アプリケーションセントリックとしてのACIの導入

内容

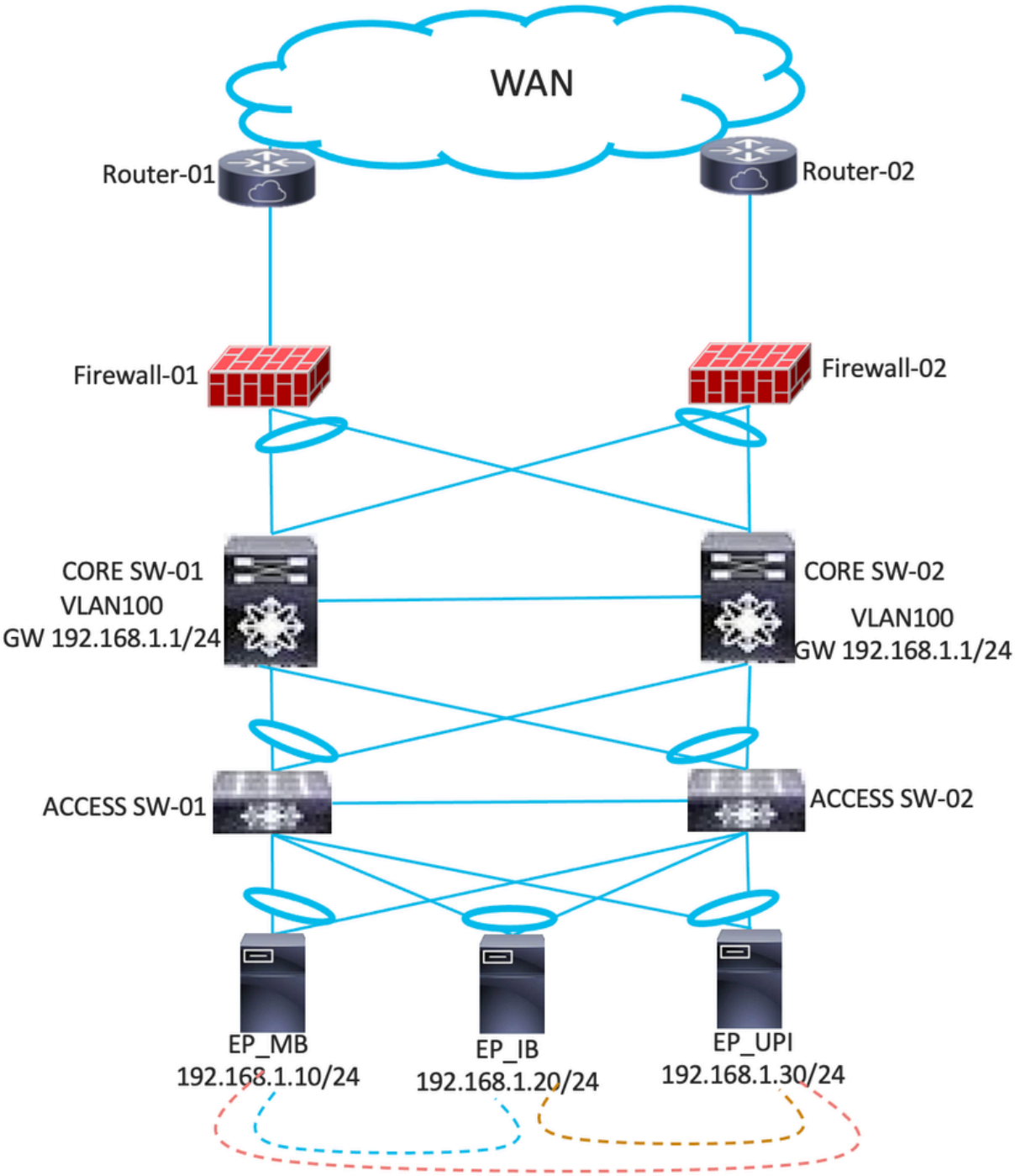
はじめに

このドキュメントでは、Cisco ACI SDNソリューションを活用するアプリケーション内またはアプリケーション間でマイクロセグメンテーションとセキュリティを実現するためのアプローチについて説明します。

従来のネットワークを使用した制約

- 従来のネットワークでは、VLAN/サブネット内でのセグメント化は不可能です。
- アプリケーションゲートウェイはコアスイッチ上にあります。2つのアプリケーションが通信する場合は、コアスイッチに複雑なアクセスコントロールリスト(ACL)が必要です。
- スイッチ間でスパニングツリーループが発生すると、データセンターのフローが遮断され、トラフィックがドロップされます。
- 同じIPサブネットに複数のアプリケーションが含まれているため、アプリケーション間のセキュリティは提供されません。従来のネットワークでは、このような通信を管理することはできません。

- 図を使用して示されている例を考えてみます。EP_MB、EP_IB、およびEP_UPIの3つのアプリケーションがあり、これらは同じVLANおよびIPサブネットに属しています。L2トラフィックでは、アプリケーション間の通信が不要な場合でも、トラフィックはすべてのアプリケーションにフラッディングされます。このシナリオでは、2つのアプリケーション間の制限は不可能です。



前提条件

要件

次の項目に関する知識があることが推奨されます。

- アプリケーション間のトラフィックフローデータを収集するには、環境内にCisco Secure Workload(CSW)/Tetration(Secure Workload)を導入する必要があります。
- データを収集するには、エージェントをサーバに展開する必要があります。したがって、これは既存の導入の場合にのみ可能です。
- エージェントは、データ収集のために少なくとも3 ~ 4週間サーバに導入する必要があります。
- Application Dependency Mapping(ADM)ツールが使用できない場合は、関連データを提供する必要があります。
- サーバゲートウェイは、アプリケーションセントリックインフラストラクチャ(ACI)ファブリックを使用して設定する必要があります。

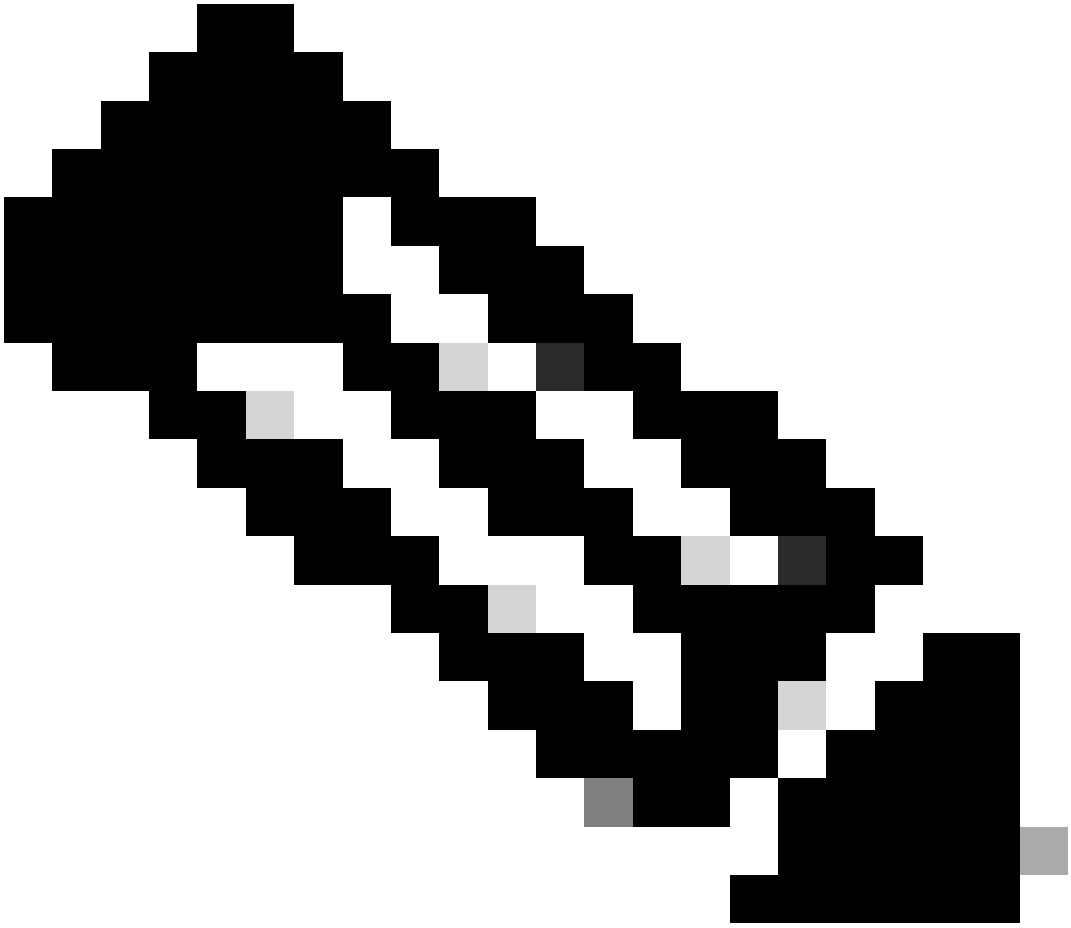
使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ソリューションの概要

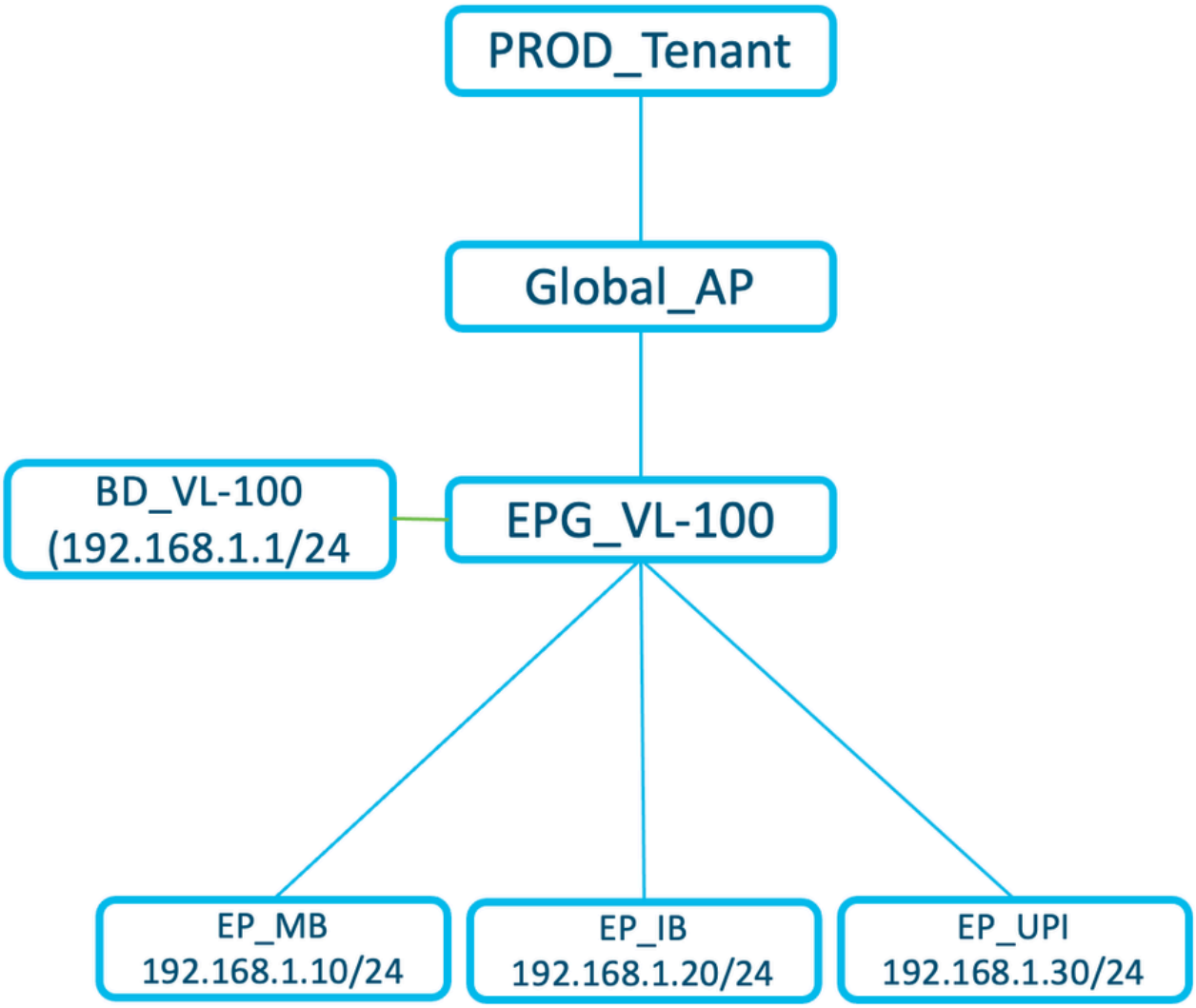
マイクロセグメンテーションを実現するには、まず従来のインフラストラクチャからCisco SDNソリューションにネットワークを移行し、アプリケーションセントリックな視点からネットワークを再設計する必要があります。このセクションでは、ADMツールを介してキャプチャされたアプリケーションフローに基づいて必要なセグメンテーションを実現するための2つの設計フェーズについて説明します。最初に、Cisco ACIソリューションをネットワークセントリックモード（既存の設計の現状）で導入し、次にアプリケーションセントリックモードに移行します。



注：この導入モードを組み合わせて、従来のネットワークからアプリケーションセントリックモードにサービスを直接移行することもできます。

ネットワーク中心の設計

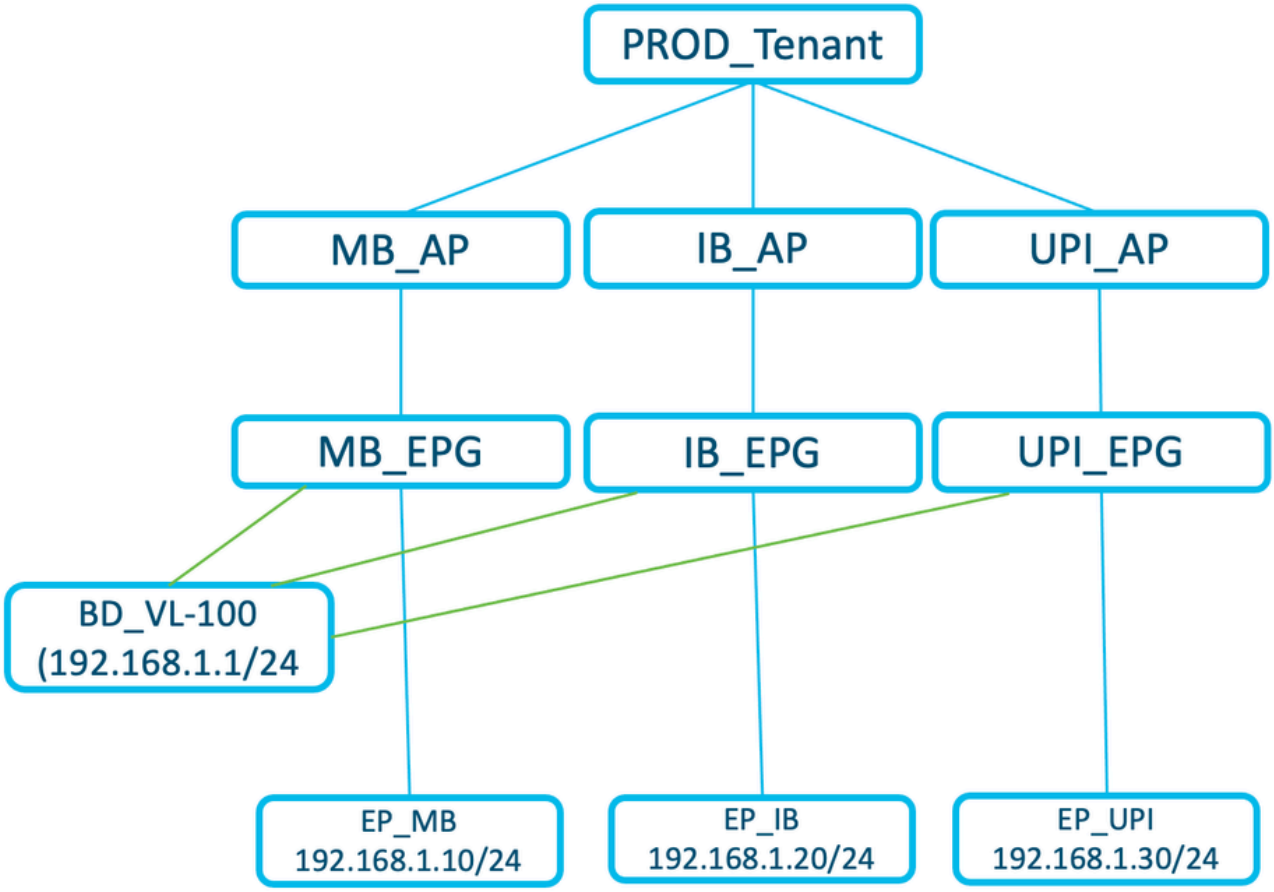
図の例では、EPG_VL-100は3つのアプリケーションEP_MB、EP_IB、およびEP_UPIを含み、同じIPサブネットを共有し、VLAN 100を使用します。



- 従来のネットワークからACIへそのまま移行
- 1つのエンドポイントグループ(EPG)に複数のアプリケーションを含めることができます。
- この導入タイプでは、同じEPG内でのアプリケーションのセグメント化はありません。
- 1 BD = 1 EPG = 1 VLAN

アプリケーション中心の設計

図に示されている例は、同じIPサブネットを共有し、各EPGにマッピングされた異なるVLANを使用する3つのアプリケーションEP_MB、EP_IB、およびEP_UPIの個別のEPGです。

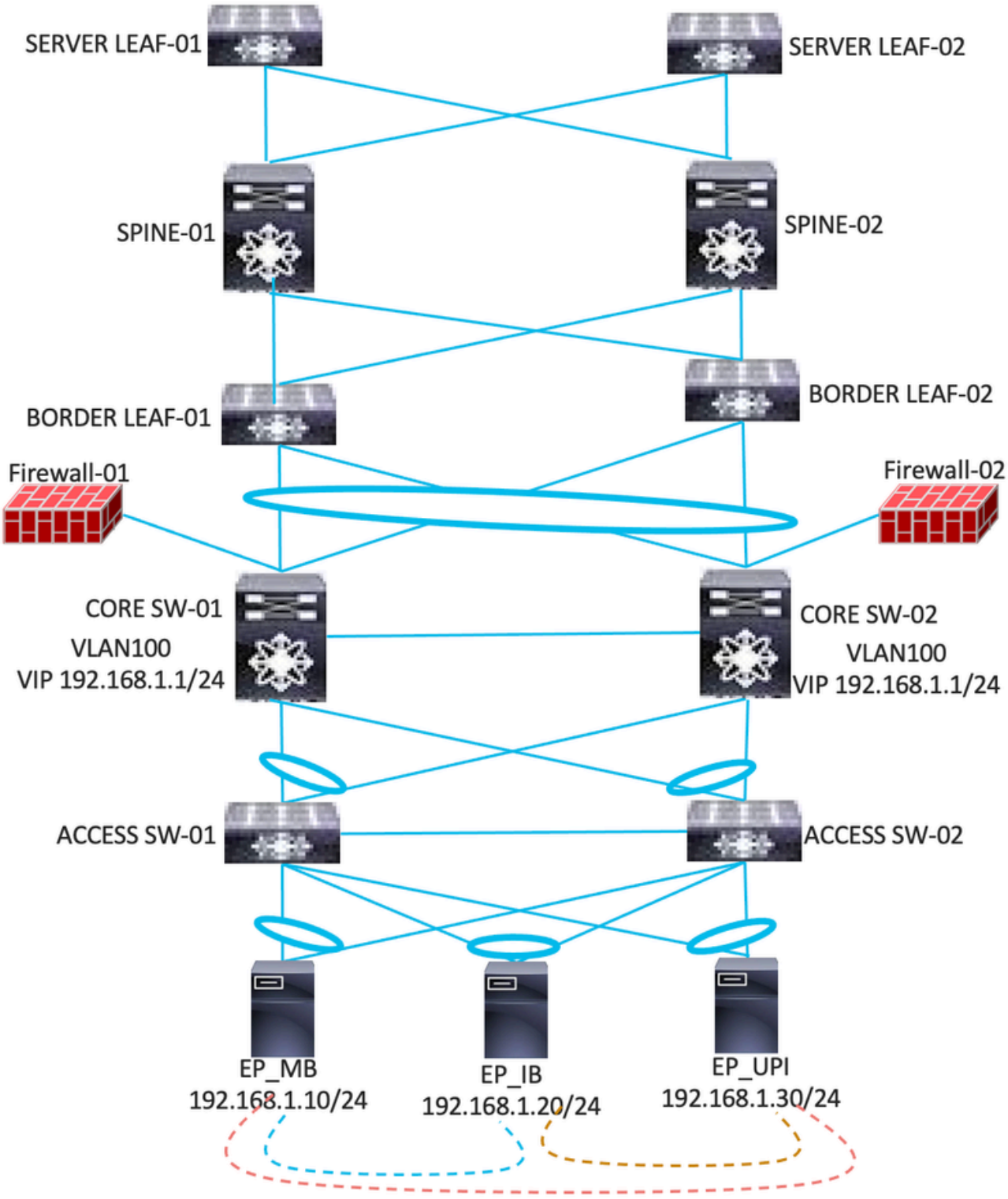


- アプリケーションセントリック導入タイプでは、アプリケーションごとに異なるEPGが設定されます。
- アプリケーションは引き続き同じIPサブネットとそのゲートウェイを使用します。
- 新しいVLANを使用するためにセグメント化されたアプリケーションEPG。
- 1 BD:IPサブネットで設定し、複数のアプリケーションEPGにマッピングします。
- 1 BD = N EPG = N VLAN
- これで、2つのEPG（アプリケーション）が契約を介して相互に通信できるようになります。

移行アプローチ

ACIをアプリケーション中心として導入する前に、ACIをネットワーク中心として導入し、さらにアプリケーションをセグメント化することができます。

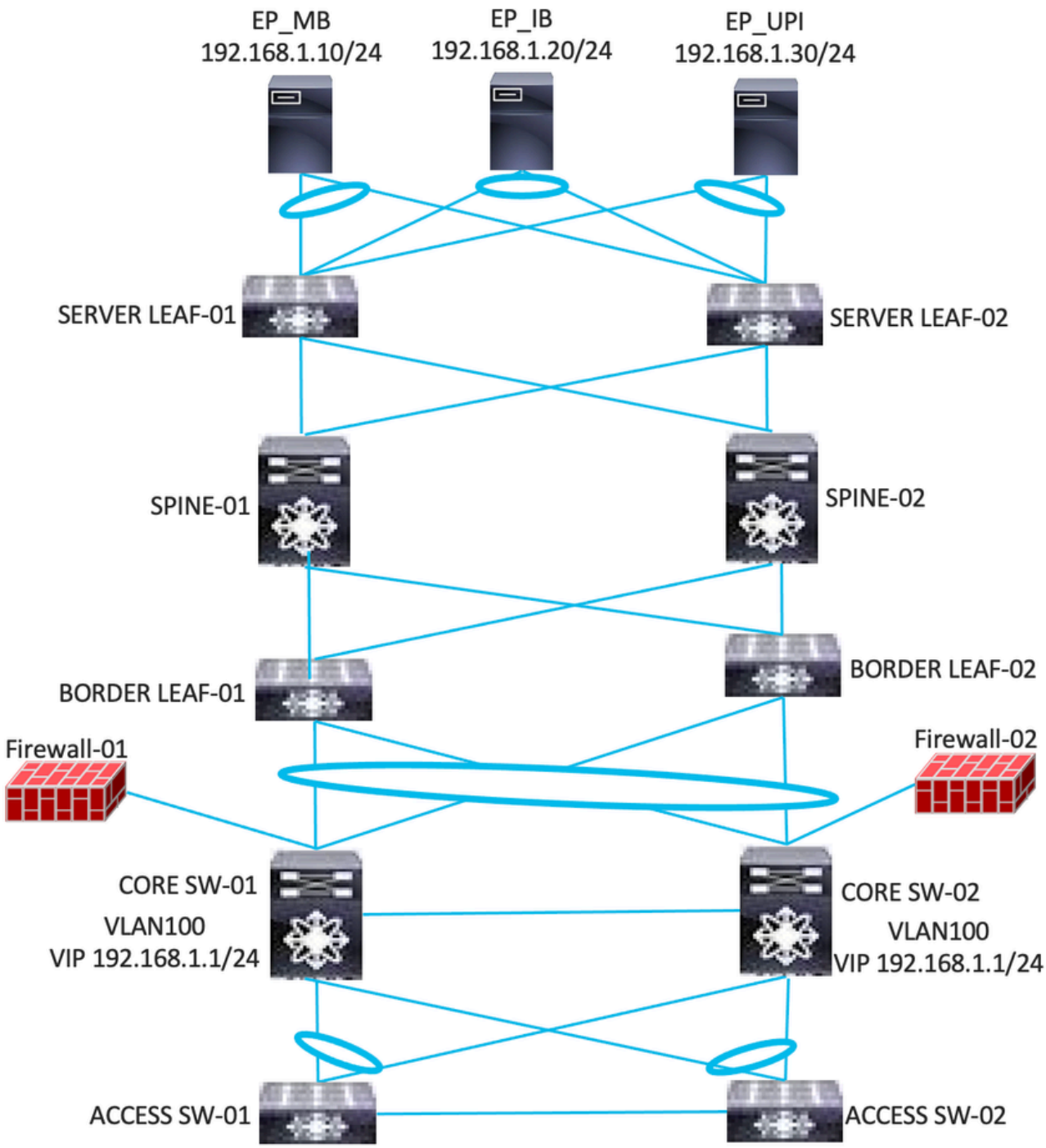
ネットワーク中心の移行アプローチ：フェーズ1



- ボーダーリーフスイッチとコアスイッチ間にレイヤ2暫定リンクを確立する必要があります。
- 従来のネットワークで設定された既存のVLANに従って、ACIでレイヤ2ブリッジドメインとエンドポイントグループを設定します。
- これらのVLANはすべて、ボーダーリーフスイッチとコアスイッチ間のレイヤ2暫定リンクに設定します。
- ACIは、コアスイッチ上に存在するすべてのエンドポイントを学習している必要があります

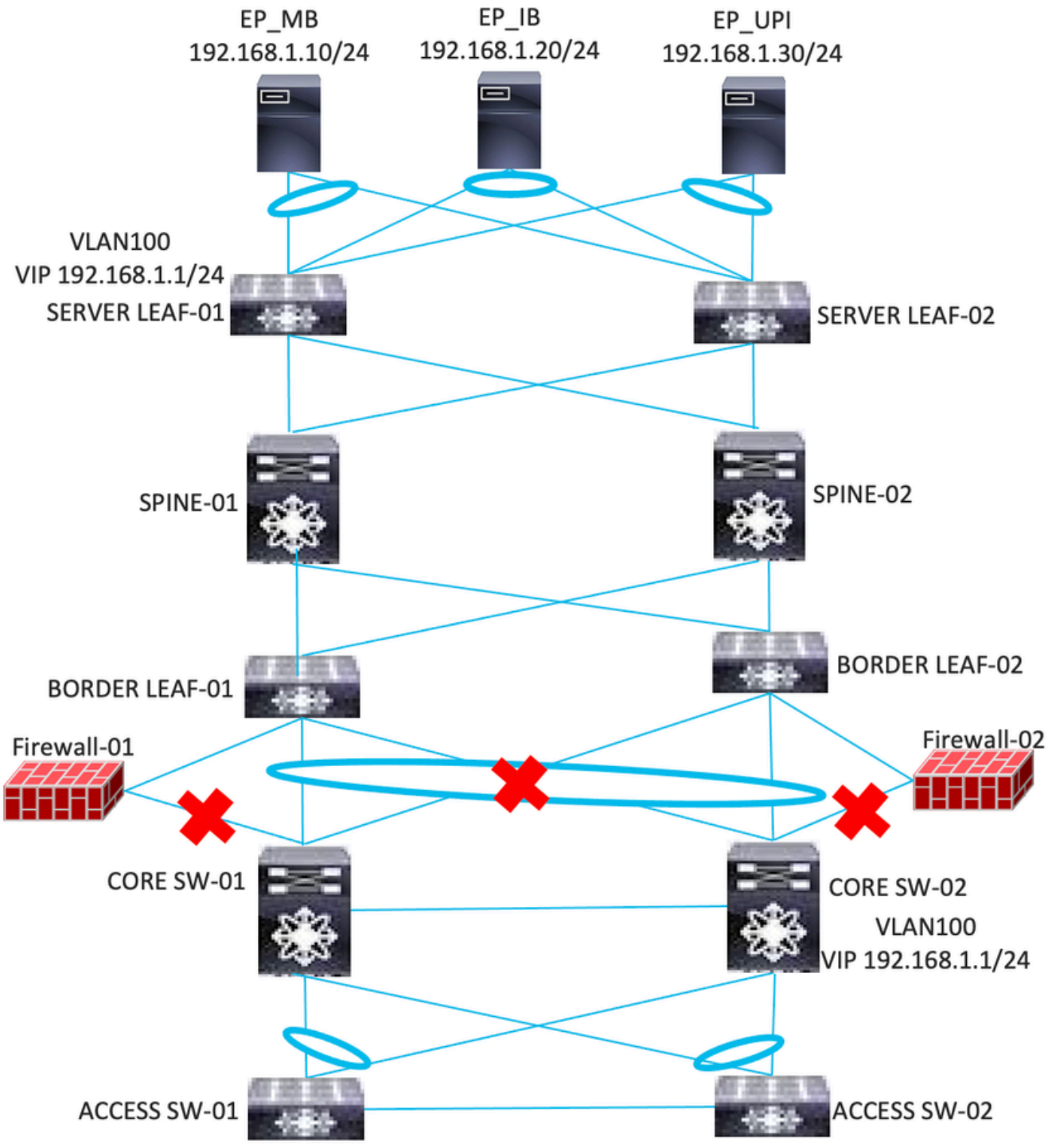
。
- ゲートウェイはコアスイッチ上に残ります。
- ファイアウォール接続はコアスイッチに残ります。

ネットワーク中心型の移行アプローチ：フェーズ2



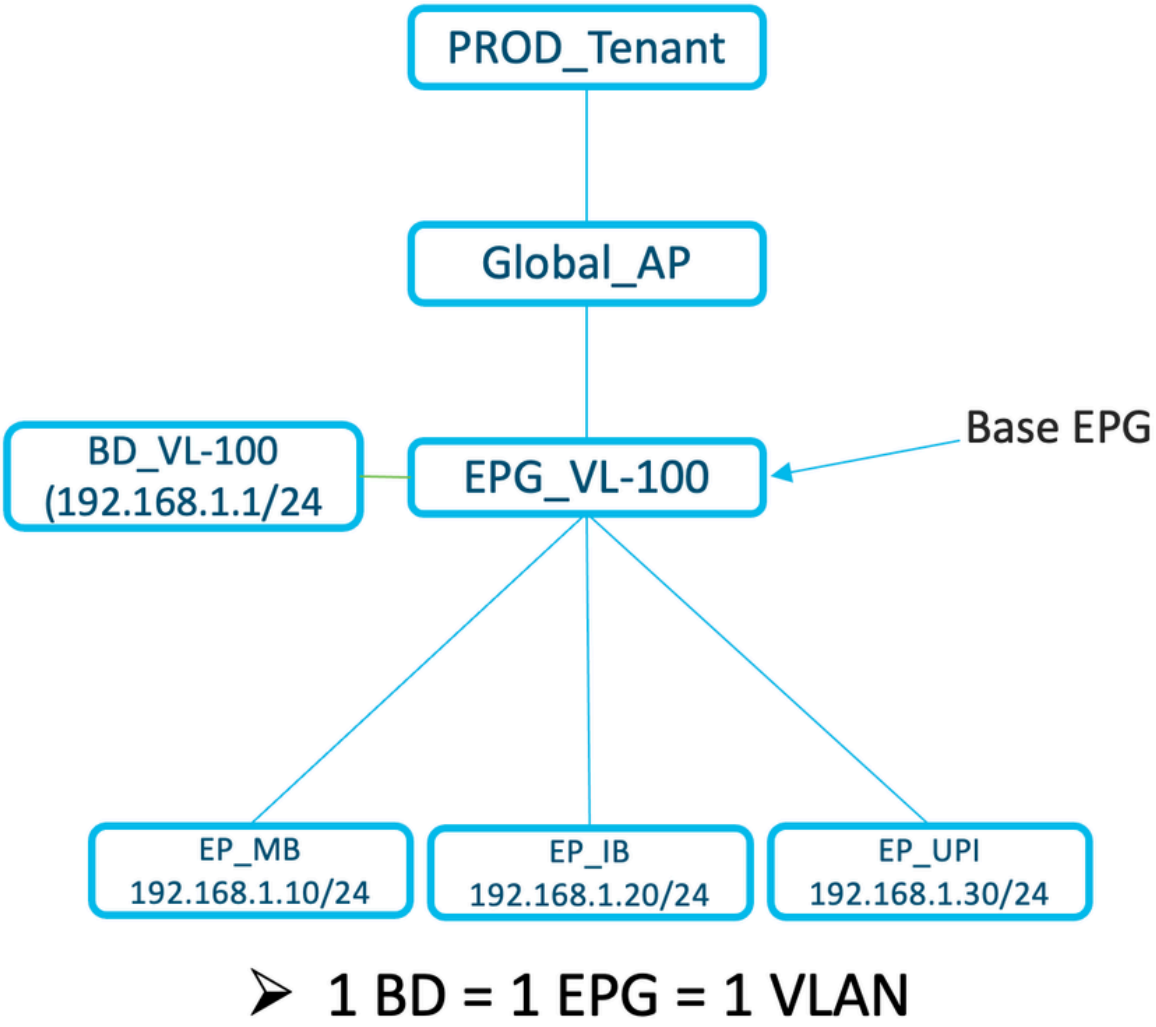
- ワークロードをアクセススイッチからサーバリーフに移行します。
- ゲートウェイはコアスイッチ上に残る。
- ゲートウェイがサーバから到達可能であることを確認します。
- サーバ/アプリケーションが到達可能であることを確認します。

ネットワーク中心型の移行アプローチ：フェーズ3

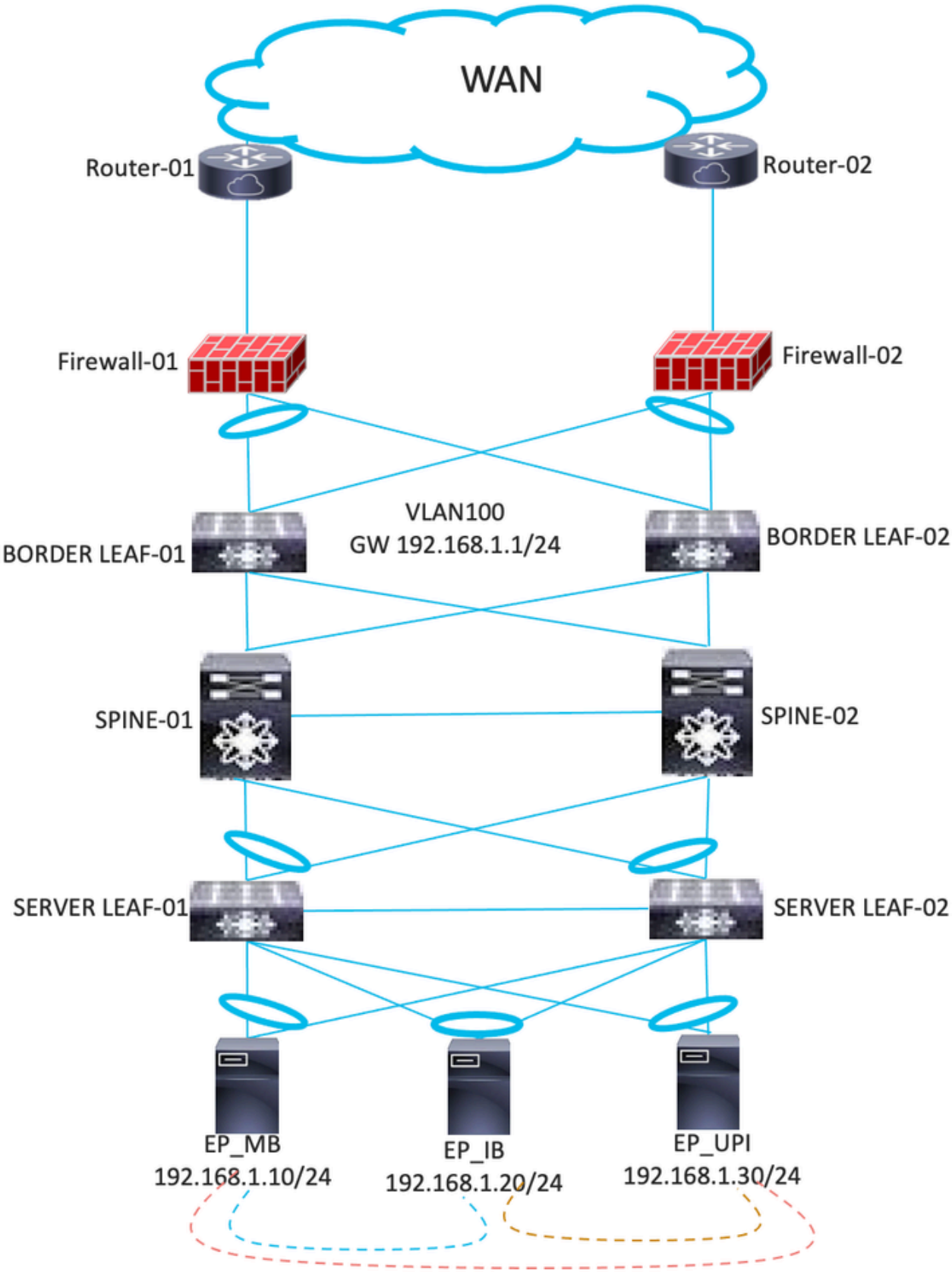


- コアスイッチのゲートウェイをシャットダウンし、ACIで設定する。
- ファイアウォールリンクをコアスイッチからACIリーフに切り替えます。
- ファイアウォール/ルータに向けてL3outを設定します。
- ファイアウォール/ルータとACIリーフにルートを追加します。
- ボーダーリーフスイッチとコアスイッチ間のリンクをシャットダウンします。
- サーバ/アプリケーションが到達可能であることを確認します。

ネットワーク中心型移行後のACIの論理表現。



アプリケーション中心型の移行アプローチ：フェーズ1



- CSW/Tetrationデータの収集と分析。
- CSW/Tetration Data（WEB、APP、およびDB）に従った新しいEPG設定
- たとえば、MBアプリケーションの場合、EPG_MB_WEB、EPG_MB_APPおよびEPG_MB_DBなどの3つのEPGが作成されます。これらのEPGは、1つのアプリケーション

プロファイルAP_MBで設定する必要があります。
- Virtual Machine Manager(VMM)の統合の場合、新しいEPG内のサーバを新しいVLANにマッピングするために、vDS設定が必要です。
- 仮想マシン(VM)を、VMM統合によってプッシュされる新しいvDSにマッピングします。
- ベアメタルの場合、サーバチームはサーバのVLAN IDを変更する必要があります。
- IPアドレッシングは、これらの導入で同じにする必要があります。
- CSW/Tetrationデータに従ったEPG間のコントラクト設定。

CSW/Tetrationデータ分析

CSW/Tetrationデータに基づく分析の例：

src_ip（送信元IP）	コンシューマ_スコープ	宛先IP	プロバイダー_スコープ	protocol	port
192.168.34.248	デフォルト：内部：本社	192.168.20.81	製品	TCP	443
192.168.78.45	デフォルト：内部：本社	192.168.20.81	製品	TCP	443
192.168.78.16	デフォルト：内部：本社	192.168.20.81	製品	TCP	443
192.168.78.25	デフォルト：内部：本社	192.168.20.81	製品	TCP	443
192.168.44.69	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.81	製品	UDP	137

192.168.44.69	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.81	製品	TCP	445
192.168.32.173	デフォルト：内部：データセンター：DC：アプリケーション：製品：DMZ	192.168.20.81	製品	TCP	7777
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	135
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	UDP	137
192.168.44.48	デフォルト：内部：データセンター：DC：ア	192.168.20.81	製品	UDP	137

	プリケーション：製品：モニタリング				
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	443
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	445
192.168.44.48	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	445
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリ	192.168.20.81	製品	TCP	5985

	ング				
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	49154
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	49169
192.168.44.29	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	4750
192.168.44.30	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.81	製品	TCP	4750
192.168.44.21	デフォルト	192.168.20.81	製品	ICMP	0

	：内部：データセンター ：DC：アプリケーション：製品：AAA				
192.168.103.80	デフォルト：内部：データセンター ：DC：アプリケーション：製品：DHCP	192.168.20.81	製品	TCP	7777
192.168.103.71	デフォルト：内部：データセンター ：DC：アプリケーション：製品：DHCP	192.168.20.81	製品	TCP	7777
192.168.103.20	デフォルト：内部：データセンター ：DC：アプリケーション：製品：DHCP	192.168.20.81	製品	TCP	7777
192.168.103.21	デフォルト：内部：データセンター ：DC：アプリケーション：製品：DHCP	192.168.20.81	製品	TCP	7777

192.168.44.68	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.85	製品DB	UDP	137
192.168.44.69	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.85	製品DB	UDP	137
192.168.44.68	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.85	製品DB	TCP	445
192.168.44.69	デフォルト：内部：データセンター：DC：アプリケーション：製品：検出	192.168.20.85	製品DB	TCP	445
172.16.32.173	デフォルト：内部：データセンター：DC：アプリケーション：製品	192.168.20.85	製品DB	TCP	1522

	：MZ				
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	TCP	135
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	UDP	137
192.168.44.48	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	UDP	137
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	UDP	161
192.168.44.47	デフォルト	192.168.20.85	製品DB	TCP	445

	：内部：データセンター ：DC：アプリケーション：製品 ：モニタリング				
192.168.44.48	デフォルト ：内部：データセンター ：DC：アプリケーション：製品 ：モニタリング	192.168.20.85	製品DB	TCP	445
192.168.44.47	デフォルト ：内部：データセンター ：DC：アプリケーション：製品 ：モニタリング	192.168.20.85	製品DB	TCP	5985
192.168.44.47	デフォルト ：内部：データセンター ：DC：アプリケーション：製品 ：モニタリング	192.168.20.85	製品DB	TCP	49154
192.168.44.47	デフォルト ：内部：データセンター	192.168.20.85	製品DB	TCP	60801

	：DC：アプリケーション：製品：モニタリング				
192.168.44.30	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	TCP	4750
192.168.44.29	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	TCP	4750
192.168.44.21	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	192.168.20.85	製品DB	ICMP	0

CSW/TetrationからのEPG推奨例：

EPG	IP
製品	192.168.20.81

RODDB	192.168.20.85

詳細に基づいて、データを分析して契約を構成する必要があります。分析データの例：

src_ip（送信元IP）	コンシューマ_スコープ	コンシューマ_EPG	宛先IP	プロバイダー_EPG	protocol	port
192.168.44.69	デフォルト：内部：データセンター ：DC：アプリケーション：製品：検出	EPG_検出	192.168.20.81	EPG – 製品 – アプリケーション	UDP	137
192.168.44.69	デフォルト：内部：データセンター ：DC：アプリケーション：製品：検出	EPG_検出	192.168.20.81	EPG – 製品 – アプリケーション	TCP	445
192.168.44.47	デフォルト：内部：データセンター ：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	135
192.168.44.47	デフォルト：内部：データセンター ：DC：アプリケーシ	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	UDP	137

	ョン：製品：モニタリング					
192.168.44.48	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	443
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	445
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	5985
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	49154

192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	49169
192.168.44.48	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	TCP	4750
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.81	EPG – 製品 – アプリケーション	ICMP	0
192.168.103.21	デフォルト：内部：データセンター：DC：アプリケーション：製品：DHCP	EPG_VL_157	192.168.20.81	EPG – 製品 – アプリケーション	TCP	7777
192.168.44.68	デフォルト：内部：データセンター	EPG_検出	192.168.20.85	EPG-PROD-DB	UDP	137

	：DC：アプリケーション：製品：検出					
192.168.44.68	デフォルト：内部：データセンター ：DC：アプリケーション：製品：検出	EPG_検出	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.69	デフォルト：内部：データセンター ：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	135
192.168.44.69	デフォルト：内部：データセンター ：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	UDP	137
192.168.44.47	デフォルト：内部：データセンター ：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	UDP	161

192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	445
192.168.44.48	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	5985
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	49154
192.168.44.47	デフォルト：内部：データセンター：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	60801
192.168.44.48	デフォルト：内部：データセンタ	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	TCP	4750

	ー ：DC：アプリケーション：製品：モニタリング					
192.168.44.47	デフォルト：内部：データセンター ：DC：アプリケーション：製品：モニタリング	EPG_モニタリング	192.168.20.85	EPG-PROD-DB	ICMP	0
192.168.48.45	デフォルト：内部：データセンター ：DC：アプリケーション：製品：バックアップ	EPG_VL_71	192.168.20.85	EPG-PROD-DB	TCP	5555

IPアドレスに基づいて、コンシューマEPGとプロバイダーEPGが示されます。重複するエントリとノースサウスのトラフィック（インターネット、DC間、ゾーン間のトラフィックなど）は、このデータから除外する必要があります。EPG_VL_157、EPG_VL_71などのVLANで名前が付けられたEPGがあります。つまり、これらのサーバは、アプリケーション中心の移行の一部としてターゲットEPGに移動されません。したがって、これらの間のコントラクトは、EPGの現在のマッピングを使用して設定されます。これらのサーバがターゲットEPGに移行されたら、クリーンアッププロセスの一部としてこれらの既存のコントラクトを削除し、適切なコントラクトをターゲットEPGに追加する必要があります。

契約

契約は、EPG間の通信に必要です。 このセクションでは、契約の設定プロセスにおける実装のフローを取り上げます。

1. 最初にVzAnyコントラクトをVirtual Routing and Forwarding(VRF)レベルで適用する必要があります。

2. CSW/Tetrationデータに基づいて、特定のEPG契約を作成する必要があります。

3. VzAnyコントラクトで未指定のトラフィック通信が許可されないように、Deny_Allルールに低い優先順位を設定します。アプリケーション中心としてまだ移行されていないアプリケーションについては、VzAny契約を通じて通信が行われます。

4. すべての移行が完了したら、VRFからVzAny契約を削除します。

CSW/Tetrationデータを分析し、適切なACIオブジェクトに変換することは、非常に重要なステップです。したがって、最初の分析の後、私たちの観察を関係者と議論し、再確認を得ることが重要です。また、実装時には、すべてのトラフィックが期待どおりに許可されていることを確認するために、慎重に検討する必要があります。トラブルシューティングのために、契約のロギングを有効にし、GUIインターフェイスまたはCLIを使用して特定のポートでのパケットドロップを追跡することもできます。

leaf# show logging ip access-list internal packet-log deny
[2019年10月1日（火）10:34:37 377572 usecs]:CName:Prod1:VRF1(VXLAN:2654209)、VlanType:Unknown、Vlan-Id:0、SMac:0x000c0c0c0c0c0c、DMac:0x000c0c0c0c、SIP:192.168.21.11、DIP1: 92.168.22.11、SPort: 0、DPort: 0、Src Intf: Tunnel7、Proto: 1、PktLen: 98
[2019年10月1日（火）10:34:36 377731 usecs]:CName:Prod1:VRF1(VXLAN:2654209)、VlanType:Unknown、Vlan-Id:0、SMac:0x000c0c0c0c0c0c、DMac:0x000c0c0c0c、SIP:192.168.21.11、DIP1: 92.168.22.11、SPort: 0、DPort: 0、Src Intf: Tunnel7、Proto: 1、PktLen: 98

contract_parser関数

IDからの名前検索を実行しながら、ゾーン分割ルール、フィルタ、ヒット統計を相互に関連付ける出力を生成するデバイス上のPythonスクリプト。このスクリプトは、マルチステップのプロセスを実行して、特定のEPG/VRFまたは他の契約関連の値にフィルタリングできる単一のコマンドに変換する点で非常に便利です。

leaf# contract_parser.py
ポイント：
[prio:RuleId] [vrf:{str}]アクションプロトコル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] permit any epg:any tn-Prod1/bd-Services(32789) [contract:implicit] [hit=0]

パケットドロップは、GUIでパスTenant > Tenant_Name > Operational > Flows/Packetsを使用し

て表示することもできます。

検討

EPG間の契約を適用する際の推奨事項：

1. ACIは、高いTernary Content Addressable Memory(TCAM)使用率を引き起こす可能性があるポリシーマッピングの観点からはファイアウォールとは見なされません。

2. 多数の個別フィルタの代わりに一連のフィルタを使用します。

(3)いずれの契約も、4つ以上のフィルタ範囲を使用しないこと。オーバーフローが発生すると、Ternary Content Addressable Memory(OTCAM)が大量に消費される可能性があります。

4. いずれかのEPGで多数のポートが必要な場合は、「permit any」コントラクトを使用してください。

5. ソリューションの一部として、多数の契約の展開が予想される場合は、それに応じて転送スケールプロファイル(FSP)を変更することを検討してください。

6. 契約のバルク番号を配置する前に、次の算式を使用してTCAMを計算します。提供EPGの数*コンシューマEPGの数*ルールの数。

7. 既存のTCAMサイズは、ACI UIで、パス「Operations」>「Capacity Dashboard」>「Leaf Capacity」を使用して確認できます。

LEAF-101# vsh_lc

module-1# show platform internal hal health-stats | grepカウント(_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

アプリケーション中心の導入とソリューションの課題

1. 契約数の増加により、リーフスイッチのTCAM使用率が高くなる可能性があります。

したがって、TCAM使用率をアクティブに追跡し、大量の設定を展開する際にTCAM値の増加予測を準備することも重要です。Maker Checkerプロセスを使用して、プッシュする設定が適切であることを確認することをお勧めします。また、適切なスケジュールされたメンテナンスウィンドウで変更を実行することをお勧めします。

2. コントラクトの1回のプッシュで一括設定（50k TCAM以上）を行うと、Policy Managerのメモリクラッシュが発生する可能性があります。

特にコンフィギュレーションのサイズが大きい場合は、コンフィギュレーションをより小さなチャンクにプッシュすることを推奨します。これにより、体系的でリスクのない方法で契約を設定できます。また、設定をプッシュするたびに、TCAM値の増加を測定します。

3. CSW/Tetration導入期間（3 ~ 4週間）中にアプリケーションが通信しない場合、トラフィックフローはキャプチャされません。

このような状況を回避するための最善のアプローチは、変更アクティビティの前にアプリケーション所有者からCSW/Tetrationデータを再確認することです。また、実装後に、ログで障害ヒットカウントを確認します。

値の追加

1. 全ての出願は，中央銀行のガイドラインに従って区分され，かつ，制限されている。

2. アプリケーション中心型の導入に移行した後のアプリケーション間通信の可視化

3. アプリケーションのマイクロセグメンテーションが実現します。

4. アプリケーションフローの1つのビュー1つのアプリケーションプロファイルでは、IPサブネットに関係なく3つのEPG（EPG_Banking_WEB、EPG_Banking_APP、およびEPG_Banking_DB）を持つために、EPGはアプリケーションプロファイルAP_Bankingなどのトラフィックフローに従ってマッピングされます。

4. アプリケーションフローを1つのビューで確認できるため、トラブルシューティングが容易になります。

5. インフラのセキュリティが向上します。

6.実施と将来の拡大のための構造的アプローチ。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。