Firewall Advanced

Making a change to some pulldowns on this page will automatically change the context below it, enabling you to fill only the appropriate fields for the change you have made.

Drop incoming ICMP Echo requests to LAN   Off ⌄

Drop incoming ICMP Echo requests to Device LAN Address   On ⌄

Drop incoming ICMP Echo requests to Device WAN Address   On ⌄

Reflexive ACL   On ⌄

ESP ALG   Off ⌄

SIP ALG   On ⌄

Save   **Cancel**   **Restore Defaults**

Help

Drop incoming ICMP Echo requests to LAN: This setting is primarily intended for the Public Subnet (IPv4 hosts). If enabled, all echo requests coming from the Internet to LAN-side devices will be dropped.

Drop incoming ICMP Echo requests to Device LAN address: This setting is primarily intended for the IPv6 address of the Device and is not applicable to IPv6 connected LAN client addresses. If enabled, all echo requests coming from the Internet to Device LAN address of the BGW320-505 will be dropped.

Drop incoming ICMP Echo requests to Device WAN address: If enabled, all echo requests coming from the Internet to WAN-side IPv4 and IPv6 addresses of the BGW320-505, will be dropped.

Reflexive ACL: When IPv6 is enabled, you can enable Reflexive Access Control Lists to deny inbound IPv6 traffic unless this traffic results from returning outgoing packets (except as configured through firewall rules).

ESP ALG: This feature helps ESP (IPsec encryption) work properly when using NAT. Can sometimes cause problems for non-NATed hosts (such as devices on the Public LAN).

SIP ALG: This feature understands the SIP protocol used by the specific applications and does a protocol packet-inspection of traffic through it. A NAT router with a built-in SIP ALG can re-write information within the SIP messages (SIP headers and SDP body) making signaling and audio traffic between the client behind NAT and the SIP endpoint possible.

Restore Defaults: Restore the Firewall configurations and Packet Filters to default state by clicking this button.

Site Map