

Implantação da ACI como centrada em aplicativos

Contents

[Introdução](#)

[Restrições usando a rede tradicional](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Visão geral da solução](#)

[Projeto centrado na rede](#)

[Design centrado em aplicativos](#)

[Abordagens de migração](#)

[Abordagem de migração centrada na rede: Fase 1](#)

[Abordagem de migração centrada na rede: Fase 2](#)

[Abordagem de migração centrada na rede: Fase 3](#)

[Abordagem de migração centrada em aplicativos: Fase 1](#)

[Análise de dados de CSW/Tetration](#)

[Contrato](#)

[contract_parser](#)

[Considerações](#)

[Alguns desafios da implantação e da solução centradas em aplicativos](#)

[Adição de Valor](#)

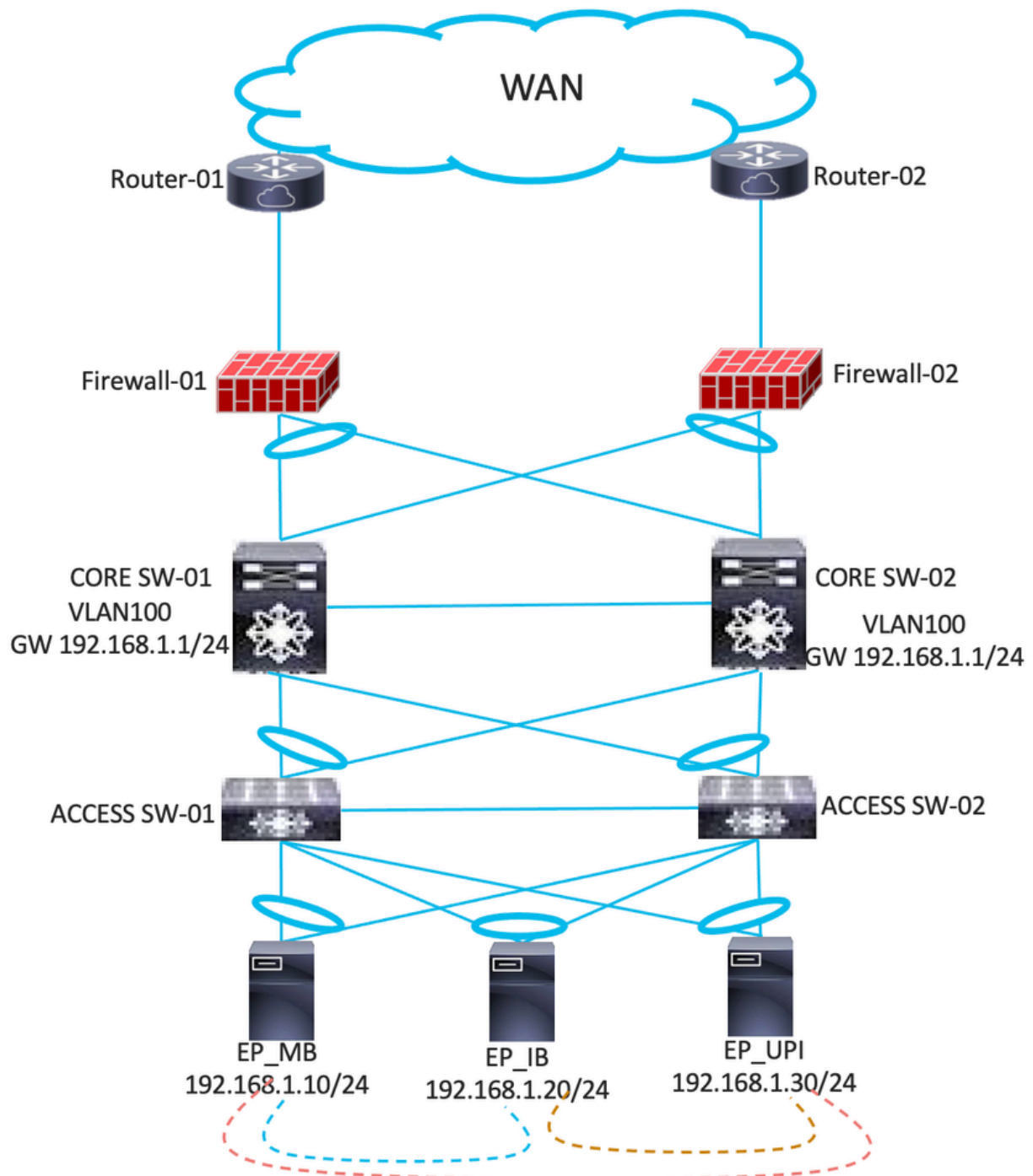
Introdução

Este documento descreve a abordagem para atingir a microssegmentação e a segurança dentro/entre os aplicativos que aproveitam a solução de SDN da Cisco ACI.

Restrições usando a rede tradicional

- Em redes tradicionais, a segmentação dentro de uma VLAN/sub-rede é impossível.
- Os gateways de aplicativos estão nos switches centrais. Se dois aplicativos desejarem se comunicar, serão necessárias Listas de Controle de Acesso (ACLs) complexas no switch central.
- O loop Spanning-Tree entre os switches interrompe o fluxo do data center e resulta em queda de tráfego.
- A mesma sub-rede IP contém vários aplicativos, o que não fornece segurança entre eles. Não é possível gerenciar essas comunicações em redes tradicionais.
- Considere um exemplo que também é descrito usando o diagrama. Você tem três

aplicativos EP_MB, EP_IB e EP_UPI que fazem parte da mesma VLAN e sub-rede IP. Com qualquer tráfego L2, o tráfego é sempre inundado para todos os aplicativos, mesmo que a comunicação entre eles não seja necessária. As restrições entre os dois aplicativos não são possíveis nesse cenário.



Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- A Cisco Secure Workload (CSW)/Tetration (Secure Workload) deve ser implantada no ambiente para coletar os dados de fluxo de tráfego entre os aplicativos.
- Os agentes devem ser implantados nos servidores para coletar os dados. Assim, isso só é possível no caso de implantação em áreas industriais abandonadas.
- Os agentes devem ser implantados nos servidores por pelo menos 3 a 4 semanas para a coleta de dados.
- Se alguma ferramenta de mapeamento de dependências de aplicativos (ADM) não estiver disponível, os dados relevantes deverão ser fornecidos.
- O gateway do servidor deve ser configurado usando a malha da infraestrutura centrada em aplicativos (ACI).

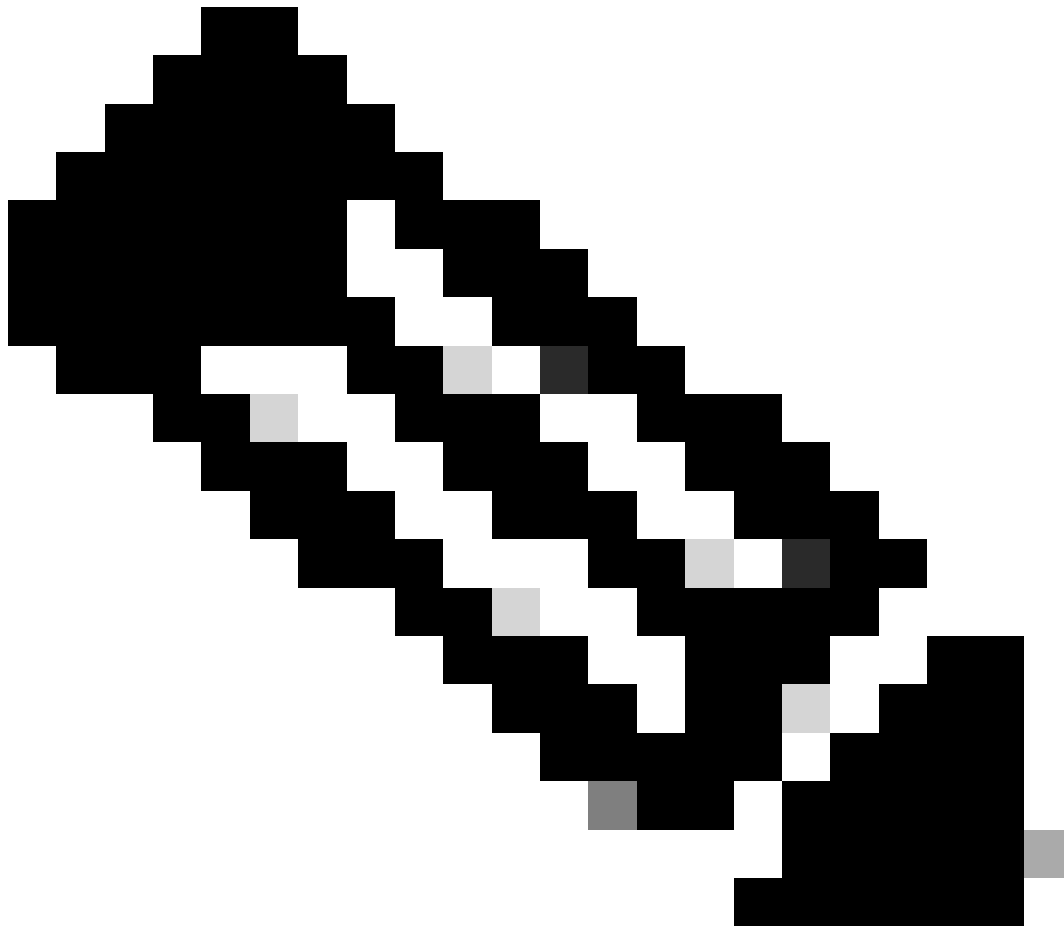
Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral da solução

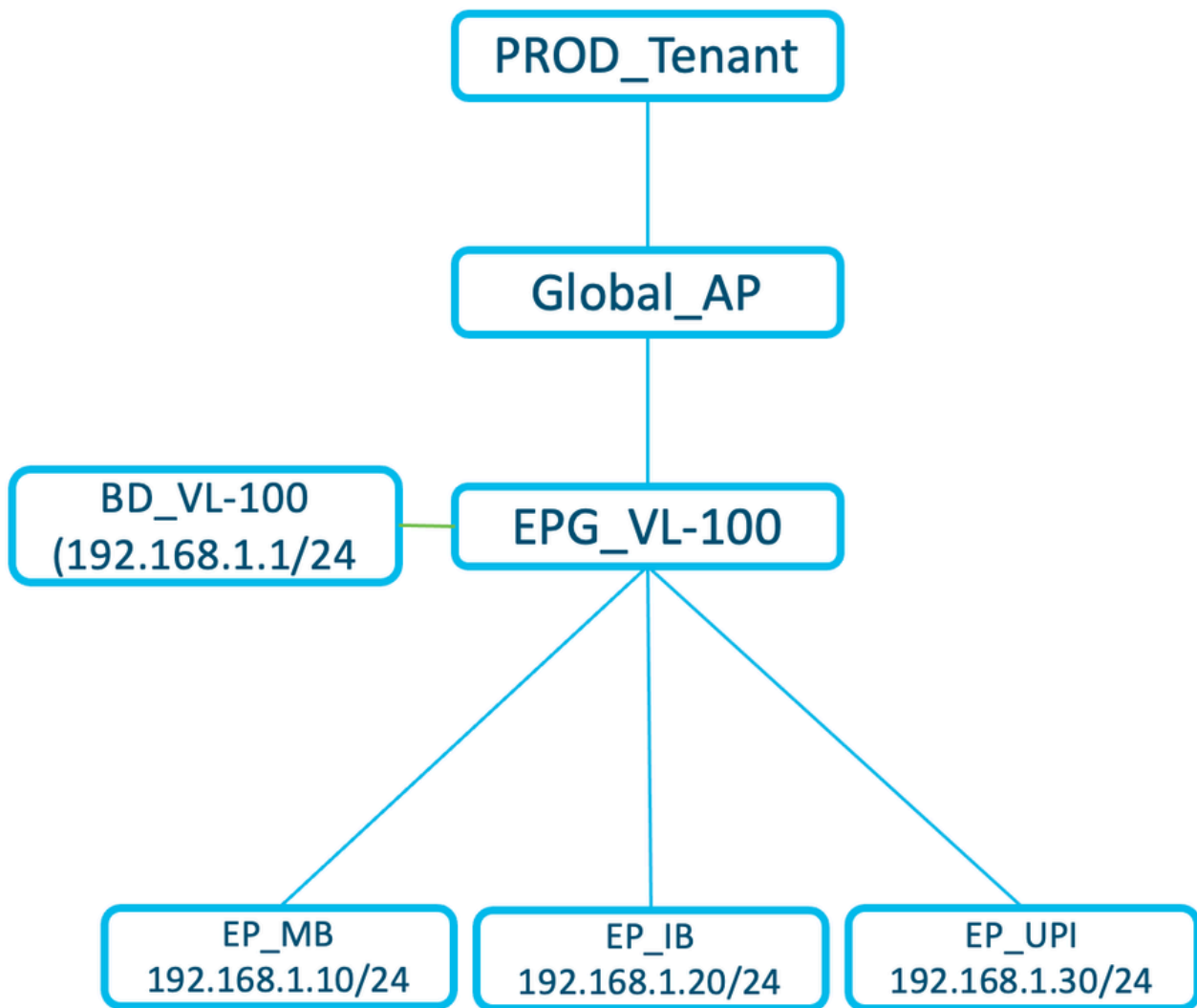
Para obter a microssegmentação, é preciso primeiro migrar a rede para uma solução de SDN da Cisco a partir da infraestrutura tradicional e reprojeter a rede a partir de uma visão centrada em aplicativos. Esta seção descreve as duas fases do projeto para atingir a segmentação desejada com base no fluxo de aplicativos que é capturado através da ferramenta ADM. Inicialmente, a solução Cisco ACI é implantada no modo centrado em rede (como está no projeto atual) e, em seguida, movida para o modo centrado em aplicativos.



Observação: você também pode combinar esse modo de implantação para migrar diretamente os serviços da rede tradicional para o modo centrado em aplicativos.

Projeto centrado na rede

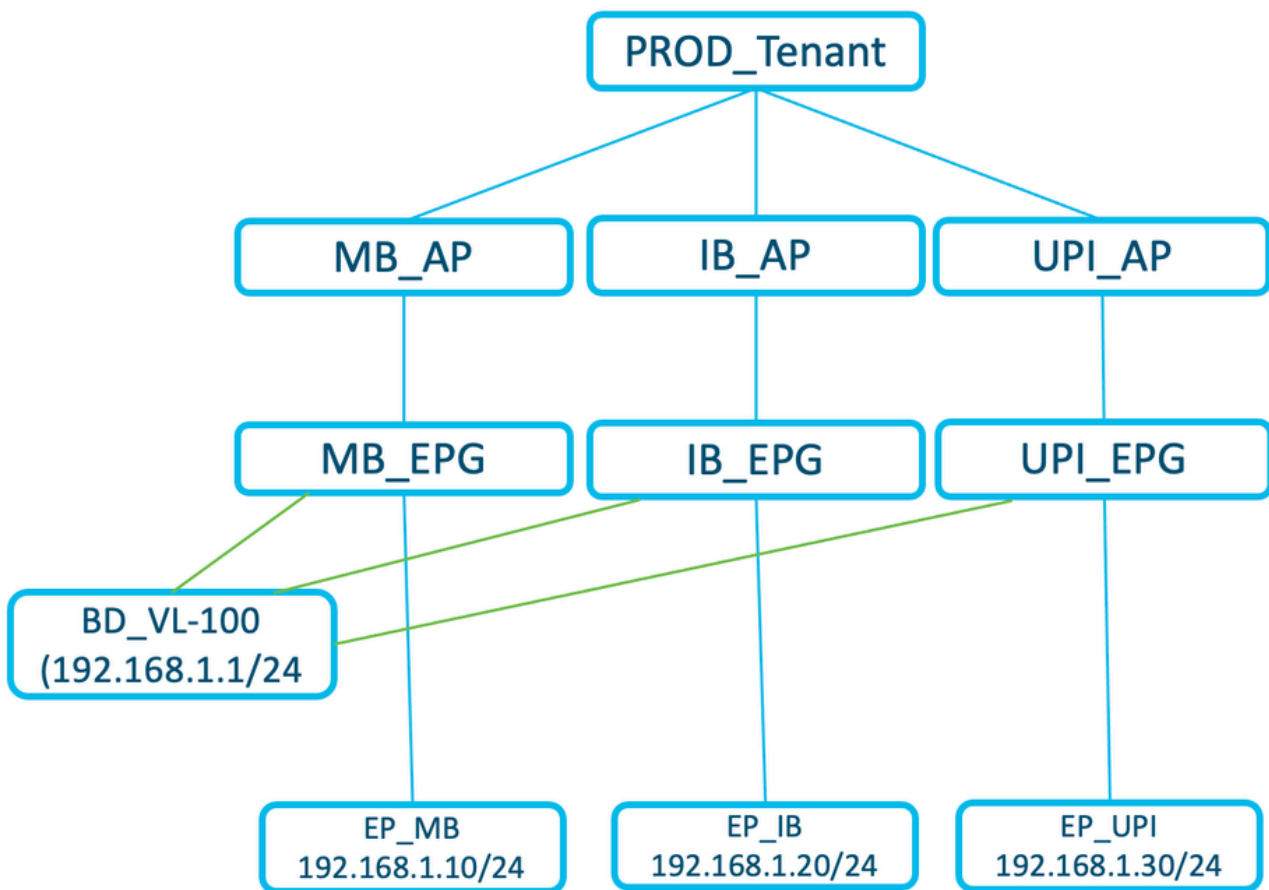
No exemplo mostrado no diagrama, EPG_VL-100 contém três aplicativos, EP_MB, EP_IB e EP_UPI, e compartilha a mesma sub-rede IP e usa VLAN 100.



- Migração atual da rede tradicional para a ACI.
- Um grupo de endpoint (EPG) pode conter vários aplicativos.
- Nenhuma segmentação de aplicativo no mesmo EPG neste tipo de implantação.
- 1 BD = 1 EPG = 1 VLAN

Design centrado em aplicativos

O exemplo mostrado no diagrama é um EPG separado para três aplicativos EP_MB, EP_IB e EP_UPI que compartilham a mesma sub-rede IP e usam VLANs diferentes mapeadas para cada EPG.

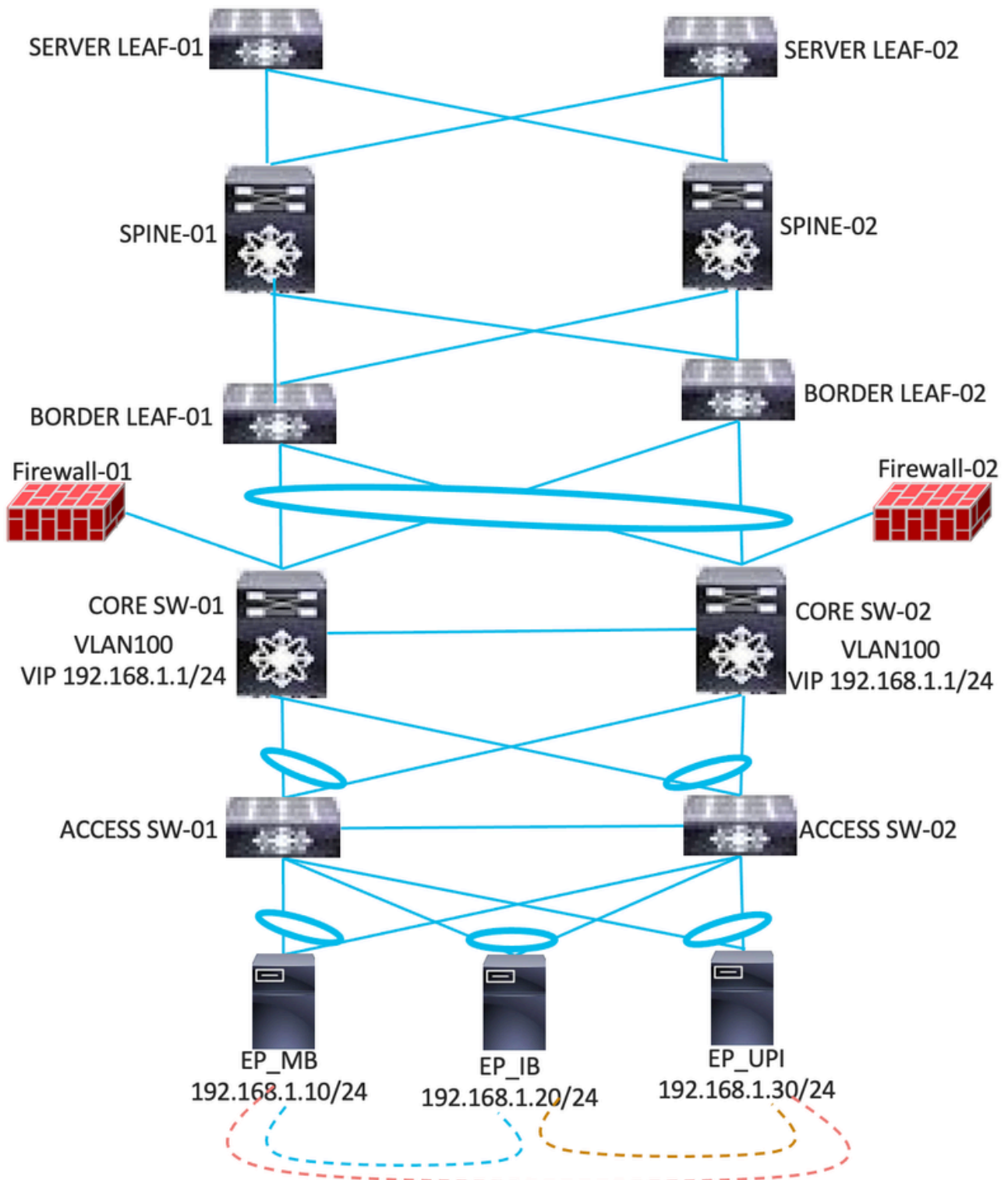


- No tipo de implantação centrada em aplicativos, diferentes EPGs são configurados de acordo com o aplicativo.
- Os aplicativos continuam usando a mesma sub-rede IP e seu gateway.
- Os EPGs do aplicativo segmentado usam uma nova VLAN.
- 1 BD a ser configurado com sub-rede IP e mapeado para EPGs de vários aplicativos.
- 1 BD = N EPG = N VLAN
- Agora, dois EPGs (aplicativos) podem se comunicar entre si por meio do Contrato.

Abordagens de migração

Antes de implantar a ACI como centrada em aplicativos, a ACI pode ser implantada como centrada em rede e, além disso, os aplicativos podem ser segmentados.

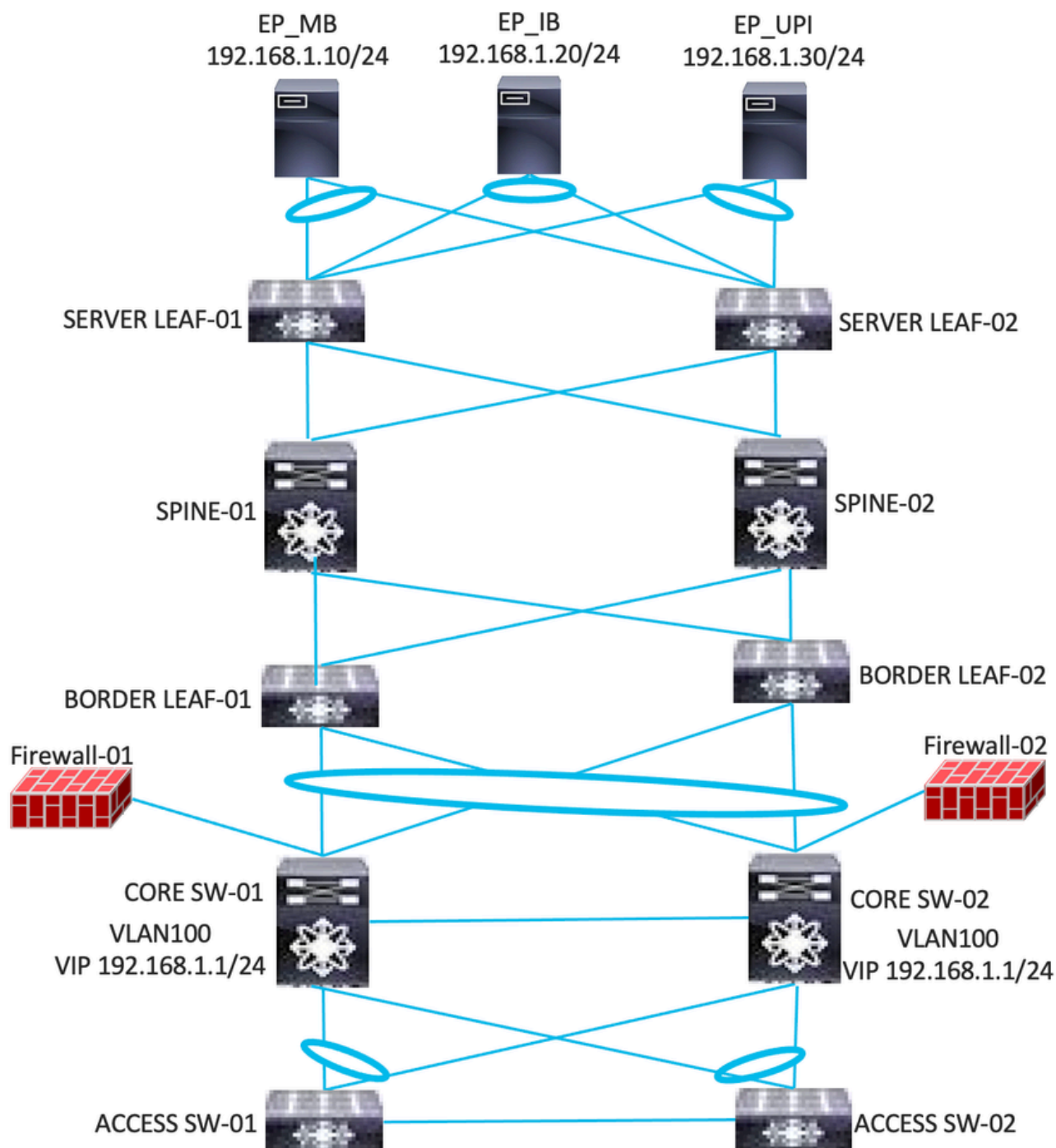
Abordagem de migração centrada na rede: Fase 1



- O link temporário da camada 2 deve ser estabelecido entre os switches Border Leaf e Core.
- Configure o domínio de ponte de camada 2 e o grupo de endpoint na ACI de acordo com as VLANs existentes configuradas em redes tradicionais.
- Configure todas essas VLANs no link intermediário de Camada 2 entre os switches Border Leaf e Core.
- A ACI deve estar aprendendo todos os endpoints presentes nos switches centrais.
- O Gateway permanece nos switches centrais.

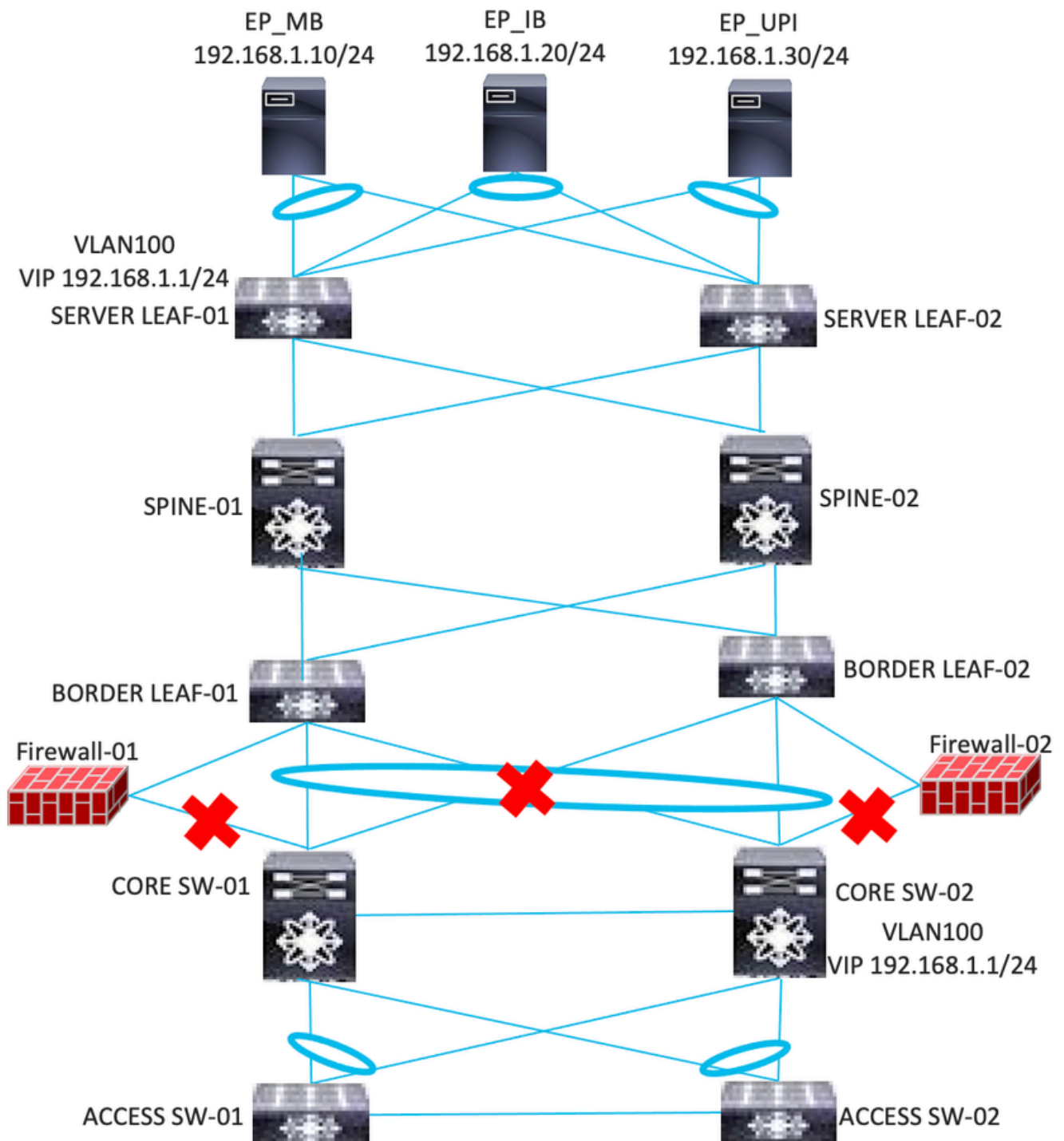
- A conectividade de firewall permanece nos switches centrais.

Abordagem de migração centrada na rede: Fase 2



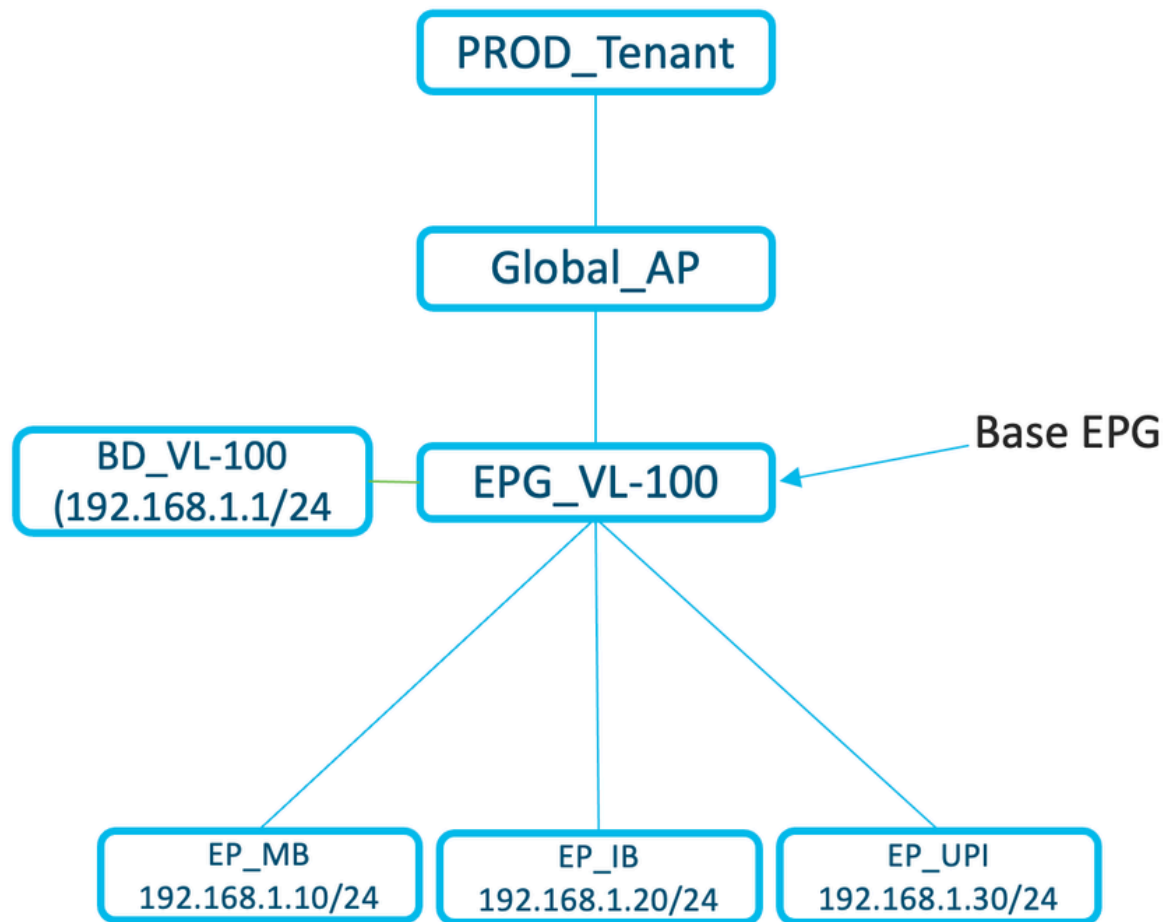
- Mude as cargas de trabalho de Switches de acesso para Folha do servidor.
- O gateway permanece nos switches centrais.
- Verifique se o Gateway pode ser acessado dos servidores.
- Verifique se o servidor/aplicativo está acessível.

Abordagem de migração centrada na rede: Fase 3



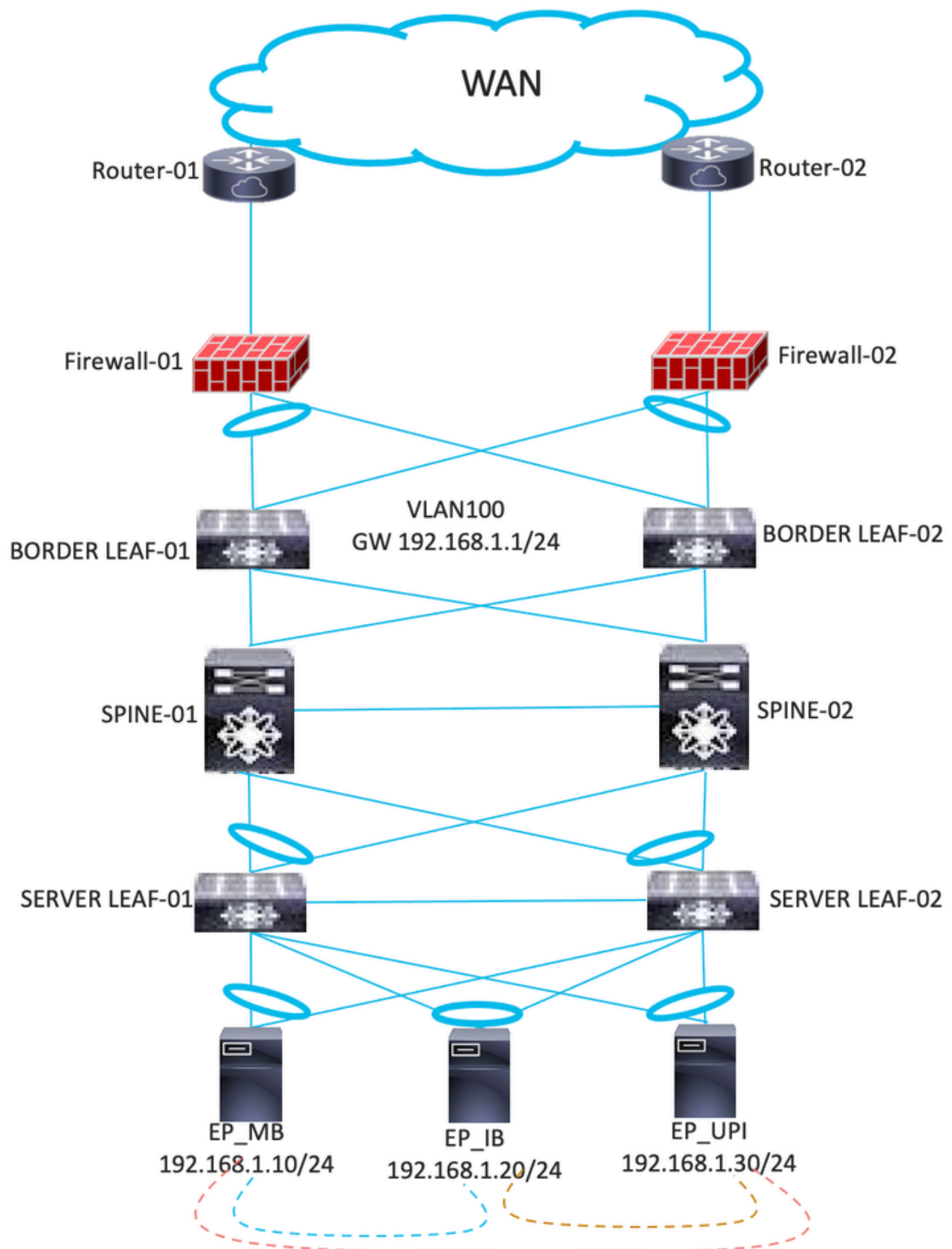
- Feche os gateways nos switches centrais e configure na ACI.
- Mude o link do firewall de Core Switches para ACI Leaf.
- Configure o L3out na direção do Firewall/Roteador.
- Adicione as rotas no firewall/roteador e no leaf da ACI.
- Desligue o link entre os switches Border Leaf e Core.
- Verifique se o servidor/aplicativo está acessível.

Representação lógica da ACI após a abordagem de migração centrada na rede.



➤ **1 BD = 1 EPG = 1 VLAN**

Abordagem de migração centrada em aplicativos: Fase 1



- Coleta e análise de dados de CSW/Tetration.
- Nova configuração de EPG de acordo com os dados de Tetration/CSW (WEB, APP e DB).
- Por exemplo, para o aplicativo MB, três EPGs são criados, como EPG_MB_WEB, EPG_MB_APP e EPG_MB_DB. Esses EPGs devem ser configurados em um perfil de

aplicativo AP_MB.

- No caso da integração do Virtual Machine Manager (VMM), a configuração do vDS é necessária para mapear os servidores no novo EPG com a nova VLAN.
- Mapeie a Máquina Virtual (VM) para o novo vDS que é enviado por meio da integração do VMM.
- Para baremetal, o grupo de servidores deve alterar a ID da VLAN no servidor.
- O endereçamento IP deve ser o mesmo para essas implantações.
- Configuração de contrato entre EPGs de acordo com os dados de CSW/Tetration.

Análise de dados de CSW/Tetration

Exemplo da análise com base nos dados do CSW/Tetration:

src_ip	escopo_consumidor	dst_ip	provider_scope	protocol	porta
192.168.34.248	Padrão:Interno:Sede	192.168.20.81	PRODAPP	TCP	443
192.168.78.45	Padrão:Interno:Sede	192.168.20.81	PRODAPP	TCP	443
192.168.78.16	Padrão:Interno:Sede	192.168.20.81	PRODAPP	TCP	443
192.168.78.25	Padrão:Interno:Sede	192.168.20.81	PRODAPP	TCP	443
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.81	PRODAPP	UDP	137
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.81	PRODAPP	TCP	445
192.168.32.173	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:DMZ	192.168.20.81	PRODAPP	TCP	7777
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	135
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	UDP	137
192.168.44.48	Padrão:Interno:Centro de	192.168.20.81	PRODAPP	UDP	137

	dados:DC:Aplicativo:Prod:Monitoramento				
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	443
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	445
192.168.44.48	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	445
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	5985
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	49154
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	49169
192.168.44.29	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	4750
192.168.44.30	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.81	PRODAPP	TCP	4750
192.168.44.21	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:AAA	192.168.20.81	PRODAPP	ICMP	0
192.168.103.80	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.71	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.103.20	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:DHCP	192.168.20.81	PRODAPP	TCP	7777

192.168.103.21	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:DHCP	192.168.20.81	PRODAPP	TCP	7777
192.168.44.68	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.85	PRODDB	UDP	137
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.85	PRODDB	UDP	137
192.168.44.68	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.85	PRODDB	TCP	445
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	192.168.20.85	PRODDB	TCP	445
172.16.32.173	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:MZ	192.168.20.85	PRODDB	TCP	1522
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	135
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	UDP	137
192.168.44.48	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	UDP	137
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	UDP	161
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	445
192.168.44.48	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	445
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	5985

192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	49154
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	60801
192.168.44.30	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	4750
192.168.44.29	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	TCP	4750
192.168.44.21	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	192.168.20.85	PRODDB	ICMP	0

Exemplo de recomendação de EPG do CSW/Tetration:

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

Com base nos detalhes, os dados devem ser analisados para a configuração do contrato.

Exemplo de dados analisados:

src_ip	escopo_consumidor	consumer_EPG	dst_IP	provider_EPG	pro
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	UD
192.168.44.69	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Descoberta	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	TCP
192.168.44.47	Padrão:Interno:Centro de dados:DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCP

192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	UD
192.168.44.48	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.48	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	ICM
192.168.103.21	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TCR
192.168.44.68	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Descoberta	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	UD
192.168.44.68	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Descoberta	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	TCR
192.168.44.69	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCR
192.168.44.69	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UD

192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UD
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCF
192.168.44.48	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCF
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCF
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCF
192.168.44.48	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TCF
192.168.44.47	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Monitoramento	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	ICM
192.168.48.45	Padrão:Interno:Centro de dados: DC:Aplicativo:Prod:Backup	EPG_VL_71	192.168.20.85	EPG-PROD-DB	TCF

Com base no endereço IP, os EPGs do consumidor e do provedor são mencionados. Entradas duplicadas e tráfego Norte-Sul (como Internet, entre DC, entre zonas, etc.) devem ser excluídos desses dados. Há alguns EPGs nomeados com VLANs, como EPG_VL_157, EPG_VL_71 e assim por diante. Isso significa que esses servidores não são movidos para o EPG de destino como parte da migração centrada em aplicativos. Assim, o contrato entre eles deve ser configurado com o mapeamento atual do EPG. Depois que esses servidores são migrados para o EPG de destino, esses contratos existentes devem ser excluídos como parte do processo de limpeza e o contrato apropriado deve ser adicionado ao EPG de destino.

Contrato

Os contratos são necessários para a comunicação entre os EPGs. O fluxo de implementação durante o processo de configuração do contrato é abordado nesta seção.

1. Inicialmente, o contrato VzAny deve ser aplicado no nível Virtual Routing and Forwarding (VRF).

2. De acordo com os dados do CSW/Tetration, devem ser criados contratos específicos de EPG.
3. Configure a regra Deny_All com baixa prioridade para que o contrato VzAny não permita comunicação de tráfego não especificada. Para os aplicativos que ainda não foram migrados como centrados em aplicativos, a comunicação acontece por meio do VzAny Contract.
4. Após toda a migração, exclua o contrato VzAny do VRF.

A análise dos dados de CSW/Tetration e sua conversão em objetos apropriados da ACI é uma etapa muito importante. Por conseguinte, após a análise inicial, é importante discutir a nossa observação com os interessados e obter uma reconfirmação sobre o mesmo. Também durante a implementação, deve-se considerar cuidadosamente a fim de garantir que todo o tráfego seja permitido conforme esperado. Para solucionar problemas, você pode ativar o registro no contrato e também rastrear qualquer queda de pacote em uma porta específica usando uma interface GUI ou CLI.

```
leaf# show logging ip access-list internal packet-log deny
```

```
[ Ter Out 1 10:34:37 2019 377572 usecs]: Nome: Prod1:VRF1(VXLAN: 2654209), VlanTipo: Desconhecido, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192 P.168.22.11, PortaSP: 0, PortaDP: 0, Intf. orig.: Túnel7, Proto: 1, PktLen: 98  
[ Ter Out 1 10:34:36 2019 377731 usecs]: Nome: Prod1:VRF1(VXLAN: 2654209), VlanTipo: Desconhecido, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192 P.168.22.11, PortaSP: 0, PortaDP: 0, Intf. orig.: Túnel7, Proto: 1, PktLen: 98
```

contract_parser

Um script Python no dispositivo que produz uma saída que correlaciona as regras de zoneamento, os filtros e as estatísticas de ocorrências ao executar pesquisas de nome de IDs. Esse script é extremamente útil porque usa um processo de várias etapas e o transforma em um único comando que pode ser filtrado para EPGs/VRFs específicos ou outros valores relacionados ao contrato.

```
leaf#contract_parser.py
```

Chave:

```
[prio:RuleId] [vrf:{str}] protocolo de ação 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]
```

As quedas de pacotes também podem ser mostradas na GUI usando o caminho: Tenant >

Tenant_Name > Operational > Flows/Packets.

Considerações

Recomendação aquando da aplicação dos contratos entre os GPE:

1. A ACI não pode ser considerada um firewall em termos de mapeamento de políticas, o que pode causar alta utilização da memória endereçável de conteúdo ternário (TCAM).
2. Use um intervalo de filtros em vez de um grande número de filtros individuais.
3. Os contratos não devem utilizar mais de quatro gamas de filtros. Ele pode consumir alto Overflow Ternary Content Addressable Memory (OTCAM).
4. Se algum EPG exigir um grande número de portas, tente usar um contrato 'permit any'.
5. Como parte da solução, se você prevê a implantação de um grande número de contratos, considere modificar o Forwarding Scale Profile (FSP) adequadamente.
6. Antes de implantar um grande número de contratos, calcule o TCAM usando a fórmula: N° de EPG de Fornecimento * N° de EPG de Consumidor * Número de regras.
7. O tamanho da TCAM existente pode ser verificado na interface do usuário da ACI usando o caminho: Operations > Capacity Dashboard > Leaf Capacity ou

```
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
```

Alguns desafios da implantação e da solução centradas em aplicativos

1. Um número maior de contratos pode levar à alta utilização de TCAM de switches leaf.

Portanto, é importante rastrear ativamente a utilização de TCAM e também preparar um aumento estimado no valor de TCAM quando uma grande quantidade de implantação de configuração é feita. É bom ter um processo de verificador do criador para garantir que a configuração que está sendo enviada seja apropriada. Além disso, é recomendável realizar as alterações com uma janela de manutenção programada adequada.

2. A configuração em massa (mais de 50 k TCAM) em um único push de contrato pode levar a um travamento de memória do Policy Manager.

Recomenda-se enviar a configuração em blocos menores, especialmente quando o tamanho da configuração for grande. Isso oferece uma abordagem sistemática e sem riscos para a configuração do contrato. Além disso, com cada envio de configuração, meça o aumento nos valores de TCAM.

3. O fluxo de tráfego não é capturado se os aplicativos não se comunicam durante o intervalo de tempo de implantação do CSW/Tetration (3 a 4 semanas).

Para evitar tal situação, a melhor abordagem é obter os dados de CSW/Tetration novamente verificados dos proprietários de aplicativos antes da atividade de alteração. Além disso, após a implementação, verifique os registros para qualquer contagem de ocorrências de falha.

Adição de Valor

1. Todas as candidaturas foram segmentadas e restringidas de acordo com as orientações relativas aos bancos centrais.

2. Visibilidade da comunicação entre aplicativos após a migração para uma implantação centrada em aplicativos.

3. Obtém-se a microssegmentação da aplicação.

4. Uma visão do fluxo da aplicação. Em um perfil de aplicativo, os EPGs são mapeados de acordo com o fluxo de tráfego, como o perfil de aplicativo AP_Banking, para ter três EPGs (EPG_Banking_WEB, EPG_Banking_APP e EPG_Banking_DB), independentemente de sua sub-rede IP.

4. Uma visão do fluxo de aplicativos facilita a solução de problemas.

5. Infra é mais seguro.

6. Abordagem estruturada para a implementação e expansão futura.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.