Policy Based Security Management for IPSec

Luis A. Sanchez
August 25, 1998
Outline

- Problems
- Requirements
- A Solution
- Next Step
Problems

- Need a common security policy specification language
- Need to specify enforcement points for each policy
- Discovery of security gateways
- Resolution of security requirements for inter-domain communication
- Consistency checking of local security policies
- Management of dynamic security associations
Requirements

- **Support for complex topologies**
  - multiple embedded tunnels

- **Support for legacy systems**
  - non IPSec compliant

- **Scalable and deployable incrementally**

- **Independence of protocol suite, KMP**

- **NAT Friendly**

- **Graceful failure**
A Solution

Security Policy Negotiation Protocol (SPP) Message Flow

Legend
SPP Messages
- REQ#: SPP-Request
- RPY#: SPP-Reply
- CMD#: SPP-Policy

Functions
- provides server and security services discovery
- domain based policy resolution
- enforcement point selection
- security association bundle management
Next Step

- Code Release: Pre-Alpha by End of Sept. 1998
- 2 Internet-Drafts underway:
  - Security Policy Specification Language
  - Security Policy System (policy exchange and resolution protocol)
- Request feedback from Community and vendors in general
- any questions:
  - lsanchez@bbn.com