

使用防火墙防止 DoS 攻击

【实验名称】

使用防火墙防止 DoS 抗攻击

【实验目的】

利用防火墙的抗攻击功能防止 SYN Flood 攻击

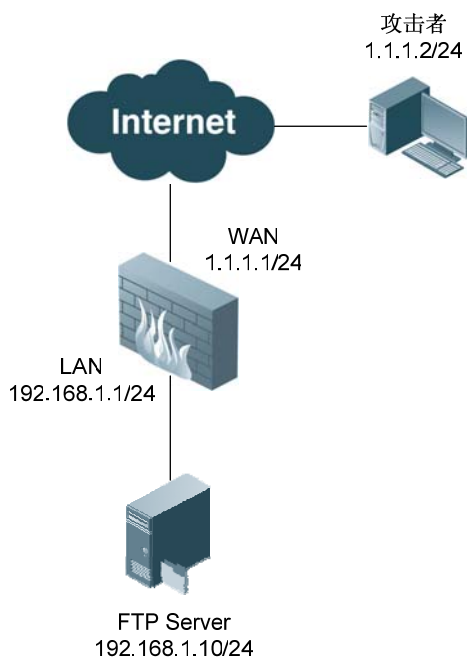
【背景描述】

某公司使用防火墙作为网络出口设备连接到 Internet，并且公司内部有一台对外提供服务的 FTP 服务器。最近网络管理员发现 Internet 中有人向 FTP 服务器发起 SYN Flood 攻击，造成 FTP 上存在大量的半开放连接，消耗了服务器的系统资源。

【需求分析】

要防止来自外部网络的 DoS 攻击，可以使用防火墙的抗攻击功能。

【实验拓扑】



【实验设备】

防火墙 1 台
PC 2 台（一台作为 FTP 服务器，一台模拟外部网络的攻击者）
FTP 服务器软件程序
SYN Flood 攻击软件程序

【预备知识】

网络基础知识
防火墙工作原理
DoS 攻击原理

【实验原理】

SYN Flood 是一种常见的 DoS 攻击，这种攻击通过使用伪造的源 IP 地址，向目标主机（被攻击端）发送大量的 TCP SYN 报文。目标主机接收到 SYN 报文后，会向伪造的源地址回应 TCP SYN_ACK 报文以等待发送端的 ACK 报文来建立连接。但是由于发送端的地址是伪造的，所以被攻击端永远不会收到合法的 ACK 报文，这将造成被攻击端建立大量的半开放连接，消耗大量的系统资源，导致不能提供正常的服务。

防火墙的抗攻击功能可以对 SYN Flood 攻击进行检测，阻止大量的 TCP SYN 报文到达被攻击端，保护内部主机的资源。

【实验步骤】**第一步：配置防火墙接口的 IP 地址**

进入防火墙的配置页面：网络配置—>接口 IP，单击<添加>按钮为接口添加 IP 地址。
为防火墙的 LAN 接口配置 IP 地址及子网掩码。

添加、编辑接口IP

* 网络接口: lan

* 接口IP: 192.168.1.1

* 掩码: 255.255.255.0

允许所有主机PING: ☐

用于管理: ☐

允许管理主机PING: ☐

允许管理主机Traceroute: ☐

确定 取消

为防火墙的 WAN 接口配置 IP 地址及子网掩码。

添加、编辑接口IP

* 网络接口:

wan

* 接口IP:

1.1.1.1

* 掩码:

255.255.255.0

允许所有主机PING:

☐

用于管理:

☐

允许管理主机PING:

☐

允许管理主机Traceroute:

☐

确定

取消

第二步：配置端口映射规则

为了使 Internet 中的用户可以访问到内部的 FTP 服务器，需要在防火墙上使用端口映射规则将 FTP 服务器发布到 Internet 中。

进入防火墙配置页面：安全策略->安全规则，单击页面上方的<端口映射规则>按钮添加端口映射规则。规则中的“公开地址”为防火墙外部接口（WAN）的地址；“内部地址”为内部 FTP 服务器的地址；“内部服务”为 FTP 服务器提供 FTP 服务使用的端口号，这里使用默认的 21 端口（FTP）；“对外服务”为 Internet 用户访问 FTP 服务器时使用的在外部看到的端口号，这里也使用默认的 21 端口（FTP）。

端口映射规则维护

满足条件

规则名:

pnat1

(1-15位 字母、数字、减号、下划线的组合)

源地址:

IP地址

掩 码

* 公开地址:

1.1.1.1

源地址转换为:

* 内部地址:

手工输入

IP地址 192.168.1.10

* 对外服务:

ftp

* 内部服务:

ftp

执行动作

检查流入网口:

wan

检查流出网口:

lan

时间调度:

流量控制:

用户认证:

☐

日志记录:

☐

隧道名:

序号:

1

连接限制:

☐ 保护主机 ☐ 保护服务 ☐ 限制主机 ☐ 限制服务

添加下一条

确定

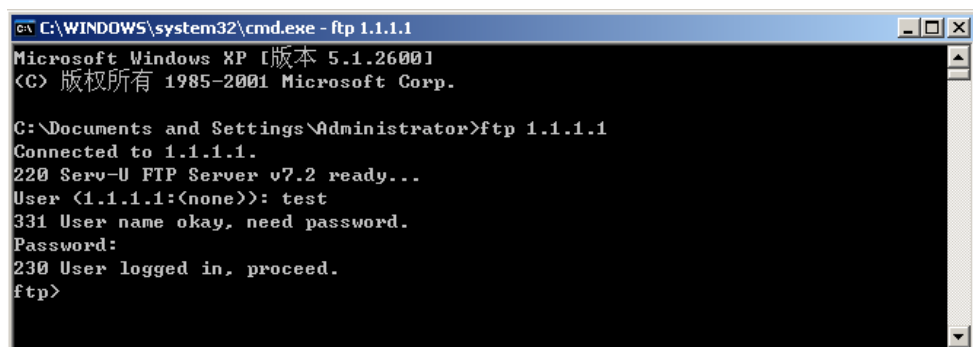
取消

第三步：验证测试

112

在内部 PC 上安装好 FTP Server 程序, 并进行相应的配置。在外部 PC 上测试到达 FTP 服务器的连通性, 注意这里使用的 FTP 目标地址为 1.1.1.1。防火墙将把发送到 1.1.1.1, 端口为 21 的请求重定向到内部的 FTP 服务器。

外部 PC 可以通过预先设置的用户名和密码登录 FTP 服务器。



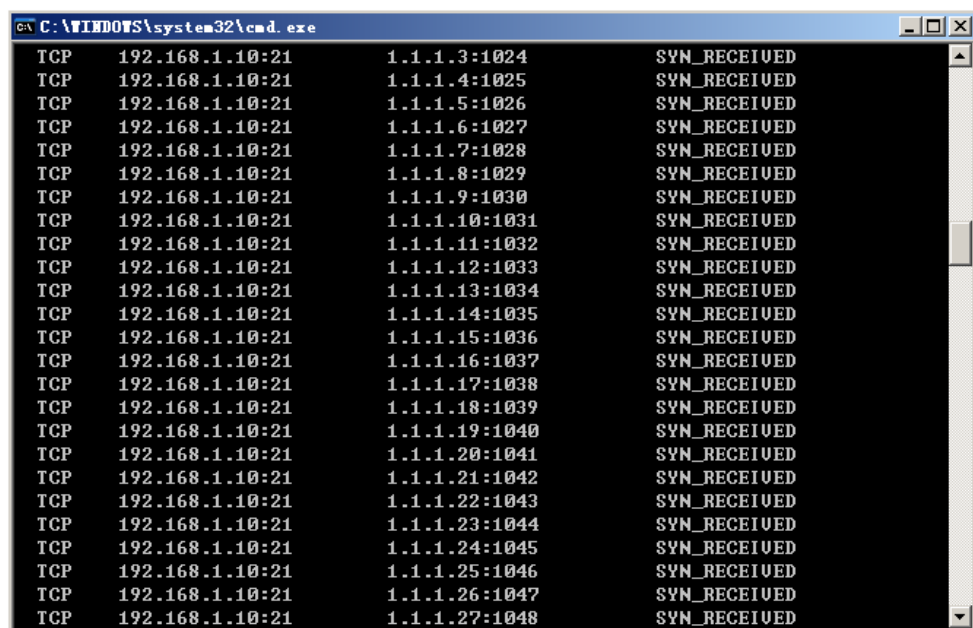
```

C:\WINDOWS\system32\cmd.exe - ftp 1.1.1.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ftp 1.1.1.1
Connected to 1.1.1.1.
220 Serv-U FTP Server v7.2 ready...
User (1.1.1.1:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp>
  
```

第四步: 实施 SYN Flood 攻击

在外部 PC 上使用 SYN Flood 工具向 FTP 服务器发起攻击。此时在 FTP 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 FTP 服务器的 21 端口建立了大量的半开放连接, 状态为 SYN_RECEIVED。



```

C:\WINDOWS\system32\cmd.exe
TCP    192.168.1.10:21      1.1.1.3:1024        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.4:1025        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.5:1026        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.6:1027        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.7:1028        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.8:1029        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.9:1030        SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.10:1031       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.11:1032       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.12:1033       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.13:1034       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.14:1035       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.15:1036       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.16:1037       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.17:1038       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.18:1039       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.19:1040       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.20:1041       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.21:1042       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.22:1043       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.23:1044       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.24:1045       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.25:1046       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.26:1047       SYN_RECEIVED
TCP    192.168.1.10:21      1.1.1.27:1048       SYN_RECEIVED
  
```

第五步: 配置抗攻击

进入防火墙配置页面: 安全策略—>抗攻击, 单击 WAN 接口后面的操作图标。

安全策略>>抗攻击										
接口名称	启用	SYN Flood	ICMP Flood	Ping of Death	UDP Flood	PING SWEEP	TCP端口扫描	UDP端口扫描	WinNuke	操作
dmz	✗	✗	✗	✗	✗	✗	✗	✗	✗	
lan	✗	✗	✗	✗	✗	✗	✗	✗	✗	
wan	✗	✗	✗	✗	✗	✗	✗	✗	✗	
wan1	✗	✗	✗	✗	✗	✗	✗	✗	✗	

启用抗攻击功能，并开启抗 SYN Flood 攻击选项，设置 SYN 包速率阈值为 10pps（小于实际攻击端的发包速率）。

抗攻击设置

启用抗攻击 ☒

☒ 抗 SYN Flood攻击
SYN包速率阈值: 10 个包/秒 (1-65535)

☐ 抗 ICMP Flood攻击
ICMP包速率阈值: 1000 个包/秒 (1-65535)

☐ 抗 Ping of Death 攻击
ICMP包长阈值: 800 字节 (1-65535)

☐ 抗 UDP Flood 攻击
UDP包速率阈值: 1000 个包/秒 (1-65535)

☐ 抗 PING SWEEP攻击
每 10 毫秒10个不同IP的ICMP包 (1-65535)

☐ 抗 TCP 端口扫描
每 10 毫秒同一IP的10个不同端口的 TCP 包 (1-65535)

☐ 抗 UDP 端口扫描
每 10 毫秒同一IP的10个不同端口的 UDP 包 (1-65535)

☐ 抗松散源路由攻击

☐ 抗严格源路由攻击

☐ 抗 WinNuke 攻击

☐ 抗 smurf 攻击

☒ 抗 TCP 无标记攻击

☒ 抗圣诞树攻击

☒ 抗 SYN & FIN 位设置攻击

☒ 抗无确认 FIN 攻击

☐ 抗 IP 安全选项攻击

☐ 抗 IP 记录路由攻击

☐ 抗 IP 流攻击

☐ 抗 IP 时间戳攻击

☐ 抗 Land 攻击

☐ 抗 teardrop 攻击

确定

全选

取消

第六步：验证测试

在外部 PC 上使用 SYN Flood 工具再次向 FTP 服务器发起攻击。此时在 FTP 服务器上通过 Windows 命令 netstat -an 可以看到外部主机与 FTP 服务器的 21 端口只建立了少量的半开放连接（大约 10 个），其他所有的 SYN Flood 攻击报文已经被防火墙阻断。

```

C:\WINDOWS\system32\cmd.exe
TCP    127.0.0.1:43958      127.0.0.1:3904      TIME_WAIT
TCP    192.168.1.10:21     1.1.1.3:1024        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.4:1025        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.5:1026        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.6:1027        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.7:1028        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.8:1029        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.9:1030        SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.10:1031       SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.11:1032       SYN_RECEIVED
TCP    192.168.1.10:21     1.1.1.12:1033       SYN_RECEIVED
TCP    192.168.1.10:139    0.0.0.0:0           LISTENING
UDP    0.0.0.0:445         *:*:
UDP    0.0.0.0:500         *:*:
UDP    0.0.0.0:4500        *:*:
UDP    127.0.0.1:123       *:*:
UDP    127.0.0.1:1025      *:*:
UDP    127.0.0.1:1052      *:*:
UDP    127.0.0.1:1900      *:*:
UDP    192.168.1.10:123    *:*:
UDP    192.168.1.10:137    *:*:
UDP    192.168.1.10:138    *:*:
UDP    192.168.1.10:1900   *:*:
C:\Documents and Settings\Administrator>

```

【注意事项】

- 设置的防火墙 SYN Flood 检测阈值 (SYN 包速率) 要小于实际攻击端的发包速率。
- 防火墙是根据 SYN 报文速率对 SYN Flood 攻击进行检测, 所以防火墙在接收报文时会有采样的时间, 这段时间内部分攻击报文可能会通过防火墙, 在目的端造成少量的半连接。
- 检测阈值不要设置的过小, 这样可能导致正常的连接请求无法建立。