Firebox 内容安全网关技术白皮书

可随您企业一起扩展的集成安全设备

Stronger Security, Simply Done™

目　　录

1 WatchGuard XTM产品优势 1
2 XTM系列产品的技术特色 4
2.1 WatchGuard的智能分层安全技术 4
2.1.1 为什么需要智能的、分层次的安全 4
2.1.2 智能分层安全引擎的组成 5
2.1.3 智能分层安全的优势 6
2.2 更强大的安全 —— 智能分层安全如何工作 7
2.2.1 提供零日威胁保护（Zero Day Protection） 7
2.2.2 前瞻性地识别并拦截黑客 9
2.2.3 保证误判率最小化 10
2.2.4 保证更好的性能 10
2.3 智能分层安全引擎的详细描述 12
2.3.1 第一层 —— 外部安全服务 12
2.3.2 第二层 —— 数据完整性 12
2.3.3 第三层 —— 虚拟专网（VPN） 13
2.3.4 第四层 —— 状态检测防火墙 13
2.3.5 第五层 —— 深度应用检测 14
2.3.6 第六层 —— 内容安全 17
2.4 XTM提供的XTM安全服务 18
2.4.1 网关防病毒服务（GAV） 18
2.4.2 入侵防御服务（IPS） 19
2.4.3 反垃圾邮件服务（spamBlocker） 20
2.4.4 URL分类过滤服务（WebBlocker） 21
2.4.5 信誉防护（Reputation Enable Defenses） 22
2.4.6 应用程序控制（Application Control） 23
3 图形化集中管理系统 25
3.1 WSM系统 25
3.2 拖拽式VPN组网技术 26
3.3 丰富的实时监控工具 26
3.4 强大的日志报告系统 27

1 WatchGuard XTM 产品优势

WatchGuard 是世界领先的高效率和全系列网络安全方案供应商，是全球排名前五位的专门生产防火墙的公司之一。WatchGuard 公司 1996 年成立于美国的华盛顿西雅图，并在北美、南美、EMEA 和亚洲等地设有办事处，全球员工总数约 400 多名。WatchGuard 为全球遍布 120 个国家和地区的 60 万台设备的用户提供不断的服务。

WatchGuard 的宗旨是保护那些通过网络开展电子商务的企业，并确保其通信安全。公司以生产即插即用网络安全设备“Firebox” 和相应的服务器安全软件而闻名于世。通过公司具有创新意义的 LiveSecurity Service，单位与用户能保持其安全系统总是处于最新状态。

WatchGuard 全球首创专用安全系统，在 1997 年首家将应用层安全运用到系统，并在 2004 年全球首创可全面升级的整合安全网关。2005 年 WatchGuard 推出了 Fireware Pro 操作系统和 Firebox Peak 高端安全设备，2009 年 WatchGuard 推出了基于全新技术的 Fireware XTM 操作系统和 Firebox XTM 10 系和 8 系高端安全设备，2011 年推出 3 系列，20 系列产品，并整合全球各种优秀的信息安全技术推出整合式的安全网络网关平台 (UTM，统一威胁管理)，为市场提供了更安全、更全面、更强大的安全设备。

WatchGuard 是生产即插即用网络安全设备的先锋，为不同规模的用户提供解决方案，从跨国大型企业和远程工作人员，一直到使用单个宽带连接的家庭办公室。WatchGuard 的分级防御机制提供了强大的、可信赖的网络安全方案，可调节安全防御的深度，以满足不同规模用户的特殊要求。

WatchGuard 中国，在 2004 年建立了北京办事处，在 2007 年建立北京研发中心。自 2002 年至今为中国用户提供了愈 50000 台 WatchGuard 产品，并且在金融保险、制造、交通、通信等行业以及众多的跨国公司和政府单位成功的实施应用。

WatchGuard 中国北京研发中心(BDC)是 WatchGuard 公司全球五个研发中心之一。其研发任务就是为公司的未来进行发明创造，提供最先进的和突破性的技术，为 WatchGuard 赢得竞争优势，创造新的商机。研发中心还在 WatchGuard 感兴趣的其它安全技术领域进行研究，同时还为中国用户提供本地化语言的操作系统及用户特定需求的研发。

WatchGuard 是世界领先的高效率和全系列网络安全方案供应商，是全球排名前五位的专门生产防火墙的公司之一，至今具备十五年的产品销售经验和用户对安全产品技术需求的积累，始终处于安全

行业领导者地位。

WatchGuard® 为全球 150 个国家提供了最为卓越的网络安全解决方案。我们的XTM统一威胁管理（XTM）产品系列提供了具有强大安全性、直观易用性以及专家指导和支持的业内最佳组合。

XTM 在保护您网络的同时，还对您的安全投资进行了保护。当您的需求增长或发生变化时，通过单一的许可文件，您可以轻松地增加 XTM 的容量或加入更多的安全功能。为获取更好的防火墙或 VPN 吞吐量，可将产品升级到同一产品线的更高端型号，而无需进行昂贵的重新购买部署。您也可以通过许可文件轻松地添加所需的扩展功能和特性，包括网关防病毒、入侵防护、Web 内容过滤、垃圾邮件拦截、信誉防护和应用程序控制等。

灵活的集中式日志数据存储支持多种行业标准格式，包括 XML、Syslog 和 WebTrends/WELF。日志通过一个加密的通道以安全可靠的形式传输，并且可被实时地查看、过滤和分类。基于 HTML 的历史报告可用于网络行为分析，而交互的、实时的监视工具使您能够及时地发现问题并为解决网络威胁而采取预防或纠正措施。

更高的安全性

- 通过WatchGuard® 专利的智能分层安全引擎技术，您获得了无需依赖签名即能针对病毒、蠕虫、间谍软件、特洛伊木马和网络攻击的主动式保护以及最为强大的安全基础。
- 智能分层安全引擎技术将防火墙、VPN、网关防毒、入侵防御、网站分类过滤、垃圾邮件拦截、信誉防护和应用程序控制等多项技术有机地整合在一起。各模块协同工作，以保护用户网络的安全运行。

更易于使用

- 我们直观的图形化界面简化了 IT 专家的网络安全工作，并提高了他们的工作效率，同时也为新手提供了不可缺少的易用性。通过简易的设置、智能化的默认值以及向导帮助，您的安全实施提升至以分钟而不是小时为单位运行。
- 统一直观的图形化管理界面，丰富的图形化日志报告和实时监控功能，使您能实

时地关注网络行为和所有设备状态。

高性价比的解决方案

- WatchGuard® 的解决方案提供了完整的集成式安全服务和能力。我们的网络安全产品价格极具竞争力，同时，简化的部署和管理降低了培训和使用成本。XTM 产品可按您对性能和安全需求增加而随时升级和扩展。
- 通过单一的许可文件，可在同一产品线中升级到高端型号或添加诸如 Gateway AV/IPS 等应用层安全服务，保护了您的业务和安全设备的投资。

强大的安全团队支持

- 作为网络安全产业的先锋，WatchGuard® 早在 1996 年已开始部署安全设备。当您成为 WatchGuard® 的合作伙伴时，将有世界级的安全专家团队时刻伴随您的左右，并致力于使您免受当前和日后的威胁。
- 我们的目标是在现在和将来保证您业务的安全以及网络的受信任。专业的 LiveSecurity® 服务为企业客户的网络安全保驾护航。

2 XTM 系列产品的技术特色

WatchGuard® 的XTM系列产品包括 2、5、8 和 10 系列、20 系列，均具有防火墙、VPN、网关防毒、入侵防御、网站分类过滤（WebBlocker）、垃圾邮件拦截（spamBlocker）、信誉防护和应用程序控制等多项网络安全与内容安全防御功能。

2.1 WatchGuard 的智能分层安全技术

2.1.1 为什么需要智能的、分层次的安全

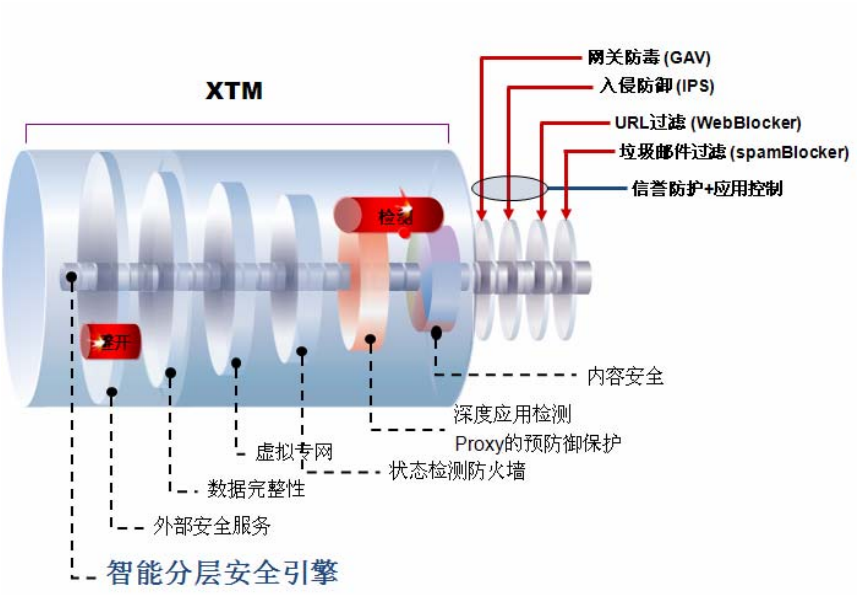
网络安全每天都在不断的发展和变化。一些新兴的技术，比如即时通讯、无线网络、高级 web 服务等都在服务于现在的商业环境，同时也被电脑黑客带来更多的机会。安全威胁变得更狡猾、更频繁、更复杂。同时我们也看到各类欺骗和有组织的犯罪越来越猖狂。今天，很多的系统管理员都清楚地意识到，当传统方式的状态检测技术防火墙独立工作时，已经不能很好地保护企业网络。

现在很多厂商都提供 XTM 产品，这是一种集多安全功能于一身的产品，包括有防火墙、VPN、防病毒、入侵防御、垃圾邮件过滤等功能。然而这些功能模块都是单独工作的，并没有一种有效地手段将他们集成在一起协同工作，相互影响。这种简单的结构上的混合，可能会导致各功能间的相互矛盾和错误的配置，反而会降低安全性。而且，这些系统并没有可扩展性设计，因此，当有新型威胁出现的时候，他们不能够快速而有效地防御。

商业网络需要一个综合的安全解决方案，即可以保护当前的威胁，又可以防御明天未知的危险。基于这些需求，WatchGuard® 公司创建了“**智能分层安全**”（ Intelligent Layered Security —— ILS）体系结构。这项技术可以最有效地抵御当前混合的、快速变化的威胁攻击。

2.1.2 智能分层安全引擎的组成

WatchGuard® 公司的ILS体系结构由 6 个安全模块层智能地组合在一起，这些模块彼此之间相互协作，可以动态地发现、拦截并报告有威胁的通讯，尽全力保证正常的应用通讯高效地传输通过设备。这种高效的设计，可以做到尽量少地牺牲系统性能，同时防御已知和未知的攻击。



“智能分层安全”引擎，是整个体系结构的神经中枢。在设计上，每个层都是相互协同工作的，并且在层间相互交换数据流信息，从而最大化地实现系统的防护性、可靠性和高处理能力。下面来看看每个层。

- **外部安全服务**

  提供了防火墙的部分保护功能，并能授权给最终用户或管理员更多的有效信息；

- **数据完整性**

  确认数据包的完整性和协议的一致性；

- **虚拟专网**

  保障了内部数据安全地在外部传输通讯；

- **状态检测防火墙**

  通过安全策略控制源地址、目的地址及端口的通讯；

- **深度应用检测**

  保证应用层协议标准的一致性；拦截有害文件及文件类型的传输；拦截危险指令或信息篡改，防止内部信息泄露；

- **内容安全**

  分析并调节适当的内容通讯，这些内容安全服务包括网关防病毒服务、入侵防御服务、反间谍软件服务、反垃圾邮件服务、URL 分类过滤服务、信誉防护和应用程序控制；

尽管在这个模型里定义了 6 个独立的层，但很多的功能是需要各层之间相互合作的。并且，每个层都被设计为可以方便扩展功能，以应对未来出现的新型威胁。

2.1.3 智能分层安全的优势

ILS 多层安全结构的设计，可以提供，

- **内容安全**

  零天防御 —— 拦截多数固有的弱点，减少网络空窗期的威胁；

  具有前瞻性的识别和拦截攻击 —— 识别攻击者和攻击行为，并自动拦截来自同一攻击地点的威胁；

  最小化误判率 —— 使用基于签名库技术的内容安全服务，如网关防病毒/入侵防御技术；

- **简单易用**

  深度应用检测与其他 ILS 层“常开启”状态；

  默认设置会拦截大量攻击，用户无需复杂配置；

  前瞻性的防御体系；

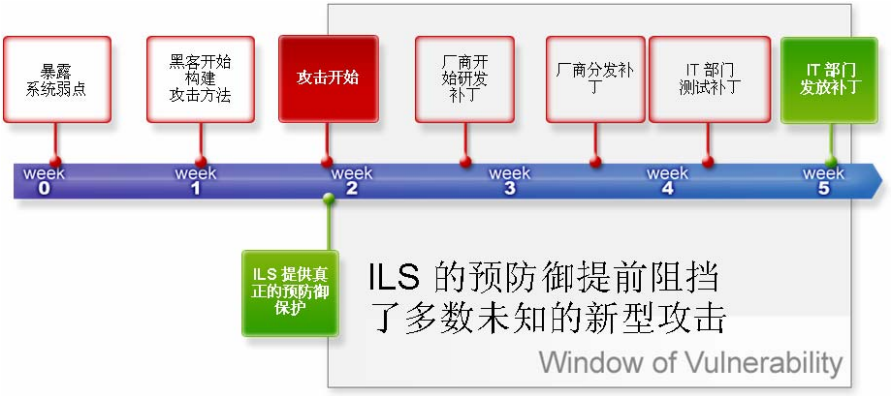
- **更出众的性能**

  分层次的设计结构，可以利用最少的处理能力发现并阻挡攻击；

2.2 更强大的安全 —— 智能分层安全如何工作

2.2.1 提供零日威胁保护（Zero Day Protection）

在网络安全的领域，人们对“预防御”攻击保护有多种不同的说法。但是，厂商们真正提供的防护服务却截然不同。零日威胁（Zero Day Threats）是指新的或未知的攻击，它们出现的时候，还没有写好相应的补丁程序或者攻击特征。零日威胁保护（Zero Day Protection）是指在发现漏洞，以及在建立和发起真正的攻击之前，就阻止新的或未知的威胁。通常称为“预防御”。



基于攻击特征的解决方案只能阻止已经识别出来的威胁。在分析出攻击特征，开发好补丁程序，并实际部署之前，您的网络对于新的威胁仍然没有任何免疫力。考虑一下当今的各式网络攻击的频率和破坏力，即使失去一分钟保护，都可能带来灾难性的后果。事实上，在分析出攻击特征或开发出补丁，并进行实际部署之前，用户需要的是几小时、几天甚至几周的等待时间。这个网络漏洞的空窗期是每一个 IT 管理者的噩梦。

深度应用检测层的核心能力是提供零日威胁保护。

- 协议异常检测（Protocol Anomaly Detection）

  协议定义了两个系统交换数据的方法。一些服务器不能够正确地处理畸形数据流。很多攻击者就制造一种 DoS 攻击方法，对某些应用层协议进行攻击从而得到服务器的管理权限。通过执行协议的 RFC 标准检测，我们可以防止这种典型的攻击。除防止协议攻击外，我们还可以防止非法的命令调用攻击和防止大量的缓存溢出攻击。

- **模式匹配**

  对于拦截那些到达电脑并执行的恶意代码是非常有效果的。换句话说，就是那些包含在可执行文件中的恶意代码。通过拦截用于承载恶意代码的文件（如 exe、pif、src 等）和 MIME 类型，我们可以有效地防止这些恶意软件达到网络内部的电脑。

  但是在一些应用中，我们必须允许这些可能存在潜在威胁的文件（如 exe、dll）进入到内部网络，例如从 Microsoft 更新软件、从 HP 站点下载打印驱动程序等。那么我们就必须清楚地定义那些安全资源，并允许安全资源通过。

- **命令限制**

  应用协议中经常包含很多命令和参数，用于数据的发送和接收。然后，有很多管理命令是我们不希望由外部网络用户使用的。我们可以拦截那些具有潜在危险的命令，例如，可以拦截 FTP 协议的 SITE 命令和 SMTP 协议的 DEBUG 命令，从而防止这一类型的攻击。

- **伪装**

  伪装可以很好地隐含服务器的真实信息，从而躲避黑客的探测。例如在 SMTP 协议中，可以伪装域名、隐含服务器类型及版本，甚至可以从 Message ID 和 MIME 中移出一些信息。这些技术可以防止黑客探测到服务器细节信息，从而使用相应的攻击手段对付服务器。

- **过滤/拦截头信息**

  另一类攻击依靠建立一些畸形协议头来攻击服务器的弱点。深度应用检测层可以很好地过滤/拦截这些协议头内部的信息。

依靠如上这些技术很好地提供零日威胁保护的能力，都是 XTM 系统预定义好的，并结合安全策略实施的，无须用户自己来解决。

2.2.2 前瞻性地识别并拦截黑客

这一机制可以对那些在发起攻击前（通过他们的行为）或者在第一次发起攻击的黑客作出识别。通过拦截攻击者的 IP 地址，可以使我们有能力动态地响应攻击行为。对于防御重复性攻击，拦截 IP 地址是非常简单而有效的方法，并可以大大减少系统资源的占用。如果我们可以预先发现一个攻击行为，那么这个机制就可以很好地保护我们免受新的、未知的攻击。

- **识别攻击**

  WatchGuard ILS 结构的效力体现在其分布式智能分析能力。每一个层都具有分析和报告攻击者 IP 地址的能力，同时可以拦截这些攻击性的 IP 地址通讯。这个能力应用于大量的不同级别攻击行为，例如 DoS 攻击、IP 选项攻击、基于 PAD 的协议异常攻击，甚至被防病毒/入侵防御系统识别到的攻击等。

- **识别攻击者行为**

  在一个攻击开始前，基于行为的分析就可以将其锁定为一个攻击者。“扫描者与攻击者的匹配几率高达 96.3% .....换句话说，每一次扫描过后，在未来某一时刻，都可能会发生来自同一个地点的攻击行为。”（网络世界，8 月 25 日，2003）

  ILS 通常可以识别的行为有，

  - 端口扫描；
  - 地址扫描；
  - 利用 IP 选项、欺骗和源路由；

- **自动拦截**

  这种自动拦截的方法就是，在用户定义的一段时间里，系统自动地拦截来自攻击者或具有攻击行为的 IP 地址通讯。在以下几个方面具有显著的效果。

  - 自动拦截黑客工具；
  - 对于来自同一地点的攻击行为，简单的 IP 地址拦截可以很好地降低系统开销；

当然，防火墙也可以手工配置来屏蔽到一些不良的端口和 IP 地址。

2.2.3 保证误判率最小化

众所周知，基于签名的技术，如防病毒引擎，都会有误判率（如将某种正常行为定义为攻击）。一般地说，误判率与签名库大小和扫描数据的多少是有直接比例关系的。那么在 ILS 体系结构中，各层协同工作，以降低需要扫描的数据量和签名库的大小。

- **网关防病毒和深度应用检测**

  前面描述过，深度应用检测层通过执行协议标准检测和对已知的有害文件类型进行拦截来发现攻击行为。对已知的有害文件类型进行拦截不会产生误判；那么减少防病毒引擎的扫描工作量，就意味着具有降低病毒检测误判率的可能性。

- **入侵检测**

  经过优化的 ILS 包含一套标准的入侵防御系统，通过签名定义的方法描述所有可能的攻击形。每种攻击对应一个签名。在 ILS 体系结构中，由于从数据完整性层到深度应用检测层，大多数攻击都被有效地拦截了。这意味着，在内容安全层的 IPS 引擎中只需要维护大约 2000 余种签名就足够了。

  另外，因为深度应用检测层可以识别大多数的协议，并将这些信息传递给 IPS 引擎。这样一来，IPS 引擎就可以针对具体协议来进行精细扫描，从而进一步缩小了查询签名库的范围，提高了处理速度。例如，扫描 SMTP 通讯而忽略其使用的端口，那么 IPS 引擎只需要在 SMTP 签名列表中搜索匹配项即可。

  这样的设计，不仅仅减少了被扫描数据流的数量，而且也减少了每次扫描时使用到的签名数量。从而进一步地降低了误报率。

2.2.4 保证更好的性能

真正网络世界中，XTM 的性能很难去衡量，因为这里是一个混合的环境。这里有大量的防火墙策略，VPN 通道，还有很多使用到的服务，如网关防病毒和反垃圾邮件等等。基于如上原因，XTM 厂商所给出的性能参数都是每项服务或功能在最佳状态下的测试值。例如，网关防病毒性能是在使用最少量的防火墙策略和其他服务都关闭情况下测试得到的。

这样就很难比较在真实网络世界中的 XTM 综合性能。虽然我们可以从厂商那里得到各类参数来比较单独某项功能或服务性能，但是更有意义的多功能和多服务综合性能效果对比就变得很难了。

通过精心设计和各安全层的相互协作影响，WatchGuard 的 ILS 体系结构使真正网络世界中的 XTM 性能达到最优状态。这表现在三个关键的设计原则上：

- **处理顺序**

  ILS 引擎最轻量化地占用系统性能来实现对数据流的检测以发现攻击行为。如前面所述，一些简单的攻击，例如畸形数据包和 DoS 攻击，首先被处理掉了。这就意味着，占用较高系统资源的服务，例如入侵防御引擎，他们所处理的数据流减少了很多。

- **各层间的信息交换**

  在很多 XTM 解决方案中，许多安全功能是独立工作的，他们之间并没有很好地利用信息共享来实现合作。ILS 会在各层间共享信息，从而能够减少并很好地调整各安全功能的处理需求。这也就意味着，各安全功能间无须多次重复处理数据，因此得到理想的性能。

- **动态拦截**

  很多真实网络世界中的攻击都来自一些自动化的攻击工具。这些工具都会在发起攻击前先扫面目标网络中存在的弱点。除 DDoS 和垃圾邮件攻击外，这些攻击工具都会使用同一个 IP 地址。

  ILS 的能力在于可以发现这些行为，例如端口扫描和地址扫描，然后利用这些信息来自动拦截。当第一次扫描或攻击开始的时候，保护机制便被触发。那么来自同一地点的后续攻击数据流都回被自动拦截。同时拦截会被保持一段时间，这样设计使得系统没有必要浪费时间再次处理和分析同类攻击行为。

2.3 智能分层安全引擎的详细描述

下面我们将介绍 WatchGuard 智能分层安全体系结构的概念，以及这种分布式系统智能所带来的更好的安全性。让我们来看看 ILS 中的每一个安全层在作些什么。

2.3.1 第一层 —— 外部安全服务

为了保证网络运行高效，在帮助管理员正确配置防火墙和相关系统的同时，补充网络的一些外部安全服务是必须的，例如漏洞分析和桌面防毒系统等。在 WatchGuard 的模型中，这个概念就表现为一个在防火墙外面工作的安全层，其完成了防火墙必须完成的一些网络功能。

外部安全服务更强调预防，它可以同其他分层有效地、安全地协同工作以达到最理想的效果。对于管理员来说，整个网络就成为了一个单一的实体，可以更安全、更简单的管理。

2.3.2 第二层 —— 数据完整性

数据完整性层是 XTM 的第一道防线。它会效验进入设备的数据，确保其遵守数据包协议规范。所有的网络通讯都必须经过这个层。这是一个最佳地拦截攻击的位置。而且对于数据流的处理也相当快速，因为只有两个结果通过或阻断。例如，这个数据包是否符合 RFC 标准？包头信息是否超过了标准规定的长度？如果是，数据包将被直接丢弃。这一层的主要职责是：

- **数据流标准化**
  - 通过 IP 效验保护你的网络，阻止任何畸形的 TCP/IP 数据流流进入下一层；
  - 利用 WatchGuard 专利的反攻击机制，发现并阻挡 DoS、DDoS 和分片重组攻击，保证正确的数据流顺利通过并进入下一层；例如防御 IPSec、IKE、ICMP、UDP、SYN flood 攻击等等；

- **发现并拦截一下通讯**
  - 端口扫描；
  - 地址扫描；
  - 欺骗攻击；

对数据流标准化检测和对已知攻击的拦截可以改善整体系统的性能，因为 ILS 能够快速地处理这一层的数据，并保证后续其他层仅接收到正确的、合法的数据包。

2.3.3 第三层 —— 虚拟专网（VPN）

一旦数据流被确认为有效的、标准的，ILS 接下来确认该数据流是否为来自一个已知 VPN 连接点的加密流。如果是，VPN 层将对数据流解密并向下一层传输；如果该数据流是由未知的密钥加密的，那么该通讯被阻断。如果数据流不是加密的或不是来自一个已知 VPN 连接点的，那么 VPN 层将不作任何处理，数据流将被传递到下一层。

VPN 层支持 PPTP 和 IPSec 协议，并可以组建移动用户 VPN 和分支机构间 VPN 通讯。通过正确的 VPN 配置，你可以通过 Internet，对外出的私有数据进行安全地加密传输。

2.3.4 第四层 —— 状态检测防火墙

在这一层，管理员可以根据源 IP 地址、目的 IP 地址和通讯端口来设定数据流是否可以通过防火墙。ILS 的 NAT 功能也在这一层得以执行。

虽然很多种类的攻击手段都依靠使用畸形包来获得目的主机的响应信息，但是个别遵守全部 RFC 标准的包依然会含有恶意企图。例如，一个黑客获取了用户网络信息，那么他就可能会尝试发送一个含有“Reply”标记的包进入用户网络，这样就伪装成了一个来自被访问的目的服务器响应包。对于一台非状态检测设备来说，虽然也检测 2 层以上信息，但会认为这就是来自目的服务器的响应而允许其进入用户网络。然而一台状态检测设备就会知道，从来没有向黑客的 IP 地址发送过“请求”数据包，同时在内部没有发出“请求”时，也不允许一个“响应”包通过并进入网络，这样，状态检测设备就会丢弃那个伪装的“响应”包。

ILS 在这一层提供了这样的状态保护，并且进一步地提高了其功能。状态防火墙层会跟踪所有会话的端口和协议信息，并为这些会话建立状态表。当发现一个攻击行为时，同时会触发攻击躲避机制。通过这些，ILS 可以击败有目的性的攻击，并且还可以避免由同一攻击源重

复攻击所引起的防火墙负载升高。

2.3.5 第五层 —— 深度应用检测

通过了状态检测防火墙层的数据流被传递到深度应用检测层，在这里 ILS 将判断该数据流是否“适合使用”。如果不需要进一步检测，那么数据流将被直接转发以达到最佳性能。在深度应用检测层，TCP 连接被终止了，并且在防火墙两侧重新建立新的连接。发出的数据包将被重新格式化以防止攻击出现。

深度应用检测层可以发现、管理、防止或阻断：

- 协议异常；缓冲区溢出；
- 未授权连接；
- TCP 劫持；
- 网络信息泄露；
- 基于 MIME 类型或模式的有害附件、病毒、蠕虫等（如*.bat, *.cmd, *.com, *.exe, *.hta, *.inf, *.pif, *.scr, *.wsh 等）；
- 使用潜在的危险命令；

在前面“更强大的安全 —— 智能分层安全如何工作”一节中，我们看到深度应用检测层防御攻击的核心机制，它们是：

- 协议异常分析（PAD）；
- 模式匹配；
- 命令限制；
- 伪装；
- 过滤/拦截信息头；

基于精确标准定义和策略判断，深度应用检测层可以提供零日威胁防御来应对更广泛的攻击类型，而且可以有效地减少误报率。下面让我们来看看 ILS 如何在 HTTP、SMTP、FTP、DNS 和 TCP 这些核心应用协议上作精细的控制。

♦ HTTP Client

HTTP Client 协议处理器可以很好地控制什么样的信息流可以到达用户的浏览器或其它 HTTP 客户端。管理员可以做到：

- 拦截那些不严格遵守 HTTP 协议 RFC 标准的数据流；比如 QQ 在使用 TCP 80 端口通讯时，因为没有采用 HTTP 协议标准，所以会被 HTTP Client 协议处理器自动拦截；很多在线视频软件也使用 TCP 80 端口以示图逃过防火墙策略控制，但传输的内容因为没有遵守 HTTP 协议标准，同样也会被 HTTP Client 协议处理器自动拦截；
- 利用模式匹配，检测病毒、蠕虫、木马等有害信息；
- 可以删除或阻挡 Cookie、Applet、ActiveX 及未知的 HTTP 头信息；
- 限制 HTTP 请求的方法；控制 HTTP 的命令；
- 隐藏服务器信息；
- 控制认证方法；
- 限制请求和访问头类型，来防止畸形或未知的头类型；
- 控制附件类型；URL 地址控制；
- 转发数据流到 IPS 模块；
- 调用 ILS 自动拦截机制，减少处理同一攻击源所消耗的负载；

♦ HTTP Server

HTTP Server 协议处理器可以很好地控制什么样的信息流可以到达用户的 Web 服务器。它所能控制的内容与 HTTP Client 处理器是类似的，当然也有一些差异。

♦ SMTP Incoming 或 Outgoing

我们所看到的大量破坏性攻击都是混合型攻击，例如蠕虫使用多重感染和繁殖的方法大量传播，大多数蠕虫选择使用 SMTP（或者说是邮件服务器）作为其传播的载体。WatchGuard 的 SMTP 协议处理器可以阻挡：

- 存在潜在危险的邮件附件；
- 不合法的 SMTP 命令；
- 协议异常；

SMTP 协议处理器可以将发送畸形数据流的站点自动添加到拦截黑名单中，因此 SMTP 协议处理器可以非常有效地对付这类攻击。管理员在使用 SMTP 协议处理器可以做到：

- 拦截那些不严格遵守 SMTP 协议 RFC 标准的数据流；
- 利用模式匹配，过滤附件名及 MIME 类型；
- 限制 SMTP 命令及参数的使用；
- 伪装服务器信息；
- 控制允许或不允许的邮件头信息；
- 控制邮件大小；
- 限制最大收件人数量；
- 限制邮件地址长度；
- 控制 bat/CHUNKING、ETRN 和 8-bit 或 Binary MIME 在 ESMTP 中的使用；
- 控制 ESMTP 认证类型；
- 控制 SMTP 问候语的长度；
- SMTP 转发保护；
- 源、目的邮件地址黑白名单；
- 转发数据流到防病毒模块；
- 转发数据流到 IPS 模块；
- 调用 ILS 自动拦截机制，减少处理同一攻击源所消耗的负载；

♦ FTP

WatchGuard 的 FTP 协议处理器可以帮助管理员管理 FTP 服务器，有效地控制 FTP 资源的使用：

- 拦截那些不严格遵守 FTP 协议 RFC 标准的数据流；
- 强制会话超时；
- 限制 FTP 命令及参数的使用；
- 伪装服务器信息；
- 限制如用户名、口令、命令行、文件名的长度；
- 限制可以下载的文件类型；
- 控制上传文件及其路径；

- 转发数据流到防病毒模块；
- 转发数据流到 IPS 模块；
- 调用 ILS 自动拦截机制，减少处理同一攻击源所消耗的负载；

♦ DNS

一些黑客工具可以利用 DNS 查询和应答来获得你的 DNS 服务器管理权，从而可以进一步控制那些使用这台 DNS 服务器的用户。这类攻击使用畸形的 DNS 请求包来传递恶意代码。WatchGuard 的 DNS 协议处理器可以检测 DNS 请求的头部信息，并且可以阻断那些可疑的内容。DNS 协议处理器可以做到：

- 拦截那些不严格遵守 DNS 协议 RFC 标准的数据流；
- 伪装服务器信息；
- DNS 包头检测，丢弃那些不正确的部分；
- 控制 DNS 代码、查询类型和查询名称；
- 转发数据流到 IPS 模块；
- 调用 ILS 自动拦截机制，减少处理同一攻击源所消耗的负载；

♦ TCP

TCP 协议处理器主要完成在防火墙两侧重新建立 TCP 连接的过程。这就意味着，数据包被重新规范化并且得到了整合。这样就可以更好地发现攻击行为。TCP 协议处理器同时还可以处理使用非标准端口的 HTTP 协议通讯，处理机制与 HTTP 协议处理器一样。

2.3.6 第六层 —— 内容安全

内容安全层很有针对性地对一些协议数据流作更深一步的检测。在这一层里，对用户来说安全服务都是可选项目，这包括网关防病毒服务、入侵防御服务、反垃圾邮件、URL 分类过滤、信誉防护和应用程序控制。

参见“XTM 提供的 XTM 安全服务”部分的详细内容。

2.4 XTM 提供的 XTM 安全服务

2.4.1 网关防病毒服务（GAV）

WatchGuard 的网关防病毒服务可以识别并拦截病毒、蠕虫、木马、间谍软件等可能会进入到你的网络的那些恶意代码。WatchGuard 建议用户在使用网关防病毒的同时也要使用桌面杀毒系统，这样做有两个好处：

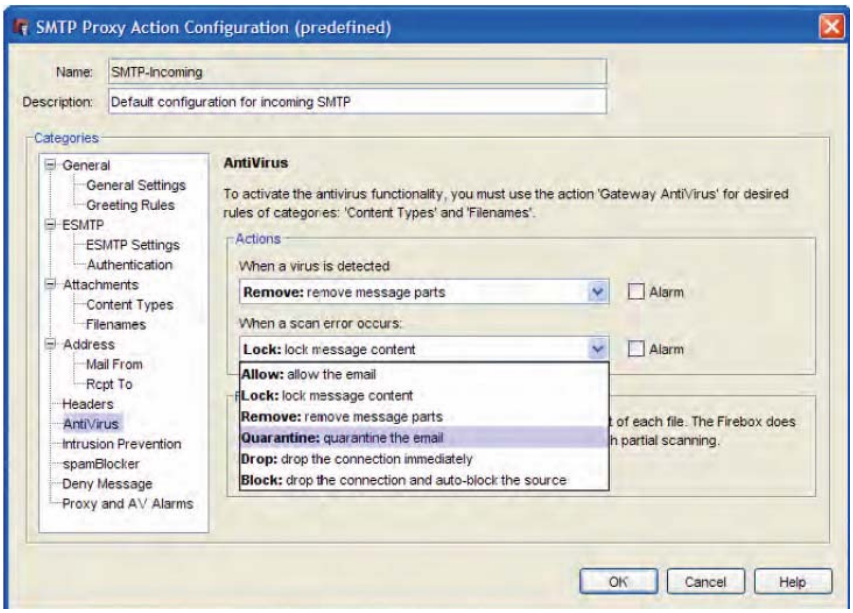
- 由于是网关级别的防御，因此不会象桌面杀毒系统那样被某些新兴病毒关闭而失去安全防御能力；
- 两套防病毒系统同时运行，可以提高病毒库升级的平均响应时间，这比只单独依赖一套系统要好很多；

在 ILS 里，将网关防病毒与其他安全层结合在一起工作，可以得到更多的益处：

- 效率 —— 网关防病毒只处理那些通过了深度应用检测层处理的数据流，需要扫描的内容大大减少了；
- 更细化的控制 —— 网关防病毒扫描的文件类型可以订制；

WatchGuard 的网关防病毒服务可以对感染文件进行允许、阻断、锁定操作。文件锁定可以满足那些需要这种有害文件的网络管理员的需求。当系统检测到一个有害文件时，便对其加密并传递给最终用户。这样可以防止用户无疑中执行了该有害文件；如果用户希望去解开压缩并还原原始文件，那么他必须从管理员那里得到正确的工具。当然用户也可以直接删除到这些没有用的文件。

WatchGuard 的网关防病毒签名库的升级是自动的，并且用户可以控制其升级的时间间隔。我们在 Internet 上平均每 4 小时便会更新一次病毒签名库。



2.4.2 入侵防御服务（IPS）

WatchGuard 的入侵防御服务可以对那些含有恶意攻击脚本的通讯协议作在线检测。在线检测 IPS 系统面临两个问题：速度和误报率。与其他 ILS 安全层紧密结合在一起的 IPS 服务，在这两方面表现相当不错。因为 ILS 的其他安全层大约可以拦截 60%~70%的攻击行为。那么对于这些攻击的签名库已经不再需要了。这样就降低了 IPS 在签名库中的检索数量同时提高了检索时间还有误报率。

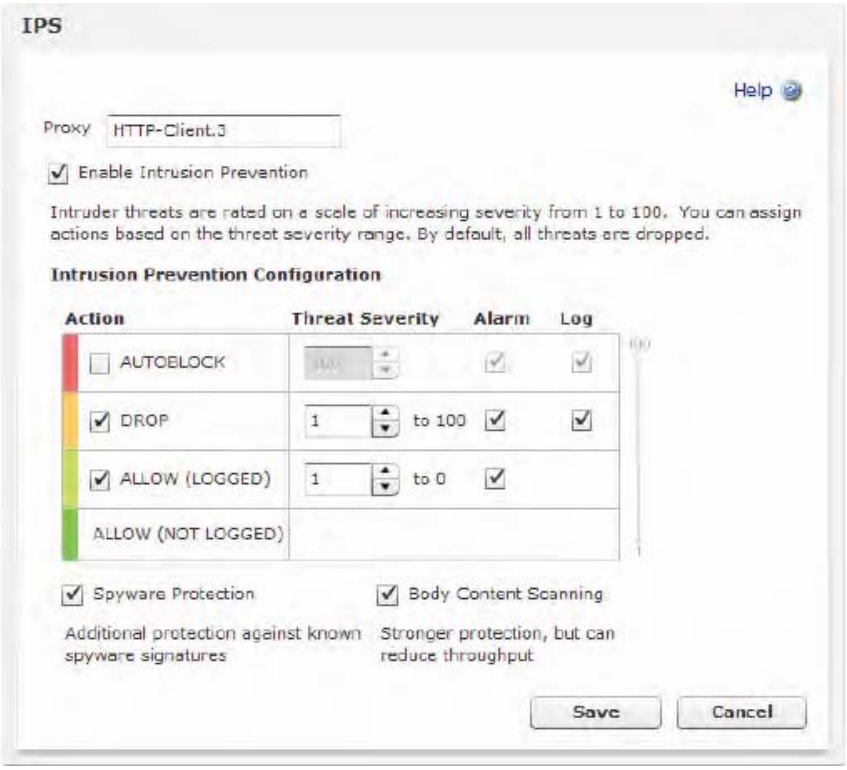
深度应用检测层可以明确地知道通讯协议，它会调用 IPS 只针对已知的协议作检测。这就意味着 IPS 有目的性的检测某协议的签名库子集，而不是在整个签名库中遍历。同样 IPS 也可以调用 ILS 的自动拦截功能。当 IPS 发现了第一个攻击行为后，将攻击者的 IP 地址传递给自动拦截系统，那么该攻击者的后续任何攻击行为都被阻挡在“外部安全服务层”，从而进一步节省了系统开销。这不像其他的 IPS 那样，对每一次攻击都要进行深入分析，而白白浪费系统资源，降低处理能力。

- **间谍软件的防御**

  间谍软件会通过 P2P 传播，也会通过感染文件、Cookie 和下载传播。间谍软件会盗取用户的键盘信息、密码文件、认证信息等内容。它也会消耗 PC 的资源和网络带宽。WatchGuard 的 IPS 引擎可以依据签名特征和独特的意图分析来拦截间谍软件。IPS

引擎可以对抗：

- 拦截站点 —— IPS 引擎会主动拦截通过 HTTP 协议对已知间谍主机或下载站点的访问；
- 基于签名的内容检测 —— IPS 引擎会不断地升级攻击特征签名库，利用特征来拦截间谍软件的下载；
- 截断配置 —— 间谍软件一般都会向外传递一份安装报告，并下载一份初始化配置文件；IPS 引擎会识别并拦截这种通讯；
- 自动安装 —— 在一个安全网络中的被感染主机，会利用网络连接建立一个新的通讯通道，用于传输窃取的信息、下载另外的间谍程序或者非法广告；IPS 引擎都可以识别并拦截这些通讯；



2.4.3 反垃圾邮件服务（spamBlocker）

垃圾邮件大约占据了当今邮件总量的 63%，这也是绝大多数公司所面临的头痛问题。WatchGuard 的反垃圾邮件服务利用 Commtouch 公司的循环模式检测（RPD）技术给予用户实时的保护，对于垃圾邮件、病毒邮件爆发的检测率高达 99.95%，而且在设备中还不使用任何签名及过滤。

与评估关键字和内容所不同，这项技术实时分析大量的 Internet 流量，并当垃圾邮件爆发的瞬间立刻分析出其特征（或者叫 DNA）。每天都对将近 500 万条样本信息进行高级运算分析，在 1、2 分钟内就可以识别并分类新的具有代表性的垃圾邮件特征。spamBlocker 利用这项技术直接通过 Commtouch 检测中心（大约维护 2 亿个垃圾邮件特征）比较可疑邮件，给予用户最新的垃圾邮件防御。

这项技术具如下 4 项特点：

- 对垃圾邮件、病毒邮件的爆发做出极其快速地反映；
- 几乎为零的误判率 —— 可以很好地从垃圾邮件中识别出正常通讯；
- 高垃圾邮件识别率 —— 拦截 97%的无效邮件；
- 与语言无关 —— 对于垃圾邮件的拦截不依赖于语言、内容和信息格式；

spamBlocker 利用邮件通讯的基本特性来鉴别是否为垃圾邮件，并将 97%的垃圾邮件阻挡在网关以外，而且这些处理都是瞬间完成的。利用大量的信息特性而不是检索那些单独的内容、语言或格式，spamBlocker 可以实时鉴别全球的垃圾邮件，包括那些邮件钓鱼攻击，同时还保证了其他网络通讯的高处理性能。

为了更好地服务于邮件用户，spamBlocker 支持外部隔离服务器，那些被识别为垃圾或含病毒的邮件，会被发送到指定的邮件服务器中保存，并定期通过邮件通告通知邮件接收人领取隔离的邮件。

2.4.4 URL 分类过滤服务（WebBlocker）

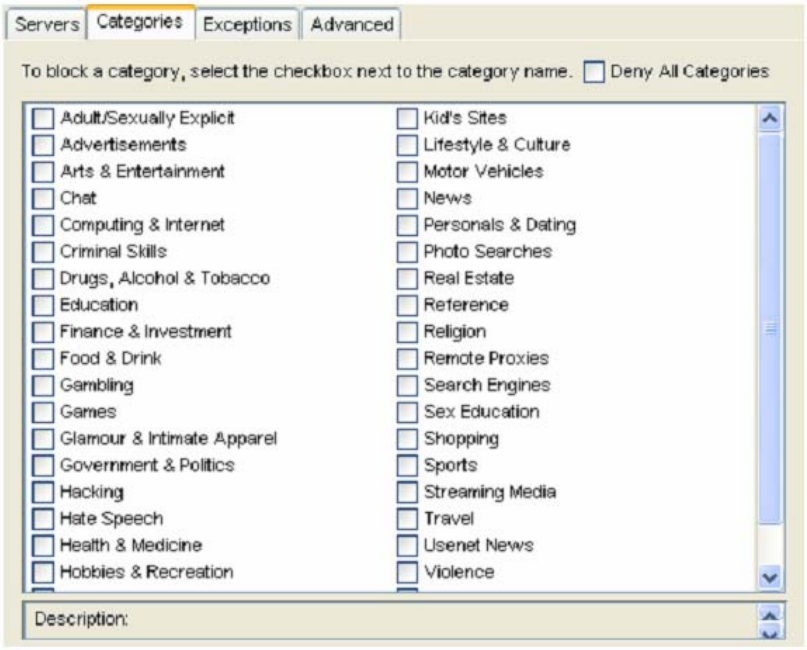
WatchGuard 的 WebBlocker URL 分类过滤服务使你不单单可以配置哪些用户能够进行 Web 访问，还允许你定义哪些 Web 是可以访问的。在 WSM 中，使用可视化的配置，你可以对允许访问的 Web 类型和什么时间段可以访问这些内容做出快速分类处理。

WebBlocker 采用全球 Web 过滤技术的领导者 —— SurfControl 公司的数据库和引擎技术，保证了分类的正确性和覆盖的全面性。WebBlocker 使用多种分类来帮助用户拦截那些不

希望进入网络的内容。

- 拦截间谍软件站点和那些已知的存在恶意代码的站点；
- 拦截在工作场所不适宜观看的内容；如色情信息；
- 拦截与工作无关的内容，提高工作效率；

利用客户订制化列表、用户身份认证、基于时间的不同访问策略等技术，WebBlocker 可以帮助你有效地执行网络管理政策。WebBlocker 还可以帮助你和你的网络远离那些含有病毒、蠕虫、间谍软件、恶意程序的网站。



2.4.5 信誉防护（Reputation Enable Defenses）

更好地应对 WEB 威胁

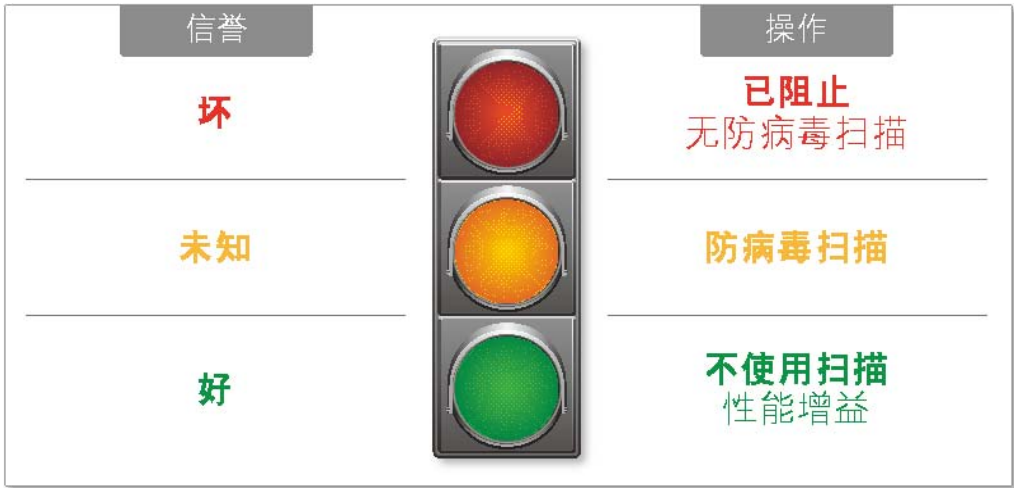
启用信誉系统的防御可通过信誉查找将 URL 评定为好、坏或未知，从而提供安全的 Web 浏览体验。这种查找依靠一个基于云的强大信誉数据库对来自多个源的数据进行汇总，包括业内领先的防病毒引擎。立即拦截信誉明显很差的 URL。通过持续更新信誉数据库，能随时了解动态 Web 内容和不断变化的 Web 情况，从而做到实时保护，无需每小时或每天等待接收更新。信誉评分根据特定 URL 来确定，而非只是网站或 IP 地址。

更快、更有成果的 WEB 冲浪

启用信誉系统的防御能够加速浏览，因为它不必扫描所有 Web 流量即可识别威胁。具

有较好信誉评分的 URL 能够安全地通过 AV 扫描。信誉评分的本地缓存可快速处理 URL。更高效地使用设备资源可提升用户能力。最多可跳过 50% 的 URL 扫描，同时不会影响安全性，从而加快了浏览速度，网关吞吐量也大幅提高。

信誉评分



2.4.6 应用程序控制（Application Control）

使用 WatchGuard 应用控制工具，随时掌握您网络上运行的应用程序情况，实现更高的安全性和生产率。通过该工具，还可对公司内应用程序的可用性、使用人和使用时间进行管理。对 1,500 多种按类别管理的应用程序实施完整控制。依靠超过 2,500 个签名和复杂行为分析来识别试图进入您网络的应用程序，不论目的地地址或 L7 协议如何，包括专门设计用来绕过普通安全措施的加密应用程序。通过类别、应用程序和应用程序子功能为用户和组建立可接受的使用策略，以实现最大的灵活性。利用对您网络上被访问对象的实时和历史可视性来报告应用程序的使用。利用这些信息可以展示遵从性，评估员工需求，以及改善可接受的使用策略。

应用控制举足轻重

通过应用控制工具，您可以根据用户的部门、工作职能和当日时间有选择地允许、阻止或限制访问应用程序，并生成使用报告。例如，你可以选择：阻止使用 YouTube、Skype 和 QQ，可选择始终阻止、重要营业时间内阻止，或者从不阻止；阻止任何非管理团队成员使用 P2P 应用程序；允许市场部门访问 Facebook 及其他社群网站；允许使用 Windows Live Messenger 发送即时消息，但不允许用于传输文件；将流媒体应用程序的使用限制在一天的

特定时段；报告公司内使用的前十个应用程序；报告公司内任何个人使用（或试图使用）的应用程序。

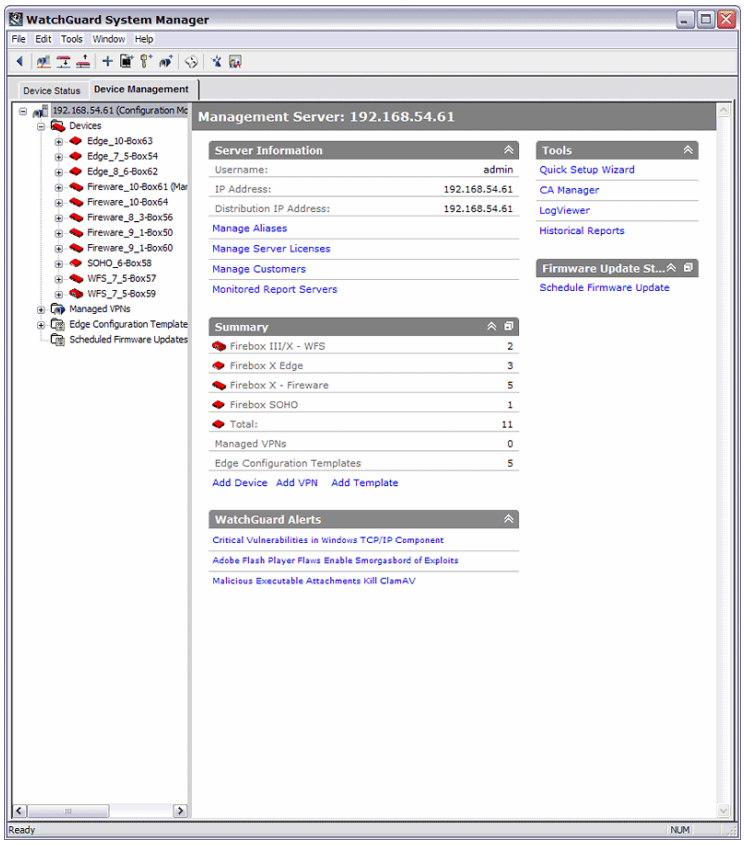
控制和阻止 2,500 多种 WEB 2.0 和业务应用程序

3 图形化集中管理系统

3.1 WSM 系统

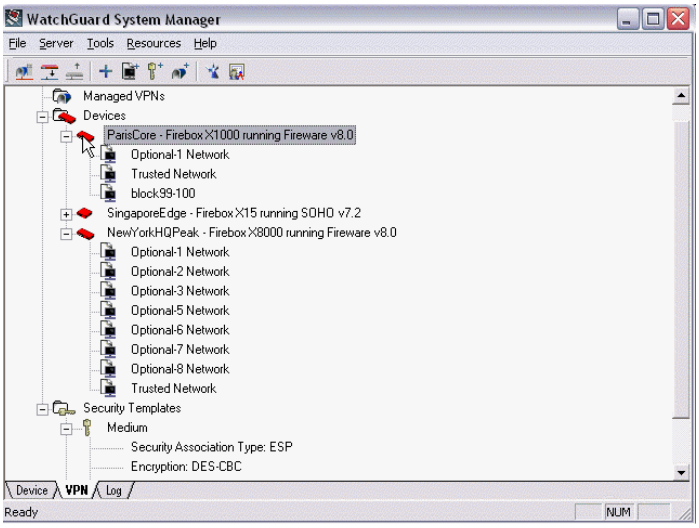
我们认为一套安全管理系统应该使用户得到帮助而不是将用户搞混乱。图形化的 WatchGuard System Manager（WSM）就是这样一套强大管理系统，对于所有网络管理员来说，WSM 是非常简单、易用的管理工具，为刚入门的网络管理员提供了不可缺少的易用性。同时，WSM 为专业人士提供了更有效的、更细腻化的管理方法。功能丰富、操作直观的用户界面，使您可以在集中化的配置和管理所有 XTM 产品及其安全服务。

- 大量的配置向导工具，节省了网络管理员的时间；
- 实时的、图形化的网络监控工具，使网络管理员随时掌控网络状况；
- 安全的集中化管理，可以在远程管理上百台 XTM 设备；
- 丰富的日志报告，是网络管理员分析网络的好助手；



3.2 拖拽式 VPN 组网技术

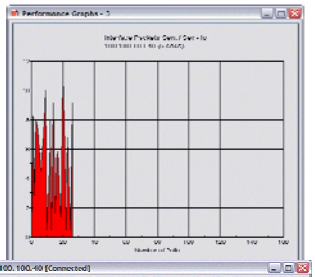
WSM 软件可以专门针对大型复杂网络的 VPN 部署进行灵活地控制。WatchGuard 独有的 DVCP 技术使得我们在部署 IPSec VPN 时变得相当轻松。即在中心点只需要一个固定 IP 地址，下面各分支机构允许使用动态的 IP 地址，我们可以轻松建立 VPN 隧道。

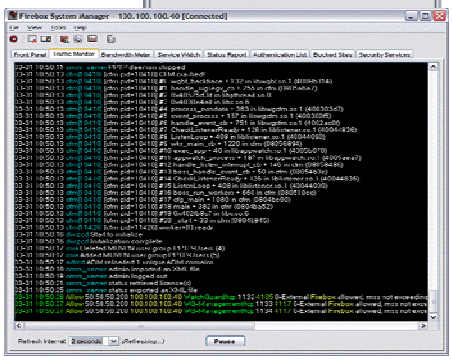


DVCP 技术来简化了 VPN 隧道的创建，它能认别一个 XTM 网络中必要的配置设定，并在不同位置之间自动建立 IPSec VPN。网络管理员可在任何地方通过我们的 WSM 软件对各个 VPN 隧道进行监控和配置，以确保网络的实时运行。这样在很大程度上可以减轻网络管理员的维护负担。

3.3 丰富的实时监控工具

WatchGuard System Manager（WSM）拥有一组实用的设备管理工具。

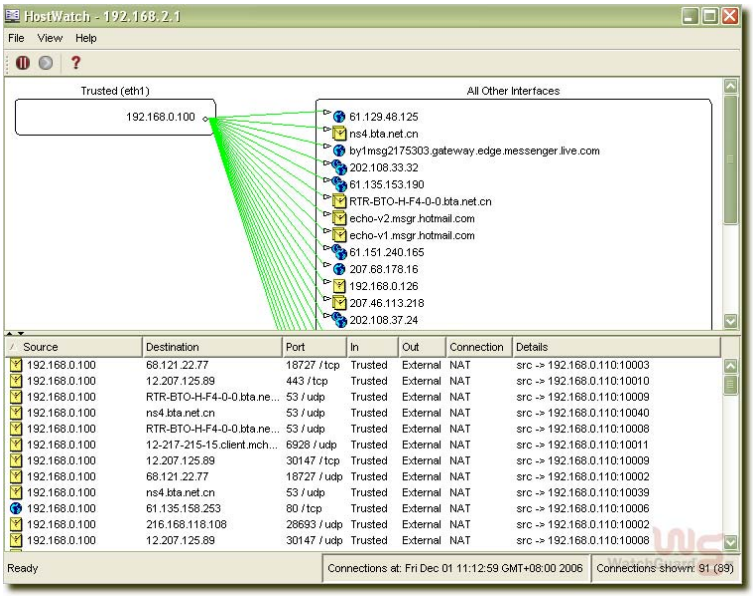




- XTM System Manager
  - 通讯日志实时查询；
  - 网络带宽实时显示；
  - 系统 CPU 利用率实时监控；
  - 通讯访问所匹配的安全策略数量监控；
  - VPN 带宽监控；
  - 认证用户监控、管理；

♦ HostWatch

用于帮助管理员实时地了解网络通讯状况。该工具可以显示出设定接口内 IP 地址对外的通讯情况，包括源 IP 地址、目的 IP 地址、使用的通讯端口、数据流向等信息。IP 地址和端口过滤功能，还可以方便管理员具体地了解某一台 PC 的通讯信息。同时，管理员可以立刻终止该 IP 地址对外的通讯连接。



3.4 强大的日志报告系统

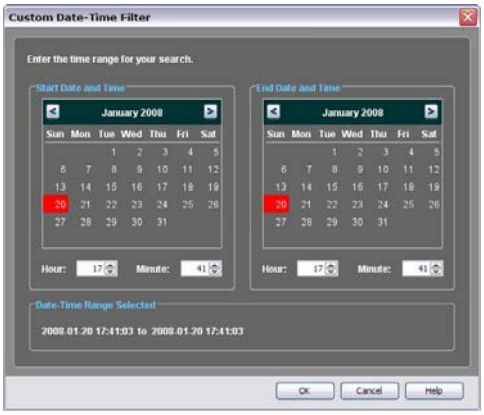
♦ 日志服务器

日志服务器采用了高级数据库技术，支持海量存储、快速检索、数据加密传输、远程访问。支持多台 XTM 共同存储在同一个日志服务器中。

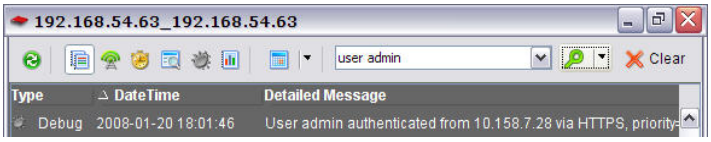
♦ LogViewer

LogViewer 工具是管理人员全面、详细分析日志数据的最强有力的工具。LogViewer 实时地从专用的日志服务器中提取数据，并可按照 6 种分类呈现在用户面前。

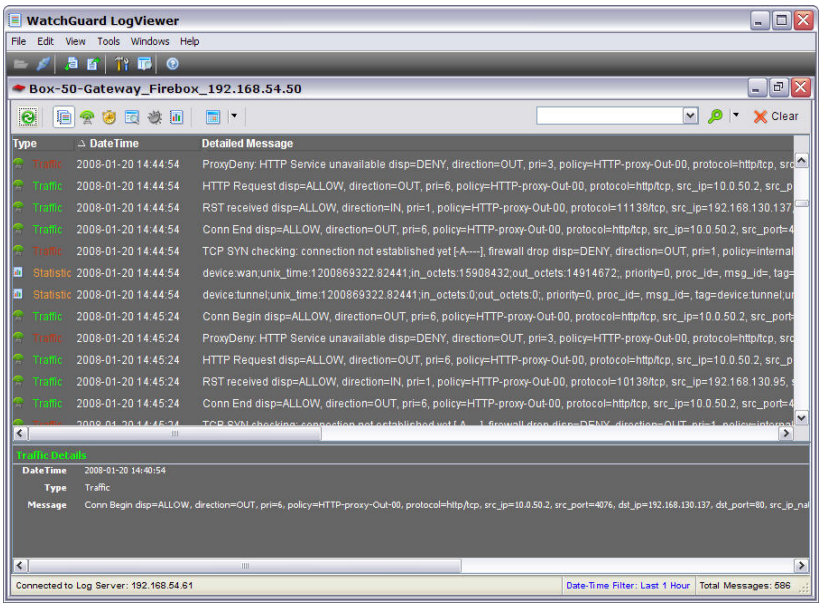
- 管理员可以快速地按照时间检索数据



- 管理员可以从海量日志中以关键字方式对数据进行搜索，并快速显示出来。



- 同时，在日志显示窗口中可以让管理员很清晰地看到每条日志的时间、IP 地址、通讯端口、翻译地址、处理方式等等详细信息。是管理员分析网络问题的绝好利器。



♦ Report Manager

日志报告系统实时地从日志服务器中提取数据进行分析，按照预算设计好的日志模板产生日志报告，并可以随日志数据的变化在线更新日志报告结果。管理员可以根据需要自己选择需要的日志报告模板，了解关心的数据通讯。例如：

- Web 通讯的数据流量

- 通过设备的数据流量图表