Implications of IPv6 Addressing on Security Operations

Fernando Gont

RIPE 86
Rotterdam, Netherlands. May 22-26, 2023

Motivation for this talk

How are organizations doing IPv6 security operations?

- IPv6/IPv4 differences are non-obvious outside of IPv6-savvy circles
- Such groups seem continue applying IPv4 practices -> fail!
- This talk has been motivated by interactions with such groups

Background

Some common tasks in security operations

- Enforcing Address-based Access Control Lists (ACLs)
  - Allow-lists:
    - Meant to **allow** access from a specified prefix
  - Block-lists:
    - Meant to **block** access from a specified prefix
- Network activity correlation
  - Analyze relationship between different network activities

What do we mean by IPv6 addressing “differences”?

- IPv6 addresses have an associated:
  - address scope: global, link-local, etc.
  - stability property: stable vs. temporary
  - intended usage: outgoing vs. incoming communications
- IPv6 hosts typically use multiple addresses simultaneously
- IPv6 users typically control a large IPv6 address block (e.g. a /64)

What is behind an IPv6 address or prefix?

- Multiple addresses may map to a single host
  - Host typically configure multiple addreses from a /64
  - But a user might control a larger address block (e.g. a whole /48)
  - **“Different IPv6 addresses” does not imply “different hosts”**
- A single IPv6 address may map to multiple hosts
  - NAT-PT for IPv6 is not uncommon
  - Kubernetes typically does IPv6 ULAs + NAT
  - **“Same address” does not imply “same host”**
- All these aspects are key when doing IPv6 security operations

IPv6 Security Operations

Challenges

ACLs: Allow-lists

- Use of temporary addresses (RFC8981) means:
  - Addresses change on a regular basis
  - Addresses from multiple hosts may be intermingled in the same /64
- But...What should we “allow”?
- If specifying /128s, the ACLs might fail

ACLs: Block-lists

- Quite often, these are dynamically introduced, e.g.
  - SIEM/IPS
  - fail2ban
  - IP reputation services (e.g., abuseipdb.com)
- But...what should we “block”?
- If blocking /128s, a skilled attacker might:
  - Intentionally exhaust the number of entries in your block-list
  - Circumvent the block-list (i.e., use *throw-away* IPv6 addresses)

Network Activity Correlation

- Non-trivial exercise:
  - Multiple systems might be behind a /128, or,
  - A single system might jump around within a /48, or,
  - Anything in between

IPv6 Security Operations

Possible Advice

ACLs: Allow-lists

- Employ stable addresses (only):
  - Use:
    - manual configuration, or,
    - DHCPv6, or,
    - SLAAC & disable temporary addresses (e.g. via group policies)
  - Specify allow-lists as /128s
- Embrace temporary addresses usage:
  - Segregate systems into different subnets
  - Specify allow-lists as e.g. /64s

ACLs: Block-lists

- Must select appropriate granularity to avoid circumvention
- If block-lists are dynamically-generated:
  - May need to dynamically aggregate ACLs
  - Possibly adjust the ACL lifetime based on the aggregation level

ACLs: Block-lists (II)

- One possible implementation for dynamic block-lists:

LEVEL	PREF_LEN	AGGR_THRES	ACL_LIFETIME
1	/128	10	1 hour
2	/64	10	45 min
3	/56	10	30 min
4	/48	N/A	15 min

"Where possible, aggregate at least $\texttt{AGGR\_THRES}_N$ $\texttt{LEVEL}_N$ ACLs into a single $\texttt{LEVEL}_{(N+1)}$ ACL. Remove this new ACL after $\texttt{ACL\_LIFETIME}_{(N+1)}$"

Network Activity Correlation

- Tools should readily allow activity correlation on a per-prefix basis

Conclusions

Conclusions

- 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!
- **Security operations require changes to embrace IPv6**

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com