NAT技术及其在防火墙中的应用

本文较为深入地讨论了NAT的工作原理，介绍了它在防火墙中的应用。最后，对NAT技术的安全性进行了分析。

上海同济大学计算机系　户现锋　张大陆

前言

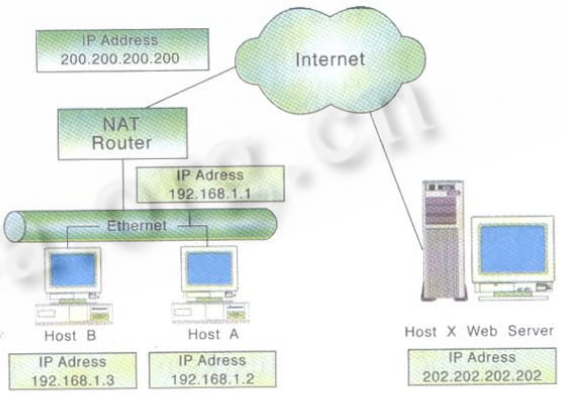
随着因特网的飞速发展，每年连入的主机数都要翻倍。由于开始设计因特网的时侯并没有考虑到这么大的规模，所以分组的地址选择了32位，它可以使分组的格式很好的对齐，但随着连入网络的网络越来越多，因特网面临着B类地址耗尽，路由表爆炸和整个地址耗尽的危机。NAT(Network address translation)技术和(CIDR)无类域间路由就是为解决这些问题而开发的一种直接的解决方案，它可以使因特网得到足够的喘息时间来等待新一代IP协议的出台。由于NAT技术提供了一种掩饰网络内部本质的一种方法，即NAT通过一个外部地址来响应外部世界的寻址，从而在防火墙中得到了广泛的应用。

NAT技术的工作原理

网络地址翻译(NAT)的基本功能就是用一个或几个IP地址来实现一个局域网络上的所有主机都可以访问Internet。NAT技术可以为TCP、UDP以及Icmp的部分信息进行透明中继，下面就以TCP为主要对象讨论其工作原理。

TCP是建立在所谓的连接抽象(connection abstraction)之上的，它所对应的对象不是TCP的一个单独的端口而是一条虚电路连接，也就是说TCP是使用连接而不是使用协议端口号作为基本的抽象概念。在TCP中连接是用一对端点来标识的。TCP把端口(endpoint)定义为一对整数，即(host,port)，这样我们可以将一条TCP连接用一个四元组(source address:source port : destination address: destination port)来定义，这样的一个连接抽象允许多个连接共享一个端点，例如：两条连接(191.168.1.1:1184:192.168.1.3:80)、(192.168.1,2:1184:192.168.1.3:80)共享同一个端口(192.168.1.3:80)，但这样并不会引起岐义。从而可以看出这种基于连接的抽象为利用一个IP地址进行外部世界的访问提供了基础。实际上，虽然UDP是无连接的，但我们可以将它作为虚连接来看待。

NAT网关上运行的TCP/IP网关软件与常规的网关软件并不相同。通常常规路由器只是机械的根据IP包中的目的IP地址以及路由表将IP数据报从一个网络转发给另一个网络，而NAT网关在Internet内部网络和Internet之间中继IP数据报并非凭借目的IP地址，它的中继是面向连接的。如下图所示：



假设在局域网LAN A接入Internet处有一个NAT网关，网关处理所有网络内外之间的TCP/IP连接。NAT网关具有内网端口和外网端口，两个端口各被分配一个IP地址，其中外网端口的IP地址是合法的全球唯一的IP地址，200.200.200.200，内网端口的IP地址是一般为保留地址，比如设为192.168.1.1。当内部网络中的一台主机例如A，要访问Internet上的WEB服务器X(主机地址为202.202.202.202)，那么首先A要与X建立TCP连接，设定主机A与此次连接分配的TCP端口为1030，此时主机A将IP数据包(D=202.202.202.202:80,S=192.168.1.2:1030)发向NAT网关，当NAT接受到数据包后，会动态的分

配一个未用TCP端口，例如：1330，然后修改数据包中的地址为(D=202.202.202:80,S=200.200.200.200:1330)，计算数据包的校验和后发向Internet。我们可以看到此数据包中已经不含任何私有地址的信息。NAT已记录下这对映射：(D=202.202.202.202:80,S=192.168.1.2:1030)<->(D=202.202.202:80,S=200.200.200.200:1330)。以后当NAT接受到这一对主机间的任何一个IP分组时，NAT网关会查询内部的映射记录表格，根据这条映射关系使其顺利通过NAT，反之亦然。

总之，NAT的地址转换过程存在三个不同的阶段：

1. 连接关系的映射关系的建立阶段

这发生在会话的开始，当内部的一台机器要与外部的一台机器发生通信时发生，NAT动态的为其分配未使用的TCP端口号，并且会记下这个映射关系，为以后转发IP数据包的使用。

2. 映射关系的查找与转换阶段

当有外部进入的数据报或从内部出去的数据报通过NAT时，NAT都在内部进行了查找以便找到对应的映射进行地址转换。

3. 映射关系解除阶段

当一次TCP的连接关闭时，NAT会释放分配给这条连接的端口，以便以后的连接可以继续使用。

NAT技术在防火墙中的应用

防火墙的主要功能就是防止外部主机对内网中主机的非授权访问，而限制从外部网络到内部网络的连接是一个主要技术之一，NAT具有这种功能。当外网的主机要主动访问内网的主机时，一般情况下要首先与内网中的某台主机建立连接(多数内网不允许从外部发起连接)，但是，首先它不知道内网主机的IP地址(由前面的分析可知，在Internet传输的IP数据报并没有含有内部网络地址的私有信息，这样，内网中的主机对于外部主机是不可见的，它们被NAT保护起来了)，其次内网主机地址一般是内部保留地址，不允许在Internet上传输，再次NAT内部的记录表中也没有与这个外部来的连接的表项，将不允许连接的请求通过NAT，这样就起到了防火墙安全防护的作用。

另外，通过使用代理技术也可以使用一个IP地址供多个同时上网，但是这种技术的一个缺点就是需要对客户端的软件进行修改的配置，给用户带来很多不便，更为重要的是需要为每一种应用都编写特定的代理服务器，使得系统扩展性不是很好。而NAT技术则工作在网络中较低的层次，逻辑上是工作在IP层，给用户连接Internet提供了更大的透明性，其工作则更象一个路由器而并非一个代理网关，同时也使得网络应用的扩展，并不需要给每种新的应用都开发一种代理服务。由于NAT技术并没有工作在应用层(代理网关工作在应用层，它理解提供服务的每一种协议细节)，NAT并不需要理解和操纵应用层的数据，从而具有更高的效率。使得NAT技术在防火墙中得到应用。

NAT技术的安全性分析

下面对NAT技术的安全性做一些分析：

1.NAT可以作为一个单向的过滤器，限制从外部主机到内部主机的连接。另外当端口地址在NAT内动态分配时，使得外部攻击者对NAT域中的一个特定主机的攻击更加困难。

2. 当NAT设备不在安全域中时，应用级的负载可以进行端到端的加密，比如利用SSL。只要负载中不包含IP地址和运输层的端口信息，就可以提高安全性。

3. 如果将NAT设备和应用网关相结合，可以为应用层中含有IP地址信息的连接进行地址翻译，确保数据报不含有私有的地址信息，这样NAT可以做到对协议的透明，起到透明路由器的作用。

4. 由于NAT设备是作为一台Internet主机出现，因此也被作为攻击的对象。例如易受SYN Flood和Ping flood attacks，应采用相应的技术对NAT设备进行保护。

5.NAT在做到地址隐藏的同时，也减少了提供安全的额外选择，例如IPsec的选用，目前，我们正在进行二者的集成与开发之中。■

参考文献

1 K.Egevang,P.Francis.The IP Network Address Translator (NAT).RFC1631 1994-05

2 P.Srisuresh,M.Holdrege.IP Network Address Translator (NAT) Terminology and Considerations.RFC2663 1999-08

3 Kent,S.and R.Atkinson,"Security Architecture for the Internet Protocol",RFC2401,1998-11

4 IETF.Security L2TP using IPSEC,1999

5 Netscape Communication Corp .The SSL protocol Version 3.0,1996

6 Tanenbaum AS.Computer Networks.Third Edition_Prentice-Hall,1996