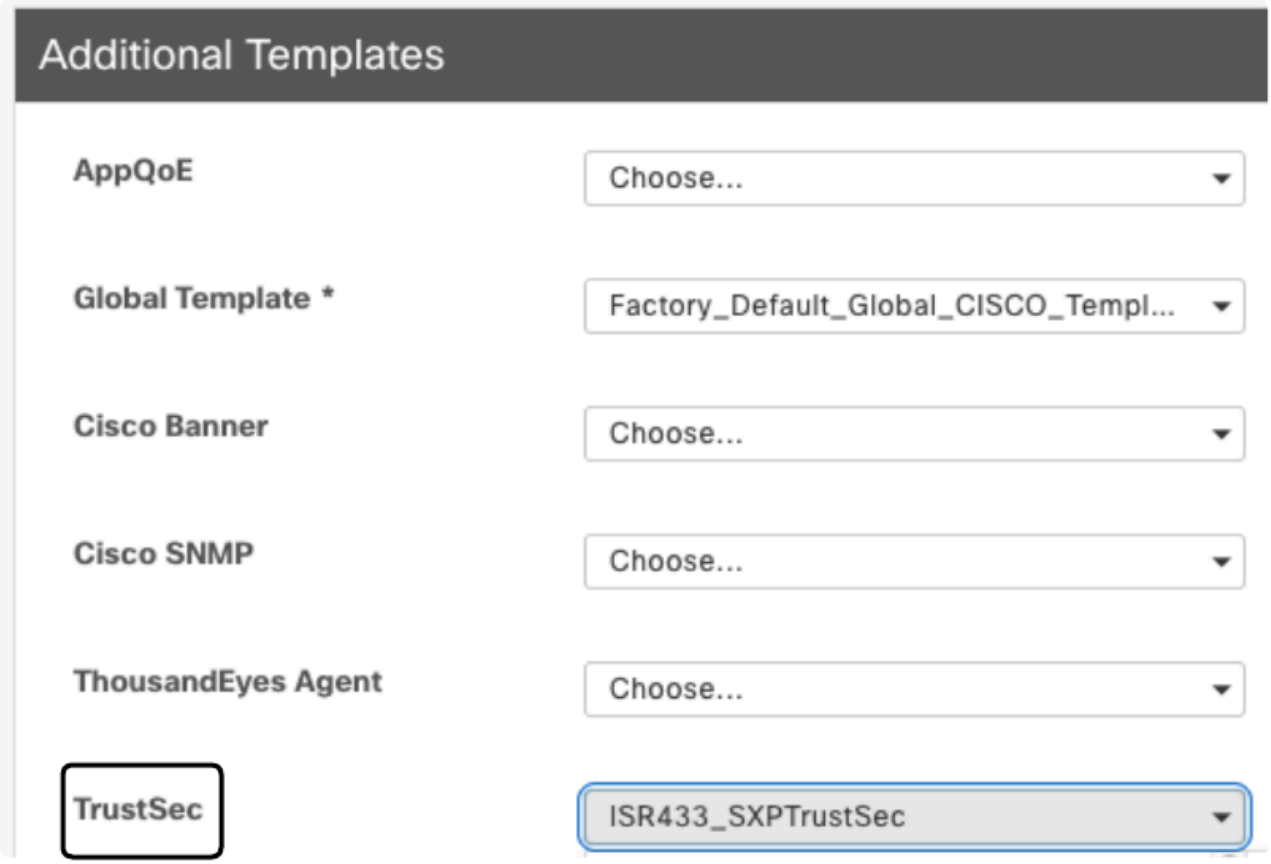


Configurazione connessione SXP

Nota: Cisco ISE ha un limite sul numero di sessioni SXP che può gestire. Pertanto, in alternativa, è possibile utilizzare un riflettore SXP per la rete orizzontale in scala.

Nota: Si consiglia di utilizzare un riflettore SXP per stabilire un peer SXP con i dispositivi Cisco IOS® XE Catalyst SD-WAN.

- Selezionare Configurazione > Modelli > Modello dispositivo > Modelli aggiuntivi > TrustSec.
- Selezionare il modello di funzionalità TrustSec creato in precedenza, quindi fare clic su Salva.



Sezione Modelli aggiuntivi

Verifica

Eseguire il comandoshow cts sxp connections vrf (service vrf)per visualizzare le informazioni sulle connessioni 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

Eseguire il comando **show cts role-based sgt-map** tPer visualizzare la mappa SGT Cisco TrustSec globale tra i binding IP-Address e 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
```

Eseguire il comando **show cts environment-data** per visualizzare i dati globali dell'ambiente 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
```

Eseguire il comandoshow cts pacsper visualizzare la PAC Cisco TrustSec fornita.

<#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

Eseguire il comandoshow cts role-based permissions tPer visualizzare i criteri 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

Eseguire il comando`show cts rbacl (SGACLName)`per visualizzare la configurazione dell'elenco di controllo di accesso (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
```

Informazioni correlate

- Guida alla configurazione della sicurezza di Cisco Catalyst SD-WAN
- Guida alla configurazione di Cisco TrustSec

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).