Come configurare le impostazioni base del firewall sui modelli RV130 e RV130W

Obiettivo

Le impostazioni di base del firewall consentono di proteggere la rete creando e applicando regole utilizzate dal dispositivo per bloccare e consentire in modo selettivo il traffico Internet in entrata e in uscita.
Funzionalità quali Universal Plug and Play semplificano la connessione di periferiche in rete senza richiedere configurazioni aggiuntive.

UPnP (Universal Plug and Play) consente il rilevamento automatico delle periferiche in grado di comunicare con la periferica. Il blocco dei contenuti consente di proteggere il computer poiché è possibile inviare determinati contenuti al dispositivo, compromettendo la sicurezza o infettando il computer con software dannoso. La possibilità di bloccare contenuti specifici sulle porte desiderate è utile per una maggiore sicurezza del firewall.

Lo scopo di questo documento è mostrare come configurare le impostazioni base del firewall sui modelli RV130 e RV130W.

Dispositivi interessati

RV130

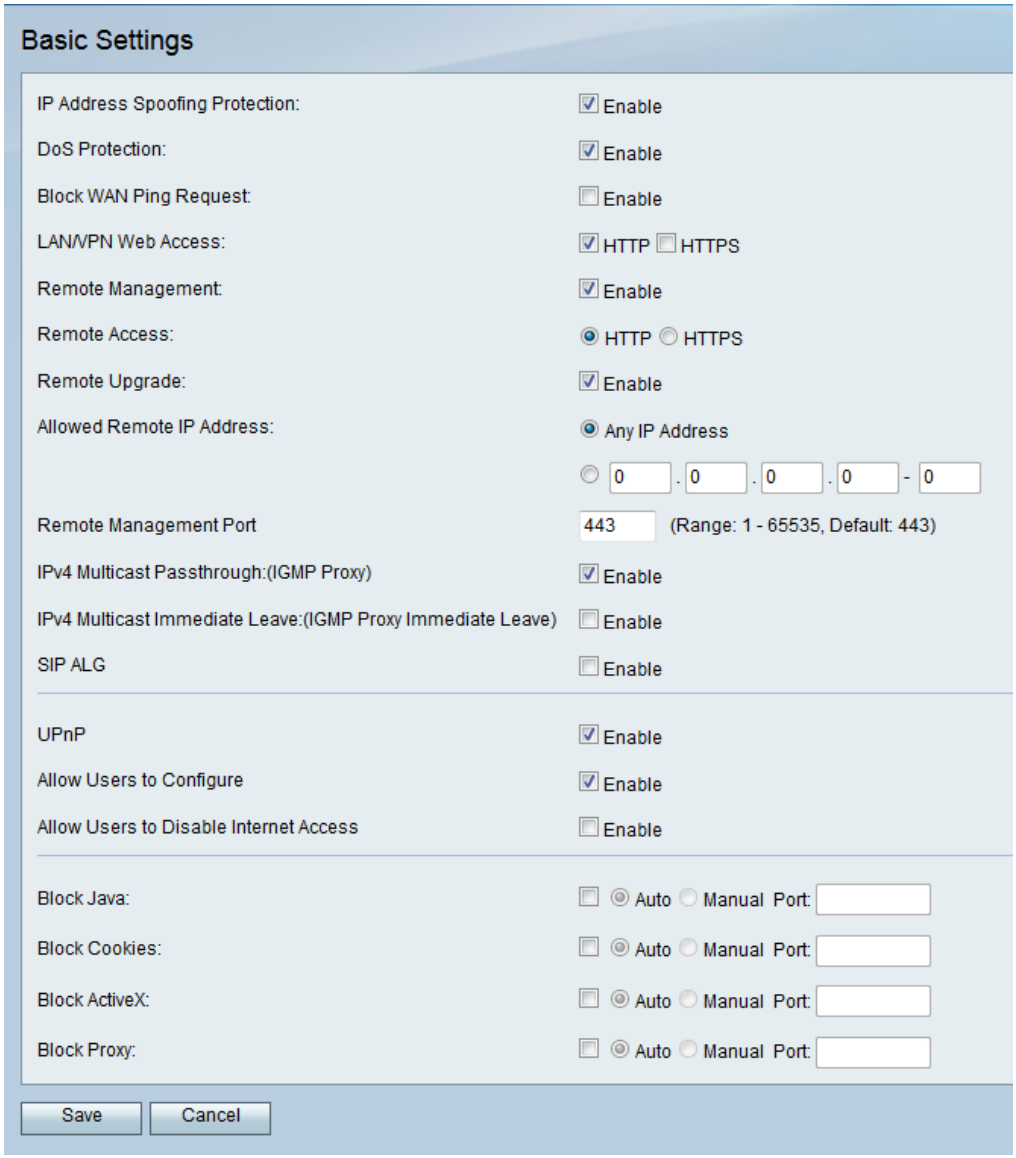
RV130W

Versione del software

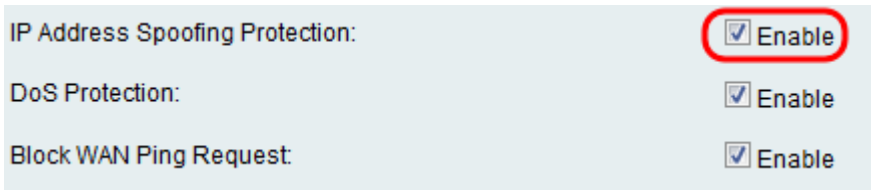
·v1.0.1.3

Configurazione delle impostazioni di base del firewall

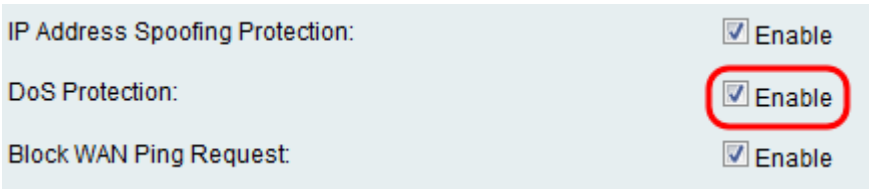
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Firewall > Impostazioni di base**. Viene visualizzata la pagina Impostazioni di base:



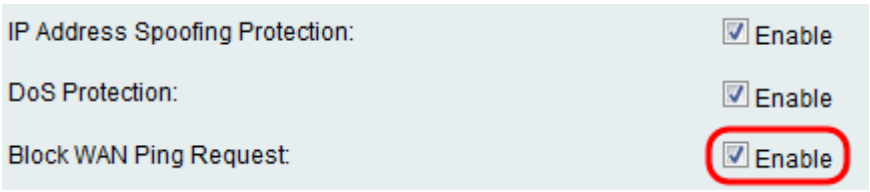
Passaggio 2. Nel campo *Protezione da spoofing degli indirizzi IP*, selezionare la casella di controllo **Abilita** per proteggere la rete dallo spoofing degli indirizzi IP. Lo spoofing dell'indirizzo IP si verifica quando un utente non autorizzato tenta di accedere a una rete rappresentando un altro dispositivo attendibile utilizzando il proprio indirizzo IP. Si consiglia di attivare *Protezione da spoofing degli indirizzi IP.*



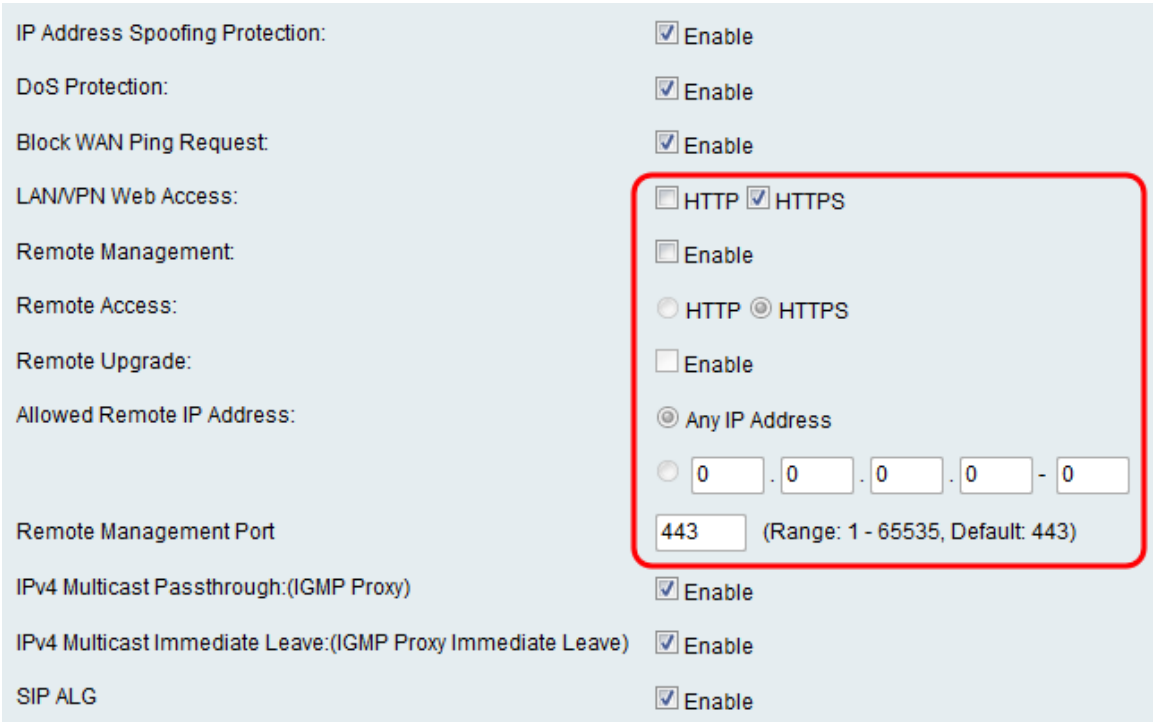
Passaggio 3. Nel campo *Protezione DoS*, selezionare la casella di controllo **Abilita** per proteggere la rete dagli attacchi Denial of Service. La protezione Denial of Service viene utilizzata per proteggere una rete da un attacco Distributed Denial of Service (DDoS). Gli attacchi DDoS hanno lo scopo di inondare una rete fino al punto in cui le risorse della rete non sono più disponibili.



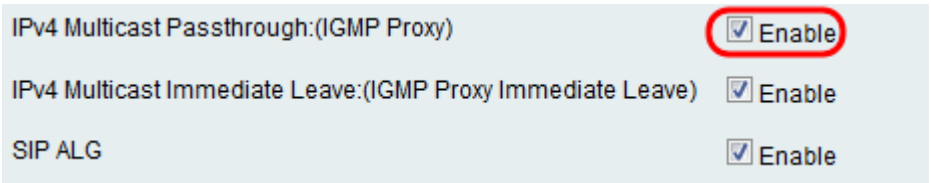
Passaggio 4. Nel campo *Blocca richiesta ping WAN*, selezionare la casella di controllo **Abilita** per interrompere le richieste di ping verso il dispositivo dalla rete WAN esterna.



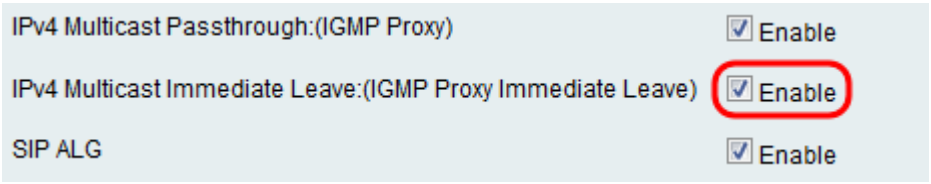
Passaggio 5. I campi elencati da *Accesso Web LAN/VPN a Porta di gestione remota* vengono utilizzati per configurare Accesso Web LAN e Gestione remota. Per ulteriori informazioni su queste configurazioni, consultare il documento sulla configurazione di LAN e Remote Management Web Access sui modelli RV130 e RV130W.



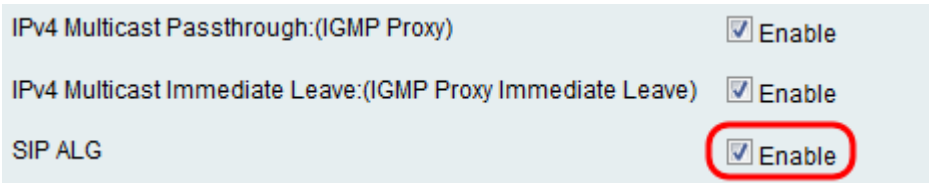
Passaggio 6. Nel campo *IPv4 Multicast Passthrough:(Proxy IGMP)*, selezionare la casella di controllo **Enable** (Abilita) per abilitare il passthrough multicast per IPv4. In questo modo i pacchetti IGMP del gruppo dalla rete WAN esterna vengono inoltrati alla LAN interna.



Passaggio 7. Nel campo *Uscita immediata multicast IPv4: (Uscita immediata proxy IGMP)*, selezionare la casella di controllo **Abilita** per abilitare l'Uscita immediata multicast. La possibilità di lasciare immediatamente il sistema garantisce una gestione ottimale della larghezza di banda agli host della rete, anche durante i periodi di utilizzo simultaneo da parte di gruppi multicast.



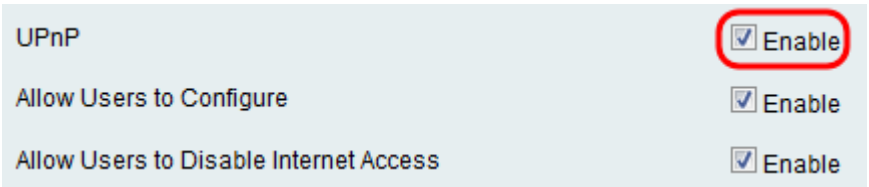
Passaggio 8. Nel campo *SIP (Session Initiation Protocol) Application Layer Gateway (ALG)*, selezionare la casella di controllo **Abilita** per consentire al traffico SIP (Session Initiation Protocol) di attraversare il firewall. Il SIP (Session Initiation Protocol) fornisce piattaforme per segnalare la configurazione di chiamate vocali e multimediali sulle reti IP. Application Layer Gateway (ALG) o anche Application Level Gateway è un'applicazione che converte le informazioni sull'indirizzo IP all'interno del payload di un pacchetto di applicazioni.



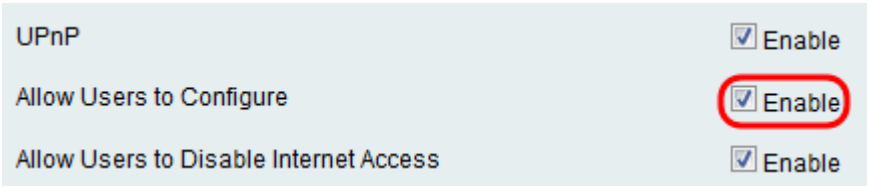
Nota: Il dispositivo supporta un massimo di 256 sessioni SIP ALG.

Configurazione di Universal Plug and Play

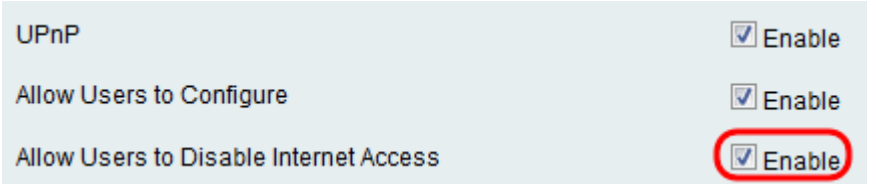
Passaggio 1. Nel campo *UPnP*, selezionare **Enable** to enable the Universal Plug and Play (UPnP).



Passaggio 2. Nel campo *Consenti agli utenti di configurare*, selezionare la casella di controllo **Abilita** per consentire agli utenti che dispongono del supporto UPnP di impostare le regole di mapping delle porte UPnP sui propri computer o su altri dispositivi abilitati per UPnP. Se disattivata, la periferica non consente all'applicazione di aggiungere la regola di inoltro.



Passaggio 3. Nel campo *Consenti agli utenti di disabilitare l'accesso a Internet*, selezionare la casella di controllo **Abilita** per consentire agli utenti di disabilitare l'accesso a Internet.



Blocco del contenuto

Passaggio 1. Selezionare la casella di controllo nel campo corrispondente al contenuto che si desidera bloccare dal dispositivo.

Le opzioni disponibili sono definite come segue:

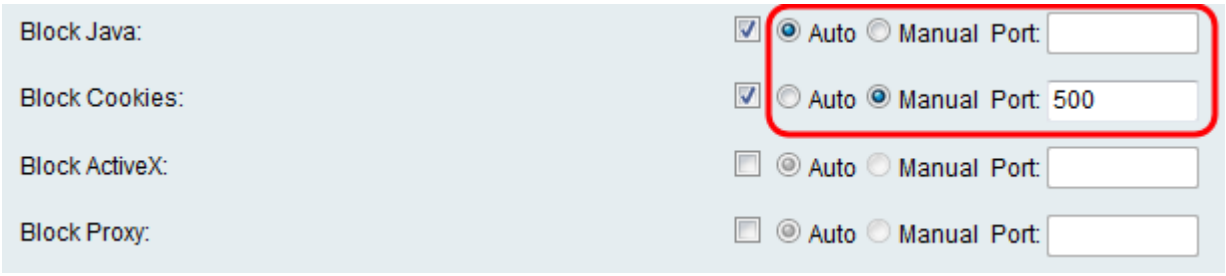
·Blocca Java — blocca il download di applet Java.

·Blocca cookie - Impedisce al dispositivo di ricevere informazioni sui cookie dalle pagine Web.

·Blocca ActiveX — blocca le applet ActiveX che possono essere presenti quando si utilizza Internet Explorer sul sistema operativo Windows.

·Blocca proxy — impedisce al dispositivo di comunicare ai dispositivi esterni tramite un server proxy. In questo modo il dispositivo non aggira le regole firewall.

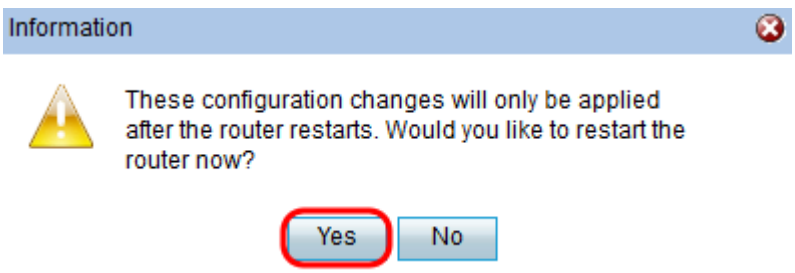
Passaggio 2. Selezionare il pulsante di opzione **Automatico** per bloccare automaticamente tutte le istanze di un determinato contenuto oppure fare clic sul pulsante di opzione **Manuale** e immettere una porta specifica nel campo corrispondente in cui il contenuto verrà bloccato.



Nota: È possibile immettere qualsiasi numero desiderato nell'intervallo (1-65535) per il valore della porta.

Passaggio 3. Fare clic su **Save** per salvare le impostazioni.

Passaggio 4. Viene visualizzata una finestra in cui viene richiesto di riavviare il router. Fare clic su **Sì** per riavviare il router e applicare le modifiche.



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).