

Configurazione del firewall sul router VPN RV315W

Obiettivo

Un firewall crea un bridge tra una rete interna protetta e una rete esterna non protetta. Il firewall controlla l'analisi del traffico di rete in entrata e in uscita dei pacchetti dati. Questo articolo spiega come bloccare diverse funzioni come proxy, cookie, ecc. sul router VPN RV315W.

Dispositivo applicabile

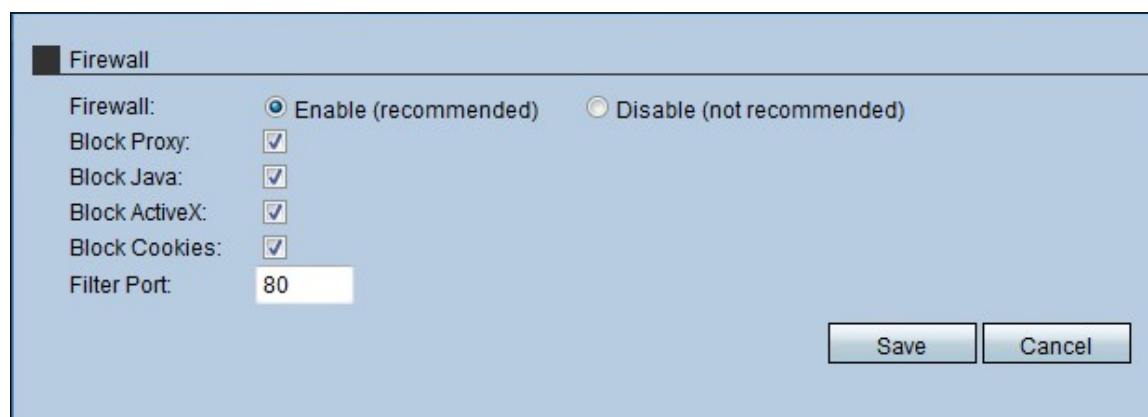
RV315W

Versione del software

•1.01.03

Configurazione firewall

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Firewall**. Viene visualizzata la pagina *Firewall*:



The screenshot shows the Firewall configuration interface. At the top, there is a title bar with a small square icon and the word "Firewall". Below this, the "Firewall:" label is followed by two radio buttons: "Enable (recommended)" which is selected, and "Disable (not recommended)". Underneath, there are four checked checkboxes: "Block Proxy:", "Block Java:", "Block ActiveX:", and "Block Cookies:". Below these is a text input field labeled "Filter Port:" containing the number "80". At the bottom right, there are two buttons: "Save" and "Cancel".

Passaggio 2. Fare clic sul pulsante di opzione **Enable (Abilita)** per abilitare le funzionalità del firewall sull'RV315W.

Nota: I passaggi da 3 a 7 sono facoltativi.

Passaggio 3. Selezionare la casella di controllo **Blocca proxy** per bloccare il proxy sul dispositivo. I server proxy sono server che forniscono un collegamento tra due reti separate. I server proxy dannosi possono registrare tutti i dati non crittografati inviati, ad esempio gli accessi o le password.

Passaggio 4. Selezionare la casella di controllo **Blocca Java** per impedire il download delle applet Java. Java è un linguaggio di programmazione comune utilizzato da molti siti Web. Tuttavia, le applet Java create per scopi dannosi possono rappresentare una minaccia per la sicurezza di una rete. Una volta scaricata, un'applet Java ostile può sfruttare le risorse di rete.

Passaggio 5. Selezionare la casella di controllo **Blocca ActiveX** per impedire il download delle applicazioni ActiveX. ActiveX è un tipo di applet utilizzato da molti siti Web. Anche se in genere sicuro, una volta installata un'applet ActiveX dannosa in un computer, può fare tutto ciò che un utente può fare. Può inserire codice dannoso nel sistema operativo, navigare in una Intranet protetta, cambiare una password o recuperare e inviare documenti.

Passaggio 6. Selezionare la casella di controllo **Blocca cookie** per impedire il download delle applicazioni Cookie. I cookie vengono creati dai siti Web per archiviare informazioni sugli utenti. I cookie possono tenere traccia della cronologia Web dell'utente che può portare a un'invasione della privacy.

Passaggio 7. Immettere il numero di porta utilizzato dal dispositivo per filtrare il traffico HTTP nel campo Porta filtro. Questo controllo del traffico viene eseguito solo sul traffico HTTP. Il protocollo HTTP (HyperText Transfer Protocol) viene utilizzato per accedere e distribuire informazioni su Internet tramite la connessione stabilita dal server e dall'host.

Passaggio 8. Fare clic su **Save** per salvare le modifiche apportate alla configurazione del firewall.