Cisco ASAv
技术决策制定者

Goran Saradzic
技术营销工程师

2013 年 11 月

免责声明

本演示中介绍的许多产品和功能处于不同的开发阶段，将在可用时提供。

思科可自行决定更改此路线图，并且对本文档中列出的任何产品或功能的交付延期或无法交付，思科概不负责。

今日新闻

思科将为下一代数据中心和云应用推出一款新的虚拟自适应安全设备。

思科将 ASA 软件发展为具有 REST API 和灵活许可的开放式架构。

今日新闻

- 数据中心趋势
- 数据中心安全挑战
- 虚拟安全设备
- 技术概述

数据中心趋势

动态工作负载	动态地实例化和移除应用工作负载
异类	涵盖物理和虚拟基础设施的部署
分布式部署	按需横向扩展/纵向扩展调配
独立于基础设施	对底层网络基础设施透明
感知云	旨在无缝迁移到公共云和私有云

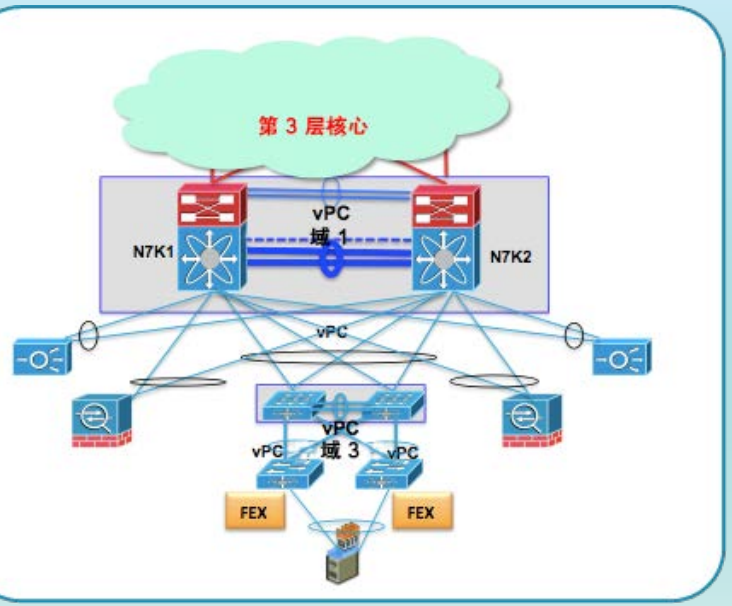
全球数据中心流量（按目标）

来源：2012 年思科® 全球云指数

- 数据中心趋势
- 数据中心安全挑战
- 虚拟安全设备
- 技术概述

孤岛部署

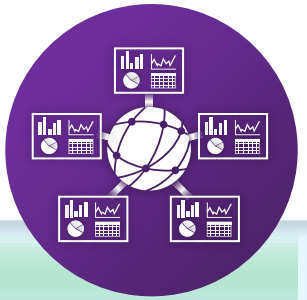
- 以边界为中心的安全保护方法
- 进行服务插入必须对网络结构（例如 VLAN、子网等）十分了解，部署限定在网络中的固定位置
- 东-西流量检测复杂且昂贵



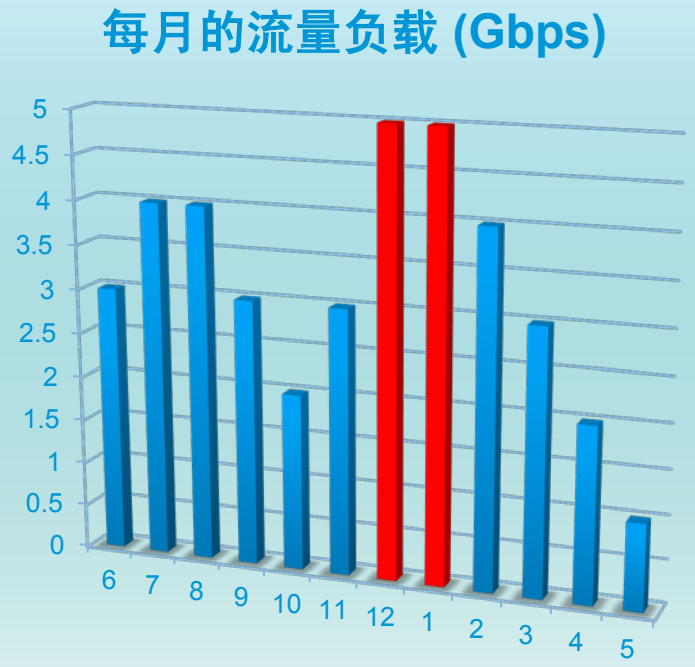
手动调配带来的挑战

- 静态的策略调配不能与动态的工作负载保持同步
- 每台设备的防火墙规则呈爆炸式增长是常见的现象
- 多租户部署中的运营挑战
- 容易出错的安全策略生命周期管理
- 多个管理域

无弹性的扩展



- 实施涵盖物理和虚拟工作负载的策略需要复杂的流量引导设计
- 超额调配以满足应用和安全服务级别协议 (SLA) 要求会增加成本
- 安全资源使用效率低会增加风险



客户在寻找什么？

- 数据中心趋势
- 数据中心安全挑战
- 虚拟安全设备
- 技术概述

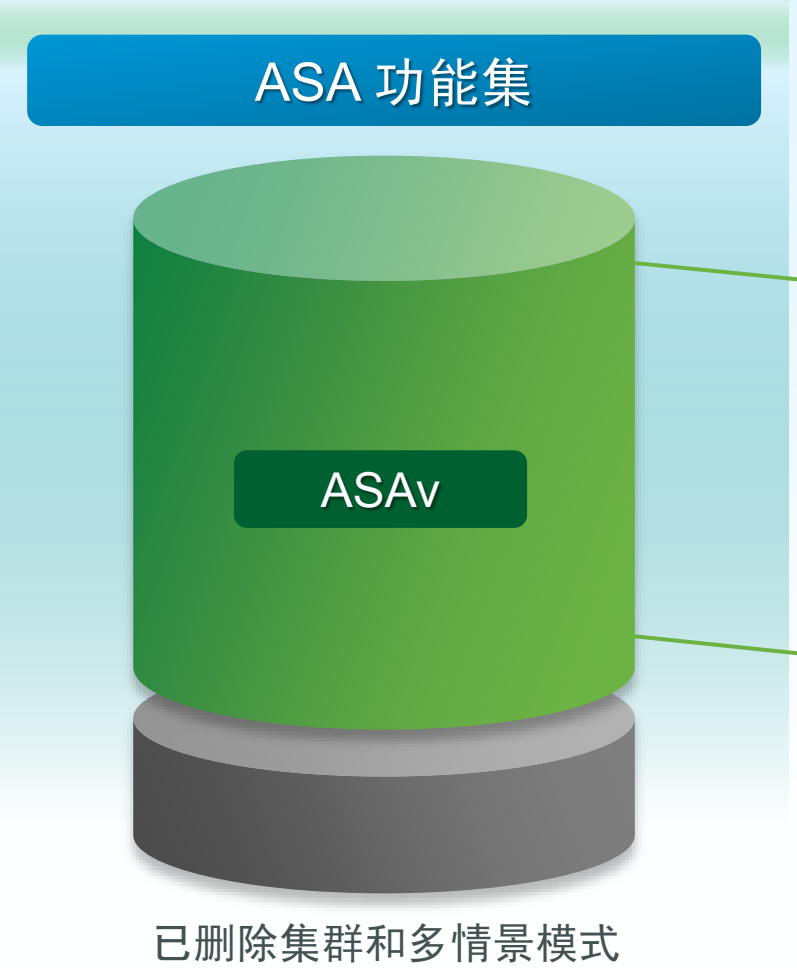
Cisco ASAv 安全设备简介

Cisco® ASAv 安全设备

将久经考验的思科安全性从物理环境带到虚拟化环境

ASA 发展

ASAv
物理 ASA 功能奇偶校验



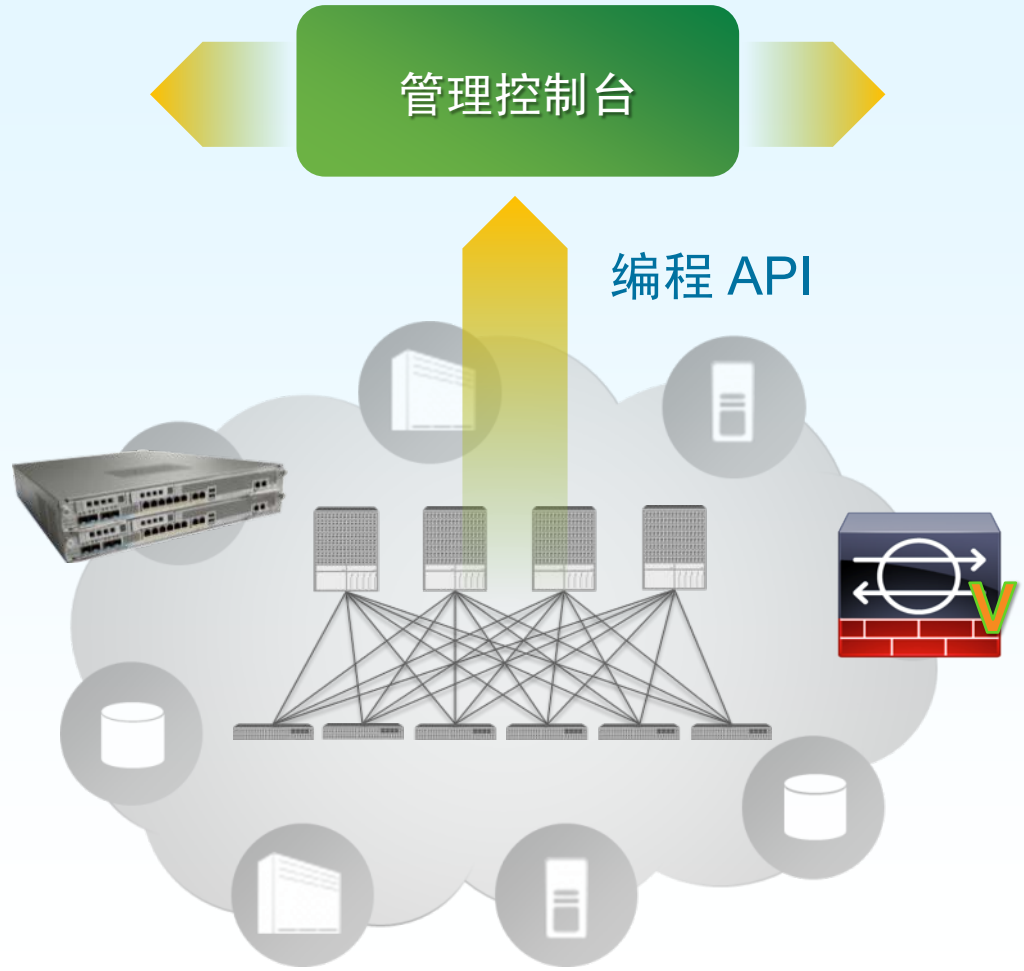
- 物理封装功能集奇偶校验
- 通过虚拟化扩展
- 最多 10 个 vNIC 接口
- 软件中的加密

- SDN 和传统管理工具
- 扩展至 4 个 vCPU 和 8 GB 内存
- 能够在物理和虚拟 ASA 上管理一个策略

集中式策略管理和自动化

集中式策略管理和自动化

- 南向 RESTful API，成熟的安全管理解决方案
- 涵盖物理和虚拟基础设施的统一访问机制
- 基于角色的访问控制 (RBAC)
- 遥测勘测功能

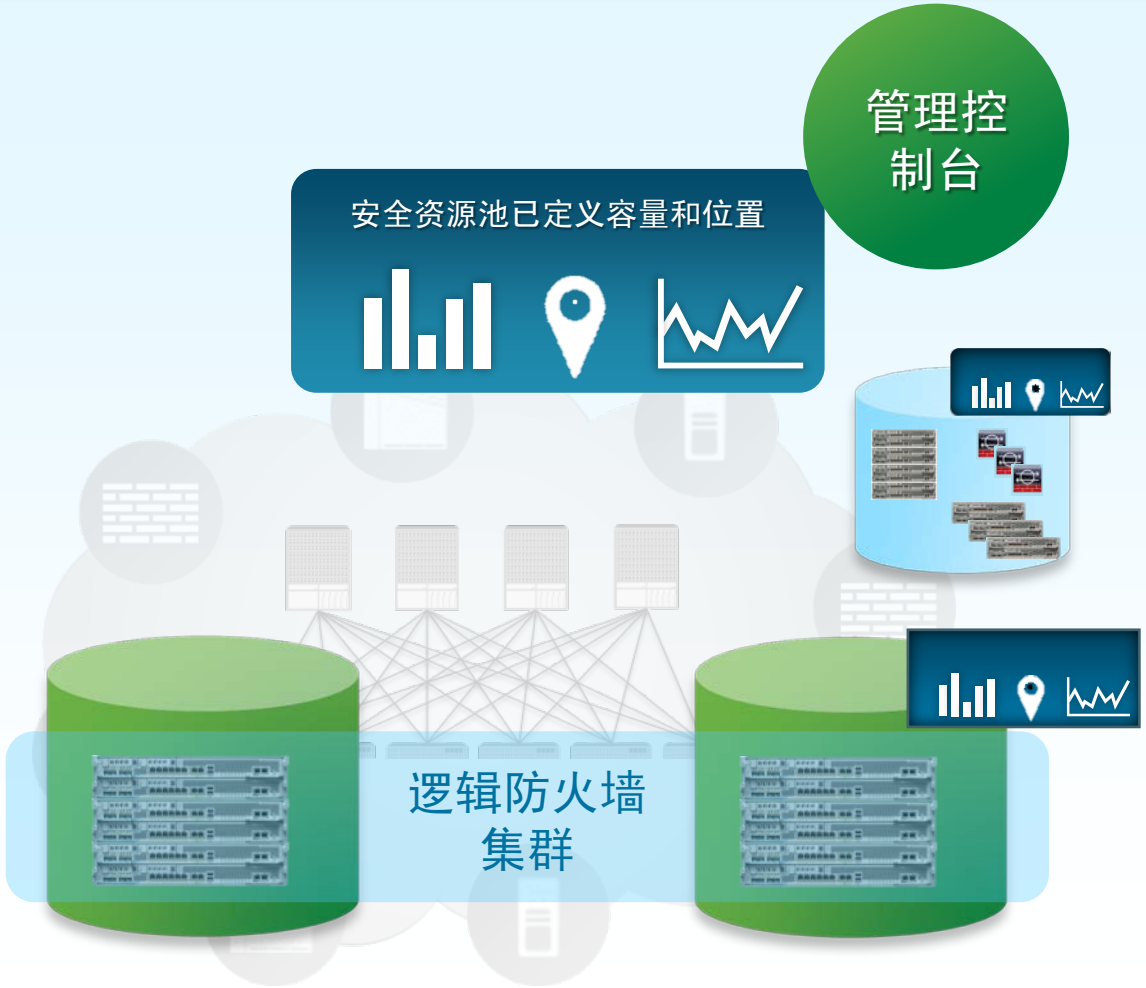


弹性扩展

安全资源池

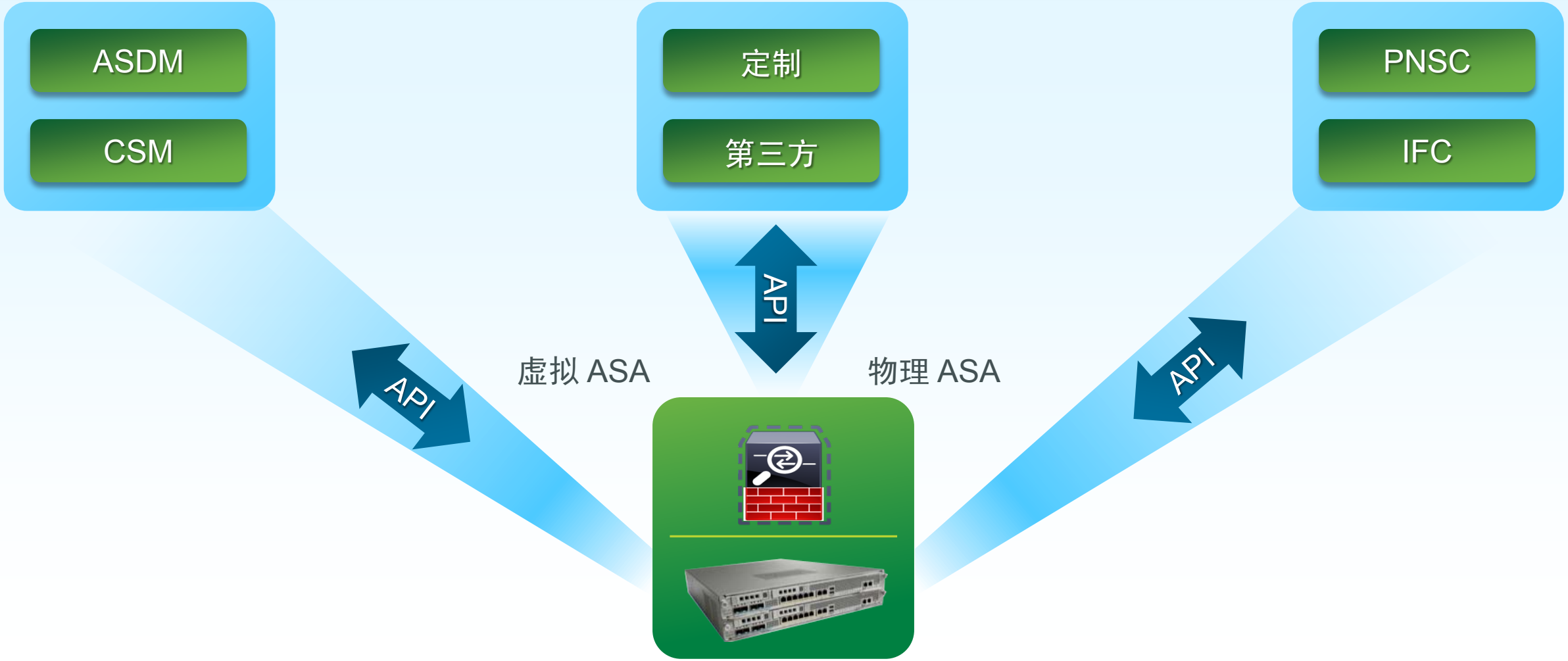
按需横向扩展/纵向扩展安全性

- N 路非状态负载分配
- 具有状态同步功能的 16 路负载分配*
- 适用于不同类型的虚拟基础设施
- 涵盖物理和虚拟设备的池
- 位置感知型智能流量引导，便于实施安全策略



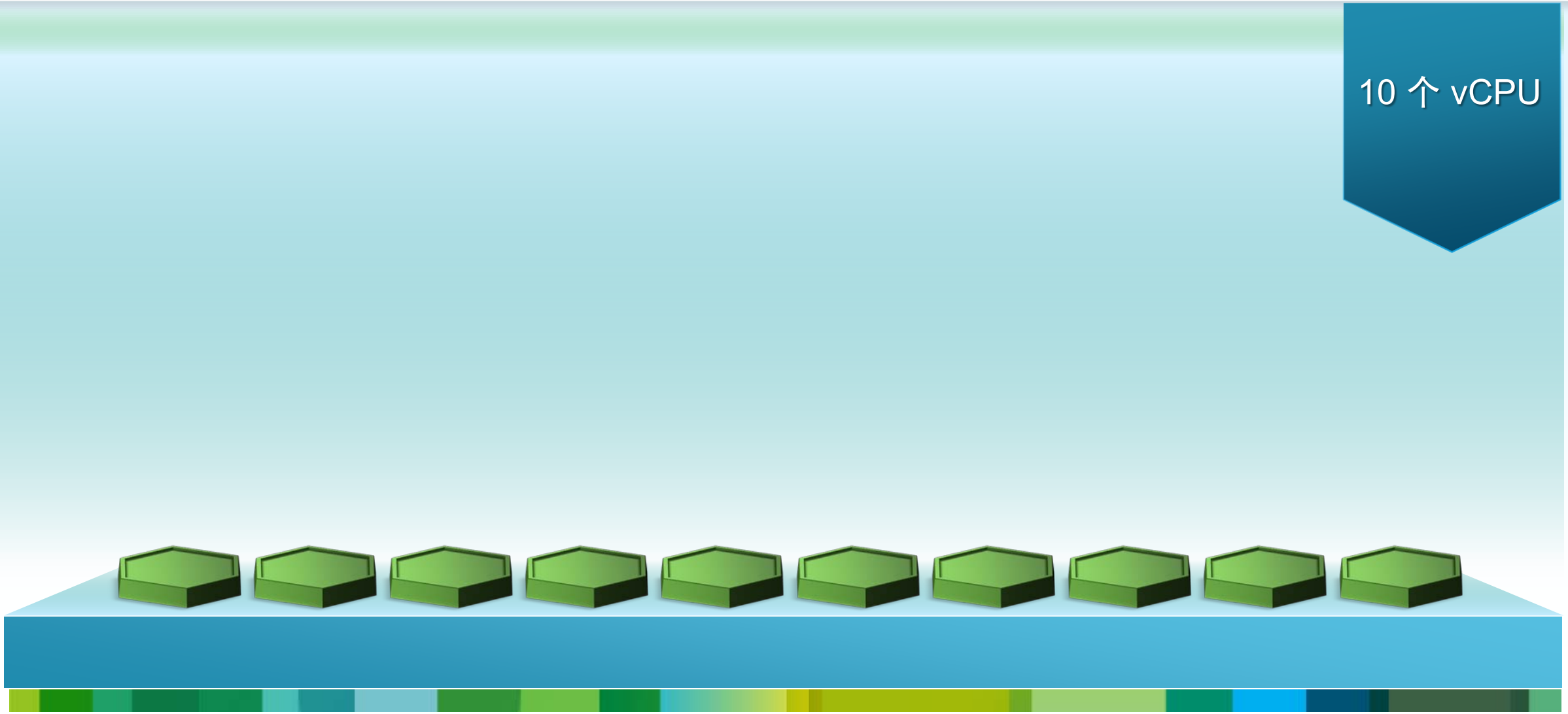
*仅限物理 ASA 集群

通过 API 实现的开放式管理



ASAv 灵活许可

灵活的许可



灵活的许可

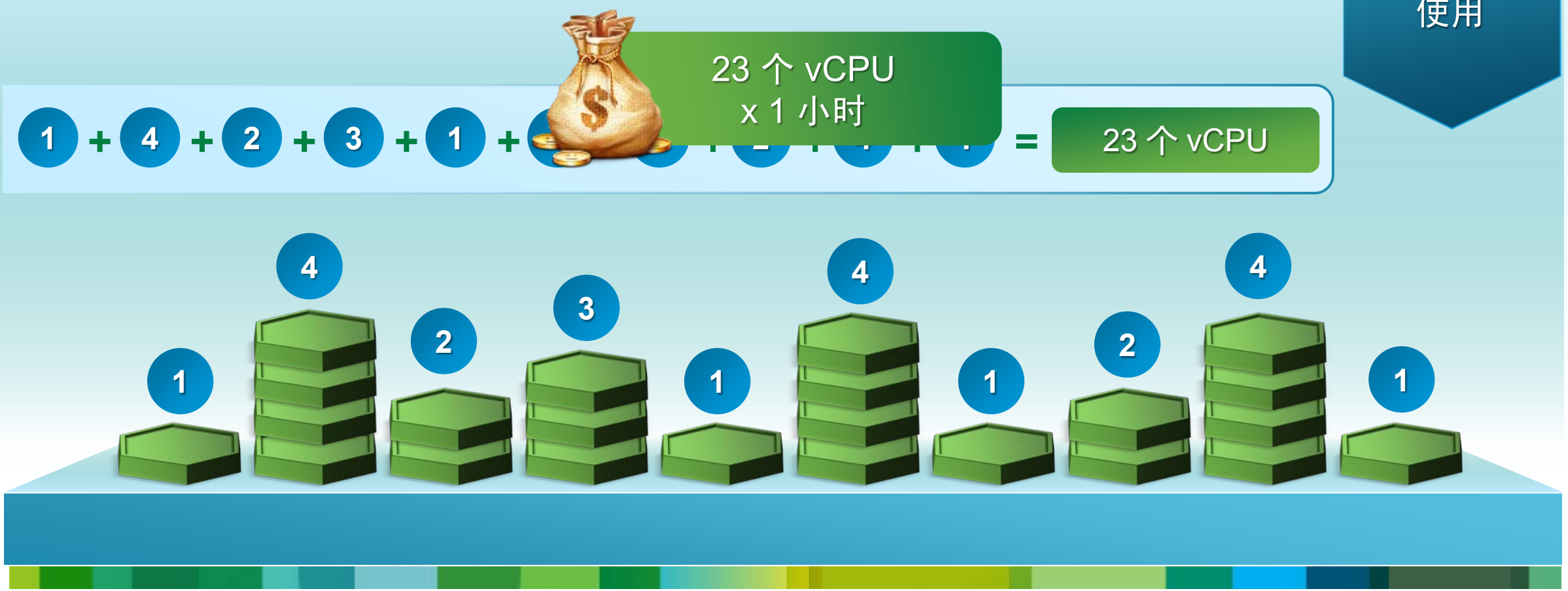
基于
使用

灵活的许可

基于
使用

灵活的许可

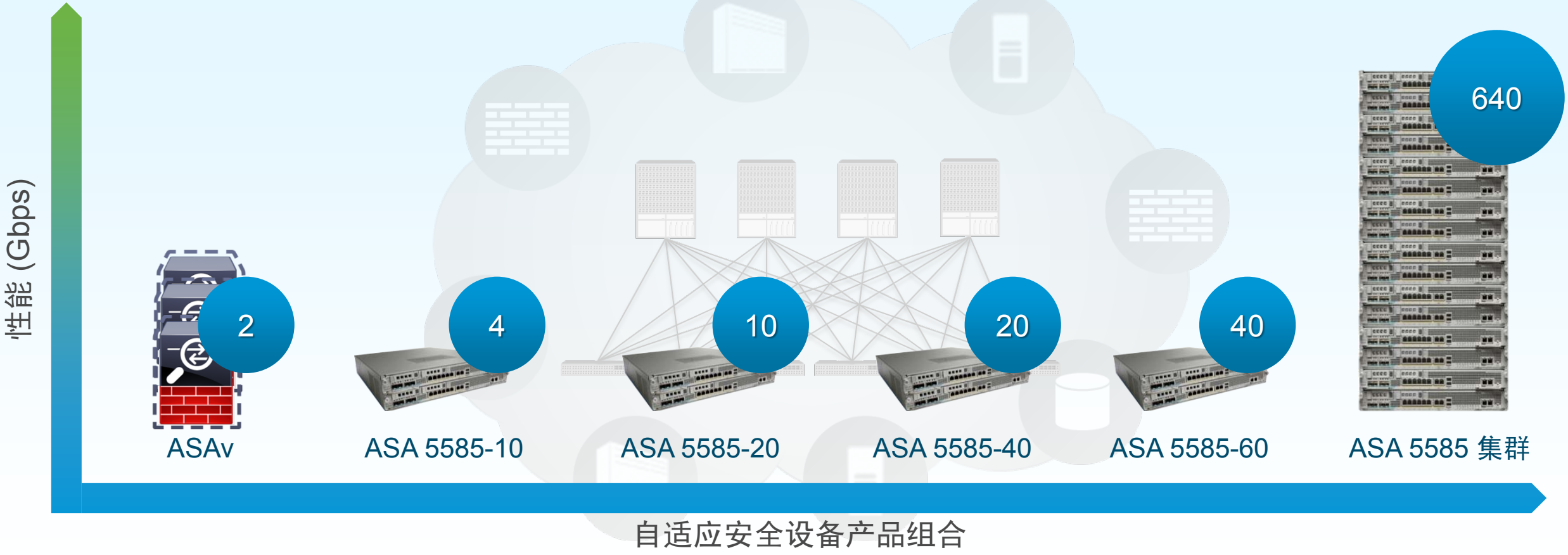
基于
使用



灵活的许可

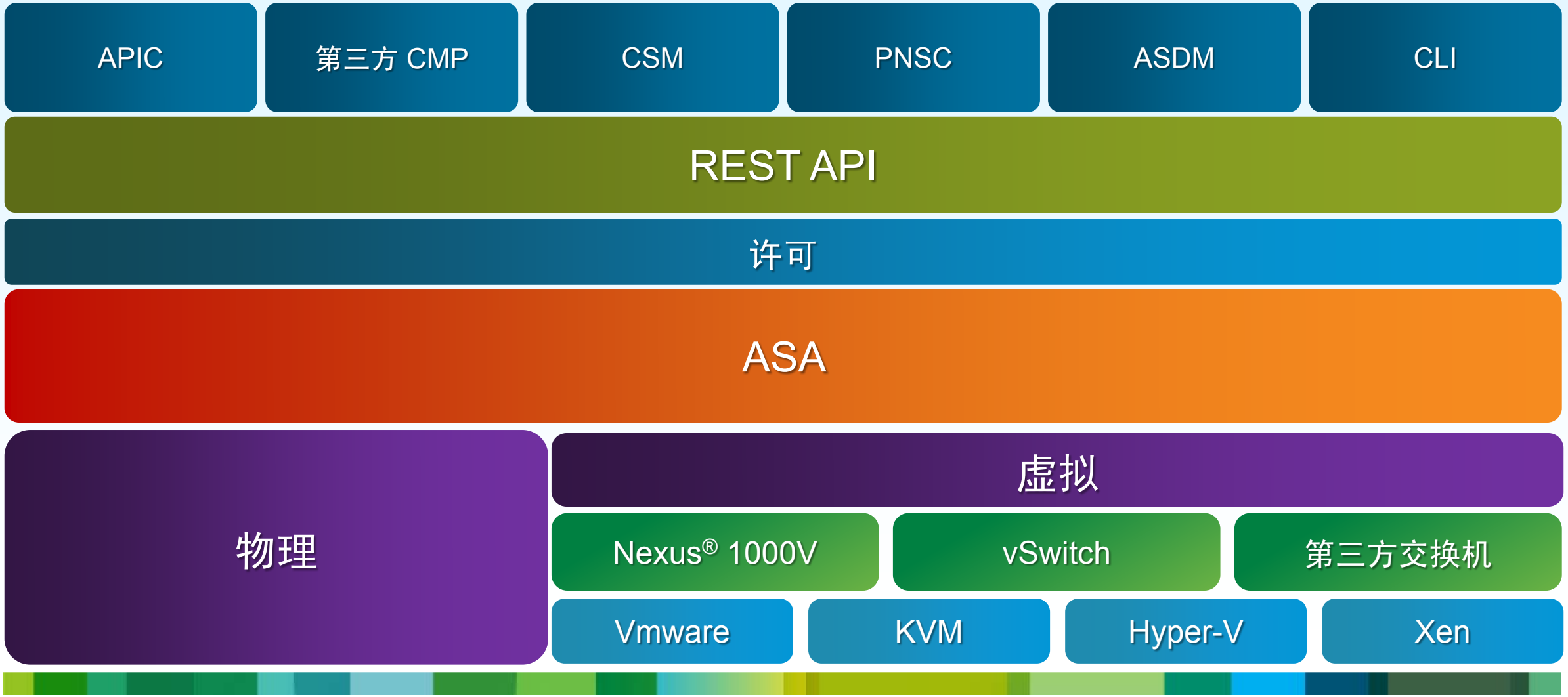
基于
使用

数据中心中的思科自适应安全设备



专为实现灵活性、可扩展性、可编程性和应用感知而设计

功能全面的开放式虚拟平台



- 数据中心趋势
- 数据中心安全挑战
- 虚拟安全设备
- 技术概述

ASAv 功能总结

虚拟机中的完整功能集

- 使用多个 vCPU（最多 4 个）和具有中继功能的 vNIC（最多 10 个），以及 VTEP（最多 1000 个）
- 基于期限的堆叠式许可模式
- 虚拟化优势取代对多情景和集群的需求

扩展虚拟 ASA 防火墙使用案例

- 使用 vPATH 和 VNMC 吸收 ASA 1000V 租户边缘路由防火墙
- 允许路由防火墙与任何接口上的任何主机（虚拟机或物理主机）进行通信
- 通过 VXLAN 或 VLAN 启用透明防火墙
- 通过服务标记交换模式启用交换矩阵集成

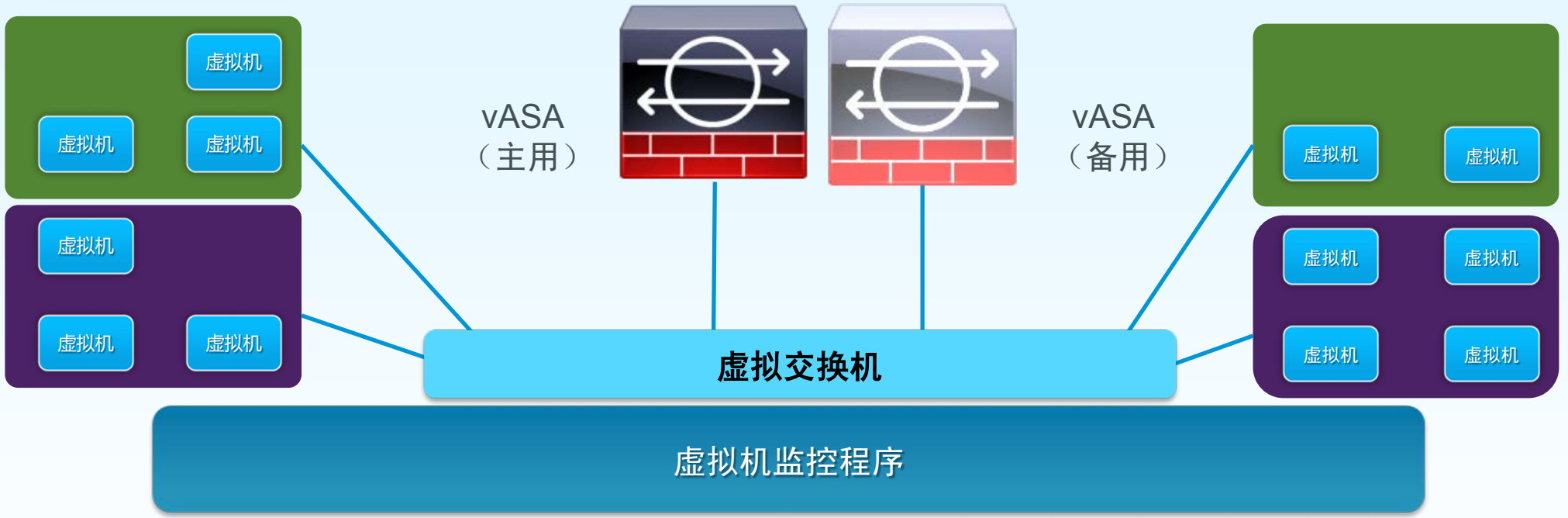
启用非 vPATH 独立模式

- ASAv 部署在虚拟机监控程序上并连接到 vSwitch

“主用/备用”故障转移

- 备用 ASAv 驻留在单独的主机上以改善冗余

vASA 和 vSwitch



每个 vASA 10 个接口（vNIC）

VLANs 及 Dot1Q VxLAN

多达 200 个 VLAN 或 1000 个 VxLAN 子接口

vASA
策略实施的三种模式

路由防火墙

- 在 vNIC 之间路由流量
- 维护 ARP 和路由表
- 租户边缘防火墙

透明防火墙

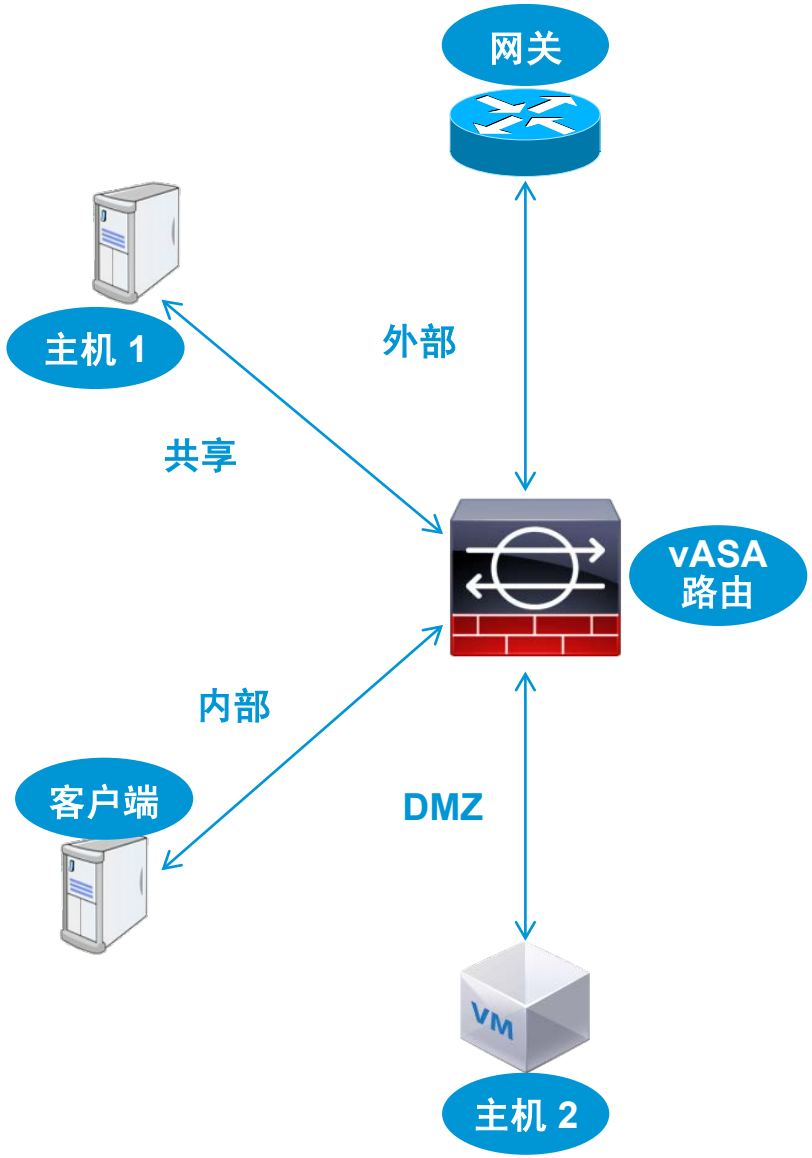
- VLAN 或 VxLAN 桥接/拼接
- 维护 MAC 地址表
- 不会破坏第 3 层设计

服务标记交换

- 在服务标记之间应用检测
- 没有网络参与
- 交换矩阵集成模式

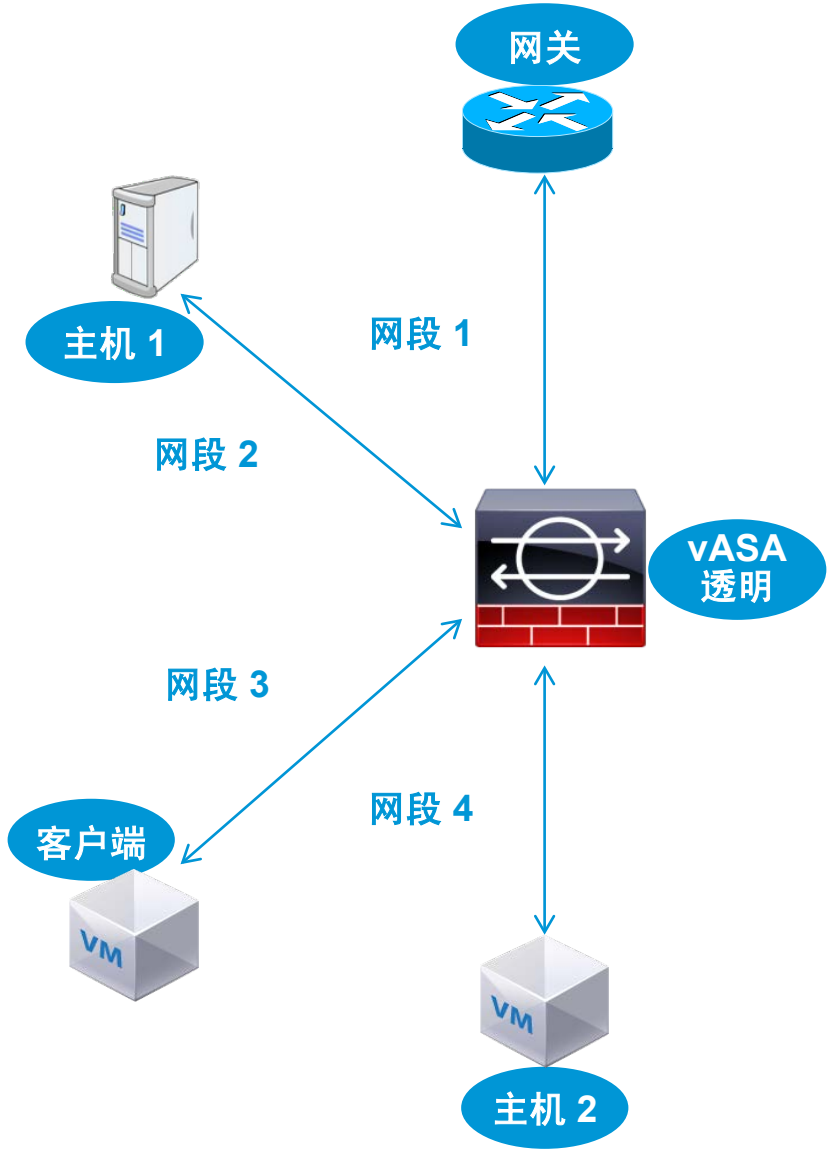
路由防火墙

- 路由 – 租户边缘使用案例
- 主机的第一跳网关
- 启用所有客户端主机（虚拟机或物理主机）
- 扩展数据接口数量
- 在多个子网之间路由
- 网络中的传统第 3 层边界



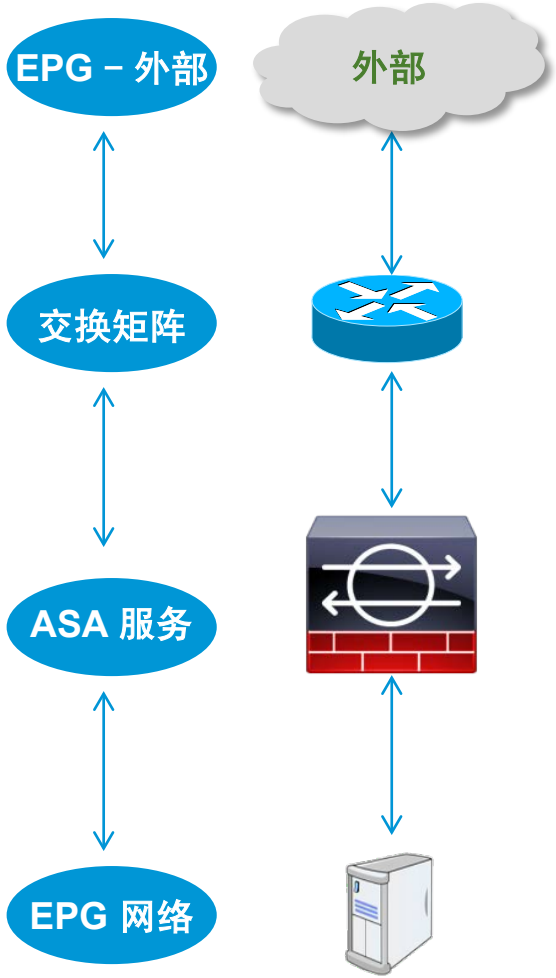
透明防火墙

- 最多桥接 4 个（子）接口
- 每个 vASA 最多 8 个 BVI
- 提供 NAT 和 ACL
- 非破坏性的 PCI 合规性
- 主机之间的传统第 2 层边界
- 一个广播域中的所有网段

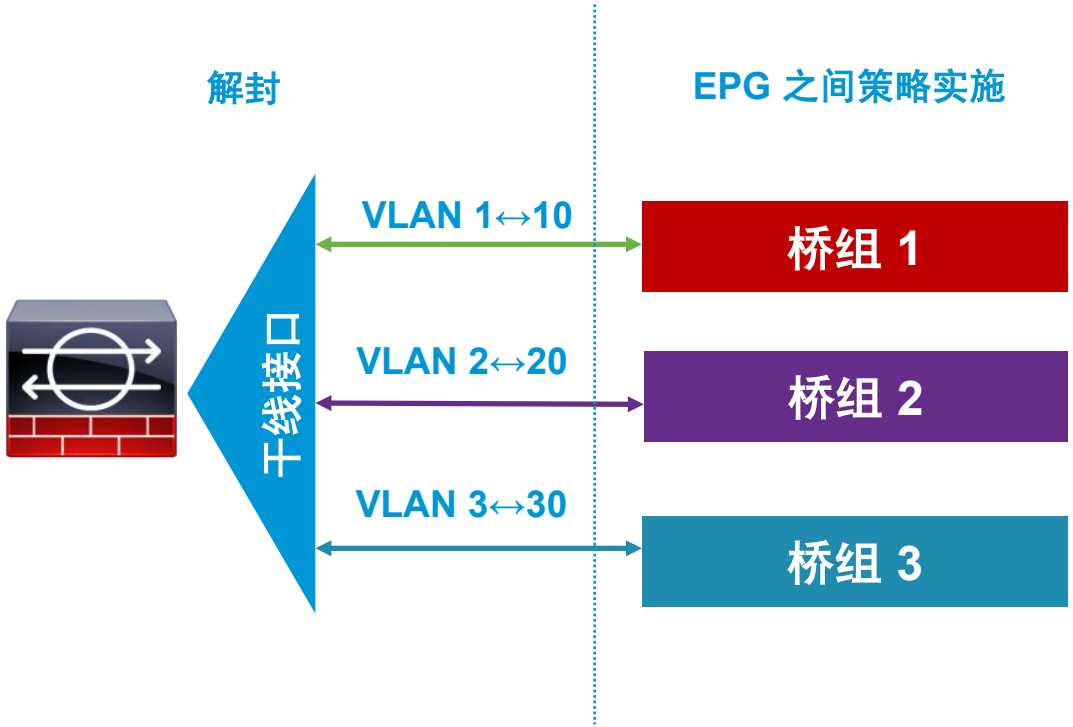


防火墙服务标记交换

- 执行 EPG 之间的策略实施
- 集中式 IFC 按需调配
- 保持策略绑定的服务标记
- 专为交换矩阵集成而设计
- 仍然提供 NAT 和 ACL
- 无传统网络交互（抽象成交换矩阵的桥接或路由功能）

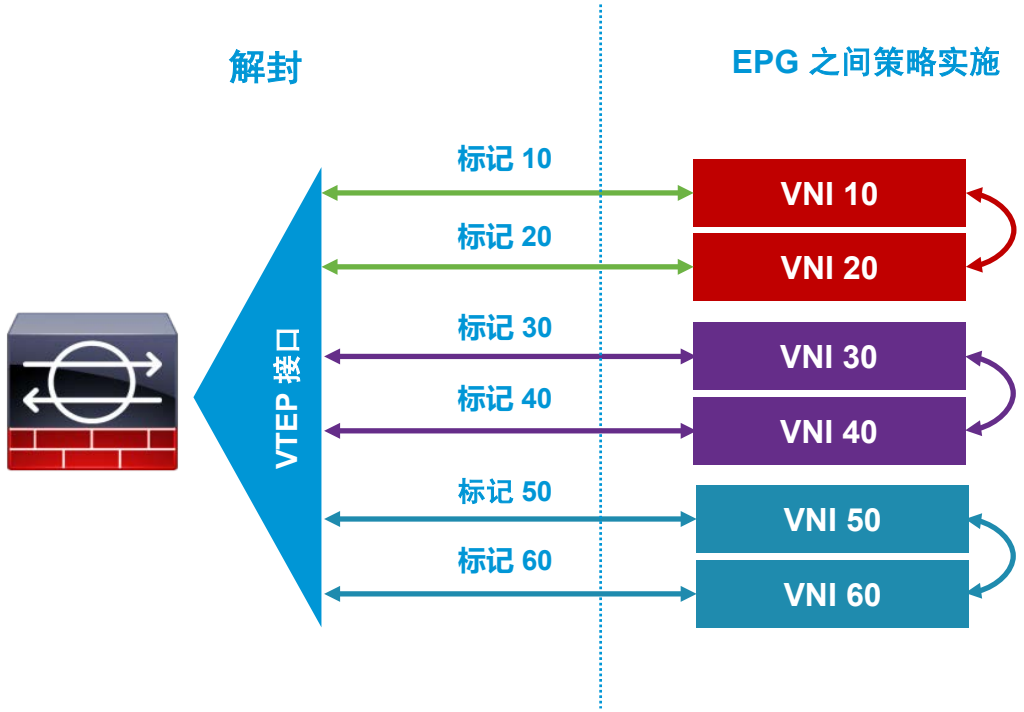


vASA VLAN
网络桥接/路由



- ASA 透明和路由防火墙
- 设备与网络交互
- 维护 MAC、ARP 和/或路由表

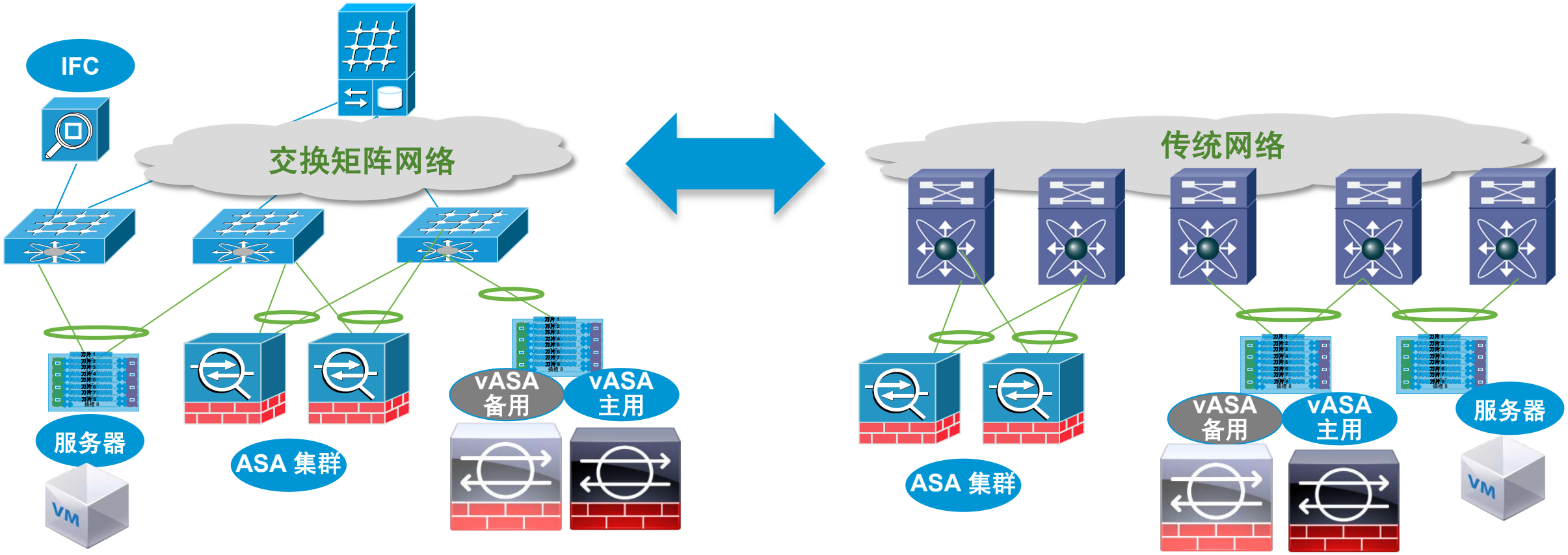
vASA VxLAN
服务标记交换



- 新的 ASA 交换矩阵集成模式
- 抽象成交换矩阵的网络功能
- VxLAN 不限于 STS 模式

ASA 部署

灵活的安全产品：交换矩阵与传统网络



ASA 物理和虚拟变体满足传统和以应用为中心的模型

ASAv 性能和可扩展性

产品手册指标	ASAv（1 个 vCPU）	ASAv（2 个 vCPU）	ASAv（3 个 vCPU）	ASAv（4 个 vCPU）
状态检测吞吐量（最大值）	1 Gbps	1.2 Gbps	1.5 Gbps	2 Gbps
状态检测吞吐量（多协议）	500 Mbps	600 Mbps	750 Mbps	1 Gbps
并发会话数	100,000	250,000	350,000	500,000
每秒连接数	10,000	15,000	15,000	20,000
每秒数据包数（64 字节）	450,000	500,000	600,000	700,000
VLAN	50	100	100	200
Cisco® Cloud Web Security 用户数	100	250	250	500
S2S IPSec IKEv1 客户端 VPN 用户会话数	250	250	250	750
Cisco AnyConnect® 或无客户端用户会话数	250	250	250	750

* 当产品接近首次发货 (FCS) 时，性能数值可能发生变化

vASA 功能交付

- VMware 虚拟机监控程序（vSwitch 和 dvSwitch）
- 非 vPATH 支持
- 通过服务标记交换 (STS) 模式实现交换矩阵集成
- 基于期限的许可（vCPU、非插槽）
- ASA 和 vASA 的 SDN 管理
- vASA 的 CSM 管理
- 10 个 vNIC 容量
- 200 个 VLAN 子接口
- 1000 个 VxLAN

2014 日历年上半年

- Hyper-V
- KVM
- Xen
- vPATH 和 PNSC (VNMC) 集成
- 基于使用的许可
- 增加到 VxLAN 规模 (10,000)

2014 日历年下半年

vASA 优势总结

虚拟 ASA 上支持物理 ASA 上的所有功能。

纵向扩展

横向扩展

多个具有中继的接口和 VTEP

API 驱动的管理

基于期限的许可

多个管理器

多个虚拟机监控程序

多个交换机

灵活的许可

谢谢。