Virtual Private Network (VPN) traffic leakages in dual-stack hosts/networks

(draft-gont-opsec-vpn-leakages-00)

Fernando Gont

IETF 85
Atlanta, GA, USA. November 4-9, 2012

Introduction

- Many VPN implementations do not support IPv6
  - they block local IPv4 connectivity
  - but do nothing about 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 as a result of **malicious activity**

Problem statement

- Sensitive traffic might leak out
  - e.g. user/passwords sent in the clear
- A host might get owned over the non-secured IPv6
  - then the 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
- Support IPv6, and 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?

Moving forward

- Adopt as opsec wg item?