Implications of IPv6 Addressing on Security Operations
(draft-ietf-opsec-ipv6-addressing)

F. Gont, SI6 Networks
G. Gont, SI6 Networks
Introduction
Motivation

- Differences in IPv6 vs. IPv4 addressing have concrete implications on security operations
- These might be non-obvious outside of IPv6-savvy circles, e.g.,
  - Cloud operations groups
  - Security operations groups
- Such groups continue applying IPv4 practices -> fail!
- This document has been motivated by conversations with such groups
What is behind an IPv6 prefix?

- Multiple addresses may map to a single host
  - Host typically configure multiple addresses
  - Addresses typically selected from /64
  - But a user might control a larger address block (e.g. a whole /48)
- A single IPv6 address may map to multiple hosts
  - NAT-PT for IPv6 not uncommon
  - Kubernetes typically do IPv6 ULAs + NAT
- All these aspects are key when doing IPv6 security operations
Security Operations topics

• Current version of the document discusses:
  • Enforcing Access Control Lists (ACLs)
    – Allow lists
    – Block lists
  • Network activity correlation
• But a number of additional topics have been suggested
Suggested Topics
Neighbor Cache Exhaustion

- Hosts maintain a table of IP address → MAC address mappings
  - IPv4: ARP Cache
  - IPv6: Neighbor Cache
- IPv4 subnet sizes introduce an artificial limit on the ARP cache
- But the Neighbor Cache could grow without bounds (\(2^{64}\) entries)
- Problem and operational mitigations in RFC 6583
Firewalling

- Packet filtering based on IPv6 addresses (including bogons)
- Packet filtering for typical scenarios
  - e.g., stable + privacy addresses
- Some hints in: draft-gont-v6ops-ipv6-addressing-considerations
Network Reconnaissance for security audits

- IPv6 brute-force address scans are unfeasible
- Alternative techniques exist:
  - Pattern-based IPv6 address scans
  - DNS reverse mappings
  - Learning information from IPAM platforms
  - ....and others
- Topic discussed in detail in RFC 7707
Moving forward
Moving forward

- Which topics to include?
- Any others that should be considered?