**IP and TCP/IP Anomaly Detection**

The Internet Protocol standard RFC 791, *Internet Protocol* specifies a set of eight options that provide special routing controls, diagnostic tools, and security. Attackers can misconfigure IP options to evade detection mechanisms and/or perform reconnaissance on a network.

To detect (and block) anomalous IP fragments as they pass through the zone, configure the settings as described in [Table 1](http://www.juniper.net/techpubs/en_US/nsm2011.4/topics/task/operational/security-service-firewall-ip-tcp-ip-anomaly-detection.html#ip-tcp-anomaly).

*Table 1: IP Setting Options*

| IP Setting Options | Your Action |
| --- | --- |
| Block Bad IP Options | Select this option to block packets with an IP datagram header that contains an incomplete or malformed list of IP options. |
| Timestamp IP Option Detection | Select this option to block packets in which the IP option list includes option 4 (Internet Timestamp). The timestamp option records the time when each network device receives the packet during its trip from the point of origin to its destination, as well as the IP address of each network device and the transmission duration of each one. If the destination host has been compromised, attackers can discover the network topology and addressing scheme through which the packet passed. |
| Security IP Option Detection | Select this option for hosts to send security, compartmentation, TCC (closed user group) parameters, and Handling Restriction Codes compatible with U.S. Department of Defense requirements. |
| Stream IP Option Detection | Select this option to block packets in which the IP option is 8 (Stream ID). Packets must use the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept. |
| Record Route IP Option Detection | Select this option to block packets in which the IP option is 7 (Record Route). Attackers might use this option to record the series of Internet addresses through which a packet passes, enabling them to discover network addressing schemes and topologies. |
| Loose Source IP Option Detection | Select this option to block packets in which the IP option is 3 (Loose Source Routing). The Loose Source Routing option enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP can use any number of routes from other intermediate gateways to reach the next address in the route. |
| Strict Source IP Option Detection | Select this option to block packets in which the IP option is 9 (Strict Source Routing). The Strict Source Routing enables the packet to supply routing information used by the gateways when forwarding the packet to the destination; the gateway or host IP must send the datagram directly to the next address in the source route, and only through the directly connected network indicated in the next address to reach the next gateway or host specified in the route. |
| Source Route IP Option Filter | Select this option to block all IP traffic that contains the Source Route option. The Source Route option enables the IP header to contain routing information that specifies a different source than the header source. Attackers can use the Source Route option to send a packet with a phony source IP address; all responses to the packet are sent to the attacker’s real IP address. |

Attackers can craft malicious packets (and packet fragments) that contain anomalies designed to bypass detection mechanisms and gain targeted information about a network. Because different operating systems (OS) respond differently to anomalous packets, attackers can determine the OS running on a target by examining the target’s response to the packet. To protect targets in the security zone from these reconnaissance attempts, you can configure the settings as described in [Table 2](http://www.juniper.net/techpubs/en_US/nsm2011.4/topics/task/operational/security-service-firewall-ip-tcp-ip-anomaly-detection.html#tcp-ip-setting-option).

*Table 2: TCP/IP Setting Options*

| TCP Setting Options | Your Action |
| --- | --- |
| SYN Fragment Detection | Select this option to detect TCP fragments that contain a SYN flag. A SYN flag in TCP segment initiates a connection but does not usually contain a payload. Because the packet is small, it should not be fragmented. |
| Drop Packet without TCP Flags Set | Select this option to detect TCP segment headers that do not have at least one flag control set. |
| Block SYN with FIN TCP Segments | Select this option to detect packets in which both the SYN and FIN flags are set. The SYN flag synchronizes sequence numbers to initiate a TCP connection and the FIN flag indicates the end of data transmission to finish a TCP connection, so both flags should never be set in the same packet. |
| Block FIN without ACK TCP Segments | Select this option to detect packets in which the FIN flag is set, but the ACK flag is not. The FIN flag signals the conclusion of a session and terminates the connection; normally the ACK flag is also set to acknowledge the previous packet received. |
| Drop Packets with an Unknown Protocol | Select this option to drop packets in which the protocol field is set to 101 or greater. Protocol types 101 and higher are currently reserved and undefined. |