NTNU | Kunnskap for en bedre verden

VPN

INFT1007 Datakommunikasjon, leksjon 12

Helge Hafting

VPN - Behov i forretningslivet

- Virtuelt Privat Nettverk

VPN - Behov i forretningslivet

- Virtuelt Privat Nettverk
- Fordi:
  - Organisasjoner gir tilgang til interne tjenester basert på at man er i lokalnettet. Brannmuren stopper utenforstående, for ute fins farlige folk.
  - Hjemmebrukere/reisende trenger interne ressurser
  - Kontorer i ulike byer trenger hverandres ressurser
    - leide linjer er dyrt
    - forbindelse via Internettet er utrygt

VPN - Alternativ til VPN

- Man har prøvd å gi tilgang basert på IP-adresse.
  - I noen fall kan IP-adresser forfalskes
  - Brysomt å holde orden på, adresser skifter over tid
  - Hjemmebrukere/reisende har *ikke* fast IP.
  - Interne tjenester er tidvis på private ip-adresser som 10.x.x.x, disse rutes ikke på internettet.

VPN - Sikker forbindelse

- VPN gir oss en sikker forbindelse via internettet
  - Kryptering beskytter mot avlytting og innbrudd
  - Passord holder utenforstående ute
  - Vi får en «tunnel» tvers gjennom det usikre Internettet

VPN - VPN for å skjule identitet

- Tjenester vi bruker på nett, ser hvor vi er
  - de ser ip-adressen vi bruker
  - ip-adresser kan spores til stedet vi er
- Om vi bruker VPN, ser de VPN-tjenerens adresse heller enn vår
- Nyttig for menneskerettsaktivister som bruker Internett
  - kan være farlig å bli funnet
- Nyttig for å omgå geografiske sperrer/geografisk prising
  - film- og musikktjenester
  - dataspill

VPN - Typer løsninger

«Ekte» Ekte VPN, implementerer et virtuelt nettverk med kryptering, tunneller og virtuelle nettverkskort.

- Overfører alle slags nettverkstrafikk
  - Mer enn bare IP
- Kan brukes til alt

VPN - Typer løsninger

«Ekte» Ekte VPN, implementerer et virtuelt nettverk med kryptering, tunneller og virtuelle nettverkskort.

- Overfører alle slags nettverkstrafikk
  - Mer enn bare IP
- Kan brukes til alt

«Uekte» Andre løsninger som gir sikker tilgang over nett, men som ikke er VPN.

- Har begrensninger i forhold til ekte VPN
- F.eks. SSL-baserte webapplikasjoner.

VPN - Klient VPN

- Enkeltstående PCer knyttes opp mot et internt nettverk.
- Løsning for hjemmekontor og reisende.
- PC kontakter VPN-konsentrator.

VPN - Nettverk-nettverk VPN

- Hele nettverk knyttes sammen.
- Fra hvert nett når man alle tjenester i det/de andre nettverk(ene).
- Løsning for å koble sammen spredte avdelinger
- Implementeres på rutere

VPN - Problemer

- Mange ulike teknologier
- Mange ulike produkter
- VPN-teknologi er under utvikling
- Dårlig kompatibilitet mellom løsninger fra ulike leverandører
- Teknologien har egne problemer, f.eks. «hvordan formidle krypteringsnøkler og passord på sikker måte»

VPN - Problemer

- Mange ulike teknologier
- Mange ulike produkter
- VPN-teknologi er under utvikling
- Dårlig kompatibilitet mellom løsninger fra ulike leverandører
- Teknologien har egne problemer, f.eks. «hvordan formidle krypteringsnøkler og passord på sikker måte»
  - E-post er ikke spesielt sikkert

VPNløsninger - Hovedtyper

- IPSec
  - Sikkerhetsprotokoller bakt inn i IP
  - Basis for mange VPN-løsninger
  - Lite kompatibilitet mellom ulike løsninger
- Tunneller med virtuelle nettkort og SSL/TLS.
  - OpenVPN.
  - ssh-baserte opplegg
- Andre tunnelløsninger.
  - PPTP, L2TP (Probl. med både NAT og sikkerhet)
  - SSTP, erstatter de to over, følger med windows.
- Web-baserte løsninger, (uekte VPN). HTTPS mot en tjener med web-applikasjoner.

VPNløsninger - IPSec

- IETF-protokoll, utvider IP. (Opprinnelig IPv6)
- Tre hovedfunksjoner:
  - Autentisering, vi har rett avsender (AH)
  - Integritet/signatur, ingen har endret pakka (AH)
  - Konfidensialitet, innholdet er hemmelig (ESP)

AH Autentication Header, m. sjekksum

ESP Encapsulating Security Payload, krypterer pakka

VPNløsninger - IPSec, transport-/tunnell-modus

IP-pakke

IP-hode	Nyttelast

IPSec transport-modus

IP-hode	IPSec-hode	Nyttelast (kryptert hvis ESP)

IPSec tunnel-modus (VPN)

<table>
<tr><td rowspan="2">Nytt IP-hode</td><td rowspan="2">IPSec-hode</td><td colspan="2">Nyttelast (kryptert hvis ESP):</td></tr>
<tr><td>Gammelt IP-hode</td><td>Nyttelast</td></tr>
</table>

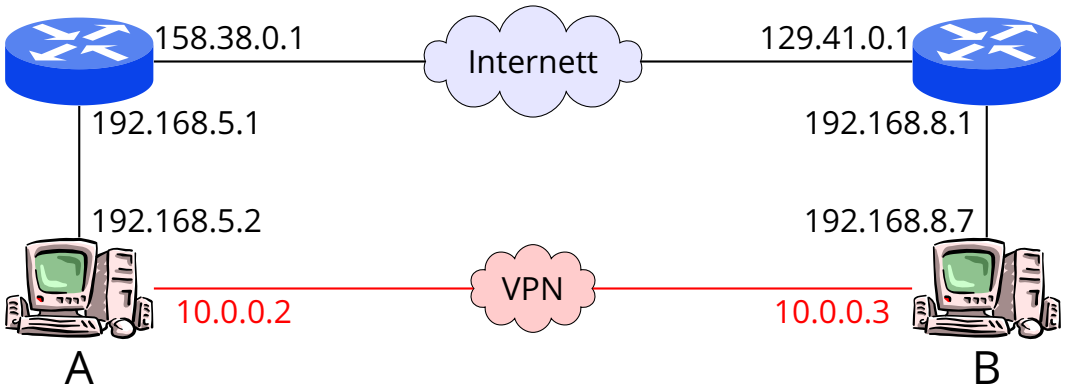
VPNløsninger - IPSec – problemer

- Komplisert å sette opp
- Kompatibilitetsproblemer
- AH fungerer ikke med NAT
- Derfor, mange andre alternativer:
  - Checkpoint VPN-1
  - Cisco VPN
  - Microsofts løsning (IPSec+L2TP)/SSTP
  - OpenVPN

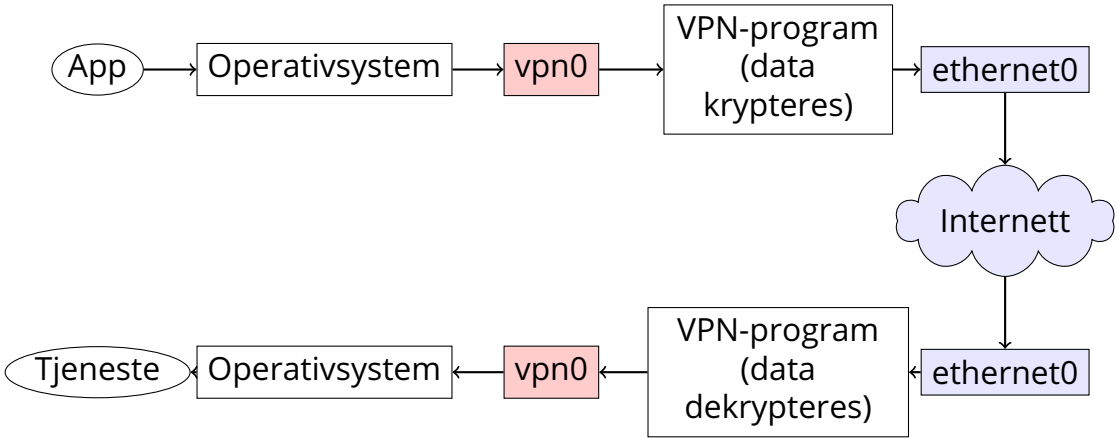
VPNløsninger - Tunnell med TLS/SSL

- Populær metode
- Enklere å sette opp
- Åpne løsninger fins
- Kan gå over UDP eller TCP
- Tunnel ved hjelp av PPP
- Kryptering ved hjelp av TLS/SSL

VPNløsninger - Tunnel, oversikt



VPNløsninger - Tunnel, detaljer



VPNløsninger - TCP eller UDP?

- Bør VPN-pakker sendes med TCP eller UDP?

VPNløsninger - TCP eller UDP?

- Bør VPN-pakker sendes med TCP eller UDP?
  - TCP har pålitelig overføring, med retransmisjon og flytkontroll
  - UDP har mindre overhead
  - En del brannmurer stopper UDP

VPNløsninger - TCP eller UDP?

- Bør VPN-pakker sendes med TCP eller UDP?
  - TCP har pålitelig overføring, med retransmisjon og flytkontroll
  - UDP har mindre overhead
  - En del brannmurer stopper UDP
- Som regel foretrekkes UDP
  - Protokoller som trenger pålitelig overføring, kjører TCP inni tunnellen

VPNløsninger - TCP eller UDP?

- Bør VPN-pakker sendes med TCP eller UDP?
  - TCP har pålitelig overføring, med retransmisjon og flytkontroll
  - UDP har mindre overhead
  - En del brannmurer stopper UDP
- Som regel foretrekkes UDP
  - Protokoller som trenger pålitelig overføring, kjører TCP inni tunnellen
  - To lag med TCP gir mer overhead, men ikke mer sikkerhet

VPNløsninger - TCP eller UDP?

- Bør VPN-pakker sendes med TCP eller UDP?
  - TCP har pålitelig overføring, med retransmisjon og flytkontroll
  - UDP har mindre overhead
  - En del brannmurer stopper UDP
- Som regel foretrekkes UDP
  - Protokoller som trenger pålitelig overføring, kjører TCP inni tunnellen
  - To lag med TCP gir mer overhead, men ikke mer sikkerhet
  - UDP-basert vpn kan virke selv om vi «roamer» mellom ulike trådløse nett

VPNløsninger - Uekte vpn

- Gir sikker tilgang, men uten å lage tunneller
- Vanligvis web-baserte løsninger med https
- Bruker ofte java/activeX når http ikke er nok
- Fordeler
  - Ingen installasjon på klientene, alle støtter https
  - NAT og brannmur går greit
- Ulemper
  - Gir ikke full tilgang
  - Begrensninger i java/activeX