

Configurar a propagação do TrustSec SGT SXP no SD-WAN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Integração do Cisco TrustSec](#)

[Métodos de Propagação SGT](#)

[Propagação SGT com SXP](#)

[Ativar a propagação SGT SXP e baixar políticas SGACL](#)

[Etapa 1. Configurar os parâmetros do raio](#)

[Etapa 2. Configurar os parâmetros do SXP](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração do método de Propagação do Security Group Tag Exchange Protocol (SXP) em Redes de Longa Distância Definidas por Software (SD-WAN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida pelo software Cisco Catalyst (SD-WAN)
- Malha de acesso definido por software (SD-Access)
- Cisco Identify Service Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas em:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Integração do Cisco TrustSec

A propagação de SGT com integração do Cisco TrustSec é suportada pelo Cisco IOS® XE Catalyst SD-WAN versão 17.3.1a e posteriores. Esse recurso permite que os dispositivos de borda Cisco IOS® XE Catalyst SD-WAN propaguem tags em linha Security Group Tag (SGT) que são geradas pelos switches habilitados para Cisco TrustSec nas filiais para outros dispositivos de borda na rede Cisco Catalyst SD-WAN.

Conceitos básicos do Cisco TrustSec:

- Associações SGT: Associação entre IP e SGT, todas as vinculações têm a configuração mais comum e aprendem diretamente com o Cisco ISE.
- Propagação SGT: Os métodos de propagação são usados para propagar esses SGTs entre saltos de rede.
- Políticas SGTACLs: Conjunto de regras que especificam os privilégios de uma fonte de tráfego dentro de uma rede confiável.
- Aplicação de SGT: Onde as políticas são aplicadas, com base na política de SGT.

Métodos de Propagação SGT

Os métodos de propagação de SGT são:

- Marcação em linha de propagação SGT
- Propagação SGT SXP

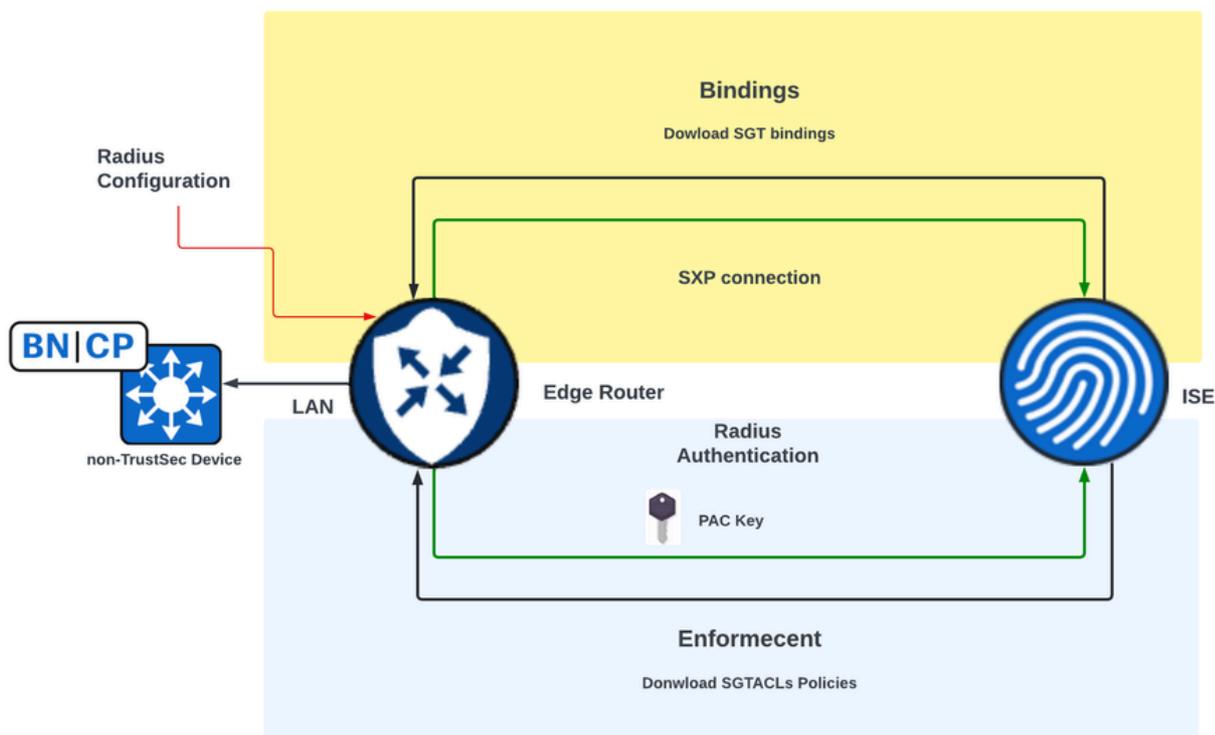
Propagação SGT com SXP

Para a propagação de marcação em linha, as filiais precisam ser equipadas com switches habilitados para Cisco TrustSec que sejam capazes de lidar com marcação em linha SGT (dispositivos Cisco TrustSec). Se o hardware não suportar Inline Tagging, a Propagação SGT usará o Security Group Tag Exchange Protocol (SXP) para propagar SGTs pelos dispositivos de rede.

O Cisco ISE permite a criação de uma Associação IP-para-SGT (IP-SGT Dinâmico) e, em seguida, faz o download da Associação IP-SGT usando o SXP para um dispositivo Cisco IOS® XE Catalyst SD-WAN para propagação do SGT pela rede Cisco Catalyst SD-WAN. Além disso, as políticas para o tráfego SGT na saída de SD-WAN são aplicadas por meio do download de políticas SGACL do ISE.

Exemplo:

- O Switch Cisco (nó de borda) não suporta Marcação em linha (dispositivo não TrustSec).
- O Cisco ISE permite o download da vinculação IP-SGT através da conexão SXP para um dispositivo Cisco IOS® XE Catalyst SD-WAN (roteador de borda).
- O Cisco ISE permite o download de políticas SGACL através da integração Radius e da chave PAC para um Dispositivo Cisco IOS® XE Catalyst SD-WAN (roteador de borda).



Requisitos para ativar a propagação do SXP e fazer o download de políticas SGACL em dispositivos de borda SD-WAN

Note: As políticas SGACL não são aplicadas ao tráfego de entrada, apenas ao tráfego de saída em uma rede Cisco Catalyst SD-WAN.

Observação: o recurso Cisco TrustSec não é suportado por mais de 24K políticas SGT no modo de controlador.

Ativar a propagação SGT SXP e baixar políticas SGACL

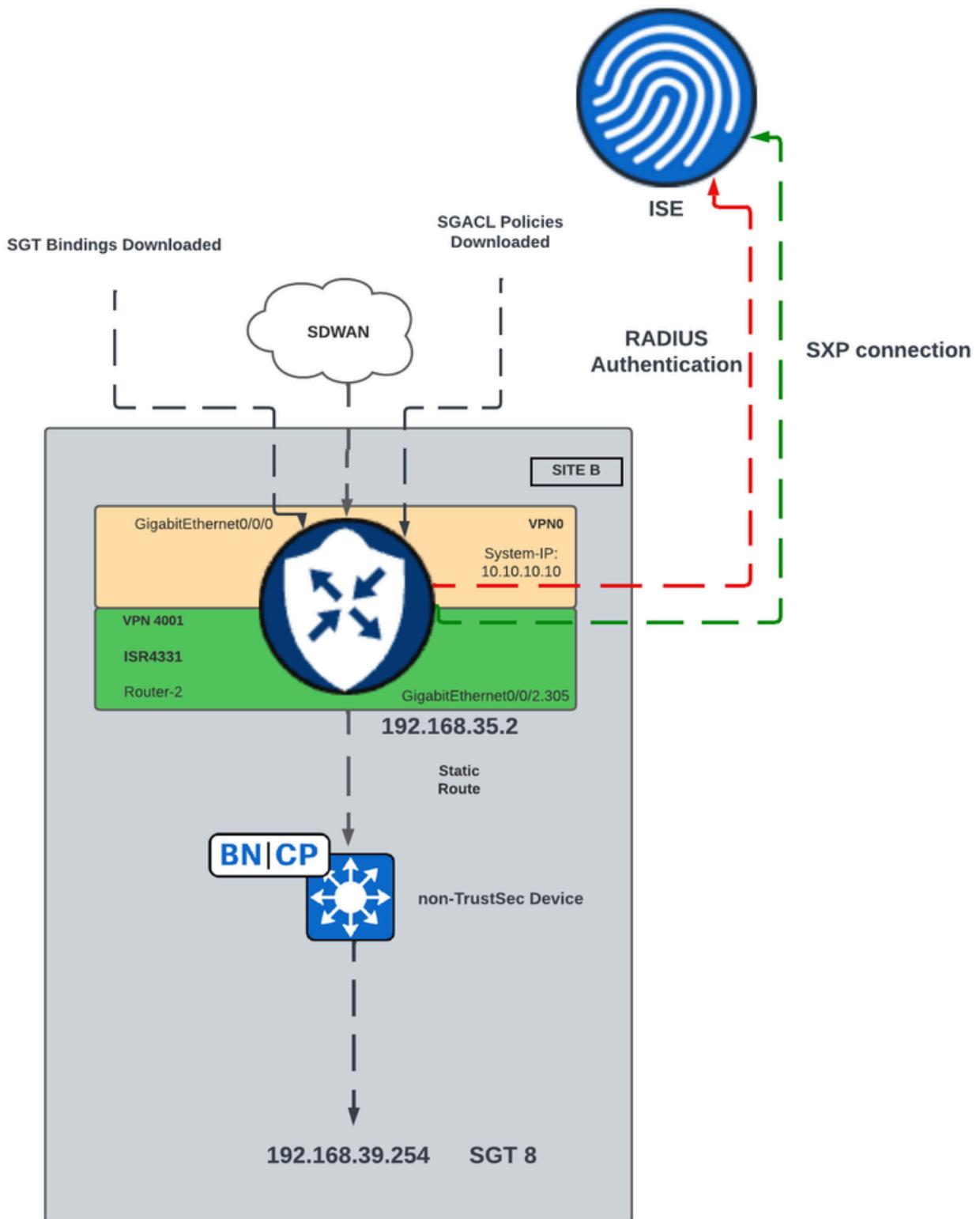


Diagrama de Rede para Propagação SGT SXP em SD-WAN

Etapa 1. Configurar os parâmetros do raio

- Faça login na GUI do Cisco Catalyst SD-WAN Manager.
- Navegue para Configuration > Templates > Feature Template > Cisco AAA. Clique em

RADIUS SERVER.

- Configure os parâmetros RADIUS SERVER e a chave.

Feature Template > Cisco AAA > AAARadius

New RADIUS Server

Address



10.4.113.0

Authentication Port



1812

Accounting Port



1813

Timeout



5

Retransmit Count



3

Key Type



Key

PAC Key

Key



Configuração de servidor RADIUS

- Insira os valores para configurar os parâmetros do Grupo Radius.

▼ RADIUS

RADIUS SERVER **RADIUS GROUP** RADIUS COA TRUSTSEC

[New RADIUS Group](#)

VPN ID

Source Interface

Radius Server

Configuração do grupo RADIUS

- Insira os valores para configurar os parâmetros do COA Radius.

▼ RADIUS

RADIUS SERVER RADIUS GROUP **RADIUS COA** TRUSTSEC

Domain Stripping Yes No Right to Left

Authentication Type Yes All Session Key

Port

Server Key Password

[New RADIUS CoA](#)

Client IP

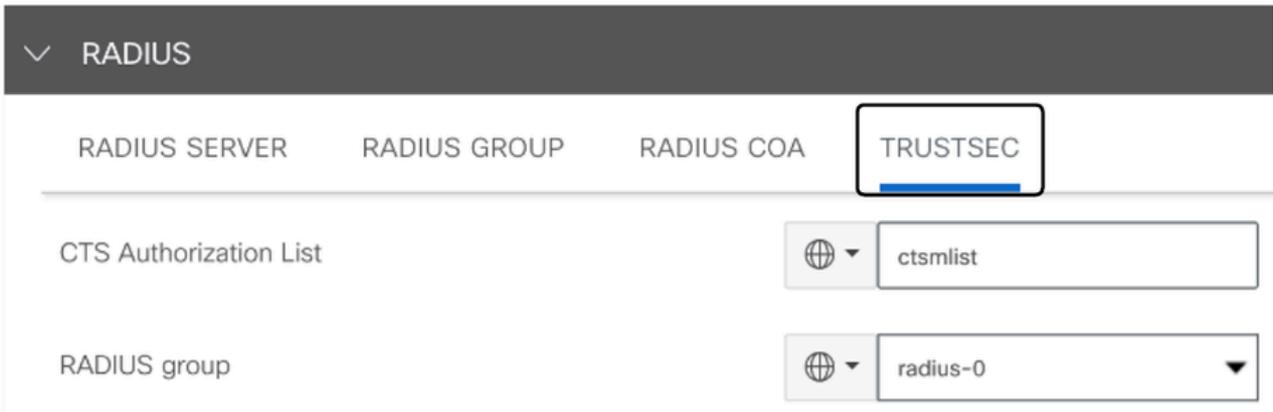
VPN ID

Server Key Password

 **Note:** Se o COA Radius não estiver configurado, o roteador SD-WAN não poderá fazer download das políticas SGACL automaticamente. Depois de criar ou modificar uma política SGACL do ISE, o comando `cts refresh policy` é usado para baixar as políticas.

- Navegue até a seção TRUSTSEC e insira os valores.

[Feature Template](#) > [Cisco AAA](#) > [AAARadius](#)



RADIUS			
RADIUS SERVER	RADIUS GROUP	RADIUS COA	TRUSTSEC
CTS Authorization List			ctsmlist
RADIUS group			radius-0

Configuração do TRUSTSEC

- Anexe o modelo de recurso Cisco AAA ao modelo do dispositivo.

Etapa 2. Configurar os parâmetros do SXP

- Navegue até `Configuration > Templates > Feature Template > TrustSec`.
- Configure as credenciais CTS e atribua uma Ligação SGT às interfaces do dispositivo.

GLOBAL

Device SGT	<input type="text" value="2"/>
Credentials ID	<input type="text" value="FLM2206W092"/> ⓘ
Credentials Password	<input type="password" value="....."/>
Enable Enforcement	<input checked="" type="radio"/> On <input type="radio"/> Off

Modelo de recurso TrustSec

- Navegue até a seção SXP Default e insira os valores para configurar os parâmetros SXP Default.

SXP DEFAULT

Enable SXP	<input checked="" type="radio"/> On <input type="radio"/> Off
Source IP	<input type="text" value="192.168.35.2"/>
Password	<input type="password" value="....."/>

Configuração padrão do SXP

- Navegue até Conexão SXP e configure os parâmetros Conexão SXP e clique em Salvar.

✓ SXP CONNECTION

New Connection

Peer IP	Source IP	Preshared Key	Mode	Mode Type	Minimum Hold Time	Action
10.88.244.146	192.168.35.2	Password	Local	Listener	0	 

Configuração da conexão SXP

 Note: O Cisco ISE tem um limite no número de sessões SXP que ele pode tratar. Portanto, como alternativa, um refletor SXP para rede horizontal em escala poderia ser usado.

 Note: É recomendável usar um refletor SXP para estabelecer um peer SXP com os dispositivos Cisco IOS® XE Catalyst SD-WAN.

- Navegue até Configuration > Templates > Device Template > Additional Templates > TrustSec.
- Selecione o modelo de recurso TrustSec criado anteriormente e clique em Salvar.

Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
ThousandEyes Agent	Choose...
TrustSec	ISR433_SXPTrustSec

Seção Modelos Adicionais

Verificar

Execute o comando `show cts sxp connections vrf (service vrf)` para exibir as informações de conexões do 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
```

Execute o comando `show cts role-based sgt-map t` para exibir o mapa SGT global do Cisco TrustSec entre o endereço IP e as vinculações 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 through 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

Execute o comando `show cts environment-data` para exibir os dados globais do 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

Execute o comando `show cts pacs` para exibir a PAC do Cisco TrustSec fornecida.

```
<#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
```

Execute o comando `show cts role-based permissions` para exibir as Políticas 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
```

Execute o comando `show cts rbacl (SGACLName)` para exibir a configuração da lista de controle de acesso (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
```

Informações Relacionadas

- [Guia de configuração de segurança do Cisco Catalyst SD-WAN](#)
- [Guia de configuração do Cisco TrustSec](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.