

# SD-WANでのTrustSec SGT SXP伝播の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Cisco TrustSecの統合](#)

[SGTの伝播方法](#)

[SXPを使用したSGT伝播](#)

[SGT SXP伝播の有効化とSGACLポリシーのダウンロード](#)

[ステップ 1: RADIUSパラメータの設定](#)

[ステップ 2: SXPパラメータの設定](#)

[確認](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、ソフトウェア定義ワイドエリアネットワーク(SD-WAN)でのSecurity Group Tag Exchange Protocol(SXP)の伝播方式の設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalystソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- ソフトウェア定義型アクセス ( SDアクセス ) ファブリック
- Cisco Identify Service Engine(ISE)

### 使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco IOS® XE Catalyst SD-WAN Edgesバージョン17.9.5a
- Cisco Catalyst SD-WAN Managerバージョン20.12.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### Cisco TrustSecの統合

Cisco TrustSec統合を使用したSGT伝播は、Cisco IOS® XE Catalyst SD-WANリリース17.3.1a以降でサポートされています。この機能により、Cisco IOS® XE Catalyst SD-WANエッジデバイスは、ブランチ内のCisco TrustSec対応スイッチによって生成されたセキュリティグループタグ (SGT)インラインタグを、Cisco Catalyst SD-WANネットワーク内の他のエッジデバイスに伝播できます。

Cisco TrustSecの基本概念：

- SGTバインディング：IPとSGT間のアソシエーション。すべてのバインディングは最も一般的な設定を持ち、Cisco ISEから直接学習する
- SGT伝播：これらのSGTをネットワークホップ間で伝播するために、伝播方法が使用されます。
- SGTACLポリシー：信頼ネットワーク内のトラフィックソースの権限を指定するルールのセット。
- SGT適用：SGTポリシーに基づいてポリシーが適用される場所。

### SGTの伝播方法

SGTの伝播方法は次のとおりです。

- SGT伝播インラインタギング
- SGT SXP伝播

### SXPを使用したSGT伝播

インラインタギングの伝播では、SGTインラインタギングを処理できるCisco TrustSec対応スイッチ (Cisco TrustSecデバイス) をブランチに装備する必要があります。ハードウェアがインラインタギングをサポートしていない場合、SGT伝播ではSecurity Group Tag Exchange Protocol(SXP)を使用してネットワークデバイス全体にSGTを伝播します。

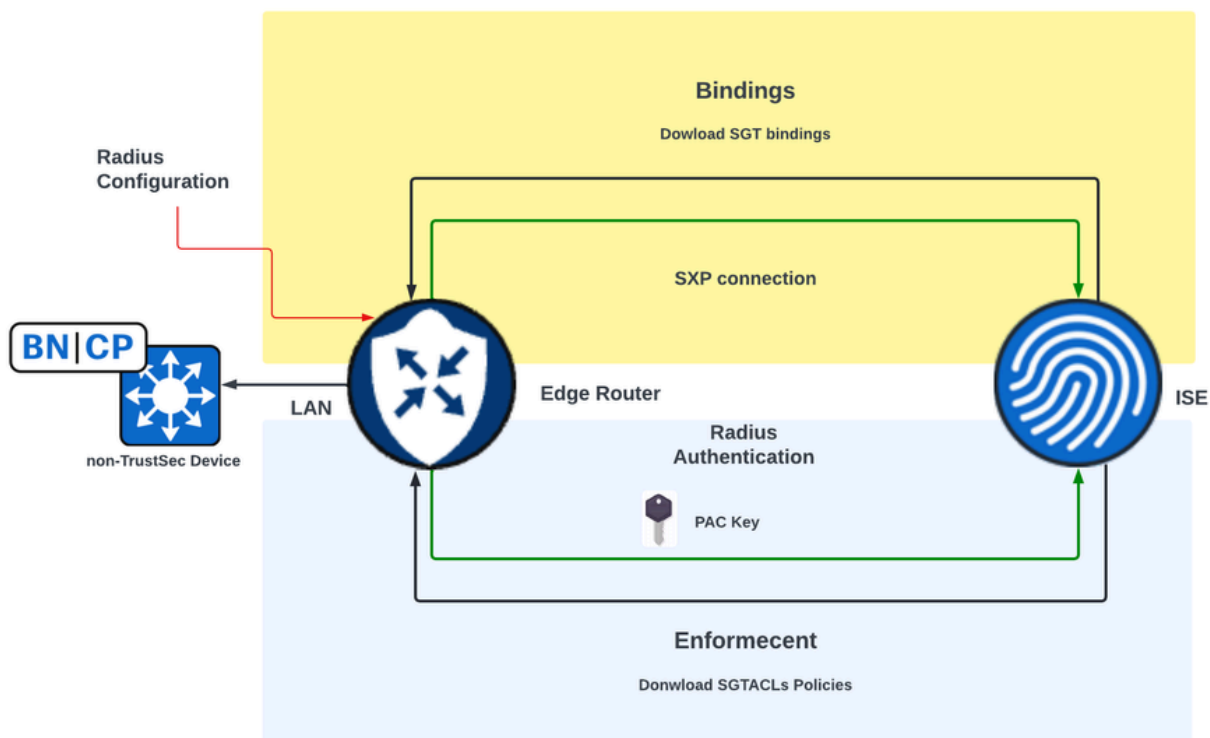
Cisco ISEでは、IP-to-SGTバインディング (ダイナミックIP-SGT) を作成してから、SXPを使用してIP-SGTバインディングをCisco IOS® XE Catalyst SD-WANデバイスにダウンロードし、Cisco Catalyst SD-WANネットワークを介してSGTを伝搬します。また、SD-WAN出力のSGTトラフィックのポリシーは、ISEからSGACLポリシーをダウンロードすることで適用されます。

例：

- Ciscoスイッチ (ポーターノード) は、インラインタギング (TrustSec以外のデバイス) をサポートしていません。
- Cisco ISEでは、SXP接続を使用してCisco IOS® XE Catalyst SD-WANデバイス (エッジル

ータ)にIP-SGTバインディングをダウンロードできます。

- Cisco ISEでは、RADIUS統合およびPACキーを使用して、Cisco IOS® XE Catalyst SD-WANデバイス(エッジルータ)

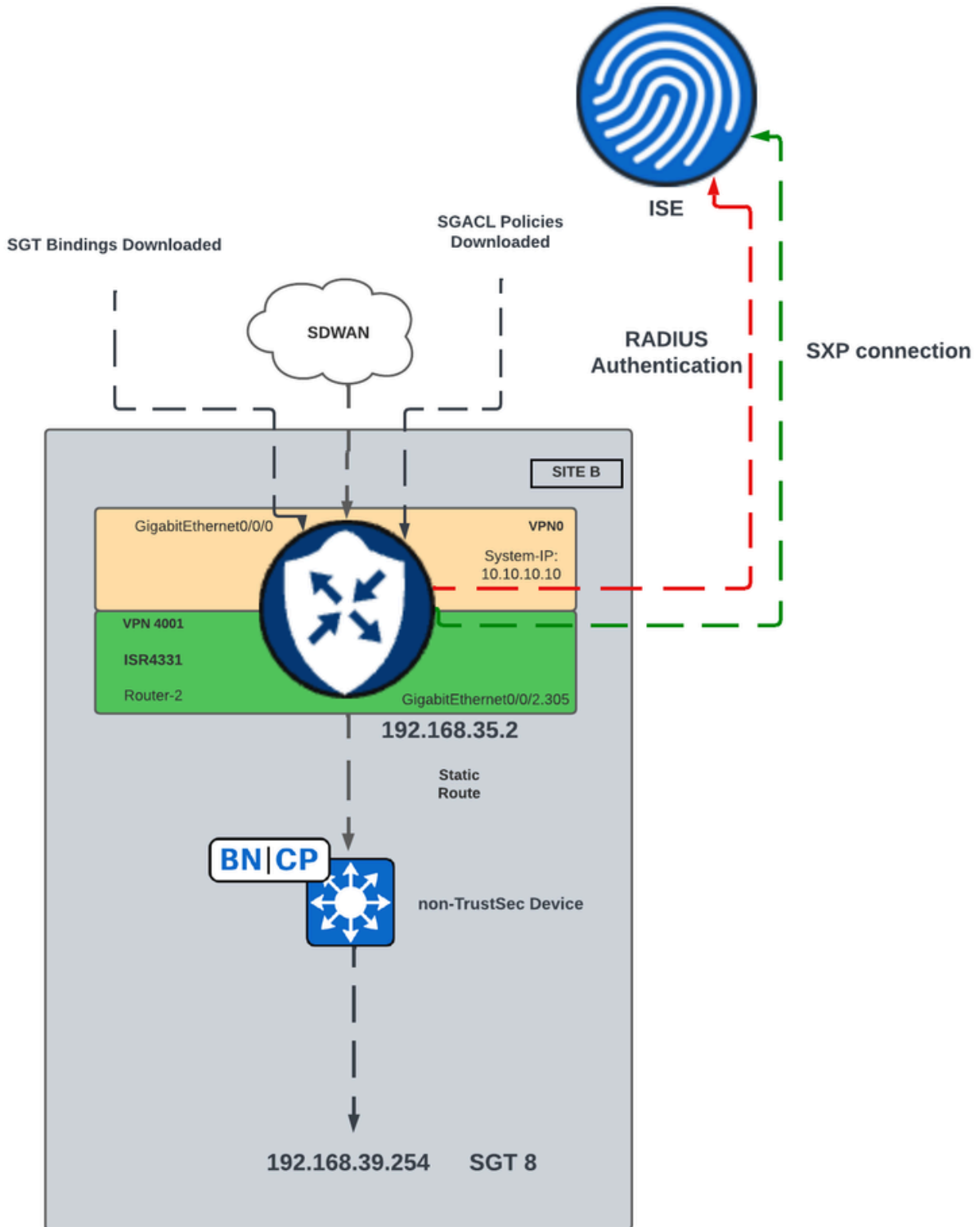


SD-WANエッジデバイスでSXP伝播とダウンロードSGACLポリシーを有効にするための要件

✎ 注:SGACLポリシーは入カトラフィックには適用されず、Cisco Catalyst SD-WANネットワークの出カトラフィックにのみ適用されます。

✎ 注 : Cisco TrustSec機能は、コントローラモードで24Kを超えるSGTポリシーではサポートされません。

## SGT SXP伝播の有効化とSGACLポリシーのダウンロード



SD-WANでのSGT SXP伝播のネットワーク図

## ステップ 1 : RADIUSパラメータの設定

- Cisco Catalyst SD-WAN ManagerのGUIにログインします。
- Configuration > Templates > Feature Template > Cisco AAAの順に移動します。 RADIUS

SERVERをクリックします。

- RADIUSサーバのパラメータとキーを設定します。

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



.....

RADIUS サーバの設定

- 値を入力して、RADIUSグループのパラメータを設定します。

▼ RADIUS

RADIUS SERVER   **RADIUS GROUP**   RADIUS COA   TRUSTSEC

[New RADIUS Group](#)

VPN ID  0

Source Interface  GigabitEthernet0/0/0

Radius Server  radius-0

RADIUSグループの設定

- 値を入力して、Radius COAパラメータを設定します。

▼ RADIUS

RADIUS SERVER   RADIUS GROUP   **RADIUS COA**   TRUSTSEC

Domain Stripping   Yes  No  Right to Left

Authentication Type   Yes  All  Session Key

Port  1700


Server Key Password

[New RADIUS CoA](#)

Client IP  10.4.113.0

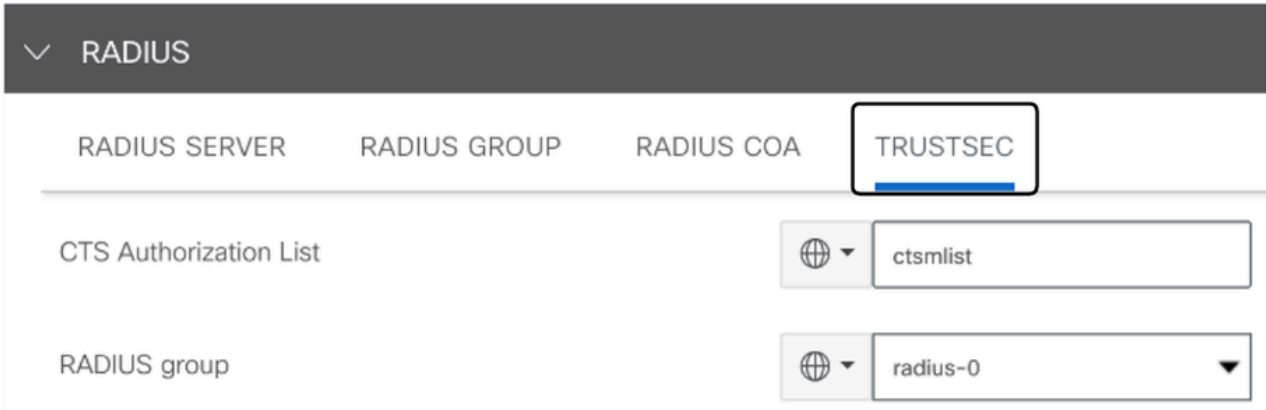
VPN ID  4001

Server Key Password

 注:Radius COAが設定されていない場合、SD-WANルータはSGACLポリシーを自動的にダウンロードできません。ISEからSGACLポリシーを作成または変更した後、ポリシーをダウンロードするには、コマンドcts refresh policyを使用します。


- TRUSTSECセクションに移動し、値を入力します。


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



▼ RADIUS

RADIUS SERVER    RADIUS GROUP    RADIUS COA    **TRUSTSEC**

CTS Authorization List     ▼    ctsmlist

RADIUS group     ▼    radius-0 ▼

#### TRUSTSECの設定

- Cisco AAA機能テンプレートをデバイステンプレートに添付します。

#### ステップ 2 : SXPパラメータの設定

- Configuration > Templates > Feature Template > TrustSecの順に移動します。
- CTSクレデンシャルを設定し、SGTバインディングをデバイスインターフェイスに割り当てます。

GLOBAL

Device SGT

Credentials ID

ⓘ

Credentials Password

Enable Enforcement

On  Off

TrustSec機能テンプレート

- SXP Defaultセクションに移動し、値を入力してSXP Defaultパラメータを設定します。

SXP DEFAULT

Enable SXP

On  Off

Source IP

Password

SXPのデフォルト設定

- SXP Connectionに移動し、SXP Connectionパラメータを設定してから、Saveをクリックします。





## ▼ 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	 

### SXP接続設定

 注: Cisco ISEでは、処理できるSXPセッションの数に制限があります。そのため、代わりにスケールネットワーク水平用のSXPリフレクタを使用できます。

 注: Cisco IOS® XE Catalyst SD-WANデバイスでSXPピアを確立するには、SXPリフレクタを使用することをお勧めします。

- Configuration > Templates > Device Template > Additional Templates > TrustSecの順に移動します。
- 以前に作成したTrustSec機能テンプレートを選択し、Saveをクリックします。

### Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
ThousandEyes Agent	Choose...
<b>TrustSec</b>	<b>ISR433_SXPTrustSec</b>

Additional Templatesセクション

## 確認

```
show cts sxp connections vrf (service
```

vrf)コマンドを実行して、Cisco TrustSec SXPの接続情報を表示します。

```
<#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
```

show cts role-based sgt-map tコマンドを実行します。o IPアドレスバインディングとSGTバインディング間のグローバルCisco TrustSec SGTマップを表示します。

<#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

show cts environment-data コマンドを実行して、グローバルCisco TrustSec環境データを表示します。

<#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

show cts pacs コマンドを実行して、プロビジョニングされたCisco TrustSec PACを表示します。

```
<#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
```

コマンド show cts role-based permissions を実行します。o SGACLポリシーの表示

```
<#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
```

show cts rbacl (SGACLName)コマンドを実行して、アクセスコントロールリスト(SGACL)設定を表示します。

```
<#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
```

## 関連情報

- [Cisco Catalyst SD-WANセキュリティ設定ガイド](#)
- [Cisco TrustSec設定ガイド](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。