The Land and LaTierra attacks works by sending a packet to a victim and making the victim respond back to itself, which in turn generates yet another response to itself, etc etc. This will either bog the victim's machine down, or make it crash.

The attack is accomplished by using the victim's IP address in the source field of an IP packet as well as in the destination field.

[Solution]

Netdefend Firewall protects against this attack by applying IP spoofing protection to all packets. In its default configuration, it will simply compare arriving packets to the contents of the routing table; if a packet arrives on an interface that is different from the interface where the firewall expects the source to be, the packet will be dropped.

Land and LaTierra attacks will show up in Netdefend Firewall logs as drops with the rule name set to "AutoAccess" by default, of, if you have written custom Access rules as below, the name of the Access rule that dropped the packet. The sender IP address is of no interest; it is always the same as the destination IP address.

Note that applying wide-open "Accept" rules in the "Access" section will disable this protection.