Configurazione del registro di sistema sui router VPN RV016, RV042, RV042G e RV082

Obiettivo

Per registrare i dati del computer viene utilizzato un registro di sistema (Syslog). È possibile definire le istanze che genereranno un registro. Ogni volta che si verifica un'istanza, l'ora e l'evento vengono registrati e inviati a un server syslog o in un messaggio di posta elettronica. Syslog può quindi essere utilizzato per analizzare e risolvere i problemi di una rete e per aumentare la sicurezza della rete.

Questo documento spiega la procedura per configurare un server Syslog su router VPN RV016, RV042, RV042G e RV082.

Dispositivi interessati

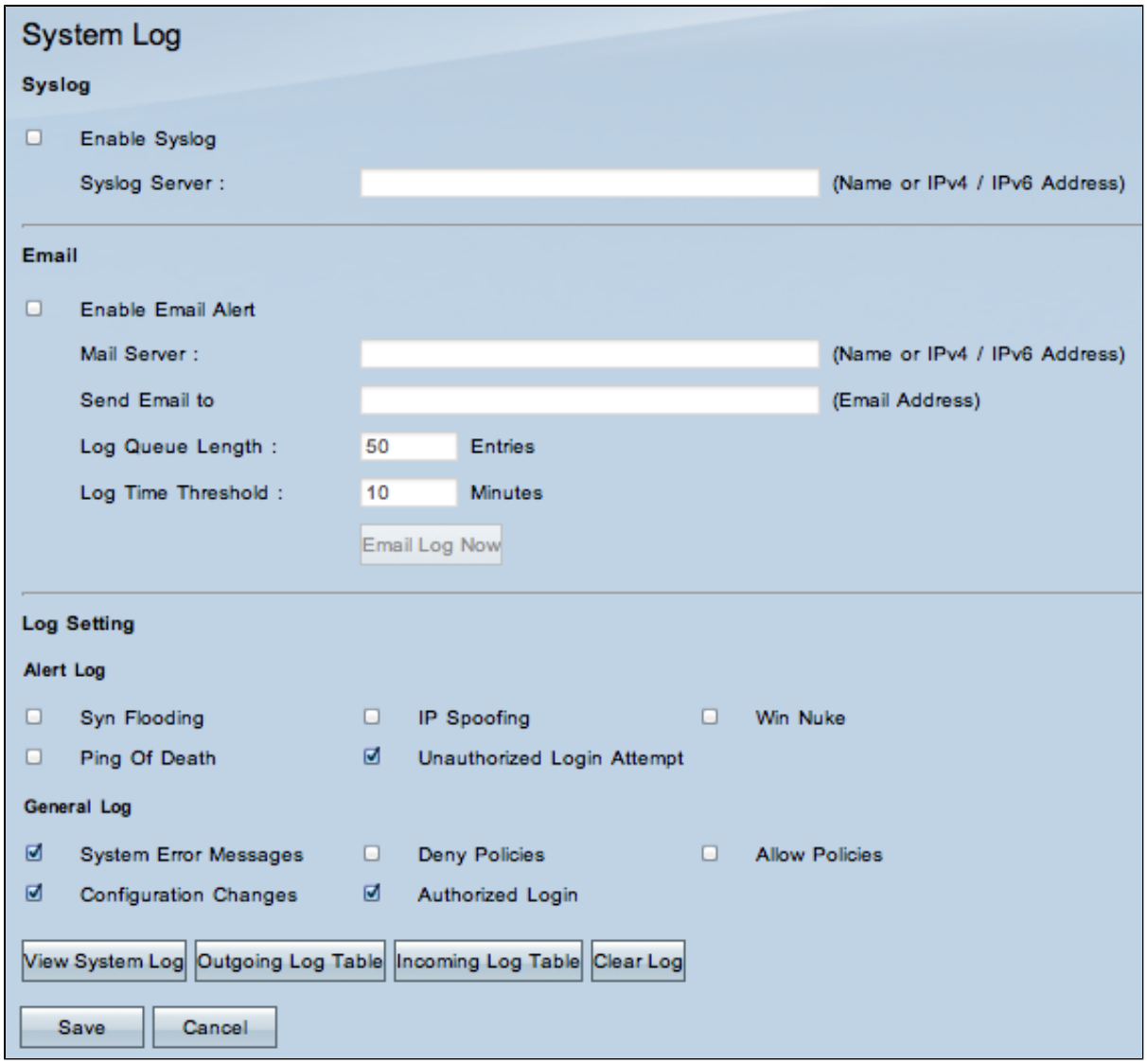
· RV016
RV042
RV042G
RV082

Versione del software

· v4.2.1.02

Configurazione di syslog e avvisi

Passaggio 1. Accedete all'utility di configurazione Web e scegliete **Log > Log di sistema**. Viene visualizzata la pagina *Log di sistema*:



Syslog

Questa sezione spiega come abilitare il router per inviare file di registro dettagliati al server syslog quando vengono registrati gli eventi.

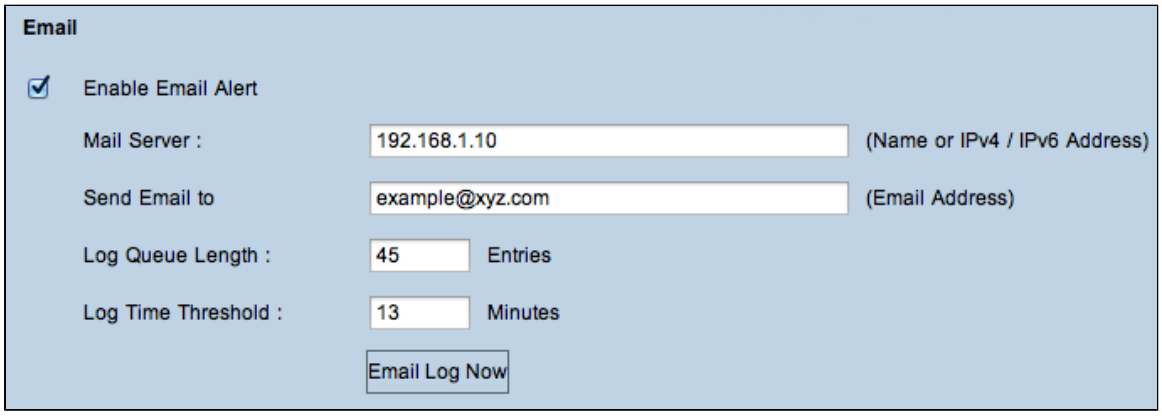
Passaggio 2. Selezionare la casella di controllo **Attiva syslog** per attivare il servizio syslog sul dispositivo.

Timesaver: passare al punto 4 se Syslog deve essere disabilitato.

Passaggio 3. Immettere il nome di dominio o l'indirizzo IP del server syslog nel campo Server syslog.

Email

Questa sezione spiega come abilitare il router all'invio di avvisi e-mail quando vengono registrati gli eventi.



Passaggio 4. Selezionare **Abilita avviso e-mail** per abilitare la funzione. In questo modo il router può inviare avvisi e-mail all'indirizzo e-mail specificato dall'utente.

Timesaver: passare al punto 10 se è necessario disabilitare l'avviso e-mail.

Passaggio 5. Immettere l'indirizzo IPv4 o IPv6 del server SMTP dell'ISP nel campo Mail Server.

Nota: l'ISP potrebbe richiedere l'identificazione del router con un nome host. Scegliere **Setup > Network** (Configurazione > Rete) per definire il nome host del router.

Passaggio 6. Immettere l'indirizzo di posta elettronica a cui si desidera inviare gli avvisi nel campo Invia e-mail a.

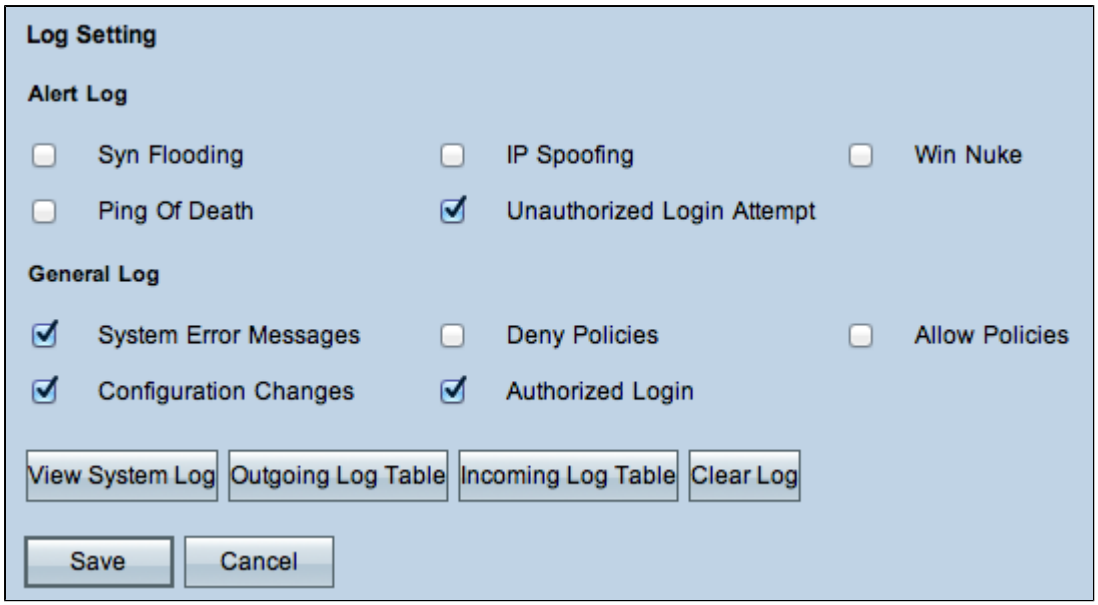
Passaggio 7. Immettere il numero di voci di log da includere nel messaggio e-mail nel campo Lunghezza coda log. Il valore predefinito è 50.

Passaggio 8. Immettere il numero di minuti per la raccolta dei dati prima dell'invio del registro nel campo Soglia tempo registro. La soglia del tempo di registrazione è il tempo massimo di attesa prima dell'invio di un messaggio di log e-mail. Alla scadenza della soglia di tempo di log, viene inviato un messaggio di posta elettronica indipendentemente dal fatto che il buffer di log della posta elettronica sia pieno o meno. L'impostazione predefinita è 10 minuti

Passaggio 9. (Facoltativo) Fare clic su **Invia registro e-mail ora** per inviare istantaneamente un messaggio all'indirizzo e-mail specificato per verificare le impostazioni.

Impostazione registro

In questa sezione viene illustrata la varietà di eventi che è possibile segnalare nei registri:



Passaggio 10. L'area Alert Log contiene tipi comuni di attacchi e tentativi di accesso non autenticati. Selezionare le caselle di controllo relative a qualsiasi tipo di attacco desiderato per includerlo nel registro eventi oppure deselezionarle per escluderlo dal registro eventi.

· SYN Flooding: l'utente malintenzionato invia molti pacchetti SYNC in modo continuo, il che fa sì che il router apra più sessioni in modo che il traffico diventi molto sovraccarico e che il router neghi il traffico legittimo.

· Spoofing IP: l'utente malintenzionato invia pacchetti da un falso indirizzo IP di origine per far apparire l'attacco come traffico legittimo.

· Win Nuke - L'aggressore invia un messaggio fuori banda a un computer Windows per arrestare il computer di destinazione.

· Ping of Death (Ping della morte) - L'aggressore invia un pacchetto IP di grandi dimensioni per arrestare il computer di destinazione.

· Tentativo di accesso non autorizzato: un utente ha tentato di accedere all'utilità di configurazione del router senza autenticazione corretta.

Passaggio 11. L'area Registro generale include le azioni eseguite per applicare i criteri configurati, nonché gli eventi di routine quali gli accessi autorizzati e le modifiche alla configurazione. Selezionare la casella di controllo di qualsiasi evento desiderato per includerlo nel registro generale. Deselezionare la casella di controllo per omettere la voce dal registro generale.

· Messaggi di errore di sistema â€" Tutti i messaggi di errore di sistema.

· Regole di negazione: istanze del router a cui è stato negato l'accesso in base alle regole di accesso specificate.

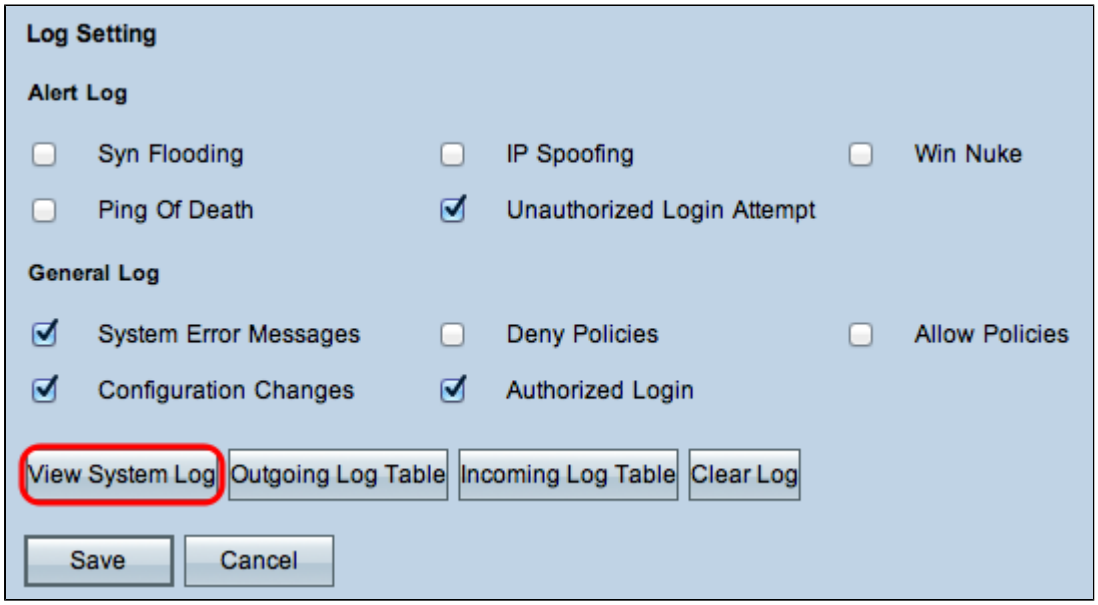
· Consenti regole: istanze quando il router ha consentito l'accesso in base alle regole di accesso specificate.

· Modifiche alla configurazione - Istanze in cui un utente ha salvato le modifiche alla configurazione.

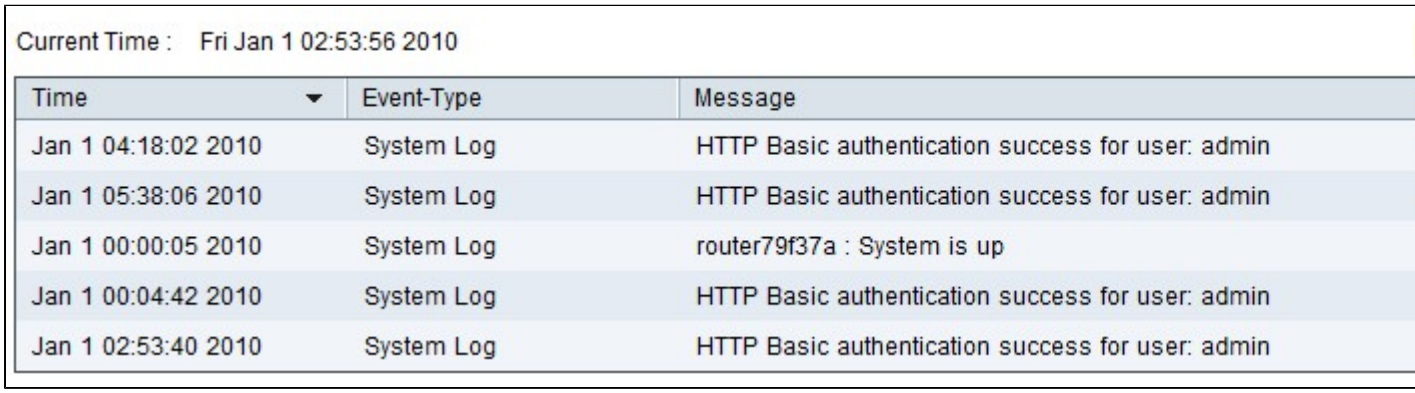
· Accesso autorizzato: si verifica quando qualcuno accede correttamente all'utility di configurazione del router dopo aver immesso il nome utente e la password corretti.

· Evento di blocco dell'output: istanze in cui è presente un evento nella reputazione Web di ProtectLink o nel filtro URL.

Nota: l'evento di blocco output è disponibile solo sui router VPN RV082.



Passaggio 12. (Facoltativo) Per visualizzare il registro eventi di sistema, fare clic su **Visualizza registro eventi di sistema**. Viene visualizzata la finestra *Log di sistema*:



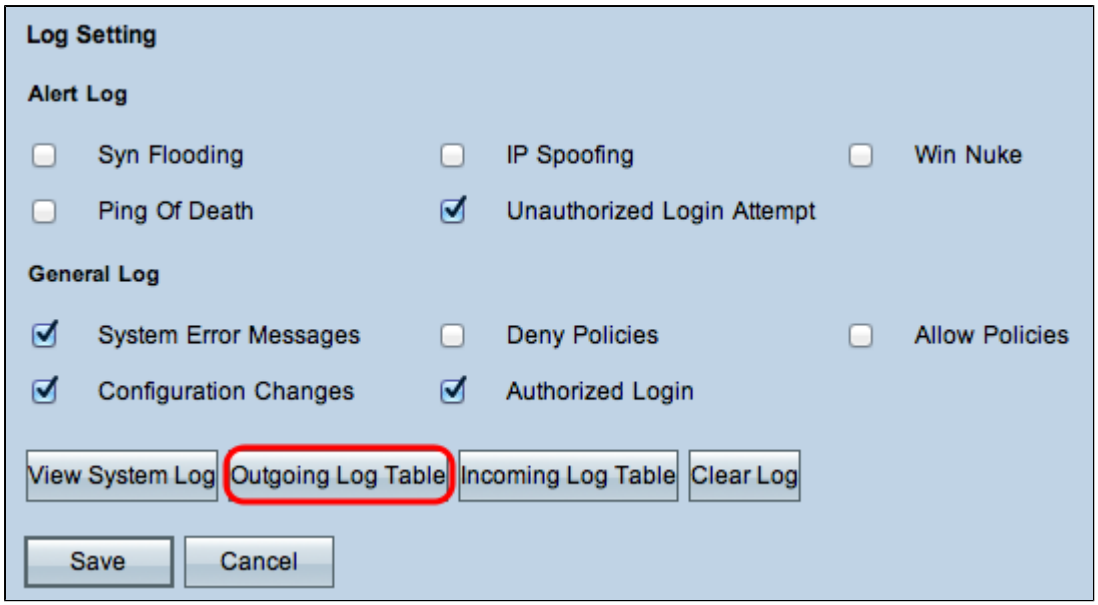
Nota: le voci del log forniscono la data e l'ora del tipo di evento e un messaggio. Questo messaggio indica il tipo di criterio, ad esempio la regola di accesso, l'indirizzo IP LAN dell'origine e l'indirizzo MAC.

Passaggio 13. Scegliere un registro specifico dall'elenco a discesa.

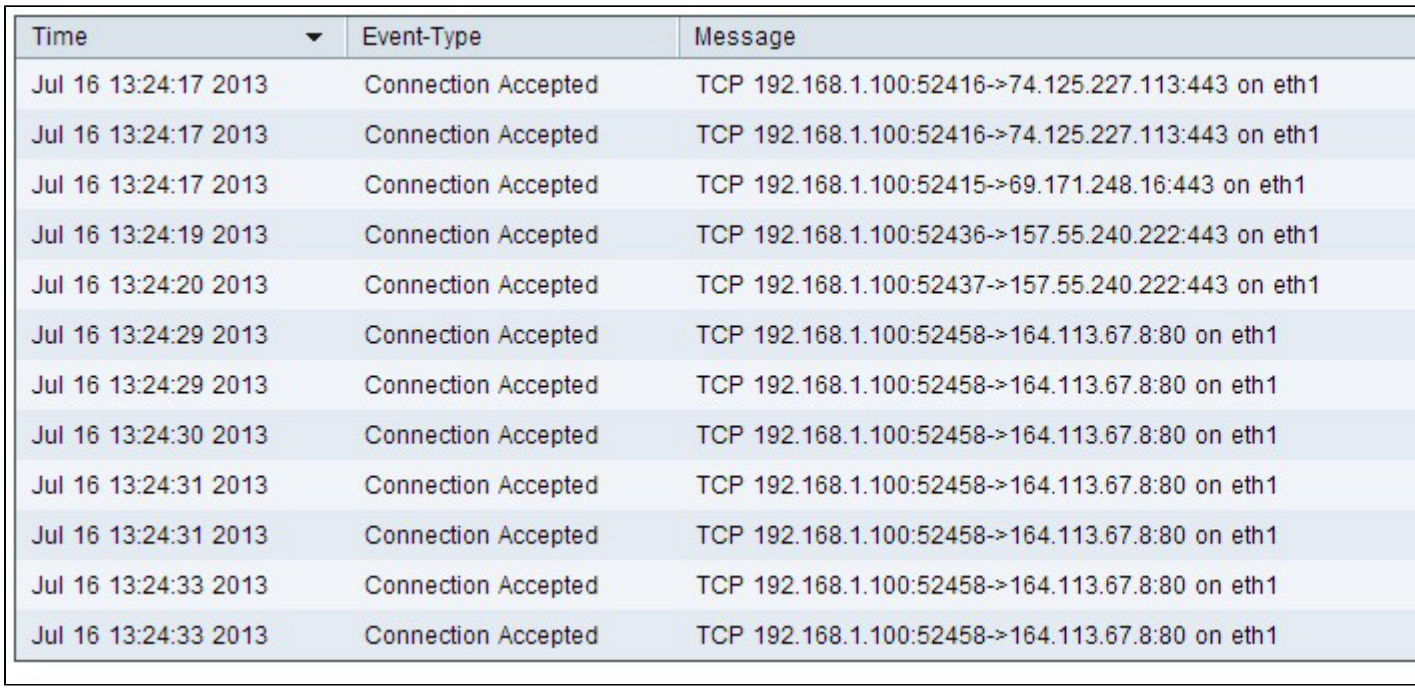
Passaggio 14. (Facoltativo) Per aggiornare i dati, fare clic su **Aggiorna**.

Passaggio 15. (Facoltativo) Per cancellare tutte le informazioni visualizzate, fare clic su **Cancella**.

Passaggio 16. Fare clic su **Chiudi** per chiudere la finestra.



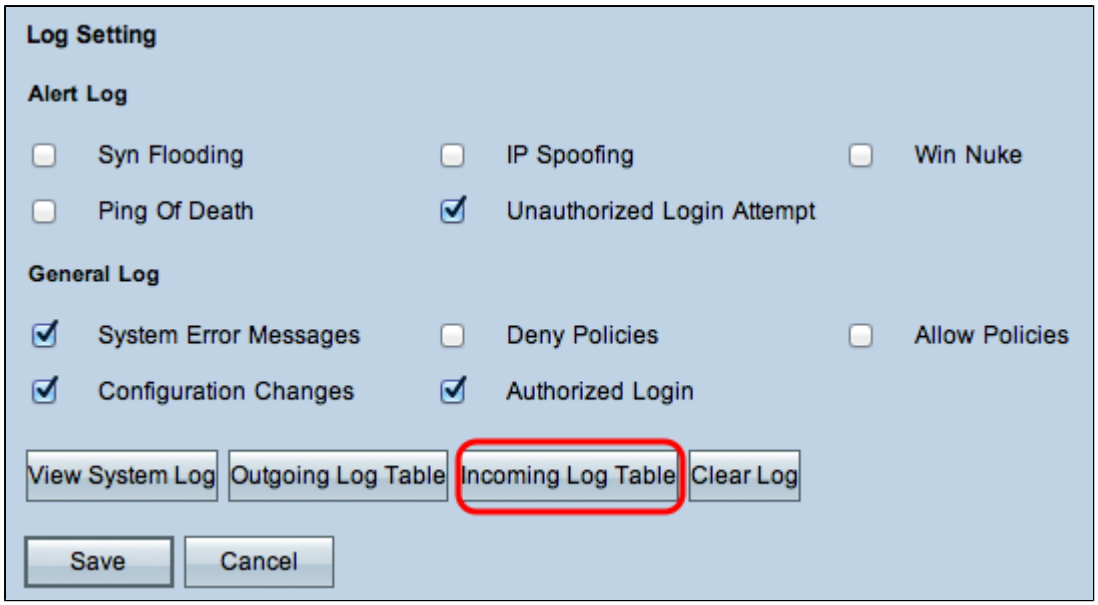
Passaggio 17. (Facoltativo) Per visualizzare le informazioni sui pacchetti in uscita, fare clic su **Tabella log in uscita**. Le informazioni verranno visualizzate in una nuova finestra.



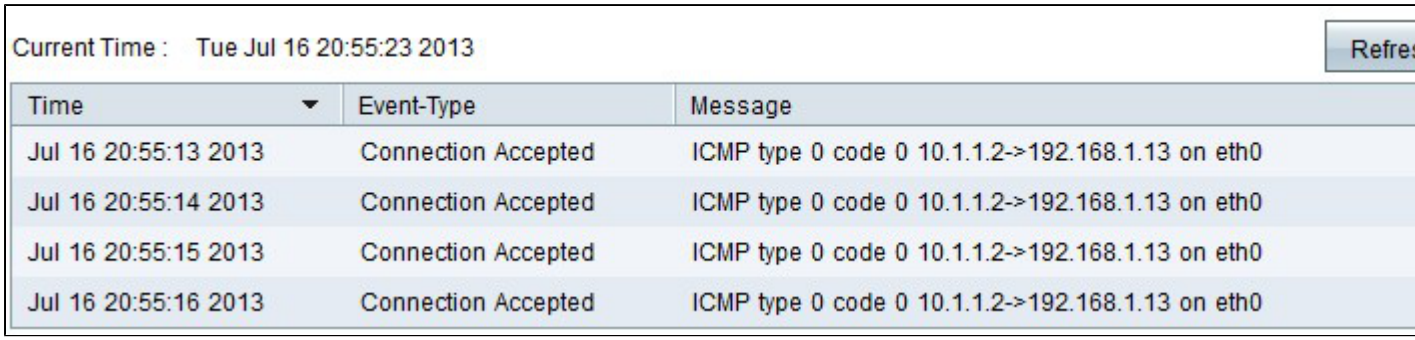
Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
Jul 16 13:24:19 2013	Connection Accepted	TCP 192.168.1.100:52436->157.55.240.222:443 on eth1
Jul 16 13:24:20 2013	Connection Accepted	TCP 192.168.1.100:52437->157.55.240.222:443 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:30 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1

Passaggio 18. (Facoltativo) Per aggiornare i dati, fare clic su **Aggiorna**.

Passaggio 19. Fare clic su **Close** (Chiudi) per chiudere la finestra.

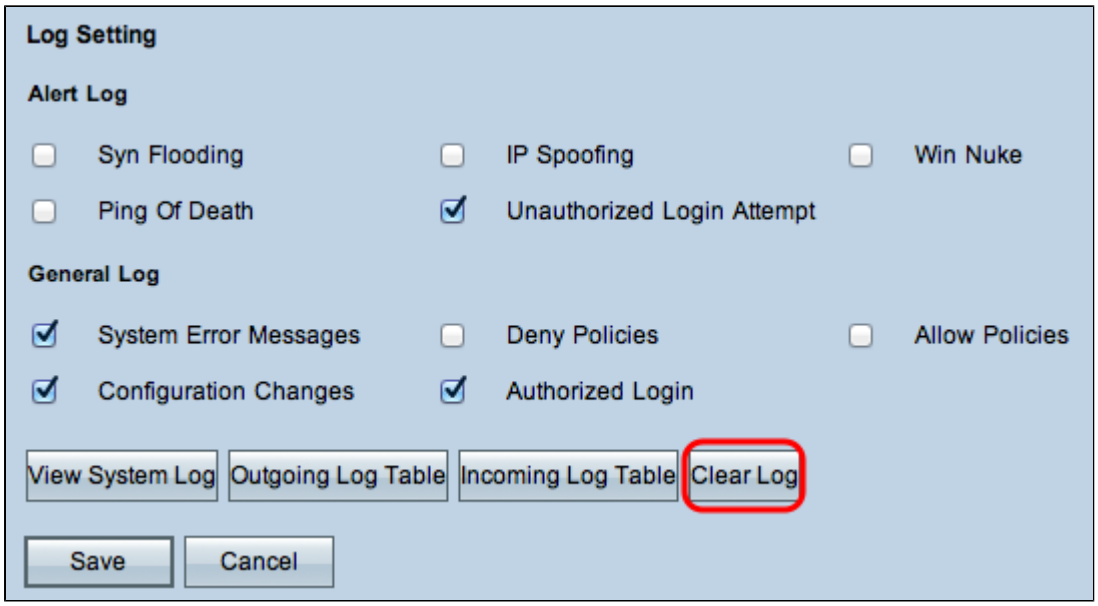


Passaggio 20. (Facoltativo) Fare clic su **Incoming Log Table** per visualizzare le informazioni sui pacchetti in arrivo. Le informazioni vengono visualizzate in una nuova finestra. Se viene visualizzato un avviso relativo alla finestra popup, consentire il contenuto bloccato.



Passaggio 21. (Facoltativo) Per aggiornare i dati, fare clic su **Aggiorna**.

Passaggio 22. Fare clic su **Close** (Chiudi) per chiudere la finestra.



Passaggio 23. (Facoltativo) Per cancellare il registro, fare clic su **Cancella registro ora**. Fare clic su

questo pulsante solo se non è necessario visualizzare nuovamente le informazioni in futuro.

Passaggio 24. Fare clic su **Save** (Salva) per salvare la configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).