

RV315W VPN路由器上的應用級網關配置

目標

當路由器後面的裝置使用已啟用應用級網關(ALG)服務的應用時，路由器會將資料流中裝置的私有IP地址轉換為公有IP地址。它還記錄會話埠號，並動態建立隱式NAT埠轉發，以便應用流量從WAN進入LAN。應用級網關(ALG)允許某些NAT不相容的應用程式正常運行。阻斷服務(DoS)攻擊是指攻擊者向網站傳送大量流量，從而限制網站的功能。本文說明如何在RV315W VPN路由器上配置DoS保護。

適用的裝置

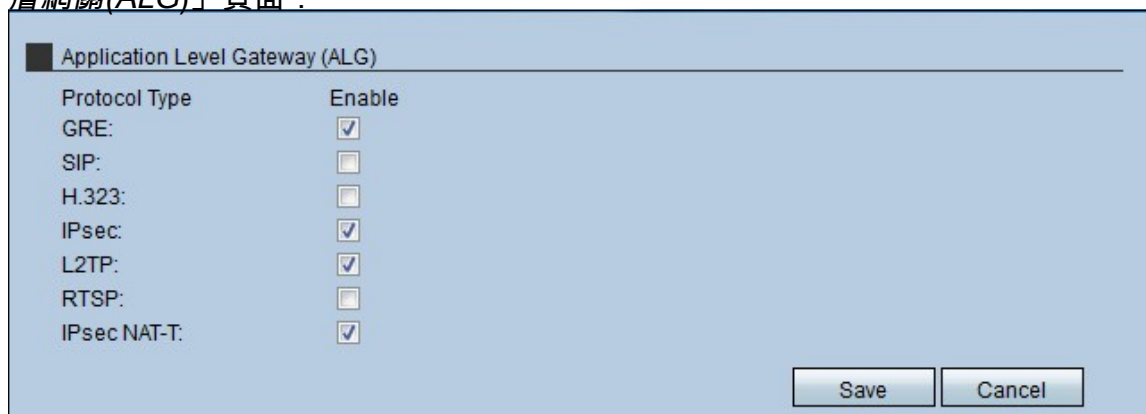
·RV315W

軟體版本

·1.01.03

應用層閘道

步驟1.登入到Web配置實用程式並選擇Security >Application Level Gateway。將打開「應用層網關(ALG)」頁面：



Protocol Type	Enable
GRE:	<input checked="" type="checkbox"/>
SIP:	<input type="checkbox"/>
H.323:	<input type="checkbox"/>
IPsec:	<input checked="" type="checkbox"/>
L2TP:	<input checked="" type="checkbox"/>
RTSP:	<input type="checkbox"/>
IPsec NAT-T:	<input checked="" type="checkbox"/>

步驟2.選中RV315W用於使網關分級的協定型別的Enable覈取方塊。可能的通訊協定包括：

- GRE — 通用路由封裝(GRE)是一種協定，用於在資料使用網關連線（點對點）並通過IP網路傳送時封裝資訊。
- SIP — 會話初始協定(SIP)是一種應用層控制（信令）協定，它處理通過Internet建立、修改和斷開語音和多媒體會話。當UC500、UC300或SIP電話等語音裝置連線到路由器後面的網路時，啟用SIP ALG。
- H.323 — 提供音訊、資料和視訊會議的標準電話會議協定套件。它允許客戶端電腦之間通過不能提供保證服務品質的基於資料包的網路進行即時點對點和多點通訊。
- IPsec — 網際網路通訊協定安全(IPsec)用於驗證和加密IP封包。此通訊協定非常有用，因為它可以確保對傳送到主機的資料進行保護。
- L2TP — 第2層隧道協定(L2TP)是服務提供商使用的協定，它允許點對點連線，但為了安全起見，使用第2層應用。
- RTSP — 即時流協定(RTSP)是一種協定，用於控制和管理網關（點對點）中的媒體流量，此功能允許使用者即時控制媒體。
- IPsec NAT-T — 是IPsec和NAT的組合，表示使用IPsec協定傳送資料包，但同時為網路地

址轉換(NAT)建立資料包，這些資料包經過加密以提高安全級別。

步驟3.按一下「**Save**」。