Advanced IPv6 Residential Security
draft-vyncke-advanced-ipv6-security-00.txt

Mark Townsley townsley@cisco.com

Eric Vyncke evyncke@cisco.com

November 2009

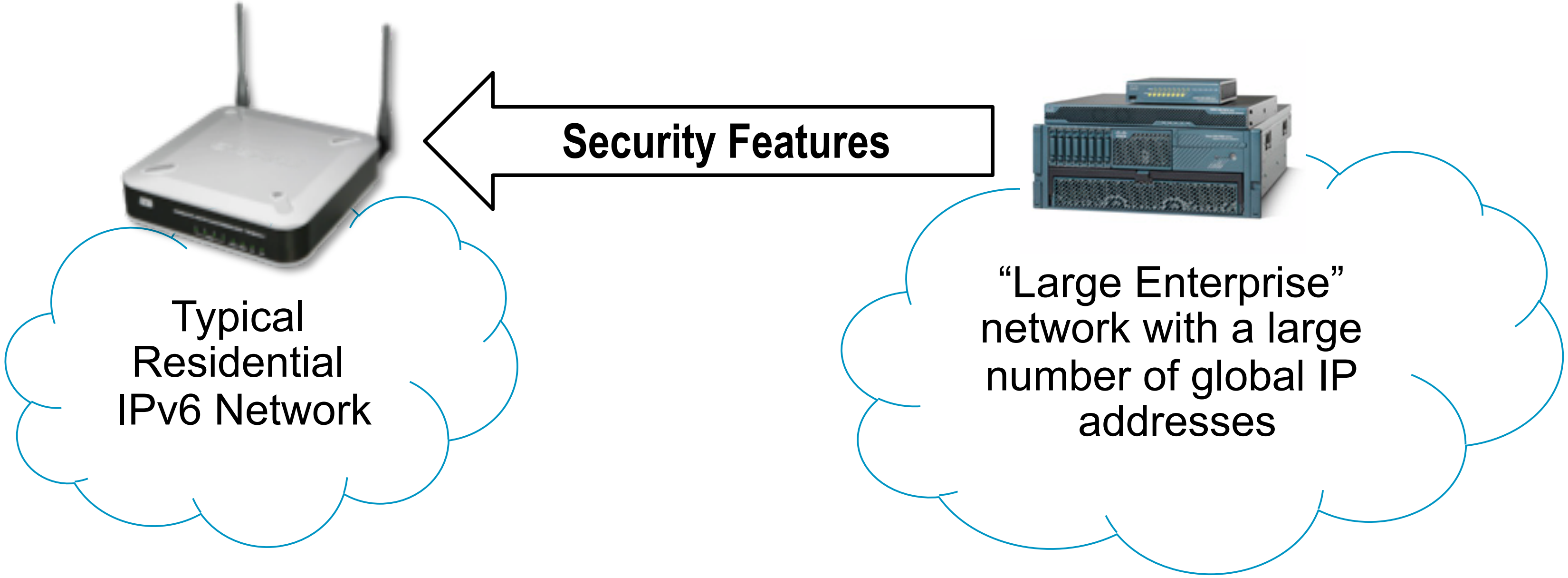
Basic Idea

Typical Residential IPv6 Network

“Large Enterprise” network with a large number of global IP addresses

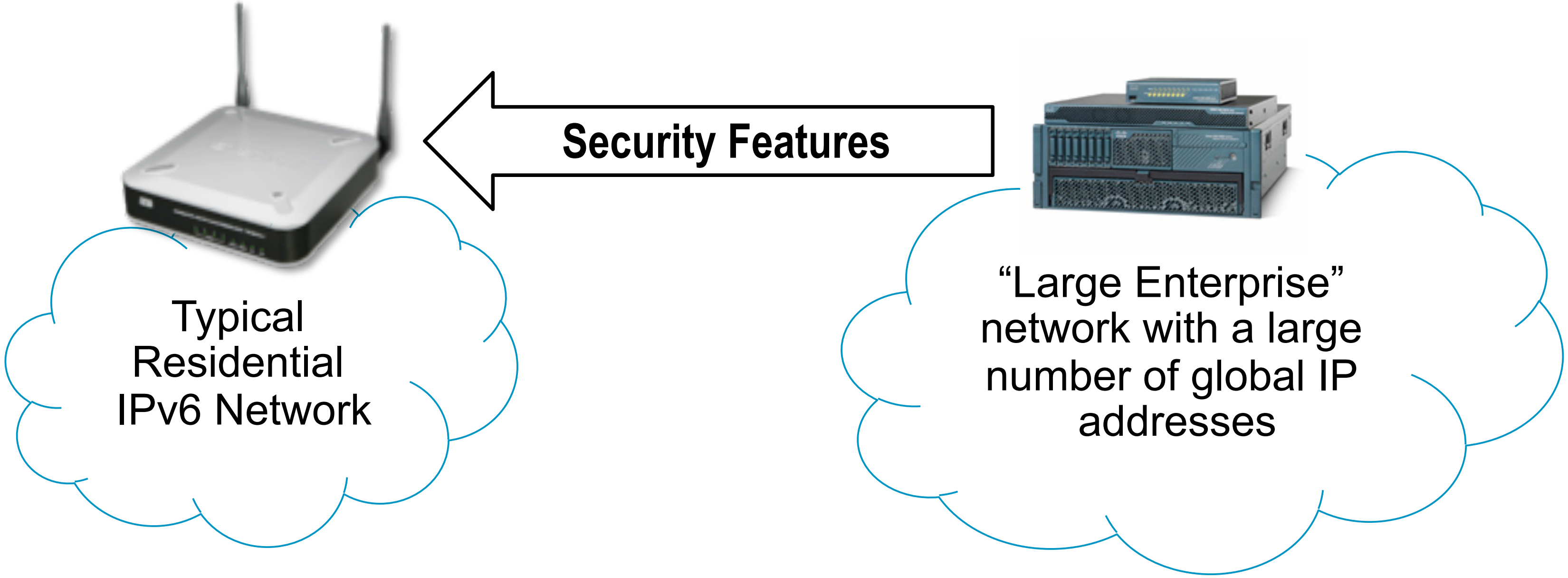
- Observation: Expansive addressing in IPv6 allows any residential network to resemble an enterprise network with a large IPv4 global address block

Basic Idea


Security Features
Typical Residential IPv6 Network
"Large Enterprise" network with a large number of global IP addresses

- V6ops is in the process of defining what residential IPv6 security should look like, so perhaps we should examine security features that are used in enterprise networks today and see how they might apply in a residential security setting

Basic Idea

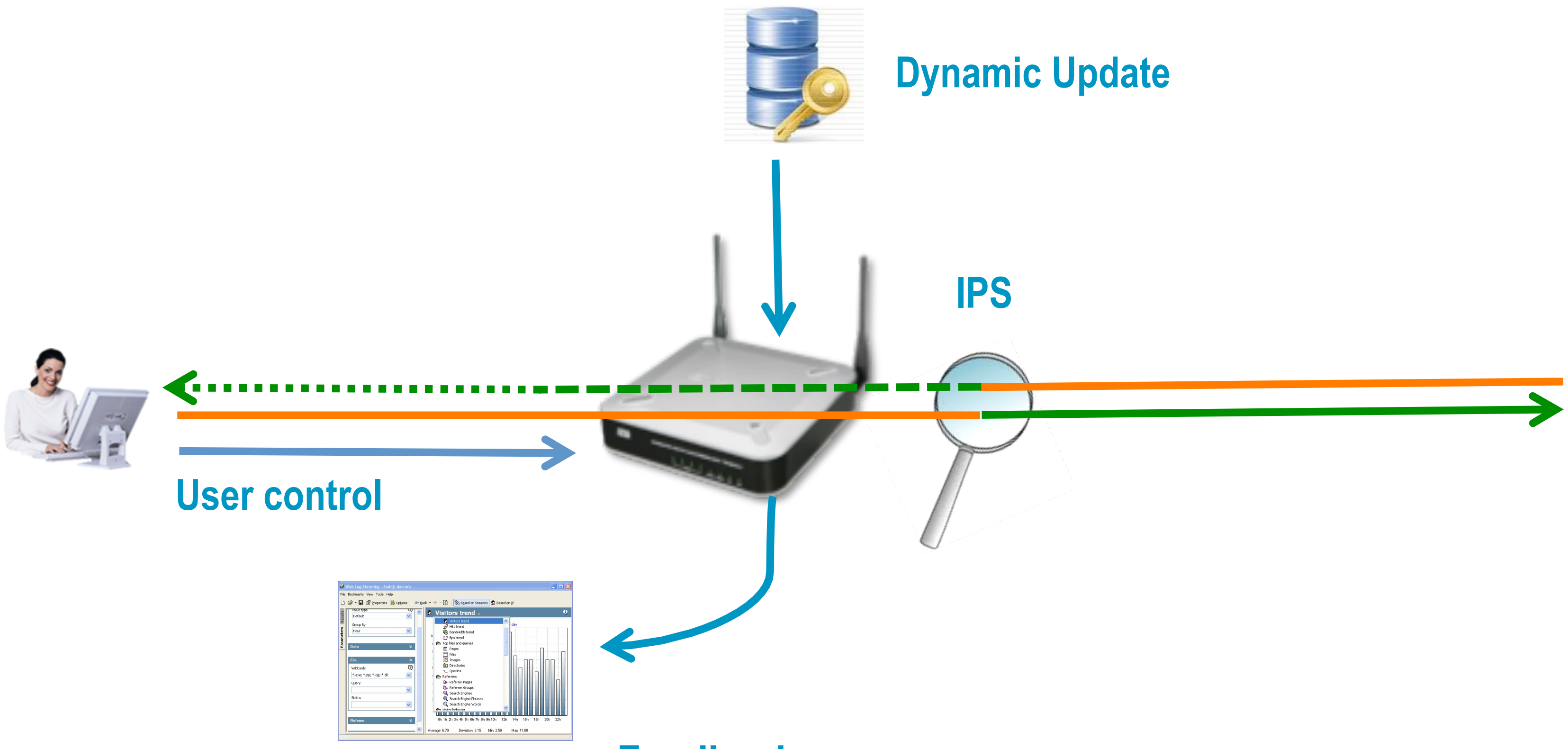

Security Features
Typical Residential IPv6 Network
"Large Enterprise" network with a large number of global IP addresses

- These techniques are not IPv6-specific per se, but we are discussing them within the context of IPv6 here in v6ops.

Overview

- 7 security policies are identified in the -00. These are largely based on features which are commonly available in security gear for enterprises today
- Home edge router is actively updated like many other consumer devices are today (PCs, iPods, etc.)
- Business model may include a paid subscription service from the manufacturer, a participating service or content provider, consortium, etc.

Advanced Security



Dynamic Update

IPS

User control

Feedback

Why is this important to IPv6?

- Security policy can be adjusted to match the threat as IPv6 attacks arrive
- We don't break end-to-end IPv6, unless we absolutely have to
- While providing arguably better security, troubleshooting, etc. than we would otherwise

Security Policies

1. RejectBogon:
   - including uRPF checks
2. BlockBadReputation:
   - inbound and **outbound*** traffic
3. AllowReturn:
   - Applying IPS on in/ outbound traffic
4. AllowToPublicDnsHost
   - Allow inbound traffic to inside host with a AAAA & reverse-DNS
5. ProtectLocalOnly:
   - Block all inbound traffic to inside which never transmitted to the outside (à la full-cone)
6. CrypoIntercept:
   - Intercept all inbound SSL/TLS connection, present self-signed cert, decrypt and re-encrypt (in order to apply IPS)
7. ParanoidOpeness:
   - Rate-limit remaining incoming connections

Conclusion

- “simple-security” as is being defined now, is not the only possible residential gateway security model
- “Advanced” security methods can provide adaptable and robust security that can better track threats as attacks appear on IPv6…

  ….giving us the chance for more open policies with respect to end-to-end connectivity

Possible Next Steps…

- Nothing, continue with simple-security as is
- See what modern security methods we might be able to bring into simple-security, while keeping the “static” mode of operation it assumes now
- Define an “advanced security” mode that includes dynamic tracking of threats as attacks arrive, and adjusts policies accordingly