基于广域网防火墙技术的 FTP 被动模式的文件传输

The passive modul file Transfer through firewall Based On FTP

周晓林 彭延昌 胡庆梅 周冉 陈宝锋 (安徽省气象台 合肥 230031)

摘要:在广域网中使用 FTP 命令穿过防火墙进行文件传输时,如果使用主动模式,那么对大于 1024 的端口进行过滤实际上是不可能的。因为这个通路由于安全问题,在防火墙上是关闭的,那么唯一的方法就是使用被动模式的 FTP 工具。在被动模式下,所有的 FTP 连接和数据传输请求都由 FTP 客户发起,这样就可以避免服务器反过来连接私用网络的机器和大于 1024 的端口问题。

关键词:广域网 VPN 防火墙 FTP 被动模式

1 前言

随着互连网技术的不断深入发展和应用,网络安全也越来越受到用户的关注,防火墙技术也成为单位组织通过广域网与外界组织进行网络互连免受网络病毒侵害的一道屏障,但是在使用防火墙技术的同时,也要考虑到防火墙对现有业务的影响,在广域网中使用 FTP 命令穿过防火墙进行文件传输时,由于 FTP 命令使用两个连接:首先客户向服务器的 21 端口发出请求,建立一个连接。但是这个连接仅用于传输 FTP 命令。当客户程序正式要求传输文件时,服务器向客户机发出要求,建立第二条连接,文件内容由这条连接传递。第二条连接在服务器和客户端都使用较高的端口号(大于 1024),这个通路由于安全问题,在防火墙上是关闭的,这样造成第二条连接在服务器和客户端的链路不能连通,数据不能通过 FTP 命令传输。但是可通过目前发展的 FTP 工作模式,即第二条连接不由服务器发起,而是让客户机向服务器的 20 端口发出请求,用这个连接和 FTP 被动模式来传递数据。下面介绍基于防火墙技术和 FTP 被动模式的广域网文件传输的实现。

2 基于 VPN 技术广域网的路由协议设置

在完成基于防火墙技术和 FTP 被动模式的广域网文件传输的实现之前,首先完成异地路由器对接以便建立异地通信。下面仅以基于 VPN 技术来实现异地路由器对接。(采用两台华为路由器 :R1、R2)其配置要同时支持 GRE 和 IPsec 协议。配置以省气象台:内部网段网号(202.21.81.0);互连网段网号(218.22.10.0);

路由器内部端口 IP 地址(202.21.81.250);路由器 Internet 端口 IP 地址(218.22.10.171);隧道端口 IP 地址(192.168.1.1)与亳州市气象局:内部网段网号(202.21.95.0);互连网段网号(218.22.248.0);路由器内部端口 IP 地址(202.21.95.254);路由器 Internet 端口 IP 地址(218.22.248.82);隧道端口 IP 地址(192.168.1.2)互连为例。

2.1 对于路由器 R1:省气象台端配置如下

```
access - list normal 101 permit ip 202.21.0.0 0.0.255.255 202.21.0.0 0.0.255.255 (访问控制列表 101,供 Vpn 使用)
access - list normal 101 deny ip any any (访问控制列表 101,供 Vpn 使用)
hostname behf (路由器名称)
crypto IPsec transform tran (设定 IPsec 加密验证组,选择加密方式)
esp - new hash sha1 - hmac - 96
!
crypto map map_102 10 manual (设定 Vpn 通道验证方式,及验证密码)
match address 101 (引用访问列表)
set transform tran(引用转换方式)
set local - address 192.168.1.1(设置本端地址)
```

```
set peer 192.168.1.2(设置对端地址)
set session-key inbound esp spi 58102 (设置 SPI)
set session-key inbound esp string-key bfbz (设置密钥)
set session-key outbound esp spi 58321
set session-key outbound esp string-key behf
!
 interface Ethernet0 (外网接口设置)
 speed auto
 duplex auto
 no loopback
 description internet
 ip address 218.22.10.171 255.255.255.240
 nat inside 110 interface
  !
 interface Ethernet1 (内网接口设置)
 speed auto
 duplex auto
 no loopback
 ip address 202.21.81.250 255.255.255.0
  interface Tunnel102 (设置 Vpn 隧道,引用验证方式)
  encapsulation tunnel
  description bfbz
  ip address 192.168.1.1 255.255.255.252
  crypto map map_102
  tunnel source 218.22.10.171
  tunnel destination 218.22.248.82
   !
  exit
  ip route 0.0.0.0 0.0.0.0 218.22.10.161 preference 60 (默认路由)
  ip route 202.21.95.0 255.255.255.0 Tunnel 102 preference 60 到亳州市气象台路由。
```

2.2 对于路由器 R2:亳州市配置如下

```
 access-list normal 101 permit ip 202.21.0.0 0.0.255.255 202.21.0.0 0.0.255.255 (访问控制列表 101,共 Vpn 使用)
 access-list normal 101 deny ip any any (访问控制列表 101,共 Vpn 使用)
 hostname bfbz (路由器名称)
 !
 !
 crypto IPsec transform tran (设定 IPsec 加密验证组,选择加密方式)
  esp-new hash sha1-hmac-96
  esp-new encrypt blowfish
 !
 crypto map map_321 10 manual (设定 Vpn 通道验证方式,及验证密码)
  description beah
  match address 101
  set transform tran
  set local-address 192.168.1.2
  set peer 192.168.1.1
  set session-key inbound esp spi 58321
  set session-key inbound esp string-key behf
  set session-key outbound esp spi 58102
  set session-key outbound esp string-key bfbz
 !
 interface Ethernet0 (外网接口设置)
  speed auto
  duplex auto
  no loopback
  ip address 218.22.248.82 255.255.255.248
  nat inside 110 interface
 !
 interface Ethernet1 (内网接口设置)
  speed auto
  duplex auto
  no loopback
  ip address 202.21.95.254 255.255.255.0
 !
  interface Tunnel321 (设置 Vpn 隧道,引用验证方式)
  ip address 192.168.0.2 255.255.255.252
  crypto map map_321
  tunnel source 218.22.248.82
  tunnel destination 218.22.10.171
   !
 ip route 0.0.0.0 0.0.0.0 218.22.248.92 (默认路
```

由)

ip route 202.21.0.0 255.255.0.0 Tunnel 321 到省气象台路由。

3 防火墙技术的实现

防火墙有两种,称为代理防火墙和包过滤型防火墙。包过滤型防火墙具有较强的灵活性和功能,目前采用较为广泛。设计防火墙的策略有两种基本的思路,一种是一开始就禁止所有的数据包流通,然后根据需要打开的服务,依次开放各种端口;另一种是一开始就开放所有的服务,然后对不可靠的端口进行封锁。原则上,前一种方法比较可靠。在设计过滤策略的时候,主要的应该是考虑 TCP/IP 连接的方式,TCP/IP 连接是双向的,如果要访问某台主机的 WWW 服务,那么这个连接涉及的是:对方的主机地址、对方的 WWW 端口地址(80)、自己的 IP 地址。除此之外,FTP 程序还要申请一个端口地址用来通信。按照上述,FTP 使用的两个端口为:端口 21(FTP)和端口 20(FTP - -data),分别用于 FTP 命令和发送 FTP 数据。所以在防火墙上应该开放这些端口、以及相应的地址和协议。在防火墙上开放了这些端口、以及相应的地址和协议之后,FTP 数据便可以通过上述的防火墙。但在端到端经过防火墙进行 FTP 传输文件时,还要使用正确的传输模式。

本单位防火墙网络接口共有 3 个 10/100M 网络接口,分别为 eth0、eth1、eth2,默认设置为 10/100M 自适应方式,特别情况下,如果需要强制设定接口的速率、双工方式,可以使用如下命令:

ifstat eth? [10|100] [0|1]

设置 eth? 的速率为 10M 或 100M,双工方式为半双工(0)或全双工(1)。

例如:设置 eth0 为 100M 全双工的命令为:

ifstat eth0 100 1

防火墙具体配置内容如下:

```
#设置机器名字
hostname gateway.ahqx
#加载相关模块
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ip_conntrack_h323
modprobe ipt_state
modprobe iptable_nat
modprobe ip_nat_ftp
modprobe ip_nat_h323
echo 80000 > /proc/sys/net/ipv4/ip_conntrack
_max
#设置网桥
brctl addbr br0
brctl stp br0 0
brctl addif br0 eth0
brctl addif br0 eth1
ip link set eth0 up
ip link set eth1 up
# IP 地址设置
ip addr add 218.22.3.176/28 dev br0
ip addr add 172.21.18.252/24 dev eth2
ip link set br0 up
ip link set eth2 up
# IP 路由设置
ip route add 0/0 via 218.22.3.161
ip route add 172.21.0.0/16 via 172.21.18.2
# IP 包过滤设置
# 清空所有规则
iptables -F
iptables -t nat -F
#允许所有已经建立连接的数据包
iptables -A FORWARD -j ACCEPT -m state -
-state ESTABLISHED,RELATED
#允许访问 80(www)
iptables -A FORWARD -j ACCEPT -d 218.22.
3.175
#iptables -A FORWARD -j ACCEPT -d 218.22.
3.175 -p tcp - -dport 80
. . .
. . .
. . .
#允许访问 20、21(ftp)
iptables -A FORWARD -j ACCEPT -d 218.22.
3.175 -p tcp - -dport 20
iptables -A FORWARD -j ACCEPT -d 218.22.
3.175 -p tcp - -dport 21
```

```
#其他的记日志(最多 10 个/sec)
iptables -A FORWARD -j LOG -d 218.22.3.175 --log-prefix 'Stream' -m limit --limit 10/sec
#其他的拒绝
iptables -A FORWARD -j REJECT -d 218.22.3.175
```

4 FTP 被动模式广域网文件传输的实现

在防火墙技术的实现之后,可以使用 FTP 命令通过防火墙进行广域网文件传输。在进行 FTP 传输时有主动模式和被动模式两种模式。在主动模式中,除了前面说道的 20、21 端口之外,实际上数据连接是从服务器发起,因此它在服务器上分配一个端口(大于 1024),再申请一个客户机上的端口(同样大于 1024),然后构造这个连接。显然,这两个端口的值都是不固定的,因此实际上没有办法来判断一个连接会不会是 FTP 主动模式的数据,这也就是说如果使用主动模式,那么对大于 1024 的端口进行过滤实际上是不可能的。因为这个通路由于安全问题,在防火墙上是关闭的,那么唯一的方法就是使用被动模式的 FTP 工具。在被动模式下,所有的 FTP 连接和数据传输请求都由 FTP 客户发起,这样就可以避免服务器反过来连接私用网络的机器和大于 1024 的端口。

4.1 基于 LINUX/UNIX 系统的被动模式的 FTP 文件传输

在 LINUX/UNIX 系统下进行被动模式的 FTP 文件传输方法是:首先使用 FTP 命令连接远程主机,在文件传输之前使用 passive 命令来确定被动模式,最后进行文件传输。

具体如下:

```
ftp 218.22.45.168
benj
benj
passive
prompt
mput VP*.EHF
close
bye
```

上述代码表示经过防火墙将一批文件名为 VP*.EHF 的文件传到远程机器 IP 地址为 218.22.45.168,ftp 用户名为 benj,用户密码为 benj 的机器上,并保存 VP*.EHF 的文件在该机上,采用的是被动模式(passive)的 FTP 文件传输。

4.2 基于 WINDOWS 系统的被动模式的 FTP 文件传输

通常基于 GUI 的 FTP 客户软件一般都是使用被动模式,只要在 WINDOWS 系统上安装 leapftp、cute_ftp 等图形 FTP 客户软件,即可完成与上述相同的被动模式的 FTP 文件传输。

5 结束语

在实现基于 UNIX 系统的被动模式的 FTP 文件传输和基于 WINDOWS 系统的被动模式的 FTP 文件传输之后,便可以通过批处理程序和提交进程来完成日常工作中大量批文件异地自动定时相互传输,UNIX 系统通过 crontab 命令提交进程。crontab 命令使系统在指定的时间周期性地执行调度命令,而这里的时间不是一个具体时间,比如每天 10:00、每月 10 日等;WINDOWS 系统通过配置计划任务来实现,具体方法可参照有关书籍和文章,在完成上述过程之后,便可以实现基于广域网防火墙技术的 FTP 被动模式的定时自动文件传输。上述防火墙是在灵巧网关 Smart Gateway 1.0 系统上配置通过。

参考文献

1 SYNGRESS MEDIA 公司著, Cisco 局域网交换配置技术,机械工业出版社, 2000.6。

2 蔡皖东, 计算机网络技术, 西安电子科技大学出版社, 1998.2。

3 黄永峰、闲勇、刘宪军、权进国等, Windows /Unix/ Linux 综合组网技术,清华大学出版社,2002.7。

4 华为技术有限公司,《Quiday NetEngine16E/08E/05 路由器用户手册-配置指导二分册》。

5 安徽华脉网络有限公司,《VPN 实验系统配置指导手册》。

6 王虹宇、张福利,LINUX 服务器管理员教程, 国防工业出版社。

7 周晓林、江双五等,《广域网下不同操作系统之间的批文件自动定时互相传输》,成都, 计算机应用研究,2005 年增刊。