The bridge to possible

Security as Code

Automating Public Cloud Security with Cisco Multicloud Defense and Terraform

David Staudt – DevNet Developer Advocate
@dstaudtatcisco

DEVNET-2136

cisco Live!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2136

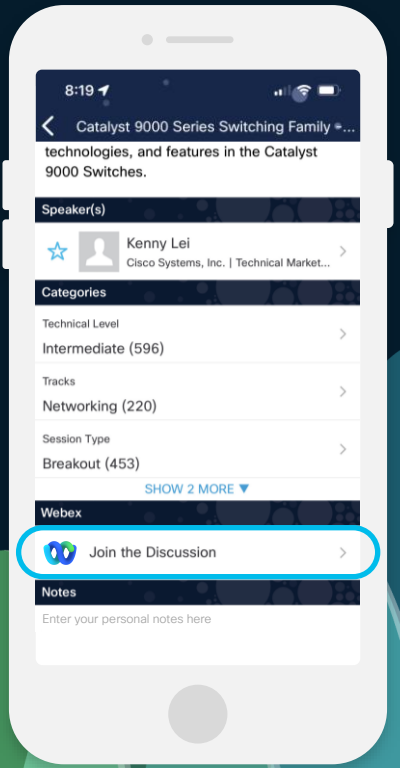
Questions?

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

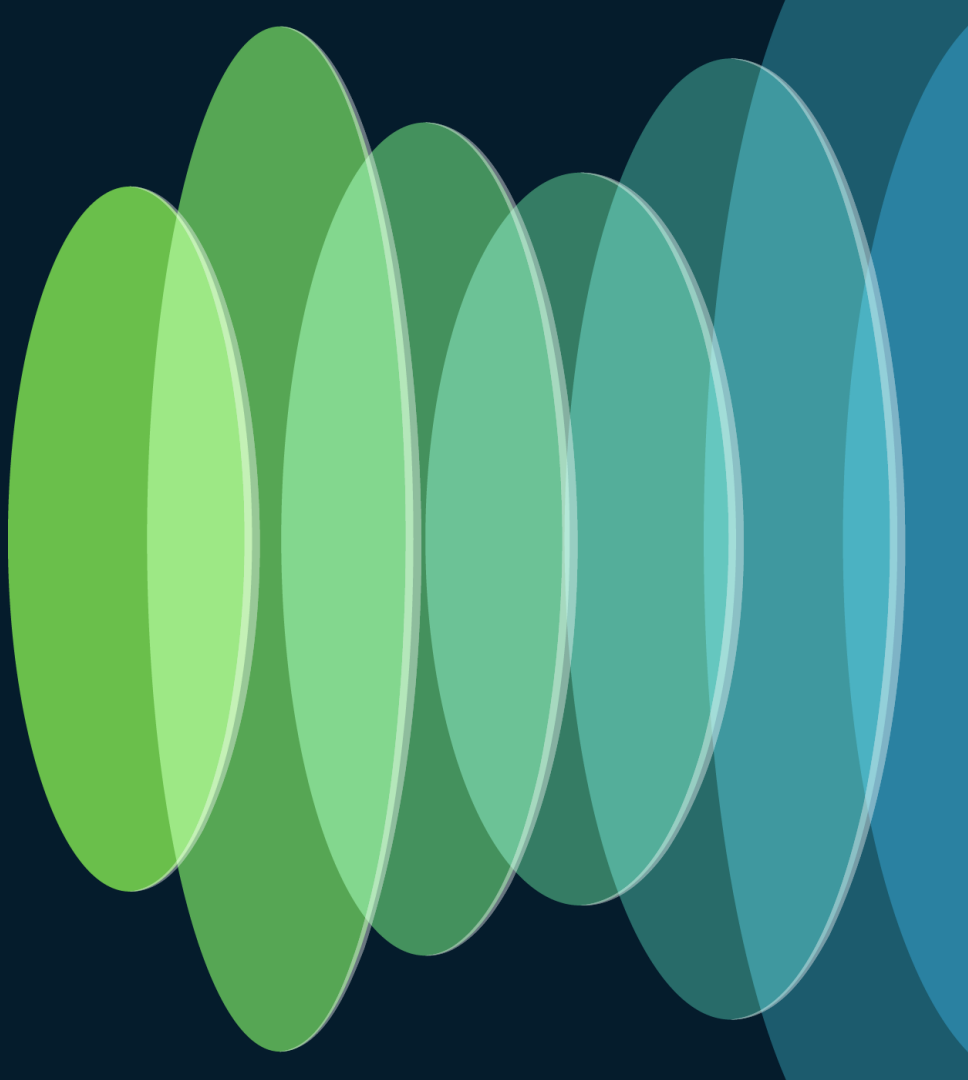
Webex spaces will be moderated by the speaker until June 7, 2024.



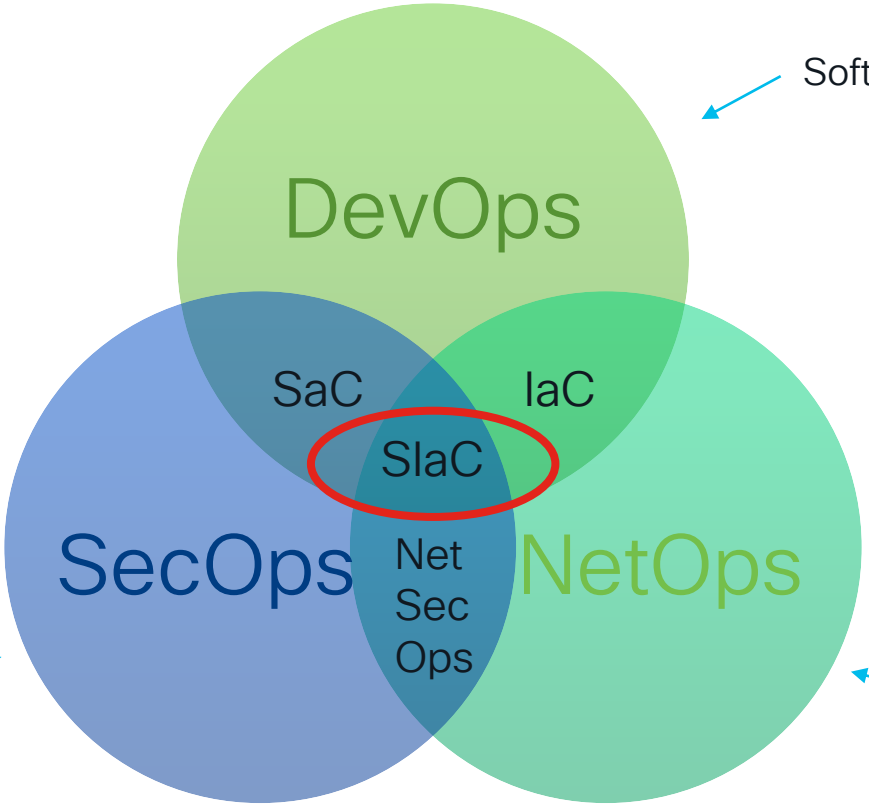
Agenda

- Security as Code
- What is Terraform?
- What is Cisco Multicloud Defense?
- GitHub Project Overview
- Demo / Walk-Through
- Going Further

Security Infrastructure as Code



Security Infrastructure as Code

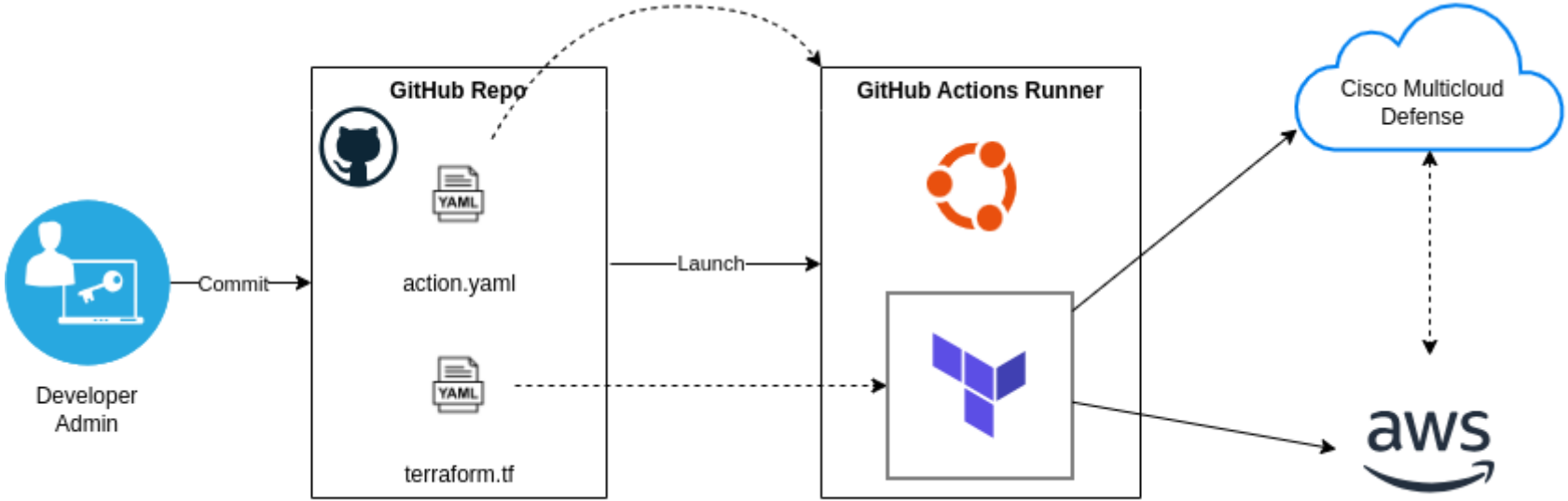


Software deployment automation

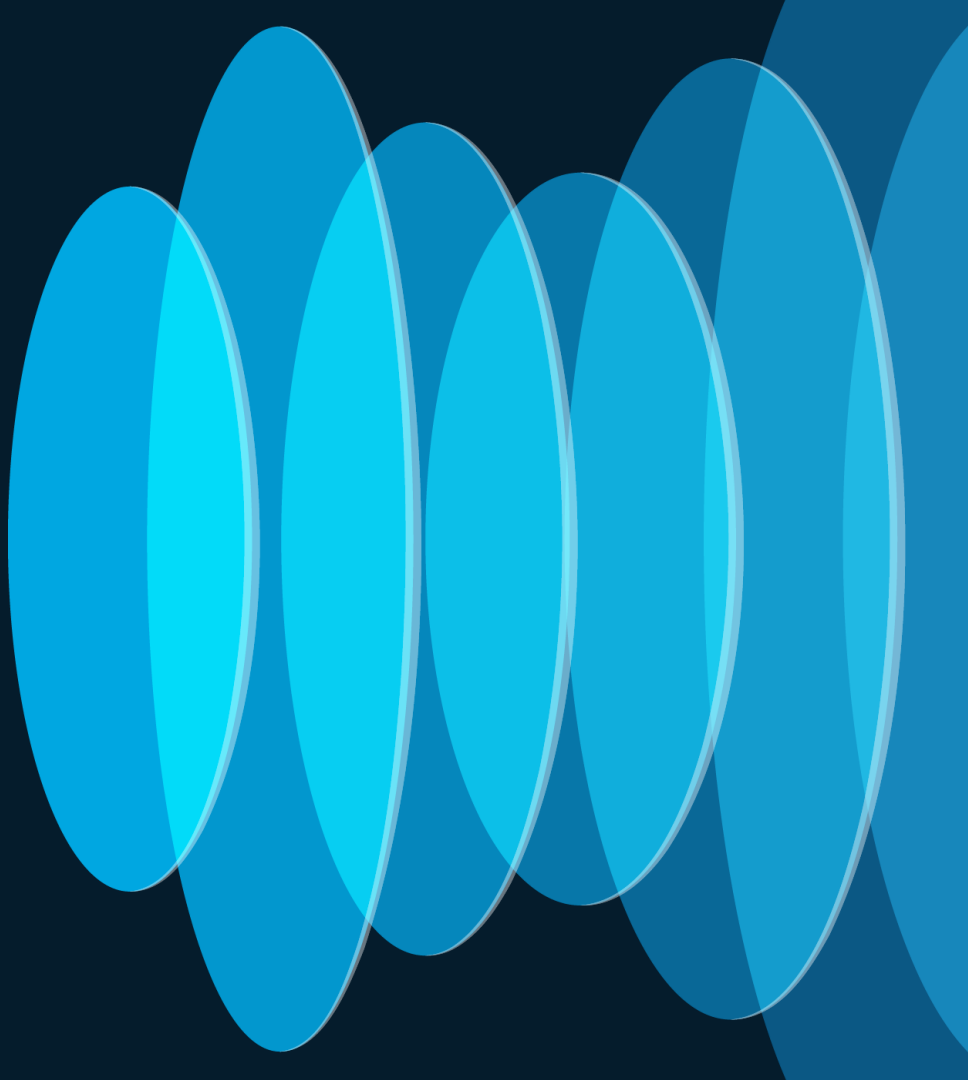
Security config automation

Network config automation

Security Infrastructure as Code - Pipeline



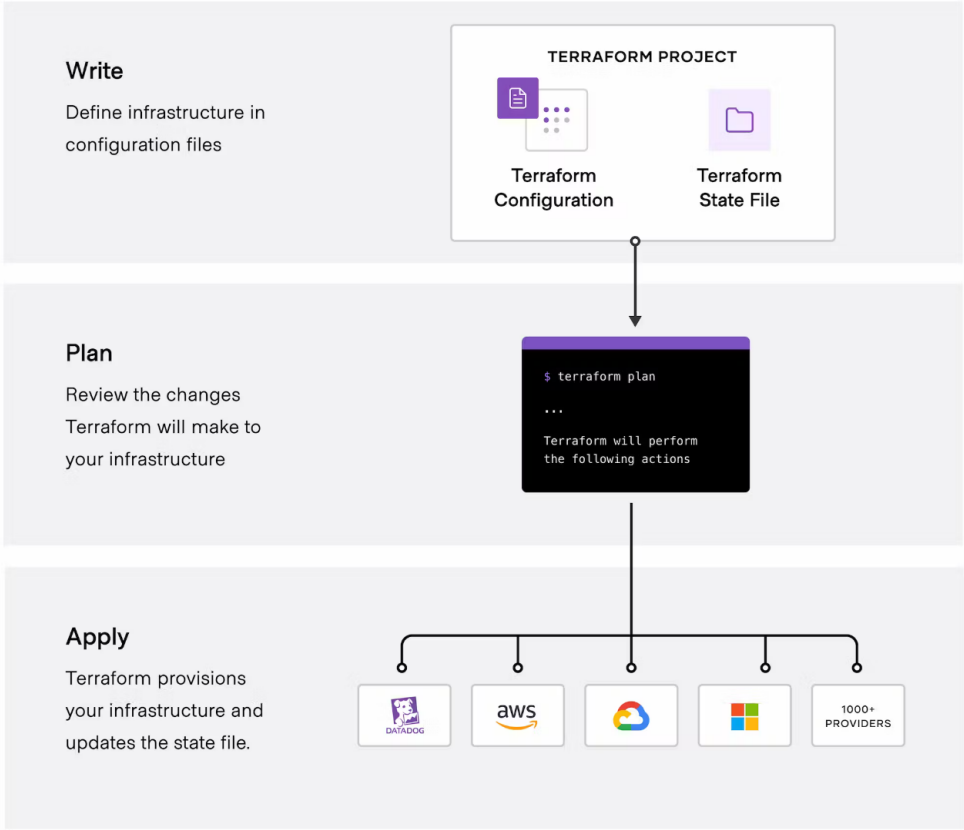
What is Terraform?



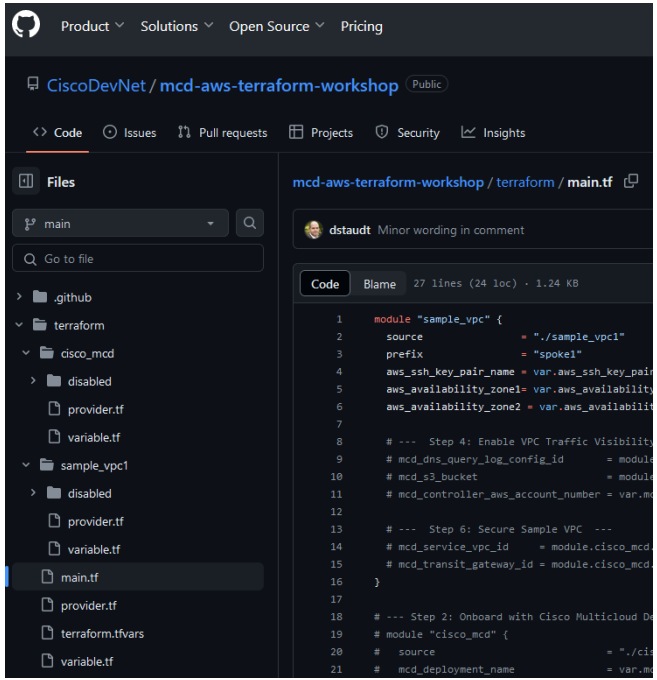
What is Terraform?

- Define infrastructure using human / machine readable config files
- Single source-of-truth
- Declarative – desired state vs. step-by-step
- Automated provisioning of cloud / on-prem components
- Built-in and third-party providers abstract and affect the configuration via APIs

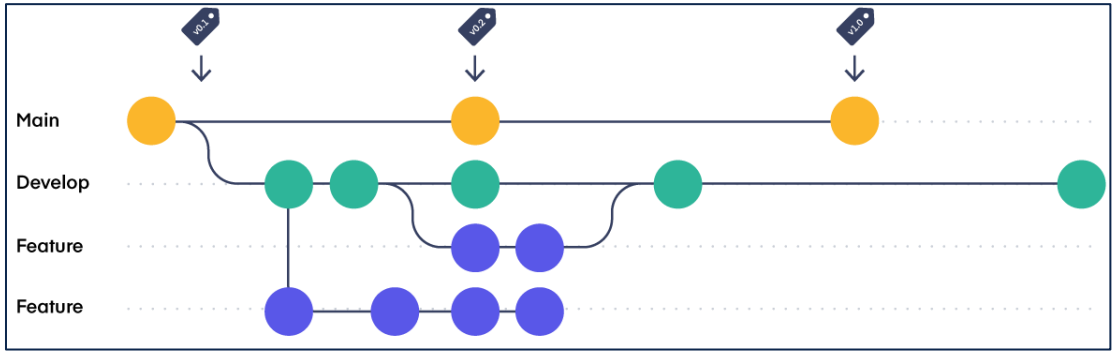
Infrastructure as Code



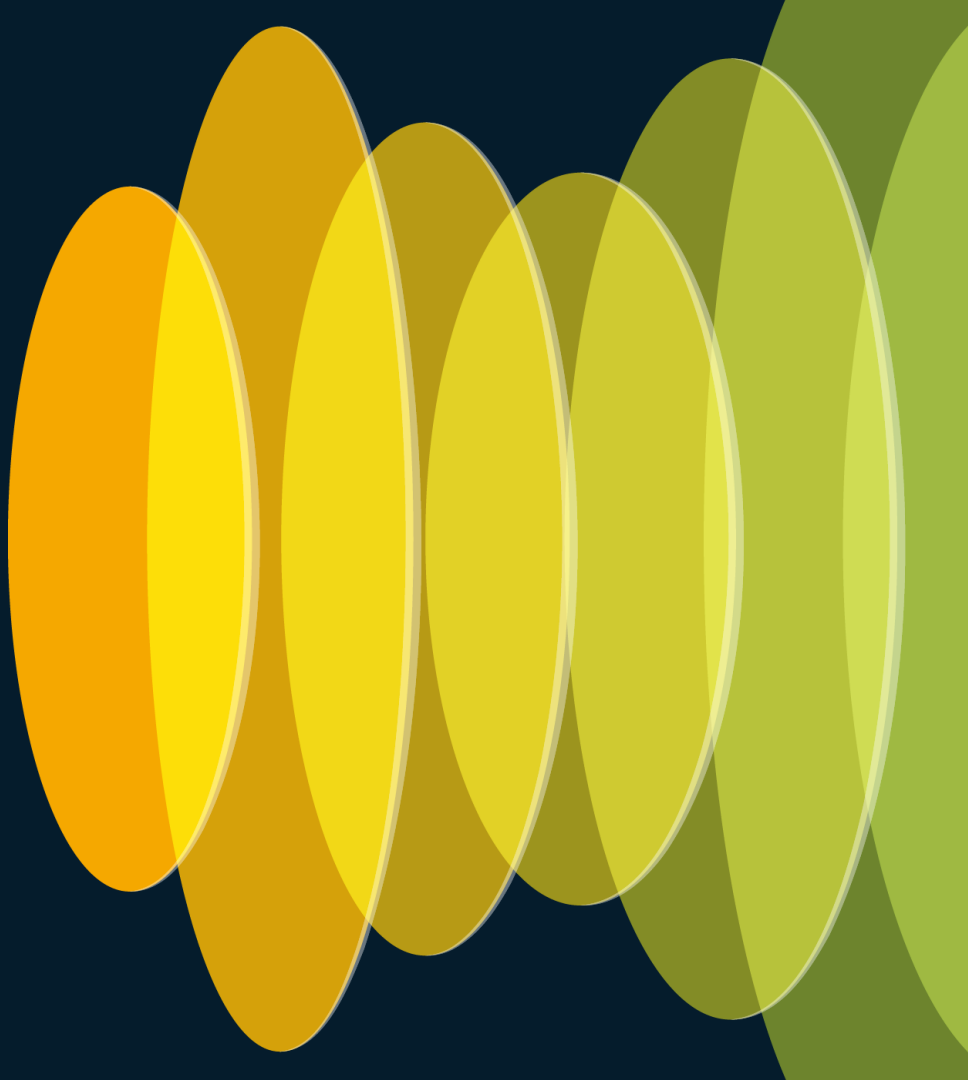
Single Source-of-Truth



Version control workflow



What is Cisco Multicloud Defense?



Cisco Multicloud Defense

Protect all your cloud environments using a single SaaS control-plane

Simplify multicloud security

Manage security across public and private clouds from one place. Create, enforce, and update policies across all your clouds in real time.

Gain multidirectional protection

Ingress, egress, and east-west protection stops inbound threats, blocks command and control, data exfiltration, and prevents lateral movement.

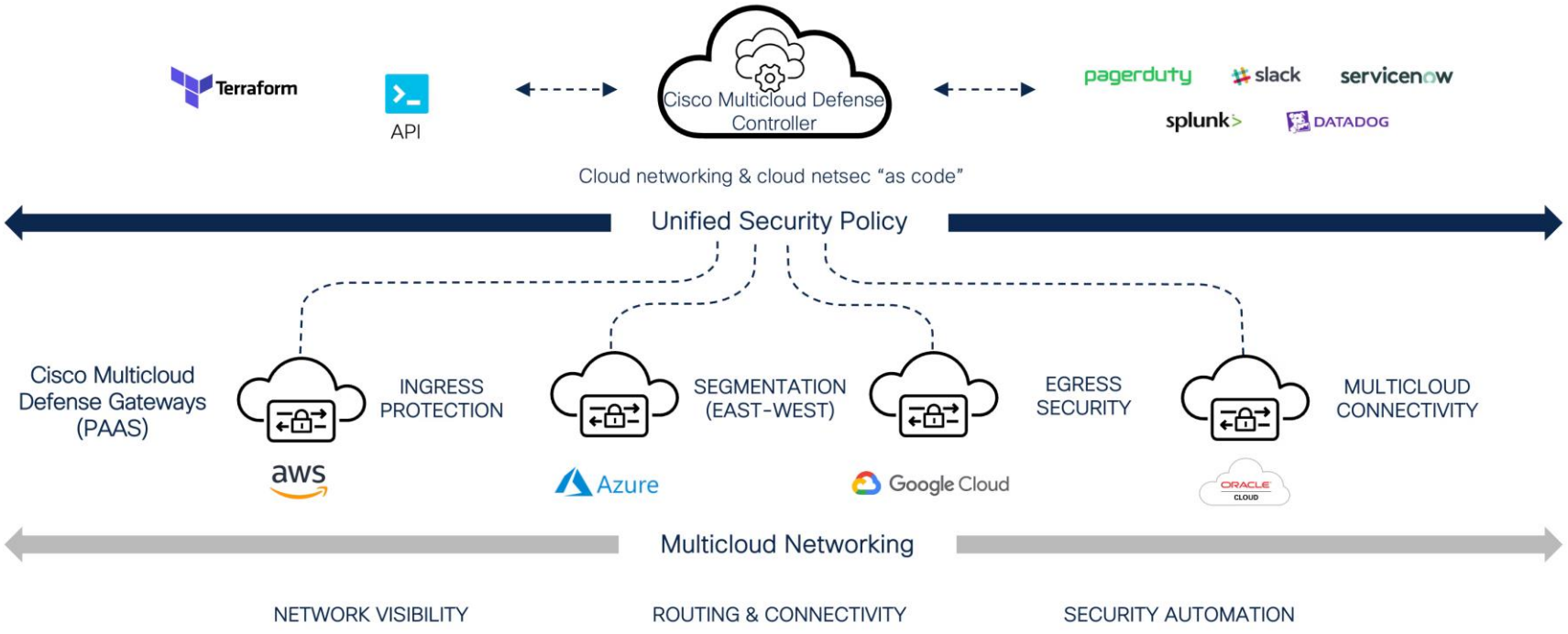
Increase operational efficiency

Automate underlying cloud network constructs and integrate with infrastructure as code (IaC) for greater agility, flexibility, and scale.

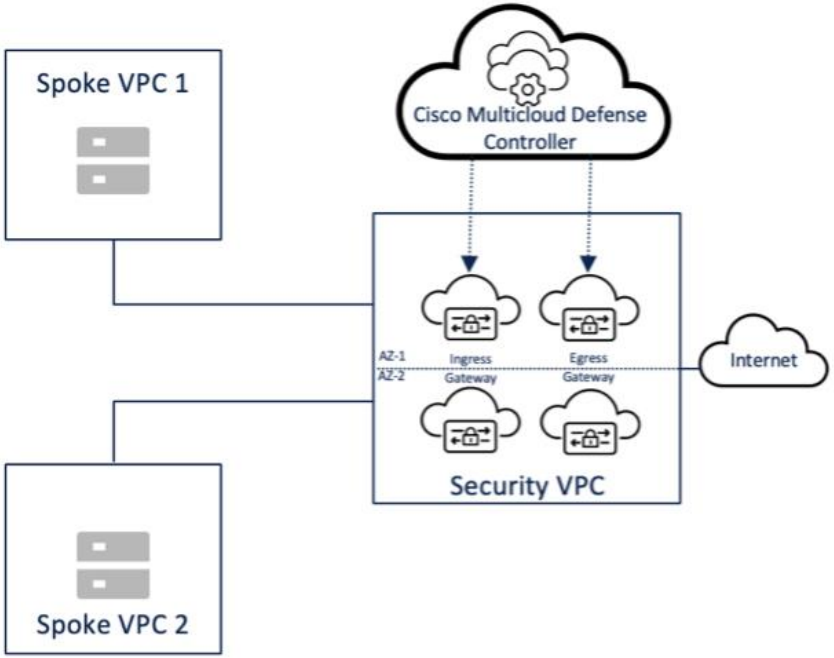
Reduce risk, maintain compliance

Proactively close security gaps within your cloud environment using real-time asset discovery.

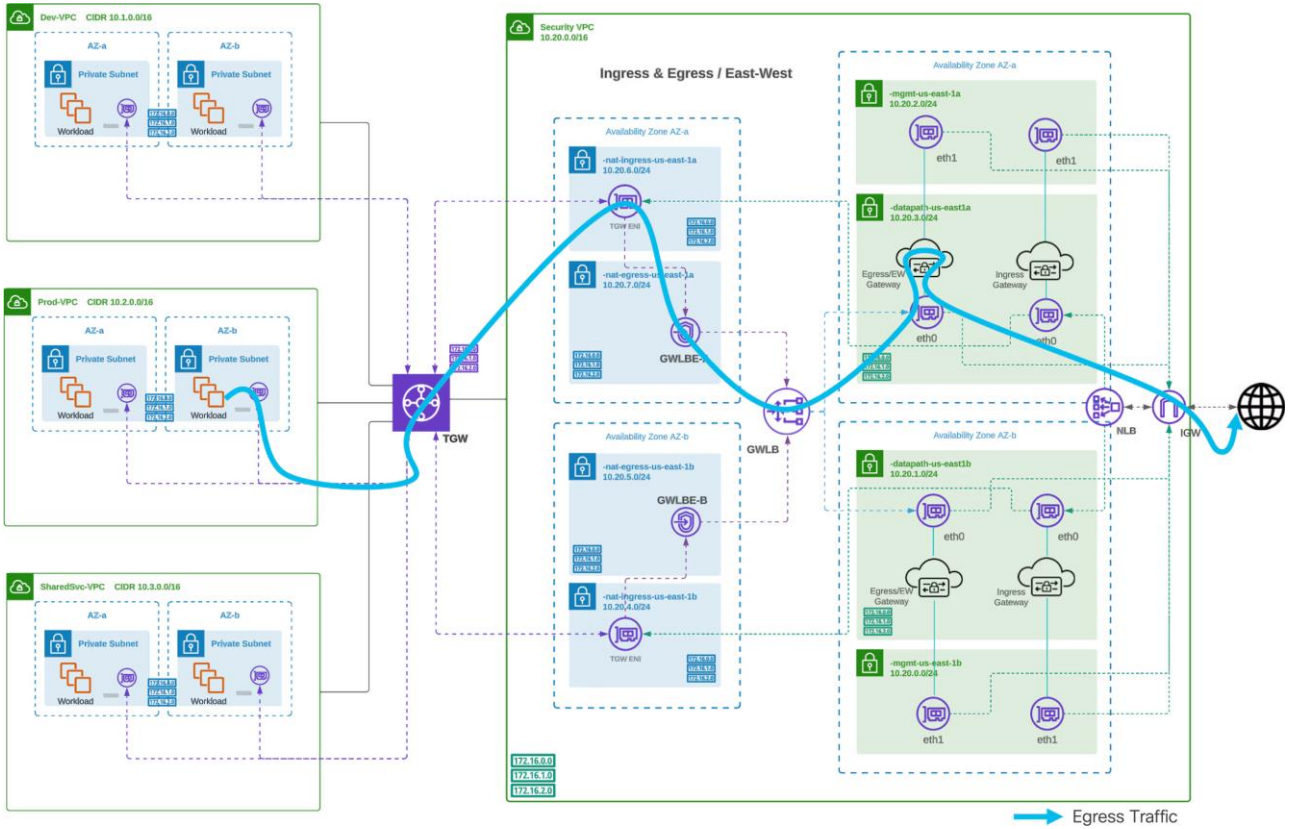
Cisco Multicloud Defense – How does it work?



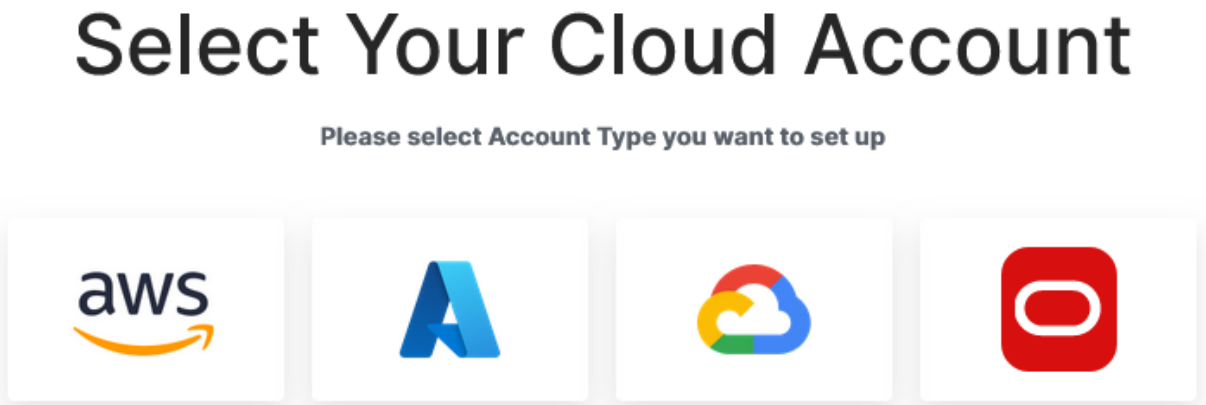
Cisco Multicloud Defense – Hub and Spoke



Cisco Multicloud Defense – How does it work?



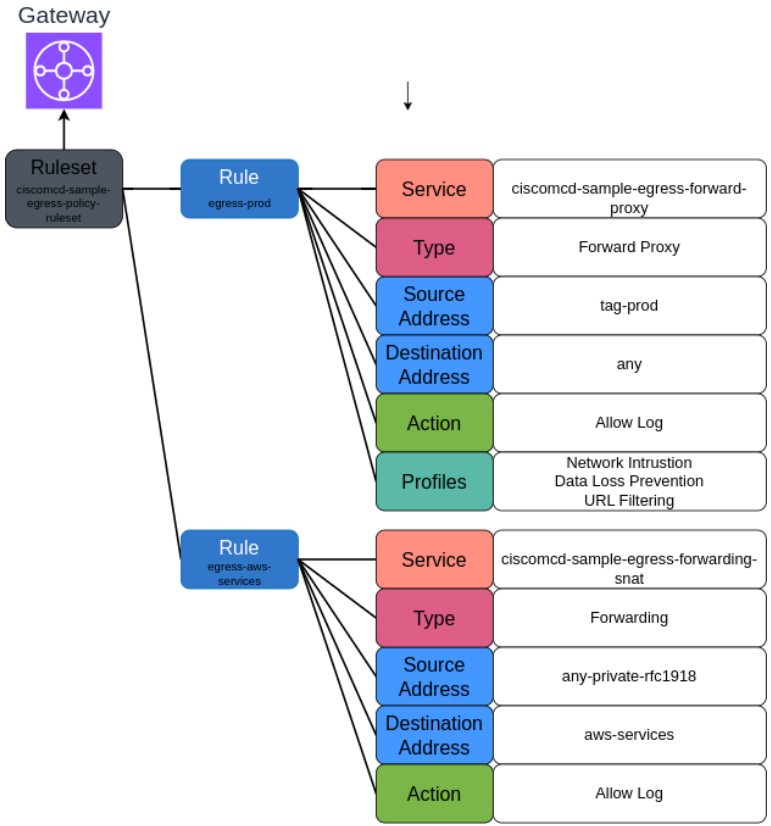
Putting the “Multi” in Multicloud



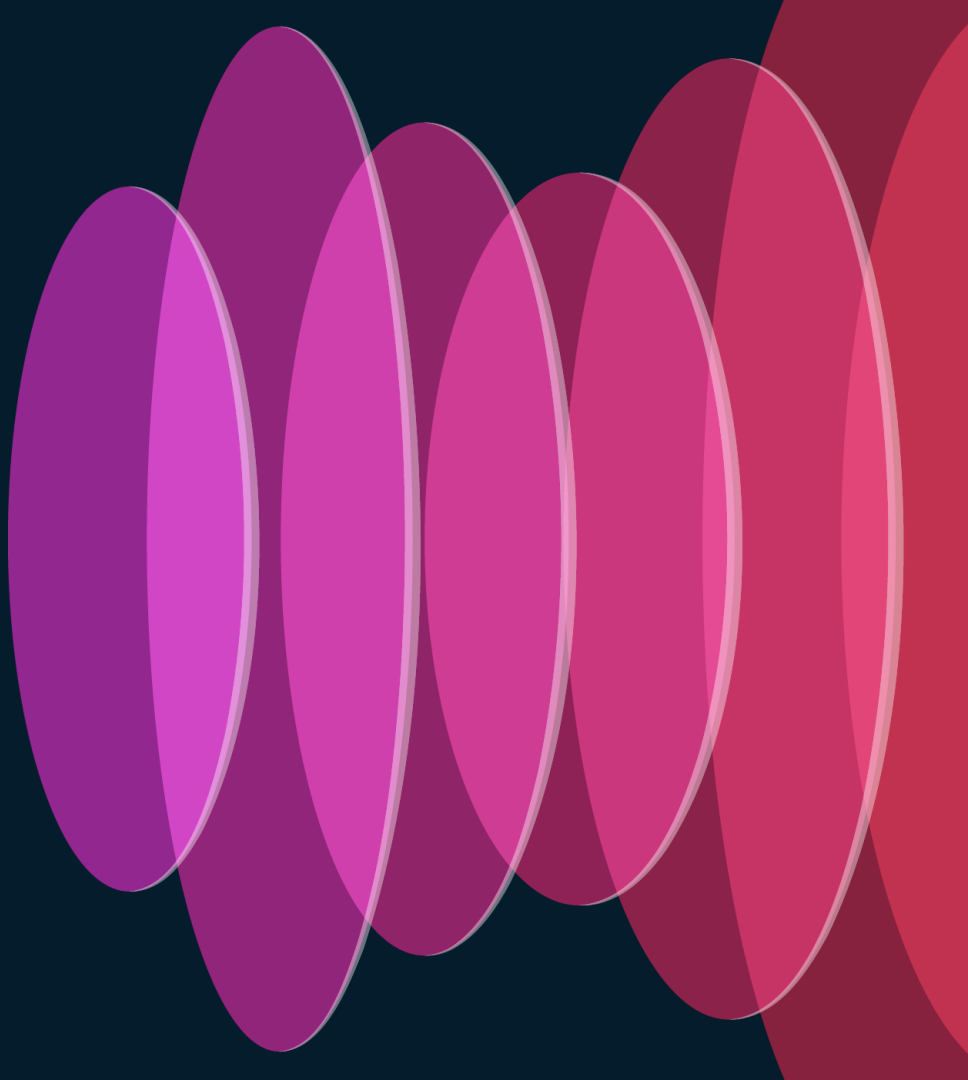
Cisco Multicloud Defense – Capabilities

- Decryption
- URL Filtering
- IPS / IDS
- FQDN Filtering
- Data Loss Prevention
- Malicious IPs
- Anti Malware
- Packet Capture
- Web App Firewall
- Log Forwarding
- Layer 7 DoS
- Metrics Forwarding
- NTP
- IPSEC / BGP

Cisco Multicloud Defense - Policies

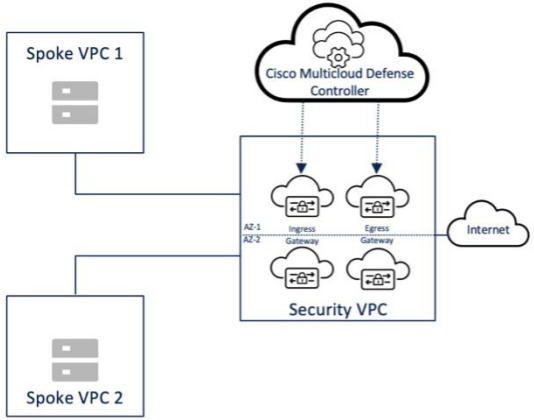


SIaC Project Overview



SlaC Project Overview and Tour

- Build and test a simple DevOps / SlaC pipeline using Terraform and GitHub Actions to deploy and update cloud configurations.
- Deploy and verify Cisco Multicloud Defense traffic / flow monitoring for a sample AWS private virtual cloud.
- Implement Cisco Multicloud Defense protection capabilities and configure custom security rules.



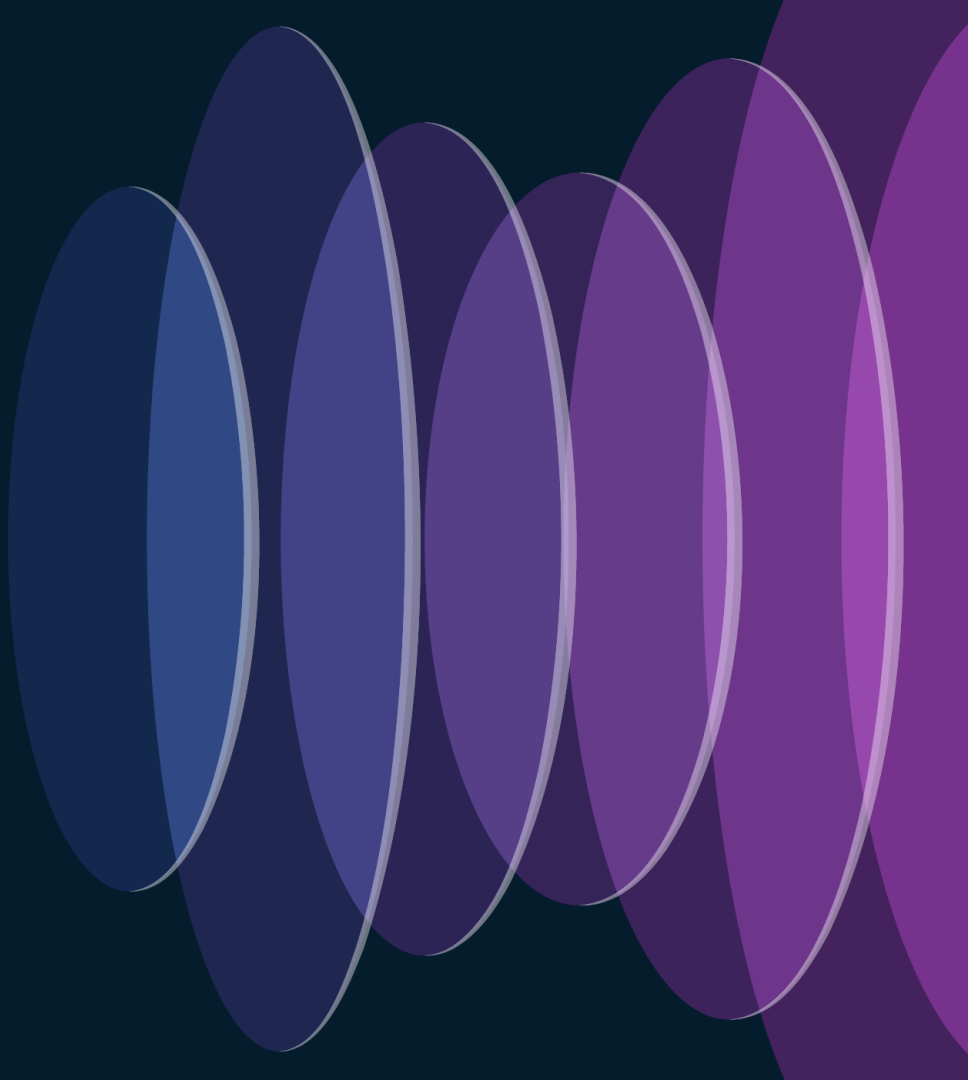
Learning Lab

CiscoDevNet/mcd-aws-terraform-workshop

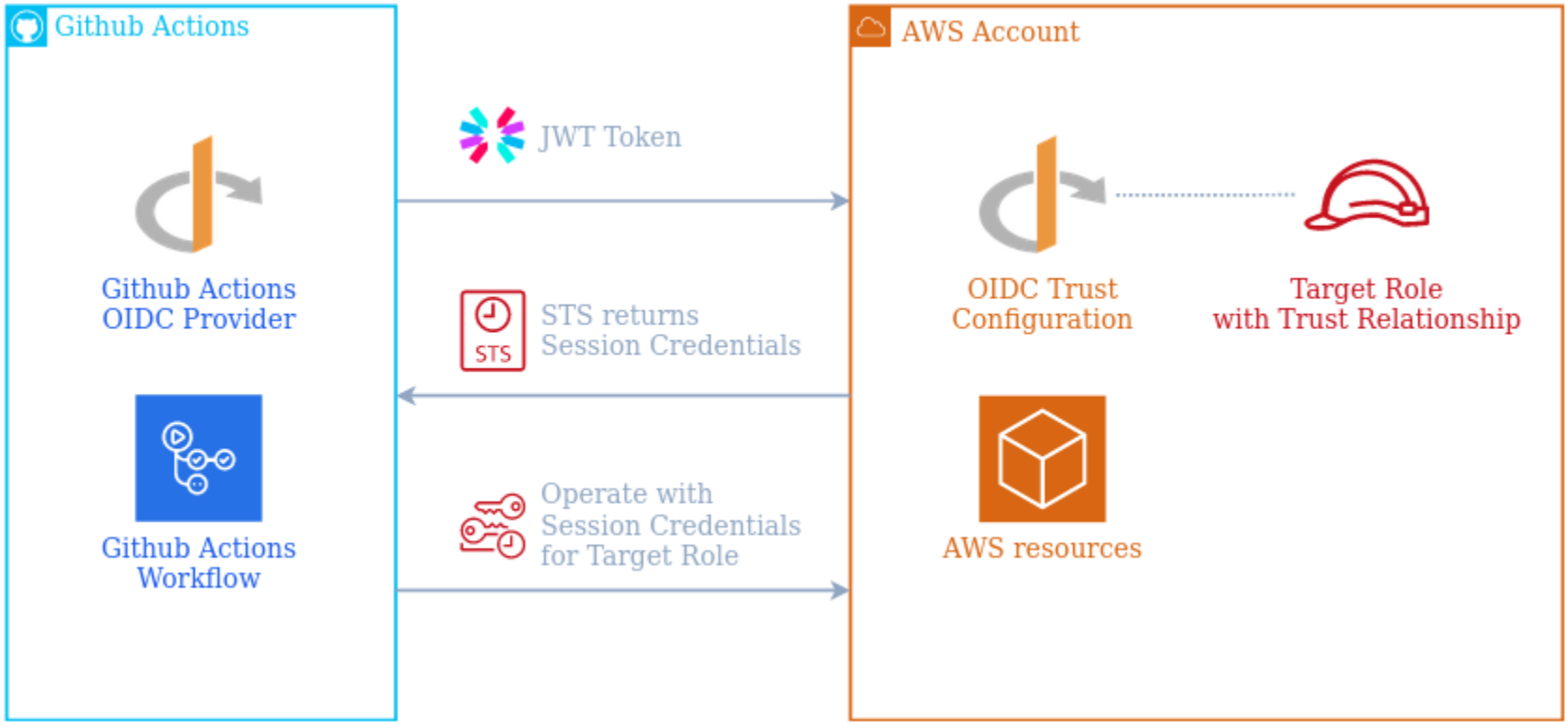
SlaC Project – Step-by-Step

1. **Infrastructure:** Create base application VPC + instances.
2. **Prepare** – Create IAM policies / roles.
3. **Discover** – Configure logging to S3 bucket, onboard AWS account to Multicloud Defense.
4. **Monitor** – Modify VPC to forward DNS query and flow logs to the S3 log bucket.
5. **Deploy** – Provision the Multicloud Defense service VPC + transit gateway.
6. **Protect** – Modify VPC to route all traffic through the service VPC – attach app VPC to service VPC.
7. **Defend** – Configure custom security policies to detect / prevent exfiltration of social security numbers and restrict GitHub URLs.
8. **Cleanup** – With a single command.

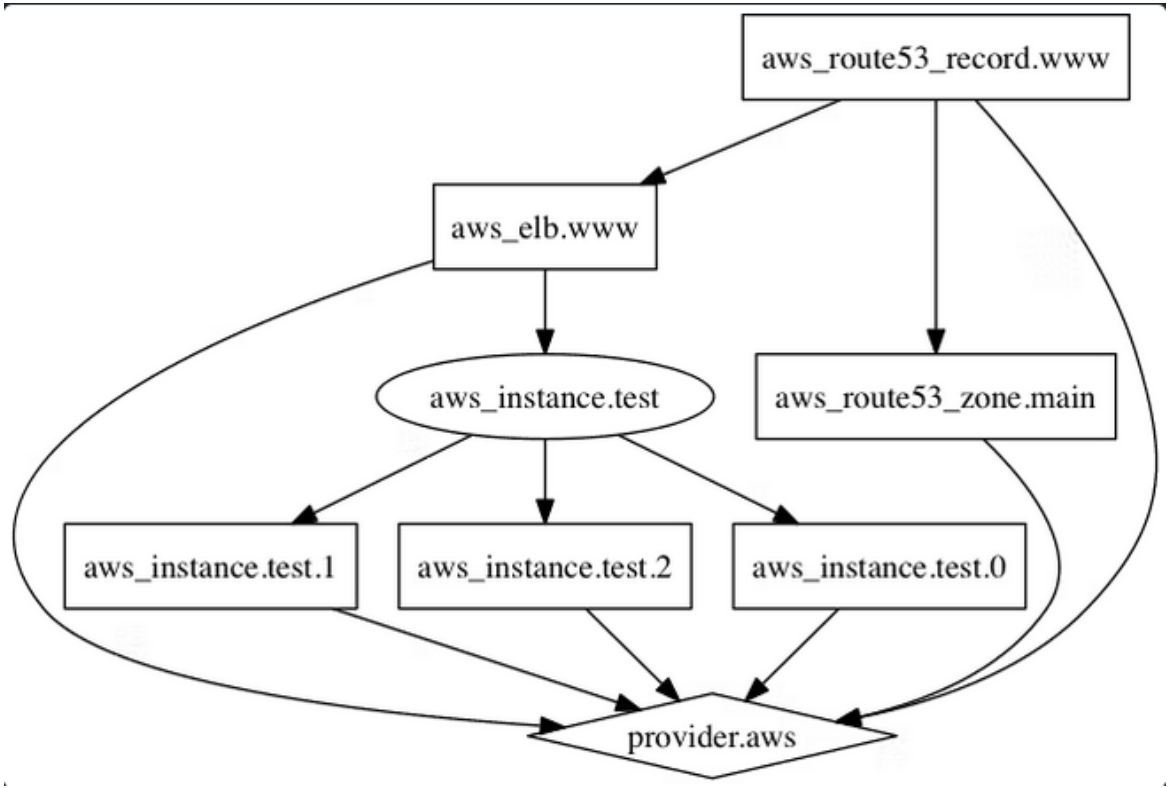
Demo / Walk-through



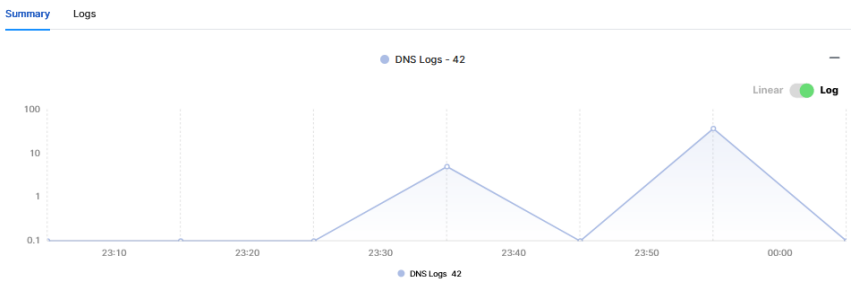
GitHub OIDC Auth in AWS



Terraform Dependencies

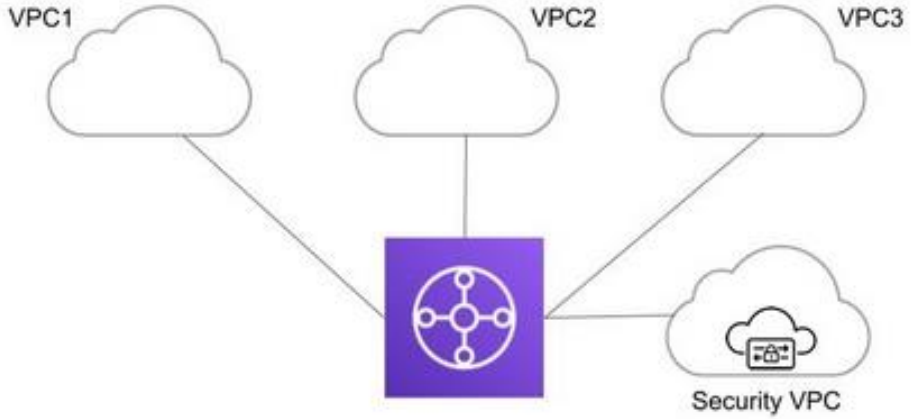


DNS Traffic

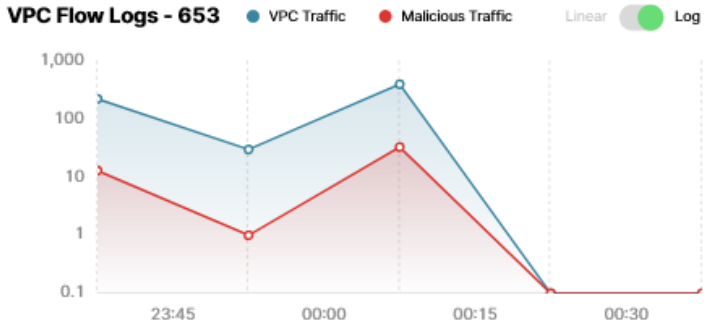


Details		Instance Info		DNS		
Date and Time (UTC)		Instance Name		Resolved IP	FQDN	Dest Country
2023-11-16T22:13:49.0...		spoke1-z1-app	tags	34.237.137.22	us-east-1.ec2.archive.ubuntu.com.	United States
2023-11-16T22:13:49.0...		spoke1-z1-app	tags		_http._tcp.security.ubuntu.com.	
2023-11-16T22:13:42.0...		spoke1-z1-app	tags	2a03:2880:f1...	www.facebook.com.	
2023-11-16T22:13:42.0...		spoke1-z1-app	tags	31.13.66.35	www.facebook.com.	United States
2023-11-16T22:13:32.0...		spoke1-z1-app	tags	2607:f8b0:40...	www.google.com.	
2023-11-16T22:13:32.0...		spoke1-z1-app	tags	142.251.16.1...	www.google.com.	United States
2023-11-16T22:13:29.0		spoke1-z1-app	tags		ssmmessages.us-east-1.amazona	

Hub and Spoke – Transit Gateway

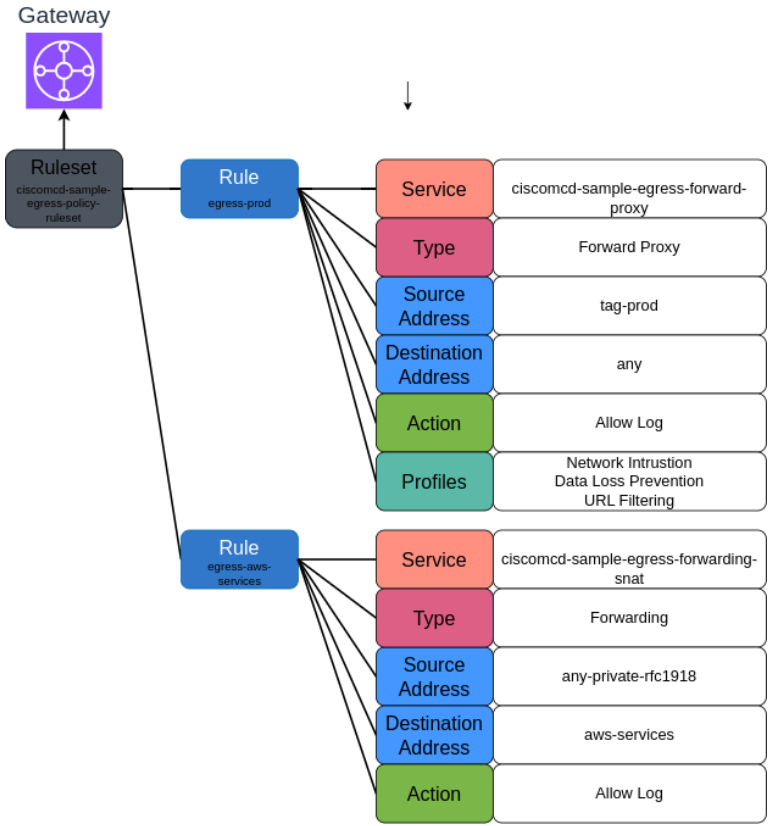


DNS Traffic – Malicious



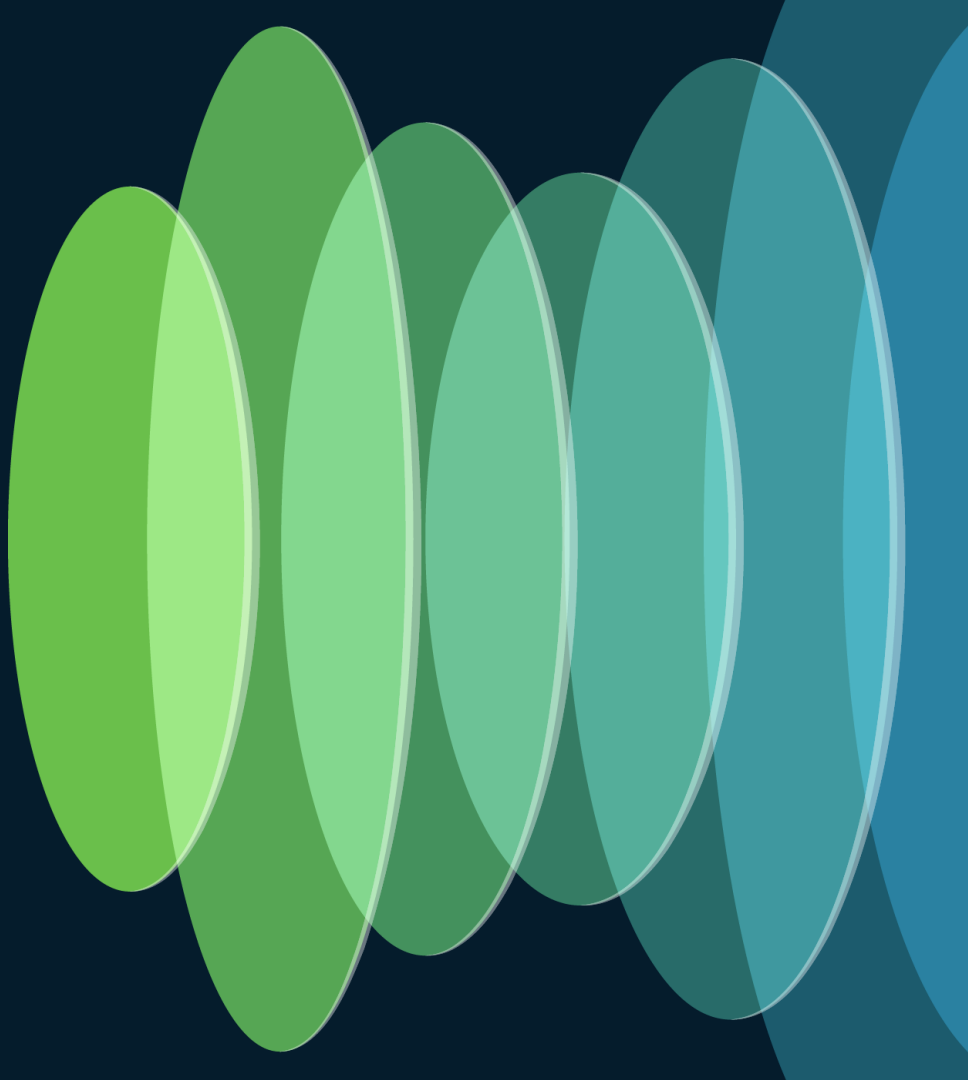
Details	Instance Info		DNS		
Date and Time	Instance Name		Resolved IP	Src IP	FQDN
2023-09-07T13:26:43.000	spoke1-z2-app	tags	67.220.242.20	10.0.3.146	ec2messages.us-east-1.amazonaws.com.
2023-09-07T13:26:41.000	spoke1-z1-app	tags		10.0.0.112	ec2messages.us-east-1.amazonaws.com.
2023-09-07T13:26:40.000	spoke1-z1-app	tags		10.0.0.112	purplehoodie.com.
2023-09-07T13:26:40.000	spoke1-z1-app	tags	64.190.63.136	10.0.0.112	purplehoodie.com.
2023-09-07T13:26:39.000	spoke1-z1-app	tags		10.0.0.112	17ebook.com.
2023-09-07T13:26:39.000	spoke1-z1-app	tags	72.14.185.43	10.0.0.112	17ebook.com.
2023-09-07T13:26:37.000	spoke1-z1-app	tags		10.0.0.112	mspy.com.
2023-09-07T13:26:37.000	spoke1-z1-app	tags	93.184.216.34	10.0.0.112	www.example.com.

Cisco Multicloud Defense - Policies



```
$ curl https://www.example.com -kw "HTTP Status: %{http_code}\n" -d "999-05-1120 999-05-1121" -o /dev/nu
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   450  100   427  100    23   5673    305 --:--:-- --:--:-- --:--:--  6000
HTTP Status: 503
$ curl -kw "HTTP Status: %{http_code}\n" https://github.com/CiscoDevNet/mcd-aws-terraform-workshop -o /d
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  278k    0  278k    0     0   537k      0 --:--:-- --:--:-- --:--:--  537k
HTTP Status: 200
$ curl -kw "HTTP Status: %{http_code}\n" https://github.com/BadActor/mcd-aws-terraform-workshop
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
        <head>
                <title>Access is restricted</title>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />   <head>

        <body>

                <div class="content">

                        <pre>
                                The URL being accessed has been blocked for security reasons
                        </pre>
                </div>
        </body>
</html>
HTTP Status: 503
$
```

Going Further



Going Further

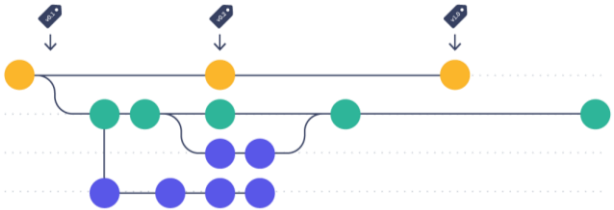
- **Put the “Multi”- in Multi-Cloud**

  Provider-specific Terraform will need to be modified, the MCD configs should remain common for all

- **Staged Git Workflow and Environments**

  Branch / pull requests / Merge

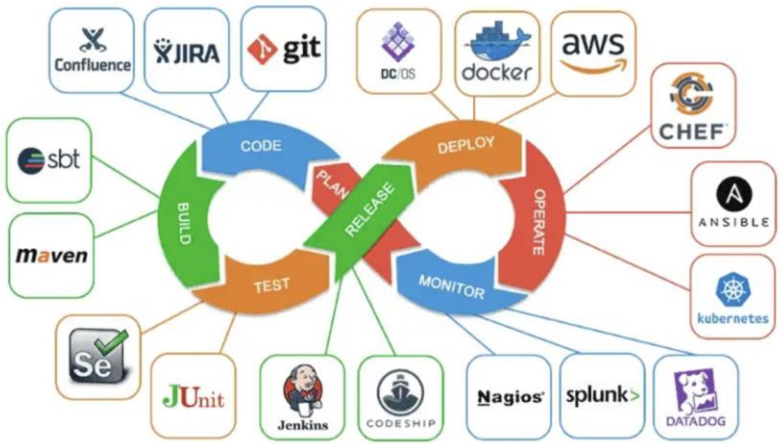
  Dev -> QA -> UAT -> Production

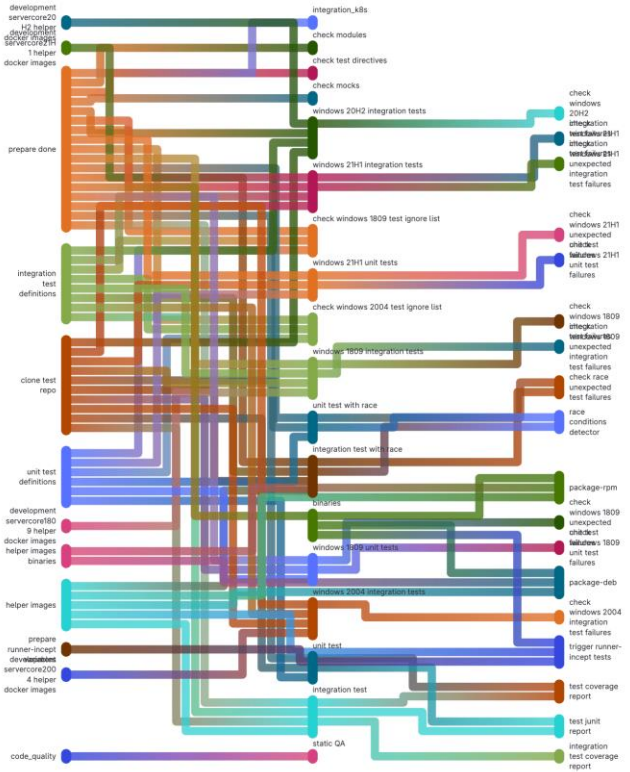


Going Further

- **Expanded CI / CD Pipeline**

  Automate more: testing / app deployment





Going Further – Learning Resources

- Cisco Solutions: What is Infrastructure as Code?
- Learning Labs:

  Cisco Multicloud Defense – Introduction

  Cisco Multicloud Defense – Terraform

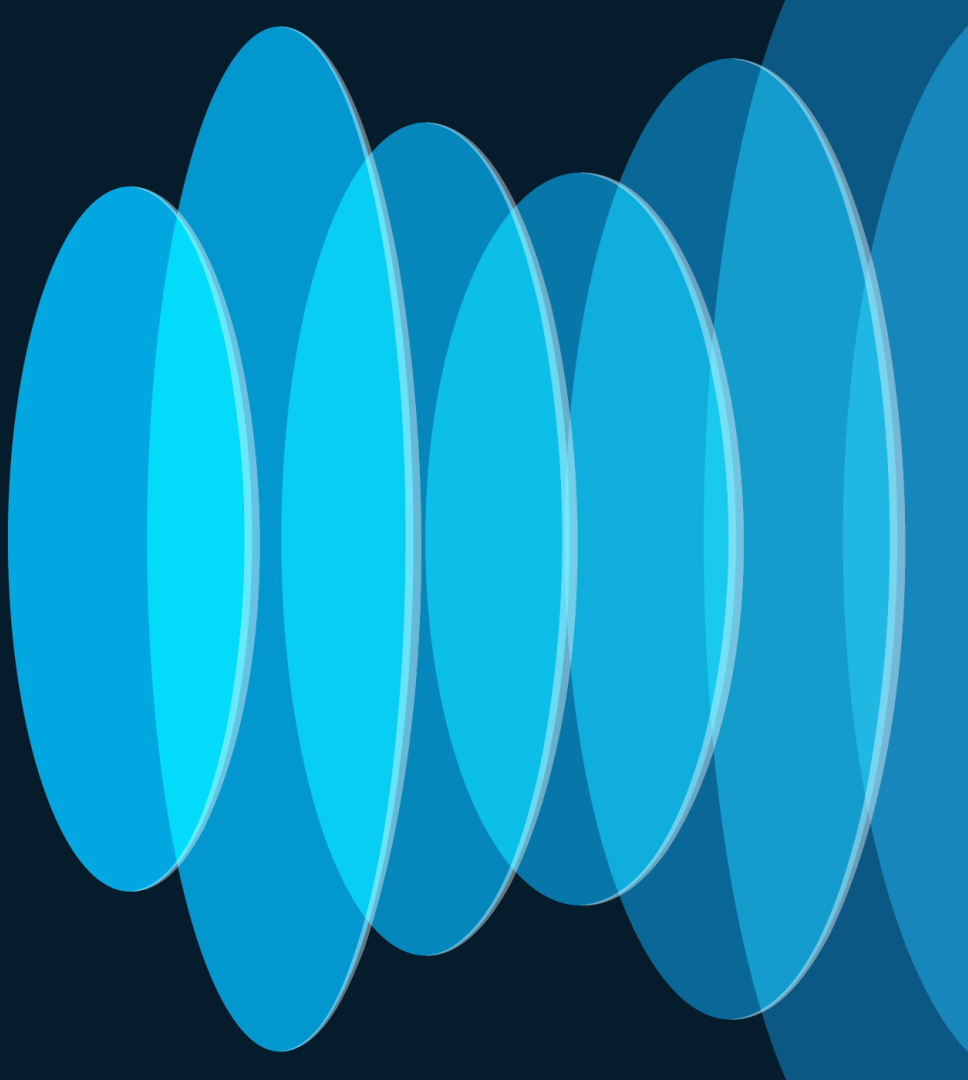
  Infrastructure-as-Code Labs

  Terraform Labs

  DevOps Labs

  CI / CD Labs

Q & A



Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

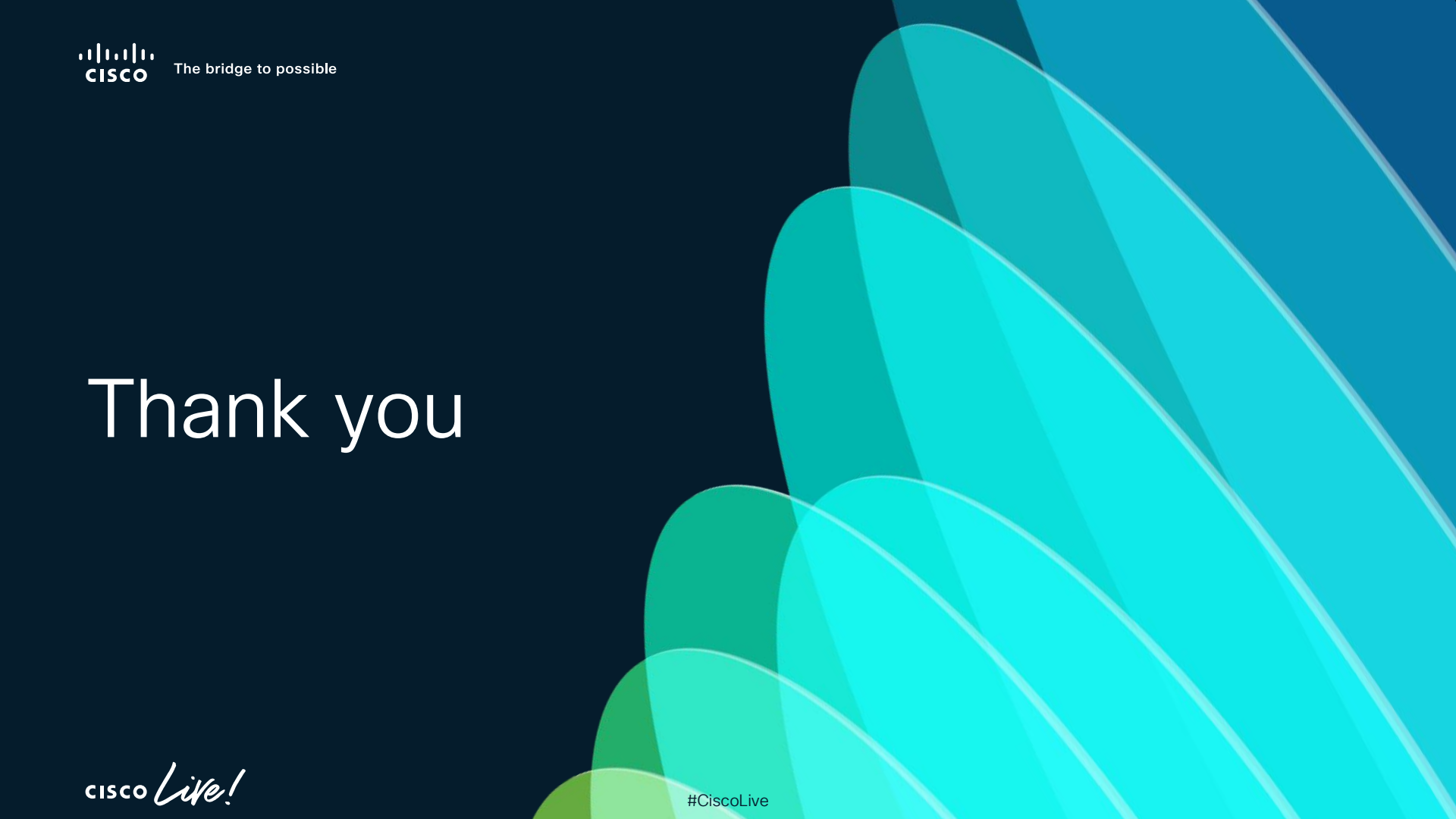
Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

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

Contact me at: **dstaudt@cisco.com**


The bridge to possible
Thank you
cisco Live!
#CiscoLive