NTA UBA 马永鸿 2020-11-27 发表

纪网及						
	说明					
不涉及						
配置步	骤					
1. (1)	下发服务器配 :配置管理页面]置 面,单击"服	资器管理"链接,	进入服务器管理	里页面	
曝 业务 > ■	2011年2月19日 1月19日 1月1900 1月190000000000000000000000000000					大加入收藏 ⑦蒂助
服务器列	康					
BEF						
共有						
服务器	名称 ♀	服务册IP ♀	描述 ≎	捕获流量日志	配置下发	修改
127.0	0.1	127.0.0.1			v	R
(2)	击修改图标	讲入服务	器配置页面			
 (2) 単 用户行为审 设备信息 	建击修改图标,	进入服务	器配置页面			
 (2) 単 用户行为律 设备信息 选择 	善修改图标,	进入服务	器配置页面	设备P	没售油	đ
 (2) 单 用户行为审 设备信息 选择 未知题符 	建击修改图标, 計 論	进入服务	器配置页面	设备IP	设备运	ć
(2) 单 用户行为律 设备信息 选择 未找强府 来集器信息	单击修改图标, ↔	进入服务	器配置页面	设备IP	2810 2	ž
 (2) 単 用户行为库 设备信息 选择 未找到符 来舞器信息 选择 	2 击修改图标, ↔ 6 5 6 5 6 5 6 5 6 5 6 6 6 6 6 6 6 6 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 7 7 7 7 7 7 7 7 7 7 7 7	进入服务 设备名	器配置页面 *	波藝P 信用時十分析	设备编	适用特殊应用申计
 (2) 単 用户行为非 设备信息 选择 未找误符 来算器信息 送择 ※ 	畫書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書	进入服务 	器配置页面 * ^{兩十名称}	设备IP 信用局卡分析 不自用	说 各部 启用-七层应用 (20) 启用	送 后用He种应用申计 ① Web 『FTP 』 Mail
 (2) 単 用户行为律 设备信息 选择 未地級所 来集藝信息 透择 水場 市内 立た信 	畫書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書	进入服务 读备名 2221	器配置页面 * ^{两+名称}	波音即 启周時+分析 不由用	设备运 尼用七层应用 R 的 启用	适用HHF标应/用申计 WebFTPMail
 (2) 単 用户行为非 设备信息 选择 未按场府 死業時倍的 政策 水場時倍的 水場所 水場時倍的 水場時倍的 水場時倍的 水場時倍的 水場時 水場時倍的 水場時 <li< td=""><td>書击修改图标,</td><td>进入服务 读路名I 2221</td><td>器配置页面 *</td><td> 送倉IP 倉田町1分析 石泉用 </td><td>(第二) (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本</td><td>选 后用HHH和应用申计 WebFTPMail #200</td></li<>	書击修改图标,	进入服务 读路名I 2221	器配置页面 *	 送倉IP 倉田町1分析 石泉用 	(第二) (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本	选 后用HHH和应用申计 WebFTPMail #200
 (2) 単 用户行为非 设备信息 选择 未找场所 采集器信息 透择 水均磁振 小网信息 内网信息 内网信息 	書击修改图标,	进入服务 梁集翻P 2221	器配置页面 *	 设备IP 启用局十分析 不負用 副験 	京市 七 品 加 用 内 的 局 市	送 后用杨殊应用申计 WebFTPMail 2200
 (2) 単 用户行为非 设备信息 选择 未找場所 来集器信息 政理 内网信息 1110/24 	書击修改图标, は 金素(中的20表。 2221 ま	进入服务 線絡部 2221	器配置页面 *	 设备IP 応用時十分析 不良考 副除 ・ 	約日 高田 七日 加田 日日 同日 同日 同日 日日 日日 日日 日日 日日 日日	送 启即杨殊应用申计 () Web () FTP () Mail 2000
(2) 単 用户行方律 设备信息 進择 未找設府 未発表情信 述择 一 大列間直交信 内网面交信 内网面交信 11110/2 ² 2220/2 ²	主書修改图标, は 全集件的记录。 案 案 案 案 案 条 を ま を 、 、 、 、 、 、 、 、 、 、 、 、 、	进入服务 線絡部 2221	器配置页面 *	 设备IP 応用時十分析 不負用 一 一 一 一 一 二 二	約2000 約1月-1日20月11月 1月月 1月月 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日	き 「空田時時私田町計 「Web」FTP Mail 2000

(3)配置服务器参数。

在上图的基本信息中各项均保持默认配置即可。在用户行为审计中的设备信息列表中选中采集器"2.2.2. 1"并启用四类特殊应用监控。内网信息中增加内网用户的三个网段。单击<下发>按钮保存并下发服务 器配置。

2. 增加审计任务

点击"网络流量分析与审计快速配置向导"中"用户行为审计管理"链接,进入自定义行为审计页面,增加 一个用户行为审计任务。

Z _E :	业务 > 配置管理 > 用户行为审计管理					0
	自定义行为审计一览					
	地加 刷研 新学					
	□ 自定文审计名称 ▲	审计服务器	审计类型	审计	修改	删除
	未找到符合条件的记录。					
	共有0条记录,当前第0-0,第1/1页。				« < >	» 50 V

单击<增加>按钮,进入选择审计类型界面。

g _日 业务 > δ3 首提 > 用户行为审计管理 > 选择审计类型
选择审计类型
(通用数+
根据源、目的、端口、协议、应用等信息对用户行为进行审计查询。
 地址转换审计 根据转换期后IP地址如果口等信息对用户的网络行为进行审计和跟踪。
● Web访问审计 对用户Web访问的行为进行审计,重看用户访问的站点、浏览的文件。
文件》 撤审计 对用户FTP文件传输的行为进行审计, 查看用户FTP帐号、上传/下载的文件。
 邮件审计 对用户邮件发送进行审计,查看邮件按件人、收件人和邮件标题。
○ Telnet带计 对用户Telnet行为进行审计, 查看Telnet用户名、执行命令。
下一步 返回

Web 访问审计配置页面

自定义Web访问审计		
自定义审计名称*	web	
审计服务器 *	127.0.0.1	•
任务读者	管理员分组 细产员分组 查看员分组	选择政 官 删除
访问审计条件		
	访问站点	
	标题	
	URI	
审计条件		
	●满足以下所有条件 ○满足以下任一条件	
	2項LP	0
	ERSIP	0
		3
	设备IP	(?)

確定 取消

文件传输审计任务配置页面

加自定义文件传输审计				
自定义审计名称 *	2			
审计服务器 *	127.0.0.1	•	·	
任务读者	管理员分组 维护员分组 查看员分组		选择读者 删除	
件传输审计条件				
	FTP用户名			
	文件名			
	传输方式不	硍		-
本审计条件				
	● 満足以下所有条件	一满足以下任一条件		
	源IP			0
	EASIP			?
	目的端口			(?)
	设备P		\searrow	0

邮件审计任务配置页面

业务 > 配置管理 > 用户行为审	┼管理 > 増加自定义邮件审计		
增加自定义邮件审计			
自定义审计名称 *	3		
审计服务器 *	127.0.0.1		
任务读者	管理员分组 缩2员分组 查看员分组	选择读者 量除	
邮件审计条件			
	发件人		
	收件人		
	主题		
全本审订录件			
		(?)	
		0	
		0	
		0	
		~	
		記: 取消	激活 Windows

Telnet 审计任务配置页面

自定义审计名称 *	4	
审计服务器 *	127.0.0.1	•
任务读者	管理员公组 维护员分组 查看员公组	选择政告 1893
lnet审计条件		
	Telnet 用户名	
	执行命令	
本审计条件		
	●满足以下所有条件 ─ 满足以下任一条件	
) 源ID	0
	EASIP	0
	目的端口	0
	设备IP	0

根据任务类型,完成如下操作:

•根据审计内容, 输入自定义通用审计名称。

•选择设备所属的流量分析服务器,本例中选择127.0.0.1。

•选择查询条件,本例中选中"满足以下所有条件"。

单击<确定>按钮,完成增加审计任务的操作。

3. 验证结果

(1) 查看已创建的任务

完成任务增加后,在左导航树中出现四类审计任务菜单项

ţ	2番配置管理	>
¥	自规检查	>
쒤	智能策略中心	>
٧	/LAN管理	>
A	CL管理	>
v	XLAN管理	>
۷	CFC管理	>
ÿ	治量 分析与审计	~
	制,采集器流量分析任务	>>>
	器 _目 Web访问审计	>>>
	国田 Web访问审计 国田 文件传输审计	>>> >>>
	国 _田 Web访问审计 国 _田 文件传输审计 国 _田 邮件审计	>>> >>> >>>
	물 ₈ Web访问第计 물 ₈ 文件特胎审计 물 ₈ 邮件审计 물 ₈ Telnet第计	>>> >>> >>> >>>
	물 _월 Web访问第计 물 _월 文件特徵第计 물 _월 邮件审计 물 _월 Telnet第计 물 _월 用户行为第计	>>> >>> >>> >>>
	An Web访问审计 An 文件特徴审计 An 邮件审计 An Teinet审计 An Teinet审计 An 用户行为审计 An 流量日志审计	>>> >>> >>> >>>
	Nuebio同审计 Nuebio同审计 Nuebio同审计 Nuebio同审计 End 邮件审计 End 同中行为审计 End 用中行为审计 End 法量日志审计 Numerical 和助行为审计 Set 法重任法	>>> >>> >>> >>>
	B Web访问审计 E 文件传输审计 E 文件传输审计 E 邮件审计 E Telnet审计 E 用户行为审计 E 流量日志审计 S 規環律空间使用 長 数据特徴	>>> >>> >>> >>>
	Image: Second	>>> >>> >>>

分别单击上述四个菜单项,进入相应的审计任务列表。例如,查看Web访问审计任务如图所示。

習目业务 > 配置管理 > 用户行为审计管理					⑦蒂
自定义行为审计一览					
地加 刷新 删除					
白定文审计名称 🔺	审计服务器	审计类型	审计	修改	删除
web	127.0.0.1	Web访问	Π	8	1
共有1条记录,当前第1-1,第1/1页。			4	$\langle \langle 1 \rangle$	» 50 V

数据不会立即产生,请等待一段时间后,点击"Web访问审计"对应的图标,可以查看到审计结果。

户行为通用审计	(提示:如果日志	较大,查询操作可	「能会花要数分钟	或更长时间。)					
查询时间		小时]						
开始时间	202	0-09-23 20:14							
结束时间	202	0-09-23 21:14							
志审计结果:2020	-09-23 20:24:27-2	2020-09-23 21:09	:13						
定利异面							分组	不分组	^
开始时间 ♀	邇IP ≎	EIMIP ≎	源端口 ≎	目的端口 ≎	协议 ≎	应用♀	包数≎	流量 ♀	设备IP ≎
2020-09-23 2	₿. 192.168.111	B. 224.0.0.252	65214	5355	UDP	UDP协议未知	1	79.00 B	2.2.2.1
2020-09-23 2	₿. 192.168.111	B. 224.0.0.252	56218	5355	UDP	UDP协议未知	2	0.15 KB	2.2.2.1
2020-09-23 2	B.1.1.1	B 2.2.2.1	18802	49572	UDP	UDP协议未知	1	0.35 KB	2221
2020-09-23 2	B.1.1.1	B 2.2.2.1	20	38116	тср	ftp-data	5	0.28 KB	2.2.2.1
2020-09-23 2	B. 192.168.111	B. 224.0.0.252	61655	5355	UDP	UDPHING THE	2	0.15 KB	2.2.2.1
2020-09-23 2	B. 192.168.111	B. 224.0.0.252	59969	5355	UDP	UDP协议未知	2	0.15 KB	2221
2020-09-23 2	B. 192.168.111	B. 224.0.0.252	58547	5355	UDP	UDP协议未知	2	0.15 KB	2.2.2.1
2020-09-23 2	B.1.1.1	B. 2.2.2.1	21	59861	тср	FTP	10	0.95 KB	2221
2020-09-23 2	D. 192.168.111	B. 224.0.0.252	59836	5355	UDP	UDP协议未知	2		2221
2020-09-23 2	B. 192.168.111	B. 224.0.0.252	52657	5355	UDP	UDP协议未知	2	REEU T空市川田内又 Wind 0.15.KB	222.1
2020 00 22 2	B. 103100.111	Bankaara	51071	5255	LIDR	LIDP#bi0#TO	2	015 KB	2221

无