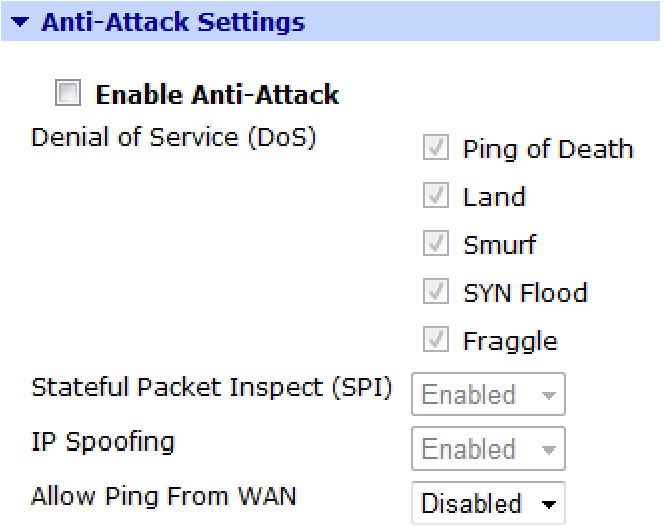
Anti-Attack Settings on DIGI WI-POINT 3G

The DIGI WI-POINT 3G has a feature called Anti-Attack. This feature keeps the Digi Wi-Point3G safe from a hacker's attack from the Internet. The Anti-Attack feature includes the following safe guards for Denial of Service (DoS), Stateful Packet Inspect (SPI), IP Spoofing, and "Allow Ping From WAN".



▼ Anti-Attack Settings

□ **Enable Anti-Attack**

Denial of Service (DoS)
☑ Ping of Death
☑ Land
☑ Smurf
☑ SYN Flood
☑ Fraggle

Stateful Packet Inspect (SPI): Enabled
IP Spoofing: Enabled
Allow Ping From WAN: Disabled

To configure the settings for Anti-Attack, you may go to the "***Configuration***"->"***Security***" page, and click on the "***Anti-Attack Settings***".

Denial of Service (DoS)

Denial of Service (DoS) includes "Ping of Death", "Land", "Smurf", "SYN Flood" and "Fraggle". When the box is checked, the DIGI WI-POINT 3G will be able to defend against the attacks.

Ping of Death: Ping of Death uses a 'PING' utility to create an IP packet that exceeds the maximum 65535 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot.

Land: In a LAN attack, hackers flood SYN packets to the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Smurf: Smurf, and Smurf type attacks, begin when a hacker sends a large amount of ICMP echo (ping) traffic to a subnet broadcast address (say, for instance, xxx.xxx.xxx.255 - the 255 number marks this as a broadcast address). This traffic will have a spoofed return address. This spoofed address will be the address of the intended victim of the attack. When individual machines on the network receive the ICMP echo requests, they will reply with an echo reply. These replies will all go to the address spoofed in the original ICMP echo requests. On networks with a large number of systems, the traffic generated could be voluminous indeed. The system which is the victim of the attack (as indicated by the spoofed IP address) quickly becomes overwhelmed by incoming traffic, and will almost certainly lose connectivity to the Internet.

SYN Flood: SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response, while the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

Fraggle: The Fraggle DoS attack is essentially based on the same concept as the Smurf attack (namely that generating huge amounts of network traffic will disable a machine or cause it to lose connectivity to the Internet), but uses UDP instead of ICMP. Although it is not as serious as some other attacks of this type, it will still generate a huge amount of network traffic. Here is how it works: a hacker is armed with a list of broadcast addresses, to which he/she sends spoofed UDP packets. Usually the packets are directed to port 7 on the target machines, which is the echo port. Other times, it is directed to the chargen port (a port that generates a number of characters when queried). Sometimes a hacker is able to set up a loop between the echo and chargen ports, generating all that much more network traffic.

Stateful Packet Inspect (SPI)

Stateful Packet Inspection is a smarter form of packet filtering, which inspects headers of network "packets." it blocks any packet arriving at the securityservices claiming to be a solicited response.

IP Spoofing

Many DoS attacks also use IP Spoofing as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or security services into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or security services.

Allow Ping from WAN

By default, DIGI WI-POINT 3G will drop the ping requests from the Internet, and it will not response to those request. Some of the attacks are performed by sending lots of fast ping with different size packets, if the router responses to these requests, it will use a lot of resources. If you want to ping the router from the Internet to see if the router is reachable or not, you would set this option to “***Enabled***”. This assumes that the mobile carrier allows you to ping the mobile IP.