“思科数据中心安全解决方案介绍”在线研讨会-精彩问答

序号	问题	回答
1	思科安全监测产品可以和其他国产安全厂商的产品联动吗	思科安全产品可以提供API，然后与国产安全厂商进行联动，国内我们也有这样的案例。
2	如果数据中心有WEB服务，国内很多采用WAF产品进行防护，我们思科是否有这方面的解决方案？还是用AMP的方案？	思科目前不提供WAF产品方案，数据中心我们建议Firepower NGIPS和WAF产品都进行部署，IPS更多针对平台、通用漏洞，WAF更多针对与WEB相关的安全问题。
3	思科的SDN网络leaf安全区域可以对同一硬件交换机下联的不同接口用户进行安全策略管控吗	思科在园区网及数据中心都有SDN方案，园区网用户可以通过交换机直接进行安全策略管控。
4	思科有虚拟服务器产品吗？或计划有？	思科有NFV类安全产品，FTDv下一代防火墙，ASAv防火墙以及其他安全产品也均支持虚拟化平台。
5	流量镜像和flow，对于流量可视化哪个比较好，还是两者可以同时使用？	流量镜像和flow各有好处。Flow容易部署，方便覆盖更广的区域。镜像能够看到更详的细数据包payload内容。通常两种方式要结合使用，例如：南北用镜像，东西用netflow。
6	可视化访问关系，会产生或输出表格统计信息吗	可以
7	传统中型制造业，以什么样的优先级建设数据中心的安全呢？管理层限制了投入总量……	制造业因为低利润对投入控制的非常严格。一方面，需要安全人员讲解给管理层安全是什么？风险是什么？出现风险带来哪些危害，特别是财务上的损失。这样才能通过合理手段来衡量安全的价值，增加安全投入。另一方面，在优先级建设上，核对资产，标识资产价值，对应进行合理的安全方案投入。

8	firepower 9300 防火墙有自动信息收集功能吗？	Firepower9300防护墙使用FTD软件就可以进行自动主机信息收集了。
9	在思科的经验或者产品实际使用中，特征库检测和行为检测拦截或发现攻击的比例是多少：多少比例是通过特征发现，多少比例是通过行为检测？	我们并没有专门进行这类统计。无论是什么比例，任何一方缺失，都将会导致特定风险缺乏防御手段，并可能导致客户无法挽回的损失。
10	EPG能直接在交换机上部署吗？配置EPG后交换机上的ACL是什么样的？还是EPG仅仅是上层服务抽象，交换机上依然是基于五元组的ACL？	可以直接在交换机部署，在交换机上至EPG直接的访问控制列表，已经不是IP五元组ACL
11	集中式防火墙很难应对数据中心内上T的流量吧？	东西流量很大的情况，可以考虑直接利用ACI的交换机通过EPG之间的filter来完成访问控制。
12	安全域-安全子域划分，并配置边界防火墙这样的策略，按经验最合适划分多少层：互联网出口、业务系统、服务器本身？或者还有其他更合适的做法？或者划分更细？	这个没有统一的说法，通常根据客户实际情况进行划分。划分原则一般是管理需求，资产重要性，业务部署位置以及合规要求等进行划分。
13	网络威胁如何更好的防范？	这个问题太宽泛，简单说网络威胁防范有很多方面，人员管理，流程，技术多个方面。技术上又有不同问题不同解决方法。针对威胁防御，通常会设计到威胁情报、特征技术及行为分析技术，而行为分析又分为异常检测及恶意行为检测等。