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

VPN Schher hommuniliation IPSec med IPY/IPG + alle ovre protohaller. SSI/TLS anvendelse TCP. (Open Vpn) Overblich Secure Froter Gateman HIR IP Sec Internet Ipsec SC IP Pakke Ipsec Pakke Mode Pakke SC Pakke SC Pakke SC Pakke Tomel Pakke Ipsec Pranspor Mode A Replay

| Protohol | |
|----------------|---|
| · AIA A | uthen ti-cation Header |
| A | other tication HMAC |
| 1 | integraty SHAZ |
| | Schvensnummer start 0, ++, |
| | Encapsulating Secure Payload |
| | Confiduntiality 3xDES AES. Private (Public her, |
| | Selvenenumer Diffie-Helmannet |
| * ESP+AH | |
| Modes | P For buddelser |
| | Transport Tunnel Hassen SE->H |
| | TPLIT |
| | IP PATA IPSECIP PATA H->SC->H |
| and the second | ESP AH EL ESP |
| | EC AHEESP |
| | |

Secure Gateway Security Association Dato base Est I OS SAD Security Policy DB. SPD Styrer hvordan datagram behandles " Hvad " Huis IP sec Pakke find SA i SAD. med SPI SAD med SA find rigter Wordan SPI Security parameter Index It Hvordan SG IR trilde Mod taser Shide 8.9 Algoritmer. Hash Kryptering & nagler.

TKE Internet her Exchange SG1E IKE SG2. Runnel SG2. Simmetristy Nogle Forhandling U SA Pa SCI & SGZ