商务领航2-2 防病毒典型配置

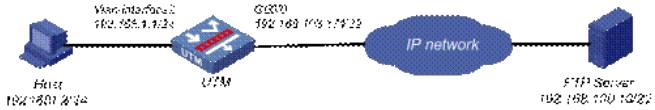
郑雅敏 2009-06-24 发表

商务领航2-2 防病毒典型配置

一、 组网需求：

某公司的内网网段为192.168.1.0/24。内网用户Host主机连接到UTM的GE0/3接口上，通过DHCP自动获取到IP地址为192.168.1.2/24，在UTM上配置防病毒策略，阻止公司内部的用户通过FTP向外网上传病毒， 或者通过邮件附件向外发送病毒。（注：B2-2默认防病毒策略已经开启，此案例前提是取消默认的IPS和AV策略，重新创建新的防病毒策略。）

二、 组网图：



三、 配置步骤：

1. 基本配置

1.1配置WAN接口GE0/0地址

在左侧导航栏中点击“接口配置 > WAN接口设置”，配置GE0/0，连接模式选择“手动指定IP地址”，IP地址输入“192.168.103.171”，子网掩码为“22”，网关地址为“192.168.100.254”，DNS1为“10.72.66.36”，DNS2为“10.72.66.37”，然后点击<应用>按钮完成配置。

在左侧导航栏中点击“接口配置 > 高级设置”，查看当前接口配置结果：

名称	IP地址	网络掩码	安全域	状态	操作
GigabitEthernet0/0	192.168.103.171	255.255.252.0	Untrust		
GigabitEthernet0/1			Untrust		
GigabitEthernet0/2			Trust		
GigabitEthernet0/3			Trust		
GigabitEthernet0/4			Trust		
NULL0			-		
Vlan-interface1	192.168.2.1	255.255.255.0	Trust		
Vlan-interface2	192.168.1.1	255.255.255.0	Trust		

1.2 引流策略

配置将Trust和Untrust之间匹配ACL 3901的流量都引到段31上。

源域	目的域	段ID	访问控制列表ID	操作
Untrust	Trust	31	3901	
Trust	Untrust	31	3901	

2. 防病毒策略的主要配置步骤（非默认防病毒策略）

点击导航栏“IPS | AV | 应用控制 > 高级设置”，点击“应用安全策略”，进入深度检测页面。

2.1创建防病毒策略

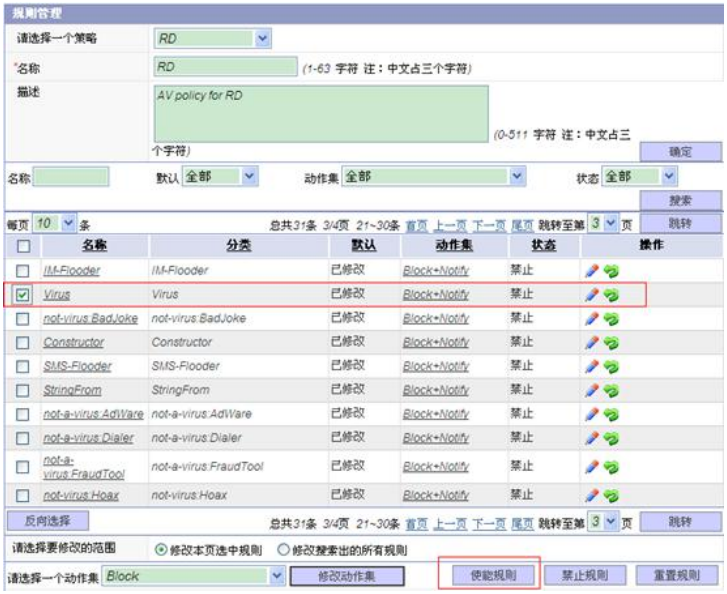
选择“防病毒 > 策略管理”，进入防病毒策略的显示页面。

单击<创建策略>按钮，进入创建防病毒策略的配置页面，输入策略名称为“RD”，输入描述为“AV policy for RD”，选择从指定策略拷贝规则为“Anti-Virus Policy”，单击<确定>按钮完成操作。

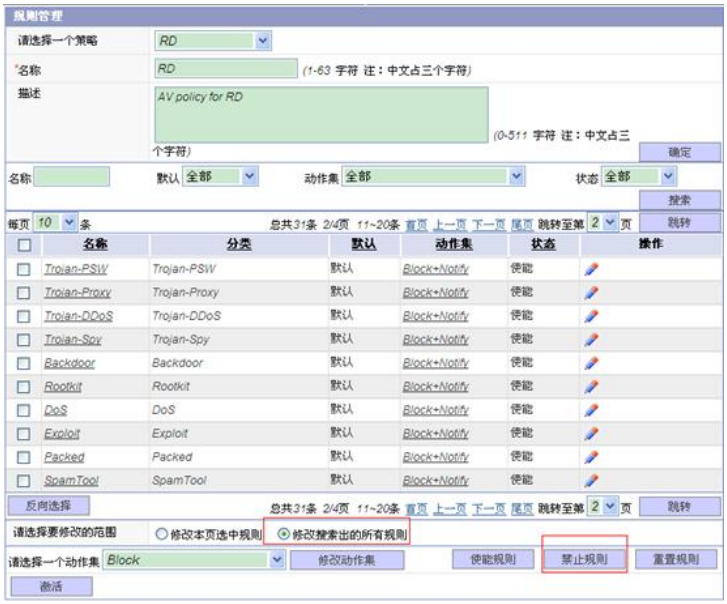
2.2配置防病毒规则

完成策略配置后，页面跳转到“防病毒 > 规则管理”的页面，策略已默认选择为“RD”，可以进行如下配置：

1) 选中“修改搜索出的所有规则”，单击<禁止规则>按钮,禁止所有规则。



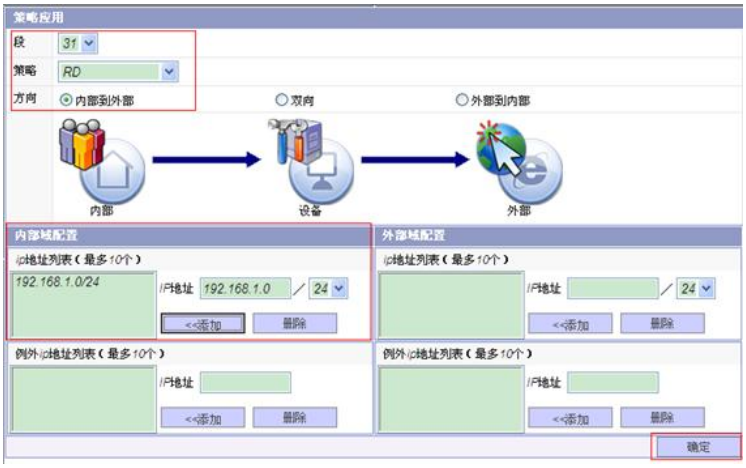
2) 选中规则“Virus”前的复选框，点击<使能规则>。



2.3 应用防病毒策略到段上

选择“防病毒 > 段策略管理”，单击<新建段策略>按钮。

在应用策略页面进行如下配置：选择要关联的段为“31”，选择策略为“RD”，选择方向为“内部到外部”，在内部域IP地址列表中添加IP地址为“192.168.1.0/24”， 单击<确定>按钮完成操作。



2.4 激活配置

完成上述的配置后，页面跳转到段策略的显示页面。单击<激活>按钮，弹出确认对话框。在确认对话框中单击<确定>按钮后，将配置激活。

四、验证结果

首先用户需要自制一个用于测试的eicar病毒，方法如下：

打开“记事本”，将下面一行文本拷贝进去，保存文件，文件类型选择“所有文件”，并把文件命名为“EICAR.COM”。

“X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*---------”

完成以上步骤以后，产生的文件应该有68或70个字节长.，然后再把EICAR.COM文件打包成后面测试用到的文件eicar.rar。eicar病毒是标准防病毒测试文件，由EICAR组织和全球反病毒公司共同推出的用于测试防病毒产品防毒功能的测试文件。

用户登录位于外网的IP地址为192.168.100.10的FTP服务器，上传eicar,rar文件，上传失败，选择“日志管理 > 病毒日志 > 最近日志”界面，可以看到产生的阻断日志。

用户收发邮件的服务器为位于外网的IP地址为192.168.100.240邮件服务器，用户向外发送带有附件为eicar.rar的邮件时，发送失败，选择“日志管理 > 病毒日志 > 最近日志”界面，可以看到产生的阻断日志。

四、配置关键点及注意事项：

(1) 主要配置步骤中的配置是在“应用安全策略”界面进行的。

(2) 已经应用到段上的防病毒策略不能删除。

(3) 系统预定义的防病毒策略和规则不能删除。

(4) 一个报文在一个段上只能匹配一条防病毒段策略。当一个段上应用了多个防病毒策略，则系统在对报文进行匹配时，会根据段策略中指定的IP地址范围的精确程度，越精确的（即IP地址范围越小的）段策略越优先匹配；当有多个段策略的IP地址范围精确程度相同时，则先配置的段策略优先匹配。