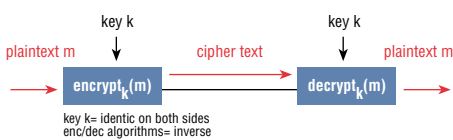


IP security reference card

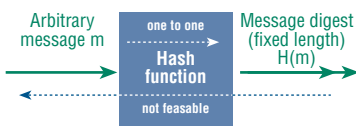
SYMMETRIC CRYPTO



Historic:	Symmetric Ciphers	
	Stream cipher	Block cipher
Caesar Substitution Vigenère Vernam ...	Applied on each digit	Applied on equal data blocks
	RC4, SEAL	(3)DES, ECB, CFB, OFB, ... IDEA, RC2, AES RC5, Blowfish, CAST-128

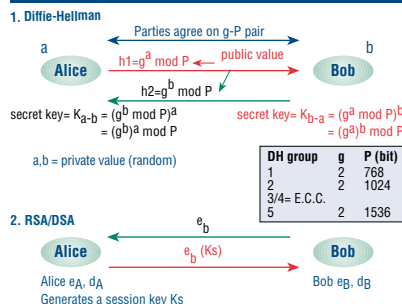
Name	Key Length (bit)	Block Size (bit)
DES	56	64
3DES	112/168	64
IDEA	128	64
Blowfish	32-448	64
CAST-128	40-128	64
RC2	8-1024	64
RC5	0-2040	128
AES	128-256	128

HASHING

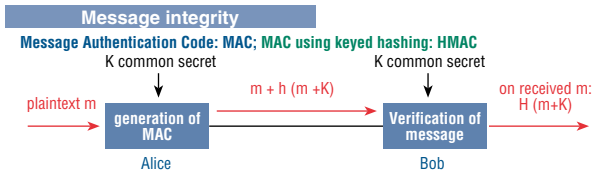
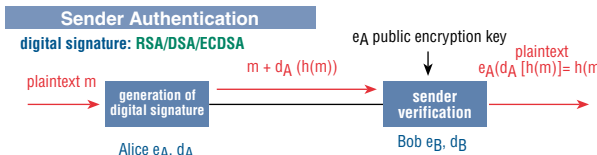
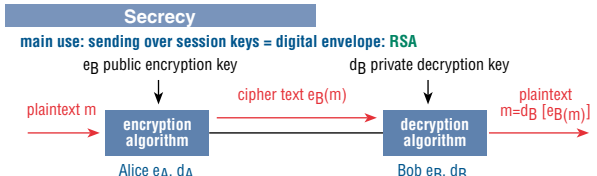


Algorithm	Output (bit)
Checksum	16
MD4	128
MD5	128
SHA-1	160
SHA-xxx	256 / 384 / 512
RIPEMD-160	160

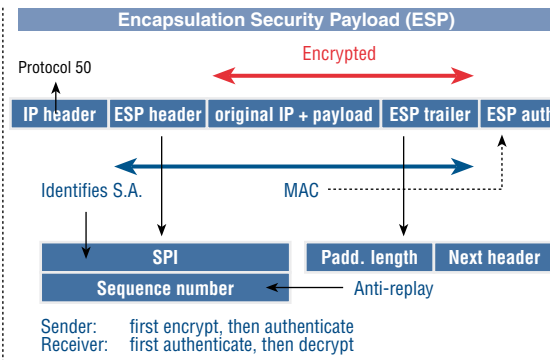
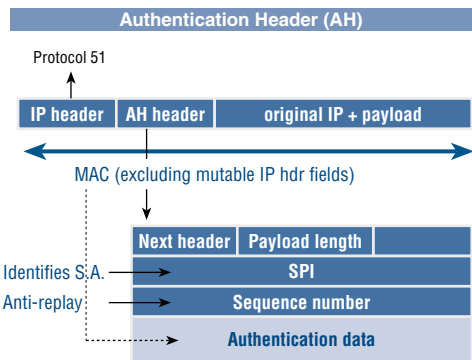
KEY EXCHANGE MECHANISMS



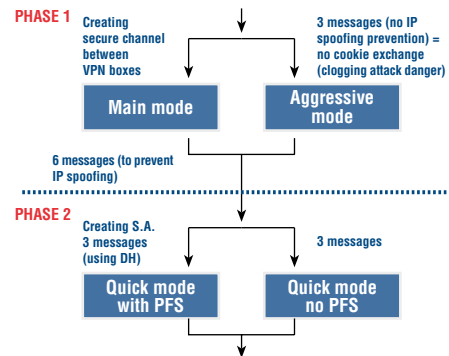
PUBLIC KEY CRYPTO



IPsec (TUNNEL MODE)

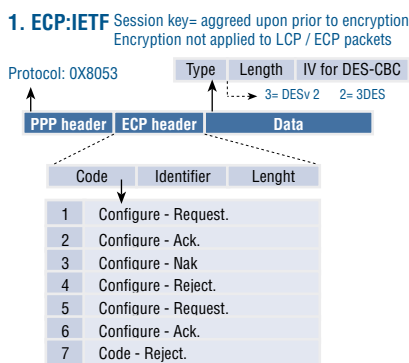


IKE NEGOTIATION



PPP SECURITY

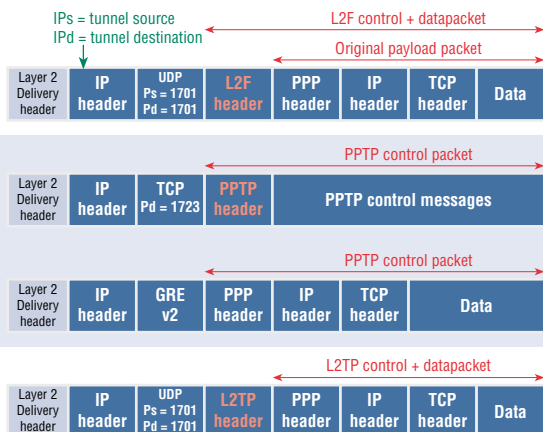
Encryption



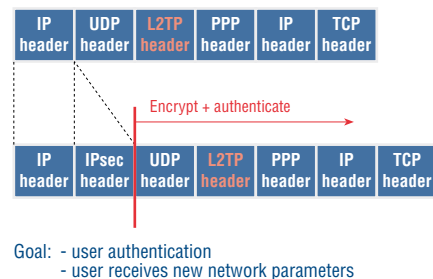
2. MPPE: Microsoft PtoP encryption:
RC4 key length negotiable: 40-56-128 bits

Authentication: EAP (RFC 2284)

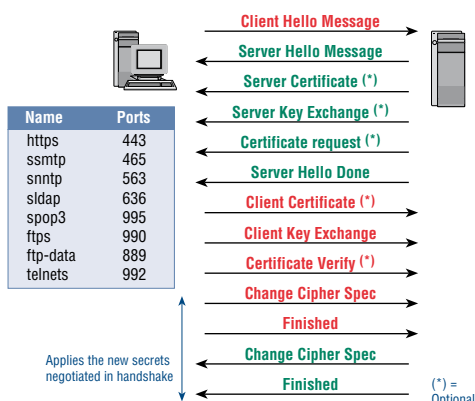
L2F - PPTP - L2TP



L2TP IN IPSEC (TRANSPORT MODE)



OVERVIEW OF TLS HANDSHAKE MESSAGES



OPENSSL (COMMAND OVERVIEW)

Generating keys
openssl genrsa [-out filename] [-passout arg] [-des] [-des3] [-idea] [-f4] [-3] [-rand file(s)] [numbits]

Requesting a certificate
openssl req [-in filename] [-out filename] [-new] [-key filename] [-keyout filename] [-md5sha1md2] [-config filename] [-subj arg] [-x509] [-days n] [-set_serial n] [-extensions section] [-reqexts section]

Generating a certificate
openssl x509 [-in filename] [-out filename] [-serial] [-hash] [-email] [-startdate] [-enddate] [-purpose] [-req] [-md2] [-md5] [-sha1] [-mdc2] [-clrext] [-extfile filename] [-extensions section]

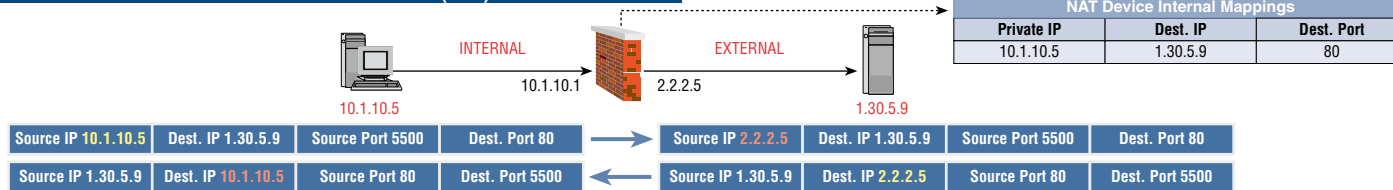
CA management
openssl ca [-gencrl] [-revoke file] [-crl_reason reason] [-crl_hold instruction] [-crlays days] [-days arg] [-md arg] [-cert file] [-selfsign] [-in file] [-out file] [-notext] [-outdir dir] [-infile] [-extensions section] [-extfile section]

Encoding
openssl enc [-ciphername] [-in filename] [-out filename] [-pass arg] [-e] [-d] [-a] [-A] [-k password] [-kfile filename] [-K key] [-iv IV] [-P] [-bufsize number] [-nopad] [-debug]

SECURITY RELATED URLS

- ICRI: <http://www.law.kuleuven.ac.be/icri/>
- PacketStorm: <http://www.packetstormsecurity.com/>
- SANS: <http://www.sans.org>
- CVE database: <http://cve.mitre.org>
- CERT: <http://www.cert.org>
- SecurityFocus: <http://www.securityfocus.com>
- Linux Security: <http://www.linuxsecurity.com>
- NIST: <http://csrc.nist.gov>
- mailinglist overview: <http://archives.neohapsis.com>
- BUGTRAQ Mailinglist: <http://www.securityfocus.com>
- SECUNIA Mailinglist: <http://www.secunia.co.uk>
- Sec. Resource Center: <http://csrc.nist.gov/>
- COAST: <http://www.cerias.purdue.edu/coast>
- IPTables: <http://www.netfilter.org>
- Internet Storm Center: <http://incidents.org>
- SNORT signatures updates: <http://www.whitehats.com/ids/>
- Microsoft Security Downl.: <http://www.microsoft.com/downloads>
- BCVG: <http://www.ebcug.com/info.php>
- Newsgroups: <http://www.comp.security.announce>
- <http://www.comp.os.linux.security>
- <http://www.comp.os.ms-windows.nt.admin.security>

NETWORK ADDRESS TRANSLATION (NAT) ONLY

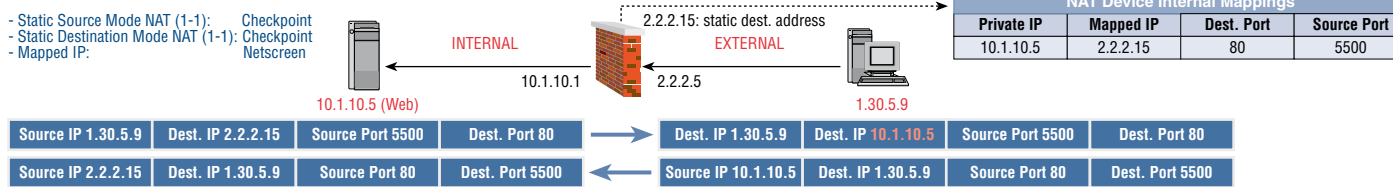


JOHN CORDIER ACADEMY

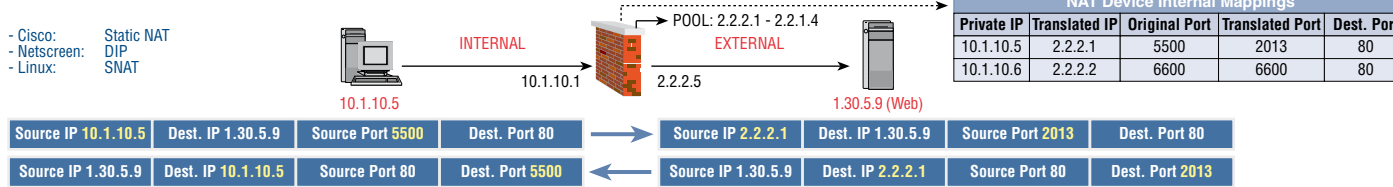
www.jccademy.com

IP Security reference card[©] v.2.0

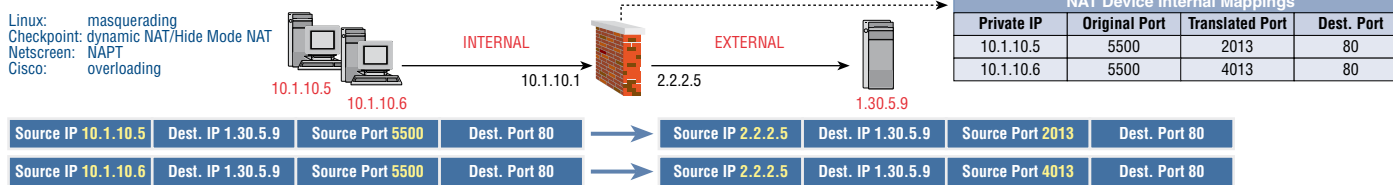
STATIC SOURCE/DESTINATION MAPPING



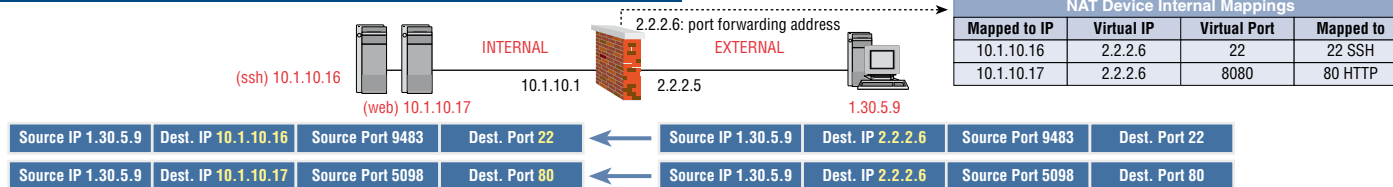
MULTIPLE ADDRESSES TRANSLATED TO A POOL OF ADDRESSES



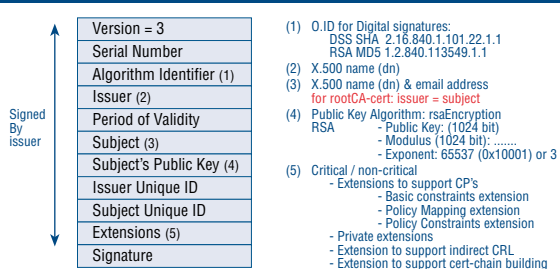
NETWORK ADDRESS & PORT TRANSLATION



PORT FORWARDING



X509 v3 CERTIFICATE



X509 CRL FORMAT

