Connected Site-Local

Considered Harmful

Rob Austein <sra@hactrn.net>
55th IETF, Atlanta

Scopes And Borders

Scopes (which imply borders)

- node
- link
- site
- global

Things that change at borders

- routing
- security
- naming
- addressing

Is single "site" border a good place to put a border for all of these things?

Applications and Scope

Some applications are intrinsicly scoped (eg: RA, ND)

Most applications have no concept of scope

- Globally scoped by design

Most applications have no way of expressing scope

- Scope constrained by mechanisms external to the protocol

=> Stuff leaks across the borders

- Names leak (mail, web, files)
- Addresses leak (early name->address binding)

One Size Does Not Fit All

Site border sounds at first like a nice simple approach

...But it’s wrong

Are these the same border?

- Autonomous system
- Address realm
- Two-faced DNS border
- Firewall
- Demarcation point

Private addresses do not enhance security

Attacks via a border machine

Attacks via leakage

Weakened node security due to false sense of security

Firewalls have to filter bad global stuff anyway

- Private addresses are just one more thing to filter
- Private addresses do not make filtering easier

Reachability versus Ambiguity

Firewalls limit reachability

- But if you do get through, it’s not ambiguous

Private address realms also limit reachability

- But if you do get through, it is ambiguous

This is not an improvement

draft-ietf-dnsop-dontpublish-unreachable

Multiple sites

Devices that have to live in multiple sites are hard

- Multiple routing tables
- Mulitple naming realms
- Multiple (potentially colliding) addressing realms
- Complex forwarding and leakage rules

Recommendations

If we have to keep site-local at all, only use in disconnected case

Globally unique addresses would be better even in disconnected case