Virtual Private Network (VPN) traffic leakages in dual-stack hosts/networks
(draft-gont-opsec-vpn-leakages-00)

Fernando Gont
Many VPN implementations do not support IPv6
- they block local IPv4 connectivity
- but do nothing about the IPv6 connectivity

In dual-stack host/network scenarios, hosts might end up using IPv6:
- there could be IPv6-based recursive DNS servers
- a domain-name might have AAAA records
  ...either legitimately, or maliciously
Problem statement

- Sensitive traffic might leak out (privacy issue):
  - e.g. user/passwords sent in the clear
- A host might get owned over the unsecured IPv6
  - then trust relationship implied by the VPN could be leveraged by the attacker
- Popular VPN implementations found vulnerable to these issues
Possible mitigations

- Disable IPv6 when employing the VPN
- Police Neighbor Discovery and DHCPv6 packets
  - may prove to be tricky
  - ND messages could be leveraged to install more-specific routes to cause traffic leakages
  - What should be done with link-local traffic?
Thanks!

- Feedback welcome on opsec@ietf.org

Fernando Gont
fgont@si6netorks.com