cisco Secure

零信任“微分段”技术在多云环境下的最佳实践

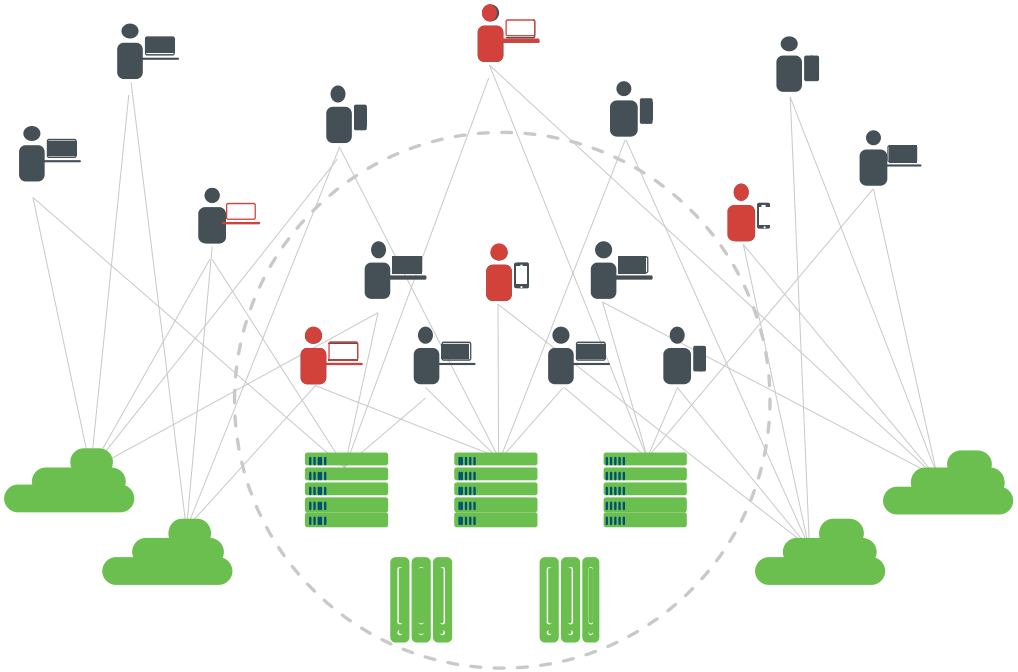
Cisco Tetration Solution

Robin Wei
TSA
Nov 10, 2020

Agenda

- 用零信任“微分段”技术保护多云应用
- 如何实现“微分段”保护
- “多云”微分段场景
- 总结

用户业务发展的新态势



应用发展的趋势

运行在任何环境——“多云”（传统、私有云、公有云）

动态适应业务要求——“敏捷”

每个应用的独特性——“个性”

用户业务向“多云”迁移道路上的“绊脚石”

- 数据中心的安全边界在哪里？
- 东西向访问如何监控和保护？
- “多云”环境下安全策略如何定义？
- 应用迁移的同时，安全策略是否自动随行？

零信任

零信任的效果是

无处不在的最小特权访问

(即授予访问权限，但使其具体化！)

零信任架构的发展历程

Jericho 论坛 | ZT 零信任 | BeyondCorp | ZTX 零信任扩展 | ZTA 零信任架构

2004 | 2010 | 2014 | 2017 | 今天

去边界化

一个国际化的企业CISO及供应商小组（思科举办了初始会议）

着力解决“去边界化”问题

早期成果：“需要建立信任”

出现多种模型

Forrester 提出“零信任 Zero Trust”，偏重于下一代防火墙(NGFW)

Google云的首个零信任架构 ---- BeyondCorp

Gartner’s Continuous Adaptive Risk and Trust Assessment

Forrester 的零信任拓展(Zero Trust eXtended)

广义

业界普遍接受“零信任架构”作为一般术语

客户兴趣

思科零信任架构下，“微分段”技术保护“多云”环境安全

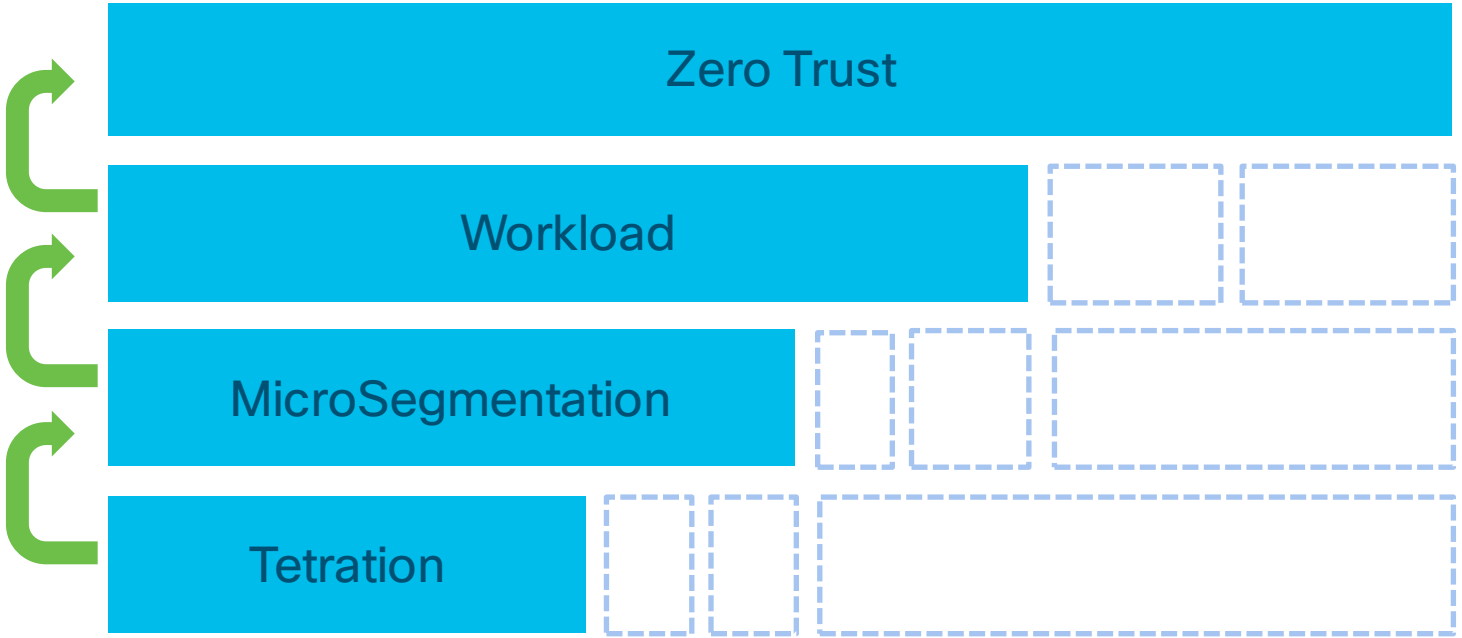
Tetration

“多云”数据中心微分段保护

应用访问的“最小”授权

分布式、“微”防火墙

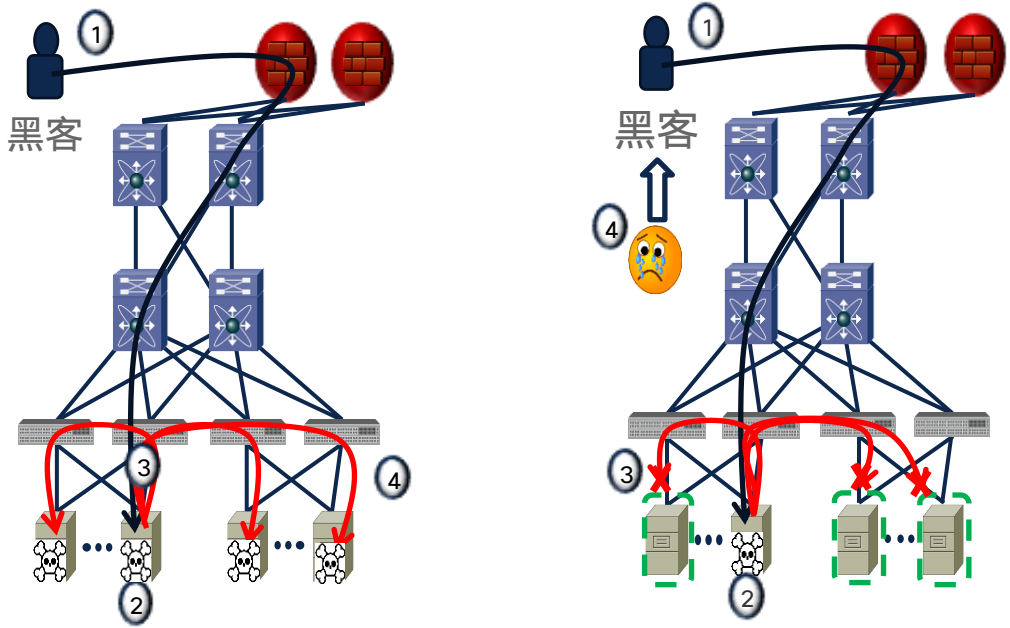
Tetration在零信任上的全局视角



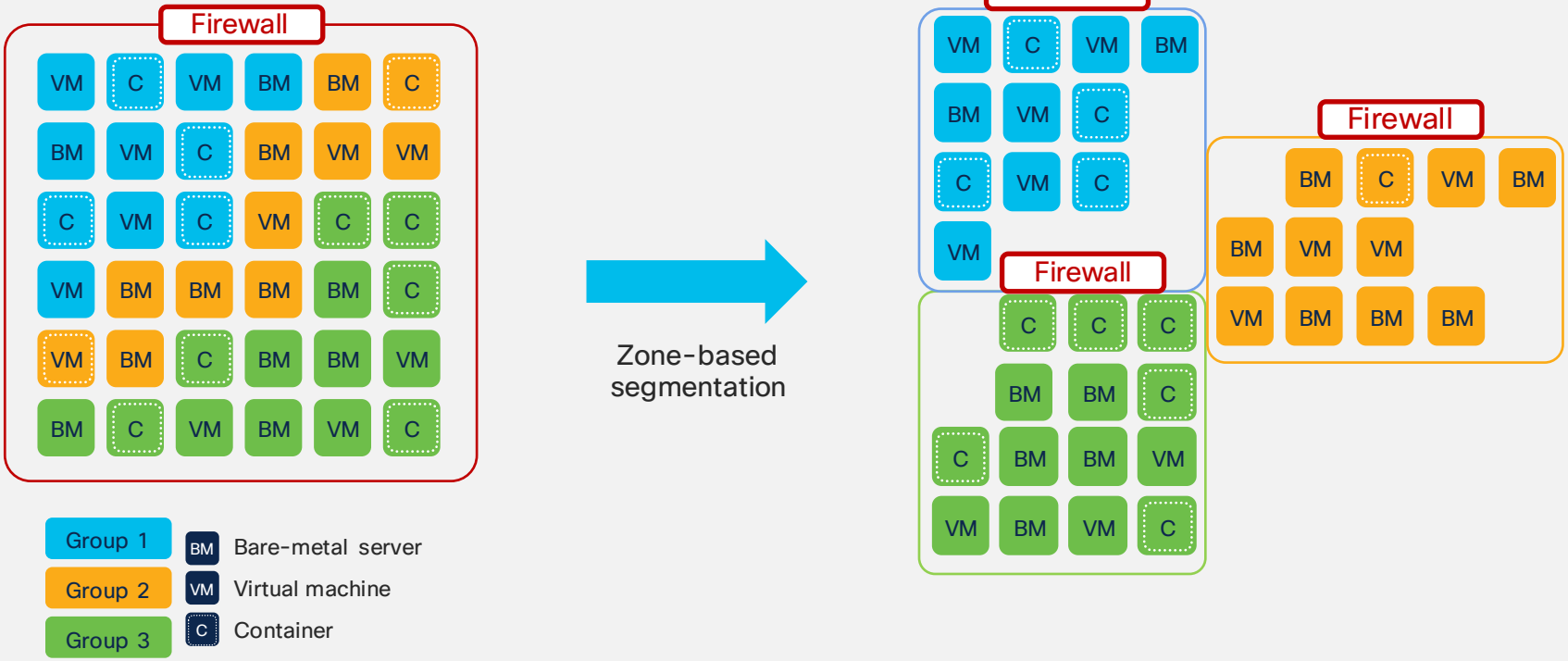
Agenda

- 用零信任“微分段”技术保护多云应用
- 如何实现“微分段”保护
- “多云”微分段场景
- 总结

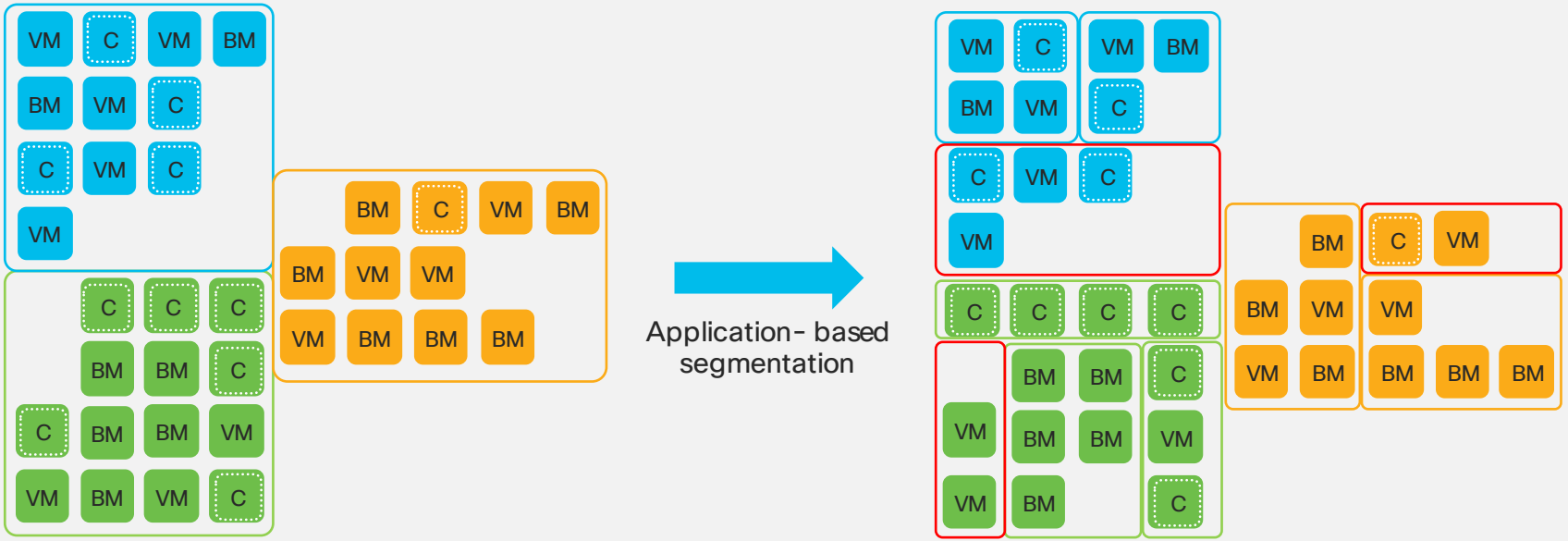
“微分段”保护的初衷



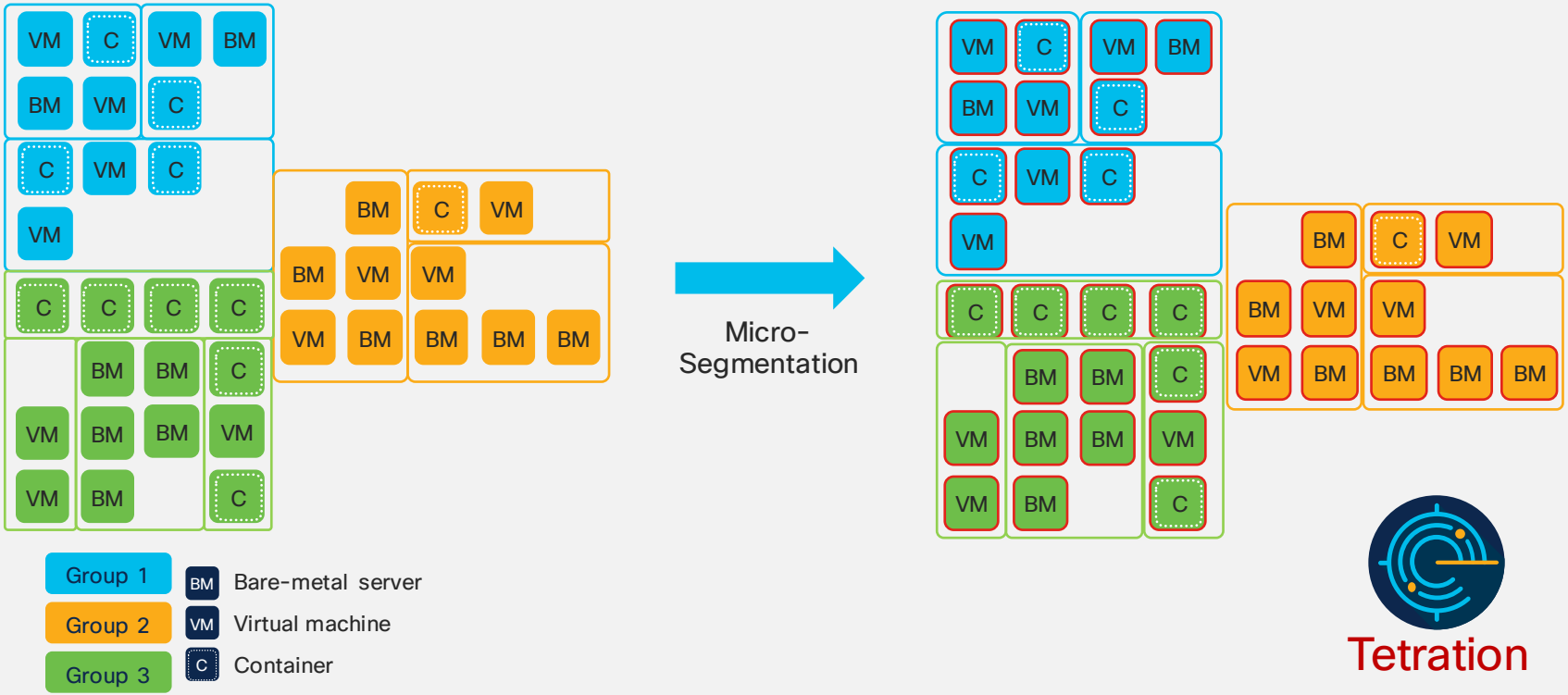
第一阶段：基于安全域的边界划分和保护



第二阶段：基于应用类型的边界划分和保护

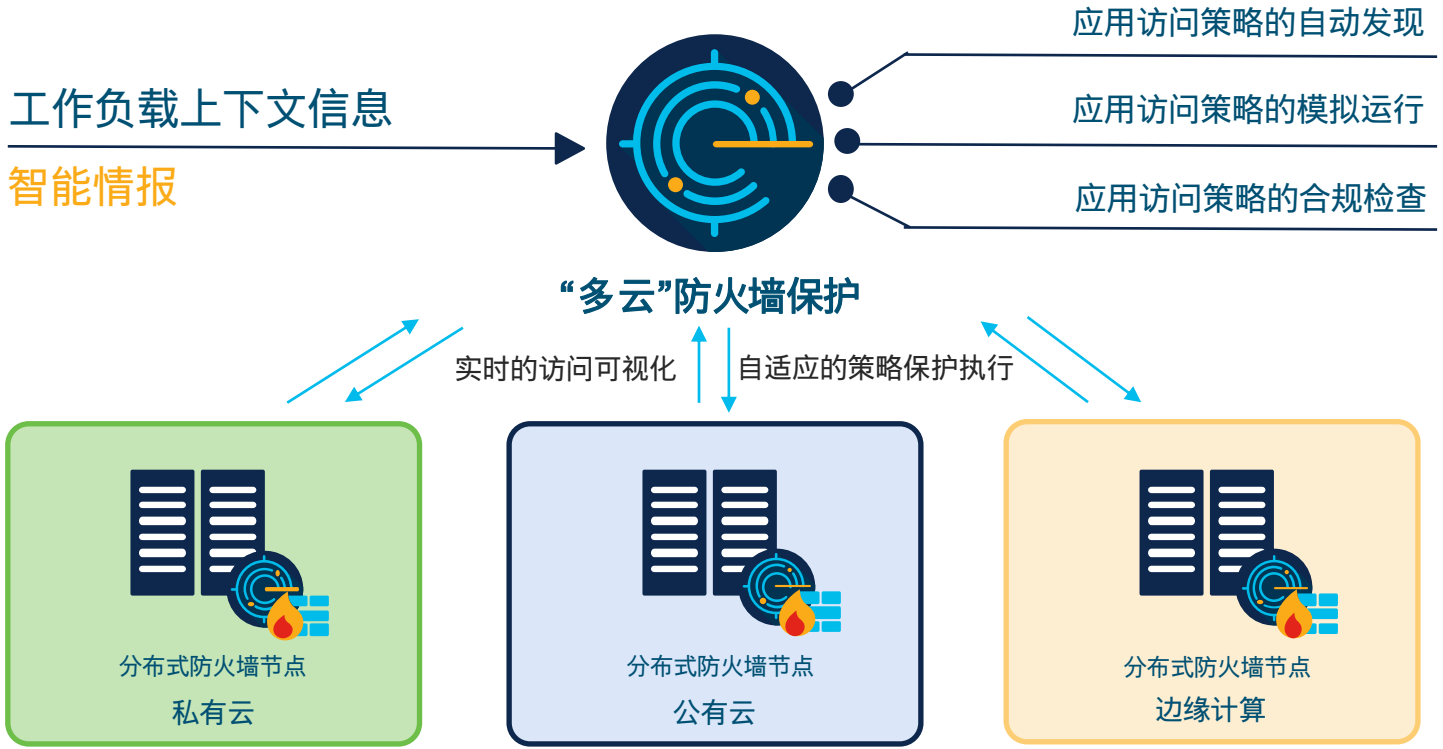


第三阶段：基于“微分段”的保护



Tetration“多云”微防火墙架构

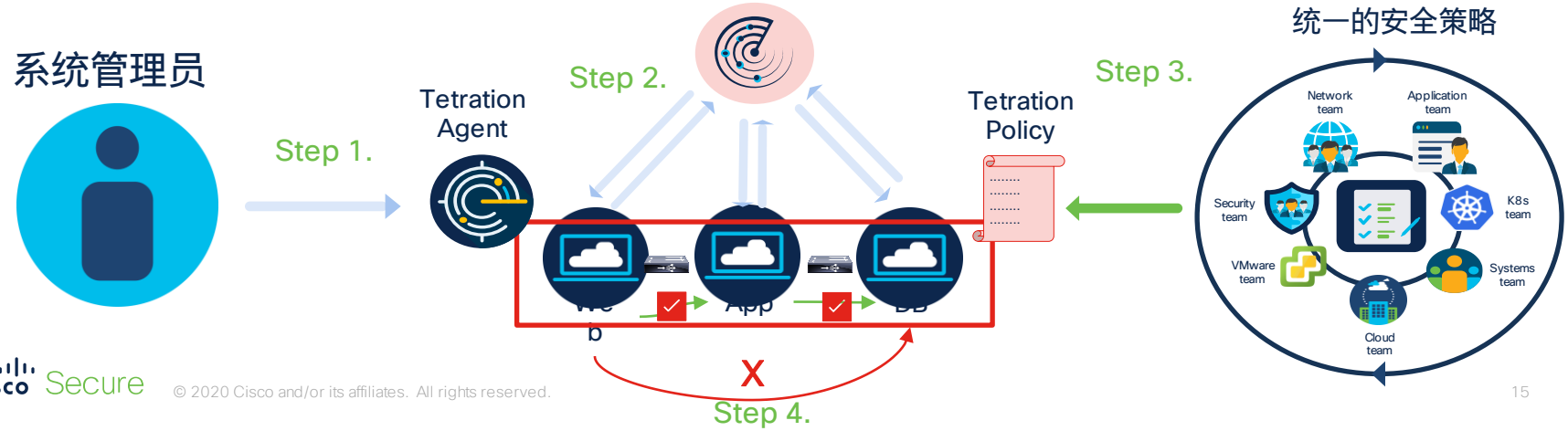
基于Agent，分布式，策略随行



Tetration“多云”防火墙让微分段的工作更轻松!

1.应用部门更新应用变更信息 → 2.应用部门填写防火墙策略申请表格 → 3.应用部门提交申请到网络安全部门 → 4.网络安全部门测试和下发安全策略 → 5.应用部门进行业务访问验证 → **6.安全策略自动发现和下发执行**

收集网络流和控制数据信息



Tetration工作负载微分段实现方法

一、收集数据，自动发现各种Workload和上下文属性

二、应用访问依赖关系自动识别

三、自动生成应用访问策略白名单

四、策略的自动模拟和验证

五、策略下发执行

六、持续策略合规与审计

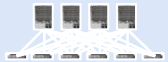
Tetration 策略生命周期-100%自动策略发现，管理与执行

跨异构基础架构的统一的策略实施

Public Cloud

Bare Metal

Virtual



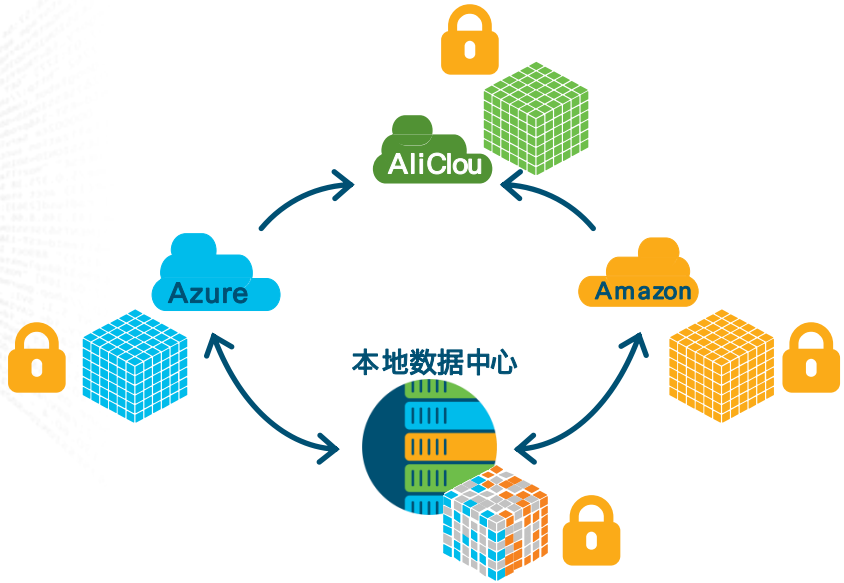
Cisco ACI*

Legacy Network*

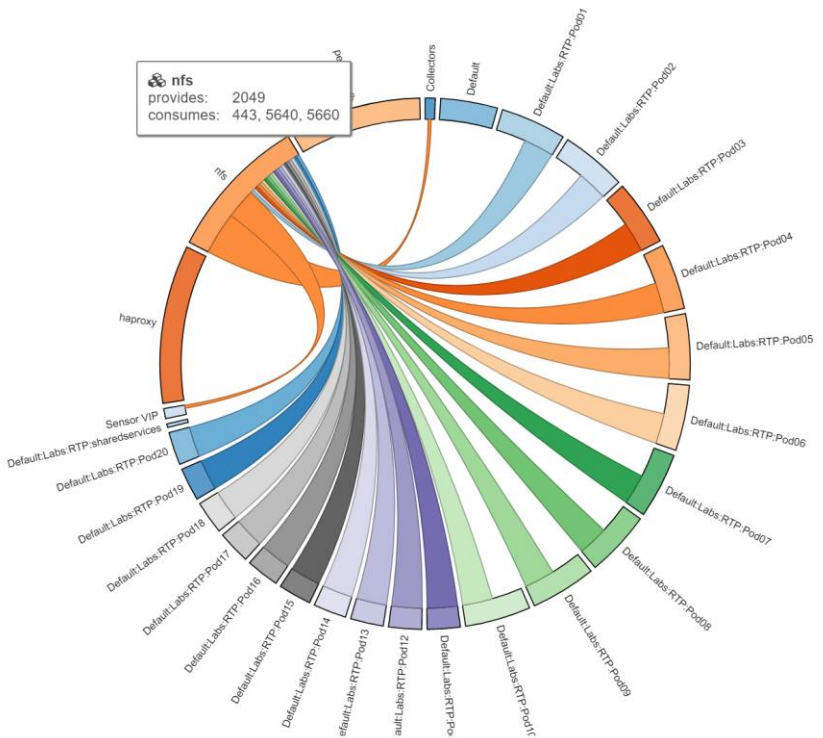
第一步：Tetration实现跨平台信息收集

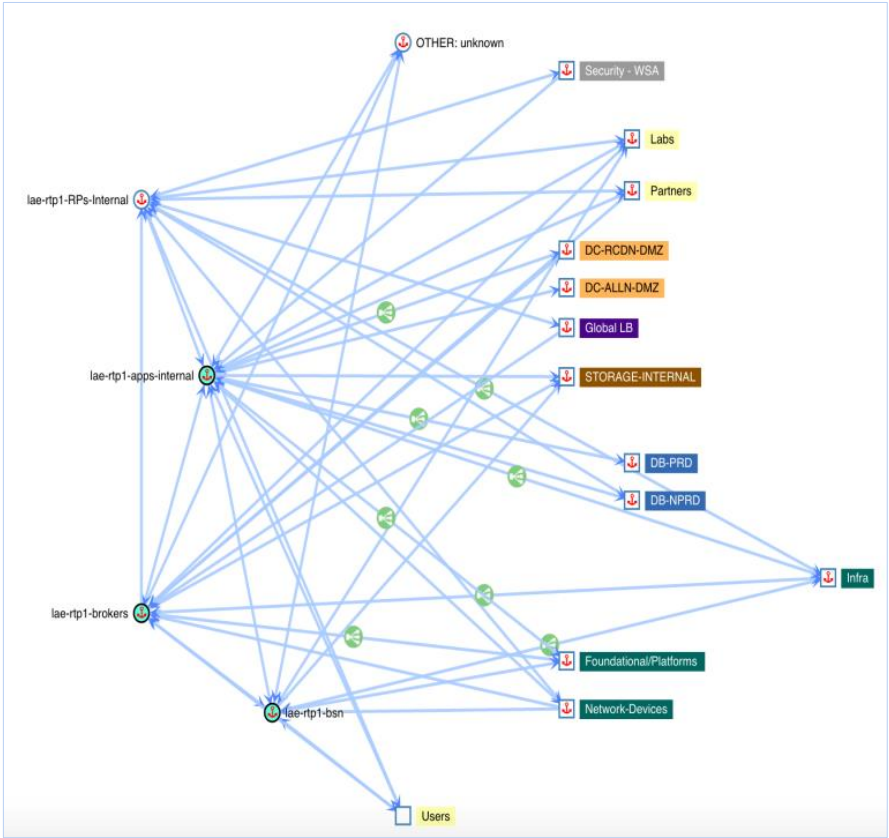
- 为每个工作负载安装Agent
- 收集工作负载的流量信息
- 收集工作负载的进程信息和软件信息
- 收集应用范围和分组信息
- 收集工作负载的上下文属性信息，例如：IP地址、主机名、所属应用、部门、用户等等
- Tetration对收集的所有信息进行上下文的关联、组织、呈现和管理。

Cisco Tetration Analytics



第二步：应用之间的访问依赖关系自动分析





第三步：自动生成应用访问策略白名单

Windows firewalls place DENY rules on top impacting the results below. See User Guide for more information.

Priority	Action	Consumer	Provider	Services
100	ALLOW	database	pod_108	UDP : 53 (DNS) ...
100	ALLOW	wkst1	pod_108	ICMP ...
100	ALLOW	load_balancer	pod_108	UDP : 53 (DNS) ...
100	ALLOW	webserver*	pod_108	UDP : 53 (DNS) ...
100	ALLOW	pod_108	database	UDP : 123 (NTP)
100	ALLOW	webserver*	database	TCP : 3306 (MySQL)
100	ALLOW	pod_108	wkst1	UDP : 137-138 ...
100	ALLOW	pod_108	load_balancer	TCP : 80 (HTTP) ...

Cluster: webserver*

Cluster Actions

Name webserver*

Description

View Cluster Details

Cluster细节 Very High

Edit Cluster Query

Endpoints (2)

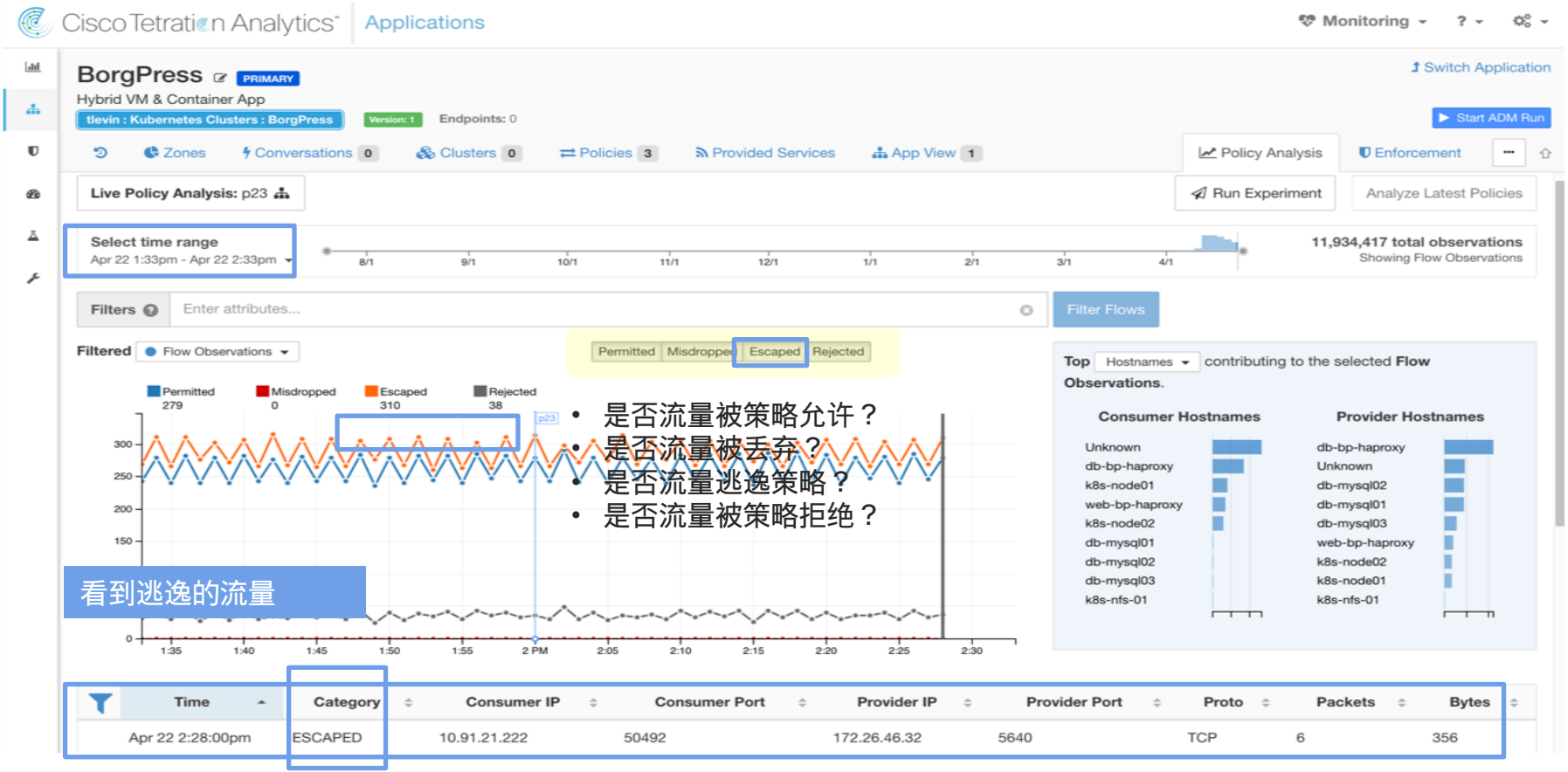
198.19.196.58	webserver1	CentOS...
198.19.196.59	webserver2	CentOS...

Neighbors (2)

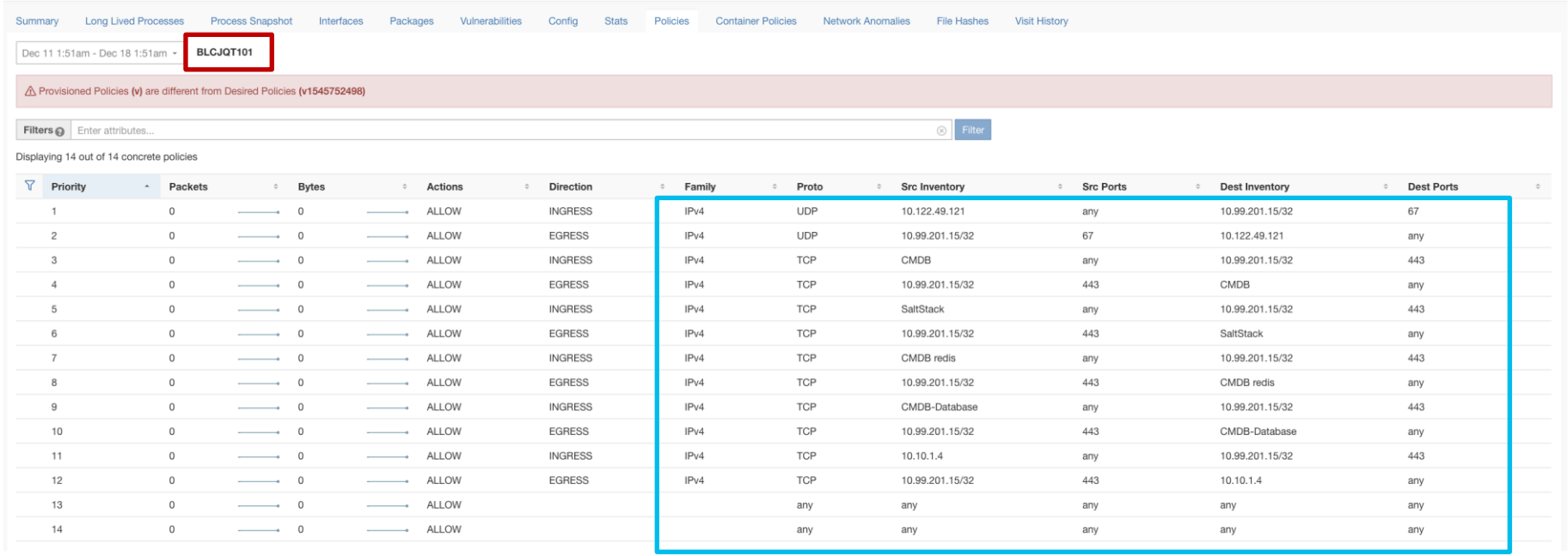
database
load_balancer

第四步：基于历史流量进行策略自动学习和分析

Policy simulation

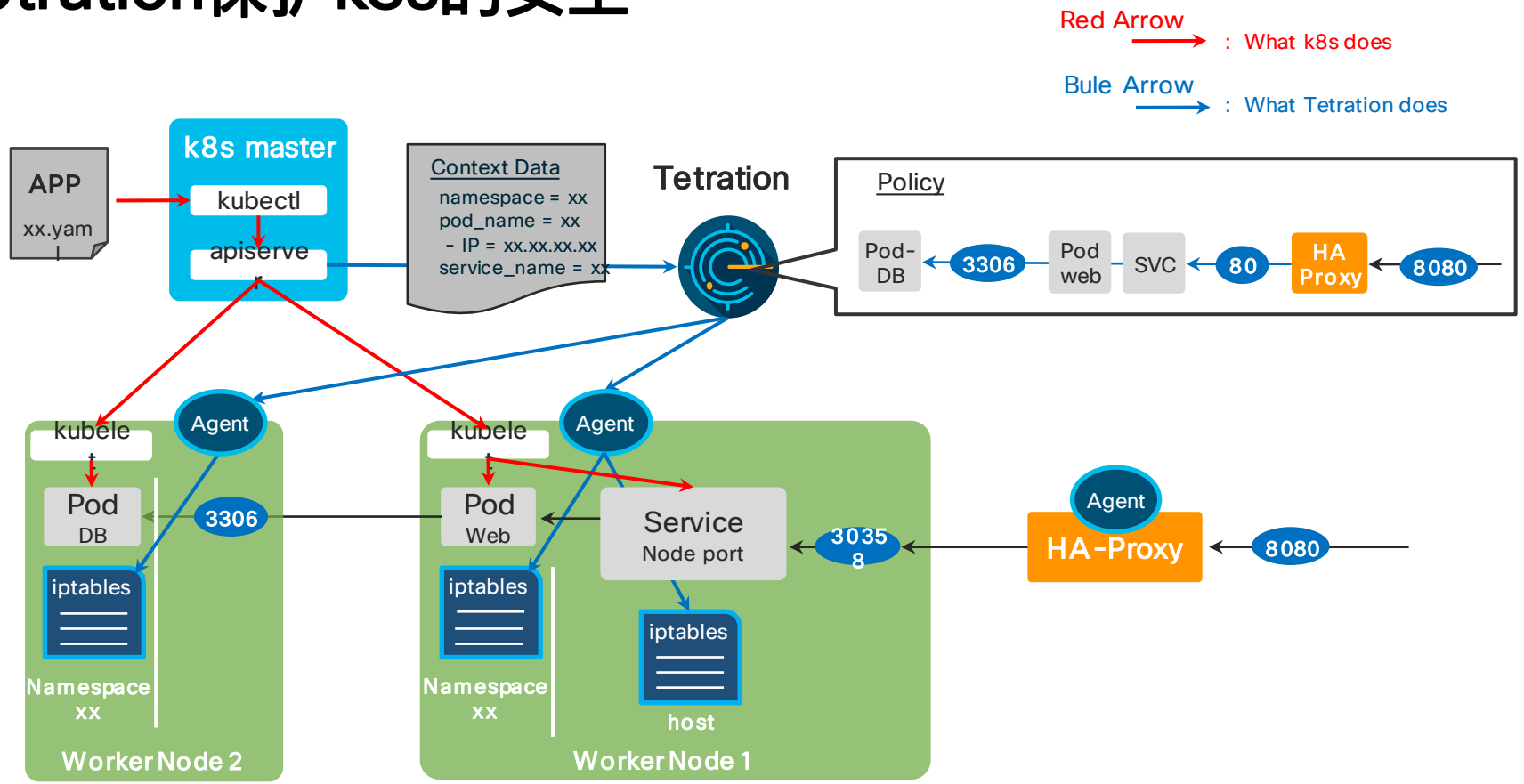


第五步：策略自动推送，并根据应用变化动态更新



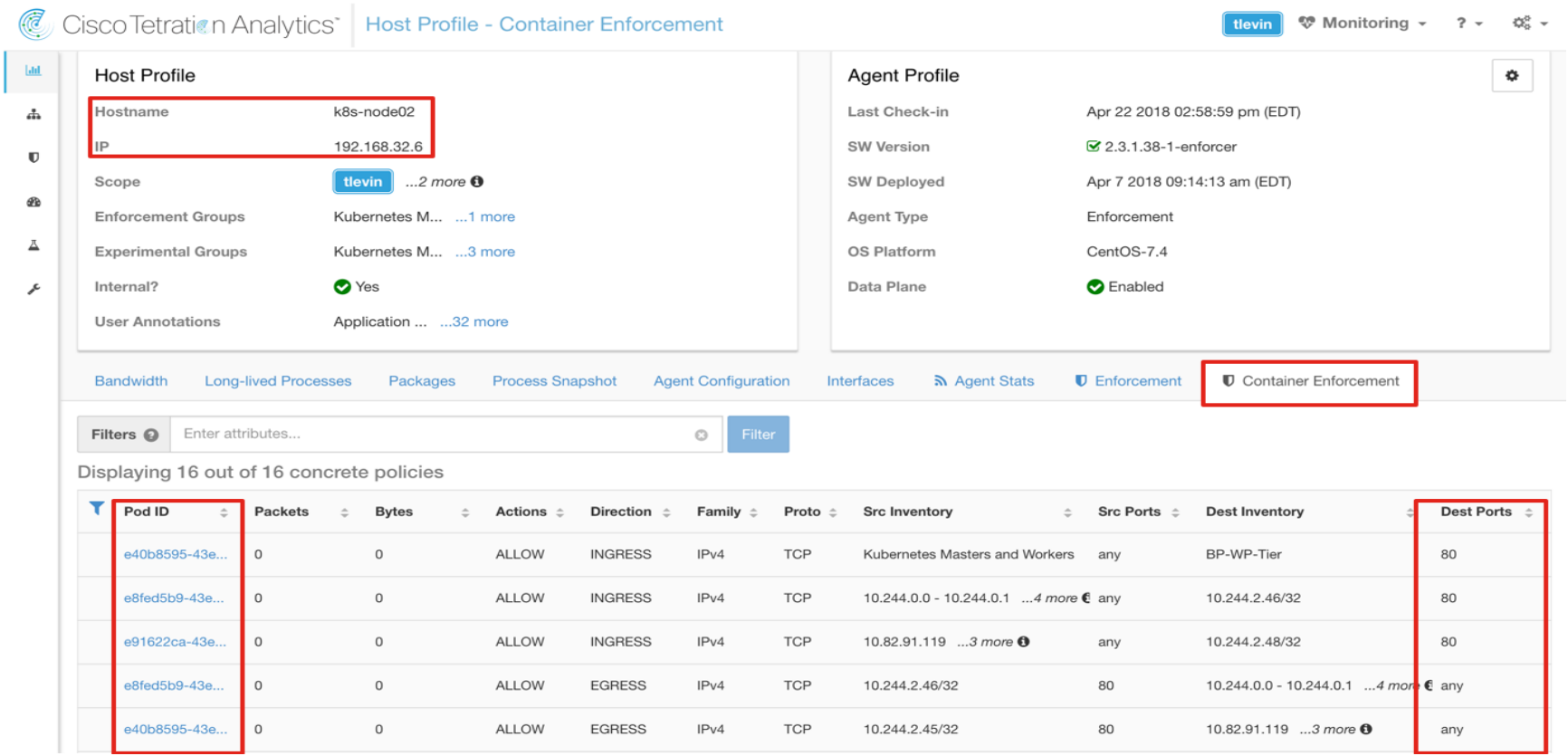
Priority	Packets	Bytes	Actions	Direction	Family	Proto	Src Inventory	Src Ports	Dest Inventory	Dest Ports
1	0	0	ALLOW	INGRESS	IPv4	UDP	10.122.49.121	any	10.99.201.15/32	67
2	0	0	ALLOW	EGRESS	IPv4	UDP	10.99.201.15/32	67	10.122.49.121	any
3	0	0	ALLOW	INGRESS	IPv4	TCP	CMDB	any	10.99.201.15/32	443
4	0	0	ALLOW	EGRESS	IPv4	TCP	10.99.201.15/32	443	CMDB	any
5	0	0	ALLOW	INGRESS	IPv4	TCP	SaltStack	any	10.99.201.15/32	443
6	0	0	ALLOW	EGRESS	IPv4	TCP	10.99.201.15/32	443	SaltStack	any
7	0	0	ALLOW	INGRESS	IPv4	TCP	CMDB redis	any	10.99.201.15/32	443
8	0	0	ALLOW	EGRESS	IPv4	TCP	10.99.201.15/32	443	CMDB redis	any
9	0	0	ALLOW	INGRESS	IPv4	TCP	CMDB-Database	any	10.99.201.15/32	443
10	0	0	ALLOW	EGRESS	IPv4	TCP	10.99.201.15/32	443	CMDB-Database	any
11	0	0	ALLOW	INGRESS	IPv4	TCP	10.10.1.4	any	10.99.201.15/32	443
12	0	0	ALLOW	EGRESS	IPv4	TCP	10.99.201.15/32	443	10.10.1.4	any
13	0	0	ALLOW			any	any	any	any	any
14	0	0	ALLOW			any	any	any	any	any

Tetration保护k8s的安全



K8S NODE上针对POD的Enforced Policy

Tetration container enforced rules - UI view



策略推送到Node上，自动更新iptables rule

Tetration enforced rules - endpoint view

```
[root@db-mysql01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
TA_GOLDEN_INPUT  all  --  0.0.0.0/0            0.0.0.0/0
TA_INPUT   all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
TA_GOLDEN_OUTPUT  all  --  0.0.0.0/0            0.0.0.0/0
TA_OUTPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain TA_GOLDEN_INPUT (1 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_b11a75d589e301459a6fb909ff60 src multiport sports 5660 ctstate ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_f5a83dd0cb816615ab0dd908e43e src multiport sports 5640 ctstate ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_61ce598c76a8d629f3a8288b461d src multiport sports 443 ctstate ESTABLISHED
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain TA_GOLDEN_OUTPUT (1 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_b11a75d589e301459a6fb909ff60 dst multiport dports 5660 ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_f5a83dd0cb816615ab0dd908e43e dst multiport dports 5640 ctstate NEW,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_61ce598c76a8d629f3a8288b461d dst multiport dports 443 ctstate NEW,ESTABLISHED
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain TA_INPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_45b71907aa0f113b331a5b9d86ea src match-set ta_6e21ff4fff7a628fb0fa9b4a8880 dst multiport dports 3306
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain TA_OUTPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_6e21ff4fff7a628fb0fa9b4a8880 src match-set ta_45b71907aa0f113b331a5b9d86ea dst multiport sports 3306
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

第六步、安全策略持续合规和审计

收集历史流量
分析策略的偏差情况

检查，审计和告警

策略生命周期管理

帮助运维人员优化策略

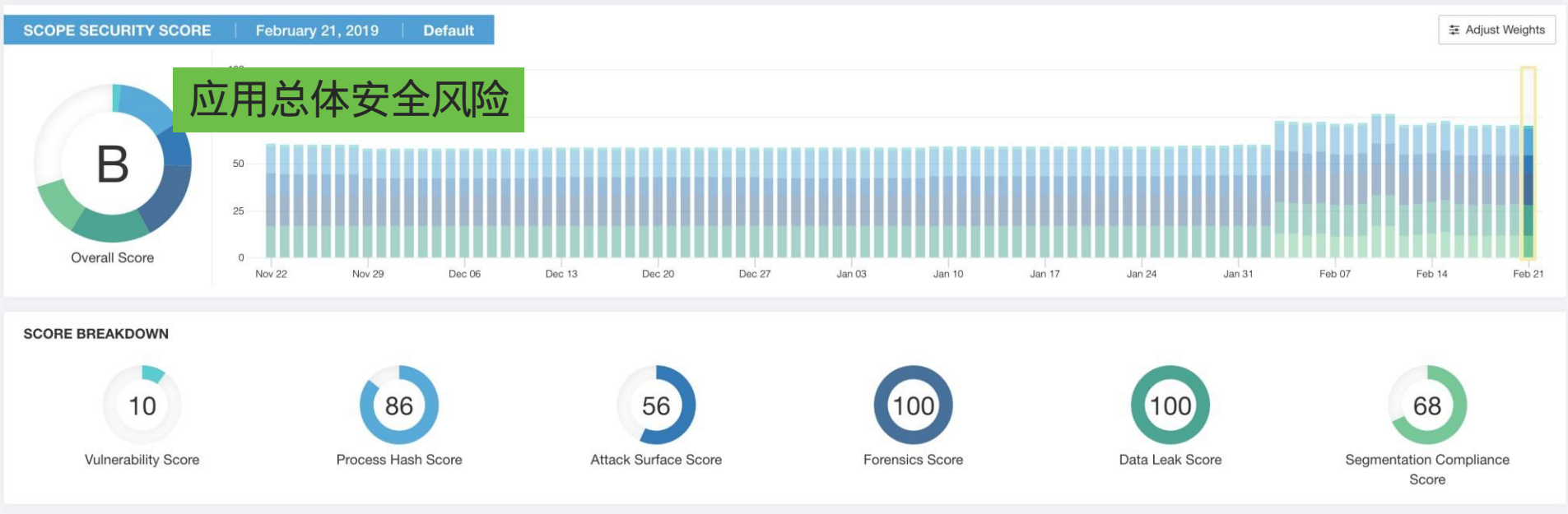
Jul 13 6:05:00am	PERMITTED	dbsrv-17-254	dbsrv-17-81	172.17.17.254	172.17.17.81	41402	4567	TCP

Jul 13 06:03:00 am (EDT)

	Consumer	Provider
Flags	PSH ACK	PSH ACK
ICMP Type and Code		
Byte Count	60,602 (483,726,466 so far)	63,242 (480,773,228 so far)
Packet Count	471 (3,821,569 so far)	511 (3,776,594 so far)
SRTT	10.6ms	
Process	/usr/sbin/mysqld --wsrep_start_position=84dc603a-c08c-11ea-a5b7-5e9d60b6d6fc:114	/usr/sbin/mysqld --wsrep-new-cluster --wsrep_start_position=84dc603a-c08c-11ea-a5b7-5e9d60b6d6fc:114
Drop Reason	N/A	N/A

我是否应该允许这个流量？

高级安全监控和保护功能



漏洞 | 文件哈希 | 攻击面 | 合规取证 | 流量异常 | 微分段审计

漏洞监控和管理

✻ Scope = PCI and OS *contains* Windows and (

Package CVE = CVE-2017-0146 or

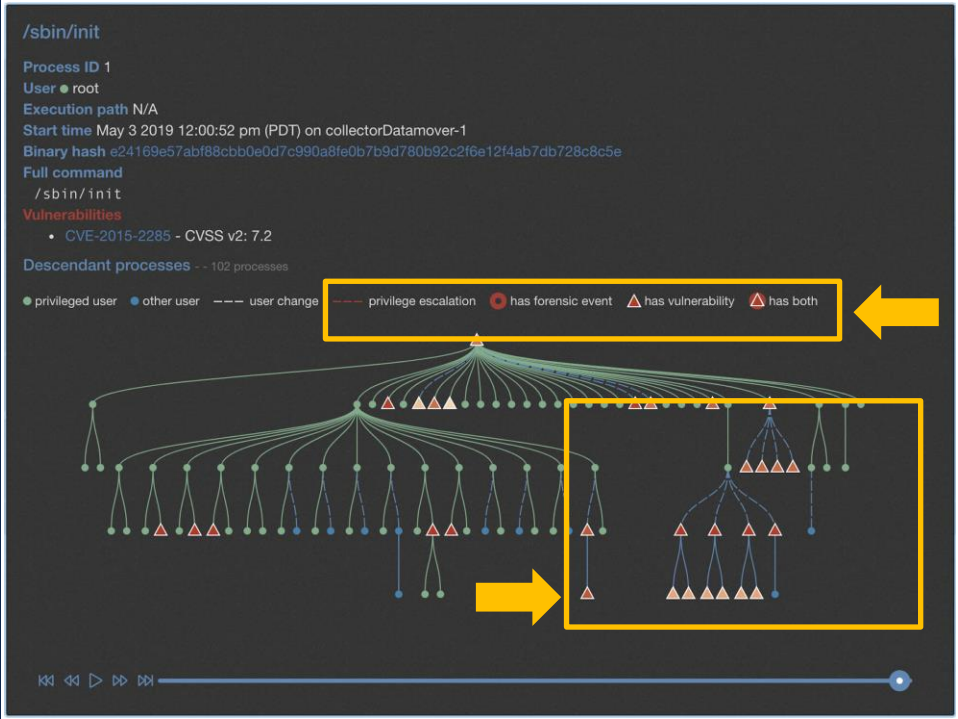
Package CVE = CVE-2017-0147)

阻断有“永恒之蓝”漏洞的机器，针对SMB445进、出的访问，避免WannaCry的攻击

DENY	Everything	PCI Susceptible to WannaCry	TCP: 445
DENY	PCI Susceptible to WannaCry	Everything	TCP: 445

进程快照、调用过程和攻击关联分析

- 进程Hash是否安全——安全情报关联分析
- 进程和有漏洞的软件关联
- 进程和“提权”操作关联
  - Privilege escalation
  - Shell-code execution
  - Side channel attack
  - Raw socket creation
  - User login activities
  - File access pattern
- 进程和异常活动关联
- 进程的调用和执行过程回放



Cisco Tetration Agent的支持和部署

软件Agent支持的系统（物理机，虚拟机，公有云和容器）

- Linux servers
  (virtual machine and bare metal)
- Windows servers
  (virtual machines and bare metal)
- IBM zSystems
  (z/Linux Operating System)
- IBM PowerPC and pSeries systems
  (AIX Operating System)
- Windows desktop VM
  (virtual desktop infrastructure only)
- Container host
  (Linux container host OS)

用户关注关键点:

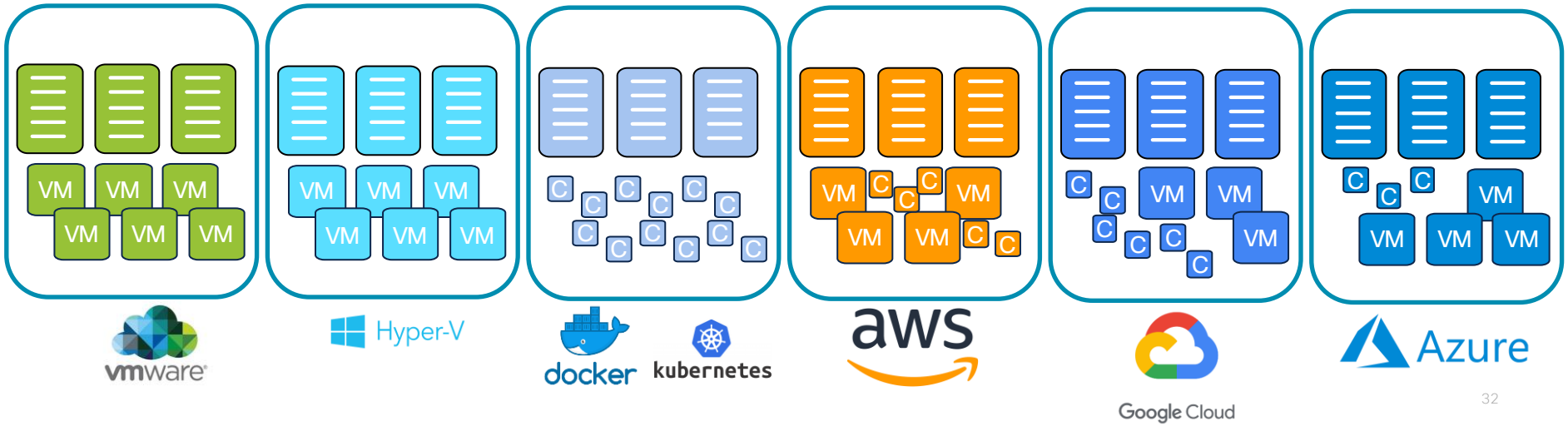
- 低CPU和内存占用率(可强制)
- 低网络资源占用率，采集每个访问数据流，不采集payload数据
- 利用操作系统底层防火墙引擎，稳定高效，自身高安全性，代码签名和授权

Agenda

- 用零信任“微分段”技术保护多云应用
- 如何实现“微分段”保护
- “多云”微分段场景
- 总结

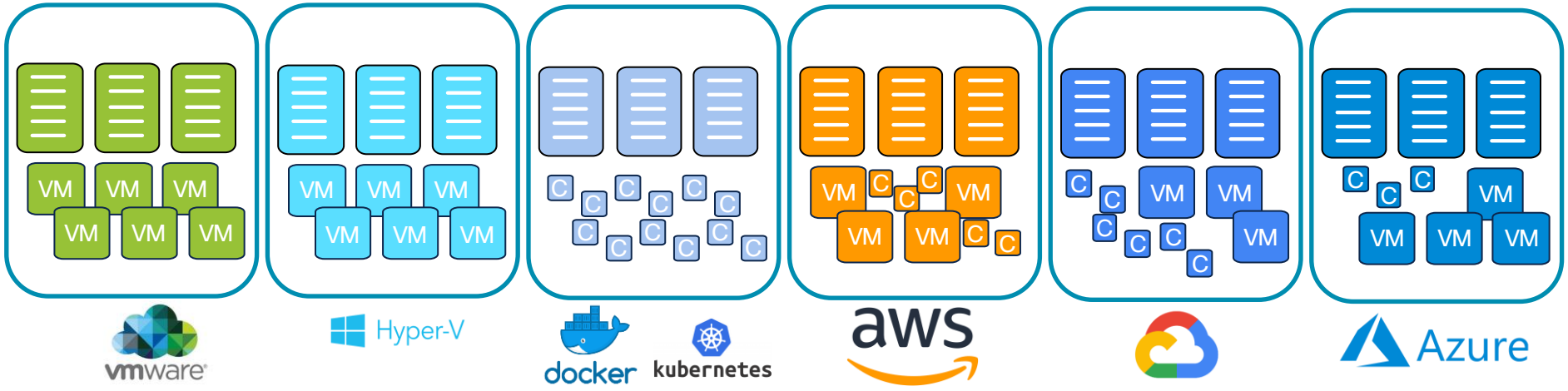
Tetration让“多云”微分段更简单

- 基于应用Scope/Group的动态策略
- 策略自动应用到每一个服务器，而不依赖于基础网络



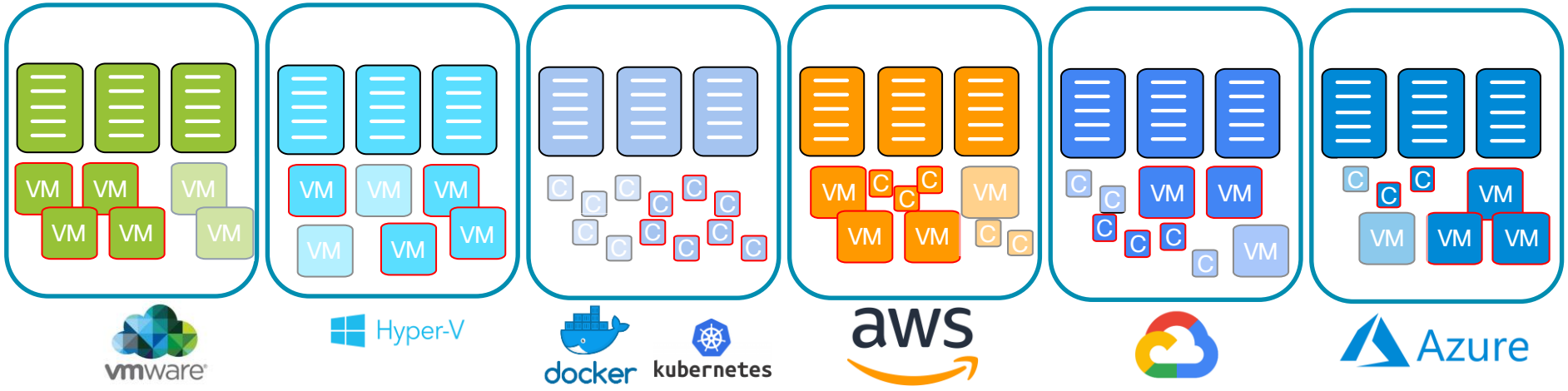
Tetration让“多云”微分段更简单

- 基于应用Scope/Group的动态策略
- 策略自动应用到每一个服务器，而不依赖于基础网络
- 例如: 生产环境不允许访问非生产环境



Tetration让“多云”微分段更简单

- 基于应用Scope/Group的动态策略
- 策略自动应用到每一个服务器，而不依赖于基础网络
- 例如: 生产环境不允许访问非生产环境



Agenda

- 用零信任“微分段”技术保护多云应用
- 如何实现“微分段”保护
- “多云”微分段场景
- 总结

Cisco Tetration保护“多云”业务的安全

跨越任何技术平台、任何基础架构和任何云，保护工作负载的安全

Key Takeaways

Tetration保护workload的安全，是思科“零信任”架构的重要组成部分。

应用“微分段（分布式“微”防火墙）”是Tetration的核心价值，策略自动化、一致性和业务随行。

Tetration适合“多云”环境微分段保护，保障业务快速、安全发展。


cisco
Secure