CISCO

You make **possible**

End-2-end policy from the Campus to the DC and back, a packet journey with SDA to ACI

Ramses Smeyers – Principal Engineer, CX

BRKOPS-2110

Barcelona | January 27-31, 2020

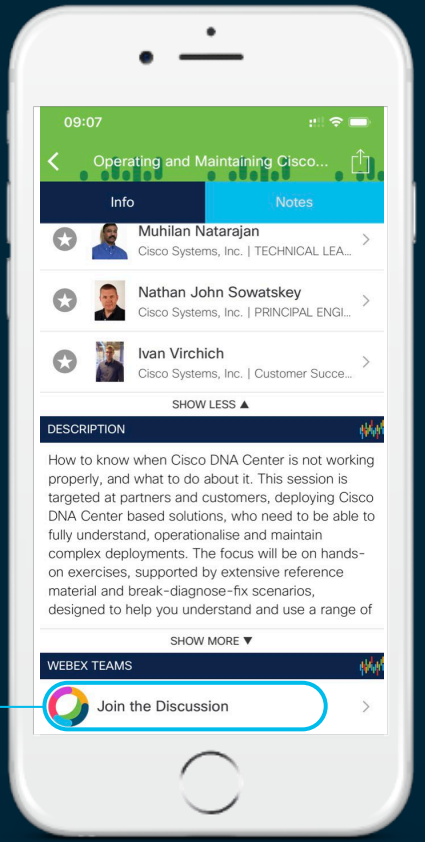
Cisco Webex Teams

Questions?

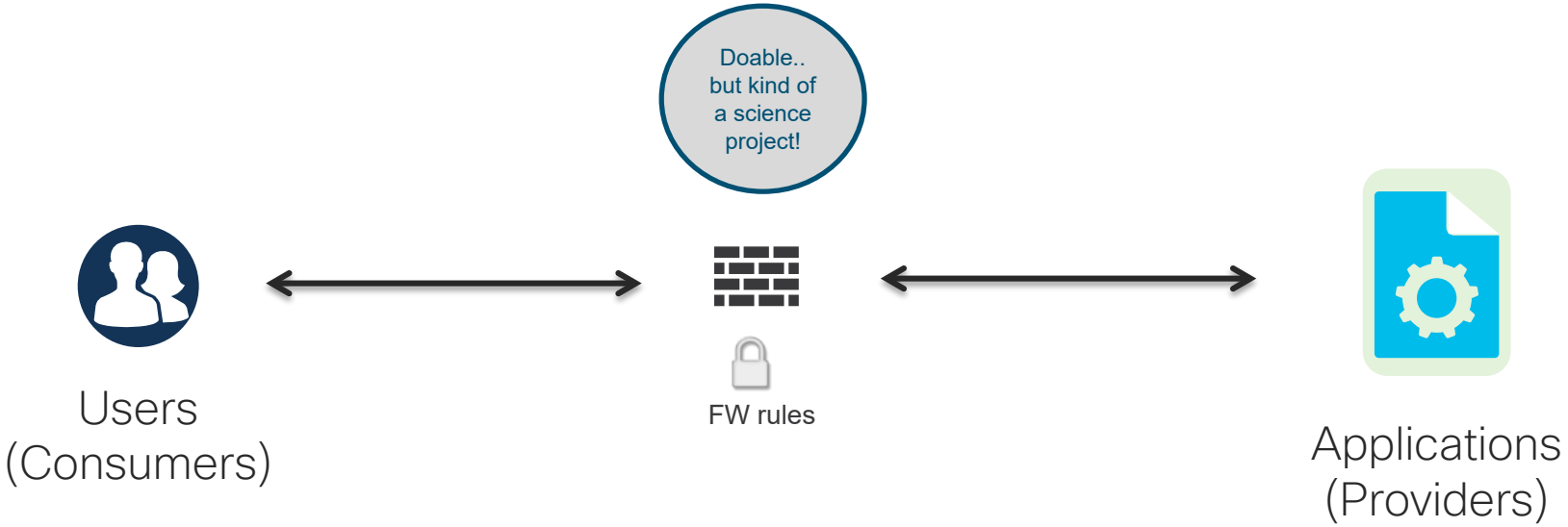
Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Why do we Build Networks?



Agenda

- ACI / SDA integration today
- A day in the life of a packet
- Demo
- ACI / SDA integration, the future

ACI / SDA integration today

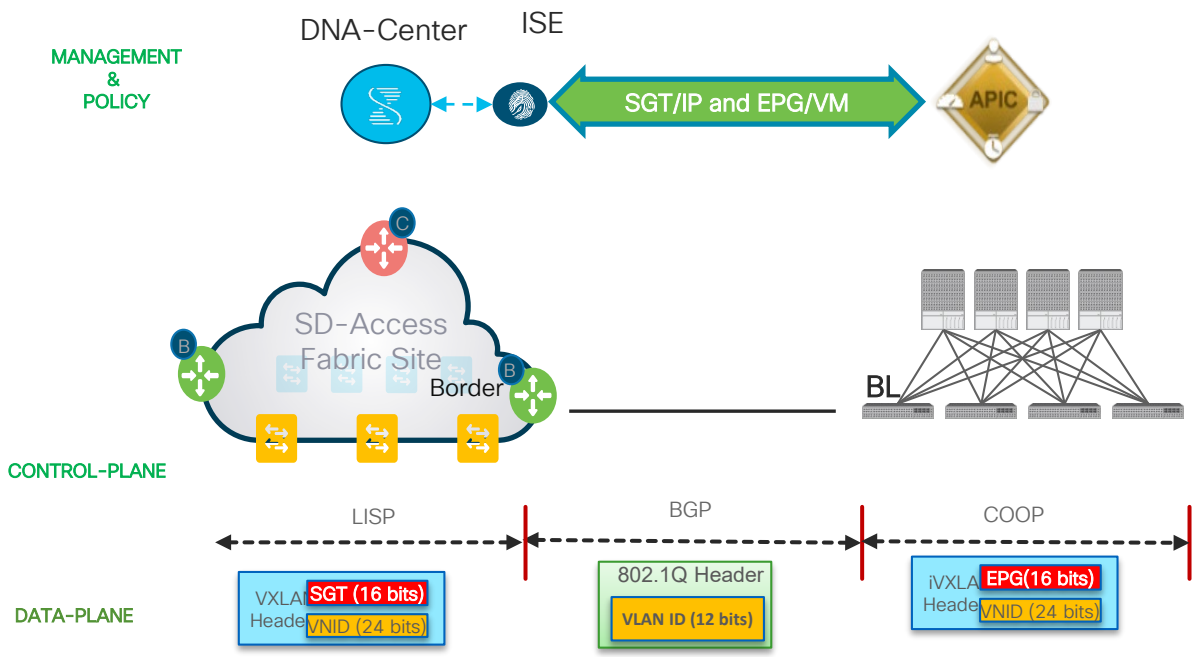
Good News

SD-Access and ACI Fabric Similarities

SD-Access Fabric	ACI Fabric
• Underlay	• Underlay
• Overlay	• Overlay
• Logical constructs	• Logical constructs
• Virtual Network	• VRF
• SGT	• EPG
• User Endpoint	• App Endpoint
• Group Based Access Control	• Contract

ACI and SDA Pairwise Integration

SDA-ACI: Group/Identity Mapping

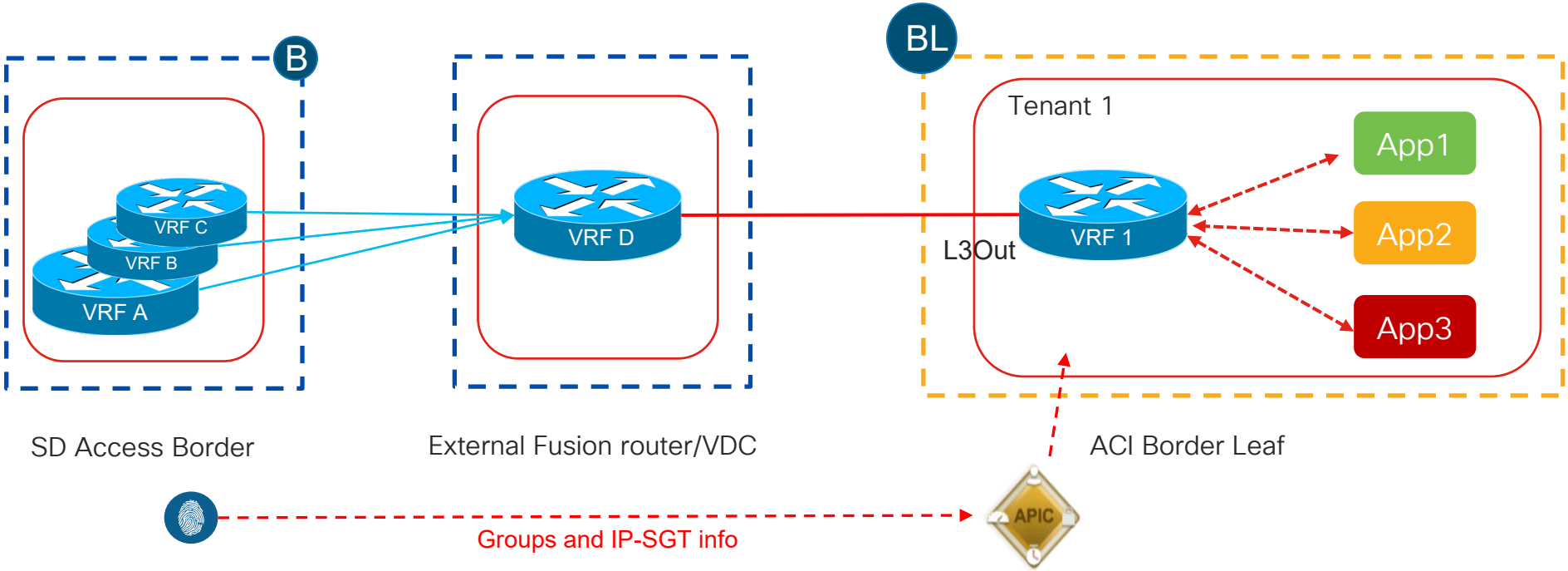


SGT -> External EPG	250
Number of Mappings	64k
Mappings per External EPG	8k
Transaction rate (target)	100/s

a) IP Data path
b) Exchange of SGT and EPG at the control plane layer
c) IP-SGT/EPG bindings in both directions

SDA-ACI

Current Solution: Single VRF, Single Tenant

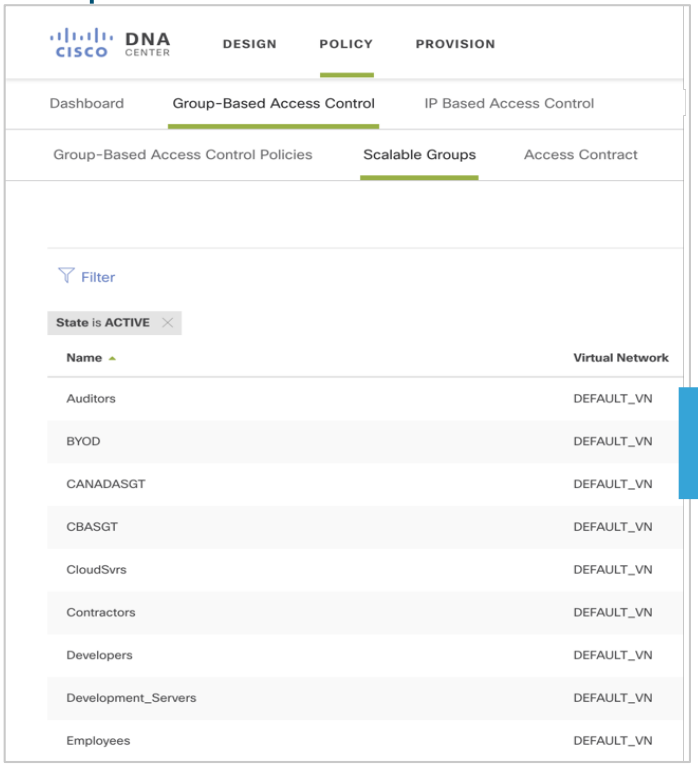


Note: Shared L3Out on ACI BL nodes currently not supported

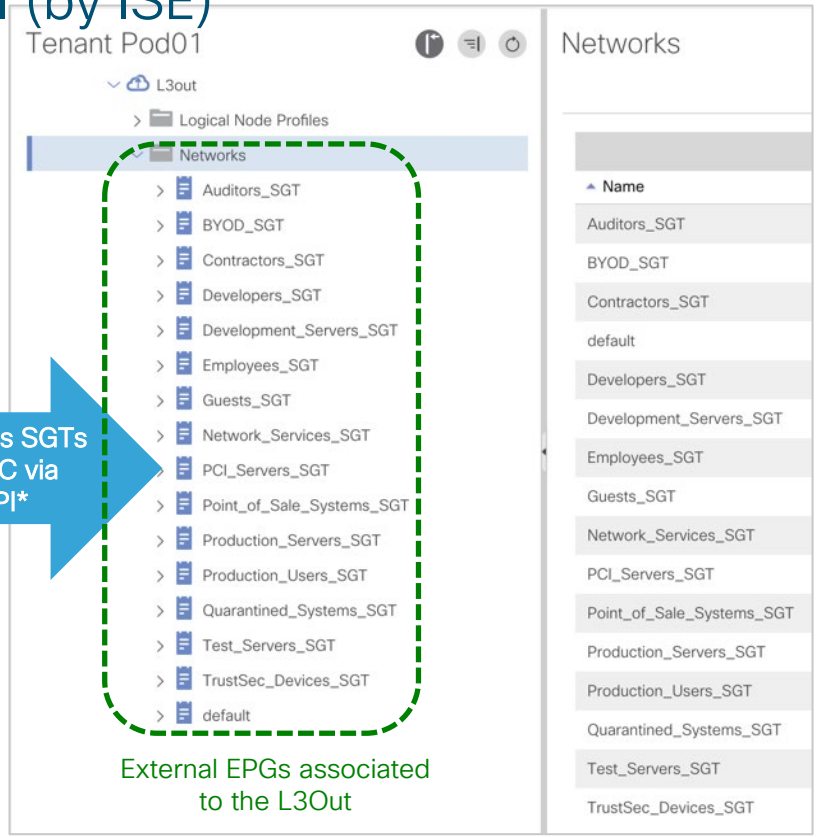
Where will the Policy Be applied?

Policy Enforcement on the Application Domain

Groups Provisioned from SDA to ACI (by ISE)



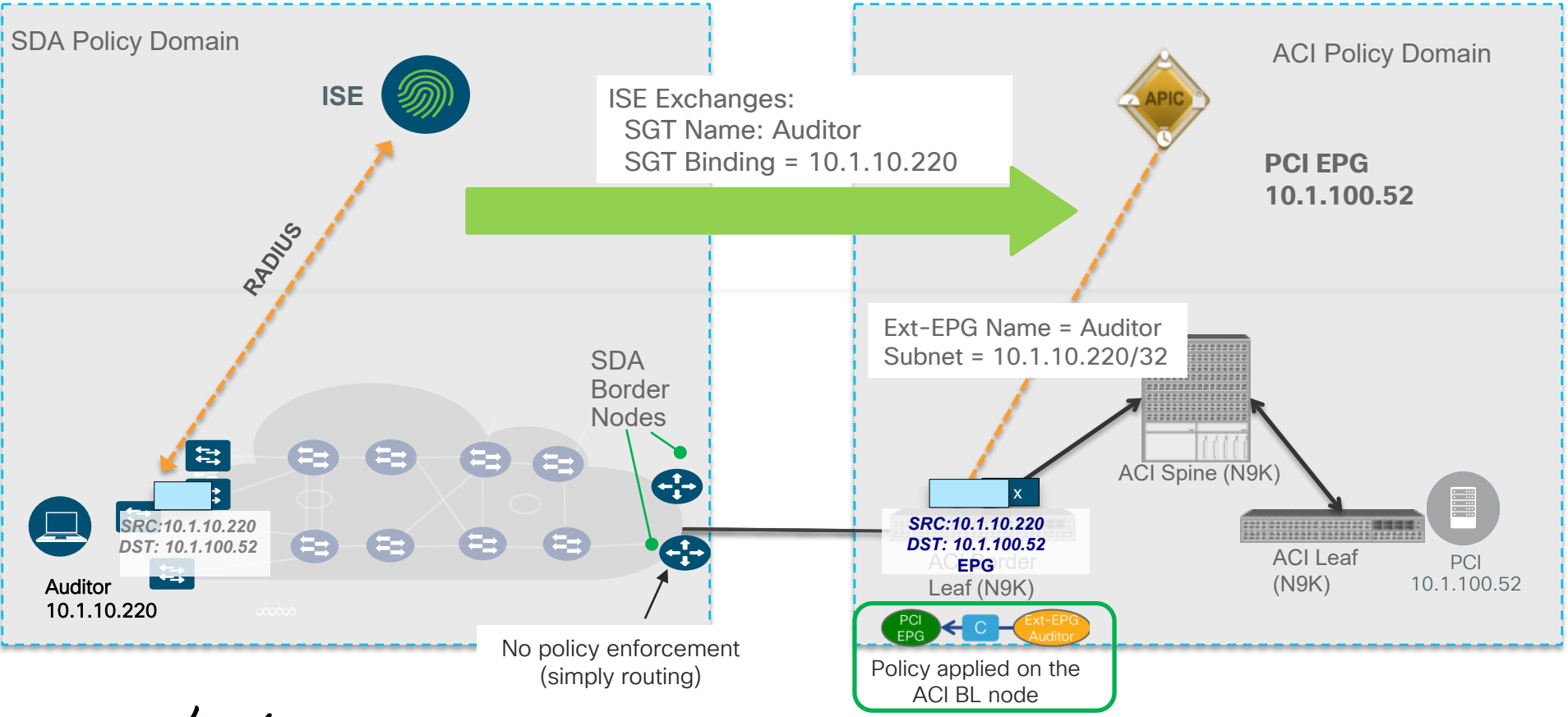
ISE provisions SGTs info to APIC via REST API*



* Provisioning of SGTs to APIC can be controlled at the SGT level

Policy Enforcement on the Application Domain

Applying Policy on the ACI BL Nodes



Policy Enforcement on the Application Domain
Enforcement Scale in ACI

	EX	FX	FX2
SGT⇔External EPG	250	250	250
SGT IPv4 Mapping (/32)	64k	64k	64k
SGT IPv6 Mapping (/128)	24k	48k	24k
SGT IPv4+IPv6 Mapping (Dual-Stack)	24k + 24k	32k + 32k	24k + 24k
Policy	8k	128k	8k
Max. IPv4 Bindings per Ext-EPG	8k	8k	8k
Max. IPv6 Bindings per Ext-EPG	8k	8k	8k

Note: “Egress Policy Enforcement” on Campus Facing ACI Border Leaf

Policy Enforcement on the SDA Domain

SDA Learning Groups from ACI

Group-Based Access Control Policies | Scalable Groups

Name
AP_DB_EPG
AP_Development_Svr_EPG
AP_HIPAA_Svr_EPG
AP_Medical_Records_EPG
AP_PCI_Svr_EPG
AP_production_app_EPG
AP_production_web_EPG

SGTs created in DNAC

ISE retrieves Application EPGs from APIC via REST API*

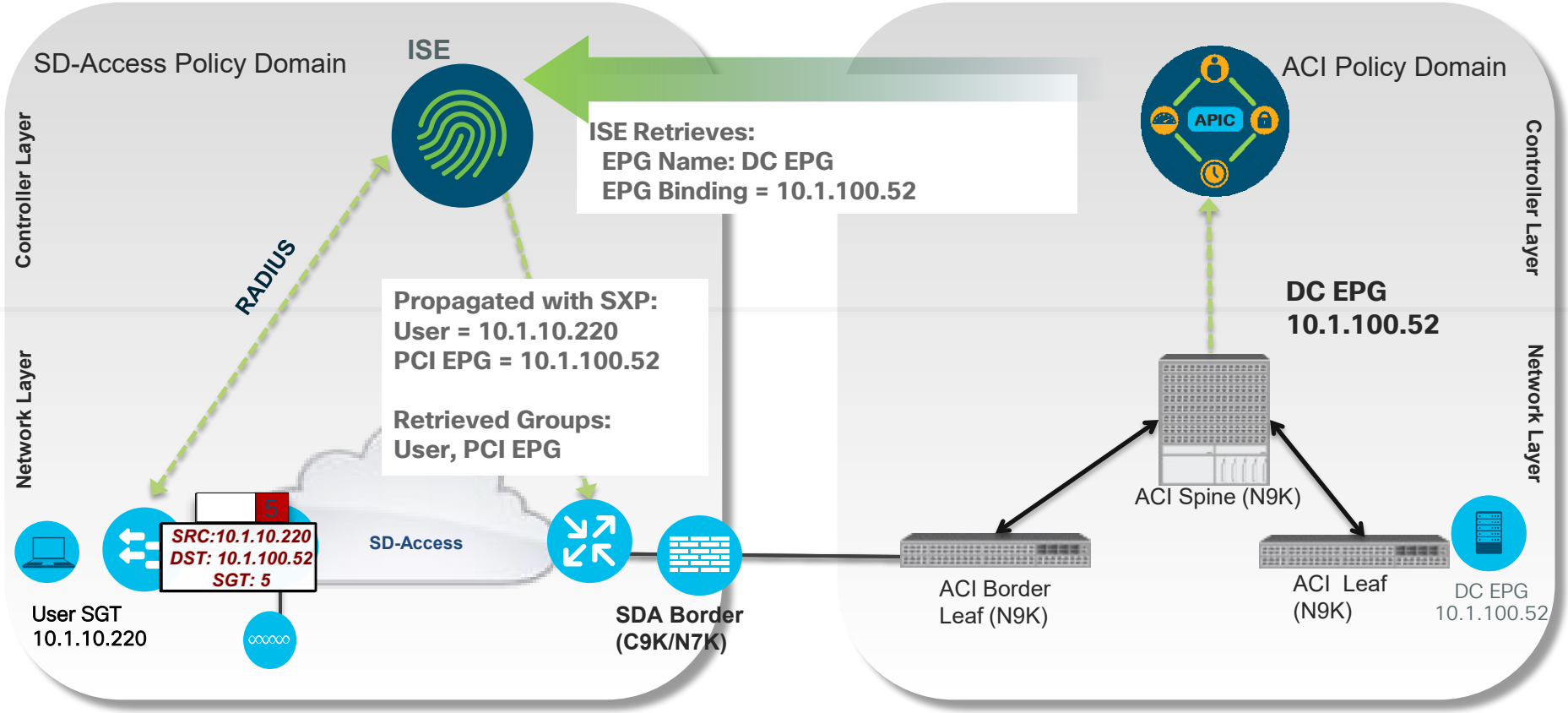
- Tenant Pod01
  - Application Profiles
    - AP
      - Application EPGs
        - DB
        - Development_Svr
        - HIPAA_Svr
        - Medical_Records
        - PCI_Svr
        - production_app
        - production_web

Application EPGs associated to the ACI Tenant integrated with ISE

* All the EPGs defined for the specific Tenant are retrieved

Policy Enforcement on the SDA Domain

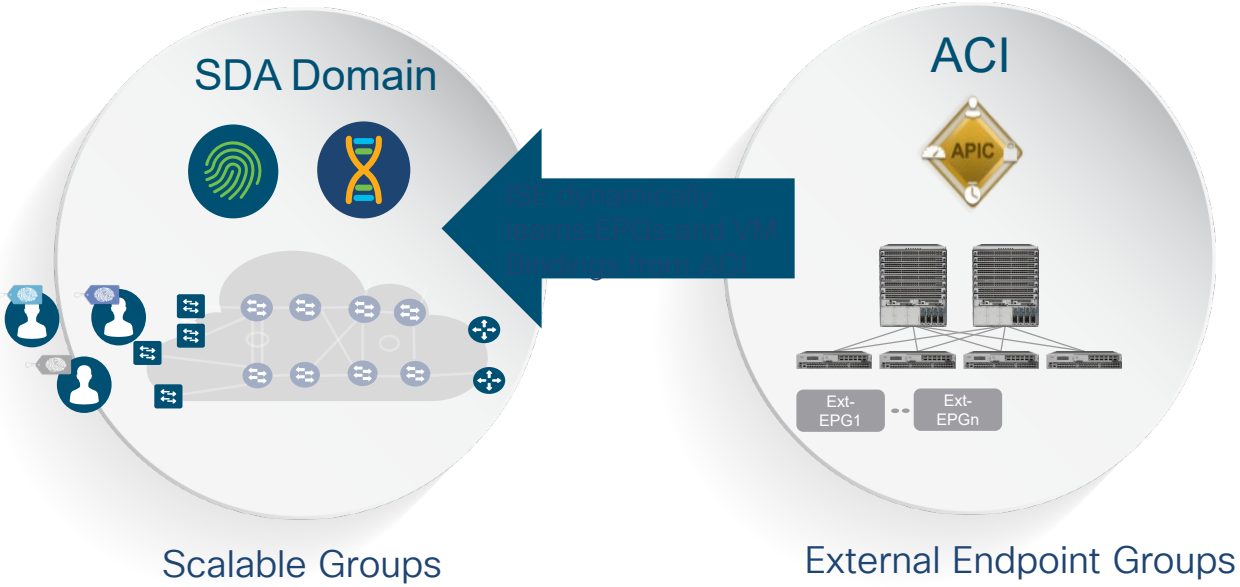
SDA Learning Groups from ACI



Policy Enforcement on the SDA Domain
Scaling Enforcement in SDA Environment

ISE/SDA Scale	
Numbers of Groups	1000
Number of Mappings*	250k
SXP Peers*	200
pxGrid Peers**	200

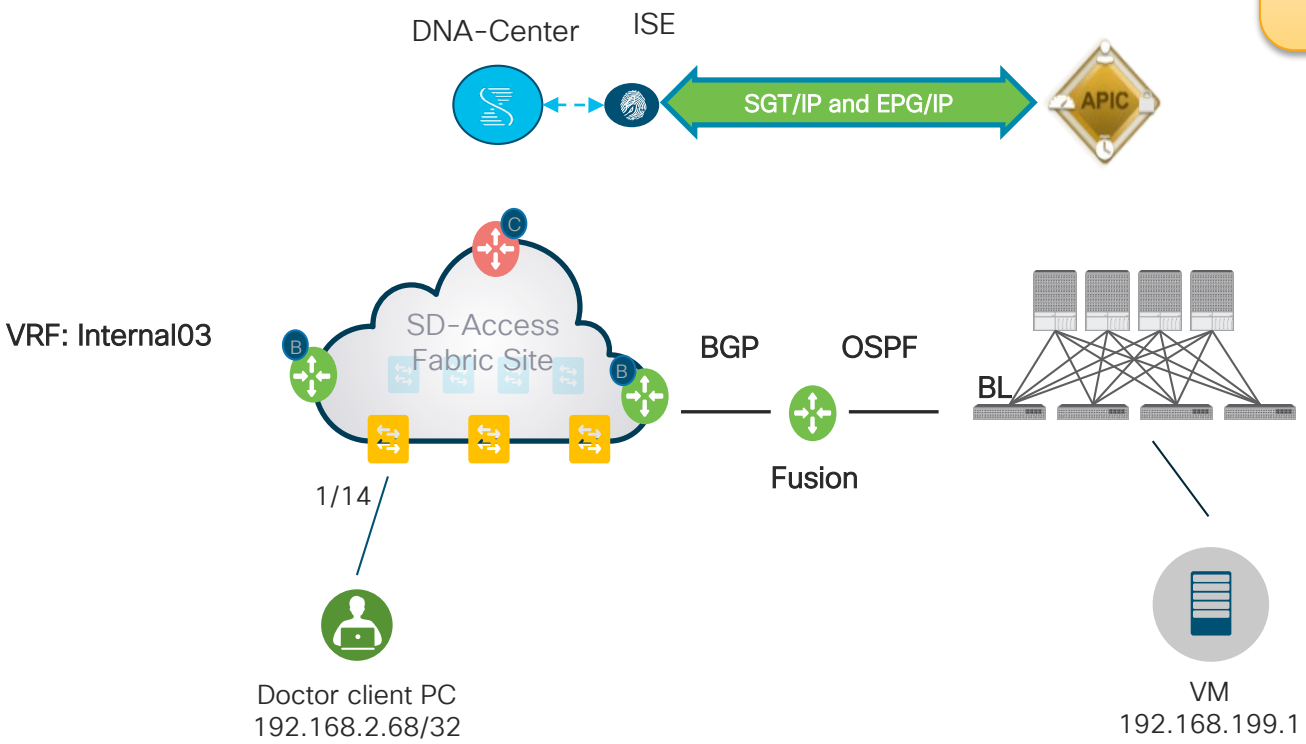
*Per pair of ISE SXP Nodes
** Per ISE pxGrid node



A day in the life of a packet

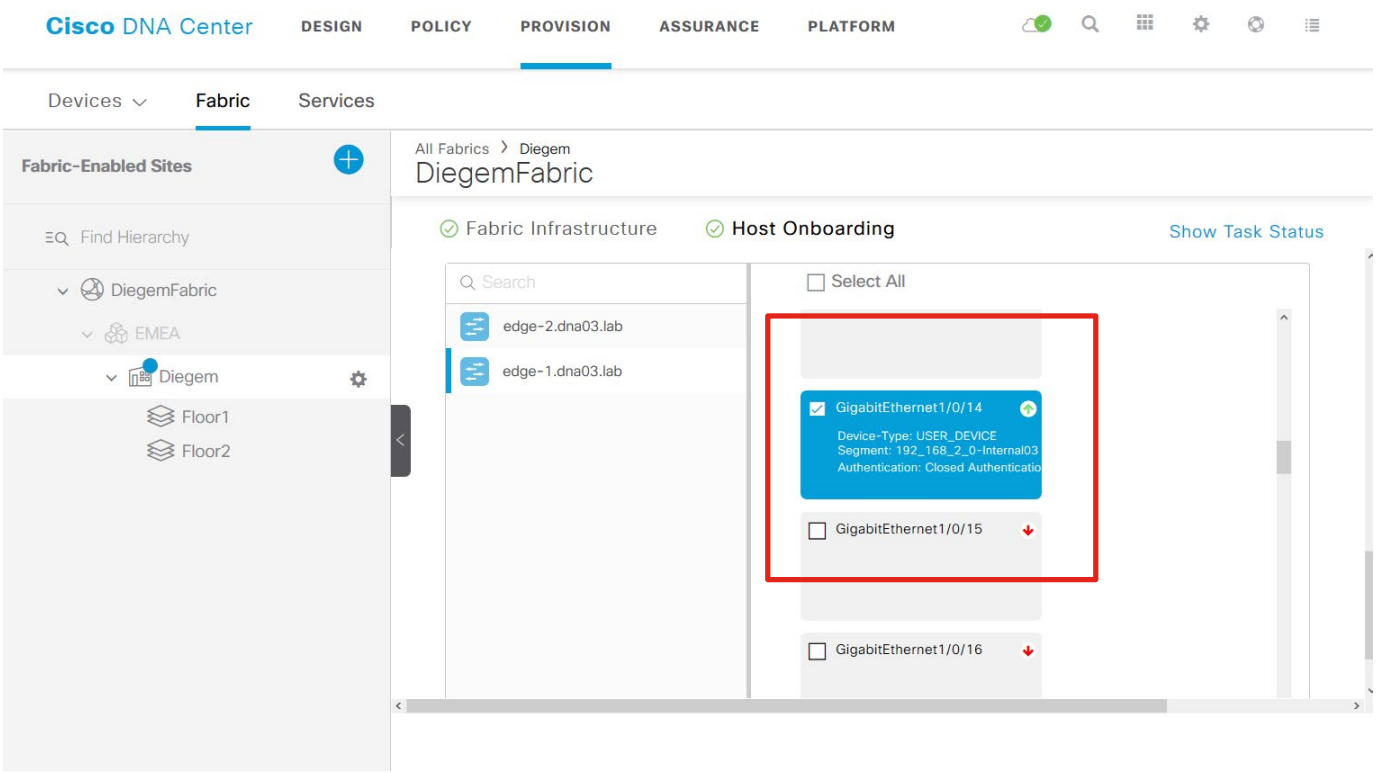
Our setup for today

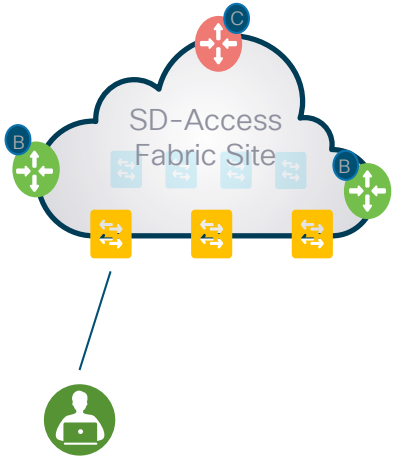
ISE with ACI Policy plane integration



From SDA → ACI

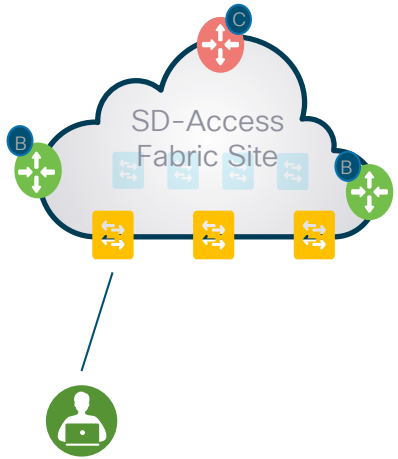
Doctor logs into PC



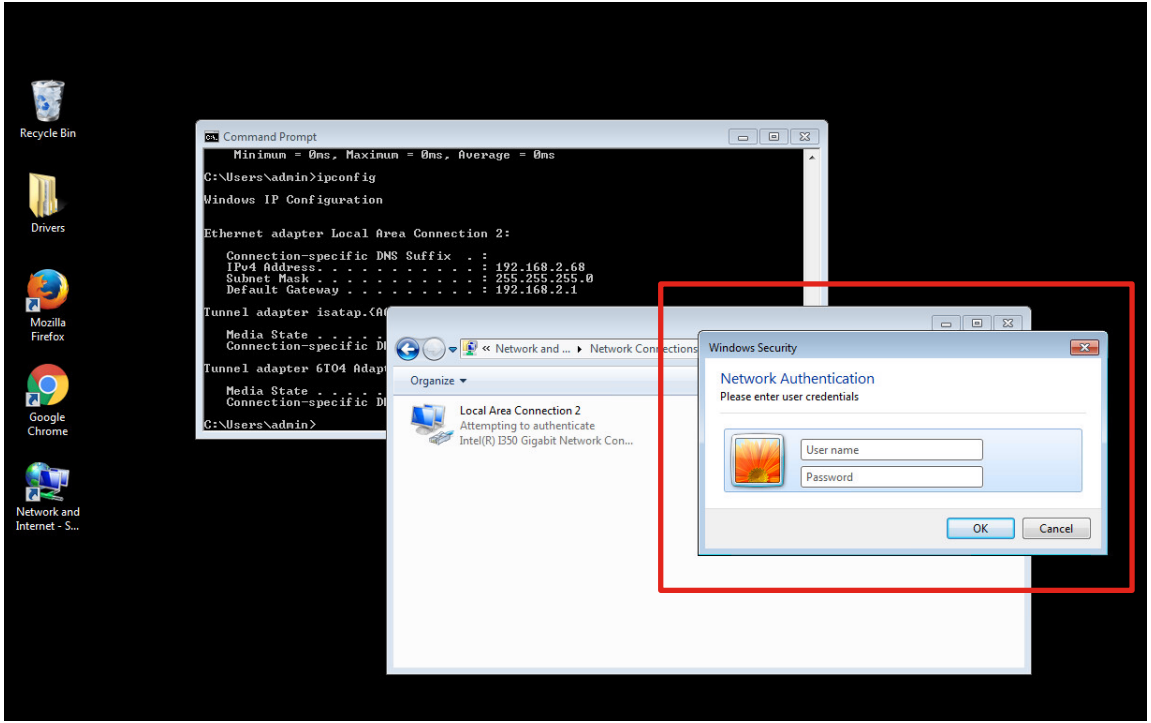


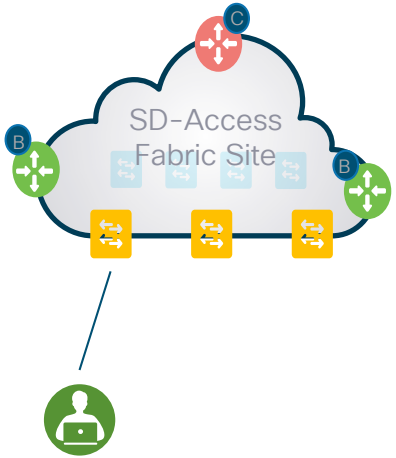
Doctor logs into PC

```
edge-1#show run int GigabitEthernet 1/0/14
Building configuration...

Current configuration : 398 bytes
!
interface GigabitEthernet1/0/14
 switchport access vlan 1023
 switchport mode access
 device-tracking attach-policy IPDT_MAX_10
 load-interval 30
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 no macro auto processing
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
end
```

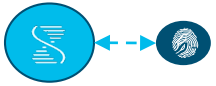


Doctor logs into PC

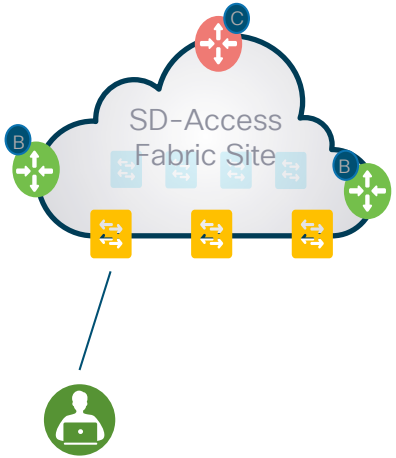




Doctor logs into PC

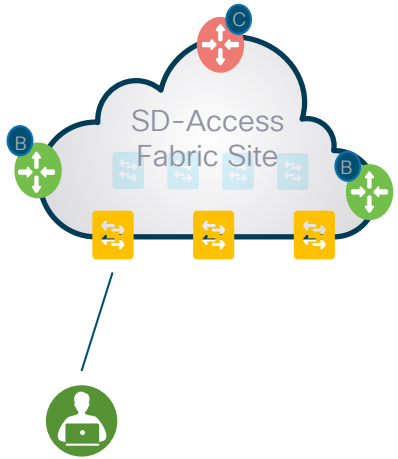


```
edge-1#show authentication  sessions interface GigabitEthernet 1/0/14
Interface              MAC Address    Method  Domain  Status Fg  Session ID
--------------------------------------------------------------------------------
Gi1/0/14               a036.9f8f.7a73 dot1x   DATA    Auth       420210AC00000018AE7B8D4C
```



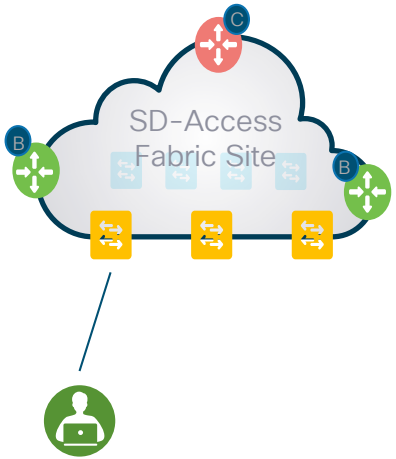
Doctor logs into PC

```
edge-1#show authentication sessions interface GigabitEthernet 1/0/14 details
            Interface:  GigabitEthernet1/0/14
              IIF-ID:  0x10D33F27
         MAC Address:  a036.9f8f.7a73
        IPv6 Address:  Unknown
        IPv4 Address:  192.168.2.68
          User-Name:  derek
         Device-type:  Microsoft-Workstation
         Device-name:  MSFT 5.0
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
  Acct update timeout:  172800s (local), Remaining: 171376s
    Common Session ID:  420210AC00000018AE7B8D4C
     Acct Session ID:  0x0000000b
              Handle:  0x9e00000e
      Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Local Policies:

Server Policies:
            SGT Value:  16


Method status list:
       Method          State
        dot1x         Authc Success

edge-1#
```



Doctor logs into PC

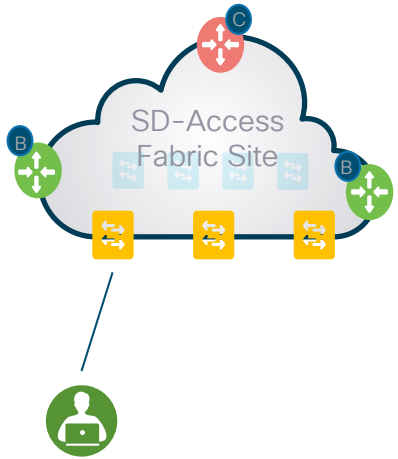
```
edge-1#show cts role-based sgt-map vrf Internal03 all
%IPv6 protocol is not enabled in VRF Internal03
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.2.68             16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1
```



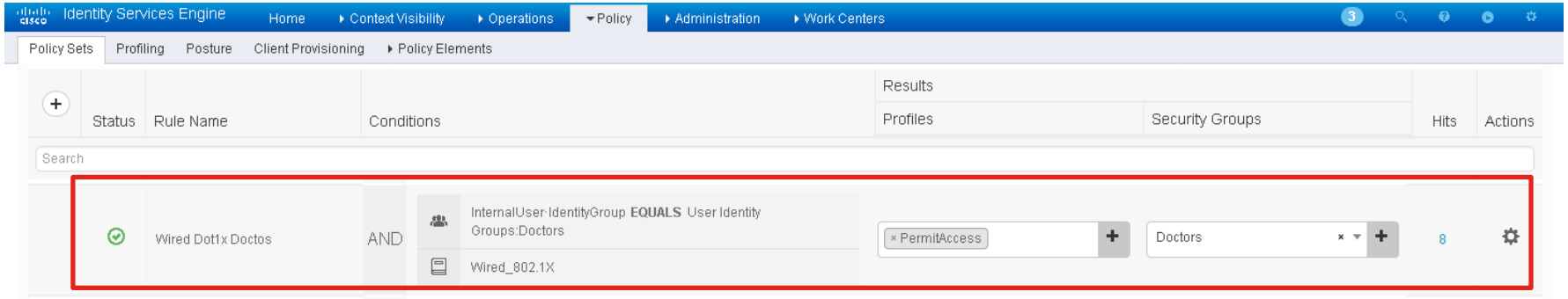
Doctor logs into PC

```
edge-1#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 172.16.201.205, port 1812, A-ID
A7D68ABA7F1ED5D4929F31A08C22A8AA
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-
time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
    3-00:Network_Services
    4-00:Employees
    5-05:Contractors
    6-00:Guests
    7-00:Production_Users
    8-00:Developers
    9-06:Auditors
    10-00:Point_of_Sale_Systems
    11-00:Production_Servers
```

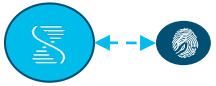
```
    12-06:Development_Servers
    13-00:Test_Servers
    14-00:PCI_Servers
    15-02:BYOD
    16-0187:Doctors
    17-0173:Nurses
    18-09:Patients
    19-02:IT
    20-00:Nurses_contractors
    21-00:BTH
    255-00:Quarantined_Systems
    10001-00:E_commerce_WebEPG
    10002-00:E_commerce_AppEPG
    10003-00:E_commerce_DbEPG
Environment Data Lifetime = 86400 secs
Last update time = 11:46:09 UTC Thu Jan 16 2020
Env-data expires in   0:21:55:32 (dd:hr:mm:sec)
Env-data refreshes in 0:21:55:32 (dd:hr:mm:sec)
Cache data applied          = NONE
State Machine is running
edge-1#
```



Doctor logs into PC



Doctor sends traffic – SDA side



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Components | TrustSec Policy | Policy Sets | SXP | Troubleshoot | Reports | Settings

Click here to do visibility setup Do not show this again.

- Security Groups
- IP SGT Static Mapping
- Security Group ACLs
- Network Devices
- Trustsec AAA Servers

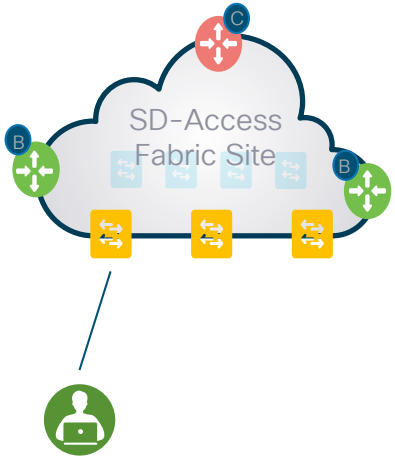
Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

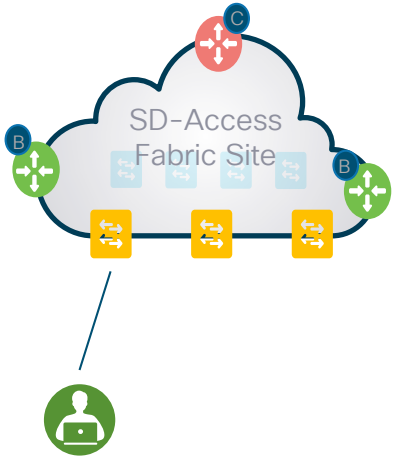
Selected 0 Total 25 Ref

Edit | Add | Import | Export | Trash | Push | Verify Deploy | Show All

Icon	Name	SGT (Dec / Hex)	Description	Learned from
	Auditors	9/0009	Auditor Security Group	
	BTH	21/0015		
	BYOD	15/000F	BYOD Security Group	
	Contractors	5/0005	Contractor Security Group	
	Developers	8/0008	Developer Security Group	
	Development_Servers	12/000C	Development Servers Security Group	
	Doctors	16/0010		
	Employees	4/0004	Employee Security Group	
	E_commerce_AppEPG	10002/2712	Learned from APIC. Suffix: EPG Application profile f...	ACI
	E_commerce_DbEPG	10003/2713	Learned from APIC. Suffix: EPG Application profile f...	ACI
	E_commerce_WebEPG	10001/2711	Learned from APIC. Suffix: EPG Application profile f...	ACI
	Guests	6/0006	Guest Security Group	
	IT	19/0013		

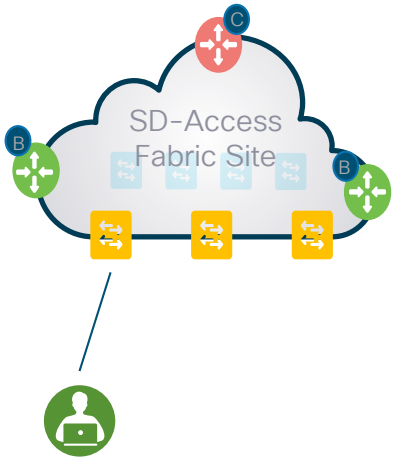


Doctor sends traffic – SDA side



Doctor sends traffic – SDA side

```
edge-1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 17:Nurses to group 16:Doctors:
        Permit IP-00
IPv4 Role-based permissions from group 10001:E_commerce_WebEPG to group 16:Doctors:
        Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

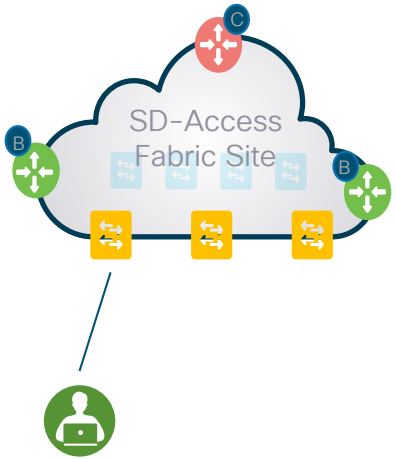


Return traffic

SDA does egress policy

Doctor sends traffic – SDA side

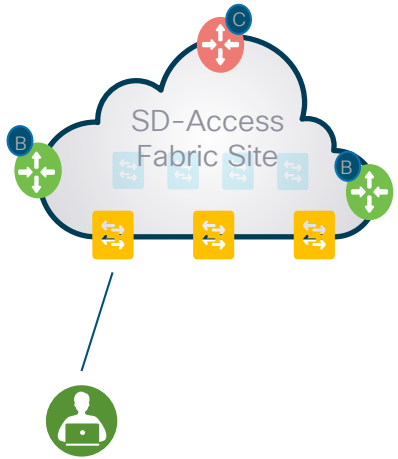
```
edge-1#show ip route vrf Internal03

Routing Table: Internal03
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1022
L        192.168.1.1/32 is directly connected, Vlan1022
      192.168.2.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan1023
L        192.168.2.1/32 is directly connected, Vlan1023
l        192.168.2.68/32 [10/1] via 192.168.2.68, 00:22:48, Vlan1023
edge-1#
```



Doctor client PC
192.168.2.68/32

Doctor sends traffic – SDA side

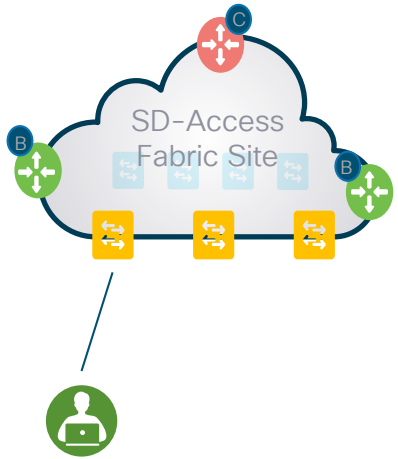
```
edge-1#show run int vlan 1023

interface Vlan1023
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45e
 vrf forwarding Internal03
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 172.16.201.201
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_168_2_0-Internal03-IPV4
end

edge-1#show ip vrf
  Name                    Default RD          Interfaces
  Guest03                 <not set>           Vl1024
                                              Lo4100
  Internal03              <not set>           Vl1023
                                              Vl1022
                                              Lo4099
  Mgmt-vrf                <not set>           Gi0/0
```



Doctor client PC
192.168.2.68/32

Doctor sends traffic – SDA side

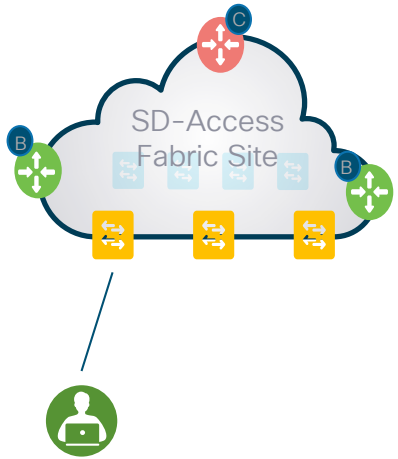
```
edge-1# sh run | s instance-id 4099
 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid 192_168_1_0-Internal03-IPV4
   database-mapping 192.168.1.0/24 locator-set rloc_a88cb7ab-0d01-444e-9ee5-977f707b46ca
   exit-dynamic-eid
  !
  dynamic-eid 192_168_2_0-Internal03-IPV4
   database-mapping 192.168.2.0/24 locator-set rloc_a88cb7ab-0d01-444e-9ee5-977f707b46ca
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Internal03
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id
```



Doctor client PC
192.168.2.68/32

Doctor sends traffic – SDA side

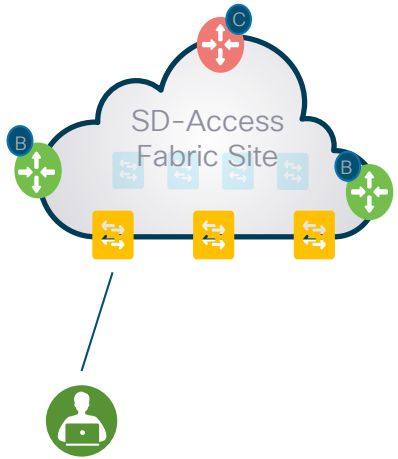
```
edge-1#sh ip lisp instance-id 4099 database 192.168.2.68/32
LISP ETR IPv4 Mapping Database for EID-table vrf Internal03 (IID 4099), LSBs: 0x1
Entries total 2, no-route 0, inactive 1

192.168.2.68/32, dynamic-eid 192_168_2_0-Internal03-IPV4, inherited from default locator-set rloc_a88cb7ab-
0d01-444e-9ee5-977f707b46ca
  Locator      Pri/Wgt  Source     State
  172.16.2.97   10/10   cfg-intf   site-self, reachable

edge-1#   sh ip int brief | i Loopback0
Loopback0              172.16.2.97     YES NVRAM  up                    up

border-1#sh ip lisp | i Map
  Map Server (MS):                    enabled
  Map Resolver (MR):                  enabled
  ITR Map-Resolver(s):                172.16.1.254
  ETR Map-Server(s):                  172.16.1.254
  ITR Solicit Map Request (SMR):      accept and process
  Map-cache:
    Map-cache limit:                  32768
    Map-cache activity check period:  60 secs

border-1#sh lisp site | i Site|Register|192.168.2.68
LISP Site Registration Information
Site Name      Last      Up     Who Last            Inst     EID Prefix
               Register        Registered          ID
               00:30:15  yes#   172.16.2.97:46316   4099     192.168.2.68/32

border-1#sh ip int brief | i Loopback0
Loopback0              172.16.1.254    YES NVRAM  up                    up
```



Doctor client PC
192.168.2.68/32

Doctor sends traffic – SDA side

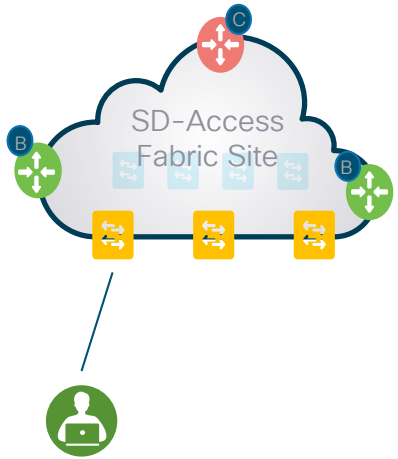
```
edge-1#lig instance-id 4099 192.168.199.1
Mapping information for EID 192.168.199.1 from 172.16.1.254 with RTT 2 msecs
192.168.199.0/24, uptime: 3d00h, expires: 23:59:59, via map-reply, complete
  Locator      Uptime    State     Pri/Wgt    Encap-IID
  172.16.1.254  3d00h    up        10/10      -
edge-1#

edge-1#sh ip lisp instance-id 4099 map-cache 192.168.199.1
LISP IPv4 Mapping Cache for EID-table vrf Internal03 (IID 4099), 7 entries

192.168.199.0/24, uptime: 3d00h, expires: 23:58:06, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 3d00h, map-source: 172.16.1.254
  Idle, Packets out: 11139(6416064 bytes) (~ 00:33:24 ago)
  Locator      Uptime    State     Pri/Wgt    Encap-IID
  172.16.1.254  3d00h    up        10/10      -
    Last up-down state change:         3d00h, state change count: 1
    Last route reachability change:    3d02h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            never
```



Doctor client PC
192.168.2.68/32

Doctor sends traffic – SDA side

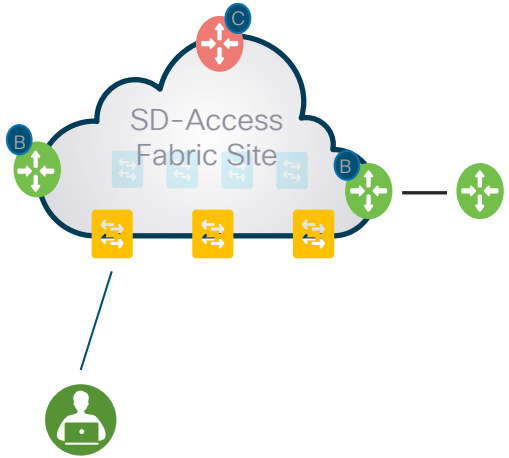
```
border-1#show ip route vrf Internal03

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        172.16.4.4/30 is directly connected, Vlan3002
L        172.16.4.5/32 is directly connected, Vlan3002
B        172.16.201.0/24 [20/0] via 172.16.4.6, 3d01h
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
B        192.168.1.0/24 [200/0], 01:06:19, Null0
C        192.168.1.1/32 is directly connected, Loopback1022
I        192.168.1.3/32 [250/1], 01:06:19, Null0
I        192.168.1.4/32 [250/1], 01:16:49, Null0
I        192.168.1.5/32 [250/1], 01:17:59, Null0
      192.168.2.0/24 is variably subnetted, 3 subnets, 2 masks
B        192.168.2.0/24 [200/0], 00:41:30, Null0
C        192.168.2.1/32 is directly connected, Loopback1023
I        192.168.2.68/32 [250/1], 00:41:30, Null0
B     192.168.199.0/24 [20/20] via 172.16.4.6, 3d01h
      192.168.200.0/30 is subnetted, 2 subnets
B        192.168.200.0 [20/0] via 172.16.4.6, 3d01h
B        192.168.200.4 [20/0] via 172.16.4.6, 3d01h
```



No egress policy on border

Doctor sends traffic – Fusion side

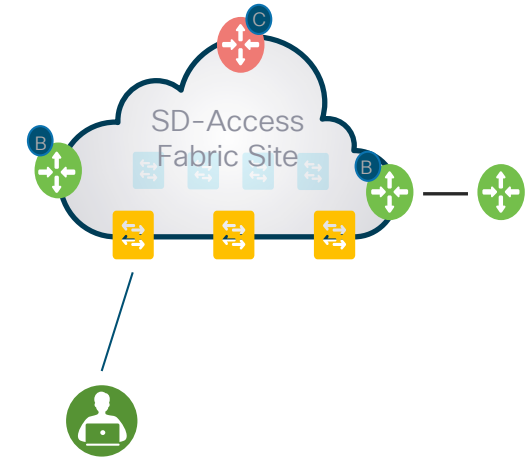
```
bdsol-dna03-fusion1#show ip route vrf Internal03

      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.4.4/30 is directly connected, GigabitEthernet0/0/0.3002
L        172.16.4.6/32 is directly connected, GigabitEthernet0/0/0.3002
B        172.16.201.0/24
          is directly connected, 7w0d, GigabitEthernet0/0/2.3653
L        172.16.201.1/32 is directly connected, GigabitEthernet0/0/2.3653
B     192.168.1.0/24 [20/0] via 172.16.4.5, 3d01h
B     192.168.2.0/24 [20/0] via 172.16.4.5, 3d01h
O E2  192.168.199.0/24
          [110/20] via 192.168.200.5, 3d01h, GigabitEthernet0/2/0.901
          [110/20] via 192.168.200.1, 3d01h, GigabitEthernet0/1/0.901
      192.168.200.0/24 is variably subnetted, 6 subnets, 2 masks
C        192.168.200.0/30 is directly connected, GigabitEthernet0/1/0.901
L        192.168.200.2/32 is directly connected, GigabitEthernet0/1/0.901
C        192.168.200.4/30 is directly connected, GigabitEthernet0/2/0.901
L        192.168.200.6/32 is directly connected, GigabitEthernet0/2/0.901
O        192.168.200.201/32
          [110/2] via 192.168.200.1, 3d01h, GigabitEthernet0/1/0.901
O        192.168.200.202/32
          [110/2] via 192.168.200.5, 3d01h, GigabitEthernet0/2/0.901
```



BGP / OSPF route redistribution

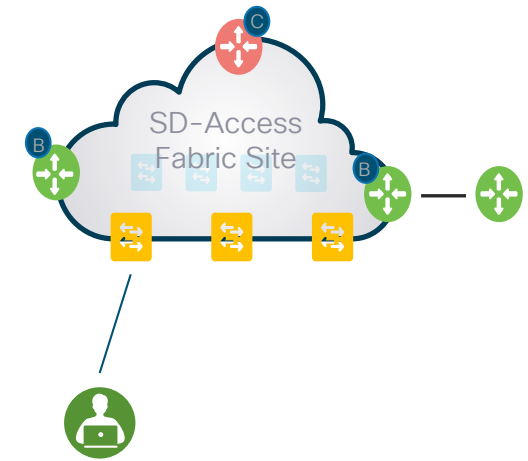
Doctor sends traffic – Fusion side

```
bdsol-dna03-fusion1#show running-config  | sec router
router ospf 1 vrf Internal03
 router-id 192.168.200.200
 redistribute bgp 65000 subnets
 network 192.168.200.0 0.0.0.3 area 0.0.0.0
 network 192.168.200.4 0.0.0.3 area 0.0.0.0
router bgp 65000
 bgp log-neighbor-changes
 redistribute connected
 maximum-paths eibgp 2
 !
address-family ipv4 vrf Internal03
  redistribute connected
  redistribute ospf 1 route-map OSPFtoInternal03BGP
  neighbor 172.16.4.5 remote-as 65003
  neighbor 172.16.4.5 activate
 exit-address-family
```



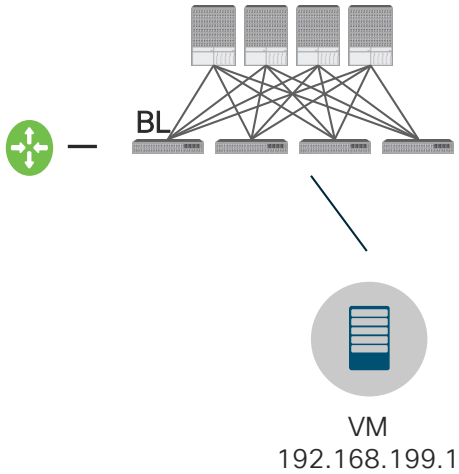
Doctor sends traffic – Fusion side

```
bdsol-dna03-fusion1#show running-config  | sec router
router ospf 1 vrf Internal03
 router-id 192.168.200.200
 redistribute bgp 65000 subnets
 network 192.168.200.0 0.0.0.3 area 0.0.0.0
 network 192.168.200.4 0.0.0.3 area 0.0.0.0
router bgp 65000
 bgp log-neighbor-changes
 redistribute connected
 maximum-paths eibgp 2
 !
address-family ipv4 vrf Internal03
  redistribute connected
  redistribute ospf 1 route-map OSPFtoInternal03BGP
  neighbor 172.16.4.5 remote-as 65003
  neighbor 172.16.4.5 activate
 exit-address-family

bdsol-dna03-fusion1# show ip ospf  neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.200.202   0   FULL/  -        00:00:36    192.168.200.5   GigabitEthernet0/2/0.901
192.168.200.201   0   FULL/  -        00:00:32    192.168.200.1   GigabitEthernet0/1/0.901
bdsol-dna03-fusion1#
```



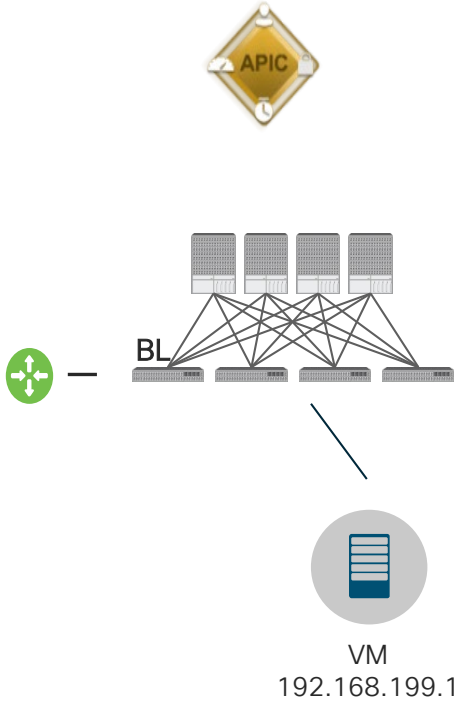
Doctor sends traffic – ACI side

```
bdsol-aci12-leaf3# show vrf
 VRF-Name                          VRF-ID State    Reason
 black-hole                          3 Up      --
 BRKOPS2110:BRKOPS2110                    5 Up      --
 management                            2 Up      --
 overlay-1                           4 Up      --

bdsol-aci12-leaf3# show ip ospf neighbors vrf BRKOPS2110:BRKOPS2110
 OSPF Process ID default VRF BRKOPS2110:BRKOPS2110
 Total number of neighbors: 1
 Neighbor ID     Pri State           Up Time  Address         Interface
 192.168.200.200   1 FULL/ -         3d01h    192.168.200.2   Eth1/41.9
```



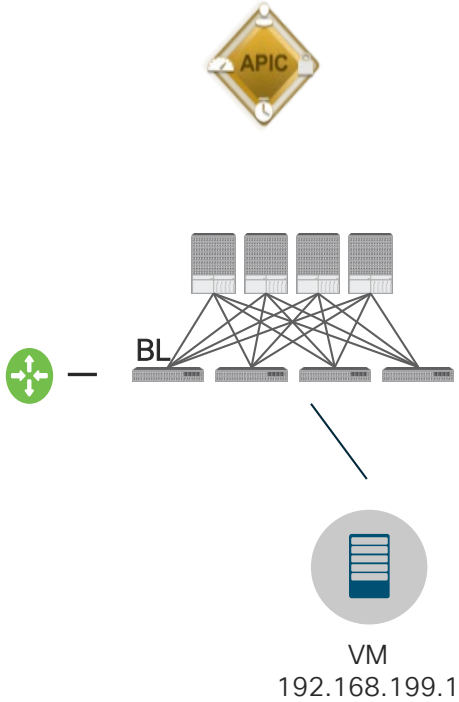
Doctor sends traffic – ACI side

```
bdsol-aci12-leaf3# show endpoint ip 192.168.199.1
Legend:
 s - arp          H - vtep          V - vpc-attached    p - peer-aged
 R - peer-attached-rl B - bounce        S - static        M - span
 D - bounce-to-proxy  O - peer-attached   a - local-aged      m - svc-mgr
 L - local        E - shared-service
+-----------------------------------+---------------+-----------------+--------------+-------------+
     VLAN/                    Encap        MAC Address      MAC Info/       Interface
     Domain                   VLAN         IP Address       IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+

bdsol-aci12-leaf3# show ip route vrf BRKOPS2110:BRKOPS2110
172.16.201.0/24, ubest/mbest: 1/0
   *via 192.168.200.2, eth1/41.9, [110/1], 3d01h, ospf-default, type-2, tag 3489725928
192.168.1.0/24, ubest/mbest: 1/0
   *via 192.168.200.2, eth1/41.9, [110/1], 3d01h, ospf-default, type-2, tag 3489725928
192.168.2.0/24, ubest/mbest: 1/0
   *via 192.168.200.2, eth1/41.9, [110/1], 3d01h, ospf-default, type-2, tag 3489725928
192.168.199.0/24, ubest/mbest: 1/0, attached, direct, pervasive
   *via 10.0.184.64%overlay-1, [1/0], 3d02h, static
192.168.200.0/30, ubest/mbest: 1/0, attached, direct
   *via 192.168.200.1, eth1/41.9, [0/0], 3d03h, direct
192.168.200.1/32, ubest/mbest: 1/0, attached
   *via 192.168.200.1, eth1/41.9, [0/0], 3d03h, local, local
192.168.200.4/30, ubest/mbest: 1/0
   *via 192.168.200.2, eth1/41.9, [110/41], 3d01h, ospf-default, intra
192.168.200.201/32, ubest/mbest: 2/0, attached, direct
   *via 192.168.200.201, lo1, [0/0], 3d03h, local, local
   *via 192.168.200.201, lo1, [0/0], 3d03h, direct
192.168.200.202/32, ubest/mbest: 1/0
   *via 10.0.88.69%overlay-1, [1/0], 3d03h, bgp-101, internal, tag 101
bdsol-aci12-leaf3#
```



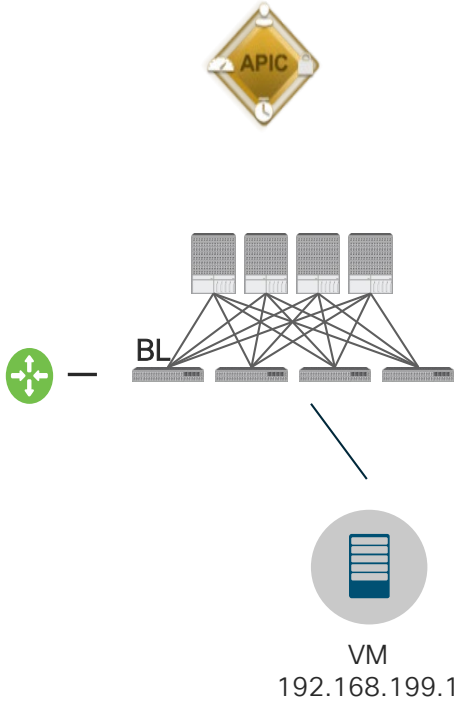
Doctor sends traffic – ACI side

```
bdsol-aci12-spine1# show ip int vrf overlay-1
IP Interface Status for VRF "overlay-1"
lo0, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: ptep
  IP address: 10.0.88.66, IP subnet: 10.0.88.66/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
lo1, Interface status: protocol-up/link-up/admin-up, iod: 81, mode: anycast-v6
  IP address: 10.0.184.66, IP subnet: 10.0.184.66/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
lo2, Interface status: protocol-up/link-up/admin-up, iod: 82, mode: anycast-v4
  IP address: 10.0.184.64, IP subnet: 10.0.184.64/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
lo3, Interface status: protocol-up/link-up/admin-up, iod: 83, mode: anycast-mac
  IP address: 10.0.184.65, IP subnet: 10.0.184.65/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
lo4, Interface status: protocol-up/link-up/admin-up, iod: 84, mode: anycast-mac,external
  IP address: 10.0.0.33, IP subnet: 10.0.0.33/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
...
```

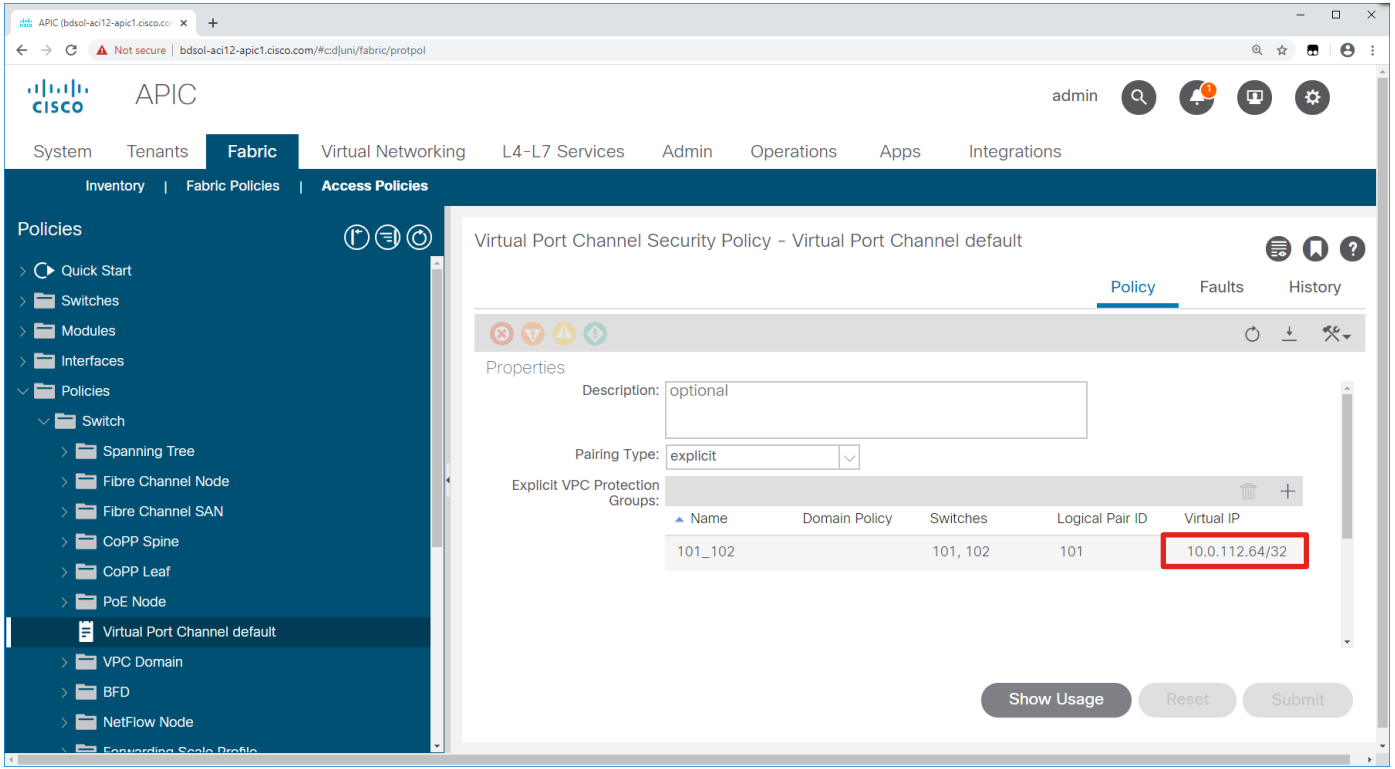


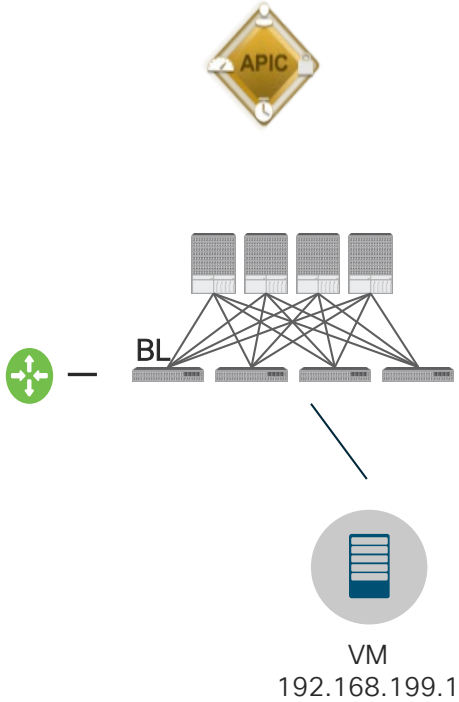
Doctor sends traffic – ACI side

```
bdsol-aci12-spine1# show coop internal info ip-db


------------------------------
IP address : 192.168.199.1
Vrf : 2752512
Flags : 0
EP bd vnid : 16056262
EP mac :  00:50:56:B6:3F:9D
Publisher Id : 10.0.88.64
Record timestamp : 01 16 2020 14:05:25 230714325
Publish timestamp : 01 16 2020 14:05:25 231331696
Seq No: 0
Remote publish timestamp: 01 01 1970 00:00:00 0
URIB Tunnel Info
Num tunnels : 1
        Tunnel address : 10.0.112.64
        Tunnel ref count : 1


bdsol-aci12-spine1# acidiag fnvread | grep 10.0.88.64
    102       1    bdsol-aci12-leaf2      SAL1951VHXH      10.0.88.64/32   leaf        active   0
bdsol-aci12-spine1#
```



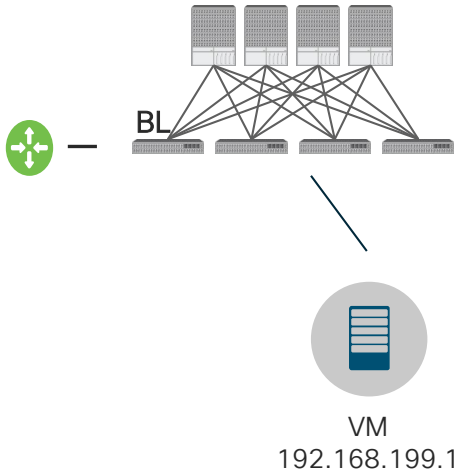
Doctor sends traffic – ACI side





Doctor sends traffic – ACI side

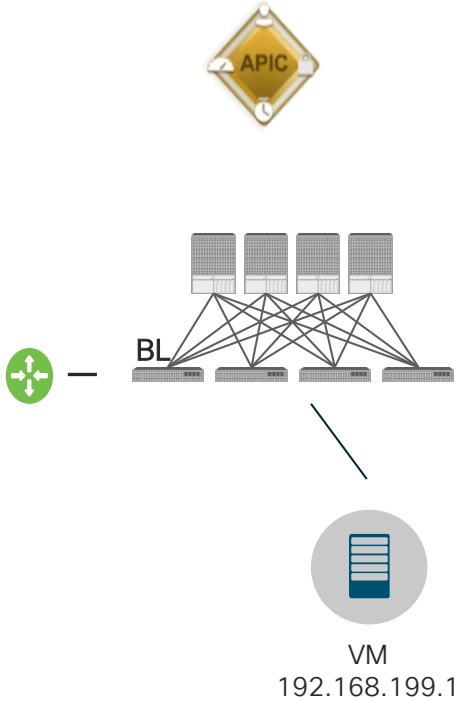
```
bdsol-aci12-leaf2# show endpoint ip 192.168.199.1
Legend:
 s - arp          H - vtep          V - vpc-attached    p - peer-aged
 R - peer-attached-rl B - bounce        S - static        M - span
 D - bounce-to-proxy  O - peer-attached   a - local-aged      m - svc-mgr
 L - local         E - shared-service
+-----------------------------------+---------------+-----------------+--------------+-------------+
     VLAN/                    Encap        MAC Address      MAC Info/      Interface
     Domain                   VLAN         IP Address       IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
2                            vlan-1068    0050.56b6.3f9d LaV                   po5
BRKOPS2110:BRKOPS2110                     vlan-1068     192.168.199.1 LaV                po5


bdsol-aci12-leaf2#
```



What about policy ?

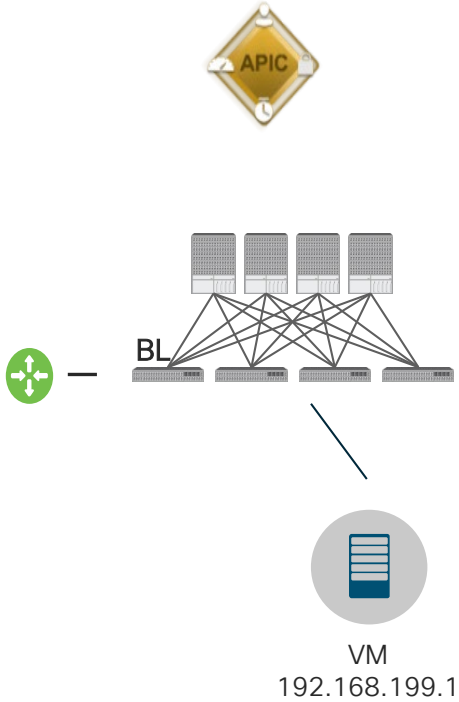
Doctor sends traffic – ACI side

```
apic1# moquery -d uni/tn-BRKOPS2110/ap-E-commerce/epg-Web          # see also moquery -c fvAEPg

# fv.AEPg
name              : Web
annotation        :
childAction       :
configIssues      :
configSt          : applied
descr             :
dn                : uni/tn-BRKOPS2110/ap-E-commerce/epg-Web
exceptionTag      :
extMngdBy         :
floodOnEncap      : disabled
fwdCtrl           :
hasMcastSource    : no
isAttrBasedEPg    : no
isSharedSrvMsiteEPg  : no
lcOwn             : local
matchT            : AtleastOne
modTs             : 2020-01-13T11:47:29.279+00:00
monPolDn          : uni/tn-common/monepg-default
nameAlias         :
pcEnfPref         : unenforced
pcTag             : 16386
prefGrMemb        : exclude
prio              : unspecified
rn                : epg-Web
scope             : 2752512
shutdown          : no
status            :
triggerSt         : triggerable
txId              : 11529215046069378734
uid               : 15374
```



Doctor sends traffic – ACI side

```
apic1# moquery -d uni/tn-BRKOPS2110/out-Router1-BRKOPS2110/instP-DoctorsSGT
Total Objects shown: 1

# l3ext.InstP
name              : DoctorsSGT
annotation        : orchestrator:ise
childAction       :
configIssues      :
configSt          : applied
descr             :
dn                : uni/tn-BRKOPS2110/out-Router1-BRKOPS2110/instP-DoctorsSGT
exceptionTag      :
extMngdBy         :
floodOnEncap      : disabled
isSharedSrvMsiteEPg  : no
lcOwn             : local
matchT            : AtleastOne
mcast             : no
modTs             : 2020-01-13T14:08:14.550+00:00
monPolDn          : uni/tn-common/monepg-default
nameAlias         :
pcTag             : 49155
prefGrMemb        : exclude
prio              : unspecified
rn                : instP-DoctorsSGT
scope             : 2752512
status            :
targetDscp        : unspecified
triggerSt         : triggerable
txId              : 11529215046069384275
uid               : 15374

apic1#
```



How does it end up in DoctorsSGT ?

Doctor sends traffic – ACI side

APIC (bdsol-aci12-apic1.cisco.co

Not secure | bdsol-aci12-apic1.cisco.com/#bTenants:BRKOPS2110|uni/tn-BRKOPS2110/out-Router1-BRKOPS2110/instP-DoctorsSGT

cisco APIC

admin

System | Tenants | Fabric | Virtual Networking | L4-L7 Services | Admin | Operations | Apps | Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | BRKOPS2110 | mgmt | infra

BRKOPS2110

- VRFs
- External Bridged Networks
- L3Outs
  - Router1-BRKOPS2110
    - Logical Node Profiles
    - External EPGs
      - AuditorsSGT
      - BYODSGT
      - ContractorsSGT
      - DevelopersSGT
      - Development_ServersSGT
      - DoctorsSGT
      - EmployeesSGT
      - GuestsSGT
      - Network_ServicesSGT
      - Nurses_contractorsSGT
      - Outside

External EPG Instance Profile - DoctorsSGT

Policy | Operational | Stats | Health | Faults | History

General | Contracts | Subject Labels | EPG Labels

Healthy

Properties

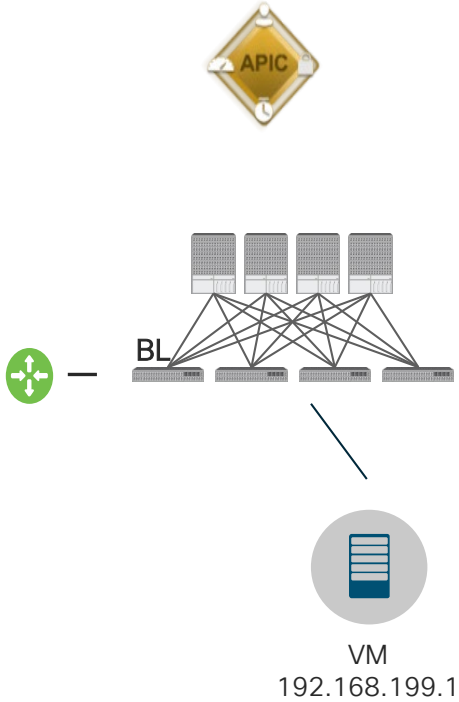
Subnets:

IP Address	Scope	Name	Aggre	Ro Co Prc
192.168.1.4/32	External Subnets for the External EPG			
192.168.2.68/32	External Subnets for the External EPG			

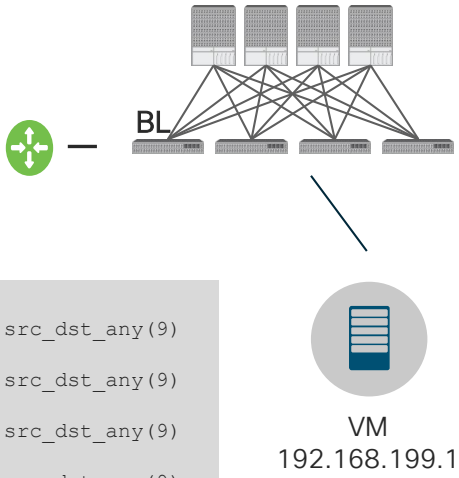
Show Usage | Reset | Submit

Last Login Time: 2020-01-16T14:34 UTC+00:00

Current System Time: 2020-01-16T15:16 UTC+00:00



Doctor sends traffic – ACI side




```
bdsol-aci12-leaf2# show zoning-rule  | grep 2752512 | egrep "16386|49155"
|   4105  | 16386  |   15   | default  |    uni-dir     | enabled | 2752512  |  external_app |  permit  |    src_dst_any(9)
|
|   4111  | 32770  | 16386  | default  |    uni-dir     | enabled | 2752512  |  external_app |  permit  |    src_dst_any(9)
|
|   4114  | 16386  | 16389  | default  |     bi-dir     | enabled | 2752512  | frontend_mgmt |  permit  |    src_dst_any(9)
|
|   4112  | 16389  | 16386  | default  | uni-dir-ignore | enabled | 2752512  | frontend_mgmt |  permit  |    src_dst_any(9)
|
|   4101  | 16386  | 49155  | default  | uni-dir-ignore | enabled | 2752512  |  external_app |  permit  |    src_dst_any(9)
|
|   4113  | 49155  | 16386  | default  |     bi-dir     | enabled | 2752512  |  external_app |  permit  |    src_dst_any(9)
|
bdsol-aci12-leaf2#
```

From ACI → SDA

Next slides will cover the difference compared to SDA → ACI

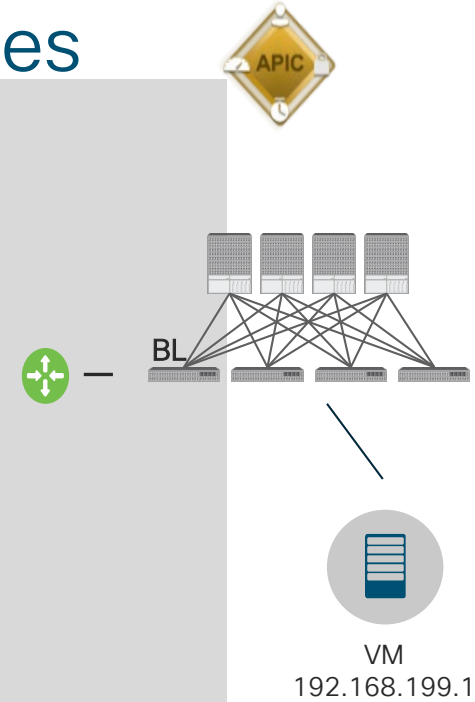
ACI Leaf

- Use VRF specific “Policy Control Enforcement Direction”

Policy Control Enforcement Direction: Egress Ingress

Return traffic – ACI side – external routes

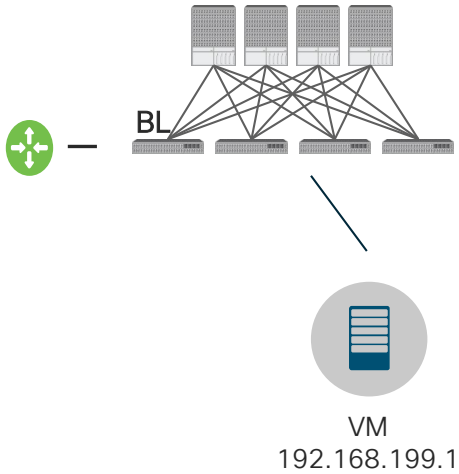
```
bdsol-aci12-leaf2# show ip route vrf BRKOPS2110:BRKOPS2110
IP Route Table for VRF "BRKOPS2110:BRKOPS2110"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.201.0/24, ubest/mbest: 2/0
    *via 10.0.88.71%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
    *via 10.0.88.69%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
192.168.1.0/24, ubest/mbest: 2/0
    *via 10.0.88.71%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
    *via 10.0.88.69%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
192.168.2.0/24, ubest/mbest: 2/0
    *via 10.0.88.71%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
    *via 10.0.88.69%overlay-1, [200/1], 3d02h, bgp-101, internal, tag 101
192.168.199.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.184.64%overlay-1, [1/0], 3d03h, static
192.168.199.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 192.168.199.254, vlan1, [0/0], 3d03h, local, local
192.168.200.0/30, ubest/mbest: 1/0
    *via 10.0.88.71%overlay-1, [200/0], 3d03h, bgp-101, internal, tag 101
192.168.200.4/30, ubest/mbest: 1/0
    *via 10.0.88.69%overlay-1, [200/0], 3d03h, bgp-101, internal, tag 101
192.168.200.201/32, ubest/mbest: 1/0
    *via 10.0.88.71%overlay-1, [1/0], 3d03h, bgp-101, internal, tag 101
192.168.200.202/32, ubest/mbest: 1/0
    *via 10.0.88.69%overlay-1, [1/0], 3d03h, bgp-101, internal, tag 101
bdsol-aci12-leaf2# acidiag fnvread | egrep "10.0.88.71|10.0.88.69"
     103        1    bdsol-aci12-leaf3      SAL1940QA95      10.0.88.71/32    leaf         active
     104        1    bdsol-aci12-leaf4      SAL1940QAD8      10.0.88.69/32    leaf         active
bdsol-aci12-leaf2#
```



How do we receive these routes ?

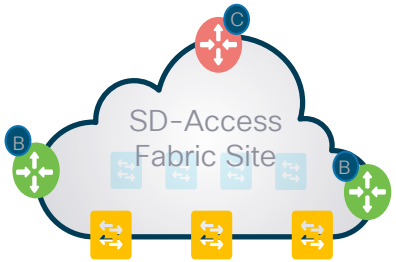
Return traffic – ACI side – external routes

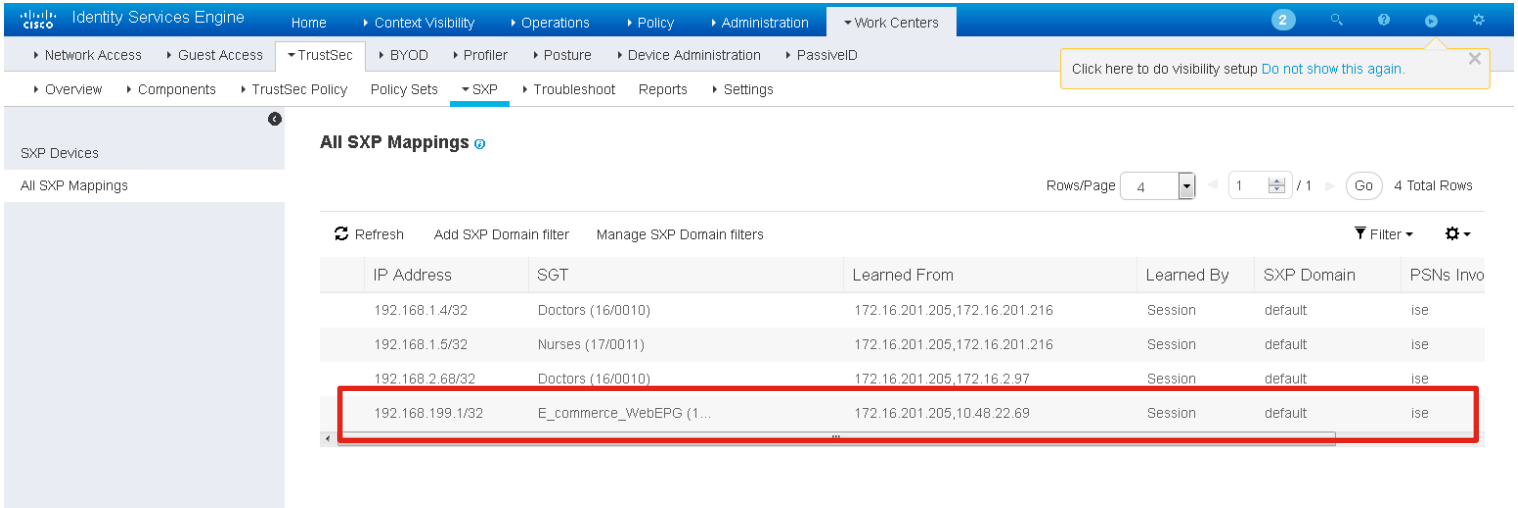
```
bdsol-aci12-leaf2# show bgp vpnv4 unicast vrf BRKOPS2110:BRKOPS2110
BGP routing table information for VRF overlay-1, address family VPNv4 Unicast
BGP table version is 116, local router ID is 10.0.88.64
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

   Network            Next Hop            Metric     LocPrf     Weight Path
Route Distinguisher: 102:2752512    (VRF BRKOPS2110:BRKOPS2110)
*>i172.16.201.0/24    10.0.88.69               1        100          0 ?
*|i                   10.0.88.71               1        100          0 ?
*>i192.168.1.0/24     10.0.88.69               1        100          0 ?
*|i                   10.0.88.71               1        100          0 ?
*>i192.168.2.0/24     10.0.88.69               1        100          0 ?
*|i                   10.0.88.71               1        100          0 ?
* i192.168.200.0/30   10.0.88.69              41        100          0 ?
*>i                   10.0.88.71               0        100          0 ?
* i192.168.200.4/30   10.0.88.71              41        100          0 ?
*>i                   10.0.88.69               0        100          0 ?
*>i192.168.200.201/32 10.0.88.71               0        100          0 ?
*>i192.168.200.202/32 10.0.88.69               0        100          0 ?


bdsol-aci12-leaf2#
```



Route reflectors send outside L3out routes trough the fabric

Return traffic – SDA side – classify traffic

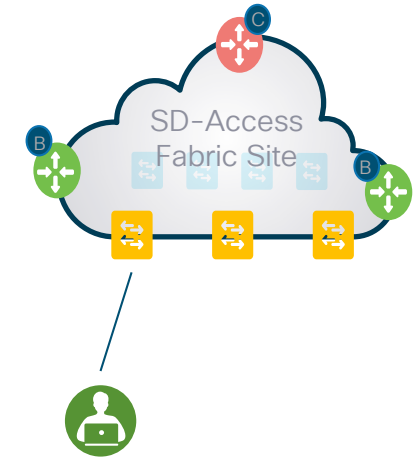




Doctor client PC
192.168.2.68/32

Return traffic – SDA side – classify traffic

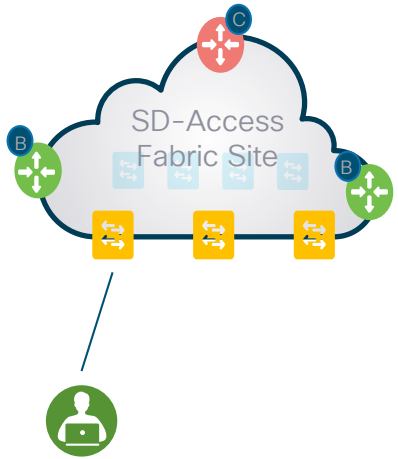
```
border-1#show running-config  | inc sxp
cts sxp enable
cts sxp default password 7 <secret>
cts sxp connection peer 172.16.201.205 source 172.16.4.5 password default mode local
listener hold-time 0 0 vrf Internal03

border-1#show cts sxp connections vrf Internal03
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Key-Chain: Not Set
 Default Key-Chain Name: Not Applicable
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
---------------------------------------------
Peer IP          : 172.16.201.205
Source IP        : 172.16.4.5
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Hold timer is running
Duration since last state change: 2:05:02:27 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```



Doctor client PC
192.168.2.68/32

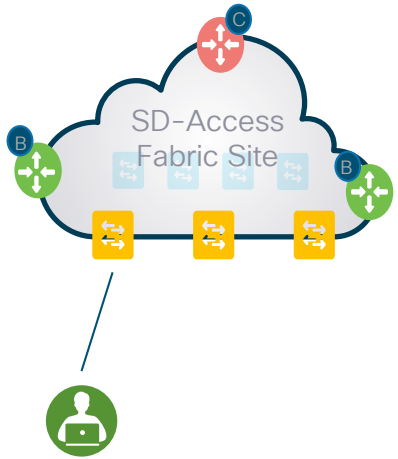
Return traffic – SDA side – classify traffic

```
border-1#show ip int brief | inc 172.16.4.5
Vlan3002               172.16.4.5      YES NVRAM  up                    up
border-1#show run int Vlan3002
Building configuration...

Current configuration : 186 bytes
!
interface Vlan3002
 description vrf interface to External router
 vrf forwarding Internal03
 ip address 172.16.4.5 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end

border-1#
```



Return traffic – SDA side – classify traffic

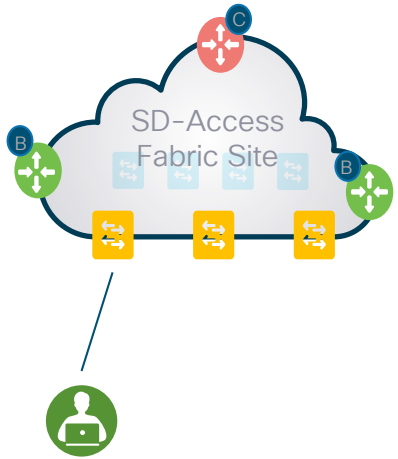
```
bdsol-dna03-fusion1#show ip route vrf Internal03

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.4.4/30 is directly connected, GigabitEthernet0/0/0.3002
L        172.16.4.6/32 is directly connected, GigabitEthernet0/0/0.3002
B        172.16.201.0/24
           is directly connected, 7w0d, GigabitEthernet0/0/2.3653
L        172.16.201.1/32 is directly connected, GigabitEthernet0/0/2.3653
B     192.168.1.0/24 [20/0] via 172.16.4.5, 3d02h
B     192.168.2.0/24 [20/0] via 172.16.4.5, 3d02h
O E2  192.168.199.0/24
           [110/20] via 192.168.200.5, 3d02h, GigabitEthernet0/2/0.901
           [110/20] via 192.168.200.1, 3d02h, GigabitEthernet0/1/0.901
      192.168.200.0/24 is variably subnetted, 6 subnets, 2 masks
C        192.168.200.0/30 is directly connected, GigabitEthernet0/1/0.901
L        192.168.200.2/32 is directly connected, GigabitEthernet0/1/0.901
C        192.168.200.4/30 is directly connected, GigabitEthernet0/2/0.901
L        192.168.200.6/32 is directly connected, GigabitEthernet0/2/0.901
O        192.168.200.201/32
           [110/2] via 192.168.200.1, 3d02h, GigabitEthernet0/1/0.901
O        192.168.200.202/32
           [110/2] via 192.168.200.5, 3d02h, GigabitEthernet0/2/0.901
bdsol-dna03-fusion1#
```



Doctor client PC
192.168.2.68/32

Return traffic – SDA side – classify traffic

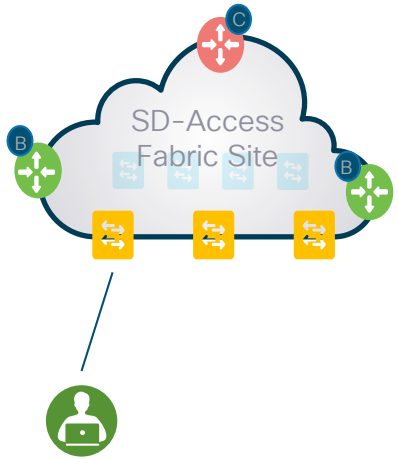
```
vrf definition Internal03
 rd 1:4098
 !
 address-family ipv4
  import ipv4 unicast map globalToInternal03
  export ipv4 unicast map Internal03ToGlobal
  route-target export 1:4098
  route-target import 1:4098
 exit-address-family

route-map Internal03ToGlobal permit 10
 match ip address prefix-list Internal03ToGlobal

ip prefix-list Internal03ToGlobal seq 5 permit 192.168.1.0/24
ip prefix-list Internal03ToGlobal seq 6 permit 192.168.2.0/24
ip prefix-list Internal03ToGlobal seq 7 permit 172.16.4.4/30
```



Doctor client PC
192.168.2.68/32

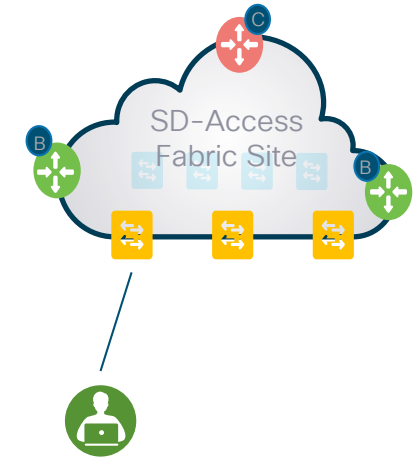
Return traffic – SDA side – classify traffic

```
border-1#show cts sxp sgt-map  vrf Internal03
SXP Node ID(generated):0xC0A80301(192.168.3.1)
IP-SGT Mappings as follows:
IPv4,SGT: <192.168.1.4 , 16:Doctors>
source  : SXP;
Peer IP : 172.16.201.205;
Ins Num : 1;
Status  : Active;
Seq Num : 7
Peer Seq: AC10C9CD,AC10C9D8,
IPv4,SGT: <192.168.1.5 , 17:Nurses>
source  : SXP;
Peer IP : 172.16.201.205;
Ins Num : 1;
Status  : Active;
Seq Num : 11
Peer Seq: AC10C9CD,AC10C9D8,
IPv4,SGT: <192.168.2.68 , 16:Doctors>
source  : SXP;
Peer IP : 172.16.201.205;
Ins Num : 1;
Status  : Active;
Seq Num : 13
Peer Seq: AC10C9CD,AC100261,
IPv4,SGT: <192.168.199.1 , 10001:E_commerce_WebEPG>
source  : SXP;
Peer IP : 172.16.201.205;
Ins Num : 1;
Status  : Active;
Seq Num : 3
Peer Seq: AC10C9CD,0A301645,
Total number of IP-SGT Mappings: 4
border-1#
```



Return traffic – SDA side – classify traffic

```
edge-1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 17:Nurses to group 16:Doctors:
        Permit IP-00
IPv4 Role-based permissions from group 10001:E_commerce_WebEPG to group 16:Doctors:
        Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE


edge-1#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          3500021    7260335    0          0
17      16      0          0          0          0          0          0
10001   16      0          0          0          3939       0          0
edge-1#
```



Egress policy on edge

Demo

ACI / SDA integration, the future

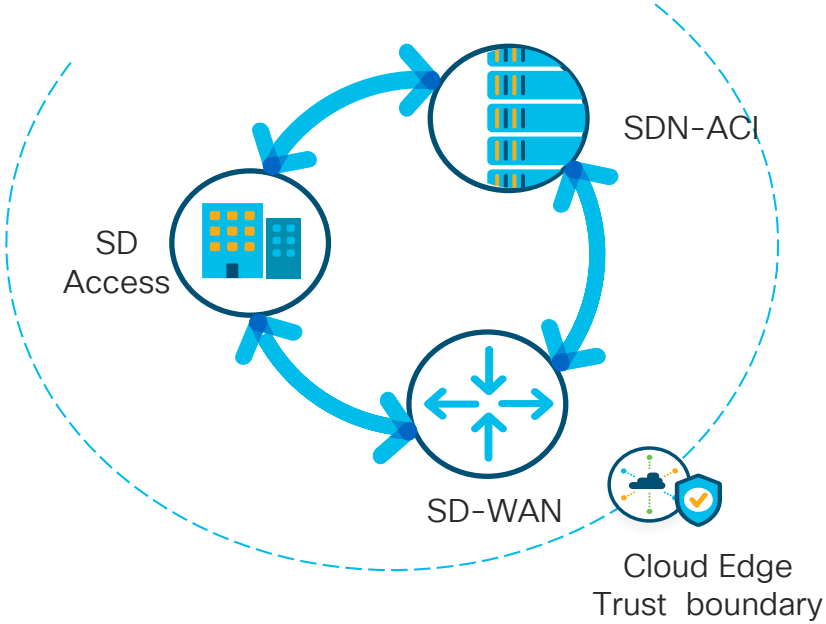
Our Direction

Policy

Automation

Telemetry, Analytics and Assurance

Security, Identity and Segmentation



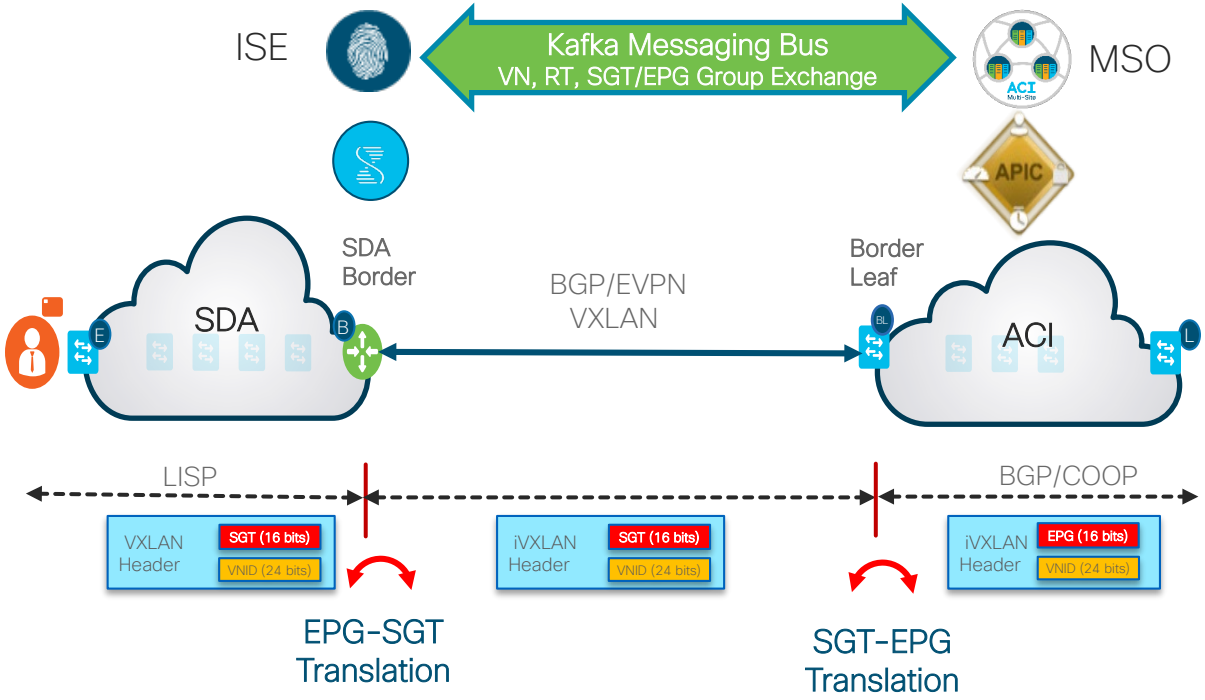
Disclaimer

- Phase 2 of ACI/SDA integration is currently planned for Q3CY20. As a consequence some of the specific implementation options described in the following slides may slightly change before FCS

Phase 2 SDA-ACI

Overall Architecture

Q3CY20



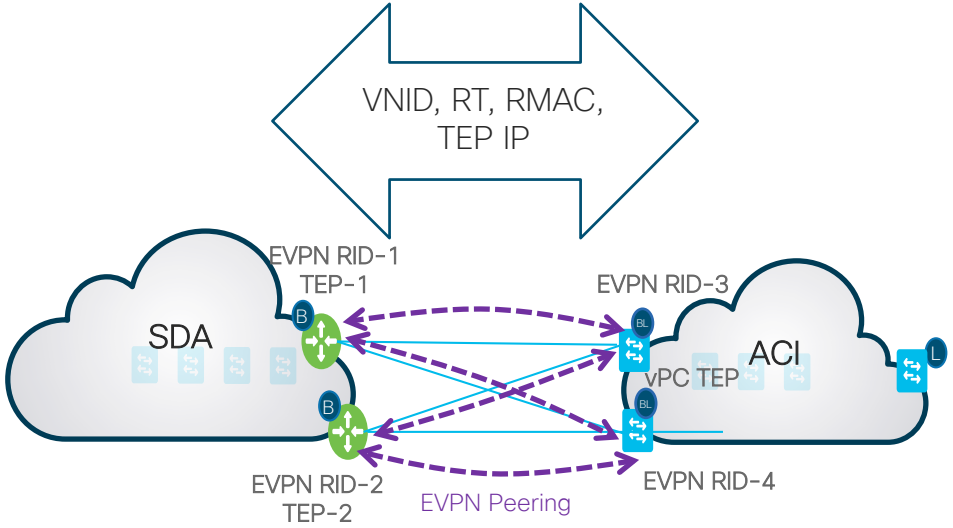
Area	Description
Policy Plane	• {VN, IP, group} sharing via Kafka Messaging Bus • Route Targets exchange between ACI and SDA (through ISE)
Control Plane	• BGP-EVPN with exchange of subnet information
Data Plane	• iVXLAN with group information • Endpoint data-plane learning on ACI BL nodes

Underlay Connectivity between SDA Border Nodes and ACI BL Nodes

Control Plane Considerations

Control Plane Considerations

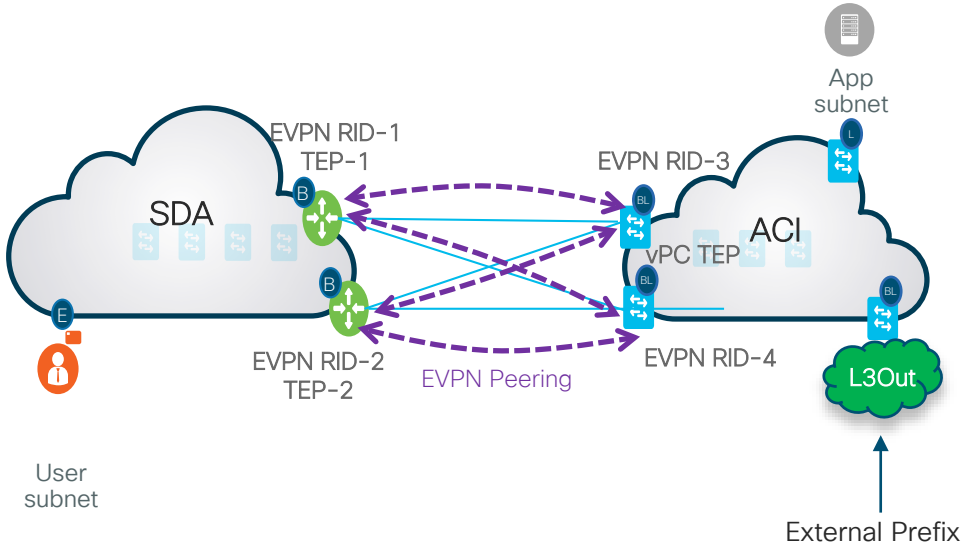
ACI-SDA BGP EVPN Peering



- BGP EVPN peerings to exchange prefix information for Campus and Application subnets
  - Full mesh BGP EVPN adjacencies between EVPN RIDs
- Information exchanged between border nodes:
  - VNIDs for the VRFs defined in each domain (downstream VNID assignment)
  - Route-Targets (RTs) value used to control import/export of prefixes into each VRF (Symmetric RT approach)
  - Router-MAC for the border node originating the prefix
  - TEP IP address to be used as next-hop
- VNID, RMAC, and TEP IP are used to construct VXLAN header for packets forwarded between SDA and ACI domains

Control Plane Considerations

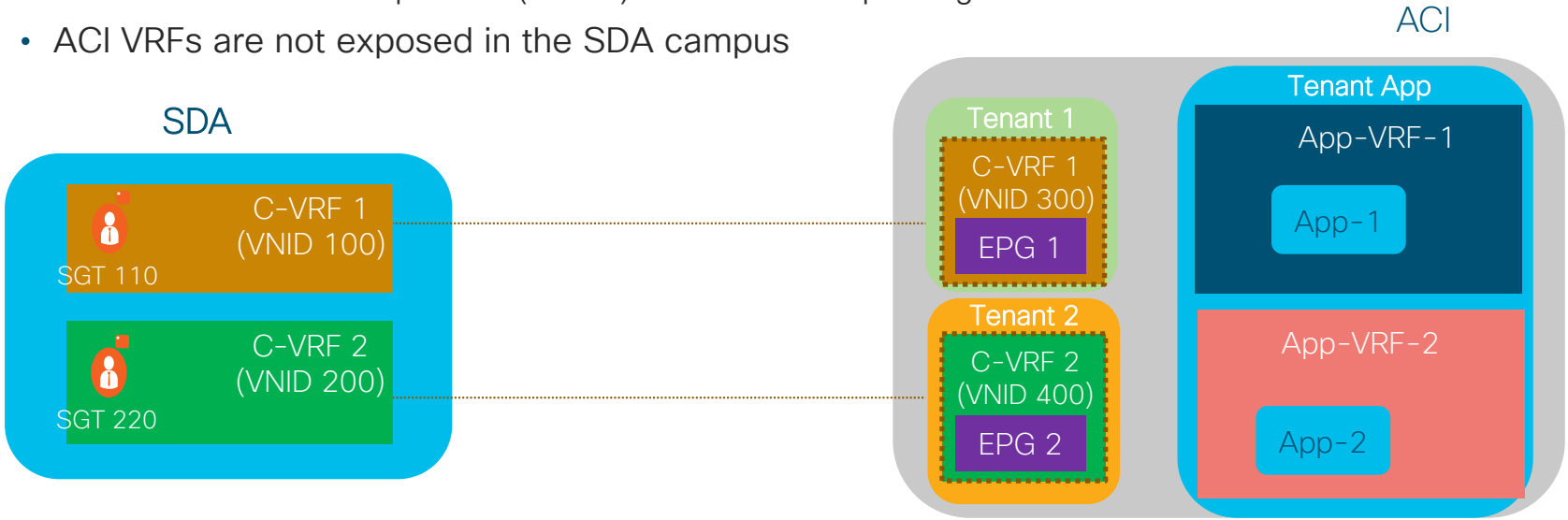
Route Exchange



- Routes are exchanged as EVPN type-5 routes with VNID of dedicated VRF
- Routes are imported within a domain based on the specific VRF RT import policies
- SDA border nodes push to ACI the subnets' routes for the users in the Campus requiring connectivity to the ACI services
- ACI BL nodes advertise the following routes to the SDA border nodes:
  - BD subnets for applications made available from ACI fabric
  - Prefix routes learnt in the ACI fabric from peers connected to other BL L3Outs
  - Specific /32 and /128 host routes for BDs that are stretched between ACI Pods/Sites (not at FCS)

Campus VRF Extension into ACI

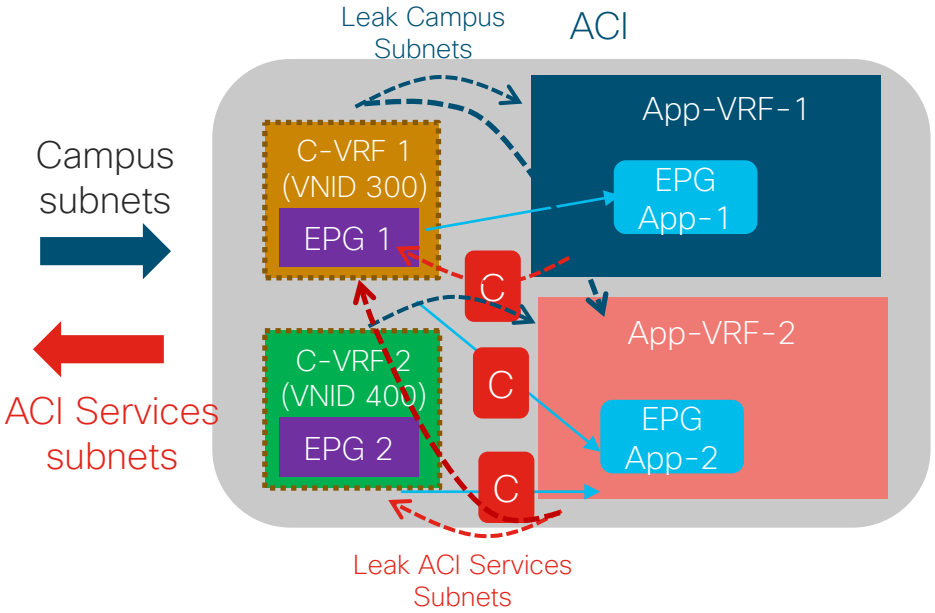
- Support multi-tenancy/multi-VRF design with minimal or no change to existing design on SDA and ACI side
- Allow campus to expose multiple VRFs to DC and ACI to expose apps from multiple VRFs to campus
  - SDA initiates a “Remote Tenant” setup in the ACI domain for each Campus VRF
  - For each defined Campus VRF (C-VRF) there is a corresponding C-VRF created on ACI
- ACI VRFs are not exposed in the SDA campus



Campus VRF Extension into ACI

Route-Leaking in ACI

- **Campus SG consuming an ACI Service:** in ACI is represented as a “shared service” contract between C-VRF and the VRF(s) of the different Application EPGs representing the ACI services
- The subnets representing the ACI services will be leaked into C-VRF on the ACI Border Leaf nodes and advertised toward the Campus through BGP EVPN
- Similarly, the campus Subnets are advertised from the SDA border nodes into the C-VRF in ACI through BGP EVPN and leaked into one or more application VRFs

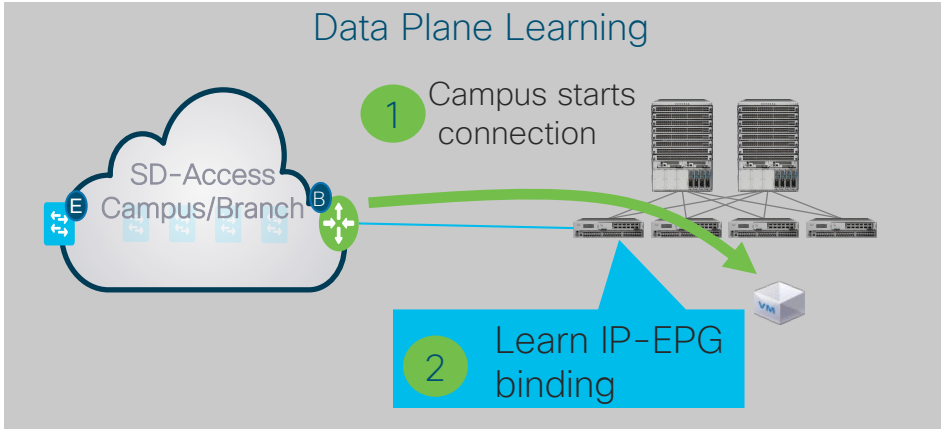


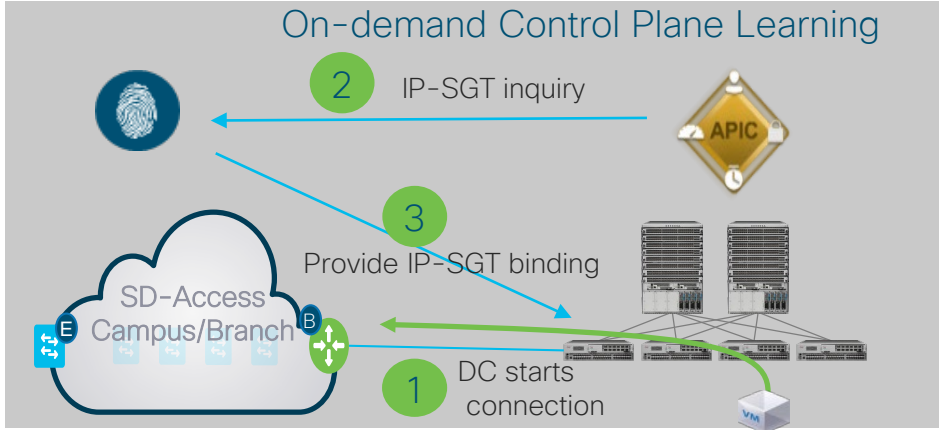
Data Plane Considerations

Phase 2 SDA-ACI

ISE-APIC/MSO Policy and Data Plane Learning

- Each campus SGT is represented as an External EPG in the ACI Border Leaf
- ACI BL learns the mapping of IP-SGT-EPG from data packet
  - Required because adjacent Campus IP addresses may be assigned to different SGTs
- Inquiry ISE for IP-SGT mapping when needed
  - E.g. when EP in ACI initiates the connection toward the campus
- Each domain can apply their policies independent of the other domain
  - On ACI the policy is always applied on the BL nodes (permit/deny/redirect to L4L7 graph, etc.)



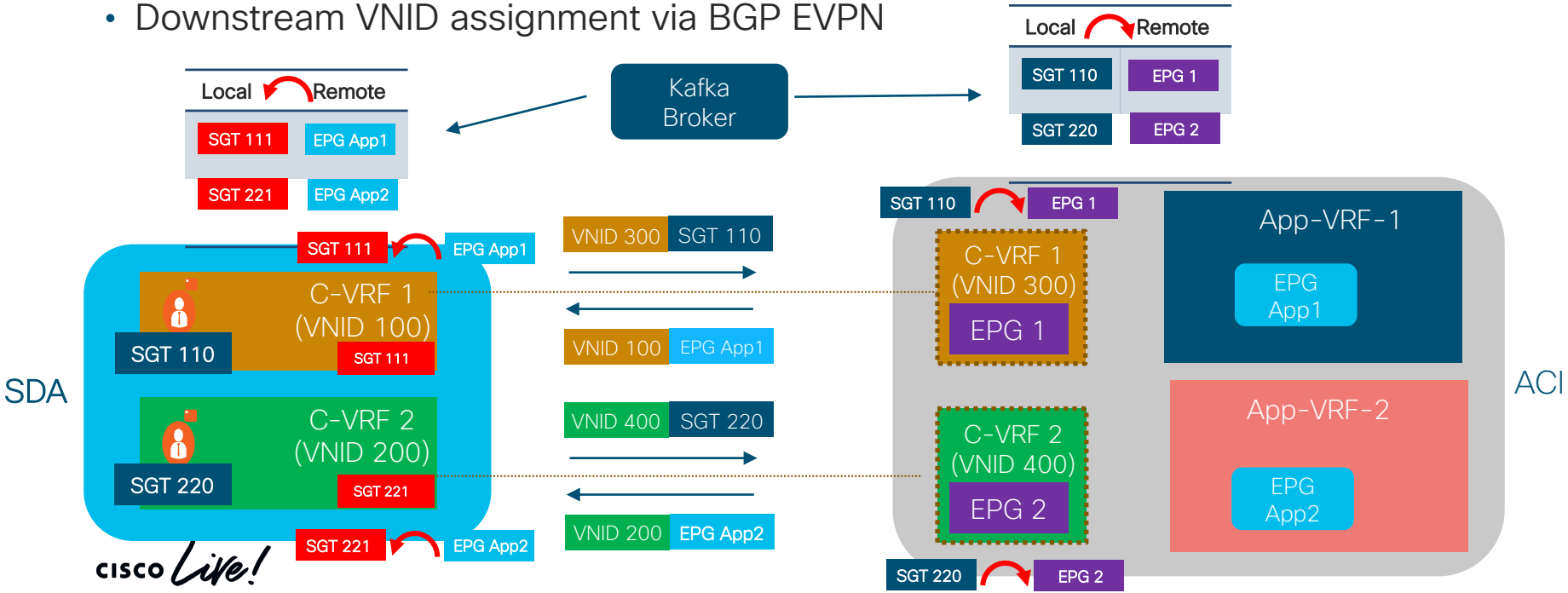


cisco Live!

Campus VRF Extension into ACI

Class-ID Translation between Domains

- Class-ID translations to keep SDA and ACI separated domain for resource allocation
  - Pushed into each domain via Kafka
- Downstream VNID assignment via BGP EVPN



Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**