SecPath UTM的IPS典型配置

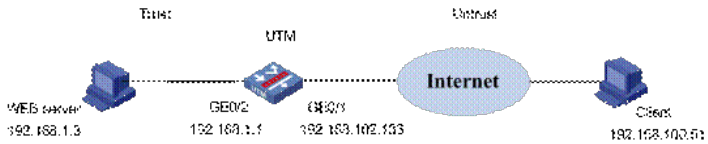
万欣 2009-06-06 发表

SecPath UTM的IPS典型配置

一．组网需求

某公司的内网网段为192.168.1.0/24，外网网段为192.168.100.0/22。内网作为Web Server的主机192.168.1.3连接到UTM的GE0/2接口上，在UTM上配置IPS策略，阻止外部网络中的PC向内部服务器发起攻击。

二．组网图



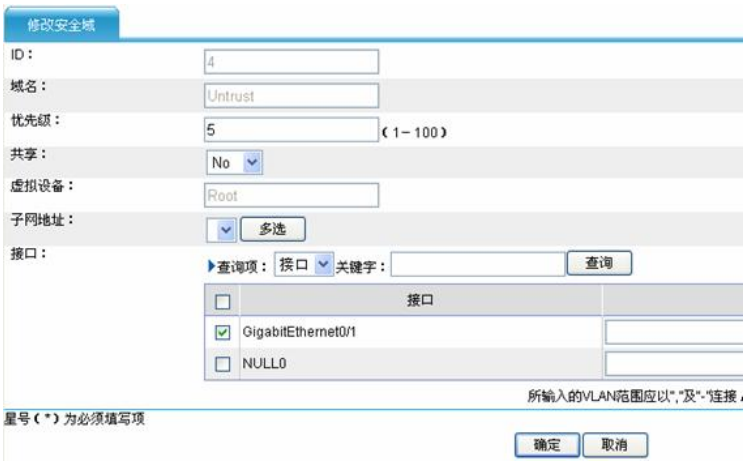
三．配置步骤

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。

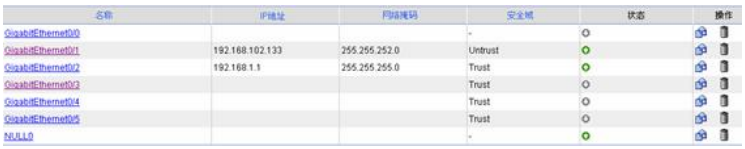
2.将接口加入安全域

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Trust域，点击< 确定 >按钮 返回“安全域”界面。



3．同理，配置接口GE0/2并加入安全域

同样配置接口GE0/2的IP地址为192.168.1.1/24，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：



4．配置NAT Server

在该例中需要配置NAT Server，以给内部Web服务器192.168.1.3一个从外部可以访问的地址192.168.102.132。点击导航栏“防火墙 > NAT > 内部服务器”，在“内部服务器转换”页签下点击< 新建 >，进行如下配置：

在“新建内部服务器”中，选择接口为GE0/1，协议类型为TCP，外部IP地址为192.168.102.132，内部IP地址为：192.168.1.3，外部和内部端口均为80。如下图所示：

5．域间策略

配置允许Untrust域访问Trust域的内部Web服务器。点击导航栏“防火墙 > 安全策略 > 域间策略”，点击< 新建 >，配置源域为Untrust，目的域为Trust；源IP地址为任意地址，目的IP地址为192.168.1.0/24网段，动作为允许，如下图：

6．引流策略

将Trust和Untrust之间匹配ACL 3000的流量都引到段0上。

首先需配置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。

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．创建IPS策略

点击“IPS > 策略管理”，进入IPS策略的显示页面。

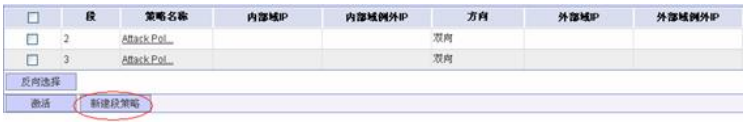
单击< 创建策略 >按钮，进入创建IPS策略的配置页面，输入策略名称为“IPS enable”，输入描述为“IPS enable all”，选择从指定策略拷贝规则为默认策略“Attack Policy”，单击< 确定 >按钮完成操作。

9．配置IPS规则

完成上一步策略配置后，页面跳转到“IPS > 规则管理”的页面，策略已默认选择为“IPS enable”，进行如下配置：选中“修改搜索出的所有规则”，单击< 使能规则 >按 钮。

10．应用IPS策略到段上

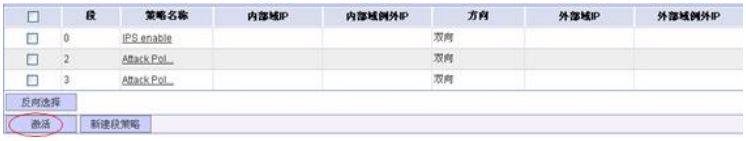
选择“IPS > 段策略管理”，单击< 新建段策略 >按钮。



在应用策略页面进行如下配置：选择要关联的段为“0”，选择策略为“IPS enable”，选择方向为“双向”， 单击< 确定 >按钮完成操作。

11．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

首先作为攻击方的外部PC需要安装一个软件X-Scan v3.3，该软件可以用来扫描目标机的端口。
X-Scan常用的扫描工具，采用多线程方式对指定IP地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。
外网用户（192.168.100.51）开启X-Scan，扫描目的主机：192.168.102.132。
选择“日志管理 >攻击日志 > 最近日志”界面，可以看到产生的阻断日志。