SDA를 사용하는 Cisco ISE TrustSec Allow-List 모델(기본 거부 IP)

목차

소개

이 문서에서는 SDA(Software Defined Access)에서 TrustSec의 allow-list(Default Deny IP) 모델을 활성화하는 방법에 대해 설명합니다. 이 문서에는 ISE(Identity Services Engine), DNAC(Digital Network Architecture Center) 및 스위치(Border and Edge)를 포함하는 여러 기술 및 구성 요소가 포함되어 있습니다.

두 가지 Trustsec 모델을 사용할 수 있습니다.

- 거부 목록 모델(기본 허용 IP):이 모델에서 기본 작업은 Permit IP이며 SGACL(Security Group Access List)을 사용하여 모든 제한 사항을 명시적으로 구성해야 합니다. 이는 일반적으로 네트워크 내 트래픽 흐름을 완전히 이해하지 못한 경우에 사용됩니다.이 모델은 구현하기가 매우 쉽습니다.

- 허용 목록 모델(기본 거부 IP):이 모델에서는 기본 작업이 Deny IP(IP 거부)이므로 SGACL을 사용하여 필요한 트래픽을 명시적으로 허용해야 합니다.이는 일반적으로 고객이 네트워크 내 트래픽 흐름의 종류를 올바르게 이해할 때 사용됩니다.이 모델에서는 컨트롤 플레인 트래픽에 대한 자세한 연구가 필요하며, 컨트롤 플레인 트래픽은 활성화되는 순간 모든 트래픽을 차단할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Dot1x/MAB 인증
- Cisco TrustSec(CTS)
- SXP(Security Exchange Protocol)
- 웹 프록시
- 방화벽 개념
- DNAC

사용되는 구성 요소

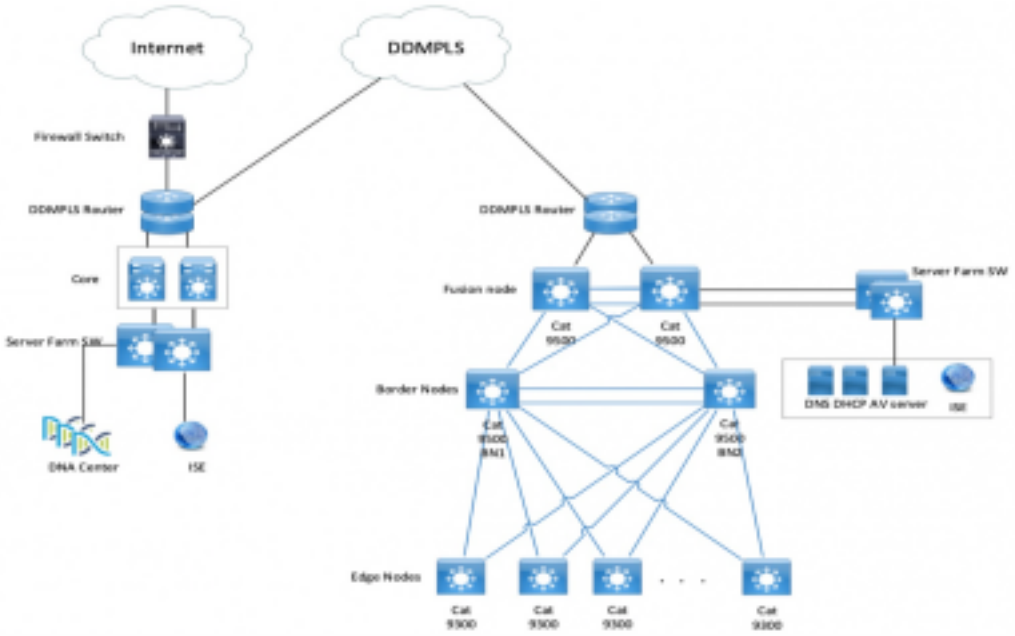
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9300 Edge 및 9500 Border Node(스위치)(IOS 16.9.3 포함)
- DNAC 1.3.0.5
- ISE 2.6 패치 3(2개의 노드 - 이중 구축)
- DNAC와 ISE는
- 경계 및 에지 노드는 DNAC에서 프로비저닝됨
- SXP 터널은 ISE(스피커)에서 두 보더 노드(리스너)로 설정됩니다.
- IP 주소 풀이 호스트 온보딩에 추가됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



구성

다음은 허용 목록 모델(기본 거부 IP)을 활성화하는 단계입니다.

1. 스위치 SGT를 Unknown에서 TrustSec 디바이스로 변경합니다.
2. CTS 역할 기반 적용을 비활성화합니다.
3. DNAC Template(DNAC 템플릿)을 사용하는 경계 및 에지 스위치의 IP-SGT 매핑.
4. DNAC 템플릿을 사용하여 대체 SGACL입니다.
5. trustsec Matrix에서 Allow-List(기본 거부 IP)를 활성화합니다.
6. 엔드포인트/사용자에 대한 SGT를 생성합니다.
7. 엔드포인트/사용자에 대한 SGACL을 생성합니다(프로덕션 오버레이 트래픽의 경우).

1단계. 스위치 SGT를 Unknown(알 수 없음)에서 TrustSec 디바이스로 변경합니다.

기본적으로 알 수 없는 SGT(Security Group Tag)는 네트워크 디바이스 권한 부여를 위해 구성됩니다.TrustSec 디바이스 SGT로 변경하면 가시성이 향상되고 스위치에서 시작한 트래픽에 대해 SGACL을 생성할 수 있습니다.

Work Centers(**작업 센터) > TrustSec > TrustSec Policy(TrustSec 정책) > Network Device Authorization(네트워크 디바이스 권한 부여)**으로 이동한 다음 Trustsec_Devices(알 수 없음)에서 변경합니다.

2단계. CTS 역할 기반 적용을 비활성화합니다.

- 허용 목록 모델(기본 거부)이 설정되면 언더레이 멀티캐스트 및 브로드캐스트 트래픽(예: IS-IS(Intermediate System-to-Intermediate System), BFD(Bidirectional Forwarding Detection), SSH(Secure Shell) 트래픽 등)이 패브릭에서 차단됩니다.

- 패브릭 에지와 테두리에 연결되는 모든 TenGig 포트는 여기에 명령을 사용하여 구성해야 합니다.이러한 상황에서 이 인터페이스에서 시작된 트래픽은 시행 대상이 아닙니다.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **참고:**DNAC에서 범위 템플릿을 사용하여 간단하게 수행할 수 있습니다.그렇지 않으면 모든 스위치에서 프로비저닝 중에 수동으로 수행해야 합니다.아래 코드 조각은 DNAC 템플릿을 통해 수행하는 방법을 보여줍니다.

```
interface range $uplink1

no cts role-based enforcement
```

DNAC 템플릿에 대한 자세한 *내용은* 이 URL에서 문서를 *참조하십시오*.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_010000.html

3단계. DNAC 템플릿을 사용한 보더 및 에지 스위치의 IP-SGT 매핑.

모든 ISE가 중단되더라도 스위치에서 로컬 IP-SGT 매핑을 사용할 수 있도록 하는 것이 좋습니다.이를 통해 언더레이가 구축되고 중요한 리소스에 대한 연결이 그대로 유지됨

첫 번째 단계는 SGT에 중요 서비스를 바인딩하는 것입니다(예: Basic_Network_Services/1000). 이러한 서비스 중 일부는 다음과 같습니다.

- 언더레이/ISIS 서브넷
- ISE/ DNAC
- 모니터링 툴
- OTT의 경우 AP의 서브넷
- 터미널 서버
- 주요 서비스 - 예:IP 전화

예:

```
cts role-based sgt-map <ISE/DNAC Subnet> sgt 1000

cts role-based sgt-map  sgt 2

cts role-based sgt-map <Wireless OTT Infra> sgt 1000

cts role-based sgt-map <Underlay OTT AP Subnet> sgt 2

cts role-based sgt-map <Monitoring Tool IP> sgt 1000

cts role-based sgt-map vrf CORP_VN <Voice Gateway and CUCM Subnet> sgt 1000
```

4단계. DNAC 템플릿으로 SGACL을 대체합니다.

SGT 매핑은 SGT를 사용하여 관련 SGACL이 생성될 때까지 사용되지 않습니다. 따라서 다음 단계

는 ISE 노드가 다운될 경우(ISE 서비스가 다운되면 SXP 터널이 다운되어 SGACL과 IP SGT 매핑이 동적으로 다운로드되지 않음) 로컬 폴백 역할을 하는 SGACL을 생성하는 것입니다.

이 컨피그레이션은 모든 에지 및 경계 노드에 푸시됩니다.

대체 역할 기반 ACL/계약**:**

```
ip access-list role-based FALLBACK

permit ip
```

TrustSec 디바이스에 대한 TrustSec 디바이스:

```
cts role-based permissions from 2 to 2 FALLBACK
```

SGACL 위 패브릭 스위치 내 통신 보장 및 IP 언더레이

SGT 1000에 대한 TrustSec 디바이스:

```
cts role-based permissions from 2 to 1000 FALLBACK
```

SGACL 위 스위치 및 액세스 포인트에서 ISE, DNAC, WLC 및 모니터링 툴로의 통신 보장

SGT 1000에서 TrustSec 디바이스로:

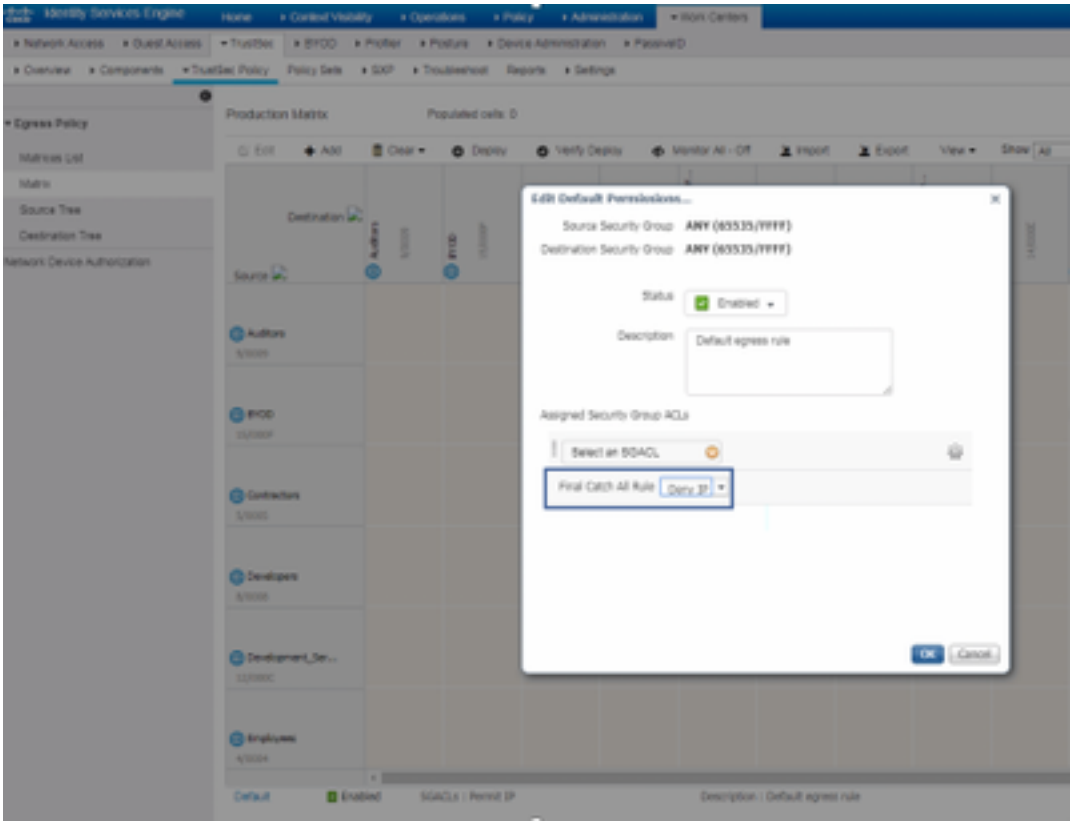
```
cts role-based permissions from 1000 to 2 FALLBACK
```

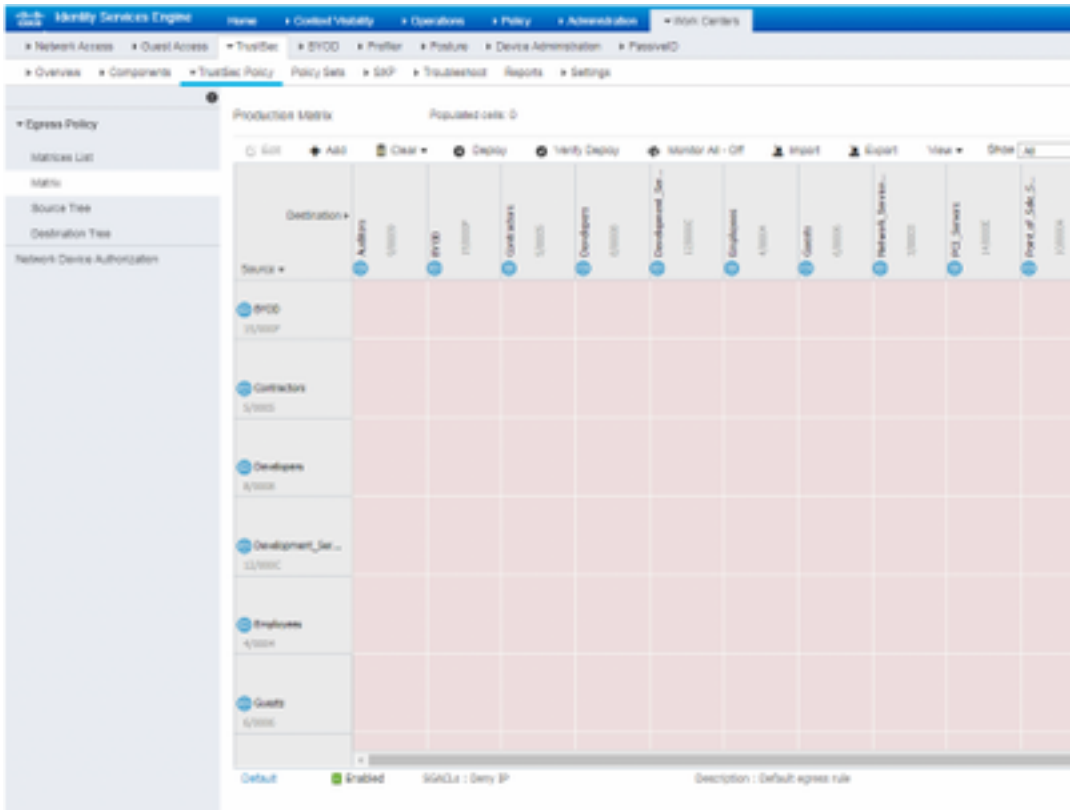
SGACL 위 액세스 포인트에서 ISE, DNAC, WLC 및 모니터링 툴로의 통신 보장

5단계. TrustSec Matrix에서 Allow-List Model(기본 거부)을 활성화합니다.

네트워크의 대부분의 트래픽을 거부하고 더 적은 범위를 허용해야 합니다.그러면 명시적 허용 규칙과 함께 기본 거부를 사용하는 경우 필요한 정책이 더 적습니다.

Work Centers(**작업 센터) > TrustSec > TrustSec Policy(TrustSec 정책) > Matrix(매트릭스) > Default(기본값)로 이동하고** 최종 catch 규칙에서 **Deny All(모두 거부)**으로 변경합니다.



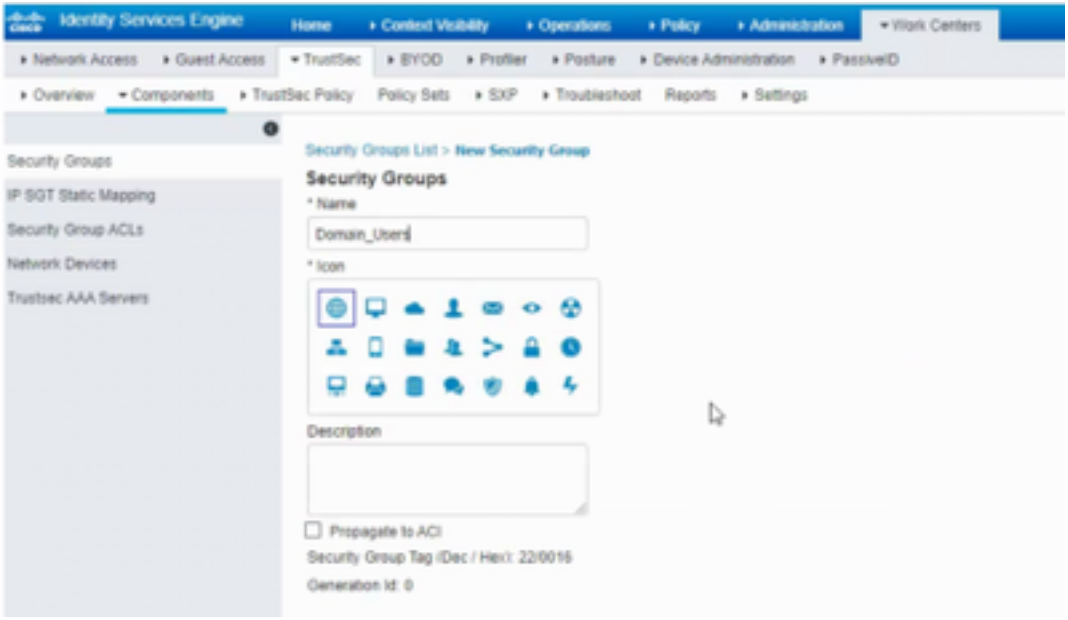


참고:이 이미지는 (모든 열은 기본적으로 빨간색으로 표시됨), Default Deny(기본 거부)가 활성화되었으며 SGACL을 만든 후 선택적 트래픽만 허용할 수 있음을 나타냅니다.

6단계. 엔드포인트/사용자에 대한 SGT를 생성합니다.

SDA 환경에서는 ISE/DNAC에서 SGT 데이터베이스가 일치하지 않아 데이터베이스가 손상된 경우가 많으므로 DNAC GUI에서만 새 SGT를 생성해야 합니다.

SGT를 생성하려면 DNAC **> Policy(정책) > Group-Based Access Control(그룹 기반 액세스 제어) > Scalable Groups(확장형 그룹) > Add Groups(그룹 추가)에 로그인하고, ISE Scalable Group(ISE 확장형 그룹)**으로 리디렉션하는 페이지 Add(추가)를 클릭하고 SGT 이름을 입력하고 저장합니다.



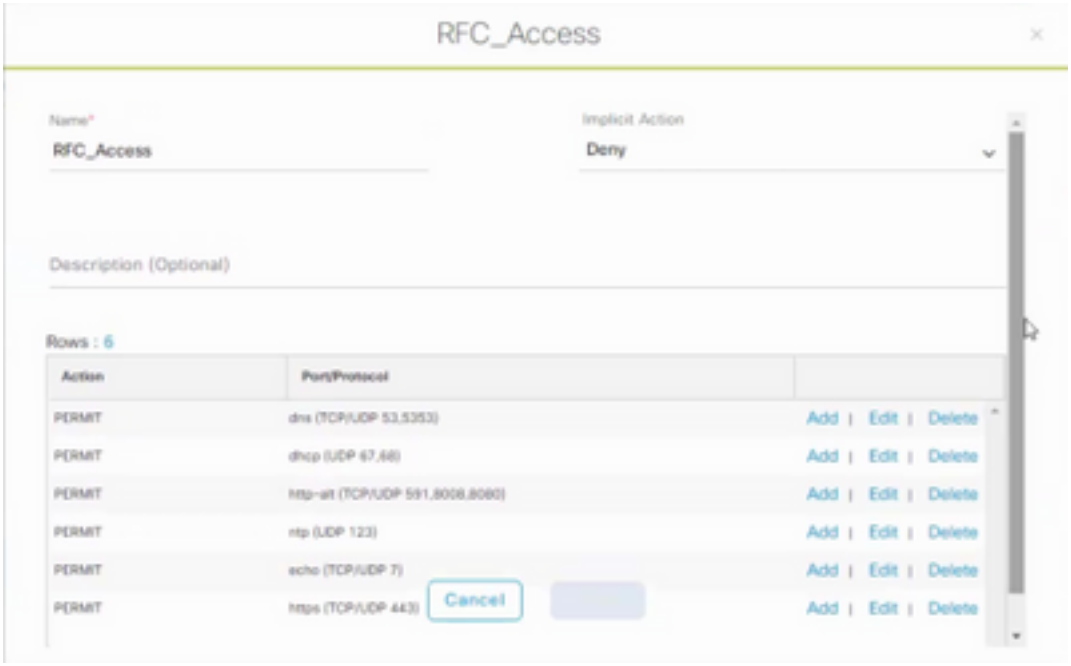
동일한 SGT가 PxGrid 통합을 통해 DNAC에 반영됩니다.이는 향후 모든 SGT 생성에 대해 동일한 절차입니다.

7단계. 엔드포인트/사용자에 대한 SGACL을 생성합니다(프로덕션 오버레이 트래픽의 경우).

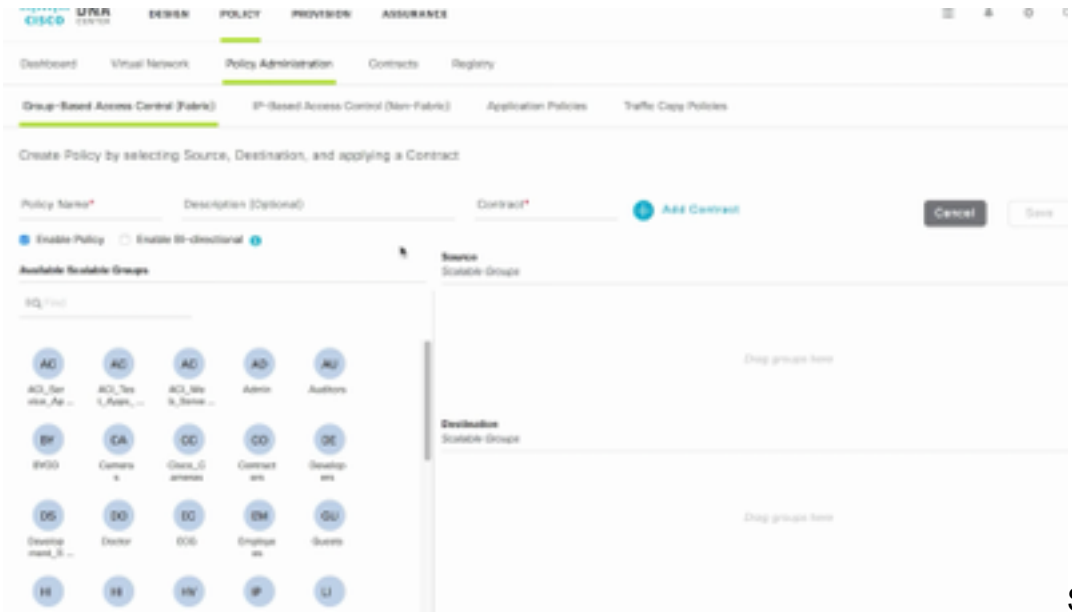
SDA 환경에서 새 SGT는 DNAC GUI에서만 생성해야 합니다.

```
Policy Name: Domain_Users_Access

Contract : Permit

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)

Destination SGT: Domain_Users, Basic_Network_Services, DC_Subnet, Unknown (Drag from Available
Security Group)



Policy Name: RFC_Access

Contract : RFC_Access (This Contract contains limited ports)

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)

Destination SGT: RFC1918 (Drag from Available Security Group)
```

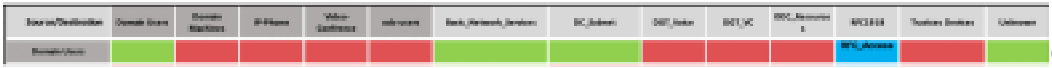
계약을 생성하려면 DNAC에 로그인하고 **Policy(정책)** > Contracts(계약) **> Add Contracts(계약 추가) > Add required protocol(필수 프로토콜 추가)**로 이동한 다음 **Save(저장)**를 클릭합니다.



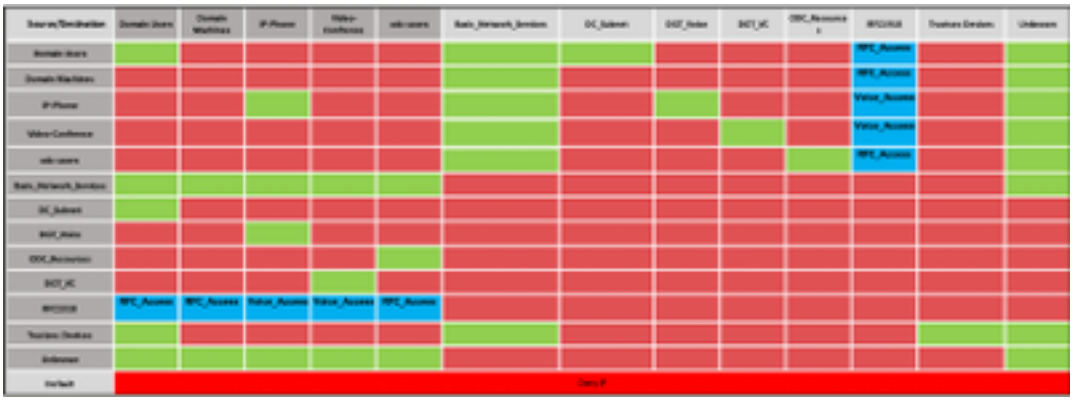
계약을 생성하려면 DNAC에 로그인하고 **Policy(정책) > Group-Based Access Control(그룹 기반 액세스 제어) > Group-Based-Access-Policies(그룹 기반 액세스 제어) > Add Policies(정책 추가) > Create policy(지정된 정보 포함)로** 지금 **Save(저장)를 클릭한 다음 Deploy(구축)로 이동합니다.**

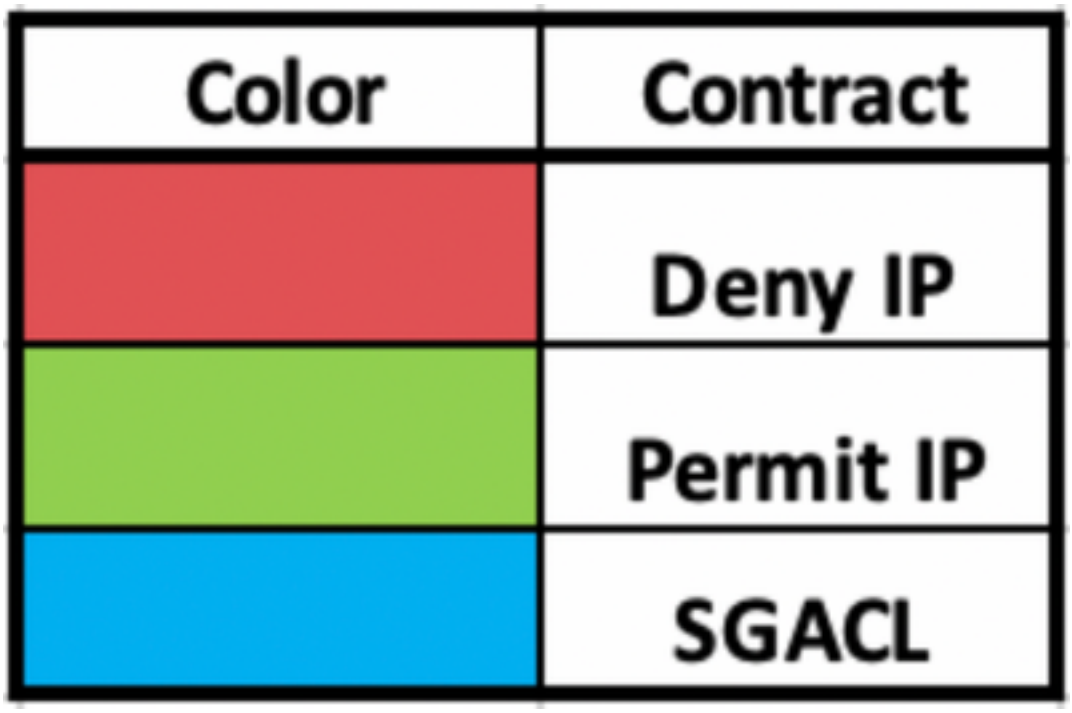


SGACL/Contract가 DNAC에서 구성되면 ISE에 자동으로 반영됩니다. 다음은 sgt에 대한 단방향 매트릭스 보기의 예입니다.



아래 이미지와 같이 SGACL 매트릭스는 허용 목록(기본 거부) 모델의 예제 뷰입니다.





다음을 확인합니다.

네트워크 디바이스 SGT

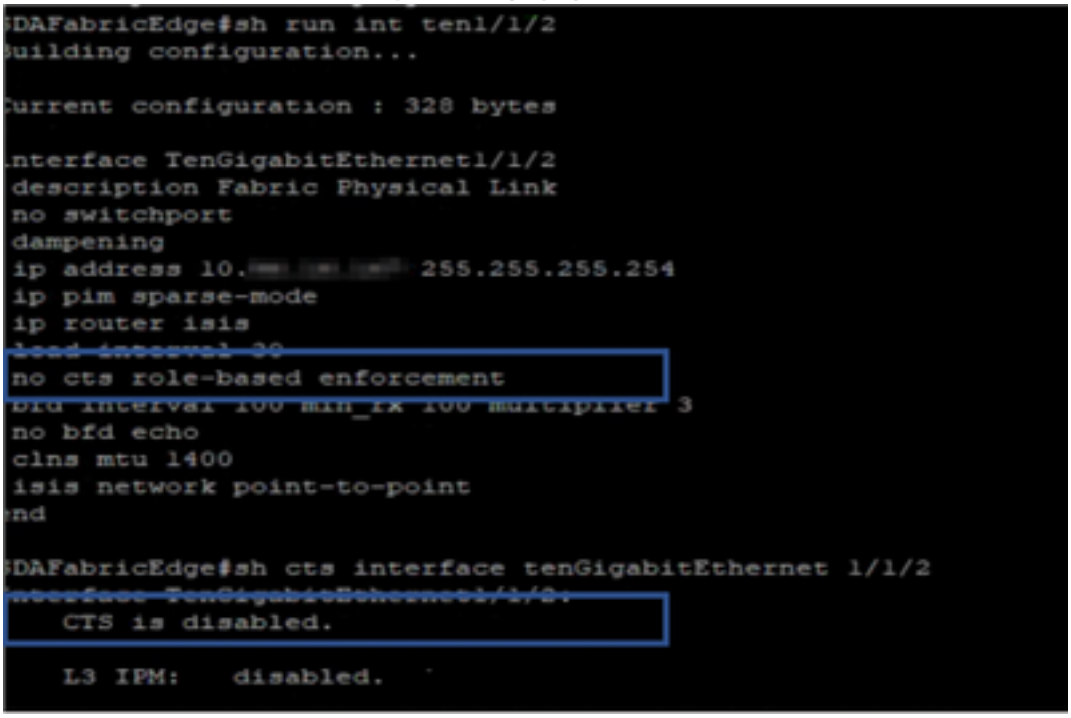
ISE에서 받은 스위치 SGT를 확인하려면 다음 명령을 실행합니다. **show cts environmental-data**

```
SDAFabricEdge#sh cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-15:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 2 server(s):
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
```

업링크 포트에 시행

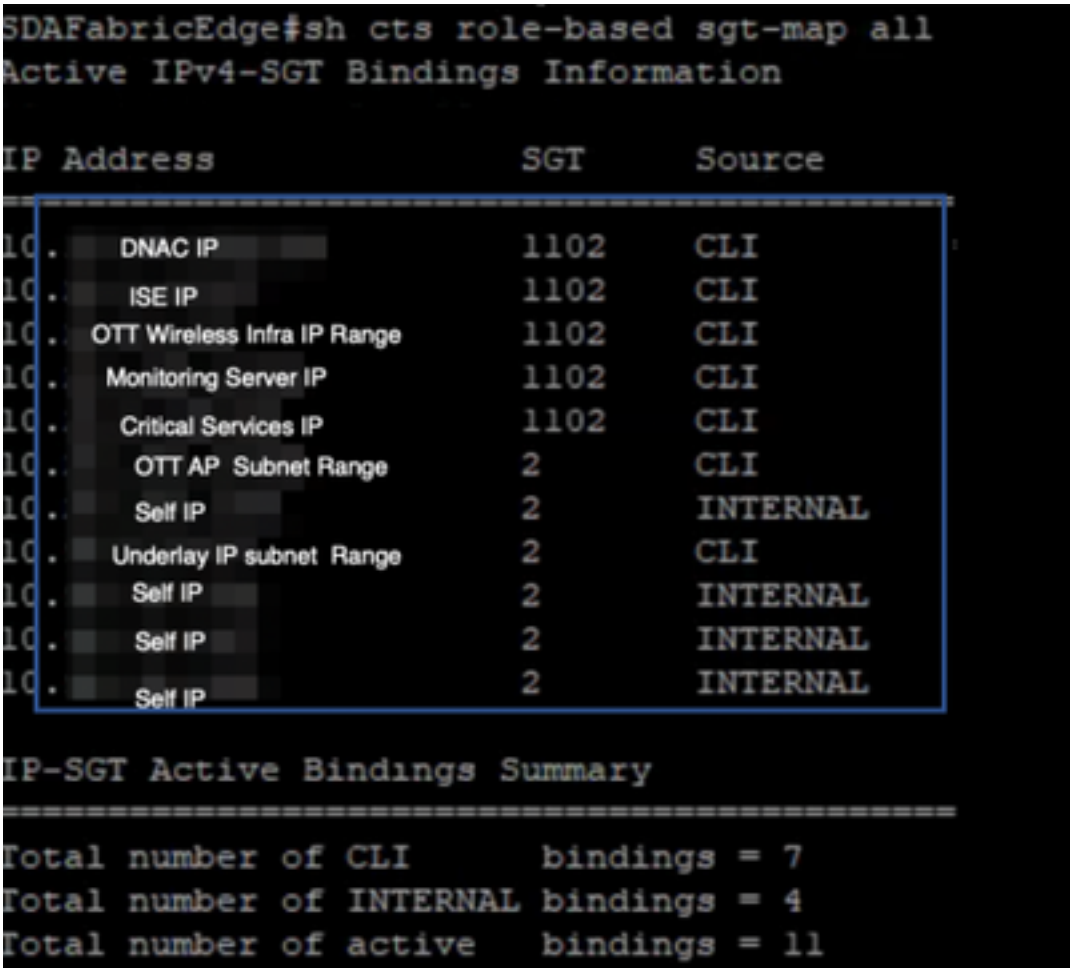
업링크 인터페이스에서 시행을 확인하려면 다음 명령을 실행합니다.

- show run interface <uplink>
- show cts interface <업링크 인터페이스>



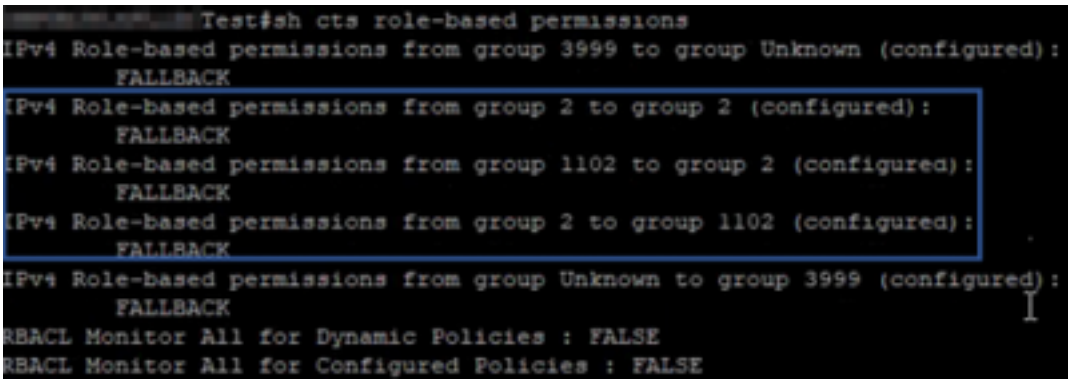
로컬 IP-SGT 매핑

로컬로 구성된 IP-SGT 매핑을 확인하려면 sh cts role-based sgt-map all 명령을 실행합니다.



로컬 폴백 SGACL

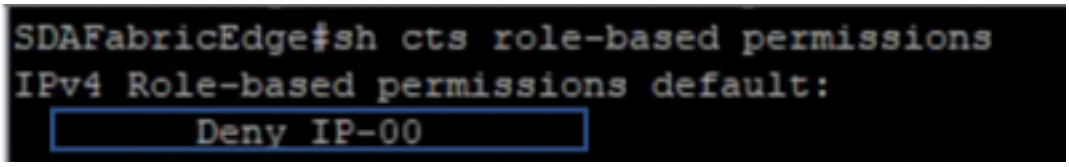
FALLBACK SGACL을 확인하려면 **sh cts role-based permission** 명령을 실행합니다.



참고:ISE에서 푸시하는 SGACL은 로컬 SGACL보다 우선합니다.

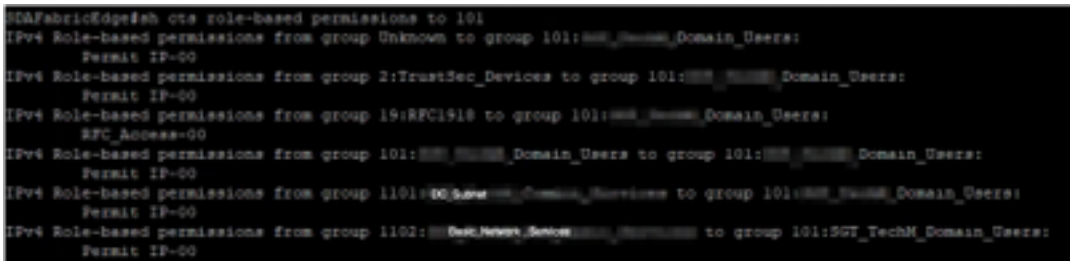
패브릭 스위치에서 허용 목록(기본 거부) 지원

허용 목록(기본 거부) 모델을 확인하려면 **sh cts 역할 기반 권한** 명령을 실행합니다.



패브릭에 연결된 엔드포인트용 SGACL

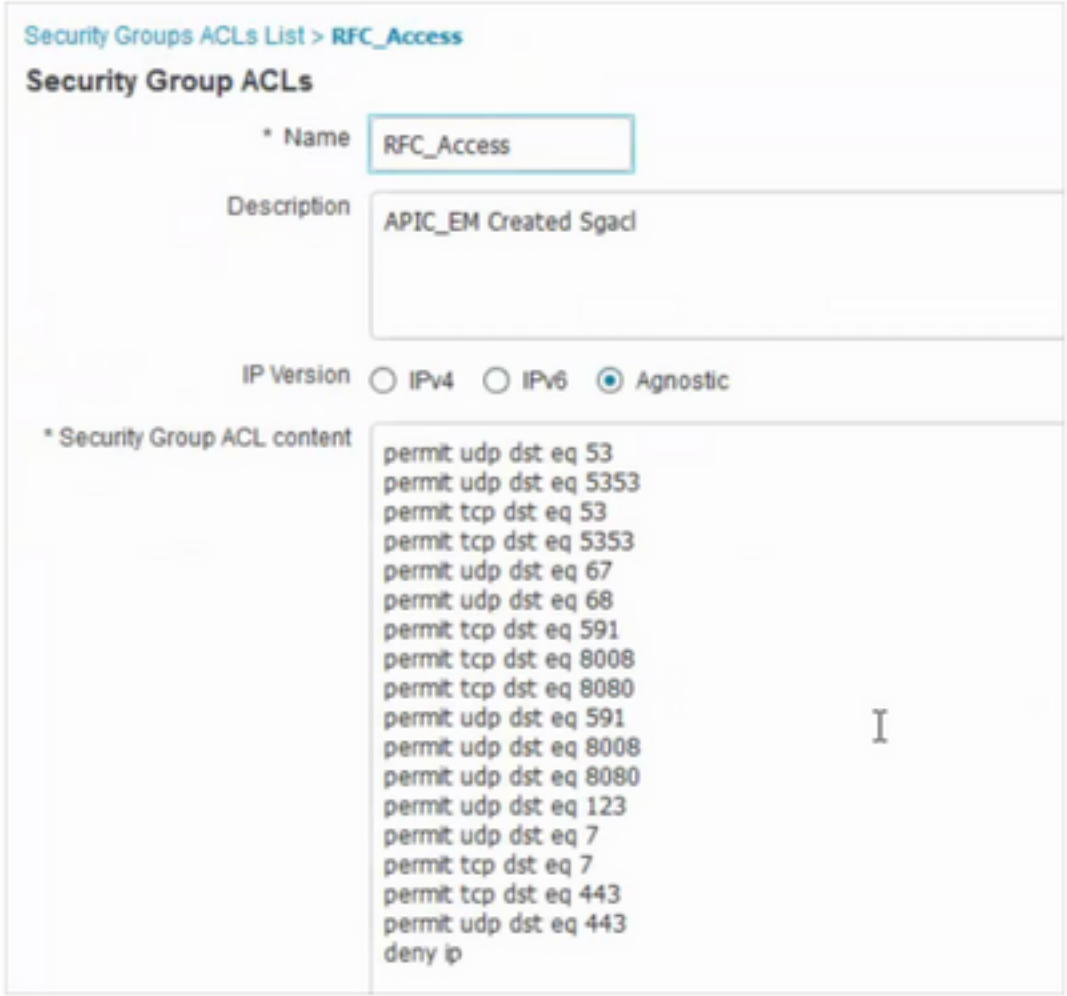
ISE에서 다운로드한 SGACL을 확인하려면 sh cts role-**based permission** 명령을 실행합니다.



DNAC에서 생성된 계약 확인

ISE에서 다운로드한 SGACL을 확인하려면 다음 명령을 실행합니다. **show access-list <ACL/Contract Name>**

```
Role-based IP access list RFC_Access-00 (downloaded)
    10 permit udp dst eq domain
    20 permit udp dst eq 5353
    30 permit tcp dst eq domain
    40 permit tcp dst eq 5353
    50 permit udp dst eq bootps
    60 permit udp dst eq bootpc
    70 permit tcp dst eq 591
    80 permit tcp dst eq 8008
    90 permit tcp dst eq 8080
    100 permit udp dst eq 591
    110 permit udp dst eq 8008
    120 permit udp dst eq 8080
    130 permit udp dst eq ntp
    140 permit udp dst eq echo
    150 permit tcp dst eq echo
    160 permit tcp dst eq 443
    170 permit udp dst eq 443
    180 deny ip
```



패브릭 스위치에서 언더레이 SGACL 카운터

SGACL 정책 적중 수를 확인하려면 다음 명령을 실행합니다. **Show cts role-based counter**

```
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          0          0          0          0
2       2       0          0          1644843    0          0          0
1101    2       0          0          0          0          0          0
1102    2       0          0          0          0          0          0
101     101     0          0          0          0          0          0
1101    101     0          0          0          57647      0          0
1102    101     0          0          0          12541      0          0
1103    101     0          0          0          25         0          0
```

문제 해결

문제 1. 두 ISE 노드가 모두 다운된 경우.

두 ISE 노드가 모두 다운된 경우, ISE에서 수신한 IP-SGT 매핑이 제거되고 모든 DGT가 알 수 없는 태그로 지정되며 5-6분 후에 존재하는 모든 사용자 세션이 중지됩니다.

> **참고:**이 문제는 sgt (xxxx) -> unknown (0) SGACL 액세스가 DHCP, DNS 및 웹 프록시 포트로 제한된 경우에만 적용됩니다.

해결책:

1. SGT 생성(예:RFC1918).
2. 두 경계 모두에 RFC 전용 IP 범위를 푸시합니다.
3. sgt (xxxx) —> RFC1918에서 DHCP, DNS 및 웹 프록시에 대한 액세스 제한
4. IP 허용 계약으로 sgacl sgt(xxxx) —> 알 수 없는 를 생성/수정합니다.

이제 두 ise 노드가 모두 다운되면 SGACL sgt—>알 수 없는 적중 및 존재하는 세션이 그대로 유지됩니다.

문제 2. IP-Phone 단방향 음성 또는 음성 없음

IP로의 확장이 SIP에서 수행되었으며 실제 음성 통신은 IP에서 IP로의 RTP를 통해 이루어집니다 .CUCM 및 음성 게이트웨이가 DGT_**Voice에 추가되었습니다**.

해결책:

1. IP_Phone —> IP_Phone에서 트래픽을 허용하여 동일한 위치 또는 east-west 음성 통신을 활성화할 수 있습니다.
2. 나머지 위치는 DGT RFC1918의 허용 RTP 프로토콜 범위에 의해 허용될 수 있습니다. IP_Phone —> 알 수 없음에 대해 동일한 범위를 허용할 수 있습니다.

문제 3. 중요한 VLAN 엔드포인트에 네트워크 액세스가 없습니다.

DNAC는 데이터를 위한 중요 VLAN과 스위치를 프로비저닝하며, 컨피그레이션에 따라 ISE 중단 중 새로운 모든 연결은 중요 VLAN 및 SGT 3999를 가져옵니다.Default Deny in trustsec 정책은 네트워크 리소스에 액세스하기 위해 새 연결을 제한합니다.

해결책:

DNAC 템플릿을 사용하여 모든 에지 및 보더 스위치에서 중요 SGT를 위한 SGACL 푸시

```
cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK
```
이러한 명령은 컨피그레이션 섹션에 추가됩니다.

참고:모든 명령을 단일 템플릿으로 결합할 수 있으며 프로비저닝 중에 푸시할 수 있습니다.

문제 4. 패킷 드롭 인 중요 VLAN.

ISE 노드가 다운되어 시스템이 중요 VLAN에 있게 되면 중요 VLAN의 모든 엔드포인트에 대해 3~4분마다 패킷 삭제(최대 10회 삭제 관찰됨)가 발생합니다.

관찰:서버가 DEAD일 때 인증 카운터가 증가합니다.서버가 DEAD로 표시되면 클라이언트가 PSN으로 인증하려고 합니다.

해결 방법:

ISE PSN 노드가 다운된 경우 엔드포인트에서 인증 요청이 없어야 합니다.

DNAC를 사용하여 radius 서버 아래에서 이 명령을 푸시합니다.

자동 테스터 사용자 이름 자동 테스트 프로브 온

스위치에서 이 명령을 사용하면 정기적인 테스트 인증 메시지를 RADIUS 서버로 전송합니다.서버에서 RADIUS 응답을 찾습니다.성공 메시지는 필요하지 않습니다. 서버가 활성 상태임을 보여주므로 실패한 인증 접미사가 필요합니다.

추가 정보

DNAC 최종 템플릿:

```
interface range $uplink1

no cts role-based enforcement

! .

cts role-based sgt-map <ISE Primary IP> sgt 1102

cts role-based sgt-map <Underlay Subnet> sgt 2

cts role-based sgt-map <Wireless OTT Subnet>sgt 1102

cts role-based sgt-map <DNAC IP> sgt 1102

cts role-based sgt-map <SXP Subnet> sgt 2

cts role-based sgt-map <Network Monitoring Tool IP> sgt 1102

cts role-based sgt-map vrf CORP_VN <Voice Gateway Subnet> sgt 1102

!
```

```
ip access-list role-based FALLBACK

permit ip

!

cts role-based permissions from 2 to 1102 FALLBACK

cts role-based permissions from 1102 to 2 FALLBACK

cts role-based permissions from 2 to 2 FALLBACK

cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK
```

참고:에지 노드의 모든 업링크 인터페이스는 시행 없이 구성되며 업링크가 경계 노드에만 연결된다고 가정합니다.경계 노드에서 에지 노드를 향하는 업링크 인터페이스는 시행 없이 구성해야 하며 수동으로 구성해야 합니다.