Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

IIRO KURONEN

# Tietoturva hajautetussa automaatioratkaisussa

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN
KOULUTUSOHJELMA
2020

Tekijä
Kuronen, Iiro

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
05/2020

Sivumäärä
40
Liitteitä
-

Julkaisun kieli
Suomi

Julkaisun nimi
**Tietoturva hajautetussa automaatioratkaisussa**

Tutkinto-ohjelma
Sähkö- ja automaatiotekniikan koulutusohjelma

Teknologian jatkuva kehitys luo uusia haasteita sekä hyötyjä teollisuudelle. Energia- ja tuotantotehokkuutta yritetään jatkuvasti parantaa, jolloin tarvitaan paljon dataa teollisuuslaitteilta, jotta pystytään ennaltaehkäisemään vikatilanteita sekä nopeasti korjaamaan ne. Laitteilta kerätty data on myös pidettävä turvassa vääriltä tahoilta.

Opinnäytetyö tehtiin Satmatic Oy:lle. Työssä tutkittiin, miten turvallinen tiedonsiirto toteutuu eri laitevalmistajien laitteissa. Työssä otettiin huomioon Siemensin, Phoenix Contactin sekä Tosiboxin laitteiden kanssa saavutettavat etäkäyttö ratkaisut.

Tavoitteena oli oppia miten turvallinen ja luotettava tiedonsiirtoväylä saadaan aikaan ja mitä eri ratkaisu vaihtoehtoja laitevalmistajilla on. Työssä perehdyttiin teoriaan mitä tietoturva ja kyberturvallisuus tarkoittaa ja miten turvallinen tiedonsiirto toteutetaan tekniikaltaan.

Asiasanat
virtuaaliset yksityisverkot, tietoturva, palomuuri, etäkäyttö, automaatio

Author
Kuronen, Iiro

Type of Publication
Bachelor's thesis

Date
05/2020

Number of pages
40
Appendices
-

Language of publication:
Finnish

Title of publication
**Data security in decentralised automation solution**

Degree program
Degree Programme in Electrical and Automation Engineering

Technology develops continuously and because of this it will create new challenges and advantages to the industry. An attempt is made continuously to improve energy efficiency and production efficiency in which case much data is needed from the industry devices so that it is possible for to prevent fault situations and to fix them quickly. The data that has been collected from the devices must also be kept in the protection from the wrong parties.

The thesis was made to Satmatic Oy. The purpose of the thesis was to study how the safe data transfer will be implemented in the different component manufacturers' devices. Siemens, Phoenix Contact and Tosibox's remote access devices were dealt with in this thesis.

The objective was to learn how safe and reliable data transfer is and what kind of different solution alternatives the component manufacturers have. Theory about data security and the cyber security will be studied in the work and how safe data transfer is carried out from technical point of view.

Key words
virtual private network, data security, firewalls, remote access, automation

# SISÄLLYS

KÄYTETYT TERMIT JA LYHENTEET

| | |
|---|---|
| Brute-force | Raakahyökkäys, kryptoanalyysihyökkäys, jossa yritetään järjestelmällisesti yrityksen ja erehdyksen kautta kokeilemalla löytää oikea salasana tai salausavain |
| VPN | Virtual Private Network, virtuaalinen erillisverkko |
| GRE | Generic Routing Encapsulation, tunnelointiprotokolla, joka voi kapseloida laajan valikoiman verkkokerrosprotokollapakettityyppejä IP-tunnelien sisään |
| Site-to-Site | Erilliset verkot yhdistävä VPN-yhteys |
| AH | Authentication Header, autentikointiotsake, IPsec:in pakettivirtojen suojaamiseen käyttämä protokolla |
| ESP | Encapsulating Security Payload, IPsec:in pakettivirtojen suojaamiseen käyttämä protokolla |
| IPsec | IP Security, joukko TCP/IP-pinoon kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen |
| HMAC | Hash-based Message Authentication Code, tietojärjestelmän eheys algoritmi |
| PSK | Pre-Shared Key, ennalta jaettu salausavain |
| RSA | Rivest, Shamir, Aldeman, nimi tulee heidän sukunimiensä alkukirjaimista (RSA), julkisen avaimen salausalgoritmi |
| TLS | Transport Layer Security, salausprotokolla |

| | |
|---|---|
| NAT | Network Address Translation, osoitteenmuunnos |
| UDP | User Datagram Protocol, yhteydetön viestinvälitysprotokolla |
| TCP | Transmission Control Protocol, yhteydellinen viestinvälitysprotokolla |
| ACL | Access Control List, käyttöoikeusluettelo, käyttöoikeusmerkintöjen järjestetty luettelo |
| ACE | Access Control Entry, käyttöoikeusmerkintä |

# 1 JOHDANTO

Teknologia kehittyy jatkuvasti ja se luo uusia haasteita sekä hyötyjä teollisuudelle. Energia- ja tuotantotehokkuutta yritetään jatkuvasti parantaa, jolloin tarvitaan paljon dataa teollisuuslaitteilta, jotta pystytään ennaltaehkäisemään vikatilanteita sekä nopeasti korjaamaan ne. Laitteilta saatava data on pidettävä turvassa vääriltä tahoilta.

Opinnäytetyön tarkoituksena on tutkia, miten turvallinen tiedonsiirto toteutuu. Työssä otetaan huomioon Siemensin, Phoenix Contactin sekä Tosiboxin laitteiden kanssa saavutettavia ratkaisuja. Eri laitevalmistajilla on omia pieniä erikoisominaisuuksia, jotka erottavat ne muista ja luovat kilpailua, kuitenkin ratkaiseva tekijä useasti on kustannus tehokkuus ja käyttäjäystävällisyys.

Tietoturva ja kyberturvallisuus ovat kohtalaisen uusia käsitteitä. Arkaluontoista tietoa henkilöistä, tunnuksista, laitteista jne. ei saa joutua vääriin käsiin, koska se voi vahingoittaa henkilöitä tai jopa aiheuttaa liiketoiminnan päättymisen. Siksi on tärkeä perehdyttää kaikki siihen, miten tietoturva riskiä voidaan pienentää, jotta kyseisiä asioita ei pääse tapahtumaan.

# 2 SATMATIC OY

Satmatic Oy on yksi Suomen johtavista sähkö- ja automaatiotekniikan rakentajista. Ulvilassa ja Keravalla työskentelee lähes 100 henkilöä. Lisäksi Satmaticiin kuuluu Kurikassa toimiva Suomen johtava muuntamovalmistaja Finnkumu Oy.

Satmatic Oy on osa pörssiyhtiö AS Harju Elekteriä, joka on perustettu vuonna 1968 ja on nykyään yksi suurimmista sähkö- ja automaatiotekniikan rakentajista Itämeren alueella. Koko konsernissa työskentelee noin 500 alan ammattilaista.

Satmatic Oy tukee asiakkaiden menestystä, täyttää lupaukset ja panostaa pitkäjänteiseen yhteistyöhön. Satmatic Oy työskentelee sekä sopimusvalmistusperiaatteella että projektiluonteisesti. Palvelut kattavat asiakkaan haluaman laajuuden, esisuunnittelusta huoltoon. (Satmatic Oy:n www-sivut. 2020.)

# 3 TIETOTURVA

Digitaalinen maailma muuttuu valtavalla vauhdilla. Uudet viestintäteknologiat avaavat uusia mahdollisuuksia, mutta niitä käyttämällä voi altistaa itsensä ja muut riskeille. Monet aliarvioivat nämä riskit. Myös suhteellisen vapaissa maissa verkkosurffailijan tietoja voidaan väärinkäyttää muiden toimesta. Väärinkäyttäjiä voivat olla yritykset, hallitukset tai yksittäiset hakkerit. Joskus tietoja voidaan käyttää väärin myös vahingossa.

Tietoturva tarkoittaa nimensä mukaisesti tiedon turvaamista esimerkiksi yritysten tiedostot, sähköpostit, pankkitunnukset ja salasanat. Tietoturvalla tarkoitetaan myös toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudella tarkoitetaan, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Eheydellä tarkoitetaan, että vain tietoon oikeutetut voivat muuttaa niitä. Käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla käyttöön oikeutetuilla silloin kun sitä tarvitaan.

Jokaisen on hyvä miettiä mikä turvallisuus taso on hyvä itselle, tavallinen verkon käyttäjä ei välttämättä tarvitse yhtä tiukkaa tietoturvaa kuin henkilö, joka käsittelee arkaluontoisempia tietoja. Usein ajatellaan, että tietojen turvaamiseksi riittää vain hyvä salasana, mutta se ei pidä paikkaansa. Kun lähetät esimerkiksi sähköposteja niin niihin voi joku väärä taho päästä käsiksi. Tietomurto voi tapahtua, vaikka kun lataan puhelimeesi tai tietokoneellesi ohjelmia verkosta tai avaat verkkosivuilla erilaisia linkkejä tai mainoksia. Kannattaa siis tutustua verkkosivuun ja arvioida sivun luotettavuus ennen kuin tekee mitään. (Traficomin www-sivut. 2020.)

## 3.1 Tietoturvan uhat

Tietoturvan uhkina pidetään erilaisia huijausyrityksiä, henkilökohtaisen yksityisyyden loukkauksia, vanhentuneet tietokoneohjelmat, roskapostia, teollisuusvakoilua, piratismia, viruksia, verkkoterrorismia. Tietoturvauhkia ovat luvaton pääsy, tiedon luvaton käyttö, salaisen tiedon paljastuminen, tiedon sekaannus, tiedon muuntuminen, salaisen tiedon tutkituksi tuleminen, tiedon kopioituminen ja tiedon hävittäminen. Suurin osa

tietoturvan uhista voi tapahtua, jos salasanan suojaus taso on liian matala. Tietoturva uhkia on myös itse ihmiset ja heidän tekemät virheet/laiminlyönnit.

## 3.2 Tietoturva uhkien torjuminen

Suuri osa tietoturvan uhista voi tapahtua, jos salasanan suojaus taso on liian matala, siksi salasanan kannattaa sisältää tarpeeksi paljon merkkejä ja erikoismerkkejä. On suotavaa, että vaihtaa salasanan aina muutaman kuukauden välein tai aina kun on kohdannut mahdollisesti tietoturva uhan mahdollisuuden. Suurin tietoturvariski yritykselle/organisaatiolle on sen omat työntekijät.

Vastuu tietoturvasta on lopulta melkein aina itse käyttäjillä. Tietoturvaohjelmat ja erilaiset sovellutukset auttavat parantamaan tietoturvaa tiettyyn pisteeseen asti, mutta käyttäjien pitää olla myös perillä asioista. Tekniset tietoturvaratkaisut eivät välttämättä estä ihmisten tekemiä virheitä, siksi on tärkeä kouluttaa henkilöstö oikeanlaiseen tietoturvaan. (Traficomin www-sivut. 2020.)

# 4 KYBERTURVALLISUUS

Kyberturvallisuus kattaa tietoturvallisuuden kentästä nimenomaan verkkojen kautta tehtävät tietomurrot, ei niinkään fyysistä tasoa, jossa joku varastaisi, vaikka tietokoneen. Tämän lisäksi kyberturvallisuus liittyy erityisesti myös tietojärjestelmien varassa toimivan infrastruktuurin turvallisuuteen. Hyviä esimerkkejä ovat sähköverkkojen ohjausjärjestelmät, teollisuuslaitosten automaatiojärjestelmät ja tulevaisuudessa esimerkiksi autonomiset ajoneuvot.

Kyberturvallisuus on suhteellisen uusi ja sisällöltään vielä vakiintumaton termi. Käytännössä sillä viitataan organisaatioiden ja yhteiskunnan digitalisoitumisen aiheuttamiin uudenlaisiin turvallisuushaasteisiin. Kyberturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla organisaatio suojaa liiketoiminnassa tarvittavat järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet kyberuhkilta. Kyberuhkat ovat haitallisia tapahtumia, jotka voivat vaikuttaa organisaation toimintaan, talouteen, sen hallussa olevaan tietoon ja pahimmillaan jopa liiketoiminnan jatkuvuuteen. (Traficomin www-sivut. 2020.)

## 4.1 Kyberturvallisuus yrityksessä

Yritykset ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä. Samalla niihin kohdistuvat kyberuhkat lisääntyvät jatkuvasti. Tietoturva ei ole enää vain tekninen ongelma, vaan se tulee nostaa omistajien agendalle, osaksi yrityksen riskienhallintaa. Hyvin rakennettu kyberturvallisuus suojaa yrityksen toimintakykyä ja varmistaa, että liiketoiminnassa voidaan hyödyntää digitaaliteknologian tarjoamia hyötyjä täysimääräisesti. Tämän vuoksi myös yritysten hallitusten jäsenillä tulee olla riittävät tiedot kyberturvallisuudesta ja siihen liittyvistä liiketoimintariskeistä.

Kaikissa yrityksissä tietoja käsitellään ja välitetään sähköisesti tietoverkkojen avulla tämän vuoksi pitää ottaa huomioon, että myös verkkorikolliset hyödyntävät tietoverkkoja. Rikollisten motiivit ja taustat vaihtelevat, ne voivat olla organisoidusta rikosjärjestöstä tai nuoria tietokoneharrastajia. Koska kyberrikollisuus aiheuttaa monenlaisia uhkia yritykselle, vakavia ja vähemmän vakavia, on tärkeä ulkoistaa tekninen

osaaminen ulkopuoliselle ammattilaiselle, jos yrityksellä ei ole tarvittavaa osaamista. (Traficomin www-sivut. 2020.)

## 4.2 Kyberhyökkäykset

Tässä työssä keskitytään teollisiin kohteisiin. Kyberhyökkäyksiä tehdään yrityksiin laitetasolle kuten valvonta kameroihin ja hallinto tasolle kuten sähköposteihin ja salasanoihin häiritäkseen yrityksen toimintaa ja kalastellakseen tietoja. Hyökkääjät voivat olla valtiot, kyberkriminaalit, terroristit, kilpailijat, entiset työntekijät ja hakkerit. Hyökkäykset kohdistuvat eniten energian tuotanto alalle ja sähköverkkoon sekä veden käsittelyyn, mutta myös esimerkiksi koteihin, toimistoihin ja erilaisiin tuotanto laitoksiin kuten juomien.

Hyökkäykset toteutetaan usein kohdennetusti esimerkiksi jonkun työntekijän sähköpostin salasanaan Brute force:lla. Hyökkäyksen kohteina hyvin usein on myös eri toimilaitteet tehtaissa tai toimistoissa, ne voivat olla mitä vain internettiin kytkettyjä laitteita ohjelmoitavat logiikat, robotit, tulostimet, tietokoneet. Yksi suurimmista kyberhyökkäyksistä tapahtui amerikkalaisessa energiantuotanto laitoksessa, se sai alkunsa sähköpostiin lähetetystä epäaidosta Dropbox-linkistä. (Davor, T. 2020. HMS Cyber Security)

## 4.3 Hyökkäysten torjuminen

Laitevalmistajilla on ainainen kilpajuoksu kyberuhkia vastaan niiden torjumiseksi. Tuotekehittäjien haasteita ovat laitteiden jatkuva kehitys langattomuuteen ja monipuoliseen kommunikointiin eri tasoilla samanaikaisesti. Koska laitteiden moni ulottuvuus kasvaa koko ajan niin ohjelmistojen koko ja eri käyttöliittymien kirjo kasvaa koko ajan, jolloin laitteen vaadittava suoritusteho kasvaa. Kun laitteista tulee koko ajan moniulottuvaisempia niin niiden turvallisuutta on hyvin vaikea toteuttaa. Laitteet ovat myös entistä enemmän internet yhteydellä varustettuja, jolloin niiden ominaisuuden ja haavoittuvuudet voi löytää kuka vain internetin välityksellä.

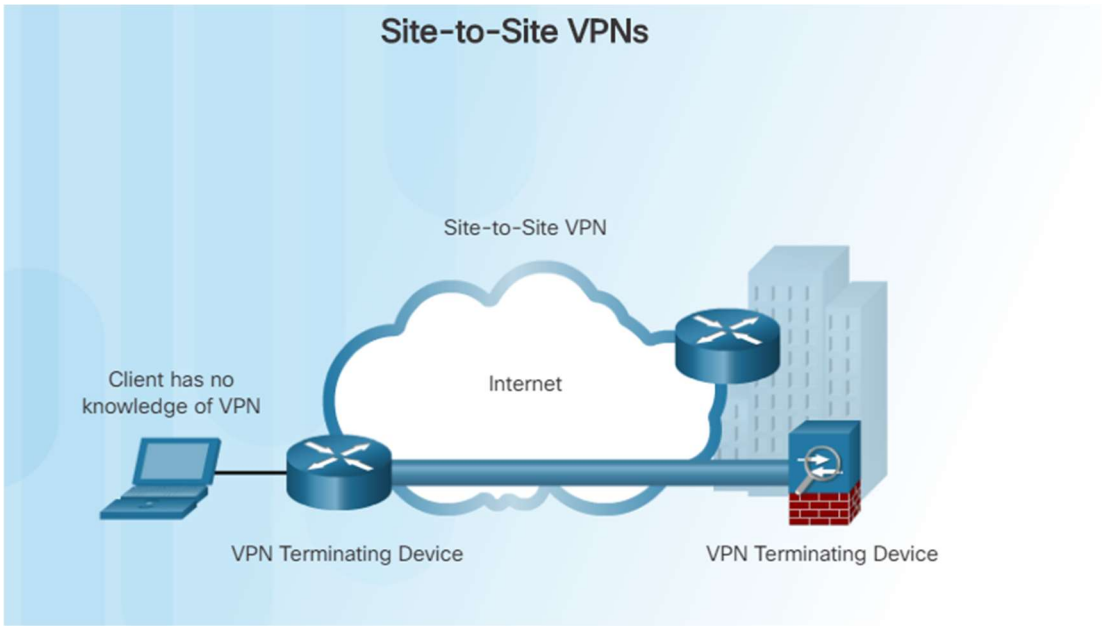
Esimerkkejä eri tekijöistä ohjelmiston haavoittuvuuteen: puuttuva eheys, ylikuormitus, vanhentunut ohjelmisto, puuttuva todennus. Laitteen turvallinen elinkaari saavutetaan ajantasaisilla päivityksillä, tiedottaminen havaituista haavoittuvuuksista, käyttämällä vain turvalliseksi todettuja komponentteja ja antamalla laitteen haltijalle teknistä tukea tarvittaessa. Laitteisto tasolla kyberhyökkäyksiä torjutaan laitteen sisäänrakennetulla ohjelmistolla ja tekniikalla. Laitteesta lähtevää ja saapuvaa liikennettä suojataan kyberhyökkäyksiltä palomuureilla ja VPN tekniikalla. (Davor, T. 2020. HMS Cyber Security)

# 5 VPN

Organisaatiot käyttävät VPN-verkkoja (Virtual Private Network) luomaan päästä päähän ulottuvan yksityisverkkoyhteyden kolmannen osapuolen verkkojen kautta kuten internetin. VPN on yksityinen, koska liikenne salataan pitämään datan luottamuksellisena, kun sitä kuljetetaan julkisen verkon läpi. VPN:t käyttävät tunnelia mahdollistaakseen etäkäyttäjille päästä keskeisiin sivustoverkkoresursseihin. Ensimmäiset VPN:t olivat ainoastaan IP-tunneleita, jotka eivät sisältäneet datan todentamista tai salausta. Esimerkiksi yleinen reititys kapselointi (GRE) on tunnelointiprotokolla, joka voi kapseloida laajan valikoiman verkkokerrosprotokollapakettityyppejä IP-tunnelien sisään. Tämä luo virtuaalisen site-to-site linkin reitittimiin etäisissä pisteissä IP-verkossa. Kuitenkaan pelkät VPN:t eivät voi taata, että tieto pysyy turvassa kulkiessaan tunnelin poikki. Tästä syystä nykyaikaisia kryptografisia menetelmiä sovelletaan VPN:iin luomaan turvallinen, päästä päähän ulottuva, yksityisverkkoyhteys. (Cisco Networking Academy. 2020.)

## 5.1 Site-to-site VPN

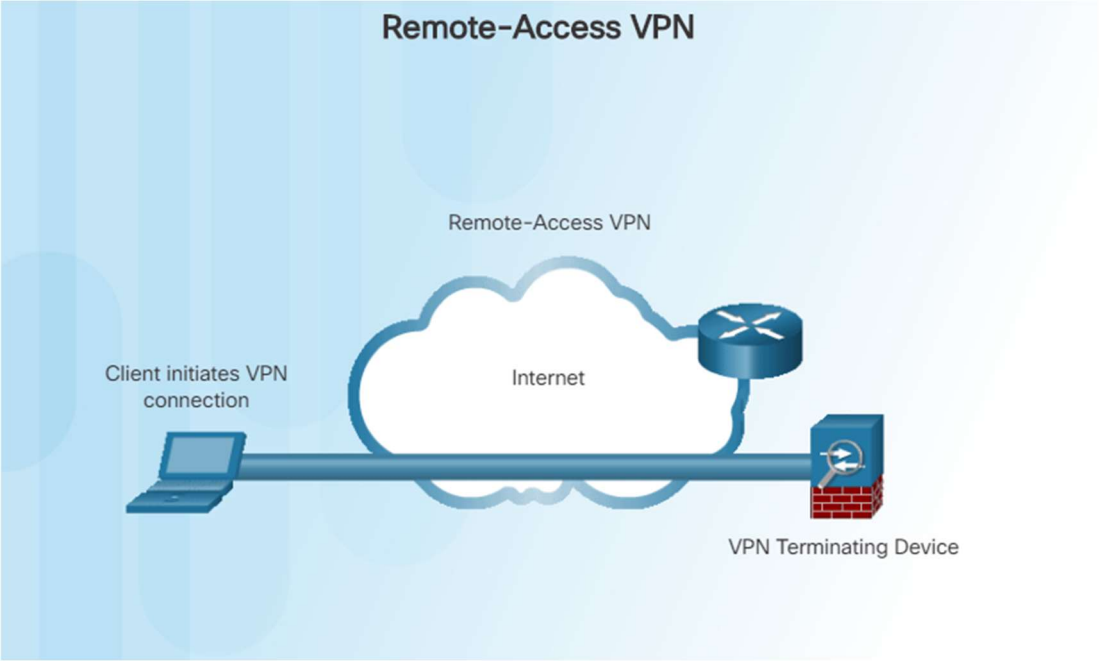
Site-to-site VPN luodaan, kun VPN-yhteyden kummallakin puolella laitteet ovat tietoisia VPN-kokoonpanosta etukäteen. VPN pysyy staattisena, ja sisäisillä isännillä ei ole yhtään tietoa, että VPN on olemassa. Site-to-site välisessä VPN:ssä isännät lähettävät ja vastaanottavat normaalia TCP/IP-protokolla-liikennettä VPN-yhdyskäytävän välityksellä, joka voi olla reititin, palomuuri, VPN-keskitin, tai ASA. VPN-yhdyskäytävä on vastuussa lähtevän liikenteen kapseloimisesta ja sen salaamisesta tietystä asemasta ja lähettämisestä VPN-tunnelin välityksellä internetin kautta vertais VPN-yhdyskäytävälle toiselle asemalle. Vastaanotossa vertais VPN-yhdyskäytävä purkaa otsikot, avaa sisällön ja välittää pakettia kohdeisäntää kohti sen yksityisverkon sisällä. (Cisco Networking Academy. 2020.)




Kuva 1. Site-to-site VPN (Cisco Networking Academy 2020)

## 5.2 Remote-access VPN

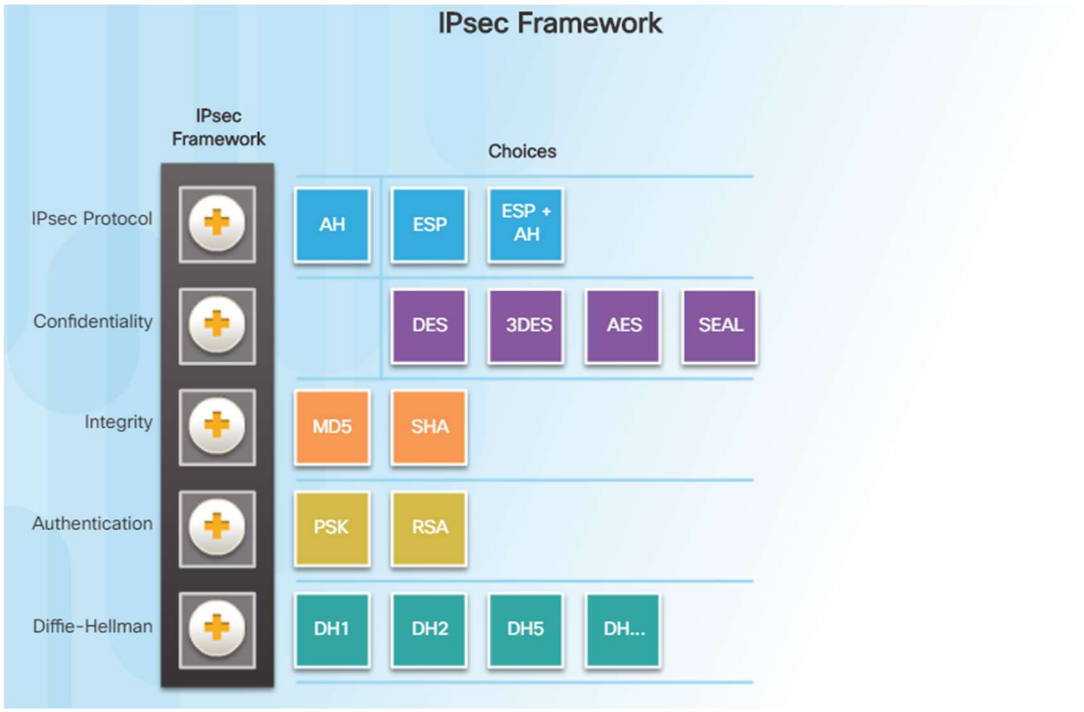
Etäkäyttö-VPN luodaan, kun VPN-tietoa ei ole staattisesti asetettu vaan sen sijaan sallii dynaamisesti vaihtaa yhteys tietoa, joka voidaan sallia ja poistaa käytöstä tarvittaessa. VPN:ien saapumisen avulla etäkäyttäjä yksinkertaisesti tarvitsee pääsyä internetiin kommunikoidakseen keskustoimiston kanssa kuten näytetty kuvassa. Etäkäyttäjien tapauksessa niiden internetyhteys on tyypillisesti laajakaistayhteys. Etäkäyttäjällä ei välttämättä aina ole VPN-yhteys ylhäällä. Etäkäyttäjän PC on vastuussa VPN:n luomisesta. Tieto, jota tarvitaan muodostamaan VPN-yhteys, kuten etäkäyttäjän IP-osoite, muuttuu dynaamisesti riippuen etäkäyttäjän sijainnista silloin kun yhteyttä yritetään. (Cisco Networking Academy. 2020.)



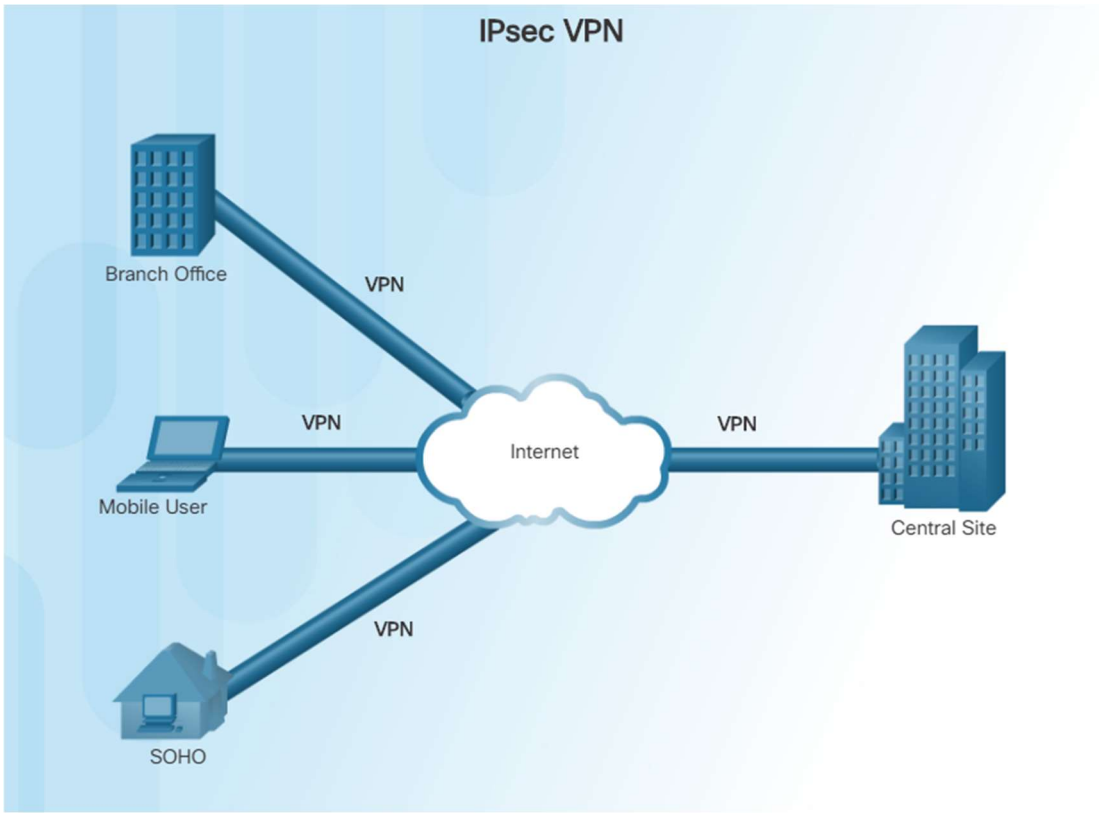

Kuva 2. Remote-access VPN (Cisco Networking Academy 2020)

## 5.3 IPsec-protokolla

IPsec on sarja protokollia, jotka on kehitetty IETF:n tuella saavuttamaan turvalliset palvelut IP-paketti kytkentäisille verkoille. IPsec:in kaksi pääprotokollaa ovat Authentication header (AH) ja Encapsulation Security Protocol (ESP). IP-turvallisuus (IPsec)-protokolla tarjoaa puitteita turvallisten VPN:ien konfiguroimista varten. Se on luotettava tapa ylläpitää viestinnän yksityisyyttä virtaviivaistaessaan operaatioita, vähentäen kustannuksia ja sallien joustavan verkkohallinnon. IPsec on IETF-standardi (RFC 2401-2412), joka määrittelee, miten VPN on turvallistettu yli IP-verkkojen. IPsec suojaa ja todentaa IP-paketteja lähetyksen ja vastaanoton välillä. IPsecin palvelut sallivat todentamisen, eheyden, pääsynvalvonnan ja luottamuksellisuuden. IPsecin kanssa tieto, jota on vaihdettu etäsijaintien välillä, voi olla salattu ja varmennettu. Sekä etäkäyttö (remote-access) että usean paikan (site-to-site) väliset VPN:t voidaan ottaa käyttöön käyttäen IPsec:iä. (Cisco Networking Academy. 2020.)



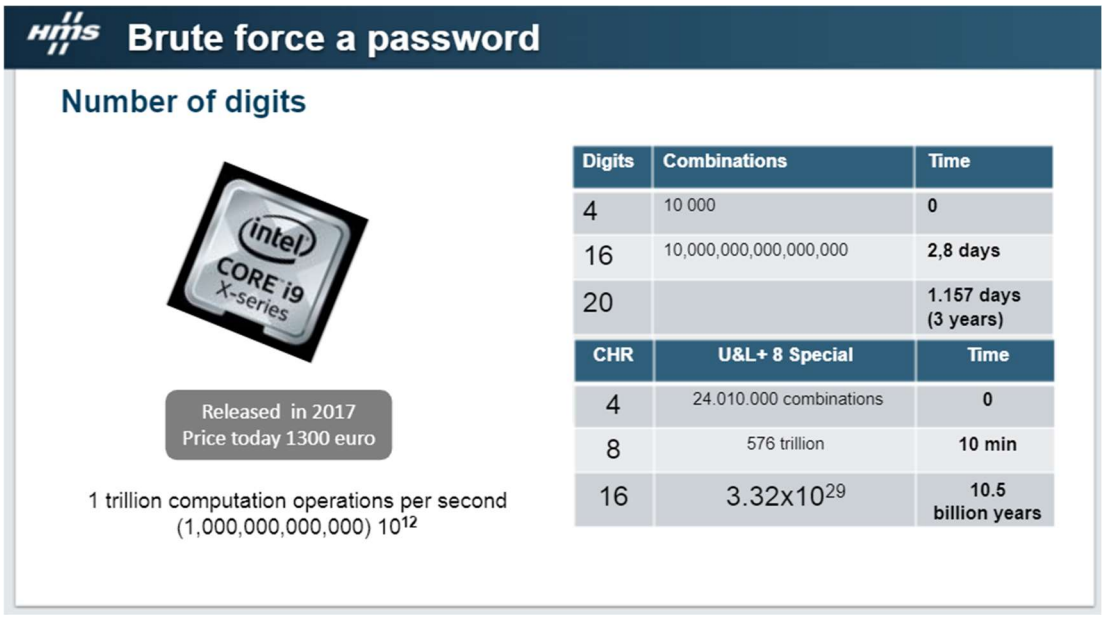

Kuva 3. IPsec rakenne (Cisco Networking Academy 2020)



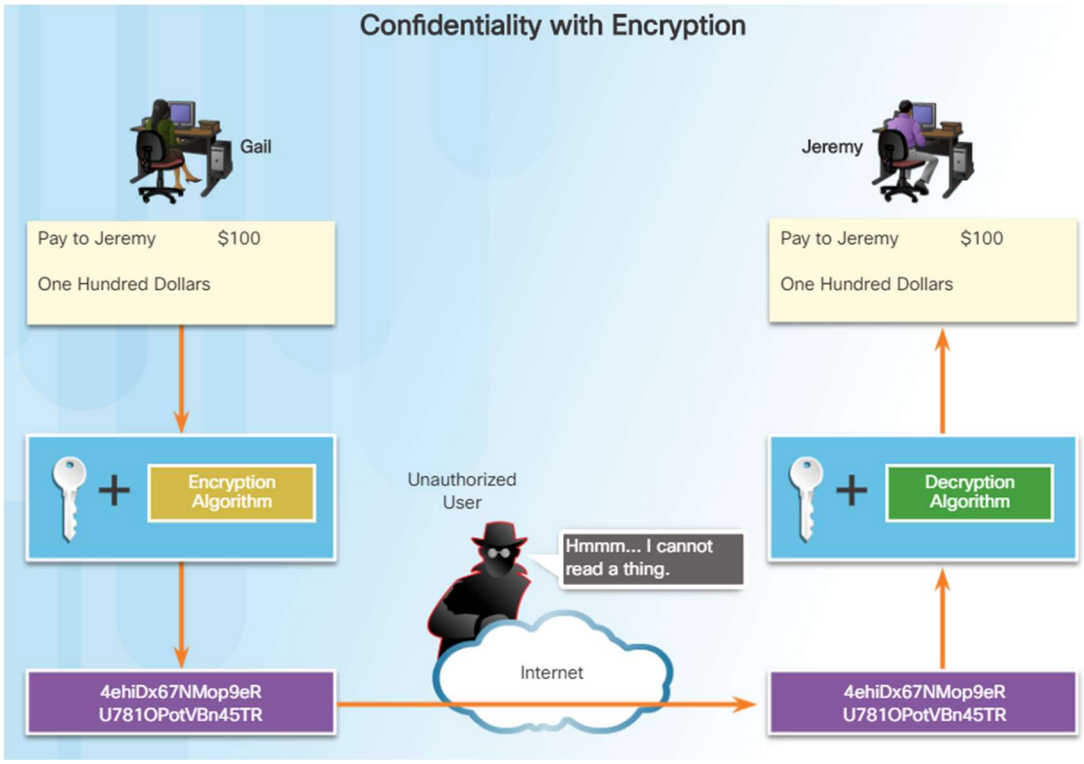

Kuva 3. IPsec VPN (Cisco Networking Academy 2020)

### 5.3.1 Encryption, salaus

Luottamuksellisuus saavutetaan salaamalla data kuten näytetty kuvassa 1. Turvallisuuden aste riippuu käytetyn avaimen pituudesta salausalgoritmissa. Jos joku yrittää hakkeroida avaimen brute-force hyökkäyksellä, mahdollisuuksien lukumäärä yrittää on avaimen pituuden funktio. Aika käsitellä kaikkia mahdollisuuksia on hyökkäävän laitteen tietokoneen tehon funktio. Mitä lyhyempi avain, sitä helpompaa on rikkoa. 64-bittinen avain voi tarvita suunnilleen yhden vuoden murtuakseen suhteellisen pitkälle kehitetyllä tietokoneella. Samalla koneella 128-bittinen avain voi tarvita suunnilleen 10^19 vuotta murtaa. (Cisco Networking Academy. 2020.)




Kuva 4. Salasanan merkkien määrän vaikutus salasanan vahvuuteen (Davor, T. 2020. HMS Cyber Security)




Kuva 5. Luottamuksellisuus saavutetaan salauksella (Cisco Networking Academy 2020)

### 5.3.2 Integrity, eheys

Tietojärjestelmän eheys tarkoittaa, että data, joka vastaanotetaan, on juuri sama data, joka lähetettiin. Potentiaalisesti dataa voitiin siepata ja muuttaa. Esimerkiksi, kuvassa 1, olettaa, että sekki 100 dollarille on kirjoitettu Alexiin. Sekki postitetaan sitten Alexiin, mutta jonka hyökkääjä sieppasi. Hyökkääjä muuttaa nimeä sekillä Jeremyyn ja määrään sekillä 1,000 dollariin ja yrityksiin lunastaa se. Riippuen väärennyksen laadusta muuttuneessa tarkistuksessa hyökkääjä voisi onnistua. (Cisco Networking Academy. 2020.)

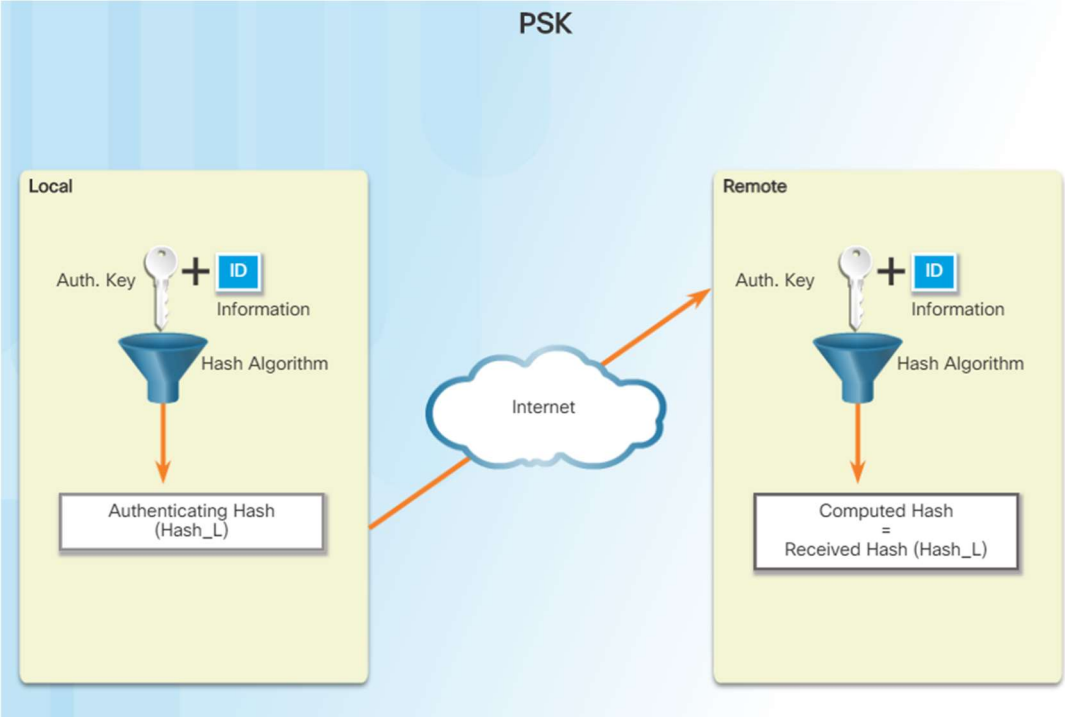
VPN-dataa siirretään julkisen internetin kautta, siksi menetelmä osoittaa, että tietojärjestelmän eheyttä tarvitaan takaamaan, että sisältö ei ole muuttunut. Hajautettu MAC (HMAC) on tietojärjestelmän eheys algoritmi, joka takaa viestin yhtenäisyyden käyttäen hajautusarvoa.


Kuva 6. Eheys Hash algoritmeilla (Cisco Networking Academy 2020)

### 5.3.3 Authentication, todentaminen

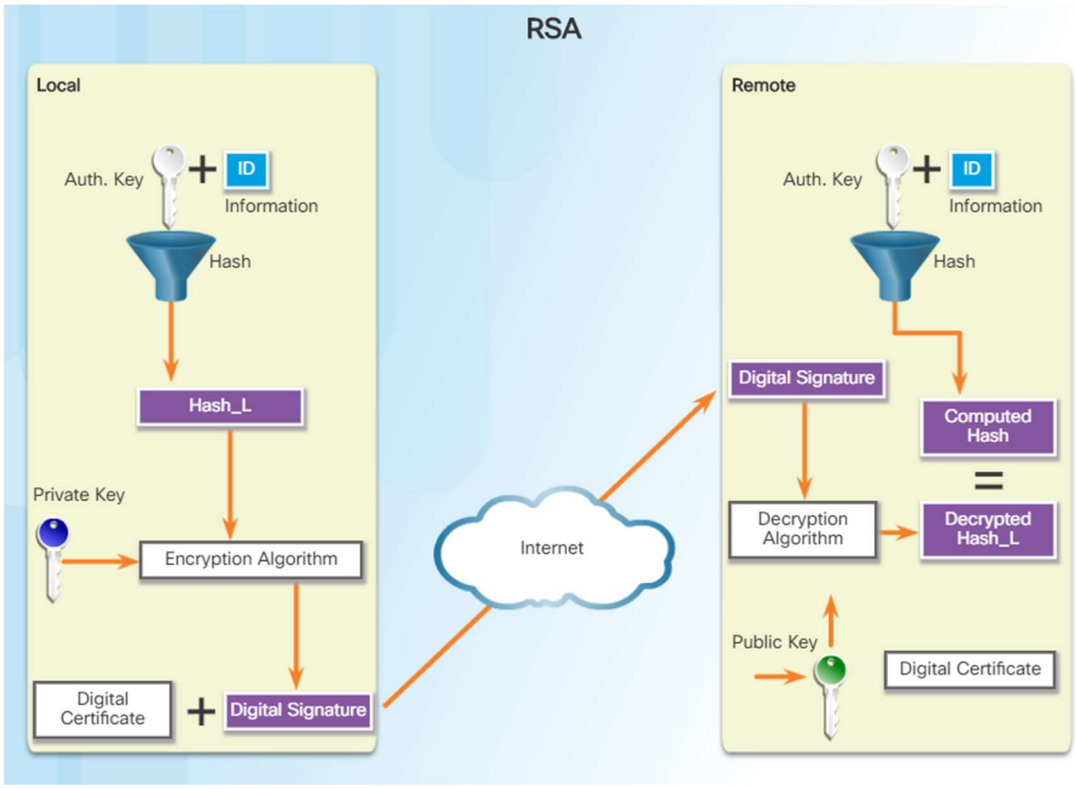
Harjoittaessaan liiketoimintaa pitkän matkan on välttämätöntä tietää, kuka on puhelimen, sähköpostin tai faksin toisessa päässä. Sama on totta VPN-verkoissa. VPN-tunnelin toisessa päässä laite täytyy todistaa aidoksi, ennen kuin viestintäpolkua pidetään turvallisena.

Esimerkki PSK- todentamisesta näkyy kuvassa 7. Paikallisessa laitteessa, todennusavain ja identiteettitieto lähetetään hajautusalgoritmin välityksellä muodostamaan hajautus paikalliselle vertaiselle (Hash_L). Yksisuuntainen todentaminen perustetaan lähettämällä Hash_L:n etäiseen laitteeseen. Jos etäinen laite voi itsenäisesti luoda saman hajautuksen, paikallinen laite todennetaan. Sen jälkeen, kun etäinen laite todentaa paikallisen laitteen, todentamisprosessi alkaa päinvastaiseen suuntaan ja kaikkia askelia toistetaan etäisestä laitteesta paikalliseen laitteeseen. (Cisco Networking Academy. 2020.)




Kuva 7. PSK todentaminen (Cisco Networking Academy 2020)

Esimerkki RSA- todentamisesta näkyy kuvassa 8. Paikallisessa laitteessa, todennusavain ja identiteettitieto lähetetään hajautusalgoritmin välityksellä muodostamaan hajautuksen paikalliselle vertaiselle (Hash_L). Sitten Hash_L on salattu käyttäen paikallisen laitteen yksityistä salausavainta. Tämä luo digitaalisen allekirjoituksen. Digitaalinen allekirjoitus ja varmenne ohjataan etäiseen laitteeseen. Allekirjoituksen avaamista varten julkinen salausavain sisältyy varmenteeseen. Etäinen laite tarkistaa digitaalisen allekirjoituksen avaamalla sen käyttäen julkista salausavainta. Tulos on Hash_L. Seuraavaksi etäinen laite itsenäisesti luo Hash_L:n talletetusta tiedosta. Jos laskettu Hash_L on yhtä suuri kuin avattu, Hash_L, paikallinen laite todennetaan. Sen jälkeen, kun etäinen laite todentaa paikallisen laitteen, todentamisprosessi alkaa päinvastaiseen suuntaan ja kaikkia askelia toistetaan etäisestä laitteesta paikalliseen laitteeseen. (Cisco Networking Academy. 2020.)




Kuva 8. RSA todentaminen (Cisco Networking Academy 2020)

## 5.4 OpenVPN

OpenVPN on SSL VPN -ohjelmisto. Ohjelmisto on saatavilla Solaris-, Linux-, OpenBSD-, FreeBSD-, NetBSD-, QNX-, Mac OS X-, Raspberry Pi- ja Windows -tietokoneille, sekä Windows Mobile-, iOS ja Android-älypuhelimille. Toisin kuin useimmat SSL VPN -järjestelmät, siihen ei oteta yhteyttä selaimella, vaan tietokoneeseen tai älypuhelimeen on asennettava OpenVPN-ohjelmisto. Etukäteen asennettava ohjelmisto takaa sen, ettei yhteyksiä muodostu kuin vain niihin laitteisiin mihin ohjelma on asennettu.

Toisin, kuin monet muut VPN-protokollat, toimii OpenVPN käyttäjänympäristössä (user space) kernelin sijaan (kernel space). Mikä mahdollistaa järjestelmän suorittamisen vähemmillä käyttöoikeuksilla.

OpenVPN hyödyntää TLS-protokollaa yhteysosapuolten avaintenvaihtoon. Avaintenvaihdon jälkeen OpenVPN hyödyntää IPsec:n ESP-protokollaa tiedon salaamiseen. ESP:n käyttö mahdollistaa NAT:n ohittamisen asiakaspäässä. Käytössä on kaikki

salaus- ja tiivistysalgoritmit, jotka löytyvät OpenSSL-ohjelmistosta. OpenVPN mahdollistaa myös HMAC-allekirjoituksen käyttöön ottamisen TLS-kättelyssä, jonka ansiosta vain oikean staattisen avaimen omaavat järjestelmät pystyvät aloittamaan avaintenvaihdon.

OpenVPN pystyy tarkistamaan järjestelmään yhteyttä ottavien laitteiden oikeellisuuden sertifikaateilla tai staattisilla salasanoilla. Käytettäessä sertifikaatteja OpenVPN mahdollistaa, sekä palvelimen, että asiakaskoneen tunnistuksen.

OpenVPN-ohjelmistolla on mahdollista luoda sekä site-to-site, että remote-access yhteyksiä. OpenVPN pystyy tunneloimaan liikenteen käyttämällä, joko UDP- tai TCP-protokollaa. (OpenVPN:n www-sivut. 2020.)

# 6 PALOMUURI

Kun verkot jatkoivat kasvamista ajan kuluessa, niitä käytettiin yhä useammin datan siirtämiseen ja arkaluontoisen tiedon tallentamiseen. Tämä vahvisti tarvetta vahvemmille turvallisuusteknologioille, jotka johtivat palomuurin keksimiseen. Verkkotyöskentelyn maailmassa palomuurit erottavat suojatut alueet ei-suojatuista. Tämä estää luvattomia käyttäjiä pääsemästä suojeltuihin verkkoresursseihin. Nykyään on olemassa monia palomuuri tyyppejä, kuten paketti suodatus, tilallinen, sovellusyhdyskäytävä, valtakirja, osoitteenmuodostus, isäntäpohjainen-, läpinäkyvä- ja hybridipalomuurit. Nykyaikaisen verkon suunnittelun täytyy huolellisesti sisältää yhden tai useamman palomuurin oikea sijoitus suojelemaan resursseja, joita täytyy suojella salliessa turvallisen pääsyn resursseihin, joiden täytyy pysyä saatavilla. (Cisco Networking Academy. 2020.)

## 6.1 Palomuurin edut ja haitat

On useita etuja palomuurin käyttämisessä verkossa:

- Estää herkkien isäntien, resurssien ja sovellusten altistumisen ulkopuolisilta käyttäjiltä
- Puhdistaa protokollavirtausta, joka ehkäisee protokollavirheiden hyväksikäytön.
- Torjuu vahingollisen datan palvelimista ja käyttäjiltä.
- Vähentää turvallisuushallinnan monimutkaisuutta siirtämällä suurimman osan verkkoon pääsyn ohjauksesta muutamalle palomuurille verkossa.

Palomuurin heikkoudet:

- Väärin konfiguroidulla palomuurilla voi olla vakavia seurauksia verkolle kuten tuleminen järjestelmän kaatavaksi häiriöpisteeksi.
- Dataa monista sovelluksista ei voida välittää palomuurin yli turvallisesti.
- Käyttäjät saattavat proaktiivisesti etsiä keinoja päästäkseen palomuurin ympäri saadakseen torjuttua materiaalia, joka voi altistaa verkon potentiaaliselle

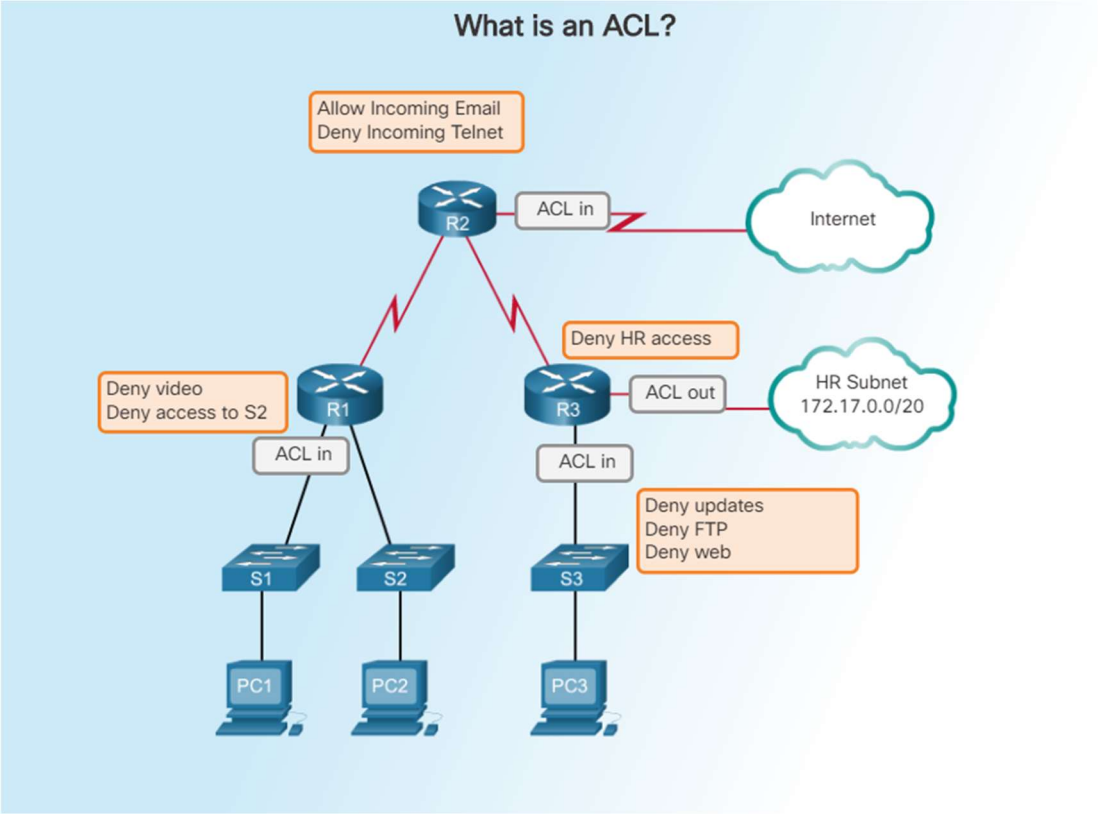
hyökkäykselle.

- Verkon suorituskyky voi hidastua.
- Luvaton liikenne voidaan tunneloida tai kätkeä laillisena liikenteenä palomuurin läpi.

## 6.2 Peruskäyttöoikeusluettelo, ACL

Alussa, peruskäyttöoikeusluettelot (ACL:t), mukaan lukien normaali, laajennettu, numerointi ja nimeäminen, oli ainoa keino palomuuri suojauksen tarjoamiseksi. Muut palomuuriteknologiat alkoivat kehittyä vasta 1990-luvun lopussa. ACL:iä käytetään laajalti tietokoneiden verkoittamisessa, ja verkkoturvallisuudessa lieventääkseen verkon hyökkäyksiä ja hallitakseen verkkoliikennettä. Pääkäyttäjät voivat käyttää ACL:iä määrittelemään ja ohjaamaan liikenteen luokkia verkkotyöskentelylaitteissa vastaamaan annettuja turvallisuusvaatimuksia. ACL:iä voidaan määritellä kerroksille 2, 3, 4 ja 7 avointen järjestelmien yhteen liittämiseksi (OSI)-mallista. (Cisco Networking Academy. 2020.)


Kuva 9. OSI-malli (Wikipedia www-sivut 2020)




Kuva 9. ACL (Cisco Networking Academy 2020)

Normaaleja ja laajennettuja IP ACL:iä voidaan käyttää luomaan paketteja suodattavat palomuurikyvyt. Ne ovat olennaiset työkalut, joita käytetään perusverkkoliikenteen suodattamiseen ja lievittääkseen monenlaisia verkon hyökkäyksiä. Päättääkseen mitä niistä käyttää riippuu liikenteen tyypistä ja liikenteen lähteestä ja päämäärästä. ACL:t ovat yhteydessä verkkoliikenteen virtaukseen. Verkkotopologia määrittää, miten ACL:t luodaan ja sovelletaan.

Luokitellessaan liikennettä ACL:ien tavallisimmat tyypit käyttävät IPv4 ja IPv6-osoitteita ja TCP-protokollaa ja UDP-protokollaa. Standardit ja laajennetut IPv4 ACL:t voidaan nimittää tai numeroida. IPv6 ACL:ien täytyy käyttää nimeä.

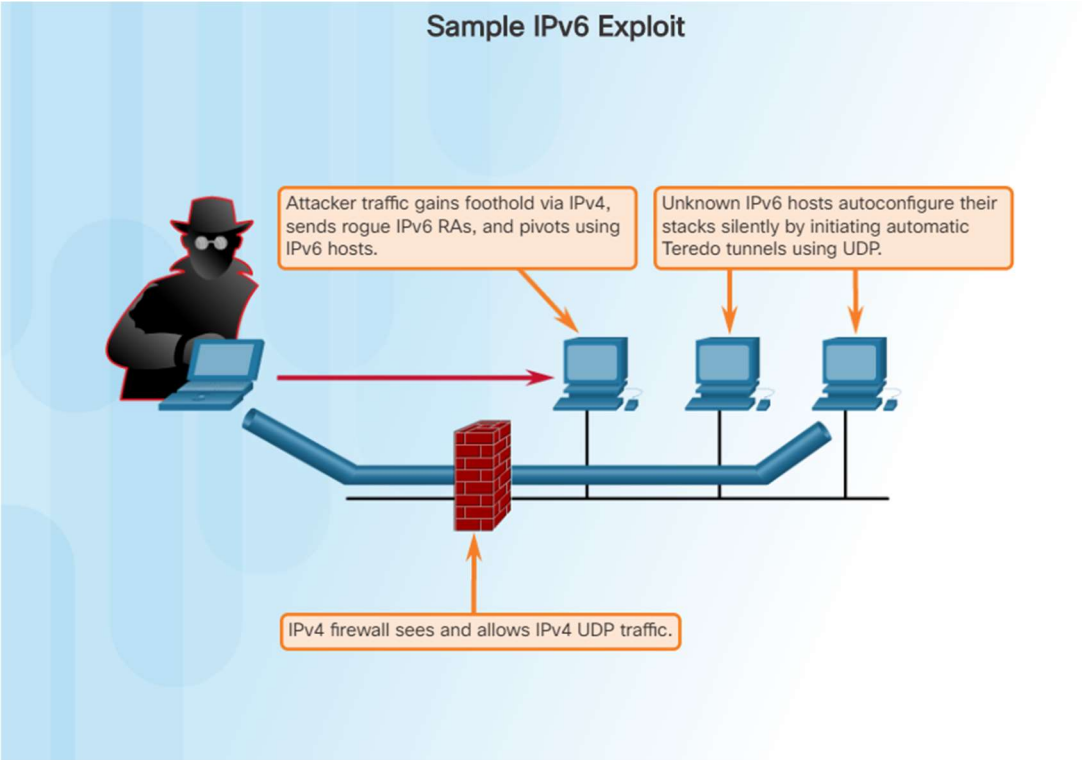
## 6.3 IPv4 ja IPv6

Viime vuosina monet verkot ovat aloittaneet siirtymisen IPv6-ympäristöön. Osa tarvetta siirtymiselle IPv6:een johtuu luontaisista heikkouksista IPv4:ssa. IPv4 suunniteltiin ilman useita nykypäivän verkkovaatimuksia:

- Turvallisuus – IP-turvallisuus (IPsec)
- Laite-verkkovierailu – Mobiili IP
- Palvelutaso – RSVP
- Osoitteen skaalattavuus – DHCP, verkko-osoitteen muunnos (NAT), luokaton reititys (CIDR), muuttuvamittainen aliverkonnaamiointi (VLSM)

Kuitenkin kun siirtyminen IPv6:een jatkuu, IPv6:n hyökkäykset tulevat koko ajan läpitunkevammiksi. IPv4 elää sovussa IPv6:n kanssa ja vähitellen korvataan IPv6:lla. Tämä luo potentiaalisia suojausongelmia. Esimerkki turvallisuushuolesta on, kun hyökkääjät hyödyntävät IPv4:ta käyttääkseen hyväksi IPv6:ta Dual-stack:ssä. Dual-stack on yhdentymismenetelmä, jossa laitteella on toteutus ja liitettävyys sekä IPv4 että IPv6-verkkoihin. Sen seurauksena laitteella on kaksi protokollapinoa. (Cisco Networking Academy. 2020.)

Hyökkääjät voivat onnistua salaisissa hyökkäyksissä, jotka johtavat luottamuksen hyväksikäyttöön käyttämällä Dual-stack isäntiä. Teredon tunneloituminen, esimerkiksi, on IPv6-muutos-teknologia, joka toimittaa automaattista IPv6-osoite siirtoa, kun IPv4/IPv6:n isännät sijaitsevat IPv4-verkko-osoitteen muunnos laitteiden (NAT) takana. Tämä saadaan aikaan upottamalla IPv6-paketit IPV4 UDP-pakettien sisälle. Hyökkääjä saa jalansijan IPv4-verkossa. Vahingoittunut isäntä lähettää vääriä reititin ilmoituksia, joka saa Dual-stack isäntiä saamaan IPv6-osoitteen. Hyökkääjä voi silloin käyttää tätä jalansijaa liikkumaan paikasta toiseen tai pyöriä verkon sisällä. Hyökkääjä voi vaarantaa muita isäntiä ennen liikenteen lähettämistä takaisin verkosta. (Cisco Networking Academy. 2020.)




Kuva 11. Esimerkki IPv6 hyökkäyksestä (Cisco Networking Academy 2020)

On välttämätöntä kehittää ja toteuttaa strategia lievittääkseen hyökkäyksiä IPv6-infrastruktuureja ja protokollia vastaan. Tämän lievennysstrategian pitäisi sisältää suodatuksen rajapinnassa käyttäen eri tekniikoita kuten IPV6 ACL:iä.

ACL:n toiminnallisuus IPv6:ssa muistuttaa ACL:ää IPv4:ssa. Kuitenkaan ei ole mitään vastaavaa IPv4-standardia ACL:lle ja kaikki IPV6 ACL:t täytyy konfiguroida nimellä. IPV6 ACL:t sallivat suodatuksen perustuen lähtö ja tulo-osoitteisiin, jotka kulkevat saapuvana ja lähtevänä tietylle rajapinnalle. Ne myös tukevat liikenteen suodatusta perustuen IPv6-optio-tunnistetietoihin ja vaihtoehtoisesti, ylemmän tason protokolla tyyppistä tietoa ohjauksen hienompaa rakeisuutta varten, samankaltainen kuin laajennetut ACL:t, IPv4:ssa. (Cisco Networking Academy. 2020.)

# 7 TEOLLISUUSAUTOMAATIO LAITTEET

Etäkäytön kysyntä kasvaa jatkuvasti. Etäkäyttö parantaa tuotantopisteiden toiminnan seurantaa ja laitteiden ennakoivaa kunnossapitoa. Etäkäytön avulla saadaan paljon tietoa ennen paikan päällä käyntiä, mikä nopeuttaa ongelmien ratkaisuja.

## 7.1 Siemens

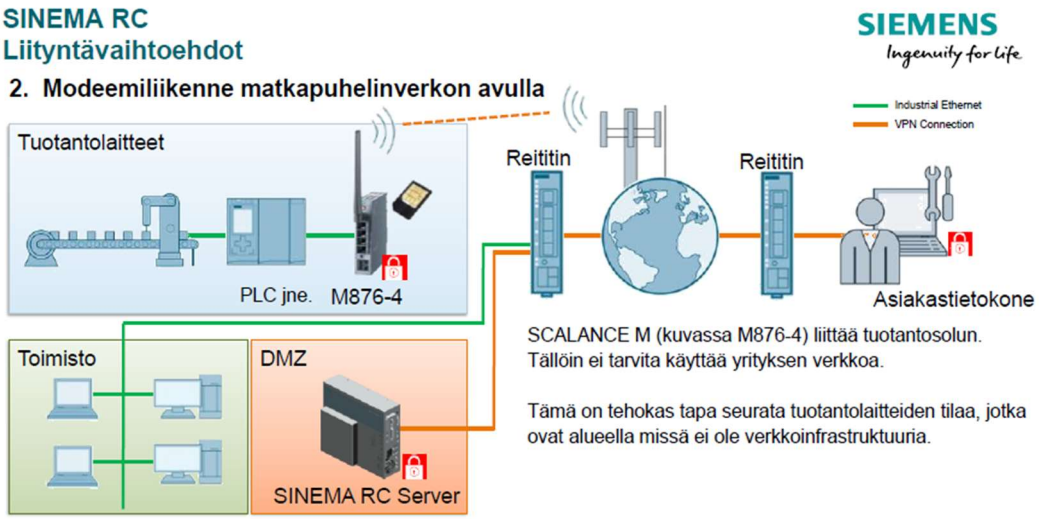
Siemens Osakeyhtiö toimittaa tuotteita, ratkaisuja ja palveluita sähköistykseen, automaatioon ja digitalisaatioon. Siemensin teknologiaratkaisut edistävät kestävää energiantuotantoa, älykästä energiajärjestelmää, tehokasta liikennettä sekä kilpailukykyistä teollisuutta. (Siemensin www-sivut. 2020.)

Siemensillä on laaja tuotevalikoima, joilla saadaan aikaan langaton etäyhteys automaattisten laitteiden välille. Tässä työssä kuitenkin keskitytään Siemensin uuteen Sinema RC:hen.

### 7.1.1 Sinema RC

SINEMA Remote Connect (SINEMA RC) yhteyspalvelin yhdistää eri tuotantosolut ja käyttäjät toisiinsa. SINEMA RC muodostaa yhteyden turvallisesti OpenVPN:n salatulla viestinnällä. Tämä mahdollistaa turvallisen ja edullisen etätiedonkeruun ja ylläpidon Internetin välityksellä sekä toimistoissa että tehtaissa tai laitevalmistajien ja loppukäyttäjien välillä kautta maailman. (Siemenssin www-sivut. 2020.)

Peruskokoonpanossa Sinema RC palvelin asennetaan asiakastietokoneeseen tai vaikka virtuaalitietokoneeseen esimerkiksi Azureen. Asiakastietokone sitten yhdistetään langattomasti VPN:n kautta esimerkiksi SCALANCE M:ään. SCALANCE M876-4 tukee myös matkapuhelinverkkoja, jolloin myös kannettavilla tableteilla ja älypuhelimilla pääsee Sinema RC palvelimeen kiinni.




KUVA 12. Etäkäyttöratkaisu SINEMA Remote Connect Tuotteen yleiskuvaus (Pyykkö 2020, 7)

Sinema RC- ja SCALANCE M -asetukset voidaan konfiguroida web-selaimella, joten erityistä ohjelmistoa ei tarvita. Protokolla on myös riippumaton, joten sitä voidaan käytää ympäristöstä riippumatta. Sinema RC palvelimella on omat tekniset vaatimukset CPU:lle, RAM muistille, verkkosovittimelle ja kovalevylle.

TAULUKKO 1. SINEMA RC tekniset vaatimukset (Siemensin www-sivut. 2020.)

| TYYPPI | MIN. vaatimukset | Suositellut tekniset tiedot |
|---|---|---|
| CPU | Dual Core CPU<br>2.4Ghz | Quad Core CPU<br>2.66Ghz |
| RAM | 2GB | 4GB |
| Verkkosovitin | 1 | 1 |
| Kovalevy | 60GB | 60GB |

Sinema RC käyttämiseksi tarvitaan lisenssejä. Asiakaslisenssi tarvitaan jokaiselle samanaikaiselle etäkäyttäjälle, koska jokainen samanaikainen käyttäjä luo VPN yhteyden. Jotta Sinema RC palvelin olisi VPN-yhteyskohde niin sen rekisteröinniksi tarvitaan VPN-yhteyslisenssi, niitä on saatavilla 64, 256 ja 1024 lisenssin paketteina. SCALANCE M saadaan aktivoitua Sinema RC VPN-verkkoon KEY-PLUG lisenssillä, mikä on fyysinen kortti mikä laitetaan SCALANCE M- laitteeseen kiinni.

Sinema RC:n selainpohjaisella käyttöliittymällä voidaan helposti parametroida eri laitteita, jotka ovat siihen yhdistetty. Sillä voidaan myös nopeasti reagoida tapahtuviin vika tilanteisiin, koska hälytystiedot näkyvät mistä automaatiosolusta hälytys tulee ja mikä on syy. Jos Sinema RC palvelin menettää IP-yhteyden etäkäyttö laitteisiin esimerkiksi sähkökatkon takia, niin se yrittää automaattisesti luoda yhteyttä uudelleen.

### 7.1.2 SCALANCE M876-4 ja KEY-PLUG

SCALANCE M876-4 on 4G reititin langattomaan IP-kommunikointiin. Ominaisuuksina muun muassa: VPN yhteys (IPsec, OpenVPN), palomuuri, NAT, PSK-todennus. KEY-PLUG sisältää konfigurointi datan, jolloin vanhan laitteen hajotessa uusi laite voidaan ottaa käyttöön samalla KEY-PLUG:lla. KEY-PLUG sisältää myös lisenssin millä luodaan yhteys Sinema RC:hen.


KUVA 13. KEY-PLUG (Siemens Industry Mall www-sivut 2020)

## 7.2 Phoenix Contact Oy

Phoenix Contact Oy on saksalaisen, vuonna 1923 perustetun Phoenix Contact GmbH & Co:n suomalainen tytäryhtiö. Yritys on kansainvälisesti kasvava sähköisen liitäntä- ja automaatioteknologian sekä ylijännitesuojausratkaisujen toimittaja. Suomessa työntekijöitä on noin 50. Phoenixilla on kattava jälleenmyynti- ja tukkuriverkosto maanlaajuisesti, jotka palvelevat kaikkia teollisuuden aloja. (Phoenix Contactin www-sivut. 2020.)

Phoenix Contact:lla on myös laaja tuotevalikoima, joilla saadaan aikaan langaton etäyhteys automaattisten laitteiden välille. Tässä työssä perehdytään yhteen ratkaisu vaihtoehtoon Phoenixin osalta.

### 7.2.1 TC ROUTER

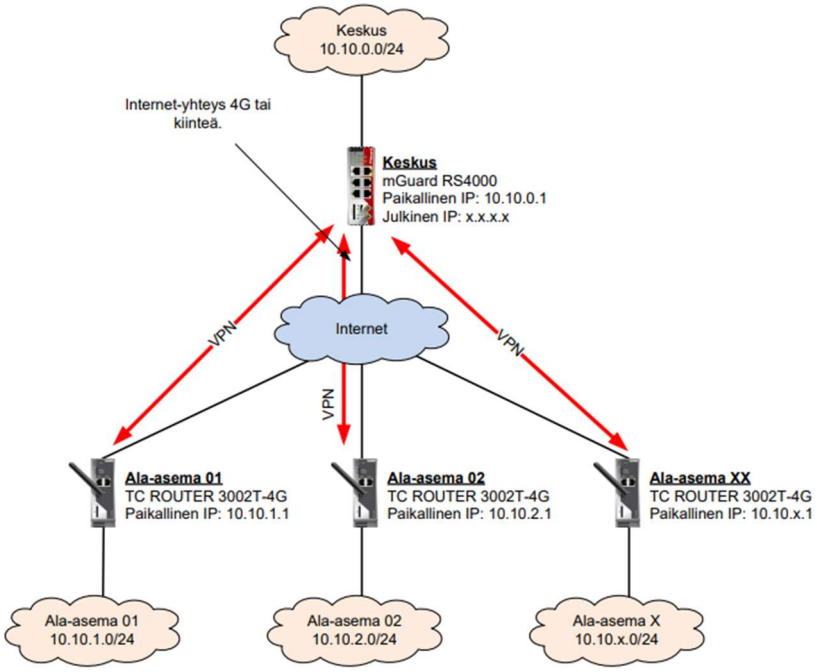
TC-REITITIN on matkapuhelin verkko kommunikointiin, joka yltää lähes 150 Mbps:n 4G LTE verkon kautta. Tämä mahdollistaa mobiililaajakaista yhteyden erittäin haastavissa asema verkoissa, joissa langallinen Internet-yhteys ei ole käytettävissä tai saatavilla. TC-reitittimellä voi olla kolme samanaikaista VPN yhteyttä. Näitä yhteyksiä voidaan käyttää lähettämään arkaluonteista tietoa turvallisesti matkapuhelinverkon kautta. Lisäksi TC-REITITIN tarjoaa korkeaa turvallisuus tasoa IPsecin tai OpenVPN:n tunnelien ansiosta, sekä integroitu tilallinen paketin tarkastus palomuuri. TC-reititin konfiguroidaan selain pohjaisella käyttöliittymällä mikä on samankaltainen kuin Siemensin Sinema RC:n. Vaihtoehtoisesti konfiguroinnin voi tehdä microSD-kortilla. TC-reitittimellä on kaksi konfiguroitavaa inputtia ja yksi konfiguroitava output. (Phoenix Contactin www-sivut. 2020.)

Kuva 14. TC ROUTER 3002T-4G – 2702528 (Phoenix Contact www-sivut 2020)

### 7.2.2 TC MGUARD

TC mGuard turvallisuuslaitteet ovat teollisia matkapuhelinverkko reitittimiä, jotka on varustettu mGuard-teknologialla. Reitittimet tarjoavat etäisylläpito infrastruktuuria koneiden ja järjestelmien suojatulle yhteydelle internetin kautta. Turvallinen etäinen viestintä maailmanlaajuisesti tapahtuu 4G LTE:n sekä UMTS:n ja CDMA-verkkojen kautta. SD-kortin avulla konfigurointimuistina laitteet voidaan nopeasti ja helposti käynnistää tai korvata. Konfigurointi voidaan myös tehdä selain pohjaisessa käyttöliittymässä. MGuard:lla voi olla 10 samanaikaista VPN yhteyttä, mutta lisenssejä lisäämällä niitä voi olla jopa 250. MGuard on turvallisuus tasoltaan tehokkaampi kuin TC-reititin, koska mGuard tarjoaa enemmän turvallisuusfunktioita. Siksi TC-reititin laitteet laitteet on hyvä asentaa mGuard laitteen taakse kuten kuvassa 16 näkyy. (Phoenix Contactin www-sivut. 2020.)


Kuva 15. TC MGUARD RS4000 4G VPN (Phoenix Contact www-sivut 2020)




Kuva 16. Esimerkki ratkaisu (Sivén 2020, 1)

## 7.3 TOSIBOX®

TOSIBOX® tarjoaa tietoturvallisia ratkaisuja etäyhteen teollisuus- ja kiinteistöautomaatiossa. TOSIBOX® on yhteensopiva kaikkien teollisuusautomaatiota tarjoavien toimijoiden kanssa protokollasta riippumatta. TOSIBOX®-tuotteet valmistetaan Suomessa, ja niitä käytetään yli 120 maassa. (Tosibox www-sivut. 2020.)

### 7.3.1 TOSIBOX Mobile Client

TOSIBOX® Mobile Client luo turvalliset etäyhteydet myös mobiililaitteisiin. Sovellus on saatavilla iOS- ja Android -laitteille. Mobile Client mahdollistaa turvallisen yhteyden TOSIBOX® Lukko-laitteisiin WiFi- tai datayhteyden kautta. Mobile Clientin

käyttö oikeudet ovat laitteistokohtaisia, joten samaa tunnusta ei voida käyttää kuin yhdessä mobiililaitteessa. VPN- yhteyden tyyppi on Android- laitteilla OpenVPN yhteys ja IPsec iOS-laitteilla. (Tosibox www-sivut. 2020.)

### 7.3.2 TOSIBOX Avain

TOSIBOX® Avain on älykäs salausavain, jonka avulla muodostetaan turvallinen yhteys tietokoneen ja yhden tai useamman TOSIBOX® Lukon välille. Avainta voidaan käyttää siis useamman Lukon käyttöönotossa. Salausavain on 2048 bittinen RSA. Avain pitää sisällään TOSIBOX® Key -ohjelmiston ja asetukset sekä yhden Mobile Clientin.


Kuva 17. TOSIBOX® Avain (Tosibox www-sivut 2020)

### 7.3.3 TOSIBOX® Lukko 150

TOSIBOX® Lukko 150 on teollisuusreititin sisäänrakennetulla palomuurilla. Lukko toimii päätepisteenä turvallisille etäyhteyksille salatulla VPN yhteydellä. Lukossa on patentoitu TOSIBOX® Plug & Go™ -yhteysmenetelmä, jonka avulla laitteen saa toimintavalmiiksi alle viidessä minuutissa ilman ohjelmien asentamista, verkon konfigurointia tai muun erityisosaamisen tarvetta. Lukolla voi olla jopa 10 yhtaikaista VPN yhteyttä ja katkenneet VPN yhteydet yhdistetään automaattisesti. Käyttää muun muassa PSK-todennusta. Lukko toimii sekä 4G-yhteydellä että RJ-45 liitännällä ja on verkko-operaattorista riippumaton. (Tosibox www-sivut. 2020.)

Lukko 150 voidaan liittää RJ-45 liitännällä kohteessa olevaan logiikkaan, jolloin saadaan logiikkaan etäyhteys. Lukko pitää käyttöön ottaessa aktivoida Tosibox avaimella, joka laitetaan reitittimen USB-porttiin.


Kuva 18. TOSIBOX® Lukko 150 (Tosibox www-sivut 2020)

### 7.3.4 TOSIBOX 4G Modem

Jotta Tosibox lukot saadaan yhdistettyä 4G mobiiliverkkoon niin tarvitaan joko Tosibox 4G teollisuus modeemi tai USB-porttiin laitettava 4G modeemi. USB-porttiin ei kuitenkaan voida mitä tahansa modeemia laittaa vaan Tosiboxin sivuilta näkee yhteensopivat laitteet.


Kuva 19. TOSIBOX® 4G Modem (Tosibox www-sivut 2020)

Kuva 20. Huawei E3372(4G) (Tosibox www-sivut 2020)

### 7.3.5 TOSIBOX® Lukko 500i

TOSIBOX® Lukko 500i on samankaltainen laite kuin Lukko 150, mutta paljon tehokkaampi. VPN läpäisykyky on 70 Mbit/s ja siihen voi yhdistää 50 alilukkoa. Mallissa myös sisäänrakennettu LTE modeemi, internet liitäntää varten. VPN-läpisyöttö paljon dataa siirtäville sovelluksille, päästä päähän salaus. Sisäänrakennettu palomuuri ja verkko-operaattorista riippumaton. Käyttää muun muassa PSK-todennusta. Lukko 500i voidaan asentaa esimerkiksi pääasemaksi, joka kerää kaikilta muilta asemilta dataa joihin on asennettu esimerkiksi Lukko 150 reitittimet ja lähettää ne sitten edelleen valvomo tietokoneeseen. (Kuronen sähköposti 14.5.2020)


Kuva 21. TOSIBOX® Lukko 500i (Tosibox www-sivut 2020)

# 8 YHTEENVETO

Kaikilla edellä mainituilla laitteilla ja järjestelmillä saadaan aikaan turvallinen ja käyttäjäystävällinen etäkäyttöratkaisu teollisuusympäristöön. Suurimmat erot laitevalmistajien välillä kuitenkin tulee niiden hinnasta ja elinkaaresta sekä skaalautuvuudesta. Siemensin Sinema RC on erittäin hyvin skaalautuva ja käyttäjäystävällinen Sinema RC-palvelinta voidaan käyttää myös muiden asiakkaiden automaatiojärjestelmissä ja vielä ympäri maailmaa. Sen takia Sinema RC on hyvin kustannustehokas ja Siemens on aina ollut tunnettu laadukkaista ja pitkän elinkaaren omaavista laitteista. SCALANCE M:llä on myös oma sisäänrakennettu palomuuri, joka estää ei-haluttuja käyttäjiä pääsemästä siihen kiinni ja suodattaa ei-halutun liikenteen pois. Tietoturva riskit ovat minimoitu, koska näiden laitteiden välinen liikenne on VPN:n kanssa tunneloitu, jolloin tieto on salattu, eheä ja todennettu.

Phoenixin aikaisemmin mainitut laitteet muistuttavat hieman Siemensin laitteita, nekin ovat tarkoitettu 4G- matkapuhelinverkon kanssa kommunikointiin ja niillä on myös selainpohjainen käyttöliittymä. Ne eivät kuitenkaan ole yhtä skaalautuvia kuin Siemensin Sinema RC-palvelin ja vaatii hieman enemmän parametrointia käyttöönotossa. Phoenixin laitteilla on kuitenkin toteutettu tietoturva erittäin hyvin.

Tosibox laitteet ovat tarkoitettu nimenomaan teollisuus- ja kiinteistöautomaatiossa. Tosibox on yhteensopiva kaikkien teollisuusautomaatiota tarjoavien toimijoiden kanssa protokollasta riippumatta, joten tosiboxin takana olevat laitteet voivat olla monen eri laitevalmistajan esim. Siemens, Phoenix. Tosiboxin patentoidulla yhteys menetelmällä yhteys voidaan saada aikaan, vaikka molemmat osapuolet olisivat palomuurin tai NAT:ien takana, minkä ansiosta Tosibox laitteissa ei ole mitään palveluja, jotka olisivat kaiken aikaa kuunneltuina, tai altistuneena internetille. Tosibox ei myöskään tarvitse kiinteistä IP-osoitetta, eikä muita operaattorin palveluita. Kohteissa voidaan siis hyödyntää myös halvimpia 4G-liittymiä.

Kaikkia näitä edellä mainittuja laitteita yhdistää niiden samanlainen VPN-tekniikka, johon kuuluu IPsec ja OpenVPN ja niiden salaus algoritmit, joten selkeästi tietoturvallisinta laitetta ei ole. Siksi laitteiden loppukäyttäjillä on suuri vastuu niiden

käyttöönoton aikana tehdyistä parametroinneista, salasanojen valitsemisesta ja laitteistopäivitysten asentamisesta. Loppukäyttäjiä pitää siksi opastaa hyvin laitteen kanssa toimimiseen, jotta mitään suurta vahinkoa ei pääse tapahtumaan.

Näistä kolmesta ratkaisu vaihtoehdosta minä valitsisin kuitenkin Siemensin Sinema RC:n, koska se on erittäin käyttäjäystävällinen ja siinä on helppokäyttöön otto. Siemensin tuotteet ovat myös laadukkaita, joten niiden elinkaari on pitkä. Sinema RC:n yksi ominaisuus on myös, että palvelimeen voi yhdistää useita eri asiakas kohteita. Kuitenkin yritys itse tekee päätöksen minkä laitevalmistajan etäkäyttöratkaisun he valitsevat.

# LÄHTEET


Siemenssin www-sivut. 2020. Viitattu 4.5.2020. https://new.siemens.com/fi/fi.html

Phoenix Contactin www-sivut. 2020. Viitattu 6.5.2020. https://www.phoenixcontact.com/online/portal/fi?1dmy&urile=wcm%3apath%3a/fifi/web/home

Tosibox www-sivut. 2020. Viitattu 8.5.2020. https://www.tosibox.com/fi/

OpenVPN:n www-sivut. 2020. Viitattu 1.5.2020. https://openvpn.net/

Traficomin www-sivut. 2020. Viitattu 20.4.2020. https://www.kyberturvallisuuskeskus.fi/fi/

Pyykkö, T. 2020. Sinema RC. Luento Sinema RC järjestelmästä 27.3.2020.

Kuronen, I. Tosibox Central lock, Tosibox virtual Central lock. Vastaanottaja: tomi.liias@tosibox.com. Lähetetty 14.5.2020 klo 10.39. Viitattu 14.5.2020.

Davor, T. 2020. HMS Cyber Security. Viitattu 25.4.2020. https://console.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=https%3A%2F%2Fwww.hms-networks.com%2Fcampaign-landing-pages%2Fiiot-webinar-month&eventid=2246183&sessionid=1&key=3210FD66B908C80DB013E5B6DBE6127B&regTag=&sourcepage=register

Cisco Networking Academy. 2020. CCNA Security: Implementing Network Security 2.01. Viitattu 26.4.2020. https://www.netacad.com/courses/security/ccna-security

Sivén, J. 2020. Example_Remote connection_mGuard-TC router.

Siemens Industry Mall www-sivut. 2020. Viitattu 10.5.2020. https://mall.industry.siemens.com/goos/WelcomePage.aspx?language=en&regionUrl=/

Satmatic Oy:n www-sivut. 2020. Viitattu 20.3.2020. https://www.satmatic.fi/Satmatic