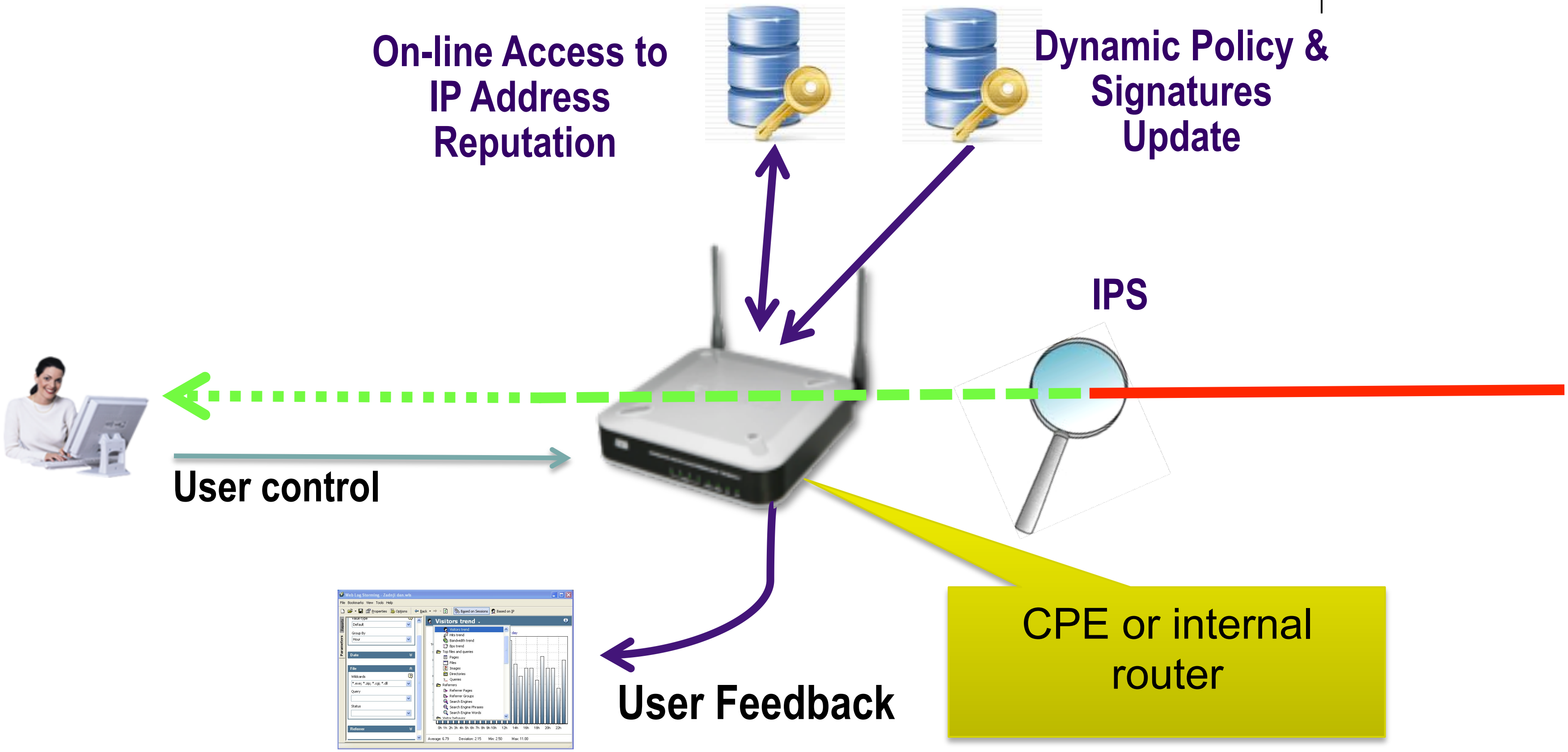
Advanced IPv6 Residential Security draft-vyncke-advanced-ipv6-security-03

Eric Vyncke ev@cisco.com
Mark Townsley townsley@cisco.com
Andrew Yourtchenko ay@cisco.com

November 2011

Advanced Security



On-line Access to IP Address Reputation

Dynamic Policy & Signatures Update

IPS

User control

User Feedback

CPE or internal router

In short: traffic is allowed until proven guilty

Overview

- 7 policies are identified in the -03. These are largely based on features which are commonly available in "advanced" security gears (UTM) for enterprises for several years
- Home edge/internal router is not something that is purchased and thrown away when obsolete. Instead, it is actively updated like many other consumer devices are today (PCs, iPods and iPhones, etc.)
- Business model may include a paid subscription service from the manufacturer, a participating service or content provider, consortium, etc.

Why is this important to IPv6 & HOMENET?

- RFC 6092 defaults to inbound-disallowed (transparent mode is an option) and will break end-to-end in HOMENET configurations
- ‘intra-home’ router does not always have *trusted* vs. *untrusted* sides
- Security policy can be adjusted to match the threat as attacks arrive
- **We don’t break end-to-end IPv6, unless we absolutely have to**

Opening THE Can of Worms NAT is Useless for Security

- Most botnet members are behind a NAT
  - Malware are downloaded nowadays…
- Allowing PCP or UPnP to open NAT pin-holes puts a huge trust in the host integrity
- There is a need to apply security between *guest* and *home* security domains

Default Security Policy

1. RejectBogon:
   - including uRPF checks
2. BlockBadReputation:
   - for in/**outbound** traffic
3. AllowReturn:
   - and apply 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
   - Goal is to apply IPS
7. ParanoidOpeness:
   - **Allow ALL inbound traffic by default**
   - See more next slide

More on Paranoid Openness

- Rate limit (SYN & plain data)
  - To protect low-bandwidth residential links
  - Basic protection against host scan
- If authenticated flow (e.g. HTTP)
  - Perform dictionary attack on credential and reject too obvious ones (or default ones)
  - Goal is to force user to select good credentials
- IPS must be applied
  - If protocol unknown, then flow MAY be permitted
  - If attack is detected, then flow MUST be denied

-00 at IETF 76

- -00 presented at V6OPS & SAAG
- Globally positive reaction
  - The crypto part could be improved/better presented
  - Paranoid Openness is very much needed for IPv6
  - Already known as Universal Threat Mitigation for large enterprises
  - Could/should cross pollination with simple-security ID

Between IETF76 & 82

- But, little progress done (Eric’s & Mark’s fault)
- -03 delta
  - Some cosmetics
  - More reference to UTM
  - Reference to previous I-D & RFC 6092
  - More consistent with HOMENET