VPN and IPsec
Virtual Private Network

- Creates a secure tunnel over a public network
  - Client to firewall
  - Router to router
  - Firewall to firewall

- Uses the Internet as the public backbone to access a secure private network
  - Remote employees can access their office network

- Two types:
  - Remote access
  - Site-to-site VPN
VPN Implementation

• Hardware
  – Usually a VPN-type router
  – Pros: highest network throughput, plug and play, dual purpose
  – Cons: cost and lack of flexibility

• Software
  – Ideal for two end-points in different organisations
  – Pros: flexible, and low relative cost
  – Cons: lack of efficiency, more labor training required, lower productivity; higher labor costs

• Firewall
  – Pros: cost effective, tri-purpose, hardens the operating system
  – Cons: still relatively costly
VPN Protocols

• PPTP (Point-to-Point tunneling Protocol)
  – Developed by Microsoft to secure dial-up connections
  – Operates in the data-link layer

• L2F (Layer 2 Forwarding Protocol)
  – Developed by Cisco
  – Similar as PPTP

• L2TP (Layer 2 Tunneling Protocol)
  – IETF standard
  – Combines the functionality of PPTP and L2F

• IPsec (Internet Protocol Security)
  – Open standard for VPN implementation
  – Operates on the network layer
Other Modern VPNs

- **MPLS VPN**
  - Used for large and small enterprises
  - Pseudowire, VPLS, VPRN

- **GRE Tunnel**
  - Packet encapsulation protocol developed by Cisco
  - Not encrypted
  - Implemented with IPsec

- **L2TP IPsec**
  - Uses L2TP protocol
  - Usually implemented along with IPsec
  - IPsec provides the secure channel, while L2TP provides the tunnel
Advantages of VPN

• Cheaper connection
  – Use the Internet connection instead of a private lease line

• Scalability
  – Flexibility of growth
  – Efficiency with broadband technology

• Availability
  – Available everywhere there is an Internet connection
Disadvantages of VPN

• VPNs require an in-depth understanding of public network security issues and proper deployment precautions
• Availability and performance depends on factors largely outside of their control
• VPNs need to accommodate protocols other than IP and existing internal network technology
**IPsec**

- Provides Layer 3 security (RFC 2401)
  - Transparent to applications (no need for integrated IPsec support)
- A set of protocols and algorithms used to secure IP data at the network layer
- Combines different components:
  - Security associations (SA)
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)
  - Internet Key Exchange (IKE)
- A security context for the VPN tunnel is established via the ISAKMP
What is IPSec?

• IETF standard that enables encrypted communication between peers:
  – Consists of open standards for securing private communications
  – Network layer encryption ensuring data confidentiality, integrity, and authentication
  – Scales from small to very large networks
IPsec Standards

• RFC 4301 “The IP Security Architecture”
  – Defines the original IPsec architecture and elements common to both AH and ESP

• RFC 4302
  – Defines authentication headers (AH)

• RFC 4303
  – Defines the Encapsulating Security Payload (ESP)

• RFC 2408
  – ISAKMP

• RFC 5996
  – IKE v2 (Sept 2010)

• RFC 4835
  – Cryptographic algorithm implementation for ESP and AH
Benefits of IPsec

• Confidentiality
  – By encrypting data

• Integrity
  – Routers at each end of a tunnel calculates the checksum or hash value of the data

• Authentication
  – Signatures and certificates
  – All these while still maintaining the ability to route through existing IP networks

“IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6” - (RFC 2401)
Benefits of IPsec

• Data integrity and source authentication
  – Data “signed” by sender and “signature” is verified by the recipient
  – Modification of data can be detected by signature “verification”
  – Because “signature” is based on a shared secret, it gives source authentication

• Anti-replay protection
  – Optional; the sender must provide it but the recipient may ignore

• Key management
  – IKE – session negotiation and establishment
  – Sessions are rekeyed or deleted automatically
  – Secret keys are securely established and authenticated
  – Remote peer is authenticated through varying options
Different Layers of Encryption

- **Application Layer** – SSL, PGP, SSH, HTTPS
- **Network Layer** – IPsec
- **Link Layer Encryption**
IPsec Modes

• Tunnel Mode
  – Entire IP packet is encrypted and becomes the data component of a new (and larger) IP packet.
  – Frequently used in an IPsec site-to-site VPN

• Transport Mode
  – IPsec header is inserted into the IP packet
  – No new packet is created
  – Works well in networks where increasing a packet’s size could cause an issue
  – Frequently used for remote-access VPNs
Tunnel vs. Transport Mode IPsec

Without IPsec

Transport Mode IPsec

Tunnel Mode IPsec
Transport vs Tunnel Mode

**Transport Mode:** End systems are the initiator and recipient of protected traffic

**Tunnel Mode:** Gateways act on behalf of hosts to protect traffic
IPsec Architecture

- AH: Authentication Header
- ESP: Encapsulating Security Payload
- IKE: The Internet Key Exchange

IPsec Security Policy
Security Associations (SA)

- A collection of parameters required to establish a secure session
- Uniquely identified by three parameters consisting of
  - Security Parameter Index (SPI)
  - IP destination address
  - Security protocol (AH or ESP) identifier
- An SA is either uni- or bidirectional
  - IKE SAs are bidirectional
  - IPsec SAs are unidirectional
    - Two SAs required for a bidirectional communication
- A single SA can be used for AH or ESP, but not both
  - must create two (or more) SAs for each direction if using both AH and ESP
Security Parameter Index (SPI)

• A unique 32-bit identification number that is part of the Security Association (SA)
• It enables the receiving system to select the SA under which a received packet will be processed.
• Has only local significance, defined by the creator of the SA.
• Carried in the ESP or AH header
• When an ESP/AH packet is received, the SPI is used to look up all of the crypto parameters
How to Set Up SA

• Manually
  – Sometimes referred to as “manual keying”
  – You configure on each node:
    • Participating nodes (i.e. traffic selectors)
    • AH and/or ESP [tunnel or transport]
    • Cryptographic algorithm and key

• Automatically
  – Using IKE (Internet Key Exchange)
ISAKMP

• Internet Security Association and Key Management Protocol
• Used for establishing Security Associations (SA) and cryptographic keys
• Only provides the framework for authentication and key exchange, but key exchange is independent
• Key exchange protocols
  – Internet Key Exchange (IKE)
  – Kerberized Internet Negotiation of Keys (KINK)
Authentication Header (AH)

- Provides source authentication and data integrity
  - Protection against source spoofing and replay attacks
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- If both AH and ESP are applied to a packet, AH follows ESP
- Operates on top of IP using protocol 51
- In IPv4, AH protects the payload and all header fields except mutable fields and IP options (such as IPsec option)
**AH Header Format**

- **Next Header (8 bits):** indicates which upper layer protocol is protected (UDP, TCP, ESP)
- **Payload Length (8 bits):** size of AH in 32-bit longwords, minus 2
- **Reserved (16 bits):** for future use; must be set to all zeroes for now
- **SPI (32 bits):** arbitrary 32-bit number that specifies to the receiving device which security association is being used (security protocols, algorithms, keys, times, addresses, etc)
- **Sequence Number (32 bits):** start at 1 and must never repeat. It is always set but receiver may choose to ignore this field
- **Authentication Data:** ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)
Encapsulating Security Payload (ESP)

- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
  - uses symmetric key encryption
- Must encrypt and/or authenticate in each packet
  - Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload
ESP Header Format

- SPI: arbitrary 32-bit number that specifies SA to the receiving device
- Seq #: start at 1 and must never repeat; receiver may choose to ignore
- IV: used to initialize CBC mode of an encryption algorithm
- Payload Data: encrypted IP header, TCP or UDP header and data
- Padding: used for encryption algorithms which operate in CBC mode
- Padding Length: number of bytes added to the data stream (may be 0)
- Next Header: the type of protocol from the original header which appears in the encrypted part of the packet
- Authentication Header: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)
Packet Format Alteration for AH Transport Mode

Authentication Header

Without AH

Original IP Header | TCP/UDP | Data

With AH

Original IP Header | AH Header | TCP/UDP | Data

Authenticated except for mutable fields in IP header
(ToS, TTL, Header Checksum, Offset, Flags)
Packet Format Alteration for ESP Transport Mode

Encapsulating Security Payload

Before applying ESP:

- Original IP Header
- TCP/UDP
- Data

After applying ESP:

- Original IP Header
- ESP Header
- TCP/UDP
- Data
- ESP Trailer
- ESP Authentication

Encrypted

Authenticated
Packet Format Alteration for AH Tunnel Mode

**Authentication Header**

Before applying AH:

Original IP Header | TCP/UDP | Data

After applying AH:

New IP Header | AH Header | Original IP Header | Data

Authenticated except for mutable fields in new IP header

(ToS, TTL, Header Checksum, Offset, Flags)
Packet Format Alteration for ESP Tunnel Mode

Encapsulating Security Payload

Before applying ESP:

- Original IP Header
- TCP/UDP
- Data

After applying ESP:

- Original IP Header
- ESP Header
- ESP Authentication

| New IP Header | ESP Header | Original IP Header | TCP/UDP | Data | ESP Trailer | ESP Authentication |

| Encrypted |

| Authenticated |
Internet Key Exchange (IKE)

• “An IPsec component used for performing mutual authentication and establishing and maintaining Security Associations.” (RFC 5996)
• Typically used for establishing IPsec sessions
• A key exchange mechanism
• Five variations of an IKE negotiation:
  – Two modes (aggressive and main modes)
  – Three authentication methods (pre-shared, public key encryption, and public key signature)
• Uses UDP port 500
## IKE Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main mode</td>
<td>Three exchanges of information between IPsec peers. Initiator sends one or more proposals to the other peer (responder) Responder selects a proposal</td>
</tr>
<tr>
<td>Aggressive Mode</td>
<td>Achieves same result as main mode using only 3 packets First packet sent by initiator containing all info to establish SA Second packet by responder with all security parameters selected Third packet finalizes authentication of the ISAKMP session</td>
</tr>
<tr>
<td>Quick Mode</td>
<td>Negotiates the parameters for the IPsec session. Entire negotiation occurs within the protection of ISAKMP session</td>
</tr>
</tbody>
</table>
Internet Key Exchange (IKE)

- **Phase I**
  - Establish a secure channel (ISAKMP SA)
  - Using either main mode or aggressive mode
  - Authenticate computer identity using certificates or pre-shared secret

- **Phase II**
  - Establishes a secure channel between computers intended for the transmission of data (IPsec SA)
  - Using quick mode
Overview of IKE

1. Traffic which needs to be protected

2. IKE Phase 1

   Secure communication channel

3. IKE Phase 2

   IPsec Tunnel

4. Secured traffic exchange
## ISAKMP Header Format

The ISAKMP header format consists of several fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator Cookie</td>
<td>0-31</td>
</tr>
<tr>
<td>Responder Cookie</td>
<td></td>
</tr>
<tr>
<td>Next Payload</td>
<td></td>
</tr>
<tr>
<td>Major Version</td>
<td>0-31</td>
</tr>
<tr>
<td>Minor Version</td>
<td>0-31</td>
</tr>
<tr>
<td>Exchange Type</td>
<td>0-31</td>
</tr>
<tr>
<td>Flags</td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>0-31</td>
</tr>
<tr>
<td>Total Length of Message</td>
<td>0-31</td>
</tr>
</tbody>
</table>
ISAKMP Message Format

Next Payload: 1 byte; identifier for next payload in message. If it is the last payload, it will be set to 0.

Reserved: 1 byte; set to 0

Payload Length: 2 bytes; length of payload (in bytes) including the header

Payload: The actual payload data
IKE Phase 1 (Main Mode)

• Main mode negotiates an ISAKMP SA which will be used to create IPsec SAs

• Three steps
  – SA negotiation (encryption algorithm, hash algorithm, authentication method, which DF group to use)
  – Do a Diffie-Hellman exchange
  – Provide authentication information
  – Authenticate the peer
IKE Phase 1 (Main Mode)

1. Negotiate IKE Policy
   - IKE Message 1 (SA proposal)
   - IKE Message 2 (accepted SA)

2. Authenticated DH Exchange
   - IKE Message 3 (DH public value, nonce)
   - IKE Message 4 (DH public value, nonce)

3. Compute DH shared secret and derive keying material

4. Protect IKE Peer Identity
   - IKE Message 5 (Authentication material, ID)
   - IKE Message 6 (Authentication material, ID) (Encrypted)
IKE Phase 1 (Aggressive Mode)

- Uses 3 (vs 6) messages to establish IKE SA
- No denial of service protection
- Does not have identity protection
- Optional exchange and not widely implemented
IKE Phase 2 (Quick Mode)

- All traffic is encrypted using the ISAKMP Security Association
- Each quick mode negotiation results in two IPsec Security Associations (one inbound, one outbound)
- Creates/refreshes keys
IKE Phase 2 (Quick Mode)

1. Message 1 (authentication/keying material and SA proposal)
2. Validate message 1
3. Message 2 (authentication/keying material and accepted SA)
4. Validate message 2
5. Message 3 (hash for proof of integrity/authentication)
6. Validate message 3
7. Compute keying material
IKE v2: Replacement for Current IKE Specification

• Feature Preservation
  – Most features and characteristics of baseline IKE v1 protocol are being preserved in v2

• Compilation of Features and Extensions
  – Quite a few features that were added on top of the baseline IKE protocol functionality in v1 are being reconciled into the mainline v2 framework

• Some New Features
IKE v2: What Is Not Changing

• Features in v1 that have been debated but are ultimately being preserved in v2
  – Most payloads reused
  – Use of nonces to ensure uniqueness of keys

• v1 extensions and enhancements being merged into mainline v2 specification
  – Use of a ‘configuration payload’ similar to MODECFG for address assignment
  – ‘X-auth’ type functionality retained through EAP
  – Use of NAT Discovery and NAT Traversal techniques
IKE v2: What Is Changing

• Significant Changes Being to the Baseline Functionality of IKE
  – EAP adopted as the method to provide legacy authentication integration with IKE
  – Public signature keys and pre-shared keys, the only methods of IKE authentication
  – Use of ‘stateless cookie’ to avoid certain types of DOS attacks on IKE
  – Continuous phase of negotiation
How Does IKE v2 Work?

IKE_SA_INIT (Two Messages) ➔ IKE_SA Authentication Parameters Negotiated

IKE_AUTH (Two Messages) ➔ IKE Authentication Occurs and One CHILD_SA Created

CREATE_CHILD_SA (Two Messages) ➔ Second CHILD_SA Created

Protected Data ➔
Considerations For Using IPsec

• Security Services
  – Data origin authentication
  – Data integrity
  – Replay protection
  – Confidentiality

• Size of network

• How trusted are end hosts – can apriori communication policies be created?

• Vendor support

• What other mechanisms can accomplish similar attack risk mitigation
Non-Vendor Specific Deployment Issues

• Historical Perception
  – Configuration nightmare
  – Not interoperable

• Performance Perception
  – Need empirical data
  – Where is the real performance hit?

• Standards Need Cohesion
Vendor Specific Deployment Issues

• Lack of interoperable defaults
  – A default does NOT mandate a specific security policy
  – Defaults can be modified by end users

• Configuration complexity
  – Too many knobs
  – Vendor-specific terminology

• Good News: IPv6 support in most current implementations
IPsec Concerns

• Are enough people aware that IKEv2 is not backwards compatible with IKEv1?
  – IKEv1 is used in most IPsec implementations
  – Will IKEv2 implementations first try IKEv2 and then revert to IKEv1?

• Is IPsec implemented for IPv6?
  – Some implementations ship IPv6 capable devices without IPsec capability and host requirements is changed from MUST to SHOULD implement

• OSPFv3
  – All vendors ‘IF’ they implement IPsec used AH
  – Latest standard to describe how to use IPsec says MUST use ESP w/Null encryption and MAY use AH
IPsec Concerns (cont)

• What is transport mode interoperability status?
  – Will end user authentication be interoperable?

• PKI Issues
  – Which certificates do you trust?
  – How does IKEv1 and/or IKEv2 handle proposals with certificates?
  – Should common trusted roots be shipped by default?
  – Who is following and implementing pki4ipsec-ikecert-profile (rfc4945)

• Have mobility scenarios been tested?
  – Mobility standards rely heavily on IKEv2

• ESP – how determine if ESP-Null vs Encrypted
IPsec Best Practices

• Use IPsec to provide integrity in addition to encryption
  – Use ESP option

• Use strong encryption algorithms
  – AES instead of DES

• Use a good hashing algorithm
  – SHA instead of MD5

• Reduce the lifetime of the Security Association (SA) by enabling Perfect Forward Secrecy (PFS)
  – Increases processor burden so do this only if data is highly sensitive
Configuring IPsec

- **Step 1:** Configure the IKE Phase 1 Policy (ISAKMP Policy)
  - `crypto isakmp policy [priority]`

- **Step 2:** Set the ISAKMP Identity
  - `crypto isakmp identity {ipaddress|hostname}`

- **Step 3:** Configure the IPsec transfer set
  - `crypto ipsec transform-set transform-set-name <transform1> <transform2> mode [tunnel|transport]`
  - `crypto ipsec security-association lifetime seconds seconds`
Configuring IPsec

• Step 5: Creating map with name
  – crypto map crypto-map-name seq-num ipsec-isakmp
  – match address access-list-id
  – set peer [ipaddress|hostname]
  – set transform-set transform-set-name
  – set security-association lifetime seconds seconds
  – set pfs [group1|group2]

• Step 6: Apply the IPsec Policy to an Interface
  – crypto map crypto-map-name local-address interface-id
IPsec Layout

Encrypted session

R1

Public Network

R2
Router Configuration

crypto isakmp policy 1
  authentication pre-share
  encryption aes
  hash sha
  group 5

crypto isakmp key Training123 address 172.16.11.66
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map LAB-VPN 10 ipsec-isakmp
  match address 101
  set transform-set ESP-AES-SHA
  set peer 172.16.11.66
Router Configuration

```
int fa 0/1
crypto map LAB-VPN
Exit

access-list 101 permit ip 172.16.16.0 0.0.0.255 172.16.20.0 0.0.0.255
```
IPsec Debug Commands

- sh crypto ipsec sa
- sh crypto isakmp peers
- sh crypto isakmp sa
- sh crypto map
## Capture: Telnet

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Seq</th>
<th>Ack</th>
<th>Win</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 3.1259855</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 3.127649</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 3.127651</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 3.279317</td>
<td>2001:0:dd:4a:1</td>
<td>ICMPv6</td>
<td>68 Neighbor Solicitation for 2001:0:dd:4a:1 from 00:00:00:00:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 3.208382</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 3.478005</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 3.471802</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 3.471804</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 3.572494</td>
<td>192.168.1.1</td>
<td>TCP</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 3.554380</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 3.856188</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 3.555190</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 3.978556</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 3.989454</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23 3.900940</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24 3.990046</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 4.180949</td>
<td>192.168.1.1</td>
<td>Telnet</td>
<td>68 Telnet Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Additional Information**

- **Telnet**: The Telnet protocol is used for remote shell access over a network. It is a client-server protocol that uses TCP for transport and provides a virtual terminal interface.
- **IP**: The Internet Protocol (IP) is the fundamental communications protocol used to send and receive data packets over the internet.
- **TCP**: The Transmission Control Protocol (TCP) is a transport layer protocol that provides a reliable, ordered, and connection-oriented service.
Capture: Telnet + IPsec
Pretty Good IPsec Policy

• IKE Phase 1 (aka ISAKMP SA or IKE SA or Main Mode)
  – 3DES (AES-192 if both ends support it)
  – Lifetime (8 hours = 480 min = 28800 sec)
  – SHA-2 (256 bit keys)
  – DH Group 14 (aka MODP# 14)

• IKE Phase 2 (aka IPsec SA or Quick Mode)
  – 3DES (AES-192 if both ends support it)
  – Lifetime (1 hour = 60 min = 3600 sec)
  – SHA-2 (256 bit keys)
  – PFS 2
  – DH Group 14 (aka MODP# 14)
Questions