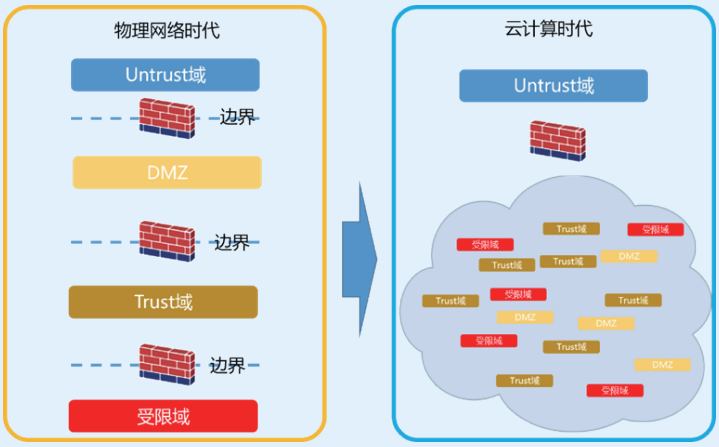
微隔离技术小贴士

云计算让传统安全手段难以适应

企业在选择私有云、虚拟化技术已经成为不可阻挡的趋势。但是云计算和虚拟化已经改变了传统的网络安全架构（见图1）。

相当长一段时间，企业内部通过划分安全域，做边界的防护来保证客户机、服务器的安全通信。比如DMZ区就放一些允许被外部访问的服务器，Trust域内的物理服务器可以互访，受限制访问域的服务器可以互访，而Trust域的物理服务器可以访问DMZ区域的物理服务器。这些区域间有可能是物理隔离的，或者是通过交换机和安全设备（一般是防火墙）提供安全域间的连接。在这些安全设备上配置的是白名单模式的策略，只允许符合规则的流量才通过，其它的都阻断掉。除了安全设备，还部署类似入侵防御系统来识别防火墙误放过的威胁。



但是，当云计算和虚拟化取代了以前的物理服务器、网络设备和网线，情况发生了变化。数据中心里，是以虚拟化环境中的一群虚拟机的形式存在的，物理边界消失了。尽管虚拟化环境中也还有物理服务器和其它设备，物理拓扑已经不再决定逻辑拓扑了。如果按照传统的概念，可能在一台物理服务器上的几十台虚机就分别属于多个安全域。怎么办?

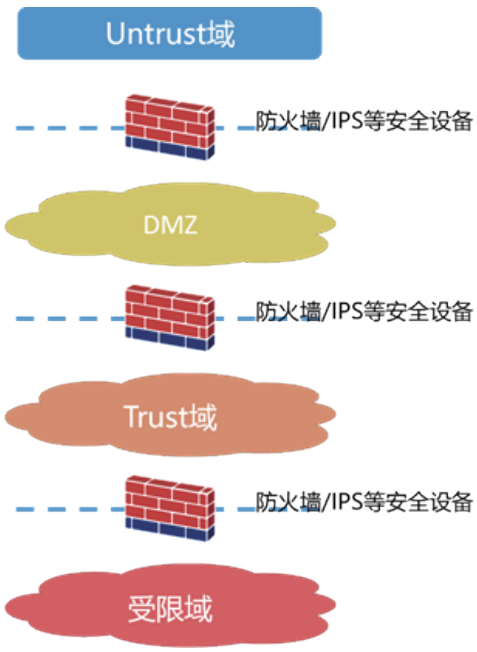
使用云计算和虚拟化的好处不言而喻，但不意味着风险可以被忽略。相反，终端间未授权的通信和攻击带来的风险更大，因此网络安全仍然会在虚拟化环境中发挥主要作用。

借鉴传统物理域的资源池划分

一些用户和厂家在借鉴传统的边界防护理念，只是在不同的安全域中采用虚拟化技术来建设，通过边界的安全设备如防火墙、IPS等设备做边界防护，阻断未经授权或不符合要求的流量。

这种粗线条的划分，对于一些经费充裕的客户是可以考虑的。他们可以忍受几台服务器组成一个小的计算资源池，买一套独立的虚拟化软件，上面只运行了不多的虚机。这种组网会带来的问题:

1、 成本高。
2、 虚机无法在多个资源池迁移，浪费有限的计算资源。
3、 无法限制云内部的安全威胁。
4、 管理上更麻烦。



微隔离——虚机的贴身保镖

微隔离（Microsegmentation）曾经是一个老名词，在云计算和虚拟化时代里有了新含义。虽然不同厂商在微隔离上的做法不同，都是要解决云计算中边界消失后，无法有效提供安全防护的难题，提供小到虚机级的防护，为虚机提供贴身保镖!

微隔离（Microsegmentation）这个名词诞生于网络交换领域。提出时恰逢以太网交换机面世，逐步取代集线器、同轴电缆等共享介质组网方式。在那个时代，微隔离指通过限制以太网的冲突域，来提升整个网络的性能，也就是从10Mbps共享到桌面（用HUB或者铜缆串接）发展到10Mbps交换到桌面。

在云计算时代，微隔离又有了新的含义，主要是指利用软件或者硬件的技术手段，在云计算或虚拟化环境中，划分更多逻辑上的安全域，形成逻辑的安全边界，实现访问控制、威胁检测与阻断、监控和审计等等安全功能。

微隔离是个新概念，不同厂家的技术背景不同，对云计算安全的理解不同，所以不同的厂家提供的微隔离方案在实现机理、功能上均不相同，解决问题的侧重点也不同。

从厂商维度看，微隔离产品技术方案分那么几大流派：云计算/虚拟化产品供应商、网络产品供应商、网络安全供应商和主机安全供应商。

从实现的技术方案维度看，微隔离产品技术方案又分以下几个流派：

- 用物理安全设备隔离虚拟化环境
- 主机代理
- 虚拟交换机隔离
- 基于Hypervisor的控制
- 不基于Hypervisor的网络安全方案

应该说不同的厂家实现思路不同，也有跨界的组合。

实现架构	安全控制方法	策略执行	环境依赖性	代表厂家
物理安全设备隔离虚拟化环境	独立安全设备进行安全域隔离	报文头、内容和行为做策略	不依赖	传统网络安全厂商
主机代理	在每个虚机上加载代理软件	对进出虚机流量，虚机内应用、内容进行控制	对虚机操作系统强依赖	主机安全厂商塞门铁克、趋势等
利用虚拟交换机的能力	在虚拟交换机（物理交换机）上进行控制，如 VLAN ACL	在虚拟网卡对虚拟机的识别和报文头做策略	取决于虚拟交换机能力	思科、vMware 微软等、开源系统
基于 Hypervisor 的控制	在 Hypervisor （通过 API）再加上虚拟机上安装的安全软件	在虚拟网卡上对基于虚拟机的识别、报文头或内容做策略	依赖虚拟化平台的 API	思科、vmware CheckPoint 、趋势、Juniper 等
不基于 Hypervisor 的网络安全控制	在一个虚拟机或外部物理设备上实现功能	在安全域或隔离边界上基于虚拟机的识别、报文头或内容做策略	不依赖虚拟化环境，需要引流	思科、山石网科、飞塔、IBM、Juniper 、Palo Alto

微隔离是个新技术领域，即使是每个分类各个厂家实现思路也不同，比如山石网科的山石云•格，就是一个不基于Hypervisor，采用全分布式架构的微隔离产品。

云计算是一个API驱动的技术，所以在微隔离技术领域里，并非是“非黑即白”，“有你没我”的态势。在微隔离领域不同的技术门派相互合作共赢将成为主流!

山石网科与云计算平台、虚拟化产品供应商的深度合作陆续展开!