Configurazione base del firewall sul router VPN CVR100W

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 sul router VPN CVR100W.

Dispositivo applicabile

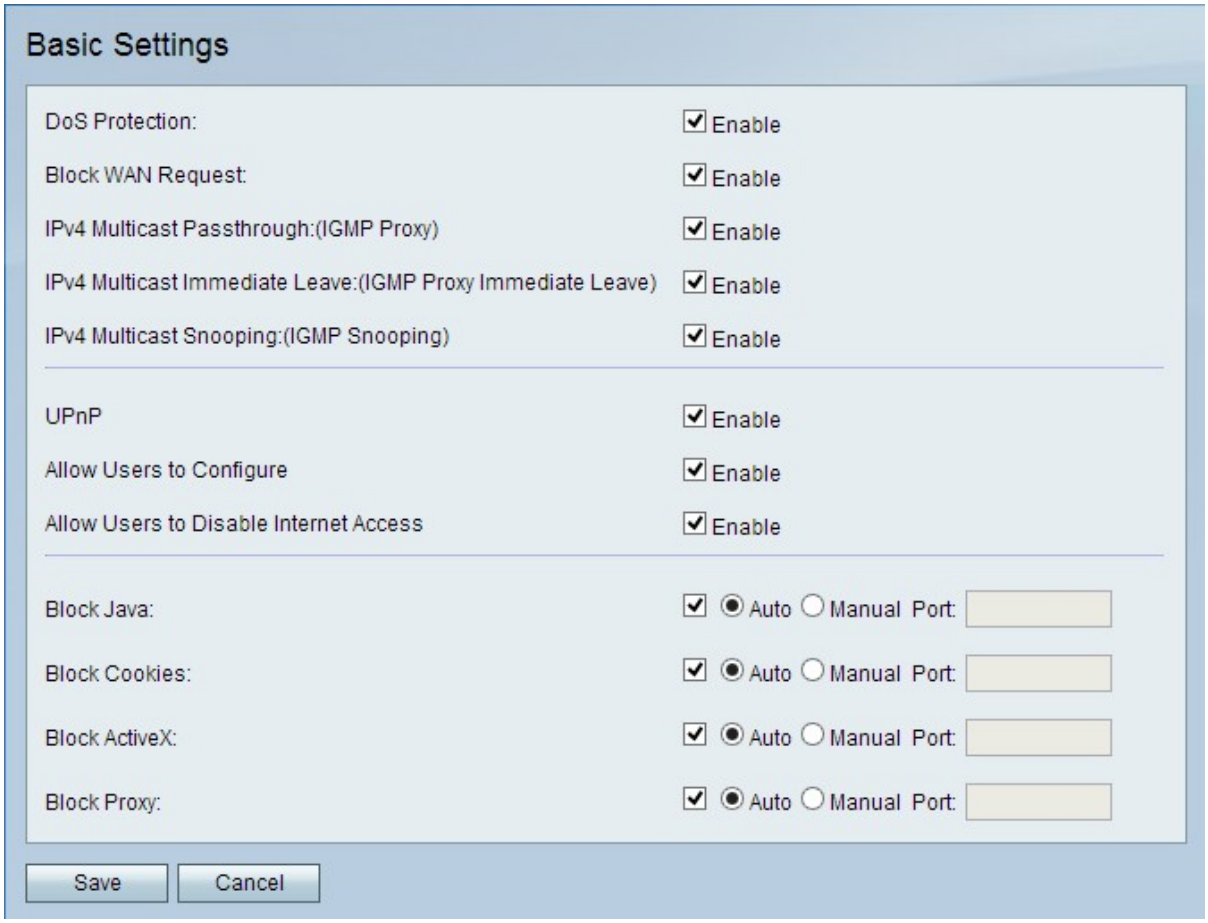
·CVR100W

Versione del software

•1.0.1.19

Configurazione 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*:



Nota: I passi da 2 a 13 sono facoltativi. È possibile configurare queste opzioni in base alle

proprie esigenze.

Passaggio 2. Per abilitare la protezione DoS (Denial of Service) sul CVR100W, selezionare **Abilita** nel campo Protezione DoS. 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. Il CVR100W utilizza la protezione DoS per proteggere la rete attraverso la restrizione e la rimozione dei pacchetti indesiderati.

Passaggio 3. Per bloccare tutte le richieste ping verso il CVR100W dalla WAN, selezionare **Enable** (Abilita) nel campo Block WAN Request (Blocca richiesta WAN).

Passaggio 4. Per consentire al traffico multicast IPv4 di passare attraverso il CVR100W da Internet, selezionare **Enable** (Abilita) nel campo IPv4 Multicast Passthrough. Il multicast IP è un metodo utilizzato per inviare datagrammi IP a un gruppo designato di ricevitori in una singola trasmissione.

Passaggio 5. Il proxy IGMP consente al router di interagire con altri dispositivi usando i messaggi IGMP. Immediate Leave consente al CVR100W di lasciare il gruppo multicast a una velocità ottimale. Per abilitare l'uscita immediata del proxy IGMP, selezionare **Enable** nel campo IPv4 Multicast Immediate Leave.

Passaggio 6. Per abilitare lo snooping IGMP, che consente agli altri switch della rete di restare in ascolto sui messaggi che vanno avanti e indietro tra il computer e il CVR100W, selezionare **Enable** nel campo IPv4 Multicast Snooping.

Passaggio 7. Per abilitare Universal Plug and Play (UPnP), selezionare **Enable** (Abilita) nel campo UPnP. UPnP consente il rilevamento automatico dei dispositivi in grado di comunicare con il CVR100W.

Passaggio 8. Per consentire agli utenti con dispositivi UPnP di configurare le regole di mapping delle porte UPnP, selezionare **Abilita** nel campo Consenti agli utenti di configurare. 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 9. Per consentire agli utenti di disabilitare l'accesso a Internet al dispositivo, selezionare **Abilita** nel campo Consenti agli utenti di disabilitare l'accesso a Internet.

Passaggio 10. Per impedire il download di applet Java, selezionare **Block Java** nel campo Block 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 11. Se non si desidera che un sito Web crei cookie, selezionare **Blocca cookie** nel campo Blocca cookie. 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 12. Per impedire il download di applet ActiveX, selezionare **Blocca ActiveX** nel campo Blocca 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 13. Per bloccare i server proxy, selezionare **Blocca proxy** nel campo Blocca 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 14. Fare clic su **Salva** per salvare le modifiche apportate.