Configurazione delle impostazioni base del firewall sul router serie RV34x

Obiettivo

In questo articolo viene spiegato come configurare le impostazioni base del firewall sul router serie RV34x.

Introduzione

L'obiettivo principale di un firewall è controllare il traffico di rete in entrata e in uscita analizzando i pacchetti di dati e determinando se consentirne il passaggio o meno, in base a un set di regole predeterminato. Un router è considerato un potente firewall hardware a causa di funzioni che consentono di filtrare i dati in ingresso. Un firewall di rete crea un bridge tra una rete interna considerata sicura e attendibile e un'altra rete, in genere una rete interna esterna come Internet che si presume non sia sicura e non attendibile.

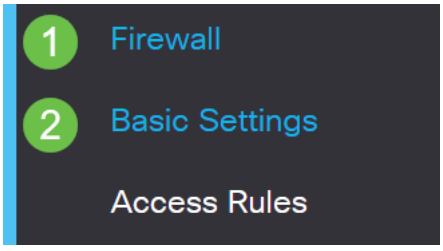
Dispositivi interessati | Versione firmware

- Serie RV34x | 1.0.03.21 (scarica la versione più recente)

Configurare le impostazioni di base del firewall

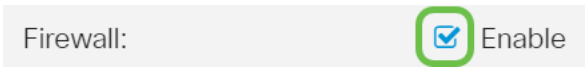
Passaggio 1

Accedere all'interfaccia utente Web e scegliere **Firewall >Impostazioni di base**.



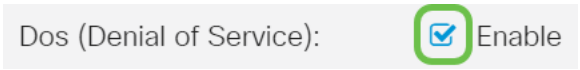
Passaggio 2

Selezionare la casella di controllo **Attiva** firewall per attivare la funzionalità del firewall. L'opzione è abilitata per impostazione predefinita.



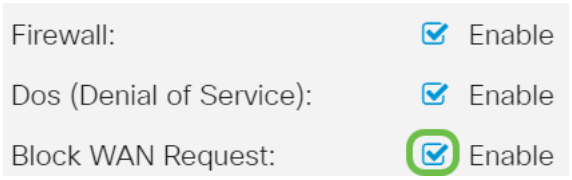
Passaggio 3

Selezionare la casella di controllo **Abilita** DOS (Denial of Service) per proteggere la rete dagli attacchi DoS. L'opzione è abilitata per impostazione predefinita.



Passaggio 4

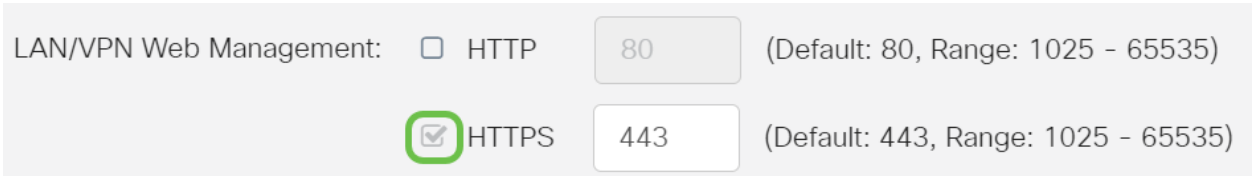
Selezionare la casella di controllo **Enable** Block WAN Request per negare le richieste ping al router serie RV34x. L'opzione è abilitata per impostazione predefinita.



Passaggio 5

Nell'area Gestione Web LAN/VPN selezionare la casella di controllo **HTTP** e/o **HTTPS** per abilitare il traffico proveniente da questi protocolli. Per questo esempio, la casella di controllo HTTPS è selezionata.

- HTTP: Hyper Text Transfer Protocol è un protocollo di trasferimento dati utilizzato su Internet.
- HTTPS: Hyper Text Transfer Protocol Secure è una versione protetta di HTTP che crittografa i pacchetti per aumentare la sicurezza.

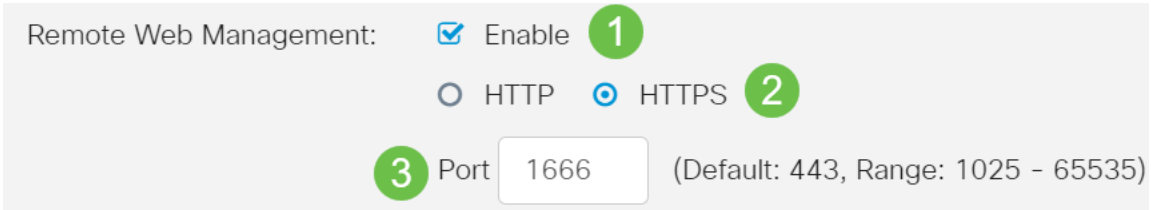


Passaggio 6 (facoltativo)

Selezionare la casella di controllo **Abilita** gestione Web remota per abilitare la gestione remota. In caso contrario, andare al passaggio 8.

Scegliere il tipo di protocollo utilizzato per la connessione al firewall scegliendo un pulsante di opzione. Le opzioni sono **HTTP** e **HTTPS**.

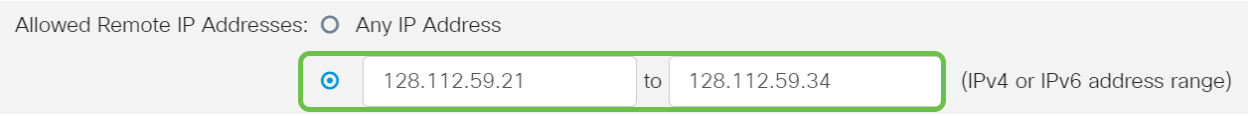
Immettere un numero di porta compreso tra 1025 e 65535, che consente la gestione remota. L'impostazione predefinita è 443. Nell'esempio viene utilizzato 1666.



Passaggio 7

Nell'area Indirizzi IP remoti consentiti scegliere un pulsante di opzione per consentire a

qualsiasi indirizzo IP di accedere alla rete in remoto o per specificare un intervallo di indirizzi IPv4 o IPv6. Nell'esempio è stato scelto un intervallo IP. Nell'esempio, l'indirizzo IP iniziale è 128.112.59.21 e l'indirizzo IP finale è 128.112.59.34.



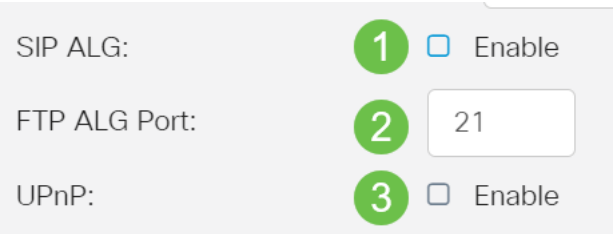
Passaggio 8 (facoltativo)

Selezionare la casella di controllo **Enable** SIP ALG per abilitare il protocollo ALG (Application Layer Gateway) del protocollo SIP (Session Initiation Protocol) al passaggio attraverso il firewall. Questa funzione può essere abilitata per facilitare il passaggio dei pacchetti SIP attraverso il firewall. Un pacchetto SIP viene usato per avviare le connessioni del traffico vocale. Se il provider VoIP utilizza un protocollo di attraversamento NAT (Network Address Translation) diverso, è possibile disabilitare questa funzionalità, che rappresenta l'impostazione predefinita.

Specificare la porta FTP (File Transfer Protocol) di SIP ALG nel campo *FTP ALG Port*. Il valore predefinito è 21.

Selezionare la casella di controllo **Attiva** UPnP per attivare Universal Plug and Play (UPnP). Questa funzione è disabilitata per impostazione predefinita.

In questo esempio, queste opzioni rimangono disattivate.

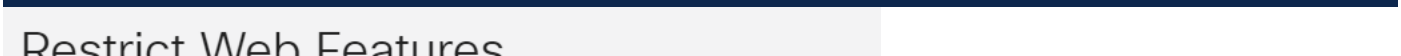


Passaggio 9 (facoltativo)

Nell'area Limita funzionalità Web selezionare le caselle di controllo relative ai tipi di funzionalità Web da bloccare nell'area Blocca. Queste caselle di controllo sono disattivate per impostazione predefinita. Le opzioni sono:

Java — tutti gli elementi Web contenenti questo tipo di elemento Web verranno bloccati. Questa impostazione consente di prevenire gli attacchi Web basati su Java.
Cookie: i cookie sono dati memorizzati nel computer per consentire ai siti Web di individuare gli utenti che vi accedono. Il blocco dei cookie può impedire l'accesso ai dati da parte di cookie dannosi.
ActiveX: è un plug-in sviluppato da Microsoft per migliorare l'esperienza di esplorazione. Il blocco può impedire che plug-in ActiveX dannosi danneggino i dispositivi di rete.
Accesso al server HTTP proxy: i server proxy HTTP nascondono i dettagli degli utenti finali agli hacker. Lavorano come intermediari in modo che un cliente non acceda direttamente a Internet. Tuttavia, se gli utenti locali hanno accesso ai server proxy WAN, potrebbero essere in grado di aggirare i filtri dei contenuti sul router per accedere ai siti Internet bloccati dal router.

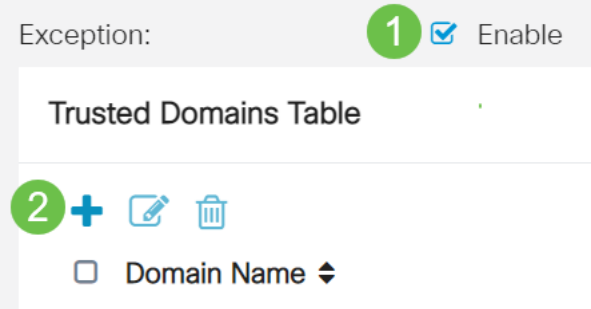
In questo esempio, le caselle di controllo sono disabilitate.



Passaggio 11 (facoltativo)

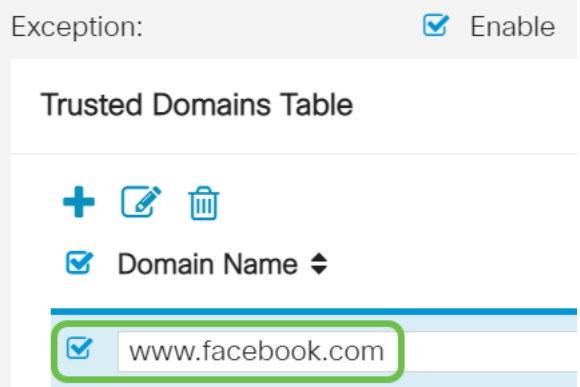
Selezionare la casella di controllo **Abilita** eccezione per consentire solo alcune funzionalità Web, ad esempio Java, Cookie, ActiveX o Accesso ai server proxy HTTP e limitare tutte le altre. Questa opzione è disattivata per impostazione predefinita. Nell'esempio, questa opzione è disabilitata.

Nella tabella Domini trusted fare clic sull'**icona Aggiungi** per aggiungere i domini trusted o autorizzati ad accedere alla rete.



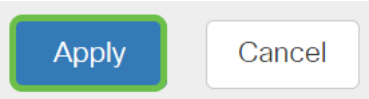
Passaggio 12

Nel campo *Nome dominio*, immettere un nome di dominio a cui concedere l'accesso alla rete. Nell'esempio viene utilizzato www.facebook.com.



Passaggio 13

Fare clic su Apply (Applica).



Passaggio 14 (facoltativo)

Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull'**icona Salva** nella parte superiore della pagina.

Conclusioni

A questo punto, è necessario configurare correttamente le impostazioni base del firewall sul router serie RV34x.