计算机科学2001Vol.28№.7

网络地址翻译系统的原理和应用

Principle and Application of Network Address Translation Systems

包 亮 潘金贵

(软件新技术国家重点实验室 南京大学多媒体计算机研究所 南京210093)

Abstract Since Network Address Translation(NAT)systems, which will translate address between two address realms, were first introduced to solve the address shortage problem, they have been adopted in many domains. In this paper, basic principles, primary forms and application will be discussed. And some countermeasure on the co-exist with IPSec will be given.

Keywords NAT, NTA system, IP security system

1 引言

自1983年TCP/IP协议族成为Internet基础协议之后,获得了迅速的发展。由于该协议族的开放、简单、高效的缘故,这一套包括TCP、UDP、ICMP、ARP、IP等诸多协议的协议族也成为事实上的标准。IP协议属于网络层的协议,负责寻径、流量控制、处理拥塞等。IP地址是IP协议最基础的要素,它唯一地标识连接到Internet上的每一台主机。根据协议的最初设计,如果不精确地计算,一共可以提供4,294,967,296个IP地址,但是IP地址分配方案,其地址空间被大量地浪费,随着Internet的迅速发展,当前IP地址已经接近枯竭。另一方面,IP协议也为那些需要使用IP协议但是又不需要直接连接Internet的组织/企业保留一些私有IP地址(private IP address)[RFC1918],并限制在Intranet内部使用,当这些公司把自己的内部网和Internet相连时,通常,他们只获得有限的经权威机构分配的公开IP地址(public IP address),为了解决使用有限的公开IP地址将整个Intranet接入Internet,1994年,Internet Society下属的Network Working Group就提出了Nework Address Translation(NAT)的解决方案[RFC1631],使用一个私有的A类地址为Intranet内部机器分配地址,在网关处进行地址翻译使内部网机器都可以透明接入Internet。该方案几经改进、形成了目前流行的完善版本[RFC2663],而目前的NAT系统已经不仅仅用于解决地址短缺问题,还在很多其他方面获得了广泛的应用。本文试图从基本结构、处理流程、常用分类等角度对NAT进行分析,并指出在应用中出现的问题和对策。

在本文中,Internet、外部网络均指公司/组织以外的网络,Intranet、内部网络均指公司/组织内部的网络,出站流量(outbound traffic)指从内部网络经过NAT router流向外部网络的TCP/IP报文,入站流量(inbound traffic)指从外部网络经过NAT router流向内部网络的TCP/IP报文。

2 NAT的基本结构

一个典型的NAT系统如图1所示,图中,内部网络所有主机使用局域网(LAN)相连,可以采用任意支持IP协议的技术。具有NAT功能的路由器(以下简称NAT router)有至少两个以上的网络接口,其中一个接口连接公共的Internet,具有公开IP地址,比如202.119.37.8,所有的外出的TCP/IP流量经过这个接口流向Internet;另一个接口连接内部网络,使用任意的(一般是私有的)IP地址,例如192.168.5.2,所有内部网络的外出流量被首先定位到这个网络接口。内部网络IP地址分配方案可以采用DHCP协议动态分配私有地址,也可以在每台客户机静态设置地址,但是,对于每台需要访问外部网络的机器都要将网关设置为NAT router的内部网络接口地址192.168.5.2。

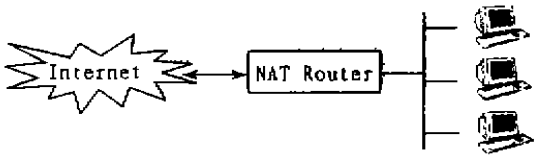


图1 一个典型的NAT系统

包 亮 硕士研究生,主要研究领域为多媒体计算机和网络通信。潘金贵 教授,主要研究领域为中间件、Agent技术、多媒体远程教育、多媒体移动教学。

3 NAT 的工作原理

假设内部网络的一台主机需要访问外部网络上一台主机上的 WWW 服务，比如202.119.32.6，该主机将产生一个 IP 包，其源地址为私有地址如192.168.5.120，目的地址为202.119 32.6(见图2步骤①)。该 IP 包因为目的地址为外部网络，所以被发送到网关，这里就是 NAT router 的内部接口192.168.5.2。具有私有地址的 IP 包在到达 NAT rourer 的时候源地址字段都被修改成公开 IP 地址，例如202.119.37.8，目的地址维持不变，在记录了这次地址翻译(这样的翻译条目被称为一个 entry)后转发出去(步骤②)。当 Internet 上服务器202.119.32.6收到请求响应返回 IP 包的时候，因为从该 WWW 的角度看该 IP 包是从202.119.37.8 发送过来的，所以源地址是202.119.32.6，目的地址是202.119.37.8(步骤③)。该 IP 包的目的地址为 NAT router 的外部接口地址，所以将被 NAT router 接收到，根据从 NAT router 所维护的活动翻译条目表中查询到的信息，该 IP 包是主机192.168.5.120发送的请求的回应，源地址维持不变，目的地址被修改成为192.168.5.120，然后发送给内部网络等待响应的主机(步骤④)。整个过程如图2所示。

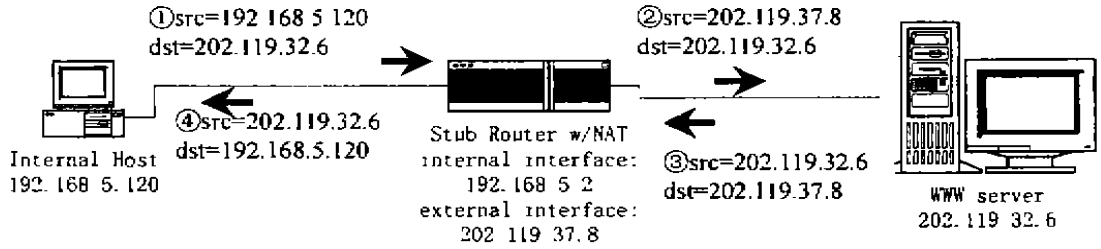


图2 NAT router 进行地址翻译的例子

上面给出的是一个典型的 NAT 系统工作的实例，目的是说明 NAT 系统的基本工作原理，但是上例中并没有给出包括如何决定出站报文使用的 IP 地址，如何维护翻译条目状态表，如何处理包含地址信息的特殊协议等一些具体的细节。按照 RFC2663，所有的 NAT 系统应该具有以下特征：透明的地址分配方案；透明的路由寻址方案；转换 ICMP 报文的负荷字段。

3.1 透明地址分配

对于出站流量需要修改内部私有 IP 地址为外部公开 IP 地址，这个操作被称为 IP 的绑定。绑定的 IP 地址通常有两种做法，即静态地址分配和动态地址分配。前者由 NAT 上的静态地址映射表决定内部主机出站 IP 包使用哪一个公开 IP 地址，这种方式的最大优点就是不需要 NAT 对映射表按照会话流进行维护。另一种动态绑定指，外出 IP 包的地址被翻译成什么样的 IP，取决于服务的需要和当前资源空闲情况。这样一来，NAT 系统必须维护当前活动的所有 session 的地址翻译对照表。在 session 活动期间，NAT 根据该表对进/出站的 IP 包的地址进行翻译；而在 session 结束之后，被占用的外部公开 IP 地址被回收以供其他连接使用。

3.2 透明路由寻址

NAT router 本身作为一种路由器，除具有寻径、中继和转发功能外，所有外出的 IP 包要经过它的处理才能转发出去，而所有进入的 IP 包也需要经过它的翻译才能送给真正产生请求的内部主机。这个翻译过程在 NAT router 中已经成为路由过程的一个必要步骤，因为只有具有有效的外部公开 IP 地址的包才可以在外部网络上传输，同样地，也只有具有有效的内部私有 IP 地址的包才可以成功传送到指定内部主机。这种特征对于用户来说是透明的，用户并不会意识到有这样一个翻译过程的存在。

3.3 转换 ICMP 报文的负荷字段

ICMP 被信宿机或者网关用来向信源机报告数据包传输中的差错和控制信息[RFC792]，在这些报文中通常包含信源机和/或信宿机的 IP 地址，这些地址需要进行适当的转换才能由 NAT 系统发送给最终目的接受者。

4 NAT 系统的常见形式

由于存在多种应用环境，为适应应用的需要，NAT 系统也演化出多种形式。如果对它们进行一个简单的分类，将包括出站 NAT，双向 NAT 和双重 NAT 三种形式。以下将进行简单介绍。

4.1 出站 NAT

这种 NAT 的应用环境主要针对一个企业或者组织拥有少量 IP 地址，但是希望将内部网络所有机器接入 Internet 的时候，因为在某一个固定时刻需要接入 Internet 的主机数目通常是小于该企业/组织拥有的所有主机的数目的，这使得出站 NAT 的应用变为可能。出站 NAT 允许内部网络直接发起和外部主机的连接请求，在 IP 包到达它的时候将其中的地址翻译成

全球唯一的公开外部地址。在这种系统中，外部主机的地址是唯一的和全球有效的，而内部网络地址则只在内部网络是唯一的，在外部网络可能是无效的。也正因为这个原因，这种 NAT 系统只能够允许内部主机发起和外部网络的通讯，而外部主机无法发起和内部主机的通讯。这是 NAT 系统草案中最基本的形式，故又被称为传统 NAT(traditional NAT)。在长期的发展过程中，传统的出站 NAT 形成了两种变形，一种是基本的基于地址的 NAT(以下称为 basic NAT)，另一种是基于地址和端口的 NAT，称为 NAPT[RFC2663]。

4.1.1 基本 NAT 系统(basic NAT) 只对 IP 包中的地址字段部分进行翻译，在这种情况下，如果内部网络同时有多个 IP 包要通过网关，那么在只能翻译 IP 地址字段的限制条件下，NAT 系统必须拥有一个在外部网络有效的地址池(globally unique address pool)，不同内部主机的 IP 包将获得从地址池按一定算法选择的 IP 地址，在3.1节提到，这种分配算法可以是静态的，也可以是动态的。当内部主机数量和外部地址池中地址数量相等的时候，选择静态映射可以获得较高的效率。

4.1.2 地址/端口翻译(NAPT) 实际上是对 basic NAT 的一种扩展，它不仅对 IP 包的源/目的地址字段进行翻译，还要翻译 IP 包的源端口，因为被翻译的字段的增加，可以使用的外部地址空间大大增加。假设原来两台内部主机 192.168.5.201 和 192.168.5.202都使用各自本机的1234号端口请求一台外部网络上的 Web 服务器(202.119.32.12)的页面，在基本的 NAT 的处理中，因为不改变源端口号，只能是将两个 IP 包中的源地址分别翻译成两个不同的外部公开的 IP，例如 202.119.36.193 和 202.119.36.194。但是在 NAPT 中，这两个 IP 包的翻译结果可以有相同的源地址，只需要修改成具有不同的源端口号。表1是两种翻译方案的对比。

表1 Basic NAT 和 NAPT 对于 IP 包翻译结果的对比

原 IP 包	Basic NAT	NAPT
(192.168.5.201, 1234,202.119.32.12,80)	(202.119.36.193, 1234, 202.119.32.12,80)	(202.119.36.193, 60001, 202.119.32.12,80)
(192.168.5.202, 1234,202.119.32.12,80)	(202.119.36.194, 1234, 202.119.32.12,80)	(202.119.36.193, 60002, 202.119.32.12,80)

由于端口也被纳入翻译范围，NAT 可以使用少量(最少可以是只有一个)IP 地址同时处理多个出站请求。这种特性使 NAPT 非常适合拥有不多 IP 地址的小型组织将整个内部网络接入 Internet。

4.2 双向 NAT 系统(bi-directional NAT)

双向 NAT 系统与 basic NAT 系统的区别在于这样的 NAT 系统不仅允许内部主机发起与外部网络的连接，而且也允许外部网络的主机发起与内部主机的连接。这种情况下外部主机发起的连接请求被 NAT 接收到之后，目的地址被翻译成内部网络上有效的 IP 地址，发送给指定的内部网络主机。外部主机既不知道内部主机的地址，即使知道这样的地址也是不能在 Internet 上路由的，所以通常需要使用 DNS-ALG [RFC2694]进行内外部网络主机名字空间到 IP 地址的转换。DNS-ALG 是应用层的 DNS 网关，负责对外部网络提供内部主机名字到全局公开 IP 的映射，例如内部一台提供 www 服务的主机使用域名 www.companyb.com，在内部网络上它使用 RFC1918 中规定的保留地址，但是外部主机使用该 DNS 查询到的 IP 却是在 Internet 上有效的 IP，然后外部主机就可以使用这样的合法 IP 发起连接，连接被定向到 NAT router，在进行了网络地址的翻译操作之后内外部主机就可以建立起一个连接。除了需要使用一个特定的 DNS 对外提供内部主机名字的解析外，其原理和 basic NAT 完全一样。

4.3 双重 NAT 系统(twice NAT)

双重 NAT 系统翻译的字段范围除了源地址和端口外，还包括目的地址和端口。这种应用一般发生在内部网络和外部网络发生地址冲突的情况下，考虑一家公司 A 曾经是 ISPA 的客户，使用 ISPA 分配的地址 202.5.3.0，但是后来更换了服务商，在 ISPA 和该客户的合同结束之后，ISPA 又把地址分配给了公司 B。如果公司 A 不打算调整其内部网络的 IP 地址，那么公司 A 和公司 B 之间的通讯将发生问题，任意一家公司的网络上的主机如果试图和另外一家公司的主机发起连接，它的 IP 包都会被本地路由器认为是本地地址而在本地网络广播。在这种情况下，双向 NAT 显得特别有必要，双向的翻译操作解决了地址冲突问题。但是，这种应用必须配合应用层 DNS 网关(DNS-ALG)一起使用。

仍以上面的例子说明，假设公司 A 网络的一台主机 hostA(202.5.3.1)试图连接公司 B 的 Web 服务器 www.companyb.com，这台服务器在 Internet 上全球唯一的 IP 地址是202.5.3.6，但是 host A 不能直接使用这个地址进行连接。因为目的地址属于202.5.3.0子网的话将不被路由。所以，host A 应该是首先查询 DNS-ALG，该 DNS 返回一个伪地址，比如说 192.168.3.6，然后 host A 根据查询到的这个地址发起连接，双向 NAT 接受到这样的 IP 包之后，把源地址202.5.3.1修改成公司 A 新的 Internet 地址，比如

203.10.3.1，而目的地址192.168.3.6修改成202.5.3.6，这样一来，公司B的Web服务器接受到的IP的请求好象是来自新的地址203.10.3.1，虽然实际上请求连接的主机仍然保留了旧的IP地址。在响应请求的时候，Web服务器响应的IP包源地址是202.5.3.1，目的地址是203.10.3.1，这样的IP包可以正常地在全球Internet上寻址传输，当到达双向NAT的时候，地址再次被修改，源地址仍然被还原成192.168.3.6，目的地址改为host A的内部网络地址202.5.3.1。具体过程如图3所示。

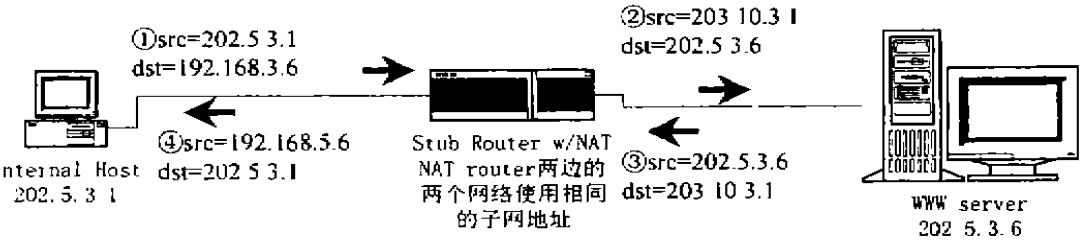


图3 双向NAT的翻译过程

对于双向NAT来说，它所连接的两个网络是完全隔绝的，即使是域名空间也是靠内部网络的DNS-ALG完成的，所以可能出现内外部网络使用相同的IP地址的情况。既然两个网络之间完全不知道对方的IP地址安排，使用相同的IP地址也就没有什么问题。两个网络之间也不应该有任何路由信息的交换，唯一沟通的桥梁是双向NAT系统本身在两个网络之间进行地址翻译。

5 NAT系统应用举例——虚拟服务器

在实际应用中，NAT系统的应用范围已经远远超过解决Internet上地址紧张这类问题，诸如虚拟服务器、备份服务器群集、冗余路由等应用也可以使用NAT来实现，我们知道，对于繁忙的站点，通常使用多服务器系统提供服务以提高处理能力。常见的解决方案是应用层的，比如DNS轮转法[RFC1794]。也就是说，对于同一个FQDN(Fully Qualified Domain Name)的查询，可以从一组IP中任意选择一个返回，而这些IP对应这一组服务器。但是DNS轮转法受到DNS缓冲的影响，在访问量不太大的情况下，缓冲被刷新的间隔比较长，可能导致相比之下某台服务器的负载远高于其他服务器。只有在该域名被大量不同客户访问的情况下才能取得比较好的负载均衡效果。DNS轮转法还有一个显著缺点就是不能有效地处理服务器失效的情况，即失效服务器的IP仍然可能被轮转DNS返回。这种情况下应用NAT系统可以获得良好的效果。图4是使用NAT系统实现虚拟服务器的例子。

Internet上对该虚拟服务器(VS)的访问使用NAT router的外部地址。在请求IP包到达VS之后，VS根据它所掌握的实际服务器的负载情况对目的地址字段进行相应的修改，从而将该IP包转发到目前相对负载较轻的实际服务器。对于请求的响应也经过NAT router的修改使之看上去象从VS的IP返回的报文。该方法有两个优点，首先，所有的进/出IP包都经过VS，因此VS在决定使用哪个实际服务器的时候可以根据IP流量进行比较精确的选择；其次，当某一个实际服务器RS1失效的时候，VS在把报文转发给RS1的时候会发现超时，这时VS可以不把错误返回给发出请求的client，而是自动尝试另一台服务器RS2，从而实现服务器的无缝冗余。

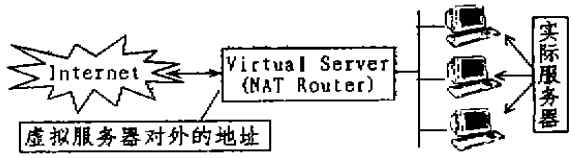


图4 虚拟服务器的实现

假设服务器失效是独立事件，服务器i失效的概率是$p_i(i=1..n)$，NAT router失效的概率是p_{NAT}，那么整个虚拟服务器系统失效的概率就是：

$$p_{sys}=1-((1-\prod_{i=1}^{n}p_i)*(1-p_{NAT}))$$

显而易见，这样的系统可靠性要高得多。这样做法的缺点是所有进出的IP包都要经过NAT router的翻译，查表操作和计算校验和的操作会使NAT的计算能力成为潜在的瓶颈。

6 实现NAT系统时的安全考虑

6.1 对内部主机的保护

出站NAT(即traditional NAT)实际上可以看作一个单向的过滤路由器，因为外部主机不能主动发起会话，因此客观上从外部主机流向内部网络的流量受到限制。而双向NAT系统中，如果用来向外部主机提供解析内部主机名字服务的应用层DNS(DNS-ALG)

合理设置，也可以避免敏感主机暴露在外部网络可以到达的范围内，从根本上说，这种防御是基于一种"未知即是安全"的思想，主要手段是通过对外隐藏内部网络结构以保护内部网络。但是，如果认为仅仅安装一个NAT系统就可以安全地保护内部网络的想法是错误的，因为如果只使用NAT作为安全方案中唯一的保护手段无疑使NAT系统成为最显著的攻击目标。由于NAT系统本身的需要，它工作在内外部网络的交界处，这一方面使得任何攻击者可以通过Internet从任意点连接它；另一方面，一旦获得它的控制权就可以借助它更方便地进入内部网络。因此，在有较高安全要求的情况下，NAT系统应该和应用层网关或/和应用层防火墙联合使用。

6.2 对出入站流量的保护

上面只讨论了对内部主机的保护，但是，以明文方式(plain text)在Internet主干网络上传送的数据仍然暴露在多种威胁之下，例如远程访问时的ISP，逐段链路上的路由器等，传输途中任意一个设备都可以获得数据内容并且加以修改。为了全面解决这些数据泄密的隐患，Internet Engineering Task Force(IETF)下的IP Security working group于1998年提出了IP Security(IPSec)技术[4]，这是一套综合的解决方案，它工作在IP层上，对上层的协议(TCP、UDP、ICMP、BGP等)提供包括以下所有方面的服务[5]：

·数据源身份认证。证实数据报文是声称的发送者发送的；

·数据完整性。证实数据报文在传输途中没有被修改过，无论是故意改动还是传输错误；

·数据保密。通过加密隐藏明文的消息；

·重放攻击保护。如果攻击者截获数据报文在稍后某个时间重新发送，应该能够检测；

·自动的密钥管理和安全关联管理。保证只需少量或者根本不需要手工配置就可以在扩展的网络上简单地实现安全策略。

IPSec安全体系的主要协议包括IP认证报头(AH)、IP负载安全封装(ESP)和因特网安全关联与密钥管理协议(ISAKMP)。这其中，ISAKMP提供自动建立安全关联和管理密钥的功能，AH提供数据源身份认证、数据完整性保护和重放攻击保护，而ESP除了可以提供AH提供的所有功能之外，还可以进行数据保密，AH和ESP都有两种运用模式，分别称为传输模式(Transport Mode)和通道模式(Tunnel Mode)。以ESP为例，它操作的单位是单个的报文，在传输模式下，原来的IP包的头部不变，被加密保护的是IP包的载荷(payload)部分，也就是对上层协议进行保护；而在通道模式下，整个IP包被作为加密保护的对象，由ESP处理过程另外加上一个新的IP头部，如图5所示。

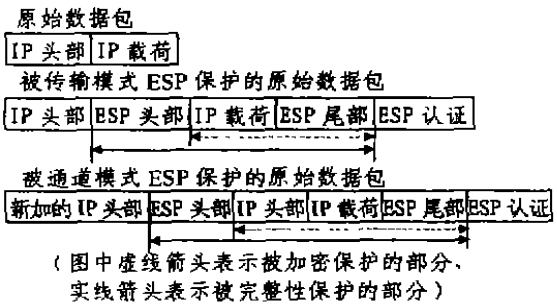
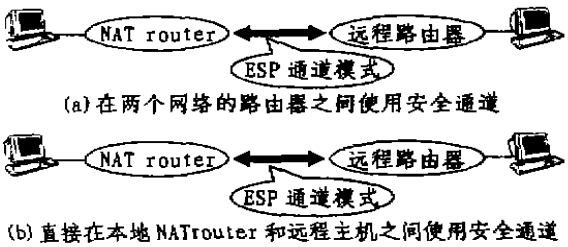


图5 传输模式的ESP和通道模式的ESP

从图中可以看出，ESP的做法是在IP头部之后和要保护的数据之前插入一个ESP头部，在新生成的整个报文的尾部再增加一个ESP尾。受保护的数据可以是一个上层协议也可以是整个IP数据包。当使用ESP保护IP包的数据完整性的时候，如果接收端检查TCP/UDP包校验和时，由于源地址和目的地址被修改，会出现接收端因为校验和不对而丢弃。当使用NAT系统的时候，直接应用端到端的IPSec方案的话，将出现一个不可调和的矛盾—NAT系统需要修改IP包，而IPSec的数据完整性保护的目的就是禁止传输途中任何系统修改IP包，针对两者根本性的冲突，可以考虑如下的临时措施：假如NAT系统是可以信任的，那么可以使用网关到网关的安全通道或者网关到目的主机的安全通道。内部网络主机仍然使用通常的通道和网关进行通讯，IP包正常广播和寻径，当需要离开本地网络的IP包到达网关时，在外出之前被网关使用IPSec协议处理，然后通过公共的Internet传输，在到达目的主机所在网络后或者被目的网络的网关进行安全性检查之后以明文交给目的主机，或者直接送到目的主机由目的主机上的协议栈自行处理，这两种方式示意如图6。



(a) 在两个网络的路由器之间使用安全通道

(b) 直接在本地NATrouter和远程主机之间使用安全通道

图6 网关到网关和网关到主机的安全通道

7 实际应用系统

目前我们已经成功使用NAT系统作为实验室地

址短缺问题的解决方案。实验室共30余台机器，但是因为能够分配到的IP地址仅有三个，为了使所有机器能够自由地接入Internet，我们使用一台双Pentium® CPU的机器作为NAT router，安装两块Intel Ether Express网卡，分别使用内部地址192.168.5.2和外部地址202.119.37.8；软件使用RedHat Linux 6.0。在具有2.0.*以上版本的内核的Linux发行中，其中内含了ipchains，这是一个简单高效的透明网关的实现，其余30多台机器将网关设置为192.168.5.2即可实现透明访问Internet，利用ipchains的管理功能，还可以实现"黑名单"功能，如拒绝内部网络某些特定IP访问外部地址以及限制所有机器访问外部网络某些不健康的资源。唯一需要注意的是，这样的系统结构导致使用诸如NetBEUI协议工作的软件失效；在访问ftp的时候也需要显式指定使用PASV方式并且在NAT系统上使用对FTP协议的补丁模块。

结束语 在目前中小型网络环境中，NAT方案获得了广泛的应用，其应用领域已经从单纯的解决地址冲突扩展到了负载均衡、多穴路由等领域，而且由于IPv6的实用系统进展缓慢，决定了当前的IP协议体系还需要存在很长一段时间，NAT系统还会继续发展和完善。与此同时，虚拟私用网络(Virtual Private Network，VPN)的需求也在逐渐增强，这将导致IPSec安全体系的广泛采用。相信在IPv6没有普及开来之前，能够实施IPSec安全体系的变形NAT方案将成为对安全性有较高需求的私有网络的首选方案。

参考文献

1 周明天，汪文勇. 网络原理与技术. 清华大学出版社，1993
2 Using IPSec to Construct Secure Virtual Private Networks. IBM Corp，1998
3 Kent S，Atkinson R. IP Encapsulating Security Payload (ESP). RFC 2406，November 1998
4 Kent S，Atkinson R. Security Architecture for the Internet Protocol. RFC 2401，November 1998
5 Srisuresh P，Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663，August 1999
6 Srisuresh P，Tsirtsis G，Akkiraju P，Heffernan A. DNS extensions to Network Address Translators (DNS-ALG). RFC2694，September 1999
7 Hasenstein M. IP Network Address Translation. 1997

(上接第28页)

的结合也将成为访问控制技术的趋势之一，如具有人工智能特性的自适应访问控制技术、与入侵检测系统相结合的访问控制技术等。

参考文献

1 陈爱民，于康友，管海明编著. 计算机的安全与保密. 北京：电子工业出版社，1992. 141～145
2 America Department of Defense. TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA，CSC-STD-001-83，15 Aug 83
3 Harrison M H，Ruzzo W L，Ullman J D. Protection in Operating Systems. Communications of ACM，19(8)：461～471
4 Sandhu R S. The Typed Access Matrix Model. In Proc. of IEEE Symposium on Security and Privacy，Oakland. California，1992. 122～136
5 Sandhu R S，Ganta S. On Testing for Absence of Rights in Access Control Models. In Proc. of IEEE Computer Security Foundations Workshop VI，Franconia NH，1993. 109～118
6 Osborn S. Mandatory access control and role-based access control revisited. In：Proc. of the second ACM workshop on Role-based access control. November 1997. 31～40
7 Badger L. Controlled Execution UNIX. In：Proc. of the 17th National Computer Security Conf. 1994. 66～76
8 Brewer D E，Nash. The Chinese Wall Security Policy. IEEE Symposium on Security and Privacy，1989. 215～228
9 Sandhu R S. Lattice-Based Enforement of Chinese Walls. Comupters & Security，1992，11(8)：753～763
10 Smith Dr. C L，et al. A Survey to Determine Federal Agency Needs for a Role-Based Access Control Security Product. In Proc of the 3rd Int Software Engineering Standards Symposium(ISESS '97)，P222～232
11 Sandhu R S，Coyne E J，et al. Role-Based Access Control Models. IEEE Computer，1992，29(2)：38～47
12 Awischus R. Role based access control with the security administration manager (SAM). In：Proc. of the second ACM workshop on Role-based access control. November 1997. 61～68
13 Thomas R K，Sandhu R S. Task-base Authorization Controls (TBAC). A Family of Models for Active and Enterprise-oriented Authorization Management. In：Proc. of the IFIP WG11.3 Workshop on Database Security，California，August 1997
14 Denning D E. The Limits of Formal Security Models，America National Computer Systems Security Award Acceptance Speech，October1999
15 Sandhu R S. The Ntree：A Two Dimension Partial Order for Protection Groups. ACM Transactions on Computer Systems，1988，6(2). 197～222
16 The Reflected Tree Hierarchy for Protection and Sharing. Information Processing Leters，1989，30(1)