Konfiguration des Gateway auf Anwendungsebene auf RV315W VPN-Routern

Ziel

Wenn ein Gerät hinter dem Router eine Anwendung verwendet, für die der Router über einen ALG-Dienst (Application-Level Gateway) verfügt, übersetzt der Router die private IP-Adresse des Geräts im Datenstrom in eine öffentliche IP-Adresse. Darüber hinaus werden Sitzungsportnummern aufgezeichnet und dynamisch eine implizite NAT-Port-Weiterleitung für den Anwendungsdatenverkehr vom WAN zum LAN erstellt. Mit Application Level Gateway (ALG) können bestimmte nicht kompatible NAT-Anwendungen ordnungsgemäß ausgeführt werden. Ein Denial of Service (DoS)-Angriff ist, wenn ein Angreifer eine Website mit Datenverkehr überflutet, wodurch die Funktionsfähigkeit der Websites eingeschränkt wird. In diesem Artikel wird erläutert, wie der DoS-Schutz auf dem RV315W VPN-Router konfiguriert wird.

Anwendbares Gerät

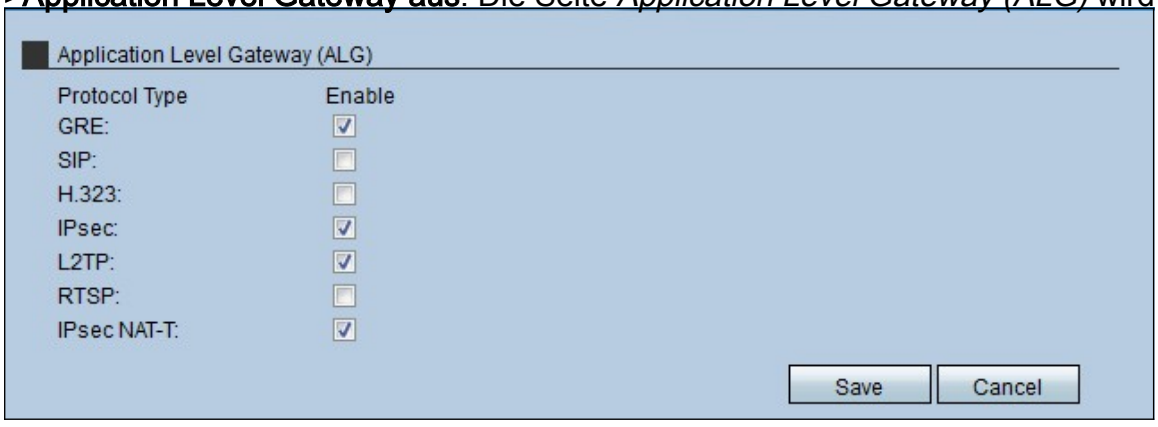
RV315W

Softwareversion

·1.01.03

Gateway auf Anwendungsebene

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security >Application Level Gateway aus**. Die Seite *Application Level Gateway (ALG)* wird geöffnet:



Schritt 2: Aktivieren Sie das **Kontrollkästchen Aktivieren** für den Protokolltyp, den der RV315W zum Leeren des Gateways verwendet. Mögliche Protokolle sind:

·GRE - Generic Routing Encapsulation (GRE) ist ein Protokoll, das die Informationen kapselt, wenn die Daten eine Gateway-Verbindung (Point-to-Point) verwenden und über IP-Netzwerke gesendet werden.
· SIP - Das Session Initiation Protocol (SIP) ist ein Signalisierungsprotokoll auf Anwendungsebene, das die Einrichtung, Änderung und Beendigung von Sprach- und Multimedia-Sitzungen über das Internet übernimmt. Aktivieren Sie die SIP-ALG, wenn

Sprachgeräte wie UC500, UC300 oder SIP-Telefone mit dem Netzwerk hinter dem Router verbunden sind.
· H.323 - Eine standardmäßige Protokoll-Suite für Telekonferenzen, die Audio-, Daten- und Videokonferenzen bereitstellt. Sie ermöglicht die Point-to-Point- und Multipoint-Echtzeitkommunikation zwischen Client-Computern über ein paketbasiertes Netzwerk, das keine garantierte Quality of Service bietet.
· IPsec — IPsec (Internet Protocol Security) dient zur Authentifizierung und Verschlüsselung von IP-Paketen. Dieses Protokoll ist sehr nützlich, da es den Schutz der Daten gewährleistet, die an einen Host gesendet werden.
· L2TP — Layer 2 Tunneling Protocol (L2TP) ist ein Protokoll, das von Service Providern verwendet wird und eine Punkt-zu-Punkt-Verbindung ermöglicht, jedoch mit der Anwendung von Layer 2 für die Sicherheit.
· RTSP — Real Time Streaming Protocol (RTSP) ist ein Protokoll, das den Medienverkehr in einem Gateway steuert und verwaltet (Point-to-Point). Mit dieser Funktion kann der Benutzer die Medien in Echtzeit steuern.
· IPsec NAT-T - Die Kombination aus IPsec und NAT, die impliziert, dass das Paket mit dem IPsec-Protokoll gesendet wird, aber gleichzeitig Datagramme für die Network Address Translation (NAT) erstellt, die verschlüsselt werden, um die Sicherheitsstufe zu erhöhen.

Schritt 3: Klicken Sie auf **Speichern**.