APNIC eLearning:
IPSec Basics

Contact: training@apnic.net

Overview

- Virtual Private Networks
- What is IPsec?
- Benefits of IPsec
- Tunnel and Transport Mode
- IPsec Architecture
- Security Associations and ISAKMP
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)
- IPSec Tunnel Creation

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
- VPN Protocols
  - PPTP (Point-to-Point tunneling Protocol)
  - L2F (Layer 2 Forwarding Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
  - IPSec (Internet Protocol Security)

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

Why IPsec?

- Internet Protocol (IP) is not secure
  - IP protocol was designed in the early stages of the Internet where security was not an issue
  - All hosts in the network are known
- Possible security issues
  - Source spoofing
  - Replay packets
  - No data integrity or confidentiality

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

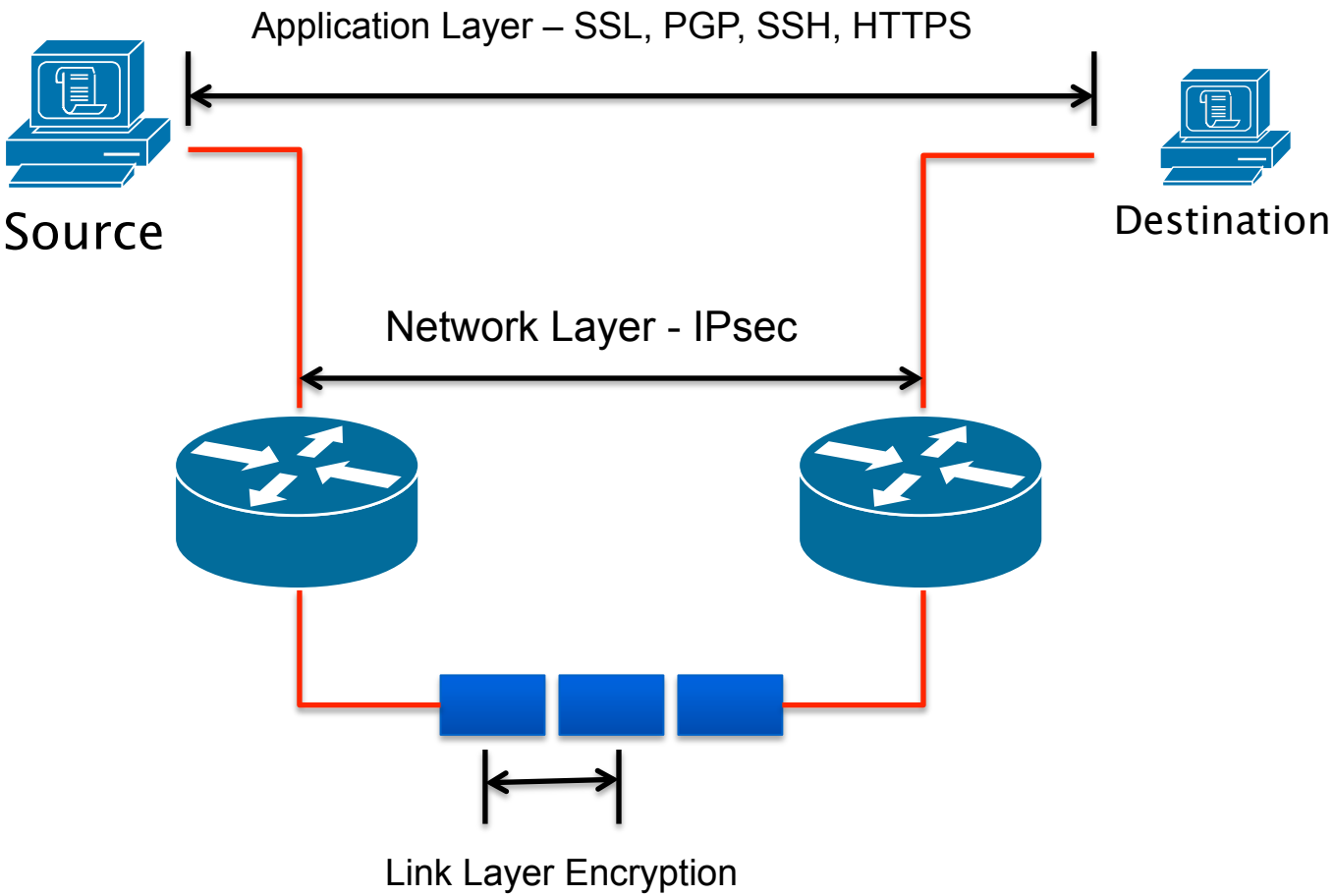
- Confidentiality
  - By encrypting data
- Integrity
  - Routers at each end of a tunnel calculates the checksum or hash value of the data
- Authentication
  - Signatures and certificates
  - All these while still maintaining the ability to route through existing IP networks

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

Benefits of IPsec

- Offers Confidentiality (encrypting data), Integrity , and Authentication
- 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

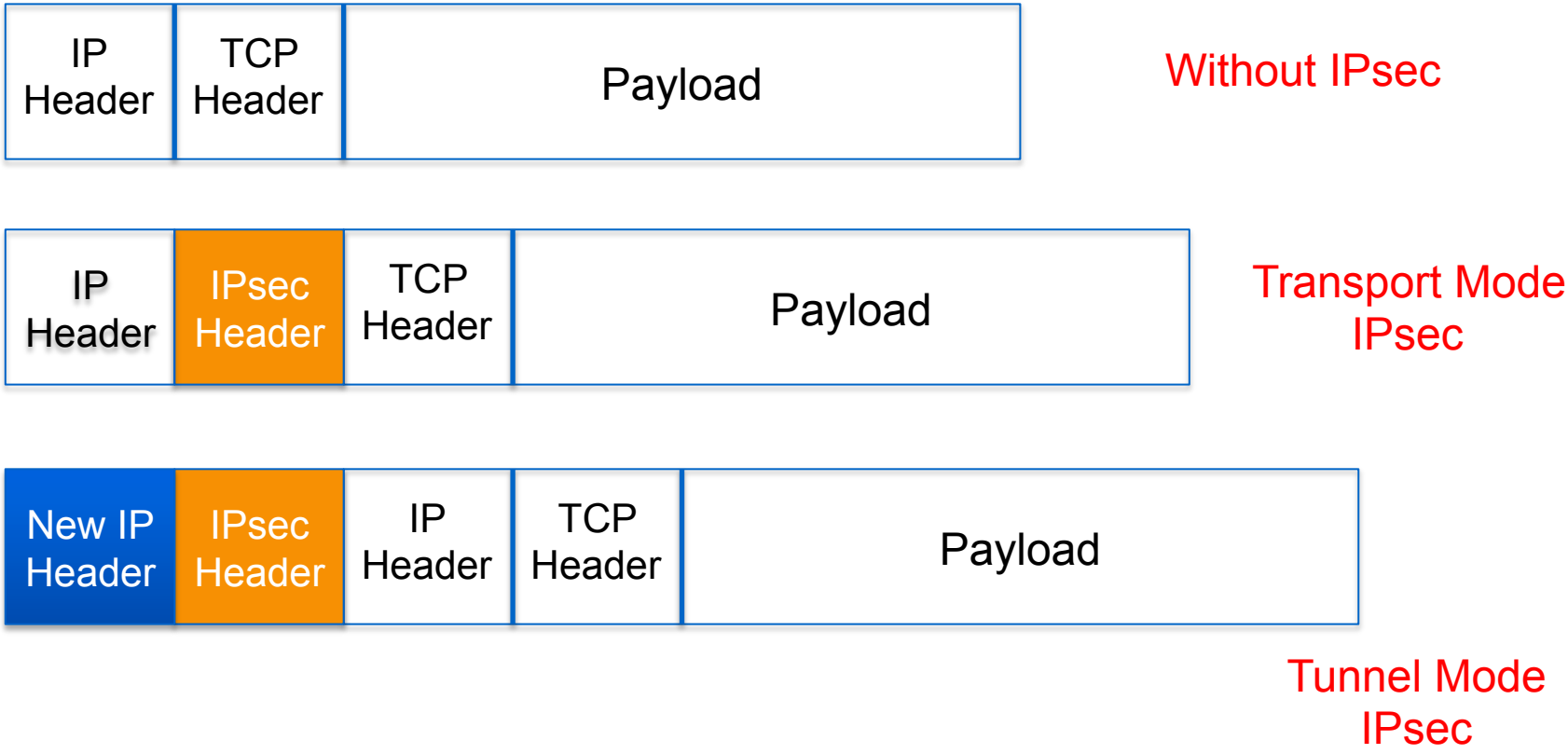
Different Layers of Encryption



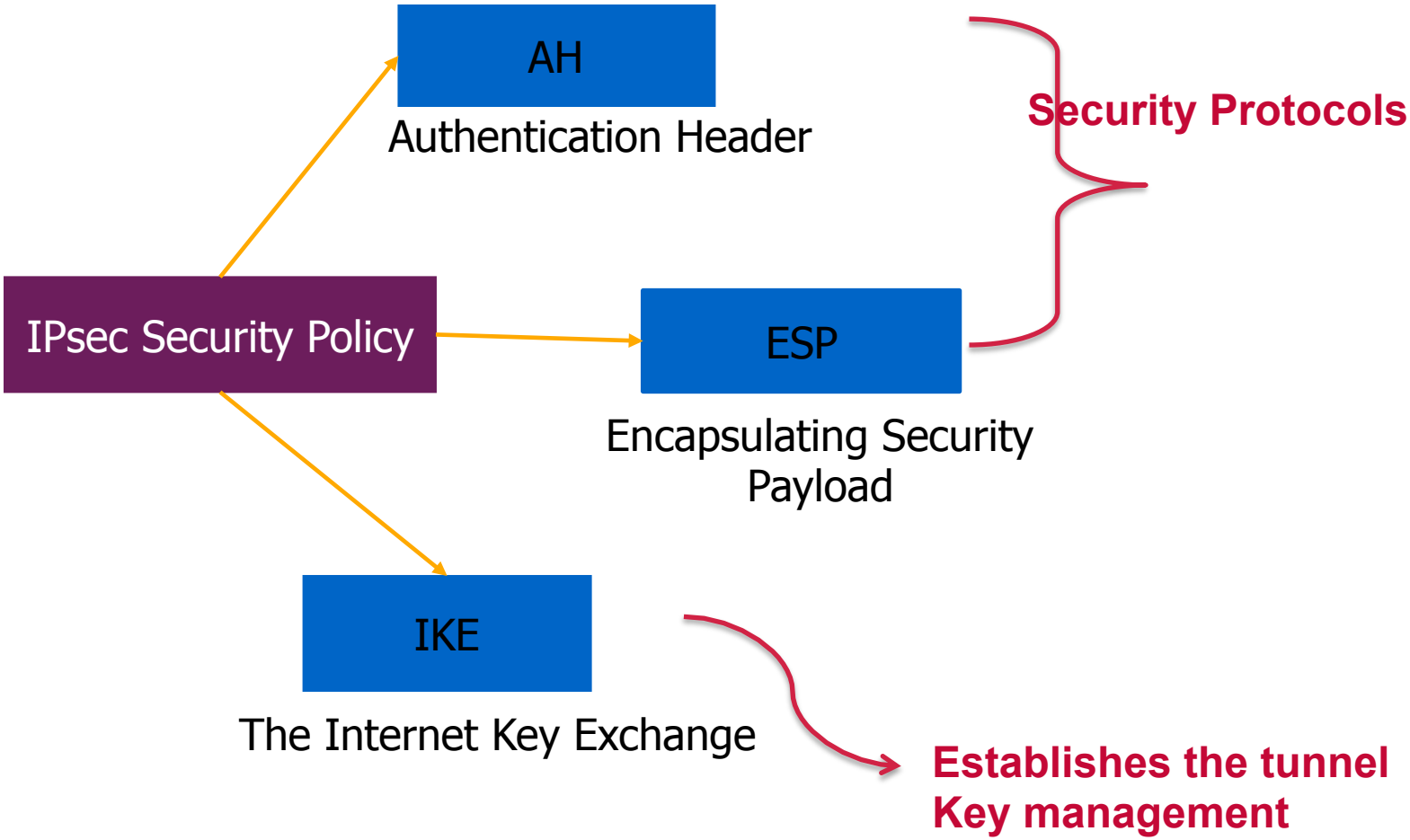
IPsec Modes

- 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



IPsec Architecture



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 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

How to Set Up an 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
- Defined by RFC 2408
- Used for establishing Security Associations (SA) and cryptographic keys
- Only provides the framework for authentication and key exchange, but key exchange independent
- Key exchange protocols
  - Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK)

Authentication Header (AH)

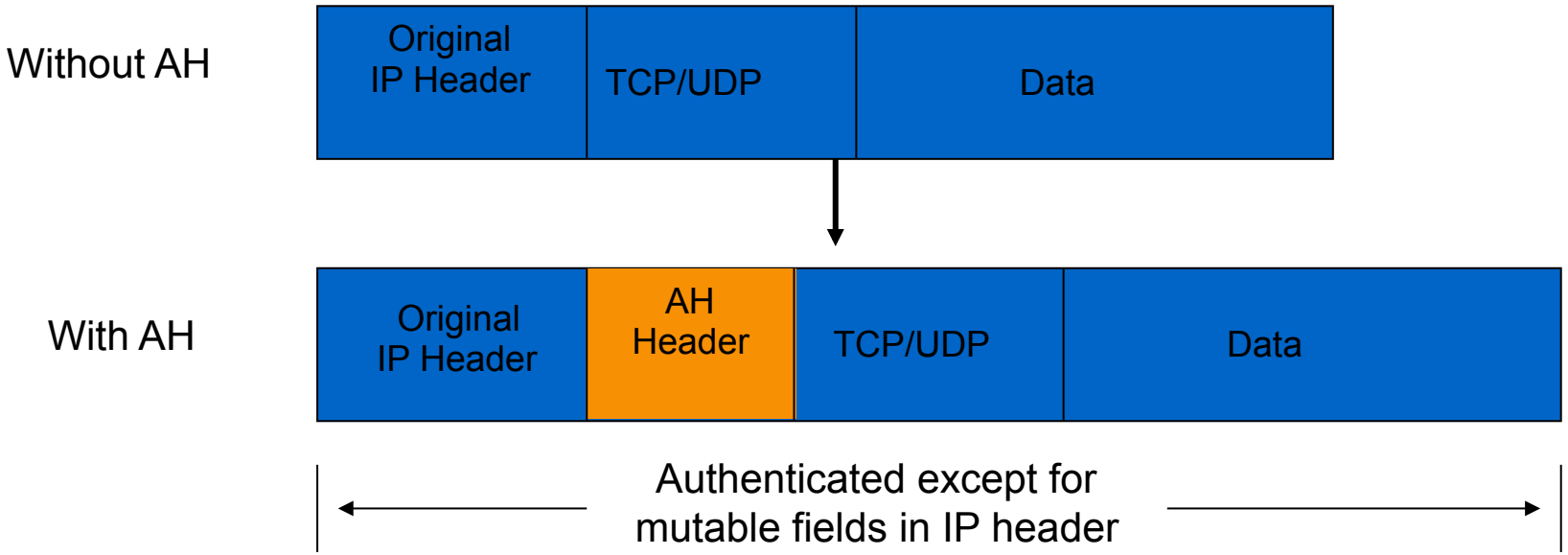
- Provides source authentication and data integrity
  - Protection against source spoofing and replay attacks
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- If both AH and ESP are applied to a packet, AH follows ESP
- Operates on top of IP using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

Encapsulating Security Payload (ESP)

- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
  - It 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

Packet Format Alteration for AH Transport Mode

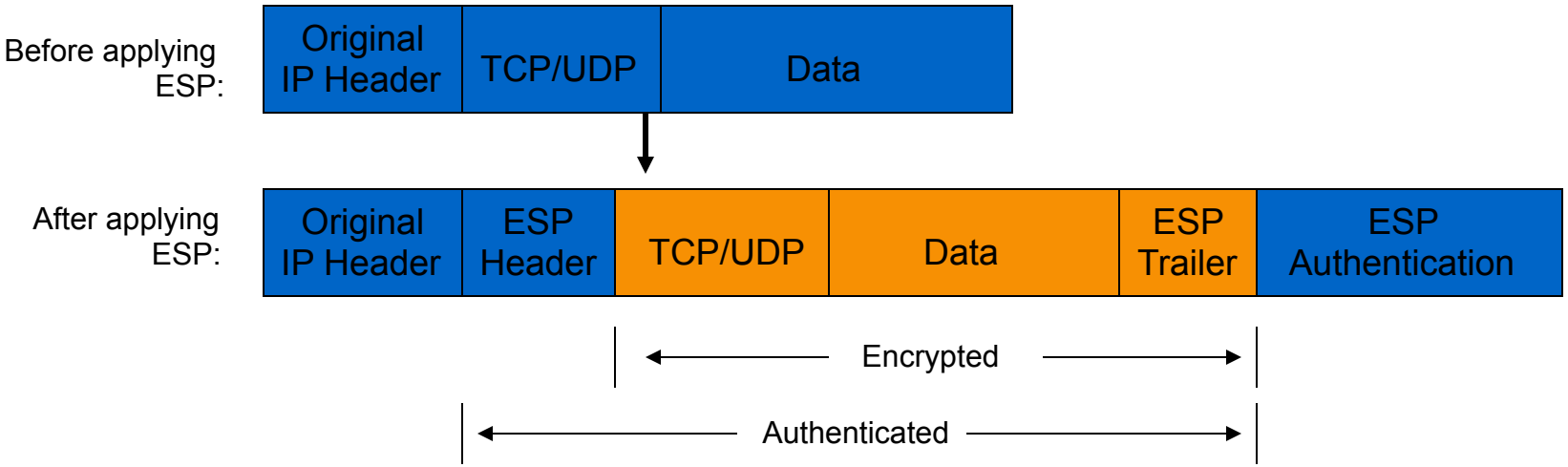
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

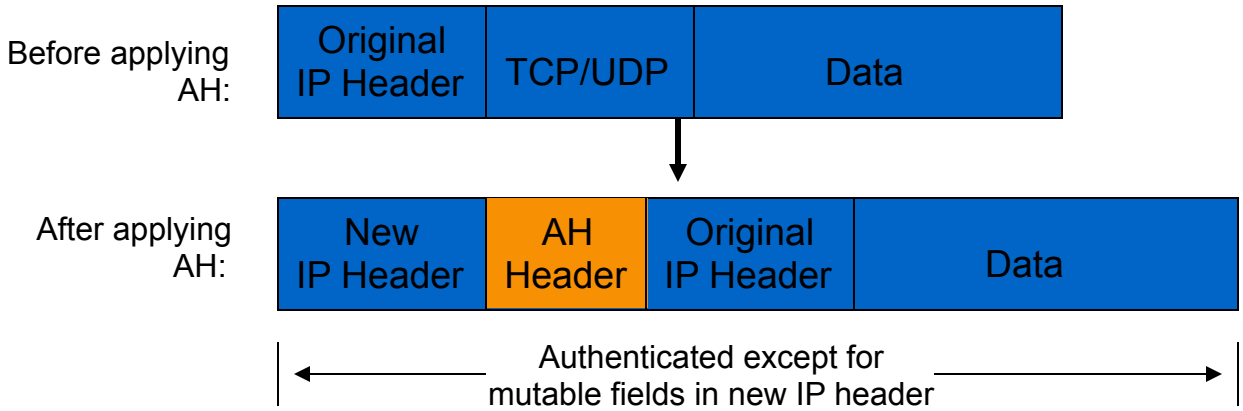
Packet Format Alteration for ESP Transport Mode

Encapsulating Security Payload



Packet Format Alteration for AH Tunnel Mode

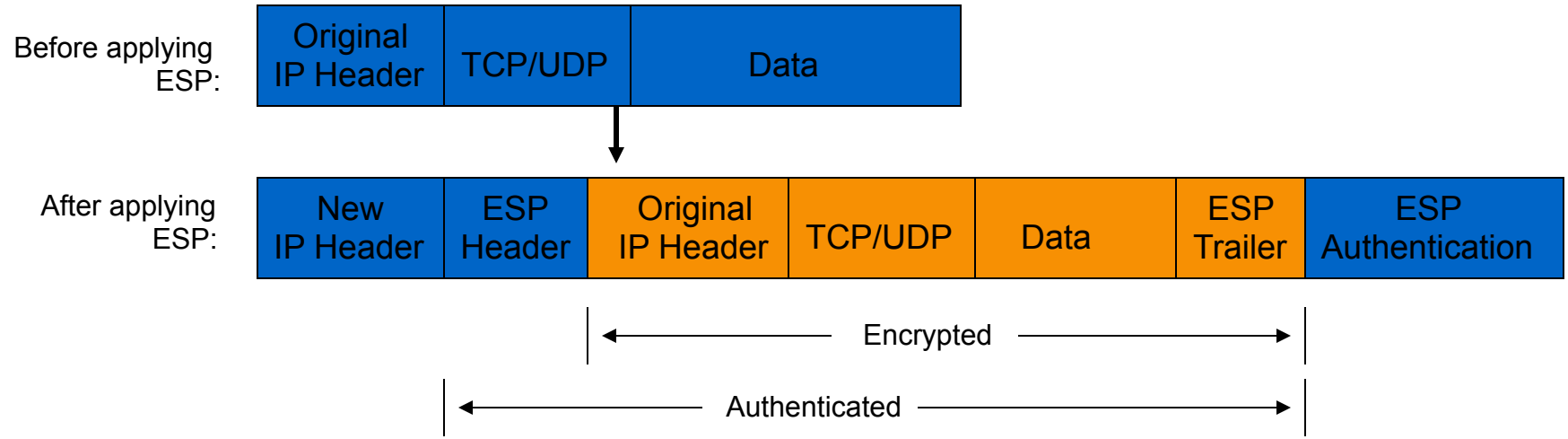
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

Packet Format Alteration for ESP Tunnel Mode

Encapsulating Security Payload



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

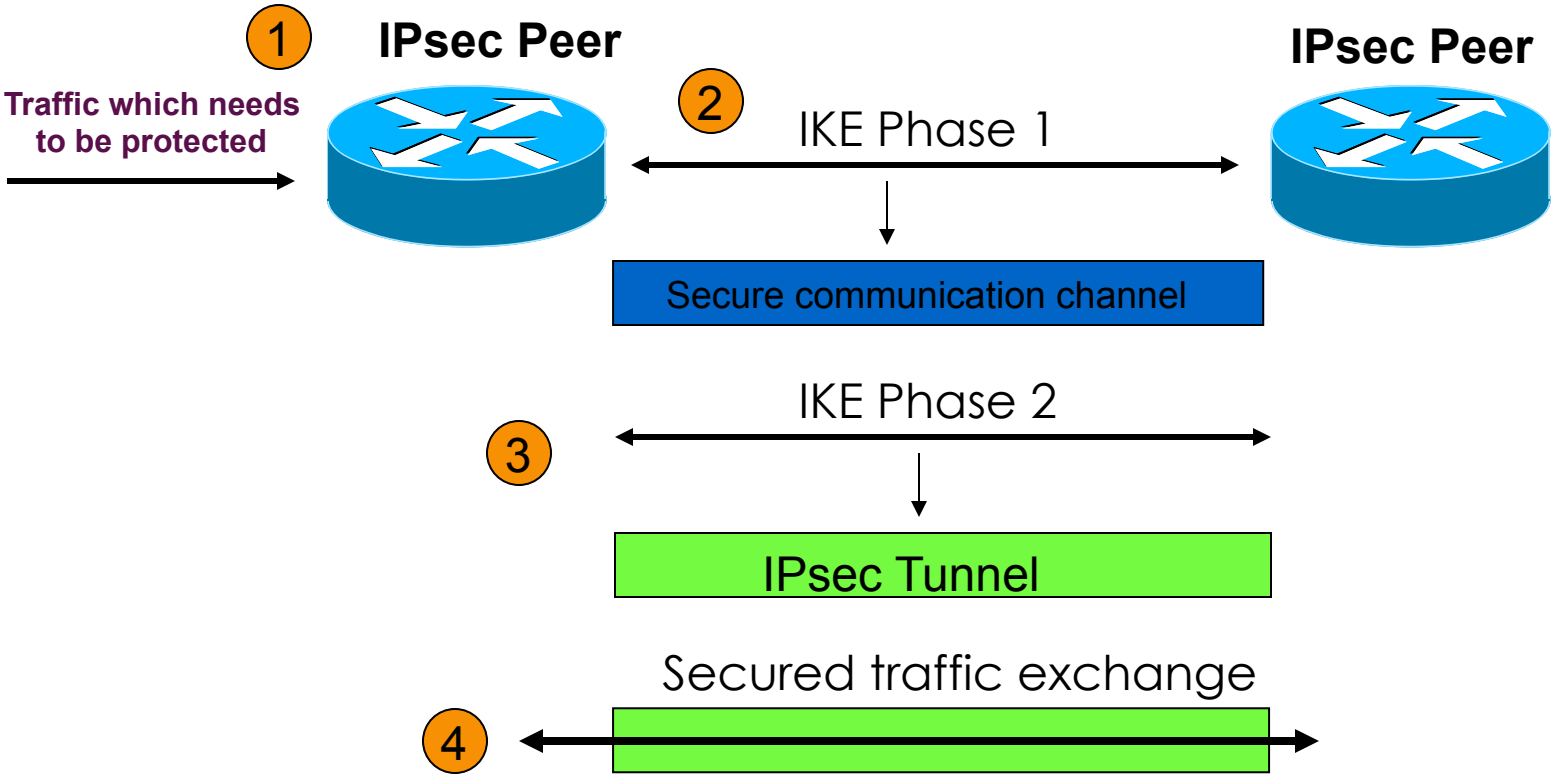
Mode	Description
Main mode	Three exchanges of information between IPsec peers. Initiator sends one or more proposals to the other peer (responder) Responder selects a proposal
Aggressive Mode	Achieves same result as main mode using only 3 packets First packet sent by initiator containing all info to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

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

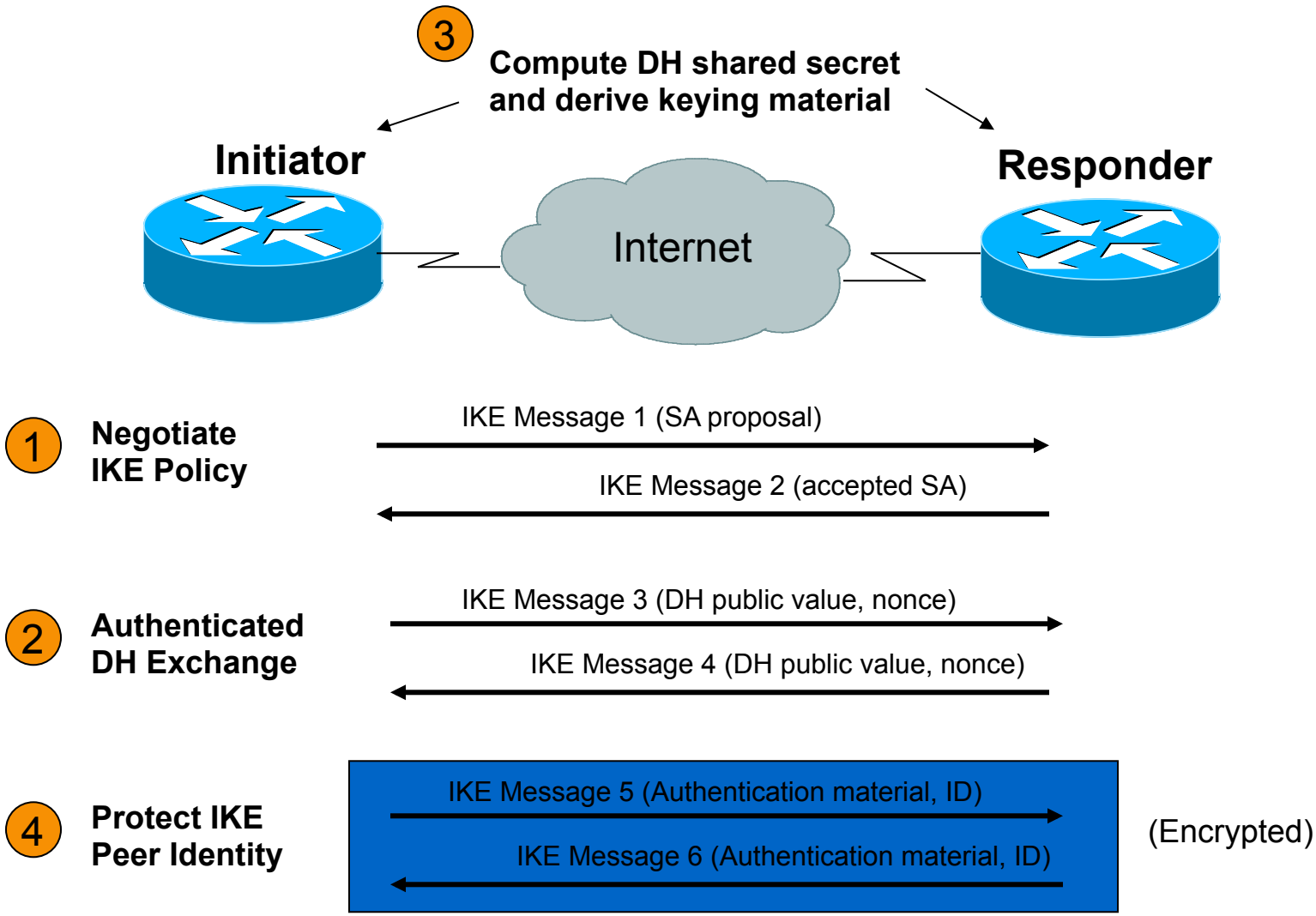
Overview of IKE



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)



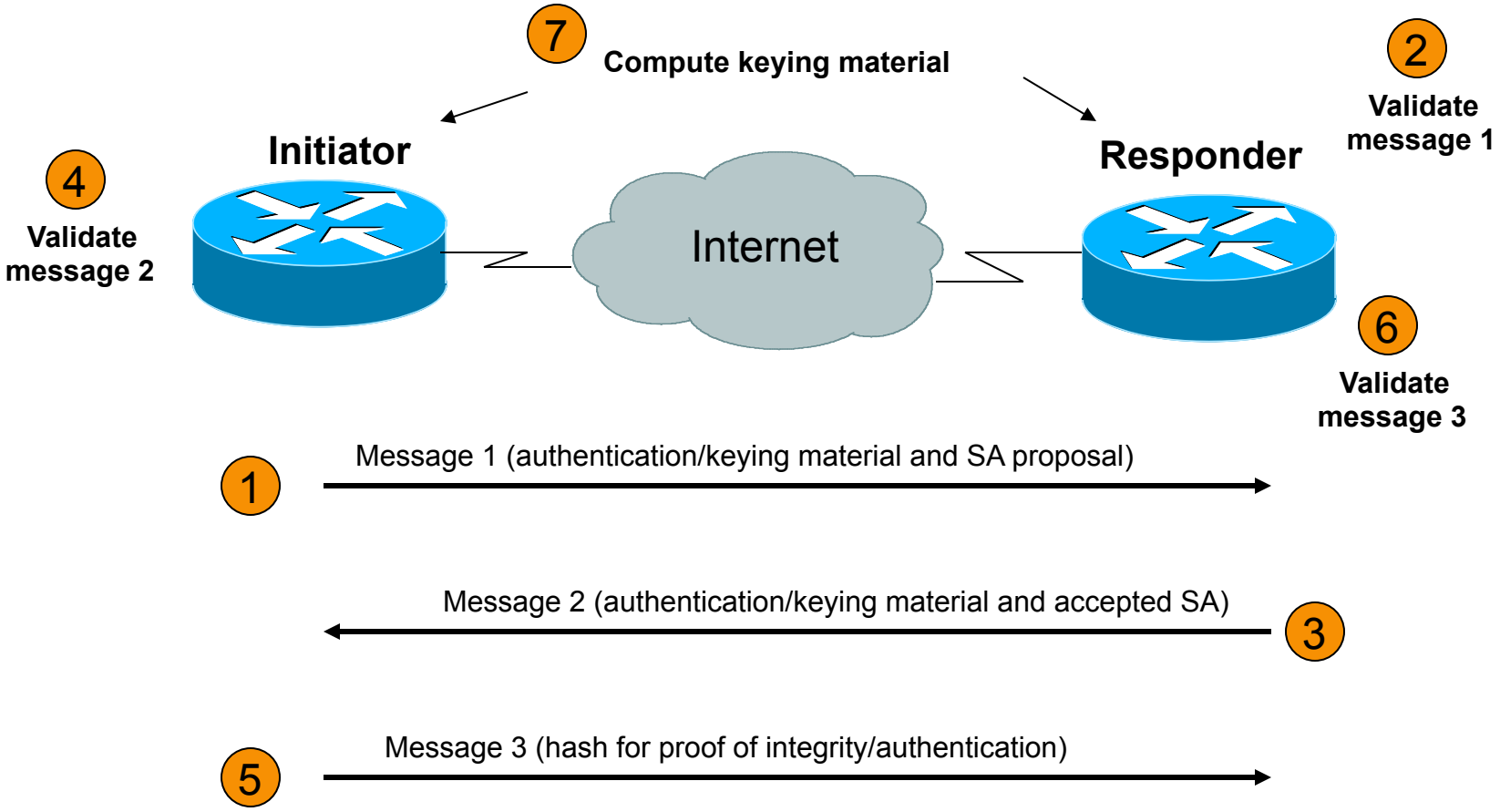
IKE Phase 1 (Aggressive Mode)

- 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)



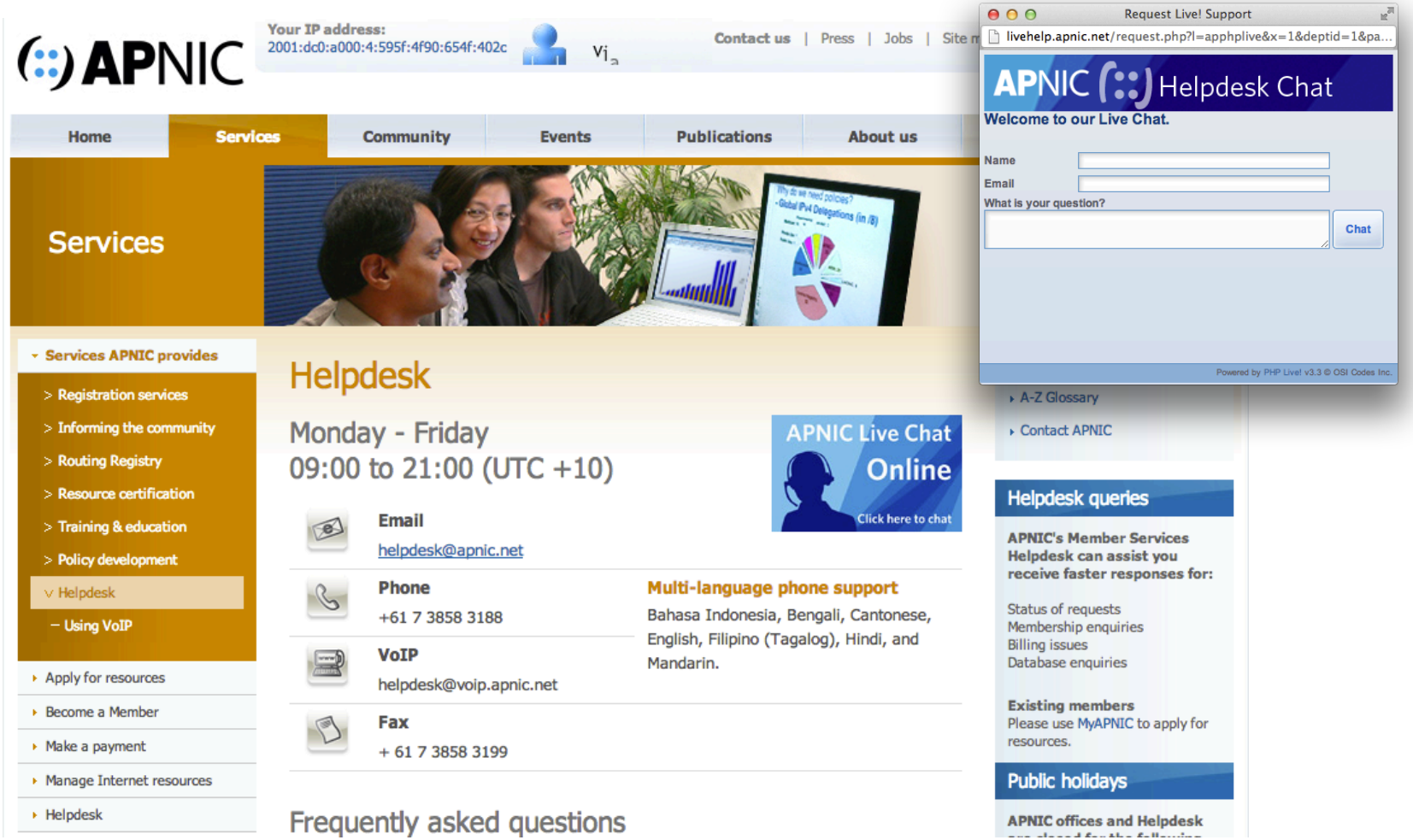
IPsec Best Practices

- Use IPsec to provide integrity in addition to encryption.
  - Use ESP option
- Use strong encryption algorithms 3DES and AES instead of DES
- Use SHA instead of MD5 as a hashing algorithm
- 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

Questions

- Please remember to fill out the feedback form
  - <survey-link>
- Slide handouts will be available after completing the survey

APNIC Helpdesk Chat



Thank You!

End of Session

APNIC