构建基于校园网的堡垒路由器

Building Fort Router Based on Campus Network

摘要：本文讨论了在典型校园网环境中将一台路由器配置为堡垒路由器的实现方法，使之成为校园网抵御外部攻击的第一道安全屏障。

关键词：校园网　堡垒路由器　网络安全

宋博强　陈洪涛　张晟

（北京军医学院网络管理中心　100071）

在典型的校园网环境中，路由器一般处于防火墙的外部，负责与INTERNET的连接。这种拓扑结构实际上是将路由器暴露在校园网安全防线的外面，如果路由器本身又未采取适当的安全防范策略，就可能成为攻击者发起攻击的一块跳板，对内部网络安全造成威胁。

本文以CISCO路由器2621为例，详细介绍了将一台路由器配置为堡垒路由器的实现方法，使之成为校园网抵御外部攻击的第一道安全屏障。

1　基于访问表技术建立安全防范策略

1.1　防止外部的IP地址欺骗

外部网络的用户可能使用内部网的合法IP地址或者回环地址作为源地址，从而实现非法访问。针对此类问题可建立如下访问列表：

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.255.255 any
! 阻止源地址为私有地址的所有通信流
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
! 阻止源地址为回环地址的所有通信流
access-list 101 deny ip 224.0.0.0 7.255.255.255 any
! 阻止源地址为多目地址的所有通信流
access-list 101 deny ip host 0.0.0.0 any
! 阻止没有列出源地址的通信流
```

说明：可以在外部接口的向内方向使用101过滤。

1.2　防止外部的非法探测

非法访问者对内部网络发起攻击前，往往会用PING或者TRACERT命令探测你的网络，所以可以禁止从外部用ping、traceroute探测你的网络。建立如下访问列表：

```
access-list 102 deny icmp any any echo
!阻止用 ping 探测你的网络
access-list 102 deny icmp any any time-exceeded
!阻止用 traceroute 探测你的网络
```

说明：在外部接口的向外方向使用102过滤。在这里主要是阻止答复输出，不阻止探测进入。

1.3 .保护路由器不受攻击

路由器一般可以通过TELNET或SNMP访问，应该确保INTERNET上没有人能用这些协议攻击你的路由器。假定路由器外部接口serial0的IP为200.200.200.1，内部接口fastethernet0的IP为200.200.100.1。可以生成阻止TELNET、SNMP服务的向内过滤，建立如下访问列表：

```
access-list 101 deny tcp any 200.200.200.1 0.0.0.0 eq 23
access-list 101 deny tcp any 200.200.100.1 0.0.0.0 eq 23
access-list 101 deny udp any 200.200.200.1 0.0.0.0 eq 161
access-list 101 deny udp any 200.200.100.1 0.0.0.0 eq 161
```

！在外部接口的向内方向使用101过滤。当然这会对管理员的使用造成一定的不便，这就需要你在方便与安全之间做出选择。

1.4　阻止对关键端口的非法访问

关键端口可能是内部系统使用的端口或者是防火墙本身暴露的端口。

对这些端口的访问应该加以限制，否则这些设备就很容易受到攻击。建立如下访问列表：

access-list 101 deny tcp any any eq 135

access-list 101 deny tcp any any eq 137

access-list 101 deny tcp any any eq 138

access-list 101 deny tcp any any eq 139

access-list 101 deny udp any any eq 135

access-list 101 deny udp any any eq 137

access-list 101 deny udp any any eq 138

access-list 101 deny udp any any eq 139

!示例中列出的一些关键端口，都是WINDOWS环境中提供一些服务的端口。针对不同的应用环境，关键端口也会不同，具体可以参见相关的网络安全白皮书。此外，对一些常见的特洛依马程序及其使用的缺省端口也应阻止。可以在外部接口的向内方向使用101过滤。

1.5 对内部网的重要服务器进行访问限制

对于没有配备专用防火墙的校园网，采用动态分组过滤技术建立对重要服务器的访问限制显得尤为重要。对于配备了专用防火墙的校园网，此项任务可以在防火墙上完成，这样可以减轻路由器的负担。无论是基于路由器实现，还是在防火墙上完成设置，首先都应该制定一套访问规则。可以考虑建立如下的访问规则：

· 允许外部用户到WEB服务器的向内连接请求；

· 允许WEB服务器到外部用户的向外答复；

· 允许外部SMTP服务器向内部邮件服务器的向内连接请求；

· 允许内部邮件服务器向外部SMTP服务器的向外答复；

· 允许内部邮件服务器向外DNS查询；

· 允许到内部邮件服务器的向内的DNS答复；

· 允许内部主机的向外TCP连接；

· 允许对请求主机的向内TCP答复。

其他访问规则可以根据各自的实际情况建立。列出允许的所有通信流后，设计访问列表就变得简单。注意应将所有向内对话应用于路由器外部接口得IN方向，所有向外对话应用于路由器外部接口得OUT方向。

2 常见攻击手段及其对策

2.1 防止外部ICMP重定向欺骗

攻击者有时会利用ICMP重定向来对路由器进行重定向，将本应送到正确目标得信息重定向到他们指定的设备，从而获得有用信息。禁止外部用户使用ICMP重定向的命令如下：

interface serial0

no ip redirects

2.2 防止外部源路由欺骗

源路由选择是使用数据链路层信息来为数据报进行路由选择。该技术跨越了网络层的路由信息，使入侵者可以为内部网的数据报指定一个非法的路由，原本应该送到合法目的地的数据报就会被送到入侵者指定的地址。禁止使用源路由的命令如下：

no ip source-route

2.3 防止盗用内部IP地址

攻击者可能会盗用内部IP地址进行非法访问，针对这一问题，可以利用CISCO路由器的ARP命令将固定IP地址绑定到某一MAC地址之上。具体命令如下：

arp 固定IP地址 MAC地址 arpa

2.4 在源站点防止smurf

要在源站点防止smurf，关键是阻止所有的向内回显请求。这就要防止路由器将指向网络广播地址的通信映射到局域网广播地址。可以在LAN接口方式中输入如下命令：

no ip directed-broadcast

3 关闭路由器上不用的服务

3.1 利用端口扫描检查运行服务

路由器除了提供路径选择外，它还是一台服务器，可以提供一些有用的服务。路由器运行的这些服务可能会成为敌人攻击的突破口，为了安全起见，最好关闭这些服务。

通过查看路由器的配置文件可以了解路由器启用了哪些服务。但这种方法会有疏漏。因为路由器的配置文件只显示与缺省设置不同的配置，而CISCO IOS版本不同，缺省启用的服务也会不同。为了防止忽略一些关键信息，可以对路由器进行端口扫描，以了解它正在启用的服务。

3.2 关闭CISCO路由器上常用服务

CISCO路由器提供的大多数服务都是用于管理或诊断的，常用的包括：

· CSICO发现协议，关闭命令：no cdp run

· FINGGER服务，关闭命令：no ip finger

· HTTP服务，关闭命令：no ip http server

· SNMP服务，关闭命令：no snmp