Déploiement de l'ACI axée sur les applications

Table des matières

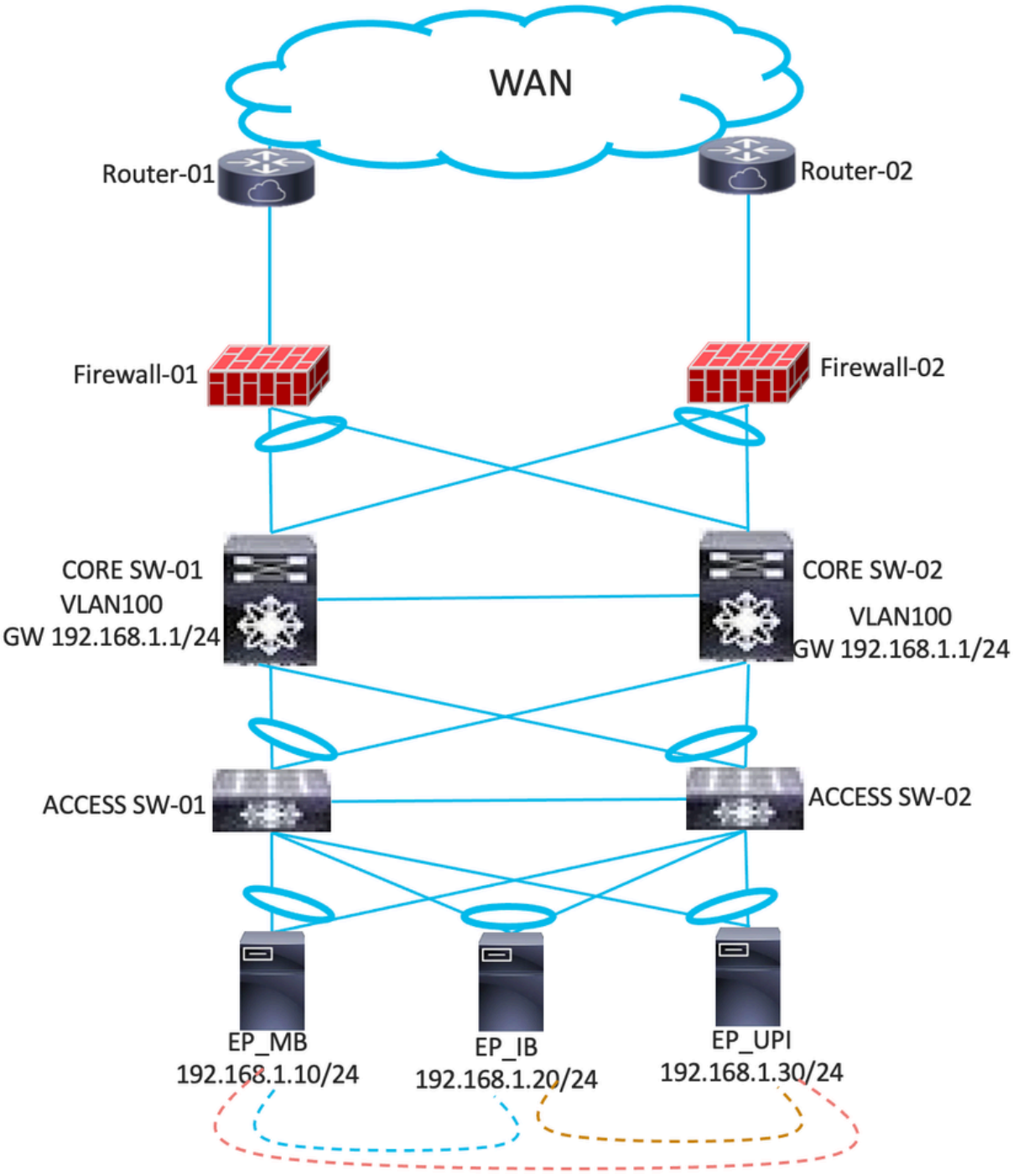
Introduction

Ce document décrit l'approche permettant de réaliser la microsegmentation et la sécurité au sein des applications et entre celles-ci, en exploitant la solution Cisco ACI SDN.

Contraintes liées au réseau traditionnel

- Dans les réseaux traditionnels, la segmentation au sein d’un VLAN/sous-réseau est impossible.
- Les passerelles d'application se trouvent sur les commutateurs principaux. Si deux applications souhaitent communiquer, des listes de contrôle d’accès (ACL) complexes sont requises sur le commutateur principal.
- La boucle Spanning Tree entre les commutateurs interrompt le flux du data center et entraîne une perte de trafic.
- Le même sous-réseau IP contient plusieurs applications, ce qui n'assure pas la sécurité entre elles. La gestion de ces communications n’est pas possible sur les réseaux traditionnels.
- Prenons un exemple qui est également représenté à l'aide du schéma. Vous disposez de

trois applications EP_MB, EP_IB et EP_UPI qui font partie du même VLAN et du même sous-réseau IP. Avec tout trafic de couche 2, le trafic est toujours diffusé à toutes les applications, même si aucune communication entre elles n'est requise. Les restrictions entre les deux applications ne sont pas possibles dans ce scénario.



Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Workload (CSW)/Tetration (Secure Workload) doit être déployé dans l'environnement afin de collecter les données de flux de trafic entre les applications.
- Les agents doivent être déployés sur les serveurs afin de collecter les données. Par conséquent, cela n'est possible que dans le cas d'un déploiement sur site.
- Les agents doivent être déployés sur les serveurs pendant au moins 3 à 4 semaines pour la collecte des données.
- Si des outils de mappage des dépendances des applications (ADM) ne sont pas disponibles, les données pertinentes doivent être fournies.
- La passerelle de serveur doit être configurée à l'aide du fabric ACI (infrastructure axée sur les applications).

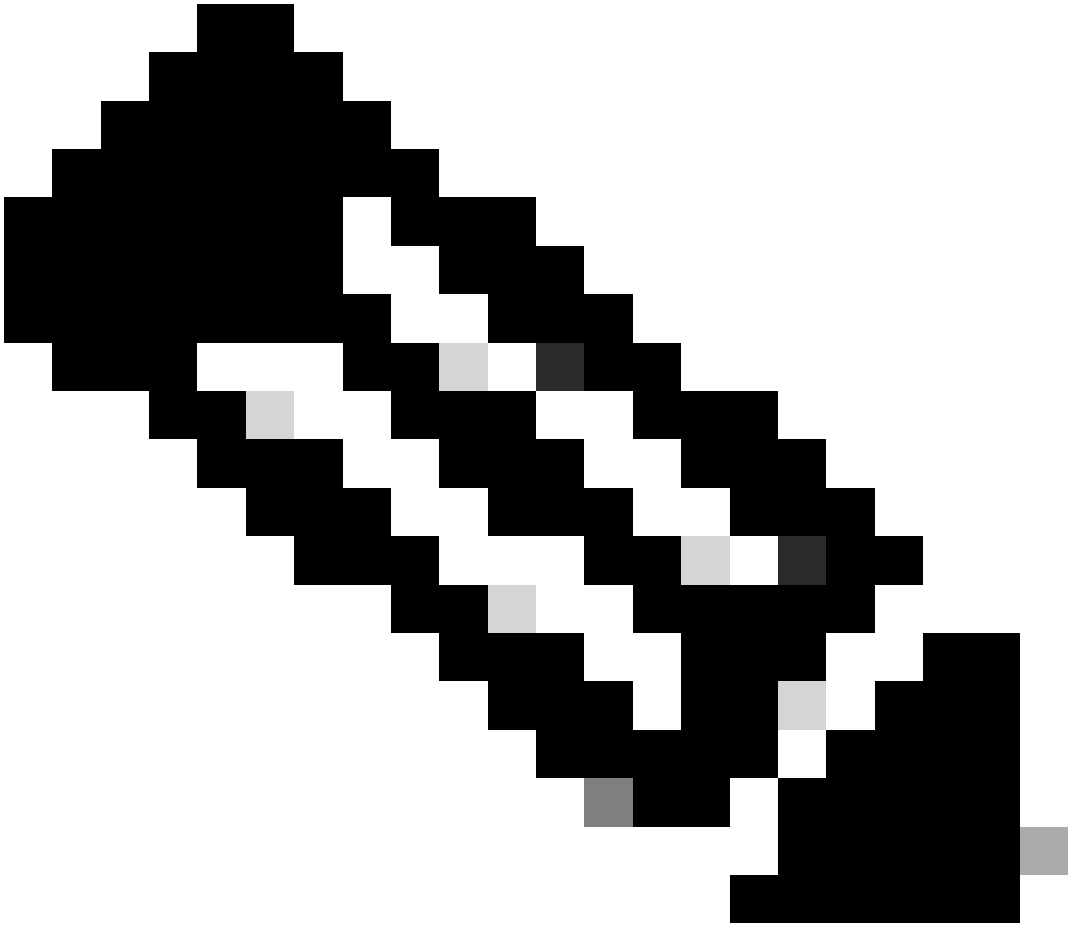
Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Présentation de la solution

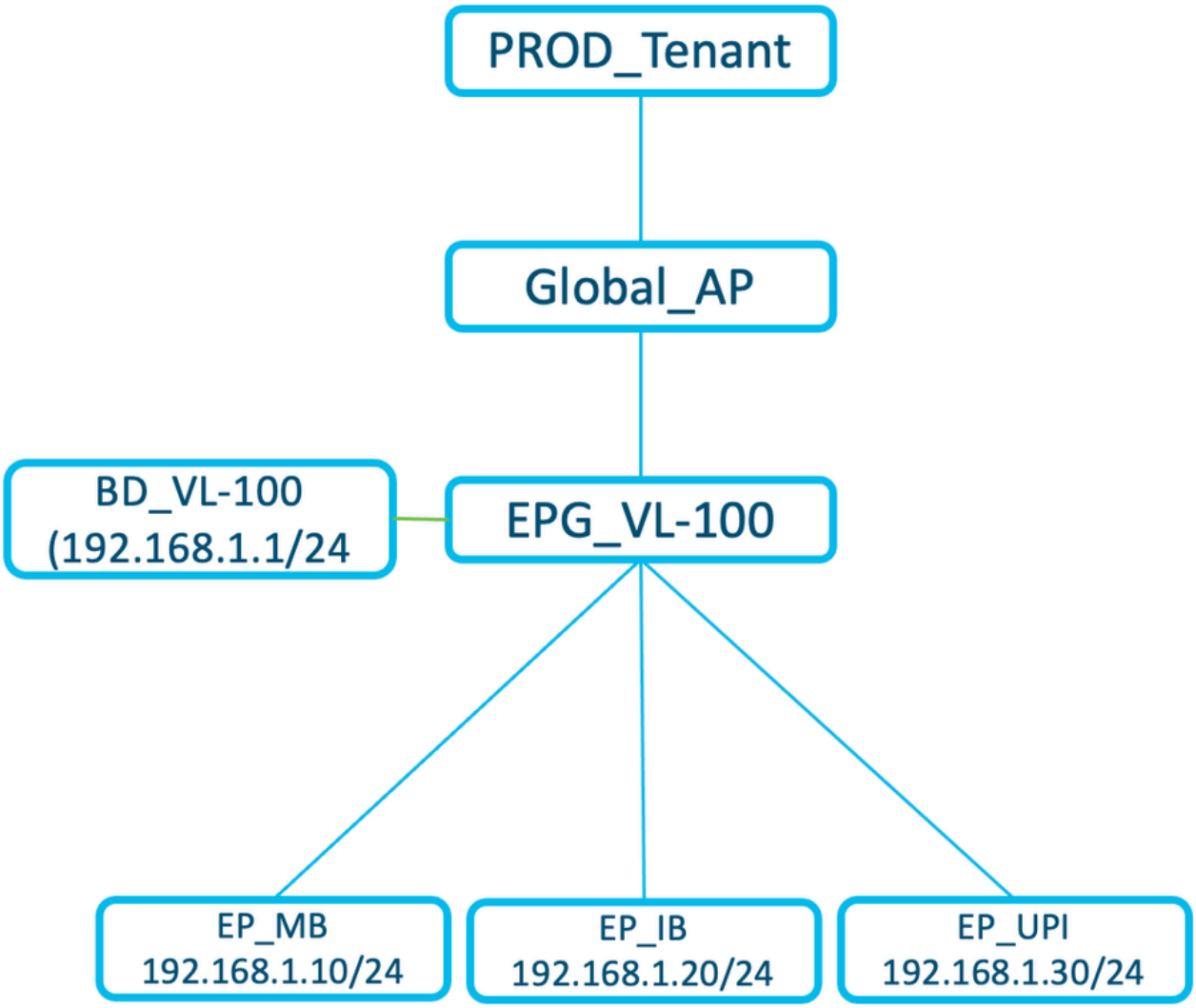
Pour parvenir à la microsegmentation, vous devez d'abord migrer le réseau vers une solution Cisco SDN à partir d'une infrastructure traditionnelle et reconcevoir le réseau à partir d'une vue axée sur les applications. Cette section décrit les deux phases de la conception afin d'obtenir la segmentation souhaitée en fonction du flux d'application capturé via l'outil ADM. Dans un premier temps, la solution Cisco ACI est déployée en mode centré sur le réseau (tel quel par rapport à la conception existante), puis déplacée vers le mode centré sur les applications.



Remarque : vous pouvez également combiner ce mode de déploiement afin de migrer directement les services du réseau traditionnel vers le mode axé sur les applications.

Conception axée sur le réseau

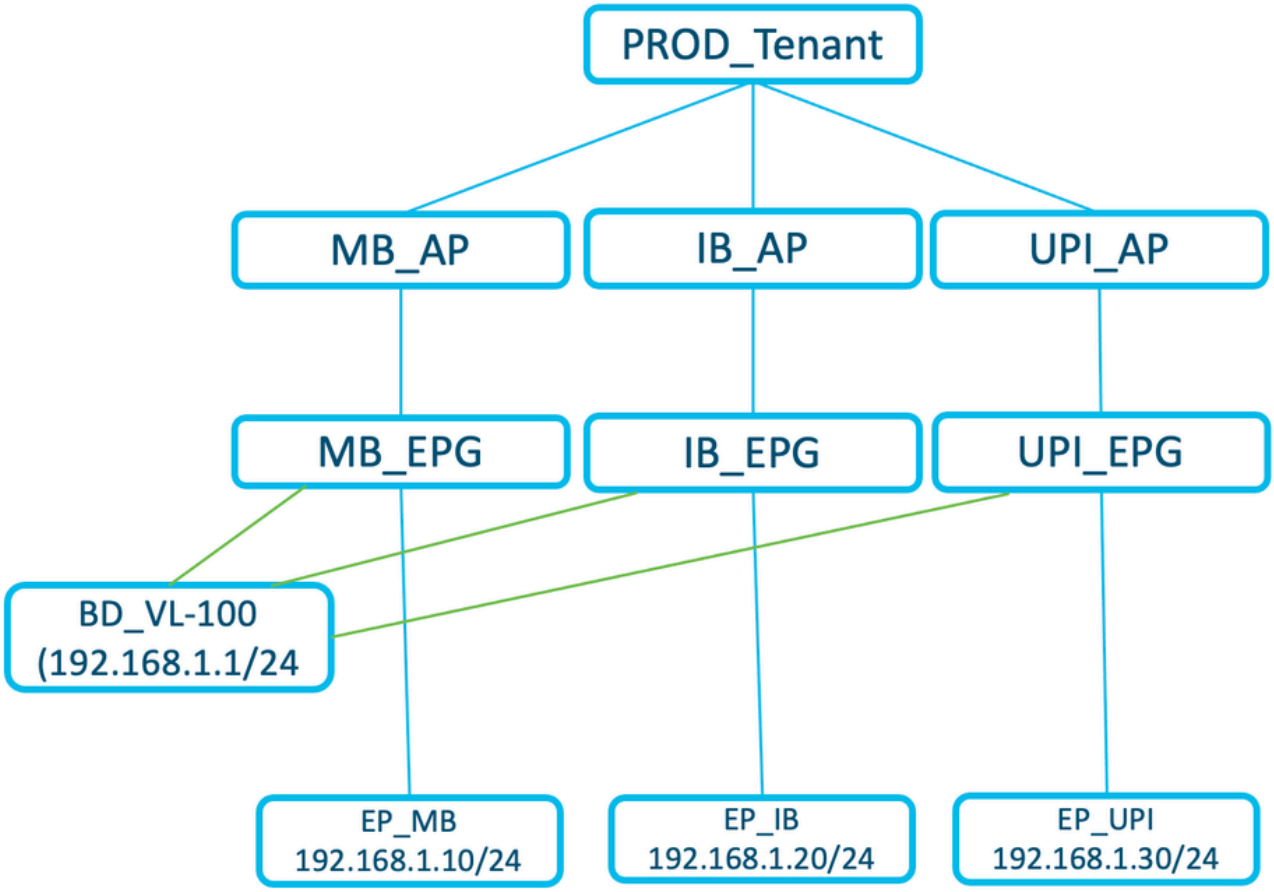
Dans l'exemple représenté sur le schéma, EPG_VL-100 contient trois applications, EP_MB, EP_IB et EP_UPI, et partage le même sous-réseau IP et utilise VLAN 100.



- Migration en l'état du réseau traditionnel vers l'ACI.
- Un groupe de terminaux (EPG) peut contenir plusieurs applications.
- Aucune segmentation d'application dans le même EPG dans ce type de déploiement.
- 1 BD = 1 EPG = 1 VLAN

Conception axée sur les applications

L'exemple représenté sur le schéma est un EPG distinct pour trois applications EP_MB, EP_IB et EP_UPI partageant le même sous-réseau IP et utilisant des VLAN différents mappés à chaque EPG.

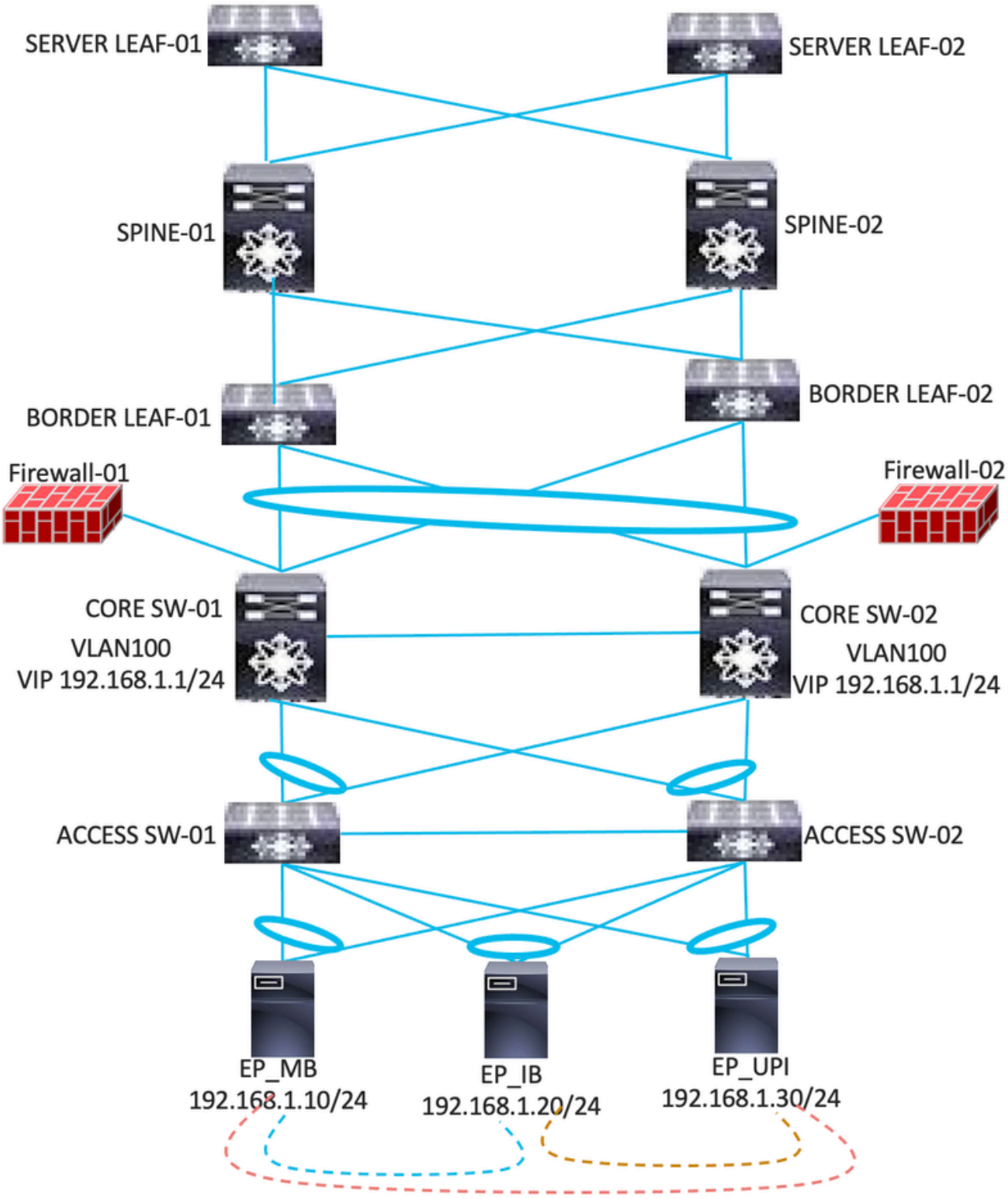


- Dans le type de déploiement axé sur les applications, différents groupes de terminaux sont configurés en fonction de l'application.
- Les applications continuent à utiliser le même sous-réseau IP et sa passerelle.
- Les EPG d'application segmentés pour utiliser un nouveau VLAN.
- 1 BD à configurer avec un sous-réseau IP et mappé à plusieurs EPG d'application.
- 1 BD = N EPG = N VLAN
- Désormais, deux EPG (applications) peuvent communiquer entre eux via le contrat.

Approches de migration

Avant de déployer l'ACI en tant qu'ACI axée sur les applications, l'ACI peut être déployée en tant qu'ACI axée sur le réseau et, en outre, les applications peuvent être segmentées.

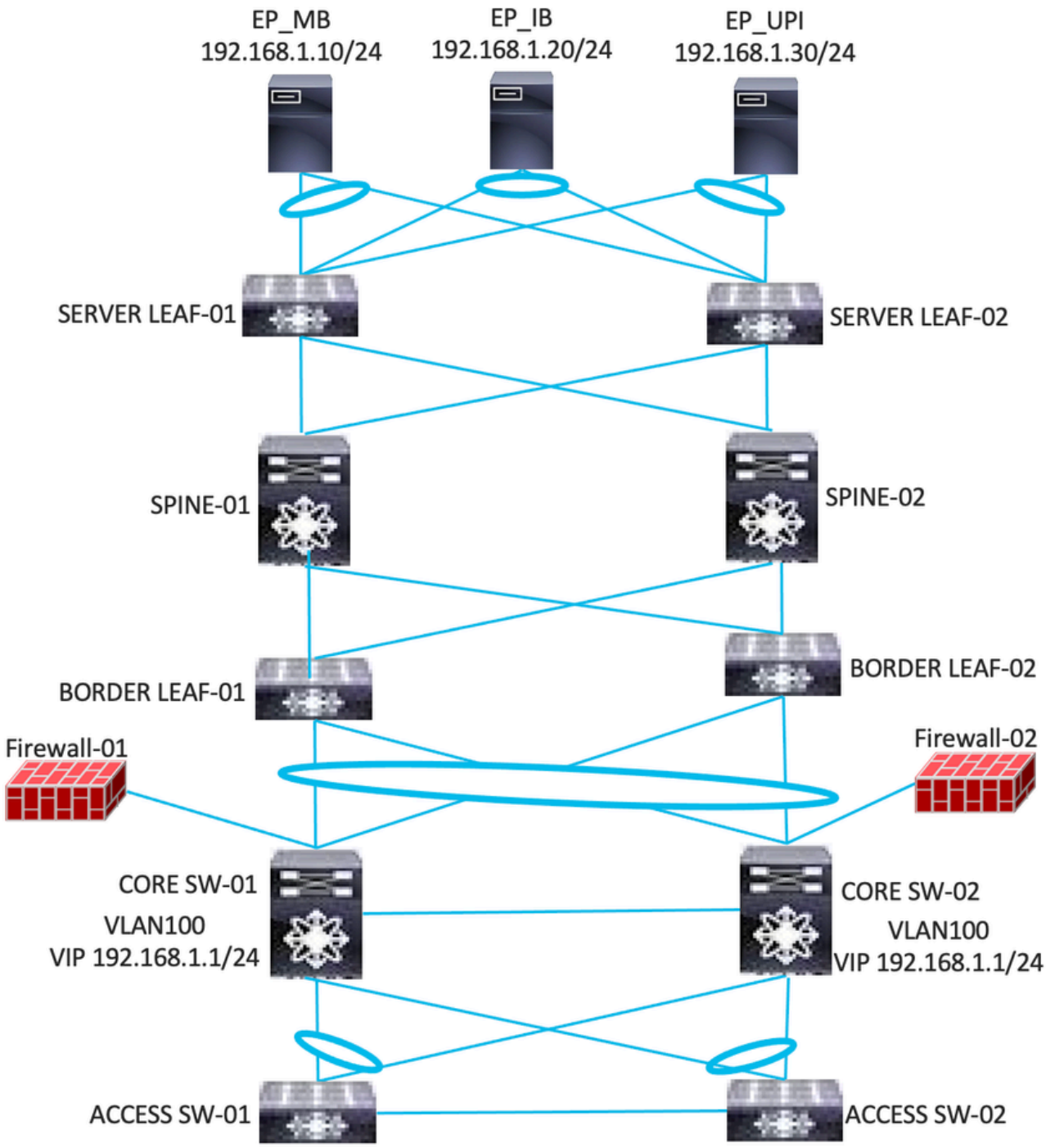
Approche de la migration axée sur le réseau : Phase 1



- Une liaison intermédiaire de couche 2 doit être établie entre les commutateurs de périphérie et de coeur de réseau.
- Configurez le domaine de pont de couche 2 et le groupe de terminaux sur l'ACI en fonction des VLAN existants configurés dans les réseaux traditionnels.
- Configurez tous ces VLAN sur la liaison intermédiaire de couche 2 entre les commutateurs de périphérie et de coeur de réseau.
- L'ACI doit apprendre tous les terminaux présents sur les commutateurs principaux.

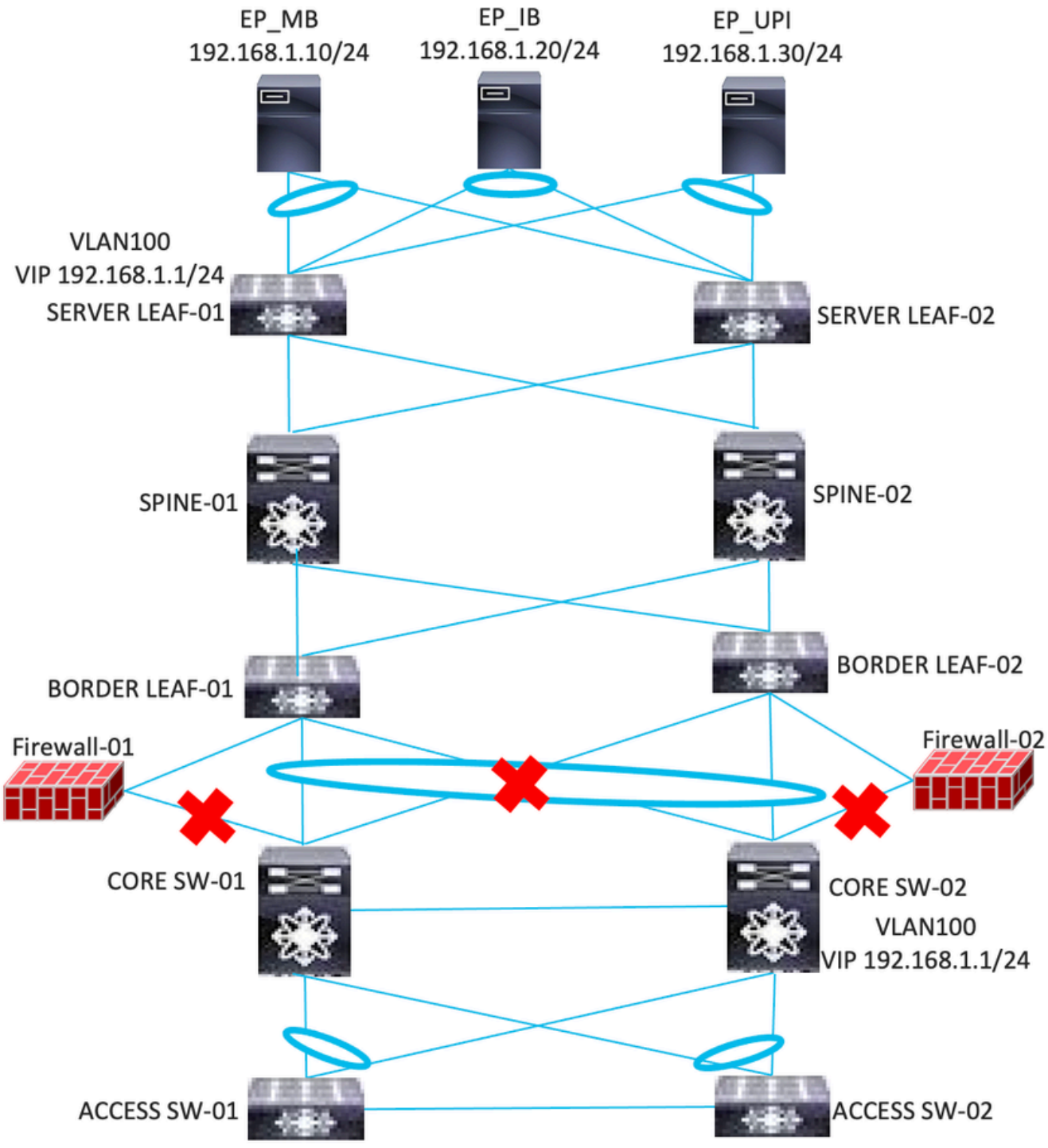
- Le modem routeur reste sur les commutateurs principaux.
- La connectivité du pare-feu reste sur les commutateurs principaux.

Approche de la migration axée sur le réseau : Phase 2



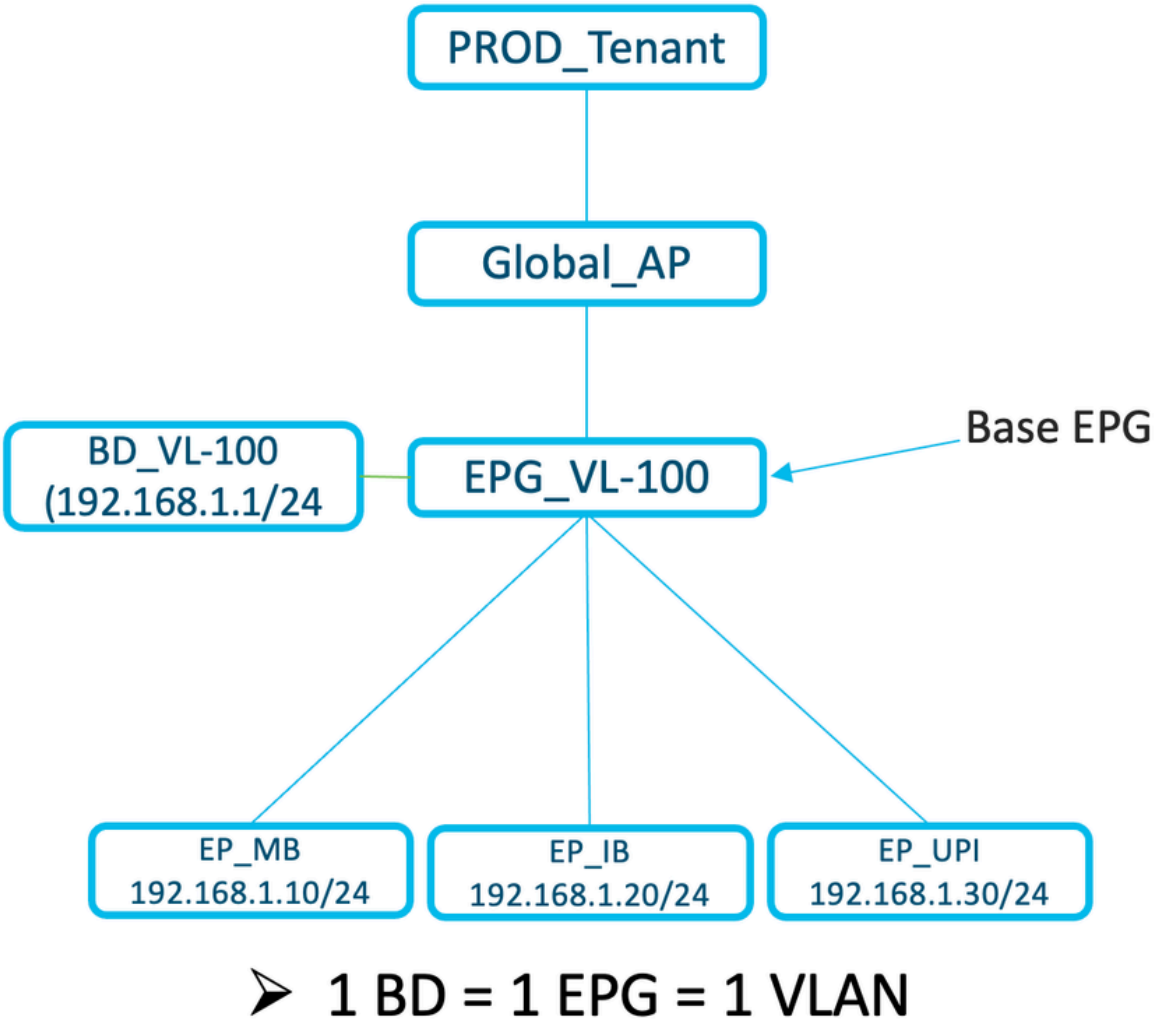
- Transférez les charges de travail des commutateurs d'accès vers les serveurs Leaf.
- La passerelle reste sur les commutateurs principaux.
- Vérifiez que le modem routeur est accessible à partir des serveurs.
- Vérifiez que le serveur/l'application est accessible.

Approche de la migration axée sur le réseau : Phase 3

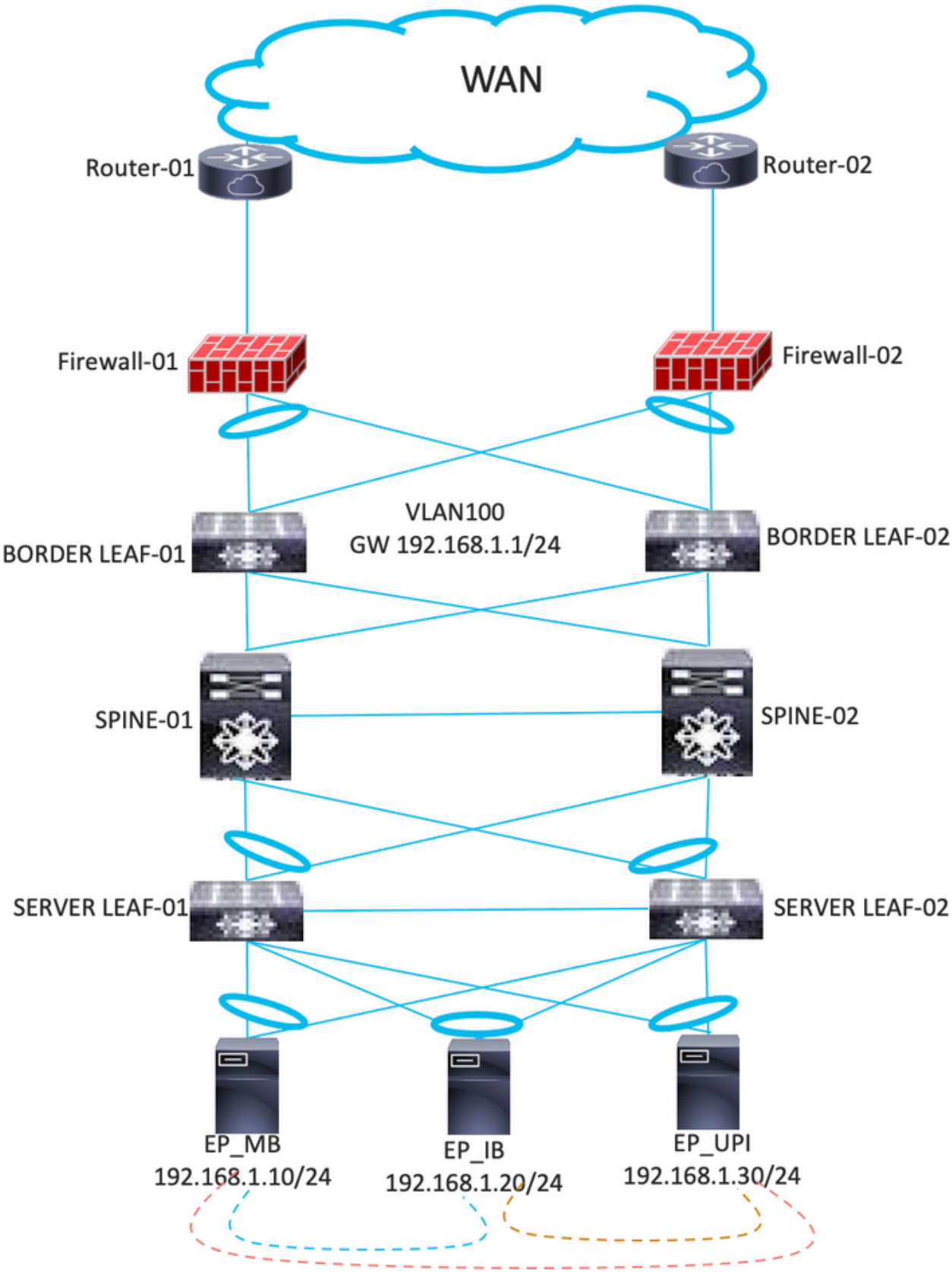


- Fermez les passerelles sur les commutateurs principaux et configurez sur l'ACI.
- Transférez le lien du pare-feu des commutateurs principaux vers le leaf ACI.
- Configurez l'interface L3out vers le pare-feu/routeur.
- Ajoutez les routes dans le pare-feu/routeur et l'ACI Leaf.
- Arrêtez la liaison entre les commutateurs de périphérie et les commutateurs principaux.
- Vérifiez que le serveur/l'application est accessible.

Représentation logique de l'ACI après l'approche de migration axée sur le réseau.



Approche de la migration axée sur les applications : Phase 1



- Collecte et analyse des données CSW/Tetration.
- Nouvelle configuration EPG selon CSW/Tetration Data (WEB, APP et DB).
- Par exemple, pour l'application MB, trois EPG sont créés, tels que EPG_MB_WEB, EPG_MB_APP et EPG_MB_DB. Ces EPG doivent être configurés sous un profil

d'application AP_MB.

- Dans le cas de l'intégration de Virtual Machine Manager (VMM), la configuration vDS est requise pour mapper les serveurs dans le nouvel EPG avec le nouveau VLAN.
- Mappez la machine virtuelle (VM) au nouveau vDS qui est poussé par l'intégration VMM.
- Pour les serveurs sans système d'exploitation, l'équipe du serveur doit modifier l'ID VLAN sur le serveur.
- L’adressage IP doit être identique pour ces déploiements.
- Configuration du contrat entre les groupes de terminaux conformément aux données CSW/Tetration.

Analyse des données CSW/Tetration

Exemple d'analyse basée sur les données CSW/Tetration :

ip_src	scope_consommateur	ip_dst	provider_scop
192.168.34.248	Par défaut:Interne:Siège social	192.168.20.81	PRODAPP
192.168.78.45	Par défaut:Interne:Siège social	192.168.20.81	PRODAPP
192.168.78.16	Par défaut:Interne:Siège social	192.168.20.81	PRODAPP
192.168.78.25	Par défaut:Interne:Siège social	192.168.20.81	PRODAPP
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODAPP
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODAPP
192.168.32.173	Par défaut:Interne:Datacenter:DC:Application:Prod:DMZ	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.48	Par	192.168.20.81	PRODAPP

	défaut:Interne:Datacenter:DC:Application:Prod:Surveillance		
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.48	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.29	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.30	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.81	PRODAPP
192.168.44.21	Par défaut:Interne:Datacenter:DC:Application:Prod:AAA	192.168.20.81	PRODAPP
192.168.103.80	Par défaut:Interne:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.71	Par défaut:Interne:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.20	Par défaut:Interne:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODAPP
192.168.103.21	Par défaut:Interne:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODAPP
192.168.44.68	Par	192.168.20.85	PRODDB

	défaut:Interne:Datacenter:DC:Application:Prod:Discovery		
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
192.168.44.68	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODDB
172.16.32.173	Par défaut:Interne:Datacenter:DC:Application:Prod:MZ	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.48	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.48	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.47	Par	192.168.20.85	PRODDB

	défaut:Interne:Datacenter:DC:Application:Prod:Surveillance		
192.168.44.30	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.29	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB
192.168.44.21	Par défaut:Interne:Datacenter:DC:Application:Prod:Surveillance	192.168.20.85	PRODDB

Exemple de recommandation EPG de la CSW/Tetration :

EPG	IP
PRODAPP	192.168.20.81
RODDB	192.168.20.85

En fonction des détails, les données doivent être analysées pour la configuration du contrat.
Exemple de données analysées :

ip_src	scope_consommateur	consommateur_EPG	dst_IP	fournisseur_EPG	pr
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	DÉCOUVERTE_EPG	192.168.20.81	EPG-PROD-APP	U
192.168.44.69	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	DÉCOUVERTE_EPG	192.168.20.81	EPG-PROD-APP	T
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	T
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	U

192.168.44.48	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.48	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	TC
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.81	EPG-PROD-APP	IC
192.168.103.21	Par défaut : Interne : Datacenter : DC : Application : Prod : DHCP	EPG_VL_157	192.168.20.81	EPG-PROD-APP	TC
192.168.44.68	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	DÉCOUVERTE_EPG	192.168.20.85	EPG-PROD-DB	U
192.168.44.68	Par défaut:Interne:Datacenter:DC:Application:Prod:Discovery	DÉCOUVERTE_EPG	192.168.20.85	EPG-PROD-DB	TC
192.168.44.69	Par défaut : Interne :	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	TC

	Datacenter : DC : Application : Prod : Surveillance				
192.168.44.69	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	U
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	U
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	T
192.168.44.48	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	T
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	T
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	T
192.168.44.48	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	T
192.168.44.47	Par défaut : Interne : Datacenter : DC : Application : Prod : Surveillance	SURVEILLANCE_EPG	192.168.20.85	EPG-PROD-DB	IC
192.168.48.45	Par défaut : Interne : Datacenter : DC : Application : Prod : Sauvegarde	EPG_VL_71	192.168.20.85	EPG-PROD-DB	T

En fonction de l'adresse IP, les groupes de terminaux du consommateur et du fournisseur sont

mentionnés. Les entrées dupliquées et le trafic Nord-Sud (comme le trafic Internet, inter-DC, inter-zones, etc.) doivent être exclus de ces données. Il existe des groupes de terminaux nommés avec des VLAN, tels que EPG_VL_157, EPG_VL_71, etc. Cela signifie que ces serveurs ne sont pas déplacés vers l'EPG cible dans le cadre d'une migration axée sur les applications. Ainsi, le contrat entre eux doit être configuré avec le mappage actuel de l'EPG. Une fois ces serveurs migrés vers l'EPG cible, ces contrats existants doivent être supprimés dans le cadre du processus de nettoyage et le contrat approprié doit être ajouté à l'EPG cible.

Contrat

Les contrats sont requis pour la communication entre les groupes de terminaux. Le flux d'implémentation pendant le processus de configuration du contrat est capturé dans cette section.

1. Au départ, le contrat VzAny doit être appliqué au niveau VRF (Virtual Routing and Forwarding).

2. Selon les données CSW/Tetration, des contrats EPG spécifiques doivent être créés.

3. Configurez la règle Deny_All avec une priorité faible afin que le contrat VzAny n'autorise pas la communication de trafic non spécifié. Pour les applications qui ne sont pas encore migrées en tant qu'applications centrées, la communication s'effectue via VzAny Contract.

4. Après toute la migration, supprimez le contrat VzAny du VRF.

L'analyse des données CSW/Tetration et leur conversion en objets ACI appropriés constituent une étape très importante. Par conséquent, après l'analyse initiale, il est important de discuter de notre observation avec les intéressés et d'obtenir une nouvelle confirmation sur le même. Lors de la mise en oeuvre, il convient également d’examiner attentivement la question afin de s’assurer que tout le trafic est autorisé comme prévu. Pour le dépannage, vous pouvez activer la journalisation sur le contrat et également effectuer le suivi de tout abandon de paquet sur un port spécifique à l'aide d'une interface graphique utilisateur ou d'une interface de ligne de commande.

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: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.22 1, 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: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21.11, DIP: 192.168.22.22 1, SPort : 0, DPort : 0, Src Intf : Tunnel7, Proto : 1, PktLen : 98

contract_parser

Script Python sur le périphérique qui produit une sortie qui corrèle les règles de zonage, les filtres et les statistiques d'accès tout en effectuant des recherches de noms à partir d'ID. Ce script est extrêmement utile dans la mesure où il prend un processus en plusieurs étapes et le transforme en une commande unique qui peut être filtrée en fonction de groupes de terminaux/VRF spécifiques ou d'autres valeurs liées au contrat.

leaf# contract_parser.py
Clé :
[prio:RuleId] [vrf:{str}] protocole d'action src-epg [src-l4] dst-epg [dst-l4] [flags][contrat:{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]

Les abandons de paquets peuvent également être affichés dans l'interface utilisateur graphique en utilisant le chemin : Tenant > Nom_Tenant > Opérationnel > Flux/Paquets.

Considération

Recommandation lors de l'application des contrats entre les groupes de terminaux :

1. L'ACI ne peut pas être considérée comme un pare-feu en termes de mappage de stratégie, ce qui peut entraîner une utilisation élevée de la mémoire TCAM (Ternary Content Addressable Memory).

2. Utilisez une plage de filtres au lieu d'un grand nombre de filtres individuels.

3. Tout contrat ne doit pas utiliser plus de quatre gammes de filtres. Elle peut consommer une quantité importante de mémoire adressable par contenu ternaire (OTCAM).

4. Si des groupes de terminaux nécessitent un grand nombre de ports, essayez d'utiliser un contrat « permit any ».

5. Dans le cadre de la solution, si vous prévoyez le déploiement d'un grand nombre de contrats, envisagez de modifier le profil d'échelle de transfert (FSP) en conséquence.

6. Avant de déployer un nombre important de contrats, calculez le TCAM à l'aide de la formule : Nbre de EPG de fourniture * Nbre d'EPG de consommateur * Nombre de règles.

7. La taille TCAM existante peut être vérifiée sur l'interface utilisateur de l'ACI en utilisant le chemin : Operations > Capacity Dashboard > Leaf Capacity ou

LEAF-101# vsh_lc

module-1# show platform internal hal health-stats | _compte grep

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

Quelques défis du déploiement et de la solution axés sur les applications

1. Un plus grand nombre de contrats peut entraîner une utilisation TCAM élevée des commutateurs Leaf.

Par conséquent, il est important de suivre activement l'utilisation de la TCAM et de préparer une augmentation estimée de la valeur de la TCAM lorsqu'une grande quantité de déploiement de configuration est effectuée. Il est bon d'avoir un processus de vérificateur de machine afin de s'assurer que la configuration poussée est appropriée. En outre, il est recommandé d'effectuer les modifications avec une fenêtre de maintenance planifiée appropriée.

2. La configuration en bloc (plus de 50 000 TCAM) en une seule opération de type push of contract peut entraîner une panne de mémoire de Policy Manager.

Il est recommandé de pousser la configuration en segments plus petits, en particulier lorsque la taille de la configuration est importante. Cela permet d'adopter une approche systématique et sans risque de la configuration des contrats. En outre, à chaque poussée de configuration, mesurez l'augmentation des valeurs TCAM.

3. Le flux de trafic n'est pas capturé si les applications ne communiquent pas pendant l'intervalle de temps de déploiement CSW/Tetration (3 à 4 semaines).

Afin d'éviter une telle situation, la meilleure approche est d'obtenir une nouvelle vérification des données CSW/Tetration auprès des propriétaires de l'application avant l'activité de modification. Après l'implémentation, vérifiez également dans les journaux le nombre d'échecs.

Valeur Ajoutée

1. Toutes les applications ont été segmentées et restreintes conformément aux directives relatives à la banque centrale.

2. Visibilité des communications entre applications après la migration vers un déploiement axé sur les applications.

3. La micro-segmentation de l'application est réalisée.

4. Une vue du flux d'applications. Dans un profil d'application, les EPG sont mappés en fonction du flux de trafic, tel que le profil d'application AP_Banking, afin d'avoir trois EPG (EPG_Banking_WEB, EPG_Banking_APP et EPG_Banking_DB) indépendamment de leur sous-réseau IP.

4. Une vue unique du flux d’applications facilite le dépannage.

5. Infra est plus sûr.

6. Approche structurée pour la mise en oeuvre et l'expansion future.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.