在RV016、RV042、RV042G和RV082 VPN路由器的系统日志配置

客观

系统日志(Syslog)用于记录计算机数据。您能定义将生成一本日志的实例。每当实例发生，时间和事件在电子邮件被记录并且被发送到系统日志服务器或被发送。Syslog可能然后用于与增量网络安全一起分析和排除网络故障。

本文解释程序配置在RV016、RV042、RV042G和RV082 VPN路由器的一个系统日志服务器。

可适用的设备

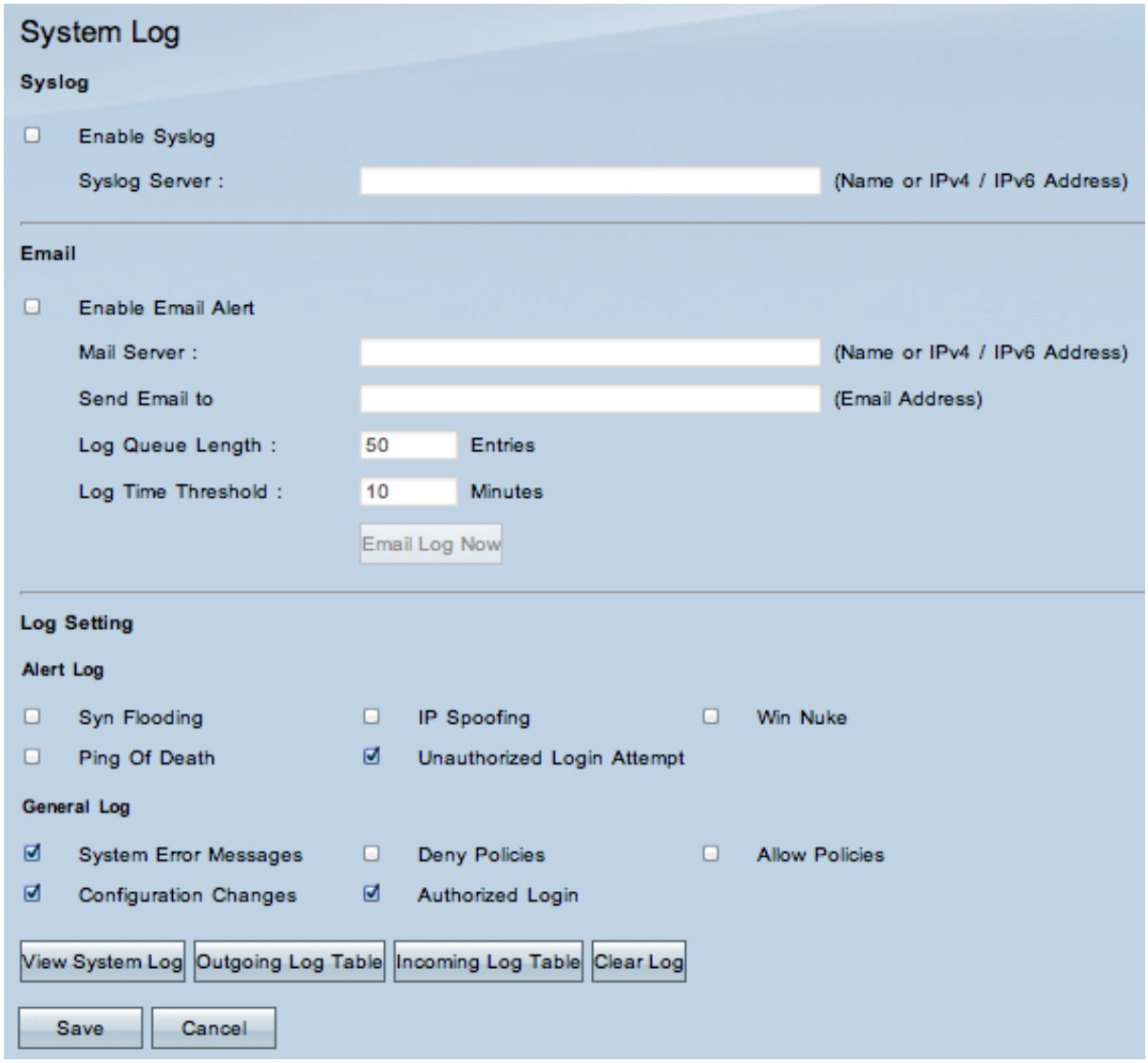
- RV016
- RV042
- RV042G
- RV082

软件版本

- v4.2.1.02

Syslog和戒备的配置

步骤1.登陆到Web配置工具并且选择**日志>System日志**。*系统日志*页打开：



系统日志

当事件被记录时，此部分如何说明对enable (event)发送详细日志文件的路由器到您的系统日志服务器。

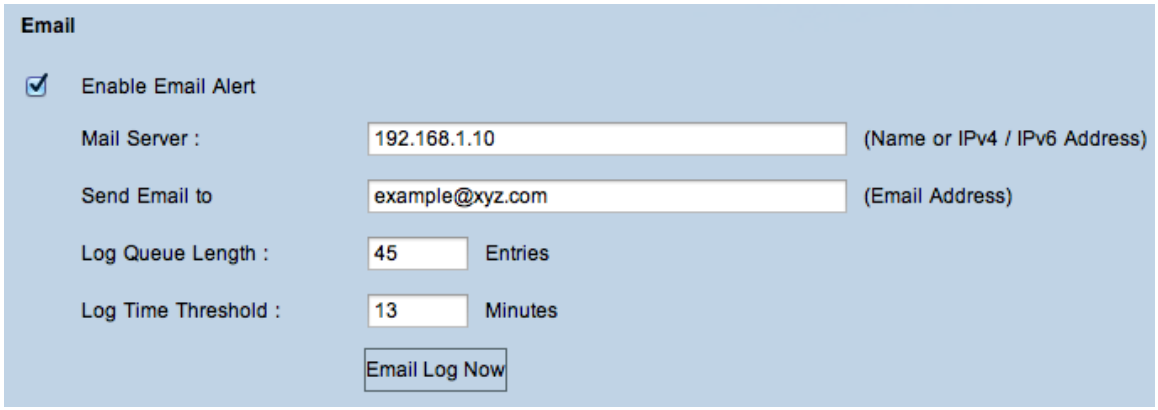
Step 2.检查**Enable (event) Syslog**复选框对enable (event)在设备的系统日志服务。

节时： 如果Syslog需要被禁用，请跳到第4步。

步骤3.输入域名或系统日志服务器的IP地址在系统日志服务器领域。

发送邮件

当事件被记录时，此部分如何说明对enable (event)发送电子邮件告警的路由器。



第4.步。检查**Enable (event)电子邮件告警**对enable (event)功能。此enable (event)发送电子邮件告警的路由器到用户指定了电子邮件地址。

节时：如果电子邮件告警需要被禁用，请跳到第10步。

步骤5.输入您的ISP SMTP服务器的IPv4或IPv6地址在邮件服务器领域。

Note:您的ISP可能要求您识别您的有主机名的路由器。选择定义您的路由器主机名的**设置>网络**。

步骤6.输入您要发送在发送电子邮件的戒备到字段的电子邮件地址。

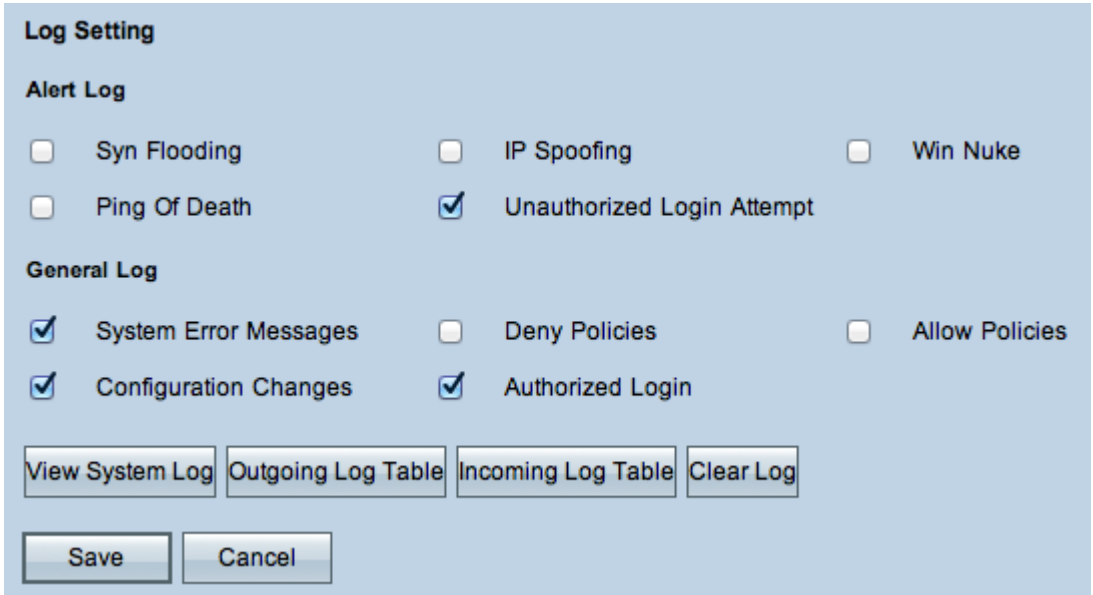
步骤7.输入日志条目的数量包括在电子邮件在日志队列长度字段。默认值是50。

步骤8.输入分钟的数量在发送登录日志时间阈值字段前收集数据。在发前，日志时间阈值是最长等待时间电子邮件日志消息。当日志时间阈值到期时发送电子邮件是否电子邮件日志缓冲器是充分。默认值是10分钟

第9.步(可选)**当前**点击**电子邮件日志**立刻传送信息到指定的电子邮件地址测试设置。

日志设置

此部分说明在日志可以报告的各种事件：



第10.步。提醒的日志地区包含攻击和未经鉴定的登录尝试的常用类型。检查复选框任一种期望攻击包括他们在事件日志或者不选定他们从事件日志省略他们。

•SYN充斥—造成路由器开始多个会话的攻击者不断地发送许多同步信息包，以便数据流变得非常拥挤，并且导致否决合法数据流的路由器。

•IP伪装—攻击者从一个假IP原地址发送信息包做攻击看起来合法数据流。

•成功核武器—攻击者发送在波段消息外面到Windows机器做目标计算机失败。

•致死ping —攻击者发送一个大IP信息包做目标计算机失败。

•未授权的登录尝试—某人设法登陆到路由器配置工具，不用适当的验证。

第11.步。一般日志地区包括进行强制执行被配置的策略以及惯例事件例如被核准的登录和配置更改的动作。检查复选框所有期望事件包括它在一般日志。非选定复选框从一般日志省略它。

•系统错误消息—所有系统错误消息。

•拒绝策略—实例，当根据您的访问的路由器拒绝访问规定。

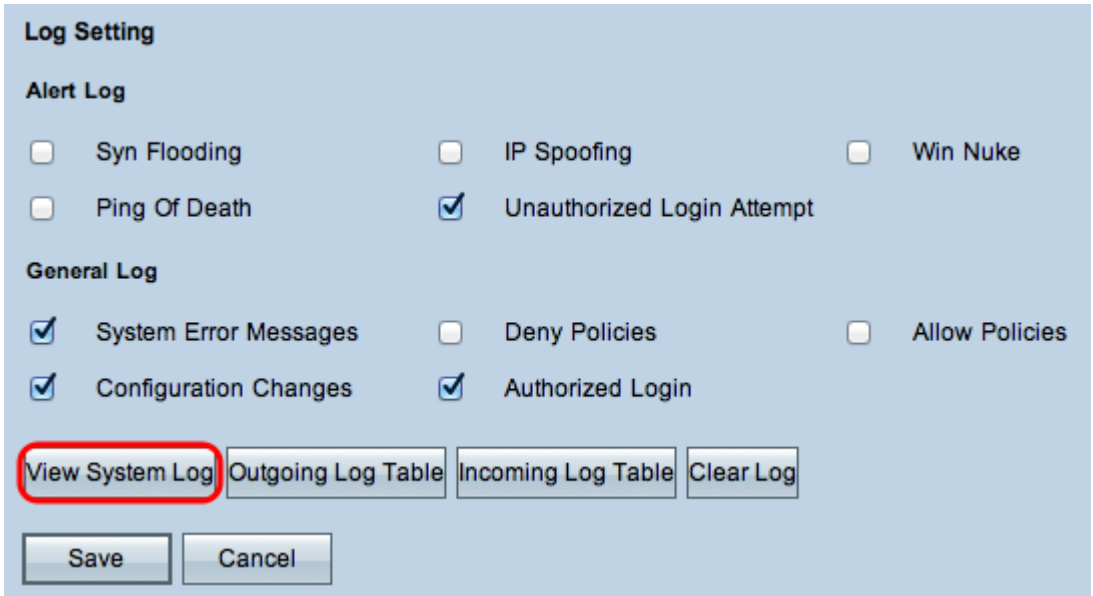
•允许策略—实例，当路由器准许根据您的访问的访问规定。

•配置更改—实例，当某人在配置上的被保存的变化。

•被核准的洛金—实例，当某人顺利地登录到路由器配置工具在输入正确的用户名和密码以后。

•输出阻塞事件—实例有在ProtectLink Web名誉的地方一个事件或者URL过滤。

Note:输出阻塞事件只是可用的在RV082 VPN路由器。



步骤12。(可选)查看系统日志点击**视图系统日志**。*系统日志*窗口出现：

Note: 日志条目提供事件类型和消息的日期和时间。此消息指示策略的种类例如访问规则、来源的LAN IP地址和MAC地址。

第13步。从下拉列表选择一本特定的日志。

步骤14。(可选)更新数据点击请**刷新**。

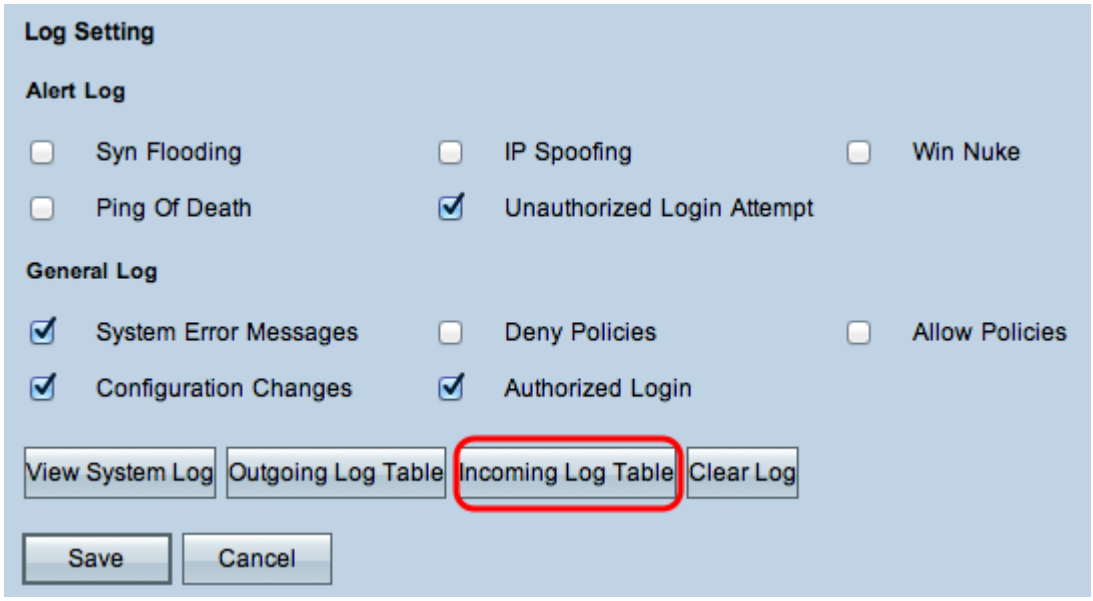
第15步。(可选)清除所有显示的信息**清楚请**点击。

第16步。点击**接近**close窗口。

第17步。(可选)查看关于流出的信息包的信息，请点击**流出的日志表**。信息出现于一个新建窗口。

第18步。(可选)更新数据点击请**刷新**。

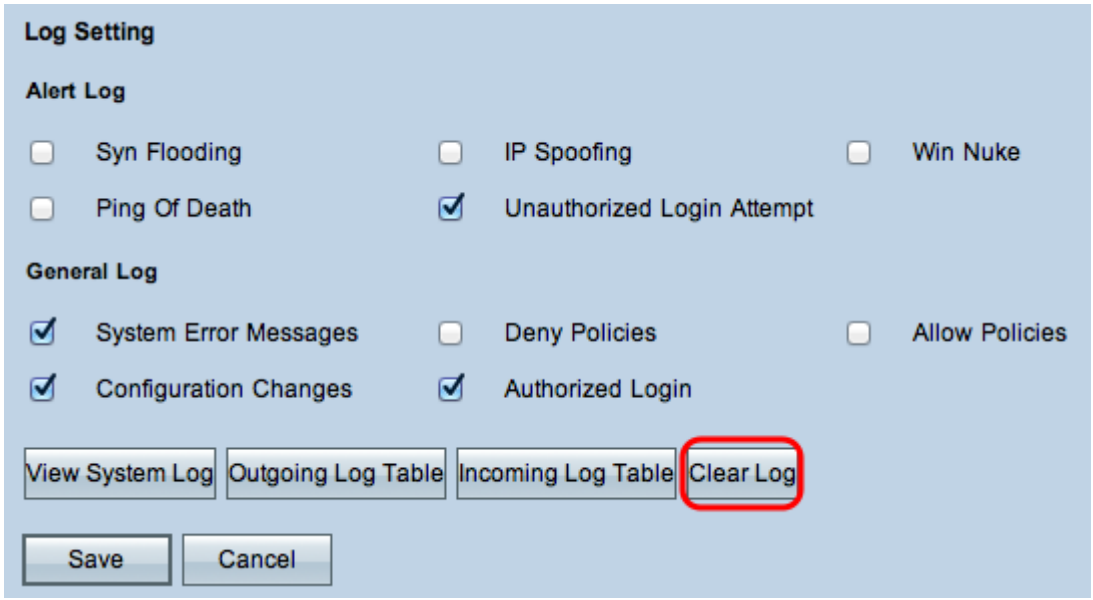
第19步。点击**接近**close窗口。



第20步。(可选)请点击**流入日志表**查看关于流入信息包的信息。信息在一个新建窗口打开。如果警告出现关于弹出式窗口，请允许封锁的内容。

第21步。(可选)更新数据点击请**刷新**。

第22步。点击**接近**close窗口。



第23步。(可选)清除日志，**当前请**点击**清楚的日志**。只有当信息不需要在将来，再查看请点击此按钮。

第24步。点击**"Save"**保存配置。