SDWAN과 ACI의 통합 구성 및 확인

목차

약어

ACI - Application Centric Infrastructure

EPG - 엔드포인트 그룹

L3out - 레이어 3 출력

AAR - 애플리케이션 인식 라우팅

SLA - 서비스 레벨 계약

DC - 데이터 센터

WAN - WAN

SDN - 소프트웨어 정의 네트워킹

SD DC - 소프트웨어 정의 데이터 센터

SD WAN - 소프트웨어 정의 WAN(Wide Area Network)

QOS - Quality of Service

VRF - 가상 라우팅 및 포워딩

소개

이 문서에서는 Cisco의 SD-DC(Software Defined - Data Center) 솔루션인 ACI(Application Centric Infrastructure)를 SD-WAN(Software Defined - Wide Area Network)과 통합하는 컨피그레이션 단계 및 그 검증에 대해 설명합니다.

SDN(소프트웨어 정의 네트워킹) 특정 네트워크 세그먼트를 수용할 수 있도록 향상되었습니다.

1. 소프트웨어 정의 - 데이터 센터(SD-DC)
2. 소프트웨어 정의 - SD-WAN(Wide Area Network)

Cisco 솔루션은 SD-DC(Application Centric Infrastructure ACI)의 QoS(Quality of Service) 및 SD-WAN의 AAR(Application Aware Routing)/SLA(Service Level Agreements) 프로필의 강력한 기능을 제공합니다.

통합을 계획하고 있고 경로 전반에 걸쳐 원활한 트래픽 처리를 원하는 고객이 늘어남에 따라 Cisco는 SD-DC 및 SD-WAN 통합을 마련했습니다.

이 통합은 두 가지 활용 사례에 중점을 둡니다.

1. ACI(DC)에서 SDWAN(비 ACI 지사)으로의 트래픽
2. SDWAN(non ACI Branch)에서 ACI(DC)로의 트래픽

사전 요구 사항

요구 사항

SD-WAN과의 통합은 ACI에 구성된 L3 out을 통해 이루어지므로 지원되는 프로토콜이 포함된 L3out을 구성해야 합니다.

통합은 관리 네트워크를 통해 이루어지므로 ACI(APIC 컨트롤러)와 vManage 간의 관리 연결이 필요합니다.

사용되는 구성 요소

ACI 패브릭, SDWAN(vManage, vSmart Controller, vEdge)

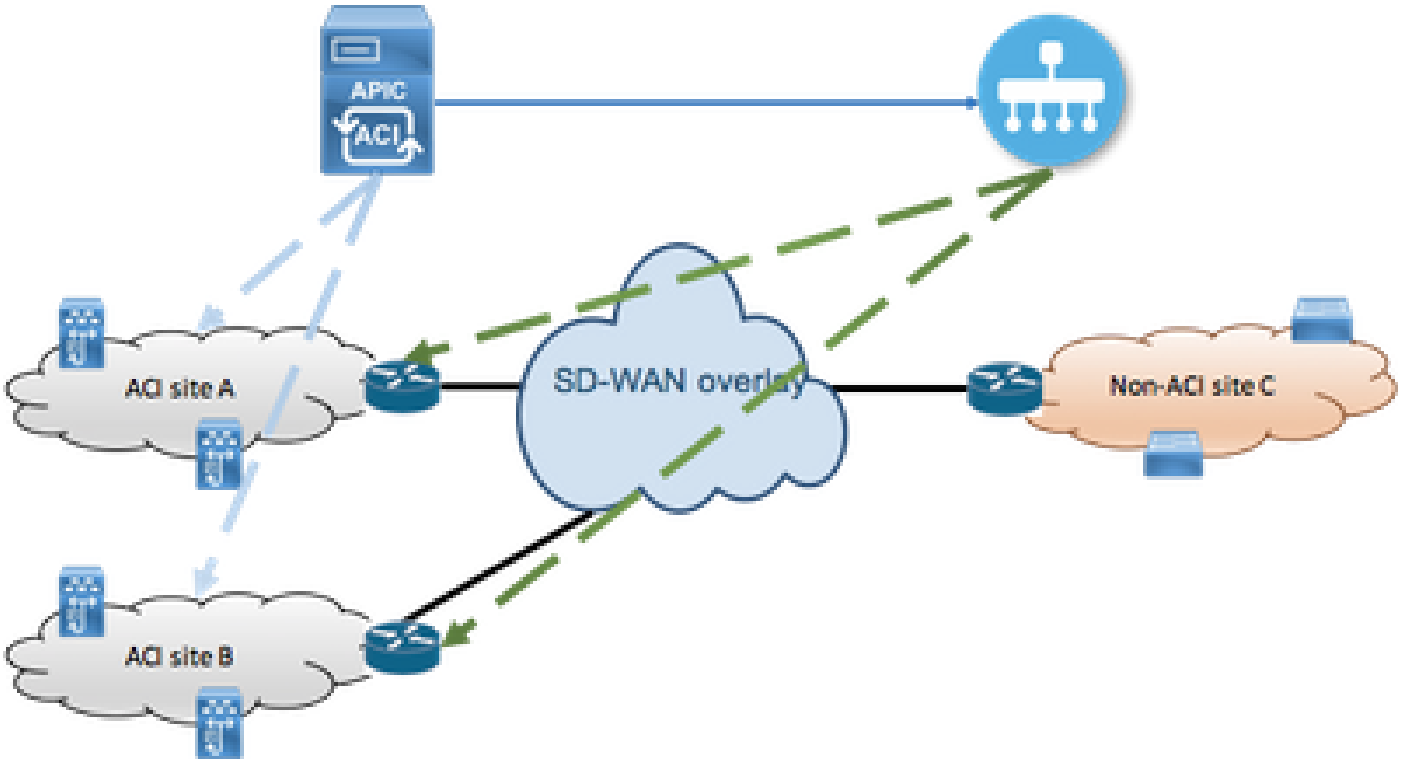
이 문서는 ACI 버전 4.2(3l)를 기반으로 합니다.

설정

네트워크 다이어그램

참조할 토폴로지:

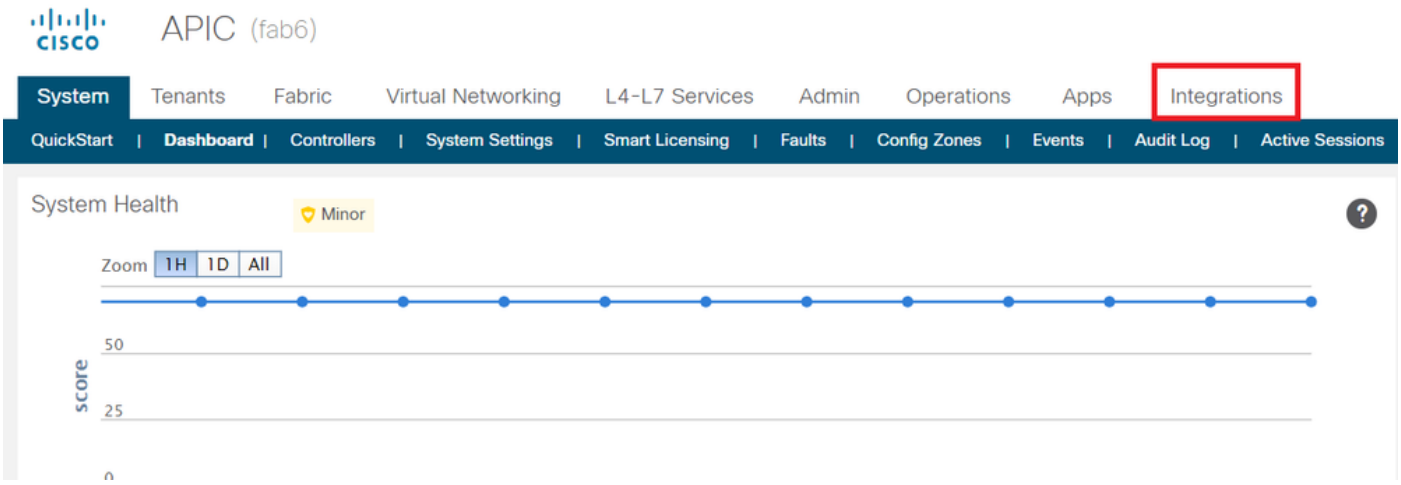
토폴로지에서는 ACI 사이트 A를 DC로, 비 ACI 사이트 C를 SDWAN 브랜치 사이트로 간주합니다.



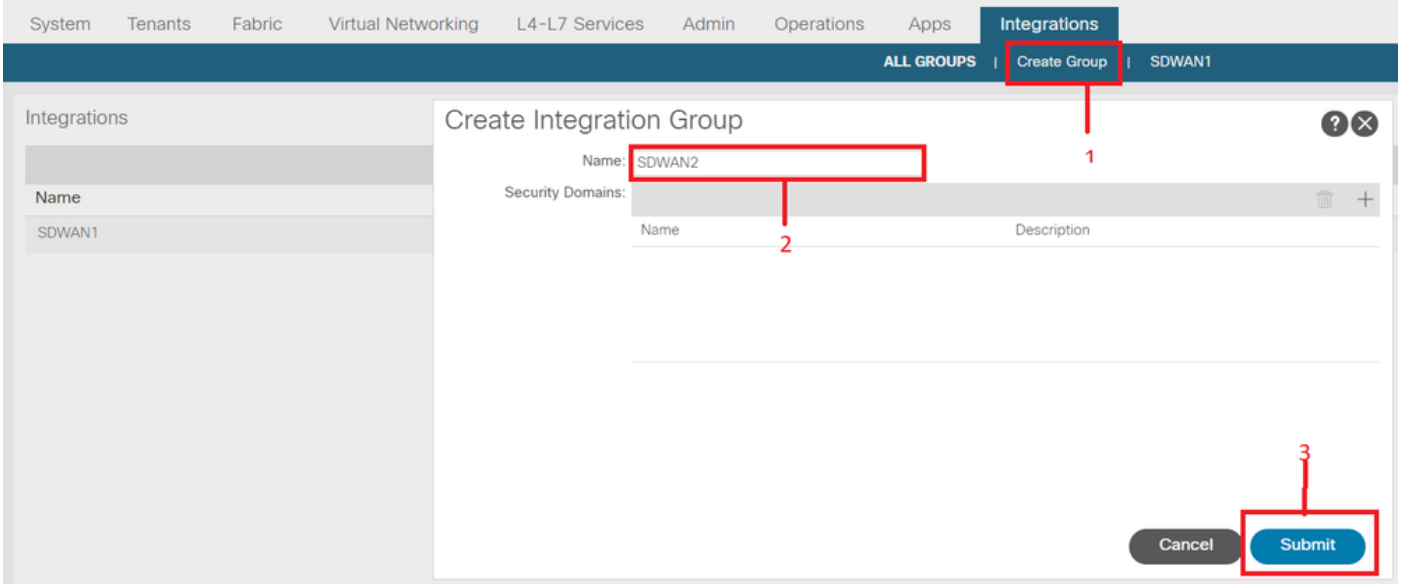
설정

섹션 A: 통합 컨피그레이션

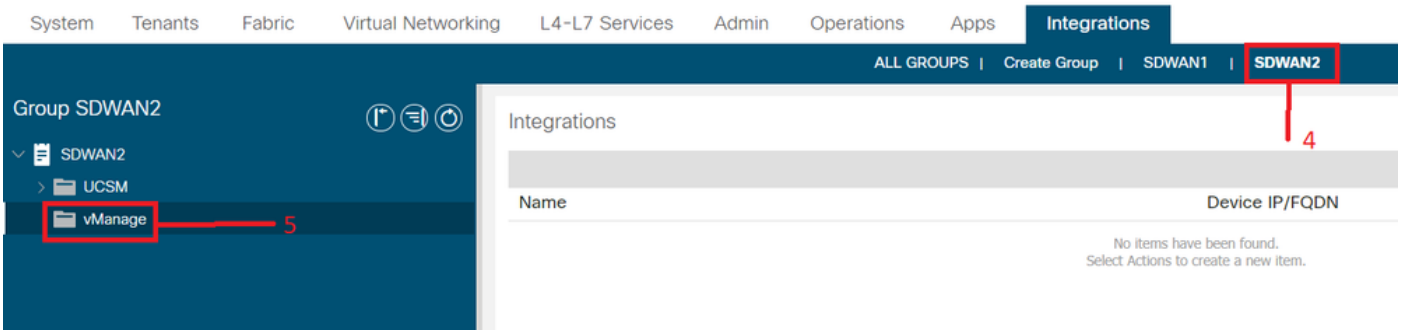
1. APIC GUI(Graphical User Interface)를 열고 System(시스템) 탭 아래의 Integrations(통합) 탭으로 이동합니다.



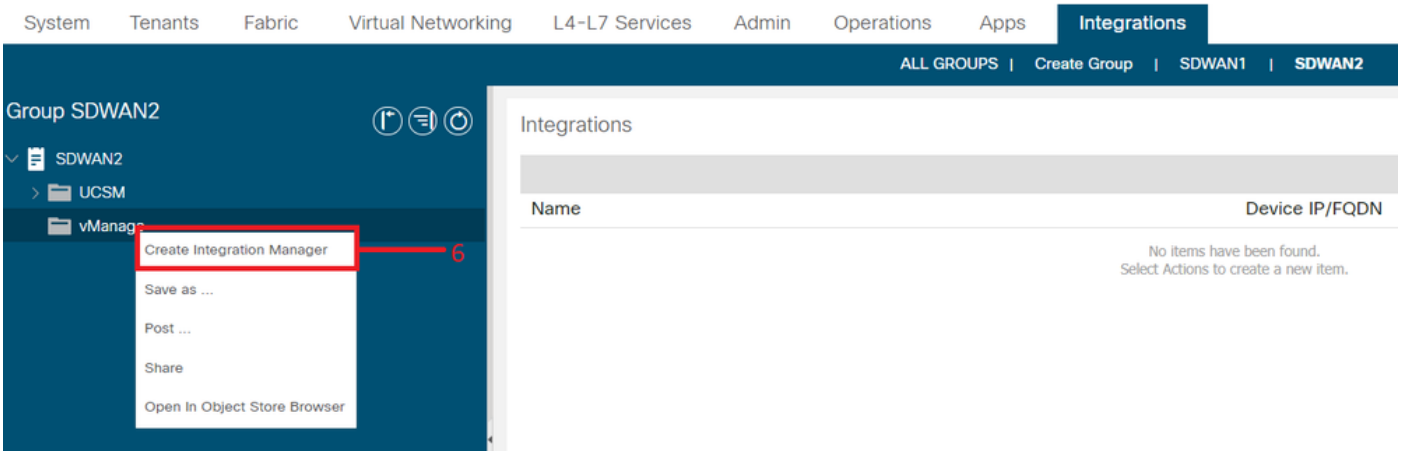
2. 통합 그룹 생성



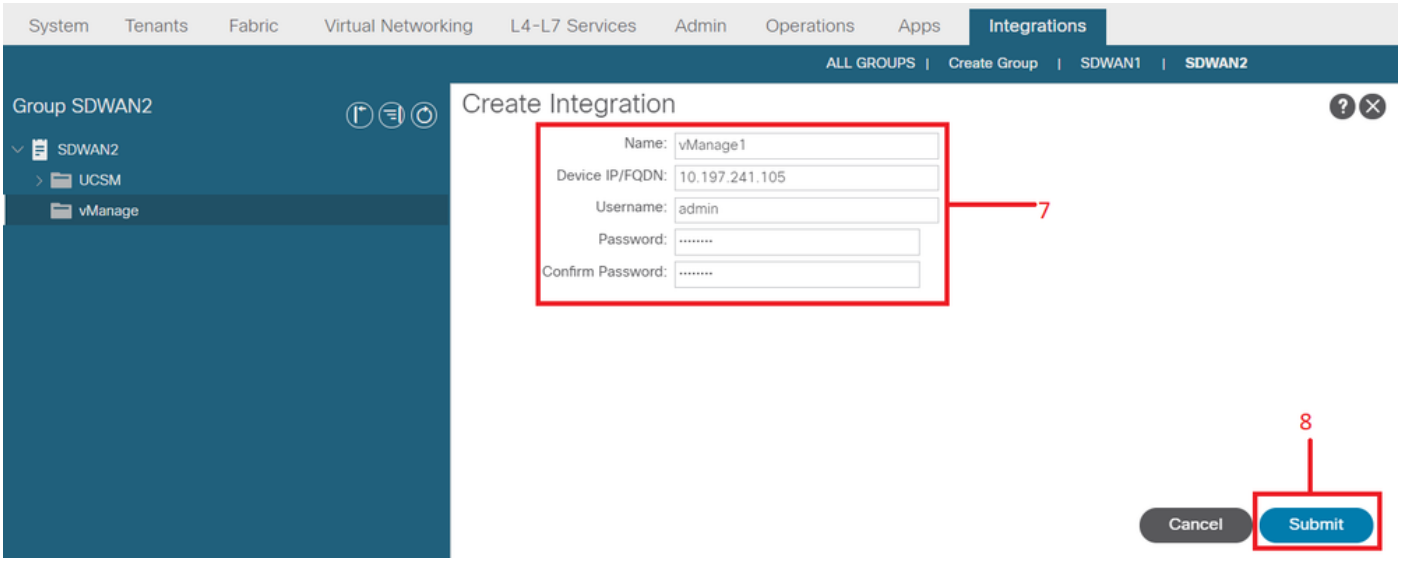
3. 새로 생성된 통합 그룹 "SDWAN2"로 이동하여 vManage를 마우스 오른쪽 버튼으로 클릭합니다



4. vManage를 마우스 오른쪽 버튼으로 클릭하고 Integration Manager 생성을 선택합니다.



5. Integration Manager 이름, 디바이스 IP/FQDN, 사용자 이름, 비밀번호 등 적절한 세부 정보를 입력합니다.



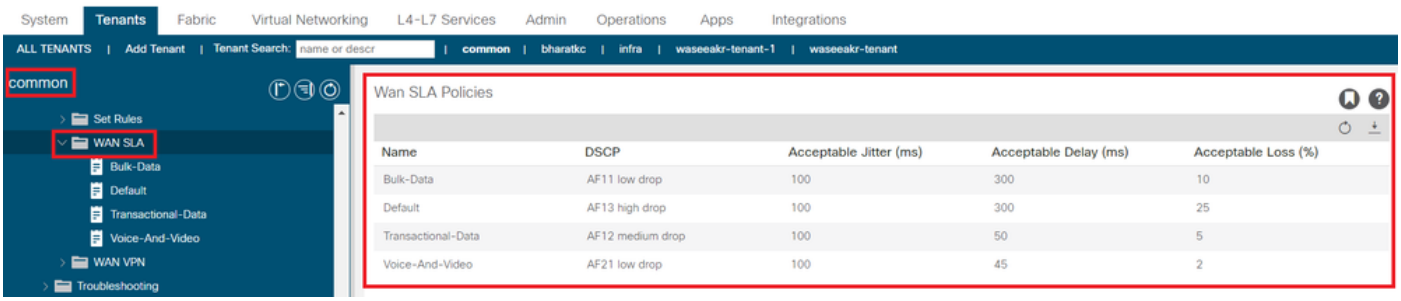
6. 상태 필드에서 등록이 성공했는지 확인합니다. 성공하지 못하거나 오류가 발견되면 제공된 정보가 정확한지 확인합니다. 파트너 ID는 vManage 컨트롤러의 식별자입니다. Integrations -><그룹 이름>->vManage -> <Integration Manager 이름> -> 시스템 정보로 이동하여 상태를 확인할 수 있습니다.

섹션 B: WAN SLA 정책 컨피그레이션

사전 구성된 WAN SLA 프로필은 Tenants(테넌트)->common(공통)->Policies(정책)->Protocols(프로토콜)->WAN SLA에서 찾을 수 있습니다.

이는 WAN SLA 정책을 사용하여 계약을 구성하는 동안 다른 테넌트에서 상속될 수 있습니다.

이는 사전 구성된 SLA이며 변경할 수 없습니다.

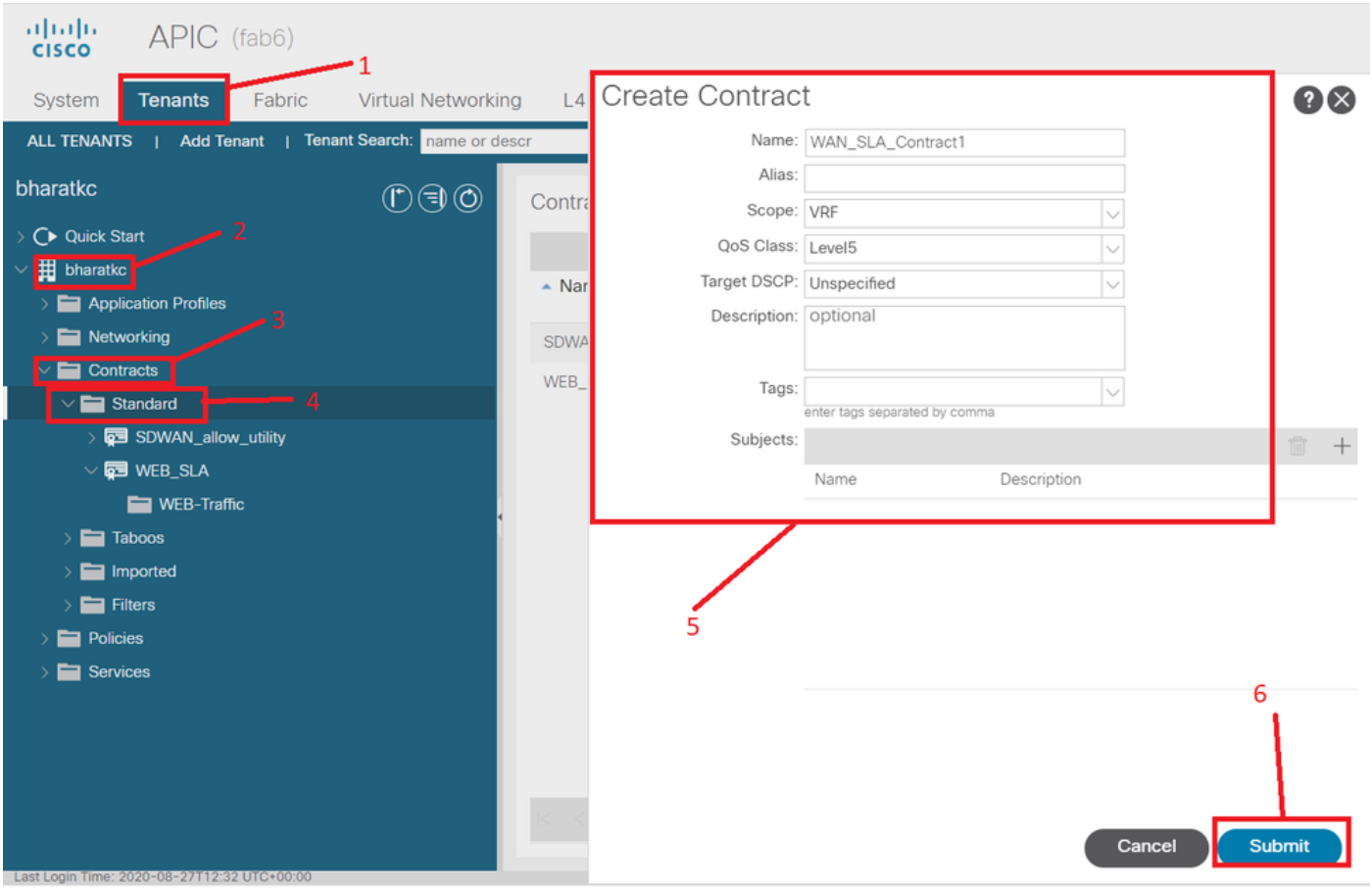


이 ACI 통합에 매핑된 SD-WAN 측에 구성된 VPN도 Tenants(테넌트)->common(공통)->Policies(정책)->Protocols(프로토콜)->WAN SLA에 반영됩니다.

1. WAN 서비스를 매핑할 테넌트/VRF에서 계약을 생성합니다.

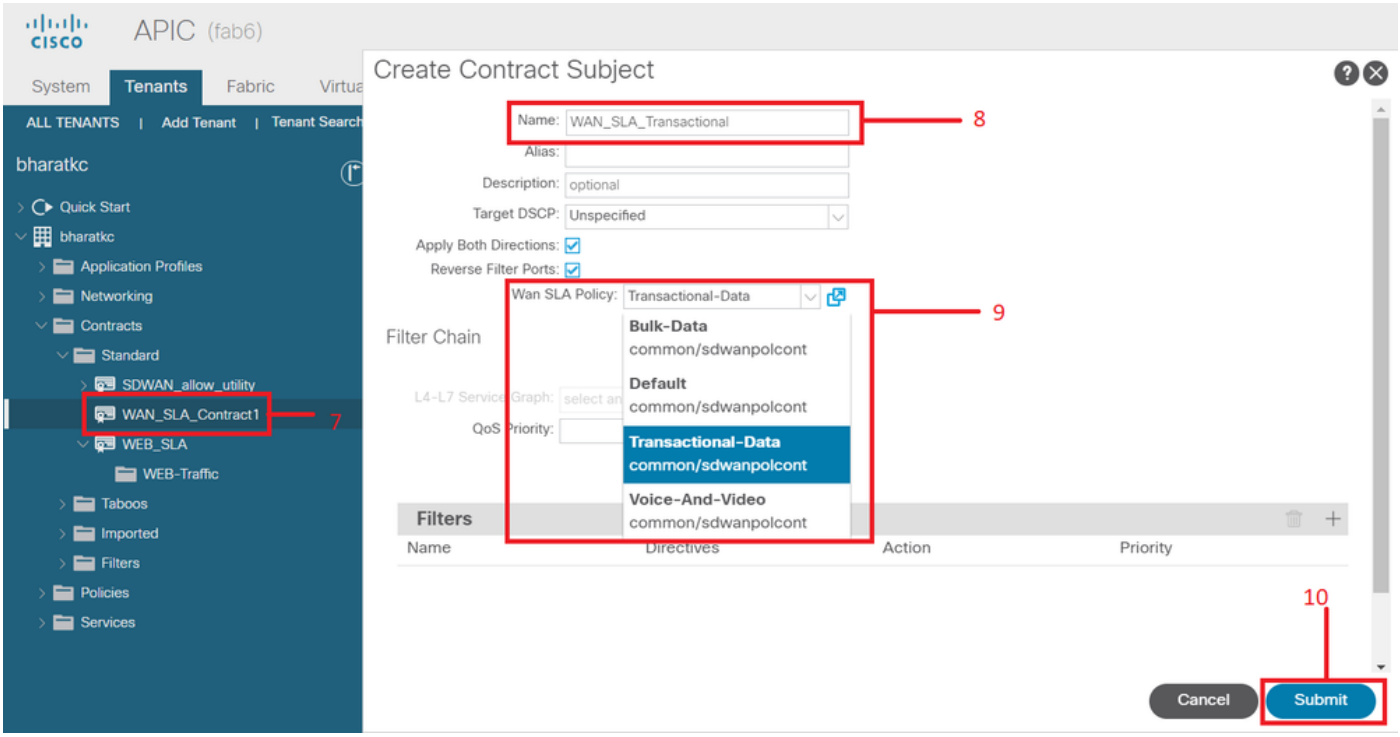
QoS Priority(QoS 우선순위) 값은 Unspecified(미지정) 이외의 값으로 설정해야 합니다. QoS Priority(QoS 우선순위) 값이 Unspecified(미지정)로 설정된 경우 WAN SLA 정책이 작동하지 않습니다.

Tenants(테넌트) -><tenant name(테넌트 이름)->Contracts(계약)->Standard(표준)로 이동하십시오.



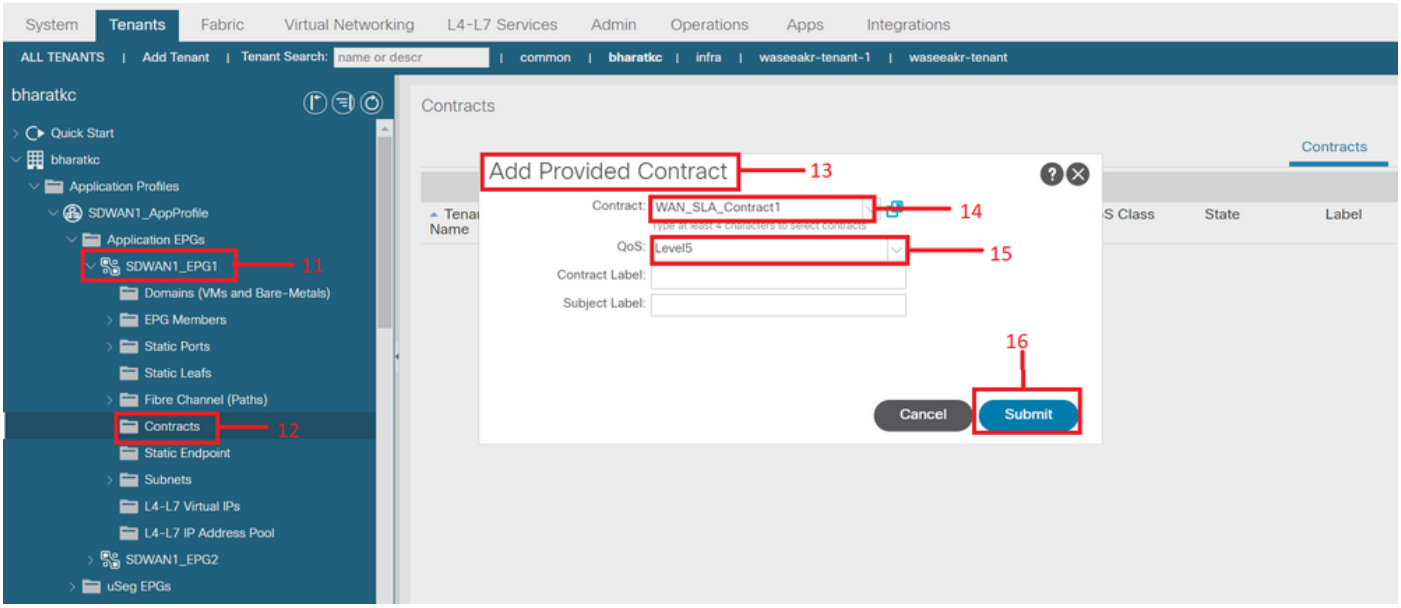
2. Contract Subject(계약 주체)를 생성하고 Contract Subject(계약 주체)에서 WAN SLA Policy(WAN SLA 정책)를 지정합니다.

QoS Priority(QoS 우선순위) 값은 Unspecified(미지정) 이외의 값으로 설정해야 합니다. QoS Priority(QoS 우선순위) 값이 Unspecified(미지정)로 설정된 경우 WAN SLA 정책이 작동하지 않습니다.



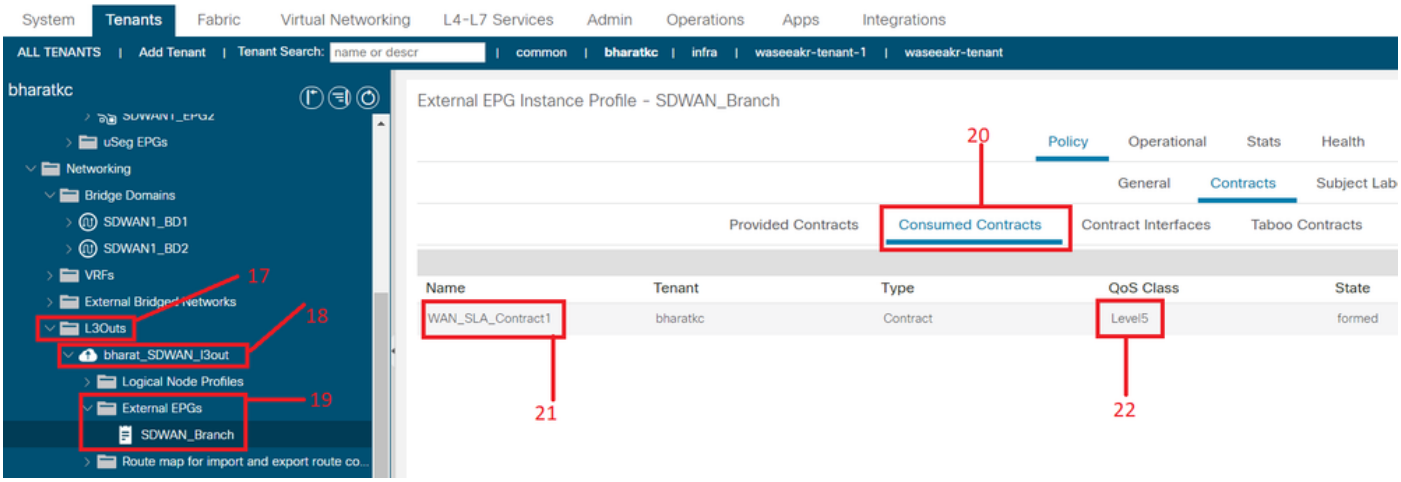
3. EPG에서 계약을 제공합니다.

Tenants(테넌트) -><tenant name(테넌트 이름)->Application Profiles(애플리케이션 프로파일)->Application EPG(애플리케이션 EPG)->Contracts(계약)로 이동하십시오.



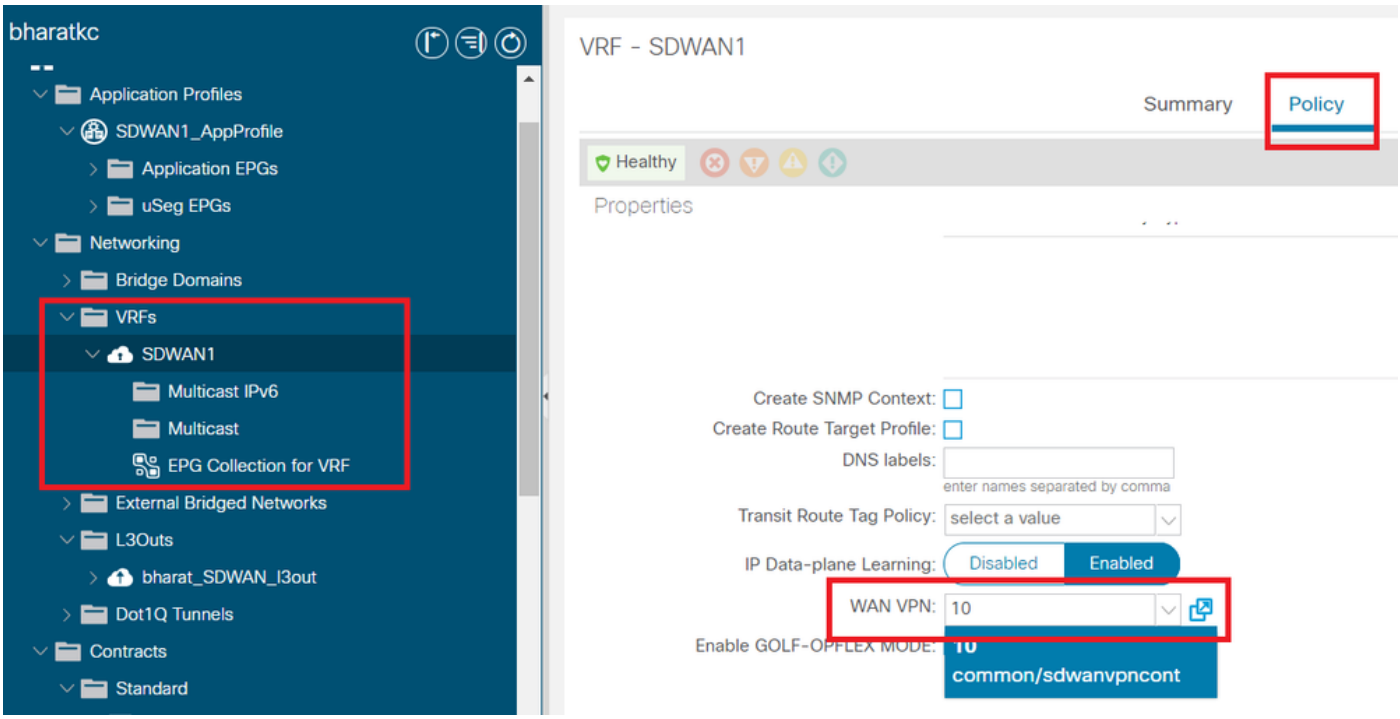
4. SD-WAN에 대해 구성된 L3out에서 계약 사용

Tenants(테넌트) -><tenant name(테넌트 이름)->L3outs(L3outs)->External EPG(외부 EPG)->Consumed Contracts(소비된 계약)로 이동하십시오. L3out 외부 EPG에서 contract를 제공하고 EPG에서 소비하는 것도 가능하고 유효합니다



5. WAN VPN을 테넌트 VRF에 일치

Tenants(테넌트) -><tenant name(테넌트 이름)->VRFs(VRF)->Policy(정책)->WAN VPN으로 이동하십시오.



다음을 확인합니다.

섹션 3: 확인

1. 컨피그레이션 확인

ACI의 컨피그레이션에 따라 컨피그레이션이 두 SDWAN 디바이스 모두에 푸시됩니다.

DC 엔드(L3out에 연결됨) SDWAN 경로

<#root>

```
ASR1001-X-DC#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)
from-vsmart sla-class Bulk-Data
 loss    10
 latency 300
 jitter  100

from-vsmart sla-class Default
 loss    25
 latency 300
 jitter  100

from-vsmart sla-class Transactional-Data
 loss    5
 latency 50
 jitter  100

from-vsmart sla-class Voice-And-Video
 loss    2
 latency 45
 jitter  100

from-vsmart data-policy _vpn-10_data_policy
 direction from-service
 vpn-list vpn-10
  default-action accept

-->>> DSCP to SLA Mapping
from-vsmart app-route-policy _412898115_vpn_412898115
 vpn-list 412898115_vpn
  sequence 10
   match
    dscp 14
   action
    sla-class Default
    no sla-class strict
  sequence 20
   match
```

```
    dscp 18
   action
    sla-class Voice-And-Video
    no sla-class strict
  sequence 30
   match
    dscp 12
   action
    sla-class Transactional-Data
    no sla-class strict
  sequence 40
   match
    dscp 10
   action
    sla-class Bulk-Data
    no sla-class strict

from-vsmart lists vpn-list 412898115_vpn
 vpn 10

from-vsmart lists vpn-list vpn-10
 vpn 10
```

```
ASR1001-X-DC#
```

브랜치 엔드 SDWAN 라우터

<#root>

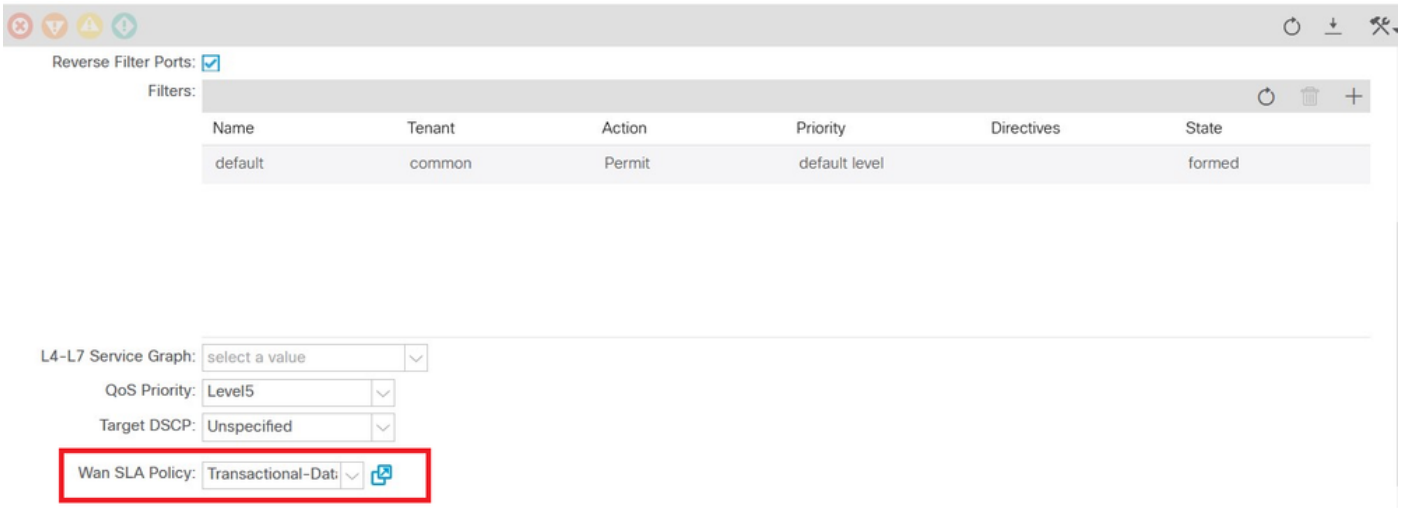
```
ASR1001-X-Branch#show sdwan policy from-vsmart
-->>> SLA Policy (parameters)
from-vsmart sla-class Bulk-Data
 loss    10
 latency 300
 jitter  100

from-vsmart sla-class Default
 loss    25
 latency 300
 jitter  100

from-vsmart sla-class Transactional-Data
 loss    5
 latency 50
 jitter  100

from-vsmart sla-class Voice-And-Video
 loss    2
 latency 45
 jitter  100

-->>> DSCP to SLA Mapping
from-vsmart app-route-policy _412898115_vpn_412898115
 vpn-list 412898115_vpn


sequence 10


   match


    dscp 14


   action


    sla-class Default


    no sla-class strict


  sequence 20


   match
```

```
    dscp 18
   action
    sla-class Voice-And-Video
    no sla-class strict
  sequence 30
   match
    dscp 12
   action
    sla-class Transactional-Data
    no sla-class strict
  sequence 40
   match
    dscp 10
   action
    sla-class Bulk-Data
    no sla-class strict

from-vsmart lists vpn-list 412898115_vpn
 vpn 10

ASR1001-X-Branch#
```

1. QoS 확인

예 1

WAN SLA 정책 "트랜잭션 데이터". Tenants(테넌트) -><tenant name(테넌트 이름)->Contracts(계약)->Standard(표준)-><Contract Name(계약 이름)>-><Contract Subject(계약 주체)>-> General(일반)- WAN SLA Policy(WAN SLA 정책)로 이동하십시오.



<#root>

```
  sequence 30
   match
```

dscp 12

```
   action
    sla-class
```

Transactional-Data

```
    no sla-class strict
```

방향:

1. DC에서 SDWAN으로의 트래픽.

아래 캡처에서 볼 수 있듯이, DC에서 시작된 트래픽은 dscp 00이지만 SDWAN에 도달하는 트래픽은 DSCP 12(16진수 0x0c)를 사용합니다.

이는 WAN SLA 정책에 따른 DSCP 값 변경을 나타냅니다.

소스(DC)에서 수행된 패킷 캡처는 원래 DSCP 값을 0으로 반영합니다.

인터넷 프로토콜, 소스: 192.168.10.2(192.168.10.2), 일광 절약 시간: 172.16.20.2(172.16.20.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x00(DSCP 0x00: 기본값, ECN: 0x00)

0000 00... = 차등 서비스 코드포인트: 기본값(0x00)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa0d5(41173)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 255

프로토콜: ICMP(0x01)

헤더 체크섬: 0x9016 [correct]

[좋음: 참]

[불량: False]

출처: 192.168.10.2(192.168.10.2)

대상: 172.16.20.2(172.16.20.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0xc16a [correct]

식별자: 0x4158

시퀀스 번호: 768(0x0300)

데이터(56바이트)

WAN SLA 정책에 따라 DSCP 12(16진수 0x0c) 값의 변경 사항을 반영하는 대상(SDWAN 브랜치 사이트)의 패킷 캡처

인터넷 프로토콜, 소스: 192.168.10.2(192.168.10.2), 일광 절약 시간: 172.16.20.2(172.16.20.2)

버전: 4

헤더 길이: 20바이트

Differentiated Services(차별화된 서비스) 필드: 0x30(DSCP 0x0c: Assured Forwarding 12, ECN: 0x00)

0011 00... = 차별화된 서비스 코드포인트: Assured Forwarding 12(0x0c)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa0d1(41169)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 251

프로토콜: ICMP(0x01)

헤더 체크섬: 0x93ea [correct]

[좋음: 참]

[불량: False]

출처: 192.168.10.2(192.168.10.2)

대상: 172.16.20.2(172.16.20.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0x6e30 [correct]

식별자: 0xc057

시퀀스 번호: 1024(0x0400)

데이터(56바이트)

2. SDWAN에서 DC로의 트래픽

아래 캡처에서 볼 수 있듯이 SDWAN 브랜치 사이트에서 시작된 트래픽은 dscp 00이지만 DC에 도달하는 트래픽은 WAN SLA 정책에 따라 DSCP 값의 변화를 반영하는 DSCP 12(16진수 0x0c)를 사용합니다.

소스(SDWAN 브랜치)에서 수행된 패킷 캡처는 원래 DSCP 값을 00으로 반영합니다.

인터넷 프로토콜, 소스: 172.16.20.2(172.16.20.2), Dst: 192.168.10.2(192.168.10.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x00(DSCP 0x00: 기본값, ECN: 0x00)

0000 00... = 차등 서비스 코드포인트: 기본값(0x00)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa0c8(41160)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 255

프로토콜: ICMP(0x01)

헤더 체크섬: 0x9023 [correct]

[좋음: 참]

[불량: False]

출처: 172.16.20.2(172.16.20.2)

대상: 192.168.10.2(192.168.10.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0xd3ff [correct]

식별자: 0x5c79

시퀀스 번호: 1(0x0001)

데이터(56바이트)

WAN SLA 정책에 따라 DSCP 12(16진수 0x0c) 값의 변경을 반영하는 DC(대상)의 패킷 캡처

인터넷 프로토콜, 소스: 172.16.20.2(172.16.20.2), Dst: 192.168.10.2(192.168.10.2)

버전: 4

헤더 길이: 20바이트

Differentiated Services(차별화된 서비스) 필드: 0x30(DSCP 0x0c: Assured Forwarding 12, ECN: 0x00)

0011 00... = 차별화된 서비스 코드포인트: Assured Forwarding 12(0x0c)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa073(41075)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 251

프로토콜: ICMP(0x01)

헤더 체크섬: 0x9448 [correct]

[좋음: 참]

[불량: False]

출처: 172.16.20.2(172.16.20.2)

대상: 192.168.10.2(192.168.10.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0x741a [correct]

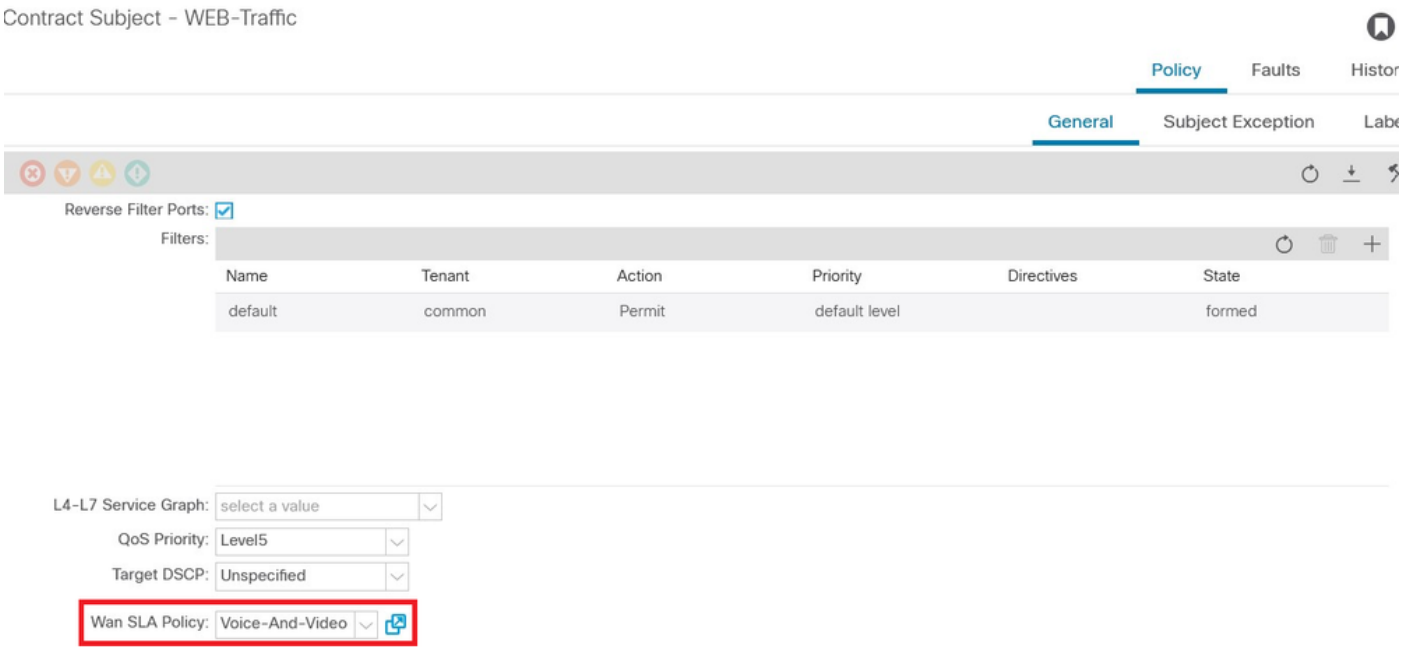
식별자: 0x5c79

시퀀스 번호: 43776(0xab00)

데이터(56바이트)

예 2

WAN SLA 정책 "Voice-And-Video" 테넌트-><테넌트 이름>->계약->표준-><계약 이름>-><계약 주체>-> 일반- WAN SLA 정책으로 이동하십시오.



<#root>

```
  sequence 20
   match
```

dscp 18

```
   action
```

sla-class Voice-And-Video

```
    no sla-class strict
```

1. DC에서 SDWAN으로의 트래픽.

아래 캡처에서 볼 수 있듯이, DC에서 시작된 트래픽은 DSCP 00이지만 SDWAN으로 향하는 트래픽은 DSCP 18(16진수 0x12)입니다.

이는 WAN SLA 정책에 따른 DSCP 값 변경을 나타냅니다.

소스(DC)에서 수행된 패킷 캡처는 원래 DSCP 값을 0으로 반영합니다.

인터넷 프로토콜, 소스: 192.168.10.2(192.168.10.2), 일광 절약 시간: 172.16.20.2(172.16.20.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x00(DSCP 0x00: 기본값, ECN: 0x00)

0000 00... = 차등 서비스 코드포인트: 기본값(0x00)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa2b6(41654)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 255

프로토콜: ICMP(0x01)

헤더 체크섬: 0x8e35 [correct]

[좋음: 참]

[불량: False]

출처: 192.168.10.2(192.168.10.2)

대상: 172.16.20.2(172.16.20.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0x3614 [correct]

식별자: 0x8c5f

시퀀스 번호: 512(0x0200)

데이터(56바이트)

DSCP 값 18(0x12)의 변경 사항을 WAN SLA 정책과 일치시키는 대상(SDWAN 브랜치 사이트)의 패킷 캡처

인터넷 프로토콜, 소스: 172.16.20.2(172.16.20.2), Dst: 192.168.10.2(192.168.10.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x48(DSCP 0x12: Assured Forwarding 21, ECN: 0x00)

0100 10.. = 차별화된 서비스 코드포인트: Assured Forwarding 21(0x12)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa2b8(41656)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 255

프로토콜: ICMP(0x01)

헤더 체크섬: 0x8deb [correct]

[좋음: 참]

[불량: False]

출처: 172.16.20.2(172.16.20.2)

대상: 192.168.10.2(192.168.10.2)

인터넷 제어 메시지 프로토콜

유형: 0(에코(ping) 응답)

코드: 0()

체크섬: 0x8a13 [correct]

식별자: 0x8c5f

시퀀스 번호: 1024(0x0400)

데이터(56바이트)

2. SDWAN에서 DC로의 트래픽

원본 DSCP 값(00)을 표시하는 소스(SDWAN 브랜치)의 패킷 캡처

인터넷 프로토콜, 소스: 172.16.20.2(172.16.20.2), Dst: 192.168.10.2(192.168.10.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x00(DSCP 0x00: 기본값, ECN: 0x00)

0000 00... = 차등 서비스 코드포인트: 기본값(0x00)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa1bb (41403)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 255

프로토콜: ICMP(0x01)

헤더 체크섬: 0x8f30 [correct]

[좋음: 참]

[불량: False]

출처: 172.16.20.2(172.16.20.2)

대상: 192.168.10.2(192.168.10.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0x68e5 [correct]

식별자: 0x1d03

시퀀스 번호: 2048(0x0800)

데이터(56바이트)

WAN SLA 정책에 따라 DSCP 값 18(0x12)의 변경 사항을 반영하는 DC(Destination)의 패킷 캡처

인터넷 프로토콜, 소스: 172.16.20.2(172.16.20.2), Dst: 192.168.10.2(192.168.10.2)

버전: 4

헤더 길이: 20바이트

차등 서비스 필드: 0x48(DSCP 0x12: Assured Forwarding 21, ECN: 0x00)

0100 10.. = 차별화된 서비스 코드포인트: Assured Forwarding 21(0x12)

.... ..0. = ECN 가능 전송(ECT): 0

....0 = ECN-CE: 0

전체 길이: 84

식별: 0xa1bb (41403)

플래그: 0x00

0.. = 예약된 비트: 설정되지 않음

.0. = 조각화 안 함: 설정되지 않음

..0 = 추가 조각: 설정되지 않음

조각 오프셋: 0

TTL(Time to Live): 251

프로토콜: ICMP(0x01)

헤더 체크섬: 0x92e8 [correct]

[좋음: 참]

[불량: False]

출처: 172.16.20.2(172.16.20.2)

대상: 192.168.10.2(192.168.10.2)

인터넷 제어 메시지 프로토콜

유형: 8(에코(ping) 요청)

코드: 0()

체크섬: 0x68e5 [correct]

식별자: 0x1d03

시퀀스 번호: 2048(0x0800)

데이터(56바이트)

문제 해결

다음 로그 파일은 문제 해결 측면에서 유용합니다. .

제어 경로 디버깅

APIC techsupport 파일
PolicyDistributor Logs(정책 배포자 로그), PolicyManager Logs(정책 관리자 로그), PolicyElement(정책 요소), Edmgr 로그를 통해 leaf 및 spine에 푸시되는 관련 컨피그레이션에 대한 통찰력을 제공할 수 있습니다.

데이터 경로 디버깅

L3out 인터페이스의 패킷 캡처 및 vEdge 라우터의 인터페이스.

ELAM도 도울 수 있습니다.

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.