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。

接口编辑	
接口名称:	GigabitEthernet0/1
接口类型:	不设置 🕑
VID:	
MTU :	1500 (46-1500,缺省值=1500)
TCP MSS :	1460 (128-2048,缺省值=1460)
工作模式:	 ○ 二层模式 ③ 三层模式
IP配置:	○无IP配置 ●静态地址 ○DHCP ○BOOTP ○PPP协商 ○借用地址
IP地址:	192.168.102.139
网络掩码:	22 (255.255.252.0)
其他接口:	GigabitEthernet0/0 🖌
	确定返回

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。

ID :	4	
域名:	Untrust	
忧先级:	5 (1-100)	
共享:	No 🗸	
虚拟设备:	Root	
子网地址:	· ● 多选	
接口:	▶查询项: 接口 ¥ 关键字:	查询
	日 接口	
	GigabitEthernet0/1	
	NULL0	
		所输入的VLAN范围应以"."及"-"连邦

2.配置接口GE0/4

完成后的界面:

SW	iPtaté	阿结接码	安全城	状态
GigabitEthernet0/0			Untrust	0
GigabitEthernet0/1	192.168.102.139	255.255.252.0	Untrust	0
GigabitEthernet0/2			Trust	0
GigabitEthernet0/3				0
GigabitEthernet0/4	4.1.1.1	255,255,255.0	Trust	0
GigabitEthernet0/5				0
NULLO				0

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:

規則ID	操作	墓述	时间段
	permit	ip source 4.1.1.0 0.0.0.255	无限制

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。

	接口	ACL	地址油索引	地址种族方式	关联的VRRP编
GigabitEthernet0	W8	3004	0.00000000000	Easy IP	

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/P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:

規則D	操作	業法	时间段
	permit	ip source 4.1.1.0 0.0.0.255	无限制
	permit	ip destination 4.1.1.0 0.0.0.255	无限制

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。

遺城: All zones 🌱 目的地	t: All zones 💙 🧕 査询			
調味	目的地	Rio	の何控制列表の	読作
Trust	Untrust	0	3000	(P) 0
Untrust	Trust	0	3000	(P)

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。

流日志通讯配置		
*远端集中网管IP地址	192.168.96.15	
远端集中网管主机名		(1-40 字符 注:中文占三个字符)
远端集中网管端口号	30010	(1 - 65535)
日志发送速率	500	(50-5000) 默认为500,单位:报文数/每秒

(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。

流日志配置	
链路使用日志记录状态	☑ 记录流日志
用户使用日志记录状态	🗹 记录流日志
会话使用日志记录状态	🗹 记录流日志
激活	

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

添加服务 摄除服务	11 11 11 11 11 11 11 11 11 11 11 11 11				
E Default	*服务名	Default	(1-256	字符 注:中文占三个字	将)
■游戏软件	描述	Default Service	0	(0-511 学符	注:中文占三个字符)
◎ 语首软件 ◎ 即天软件	计数器	Default Court	ter	~	
■网络管理 → ☆ # 80 / 88	会话使用日志标志	□ 记录日志	回应用到其所有子	服务	
三义件旅方器 国路由	在服务树中拖曳服务可修改多	之服务			
Ⅲ流媒体		协议		服务器地址	发起方向
€P2P	100-100				

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。

n x		
хш		
没么士却么实TD抽开。	192 168 102 139	
设备标签:	U200-CA	
区域:	未知区域 ▼	
时间矫正:	以格林威治时钟处理 🗸	
④ 使用访问模板	缺省模板 🖌	
○ 指定访问参数	设备访问参数	
	SNMP团体子:	
	设备Web管理用户名:	
	设备Web管理密码:	
	设备Web管理密码: 设备Web端口号:	
	设备Web管理密码: 设备Web端口号: 设备teinet用户名:	

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。