在SD-WAN中配置TrustSec SGT SXP传播

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- Cisco TrustSec集成
- SGT传播方法
- 使用SXP的SGT传播

启用SGT SXP传播和下载SGACL策略

- 步骤1.配置Radius参数
- 步骤2.配置SXP参数

验证

相关信息

简介

本文档介绍软件定义广域网(SD-WAN)中的安全组标记交换协议(SXP)传播方法配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- 软件定义接入（SD接入）交换矩阵
- 思科身份服务引擎(ISE)

使用的组件

本文档中的信息基于：

- 思科IOS® XE Catalyst SD-WAN Edge版本17.9.5a
- Cisco Catalyst SD-WAN Manager版本20.12.4。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco TrustSec集成

Cisco IOS® XE Catalyst SD-WAN版本17.3.1a及更高版本支持SGT Propagation with Cisco TrustSec Integration。此功能使Cisco IOS® XE Catalyst SD-WAN边缘设备能够将分支中支持Cisco TrustSec的交换机生成的安全组标记(SGT)内联标记传播到Cisco Catalyst SD-WAN网络中的其他边缘设备。

Cisco TrustSec的基本概念：

- SGT绑定：IP与SGT之间的关联，所有绑定都有最常见的配置，并直接从Cisco ISE学习。
- SGT传播：传播方法用于在网络跳之间传播这些SGT。
- SGTACL策略：一组规则，用于指定受信任网络中流量源的权限。
- SGT实施：根据SGT策略实施策略的位置。

SGT传播方法

SGT传播方法如下：

- SGT传播内联标记
- SGT SXP传播

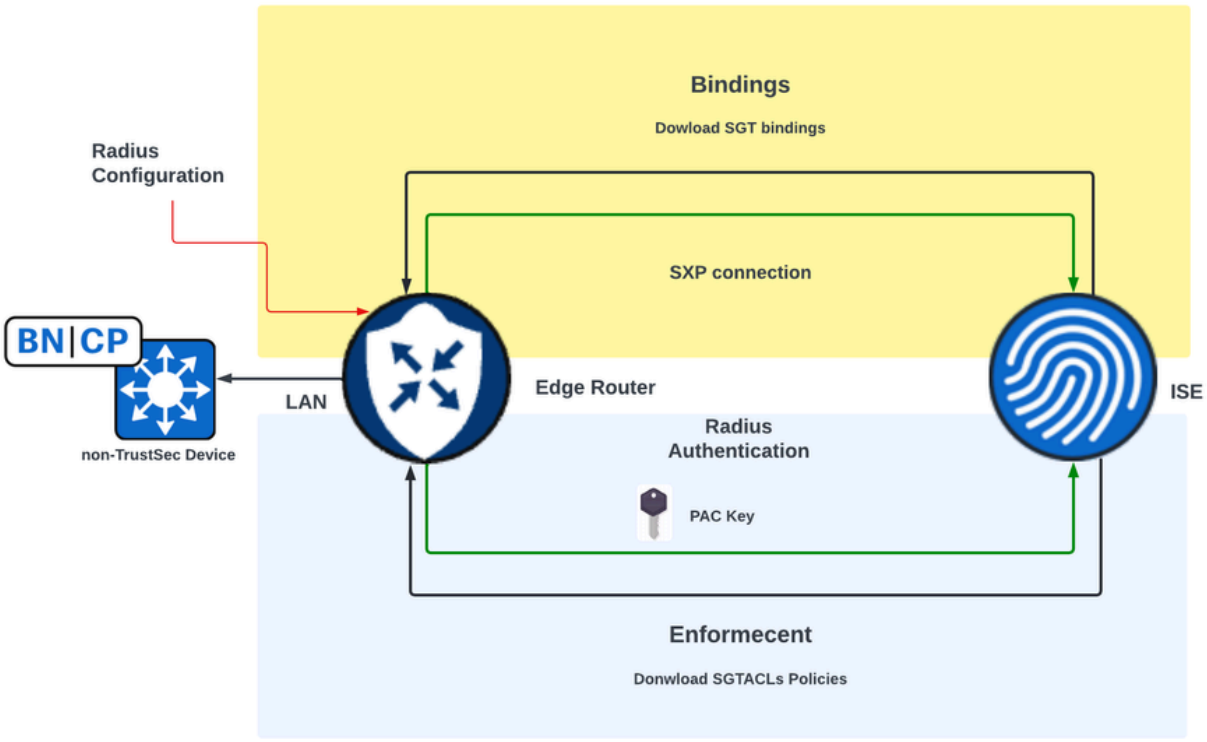
使用SXP的SGT传播

对于内联标记传播，分支机构需要配备支持Cisco TrustSec的交换机，以便处理SGT内联标记（Cisco TrustSec设备）。 如果硬件不支持内联标记，SGT传播使用安全组标记交换协议(SXP)跨网络设备传播SGT。

思科ISE允许创建IP到SGT绑定（动态IP-SGT），然后使用SXP将IP-SGT绑定下载到Cisco IOS® XE Catalyst SD-WAN设备，以通过Cisco Catalyst SD-WAN网络传播SGT。此外，SD-WAN出口上的SGT流量的策略通过从ISE下载SGACL策略实施。

示例：

- 思科交换机（边界节点）不支持内联标记（非TrustSec设备）。
- Cisco ISE允许通过SXP连接下载IP-SGT绑定到Cisco IOS® XE Catalyst SD-WAN设备（边缘路由器）。
- 思科ISE允许通过Radius集成和PAC密钥将SGACL策略下载到 Cisco IOS® XE Catalyst SD-WAN设备（边缘路由器）。

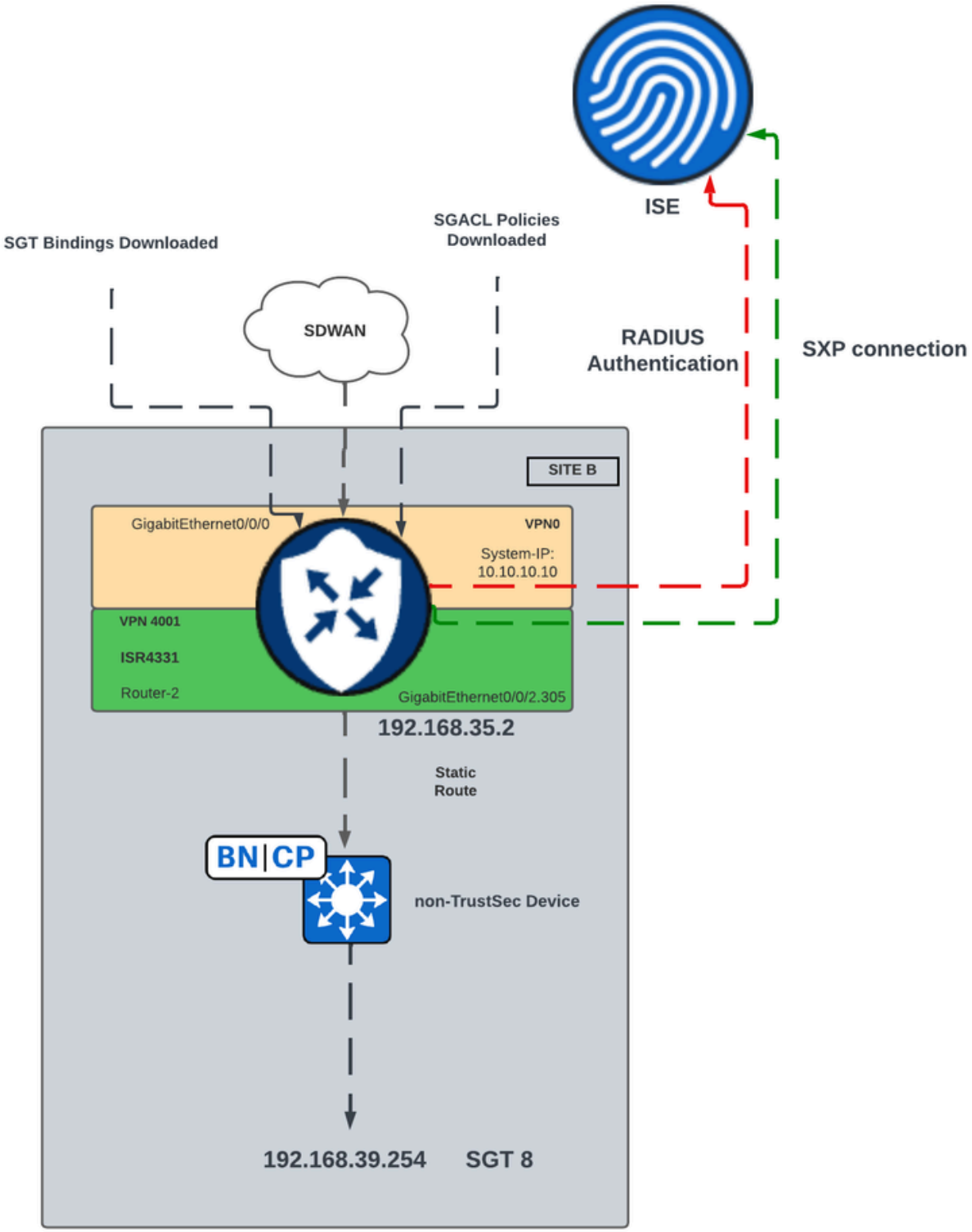


在SD-WAN边缘设备上启用SXP传播和下载SGACL策略的要求

注意： SGACL策略不针对入口流量实施，仅针对Cisco Catalyst SD-WAN网络中的出口流量。

注意：超过24K的SGT策略在控制器模式下不支持Cisco TrustSec功能。

启用SGT SXP传播和下载SGACL策略

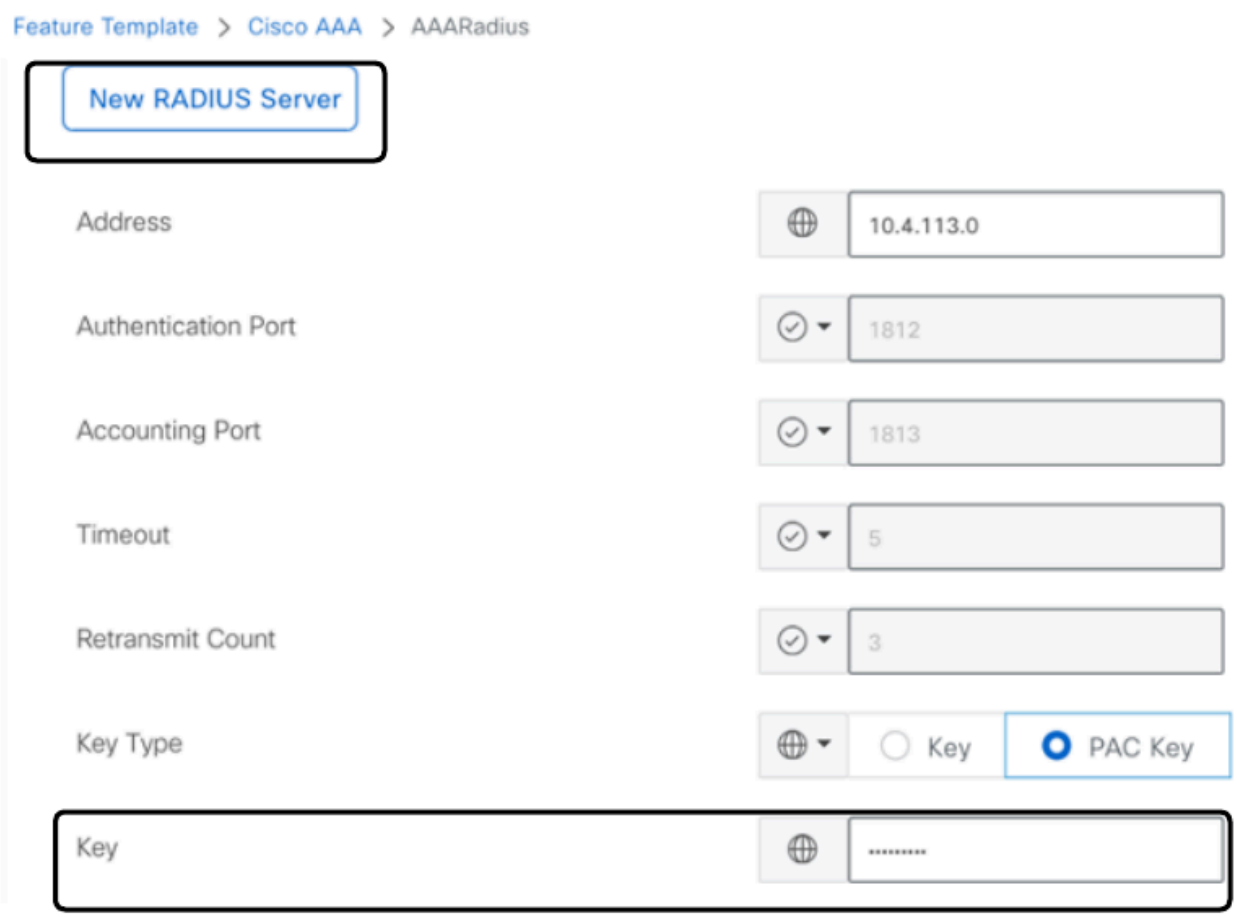


SGT SXP在SD-WAN中传播的网络图

步骤1.配置Radius参数

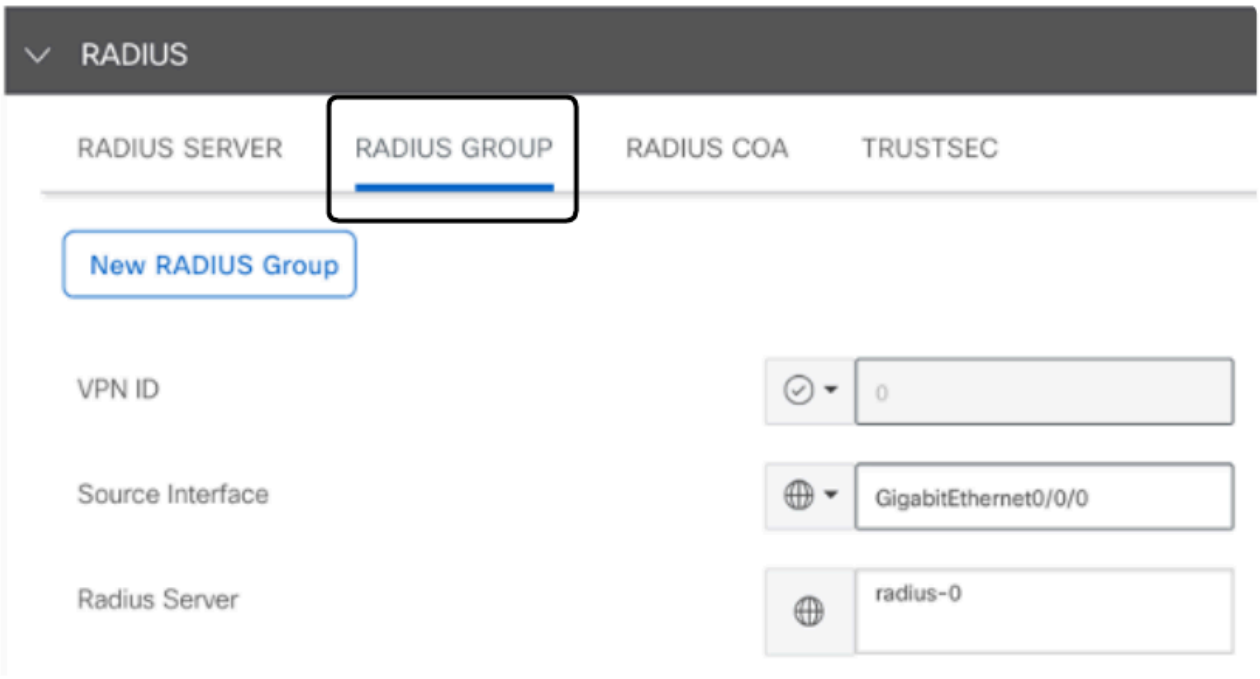
- 登录到Cisco Catalyst SD-WAN Manager GUI。
- 导航到配置>模板>功能模板> Cisco AAA。单击RADIUS SERVER。

- 配置RADIUS SERVER参数和密钥。



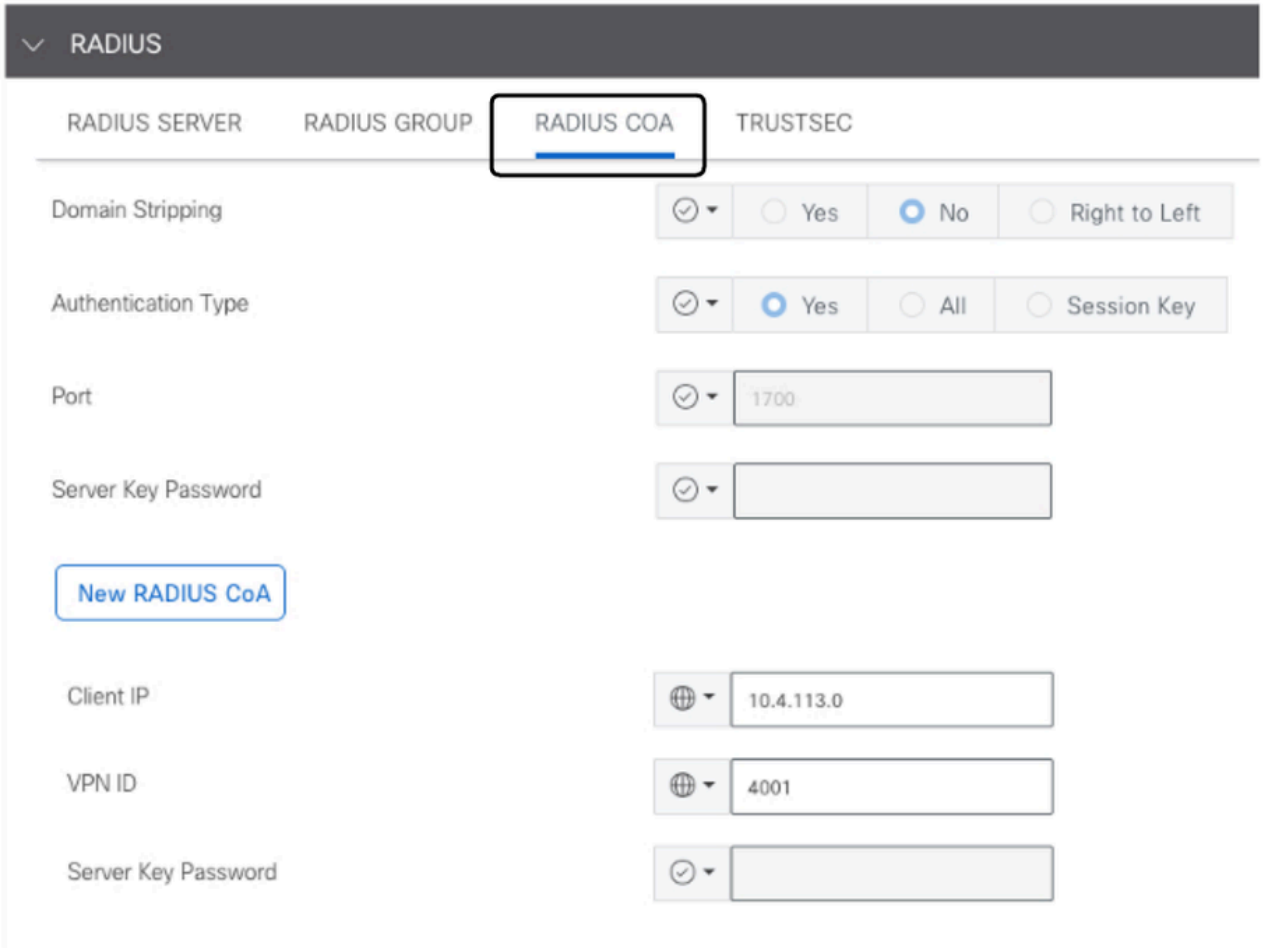
RADIUS 服务器配置

- 输入值以配置Radius Group参数。



RADIUS组配置

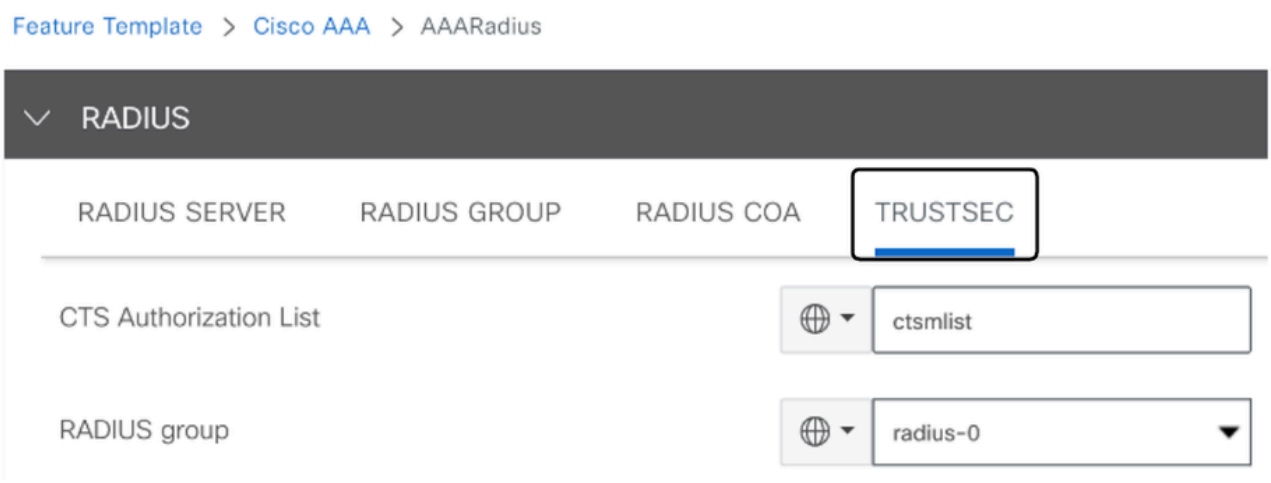
- 输入值以配置Radius COA参数。



RADIUS COA配置

注意：如果未配置Radius COA，则SD-WAN路由器无法自动下载SGACL策略。从ISE创建或修改SGACL策略后，命令cts refresh policy用于下载策略。

- 导航到TRUSTSEC部分并输入值。

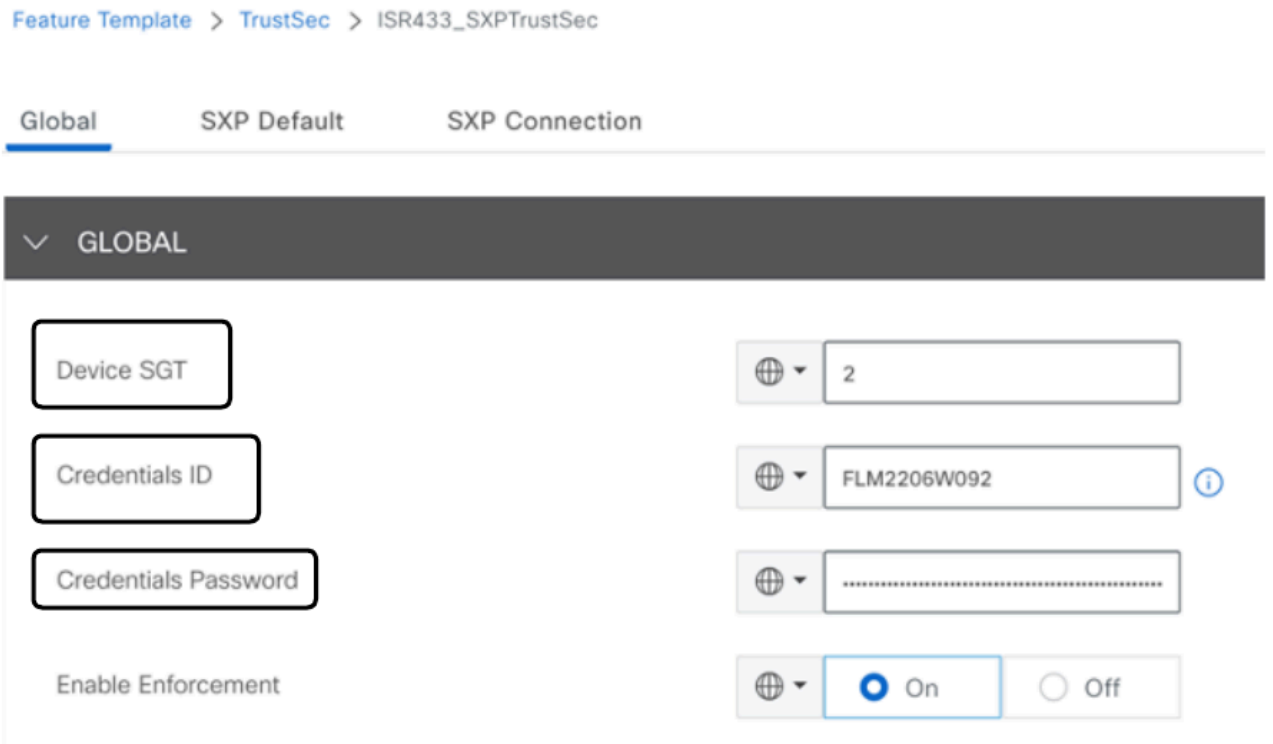


TRUSTSEC配置

- 将Cisco AAA功能模板附加到设备模板。

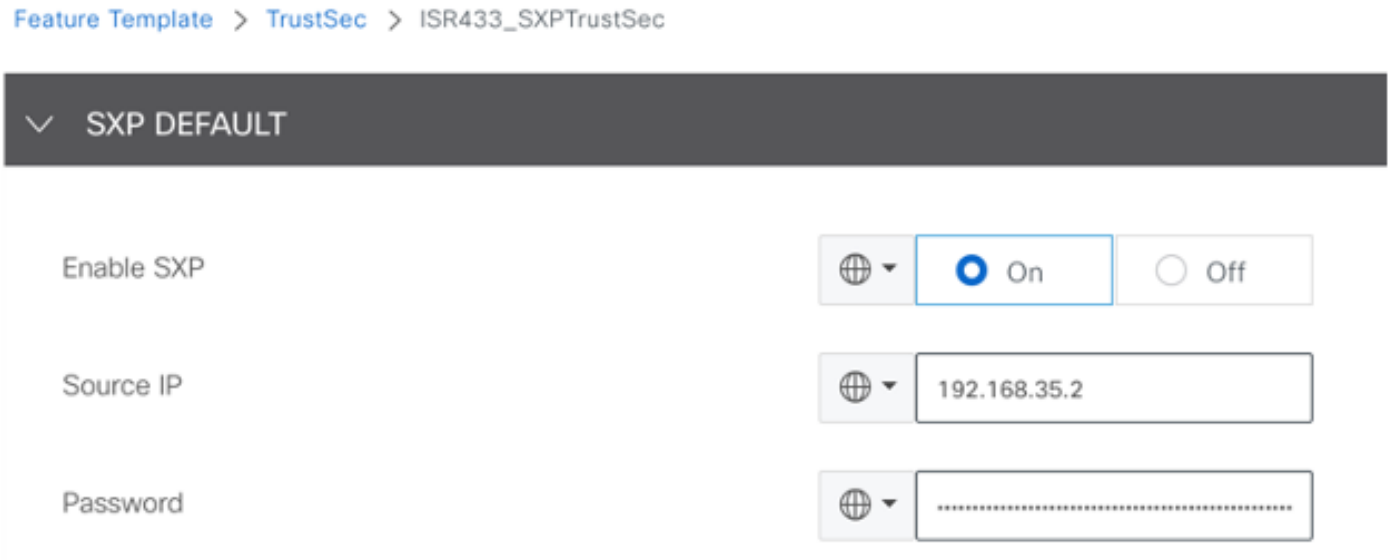
步骤2.配置SXP参数

- 导航到配置>模板>功能模板> TrustSec。
- 配置CTS凭证并将SGT绑定分配给设备接口。



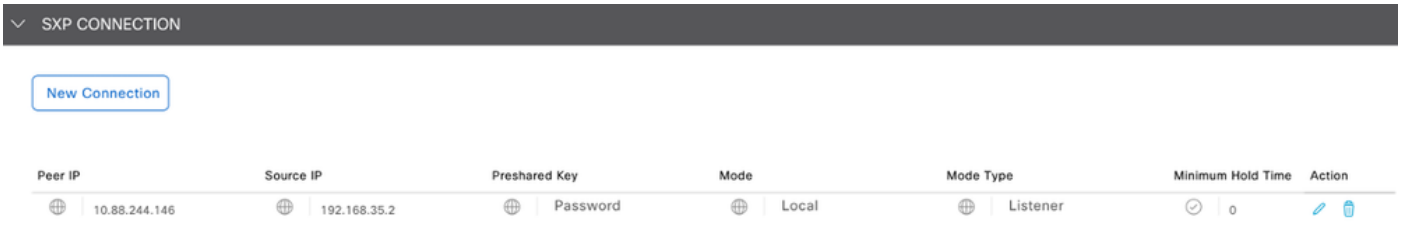
TrustSec功能模板

- 导航到SXP Default部分并输入值以配置SXP Default参数。



SXP默认配置

- 导航到SXP连接并配置SXP连接参数，然后单击保存。

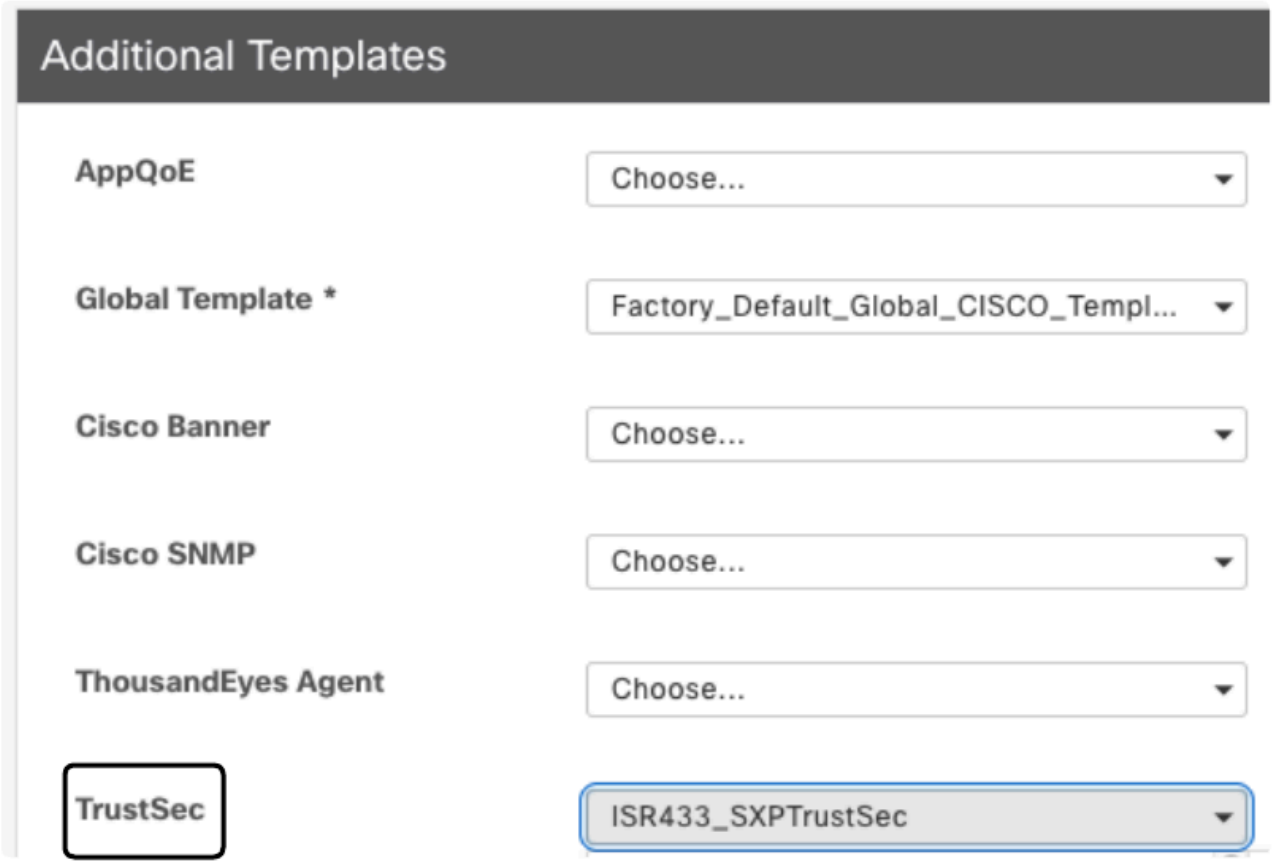


SXP连接配置

注意： 思科ISE对其可以处理的SXP会话数量有限制。因此，作为替代方案，可以使用用于水平扩展网络的SXP反射器。

注意：建议使用SXP反射器与Cisco IOS® XE Catalyst SD-WAN设备建立SXP对等设备。

- 导航到Configuration > Templates > Device Template > Additional Templates > TrustSec。
- 选择之前创建的TrustSec功能模板，然后单击Save。



“附加模板”部分

验证

运行命令show cts sxp connections vrf (service vrf)以显示Cisco TrustSec SXP连接信息。

<#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

运行命令**show cts role-based sgt-map t**显示IP地址和SGT绑定之间的全局Cisco TrustSec SGT映射。

<#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
```

运行命令**show cts environment-data**以显示全局Cisco TrustSec环境数据。

```
<#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

运行命令show cts pacs，以显示调配的Cisco TrustSec PAC。

<#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

运行命令show cts role-based permissions t显示SGACL策略。

<#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
```

运行命令show cts rbacl (SGACLName)以显示访问控制列表(SGACL)配置。

<#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
```

相关信息

- Cisco Catalyst SD-WAN安全配置指南
- Cisco TrustSec配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。