政务云安全建设实践

——温州政务云安全建设分享

黄锡斌
高级工程师、副经理

目 录
content

扫码观看大会视频

一、温州市政务云建设背景

背景

- 温州市电信从2012年开始为政府部门提供“服务器虚拟化”服务，为政府部门网站提供IDC平台、虚拟主机服务。
- 运营商建设电子政务云，售卖云服务，利润较低。
- 政务云建设初期，就考虑了安全资源如何运营和增值的问题
- 电信作为政务云承建方，希望交付的安全方案与租户上云业务分离，权责划分清晰

二、 政务云安全方案选型过程

政务云安全方案选型

温州市政务云安全方案选型，参考了其他省份政务云安全建设方案，考察了以下三种租户安全实现方案：

纯安全硬件

- 出口部署安全设备
- 租户侧依靠操作系统自带安全规则或软件

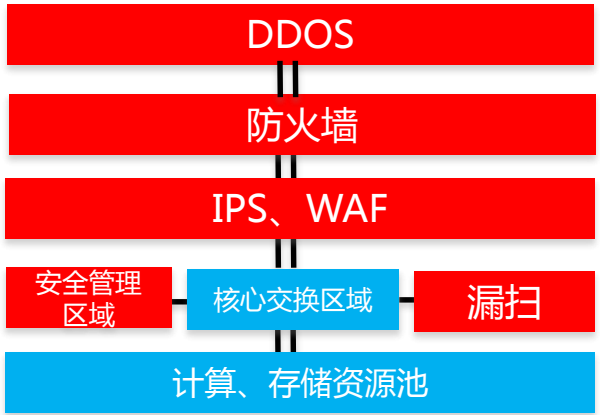
接口引流

- 通过虚拟化底层接口引流
- 利用虚拟化底层接口实现租户侧安全

硬件一虚多

- 借助专有硬件安全设备一虚多技术
- 通过硬件设备的分级分权管理分配管理权

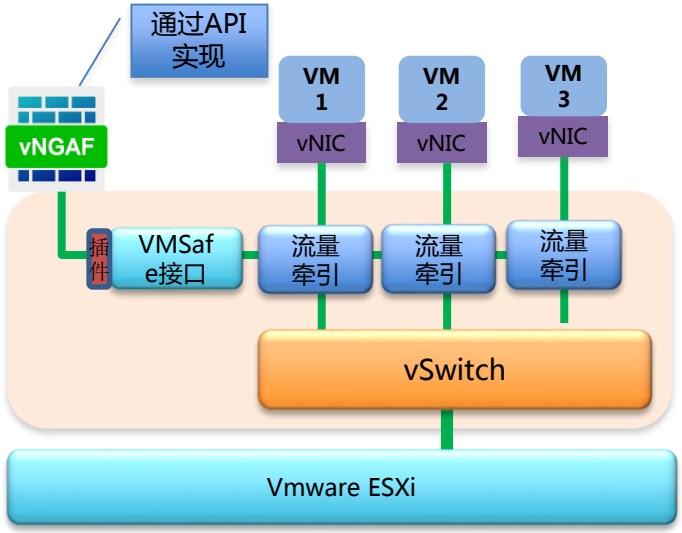
纯安全硬件部署方案



	描述
优点	1. 租户侧无需安装任何软件或agent 2. 能够实现政务云平台层面的安全防护
缺点	1. 无法区分租户 2. 无法实现差异化收费运营模式 3. 租户无法自管理 4. 安全策略无法个性化设备，容易误判、误报

部署硬件设备，如防火墙、IPS、WAF等安全硬件设备，通过网络地址的方式区分用户并分配策略。

接口引流方案

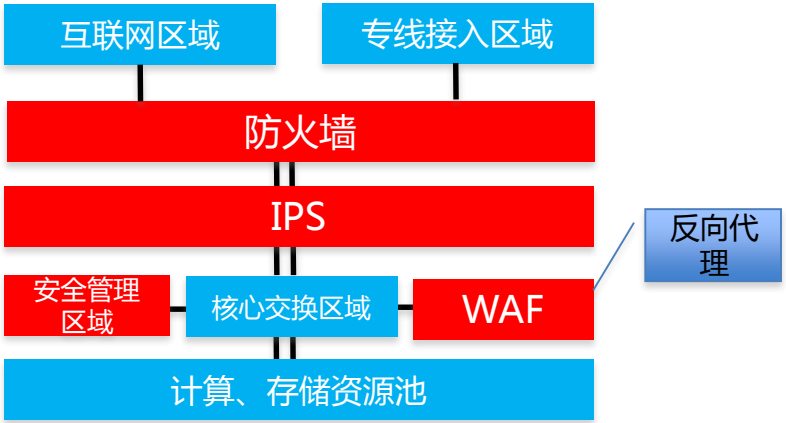


	描述
优点	1. 通过虚拟化平台底层引流，租户侧无需安装任何软件或agent 2. 平台运营方可以实现差异化配置和部署 3. 能够实现安全业务收益
缺点	1. 租户不可管理，安全不可视 2. 过于依赖平台方提供的技术、接口 3. 目前实现最好的是vmware，华为、华三均不支持

通过云平台技术提供方提供的接口，通过云平台API进行引流，结合第三方安全厂商安全产品提供安全功能

扫码观看大会视频

硬件一虚多+网络引流方案——最终确定采用的方案



	描述
优点	1. 租户侧无需安装任何软件或agent 2. 支持管理员分级分权管理 3. 能够实现IPS 简单的WAF 功能 4. 能够实现简单的差异化安全服务运营
缺点	1. 缺少安全厂商产品后续支撑，很多功能交付不尽人意，无法使用 2. 在租户侧无法实现自管理，租户自身业务安全状况不可视 3. 安全功能有限（负载、IPS、传统FW）

温州政务云在项目选型阶段，受限于当时的技术，采用了以上安全方案，通过出口安全硬件一虚多、WAF反向代理，实现租户侧安全能力交付，每年实现安全营收100w左右

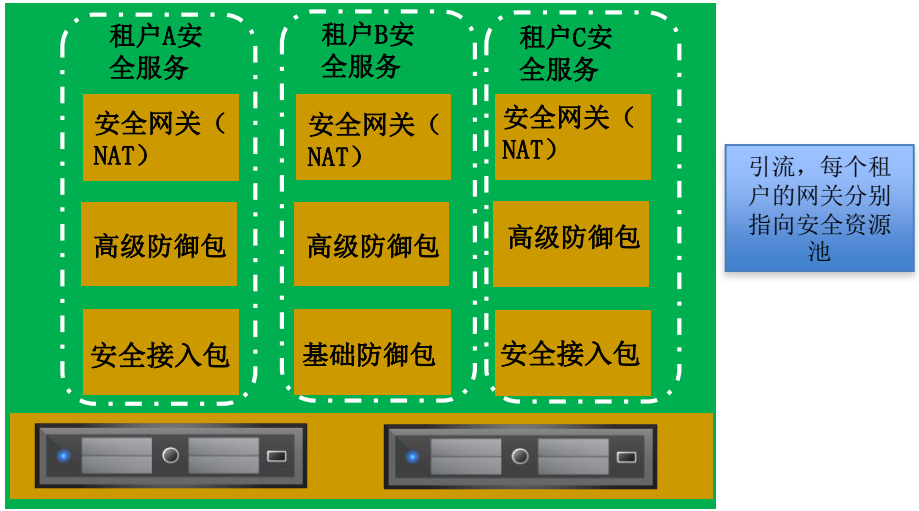
扫码观看大会视频

原有方案使用中遇到的问题

现有方案使用过程中遇到的问题	希望新的安全方案能够解决的问题
安全功能过少，租户安全需求难满足	能够提供丰富的安全功能
租户上云后，安全策略调试繁琐	能够提供流程化、自动化的安全功能配置
租户无法管理购买的安全服务	能够提供独立的租户安全子管理界面
缺少租户安全可视界面	能够提供独立的租户业务安全可视界面
目前安全增值能力较弱，仍无法持续运营	通过将安全服务化交付，满足

三、政务云云安全资源池方案

温州市政务云安全资源池方案

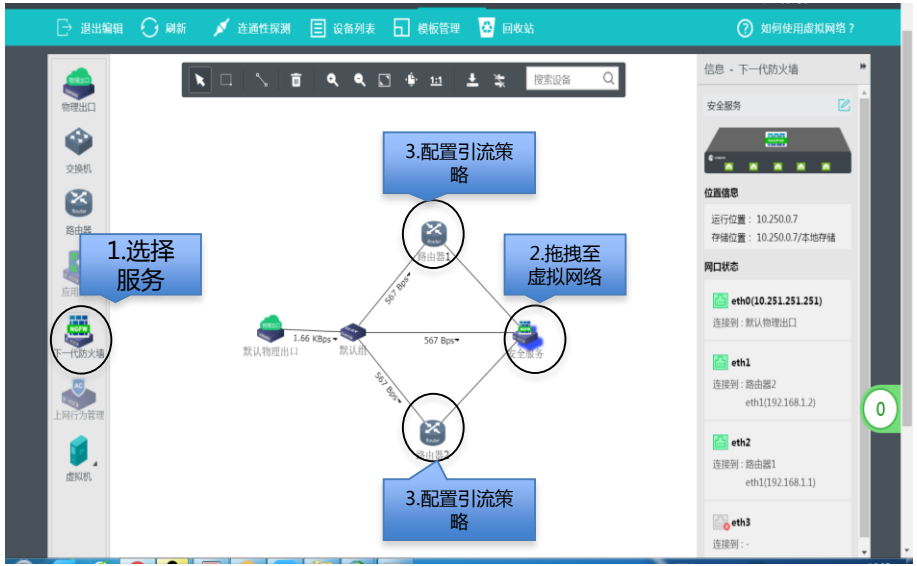


部署

- 需要在已有架构上实施，通过在出口设备上引流到云安全资源池
- 实施后，可以将原有IPS WAF设备下线，网络整体架构清晰
- 每租户的网关直接指向云安全资源池的独立的安全网关，同时使用NAT功能
- 跟据租户需求，匹配安全服务

扫码观看大会视频

温州市政务云安全资源池方案



为租户释放安全服务过程

租户侧自管理界面

扫码观看大会视频

目前温州政务云采用的安全服务包

提供安全运营报告、安全策略检测、加固咨询、威胁分析、渗透测试、远程应急响应、通报问题处理运营服务

提供业务可用性检测、资产暴露面、云端漏洞监测安全组件

提供堡垒机、数据库审计组件

提供web防护、网页防篡改、敏感信息防泄密安全组件

提供应用控制、防病毒网关、IPS功能

提供IPSEC VPN、SSL VPN、安卓/IOS/windows安全接入SDK等多种安全接入组件

扫码观看大会视频

云安全资源池为政务云带来的价值

功能全面	租户安全自管理	交付流程简单	权责划分清晰
安全接入：SSL 防御：IPS WAF 数据库审计 运维：堡垒机 多重服务包组合售卖满足不同租户需求	租户在购买安全服务后，可以独立管理安全服务，如配置vpn用户，配置WAF、IPS策略。 租户业务安全可视	图形化交付流程 租户购买安全服务后，通过鼠标拖拽即可完成交付	电信负责平台安全以及租户安全资源池，租户关注自身业务安全 与租户侧操作系统、业务软件无任何耦合关系

2016 The Computing Conference

THANKS

SANGFOR
深信服科技