IPv6 Deployment to Government Networks - and - Trying to run IPv6-Only

Ron Broersma
Federal IPv6 Task Force
DREN Chief Engineer
SPAWAR Network Security Manager

“If you don’t support IPv6, and are not aggressively deploying IPv6 to your networks, then you are aiding terrorists, murderers, rapists, and other criminals.”

Measuring “feature parity”

- We want network products to support IPv6 just as well as they support IPv4 (called “feature parity”)
  - features and functionality
  - performance and security
  - manageability, configurability
- How do you measure feature parity in a product?
  - Test it in an IPv6-only environment and see what’s missing.

War Stories

- Bluecoat
- Fireeye (NX, PX, EX)
- Cisco Ironport
- Fidelis
- A10
- Gigamon
- Aruba Airwave

Lessons

- Vendors all claim that their products support IPv6
  - This means ABSOLUTELY NOTHING
  - Meaning of "supports IPv6":
    - customer: full feature parity, works on IPv6-only
    - provider: product won't crash if it sees an IPv6 packet
- Vendors are not testing their products in IPv6-only environments
- Vendors are not "eating their own dogfood"

Lessons

- When it is discovered that a feature lacks IPv6 support, what is the response?
  - customer: “it’s a bug that needs to be fixed immediately”.
  - provider: “we will submit a request for enhancement to add that feature to the product roadmap”. Translation: years.

DREN III contracting success (2012)

- In this contract for services, it was mandated that IPv6 had to work as well as IPv4, that IPv4 was considered a "legacy protocol", and that all network management had to operate over IPv6-only.
  - This took a single paragraph, not piles of paper listing every single requirement
  - Very successful at achieving goal
  - Some products had to be replaced due to lack of full IPv6 support

DREN strategy

- We want vendors to have a “corporate commitment to IPv6 support”
  - committed to fully supporting IPv6 in all products
- If a vendor’s company and product websites are not IPv6-enabled, then clearly they do not have a corporate commitment to IPv6.
- Result: Do not consider purchasing from vendors whose website is not IPv6-enabled

DREN Strategy

http://www.internetsociety.org/deploy360/blog/2014/09/us-dods-dren-will-only-buy-products-with-an-ipv6-website/

- If a vendor contacts us to market their products, and doesn't meet this requirement, we just respond with that link, and a link to their status at ip6.nl.
  - this is a great filter, and is very effective

Operating IPv6-only (removing IPv4)

- Since 2007 – trying to run SPAWAR management LAN as IPv6-only, to make sure all products could be managed strictly over IPv6.
  - isolated network, so a good place to try this
  - still not fully successful
  - non-compliant products are moved to a separate "Management-LAN-of-shame".

Operating IPv6-only (removing IPv4)

- In the production network, we want to start removing IPv4 from various segments of the network.
- Motivation
  - dual stack gets old after a while
  - dual stack adds complexity and is sometimes hard to keep all the security in sync
  - reduces the "attack surface"
  - IPv4 limits the full realization of IPv6 benefits
- Opportunity
  - NAT64/DNS64 (clients), or static NAT64 (data centers)

Operating IPv6-only (removing IPv4)

- Realization: Internet pioneers are ready to start removing IPv4 now, even if the rest of the world is not there yet
- Prediction: after you run dual stack for a while, you will look for ways to disable IPv4 in parts of your network
  - probably within the lifetime of products you are buying today

Why the lack of IPv6 in some government networks?

- Excuses:
  - "We have enough IP addresses"
  - "It has not been identified as a requirement"
  - "We have higher priorities (CyberSecurity)"
  - "IPv6 is not secure"
- But I say...
  - Lack of IPv6 is a security problem...

Lack of IPv6 is a security problem

- If both endpoints of any IP connection are not IPv6-enabled, then traffic must still go via IPv4
- IPv4 address space exhaustion forces reuse of IPv4 addresses through multiple layers of address translation (NAT, CGN)
- Translation adds complexity, and reduces performance/ reliability/scalability
  - added complexity brings added risk
- Translation impedes behavioral based security protections
- Translation impedes law enforcement from tracking criminals.
  - if you don't support IPv6, then all of your Internet traffic is forced over IPv4 paths and possibly through CGNs which obscures the true IP addresses and can't be easily traced.

IPv6 offers improved security because of vast address space

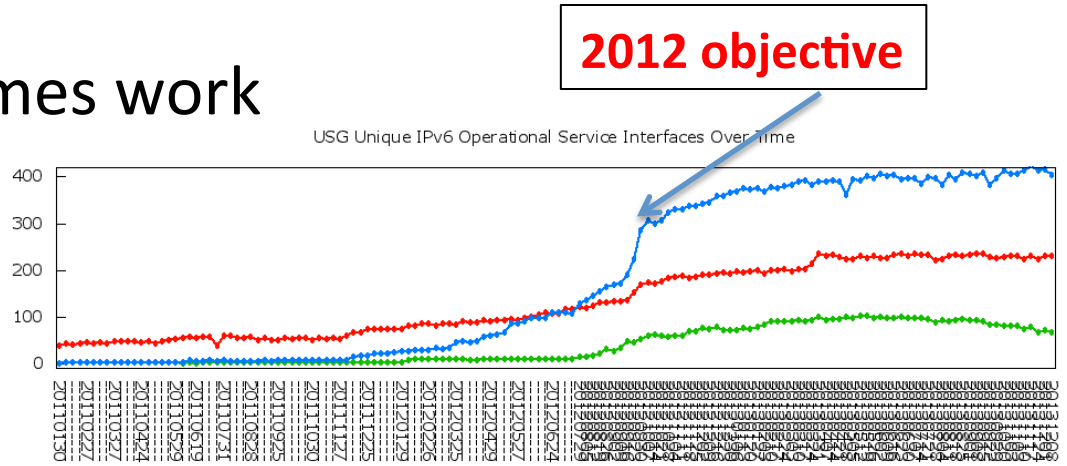
- Adversaries cannot map networks as easily
  - not possible to scan an entire subnet of addresses.
- Privacy addresses make it harder to track devices from day to day.
- Offers ability to encode security domains for simplification of ACLs and security policies.
- Offers true end-to-end security without translators or tunneling.
- Can dedicate IP addresses to services and applications, for finer grained separation.
- Doesn't break DNSSEC for those needing to do NAT64/ DNS64 to reach you.

Impediments to removing IPv4

- If others can't remove IPv4 due to your lack of IPv6 support, then security benefits are not realized
  - if you aren't part of the solution, then you are part of the problem.
- If products from industry cannot operate IPv6-only, then IPv4 can't be removed where those products are used, and security benefits are not realized

Thinking about Government Policy

- Mandates sometimes work



- Acquisition regulations, USGv6 profile and testing, RIPE-554, and IPv6-ready logo are necessary but not sufficient to achieve what we need today
  - only refer to standards based features, not the "secret sauce" of the product
- How do we "raise the bar"?

Raising the bar (a proposal)

- Accelerate IPv6 deployment in government networks:
  - All new Government initiatives MUST support IPv6
    - too hard to bolt it on later, so do it right from the beginning
  - Avoid companies that do not have a "corporate commitment to IPv6"
    - "Lack of IPv6 is a bug, not just a missing feature"
    - The commitment approach is better than a massive paperwork drill to document every single requirement and product feature
  - All products MUST fully function with IPv6-only
    - you will need this during the lifetime of any new products you purchase
  - Measure and report organizational progress
    - wall of shame can offer incentives

Setting Government Policy is hard

- You can't just require "feature parity" in all products that are purchased
  - no easy way to measure it
  - no current definition stands up to legal challenge
  - some things are just different between IPv4 and IPv6 (e.g. arp vs. neighbor discovery)
- It is hard to require vendors to put their IPv6 corporate commitment in writing
  - viewed as an open-ended future commitment
  - where is the repository for this information?
- Changing the acquisition regulations takes 2 years
  - still easy to overlook, ignore, or waive the requirement
- Grass roots efforts may work just as well, or better

Current USG discussions

- Update the USGv6 “supplier’s declaration of conformity (SDOC)” to include additional questions to document support for operating with full functionality in an IPv6-only situation.
- Use IPv6-only language instead of dual-stack
  - dual stack dilutes the issue
  - it achieves the same thing as stating dual-stack
  - the end goal is IPv6-only anyway
  - helps focus the “feature parity” requirement
- Work with Industry to get stronger commitments
  - corporate commitment, in writing
  - support for IPv6-only
  - “it’s a bug, not just a missing feature”
- Establish “IPv6 Everywhere” mandate (2020?)

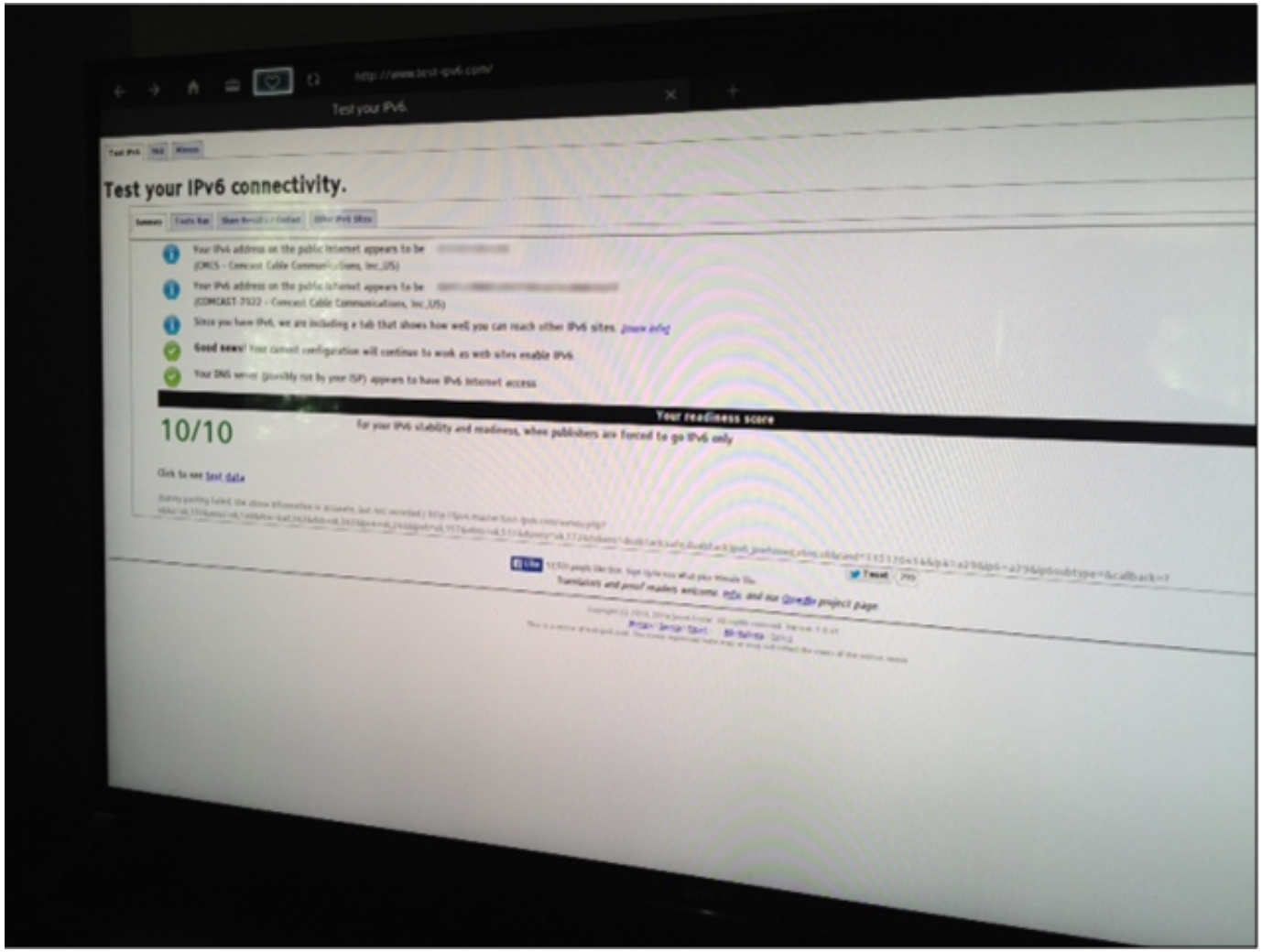
Corporate Commitment to IPv6: What would it look like?

- Vendor agrees, in writing, to the following:
  - their public facing services will be IPv6-enabled (web, mail, dns), for their corporate website and for each product/support site
  - they "eat their own dogfood”
  - they will stipulate that their products operate with full functionality in an IPv6-only environment
  - part of their quality assurance testing for a product will be to test it in an IPv6-only environment.
  - any lack of support for IPv6 will be treated as a "bug", and not as just some missing "feature".

Summary

- There are security benefits that can be realized with IPv6
- Until we can remove IPv4 baggage from segments of our network, we will not realize the full benefits of IPv6
- Progress is impeded by the remaining IPv4-only world, and by vendor products that can't operate IPv6-only
- Government mandates help but have limitations, yet we need to be more aggressive and "raise the bar"

Even my TV does IPv6



END

ron@dren.hpc.mil