

IPv6 Distributed Security

Alvaro Vives (alvaro.vives@consulintel.es)

Jordi Palet (jordi.palet@consulintel.es)

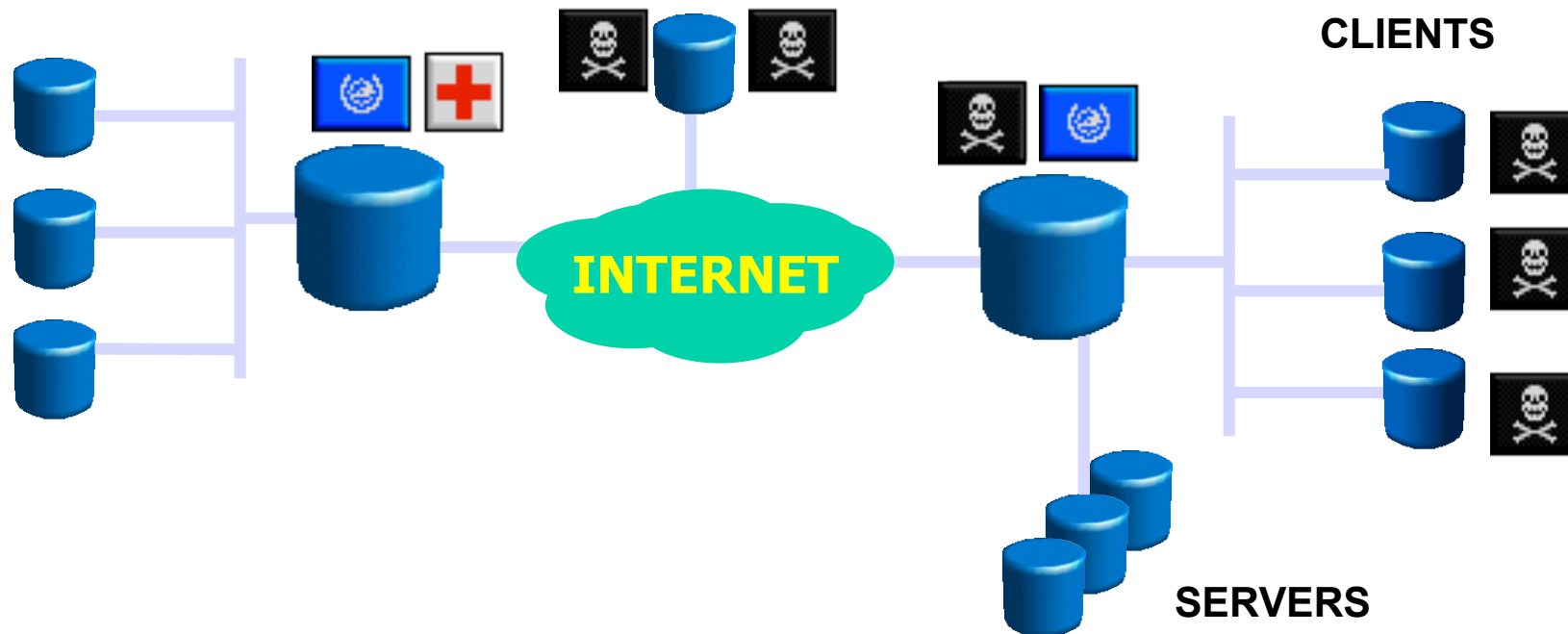
Motivation

- 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
 - Increased number of IP devices
 - Increased number of “nomadic” devices
- Identify IPv6 Issues that justify the need of a new security model

What is Security ?

- Security in the "big scope" of the word, trying to include as much as possible
- A host, a network or some information, will be secure when no attacks could succeed against them
- A success will mean compromise of availability, integrity, confidentiality or authenticity
- The realistic objective is to be as much secure as possible in a precise moment

Network-based Security Model (I)



 THREAT  Sec. Policy 1  Sec. Policy 2  Policy Enforcement Point (PEP)

Network-based Security Model (II)

- **Main Assumptions:**
 - Threats come from “outside”
 - Everybody from the same LAN segment is trusted
 - Protected nodes won’t go “outside”
 - No backdoors (ADSL, WLAN, etc.)
 - The hosts will not need to be directly accessed from outside (at least not in a general manner)

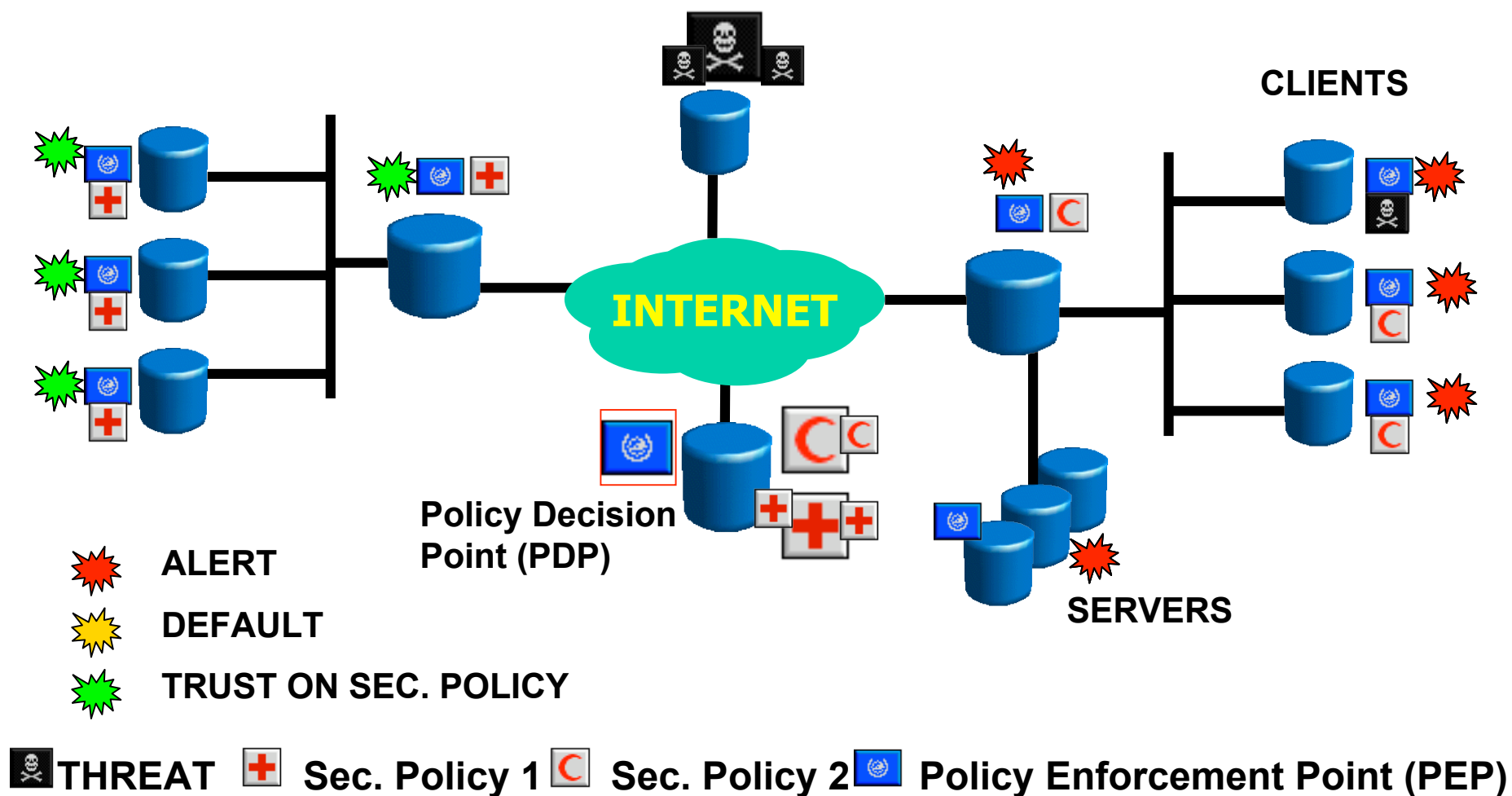
Network-based Security Model (III)

- **Advantages:**
 - Simplicity and easiness
 - Minimum points of configuration
 - Few/no protocols and mechanism to implement “security”

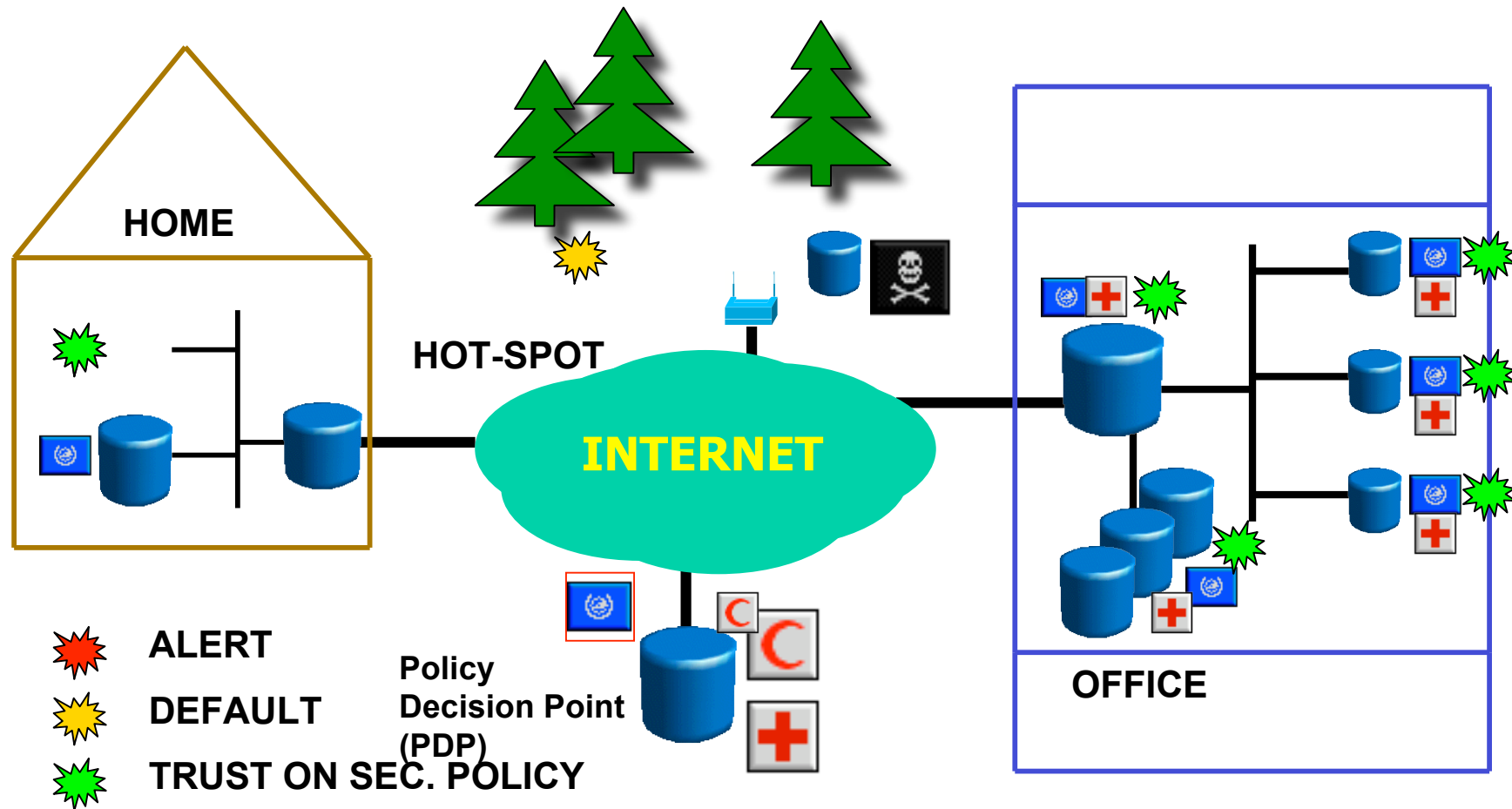
Network-based Security Model (IV)

- **Main Drawbacks:**
 - Centralized model: Single point of failure in terms of performance and availability
 - Do not address threats coming from inside (even if more dangerous)
 - FW usually acts as NAT/Proxy: No end-to-end
 - Special solutions are needed for Transport Mode Secured Communications
 - Virtual organizations (GRIDs) don't work
 - Lack of secure end-to-end prevents innovation

Host-based Security Model (I)



Host-based Security Model (II)



 **THREAT**
 **Sec. Policy 1**
 **Sec. Policy 2**
 **Policy Enforcement Point (PEP)**

Host-based Security Model (III)

- **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
 - But “isolating” it could be a solution

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. Addresses

- Much more addresses -> hosts with more than one
- Randomly generated addresses
- Link-local Addresses
- Multicast

IPv6 Issues (II)

5. Neighbor Discovery

- RA, RS, NA, NS and Redirect Messages could be used in a malicious way -> SEND

6. Routing Header

7. Home Address Option

8. Embedded Devices

- Number of devices with almost no resources to perform security tasks -> should be taken into account in a possible solution

IPv6 Distributed Security

- Interior Security
- The Visiting Node
- Default Security
- Security Policy Server and Protocol
- Single versus Multiple Points of Attack
- Non-security capable nodes and security workload distribution
- Location of the Security Policy Server
- Virus
- Spam

Requirements towards a Solution

- Dynamic security policy specification language, exchange protocol and server
- Authentication of entities
- Support of SEND protocol
- Support for unmanaged nodes/devices
- Control and node/network partition mechanism
 - Securization of the rest of the network in case of a threat, even if internal
- Alert/notification mechanism
 - Facilitate the inter-node and/or node-policy server communication
- Node or host firewall, with a secure “default configuration”, that can be updated by a trusted dynamic security policy server. Should also include functionalities such as:
 - Integral thread protection
 - Resolution and arbitration of conflicts between different security policies
 - Support for end-to-end application level security (i.e., Web Services security standards)
 - Intrusion detection
 - Collection of audit information
- Optionally it could also include:
 - Anti-virus
 - Anti-spam

Standardization Status

- Problem Statement:
 - draft-vives-v6ops-ipv6-security-ps-02
- Requirements:
 - draft-palet-v6ops-ipv6security-01

Next Steps

- Get inputs from the WG and security area
- Continue the work
 - Solutions
 - Implementation
 - Trial in real networks, not just labs

Thanks !

Questions ?