

SD-WAN에서 TrustSec SGT SXP 전파 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Cisco TrustSec 통합](#)

[SGT 전파 방법](#)

[SXP를 사용한 SGT 전파](#)

[SGT SXP 전파 활성화 및 SGACL 정책 다운로드](#)

[1단계. Radius 매개변수 구성](#)

[2단계. SXP 매개변수 구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 SD-WAN(Software-Defined Wide-Area Network)의 SXP(Security Group Tag Exchange Protocol) 전파 방법 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst SD-WAN(Software-Defined Wide Area Network)
- SD-Access(Software-Defined Access) 패브릭
- Cisco ISE(Identify Service Engine)

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco TrustSec 통합

Cisco TrustSec 통합을 통한 SGT 전파는 Cisco IOS® XE Catalyst SD-WAN 릴리스 17.3.1a 이상에서 지원됩니다. 이 기능을 통해 Cisco IOS® XE Catalyst SD-WAN 에지 디바이스는 브랜치의 Cisco TrustSec 지원 스위치에 의해 생성된 SGT(Security Group Tag) 인라인 태그를 Cisco Catalyst SD-WAN 네트워크의 다른 에지 디바이스로 전파할 수 있습니다.

Cisco TrustSec의 기본 개념:

- SGT 바인딩: IP와 SGT 간의 연결에서는 모든 바인딩이 가장 일반적인 컨피그레이션을 가지며 Cisco ISE에서 직접 학습합니다.
- SGT 전파: 전파 방법은 네트워크 홉 간에 이러한 SGT를 전파하는 데 사용됩니다.
- SGTACL 정책: 신뢰할 수 있는 네트워크 내에서 트래픽 소스의 권한을 지정하는 규칙 집합.
- SGT 시행: SGT 정책에 따라 정책이 시행되는 위치입니다.

SGT 전파 방법

SGT 전파 방법은 다음과 같습니다.

- SGT 전파 인라인 태깅
- SGT SXP 전파

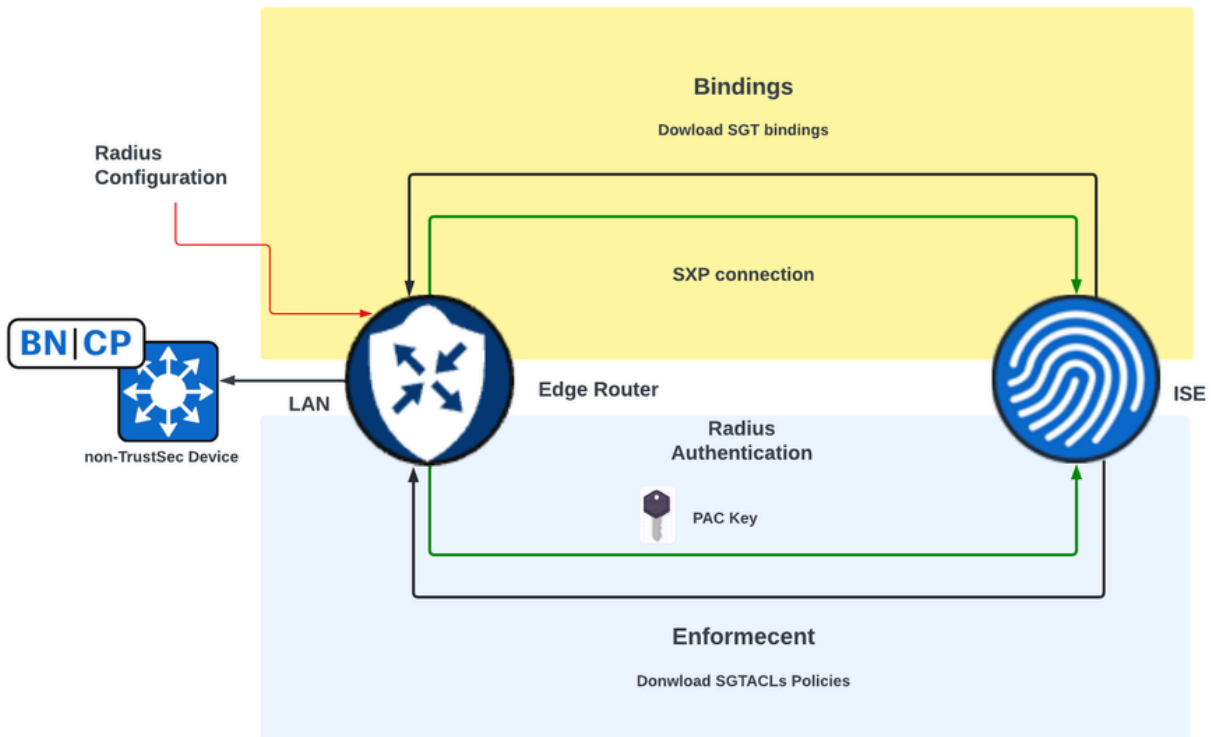
SXP를 사용한 SGT 전파

인라인 태깅 전파를 위해 브랜치에는 SGT 인라인 태깅(Cisco TrustSec 디바이스)을 처리할 수 있는 Cisco TrustSec 지원 스위치가 있어야 합니다. 하드웨어가 인라인 태깅을 지원하지 않는 경우 SGT 전파에서는 SXP(Security Group Tag Exchange Protocol)를 사용하여 네트워크 디바이스 전반에 SGT를 전파합니다.

Cisco ISE에서는 IP-SGT 바인딩(동적 IP-SGT)을 생성한 다음 SXP를 사용하여 IP-SGT 바인딩을 Cisco IOS® XE Catalyst SD-WAN 장치로 다운로드하여 Cisco Catalyst SD-WAN 네트워크를 통해 SGT를 전파할 수 있습니다. 또한 SD-WAN 이그레스의 SGT 트래픽에 대한 정책은 ISE에서 SGACL 정책을 다운로드하여 시행됩니다.

예:

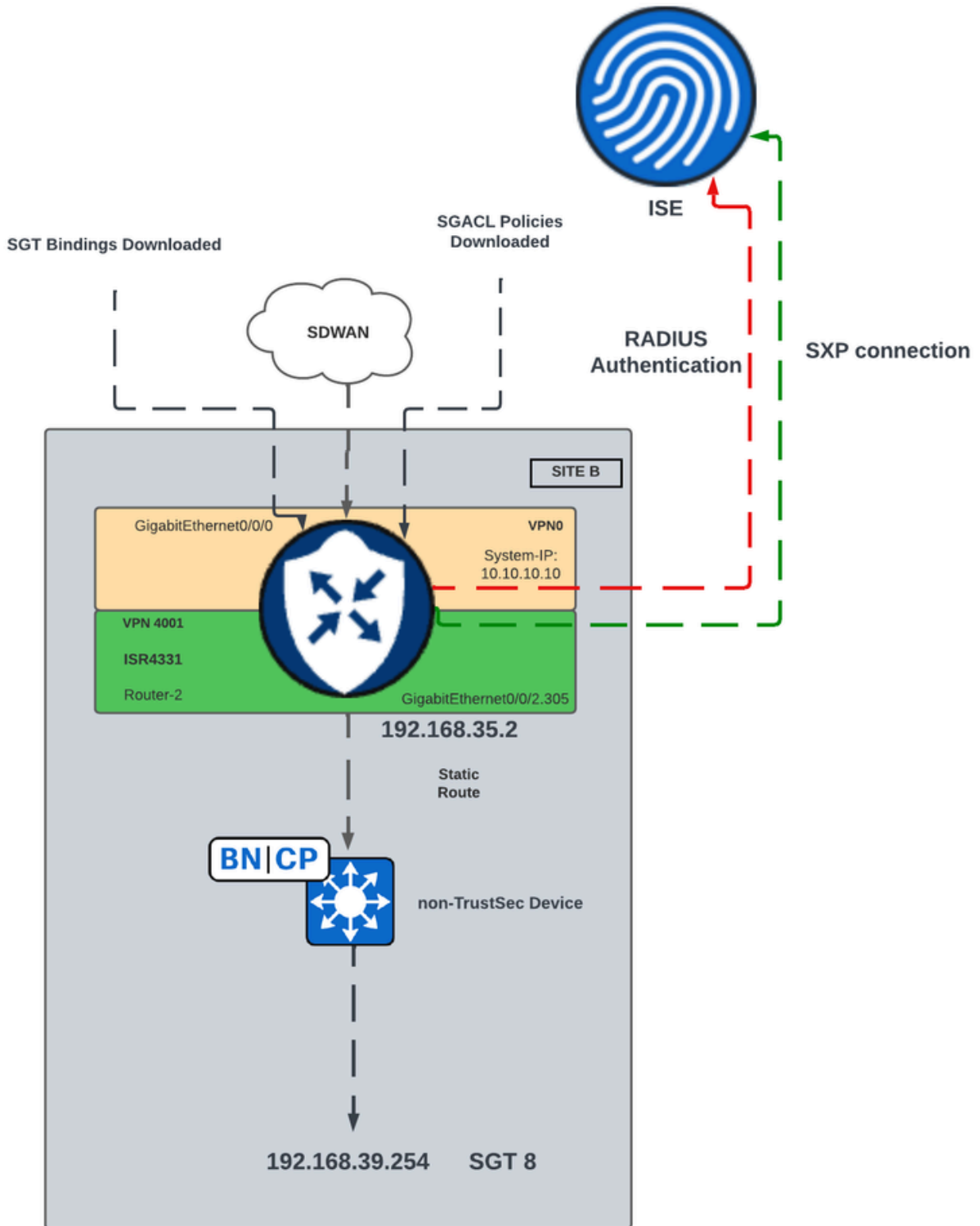
- Cisco 스위치(Border node)는 인라인 태깅(non-TrustSec 디바이스)을 지원하지 않습니다.
- Cisco ISE는 SXP 연결을 통해 Cisco IOS® XE Catalyst SD-WAN 디바이스(에지 라우터)에 IP-SGT 바인딩을 다운로드할 수 있습니다.
- Cisco ISE는 Radius 통합 및 PAC 키를 통해 SGACL 정책을 다음에 다운로드할 수 있습니다. Cisco IOS® XE Catalyst SD-WAN 디바이스(에지 라우터).



SD-WAN 에지 디바이스에서 SXP 전파 및 다운로드 SGACL 정책을 활성화하기 위한 요구 사항

- ✎ 참고: SGACL 정책은 인그레스 트래픽에 적용되지 않으며 Cisco Catalyst SD-WAN 네트워크의 이그레스 트래픽에만 적용됩니다.
- ✎ 참고: Cisco TrustSec 기능은 컨트롤러 모드에서 24K 이상의 SGT 정책에 대해 지원되지 않습니다.

SGT SXP 전파 활성화 및 SGACL 정책 다운로드



SD-WAN에서 SGT SXP 전파를 위한 네트워크 다이어그램

1단계. Radius 매개변수 구성

- Cisco Catalyst SD-WAN Manager GUI에 로그인합니다.
- Configuration(컨피그레이션) > Templates(템플릿) > Feature Template(기능 템플릿) > Cisco

AAA로 이동합니다. RADIUS SERVER(RADIUS 서버)를 클릭합니다.

- RADIUS 서버 매개변수 및 키를 구성합니다.

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 서버 컨피그레이션

- Radius 그룹 매개변수를 구성하려면 값을 입력합니다.

RADIUS SERVER **RADIUS GROUP** RADIUS COA TRUSTSEC

[New RADIUS Group](#)

VPN ID

Source Interface

Radius Server

RADIUS 그룹 컨피그레이션

- Radius COA 매개변수를 구성 하려면 값을 입력 합니다.

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

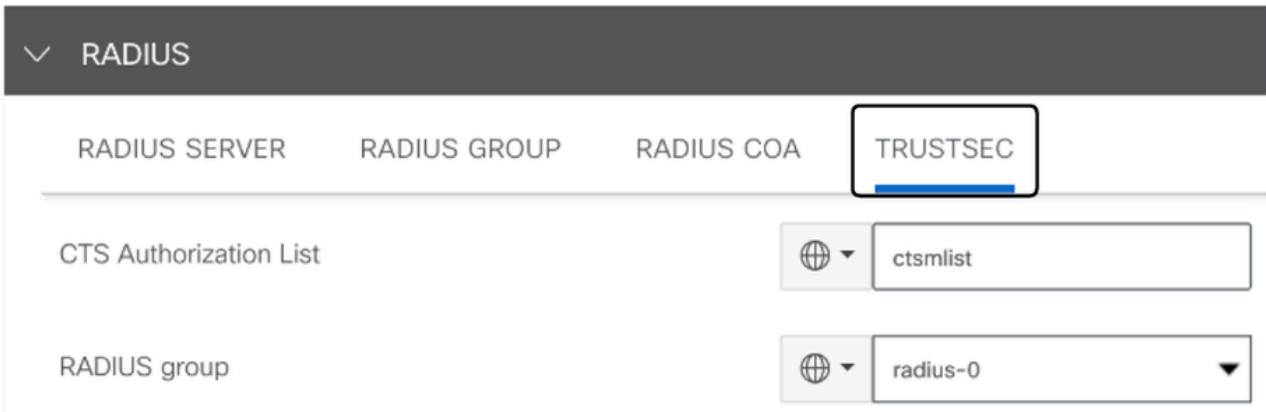
VPN ID

Server Key Password

 참고: Radius COA가 구성되지 않은 경우 SD-WAN 라우터는 SGACL 정책을 자동으로 다운로드할 수 없습니다. ISE에서 SGACL 정책을 생성하거나 수정한 후 `cts refresh policy` 명령을 사용하여 정책을 다운로드합니다.

- TRUSTSEC 섹션으로 이동하고 값을 입력합니다.

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



Feature Template > Cisco AAA > AAARadius

TRUSTSEC

CTS Authorization List: ctsmlist

RADIUS group: radius-0

TRUSTSEC 컨피그레이션

- 디바이스 템플릿에 Cisco AAA 기능 템플릿을 연결합니다.

2단계. SXP 매개변수 구성

- Configuration(컨피그레이션) > Templates(템플릿) > Feature Template(기능 템플릿) > TrustSec으로 이동합니다.
- CTS 자격 증명을 구성하고 디바이스 인터페이스에 SGT 바인딩을 할당합니다.

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 기능 템플릿

- SXP Default(SXP 기본) 섹션으로 이동하고 SXP Default(SXP 기본) 매개변수를 구성하는 값을 입력합니다.

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 기본 컨피그레이션


- SXP Connection(SXP 연결)으로 이동하고 SXP Connection(SXP 연결) 매개변수를 구성한 다음 Save(저장)를 클릭합니다.


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 연결 컨피그레이션

 참고: Cisco ISE는 처리 할 수 있는 SXP 세션 수에 제한 이 있습니다. 따라서, 대안으로, 스케일 네트워크 수평을 위한 SXP Reflector가 사용될 수 있다.

 참고: Cisco IOS® XE Catalyst SD-WAN 디바이스를 사용하여 SXP 피어를 설정하려면 SXP 리플렉터를 사용하는 것이 좋습니다.

- Configuration(컨피그레이션) > Templates(템플릿) > Device Template(디바이스 템플릿) > Additional Templates(추가 템플릿) > TrustSec으로 이동합니다.
- 이전에 생성한 TrustSec 기능 템플릿을 선택하고 Save를 클릭합니다.

Additional Templates

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

추가 템플릿 섹션

다음을 확인합니다.

명령을 `show cts sxp connections vrf (service vrf)` 실행하여 Cisco TrustSec SXP 연결 정보를 표시합니다.

```
<#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
```

명령 실행 `show cts role-based sgt-map` tIP 주소와 SGT 바인딩 간에 전역 Cisco TrustSec SGT 맵을 표시합니다.

```
<#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

전역 Cisco TrustSec 환경 데이터 `show cts environment-data`를 표시하려면 이 명령을 실행합니다.

```
<#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

명령을 실행하여 `show cts pacs` 프로비저닝된 Cisco TrustSec PAC를 표시합니다.

```
<#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
```

명령을 실행합니다 `show cts role-based permissions` .SGACL 정책을 표시합니다.

```
<#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
```

명령을 실행하여 `show cts rbacl (SGACLName)SGACL(Access Control List)` 컨피그레이션을 표시합니다.

```
<#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
```

관련 정보

- [Cisco Catalyst SD-WAN 보안 컨피그레이션 가이드](#)
- [Cisco TrustSec 컨피그레이션 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.