

CISCO *Live!*



#CiscoLive



The bridge to possible

Decoding Kubernetes Networking and Policy as Code

Using Cisco Secure Workload

Amandeep Singh, Technical Marketing Engineer
BRKSEC-2250



#CiscoLive

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-2250>



Agenda

- Introduction – Firewall is a function
- Anatomy of Iptables
- Decoding Kubernetes Networking
 - User to Pod
 - Pod to Pod
- Network Policy
 - CNI
 - Service Mesh
 - Secure Workload
- Secure Workload– Policy as code
 - Orchestration and Policy

Firewall is a function!

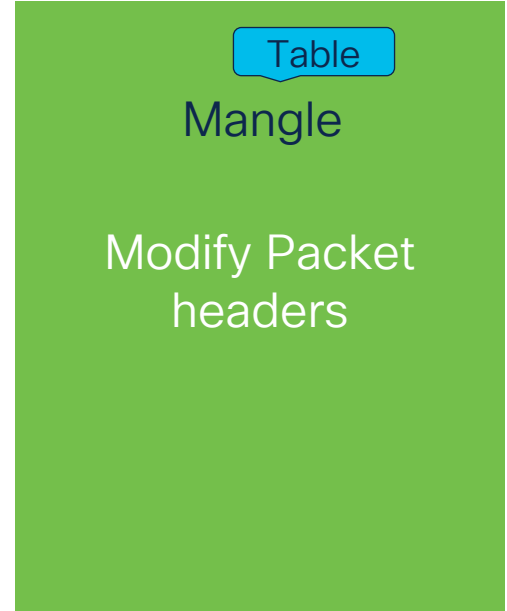
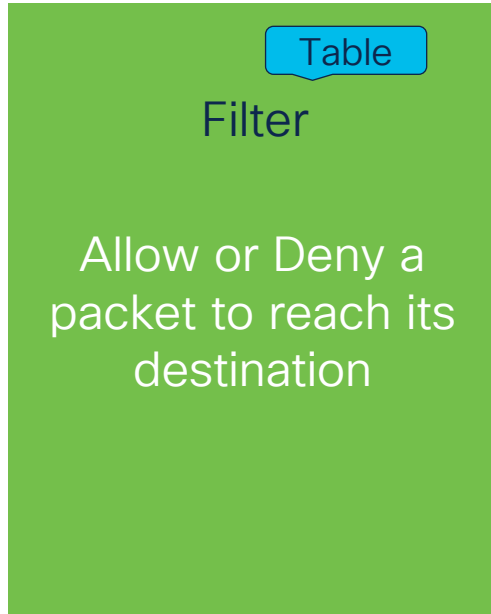
- Firewall is not a device, it's a function.
- Evolution of Firewalls
 - Function- Access lists to Next-Generation...
 - Attack surface- OnPrem to Public cloud to Hybrid & Multi-cloud
 - Enforcement points- Networks(ADCs, Network firewalls and more) to Hosts
- Host based firewalling- Iptables and netfilter
 - Introduced in Linux Kernel 2.4
 - Successor- nftables



Anatomy of Iptables

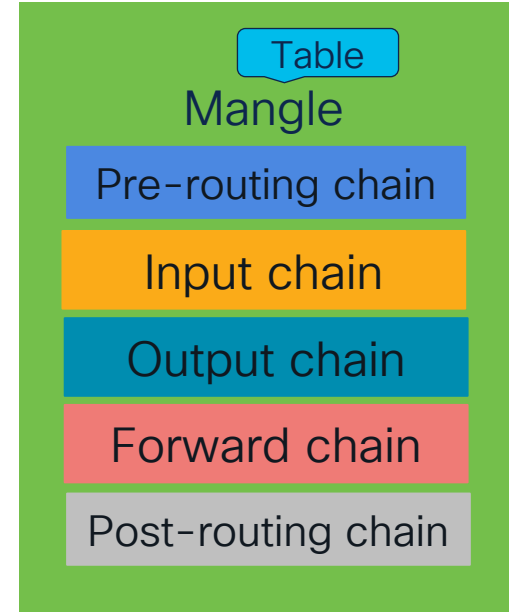
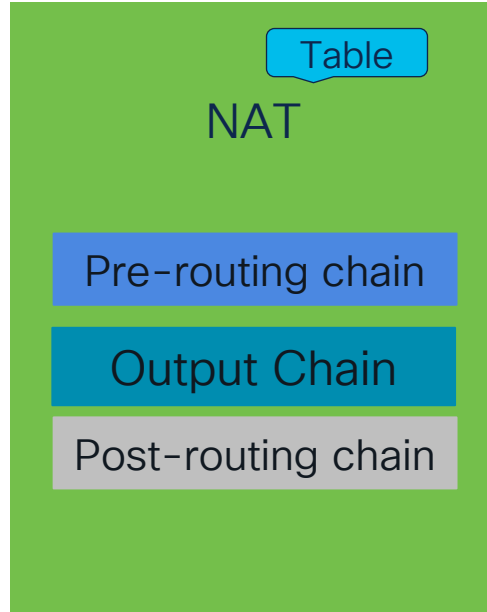
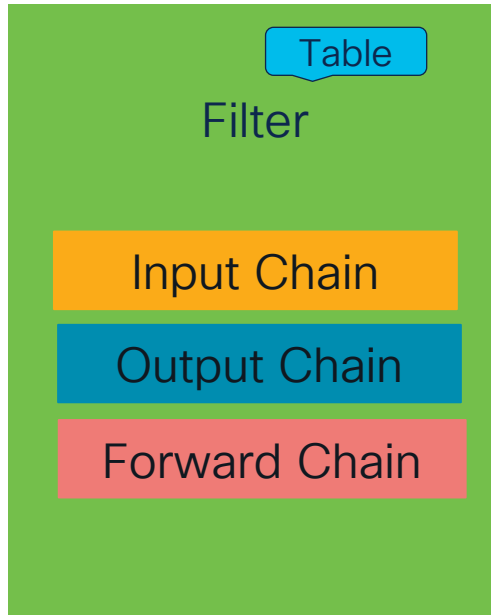
Linux Iptables - Structure

Tables - Packet Processing system



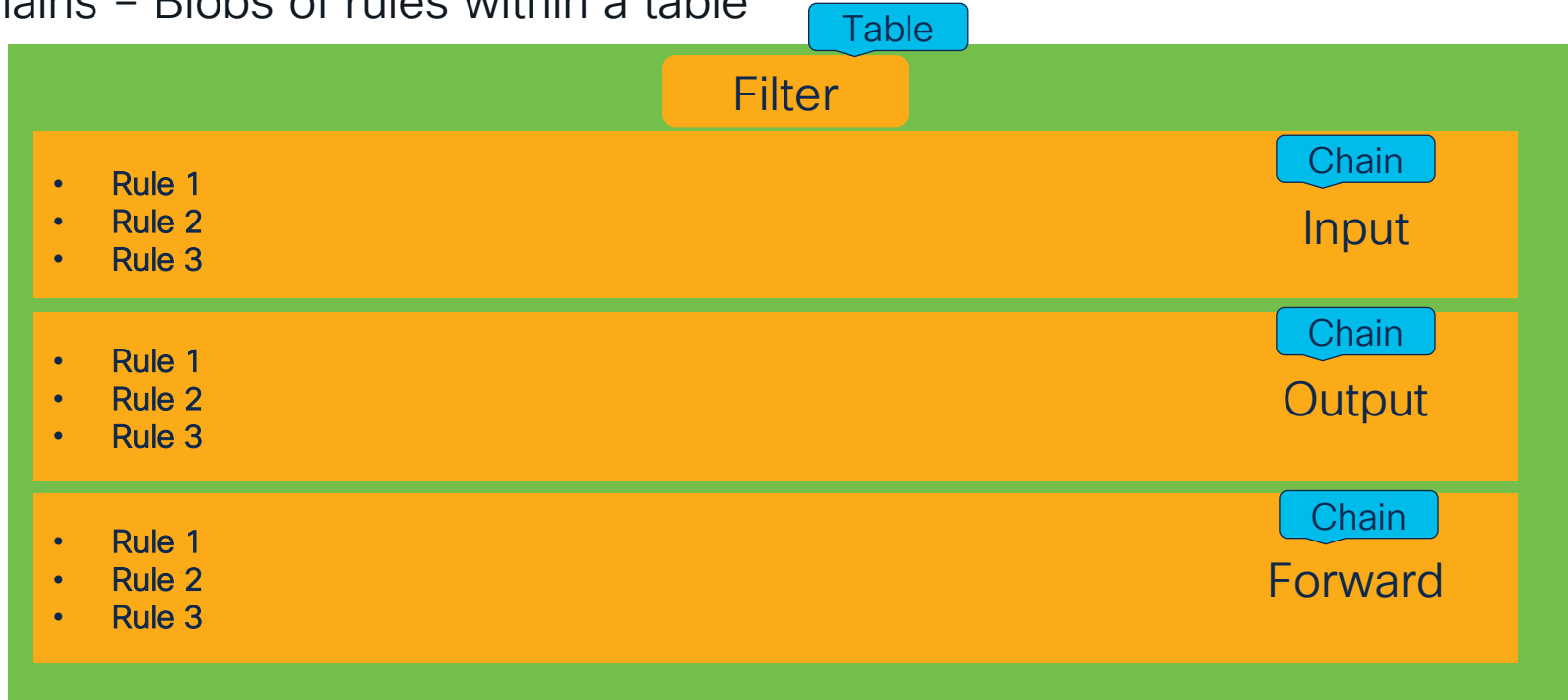
Linux Iptables - Structure

Chains – Blobs of rules within a table



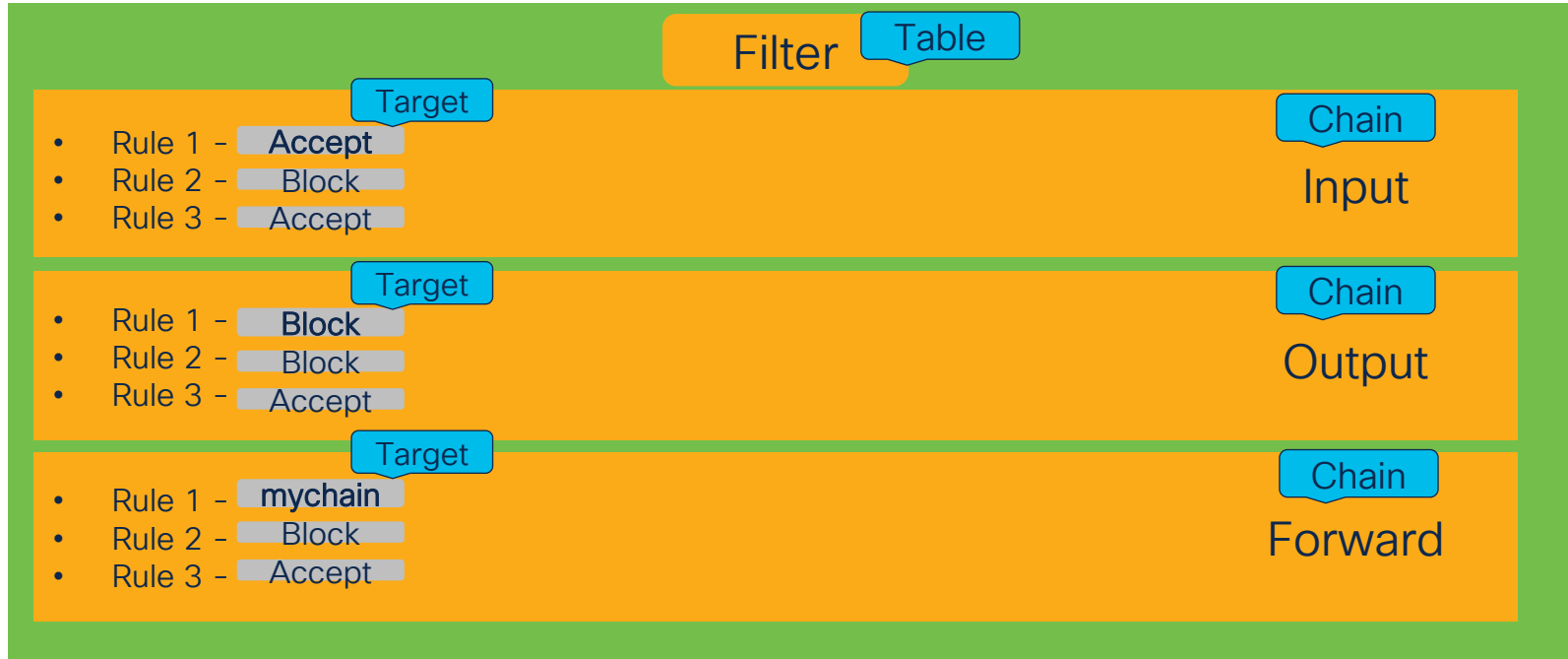
Linux Iptables - Structure

Chains – Blobs of rules within a table

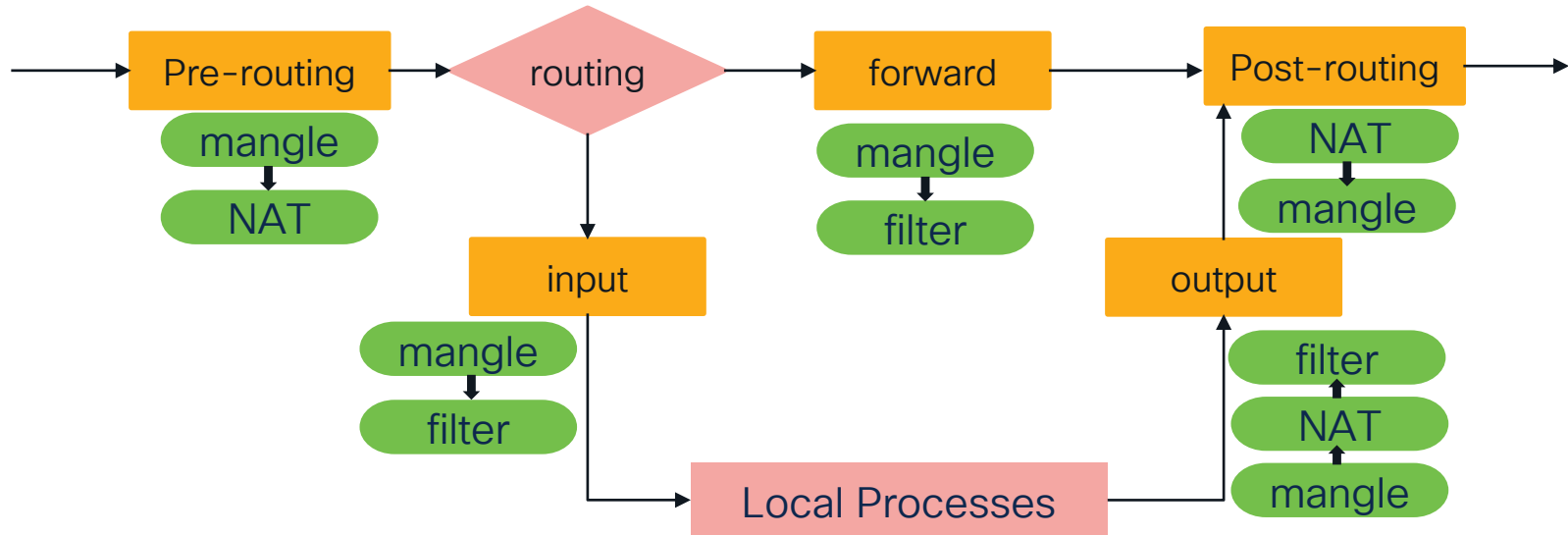


Linux Iptables - Structure

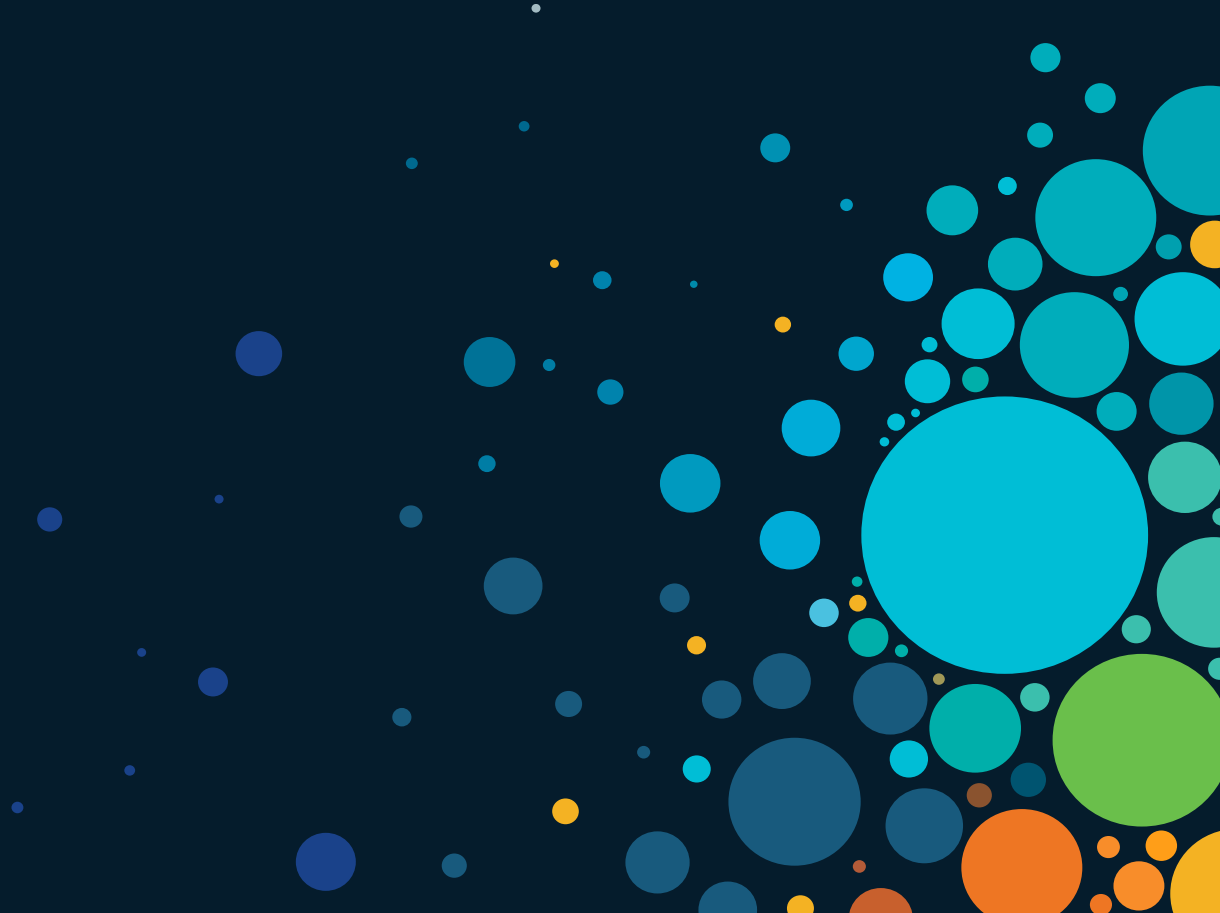
Targets – Action taken when a packet matches a rule.



Iptables packet processing



Decoding Kubernetes Networking



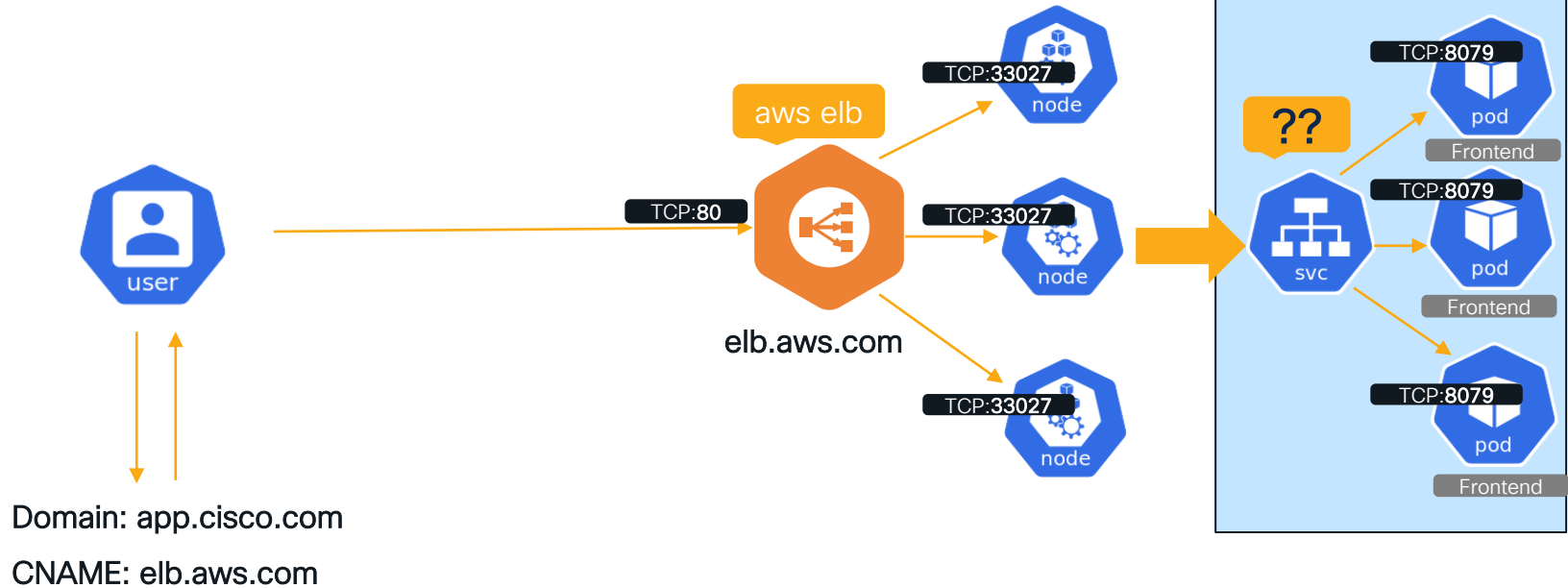
Decoding Kubernetes networking

User to pod



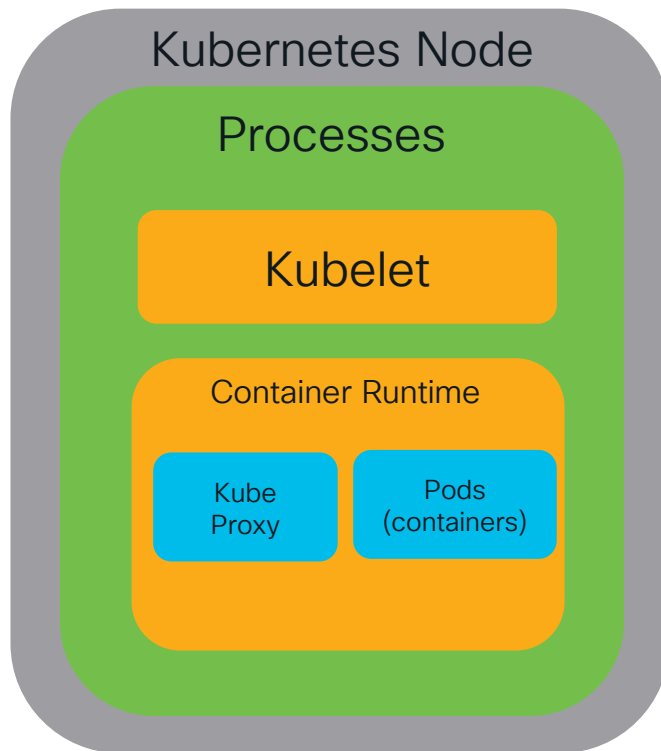
Decoding Kubernetes networking

User to pod



Decoding Kubernetes networking

User to pod



Decoding Kubernetes networking

User to pod

Source: User-IP
Destination: Node-IP:Port

Iptables - NAT

Chain:
KUBE-SERVICES

Chain:
KUBE-
NODEPORTS

Chain:
KUBE-SVC-
NNLTN4FUSGD4
44WY

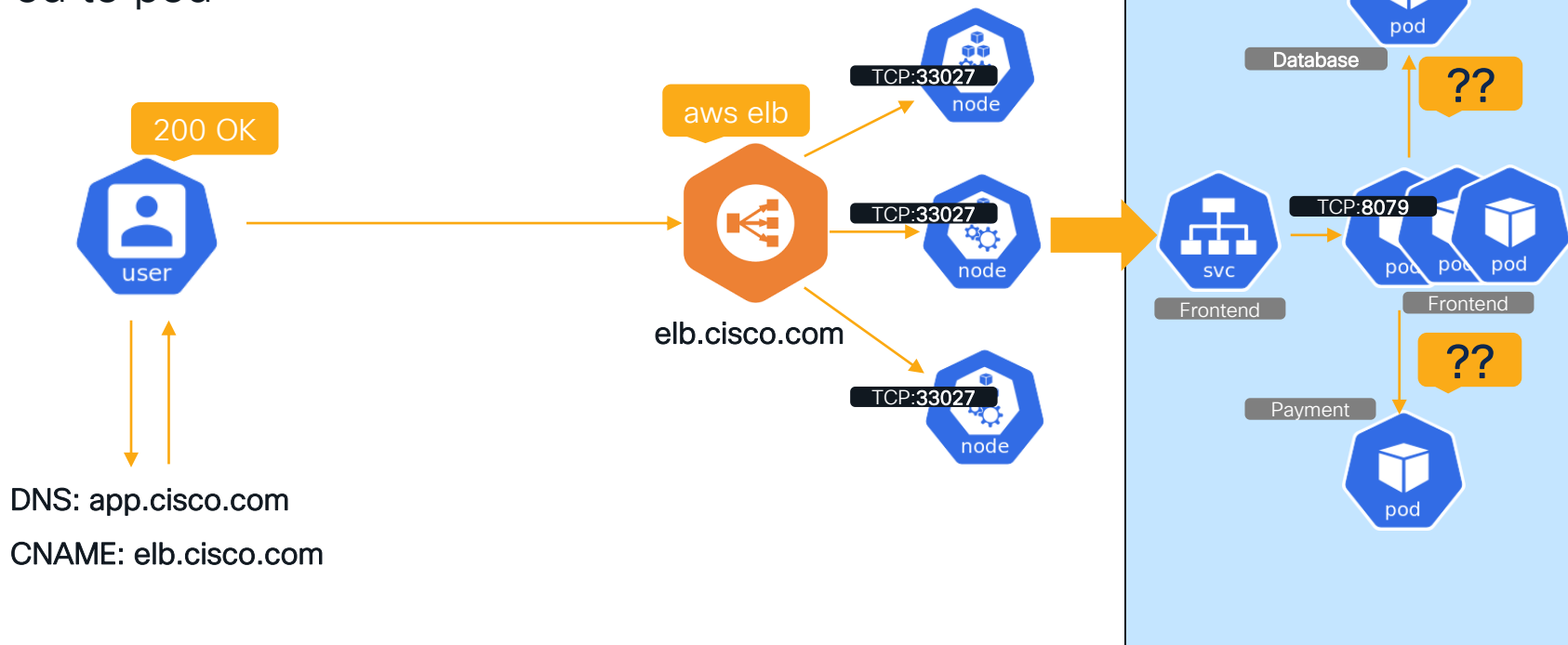
Chain:
KUBE-SEP-
N7UHNZZZNGSEB
2MW

Chain KUBE-SEP-N7UHNZZZNGSEB2MW (1 references)

target	prot	opt	source	destination
KUBE-MARK-MASQ	all	--	ip-10-20-20-222.ec2.internal	anywhere /* sock-shop/front-end */
DNAT	tcp	--	anywhere	anywhere /* sock-shop/front-end */ tcp to:10.20.20.222:8079

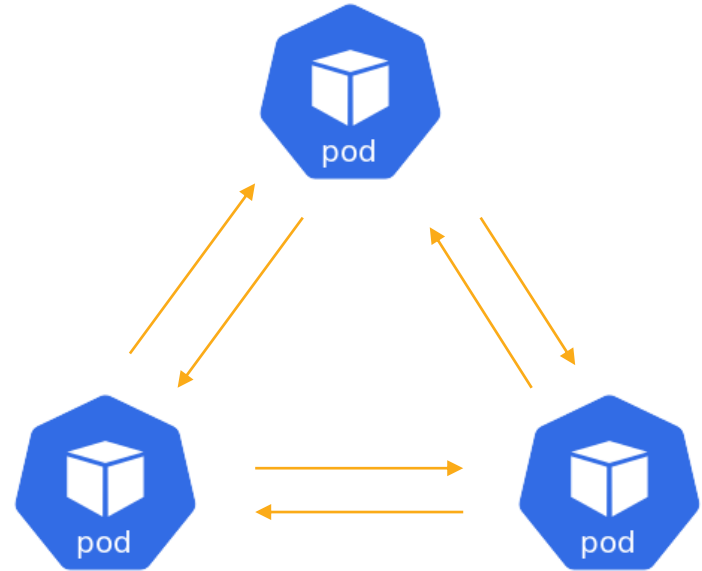
Decoding Kubernetes networking

Pod to pod



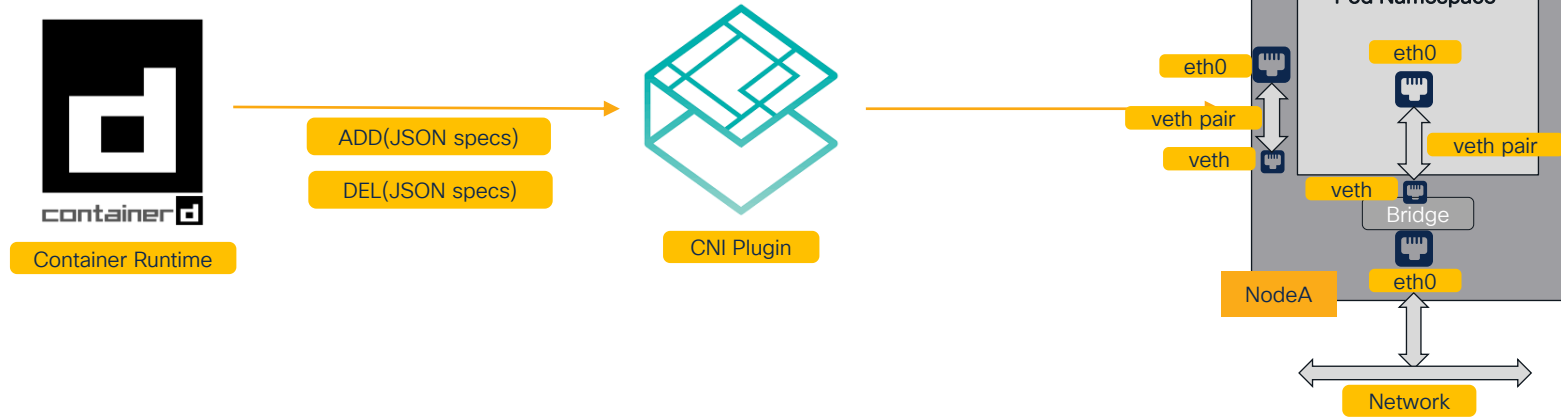
K8s networking model – Basic requirements

- Every pod gets its own IP address and containers within a pod share the pod IP
- Pods can communicate with all other pods in the cluster without NAT
- Isolation is defined using network policies



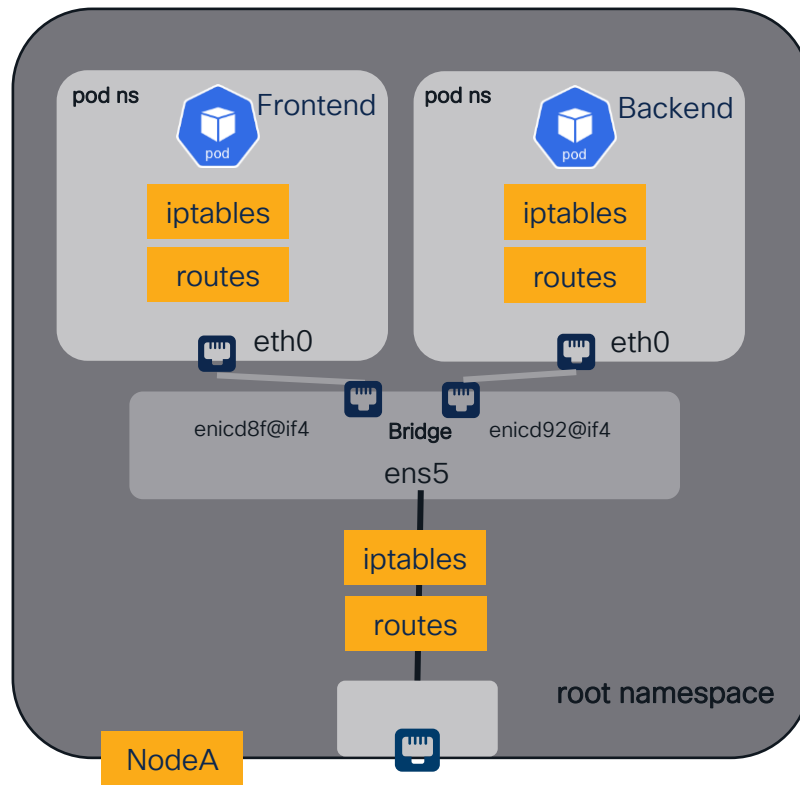
Decoding Kubernetes networking

Pod to Pod – CNI Plugin



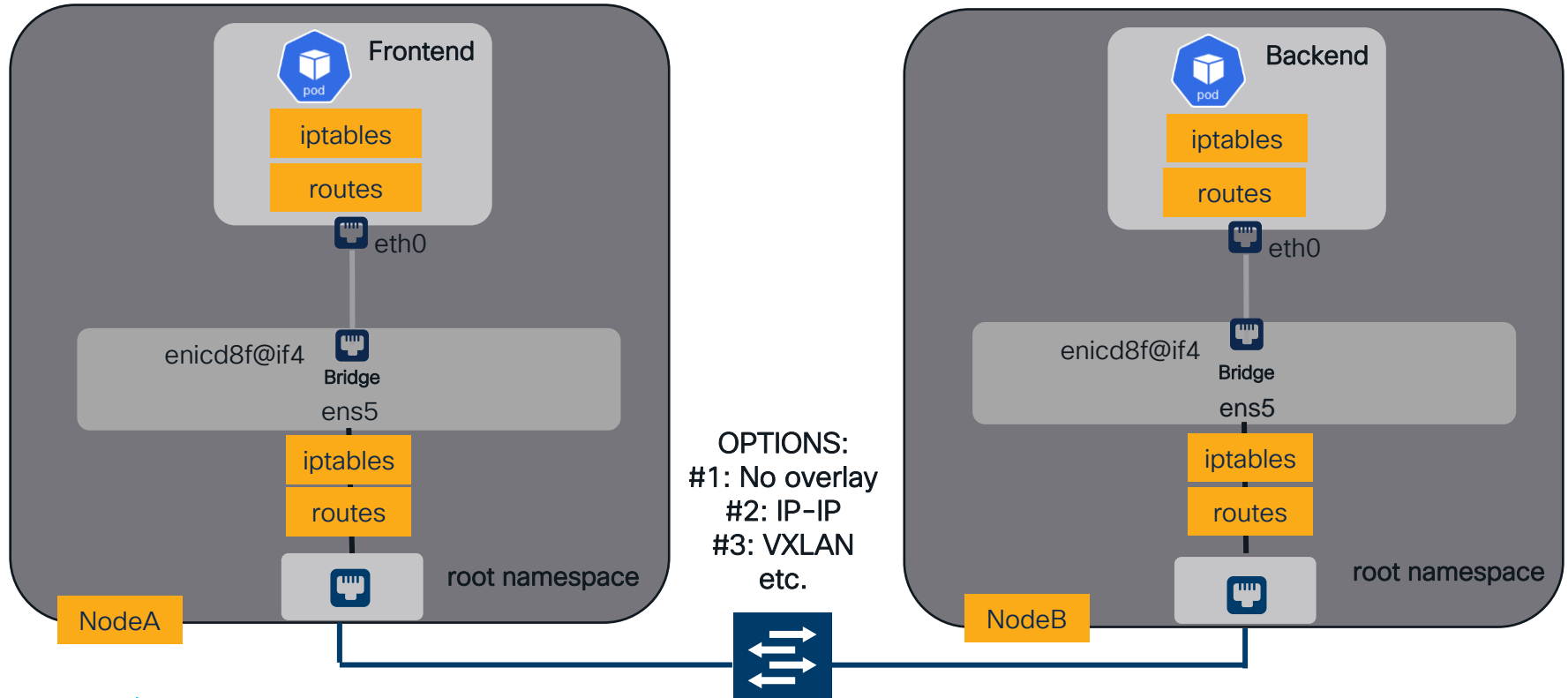
Decoding Kubernetes networking

Pod to Pod networking – Intra node



Decoding Kubernetes networking

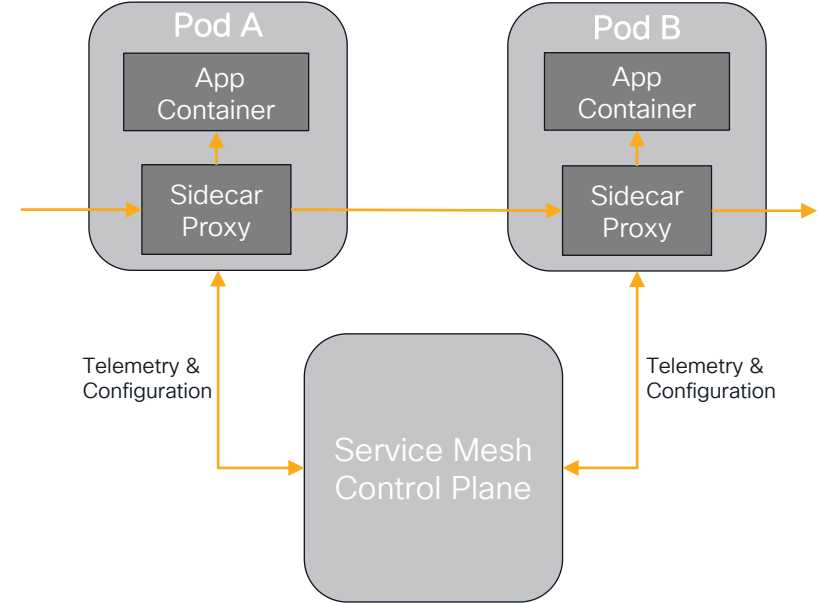
Pod to Pod networking – Inter node



Network policy

Service Mesh

- A service mesh is a dedicated infrastructure layer that you can add to your applications.
- Allows you to transparently add capabilities like:
 - Observability
 - Traffic management
 - **Security**



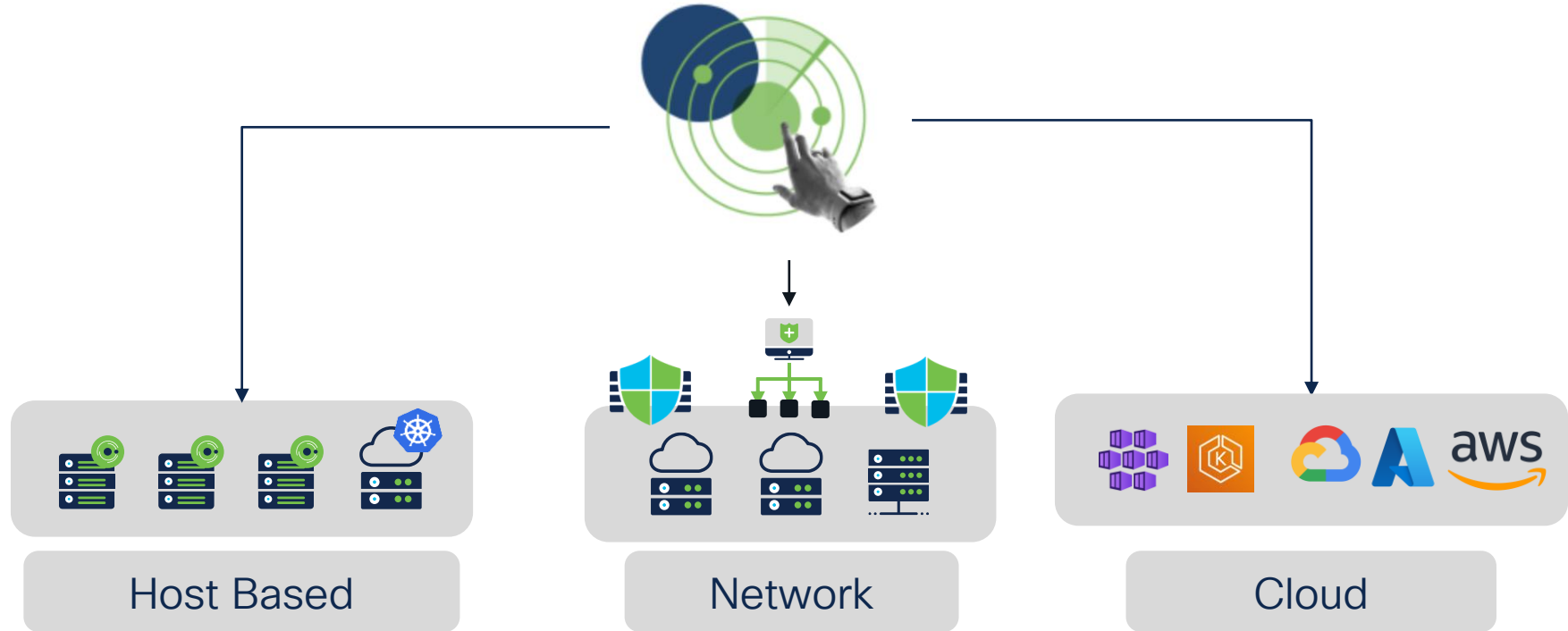
Network policy

Enforcement points:

- Iptables – kernel level
 - Enforced on the node
 - L3-L4 aware
 - CNI Plugins
- Sidecar – User space
 - Enforced on the pod (via sidecar proxy)
 - HTTP aware
 - Service Mesh –example – Istio

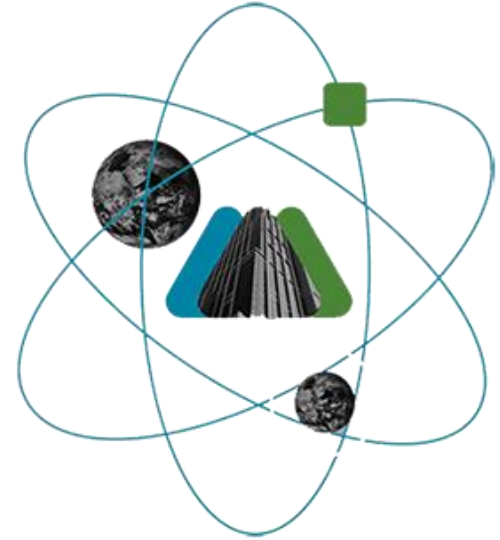


Secure Workload - Overview



Secure Workload – Kubernetes

- Orchestration – EKS, AKS, GKE, Unmanaged K8s, OpenShift
- Supported Node OS – Ubuntu, RHEL, RHCOS and more...
- Workload Visibility to policy discovery and enforcement
- Enforcement – Iptables and IpSets



Secure Workload – Policy as Code

Flow ingestion: Agent installation



How it Works

Download
Select a platform and click 'Download'

Which platform is your agent going to be installed on?

Does your network require HTTP Proxy to reach Tetration?

Linux Windows AIX
Kubernetes

Yes No



Installation precheck

Dependencies for installer script

Run installer script with -precheck as user:

```
$ bash tetration_daemonset_installer.sh --pre-check
```

The usage of this installer script is as follows:

```
$ bash tetration_daemonset_installer.sh
```

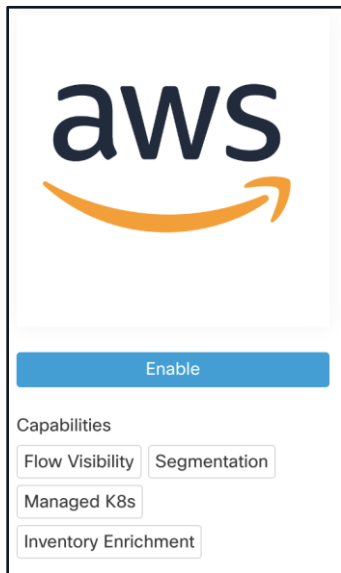


```
secureworkload-demo-pod1:~/environment $ kubectl get pods -n tetration
NAME                READY   STATUS    RESTARTS   AGE
tetration-agent-94chq 1/1     Running   0           8h
tetration-agent-fgv6h 1/1     Running   0           8h
tetration-agent-j8qg4 1/1     Running   0           8h
secureworkload-demo-pod1:~/environment $
```

Context ingestion: Cloud connector



How it Works



Enable and select capabilities

- Gather Labels from AWS cloud
- Gather metadata from EKS

Name of the connector

SecureAWSConnector

Select Activities to be performed with Cisco Secure Workload on your AWS Resources

☒ Gather Labels ⓘ ☐ Ingest Flow Logs ⓘ ☐ Segmentation ⓘ ☒ Managed kubernetes services ⓘ

The recommended AWS (IAM) roles and permissions depend on the selections you make above.

Context ingestion: Cloud connector



- CloudFormation template to create an IAM Policy on AWS with least privilege.
- Attach the policy to an AWS IAM user.
- AWS API Keys from the IAM user – Read only permissions

✓ Activities

2 Roles and Settings

3 Select VPC

Cisco Secure Workload requires relevant permissions to access and read flow logs settings and perform policy enforcement.

Based on the capability selections, the following CloudFormation template has been auto-generated. Use this to apply the relevant permissions to the desired user:

```
{
  "Resources": {
    "ManagedPolicy": {
      "Type": "AWS::IAM::Policy",
      "Properties": {
        "PolicyName": {
          "Ref": "PolicyName"
        },
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                "ec2:DescribeVpcs"
              ]
            }
          ]
        }
      }
    }
  }
}
```

Additional Help

[> Create a Cloud Formation Stack](#)

[> Create a New User](#)

[> Example Commands](#)

Access Key

.....

Secret Key

.....

Context ingestion: Cloud connector

4



How it Works

- Select the VPCs with EKS clusters to onboard
- Add an IAM role to access EKS with read-only privileges.

<input checked="" type="checkbox"/>	▼ app-first-sec-11-Spoke-VPC	us-east-1	<input checked="" type="checkbox"/>
Select kubernetes clusters:			
<input checked="" type="checkbox"/>	app-first-sec	orkloadEKSAAssumeRole	

✓ Connector configured successfully!

Policy as code – Inventory filters

Ansible Playbooks – Filters

```
- name: Add front-end filter
  tetration_inventory_filter:
    provider:
      server_endpoint: "{{ secureworkload_url }}"
      api_key: "{{ api_key }}"
      api_secret: "{{ api_secret }}"
      app_scope_id: "{{ scope_id }}"
    state: present
    name: front-end
    query:
      filters:
        - field: user_orchestrator_name
          type: eq K8s metadata
          value: webfront
        - field: user_orchestrator_system/namespace
          type: eq K8s metadata
          value: ciscolive-ns
      type: and
```


Policy as code – Network policy

Ansible Playbooks – Policy

```
- name: Add Policy front-end to orders-svc
  tetration_application_policy:
    provider:
      server_endpoint: "{{secureworkload_url}}"
      api_key: "{{ api_key }}"
      api_secret: "{{ api_secret }}"
    app_scope_id: "{{scope_id }}"
    provider_filter_name: orders-svc Destination
    consumer_filter_name: front-end Source
    version: v0
    rank: DEFAULT Action
    policy_action: ALLOW
    priority: 100
    state: present
    register: front_end_orders_svc_policy
```

```
- name: Add Ports to Policy front-end to orders-svc
  tetration_application_policy_ports:
    provider:
      server_endpoint: "{{secureworkload_url}}"
      api_key: "{{ api_key }}"
      api_secret: "{{ api_secret }}"
    app_scope_id: "{{scope_id }}"
    policy_id: "{{ front_end_orders_svc_policy.object.id }}"
    version: v0 Protocol
    proto_name: TCP
    start_port: "{{ port }}"
    end_port: "{{ port }}"
    state: present
    loop: Port Number
    - 80
    loop_control:
      loop_var: port
      label: "Adding port {{ port }} to Sock Shop Policy"
```

Demo - Policy as Code

bash - "ip-10-10-10-217" x

📄 x

```
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $  
app-first-sec-11:~/environment $
```

I

Cisco Secure Workload - References

- Policy as code
 - [Secure Workload - Terraform](#)
 - [Secure Workload - Ansible](#)
- Cisco Validated Design
 - [Securing Cloud Native Applications in AWS](#)
 - [Securing Cloud Native Applications in Azure](#)
- Cisco Developer Network - Labs
 - [Securing Cloud Native Applications](#)
 - [Secure Workload - OpenAPI](#)

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.



Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN
Posture
Telemetry
Threat
Query



ThousandEyes (Visibility)

Device Mgmt



Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

ZERO TRUST

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible



SDWAN



On-Premises

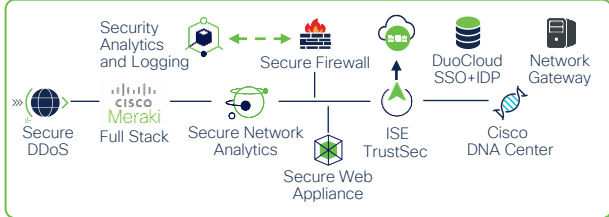
SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



App Observability | Detection | Response



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

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

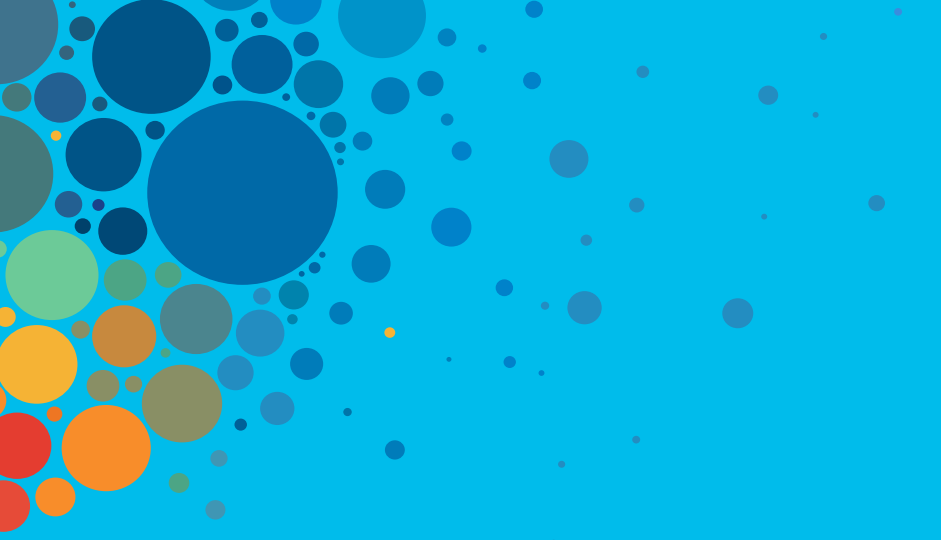
Cisco Guided Study Groups

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive