將ACI部署為以應用為中心的

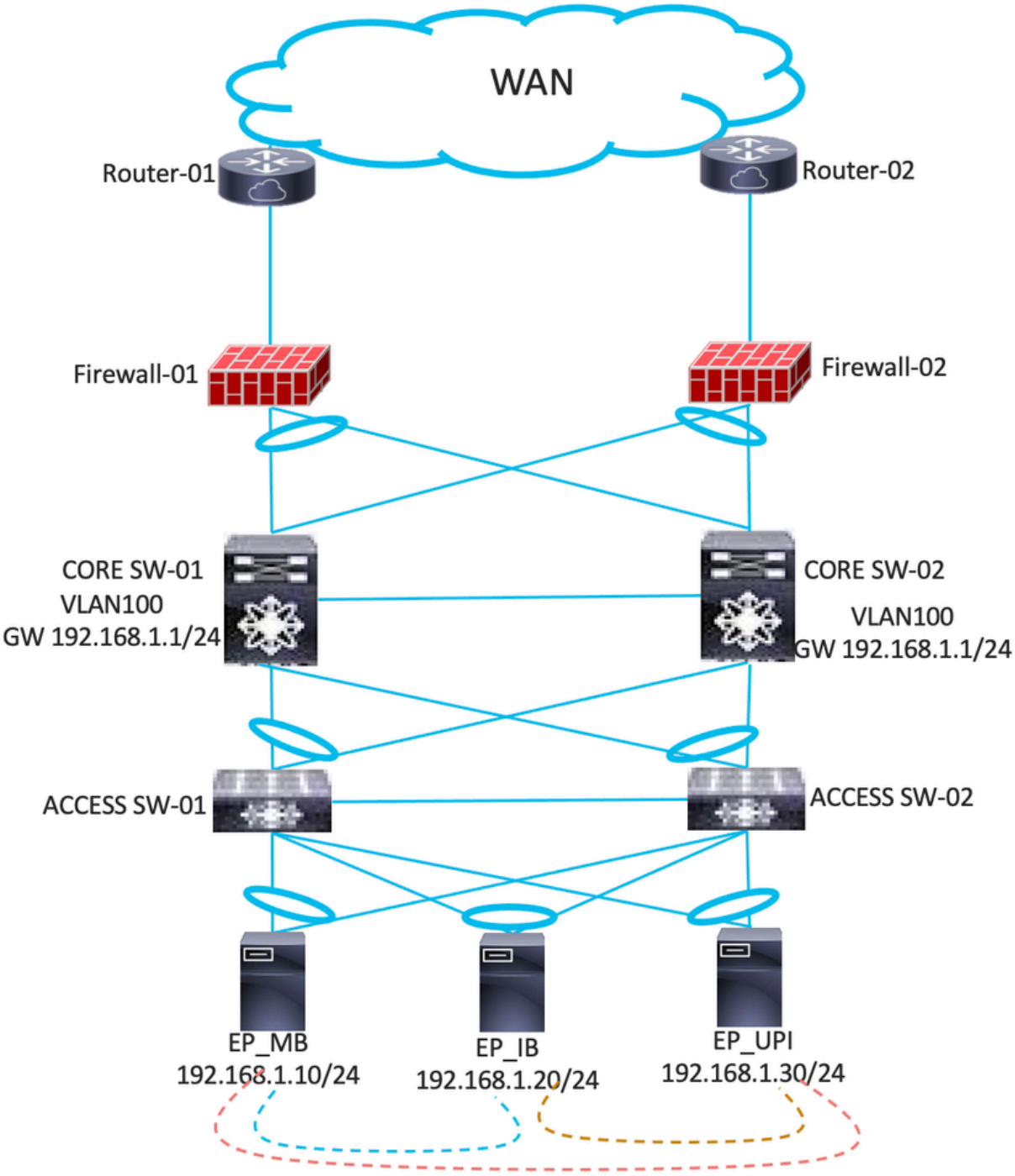
目錄

簡介

本文檔介紹利用思科ACI SDN解決方案在應用內部/之間實現微分段和安全的方法。

使用傳統網路的限制

- 在傳統網路中，不可能在VLAN/子網內進行分段。
- 應用網關位於核心交換機上。如果兩個應用程式想要通訊，則核心交換器上需要複雜的存取控制清單(ACL)。
- 交換機之間的生成樹環路會中斷資料中心流量並導致流量下降。
- 同一個IP子網包含多個應用程式，它們之間不提供安全性。傳統網路無法管理這些通訊。
- 請考慮使用圖示所描述的範例。您有三個應用程式EP_MB、EP_IB和EP_UPI，它們屬於同一VLAN和IP子網。對於任何L2流量，流量始終會泛洪到所有應用，即使它們之間不需要通訊。在此案例中，兩個應用程式之間的限制是不可能的。



必要條件

需求

思科建議您瞭解以下主題：

- 必須在環境中部署思科安全工作負載(CSW)/Tetration（安全工作負載），以便收集應用之間的流量資料。
- 必須在伺服器上部署代理才能收集資料。因此，這只有在棕地部署的情況下才可能實現。
- 代理程式必須在伺服器上部署至少3-4週，才能進行資料收集。

- 如果無法使用任何應用程式相依性對應(ADM)工具，則必須提供相關資料。
- 必須使用以應用為中心的基礎設施(ACI)交換矩陣配置伺服器網關。

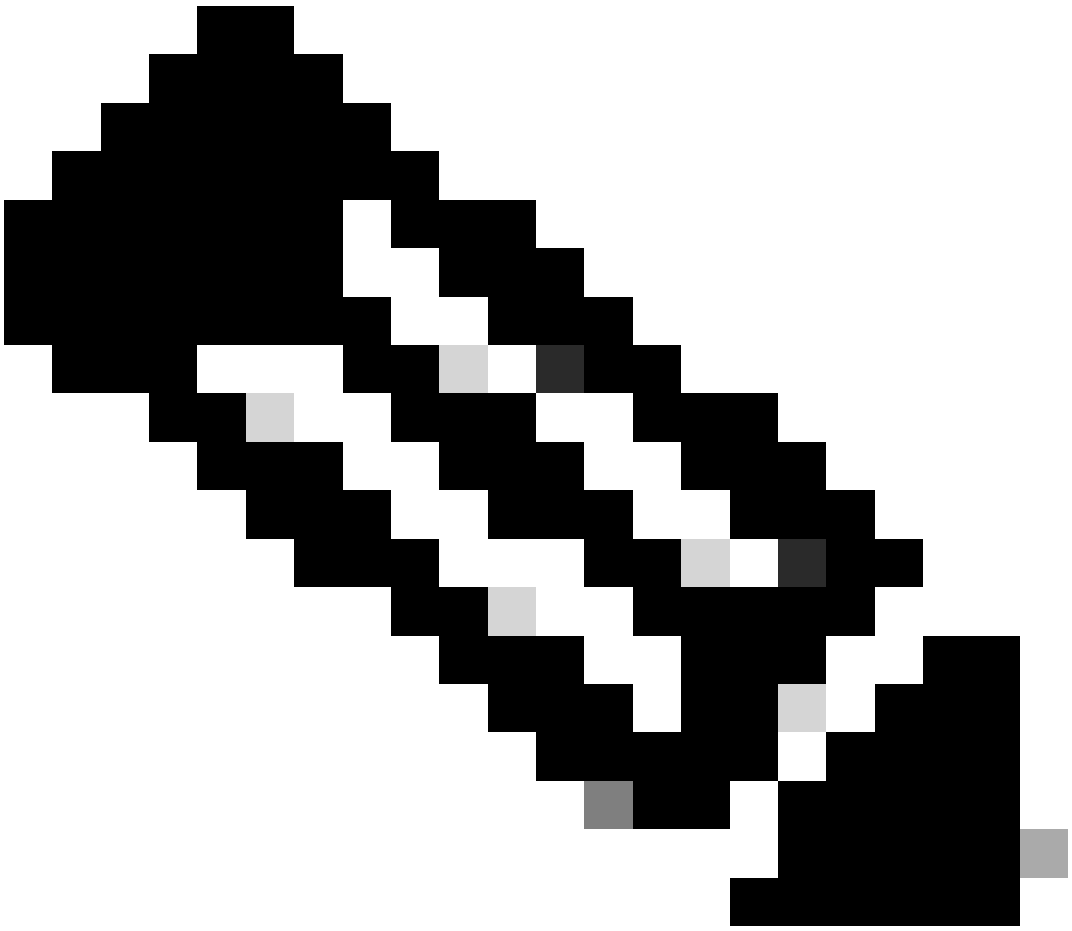
採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

解決方案概述

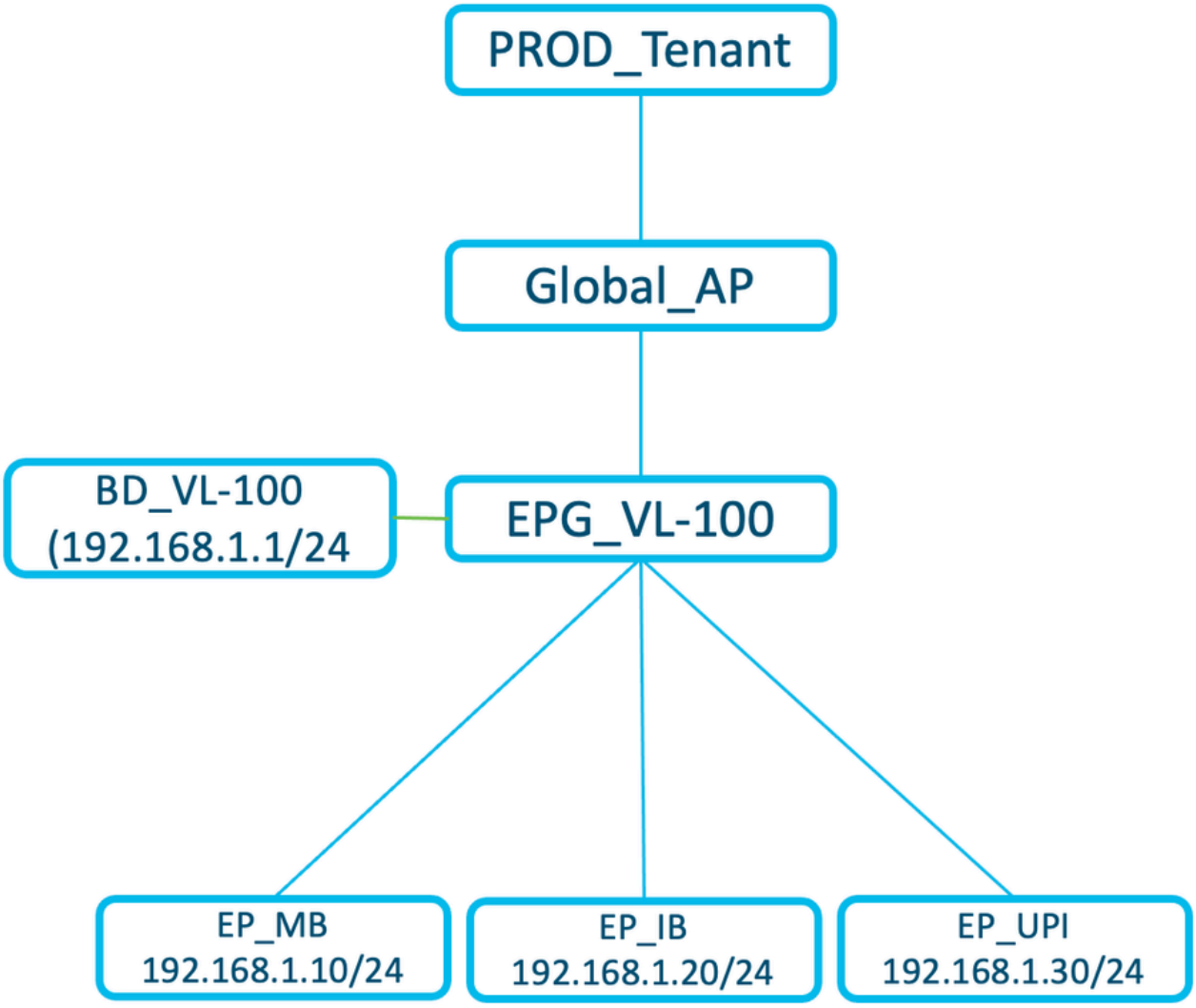
要實現微分段，您必須首先將網路從傳統基礎設施遷移到Cisco SDN解決方案，然後從以應用為中心的角度重新設計網路。本節介紹兩個設計階段，以便根據透過ADM工具捕獲的應用程式流實現所需的分段。首先，思科ACI解決方案以網路中心模式部署（按現有設計部署），然後轉向以應用為中心的模式。



注意：您也可以將此部署模式組合在一起，以便將服務從傳統網路直接遷移到以應用為中心的模式。

以網路為中心的設計

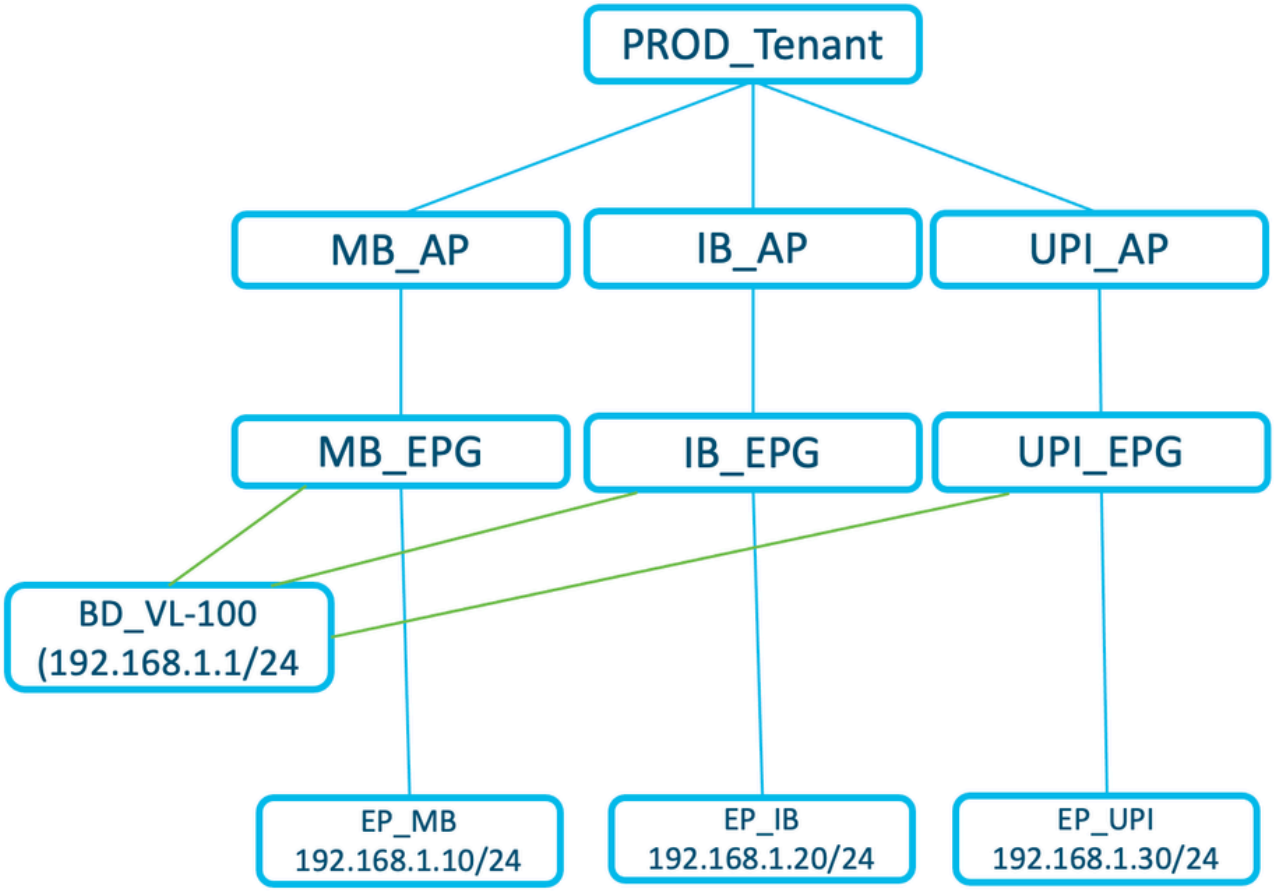
在圖中所示的示例中，EPG_VL-100包含三個應用程式：EP_MB、EP_IB和EP_UPI，並且共用同一個IP子網並使用VLAN 100。



- 從傳統網路向ACI的原樣遷移。
- 一個終端組(EPG)可以包含多個應用。
- 此部署型別中的同一EPG內沒有應用分段。
- 1 BD = 1 EPG = 1 VLAN

以應用為中心的設計

圖中所示的示例是三個應用程式EP_MB、EP_IB和EP_UPI共用同一IP子網並使用對映到每個EPG的不同VLAN的獨立EPG。

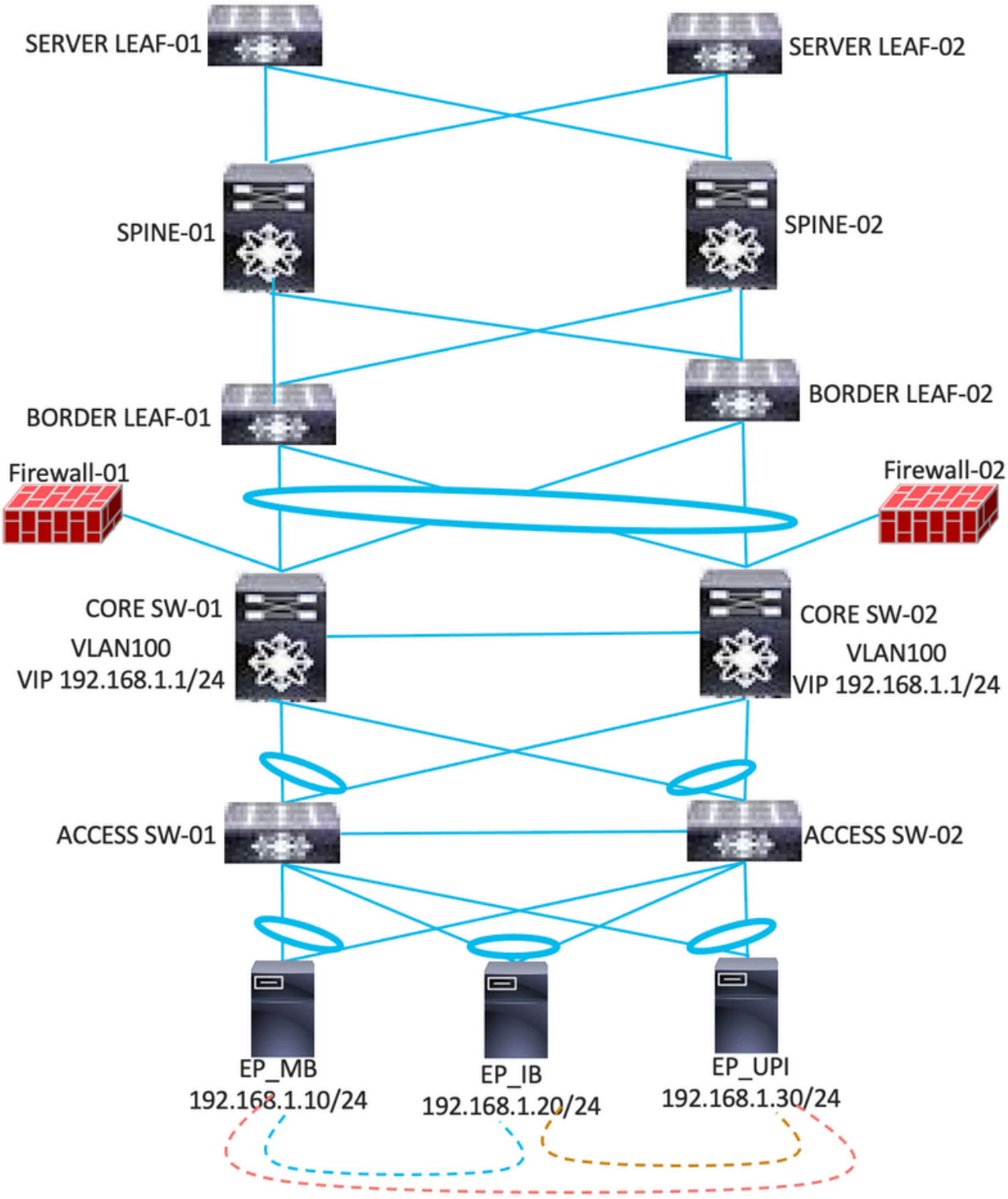


- 在以應用為中心的部署型別中，根據應用配置不同的EPG。
- 這些應用程式繼續使用相同的IP子網及其網關。
- 分段應用EPG使用新的VLAN。
- 1個BD將配置為IP子網並對映到多個應用EPG。
- 1 BD = N EPG = N VLAN
- 現在，兩個EPG（應用程式）可以透過合約相互通訊。

遷移方法

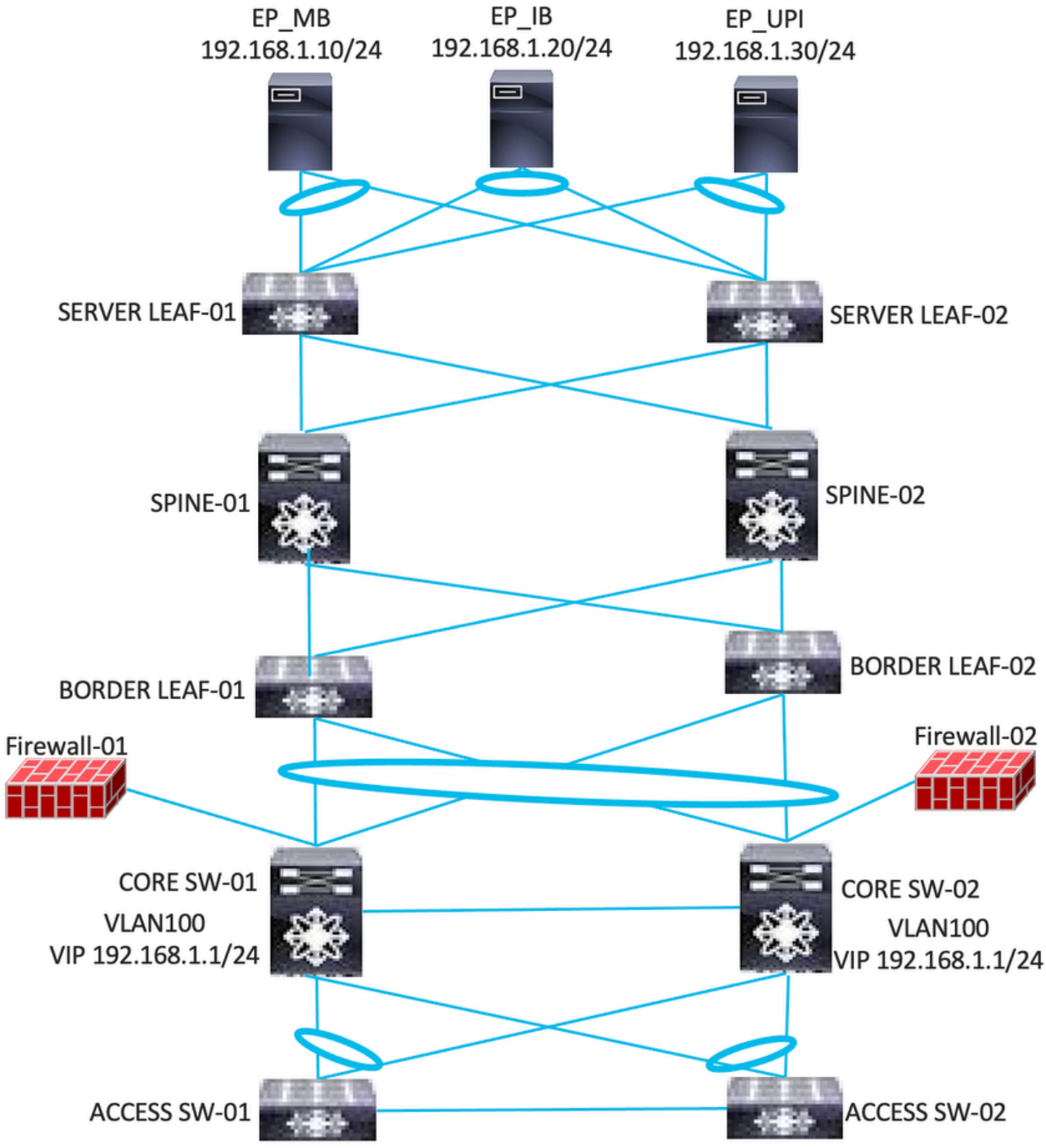
在將ACI部署為以應用為中心之前，可以將ACI部署為以網路為中心，還可以對應用進行分段。

以網路為中心的遷移方法：第1階段



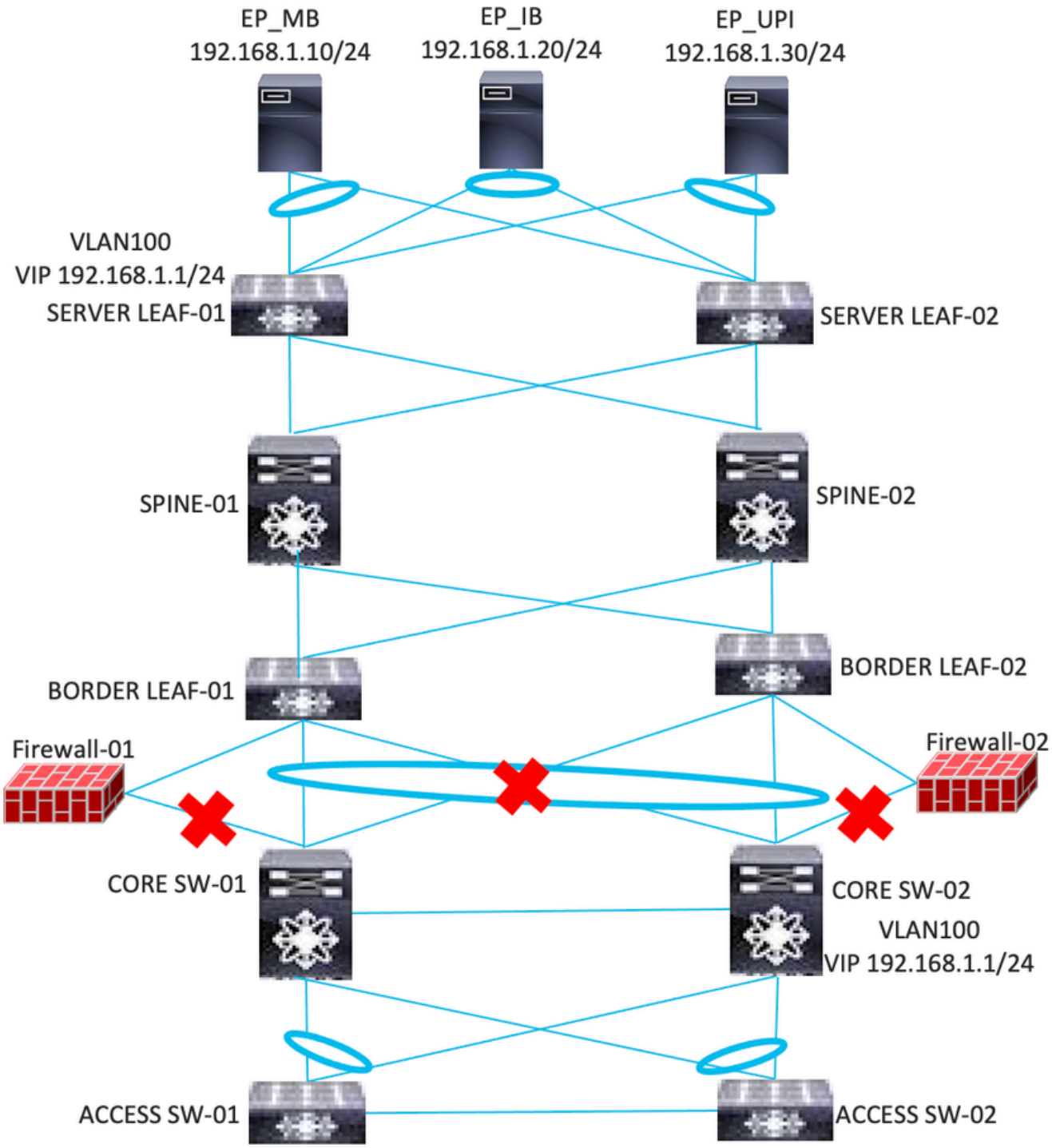
- 必須在邊界枝葉和核心交換機之間建立第2層臨時鏈路。
- 根據傳統網路中配置的現有VLAN，在ACI上配置第2層網橋域和終端組。
- 在邊界枝葉和核心交換機之間的第2層臨時鏈路上配置所有這些VLAN。
- ACI必須瞭解核心交換機上存在的所有終端。
- 網關仍保留在核心交換機上。
- 防火牆連線仍保留在核心交換機上。

以網路為中心的遷移方法：第2階段



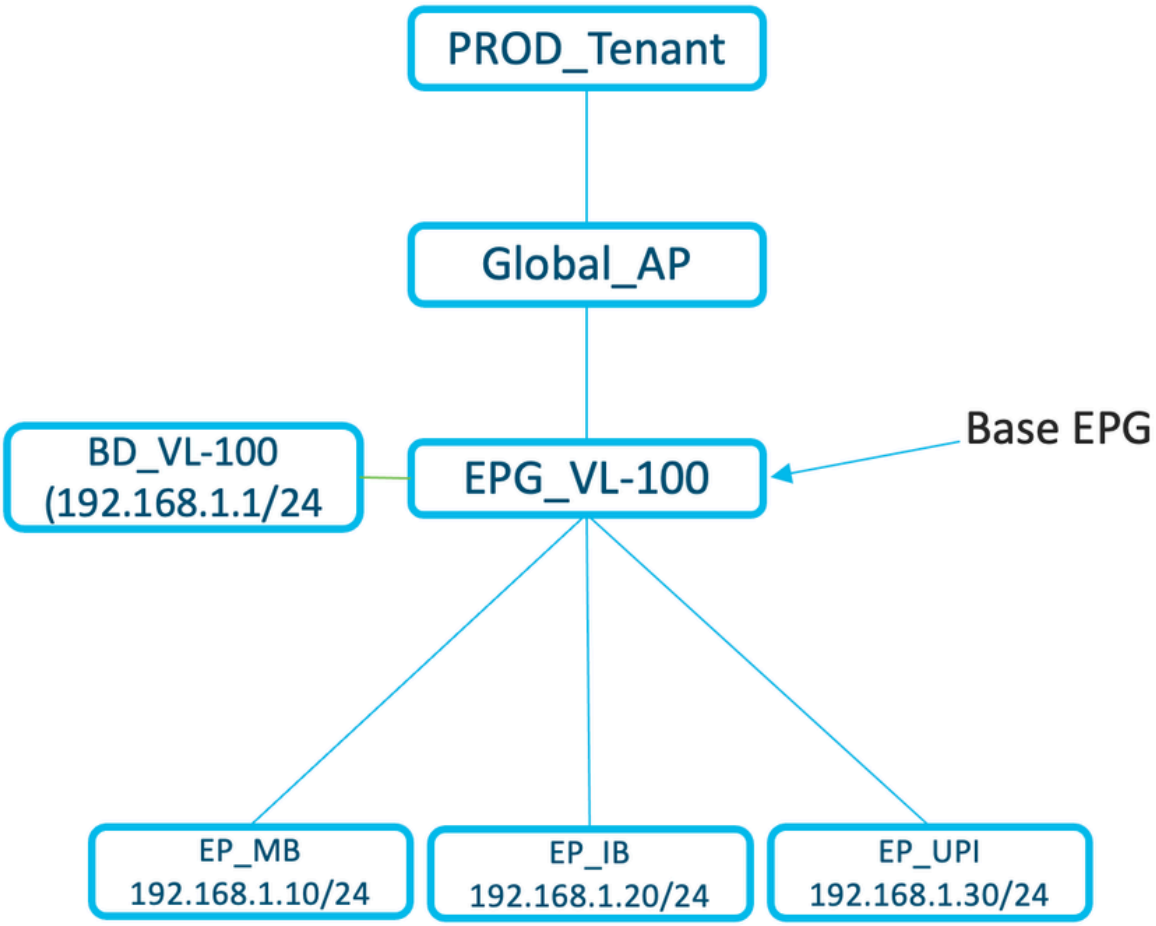
- 將工作負載從接入交換機轉移到伺服器枝葉。
- 網關保留在核心交換機上。
- 確認可從伺服器連線至閘道。
- 確認伺服器/應用程式可連線。

以網路為中心的遷移方法：第3階段

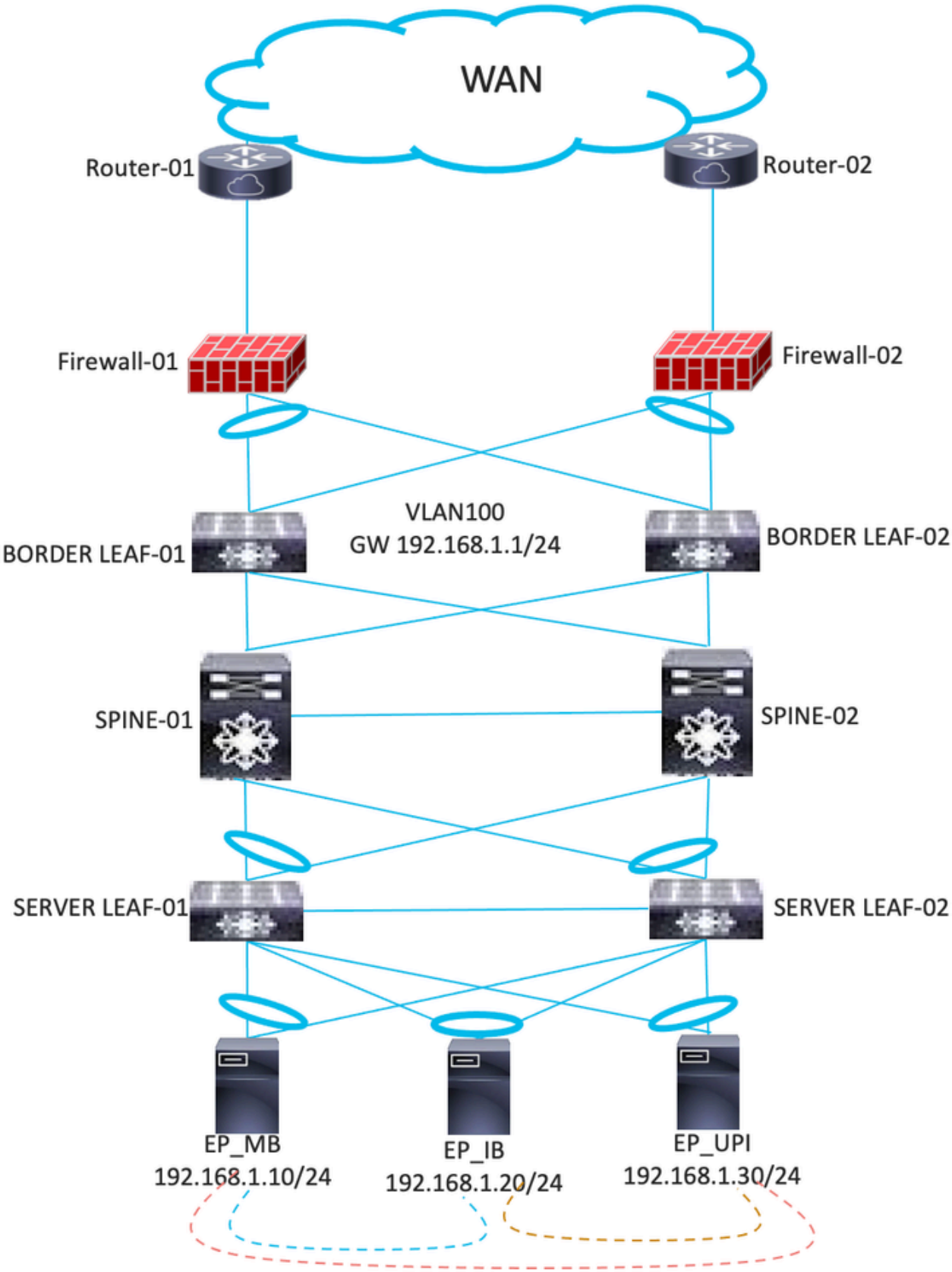


- 關閉核心交換機上的網關並配置ACI。
- 將防火牆鏈路從核心交換機轉移到ACI枝葉。
- 配置通往防火牆/路由器的L3out。
- 在防火牆/路由器和ACI枝葉中增加路由。
- 關閉邊界枝葉和核心交換機之間的鏈路。
- 確認伺服器/應用程式可連線。

以網路為中心的遷移方法後ACI的邏輯表示。



以應用為中心的遷移方法：第1階段



- CSW/Tetration資料的收集和分析。
- 根據CSW/Tetration資料（WEB、APP和DB）新建EPG配置。
- 例如，對於MB應用程式，會建立三個EPG，例如EPG_MB_WEB、EPG_MB_APP和EPG_MB_DB。這些EPG必須在一個應用配置檔案AP_MB下配置。

- 如果是Virtual Machine Manager (VMM)整合，則需要vDS配置來將新EPG中的伺服器對映到新VLAN。
- 將虛擬機器(VM)對映到透過VMM整合推送的新vDS。
- 對於裸機，伺服器組必須更改伺服器上的VLAN ID。
- 這些部署的IP編址相同。
- 根據CSW/Tetration資料在EPG之間配置合約。

CSW/Tetration資料分析

基於CSW/Tetration資料的分析示例：

src_ip	consumer_scope	dst_ip	provider_scope	通訊協定	連接埠
192.168.34.248	預設：內部：總部	192.168.20.81	PRODAPP	TCP	443
192.168.78.45	預設：內部：總部	192.168.20.81	PRODAPP	TCP	443
192.168.78.16	預設：內部：總部	192.168.20.81	PRODAPP	TCP	443
192.168.78.25	預設：內部：總部	192.168.20.81	PRODAPP	TCP	443
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：探索	192.168.20.81	PRODAPP	UDP	137
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：探索	192.168.20.81	PRODAPP	TCP	445
192.168.32.173	預設：內部：資料中心：DC：應用程式：產品：DMZ	192.168.20.81	PRODAPP	TCP	7777
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	135
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品	192.168.20.81	PRODAPP	UDP	137

	：監督				
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	UDP	137
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	443
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	445
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	445
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	5985
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	49154
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	49169
192.168.44.29	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	4750
192.168.44.30	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.81	PRODAPP	TCP	4750
192.168.44.21	預設：內部：資料中心	192.168.20.81	PRODAPP	ICMP	0

	：DC：應用程式 ：Prod：AAA				
192.168.103.80	預設：內部：資料中心 ：DC：應用程式 ：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.71	預設：內部：資料中心 ：DC：應用程式 ：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.20	預設：內部：資料中心 ：DC：應用程式 ：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.21	預設：內部：資料中心 ：DC：應用程式 ：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.44.68	預設：內部：資料中心 ：DC：應用程式：產品 ：探索	192.168.20.85	PRODDB	UDP	137
192.168.44.69	預設：內部：資料中心 ：DC：應用程式：產品 ：探索	192.168.20.85	PRODDB	UDP	137
192.168.44.68	預設：內部：資料中心 ：DC：應用程式：產品 ：探索	192.168.20.85	PRODDB	TCP	445
192.168.44.69	預設：內部：資料中心 ：DC：應用程式：產品 ：探索	192.168.20.85	PRODDB	TCP	445
172.16.32.173	預設：內部：資料中心 ：DC：應用程式 ：Prod：MZ	192.168.20.85	PRODDB	TCP	1522

192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	135
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	UDP	137
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	UDP	137
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	UDP	161
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	445
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	445
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	5985
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	49154
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	60801
192.168.44.30	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	4750

192.168.44.29	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	TCP	4750
192.168.44.21	預設：內部：資料中心：DC：應用程式：產品：監督	192.168.20.85	PRODDB	ICMP	0

CSW/Tetration的EPG建議示例：

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

根據詳細資訊，必須分析合約配置的資料。分析資料的範例：

src_ip	consumer_scope	消費者_EPG	dst_IP	provider_EPG	通訊協定	連接埠
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：探索	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	UDP	137
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：探索	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	135
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	UDP	137

	：監督					
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	443
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	5985
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	49154
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	49169
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	4750
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	ICMP	0
192.168.103.21	預設：內部：資料中心：DC：應用程式：Prod：DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TCP	7777

192.168.44.68	預設：內部：資料中心：DC：應用程式：產品：探索	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.68	預設：內部：資料中心：DC：應用程式：產品：探索	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	135
192.168.44.69	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UDP	161
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	5985
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	49154
192.168.44.47	預設：內部：資	EPG_MONITORING	192.168.20.85	EPG-PROD-	TCP	60801

	料中心：DC：應用程式：產品：監督			DB		
192.168.44.48	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	4750
192.168.44.47	預設：內部：資料中心：DC：應用程式：產品：監督	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	ICMP	0
192.168.48.45	預設：內部：資料中心：DC：應用程式：產品：備份	EPG_VL_71	192.168.20.85	EPG-PROD-DB	TCP	5555

根據IP地址，會提及消費者和提供商EPG。必須在此資料中排除重複條目和北-南流量（例如Internet、DC間、區域間流量等）。有些EPG以VLAN命名，例如EPG_VL_157、EPG_VL_71等。這意味著在以應用為中心的遷移過程中，這些伺服器不會移動到目標EPG。因此，它們之間的合約將配置當前EPG對映。將這些伺服器遷移到目標EPG後，作為清除過程的一部分，必須刪除這些現有合約，並且必須將相應的合約增加到目標EPG中。

合約

EPG之間的通訊需要合約。 本節將介紹合約配置流程中的實施流程。

1. 最初Vz任何合約必須應用於虛擬路由和轉發(VRF)級別。

2. 根據CSW/Tetration資料，必須建立特定的EPG合約。

3. 將Deny_All規則配置為低優先順序，以便VzAny合約不允許未指定的流量通訊。對於尚未作為以應用為中心的應用進行遷移的應用，通訊透過VzAny合約進行。

4. 完成所有遷移後，從VRF中刪除VzAny合約。

分析CSW/Tetration資料並將其轉換為適當的ACI對象是非常關鍵的一步。因此，經過初步分析後，有必要與有關方面討論我們的觀察結果，並就此得到重新確認。此外，在實施過程中，必須仔細考慮以確保所有流量都能如預期那樣被允許。對於故障排除，您可以啟用合約登入，還可以使用GUI介面或CLI跟蹤特定埠上的任何資料包丟棄。

leaf# show logging ip access-list internal packet-log deny
[2019年10月1日星期二10:34:37 377572 usecs]：CName：Prod1：VRF1(VXLAN：

2654209)，VlanType：未知，Vlan-
Id：0，SMac：0x000c0c0c0c0c，DMac：0x000c0c0c0c0c，SIP：192.168.21.11，DIP：192.168
.22.11，埠：0，DP埠：0，源介面：隧道7，協定：1，PktLen：98
[2019年10月1日星期二10:34:36 377731 usecs]： CName： Prod1：VRF1(VXLAN： 2654209)，
VlanType： Unknown， Vlan-Id： 0， SMac： 0x000c0c0c0c0c， DMac：0x000c0c0c， SIP：
192.16.21.11， DIP： 192.168 .22.11，埠：0，DP埠：0，源介面：隧道7，協定：1，PktLen：98

contract_parser

一種裝置上Python指令碼，用於生成輸出，該輸出將分割槽規則、過濾器和命中統計資訊關聯，同時從ID執行名稱查詢。此指令碼非常有用，因為它採用多步驟過程並將其轉化為單個命令，該命令可過濾為特定EPG/VRF或其他合約相關值。

leaf# contract_parser.py
主要:
[prio：RuleId] [vrf：{str}]操作協定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 [合約：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) [合約：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]允許任何epg：any tn-Prod1/bd-Services(32789)
[contract：implicit] [hit=0]

也可以使用路徑Tenant > Tenant_Name > Operational > Flows/Packets在GUI中顯示資料包丟棄。

考慮事項

在應用EPG之間的合約時提出的建議：

1. 在策略對映方面，不能將ACI視為防火牆，因為這樣會導致三重內容可定址記憶體(TCAM)利用率過高。

2. 使用一定範圍的過濾條件，而不使用大量的個別過濾條件。

3. 任何合約不得使用超過四個範圍的過濾條件。本發明可消耗高溢位三元內容可定址儲存器(OTCAM)。

4. 如果任何EPG需要大量埠，請嘗試使用「允許任何」合約。

5. 作為解決方案的一部分，如果您預計部署大量合約，請考慮相應地修改轉發規模配置檔案(FSP)。

6. 在部署大量合約之前，請使用以下公式計算TCAM：提供EPG的數量*消費者EPG的數量*規則數量。

7. 可以使用以下路徑在ACI UI上檢查現有的TCAM大小：操作>容量控制台>枝葉容量或

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

以應用為中心的部署和解決方案面臨的一些挑戰

1. 合約數量較多可能導致枝葉交換機的TCAM利用率較高。

因此，主動追蹤TCAM使用率，並在完成大量配置部署後預估TCAM價值增加非常重要。最好使用maker檢查器進程，以確保推送的配置正確。此外，建議使用適當的計畫維護時段執行更改。

2. 一次推送一次合約即可進行批次配置（超過50,000個TCAM）可能會導致策略管理器記憶體崩潰。

建議以較小的區塊推送配置，尤其是在配置較大時。這為合約配置提供了一種系統化和無風險的方法。此外，每次推入組態時，都會測量TCAM值的增加量。

3. 如果應用在CSW/Tetration部署時間間隔（3-4週）內未通訊，則不會捕獲流量。

為了避免這種情況，最佳方法是在更改活動之前從應用程式所有者那裡重新驗證CSW/Tetration資料。此外，在實作之後，請確認記錄中是否有任何失敗命中計數。

增值

1. 所有申請都按照中央銀行準則進行了分割和限制。

2. 遷移到以應用為中心的部署後，應用間通訊的可視性。

3. 實現了應用的細分。

4. 單一應用程式流程檢視表。在一個應用配置檔案中，EPG根據流量對映，如應用配置檔案AP_Banking，以便具有三個EPG（EPG_Banking_WEB、EPG_Banking_APP和

EPG_Banking_DB），而不管它們的IP子網如何。

4. 單一的應用流檢視使故障排除更容易。

5. 基礎設施更安全。

6.實施和未來擴展的結構化方法。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。