Implementación de ACI centrada en aplicaciones

Contenido

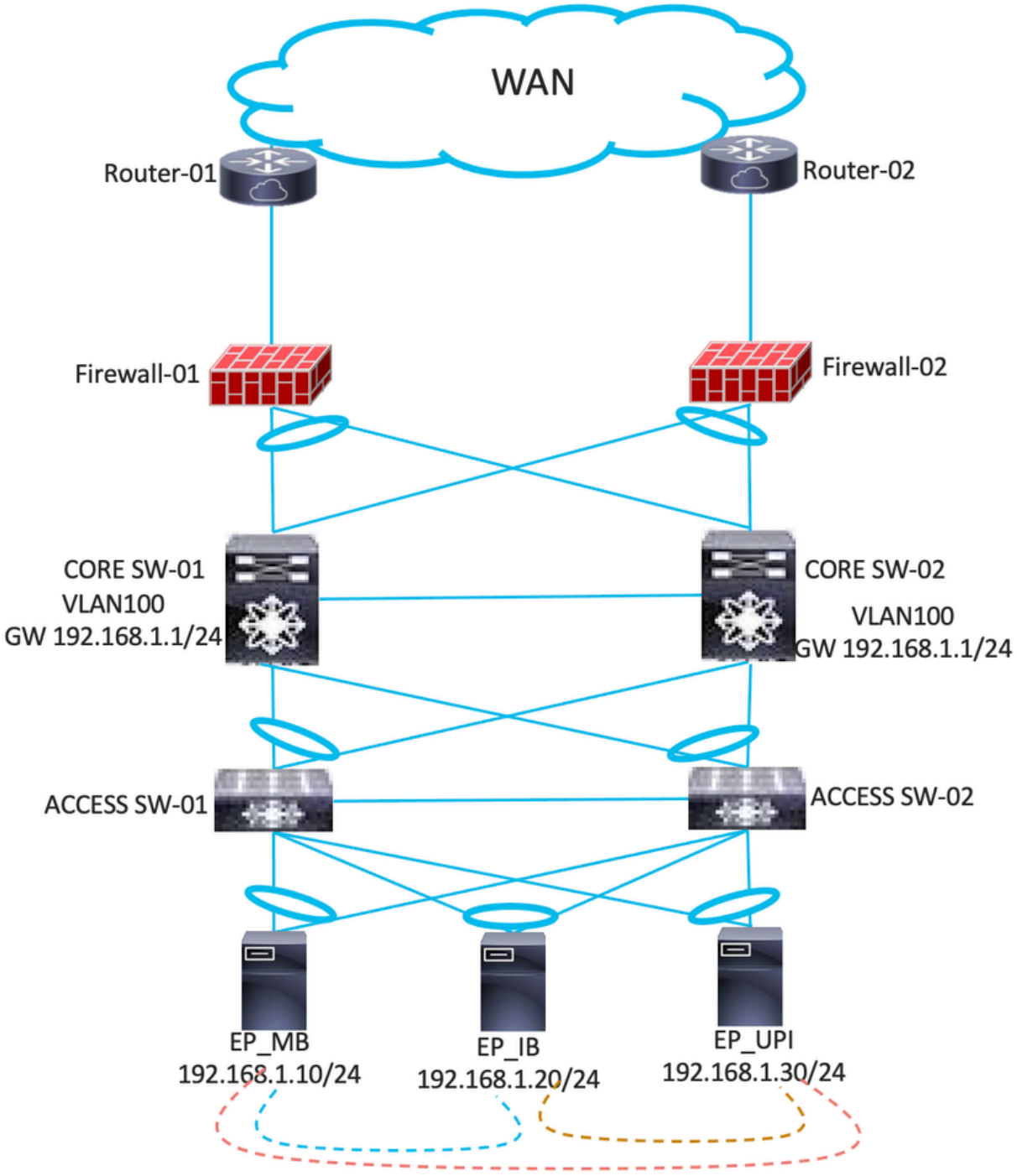
Introducción

Este documento describe el enfoque para lograr la microsegmentación y la seguridad dentro de las aplicaciones y entre ellas, aprovechando la solución SDN de Cisco ACI.

Restricciones de la red tradicional

- En las redes tradicionales, la segmentación dentro de una VLAN/Subred es imposible.
- Los gateways de aplicaciones se encuentran en switches de núcleo. Si dos aplicaciones desean comunicarse, se requieren listas de control de acceso (ACL) complejas en el switch principal.
- El bucle de árbol de extensión entre los switches interrumpe el flujo del Data Center y provoca una caída del tráfico.
- La misma subred IP contiene varias aplicaciones, lo que no proporciona seguridad entre ellas. La gestión de estas comunicaciones no es posible en las redes tradicionales.
- Considere un ejemplo que también se representa utilizando el diagrama. Tiene tres aplicaciones EP_MB, EP_IB y EP_UPI que forman parte de la misma VLAN y subred IP. Con cualquier tráfico L2, el tráfico siempre se inunda en todas las aplicaciones, aunque no

se requiera comunicación entre ellas. Las restricciones entre las dos aplicaciones no son posibles en este escenario.



Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Workload (CSW)/Tetration (Secure Workload) se debe implementar en el entorno para recopilar los datos de flujo de tráfico entre las aplicaciones.

- Los agentes se deben implementar en los servidores para recopilar los datos. Por lo tanto, esto solo es posible en el caso de implementaciones antiguas.
- Los agentes deben estar implementados en los servidores durante al menos 3-4 semanas para la recopilación de datos.
- Si alguna de las herramientas de asignación de dependencias de la aplicación (ADM) no está disponible, se deben proporcionar los datos relevantes.
- La puerta de enlace del servidor se debe configurar mediante el fabric de infraestructura centrada en aplicaciones (ACI).

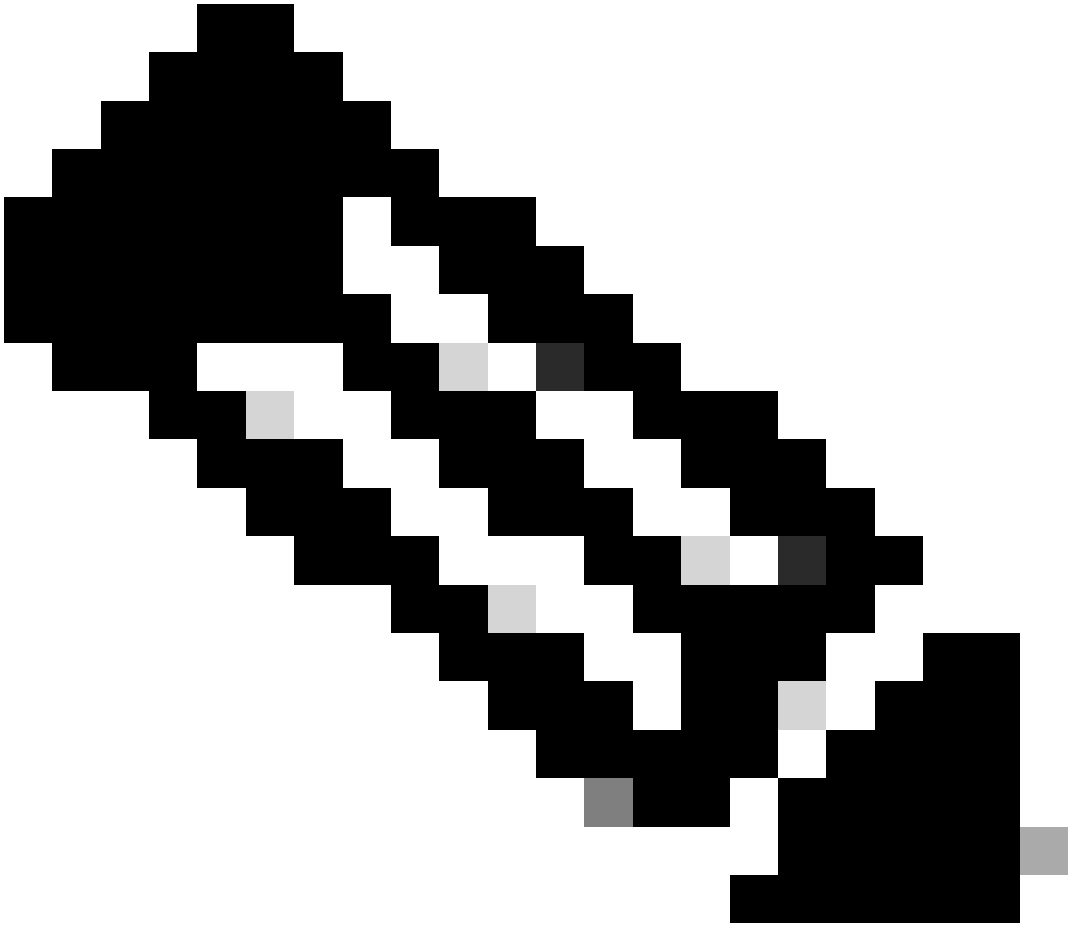
Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de soluciones

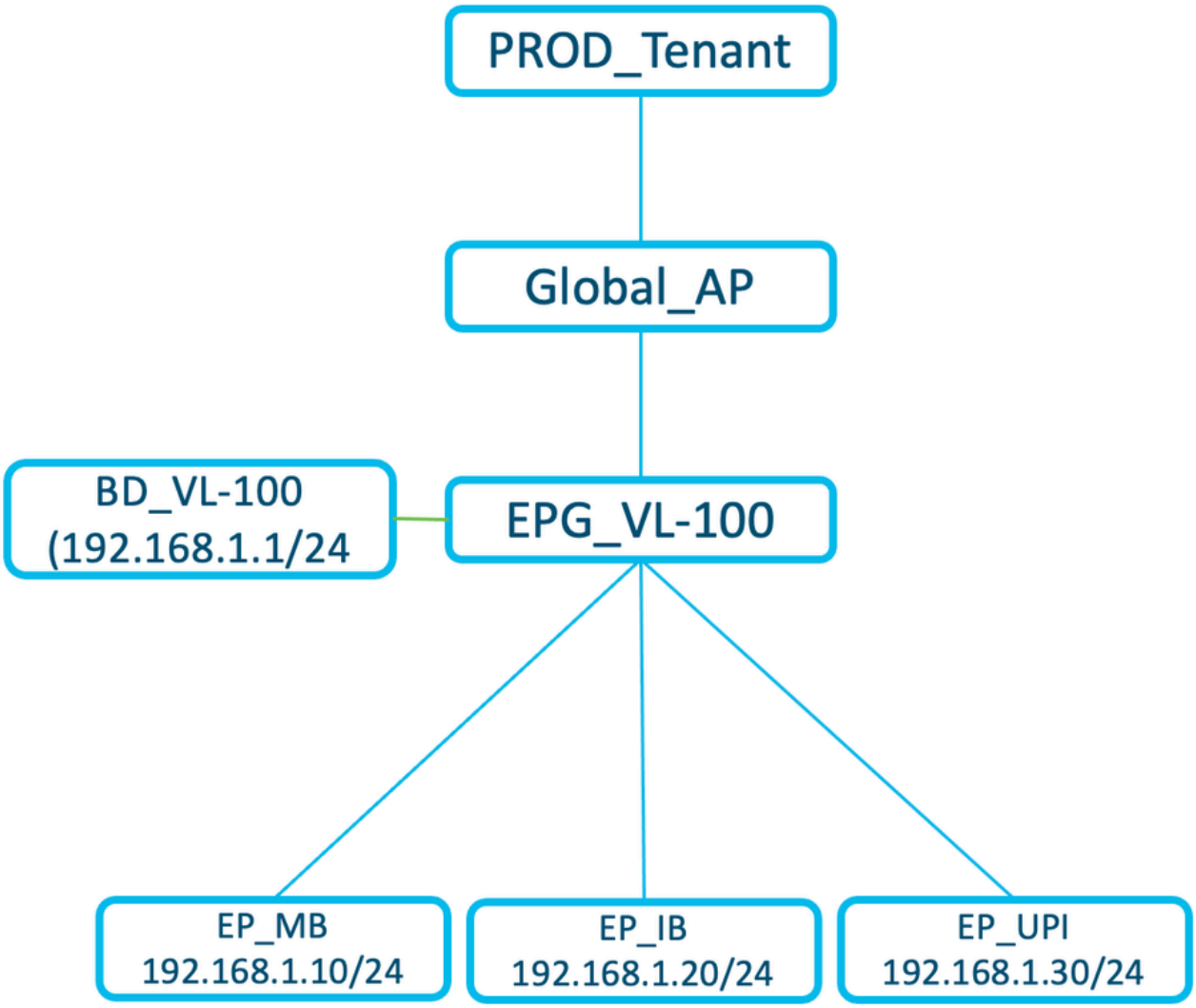
Para lograr la microsegmentación, primero debe migrar la red a una solución de SDN de Cisco desde la infraestructura tradicional y volver a diseñar la red desde una perspectiva centrada en las aplicaciones. En esta sección se describen las dos fases de diseño para lograr la segmentación deseada en función del flujo de la aplicación que se captura a través de la herramienta ADM. En un primer momento, la solución de Cisco ACI se implementa en el modo centrado en la red (tal cual en el diseño existente) y, a continuación, se pasa al modo centrado en las aplicaciones.



Nota: También puede combinar este modo de implementación para migrar directamente los servicios de la red tradicional al modo centrado en aplicaciones.

Diseño centrado en la red

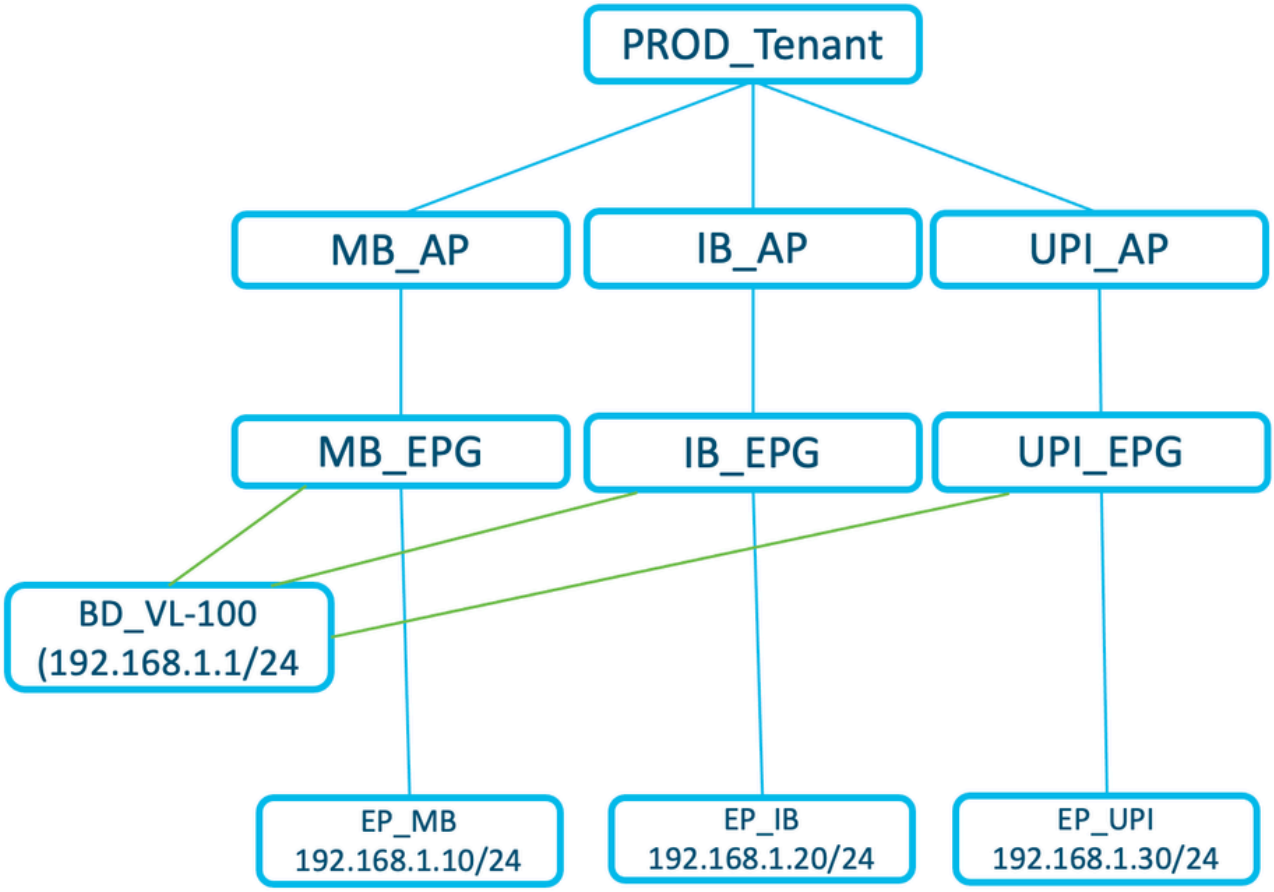
En el ejemplo que se muestra en el diagrama, EPG_VL-100 contiene tres aplicaciones, EP_MB, EP_IB y EP_UPI, y comparte la misma subred IP y utiliza VLAN 100.



- Migración "tal cual" de la red tradicional a ACI.
- Un grupo de terminales (EPG) puede contener varias aplicaciones.
- No hay segmentación de aplicaciones en el mismo EPG en este tipo de implementación.
- 1 BD = 1 EPG = 1 VLAN

Diseño centrado en aplicaciones

El ejemplo que se muestra en el diagrama es un EPG independiente para tres aplicaciones: EP_MB, EP_IB y EP_UPI que comparten la misma subred IP y utilizan diferentes VLAN asignadas a cada EPG.

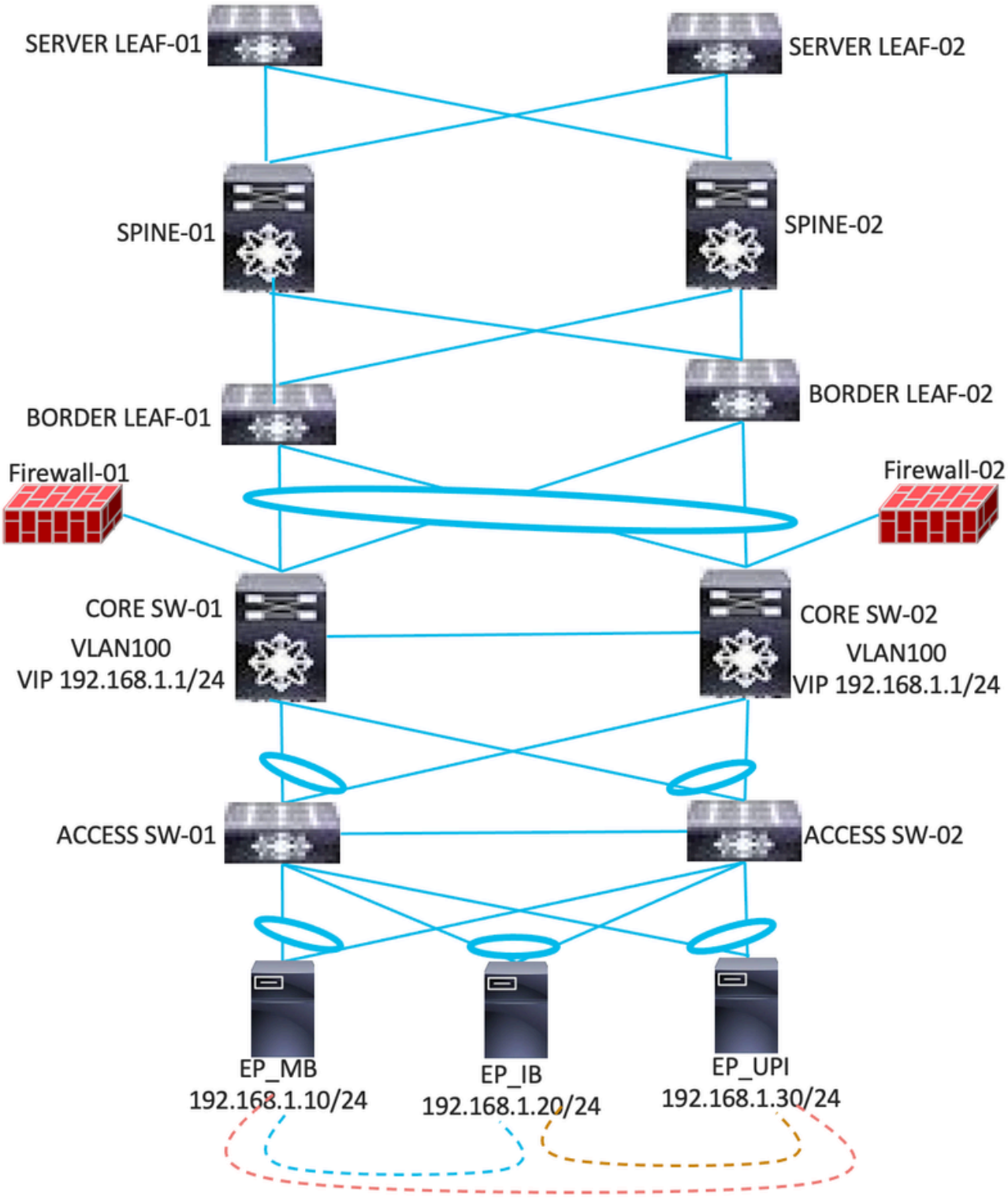


- En el tipo de implementación centrada en aplicaciones, se configuran diferentes EPG según la aplicación.
- Las aplicaciones continúan utilizando la misma subred IP y su gateway.
- Los EPG de aplicación segmentados para utilizar una nueva VLAN.
- 1 BD se configurará con una subred IP y se asignará a varios EPG de aplicación.
- 1 BD = N EPG = N VLAN
- Ahora, dos EPG (aplicaciones) pueden comunicarse entre sí mediante un contrato.

Enfoques de migración

Antes de implementar ACI como centrada en aplicaciones, ACI se puede implementar como centrada en la red y, además, las aplicaciones se pueden segmentar.

Enfoque de migración centrado en la red: fase 1

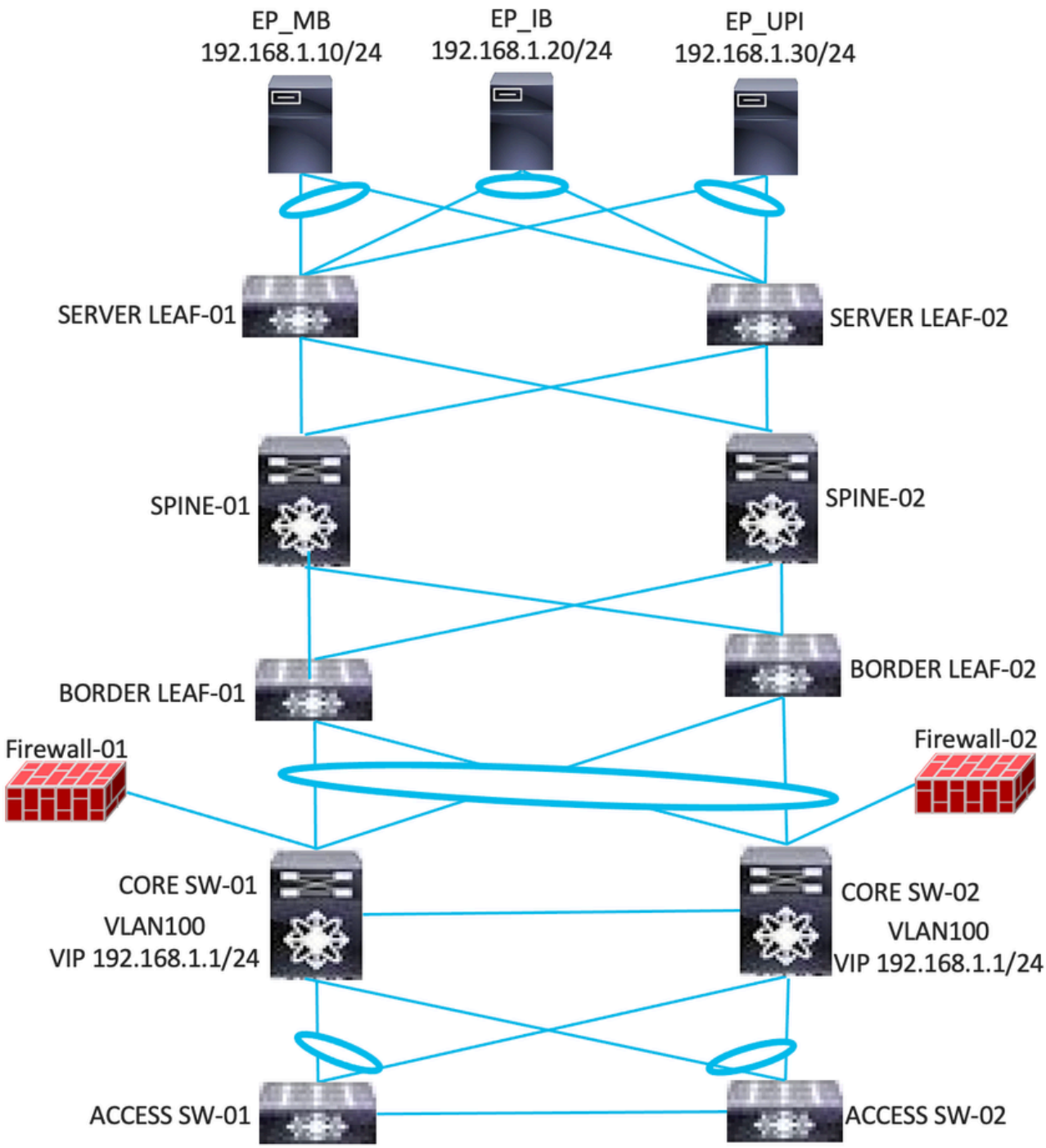


- Se debe establecer un link provisional de Capa 2 entre los switches de hoja de borde y de núcleo.
- Configure el dominio de puente de capa 2 y el grupo de terminales en ACI según las VLAN existentes configuradas en las redes tradicionales.
- Configure todas estas VLAN en el link interino de Capa 2 entre los switches de hoja de borde y núcleo.
- ACI debe estar aprendiendo todos los terminales que están presentes en los switches de

núcleo.

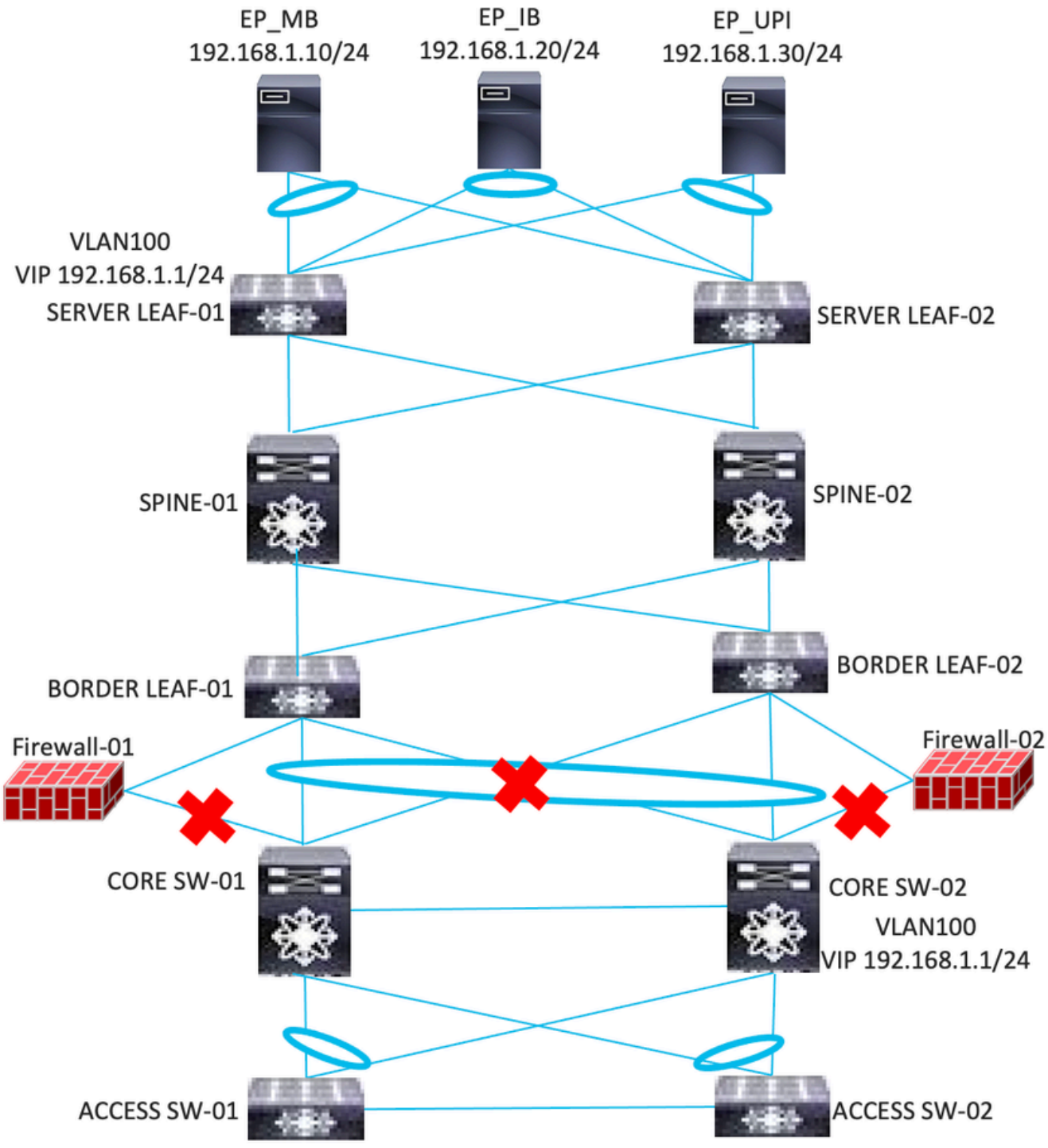
- La puerta de enlace permanece en los switches de núcleo.
- La conectividad del firewall permanece en los switches de núcleo.

Enfoque de migración centrado en la red: fase 2



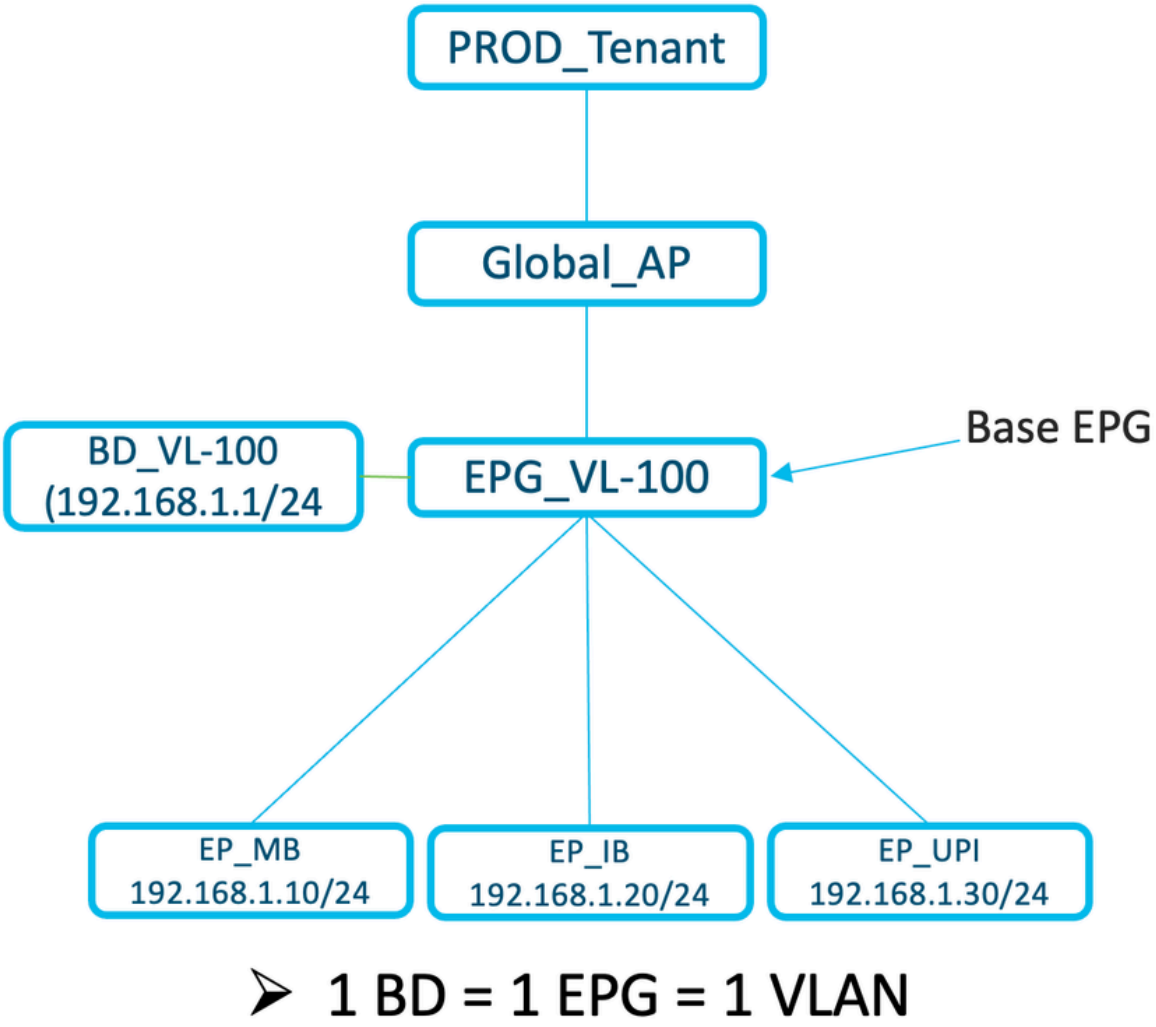
- Cambie las cargas de trabajo de switches de acceso a Server Leaf.
- La puerta de enlace permanece en los switches principales.
- Compruebe que la puerta de enlace está accesible desde los servidores.
- Verifique que el servidor/aplicación sea accesible.

Enfoque de migración centrado en la red: fase 3

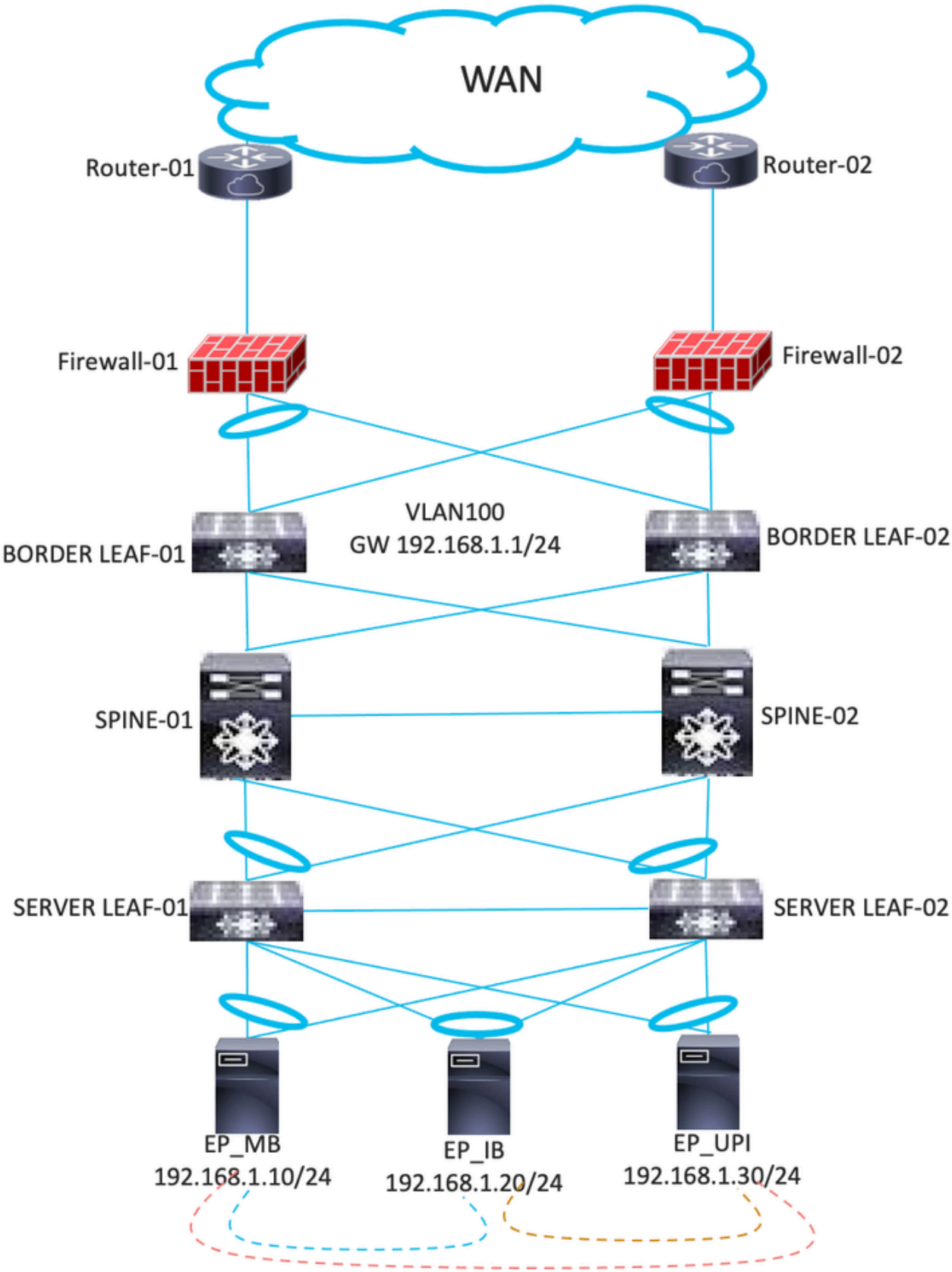


- Cierre los gateways en los switches principales y configúrelos en ACI.
- Cambie el enlace del firewall de los switches de núcleo a la hoja de ACI.
- Configure el L3out hacia el firewall/router.
- Agregue las rutas del firewall/router y la hoja de ACI.
- Cierre el enlace entre los switches de núcleo y de hoja de frontera.
- Verifique que el servidor/aplicación sea accesible.

Representación lógica de ACI después del enfoque de migración centrada en la red.



Enfoque de migración centrado en las aplicaciones: fase 1



- Recopilación y análisis de datos de CSW/Tetration.
- Nueva configuración de EPG según CSW/Tetration Data (WEB, APP y DB).
- Por ejemplo, para la aplicación MB, se crean tres EPG, como EPG_MB_WEB, EPG_MB_APP y EPG_MB_DB. Estos EPG deben configurarse en un AP_MB de perfil de

aplicación.

- En el caso de la integración de Virtual Machine Manager (VMM), se requiere la configuración de vDS para asignar los servidores del nuevo EPG a la nueva VLAN.
- Asigne la máquina virtual (VM) al nuevo vDS que se envía mediante la integración de VMM.
- En el caso de las conexiones básicas, el equipo del servidor debe cambiar el ID de VLAN en el servidor.
- El direccionamiento IP debe ser el mismo para estas implementaciones.
- Configuración de contratos entre EPG según los datos de CSW/Tetration.

CSW/Tetration Data Analysis

Ejemplo del análisis basado en los datos de CSW/Tetration:

src_ip	consumer_scope	dst_ip	alcance_proveedor	Protocolo	p
192.168.34.248	Predeterminado:Interno:Sede	192.168.20.81	PRODAPP	TCP	4
192.168.78.45	Predeterminado:Interno:Sede	192.168.20.81	PRODAPP	TCP	4
192.168.78.16	Predeterminado:Interno:Sede	192.168.20.81	PRODAPP	TCP	4
192.168.78.25	Predeterminado:Interno:Sede	192.168.20.81	PRODAPP	TCP	4
192.168.44.69	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.81	PRODAPP	UDP	1
192.168.44.69	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.81	PRODAPP	TCP	4
192.168.32.173	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:DMZ	192.168.20.81	PRODAPP	TCP	7
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP	1
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	UDP	1
192.168.44.48	Predeterminado:Interno:Data	192.168.20.81	PRODAPP	UDP	1

	Center:DC:Aplicación:Producto:Supervisión			
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.48	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.29	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.30	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.81	PRODAPP	TCP
192.168.44.21	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:AAA	192.168.20.81	PRODAPP	ICMP
192.168.103.80	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:DHCP	192.168.20.81	PRODAPP	TCP
192.168.103.71	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:DHCP	192.168.20.81	PRODAPP	TCP
192.168.103.20	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:DHCP	192.168.20.81	PRODAPP	TCP

192.168.103.21	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:DHCP	192.168.20.81	PRODAPP	TCP	
192.168.44.68	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.85	PRODDB	UDP	
192.168.44.69	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.85	PRODDB	UDP	
192.168.44.68	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.85	PRODDB	TCP	
192.168.44.69	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Detección	192.168.20.85	PRODDB	TCP	
172.16.32.173	Predeterminado:Interno:Data Center:DC:Aplicación:Prod:MZ	192.168.20.85	PRODDB	TCP	
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	UDP	
192.168.44.48	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	UDP	
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	UDP	
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	
192.168.44.48	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	

192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	4
192.168.44.47	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	6
192.168.44.30	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	4
192.168.44.29	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	TCP	4
192.168.44.21	Predeterminado:Interno:Data Center:DC:Aplicación:Producto:Supervisión	192.168.20.85	PRODDB	ICMP	0

Ejemplo de recomendación de EPG del CSW/Tetration:

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

Según los detalles, los datos deben analizarse para la configuración del contrato. Ejemplo de datos analizados:

src_ip	consumer_scope	consumer_EPG	dst_IP	provider_EPG	Pr
192.168.44.69	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Detección	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	U
192.168.44.69	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Detección	EPG_DISCOVERY	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center:	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC

	DC:Aplicación:Producto:Supervisión				
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	U
192.168.44.48	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.48	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.81	EPG-PROD-APP	IC
192.168.103.21	Predeterminado:Interno:Data Center: DC:Aplicación:Prod:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TC
192.168.44.68	Predeterminado:Interno:Data Center:	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	U

	DC:Aplicación:Producto:Detección				
192.168.44.68	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Detección	EPG_DISCOVERY	192.168.20.85	EPG-PROD-DB	TC
192.168.44.69	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.69	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UI
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	UI
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.48	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.47	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.48	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Supervisión	EPG_MONITORING	192.168.20.85	EPG-PROD-DB	TC
192.168.44.47	Predeterminado:Interno:Data	EPG_MONITORING	192.168.20.85	EPG-PROD-	IC

	Center: DC:Aplicación:Producto:Supervisión			DB	
192.168.48.45	Predeterminado:Interno:Data Center: DC:Aplicación:Producto:Copia de seguridad	EPG_VL_71	192.168.20.85	EPG-PROD-DB	T

En función de la dirección IP, se mencionan los EPG del proveedor y del consumidor. Las entradas duplicadas y el tráfico Norte-Sur (como el tráfico de Internet, entre DC, entre zonas, etc.) deben excluirse de estos datos. Hay algunos EPG denominados con VLAN como EPG_VL_157, EPG_VL_71, etc. Esto significa que estos servidores no se mueven al EPG de destino como parte de la migración centrada en aplicaciones. Por lo tanto, el contrato entre ellos debe configurarse con el mapeo actual de EPG. Una vez que estos servidores se migran al EPG de destino, estos contratos existentes deben eliminarse como parte del proceso de limpieza y el contrato adecuado debe agregarse al EPG de destino.

Contrato

Se requieren contratos para la comunicación entre los EPG. En esta sección se describe el flujo de implementación durante el proceso de configuración del contrato.

1. Inicialmente, VzCualquier contrato debe aplicarse en el nivel de reenvío y routing virtuales (VRF).

2. Según los datos CSW/Tetration, deben crearse contratos EPG específicos.

3. Configure la regla Deny_All con prioridad baja para que el contrato VzAny no permita la comunicación de tráfico sin especificar. Para las aplicaciones que aún no se han migrado como centradas en aplicaciones, la comunicación se realiza mediante VzAny Contract.

4. Después de toda la migración, suprima el contrato VzAny del VRF.

El análisis de los datos de CSW/Tetration y su conversión en objetos ACI adecuados es un paso muy importante. Por lo tanto, después del análisis inicial, es importante discutir nuestra observación con el interesado y obtener una reconfirmación sobre el mismo. También durante la implementación, se debe realizar una cuidadosa consideración para garantizar que todo el tráfico se permita según lo esperado. Para la resolución de problemas, puede habilitar el registro en el contrato y también realizar un seguimiento de cualquier caída de paquetes en un puerto específico mediante una interfaz GUI o CLI.

leaf# show logging ip access-list internal packet-log deny
[Mar Oct 1 10:34:37 2019 377572 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.11 68.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
[Mar Oct 1 10:34:36 2019 377731 usecs]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType:

Unknown, Vlan-Id: 0, SMac: 0x000c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.11 68.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98

contract_parser

Un script Python en el dispositivo que produce un resultado que correlaciona las reglas de zonificación, los filtros y las estadísticas de aciertos mientras se realizan búsquedas de nombres desde ID. Esta secuencia de comandos es extremadamente útil, ya que toma un proceso de varios pasos y lo convierte en un solo comando que se puede filtrar a EPG/VRF específicos u otros valores relacionados con el contrato.

leaf# contract_parser.py
Clave:
[prio:RuleId] [vrf:{str}] action protocol 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]

Las caídas de paquetes también se pueden mostrar en la GUI mediante la ruta: Arrendatario > Nombre_arrendatario > Operativo > Flujos/Paquetes.

Consideración

Recomendación al aplicar los contratos entre los GPE:

1. La ACI no puede considerarse un firewall en términos de asignación de políticas, lo que puede provocar un uso elevado de la memoria de contenido ternario direccionable (TCAM).

2. Utilice un rango de filtros en lugar de un gran número de filtros individuales.

3. Los contratos no podrán contener más de cuatro gamas de filtros. Puede consumir memoria de desbordamiento de contenido ternario direccionable (OTCAM).

4. Si cualquier EPG requiere un gran número de puertos, intente usar un contrato de 'permitir cualquier'.

5. Como parte de la solución, si prevé la implementación de un gran número de contratos, considere la posibilidad de modificar el perfil de escala de reenvío (FSP) en consecuencia.

6. Antes de desplegar un número masivo de contratos, calcule el TCAM mediante la fórmula: No. de Proporcionar EPG * No. de Consumidor EPG * Número de reglas.

7. El tamaño de TCAM existente se puede comprobar en la interfaz de usuario de ACI mediante la ruta: Operaciones > Panel de capacidad > Capacidad de hoja o

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

Algunos retos de la implementación y la solución centradas en las aplicaciones

1. Un mayor número de contratos puede conducir a una alta utilización de TCAM de los switches de hoja.

Por lo tanto, es importante realizar un seguimiento activo de la utilización de TCAM y también preparar un aumento estimado del valor de TCAM cuando se realiza una gran cantidad de implementación de configuración. Es bueno tener un proceso de verificador de fabricante para asegurarse de que la configuración que se envía es apropiada. Además, se recomienda llevar a cabo los cambios con una ventana de mantenimiento programada adecuada.

2. La configuración masiva (más de 50.000 TCAM) en una sola inserción de contrato puede provocar una caída de la memoria del administrador de políticas.

Se recomienda insertar la configuración en fragmentos más pequeños, especialmente cuando la configuración es de gran tamaño. Esto proporciona un enfoque sistemático y sin riesgos para la configuración de los contratos. Además, con cada empuje de configuración, mida el aumento en los valores TCAM.

3. El flujo de tráfico no se captura si las aplicaciones no se comunican durante el intervalo de tiempo de implementación CSW/Tetration (3-4 semanas).

Para evitar tal situación, el mejor enfoque es obtener los datos de CSW/Tetration verificados de los propietarios de la Aplicación antes de la actividad de cambio. Además, después de la implementación, verifique los registros de cualquier recuento de aciertos de error.

Adición de valor

1. Todas las solicitudes han sido segmentadas y restringidas de acuerdo con las directrices del Banco Central.

2. Visibilidad de la comunicación entre aplicaciones después de migrar a una implementación centrada en aplicaciones.

3. Se logra la microsegmentación de la aplicación.

4. Una vista del flujo de aplicaciones. En un perfil de aplicación, los EPG se asignan según el flujo de tráfico, como el perfil de aplicación AP_Banking, para tener tres EPG (EPG_Banking_WEB, EPG_Banking_APP y EPG_Banking_DB) independientemente de su subred IP.

4. Una vista del flujo de aplicaciones facilita la resolución de problemas.

5. Infra es más seguro.

6. Enfoque estructurado para la aplicación y la expansión futura.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).