Distribuzione di ACI come applicazione incentrata

Sommario

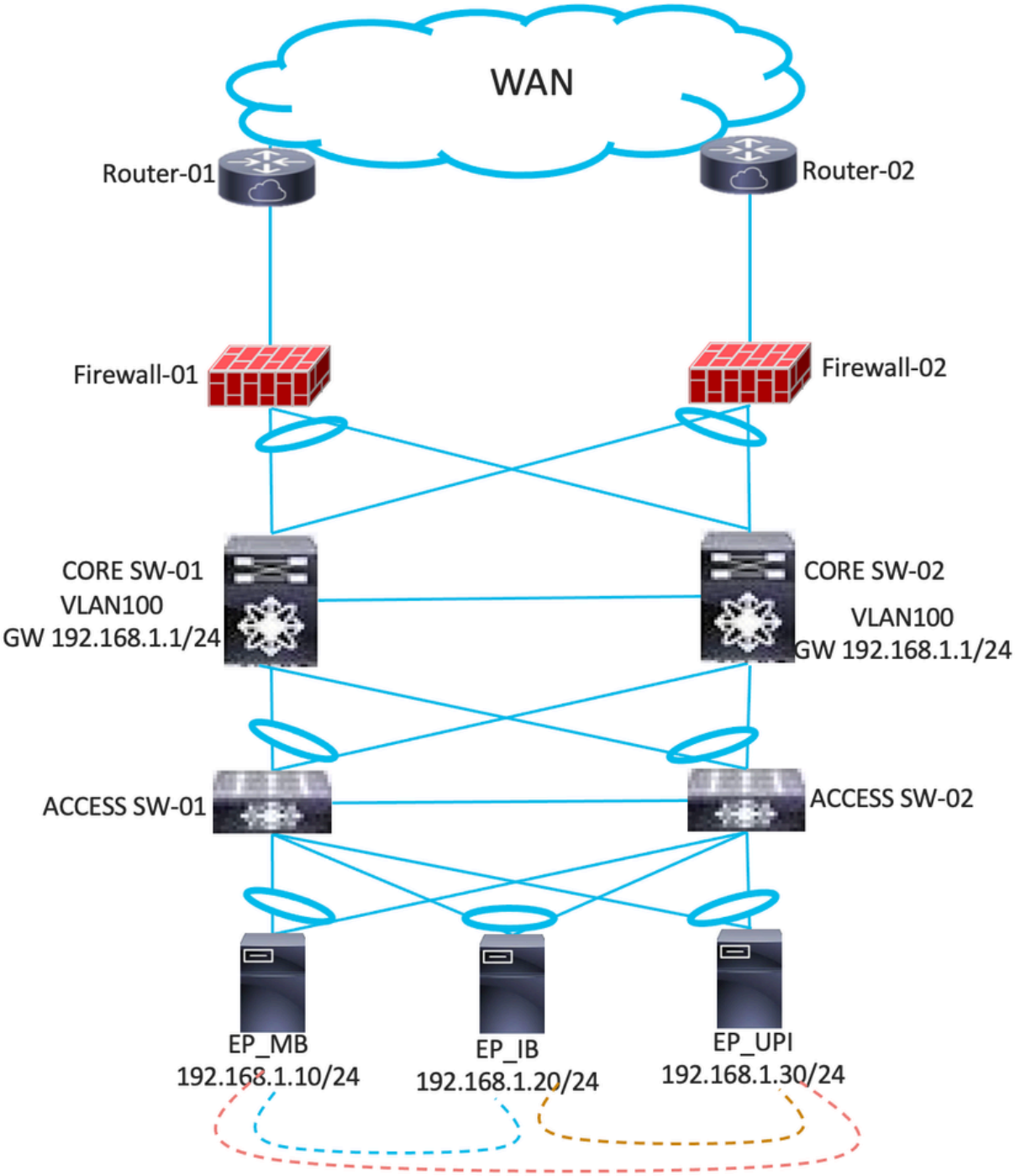
Introduzione

Questo documento descrive l'approccio per raggiungere la micro-segmentazione e la sicurezza all'interno e tra le applicazioni utilizzando la soluzione Cisco ACI SDN.

Vincoli che utilizzano la rete tradizionale

- Nelle reti tradizionali, la segmentazione all'interno di una VLAN/subnet è impossibile.
- I gateway delle applicazioni si trovano sugli switch di base. Se due applicazioni vogliono comunicare, sullo switch principale sono necessari Access Control Lists (ACL) complessi.
- Il loop Spanning-Tree tra gli switch interrompe il flusso del centro dati e genera una perdita di traffico.
- La stessa subnet IP contiene più applicazioni, che non forniscono la protezione tra di esse. La gestione di queste comunicazioni non è possibile sulle reti tradizionali.
- Si consideri un esempio illustrato anche mediante il diagramma. Sono disponibili tre applicazioni: EP_MB, EP_IB e EP_UPI che fanno parte della stessa VLAN e subnet IP. Con

qualsiasi traffico L2, il traffico viene sempre inondato verso tutte le applicazioni, anche se non è richiesta la comunicazione tra di esse. Le restrizioni tra le due applicazioni non sono possibili in questo scenario.



Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Per raccogliere i dati del flusso di traffico tra le applicazioni, è necessario implementare

nell'ambiente Cisco Secure Workload (CSW)/Tetration (Secure Workload).
- Gli agenti devono essere distribuiti sui server per raccogliere i dati. Pertanto, ciò è possibile solo in caso di distribuzione in modalità brownfield.
- Gli agenti devono essere installati sui server per almeno 3-4 settimane per la raccolta dei dati.
- Se non sono disponibili strumenti ADM (Application Dependency Mapping), è necessario fornire i relativi dati.
- Il gateway del server deve essere configurato utilizzando il fabric ACI (Application Centric Infrastructure).

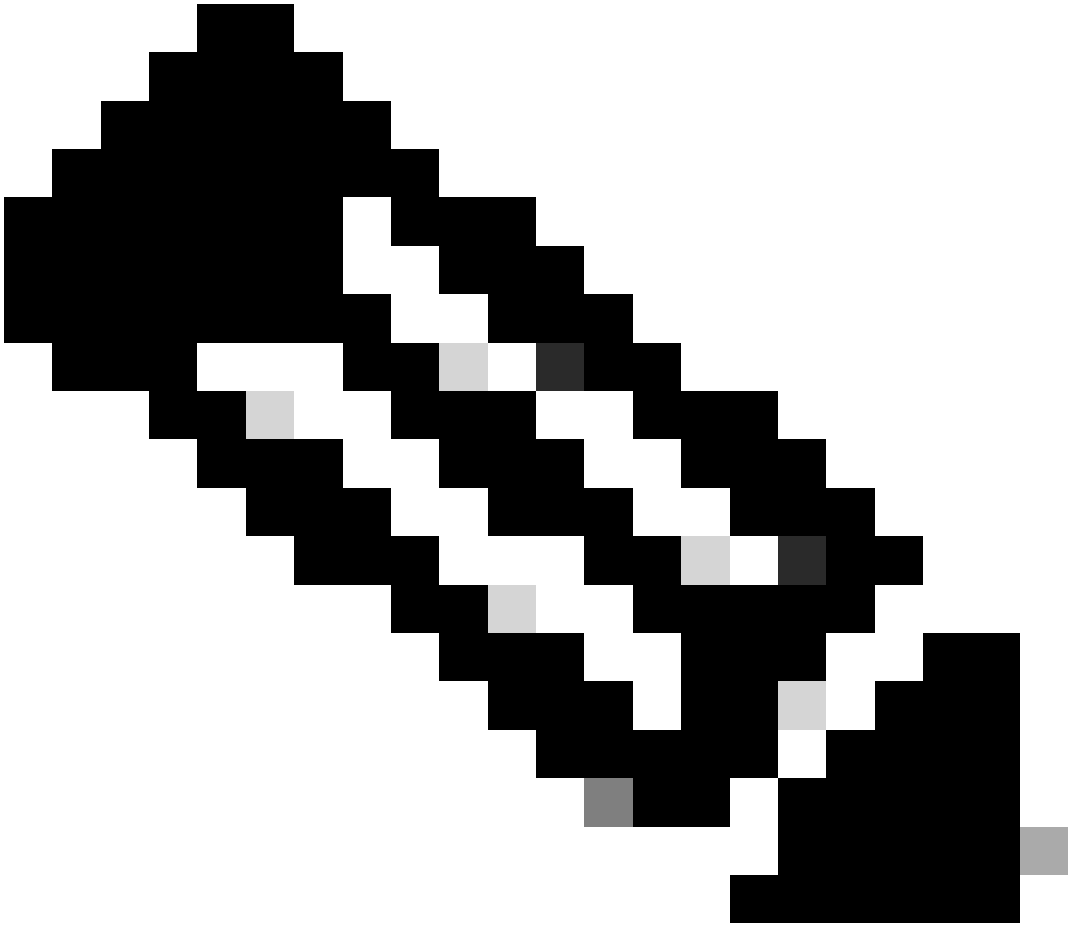
Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica della soluzione

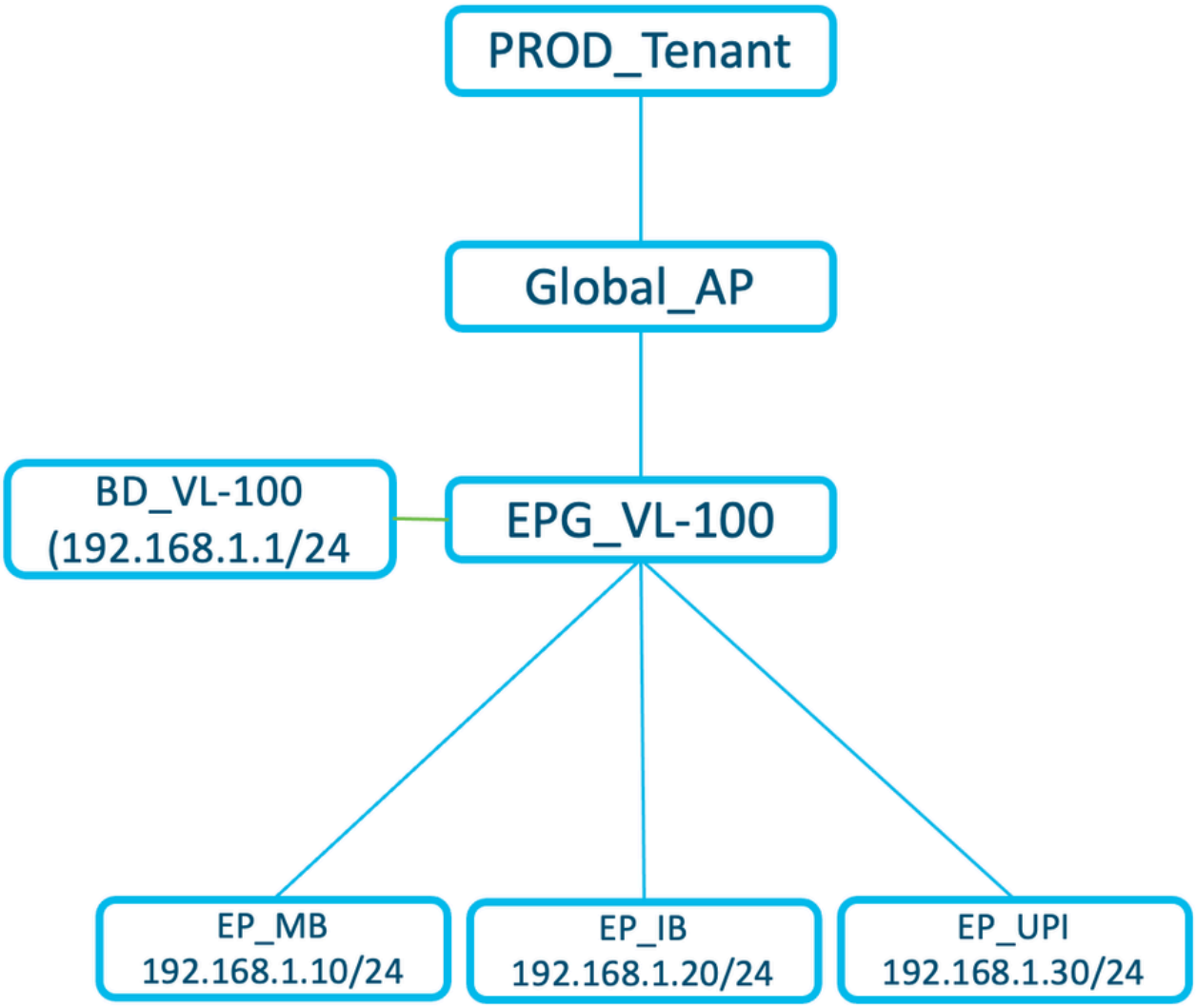
Per ottenere una micro-segmentazione, è necessario innanzitutto migrare la rete a una soluzione SDN Cisco dall'infrastruttura tradizionale e riprogettare la rete da una vista incentrata sull'applicazione. In questa sezione vengono descritte le due fasi di progettazione necessarie per ottenere la segmentazione desiderata in base al flusso dell'applicazione acquisito tramite lo strumento ADM. Inizialmente, la soluzione Cisco ACI viene implementata in modalità Network Centric (così come è con la progettazione esistente) e quindi spostata verso la modalità application-centric.



Nota: è inoltre possibile combinare questa modalità di distribuzione per eseguire la migrazione diretta dei servizi dalla rete tradizionale alla modalità incentrata sull'applicazione.

Progettazione incentrata sulla rete

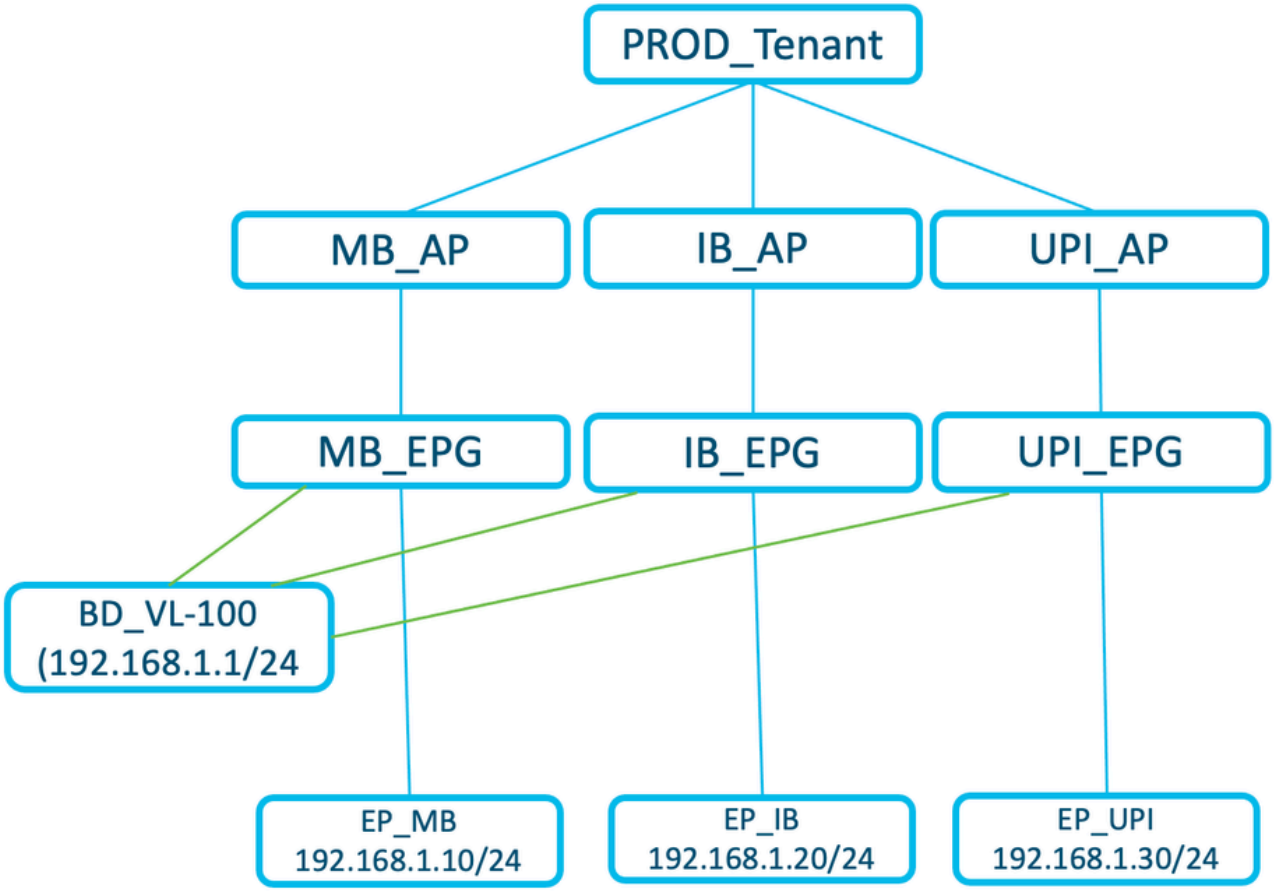
Nell'esempio mostrato nel diagramma, EPG_VL-100 contiene tre applicazioni, EP_MB, EP_IB e EP_UPI, condivide la stessa subnet IP e utilizza VLAN 100.



- Migrazione As-Is dalla rete tradizionale ad ACI.
- Un gruppo di endpoint (EPG) può contenere più applicazioni.
- Nessuna segmentazione delle applicazioni all'interno dello stesso EPG in questo tipo di distribuzione.
- 1 BD = 1 EPG = 1 VLAN

Progettazione incentrata sull'applicazione

L'esempio mostrato nel diagramma è un EPG separato per tre applicazioni: EP_MB, EP_IB e EP_UPI che condividono la stessa subnet IP e utilizzano VLAN diverse mappate a ciascun EPG.

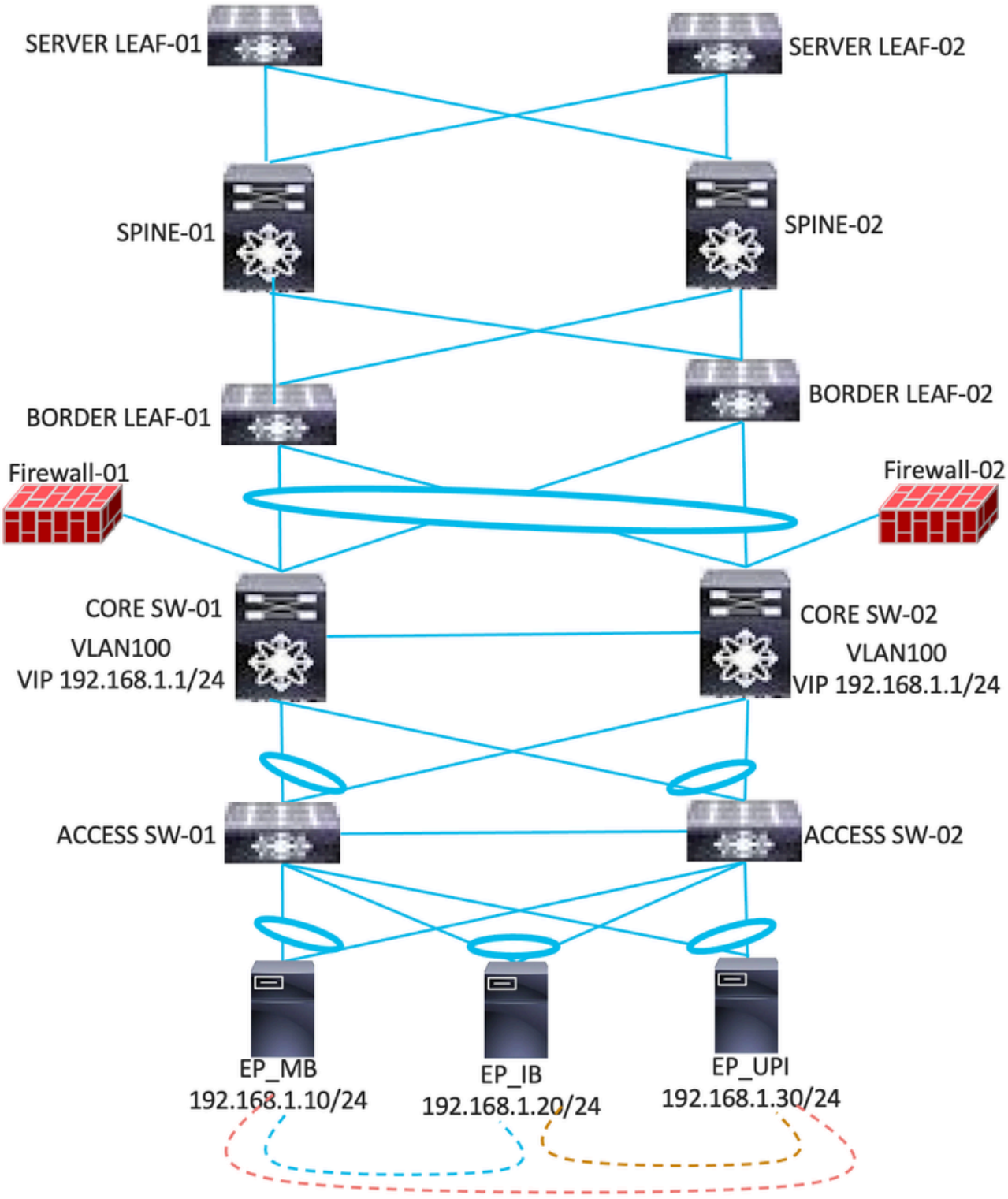


- Nel tipo di distribuzione incentrata sull'applicazione, vengono configurati diversi EPG in base all'applicazione.
- Le applicazioni continuano a utilizzare la stessa subnet IP e il relativo gateway.
- Gli EPG delle applicazioni segmentate per usare una nuova VLAN.
- 1 BD da configurare con subnet IP e mappare su più EPG dell'applicazione.
- 1 BD = N EPG = N VLAN
- Ora due EPG (applicazioni) possono comunicare tra loro tramite contratto.

Approcci alla migrazione

Prima di distribuire ACI come applicazione-centrico, ACI può essere distribuito come rete-centrico e ulteriormente, le applicazioni possono essere segmentate.

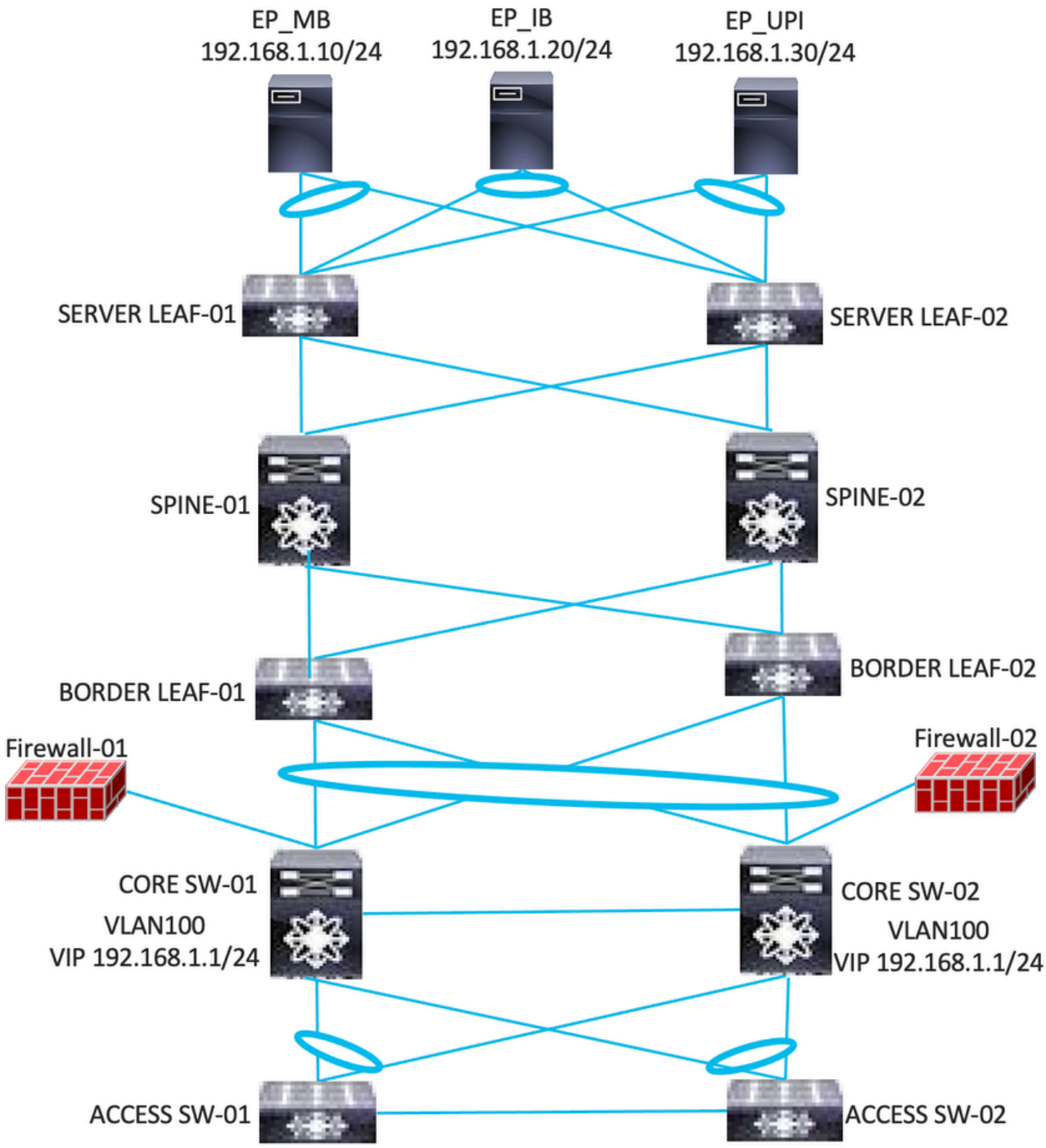
Approccio alla migrazione incentrata sulla rete: fase 1



- È necessario stabilire un collegamento temporaneo di layer 2 tra Border Leaf e Core Switch.
- Configurare il gruppo di domini e di endpoint con bridging di layer 2 sull'ACI in base alle VLAN esistenti configurate nelle reti tradizionali.
- Configurare tutte queste VLAN sul collegamento provvisorio di layer 2 tra gli switch Border Leaf e Core.
- ACI deve apprendere tutti gli endpoint presenti sugli switch core.
- Il gateway rimane sugli switch core.

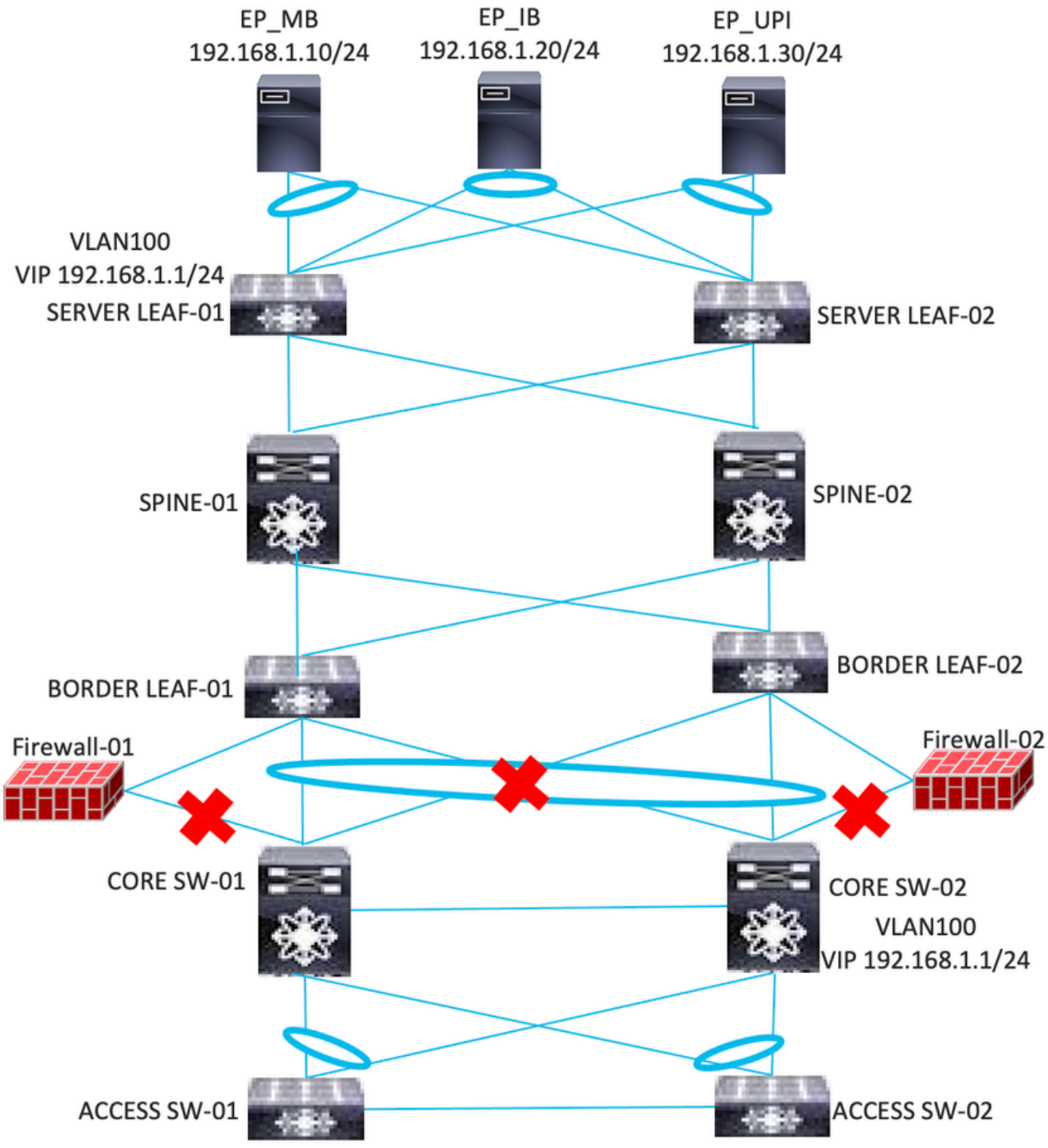
- La connettività del firewall rimane sugli switch core.

Approccio alla migrazione incentrata sulla rete: fase 2



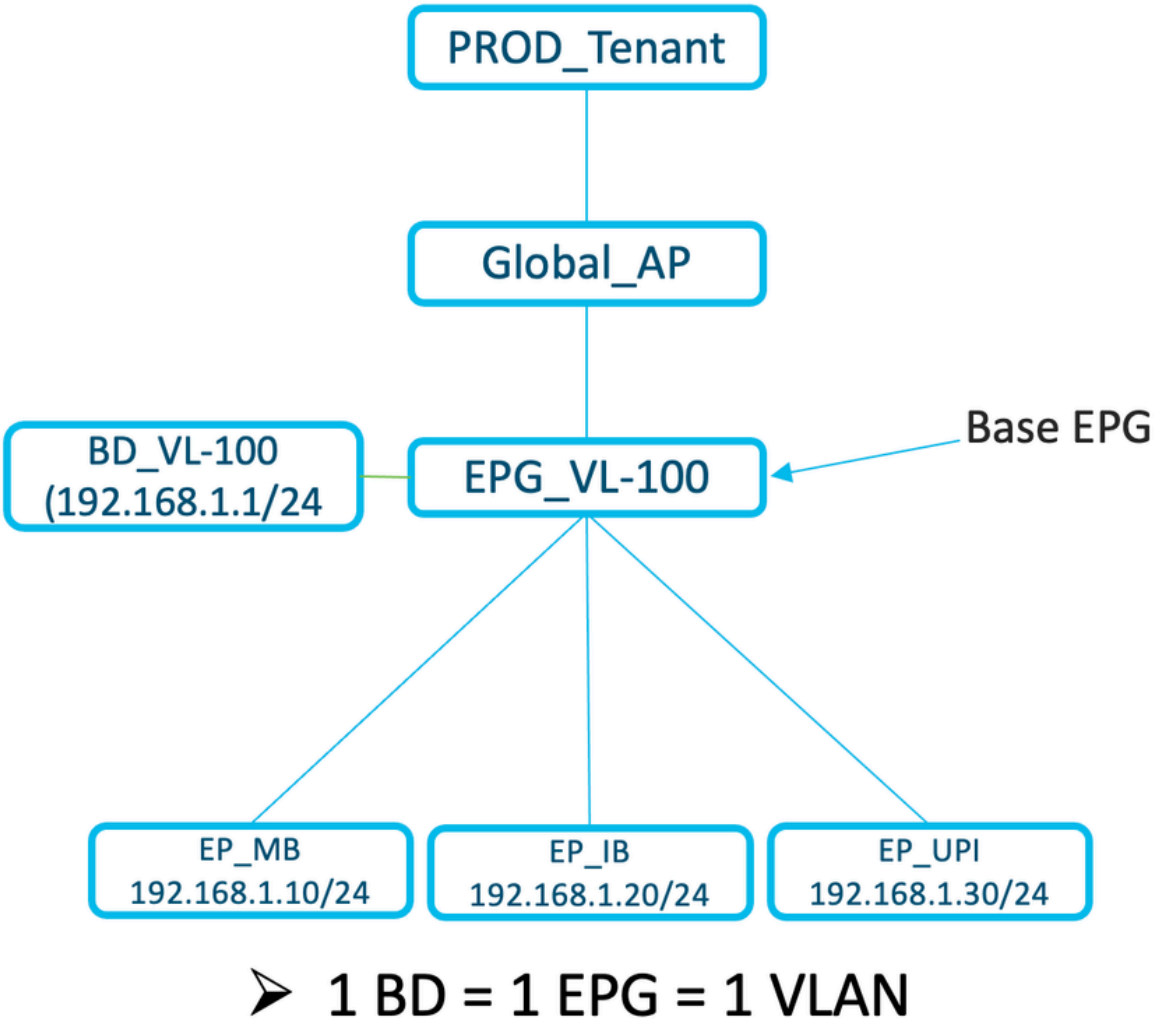
- Spostare i carichi di lavoro dagli switch di accesso alla foglia del server.
- Il gateway rimane sugli switch core.
- Verificare che il gateway sia raggiungibile dai server.
- Verificare che il server o l'applicazione sia raggiungibile.

Approccio alla migrazione incentrata sulla rete: fase 3

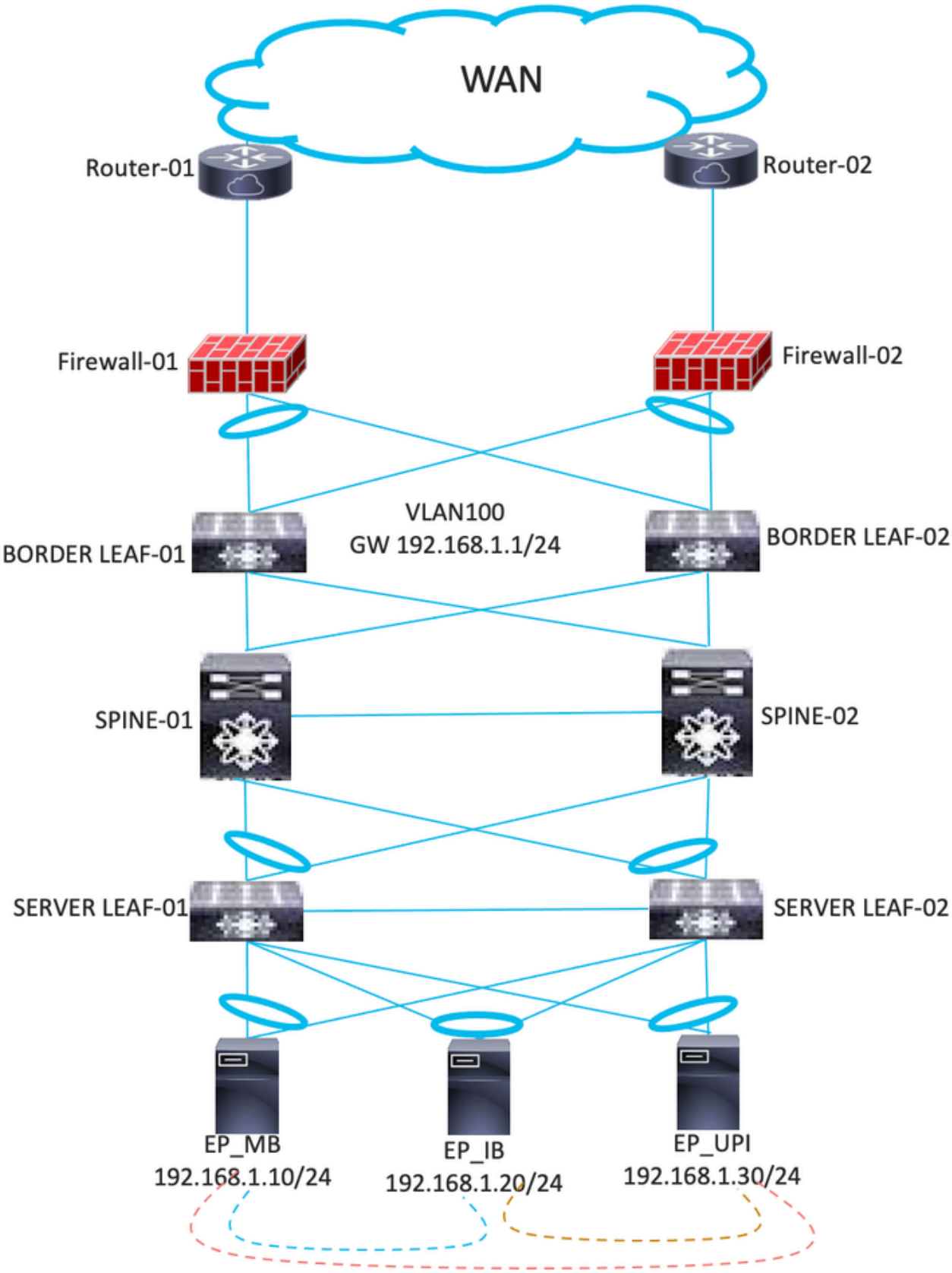


- Spegnere i gateway sugli switch core e configurare su ACI.
- Spostare il collegamento al firewall dagli switch principali a ACI Leaf.
- Configurare l'uscita L3 verso il firewall/router.
- Aggiungere le route nel firewall/router e nella foglia ACI.
- Chiudere il collegamento tra Border Leaf e Core Switch.
- Verificare che il server o l'applicazione sia raggiungibile.

Rappresentazione logica di ACI dopo l'approccio alla migrazione incentrata sulla rete.



Approccio alla migrazione incentrata sull'applicazione: fase 1



- Raccolta e analisi dei dati CSW/Tetration.
- Nuova configurazione EPG in base ai dati CSW/Tetration (WEB, APP e DB).
- Ad esempio, per l'applicazione MB, vengono creati tre EPG come EPG_MB_WEB, EPG_MB_APP e EPG_MB_DB. Questi EPG devono essere configurati in un profilo

applicazione AP_MB.

- In caso di integrazione di Virtual Machine Manager (VMM), è necessaria la configurazione vDS per il mapping dei server nel nuovo EPG con la nuova VLAN.
- Eseguire il mapping della macchina virtuale (VM) al nuovo vDS sottoposto a push tramite l'integrazione VMM.
- Per i baremetal, il team del server deve modificare l'ID VLAN sul server.
- L'indirizzo IP deve essere lo stesso per queste implementazioni.
- Configurazione del contratto tra EPG in base ai dati CSW/Tetration.

Analisi dei dati CSW/Tetration

Esempio di analisi basata sui dati CSW/Tetration:

ip_origine	ambito_consumer	dst_ip	ambito_
192.168.34.248	Predefinito:Interno:Sede centrale	192.168.20.81	PRODA
192.168.78.45	Predefinito:Interno:Sede centrale	192.168.20.81	PRODA
192.168.78.16	Predefinito:Interno:Sede centrale	192.168.20.81	PRODA
192.168.78.25	Predefinito:Interno:Sede centrale	192.168.20.81	PRODA
192.168.44.69	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODA
192.168.44.69	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.81	PRODA
192.168.32.173	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:DMZ	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.48	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA

192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.48	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.29	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.30	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.81	PRODA
192.168.44.21	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:AAA	192.168.20.81	PRODA
192.168.103.80	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODA
192.168.103.71	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODA
192.168.103.20	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODA
192.168.103.21	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:DHCP	192.168.20.81	PRODA
192.168.44.68	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODD
192.168.44.69	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODD
192.168.44.68	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODD

192.168.44.69	Impostazione predefinita:Internal:Datacenter:DC:Application:Prod:Discovery	192.168.20.85	PRODI
172.16.32.173	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:MZ	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.48	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.48	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.47	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.30	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.29	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI
192.168.44.21	Predefinito:Interno:Datacenter:DC:Applicazione:Prod:Monitoraggio	192.168.20.85	PRODI

Esempio di raccomandazione EPG da CSW/Tetration:

EPG	IP
PRODAPP	192.168.20.81

RODDB	192.168.20.85

In base ai dettagli, i dati devono essere analizzati per la configurazione del contratto. Esempio di dati analizzati:

ip_origine	ambito_consumer	EPG_consumer	dst	provider_EP
192.168.44.69	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Individuazione	INDIVIDUAZIONE_EPG	192.168.20.81	EPG-PROD APP
192.168.44.69	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Individuazione	INDIVIDUAZIONE_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.48	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.48	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD APP
192.168.44.47	Predefinito:Interno:Datacenter:	MONITORAGGIO_EPG	192.168.20.81	EPG-PROD

	DC:Applicazione:Prod:Monitoraggio			APP
192.168.103.21	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:DHCP	EPG_VL_157	192.168.20.81	EPG-PROD APP
192.168.44.68	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Individuazione	INDIVIDUAZIONE_EPG	192.168.20.85	EPG-PROD DB
192.168.44.68	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Individuazione	INDIVIDUAZIONE_EPG	192.168.20.85	EPG-PROD DB
192.168.44.69	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.69	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.48	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.48	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB
192.168.44.47	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Monitoraggio	MONITORAGGIO_EPG	192.168.20.85	EPG-PROD DB

192.168.48.45	Predefinito:Interno:Datacenter: DC:Applicazione:Prod:Backup	EPG_VL_71	192.168.20.85	EPG-PROD DB

In base all'indirizzo IP, vengono menzionati gli EPG del consumer e del provider. Le voci duplicate e il traffico Nord-Sud (ad esempio Internet, traffico tra controller di dominio, traffico tra zone e così via) devono essere esclusi da questi dati. Alcuni EPG vengono denominati con VLAN, ad esempio EPG_VL_157, EPG_VL_71 e così via. Ciò significa che questi server non vengono spostati nell'EPG di destinazione come parte della migrazione incentrata sull'applicazione. Quindi, il contratto tra di loro deve essere configurato con l'attuale mappatura di EPG. Una volta eseguita la migrazione di questi server a EPG target, i contratti esistenti devono essere eliminati come parte del processo di pulizia e il contratto appropriato deve essere aggiunto a EPG target.

Contratto

I contratti sono necessari per la comunicazione tra gli EPG. In questa sezione viene illustrato il flusso di implementazione durante il processo di configurazione del contratto.

1. Inizialmente, il contratto VzAny deve essere applicato al livello VRF (Virtual Routing and Forwarding).

2. In base ai dati di CSW/Tetration, devono essere creati contratti EPG specifici.

3. Configurare la regola Deny_All con priorità bassa in modo che il contratto VzAny non consenta comunicazioni del traffico non specificate. Per le applicazioni non ancora migrate come basate sulle applicazioni, la comunicazione avviene tramite il contratto VzAny.

4. Dopo tutta la migrazione, eliminare il contratto VzAny dal VRF.

L'analisi dei dati CSW/Tetration e la loro conversione in oggetti ACI appropriati è un passo molto critico. Quindi, dopo l'analisi iniziale, è importante discutere la nostra osservazione con gli interessati e ottenere una riconferma sullo stesso. Anche durante l'implementazione, è necessario prestare particolare attenzione per garantire che tutto il traffico sia autorizzato come previsto. Per la risoluzione dei problemi, è possibile abilitare la registrazione sul contratto e anche il rilevamento di qualsiasi perdita di pacchetto su una porta specifica usando un'interfaccia GUI o una CLI.

foglia# show logging ip access-list internal packet-log deny
[Mar 1 ott 10:34:37 2019 377572 usec]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: sconosciuto, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21 1, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98
[Mar 1 ott 10:34:36 2019 377731 usec]: CName: Prod1:VRF1(VXLAN: 2654209), VlanType: sconosciuto, Vlan-Id: 0, SMac: 0x000c0c0c0c0c, DMac:0x000c0c0c0c0c, SIP: 192.168.21 1, DIP: 192.168.22.11, SPort: 0, DPort: 0, Src Intf: Tunnel7, Proto: 1, PktLen: 98

parser_contratto

Script Python sul dispositivo che genera un output che mette in correlazione le regole di zoning, i

filtri e le statistiche di accesso durante l'esecuzione di ricerche di nomi da ID. Questo script è estremamente utile in quanto prende un processo a più fasi e lo trasforma in un singolo comando che può essere filtrato in base a EPG/VRF specifici o ad altri valori correlati al contratto.

foglia# parser_contratto.py
Chiave:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [flag][contratto:{str}] [hit=count]

[7:4131] [vrf:common:default] permette 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] permette 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] consente qualsiasi epg:any tn-Prod1/bd-Services(32789) [contract:implicit] [hit=0]

I pacchetti scartati possono essere mostrati anche nella GUI usando il percorso: Tenant > Nome_Tenant > Operativo > Flussi/Pacchetti.

Considerazioni

Raccomandazione nell'applicare i contratti tra EPG:

1. ACI non può essere considerato un firewall in termini di mappatura delle policy che può causare l'utilizzo di TCAM (Content Addressable Memory) ad alto livello.

2. Utilizzare un intervallo di filtri anziché un numero elevato di singoli filtri.

3. I contratti non devono utilizzare più di quattro intervalli di filtri. Può consumare elevata capacità di overflow della memoria indirizzabile del contenuto ternario (OTCAM).

4. Se un EPG richiede un numero elevato di porte, provare a utilizzare un contratto "allow any" (permette qualsiasi).

5. Come parte della soluzione, se si prevede la distribuzione di un numero elevato di contratti, valutare l'opportunità di modificare di conseguenza il profilo della scala di inoltro (FSP).

6. Prima di distribuire un numero di contratti in blocco, calcolare il TCAM utilizzando la formula: N. di Fornisci EPG * N. di EPG consumer * Numero di regole.

7. La dimensione TCAM esistente può essere verificata sull'interfaccia utente ACI utilizzando il percorso: Operazioni > Dashboard capacità > Capacità foglia o

LEAF-101# vsh_lc

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

conteggio_mcast : 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

Alcune sfide dell'installazione e della soluzione incentrata sull'applicazione

1. Un maggior numero di contratti può comportare un elevato utilizzo TCAM di switch foglia.

Pertanto, è importante tenere traccia in modo attivo dell'utilizzo di TCAM e preparare un aumento stimato del valore di TCAM quando viene eseguita una grande quantità di installazione della configurazione. È consigliabile utilizzare un processo di controllo del produttore per garantire che la configurazione sottoposta a push sia appropriata. Inoltre, si consiglia di apportare le modifiche con un'adeguata finestra di manutenzione pianificata.

2. La configurazione di massa (oltre 50.000 TCAM) in un singolo push di contratto può causare un crash della memoria di Policy Manager.

Si consiglia di eseguire il push della configurazione in blocchi più piccoli, in particolare quando la configurazione è di grandi dimensioni. Ciò fornisce un approccio sistematico e privo di rischi alla configurazione del contratto. Inoltre, a ogni pressione della configurazione, misurare l'aumento dei valori TCAM.

3. Il flusso del traffico non viene acquisito se le applicazioni non comunicano durante l'intervallo di tempo di installazione di CSW/Tetration (3-4 settimane).

Per evitare una situazione di questo tipo, l'approccio migliore consiste nel verificare nuovamente i dati CSW/Tetration dai proprietari dell'applicazione prima di eseguire l'attività di modifica. Inoltre, dopo l'implementazione, verificare i log per individuare eventuali riscontri di errore.

Incremento valore

1. Tutte le domande sono state segmentate e limitate in base agli orientamenti per le banche centrali.

2. Visibilità della comunicazione tra applicazioni dopo la migrazione alla distribuzione incentrata

sulle applicazioni.

3. L'applicazione è sottoposta a microsegmentazione.

4. Una vista del flusso dell'applicazione. In un profilo applicazione, gli EPG vengono mappati in base al flusso di traffico, ad esempio il profilo applicazione AP_Banking, in modo da avere tre EPG (EPG_Banking_WEB, EPG_Banking_APP e EPG_Banking_DB) indipendentemente dalla subnet IP.

4. Una vista del flusso dell'applicazione semplifica la risoluzione dei problemi.

5. L'infrastruttura è più sicura.

6. Approccio strutturato per l'attuazione e la futura espansione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).