Configurazione di Application Level Gateway sui router VPN RV315W

Obiettivo

Quando un dispositivo dietro il router utilizza un'applicazione per la quale il router ha abilitato il servizio Application-Level Gateway (ALG), il router converte l'indirizzo IP privato del dispositivo all'interno del flusso di dati in un indirizzo IP pubblico. Registra inoltre i numeri delle porte di sessione e crea in modo dinamico l'inoltro implicito delle porte NAT affinché il traffico delle applicazioni arrivi dalla WAN alla LAN. Application Level Gateway (ALG) consente il corretto funzionamento di alcune applicazioni incompatibili NAT. Un attacco Denial of Service (DoS) si verifica quando un utente malintenzionato inonda un sito Web di traffico, limitando la capacità di funzionamento del sito. Questo articolo spiega come configurare la protezione DoS sul router VPN RV315W.

Dispositivo applicabile

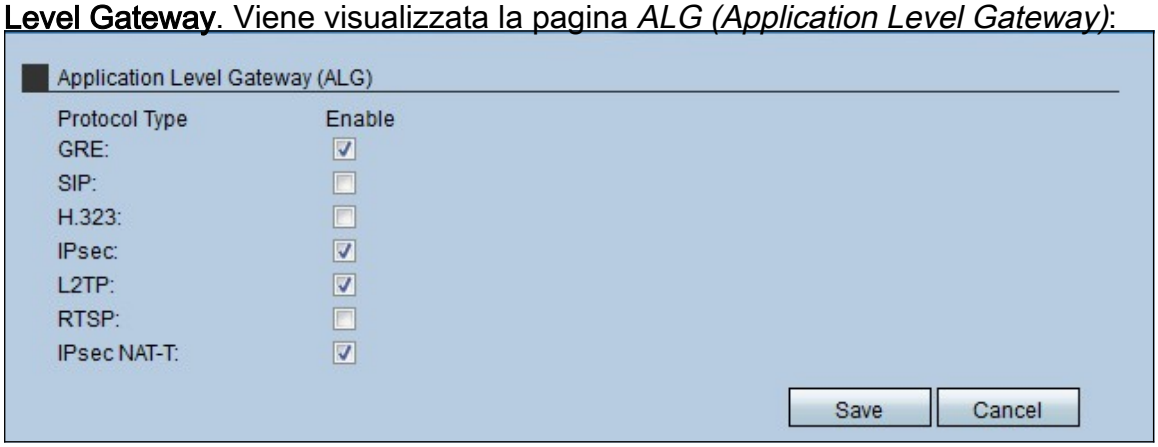
RV315W

Versione del software

•1.01.03

Application Level Gateway

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Security >Application Level Gateway**. Viene visualizzata la pagina *ALG (Application Level Gateway)*:



Passaggio 2. Selezionare la casella di controllo **Enable** (Abilita) del tipo di protocollo usato dall'RV315W per livellare il gateway. I protocolli possibili sono:

·GRE - Generic Routing Encapsulation (GRE) è un protocollo che incapsula le informazioni quando i dati usano una connessione gateway (point-to-point) e vengono inviati sulle reti IP.
· SIP: Session Initiation Protocol (SIP) è un protocollo di controllo (segnalazione) del livello applicazione che gestisce la configurazione, la modifica e l'eliminazione di sessioni vocali e multimediali su Internet. Abilitare SIP ALG quando i dispositivi voce, ad esempio UC500, UC300 o i telefoni SIP, sono collegati alla rete dietro il router.

· H.323 - Una suite di protocolli di teleconferenza standard che fornisce audio, dati e videoconferenze. Consente la comunicazione punto-punto e multipunto in tempo reale tra computer client su una rete basata su pacchetti che non fornisce una qualità del servizio garantita.
· IPsec: Internet Protocol Security (IPsec) viene utilizzato per autenticare e crittografare i pacchetti IP. Questo protocollo è molto utile perché garantisce la protezione dei dati inviati a un host.
· L2TP: Layer 2 Tunneling Protocol (L2TP) è un protocollo utilizzato dai provider di servizi che consente una connessione point-to-point, ma con l'applicazione del layer 2 per la sicurezza.
· RTSP: Real Time Streaming Protocol (RTSP) è un protocollo che controlla e gestisce il traffico dei supporti in un gateway (point-to-point). Questa funzione consente all'utente di controllare i supporti in tempo reale.
· IPsec NAT-T: è la combinazione di IPsec e NAT che implica che il pacchetto viene inviato con il protocollo IPsec ma crea, allo stesso tempo, datagrammi per Network Address Translation (NAT) che vengono crittografati per migliorare il livello di sicurezza.

Passaggio 3. Fare clic su **Salva**.