Configurazione base del firewall sui router RV320 e RV325

Obiettivo

Questo articolo spiega come configurare le impostazioni base del firewall sulla serie RV32x VPN Router.

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. I firewall di rete proteggono una rete interna del computer (casa, scuola, intranet aziendale) dall'accesso dannoso dall'esterno. È inoltre possibile configurare i firewall di rete per limitare l'accesso all'esterno da parte degli utenti interni.

Dispositivi interessati

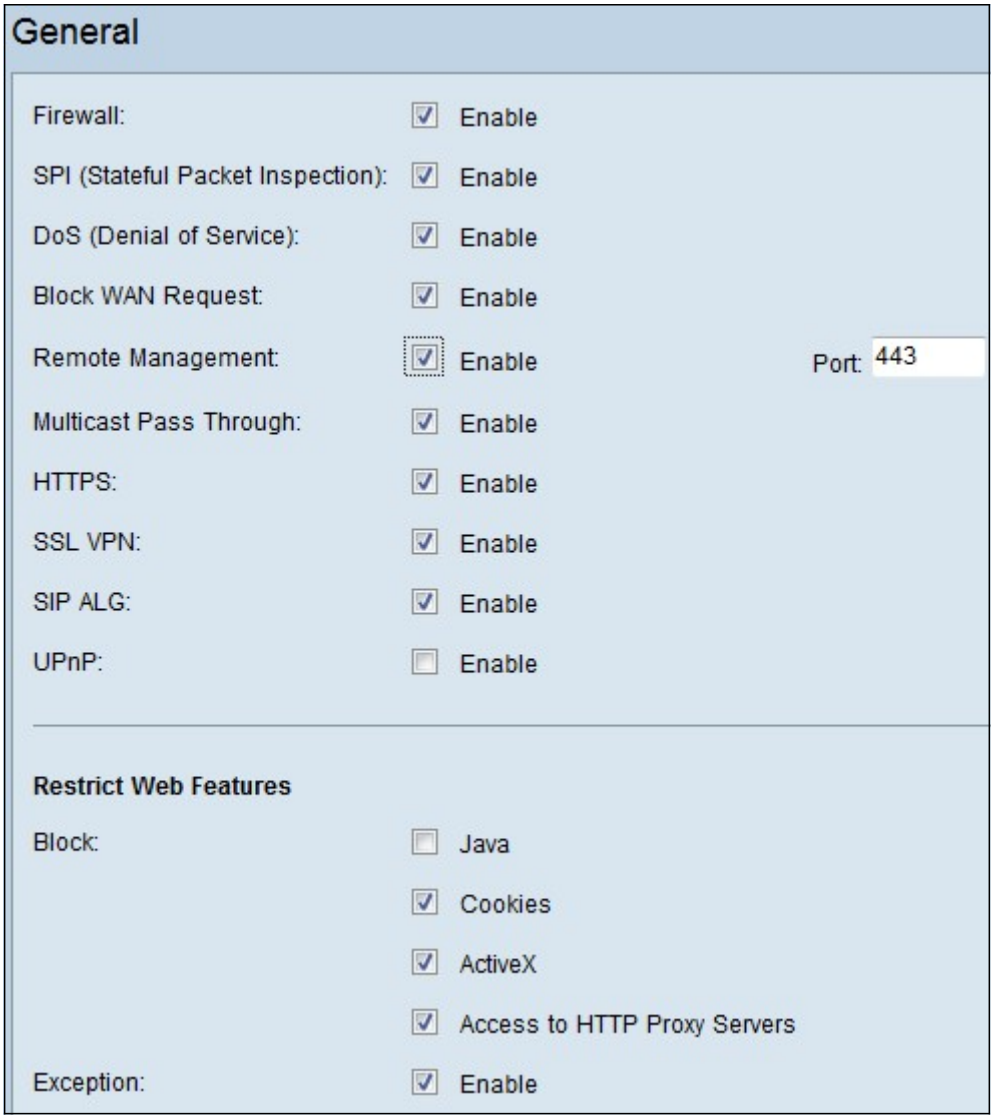
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Versione del software

- v1.1.0.09

Impostazioni di base

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



Passaggio 2. In base alle proprie esigenze, selezionare la casella di controllo **Abilita** corrispondente alle funzioni che si desidera abilitare.

- Firewall: i firewall del router possono essere disattivati (disattivati) o attivati per filtrare determinati tipi di traffico di rete attraverso le cosiddette regole firewall. Un firewall può essere utilizzato per filtrare tutto il traffico in entrata e in uscita e basato su.
- SPI (Stateful Packet Inspection): controlla lo stato delle connessioni di rete, come i flussi TCP e le comunicazioni UDP. Il firewall distingue i pacchetti legittimi per i diversi tipi di connessione. Solo i pacchetti che corrispondono a una connessione attiva nota sono consentiti dal firewall, tutti gli altri vengono rifiutati.
- DoS (Denial of Service) - Utilizzato 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. RV320 utilizza la protezione DoS per proteggere la rete attraverso la restrizione e la rimozione dei pacchetti indesiderati.
- Blocca richiesta WAN — blocca tutte le richieste ping al router dalla porta WAN.
- Gestione remota: consente l'accesso al router da una rete WAN remota.
  - Porta: immettere un numero di porta da gestire in remoto.
- Pass-through multicast: consente il passaggio di messaggi IP multicast attraverso il dispositivo.
- HTTPS (Hypertext Transfer Protocol Secure): protocollo di comunicazione per la comunicazione sicura su una rete di computer. Fornisce la crittografia bidirezionale da client e

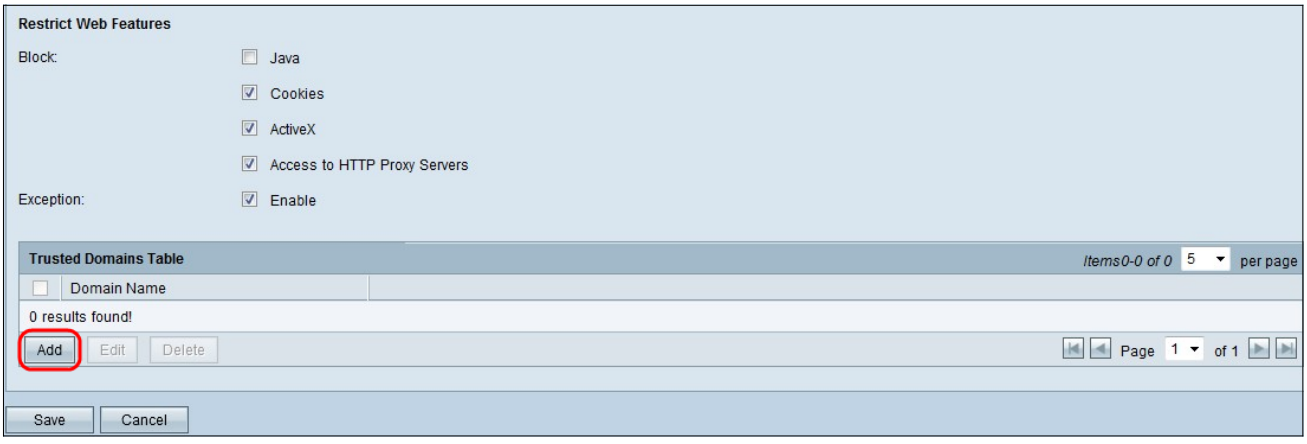
server.
- SSL VPN: consente una connessione SSL VPN effettuata tramite il router.
- SIP ALG: SIP ALG offre funzionalità che consentono il traffico Voice over IP dal lato privato al lato pubblico e dal lato pubblico al lato privato del firewall quando vengono utilizzati l'indirizzo di rete e la conversione delle porte (NAPT). NAPT è il tipo più comune di traduzione degli indirizzi di rete.
- UPnP (Universal Plug and Play): consente il rilevamento automatico delle periferiche in grado di comunicare con il router.

Passaggio 3. In base alle proprie esigenze, selezionare la casella di controllo **Abilita** corrispondente alle funzioni che si desidera bloccare.

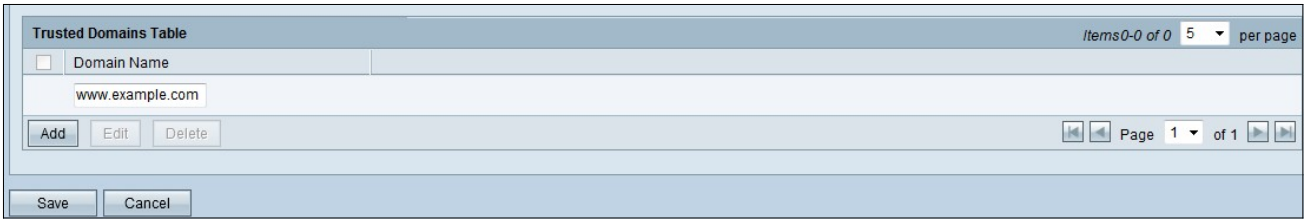
- Java — la selezione di questa casella impedisce il download e l'esecuzione delle applet Java. Java è un linguaggio di programmazione comune utilizzato da molti siti Web. Tuttavia, le applet Java create per scopi dannosi possono rappresentare una minaccia per la sicurezza di una rete. Una volta scaricata, un'applet Java ostile può sfruttare le risorse di rete.
- Cookie: i cookie vengono creati dai siti Web per memorizzare informazioni sugli utenti. I cookie possono tenere traccia della cronologia Web dell'utente che può portare a un'invasione della privacy.
- 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.
- Accesso ai server proxy HTTP: i server proxy 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.
- Eccezione: consente le funzionalità selezionate (Java, Cookie, ActiveX o Accesso ai server proxy HTTP), ma limita tutte le funzionalità non selezionate nei domini trusted configurati. Dominio trusted che ha accesso alla rete trusted. È possibile configurare un dominio trusted che consenta agli utenti di un dominio esterno di accedere alle risorse di rete. Se questa opzione è disattivata, un dominio trusted consente tutte le funzionalità.

Nota: Risparmio di tempo: se non è stata selezionata la casella di controllo Eccezione, saltare il passaggio 4.

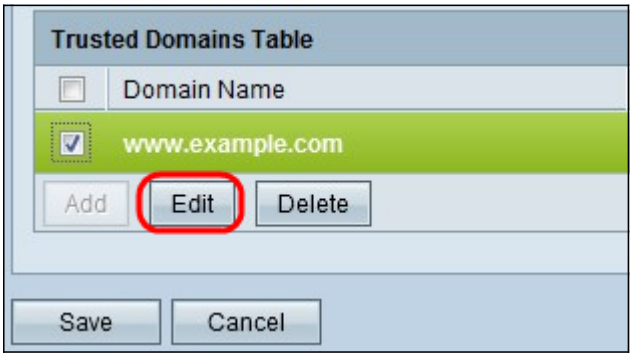
Passaggio 4. Fare clic su Aggiungi, immettere un nuovo dominio trusted e fare clic su Salva per creare un dominio trusted.



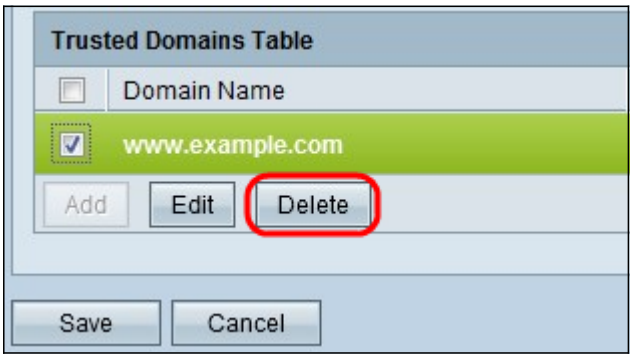
Passaggio 5. Fare clic su Salva per aggiornare le modifiche.



Passaggio 6. (Facoltativo) Per modificare il nome del dominio trusted, selezionare la casella di controllo del dominio trusted che si desidera modificare, fare clic su Modifica, modificare il nome del dominio e fare clic su Salva.



Passaggio 7. (Facoltativo) Per eliminare un dominio dall'elenco dei domini trusted, selezionare la casella di controllo del dominio trusted che si desidera eliminare e fare clic su Elimina.



Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco