洞悉万千威胁，阻断分秒之间，选择最适合您的下一代防火墙

2017年7月27日

序号	问题	回答
1	什么是BYOD？	BYOD（Bring Your Own Device）指携带自己的设备办公，这些设备包括个人电脑、手机、平板等.
2	何謂更強的可視性?	不仅仅看到用户、应用、设备等等，还能分析到相关的漏洞和威胁。
3	思科漏洞库有谁来提供？	由思科Talos团队提供和维护，不仅有公共的漏洞库CVE，而且思科和很多相关的厂商有直接的合作。
4	FirePower是ASA的取代品吗？	Firepower 是思科定位为下一代防火墙系列，ASA定位是传统防火墙场景，所以两者并不是完全替代的。例如数据中心 更多使用的传统防火墙。
5	深信服的NGAF有没有这些功能？	可视化功能大家都有，但对可视化的威胁分析，这里思科有很多独到之处。例如应用漏洞的分析，威胁轨迹的跟踪等等
6	能监控企业内部发起的ss或vpn吗？前一页ppt没有提到这个方面	思科Firepower 防火墙可以支持SSLVPN 解密后的威胁分析，需要灌入SSLVPN私钥和公钥就可以实现。
7	请问能控制微信里不让发送文件、视频吗？	可以监控和分析微信行为，包括发送文件
8	請問針對工業用監控系統設備的可視化是否支援? 支援那些？	我们有专门的SCADA协议的威胁监控。
9	对于国内比较流行的应用，识别率高吗？	是的，支持国内常见的100多种应用。例如qq 威胁 支付宝等等

10	对app智能可视化识别还是需要手动进行信息录入来进行识别	我们可以直接设备移动设备，所以app 也是区分不同移动类型设备
11	分析意图吗	分析威胁意图，通过关联事件，直接提供感染指数进行快速定位
12	这个URL库是每年都要买，还是买一次就行？	URL 库一般是 1年 3年 5年的使用授权。
13	思科的下一代防火墙支不支持中文?	支持中文
14	SSL解密如何能保证用户的信息不被看到或泄露？	仅对威胁行为和数据建立过程进行安全分析
15	SSL是为了加密用户和服务器之间的流量的,NGFW作为用户和服务器中间的设备,解密ssl需要相应的前置条件吗?	可以通过灌入公钥和私钥 进行ssl解密
16	对IPSec能解密吗？	目前不支持
17	思科的SSL解密引擎是开放的吗？	SSLVPN 解密功能是思科firepower 防火墙里面的一个功能
18	跟其他品牌的有哪些优势？现在用的华为，最近发现很多红色警告信息，感觉被入侵了	优势很多，刚刚李老师也提到了，威胁是要防御的。我们对威胁防御的能力是业界最好的。
19	AMP文件检测需要另外的设备吗？	不需要，仅仅需要购买Firepower防火墙的AMP授权就可以
20	这个系统有IT基础的普通用户能够上手使用吗？还是必须招聘专业的思科工程师才行？	思科下一代防火墙 全面图形化界面，支持中文，同时加入很多的安全后台分析功能，减少人为分析工作量和专业能力。例如感染指数，安全策略推荐功能。

21	如何实现防御的智能化呢？或者说智能化呢？	智能化主要是指对于安全事件进行联动行为，例如发现一个威胁，Firepower 可以让ISE进行快速隔离。
22	公网的SSL解密如何实现？	灌入SSLVPN公钥和私钥
23	FirePower可以对用户访问互联网的行为进行定义吗？如通过定义访问策略允许哪些子网访问特定internet的url和协议	是的，可以。
24	https 的内容可以解密吗?	可以
25	支持 2-7層？	是的
26	对漏扫完后有相应的解决方案吗？	是的，可以通过分析后，提供针对的安全策略推荐
27	本页关于高危漏洞的预测来自哪里？	来自思科的Talos 安全情报分析团队
28	可取代IPS？	大部分功能可以取代
29	支付宝的流量都是加密的，防火墙也能够监测吗？	可以支持ssl 解密
30	下一代防火墙能加入杀毒软件引擎吗？	是的 可以支持AMP 恶意软件查杀功能
31	这个防火墙那可以做为代理服务器吗？	不可以，http 代理服务器，思科有专门的产品 WSA
32	数据处理能力怎么样？	10-240Gbps 不同的处理能力都有。

33	firepower 2100 和4100 对路由协议和VPN的支持，是怎样的？有什么区别吗？	路由协议和VPN都支持，2100和4100 都是思科的下一代防火墙，主要是性能和定位不同
34	对于访问日志的记录，firepower是和传统的ASA一样仅记录IP，还是可以记录域名	可以记录url，ASA也可以记录url，需要配置inpsect http 就可以实现
35	FirePower能兼容传统防火墙ASA的所有配置吗？例如我想用FirePower替换掉我现有的ASA，但是现存ASA的配置我要保留	的，我们有相关的迁移工具。
36	现有系统或应用增加本系统，能否实现不停机切换？	不停机切换，需要看您应用的连接方式，如果是配置调试完成，进行地址切换，可以尽量避免切换
37	此款产品适合多大的网络规模？	SOHO，分支，数据中心不同场景都可以支持
38	思科防火墙是如何实现ssl解密的？	ssl数据流的公钥和私钥的导入后，就可以分析
39	SSL 解密對Firepower 的效能影響有多大?	是的，添加SSL解密会对性能影响，具体型号的影响请查看产品Datasheet
40	歷史事件Data可追溯到多久前?是否可存放？或data都是即時的?	30天-60天，具体要看数据量，如果要追溯到几年前，需要外部存储。
41	支持沙盒功能吗？支持哪种类型的沙盒？需要购买那个授权？	支持，需要购买AMP 授权
42	支持外部数据库吗？	支持
43	可以定位到攻击源是谁吗？	是的，但如果是跳板机器。就需要进一步分析了

44	现网的5585可以升级到到Firepower防火墙吗	ASA5585 可以购买Firepower 模块实现
45	信息怎么存储？	本地磁盘或者外部存储
46	无线网络的射频入侵检测能识别吗？	我们无线AP 就自带IPS 功能。
47	快速响应和自动隔离主机,是默认启用还是需要自定义配置? 隔离之后的恢复策略是怎样的?	可以默认启动也可以手动，通过ISE 进行策略CoA 授权
48	如果威胁服务器和客户端建立ssl连接，我们没有服务器的私钥，还能解密数据信息吗？	不能
49	Firepower 防火墙上管理是不是必须要购买 Firepower Management Center呢	不是，有on box FDM 进行管理，但功能要少于FMC
50	firepower怎么拿到SSL的公钥和私钥？另外，SSL加密的数据都是用户的业务数据，用户一般也不希望思科防火墙能看到，这个矛盾怎么解决？	需要客户自己提供
51	还是本身设备自己就可以管理了 ？	设备本身包括FDM 管理功能
52	公网每个SSL站点都是不同的公钥和私钥, 也就是我想解密所有内网用户访问的所有SSL网站是不现实的 对吗?	需要客户自己提供
53	这个会跟 cisco 的 web security 有集成吗	目前不会
54	现网使用的ASA5585是否可以升级到具备Firepower功能的防火墙?	ASA5585 可以购买Firepower 模块实现

55	如果功能全开的情况下，性能会怎样？	思科Firepower 2100 系列开启全部功能没有任何损失
56	国内有云端服务器吗？	目前没有
57	这个跟电脑端的 AMP 会有集成吗	可以集成
58	沙箱如果不使用云端的，本地必须购买相应的设备是吗？ FirePower里不集成?	Firepower提供本地分析能力。
59	沙箱要授权吗	需要AMP 授权
60	5525-FWPR 和 之前 的 5525-IPS 能做failover 吗， 5525 - IPS 能升级到 FWPR吗	不能
61	可以直接作用于出口吗	是的
62	如果病毒是从内部产生的，firepower怎么处理？	如果内部vlan威胁，我们有专门的解决方案 Stealthwatch 实现
63	文件轨迹技术 是否需要配合其它技术才可正常工作？	需要购买AMP授权
64	遷移工具是指ASDM設定格式轉移到FTD格式嗎?	是CLI 转FTD
65	因为文件在主机之间传输可能根本没有经过防火墙, FW是如何监测轨迹的?	是的不能， 如果内部vlan威胁，我们有专门的解决方案 Stealthwatch 实现
66	文件的传递就能够被表示为恶意软件，那公司内的文件共享还能用？	是恶意文件传播，例如蠕虫

67	在企业DHCP环境下，IP地址是经常变动的，Firepower是通过IP地址来定位主机的么？如何能确保准确性？	建议结合AD 进行 ip 和用户身份的映射
68	问一下，防火墙部署在边界，在区域内部的报文也能捕获吗？还是需要通过端口镜像方式？	如果内部vlan威胁，我们有专门的解决方案 Stealthwatch 实现
69	ASA5585是否已停产？传统这块ASA5500还有那几款会继续提供销售？21、41、91现在是否都已可以正式下单？	ASA5585 没有停产计划，21 41 91 可以下单
70	内网的威胁试图在入侵其他主机的时候，只需要通过内网交换机就行。不会在进过防火墙了，下一代防火墙如何阻断它呢？内网如果使用的是不同品牌的交换机呢？	如果内部vlan威胁，我们有专门的解决方案 Stealthwatch 实现。通过netflow/sflow 进行流量分析。一样可以通过ISE 进行联动。目前联动可以通过下推VLAN 和 ACL shi'x
71	你们的这个检测技术有和哪几个厂商的对比过？	是的，具体可以参考我们网站的信息
72	问一下， 部署的时候是旁路还是串接，如果是串接，是否只能检测流经的数据流量？如何检测病毒或程序在内部的传输？	支持旁路和串联，串联仅能做监控。 如果内部vlan威胁，我们有专门的解决方案 Stealthwatch 实现。通过netflow/sflow 进行流量分析。
73	请问，为什么3月/2017的 TTD反而拉高到16.3？这个数字是前个月 3.7的超过四倍之多。	这是因为恶意文件在那时出现较大的演进，可以看到紧接着的后续两个月思科Talos很快跟上变换，又将TTD拉回到非常低的水平。 思科对外公布的“均值TTD” 是过去一段时间的 平均值，思科2017年中网络安全报告 公布TTD 缩减为3.5 小时 ，是取 2016 年11月 到2017年5月 这段时间的数值。 行业的TTD 为100-200天
74	FMC 管理节点的授权 现在是不是已经免费了？	没有，目前有2设备版本 10设备版本 25设备版本
75	想问下：firepower的 所有设置 管理都再FMC 操作吗？ 而不是在ASA上 是这样吗？	建议用FMC，on box 包括一个管理工具FDM ，也可以管理。但功能较少

76	那用户要购买是的话，还是建议使用FMC进行管理吧	是的
77	我们思科下一代防火墙，我们的等级保护，能够符合要求吗？	是的
78	請問思科专门的SCADA协议的威胁监控內容是甚麼?	思科防火墙通过能够理解SCADA协议，并内置大量特征库，针对SCADA攻击进行保护
79	你们的ISE身份策略 和 统一身份有什么区别？	是一个意思
80	2100系列都能自动分配带宽吧	可以按照策略，匹配应用，IP，用户来分配带宽
81	集群是否所有型号的FP都可以支持？ 支持条件是什么	是的
82	ASA with FPWR 和 ASA with FTD有什么区别呢？	ASA with FPWR是通过在ASA上加在FPWR模块来完成高级安全防御，FTD中ASA和FPWR的代码全面集成，一套runing Image，做到了真正的数据包一次解包，完成各层检测
83	请问CCL层多台防火墙集群，防火墙跟防火墙的连接，需要通过交换机实现吗？	需要，防火墙实现多台集群，CCL通过交换机连接才能够在每台之间建立通讯，完成异步流量处理
84	防火墙支持哪些部署方式（桥接、路由等）	支持桥接、路由及IRB方式，IRB是指可以在桥接接口配置路由。通过此功能防火墙可以像L3交换机一样工作
85	对于firepower的log，r是和传统的思科防火墙ASA一样仅记录源和目的IP，还是可以记录域名	Firepower日志根据不同协议分为多种，它可以记录IP五元组、用户、应用、URL、文件名、文件尺寸等等信息，如果数据流是DNS请求，则会记录DNS请求域名记录及DNS响应域名及IP信息
86	思科下一代防火墙跟PA防火墙相比，哪些功能比较有优势	http://www.cisco.com/c/m/en_us/products/security/firewalls/competitive-comparison.html

87	请教下：新一代防火墙是网页版的还是软件版的，如果过滤了木马，能不能进行移	Firepower的FDM是通过网页版管理的，一旦检测到木马，可以直接将文件删除。
88	新一代防火墙是不是也相当于一款杀毒软件	Firepower有病毒的检测的能力，但超过普通杀毒软件的恶意软件检测能力。能非常有效的检测并隔离勒索软件。
89	文件在内网中传递不过防火墙，FP怎么知道文件传递路径的？	防火墙可以跟踪到穿越的文件传输，在内网中文件轨迹跟踪，通过AMP终端安全产品收集并发送给防火墙。
90	或者说文件传递要过FP	和上一个问题一致
91	思科的NGFW针对APT或者未知攻击也是通过沙盒来实现的吗	沙盒，及Talos通过大数据发现的情报信息，同时Firepower还是支持服务器流量分析，及服务器信息白名单，通过这些方法也能非常有效发明服务器遭受的APT攻击
92	firepower device manager 需要单独采购吗？还是和防火墙设备集成的？ 谢谢	不需要，和防火墙集成在一起
93	URL 的分類,如果析別不出來 可以怎麼辦	目前URL的分类跟踪还是比较紧密的，很少遇到这类情况。如果个别分类不准确可以提交思科后台，或者通过URL手动建组来完成策略设定