

保障系统安全的网络管理工具 PDF转换可能丢失图片或格式
，建议阅读原文

https://www.100test.com/kao_ti2020/274/2021_2022__E4_BF_9D_E9_9A_9C_E7_B3_BB_E7_c67_274990.htm 在中小型企业中，负责管理网络的管理人员一般同时也是保障网络安全的人员。同样地，安全管理和网络管理的要求也就融入到网络操作的一个更加宽广的领域中。网络管理工具数量繁多并且价格不菲，不过更多的管理人员已开始认识到使用这些工具来促进安全的价值。然而，使用网络管理工具增强安全性对多数厂商来说是一个崭新的概念。大多数管理工具在跟踪网络接口、服务器进程和网络数据统计等方面做得还是不错的。不过，通过选择合适的工具并且将其用于保持网络安全，你就可以从网络管理工具中得到最大的好处。知道你正在找什么 在对网管工具进行调查研究时，需要记住最好的工具有三个关键特征：一个简单的界面：你所需要的所有信息应该在一个界面上，你不应该在不同的屏幕之间切换。对于任何一个需要看到这些信息的管理人员来说，这个界面应是基于Web的并且是可以定制的。通过给系统超级用户、管理人员和部门领导等一个定制的他们可以依赖的视图，这些工具可以成为对你的网络操作的另一套监视器。识别正常的操作的能力：大多数安全相关事件发生于你网络的正常操作参数之外。你的网管工具必须能够找出正常通信与非正常通信的不同来，并且它还能够正确地报告这种信息。可作为行动依据的信息：如果你打算用某个工具管理网络的安全，就必须能够按照从某个屏幕上获得的信息采取行动。换句话说，你应该能够检测相关的安全事件，并且使用相同的工具来处理问题。找到恰

当的工具在不同的时点上，笔者用过几个最著名的工具，其中包括HP OpenView, SolarWinds Network Management Toolset, 以及 Cisco Network Management Toolkit。这些都是可行的选择，不过笔者还是推荐你使用Concord Communication的SPECTRUM suite of solutions。SPECTRUM提供了一个简单的基于Web的“一次单击”界面，并且可为多种用户定制。使用SPECTRUM你可以构建你网络的正常通信模式，并可以提供这种通信的多种报告，而且在某些不正常通信发生时可以收到有关的通知信息。此外，SPECTRUM界面提供的信息是相当有意义的。它允许你进一步探究问题并且找到一个快速的解决方案。例如，一家公司最近请笔者去解决其网络中的性能问题。使用SPECTRUM，笔者就能够快速地发现原来是病毒正在消耗绝大多数的网络带宽。这是一个大型的网络，不过SPECTRUM能够识别被感染计算机的MAC地址，而且可以关闭交换机的相应端口。一旦SPECTRUM确认通信模式不正常，笔者就用其内置的事件关联工具来阻止病毒感染企业的整个网络。

结束语在当今的公司环境中，预算和人员受到高度的限制。如果你的网络管理工具不能识别出你网络的正常通信，那你应该找另一个工具试一试。不管你为你的网络选择了什么网络管理工具，它还必须能够提供安全管理功能。选择恰当的双用途网络管理工具，你就会有更多的时间来投身到保障网络安全的工作中去。

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