Bereitstellung der ACI als anwendungszentriert

Inhalt

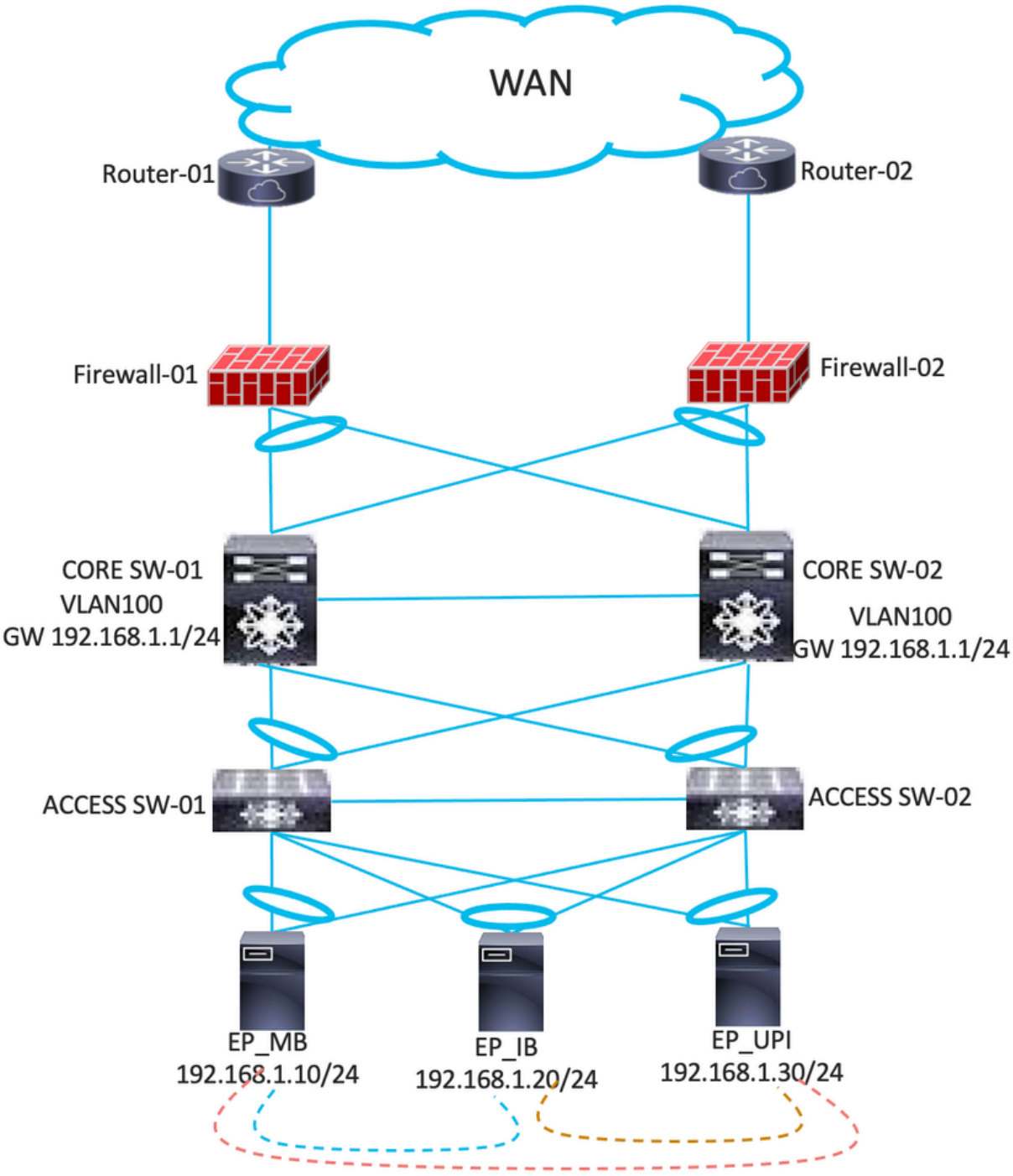
Einleitung

In diesem Dokument wird der Ansatz für Mikrosegmentierung und Sicherheit innerhalb/zwischen den Anwendungen beschrieben, die die SDN-Lösung der Cisco ACI nutzen.

Einschränkungen bei Verwendung traditioneller Netzwerke

- In herkömmlichen Netzwerken ist eine Segmentierung innerhalb eines VLAN/Subnetzes nicht möglich.
- Die Anwendungs-Gateways befinden sich auf Core-Switches. Wenn zwei Anwendungen kommunizieren möchten, sind auf dem Core-Switch komplexe Zugriffskontrolllisten (Access Control Lists, ACLs) erforderlich.
- Die Spanning-Tree-Schleife zwischen den Switches unterbricht den Datenfluss im Rechenzentrum und führt zu einem Datenverlust.
- Das gleiche IP-Subnetz enthält mehrere Anwendungen, die untereinander keine Sicherheit bieten. Die Verwaltung dieser Kommunikation ist in herkömmlichen Netzwerken nicht möglich.
- Betrachten wir ein Beispiel, das auch anhand des Diagramms veranschaulicht wird. Es gibt

drei Anwendungen, EP_MB, EP_IB und EP_UPI, die Teil desselben VLAN und IP-Subnetzes sind. Bei jedem L2-Datenverkehr wird der Datenverkehr immer an alle Anwendungen geleitet, auch wenn keine Kommunikation zwischen ihnen erforderlich ist. Die Einschränkungen zwischen den beiden Anwendungen sind in diesem Szenario nicht möglich.



Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Workload (CSW)/Tetration (Secure Workload) muss in der Umgebung bereitgestellt werden, um die Datenverkehrsflussdaten zwischen den Anwendungen zu erfassen.
- Agenten müssen auf den Servern bereitgestellt werden, um die Daten zu erfassen. Dies ist also nur bei brachliegenden Einsätzen möglich.
- Die Agenten müssen für die Datenerfassung mindestens 3-4 Wochen auf den Servern bereitgestellt werden.
- Wenn keine ADM-Tools (Application Dependency Mapping) verfügbar sind, müssen die entsprechenden Daten bereitgestellt werden.
- Das Server-Gateway muss mithilfe der Application Centric Infrastructure (ACI) Fabric konfiguriert werden.

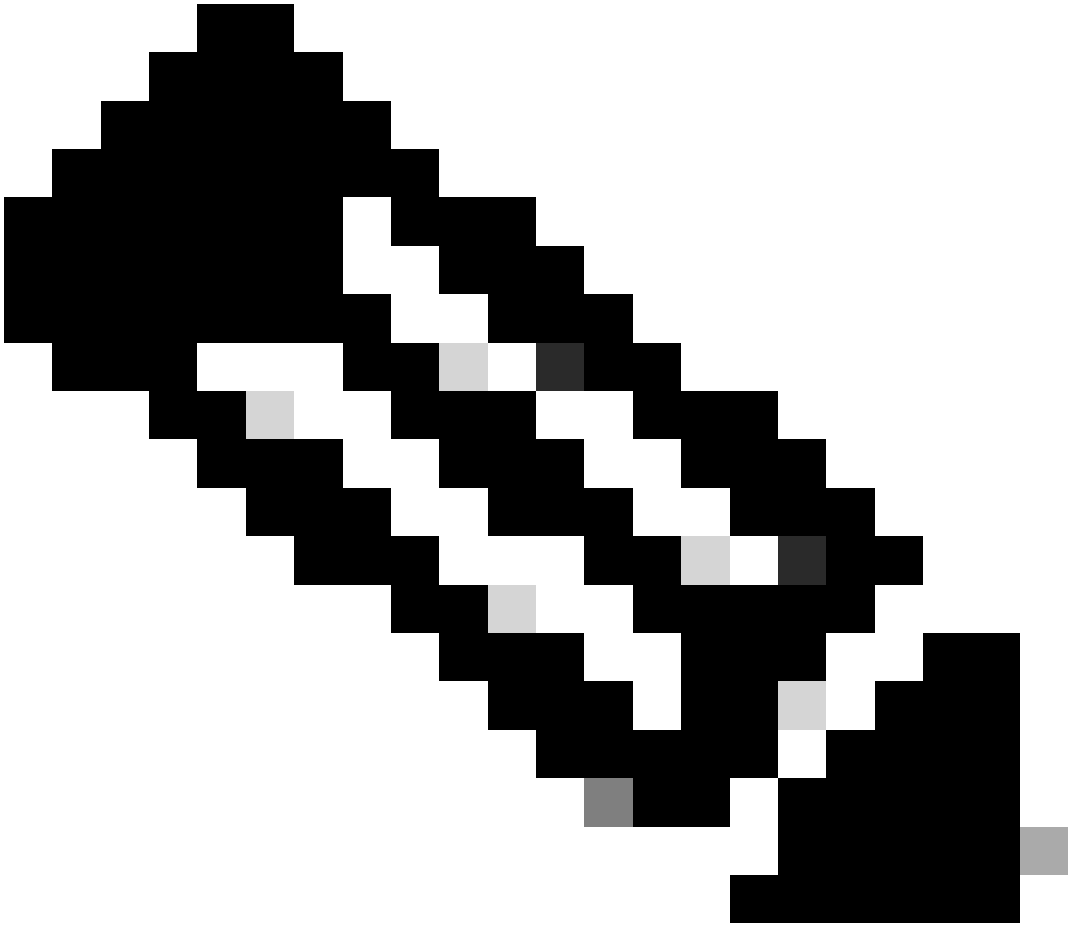
Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Lösungsüberblick

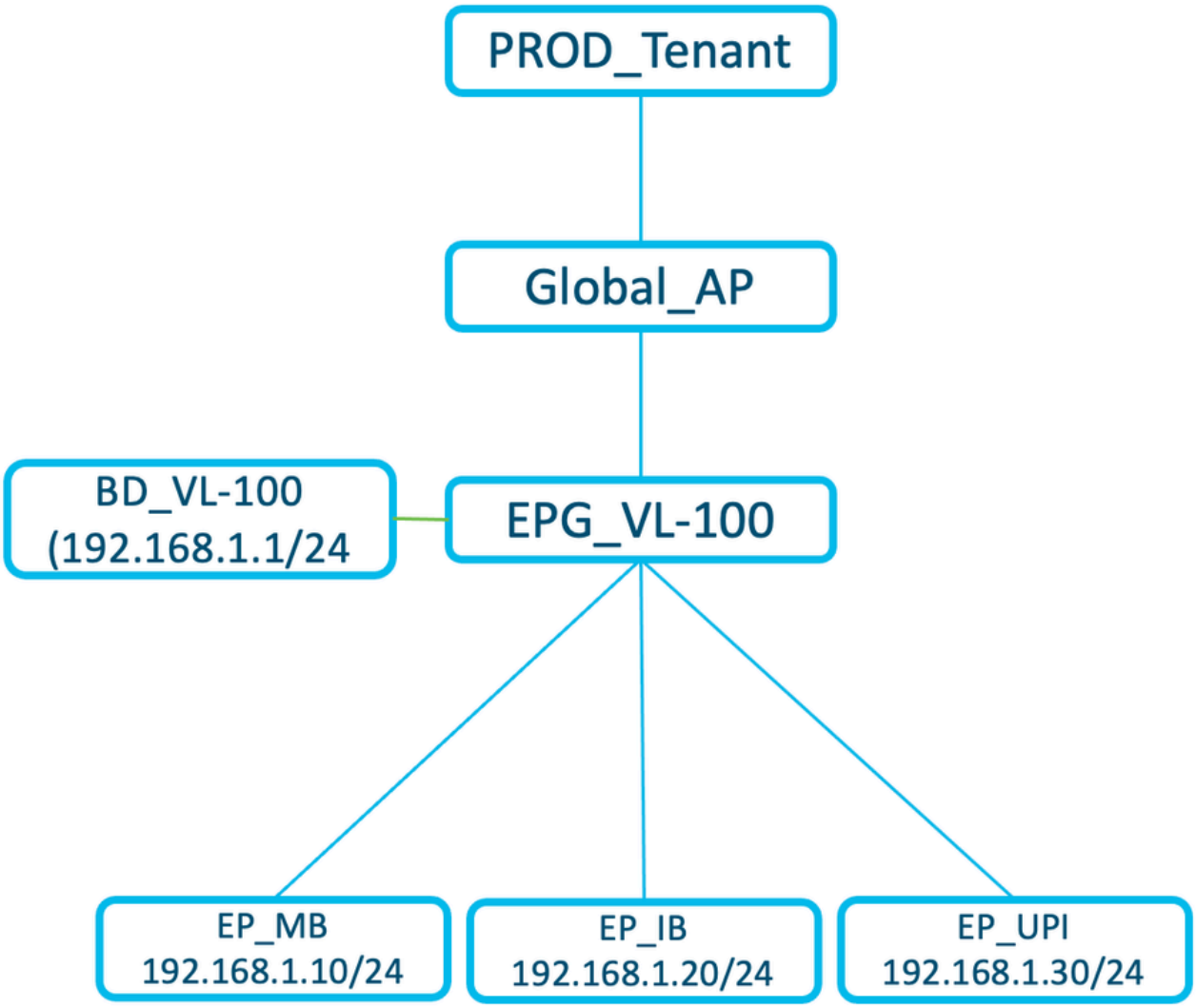
Um eine Mikrosegmentierung zu erreichen, müssen Sie zunächst das Netzwerk von einer herkömmlichen Infrastruktur zu einer Cisco SDN-Lösung migrieren und das Netzwerk anwendungszentriert umgestalten. In diesem Abschnitt werden die beiden Entwurfsphasen beschrieben, um die Segmentierung je nach Anwendungsfluss, der über das ADM-Tool erfasst wird, nach Bedarf zu erreichen. Zunächst wird die Cisco ACI-Lösung im Network Centric Mode bereitgestellt (wie beim vorhandenen Design) und anschließend in den anwendungsorientierten Modus überführt.



Hinweis: Sie können diesen Bereitstellungsmodus auch kombinieren, um Services direkt vom traditionellen Netzwerk in den anwendungsorientierten Modus zu migrieren.

Netzwerkorientiertes Design

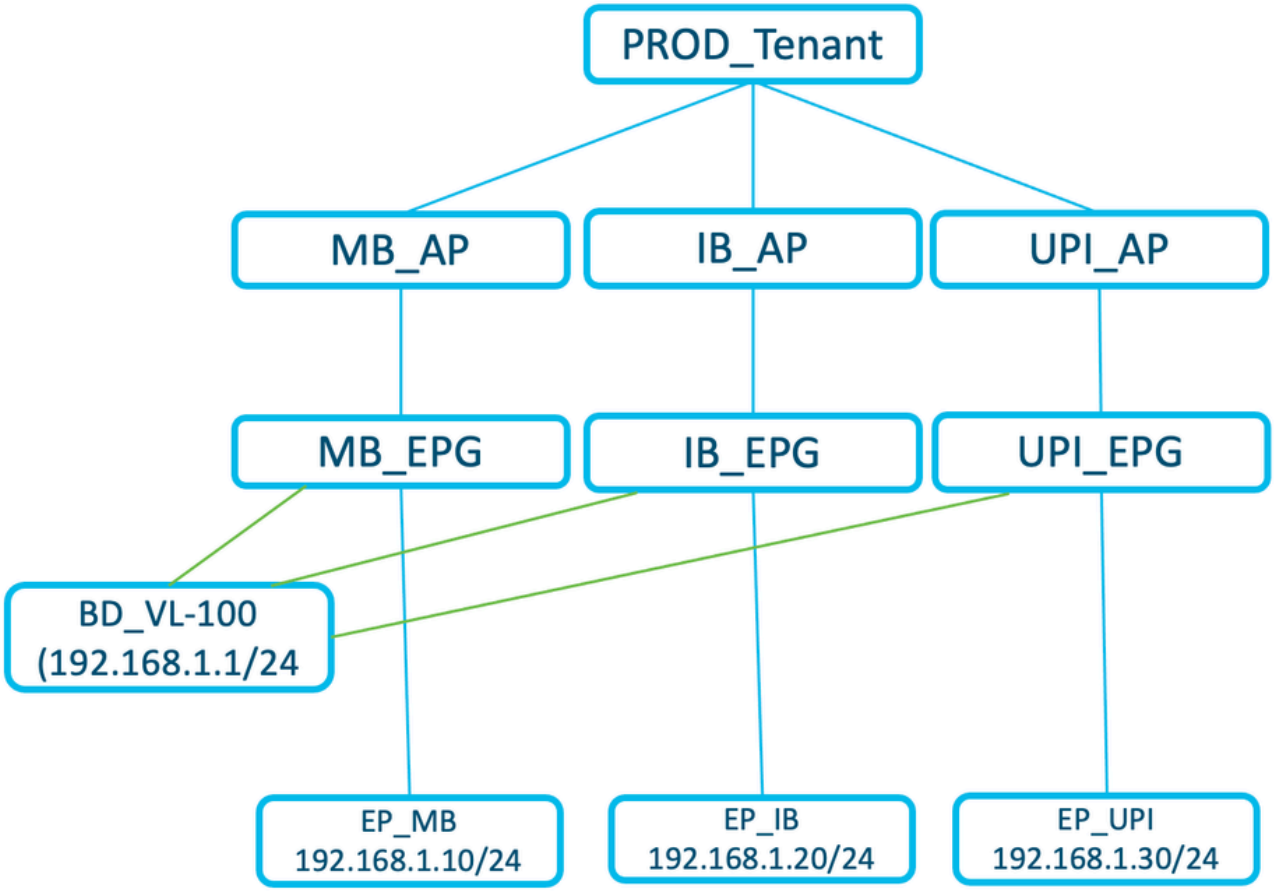
In dem im Diagramm gezeigten Beispiel enthält EPG_VL-100 drei Anwendungen, EP_MB, EP_IB und EP_UPI, verwendet dasselbe IP-Subnetz und VLAN 100.



- Aktuelle Migration vom traditionellen Netzwerk zur ACI
- Eine Endpunktgruppe (EPG) kann mehrere Anwendungen enthalten.
- In diesem Bereitstellungstyp gibt es innerhalb derselben EPG keine Anwendungssegmentierung.
- 1 BD = 1 EPG = 1 VLAN

Anwendungsorientiertes Design

Das im Diagramm gezeigte Beispiel ist eine separate EPG für drei Anwendungen (EP_MB, EP_IB und EP_UPI), die dasselbe IP-Subnetz nutzen und unterschiedliche, jeder EPG zugeordnete VLANs verwenden.

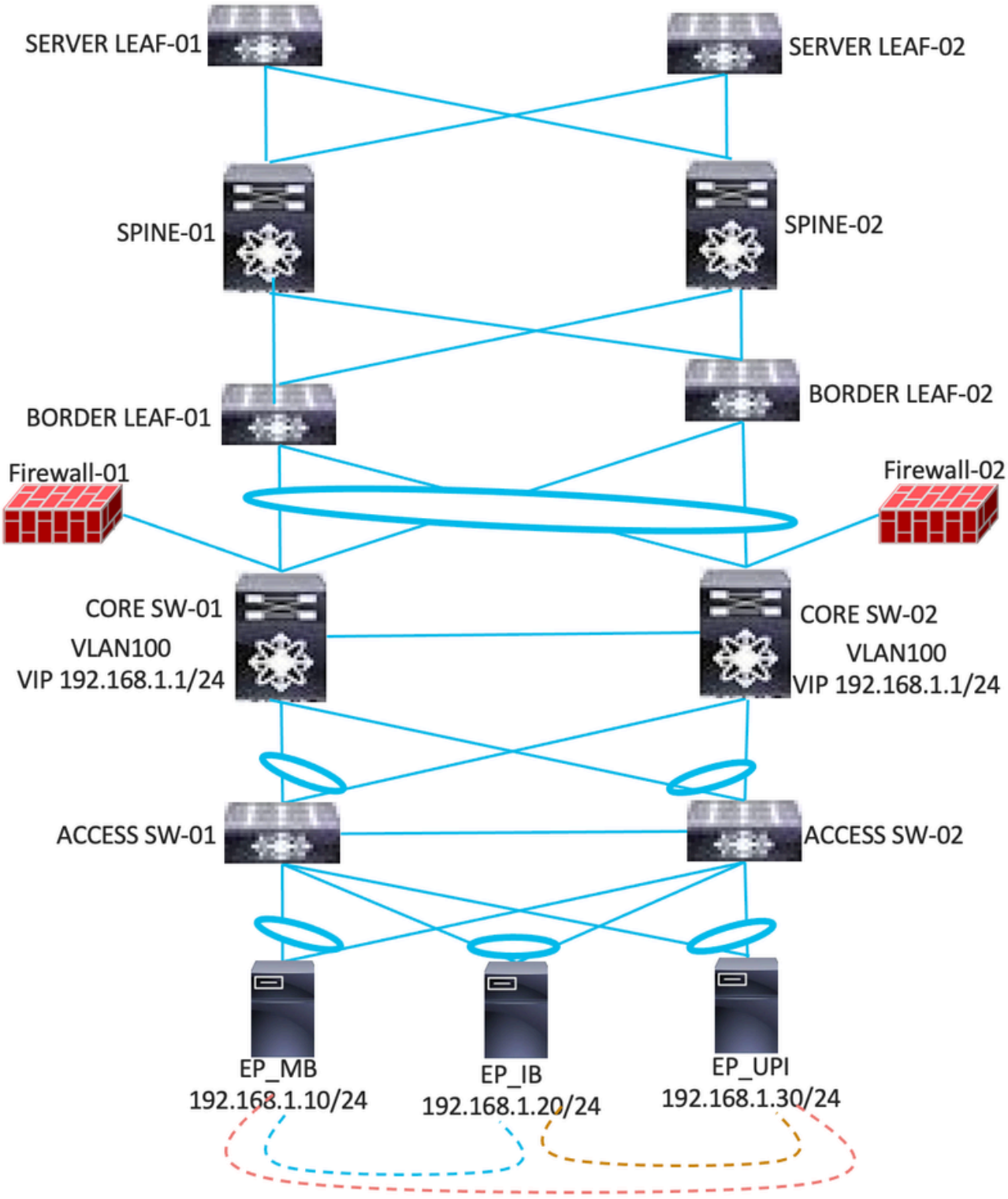


- Beim anwendungsorientierten Bereitstellungstyp werden je nach Anwendung unterschiedliche EPGs konfiguriert.
- Die Anwendungen verwenden weiterhin dasselbe IP-Subnetz und denselben Gateway.
- Die segmentierten Anwendungs-EPGs zur Verwendung eines neuen VLAN.
- 1 BD für die Konfiguration mit dem IP-Subnetz und die Zuordnung zu mehreren Anwendungs-EPGs.
- 1 BD = N EPG = N VLAN
- Jetzt können zwei EPGs (Anwendungen) über den Vertrag miteinander kommunizieren.

Migrationsansätze

Vor der anwendungsorientierten Bereitstellung der ACI kann die ACI netzwerkzentriert bereitgestellt und die Anwendungen segmentiert werden.

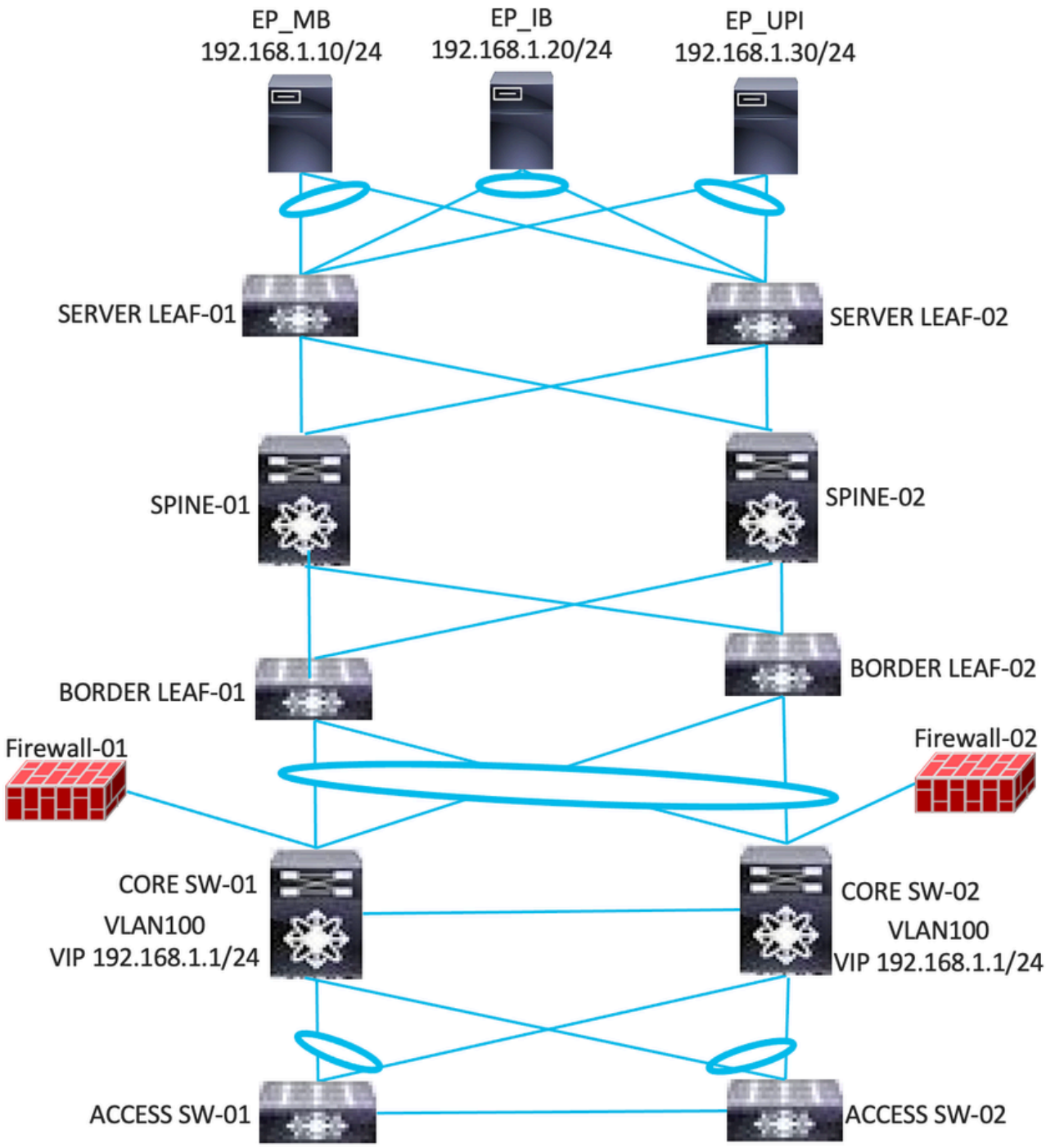
Ansatz für die netzwerkzentrierte Migration: Phase 1



- Zwischen Border Leaf- und Core-Switches muss eine Layer-2-Zwischenverbindung hergestellt werden.
- Konfigurieren Sie die Layer-2-Bridge-Domäne und die Endpunktgruppe auf der ACI entsprechend der vorhandenen, in herkömmlichen Netzwerken konfigurierten VLANs.
- Konfigurieren Sie alle diese VLANs auf der Layer-2-Zwischenverbindung zwischen Border Leaf und Core Switches.
- Die ACI muss alle Endgeräte kennen, die auf Core-Switches vorhanden sind.

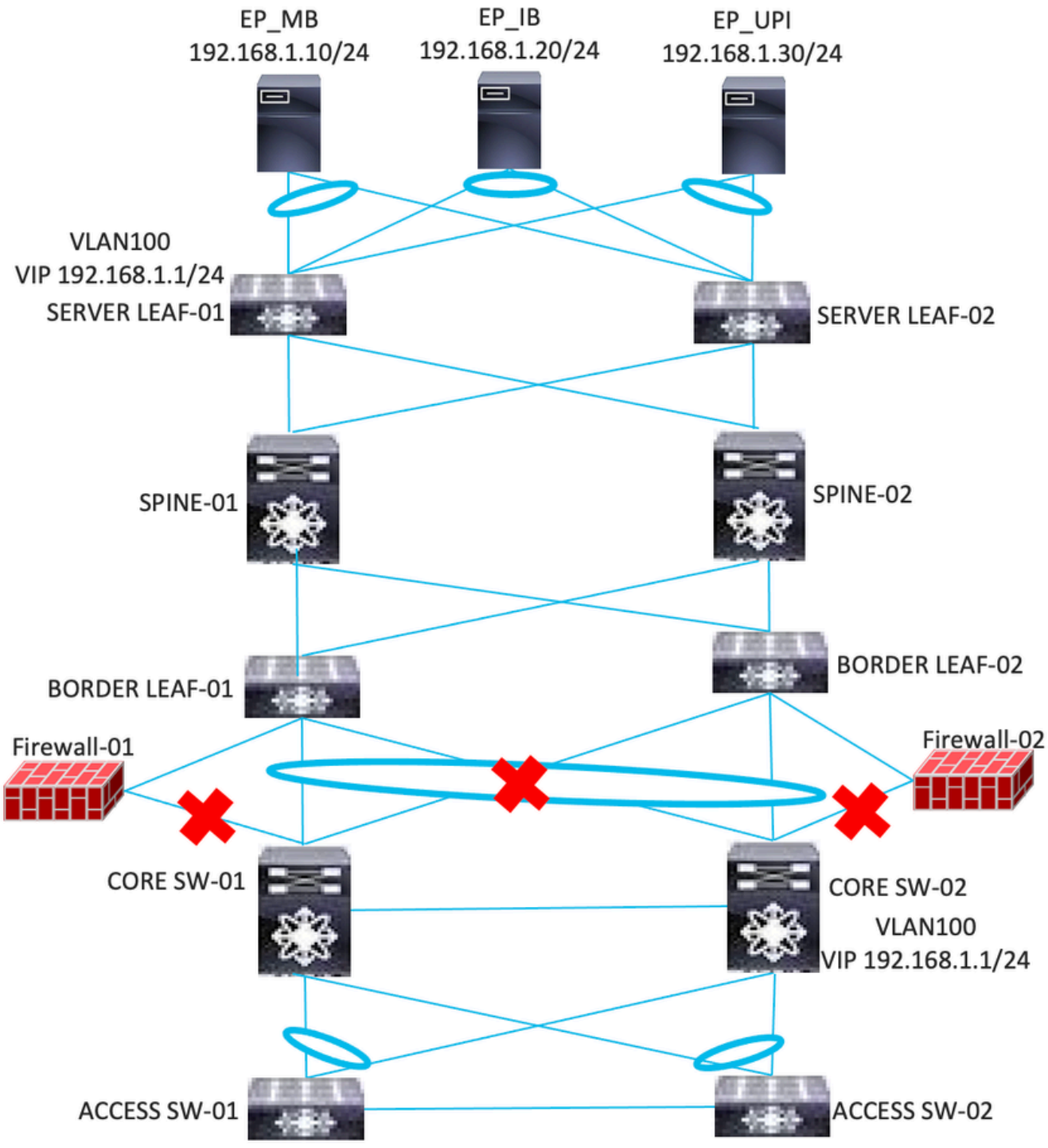
- Das Gateway verbleibt auf den Core-Switches.
- Die Firewall-Konnektivität bleibt bei Core-Switches erhalten.

Ansatz für die netzwerkzentrierte Migration: Phase 2



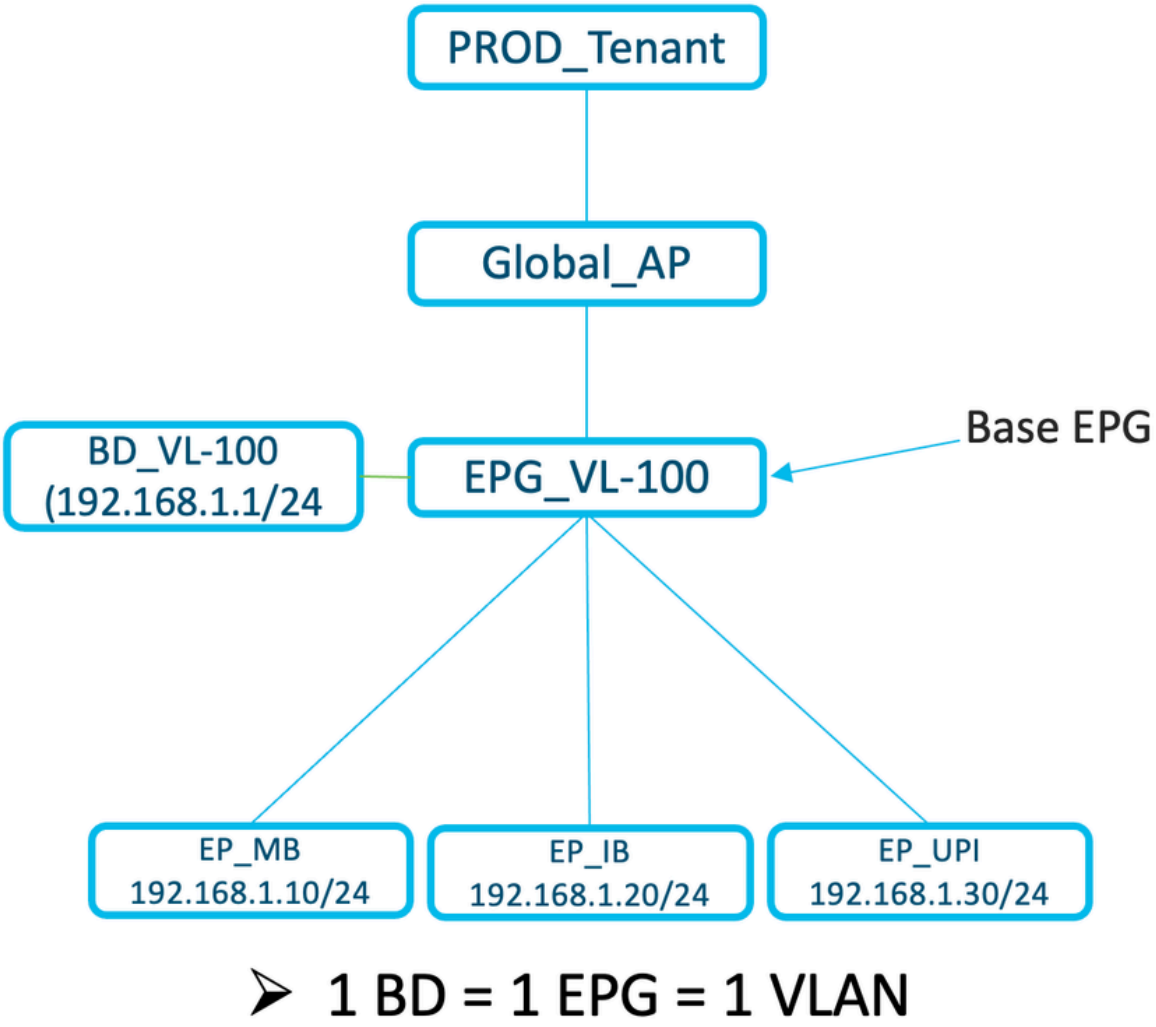
- Verschieben Sie die Workloads von Access Switches auf einen Server-Leaf.
- Gateway bleibt auf Core-Switches.
- Überprüfen Sie, ob das Gateway über die Server erreichbar ist.
- Überprüfen Sie, ob der Server/die Anwendung erreichbar ist.

Ansatz für die netzwerkzentrierte Migration: Phase 3

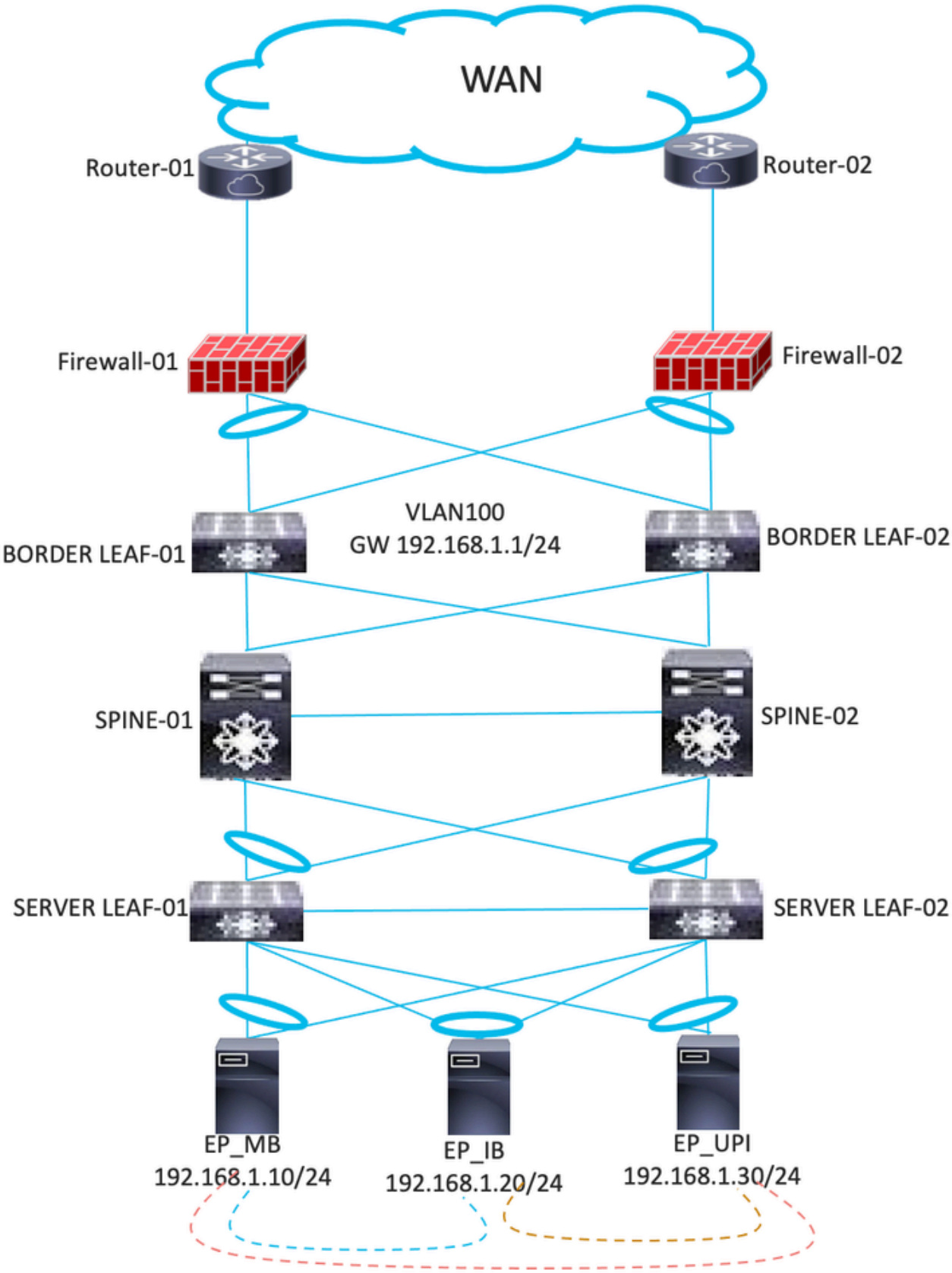


- Schließen Sie die Gateways der Core-Switches, und konfigurieren Sie sie auf der ACI.
- Firewall-Link von Core-Switches auf ACI-Leaf verlagern
- Konfigurieren Sie den L3out zur Firewall/zum Router.
- Fügen Sie die Routen der Firewall/des Routers und der ACI hinzu.
- Fahren Sie die Verbindung zwischen Border Leaf und Core Switches herunter.
- Überprüfen Sie, ob der Server/die Anwendung erreichbar ist.

Logische Darstellung der ACI nach dem Network Centric Migration-Ansatz.



Anwendungsorientierter Migrationsansatz: Phase 1



- Erfassung und Analyse von CSW/Tetration-Daten.
- Neue EPG-Konfiguration gemäß CSW/Tetration Data (WEB, APP und DB).
- Für die MB-Anwendung werden beispielsweise drei EPGs erstellt, z. B. EPG_MB_WEB, EPG_MB_APP und EPG_MB_DB. Diese EPGs müssen unter einem Anwendungsprofil

(AP_MB) konfiguriert werden.
- Im Falle der Virtual Machine Manager (VMM)-Integration ist eine vDS-Konfiguration erforderlich, um die Server in der neuen EPG dem neuen VLAN zuzuordnen.
- Ordnen Sie die virtuelle Maschine (VM) der neuen vDS zu, die durch VMM-Integration unterstützt wird.
- Bei Baremetals muss das Serverteam die VLAN-ID auf dem Server ändern.
- Die IP-Adressierung ist für diese Bereitstellungen identisch.
- Vertragskonfiguration zwischen EPGs gemäß CSW-/Tetration-Daten.

CSW/Tetration Datenanalyse

Beispiel der Analyse auf Basis der CSW/Tetration Daten:

src_ip	Consumer_Scope	dst_ip	Provider_Sco
192.168.34.248	Standard:Intern:Hauptsitz	192.168.20.81	PRODAPP
192.168.78.45	Standard:Intern:Hauptsitz	192.168.20.81	PRODAPP
192.168.78.16	Standard:Intern:Hauptsitz	192.168.20.81	PRODAPP
192.168.78.25	Standard:Intern:Hauptsitz	192.168.20.81	PRODAPP
192.168.44.69	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODAPP
192.168.44.69	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODAPP
192.168.32.173	Standard:Intern:Datacenter:DC:Application:Prod:DMZ	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.48	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP

192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.48	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.29	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.30	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.81	PRODAPP
192.168.44.21	Standard:Intern:Datacenter:DC:Application:Prod:AAA	192.168.20.81	PRODAPP
192.168.103.80	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.71	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.20	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.21	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:DHCP	192.168.20.81	PRODAPP
192.168.44.68	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
192.168.44.69	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
192.168.44.68	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
192.168.44.69	Standard:Intern:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
172.16.32.173	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:MZ	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB

192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.48	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.48	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.47	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.30	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.29	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB
192.168.44.21	Standard:Intern:Datacenter:DC:Application:Prod:Monitoring	192.168.20.85	PRODDB

Beispiel für EPG-Empfehlung aus der CSW/Tetration:

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

Basierend auf den Details müssen die Daten für die Vertragskonfiguration analysiert werden.
Beispiel für analysierte Daten:

src_ip	Consumer_Scope	Consumer_EPG	dst_IP	provider_EPG

192.168.44.69	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Erkennung	EPG_ERKENNUNG	192.168.20.81	EPG-PROD-APP
192.168.44.69	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Erkennung	EPG_ERKENNUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.48	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.48	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.44.47	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.81	EPG-PROD-APP
192.168.103.21	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP
192.168.44.68	Standard:Intern:Rechenzentrum: RZ:Anwendung:Prod:Erkennung	EPG_ERKENNUNG	192.168.20.85	EPG-PROD-DB

192.168.44.68	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Erkennung	EPG_ERKENNUNG	192.168.20.85	EPG-PROD-DB
192.168.44.69	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.69	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.47	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.47	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.48	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.47	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.47	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.48	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.44.47	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Überwachung	EPG_ÜBERWACHUNG	192.168.20.85	EPG-PROD-DB
192.168.48.45	Standard:Intern:Rechenzentrum:RZ:Anwendung:Prod:Backup	EPG_VL_71	192.168.20.85	EPG-PROD-DB

Basierend auf der IP-Adresse werden die Consumer- und Provider-EPGs genannt. Doppelte Einträge und Nord-Süd-Datenverkehr (z. B. Internet, Inter-DC, Datenverkehr zwischen Zonen usw.) müssen von diesen Daten ausgeschlossen werden. Es gibt einige EPGs, die mit VLANs wie EPG_VL_157, EPG_VL_71 usw. benannt sind. Dies bedeutet, dass diese Server im Rahmen der anwendungsorientierten Migration nicht in die Ziel-EPG verschoben werden. Der Vertrag zwischen ihnen muss also mit der aktuellen Zuordnung der EPG konfiguriert werden. Nach der Migration

dieser Server in die Ziel-EPG müssen diese bestehenden Verträge im Rahmen des Bereinigungsprozesses gelöscht und der entsprechende Vertrag zur Ziel-EPG hinzugefügt werden.

Vertrag

Für die Kommunikation zwischen den EPGs sind Verträge erforderlich. In diesem Abschnitt wird der Implementierungsfluss während des Vertragskonfigurationsprozesses erfasst.

1. Zunächst muss VzAny-Vertrag auf VRF-Ebene (Virtual Routing and Forwarding) angewendet werden.

2. Gemäß CSW/Tetration-Daten müssen spezielle EPG-Verträge erstellt werden.

3. Konfigurieren Sie die Deny_All-Regel mit niedriger Priorität, sodass der VzAny-Vertrag keine Kommunikation mit nicht angegebenem Datenverkehr zulässt. Für die Anwendungen, die noch nicht anwendungszentriert migriert sind, erfolgt die Kommunikation per VzAny-Vertrag.

4. Löschen Sie nach der Migration den VzAny-Vertrag aus der VRF-Instanz.

Die Analyse von CSW/Tetration-Daten und deren Umwandlung in entsprechende ACI-Objekte ist ein sehr wichtiger Schritt. Daher ist es nach der ersten Analyse wichtig, unsere Beobachtung mit den Betroffenen zu diskutieren und eine erneute Bestätigung auf dem gleichen. Auch bei der Implementierung muss sorgfältig abgewogen werden, um sicherzustellen, dass der gesamte Datenverkehr wie erwartet zugelassen wird. Zur Fehlerbehebung können Sie die Protokollierung im Vertrag aktivieren und über eine GUI-Schnittstelle oder CLI sämtliche Paketverluste an einem bestimmten Port nachverfolgen.

leaf# show logging ip access-list internal packet-log deny
[Di, 1. Okt. 10:34:37 2019 377572 Benutzer]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unbekannt, Vlan-ID: 0, SMac: 0x000c0c0c0c, DMac:0x000c c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
[Di, 1. Okt. 10:34:36 2019 377731 Benutzer]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unbekannt, Vlan-Id: 0, SMac: 0x000c0c0c0c, DMac:0x000c c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98

Contract_Parser

Ein geräteinternes Python-Skript, das eine Ausgabe erzeugt, die die Zoning-Regeln, Filter und Trefferstatistiken korreliert, während Namenssuchen von IDs durchgeführt werden. Dieses Skript ist äußerst nützlich, da es einen mehrstufigen Prozess ausführt und in einen einzigen Befehl umwandelt, der auf bestimmte EPGs/VRFs oder andere vertragsbezogene Werte gefiltert werden kann.

leaf# contract_parser.py
Wichtigste:
[prio:RuleId] [vrf:{str}] Aktionsprotokoll 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_off 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_off 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] permit any epg:any tn-Prod1/bd-Services(32789) [contract:implicit] [hit=0]

Die Paketverluste können auch in der GUI über den Pfad angezeigt werden: Tenant > Tenant_Name > Operational > Flows/Packets.

Erwägung

Empfehlung bei der Anwendung der Verträge zwischen den EPGs:

1. Die ACI kann im Hinblick auf die Richtlinienzuordnung nicht als Firewall angesehen werden, was zu einer hohen Auslastung des Ternary Content Addressable Memory (TCAM) führen kann.

2. Verwenden Sie eine Reihe von Filtern anstelle einer großen Anzahl von Einzelfiltern.

3. Jeder Vertrag darf nicht mehr als vier Filterbereiche verwenden. Es kann einen hohen Overflow Ternary Content Addressable Memory (OTCAM) beanspruchen.

4. Falls EPGs eine große Anzahl von Ports erfordern, verwenden Sie einen "permit any"-Vertrag.

5. Wenn Sie im Rahmen der Lösung die Bereitstellung einer großen Anzahl von Verträgen vorhersehen, sollten Sie das Forwarding Scale Profile (FSP) entsprechend ändern.

6. Bevor Sie eine große Anzahl von Verträgen bereitstellen, berechnen Sie den TCAM nach folgender Formel: Anzahl EPG bereitstellen * Anzahl EPG für Privatnutzer * Anzahl Regeln.

7. Die vorhandene TCAM-Größe kann in der ACI-Benutzeroberfläche überprüft werden. Verwenden Sie hierzu den Pfad: Operations > Capacity Dashboard > Leaf Capacity or

LEAF-101# vsh_lc

module-1# show platform internal hal health-stats | grep_count

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

Herausforderungen bei der anwendungsorientierten Bereitstellung und Lösung

1. Eine größere Anzahl von Verträgen kann zu einer hohen TCAM-Nutzung von Leaf-Switches führen.

Daher ist es wichtig, die TCAM-Auslastung aktiv zu verfolgen und eine geschätzte Steigerung des TCAM-Werts vorzubereiten, wenn ein großer Teil der Konfigurationsbereitstellung durchgeführt wird. Es empfiehlt sich, einen Prozess zur Maker-Überprüfung einzuführen, um sicherzustellen, dass die Konfiguration, die verschoben wird, angemessen ist. Außerdem wird empfohlen, die Änderungen mit einem ordnungsgemäßen Wartungsfenster durchzuführen.

2. Massenkonfigurationen (mehr als 50.000 TCAMs) in einem einzigen Vertragsschritt können zu einem Speicherabsturz des Policy Managers führen.

Es wird empfohlen, die Konfiguration in kleineren Blöcken zu verschieben, insbesondere wenn die Konfiguration groß ist. Dies ermöglicht einen systematischen und risikolosen Ansatz für die Vertragskonfiguration. Messen Sie bei jedem Konfigurationsschub die Erhöhung der TCAM-Werte.

3. Der Datenverkehrsfluss wird nicht erfasst, wenn die Anwendungen nicht innerhalb der Bereitstellungszeit von CSW/Tetration (3-4 Wochen) kommunizieren.

Um eine solche Situation zu vermeiden, ist der beste Ansatz, die CSW/Tetration-Daten von den Anwendungseigentümern vor der Änderung überprüfen zu lassen. Überprüfen Sie nach der Implementierung die Protokolle auf die Anzahl der Fehlschläge.

Wertschöpfung

(1) Alle Anwendungen wurden segmentiert und gemäß den Leitlinien für das Zentralbankwesen eingeschränkt.

2. Transparenz der anwendungsübergreifenden Kommunikation nach der Migration zu einer anwendungszentrierten Bereitstellung

3. Mikrosegmentierung der Anwendung wird erreicht.

4. Eine Ansicht des Anwendungsflusses. In einem Anwendungsprofil werden die EPGs entsprechend dem Datenverkehrsfluss (z. B. Anwendungsprofil AP_Banking) zugeordnet, damit unabhängig vom IP-Subnetz drei EPGs (EPG_Banking_WEB, EPG_Banking_APP und EPG_Banking_DB) vorhanden sind.

4. Eine Ansicht des Anwendungsflusses erleichtert die Fehlerbehebung.

5. Infra ist sicherer.

6. Strukturierter Ansatz für die Umsetzung und künftige Erweiterung.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.