第3章

安全接入网关日志 管理与分析

在完成安全接入网关的基本配置和功能设置外,还需要掌握安全接入网关的日志分析。安全接入网关提供用户、管理、系统、ID、详细日志等丰富的日志信息,从而使网关更 好地起到防护效果。

【实验目的】

通过查询日志,全面了解系统运行状态,检索并分析用户业务访问日志,实时监控在 线用户,从而快速定位问题,提高管理的效率与质量。

【知识点】

安全接入网关的日志审查的溯源功能。

【场景描述】

A 公司的安全接入网关设备已投入使用了一段时间,设备的管理人员小王想要通过 查询日志,全面了解系统运行状态,检索并分析用户业务访问日志,实时监控在线用户,从 而快速定位问题,提高管理的效率与质量。请思考小王应如何解决这个问题。

【实验原理】

安全接入网关为管理员提供详细的系统运行状态、用户业务访问日志,并提供在线用 户的监控。针对系统的历史运行状态,管理员可以在"系统报表"一节得到更多的信息。

【实验设备】

安全设备: VPN 1 台。 主机终端: Windows 7 主机 1 台。

【实验拓扑】

实验拓扑如图 3-1 所示。

【实验思路】

(1) 登录安全接入网关的管理员后台,查询账号登录情况。

(2) 创建新用户并登录,观察日志记录变化。



图 3-1 安全接入网关日志审查实验拓扑图

(3)使用用户账号进行操作,观察日志记录变化。

【实验步骤】

(1) 在管理机中打开浏览器,在地址栏中输入安全接入网关产品管理员的登录地址 "https://10.0.0.1:4430/admin"(以实际设备 IP 地址为准),进入安全接入网关的登录界 面。输入管理员用户名"admin"、密码"! 1fw@2soc # 3vpn"和验证码,单击"登录"按钮, 登录安全接入网关。

(2)进入安全接入网关设备后,会显示它的面板界面。单击"日志与监控中心"按钮,进入"日志与监控"相应界面。

【实验预期】

(1) 能够查看系统运行状态日志。

(2) 能够检索并分析用户业务访问日志。

(3)能够实时监控在线用户。

【实验结果】

(1) 将鼠标指针放在"日志与监控"界面下的"日志查询"按钮上,在显示出的子菜单中选择"日志查询"选项,如图 3-2 所示。



图 3-2 日志 首 间

(2) 在"日志查询"界面中,可以查询安全接入网关的账号登录信息,其中置顶项为本

次登录的信息,如图 3-3 所示。

()	• •)• é	192.168.2.20 J	○ ▼ ★ 证书错误	C @ 360Co	nnect	- o
Π	沪	管理	里 系統 360ID 详细E	志 虚拟服务	器日志 日志	归档	
		等级:	全部	~ 结果	全部		操作员: 子类型: 全部 v 👂
		应用:	全部	~ IP地址	;		从: 間 到: 間
				9、查询	V 1	EE	₱₩EXCEL 🗸 ₱₩HTML 🔏 ₱₩PDF
4	等级	I	时间	子类型	结果	详细信息	348.
	e=		2017-12-28 10:28:22	四串	5775		管理员[admin:本地认证]登录系统:IP[192.168.77.88], 接口[GE1], 登录方式[HTTPS],认证服务器为[本地认
	DE/JN		2017-12-20 10.20.52	豆氷	10640	362/34	证), 认证类型[LOCAL].
1	提示	:	2017-12-28 10:05:54	登录	成功	显示	管理员[admin:本地认证]超时[3600]秒后豐出.
							管理员[admin:本地认证]登录系统:IP[192.168.77.88],接口[GE1],登录方式[HTTPS],认证服务器为[本地认
1	陡不		2017-12-28 09:05:58	豆求	26-20	並示	证), 认证类型[LOCAL].
1	提示		2017-12-27 21:31:50	受灵	成功	显示	用户[yonghu:本地认证]超时[86400]秒后登出系统。
1	提示		2017-12-27 10:57:46	登录	成功	显示	管理员[admin:本地认证]超时[3600]秒后登出.

图 3-3 账号登录信息记录

(3)选择"日志与监控"界面中的"系统"选项卡,在系统日志查询界面中可以查询系统的运行状态,并可以利用关键字查询来检索用户业务访问日志,如图 3-4 所示。

đ	ł	系	统设置	SSL-VPN CA管	里 IPSec-VF	N 防火墙 日志与监	控			欢迎您: admin@192.168.77.8
			〕 日志查询	〇 用户状态	21	3 <u>~</u> 能名 系统状态	应用状态	日志服务	5篇	
F	用户 管理	系统 ID	详细日志	虚拟服务器日志	日志归档					
	等级:	全部	~	子类型: 全部		~ "Ж:			到:	
	结果:	全部	Y		9、査询					
	等级	时间		子类型	结果	消息				
	警报	2017-12-26 21:17	7:33	系统	成功	系统启动				
	警报	2017-12-26 21:16	5:36	系统	成功	命令行:系统重启				
	警报	2017-12-15 10:45	5:33	系统	成功	系统启动				
	警报	2017-12-15 10:18	3:58	系统	成功	命令行:系统重启				
	警报	2017-12-15 10:18	3:51	系统	成功	系统自动任务:重启系统。				
	警报	2017-12-13 10:42	2:24	系统	成功	系统启动				

图 3-4 系统日志查询界面

(4)选择"用户"选项卡,返回用户"日志查询"界面,并利用关键字查询来检索用户业务访问日志,如图 3-5 所示。

(5)单击"等级"菜单栏的下拉按钮,选择"警告"选项,之后单击"查询"按钮,可以看 到近期出现的警告级别的日志信息,如图 3-6 所示。

(6)新建用户组。单击上方功能面板 SSL-VPN 按钮,将鼠标指针放在"用户管理"按钮上,在显示的子菜单中选择"用户和组"选项,进入"用户和组"界面。

166

				自动	i A	同時状态	213 访问排名	系統状态	应用状态	日志服务器		
	沪	管理	系统 ID	详细日	志虚拟服务	器日志	日志归档					_
		等级:	全部		✓ 结果	: 全部	~	操作员:		子类型:	全部 >	Ø
		应用:	全部		~ IP地址	÷		Ж:		2 到:		
					9、查询	1	″重置 🖌 🤅	≩出EXCEL	✓ 导出HTML	✔ 导出PDF		_
4	夸级	时	间		子类型	结果	详细信息	消息				
	-	24	10 01 02 00 47 20		00 M.	-	-	管理员[admin:2	▶地认证]登录系统:IP[19	92.168.77.88], 接口[G	E1], 登录方式[HTTPS],认证服务器	沩[本地认
1	22/35	20	718-01-03 08:47:59		₩ ₩	19640		证], 认证类型[Li	DCAL].			
ł	眎	20	018-01-03 08:47:39		登录	成功	显示	管理员[admin:7	「地认证]登出系统 [重复	瞪录].		
								管理员[admin:2	毕地认证]登录系统:IP[19	92.168.55.66], 接口[G	E1], 登录方式[HTTPS],认证服务器	沩[本地认
1	是示	20	018-01-03 08:46:35		登求	6890	显示	证], 认证类型[L0	DCAL].			
1	眎	20	018-01-03 08:46:35		登录	成功	显示	管理员[admin:4	▶地认证]登出系统 [重复	受录].		

图 3-5 用户日志检索栏



图 3-6 警告日志信息筛选

(7) 安全接入网关默认有一个"默认组"选项。在左侧"用户组"栏中单击"添加"按钮,添加用户组。

(8) 在添加组界面中,在"名字"输入框中填入"用户组",其他保持默认配置。单击"保存"按钮,保存配置。

(9) 在弹出的"提示"界面中单击"返回列表"按钮,查看新添加的用户组,如图 3-7 所示。

(10) 添加用户。在右侧"用户列表"界面中单击"添加"按钮,进入添加用户界面。

(11) 在添加用户界面中,在"名字"输入框中填入"test",在"密码"和"确认密码"输入 框中填入"123456",在"状态"选择框中选择"允许"选项,在"组信息"选择框中选择"用户 组"选项,其他保持默认配置。单击"保存"按钮,保存配置。

(12)单击"保存"按钮后,在弹出的"提示"界面中单击"返回列表"查看新添加的用户信息,如图 3-8 所示。

用户和组						
用户组	用户列表					
 添加 💥 删除 更多 • () 	 添加 米里添加 ※ 	导出 💥 删除	💥 删除全部	部用户 🔒 转证书用户	▶ 备份恢复	备份导出
组名字	用户名:	手机号码:		邮箱地址:	:	状态: 全部
 ▲ □□ 全部 ▶ □□□ 默认组 ▶ □□ 用户组 	□ 用户名	认证	状态 1	Mini网关地址池	手机号码	邮箱地





图 3-8 用户列表

(13) 打开新浏览页,在地址栏中输入安全接入网关用户的登录地址"https://10.0.0. 1:4430/admin"(以实际设备 IP 地址为准),进入安全接入网关的登录界面。输入用户名 "test"、密码"123456"和验证码,单击"登录"按钮,登录安全接入网关。

(14)返回管理员界面的"日志与监控"界面,在用户日志信息列表中发现 test 用户的 登录信息,如图 3-9 所示。

đ	ł	系统省	置 SSL-VPN	CA管理	IPSec-VPN	防火墙 日志与监控 欢迎您: admin@192.168.77.88 [→
		Bi		同時代表	21 <u>3</u> 访问排名	
E	用户	管理 系统 ID 详	細日志 虚拟服	务器日志 日;	あ旧档	
	轉	級: 全部	~ 结	₽: 全部	•	> 操作员: 子类型: 全部 →
	应	用:全部	~ IP地	ıl:		Ж. 🖺 🖤
			9、首		ŧ₹ 🗸	₽₩EXCEL 🖋 ₽₩HTML 🖋 ₽₩PDF
	等级	时间	子类型	结果	详细信息	消息
	提示	2018-01-03 09:55:28	登录	成功	显示	用户[test本地认证], 获取服务列表, (操作系统版本号[WinNT10]).
						用户[test:本地认证]登录系统:IP[192.168.77.88], 接口[GE1], 登录方式[HTTPS],认证服务器为[本地认证], 认
	提示	2018-01-03 09:55:28	登录	成功	显示	证类型[LOCAL].
						" 管理员[admin:本地认证]登录系统IP[192.168.77.88],接口[GE1],登录方式[HTTPS],认证服务器为[本地认
	提示	2018-01-03 09:34:08	豆求	196421	並不	证], 认证类型[LOCAL].

图 3-9 test 用户登录信息

(15) 单击用户登录界面中"设置"下拉列表框下的"密码修改"按钮,如图 3-10 所示。

			欢迎您: test 日期: 1/3/2018 登
	合 全部应用	全部应用	
į	∲ 设置 ✓	工作的工具	
-	关联程序		
	▲ 下载		

图 3-10 修改用户密码

(16) 按照密码强度将新密码设置为"qq123QQ"(也可自行设置),单击"提交"按钮, 如图 3-11 所示。

	密码修改 🛛 🗙
认证服务器	本地认证
用户名	test
旧密码	*
密码	******
702.51 579777	(6-32 数字:2位,大写字母:2位,小写字母:2位)
佣认咨伯	*
	提交

图 3-11 设置新密码

(17)返回管理员界面,进入"日志与监控"界面下的"日志查询"选项卡,在"用户"界面的日志列表中可以看到此次修改密码操作的信息,如图 3-12 所示。

ŝ	系统设置	SSL-VPN	CA管理	IPSec-VPN	次增 日志与监控 欢迎您: admin@192.168.75
	自志意	in A	同時状态	213 访问排名	「「」 「 「」 「」 「 「」 「」 「 「」 「 「」 「 「」 「 「」 「 「」 「 「 「」 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「 「
用户(管理系统 ID 详细日	日志 虚拟服务	瑞日志 日志	归档	
*	级: 全部	~ 结果	全部		操作员: 子英型: 全部 🗸
应	用:全部	~ IP地址	:		从: 西 到:
		号, 查询	1	itter 🖌 🗸	ЭШЕХСЕL 🖉 ЭШНТМL 🖉 ЭШРDF
等级	时间	子类型	结果	详细信息	消息
提示	2018-01-03 10:02:44	登录	成功	显示	用户[test本地认证],傅改密码[成功].
提示	2018-01-03 10:02:22	登录	失败	显示	用户[test本地认证],修改密码(失败].
提示	2018-01-03 10:02:06	登录	失敗	显示	用户[test本地认证], 修改密码[失败].
提示	2018-01-03 09:55:28	登录	成功	显示	用户[test:本地认证], 获取服务列表, (操作系统版本号[WinNT10]).
提示	2018-01-03 09:55:28	登录	成功	显示	用户[test本地认证]登录系统1P[192.168.77.88],接口[GE1],登录方式[HTTPS],认证服务器为体地认证]

图 3-12 密码修改信息

(18)将鼠标指针放在"用户状态"按钮上,在显示出的子菜单中选择"在线用户"选项,如图 3-13 所示。



图 3-13 在线用户监控界面

(19) 在用户监控界面中可以看到 test 用户的在线情况,如图 3-14 所示。

Å	系统设置 SSL	VPN CA管理	IPSec-VPN 防火墙	日志与监控		欢迎您:	admin@192.168.77.88
	日本書演		213				
在线用户在线管理员	HICKER (P)	账号计注策部 1	בראנטיונא אפריינא			291-	
17		Q. 查询	₩ 终止 ♥ !	эщехсеl 🗸 эн	HTML ダ 导出PDF	30	
日名字	账	引认证类型	登录时间	登录IP	NC IP	客户端类	离线倒计时
🗆 🧠 test	本地	的证	2018-01-03 09:55:28	192.168.77.88		HTTPS	23小时17分钟

图 3-14 用户在线信息

(20) 在"在线管理员"界面中可以看到当前在线的管理员账号信息,如图 3-15 所示。

畲	系统设置	SSL-VPN CA管理	IPSec-VPN	防火墙 日志与监控			欢迎您: admin@192.16
	日志宣道	し 用户状态	2 <u>1</u> 3 访问排名	系統状态	应 用状态	日志服务器	
在线用户 在线	管理员 日志查询 IKE协商日	日志查询相关信息 志 IKE协商日志相关信息 从:			·····································	🗙 终止	
□ 名字			账号认证类型	登录时	ŋ	登录IP	离线倒计时
□ *admin			本地认证	2018-0	1-03 09:34:08	192.168.77.88	1小时

图 3-15 管理员在线信息

(21)将鼠标指针放在"用户状态"按钮上,在显示出的子菜单中选择"用户会话"选项,如图 3-16 所示。

ť	ŝ	系统设置	SSL-VPN CA管理	IPSec-VPN	防火墙 日志	与监控		25	び印念: adm
		日志查询	〇 用户状态	21 <u>3</u> 访问排名	系统状态	あ 应用状表			
	在线用户 在线管理员 名字:		在线用户在线机 用户会话用户: 账号认证类型:	用户相关信息 会话相关信息 全部	~	ж:		到:	
			9、查询	🗙 终止	✓ 导出EXCI	EL 🗸 导出HTI	ML 学出PDF		
	□ 名字	ļ	账号认证类型	登录时间	璒	绿IP	NC IP	客户端类	离线
	🗆 🔍 test		本地认证	2018-01-03 11:0	2:18 19	92.168.77.88		HTTPS	23

图 3-16 用户会话选项

(22) 在"用户会话"界面中,可以看到 test 用户的登录会话信息,如图 3-17 所示。

1	ĥ	系统设置	SSL-VPN	CA管理 II	Sec-VPN	防火爆	日志与监控			欢迎您: admin@	192.168.77.8	8 [→
		Ê	ſ	D	2 1 3		~					
		日志査询	1 用户	中状态	访问排名		系统状态	应用状态	日志服务器			
	用户会话											
	名字:		ж :):			9、查询			9
	名字	登录时间		登出时间			登录IP		操作系统/浏览器	流量	详细	
									Mozilla/5.0 (Windows NT 10.0;			
	test	2018-01-	03 11:02:18				192.168.77.88		WOW64; Trident/7.0; rv:11.0) like	0	显示	
									Gecko			

图 3-17 用户会话信息

(23) 单击用户会话信息列表的"详细"列下的"显示"选项,如图 3-18 所示。

fi	系统设置	SSL-VPN	CA管理 IF	Sec-VPN	防火爆	日志与监控			欢迎您: admin@	9192.168.77.8	38 [→
	日志查询	甩	〇 户状态	213 访问排名		系统状态	正 应用状态	日志服务器			
用户会话		ж:			到:			Q、 查询			Ø
名字	登录时间		登出时间			登录IP		操作系统/浏览器	流量	详细	
test	2018-01-(03 11:02:18				192.168.77.88		Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko	0	显示]

图 3-18 用户详细会话信息

(24) 在"用户详细信息"列表中,可以看到 test 用户的详细信息,如图 3-19 所示。

【实验思考】

(1) 审查日志的安全意义是什么?

(2) 日志信息分级的优点是什么?

ſ	系统设置 S	SL-VPN CA管理	IPSec-VPN	防火墙 日志与监控			欢迎您: admin@192.168.77.88
	日志查询	同時代表	21 <u>3</u> 访问排名	系统状态	正 应用状态	日志服务器	
用户详细信	慮						
用户会话:te	est 登录时间是:2018-01-03 11:02:13	8 登出时间是: 登	送录IP:192.168.77.8	38			
返回							
返回	时间	动作	结果	消息			
返回 等级 提示	时间 2018-01-03 11:02:18	动作登录	结果成功	消息 用户[test:本地认证], 获取服	务列表, (操作系統	版本号[WinNT10]) .	
返回 等级 提示	时间 2018-01-03 11:02:18	动作 登录	结果成功	消息 用户[test本地认证],获取服 用户[test本地认证]登录系统	务列表, (操作系统 6:IP[192.168.77.	版本号[WinNT10]) . 88], 接口[GE1], 登录方式	c(HTTPS),认证服务器为(本地认证), 认证类型

图 3-19 test 用户详细信息