This category of attacks all make use of "amplifiers": poorly configured networks who amplify a stream of packets and send it to the ultimate target. The goal is excessive bandwidth consumption - consuming all of the victim's Internet connection capacity. An attacker with sufficient bandwidth can forgo the entire amplification stage and simply stream enough bandwidth at the victim. However, these attacks allows attackers with less bandwidth than the victim to amplify their data stream to overwhelm the victim.

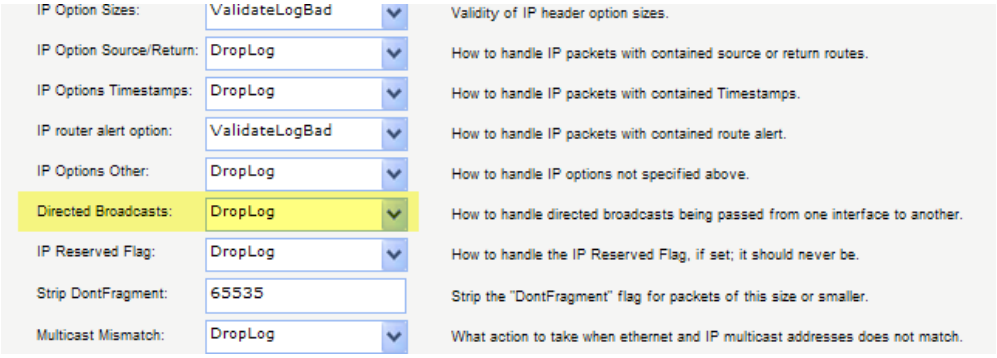
- "Smurf" and "Papasmurf" send ICMP echo packets to the broadcast address of open networks with many machines, faking the source IP address to be that of the victim. All machines on the open network then "respond" to the victim.
- "Fraggle" uses the same general idea, but instead using UDP echo (port 7) to accomplish the task. Fraggle generally gets lower amplification factors since there are fewer hosts on the Internet that have the UDP echo service enabled.

[Solution]

Smurf attacks will show up in Netdefend Firewall logs as mases of dropped ICMP Echo Reply packets. The source IP addresses will be those of the amplifier networks used.
Fraggle attacks will show up in Netdefend Firewall logs as masses of dropped (or allowed, depending on policy) packets. The source IP addresses will be those of the amplifier networks used.

Avoiding becoming an amplifier

Even though the brunt of the bandwidth stream is at the ultimate victim's side, being selected as an amplifier network can also consume great resources. In its defalt configuration, Netdefend Firewall explicitly drops packets sent to broadcast address of directly connected networks (configurable via Advanced Settings -> IP -> DirectedBroadcasts) as below. However, with a reasonable inbound policy, no firewall-protected network should ever have to worry about becoming a smurf amplifier.



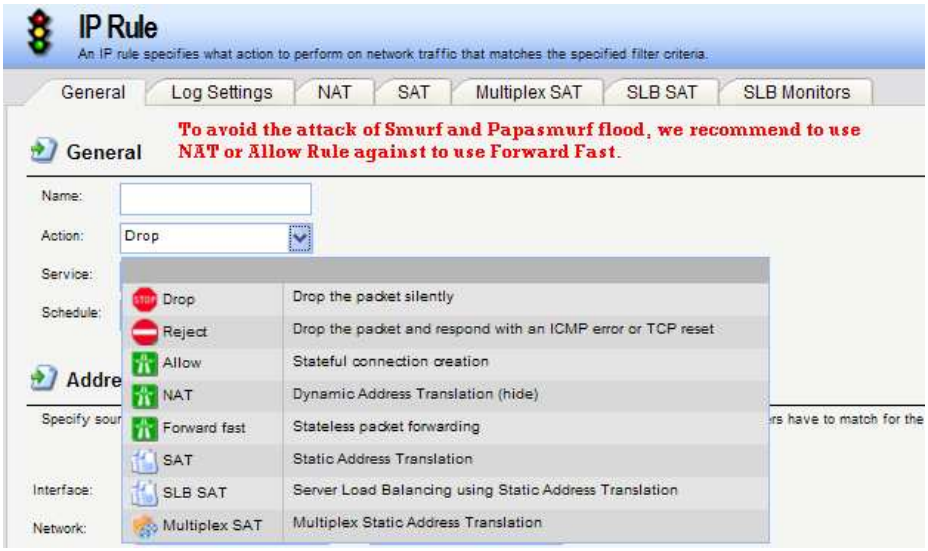
Protection at the ultimate victim side

Smurf, and its followers, are resource exhaustion attacks. More specifically: they exhaust your Internet connection. In the general case, the firewall is situated at the "wrong" side of the Internet connection bottleneck to provide much protection against this class of attacks. The damage has already been done by the time the packets reach the firewall.

However, Netdefend Firewall may be of some help in keeping the load off of internal servers, making them available for internal service, or perhaps service via a secondary Internet connection not targeted by the attack.

- Smurf and Papasmurf floods will be seen as ICMP Echo Responses at the victim side. Unless "FwdFast" rules are in use, such packets are never allowed to initiate new connections, regardless of whether or not there are rules that allow the traffic.(For some

specific network environment the FwdFast rule must be involved, if so, we recommend to use the filter function in IP rules for particular source network.)



- Fraggle packets may arrive at any UDP destination port of the attacker's discretion. Tightening ones inbound ruleset may help.
- Traffic Shaping may also help absorb some of the flood before it reaches protected servers.