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。

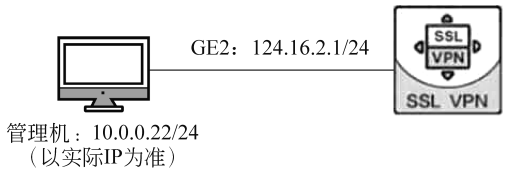

图 3-1　安全接入网关日志审查实验拓扑图

（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　日志查询

（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。

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。

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。

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。

图 3-7　用户组列表

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。

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。

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。

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。

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。

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。

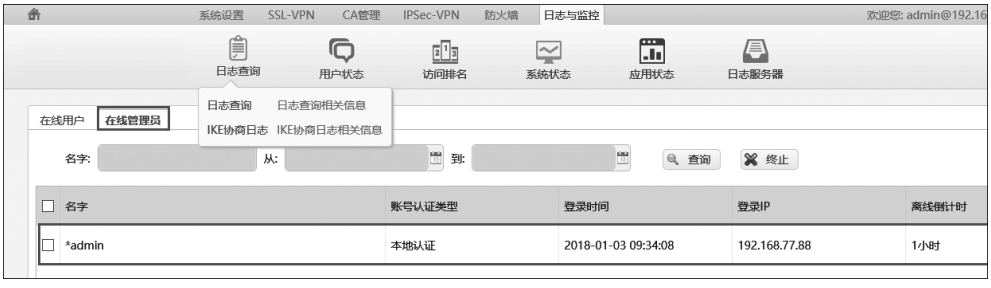

图 3-15　管理员在线信息

(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。

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。

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。

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?

图 3-19　test 用户详细信息