

CISCO *Live!*



#CiscoLive



The bridge to possible

# How to build a Secure Multi-Cloud environment with Cisco Secure Workload

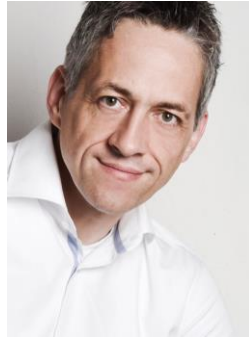
This session will cover the challenges customers are facing in a Multi-Cloud environment and how Cisco Secure Workload will support them on a road to zero trust for their applications. The session will touch briefly on Cisco Data Center architecture like ACI, and cloud deployments and how Cisco Secure Workload will help them to reduce their attack surface, manage compliance state and how to reduce security risks.

Dirk Stoeckmann, TSA Workload Security Engineering  
@dstoeckm  
BRKSEC-1773



#CiscoLive

# Who am I



Married,  
2 girls (17/12)  
21 years with Cisco



Dirk  
Stoeckmann  
CCIE No. 5748

#CiscoLive

BRKSEC-1773



# Cisco Webex App

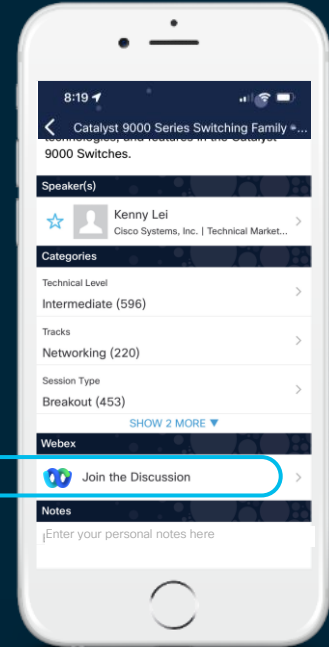
## Questions?

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 by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1773>



# Agenda

- IT policy control
- Cisco Secure Workload foundation
- Data center fabric, the ACI way
- Cloud environments, what is so different
  - AWS as a reference cloud
- Manage your policy across clouds
- Conclusion

# Wikipedia



**CISCO** *Live!*



# What is a data center and why do we build them?

Wikipedia





# Cyber attacks public administration Q1 2022

Major cyber attacks on public administrations 1st quarter 2022					
January		February		March	
 Jan 05, 2022 Albuquerque (USA) County administration	 Jan 16, 2022 Saint-Jean-de-M... (F) Municipality	 Feb 01, 2022 Monforte de Lem... (E) City administration	 Feb 18, 2022 Lisbon (P) Min. of Foreign Affairs	 04 Mar 2022 Maizières-lès-M... (F) Municipalities	 18 Mar 2022 Ottawa (CDN) Governm. research org
 Jan 2022 Griggsville (USA) School district	 Jan 17, 2022 Getxo (E) City council	 Feb 03, 2022 Quincy (USA) City administration	 Feb 20, 2022 Vitória (BR) Labor court	 06 Mar 2022 Odense (DK) Survey, citizen portal	 Mar 19, 2022 Banff (CDN) City government
 Jan 10, 2022 Yverdon-les-Bai... (CH) IT service prov., municip...	 Jan 19, 2022 Ottawa (CDN) Min. of Foreign Affairs	 Feb 2022 Antwerp (B) Crematoria	 Feb 21, 2022 Mozambique Government	 06 Mar 2022 Sens (F) City administration	 19 Mar 2022 Plainfield (USA) City administration
 Jan 10, 2022 Trezzano sul Na... (I) Municipal admin.	 Jan 20, 2022 Salvador (BR) State government	 Feb 06, 2022 Bogotá (CO) Agency	 Feb 23, 2022 Kyiv (UA) State institutions	 07 Mar 2022 Sens (F) City administration	 20 Mar 2022 Dingolfing (D) City administration
 Jan 10, 2022 North Port (USA) Local government	 Jan 20, 2022 Rivoli (I) Municipality	 Feb 2022 (USA) Government	 Feb 23, 2022 Ukraine (UA) Government	 07 Mar 2022 Ukraine (UA) Government	 20 Mar 2022 San Antonio (USA) Property appraisal
 Jan 11, 2022 Neenah (USA) School district	 Jan 21, 2022 Saint-Cloud (F) City administration	 Feb 12, 2022 Istanbul Municipality	 Feb 24, 2022 Europe Government officials	 08 Mar 2022 Bochum (D) City administration	 22 Mar 2022 Aix-les-Bains (F) Local government
 Jan 2022 ? London Foreign office	 Jan 22, 2022 Indien Disaster response	 Feb 15, 2022 New Delhi Government television	 Feb 24, 2022 Ukraine (UA) Government	 08 Mar 2022 Alcamo (I) Municipality	 March 2022 France (F) Government org.
 Jan 13, 2022 Ukraine (UA) Government	 Jan 24, 2022 Verviers (B) City administration	 Feb 16, 2022 Hiroshima (J) Prefecture	 24 Feb 2022 Spokane (USA) Health district	 10 Mar 2022 Suhl (D) City administration	 23 Mar 2022 Saumur (F) City administration
 Jan 13, 2022 Pembroke Pines (USA) City administration	 Jan 24, 2022 Albany (USA) County administration		 Feb 26, 2022 Moscow (RUS) Space Agency	 11 Mar 2022 San Bartolomé d... (E) City administration	 25 Mar 2022 Nauru (NR) Public administration
 Jan 13, 2022 Albuquerque (USA) School district	 Jan 27, 2022 New Bedford (USA) Police			 13 Mar 2022 Villafranca di ... (I) Municipality	 26 Mar 2022 Moscow (RUS) Aviation authority
 Jan 14, 2022 Ukraine (UA) Government	 Jan 28, 2022 Paris (F) Ministry of Justice			 14 Mar 2022 Israel (IL) Government	 Mar 30, 2022 São Paulo (BR) Court
				 15 Mar 2022 Praha (CZ) City district admin.	

Total: 62

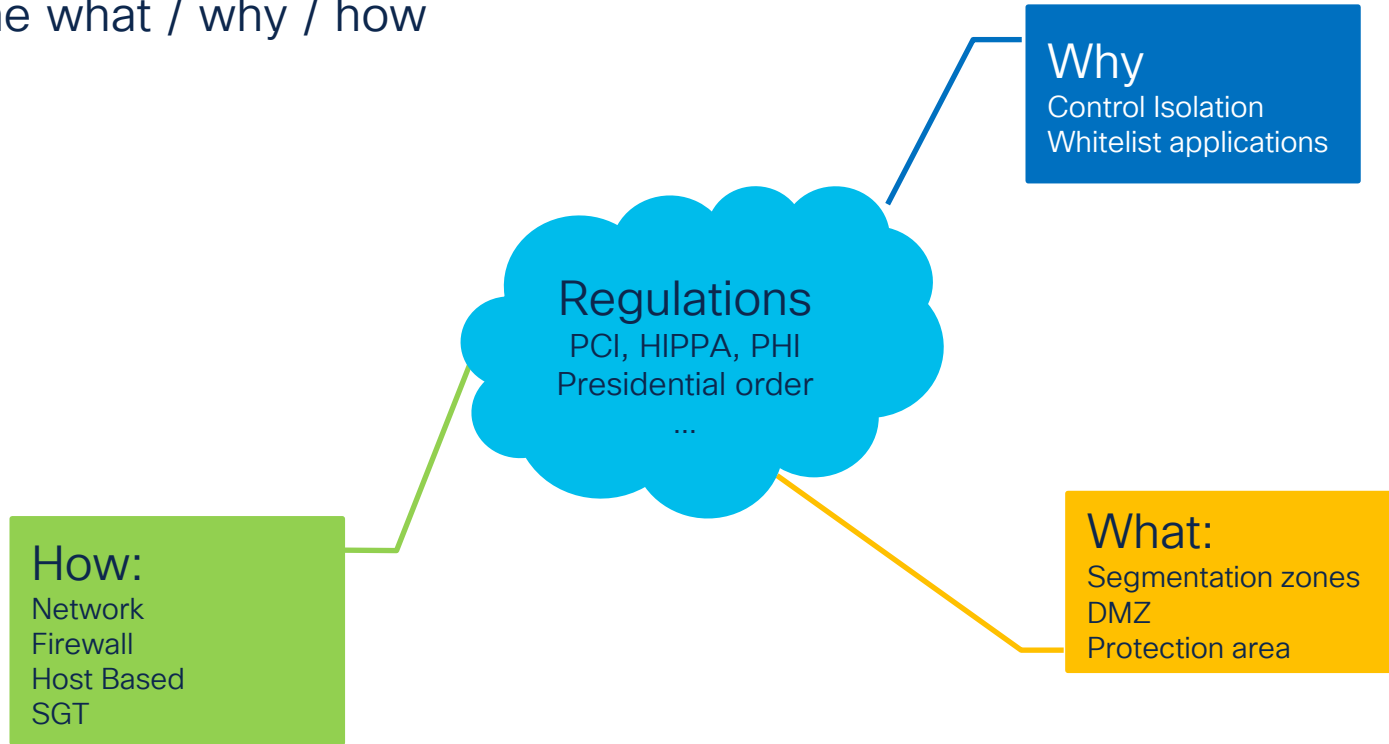
KonBriefing.com

<https://konbriefing.com/en-topics/cyber-attacks-2022-ind-public-administrations-q1.html>

License [CC BY 4.0](#). Credits: KonBriefing.com

# Customer view

The what / why / how



# Drivers for Zero Trust



- Highly Sensitive Data
  - Personal Health Information (PHI)
  - Employee/Financial Data
- Critical System Availability
  - Patient Care
- Regulatory Demands
  - HIPAA
  - PCI
- Complexity Challenges
  - Hybrid Cloud

# Cisco Secure Workload

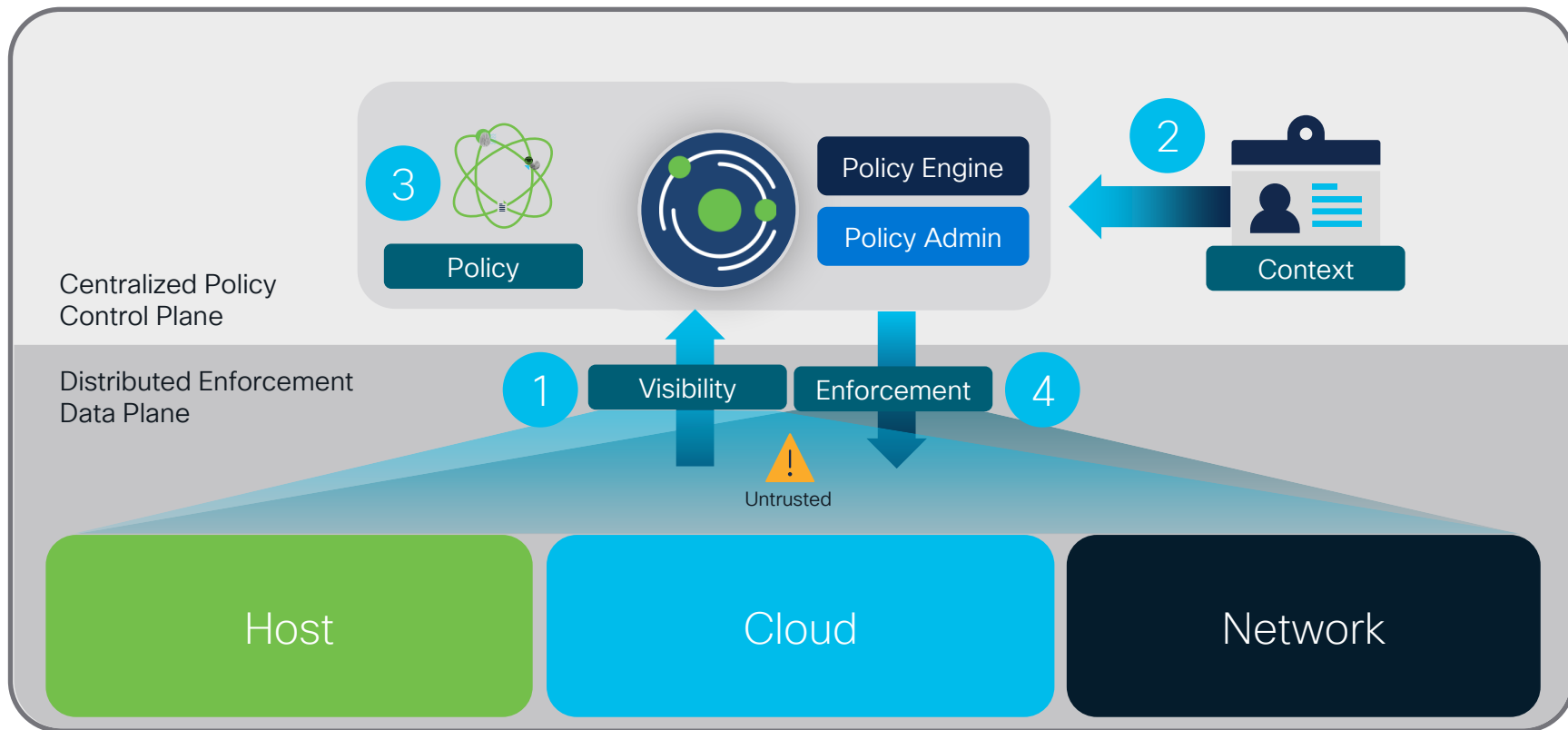




Also called policy management; policy control is a technology that enables the definition and application of business and operational rules in organizations. In today's IT information systems, security policies are static and local to **each** of the security devices.

Google search on “it policy control”

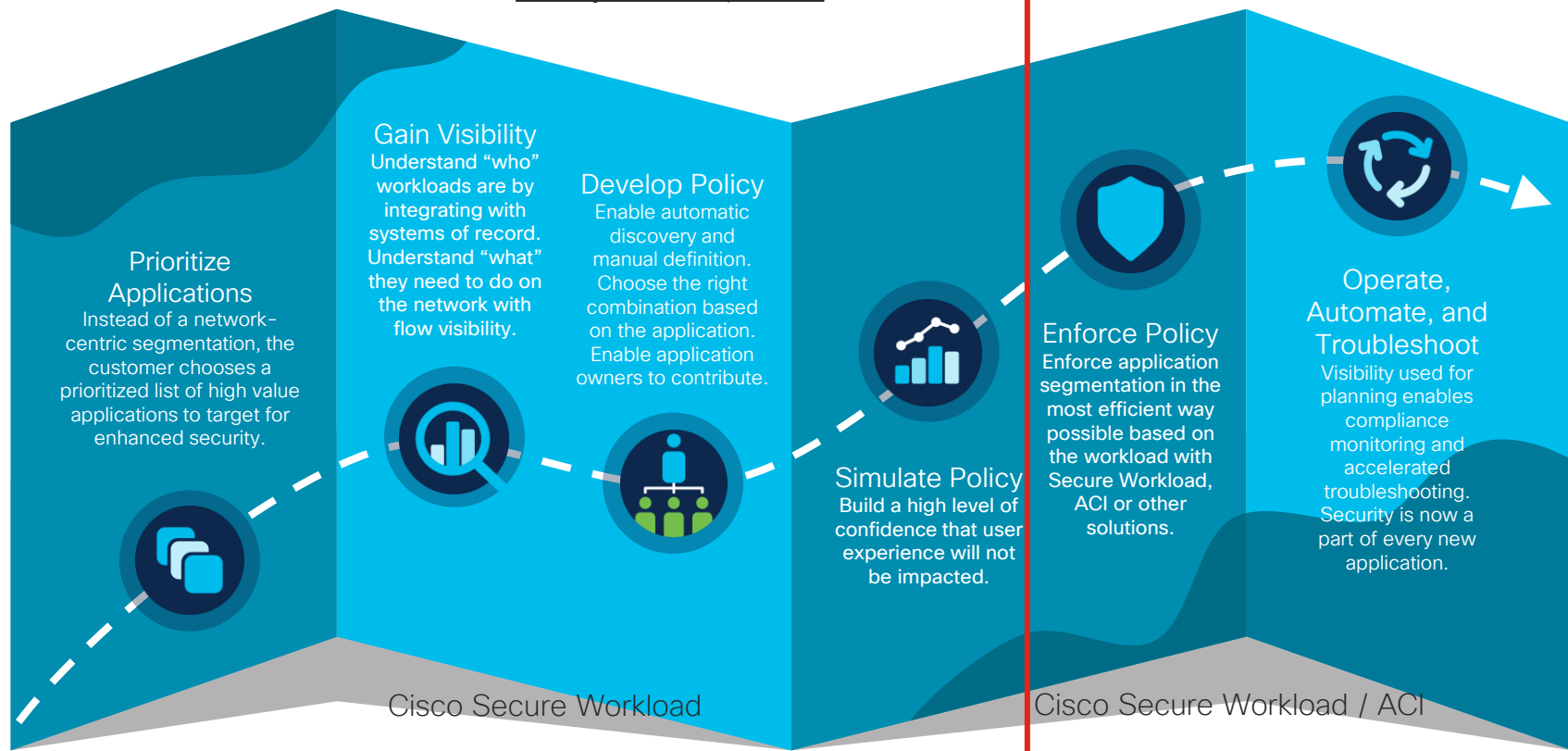
# Secure Workload Approach to Zero Trust



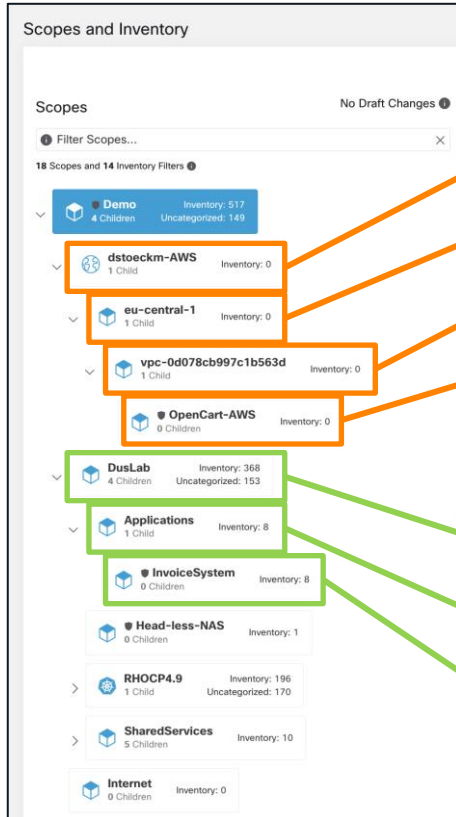
# Steps to Application Segmentation

## Policy Development

## Policy Enforcement



# Organisation of apps



## For AWS

### Query

\* orchestrator\_system/orch\_type = aws or \* Datacenter = aws

### Query

\* orchestrator\_system/region = eu-central-1 or \* location = eu-central-1

### Query

\* orchestrator\_system/virtual\_network\_id = vpc-0d078cb997c1b563d or \* Scope = vpc-0d078cb997c1b563d

### Query

\* orchestrator\_system/cluster\_name = dstoeckm-AWS or \* app\_name = opencart

## For local lab

### Query

\* Datacenter = DusLab

### Query

\* Environment = applications

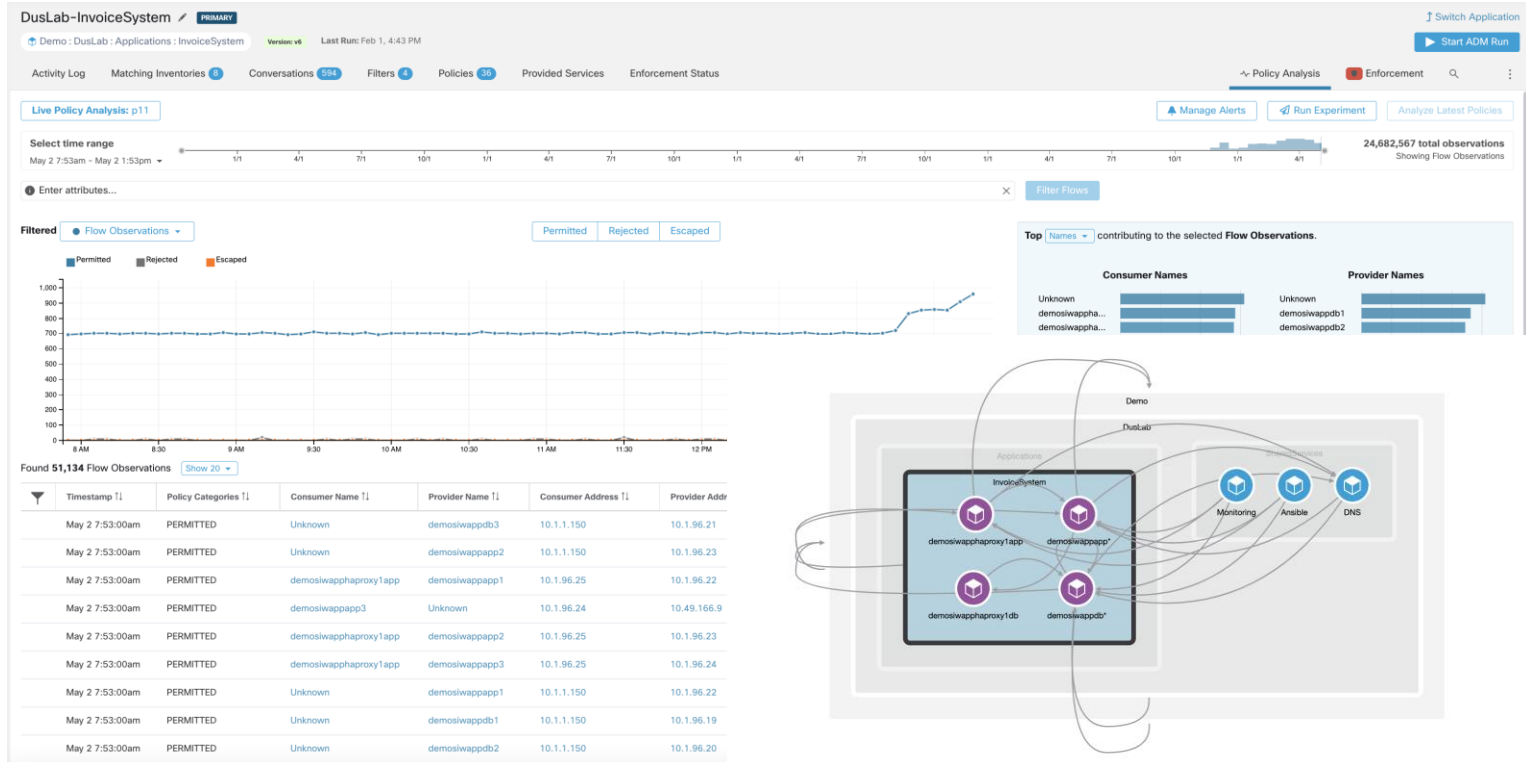
### Query

\* Scope = invoicesystem

How to organize applications based on defined labels derived from orchestrator, APIs or manual (CSV).



# Policy analytics and control

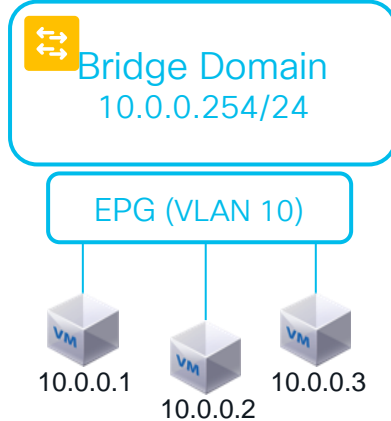


# The ACI way

# Network Centric & Application Centric Design

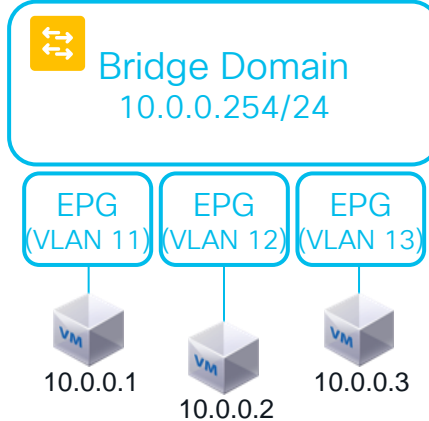
## Network Centric

A security group  
in 1 subnet



Need more granular  
security group

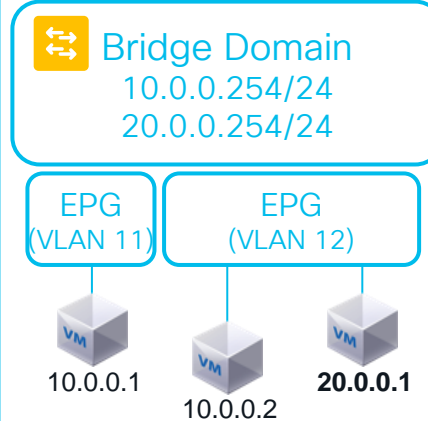
Multiple security groups  
in 1 subnet



What if multiple subnets  
need to share the same  
security rules?

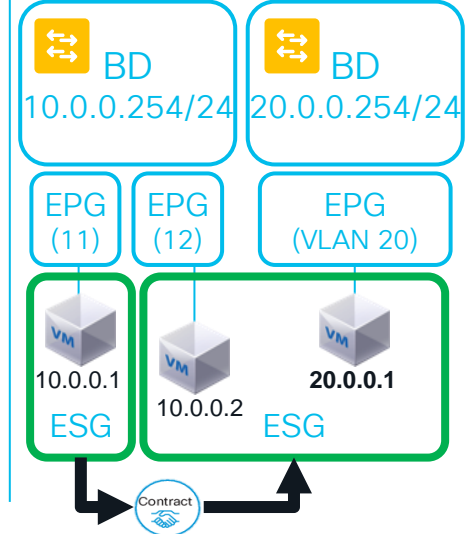
## Application Centric

Security groups across  
subnets



Sharing a broadcast  
domain brings another  
security concern

== 5.0 ==  
Endpoint Security  
Group (ESG)  
Security groups **across**  
bridge domains



Flexible security  
grouping

# Legacy

# How does this look like ACI

Def GW  
IP = 10.1.20.1/24

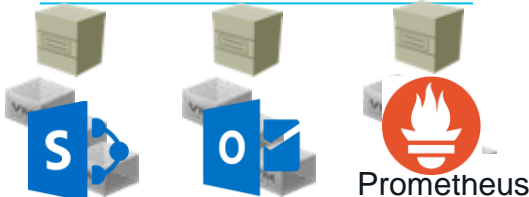
Layer 2  
VLAN 20



ACL to control traffic  
from vlan 10 to vlan 20  
:: permit IP any any

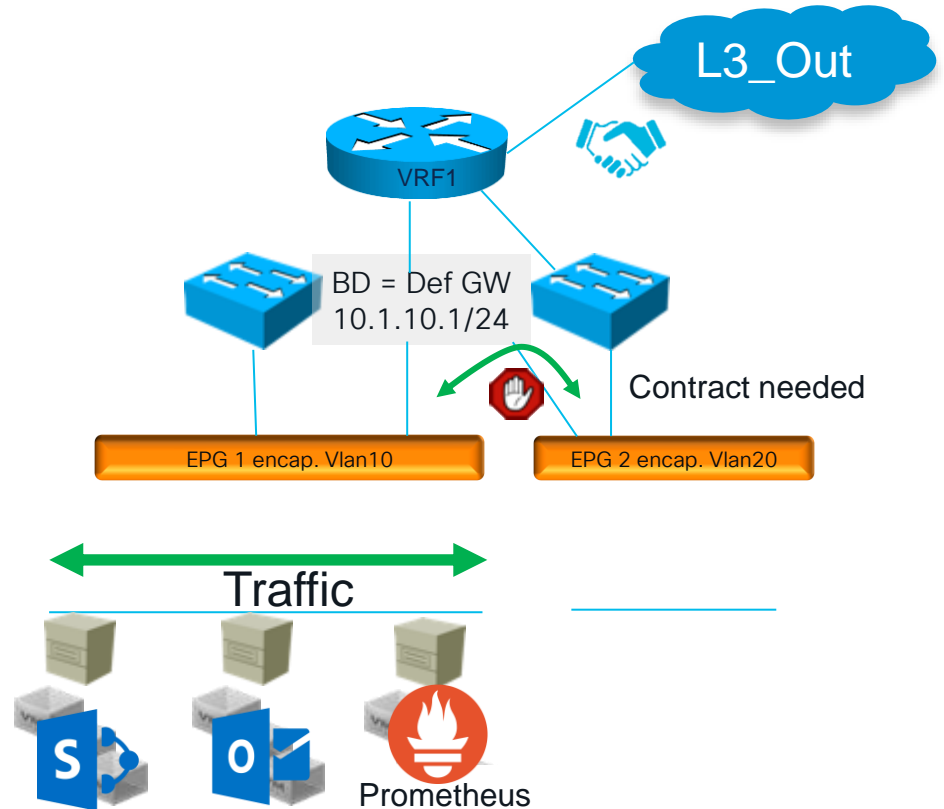


Layer 2  
VLAN 10

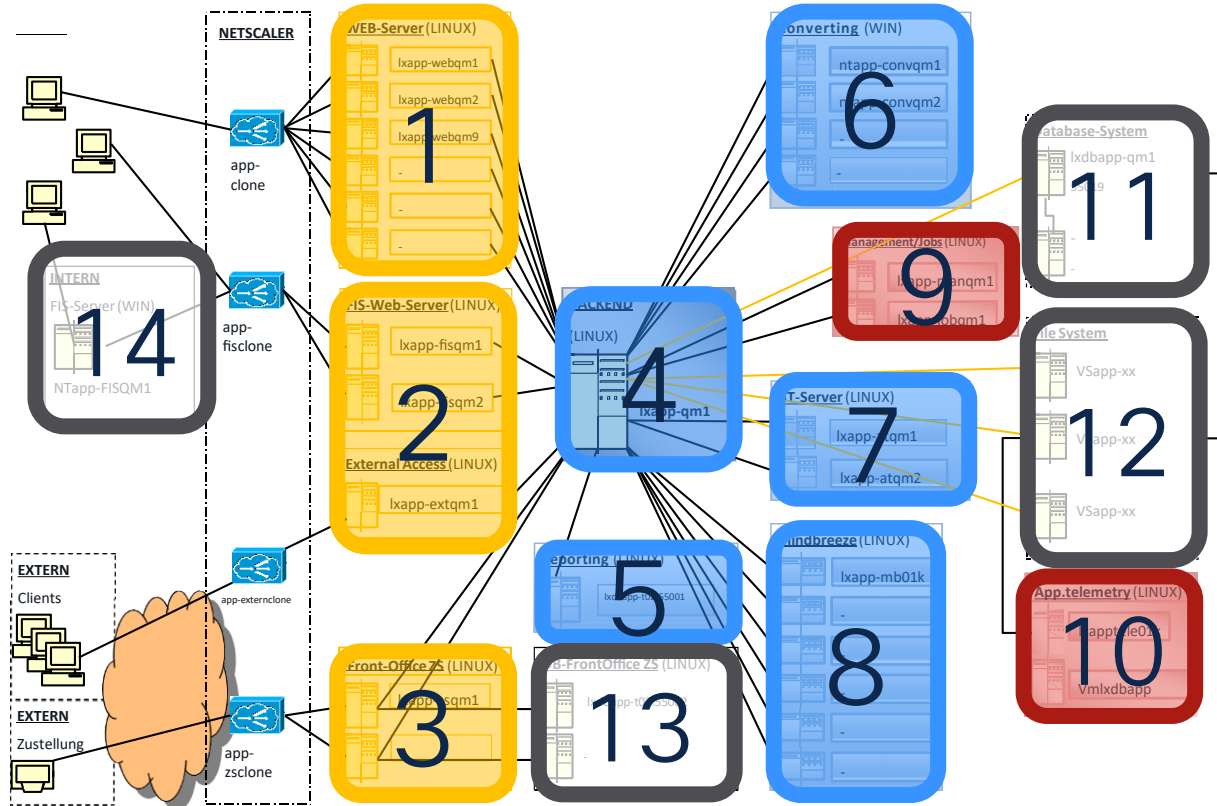


Legacy

How does this look like ACI



# Sample application under test



# Application communications – the old way

Application name:		<b>Communication matrix *</b>							
Application version:		communication between participants							
Application description:		Source		Destination		Service protocol		Ports	
Stage:		Type of communication, target or destination		type of protocol https, ssh, tls, rpc, dicom, smtp, ... In case of IP only... UDP, TCP, ...		used ports? 53, 443, 8080			
Risk level:									
add on communication matrix:									
Type	Description	Function	Device name	alternative name	IP address	network scope	DHCP		
What type of server: source or destination, web, app, middle ware									
Additional information regarding the system. Operating system, subsystem, part of a cluster		<b>Usage</b>							
		<b>Communication by Ports</b>							
		to Type	Type 1	Type 2	Type 3	...	<<<< to Type		
		from Type							
		Type 1	https/6443, https/7443			Please add participants source or destination from the first sheet			
		Type 2							
		Type 3							
		...							
		from Type ^	For easier usability please use communication by port						

# Application communication – the API way

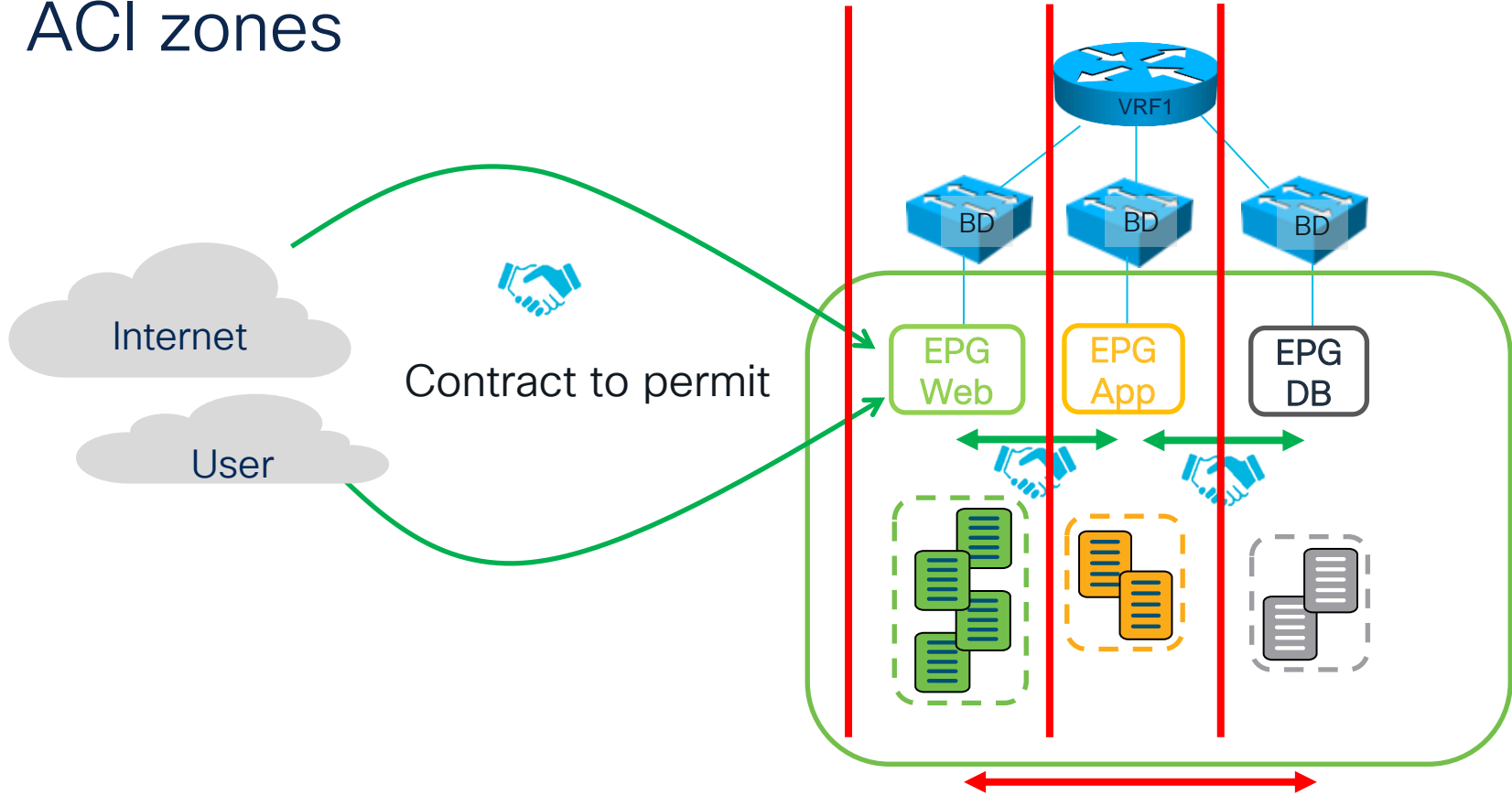
Hostname	IP	Cluster Membership
lxdappqm1	10.153.109.22	cluster
lxappmb01k	10.153.109.14	cluster
lxappatqm2	10.153.94.193	lxapp*
lxappextqm1	10.153.94.198	lxapp*
lxappjobqm1	10.153.94.194	lxapp*
lxappatqm1	10.153.94.192	lxappatqm1
lxappfisqm1	10.153.94.199	lxappfisqm*
lxappfisqm2	10.153.94.197	lxappfisqm*
lxappmanqm1	10.153.94.200	lxappmanqm1
lxappqm1	10.153.109.23	lxappqm1
lxappwebqm1	10.153.94.201	lxappwebqm*
lxappwebqm2	10.153.94.202	lxappwebqm*
lxappwebqm9	10.153.109.36	lxappwebqm*
lxappzsqm1	10.153.92.85	lxappzsqm1
ntappconvqm1	10.153.92.205	ntapp*
ntappconvqm2	10.153.93.8	ntapp*
ntappfisqm1	10.153.94.76	ntapp*



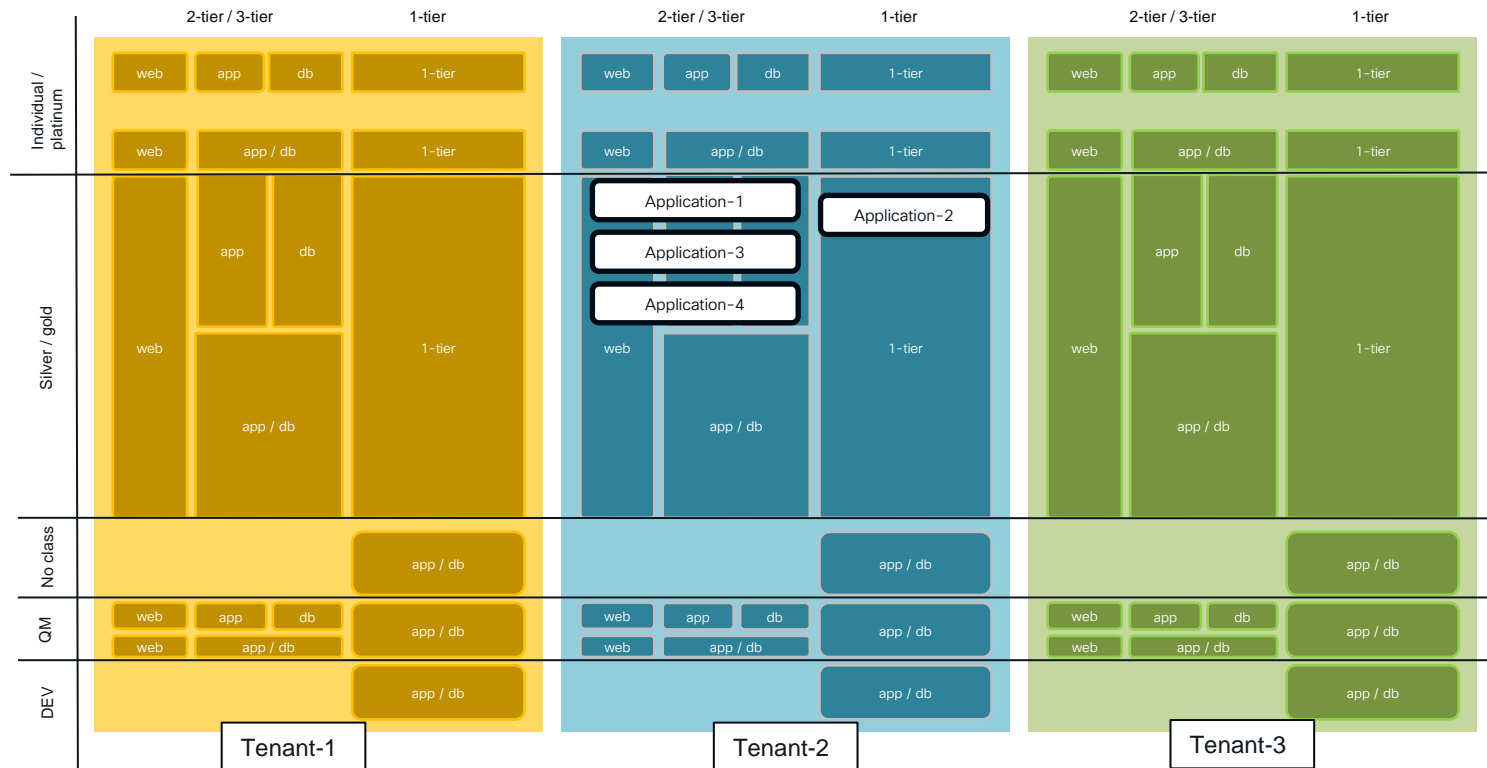
Consumer Group	Provider Group	Services
lxappwebqm9	ntapp*	TCP=81-82
lxappfisqm*	Tetration_Config	TCP=443; ICMP
Customer_PoC	lxappqm1	UDP=161; TCP=22, 80, 7937-7938, 7940, 10001; ICMP
lxappzsqm1	Tetration_Config	ICMP; TCP=443
lxappqm1	lxapp*	TCP=33644, 33660, 35394, 36342, 38124, 43596, 44060, 52908, 52916, 58546, 60628
lxappatqm1	lxappqm1	TCP=12100-12102, 12104, 12106-12110, 12112-12118, 12120, 12122
lxappfisqm*	lxappqm1	TCP=12100-12108, 12110, 12112, 12114-12118, 12120, 12122
cluster	Tetration_Collectors	ICMP; TCP=5660
lxapp*	File-System	TCP=445, 2049
ntapp*	Tetration_Collectors	TCP=5640, 5660
lxappwebqm*	lxappqm1	TCP=12100-12123
lxapp*	lxappqm1	TCP=12100-12102, 12104, 12106, 12108-12110, 12112, 12114-12116, 12118, 12120, 12122
lxappqm1	File-System	TCP=445, 2049
lxappwebqm9	Tetration_Collectors	ICMP; TCP=5660



# ACI zones



# ACI design from a Secure workload customer



# Multi Cloud

AWS as a reference

# What is a multi cloud environment



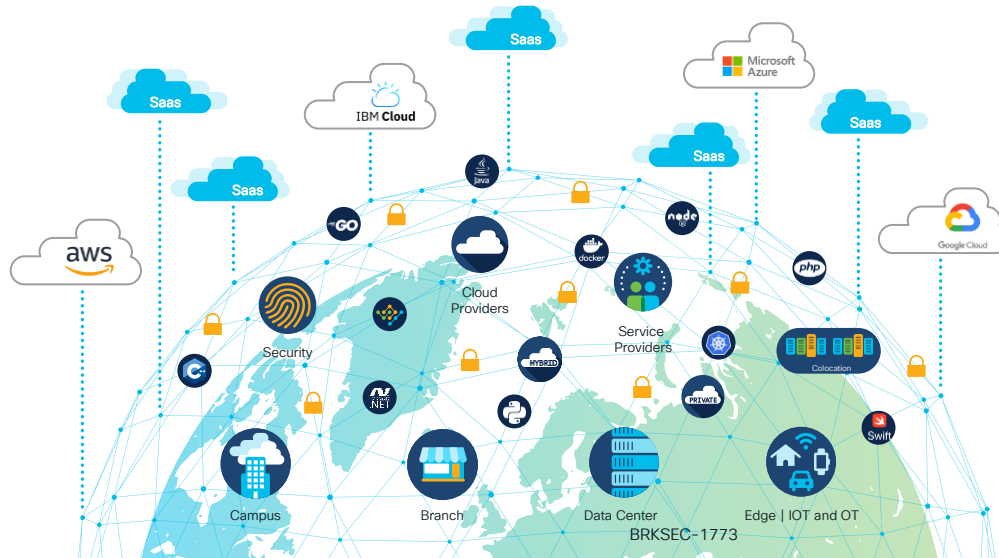
IT Ops

Management?  
Security?  
Orchestration?

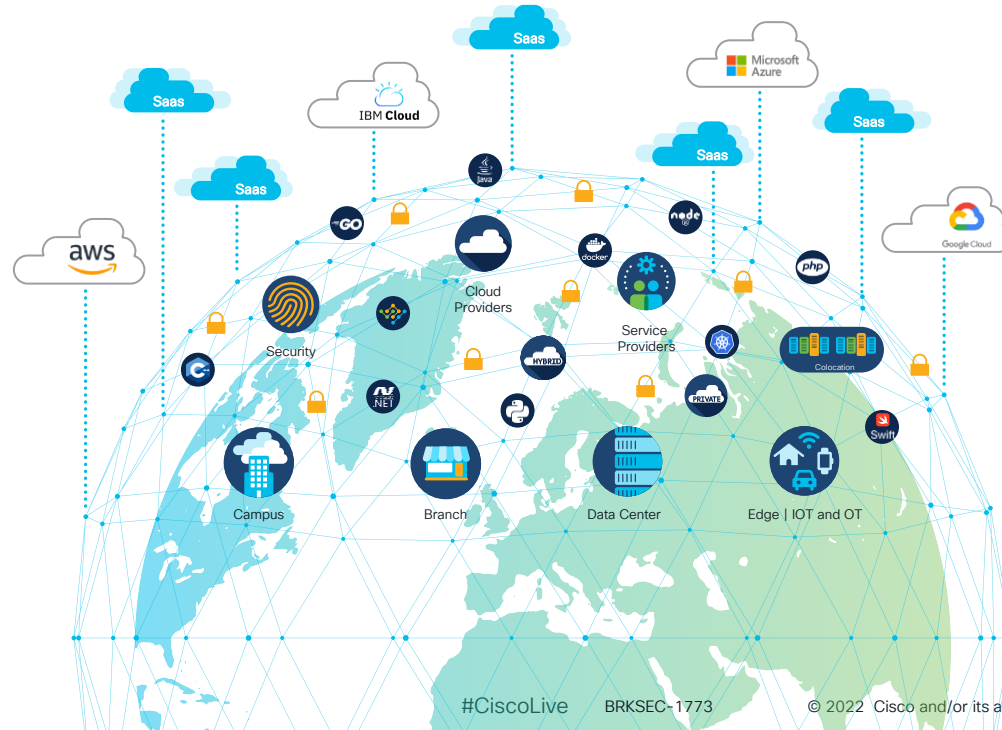
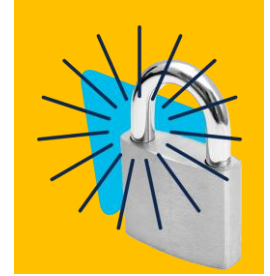
If you want us to use  
on-prem resources,  
they have to be  
consumable via IaC



DevOps

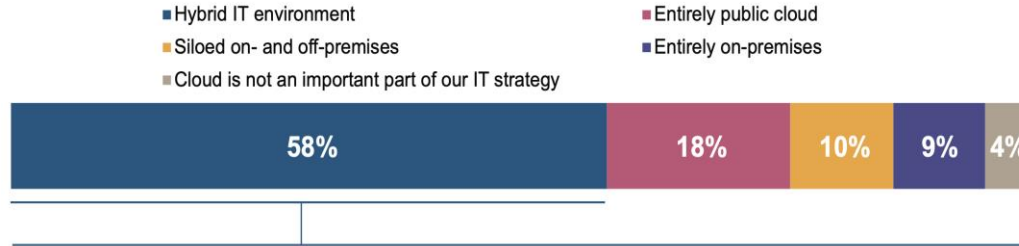


# The internet is your runtime

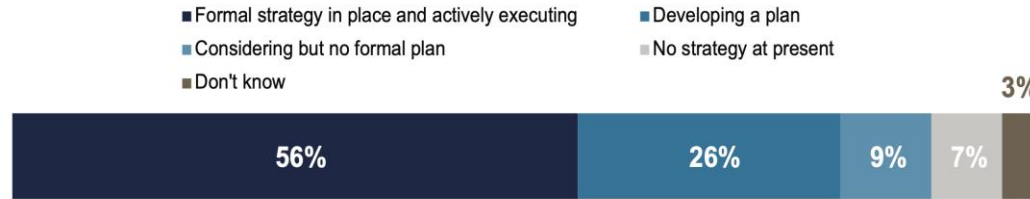


# What is happening on multi cloud

## Strategic Directions for Organizational IT



## State of Hybrid Implementation



Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Vendor Evaluations - Quarterly Advisory Report

The first use of public cloud for many organizations was **experimental**. Small projects or individual efforts were trials to see what it was and how it could be used. Today, most organizations have a **deeper understanding** of public cloud and are putting it to work in some form. The next stage in this journey is **mastering the ability** to coordinate operations across cloud and on-premises environments, a hybrid cloud operational pattern.

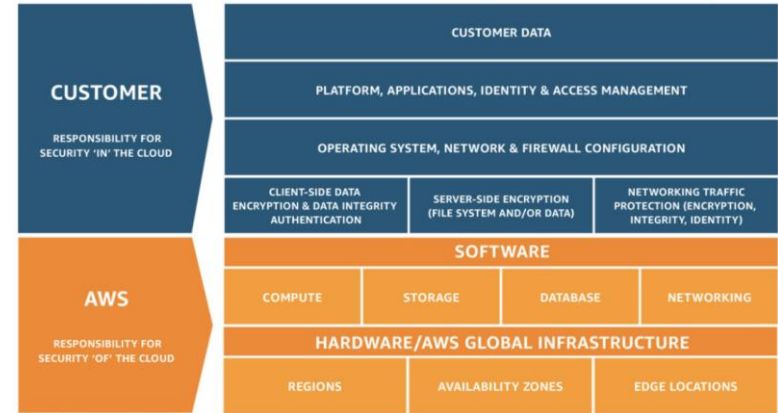
# AWS



# AWS - Shared Responsibility Model

**AWS responsibility “Security of the Cloud”** – AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

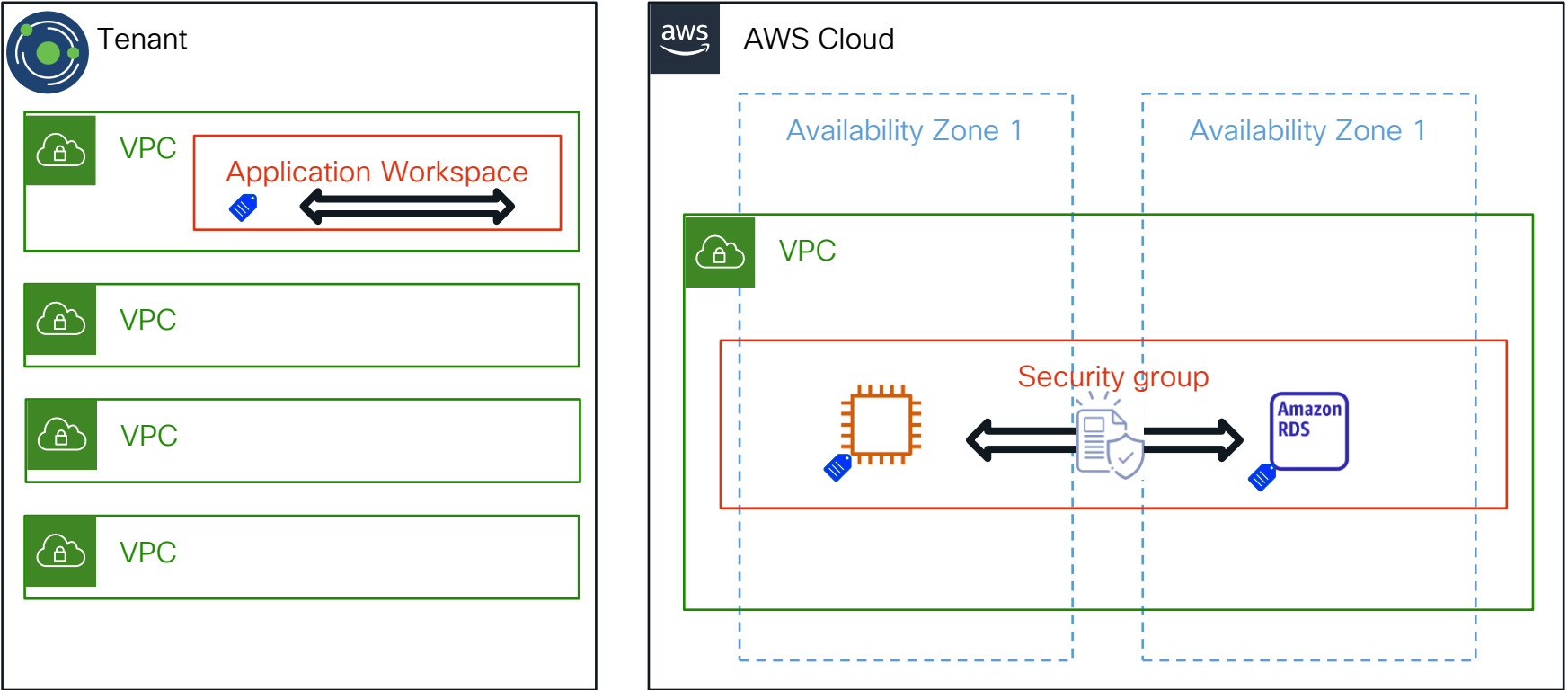
**Customer responsibility “Security in the Cloud”** – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the **AWS-provided firewall (called a security group)** on each instance.



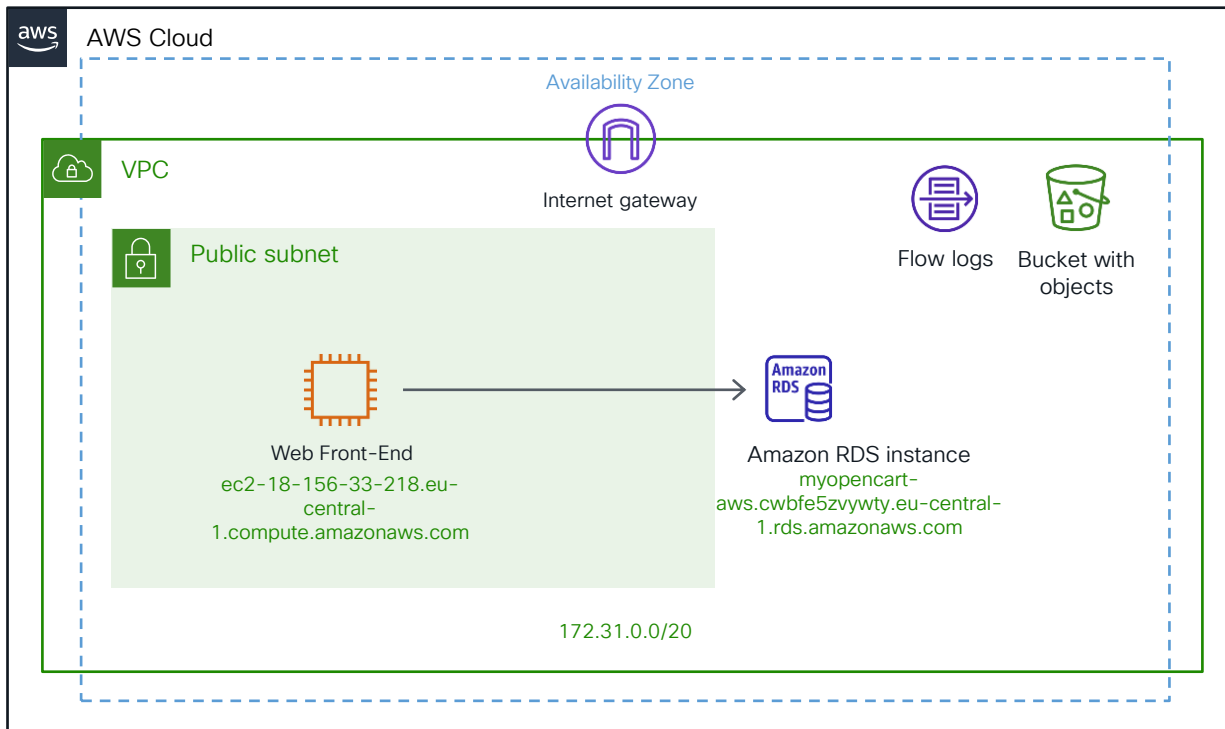
<https://aws.amazon.com/compliance/shared-responsibility-model/>  
<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>



# Policy mapping AWS



# Opencart w/ AWS RDS



# Cisco Secure Workload AWS Connector



Cisco Secure Workload

vpc-54aa3b3e



CISCO SECURE

[Back to Connectors](#)

## Connector



AWS

Enabled on Nov 18th, 2021

Enable Another

Edit Connector

Delete Connector

### Capabilities

Flow Visibility Segmentation

Managed K8s

Inventory Enrichment

AWS BETA

### Info AWS

HTTP Proxy: <http://proxy.esl.cisco.com:80>

Security Groups Per Region: 2500

Total Virtual Networks: 1

Full Scan Interval: 3600 seconds

Security Groups Per Network Interface: 5


Total Kubernetes Clusters: 0

Delta Scan Interval: 60 seconds

Rules per Security Group: 60

IAM Policy: [↓](#)

VPC Id	VPC Name	VPC Region	Gather Labels	Flow Logs Ingest	Segmentation
vpc-54aa3b3e	vpc-54aa3b3e	eu-central-1	enabled	enabled	enabled

	Address ↑↓	* User_Application ↑↓	* User_Database ↑↓	* User_Datacenter ↑↓	* User_ESX ↑↓	* User_Environment ↑↓	* User_ISE_ctsSecurityGroup ↑↓	* User_ISE_d
	172.31.1.152	oc		aws		cloud_app		
	18.156.33.218	oc		aws		cloud_app		

Rows per page

40 ▾

<

1

>

# AWS Ingested Labels



Cisco Secure Workload

Scopes and Inventory / Inventory Profile / Labels and Scopes

## Labels and Scopes

172.31.1.152  
aws Type: TAGGED

Total Security Groups: 1

**LABELS AND SCOPES**

Labels

INTERFACES

ENFORCEMENT HEALTH

CONCRETE POLICIES

SECURITY GROUP POLICIES

Cisco Secure Workload

vpc-54aa3b3e

172.31.1.152  
aws Type: TAGGED

Total Security Groups: 1

Total Concrete Policies: 17

Total Labels: 16

Enforcement Groups: DusLab...2 more

Experimental Groups: DusLab...4 more

Label key T1	Label value T1
user_orchestrator_system/cluster_name	AWS_CONNECTOR
user_orchestrator_system/container_runtime_version	
user_orchestrator_system/hostnetwork	
user_orchestrator_system/interface_id	eni-0d30e61629b753b75
user_orchestrator_system/kernel_version	
user_orchestrator_system/kubelet_version	
user_orchestrator_system/kubeproxy_version	
user_orchestrator_system/machine_id	i-08aaac79c904da53b
user_orchestrator_system/machine_name	ec2-18-156-33-218.eu-central-1.compute.amazonaws.com
user_orchestrator_system/namespace	

Rows per page: 10 < 1 2 3 ... 8 9 10 11 12 >

# Cisco Secure Workload



Cisco Secure Workload

vpc-54aa3b3e



## Flow Search

### Select time range

Sep 11 8:22pm - Nov 22 2:14pm



228,360 total observations

Showing Flow Observations

Enter attributes...

Filter Flows

Flow Observations



Current scope is vpc-54aa3b3e

Current selection: Sep 11 8:22pm to Nov 22 2:14pm

Found 228,360 Flow Observations (149ms)

Show 20

In order

Sampled

Explore Observations

Top Addresses contributing to the selected Flow Observations.

### Consumer Addresses

10.49.166.103

172.31.1.152

### Provider Addresses

18.156.33.218

172.31.34.108

Timestamp ↑	Consumer Name ↑	Provider Name ↑	Consumer Address ↑	Provider Address ↑	Consumer Port ↑	Provider Port ↑	Protocol ↑	Consumer Resource Type ↑
Nov 19 3:41:00pm	Unknown	Unknown	172.31.1.152	172.31.34.108	50478	3306	TCP	Other
Nov 19 3:51:00pm	Unknown	Unknown	172.31.1.152	172.31.34.108	50478	3306	TCP	Other
Nov 19 4:19:00pm	Ansible-7	Unknown	10.49.166.103	18.156.33.218	54322	80	TCP	Workload
Nov 19 4:19:00pm	Ansible-7	Unknown	10.49.166.103	18.156.33.218	54460	80	TCP	Workload

# Cisco Secure Workload

Cisco Secure Workload

PRIMARY

DusLab : AWS : eu-central-1 : vpc-54aa3b3e Version: v2 Last Run: 3:17 PM

Activity Log Matching Inventories 3 Conversations 313 Filters 2 Policies 11 Provided Services Enforcement Status

Quick Analysis Filter Policies ... + Policy

Policy Analysis Enforcement

Scope **vpc-54aa3b3e**

Full Name DusLab:AWS:eu-central-1:vpc-54aa3b3e

Primary App AWS-eu-central-1-vpc-54aa3b3e

Query **\* orchestrator\_system/virtual\_network\_j**  
**or \* Scope = vpc-54aa3b3e**

View Scope Details

> Services 0

> Pods 0

> Workloads 0

> IP Addresses 3

```
graph TD
    subgraph DusLab
        subgraph AWS
            subgraph eu-central-1
                subgraph vpc-54aa3b3e
                    Opencart_Web[Opencart Web]
                    AWS_RDS[AWS RDS]
                    Opencart_Web <--> AWS_RDS
                end
            end
        end
    end
```

# Cisco Secure Workload

The screenshot displays the Cisco Secure Workload interface. At the top, the header shows the Cisco Secure Workload logo and navigation links. The main content area is titled "AWS-eu-central-1-vpc-54aa3b3e" and includes a "PRIMARY" status badge. Below the title, there are tabs for "Activity Log", "Matching Inventories", "Conversations", "Filters", "Policies", "Provided Services", and "Enforcement Status". The "Policies" tab is currently selected, showing a list of policies with columns for Priority, Action, Consumer, Provider, and Protocols And Ports. The table lists three policies, all with a priority of 100 and an action of "ALLOW". The first policy is for "Opencart Web" on "DusLab" with protocols "TCP : 80 (HTTP) ...5 more". The second policy is for "Opencart Web" on "AWS RDS" with protocols "TCP : 3306 (MySQL)". The third policy is for "DusLab" on "Opencart Web" with protocols "TCP : 22 (SSH) ...2 more". To the right of the table, there are links to "Download table data as JSON" and "Download table data as CSV". On the far right, a sidebar shows "Policy Actions" with details for Priority (100), Action (ALLOW), Consumer (DusLab), and Provider (Opencart Web). Below this, there is a section for "Protocols and Ports" showing a list of protocols: "TCP : 22 (SSH)", "TCP : 80 (HTTP)", and "TCP : 443 (HTTPS)".

Cisco Secure Workload

AWS-eu-central-1-vpc-54aa3b3e PRIMARY

DusLab : AWS : eu-central-1 : vpc-54aa3b3e Version: v2 Last Run: 3:17 PM

Activity Log Matching Inventories 3 Conversations 313 Filters 2 Policies 11 Provided Services Enforcement Status

Quick Analysis Filter Policies ...

Absolute policies 0 Default policies 10 Catch All DENY Add Default Policy

Priority	Action	Consumer	Provider	Protocols And Ports
100	ALLOW	Opencart Web	DusLab	TCP : 80 (HTTP) ...5 more
100	ALLOW	Opencart Web	AWS RDS	TCP : 3306 (MySQL)
100	ALLOW	DusLab	Opencart Web	TCP : 22 (SSH) ...2 more

Download table data as JSON Download table data as CSV

Policy Actions

Priority 100

Action ALLOW

Consumer DusLab

Provider Opencart Web

Flows View Conversations

Protocols and Ports 3

- TCP : 22 (SSH)
- TCP : 80 (HTTP)
- TCP : 443 (HTTPS)

Delete All + Add

# Organise by lable



Cisco Secure Workload

vpc-54aa3b3e

cisco SECURE

## Scopes and Inventory

### Scopes

No Draft Changes

Filter Scopes...

36 Scopes and 32 Inventory Filters

**Head-Less-NAS**  
0 Children Inventory: 1

**Duo**  
0 Children Inventory: 2  
Overlaps 1 Scope

**MA01**  
0 Children Inventory: 15

**AWS**  
1 Child Inventory: 3

**eu-central-1**  
1 Child Inventory: 3

**vpc-54aa3b3e**  
0 Children Inventory: 3



DusLab : AWS : eu-central-1  
vpc-54aa3b3e

Primary Workspace

AWS-eu-central-1-vpc-54aa3b3e

Query

\* orchestrator\_system/virtual\_network\_id = vpc-54aa3b3e  
or \* Scope = vpc-54aa3b3e

Delete Edit Add

All Inventory 3

Overlapping Scopes 0

Suggested Child Scopes

Usages

Enter attri

Services 0

Showing 3 of

\* orchestrator\_system/orch\_type = aws  
\* orchestrator\_system/region = eu-central-1  
\* orchestrator\_system/virtual\_network\_id = vpc-54aa3b3e

Address ↑↓
18.156.33.218
172.31.34.108
172.31.1.152

Public IP of EC2 instance

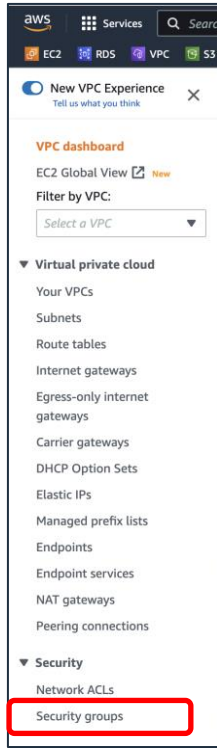
Private IP of RDS DB instance

Private IP of EC2 instance

CISCO Live!



# AWS view on the policy – Inbound rules



sg-03197f5656cb1e2d9 - csw\_2d67c1ff\_1548786950\_000\_1655241904

**Details**

Security group name csw_2d67c1ff_1548786950_000_1655241904	Security group ID sg-03197f5656cb1e2d9	Description Cisco Secure Workload Security group for npc version(1548786950) with filtersHash(2d67c1ff)	VPC ID vpc-0d078cb997c1b563d
Owner 104129875034	Inbound rules count 15 Permission entries	Outbound rules count 10 Permission entries	

**Inbound rules** | Outbound rules | Tags

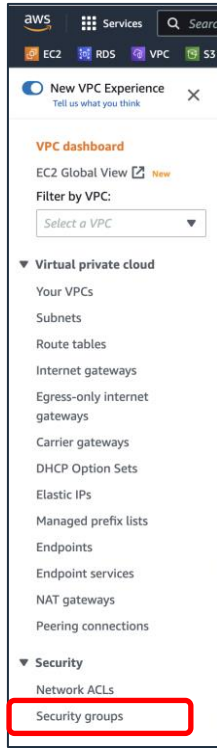
You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

**Inbound rules (15)**

Filter security group rules

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sg-0de8374fde775eb80	IPv4	All ICMP - IPv4	ICMP	All	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0f204d07a81759a3e	IPv4	HTTP	TCP	80	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-05affe0de6f5cd7c0	IPv4	DNS (UDP)	UDP	53	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0f81e92686bd126...	IPv4	HTTPS	TCP	443	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0f2d541309e13f752	IPv4	HTTPS	TCP	443	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0f297307c2580fee6	IPv4	HTTP	TCP	80	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-04393c6778e28ee9c	IPv4	SSH	TCP	22	10.49.166.105/32	PolicyId=ABSOLUTE:100:ALLOW:61a61206755f025bdf4363a619...
<input type="checkbox"/>	-	sg-04e6173a635b9ffae	IPv4	DNS (UDP)	UDP	53	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0a2f60ee9e51b1d42	IPv4	DNS (UDP)	UDP	53	172.31.6.162/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0d620152e1697a...	IPv4	Custom UDP	UDP	123	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-018a72f12087a2e67	IPv4	SSH	TCP	22	10.49.166.105/32	PolicyId=ABSOLUTE:100:ALLOW:61a61206755f025bdf4363a619...
<input type="checkbox"/>	-	sg-0c602ec9e2fde6eb1	IPv4	Custom UDP	UDP	123	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0ffb398a84c45706d	IPv4	HTTP	TCP	80	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f43c45:61a80...
<input type="checkbox"/>	-	sg-0e45f81a18de68e1e	IPv4	All ICMP - IPv4	ICMP	All	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3842f1:619fc...
<input type="checkbox"/>	-	sg-0fbd9d460298194...	IPv4	SSH	TCP	22	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f43c45:61a80...

# AWS view on the policy –Outbound Rules



## sg-03197f5656cb1e2d9 - csw\_2d67c1ff\_1548786950\_000\_1655241904

Actions

### Details

Security group name csw_2d67c1ff_1548786950_000_1655241904	Security group ID sg-03197f5656cb1e2d9	Description Cisco Secure Workload Security group for npc version(1548786950) with filtersHash(2d67c1ff)	VPC ID vpc-0d078cb997c1b563d
Owner 104129875034	Inbound rules count 15 Permission entries	Outbound rules count 10 Permission entries	

Inbound rules | **Outbound rules** | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

### Outbound rules (10)

Filter security group rules

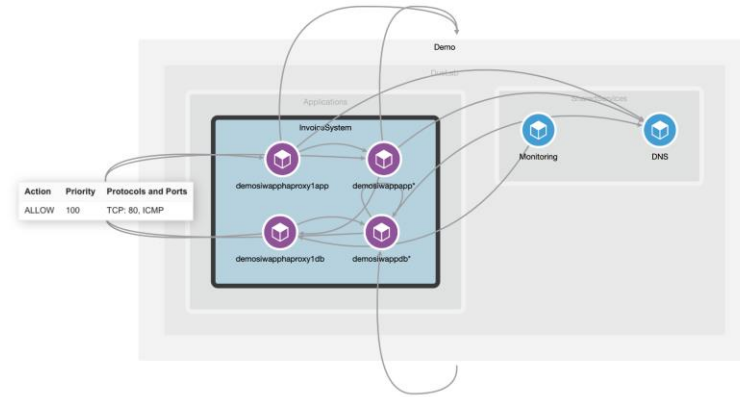
	Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
<input type="checkbox"/>	-	sgr-0e902386c4d68de...	IPv4	HTTP	TCP	80	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f4...
<input type="checkbox"/>	-	sgr-04140b71fd5c825f7	IPv4	MySQL/Aurora	TCP	3306	172.31.6.162/32	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3...
<input type="checkbox"/>	-	sgr-01565ba6b075b4...	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:61a4fc2c755f024910f4...
<input type="checkbox"/>	-	sgr-0f99b72eb817a284b	IPv4	HTTP	TCP	80	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f4...
<input type="checkbox"/>	-	sgr-07c785e67ae87af2e	IPv4	HTTP	TCP	80	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3...
<input type="checkbox"/>	-	sgr-0948629a2f93fa193	IPv4	HTTPS	TCP	443	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3...
<input type="checkbox"/>	-	sgr-07a6b3bdf0438c244	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3...
<input type="checkbox"/>	-	sgr-05eec3e6efdf0bb8d	IPv4	Custom UDP	UDP	123	0.0.0.0/0	PolicyId=DEFAULT:100:ALLOW:61a80252d41170396f3...
<input type="checkbox"/>	-	sgr-09637944ab28c4ebc	IPv4	SSH	TCP	22	3.66.214.125/32	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f4...
<input type="checkbox"/>	-	sgr-0d9e23b2f832521...	IPv4	SSH	TCP	22	172.31.0.247/32	PolicyId=DEFAULT:100:ALLOW:619fccbb755f024e84f4...

# Conclusion

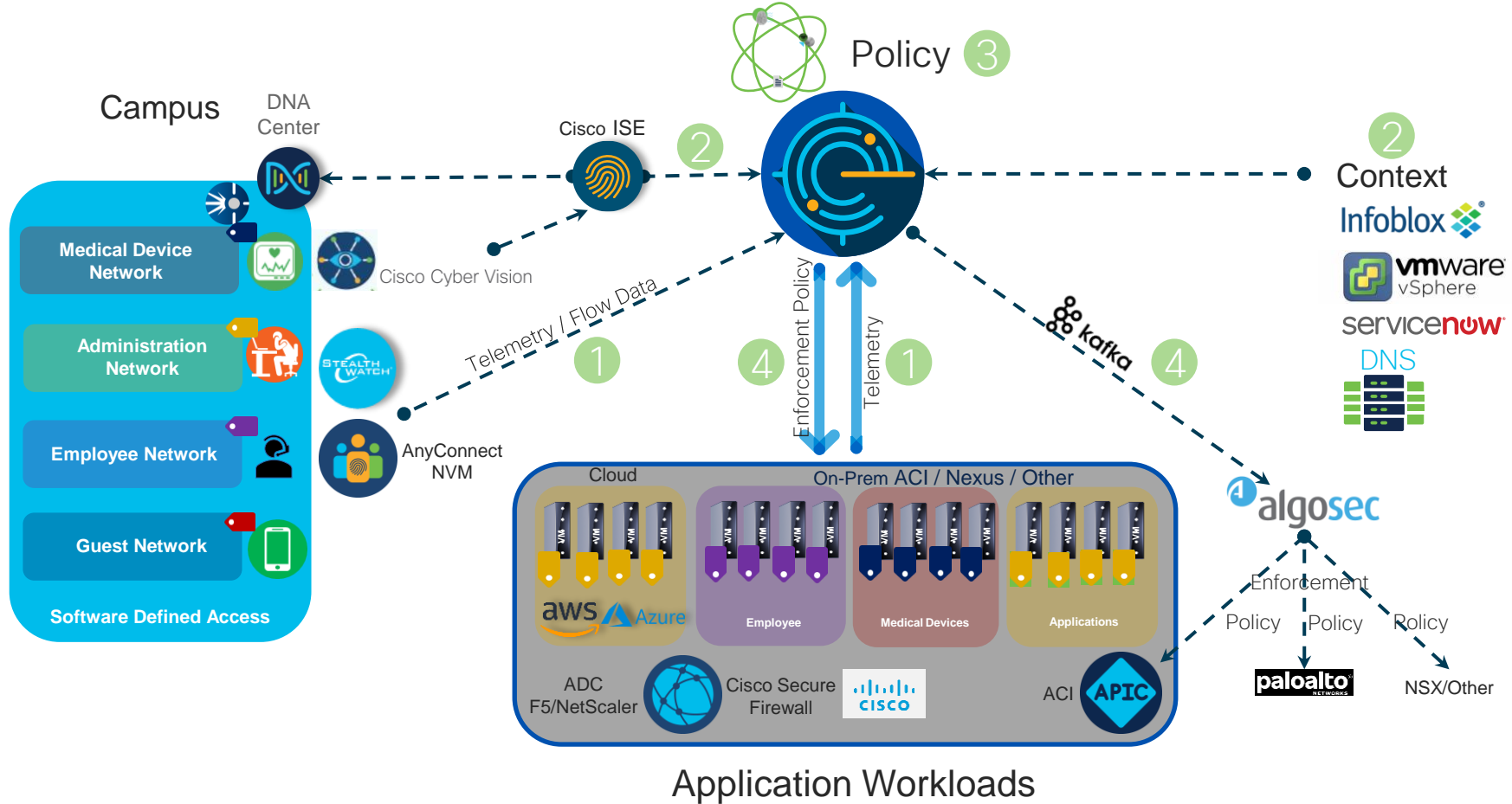


# Micro segmentation strategy

- Protect your app / deployment from access from the beginning
- Build a policy from outside in
- Continuously optimise your policy, established process for policy live cycle
- Include application owner and NetSecOps from the beginning



# Zero Trust Architecture



# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.





# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

### Cisco Guided Study Groups

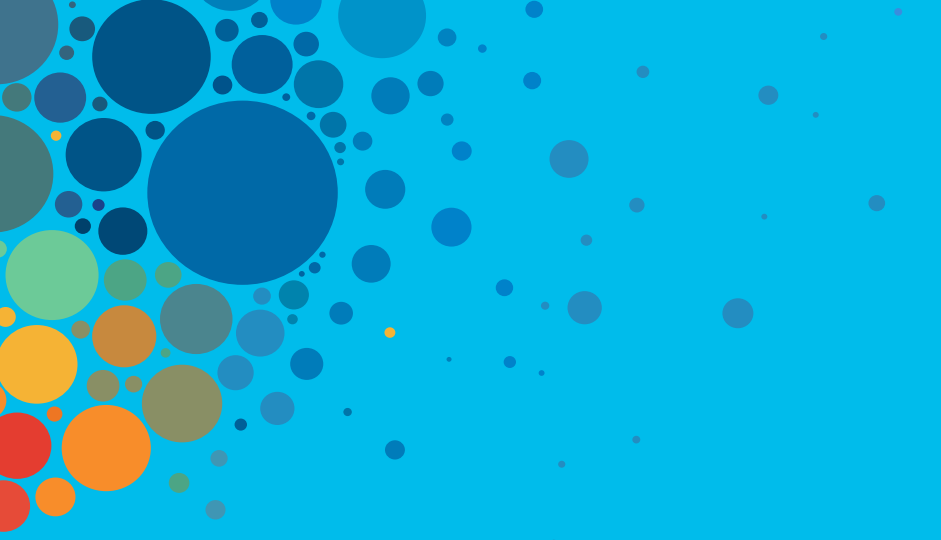
180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**





# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive