(m) 防火墙通过安全策略实现过滤HTTPS网站配置方法(WEB界面)

URL过滤 张新姿 2020-11-08 发表

组网及说明

1 配置需求或说明 1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙:如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

注: 本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

防火墙部署在互联网出口,需要实现通过安全策略限制访问www.baidu.com的目的。

2 组网图



配置步骤

1 配置步骤

1.1 防火墙连接互联网配置

上网配置略,请参考《轻轻松松配安全》2.1章节防火墙连接互联网上网配置方法案例。

1.2 开启本地DNS代理

#开启设备本地DNS代理功能,用于解析域名。

HBC s	xPath F100-A-G2
96	« DHSR/H
- VRF	DNS(Domain Name System,城岛系统)是一种用于TCP/IP应用程序的分布式数据库,提供地名与IP地址之间的转换。
B 100	総計器所型 @ IP-4 DNS服用器 ① IP-4 DNS服用器
CE255	VRF SR
DNS	地名服务器地址 114.114.114 🖉
DNS#PIA	地名委用器地址
- DDNS邮户IA	最多可以应责6个ONS服务器。
周极设置	
DP	

1.3 配置安全策略

#在"策略">"安全策略"中点击新建,创建名称为"denybaidu"的安全策略,源安全域为"trust",动作选择 拒绝,目的地址位置点击下拉菜单后点击"添加IPV4地址对象组"。



#新建对象组名为"baidu"的对象组,点击添加按钮。

新建IPv4地址对象组			? ×
对象组6称 bak	u		(1-31字符) (1-127字符)
安全城		×	
🛞 15.10 💼 19.10			
2 ×2	内容	理粉地址	69.6B
	建定	R211	

#对象选择主机名, 输入<u>www.baidu.com</u>点击确定完成配置。



#检查配置无误后点击确认按钮完成配置;

安全策略			?
名称	denybaidu	• (1-127李	符) 🔺
源安全域	Trust	▼ (多选)	
目的安全城	派法样目的安全地	▼ (参选)	
关型	IPv4 ① IPv6		
描述信息		(1-127李符	F)
动作	◎ 允许 ● 拒绝		- 1
源IP地址	请选择或输入对象组	▼ [多选]	
目的IP地址	baidu	▼ [参选]	
服务	请选择服务	▼ [孝选]	
应用	请选择众用	▼ (多选)	_
应用组	清选库点用组	▼ (孝徳)	
用户	派选择但户	~	
101/0102	请选择时间段	~	
VRJF	公開	*	
内容安全			-
1P53RUI0		~	
10.371238.90.45		*	
文件过速照照		~	
防防毒菌的		~	
			*

#在"策略">"安全策略"中继续新建名称为"passany"的安全策略,源安全域为"trust"、目的安全域为"untr ust"、动作选择允许。



1.4 保存配置

							· · · · · · · · · · · · · · · · · · ·
нзс	SecPath F100-A-G2	C		9		an Ref	
	Int Owner Party						****
1.600	DNS (Domain Name S	uncer manage and strategy (c) p	1.00 MO(41	ARA. STORE	TABLE ADAM		
Cas 🖬		a los inclusions		Ind Decision in			
0.016	Reader 1						
	7454	2/8					
C 105	*****	The loss she had			-		
1 Detector		The mediation			100		
CANCER	NUMBER OF T						
0108/198							
- DONTIGE THE	●FTG1品数510A	(田市道,					

1.5 测试结果

使用浏览器打开<u>www.baidu.com</u>,不能正常访问:

- 892-898744, 5 X	🕲 www.baidu.com	× Ø www.baidu.com	X ist www.sina.com.cn	× D stra spirit	x +	- a ×
← → C ② baidu.com						* 0 i
	8					
	T 24					
	7672					
	Webs	Windows Departments Pro- 以下方法: 检查阿德连接 检查代理服务器和防火墙 运行 Windows 网络诊断				
	BR,CO	NNECTION_TIMED_OUT				

(primits m

使用浏览器打开<u>www.alipay.com</u>,可以正常访问:

10053348



查看pc针对百度解析的地址为39.156.66.18:



ject-policy. Src-zone=Trust, Dst-Zone=untrust:If-In=GfgabitEthernet2/0/6(71), If-out=GigabitEthernet2/0/5(70); Pa Cket Info:Src-Pel92.168.2.2, Dst-IP=39.156.66.14, VPN-Instance=none,Src-Port=53187, Dst-Port=443. Protocol=TCF(6). J. Flag=SN. Seq=65486228.
*ug 29 11:24:33:812 2020 H92 ASPF/7/PACKET: -cortext-1: The first packet was dropped by packet filter or object- policy. pr:-conservut, Ds: Toone-untrust; 11:1-mod-gabitethrenet2/06/57(D). Jf:Out=Gabitethernet2/06/57(D): packet Inf0:Src-In=02.168.2, Ds: IP=J9.158.66.14, VPM-Instance-none,Src-Port=5188, DsE-Port=443. Protocol=tCP(6). Fl ag=Svb. seq=219944221.
*ug 29 11:24:1043 2020 H92 ASPF/7/PACKET: -context-1: The first packet was dropped by packet filter or object- policy. pr:-cone-trust, ps: Cone-trust, ps: Ti-mod-gabitterener2/06/SCDJ. if-out-calgabitterener2/06/SCDJ packet Inf0:SFc-IP=02.168.2, bs: IP=J9.156.66.18, VPM-Instance-none.Src-Port=5219, bs: Port=443. Protocol=tCP(6). Fl ag=SVM. seq=112947972.
Lug 29 11:24:38:64 2020 HS ASPF.7/PACKET: -cortext-1: The first packet was dropped by packet filter or object- policy. src-cm=Fust, psc-tone-untrust: Ti-modipalitienternet2/0/6701, J.f.Out-collapitithernet2/0/6701) packet Inf0:src-im-192.168.2, bsc-im-19.156.66.14, VMN-Instance-none,src-Port=5207, bsf-Port=443. Protocol=TCP(6). Fl ag=TW. seg=384847735.

配置关键点