

一 应用背景

现在，中小企业用户的网络安全意识正在逐步增强。有调查显示，近 90% 的被调查用户都在使用病毒防御方面的产品。防病毒软件的大量部署与计算机病毒的发展息息相关，一台具有安全漏洞的计算机在连入互联网之后十五分钟就可能受到感染。但是，应当注意到中小企业所面临的安全威胁远不只计算机病毒这一种。除了计算机病毒之外，垃圾邮件、企业网络资源滥用、网络非法入侵等等都是对中小企业信息基础架构造成破坏的隐患。

很多中小企业在构建网络安全系统时，并没有很好的规划，而是简单地采购了防火墙、防病毒和防入侵等网络安全产品就匆匆上马。这种安全手段被称作安全产品堆叠。堆叠法在当前的威胁面前会产生三个直接的弊端：资源浪费，功能重复；管理复杂，难以制定整体安全策略；难以协调，产生兼容性问题。

除了上述这三点直接弊端外，安全堆叠带来的安全效能低下引发的不为人发觉的威胁才是最大的隐患。所以，搭建网络安全系统绝对不能只是到市场上采购各种安全产品，然后简单地接入到网络中就万事大吉必须评估企业的整体网络安全需求，按需定制安全策略，对安全产品统一部署和管理。针对这种需求趋势，O2Micro 给出了自己的 UTM 解决方案——SifoWorks U 系列产品。

二 需求分析

- 1) 目前很多企业都部署了自己的邮件系统，员工之间的沟通以及业务的处理均通过电子邮件来实现，但随之而来的垃圾邮件泛滥亦对邮件系统的正常使用造成了严重的威胁，极大的影响了工作效率。
- 2) 计算机病毒对联网的企业用户来说是最大的安全威胁，中小企业需要由一个集中管理、可在线升级的防病毒引擎对网页和邮件中的病毒/蠕虫/恶意软件进行全面的防护。
- 3) IM/P2P 应用在企业用户中的应用越来越普遍，P2P 应用对带宽的占用不容忽视，需要对 IM/P2P 应用进行全面的管理和控制，减少带宽占用。
- 4) 一个 24 小时连通无故障的网络对企业的正常运营至关重要，网络安全设备需要提供完善的负载均衡以及高可用性，防止断网。
- 5) 针对网络中越来越多的攻击手段，需要对这些攻击做出实时的响应，保障网络的正常运行。
- 6) 企业网络接入开放的互联网，为防止企业机密信息被窃取，需要提供在开放网络中提供安全传输信息的机制。另外，还要针对企业出差用户或者分支机构提供安全远程访问公司内部网络的能力。

三 基于 UTM 技术的统一安全网关解决方案——SifoWorks-U series

(一) 丰富的功能特性

1 病毒扫描

SifoWorks-U 系列安全网关可针对多种协议如 HTTP、FTP、POP3、SMTP 等流量进行即时扫描，在网关确保企业网络不受潜藏于网页与邮件中的病毒、蠕虫及恶意软件的危害。U 系列产品可支持 Clam AV 与 Sophos 双病毒扫描引擎。

2 入侵检测防护

U 系列内建的入侵检测防护系统 (IDP) 可支持多达 2900 种以上的攻击特征。同时可自动在线免费更新特征资料库。以最经济的方式保护企业网络。用户亦可自定义攻击特征以应用多变的入侵威胁。

3 联合攻击防御

U 系列支持联合共和攻击防御，当系统发现异常流量时，可联合企业内部的路由器/交换机将特定攻击来源 IP 封锁，在第一时间避免大量攻击包在企业内部广播，造成网络缓慢甚至瘫痪。

4 QoS 带宽管理

U 系列可保障特定应用服务与服务器之间的网络带宽。包含最大使用带宽与保证带宽，同时可提供报文优先排序功能。针对个别 IP 来源的带宽使用上，系统亦支持下载问题限制以及 Session 数限制设定，让管理员有效掌握企业网络的资源利用。

5 双向多线路负载均衡

U 系列支持强大的流量负载均衡功能。对外可针对企业网页、邮件服务或特定服务器提供流量负载均衡；而企业的内部上网流量，系统亦可支持双路 ISP 线路并提供多种流量负载均衡模式。有效利用网络带宽并确保稳定、不断线。

6 垃圾邮件扫描

U 系统支持完整的垃圾邮件扫描功能。可使用透明模式或转发模式轻松整合现有的网络架构。贝叶斯算法/指纹辨识数据库与网络 RBL 数据库等多重邮件过滤机制，用户亦可以自定义过滤规则及黑白名单以应用不同过滤条件需求。此外，还提供自学习功能，可大幅增加垃圾邮件拦截的准确率。

7 流量内容过滤

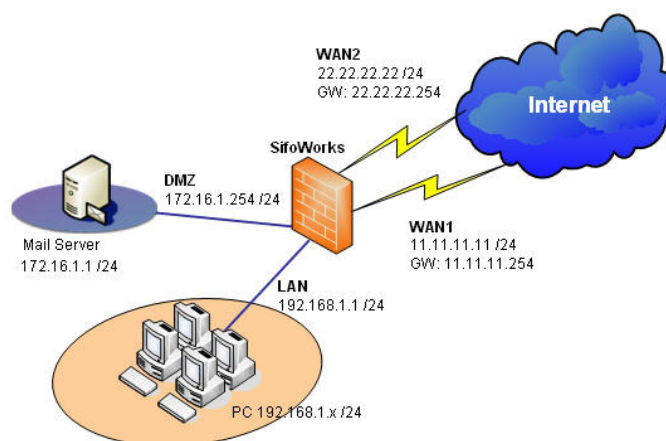
针对可能造成安全漏洞或占用网络带宽的即时通讯与点对点下载软件，U 系列辨识并限制多种知名软件，如：MSN、QQ、ICQ、Skype、BT 等等，让企业根据不同需求轻松管理此类软件。

8 完整的 VPN 功能

除了 IPSec VPN 之外，U 系列产品还特别提供了 SSL VPN 功能以应对移动办公需求。

(二) 应用案例

针对中小企业的多种不同安全需求，O2Micro 的 SifoWorks U 系列解决方案以其丰富的功能特性、良好的操作及管理界面、高性价比等优点将为成为中小企业的首选解决方案。其应用案例拓扑如下图所示：



在本案例中，一台 U 系列产品做为安全网关部署在企业网络与互联网的接口处，通过 WAN1 和 WAN2 双 ISP 线路提供流量的负载均衡及容错(failover)。同时集成的 IDP 及防病毒引擎可检测并阻止攻击行为与恶意软件，保障网络带宽使用。设定 Anti-Spam 相关参数，保障企业内部的邮件服务器。