Atomic 카운터 정책 구성

목차

소개

이 문서에서는 패브릭에서 미세 카운터 정책이 작동하는 방식에 대해 설명합니다.이 기능을 사용하면 패브릭에서 트래픽 삭제/초과 패킷을 모니터링할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ACI(Application Centric Infrastructure)
- APIC 버전 1.0(3n)
- n9000-aci 버전 11.0(3n)

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.

배경 정보

이 약어는 다음 문서에서 사용됩니다.

- APIC - 애플리케이션 정책 인프라 컨트롤러
- TEP - 터널 엔드포인트
- VRF - 가상 라우팅 및 포워딩
- TCAM - Ternary Content-Addressable Memory
- EPG - 엔드포인트 그룹
- MO - 관리 개체

"문제 해결" 섹션에 포함된 몇 가지 중요한 정보를 통해 주제를 이해할 수 있습니다.가장 중요한 것은 측정되는 트래픽이 모든 원자성 카운터 정책을 활용하려면 패브릭을 통과해야 합니다(leaf > spine > leaf).동일한 leaf에 연결된 두 엔드포인트에 대한 정책을 만들면 전송 카운터가 증가하도록 허용됩니다.

Atomic 카운터 유형은 두 개 이상입니다.이 문서에서는 온디맨드 atomic 카운터 정책을 구성하는 방법을 설명합니다.관리자는 이러한 기능을 설정하거나 해제할 수 있습니다.leaf 간 트래픽을 측정하는 "always-on" atomic 카운터도 있습니다.TEP-to-TEP atomic 카운터입니다.이러한 항목은 다음과 같습니다.

- dbgIngrTep(인그레스 TEP 카운터)
- dbgEgrTep(이그레스 TEP 카운터)

각 leaf의 각 TEP에 대해 계산됩니다.이러한 수치에 대해 APIC(Application Policy Infrastructure Controller)를 폴링할 수 있지만 권장되지는 않습니다.네트워크에서 트래픽을 모니터링하려는 고객에게 가장 좋은 방법은 온디맨드 카운터를 구성하는 것입니다.

작동하기 위해 atomic 카운터는 eVXLAN 헤더에서 "M" 비트를 켜거나 끕니다.시간은 물론 "패킷"과 관련하여 증가합니다. M 비트는 패킷에 대해 어떤 은행(홀수 또는 짝수)이 증가하는지 노드에 알려줍니다.Atomic 카운터는 해당 Odd 및 Even 뱅크의 카운터에 대한 노드를 폴링하여 작동합니다.예를 들어, APIC은 구성된 온디맨드 정책 때문에 리프 1에서 홀수 은행 및 리프 4에서 짝수 은행을 측정할 수 있습니다.이를 통해 APIC는 각 은행 카운트에서 전송 및 수신된 패킷을 추출하고, 그 차이에 따라 삭제 및 초과 패킷 수를 추출할 수 있습니다.

온디맨드 정책이 구성되면 TCAM 항목이 일치하고 홀수/짝수 비트가 설정된 경우 카운터가 증가합니다.즉, atomic 카운터가 작동하기 전에 측정하려는 두 엔드포인트/엔드포인트 그룹/IP 간의 계약을 통해 정책을 설정해야 합니다.

다음은 atomic 정책 카운터를 구성할 때 고려해야 할 몇 가지 주의 사항입니다.

- 엔드포인트가 동일한 테넌트 내의 서로 다른 테넌트 또는 다른 컨텍스트(VRF)에 있는 경우 미세 카운터 사용이 지원되지 않습니다.
- IP 주소가 학습되지 않은 순수 레이어 2 컨피그레이션에서는(IP 주소는 0.0.0.0) 엔드포인트-투-EPG 및 EPG-to-endpoint atomic 카운터 정책이 지원되지 않습니다.이러한 경우 엔드포인트-투-엔드포인트 및 EPG-to-EPG 정책이 지원됩니다.외부 정책은 VRF(Virtual Routing and Forwarding) 기반이며, 여기에는 학습된 IP 주소가 필요하며 지원됩니다.
- atomic 카운터 원본 또는 대상이 끝점일 경우 끝점은 동적이어야 하며 정적이 아니어야 합니다.동적 끝점(fv:CEp)과 달리 고정 끝점(fv:StCEp)에는 atomic 카운터에 필요한 자식 개체(fv:RsCEpToPathEp)가 없습니다.
- 리프 스위치가 모든 스파인 스위치로 풀 메쉬에 있지 않은 트랜짓 토폴로지에서 leaf-to-

leaf(TEP to TEP) 카운터가 예상대로 작동하지 않습니다.
- Leaf-to-Leaf(TEP에서 TEP) atomic 카운터의 경우 터널 수가 하드웨어 제한을 늘리면 시스템은 Trail 모드에서 Path Mode로 모드를 변경하며 사용자는 더 이상 Spine당 트래픽이 표시되지 않습니다.
- atomic 카운터는 스파인 프록시 트래픽을 계산하지 않습니다.
- 패브릭에 들어가기 전 또는 리프 포트로 전달되기 전에 삭제된 패킷은 미세 카운터에서 무시됩니다.
- 하이퍼바이저에서 전환되는 패킷(동일한 포트 그룹 및 호스트)은 계산되지 않습니다.
- atomic 카운터에는 활성 NTP(Fabric Network Time Protocol) 정책이 필요합니다.
- fvCEp를 소스 및/또는 대상으로 구성한 atomic 카운터 정책은 fvCEp MO(managed objects)에 있는 MAC 및 IP 주소 간 트래픽만 계산합니다. fvCEp MO에 빈 IP 주소 필드가 있는 경우 IP 주소에 관계없이 해당 MAC 주소로 들어오거나 들어오는 모든 트래픽이 계산됩니다.APIC에서 fvCEp에 대해 여러 IP 주소를 학습한 경우 fvCEp MO 자체에 있는 하나의 IP 주소로부터의 트래픽은 이전에 설명한 대로 계산됩니다.특정 IP 주소에 대한 미세 카운터 정책을 구성하려면 fvIp MO를 소스 및/또는 대상으로 사용합니다.
- fvCEp 뒤에 fvIp가 있는 경우 fvCEp 기반 정책이 아니라 fvIP 기반 정책을 추가해야 합니다.

자세한 내용은 Cisco APIC 트러블슈팅 가이드 - Atomic 카운터 지침 및 제한 사항을 참조하십시오.

구성

atomic 카운터 정책을 구성하려면 다음 단계를 완료하십시오.

1. 구성할 atomic 카운터 정책의 유형을 결정합니다.
2. 정책을 생성합니다.
3. 정책에 사용할 필터를 추가합니다.

구성할 atomic 정책의 유형 결정

이러한 유형의 온디맨드 atomic 카운터 정책을 구성할 수 있습니다.

- EP에서 EP로
- EP에서 EPG로
- EP에서 내선
- EPG에서 EP로
- EPG에서 EPG로
- IP에 EPG
- IP로 확장
- IP-EPG

각 약어의 의미는 다음과 같습니다.

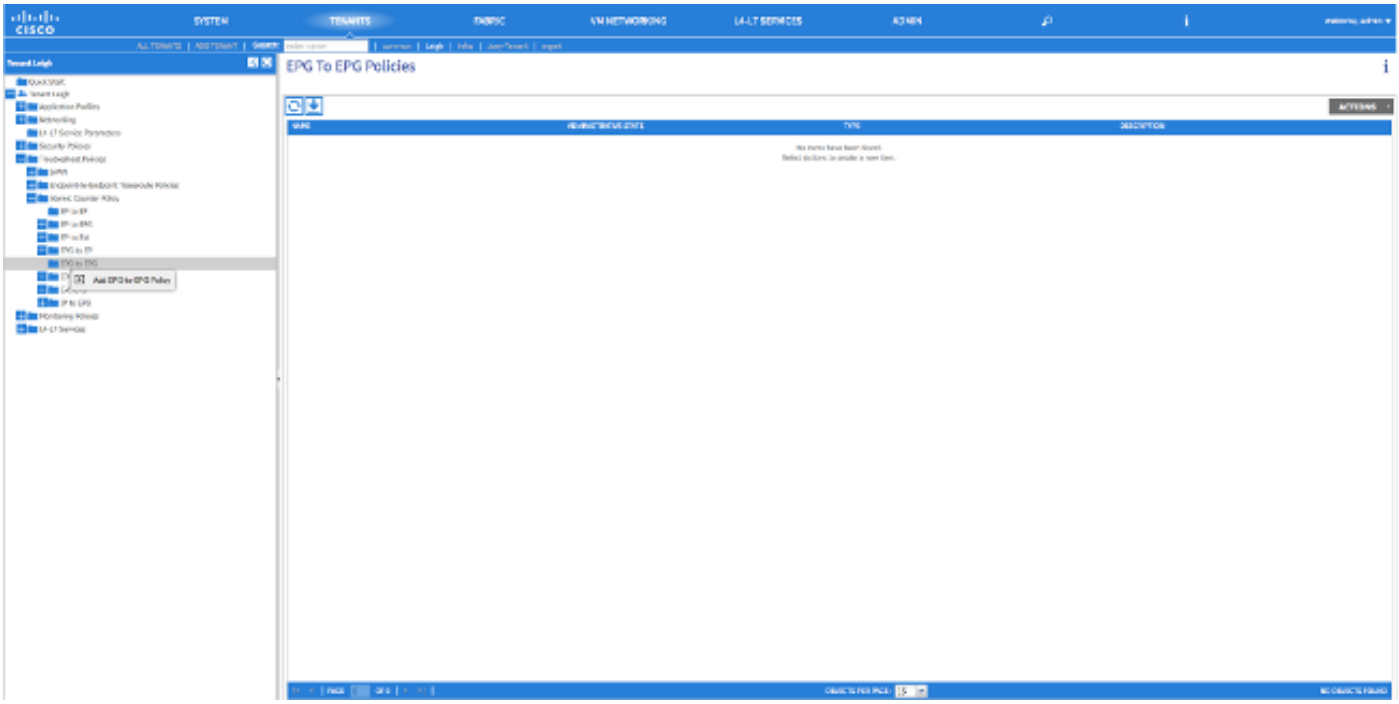
- EP - 엔드포인트
- EPG - 엔드포인트 그룹
- 외부 네트워크
- IP - IP 주소

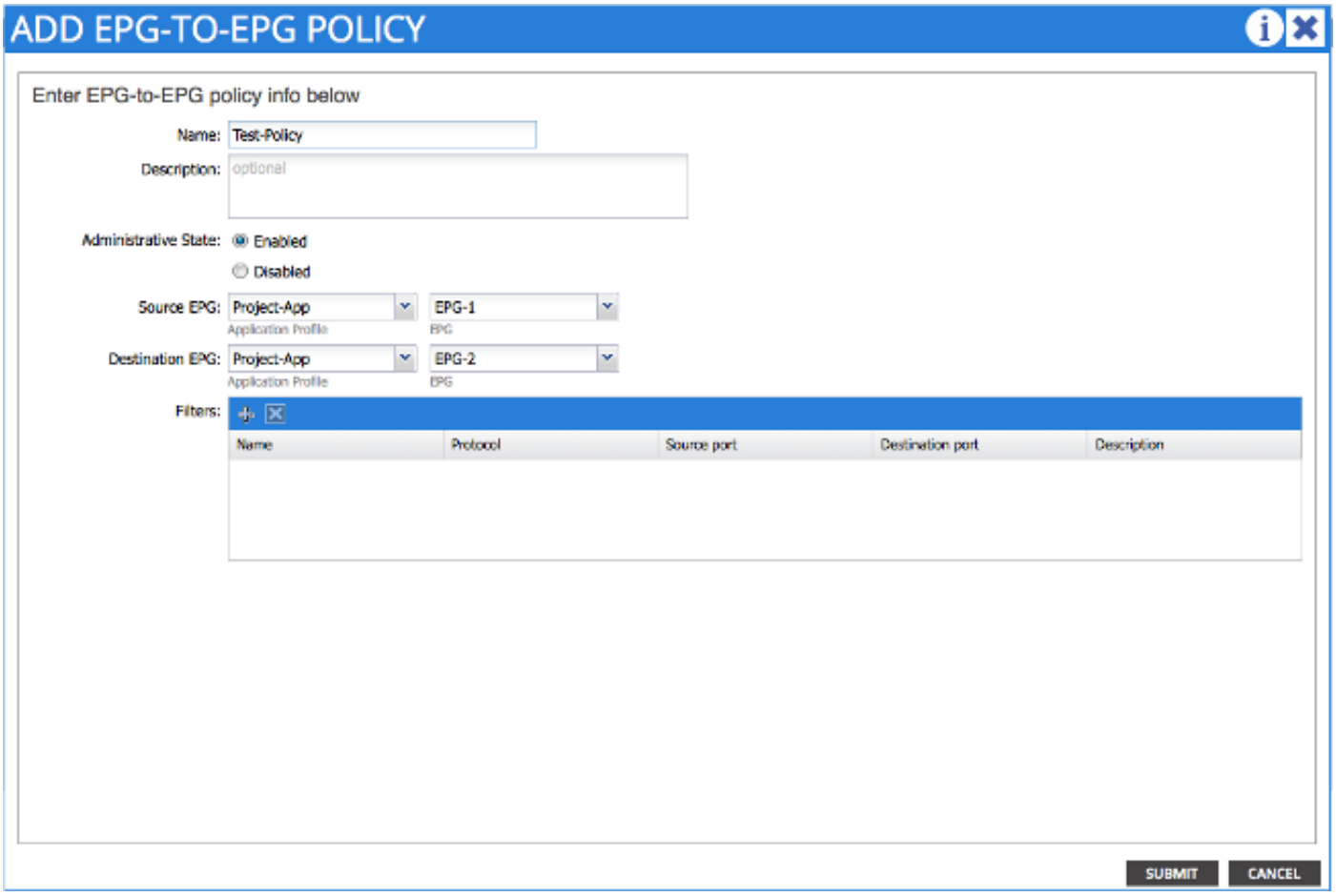
EP 기반 정책의 경우 정책을 구성하기 전에 패브릭에서 엔드포인트를 이미 학습해야 합니다.

구성하도록 선택하는 정책 유형에 따라 다음 섹션에서 구성해야 하는 매개변수가 결정됩니다.

정책 생성

이 섹션에서 사용되는 스크린샷은 EPG-EPG 정책을 위한 것입니다.보기는 구성하는 유형에 따라 달라질 수 있지만 핵심 개념은 동일합니다.





EP에서 EP로

두 소스 유형 중에서 선택할 수 있습니다.EP 및 IP.EP를 선택하는 경우 패브릭에서 학습된 엔드포

인트를 선택합니다.IP를 선택하는 경우 패브릭에서 학습된 엔드포인트와 IP 주소를 선택합니다.이를 통해 특정 엔드포인트와 엔드포인트 뒤에 있을 특정 IP 호스트 간에 더 세부적으로 결정할 수 있습니다.

EPG에서 EPG로

정책의 소스 및 대상 EPG를 선택합니다.이는 소스 EPG의 모든 엔드포인트에서 대상 EPG의 엔드포인트로 이동하는 트래픽을 측정합니다.

EP에서 EPG로

소스를 선택하는 프로세스는 "EP to EP" 정책과 동일합니다.대상을 선택하는 프로세스는 "EPG to EPG" 정책과 동일합니다.

EP에서 내선

소스를 선택하는 프로세스는 "EP to EP" 정책과 동일합니다.카운터의 대상으로 사용할 패브릭 외부에 IP 주소를 지정하려면 "외부 IP"를 입력해야 합니다.주소 뒤에 "/"를 입력하고 서브넷 크기를 지정하여 특정 IP 주소 또는 IP 주소 범위를 선택할 수 있습니다.

EPG에서 EP로

소스를 선택하는 프로세스는 "EPG to EPG" 정책과 동일합니다.대상을 선택하는 프로세스는 "EP to EP" 정책과 동일합니다.

IP에 EPG

소스를 선택하는 프로세스는 "EPG to EPG" 정책과 동일합니다.대상을 선택하는 프로세스는 "EP to Ext" 정책과 동일합니다.

IP로 확장

트래픽의 소스 IP 주소를 선택하고 "Source IP" 필드에 입력합니다.특정 IP 주소 또는 IP 서브넷일 수 있습니다.대상을 선택하는 프로세스는 "EP to EP" 정책과 동일합니다.

IP-EPG

소스를 선택하는 프로세스는 "Ext to IP" 정책과 동일합니다.대상을 선택하는 프로세스는 "EPG to EPG" 정책과 동일합니다.

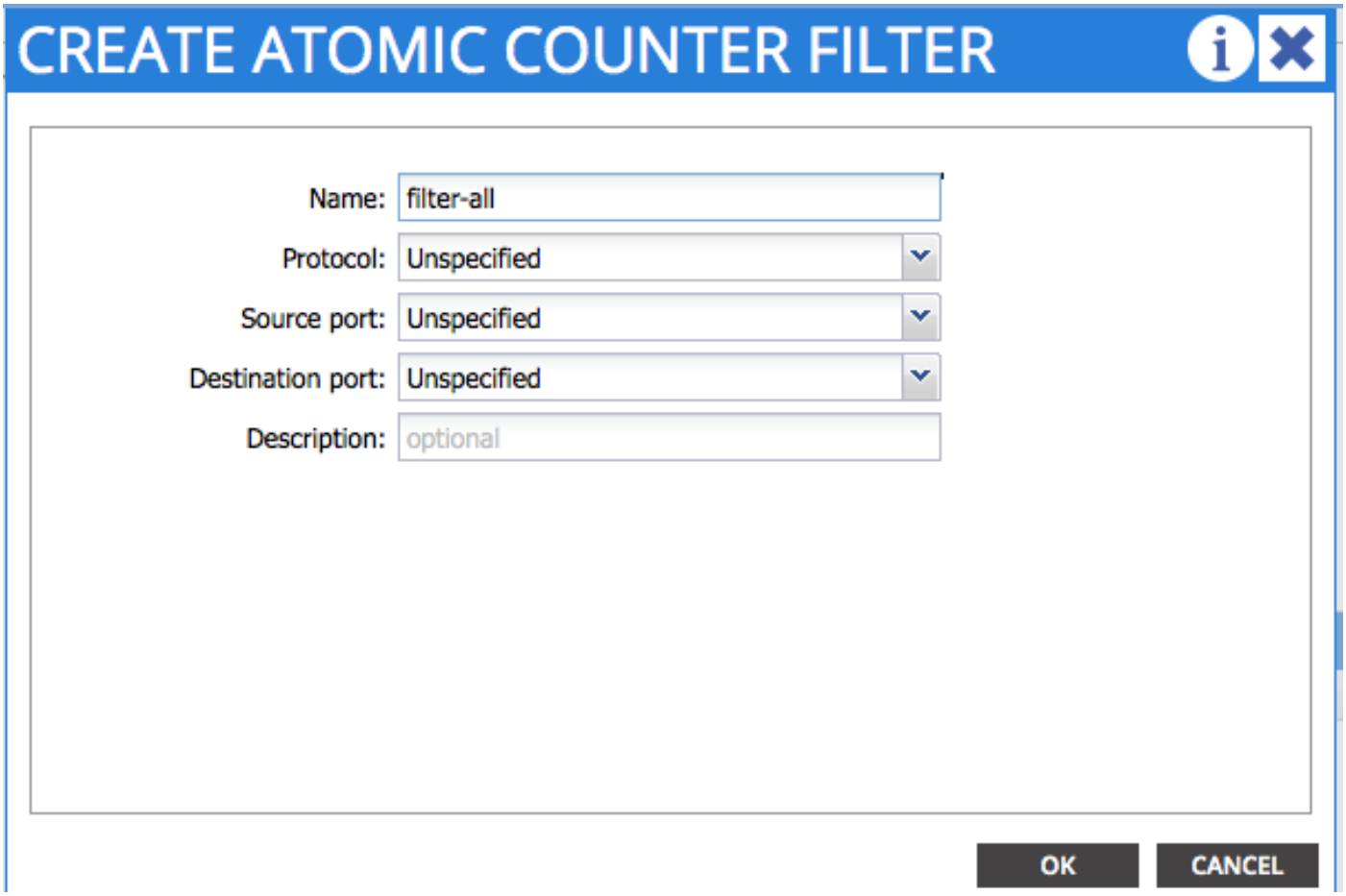
정책에 사용할 필터 추가

여기서 볼 수 있는 화면은 구성한 정책의 유형에 관계없이 일관됩니다.Atomic Counter Filter는 패브릭의 Contracts에 적용하는 필터와 다른 객체 유형이지만 유사한 기능을 수행합니다.

- Name(이름) - 여기에 Atomic Counter Filter의 이름을 입력합니다.이 필터는 이 정책에만 해당되며 재사용되지 않습니다.
- 프로토콜 - 드롭다운 목록에서 프로토콜을 선택하거나 0~255 사이의 프로토콜에 해당하는 번

호를 입력할 수 있습니다. 0~255 범위의 범위는 IP 패킷 헤더에 포함된 IP 프로토콜 번호에 해당합니다.

- 소스 포트 - 드롭다운 목록에서 일반적으로 사용되는 프로토콜 중 하나를 선택하거나 0~65535 사이의 숫자를 입력할 수 있습니다.
- 대상 포트 - 드롭다운 목록에서 일반적으로 사용되는 프로토콜 중 하나를 선택하거나 0~65535 사이의 숫자를 입력할 수 있습니다.
- Description(설명) - 이는 식별에 도움이 되는 필터에 대한 설명입니다.이 필터에 의해 식별되거나 식별되지 않는 트래픽에는 영향을 주지 않습니다.



REST API를 사용하여 atomic 카운터를 구성할 수도 있습니다.다음은 EPG-to-EPG 정책을 생성하는 데 사용되는 POST 요청의 예입니다.

URL - https://**<apic-ip>**/api/node/mo/uni/tn-Leigh/epgToEpg-Test-Policy.json

JSON

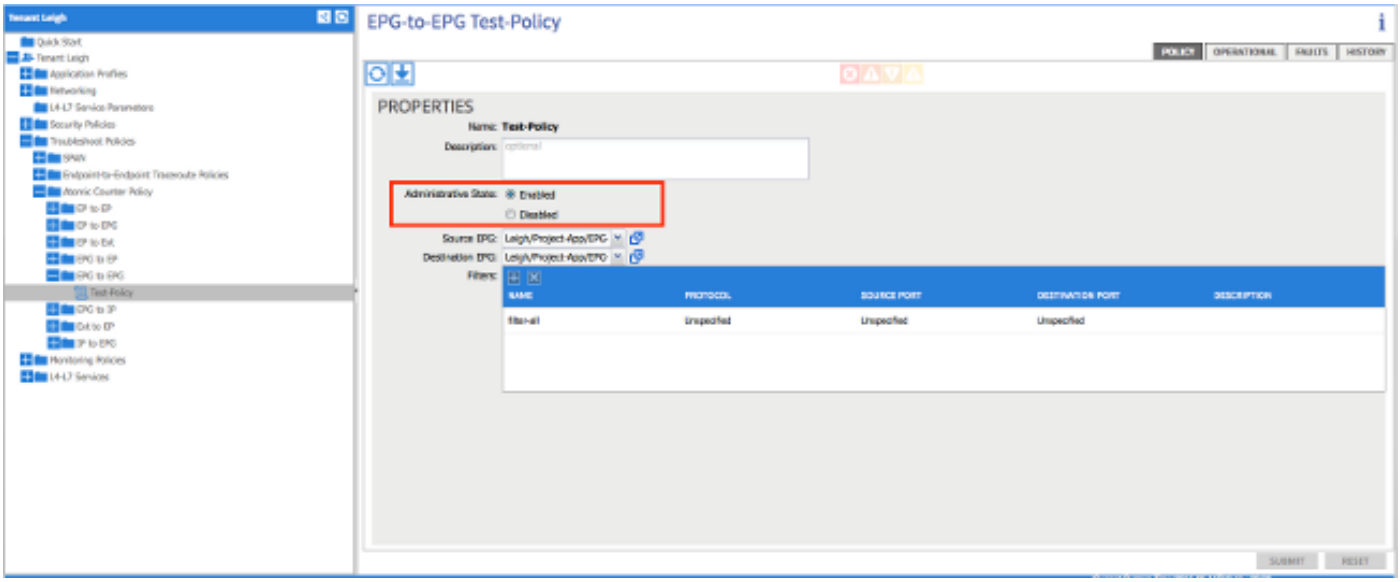
```
{"dbgacEpgToEpg":
   {"attributes":
       {"dn":"uni/tn-Leigh/epgToEpg-Test-Policy",
       "name":"Test-Policy",
       "rn":"epgToEpg-Test-Policy",
       "status":"created"},
       "children":[
            {"dbgacFilter":
                {"attributes":
                    {"dn":"uni/tn-Leigh/epgToEpg-Test-Policy/filt-filter-all",
                    "name":"filter-all",
                    "rn":"filt-filter-all",
                    "status":"created"},
```

```
                "children":[]}},
            {"dbgacRsFromEpg":
                {"attributes":
                    {"tDn":"uni/tn-Leigh/ap-Project-App/epg-EPG-1",
                    "status":"created,modified"},
                    "children":[]}},
            {"dbgacRsToEpgForEpgToEpg":
                {"attributes":
                    {"tDn":"uni/tn-Leigh/ap-Project-App/epg-EPG-2",
                    "status":"created"},
                    "children":[]
                }
            }
        ]
    }
}
```

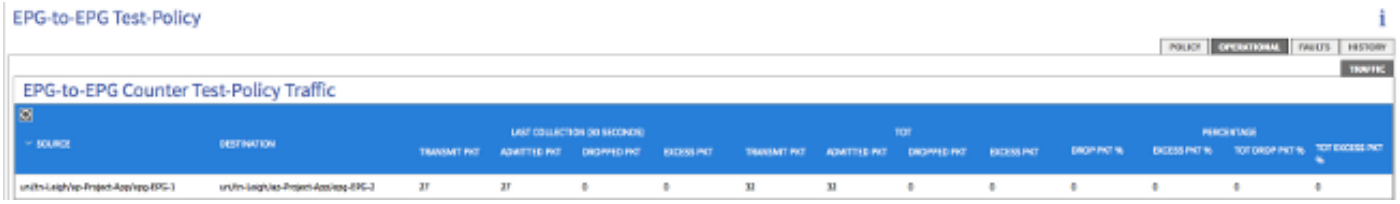
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

구성한 atomic 카운터 정책이 작동 중인지 확인하는 가장 쉬운 방법은 "Policy(정책)" 탭에서 "Administrative State(관리 상태)"가 "Enabled(활성화됨)"로 설정되었는지 확인하는 것입니다.



정책의 각 통계에 대한 카운터를 보려면 "Operational(운영)" 탭으로 이동합니다.트래픽 플로우에서 전송 및 허용 패킷의 수가 증가하는지 여기서 확인할 수 있습니다.1% 이상의 패킷이 삭제되고 5% 이상의 패킷이 삭제될 경우 주요 결함이 트리거될 경우 사소한 결함이 트리거됩니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

카운터가 증가하지 않으면 다음과 같은 몇 가지 문제가 발생할 수 있습니다.

- 정책이 활성화되었습니까?
- 정책에 대한 필터가 올바르게 구성되었습니까?
- 두 엔드포인트 또는 디바이스 간에 트래픽을 측정하는 계약이 있습니까?

정책이 올바르게 구성되고 활성화되었으며 성공적으로 테스트된 엔드포인트가 트래픽을 전달할 경우, 두 엔드포인트가 동일한 leaf에 연결되었을 가능성이 높습니다.하드웨어 아키텍처의 설계로 인해 트래픽은 leaf의 Northstar ASIC를 통해 카운터를 증가시켜야 합니다.트래픽이 하나의 leaf만 통과하는 경우 전송 카운터가 증가하기만 하면 됩니다.

삭제된 패킷 또는 초과 패킷의 수가 많을 경우 두 디바이스 간에 초과 서브스크립션이 있을 가능성이 있습니다.