IPv6 distributed security requirements
<draft-palet-v6ops-ipv6security-00.txt>

Jordi Palet (jordi.palet@consulintel.es)

Alvaro Vives (alvaro.vives@consulintel.es)

Gregorio Martinez (gregorio@dif.um.es)

Antonio Skarmeta (skarmeta@dif.um.es)

Motivation

- Current security policies doesn’t longer apply for end-to-end security with IPv6
  - Border firewall = bottleneck
- Users and devices start to be “nomadic”
  - “Static” security setup-ups are a wrong approach
- Different visited networks have different security requirements
  - Manual changes are dangerous
  - Will not be acceptable for the network manager
- Increase in security means increase in processing power
  - Distribution of security “overhead” could be a solution

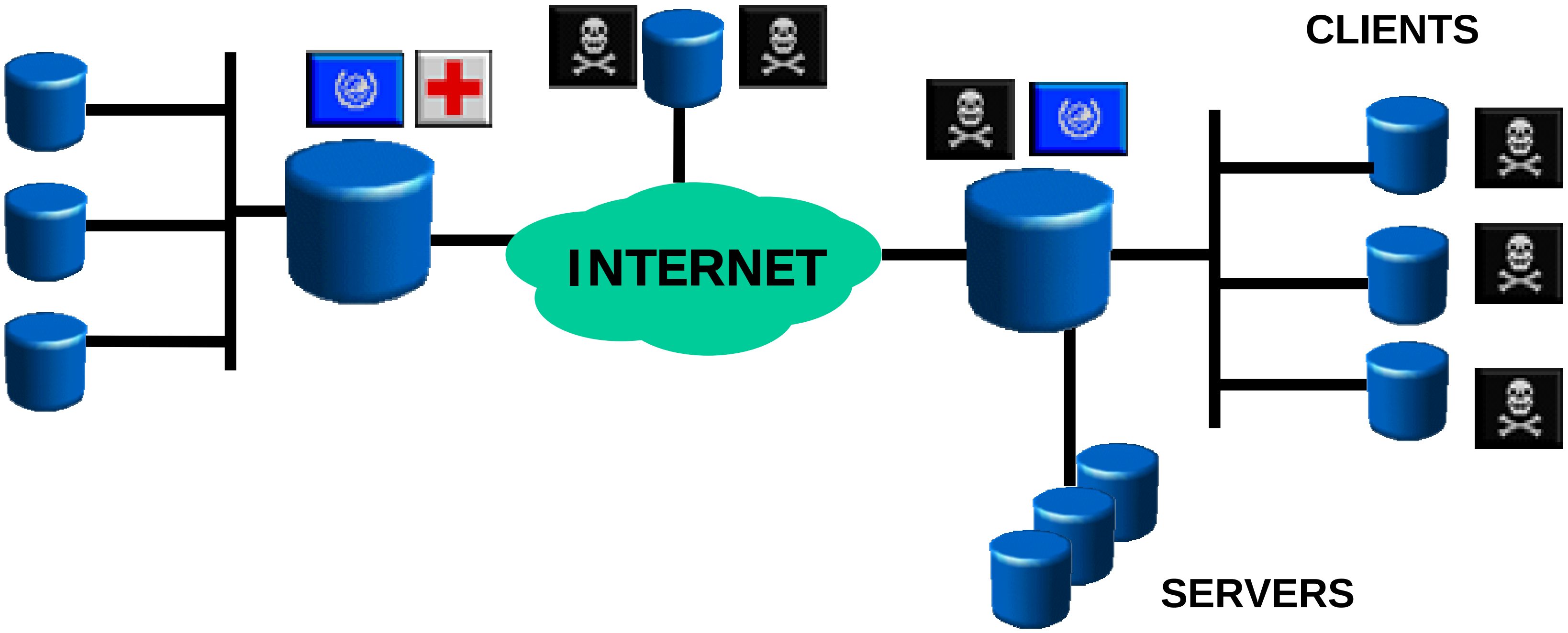
Approach for Solution

- Extensive use of “personal firewalls”
  - Can cope with “interior” security
- Personal firewalls should be enabled by default
- They should look for a security policy manager in the visited network
  - Acquire and implement the required local policy
  - If their processing capabilities are exceeded, then rely on a distributed firewall approach
- If IDS are present, the “local” security policy manager can get feedback from it, and suggest security changes to the complete network
- Can we cope with virus and spam ?

Concepts

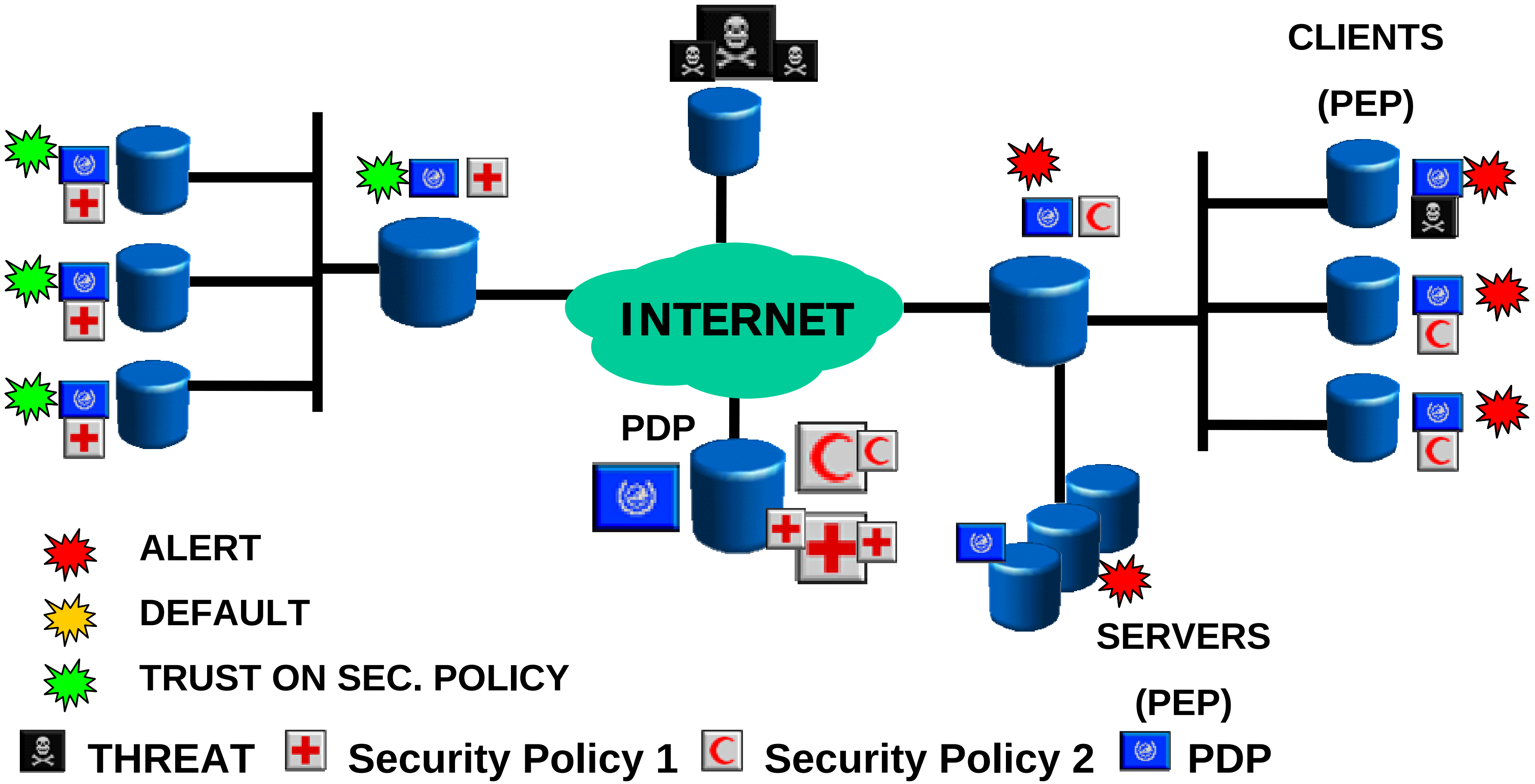
- **Attack/Threat:** Either passive or active
- **Security** (S): Protection against attacks+IPsec
- **Policy Management Tool** (PMT): Used by the network administrator to edit the policies
- **Policy Decision Points** (PDP): Entity which distribute S policies
- **Security Policy** (SP): Information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

Actual Security Scheme



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

Distributed Security Scheme



CLIENTS

(PEP)

INTERNET

PDP

SERVERS

(PEP)

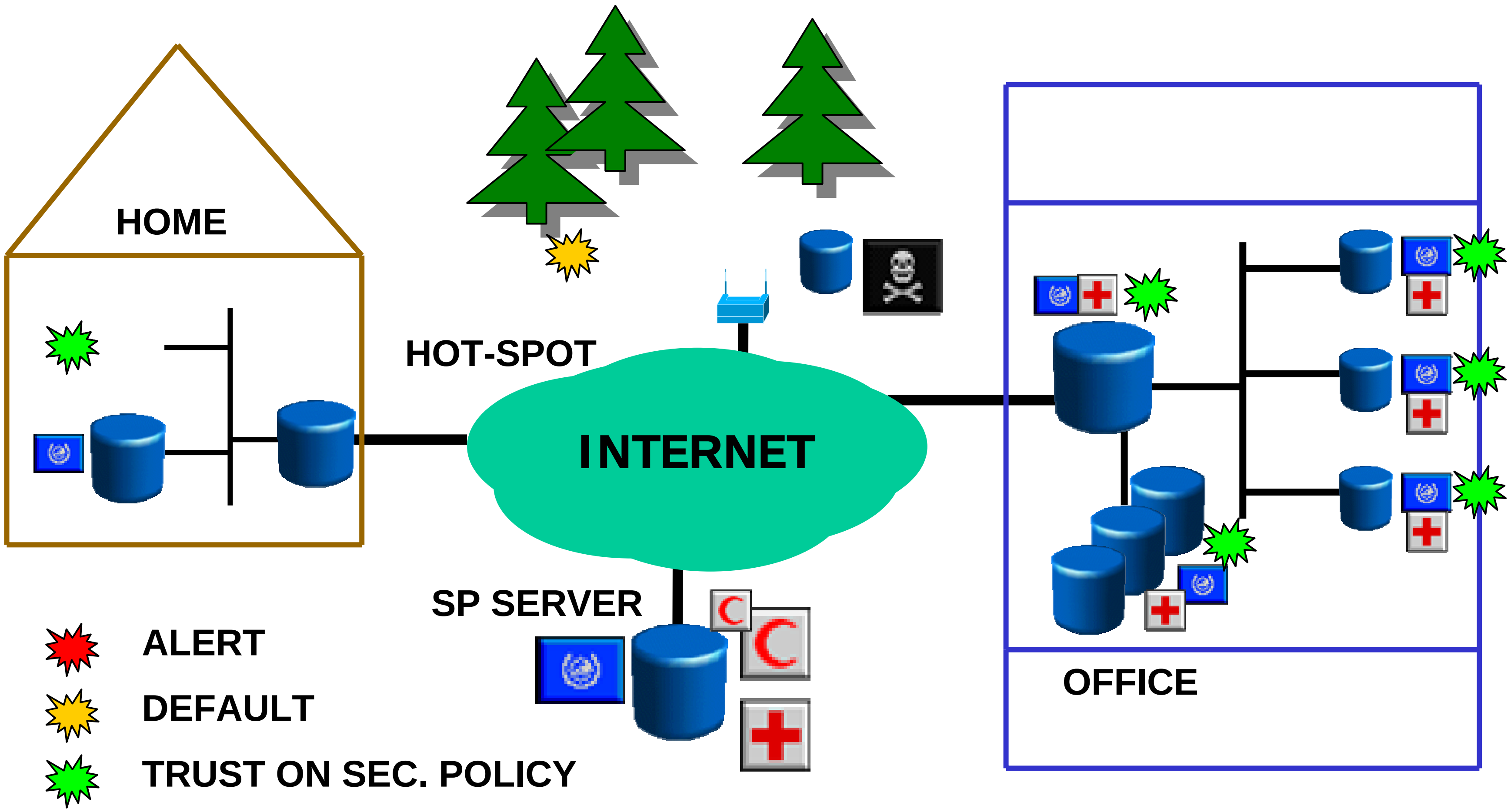
ALERT

DEFAULT

TRUST ON SEC. POLICY

THREAT Security Policy 1 Security Policy 2 PDP

Distributed Security Example



HOME

HOT-SPOT

INTERNET

SP SERVER

OFFICE

ALERT

DEFAULT

TRUST ON SEC. POLICY

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