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。

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 ◎ 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:	192.168.102.133
网络掩码:	22 (255.255.252.0)
其他接口:	GigabitEthemet0/0 💌
	确定 返回

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。

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

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:

58	IPittate	网络视网	安全城	状态		操作
GigabitEthemet0/0				0	1	0
GigabitEthernet0/1	192.168.102.133	255.255.252.0	Untrust	0	1	1
GigabitEthemet0/2	192.168.1.1	255.255.255.0	Trust	0	1	0
OlgabitEthemet0/3			Trust	0	1	1
GigabitEthernet0/4			Trust	0	100	1
GigabitEthemet0/5			Trust	0	1	1
NULLO				0	6	8

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:

	VPN索例	外部P地址	外雷藏口	内部IP地址	内部端口	物议类型	关联的VRRP组	論
				-				
ISMAR								
and a state of the		AL MILLION			N DENKITS		14.70 m 84	
			HE 197		27 DENNEL -		23 PLX 64-122	

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I P地址为:192.168.1.3,外部和内部端口均为80。如下图所示:

接口:	GigabitEthernet0/1 💌	
VPN实例:	~	
协议类型:	6(TCP)	
外部IP地址		
●指定IP地址:	192.168.102.132	
○ 使用接口的IP地址:	当前接口 🖌	
外部端口:	 80 	0-65535,0表示任意端口)
	0	(1- 65535
内部IP地址:	192.168.1.3	
	l H	
内部端口:	80 0-6	5535,0表示任意端口)
□ 価約\/PPP关联	关联的VRRP组:	(1-255)

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:

修改访问控制列表规则		
源域	Untrust	
目的域	Trust	
规则ID	0	
描述	(1-31字符)	
VPN实例	×	
源IP地址		
○新建IP地址	1	*IP地址通配符需要面
 · 源IP地址 	any_address 🛛 🖌 多选	
目的IP地址		
○新建IP地址		*IP地址通配符需要前
●目的IP地址	192.168.1.0/0.0.0.255 🖌 多选	
服务		
名称	any_service 💙 多选	• 毎- 甘北
过滤动作	Permit 🛩	• 过滤
时间段	~	
□启用MAC匹配		
开启Syslog日志功能 🗌	启用规则 🗹	
星号(*)为必须填写项	Ĩ	确定 取消

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:

規則D	操作	描述	时间段	操作
	permit	ip source 192 168 1 0 0 0 0 255	无限制	0
	permit	ip destination 192.168.1.0 0.0.0.255	无限制	1

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。

遺紙: All zones 🎽 目的地	t: All zones 💙 🧕 査询			
an	目的地	Ro	の何控制列表の	読作
Trust	Untrust	0	3000	(P) 🗊
Untrust	Trust	0	3000	(P)

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。

应用安全预略				
在应用安全策略配置中	,您可以配置详细的AVIPS-URL过滤、	Anti-spam策略,	并对IMP2P等上百种应用软件进行控制和审计。	并提供详细的日志信息。
• 应用安全策略				
-				

8. 创建IPS策略

点击"IPS > 策略管理",进入IPS策略的显示页面。

毎页 25	**	息共1条 1/	1页 1~1条 首页上一页下一页 尾页 统转至第 1 😪页
	名称	篇述	操作
13	Mattack Policy	Attack Policy	2 🕤 👄
反向	念择	息共1条 1/	1页 1~1条 首页上一页下一页尾页 跳转至第 1 💌页
谢.	舌 位證兼唱		

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"IP S 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。

策略因型	双击防护策略			
名称	IPS enable	(1-63 字符 注:中文占三个字符)		
単述	IPS enable all		(0-511 芋将 径:中文占三个芋将)	
从指定前临终员规则	Attack Policy			

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。

请选择	一个动作和	R Block	✓ 修改助	作果			(使能想	R则) 禁止规则
诸法邦	業要修改的	46.00	○修改本页迭中規則 ④ 的	改養素出的所有	規則		~	
反共	制造择				息共2	2530条 1/102页 1	~25条 首页 上一页 下一页	鳳页 跳转至第 1 💌
	150999	086 Tencent G Remote B	G: VQQPLAYER.OCX.ActiveX uffer Overflow	Vulnerability	Major	默认	Permit+Notify	禁止
	150999	1085 Microsoft Office Works Converter: Stack- based Buffer Overflow (MS08-011)		Vulnerability	Major	服大议	Permit+Notify	黨止
	150999	081 GlobalLin Buffer Ove	k HanGamePluginCn18 dll ActiveX rflow	Vulnerability	Major	数大さん	Block+Notify	使能

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。

	R	策略名称	内部域IP	内部域例外IP	方向	外部域即	外部域例外的
	2	Attack Pol.			观向		
	3	Attack Pol			观向		
反向选	择						
激活	863	8段策略					

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。

	0 💌			
16	IPS enable			
M	〇内部到外部	 	○ 外部到内部	
	1		•	
	内部 211 (第4) 最多10个)	ਲੇਛ	外面 外面地质器 比线处列表(最多10个)	
	印地	± /24 -		IP\$832
		版加 新能</td <td></td> <td>~~添加 最節</td>		~~添加 最節
NPA lot	11120天(最多10个)		例外10地址列表(最多10个)	添加 単時
NEPH ID H	地达列表(最多10个) 印故	<<添加。	例外由地址则表《最多10个》	<<約22 <= #### #P\$&注 <<= #222 ####

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。

	R	策略名称	内部域IP	内部域例外IP	方向	外部域IP	外部域例外IP
	0	IPS enable			双向		
	2	Attack Pol			双向		
	3	Attack Pol			双向		
反何法	14) #68	- 段 兼略					

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。

	攻击印	时间数	攻击名称	段	方良	RP	LIMP	教端口	日的場	的収束	10月10	<u>命中次</u>	洲	Packet Trace
t	151001629	2009-05-19 15:50:12	Apache for Win32, bat/ cmd File Remote Command Execution Vulnerability	0	从外到 里	192 168 100 51	192.168.1.3	2308	80	TCP	HTTP (TCP)	16	-	
2	151001629	2009-05-19 15:50:12	Apache for Win32_ball cmd File Remote Command Execution Vulnerability	0	从外到 里	192.168.100.51	192.168.1.3	2308	80	тср	HTTP (TCP)	1	-1	
3	151001658	2009-05-19 15:50:08	AWStats Remote Command Execution Vulnerability	0	从外到 里	192.168.100.51	192.168.1.3	2251	80	TCP	HTTP (TCP)	19	-#2	
4	151001658	2009-05-19 15:50:08	AVVStats Remote Command Execution Vulnerability	0	从外到里	192.168.100.51	192.168.1.3	2251	80	TCP	HTTP (TCP)	1		
5	151000039	2009-05-19 15:49:38	Multiple Vendor WEB-INF Directory Contents Disclosure Vulnerability	0	从外到 里	192.168.100.51	192,168.1.3	2049	80	TCP	HTTP (TCP)	1		
6	151001630	2009-05-19 15:49:30	MS00-057 Microsoft IIS Unicode Directory Traversal Vulnerability	0	从外到里	192.168.100.51	192 168 1 3	1808	80	TCP	HTTP (TCP)	1	7 2	
7	151001630	2009-05-19	MS00-057 Microsoft IIS Unicode Directory Traversal Vulnerability	0	从外到里	192.168.100.51	192.168.1.3	1808	80	TCP	HTTP	179	₽≇	