

Cisco采取措施阻断来自Web和E-mail攻击 PDF转换可能丢失
图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/251/2021_2022_Cisco_E9_87_87_E5_8F_c101_251102.htm Cisco公司将在防火墙中加入对恶意程序和垃圾邮件的检查，使用的技术来自它最近收购的IronPort System公司。五角大楼上周遭到了基于E-mail的攻击，这次攻击造成国防部1500台电脑无法联网。正值五角大楼刚刚摆脱攻击之际，Cisco公司提出了对付此类攻击的战略规划。Cisco公司透露，它将在防火墙中加入新技术对恶意程序和垃圾邮件进行检查，这种防火墙既可独立运行，又可嵌入其他网络设备中。防火墙将使用Web和E-mail检测技术，此项技术来自Cisco以8.3亿美元收购的IronPort Systems公司。对于宣称世界上商业防火墙中每三款就有一款是自己制造的Cisco而言，这是值得记录的一笔，特别是在安全领域持续进行残酷合并的形势下。包括Cisco，Hewlett-Packard和IBM在内的技术供应商都争相把外来的安全技术尽快融入到自己的产品和服务中。Cisco已经针对IronPort的技术制定了庞大的计划，其中包括在Cisco的防火墙和IronPort的E-mail、Web网关之间建立通信链路，以图在网络边界上先发制人地消除IT安全威胁。Cisco计划使用IronPort的SenderBase服务来进一步扩展它的“自我防御网络”战略，该项服务是一个收集了世界上超过10万个ISP（互联网服务提供商）、大学和企业信息的数据库。到2008年初，Cisco希望能建立起Cisco的防火墙和IronPort的E-mail、Web网关之间的通信链路，达到完善网络流量检测功能的效果。Cisco宣称占有38%防火墙市场，它的防火墙用户可以通过软件升级享受这次与IronPort整合的新

成果，而不必购买新的防火墙设备、路由器或者交换机。Cisco将首先完成SenderBase数据库与Cisco的ASA系列防火墙之间的通信，但是最终公司将使所有出售的防火墙产品都能使用SenderBase数据库的数据，包括路由器和交换机中的嵌入式防火墙。Cisco安全技术部总经理、高级副总裁理查德帕莫说，“这一技术使自我防御网络的概念更上一层楼，它采用分布式共享的方式共享恶意发信人的信息。”SenderBase数据库通过测定不同IP地址发出的网络流量状况来决定IP地址的信誉。数据库根据一些要素记录IP地址的信誉得分，例如，它们已经存在多长时间；在一段时间内它们是否不断发送相同大小的E-mail或者其他网络流量；IP地址能否接收E-mail流量（垃圾邮件地址通常是不能接收的）；IP地址是否已经在黑名单中。前IronPort公司CEO、帕莫管辖下的IronPort业务部新任经理斯科特韦斯说，“不规则的跟踪是保护我们的网络免遭新式攻击的最佳途径。”SenderBase数据库记录的信誉得分告诉网络安全设备在检查某一网络流量时应给予的重视程度。SenderBase数据库对网络上任何活动的E-mail或Web服务器测量了超过110个参数，以决定一个E-mail、即时信息、或Web流是否构成安全威胁。每天数据库要接受来自IronPort网关设备的超过50亿次查询，这些网关安装在它的用户设备上。那些等待惠普和IBM更深入的加强网络安全的IT运营商也看到了希望，因为惠普上周说它计划收购Web程序安全提供商SPI Dynamics公司，而IBM最近则宣布将通过收购Watchfire公司增强Web程序安全供应。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