Son of IKE Requirements

Cheryl Madson

Cisco Systems

Outline

- Changes since –00 draft
- Scenarios
- General operational requirements
- Protocol requirements
- Policy requirements
- Security requirements

Changes since –00 draft

- A lot ;-)
- Draft –00 covered only protocol issues
  - Simplicity shouldn’t be the only goal; designing a well-behaved protocol that meets the core scenarios while having sufficient (but not infinite) flexibility is important
- Current draft adds scenarios, and security, operational and policy requirements; original protocol discussion **summarized** here

Scenarios

- Attempted to define model for capturing key characteristics of each scenario.
  - Operational characteristics
    - General description
    - Dynamic addressing
    - NAT
    - QoS
  - Policy

Scenarios

- Security characteristics
  - Authentication
  - Identity
  - Identity protection
- WG needs to decide on model

Scenarios

- Key scenarios
  - This is not an attempt at a complete list of possible scenarios, but these are key categories that the WG may wish to consider.
  - Scenarios should help to drive scoping and requirements
  - Additional “problem areas” introduced other issues that may affect one or more scenarios

Key Scenarios

- VPN site-to-site tunnels
- Secure remote access
- End-to-end security
- IP storage
- PPVPN/MPLS
- Mobile IP/Wireless
- Delay sensitive applications

Operational Requirements

- Scalability
  - Lightweight (memory/cpu/etc.) desirable for both small-footprint devices and those larger devices supporting tons of connections
- Fast setup
  - Expense of processing new negotiation requests includes a cost based on number of messages and amount of processing (including authentication)
  - Cost of connection maintenance vs. cost of “no maintenance”
  - Some scenarios may require both “fast” and “low delay”

Operational Requirements

- One-phase vs. two-phase exchange
  - Certain scenarios will have multiple IPsec connections between a pair of IPsec endpoints
    - IPsec tunnels may be negotiated simultaneously or sequentially (e.g. configuration-driven vs. demand-driven)
    - Possibly desirable to amortize cost of initial negotiation across the additional tunnels

Operational Requirements

- Something needs to guarantee operational integrity of “tunnel management channel”
  - Primary goal is mechanisms to ensure protocol convergence
    - Two endpoints who have very different views of the state of connection result in black holes
    - Can’t always throw “routing” at this problem
  - Reachability between tunnel endpoints (DPD, etc.)
  - Communication of SA deletion (especially premature deletion due to operator action) to peer

Protocol Requirements

- Protocol Interaction
  - With “supporting” protocols, such as IPSP
- Identity
  - <to be covered via a separate presentation>
- Interaction with NAT
  - NATs aren’t disappearing anytime soon…
- General design criteria
  - Synopsis of discussion from –00 draft
  - (reasonable) modularity, (reasonable) extensibility, (reasonable) protocol convergence, (reasonable) simplicity

Policy Requirements

- Provisioning and management
  - Configuration
  - Discovery
- Expanding the selector set
  - QoS DSCP
  - VPN tags
  - Lists of selector entries

Policy Requirements

- SPD selectors and dynamic policy
  - Capability of adding to/removing from list
    - Ex. SCTP
  - Protocols that can dynamically discover traffic to be protected/application-controlled filter specification
    - Policy model must accommodate

Policy Requirements

- Retaining SAs in face of address changes
  - Not specifically a requirement, but this could make certain operational scenarios much easier
    - mobileIP, IPv6, NAT(? Maybe)
  - May need combining with modifying spd selectors
- Authorization
  - (help!)
- Additional per-connection policy
  - Inner address assignment, etc.
  - Identify absolute minimum for bootstrap, provide other via separate mechanism

Security Requirements

- Key agreement
- Key generation
- Authentication
- Resistance to DoS attacks
- Resistance to replay attacks
- Resistance to downgrade attacks
- Identity hiding
- PFS