白皮书

Cisco 威胁防御软件包

为中小型企业提供全面的威胁防御系统

网络面临的攻击越来越多。此外，无论是接入时遇到的exploit攻击，还是网络本身的蠕虫问题（如SOL Slammer 或Blaster），攻击者每发动一次攻击所带来的损失都在大幅上升。通过传统工具（如防火墙和路由器等）提供完整的网络安全解决方案非常困难，因为各种应用已经变得越来越分散。现在整体网络安全解决方案都应该能够检测并防止已知和未知的攻击。网络防御必须从传统的被动方式转变为主动方式，从而在最短的时间内对攻击予以反击。

Code Red、Nimda、SQL Slammer 和 Blaster 蠕虫对互联网和企业局域网都有着重大影响。每个攻击都可以找到进攻网络的途径，IT员工在清除蠕虫，降低蠕虫所带来的影响时，会耗费大量的时间。并且永远都有即将出现的下一个蠕虫。

当企业网络受到这些蠕虫的影响时，中小型网络同样也受到了严重的影响，并且清除病毒所需的时间也更多。现在，有效消除这些攻击的技术已经发展成熟，思科向中小型企业（SMB）推出了捆绑网络入侵检测系统（NIDS）和主机入侵检测保护系统（HIPS）软件的 Cisco 威胁防御软件包。

网络入侵检测

抵御蠕虫进攻的第一道防线就是网络入侵检测系统（NIDS）。该设备能够识别网络数据流中是否有蠕虫，并且在进攻者到达终端目标之前将其阻拦。根据签名对网络数据流进行分析后，Cisco NIDS可以通知系统管理员网络中出现了蠕虫，并且终止蠕虫与遭到攻击的系统之间的通信。Cisco NIDS数据库包括SQL Slammer、Blaster等大量蠕虫使用的 Exploit 签名。通过监控企业 LAN 或 DMZ，Cisco NIDS Sensor 可以识别攻击蠕虫，并且能通过几个响应操作，成功地防止它攻击目标主机。

Cisco 威胁防御软件包提供灵活的部署选择，路由器既可以部署设备感应器，也可以部署网络模块。

图 1
Cisco IDS 4215 Sensor

图 2
Cisco IDS 网络模块

Cisco IDS 4215 是单机架式（RU）、随时可联线的设备传感器，可提供 80 Mbps 的全功能入侵保护，监控 T1 和 T3 环境（图 1）。

除了提供传统的 NIDS 传感器设备外，Cisco 还推出了 NIDS 模块（图 2）。这些模块能够匹配 Cisco 2600XM、2691、3660、3725 和 3745 路由器的网络模块插槽，并且提供与路由器紧密集成的功能强大的IDS传感器。该模块克服了传统NIDS解决方案不能检测加密数据流的弱点。各种形式的加密数据流在SMB网络和分支机构中很普遍。由于Cisco接入路由器可以对IPSec和通用路由封装（GRE）隧道进行解密，所以在路由器中集成 NIDS 模块可以对该数据流进行检测。

NIDS 可以根据攻击中使用的 Exploit 签名识别攻击，但是可能出现良性数据流被 NIDS 引擎错误解析，并且最终导致错误告警的情况。该技术可以获得 NIDS 传感器生成的告警，并且自动使该告警生效。Cisco Threat Response 服务器与 Cisco IDS 传感器一起操作，先验证告警，然后使告警生效。生成告警后，Cisco Threat Response 将立即检查攻击的目标系统。它将调查该系统是否能够抵御该攻击，如果能够抵御的话，那么在成功发起攻击时是否能够采取响应措施。

主机入侵防御

在终端部署一个主机入侵防御系统可以提供蠕虫和病毒保护。HIPS 对使用系统策略数据库的主机的流程进行监控。Cisco Security Agent 主要从其他方向接近攻击，而不是只注重探测阶段所见到的攻击。Cisco Security Agent 注重操作行为，以此来预防对主机的恶意攻击。不管是什么攻击，如果关注操作行为，就可以检测并阻拦任何破坏活动。

Cisco Security Agent 使用预先定义和用户定义的安全策略来决定是否允许采用某种特殊操作或行为。这些策略保存在与 Cisco VPN/ 安全管理解决方案(VMS)（CiscoWorks 软件套件的一部分）紧密集成的中央管理控制台上。Cisco Security Agent 管理控制台提供一个中央位置，当管理器被轮询时，Cisco Security Agent 就在该位置定义和下载策略。在默认情况下，Cisco Security Agent 将提供预先定制的策略来预防最常见的恶意攻击。恶意攻击（通常是不受欢迎的）不需要（或者在很少的程度上需要）对 Cisco Security Agent 进行环境调整。对于部分要求接入系统资源的应用而言，系统呼叫是被 Cisco Security Agent 拦截的，该设备然后将把这些呼叫与高速缓存的策略进行比较。Cisco Security Agent 将这一特殊的 OS 呼叫与该应用或程序生成的其他呼叫关联起来，并将这些事件关联在一起检测恶意攻击。如果该请求没有违反策略，它可以通过设备中心，并在此实施。如果该请求违反了策略，那么它将被阻拦，并生成一个告警，然后从代理设备上发送到Cisco Security Agent 管理控制台上。

Cisco VMS

部署 IDS 和 IPS 需要能够管理 IDS 传感器和 IPS 代理策略。要从这些设备上捕获告警，然后使其与中转的信息关联起来，这在快速识别和响应潜在的安全事件中具有十分重要的意义。Cisco VMS 允许网络管理员能通过单个共用接口部署多个主机上运行的 IDS 传感器和 Cisco Security Agent。Cisco VMS 简化了整个网络上的这些设备和代理的配置及管理。此外，Cisco VMS Security Monitor 还提供一个特殊接口，可以获取来自这些代理和设备的告警，使网络管理人员能够更详细地对这些告警进行调查。

通过将 Cisco IDS 传感器、NIDS 网络模块、Cisco Security Agent、Cisco Threat Response 软件和 Cisco VMS 套件软件相结合，Cisco 为 SMB 提供了必备的工具，用来查看网络，识别攻击，以及对这些攻击进行正确的响应等。这些工具的组合使 SMB 网络人员能防御网络攻击，从而保证公司业务的安全。

订购信息

表 1 列出了 Cisco 威胁防御软件包（Cisco Threat Defense Bundles）的相关订购信息。

表 1 Cisco 威胁防御软件包（Cisco Threat Defense Bundles）订购信息

部件编号	产品描述
IDS4215-CSA-BUN-K9	Cisco Threat Defense IDS 4215/Cisco Security Agent 软件包 • 1 个 Cisco IDS 4215 电器传感器 • 1 个 Cisco Security Agent 服务器 • 10 个 Cisco Security Agent 桌面代理 • Cisco Threat Response 软件 • Cisco VMS-Basic
NM-CIDS-K9-CSA (系统) NM-CIDS-K9-CSA= (备件)	Cisco 威胁防御 IDS 网络模块 / 思科安全代理（Cisco Security Agent）软件包： • 1 个用于 Cisco 接入路由器的 Cisco IDS 网络模块 • 1 个思科安全代理服务器（Cisco Security Agent Server） • 10 个 Cisco Security Agent 桌面代理 • Cisco Threat Response • Cisco VMS-Basic
CON-SNT-IDS4215B	支持 IDS4215-CSA-BUN-K9 的 Cisco SMARTNet® Support
CON-SNT-NMCIDSK9	支持 NM-CIDS-K9-CSA 的 Cisco SMARTNet Support

出口信息

Cisco 威胁防御软件包受出口控制。详细情况请参见出口法规网站：http://www.cisco.com/wwl/export/crypto/

如有特殊疑问，请联系：export@cisco.com

附加信息：

如需了解有关思科入侵保护系统的更多信息，请访问下列网址：

http://www.cisco.com/go/ids。

如需了解有关思科VMS (IDS 管理)的更多信息，请访问下列网址：

http://www.cisco.com/go/vms。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街一号东方广场东一办公楼19-21层
邮政编码：100738
电话：(8610) 65267777
传真：(8610) 85181881

广州
广州市天河北路233号中信广场43楼
邮政编码：510620
电话：(8620) 87007000
传真：(8620) 38770077

上海
上海市淮海中路222号力宝广场32-33层
邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

成都
成都市顺城大街308号冠城广场23层
邮政编码：610017
电话：(8628) 86758000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 **http://www.cisco.com**