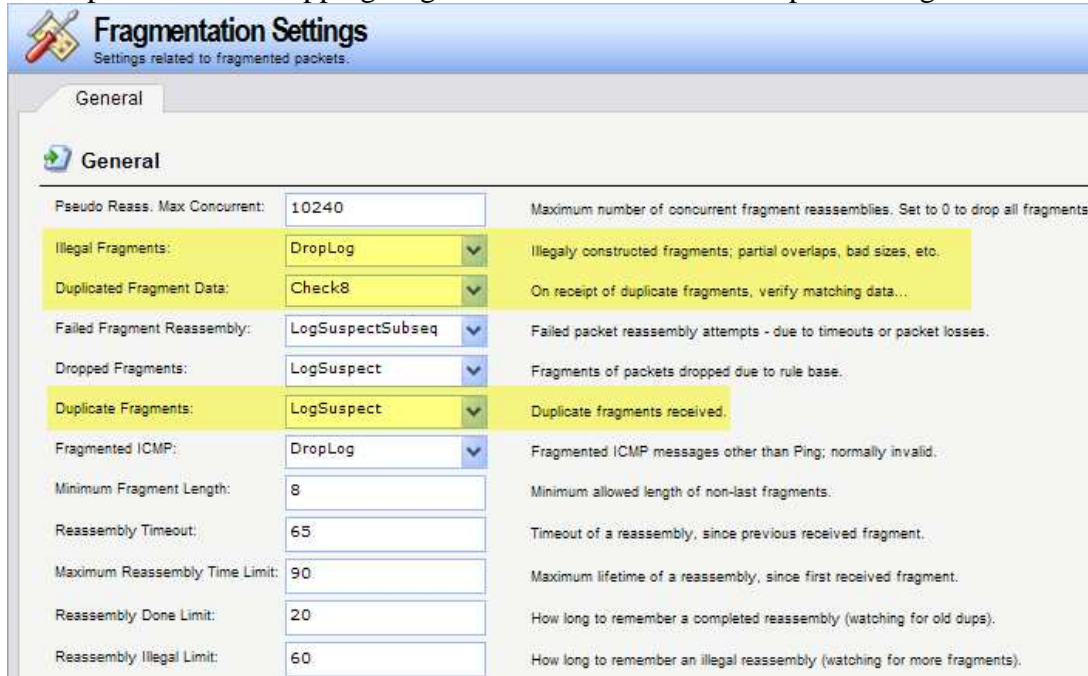


Teardrop and its followers are fragment overlap attack. Many IP stacks have shown erratic behavior (excessive resource exhaustion or crashes) when exposed to overlapping fragments.

[Solution]

By default settings of Netdefend Firewall below, it protects fully against fragmentation overlap attacks. Overlapping fragments are never allowed to pass through the firewall.



The screenshot shows the 'Fragmentation Settings' window in Netdefend Firewall. The title bar reads 'Fragmentation Settings' with a subtitle 'Settings related to fragmented packets.' Below the title bar is a 'General' tab. The main area is titled 'General' and contains a list of settings:

Setting Name	Value	Description
Pseudo Reass. Max Concurrent:	10240	Maximum number of concurrent fragment reassemblies. Set to 0 to drop all fragments.
Illegal Fragments:	DropLog	Illegally constructed fragments; partial overlaps, bad sizes, etc.
Duplicated Fragment Data:	Check8	On receipt of duplicate fragments, verify matching data...
Failed Fragment Reassembly:	LogSuspectSubseq	Failed packet reassembly attempts - due to timeouts or packet losses.
Dropped Fragments:	LogSuspect	Fragments of packets dropped due to rule base.
Duplicate Fragments:	LogSuspect	Duplicate fragments received.
Fragmented ICMP:	DropLog	Fragmented ICMP messages other than Ping; normally invalid.
Minimum Fragment Length:	8	Minimum allowed length of non-last fragments.
Reassembly Timeout:	65	Timeout of a reassembly, since previous received fragment.
Maximum Reassembly Time Limit:	90	Maximum lifetime of a reassembly, since first received fragment.
Reassembly Done Limit:	20	How long to remember a completed reassembly (watching for old dups).
Reassembly Illegal Limit:	60	How long to remember an illegal reassembly (watching for more fragments).

Teardrop and its followers will show up in Netdefend Firewall logs as drops with the rule name set to "IllegalFrag". The sender IP address may be spoofed.