Bogon Rule (partly) Blocking IPV6

Hello,

When defining rules for Simple Service Discovery Protocol (SSDP), I discovered a serious bug. Luckily with “some form of” workaround possible.

I have a network divided in multiple subnets using a vlan per subnet. For each subnet there is a interface witch corresponding rules.

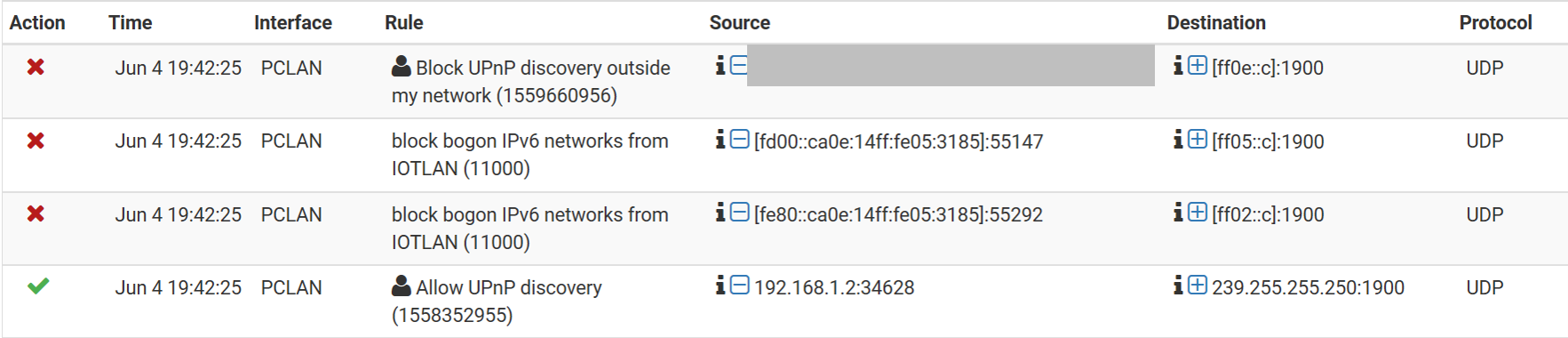
Since I am using firewall rules as strict as possible, I normally have the Bogon-rule active for each interface (WAN and LAN).

I observed following issue and ***expect the problem to be wider than*** that:

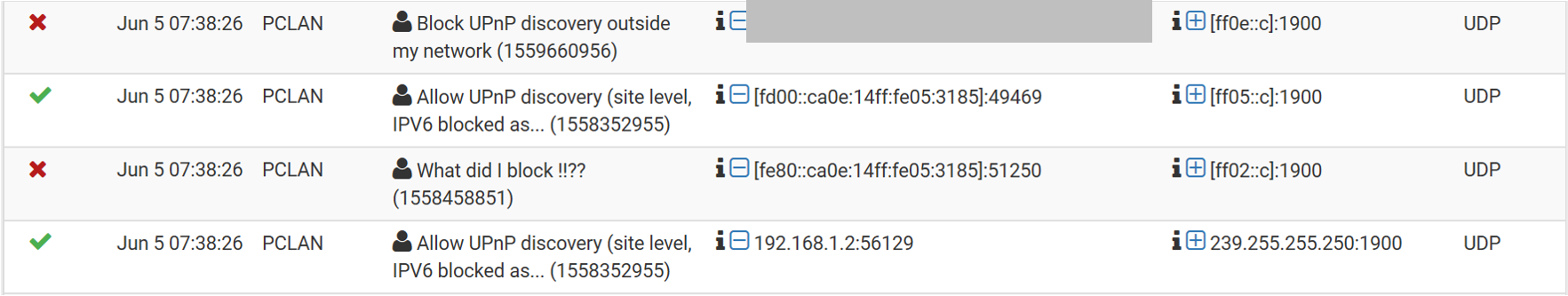
* SSDP owns the following address ranges
  + IPV4: 239.255.255.250 (IPv4 site-local address)
  + IPV6: [FF02::C] (IPv6 [link-local](https://en.wikipedia.org/wiki/Link-local_address))
  + IPV6: [FF05::C] (IPv6 site-local)
  + IPV6: [FF08::C] (IPv6 organization-local)
  + IPV6: [FF0E::C] (IPv6 global)
* I defined a rule to block IPv6 global (Block UPnP discovery outside my network), with the intention to pass the rest.
* So IMHO IPV6: [FF05::C] (IPv6 site-local) should pass
* However I observed that the “block bogon IPV6-rule” blocks the other IPV6-local traffic, and that is IMHO not OK.

Attached two pieces of firewall logs, the upper one with bogon-rule activated. And below that a piece where the bogon-rule is not active.

Bogon-rule-active



Bogon-rule-not-active



Sincerely,

Louis