ACI를 애플리케이션 중심으로 구축

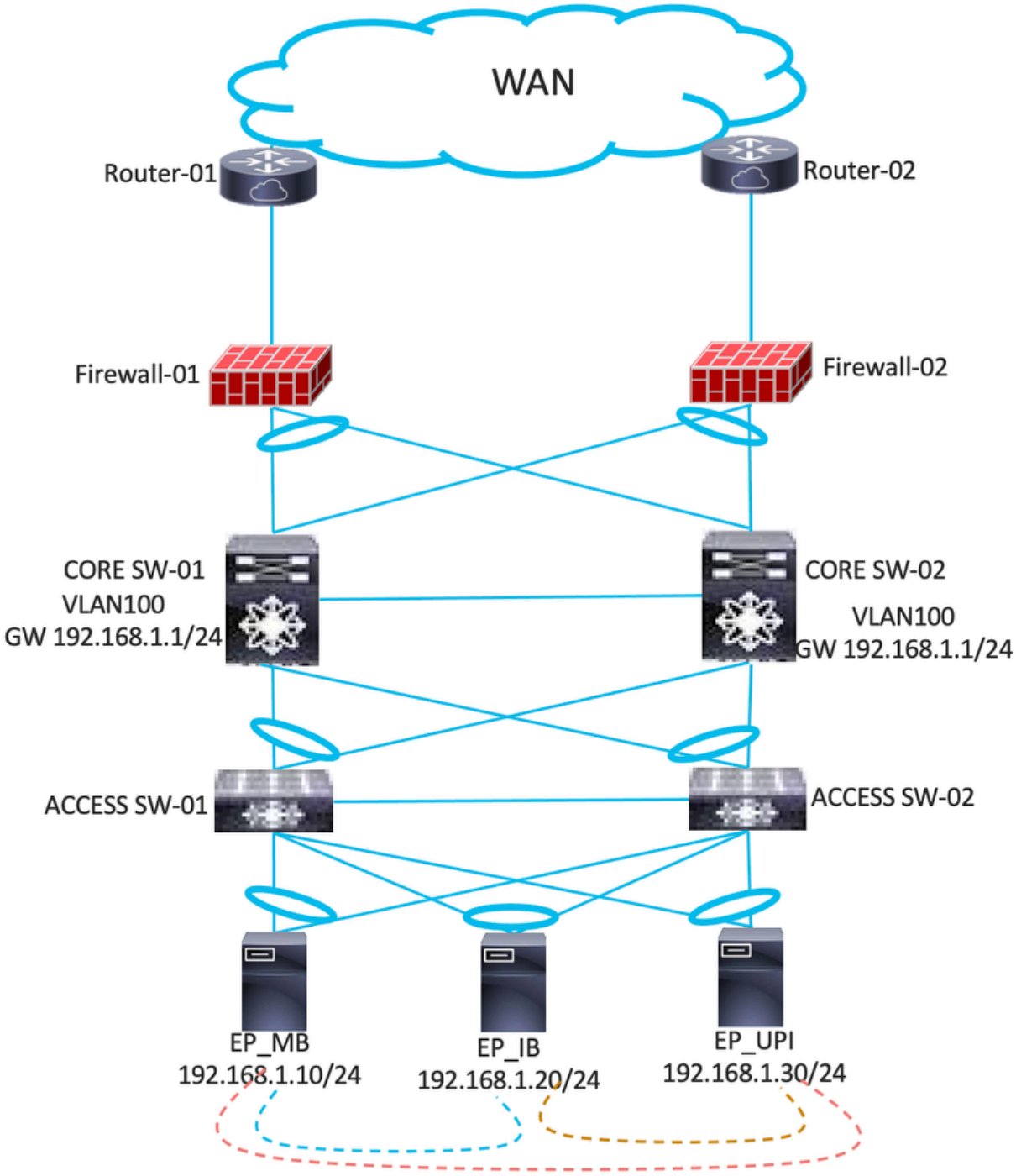
목차

소개

이 문서에서는 Cisco ACI SDN 솔루션을 활용하는 애플리케이션 내/애플리케이션 간 마이크로 세그멘테이션 및 보안을 실현하기 위한 접근 방식을 설명합니다.

기존 네트워크를 사용하는 제약 조건

- 기존 네트워크에서는 VLAN/서브넷 내에서 세그멘테이션을 수행할 수 없습니다.
- 애플리케이션 게이트웨이는 코어 스위치에 있습니다. 두 애플리케이션이 통신하려는 경우, 코어 스위치에 복잡한 ACL(Access Control List)이 필요합니다.
- 스위치 간 스패닝 트리 루프는 데이터 센터 흐름을 끊고 트래픽 감소를 초래합니다.
- 동일한 IP 서브넷에 여러 애플리케이션이 포함되어 있으며, 이러한 애플리케이션은 애플리케이션 간의 보안을 제공하지 않습니다. 기존 네트워크에서는 이러한 커뮤니케이션을 관리할 수 없습니다.
- 다이어그램을 사용하여 표시된 예를 고려하십시오. 동일한 VLAN 및 IP 서브넷에 속하는 3개의 애플리케이션 EP_MB, EP_IB 및 EP_UPI가 있습니다. 모든 L2 트래픽에서는 트래픽이 항상 모든 애플리케이션으로 플러딩되며, 이러한 애플리케이션 간의 통신이 필요하지 않습니다. 이 시나리오에서는 두 애플리케이션 간의 제한을 사용할 수 없습니다.



사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 애플리케이션 간의 트래픽 흐름 데이터를 수집하려면 Cisco CSW(Secure Workload)/Tetration(Secure Workload)을 환경에 구축해야 합니다.
- 데이터를 수집하려면 서버에 에이전트를 구축해야 합니다. 따라서 이는 브라운필드 구축의 경우에만 가능합니다.

- 에이전트는 데이터 수집을 위해 최소 3-4주 동안 서버에 구축되어야 합니다.
- ADM(Application Dependency Mapping) 툴을 사용할 수 없는 경우 관련 데이터를 제공해야 합니다.
- 서버 게이트웨이는 ACI(Application Centric Infrastructure) 패브릭을 사용하여 구성해야 합니다.

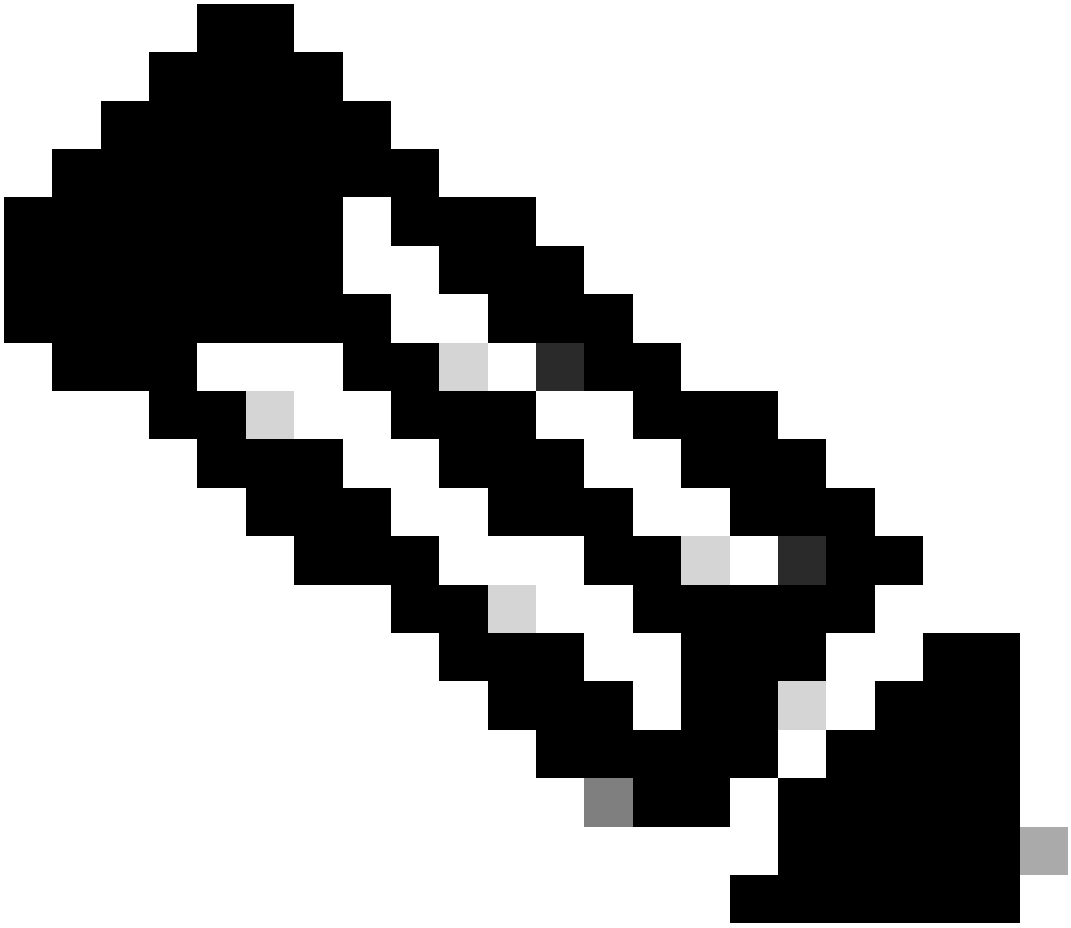
사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

솔루션 개요

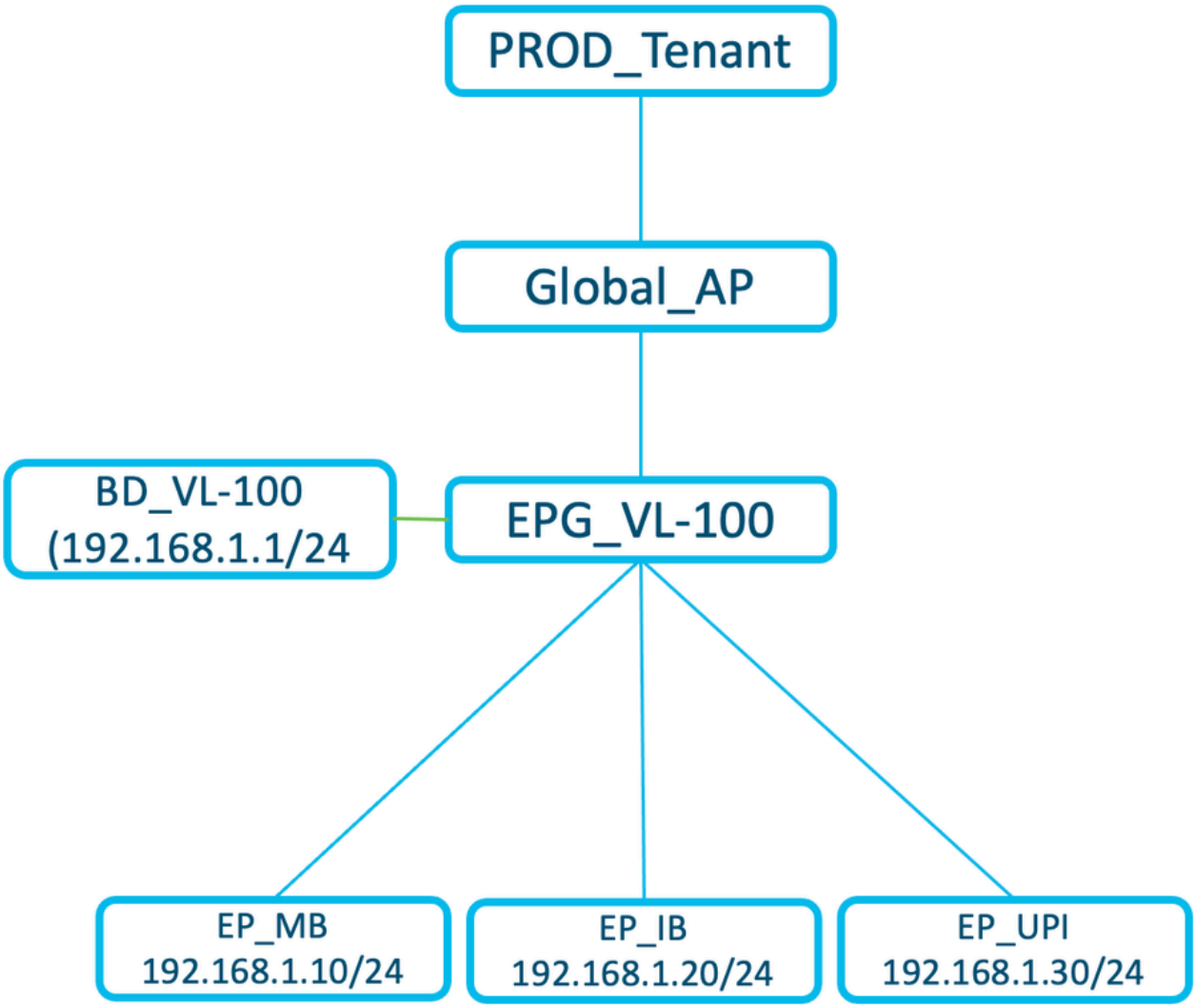
마이크로 세그멘테이션을 수행하려면 먼저 기존 인프라에서 Cisco SDN 솔루션으로 네트워크를 마이그레이션하고 애플리케이션 중심 관점에서 네트워크를 재설계해야 합니다. 이 섹션에서는 ADM 툴을 통해 캡처되는 애플리케이션 플로우를 기반으로 원하는 대로 세그멘테이션을 수행하기 위한 설계의 두 단계에 대해 설명합니다. 처음에 Cisco ACI 솔루션은 네트워크 중심 모드(기존 설계 그대로)로 구축되었다가 애플리케이션 중심 모드로 전환되었습니다.



참고: 기존 네트워크에서 애플리케이션 중심 모드로 서비스를 직접 마이그레이션하기 위해 이 구축 모드를 함께 결합할 수도 있습니다.

네트워크 중심 설계

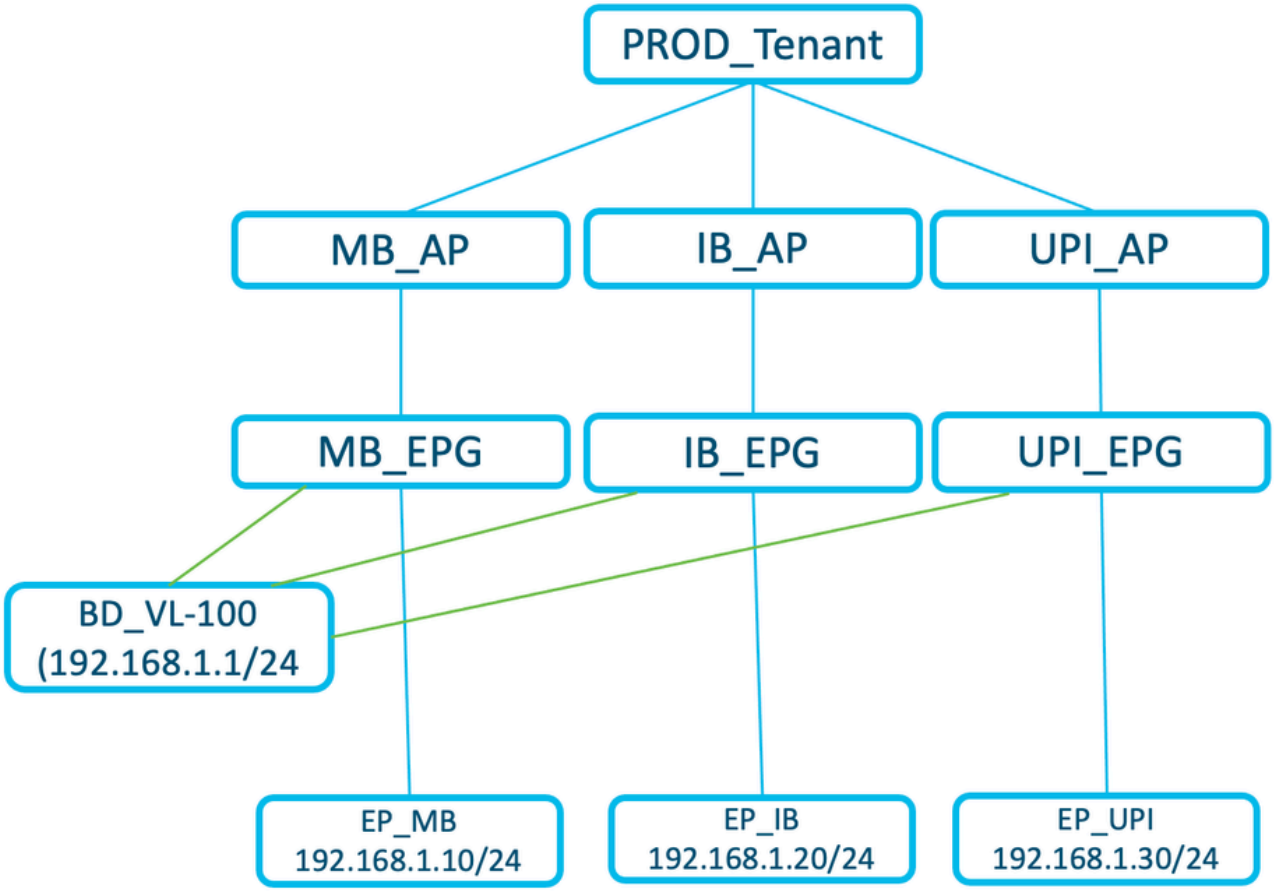
다이어그램에 나와 있는 예에서 EPG_VL-100은 EP_MB, EP_IB 및 EP_UPI의 세 가지 애플리케이션을 포함하며 동일한 IP 서브넷을 공유하며 VLAN 100을 사용합니다.



- 기존 네트워크에서 ACI로 현재 상태 마이그레이션
- 하나의 엔드포인트 그룹(EPG)에 여러 애플리케이션이 포함될 수 있습니다.
- 이 구축 유형의 동일한 EPG 내에 애플리케이션 세그멘테이션이 없습니다.
- 1 BD = 1 EPG = 1 VLAN

애플리케이션 중심 설계

다이어그램에 표시된 예는 동일한 IP 서브넷을 공유하고 각 EPG에 매핑된 서로 다른 VLAN을 사용하는 3개의 애플리케이션 EP_MB, EP_IB 및 EP_UPI에 대한 별도의 EPG입니다.

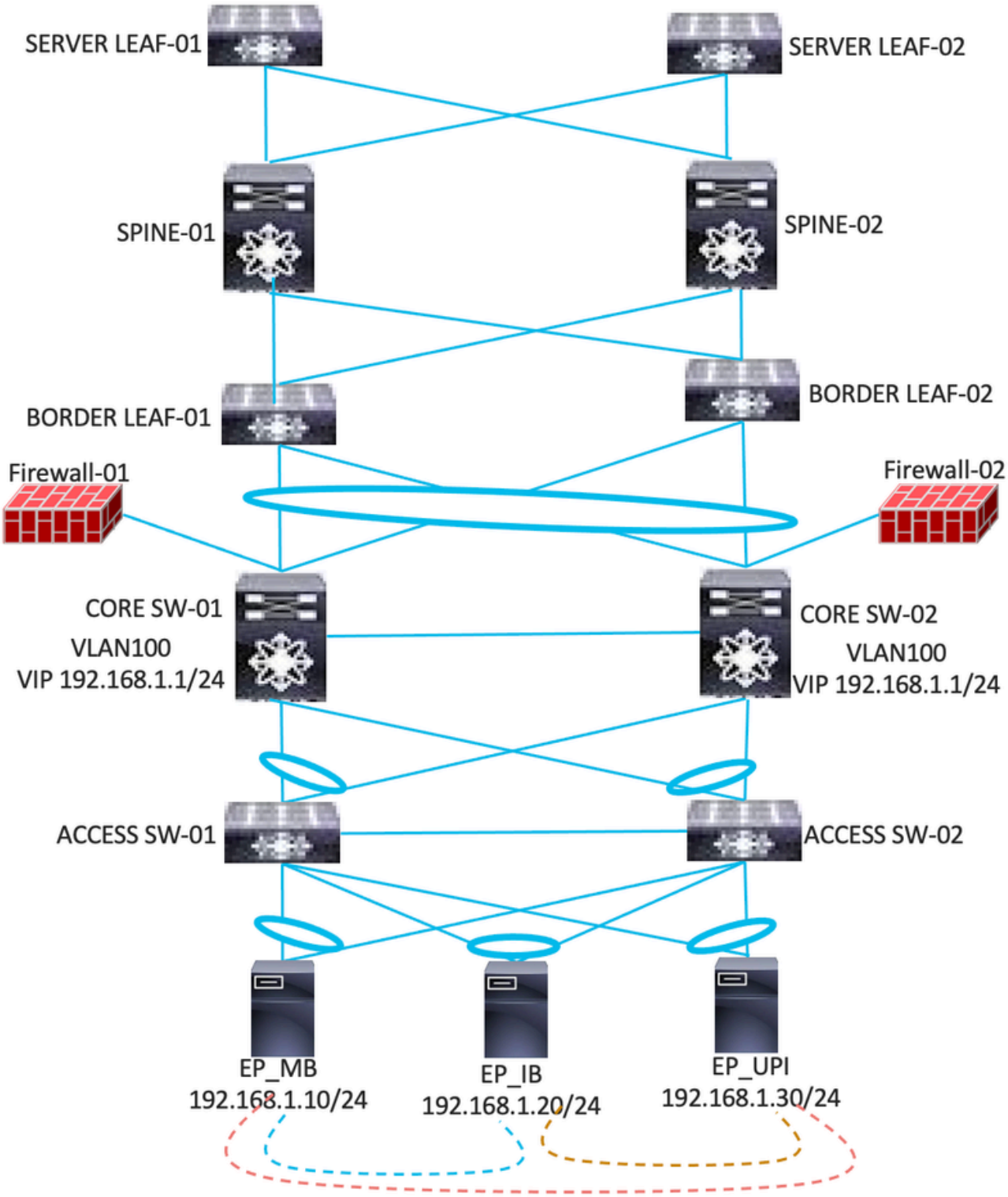


- Application-Centric 구축 유형에서는 애플리케이션에 따라 다른 EPG가 구성됩니다.
- 애플리케이션은 동일한 IP 서브넷 및 게이트웨이를 계속 사용합니다.
- 새 VLAN을 사용하기 위한 세그먼트화된 애플리케이션 EPG.
- IP 서브넷으로 구성되고 여러 애플리케이션 EPG에 매핑되는 BD 1개.
- 1 BD = N EPG = N VLAN
- 이제 2개의 EPG(애플리케이션)가 Contract를 통해 서로 통신할 수 있습니다.

마이그레이션 접근 방식

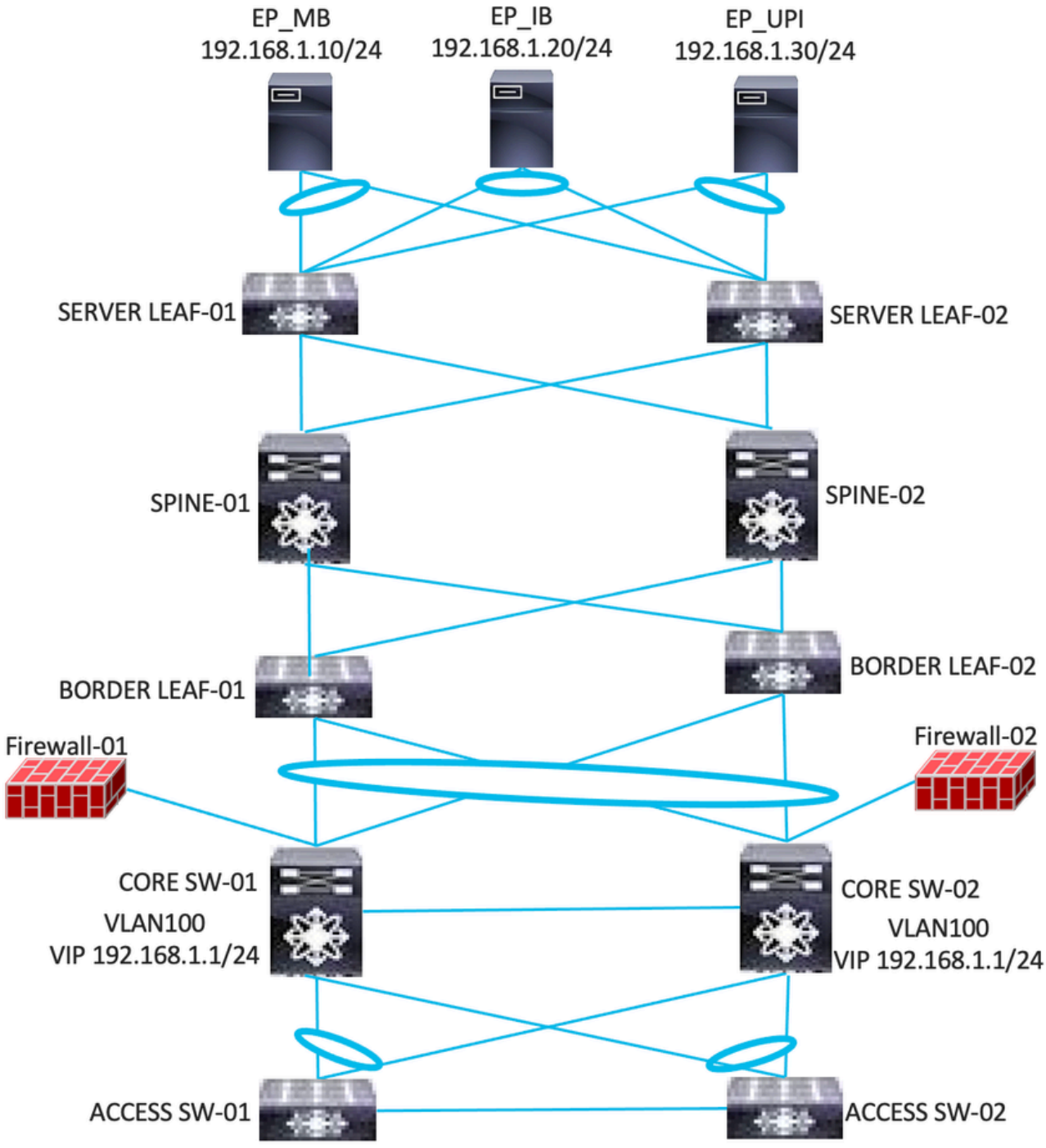
ACI를 애플리케이션 중심으로 구축하기 전에 ACI를 네트워크 중심으로 구축할 수 있으며 더 나아가 애플리케이션을 세분화할 수 있습니다.

네트워크 중심 마이그레이션 접근 방식: 1단계



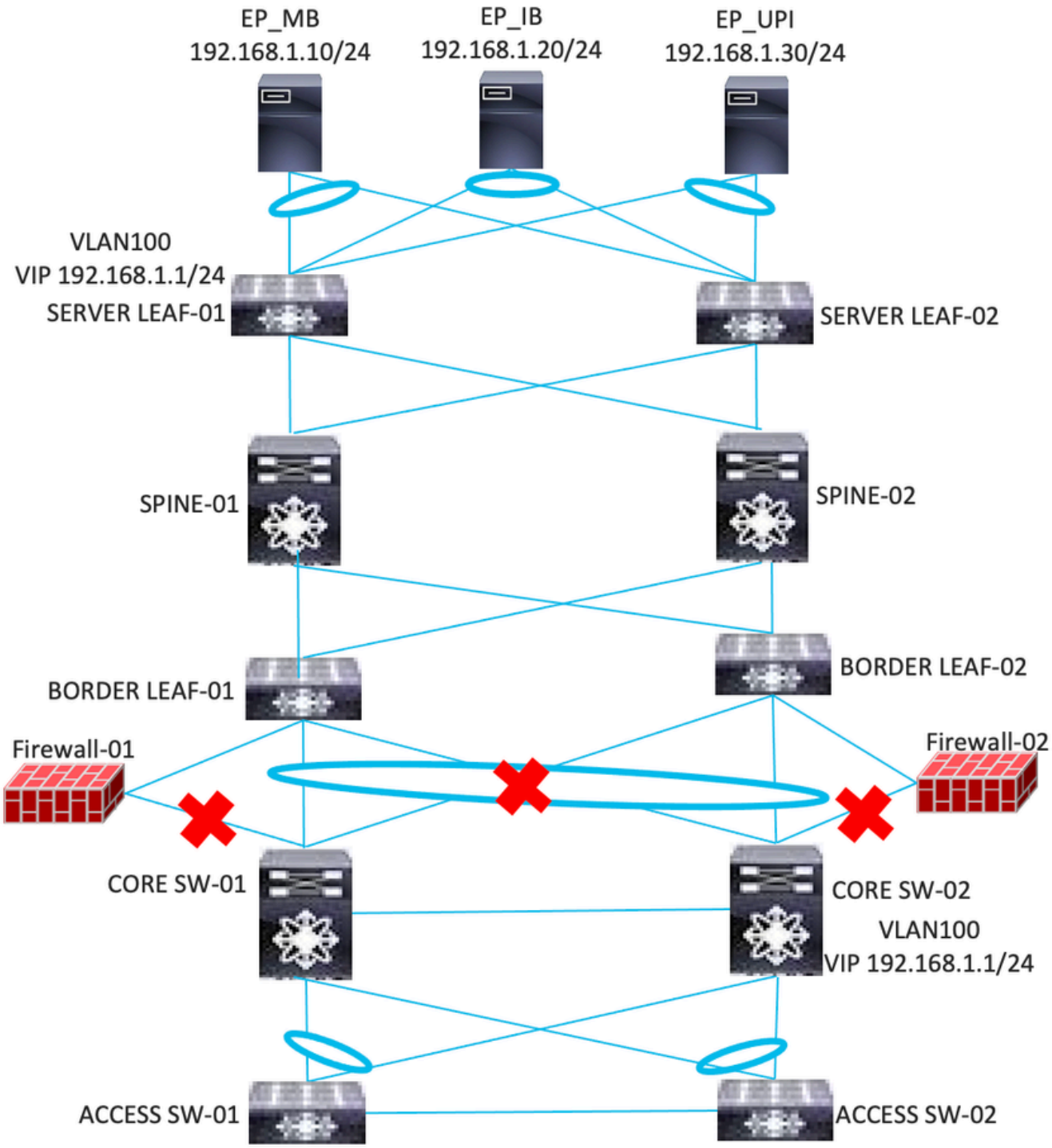
- 경계 리프 스위치와 코어 스위치 간에 레이어-2 중간 링크를 설정해야 합니다.
- 기존 네트워크에 구성된 기존 VLAN에 따라 ACI에서 레이어 2 브리지 도메인 및 엔드포인트 그룹을 구성합니다.
- 보더 리프 스위치와 코어 스위치 간의 레이어 2 중간 링크에서 이 모든 VLAN을 구성합니다.
- ACI는 코어 스위치에 있는 모든 엔드포인트를 학습해야 합니다.
- 게이트웨이는 코어 스위치에 유지됩니다.
- 방화벽 연결은 코어 스위치에 유지됩니다.

네트워크 중심 마이그레이션 접근 방식: 2단계



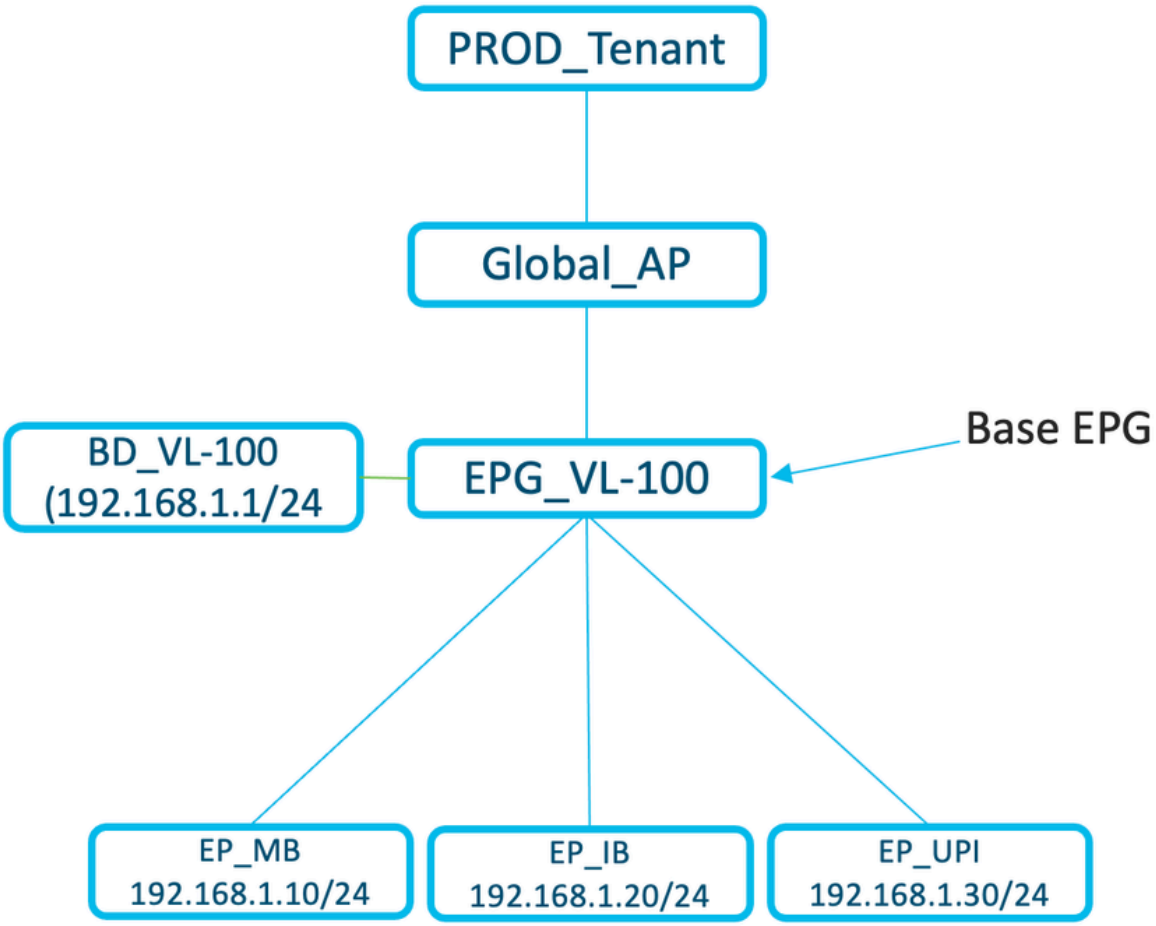
- 워크로드를 액세스 스위치에서 서버 리프로 이동합니다.
- 게이트웨이는 코어 스위치에 유지됩니다.
- 서버에서 게이트웨이에 연결할 수 있는지 확인합니다.
- 서버/애플리케이션에 연결할 수 있는지 확인합니다.

네트워크 중심 마이그레이션 접근 방식: 3단계



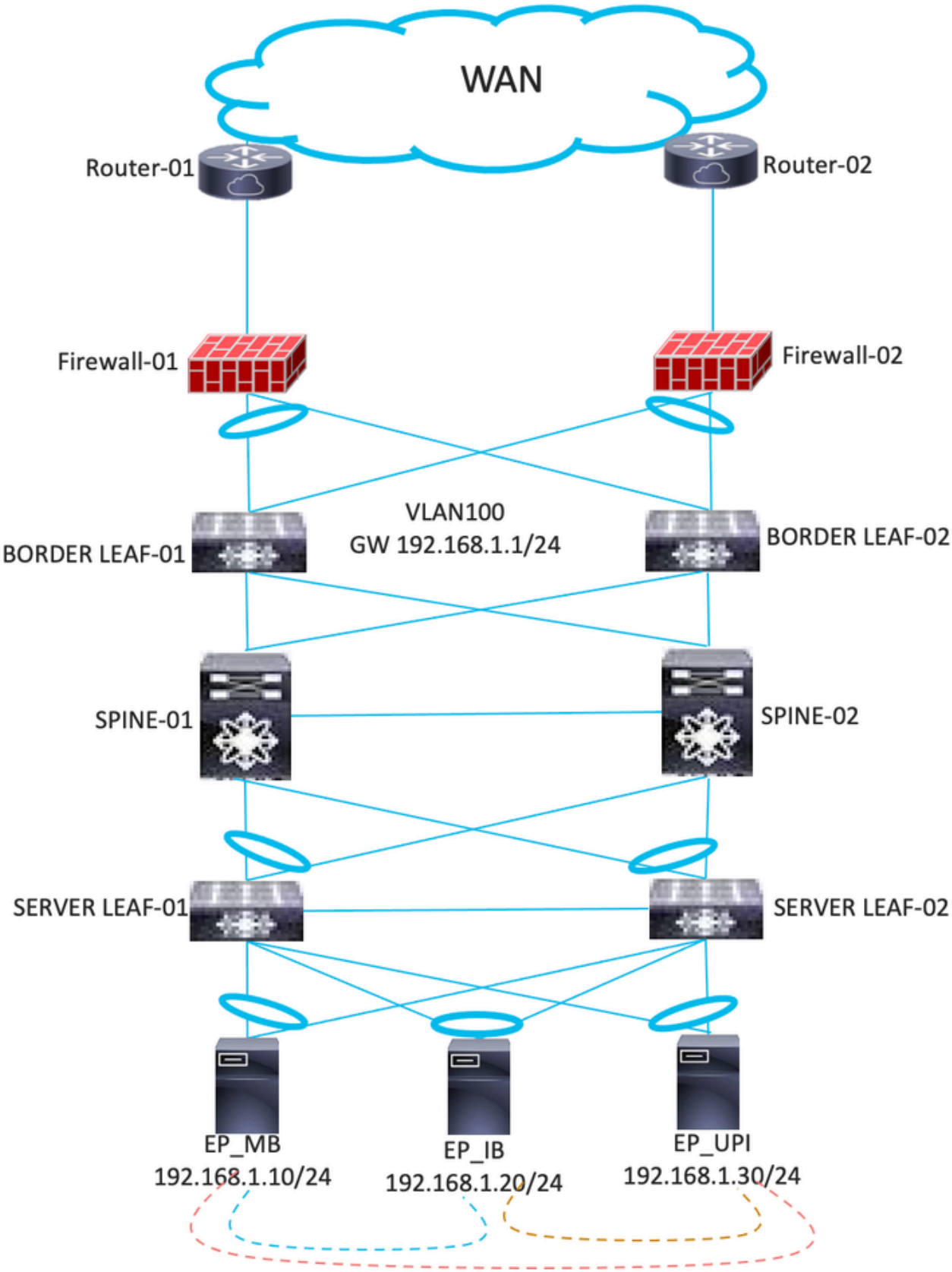
- 코어 스위치에서 게이트웨이를 종료하고 ACI에서 구성합니다.
- 방화벽 링크를 코어 스위치에서 ACI 리프로 이동합니다.
- 방화벽/라우터를 향해 L3out을 구성합니다.
- 방화벽/라우터 및 ACI Leaf에 경로를 추가합니다.
- Border Leaf 및 Core 스위치 간의 링크를 종료합니다.
- 서버/애플리케이션에 연결할 수 있는지 확인합니다.

Network Centric Migration 접근 방식 이후의 ACI를 논리적으로 나타냅니다.



➢ 1 BD = 1 EPG = 1 VLAN

애플리케이션 중심 마이그레이션 접근 방식: 1단계



- CSW/Tetration 데이터 수집 및 분석
- CSW/Tetration 데이터(WEB, APP, DB)에 따른 새 EPG 컨피그레이션.
- 예를 들어, MB 애플리케이션의 경우 EPG_MB_WEB, EPG_MB_APP, EPG_MB_DB 등 3개의 EPG가 생성됩니다. 이러한 EPG는 하나의 애플리케이션 프로파일 AP_MB 아래에 구성해야

합니다.

- VMM(Virtual Machine Manager) 통합의 경우 새 EPG의 서버를 새 VLAN과 매핑하려면 vDS 컨피그레이션이 필요합니다.
- VMM 통합을 통해 푸시되는 새 vDS에 VM(가상 머신)을 매핑합니다.
- 베어 메탈의 경우 서버 팀은 서버의 VLAN ID를 변경해야 합니다.
- 이러한 구축에서는 IP 주소 지정이 동일합니다.
- CSW/Tetration 데이터에 따른 EPG 간 계약 컨피그레이션

CSW/Tetration 데이터 분석

CSW/Tetration 데이터를 기반으로 한 분석의 예:

src_ip	소비자 범위	dst_ip	공급자 범위	프로토콜	포트
192.168.34.248	기본값: 내부: 본사	192.168.20.81	프로다프	TCP	443
192.168.78.45	기본값: 내부: 본사	192.168.20.81	프로다프	TCP	443
192.168.78.16	기본값: 내부: 본사	192.168.20.81	프로다프	TCP	443
192.168.78.25	기본값: 내부: 본사	192.168.20.81	프로다프	TCP	443
192.168.44.69	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:검색	192.168.20.81	프로다프	UDP	137
192.168.44.69	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:검색	192.168.20.81	프로다프	TCP	445
192.168.32.173	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:DMZ	192.168.20.81	프로다프	TCP	7777
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	135
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	UDP	137

192.168.44.48	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	UDP	137
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	443
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	445
192.168.44.48	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	445
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	5985
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	49154
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	49169
192.168.44.29	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	4750
192.168.44.30	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.81	프로다프	TCP	4750
192.168.44.21	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:AAA	192.168.20.81	프로다프	ICMP	0

192.168.103.80	기본값:내부:데이터 센터:DC:애플리케이션:Prod:DHCP	192.168.20.81	프로다프	TCP	7777
192.168.103.71	기본값:내부:데이터 센터:DC:애플리케이션:Prod:DHCP	192.168.20.81	프로다프	TCP	7777
192.168.103.20	기본값:내부:데이터 센터:DC:애플리케이션:Prod:DHCP	192.168.20.81	프로다프	TCP	7777
192.168.103.21	기본값:내부:데이터 센터:DC:애플리케이션:Prod:DHCP	192.168.20.81	프로다프	TCP	7777
192.168.44.68	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	192.168.20.85	프로들	UDP	137
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	192.168.20.85	프로들	UDP	137
192.168.44.68	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	192.168.20.85	프로들	TCP	445
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	192.168.20.85	프로들	TCP	445
172.16.32.173	기본값:내부:데이터 센터:DC:애플리케이션:Prod:MZ	192.168.20.85	프로들	TCP	1522
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	135
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	UDP	137

192.168.44.48	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	UDP	137
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	UDP	161
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	445
192.168.44.48	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	445
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	5985
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	49154
192.168.44.47	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	60801
192.168.44.30	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	4750
192.168.44.29	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	TCP	4750
192.168.44.21	기본값:내부:데이터 센터 :DC:애플리케이션:Prod:모니터링	192.168.20.85	프로들	ICMP	0

CSW/Tetration의 EPG 권장 예:

EPG	IP
프로다프	192.168.20.81
로드브	192.168.20.85

세부 사항을 기준으로 계약 구성을 위해 데이터를 분석해야 합니다. 분석된 데이터의 예:

src_ip	소비자 범위	소비자_EPG	dst_IP	공급자_EPG	프로토콜	포트
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	EPG_검색	192.168.20.81	EPG-PROD-APP	UDP	137
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	EPG_검색	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	135
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	UDP	137
192.168.44.48	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	443

192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	5985
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	49154
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	49169
192.168.44.48	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	TCP	4750
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.81	EPG-PROD-APP	ICMP	0
192.168.103.21	기본값:내부:데이터 센터:DC:애플리케이션:Prod:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TCP	7777

192.168.44.68	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	EPG_검색	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.68	기본값:내부:데이터 센터:DC:애플리케이션:Prod:검색	EPG_검색	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	TCP	135
192.168.44.69	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	UDP	161
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.48	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	TCP	5985
192.168.44.47	기본값:내부:데	EPG_모니터	192.168.20.85	EPG-	TCP	49154

	이터 센터:DC:애플리케이션:Prod:모니터링	링		PROD-DB		
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	TCP	60801
192.168.44.48	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	TCP	4750
192.168.44.47	기본값:내부:데이터 센터:DC:애플리케이션:Prod:모니터링	EPG_모니터링	192.168.20.85	EPG-PROD-DB	ICMP	0
192.168.48.45	기본값:내부:데이터 센터:DC:애플리케이션:Prod:백업	EPG_VL_71	192.168.20.85	EPG-PROD-DB	TCP	5555

IP 주소를 기준으로 소비자 및 제공자 EPG가 언급된다. 중복 항목 및 남북 트래픽(예: 인터넷, DC 간, 영역 간 트래픽 등)은 이 데이터에서 제외해야 합니다. EPG_VL_157, EPG_VL_71 등과 같이 VLAN이 있는 일부 EPG가 있습니다. 즉, 이러한 서버는 애플리케이션 중심 마이그레이션의 일환으로 대상 EPG로 이동되지 않습니다. 따라서 이 사이의 계약은 현재 EPG 매핑으로 구성됩니다. 이러한 서버가 대상 EPG로 마이그레이션되면 정리 프로세스의 일부로 이러한 기존 계약을 삭제하고 대상 EPG에 적절한 계약을 추가해야 합니다.

계약

계약은 EPG 간의 통신에 필요합니다. 이 섹션에서는 계약 컨피그레이션 프로세스 중 구현 흐름을 살펴봅니다.

1. 초기 Vz모든 계약은 VRF(Virtual Routing and Forwarding) 레벨에 적용되어야 합니다.

2. CSW/Tetration 데이터에 따라 특정 EPG 계약을 생성해야 합니다.

3. VzAny 계약에서 지정되지 않은 트래픽 통신을 허용하지 않도록 우선 순위가 낮은 Deny_All 규칙을 구성합니다. 아직 애플리케이션 중심으로 마이그레이션되지 않은 애플리케이션의 경우, VzAny Contract를 통해 통신이 이루어집니다.

4. 마이그레이션을 모두 마친 후 VRF에서 VzAny 계약을 삭제합니다.

CSW/Tetration 데이터를 분석하여 적절한 ACI 객체로 변환하는 작업은 매우 중요한 단계입니다. 따라서, 초기 분석 후, 우리의 관찰을 관계자와 논의하고 같은 부분에 대한 재확인을 받는 것이 중요합니다. 또한 구현 중에 모든 트래픽이 예상대로 허용될 수 있도록 신중하게 고려해야 합니다. 트러블슈팅을 위해 계약에서 로깅을 활성화하고 GUI 인터페이스 또는 CLI를 사용하여 특정 포트에서 패킷 삭제를 추적할 수도 있습니다.

```
leaf# show logging ip access-list internal packet-log deny
[ Tue Oct 1 10:34:37 2019 377572 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType:
Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c, DMac:0x000c0c0c, SIP: 192.168.21.11, DIP:
192.168.22.11, SPort: 0, DPort: 0, Src intf: Tunnel7, Proto: 1 pktLen: 98
[ Tue Oct 1 10:34:36 2019 377731 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType:
Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c, DMac:0x000c0c0c, SIP: 192.168.21.11, DIP:
192.168.22.11, SPort: 0, DPort: 0, Src intf: Tunnel7, Proto: 1 pktLen: 98
```

contract_파서

ID에서 이름 조회를 수행하는 동안 영역 지정 규칙의 상관관계를 분석하고, 필터링하고, 통계를 적중하는 출력을 생성하는 디바이스 상의 Python 스크립트. 이 스크립트는 다단계 프로세스를 거쳐 특정 EPG/VRF 또는 기타 계약 관련 값으로 필터링할 수 있는 단일 명령으로 전환된다는 점에서 매우 유용합니다.

```
leaf# contract_parser.py
키:
[prio:RuleId] [vrf:{str}] 동작 프로토콜 src-epg [src-l4] dst-epg [dst-l4] [flags][contract:{str}]
[hit=count]

[7:4131] [vrf:common:default] permit ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-
L3Out1/instP-extEpg(25) eq 123 [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[7:4156] [vrf:common:default] permit ip tcp tn-Prod1/l3out-L3Out1/instP-extEpg(25) eq 123 tn-
Prod1/ap-Services/epg-NTP(16410) [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[12:4169] [vrf:common:default] deny,log any tn-Prod1/l3out-L3Out1/instP-extEpg(25) epg:any
[contract:implicit] [hit=0]
[16:4167] [vrf:common:default] allow any epg:any tn-Prod1/bd-Services(32789) [contract:implicit]
[hit=0]
```

패킷 삭제는 GUI에서 Tenant(테넌트) > Tenant_Name(테넌트 이름) > Operational(운영) > Flows/Packets(플로우/패킷) 경로를 사용하여 표시할 수도 있습니다.

고려 사항

EPG 간 계약을 적용하는 동안 권장사항:

1. ACI는 TCAM(Ternary Content Addressable Memory) 사용률을 높일 수 있는 정책 매핑의 관점에서 방화벽으로 간주할 수 없습니다.

2. 많은 개별 필터 대신 다양한 필터를 사용합니다.

3. 모든 계약에서 4개 이상의 필터 범위를 사용해서는 안 됩니다. 이는 높은 오버플로 OTCAM(Ternary Content Addressable Memory)을 사용할 수 있습니다.

4. EPG에 많은 수의 포트가 필요한 경우 'permit any' 계약을 사용하십시오.

5. 솔루션의 일부로서, 많은 수의 계약이 구축될 것으로 예상될 경우 FSP(Forwarding Scale Profile)를 적절하게 수정하는 것도 고려해 보십시오.

6. 대량 계약 배포 전에 다음 공식을 사용하여 TCAM을 계산합니다. 제공 EPG 번호 * 소비자 EPG 번호 * 규칙 수.

7. ACI UI에서 Operations(운영) > Capacity Dashboard(용량 대시보드) > Leaf Capacity(리프 용량) 경로를 사용하여 기존 TCAM 크기를 확인할 수 있습니다.

LEAF-101# vsh_lc

module-1# show platform internal hal health-stats | grep 개수(_c)

mcast_count: 0

max_mcast_count: 8192

policy_count: 221

max_policy_count: 65536

policy_otcam_count: 322

max_policy_otcam_count: 8192

policy_label_count: 0

max_policy_label_count: 0

앱 중심 구축 및 솔루션의 몇 가지 과제

1. 계약 건수가 많을수록 리프 스위치의 TCAM 활용률이 높습니다.

따라서 TCAM 사용률을 적극적으로 추적하고 대량의 컨피그레이션 구축이 완료되면 TCAM 값이 증가할 것으로 예상하는 경우에도 준비하는 것이 중요합니다. 푸시되는 컨피그레이션이 적절한지 확인하기 위해 메이커 검사기 프로세스를 사용하는 것이 좋습니다. 또한, 적절한 예약된 유지 보수 기간을 사용하여 변경을 수행하는 것이 좋습니다.

2. 한 번의 계약 밀어넣기로 대량 컨피그레이션(50k TCAM 이상)을 수행하면 정책 관리자 메모리 충돌이 발생할 수 있습니다.

특히 컨피그레이션의 크기가 큰 경우 컨피그레이션을 더 작은 청크로 푸시하는 것이 좋습니다. 이를 통해 계약 구성에 대한 체계적이고 위험 부담이 없는 접근 방식을 제공합니다. 또한 각 컨피그레이션 푸시를 사용하여 TCAM 값 증가를 측정합니다.

3. 애플리케이션이 CSW/Tetration 구축 시간 간격(3-4주) 동안 통신하지 않으면 트래픽 흐름이 캡처되지 않습니다.

이러한 상황을 방지하기 위해 가장 좋은 방법은 변경 활동 전에 애플리케이션 소유자로부터 CSW/Tetration 데이터를 재확인하는 것입니다. 또한 구현 후 로그에서 오류 적중 횟수를 확인합니다.

부가 가치

1. 중앙은행지침에 따라 모든 신청이 세분화·제한되어 있을 것

2. 애플리케이션 중심 구축으로 마이그레이션한 후 애플리케이션 간 통신의 가시성

3. 신청의 미시적(미시적) 분할이 이루어질 것

4. 애플리케이션 흐름을 한눈에 볼 수 있는 기능 하나의 애플리케이션 프로필에서 EPG는 IP 서브넷에 관계없이 3개의 EPG(EPG_Banking_WEB, EPG_Banking_APP, EPG_Banking_DB)를 보유하기 위해 애플리케이션 프로필 AP_Banking과 같은 트래픽 흐름에 따라 매핑됩니다.

4. 애플리케이션 흐름을 한눈에 볼 수 있어 문제 해결이 더 쉬워집니다.

5. 인프라가 더 안전합니다.

6. 체계적인 추진방식 및 향후 추진방향

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.