

## 第一章 中小企业安全路由器基本配置

网络安全对于中小企业网管来说，已是必修的一门课。本系列文章集结 Qno 侠诺在中国各地支持企业用户的心得，提供给读者参考。本篇文章先从基本配置谈起，也就是路由器的广域网及局域网如何进行配置，旨在让中小企业用户在进行规划时，就能善用路由器的各种功能，提供给内部用户更好的网络服务，提升企业的经营效益。

下表列出一般中小企业在进行安全路由器的基本配置时，常会面临的问题：

项目	问题	解决功能
1	何时适用 WAN 接入？多 WAN 接入可解决哪些问题？有哪些不同负载均衡模式可用？	多 WAN 设定、策略路由、负载均衡
2	局域网 IP 如何配置？何时使用固定 IP？何时使用 DHCP 分发 IP？	DHCP 服务器
3	如何防止未经充许计算机上网？如何防止无线网络被外人使用？	IP/MAC 绑定
4	如何把用户依部门分群组管理？如何简化对用户的管理工作？	群组管理
5	如何建立公开服务器？不同配置方式优缺点如何？如何能有较高的公开服务器安全？	DMZ 硬件接口、One-to-one NAT、Qno 动态域名服务、内部 DMZ

综合 Qno 侠诺技术服务部的实际支持经验，一般中小企业在进行安全路由器的基本配置时，需要特别注意的有广域网端、局域网端及公共服务器三个方面。以下分别就这三个方面加以介绍。

### 1. 1 广域网端

广域网端就是路由器对外接往网络运营商的线路。广域网线路也是宽带接入的主要路径，因此若是发生掉线或是拥塞，则企业的宽带接入就会中断！这个状况对于有些企业会产



生很大的困扰。因此广域网端在安全上的首要思维，就是如何确保线路的稳定，维持企业在各种情况下的运作。

大部份的中小企业，由于上网人数较少、或是经费有限，因此大多采用单线 ADSL 即可。如服务业或是外贸行业等企业带宽的需要较大，或是对于网络要求较高的，则可能采用相对费用较高的光纤。根据 Qno 侠诺支持用户的经验，当发生以下情况时，较倾向采用多 WAN 线路的配置：

### • 需要大量上 / 下载时：

由于信息化的结果，很多企业需要不时进行大量的上下下载的操作。例如成都的某矿产商贸公司每天下班时，需要上传销售报告及存货数据，需要较多的时间。又例如位于宁波的某民营企业，时时需要从国外客户的服务器，下载设计图面作为生产之用。当要进行下载时，网管一般都不希望受到一般用户上网或下载影响，因此可申请二条线路：一般情况下二条线路都开放作为用户上网用；但是当需要进行特别工作时，则可加以管制，保留特定的线路给大量上下下载的工作，以确保重要的数据能准时传送。采用多 WAN 配置后，网管加班在办公室等待数据传送的情况，就可大大减少了！

### • 有跨网问题时：

笔者有次到山东济南时，有位用户说他们的企业是一个农产品的商贸公司，常常需要和在北京的总部建立 VPN 联机，但是不知道为什么，总是联机很不稳定，常常数据还没传完，又得重新联机。这种情况，很可能就是 VPN 建立跨过不同的运营商网络所产生的不稳定问题，例如总部采用网通的线路，而分支采用电信的线路，跨网带宽不足，而产生的现象。这种情况，也可采用多 WAN 路由器解决，即总部同时接入网通及电信的线路，属于网通线路的外点从网通的入口建立 VPN，电信的外点则从电信线路建 VPN，这样即可解决跨网带宽小或不稳定的情况。

### • 需要备援时：

多 WAN 线路的另一个优点是提供备援功能。一个常见的情况是有些地区运营商会给光纤用户赠送 ADSL 线路，这时就可以 ADSL 配合光纤作备援，在前者发生故障时，以 ADSL 先顶着用。有的用户则希望用不同运营商的线路，这样在 A 运营商线路或机房发生问题时，可以 B 运营商线路替代。对于某些行业，例如媒体行业，需要随时可以上网，这个功能就十分地需要。

### • AD 带宽不足时：

一般企业用 ADSL 来的多，根据统计显示中小企业宽带用户增加最多的就是采用 ADSL 上网。但有些地区提供的 ADSL 相对带宽显得较小，例如 64K/64K 的线路，对于企业应用

显然不足，不过申请光纤又比几条 ADSL 还来得贵，在这种情况下，利用多 WAN 路由器汇聚多条 ADSL 线路，不失为一可行又省钱的方法。

多条广域网联机，一般都必须进行负载均衡的配置，以有效使用不同广域网联机的带宽。一般最大的分类为联机数均衡及 IP 均衡：联机数均衡能将带宽平均作到最佳化，也就是能作到有效合并多条线路带宽的效果，但是联机数均衡对于某些认定双方 IP 的应用，例如 QQ Live，会产生联机不稳定情况。IP 均衡则用于用户人数较多，应用的软件类别较多时，由于不同的用户会走不同的广口，也可起到有效平均带宽的效果。指定路由适用在设定特别应用到特定广域网端口，例如 VoIP 或是邮件传送等。策略路由功能是针对不同运营商，例如电信网通线路分流而进行，用户可自行进入配置或使用内建策略。

由于广域网端为企业上网唯一的路线，因此对于企业上网有决定性的的重要性。Qno 侠诺的市场调查显示，现阶段很多企业对于无线宽带接入，例如 3G 或是 WiMax 都表示了相当的兴趣，希望能用无线接入作为有线接入的辅助，这或多或少也代表了企业对于广域网端接入的重视及期望。

## 1. 2 局域网端

局域网端则是对内接到企业用户的线路，有些路由器本身有局域网端口，可下接交换机；有的网管则会将路由器先接到骨干交换机，再向下接到一般的交换机。以上这两种作法均可，后者适合较大吞吐量的应用情况，一般的企业应用，路由器的局域端口是可以因带宽转发的。在硬件配置，这是较为简单的。

侠诺的技术服务人员的经验指出，要进行一个好的安全网络的配置，IP 的管理是很重要的。IP 就是计算机在互联网的地址，因此要能有效管理地址，才能预防攻击或针对有问题的计算机加以管制。对于网管而言，在 IP 管理方面要注意的事项，主要为计算机采用固定 IP 地址、DHCP 服务器发放固定 IP 地址、防止未允许的计算机上网及群组管理等四个重要项目，以下分别为之说明：

### • 计算机采用固定 IP 地址：

计算机采用固定 IP 地址，是最严密的配置方式。这个作法，必须要求用户在计算机中，手动键入 IP 地址相关数据。这样作的好处是每台机器的 IP 都必须是事先指定，没有事先指定的 IP，则无法上网，外来的用户或是计算机不能轻易地通过企业网络上网。不过对于用户而言，必须要设定固定 IP，到其它场合，又必须重新设定，对于部份常需要移动的用户，例如业务人员或是高阶主管，造成不小的困扰。

### • DHCP 服务器发放固定 IP 地址：

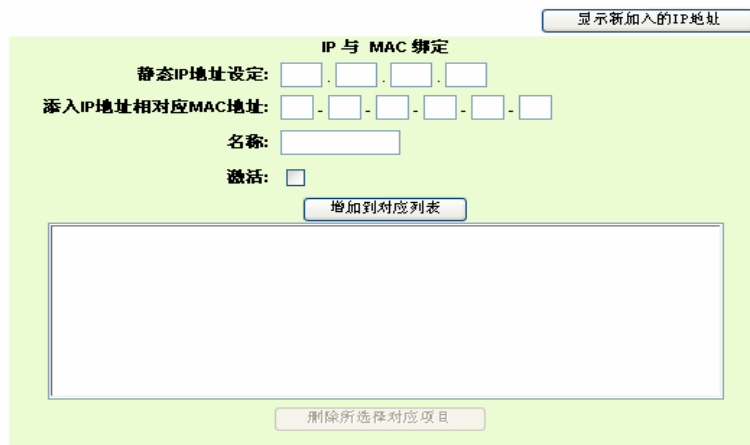
DHCP 服务器的好处是用户无需在计算机上作任何设置，对于用户较方便。但是 DHCP

的缺点是若不加以管制，随便一个用户也能进入企业的网络，也容易发动对内部的攻击，造成影响。因此对于企业而言，较好的方式是通过 DHCP 发放 IP 地址，但同时限定计算机能取得的 IP 地址，以便进行管理。Qno 侠诺路由器产品的 IP/MAC 绑定功能，即可以经由网管的配置，认明计算机的 MAC 地址发放特定的 IP，这样就可针对 IP 进行管理。同时 IP/MAC 绑定功能也可防止用户修改 IP，以取得较高权限问题，错误的 MAC/IP 组合，将会被路由器 " 封锁错误 MAC 地址 " 阻挡，这个功能也可防止 ARP 攻击。

## • 防止未允许的计算机上网：

对于网管而言，未被管制的计算机，往往会引发安全的问题。有些用户会自行带入中毒的计算机，甚至其它用户通过无线网络进入公司网络。这样的情况，可通过防止未允许的计算机上网来解决。Qno 侠诺的 IP/MAC 绑定功能中，提供有 " 封锁不在对应列表中的 MAC 地址 " 的功能，达到网管未配置的 MAC 地址，完全无法上网的作用。

### IP 与 MAC 绑定



- 封锁在对应列表中IP地址错误的MAC地址
- 封锁不在对应列表中的MAC地址

图一： Qno 侠诺路由器的 IP/MAC 绑定功能，网管可将用户的 IP 及 MAC 地址键入，这样可以达到使用 DHCP 服务时，每次发放固定 IP 给用户。另外提供的 " 封锁错误 MAC 地址 " 及 " 封锁不在对应列表中的 MAC 地址 " 则可提供更进阶的功能，提供进一层的安全保障。

## • 群组管理：

除了 IP/MAC 绑定，可有效管制用户外，适当采用群组的功能，也能更方便的对用户加以管理。例如 Qno 侠诺提供的 IP 群组功能，就能将不同的 IP 用户设为不同群组，例如企业高阶主管设为一组、业务部门设为一组、内部行政人员设为一组。不同群组的用户，适用不同的管制权限或是带宽管理原则，这样可以大幅简化管理工作，也可避免管制时出现漏网之鱼的现象。

IP GROUP

群组：

---

群组名称：

IP 地址： .  .  .  ~

图二：IP 群组功能，可将不同 IP 用户分类为不同群组，并加以命名，经由群组的管理，以达到全面性的管制功能。也可避免因配置的漏失，而产生安全的漏洞。

### 1. 3 内部建置公开服务器

以往可能较大的企业才会设置公开的服务器，让外部的用户存取。但是信息化的普及让中小企业也可能要架设不同的公开服务器给外部的用户。例如像图文件交换、技术更新信息、报告缴交等都可经由架设公开服务器的方式达成。

企业要提供公开的服务，必须提供一个固定的 IP 地址让互联网用户键入在服务器地址栏。一般的方式是使用 IP 地址或是域名来作为辨别，但是这两种方法对于中小企业都较为昂贵，每个月的费用较高。还好 DDNS 的出现，可允许企业用动态 IP，即使使用 ADSL 取得动态 IP，也可让用户以记忆域名的方式来存取服务器。Qno 侠诺也将提供动态域名 DDNS 的服务给企业用户，现正进行最后阶段的测试工作，将于近日内开放给侠诺的用户，请读者拭目以待。

以下针对不同的需要，说明内部建置公开服务器的配置，主要分为有固定公网 IP、提供一个公开服务器、及提供多个公开服务器等情况说明：

- **有一个或多个固定公网 IP，想要较高等级的安全性：**

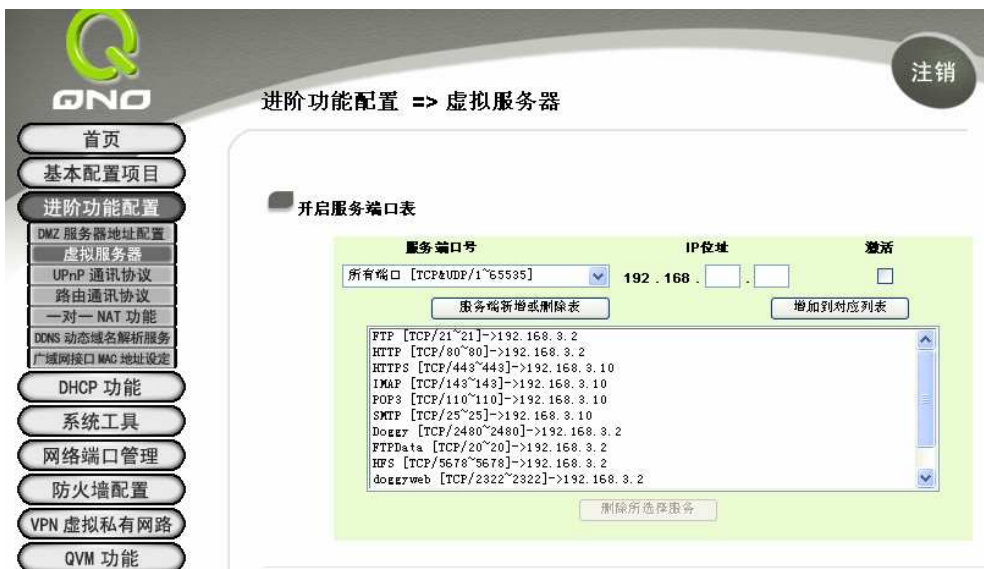
若有多个固定 IP，又想将服务器隔离到外网，得到最高的安全性，则可通过 Qno 侠诺路由器的硬件 DMZ 端口，连接到一个或多个服务器，这样完全隔离，外部用户网络封包完全不会进入内网，可得到最高的安全性。这种应用是最安全的，但是笔者发现对于网管来说也最不熟悉的。

- **有一个或多个固定公网 IP，允许以内部服务器向外公开：**

有些应用希望服务器能很方便地被内网及外网的用户存取,而又有固定公网 IP 可用时,则可采用 One to one NAT 的功能,将内网服务器与公网 IP 产生对应关系,这样这个服务器对于外网用户,就像公网服务器,而对内网用户,则像内网服务器一般。这种配置相当方便,故十分普及,但由于没有适当的隔离,因此需要作一些带宽或是限制的防火墙设定,以增加安全性。

- 使用 DDNS 提供多个公开服务器,需要较高安全性:

企业若采用 ADSL 上网,则往往没有固定 IP 使用,必须申请动态域名服务。Qno 侠诺用户可向侠诺进行申请相关服务。虚拟服务器一次开放限定网络端口,因此对于不正常的端口要求,可以不予理会,相对安全性也较高。这适合特定的服务器端口使用。采用虚拟服务器功能技术上,可以开放内部多个服务器。



图三: 虚拟服务器是以网络服务端口对应的方式,开放到内部的服务器上,由于只开放有限的端口,因此可得到较高的安全性。

- 使用 DDNS 配合动态 IP 提供一个不特定端口公开服务器,安全性要求低:

有些应用并没有特定端口,服务器会依应用的需要自行和客户端软件决定沟通端口,这时就不能用虚拟服务器。典型的例子是视频监控,或远程数码摄像头,大多采用特殊的端口,这时只能把所有端口服务的要求,通过“内部 DMZ 服务器”功能,转到该服务器去。这个功能是软件 DMZ,不用连接到实体的 DMZ 口,而是指向一部内部服务器。但由于所有端口开放,安全性也较低,建议要设置对应的防火墙管制规则才好。这个功能一个 WAN 口只能提供一个服务器使用。

## 进阶功能配置 => DMZ服务器地址配置

内部DMZ服务器IP地址： 192 . 168 .  .

图四：DMZ 服务器适合网络摄像头等，不确定端口的应用，但相对安全必须作对应的防火墙配置。

以上针对广域网、局域网、及开放服务器三方面，就中小企业安全路由器的功能常遇到的一些问题，做了初步的介绍。相信对于企业网管，有相当的帮助。我们下一章节，来谈谈中小企业安全路由器“配置及管理”相关的功能。