

Crypto Applications: VPN and IPsec

Sheryl Hermoso, APNIC
sheryl@apnic.net

Virtual Private Networks

- Creates a secure tunnel over a public network
- Any VPN is not automagically secure. You need to add security functionality to create secure VPNs. That means using firewalls for access control and probably IPsec or SSL/TLS for confidentiality and data origin authentication.

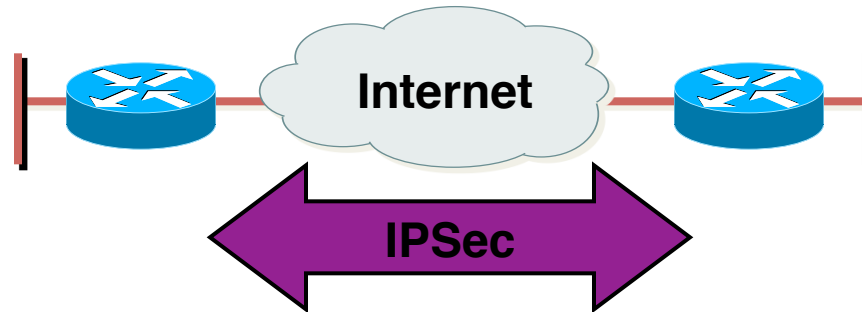
VPN Protocols

- 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 VPN Implementations

- 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

What is IPSec?

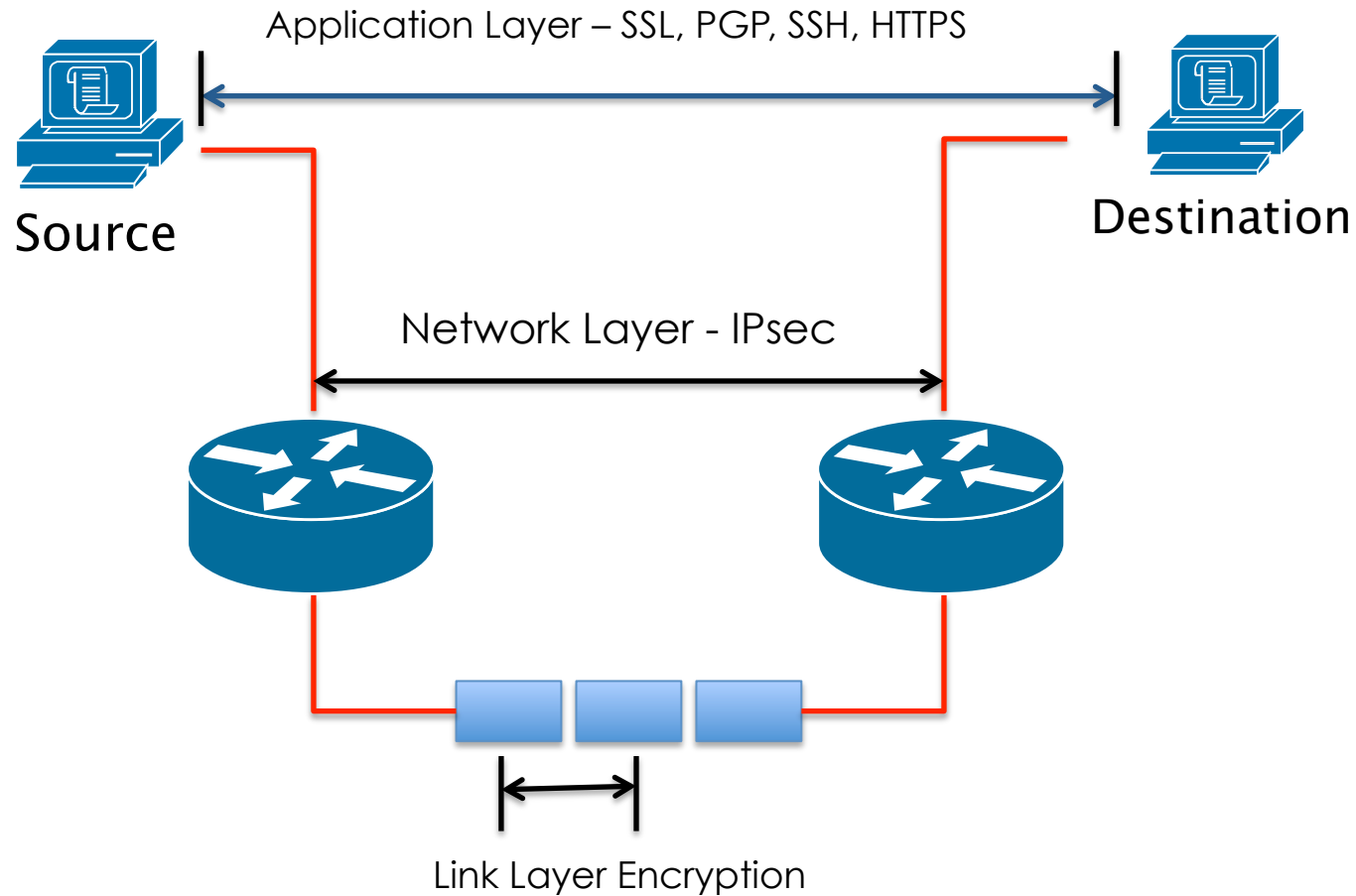


- IETF standard that enables encrypted communication between peers:
 - Consists of open standards for securing private communications
 - Network layer encryption ensuring data confidentiality, integrity, and authentication
 - Scales from small to very large networks

What Does IPsec Provide ?

- Confidentiality - many algorithms to choose from
- Data integrity and source authentication
 - Data “signed” by sender and “signature” verified by the recipient
 - Modification of data can be detected by signature “verification”
 - Because “signature” 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



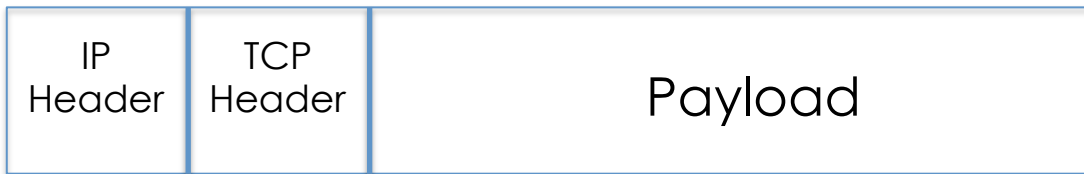
Relevant Standard(s)

- IETF specific
 - rfc2409: IKEv1
 - rfc4301: IPsec Architecture (updated)
 - rfc4303: IPsec ESP (updated)
 - rfc5996: IKEv2 (previously rfc4306 and rfc4718)
 - rfc4945: IPsec PKI Profile
- IPv6 and IPsec
 - rfc4294: IPv6 Node Requirements
 - Rfc4552: Authentication/Confidentiality for OSPFv3
 - rfc4877: Mobile IPv6 Using IPsec (updated)
 - rfc4891: Using IPsec to secure IPv6-in-IPv4 Tunnels

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

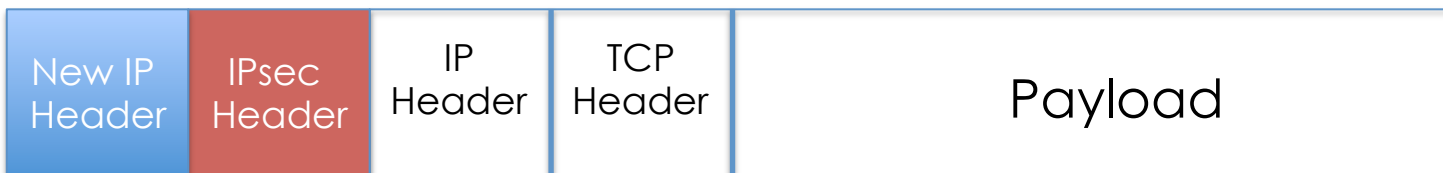
Tunnel vs. Transport Mode IPsec



Without IPsec

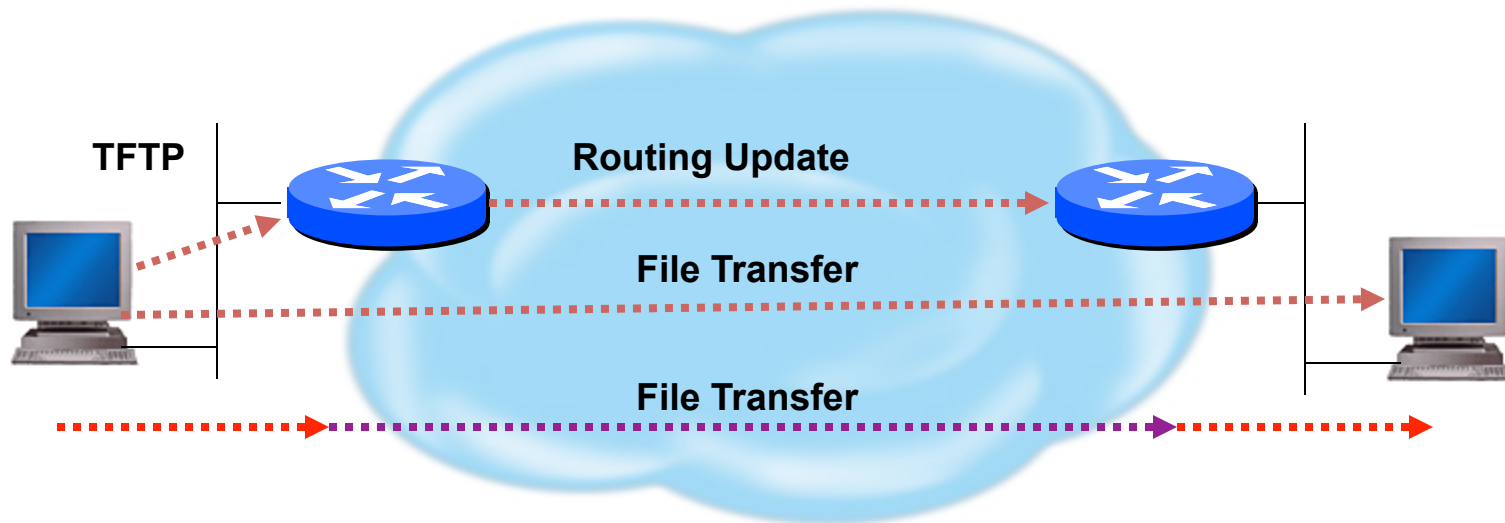


Transport Mode
IPsec



Tunnel Mode
IPsec

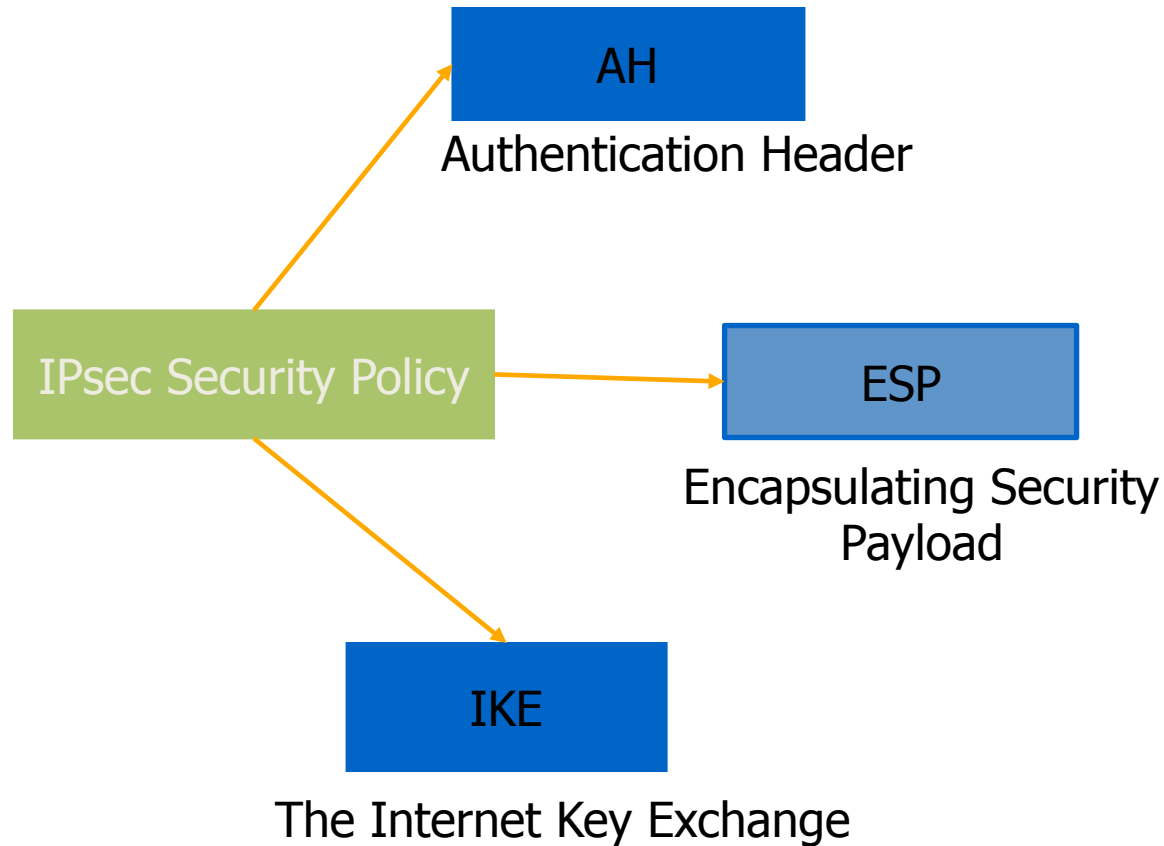
Transport vs Tunnel Mode



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



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

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)

DEPRECATED

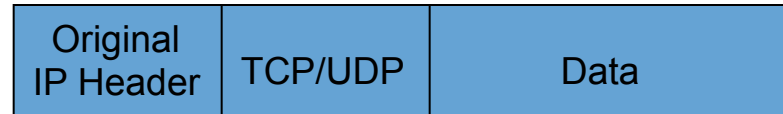
Encapsulating Security Payload (ESP)

- 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

IPv4 IPsec AH

IPv4 AH Transport Mode:

Before
applying AH:



After
applying AH:



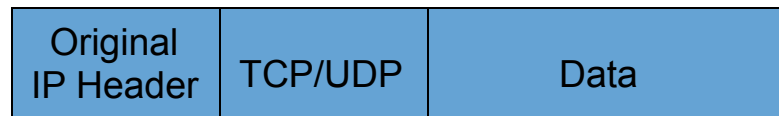
← Authenticated except for
mutable fields in IP header →

Mutable Fields:

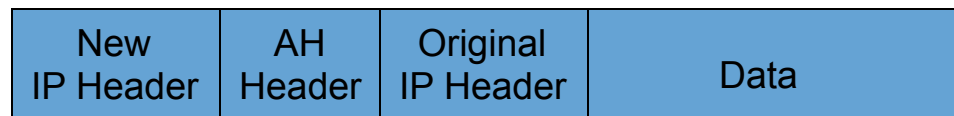
- ToS
- TTL
- Hdr Checksum
- Offset
- Flags

IPv4 AH Tunnel Mode:

Before
applying AH:



After
applying AH:



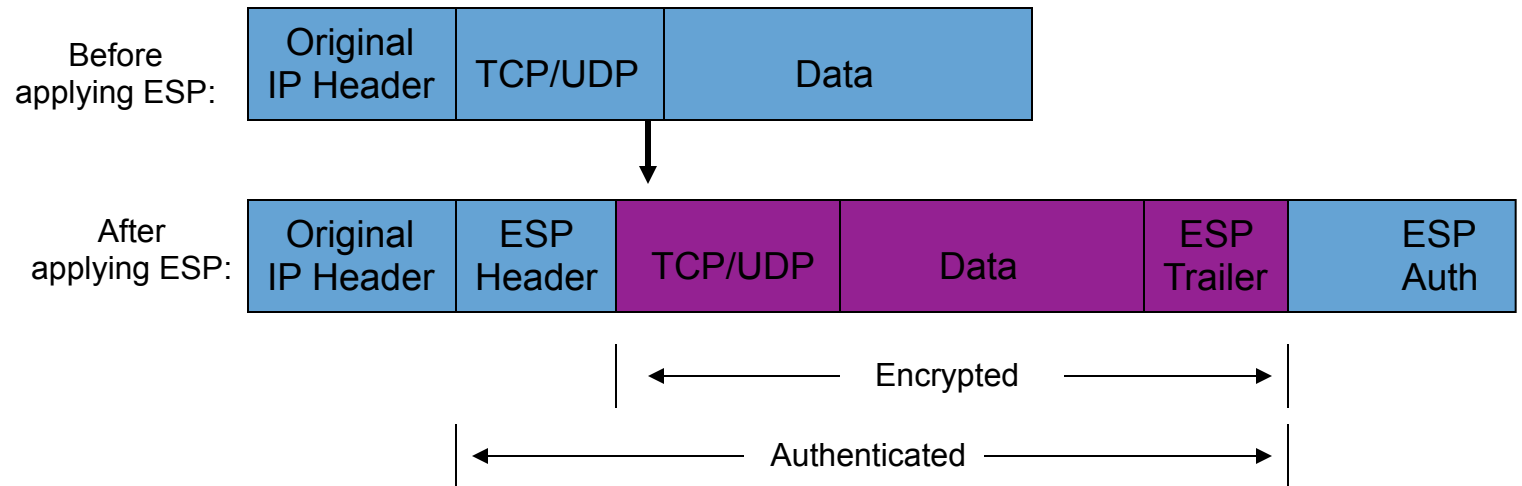
← Authenticated except for
mutable fields in new IP header →

Mutable Fields:

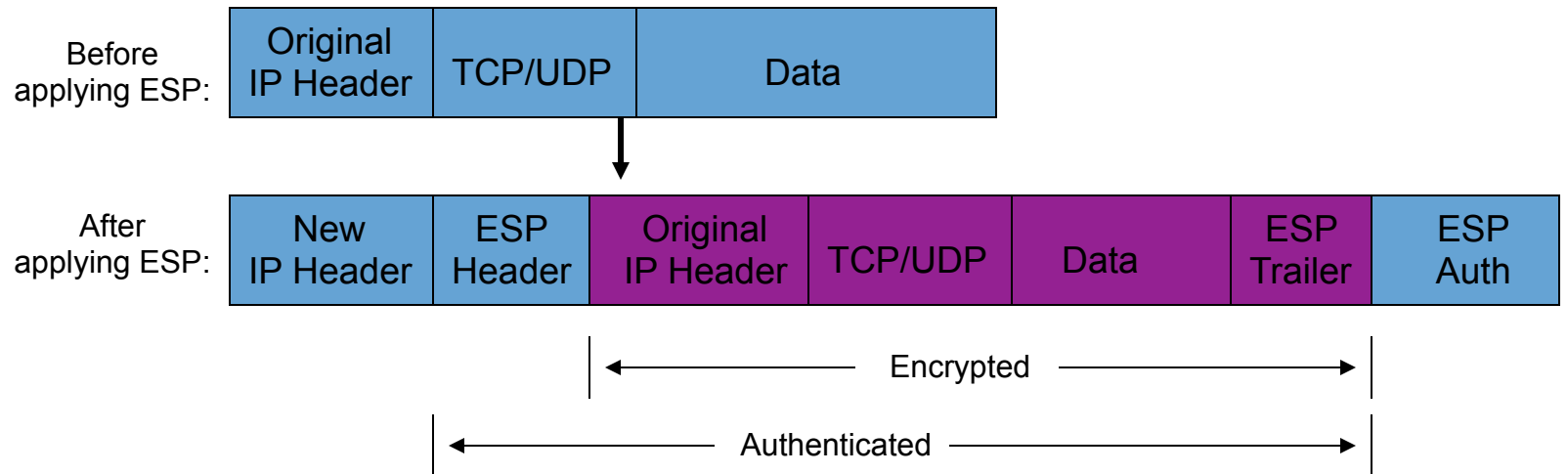
- ToS
- TTL
- Hdr Checksum
- Offset
- Flags

IPv4 IPsec ESP

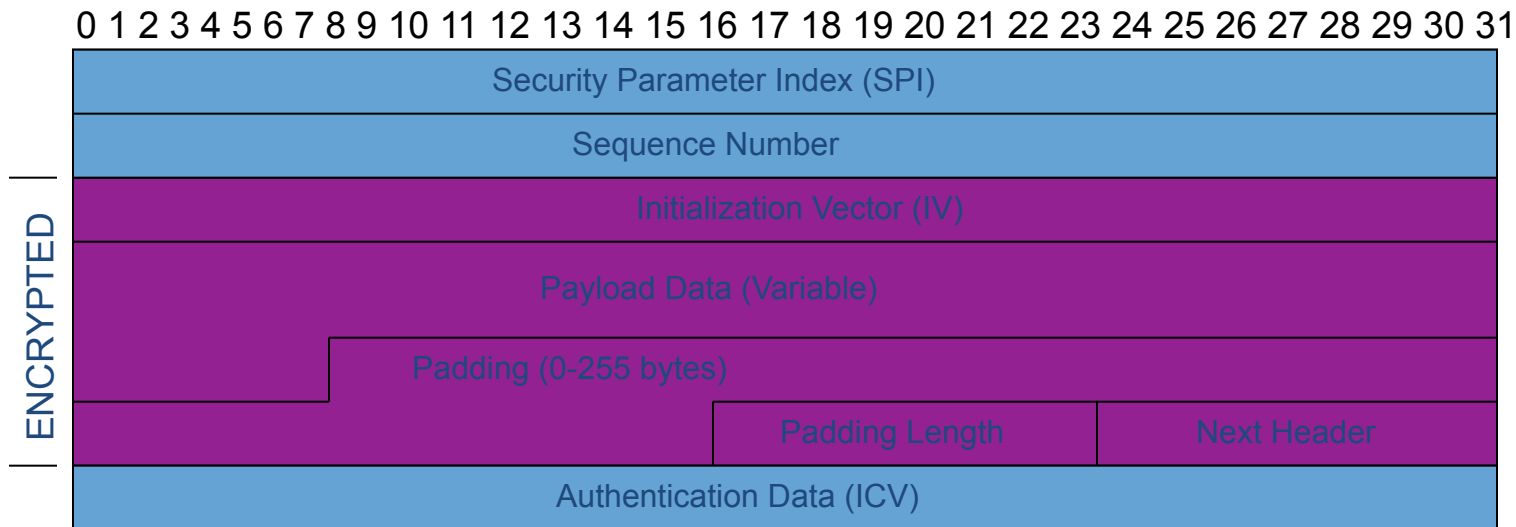
IPv4 ESP Transport Mode:



IPv4 ESP Tunnel Mode:



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
- Auth Data:** ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

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 Diffie-Hellman (DH) key exchange Establish ISAKMP session
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

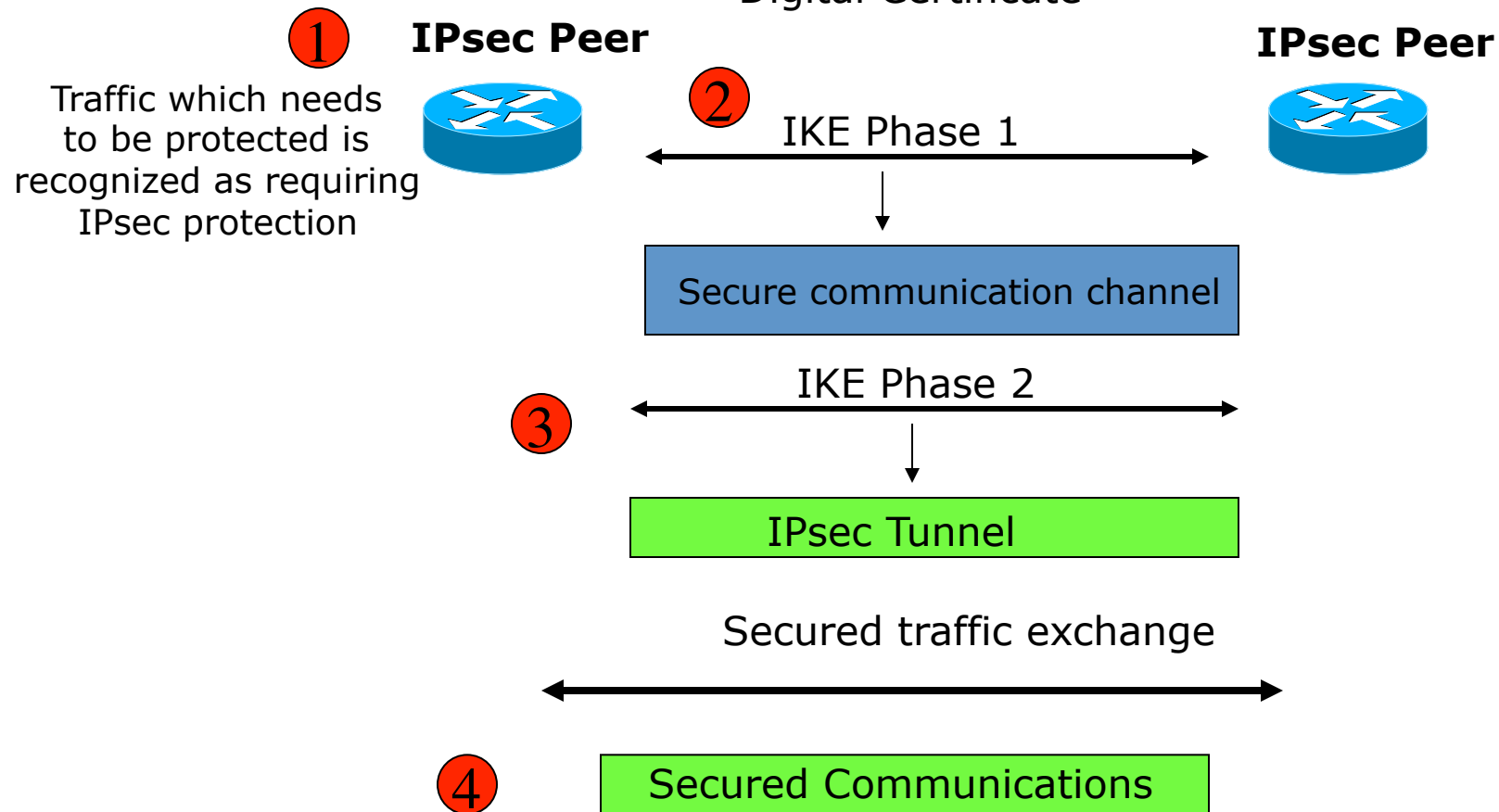
Internet Key Exchange (IKE)

- 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

IPsec with IKE

Peers Authenticate using:

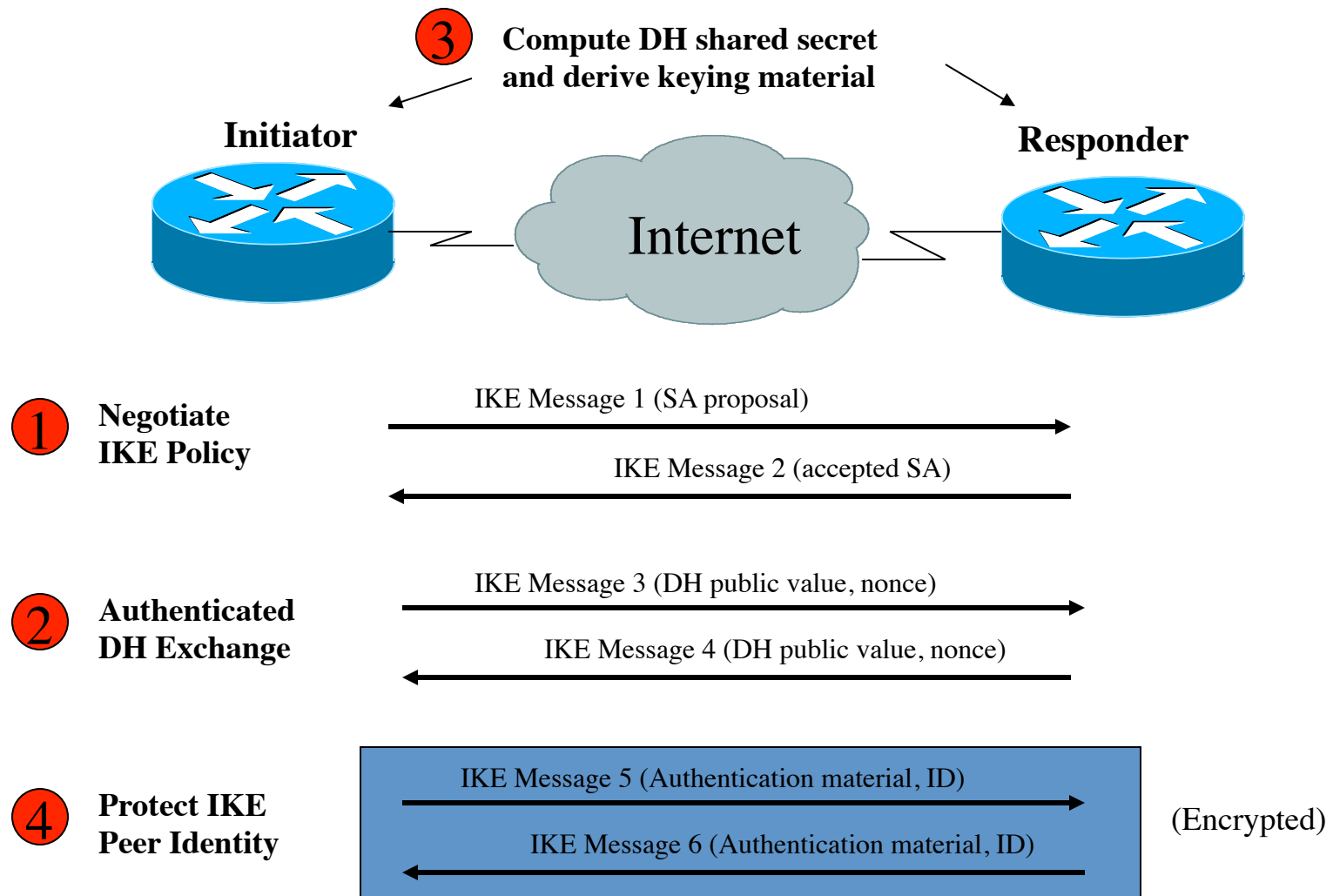
- Pre-shared key
- Digital Certificate



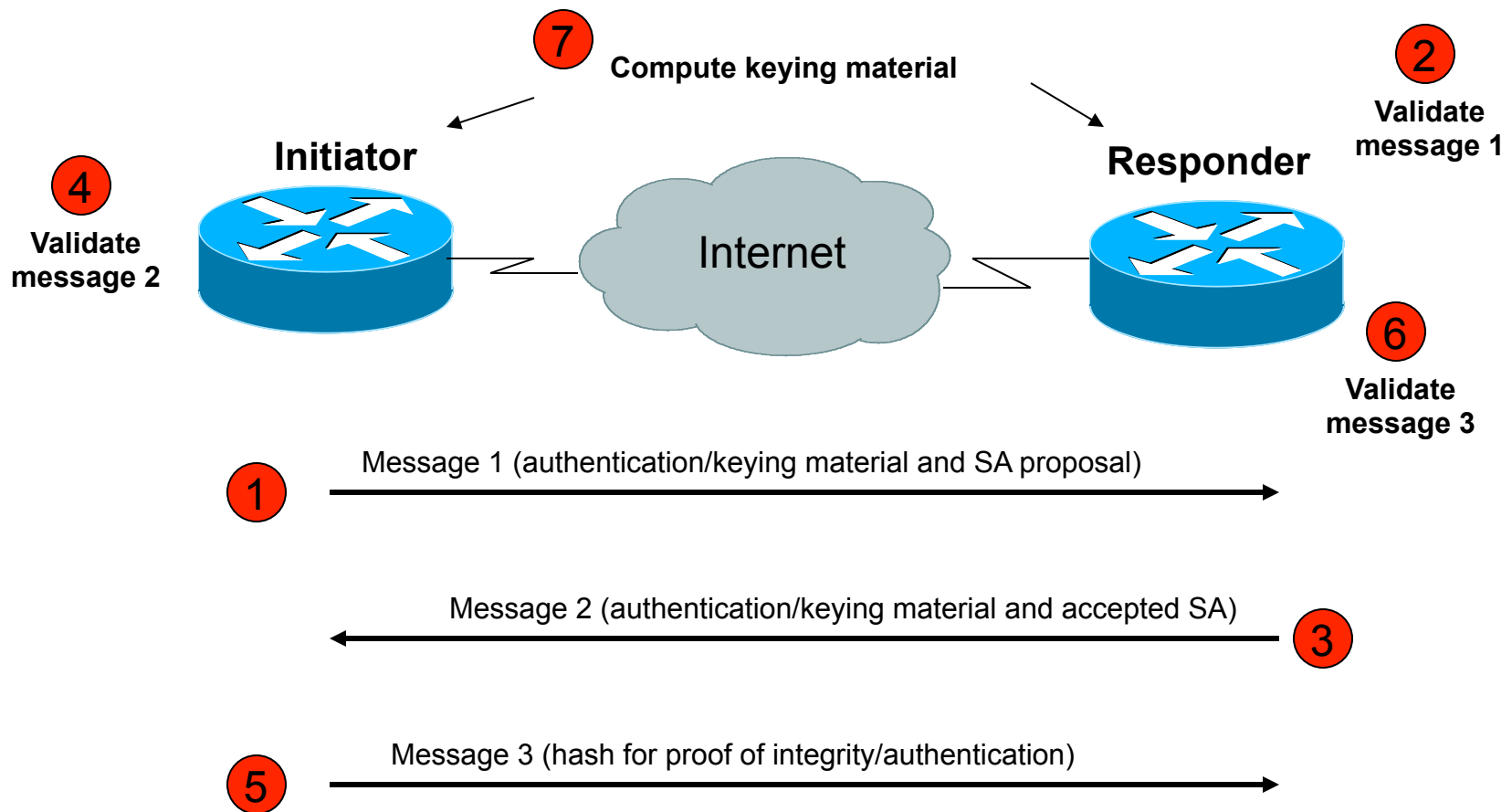
IPsec IKE Phase 1 Uses DH Exchange

- First public key algorithm (1976)
- Diffie Hellman is a key establishment algorithm
 - Two parties in a DF exchange can generate a shared secret
 - There can even be N-party DF changes where N peers can all establish the same secret key
- Diffie Hellman can be done over an insecure channel
- IKE authenticates a Diffie-Hellman exchange
 - Pre-shared secret
 - Nonce (RSA signature)
 - Digital signature

IKE Phase 1 Main Mode



IKE Phase 2 Quick Mode



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

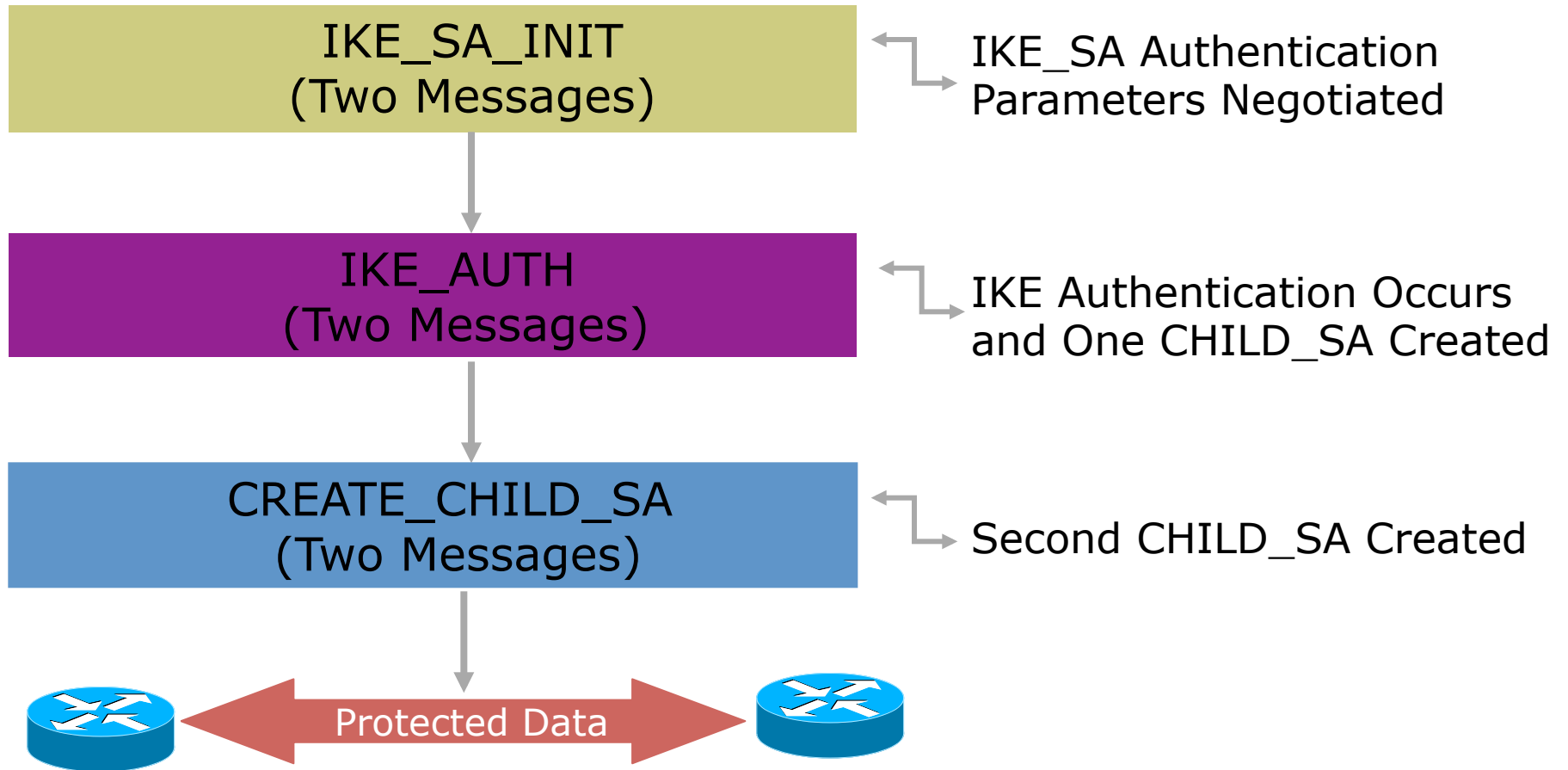
IKE v2: What Is Not Changing

- 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?



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 to determine if ESP-Null vs Encrypted

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)

Sample 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
```

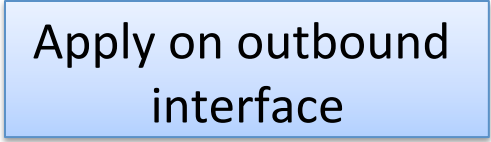
Phase 1 SA

Encryption and
Authentication

Phase 2 SA

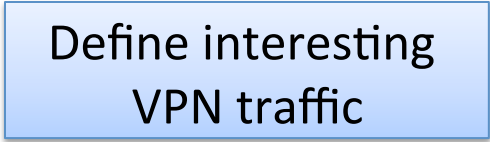
Sample Router Configuration

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



Apply on outbound
interface

```
access-list 101 permit ip  
172.16.16.0 0.0.0.255 172.16.20.0  
0.0.0.255
```



Define interesting
VPN traffic

Capture: Telnet

8	3.113043	Cisco_de:76:91	Spanning-tree-(for-bridges)STP	60	Conf. Root = 32768/1/00:13:80:de:76:80 Cost = 0 Port =
9	3.125855	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
10	3.127649	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
11	3.127651	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=1 Ack=2 Wi
12	3.279317	2001:df0:aa::5	ff02::1:ff00:1	ICMPv6	86 Neighbor Solicitation for 2001:df0:aa::1 from 00:0d:28:49
13	3.328358	192.168.1.1	172.16.2.1	TCP	60 56784 > telnet [ACK] Seq=2 Ack=2 Win=3987 Len=0
14	3.470005	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
15	3.471802	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
16	3.471804	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=2 Ack=3 Wi
17	3.672949	192.168.1.1	172.16.2.1	TCP	60 56784 > telnet [ACK] Seq=3 Ack=3 Win=3986 Len=0
18	3.854380	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
19	3.856188	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
20	3.856190	172.16.2.1	192.168.1.1	TELNET	60 [TCP Retransmission] Telnet Data ...
21	3.978556	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
22	3.980454	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
23	3.980456	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=6 Ack=5 Wi
24	4.099046	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
25	4.100949	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
26	4.100950	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=7 Ack=6 Wi
27	4.243593	192.168.1.1	172.16.2.1	TELNET	60 Telnet Data ...
28	4.245501	172.16.2.1	192.168.1.1	TELNET	60 Telnet Data ...
29	4.245503	172.16.2.1	192.168.1.1	TCP	60 [TCP Keep-Alive] telnet > 56784 [PSH, ACK] Seq=8 Ack=7 Wi

```

Follow TCP Stream
Stream Content
.....!.....P.....
User Access Verification
Password: ..... apn.....apnic2
router2>
router2>
router2>
router2>eenn
% No password set
router2>
router2>
router2>
router2>
router2>
router2>
router2>ssh iipp ??
accounting The active IP accounting database

```

```

router2>ssh iipp ??
accounting The active IP accounting database
admission Network Admission Control information
aliases IP alias table
arp IP ARP table
as-path-access-list List AS path access lists
auth-proxy Authentication Proxy information
bgp BGP information
cache IP fast-switching route cache
casa display casa information
cef Cisco Express Forwarding
ddns Dynamic DNS
dfp DFP information
dhcp Show items in the DHCP database
dvmrp DVMRP information
eigrp IP-EIGRP show commands
extcommunity-list List extended-community list
flow NetFlow switching
helper-address helper-address table
host-list Host list
http HTTP information
igmp IGMP information
inspect CBAC (Context Based Access Control) information
--More--
router2>sh ip .. .. iipp iinnntt.
router2>sh ip interface ??
Async Async interface
BVI Bridge-Group Virtual Interface
CDMA-Ix CDMA Ix interface
CTunnel CTunnel interface
Dialer Dialer interface

```

Capture: Telnet + IPsec

178 67.482083	2001.010.aa.0	192.168.1.100.2	ICMPv6	88 Neighbor Solicitation for 2001.
179 67.594031	192.168.1.1	192.168.1.2	ESP	134 ESP (SPI=0x7ea7f8ed)
180 67.601908	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
181 67.601910	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
182 67.605809	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
183 67.626089	192.168.1.2	192.168.1.1	ESP	134 ESP (SPI=0x742f79b4)
184 67.626091	192.168.1.2	192.168.1.1	ESP	134 ESP (SPI=0x742f79b4)
185 67.627695	192.168.1.2	192.168.1.1	ESP	166 ESP (SPI=0x742f79b4)
186 67.627697	192.168.1.2	192.168.1.1	ESP	166 ESP (SPI=0x742f79b4)
187 67.631728	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
188 67.632884	192.168.1.1	192.168.1.2	ESP	118 ESP (SPI=0x7ea7f8ed)
189 67.751716	192.168.1.1	192.168.1.2	ESP	150 ESP (SPI=0x7ea7f8ed)
190 67.765217	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
191 67.765219	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
192 67.766634	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
193 67.766636	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
194 67.768056	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
195 67.768058	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
196 67.769385	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
197 67.769387	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
198 67.770803	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
199 67.770804	192.168.1.2	192.168.1.1	ESP	118 ESP (SPI=0x742f79b4)
200 67.770805	192.168.1.1	192.168.1.2	ESP	134 ESP (SPI=0x7ea7f8ed)

Thank You. Questions?

