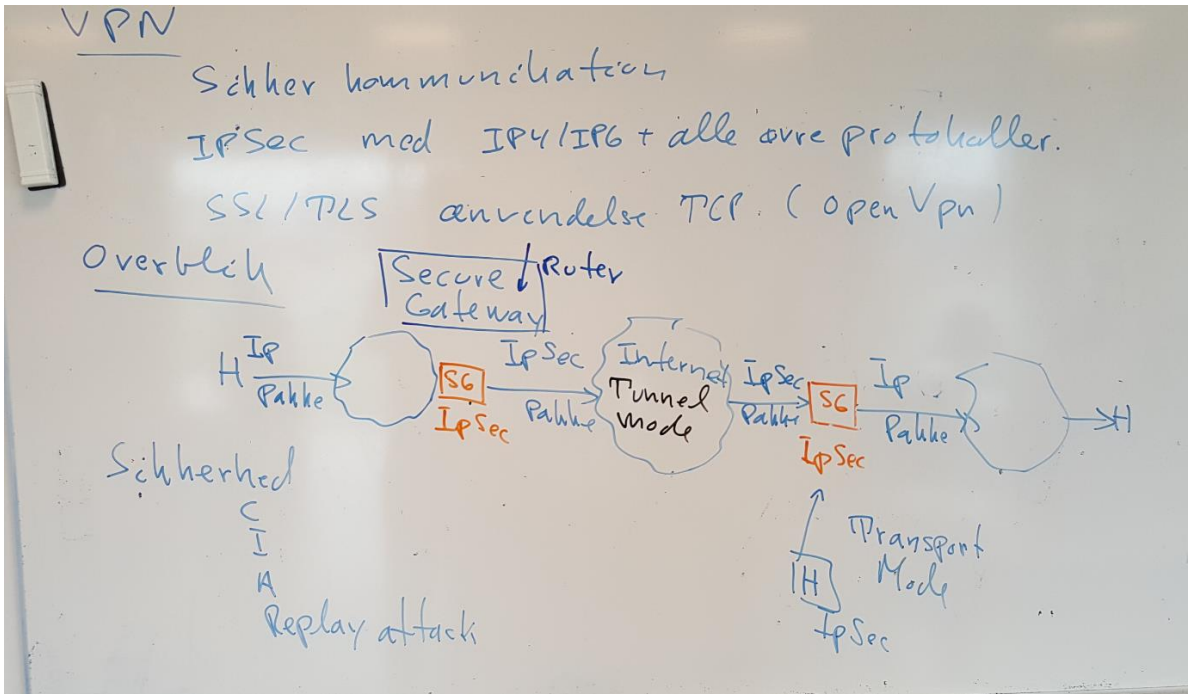
IPSEC & VPN WHITEBOARD LECTURES BY MICHAEL CLAUDIUS 22. MARCH 2019



Protokoller

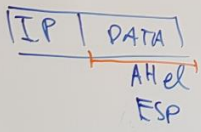
AH Authenti-cation Header
Authentication HMAC
Integrity SHA2
Sekvensnummer start 0 ++

ESP Encapsulating Secure Payload
Confidentiality 3xDES AES. Private/Public key
Sekvensnummer Diffie-Hellmann++

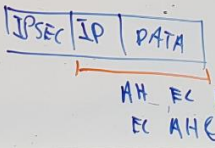
* ESP+AH

Modes

Transport

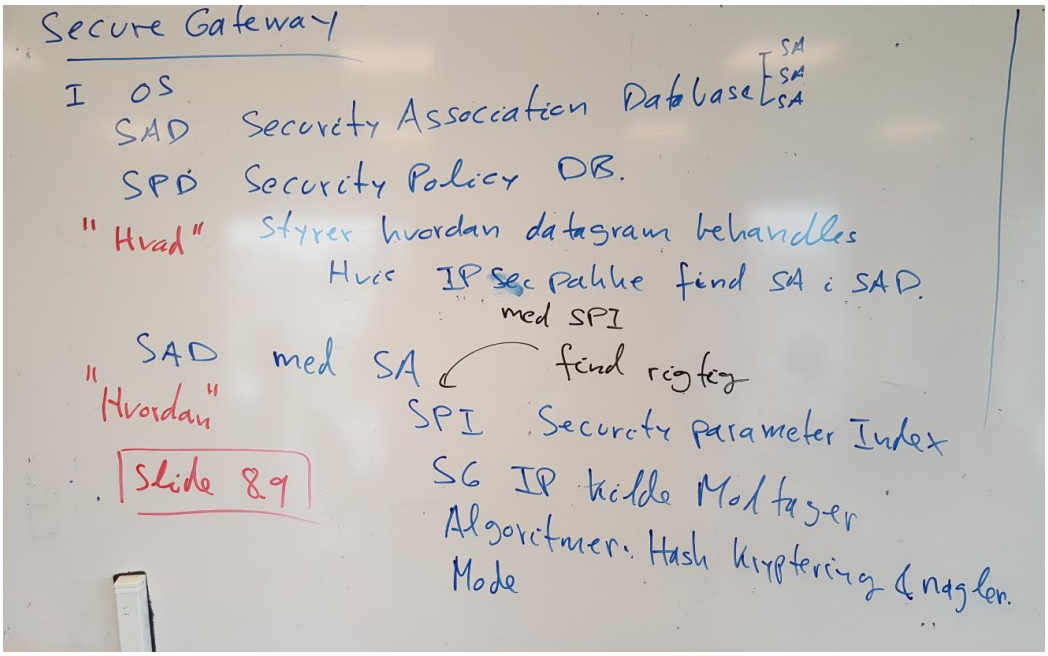


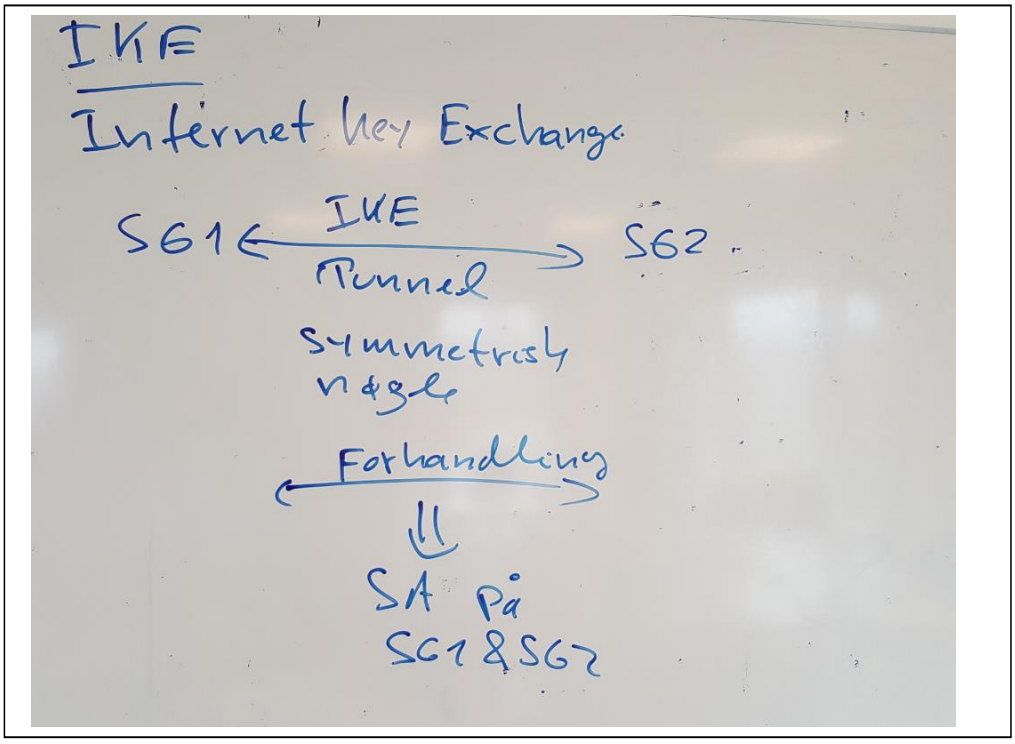
Tunnel



AH el ESP
el AH & ESP

Forbindelser
H → SG → SG → H
H → H
H → SG → H


Secure Gateway
I OS
SAD Security Association Database
SA
SA
SA
SPD Security Policy DB.
"Hvad" Styrer hvordan datagram behandles
Hvis IP pakke find SA i SAD.
med SPI
SAD med SA
find rigtig
"Hvordan"
SPI Security parameter Index
Slide 89
SG IP header Modtager
Algoritmer: Hash kryptering & nøgler.
Mode


IKE
Internet key Exchange
SG1
IKE
Tunnel
SG2
symmetrisk
nøgle
Forhandling
SA på
SG1 & SG2