Introduction to IPsec Virtual Private Networks

Session SEC-110

Agenda

• Introduction to VPNs and IPsec
• IPsec Technologies
• IPsec VPN Implementation
• Summary
What Are VPNs?

Connectivity Deployed on a Shared Infrastructure with the Same Policies and Performance as a Private Network, with Lower Total Cost of Ownership

What Is IPsec?

- IPsec: An Internet standard* framework for the establishment and management of data privacy between network entities
  
  Still in draft standard status
  
  Therefore...

*RFC 2401–2412
...An IPsec VPN Is...

- A VPN which uses IPsec to insure data authenticity and confidentiality
- IPsec is the framework that lets you negotiate exactly which options to use
- MPLS VPNs allow the separation of IP traffic across service provider networks

Agenda

- Introduction to VPNs and IPsec
- IPsec Technologies
- IPsec VPN Implementation
- Summary
Introduction to IPsec Technologies

- Security associations
- Key management
- Encryption
- Authentication
- Digital certificates and signatures
- Data integrity
- Non-repudiation

Security Association

- Agreement between two entities on a security policy, including:
  - Encryption algorithm
  - Authentication algorithm
  - Shared session keys
  - SA lifetime
- Types of security associations
  - Bi-directional for management (IKE SA)
  - Unidirectional for data (IPSec SA)
IPSec Modes

- **Tunnel Mode**
  - IP HDR
  - IPsec HDR
  - Data
  - May Be Encrypted

- **Transport Mode**
  - IP HDR
  - IPsec HDR
  - Data
  - May Be Encrypted

Key Management

- Public key cryptosystems enable secure exchange of private crypto keys across open networks
- Re-keying at appropriate intervals
- IKE = Internet Key Exchange protocols
  - Incorporates ISAKMP/Oakley
Encryption

- Current standards: DES and Triple-DES
  Over 20 years in the field
- AES beginning deployment
  New standard
  More computationally efficient
  Longer keys = more secure

Authentication

- IPsec standards focus on authentication of two network devices to each other
  IP address/preshared key
  Digital certificates
- User authentication is added on top if required
  RADIUS and TACACS+ are the standard protocols for authentication servers
- XAUTH is being added to the standards to address user authentication
Digital Certificates

- Mathematical proof of various network actions:
  - The sender is really who they claim to be
  - The data has not been changed in transit
  - The receiver can prove the identity of the sender

- Certificates provide scalable authentication

What’s in a Certificate?

- Digital Certificates contain:
  - Serial Number
  - Validity dates
  - Issuer’s name
  - Subject’s name
  - Subject’s public key info

- Signed by CA
How Certificates Work

Certificate Authority
Trusted Third Party

Tom
Request Certificate

Issue Certificates

Digital Certificates

Harry
Request Certificate

Issue Certificates

Certificate Validation (CRL)

Data Integrity

- Data received = data sent
- Mathematical algorithms + digital signatures
Non-Repudiation

- Prevents a party involved in a communication from later denying having participated
- Proof of identity of sender
- Mathematical algorithms + digital signature

Agenda

- Introduction to VPNs and IPsec
- IPsec Technologies
- IPsec VPN Implementation
- Summary
Site-to-Site and Remote Access VPNs

- **Site-to-site**
  - Between two network entities
  - Trusted networks behind each entity

- **Remote access**
  - Central control of remote users
  - No trusted networks at remote location

---

IPsec VPN Implementation

- **PC to Server**
- **Router to Router**
- **PC to Router**
- **Router to Firewall**
Network-Based Implementation

- Routers
  All-purpose network device
- Firewalls
  All-purpose security device
- Dedicated devices
  Single purpose which stands by itself
- Mixed environments

Host-Based Implementation

- Servers
  When network devices not accessible for VPN configuration
- Clients
  Centrally controlled by Remote Access Concentrator
  XAUTH/Mode Config
  Software clients for many platforms
  Hardware clients
Summary

• An IPsec VPN is a VPN which uses IPSec for privacy
• IPsec utilizes a range of technologies to provide privacy for the VPN
• IPsec can be implemented at the network level or host level

Additional Information

• Cisco SAFE Blueprint
  http://www.cisco.com/GO/SAFE

• Cisco Security Information
  http://www.cisco.com/GO/VPN
  http://www.cisco.com/GO/Security
Where to Go from Here?

- SEC-210 Deploying and Managing Enterprise IPsec VPNs
- SEC-211 Deploying and Managing Provider-based IPsec VPNs
- SEC-214 Deploying Complex and Large Scale IPsec VPNs
- SEC-310 Troubleshooting the Implementation of IPsec VPNs

Introduction to IPsec Virtual Private Networks
Session SEC-110
Please Complete Your Evaluation Form

Session SEC-110