

配置SD-WAN中的TrustSec SGT SXP傳播

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[Cisco TrustSec整合](#)

[SGT傳播方法](#)

[使用SXP的SGT傳播](#)

[啟用SGT SXP傳播並下載SGACL策略](#)

[步驟1.設定Radius引數](#)

[步驟2.配置SXP引數](#)

[驗證](#)

[相關資訊](#)

簡介

本檔案介紹軟體定義廣域網(SD-WAN)中的安全群組標籤交換通訊協定(SXP)傳播方法組態。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- 軟體定義存取(SD-Access)光纖
- 思科識別服務引擎(ISE)

採用元件

本檔案中的資訊是根據：

- Cisco IOS® XE Catalyst SD-WAN邊緣版本17.9.5a
- Cisco Catalyst SD-WAN管理器版本20.12.4。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco TrustSec整合

Cisco IOS® XE Catalyst SD-WAN版本17.3.1a及更高版本支援與Cisco TrustSec整合的SGT傳播。此功能使Cisco IOS® XE Catalyst SD-WAN邊緣裝置可以將分支機構中啟用Cisco TrustSec的交換機生成的安全組標籤(SGT)內聯標籤傳播到Cisco Catalyst SD-WAN網路中的其他邊緣裝置。

Cisco TrustSec的基本概念：

- SGT繫結：IP與SGT之間的關聯，所有繫結都有最常見的配置，並直接從思科ISE學習。
- SGT傳播：傳播方法用於在網路跳之間傳播這些SGT。
- SGTACL策略：一組規則，用於指定受信任網路中流量源的許可權。
- SGT實施：根據SGT策略實施策略的位置。

SGT傳播方法

SGT傳播方法有：

- SGT傳播內嵌標籤
- SGT SXP傳播

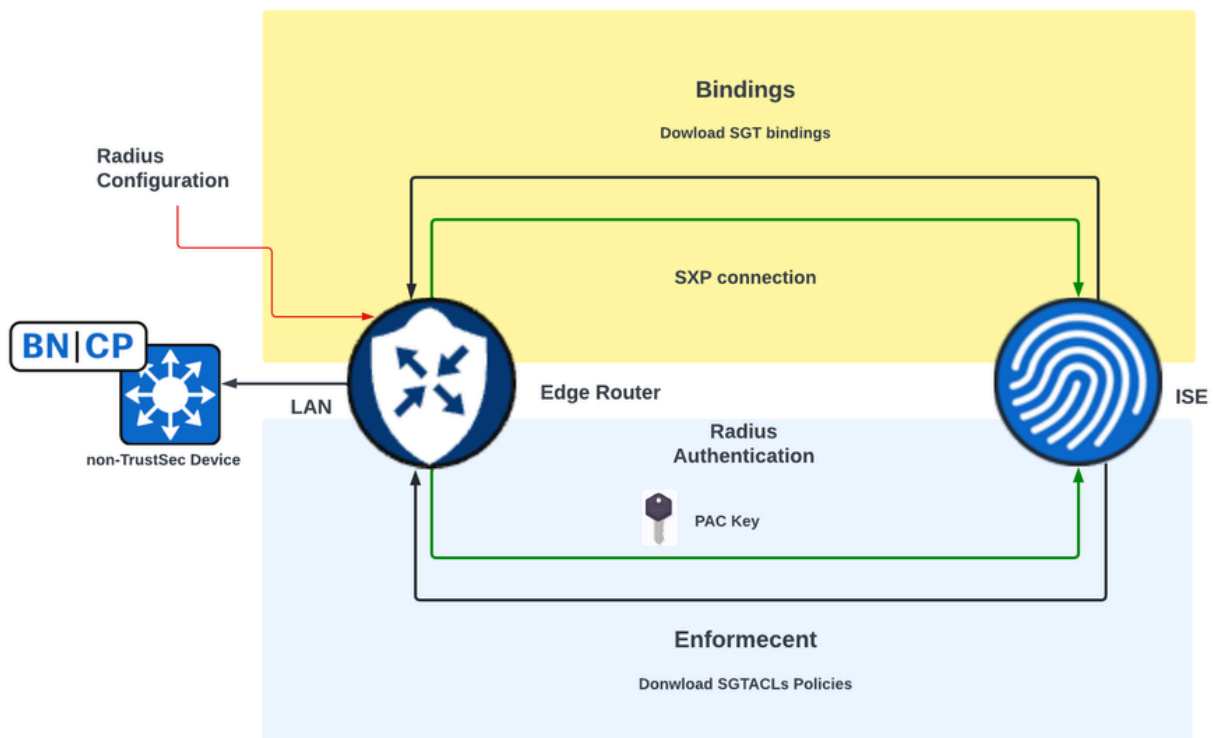
使用SXP的SGT傳播

對於內聯標籤傳播，分支機構需要配備支援Cisco TrustSec且能夠處理SGT內聯標籤的交換機（Cisco TrustSec裝置）。如果硬體不支援內聯標籤，則SGT傳播使用安全組標籤交換協定(SXP)在網路裝置上傳播SGT。


Cisco ISE允許建立IP到SGT繫結（動態IP-SGT），然後使用SXP將IP-SGT繫結下載到Cisco IOS® XE Catalyst SD-WAN設備，以便通過Cisco Catalyst SD-WAN網路傳播SGT。此外，通過從ISE下載SGACL策略，在SD-WAN出口上實施SGT流量的策略。

範例：

- 思科交換機（邊界節點）不支援內聯標籤（非TrustSec裝置）。
- Cisco ISE允許通過SXP連線下載IP-SGT繫結到Cisco IOS® XE Catalyst SD-WAN裝置（邊緣路由器）。
- 思科ISE允許通過Radius整合和PAC金鑰將SGACL策略下載到Cisco IOS® XE Catalyst SD-WAN裝置（邊緣路由器）。

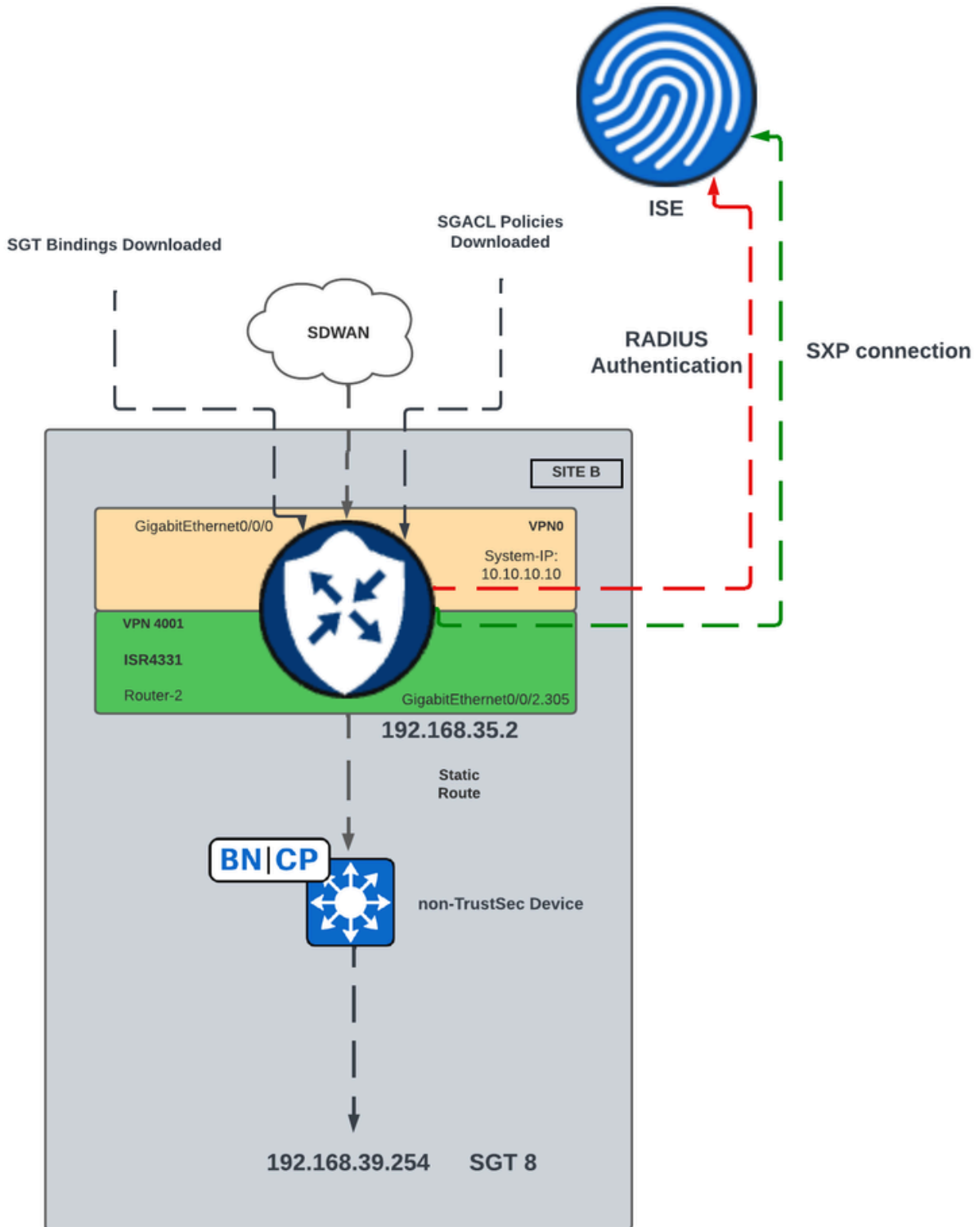


在SD-WAN邊緣裝置上啟用SXP傳播和下載SGACL策略的要求

 附註： SGACL策略不強制用於入口流量，只強制用於Cisco Catalyst SD-WAN網路中的出口流量。

 注意：在控制器模式下，超過24K SGT策略不支援Cisco TrustSec功能。

啟用SGT SXP傳播並下載SGACL策略



SGT SXP在SD-WAN中傳播的網路圖

步驟1.設定Radius引數

- 登入到Cisco Catalyst SD-WAN Manager GUI。
- 導航到Configuration > Templates > Feature Template > Cisco AAA。單擊RADIUS

SERVER。

- 設定RADIUS SERVER參數和金鑰。

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伺服器配置

- 輸入值以配置Radius Group引數。

RADIUS SERVER **RADIUS GROUP** RADIUS COA TRUSTSEC

[New RADIUS Group](#)

VPN ID

Source Interface

Radius Server

RADIUS群組組態

- 輸入值以配置Radius COA引數。

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

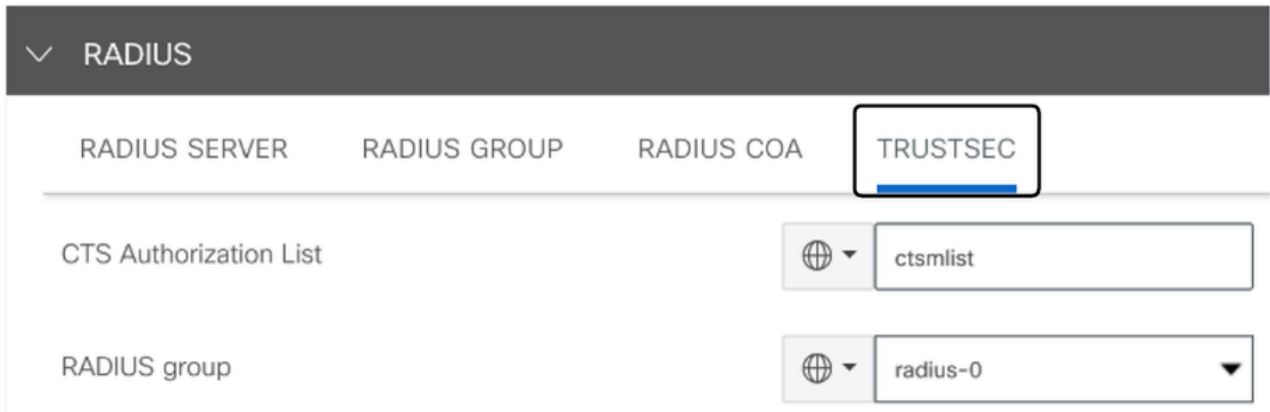
VPN ID

Server Key Password

 附註：如果未配置Radius COA，則SD-WAN路由器無法自動下載SGACL策略。從ISE建立或修改SGACL策略後，命令cts refresh policy用於下載策略。

- 導航到TRUSTSEC部分並輸入值。


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




Feature Template > Cisco AAA > AAARadius

▼ RADIUS

RADIUS SERVER RADIUS GROUP RADIUS COA **TRUSTSEC**

CTS Authorization List  ctsmlist

RADIUS group  radius-0 ▼

TRUSTSEC配置

- 將Cisco AAA功能模板附加到裝置模板。

步驟2. 配置SXP引數

- 導覽至Configuration > Templates > Feature Template > TrustSec。
- 配置CTS憑證並將SGT繫結分配給裝置介面。

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

TrustSec功能模板

- 導航到SXP Default部分並輸入值以配置SXP Default引數。

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="....."/>


SXP預設配置

- 導航到SXP Connection並配置SXP Connection引數，然後按一下Save。

SXP CONNECTION

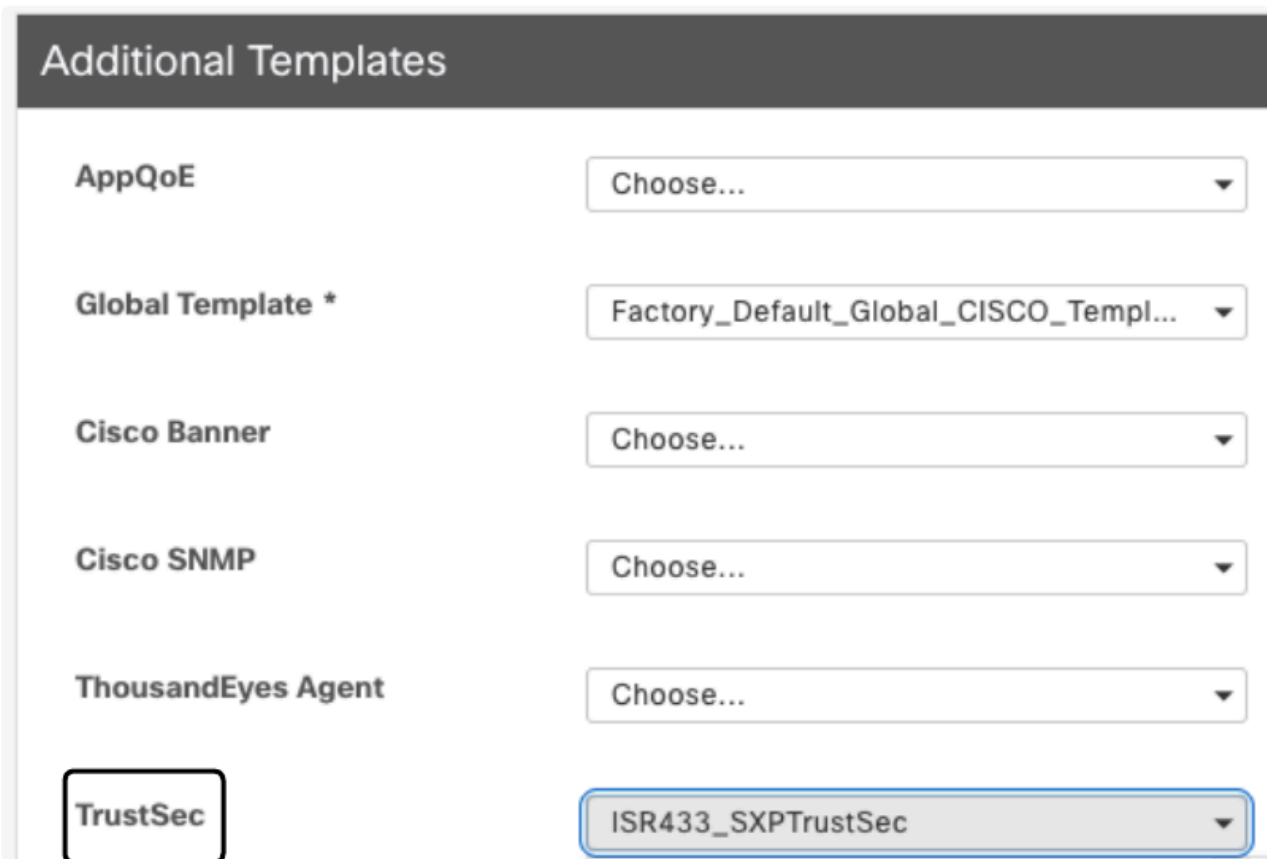
[New Connection](#)

Peer IP	Source IP	Preshared Key	Mode	Mode Type	Minimum Hold Time	Action
<input type="text" value="10.88.244.146"/>	<input type="text" value="192.168.35.2"/>	<input type="text" value="Password"/>	<input type="text" value="Local"/>	<input type="text" value="Listener"/>	<input type="text" value="0"/>	<input type="button" value="edit"/> <input type="button" value="delete"/>

 附註：思科ISE對其可以處理的SXP會話數量有限制。因此，作為替代方案，可以使用用於水準擴展網路的SXP反射器。

 附註：建議使用SXP反射器與Cisco IOS® XE Catalyst SD-WAN裝置建立SXP對等裝置。

- 導航到Configuration > Templates > Device Template > Additional Templates > TrustSec。
- 選擇先前建立的TrustSec功能模板，然後按一下Save。



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

「其他模板」部分

驗證

運行命令 `show cts sxp connections vrf (service vrf)` 以顯示Cisco TrustSec SXP連線資訊。

```
<#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
```

運行命令 `show cts role-based sgt-map` 顯示IP地址和SGT繫結之間的全域性Cisco TrustSec SGT對映。

```
<#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

運行命令 `show cts environment-data` 以顯示全域性Cisco TrustSec環境資料。

<#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

運行命令 `show cts pacs` , 顯示已調配的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: 000200B80003000100040010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8

執行命令 `show cts role-based permissions` 顯示 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

運行命令 `show cts rbacl (SGACLName)` 以顯示存取控制清單(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
```

相關資訊

- [Cisco Catalyst SD-WAN安全配置指南](#)
- [Cisco TrustSec配置指南](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。