SecPath防火墙WEB和邮件过滤的配置

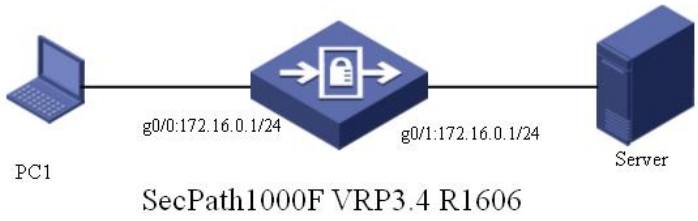
巫继雨 2006-08-31 发表

SecPath防火墙WEB和邮件过滤的配置

一、组网需求

用一台防火墙连接两台PC，PC1模拟局域网（内网）用户，PC2模拟Internet（外网）上的Server。在PC2上开启Web和邮件服务，使PC1可以访问Web服务器上的网页和发送邮件。

二、网络拓扑



三、配置步骤

//定义ASPF策略1，并进入该ASPF策略视图

[SecPath1000F]aspf-policy 1

[SecPath1000F-aspf-policy-1]detect http *//配置检测http协议*

[SecPath1000F-aspf-policy-1]detect smtp *//配置检测smtp协议*

[SecPath1000F-aspf-policy-1]detect tcp *//配置检测tcp协议*

[SecPath1000F-aspf-policy-1]quit

[SecPath1000F]acl number 2001

//配置需要进行NAT转换的IP地址范围

[SecPath1000F-acl-basic-2001]rule permit source 172.16.0.0 0.0.0.255

[SecPath1000F]interface GigabitEthernet 0/0 *//进入连接PC的接口视图*

[SecPath1000F-GigabitEthernet0/0]ip address 172.16.0.1 24

[SecPath1000F-GigabitEthernet0/0]quit

[SecPath1000F]interface GigabitEthernet 0/1 *//进入连接Server的接口视图*

[SecPath1000F-GigabitEthernet0/1]ip address 192.168.100.1 24

//对接口的出方向的报文应用ASPF策略1

[SecPath1000F-GigabitEthernet0/1]firewall aspf 1 outbound

//直接使用该接口的IP地址作为NAT转换后的IP地址，对匹配标准访问控制列表2001的//数据报文的源IP地址进行NAT转换

[SecPath1000F-GigabitEthernet0/1]nat outbound 2001 [SecPath1000F-GigabitEthernet0/1]quit

//设置防火墙缺省过滤规则为允许

[SecPath1000F]firewall packet-filter default permit

[SecPath1000F]firewall zone trust

[SecPath1000F-zone-trust]add interface GigabitEthernet 0/0

[SecPath1000F]firewall zone untrust

[SecPath1000F-zone-untrust]add interface GigabitEthernet 0/1

[SecPath1000F]firewall url-filter host enable *//使能Web地址过滤功能*

//添加拒绝访问www.sohu.com的过滤条目

[SecPath1000F]firewall url-filter host add deny www.sohu.com

[SecPath1000F]firewall webdata-filter enable *//使能Web内容过滤功能*

//添加拒绝访问含有以hello开头的字符串的网页的过滤条目

[SecPath1000F]firewall webdata-filter add ^hello

[SecPath1000F]firewall smtp-filter rcptto enable *//使能邮件地址过滤功能*

[SecPath1000F]firewall smtp-filter rcptto add deny *@hotmail.com

//添加拒绝收件人地址为hotmail.com域中的所有地址"@hotmail.com"的过滤条目*

[SecPath1000F]firewall smtp-filter subject enable *//使能邮件主题过滤功能*

//添加邮件主题中含有字符串lover的过滤条目

[SecPath1000F]firewall smtp-filter subject add lover

[SecPath1000F]firewall smtp-filter content enable *//使能邮件内容过滤功能*

//添加拒绝邮件中含有字符串virus的过滤条目

[SecPath1000F]firewall smtp-filter content add virus

[SecPath1000F]firewall smtp-filter attach enable *//使能邮件附件过滤功能*

//添加附件文件扩展名为exe的过滤条目

[SecPath1000F]firewall smtp-filter attach add *.exe

四、配置要点

1，配置aspf策略，使能检测http、smtp和tcp；

2，使能URL过滤、使能SMTP过滤；

3，设置过滤内容。

五、验证结果

1．PC1无法访问Server上Url地址为www.sohu.com的网页，在防火墙上显示Url地址过滤条目被匹配的次数如下所示：

[SecPath1000F]display firewall url-filter host item-all

SN	Match-Times	Keywords
1	1	<deny>www.sohu.com

2．PC1无法访问Server上网页内容中含有以hello开头的字符串的网页，在防火墙上显示网页内容过滤条目被匹配的次数如下所示：

[SecPath1000F]display firewall webdata-filter item-all

SN	Match-Times	Keywords
1	1	^hello

3．PC1无法发送邮件收件人地址域后缀为@hotmail.com的邮件，在防火墙上显示邮件收件人地址过滤条目被匹配的次数如下所示：

[SecPath1000F]display firewall smtp-filter rcptto item-all

SN	Match-Times	Keywords
1	1	<deny>*@hotmail.com

4．PC1无法发送邮件主题中含有字符串lover的邮件，在防火墙上显示邮件主题过滤条目被匹配的次数如下所示：

[SecPath1000F]display firewall smtp-filter subject item-all

SN	Match-Times	Keywords
1	1	lover

5．PC1无法发送邮件内容中含有字符串virus的邮件，在防火墙上显示邮件内容过滤条目被匹配的次数如下所示：

[SecPath1000F]display firewall smtp-filter content item-all

SN	Match-Times	Keywords
1	1	virus

6．PC1无法发送邮件内容中含有字符串virus的邮件，在防火墙上显示邮件附件文件名过滤条目被匹配的次数如下所示：

[Firewall]display firewall smtp-filter attach item-all

SN	Match-Times	Keywords
1	1	*.exe