IPv6 Distributed Security problem statement <draft-vives-v6ops-ipv6-security-ps-03.txt>

Jordi Palet (jordi.palet@consulintel.es)
Alvaro Vives (alvaro.vives@consulintel.es)
Pekka Savola (psavola@funet.fi)

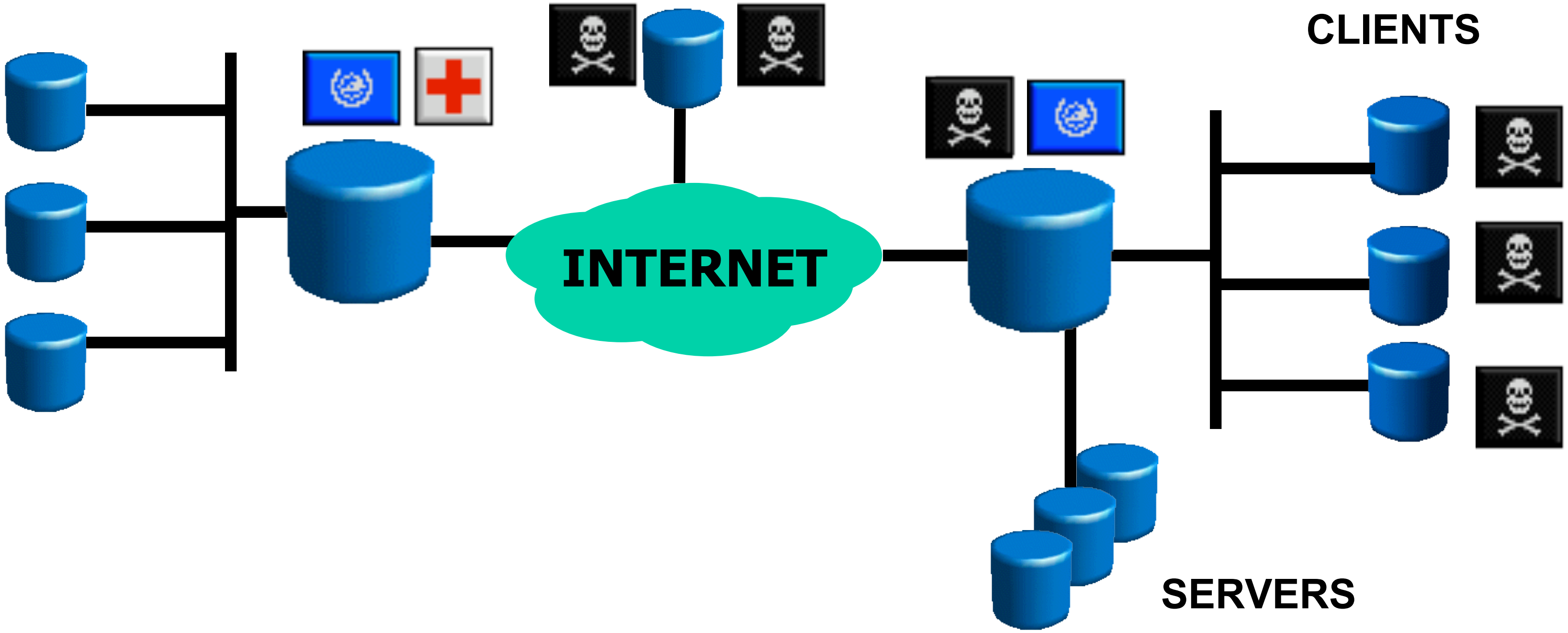
Motivation

- How would the **deployment of IPv6** affect the **security** of a network?
- IPv6 enabled devices and networks bring some issues to be taken into account by security administrators:
  - End-2-end communications
  - IPsec in all IPv6 stacks
  - Increase in the number and type of IP devices
  - Increased number of “nomadic” devices
- Identify IPv6 Issues that may justify the need of a new security model

Concepts

- **Attack/Threat:** Either passive or active
- **Security** (S): Protection against attacks+IPsec
- **Policy Management Tool** (PMT): Used by the network administrator to edit the policies
- **Policy Decision Points** (PDP): Entity which distribute S policies
- **Security Policy** (SP): Information used by PDP to provide S
- **Policy Enforcement Points** (PEP): Apply SP (Clients)

Network-based Security Scheme (I)



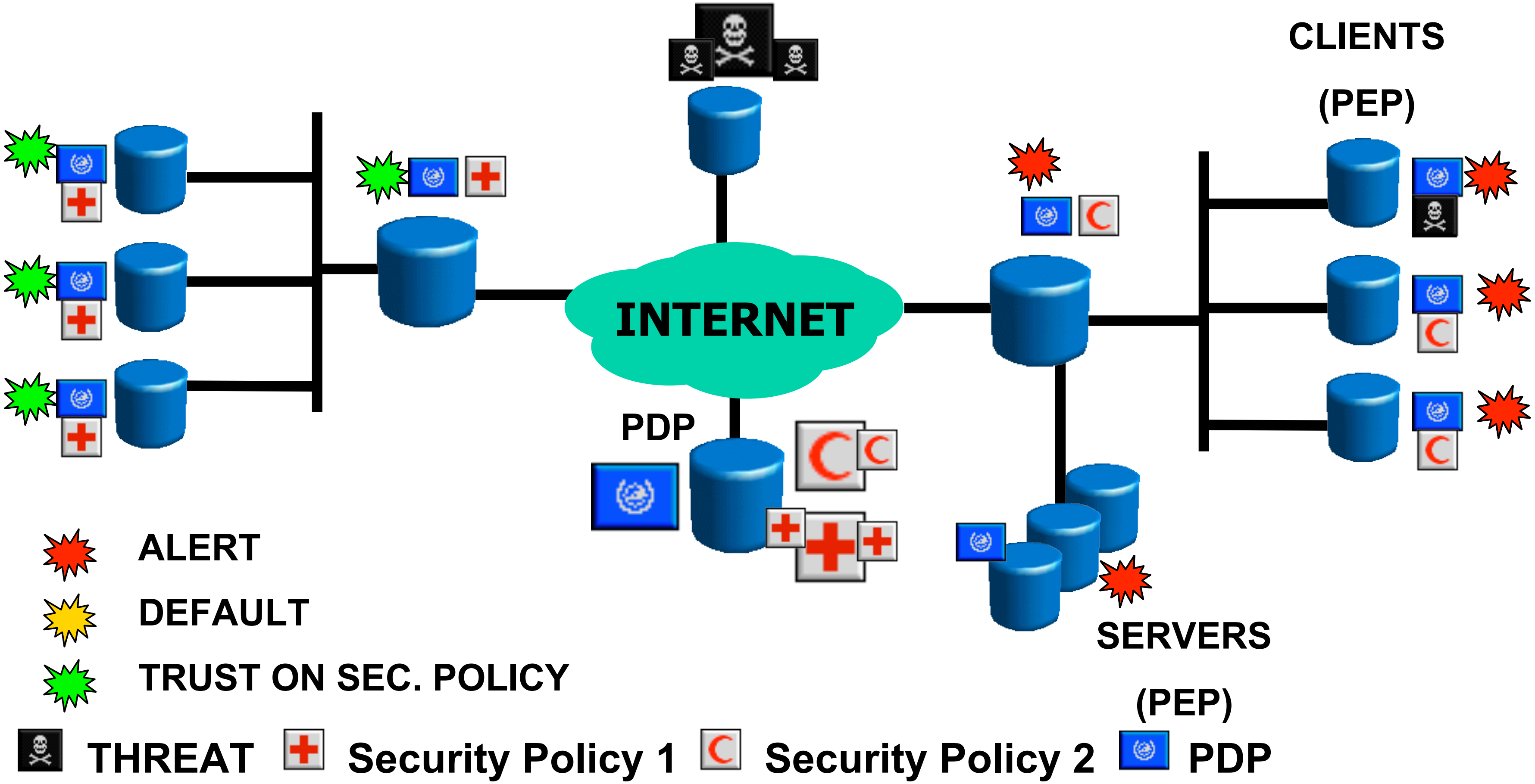
☠ THREAT ✚ Security Policy 1 ☾ Security Policy 2 ◙ PDP

Network-based Security Scheme (II)

- **Main Assumptions:**
  - Threats come form “outside”
  - Protected nodes won’t go “outside”
  - No backdoors (ADSL, WLAN, etc.)

- **Main Drawbacks:**
  - Centralized model
  - Do not address threats coming from inside
  - FW usually acts as NAT/Proxy
  - Special solutions are needed for Transport Mode Secured Communications

Host-based Security Scheme



CLIENTS

(PEP)

INTERNET

PDP

SERVERS

(PEP)

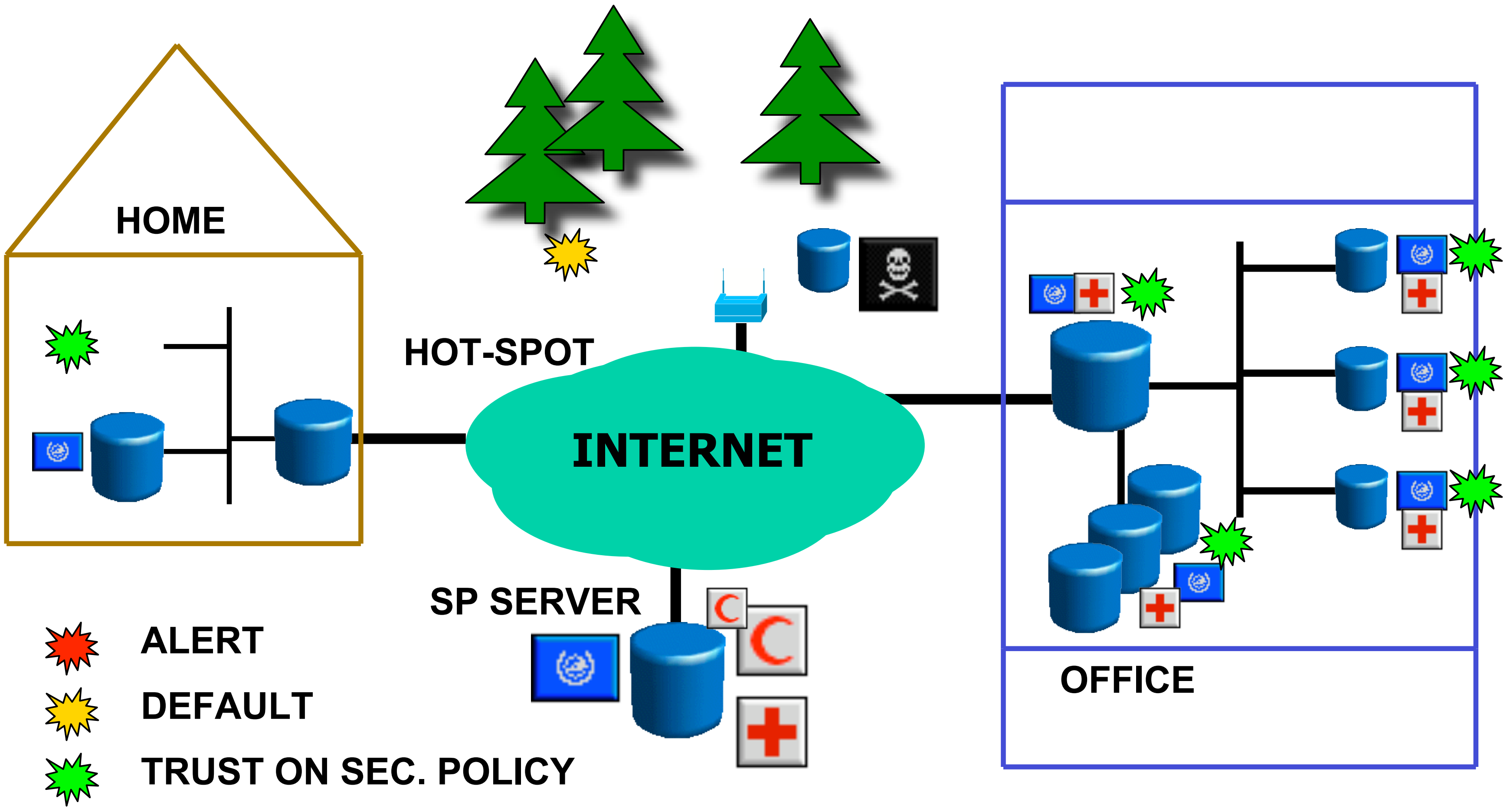
🟥 ALERT

🟨 DEFAULT

🟩 TRUST ON SEC. POLICY

☠ THREAT ✚ Security Policy 1 C Security Policy 2 ◙ PDP

Host-based Security Example



HOME

HOT-SPOT

INTERNET

SP SERVER

OFFICE

ALERT

DEFAULT

TRUST ON SEC. POLICY

THREAT Security Policy 1 Security Policy 2 PDP

Host-based Security Model (I)

- **BASIC IDEA**: Security Policy centrally defined and distributed to PEPs. The network entities will authenticate themselves in order to be trusted.

- **THREE elements:**
  - **Policy Specification Language**
  - **Policy Exchange Protocol**
  - **Authentication of Entities**

Host-based Security Model (IV)

- **Main Assumptions**:
  - Threats come from anywhere in the network
  - Each host can be uniquely and securely identified
  - Security could be applied in one or more of the following layers: network, transport and application
- **Main Drawbacks**:
  - Complexity
  - Uniqueness and secured identification of hosts is not trivial
  - Policy updates have to be accomplished in an efficient manner
  - A compromised host still is a problem
  - Is PDP dependant: more complexity to address this

Host-based Security Model (V)

- **Main Advantages:**
  - Protects against internal attacks
  - Don’t depend on where the host is connected
  - Still maintain the centralized control
  - Enables the end-2-end communication model, both secured or not
  - Better decision could be taken based on host-specific info.
  - Enables a better collection of audit info

IPv6 Issues (I)

1. **end-2-end**
   - Any host must be reachable from anywhere. NAT/Proxy is not desired.
2. **Encrypted Traffic**
   - For example IPsec ESP Transport Mode Traffic
3. **Mobility**
   - Both Mobile IP and the increase of “portable” IP devices will mean they will be in “out-of-control” networks
4. **Neighbor Discovery**
   - RA, RS, NA, NS and Redirect Messages could be used in a malicious way -> SEND

IPv6 Issues (II)

5. **Addresses**
   - Much more addresses -> hosts with more than one, difficult brute force scans
   - More human error prone
   - Randomly generated addresses
   - Link-local and Multicast Addresses
   - Multihoming
6. **Embedded Devices**
   - Big amount of devices with almost no resources to perform security tasks -> should be taken into account in a possible solution
7. **Routing Header**
8. **Home Address Option**

Open Issues

- **Need Feedback on:**
  - Should transition mechanisms be addressed? (already done in Pekka Savola’s draft)
  - The distributed Security (DS) model is the best to address the future needs?
  - Could IPv6 and DS be separated?
- **Current Discussion about:**
  - Good to go for an IPv6 issues checklist document for the security people?
  - Go for a deeper DS analysis

Thanks !

- Questions ?