RV320和RV325 VPN路由器系列上的系統日誌配置

目標

系統日誌是網路事件的記錄。日誌是用來瞭解網路運行方式的重要工具。它們對於網路管理和網路故障排除非常有用。

本文說明如何配置要記錄的日誌型別、如何檢視RV32x VPN路由器系列上的日誌，以及如何通過SMS將日誌傳送給收件人、系統日誌伺服器或通過電子郵件傳送給收件人。

適用裝置

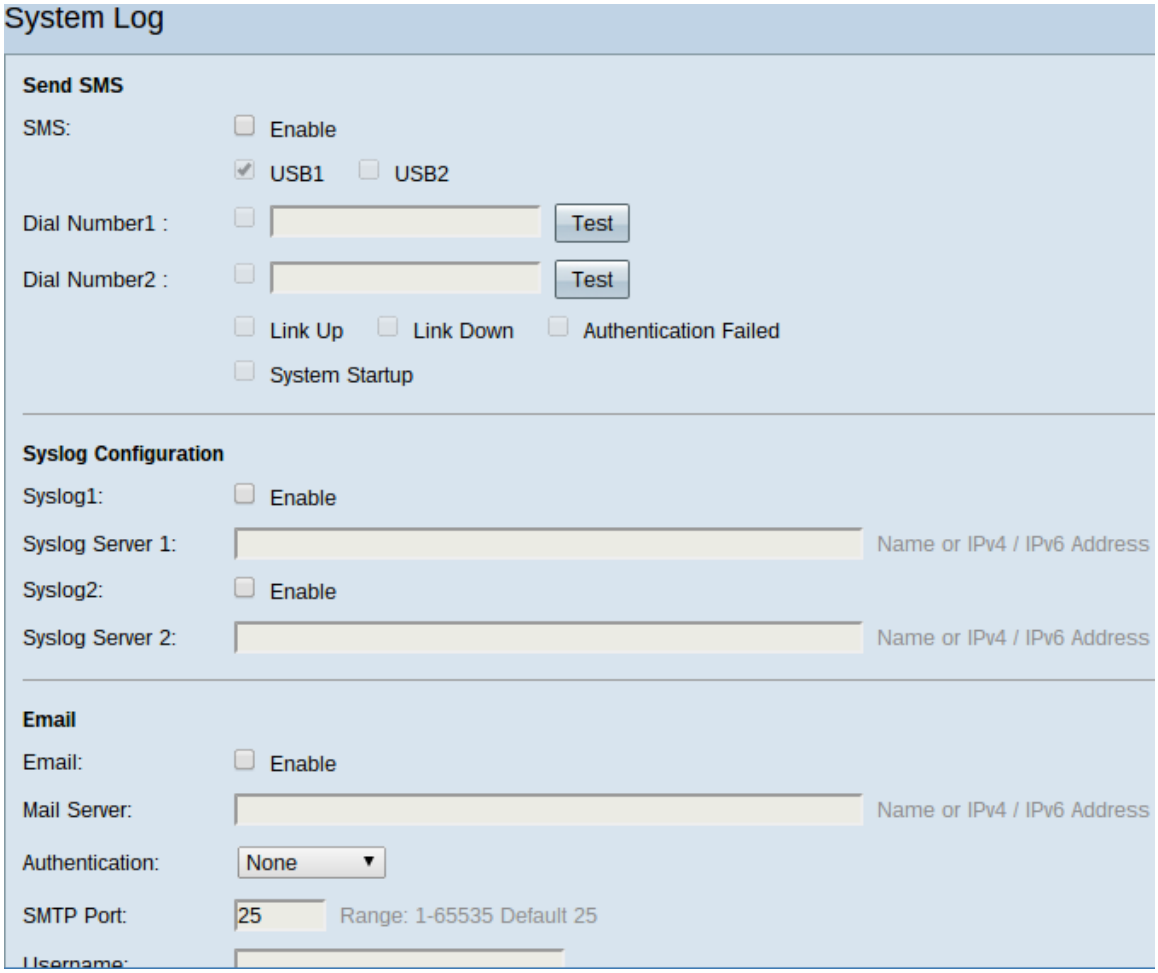
·RV320 Dual WAN VPN路由器
· RV325 Gigabit Dual WAN VPN路由器

軟體版本

·v1.1.0.09

系統日誌配置

步驟1.登入到Web配置實用程式，然後選擇**Log > System Log**。將開啟*系統日誌*頁：



有關「系統日誌」頁的資訊，請*參閱以下*部分。

·SMS系統日誌 — 如何通過SMS將系統日誌傳送到電話。

·系統日誌伺服器上的系統日誌 — 如何將系統日誌傳送到系統日誌伺服器。

·電子郵件系統日誌 — 如何將系統日誌傳送到電子郵件地址。

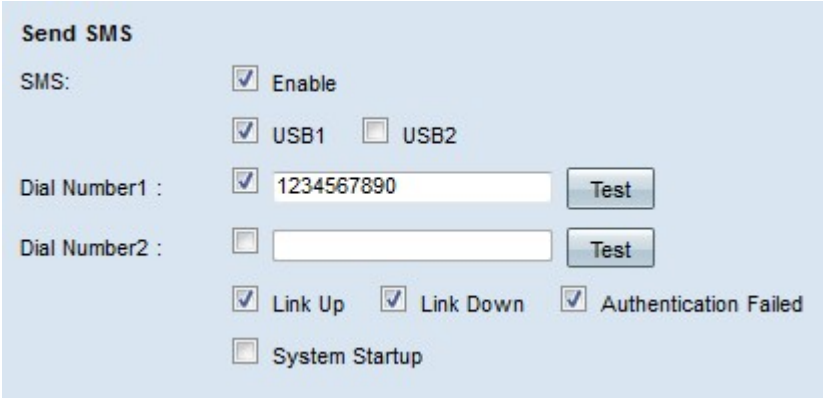
·日誌設定 — 如何配置儲存到日誌的消息的型別。

·檢視系統日誌 — 如何檢視裝置上的系統日誌。

·檢視傳出日誌表 — 如何檢視僅與傳出資料包相關的系統日誌。

·View Incoming Log Table — 如何檢視僅與傳入資料包相關的系統日誌。

按SMS分類的系統日誌



步驟1.在SMS欄位中選中**Enable**，以通過簡訊服務(SMS)消息將系統日誌傳送到客戶端。

步驟2.選中3G USB數據機所連線的USB埠的覈取方塊。

步驟3.選中Dial Number1欄位中的覈取方塊，並輸入將消息傳送到的電話號碼。

附註：按一下**測試**以測試與撥號1的連線。如果配置的號碼未收到測試消息，請確保在「撥號1」欄位中正確輸入電話號碼。

步驟4.（可選）選中Dial Number2欄位中的覈取方塊，並輸入將消息傳送到的電話號碼。

附註：按一下**測試**以測試與撥號2的連線。如果配置的號碼未收到測試消息，請確保在「撥號號碼2」欄位中正確輸入了電話號碼。

步驟5.選中將觸發傳送日誌的事件對應的覈取方塊。

·鏈路開啟 — 與RV320的連線已啟動。

·鏈路斷開 — 與RV320的連線已斷開。

·身份驗證失敗 — 身份驗證失敗。

·系統啟動 — 路由器已啟動。

步驟6.按一下「**Save**」。通過SMS配置系統日誌。

系統日誌伺服器上的系統日誌

步驟1.選中Syslog1欄位中的**Enable**，將系統日誌傳送到系統日誌伺服器。

步驟2.在Syslog Server 1欄位中輸入系統日誌伺服器的主機名或IP地址。

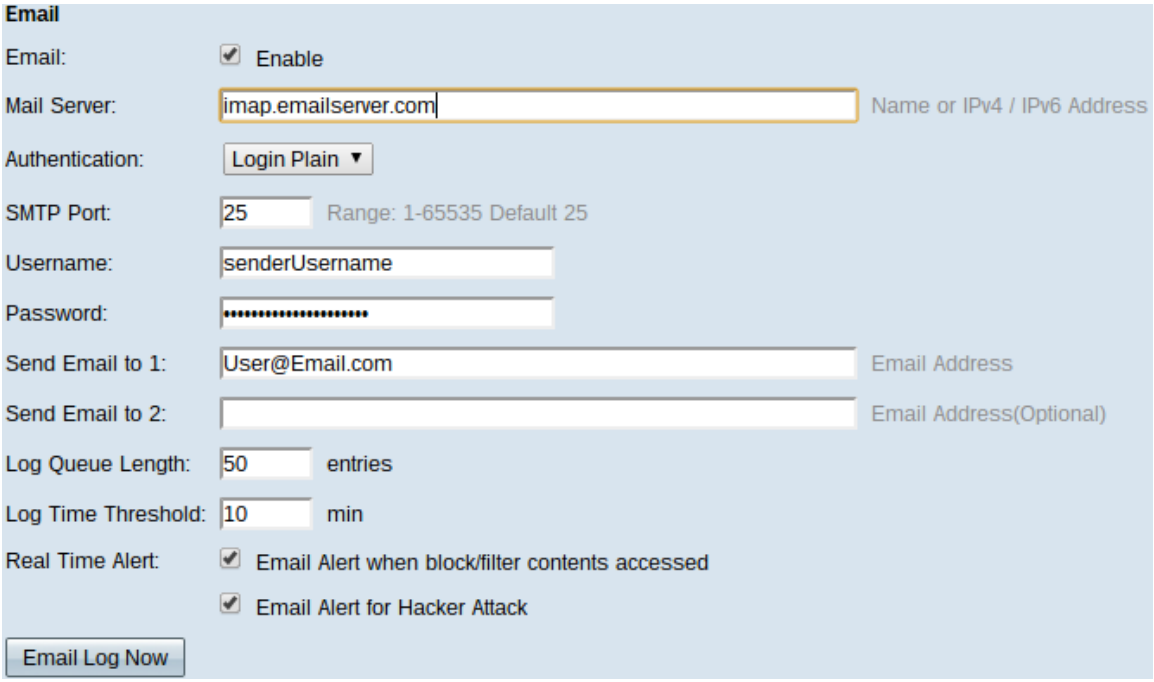
步驟3.（可選）要將日誌傳送到另一個系統日誌伺服器，請在Syslog2欄位中選中**Enable**。

步驟4.如果在Syslog2欄位中選中此覈取方塊，請在Syslog伺服器2欄位中輸入系統日誌伺服器

的主機名或IP地址。

步驟5.按一下**Save**。已配置通過系統日誌伺服器的系統日誌。

電子郵件系統日誌



步驟1.選中Email欄位中的**Enable**，以通過電子郵件向收件人傳送系統日誌。

步驟2.在「郵件伺服器」欄位中輸入郵件伺服器的域名或IP地址。

步驟3.在Authentication欄位中選擇郵件伺服器使用的身份驗證型別。

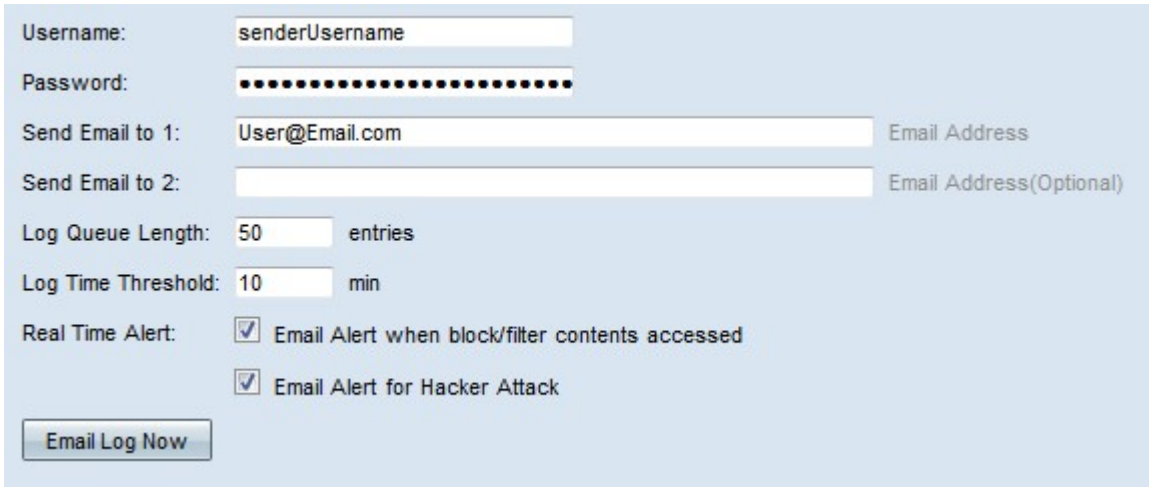
·無 — 郵件伺服器不使用身份驗證。

·純登入 — 郵件伺服器使用純文字檔案格式的身份驗證。

·TLS — 郵件伺服器使用傳輸層安全(TLS)以允許客戶端和伺服器安全地交換身份驗證資訊。

·SSL — 郵件伺服器使用安全套接字層(SSL)允許客戶端和伺服器安全地交換身份驗證資訊。

步驟4.在「SMTP埠」欄位中輸入郵件伺服器使用的簡單郵件傳輸協定(SMTP)埠。SMTP是一種允許通過IP網路傳輸電子郵件的協定。



步驟5.在「使用者名稱」欄位中輸入電子郵件發件人的使用者名稱。

步驟6.在「密碼」欄位中輸入電子郵件發件人的密碼。

步驟7.在「將電子郵件傳送到1」欄位中輸入電子郵件收件人的電子郵件地址。

步驟8。（可選）在Send Email to 2（將電子郵件傳送到2）欄位中輸入要將日誌電子郵件傳送到的其他電子郵件地址。

步驟9.在「日誌隊列長度」欄位中輸入在將日誌傳送到電子郵件收件人之前必須建立的日誌條目數。

步驟10.在Log Time Threshold欄位中輸入裝置將日誌傳送到電子郵件的間隔。

步驟11.選中Real Time Alert欄位的第一個覈取方塊，以便在被阻止或過濾的人嘗試訪問路由器時立即傳送電子郵件。

步驟12.選中Real Time Alert欄位的第二個覈取方塊，以便在駭客嘗試通過拒絕服務(DOS)攻擊訪問路由器時立即傳送電子郵件。

附註：按一下**Email Log Now**立即傳送日誌。

步驟13.按一下**「Save」**。已配置通過電子郵件的系統日誌。

日誌設定

步驟1.選中將觸發日誌條目的事件的覈取方塊。

·警報日誌 — 在發生攻擊或嘗試的攻擊時建立這些日誌。

- Syn泛洪 — 接收SYN請求的速度比路由器處理它們的速度更快。

- IP欺騙 — RV320已收到具有偽造源IP地址的IP資料包。

— 未經授權的登入嘗試 — 登入網路的被拒絕嘗試失敗。

- Ping of Death — 向介面傳送了大小異常的ping，試圖使目標裝置崩潰。

- Win Nuke — 名為WinNuke的遠端分散式拒絕服務攻擊(DDOS)已傳送到介面，試圖使目標裝置崩潰。

·常規日誌 — 這些日誌是在發生常規網路操作時建立的。

— 拒絕策略 — 已根據路由器的已配置策略拒絕使用者訪問。

— 授權登入 — 使用者已被授權訪問網路。

— 系統錯誤消息 — 發生系統錯誤。

— 允許策略 — 已根據路由器的已配置策略向使用者授予訪問許可權。

— 核心 — 在日誌中包括所有核心消息。核心是作業系統啟動時載入到記憶體的第一部分。核心消息是與核心關聯的日誌。

— 配置更改 — 路由器配置已修改。

- IPSEC和PPTP VPN — 發生IPSEC和PPTP VPN協商、連線或斷開連線。

- SSL VPN — 發生SSL VPN協商、連線或斷開連線。

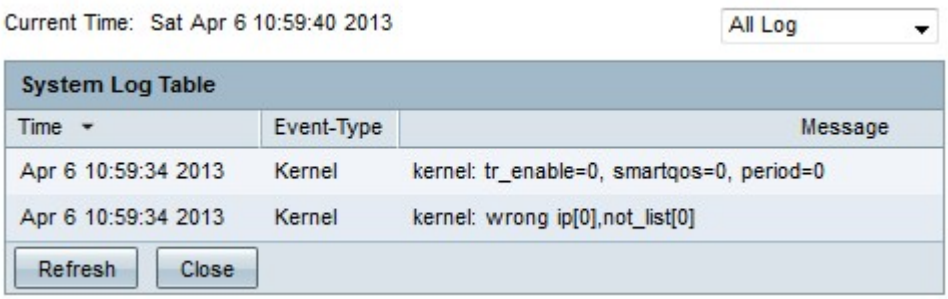
— 網路 — WAN或DMZ介面上已建立或丟失物理連線。

步驟2.按一下「**Save**」。日誌設定已配置。

附註：按一下**Clear Log**以清除當前日誌。

檢視系統日誌

步驟1.按一下**檢視系統日誌**以檢視系統日誌表。出現*System Log Table*視窗。



步驟2.（可選）從下拉選單中選擇要檢視的日誌型別。

·所有日誌 — 包括所有日誌消息。

·系統日誌 — 僅包括系統錯誤消息。

·防火牆/DoS日誌 — 僅包括警報日誌。

·VPN日誌 — 僅包括IPSec和PPTP VPN以及SSL VPN日誌。

·網路日誌 — 僅包括網路日誌。

·核心日誌 — 僅包括核心消息。

·使用者日誌 — 僅包括拒絕策略、允許策略、授權登入和配置更改日誌

·SSL日誌 — 僅包括SSL VPN日誌。

系統日誌表顯示以下資訊。

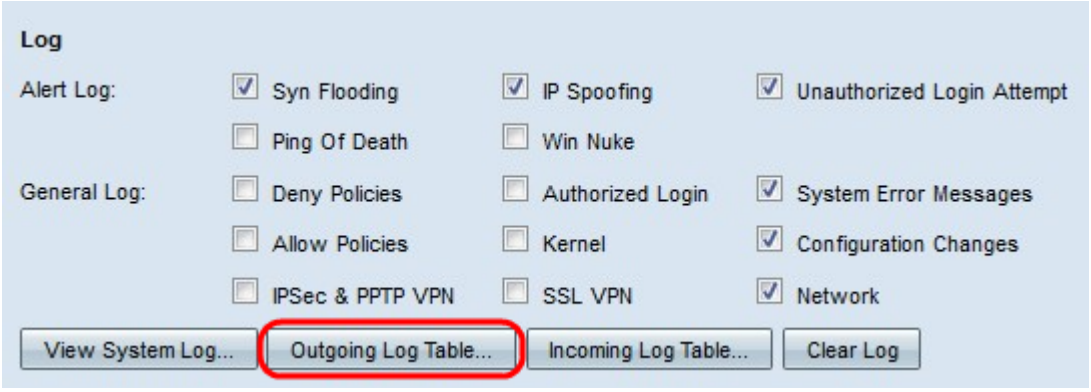
·時間 — 建立日誌的時間。

·事件型別 — 日誌的型別。

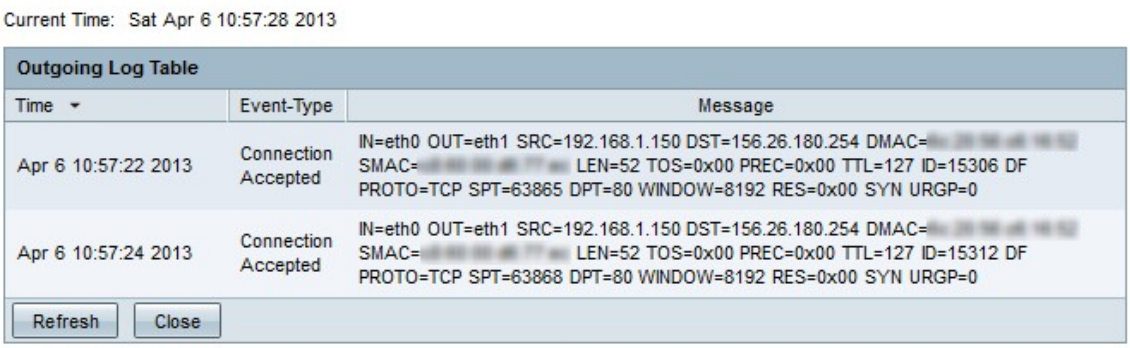
·消息 — 與日誌對應的資訊。這包括策略型別、源IP地址和源MAC地址。

附註：按一下**刷新**以刷新日誌表。

檢視傳出日誌表



步驟1.按一下**傳出日誌表**以檢視僅與傳出資料包相關的日誌表。出現*Outgoing Log Table*視窗。



傳出日誌表顯示以下資訊。

·時間 — 建立日誌的時間。

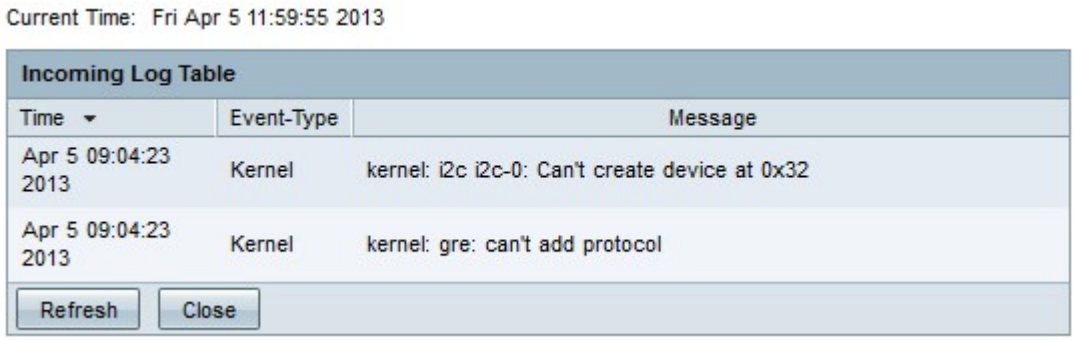
·事件型別 — 日誌的型別。

·消息 — 與日誌對應的資訊。這包括策略型別、源IP地址和源MAC地址。

附註：按一下**刷新**以刷新日誌表。

檢視傳入日誌表

步驟1.按一下**Incoming Log Table**以檢視僅與傳入資料包相關的日誌表。出現*Incoming Log Table*視窗。



傳入日誌表顯示以下資訊。

·時間 — 建立日誌的時間。

·事件型別 — 日誌的型別。

·消息 — 與日誌對應的資訊。這包括策略型別、源IP地址和源MAC地址。

附註：按一下**刷新**以刷新日誌表。