cisco Live!

Let's go

The bridge to possible

Defense in Depth Security for Multicloud Data Centers

Brenden Buresh
Distinguished Solutions Architect

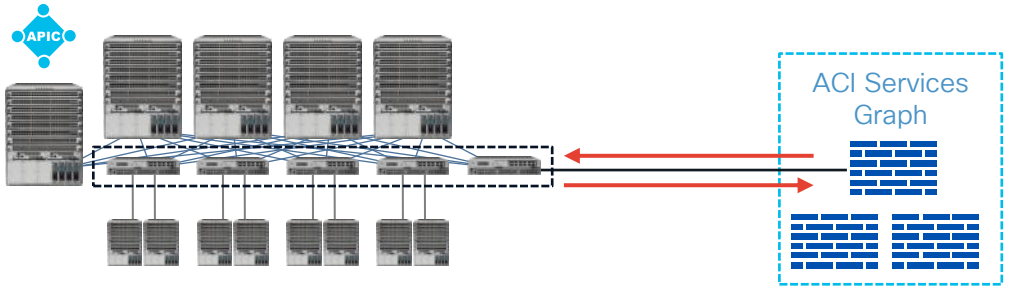
Agenda

- Introduction to ACI Fabric Fundamentals
- ACI Fabric Policy Operation and Deployment
- ACI Fabric Micro Segmentation Capabilities
- Leveraging End Point Security Groups (ESG)
- ACI Fabric L4-L7 Services Automation
- Cloud Network Controller – Public Cloud Connectivity
- Introduction to Secure Workload Platform
- Secure Workload Application Dependency Mapping
- Secure Workload Segmentation and Policy Enforcement
- Conclusion: Comprehensive Security Architecture

Introduction to ACI Fabric Fundamentals

ACI Fabric Security

Automated Security with Built in Multi Tenancy



- APIC Hardening - Cent OS 7.2
- Distributed Stateless Firewall
- Line Rate Security Enforcement
- Open: Integrate Any Security Device
- PCI, FIPS, CC, UC-APL, USG-v6

Symantec SOURCEfire Check Point SOFTWARE TECHNOLOGIES LTD. radware Smart Network. Smart Business. cisco paloalto NETWORKS intel Security FORTINET

Embedded Security

- White-list Firewall Policy Model
- RBAC rules
- Hardened CentOS 7.2
- Authenticated Northbound API (X.509)
- Encrypted Intra-VLAN (TLS 1.2)
- Secure Key-store for Image Verification

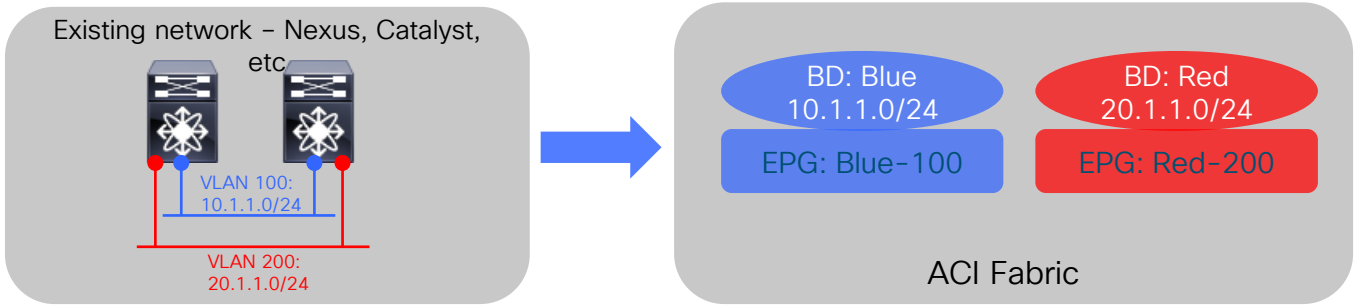
Micro-Segmentation

- Hypervisor Agnostic (ESX, Hyper-V, KVM*)
- Physical, Virtual Machine, Container
- Attribute Based Isolation/Quarantine
- Point and Click Micro-segmentation
- TrustSec-ACI Integration

Security Automation

- Dynamic Service Insertion and Chaining
- Closed Loop Feedback for Remediation
- Centralized Security Provisioning & Visibility
- Security Policy Follows Workloads

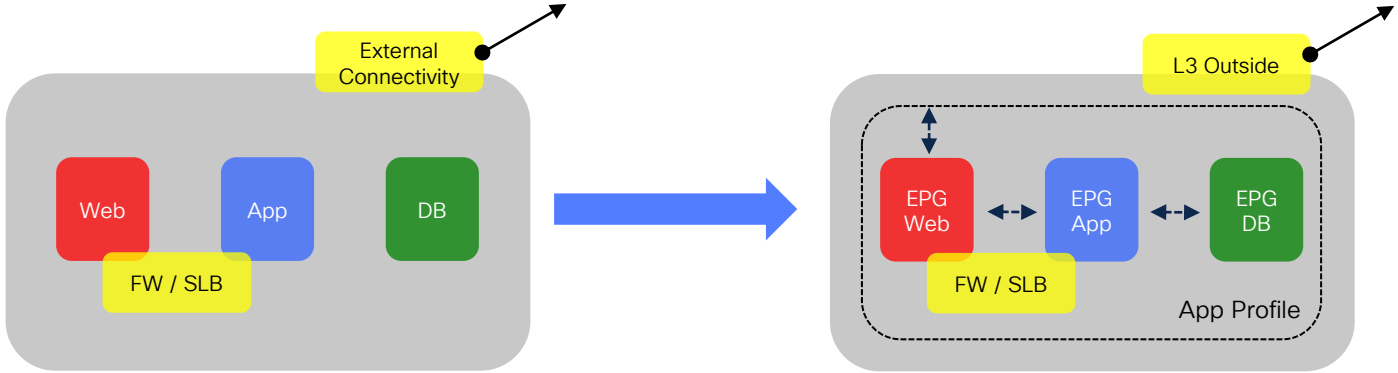
ACI Fabric – Two Deployment Models



Network Centric Mode

Leverage well known networking constructs.

VLANs, IP addresses, Subnets, Flood Domains etc.



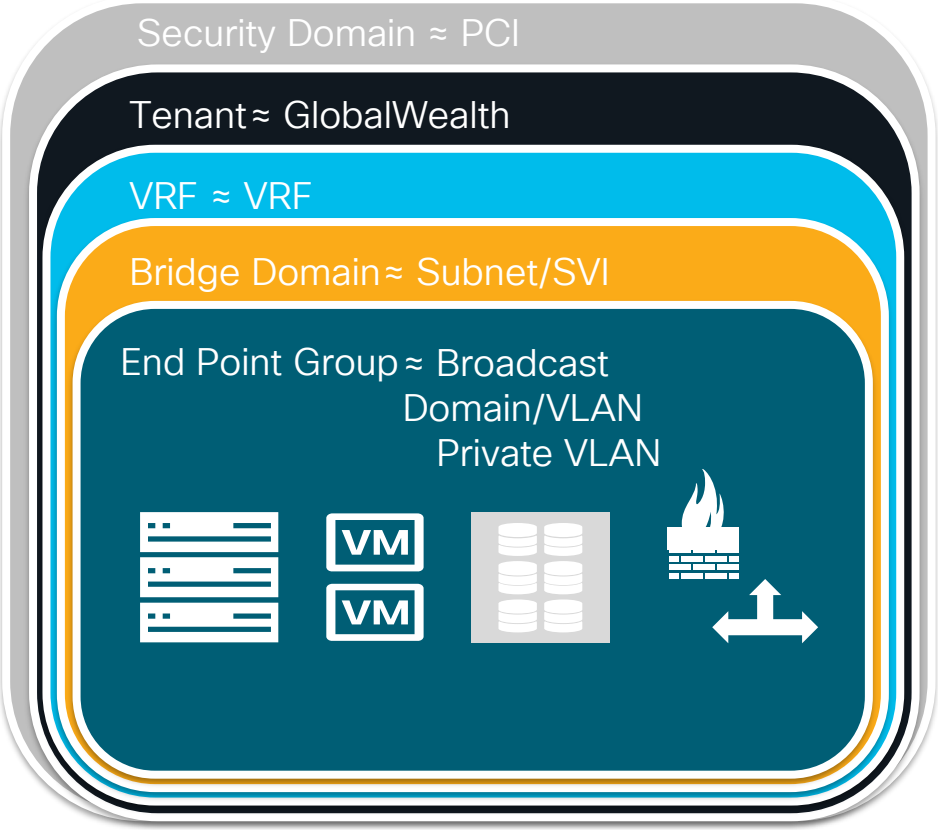
Application Centric Mode

Leverage well known application constructs.

Application profiles, dependency mapping etc.

You can mix both network centric and application centric -> typical customer transition path!

The ACI Policy Model



Contracts ≈ Access Lists

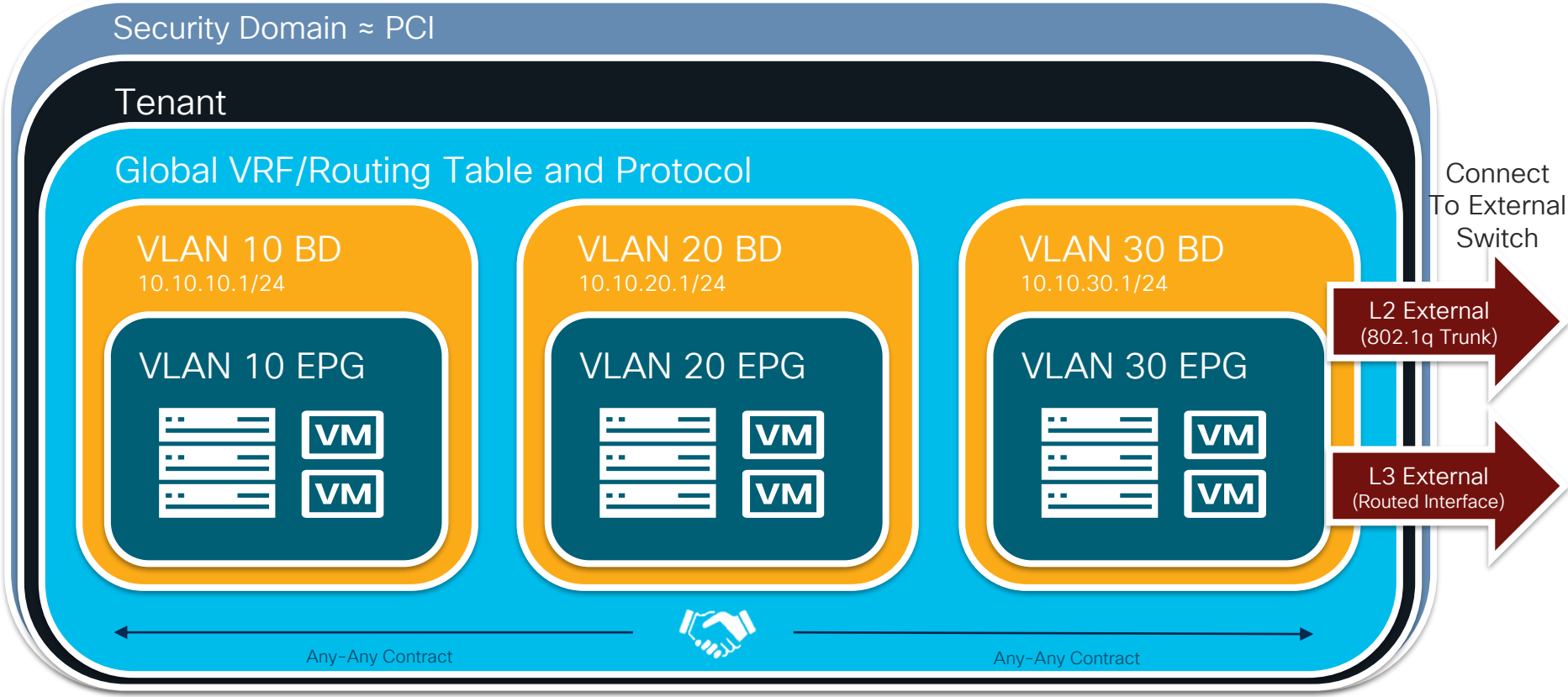
EPG1 ⟷ EPG2

Any-Any
Replicates a
Traditional Switch

L2 External EPG ≈ 802.1q Trunk

L3 External EPG ≈ L3 Routed Link

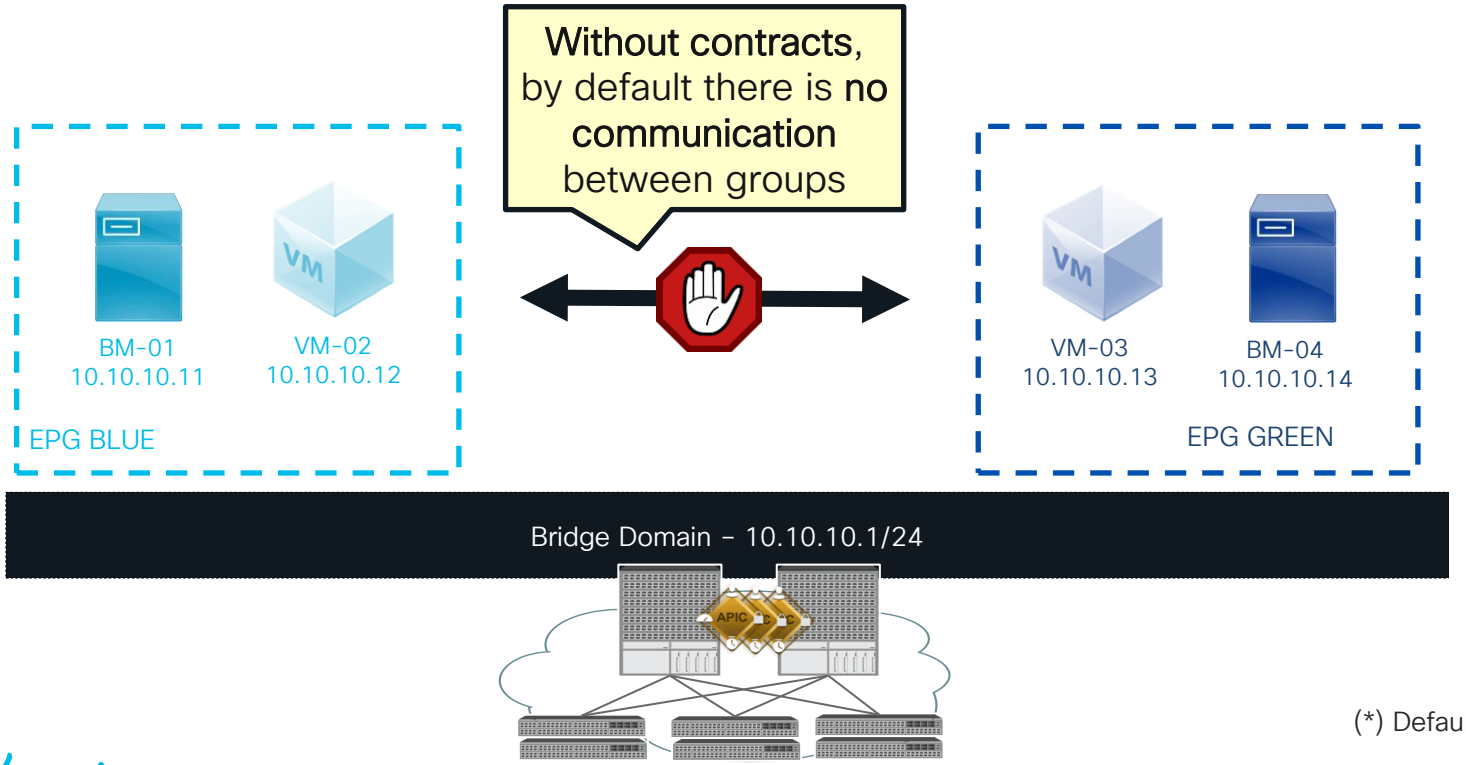
The ACI Policy Model – Network Centric Configuration



ACI Fabric Policy Operations and Deployment

Admins Define EPGs Relationship with Contracts

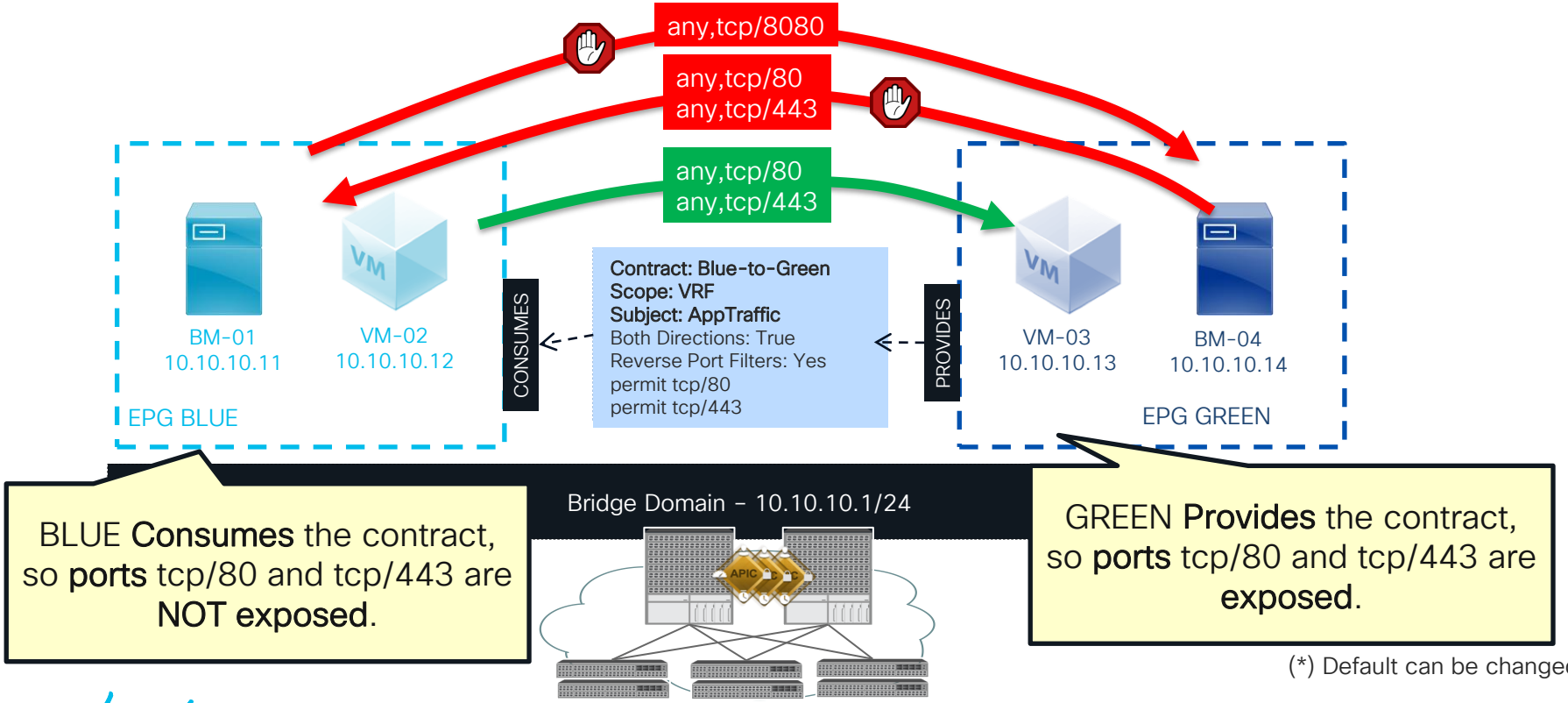
White-List Model (*): No Contract, No Communication



(*) Default can be changed

EPGs Will Have Relationships with Contracts

White-List Model (*): Contract Determines Communication



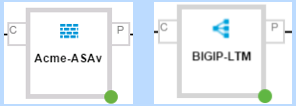
(*) Default can be changed

Contracts Also Allow Inserting Services

Next Generation Firewall, ADC, IDS/IPS, etc.

You can **insert** an NGFW, or a LB by attaching a **Service Graph** to the contract subject

Contract: Blue-to-Green
Scope: VRF
Subject: AppTraffic
Both Directions: True
Reverse Port Filters: Yes
permit tcp/80
permit tcp/443



BM-01
10.10.10.11

VM-02
10.10.10.12

EPG BLUE

CONSUMES

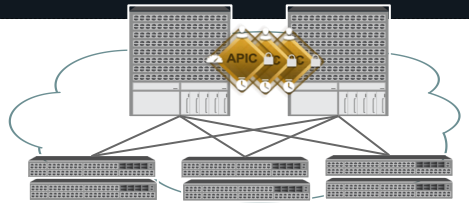
PROVIDES

VM-03
10.10.10.13

BM-04
10.10.10.14

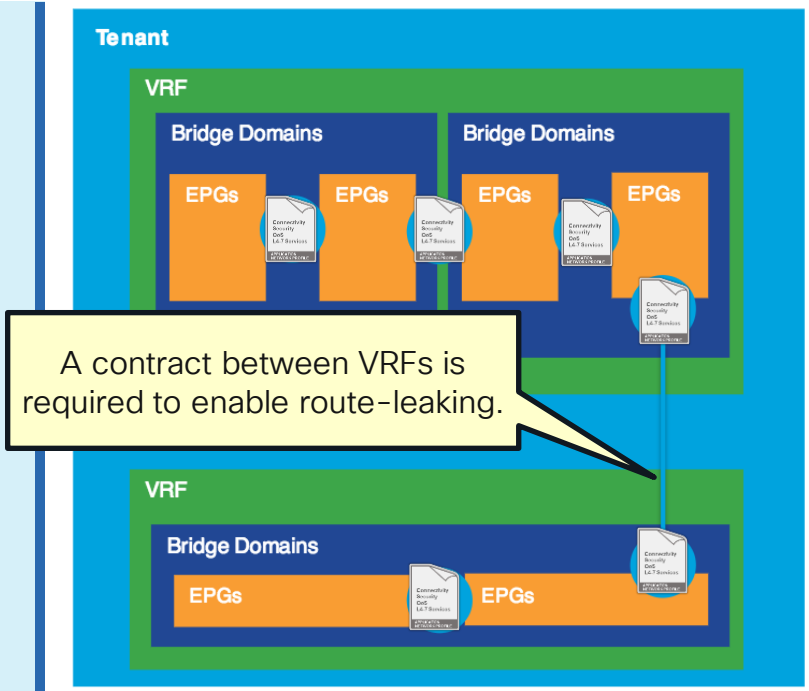
EPG GREEN

Bridge Domain – 10.10.10.1/24



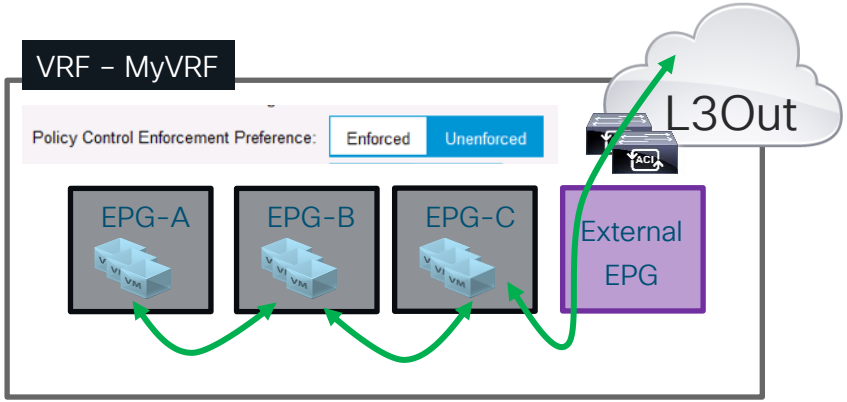
EPGs Provide and/or Consume Contracts

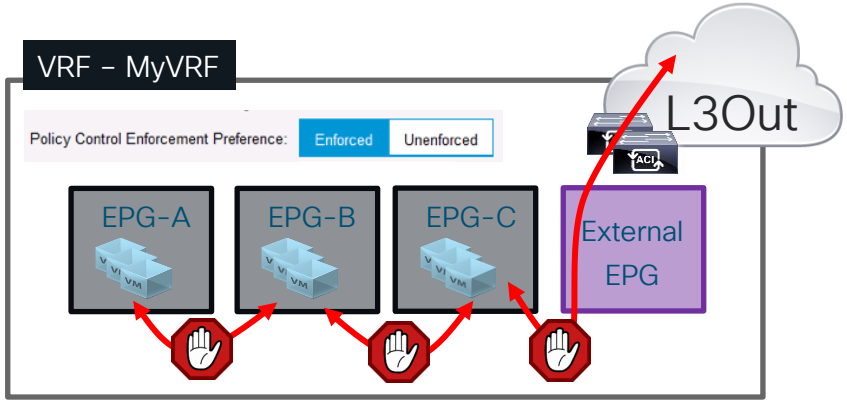
- EPGs will have associations to provide and/or to consume a contract
- An EPG can provide and/or consume multiple contracts
- Provider and consumer designations create directionality between EPG's
- Contracts can be used between EPGs in the same Application Profile, across Application Profiles, VRFs and even tenants
- Contracts also define route-leaking between VRFs



Policy Enforcement Can be Enabled/Disabled at VRF Level

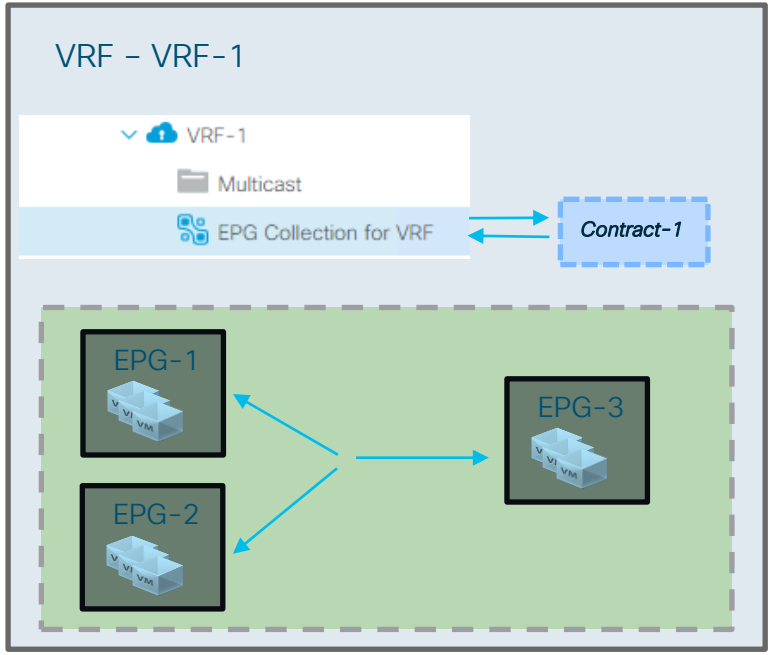
- Policy Enforce: no communication without contracts
- Policy Unenforced: all communication allowed





vzAny Can be Used to Permit all Traffic Between EPGs

- A contract defined for vzAny includes all the EPGs under the VRF and the L3Out also
- vzAny can provide and consume one contract: permit any any for instance



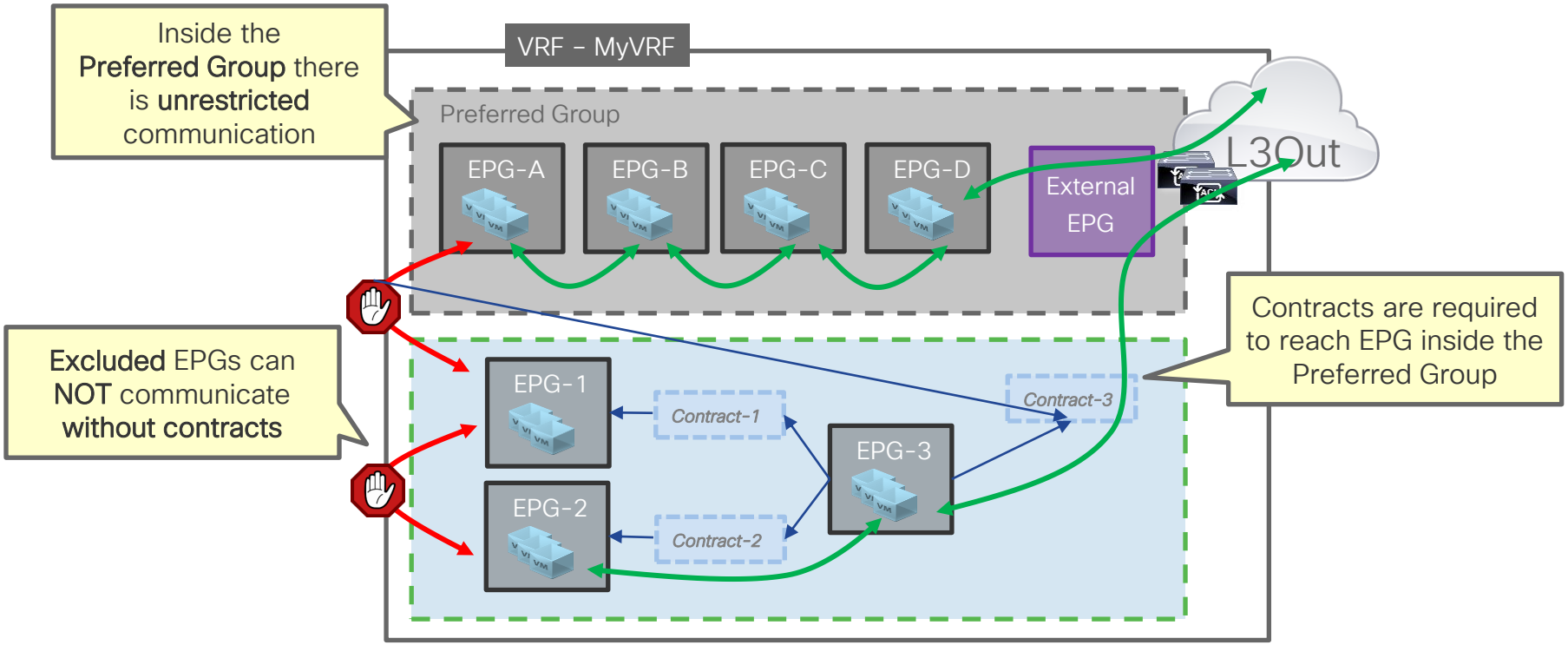
How Policy-cam is programmed

Source	Destination	Filter	Action
any	any	Contract-1	permit

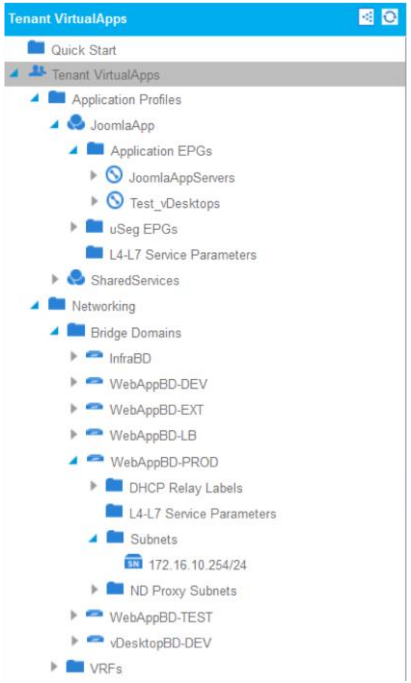
Which is equivalent to:

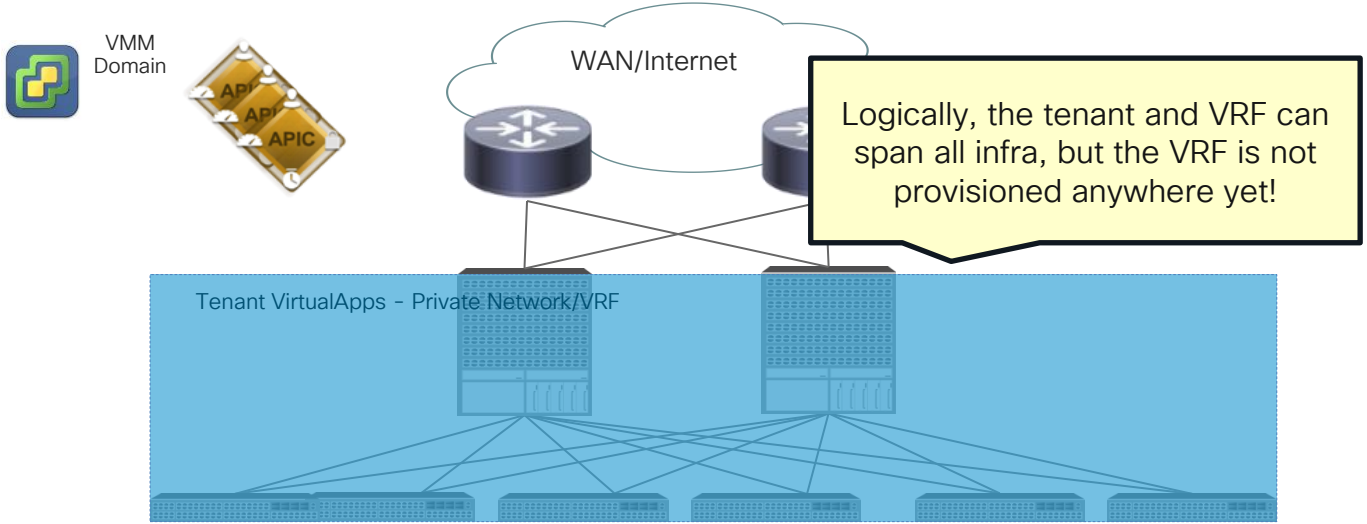
Source	Destination	Filter	Action
EPG-1	EPG-2	contract-1	permit
EPG-2	EPG-1	contract-1	permit
EPG-1	EPG-3	contract-1	permit
EPG-3	EPG-1	contract-1	permit
EPG-2	EPG-3	contract-1	permit
EPG-3	EPG-2	contract-1	permit

Preferred Group Operating Principle



APIC Programs Policy Only Where it is Required





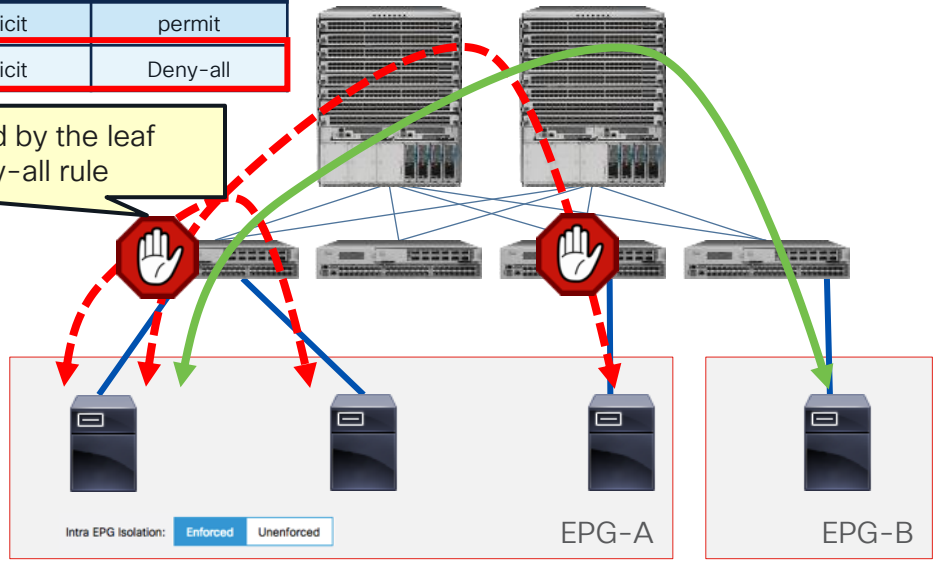
- Until EPGs are associated to domains, nothing is provisioned on any leaf
- EPG can be mapped statically (leaf/port) or dynamically (VMM)
- Policy resolution and deployment is specified when the EPG is associated to a domain
- **Resolution immediacy** – determines when to download policy to the switch software
  - Pre-provision, Immediate, On-demand
- **Deployment immediacy** – specifies when policy is configured on the hardware
  - Immediate, On-demand

ACI Fabric Micro Segmentation Capabilities

Intra EPG Isolation – Zoning Rules

Source	Destination	Filter	Action
EPG-A	EPG-B	implicit	permit
EPG-A	EPG-A	implicit	Deny-all

Intra EPG traffic will be dropped by the leaf because of the implicit deny-all rule

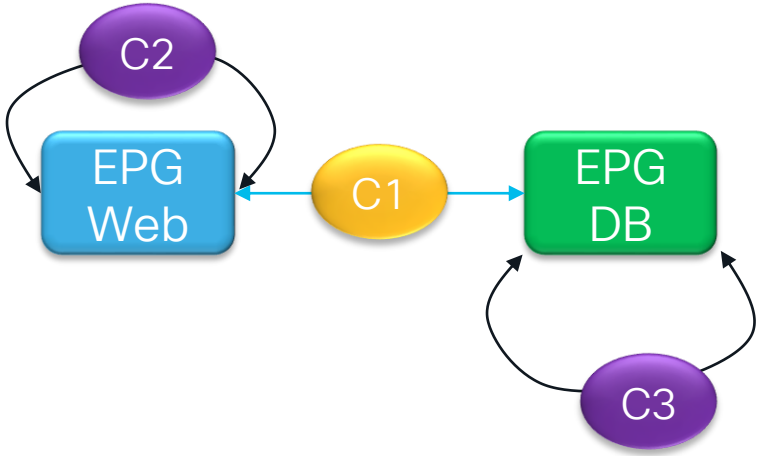


Intra EPG Contracts

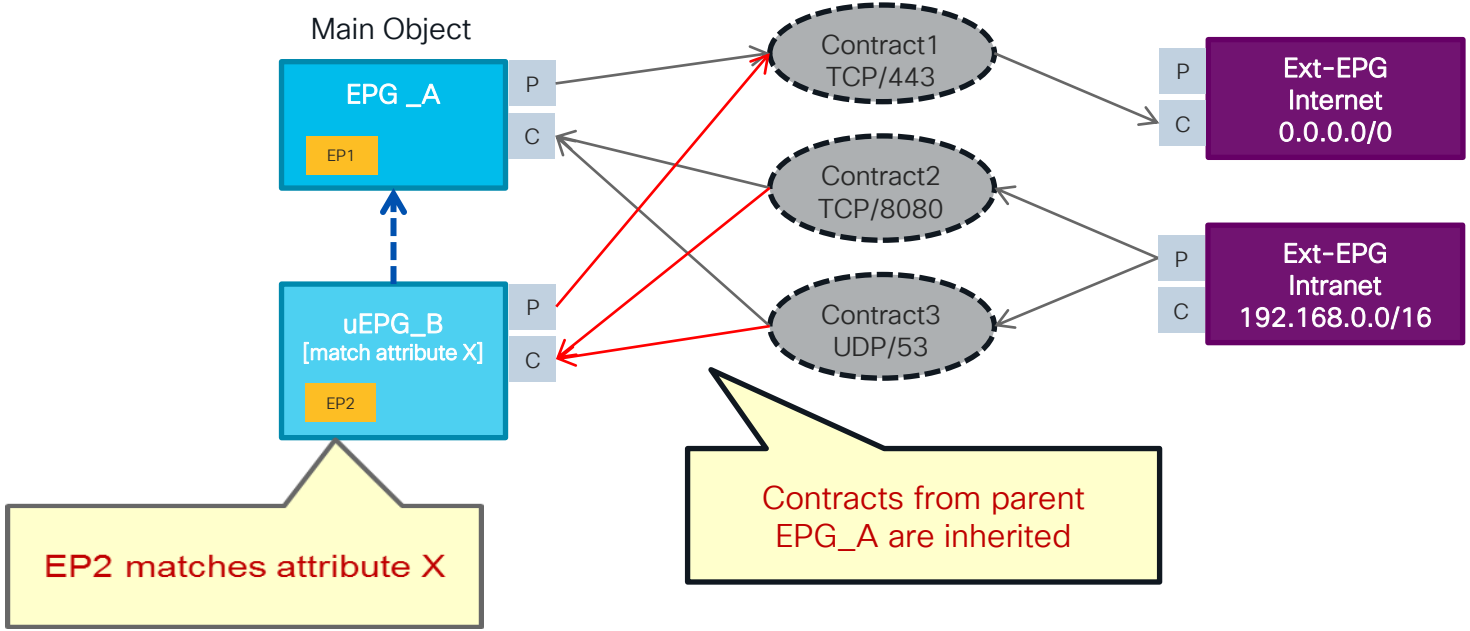
Restricting Communication Between Endpoints Inside a Group

- Since release 3.0, ACI supports “Intra-EPG Contracts”
  - Allows whitelist policy enforcement of Intra-EPG traffic
  - Can co-exist with Inter-EPG contracts
  - Eliminates the need to create uSeg EPGs or deploy external FW for Intra-EPG segmentation
  - Enforcement is on Leaf switch (i.e. Nexus 9000-EX models or above)
  - Same as regular contract scale
  - Requires proxy arp be enabled

Intra-EPG Contract:
- Src-Class = Dest-Class
- Src-Class, Src-Class, Contract

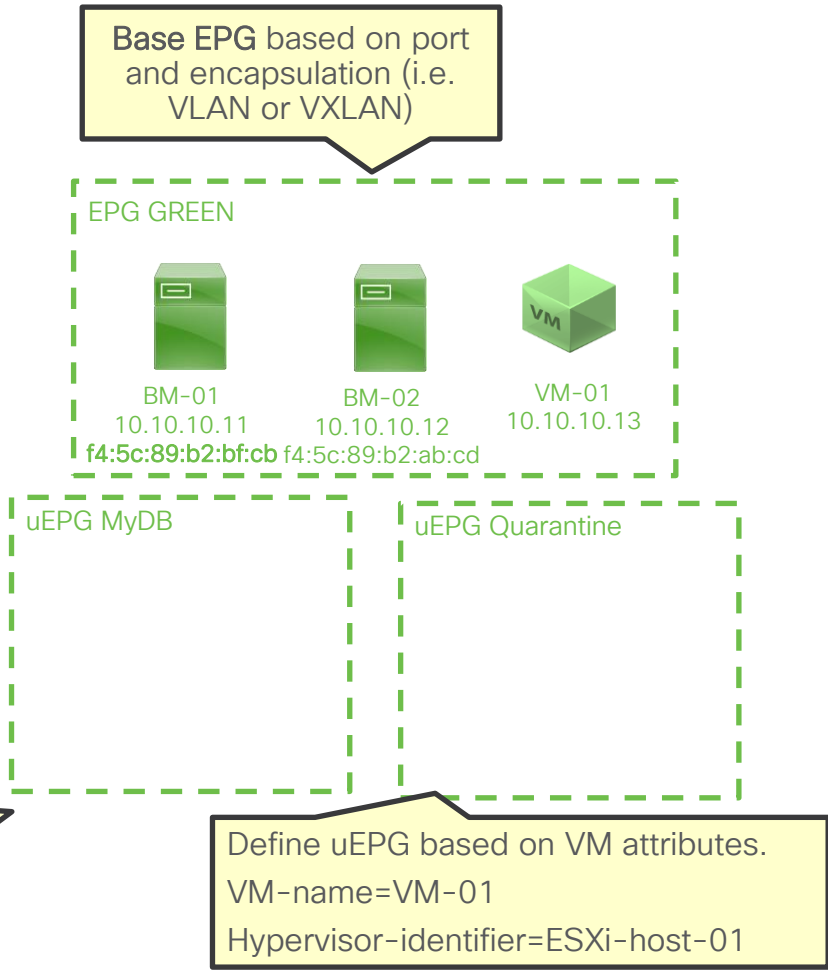


Contract Inheritance – Main & Inherited Objects



Understanding Micro EPGs

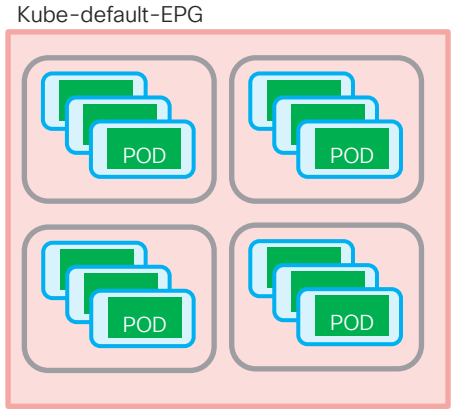
- A MicroEPG (uEPG) is equivalent to a regular EPG for all purposes, but classification is based on endpoint attributes (and dynamic in nature)
- Endpoints assigned to the uEPG regardless of the encapsulation/port
- The endpoint must be first known to a regular EPG, called "**base EPG**"



Micro Segmentation Support for Kubernetes

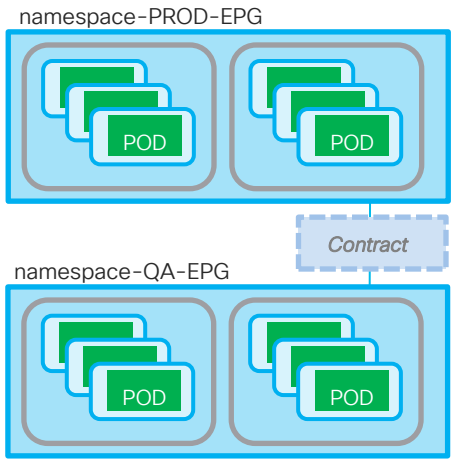
ACI CNI Plugin Supports Multiple Deployment Models

Cluster Isolation



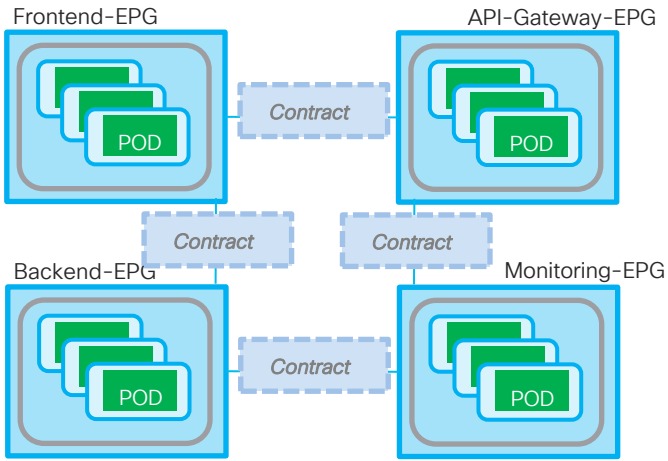
- Default behavior: single EPG for entire cluster user PODs
- No need for internal contracts

Namespace Isolation



- Each namespace mapped to an EPG
- Contracts for inter-namespace traffic are required

Deployment Isolation



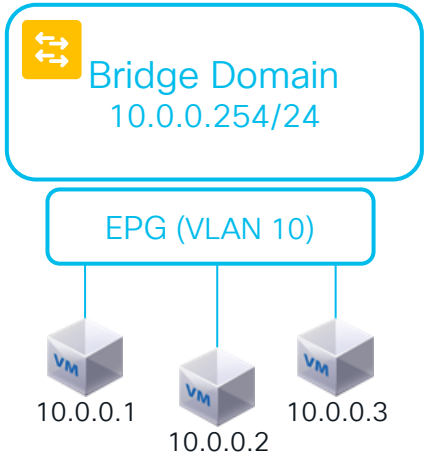
- Each deployment mapped to an EPG
- Contracts control traffic between microservice tiers

Leveraging Endpoint Security Groups (ESG)

Network Centric & Application Centric Design

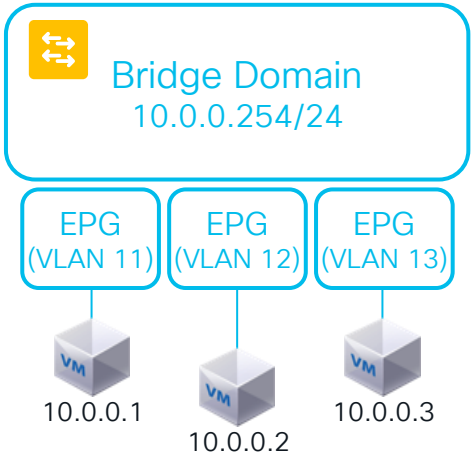
Network Centric

A security group in 1 subnet



Need more granular security group

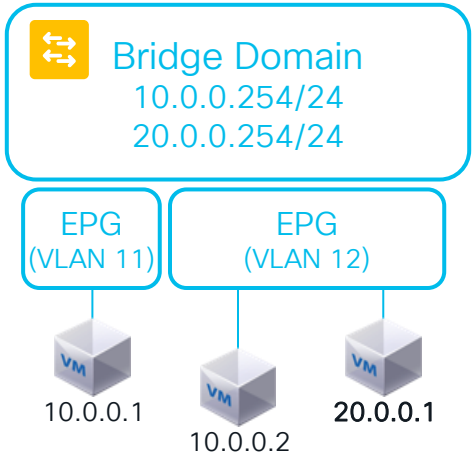
Multiple security groups in 1 subnet



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

Application Centric

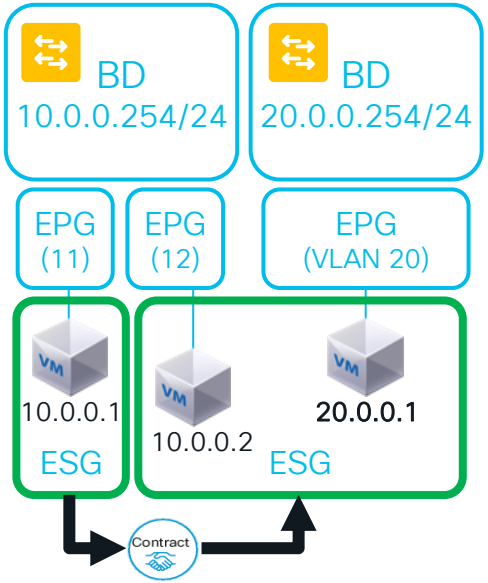
Security groups across subnets



Sharing a broadcast domain brings another security concern

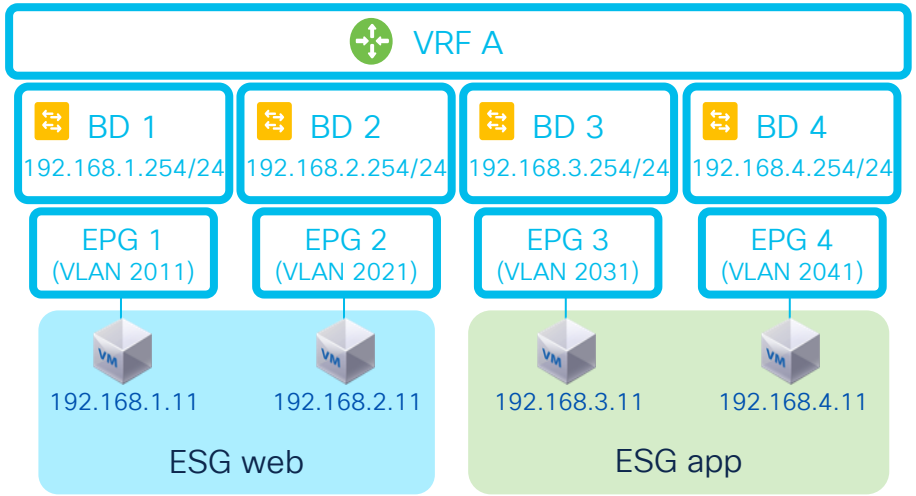
5.0 = Endpoint Security Group (ESG)

Security groups across bridge domains



Flexible security grouping

What is End Point Security Group (ESG)?

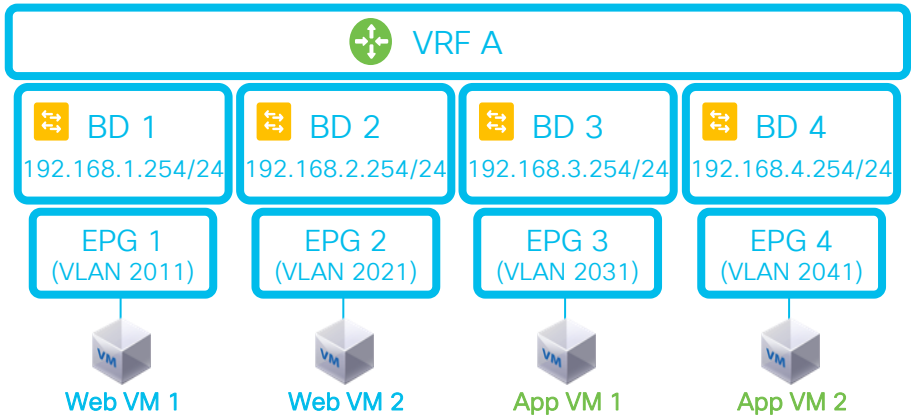


- ESG is a security group across BDs (EPG was across VLANs but within one BD)
- Configure “EP Selector” to classify endpoints into each ESG (in 5.0, IP selector only)
- EPG becomes merely a “VLAN – path” binding component.

The Primary Benefits of ESG (Example)

== Requirement ==

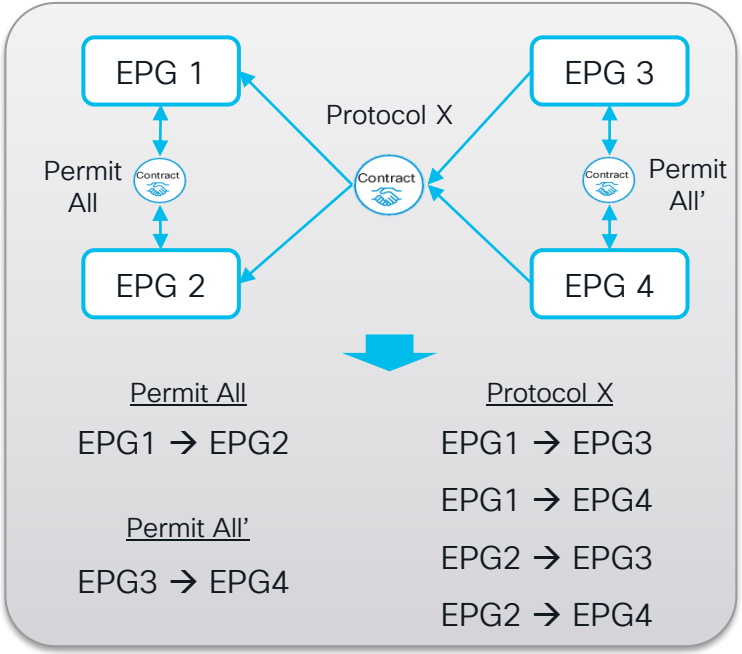
Web VMs can talk to App VMs via port X



- **Simpler Contract Configurations**
- **Policy TCAM (contract rules) Usage Optimization**

== With EPG ==

6 Contract Rules (Zoning Rules)

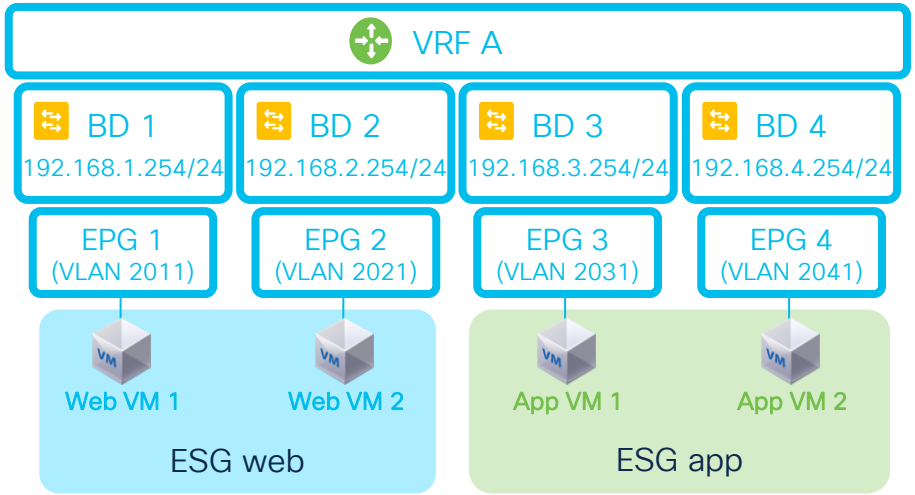


※ 12 rules for bi-directional ※

The Primary Benefits of ESG (Example Cont)

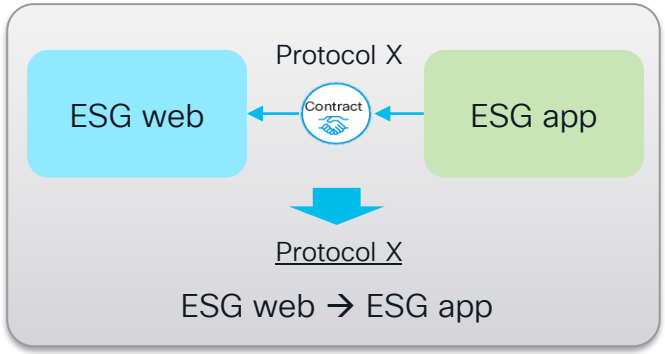
== Requirement ==

Web VMs can talk to App VMs via port X



== With ESG ==

1 Contract Rule (Zoning Rule)



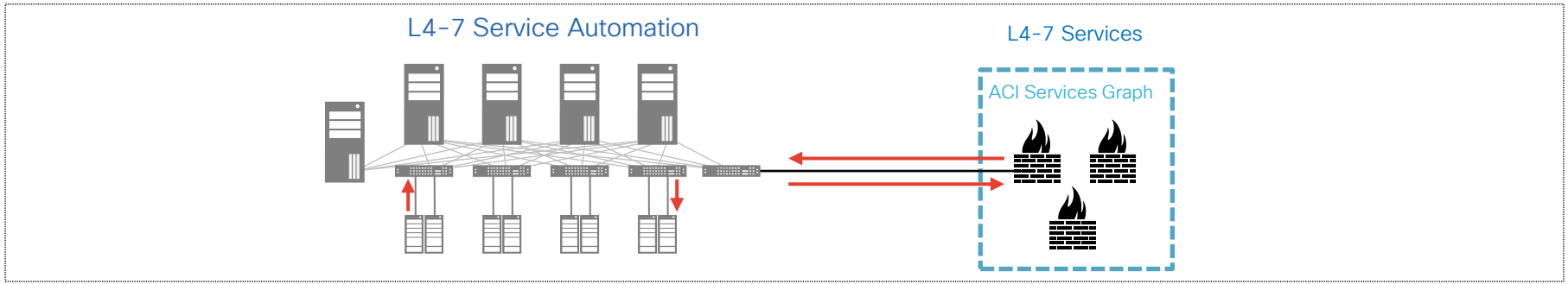
※ 2 rules for bi-directional ※

Simple & Optimized

ACI Fabric L4-L7 Services Automation

L4-L7 Service Automation – Support for All Devices

Any Device and Cluster Manager Support



Network Policy Mode

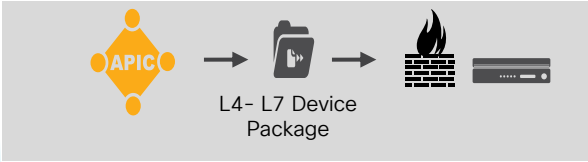
Centralized network automation L2-L3 (service stitching)

EPG model or unmanaged service graphs

Service Policy Mode

Centralized single point of management for full L2-L7 Service Automation

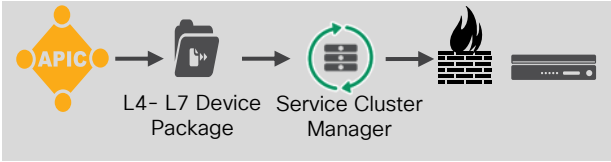
APIC manages fabric and network services



Service Manager Mode

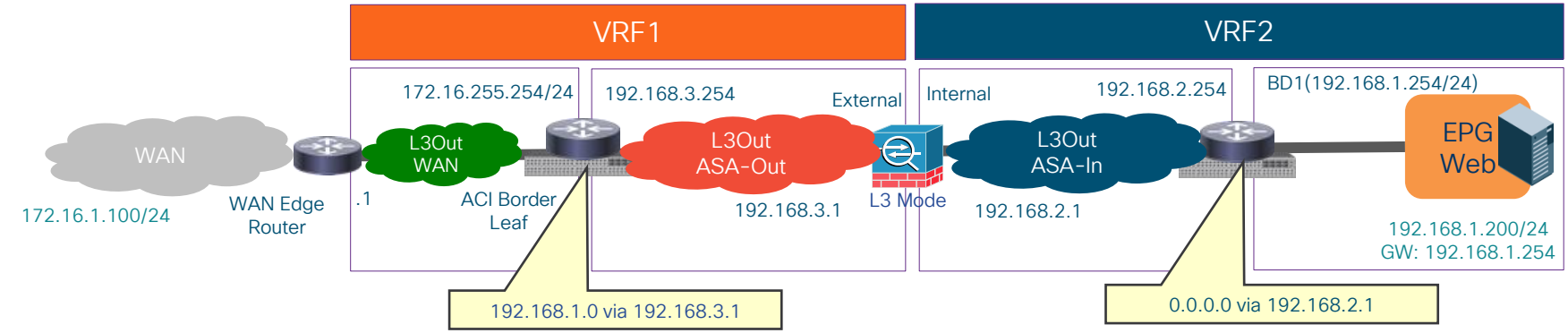
Joint management of L4-L7 service devices through Cisco APIC and a service device controller

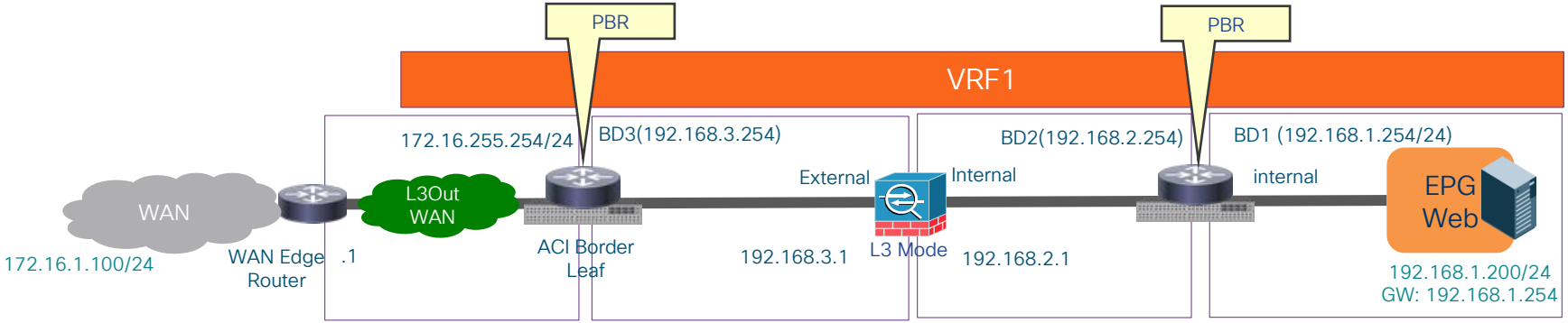
APIC manages a subset of features with operational flexibility



Service Device Insertion Comparison

VRF “Sandwich” vs Service Graph Redirect & PBR





Cloud Network Controller – Public Cloud Connectivity

Hybrid Cloud Networking Challenges

Connectivity

How do I connect applications across on premises, public clouds and edge networks?

Zero Trust and Security

How do I maintain a consistent security posture that is agnostic to where my app and clients are located?

Visibility

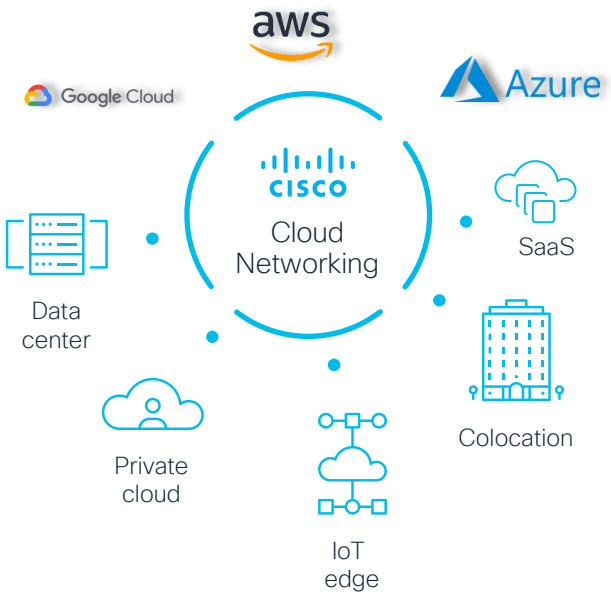
How do I observe and analyze connectivity, traces, logs, and metrics across heterogeneous networks?

Application Networking

How can I enable application intent to dynamically drive network behavior?

Connecting the Clouds

Hybrid Multi Cloud: On-Prem, AWS, Azure and Google Clouds



1. Connect across AWS, Azure, GCP and/or on-premises
2. Operate and troubleshoot heterogenous multicloud networks
3. Optimize path selection between data center and cloud (with SD-WAN transit)
4. Maintain consistent security posture across hybrid cloud environments
5. Automate L4-7 service insertion (3rd-party and cloud native)

Need for homogenous experience across heterogenous cloud environments

Hybrid Multi Cloud Networking: Capabilities

ACI and NDFC Fabrics

Automate connectivity

Visibility and troubleshooting

Segmentation and policy

App networking

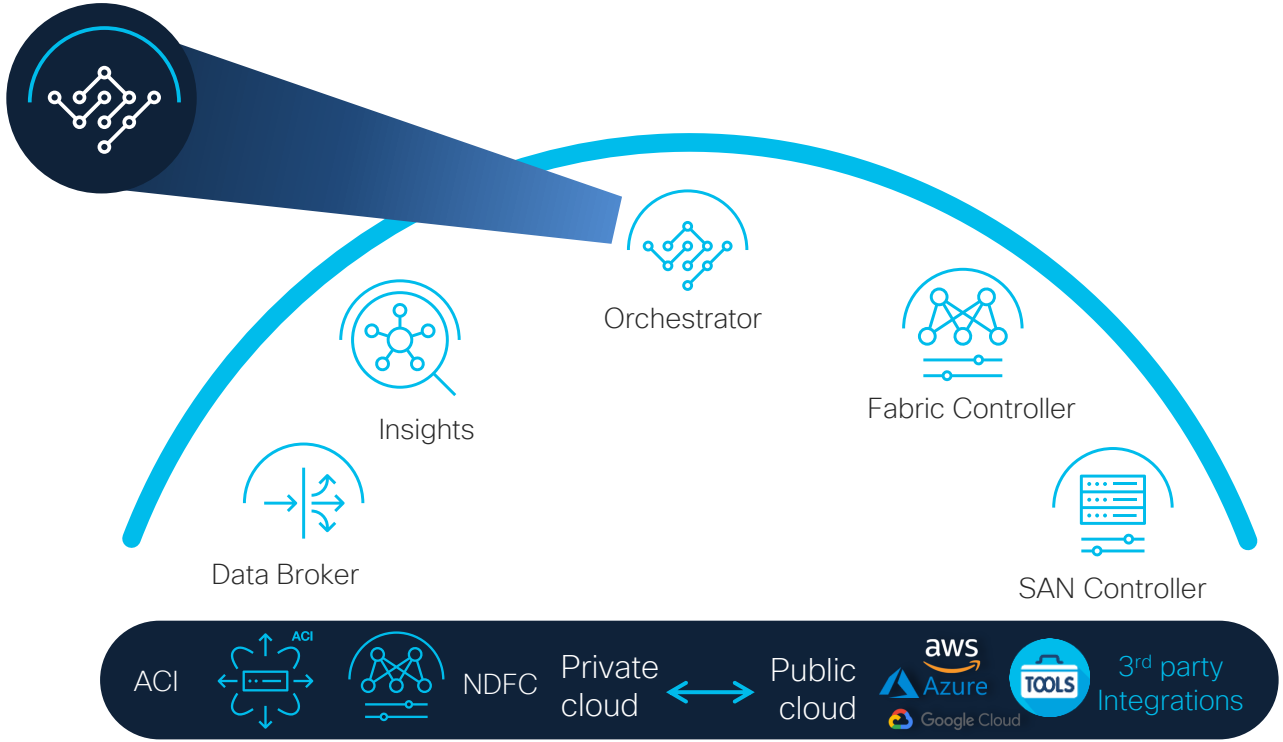
Nexus Dashboard Orchestrator (NDO)

Simplified Hybrid Multi Cloud Segmentation, Connectivity and Visualization

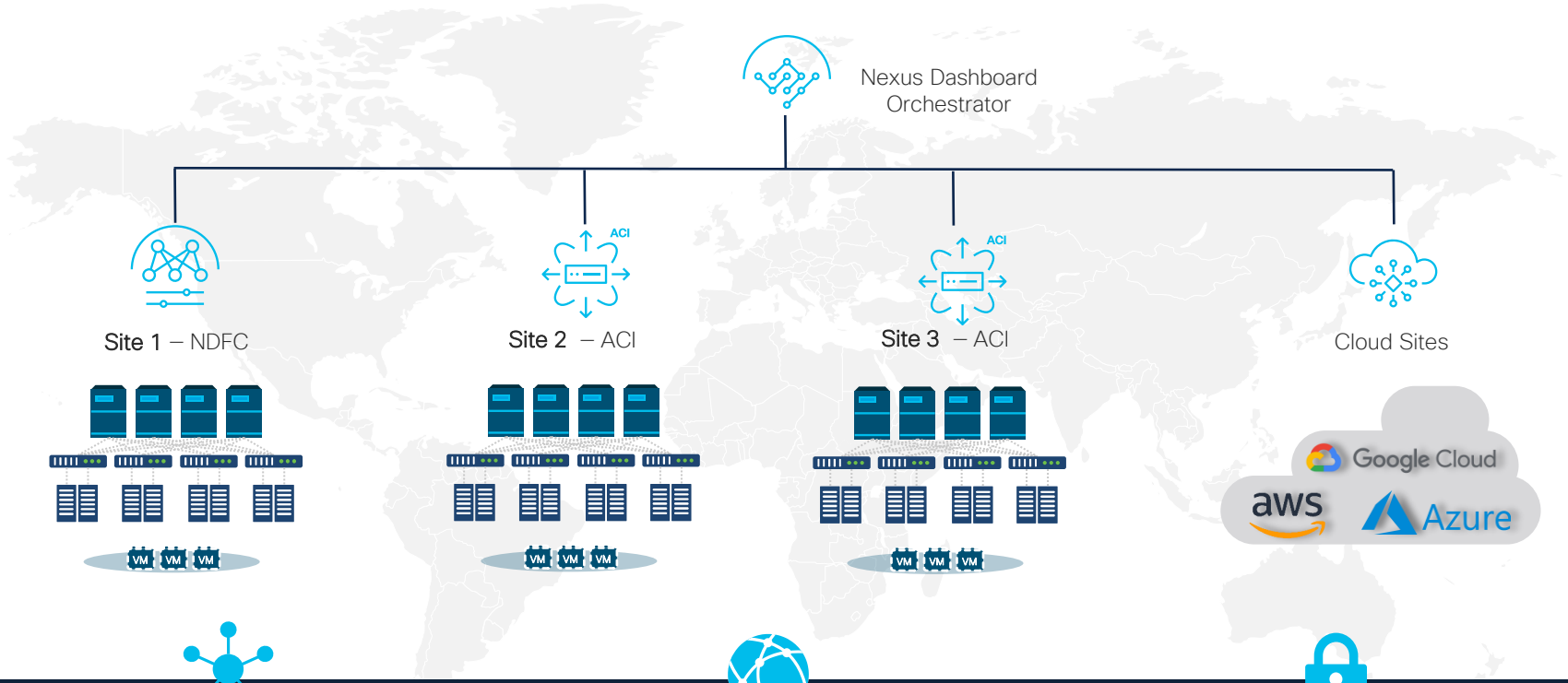
Connectivity

Segmentation

Visualization



Connect Multiple Clouds with Nexus Dashboard



Single Point of Orchestration

Consistent Network and Policy

Secure Automated Connectivity

Cisco Cloud APIC is Now Cisco Cloud Network Controller

Coupled:
Security Policy and Network Connectivity Through Contracts

De-Coupled:
Security Policy and Network Connectivity

Specify Security Policy Using Contracts

Network Connectivity Enabled Per VRF, Route Maps

Multi Cloud Networking – Solution Building Blocks

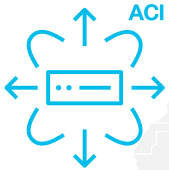
Cisco Cloud Network Controller aka “CNC”

Catalyst 8000v
or
Cloud Native Router

Nexus Dashboard Orchestrator

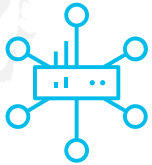
Multi Cloud Networking – Flexible Deployment Models

Cloud only



Hybrid with on-premises ACI

Hybrid with on-premises NDFC

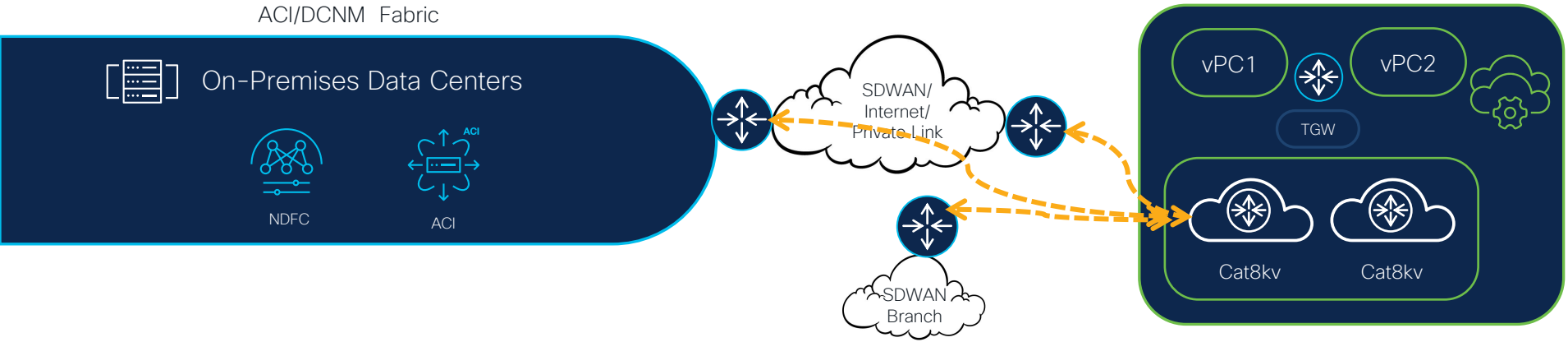


Connect to external networks

SD-WAN router
Branch router
Data Center edge router

Cisco Cloud Network Controller (CNC)

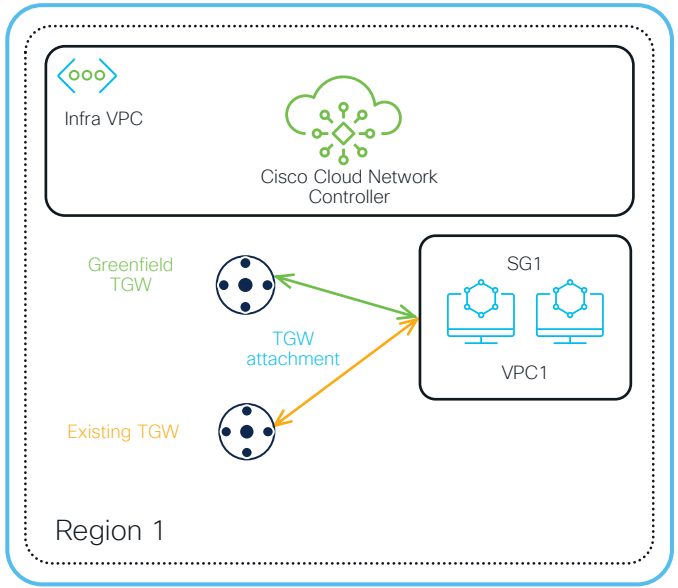
Automation Capabilities



Configuration Automation

- Cat8Kv Lifecycle Management
- TGW Lifecycle Management
- TGW Connect Tunnel Configuration
- TGW Inter-Region Peering
- VPC TGW Attach
- Security Group Rule Management
- End Point Discovery
- TGW VPN Attachment
- BGP EVPN and VXLAN Tunnel
- IPSEC and BGP for Branch connectivity
- Application Load Balancer Automation
- Route Propagation between External network and Cloud

Brownfield VPC Onboarding

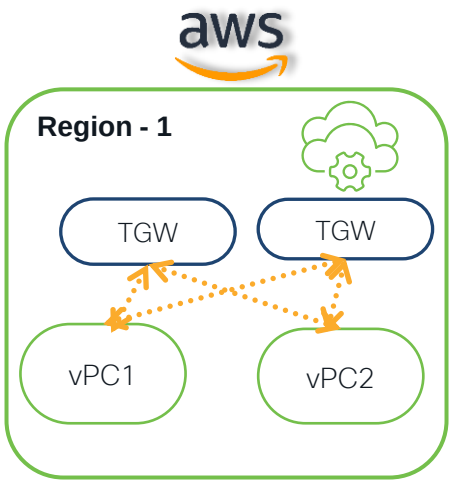


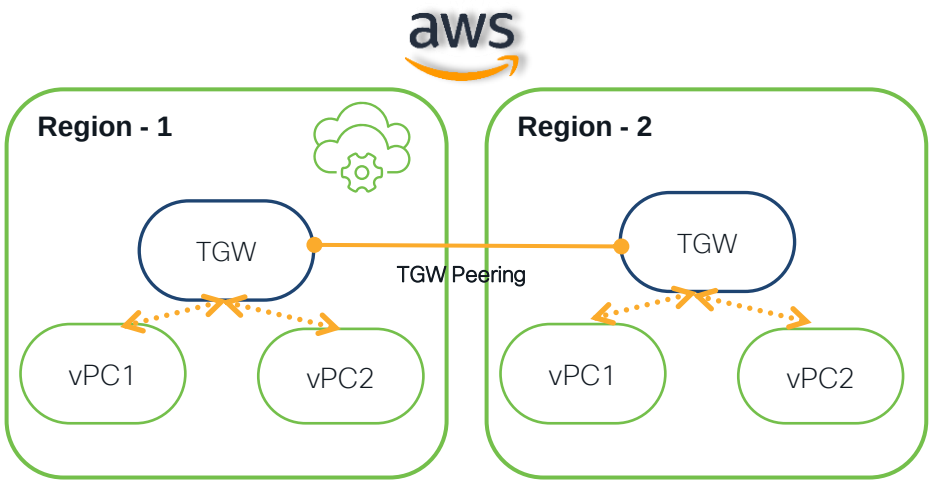
- Cloud Network Controller creates new TGW
- or VPC peering
- It copies configuration from the existing TGW:
  - Route tables cloned
  - SG rules are not copied, new created
- No changes on existing TGW
- Catalyst 8000v will take care of BGP

Benefits

Seamless Migration | Simplified Operations | Co-existence

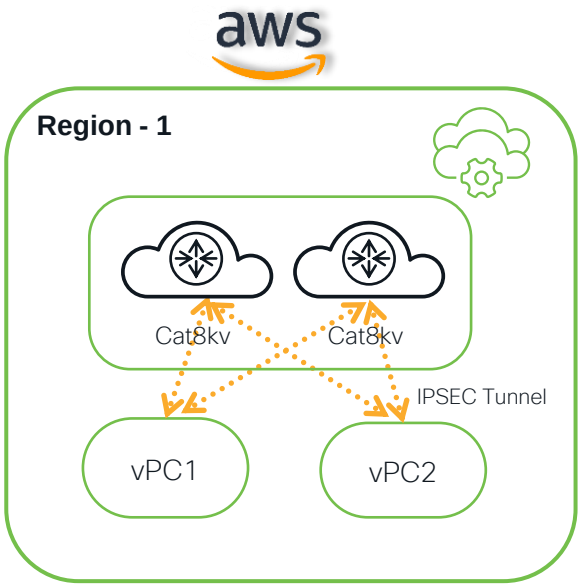
Intra-Cloud Connectivity Automation: Using TGW

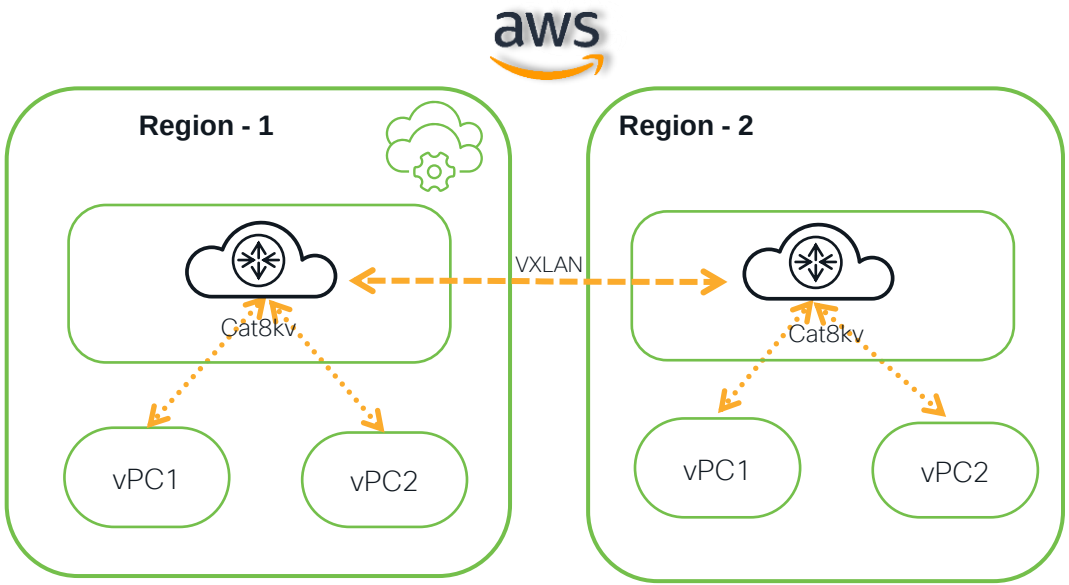




Automate Network Connectivity For Intra-Region and Inter-Region Traffic

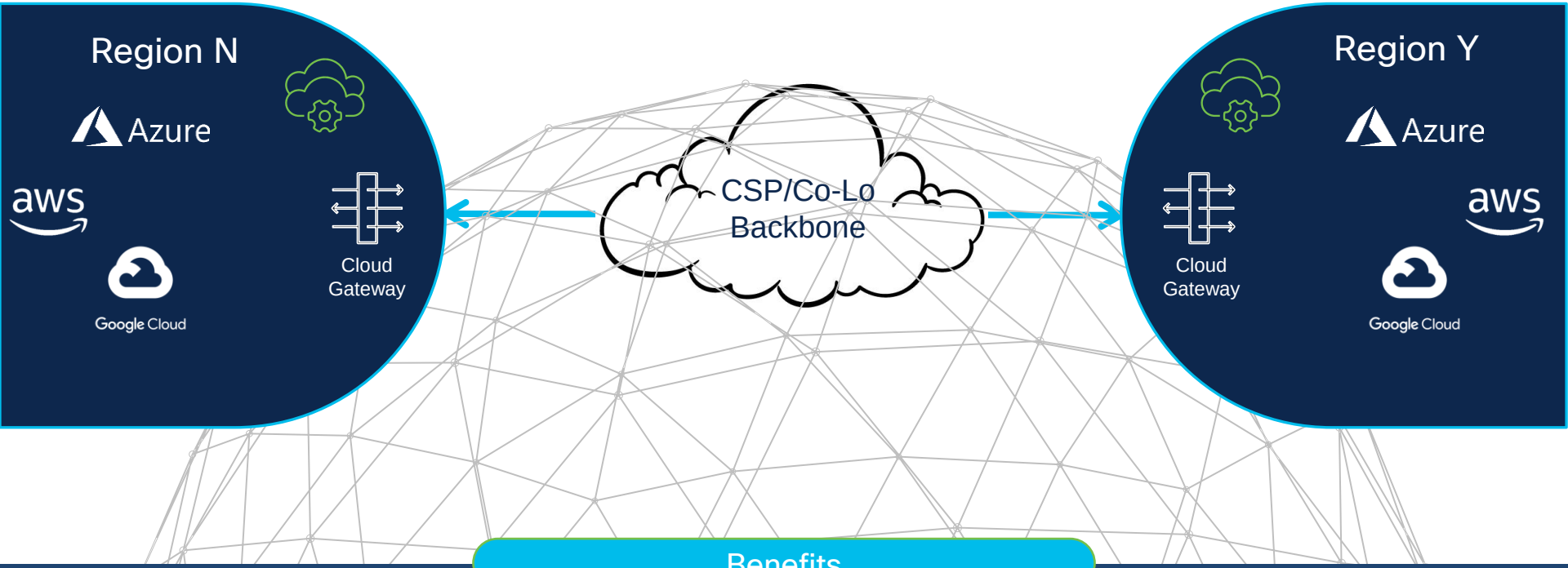
Intra-Cloud Connectivity Automation: Using Cat8Kv





Automate Network Connectivity For Intra-Region and Inter-Region Traffic

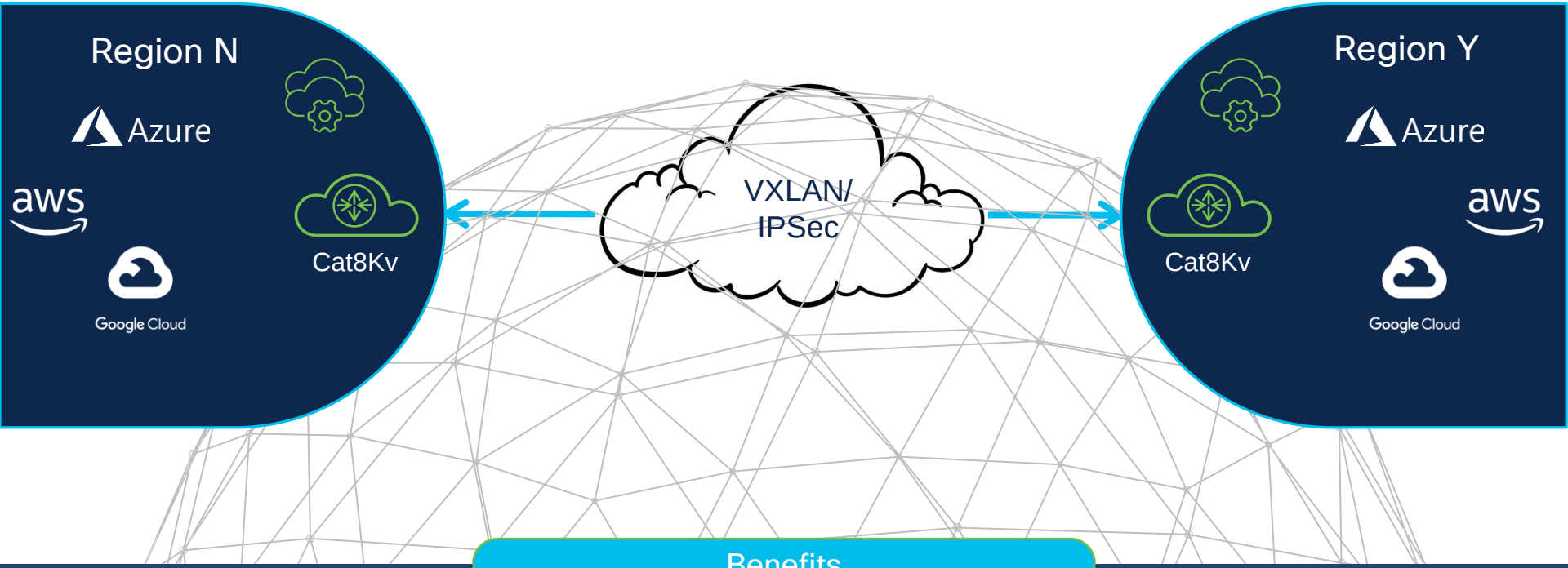
Inter-Cloud Connectivity: Using Cloud Backbone



Benefits

Extend segments across clouds | Automate service redirect

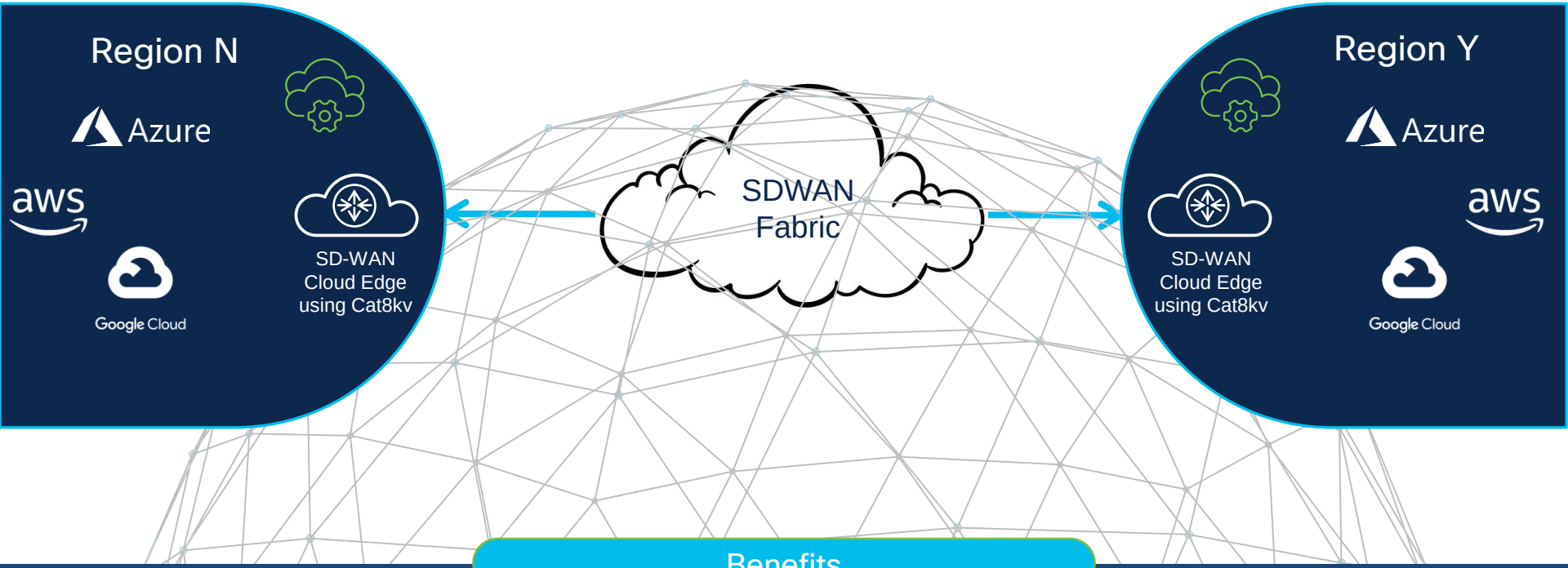
Inter-Cloud Connectivity: Using Cat8Kv



Benefits

Extend segments across clouds | Automate service redirect

Inter-Cloud Connectivity: Using SDWAN



Benefits

Extend segments across clouds | Automate service redirect

On-Premises to Cloud Connectivity: Using DX/Co-Lo

Requirements

Simplified connectivity for hybrid cloud

Enable high bandwidth underlay

Utilize cloud native routing

On-Premises to Cloud Connectivity: Using Cat8Kv

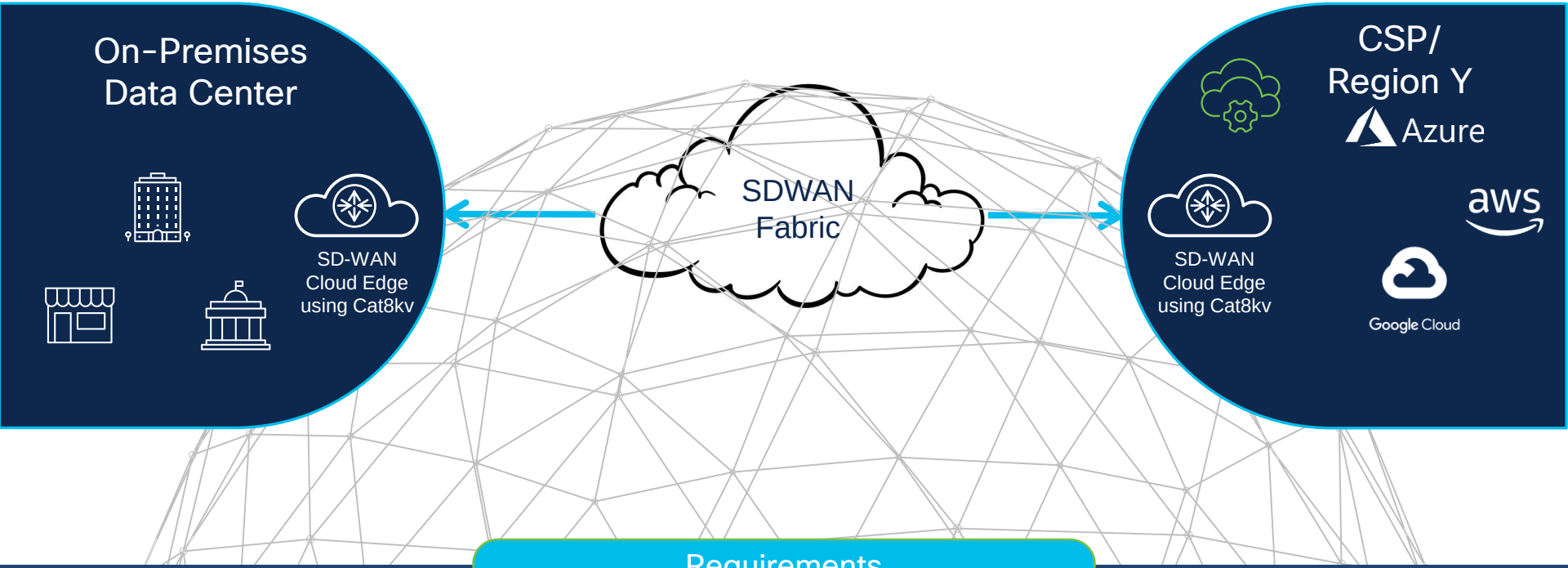
Requirements

Simplified connectivity for hybrid cloud

Enable high bandwidth underlay

Utilize cloud native routing

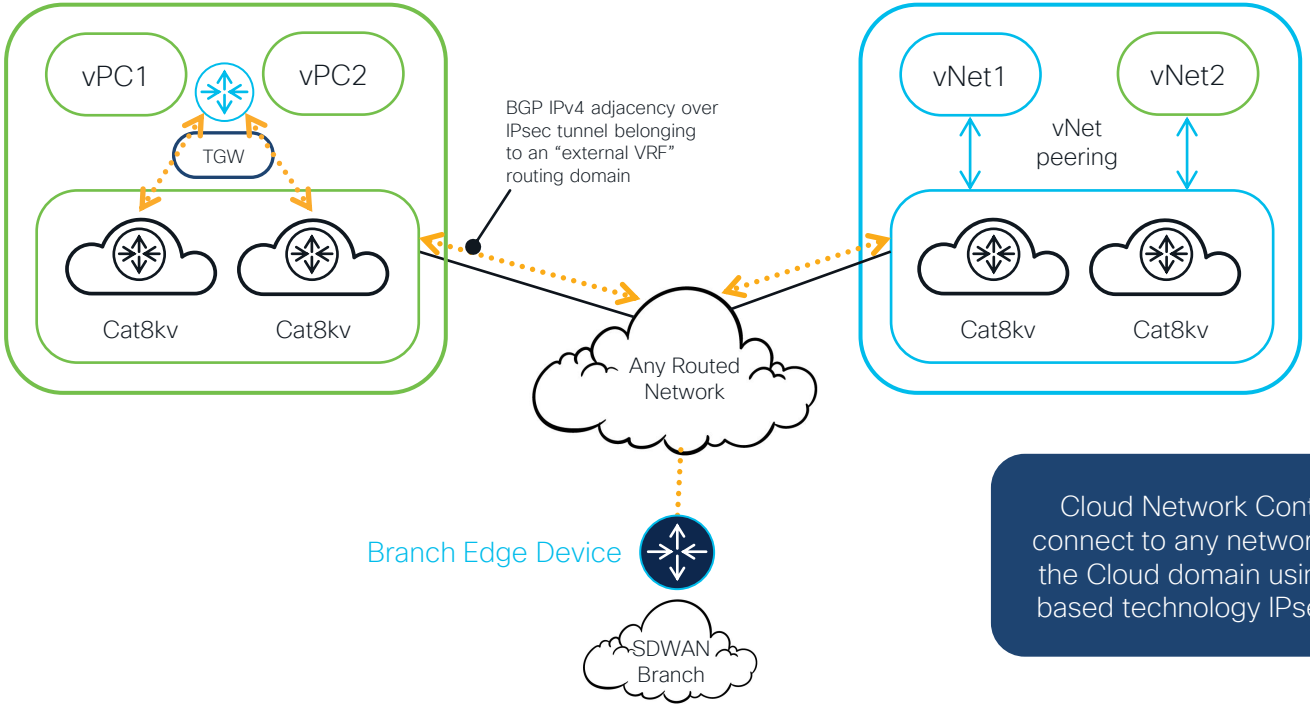
On-Premises to Cloud Connectivity: Using SDWAN



Requirements

Simplified connectivity for hybrid cloud | Enable high bandwidth underlay | Utilize cloud native routing

Branch to Cloud Connectivity: Using Cat8Kv

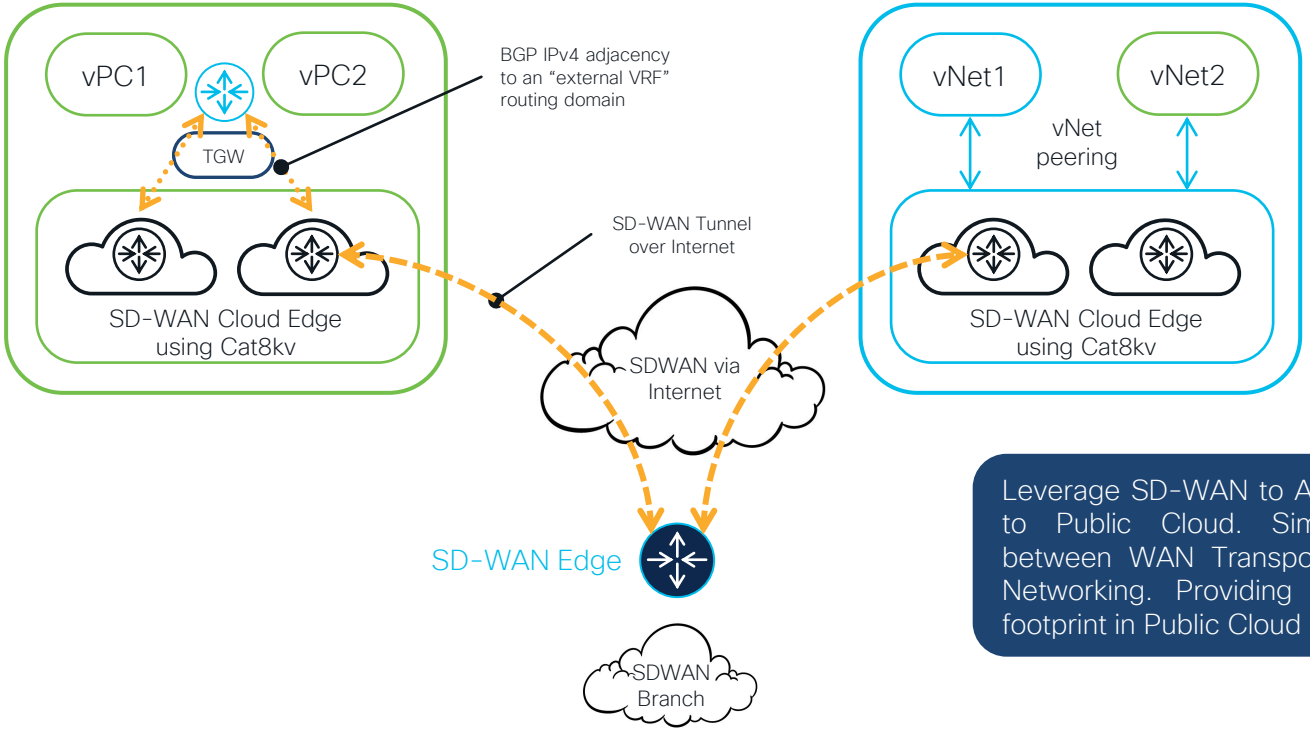


Cloud Network Controller can connect to any network outside of the Cloud domain using standard based technology IPsec and BGP

Benefits

Flexibility

Branch to Cloud Connectivity: Using SDWAN



Leverage SD-WAN to Access from Branch to Public Cloud. Simplified integration between WAN Transport and Intra-Cloud Networking. Providing reduced resource footprint in Public Cloud (Hub only)

Cisco Cloud Network Controller

Cloud Networking

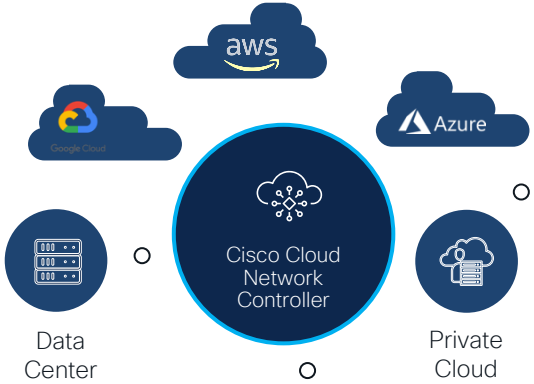
- Intra-Cloud : TGW, VNET Peering
- Inter-Cloud : C8Kv automation
- Connectivity: IPSEC, Direct Connect, Express Route

Visibility

- View and connect to brownfield VPC networks
- Inventory and topology view

L4-L7 Services

- Automate service insertion and service chaining (Load balancers, Firewalls, …)



Segmentation

- Extend segments from On-Premises to cloud
- Extend segments from cloud to cloud
- Security Group rule management

Support on Public and Private Clouds

- AWS, Azure, Google Cloud
- Azure Stack Hub

Open APIs

- Enable automation using Terraform and Ansible

Introduction to Secure Workload Platform

Segmentation is a Critical Control

Implement zero trust segmentation for least privilege communication

Apply multi-layered access controls with host level enforcement

Restrict access to commonly exploited protocols (RDP/SMB)

Where are the Firewalls?

Host Operating System

Windows Server · Red Hat Enterprise Linux · ORACLE Linux · ubuntu · aws · SUSE · CentOS · AIX

Kubernetes Nodes

RED HAT OPENSHIFT

Virtual Desktops

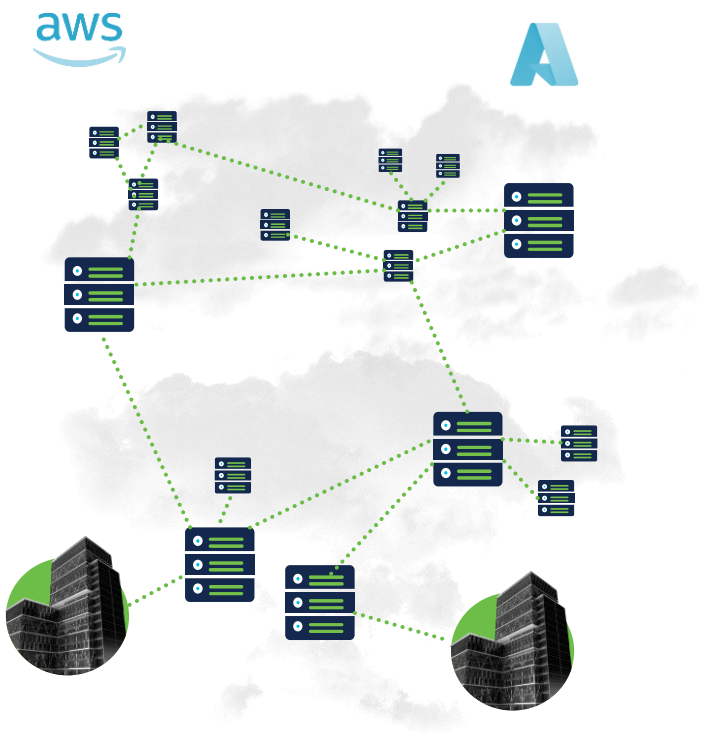
Windows 10

Cloud Security Groups

Load Balancers/
Ingress Controllers

f5 · CITRIX · HAPROXY · NGINX

Firewalls



The Policy Puzzle

Host Operating System

Kubernetes Nodes

Virtual Desktops

Windows 10

Cloud Security Groups

Load Balancers/
Ingress Controllers

Firewalls

Policy Domains

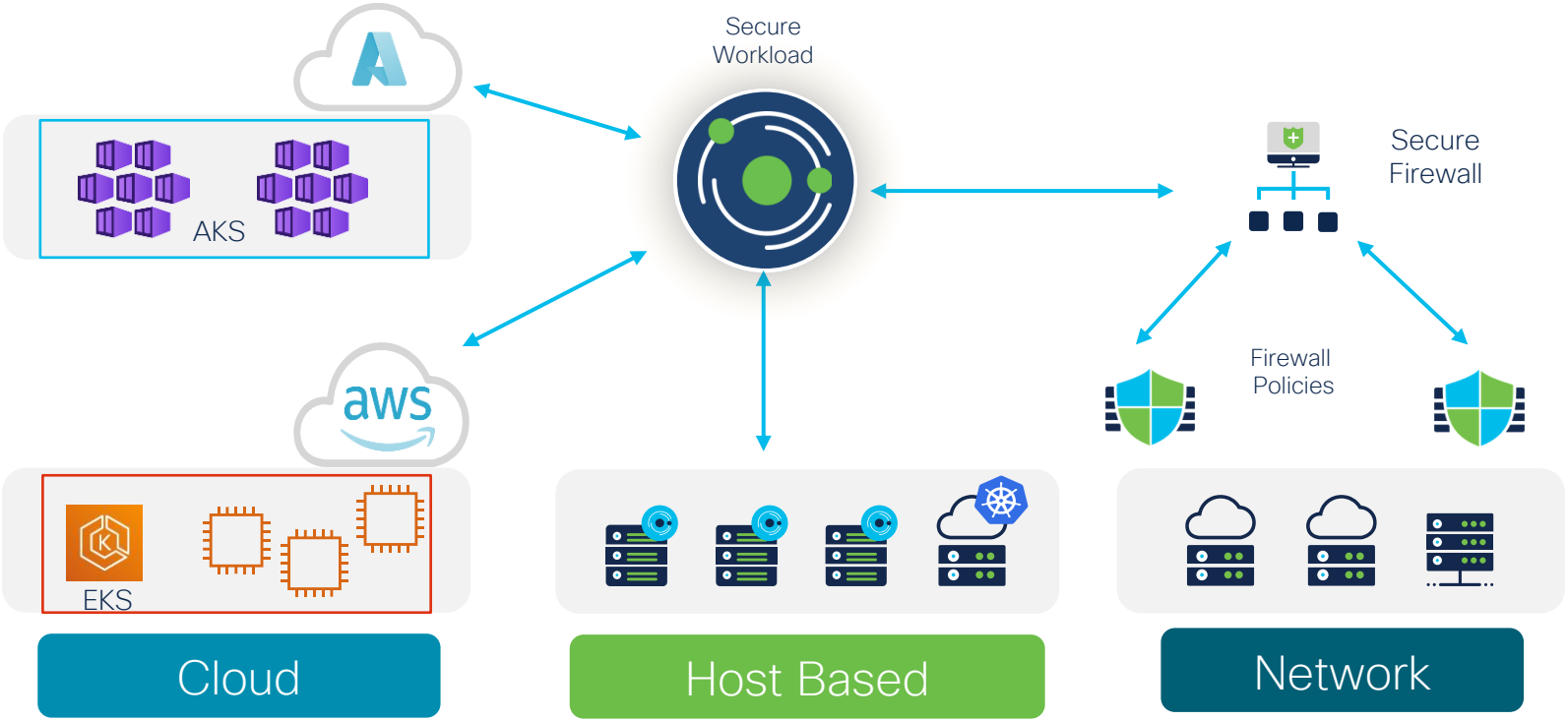
Multiple **teams** and organizations

Multiple **environments and clouds**

Each have **segmentation** methods and tools

Inconsistent and siloed islands of policy controls across network & apps

Unified Policy Across Host, Network and Cloud



Dynamically Securing the Application Environment

Profile relationships
Full visibility of all application conversations

Automated policy
Unified policy across for all application workloads

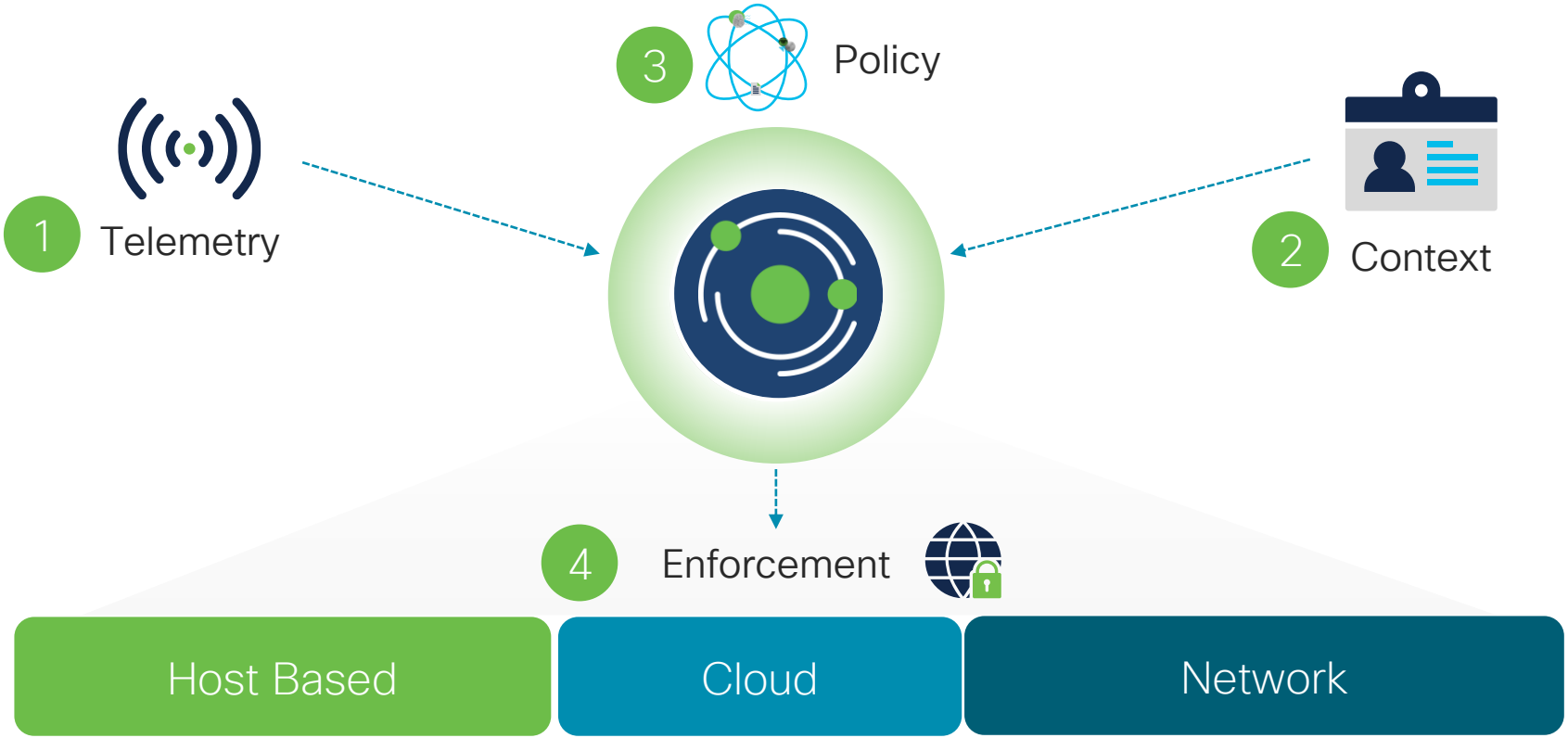
Deploy controls
Fully automated, dynamic attribute-based enforcement

Monitor compliance
Identify communications that violate policy and block if desired

Secure your application workloads:

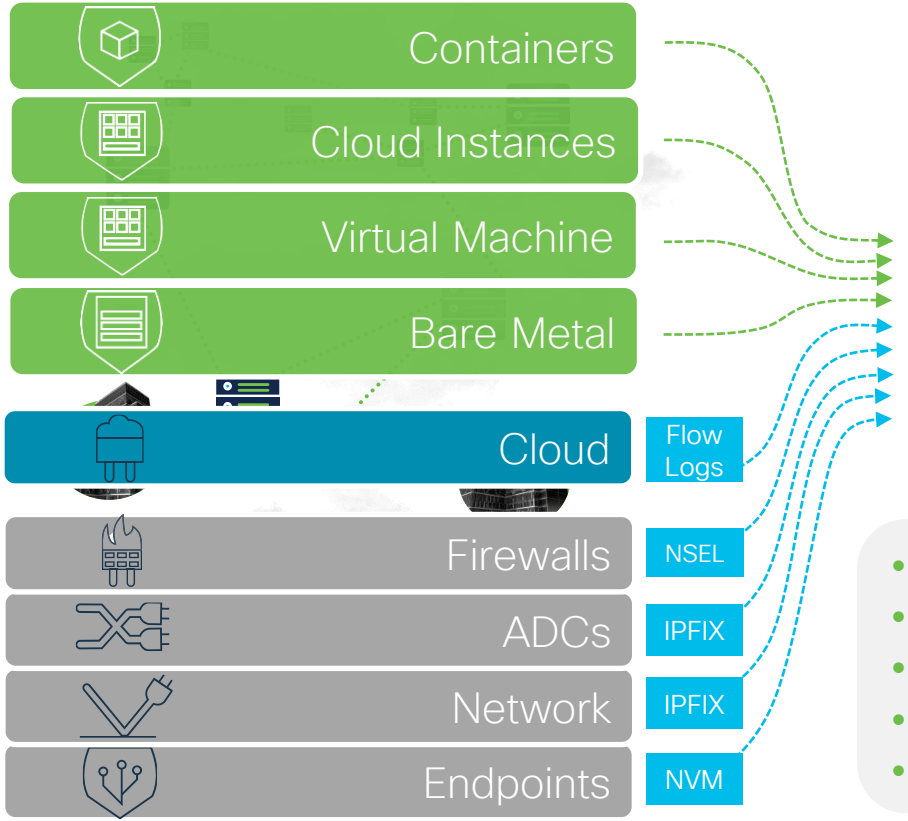
Learn | Build | Protect | Assure

Cisco Secure Workload Overview



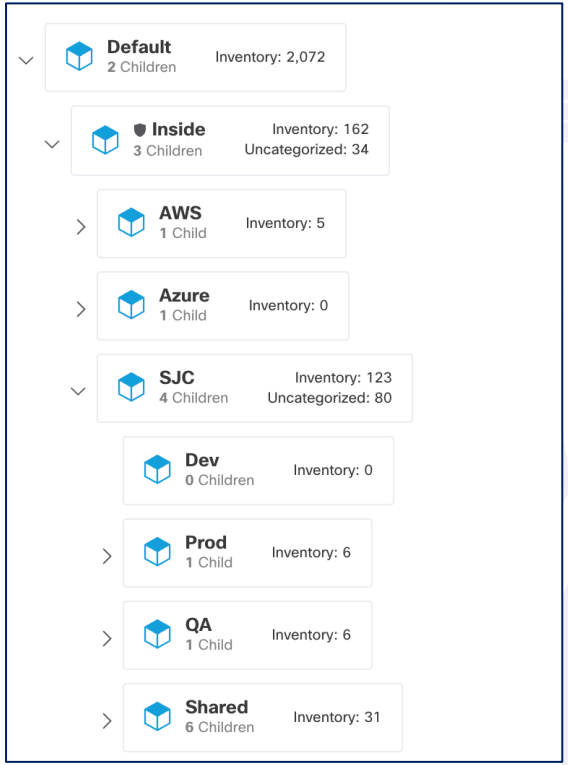
See All Communications

1 Telemetry



- Visibility of all communications
- Detailed machine/process/vulnerability
- Full coverage
- Any environment, any cloud
- Construct inventory of every endpoint

Apply Order to Chaos



Context

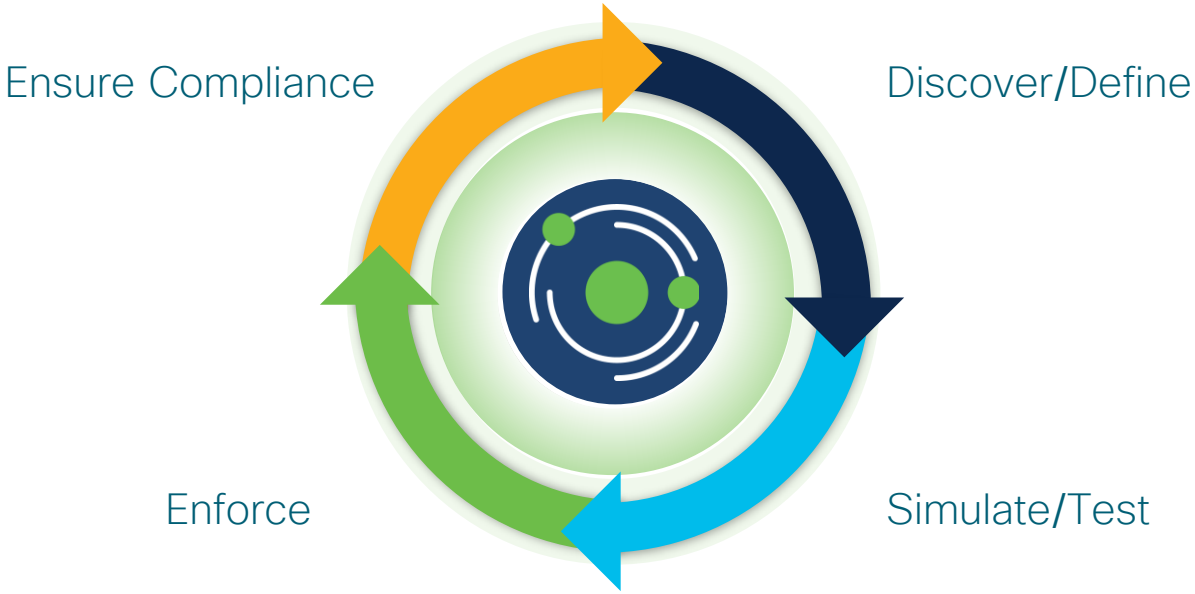
- Orchestrator — Tags/Labels
- Cloud — Tags/Labels
- CMDB — CI Attributes
- IPAM — IP Attributes
- NAC — User/Endpoint

- Dynamic labels
- Sourced from systems of record
- Continuously updated

Policy Which Lives and Breathes

3

Policy



End to End Policy Enforcement

4

Enforcement

Policy

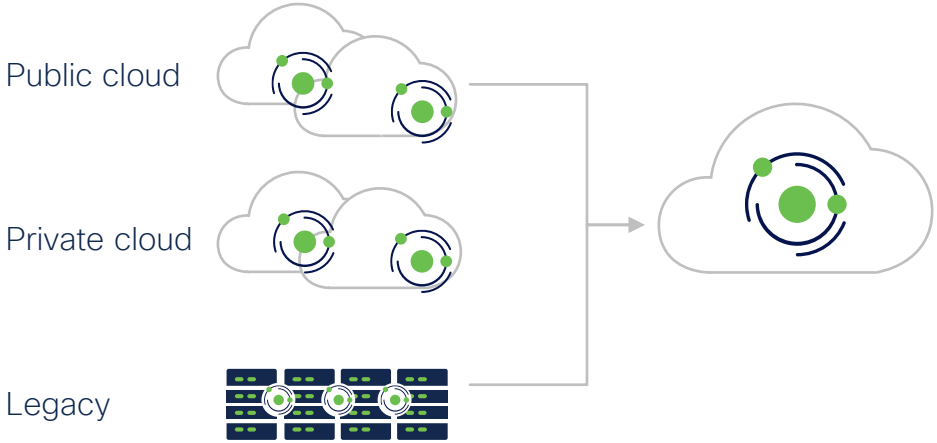
- Policy continuously updated
- Uniquely programmed per workload
- Agentless support for cloud and network visibility and enforcement

Host Based | Cloud | Network

Cisco Secure Workload – SaaS Option

Software subscription license based on number of workloads; available in 1- and 3-year terms

- Cisco Secure Workload SaaS model: No need to purchase, install, and manage hardware or software
- Fully managed and operated by Cisco
- Suitable for commercial customers and SaaS-first/SaaS-only customers
- Flexible pricing model; lower barrier to entry
- Quick turn up
- Faster time to value
- Lower total cost of ownership



Cisco Secure Workload – On-Premises Options

Cisco Secure Workload Platform (large form factor)

Suitable for deployments of more than
5000 workloads

- Built-in redundancy
- Scales to up to 25,000 workloads **

Includes:

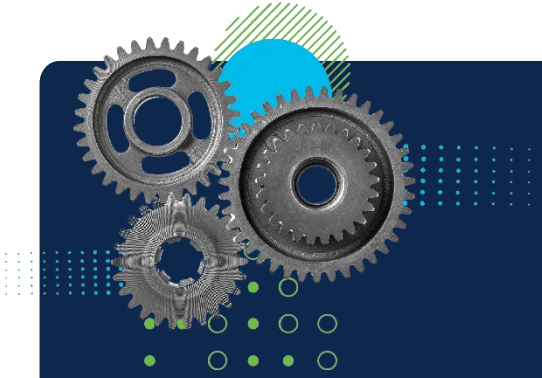
- 36 Cisco UCS® C220 servers
- 3 Cisco Nexus® 9300 platform switches

Cisco Secure Workload-M (small form factor)

Suitable for deployments of less than 5000 workloads **

Includes:

- 6 Cisco UCS C220 servers
- 2 Cisco Nexus 9300platform switches

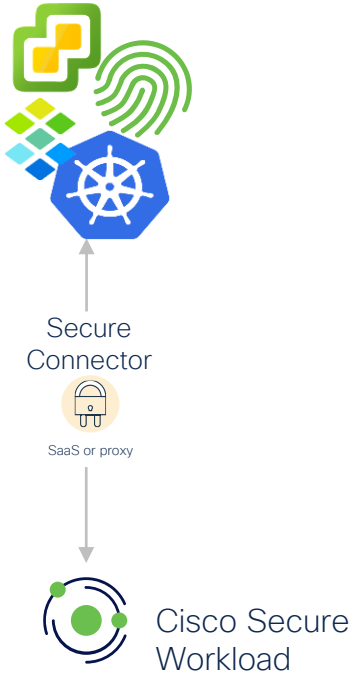


Software subscription license based on number of workloads; available in 1-, 3-, and 5-year terms

** can scale up to two times the limit with conversation-only flow telemetry enabled for all agents

Secure Connector

- When direct communication from Secure Workload to orchestrator/connector is not possible
- Communication is mutually authenticated and encrypted using TLS
- Image available from Secure Workload directly
- API key must have external integration capability and write access to the required scope
- 1 Secure Connector per root scope



VM Minimum Requirements

- RHEL/Centos 7
- 2 CPU
- 4 GB RAM
- Sufficient network bandwidth for handling data from orchestrators/connectors
- Outgoing connectivity to Secure Workload on port 443 (direct or through HTTP(S) proxy)
- Connectivity with internal orchestrator/connectors

Data Ingest Appliance

- External virtual appliance that enables connector integrations with 3rd party platforms to ingest high volume flows and data
- Fixed VMware OVA available from software.cisco.com
- Connectors available
  - Secure Firewall (ASA)
  - F5
  - Citrix
  - AnyConnect
  - ERSPAN
  - Meraki
  - Netflow

VM Specifications

- Centos 7.9
- 8 CPU
- 8 GB RAM
- 250 GB Hard disk
- 3 Network interfaces
- VM hardened by default

Connectors Specifications

- Up to 3 connectors per Ingest Appliance
- Up to 10 connectors of the same type on one tenant (rootscope)
  - ERSPAN is up to 24
  - AnyConnect 50
- Up to 100 connectors of the same type on Secure Workload
  - ERSPAN is up to 450
  - AnyConnect 500
- Up to 15k NetFlow fps (non applicable to ERSPAN)

Edge Connector Appliance

- External virtual appliance to stream alerts to different consumers and collects inventory metadata
- Fixed VMware OVA available from software.cisco.com
- Connectors available
  - Syslog
  - Email
  - Slack
  - PagerDuty
  - Kinesis
  - ServiceNow
  - Cisco ISE

VM Specifications

- Centos 7.9
- 8 CPU
- 8 GB RAM
- 250 GB Hard disk
- 1 Network interface
- VM hardened by default

Connectors Specifications

- Up to 8 connectors per Edge Connector
- Up to 1 edge connector per tenant (rootscope)
  - 1 connector type per tenant

Software Agent Overview

Installs and runs as a user process in the operating system

- No need for any OS kernel modification
- Requires root/administrative privileges

Enables telemetry collection and policy enforcement for segmentation

- Collects metadata from packet headers (no payload), process information, and installed software
- Enforces policies for segmentation through IPsets for Linux and Windows advanced firewall or Windows filtering platform for Windows servers

Software agent thresholds:

- Low CPU overhead (<1%)
- Default limit set to 3% CPU overhead

Cisco Secure Workload Agent-Based Sources

Software Agents (virtual, bare metal, and containers)

Windows servers
(Virtual machines and bare metal)

Windows desktop
(VDI and Workstation)

Linux servers
(virtual machine and bare metal)

IBM zSystems
(z/Linux operating system)

IBM PowerPC and pSeries systems
(AIX operating system)

Container host
(Linux container host OS with DaemonSet)

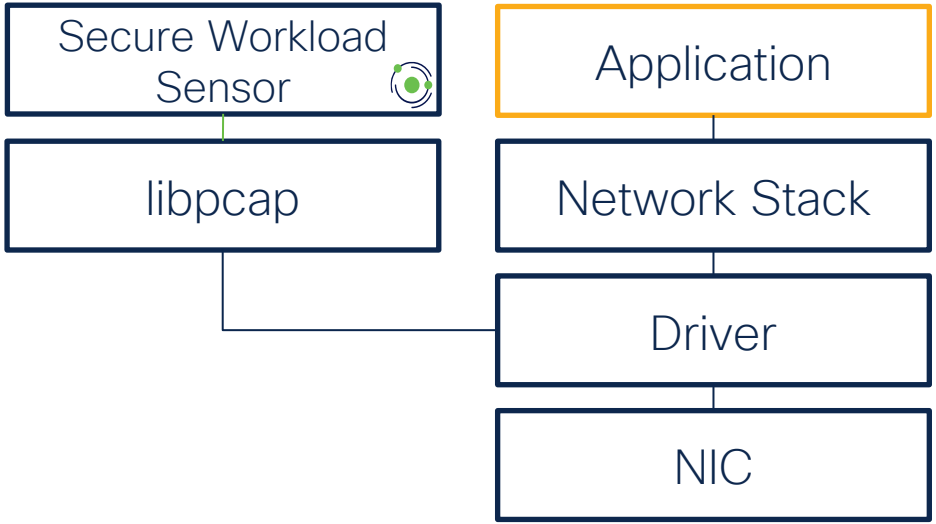
Main features

- Low CPU overhead (SLA enforced)
- Low network overhead
- Enforcement point (software agents)
- Highly secure (code signed and authenticated)
- Every flow (no sampling) and no payload
- Server process and software package information

Cisco Secure Workload Agent-Based Sources

Transparent Agent to Applications

- Runs in the Host OS, not the Hypervisor
- Access to accurate state of the application and *all* connectivity
  - No Sampling, All Packets (no payload)
- Not in the data path
  - Sits in User Space
  - Designed by Kernel Developers
  - No fingerprinting (cannot be seen)
  - No performance hit, no latency hit
- SLA Enforcement
  - CPU (<3%) and BW throttling
- Auto-upgrade or manual upgrade options



Software Agents Telemetry

Packet header metadata (Detailed Mode)

- Metadata from packet header (no payload)
  - Data up to layer-4
  - Granular IP and TCP flags
  - Volume of traffic
- Captures information from every packet, every flow
- Interfaces available on the workload
- Interface through which each communication transits
- Exports this metadata to Secure Workload every second

Process details

- Process snapshot – Inventory of process executed on a workload
  - Who ran the process
  - When it started
  - What process parameters were used
  - What was the process hash
  - What is the process lineage
- Sends complete snapshot of this information to Secure Workload

Installed software

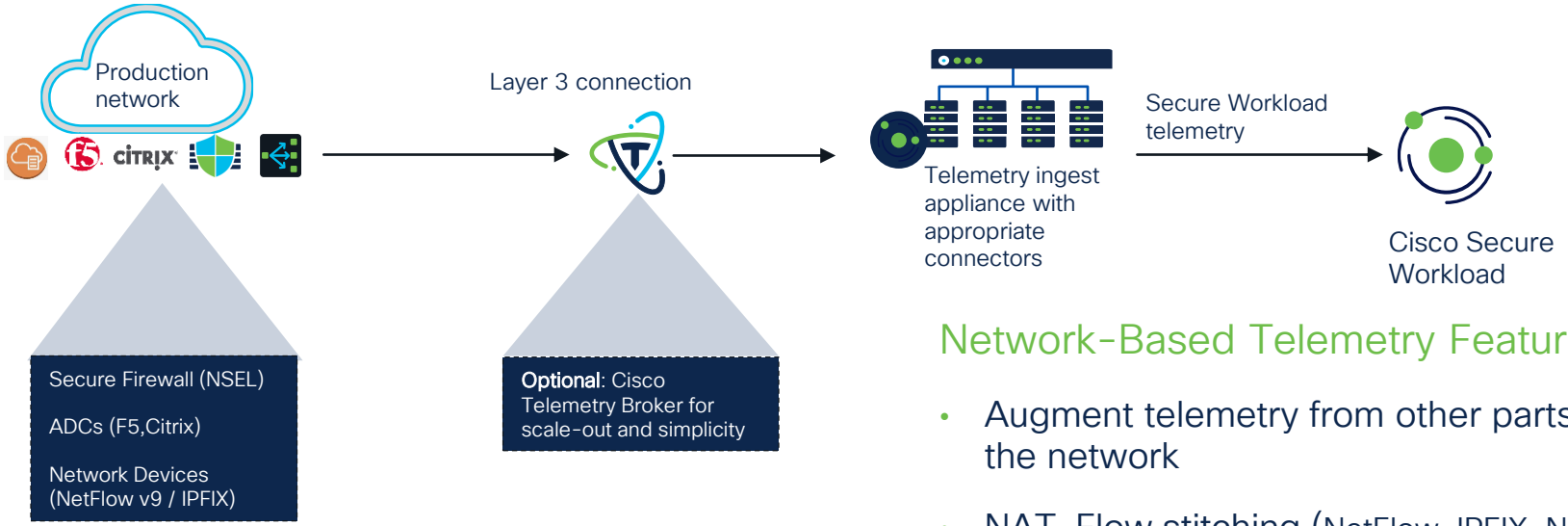
- Details about operating system version, patch level, etc.
- Inventory of all installed software packages on the workload
  - This includes versions and distributor information
- Takes a periodic snapshot of the installed software and sends it to Secure Workload

Secure Workload Software Agents

Deep Visibility and Enforcement

- Deep visibility agent
  - Capture and analyze all the packets using libpcap/winpcap
  - Gather processes information (PID, command, owner, …) to match with flows / sockets ownership
  - Windows / Linux / AIX
- Enforcement agent
  - Enforce policies using servers' local firewall
  - Fully manages IPtables / Windows Advanced Firewall – Windows Filtering Platform
  - Windows / Linux / AIX

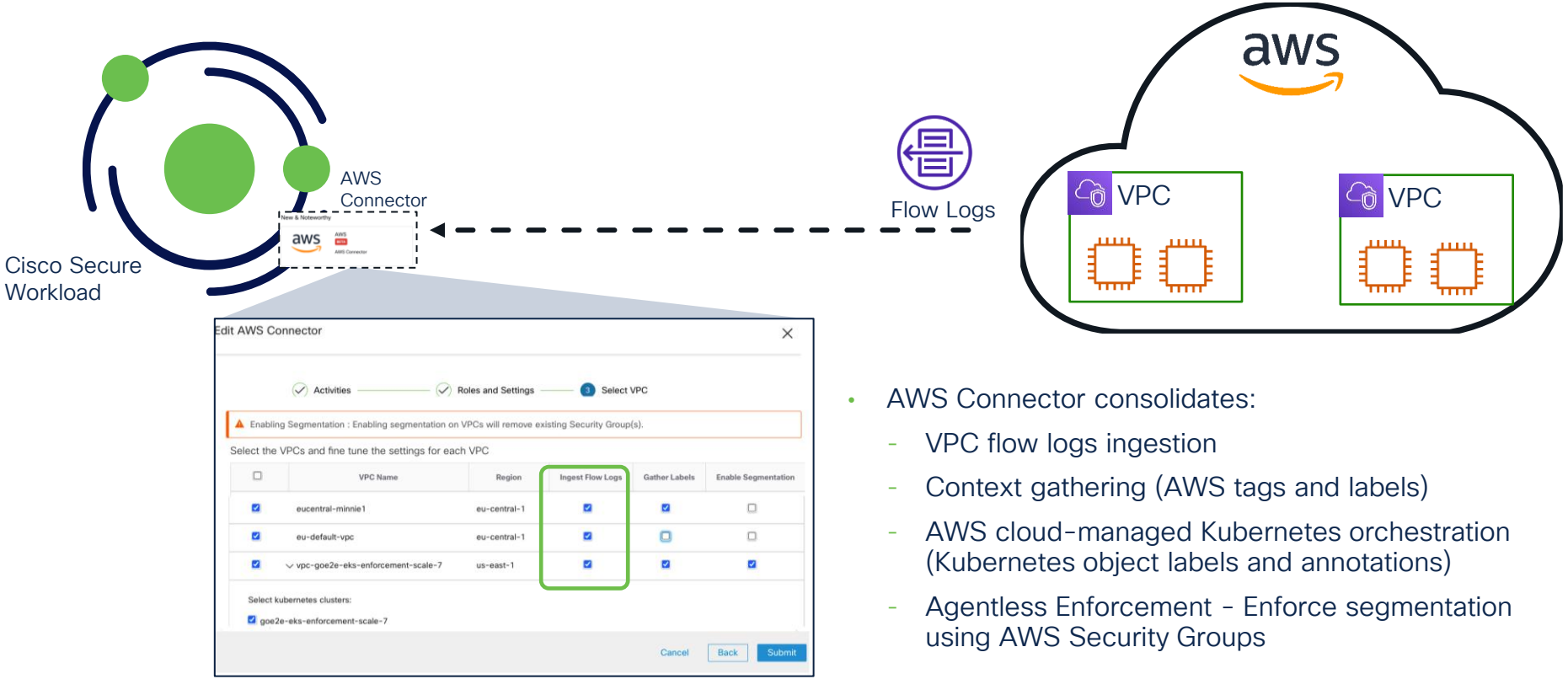
Cisco Secure Workload Network-Based Sources



Network-Based Telemetry Features

- Augment telemetry from other parts of the network
- NAT-Flow stitching (NetFlow, IPFIX, NSEL)
- Application Dependency Mapping

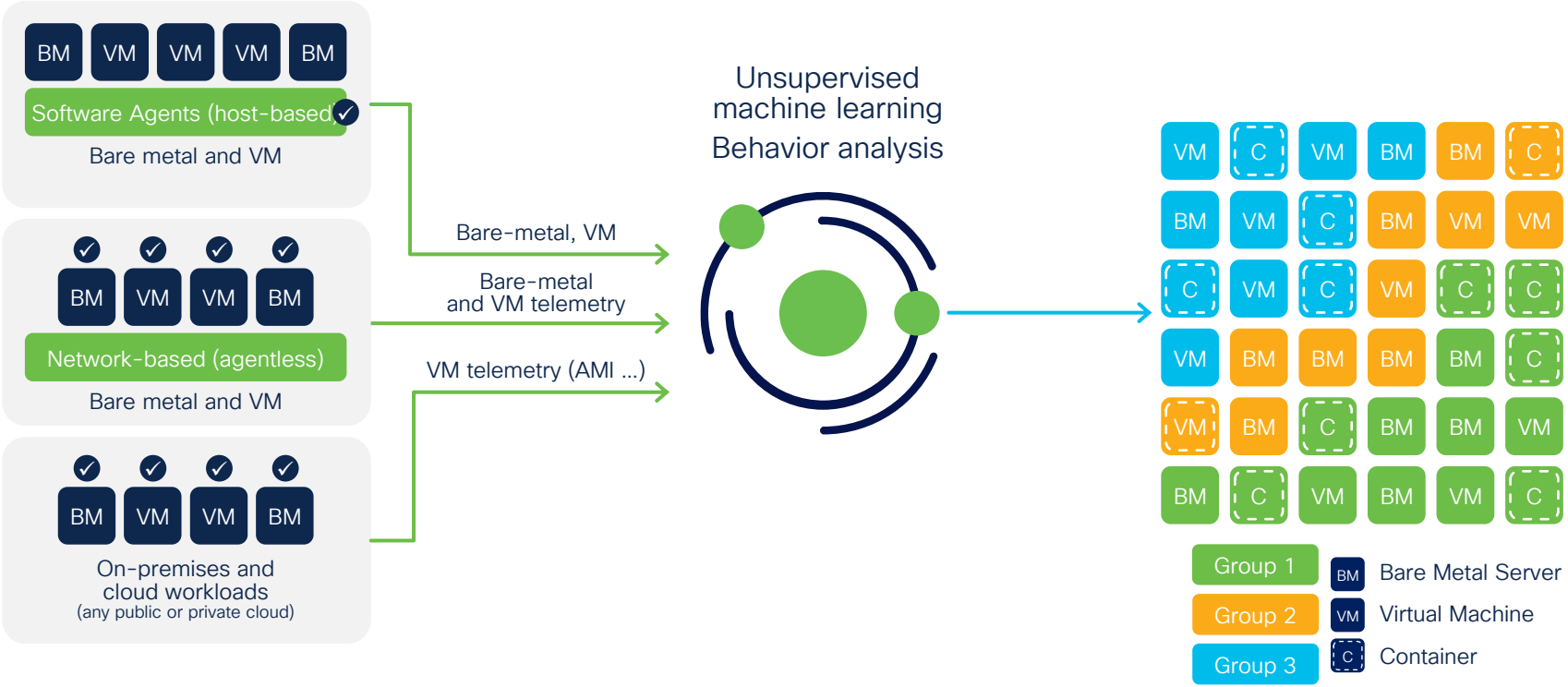
Cisco Secure Workload Cloud-Based Sources



- AWS Connector consolidates:
  - VPC flow logs ingestion
  - Context gathering (AWS tags and labels)
  - AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)
  - Agentless Enforcement - Enforce segmentation using AWS Security Groups

Secure Workload Application Dependency Mapping

Application Dependency Mapping and Cluster Grouping

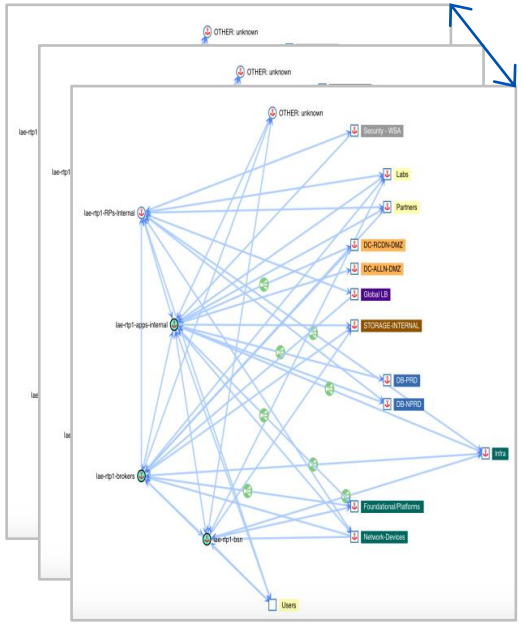


Security Policy for Segmentation

Baseline workload protection posture

- Process behavior
- Application Insights
- Network communications

Application workspaces



Baseline policy

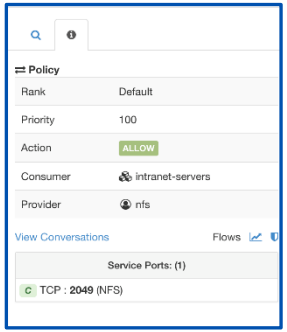
Priority	Action	Consumer	Provider	Services
100	ALLOW	commerce-servers	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	intranet-servers	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	cache	Tetration Sensor VIP	TCP : 443 (HTTPS)
100	ALLOW	commerce-servers	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	intranet-servers	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	cache	Tetration Collectors	TCP : 5660 (Tetration Enforcement)
100	ALLOW	commerce-servers	db	TCP : 3306 (MySQL)
100	ALLOW	intranet-servers	db	TCP : 3306 (MySQL)
100	ALLOW	commerce-servers	nfs	TCP : 2049 (NFS)
100	ALLOW	intranet-servers	nfs	TCP : 2049 (NFS)
100	ALLOW	intranet-servers	DNS	UDP : 53 (DNS)
100	ALLOW	commerce-servers	NTP	UDP : 123 (NTP)
100	ALLOW	intranet-servers	NTP	UDP : 123 (NTP)
100	ALLOW	cache	NTP	UDP : 123 (NTP)
100	ALLOW	snip	commerce-servers	TCP : 80 (HTTP)

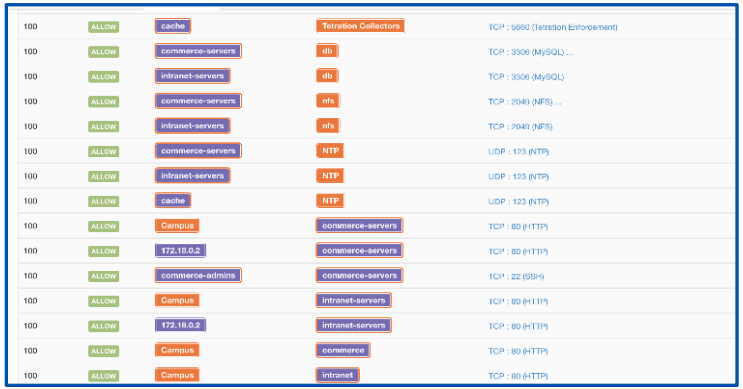
Auto Generated Segmentation Policy

Automatically generated policy based on application behavior:

- Using an application dependency map as a blueprint, Secure Workload automatically generates the micro-segmentation policy
- This policy allows the required traffic between the application components and infrastructure elements (DNS, NFS, NTP, etc.)
- The default catch-all policy is ”deny,” which can be changed to “allow” during the initial stages of enforcement to gain more confidence

NOTE: With a default catch-all of ”allow,” Secure Workload still detects policy compliance violations and alerts on them

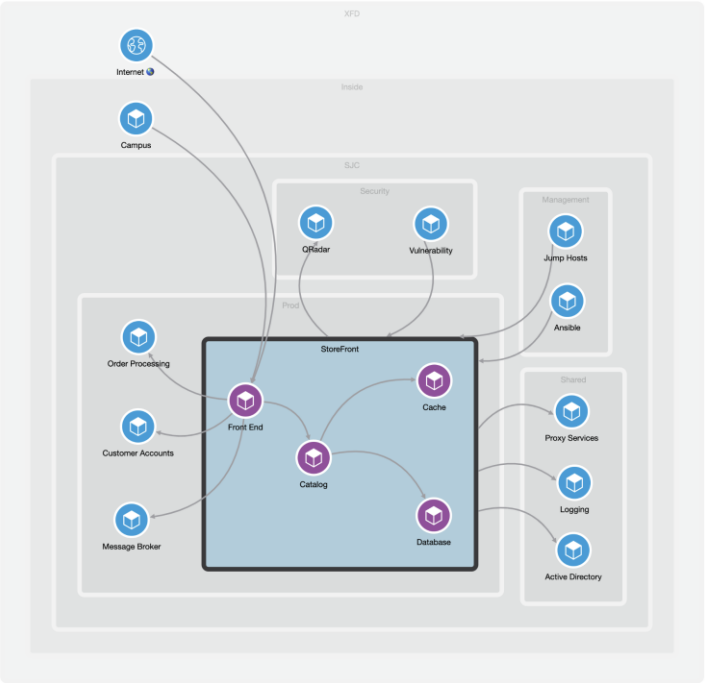




Relationship Among Application Components

Secure Workload provides the blueprint for communication dependencies between application components as well as other IT services

- How are the different application tiers communicating?
- Are there direct connections coming to database servers?
- Which communication is going through load balancers?
- How are users connecting to the application?
- Are there connections going out that should not be allowed? For example, a production database talking to a nonproduction database?



Defining a Context-Based Inventory

10.8.3.5

Owner	Acme Finance
Type	App
Service	Retail Banking
App	Invest
Environment	Production
Location	AWS
Sensitivity	High
Zone	OOS

Direct integration for automated policy definition and control

Application Context

Regulatory Context

Security Context

User/Device Context

Assign Context to Workloads - Annotations

- Up to 32 customizable tags
- Used to add context (“human or identity”) attributes to items
- Enable creating inventory filters and scopes with higher precision and more flexibility
- Manual and automated ways to assign or import tags

Manual import from user-uploaded (CSV) files or via UI

Automated import via Connectors for Endpoints

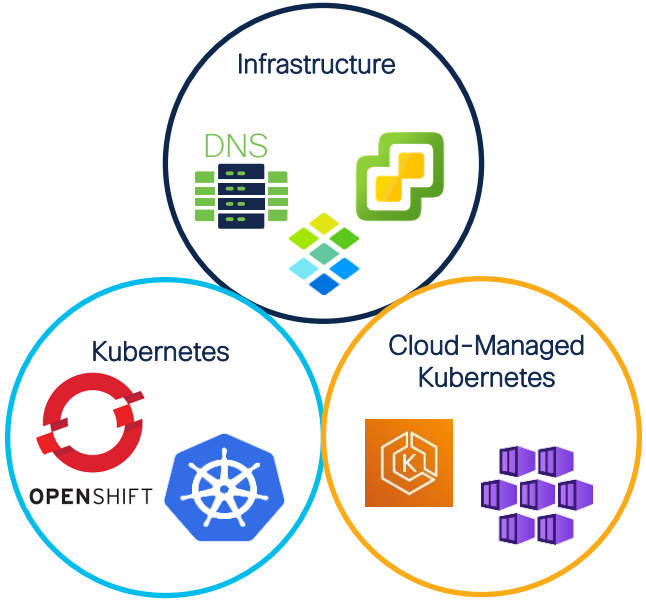
External Orchestrators dynamic import

Threat data-based annotations

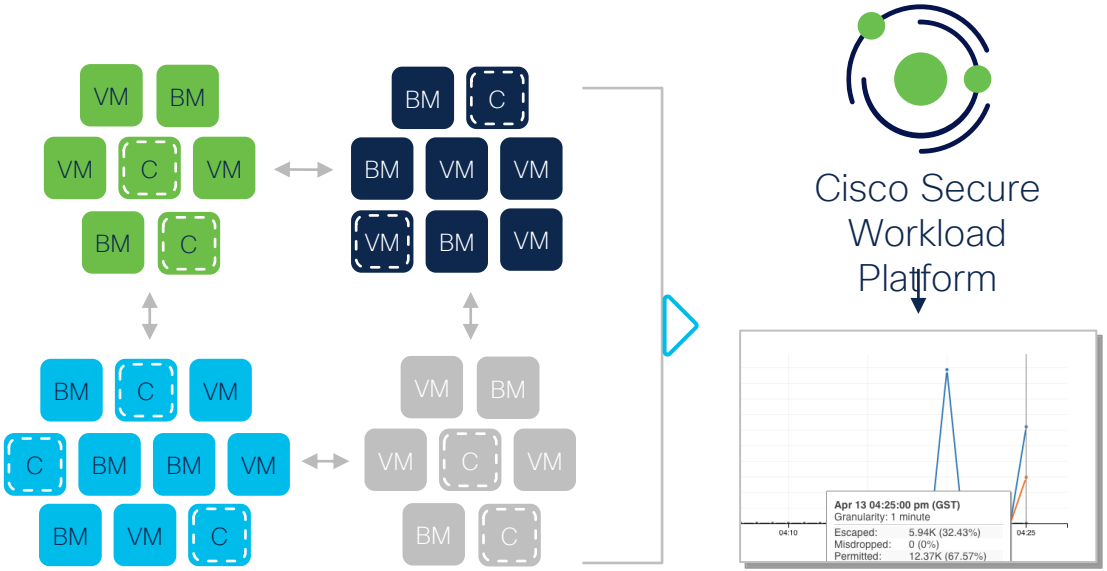
External Orchestrators - Annotations

Dynamically import attributes for your workloads

- Import attributes from infrastructure services
  - DNS Servers A/AAA and CNAME
  - VMware tags
  - Infoblox attributes
- Self-service and cloud-managed Kubernetes
  - System-define tags
  - Manifest-define tags



Real Time Policy Compliance

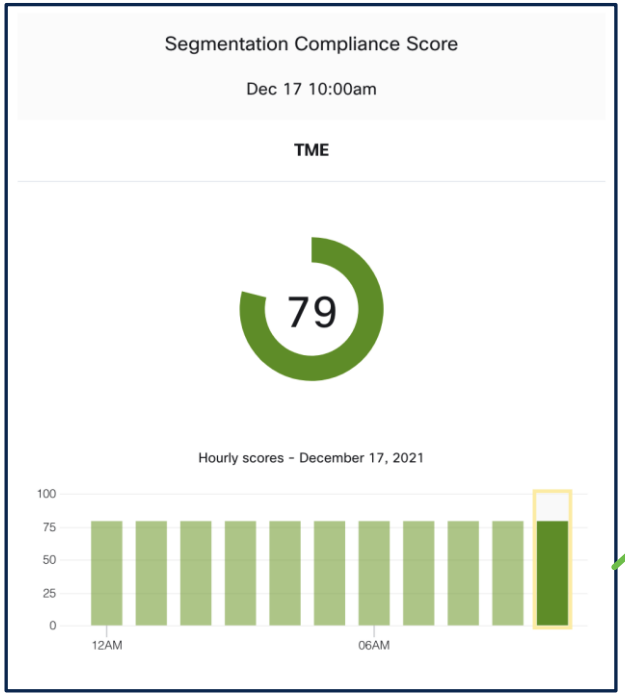


Identify policy deviations in real time

Review and update segmentation policy

Integrate noncompliance policy events with SIEM systems

Segmentation Compliance Score



Escaped	Rejected
42,844	1,542
Permitted	
386,300	

Secure Workload Segmentation and Policy Enforcement

Workload Policy Lifecycle Management

Security, Policy & Segmentation Regardless of Workload Location (Cloud, DC, CoLo)

1

Baseline workload protection posture

- Network communications
- Process behavior
- SW Vulnerabilities
- Application Insights

Baseline policy

2

Assess Impact

3

Merge intent from multiple stake holders

Unified policy

Enforcement

4

PUBLIC

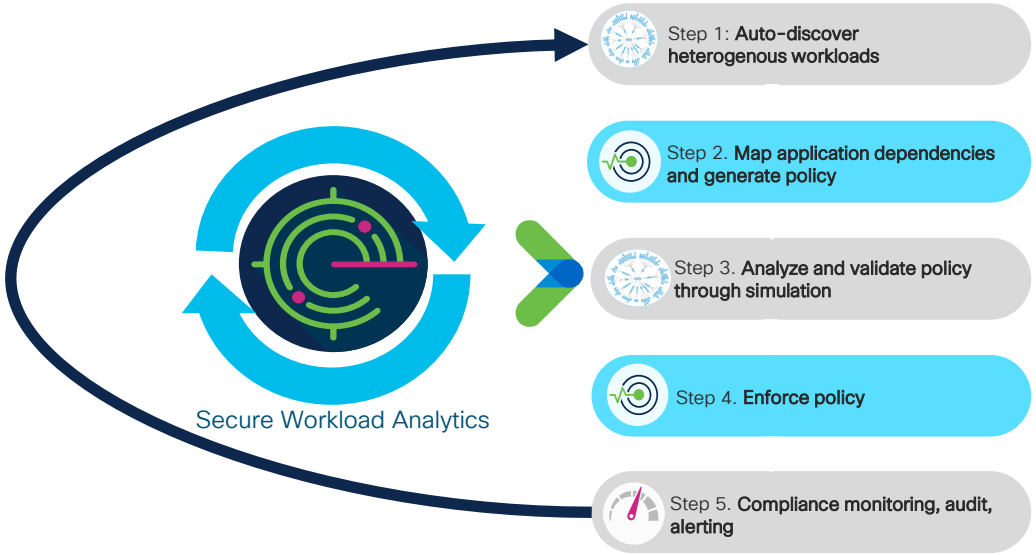
Compliance alerts

5

- Threat Intel
- Policy violations
- Risk Reports

Secure Applications Segmentation

Full Lifecycle Policy Discovery, Management and Enforcement



- Significant reduction in attack surface
- Faster time to value
- Significant reduction in security rule management
- Segmentation projects that don't last YEARS

Context Based Segmentation

Production workloads cannot talk to development workloads

Secure Workload knows which ones are production workloads and development workloads

Infosec administered and globally mandated policy intent. Users can define policies as allow-list, block-list or a combination of both

Policies are continuously updated as new servers are added, existing servers are moved, or IP addresses change

Production workload and development workload context is provided to Secure Workload through labels

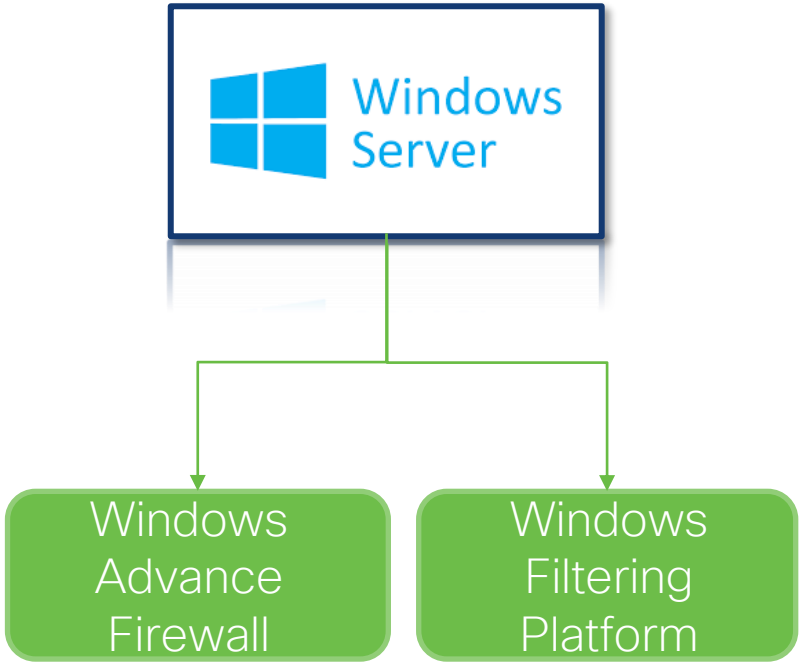
How Does Context Based Segmentation Work?

Secure Workload automatically converts your intent into allow-list and block-list

Intent		Rules
Block nonproduction applications from talking to production applications	✗	SOURCE 10.0.0.0/8 DEST 128.0.0.0/8
Allow HR applications to use the employee database	✓	SOURCE 128.0.10.0/24 DEST 128.0.11.0/24
Block all HTTP connections that are not destined for web servers	✓	SOURCE * DEST 128.0.100.0/24 PORT = 80
	✗	SOURCE * DEST * PORT = 80

Microsoft Windows Server – Enforcement

- Windows Server supports programming of firewall policies using one of the two approaches
  - Windows Advance Firewall
  - Windows Filtering Platform (WFP)
- Windows Advance Firewall uses WFP underneath to render and enforce the policies but has many drawbacks
  - Policy ordering (rendering of greylist)
  - Administrative controls (GPO, configuration dependencies, etc.)



Linux Server - Enforcement

- Using iptables

Priority	Action	Consumer	Provider	Protocol	Port	Confidence	Actions
100	ALLOW	... : DC-1 : Applications : Prod : Web Wordpress-01	Default : EMEAR : DC : DC-1	UDP	137 (NETBIOS Name Service)	Moderate	
100	ALLOW	... : DC-1 : Applications : Prod : Web Wordpress-01	... : DC-1 : Applications : Prod : Web Wordpress-01	TCP	3306 (MySQL)	Very High	

```
PolicyId=DEFAULT:100:ALLOW:61422e16497d4f4da4f0ed4f:615c7731755f020e367c51b0:6 */
ACCEPT     tcp  --  anywhere             anywhere             match-set ta_bf92c9f91e39691e301fc4ec0523 src
multiport dports mysql ctstate NEW,ESTABLISHED /*

PolicyId=DEFAULT:100:ALLOW:615c7731755f020e367c51b0:615c7731755f020e367c51b0:6 */
ACCEPT     udp  --  anywhere             anywhere             match-set ta_bf92c9f91e39691e301fc4ec0523 src
multiport dports netbios-ns ctstate NEW,ESTABLISHED /*
```

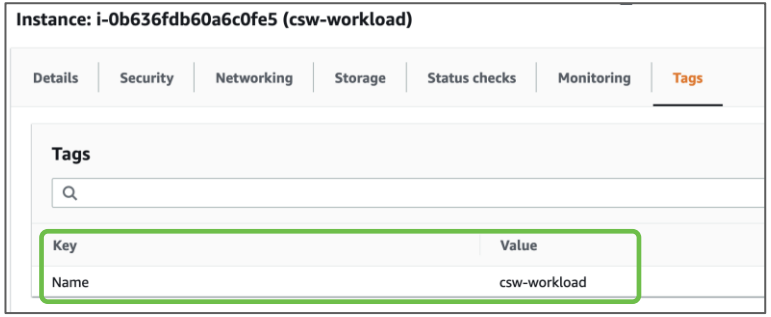
AWS Secure Connector

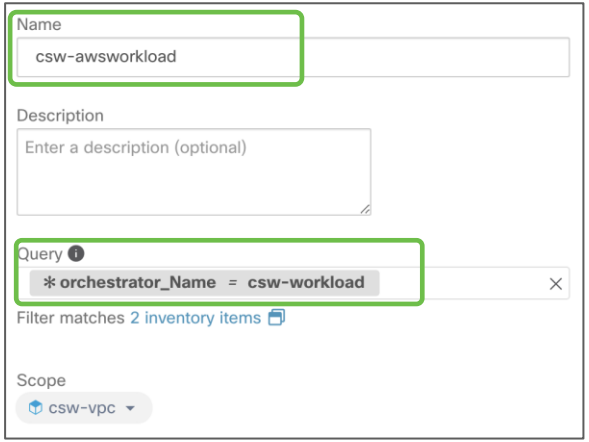
- Agentless workload enforcement through AWS Security Groups
  - Existing Security Groups will be **replaced** when enforcement is enabled for a given VPC
- Create inventory filters based on AWS tags
- Analyze policies against the VPC flow log information to eliminate any unexpected allows/blocks.
- AWS workloads matching the inventory filters are assigned with required AWS Security Groups depending on the defined segmentation policies.

Policy Lifecycle: Cloud Workloads

How it Works

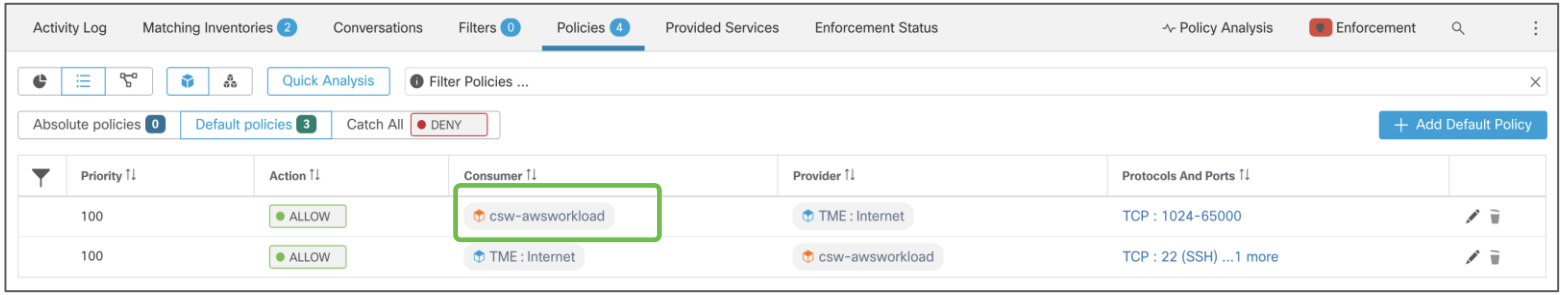
1 AWS workload with AWS tags





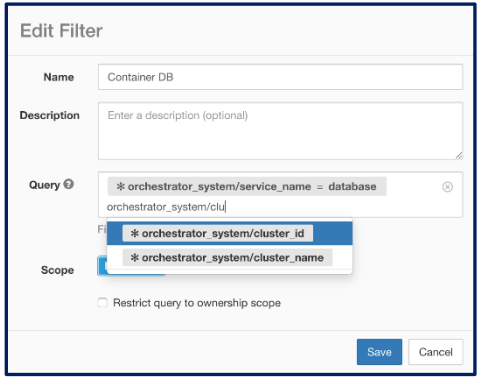
2 Inventory filter query matching the AWS tags

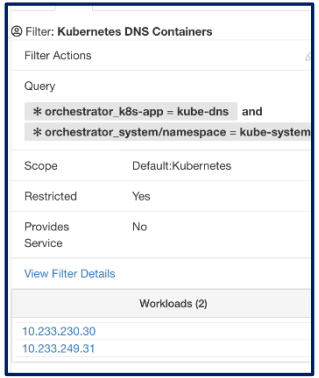
3 Segmentation Policies with inventory filter



Container Policy Definitions

- Inventory filters are defined based on the Kubernetes object names and labels (pod names, service names, etc.)
- Inventory filter that matches specified tag criteria will automatically get those policies when enforced
- If tag definitions match any higher-level policy definitions, such as InfoSec, container pods automatically inherit those policies





Priority	Action	Consumer	Provider	Services
100	ALLOW	F5 Controller	F5 Management IP	TCP : 443 (HTTPS)
100	ALLOW	Kubernetes Nodes	Kube BGP Peers	TCP : 179 (BGP)
100	ALLOW	Jenkins	Kube Masters	TCP : 6443
100	ALLOW	Default	Kubernetes Dashboard	TCP : 8443 (HTTPS)
100	ALLOW	Default : Kubernetes	Kubernetes DNS	UDP : 53 (DNS)
100	ALLOW	Kubernetes Nodes	Kubernetes DNS Containers	TCP : 8080 (HTTP) ...1 more
100	ALLOW	Kubernetes Nodes	Kubernetes Nodes	Any
100	ALLOW	Tetration	Kubernetes Nodes	TCP : 6443
100	ALLOW	Kubernetes DNS Containers	SJC15-174 Active Directory	TCP : 53 (DNS)

Breaking Down Silos

Security Architects

- Synchronized Security
- Policy enforcement on agents & network

DevSecOps

- Security at application speed
- Full Visibility & Automation

NetOps

- Full Visibility & Control
- Real time updates using dynamic objects

Auditors

- Single pane of glass view ensuring security controls across workloads & firewall

Cisco End-to-End Protections Bridges the Gap

North-South Security with
Cisco Secure Firewall
(formerly NGFW)

East-West Security with
Cisco Secure Firewall

Workload Security with
Cisco Secure Workload

Broad Visibility

- Secure Firewall at data center edge
- Visibility into Internet, branch, campus
- Attribute based policies

Coarse Control

- Segment within your data centers
- Handles workloads without agents
- Single/multi site public cloud
- Physical/virtual form factors

Fine-Grained Control

- Provides detailed inter-application controls, software-based
- Supports rapid automation

Closer to application

Secure Firewall and Secure Workload Integration

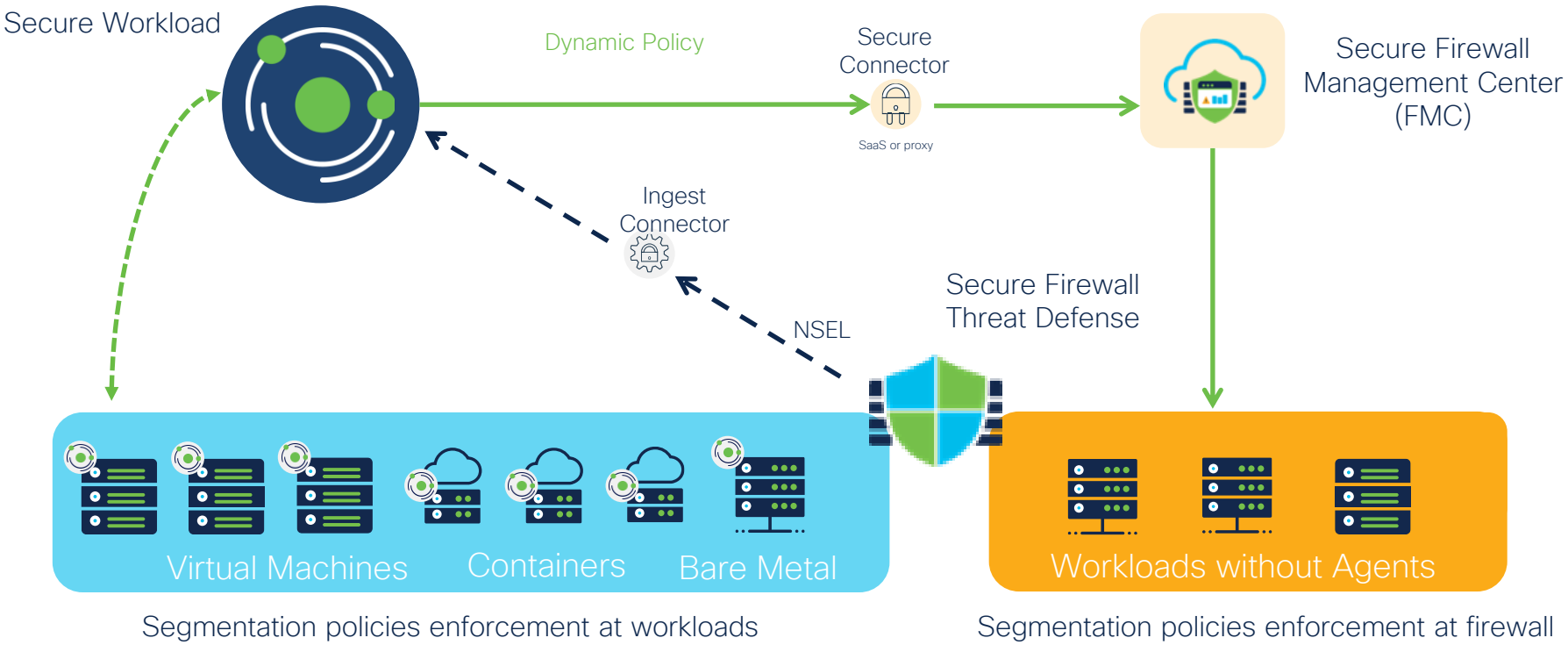
Key Functions

- Real time updates on rules using Dynamic objects without policy deployment
- Additional threat protection using Secure Firewall on existing Secure Workload policies
- Advanced access control options (intrusion and file/malware policy, URL filtering etc.)
- Fine grained policies from Secure Workload to implement contextual access-rules on firewall

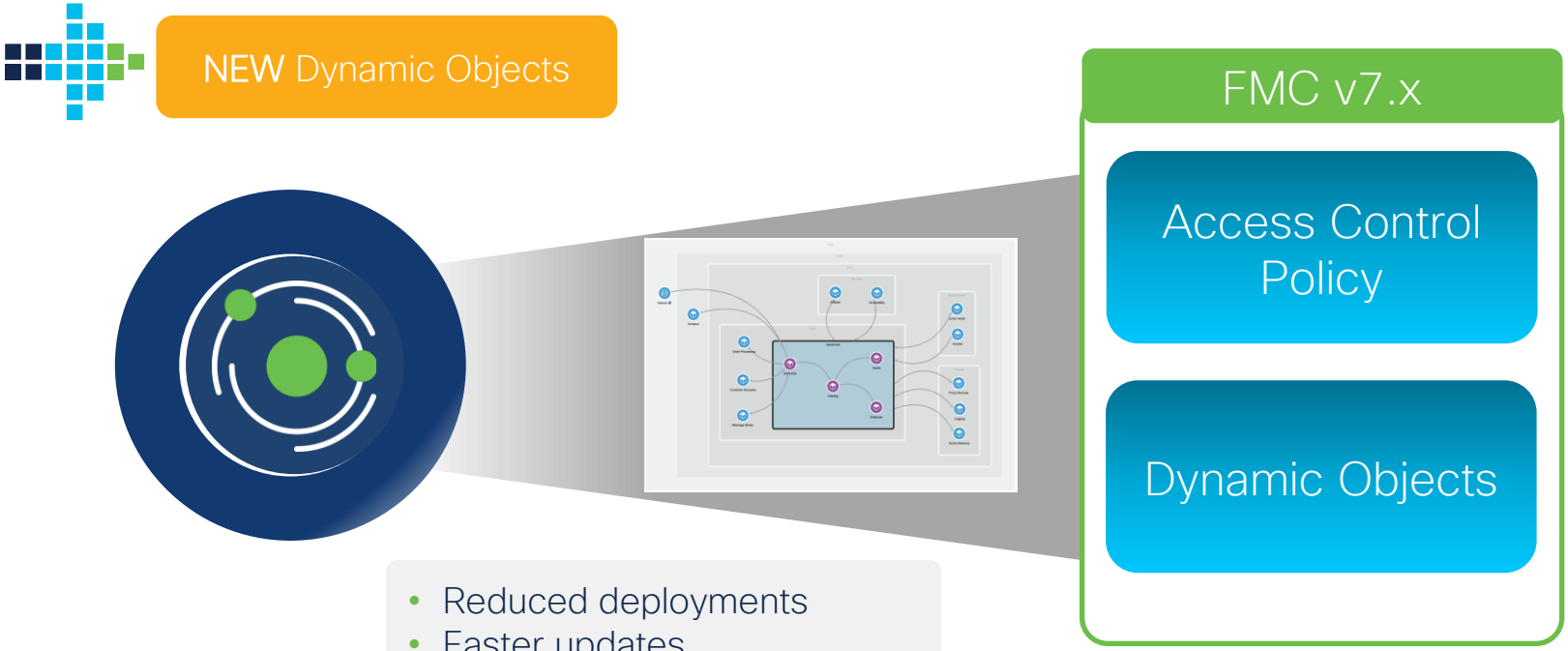
Key Capabilities

- Leveraging Secure Firewall for Policy enforcement on workloads without agents
- Enhancing static firewall rules with dynamic workload intelligence
- Ensuring security at application speed with constantly changing DevOps environment
- Automated firewall access-rule updates based on workload changes

Secure Firewall – High Level Architecture



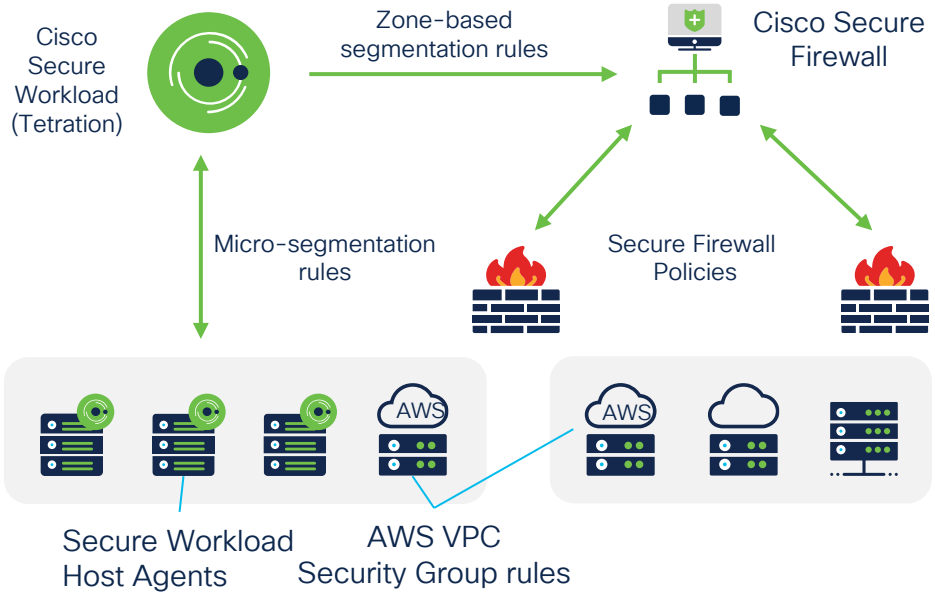
Dynamic Policy with Secure Firewall



- Reduced deployments
- Faster updates
- Greater efficiency

Cisco Secure Workload

Policy Control Across Secure Firewall and Cloud Providers



Seamless Integration
Unified segmentation policy across Secure Firewall & Secure Workload

Dynamic Policies
Policy updated dynamically based on application communications information

Expanding to Cloud Providers
Extending functionality to AWS security groups

Conclusion: Comprehensive Security Architecture

Unifying Segmentation for Defense in Depth

Edge Firewall

Secure Firewall

Macro-Segmentation

Secure Firewall

ACI

Micro-Segmentation

Secure Workload

Unified Segmentation

Deep Protection

- Threat inspection at the data center or cloud edge
- Visibility into Internet, Branch, and Campus

Zones

- Segment zones within your data center and cloud.
- Supplementary coverage for workloads without agents.

Zero Trust

- Zero trust micro-segmentation enforcement at the workload
- Automated policy discovery and compliance

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go