讲解CiscoCatalyst交换机如何防御蠕虫困扰思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_AE_B2_E8_A7_A3Cisc_c101_644519.htm 下面说一下Cisco Catalyst交换机上的一个独特解决方案，以一种非常经济、有效和可扩展的方式来防范蠕虫病毒的危害，这大大的节省了许多公司的损失。 让很多服务运营商和企业网络的管理员甚为头疼的不仅是其不断的发展变种，而且发作造成的损害也越来越严重。尽管蠕虫本身通常并不破坏任何的数据，但它所带来的直接和间接的破坏使得网络和系统拥塞。 受感染的端系统的计算资源会受到严重影响，而病毒的传播则消耗大量的链路带宽，更可怕的是网络基础设备受到影响而造成网络的不稳定甚至瘫痪。以SQL Slammer为例，发生感染传播高峰时造成的平均包丢失率为20%。 网络的不稳定引起了银行ATM自动提款机不能工作，航空公司的售票系统瘫痪，仅仅两天的时间，就有30万台主机感染了SQL Slammer，造成的损失达数十亿美元。今天的企业越来越多地把关键业务应用、语音、视频等新型应用融合到IP网络上，一个安全、可靠的网络是企业业务成功的关键。 而企业网络的内部和外部的界限越来越模糊，用户的移动性越来越强，过去我们认为是安全的内部局域网已经潜伏着威胁。我们很难保证病毒不会被带入我们的企业网络，而局域网的广泛分布和高速连接。 也使其很可能成为蠕虫快速泛滥的温床。如何应对现在新的网络安全环境呢？如何在我们的局域网上防范蠕虫，及时地发现、跟踪和阻止其泛滥，是每个网络管理人员所思考的问题。 也许这是一个非常大的命题，事实上也确实需要一个系统的、协同的

安全策略才能实现。从网络到主机，从核心层到分布层、接入层，我们要采取全面的企业安全策略来保护整个网络和其所连接的系统。 另外即使当蠕虫发生时我们要有措施将其影响尽量缓解，并保护我们的网络基础设施，保证网络的稳定运行。本文将介绍Cisco Catalyst交换机上的一个独特解决方案，以一种非常经济、有效和可扩展的方式来防范蠕虫病毒的危害。 首先我们要了解蠕虫的异常行为，并有手段来尽早发现其异常行为。发现可疑行为后要能很快定位其来源，即跟踪到其源IP地址、MAC地址、登录用户名、所连接的接入层交换机和端口号等等。要搜集到证据并作出判断，如果确是蠕虫病毒，就要及时做出响应的动作，例如关闭端口，对被感染机器进行处理。 但是我们知道，接入层Cisco Catalyst交换机遍布于每个配线间，为企业的桌面系统提供边缘接入，由于成本和管理的原因，我们不可能在每个接入层交换机旁都放置一台IDS设备。如果是在分布层或核心层部署IDS。 对于汇聚了成百上千个百兆/千兆以太网流量的分布层或核心层来说，工作在第7层的软件实现的IDS无法处理海量的数据，所以不加选择地对所有流量都进行监控是不实际的。怎么能找到一种有的放矢、行之有效而又经济扩展的解决方案呢？利用Catalyst接入层交换机所集成的安全特性和 Netflow，就可以做到！ 发现可疑流量。 我们利用Cisco Netflow所采集和输出的网络流量的统计信息，可以发现单个主机发出超出正常数量的连接请求，这种不正常的大数量的流往往是蠕虫爆发或网络滥用的迹象。 因为蠕虫的特性就是在发作时会扫描大量随机IP地址来寻找可能的目标，会产生大量的TCP或ICMP流。流记录里其实没有数据包的载荷 (payload)信息。这

是Netflow和传统IDS的一个重要区别，一个流记录里不包含高层信息，这样的好处则是可以高速地以硬件方式处理，适合于繁忙的高速局域网环境。 通常部署在核心层和分布层的Catalyst 4500和接入层Cisco Catalyst交换机都支持基于硬件的Netflow。所以Netflow不能对数据包做出深层分析，但是已经有足够的信息来发现可疑流量，而且不受“ 0日 ”的局限。如果分析和利用得当，Netflow记录非常适用于早期的蠕虫或其他网络滥用行为的检测。了解流量模式的基线非常重要。例如，一个用户同时有50-100个活动的连接是正常的，但是如果一个用户发起大量的(例如1000个)活动的流就是非正常的了。 追踪可疑的源头。识别出可疑流量后，同样重要的是追踪到源头(包括物理位置和用户ID)。在今天的移动的环境中，用户可以在整个园区网中随意漫游，仅仅知道源IP地址是很难快速定位用户的。而且我们还要防止IP地址假冒，否则检测出的源IP地址无助于我们追查可疑源头。另外我们不仅要定位到连接的端口，还要定位登录的用户名。 编辑特别推荐: 关于思科认证考试的注意事项 Cisco认证总结CCNA重难点 思科认证考试形式介绍 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com