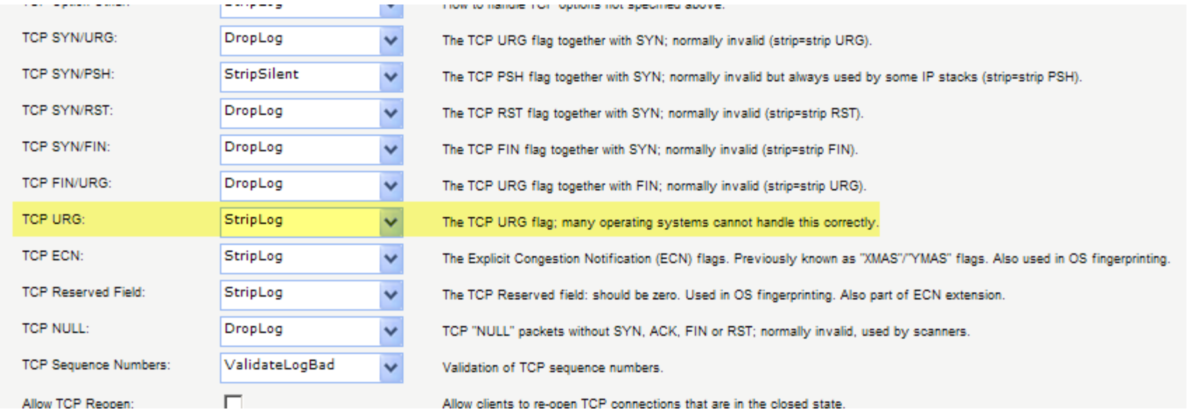
The WinNuke attack works by connecting to a TCP service that does not have handlers for "out-of-band" data (TCP segments with the URG bit set), but still accepts such data. This will usually put the service in a tight loop that consumes all available CPU time.

One such service was the NetBIOS over TCP/IP service on Windows machines, which gave the attack its name.

[Solution]

Netdefend Firewall protects against this in two ways:

- With a careful inbound policy, the attack surface is greatly reduced. Only exposed services could possibly become victims to the attack, and public services tend to be more well-written than services expected to only serve the local network.
- By stripping the URG bit by default from all TCP segments traversing the firewall (configurable via Advanced Settings -> TCP -> TCPUrg).



TCP Option Other:	StripLog	How to handle TCP options not specified above.
TCP SYN/URG:	DropLog	The TCP URG flag together with SYN; normally invalid (strip=strip URG).
TCP SYN/PSH:	StripSilent	The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH).
TCP SYN/RST:	DropLog	The TCP RST flag together with SYN; normally invalid (strip=strip RST).
TCP SYN/FIN:	DropLog	The TCP FIN flag together with SYN; normally invalid (strip=strip FIN).
TCP FIN/URG:	DropLog	The TCP URG flag together with FIN; normally invalid (strip=strip URG).
TCP URG:	StripLog	The TCP URG flag; many operating systems cannot handle this correctly.
TCP ECN:	StripLog	The Explicit Congestion Notification (ECN) flags. Previously known as "XMAS"/"YMAS" flags. Also used in OS fingerprinting.
TCP Reserved Field:	StripLog	The TCP Reserved field: should be zero. Used in OS fingerprinting. Also part of ECN extension.
TCP NULL:	DropLog	TCP "NULL" packets without SYN, ACK, FIN or RST; normally invalid, used by scanners.
TCP Sequence Numbers:	ValidateLogBad	Validation of TCP sequence numbers.
Allow TCP Reopen:	□	Allow clients to re-open TCP connections that are in the closed state.

WinNuke attacks will usually show up in Netdefend Firewall logs as normal drops with the name of the rule in your policy that disallowed the connection attempt. For connections allowed through the firewall, "TCP" or "DROP" category (depending on the TCPUrg setting) entries will appear, with a rule name of "TCPUrg". The sender IP address is not likely to be spoofed; a full three-way handshake must be completed before out-of-band segments can be sent.