## 🗩 V7 IPS设备旁路做入侵检测设备(IDS)配置举例

IPS防攻击 丁珊 2019-07-26 发表

```
组网及说明
组网图如下:
                        交换机
配置步骤
设备做旁路IDS,从交换机上将流量镜像到设备上,设备仅做检测不做阻断。
交换机上的配置:
#
interface GigabitEthernet1/0/11
port access vlan 2
mirroring-group 1 mirroring-port both
# //镜像端口
#
interface GigabitEthernet1/0/13
port bridge enable
mirroring-group 1 monitor-port
# //镜像的目的端口
#
interface GigabitEthernet1/0/15
port access vlan 2
port bridge enable
# //出接口配置
入侵检测上的配置
#
```

interface GigabitEthernet2/0/13 port link-mode bridge port access vlan 2 //配置接收镜像流量的接口 在这里放通vlan 2 主要是因为交换机上镜像过来的流量不带vlan标签,如果交换机上镜像过来的流量带 有vlan标签,可以选择trunk permit vlan all # bridge 2 blackhole add interface GigabitEthernet2/0/13 //配置黑洞转发 # security-zone name inline import interface GigabitEthernet2/0/13 vlan 2 将接口加入安全域 # security-policy ip rule 5 name inline action pass profile 5\_IPv4 //配置安全策略当中调用default的IPS策略 source-zone inline destination-zone inline

#

## 配置关键点

web界面上的配置:

也可以在web界面上对策略进行配置,示例当中调用的是default策略,现场也可以根据现网需要自行创 建新的策略,如果创建新的策略当中,设置特征筛选条件如果不进行勾选,那么所有的规则都是按照d efault规则的内容执行。

۰

HBC Sect					0	1	•	۲								
90.	· uona			经改变全部增					œ×							
<ul> <li>0 安全NIG</li> </ul>			t in the States in	60.5	inine			-	1				001	1,300.00	0, #	
0156	CANALESE .	20.0.0	THES. OWNERSES.	理论生地	mine			· (#8)								
·策略完全分析	6.0	Reat	BORRM (	目的杂生相	intere			+ 1FB1		103	1993	847.8	7.8	101	89	**
· 30000101	0.5	Any	Any 1	25	# 294	2.4			- 1	55P		408	38.2943	8	-	10
◎ 및 安全防护	🖬 islee	· infere	• inline 1	514.00				(1-127948)		500	IFS: dela.	0	0.008	8	8	
©▲NAT	0.95	Chinat .	• Trust							100	PS:dela.				5	ø
C AFT				12/1	8 ft.07	104										
O & HOWN				189,MACHEL	Any			+ 0F31	- 1							
0000000				BOPRA.	Any			· (#2)								
0.0.000000				8.9	Any			· 1421	- 11							
80 corre				0.78	Any			× 1982	- 11							
- C MARINA				18m	Att			*	- 11							
				10/622	Atv			*	- 11							
				VIU	2.00			*	- 11							
				(PSMM)	orbut.	7092		0	1 II							
				Distantian in the local distance of the loca	ALC: NO		_	-	1							
				27124948	-NONE-											
				0.0400	-NONE-											
				URLIZIEMME	-NONE-			*								
	· · · ·	E.H1E	· NTERR 25 -			82	839								89.1	-18.818

策略当中并不是所有的规则都是启用的,可以在web界面的【对象】-【应用安全】-【入侵防御】-【特征】当中搜索现网攻击特征的关键字,排查这个规则是否启用,未启用的规则是不会产生IPS日志的

HBC %			2	•	E U								
	<ul> <li>Assessed</li> </ul>												
10年8月12月 	O Ref (5.6	C RM 3. BARRING MANNUO, COURSE Q. BR 5. BREN											
	900	W240	APRA.	IL#FR	NAME.	NACH7M	118	7848	10.9	11.0	0.0	ris.	
0 应用安全		0N/,8xA250+95/0808	\$158	Unuidinia	85	0915841	888	28	88	0	0		
9 X-8038	2	GAU_ResA#学校直示规则(Cv0-2014-7187)	\$158	Linustinia	81	AMETON	NO.	78	88	.0			
10000		(MILD-REPUBLIC How have MICHTURE (2014)2008	0.000	Monadoffor	81	817.6	8.19	78	88		0		
	5	(M112-015)(88) Visio Viewer 2020 VID (2)(48)(25)(9)(87)(2)(-2).	00.01	MicrosoftOffice	88	ANETER	8118	78	88		0		
0 0164		(M113-055)#823nternet Eigliner /5/98/F@@(CVI-2012-1148)	2008	Internetlaplacer	84	APRENA	8.10	78	1.0	0	0		
estica •	2	(M14-012)882 Internet Explorer /6/9897388(CVE-2014-0002)	1008	Internetiquese	88	ANECES	810	78	2.0	Θ	0	Θ	
<ul> <li>URLIDIE</li> </ul>		(MELL-RESOLVE MORE)	07074	Medallayer	84	0810801	819	78	5.P		0		
NORS 9		Weekek ENTER DAVERBRUKERE	0.964	Security	81	21110	Nin II	78	68	.0	0	0	
0.00FM	30	MILL-000/Microsoft Informat Explorer Fight 0008/R@precifiet	2058	Internetlighteer	84		88.0	78	8.8		0		
0 9:237F	11	(MIL2-007) WE Internet Deployer DIPTINE MARKET	2008	Internetlaplace	STORN.	******	810		5.0	0	0	Θ	
RIAR	12	(M101-100/882-1+++ 0+) (M069/230-150/1383	0089	MonahOffice	85	DRIVEN/	858.8.	78	88	0	0		
ARRE	10	(MSD-508) IRROFILE face (MSD-59987588	0089	MonahOffice	84	AMETER	8110	78	88				
ACL.	14	(M112-001) #82 Love #108/Fipter#R	otex	24	8.0	encies.	NO.	78	88	0	0		
\$51.	15	(Mil2-00) BR Internet Explorer POLIDER/OPERATI	2008	InternetDiplayer	88	DenRevi	819	78	10	0	0	Θ	
4 公司管理	38	(M10-0H)882 Data Analyzar (manDactions.dl) Active); 8(H208	2058	0.8	88	DRIVEN/	8110	78	5.0		0		
6 A PG	v	MOD-DOBE-EXCER MINIO-THURCREERING	10.08	Internetloplane	81	Make	819		88	0	0	Θ	
	18	MILLOR REPORT CONTRACTOR REPORTS	0.0494	MonahOffice	84	09/5565-0	8110	18	88	0	0		
	20	(MED-017)BBE Lood FirstTable Cache Data Record 809(208/10).	0.089	MicrosoftOffice	84	EMPORING.	1011. R.	78	10		0		
	30	Adulte Reader(Acculat receptager) insulariys/FERMINER	0.000	Addeducted	88	(DercRov)	8/18	78	88	0	0		
	28	Grade NERTH MERCENTER	0.980.9	NO.	81	217.0	8110	78	88	0	0	Θ	
	- 22	(MIL4-121) IBSE Internet Explorer /SIME/EXPLOYE-2014-0120	208	Internetligiour	84	AMETER	810	118	2.0	0	0		