

ACI – "not just another network..."

Steve Sharman, Technical Solutions Architect @sps2101

cisco ile



Agenda

- Setting the scene
- Network Centric vs Application Centric
- Greenfield vs Brownfield
- Converting from Network Centric to Application Centric
- Allowing open communication
- ESGs under the covers
- L4-L7 service integration
- External connectivity
- Increasing security
- Automated blueprints





Why are you here...?

cisco ive!

ACI - "just another network", or the foundation of an internal private cloud?

There are thousands of customers globally who have successfully deployed ACI fabrics and operate them as "just another network", but what if you could operate your ACI fabric as programmable private cloud infrastructure?

In this session we will look at how you can operate your ACI fabric as the foundation of an internal private cloud. We will look at how to migrate services onto an ACI fabric (network centric) and then implement segmentation (application centric). We will look at how to use Endpoint Security Groups to wrap security around endpoints within a VRF. We will then see how we can block East / West traffic within a hypervisor, and finally we'll dynamically add in firewalls to provide targeted L7 control.

If you're thinking this might prove time consuming to implement from the UI, we will show how all the configuration can be fully automated using Terraform.

Consuming an ACI fabric as "just another cloud" allows organisations choice on where to place workloads. Whether workloads are hosted in a public cloud, or on an on-premise private cloud, the consumption model should, and can, be the same.

Before we get started...





There are lots (and lots) of details in this presentation, please download through the Ciscolive app.

Well unless you have binoculars with you...!





lcons





lcons



*arrows indicate expected direction of traffic flow i.e. from consumer to provider



Icons - small



	EPG	name
L		
	C C	





C CCI I P EPG

name

vzAny

vzAny







name

name

C CCI I P ESG
name

name

C CCI I P ESG

name

Entry name



The ACI reference application from circa 2014...

cisco ile

The mythical three tier application...!



Our reference application for this presentation...

cisco life!

Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo



cisco live!

Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo



Source/Consumer	Target/Provider	Target/Provider Port		
cart	Redis cache	TCP 6379		
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051		
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051		
outside	frontend	TCP 80/8080		
recommendation	product catalog	TCP 3550		

cisco live!

Who hasn't heard of "the journey to the cloud" ...?



AWS reference architecture

https://docs.aws.amazon.com/vpc/latest/userguide/extend-intro.html



cisco live!

Network Connectivity and Security are mandatory in the cloud...

cisco Life!

Different clouds run different hypervisors



AWS has completely re-imagined our virtualization infrastructure. Traditionally, hypervisors protect the physical hardware and bios, virtualize the CPU, storage, networking, and provide a rich set of managem capabilities. With the Nitro System, we are able to break apart those functions, offload them to dedicat hardware and software, and reduce costs by delivering practically all of the resources of a server to you instances.

Hypervisor security on the Azure fleet

Article • 11/11/2022 • 3 minutes to read • 4 contributors

In this article

Strongly defined security boundaries enforced by the hypervisor Defense-in-depth exploit mitigations Strong security assurance processes

Next steps

The Azure hypervisor system is based on Windows Hyper-V. The hypervisor system enables the computer administrator to specify guest partitions that have separate address spaces. The separate address spaces allow you to load an operating system and applications operating in parallel of the (host) operating system that executes in the root partition of the computer. The host OS (also known as privileged root partition) has direct access to all the physical devices and peripherals on the system (storage controllers, networking adaptions). The host OS allows guest partitions to share the use of these physical devices by exposing "virtual devices" to each guest partition. Thus, an operating system executing in a guest partition has access to virtualized peripheral devices that are provided by virtualization services executing in the root partition

The Azure hypervisor is built keeping the following security objectives in mind:

Objective Source

A security policy mandates no information transfer between VMs. This constraint requires capabilities in the Virtual Isolation Machine Manager (VMM) and hardware for isolation of memory, devices, the network, and managed resources such as persisted data.

VMM To achieve overall system integrity, the integrity of individual hypervisor components is established and maintained. integrity

Google Cloud

7 ways we harden our KVM hypervisor at Google Cloud: security in plaintext

January 25, 2017

Andy Honig Senior Product Manager

Nelly Porter Group Product Manager, Google Cloud

18

le Cloud uses the open-source KVM hypervisor that has been validated by scores of researchers e foundation of Google Compute Engine and Google Container Engine, and invests in additional rity hardening and protection based on our research and testing experience. Then we contribute our changes to the KVM project, benefiting the overall open-source community.

t follows is a list of the main ways we security harden KVM, to help improve the safety and security ir applications.

active vulnerability search: There are multiple layers of security and isolation built into Google's M (Kernel-based Virtual Machine), and we're always working to strengthen them. Google's cloud urity staff includes some of the world's foremost experts in the world of KVM security, and has overed multiple vulnerabilities in KVM, Xen and VMware hypervisors over the years. The Google

cisco / ille













A cloud operating model succeeds best when there is a new organizational culture...

cisco ile

Cloud operating models have changed the way that security is implemented...

cisco ile

With a cloud operating model, security rules are typically declared with the application constructs...

cisco ile

Conversely, within enterprise Data Centers security has been implemented by network and/or security administrators at a VRF boundary...

cisco

Traditional Enterprise Security Model



Traffic is routed to physical firewall which typically becomes a throughput pinch point with thousands of rules



ACI is the foundation for an internal private cloud...!



Day0 automation out-of-thebox; physical fabric and underlay



Hybrid cloud capability; public cloud-like networking constructs Single API Model for 100s of switches and 1000s of ports; cloud-like consumption model

Per-application

service-chaining



Pervasive Security Model



Infrastructure as Code with Ansible and Terraform



Network Centric vs Application Centric





What does **Google** say about the different modes...?

Google	Cisco ACI what is the difference between network centric and applica $~ imes~~ ~ \downarrow~~$ $oldsymbol{ar{e}}~~$ Q					
	Q All 🔚 Images 🕞 Videos 🖻 News 🖺 Books 🗄 More To	ols				
	About 157,000 results (0.48 seconds)					
	Network Centric approach allows existing network architecture and flows to remain the same, henceforth allowing IT resources enough period to get acclimatized with the new terminologies of ACI fabric. Application Centric approach is comparatively a new approach model where application tiers are defined by EPGs . https://ipwithease.com > Blog : Cisco ACI Network Centric vs Application Centric approach @ About featured snippets • II Feedb	ack				
	What is application centric infrastructure ACI?					
	What is network centric application?					
	What are the 3 core components of ACI Architecture? How Cisco application centric infrastructure ACI is related to SDN and how it differs?					
	Feedb	ack				
	https://community.cisco.com > application-centric > td-p					
	Difference between ACI network centric mode and application					
	Application centric is another way of thinking. Instead of having the network lead the					
	application leads. This results into a network 'bubble' (for lack of					
	https://community.cisco.com > application-centric > td-p :					

ACI network centric vs app centric - Cisco Community Application-centric mode: Application-centric mode gives ACI users the highest level of visibility and security. In this mode, we define groups and contracts ...

oogle	site:cisco.com Cisco ACI what is the difference between network cent $~ imes~~ ~ \downarrow ~$ 💿 $~$ Q							
	Q All 및 Images I Videos 圖 News [1] Books : More Tools							
	About 21,100 results (0.45 seconds)							
	https://community.cisco.com > application-centric > td-p							
	Difference between ACI network centric mode and application							
	Application centric is another way of thinking, Instead of having the network lead the application leads. This results into a network 'bubble' (for lack of							
	https://community.cisco.com > application-centric > td-p							
	ACI network centric vs app centric - Cisco Community							
	Application-centric mode: Application-centric mode gives ACI users the highest level of							
	visibility and security. In this mode, we define groups and contracts							
	https://www.cisco.com > networking > cloud-networking							
	Cisco ACI - Application Centric Infrastructure							
	Configure, operate, and analyze everything connected to your data center and cloud networks, all from one place. Connect to Cisco Nexus Dashboard. ★★★★★ Rating: 5 · 86 reviews							
	https://www.cisco.com > data-center-virtualization PDF :							
	Network Centric to ACI Centric Migration - Cisco							
	The Network-Centric model serves many customers well; it allows them to migrate their existing compute/applications/ network into ACI in a way that is familiar. 5 pages							
	https://community.cisco.com > application-centric > td-p :							
	Solved: ACI Network Centric to Application Centric Migration							
	Nov 27, 2019 — Solved: We are planning to migrate our existing infrastructure to ACI in few							
	steps. First to a Network Centric setup (EPG=VLAN=BD) with a L2							
	https://www.cisco.com > Solutions > Data Center :							
	Application Centric Infrastructure (ACI) - Data Center - Cisco							
	This solution provides automated network connectivity, consistent policy management, and simplified operations for multicloud environments. Unlock the full							

cisco (

What does **Google** say about migration from one mode to another...?

Google	Cisco ACI migrate from network centric mode to application centric mode 🛛 🗶 🏮 ९					
	Cisco ACI migrate from network centric mode to application centric mode × thtps://unofficialaciguide.com > 2017/09/08 > network : Network Centric to ACI Centric Migration Unofficial ACI Guide Sep 8, 2017 — Map existing Vians into ACI in Network-Centric Mode (L2 only – no contracts) – Create legacy EPGs and BDs on the ACI Fabric. · Create L3out for https://ipwithease.com > Blog : Cisco ACI Network Centric vs Application Centric approach Network Centric approach is considered a soft transition for customers from traditional architecture to ACI architecture. · On the other hand, Application https://www.youtube.com > watch : [HD] Cisco ACI Brownfield Network Centric to Application					
	a legacy aka brownfield environment to a Cisco ACI fabric usin YouTube · Ralph Carter · Dec 2, 2019					
https://www.linkedin.com > pulse > clsco-aci-network-cen : Cisco ACI – Network Centric vs. Application Centric Approach Jun 30, 2019 — The network-centric approach is preferred when migrating the network from legacy/traditional networking to SDN based model. This is to ensure https://www.wwt.com > > Data Center Networking : Demystifying ACI Application Centric "Mode" Through WWT Dec 15, 2020 — Network Centric is simple and straightforward VLAN, endpoint groups (EPG) and bridge domains (BDs) are mapped in a 1-to-1 relationship, hence						

Google site:cisco.com Cisco ACI migrate from network centric mode to applic X 🤳 🧔 Q

🔍 All 🗈 Videos 📱 Books 🔛 Images 🗉 News 🗄 More

About 5,050 results (0.37 seconds)

https://www.cisco.com > data-center-virtualization PDF

Network Centric to ACI Centric Migration - Cisco The Network-Centric model serves many customers well; it allows them to migrate their existing compute/applications/ network into ACI in a way that is familiar. 5 pages

https://community.cisco.com > data-center-blogs > ba-p :

All About Migration: Network Centric to ACI Centric Model Apr 12, 2019 — All legacy vlans that will be a part migrated to the ACI-Centric application exist on the fabric (or will be operational prior to the migration ...

https://www.cisco.com > ... > Technical References

Migrating Existing Networks to Cisco ACI Dec 23, 2015 — The recommended approach for a **network centric migration** consists of associating each VLAN originally defined in the brownfield infrastructure ...

https://community.cisco.com > application-centric > td-p

Difference between ACI network centric mode and application ... hai guys, I have deploy ACI infrastructure on my customer, currently using network centric mode. Later, it will be converted to application centric mode.

https://www.cisco.com > networking > cloud-networking

Cisco ACI - Application Centric Infrastructure Configure, operate, and analyze everything connected to your data center and cloud **networks**.

all from one place. Connect to **Cisco** Nexus Dashboard.

Read solution overview \cdot White Papers \cdot Cisco APIC \cdot Simulator

https://community.cisco.com > application-centric > td-p : ACI network centric vs app centric - Cisco Community Or, if the network is left in zero-trust mode, the contracts used will be very open, allowing all

cisco / ile

Where should we start...?







Design Considerations...

cisco ive!



Used for functions which are accessible from any Tenant



Typically, fewer larger subnets which can be (optionally) shared across Tenants



Dedicated subnets for tenants with VRFs that can be (optionally) shared by different Tenants





Each Tenant has their own IP Range

					All Tenants			
derived and the second				Name	Alias		Description	
System Tenants	System Tenants Fabric Virtual Networking Admin Operations Apps Integrations				Name	Allas		Description
ALL TENANTS Add Tena	ant Tenant Search: name or descr	common ciscolive-07 rwhitear shared	-services ciscolive-08		shared-services		IP range per Tenant	-3out and shared devices
All Tenants					aci-infrastructure	<u> </u>		Nexus Dashboard, MSO etc
Name	Alias	 Description 	Bridge Domains	VRFs	ciscolive-01		-	Routable IP range 10.0.11-15.x
shared-services		L3out and shared devices	0	1				
aci-infrastructure		Nexus Dashboard, MSO etc	1	0	ciscolive-02			Routable IP range 10.0.21-25.x
ciscolive-01		Routable IP range 10.0.11-15.x	5	1				
ciscolive-02		Routable IP range 10.0.21-25.x	0	1	ciscolive-03			Routable IP range 10.0.31-35.x
ciscolive-03		Routable IP range 10.0.31-35.x	0	1				Doutoble ID range 10.0.41.45 v
ciscolive-04		Routable IP range 10.0.41-45.x	0	1	CISCOIIVE-04			Routable IP range 10.0.41-45.x
ciscolive-06		Routable IP range 10.0.61-65.x	0	1	ciscolive-05			Routable IP range 10.0.51-55.x
ciscolive-07		Poutable IP range 10.0 71–75 x	6	1				risatasis in tange referer sent
Terraform		Rouable in Tange 10.0.71-75.x	5	1	ciscolive-06			Routable IP range 10.0.61-65.x
Terraform		Routable IP range 10.0.81-85.x	5	1				
ardica		Routable IP range 192.168.0-5.x	0	1	CISCOIVE-07			Routable IP range 10.0.71-75.x
rwhitear		Routable IP range 192.168.10-15.x	6	1	Terraform			
ngorse		Routable IP range 192.168.120-125.x	1	1	ciscolive-08			
demo		Routable IP range 192.168.150-155.x	3	1	Terraform			Routable IP range 10.0.81-85.x
fgandola		Routable IP range 192.168.151-158.x	11	2				
roxadiaz		Routable IP range 192.168.20-25.x	6	1	ardica			Routable IP range 192,168.0-5.x
ndsouzar		Routable IP range 192.168.30-35.X	1	0				
adealdag		Routable IP range 192,168,40-45,x	6	1	rwhitear			Routable IP range 192.168.10-15.x
ssharman		Routable IP range 192.168.50-56.x	7	1				
mgmt		Routable IP range 192.168.6.x	1	2	ngorse			Routable IP range 192.168.120-125.x
movaswan		Routable IP range 192.168.60-65.x	6	1	1	♥ Healthy		
adossant		Routable IP range 192.168.70-75.x	0	1	0	♥ Healthy		
fdagenha		Routable IP range 192.168.80-85.x	0	1	0	♥ Healthy		
ylouis		Routable IP range 192.168.90-95.x	0	1	0	♥ Healthy	_	
C Page 1 Of 1			Objects Per Page: 100			Displaying Objects 1 - 3	2 Of 32	
Last Login Time: 2022-11-26T07:06	UTC+00:00					Current System Time: 2022-11-26T07:59	UTC+00:00	

cisco live!



Convert Brownfield Network Centric environment to Application Centric environment

Network engineers "view" of their ACI environment...

cisco ile
Workloads identified by IP and Mac address



What does the application owner care about...?

cisco live!

DNS names, IP addresses, Default Gateways, and Security Rules...

cisco ile

Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo



cisco live!

Online Boutique

https://github.com/GoogleCloudPlatform/microservices-demo



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550



Endpoints span subnets



Let's convert to "Application Centric" mode



You can convert from Network Centric mode to Application Centric mode in Two Steps...

cisco ile

Step 1: Create Application Profiles and Security Groups



Step 2: Create ACI Tags to match vCenter Tags



Endpoints automatically move to new Security Group



BRKDCN-2984

cisco live!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 47

Automated conversion to "Application Centric"

cisco APIC								ssharmar			
System Tenants Fabric Virtual ALL TENANTS Add Tenant Tenant Search:	Networking Admin Op name or descr I comm	perations Apps Integrations non demo fgandola ssharman s	shared-services								
This object was created from the Terra	aform orchestrator. It is recomme	nded to only make changes from the Terrafor	m orchestrator.								
demo (È ा) (È () () () () () () () () () () () () ()	Endpoints r "network-se through EPG	napped to the egments" ESG → ESG mapping				Summary	y Policy	Operational	Health	Faults History)
Application Profiles						Client E	indpoints (Contracts I	Deployed Leaves	Tag Selectors	
Application EPGs Useg EPGs	MAC/IP	Endpoint Name	Learning Source	Hosting Server	Interface (learned)	Encap	Base EPG		Policy Tags	0 1	1
Endpoint Security Groups	> 🗐 00:50:56:A1:1A:60	tn-demo-online-boutique-ad-service	learned vmm	10.237.98.165	Pod-1/Node-101/eth1/29 (learned	vlan-1038(P) vlan-1064(S)	demo:network segments:192	<u>-</u> .168.150.0_24	vmm::vmn	ame tn-demo-ad-servio	ic
> R network-segments	 ✓ ■ 00:50:56:A1:3F:2C 	tn-demo-online-boutique-frontend-service	learned vmm	10.237.98.168	Pod-1/Node-101/eth1/32 (learned	vlan-1020(P) vlan-1021(S)	demo:network segments:192	<u>-</u> .168.152.0_24	vmm::vmn	ame tn-demo-frontend-	i.
> 🖿 Networking	192.168.152.101						demo:network segments:192	<u>-</u> .168.152.0_24			L
	> 00:50:56:A1:7F:0B	tn-demo-online-boutique-checkout-service	learned vmm	10.237.98.168	Pod-1/Node-102/eth1/32 (learned	vlan-1017(P) vlan-1018(S)	demo:network segments:192	<u>-</u> .168.151.0_24	vmm::vmn	ame tn-demo-checkout	л
> Services	> = 00:50:56:A1:7F:A5	tn-demo-online-boutique-redis-cart	learned vmm	10.237.98.166	Pod-1/Node-102/eth1/30 (learned	vlan-1017(P) vlan-1018(S)	demo:network segments:192	<u>-</u> .168.151.0_24	vmm::vmn	ame tn-demo-redis-car	a
Security	> 00:50:56:A1:8E:DB	tn-demo-online-boutique-payment-service	learned vmm	10.237.98.167	Pod-1/Node-101/eth1/31 (learned	vlan-1038(P) vlan-1064(S)	demo:network segments:192	<u>-</u> .168.150.0_24	vmm::vmn	ame tn-demo-payment	ŀ
	> 🖹 00:50:56:A1:8F:09	tn-demo-online-boutique-shipping-service	learned vmm	10.237.98.166	Pod-1/Node-101/eth1/30 (learned	vlan-1020(P) vlan-1021(S)	demo:network segments:192	<u>-</u> .168.152.0_24	vmm::vmn	ame tn-demo-shipping -	P.
	I Page 1	Of 1 > >			Objects Per Page: 100 🗸				Displa	ying Objects 1 - 11 Of 11	Γ
Last Login Time: 2023-02-03T07:03 UTC+00:00			ssharman@ss	harman-jumphost:~		_	-	-	Current System Time	: 2023-02-03T08:07 UTC+00	0:00 . % 1
ssharman-jumphost ~ → ping 192.168.152.101											

cisco ile



Allowing open communication in a Brownfield environment...

There are four options...

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html#Migrationexample

- vzAny
- Preferred Groups
- EPGs mapped Endpoint Security Groups
- Disable security (not covered, because why would you...?)

vzAny operation - consumer and provider

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html



cisco live!

Preferred Groups

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Use_vzAny_to_AutomaticallyApplyCommunicationRules_toEPGs.html



EPGs mapped to Endpoint Security Groups



Let's step back and look at the impact of the changes...

cisco ile

Bridge Domain to EPG Mapping



Isolated groups of workloads





BRKDCN-2984 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 56

Each EPG has a unique security Tag (pcTag)











cisco livel

ESGs allow control E/W traffic within the Hypervisor



Let's create an EPG matched Security Group...

cisco ile

Create EPG matched Security Group





Create Application Profile for Security Groups



cisco / ile !

Create new ESG for Network Segments





Matched EPGs now classified with a common pcTag







cisco ivel

Let's add the remaining EPG to the Security Group...

cisco ive!

Add remaining EPG to Single Security Zone



All EPGs now classified with a common pcTag









What if there is an intermediary switch layer...?

cisco ile

Define static PVLANs for VMM Domains



Specify PVLANs for VMM domain



Security across Bridge Domains with ESGs





EPG Security vs ESG Security



ESG contracts supersede EPG contracts

cisco / ille


How do you map Endpoints into an ESG...?

cisco ile

Select a Design Pattern, then enable Proxy ARP and map your Endpoints to the ESG...

cisco ile

Design Patterns



EPG and ESG in the "user" Tenant with a dedicated L3out



EPG and ESG in the "user" Tenant with a Shared L3out



Design Patterns





How do you enable Proxy ARP on the Leaf Switches...? Enabling "Allow Micro-Segmentation" Edit VMM Domain Association - VMware/ucsc-c220m5-vds-01 automatically enables Proxy ARP. Deploy Immediacy: (Immediate Option in a 100% virtual deployment, use Delimiter with or without Intra EPG isolation Enhanced Lag Policy: select an option ow Micro-Segmentation: Untagged VLAN Access: demo VLAN Mod Static Additional demoinetwork-segments 192.168.150.0_24 ACTIONS V Static Binding Enhemera Port Binding: Dynamic Binding C ▶ Quick Start Enable Summary Monitor Configure Permissions Ports Hosts VMs Netflow demo Allow Promiscuous: Reject Port binding Static binding Forged Transmits: Reject Port allocation Elastic \sim \sim Application Profiles MAC Changes: Reject VLAN ID 1046 Active Uplinks Order epg-matched-security-groups Standby Uplinks ✓ ▲ network-segments Custom EPG Name: A demo|network-segments|192.168.150.0 24 ACTIONS V \$\$ 192.168.150.0_24 Name: 192.168.150.0_24 Alias Summary Monitor Configure Permissions Ports Hosts VMs 192.168.151.0_24 Description: optional Port binding Static binding > 👫 192.168.152.0_24 Port allocation Elastic Annotations: Private VLAN Isolated (1094, 1095) > 🚞 uSeg EPGs Global Alias: -Enable Intra EPG isolation with uSeg EPG: false 🗧 🧮 Endpoint Security G cTag(sclass): 16390 Proxy ARP if you have a mixed ception Tag Enabling Intra EPG isolation / Allow Microvirtual and physical environment QoS class: Level3 (Default) Segmentation configures PVLANs on the Custom QoS: select a value Data-Plane Policer: select a value port group Intra EPG Isolation: Unenforced orwarding Control: 🗹 proxy-an Include Add an Intra EPG Proxy ARP is only available Flood in Encapsulation: Enabled when Intra ESG isolation is Contract Name Tenant Contract Type enabled Generation Contract Type: Intra EPG Contract cisco ile permit-any dem © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 77 BRKDCN-2984

Tag vs Static Mapping



78



Static Mapping of EPGs to ESGs



cisco live!



cisco live!

BRKDCN-2984

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 81

Selector Precedence

For Switched Traffic:

Precedence Order	Selector		
1	Tag Selector (Endpoint MAC Tag) Tag Selector (Static Endpoint)		
2	Tag Selector (VMM Endpoint MAC Tag)		
3	EPG Selector		

For Routed Traffic:

Precedence Order	Selector			
1	Tag Selector (Endpoint IP Tag) IP Subnet Selector (host IP)			
2	Tag Selector (BD Subnet) IP Subnet Selector (subnet)			
3	Tag Selector (Endpoint MAC Tag) Tag Selector (Static Endpoint)			
4	Tag Selector (VMM Endpoint MAC Tag)			
5	EPG Selector			



ESG Contract Matrix

Source/Destination	Source/Destination*	Supported
ESG	ESG	Yes
ESG	EPG	No**
ESG	L3out extEPG	Yes
ESG	Shared L3out extEPG	Yes
ESG	Preferred Group	No
ESG	vzAny	Yes

*includes L4-L7 Service Graphs **use EPG → ESG mapping

cisco ive!

ESGs: The Hidden Details



Policy Tags on BD Subnets (subset of a subnet)

- If only a subset of the BD subnet needs to be classified to an ESG, you can configure a smaller subnet in the same BD with "No Default SVI Gateway" option. Then attach a policy tag to the smaller subnet.
- "No Default SVI Gateway" prevents the additional subnet with this config from being deployed as an SVI on leaf nodes.

NOTE:

this config still deploys a BD route pointing to spineproxy for 192.168.1.0/30. Although this itself doesn't impact any forwarding behavior, it consumes an LPM table entry.

If many of such configs are expected, consider using IP subnet selectors instead which doesn't deploy any routes, hence no impact to the LPM table.





Tag selector (with BD subnets) or IP Subnet selector? <u>Tag selector (new)</u> IP Subnet selector (existing)

When non-IP based classifications need to be used together.

 One tag selector can manage endpoints through different types of criteria (objects)



When the BD is under tenant common while the EPGs and ESGs are in a user tenant.

Tag selectors match policy tags only within the same tenant. Use IP subnet selectors instead.



Policy Tags on endpoint IPs

- It is difficult to assign a policy tag on each endpoint directly because endpoints are dynamically learned and aged out.
- APIC 5.2(1) introduced a new object (Endpoint IP Tag) to represent an endpoint IP address so that policy tags can be assigned and maintained even when the endpoint is not learned yet, or even after the endpoint ages out.
- By matching a policy tag assigned to an endpoint IP tag, a tag selector can classify the specific endpoint IP address to an ESG in the same VRF.

<u>Guidelines:</u>

• The Endpoint IP Tag must be in the same tenant and the same VRF as the ESG.

Limitations:

• This only classifies IP addresses, not MAC addresses. See the L2 Traffic Limitation with IP-based selector slide for its impact.





Policy Tags on endpoint MACs

- It is difficult to assign a policy tag on each endpoint directly because endpoints are dynamically learned and aged out.
- APIC 5.2(1) introduced a new object (Endpoint MAC Tag) to represent an endpoint MAC address so that policy tags can be assigned and maintained even when the endpoint is not learned yet, or even after the endpoint ages out.
- By matching a policy tag assigned to an endpoint MAC tag, a tag selector can classify the entire endpoint (MAC and associated IPs) to a given ESG in the same VRF.

Guidelines:

• The Endpoint MAC Tag must be in the same tenant and the same VRF as the ESG.





Policy Tags on VMM endpoint MACs

- APIC 5.2(1) introduced a new object (VMM Endpoint MAC Tag) to represent an endpoint MAC address discovered through VMM integration.
- APIC will translate some information of VMs through VMM integration into ACI policy tags. Supported on 5.2(1):
 - VMware VM name
 - (key: __vmm::vmname, value: <VM name>)
 - VMware Tag
 - (key: <category>, value: <tag name>)
- By matching a policy tag assigned to a VMM endpoint MAC tag, a tag selector can classify the entire endpoint (MAC and associated IPs) to a given ESG in the same VRF.

Guidelines:

• The VMM Endpoint MAC Tag must be in the same tenant and the same VRF as the ESG.





Policy Tags on Static Endpoint

- Essentially the same as Endpoint MAC tags.
- APIC allows users to configure policy tags directly on an existing static endpoint instead of configuring another object (Endpoint MAC tag) for the same MAC.
- If you prefer managing all policy tags for static and non-static endpoints in one location (Endpoint MAC tag), you can configure an Endpoint Mac tag for the static endpoint MAC instead of assigning policy tags on static endpoint config.

Guidelines:

- The static endpoint with policy tags must be in the same tenant and the same VRF as the ESG.
- Only type silent host is supported.
- Configuring policy tags on both static endpoint and Endpoint MAC tag for the same MAC is not allowed.





L2 Traffic Limitation with IP-based selectors

• <u>Scenario 1:</u>

- MAC_A is matched by a selector of ESG 1
- IP_A is _not_ matched by any ESG

• <u>Result:</u>

Both MAC_A and IP_A are classified to ESG 1

• <u>Scenario 2:</u>

- MAC_A is matched by a selector of ESG 1
- \cdot IP_A is matched by a selector of ESG 2

• <u>Result:</u>

- MAC_A is classified to ESG 1
- \cdot IP_A is classified to ESG 2



• <u>Scenario 3:</u>

- MAC_A is _not_ matched by any ESG
- IP_A is matched by a selector of ESG 2
- <u>Result:</u>
 - MAC_A is _not_ classified to any ESG, and still belongs to the original EPG.
 - IP_A is classified to ESG 2

When only IP-based selectors are used, MAC addresses are not classified to ESGs.

- Switching traffic (i.e. within the same subnet) will not use ESG contracts even if its payload has the IP address classified to an ESG.
- If the two IPs in the same subnet from the same EPG are classified to different ESGs, those two endpoints can still talk freely through the MAC and its original EPG.

Workarounds for L2 Traffic Limitation

Proxy ARP (on all original EPGs)

• Proxy ARP makes sure that all traffic from the EPGs will be handled as a routing traffic. This means that all traffic uses the pcTag of IP. It does no longer matter whether the MAC still belongs to the original EPG.

How to enable Proxy ARP:

- Flood in Encapsulation
 - There is no functional difference if there is only one VLAN/EPG per BD. **Proxy ARP is enabled automatically** when Flood in Encapsulation is enabled.
- Intra EPG Isolation
 - when all endpoints are classified to ESGs, or when any endpoints that are still in original EPGs should not talk with anyone even in the same EPG.
 Proxy ARP needs to be explicitly enabled on top of Intra EPG Isolation.
- Intra EPG contract
 - If you want to set a default rule for communications between any endpoints that are still in original EPGs. If you want to allow such communications, use permit all contract.
 Proxy ARP is enabled automatically when an intra EPG contract is configured for an EPG.
- Allow Microsegmentation for VMM integration
 - Proxy ARP is enabled automatically when Allow Microsegmentation is enabled on VMM domain association.

Prepare the fabric for L4–7 Service Insertion





ACI Endpoint Update App (optional)

https://dcappcenter.cisco.com/aci-endpoint-update.html

alialia cisco	APIC (aci-dev-01)							
System	Tenants Fabric Virtual Network	king Admin Operation	s Apps Integrations					
		Installed A	apps Faults Downloads					
Apps								
	ELAM Assistant by Cisco Help you perform ELAM(Embedded Logic Analyzer Module) on ACI nodes to capture a single packet at a time and analyze where the packet goes.	ACI Endpoint Update by Cisco Pushes dynamic en from APIC to Secure Secure Firewall Mar	dpoint information e Firewall ASA and hagement Center back	us Insights Cloud nector isco us Insights Cloud Connector (3.x or er) implements Direct Streaming Nexus Cloud capable telemetry tionality. These services perform end functions only and do not have				
	Open	Open	Firewall Managemer	nt Center Overview Analys	sis Policies Device:	o Objects Integration	Deploy Q 🔮 🌣 🔞 ss	sharman 🔻 🕂
0		O O	AAA Server Access List	Dynamic Objects			T demo	× 🕂
			> Address Pools	Name	Descriptic	n	Number of Mapped IPs	
			Application Filters	APIC_DEMO_EPG-MATCHED-SECURIT	Y-GROUPS_ESG		3	Ø 🖍 🗑
			AS Path	APIC_DEMO_NETWORK-SEGMENTS_1	92.168.150.0_24		1	@ 🖍 🗑
			Cipher Suite List	APIC_DEMO_NETWORK-SEGMENTS_1	92.168.151.0_24		1	@ 🖍 🗑
			Community List	APIC_DEMO_NETWORK-SEGMENTS_1	92.168.152.0_24		1	@ 💉 🗑
			Distinguished Name DNS Server Group External Attributes Dynamic Object Security Group Tag					
С	isco ile						iston All rights recorded Cia	na Dublia 04

BRKDCN-2984 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

94

Where should you place your L4-7 devices...?

cisco ile

"common" tenant, "shared-services" tenant, or "workload/user" tenant...

cisco ile

Virtual firewall deployment





Benefits of virtual firewall / IPS

- One or more virtual firewalls exported to "user" tenants as required
- Virtual firewalls used for targeted service insertion
- Firewall throughput matches application requirements
- Firewall ruleset reduced to application requirements
- Firewall security group members pushed/pulled from APIC (where available)

Step 1: Define the Policy Based Redirect Target

 (\mathbf{f})





Step 2: Define Service Graph Template and Device Selection Policy



Step 3: Apply Service Graph to Contract Subject



External Connectivity...



Each Tenant has their own IP Range

					All Tenants		
					-		
CISCO APIC (aci-dev-01)					Name	Alias	 Description
System Tenants Fabric Virtual Networking Admin Operations Apps Integrations ALL TENANTS Add Tenant Tenant Search: mame or descr common ciscolive-07 rwhitear shared-services ciscolive-08					shared-services		L3out and shared devices
All Tenants					aci-infrastructure		Nexus Dashboard, MSO etc
Name	Alias	 Description 	Bridge Domains	VRFs	ciscolive-01		Routable IP range 10.0.11-15.x
shared-services		L3out and shared devices	0	1			Ŭ
aci-infrastructure		Nexus Dashboard, MSO etc	1	0	ciscolive-02		Routable IP range 10.0.21-25.x
ciscolive-01		Routable IP range 10.0.11-15.x	5	1			
ciscolive-02		Routable IP range 10.0.21-25.x	0	1	ciscolive-03		Routable IP range 10.0.31-35.x
ciscolive-03		Routable IP range 10.0.31-35.x	0	1			
ciscolive-04		Routable IP range 10.0.41-45.x	0	1	ciscolive-04		Routable IP range 10.0.41-45.X
ciscolive=06		Routable IP range 10.0.51-55.X	0	1	ciscolive-05		Routable IP range 10.0.51-55 v
ciscolive-07		Routebie in range 10.0.01 03.X	U				Noutable in Tange 10.0.01 00.X
Terraform		Routable IP range 10.0.71-75.x	5	1	ciscolive-06		Routable IP range 10.0.61-65.x
ciscolive-08 Terraform		Routable IP range 10.0.81-85.x	5	1			Ũ
ardica		Routable IP range 192.168.0-5.x	0	1	ciscolive-07		Doutoble ID range 10.0.71.75 v
rwhitear		Routable IP range 192.168.10-15.x	6	1	Terraform		Routable IP range 10.0.71-75.x
ngorse		Routable IP range 192.168.120-125.x	1	1			
demo		Routable IP range 192.168.150-155.x	3	1	CISCOIIVE-08		Routable IP range 10.0.81-85 x
fgandola		Routable IP range 192.168.151-158.x	11	2	Terraform		Nottable in Tange 10.0.01 00.X
roxadiaz		Routable IP range 192.168.20-25.x	6	1			
ndsouzar		Routable IP range 192.168.30-35.x	6	1	ardica		Routable IP range 192.168.0-5.x
esx-infrastructure		Routable IP range 192.168.4.x	1	0	nyhitoor		Doutable ID range 102 168 10-15 v
adealdag		Routable IP range 192.168.40-45.x	6	1	rwnitear		Routable IP range 192.106.10-15.x
ssharman		Routable IP range 192.168.50-56.x	7	1	ngorse		Routable IP range 192 168 120-125 x
mgmt		Routable IP range 192.168.6.x	1	2	ligoloo		100(00)011 101190 102.100.120 120.X
movaswan		Routable IP range 192.168.60-65.x	6	1	1	♥ Healthy	
adossant		Routable IP range 192.168.70-75.x	0	1	0	♥ Healthy	
rdagenha		Routable IP range 192.168.80-85.x	0	1	0	✓ Healthy	
yiouis		Routable IP range 192.168.90-95.x	U Objecto Ber Dover	1	0	V Healthy	
Page 1 Of 1 >			Objects Per Page: 100			Displaying Objects 1 - 32 Of 32	
Last Login Time: 2022-11-26T07:06 UTC+	+00:00					Current System Time: 2022-11-26T07:59 UTC+00:00	

cisco live!

Where should you place your L3outs...?

cisco ive

"common" tenant, "shared-services" tenant, or "workload/user" tenant...

cisco ile

External Connectivity



Dedicated VRFs and subnets for each Tenant with Dedicated L3outs





Shared networking with isolated security



Or even a combined solution...!



Option 1 – Dedicated L3out per Tenant

cisco ile

Dedicated L3out



*arrows indicates direction of traffic flow i.e. from consumer to provider
Option 2 – Shared L3out

cisco ive!

Shared L3out Route Leaking



*arrows indicates direction of traffic flow i.e. from consumer to provider

cisco ile

Shared L3out Route Leaking



*arrows indicates direction of traffic flow i.e. from consumer to provider

cisco ilel

Shared L3out External Contracts



*arrows indicates direction of traffic flow i.e. from consumer to provider

cisco ile

Why are we classifying with 0.0.0/1 and 128.0.0/1...?

cisco live!

Non dedicated border Leafs



cisco live!





Let's understand what's happening...

cisco ile

First, we need the ClassID or pcTag of the extEPG...

cisco ile

Get Class ID of the External EPG



cisco / illel

Get VRF scopes and Class IDs

	aci-dev-01-a	apic-01# sho	ow vrf vrf-0:	l detail grep shan	redB 4 -A	1								
	VRF Informat Tenant	tion: VRF	VXLAN Enc	ap Policy Enforced	Policy Tag	Consumed Contracts	Provided Contrad	ts Descript	ion F	PcTag Category Nar	ne PcTa	ag Range		
	shared- services-	vrf-01	<mark>2129920</mark>	enforced	46	- sha	ared-services:	/rf-01 uses		System	1-15)		
				1 data:1 anan dam		VXLAN Encap 2129920 and				Global .	16-1	6385		
	VRF Informat	tion:	OW VIT VIT-0.	i detaii grep demo) -B 4 -A I					_ocal (to VRF)	36-65535			
	Tenant	VRF	VXLAN Enc	ap Policy Enforced	Policy Tag	Consumed Contracts	Provided Contrad	ts Descript	ion			<u>_</u>		
	demo	vrf-01	<mark>2555904</mark>	enforced	<mark>49153</mark>	- de	emo:vrf=01 use				shared-s	shared-services:vrf-01 uses		
	aci-dev-01-a	apic-01# sho	ow vrf vrf-0:	1 detail grep ssha	arman -B 4 A		Encap 25559 pcTag 49	04 and 153				g from the Globa range	I	
	VRF Informat Tenant	tion: VRF	VXLAN Enca	ap Policy Enforced	Policy Tag	Consumed Contracts	Provided Contrac	ts Descript	ion					
Ļ	ssharman	vrf-01	<mark>3047426</mark>	enforced	49153	de	emo:vrf-01 use	es VXLAN						
			Γ		Summary	/ Dashbo	Encap 304/4 pcTag 49	26 and 153	Stats	Health Fau	lts History			
							Endpoints	Flows	Packets	Policy Tags	Resource IDs			
		Bridge Domains			ridge Domains	VRFs 😚 EPG	s ESGs	L3Out	ts External Netv	vorks ridged)				
											0			
			(Class ID		Segm	ient ID		Sco	оре	Resource II	Ds are visible		
		,		46		21299	920		212	29920	in th	<mark>e GUI</mark>		

cisco ile!

Let's check the VRF zoning-rules...

cisco ile

Check the zoning rules for the shared VRF extEPG

aci-dev-01	-apic-01#	<mark>fabric 1</mark> 0	<mark>01 show zoni</mark>	ng-rule scope <mark>2</mark>	129920 src-0	epg 41	
Node 101	(aci-dev-0	01-leaf-10) 91)				
+	+		 ++		 -+		SrcEPG /DstEPG 41 = VRF extEPG ClassID
Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	
+	++	⊦+ ⊦+	++		-+	+ +	-+
aci-dev-01	-apic-01#	<mark>fabric 10</mark>	<mark>01 show zoni</mark>	ng-rule scope 2	<mark>129920 dst-</mark>	epg 41	
Node 101	(aci-dev-0	01-leaf-10	01)				
+	+		++		-+	+	-+
RUIE ID +	Srcepg +	DSTEPG +	FilterID ++	D1r	operSt -+	Scope +	-+
+	+	++	++		-+	+	-+
							extEPG, so how is anything
							communicating?



Check the zoning rules for the shared VRF

a	ci-dev-01	-apic-01#	<mark>fabric 1</mark> 0	0 <mark>1 show zon</mark> :	ing-rule so	<mark>cope 21299</mark>	20 src-epg	46		
-	Node 101 (
- +		 +	+	 +	·	 +	 +	+	SrcEPG /Ds	stEPG 46 = VRF ClassID
	Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	l		
+	4359	+	+	+ implicit	uni-dir	+ enabled	+ 2129920	+ 		
	4293	46	0	default	uni-dir	enabled	2129920	+		
a	ci-dev-01	There are zonin to the VR	g rules F							
	Node 101 ((aci-dev-0	01-leaf-10	01)						
+	+++++++									
	Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority									
+++++++										

cisco live!

Check the zoning rules for the shared VRF and extEPG

aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 46 Node 101 (aci-dev-01-leaf-101) SrcEPG /DstEPG 46 = VRF ClassID										
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope	Name	Action	Priority							
4359 46 14 implicit uni-dir enabled 2129920 4293 46 0 default uni-dir enabled 2129920	shared-services:shared-services.vrf-01-all-ext-subnets	permit_override permit	src_dst_any(9) shsrc_any_any_perm(11)							
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg	4 <mark>6</mark>									
Node 101 (aci-dev-01-leaf-101)										
++++++++										
++	++									

aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2129920 src-epg 41</mark>										
Node 101 (aci-dev-01-leaf-101)										
Rule ID SrcEPG DstEPG FilterID Dir	operSt	Scope	Name	Acti	on Priority	İ				
$\overset{+}{} \cdots \cdots \overset{+}{} \cdots \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \cdots \overset{+}{} \cdots \cdots \cdots \cdots \overset{+}{} \cdots $										
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 21	<mark>29920 dst-e</mark>	pg 41								
Node 101 (aci-dev-01-leaf-101)										
++	+4			++-	+					
Rule ID SrcEPG DstEPG FilterID Dir	operSt	Scope	Name	Action	Priority					
+++++++	+			++-	+					

cisco live!

Why are there no zoning rules for the extEPG...?

cisco live!

Setting a scope of 0.0.0/0 triggers "system" pcTag 15

aci-dev-01-	-apic-01#	<mark>fabric 10</mark>	<mark>)1 show zon</mark> i	ing-rule	<mark>scope 21</mark>	29920	<mark>src-epg</mark>	15			
Node 101 ((aci-dev-0	01-leaf-10)1)								
++		·	·	· + + + + + +		·	 +	+	+ S	rcEPG /Ds	tEPG 15 = system classifier
Rule ID	SrcEPG	DstEPG	FilterID	Dir o	perSt	Scope	Name	Action	Prior	·	
+	• •			+	+-		+	+	, +	+	
aci-dev-01-	-apic-01#	<mark>fabric 10</mark>)1 show zon i	ing-rule	<mark>scope 21</mark>	29920	<mark>dst-epg</mark>	<mark>15</mark>			
Node 101 ((aci-dev-0	01-leaf-10)1)								
+	++	+4		+	-+	+		÷			
Rule ID	SrcEPG	DstEPG	FilterID	Dir	oper	`St	Scope				
4370	0	15	default	uni-dir	enabl	led 2	129920				
4498	0	15	implicit	uni-dir	enabl	.ed 2	129920				_
+	+	+			-+	+		+	Output	t truncated	

cisco Life

Setting a scope of 0.0.0/0 triggers "system" pcTag 15

aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2129920 src-epg 15</mark>											
Node 101 (aci-dev-01-leaf-101)											
++											
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority											
for the external subnet classifier.											
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 15 When 0.0.0.0/0 is configured,	the source	e class is set to the VRI	Class ID								
Node 101 (aci-dev-01-leaf-101)											
++	+	+	F								
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name	Action	Priority									
4370 0 15 default uni-dir enabled 2129920 shared-services:shared-services.vrf-01-all-ext-subnets	permit	any_dest_any(16)									
4498 0 15 implicit uni-dir enabled 2129920 ++	deny,log +	any_vrf_any_deny(22) +	 +								
	·		-								

cisco life!

Let's check the target tenants zoning rules...

cisco ile

Check the zoning rules for the demo VRF

aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2555904 src-epg 46</mark>	SrcEPG = shared services VRF									
Node 101 (aci-dev-01-leaf-101)	Dstepg = all epgs/esgs which are consumers of shared services									
++++++++	Action Priority									
$\frac{1}{2}$	all art subnots normit share any any norm(11)									
++++++++										
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 46										
Node 101 (aci-dev-01-leaf-101)										
	hared services VRF									
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority DstEPG = a	I EPGs/ESGs (vzAny)									
*++++++										
aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2555904 src-epg 15</mark>										
Node 101 (aci-dev-01-leaf-101)										
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority										
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority										
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority										
<pre> Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority ++++++++++++++++++++++++++</pre>	SrcEPG = vzAny									
<pre>k</pre>	SrcEPG = vzAny DstEPG = all extEPGs with 0.0.0.0/0									
<pre>k + + + + + + + + + + + + + + + + + + +</pre>	SrcEPG = vzAny DstEPG = all extEPGs with 0.0.0.0/0									
<pre> Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority ++++++++++++++++++++++++++++++++</pre>	SrcEPG = vzAny DstEPG = all extEPGs with 0.0.0/0 Action Priority									
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 15 Node 101 (aci-dev-01-leaf-101)	SrcEPG = vzAny DstEPG = all extEPGs with 0.0.0/0									
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priority aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 15 Node 101 (aci-dev-01-leaf-101) Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Image: Rule ID SrcEPG Image: Rule ID Image: Rule ID Scope Name Image: Rule ID Image: Rule ID Image: Rule ID Image: Rule ID Scope Name Image: Rule ID Image: Rule ID	SrcEPG = vzAny DstEPG = all extEPGs with 0.0.0.0/0 Action Priority -all-ext-subnets permit any_dest_any(16) deny,log any_vrf_any_deny(22)									

cisco

Check the zoning rules for the demo VRF

aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2555904 dst-epg 14</mark>											
Node 101 (aci-dev-01-leaf-101)											
<pre>+</pre>	y + +										
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 14											
Node 101 (aci-dev-01-leaf-101)	There is no zoning the consumer ten	g rule for ant, inste	DstEPG 14 in ad the zoning								
++ Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Priorit	y l	he correc	t DstEPG								
**+	+ +										
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 src-epg 46											
Node 101 (aci-dev-01-leaf-101)											
+++	Name	+ Action	Priority								
4263 46 0 default uni-dir enabled 2555904 shared-services:	<pre>shared-services.vrf-01-all-ext-subnets</pre>	permit	<pre>shsrc_any_any_perm(11)</pre>								
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2555904 dst-epg 46		+	+								
Node 101 (aci-dev-01-leaf-101)											
++++++++++	+ y										
*+++++++	+										

cisco ile

How should we resolve the unexpected communication...?

cisco ile





So, what's changed...?

cisco ive!

Get VRF scopes and Class IDs

aci-dev-01-	apic-01# show	v vrf vrf-01 d	detail grep shar	edB 4 -A	1						
VRF Informa Tenant	tion: VRF	VXLAN Encap	Policy Enforced	Policy Tag	Consumed Contracts	Provided Contracts	Description	PcTag Category Name	PcTag Range		
shared- services-	vrf-01	<mark>2129920</mark>	enforced	<mark>16386</mark>	-	-		System	1-15		
ani day 01	ania 01# aka		data:1 amon dama		Removing	0.0.0.0/0 from		Global	16-16385		
aci-dev-01-apic-01# show vrt vrt-01 detail grep demo -B 4 -A 1				the extEP	G changes the		Local (to VRF)	16386-65535			
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag	Consumed Contracts	Provided Contracts	Description				
demo	vrf-01	<mark>2555904</mark>	enforced	<mark>49153</mark>	-	-					
aci-dev-01-	aci-dev-01-apic-01# show vrf vrf-01 detail grep ssharman -B 4 A 1										
Tenant	VRF	VXLAN Encap	Policy Enforced	Policy Tag	Consumed Contracts	Provided Contracts	Description				
ssharman	vrf-01	<mark>3047426</mark>	enforced	<mark>49153</mark>	-	-					

	Summary	Dashboard	Policy	y C	perational	Stats	Healt	h Fa	ults	His	story
			Endp	oints	Flows	Packets	Polic	y Tags	Res	source	e IDs
	Bridge	e Domains	VRFs	EPGs	ESGs	L3Outs	Ex	ternal Ne	tworks	(Brido	ged)
									Õ	+	*~~
Class ID		Segn	nent ID			Scope	e				
16386		2129	920			21299	20				

cisco live

Get Class ID of the External EPG



cisco / illel

Check the zoning rules for the shared VRF

aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 16386										
Node 101 (aci-dev-01-leaf-101)										
Sr	cEPG /DstEPG 16386 = VRF ClassID									
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope										
+++++++++										
**										
aci-dev-01-apic-01# tabric 101 show zoning-rule scope 2129920 dst-epg 16386										
Node 101 (aci-dev-01-leaf-101)										
+++++++	+									
Rule ID SrcEPG DstEPG FilterID Dir operSt Scope Name Action Prior	ity									
+++++++++++++++	+									
	There are now no									
	zoning rules to the VRF									

cisco live!

Check the zoning rules for the shared VRF extEPG



cisco / ille

Do not use 0.0.0/0 in route leaking design...!

cisco ile

Check the zoning rules for the shared VRF and extEPG

aci-dev-01-apic-01# <mark>fabric 101 show zon</mark> :	ing-rule scope 21	29920 src-e	<mark>og 16386</mark>							
Node 101 (aci-dev-01-leaf-101)										
+++++++	+	 +	+	+		++				
Rule ID SrcEPG DstEPG FilterID	Dir oper:	St Scope		Name	Action Priority					
+++++++	+	+	+			+				
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 dst-epg 16386 DstEPG = all EPGs/ESGs which are consumers of shared services										
Node 101 (aci-dev-01-leaf-101)										
++++++	++-	 +	+							
Rule ID SrcEPG DstEPG FilterID	Dir operSt 1	Scope Nam	e Actior	pcTag 14 allo	ws traffic fi	rom the provider to the				
++	++-	+	+	consumer w	ithout the "	policy applied bit" set				
aci-dev-01-apic-01# fabric 101 show zoning-rule scope 2129920 src-epg 41										
Node 101 (aci-dev-01-leaf-101)										
	+	++		Name	+	on Drionity	+			
+++++++	+	++		Nallie	ACUI +	+	 +			
4301 41 14 implicit 4466 41 0 default	uni-dir uni-dir-ignore	enabled enabled	2129920 2129920	<pre>shared-services:shared-services.vrf-01-all-ext-subnets</pre>	permit_ov	rerride src_dst_any(9) hit shsrc any any perm(11)				
+++++++	+	++			+	+	+			
aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2129920 dst-epg 41</mark>										
Node 101 (aci-dev-01-leaf-101)										
++++	+	++			++-	+				
Rule ID SrcEPG DstEPG FilterID	Dir +	operSt ++	Scope	Name	Action ++-	Priority				
4487 0 41 default	bi-dir	enabled	2129920	<pre>shared-services:shared-services.vrf-01-all-ext-subnets</pre>	permit	<pre>shsrc_any_any_perm(11) .</pre>				
+++++	+	++			++-	+				

cisco live!

Let's check the target tenants zoning rules...

cisco ile

Check the zoning rules for the demo VRF

aci-dev-01-apic-01# <mark>fabric 101 show zoning-rule scope 2555904 src-epg 41</mark>							SrcEPG =	shared ser	PG			
Node 101	(aci-dev-0	01-leaf-10	91)						vsAny			
+	+	+	+		+	+				+	+	·+
Rule ID +	SrcEPG +4	DstEPG ⊦4	FilterID ++	Dir	∽ +·	operSt	Scope	Name		Action +	Priorit	:y +
4305 4228	41 41	0 0	default implicit	uni-dir- uni-d	-ignore dir	enabled enabled	2555904 2555904	<pre>shared-services:shared-services.vrf-01-all-</pre>	ext-subnets	permit deny,log	<pre>shsrc_any_any_ shsrc_any_any_</pre>	_perm(11) _deny(12)
tori day 01 apic 01# fabric 101 chay apring pula come 20000 det ang 41												
							P8 +1					
Node 101	(aci-dev-0	01-leaf-10)1) 									
+	++		+	+ D-i-n	+	-+	-+	Nama	+	-+		+
+	SPCEPG +	DSLEPG 	+iiteriD			-+	 -+	Name	ACLION	۲ +		+
4339	0	41	default	bi-dir	enabled	2555904	shared	<pre>services:shared-services.vrf-01-all-ext-subr</pre>	<mark>ts permit</mark>	shsrc_an	y_any_perm(11)	
aci-dev-01	-apic-01#											-
SrcEPG = shared services VRF												
DstEPG = all EPGs/ESGs (vzAny)									$(c (v z \Lambda p v))$			

cisco live!





Inbound to tenant ssharman: Route: 10.237.99.176/28 via demo:vrf-01 Policy: sclass = 41 | dclass = 0 (vzAny)



Scenario 1 – Provider and multiple Consumer VRFs are on the same Leaf with /0 mask

- 1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag 15 (extEPG with 0.0.0/0)
- 2. Since the leaf knows the egress port and destination VRF (shared), the packet will be sent out from that port without going through another lookup on the destination VRF (shared)
- 3. The packet comes back from the external router
- 4. The packet gets the sclass of VRF and dclass 14
- 5. The packet is allowed in the shared VRF because there are contracts between the VRF pcTag and 14 in the shared VRF
- 6. Just like step 2, the packet is sent out to the destination endpoint without going through another lookup in the destination consumer VRF because the leaf knows the egress port and its destination VRF


Scenario 2 – Provider and multiple Consumer VRFs are on different Leafs with /0 mask

- 1. The packet from the source consumer VRF hits the contract for vzAny to 15
- 2. The packet reaches the shared VRF leaf. Another lookup happens. The forwarding points another leaf
- 3. The packet gets dropped because of a internal TCAM ACL rule (not a contract) that prevents traffic bouncing back to spines without a bounce entry

cisco / ile

Scenario 1 – Provider and multiple Consumer VRFs are on the same Leaf with /1 mask

- 1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag of extEPG with 0.0.0.0/1 and 128.0.0.0./1 mask
- 2. Since the leaf knows the egress port and destination VRF (shared), the packet will be sent out from that port without going through another lookup on the destination VRF (shared)
- 3. The packet comes back from the external router
- 4. The packet gets the sclass of the extEPG and dclass 14
- 5. The packet is allowed in the shared VRF because there are contracts between the VRF pcTag and 14 in the shared VRF
- 6. Just like step 2, the packet is sent out to the destination endpoint without going through another lookup in the destination consumer VRF because the leaf knows the egress port and its destination VRF



Scenario 2 – Provider and multiple Consumer VRFs are on different Leafs with /1 mask

1. The packet from the source consumer VRF hits the contract for source EPG/ESG to pcTag of extEPG with 0.0.0.0/1 and 128.0.0.0./1 mask

- 2. The packet reaches the shared VRF leaf. Another lookup happens. The forwarding points another leaf
- 3. The packet gets dropped because of a internal TCAM ACL rule (not a contract) that prevents traffic bouncing back to spines without a bounce entry

cisco / ille

Tightening Security...



Let's tighten the contract to our online-boutique application...

cisco ile

Tighten the contract to our online-boutique application...



Before we do that, let's check our understanding on how contracts work...

cisco live

How do contracts work...?



*arrows indicates direction of traffic flow i.e. from consumer to provider

cisco ile

Consumer and Provider relationships are there to help you <u>visualize</u> the traffic flow direction i.e. (typically) from the consumer to the provider

Consumer and Provider relationships <u>do not</u> (by default) prevent TCP connections being established <u>from</u> the Provider <u>to</u> the Consumer

Contract structure...



Verifying Contract operation with netcat – Stateful = No



Verifying Contract operation with netcat – Stateful = Yes









Filter Entry <u>source</u> port = port opened on the consumer EPG/ESG

Filter Entry <u>destination</u> port = port opened on the provider EPG/ESG

Reversing the Filter ports – Stateful = No



Why would you want to reverse the Consumer and Provider Filters...?

cisco ile

vzAny as a contract Provider



BRKDCN-2984 © 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public 160

vzAny as a contract Provider



vzAny as a contract Consumer – Filters Reversed



vzAny as a contract Consumer – Filters Reversed



CISCO

Let's tighten the contract to our online-boutique application...

cisco ile

Tighten access to our online-boutique application...



Contracts: The hidden details



Contract Scope

- The scope of a contract defines where a contract is relevant, there are four options:
 - Application Profile- used to control traffic within an Application Profile
 - VRF used to control traffic between EPG/ESG within a VRF
 - Tenant used to control traffic between EPG/ESG across VRFs within a Tenant
 - Global used to control traffic between EPG/ESG in different Tenants/VRFs
- Contract definitions can be reused allowing you define once and reference many times
 - Note: Exercise caution when reusing contract definitions at this can lead to unexpected communication
 - Recommendation: define explicit contracts rather then n:1 reference



What are the components of a contract...?



Contract Scope = <u>Application</u>, Contract re-use = yes



Contract Scope = <u>VRF</u>, Contract re-use = yes



cisco live!

Contract Scope = <u>Tenant</u>, Contract re-use = yes



Contract Scope = <u>Global</u>, Contract re-use = yes



Option 1: Apply in both directions, reverse ports

cisco ile

Option 1: Apply in both directions, reverse ports (default)



Option 1: Apply in both directions, reverse ports (default)



Option 1: Apply in both directions, reverse ports (default)



Option 2: Apply in both directions, reverse ports, stateful

cisco life!

Option 2: Apply in both directions, reverse ports, stateful/ack check



Option 2: Apply in both directions, reverse ports, stateful/ack check



Option 2: Apply in both directions, reverse ports, stateful/ack check



cisco ive!
Option 3: Apply in single direction

cisco ile

Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract



Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract



cisco ive!

Option 3: Apply in single direction – requires you to specify the return ports in the same or different contract



Option 4: Apply in both directions, reverse ports, "flipped" – (this might hurt a little bit)

cisco ile

Option 4: Consumer and Provider Flipped



cisco live!

Option 4: Consumer and Provider Flipped



Option 4: Consumer and Provider Flipped



cisco live!

Option 5: Apply in both directions (not recommended)

cisco ile

Option 5: Apply in both directions (<u>no reverse ports</u>) – requires you to specify the return ports



Option 5: Apply in both directions (no reverse ports) – requires you to specify the return ports



Option 5: Apply in both directions (no reverse ports) – requires you to specify the return ports



cisco live!

Verifying contracts...

cisco live!



cisco life!





cisco ive!

vrf-01	ubuntu 92.168.1	pcTag: -01 .50.21	38 ESG ubunt	:u-01 - I - P		Cor	nt permit-to-u	buntu-02]		ESG ubunt C - CCI-	u-02	g: 5474	21
-dev-01-a	pic-01#	<pre># fabric 1</pre>	101-102 show z	<mark>oning-f</mark> i	ilter filter 12	2 								
ode 101 (a	ici-dev-	-01-lea+-1	101)											
ilterId	Name	EtherT	ArpOpc	Prot	ApplyToFrag	Stateful	SFromPort	SToPort	DFromPort	DToPort	Prio	+ Icmpv4T	Icmpv6T	+
12	12_0	ip	unspecified	+ tcp	no	no	unspecified	+ unspecified	+ 7070	7070	dport	+ unspecified	unspecified	+
de 102 (a	Name	01-leaf-1	102) +	+	ApplyToFrag		SFromPort	+	+	DToPort		+ Icmpv4T +	+ Icmpv6T +	+ TcpRule +
12	12 <u>0</u>	1p 	unspecified +	τ сρ +	no	no 	unspecified +	unspecified +	/0/0 +	/0/0 +	aport 	unspecified +	unspecified +	 +

Blueprints

•

cisco live!

Example Internal Private Cloud Design – shared subnet(s)



CISCO (

Application Centric Blueprint #1 – ESG "wrapper" for all services Source/Consumer Target/Provider Target/Provider Port cart Redis cache TCP 6379 tn-demo checkout cart TCP 7070 currency TCP 7000 🔛 vrf-01 email TCP 5000 payment TCP 50051 Consumers … TCP 3550 product catalog TCP 50051 shipping Single security zone for frontend adservice TCP 9555 TCP 7070 all application services cart checkout TCP 5050 currency TCP 7000 product catalog TCP 3550 recommendation TCP 8080 AP online-boutique C C CI I P shipping TCP 50051 ESG all-services outside TCP 80/8080 frontend TCP 3550 recommendation product catalog frontend checkout . adservice recommendation shipping email payment product catalog cart currency Redis cache



CISCO



CISCO







CISCO









Wrapping up...



Select one or more Design Patterns...

Carefully consider the use of:

- The "common" tenant
- Using a "shared services" tenant
- vzAny
- Dedicated border Leafs (recommended)
- External EPG with the classifier 0.0.0/0

Implement ESG "wrappers"...

Wrapping applications into ESGs provides the following benefits for both virtual **and** physical workloads:

- Improved application visibility
- Improved auditing capabilities
- Improved troubleshooting
- Intelligent service insertion
- Security tied applications rather than network segments
- Reduce the reliance on monolithic physical security devices

Benefits of Shared Service model...

- Looks and feels like a Public Cloud model of working
- Network team maintains control of North / South route peering
- Network team maintains control of Inter VRF route leaking
- Each Tenant can control their own CIDR range
- Each Tenant can control their own security rules
- Each Tenant can have private (non routable subnets)
- Security services can be easily inserted in the Tenants
- Do not use 0.0.0/0 as the extEPG classifier

Automation Considerations...

- A simple consumption model is everything
- Single API for all <u>networking</u> functions
- Application security requirements should be declared to the infrastructure
- Add virtual application firewalls to deployments if required
- Large physical monolithic firewalls are useful at network boundaries, however they should only provide broad security rules
- Remove unnecessary overlay networks that add layers of complexity

Now available on dCloud

Getting Started with Cisco ACI 6.0 v1

Information Resources

Overview

Cisco Application Centric Infrastructure (ACI) is a software-defined networking (SDN) solution designed for data centers, the cloud and hybrid-cloud. Cisco ACI allows network infrastructure to be defined based upon network policies - simplifying, optimizing, and accelerating the application deployment lifecycle

The Cisco Application Policy Infrastructure Controller (Cisco APIC) is the unifying point of automation and management for the Cisco Application Centric Infrastructure (Cisco ACI) fabric. The Cisco APIC provides centralized access to all fabric information, optimizes the application lifecycle for scale and performance, supporting flexible application provisioning across physical and virtual resources.

Cisco ACI virtual machine networking provides hypervisors from multiple vendors programmable and automated access to high-performance, scalable, virtualized data center infrastructure. Programmability and automation are critical features of scalable data center virtualization infrastructure. The ACI open REST API enables virtual machine (VM) integration with and orchestration of the policy-model-based ACI fabric. ACI VM networking enables consistent enforcement of policies across both virtual and physical workloads that are managed by hypervisors from multiple vendors.

This lab provides an introduction to Cisco ACI, taking the user through the initial setup process and configuring integration with a VMware vSphere. Then the user reviews the the ACI security model, and how to implement it, learning about Tenants, Application Profiles, Endpoint Groups, Endpoint Security Groups, and Contracts and Filters.

For additional information, visit www.cisco.com/go/apic.



Schedule

Cisco Webex App

Questions?

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

How

- **1** Find this session in the Cisco Live Mobile App
- 2 Click "Join the Discussion"
- 3 Install the Webex App or go directly to the Webex space
- **4** Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.




Complete your 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 (open from 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 Session Catalog and clicking the "Attendee Dashboard" at <u>https://www.ciscolive.com/emea/learn/sessions/sessioncatalog.html</u>



Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at <u>ciscolive.com/on-demand</u>.



 IIIII
 The bridge to possible

Thank you

cisco live!

cisco live!



