

Confiabilidade de Sistemas Distribuídos Dependable Distributed Systems

DI-FCT-UNL, Henrique Domingos, Nuno Preguiça


Lect. 5 Network Level Security IPSec, VPNs

2015/2016, 2nd SEM

MIEI
Mestrado Integrado em Engenharia Informática

Last lectures (L3, L4):

Fault Tolerance vs. Intrusion Tolerance

- 
- Replication and Consensus
 - BFT, Byzantine Quorums (ex., ABD)
 - BFT, SMR Approach and PAXOS
 - Randomized Consensus (Ben Or)
 - **Other approaches / case-studied later !**
 - Practical implementation
 - **Reliable and Secure Channels**
 - **Authentication (messages and participants)**
 - Secure Hash Functions or Symmetric Crypto Primitives: Can use MACs, HMACs, CMACs and secret-sharing
 - Digital signatures (Public Key Methods, PK Certificates, PKIs or CAs)
 - Possible Hybrid approaches

So... we have a combination of techniques usable for Dependable Distributed Systems

- Protection of communications
 - Secure Channels
- Orthogonal solutions to establish secure channels
 - **Transport / Session Level: TLS (SSL)**
 - **Network Level: IPSec, Secure VPNs**

Today: IPSec and Secure VPNs

- IPSec - solution for secure channel abstraction (at network-level, TCP/IP stack)
 - Can use TCP above for reliability
 - Or any other protocol above IP ... transparently
- VPN: Virtually, support for transparent remote access to a remote network
 - Virtually, the host will be “located” as a node in the remote network (as an IP node)

Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

Outline



- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

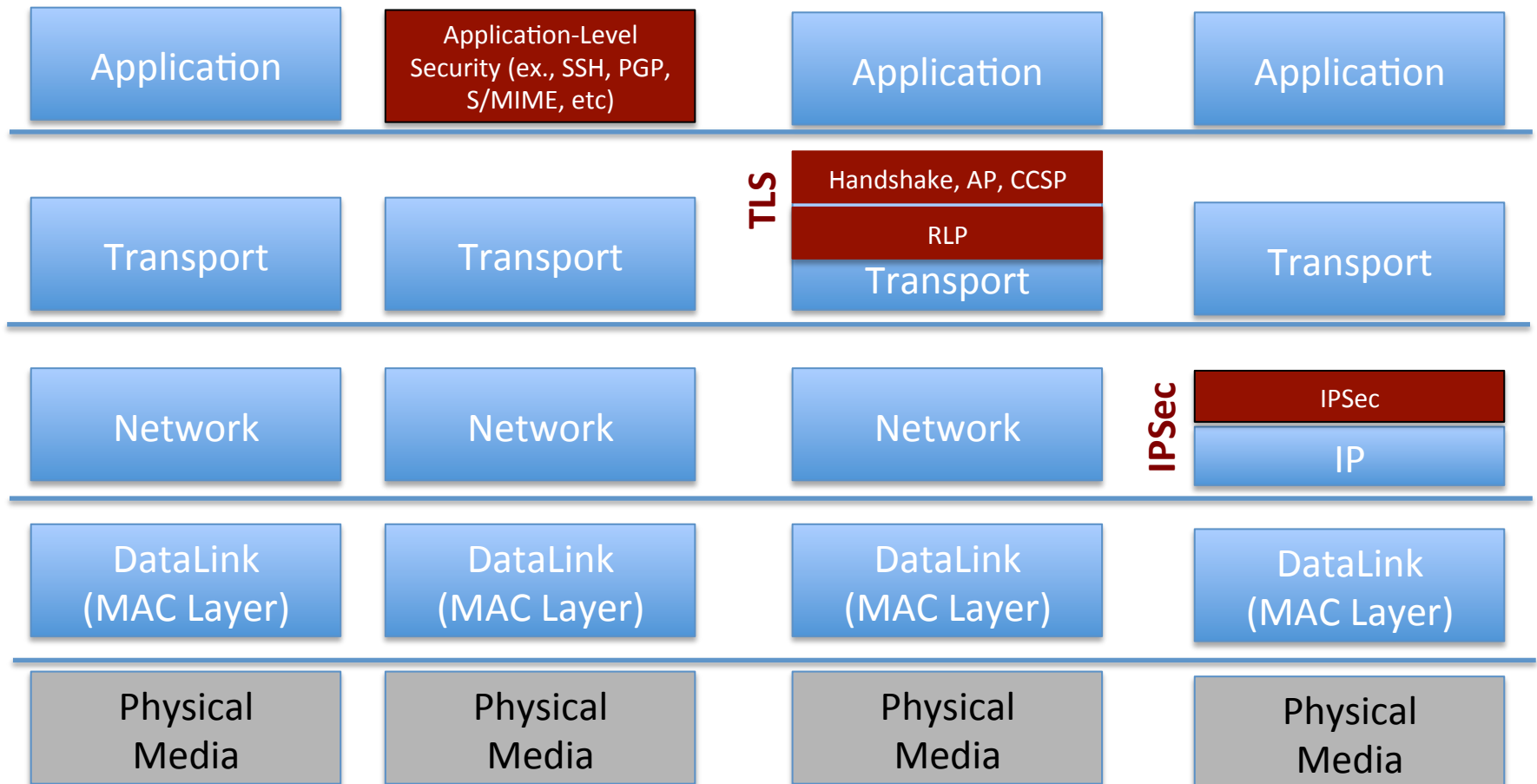
IP Security

- Network Security Layer: security subjacent to any other protocol level in the stack
 - A range of application specific security or security transport services (eg. S/MIME, PGP, Kerberos, SET, SSH, SSL, HTTPS/SSL)
- What about security concerns that “cut across” protocol layers
- Would like security implemented by the network for all applications
 - Advantages ? Drawbacks ?

“If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.”

—The Art of War, Sun Tzu

IP Security and TCP/IP Stack



Motivation for VPN (1)

- Companies, research institutions, and government organizations have long maintained **private networks** between central offices and branch offices.
- Employees/contractors **want to work securely from home or external offices, accessing to central offices**. Road warriors, all the way from salesmen to CEO's, want to be mobile and connect to the home office for whatever purpose.
- There are fast, cheap, and plentiful connections to the Internet to be had in locations as varied as libraries, airports, and Starbucks.
- How do you go about securing what is basically an unsecured medium?
 - Provided by IPSec Tunneling

Motivation for VPN (2)

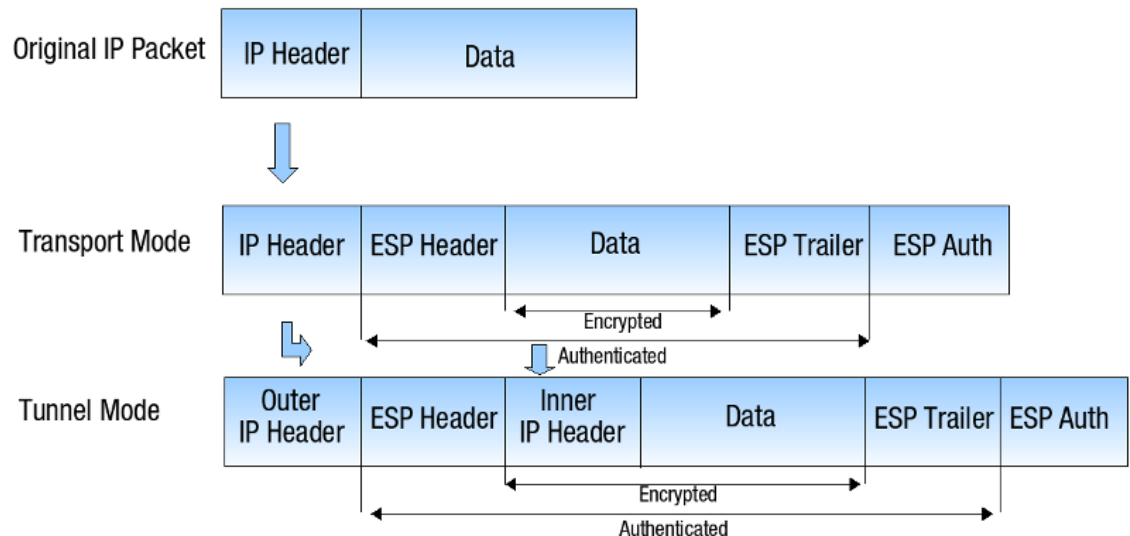
- VPNs (Virtual Private Networks) provide secure tunneling of communications over “insecure networks”.
 - Secure Tunneling over the Internet (Public IP, ISP provided IP)
 - Where “physical” private networks existed, VPNs are becoming today a commonplace
 - not only among “road warriors”, “branch offices”, and “central offices”
 - also “business-to-business partners” exchanging data through a secure tunnel wrapped around the communications traffic.

VPN Topologies and VPN Tunneling Technologies

- VPN Topologies:
 - Network-to-Network
 - Host-to-Network
 - Host-to-Host

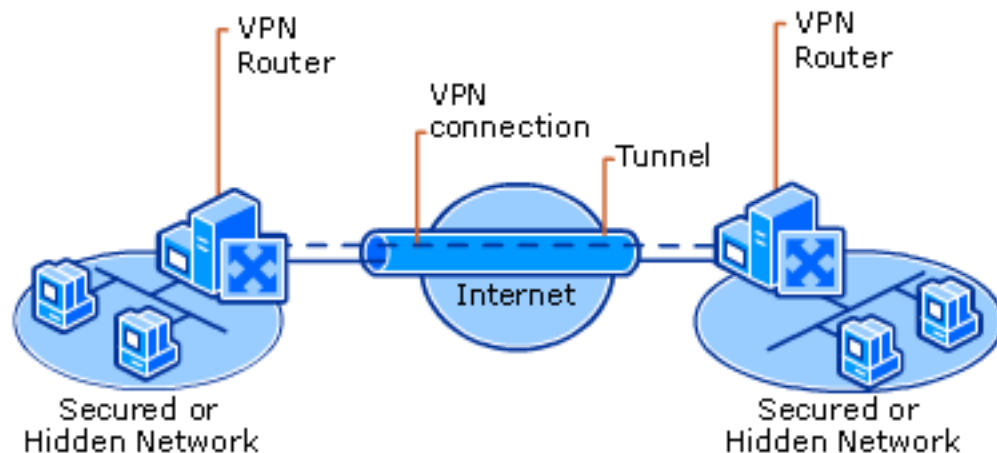
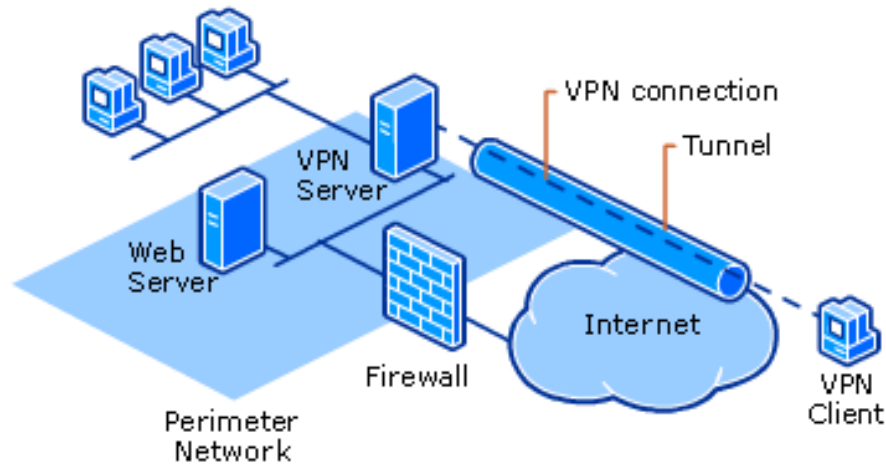
- Tunneling Technologies:

- PPTP
- L2TP
- SSL
- **IPSec**



Encapsulation

VPN Examples



VPN Support ...

- FreeS/WAN used to be the only IPSec game in town as far as Linux was concerned.
- With the advent of the 2.6 kernel series, there is now integrated support for IPSec in the kernel in addition to the survivor of FreeS/WAN, OpenSWAN.
- Also MAC-OS-X Support ...
 - <https://www.strongswan.org>
 - http://www.thegreenbow.com/doc/tgbvpn_cg_Linux_en.pdf

Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes



IP Security

- Principals as “IP endpoints”: designed entities
- Generic IP Security services (IP Protocol Level) providing security services:
 - Access-Control, Authentication, Confidentiality and Integrity
 - Key management and establishment services
- Applicable to use over LANs, across public & private WANs, & for the Internet
- Standard covering identified flaws, vulnerabilities and attacks (initially reported in 1994 IETF report)
- IPSec scope:
 - IPV4 compatibility
 - IPV6 Native Security

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication (IP Authentication) of IP packets (*)
- Anti-Replaying Protection: Rejection of replayed packets
 - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality
- Key-Establishment Services

* Remember security services: Helps in securing routing, but no routing control: different routing attacks require other contra-measures complementarily to IPSec

IP Security and TCP/IP Stack

IPSec Stack:

AH (Authentication Header) Protocol

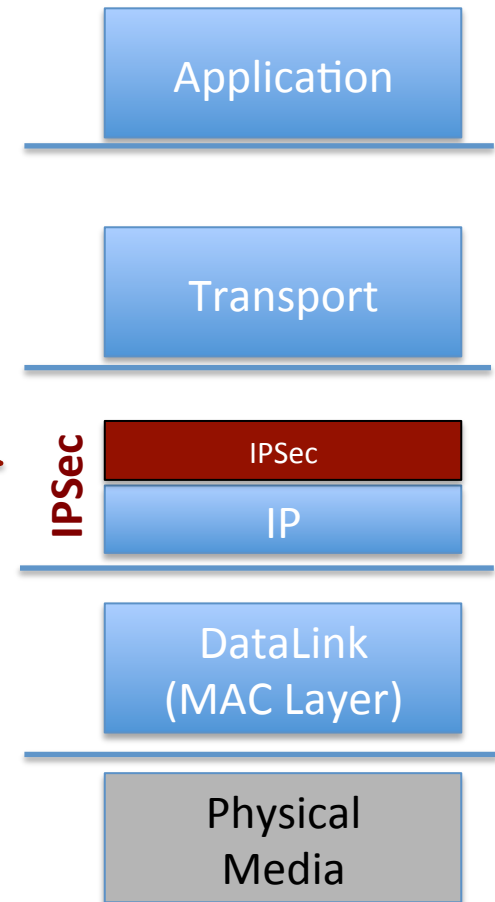
ESP (**E-O** or Encryption Only)

ESP (**E-A** or Encryption and Authentication)

+

Oakley/ISAKMP:

Establishment of Security IPSec Associations



IPSec protocol suite

Only protection against communication attacks (no intrusion adversary models)

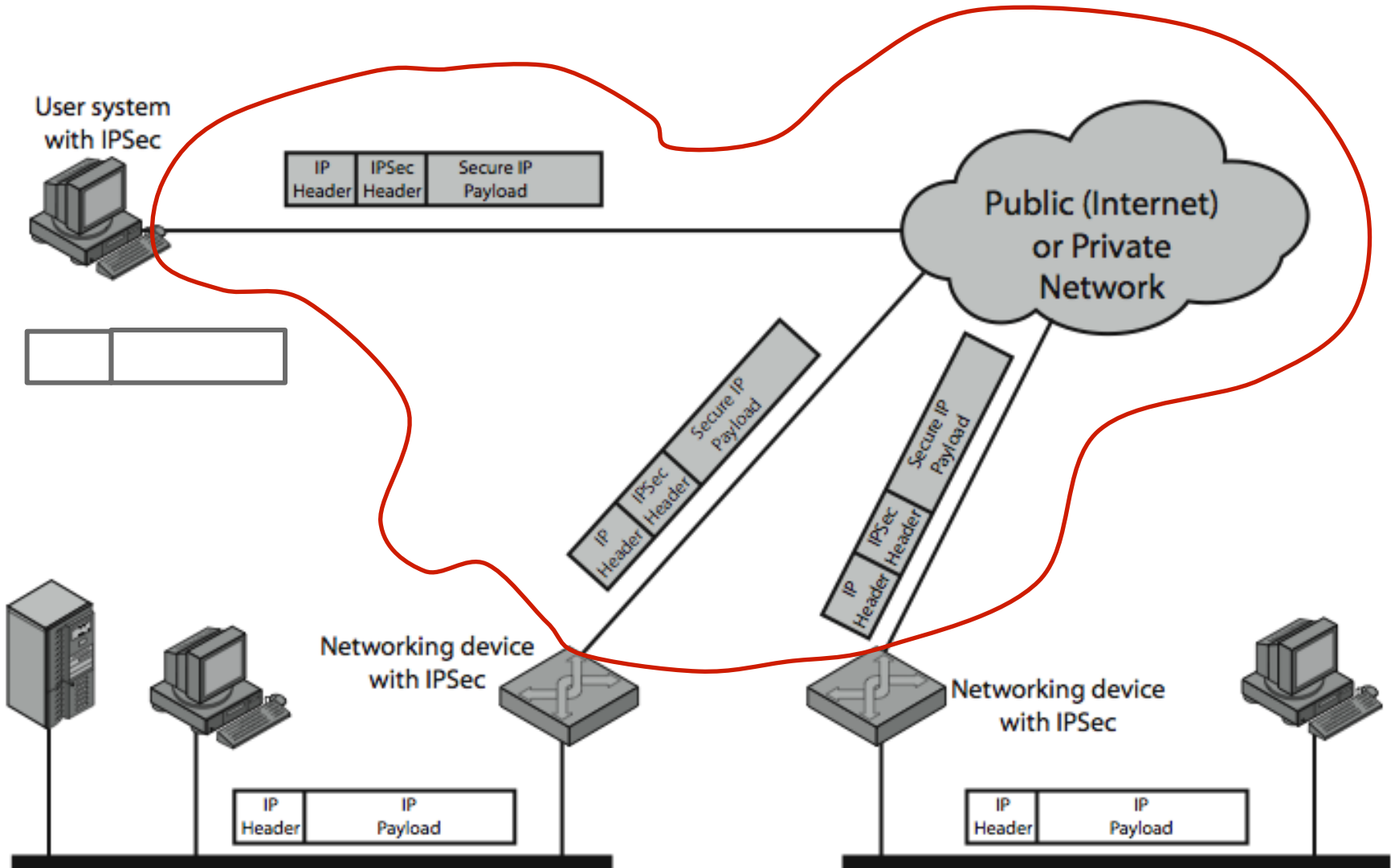
> Ex., remember ref. X.800 or RFC 2828

	AH	ESP (E-Only)	ESP (A+E)
• Access control – AC or IP packet admission	X	X	X
• Connectionless integrity	X		X
• Authentication (Origin) (authentication of the IP packet origin)	X		X
• <i>Anti-replay</i> (IP packet replay) (<i>Form of Sequential integrity</i>)	X	X	X
• Data Confidentiality		X	X
• Traffic-Flow confidentiality		X	X
• Availability (DoS, DDoS)	?	?	?
• Routing control (IP routing control)	?	?	?

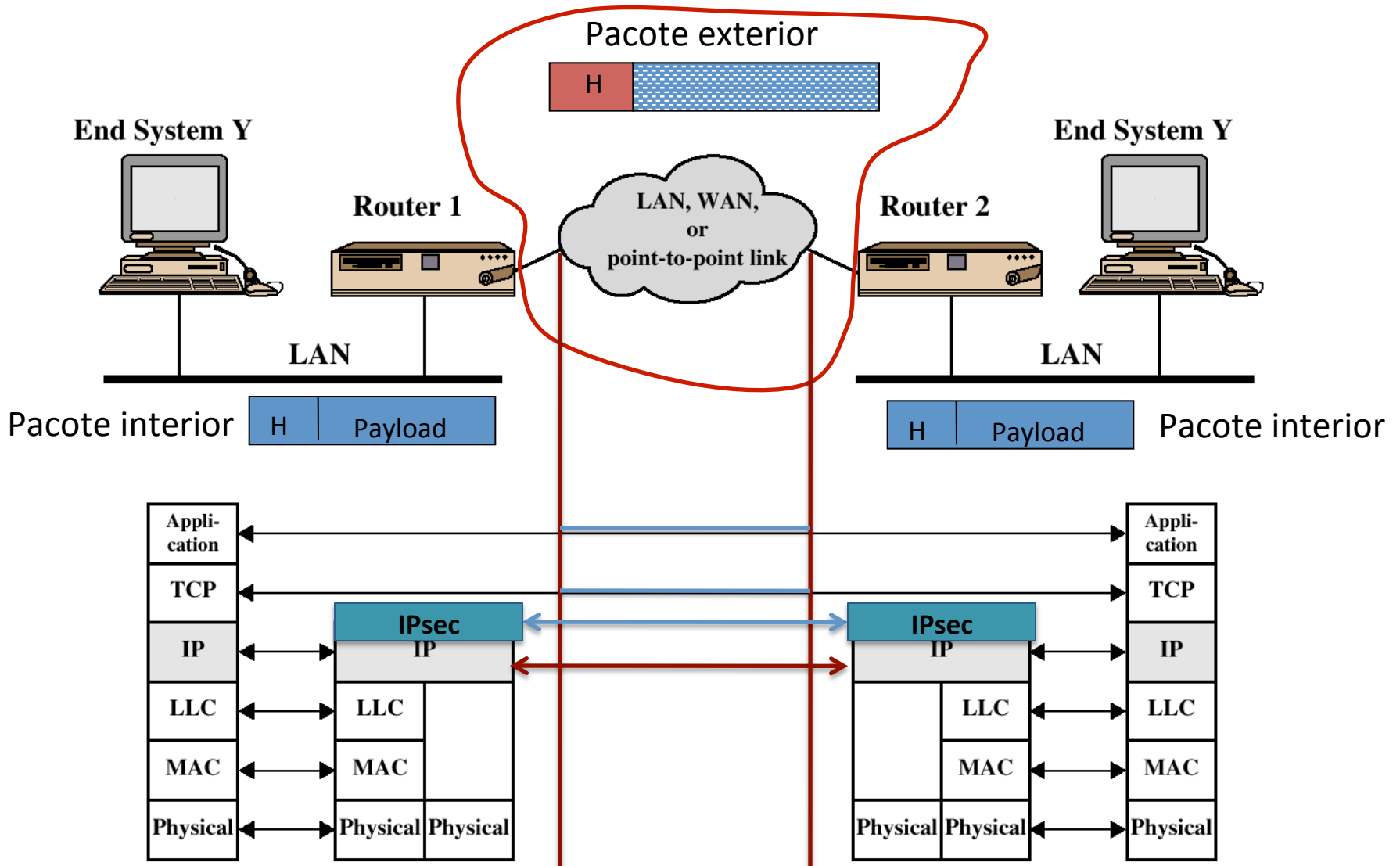
IPSec uses

- **Secure branch office connectivity** over the internet
- **In general, secure LAN-to-LAN connectivity**, as a “secure overlay solution” supported over public IP internetworking infrastructures, public IP networks (WAN scale) or Internet
- **Secure VPNs** (on top of NAT-based IP internetworking)
- **Secure Remote Transparent Access** of users to their Private Networks
- **Secure Extranet/Intranet Solution** for Private Networks or Secure Interconnection of Private Corporate Networks (inside an organization or partners)
- **Enhancing Electronic Commerce Security** (or, in general, internetworked applications, secure transactions and multi-party environments)

IPSec scenario




Secure LAN to LAN



Benefits of IPSec

- In a firewall/router:
 - provides strong security to all traffic crossing the perimeter (perimeter protection strategy)
 - Resistant to bypass
 - NAT is naturally supported
- Protection below transport layer, hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users
- Helps in securing routing architecture
 - Protection of router advertisements, authentication/authorization of advertisements, control of authenticated/authorized neighbours, authentication of redirections, countermeasures against forged update announcements

Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
-  – IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

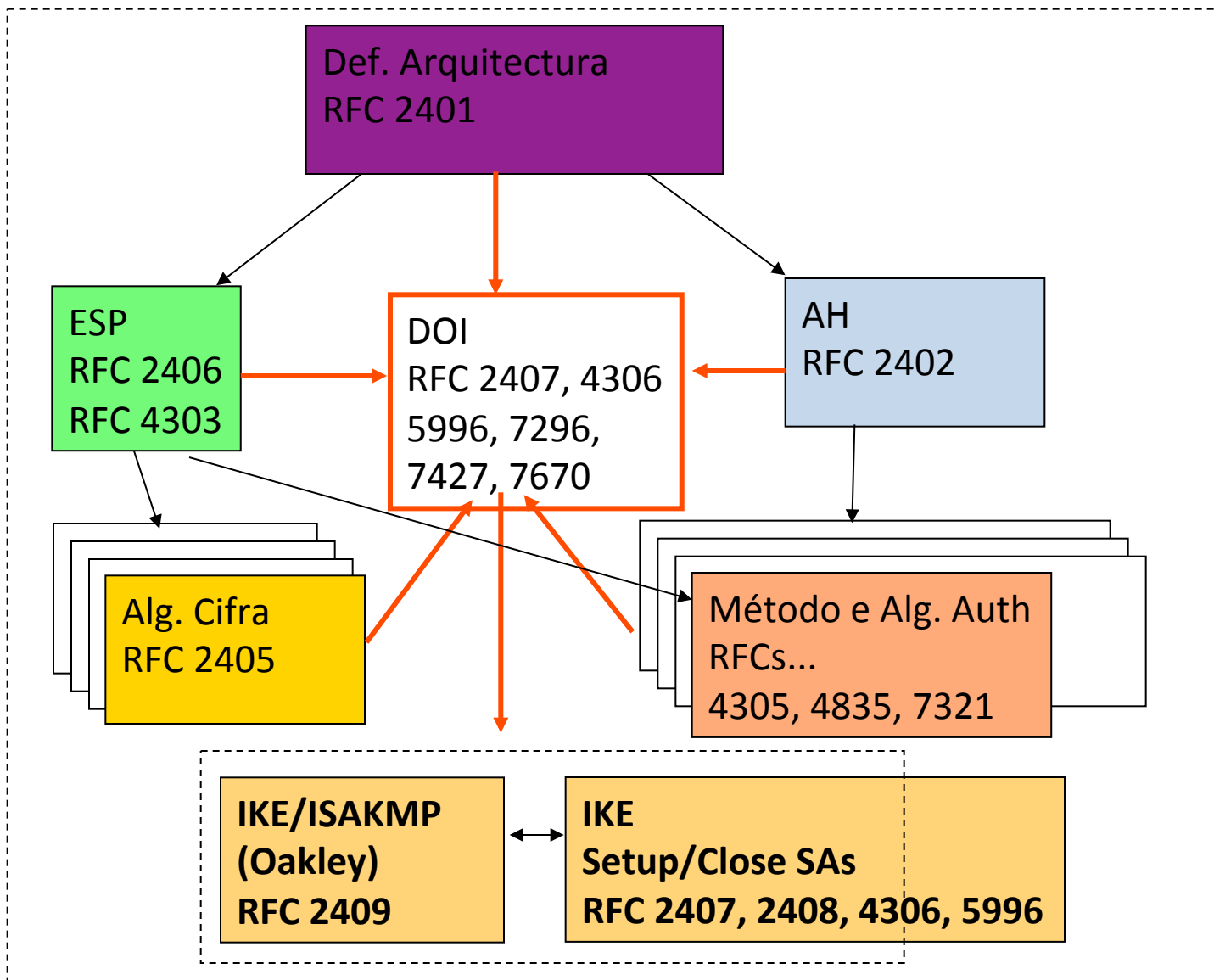
IP Security Architecture

Standard suite and documentation


- Specification quite complex and extensive, with groups of specific documents (standards):
 - Architecture
 - RFC4301 (2005) *Security Architecture for Internet Protocol*
 - Updated: RFCs 6040, (2010) 7619 (2015)
 - Authentication Header (AH)
 - RFC4302 (2005) *IP Authentication Header*
 - Encapsulating Security Payload (ESP)
 - RFC4303 (2005) *IP Encapsulating Security Payload (ESP)*
 - Internet Key Exchange (IKE)
 - RFC7296 (2014) *Internet Key Exchange (IKEv2) Protocol*
 - Updated: RFC7427 (2015), RFC 7670 (2016)
 - Cryptographic algorithms (IPSec standardized crypto-suites used in above IPSec protocols)
 - Others (security policy, MIB, ...)

IPSec standardization (IETF IPsec WGs)

Contexto do RFC 2411, 4306, 5996

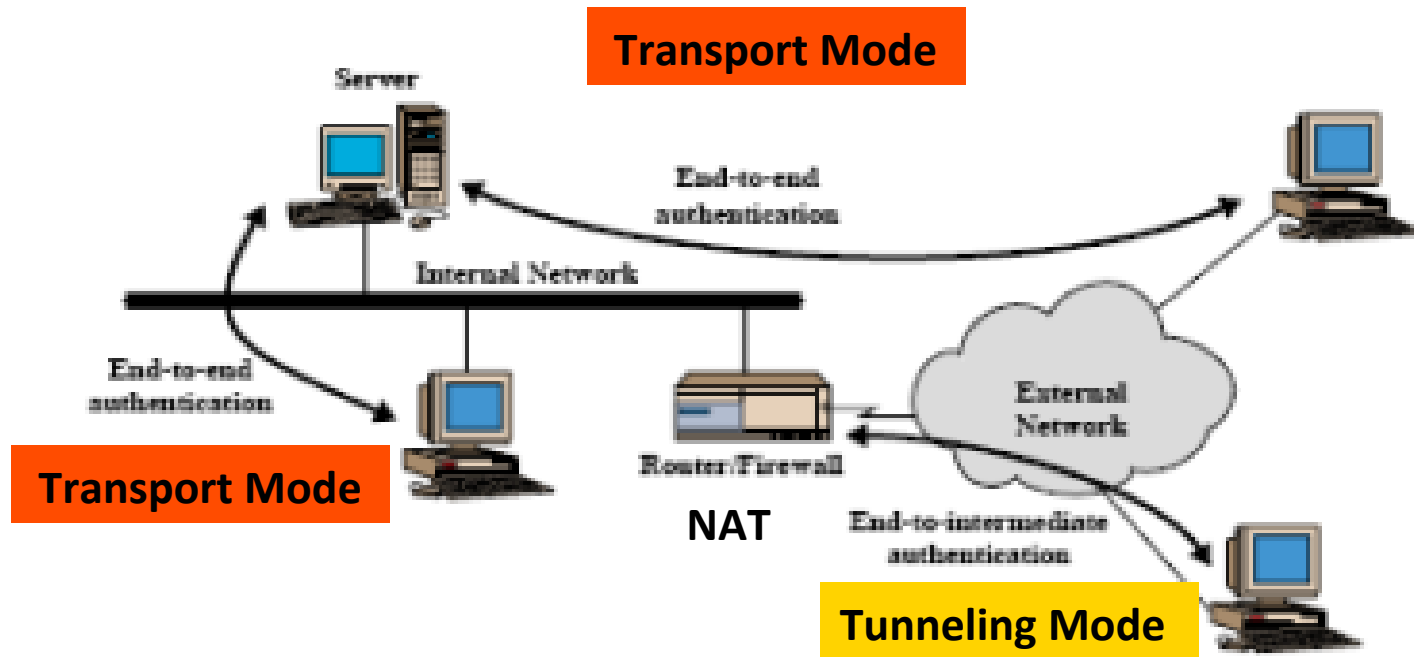


Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
-  – IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

IPSec modes

Modes are considered for different IPSec uses

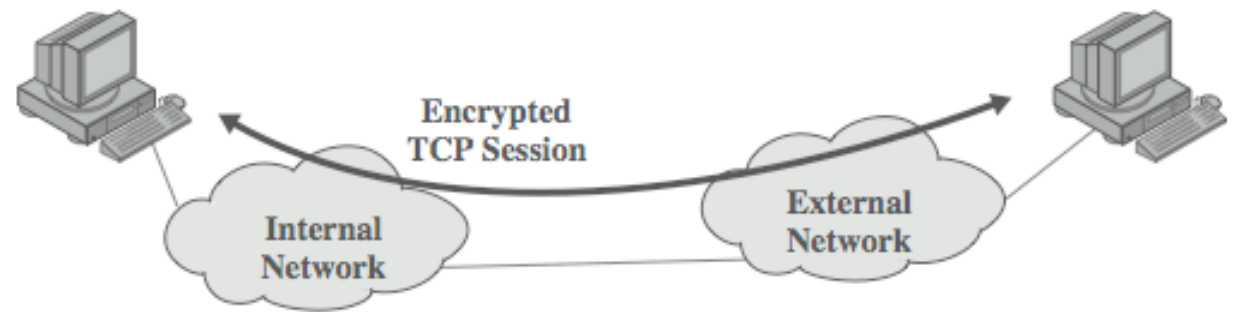


Transport Mode: End-to-End Security (Host-to-Host)

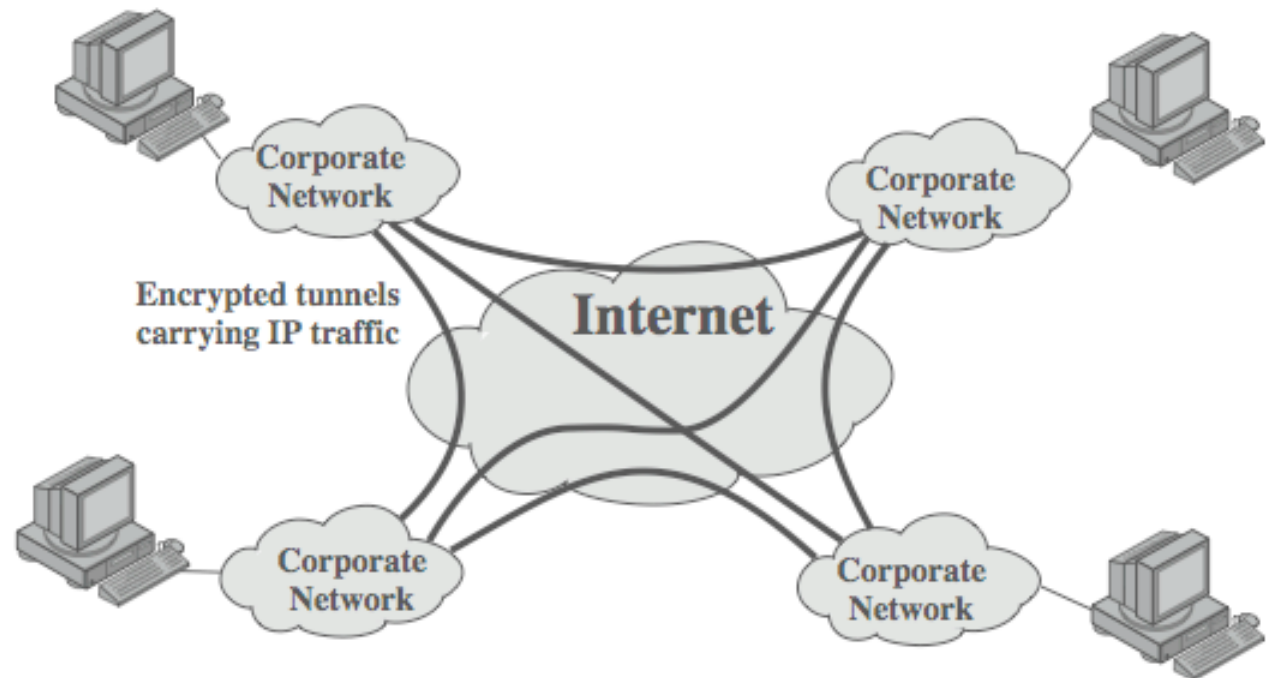
Tunnel Mode: Intermediary-Support (routers, firewalls)

Transport and Tunnel Modes

- Transport Mode, used ...
 - For End-to-End IP Protection, ex., Client/Server, PeerHost-to-PeerHost
 - To encrypt & optionally authenticate IP data (payload)
 - Can do traffic analysis but is efficient
 - Particular use for ESP “host to host” traffic, end-to-end
- Tunnel Mode
 - Encrypts entire IP packet
 - Add new header for next hop
 - No routers on way can examine inner IP header
 - Note: what about “covert channels” control, “non-controlled doors for malicious software entry points, ... ?
 - Particularly good for VPNs, gateway-to-gateway security



(a) Transport-level security



(b) A virtual private network via Tunnel Mode

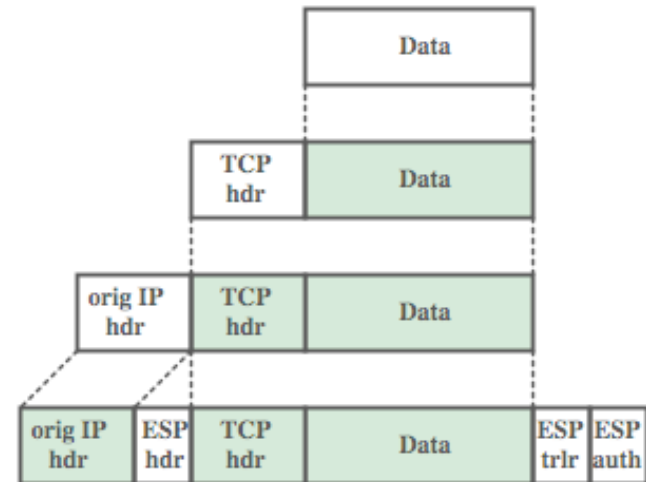
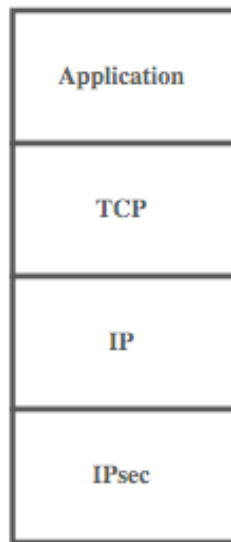
Transport and Tunnel Modes

Transport and Tunnel vs. AH and ESP

- Combinations provide 6 different base security behaviors

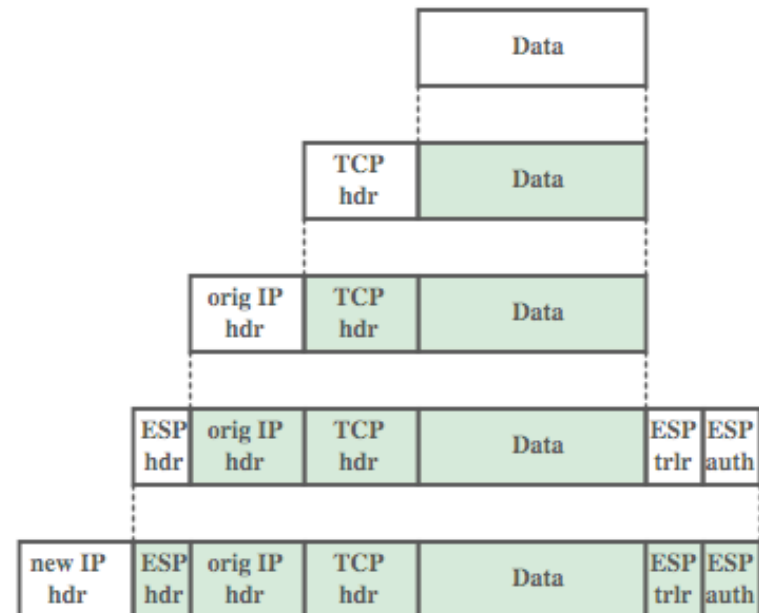
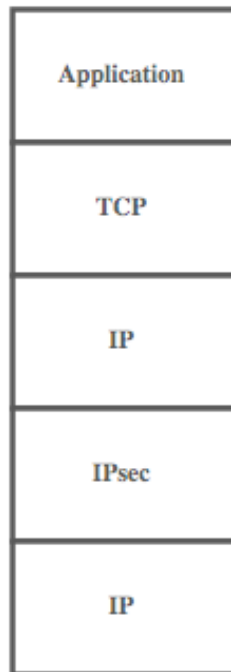
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

TCP/IP stack encapsulation




(a) Transport mode

Transport and Tunnel Mode Protocols



(b) Tunnel mode

Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
-  – IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

SADs, SPDs, and SAs

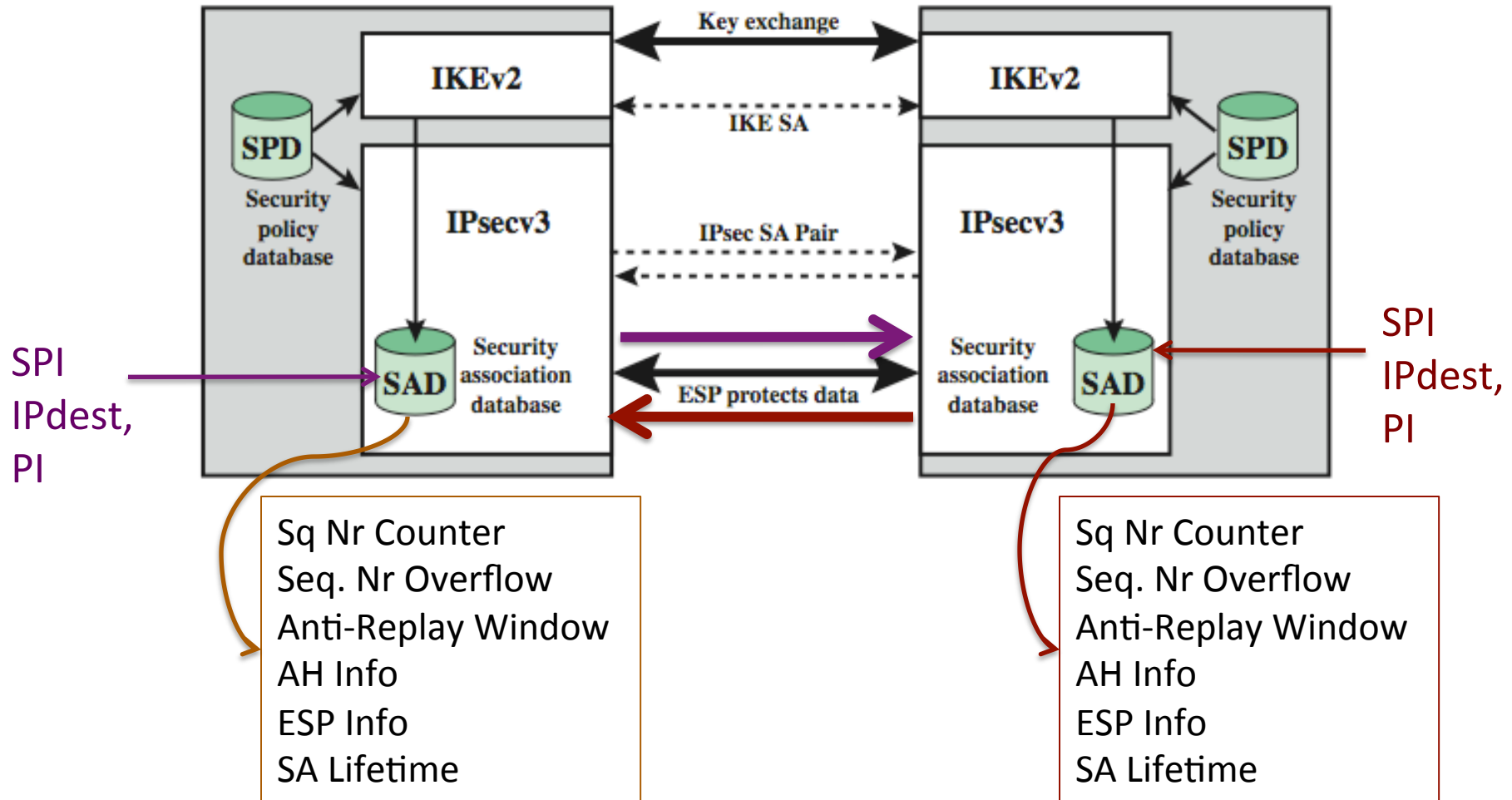
- IPSec policy: determined by the information managed in a persistent **SAD (Security Association Database)** and **SPD (Security Policy Database)**
- A **SAD** has **SAs (Security Associations)** as entries
- Each SAD entry corresponds to a SPD entry
 - In the SPD, the IPSec policies for each Security Association are established
 - Different SAs may share the same policy

Security Associations

- In IPSec there is a “**one-way relationship**” between sender & receiver that affords security for traffic flow: described in the respective security association (SA)
- An SA is defined by 3 parameters:
 - Security Parameters Index (SPI)
 - Identifier travelling in the IPSec packet headers
 - IP Destination Address (DEST IP)
 - Security Protocol Identifier (sPID)
- Has a number of other parameters
 - Seq nr., AH & ESP info, SA lifetime (or SA-TTL), etc...
- SPD in the “local database” of Security Associations is managed autonomously in each endpoint

IPSec security policy management

- IPSec architecture with SPD and SAD management

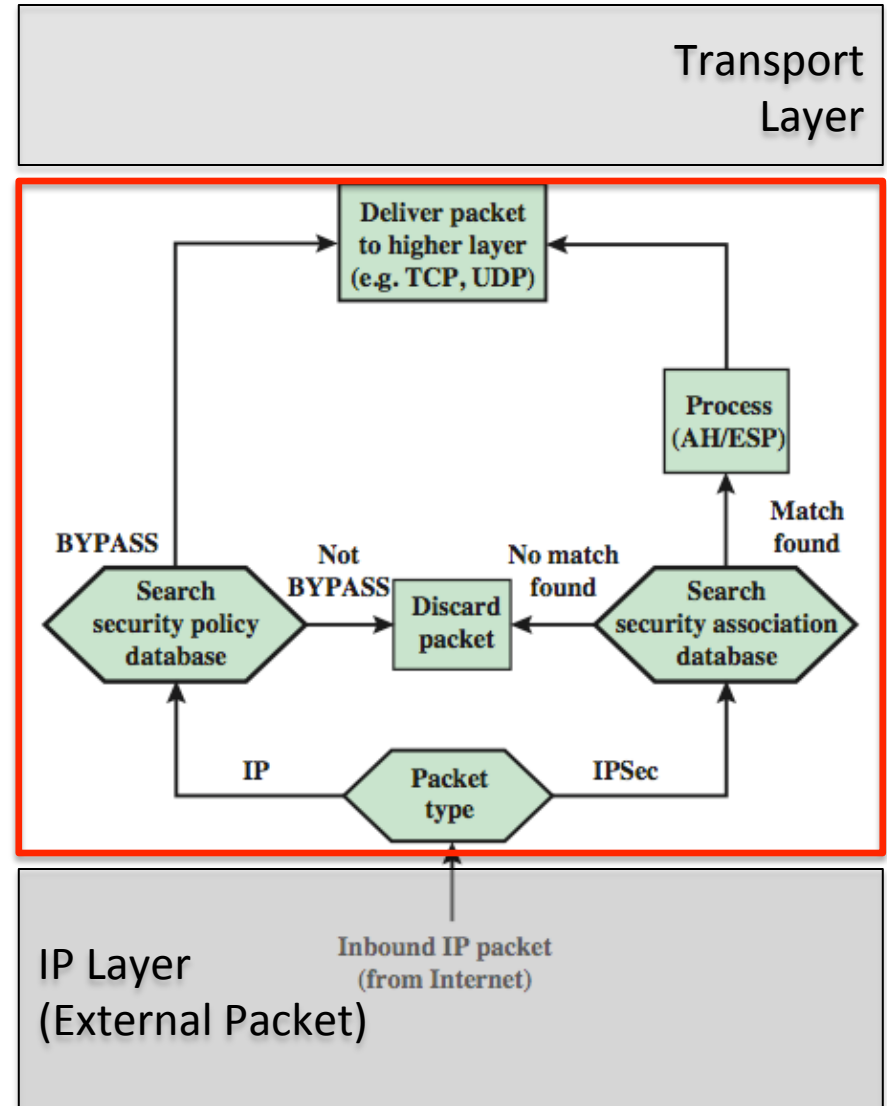
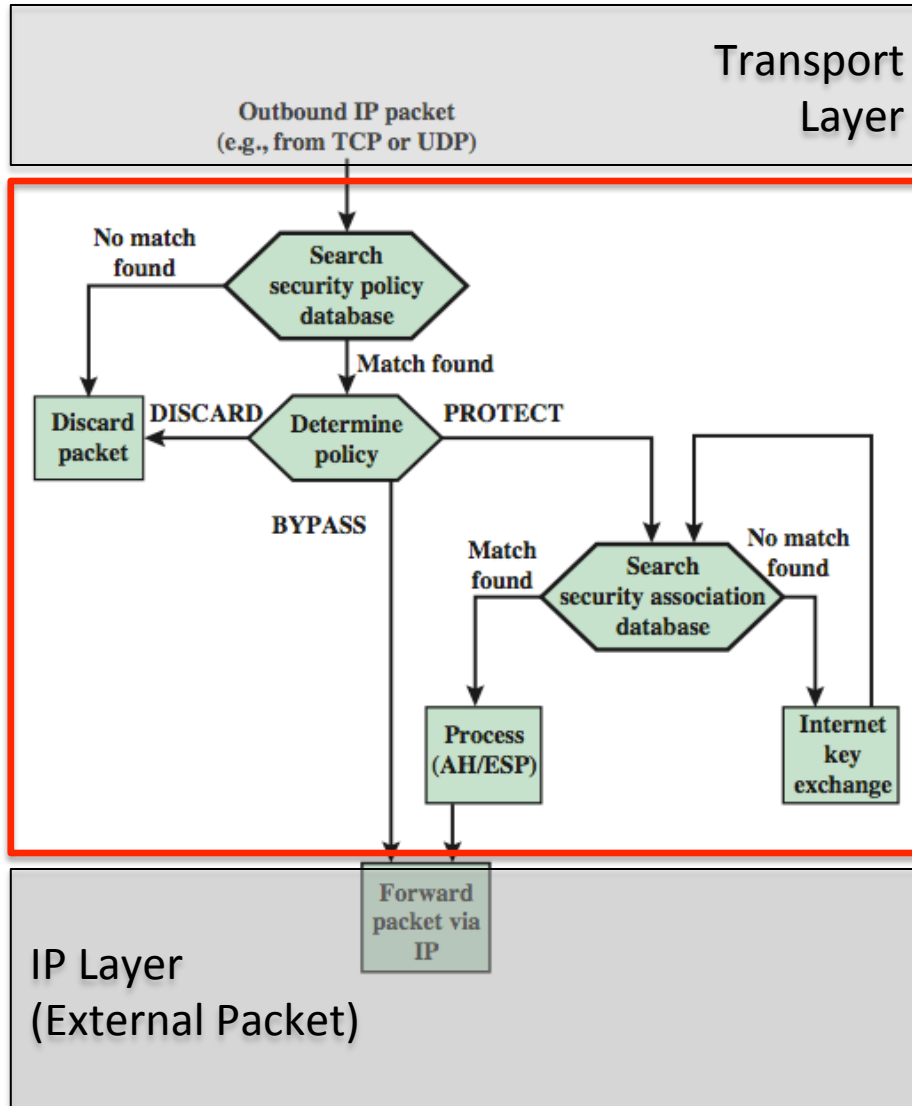


Security Policy Database


- Relates IP traffic to specific SAs
 - Match subset of IP traffic to relevant SA
 - Use selectors to filter outgoing traffic to map
 - Different selectors can be used (see bibliography)
 - Based on: local & remote IP addresses, next layer protocol, name, local & remote ports

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

IPSec packets processing



Outline

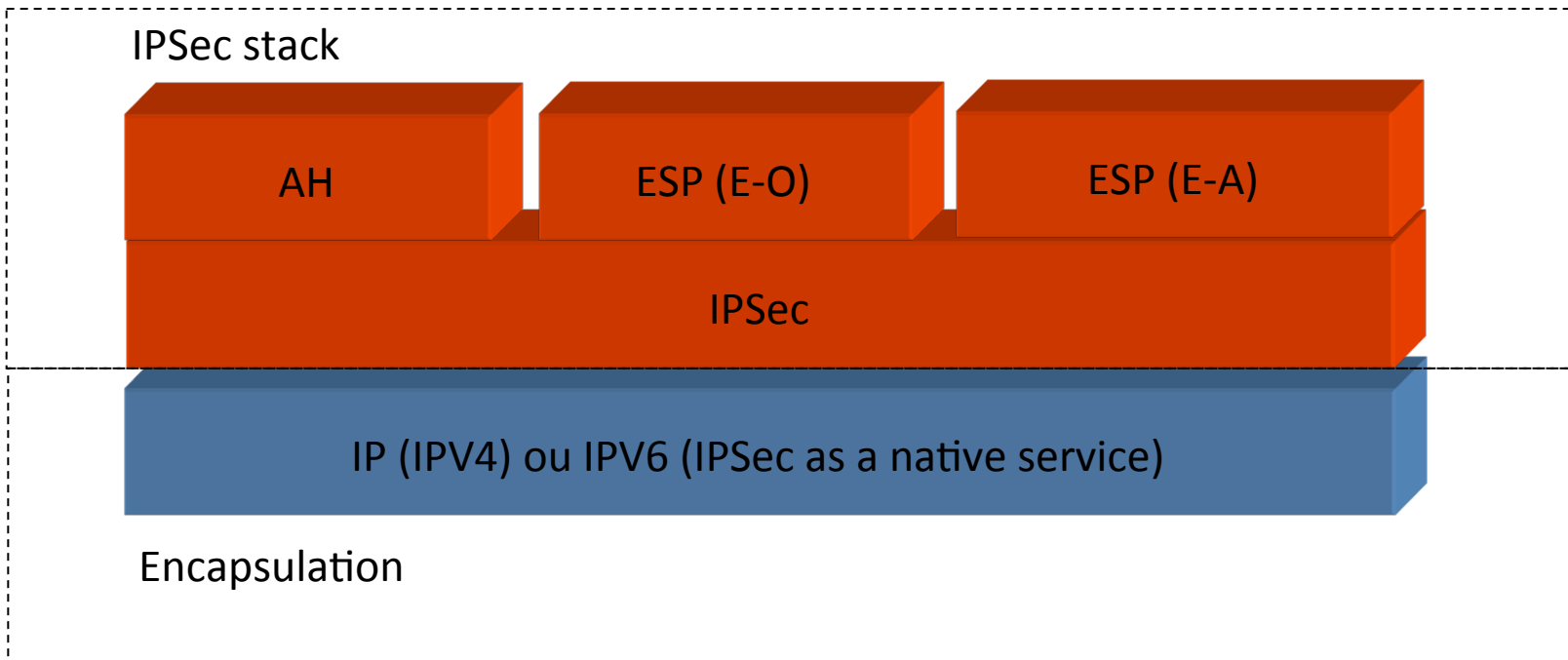
- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
-  – IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

IPSec encapsulation

RFC 2401: IPSec architecture and stack encapsulation issues

*Remember IPV4 and IPV6 to understand encapsulation issues
(bibliography)*

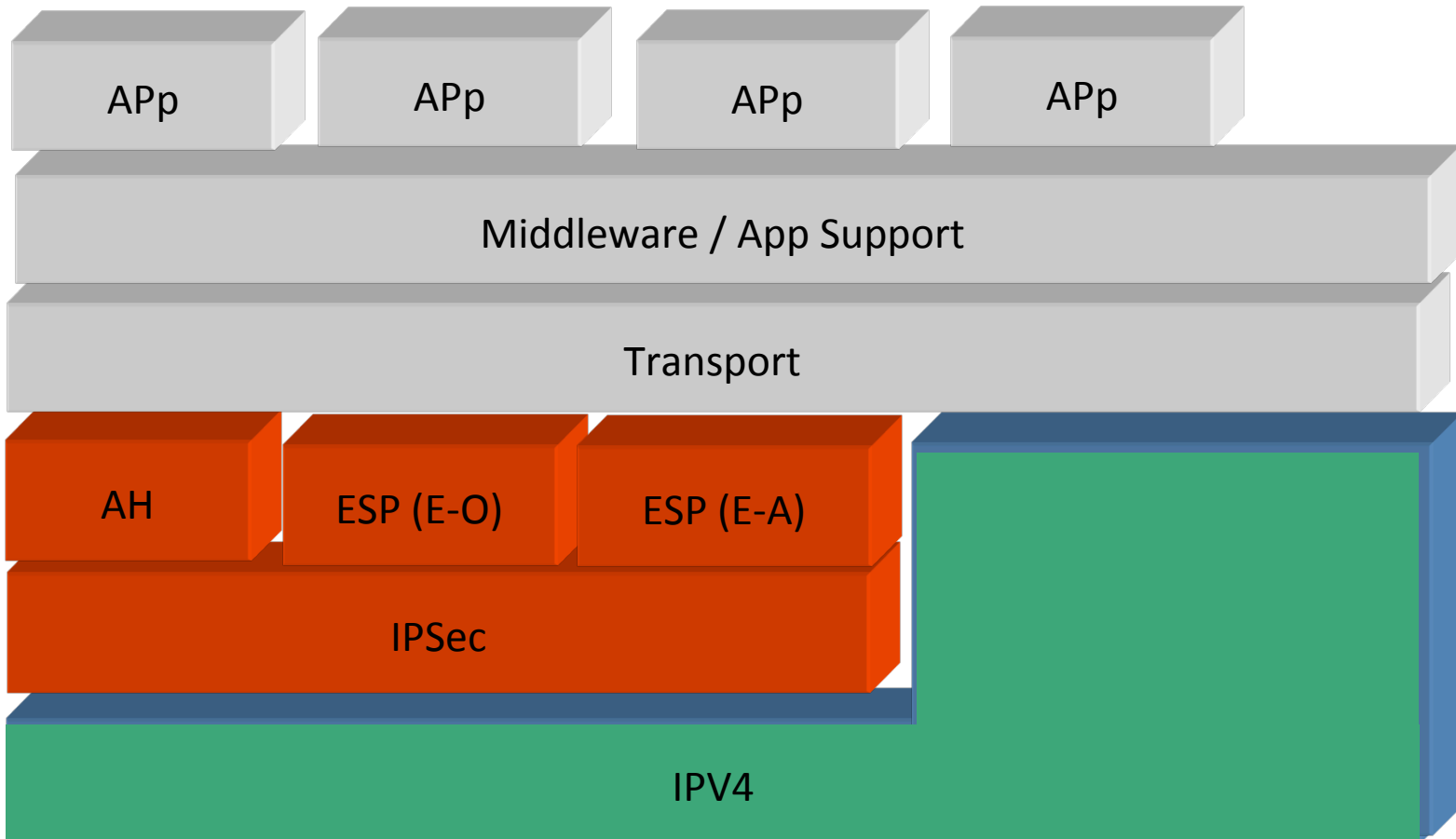
RFC 2407: DOI (Domain of Interpretation)



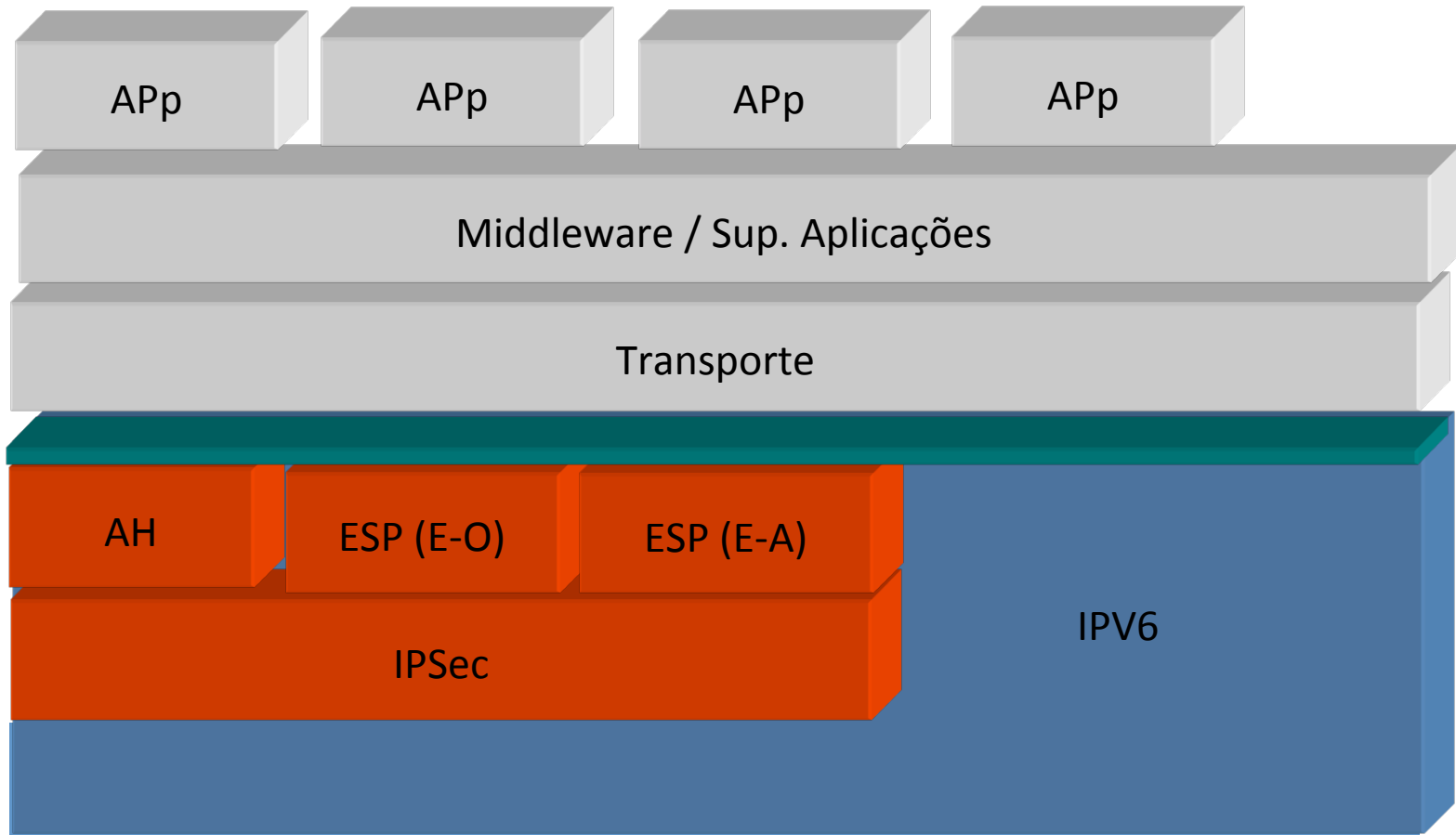
AH > RFC 2402: AH over IPV4 and over IPV6

ESP > RFC 2405, RFC 2406

IPSec / IPV4

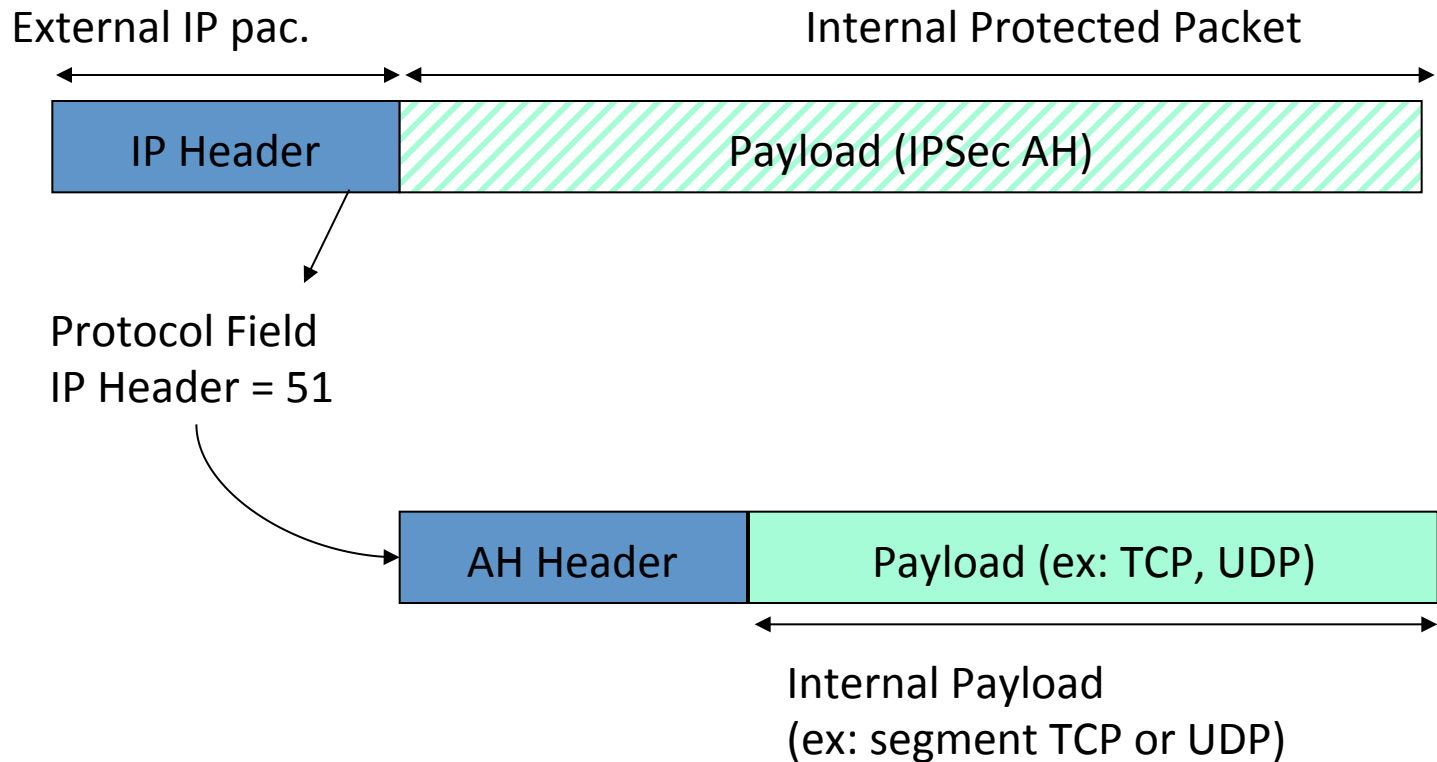


IPSec is native in IPV6 service

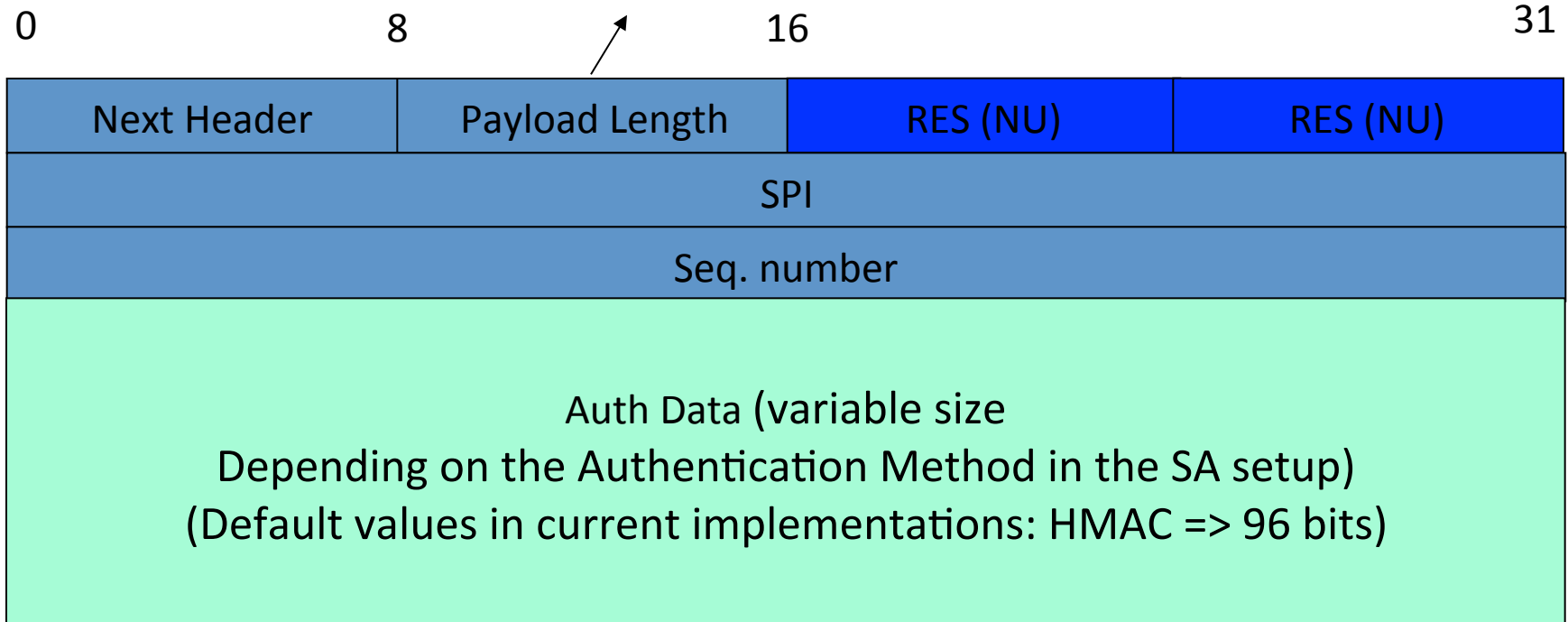


AH (Authentication Header Protocol)

Encapsulation:



AH (RFC 2402)



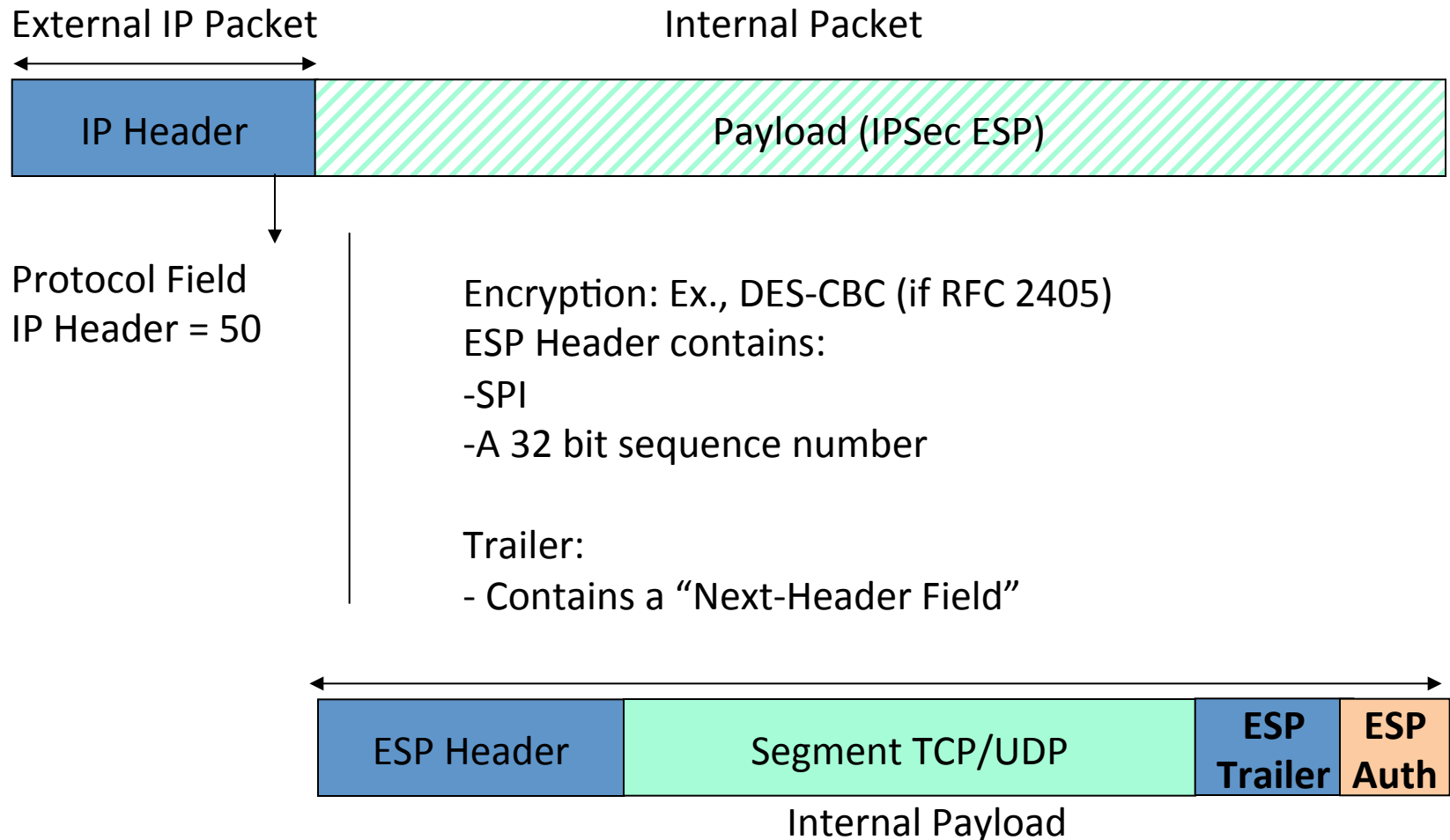
Auth Data (described in the RFC 2402)
Contains an ICV (Integrity Check Value) acting as a
MAC (HMAC-MD5-96, or HMAC-SHA-196)

Encapsulating Security Payload (ESP)

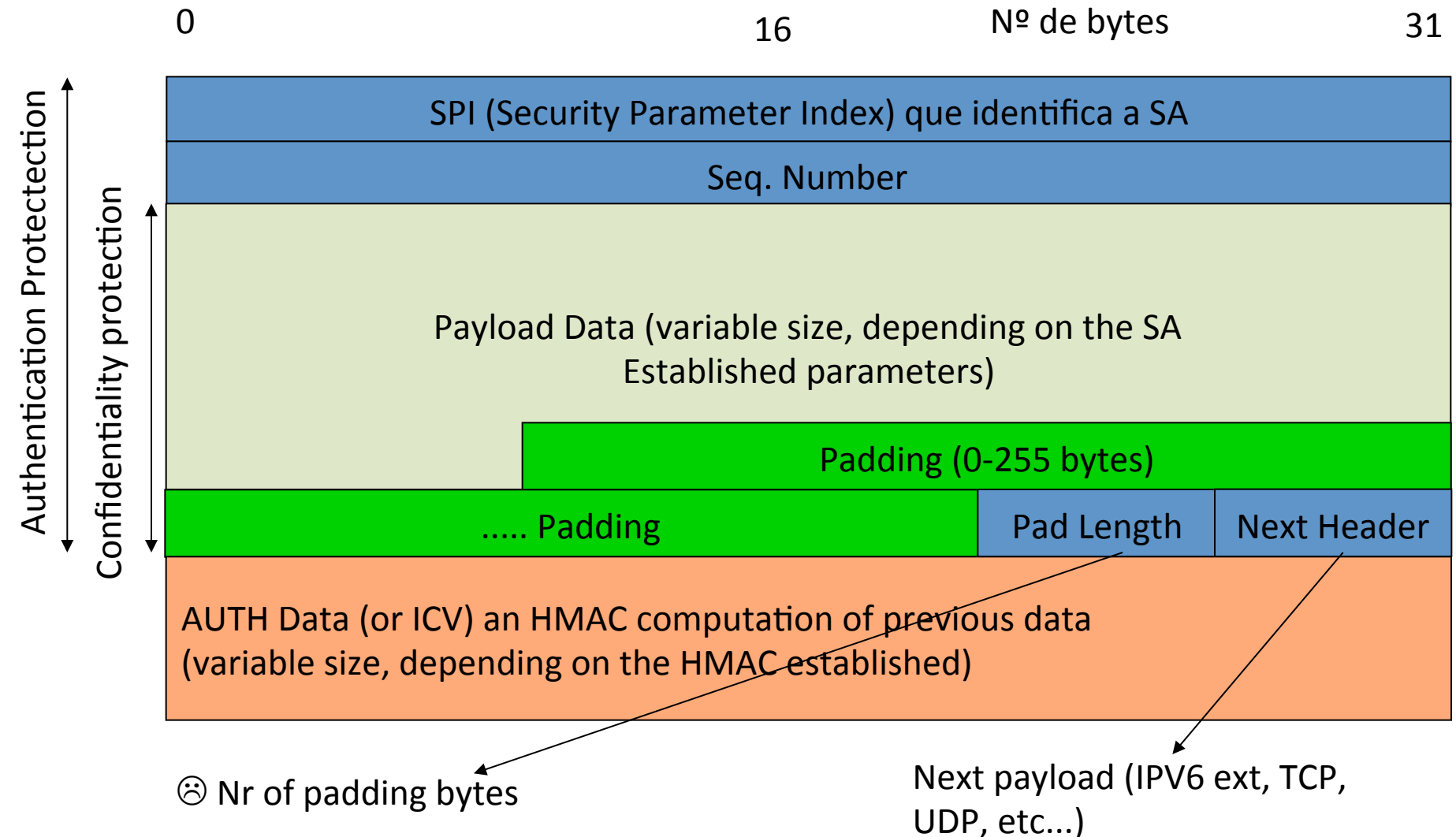
- Provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality
- Services depend on options selected when establish Security Association (SA), net location
- Can use a variety of encryption & authentication algorithms

ESP – Encapsulation Security Payload

- More complex than AH (more overhead but more security concerns)



ESP (RFC 2406 ... 4303, 4305)




Encryption & Authentication

Algorithms & Padding

- ESP can encrypt payload data, padding, pad length, and next header fields
 - if needed have IV at start of payload data
- ESP uses padding
 - to expand plaintext to required length
 - to align pad length and next header fields
 - to provide partial traffic flow confidentiality
- ESP can have optional ICV for integrity
 - is computed after encryption is performed

Outline

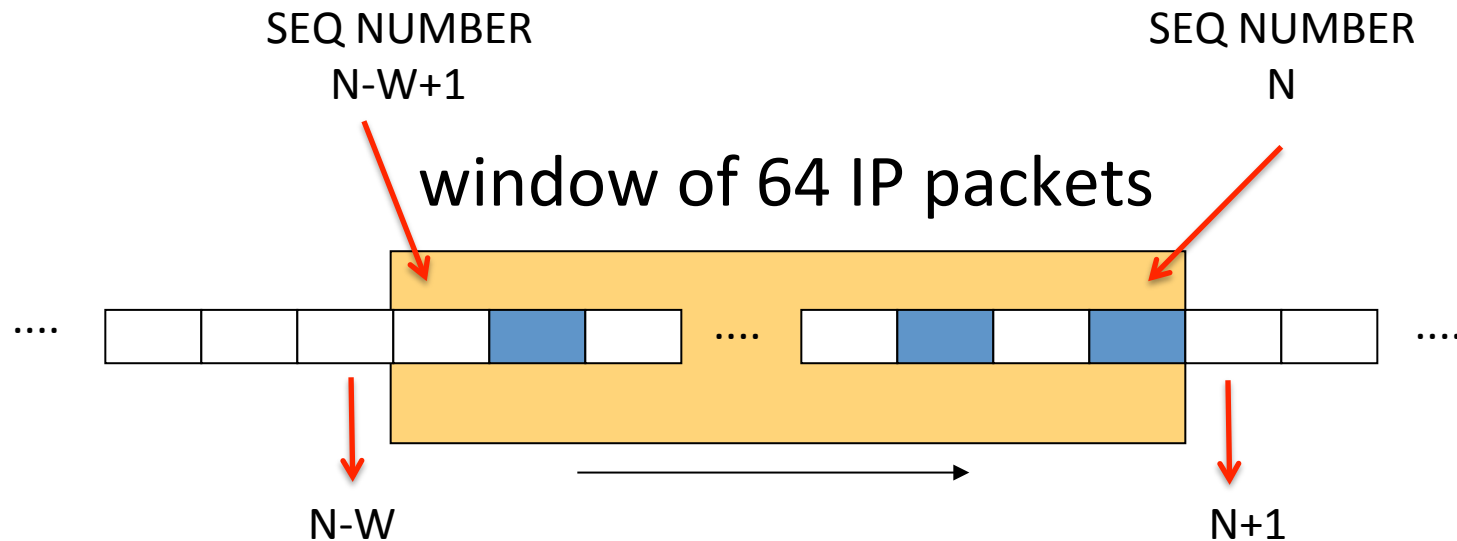
- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
-  – Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

Anti-Replay Service


- Replay: attacker resends a copy of an authenticated packet (IPsec Packet)
- IPSec Solution: use of a sequence number to thwart this attack
- Sender initializes sequence number to 0 when a new SA is established
 - increment for each packet
 - must not exceed limit of $2^{32} - 1$
- Receiver then accepts packets with seq no within window of $(N - W + 1)$
- But ... **IP is a datagram (no reliable) protocol** ... What if packets arrive out of order ?

Out-of-Order packets and control

- IPSec solution: Use of a sliding window control

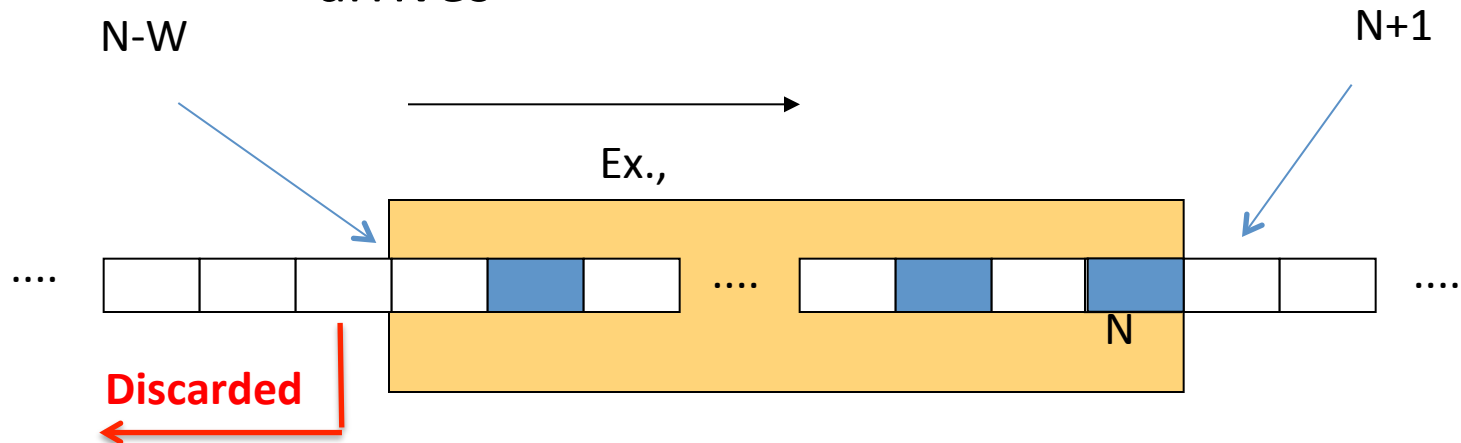


Anti-Replaying Control Window


Valid received packets in the current window marked as “valid” 

Received packets with sequence numbers on the left of the window base OR with incorrect authentication (invalid HMAC proof for the SA parameters) **are discarded**

Sliding window: window goes to the right, when a valid packet with sequence number = N arrives



Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
-  – Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

Combining Security Associations

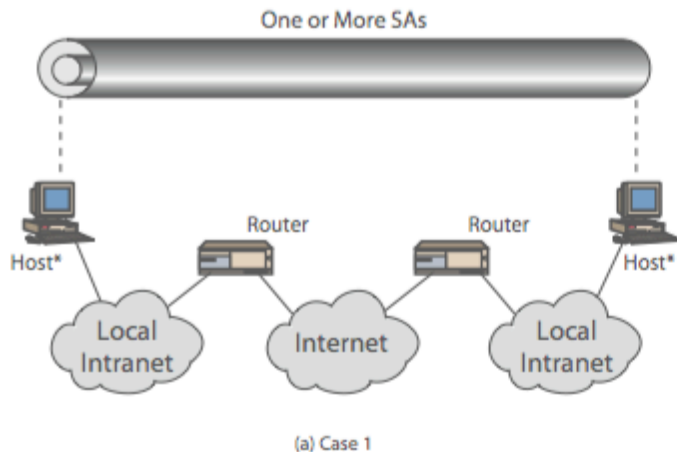
- SA's can implement either AH or ESP
- Sometimes, we need to implement both: need to combine SA's for flexibility vs. security purposes and tradeoffs
 - form a **Security Association Bundle (SAB)**
 - A SAB may terminate at different or same endpoints
 - Combination is possible in different ways, by
 - **transport adjacency**
 - **iterated tunneling**
- combining authentication & encryption
 - ESP with authentication
 - Bundled inner ESP & outer AH
 - Bundled inner transport & outer ESP

More on flexibility: Bundles vs. Modes

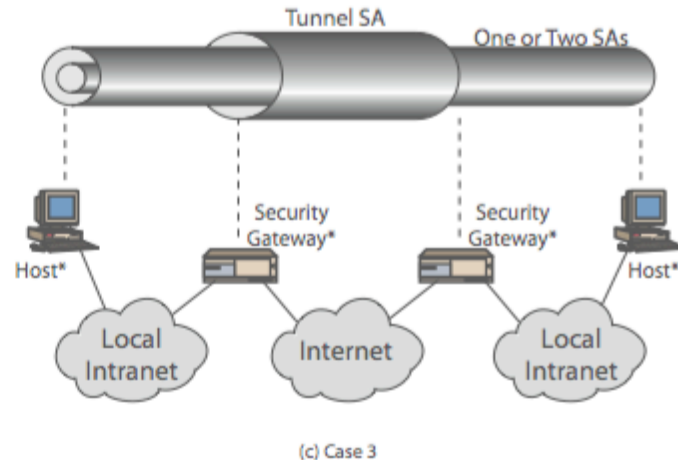
- To maximize tradeoffs, the combination can be done involving:
 - SA bundles with different policies
 - And different IPSec modes
 - Exploring adjacency or iteration

SA combinations and Bundles

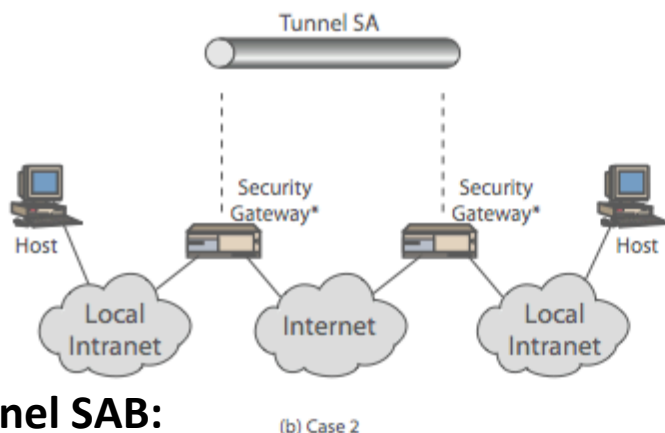
(1) 2-transport SABs



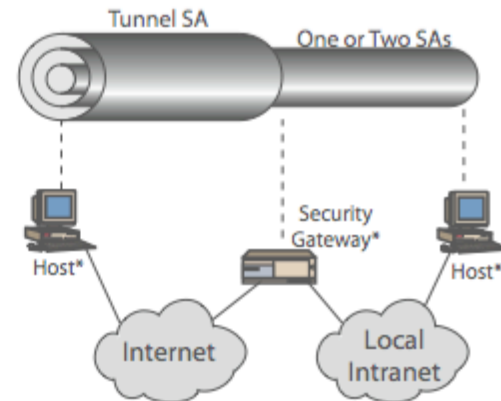
(3) 2-transport SABs and 1-tunnel SAB End-to-End security added to (2)



(2) 1-tunnel SAB: ex of single tunneled VPN solution



(4) 1-2 Transport SABs and 1 Tunnel SA: A secure Remote Access



Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes



IPSec cryptographic Suites (in RFC 7321, Aug 2014)

ESP Authenticated Encryption

Requirement	Authenticated Encryption Algorithm
-----	-----
SHOULD+	AES-GCM with a 16 octet ICV [RFC4106]
MAY	AES-CCM [RFC4309]

ESP Encryption Algorithms

Requirement	Authenticated Encryption Algorithm
-----	-----
MUST	NULL [RFC2410]
MUST	AES-CBC [RFC3602]
MAY	AES-CTR [RFC3686]
MAY	TripleDES-CBC [RFC2451]
MUST NOT	DES-CBC [RFC2405]

IPSec cryptographic Suites (in RFC 7321, Aug 2014)

AH Authenticated Encryption

The requirements for AH are the same as for ESP Authentication Algorithms, except that NULL authentication is inapplicable.

Summary of Changes from RFC 4835

Old Requirement	New Requirement	Algorithm (notes)
-----	-----	-----
MAY	SHOULD+	AES-GCM with a 16 octet ICV [RFC4106]
MAY	SHOULD+	AES-GMAC with AES-128 [RFC4543]
MUST-	MAY	TripleDES-CBC [RFC2451]
SHOULD NOT	MUST NOT	DES-CBC [RFC2405]
SHOULD+	SHOULD	AES-XCBC-MAC-96 [RFC3566]
SHOULD	MAY	AES-CTR [RFC3686]

IPSec cryptosuite (summary)

IPSec w/ IKE v1

IPSec w/ IKE v2,v3

As defined for VPNs
(RFC 4308)

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

As defined for VPNs
(RFC 4308)

IPSec w/ NSA Security Levels

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/ Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP
IKE authentication	ECDSA-256	ECDSA-384	ECDSA-256	ECDSA-384

Outline

- VPNs and IPSec: Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes



IPSec Key Management

- Handles key generation & distribution
 - SA establishment process
- Typically need 2 pairs of keys
 - 2 per direction for AH & ESP
- Manual key management
 - sysadmin manually configures every system
- Automated key management
 - automated system for on demand creation of keys for SA's in large systems
 - Protocols and schemes:
 - Oakley
 - ISAKMP, IKE

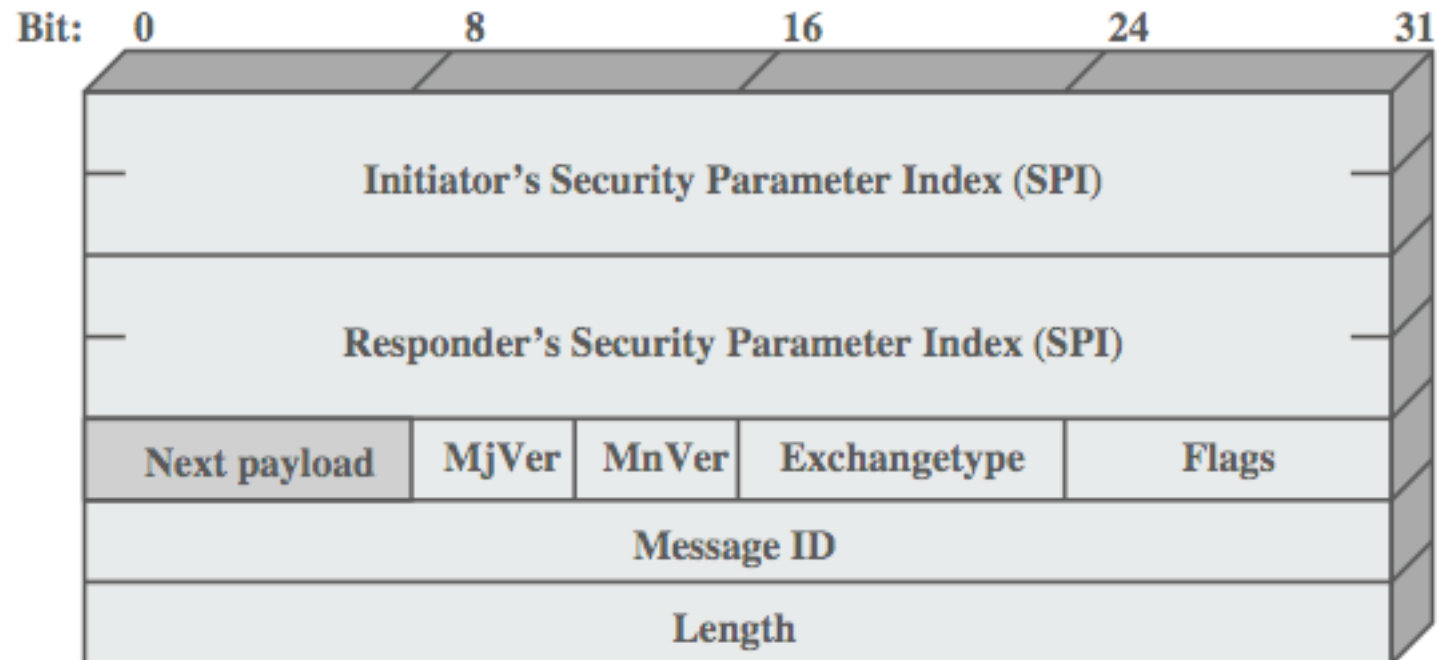
Oakley

- A key exchange protocol
- Based on Diffie-Hellman key exchange
- Adds features to address weaknesses
 - No info on parties, man-in-middle attack, cost
 - So adds cookies, groups (global params), nonces, DH key exchange with authentication
- Can use arithmetic in prime fields or elliptic curve fields

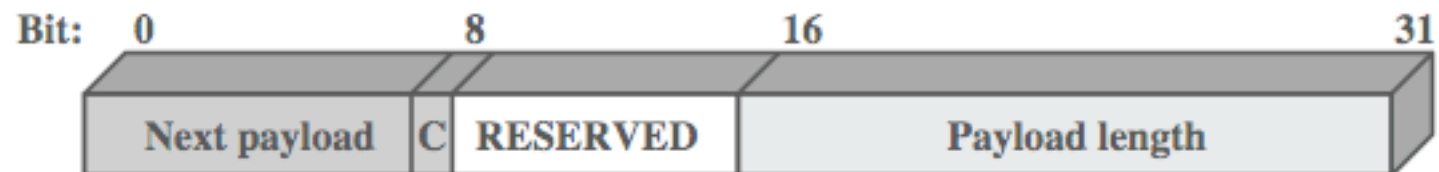
ISAKMP

- Internet Security Association and Key Management Protocol
- Provides framework for key management
- Defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- Independent of key exchange protocol, encryption alg, & authentication method
- IKEv2 no longer uses Oakley & ISAKMP terms, but basic functionality is same

IKE formats



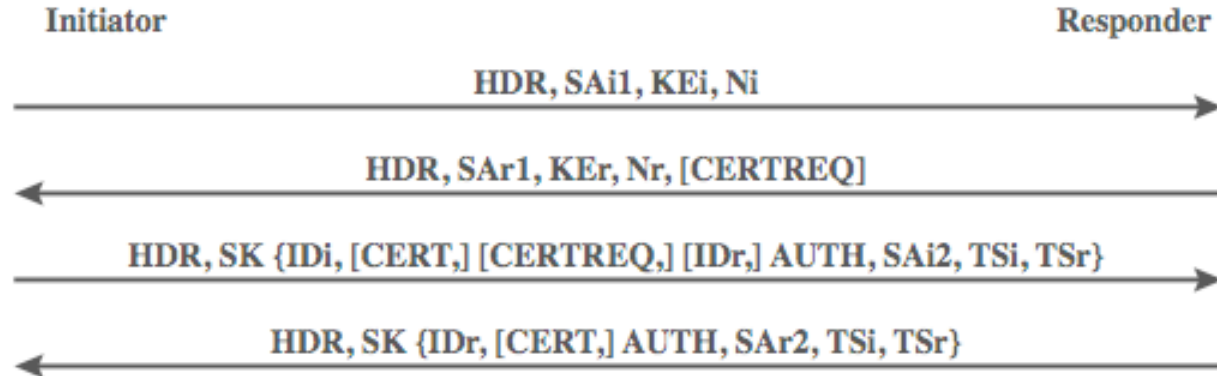
(a) IKE Header



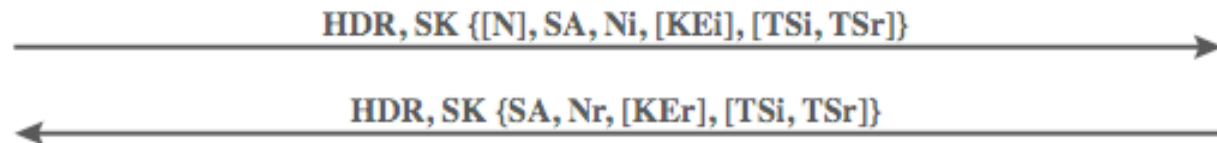
(b) Generic Payload Header

IKEV2 Exchanges

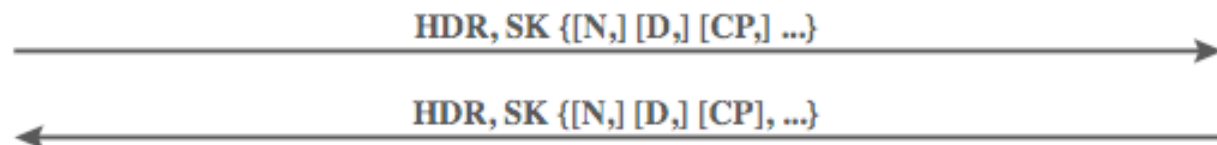
See bibliography for details



(a) Initial exchanges



(b) CREATE_CHILD_SA Exchange



(c) Informational Exchange

IKEV2 Exchanges

- Different exchanges are defined for flexibility
 - Addressing security and performance tradeoffs
 - Interesting to automatic setup in different SAs, different iterated or adjacent combinations and different modes for each specific purposes

IKE Payloads & Exchanges

- Payload types
- Have a number of ISAKMP payload types:
 - Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- payload has complex hierarchical structure
- may contain multiple proposals, with multiple protocols & multiple transforms

Outline / Conclusion

- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

Conclusions

We covered:

- VPN, IPSec Overview
- IP Security uses and benefits
- IP Security Architecture (and IPSec Stack)
- IPSec Modes: Transport vs. Tunneling
- IPSec Security Associations
- IPSec Security protocols and encapsulation
- Anti-Replaying Service
- Security and Flexibility: Combination of Security Associations
- IPSec crypto-suite
- Key Management Schemes

Key-Points (summary)

- IPSec as a capability that can be added and used with current IPV4 and IPV6 versions
- Protection at Network-Level, Establishment of IP-based Secure Communication
- Transparent to the above TCP/IP stack levels
- IPSec supports fundamental security properties: authentication, confidentiality, integrity and key-management
- Protection provided by the IPSec protocol suite, namely by AH, ESP-A and ESP-AE
 - Authentication of IP packets origins (HMACs applied to the entire original IP packet (in tunnel mode) or to all of the packet except the IP header (in transport mode))
 - Confidentiality by the encryption of encapsulated security payloads, both provided in tunnel and transport modes
 - Key management: provided by the ISAKMP framework and protocols – Oakley and IKE protocol evolutions

Key-Points (criticisms and new research directions)

- IPSec Generic Advantages / Disadvantages
- IPSec management overheads / dependencies
 - X509 Certification, CA dependencies, PKI Management
 - Practical (simple deployments): Pre-Shared Keys avoiding IKE/ISAKMP Key-Establishment
- IP Mobility and Scalability Requirements
 - Approaches using Locator/Identifier Separation Protocols (LISP)
- DoS, DDoS, ...
 - Light Weight Authentication and Integrity using Ephemeral Identifiers
- IPSec modes: what if we want to use traffic shapers or filtering-boxes
- Others ?

Suggested Reading (Evaluation)

Available in the CLIP System (CSD Materials)

- W. Stallings, Network Security Essentials - Applications and Standards (4th Ed), Prentice Hall, 2011

Other bibliography

- William Stallings, Cryptography and Network Security (version 5), Chap.19 IPSec
 - IPSec related RFCs (ref. nos slides 9.15, 9.16 e 9.17
 - Last updated RFCs: <https://en.wikipedia.org/wiki/IPsec>
 - W. Stallings, *Network Security Essentials – Applications and Standards*, Prentice Hall, v3, Chap. IPSec
 - More practical info (Linux-Based IPSec Configurations)
 - <https://help.ubuntu.com/community/IPSecHowTo>
 - <https://wiki.debian.org/IPsec>
 - VPN, VPN Software ...
 - OpenSource IPsec-based VPN Solution
 - See <https://strongswan.org>
- See also:
- http://www.thegreenbow.com/doc/tgbvpn_cg_Linux_en.pdf