RV320和RV325 VPN路由器系列的系统日志配置

目标

系统日志是网络事件记录。日志是用于了解网络如何运行的重要工具。它们对网络管理和网络故障排除非常有用。

本文介绍如何配置要记录的日志类型、如何查看RV32x VPN路由器系列上的日志，以及如何通过SMS将日志发送到收件人、系统日志服务器或通过电子邮件发送给收件人。

适用设备

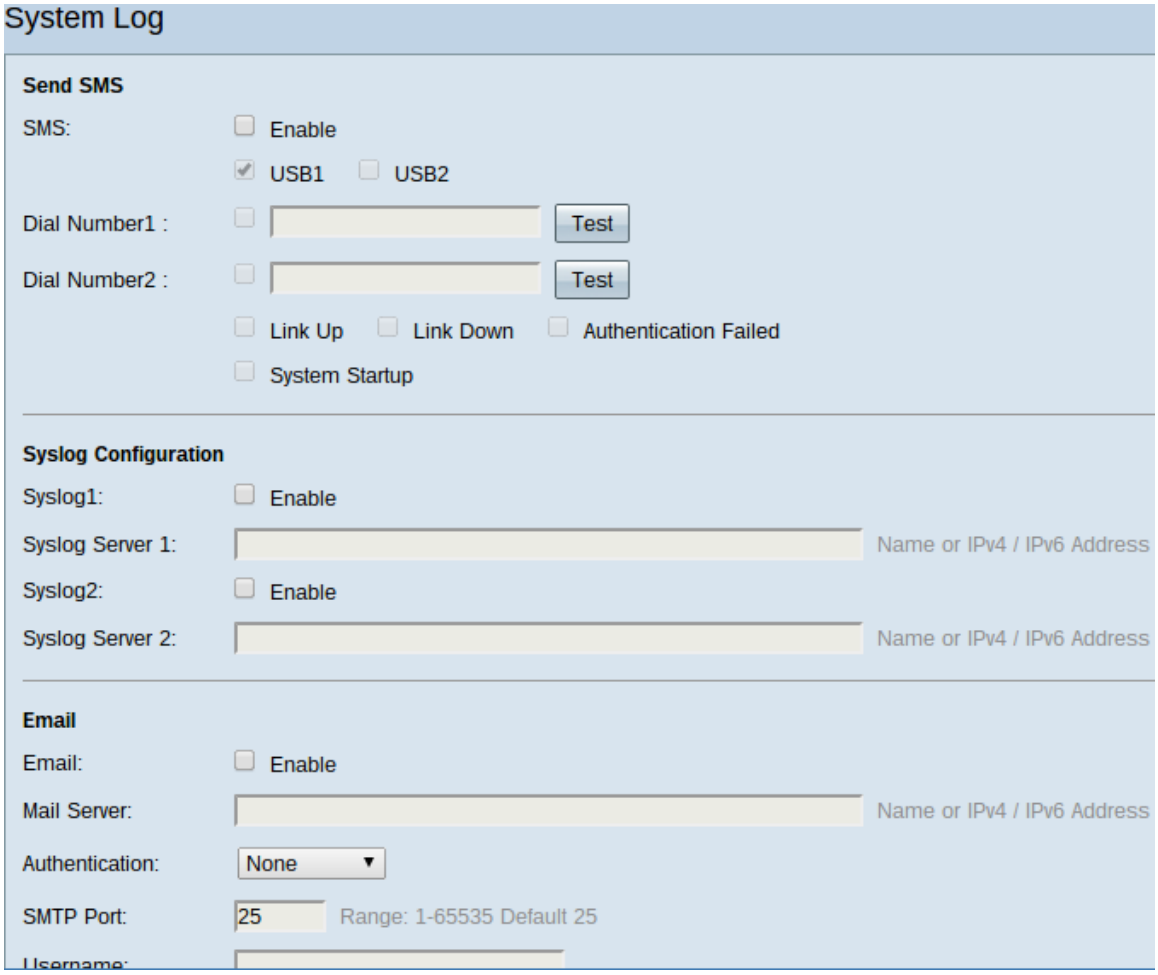
·RV320双WAN VPN路由器
· RV325千兆双WAN VPN路由器

软件版本

•v1.1.0.09

系统日志配置

步骤1.登录Web配置实用程序，然后选择Log > System Log。系统*日志*页面打开：



有关“系统日志”页的信息，请*参阅以*下各节。

·SMS系统日志 — 如何通过SMS将系统日志发送到电话

·系统日志服务器上的系统日志 — 如何将系统日志发送到系统日志服务器。

·电子邮件系统日志 — 如何将系统日志发送到电子邮件地址。

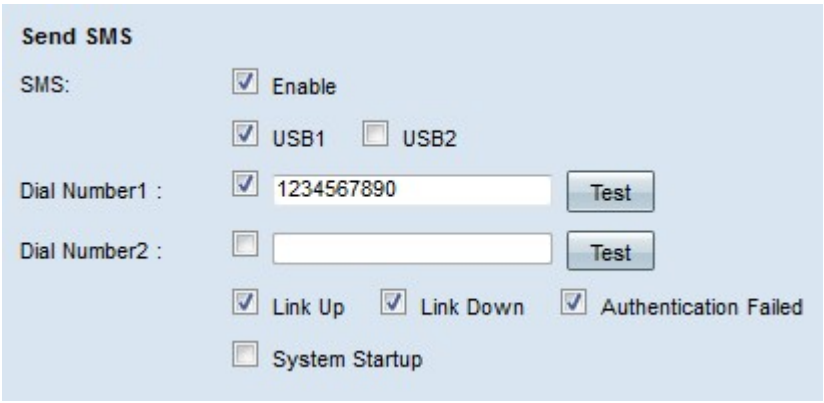
·日志设置 — 如何配置保存到日志中的消息的类型。

·View System Log — 如何查看设备上的系统日志。

·查看传出日志表 — 如何查看仅与传出数据包相关的系统日志。

·查看传入日志表 — 如何查看仅与传入数据包相关的系统日志。

按SMS划分的系统日志



步骤1.在SMS字段中选**中启**用，通过短信服务(SMS)消息将系统日志发送到客户端。

步骤2.选中3G USB调制解调器所连接的USB端口的复选框。

步骤3.选中Dial Number1字段中的复选框，并输入消息发送到的电话号码。

注意：单击**测试**以测试与拨号号码1的连接。如果配置的号码未收到测试消息，请确保在“拨号号码1”字段中正确输入了电话号码。

步骤4.（可选）选中Dial Number2（拨号号码2）字段中的复选框，并输入消息发送到的电话号码。

注意：单击**测试**以测试与拨号号码2的连接。如果配置的号码未收到测试消息，请确保在“拨号号码2”字段中正确输入电话号码。

步骤5.选中将触发要发送的日志的事件的复选框。

·Link Up — 已建立与RV320的连接。

·链路断开 — 与RV320的连接已断开。

·身份验证失败 — 身份验证失败。

·系统启动 — 路由器启动。

步骤6.单击“保**存**”。通过SMS配置系统日志。

系统日志服务器上的系统日志

步骤1.在Syslog1字段中选**Enable**，将系统日志发送到系统日志服务器。

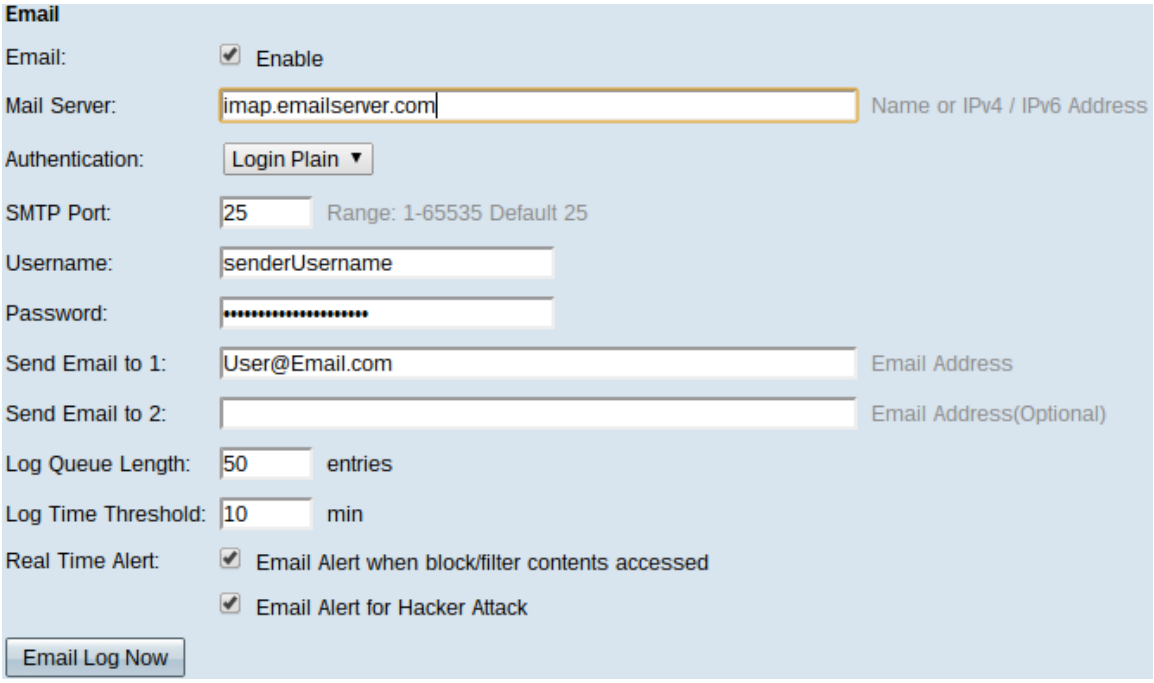
步骤2.在Syslog Server 1字段中输入系统日志服务器的主机名或IP地址。

步骤3.（可选）要将日志发送到另一个系统日志服务器，请在Syslog2字段中选**中Enable**。

步骤4.如果在Syslog2字段中选中此复选框，请在Syslog Server 2字段中输入系统日志服务器的主机名或IP地址。

步骤5.单击**Save**。通过系统日志服务器配置系统日志。

电子邮件系统日志



步骤1.在Email字段中选**择Enable**，通过电子邮件将系统日志发送到收件人。

步骤2.在Mail Server字段中输入邮件服务器的域名或IP地址。

步骤3.在Authentication字段中选择邮件服务器使用的Authentication类型。

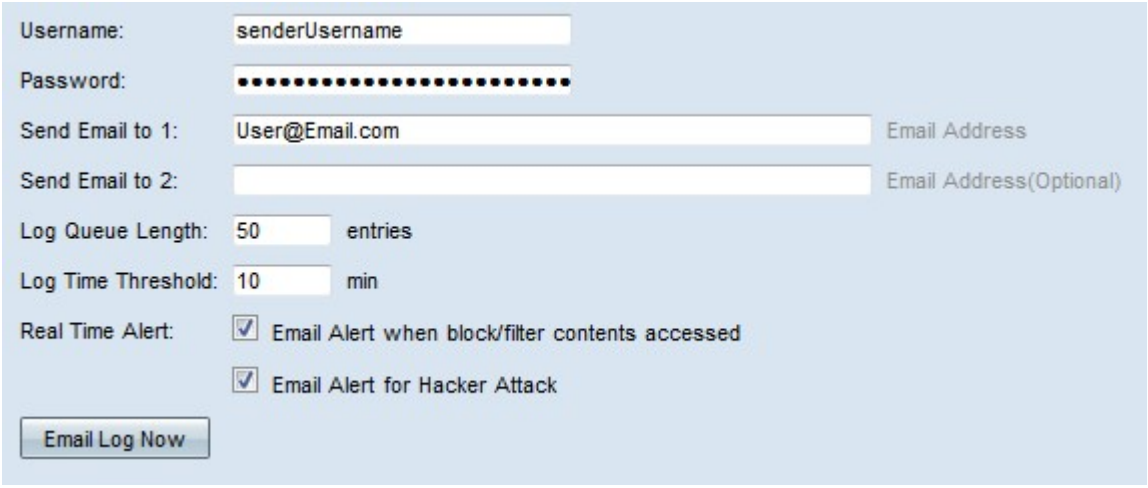
·无 — 邮件服务器不使用身份验证。

·Login Plain — 邮件服务器使用纯文本格式的身份验证。

·TLS — 邮件服务器使用传输层安全(TLS)，以允许客户端和服务器安全地交换身份验证信息。

·SSL — 邮件服务器使用安全套接字层(SSL)，以允许客户端和服务器安全地交换身份验证信息。

步骤4.在“SMTP端口”字段中输入邮件服务器使用的简单邮件传输协议(SMTP)端口。SMTP是允许通过IP网络传输电子邮件的协议。



步骤5.在Username字段中输入邮件发件人的用户名。

步骤6.在“密码”字段中输入邮件发件人的密码。

步骤7.在Send Email to 1（将电子邮件发送到1）字段中输入电子邮件收件人的电子邮件地址。

第8步。（可选）在Send Email to 2字段中输入要向其发送日志电子邮件的附加电子邮件地址。

步骤9.在Log Queue Length字段中输入在将日志发送到电子邮件收件人之前必须创建的日志条目数。

步骤10.在Log Time Threshold字段中输入设备将日志发送到电子邮件的间隔。

步骤11.选中Real Time Alert（实时警报）字段的第一个复选框，以在被阻止或过滤的人尝试访问路由器时立即发送电子邮件。

步骤12.选中Real Time Alert（实时警报）字段的第二个复选框，以便当黑客尝试通过拒绝服务(DOS)攻击访问路由器时立即发送电子邮件。

注意：单击**Email Log Now(立**即发送电子邮件日志)立即发送日志。

步骤13.单击“保**存”**。通过邮件配置系统日志。

日志设置

步骤1.选中将触发日志条目的事件的复选框。

·警报日志 — 这些日志在发生攻击或尝试攻击时创建。

- Syn泛洪 — 收到SYN请求的速度比路由器处理它们的速度快。

- IP欺骗 — RV320已接收具有伪造源IP地址的IP数据包。

— 未授权登录尝试 — 拒绝登录网络的尝试失败。

— 死亡之ping — 已向接口发送大小异常的ping，以尝试使目标设备崩溃。

- Win Nuke — 远程分布式拒绝服务攻击(DDOS)（称为WinNuke）已发送到接口，以尝试使目标设备崩溃。

·常规日志 — 这些日志在发生常规网络操作时创建。

— 拒绝策略 — 根据路由器配置的策略拒绝用户访问。

— 授权登录 — 用户已获得访问网络的授权。

— 系统错误消息 — 发生系统错误。

— 允许策略 — 已根据路由器的已配置策略向用户授予访问权限。

— 内核 — 在日志中包含所有内核消息。内核是操作系统的第一部分，在启动时加载到内存中。内核消息是与内核关联的日志。

— 配置更改 — 路由器配置已修改。

- IPSEC & PPTP VPN — 已发生IPSEC & PPTP VPN协商、连接或断开。

- SSL VPN — 发生SSL VPN协商、连接或断开连接。

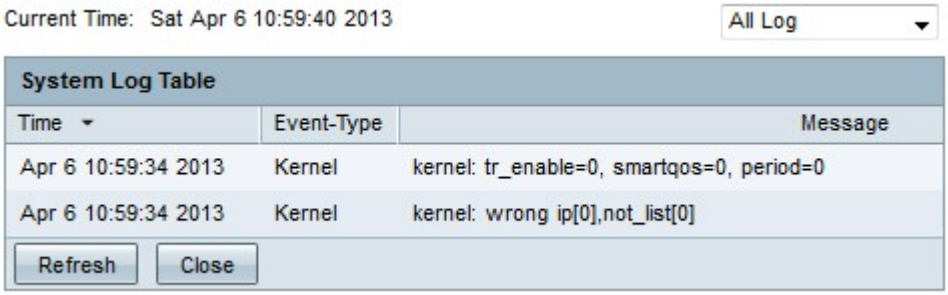
— 网络 — WAN或DMZ接口上已建立或丢失物理连接。

步骤2.单击“保**存”**。日志设置已配置。

注意：单击**清除日**志以清除当前日志。

查看系统日志

步骤1.单击“查**看系统日志**”查看系统日志表。系统将*显示“系统日*志表”窗口。



步骤2.（可选）从下拉列表中选择要查看的日志类型。

·所有日志 — 包括所有日志消息。

·系统日志 — 仅包括系统错误消息。

·防火墙/DoS日志 — 仅包括警报日志。

·VPN日志 — 仅包括IPSec和PPTP VPN和SSL VPN日志。

·网络日志 — 仅包括网络日志。

·内核日志 — 仅包括内核消息。

·用户日志 — 仅包括拒绝策略、允许策略、授权登录和配置更改日志

·SSL Log — 仅包括SSL VPN日志。

系统日志表显示以下信息。

·时间 — 日志的创建时间。

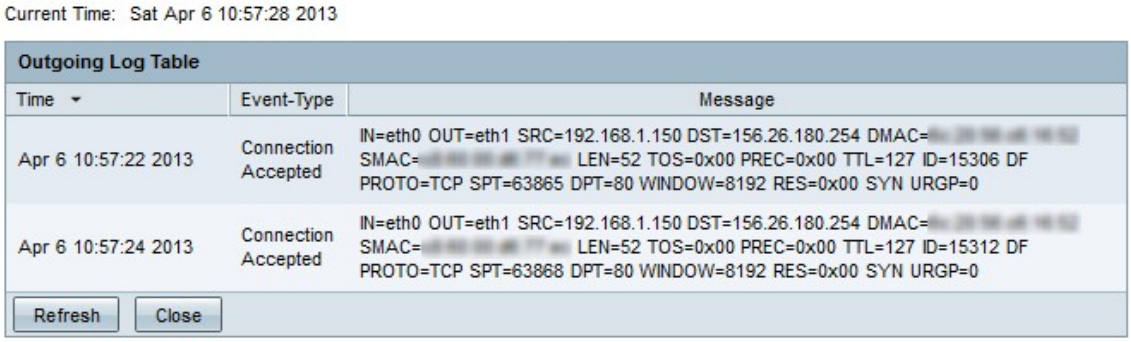
·事件类型 — 日志的类型。

·消息 — 与日志对应的信息。这包括策略类型、源IP地址和源MAC地址。

注意：单击**Refresh**刷新日志表。

查看传出日志表

步骤1.单击**Outgoing Log Table** ，查看仅与传出数据包相关的日志表。系统将*显示"传出日*志表"窗口。



外发日志表显示以下信息。

·时间 — 日志的创建时间。

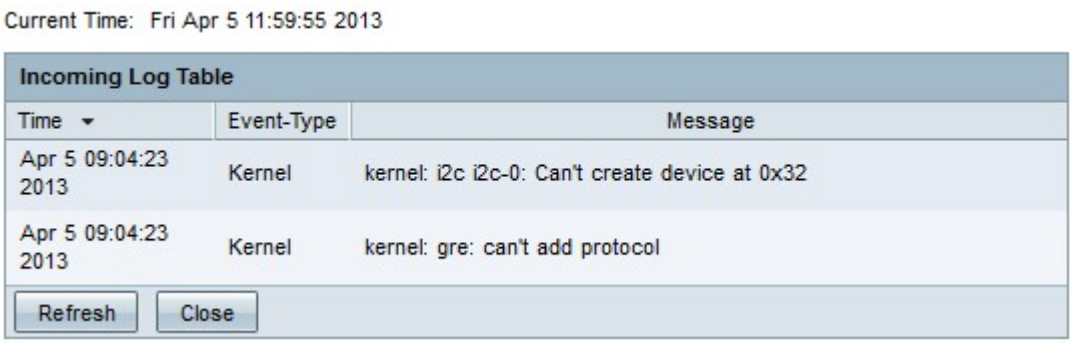
·事件类型 — 日志的类型。

·消息 — 与日志对应的信息。这包括策略类型、源IP地址和源MAC地址。

注意：单击**Refresh**刷新日志表。

查看传入日志表

步骤1.单击**Incoming Log Table**查看仅与传入数据包相关的日志表。系统将*显示"传入日志*表"窗口。



传入日志表显示以下信息。

·时间 — 日志的创建时间。

·事件类型 — 日志的类型。

·消息 — 与日志对应的信息。这包括策略类型、源IP地址和源MAC地址。

注意：单击**Refresh**刷新日志表。