郑雅敏 2009-06-24 发表

商务领航2-2 URL过滤典型配置

```
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。在Navigator上配置URL过滤策略和规则,禁止内网用户在上午(8:30~12:00)访问网站www.h3c.com.cn/Training,其它时间可以访问。
```

二、 组网图:



三、 配置步骤:

1. 基本配置

1.1 配置WAN接口GE0/0

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"192.168.102.136",子网掩码为"22",网关地址为"192.168.100.254",然后点击<应用 >按钮完成配置。

WAN接口设置				
配置 WANロ参数 以	连接到 Internet			
WAN D	GigabitEthernet0/0	×		
连接模式	手动指定IP地址	~]	
TCP-MSS	1460		(128-2048,缺省=1460)	
MTU	1500		(46-1500,缺省=1500)	
IP地址	192.168.102.136			
子阿掩码	22 (255.255.252.0)	*		
网关地址	192.168.100.254			
DNS1				
DNS2				
				应用

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	伊地址	Phianesa	安全城	状态	×	新作
GloabitEthernet0/0	192.168.102.136	255 255 252 0	Untrust	0	(P)	0
GigabitEthernet0/1			Untrust	0	1	0
GigabitEthernet0/2			Trust	0	1	1
GigabitEthernet0/3			Trust	0	0	8
GigabitEthernet0/4			Trust	0	100	8
NULLO				0	1	0
Man-Interface2	192.168.1.1	255 255 255 0	Trust	0	100	8
Vlan-Interface1	192.168.2.1	255.255.255.0	Trust	0	1	0

1.2 引流策略

将Trust和Untrust之间匹配ACL 3000的流量都引到段4上。

首先需配置ACL,点击"高级配置 > 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	無比	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4上。

COMPANY OF					
授城: All zones 🐸 目的	et: All zones 🌱 🧕 査词				
200	目的域	RO	訪得控制的原因	1 17	耕作
rust	Untrust	4	3000	60	1
Intrust	Trust	4	3000	1	8

2. URL过滤配置

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。

应用安全策略		
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		

SHEMING

2.1 创建一个时间表"morning"。

在导航栏中选择"系统管理 > 时间表管理",单击<创建时间表>按钮,在创建时间表的页面进行如下配置,在时间表格中选中"周一~周五"的"8:30~12:00"的时间段。

*38	mo	ming			€ 1-63	学程, <	中文占三	个学习)														
騙战										¢ 0-51	宇村,	中文占三	个字符	,									
控制时间	Ê(通	在唐时间	形选择生	效时间	段,望8	包表示生	(放																
0 25	1	2	3	4	5	8	7	B	9.	10	11	12	13	14	15	16	17	18	19	20	21	22	27
6日										T	1.		T										
4=																							
0E																							
10																							
0E																							-
84											1.1												

2.2 配置URL规则及说明

为缺省的URL过滤策略"URL Filter Policy"创建一个规则"h3c"。

在导航栏中选择"URL过滤 > 规则管理",单击<创建规则>按钮,进行如下配置: 输入规则名称为h3c。

选择域名过滤的"固定字符串"前的单选按钮,输入"www.h3c.com.cn"。 选择URL路径过滤的"正则表达式"前的单选按钮,输入"/Training?"。 在时间表中选择"morning",在动作集中选择"Block+Notify"。

無垢	URL Filter Policy				
名称	h3c	(1-256 宇符 8	E:中文占三个字符)		
動き			a.)-256 宇将 注:中支占三个	李符)
机名过滤	 · · ·	王则表达式 帮助			
	www.h3c.com.cn			5-255 李符 往:中文占三个	下字符)
R聯任过總	〇 图定字符串 ④	王则表达式 机助			
	/Training?			5-255 宇狩 注:中文占三个	下字符)
使能状态	⊙ 使能	○禁止			
动作集		时间表		动作集	
	morning	~	Block+Notify	*	
	Ŷ	~	Ŷ	~	
	2	*	Ŷ	~	
	호	~	Ŷ	~	
	Ŷ	*	Ŷ	~	
	~	~	*		

在一条规则中,域名过滤是必须配置的,URI路径过滤可以不配置。设置该规则在不同的时间段内触发 不同的动作集时,若指定的多个时间表中所定义的时间段有重叠,则执行页面上排在最前面的时间表 对应的动作集。

可选的时间表在"系统管理 > 时间表管理"中配置;可选的动作集在"系统管理 > 动作管理"中配置。最多可以配置6个时间表和动作集的组合。

2.3 应用URL策略到段上

在导航栏中选择"URL过滤 > 段策略管理",单击<新建段策略>按钮,进行如下配置。

R	4 💌			
86	URL Filter Policy	*		
5R	③内部到外部	○外部到内部		
	1	→ 🖳 —		
	内部	(代幕)	外部	
内部场面	内部	8 5	外篇 外 面MD2面	
in inclusion localization	内部 (最多10个)	99 10 10 10 10 10 10 10 10 10 10 10 10 10	外面 外面MACT 19曲线列表(最多10个)	
9121415 108812390 192.168	内面 表(最多10个) 1.0/24	校事 学論版: 192 168 1.0 / 24 × +<街加 服除	か第 外国MARE 総社23(K(皇夕10个)) 1社2 	24 ~
時間12155 1928年初 192168 例外には	内部 表(最多10个) 1.0/24 处列表(最多10个)	校委 F988年 152 168 1.0 / 24 (M <<8155 田府	か着 外国MARE	24 💌
PK 12: HS.6 1008: 12: 70 192: 168 PK:9-1008	内部 表(最多10个) 1.0/24 址列表(最多10个)	校委 F98.82 152.168.1.0 / 24 / · · · · · · · · · · · · · · · · · ·	か第 外国MARE 回転址列展(第4510个) 回転址列展(第4510个) PRAL PRAL PRAL PRAL PRAL PRAL	24 *

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。

		段 策略名称	内部城中	内部域例外的	方向	外部域的	外部城例外的	統作
	4	URL Filter	- 内部城/P 1921681.0/24		从重到外		1	1 %
反向遗	择							
in in		BEIRED MINE						

四、验证结果

内网用户 (192.168.1.3) 通过IE浏览器,访问http://www.h3c.com.cn没有问题,但访问http://www.h3c.com.cn/Training,无法显示网页。

选择"系统管理 > 设备管理 > 系统状态"界面,可以看到URL过滤的统计值。

10.00			PS				URLINE	-	
	CPU	٠	•	肥新	L		0	FEINE) 6
1	内存使用率		٠	古智	0			音響	0
	软件映像区使用率		****	1			防病毒		
8	风磨状态			MAGIRIE		0	•	FEIRE	Q
-			1					22	0

四、配置关键点及注意事项:

•

(1) 已经应用到段上的URL过滤策略不能删除。

(2)系统预定义的URL过滤策略和规则不能删除。

 (3) 一个报文在一个段上只能匹配一条URL过滤段策略。当一个段上应用了多个URL过滤策略,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