序号	问题	回答
1	请问Tetration Fire Wall可以理解为专为企业上云所推出的产品吗？	在“多云”环境下，安全分段和保护更复杂，Tetration的微分段技术更能帮助用户简化安全，产品本身既支持上云，也支持本地数据中心。
2	Netflow数据存在哪里？额外配置服务器进行分析还是本地处理？	收集的数据都保存在Tetration的服务器，不需要额外配置服务器做分析。
3	是否对虚机造成压力？	Tetration的Agent是很轻量级的，可以控制占用的资源比例，不会造成压力。
4	请问在Client安装Agent，这样会给Client Load带来负担吗？	Tetration的Agent是很轻量级的，可以控制占用的资源比例，不会给服务器带来影响，负载可控。
5	Tetration可以做到几层的防护，可以做到7层吗，能否取代7层防火墙在东西向流量的安全防护？	Tetration对应用进行自动分段，识别访问关系，自动生成策略，是基于四层的保护，要做到7层保护，需要使用思科NGFW。
6	Agent的安装支持哪些操作系统？会不会有支持死角？	Agent支持Linux，Windows，Aix，Container（K8s, Openshift）等主流的操作系统。
7	ACI也可以做微分段，Tetration和ACI的微分段有什么区别，两者该如何结合使用？	ACI基于EPG做分段，还是以Group为单位做的，Tetration是基于每个Workload做保护，二者可以结合。
8	漏洞关联分析会联动Talos吗？	漏洞关联是基于CVE库，Talos情报主要提供Hash和IP的保护。
9	SSL/TLS 流量如何采集分析？	Tetration并不是基于payload进行保护的，是基于workload的IP和端口进行保护，所以SSL/TLS对其没有影响。
10	微分段的后端是什么？	后端Tetration核心服务器软件。
11	从策略设置上有什么最佳实际方式吗？ 在几个维度上进行限制呢？	第一、通过自动学习生成白名单策略，第二、利用历史数据对策略进行测试，个别进行人工调整，第三、在visibility模式下运行一段时间，然后可以考虑进行Enforcement控制。 纬度的话有应用Cluser、IP、端口等。
12	学习过程涉及到测试环境和生产环境，测试环境没有办法一比一还原生产环境，学习到的策略是否能真的起到提高效率的作用？	Tetration的policy模式有两种：Visibility模式，只进行审计不做控制，Enforce模式，进行策略强制。可以考虑运行在Visibility模式下一段时间，等到策略都学习到了，再进行Enforce。
13	有下载试用版本镜像吗？	目前Tetration的测试需要联系思科的销售人员开展。
14	零信任和传统边界模式的成本差异大么， 在0-1部署过程种， 另外从现有边界模式迁移到零信任追加成本大吗？	零信任的核心是最小授权，涉及到人员、设备、网络、计算环境等方方面面。Tetration是主要实现计算环境的零信任，实现多云数据中心安全访问的最小授权。可以考虑分阶段进行，首先解决东西向流量的安全控制，局部应用成功后在推广。
15	零信任 - “永不信任、持续验证”在微分段上下文这种语境下如何理解？	零信任是方法论，涵盖了安全的整个架构。微分段是零信任在计算环境一侧的具体落地方法。目的是通过微分段，实现多云数据中心安全访问的最小授权。
16	Tetration架设在网络的那个位置？通过自主学习，进行策略管理，误判怎么办？	一般是架设在DC，自动学习后生成的Policy，可以通过历史数据进行测试验证，然后在visibility模式下运行一段时间，确保策略完整严谨，再进行Enforce。
17	Agent 是策略的实际执行者？还是另外有防火墙来执行？	Agent是很轻量级的软件，通过调用操作系统的防火墙引擎来工作，比如Linux的Iptables模块。

18	Tetration Agent都支持哪些操作系统运行？	Agent支持Linux，Windows，Aix，Container（K8s, Openshift）等主流的操作系统。
19	每一个容器，vm，服务器上都要购买防火墙吗？	每个Workload来算许可的，VM、服务器、容器都要计算许可。
20	请问这个Tetration的这个Sensor支持Linux部署吗？	支持各种主流Linux操作系统。
21	您好，能否对零信任，微分段这两个概念做个概括总结？零信任微分段的pros和cons。	零信任是方法论，涵盖了安全的整个架构。微分段是零信任在计算环境一侧的具体落地方法。目的是通过微分段，实现多云数据中心安全访问的最小授权。
22	对虚拟机的保护是否也是由iptables来执行？	对于Linux的虚拟机是通过iptables，对于Windows的虚拟是利用Windows自带FW模块进行。
23	Tetration是Agent，服务端是硬件防火墙，还是软件Server?	服务端是软件，并不是硬件防火墙。
24	策略下发之前, 是可连通的吗?	下发前都是连通的，下发了enforement的policy之后，才会做控制。
25	运行Agent需要提权到root吧？	是的。
26	这个系统需要部署哪些部件？	在操作系统上部署Agent就可以了，后台是Tetration服务器
27	我们是多云的环境，（public cloud,private cloud, container, openstack),网络架构有传统网络和ACI,根据你的讲解，我们如果进行tetration的部署测试，大的方面需要注意什么？	建议分阶段进行，第一阶段先选择合适的区域（应用），重点关注东西向访问的控制，比如ACI的EPG里面的访问控制，Contrainer中的Pod访问控制。第二阶段考虑扩展区域（应用）首先运行Visibility模式，学习到所有的访问策略，稳定后再进行策略下发。根据应用类型的划分，进行Workload的资产统计和上下文信息的导入，根据应用类型创建Scope（应用范围），对应的进行数据收集和策略学习、管理。
28	每个Agent是否有自身的安全保护机制，避免被恶意软件篡改，导致发送虚假信息？	Agent本身非管理员权限账号无法卸载删除，如果Agent被强行卸载删除，Tetration管理系统会监控到并告警。
29	EDR和这个有区别？	EDR是面向Endpoint，Tetration是面向Server端。
30	后台服务之间的连接关系如果是基于域名系统的，那么IP：端口一直在变化中，意味着在Agent学习并Update规则之前，通信会失败？	如果多个IP对应一个domain的话，这一组IP会被纳入到一个Cluser中，来学习策略，IP发生变化不会影响访问。另外Tetration对workload的管理也不单一依赖于IP，IP发生变化不影响策略的执行。