第五章 中小企业安全路由器防火墙

防火墙的概念对于大企业的网管并不陌生，但是对于中小企业还是较陌生的。不过随着路由器性能持续升级，很多路由器都可以扮演防火墙的功能，为企业网络安全多一层把关。对于中小企业而言，由于信息的限制及信息化的程度不同，因此运用防火墙的方式和大企业有所不同。相对而言，中小企业希望能利用防火墙达到最基本的安全防护，又希望适度的对内部用户加以限制，也可达到广义信息安全的目的。

Qno 侠诺整合一般中小企业在防火墙方面常碰到的问题，及对应 Qno 侠诺安全路由器的功能，介绍中小企业可在路由器防火墙方面进行的配置如下：

项次	问题	功能
1	开放（公网）IP 地址服务器及主机，如何保护？	存取服务规则
2	私有 IP 地址及服务器，如何管制？对内的管制需要定时，如何配置？如何阻挡特定的应用服务？	存取服务规则、管制内容时间排程、阻挡特定服务
3	最近有许多常见的攻击，例如 ARP 攻击、DoS 攻击，如何进行防御的配置？	洪水攻击阀值机制、语音告警功能
4	如何减少攻击对路由器效能的影响？对于广播应用，如何开放路由器防火墙？	防火墙基本配置
5	除了路由器外，如何进行整体的配置，减少企业网络受到外挂程序的破坏？	防火墙基本配置

以下针对不同功能，予以介绍

5．1 防火墙访问规则

有些企业内部使用固定 IP 地址，例如 ISP 发放公网 IP 区域、DMZ 的服务器、开放一对一 NAT 的服务器等，由于需要对互联网上用户开放服务，必须使用固定 IP。公开虽然有好处，但相对的也容易成为恶意人士攻击的目标，因此若是企业网络有这样配置的服务器或

是计算机，就必须先加以保护。

要保护公网 IP 服务器或是计算机，第一个要作的就是除了保留要提供服务的 TCP/UDP 端口，之外的网络端口全部封掉，以避免服务器受到攻击。例如提供网页服务器，只要保留 80 端口的服务让外界存取即可，其它的都加以封闭。另外，如果能限定开放服务只是特定的用户，例如其它分公司的用户，也可以只允许特定用户进入，再次降低受到攻击的可能性。

在 Qno 侠诺路由器上，这个功能可使用路由器中网络存取规则条例工具进行配置，存取规则可以依据不同的条件来过滤，例如可以设定封包要管制的进出方向是从内部到外部，还是从外部到内部，或是设定以使用者的 IP 位置、目地端 IP 位置、IP 通讯协议型态等条件来做管制，管理者可以依照实际的需求调性设置。

侠诺路由器产品中有默认的网络存取规则条例，网管可以选择关闭(deny)或是允许(allow)来调整使用者对互联网的存取。管理者可以自定存取规则并且超越路由器的默认存取条件规则。在做规则确认时是依照由前到后 1-2-3…。依序做规则判断，所以前后顺序是让您在做访问规则的设定规划中必须要考虑的，以避免您想开启或关闭的功能失效。

图一：访问规则设置，是最基本阻挡不必要存取的基本工具。对于使用公网 IP 的服务器，更是必须设置的基本项目。减少存取不但可以降低路由器的工作负担，更可增加内网的安全性。

对于采用 NAT 产生私网 IP，或称虚拟 IP 地址的计算机或内部服务器，则主要需进行内网用户的配置。主要的目的在于管控内网用户上网的行为，以避免员工上网降低生产力，或是带进不必要的病毒或攻击，这对很多网管来说是必要的。配置群组的功能，可以为不同部门的人员配置不同的存取权限。例如业务部允许上网及使用 Skype、MSN 及邮件与客户连

络，而行政部门人员只能以邮件与外部连络等。这个管制动作，对于很多企业也是可以节省很多损失的一种配置。

5．2 时间管制设定

对于内网的管制，可以加强企业网络的安全性，但是对员工而言就显得较为不方便。因此有些网管需要对防火墙设定增加一些弹性，例如下班时间，允许较大的权限可以上网，例如全部员工，在下班时间都可以观看网页，这时即可使用时间管制设定功能。

侠诺路由器产品支持的时间管制是随着每条存取服务规则一起的，网管必须在配置规则时就一并把作业时间设好。值得注意的是，这个规则是 24 小时制的，因此若需要跨过午夜零点，最好设定上半夜及下半夜两条规则，以免发生冲突或是不如预期的情况。

图二：时间管制设定是依附在每一条存取服务规则下的，针对每个规则都可以规定生效的时间。适当地组合时间管制，可为内部上网管理增加弹性。

5．3 阻挡特定服务

如果觉得一一设置阻挡很不方便，侠诺路由器提供一键挡特定的服务功能，可以通过设置将 MSN、Skype、QQ、BT 下载这些服务挡住，以方便用户的管理设置，以最简单的方法起到管制的作用。阻挡特定服务是以勾选的方法,决定限制哪些服务,另外还提供有排除功能,可以排除特定 IP 用户,例如公司老板或是高管等。

图三：本图可以看出内部网络 192.168.1.2~100 的 IP 将不提供 MSN 及时信息服务功能，中小企业可以按照需要对内网 IP 的这几个特定服务做挡定设置。

5．4 洪水攻击阀值机制及语音告警

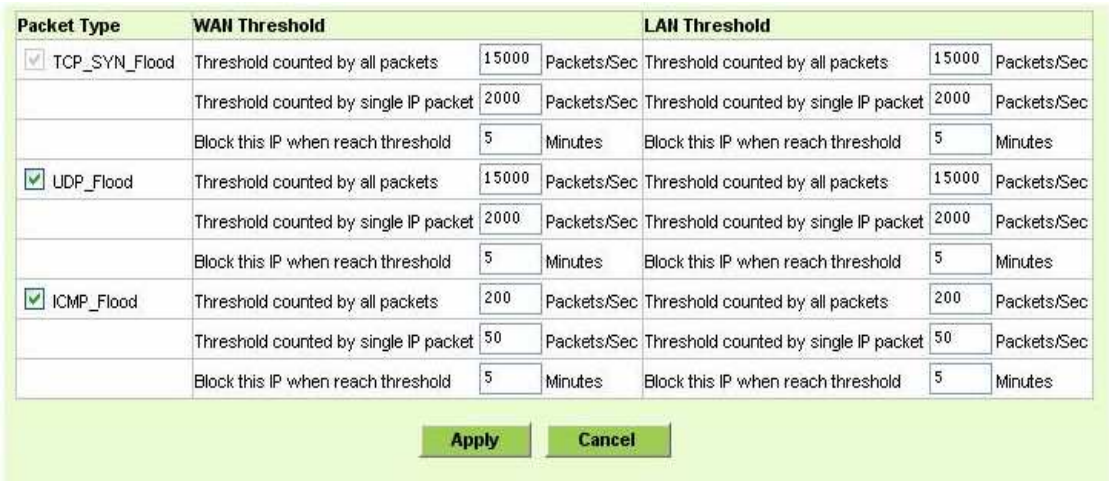
SYN Flood 及新版的 ARP 攻击是近来企业最常面临的洪水攻击。SYN Flood 是 DoS（拒绝服务攻击）与 DDoS（分布式拒绝服务攻击）方式之一，其攻击方式是利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽，CPU 满负荷或内存不足。ARP 攻击则是基于 ARP 协议特性，攻击方向受攻击计算机不断发送欺诈性质的 ARP 数据包，数据包内包含有与当前设备重复的 Mac 地址，使对方在响应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。

Qno 侠诺引入路由器产品的一些功能，能让用户有更多弹性因应这些新形态的攻击作相对的配置。以下针对不同的攻击说明这些新导入的功能。

• **洪水攻击防御的加强：**洪水攻击属于 DOS 攻击的一种，它利用网络协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。受攻的击路由器将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求，或最后产生 TCP/IP 堆栈溢出崩溃死机。

针对这种攻击，Qno 侠诺路由器软件中的防火墙功能加上洪水攻击的阀值机制，用户可针对网络广域网及局域网每秒网络包或是单一 IP 每秒发出网络包，设定阀值，如果超过特定阀值，则阻挡该 IP 或是整个网络的上网需求。在这个设定中，具有关键地位的是针对单

一 IP 设定的阀值，根据侠诺的技术支持经验发现，设定在每秒 2000 个包，应可有效抵抗攻击。值得注意的是，当设定阀值太低时，对于 QQ 视频或是相似的应用，会产生影响，因此也不能设定太低。



图四：要对抗洪水攻击，必须针对大量发出网络包的 IP 地址加以管制，除了 TCP 协议外，现在 UDP 及 ICMP 网络协议的攻击也很普遍。

另外，以往的攻击往往利用 TCP 协议进行，最近发现 UDP 及 ICMP 的攻击形式也渐渐增加，因此在产品中加进了这个功能。

• **MAC/IP 欺骗型 ARP 攻击防御的加强：**ARP 攻击利用广播封包，影响网络的运作。侠诺之前推广了双向绑定的因应之道，即在客户端及路由器端都必须进行 ARP 协议的绑定，可预防受到干扰。但是新版 ARP 变型攻击软件采取自动变换 IP 及 MAC 的方式，不断发出网络包给路由器，让路由器忙于处理无用的数据包，而影响正常的运作。

在侠诺新版的软件中，加入了自动判别的功能，可以不理会非正常 MAC 或 IP 所发出的数据包，也不加以转发，可减少攻击所产生的影响。用户可在配置路由器时，进行学习功能，并确认正当的 IP 及 MAC，之后路由器即可拒絶其它的网络包，以降低 ARP 攻击的影响。一旦本机制作用，受到影响的只会是发动攻击的计算机，因为忙于攻击而运作缓慢，但是其它用户不会受到影响。

• **语音告警功能：**新版 Qno 侠诺路由器内建发音功能，配合以上的功能，在第一时间可以针对新型态攻击阻挡，同时会以语音发出遭受攻击的讯息。此时网管可实时知道会受到攻击的情况，并可通过日志功能找出有问题的来源，加以隔离，并有效控制受害。侠诺强调同时在抵挡攻击及实时通知两方面都要作好，才能真正协助用户改善网络安全问题。

5．5 基本设置

对于企业网管来说，必须要根据不同的需求进行路由器的配置，但事实上，路由器做的事越多，效能就受到越大的影响。例如广播应用的网络包，如果允许进入内容，则对路由器效能及内网安全都造成威胁，因此 Qno 侠诺路由器的基本配置功能可让网管选择是否开启一些常见的服务，取得路由器效能及安全之间的平衡。

在基本设定功能中，有以下设定：防火墙功能及 SPI 封包侦测是进行细部带宽管理及存取规则需要的，关闭这二个功能将使部份功能无法运作，但可得到最好的效能，适用于另外配接防火墙的企业；DoS 侦测功能，会记录是否受到不正常网络包的攻击，特定情况下需用到；关闭对外的封包响应，可避免外部占用路由器资源的攻击，进一步增加效能及安全性；允许 Multicast 封包"功能"则是针对对应播应用；允许广播封包通透；最后防止 ARP 攻击必须配合客户端计算机绑定，有效对付 ARP 攻击。

图五：Qno 侠诺路由器的基本配置功能可让网管选择是否开启一些常见的服务，取得路由器效能及安全之间的平衡。

5．6 防火墙相关整体配置

除了路由器的配置以外，侠诺技术服务部门也总结了全国许多资源网管的经验，另外提供二个值得参考的改善点：

• **减少用户使用外挂软件机会：**很多环境发生攻击的事件，往往是因为用户用了外挂软件，因此如能减少用户使用外挂软件，就能减少攻击。在国内一些较先进的网吧，已经提供完整的外挂软件，不让用户自己从网络下载软件，这样可以减少攻击情况的发生。这点对于一些网吧而言，可能不太习惯，但是不失为一个有效管制方法。

• **配合三层交换管制网络：**国内许多中大型网吧采用三层交换机作为骨干交换机，由于三层交换机也具备许多管制功能，因此如能善用三层交换机之功能，也可较好的针对攻击加以抵抗。有些网管在使用时，只是把三层交换机当成一般的交换机使用，有些可惜！

小结

对于大企业而言，防火墙扮演了企业网络安全重要角色，而安全路由器对于中小企业而言，可以较经济的花费，达到需要的管制功能，不失为一个方便的解决方案。Qno 侠诺不断地为中小企业引入原本贵不及的功能，也希望为中小企业网络安全，发挥进步改善的作用。