xScreen Unified Threat Management (UTM)

技术白皮书

产品名称：xScreen UTM

文档版本号：5.0.0.0

第一篇

前言

随着网络攻击复杂性的增加，使用传统的防火墙和攻击检测技术，已经约来越难于保护网络的安全。现代的网络安全威胁来自于网络的各个层面，但更多的是来自于网络数据流量的数据部分，这一特性决定了仅仅使用防火墙或攻击检测系统，检查数据包的个别部分，已经越来越难于发现诸如病毒，蠕虫，后门程序，特洛伊木马等高级复杂的网络攻击行为。在很多成功的攻击案例中，黑客可以很快了解到网络在数据层面的安全漏洞，从而迅速使用病毒，蠕虫或者其他攻击行为，对网络资源造成不同程度的损害。随着 CodeRed、Nimda 等蠕虫病毒蔓延和爆发，整个安全业界和相关用户的关注重心逐渐转向如何防御应用层攻击，例如那些嵌入在邮件中的病毒和蠕虫等方面。下图说明了系统补丁时间和攻击之间的统计关系：

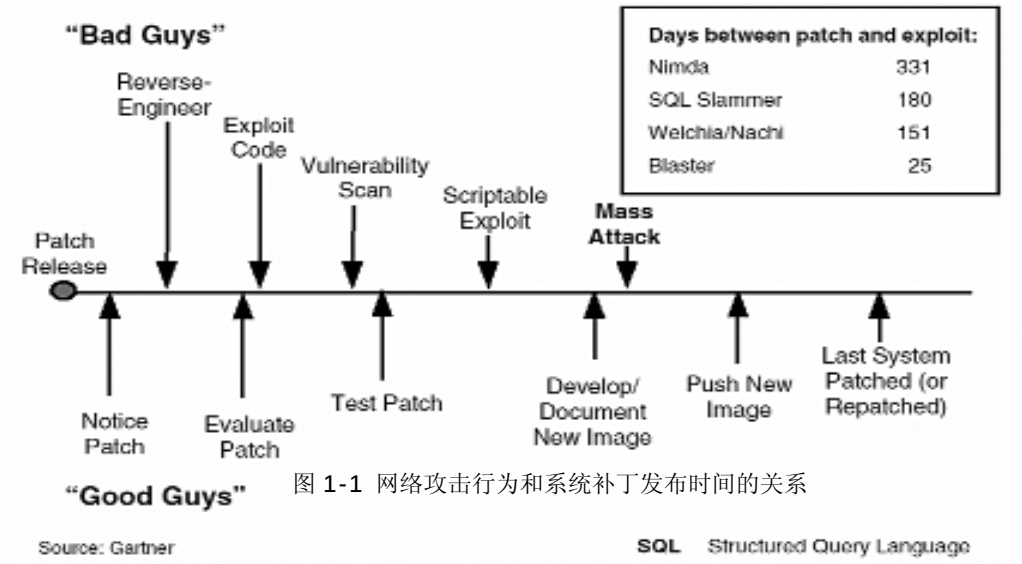

图 1-1 网络攻击行为和系统补丁发布时间的关系

另外一个吸引安全业界和用户眼球的安全问题也随着网络的普及而逐渐浮出水面——垃圾邮件；虽然垃圾邮件并不能与病毒、蠕虫那样具有明显的破坏效果，但是其影响却是长期而深远的。根据国内最近的垃圾邮件监控报告，平均每周大概产生 6 亿封垃圾电子邮件，假设人工处理每封邮件从而确认该邮件是否是垃圾邮件的作业需要 5 秒钟，这样每周就大概需要 3x1010 秒(8.4x105 小时)来处理这些邮件，如果按 30 元/小时来计算，那么光是鉴别垃圾邮件这一项，我们就要每周为此付出 25，000，000 元；如果在考虑浪费的网络带宽等其他因素在内，那我们的损失就不仅是这些了。

此外，由于垃圾邮件的泛滥，对于组织机构内部的资源消耗也是非常惊人的。华凯兴公司历经多年发展的、xScreen UTM 系列产品，是对网络进行实时多层次防护的最佳选择。xScreen UTM 系统采用先进的核检测技术，突破了网络数据深度分析的诸多难点，实时进行网络行为、内容和状态分析。

xScreen UTM 系统采用专有的易于管理的安全操作平台，包括了全套的安全服务——防火墙、VPN、入

侵检测/阻断同时还具有高效的应用层服务，如反病毒、内容过滤，垃圾邮件检测等多种功能，是一款All-in-One 产品的杰出代表，下图是 xScreen UTM 系统的架构说明图：

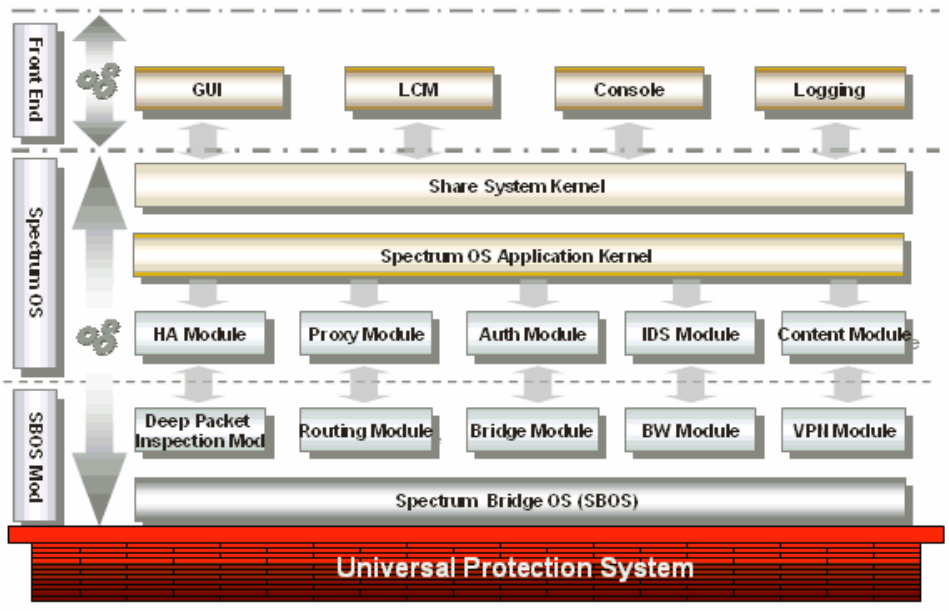

图 1-2 xScreen UTM 系统架构说明图

使用深度检测技术，保证了 xScreen UTM 系统，能够在网络的各个层面，对网络资源和数据实施防护功能。

第二篇

xScreen UTM 产品特点

稳定可靠

xScreen UTM 系列产品吸收了业界多年来在防火墙和 IDS 领域的设计和制作经验，硬件性能稳定可靠，软件功能丰富，网络适应能力强，是一款成熟的广受市场认同的 UTM 类型的主流网络安全产品。

卓越的网络及应用环境适应能力

支持众多网络通信协议和应用协议，如 802.1Q VLAN、PPPoE、802.1Q、Spanning tree、IPSec、H.323、MMS、RTSP、ORACLE SQL*NET、SIP 等协议，适用网络的范围更加广泛，保证了用户的网络应用。当 xScreen UTM 处于透明模式工作时，相当于一个二层交换机。这种特性使 xScreen

UTM 具有了极佳的环境适应能力，使用户无需改变网络拓扑结构，就可以实现全方面的安全解决方案，降低因为增加网络安全设备而导致的管理开销。

基于安全区段概念的安全策略

xScreen UTM 基于安全区段进行安全策略的定制和部署，将从接口层面的访问控制上升到安全区段层面。xScreen UTM 从体系结构上继承了传统防火墙的网络安全区段划分概念，也做了很多突破，它默认各个安全区段间的安全级别是一样的，它们之间的安全差异由用户来定制，为安全策略的定制和部署提供了很大的灵活性，同时也避免了僵硬的将网络划分为内部，外部和 DMZ 区的传统方式，使得用户能够进一步控制内部不同网络之间的安全区段。xScreen UTM 可根据企业的安全需求，将用户的整个网络划分为若干相互独立的安全区段，通过在这些安全区段间部署独立的安全策略，可以限制不同网络间的访问行为。

功能强大的网络控制描述语言

采用了基于对象的网络流量控制和描述语言，用户可以自行定义地址对象，服务对象，时间对象和访问控制行为，并且可以将已定义的对象分组；安全策略的描述基于对象元素，使之更加接近自然语言的描述方式，大大减少了维护和运营成本，让网络安全技术更加平易近人。

深度数据检测功能

采用了深度数据检测功能，以状态检测技术为核心，提供从链路层到应用层信息安全的全面控制。在链路层提供基于 MAC 地址的过滤控制能力。在网络层和传输层提供基于状态检测的 IP 分组过滤，可以根据网络地址、网络协议以及 TCP 、UDP 端口进行过滤，并进行完整的协议状态分析。下图是 xScreen UTM 系统的深度数据检测模型：

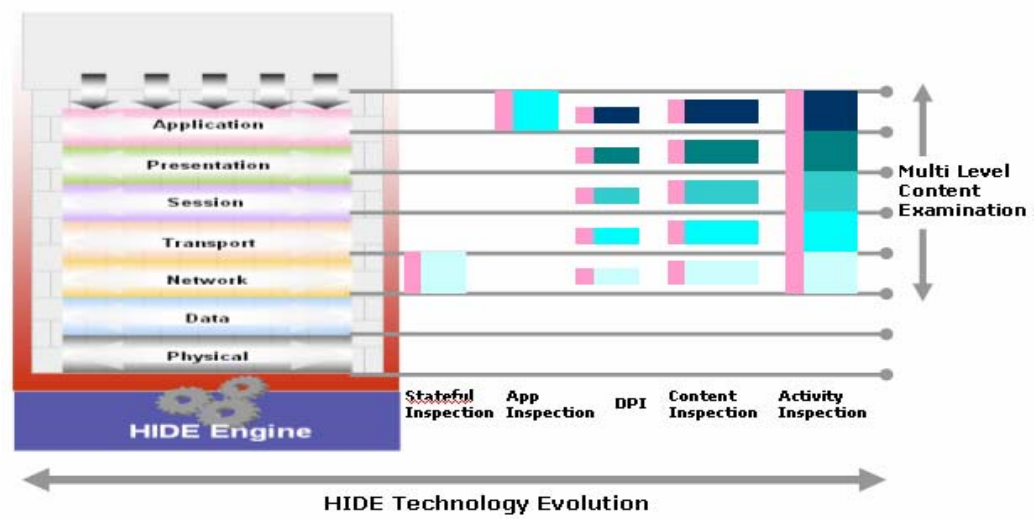

图 2-1 xScreen UTM 系统的深度数据检测模型

DoS防护

xScreen UTM 系统的网络协议栈能够自动屏蔽掉分片攻击，如 Ping of Death，Tear Drop 等，同时也能根据用户设置的 Anti-DoS 策略检测并防御以下类型的攻击行为，并提供攻击行为计数器和详尽的攻击记录日志信息：

- Land
- ICMP Flood
- UDP Flood
- Port Scan
- Address Sweep
- Syn-Flood。

提供基于IPSec协议、PPTP协议的VPN接入支持

基于 IPSec 协议的 xScreen UTM 完全兼容并符合 IPSec 标准协议，从而保证了和其它支持 IPSec 的系统相互连接，构建 IPSec 网络。支持手工和自动密钥（Pre-share key/X.509 CA 证书）两种管理方式，并支持 DES、3DES、AES、Blowfish、Two fish、Serpent 等多种加密算法和 MD5、SHA1、SHA2_256、SHA2_512 多种认证算法。

xScreen UTM 的 IPSec VPN 模块支持 IPSec 流量的 NAT 穿越、星型部署、动态对等方等多种部署方式，极大的拓展了 xScreen UTM 的应用范围，xScreen UTM 特有的透明模式下 IPSec VPN 部署使其更具有极佳的灵活性。

基于 PPTP 的华凯兴®xScreen UTM VPN 严格遵循行业标准，其 PPTP 支持 MS-CHAP 和 MS-CHAP V2 身份认证协议，同时支持 MPPE 40，128 位加密算法。

功能丰富的网络地址转换（Network Address Translation）

NAT 是网络设备必不可少的功能之一，xScreen UTM 提供丰富的 NAT 支持，支持 MIP 类型的地址映射、动态地址池的源 IP 地址转换、Conduit 方式的目标地址转换和 Round Robin 方式的服务器负载均衡。

Content Security引擎

xScreen UTM 系统的 Content Security 引擎，专门对邮件系统的 SMTP 和 POP3 协议数据流量，提供更高层次的安全防护功能。Content Security 可以对 SMTP 和 POP3 协议的邮件信息进行防病毒和垃圾邮件过滤处理，扫描邮件数据流中的病毒信息和垃圾邮件，同时对病毒感染或被确认为垃圾信息的邮件数据进行特定处理，xScreen UTM 支持的邮件处理方式包括：隔离，删除，警告，放行，拒绝接收等。

xScreen Global Manager 系统提供了系统处理邮件信息的审计分析功能，使得用户对网络内部流转的电子邮件情况有更全面了解，以便及时发现被病毒感染的主机，或封堵垃圾邮件信息。

xScreen Global Manager 系统提供了对多台 xScreen UTM 设备的病毒特征库统一升级的功能。用户可以在 xScreen Global Manger 系统中一次性升级多台 xScreen UTM 设备的病毒特征库，有效的减少了病毒升级的维护工作量。xScreen UTM 系统病毒和垃圾邮件处理示意图：

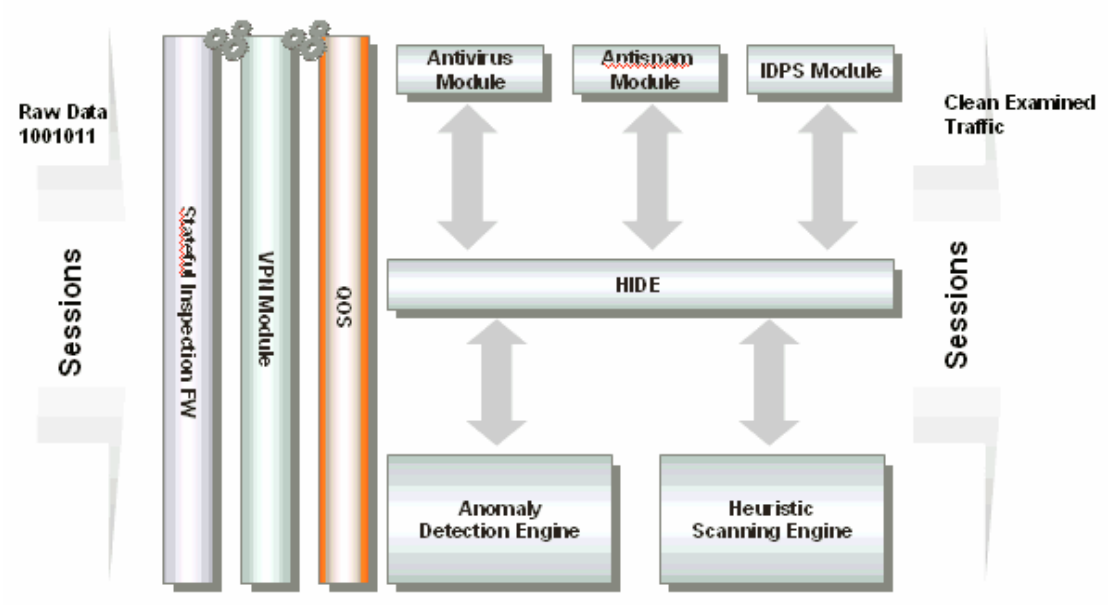

图 2-2 xScreen UTM 系统病毒和垃圾邮件处理示意图

攻击检测和防御（IDP）引擎

xScreen UTM 系统融合了攻击检测和防御处理引擎，攻击检测的处理方式基于数据流连接和网络流量特征库，并且在配置概念上和防火墙模块相类似，可以直接使用系统已经定义的各种地址对象和服务对象，定义攻击防护的目标主机或网络，以及发现攻击行为后的处理方式。攻击检测和防御处理引擎在软件架构上，和防火墙模块之间保持联动，一旦发现攻击行为，可根据用户设置的攻击检测行为，及时切断相应的网络流量，有效的避免了内部网络敏感服务器受到网络攻击。下图是 xScreen UTM 系统的 IDP 引擎处理流程示意图:

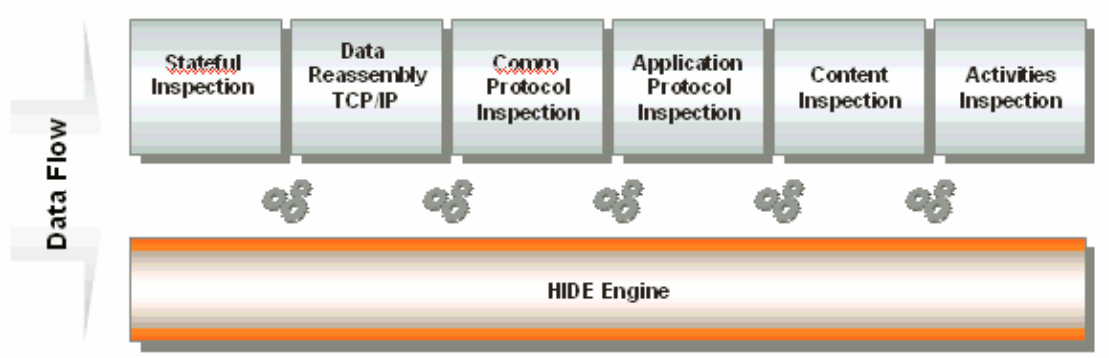

图 2-3 xScreen UTM 系统的 IDP 引擎处理流程示意图

xScreen Global Manager 系统提供了系统攻击行为的告警信息审计分析功能，使得用户对网络中的各种被发现的攻击行为能够有更全面的了解，以便及时定制合理的防御策略。

xScreen Global Manager 系统提供了对多台 xScreen UTM 设备的攻击行为特征库统一升级的功能。用户可以在 xScreen Global Manger 系统中一次性升级多台 xScreen UTM 设备的攻击行为特征库，有效的减少了攻击行为特征库的维护工作量。

功能丰富的Global Manager管理系统

xScreen UTM 提供了功能强大的 GUI Global Manager 系统，该系统基于 Windows 运行。使用 xScreen Global Manager，用户可以在一台管理服务器上，同时管理多台 xScreen UTM 主机。xScreen Global Manager 提供以下功能对 xScreen UTM 设备进行管理：

- 对多台不同地域的 xScreen UTM 设备进行统一管理和配置
- 收集并审计分析多台 xScreen UTM 设备发送的日志信息，包括事件日志，配置日志，安全日志和负载日志
- 对多台 xScreen UTM 设备进行统一的固件升级，病毒库升级和 IDP 特征库升级
- 实时监控多台 xScreen UTM 设备的运行状态和负载信息

第三篇

xScreen UTM 系统相关手册：

相关参考手册：

- xScreen UTM安装手册
- xScreen UTM版本注释
- xScreen UTM运行配置参考手册
- xScreen UTM VPN配置参考手册
- xScreen UTM CLI参考手册
- xScreen UTM Global Manager配置参考手册
- xScreen UTM白皮书

xScreen UTM 系统遵循标准：

序号	标准名称	标准代号
1.	Information Security Management – Part1: Code of practice for information security management	BS 7799-1:1999
2.	Information Security Management – Part2: Specification for information security management systems	BS 7799-1:1999
3.	信息技术包过滤安全技术要求	GB/T 18019-1999
4.	信息技术应用级安全技术要求	GB/T 18020-1999
5.	计算机信息系统安全保护等级划分准则	GB/T 17859-1999
6.	信息技术 安全技术 信息技术安全性评估准则	GB/T 18336.1-2001 GB/T 18336.2-2001 GB/T 18336.3-2001
7.	IETF组织发布的相关Internet、 TCP/IP标准	RFC

支持信息

如果希望得到关于xScreen UTM产品的报价、产品信息以及技术支持，请查阅公司网站：

http://www.xscreen.cn。