Configurazione del registro di sistema sulla serie RV320 e RV325 VPN Router

Obiettivo

I registri di sistema sono record di eventi di rete. I registri sono uno strumento importante utilizzato per comprendere il funzionamento di una rete. Sono utili per la gestione e la risoluzione dei problemi di rete.

In questo articolo viene spiegato come configurare i tipi di log da registrare, come visualizzare i log sulla serie RV32x VPN Router e come inviare i log a un destinatario tramite SMS, a un server di log di sistema o a un destinatario tramite e-mail.

Dispositivi interessati

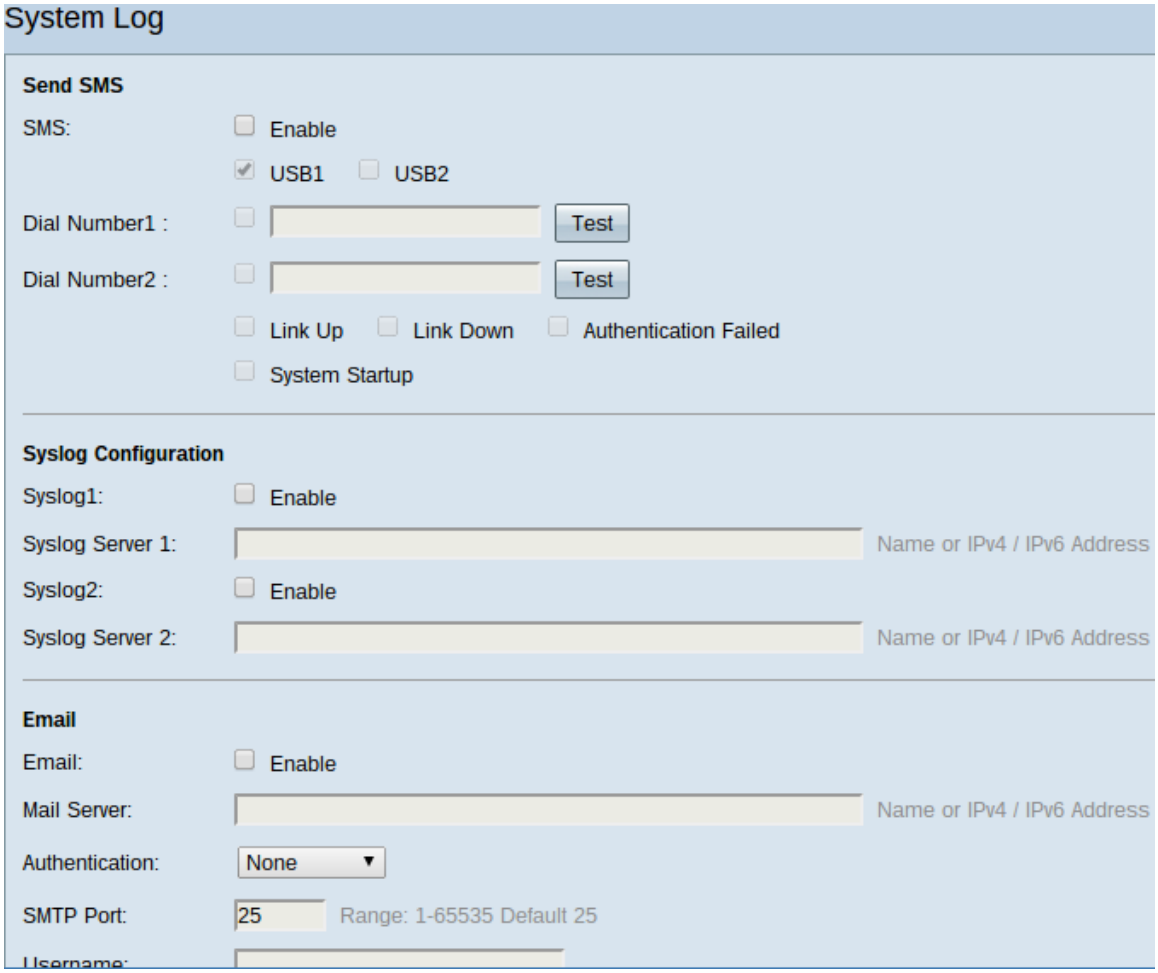
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

Versione del software

·v1.1.0.09

Configurazione registro di sistema

Passaggio 1. Accedere all'utilità Configurazione Web e scegliere **Log > Log di sistema**. Viene visualizzata la pagina *Log di sistema*:



Fare riferimento alle sezioni seguenti per informazioni sulla pagina *Log di sistema*.

·Registri di sistema via SMS — Come inviare i registri di sistema a un telefono tramite SMS.

·Log di sistema sui server di log di sistema — Spiega come inviare i log di sistema a un server di log di sistema.

·Registri di sistema via e-mail — Come inviare i registri di sistema a un indirizzo e-mail.

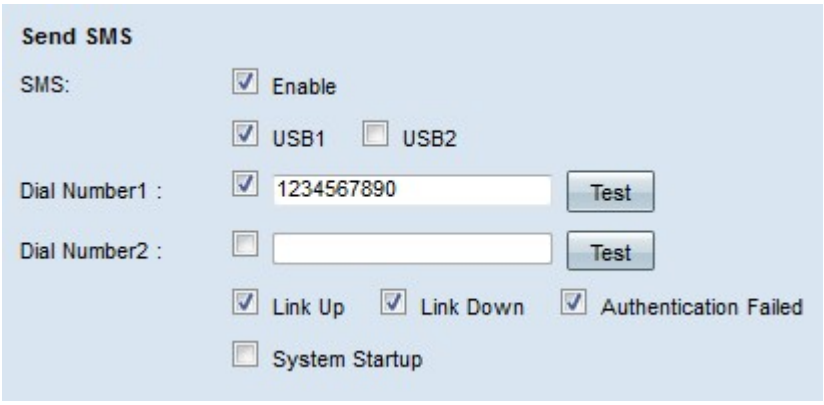
·Log Settings (Impostazioni registro) — Spiega come configurare il tipo di messaggi salvati nel registro.

·View System Log — Spiega come visualizzare i log di sistema sul dispositivo.

·View Outgoing Log Table: visualizza i log di sistema relativi solo ai pacchetti in uscita.

·View Incoming Log Table: visualizza i log di sistema relativi solo ai pacchetti in arrivo.

Registri di sistema tramite SMS



Passaggio 1. Selezionare **Abilita** nel campo SMS per inviare i log di sistema a un client tramite messaggi SMS (Short Message Service).

Passaggio 2. Selezionare le caselle di controllo delle porte USB a cui è collegato il modem 3G USB.

Passaggio 3. Selezionare la casella di controllo nel campo Componi numero1 e immettere il numero di telefono a cui inviare i messaggi.

Nota: Fare clic su **Test** per verificare la connessione al numero 1. Se il numero configurato non riceve il messaggio di prova, verificare che il numero di telefono sia stato immesso correttamente nel campo Dial Number1.

Passaggio 4. (Facoltativo) Selezionare la casella di controllo nel campo Componi numero2 e immettere il numero di telefono a cui inviare i messaggi.

Nota: Fare clic su **Test** per verificare la connessione al numero 2. Se il numero configurato non riceve il messaggio di prova, verificare che il numero di telefono sia stato immesso correttamente nel campo Dial Number2.

Passaggio 5. Selezionare le caselle di controllo degli eventi che attiveranno l'invio di un registro.

·Link Up: è stata attivata una connessione con RV320.

·Link Down: una connessione con RV320 è stata interrotta.

·Autenticazione non riuscita: un'autenticazione non è riuscita.

·Avvio del sistema — Il router viene avviato.

Passaggio 6. Fare clic su **Salva**. I registri di sistema tramite SMS sono configurati.

Log di sistema su server di log di sistema

Passaggio 1. Selezionare **Enable** nel campo Syslog1 per inviare i log di sistema a un server di log del sistema.

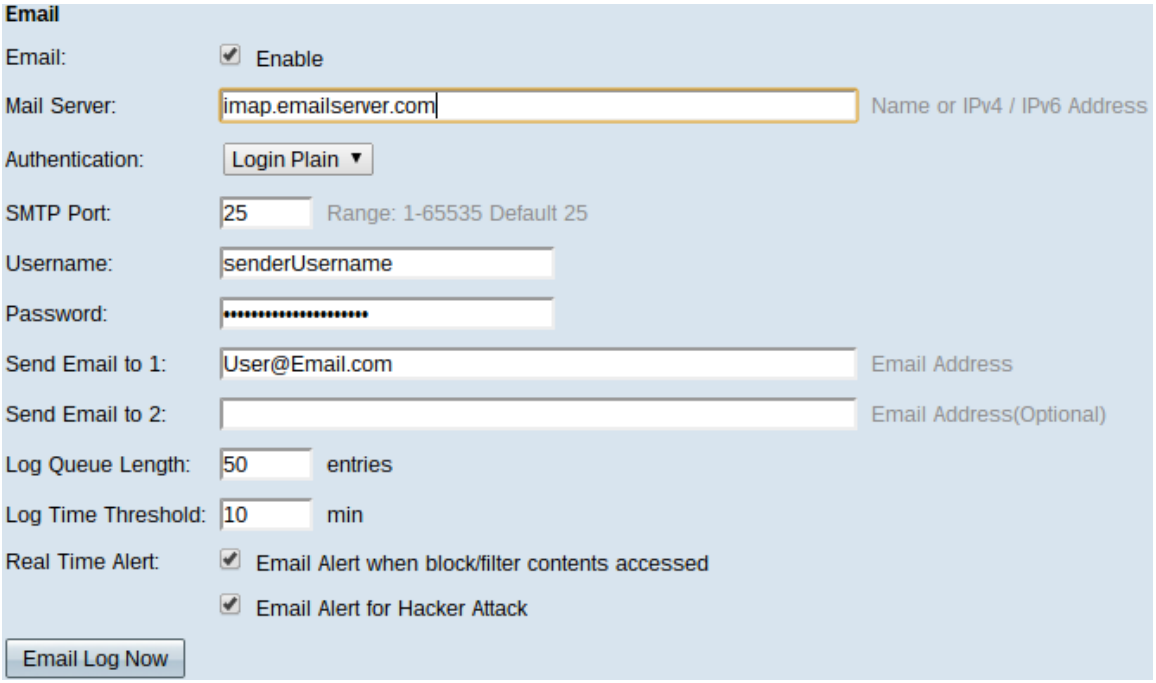
Passaggio 2. Immettere il nome host o l'indirizzo IP del server di log del sistema nel campo Syslog Server 1.

Passaggio 3. (Facoltativo) Per inviare i log a un altro server di log del sistema, selezionare **Abilita** nel campo Syslog2.

Passaggio 4. Se la casella di controllo è selezionata nel campo Syslog2, immettere il nome host o l'indirizzo IP del server di log del sistema nel campo Syslog Server 2.

Passaggio 5. Fare clic su **Salva**. Log di sistema configurati tramite server di log di sistema.

Log di sistema e-mail



Passaggio 1. Selezionare **Abilita** nel campo Posta elettronica per inviare i log di sistema a un destinatario tramite posta elettronica.

Passaggio 2. Immettere il nome di dominio o l'indirizzo IP del server di posta nel campo Server di posta.

Passaggio 3. Scegliere il tipo di autenticazione utilizzato dal server di posta nel campo Autenticazione.

·Nessuno: il server di posta non utilizza l'autenticazione.

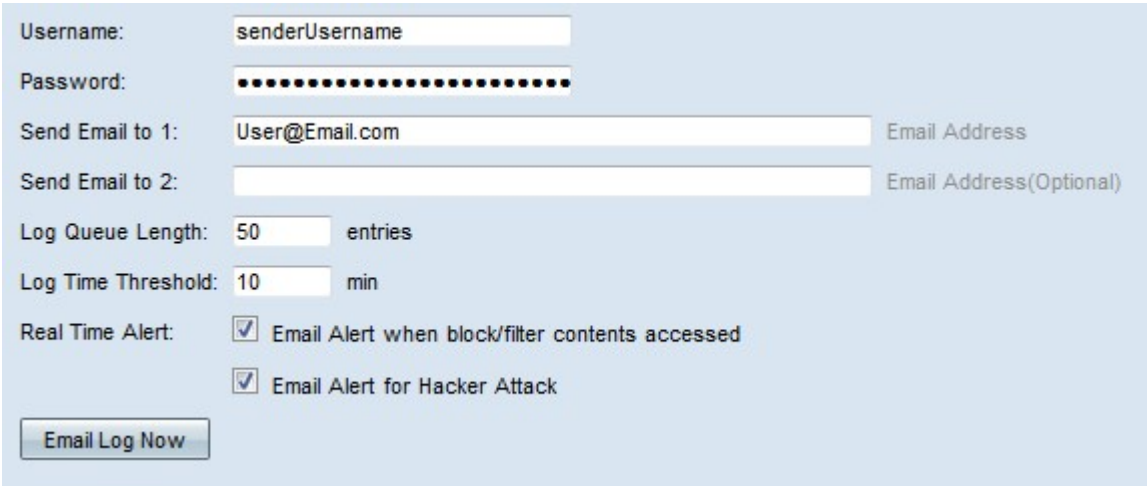
·Login Plain: il server di posta utilizza l'autenticazione in formato testo normale.

·TLS: il server di posta utilizza TLS (Transport Layer Security) per consentire al client e al server di scambiare le informazioni di autenticazione in modo sicuro.

·SSL: il server di posta utilizza Secure Sockets Layer (SSL) per consentire al client e al server di scambiare le informazioni di autenticazione in modo sicuro.

Passaggio 4. Immettere la porta SMTP (Simple Mail Transfer Protocol) utilizzata dal server

di posta nel campo Porta SMTP. SMTP è un protocollo che consente la trasmissione di e-mail su reti IP.



Passaggio 5. Immettere il nome utente del mittente e-mail nel campo Nome utente.

Passaggio 6. Immettere la password del mittente e-mail nel campo Password.

Passaggio 7. Immettere l'indirizzo e-mail del destinatario nel campo Invia e-mail a 1.

Passaggio 8. (Facoltativo) Immettere un indirizzo e-mail aggiuntivo a cui inviare i log e-mail nel campo Invia e-mail a 2.

Passaggio 9. Immettere il numero di voci di log da inserire prima che il log venga inviato al destinatario e-mail nel campo Lunghezza coda log.

Passaggio 10. Immettere l'intervallo con cui il dispositivo invia il log al messaggio di posta elettronica nel campo Soglia tempo di log.

Passaggio 11. Selezionare la prima casella di controllo del campo Avviso in tempo reale per inviare immediatamente un messaggio e-mail quando qualcuno, che è stato bloccato o filtrato, tenta di accedere al router.

Passaggio 12. Selezionare la seconda casella di controllo del campo Real Time Alert per inviare immediatamente un messaggio di posta elettronica quando un hacker tenta di accedere al router tramite un attacco Denial of Service (DOS).

Nota: Fare clic su **Invia log per posta elettronica ora** per inviare immediatamente il log.

Passaggio 13. Fare clic su **Salva**. Registri di sistema tramite posta elettronica configurati.

Impostazioni registro

Passaggio 1. Selezionare le caselle di controllo degli eventi che attiveranno una voce del registro.

·Alert Log: questi log vengono creati quando si verifica un attacco o un tentativo di attacco.

- Syn Flooding: le richieste SYN vengono ricevute più rapidamente di quanto il router sia in grado di elaborarle.

- Spoofing IP: RV320 ha ricevuto pacchetti IP con indirizzi IP di origine contraffatti.

- Tentativo di accesso non autorizzato - Tentativo di accesso alla rete rifiutato non riuscito.

- Ping of Death (Ping della morte) - Un ping di dimensioni anomale è stato inviato a un'interfaccia nel tentativo di bloccare il dispositivo di destinazione.

- Win Nuke - L'attacco DDOS (Distributed Denial of Service Attack) remoto noto come WinNuke è stato inviato a un'interfaccia nel tentativo di arrestare il dispositivo di destinazione.

·Registro generale: questi registri vengono creati quando si verificano azioni generali di rete.

- Criteri di negazione - L'accesso è stato negato a un utente in base ai criteri configurati del router.

- Login autorizzato — Un utente è stato autorizzato ad accedere alla rete.

- Messaggi di errore di sistema - Si è verificato un errore di sistema.

- Consenti criteri - L'accesso è stato concesso a un utente in base ai criteri configurati del router.

- Kernel: include tutti i messaggi del kernel nel log. Il kernel è la prima parte del sistema operativo che viene caricata in memoria all'avvio. I messaggi del kernel sono log associati al kernel.

- Modifiche alla configurazione - La configurazione del router è stata modificata.

- VPN IPSEC & PPTP: negoziazione, connessione o disconnessione di una VPN IPSEC & PPTP.

- SSL VPN: negoziazione, connessione o disconnessione VPN SSL.

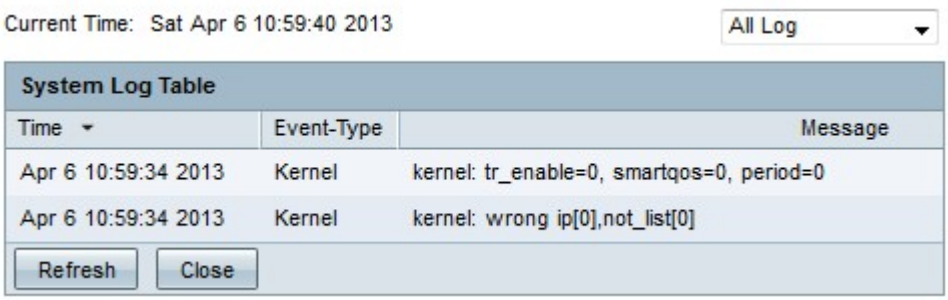
- Rete - È stata stabilita o persa una connessione fisica sulle interfacce WAN o DMZ.

Passaggio 2. Fare clic su **Salva**. Le impostazioni del registro sono configurate.

Nota: Fare clic su **Cancella registro** per cancellare il registro corrente.

Visualizza registro eventi di sistema

Passaggio 1. Fare clic su **Visualizza registro di sistema** per visualizzare la tabella del registro di sistema. Viene visualizzata la finestra *System Log Table* (Tabella registro di sistema).



Passaggio 2. (Facoltativo) Dall'elenco a discesa scegliere il tipo di log da visualizzare.

·Tutti i log - Include tutti i messaggi di log.

·Registro di sistema - Include solo i messaggi di errore del sistema.

·Registro DoS/firewall: include solo gli alert log.

·Registro VPN: include solo i registri VPN IPSec e PPTP e SSL.

·Registro di rete: comprende solo i registri di rete.

·Registro kernel: include solo i messaggi del kernel.

·Log utente: include solo le policy di negazione, le policy di autorizzazione, l'accesso autorizzato e i log delle modifiche alla configurazione

·Log SSL: include solo i log VPN SSL.

La tabella Log di sistema visualizza le informazioni riportate di seguito.

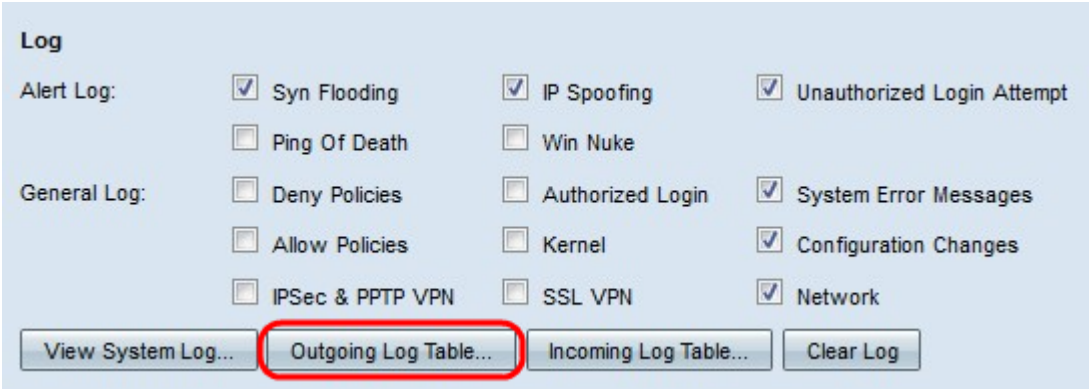
·Ora: l'ora di creazione del log.

·Event-Type: il tipo di registro.

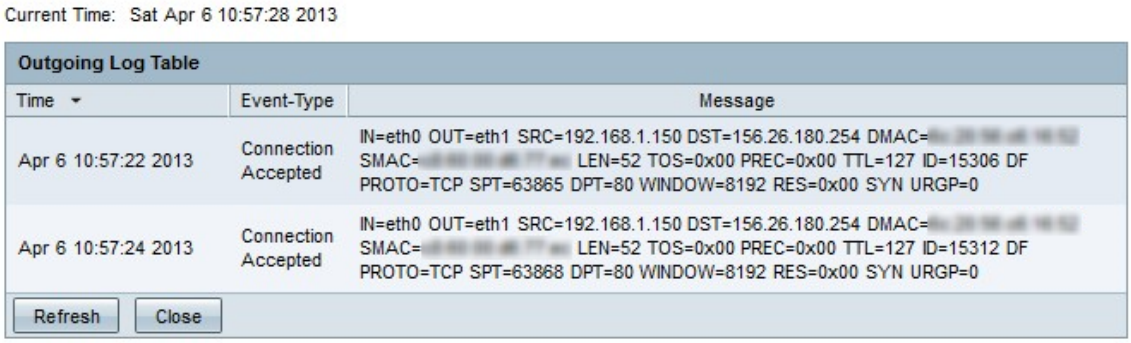
·Messaggio - Informazioni che corrispondono al registro. Sono inclusi il tipo di criterio, l'indirizzo IP di origine e l'indirizzo MAC di origine.

Nota: Fare clic su **Aggiorna** per aggiornare la tabella di registro.

Visualizza tabella log in uscita



Passaggio 1. Fare clic su **Tabella log in uscita** per visualizzare la tabella di log correlata solo ai pacchetti in uscita. Viene visualizzata la finestra *Tabella log in uscita*.



Nella tabella Registro in uscita vengono visualizzate le informazioni seguenti.

·Ora: l'ora di creazione del log.

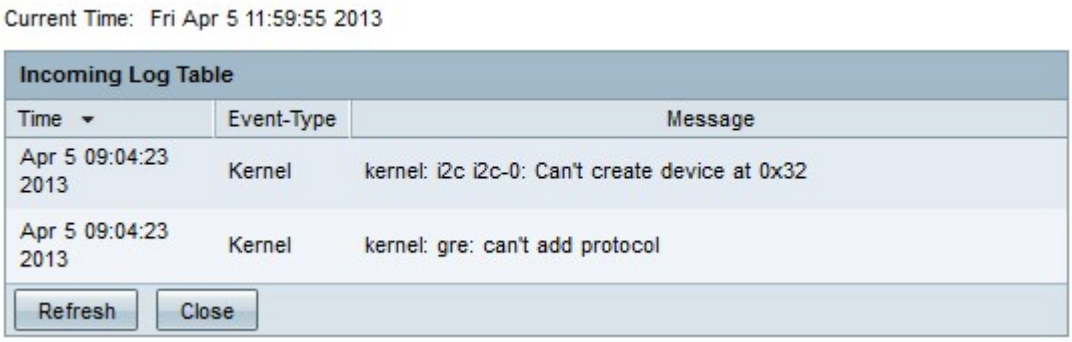
·Event-Type: il tipo di registro.

·Messaggio - Informazioni che corrispondono al registro. Sono inclusi il tipo di criterio, l'indirizzo IP di origine e l'indirizzo MAC di origine.

Nota: Fare clic su **Aggiorna** per aggiornare la tabella di registro.

Visualizza tabella registro in ingresso

Passaggio 1. Fare clic su **Tabella registro in ingresso** per visualizzare la tabella di registro relativa solo ai pacchetti in ingresso. Viene visualizzata la finestra *Tabella registro in entrata*.



Nella tabella Registro in ingresso vengono visualizzate le informazioni seguenti.

·Ora: l'ora di creazione del log.

·Event-Type: il tipo di registro.

·Messaggio - Informazioni che corrispondono al registro. Sono inclusi il tipo di criterio, l'indirizzo IP di origine e l'indirizzo MAC di origine.

Nota: Fare clic su **Aggiorna** per aggiornare la tabella di registro.