云计算的自动化安全管理

- 唐建伟 高级技术顾问
- 18670349118
- jianweit@vmware.com

vmware

湖南大成永正信息科技有限公司

虚拟化技术、数据库技术、运维服务

2014
正式成立

100+
服务客户超过100家

200+
携手渠道合作伙伴

8+
从事虚拟化数据库行业8年以上

vmware

湖南大成永正信息科技有限公司

虚拟化技术、数据库技术、运维服务

vmware®

ORACLE® Gold Partner Cloud Standard

敬请扫描二维码预约“百校虚拟化与数据库安全免费巡检”活动。预约电话：喻15874800006

vmware®

湖南大成永正信息科技有限公司

虚拟化技术、数据库技术、运维服务

案例名单（部份项目中为后台供货或提供服务\排名不分先后）

政府行业

湖南省财政厅财政
湖南省人力资源和社会保障厅
湖南省水利厅数据库
湖南省防汛办
长沙海关
长沙市交通局
长沙市轨道交通集团
长沙市人力资源和社会保障厅
株洲市交通局
岳阳市交通局
长沙市公交投资股份有限公司
湖北省人民政府
湖北省交通厅

教育行业

湖南省教育厅
中南大学
湖南大学
邵阳学院
湘潭大学
湖南工程学院
湖南工业大学
湖南商学院
湖南电子科技职业技术学院
武汉大学
长沙理工大学
长沙学院
中南林业科技大学

vmware

湖南大成永正信息科技有限公司

虚拟化技术、数据库技术、运维服务

（部份项目中为后台供货或提供服务\排名不分先后）

教育行业

南华大学
湖南文理学院
湖南第一师范学院
衡阳师院
湖南中医药大学
…

企事业单位

南车集团株洲动力机车研究所
长沙市黄花机场高速公路管理局
株洲市自来水公司
湖南合顺集团
湖南科力远
湘潭钢铁厂
湖南涟钢集团
湖南杉杉新能源
湖南克明面业股份有限公司
江西汇仁集团数据库采购项目
株洲千金药业集团
蓝思科技

vmware

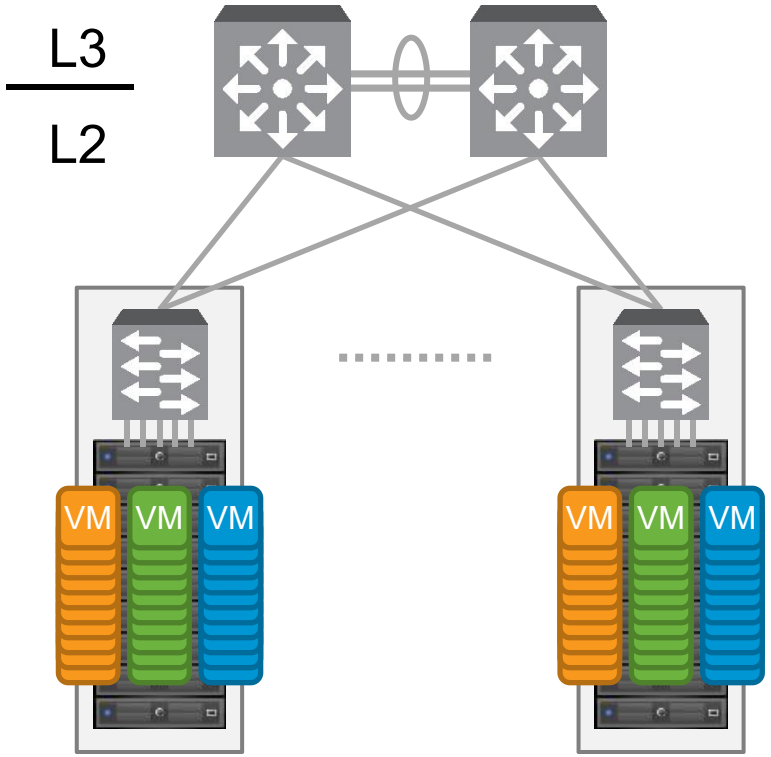
自动化

您知道吗？

- 2017年2月28号
- 手动删除服务器的脚本
- Amazon S3 3小时39分钟的宕机
- 一分钟，对亚马逊造成的损失是**$66,240**美元

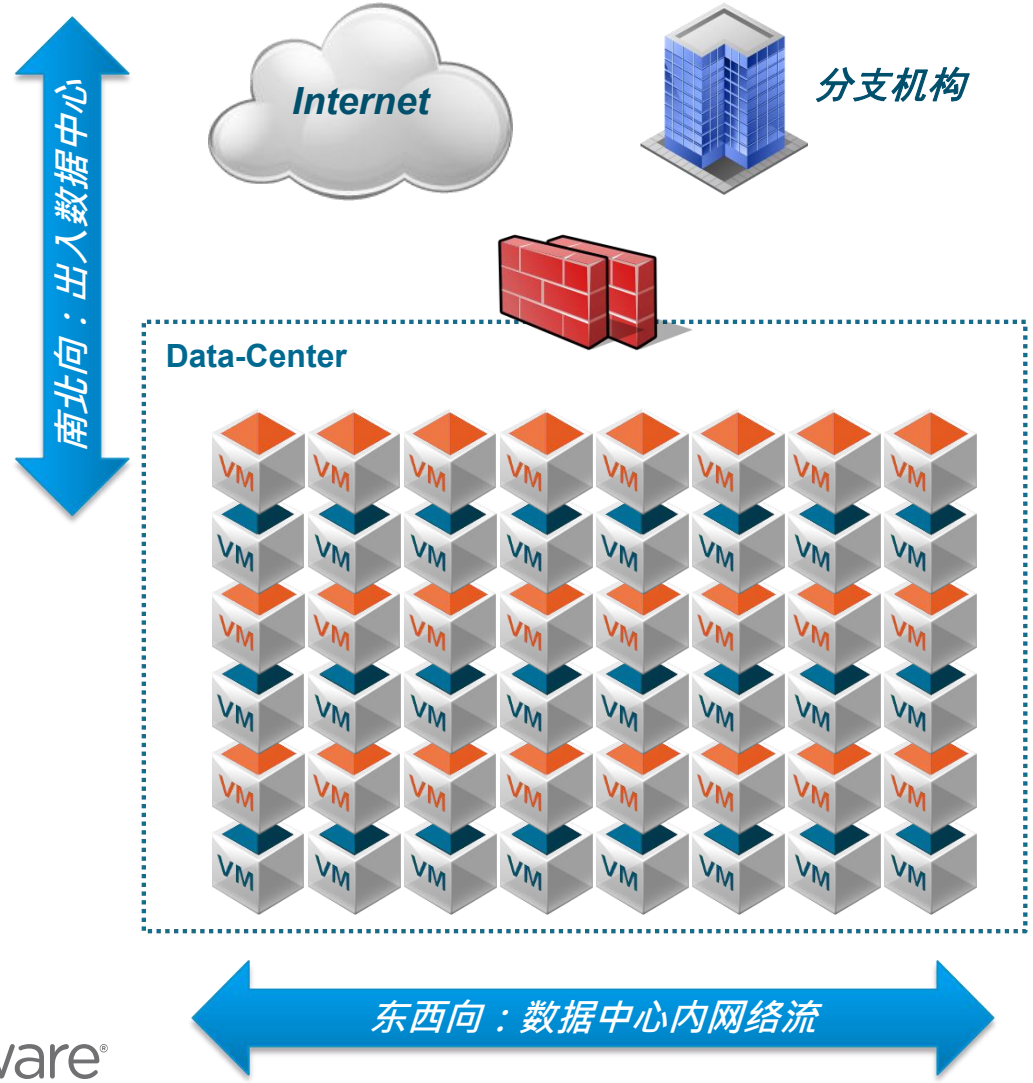

计算
网络
如何自动化？
应用
存储
安全

云计算的特性：虚拟机数量大幅增加，远超过物理环境规模



网络安全的运维困难性
大幅增加

数据中心内着重南北向防护，但东西向防护的机制极度欠缺

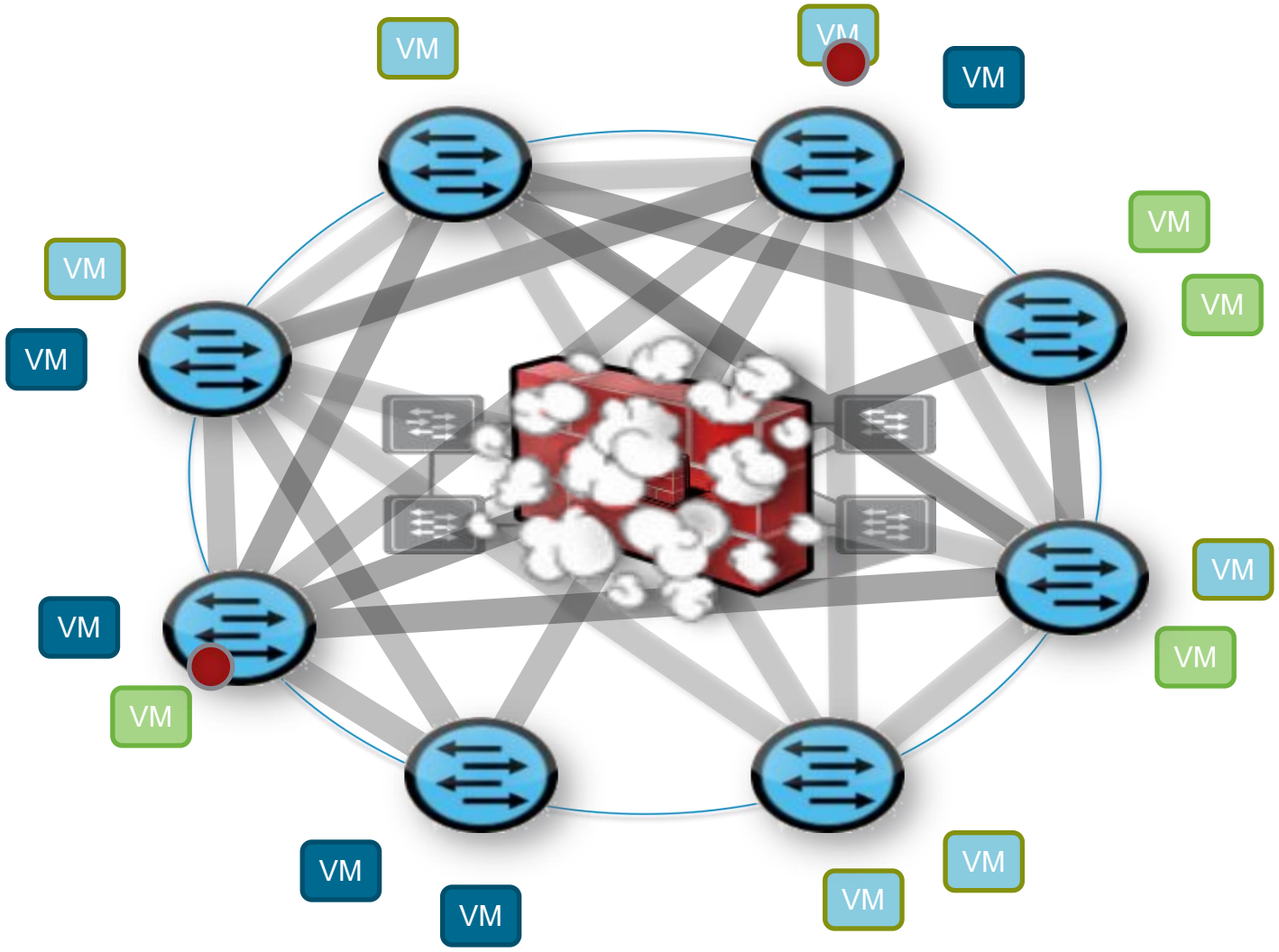


Cisco Global Cloud Index 对于数据中心网络流统计信息:

- *东西向网络流: 76.7%*
- *南北向网络流: 16.7%*
- *数据中心间之网络流: 6.6%*

数据中心内的东西向安全防护刻不容缓

南北向物理安全设备的功能如此强大，为何数据中心还是会遭受入侵？



vmware

防火墙的规则-难以阅读、不易维护

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	* Any	Web_Server	http	accept	None
2	Email_Server_Internal	Email_Server_DMZ	smtp->outgoing-email	accept	Log
3	net-10.0.0.0-24	Email_Server_DMZ	smtp	accept	Log
4	Email_Server_DMZ	net-10.0.0.0-24	smtp->incoming-email	accept	Log
5	Email_Server_DMZ	net-10.0.0.0-24	smtp	accept	Log
6	net-10.0.0.0-24	Web_Server	ftp->web-server-upload	accept	Log
7	net-10.0.0.0-24	Web_Server	ftp->web-server-download	accept	Log
8	net-10.0.0.0-24	Web_Server	ftp->ftp-scan	accept	Log
9	net-10.0.0.0-24	* Any	http	accept	Log
10	CVP_Server	www.cvp-vendor.com	http	accept	None
11	UF				
12	* An				

DMZ interface

	Proto	Source	Port	Destination	Port	Description
↑	UDP	DMZ net	*	192.168.1.2	53 (DNS)	Permit DMZ to primary DNS server
↑	UDP	DMZ net	*	192.168.1.3	53 (DNS)	Permit DMZ to secondary DNS server
↑	TCP					
↑	UDP					
✗	*					

Configuration > Firewall > Access Rules

Add | Edit | Delete | Find | Diagram | Export | Clear Hits

#	Enabled	Source	Destination	Service	Action
DMZ (2 implicit incoming rules)			Paste		
1		any	Any less secure ne...	ip	Permit
2		any	any	ip	Deny
inside (2 implicit incoming rules)					
			Any less secure ne...	ip	Permit
			any	ip	Deny
			Any less secure ne...	ip	Permit
			any	ip	Deny
			192.168.5.3	smtp	Permit
			192.168.5.5	https	Permit
			192.168.5.4	domain	Permit
			any	ip	Deny

No.	Name	Type	Source	Destination	Service	Action
1	DMZ Access	User	any	172.16.10.11-172.1...	HTTPS HTTP	Accept
2	Web to App	User	172.16.10.11-172.1...	192.168.10.11-192....	Tomcat	Accept
3	App to DB	User	192.168.10.11-192....	192.168.30.10	MySQL	Accept
4	DMZ LDAP, NTP, and DNS access	User	172.16.10.1/24	172.16.40.1/24	any	Accept

业务系统能够快速地进行部署，但安全政策的设置需要花费极大时间才能完成

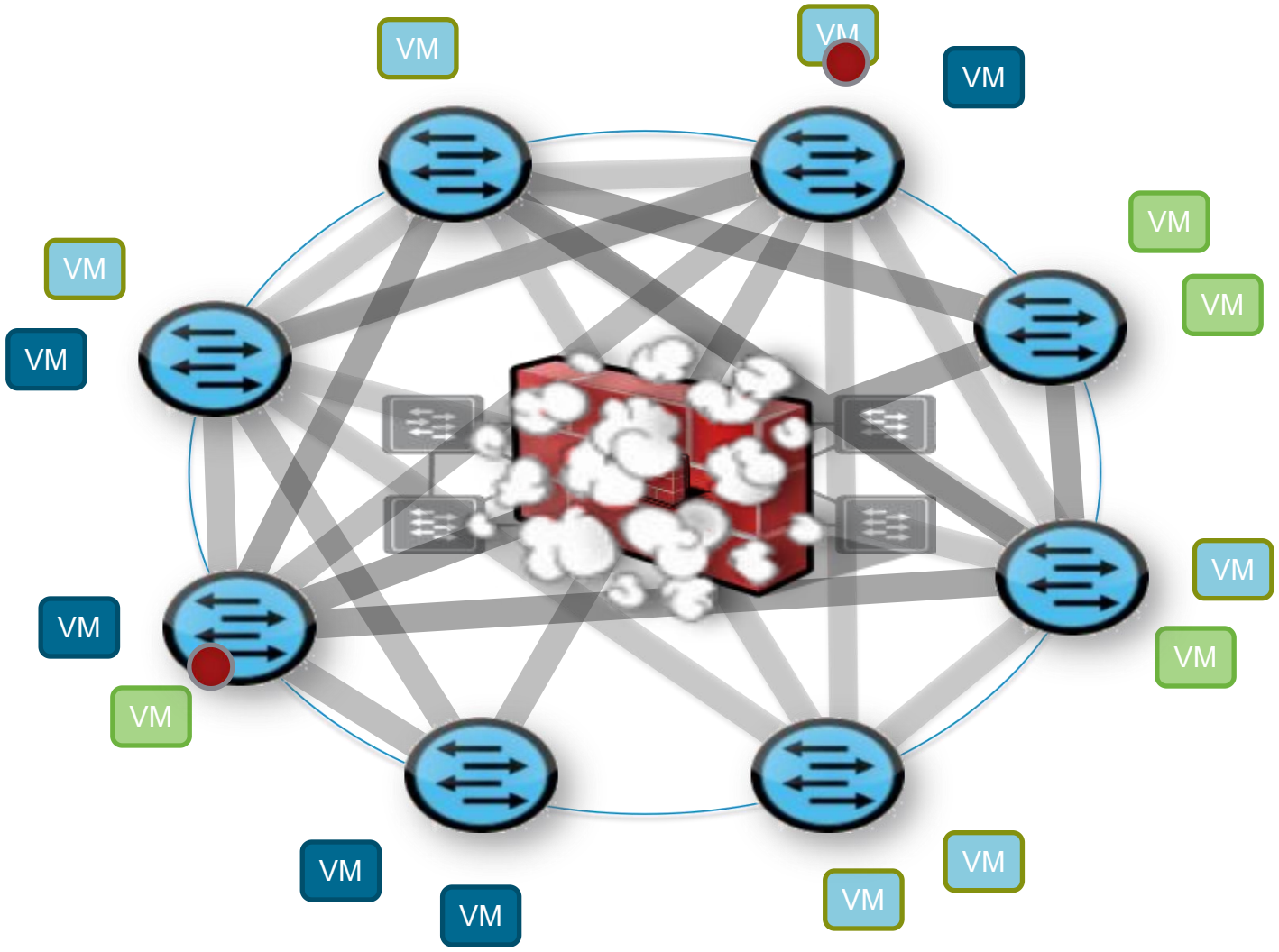
VM 37 秒

虚拟机的平均部署时间

6~8 周

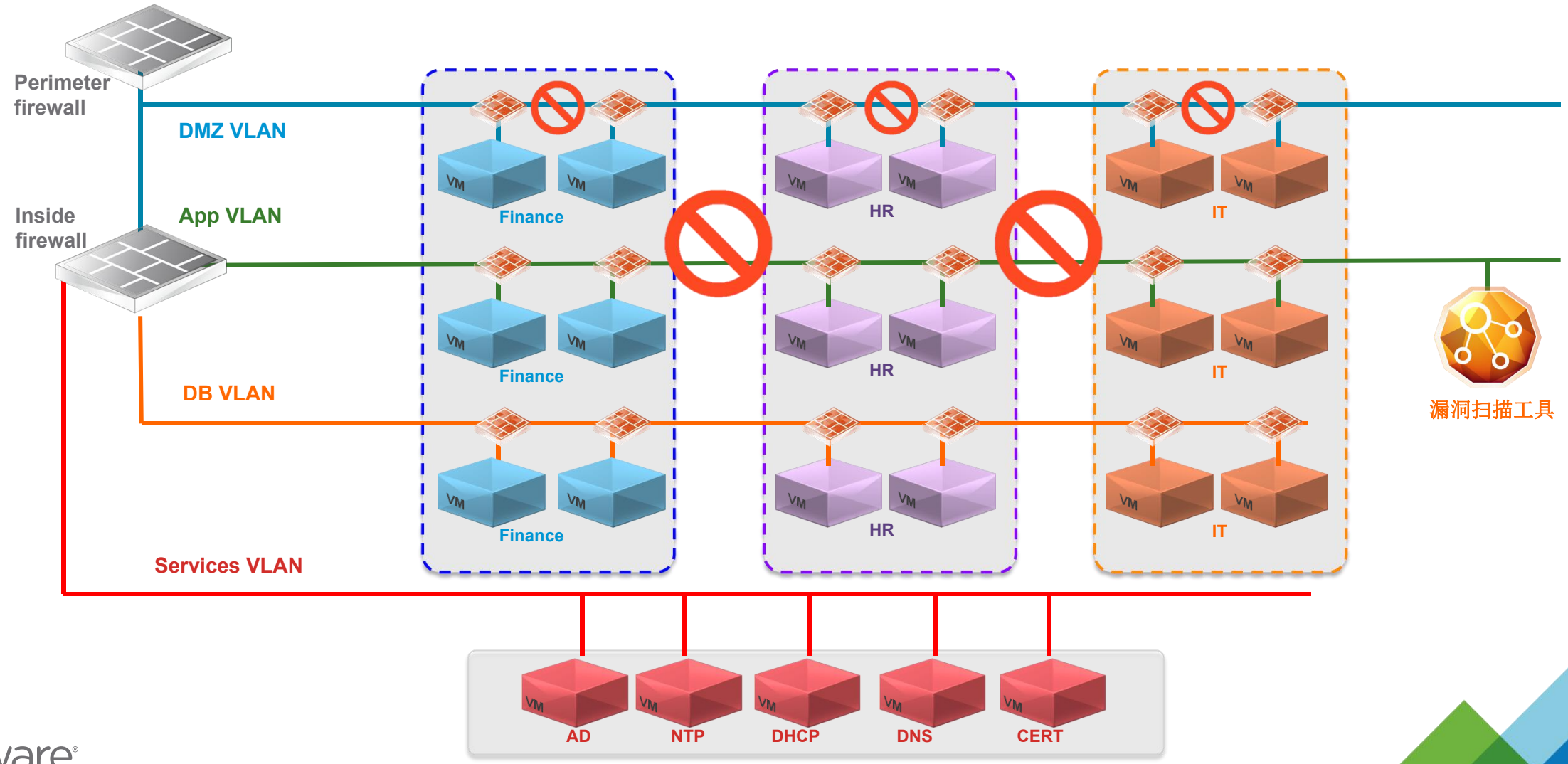
安全设置所需求的平均时间

若需要达成完善的虚拟环境防护，需要能够在数据中心内的每一个节点都有办法进行安全防护控制---VMware NSX



vmware

零信任安全机制


Perimeter firewall
Inside firewall
DMZ VLAN
App VLAN
DB VLAN
Services VLAN
Finance
HR
IT
VM
AD
NTP
DHCP
DNS
CERT
漏洞扫描工具

灵活的分布式防火墙规则对象

策略规则：

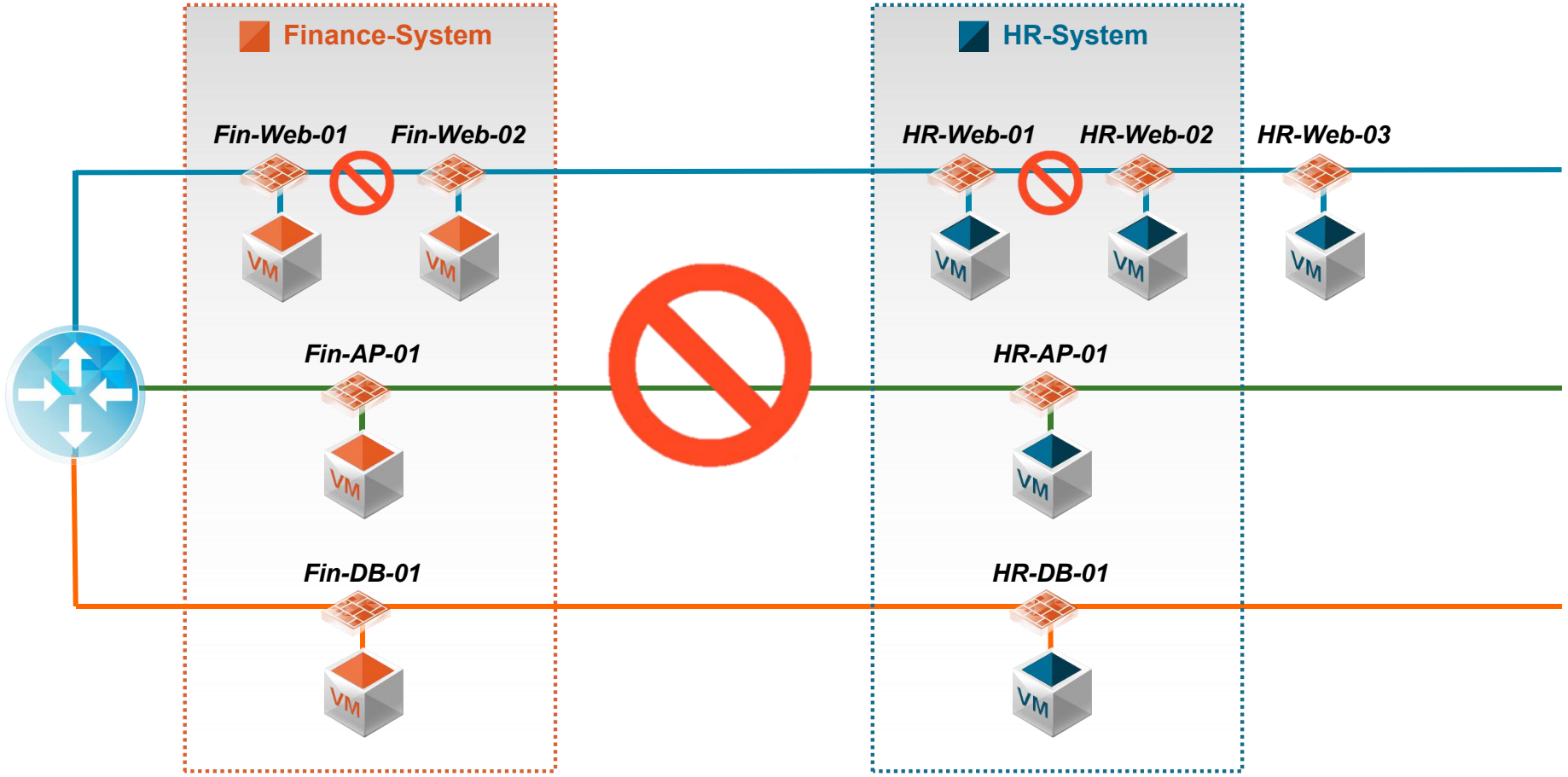
Rule ID 规则ID	Rule Name 规则名称	Source 源	Destination 目标	Service 服务	Action 动作	Applied To 规则适用范围

源或目标域	描述
IPv4 或 IPv6	IPv4 或 IPV6 地址，可以是主机地址、子网或一段地址
Datacenter 数据中心	vCenter的Datacenter属性。规则将适用于该Datacenter内所有的虚拟机/虚网卡
Cluster 集群	vCenter的 Cluster 属性。规则将适用于该Cluster内所有的所有的虚拟机/虚网卡
Network 网络	vCenter的 Network (vSwitch) 属性。规则将适用于该网络内所有的所有的虚拟机/虚网卡
Virtual App 虚拟App	vCenter 的 vAPP 属性。规则将适用于该vApp内所有的所有的虚拟机/虚网卡
Resource Pool 资源池	vCenter的资源池属性。规则将适用于该资源池内所有的所有的虚拟机/虚网卡
Virtual Machine 虚拟机	虚拟机名字属性
vNIC 虚网卡	虚拟机的虚网卡属性
Logical Switch 逻辑交换机	NSX 的逻辑交换机属性 (VNI – 或 VXLAN 网络标识).
Security Group 安全组	NSX的安全组属性 (在服务编排菜单下定义)
IP sets IP集	IPv4 或 IPv6 地址集

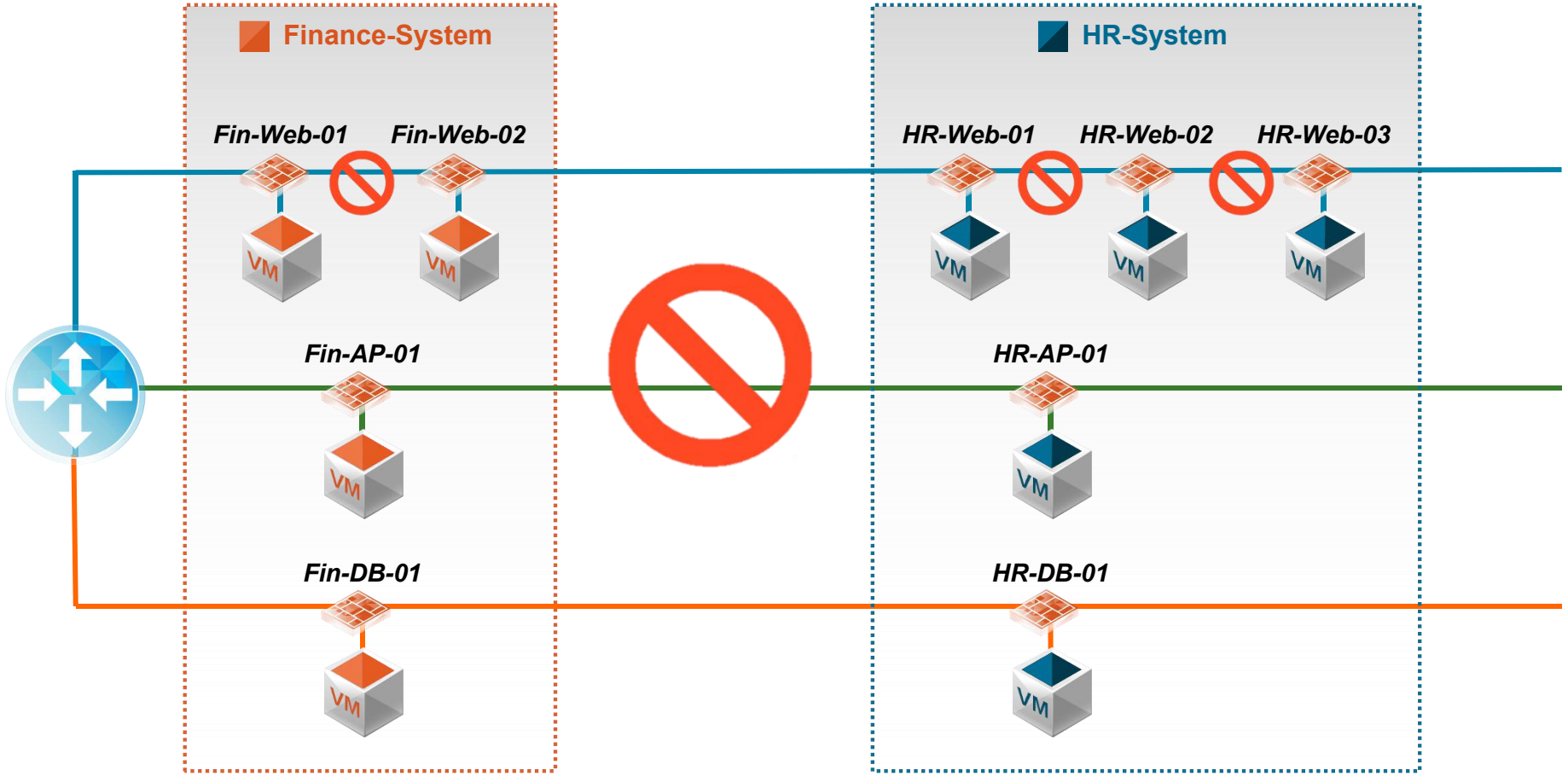
服务域	描述
协议	TCP, UDP, Oracle_TNS, FTP, SUN_RPC_TCP, SUN_RPC_UDP. NBNS_BROADCAST, NBDG_BROADCAST, ICMP, IGMP, IPCOMP, IPV6ROUTE, IPV6FRAG, IPV6ICMP, IPV6NONXT, IPV6OPTS, RSVP, GRE, ESP, AH, L2TP, SCTP, IPv4, ARP, X25, LLC, FR_ARP, BPQ, DEC, DNA_DL, DNA_RC, DNA_RT, LAT, DIAG, CUST, SCA, TEB, RAW_FR, RARP, AARP, ATALK, IEEE_802_1Q, IPX, NETBEUI, IPv6, PPP, ATMMPOA, PPP_DISC, PPP_SES, ATMFATE, LOOP 注：用户可以自己定义协议（通过点击New -> Service菜单）
端口 (L4的目标端口)	唯一端口或一组端口
高级选项: 源端口 (L4源端口)	唯一端口或一组端口

动作域	描述
Block 阻止	阻止流量
Allow 允许	允许流量
Log 记录	记录流量信息
Do not log 不记录	不记录流量信息

VMware NSX 微分段技术于客户端实际应用场景：
业务系统扩充时，新的虚拟机自动加入安全群组



VMware NSX 微分段技术于客户端实际应用场景：
业务系统扩充时，新的虚拟机自动加入安全群组，直接套用安全政策



VMware NSX不仅是提供基本的L4 防火墙防护，可同时搭配顶尖的安全厂商，提供最精细且强大的完整保护

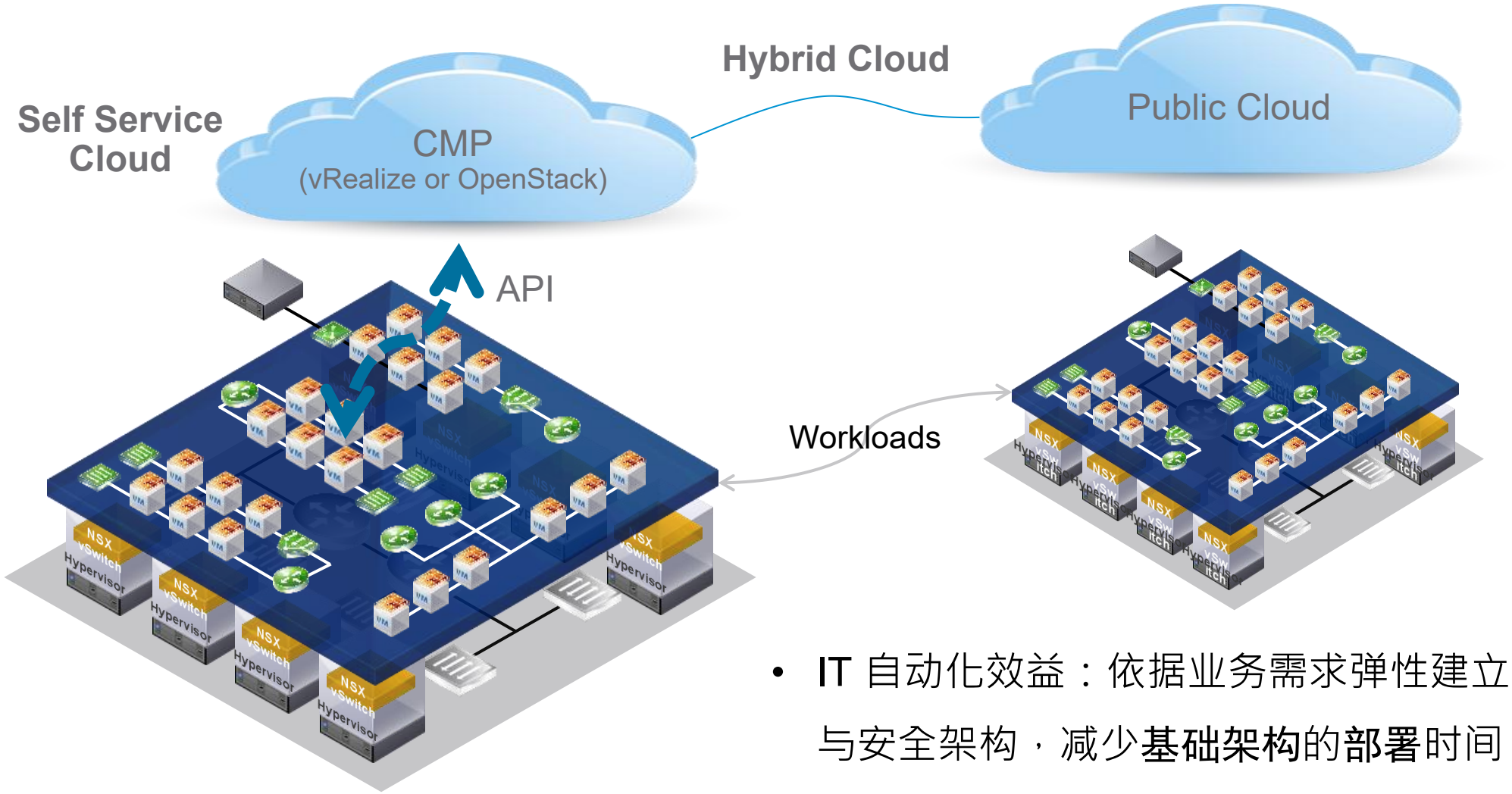
NSX — **Built-in Services**

Firewall	Data Security
Server Activity Monitoring	VPN (IPSEC, SSL)

vmware NSX PARTNER — **Third-party Services**

Antivirus	Firewall	Intrusion Prevention
Security Policy Management	Vulnerability Management	Identity and Access Mgmt
…and more in progress		

网络与安全自动化



- IT 自动化效益：依据业务需求弹性建立网络与安全架构，减少**基础架构**的**部署**时间，由数周到仅需数分钟。

结论：藉由VMware NSX微切分架构，我们能够协助您的数据中心达成

零信任等级防护

- 每一台虚拟机都受到保护
- 每一个网络封包都能进行检查
- 直接于虚拟机前就能进行最细部的安全控制

基于业务、系统的防护规则

- 安全团队进行防护时，能够借由群组方式指定特定业务、系统、或特定对象
- 或利用虚拟环境内的参数或知识进行设定

自动化达成安全策略设置

- 信息系统扩充、变更时，自动套用安全政策
- 无需手动进行资安组态变更

整合顶尖第三方安全厂家

- 完整的网络安全保护与IO保护
- 不同方案间之Security Chain管理

谢谢大家！

vmware