Configurazione delle impostazioni base del firewall su RV215W

Obiettivo

Un firewall è un insieme di funzionalità progettate per mantenere sicura una rete. Un router è considerato un potente firewall hardware. Ciò è dovuto al fatto che i router sono in grado di ispezionare tutto il traffico in entrata e di scaricare qualsiasi pacchetto indesiderato.

Questo articolo spiega come configurare le impostazioni base del firewall su RV215W.

Dispositivi interessati

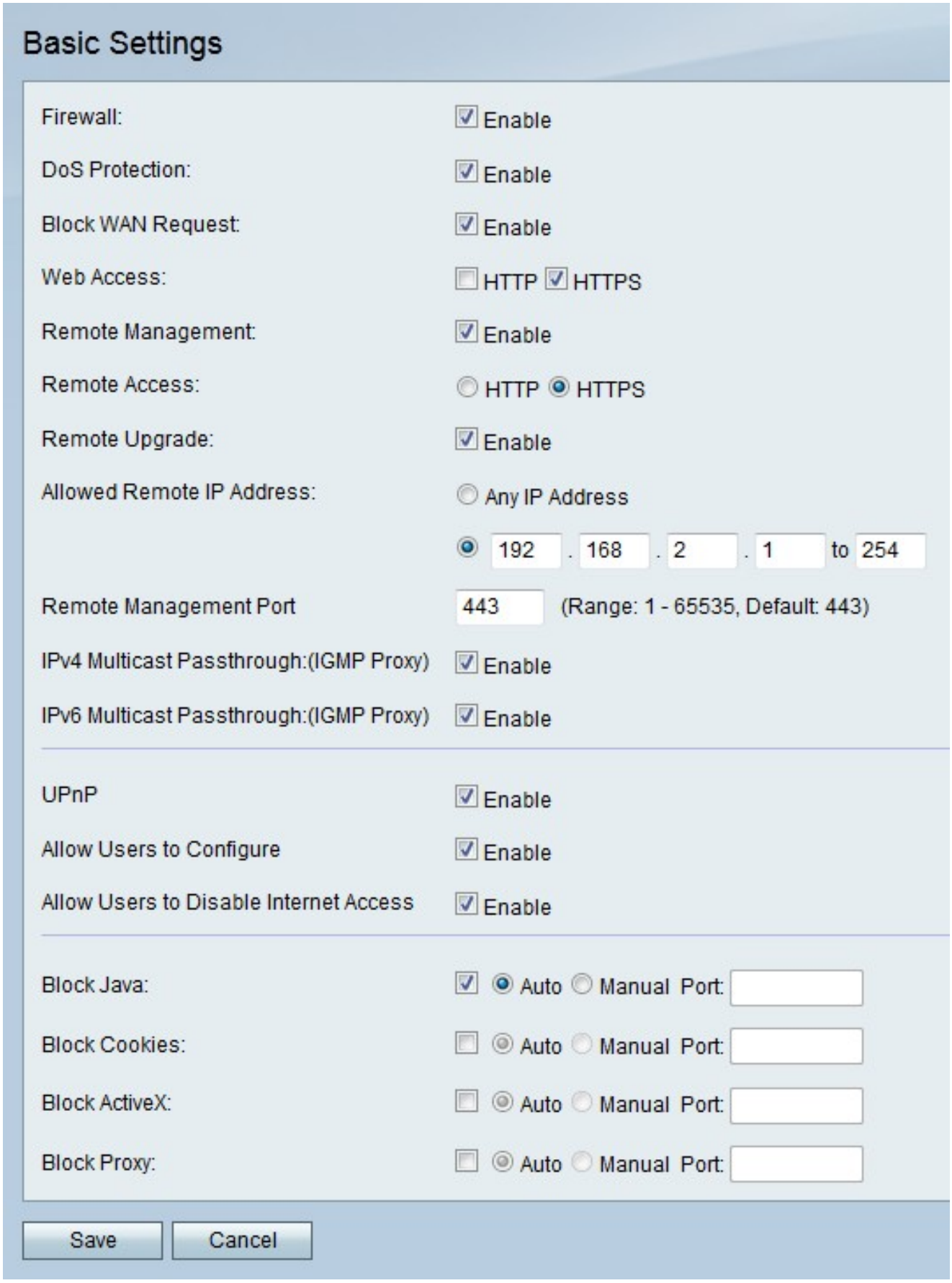
RV215W

Versione del software

•1.1.0.5

Impostazioni di base

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



Passaggio 2. Selezionare **Enable** (Abilita) nel campo Firewall (Firewall) per abilitare la configurazione del firewall sull'RV215W.

Passaggio 3. Selezionare **Enable** (Abilita) nel campo DoS Protection (Protezione DoS) per abilitare la protezione DoS (Denial of Service) sulla RV215W. La protezione DoS viene utilizzata per prevenire attacchi DDoS (Distributed Denial of Service) alla rete. Gli attacchi

DDoS hanno lo scopo di inondare una rete fino al punto in cui le risorse della rete non sono più disponibili. RV215W utilizza la protezione DoS per proteggere la rete attraverso la restrizione e la rimozione dei pacchetti indesiderati.

Passaggio 4. Selezionare **Enable** nel campo Block WAN Request per bloccare tutte le richieste ping verso l'RV215W dalla WAN.

Passaggio 5. Selezionare la casella di controllo corrispondente al tipo di accesso Web desiderato che è possibile utilizzare per connettersi al firewall nel campo Accesso Web.

Passaggio 6. Selezionare **Abilita** nel campo Gestione remota. La gestione remota consente l'accesso alla RV215W da una rete WAN remota.

Passaggio 7. Fare clic sul pulsante di opzione corrispondente al tipo di accesso Web desiderato che può essere utilizzato per connettersi al firewall dalla WAN remota nel campo Accesso remoto.

Passaggio 8. Selezionare **Aggiornamento remoto** per consentire agli utenti remoti di aggiornare RV215W.

Passaggio 9. Fare clic sul pulsante di opzione corrispondente agli indirizzi IP desiderati a cui è consentito accedere in remoto alla RV215W nel campo Indirizzo IP remoto consentito.

·Qualsiasi indirizzo IP - Sono consentiti tutti gli indirizzi IP.

·Indirizzo IP - Immettere un intervallo di indirizzi IP consentiti.

Passaggio 10. Immettere una porta per la quale è consentito l'accesso remoto nel campo Porta di gestione remota. Un utente remoto deve utilizzare la porta remota per accedere al dispositivo.

Nota: Il formato per l'accesso remoto è https://<*ip-remoto*>:<*porta-remota*>

Passaggio 11. Selezionare **Enable** nel campo IPv4 Multicast Passthrough per consentire al traffico multicast IPv4 di passare attraverso l'RV215W da Internet. Il multicast IP è un metodo utilizzato per inviare datagrammi IP a un gruppo designato di ricevitori in una singola trasmissione.

Passaggio 12. Selezionare **Enable** nel campo IPv6 Multicast Passthrough per consentire al traffico multicast IPv6 di passare attraverso RV215W da Internet.

Passaggio 13. Selezionare **Enable** nel campo UPnP per abilitare Universal Plug and Play (UPnP). UPnP consente il rilevamento automatico dei dispositivi in grado di comunicare con RV215W.

Passaggio 14. Selezionare **Abilita** nel campo Consenti agli utenti di configurare per consentire agli utenti con dispositivi compatibili con UPnP di configurare le regole di mapping delle porte UPnP. La mappatura delle porte o l'inoltro delle porte vengono utilizzati per consentire le comunicazioni tra host esterni e servizi forniti nell'ambito di una LAN privata.

Passaggio 15. Selezionare **Abilita** nel campo Consenti agli utenti di disabilitare l'accesso Internet per consentire agli utenti di disabilitare l'accesso Internet al dispositivo.

Passaggio 16. Selezionare **Blocca Java** per impedire il download delle applet Java. Le applet Java create per finalità dannose possono rappresentare una minaccia per la sicurezza di una rete. Una volta scaricata, un'applet Java ostile può sfruttare le risorse di

rete. Fare clic sul pulsante di opzione corrispondente al metodo di blocco desiderato.

·Auto — blocca automaticamente Java.

·Manual Port - Immettere una porta specifica su cui bloccare Java.

Passaggio 17. Selezionare **Blocca cookie** per escludere i cookie creati da un sito Web. I cookie vengono creati dai siti Web per memorizzare le informazioni di questi utenti. I cookie possono tenere traccia della cronologia Web dell'utente che può portare a un'invasione della privacy. Fare clic sul pulsante di opzione corrispondente al metodo di blocco desiderato.

·Auto — Blocca automaticamente i cookie.

·Manual Port - Immettere una porta specifica sulla quale bloccare i cookie.

Passaggio 18. Selezionare **Blocca ActiveX** per impedire il download di applet ActiveX. ActiveX è un tipo di applet privo di protezione. Una volta installata in un computer, un'applet ActiveX può eseguire qualsiasi operazione. Può inserire codice dannoso nel sistema operativo, navigare in una Intranet protetta, cambiare una password o recuperare e inviare documenti. Fare clic sul pulsante di opzione corrispondente al metodo di blocco desiderato.

·Auto — blocca automaticamente ActiveX.

·Manual Port - Immettere una porta specifica su cui bloccare ActiveX.

Passaggio 19. Selezionare **Blocca proxy** per bloccare i server proxy. 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. Fare clic sul pulsante di opzione corrispondente al metodo di blocco desiderato.

·Automatico: blocco automatico dei server proxy.

·Manual Port: immettere una porta specifica sulla quale bloccare i server proxy.

Passaggio 20. Fare clic su **Salva**.