# Krüpto rakendamine võrguturbes

- Ülevaade
- TLS
- SSH
- DTLS
- DNSSEC, DANE
- Meili signeerimine ja krüpteerimine
  - MIME krüptoraamistik
  - PGP
- Virtuaalsed privaatvõrgud
  - IPSec

# Krüpteerimine — konfidentsiaalsuse tagamiseks

- TLS — *de facto* standard
- SSH — konkurent TLS-le (oma nišis)
- IPSec — standard IP tasemele
- PGP — (meili) krüpteerimine ja signeerimine
- S/MIME — MIME lisandused krüpteerimiseks ja signeerimiseks
- Kerberos
- Secure RPC
- ...

# TLS

- SSL — *Secure Sockets Layer* (algne standard, tänapäeval vananenud)
- TLS (*Transport Layer Security*) — SSLv3-st edasi arenenud IETF standard
- Kiht TCP ja rakenduste vahel, loob TCP laadse "toru"
- Toru sees saab rääkida muid protokolle (HTTP, LDAP, IMAP, POP3, telnet, . . . )
- Toru kumbagi otsa saab autentida sertifikaadi abil
- Torus liikuvad andmed krüpteeritakse (+tervikluse kaitse)
- Torus liikuvad andmed võib ka pakkida (RLE, zlib)

# TLS protokollist

- Kumbki saadab oma versiooninumbri ja toetatud šifrite nimekirja
- Server saadab oma serdi (ja küsib kliendi serti, kui soovib)
- Klient autendib serverit sertifikaadi järgi (veebi puhul kontrollib ka serdi seest domeeninime)
- Klient arvutab peamise võtme senise info järgi
- Klient saadab serverile selle võtme (krüpteerituna serveri avaliku võtmega)
- Kliendi autentimise puhul saadab klient ka oma serdi ja ühe tüki signeeritud andmeid ja server kontrollib neid
- Peamisest võtmest genereeritakse vahetatavad sessioonivõtmed
- Kumbki osapool kinnitab teisele, et hakkab genereeritud võtmete abil andmeid vahetama; andmevahetus võib alata

# SSH

- SSH — *Secure SHell*
- Samuti TCP ja rakenduse vahel
- Osapoolte vahel on krüpteeritud ja võibolla ka pakitud sisuga toru
- Serverit autenditakse avaliku võtme järgi
- Klienti võib autentida kliendi võtme abil, kliendimasina võtme abil või parooli abil (interaktiivselt)
- SSH ühenduse sisse tekitatakse mitu virtuaalset kanalit (näiteks teine toru X jaoks)
- On olemas mähkurid mitmete varasemate käskude turvaliseks asendamiseks

# Datagram TLS (DTLS)

- TLS töötab TCP baiditoru otsas, vahel on vaja kaitsta ka üksikute pakettide vahetust
- DTLS — TLS-laadne küptoprotokoll paketigranulaarsusega side jaoks
- UDP, SCTP, DCCP, SRTP protokollide baasil
- Võtmevahetus ja autentimine nagu vastaval TLS versioonil, edasise side jaoks ei emuleerita baidivoogu

# DNSSEC

- DNS (*Domain Name System*) — Interneti nimeteenus
- Tavalised DNS päringute vastused on ründaja poolt võltsitavad
- DNSSEC toob juurde vastuste signeerimine ning iga domeenitaseme kohta signeerimisvõtme
- Tehniline sertifitseerimishierarhia DNS puus
- DANE — DNSSEC abil turvatud DNS-i kaudu muude võtmete levitamise initsiatiiv (HTTPS, IPSec võtmed näiteks)

# Meili signeerimine ja krüpteerimine — MIME

- S/MIME — *Secure/Multipurpose Internet Mail Extensions*
- MIME tüüpide ja reeglite komplekt signeerimise ja krüpteerimise lisamiseks
- MIME jaoks on defineeritud üldine signeerimise ja krüpteerimise raamistik (tüübid `multipart/signed` ja `multipart/encrypted`)
- S/MIME defineerib rakenduse sellele raamistikule: `application/pkcs7-signature` formaat signatuuride jaoks ja `application/pkcs7-mime` muude vajaduste jaoks
- Need tüübid sisaldavad CMS (*Cryptographic Message Syntax*) objekte (seotud X.509 infrastruktuuriga)

# Meili signeerimine ja krüpteerimine — PGP

- PGP jaoks on seni kasutatud 3 formaati:
  - PGP oma päised kirja tekstikehas
  - MIME tüübiga `application/pgp` komponent kirja kehaks — halvasti käideldav
  - MIME krüptoraamistikus formaadid `application/pgp-signature`, `application/pgp-encrypted`, `application/pgp-keys`

# VPN — virtuaalsed privaatvõrgud

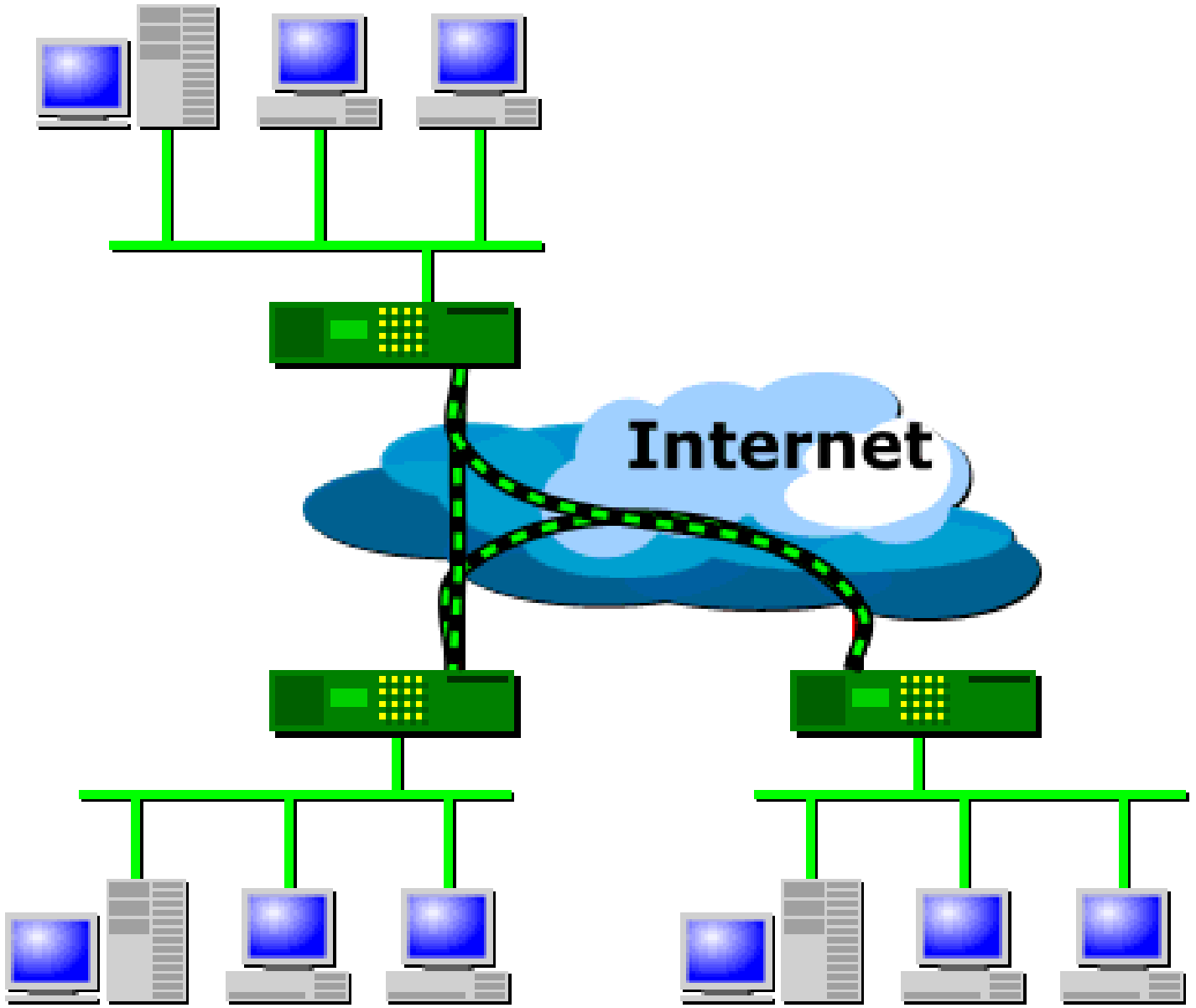
VPN idee: teeme üle Interneti krüpteeritud tunnelid oma kahe või enama võrgu vahel

- Tihti odavam kui eraldi ühendus osakondade vahel
- Internet on tänapäeval niikuinii olemas
- Võrreldes eriliiniga puudub siin reeglina garanteeritud ribalaius
- Tihti summaarselt lihtsam kui iga vajalikku teenust eraldi turvata

Mitu taset:

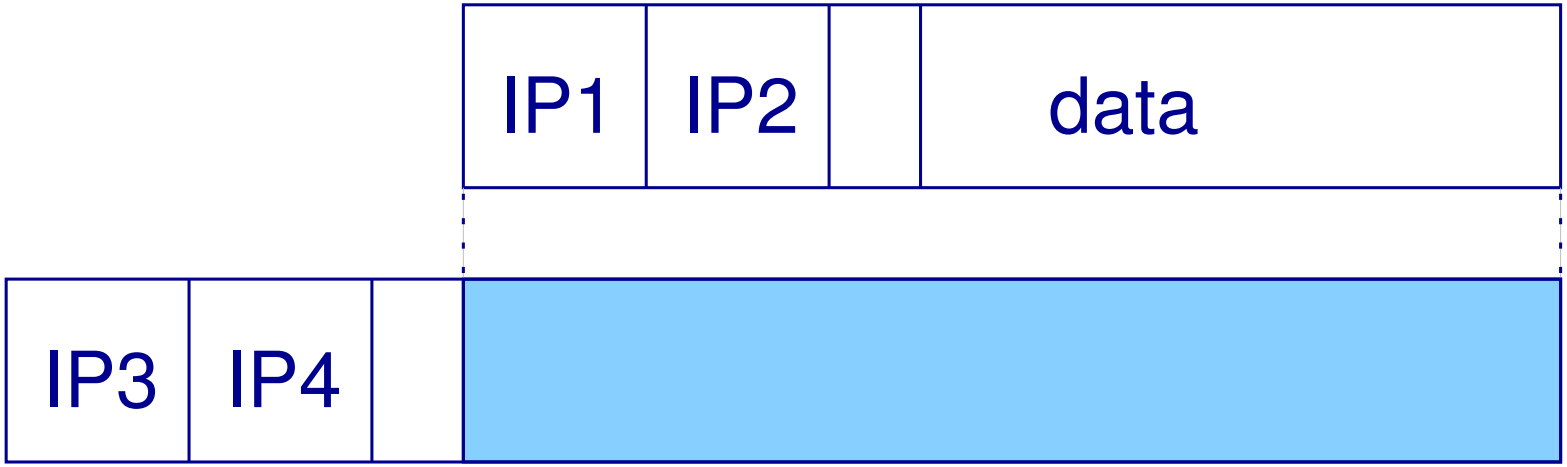
- Paljude kohtvõrkude kokku ühendamine
- Üksikud (mobiilsed) kaugtöökohad väljaspool firma võrke
- Extranet — turvalised kanalid partneritega

# VPN loogiline skeem



# VPN tehnoloogiline külg

- Üldine idee: krüpteeritakse paketid ära ja kapseldatakse saadud andmekogum mingisse (enamasti alumise kihi) paketti




- Näiteks IP-paketi kapseldamine teise IP-paketi või UDP paketi sisse
- Alguses oli igal tegijal oma protokollistik

# VPN: IPSec

- IPSec — algselt IPv6 lisavõimalus, kuid jõudis juurutamisse pigem IPv4 ajal
- Praeguse aja *de facto* formaat erinevate süsteemide vahel IP pakettide krüpteerimiseks
- IPSec lubab suvalisel hostide või ruuterite paaril omavahel krüpteeritult (ESP) ja/või autenditult (AH) andmeid vahetada
- 1999. a. kinnitati ka ametlik võtmevahetuse protokoll IKE (*Internet Key Exchange*) — selle abil saavad kaks masinat, mis teineteisest varem midagi ei teadnud, standardsel meetodil sessioonivõtmed kokku lepitud ja IPSec+IKE laiema leviku järel peaksid seega suvalised masinad olema võimelised omavahel krüpteeritult suhtlema.

# VPN: muud lahendused

- PPP üle TCP ühenduse (SSH, TLS, . . . )
- PPTP, L2TP, SSTP
- L2TP + IPSec
- **OpenVPN** — TLS + oma tunneliprotokoll
- WireGuard
- MPLS — krüpto pole kohustuslik (aga saab kasutada), põhiline idee on teenusepakkuja võrgu piires virtuaalsed torud
- . . .