ACI implementeren als Application Centric

Inhoud

Inleiding

Beperkingen bij gebruik van traditioneel netwerk

Voorwaarden

- Vereisten
- Gebruikte componenten

Overzicht van oplossing

- Centrisch ontwerp voor netwerk
- Toepassingscentrisch ontwerp

Migratiebenaderingen

- Network Centric Migration Approach: fase-1
- Network Centric Migration Approach: fase-2
- Network Centric Migration Approach: fase-3
- Toepassingsgerichte migratieaanpak: fase-1

CSW/Tetration Data Analysis

Contract

- contract_parser

overweging

Enkele uitdagingen van app-centric implementatie en oplossing

Waardetoevoeging

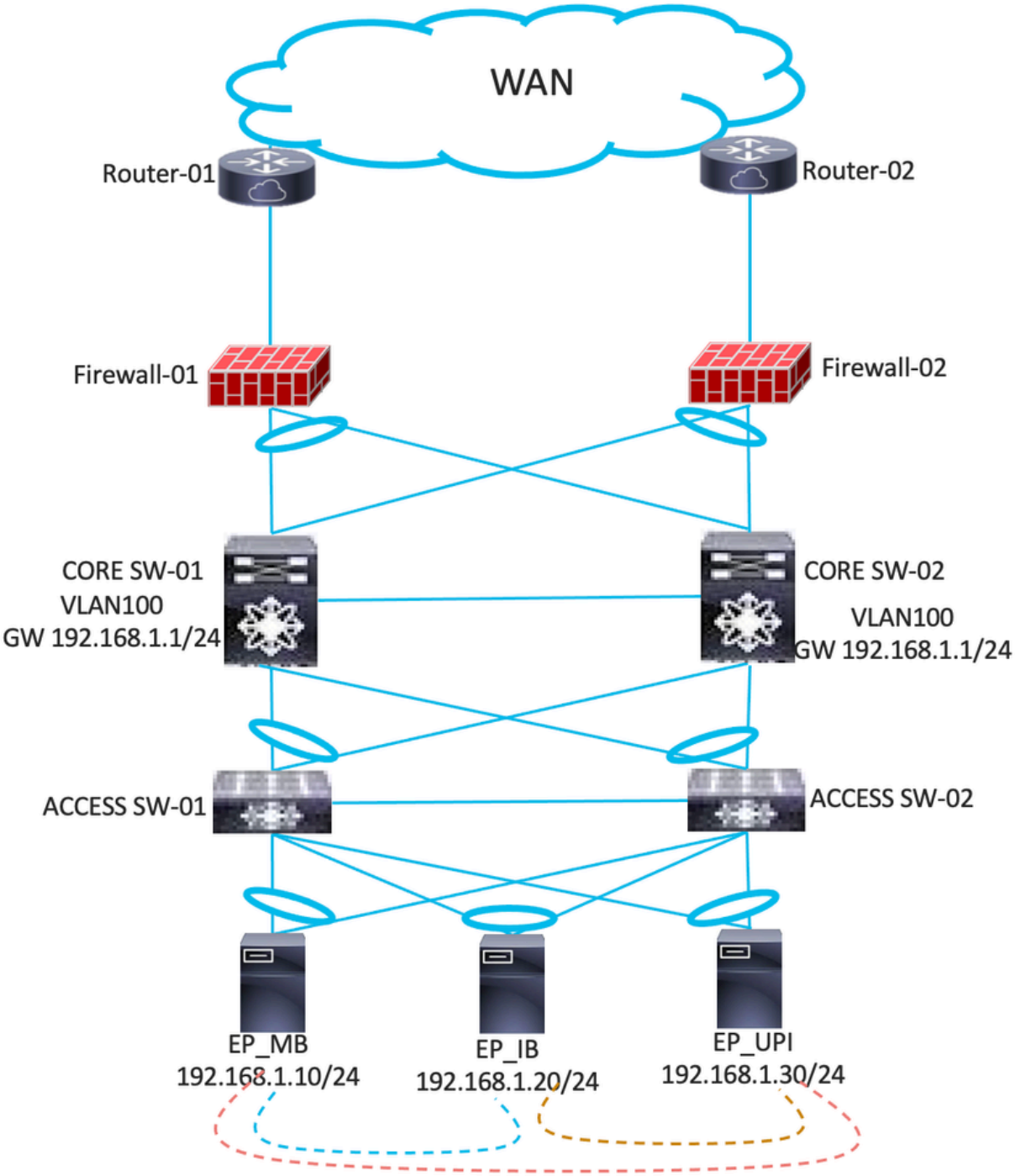
Inleiding

Dit document beschrijft de aanpak om micro-segmentatie en beveiliging binnen/tussen de toepassingen te realiseren met behulp van de Cisco ACI SDN-oplossing.

Beperkingen bij gebruik van traditioneel netwerk

- In traditionele netwerken is segmentering binnen een VLAN/subnet onmogelijk.
- De applicatiegateways bevinden zich op belangrijke switches. Als twee toepassingen willen communiceren, zijn complexe toegangscontrolelijsten (ACL's) vereist op de kern-switch.
- De Spanning-Tree-lus tussen de switches verbreekt de datacenterstroom en resulteert in een verkeersdaling.
- Hetzelfde IP-subnet bevat meerdere toepassingen, die onderling geen beveiliging bieden. Op traditionele netwerken is het niet mogelijk deze communicatie te beheren.
- Neem een voorbeeld dat ook wordt afgebeeld met behulp van het diagram. Je hebt drie applicaties EP_MB, EP_IB en EP_UPI die deel uitmaken van hetzelfde VLAN en IP-subnet. Bij elk L2-verkeer wordt het verkeer altijd overstroomd naar alle toepassingen, ook al is er geen communicatie tussen deze toepassingen nodig. De beperkingen tussen de twee

toepassingen zijn in dit scenario niet mogelijk.



Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Workload (CSW)/Tetration (Secure Workload) moet in de omgeving worden geïmplementeerd om de verkeersstroomgegevens tussen de toepassingen te verzamelen.
- Er moeten agents op de servers worden geïnstalleerd om de gegevens te kunnen

verzamelen. Daarom is dit alleen mogelijk in het geval van de inzet van brownfield.
- De agents moeten ten minste 3-4 weken op de servers worden geïnstalleerd voor het verzamelen van gegevens.
- Als er geen tools beschikbaar zijn voor Application Dependence Mapping (ADM), moeten de relevante gegevens worden verstrekt.
- Servergateway moet worden geconfigureerd met de Application Centric Infrastructure (ACI) Fabric.

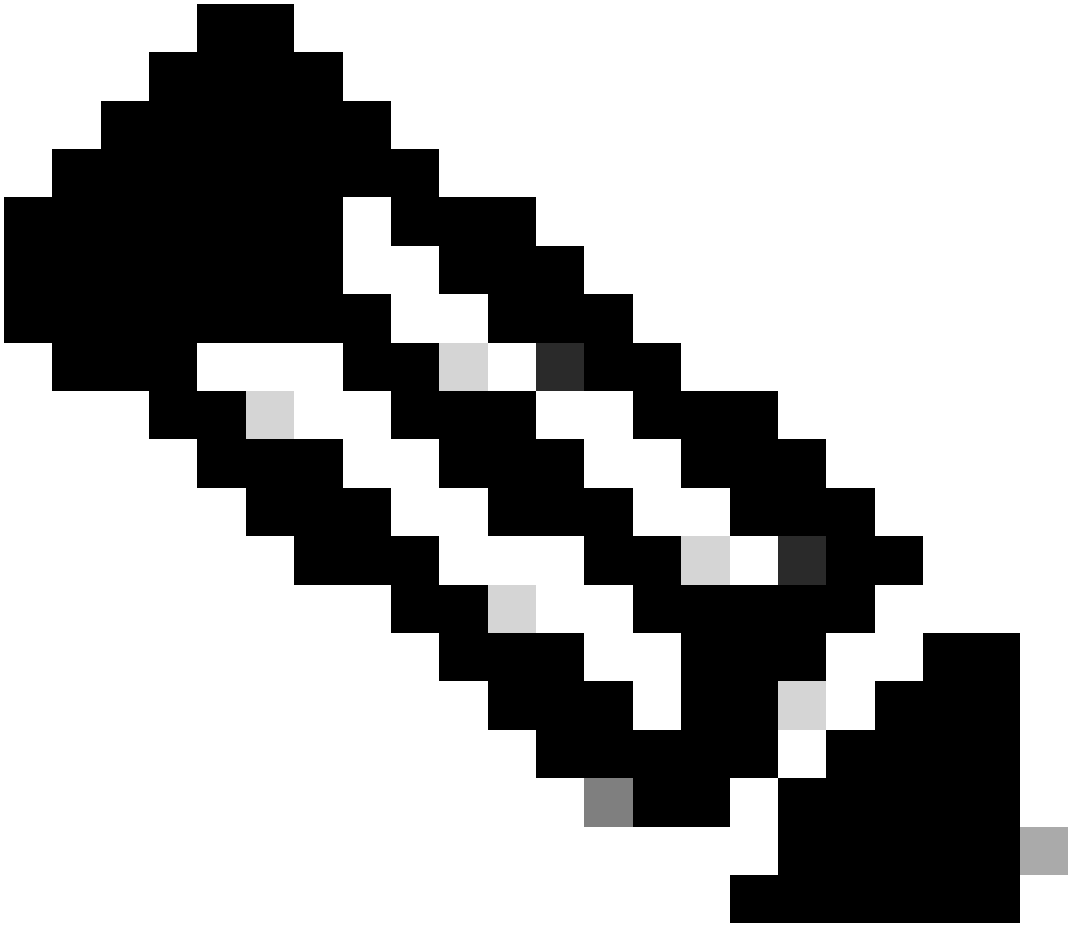
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht van oplossing

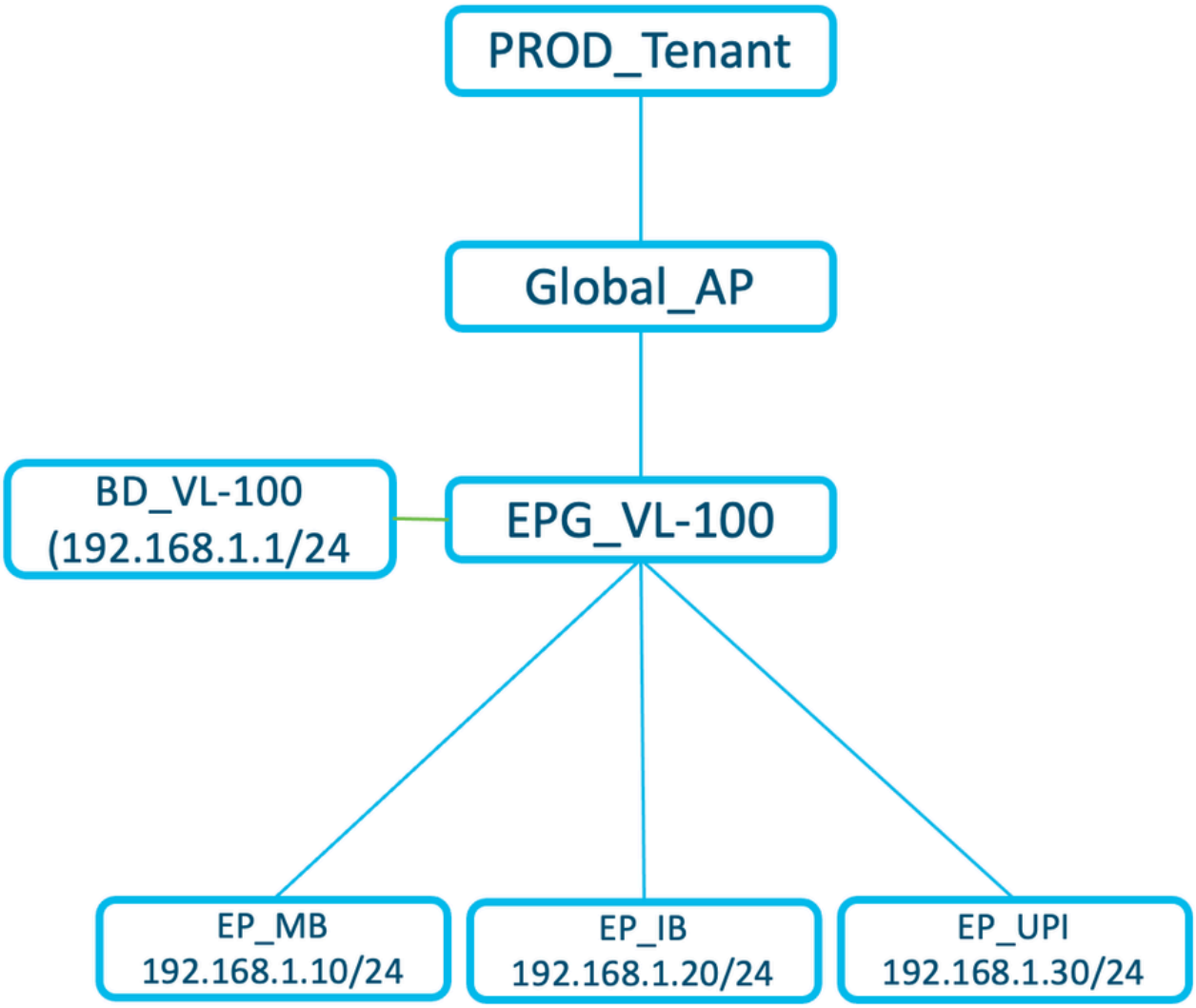
Om micro-segmentatie te bereiken, moet u eerst het netwerk naar een Cisco ISDN-oplossing van traditionele infrastructuur migreren en het netwerk opnieuw ontwerpen vanuit een toepassingsgerichte weergave. In dit deel worden de twee ontwerpfasen beschreven om de segmentatie te bereiken zoals gewenst op basis van de toepassingsstroom die via de ADM-tool wordt opgenomen. Eerst wordt de Cisco ACI-oplossing geïmplementeerd in de netwerkcentrifugemodus (as-is naar bestaand ontwerp) en vervolgens naar de toepassingscentrifugemodus verplaatst.



Opmerking: u kunt deze implementatiemodus ook combineren om services rechtstreeks van het traditionele netwerk naar de toepassingsgerichte modus te migreren.

Centrisch ontwerp voor netwerk

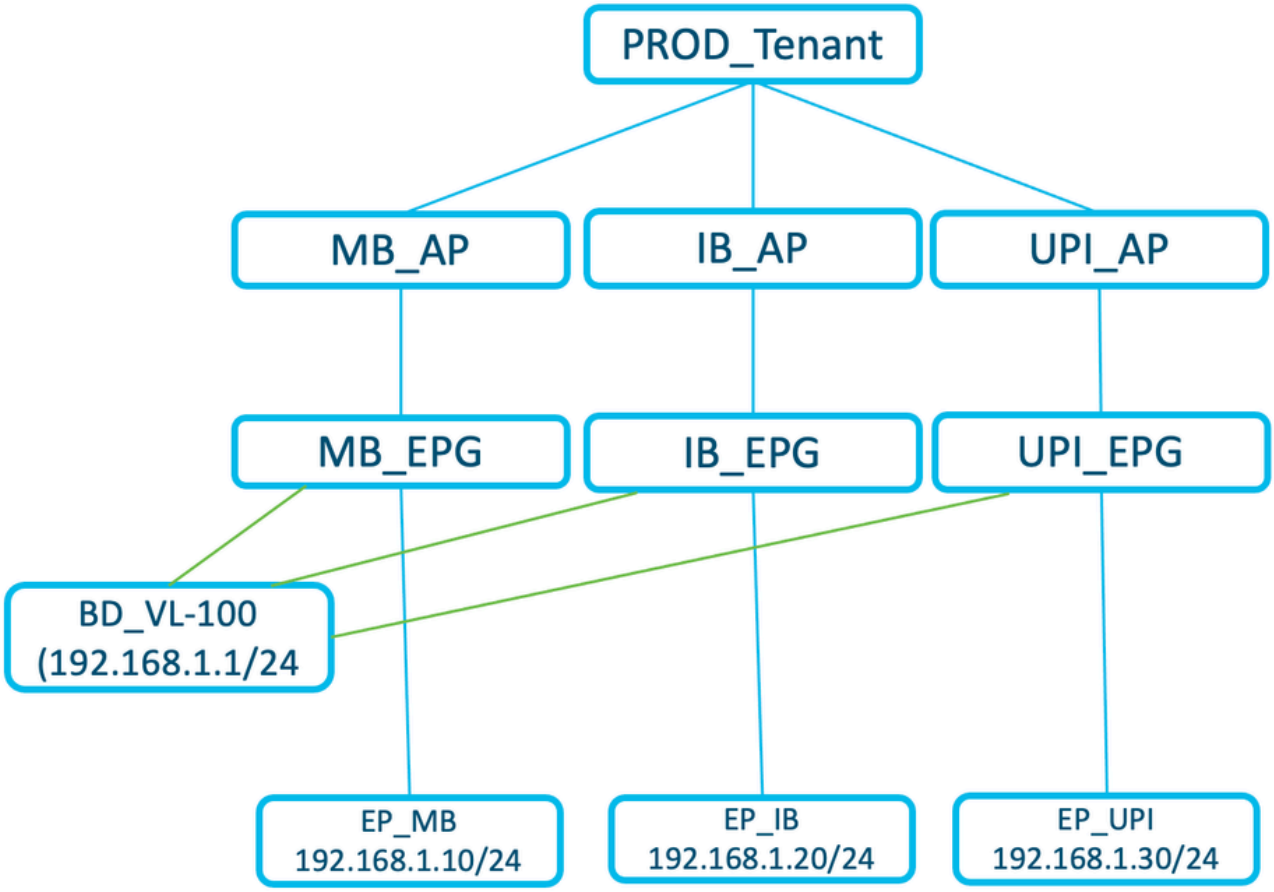
In het voorbeeld in het diagram bevat EPG_VL-100 drie toepassingen, EP_MB, EP_IB en EP_UPI, en deelt het dezelfde IP-subnetverbinding en gebruikt VLAN 100.



- Actuele migratie van traditioneel netwerk naar ACI.
- Eén Endpoint Group (EPG) kan meerdere toepassingen bevatten.
- Geen applicatiesegmentatie binnen dezelfde EPG in dit implementatietype.
- 1 BD = 1 EPG = 1 VLAN

Toepassingscentrisch ontwerp

Het voorbeeld in het diagram is een afzonderlijke EPG voor drie toepassingen EP_MB, EP_IB, en EP_UPI die hetzelfde IP-subnet delen en verschillende VLAN's gebruiken die aan elke EPG zijn toegewezen.

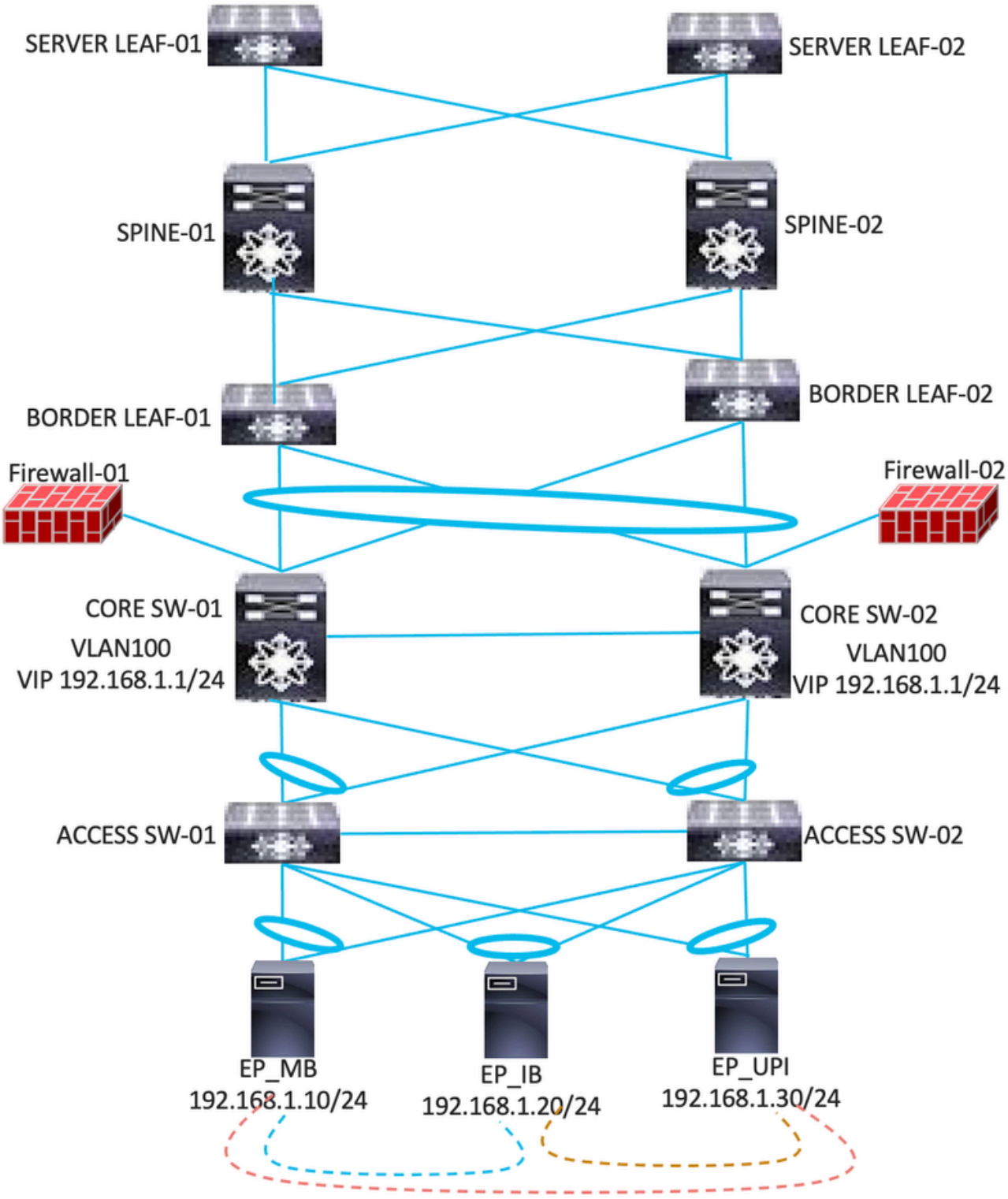


- In het implementatietype Application Centric worden verschillende EPG's geconfigureerd volgens de applicatie.
- De toepassingen blijven gebruik maken van dezelfde IP-subnetverbinding en de gateway ervan.
- De gesegmenteerde toepassing EPG's om een nieuw VLAN te gebruiken.
- 1 BD te configureren met IP-subnetverbinding en toegewezen aan meerdere EPG's van toepassingen.
- 1 BD = N EPG = N VLAN
- Nu kunnen twee EPG's (applicaties) via Contract met elkaar communiceren.

Migratiebenaderingen

Alvorens ACI als toepassing-centric op te stellen, kan ACI als netwerk-centric en verder worden opgesteld, kunnen de toepassingen worden gesegmenteerd.

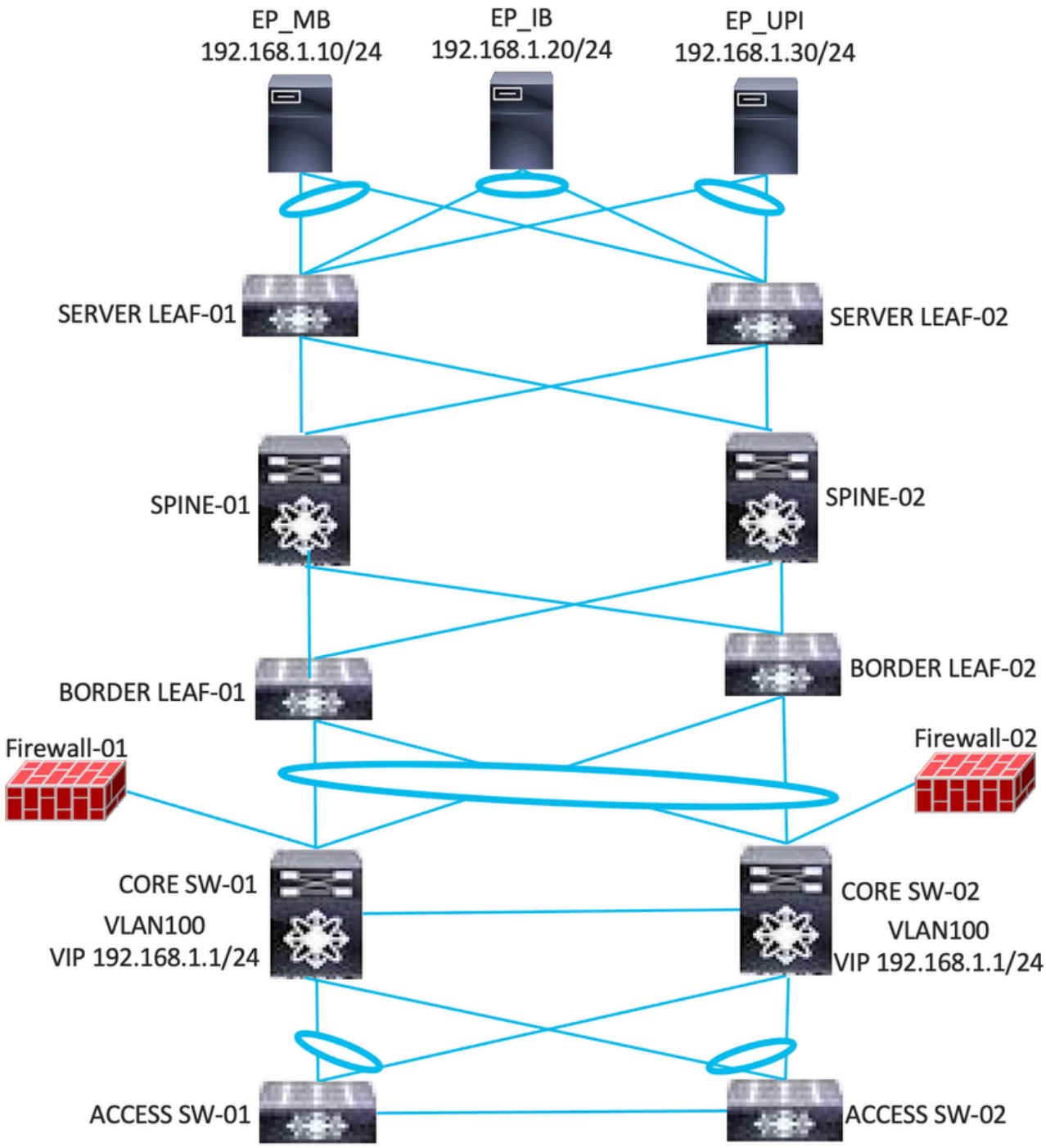
Network Centric Migration Approach: fase-1



- Layer 2-interim-link moet worden gelegd tussen border-leaf en core-Switches.
- Layer 2 Bridge Domain en Endpoint Group op ACI configureren volgens de bestaande VLAN's die in traditionele netwerken zijn geconfigureerd.
- Configureer al deze VLAN's op Layer-2 tussentijdse koppeling tussen Border Leaf en Core-Switches.
- ACI moet alle endpoints leren die op de belangrijkste switches aanwezig zijn.
- De gateway blijft op de kern switches.

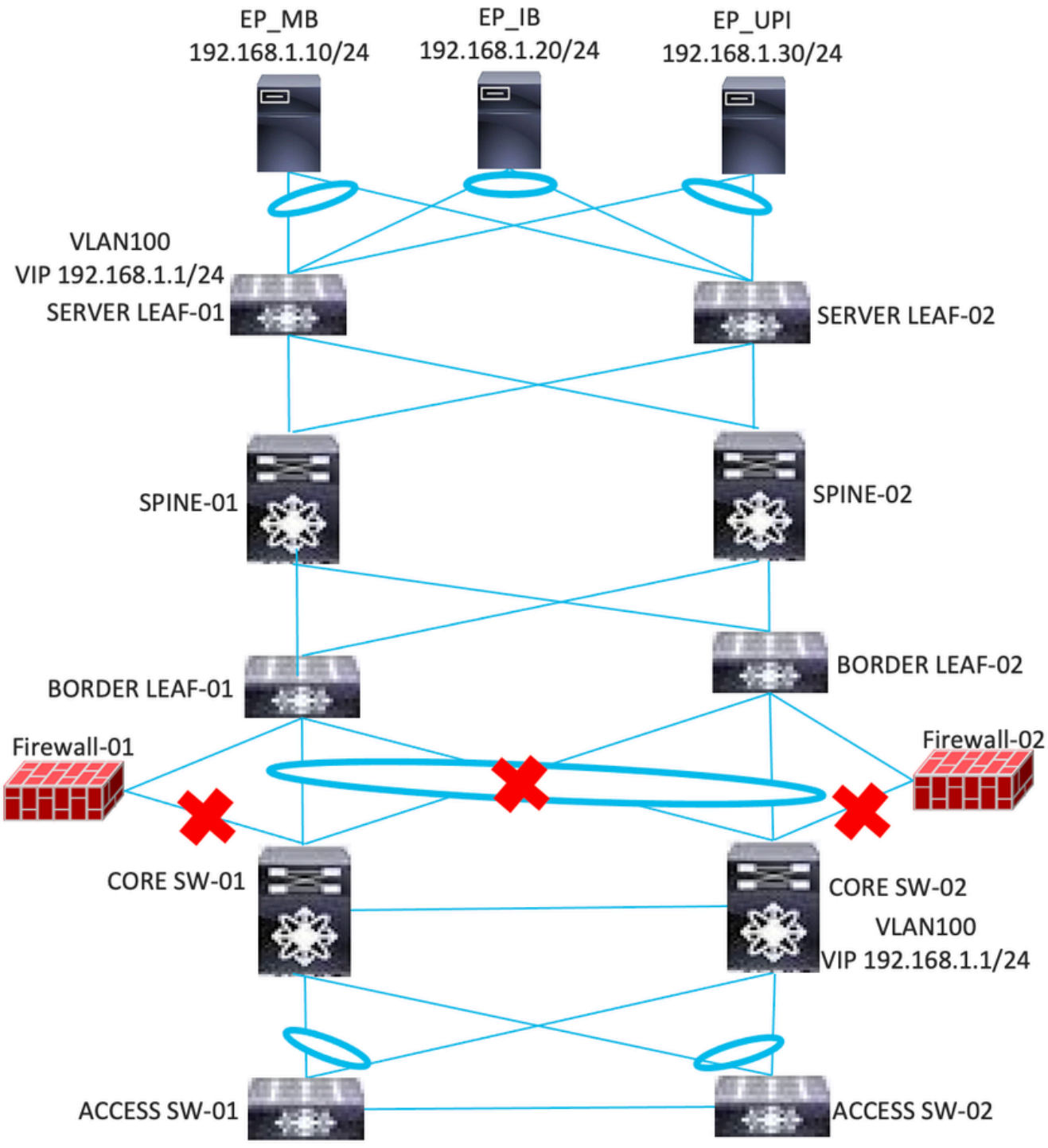
- Firewallconnectiviteit blijft beschikbaar op Core Switches.

Network Centric Migration Approach: fase-2



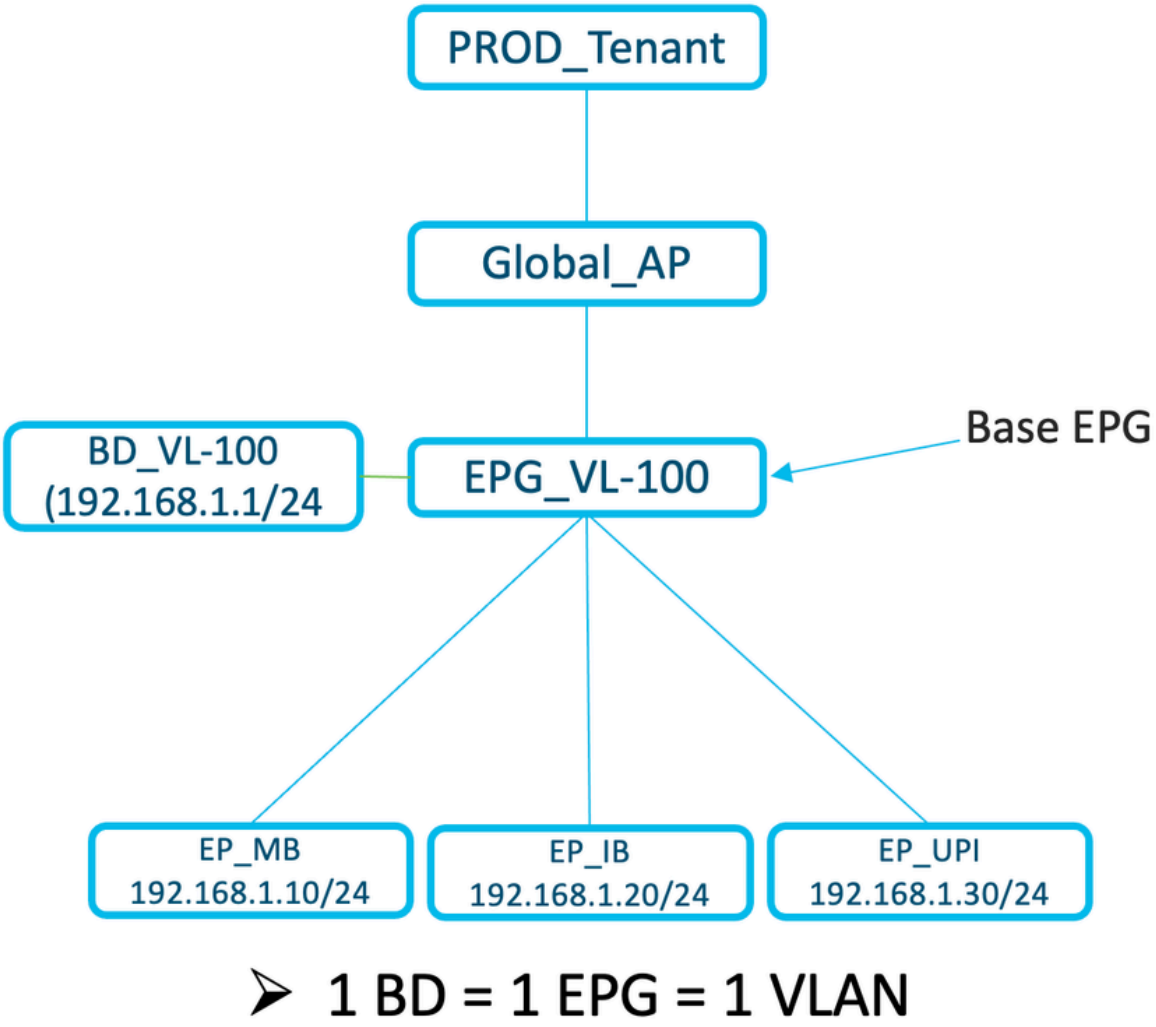
- Verplaats de werkbelasting van Access Switches naar Server Leaf.
- Gateway blijft beschikbaar op Core Switches.
- Controleer of de gateway bereikbaar is vanaf servers.
- Controleer of de server/toepassing bereikbaar is.

Network Centric Migration Approach: fase-3

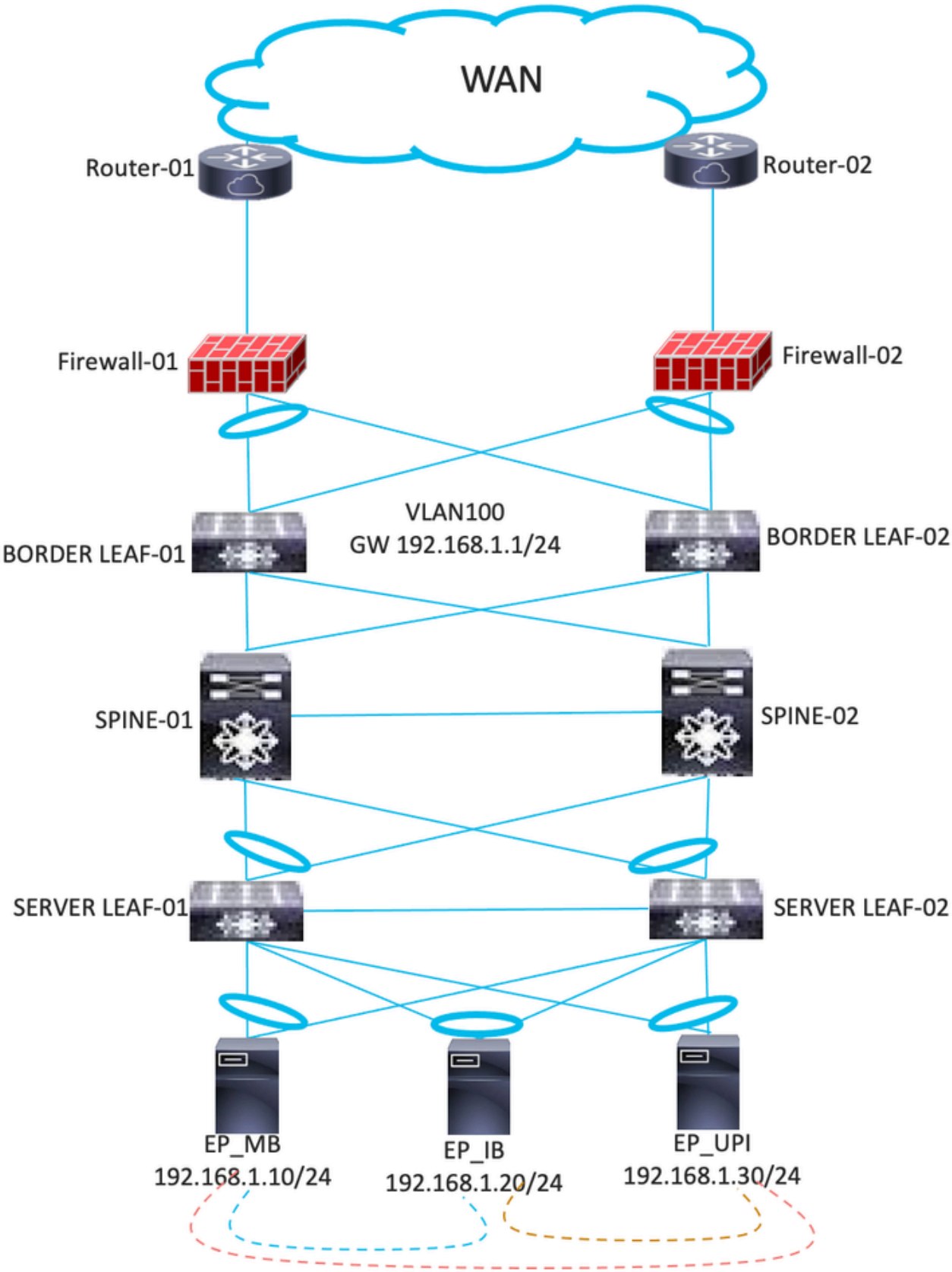


- Sluit de Gateways op Core-Switches en configureer ze op ACI.
- Verplaats de Firewall link van Core Switches naar ACI Leaf.
- Configureer de L3out naar de firewall/router.
- Voeg de routes toe in de firewall/router en ACI-blad.
- Sluit de koppeling tussen Border Leaf en Core Switches.
- Controleer of de server/toepassing bereikbaar is.

Logische weergave van ACI na benadering van netwerkcentrische migratie.



Toepassingsgerichte migratieaanpak: fase-1



- Verzamelen en analyseren van CSW-/testgegevens.
- Nieuwe EPG-configuratie volgens CSW/Tetration Data (WEB, APP en DB).
- Voor de MB-applicatie worden bijvoorbeeld drie EPG's gemaakt, zoals EPG_MB_WEB, EPG_MB_APP en EPG_MB_DB. Deze EPG's moeten worden geconfigureerd onder één

toepassingsprofiel AP_MB.

- In het geval van Virtual Machine Manager (VMM)-integratie is vDS-configuratie vereist om de servers in de nieuwe EPG met het nieuwe VLAN in kaart te brengen.
- Breng de virtuele machine (VM) in kaart aan de nieuwe vDS die door VMM-integratie wordt geduwd.
- Voor baremetals moet het serverteam de VLAN-id op de server wijzigen.
- IP-adressering moet hetzelfde zijn voor deze implementaties.
- Contractconfiguratie tussen EPG's volgens CSW-/opslaggegevens.

CSW/Tetration Data Analysis

Voorbeeld van de analyse op basis van de CSW-/testgegevens:

SRC_ip	verbruiker_toepassingsgebied	DST_ip	provider_s
192.168.34.248	Standaard:Intern:Hoofdkwartier	192.168.20.81	PRODAPP
192.168.78.45	Standaard:Intern:Hoofdkwartier	192.168.20.81	PRODAPP
192.168.78.16	Standaard:Intern:Hoofdkwartier	192.168.20.81	PRODAPP
192.168.78.25	Standaard:Intern:Hoofdkwartier	192.168.20.81	PRODAPP
192.168.44.69	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.81	PRODAPP
192.168.44.69	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.81	PRODAPP
192.168.32.173	Standaard:Intern:Datacenter:DC:Toepassing:Product:DMZ	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.48	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP

192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.48	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.29	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.30	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.81	PRODAPP
192.168.44.21	Standaard:Intern:Datacenter:DC:Toepassing:Product:AAA	192.168.20.81	PRODAPP
192.168.103.80	Standaard:Intern:Datacenter:DC:Toepassing:Product:DHCP	192.168.20.81	PRODAPP
192.168.103.71	Standaard:Intern:Datacenter:DC:Toepassing:Product:DHCP	192.168.20.81	PRODAPP
192.168.103.20	Standaard:Intern:Datacenter:DC:Toepassing:Product:DHCP	192.168.20.81	PRODAPP
192.168.103.21	Standaard:Intern:Datacenter:DC:Toepassing:Product:DHCP	192.168.20.81	PRODAPP
192.168.44.68	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.85	PRODDB
192.168.44.69	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.85	PRODDB
192.168.44.68	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.85	PRODDB
192.168.44.69	Standaard:Intern:Datacenter:DC:Toepassing:Product:Detectie	192.168.20.85	PRODDB
172.16.32.173	Standaard:Intern:Datacenter:DC:Toepassing:Product:MZ	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB

192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.48	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.48	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.47	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.30	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.29	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB
192.168.44.21	Standaard:Intern:Datacenter:DC:Toepassing:Product:Bewaking	192.168.20.85	PRODDB

Voorbeeld van een EPG-aanbeveling uit de CSW/Tetration:

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

Gebaseerd op de details, moeten de gegevens voor contractconfiguratie worden geanalyseerd.
Voorbeeld van de geanalyseerde gegevens:

SRC_ip	verbruiker_toepassingsgebied	consumer_EPG	DST_IP	provider_EPG	proto

192.168.44.69	Standaard:Intern:Datacenter: DC:Toepassing:Prod:Detectie	EPG_DISCOVERY	192.168.20.81	EPG-PROD- APP	UDP
192.168.44.69	Standaard:Intern:Datacenter: DC:Toepassing:Prod:Detectie	EPG_DISCOVERY	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	UDP
192.168.44.48	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.48	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.81	EPG-PROD- APP	ICMP
192.168.103.21	Standaard:Intern:Datacenter: DC:Toepassing:Product:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD- APP	TCP
192.168.44.68	Standaard:Intern:Datacenter: DC:Toepassing:Prod:Detectie	EPG_DISCOVERY	192.168.20.85	EPG-PROD- DB	UDP

192.168.44.68	Standaard:Intern:Datacenter: DC:Toepassing:Prod:Detectie	EPG_DISCOVERY	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.69	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.69	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	UDP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	UDP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.48	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.48	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	TCP
192.168.44.47	Standaard:Intern:Datacenter: DC:Toepassing:Product:Bewaking	EPG_BEWAKING	192.168.20.85	EPG-PROD- DB	ICMP
192.168.48.45	Standaard:Intern:Datacenter: DC:Toepassing:Product:Back-up	EPG_VL_71	192.168.20.85	EPG-PROD- DB	TCP

Op basis van het IP-adres worden de EPG’s van de consument en de aanbieder vermeld. Dubbele gegevens en Noord-Zuid-verkeer (zoals internet, inter-DC, verkeer tussen zones, enzovoort) moeten van deze gegevens worden uitgesloten. Er zijn enkele EPG's met een naam voor VLAN's zoals EPG_VL_157, EPG_VL_71, enzovoort. Dit betekent dat deze servers niet naar de doel-EPG worden verplaatst als onderdeel van een op toepassingen gerichte migratie. Dus het contract tussen hen moet worden geconfigureerd met de huidige mapping van EPG. Zodra deze

servers zijn gemigreerd naar doel-EPG, moeten deze bestaande contracten worden verwijderd als onderdeel van het opschoningsproces en moet het juiste contract worden toegevoegd aan doel-EPG.

Contract

Voor de communicatie tussen de EPG's zijn contracten vereist. De stroom van de implementatie tijdens het proces van de contractconfiguratie wordt in deze sectie opgenomen.

1. Aanvankelijk moet een VZAny-contract worden toegepast op het niveau van Virtual Routing and Forwarding (VRF).

2. Volgens CSW/Tetration-gegevens moeten er specifieke EPG-contracten worden gecreëerd.

3. Configureer de regel Deny_All met lage prioriteit zodat het VzAny-contract niet voorziet in ongespecificeerde verkeerscommunicatie. Voor de toepassingen, die nog niet zijn gemigreerd als applicatie-centric, gebeurt de communicatie via VzAny Contract.

4. Na alle migratie, het VzAny contract uit de VRF verwijderen.

De analyse van CSW-/Tetratiegegevens en de omzetting ervan in geschikte ACI-objecten is een zeer kritische stap. Daarom is het na de eerste analyse belangrijk om onze waarneming met de betrokkenen te bespreken en op dezelfde manier opnieuw te worden bevestigd. Ook tijdens de implementatie moet zorgvuldig worden overwogen om ervoor te zorgen dat al het verkeer wordt toegestaan zoals verwacht. Voor het oplossen van problemen, kunt u het registreren van het contract en ook spoor voor om het even welke pakketdaling op een specifieke haven toelaten die een GUI interface of CLI gebruiken.

leaf# toont IP access-list interne pakketlog ontkennen
[Tue Oct 1 10:34:37 2019 377572 usecs]: Naam: Prod1:VRF1(VXLAN: 2654209), VLANType: Onbekend, VLAN-ID: 0, SMac: 0x000c0c0c0c0c0c, DMac:0x000c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.28 11, SPort: 0, DPort: 0, SRC Intf: Tunnel7, Proto: 1, PktLen: 98
[Tue Oct 1 10:34:36 2019 377731 usecs]: Naam: Prod1:VRF1(VXLAN: 2654209), VLANType: Onbekend, VLAN-ID: 0, SMac: 0x000c0c0c0c0c0c, DMac:0x000c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.28 11, SPort: 0, DPort: 0, SRC Intf: Tunnel7, Proto: 1, PktLen: 98

contract_parser

Een Python-script op het apparaat dat een uitvoer produceert die de zoneringsregels, filters en hit-statistieken correleert tijdens het uitvoeren van naamsopzoekingen van ID's. Dit script is uitermate nuttig in die zin dat het een multi-step proces neemt en het in een enkele opdracht verandert die kan worden gefilterd naar specifieke EPG's/VRF's of andere contract-gerelateerde waarden.

leaf# contract_parser.py
Sleutel:
[prio:RuleID] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [vlaggen] [contract:{str}] [hit=count]

[7:4131] [vrf:vaak:standaard] laat ip tcp tn-Prod1/ap-Services/epg-NTP(16410) tn-Prod1/l3out-L3Out1/againstP-extEpg(25) eq 123 [contract:uni/tn-Prod1/brc-external_to_ntp] toe [hit=0]
[7:4156] [vrf:vaak:standaard] laat ip tcp tn-Prod1/l3out-L3Out1/AgainstP-extEPG(25) eq 123 tn-Prod1/ap-Services/epg-NTP(16410) toe [contract:uni/tn-Prod1/brc-external_to_ntp] [hit=0]
[12:4169] [vrf:vaak:standaard] ontkennen,log alle tn-Prod1/l3out-L3Out1/againstP-extEpg(25) epg:willekeurige [contract:impliciet] [hit=0]
[16:4167] [vrf:common:default] laat elke epg toe:elke tn-Prod1/bd-Services(32789) [contract:impliciet] [hit=0]

De pakketdalingen kunnen ook in GUI worden getoond via het pad: huurder > Tenant_Name > Operational > Flows/Packets.

overweging

Aanbeveling bij de toepassing van de contracten tussen de EPG's:

1. ACI kan niet worden beschouwd als een firewall in termen van beleidstoewijzing die een hoog Ternary Content Adressable Memory (TCAM)-gebruik kan veroorzaken.

2. Gebruik een reeks filters in plaats van een groot aantal afzonderlijke filters.

3. In de contracten mogen niet meer dan vier filterreeksen worden gebruikt. Het kan hoge Overflow Ternary Content Adressable Memory (OTCAM) verbruiken.

4. Als er voor een EPG een groot aantal havens nodig is, probeer dan een vergunningscontract te gebruiken.

5. Als deel van de oplossing, als u de uitrol van een groot aantal contracten voorziet, overweeg dienovereenkomstig het Forwarding Scale Profile (FSP) te wijzigen.

6. Alvorens een groot aantal contracten te sluiten, bereken de TCAM met behulp van de formule: nr. van Verstrek EPG * Nr. van de consument EPG * Aantal regels.

7. De bestaande TCAM-grootte kan op ACI UI worden gecontroleerd via het pad: Operations > Capacity Dashboard > Leaf Capacity or

LEAF-101# vsh_lc

module-1# toont platform interne hal gezondheid-stats | grop _telling

mcast_count : 0

max_mcast_count : 8192

policy_count : 221

max_policy_count : 65536

beleid_otcam_count: 322

max_policy_otcam_count: 8192

policy_label_count : 0

max_policy_label_count : 0

Enkele uitdagingen van app-centric implementatie en oplossing

1. Een groter aantal opdrachten kan leiden tot een hoog TCAM-gebruik van switches.

Daarom is het belangrijk om het gebruik van TCAM actief te volgen en ook een geschatte verhoging van TCAM-waarde voor te bereiden wanneer een grote hoeveelheid configuratie-inzet wordt gedaan. Het is goed om een maker checker proces te hebben om ervoor te zorgen dat de configuratie die wordt geduwd geschikt is. Het wordt ook aanbevolen de wijzigingen uit te voeren met een juist gepland onderhoudsvenster.

2. bulk configuratie (meer dan 50k TCAM) in een enkele duw van contract kan leiden tot een Policy Manager geheugencrash.

Het wordt aanbevolen om de configuratie in kleinere stukjes te drukken, met name wanneer de configuratie groot is. Dit biedt een systematische en risicovrije benadering van contractconfiguratie. Ook, met elke configuratieduw, meet de verhoging van TCAM waarden.

3. De verkeersstroom wordt niet opgenomen als de toepassingen niet communiceren tijdens de implementatietijd van CSW/Tetration (3-4 weken).

Om een dergelijke situatie te voorkomen, is de beste aanpak om de CSW-/Tetration-gegevens opnieuw te laten verifiëren bij de eigenaren van de toepassing voordat de wijzigingsactiviteit plaatsvindt. Ook, post-implementatie, verifieer de logboeken voor om het even welke mislukkingstoets tellen.

Waardetoevoeging

1. Alle toepassingen zijn gesegmenteerd en beperkt overeenkomstig de richtsnoeren voor centrale banken.

2. Zichtbaarheid van communicatie tussen toepassingen na migratie naar een op de toepassing gerichte inzet.

3. Micro-segmentering van de toepassing wordt bereikt.

4. Eén weergave van de toepassingsstroom. In één Toepassingsprofiel worden de EPG's in kaart gebracht volgens de verkeersstroom, zoals Toepassingsprofiel AP_Banking, om drie EPG's (EPG_Banking_WEB, EPG_Banking_APP en EPG_Banking_DB) te hebben, ongeacht hun IP-subnet.

4. Eén weergave van de toepassingsstroom maakt het oplossen van problemen eenvoudiger.

5. Infra is veiliger.

6. Gestructureerde aanpak voor de tenuitvoerlegging en toekomstige uitbreiding.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.