

Untangle™统一安全网关技术白皮书

- 病毒拦截
- 入侵拦截
- 垃圾邮件拦截
- Web 过滤
- 协议控制
- 间谍软件拦截
- 钓鱼攻击拦截
- 攻击拦截
- 防火墙
- VPN
- 路由器
- QoS
- 活动目录连接器
- 报表&日志

目 录

1.	防病毒网关	4
1.1	卡巴斯基病毒引擎	4
1.2	Clam AV 防病毒工具包	4
1.3	扫描协议	6
1.4	扫描方式	6
1.5	控制策略	6
2.	IPS	7
2.1	功能特点	7
2.2	核心技术	8
3.	垃圾邮件网关	9
3.1	核心技术	10
3.2	扫描协议	10
3.3	主要技术	10
3.4	控制策略	10
4.	Web 过滤	12
4.1	扫描协议	12
4.2	核心技术	13
4.3	控制策略	13
5.	协议控制	14
5.1	控制动作	15
5.2	技术实现	15
5.3	控制策略	15
6.	反间谍软件	16
6.1	扫描方式	17
6.2	技术要点	17
6.3	控制策略	17
7.	防网络钓鱼	18
7.1	支持的协议	18
7.2	技术要点	19
7.3	控制策略	19
8.	防 DOS 攻击	20
8.1	核心技术	20
8.2	控制策略	21
9.	防火墙	22
9.1	技术特点	23
9.2	控制策略	23
10.	VPN 与远程接入	24
10.1	OpenVPN	24
10.2	远程接入门户	25

	10.3 PC Remote.....	26
11.	路由器和 QoS.....	28
12.	报表和日志	29
13.	AD Connector.....	31
14.	策略管理	32

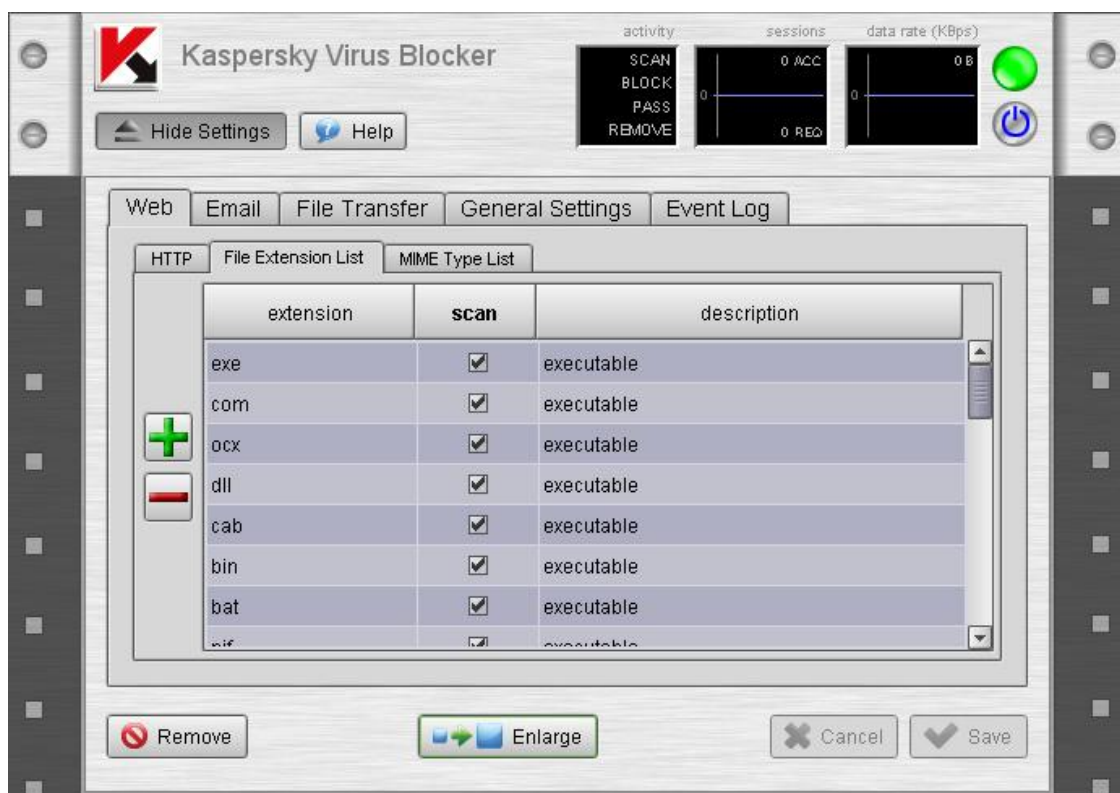
1. 防病毒网关

Untangle™统一安全网关采用业界非常优秀的两种防病毒方案：卡巴斯基杀毒引擎和 Clam AV 的防病毒应用包，在互联网入口处查杀病毒，保障您的网络不受病毒侵犯。

1.1 卡巴斯基病毒引擎

卡巴斯基病毒引擎是一款业界最为优秀的防病毒解决方案，可为您的商业应用提供最佳防护。使用它，网络管理者可轻松实现以下防护：

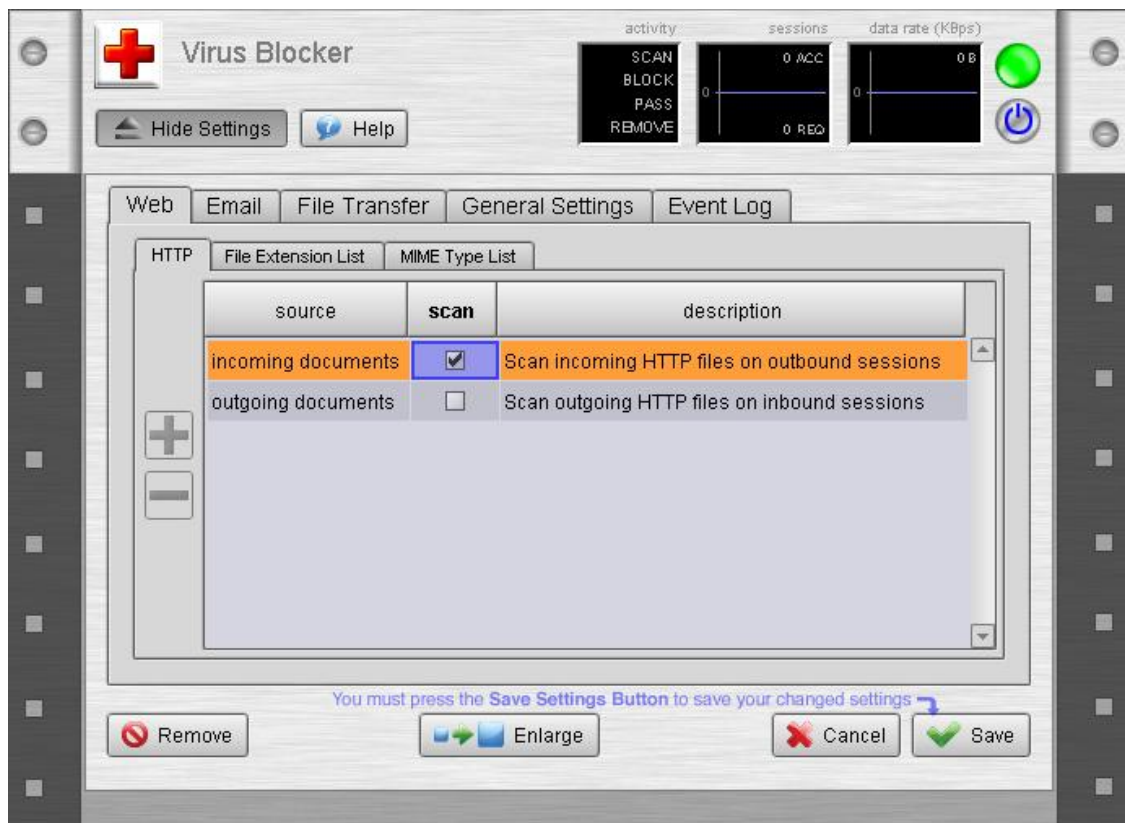
- 在网关处查杀病毒，防止病毒进入 PC 机或服务器。
- 实时保护 HTTP, SMTP, POP, IMAP & FTP 等各类应用，免受病毒攻击。
- 每小时自动更新病毒特征码



1.2 Clam AV 防病毒工具包

Clam AV 是一款优秀的网关防病毒工具包，它提供了多种病毒防护工具，包括：一个灵活、可扩展的多线程守护进程、一个命令行扫描器和一个高级的数据库自动升级程序。该工具包不但能在网络入口处阻止病毒入侵，并能有效防止病毒在公司内部网络上的传播。应用 Clam AV 的直观界面，可实现对多种协议的扫描：

- web (http), email (SMTP, POP & IMAP) 和 FTP
- 扫描文件内容和各种格式的压缩文件，如：Zip, RAR, Tar 等等
- 确保病毒码的实时更新



综合应用这两种病毒防护技术，可使您的网络远离病毒侵扰，包括：

- 查杀病毒、蠕虫和特洛伊木马
- 扫描文件内容和各种压缩文件，包括：Zip, RAR, Tar, Gzip, Bzip2, MS OLE2, MS Cabinet Files, MS CHM, 和 MS SZDD 等
- 防护“存档炸弹”，防止文件被反复压缩，因为这种反复动作通过消耗 CPU 资源而使其他的病毒扫描工具或程序崩溃。然而，Untangle 的防病毒网关可跨越这种技术威胁。

1.3 扫描协议

透明扫描 HTTP, FTP, SMTP, POP 和 IMAP 等各种协议

1.4 扫描方式

卡斯基病毒引擎和 Clam AV 病毒防护工具通过文件解压，将数据包还原成文件进行病毒扫描，并且可随心所欲地扫描大型文件。

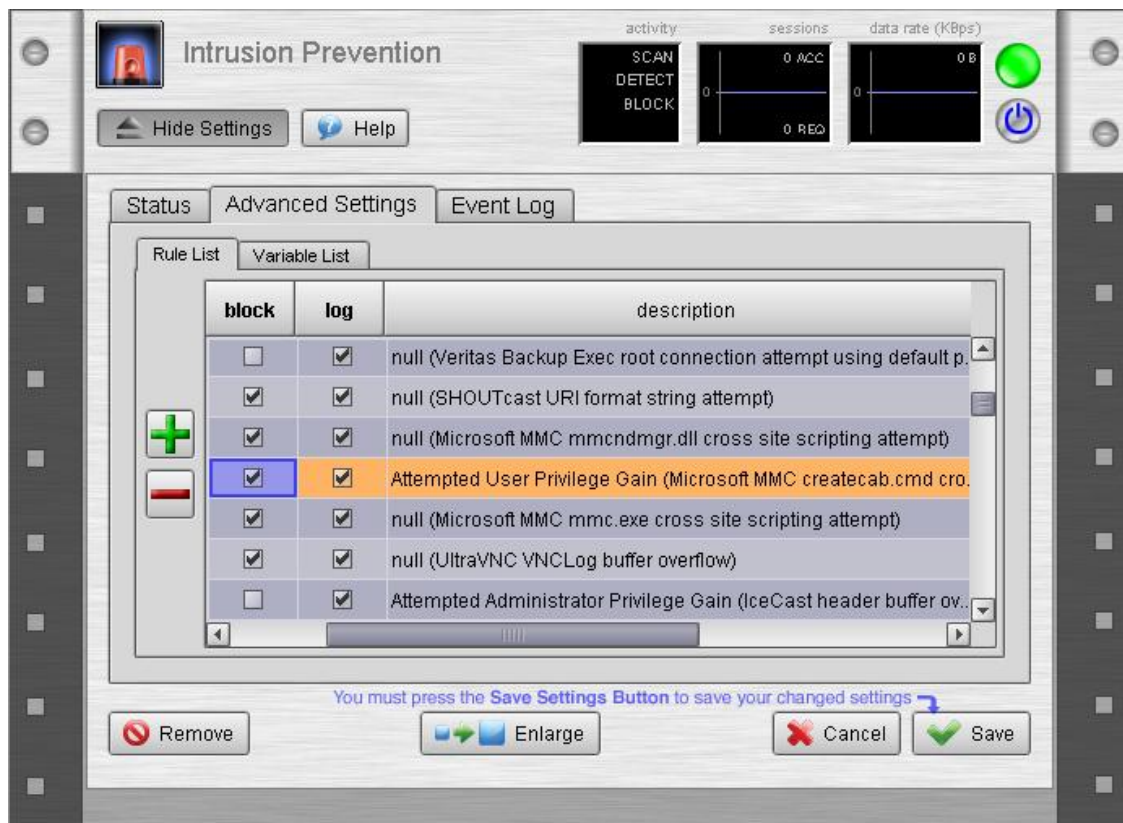
1.5 控制策略

- 可配置为对进/出的流量类型进行扫描
- 此外：
 - HTTP: 通过文件扩展名或 MIME 类型进行可配置的扫描
 - SMTP: 查杀病毒并可设定为清除感染、阻止或允许、包含或不包含发送者/接收者
 - POP and IMAP: 查杀病毒并可设定为清除感染或放行（POP 和 IMAP 的协议特性使邮件不能够被阻止，但可被扫描并被清除。）
 - FTP and HTTP: “下载继续”可被切断
- 扫描速率可配置，以支持大型文件。

2. IPS

Untangle™统一安全网关可在黑客攻击内网服务器和 PC 机之前阻止攻击企图。利用预先设定的基于特征码的 IPS，网管人员可轻松应对外部威胁。

- 提供 24/7 网络保护，免受黑客攻击。
- 降低烦人的误报。
- 确保特征码的实时自动更新。



Untangle™统一安全网关的 IPS 可以拦截所有网络流量，通过使用基于已知攻击模型的特征码检测技术，它还能够检测出网络内部的恶意行为。

在阻断恶意用户的同时，该 IPS 功能对于用户完全透明，对网络性能也没有任何影响。它不但能发现恶意行为，而且能够阻断这种恶意企图。

另外，该 IPS 功能在出厂时已通过缺省设置自定义好了，客户无需更多配置。

2.1 功能特点

- 可设定特定的特征码来阻止并记录攻击行为
- 使用自定义规则和变量来创造新的特征码

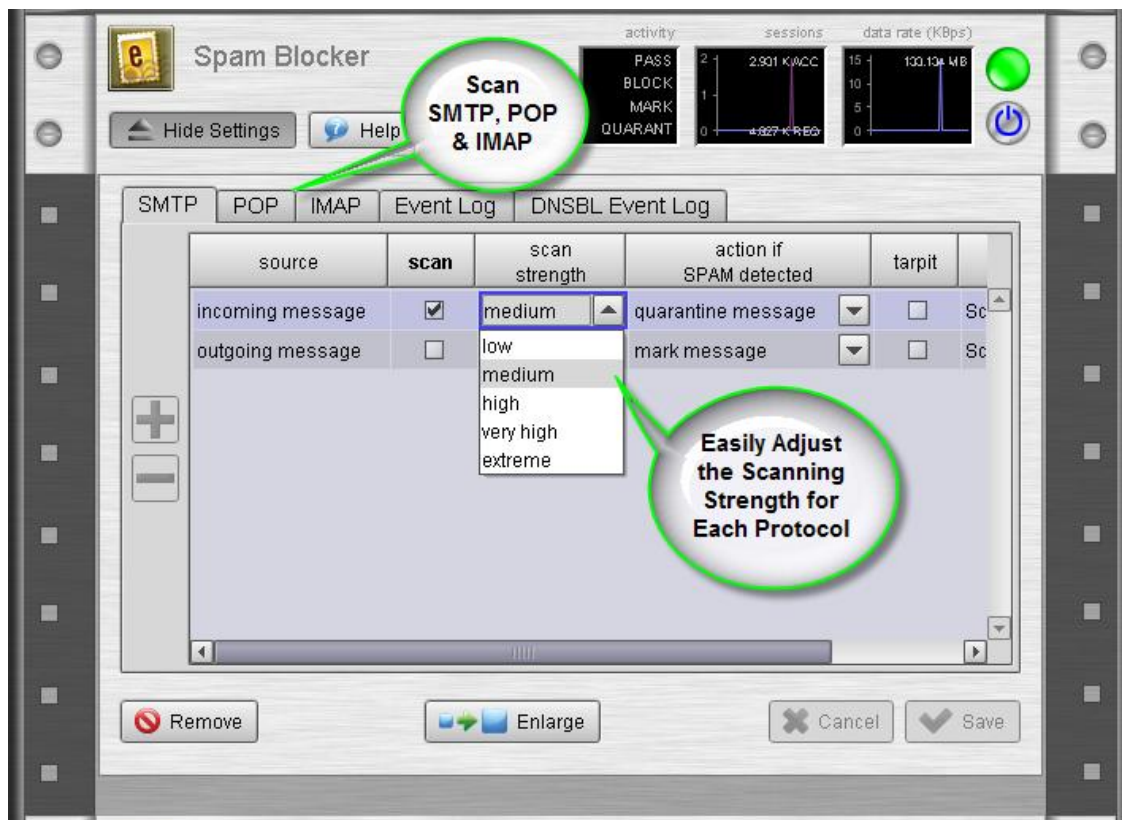
2.2 核心技术

Untangle™统一安全网关使用业界非常独特的 Snort 技术来实现 IPS 的特征码识别。通过 Snort 显著的信息包有效载荷探测技术，很多额外种类的恶意行为可以被有效探测到。

3. 垃圾邮件网关

Untangle™统一安全网关的垃圾邮件模块可在网关处阻止垃圾邮件。零配置和直观的 GUI 可让网管人员轻松应对日益泛滥的垃圾邮件。

- 最好的垃圾邮件过滤技术，包括贝叶斯过滤、Razor、实时阻止列表（RBLs）、OCR 图像垃圾邮件识别和 tarpitting 技术。
- 为每一个邮箱提供单独过滤
- 过滤 SMTP, POP 和 IMAP



该垃圾邮件网关可智能识别未经请求的大量垃圾邮件，它能扫描以下邮件协议：

- SMTP
- POP
- IMAP

每一个协议都对应为一组控制策略，可个性化设置为：

- 扫描所有垃圾邮件

- 垃圾邮件用户通知
- 管理垃圾邮件

借助于产品直观的用户界面，您可将垃圾邮件阈值设定为严格扫描、一般扫描或不扫描，并且可通过属性设置达到灵活控制，如：

- 在邮件主题中插入垃圾邮件关键词，并允许用户将垃圾邮件过滤到指定的文件夹。
- 无需将邮件标记为垃圾邮件即可将邮件发送到接收者。
- 无需通知接收者邮件为垃圾邮件，直接阻止该邮件，并且在事件记录中记录该动作。
- 隔离邮件直到用户判断其是否为垃圾邮件
- 通知发送者邮件已被阻止
- 通知扣留

3.1 核心技术

Untangle™统一安全网关的垃圾邮件过滤模块采用了目前世界上最先进的 SpamAssassin 垃圾邮件过滤技术。它能捕捉几乎所有的垃圾邮件，而不需要隔离合法邮件，通过 SpamAssassin 技术来判断是否为垃圾邮件的辨别率高达 99%，极少有垃圾邮件能躲过了 SpamAssassin 过滤器的探测。

SpamAssassin 不单是使用匹配规则来标识可能是垃圾邮件的邮件，它还采用了一种概率统计的、基于分数的方法来对消息分类。它没有寻求创建那些将消息标识为“一定是垃圾邮件”或“一定不是垃圾邮件”的规则，而是使用利用概率来推断给定的消息是垃圾邮件的可能性的规则。标准 SpamAssassin 规则集中有几百条规则，每条规则都设置了权重，通过权重组合来产生垃圾邮件分数，这些分数可以说明是否为垃圾邮件的可能性。

SpamAssassin 还使用了称为自动筛选的统计技术，来了解您收到邮件的特征，并使用它来调整垃圾邮件的分数。

3.2 扫描协议

透明扫描 SMTP, POP 和 IMAP，并能阻止、隔离或标记垃圾邮件。

3.3 主要技术

采用 SpamAssassin, Razor, 贝叶斯过滤, DNSBL/RBLs, 光学字符识别(OCR), tar pitting, 自定义调整和更新。

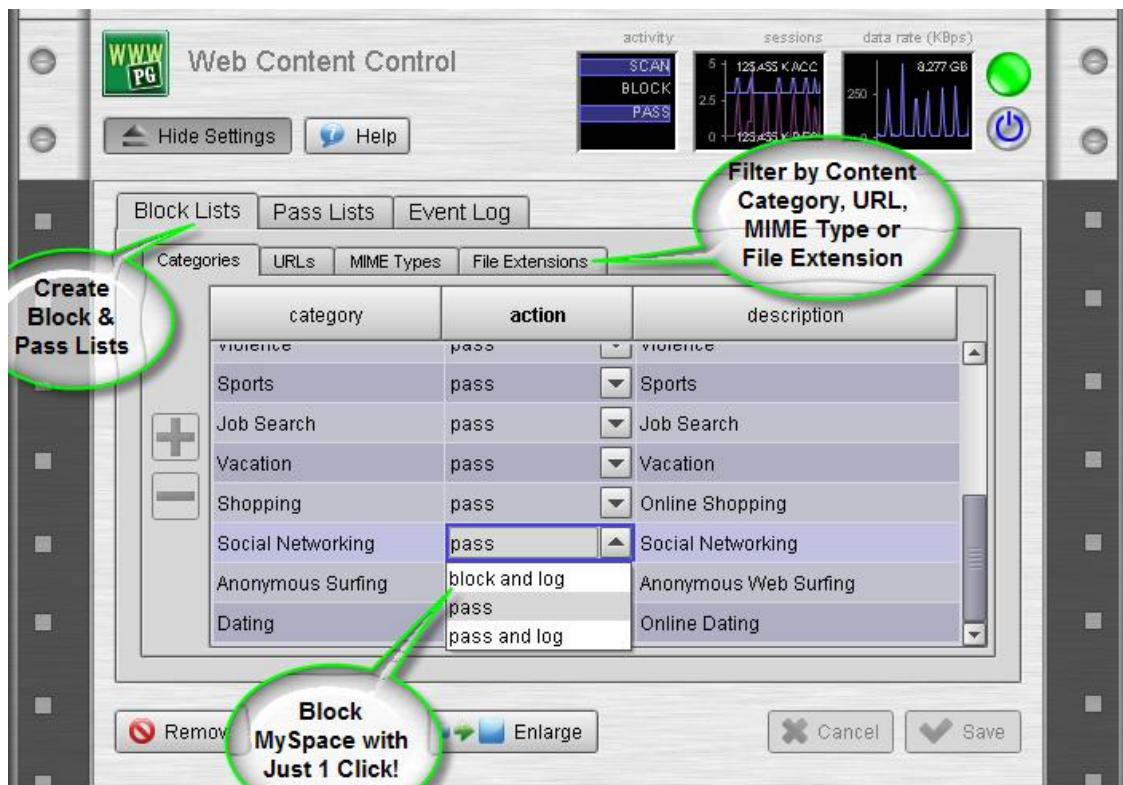
3.4 控制策略

- SMTP: 能够隔离、标记、通过/阻止进出邮件，可设定有/没有发送通知
- POP and IMAP: 标记或放行进出邮件（POP 和 IMAP 协议可以防止邮件消息被阻止或隔离，但它们可以被扫描和被标记）
- 基于每个用户的安全列表和隔离目录
- 通过浏览器来方便管理个人隔离目录和安全列表
- 可按协议、流向来调节扫描强度

4. Web 过滤

Untangle™统一安全网关能使用户实施网络使用策略，并监控用户使用行为。客户端零安装，丰富的阻止列表为用户提供了简便的 web 控制手段。

- 保护网络不受 web 上的恶意软件侵扰
- 阻止 MySpace
- 阻止视频下载



该模块采用世界上最权威的 URL 分类工具 URLBlacklist.com 来对 Web 内容进行控制。该分类包括色情、赌博等超过 50 个类别或主题。使用 Web 内容控制，可让您在工作场所定义 web 内容控制策略，同时，也可以基于主机、域名和文件类型等自定义的 URL 阻止列表来阻止更多 web 内容。

另外，您也可以通过黑名单/白名单来自定义控制策略。

4.1 扫描协议

透明扫描 HTTP 流量来记录或阻止特定行为。

4.2 核心技术

Untangle™统一安全网关的扫描引擎配以 URLblacklist.com 的 URL 分类列表，达到最佳的 URL 过滤效果。同时可自定配置过滤列表，并保持实时更新。

4.3 控制策略

- 阻止、记录所有 HTTP 流量 (Web ON/OFF)
- 阻止列表
 - **基于分类的阻止列表:** 可配置为通过、通过并记录、阻止并记录等
 - **URL 阻止列表:** 可添加特定的 URL，阻止并记录
 - **MIME Type & File Extension 阻止列表:** 可阻止特定的 MIMEs 或扩展文件
- 白名单
 - **URL 白名单:** 允许特定的 URL 通过，即使它们已在分类列表当中
 - **客户端白名单:** 可对特定的 IP 地址设定为完全不受控制

5. 协议控制

应用Untangle™统一安全网关的7层协议过滤功能，管理人员可完全掌控P2P、在线游戏等网络滥用行为。

- 通过封堵 P2P 等开放多个 TCP 端口的应用，以保证带宽。
- 通过阻止防火墙规则无法完全禁止的 IM、在线游戏等应用，来提高工作效率。
- 为任一协议编写自定义特征码。



该协议控制模块可双向阻止受控软件对受保护网络的访问，如限制视频游戏、流媒体下载、即时消息和 P2P 等应用。

协议控制模块通过使用特征码，在所有端口上来界定需要控制的协议。许多协议如 IM 和 P2P 通过传统的防火墙很难阻止，因为这些协议会进行端口跳转。一旦在缺省端口被阻断，他们就会通过 80 或 25 端口进行网络连接。而 80 和 25 端口是 Web 和 e-mail 常用的端口不能被禁止。Untangle™统一安全网关的协议控制模块能够识别这种端口跳转行为，进而阻断并记录网络连接企图。

另外，如果某个您想阻止的协议没有在协议控制模块中预先设定，您也可以通过安全网关的用户界面自定义规则来阻止额外的协议。

5.1 控制动作

透明扫描各种数据流应用，阻止并记录指定协议。

5.2 技术实现

- 基于 OSI 7 层协议对协议进行分类并过滤，不受端口或端口跳转影响。
- 使用 Untangle 自定义的扫描引擎，缺省设置、调整和更新。

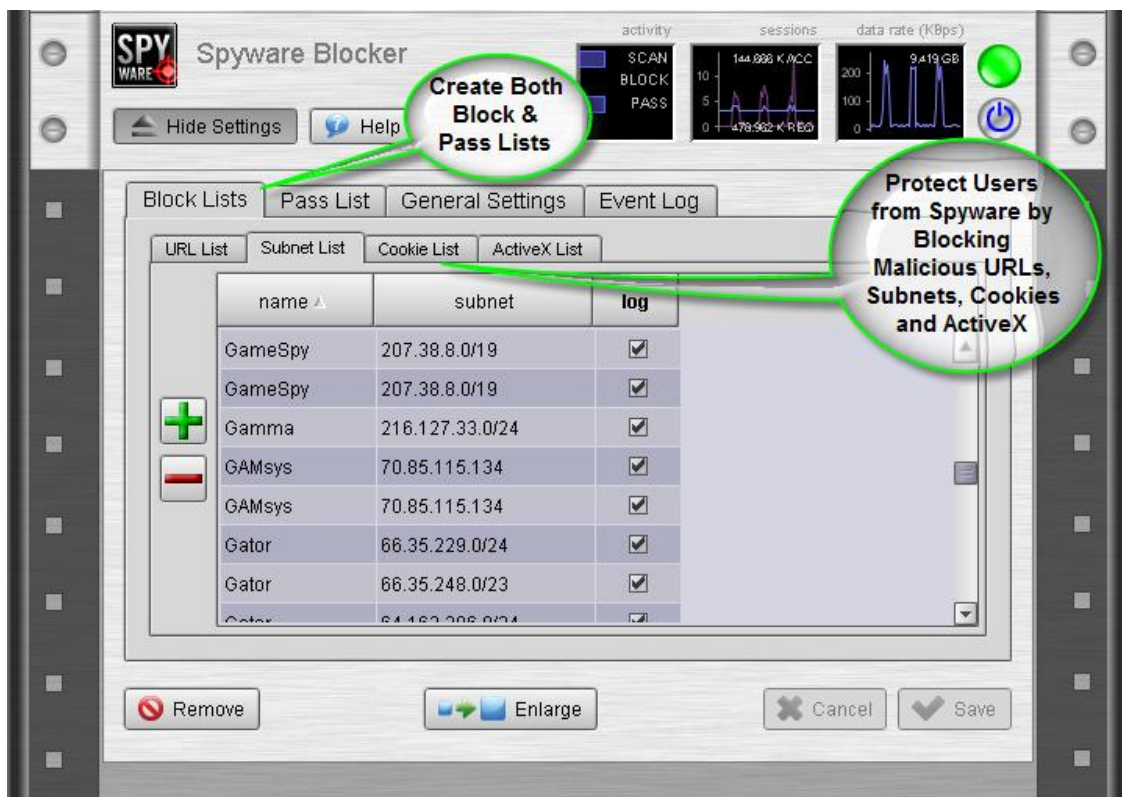
5.3 控制策略

- 缺省设置包括广泛的协议特征码，并且这些特征码可以被配置为记录或阻止。
- 可添加自定义特征码。

6. 反间谍软件

Untangle™统一安全网关的反间谍软件功能具有以下功能：

- 保护用户浏览网站时不受恶意软件威胁
- 扫描网络流量，在用户可能误装间谍软件时进行阻止
- 确保特征码实时自动更新



反间谍软件通过检查网络内部的 web 请求，实现：

- 运用病毒特征码来侦探并识别特定病毒
- 阻止 keyloggers, 这个计算机程序能够捕获并存储键盘敲击
- 提供 URL 黑名单，以阻止已知的间谍软件网站（如 gator.com）
- 提供 URL 黑名单，以组织要求 cookies 的网站
- 阻止有害的 ActiveX 控件，以免遭受间谍软件威胁
- 检查访问网站的 IP 地址并与受攻击子网的 IP 地址进行对比

当非正常事件发生时，如你要访问的合法网站被反间谍软件认为是恶意的，统一安全网关允许你创建例外规则，并将该合法网站从反间谍软件黑名单中去除。此外，统一安全网关的快速白名单允许用户临时或永久放行某些站点。

6.1 扫描方式

透明扫描任何端口的 HTTP，基于列表扫描 URL、子网、cookies 和 ActiveX 控件。

6.2 技术要点

使用基于 [ClamAV](#) 的防病毒技术，以及客户自定义的黑名单实现对间谍软件的阻止。

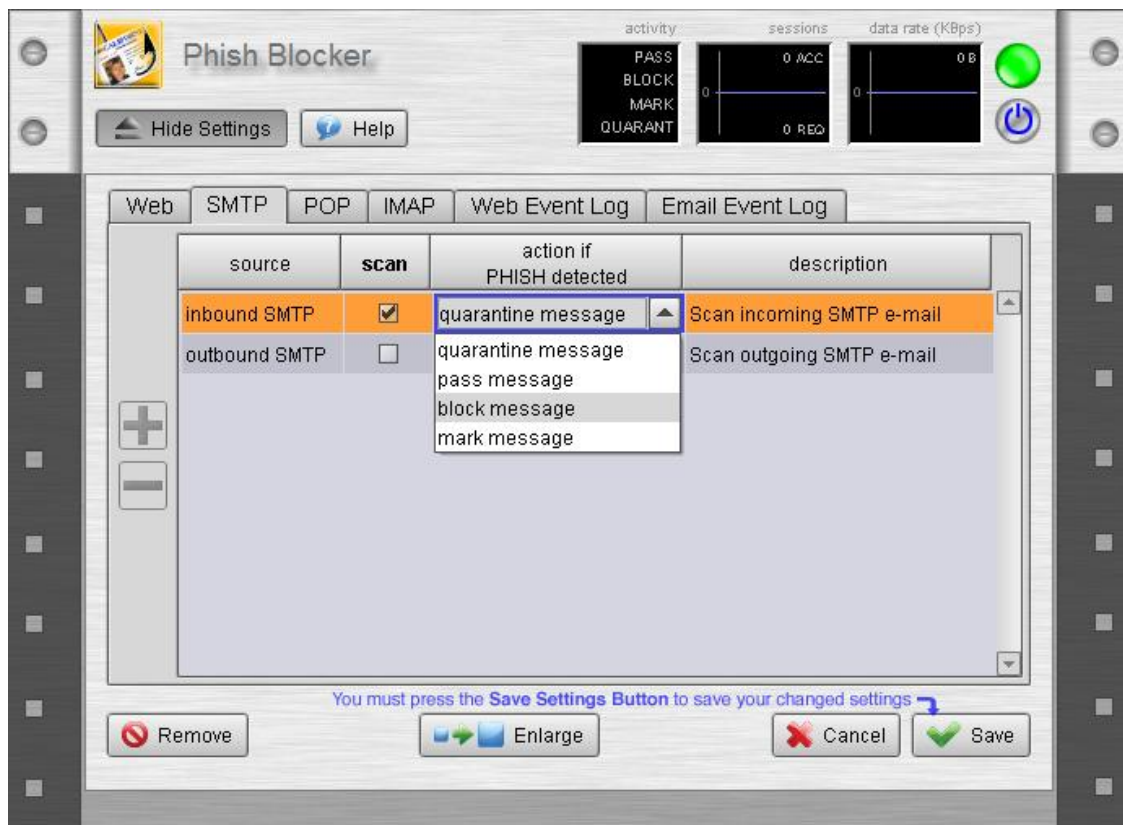
6.3 控制策略

- 自定义 cookies, 子网和 ActiveX 的黑名单
- 自定义 URL/域名 白名单
- 独特的快速白名单：网管人员可选择为某些用户设定不受限网站
 - 可配置为允许临时、基于单个用户的不受限访问
 - 也可配置为永久的不受限访问
- 阻止/允许 ActiveX

7. 防网络钓鱼

随着 email 和站点欺诈越来越难以辨别，识别网络盗贼也越来越复杂。Untangle™统一安全网关的防钓鱼功能将使事情变得简单起来。

- 保护用户免受 email 钓鱼攻击和域欺诈网站的欺骗
- 对 HTTP, SMTP, POP & IMAP 等多个协议进行保护
- 确保特征码实时自动更新



统一安全网关的防钓鱼功能主要通过身份盗窃拦截器（Identity Theft Blocker）实现的，它是一个智能 email 过滤器，它能识别有钓鱼企图的 email，这种 Email 通常包含虚假链接或窃取代码信息。身份盗窃拦截器（Identity Theft Blocker）能够扫描以下协议的 email：

- SMTP
- POP
- IMAP

7.1 支持的协议

透明扫描 SMTP, POP 和 IMAP 的钓鱼特征码

7.2 技术要点

基于 ClamAV 引擎和钓鱼特征码数据库来实现防钓鱼功能。

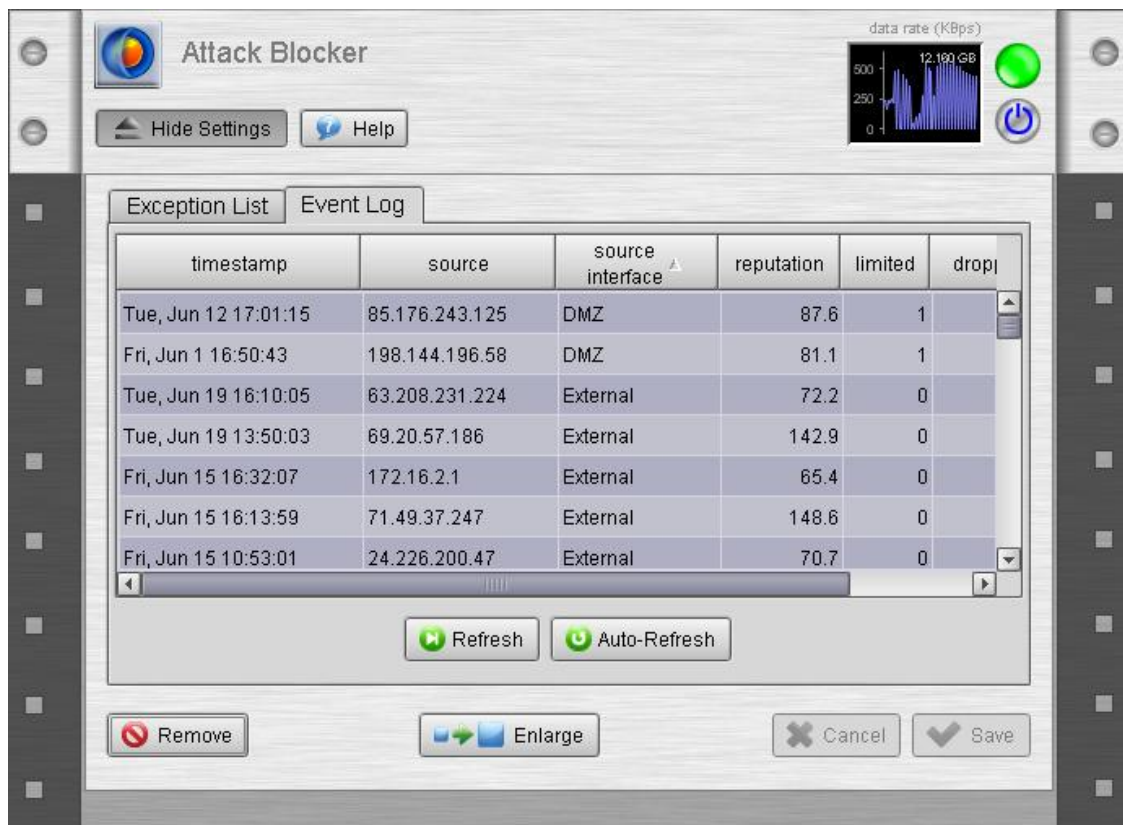
7.3 控制策略

- 可按流量类型扫描接收/发送邮件
- 此外:
 - SMTP: 一旦检查到, 可被隔离、阻止、标记或通过, 可设定发送或不发生通知
 - POP and IMAP: 一旦检查到, 只能被标记或通过 (POP 和 IMAP 协议不能被阻止或隔离)

8. 防 DOS 攻击

Untangle™统一安全网关的 Attack Blocker 防 DOS 攻击模块具有以下特点：

- 为您的网络提供 24/7 免受 DOS 攻击保护
- 启发式流量评级排序 Sort，以区分安全流量和问题流量
- 赋予合法用户基于白名单的带宽分配



Untangle™统一安全网关通过以下途径来实现防 DOS 攻击：

- 清洗接收到的所有数据包，并清除所有基于数据包的攻击，而且无需您做任何配置，产品已经内建了数据包清洗功能。
- 防止级别较低的网络攻击
- 阻止 DOS 攻击

8.1 核心技术

Attack Blocker 防 DOS 攻击模块，采用了 Untangle 独有的专利技术，该技术通过分

析网络用户的行为，迅速为主机给出评级。该技术通过判断用户是否进行 SYN 洪水攻击或端口扫描，来判断用户是否具有攻击性，一旦被认为具有攻击企图，即予以迅速负面评级，依据评级指标，Attack Blocker 最终将限制、丢弃或拒绝这些用户的网络连接请求。

运用该技术，Attack Blocker 可极大地减轻 DOS 和 DDOS 攻击。Attack Blocker 还通过解构进入统一安全网关的每一个数据包，并重新构建一个新的、值得信赖的数据包（不改变数据本身）来消除攻击。

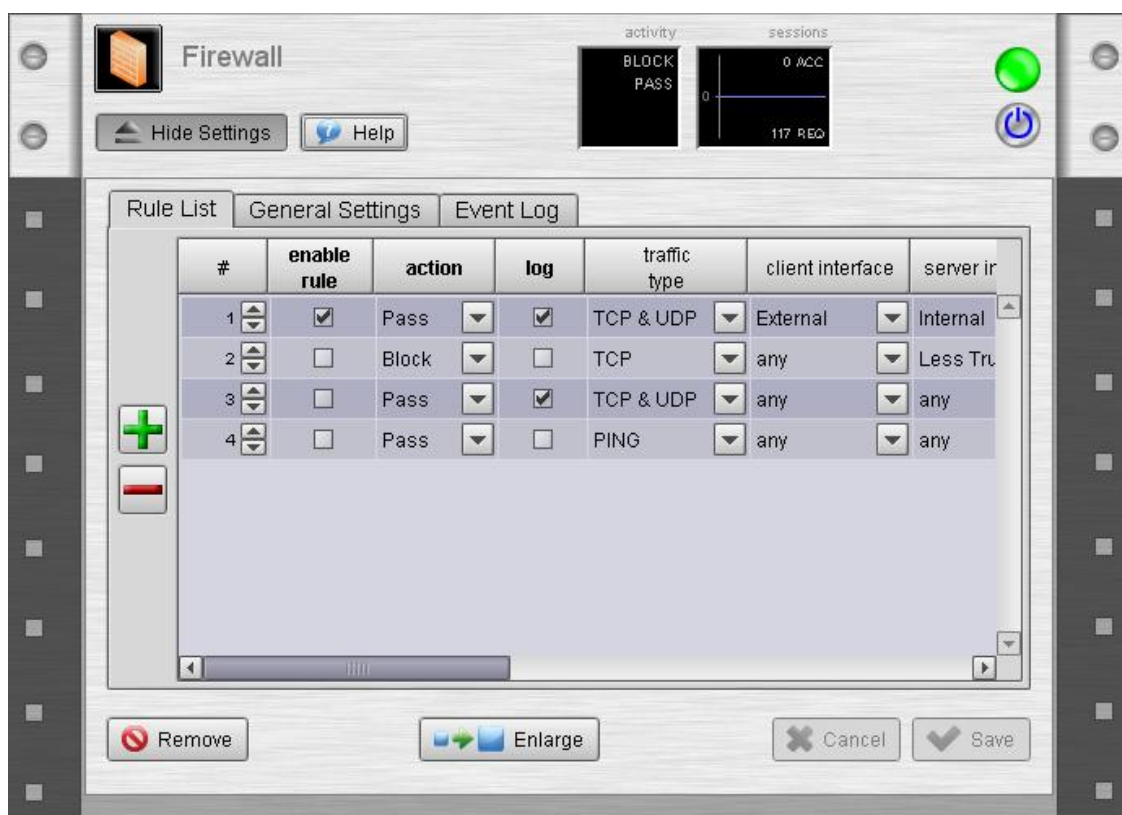
8.2 控制策略

您可通过创建例外名单来指定某个特定的主机或网络为非攻击类型。

9. 防火墙

防火墙通过划分内外网的界线，在网络边界处搭建第一道安全防线。Untangle™统一安全网关的防火墙利用 IP 地址、协议和端口等多种手段来过滤网络流量。

- 标示哪个系统和服 务（如 http, ftp 等）是公开可用的
- 创建 DMZ，并执行 NAT (基于路由器)
- 可作为透明的网桥来使用



防火墙基于简单、灵活的规则来监控和阻止网络流量，它通过以下手段来控制流量：

- 基于协议控制
- 源地址或源端口
- 目的地址或目的端口

运用以上手段，您可以创建您自己的规则列表，并且命令防火墙如何响应这些规则。

9.1 技术特点

Untangle™统一安全网关的防火墙使用了 Untangle 私有的专利技术，进行基于规则的日志记录或网络流量阻止。

9.2 控制策略

- 缺省动作为“阻止”或“放行”
- 按照以下策略来自定义日志记录、阻止或放行的规则：
 - 协议
 - 方向
 - 源地址
 - 目的地址
 - 源端口
 - 目的端口
- 可自定义规则匹配命令

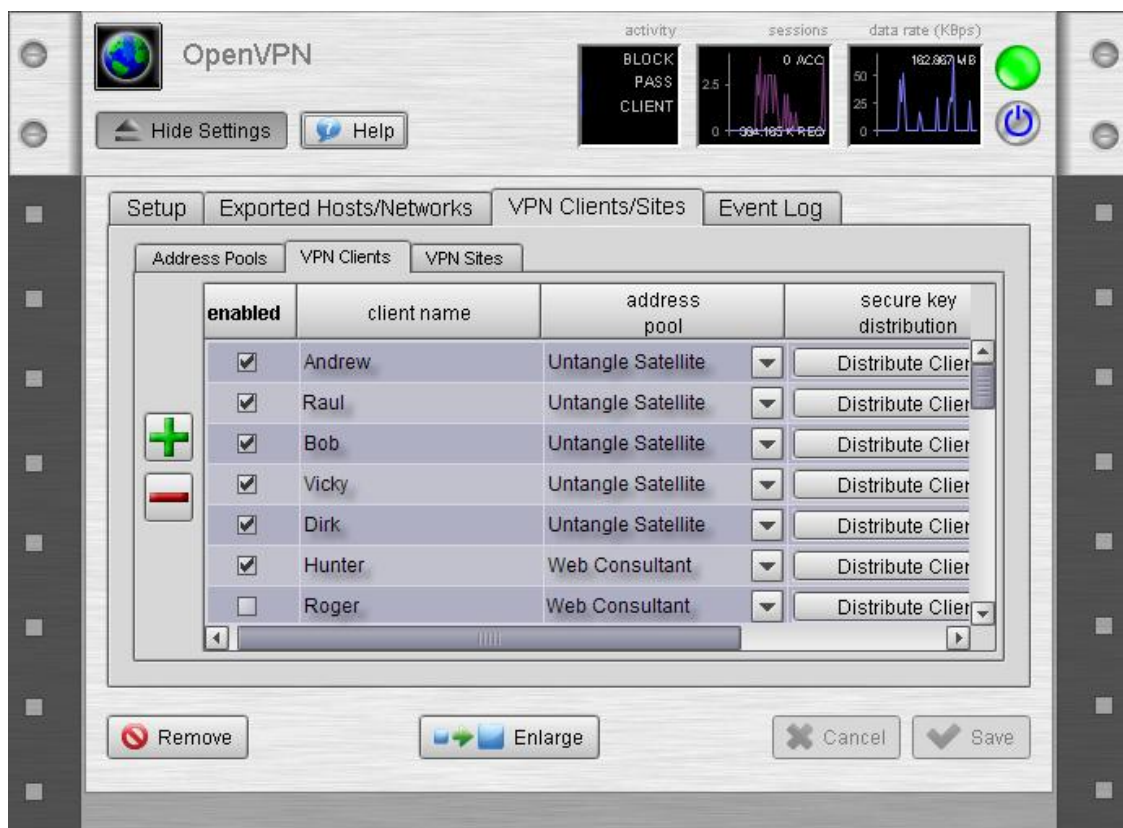
10. VPN 与远程接入

Untangle™统一安全网关提供了 3 种远程访问内网的手段，分别是 OpenVPN，远程接入门户(RAP)，和 PC Remote。

10.1 OpenVPN

OpenVPN 提供了远程安全地接入内部网络的一种有效手段，它直观的界面可使您：

- 通过安装向导，配置基本设置
- 为每一个客户端生成自定义证书
- 通过 email 分发客户端软件



OpenVPN 是一种基于 SSL 协议的 VPN，它支持点到点（site-to-site）和端到点（client-to-site）的 VPN。当你创建新的客户端或远程访问点时，OpenVPN 为每个客户端生成一个自定义可执行文件，这个文件包含客户端、配置和认证信息。用户只需安装这个自定义可执行文件即可。OpenVPN 支持下列操作系统：

- Windows 2000/XP/其他

- Linux
- OpenBSD
- FreeBSD
- NetBSD
- Mac OS X
- Solaris

技术要点

不像大多数其他使用网络层的 VPN 协议，SSL 协议运行在应用层，无需复杂操作即可提供高度安全可靠的远程网络连接。其关键点在于 tun/tap 虚拟网络适配器，tun 适配器就像 T1 一样，它是一个模拟以太网的点到点连接。

概括地说，SSL 将 IP 包装进 UDP 包中，IP 包从一个 tun 或 tap 虚拟适配器发送出去，加密后被装进一个 UDP 连接中，并被送往 Internet 上的一个远程主机，这个远程主机解密、认证后，同样使用 tun/tap 虚拟适配器对这个 IP 包进行解包。

这个 VPN 模型通过连接本地的 tun/tap 虚拟适配器和远程的 tun/tap 虚拟适配器来创建，就如同其他使用硬件适配器的 VPN 协议一样。当这个连接通过 SSH 安全端口转发工具进行转发时，VPN 的连接此时是非常安全的。

控制策略

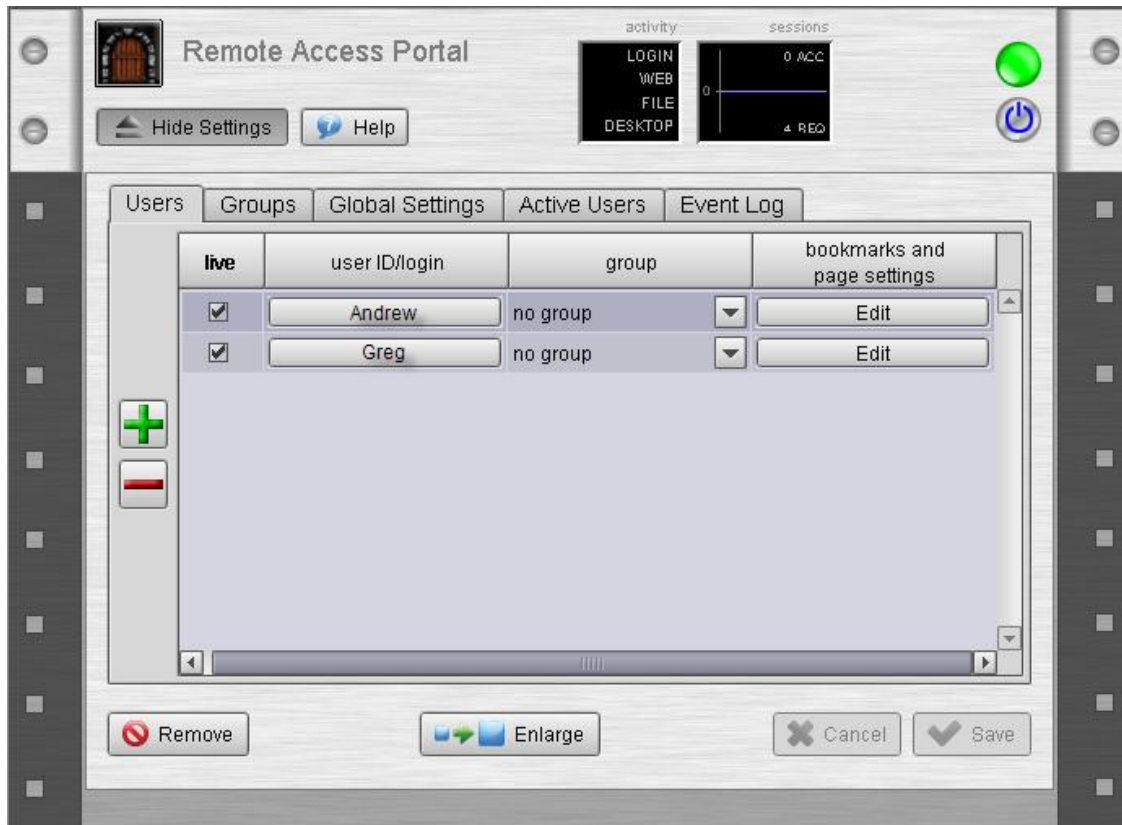
- 端到端和点到点的 VPN 设置向导
- 可选服务器端口和 DNS 覆盖设置
- 可具体指定向 VPN 开放的主机/网络
- 包含一个客户端分发工具包，以便通过 URL 或 USB key 安全分发密钥

10.2 远程接入门户

远程接入门户（RAP）提供基于 web 的远程安全内网接入，它无需任何 VPN 客户端安装。它具有：

- 任何时间、任何地点通过互联网远程接入内网
- 远程安全访问内网文件服务器、web 邮箱和其他应用
- 通过微软 AD 进行认证

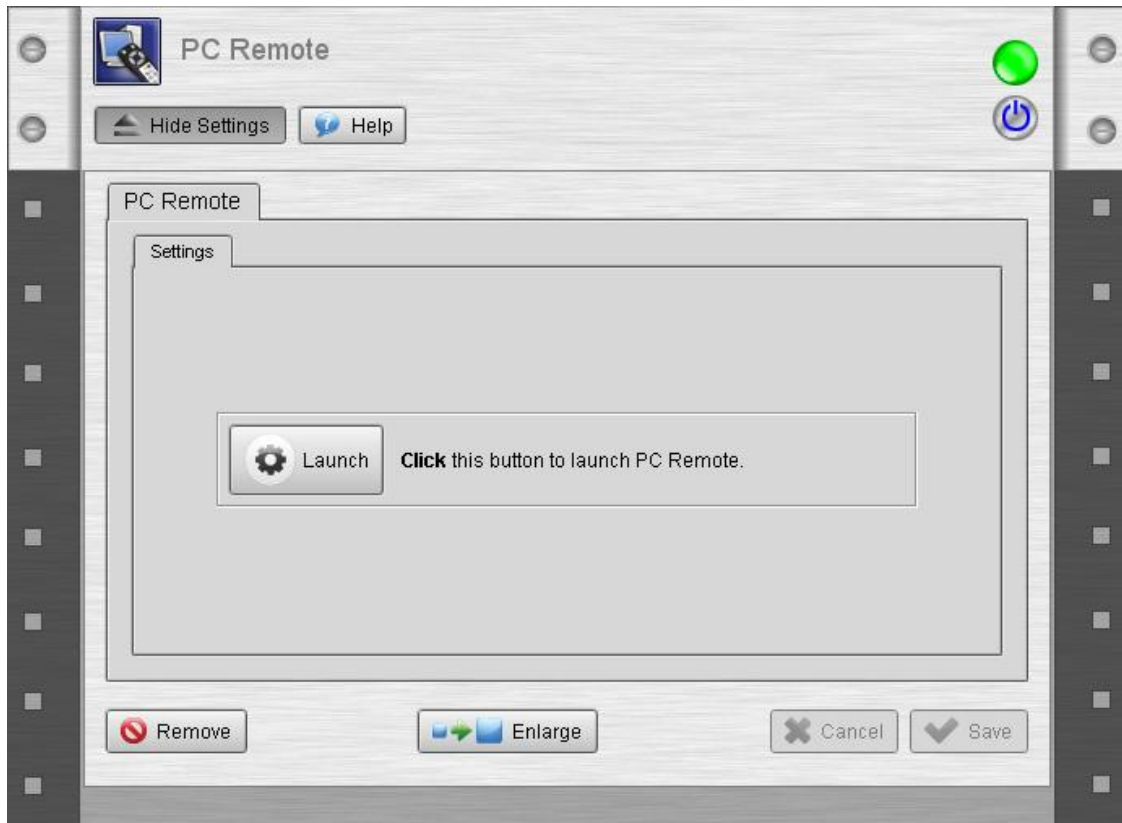
RAP 属于 SSL VPN 的一种技术。基于浏览器的无客户端安装的 SSL VPN 越来越流行，因为它的易用性和细粒度的访问控制。它也提供了非常可靠的远程连接，因为 RAP 看起来像是一个应用而非一个网络元素。通过使用应用层协议，它可以穿越 NAT、防火墙和代理服务器，这有助于从任何地点方便访问网络内部资源。



10.3 PC Remote

PC Remote 可使网管人员远程接入统一安全网关，它具有：

- 提供非现场的桌面支持和问题解决
- 基于网络快速扫描桌面用户和服务器
- 无需安装任何软件即可连接桌面用户和服务器

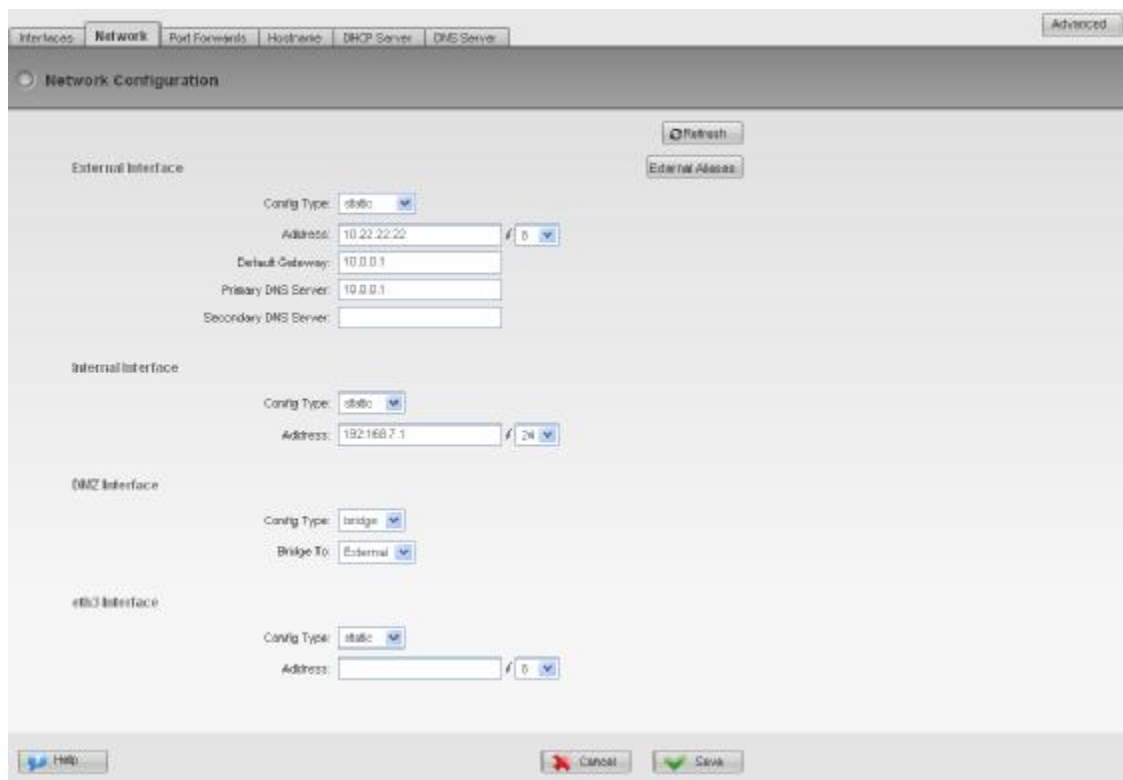


PC Remote 是网管人员最好的朋友，当您远离办公室而您的用户需要桌面帮助时，PC Remote 可帮您轻松搞定！通过 PC Remote，网管人员可接管用户桌面。配置也很简单，因为 PC Remote 可与 RDP (XP Pro & Vista) 和 VNC (Ubuntu) 系统无缝连接。不论您是在解决间谍软件所引起的问题，还是帮助进行基本配置，或是在打补丁，PC Remote 可让您通过 Internet 在任何地方针对目标电脑实施帮助。

11. 路由器和 QoS

Untangle 是一个非常灵活的应用平台，它不但作为透明网桥，还具有路由功能：

- 支持 NAT, DMZs, DHCP & DNS
- 支持多个 NAT，路由表和可配置的 MTU
- QoS 保证，优先分配流量（5.3 版本支持）



Untangle 的路由功能可通过 NAT 允许所有主机共享 internet 接入，并且提供 DHCP 和 DNS 服务，以及高级路由功能。

网管人员可配置 NAT、相关的重定向规则、以及 DMZ 主机设置。也可添加静态 DHCP 和 DNS 项，以及自定义路由以支持更多复杂网络。

QoS 流量整形功能将在 5.3 版本发布。

12. 报表和日志

Untangle 的报表非常直观，通过展现必要的数据来了解相关安全事件，并以此来实施可接受的网络使用规则。

- 监控网络使用行为和安全事件级别
- 理解流量和网络使用模型
- 支持 PDF 和 HTML 格式的报表



Untangle 软件记录事件，并形成日志文件。基于日志文件中信息的要求，可按每天、每周、每月编辑报表。

Untangle 报表可储存 30 天。当然你也可以将报表 email 给相关人员，也可以直接通过 web 来查看。

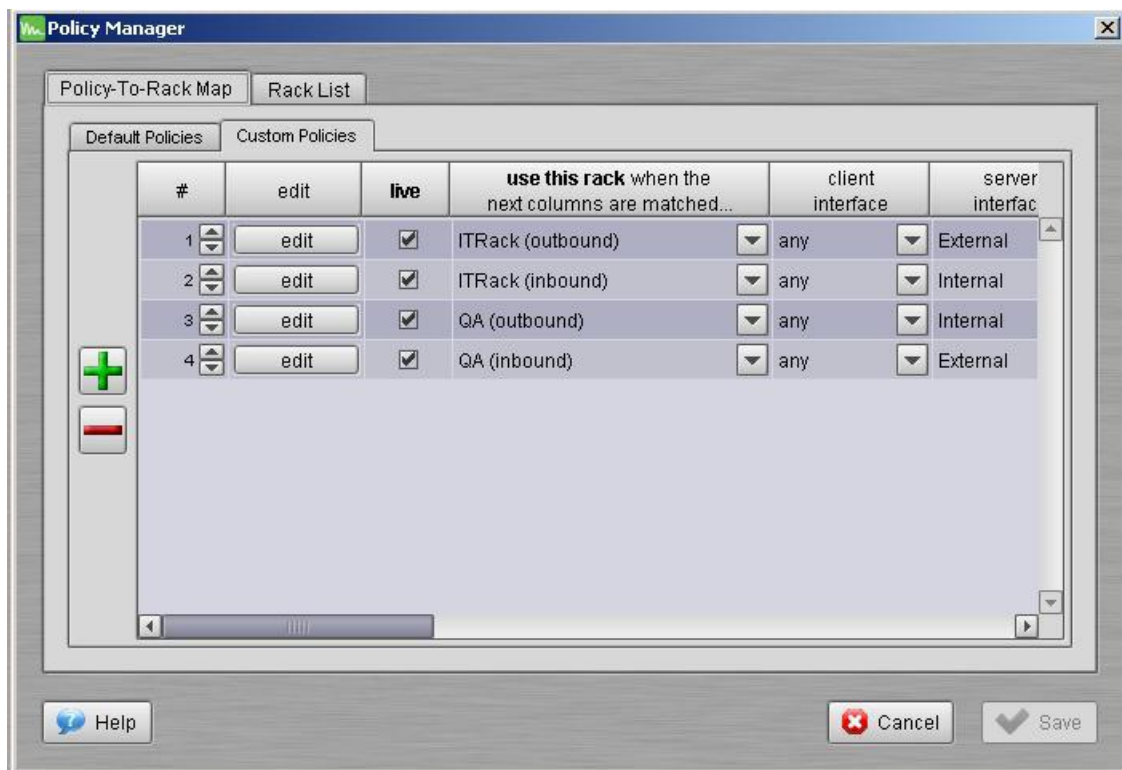
报表特点：

- 具有重要统计的总结
- 基于事件的详细报表
- 可基于以下方式获得特定用户的报表：
 - AD
 - IP 地址
- 报表可自动 email 给指定的接收者
- 可自定义日、周、月报表计划

13. AD Connector

Untangle 的 AD Connector 设计来利用 AD 服务器来简化策略管理，并且丰富报表。AD 功能如下：

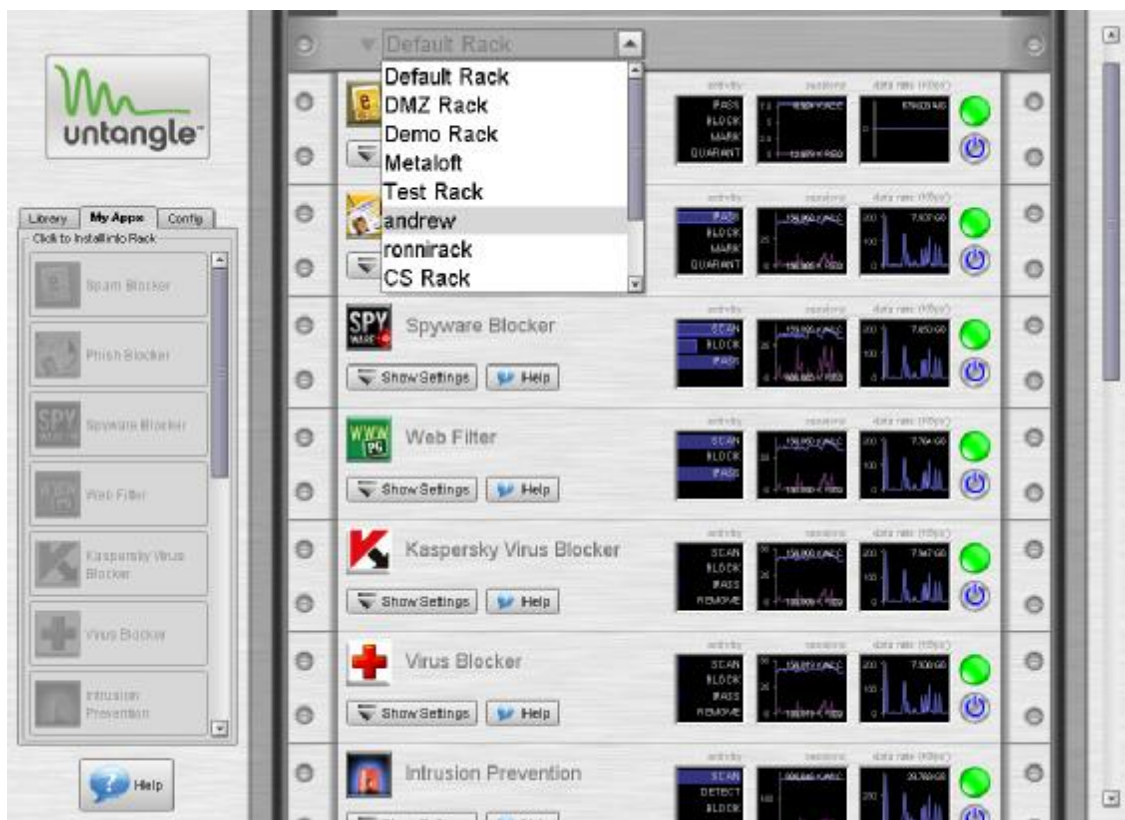
- 基于远程接入门口（RAP）来认证
- 按用户名提供报表
- 按用户名来实施策略，如 web 内容控制策略等



14. 策略管理

通过策略管理功能，可按用户或时间来设定网络准入规则。

- 按用户名来创建网络准入规则
- 按时间或一周中的某一天来创建网络准入规则
- 通过设定，允许某些用户使用某些应用，如即时通讯、游戏或视频流



策略管理增加了负责网络管理中的个性化。许多组织愿意为不同的用户（用户组）设定不同的特权，如学校中的老师和学生，图书馆中的管理员和网络终端，企业中的工程师和销售人员，等等。

另外，策略管理可按时间来灵活设定网络使用规则，如工作时间限制 P2 下载用，下班后可取消限制。