your future life

Firewall

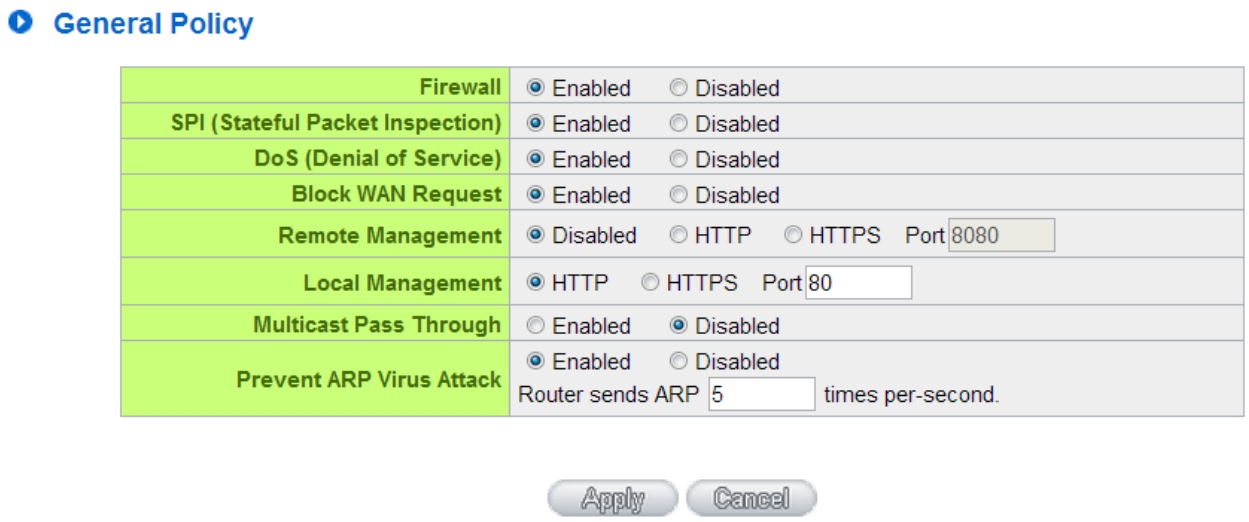
User Manual

IX. Firewall

This chapter introduces firewall general policy, access rule, and content filter settings to ensure network security.

9.1 General Policy

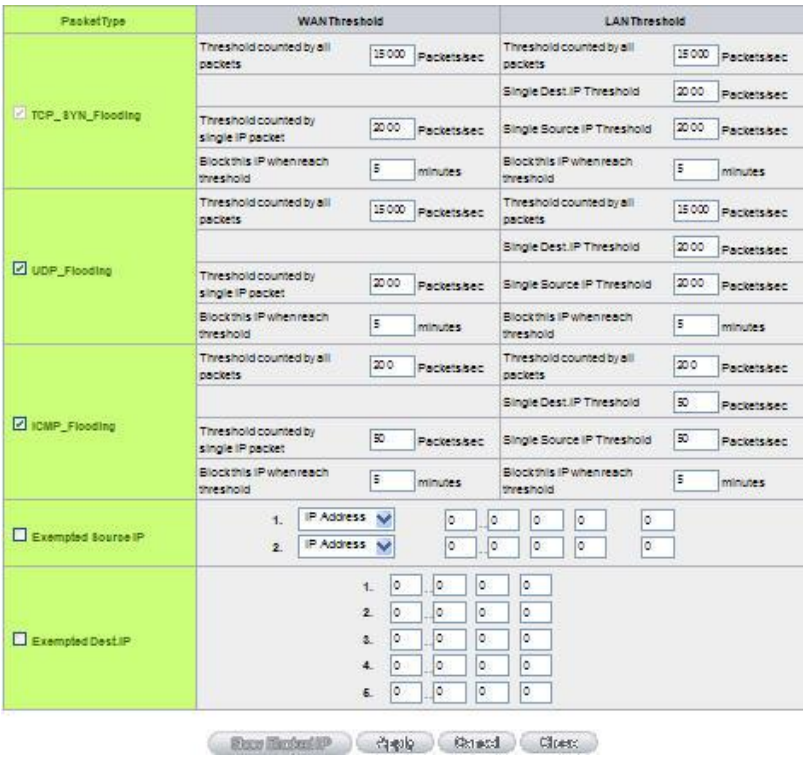
The firewall is enabled by default. If the firewall is set as disabled, features such as SPI, DoS, and outbound packet responses will be turned off automatically. Meanwhile, the remote management feature will be activated. The network access rules and content filter will be turned off.



Firewall：	This feature allows users to turn on/off the firewall.
SPI (Stateful Packet Inspection)：	This enables the packet automatic authentication detection technology. The Firewall operates mainly at the network layer. By executing the dynamic authentication for each connection, it will also perform an alarming function for application procedure. Meanwhile, the packet authentication firewall may decline the connections which use non-standard communication protocol.

DoS (Denial of Service) :	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and so on.
Block WAN request :	If set as Enabled, then it will shut down outbound ICMP and abnormal packet responses in connection. If users try to ping the WAN IP from the external, this will not work because the default value is set as activated in order to decline the outbound responses.
Remote management:	If you would like to connect VPN firewall setting page through remote management, the feature is required to be enabled. Then, the VPN firewall setting page could be accessed by inputing the WAN IP address of VPN firewall with the port number on the browser. Http mode: Default is 8080. You could change it to 80 or 1024 above. Httpsmode: Default is 443. Youc could change it to 1024 above.
Local Management :	Input the port number for controlling LAN network to VPN firewall setting page. Http mode: Default is 8080. You could change it to 80 or 1024 above. Https mode: Default is 443. Youc could change it to 1024 above.
Multicast Pass Through :	There are many audio and visual streaming media on the network. Broadcasting may allow the client end to receive this type of packet message format. This feature is off by default.
Prevent ARP Virus Attack :	This feature is designed to prevent the intranet from being attacked by ARP spoofing, causing the connection failure of the PC. This ARP virus cheat mostly occurs in Internet cafes. When attacked, all the online computers disconnect immediately or some computers fail to go online. Activating this feature may prevent the attack by this type of virus.

Advanced Setting



Packet Type: This device provides three types of data packet transmission: TCP-SYN-Flood, UDP-Flood and ICMP-Flood.

WAN Threshold: When all packet values from external attack or from single external IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes OBJ 176). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.

LAN Threshold: When all packet values from internal attack or from single internal IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.

Exempted Source IP : Input the exempted source IP.

Exempted Dest. IP : Input the exempted Destination IP addresses.

Show Blocked IP :	 Show the blocked IP list and the remained blocked time.
Restricted WEB Features :	It supports the block that is connected through: Java, Cookies, Active X, and HTTP Proxy access.
Don't Block Java / ActiveX / Cookies Proxy to Trusted Domain :	If this option is activated, users can add trusted network or IP address into the trust domain, and it will not block items such as Java/ActiveX/Cookies contained in the web pages from the trust domains.
Apply :	Click **"Apply"** to save the configuration.
Cancel :	Click **"Cancel"** to leave without making any change.