将ACI部署为以应用为中心

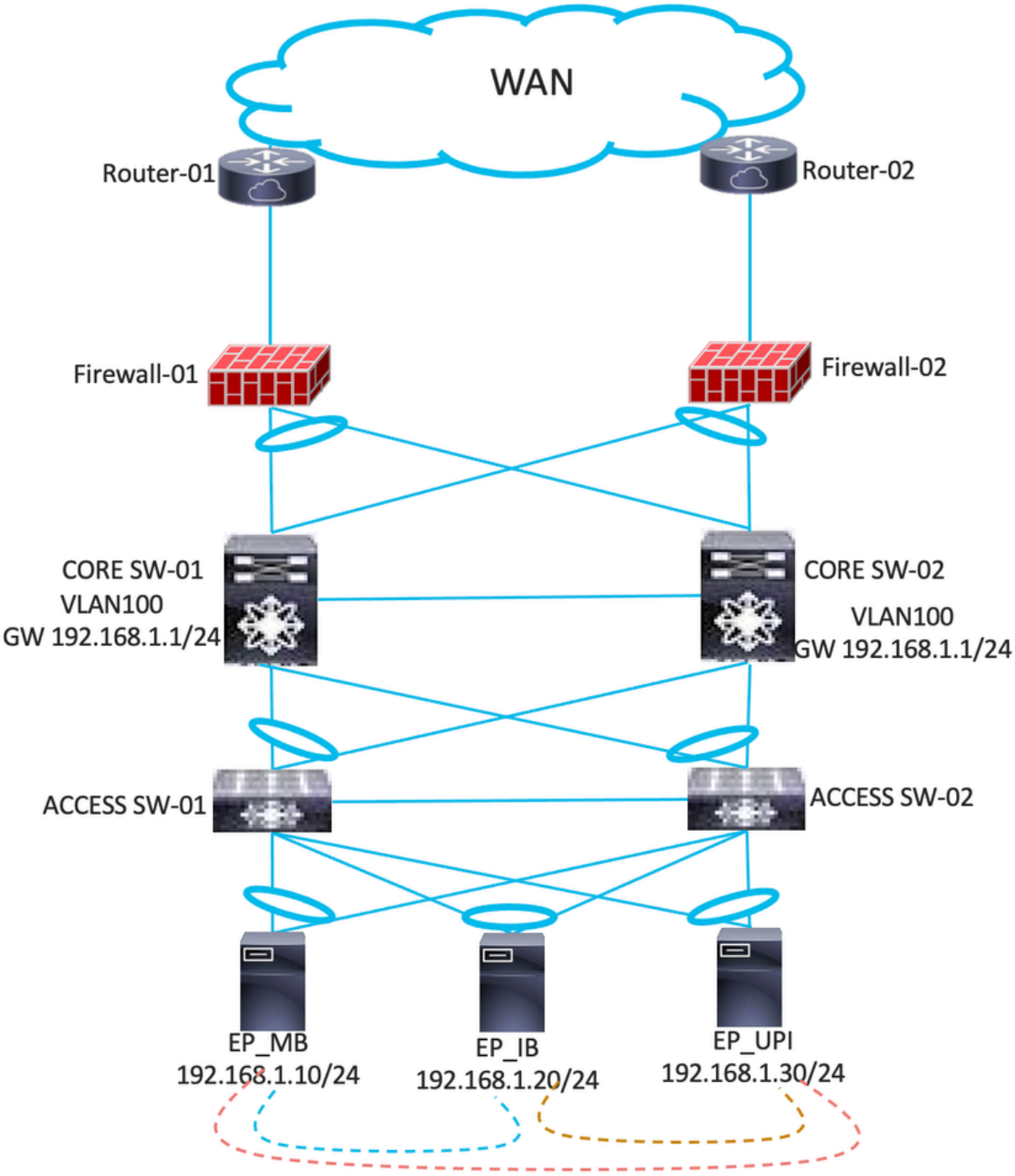
目录

简介

本文档介绍利用思科ACI SDN解决方案在应用内部/应用之间实现微分段和安全的方法。

使用传统网络的限制

- 在传统网络中，不可能对VLAN/子网进行分段。
- 应用网关位于核心交换机上。如果两个应用程序需要通信，则核心交换机上需要复杂的访问控制列表(ACL)。
- 交换机之间的生成树环路会中断数据中心流量并导致流量丢弃。
- 同一个IP子网包含多个应用，这不能提供它们之间的安全性。传统网络无法管理这些通信。
- 考虑使用图中所示的示例。您有三个应用程序EP_MB、EP_IB和EP_UPI，它们属于同一个VLAN和IP子网。对于任何L2流量，流量始终泛洪到所有应用，即使这些应用之间不需要通信。在此方案中，不可能存在两个应用程序之间的限制。



先决条件

要求

Cisco 建议您了解以下主题：

- 必须在环境中部署思科安全工作负载(CSW)/Tetration（安全工作负载），以便收集应用之间的流量数据。
- 必须在服务器上部署代理才能收集数据。因此，这只有在棕地部署的情况下才可能实现。
- 必须在服务器上部署至少3-4周的代理，才能收集数据。

- 如果任何应用程序依赖关系映射(ADM)工具不可用，则必须提供相关数据。
- 必须使用以应用为中心的基础设施(ACI)交换矩阵配置服务器网关。

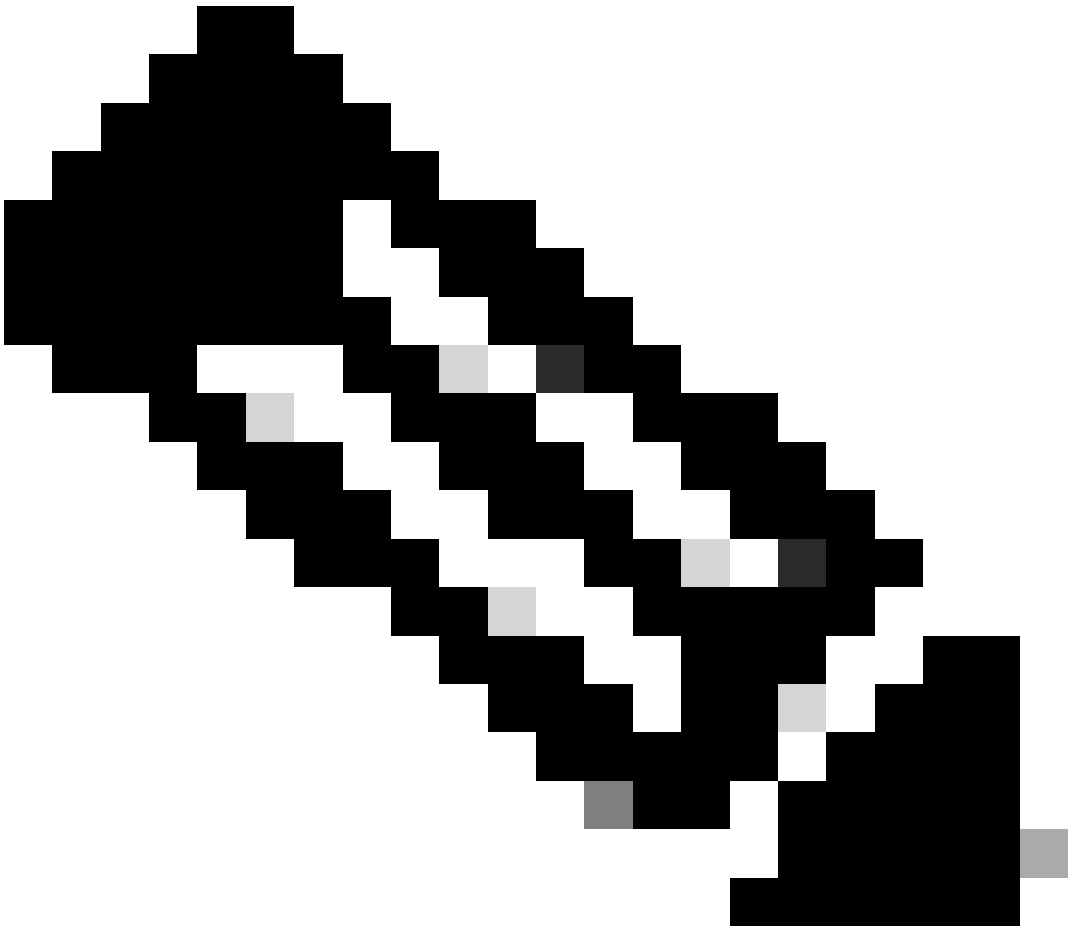
使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

解决方案概述

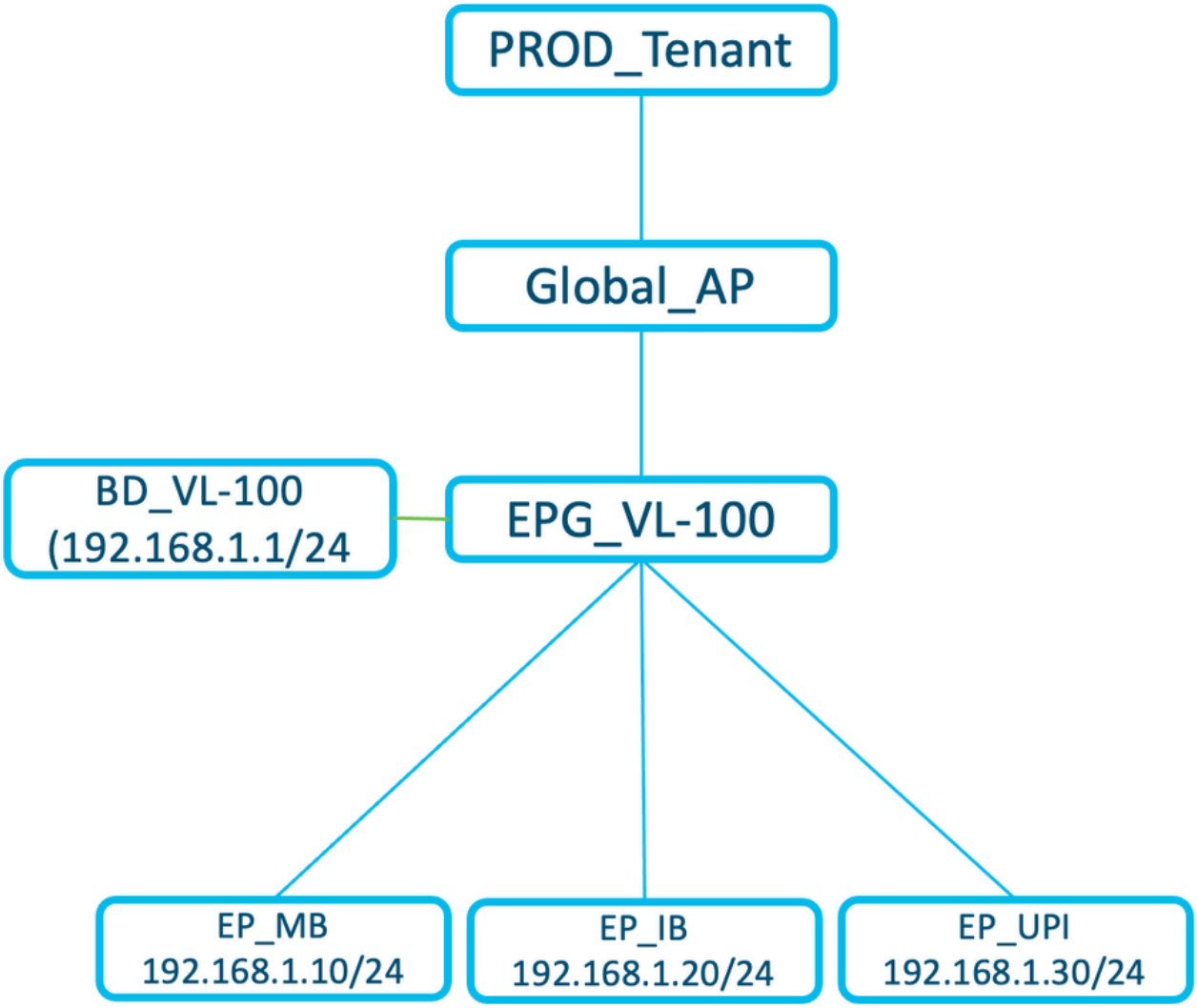
为了实现微分段，您必须首先将网络从传统基础设施迁移到思科SDN解决方案，然后从以应用为中心的角度重新设计网络。本节介绍两个设计阶段，以便根据通过ADM工具捕获的应用程序流实现所需的分段。首先，思科ACI解决方案以网络中心模式（与现有设计相同）部署，然后转向以应用为中心的模式。



注意：您也可以将此部署模式结合使用，以便将服务从传统网络直接迁移到以应用为中心的模式。

以网络为中心的设计

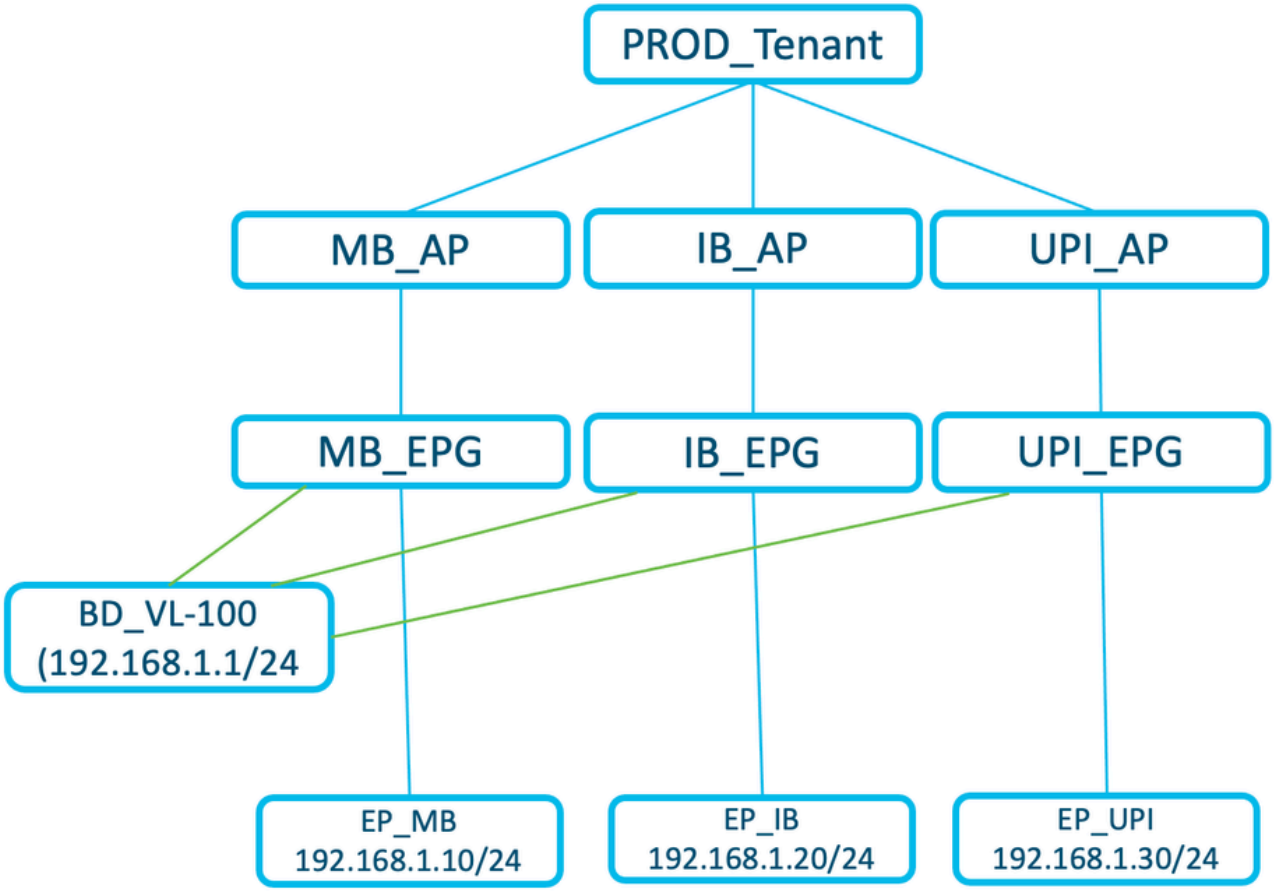
在图中所示的示例中，EPG_VL-100包含三个应用：EP_MB、EP_IB和EP_UPI，并且共享同一个IP子网并使用VLAN 100。



- 从传统网络向ACI的原样迁移。
- 一个终端组(EPG)可以包含多个应用。
- 此部署类型中的同一EPG内没有应用分段。
- 1 BD = 1 EPG = 1 VLAN

以应用为中心的设计

图中所示的示例是三个应用（EP_MB、EP_IB和EP_UPI）的独立EPG，这些应用共享同一个IP子网并使用映射到每个EPG的不同VLAN。

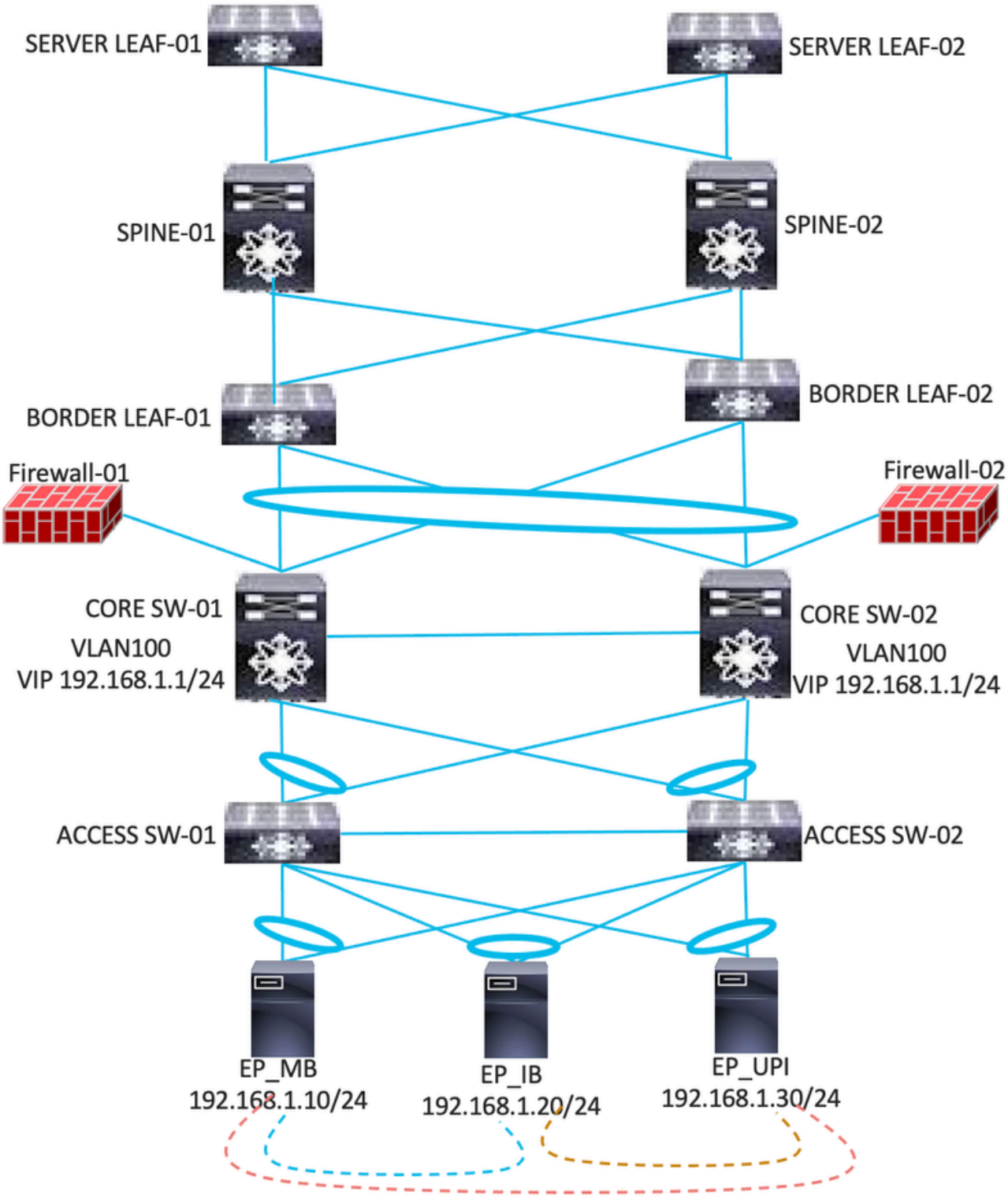


- 在以应用为中心的部署类型中，根据应用配置不同的EPG。
- 这些应用程序继续使用同一个IP子网及其网关。
- 分段应用EPG以使用新的VLAN。
- 1个BD将配置为IP子网并映射到多个应用EPG。
- 1 BD = N EPG = N VLAN
- 现在，两个EPG（应用）可以通过合同相互通信。

迁移方法

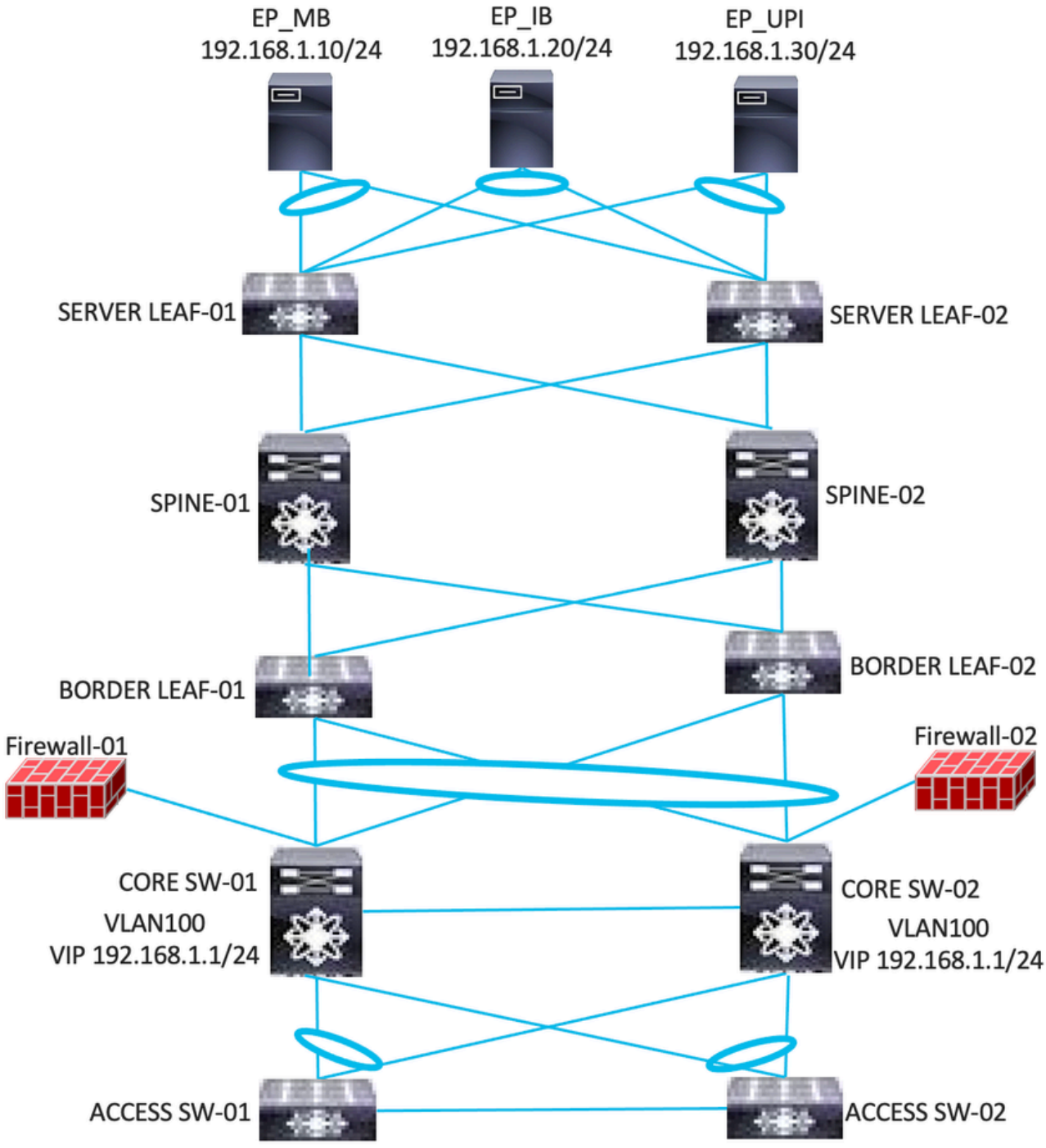
在将ACI部署为以应用为中心之前，可以将ACI部署为以网络为中心，并进一步对应用进行分段。

以网络为中心的迁移方法：第1阶段



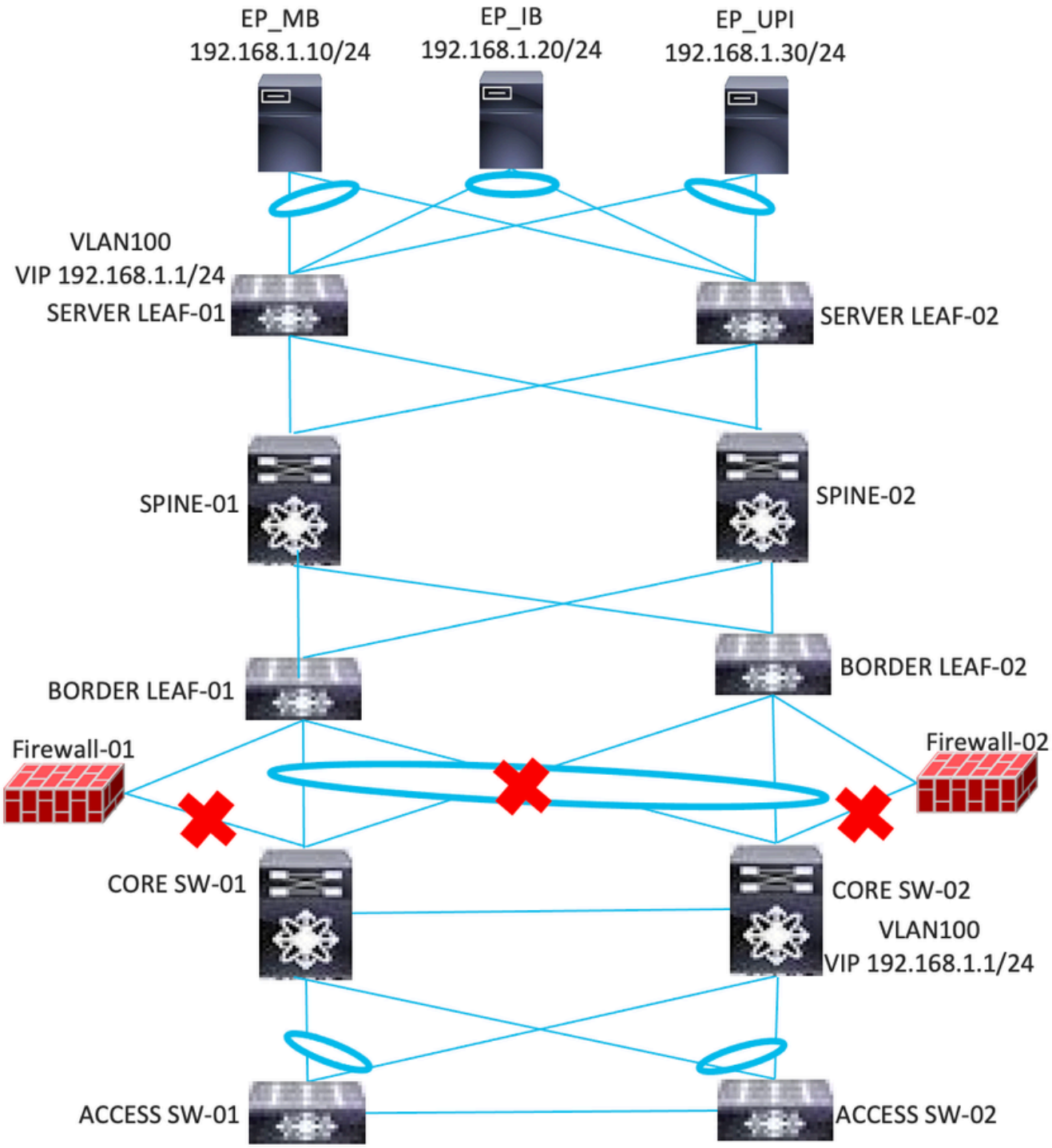
- 边界枝叶交换机和核心交换机之间必须建立第2层临时链路。
- 根据传统网络中配置的现有VLAN在ACI上配置第2层网桥域和终端组。
- 在边界枝叶交换机和核心交换机之间的第2层临时链路上配置所有这些VLAN。
- ACI必须了解核心交换机上的所有终端。
- 网关保留在核心交换机上。
- 防火墙连接仍保留在核心交换机上。

以网络为中心的迁移方法：第2阶段



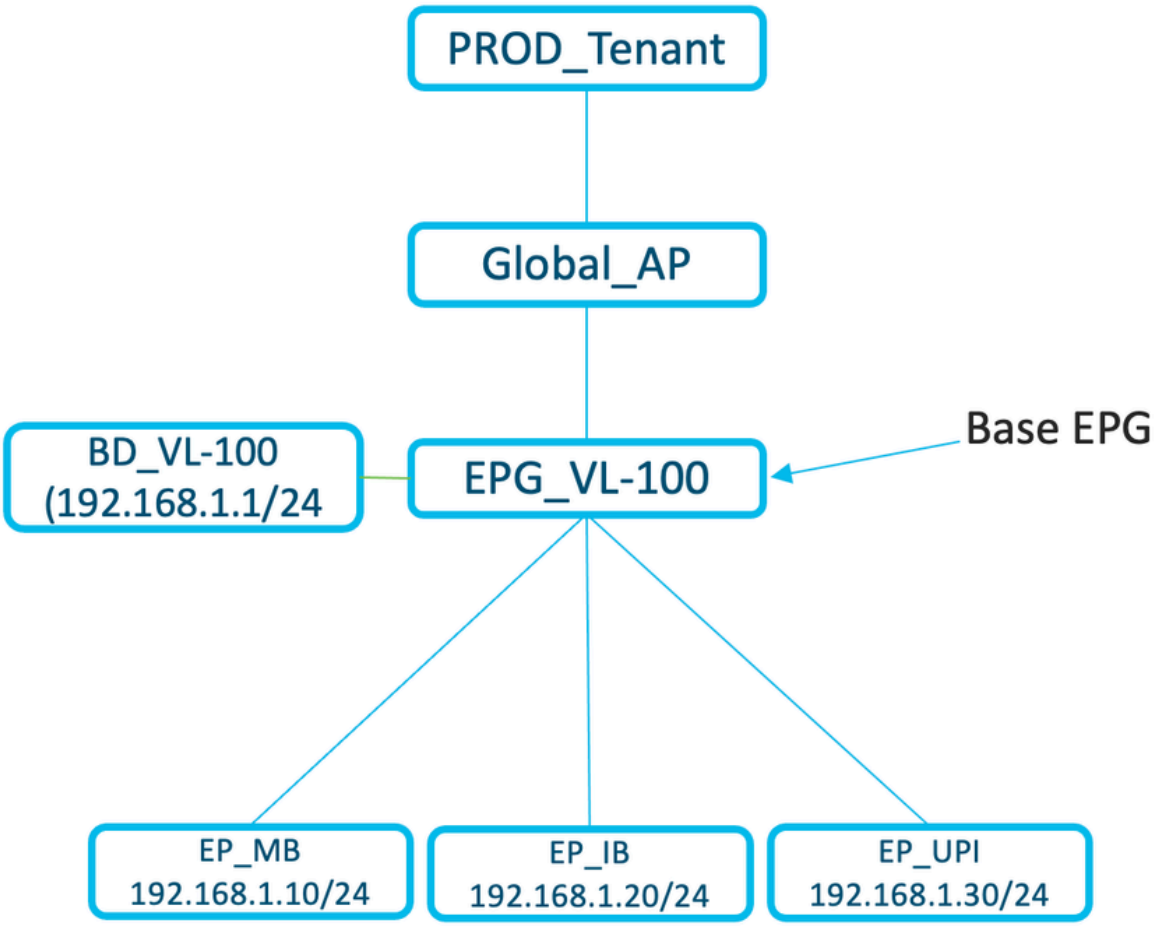
- 将工作负载从接入交换机转移到服务器枝叶。
- 网关保留在核心交换机上。
- 验证是否可从服务器访问网关。
- 验证服务器/应用程序是否可访问。

以网络为中心的迁移方法：第3阶段

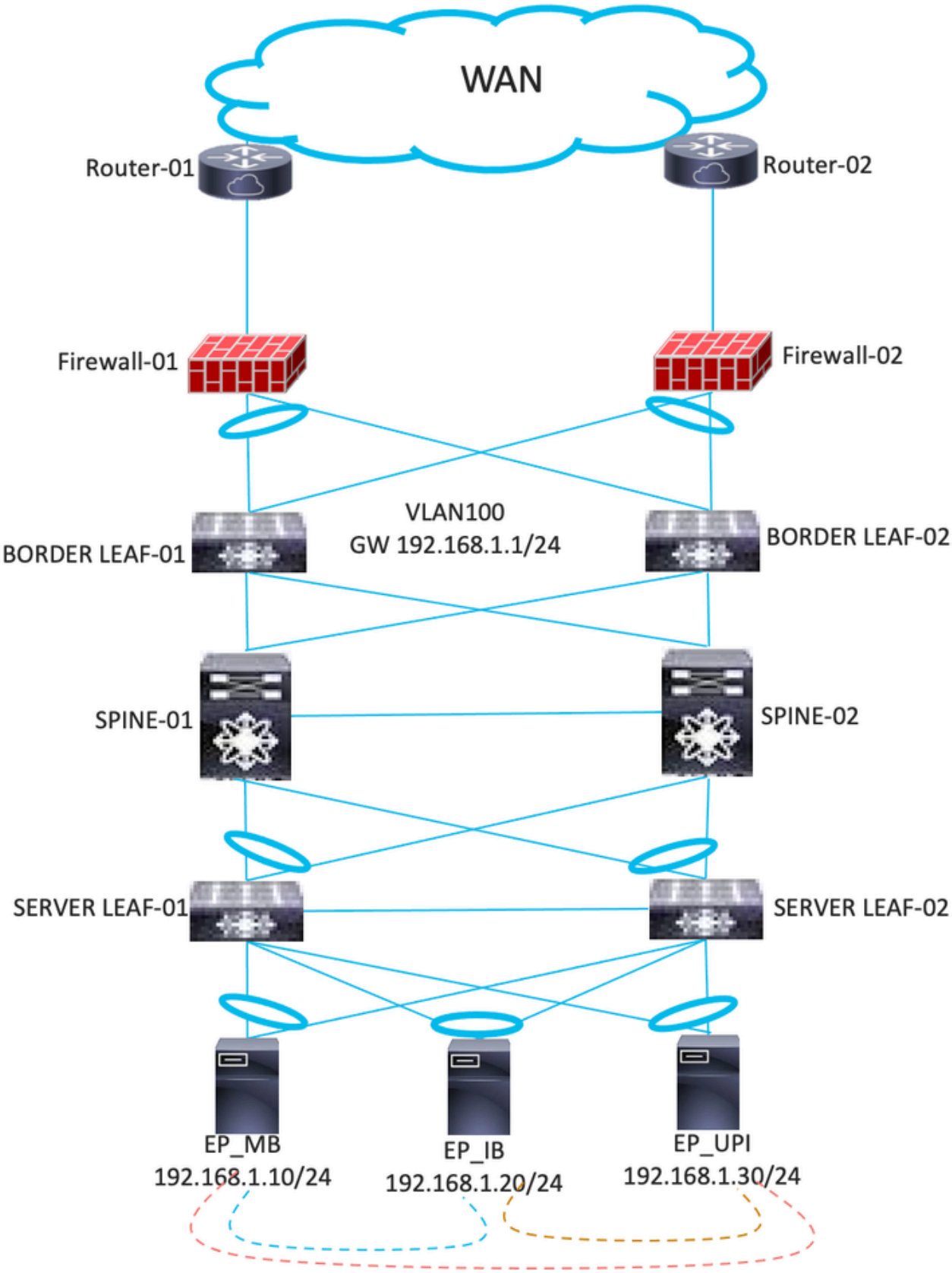


- 关闭核心交换机上的网关并在ACI上配置。
- 将防火墙链路从核心交换机转移到ACI枝叶。
- 配置朝向防火墙/路由器的L3out。
- 在防火墙/路由器和ACI枝叶交换机中添加路由。
- 关闭边界枝叶交换机和核心交换机之间的链路。
- 验证服务器/应用程序是否可访问。

以网络为中心的迁移方法后ACI的逻辑表示。



以应用为中心的迁移方法：第1阶段



- CSW/Tetration数据的收集和分析。
- 根据CSW/Tetration数据（网络、应用和数据库）新建EPG配置。
- 例如，对于MB应用，将创建三个EPG，例如EPG_MB_WEB、EPG_MB_APP和EPG_MB_DB。这些EPG必须在一个应用配置文件AP_MB下配置。

- 对于Virtual Machine Manager (VMM)集成，需要使用vDS配置将新EPG中的服务器映射到新VLAN。
- 将虚拟机(VM)映射到通过VMM集成推送的新vDS。
- 对于裸机，服务器团队必须更改服务器上的VLAN ID。
- 这些部署的IP编址相同。
- 根据CSW/Tetration数据在EPG之间配置合同。

CSW/Tetration数据分析

基于CSW/Tetration数据的分析示例：

src_ip	consumer_scope	dst_ip	provider_scope	protocol	端口
192.168.34.248	默认值：内部：总部	192.168.20.81	PRODAPP	TCP	443
192.168.78.45	默认值：内部：总部	192.168.20.81	PRODAPP	TCP	443
192.168.78.16	默认值：内部：总部	192.168.20.81	PRODAPP	TCP	443
192.168.78.25	默认值：内部：总部	192.168.20.81	PRODAPP	TCP	443
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.81	PRODAPP	UDP	137
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.81	PRODAPP	TCP	445
192.168.32.173	默认：内部：数据中心：DC：应用：生产：DMZ	192.168.20.81	PRODAPP	TCP	7777
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	135
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	UDP	137

192.168.44.48	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	UDP	137
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	443
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	445
192.168.44.48	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	445
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	5985
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	49154
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	49169
192.168.44.29	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	4750
192.168.44.30	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.81	PRODAPP	TCP	4750
192.168.44.21	默认值：内部：数据中心：DC：应用：Prod：AAA	192.168.20.81	PRODAPP	ICMP	0

192.168.103.80	默认值：内部：数据中心：DC：应用：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.71	默认值：内部：数据中心：DC：应用：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.20	默认值：内部：数据中心：DC：应用：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.21	默认值：内部：数据中心：DC：应用：Prod：DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.44.68	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.85	PRODDB	UDP	137
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.85	PRODDB	UDP	137
192.168.44.68	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.85	PRODDB	TCP	445
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：发现	192.168.20.85	PRODDB	TCP	445
172.16.32.173	默认值：内部：数据中心：DC：应用程序：Prod：MZ	192.168.20.85	PRODDB	TCP	1522
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	135

192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	UDP	137
192.168.44.48	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	UDP	137
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	UDP	161
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	445
192.168.44.48	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	445
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	5985
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	49154
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	60801
192.168.44.30	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	4750
192.168.44.29	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	TCP	4750

192.168.44.21	默认值：内部：数据中心：DC：应用程序：生产：监控	192.168.20.85	PRODDB	ICMP	0

来自CSW/Tetration的EPG建议示例：

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

根据详细信息，必须分析合同配置的数据。已分析数据的示例：

src_ip	consumer_scope	consumer_EPG	dst_IP	provider_EPG	protocol	端口
192.168.44.69	默认值：内部：数据中心：DC：应用程序：Prod：发现	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	UDP	137
192.168.44.69	默认值：内部：数据中心：DC：应用程序：Prod：发现	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	135
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	UDP	137
192.168.44.48	默认值：内部：数据中心：DC：应用程序	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	443

	：生产：监控					
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	445
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	5985
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	49154
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	49169
192.168.44.48	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP	4750
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	ICMP	0
192.168.103.21	默认值：内部 ：数据中心 ：DC：应用 ：Prod：DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TCP	7777
192.168.44.68	默认值：内部 ：数据中心 ：DC：应用程序 ：Prod：发现	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	UDP	137

192.168.44.68	默认值：内部：数据中心：DC：应用程序：Prod：发现	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	135
192.168.44.69	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UDP	161
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.48	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	5985
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	49154
192.168.44.47	默认值：内部：数据中心：DC：应用程序：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCP	60801
192.168.44.48	默认值：内部	EPG_MONITORING	192.168.20.85	EPG-PROD-	TCP	4750

	：数据中心 ：DC：应用程序 ：生产：监控			DB		
192.168.44.47	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：监控	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	ICMP	0
192.168.48.45	默认值：内部 ：数据中心 ：DC：应用程序 ：生产：备份	EPG_VL_71	192.168.20.85	EPG-PROD-DB	TCP	5555

根据IP地址，提及消费者和提供商EPG。必须从此数据中排除重复的条目和北-南流量（例如Internet、DC间、区域间流量等）。有些EPG使用VLAN命名，例如EPG_VL_157、EPG_VL_71等。这意味着在以应用为中心的迁移过程中，这些服务器不会移至目标EPG。因此，要使用EPG的当前映射配置它们之间的合同。一旦将这些服务器迁移到目标EPG，作为清理过程的一部分，必须删除这些现有合同，并且必须将相应的合同添加到目标EPG中。

合同

EPG之间的通信需要合同。 本节将介绍合同配置过程中的实施流程。

1. 最初，VzAny合同必须应用于虚拟路由和转发(VRF)级别。

2. 根据CSW/Tetration数据，必须创建特定的EPG合同。

3. 将Deny_All规则配置为低优先级，以便VzAny合同不允许未指定的流量通信。对于尚未作为以应用为中心的应用进行迁移的应用，通信通过VzAny合同进行。

4. 完成所有迁移后，从VRF中删除VzAny合同。

分析CSW/Tetration数据并将其转换为适当的ACI对象是非常关键的一步。因此，在初步分析之后，有必要与有关方面讨论我们的意见，并再次得到确认。此外，在实施过程中，必须仔细考虑以确保所有流量都按预期得到允许。对于故障排除，您可以在合同中启用日志记录，也可以使用GUI界面或CLI跟踪特定端口上的任何丢包。

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：192.16.11，DIP：192.16
.22.11，端口：0，端口：0，源接口：隧道7，端口：1，PktLen：98
[2019年10月1日星期二10:34:36 377731 usecs]：CName：Prod1：VRF1(VXLAN：
2654209)，VlanType：未知，Vlan-

Id：0，SMac：0x000c0c0c0c0c，DMac：0x000c0c0c0c0c，SIP：192.16.11，DIP：192.16.22.11，端口：0，端口：0，源接口：隧道7，端口：1，PktLen：98

contract_parser

一种设备上Python脚本，生成从ID执行名称查找时关联分区规则、过滤器和命中统计数据的输出。此脚本非常有用，因为它采用多步骤流程，并将其转换为可过滤到特定EPG/VRF或其他合同相关值的单个命令。

leaf# contract_parser.py
密钥:
[prio：RuleId] [vrf：{str}]操作协议src-epg [src-l4] dst-epg [dst-l4] [flags][合同：{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] permit any epg：any tn-Prod1/bd-Services(32789) [contract：implicit] [hit=0]

也可以使用路径Tenant > Tenant_Name > Operational > Flows/Packets在GUI中显示数据包丢弃。

考虑事项

在应用EPG之间合同时的建议：

1. 从策略映射方面来说，ACI不能被视为防火墙，否则可能导致三态内容可寻址存储器(TCAM)使用率较高。

2. 使用一系列过滤器，而不使用大量的单个过滤器。

3. 任何合同使用的过滤器范围不得超过四个。可消耗高溢出三态内容可寻址存储器(OTCAM)。

4. 如果任何EPG需要大量端口，请尝试使用“permit any”合同。

5. 作为解决方案的一部分，如果您预计会部署大量合同，请考虑相应地修改转发规模配置文件(FSP)。

6. 在部署大量合同之前，请使用以下公式计算TCAM：提供EPG的数量*消费者EPG的数量*规则数量。

7. 可以使用以下路径在ACI UI上检查现有TCAM大小：操作>容量控制面板>枝叶容量或

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

以应用为中心的部署和解决方案面临的一些挑战

1. 大量的合同可能导致枝叶交换机的TCAM使用率较高。

因此，当完成大量配置部署时，主动跟踪TCAM利用率并预估TCAM价值增加非常重要。最好使用maker检查器进程，以确保推送的配置正确。此外，建议使用适当的计划维护时段执行更改。

2. 一次推送一次合同即可执行批量配置（超过50k TCAM）可能会导致策略管理器内存崩溃。

建议以较小的块推送配置，尤其是当配置较大时。这为合同配置提供了一种系统化和无风险的方法。此外，每次推送配置时，测量TCAM值的增量。

3. 如果应用在CSW/Tetration部署时间间隔（3-4周）内无法通信，则不会捕获流量。

为了避免这种情况，最佳方法是在变更活动之前从应用所有者处重新验证CSW/Tetration数据。此外，在实施后，请验证日志中是否有任何故障命中计数。

增值

1. 所有申请都根据中央银行准则进行了划分和限制。

2. 迁移到以应用为中心的部署后，应用间通信的可视性。

3. 实现了应用的微分段。

4. 应用流的一个视图。在一个应用配置文件中，EPG根据流量映射，例如应用配置文件AP_Banking，以便具有三个EPG（EPG_Banking_WEB、EPG_Banking_APP和EPG_Banking_DB），而不管它们的IP子网如何。

4. 应用程序流的一个视图使故障排除更加容易。

5. 基础设施更安全。

6.实施和未来扩展的结构化方法。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。