SecPath UTM流日志的典型配置

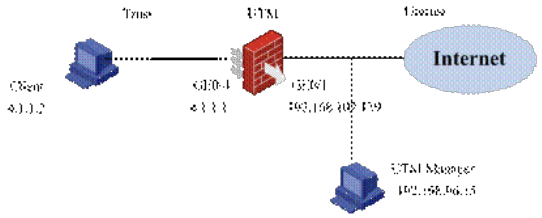
万欣 2009-06-07 发表

SecPath UTM流日志的典型配置

一．组网需求

内部用户Client（4.1.1.2）连接在UTM的GE0/4接口上，通过UTM设备访问外部网络。UTM上配置流日志功能，发送到安装有UTM Manager的远端集中网管192.168.96.15进行详细的分析和统计。

二．组网图

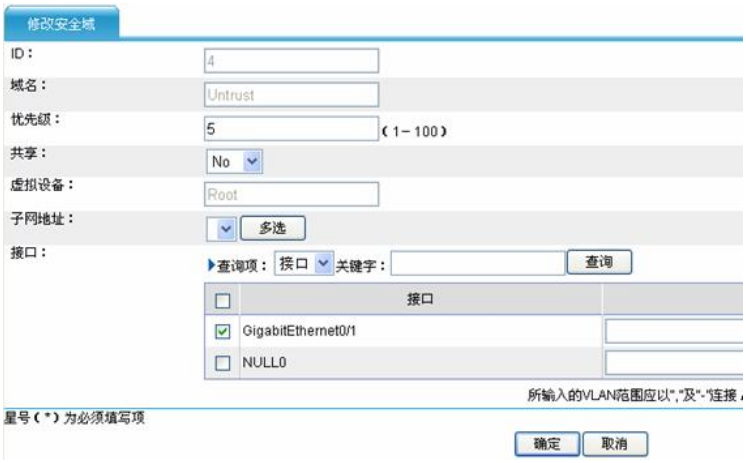


三．配置步骤

1.配置接口GE0/1

在左侧导航栏中点击“设备管理 > 接口管理”，点击GE0/1栏中的 按钮，进入“接口编辑”界面。按照下图设置接口GE0/1，然后点击< 确定 >按钮完成配置。

点击左侧导航栏“设备管理 > 安全域”，点击Untrust栏中的 按钮，进入“修改安全域”界面。按照下图将接口GE0/1加入Untrust域，点击< 确定 >按钮 返回“安全域”界面。



2.配置接口GE0/4

同样配置接口GE0/4的IP地址为4.1.1.1/24，加入到安全域Trust。在“设备管理 > 接口管理”中看到配置

完成后的界面：

名称	IP地址	网络掩码	安全域	状态
GigabitEthernet0/0			Untrust	
GigabitEthernet0/1	192.168.102.139	255.255.252.0	Untrust	
GigabitEthernet0/2			Trust	
GigabitEthernet0/3			-	
GigabitEthernet0/4	4.1.1.1	255.255.255.0	Trust	
GigabitEthernet0/5			-	
NULL0			-	

3.NAT配置

为了使内部的主机能够通过UTM连接到外网，需在GE0/1接口上配置NAT 策略，这里配置ACL3004，地址转换方式为“Easy IP”。
点击“防火墙 > ACL”，新建ID为3004的ACL，在其中添加规则，定义需要配置的流量。该例中允许源地址为4.1.1.0/24的报文通过。见下图：

点击“防火墙 > NAT > 动态地址转换”，在“地址转换关联”页签下点击< 新建 >，进行如下配置。

4.路由配置

点击“网络管理 > 路由管理 > 静态路由”，配置静态默认路由，下一跳地址192.168.100.254为外网中的路由器与GE0/1在同一个网段的接口地址。

目的IP地址	掩码	协议	优先级	下一跳	接口
0.0.0.0	0.0.0.0	Static	60	192.168.100.254	GigabitEthernet0/2

5.引流策略

配置将流量引进I-ware平台，以进行深度分析的配置。将Trust和Untrust之间匹配ACL 3000的流量都引到段0上。
首先配置ACL，点击“防火墙 > ACL”，新建ID为3000的ACL，在其中添加规则，定义需要配置的流量。如下图：

再点击“IPS | AV | 应用控制 > 高级设置”，新建引流策略，将ACL3000的流量引到段0上。

6.启用SNMP代理功能

[U200S] snmp-agent
[U200S] snmp-agent sys-info version all
[U200S] snmp-agent community read public
[U200S] snmp-agent community write private

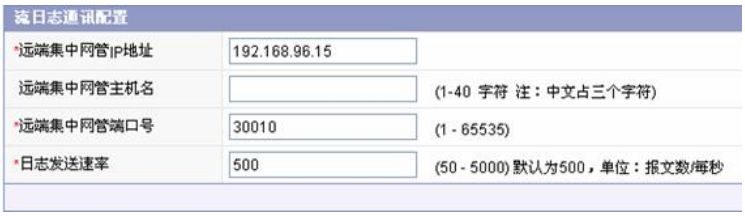
7.进入“应用安全策略”界面

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。

8.UTM配置流日志功能

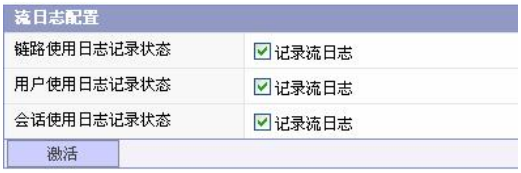
（1）配置通讯参数

在导航栏选择“日志管理 > 流日志 > 通讯配置”，进入通讯参数的配置页面，如下图，可以设置远端网管IP地址，端口号和发送速率。



（2）流日志配置

在导航栏中选择“日志管理 > 流日志 > 流日志配置”，进入流日志的配置页面，如下图。选择复选框后，点击< 确定 >，并点击< 激活 >，使配置生效。



其中，链路使用日志记录对整个链路上各种服务的流量，用户使用日志按用户对各种服务的流量进行记录，会话使用日志按会话对指定服务的流量进行记录。一般开启链路使用日志和用户使用即可。

要实现“会话使用日志记录”功能还需要先在“带宽管理 > 服务管理”中将要统计的服务开启记录日志功能。

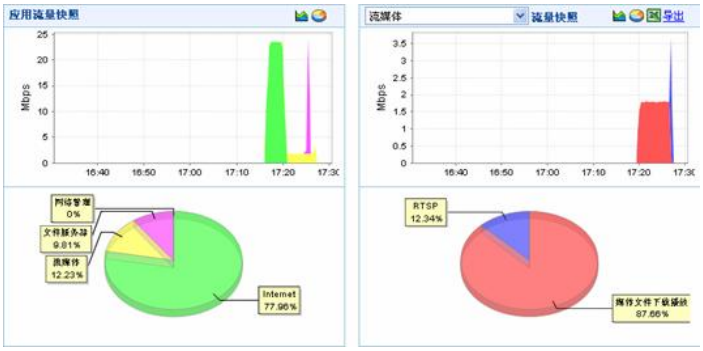
9.SecCenter添加UTM设备

在SecCenter界面，选择“系统管理 > 设备管理 > 设备列表 > 添加设备”界面，“设备主机名或IP地址”为UTM对外的接口IP地址，如果UTM的系统时区为UTC，则“时间矫正”选择“以格林威治时钟处理”，输入设备标签，其他选项采用默认配置即可。

四．验证结果

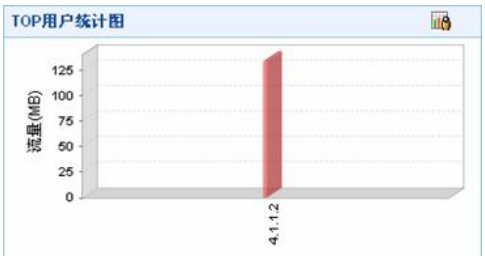
主机通过设备进行HTTP浏览，FTP下载等应用，查看SecCenter，在“带宽管理 > 网络流量快照”，可以看到对经过该设备的流量的统计分析。

（1）网络流量快照：



（2）业务流量分析：

（3）用户业务分析：



五．配置注意事项

目前只有U200-A、U200-M、U200-CA设备支持流日志。