全方位的安全保护，StealthWatch解决方案介绍		
2016年9月7日		
序号	**问题**	**回答**
1	内网用户如果成为肉鸡，如何能检测出？	内网用户被植入后门漏洞或者变成被操控的肉鸡，都可以通过思科StealthWatch解决方案查看到，
2	netflow只能在思科路由器上使用吗？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。如果有不支持flow协议的交换机我们还可以通过FlowSensor设备进行流量SPAN分析。
3	從FLOWCOLLECTO收集的的資料可以分析HTTPS資料嗎?	HTTPS加密信息我们可以通过思科FirePower下一代防火墙进行分析
4	镜像的这些流量是原始数据吗？	如果通过SPAN 把流量镜像到FlowSensor设备，这些数据就是原始数据
5	是不是只有新的cisco设备才有follow功能 ？ 或者说什么样的型号支持follow ？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。如果有不支持flow协议的交换机我们还可以通过FlowSensor设备进行流量SPAN分析。思科的大部分交换机和路由器都支持Netflow协议。
6	在Router及Core 上開啟NETFLOW功能後, 在LANCOPE上勢必會有收到重覆FLOW的問題, 面對這個狀況LANCOPE會如何處理呢?	我们会优化处理，对重复netflow会进行整理和汇总
7	針對同一個LAN的FLOW (未經GATEWAY的傳輸) Layer 2 switch的netflow也會產生FLOW訊息嗎??	是的，可以支持layer2 netflow
8	請問它與思科的防火牆間的聯防是自動阻擋嗎？	是的，自动推送策略

9	请问StealthWatch的解决方案跟思科较早前的Sourcefire的AMP方案有什么区别?思科的策略是否全部转向StealthWatch了？	Sourcefire是我们下一代入侵检测产品，通过特征码、漏洞库进行安全检测和匹配，主要部署在网络边界。StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow 流量分析，而不用更新特征码实现。
10	支持flow协议的网络设备列表有么？	可以通过链接获得 www.cisco.com/go/netflow
11	我想询问下，任何的交换机和路由器都能帮助我们发现内网中发生的问题吗？还是只有思科的相关设备才能呢？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。如果有不支持flow协议的交换机我们还可以通过FlowSensor设备进行流量SPAN分析。
12	老师刚才说的跨VLAN后，如果本地转发，只能看到80%的信息，什么意思？所有设备需要在一个VLAN？	基本的网络架构分为接入层 汇聚层 核心层，这里指如果接入层没有开启Netflow 功能 将确实20%的流量可视化能力。
13	开启Netflow会占用带宽吗？一个FC一般可以支持多少个Netflow流？	Netflow一个数据包48个字节，而且不是实时发送，会有数据收集缓冲时间，所以基本不会影响交换机带宽。依据不同的硬件型号我们有5000-250000多种不同处理性能的产品
14	您好，我想再问您一个问题，小型企业自己建立的公司网站也会遭到DDOS或CC攻击，请问怎样的硬件组合会利于网站服务器安全和流量优化，减少响应时间？	可以通过我们的FirePower下一代防火墙和StealthWatch解决方案实现。
15	必须集成思科的产品吗，交换机路由器等？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。
16	这个产品跟sourcefire 配合还是 独立的体系？ 思科对于sourcefire以及这个产品的发展战略是？ sourcefire 的部署也可以实现这些功能。 flow启用对性能影响大么？	Sourcefire是我们下一代入侵检测产品，通过特征码、漏洞库进行安全检测和匹配，主要部署在网络边界。StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow流量分析，而不用更新特征码实现。Netflow一个数据包48个字节，而且不是实时发送，会有数据收集缓冲时间，所以基本不会影响交换机带宽。

17	您好，我看了今年思科2016年中网络安全报告，结合实际，今年的勒索软件确实比较活跃，请问对于中小企业怎样有效的避免被攻击或者及时防御？	我们提供一个完整的解决方案应对勒索软件问题，可以采用ESA邮件安全网关+FirePower下一代防火墙+StealthWatch内网安全分析，结合这三类产品可以完整防御勒索软件的发生。
18	如果交换机是非思科设备，能支持你这个解决方案吗？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。
19	您刚刚提到过：需要在网络里的交换机、路由器启用flow或者netflow的功能才行。那么这个flow的功能是业界标准的吗？还是仅仅思科的产品才支持？	我们支持业界标准的Sflow 也支持思科自己的netflow，所以可以在多厂商环境中部署。
20	有虚拟机测试吗	可以提供虚机测试，请联系思科的代理商或者销售团队
21	如果一个交换机的流量是40G的吞吐，那么发出来的NetFlow是几个G？	Netflow一个数据包48个字节，而且不是实时发送，会有数据收集缓冲时间，所以基本不会影响交换机带宽。
22	那怎么保存长达3年的netflow信息，供未来查询？保存在哪里？	内部存储或者外挂存储都可以
23	sourcefire和Steal有什么区别，功能上	Sourcefire是我们下一代入侵检测产品，通过特征码、漏洞库进行安全检测和匹配，主要部署在网络边界。StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow 流量分析，而不用更新特征码实现。
24	支持flow协议的设备传输的数据包头，那么是如何去防护蠕虫、木马等安全问题的，是从软件特征码方面出发的吗？	StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow 流量分析，而不用更新特征码实现。
25	漏洞库是自己导入的还是现成的？	StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow 流量分析，而不用更新特征码实现。所以不需要导入漏洞库。

26	老师，trustsec是ISE新的功能吗？	TrustSec是思科可信化网络安全架构,包括ISE准入控制解决方案，MACSec二层加密功能等等，更详细的信息见链接 www.cisco.com/go/trustsec
27	有哪几种授权	StealthWatch的授权主要是指Flow数量的授权
28	老师，生成的flow信息的安全如何保护？？	Flow也同样有加密和认证模式，例如netflowV9可以设置加密和认证源
29	我理解这个方案部署之后需要有一个学习生成安全事件库的过程。那么贵公司是否有什么方式方法帮助客户更新这个库。类比杀毒软件公司的病毒库。SMC是否有这个情况。	StealthWatch与很多威胁防御产品不同的是通过用户的行为进行安全判断，也就是说我们有100多种安全分析算法进行flow 流量分析，而不用更新特征码实现。
30	可以管理上网用户的上网行为吗？	上网行为管理建议在边界部署思科下一代防火墙FirePower系列