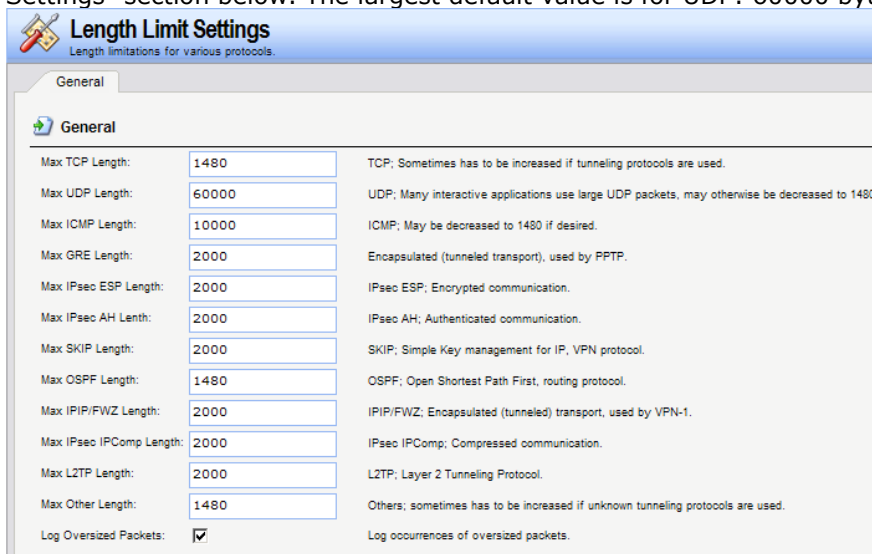


The "ping of death" is one of the earliest layer 3/4 attacks. One of the simplest ways to execute it is to run "ping -l 65510 1.2.3.4" on a Windows 95 system where 1.2.3.4 is the IP address of the intended victim. "Jolt" is simply a purpose-written program for generating such packets on operating systems whose ping commands refuse to generate oversized packets.

The triggering factor is that the last fragment makes the total packet size exceed 65535 bytes, which is the highest number that a 16-bit integer can store. When the value overflows, it jumps back to a very small number. What happens then is a function of how well the victim's IP stack is implemented.

[Solution]

Netdefend Firewall will never allow fragments through that would result in the total size exceeding 65535 bytes. In addition to that, there are configurable limits for IP packet sizes in the "Advanced Settings" section below. The largest default value is for UDP: 60000 bytes.



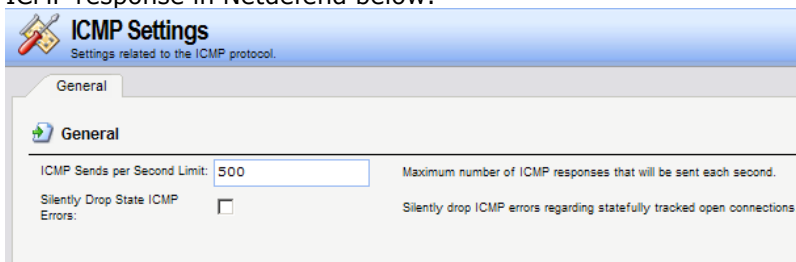
Length Limit Settings
Length limitations for various protocols.

General

General

| | | |
|--------------------------|-------------------------------------|---|
| Max TCP Length: | 1480 | TCP; Sometimes has to be increased if tunneling protocols are used. |
| Max UDP Length: | 60000 | UDP; Many interactive applications use large UDP packets, may otherwise be decreased to 1480. |
| Max ICMP Length: | 10000 | ICMP; May be decreased to 1480 if desired. |
| Max GRE Length: | 2000 | Encapsulated (tunneled transport), used by PPTP. |
| Max IPsec ESP Length: | 2000 | IPsec ESP; Encrypted communication. |
| Max IPsec AH Length: | 2000 | IPsec AH; Authenticated communication. |
| Max SKIP Length: | 2000 | SKIP; Simple Key management for IP, VPN protocol. |
| Max OSPF Length: | 1480 | OSPF; Open Shortest Path First, routing protocol. |
| Max IP/IP/FWZ Length: | 2000 | IP/IP/FWZ; Encapsulated (tunneled) transport, used by VPN-1. |
| Max IPsec IPComp Length: | 2000 | IPsec IPComp; Compressed communication. |
| Max LZTP Length: | 2000 | LZTP; Layer 2 Tunneling Protocol. |
| Max Other Length: | 1480 | Others; sometimes has to be increased if unknown tunneling protocols are used. |
| Log Oversized Packets: | <input checked="" type="checkbox"/> | Log occurrences of oversized packets. |

Ping of death will show up in Netdefend Firewall logs as drops with the rule name set to "LogOversizedPackets". The sender IP address may be spoofed. And we can set a threshold for ICMP response in Netdefend below:



ICMP Settings
Settings related to the ICMP protocol.

General

General

| | | |
|----------------------------------|--------------------------|--|
| ICMP Sends per Second Limit: | 500 | Maximum number of ICMP responses that will be sent each second. |
| Silently Drop State ICMP Errors: | <input type="checkbox"/> | Silently drop ICMP errors regarding statefully tracked open connections. |