Bay Networks

Where Information Flows.™

VPN and IPsec

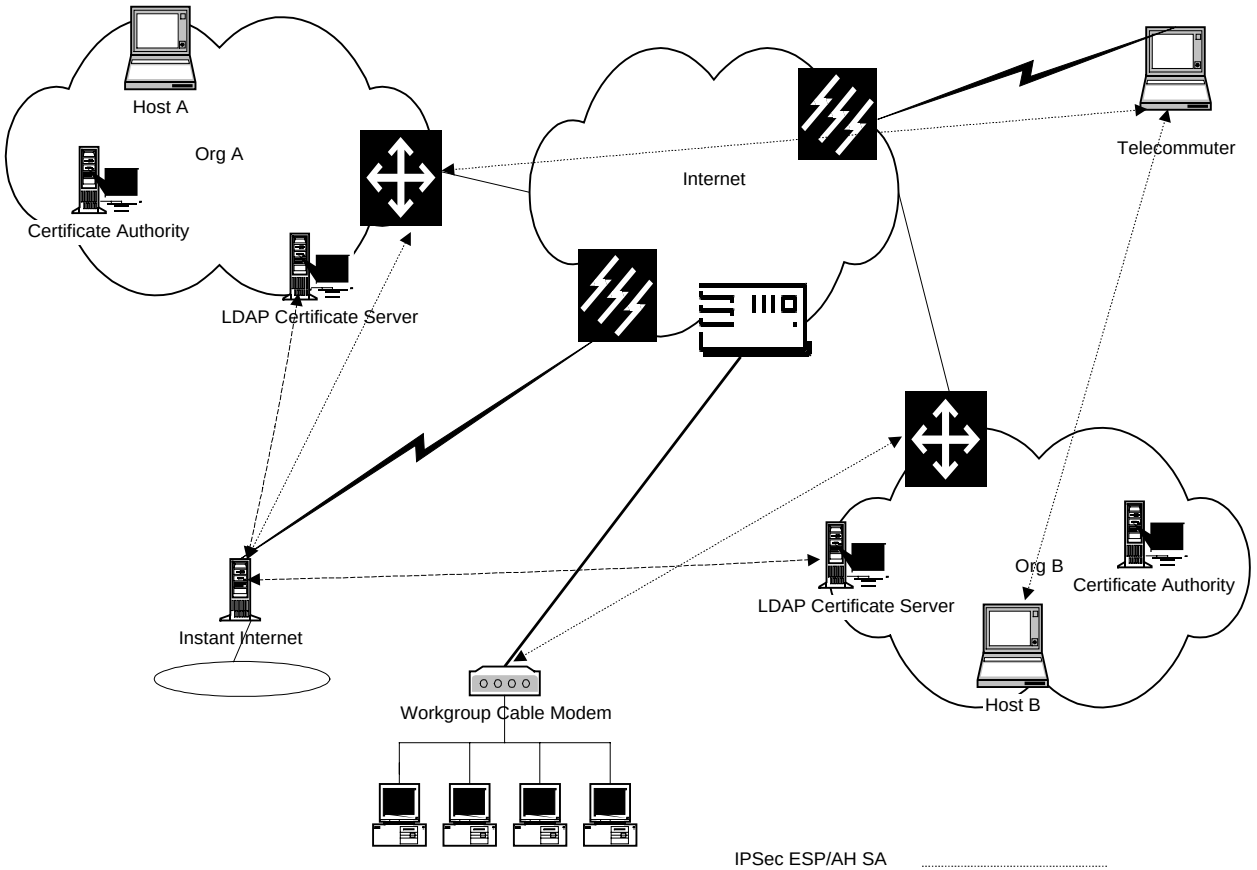
Naganand Doraswamy

Bay Architecture Lab

VPN's

- What is a VPN?
- Models of VPN
  - Dial VPN
  - Extended Intranets
  - Extranets

Example Network



Deployment Issues

- **Edge Capability**
  - — **Proxy**
  - — **Authorization**
  - — **Identity (Username or Machine)**
- **Multiple IPsec devices**
  - — **Chaining or Nesting**
  - — **Discovery**

Deployment Issues (Cont...)

- IPsec PKI Requirements
  - Certificate
    - IPsec requirements
    - DN names (IPv4, IPv6, FQDN)
    - Name Constraints
  - Directory Requirements
  - Management Issues
    - Enrollment
    - OCSP (On-line Certificate Status Protocols)

Deployment Issues (Cont...)

- **Policy**
  - **Central Vs. Distributed maintenance**
  - **Static Vs. Dynamic Discovery**
    - **Static**
      - Difficult to know before hand the network topology in the destination domain
      - Problem with multiple firewalls
      - Traffic either has to be chained or tunneled
    - **Dynamic**
      - A mechanism to dynamically determine IPsec network topology
      - DNS, TEP, or other protocols
      - Complicated cases of two routers at the boundary

IPsec Implications

- Filtering based on transport protocols field is not possible
  - — Web Caching
  - — Other mechanisms such as congestion looking at ports
- For existing firewalls to work, the encryption tunnel has to end at the firewall
- Speed
  - — Avoid encryption in the core and push it to edges

IPsec-ond

- Secure Multicast
- Dynamic Policy Discovery
- PKI related enhancements

Conclusions

- IPsec is fundamental in providing secure VPN services
- It is for real!
  - In working group last call
- Lot of implementations
  - Both host and router vendors