Aalto-yliopisto

Tietoverkkojen turvallisuus

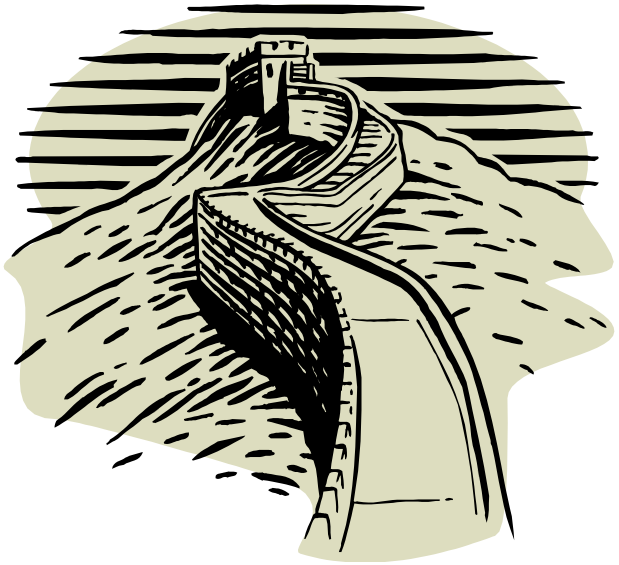
Tuomas Aura

T-110.2100 Johdatus tietoliikenteeseen
kevät 2011

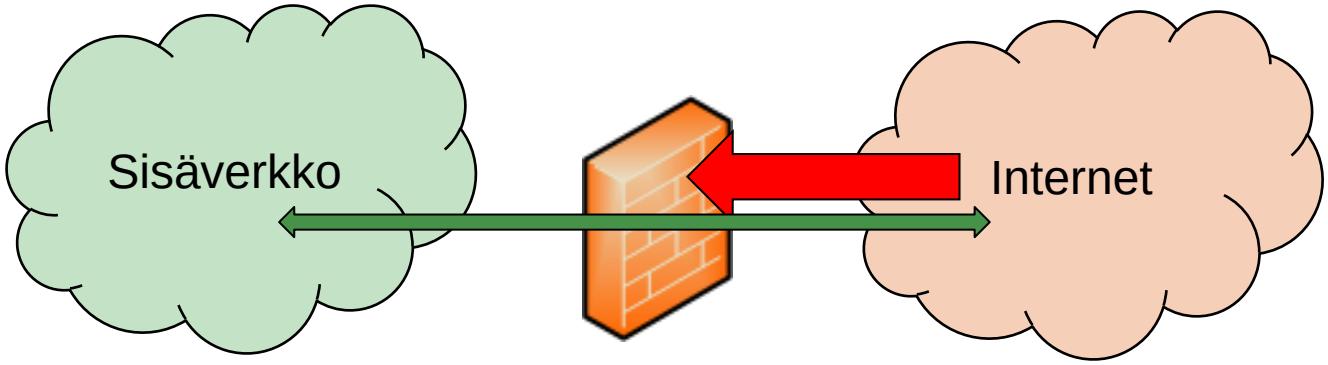
Luennon sisältö

1. Palomuurit ja rajavalvonta
   - NAT palomuurina
   - Tilaton, tilallinen ja sovellustason palomuuri
   - Julkiset palvelimet, etäkäyttö, langaton verkko
2. Tietoturvauhkien analyysi
   - Case Oodi

RAJAVALVONTA: PALOMUURIT



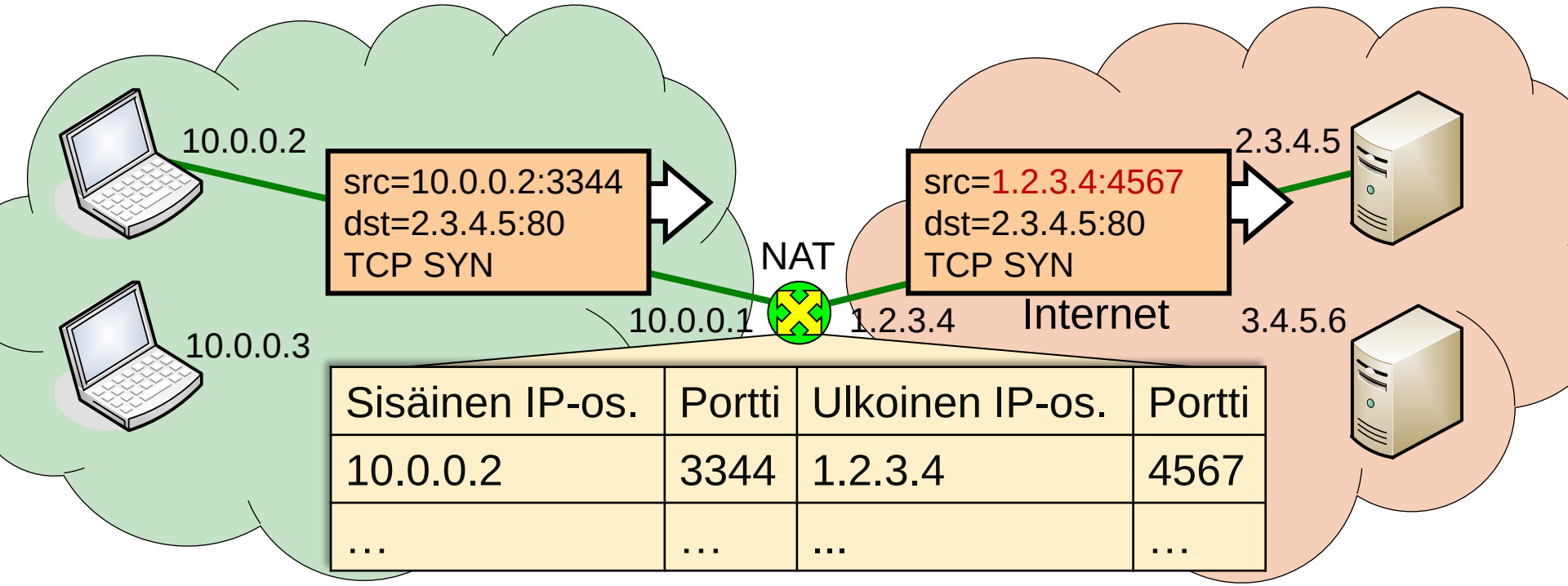
Palomuuri



- Palomuuri suodattaa liikennettä turvallisen ja turvattoman vyöhykkeen välillä
  - Sisäverkon ja Internetin välillä
  - Tietokoneen ja tietoverkon välillä
- Palomuurin tarkoitus:
  - Vähentää havoittuvuutta pienentämällä avoimia rajapintoja
  - Toteuttaa tietoturvasääntöjä
- Perinteinen turvallisuuden malli: järjestelmä jaetaan vyöhykkeisiin ja liikennettä niiden rajojen yli valvotaan *(perimeter security)*

NAT palomuurina

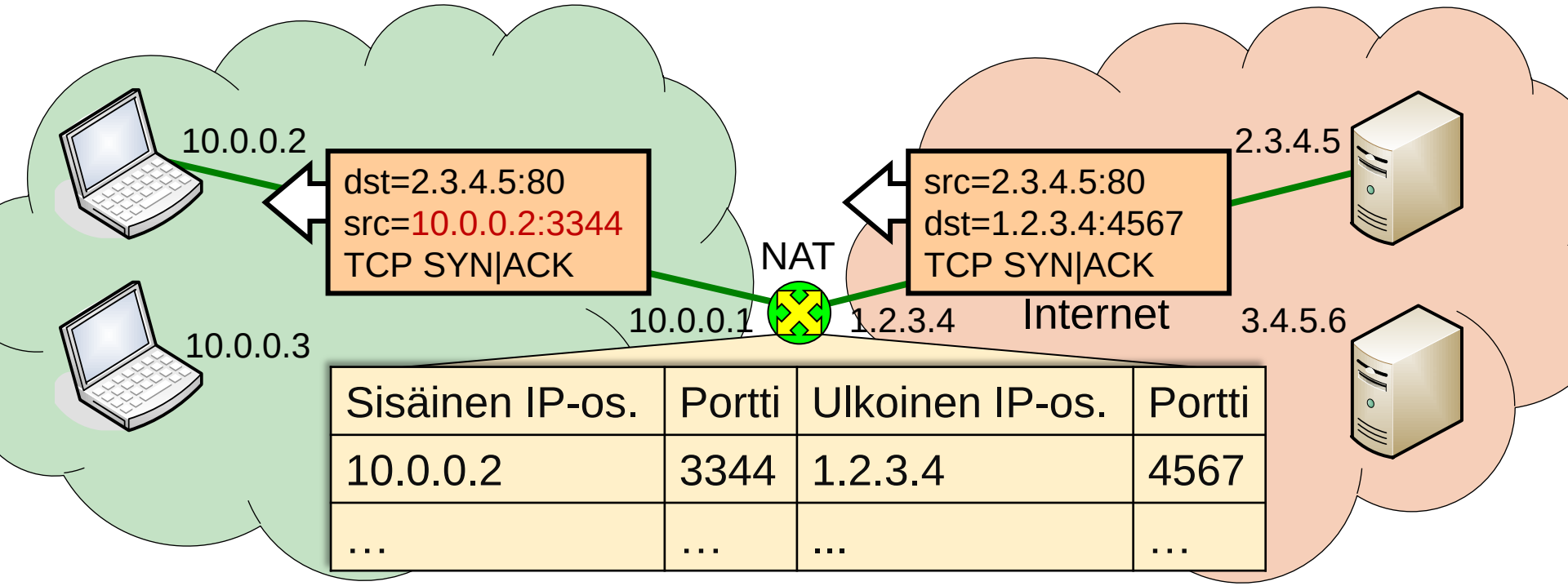
- NAT tekee muunnoksen verkon sisäisten ja ulkoisten osoitteiden välillä



yksityiset IP-osoitteet sisäverkossa → ← julkinen Internet →

NAT palomuurina

- NAT tekee muunnoksen verkon sisäisten ja ulkoisten osoitteiden välillä



Sisäinen IP-os.	Portti	Ulkoinen IP-os.	Portti
10.0.0.2	3344	1.2.3.4	4567
…	…	...	…

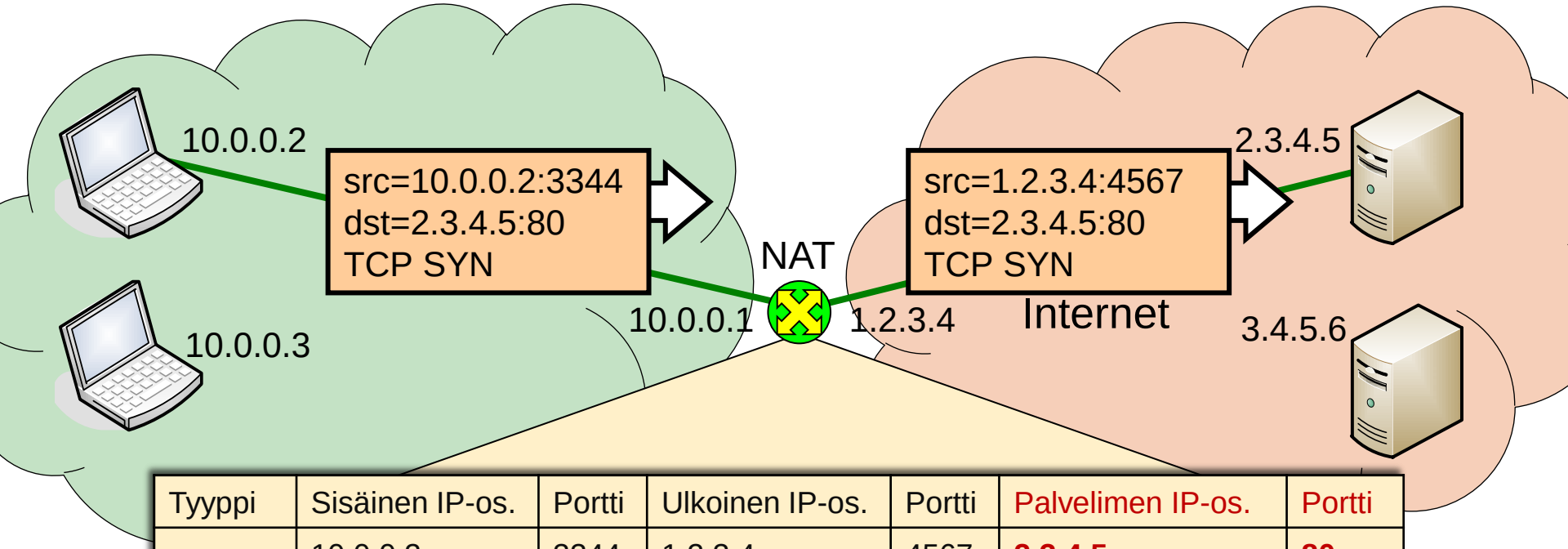
yksityiset IP-osoitteet sisäverkossa → ← julkinen Internet →

NAT palomuurina

- NAT suojaa verkkoa:
  - Piilottaa sisäverkon osoitteet ja rakenteen
  - Yhteys aloitettava (TCP SYN) sisäverkosta; Internetistä ei mahdollista luoda yhteyttä sisäverkkoon
- NAT tukee yleensä TCP ja UDP-protokollia, joskus myös ICMP:tä
  - Ensimmäinen paketti lähetettävä aina ulospäin
  - Q: Voiko hyökkääjä arvata porttinumeron ja lähettää väärennettyjä paketteja sisäverkon koneelle?

NAT palomuurina

- NAT voi sitoa yhteyden palvelimen IP-osoitteeseen ja porttiin
  - Eri NAT-toteutukset muistavat yhteydestä eri tietoja
  - Lisätieto tekee pakettien väärentämisen vaikeammaksi
- Ylläpitäjä voi avata NAT:iin pysyviä aukkoja



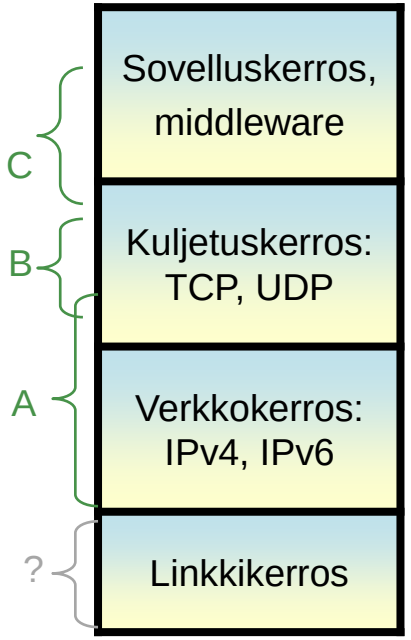
Tyyppi	Sisäinen IP-os.	Portti	Ulkoinen IP-os.	Portti	Palvelimen IP-os.	Portti
-	10.0.0.2	3344	1.2.3.4	4567	**2.3.4.5**	**80**
pysyvä	**10.0.0.3**	**80**	**1.2.3.4**	**80**	*	*

Palomuurisäännöt

- Entä jos verkossa ei ole NAT:ia?
  - ➔Reitin tai erillinen palomuuri voi silti pitää kirjaa yhteyksistä ja suodattaa niitä
- Palomuurisäännöillä verkon (tai koneen) ylläpitäjä estää ja sallii yhteyksiä
  - Yhteydet ulospäin vain tiettyihin portteihin
  - Yhteydet sisäänpäin tiettyihin koneisiin ja portteihin
- Esim:

Suunta	Protokolla	Sisäinen IP-osoite	Portti	Ulkoinen IP-osoite	Portti	Toiminto	
Ulos	TCP	10.0.0.0/24	1024–65535	*	22,80,443	Salli	SSH,HTTP,HTTPS
Ulos	UDP	10.0.0.0/24	1024–65535	*	53	Salli	DNS
Sisään	TCP	10.0.0.3	80,443	*	1024–65525	Salli	Oma web-palvelin
*	*	*	*	*	*	Estä	Oletussääntö

Palomuurityypit



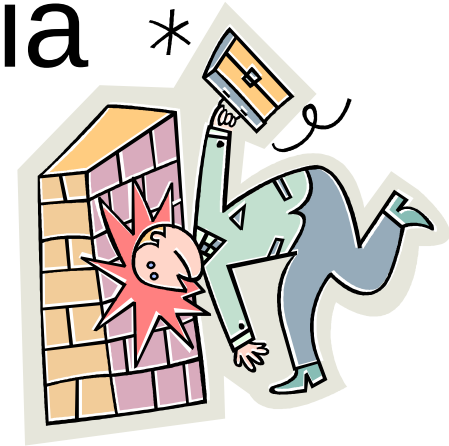
A. Tilaton palomuuri
   - Jokainen paketti käsitellään erikseen ja sallitaan tai estetään vertaamalla otsakkeita sääntöihin

B. Tilallinen palomuuri *(stateful packet inspection SPI)*
   - Tavallisin palomuurityyppi, esim. NAT
   - Palomuuri pitää kirjaa avoimista yhteyksistä

C. Sovellustason palomuuri
   1. Pakettien syvätarkastus *(deep packet inspection DPI)*
   - Palomuuri tutkii pakettien sisältöä tai rekonstruoi TCP-tavuvirran
   - Esim. URL-suodatus, virustarkistus, Internet-sensuuri
   2. Välityspalvelin *(application proxy)*:
   - Estetään palomuurisäännöillä postin välitys muiden kuin yhden SMTP-palvelimen kautta → keskitetty sähköpostin virussuodatus
   - Ohjataan ulos menevien HTTP-yhteyksien suodatus välityspalvelimella URL:n ja sisällön perusteella

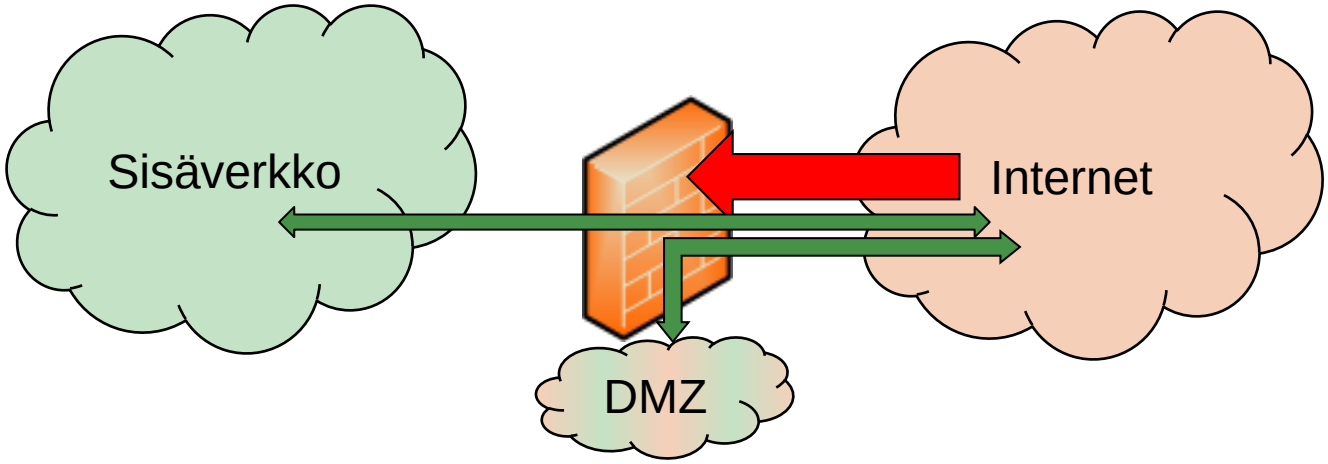
- Palomuurina toimii yleensä reititin, sovellustasolla erillinen laite

Palomuurien ongelmia *



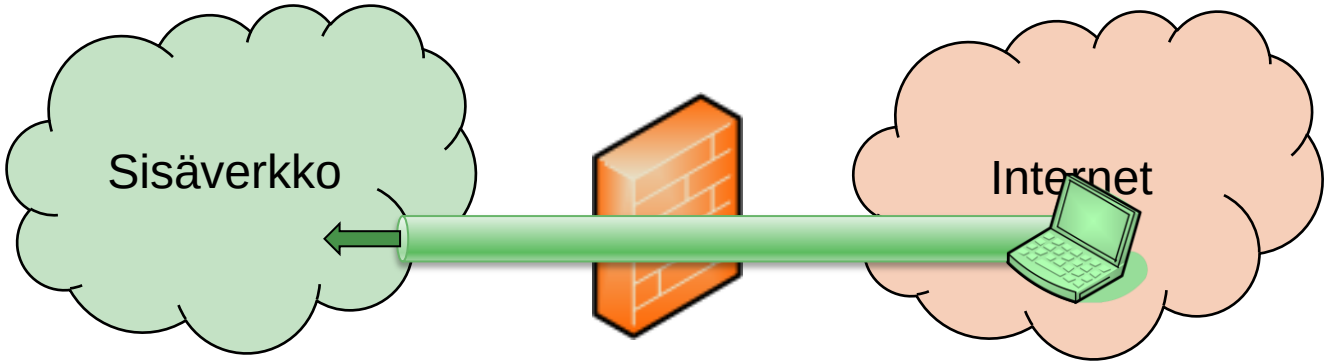
- Säännöt estävät sovellusten toimintaa
  - Palvelimet eivät toimi NAT:in tai tilallisen palomuurin takana
    → suora käyttäjien välinen kommunikaatio (esim. Internet-puhelut) vaikea toteuttaa
  - Palomuurisäntöjen muuttaminen on vaikeaa, esim. miten web-palvelin omaan koneeseesi kampuksella?
- Sovellukset kiertävät palomuurin
  - Alun perin palvelimen portti kertoi sovelluksen
  - Nykyään kaikki liikenne porteissa 80,443
    → suodattaminen mahdotonta

Palomuuri ja julkiset palvelimet



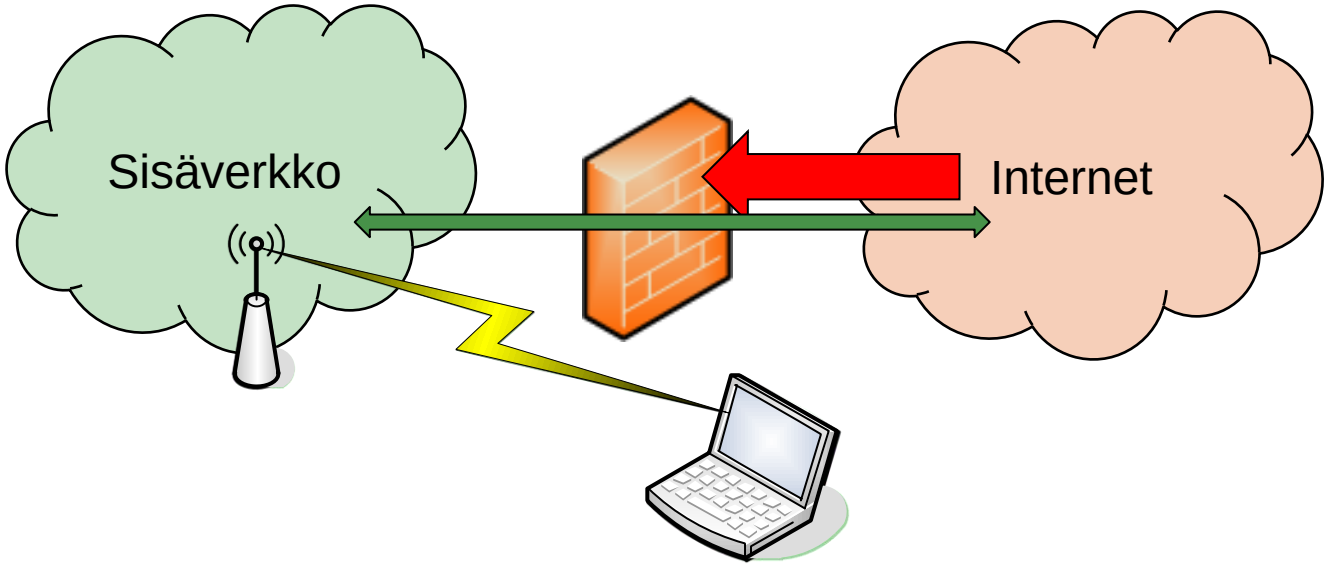
- Kuuluvatko julkiset palvelimet (esim web-palvelin) palomuurin sisä- vai ulkopuolella?
  - Tyypillisesti luodaan erillinen ”demilitarisoitu” verkkovyöhyke *(DMZ)* julkisille palvelimille

Etäkäyttöyhteydet



- Virtuaaliverkkoyhteys *(VPN):*
  - Tietokone voi kuulua loogisesti sisäverkkoon, vaikka on fyysisesti muualla
  - Kaikki paketit koneesta ohjataan salatun ja todennetun tunnelin läpi sisäverkkoon
  - Samoin useita sisäverkkoja voidaan yhdistää yhdeksi loogiseksi virtuaaliverkoksi
- Etäkäyttöyhteys suojataan kryptografialla
  - IPsec, PPTP, SSL-VPN tai SSH
  - Todennettu avaintenvaihto + datan salaus ja todennus käyttäjän koneen ja palomuurin välillä

Langaton lähiverkko



- Onko langaton lähiverkko sisäverkossa vain sen ulkopuolella?
  1. Sisällä: WLAN-tietoturvaprotokolla (WPA2) suojaa langattoman linkin kryptografialla
     → Todennettu avaintenvaihto + datan salaus ja todennus
     käyttäjän koneen ja tukiaseman välillä
     → Yhtä turvallinen kuin sisäverkon lanka-Ethernet
  2. Ulkona: esim. *Aalto Open*

Palomuurien ongelmia 2

- Edelleen reittejä palomuurin ohi:
  - Kannettavat tietokoneet kulkevat sisään ja ulos lähiverkosta
    - Windowsin palomuuria ja asetuksia voi hallita keskitetysti, mutta nykyään paljon eri järjestelmiä, puhelimia, sormitietokoneita jne.
  - Mobiililaitteet ovat samaan aikaan yhteydessä sisäverkkoon ja langattomaan Internettiin

TIETOTURVAUHKIEN ANALYYSI

Kertaus: tietoturvan tavoitteet

- Tietoturvatavoitteita:
  (*CIA = Confidentiality, Integrity, Availability*)
  - Tiedon luottamuksellisuus
  - Tiedon eheys
  - Tiedon ja palvelujen saatavuus
- Lisäksi pääsynvalvonta *(access control)*
  - Vain valtuutut tahot saavat käyttää tietoa tai palvelua
  - Esim. käyttäjän identiteetin todentaminen ja käyttöoikeuksien tarkistus
- Tällä kurssilla käsiteltyjä turvamekanismeja:
  - Kryptografia — todennettu avaintenvaihto, datan salaus ja todennus
  - Turvavyöhykkeet ja rajavalvonta

Tietoturvan suunnittelu

- Organisaation tai järjestelmän tietoturvan suunnittelu:
  - Tunnistetaan suojattava tieto-omaisuus
  - Tunnistetaan uhkat: fyysiset, tietotekniset ja sosiaaliset → mitä pahaa voi tapahtua? kuka?
  - Tehdään riski-analyysi: vahinkojen suuruus ja todennäköisyys, uhkien priorisointi
  - Päätetään suojauksen tavoitteet
  - Päätetään suojauksen keinot: tekniset suojaukset, prosessit, vastuut ja resurssit
- Tietoturva on jatkuva prosessi:
  - Turvatilannetta on valvottava; suojauksia päivitetään uhkien muuttuessa

Uhka-analyysi

- Esimerkki: opintorekisteri
  - Mitä suojeltavaa tietoa?
  - Mitä uhkia,
    kuka on hyökkääjä?
  - Uhkien priorisointi?
- Käytitkö ensin CIA-mallia?
  Riittääkö se?
- Muistitko sisäpiirin uhkat?

Opintorekisteri

Huom! Tämä on vain yksi näkemys ja uhkakuvat voivat muuttua

- Suojeltava omaisuus:
  - Opintosuoritukset, opiskelijoiden henkilötiedot
- Uhkat:
  - Henkilötietojen vuotaminen (julkisuuslain mukaan julkista!)
  - Tiedon luvaton muokkaaminen, esim. väärennetyt suoritukset
    - Luvaton pääsy tietokantaan ylläpitäjän tunnuksella
    - Rekisterin ylläpitäjän salasanan kuuntelu
    - Palvelinohjelmistojen heikkouksien hyväksikäyttö
    - Sosiaalinen hakkerointi
    - Ylläpitäjän rekisteriin siirtämän datan muokkaus verkossa
  - Suoritustiedon tuhoutuminen
    - Voiko ylläpitäjä poistaa tietoa?
  - Palvelun saatavuuden häiriöt
- Keskeiset tavoitteet:
  - Pääsynvalvonta etenkin tiedon poistolle ja kirjoittamiselle
  - Rekisterin ylläpitäjien todentaminen, salasanan ja datan suojaus
  - Opiskelijakäyttäjän todentaminen
  - Ohjelmistojen luotettavuus

3. Harmillista ja todennököistä

1. Tärkeää ja todennäköistä

4. Melko epätodennäköistä

1. Kriittistä vaikka harvinaista

3. Harmillista ja yleistä