EvilMiddlebox

An evil middlebox is a transparent device that sits inbetween an end-to-end connection that disturbs the normal end-to-end traffic in some way. As you can not see these devices which usually work on layer 2, it is difficult to debug issues that involve them. Examples are HTTP proxy, Gateway proxy (all protocols). Normally, these devices are installed for security reasons to filter out "bad" traffic. Bad traffic may be viri, trojans, evil javascript, or anything that is not known to the device. Sometimes also so called rate shapers are installed as middleboxes; while these do not change the contents of the traffic, they do drop packets according to rules only known by themselves. Bugs in such middleboxes can have fatal consequences for "legitimate" Internet traffic which may lead to performance or even worse connection issues.

Middleboxes come in all shapes and flavors. The most popular are firewalls:

- [Check Point VPN-1 & FireWall-1 NG Performance Tuning Guide|http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html]

Examples of experienced performance issues

Two examples in the beginning of 2005 in SWITCH:

- HttpProxy: very slow response from a webserver only for a specific circle of people
- GatewayProxy: tcp transfers get stalled as soon as a packet is lost on the local segment from the middlebox to the end host.

A Cisco IOS Firewall in August 2006 in Funet:

- WindowScalingProblems: when window scaling was enabled, TCP performance was bad (10-20 KBytes/sec). Some older versions of PIX could also be affected by window scaling issues.

DNS Based global load balancing problems

- Why DNS Based Global Server Load Balancing (GSLB) Doesn't Work

Juniper SRX3600 mistreats fragmented IPv6 packets

- Counting IPv6 DNS
  This firewall (up to at least version 11.4R3.7) performs fragment reassembly in order to apply certain checks to the entire datagram, for example in "DNS ALG" mode. It then tries to forward the reassembled packet instead of the initial fragments, which triggers ICMP "packet too big" messages if the full datagram is larger than the MTU of the next link. This will lead to a permanent failure on this path, because the (correct) fragmentation at the sender is annihilated by the erroneous reassembly at the firewall.

The same issue has also been found with some models of the Fortigate firewall.

– Main.ChrisWelti - 01 Mar 2005
-
- Main.PekkaSavola - 10 Oct 2006

-- Main.PekkaSavola - 07 Nov 2006

-- Main.AlexGall - 2012-10-31