IPv6 Security Best Practices and the Future of Cyber Defence

David Kennedy – Arkenox

Arkenox
IPv6 Security Solutions

UK IPv6 Council Annual Meeting
London 19th November 2024

Motivation

“Disable IPv6”

- Security often seen as the fun police - pushing back on adoption and advancements.
- Common to see advice such as “Disable IPv6”. Not even possible.

“IPSEC is the primary security benefit in IPv6”

- 14x less likely to receive email spam over IPv6 compared to IPv4.[1]
- IPv6 based filters 204% more likely to stop malicious traffic when compared to IPv4.[2]

“You can’t protect what you don’t know”

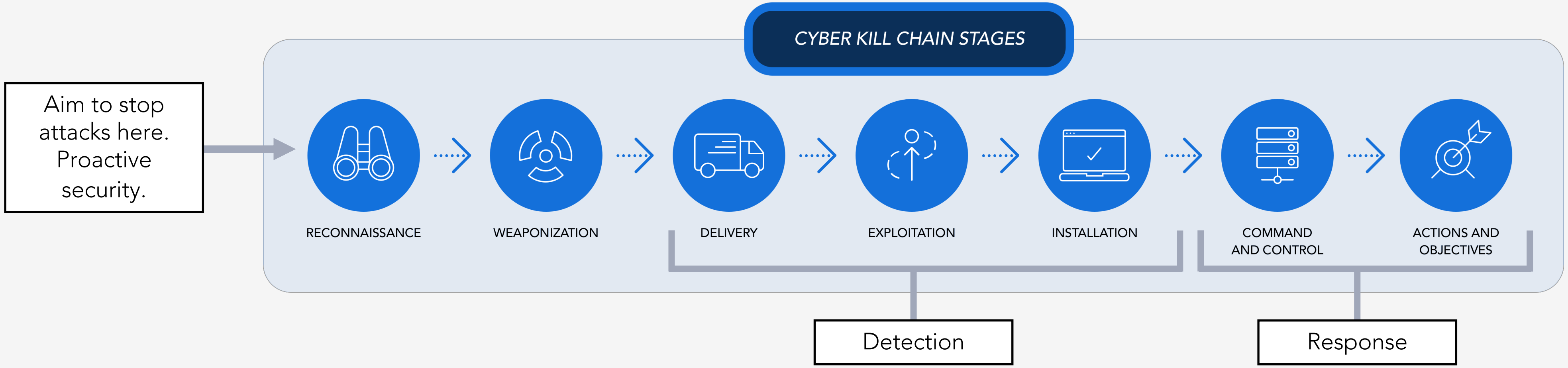
- Scanning strategies for IPv6 are constantly evolving.
- Issues often stem from not understanding IPv6 network to same level as IPv4.

1– Not that simple: Email delivery in the 21st century (2023), 2 - Towards A User-Level Understanding of IPv6 Behavior (2020)

You Can't Protect What You Don't Know

Every attack starts with understanding the target – **reconnaissance**

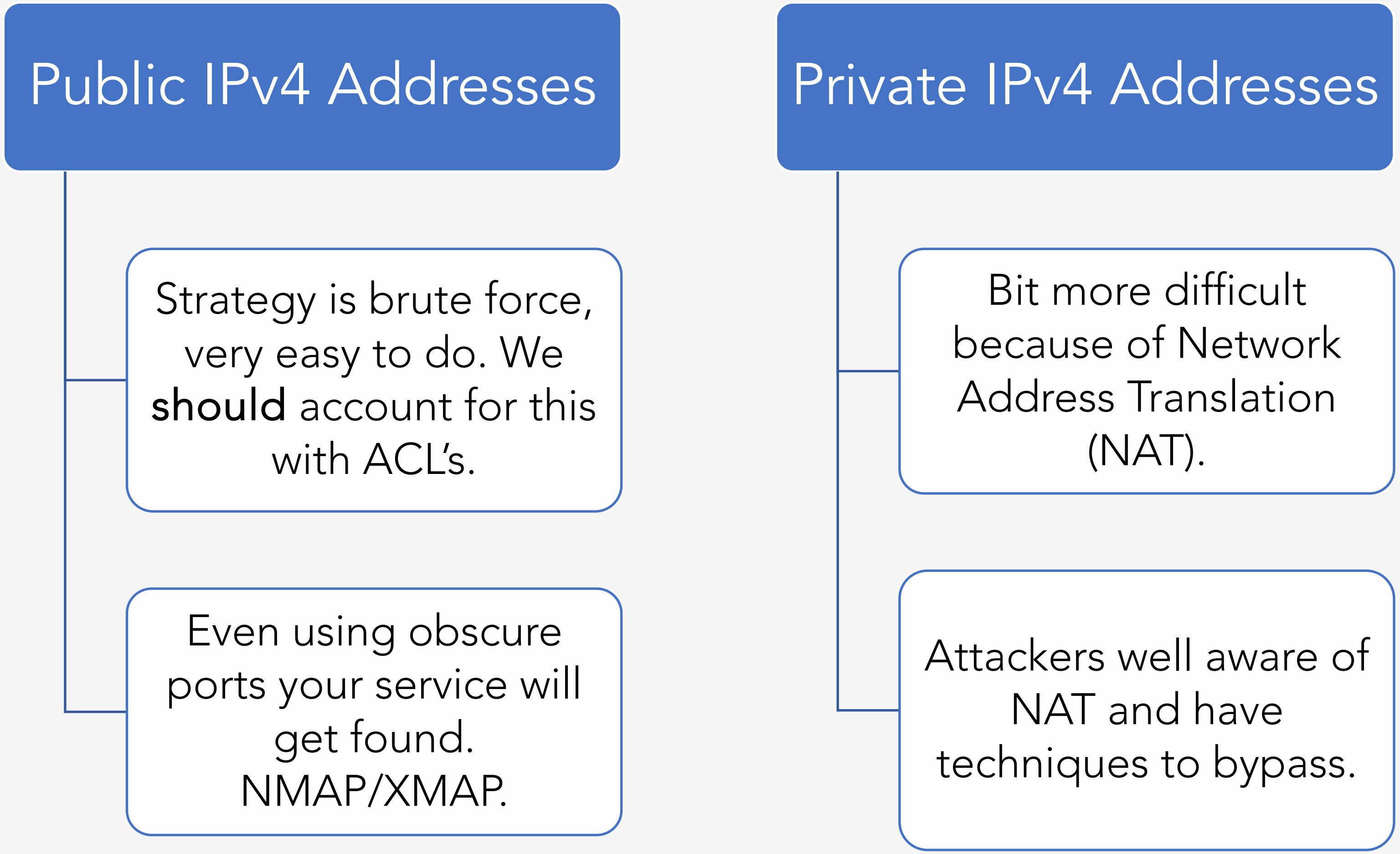
- Aim is to find oversight or weaknesses



If we can build a network that is easy to understand then:

- We can implement features that limit the ability to perform reconnaissance - stopping attacks from progressing.

Reconnaissance in IPv4



Public IPv4 Addresses

- Strategy is brute force, very easy to do. We **should** account for this with ACL's.
- Even using obscure ports your service will get found. NMAP/XMAP.

Private IPv4 Addresses

- Bit more difficult because of Network Address Translation (NAT).
- Attackers well aware of NAT and have techniques to bypass.

Reconnaissance in IPv6

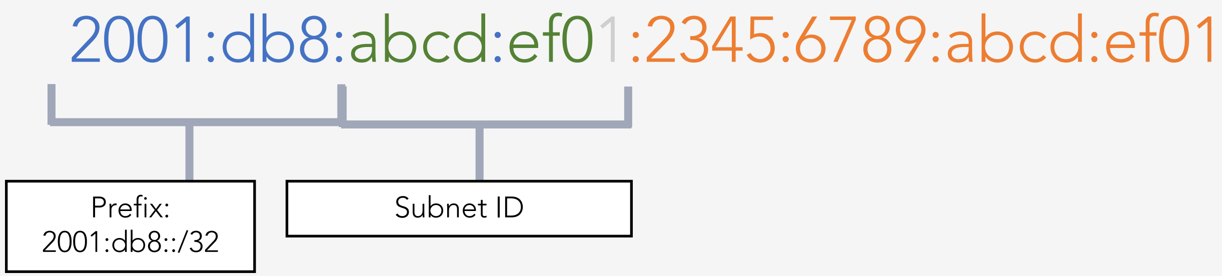
Common myth that IPv6 is not scanned – due to size of space.

- Wrong! Active scanning of global unicast addresses is occurring and happening against your networks now – our sensors see constant probing.
- But scanning strategy is different to IPv4, not feasibly possible to brute force IPv6.
- Means that some organisations do not implement correct network filters or ACL's.

IPv6 reconnaissance aims to find:

- Architectures with common and predictable patterns
- Combined with limited/no filtering and access control
- Aided by the ability for an attacker to rotate their source IP

Reconnaissance – Network Prefix/Subnets



2001:db8:abcd:ef01:2345:6789:abcd:ef01

Prefix:
2001:db8::/32

Subnet ID

Aim - Reduce the scope of reconnaissance by identifying active network prefixes/subnets.

- Fixed part of your allocation.
- Detect via DNS, rDNS, routing tables, common allocation patterns.

Identifying the prefix or subnet ID relatively easy, but still far too massive to perform IPv4 reconnaissance strategies against to find assets.

Reconnaissance – Interface ID (IID)

Should be very difficult if we all followed current RFC's. But there are still legacy global addressing strategies in use such as:

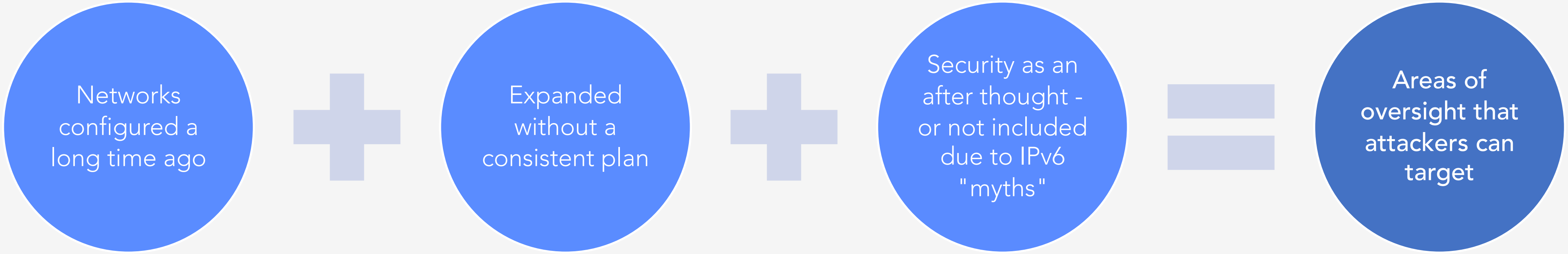
- EUI-64 - OUI = 24 bits, fffe = 16 bits. **Still around 40% of last hop routers using this method.**

Or addressing strategies that use easy to remember addresses, i.e.

- Low Byte – 2001:db8::1, 2001:db8::f
- Service Exposing Addresses - 2001:db8:1::22
- Words - 2001:db8:bad::beef
- Aliasing – Device responds to entire subnet or multiple addresses.

Rule of thumb: If an address is easy to remember, then it is easy to find. Not a bad thing if like in IPv4, we implement filtering + ACL's.

What is the Underlying Problem?



Networks configured a long time ago

+

Expanded without a consistent plan

+

Security as an after thought - or not included due to IPv6 "myths"

=

Areas of oversight that attackers can target

But IPv6 allows us to create a network with security at the foundation, with a structure that is easier to simultaneously scale and defend.

How? Going to take inspiration from a fortress for this…

Your IPv6 Network is a Fortress

Perimeter that is more clearly defined than IPv4.

- Prefix(es) allocation from RIR, LIR.
- Continuous address space, unlike with IPv4.
- Bonus: Could also ask for reservation of next adjacent address space, if possible.

We can implement rules on the network edge:

- Silently drop unsolicited inbound traffic.
- Enforce IPv6 RFCs, best practices, rate limits.
- Hierarchical nature of IPv6 means that these rules are enforced on rest of the network

Network Infrastructure

Hierarchical nature of IPv6, segment network at logical points and implement additional controls at each level:

- Based on specific use cases of each network segment.
- Sensitivity of that network segment – Guest WiFi, PCI. (RFC4864)
- Implement monitoring for each segment – alerting based on average inbound/outbound.
- First Hop Security – RA Guard (RFC6105 + RFC7113), DHCPv6 Guard/Shield (RFC7610).

Network Based Traps – Watchtower:

- Leaving the first and last 10% of your allocation empty reduces reconnaissance by simple probers.
- Go further with this, if you know part of your network is purposefully empty. You can build filters based off any activity in those areas – Observe then pull up the drawbridge.

Endpoints

Addressing Strategy Where Possible - /64 IPv6 subnet per endpoint and Temporary/Privacy Addresses.

Defence in Depth – EDR and IDS/IPS, make sure these properly support IPv6 including different address types (GUA, ULA, Link-Local) and lifetimes.

Built in Local Firewalls – Often either disabled or enabled with default configurations. Configure these to the use cases you expect for those endpoints. Especially important if using static addresses with easy to remember strategies.

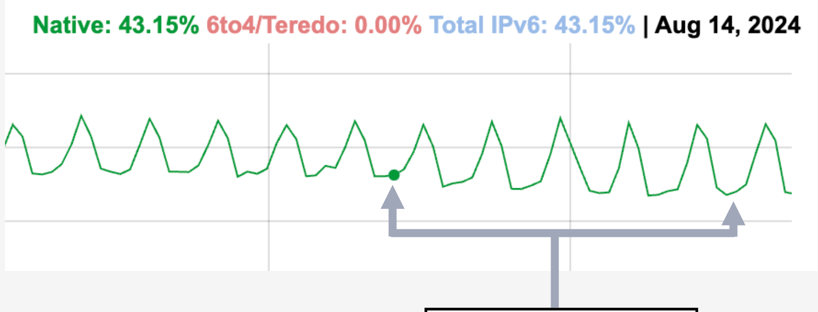
Summary

Spend time planning your IPv6 network. Embed security from the start.

- Ability to perform reconnaissance directly related to your addressing strategy
- We still need to push Cloud providers to offer feature parity with on-prem solutions.
- Check first what security solutions are available in Cloud - or are those features on the roadmap!

Change the narrative that IPv6 is a security burden to a security opportunity!

- Narrative impacts deployment of IPv6 as we saw in August.



1.5% decrease in 1 month.

Thank You.

Any questions?

Follow our LinkedIn page for regular updates about IPv6

in linkedin.com/company/arkenox

🌐 www.arkenox.com

Arkenox®

IPv6 Security Solutions