Subject: iptables classifies ESTABLISHED packets as INVALID randomly
Posted by Tony2 on Wed, 22 Oct 2008 09:49:48 GMT
View Forum Message <> Reply to Message

Dear all,

I have a problem that I was trying to troubleshot for a long time without success. So I post it here, hopefully someone can give me a hint how to move on with it. I will try to put the long story short.

- HN: running debian etch amd64, fza kernel, has several public IPs, running iptables to DNAT one of the public IP to VE

- VE: also running debian + nginx + php as a web server. no iptables, no customized routing rules.

- problem: sometimes connection to the web server is timed out. But re-connecting always works. This happens a few times per day.

- I set a cron job that tries to connect to the web server every 5min, and run tcpdump on both sides to capture the relevant packets. When the connection is timeout out, record the time for easier examination.

- run wireshark on captured packets to have a closer look: when the problem happens, I see the following:
1. the client sends a SYN packet
2. the web server sends back a SYN/ACK packet
3. iptables on HN for some reason classifies the SYN/ACK packet as INVALID and drops it. So the connection is timed out, and when the clients re-connects, it works.

- I compared the dropped packets with those in "normal" connections: nothing weird found, it looks just like the other.

- I also tried to run another kernel instead of fza (from http://download.openvz.org/debian). The result is the same.

I attached relevant files (some IPs changed). tcpdump was run on venet0.

Please let me know if you need any further information.

thanks for your consideration.

File Attachments

1) iptables-rules.gz, downloaded 371 times
2) routing.txt, downloaded 463 times
3) tcpdump-on-HN-normal-session.txt.gz, downloaded 343 times
4) tcpdump-on-HN-problematic-session.txt.gz, downloaded 348

times

Subject: Re: iptables classifies ESTABLISHED packets as INVALID randomly
Posted by Tony2 on Thu, 23 Oct 2008 07:01:42 GMT
View Forum Message <> Reply to Message

I forgot to show the log from iptables when the problem happens: it looks like this:

Oct 22 14:16:09 eu3 kernel: Detected-from-wiki: IN=venet0 OUT=eth0 SRC=192.168.100.130 DST=129.70.186.31 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=80 DPT=41348 WINDOW=5792 RES=0x00 ACK SYN URGP=0

Oct 22 14:16:09 eu3 kernel: Blocked-Invalid: IN=venet0 OUT=eth0 SRC=192.168.100.130 DST=129.70.186.31 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=80 DPT=41348 WINDOW=5792 RES=0x00 ACK SYN URGP=0

It looks like there is some problem with the connection tracking system. A workaround could be avoiding use of statefulness of iptables, but it doesn't sound like a good step.

Subject: Re: iptables classifies ESTABLISHED packets as INVALID randomly
Posted by Tony2 on Fri, 24 Oct 2008 21:52:31 GMT
View Forum Message <> Reply to Message

FWIW: I tried another kernel linux-image-2.6.24-openvz-24-004.1d1-amd64_004.1d1_amd64.deb and the result is the same.

It seems I must give up stateful rules for iptables. Any hint please?