Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the firewall will support full operation as initiated from the local LAN.

The firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Intrusion Detection Feature**

SPI and Anti-DoS firewall protection : ☑

RIP defect : ☑

Discard Ping to WAN Port : ☑

- **Stateful Packet Inspection**

Packet Fragmentation ☑

TCP Connection ☑

UDP Session ☑

FTP Service ☑

H.323 Service ☑

TFTP Service ☑

- **When hackers attempt to enter your network, we can alert you by e-mail**

E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :

- **Connection Policy**

Fragmentation half-open wait: 10 secs

TCP SYN wait: 30 sec.

TCP FIN wait: 5 sec.

TCP connection idle timeout:	3600	sec.
UDP session idle timeout:	30	sec.
H.323 data channel idle timeout:	180	sec.

- **DoS Detect Criteria**

Total incomplete TCP/UDP sessions HIGH:	300	session
Total incomplete TCP/UDP sessions LOW:	250	session
Incomplete TCP/UDP sessions (per min) HIGH:	250	session
Incomplete TCP/UDP sessions (per min) LOW:	200	session
Maximum incomplete TCP/UDP sessions number from same host:	10	session
Incomplete TCP/UDP sessions detect sensitive time period:	300	msec.
Maximum half-open fragmentation packet number from same host:	30	
Half-open fragmentation detect sensitive time period:	10000	msec.
Flooding cracker block time:	300	sec.

Apply Cancel