OULUN AMMATTIKORKEAKOULU

Marko Mustonen

VPN VIRTUAALIKONEIDEN ETÄKÄYTÖSSÄ

VPN VIRTUAALIKONEIDEN ETÄKÄYTÖSSÄ

Marko Mustonen
VPN virtuaalikoneiden etäkäytössä
Syksy 2014
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittely

Tekijä(t): Marko Mustonen
Opinnäytetyön nimi: VPN virtuaalikoneiden etäkäytössä
Työn ohjaaja: Jukka Kaisto
Työn valmistumislukukausi- ja vuosi: Syksy 2014 Sivumäärä: 57 + 2

Opinnäytetyön aiheena oli virtuaalikoneiden etäkäytön mahdollistavan VPN-ratkaisun luominen Oulun Ammattikorkeakoululle. Tavoitteena oli korvata aiemmin käytössä ollut VPN-ratkaisu nykyaikaisella ratkaisulla.

Opinnäytetyön tietoperusta koostui lähinnä tietoverkkoihin ja VPN-ratkaisuihin liittyvistä asioista. Tietoperusta kattoi esimerkiksi seuraavat käsitteet: IP-osoitteet (Internet Protocol), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), osoitteenmuunnos (NAT), aktiivihakemisto (Active Directory, AD), OSI-malli (Open System Interconnection) ja etätyöpöytäratkaisu (Remote Desktop). Lisäksi tietoperustassa käsiteltiin tietoturvaa sekä palomuurien ominaisuuksia. VPN-yhteyksien tietoperustassa esiteltiin erilaiset VPN-ratkaisut, VPN-protokollat sekä yleisesti VPN-yhteyksien tarjoamat hyödyt sekä haitat.

Tietoperusta saatiin kerättyä erinäisistä aineistoista kuten esimerkiksi kirjoista, lehdistä, artikkeleista ja joiltain osin myös verkkosivuilta. Aineistona käytettiin sekä englannin- että suomenkielistä materiaalia. Tämän lisäksi tietoa hankittiin tuotteiden osalta myös sähköposti- ja puhelinkeskusteluista sekä esimerkiksi osallistumalla webinaariin.

Oulun Ammattikorkeakoululle saatiin otettua käyttöön uusi VPN-ratkaisu käyttämällä Palo Alto Networksin fyysistä palomuurituotetta ja sen sisältämiä VPN-ominaisuuksia. Laite konfiguroitiin siten, että se sallii VPN-yhteyden muodostuksen tunnistetuille käyttäjille ja etätyöpöytäyhteyden virtuaalisille työasemille Oulun Ammattikorkeakoulun intranetissä.

Ratkaisu tulee vielä testata kunnolla opetuskäytössä ennen vanhan ratkaisun poistamista käytöstä. Tämän lisäksi tuotteen ominaisuuksia voidaan käyttää monipuolisemmin hyväksi esimerkiksi analysoimalla tietoliikennettä pidemmällä aikavälillä.

Asiasanat: tietotekniikka, tietoliikenneverkot, etäkäyttö, palomuurit – tietoturva, pääsynvalvonta, tiedonsiirto

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author(s): Marko Mustonen
Title of thesis: Accessing virtual machines remotely through VPN
Supervisor(s): Jukka Kaisto
Term and year when the thesis was submitted: fall 2014 Number of pages: 57 + 2

The purpose of this thesis was to replace the current VPN solution with a modern solution that enables remote desktop access to virtual machines located in the intranet of Oulu University of Applied Sciences. By using this solution, students are able to use their personal computers when accessing virtual machines over public internet.

The theoretical background consists of information related to computer networks and VPN solutions such as IP-address (Internet Protocol), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Network Address Translation (NAT), Active Directory (AD), OSI-model (Open System Interconnection) and Remote Desktop Protocol (RDP). In addition, matters related to security and firewalls were covered. The background information related to VPN covers different kinds of VPN solutions, VPN protocols as well as advantages and disadvantages of VPN.

The theoretical background information was gathered from books, magazines, articles as well as from a few web pages and these sources include both Finnish and English materials. A part of the background information was gathered from email and phone discussions with the technical support of Palo Alto Networks. Moreover, the participation in their webinar increased the knowledge about their product.

The new VPN solution was implemented successfully by using the hardware firewall of Palo Alto Networks and the VPN functionalities it provides. The firewall was configured so that it allows remote desktop connection through secured VPN tunnel for authenticated users. By using this solution people are able to use virtual machines located in the intranet of Oulu University of Applied Sciences through public internet.

The solution still needs to be tested properly before the old solution can be ramped down. Some of the functionalities can also be taken into use after a thorough analysis of the network traffic.

Keywords: information technology, computer networks, remote control, information security, access control, data transfer

SISÄLLYS

1 JOHDANTO 6
2 TIETOVERKOT 8
2.1 IP-osoite (Internet Protocol) 8
2.2 Dynamic Host Configuration Protocol (DHCP) 9
2.3 Domain Name System (DNS) 10
2.4 Tietoturva ja palomuurit 11
2.5 Osoitteenmuunnos (Network Address Translation, NAT) 13
2.6 Aktiivihakemisto (Active Directory, AD) 14
2.7 Etätyöpöytä (Remote Desktop) 16
2.8 OSI-malli 18
2.9 Virtual Private Network (VPN) 20
2.9.1 VPN-protokollat 23
2.9.2 Microsoft DirectAccess 27
2.9.3 Palo Alto Networks GlobalProtect 28
3 NYKYISEN YMPÄRISTÖN KUVAUS 31
4 UUDEN RATKAISUN VALINTA 33
4.1 Käyttöönotto 35
4.2 Testaus 49
5 TULOKSET JA JOHTOPÄÄTÖKSET 51
6 POHDINTA 53
LÄHTEET 56
LIITTEET 59

1 JOHDANTO

Tietoverkot ovat olleet olemassa jo suhteellisen pitkään, mutta keksimme koko ajan uusia tapoja hyödyntää tietoverkkoja päivittäisissä askareissamme. Samalla kun tietoverkot ovat kehittyneet ja yleistyneet, myös ihmisten liikkuvuus on lisääntynyt. Emme ole enää sidottuina työskentelemään toimistolla joka päivä kello 08:00-16:00 välisenä aikana. Meidän tulee pystyä pääsemään kiinni yrityksen resursseihin silloinkin kun olemme työmatkalla tai valmistelemme kotona huomisen tärkeää esitystä. Yksi nykyaikainen käyttötapa tietoverkoille onkin hyödyntää sitä esimerkiksi etätyöskentelyssä tai etäopiskelussa. Virtual Private Network-yhteydellä (VPN) saadaan luotua suojattu tunneli julkisen internetin ylitse, joka varmistaa tiedonsiirtokanavan turvallisuuden eikä tietoliikenne kulje salaamattomana julkisen internetin ylitse.

Tässä opinnäytetyössä on tarkoituksena toteuttaa etätyöskentelyn mahdollistava tietoturvallinen ratkaisu laboratoriotilaan, jota oppilaat voivat hyödyntää esimerkiksi SharePoint–kurssien etäopetustunneilla. Kyseisessä laboratoriossa on ollut etäyhteydet mahdollistava VPN -ratkaisu käytössä jo aiemmin, mutta koska tähän tarkoitukseen on omistettu yksi fyysinen kone, tahdotaan se vapauttaa uudella ratkaisulla muuhun käyttöön. Oppilaiden tulee pystyä omalta työasemaltaan kytkeytymään Oulun Ammattikorkeakoulun verkkoon ja siellä olevaan virtuaaliseen työasemaan käyttäen VPN-yhteydettä ja etätyöpöytäprotokollaa (Remote Desktop Protocol, RDP).

Opinnäytetyössä vertailtavat VPN-ratkaisut on ennalta rajattu kahteen vaihtoehtoon, joiden ominaisuuksia on tarkoitus vertailla keskenään ja valita näistä kahdesta paremmin kyseiseen käyttötarkoitukseen soveltuva ratkaisu sekä suorittaa sen varsinainen käyttöönotto. Nämä kaksi ennalta rajattua vaihtoehtoa ovat Microsoftin DirectAccess sekä Palo Alto Networksin palomuurituotteiden mukana tuleva VPN-ominaisuus GlobalProtect. Microsoft DirectAccess on ollut jo useamman vuoden saatavilla, mutta tietyt puutteet ovat hidastaneet sen yleistymistä etäkäyttöratkaisuna. Palo Alto Networksin palomuurit edustavat nykyaikaisia palomuureja kehittyneillä ominaisuuksillaan.

Opinnäytetyön tietoperustassa kappaleessa 2 käsitellään lähinnä tietoverkkoihin liittyviä asioita. Tietoperusta kattaa esimerkiksi seuraavat käsitteet: IP-osoitteet (Internet Protocol), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), aktiivihakemisto (Active Directory, AD), OSI-malli (Open System Interconnection) ja etätyöpöytäratkaisu (Remote Desktop) Tämän lisäksi keskitymme vahvasti tietoturvaan sekä palomuurien ominaisuuksiin. VPN-yhteyksien tietoperustassa on esiteltynä erilaiset VPN-ratkaisut, VPN-protokollat sekä yleisesti VPN-yhteyksien tarjoamat hyödyt sekä haitat.

Erilaiset etäkäyttöratkaisut tulevat varmasti yleistymään edelleen tulevaisuudessa, niin työpaikoilla kuin esimerkiksi opiskelussakin. Tästä syystä opinnäytetyön aihe on ajankohtainen ja myös henkilökohtaisesti kiinnostava, koska se tarjosi mahdollisuuden syventää omaa tietämystäni tietoverkoista sekä VPN-ratkaisuista. Käytännön kokemusta erilaisista VPN-ratkaisuista on jonkin verran aiempien työtehtävien kautta, mutta varsinaisesti aiempaa tietoperustaa VPN-ratkaisuista ei ole.

Opinnäytetyön toimeksiantaja on Oulun Ammattikorkeakoulu.

2 TIETOVERKOT

Tietoverkolla tarkoitetaan tilannetta, jossa kaksi tai useampi tietokone on kytketty toisiinsa kaapelilla (tai langattomasti), jotta ne voivat siirtää tietoa keskenään. Perimmäinen syy tietoverkkojen olemassa ololle on jakaminen: tiedostojen, resurssien sekä ohjelmien. Tietoverkko pitää sisällään kahdenlaisia tietokoneita: palvelimia (*server*) ja asiakaskoneita (*client*). Palvelimella käsitetään tietokonetta, joka jakaa resursseja muiden käyttöön ja resursseja hyödyntäviä koneita kutsutaan asiakaskoneiksi. (Lowe 2010, 10, 12, 14.)

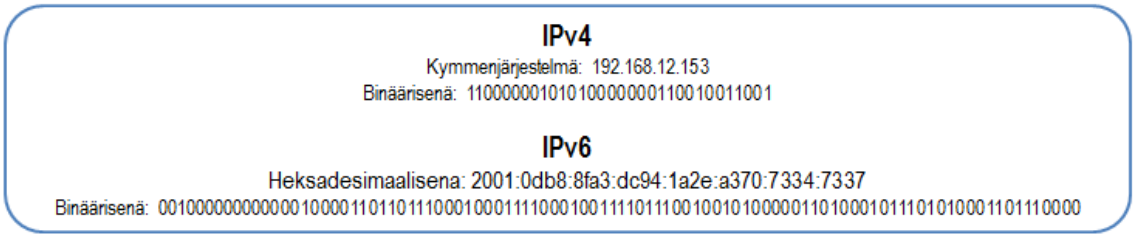
Tunnetuin tietoverkko on *internet*, joka itseasiassa ei ole yksi yhtenäinen tietoverkkokokonaisuus vaan on maailmanlaajuinen tietoverkko, joka rakentuu yhteen kytketyistä verkoista. Näitä aliverkkoja ylläpitävät erilliset ja itsenäiset tahot, esimerkiksi yritykset, yhteisöt, oppilaitokset, valtiot sekä yksityiset ihmiset. Näiden verkkojen yhteen kytkeminen mahdollistaa maailmanlaajuisen tiedon hakemisen, sen siirtämisen sekä kommunikoinnin verkkojen sekä ihmisten välillä. (Mäkelä 2014, 132).

2.1 IP-osoite (Internet Protocol)

Jokaisella tietoverkkoon liitetyllä tietokoneella tai laitteella on ennalta määritelty osoitteensa, jonka avulla verkon kyseinen tietokone yksilöidään tietoverkossa. Näin muut tietokoneet voivat esimerkiksi ottaa yhteyden tälle tietylle tietokoneelle ja kommunikoida sen kanssa. Tätä osoitetta kutsutaan IP-osoitteeksi ja perinteisesti se muodostuu neljästä numerosarjasta, jotka erotellaan pisteellä ja jotka ovat arvoltaan 0-255 eli esimerkiksi 192.100.100.100. (Mäkelä 2014, 132.)

Edellä mainittu esimerkki on IPv4-protokollan mukainen osoite, joka alun perin määriteltiin jo vuonna 1981. IPv4-protokollassa on paljon ongelmia sekä puutteita nykypäivän tarpeisiin, esimerkiksi rajallinen osoiteavaruus sekä sisäänrakennetun tietoturvan puute. Nykyään ollaankin siirtymässä IPv6-protokollan käyttöön, joka itseasiassa esiteltiin jo vuonna 1998. Täydellinen siirtyminen IPv6 käyttöön tulee kuitenkin todennäköisesti kestämään vielä vuosikymmenen, koska korvattavia laitteita on miljoonia. Siihen saakka IPv4 sekä IPv6 tulevat elämään rinnan ja erinäisten tekniikoiden avulla mahdollistetaan IPv4 ja IPv6 verkkojen kommunikointi keskenään. IPv6-protokollan myötä tulee parannuksia esimerkiksi aliverkotukseen sekä tämän lisäksi myös tieto-

turvaan, koska myöhemmin kappaleessa 2.9.1 esiteltävä IPSec-protokolla tulee IPv6-protokollassa sisäänrakennettuna. Mutta ennen kaikkea, IPv6 tulee pitämään sisällään 128-bittisen osoiteavaruuden ja osoite muodostuu kahdeksasta neljän heksadesimaalin sarjasta erotettuina kaksoispisteellä.. Tämä on huomattavasti suurempi kuin IPv4 myötä käytössä ollut 32-bittinen osoiteavaruus (kuvio 1). (Stewart, J. Michael 2014, 25-27.)



KUVIO 1. Tyypillisten IPv4- ja IPv6-osoitteiden vertailu (Stewart, J. Michael 2014, 26)

Kun yritys tai organisaatio päättää siirtyä täysin IPv6 käyttöön, täytyy muutos suunnitella hyvin sekä on ensijaisen tärkeää huolehtia henkilön koulutuksesta. Todennäköisesti tietoverkon fyysiset laitteistot jo tukevat tässä vaiheessa IPv6-protokollaa, mutta tämä tulee varmistaa esimerkiksi palomuurien osalta. Sen sijaan laitteistojen ja ohjelmistojen konfiguroinnissa on paljon asioita, jotka tulee tässä yhteydessä muuttaa tai päivittää. Esimerkkinä mainittakoot reititys, DNS, DHCP ja luonnollisesti laitteistojen osoitekonfiguraatiot tulee päivittää esimerkiksi palomuurien osalta.

2.2 Dynamic Host Configuration Protocol (DHCP)

Jokaisella tietoverkkoon kytkeytyvällä laitteella tulee olla yksilöllinen IP-osoite, jonka se saa verkkoon kytkeytyessään ennalta määritellystä osoiteavaruudesta. DHCP-palvelin (Dynamic Host Configuration Protocol) huolehtii näiden IP-osoitteiden jakamisesta sitä mukaan kun verkkoon tulee uusia laitteita ja olemassa olevia poistuu. Myös kiinteiden IP-osoitteiden määritteleminen on mahdollista, mutta varsinkin laajoissa verkoissa näiden määritteleminen ja ylläpitäminen olisi erittäin työlästä ja aikaa vievää, näin ollen DHCP-palvelinta käytetäänkin yleisesti. DHCP-palvelin löytyy yleensä yrityksen sisäisestä verkosta, mutta käytännössä se voidaan konfiguroida myös operaattorin tietoverkkoon.

IP-osoitteita on olemassa niin staattisia kuin dynaamisiakin. Staattiset IP-osoitteet pysyvät aina samoina ja dynaamiset puolestaan jaetaan DHCP-protokollan toimesta. DHCP-protokollan avulla voidaan myös jakaa asetuksia verkon laitteille kuten esimerkiksi reitittimen ja/tai DNS-palvelimen

osoitteen. (Lowe 2010, 117-118.) Kun DHCP jakaa dynaamisia osoitteita, niille annetaan ennalta määritelty voimassaoloaika, koska jos laite ei vapauta saatua IP-osoitetta, ne ennen pitkää loppuisivat annetusta osoiteavaruudesta. Laite voi kuitenkin pyytää DHCP-palvelimelta IP-osoitteen uusimista ennen sen umpeutumista. (Tanenbaum & Wetherall 2014, 470.)

2.3 Domain Name System (DNS)

Toinen tietoverkkojen kannalta oleellinen palvelu on DNS-palvelin (Domain Name System). Koska loppukäyttäjälle on lähes mahdotonta muistaa kaikkien tarvitsemiensa palveluiden ja esimerkiksi internet palvelimien IP-osoitteita, niille määritellään selkokieliset nimet esimerkiksi www.oamk.fi. Tämän lisäksi jos IP-osoite muuttuisi, se pitäisi kertoa erikseen kaikille mahdollisille kyseisen palvelun käyttäjälle. Mutta koska tietoverkot ymmärtävät nimenomaan IP-osoitetta, täytyy välillä olla käännös IP-osoitteen ja selkokielisen DNS-nimen välillä. DNS-palvelimen tehtävä on huolehtia tästä muunnoksesta, jotta tietoverkko voi esimerkiksi reitittää liikennettä IP-osoitteen avulla ja käyttäjä puolestaan käyttää selkokielistä DNS-nimeä.

Käytännössä tämä muutos tapahtuu siten, että sovellus kutsuu resolveria ja toimittaa nimen parametrinä. Resolveri tämän jälkeen lähettää kyselyn paikalliselle DNS-palvelimelle, joka hakee nimeä vastaavan IP-osoitteen omasta välimuististaan ja palauttaa sen resolverille. Tämän jälkeen resolveri palauttaa vastaavan IP-osoitteen sovellukselle. Sekä itse kysely että siihen liittyvä vastaus lähetetään UDP-paketteina. (Tanenbaum & Wetherall 2014, 611-612.) Jos DNS-palvelin sen sijaan ei tiedä oikeaa IP-osoitetta eli sitä ei ole tallennettu joko välimuistiin tai tiedon katsotaan olevan vanhentunut, lähtee DNS-palvelin selvittämään IP-osoitetta muilta nimipalvelimilta. DNS-palvelin lähtee selvittämään IP-osoitetta puumaisen nimeämishierarkian mukaisesti, esimerkiksi www.oamk.fi lähdetään selvittämään ensin juuritason nimipalvelimelta, tämän jälkeen .fi selvitetään toiselta tasolta, oamk.fi kolmannelta ja lopuksi www.oamk.fi löytyy neljännen tason nimipalvelimelta.

DNS-nimipalvelu on myös altis ulkopuolisten hyökkäyksille ja tulee suojata esimerkiksi vahvojen salasanojen avulla tietomurroilta. DNS-palveluun kohdistuva hyökkäys on usein sellainen, että hyökkääjä ohjaa liikenteen DNS-palvelun avulla oikean verkkosivun sijasta hyökkääjän määrittelemälle haitalliselle sivustolle. Näin hyökkääjä voi esimerkiksi saada käsiinsä käyttäjätunnuksia, salasanoja, sähköpostiosoitteita tai jopa maksuvälinetietoja. Karinen toteaakin, että ilman DNS-

palvelun tietoturvan parannusta, se tulee olemaan tulevaisuudessa altis hyökkäyksille. (2014, 16-17).

2.4 Tietoturva ja palomuurit

Monelle yritykselle tärkein omaisuus on heidän tietoverkkoonsa tallentamansa tieto ja näin ollen on olennaisen tärkeää suojata tuo kyseinen tieto ulkopuolisten luvattomalta pääsyltä, pahimmassa tapauksessa vaakalaudalla voi olla koko yrityksen tulevaisuus. Nykypäivänä tietoverkkoon ja sen liikenteeseen kohdistuu useita erilaisia uhkia, jotka pitää ottaa huomioon jo verkkoa suunniteltaessa. Tietoturva on otettava huomioon käytännöllisesti katsoen jokaisessa tietoverkkoihin liittyvässä asiassa eikä tietoturva pelkästään rajoitu viruksiin ja matoihin, joihin se niin usein liitetään. Esimerkiksi palvelimet tulee sijoittaa siten, että ne ovat fyysisesti suojassa niin luonnonilmiöiltä kuin ihmisiltäkin, strategisesti tärkeisiin tiloihin tulee huolehtia esimerkiksi kulunvalvonta ja kameravalvonta ja tietoturva tulee ottaa huomioon jopa itse verkkokaapeleiden asennuksessa. Myös suojaamattomat langattomat verkot ovat uhka tietoverkon tietoturvalle.

Edellä mainittujen lisäksi uhkatekijöitä tietoturvalle ovat myös erilaiset hyökkäykset, kuten esimerkiksi sosiaalinen manipulointi (*social engineering*), salasanan murtaminen (*password cracking*), tietoliikenteen haistelu (*packet sniffing*) ja palvelun esto (*denial of service*) (Beasley & Nilkaew 2012, luvut 12-2 ja 12-3). On ensisijaisen tärkeää, että yrityksen johto on sitoutunut tarvittaviin toimiin tietoturvan takaamiseksi, tämä pitää sisällään niin tarvittavien resurssien takaamisen kuin henkilöstön kouluttamisenkin. Henkilöstön tulee osata varautua esimerkiksi sosiaaliseen manipulointiin ja heidän tulee ymmärtää vaatimukset liittyen salasanoihin. Itse tietoverkon tietoturvaa voidaan lisätä esimerkiksi käyttämällä VPN-yhteyttä ja erilaisia salaus- ja tunnelointiprotokollia.

Yksi tietoturvan ja riskinhallinan tärkeimmistä näkökulmista on käyttäjätunnukset sekä käyttövaltuuksien hallinta. Käyttäjätunnuksia voi olla kahden tyyppisiä: tietokoneille voi olla määriteltynä paikallisia käyttäjätunnuksia, joilla voidaan käyttää kyseistä tietokonetta ja tämän lisäksi on olemassa toimialueelle määriteltyjä käyttäjätunnuksia, joiden avulla määritellään oikeuksia itse tietoverkkoon sekä sen resursseihin. Tyypillisesti esimerkiksi yrityksen tietoverkossa olevat käyttäjätunnukset ovat nimenomaan toimialueen käyttäjätunnuksia. Jokaisella yksittäisellä tietoverkon käyttäjällä tulee olla käyttäjätunnus ja hänen oikeuksiaan tietoverkon resursseihin kontrolloidaan

käyttäjähakemistopalvelun, kuten aktiivihakemiston, ryhmäjäsenyyksillä. Esimerkiksi verkkolevylle voi olla määriteltynä käyttäjäksi kirjoitusoikeuksilla jokin tietty ryhmä, johon sitten lisätään yksittäiset käyttäjät ja näin ollen he saavat oikeudet kyseiselle verkkolevylle. Tietoturvan kannalta onkin tärkeää, että yrityksellä on määriteltynä tietoturvapolitiikka ja henkilöille lisätään oikeudet ainoastaan sellaiseen informaatioon, johon heidän työnkuvansa puolesta tulee päästä. Yrityksen tietoturvaan kohdistuvat uhat eivät tule ainoastaan yrityksen ulkopuolelta vaan uhka voi tulla myös yrityksen sisältä, esimerkiksi henkilöiden tahattomasta tai tahallisesta toiminnasta johtuen.

Palomuuri

Toinen tietoturvan kannalta tärkeimmistä asioista on toimiva palomuuri. Palomuurin tarkoitus on suojata tietoverkkoja ja/tai yksittäisiä laitteita estämällä ei-toivottua liikennettä niin sisäänpäin kuin ulospäinkin. Palomuurin voidaankin ajatella olevan eräänlainen portinvartija ja jos palomuuri itsessään on hyökkäyksen kohteena, se tyypillisesti kytkee itsensä verkosta ja samalla estää haitallisen liikenteen pääsyn verkkoon. Palomuuri käytännössä keskeyttää tiedonsiirron hetkellisesti tutkiakseen liikkuvia paketteja ja istuntoja, jos palomuurille tuleva liikenne ei ole sallittua, sen pääsy verkkoon estetään. Liikenteen ja pakettien suodattaminen voi tapahtua joko staattisesti (static packet filtering) tai dynaamisesti (dynamic packet filtering) riippuen siitä tutkitaan paketista ainoastaan otsikkotietoa vai myös paketin sisältöä ja sitä, että kuuluuko se olemassa olevaan istuntoon.

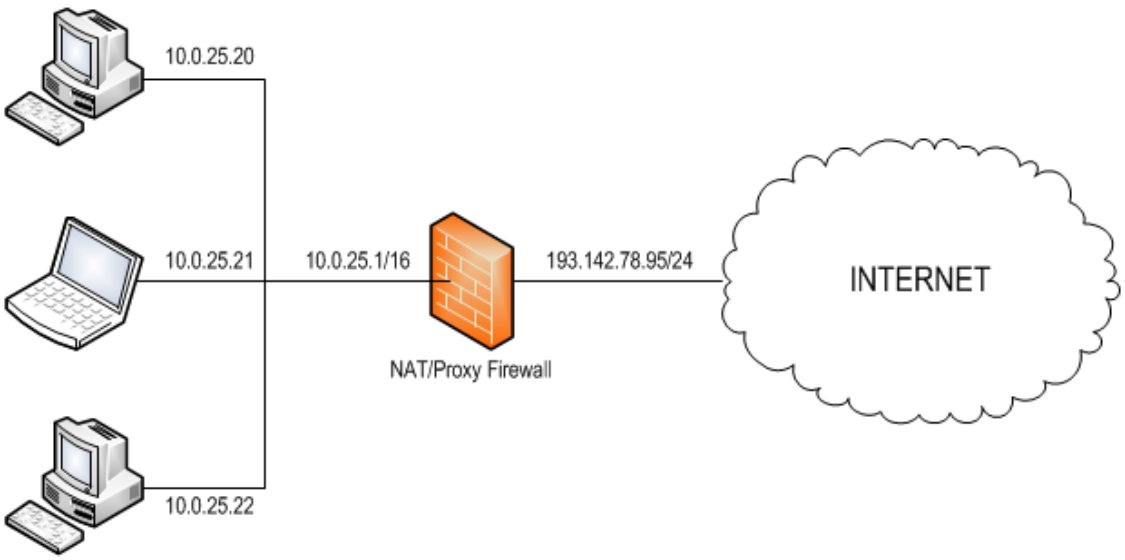
Yrityksen tietoverkkoa suojaava palomuurin tulee sijaita yrityksen oman tietoverkon ja internetin välissä. Tämän lisäksi lähes aina tietokoneissa on ohjelmistollisesti toteutettu palomuuri suojaamassa itse käyttäjän tietokonetta ja yleensä palvelimetkin ovat suojattuja omalla palomuurillaan. Perinteisesti palomuureissa on määritelty säännöillä mikä liikenne siitä pääse lävitse eli määritellään palomuurin läpäisevät IP-osoitteet, portit ja protokollat. Säännöt määritellään samalla tavalla oli sitten kyse sisäänpäin tulevasta tietoliikenteestä tai ulospäin lähtevästä. Palomuuri yleensä konfiguroidaan periaatteella *kiellä oletusarvoisesti – salli poikkeuksilla*. Perinteisen palomuurin rinnalle on viimeaikoina noussut niin sanotut sisältötietoiset palomuurit, joille määritellään säännöt niille tulevan liikenteen perusteella. Palomuuri myös kirjaa ylös kaiken saapuvan ja lähtevän liikenteen lokiin, joka mahdollistaa myöhemmän analysoinnin ja sen pohjalta tarvittavien toimenpiteiden suunnittelun. (Stewart, J. Michael 2014, 57-61.) Palomuurilla voi olla myös muita funktioita kuten esimerkiksi verkko-osoitteiden muunnos (Network Address Translation), jossa palomuurilla

muutetaan saapuvan liikenteen IP-osoite toiseksi esimerkiksi julkista siirtokanavaa varten (Stewart, J. Michael 2014, 70).

Palomuurit voidaan luokitella esimerkiksi sen mukaan ovatko ne ohjelmistollisesti toteutettuja vai fyysisiä laitteita. Ohjelmallinen palomuuri voi suojata ainoastaan yhtä isäntäkonetta kun taas fyysisellä laitteella voidaan suojata kokonainen järjestelmä tai verkko. Ohjelmallinen palomuuri jakaa resurssit isäntäkoneen muiden aktiivisien prosessien kanssa, kun taas fyysinen laitteisto on omistettu ainoastaan toimimaan palomuurina eivätkä muut prosessit kilpaile sen resursseista. Ohjelmallisesti suojatussa isäntäkoneessa on yleensä muitakin tietoturvan kannalta oleellisia komponentteja kuten esimerkiksi laitteisto, käyttöjärjestelmä ja muut ohjelmistot. Ohjelmallisesti toteuttu palomuuri on yleensä halvempi kuin fyysinen palomuuri. (Stewart, J. Michael 2014, 72).

2.5 Osoitteenmuunnos (Network Address Translation, NAT)

Osoitteenmuunnosta käytetään sisäisten IP-osoitteiden muuttamiseksi ulkoisiksi IP-osoitteiksi ja toisinpäin (kuvio 2). Osoitteenmuunnoksen tärkein tehtävä on estää ulkopuolisilta näkyvyys sisäisiin IP-osoitteisiin sekä verkon asetuksiin. Toisekseen osoitteenmuunnos vähentää tarvetta julkisten IP-osoitteiden määrälle, ilman osoitteenmuunnosta tarvittaisiin oma julkinen IP-osoite jokaiselle asiakaskoneelle, joka tarvitsee pääsyn julkiseen internettiin.



KUVIO 2. Osoitteenmuunnos palomuurilla sisäverkon ja ulkoverkon välillä

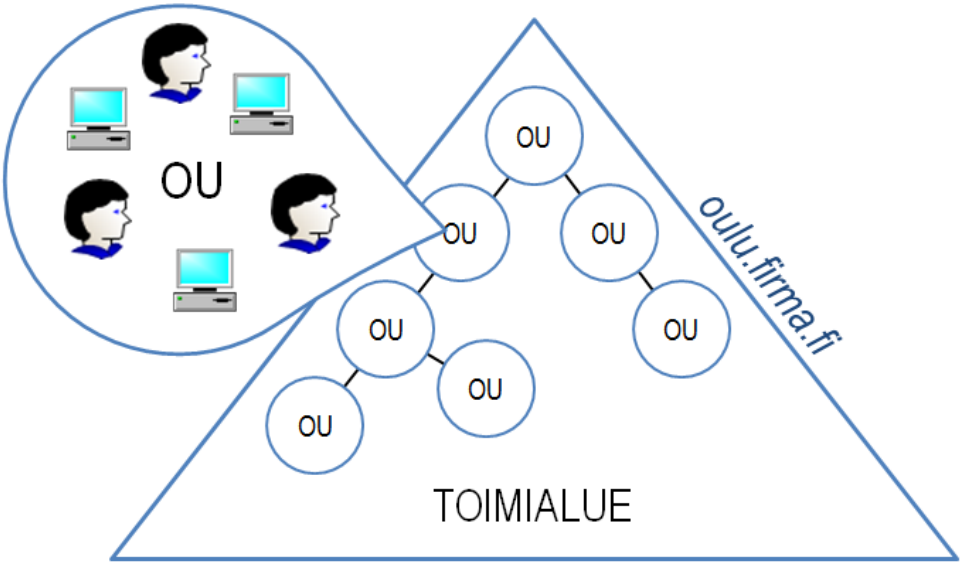
Osoitteenmuunnos on mahdollista, koska liikenne julkiseen internettiin ei ole yleensä jatkuvaa ja pitkäkestoista vaan hetkittäistä ja lyhytkestoista. Toisekseen osoitteenmuunnos varaa julkisen IP-osoitteen asiakaskoneen käyttöön ainoastaan tarvittavaksi ajaksi ja palauttaa sen takaisin vapaaksi kun istunto on päättynyt. Tämän lisäksi osoitteenmuunnos usein hyödyntää myös portteja (Port Address Translation, PAT), joka mahdollistaa saman IP-osoitteen yhtäaikaisen käytön usean asiakaskoneen toimesta. (Stewart, J. Michael 2014, 29-31).

2.6 Aktiivihakemisto (Active Directory, AD)

Käyttäjätunnukset, ryhmät sekä resurssit hallinoidaan Windows-toimialueella aktiivihakemistossa. Aktiivihakemisto autentikoi kaikki käyttäjät sekä tietokoneet ja määrittelee heille tarvittavat oikeudet ennalta määritettyjen turvallisuuspolitiikkojen kautta (Microsoft Technet 2007, viitattu 29.10.2014).

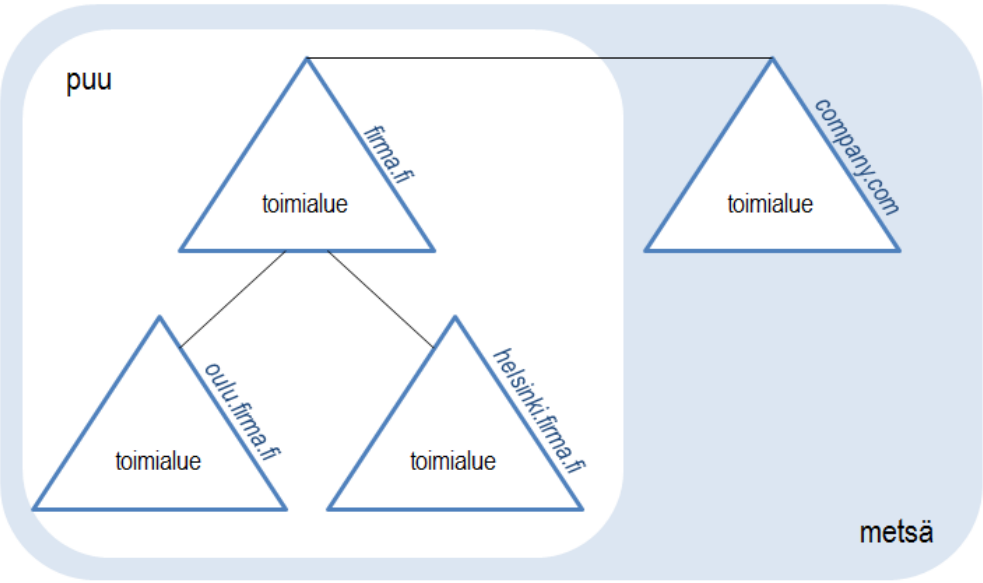
Aktiivihakemisto on Microsoftin verkkokäyttöjärjestelmä, joka alun perin esiteltiin Windows 2000 Server palvelintuotteen yhteydessä. Aktiivihakemisto on keskitetty säilytyspaikka yrityksen tietoverkon käyttäjistä, ryhmistä, tietokoneista, tulostimista, ohjelmistoista sekä palveluista. Tietoa aktiivihakemistossa voidaan myös strukturoida hierarkiseksi rakenteeksi esimerkiksi käyttämällä seuraavia komponentteja: objekti, organisaatioyksikkö (*organizational unit, OU*), toimialue (*domain*), puu (*tree*) ja metsä (*forest*). Objekteja voi olla ylätasolla kahdenlaisia: resursseja (esimerkiksi verkkolevyt, tulostimet) sekä kohteita, joihin turvallisuuspolitiikoita sovelletaan (käyttäjät, tietokoneet, ryhmät). Objekteilla on myös määriteltyjä ominaisuuksia, esimerkiksi käyttäjällä on nimi. (Desmond, Richards, Allen & Lowe-Norris 2013, luku 1-2.)

Toimialue pitää sisällään objektit, eli esimerkiksi tietokoneet ja käyttäjät. Toimialueen sisällä olevat objektit voidaan ryhmitellä hierarkisesti organisaatioyksiköiden avulla (kuvio 3). Organisaatioyksikön voidaan ajatella olevan tavallaan kansio, joka pitää sisällään loogisen ryhmän objekteja. Esimerkiksi tietyllä osastolla työskenteleville henkilöille ja heidän käytössään oleville tietokoneille voidaan luoda oma organisaatioyksikkö (OU).



KUVIO 3. Toimialueen hierarkinen OU-rakenne sekä objektit

Toimialueet ovat hallinnollinen kokonaisuus objekteja, joilla on yhteinen hakemistotietokanta, turvallisuuspolitiikka sekä luottamussuhde muiden toimialueiden kanssa. Toimialue voi kattaa useita eri fyysisiä paikkoja ja voi pitää sisällään miljoonia objekteja. Puut puolestaan ovat kokoelma toimialueita, jotka ryhmitelty hierarkisesti yhteen (kuvio 4). Puuhun liitetyllä toimialueella on transitiivinen luottamussuhde muihin puissa oleviin toimialueisiin. Metsä puolestaan koostuu puista ja metsässä yhteistä on hakemistopalveluiden rakenne, hakemiston hakupalvelu sekä aktiivihakemiston konfiguraatio. (Microsoft Technet 2014b, viitattu 25.11.2014.)



KUVIO 4. Metsät, puut, toimialueet sekä niiden keskinäiset suhteet

Objektien oikeuksia resursseihin voidaan hallinnoida aktiivihakemistossa ryhmien (security group) avulla. Oikeudet voidaan määritellä joko objektille tai jollekin tietylle objektin ominaisuudelle. Esimerkiksi verkkohakemistoa varten voidaan luoda oma ryhmänsä, jonka kautta oikeuksia kyseenomaiselle verkkolevylle hallinnoidaan. Kun käyttäjä eli objekti lisätään kyseiseen ryhmään, saa hän oikeudet kyseiselle verkkolevylle.

Aktiivihakemisto käyttää Lightweight Directory Access Protocol (LDAP) verkkoprotokollaa käyttäjien tunnistamiseen sekä heidän käyttöoikeuksiensa tarkistamiseen. Kyseessä on käytännössä hakemistopalvelu, jossa on tallennettuna tiedot käyttäjistä sekä heidän oikeuksistaan. LDAP-protokollaan perustuva käyttäjien tunnistaminen esimerkiksi VPN-yhteyksissä tekee siitä käytännössä tehokkaamman sekä parantaa ratkaisun tietoturvaa (Shrivastava & Rizvi 2014, 50-54).

2.7 Etätyöpöytä (Remote Desktop)

Yksi mielenkiintoinen tietoverkkojen hyödyntämiskohde on tietokoneiden etäkäyttö. Tietoverkossa voidaan jakaa niin verkkoyhteyttä, sovelluksia kuin resurssejakin. Esimerkkeinä jaettavista resursseista mainittakoot verkkolevyt ja tulostimet. Tämän lisäksi tietokonetta voidaan käyttää verkon ylitse virtuaalisesti aivan kuin oltaisiin käyttämässä itse laitetta fyysisesti. Etätyöpöydän avulla voidaan käyttää laitteen näyttöä, voit ajaa sen ohjelmia, käyttää sen tulostimia, kirjoittaa sen näppäimistöllä, siirtää sen hiirtä, hallita sen tiedostoja ja niin edelleen. (Pogue 2013, luku 7, Remote Desktop.)

Etätyöpöydän avulla voit esimerkiksi hallita useita työasemia ylläpitäjänä keskitetysti yhdeltä palvelimelta ja suorittaa sovelluksien asennuksia tai niiden päivityksiä (Microsoft Technet 2014a, viitattu 06.11.2014). Toisena esimerkkinä etätyöpöydän hyödyllisyydestä voidaan nostaa esille tilanne, jossa opiskelijat ottavat VPN-yhteyden kotoaan virtuaaliseen työasemaan koulun verkossa ja käyttää etätyöpöytää kuin he olisivat itse koneen ääressä koulun tiloissa. Rajoituksena ovat ainoastaan välittäjänä toimivan tietoverkon nopeus ja kykenemättömyys lisätä tai poistaa tietokoneeseen fyysisesti kytkettyjä laitteita (Stewart, J. Michael 2014, 17).

Etätyöpöytäprotokollia on olemassa lukuisia ja näiden päälle rakennettuja sovelluksia vielä huomattavasti enemmän, jotkut sovellukset käyttävät myös omaa protokollaansa sekä välityspalvelinta. Varmasti yleisin ja tunnetuin sovellus on Microsoftin oma Remote Desktop Services, joka käyt-

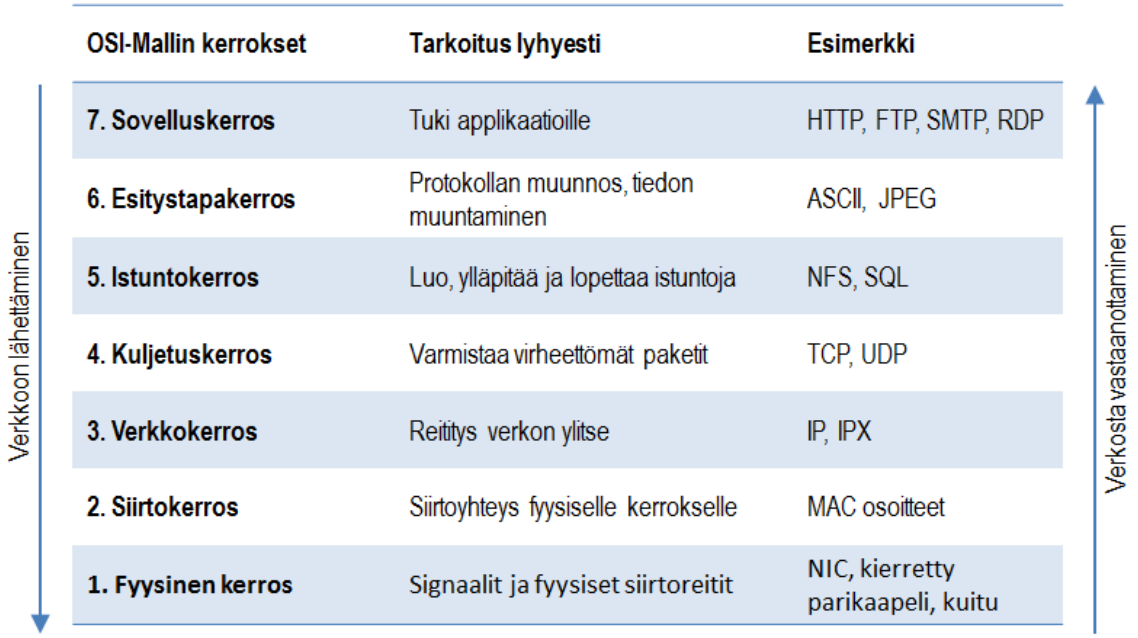
tää Remote Desktop protokollaa (RDP), joka tulee oletuksena jokaisen Microsoftin käyttöjärjestelmätuotteen mukana. Myös Linux-käyttöjärjestelmään on saatavilla RDP-protokollaa tukevia asiakasohjelmistoja. RDP-protokollossa palvelimen päässä graafinen informaatio koodataan RDP-protokollaa käyttävän ajurin toimesta ja lähetetään verkon ylitse asiakaskoneelle. Asiakaskone puolestaan tulkitsee koodatun informaation ja tämän jälkeen näyttää sen asiakaskoneella.

Microsoftin RDP-protokolla pitää sisällään erinäisiä toiminnallisuuksia, joista seuraavaksi lyhyesti. RDP käyttää RSA Security:n RC4 salausta informaatiolle, joko 56- tai 128-bittisenä. Erinäisiä mekanismeja vaadittavan kaistanleveyden minimointiin, esimerkiksi siirrettävän informaation pakkausta ja välimuistin käyttöä. RDP myös kykenee palauttamaan käyttäjän istunnon automaattisesti, jos yhteys syystä tai toisesta vahingossa katkeaa. RDP-protokolla mahdollistaa myös palvelimelta tulostamisen asiakaskoneeseen kytkettyyn tulostimeen. (Lobo & Lakshman 2014, luku 3, Remote Desktop Protocol.)

Tietoturvamielessä myös Microsoftin Remote Desktop Protocol asettaa omat haasteensa, vuonna 2011 uutisoitiin uudenlaisista verkkomadoista, jotka leviävät nimenomaan RDP-tekniikkaa käyttäen. Yksi näistä verkkomadoista oli nimeltään *Morto*. (Andreasson & Koivisto 2013, 15.) Käytännössä RDP-protokollan kanssa käytetäänkin lähes poikkeuksetta VPN-yhteyttä, joka tekee ratkaisusta huomattavasti turvallisemman.

2.8 OSI-malli

OSI-mallilla (Open System Interconnection) kuvataan tiedonsiirtoprotokollat, jotka on jaettu seitsemään eri kerrokseen riippuen niiden roolista tiedonsiirrossa (kuvio 5). Jokainen kerros toimii itsenäisesti eli saa pyynnön ylemmältä kerrokselta, suorittaa omalle kerrokselle kuuluvan tehtävän ja tämän jälkeen antaa tehtävän alemman kerroksen suoritettavaksi. Yleisesti ottaen voidaan todeta, että mitä alemmas kerroksissa siirrytään, sitä kauempana ne ovat itse käyttäjästä ja sitä enemmän ne liittyvät itse verkkoon ja sen käyttämiin protokolliin.



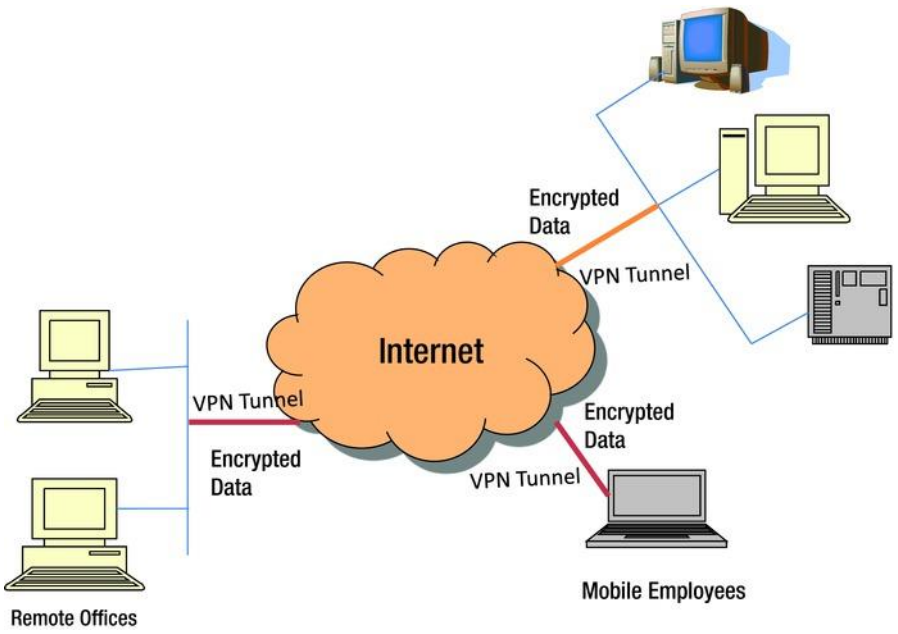
KUVIO 5. OSI-mallin seitsemän tiedonsiirron kerrosta (Beasley & Nilkaew 2012, luku 1-3, The OSI Model)

Sovelluskerros käsittää ne sovellukset, jotka ovat vuorovaikutuksessa tietoverkon kanssa eli esimerkiksi HTTP on tähän kerrokseen kuuluva protokolla ja varmaankin käytetyin ja tunnetuin sovelluskerroksen protokollista. Tässä kerroksessa käytettävät sovellukset ovat käyttäjälle näkyviä sovelluksia. *Esitystapakerros* puolestaan voi muuttaa siirrettävän datan sellaiseen muotoon, että vastapuolen esitystapakerros osaa sen tulkita. Esitystapakerros voi myös esimerkiksi salata tai pakata siirrettävän datan tiedonsiirtoa varten. *Istuntokerros* puolestaan huolehtii, että ennen datan siirtoa tietokoneiden välille luodaan istunto. Tämän lisäksi istuntokerros huolehtii myös näiden istuntojen ylläpidosta sekä niiden päättämisestä. Tunnetuin kerroksen 4 protokolla on TCP. (Lowe 2010, 399-400.)

Kuljetuskerroksen tärkein tehtävä on varmistaa, että data siirtyy tietoverkon ylitse luotettavasti ja ilman virheitä. Kuljetuskerros myös usein jakaa suuret viestit pienemmiksi, jotta ne voidaan lähettää verkon ylitse tehokkaammin. *Verkkokerros* huolehtii reitityksestä tietokoneelta toiselle eli se varmistaa sopivan reitin koneiden välille. Tämän lisäksi verkkokerros huolehtii esimerkiksi verkko-osoitteiden määrittelyn verkon laitteille. Tunnetuin kerroksen 3 protokolla on IP. *Siirtokerros* varmistaa luotettavan siirtoyhteyden fyysiseen kerrokseen ja se sisältää sekä virheen tunnistusta että niiden korjausta. Siirtokerroksella on myös toinen tehtävä, nimittäin ylläpitää taulua laitteiden fyysisistä MAC-osoitteista. *Fyysisen kerroksen* tehtävä on siirtää verkon ylitse binäärimuotoista informaatiota eli käytännössä bittejä, joiden arvo on joko 0 tai 1. Fyysisessä kerroksessa määritellään verkon fyysisiä ominaisuuksia kuten esimerkiksi kaapelit, liittimet ja kaapeleiden pituudet. Esimerkkinä kerroksen 1 laitteesta on toistin, jonka tehtävä on vahvistaa signaali kun kaapelin pituus ylittää fyysisen kerroksen määrittelemän arvon. (Lowe 2010, 396-399.)

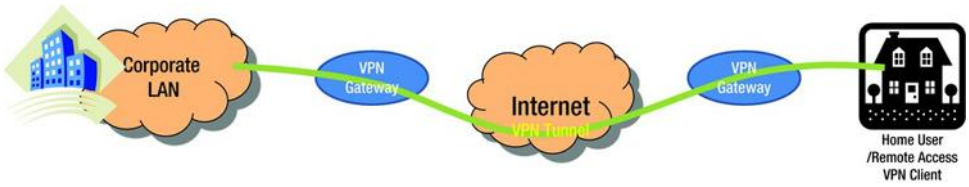
2.9 Virtual Private Network (VPN)

Yleensä vain fyysisesti samassa tietoverkossa olevia laitteita pidetään lähtökohtaisesti turvallisina. VPN-yhteys tarjoaa turvallisen ja suojatun tavan kytkeytyä tietoverkkoon julkisen internetin ylitse (kuvio 6). VPN luo virtuaalisen tunnelin kahden pisteen välille ja tieto lähetetään turvallisesti tätä tunnelia pitkin julkisen internetin ylitse (Rao & Nayak 2014, luku 12, Introduction). VPN-yhteys varmistaa, että liikenne on salattua, se siirtyy koskemattomana ja käyttäjät autentikoituja. Esimerkiksi yrityksen työntekijä voi työskennellä kotoa käsin ja siitä huolimatta käyttää yrityksensä tietoverkon tarjoamia resursseja turvallisesti. Tällaista internetin ylitse luotavaa virtuaalista tietoverkkoa kutsutaan IP-tunneliksi.



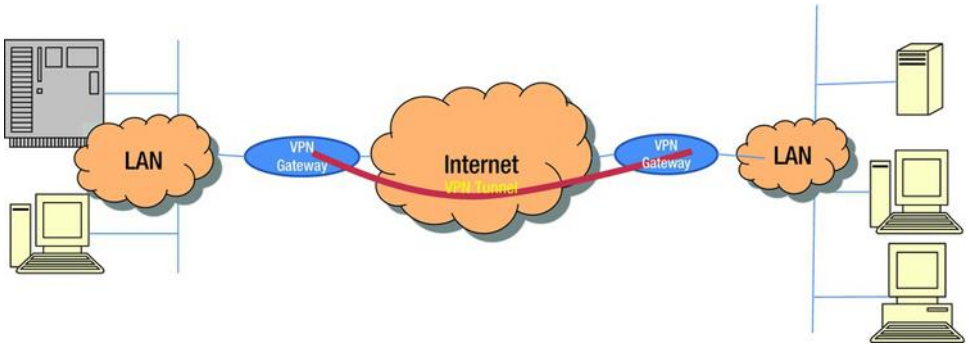
KUVIO 6. VPN-yhteys yrityksen verkkoon internetin ylitse (Rao & Nayak 2014, luku 12, Introduction)

Useimmissa tietoverkoissa VPN-tunneli mahdollistetaan palomuurireitittimen avulla, joka tukee VPN liikennettä. Tämän VPN-palvelimen tulee sijaita yrityksen demilitarisoidulla alueella (DMZ) eli aliverkossa, joka yhdistää yrityksen intranetin internettiin. Yleensä toisessa päässä tunnelia, eli loppukäyttäjän päässä, on ohjelmistopohjainen VPN-ratkaisu, joka käyttäjän tulee asentaa ja konfiguroida käyttöön. (Lowe 2010, 231-232.) Tällaiselle ratkaisulle käytetään nimitystä *remote access VPN* (kuvio 7).



KUVIO 7. Remote access VPN (Rao & Nayak 2014, luku 12, VPN Types)

Toisen tyyppinen ratkaisu on niin sanottu *site-to-site VPN* (kuvio 8), jossa ratkaisu toteutetaan yleensä molemmissa päässä joko reitittimen tai palomuurin avulla eli rautapohjaisesti (Beasley & Nilkaew 2012, luku 12-5). Tällainen ratkaisu sopii esimerkiksi kiinteäksi ratkaisuksi kahden toimipisteen tietoverkkojen välille tai vaihtoehtoisesti yrityksen ja heidän alihankkijan väliseksi kiinteäksi yhteydeksi. Yleensä remote access VPN-ratkaisussa käyttäjä antaa alkusysäyksen VPN-yhteyden muodostukselle käynnistämällä VPN-ohjelmiston, kun taas site-to-site VPN-ratkaisussa salattu yhteys on oletusarvoisesti aina olemassa ja näiden tietoverkkojen välinen tiedonsiirto salataan aina automaattisesti.



KUVIO 8. Site-to-site VPN (Rao & Nayak 2014, luku 12, VPN Types)

Koska VPN-teknologiaa voidaan käyttää hyväkseen esimerkiksi toimipisteiden väliseen tiedonsiirtoon eikä pelkästään tietoverkon sisältämien resurssien etäkäyttöön, on olemassa useitakin verkkotopologisia ratkaisuja, jotka määrittelevät kuinka ne kytkeytyvät toisiinsa. Esimerkkeinä mainittakoot *Hub-and-Spoke, Point-to-Point* ja *Full Mesh*. (Cisco 2014, luku 24, viitattu 31.10.2014.)

VPN hyödyt ja haitat

Turvallisen etäkäyttöratkaisun lisäksi VPN tarjoaa muitakin hyötyjä kuten esimerkiksi kustannussäästöt, koska liikenne menee julkisen internetin ylitse ja kiinteitä yhteyksiä ei tarvita esimerkiksi yrityksen ja sen käyttämien alihankkijoiden välille tai yrityksien omien toimipisteiden välille. VPN on myös helppo ja nopea pystyttää yrityksen nykyisen infrastruktuurin päälle ja se on myös helppo ylläpitää. (Rao & Nayak 2014, luku 12, Advantages of VPN.) VPN-yhteys tuo myös joustavuutta ja liikkuvuutta yrityksen työntekijöille, jotka VPN-yhteyden avulla voivat käyttää yrityksen resursseja mistä päin maailmaa tahansa, kunhan heillä on internet-yhteys.

VPN-yhteyksissä on tosin myös puutteita ja asioita, jotka tulee ottaa huomioon. Kun yrityksen työntekijät voivat päästä käsiksi luottamukselliseen tietoon yrityksen toimipisteen ulkopuolella sekä mahdollisesti käyttäen laitetta, joka ei ole yrityksen omistuksessa ja hallinnassa, tulee yrityksen varmistaa tietoturvapolitiikan ajantasaisuus ja että henkilöillä on pääsy ainoastaan heidän tarvitsemaan tietoon.

Toisekseen koska VPN-tunneli luodaan käyttäen julkista internet-yhteyttä, riippuu VPN-tunnelin nopeus paikallisesta internet-yhteyden nopeudesta. Useissa tapauksissa käyttäjät voivat istua fyysisesti hyvinkin kaukana käyttämistään palveluista ja tällöin täytyy suunnitella koko tiedonsiirtoketju tarkoin, jotta yhteyksissä ei synny pullonkaulaa. Esimerkiksi käyttäjä saattaa itse istua Aasiassa, mutta VPN-yhteys päätetään operaattorille Suomessa. Hänen tarvitsemansa palvelu yrityksen verkossa saattaa sijaita myös Aasiassa, mutta siitä huolimatta liikenne kiertää Suomen kautta julkista internet-yhteyttä pitkin, koska operaattorin palvelin sijaitsee Suomessa. Koska internet-yhteydet Aasiasta Eurooppaan ovat tyypillisesti hitaita, voi yhteyden hitaus muodostua ongelmaksi. VPN-yhteydet ovat yleisesti ottaen hitaampia ja niissä on enemmän viivettä kuin esimerkiksi kiinteissä yhteyksissä kahden toimipisteen välillä.

2.9.1 VPN-protokollat

VPN-tietoturva perustuu tunnelointi- sekä salausprotokolleihin, jotka varmistavat että liikenne on salattua sekä siirtyy koskemattomana ja että käyttäjät ovat autentikoituja. Ennenkuin tietoa voidaan alkaa lähettämään, täytyy turvallinen VPN-tunneli luoda. Jokaisen osapuolen täytyy tietää kuinka heidän tulee turvallisesti kommunikoida, kuinka tietoliikenne osapuolien välillä salataan ja osapuolten tulee vaihtaa salausavaimet. VPN-tunnelointi onkin käytännössä tietoliikennepakettien uudelleen paketointia.

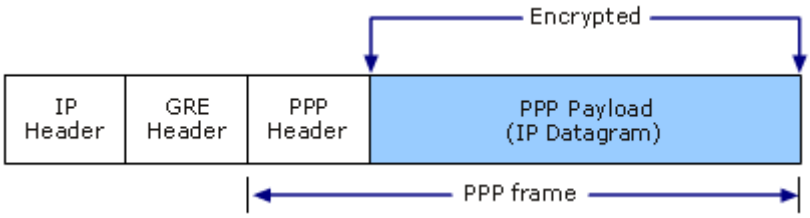
Point-to-Point Protocol (PPP)

PPP (Point-to-Point Protocol) oli modeemiaikana 1990-luvulla periaatteessa ainoa mahdollisuus kytkeytyä palveluntarjoajaan ja sitä kautta Internettiin. PPP kanssa voidaan käyttää käyttäjätunnistusta tarjoavia protokolleja kuten esimerkiksi PAP (Password Authentication Protocol) ja CHAP (Challenge Handshake Authentication Protocol). Useat VPN-tunnelointiprotokollat pohjautuvat edelleen Point-to-Point protokollaan. PPP autentikoi käyttäjän ennen tiedonsiirron aloittamista ja se tukee useita sovelluksia ja protokollia.

Point-to-Point Transport Protocol (PPTP)

PPTP (Point-to-Point Tunneling Protocol) kehitettiin vuonna 1996 Microsoftin, 3Comin sekä Alcatel-Lucentin toimesta. PPTP avulla voidaan luoda turvallinen PPP linkki TCP/IP yhteyden ylitse. PPTP koteloi PPP-paketit TCP/IP protokollan sisään lähettääkseen ne internetin ylitse ja tämän lisäksi se käyttää GRE (Generic Routing Encapsulation) protokollaa tunneloimiseen ja pakettien välittämiseen (kuvio 9). Itse Point-to-Point protokollaan se ei tee muutoksia. PPTP vaatii, että palvelimen ja asiakaskoneen välillä on olemassa oleva IP-yhteys. PPTP tukee niin PAP (Password Authentication Protocol) kuin CHAP (Challenge Handshake Authentication Protocol) autentikointimenetelmiä. PAP tarjoaa yksinkertaisen kahdensuuntaisen kättelyn kun yhteys on luotu. CHAP sen sijaan on kehittyneempi autentikointimenetelmä ja se tarjoaakin paremman suojan erinäisiä hyökkäyksiä vastaan kuin PAP. (Rao & Nayak 2014, luku 12, VPN Protocols.)

PPTP voidaan käyttää niin site-to-site VPN kuin remote access VPN yhteyksissäkin (Microsoft Technet 2008, viitattu 03.11.2014). Tosin IPSec ja SSL protokolliin pohjautuvat VPN-ratkaisut ovat korvaamassa PPTP ratkaisut ja Point-to-Point Transport protokollan kehitys onkin loppunut.



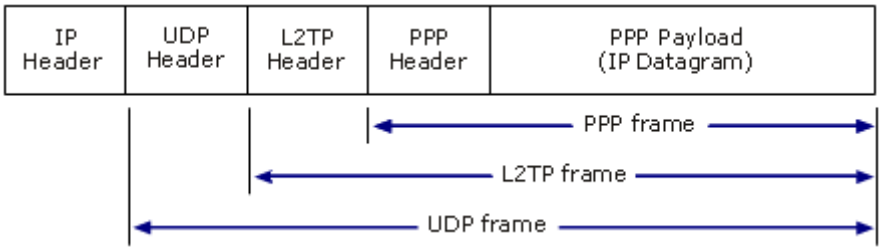
KUVIO 9. PPTP protokollan rakenne (Microsoft Technet 2008, viitattu 03.11.2014)

Layer 2 Forwarding Protocol (L2F)

L2F (Layer 2 Forwarding Protocol) on Ciscon kehittämä protokolla ja esiteltiin samoihin aikoihin kuin PPTP, mutta se ei yleistynyt koskaan kuluttajamarkkinoilla sen L2F laitteistovaatimuksien takia. Toisin kuin edellä esitelty PPTP, L2F ei vaadi erillistä client ohjelmistoa. Myöhemmin L2TP protokolla kehitettiin sekä PPTP että L2F protokolliin pohjautuen, seuraavaksi tarkemmin L2TP protokollasta. (Beasley & Nilkaew 2012, luku 12-5.)

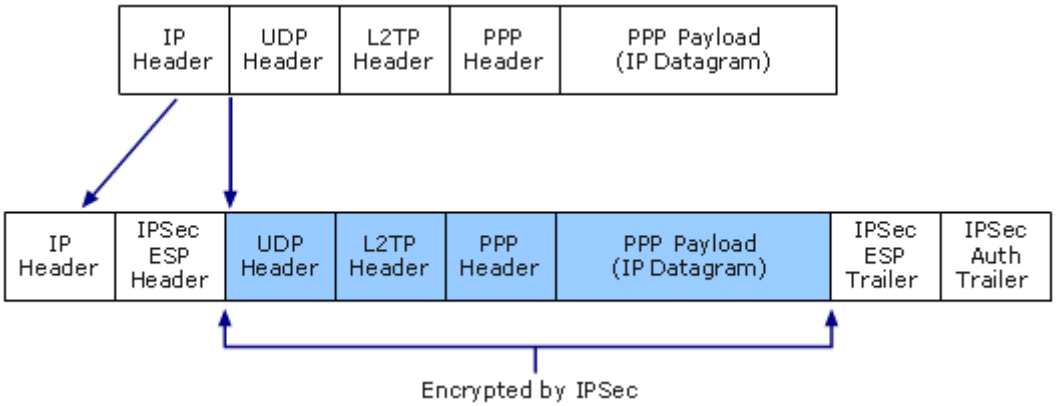
Layer 2 Tunneling Protocol (L2TP)

L2TP (Layer 2 Tunneling Protocol) esiteltiin vuonna 1999 ja sen tarkoitus yhdistää kahden aiemman eli PPTP ja L2F tunnelointiprotokkollien hyvät puolet. Se ei vaadi erillistä sitä tukevaa laitteistoa ja tunneli voidaan luoda suoraan asiakasohjelmistosta. L2TP tunnelointi tapahtuu UDP porttiin 1701 ja koska se sallii tunneloinnin, se ei tukeudu niin vahvasti Point-to-Point protokollaan (kuvio 10). Jos L2TP tunnelointiprotokollaa käytetään sellaisessa IP-verkossa, jossa PPP ei ole käytössä, tunneli voidaan luoda sen omilla autentikointimekanismeilla. (Beasley & Nilkaew 2012, luku 12-5.)



KUVIO 10. L2TP-paketin rakenne (Microsoft Technet 2008, viitattu 03.11.2014)

Koska L2TP protokolla itsessään ei sisällä salausta tai viestien luottamuksellisuutta, se usein implementoidaan yhdessä IPSec (Internet Protocol Security) protokollan kanssa eli L2TP paketit koteloidaan IPSec sisään (kuvio 11).



KUVIO 11. L2TP-paketti koteloituna IPSec-paketin sisään (Microsoft Technet 2008, viitattu 03.11.2014)

Internet Protocol Security (IPSec)

IPSec-protokolla (Internet Protocol Security) tarjoaa turvapalveluita IP-kerrokselle niin IPv4 kuin IPv6 protokollille. Sen tehtävänä on varmistaa, että liikenne on salattua sekä siirtyy koskemattomana ja että käyttäjät ovat autentikoituja. Ennenkuin IPSec tunneli voidaan luoda, sekä lähettäjän että vastaanottajan tulee välittää tunnelin perustamiseen liittyviä parametrejä, jotka IPSec välittää käyttäen IKE protokollaa (Internet Key Exchange). (Rao & Nayak 2014, luku 12, VPN Protocols.)

Mitä tulee itse tietoturvaprotokolliin, IPSec itse käyttää kahta tietoturvaprotokollaa (kuvio 12) eli AH (Authentication Header) ja ESP (Encapsulating Security Payload). AH varmentaa IP-pakettien aitouden sekä varmistaa niiden eheyden kahden tietoturva-algoritmin avulla, joita ovat MD5 (Message Digest 5) ja SHA-1 (Secure Hash Algorithm 1). ESP puolestaan salaa tietoliikenteen ja näin ollen varmistaa liikenteen luottamuksellisuuden kolmen algoritmin avulla: DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) ja AES (Advanced Encryption Standard). (Beasley & Nilkaew 2012, luku 12-5.)

IPSec-protokolla	Algoritmit	Käyttötarkoitus
AH (Authentication Header)	**MD5** (Message Digest 5) **SHA-1** (Secure Hash Algorithm 1)	Varmistaa IP-pakettien aitous sekä niiden eheys
ESP (Encapsulating Security Payload)	**DES** (Data Encryption Standard) **3DES** (Triple Data Encryption Standard) **AES** (Advanced Encryption Standard)	Tietoliikenteen salaus sekä liikenteen luottamuksellisuuden varmistaminen

KUVIO 12. IPSec-protokollan käyttämät tietoturvaprotokollat ja niiden algoritmit

Käytännössä IPSec paketoi IP-paketin uudestaan oman kehyksensä sisään (kuvio 11) ja se puretaan vasta vastaanottajan päässä. IPSec protokolla eroaakin muista aiemmin listatuista protokollista siinä, että se pitää sisällään salauksen. IPSec protokollaa voidaan käyttää niin remote access VPN ratkaisuissa kuin site-to-site VPN ratkaisuissakin.

Secure Socket Tunneling Protocol (SSTP)

SSTP (Secure Socket Tunneling Protocol) on uusin VPN-tunnelointiprotokolla ja se käyttää TCP/IP porttia 443 (HTTPS) liikenteen tunnelointiin. SSTP paketoi PPP kehykset suojatun HTTPS-protokollan (Hypertext Transfer Protocol Secure) ja SSL (Secure Sockets Layer) kanavan yli. SSL tarjoamia siirtokanavan tietoturvapalveluita ovat avaimien vaihto, liikenteen salaus ja siirtyvien pakettien eheyden tarkastus. (Microsoft Technet 2008, viitattu 03.11.2014.)

On tilanteita, joissa PPTP tai L2TP/IPSec protokollia ei voida käyttää, koska ne voivat olla esimerkiksi estettyinä. Käytännön esimerkkinä voitaisiin mainita hotellit, joissa usein VPN-siirtotie luodaan käyttäen SSTP protokollaa. SSTP sinällään tarjoaa hyvin turvallisen tavan siirtää dataa julkisessa IP-verkossa ja esimerkiksi internetselaimella käytettävät verkkopankkipalvelut toimivat poikkeuksetta SSL yli. Ongelmaksi näissä SSL suojatuissa yhteyksissä voi muodostua suorituskyky eli usein SSL VPN on suorituskyvyltään heikompi kuin esimerkiksi PPTP tai L2TP/IPSec. Sinällään SSL VPN käyttöönotto on asiakkaan kannalta helppo ja nopea, koska se ei tarvitse muuta ohjelmistoa asennettavaksi internetselaimen lisäksi.

2.9.2 Microsoft DirectAccess

Toimintaperiaate Microsoft DirectAccess -tuotteessa on hyvin samanlainen kuin VPN-yhteydessä, eli se tarjoaa tietoturvallisen tavan päästä käsiksi luottamukselliseen informaatioon sisäverkossa julkisen siirtotien, yleensä internetin, ylitse. DirectAccess-tuotteessa yhteyttä ei tarvitse erikseen muodostaa, vaan IPSec tunneli muodostuu automaattisesti kun henkilöllä on pääsy julkiseen internetiin. DirectAccess ei itsessään ole protokolla, vaan käytännössä se käyttää hyväkseen useita Microsoftin teknologioita palvelun tuottamiseen kuten aktiivihakemisto, IPSec, IPv6, digitaaliset sertifikaatit ja niin edelleen. DirectAccess eroaa VPN-yhteydestä siinä mielessä, että yhteys on kaksisuuntainen, jolloin esimerkiksi ylläpitäjät voivat ottaa yhteyden asiakaskoneeseen, käynnistää etätyöpöytäyhteyden ja suorittaa ylläpitotehtäviä asiakaskoneen päässä. Myös ohjelmistopäivitykset saadaan keskitetysti asennettua asiakaskoneille. (Krause 2013, luku Foreword.)

DirectAccess-yhteyden luominen on usein nopeampaa kuin VPN-yhteyden luominen, koska käyttäjän ei tarvitse käynnistää erillistä asiakasohjelmistoa ja kirjautua siihen erillisillä käyttäjätunnuksilla. Jos internet-yhteys katkeaa, joutuu käyttäjä luomaan VPN-yhteyden uudestaan kun taas DirectAcces hoitaa sen automaattisesti taustalla. Jos kaikki liikenne reititetään VPN-yhteyden ylitse, on VPN-yhteys myös yleensä hitaampi kuin DirectAccess. (Microsoft Technet 2009, viitattu 24.11.2014.)

DirectAccess julkaistiin Windows Server 2008 käyttöjärjestelmän myötä ja myöhemmin päivitetty versio Windows Server 2012 käyttöjärjestelmän mukana. Windows Server 2008 käyttöjärjestelmän mukana julkaistussa versiossa oli puutteita ja käytännössä se vaatikin esimerkiksi Microsoft Forefront Unified Access Gateway (UAG) asennuksen rinnalle. UAG mahdollisti esimerkiksi paremman käyttöliittymän konfigurointiin sekä sen mukana tulivat komponentit DNS64 ja NAT64, jotka puolestaan mahdollistivat DirectAccess asennuksen olemassa olevaan tietoverkkoon ilman tarvetta ottaa IPv6 käyttöön.

Tällä hetkellä uusin Windows Server 2012 mukana julkaistu DirectAccess versio on jo täysin integroitu käyttöjärjestelmään ja mahdollistaa myös etäkäyttäjille myös IPv4- ja NAT-verkkojen takana olevien palveluiden käyttöönoton. Tosin asiakasohjelmistot toimivat ainoastaan IPv6-protokollalla eikä niillä ole IPv4 mukaista osoitetta laisinkaan, DirectAccess palvelin hoitaa muunnoksen IPv4 ja IPv6 välillä ja se vaikuttaa hieman suorituskykyyn. DirectAccess käyttää joko 6to4,

Teredo tai IP-HTTPS tunnelointitekniikoita riippuen minkälaisessa verkossa se kulloinkin sijaitsee. (Horley 2013, luku 4, DirectAccess).

DirectAccess vaatii aktiivihakemiston toimiakseen, koska se käyttää aktiivihakemiston ryhmiä sekä niille määriteltyjä menettelytapoja hyväkseen asiakasohjelmistojen konfiguroinnissa. Käytännössä käyttäjän tunnistaminen, pääsynhallinta ja ryhmäpolitiikat toimivat täysin samalla tavalla kuin henkilö olisi suoraan kiinni yrityksen sisäverkossa. Sen sijaan Windows Server 2012 palvelinohjelmiston mukana tuleva versio ei enää vaadi julkisen avaimen infrastruktuuria (Public Key Infrastructure, PKI) toimiakseen, vaikkakin sitä edelleen on mahdollista käyttää. (Minasi, Green, Booth, Butler, McCabe, Panek, Rice & Roth 2013, luku 21, Introducing DirectAccess.)

2.9.3 Palo Alto Networks GlobalProtect

Palo Alto Networks on amerikkalainen yritys, joka on keskittynyt tietoverkkojen tietoturvaan ja heidän tärkeimmät tuotteensa ovat palomuureja, joiden avulla voidaan parantaa tietoverkon tietoturvaa sekä saada parempi näkyvyys ja hallittavuus yrityksen tietoverkkoon. Yrityksen valmistamat palomuurituotteet ovat niin sanottuja sisältötietoisia palomuureja eli niiden säännöt voidaan määritellä tulevan tai lähtevän liikenteen sisällön perusteella sen sijaan, että sääntöjä luotaisiin perinteisesti IP-osoitteiden, porttien ja protokollien mukaan. Tosin luonnollisesti heidän palomuurituotteitaan on mahdollista käyttää tälläkin tavalla.

Vuoden 2014 lopulla heillä on 6 fyysistä palomuurituoteperhettä sekä tämän lisäksi 4 virtuaalista ratkaisua. Tuotteet eroavat toisistaan lähinnä nopeuden, käyttäjämäärien sekä yhtäaikaisten istuntojen lukumäärien osalta eli heillä on tarjota ratkaisut niin isoon yritysverkkoon kuin pienempään toimistoonkin. Virtuaaliset ratkaisut tulevat valmiiksi esiasennettuina paketteina erinäisiin virtuaalisiin ympäristöihin, vuoden 2014 lopulla tuetut ovat VMWare, Citrix, KVM ja Amazon AWS.

Palo Alto Networksin tuotteet soveltuvat niin remote access VPN kuin site-to-site VPN ratkaisuihin ja tukevat sekä SSL että IPSec VPN-yhteyksiä (Palo Alto Networks 2014b, viitattu 19.11.2014). GlobelProtect käyttää IPSec-tunnelointiprotokollan lisäksi AES lohkosalausmenetelmää joko 128- tai 256-bittisenä.

Tuotteet saadaan integroitua aktiivihakemiston sekä LDAP:in (Lightweight Directory Access Protocol) kanssa, joten käyttäjät saadaan tunnistettua käyttäen Windowsin sisäänrakennettuja mekanismeja eikä erillistä käyttäjähallintaa tarvita. Käyttäjien tunnistamisessa voidaan käyttää sertifikaatteihin tai käyttäjätunnuksiin perustuvaa tunnistamista.

Oli kyse sitten fyysisestä tai virtuaalisesta palomuurista, niin tuotteen mukana tulee graafinen ohjelmisto palomuurin konfigurointia sekä hallintaa varten. Tällä oletusarvoisesti tuotteen mukana tulevalla ohjelmistolla ei ole varsinaisesti erillistä nimeä, mutta se on laajennettavissa Panorama nimisellä tuotteella, joka tuo keskitetyn hallinnan ja esimerkiksi lokien pidempiaikaisen säilytyksen sekä raportoinnin.

Palomuurituotteiden mukana tulee myös ilmaisversiot asiakasohjelmistoista, jotka ovat ladattavissa suoraan palomuurilta ja joiden avulla voidaan luoda VPN-yhteys kyseiseen palomuuriin. Palo Alto Networks käyttää niin asiakasohjelmistostaan kuin itse palomuurin VPN-ominaisuuksista nimitystä GlobalProtect, asiakasohjelmisto on saatavilla Windows, OS X, iOS ja Android laitteille. GlobalProtect-tuotteesta on olemassa myös maksullinen versio, jonka mukana saa esimerkiksi HIP-ominaisuudet (Host Information Profiles). HIP-ominaisuuksilla tarkoitetaan tietoisuutta päätelaitteista, joka käytännössä tarkoittaa, että se kykenee tunnistamaan onko asiakaskoneessa esimerkiksi kovalevy kryptattu tai virusohjelmisto ajantasalla. Tämän tiedon perusteella voidaan kieltää tai sallia esimerkiksi ohjelmistojen käyttö VPN-yhteyden ylitse. On mahdollista käyttää myös kolmannen osapuolen asiakasohjelmistoja kunhan ne tukevat IPSec-protokollaa. Tällöin kuitenkin ongelmaksi voi muodostua esimerkiksi yhteydet hotelleista ja muista vastaavista paikoista, jotka eivät salli IPSec-yhteyttä. Palo Alto Networksin omat asiakasohjelmistot tukevat myös SSL/HTTPS-yhteyksiä niissä tilanteissa, kun tietoverkko ei salli IPSec –yhteyttä.

Palo Alto Networks tuotteet eroavat kilpailijoiden ja markkinoilla olevien ilmaisten avoimen lähdekoodin tuotteista lähinnä siten, että palomuuri ja VPN-toiminnallisuus on yhdistettynä samassa tuotteessa, jolloin kokonaisuudesta tulee helposti hallittavissa oleva kokonaisuus sekä myös tietoturvallisempi ratkaisu. Perinteisesti palomuuri on toiminut siten, että siihen on avattu reikiä niin sisään- kuin ulostulevallekin liikenteelle IP-osoitteiden ja porttien perusteella. Palo Alto Networksin palomuureissa on mahdollista tunnistaa käyttäjät, ryhmitellä sovelluksia ja luoda oikeuskäytänteitä sen mukaan mihin sovelluksiin käyttäjien tulee päästä käsiksi. Samat oikeudet toimivat tämän jälkeen, tulipa käyttäjä sisäverkosta tai etäyhteyden ylitse. Verrattuna esimerkiksi Microsoftin DirectAccess VPN-ratkaisuun, jossa kyseessä on ainoastaan VPN-tunneli ja jos joku pääse

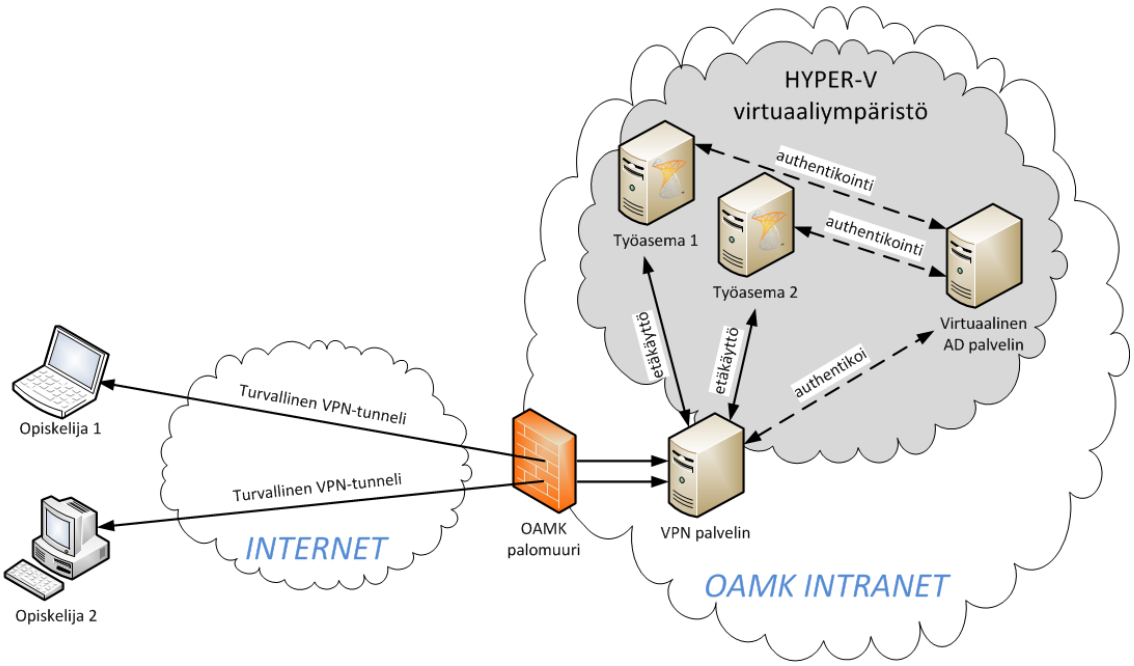
sisäverkkoon, pääsee hän sen jälkeen kaikkialle. Sisältötietoisessa palomuurissa tarvittaessa voidaan rajata käyttäjän pääsy ennalta hänelle määriteltyihin sovelluksiin ja/tai verkkosegmentteihin.

Yksi mielenkiintoinen ominaisuus Palo Alto Networksin -tuotteissa on niin sanottu *WildFire*. Tietoturvan kannalta haastavia ovat ennestään tuntemattomat uhat, jotka kohdistuvat esimerkiksi tietoverkkoihin. Koska nämä uhat ovat ennestään tuntemattomia, ei niitä vastaan ole useinkaan myöskään keinoja puolustautua. WildFire on pilvipalvelu, jonka avulla tieto tällaisista uhkatekijöistä, niiden tunnistamisesta ja torjumisesta voidaan levittää maailmanlaajuisesti viidessätoista minuutissa. Näin tarjotaan WildFire-ominaisuuden käyttäjille ajantasainen suojaus ennestään tuntemattomia uhkia vastaan. (Palo Alto Networks 2014c, viitattu 28.11.2014.)

Yhteenvetona Palo Alto Networksin tuotteista voitaisiin todeta, että ne ovat palomuurituotteita, joissa on keskitetty turvallisuuspolitiikkojen luonti ja hallinta sekä mahdollisuus segmentoida verkko osiin. Näin ollen kokonaisuus ei ole hallitsematon ja hajautettu. Ne myös tarjoavat lähes rajattomat mahdollisuudet tietoliikenteen monitorointiin sekä monipuoliset raportointimahdollisuudet.

3 NYKYISEN YMPÄRISTÖN KUVAUS

Nykyisellääänkin laboratoriotilaan on olemassa VPN-yhteys. Opiskelijat voivat käyttää omalta työasemaltaan VPN-yhteydellä virtuaalisia palvelimia, joihin on asennettu esimerkiksi Sharepoint palvelimet. Oppilaat käynnistävät koneeltaan Microsoftin oman VPN-asiakasohjelmiston ja liikenne menee suojattua VPN-tunnelia pitkin julkisen internetin ylitse aina OAMK:n palomuurille saakka. Palomuuriin on konfiguroitu avoinaiseksi niin VPN-yhteys palvelimelle kuin esimerkiksi remote desktopin käyttämä protokolla (kuvio 13).



KUVIO 13. Nykyinen VPN-ratkaisu kuvattuna ylätasolla

VPN-yhteyttä siis hoitaa yksi fyysinen palvelin ja joka puolestaan autentikoi käyttäjät omalta virtuaalisesta aktiivihakemistosta ja tämän jälkeen ohjaa liikenteen virtuaalisille työasemille esimerkiksi Sharepoint käyttöä varten. Jokaisella oppilaalla on oma tunnuksensa, hänelle henkilökohtaisesti määritelty virtuaalinen työasema ja luonnollisesti salasana. Virtuaaliympäristö on toteutettu Hyper-V ympäristöön, joka on Microsoftin oma Windowsin palvelinvirtualisointiympäristö. Samassa ympäristössä on asennettuna myös muut mahdollisesti tarvittavat palvelimet kuten esimerkiksi palvelimet tietokantoja, sähköposteja ja sovelluksia varten.

Etätyöpöytäyhteys on nykyisessä ratkaisussa hoidettu Microsoftin RDP-protokollalla sekä Microsoftin omalla etätyöpöytäohjelmistolla. Tämä ratkaisu on tarkoitus säilyttää nykyisellään eli myös jatkossa opiskelijat tulevat käyttämään samaa ratkaisua etätyöpöydälle kirjautuessaan.

Jotta tällä hetkellä VPN-yhteyttä hoitava palvelin saadaan hyödynnettyä muussa käytössä, tullaan se korvaamaan uudella VPN-ratkaisulla. Mahdollinen ratkaisu on rajattu ennalta kahteen eri vaihtoehtoon: Microsoft DirectAccess ja Palo Alto Networksin palomuurin mukana tulevaan VPN-ratkaisuun. Näiden ohjelmistojen ominaisuuksien vertailua on kuvattu tarkemmin seuraavassa kappaleessa 4.

VPN-yhteys olisi ollut teknisesti mahdollista toteuttaa myös fyysisiin työasemiin laboratoriotilassa, joihin olisi konfiguroitu tarvittavat yhteydet auki, mutta ongelmaksi tässä lähestymisessä muodostuu se, että koskaan emme voi olla varmoja onko jokin tietty fyysinen työasema päällä vai ei. Oppilaat saattaisivat sammuttaa työasemat laboratoriotilasta poistuessaan, jolloin yhteys niihin ei luonnollisesti onnistuisi. Näin ollen ympäristö täytyy rakentaa palvelimen päälle, jonka voi suurella varmuudella olettaa olevan päällä silloin kun opiskelijalla on tarve päästä käyttämään sitä.

4 UUDEN RATKAISUN VALINTA

Molemmat vertailtavat VPN-tuotteet, niin Microsoft DirectAccess kuin Palo Alto Networks GlobalProtect ovat nykyaikaisia ratkaisuja perinteisten VPN-ratkaisujen rinnalle ja tulevat varmasti yleistymään tulevaisuudessa. Molemmissa tuotteissa on omat vahvat puolensa ja ominaisuudet (kuvio 14).

Ominaisuudet	Microsoft DirectAccess	Palo Alto Networks GlobalProtect
Käytetyt protokollat ja tunnelointitekniikat	IPSec, 6to4, Teredo, IP-HTTPS	IPSec, SSL VPN
Asiakasohjelmiston käyttöjärjestelmät	Windows / Linux / OS X (* *) Linux ja OS X vaativat kolmannen osapuolen ohjelmiston	Windows / Linux (* / OS X *) esim. VPNC tai Shrew, vaatii IPSec ja X-auth
IPv6 tuki	Kyllä	Kyllä
Etäkäyttötyöpöytä (RDP)	Kyllä	Kyllä
Aktiivihakemistointegraatio	Kyllä	Kyllä
Erillinen asiakasohjelmisto	Ei	Kyllä
Public Key Infrastructure (PKI) tuki	Kyllä	Kyllä
Muuta	Automaattinen yhteys Yhteys kaksisuuntainen	Integroitu palomuureen Sisältötietoisuus HIP-ominaisuus Wildfire

KUVIO 14. Microsoft DirectAccess ja Palo Alto Networks GlobalProtect tuotteiden ominaisuuksien vertailu

Suurimmat erot ratkaisujen välillä ovat niiden käyttötarkoitukset. DirectAccess sopii hyvin esimerkiksi yrityksen mobiilikäyttäjille, jotka työskentelevät milloin mistäkin ja joilla on jatkuva tarve olla yhteydessä yrityksen sisäverkkoon. Yhteydenmuodostus on myös näkymätön itse käyttäjälle ja näin ollen myös vaivaton. DirectAccess mahdollistaa myös helpon keinon yrityksen mikrotukihenkilöille ottaa yhteyttä työntekijän koneelle mahdollista ongelmanratkaisua varten tai esimerkiksi ohjelmiston päivittämistä varten. Windows Server 2012 käyttöjärjestelmän mukana päivitetyt DirectAccess ominaisuudet tarjoavat jo erittäin varteenotettavan mahdollisuuden yrityksen resurssien etäkäyttöön.

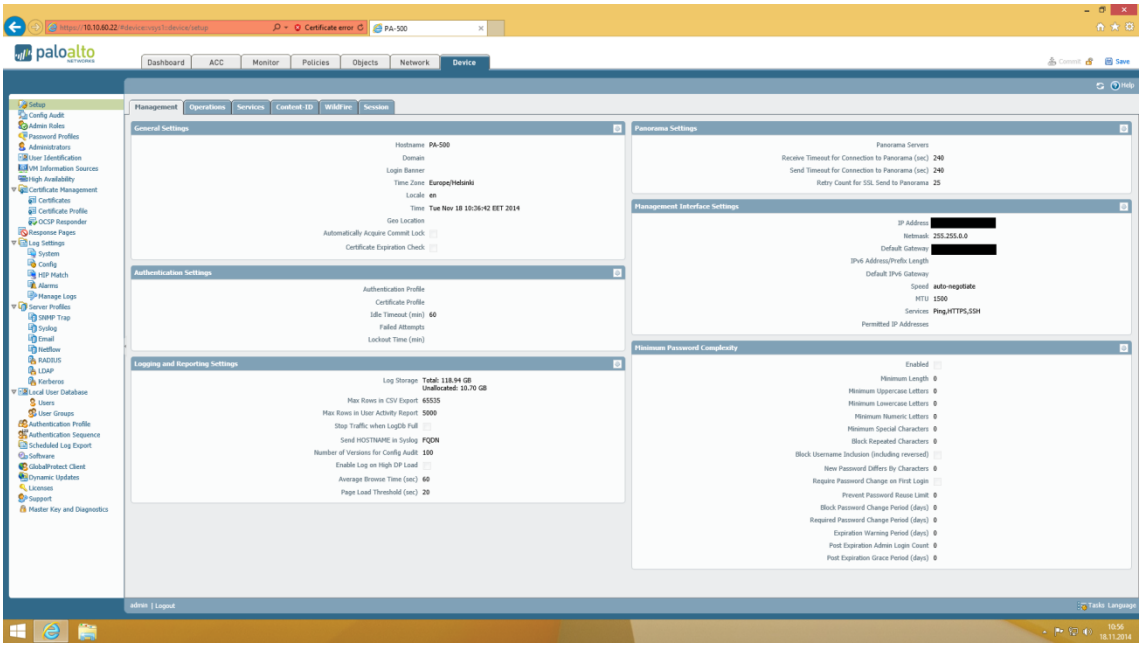
GlobalProtect eduksi on luonnollisesti laskettava, että VPN-ratkaisu tulee fyysisen palomuurin mukana. Palo Alto Networksin palomuurit ovat alansa edelläkävijöitä esimerkiksi sisältötietoisuutensa sekä HIP-ominaisuuksiensa vuoksi. Ne tarjoavat myös todella kattavat konfigurointimahdollisuudet sekä lokitiedostot. Palo Alto Networksin palomuurit soveltuvat niin pienemmän kuin suuremmankin yritysverkon suojaksi. Asiakaskoneille tosin tarvitaan erilliset asiakasohjelmistot, joko Palo Alto Networksin GlobalProtect tai sitten muu IPSec-protokollaa tukeva asiakasohjelmisto.

Toteutettavaksi ratkaisuksi päädyttiin valitsemaan fyysinen Palo Alto Networksin palomuurituote ja sen kautta tulevat VPN-ominaisuudet. Oppilaiden ei tarvitse olla jatkuvassa yhteydessä virtuaalisiin työasemiin ja näin ollen erikseen käynnistettävä VPN-yhteys palvelee käyttötarkoitusta paremmin. Tarvetta ei ollut myöskään kahdensuuntaiselle yhteydelle, jonka DirectAccess mahdollistaa. Palomuuri tarjoaa myös tulevaisuudessa mahdollisuuden rajoittaa yhteyksiä sisällön perusteella, jolloin voidaan määritellä minkälainen liikenne palomuurin läpäisee. Siinä tapauksessa, että yritys olisi hankkimassa VPN- etäkäyttöratkaisua omille työntekijöilleen, tulisi heidän arvioida kriittisesti myös muita mahdollisia valintakriteereitä kuten esimerkiksi hinta, skaalautuvuus, nopeus, tuki, saatavuus, luotettavuus, käytettävyys ja konfiguroitavuus.

Asennettavaksi malliksi päädyttiin valitsemaan Palo Alto Networksin PA-500, joka tarjoaa riittävän määrän ominaisuuksia ja suorituskykyä käyttötarkoitusta varten. Se tukee 64000 yhtäaikaista istuntoa, 250 IPSec VPN-tunnelia, 100 yhtäaikaista SSL VPN käyttäjää sekä tarjoaa 50Mbps nopeuden IPSec VPN käyttäjille. (Palo Alto Networks 2014a, viitattu 26.11.2014.)

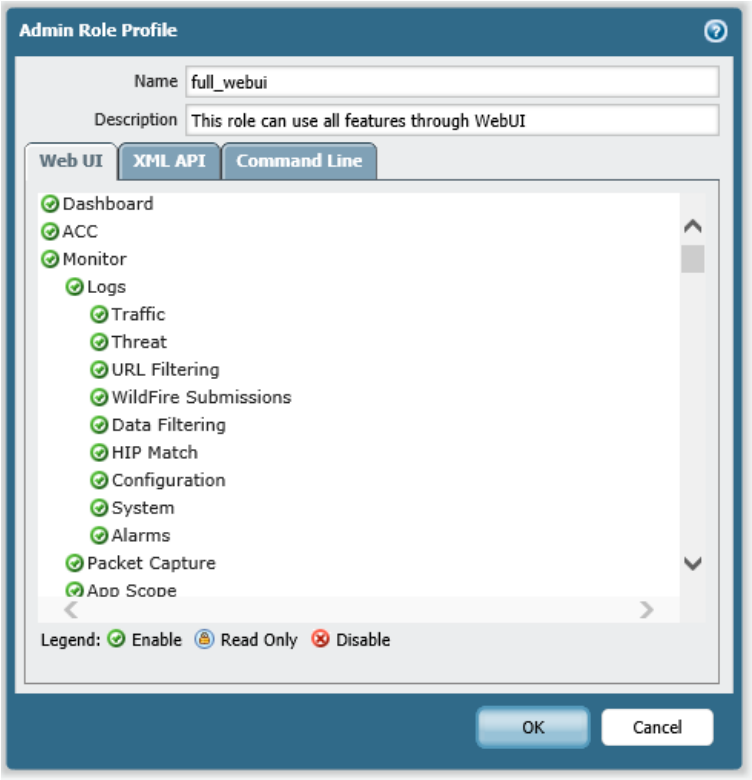
4.1 Käyttöönotto

Ensimmäiseksi laite täytyi rekisteröidä sekä aktivoida sen lisenssi. Tämän jälkeen palomuurille konfiguroitiin IP-osoite, oletusyhdyskäytävä sekä määriteltiin DNS-palvelin. Alustavat konfiguroinnit laitteelle suoritettiin kytkemällä tietokone laitteen Console-porttiin. Kun yhteys palomuurilta oli testattu ja todettu toimivaksi, päivitettiin seuraavaksi palomuurin ohjelmistot. Jatkossa laitteen konfigurointi voitiin suorittaa joko käyttäen graafista käyttöliittymää tai komentopohjaista käyttöliittymää (Command Line Interface, CLI). Graafista käyttöliittymää (kuvio 15) käyttäen voitiin määritykset tehdä verkkoselaimen avulla. DHCP-palvelinta palomuurille ei tarvinnut määritellä, koska IP-osoiteavaruus varataan VPN-yhteyden luonnin yhteydessä ja GlobalProtect tulee hoitamaan IP-osoitteiden allokoinnin asiakasohjelmistoille ja VPN-yhteyksille.



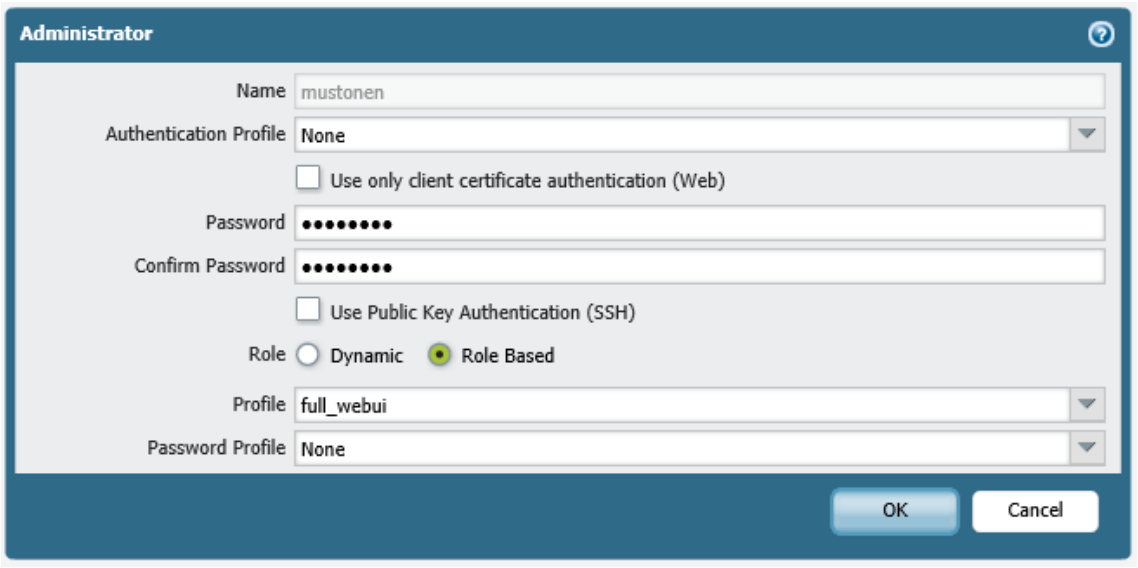
KUVIO 15. Palo Alto Networks palomuurin konfigurointi Device-välilehden alla

Jokaiselle ylläpitäjälle luotiin myös oma ylläpitotunnuksensa palomuurille tarvittavilla oikeuksilla. Näin palomuuri saatiin suojattua tarpeettomilta muutoksilta ja lokiin kirjautui jokaisen ylläpitäjän tekemät muutokset. Ylläpitäjiä varten luotiin ensin rooli tarvittavilla oikeuksilla (kuvio 16), kyseiset oikeudet voidaan määritellä erikseen Web UI, XML API ja Command Line käyttöliittymille. Roolin luominen tapahtui Device-välilehdeltä kohdasta Admin Roles, ruudun alareunassa on Add-painike, jonka kautta uusi rooli luotiin. Käyttöliittymän logiikka toimii samoin muissakin konfiguroinneissa.



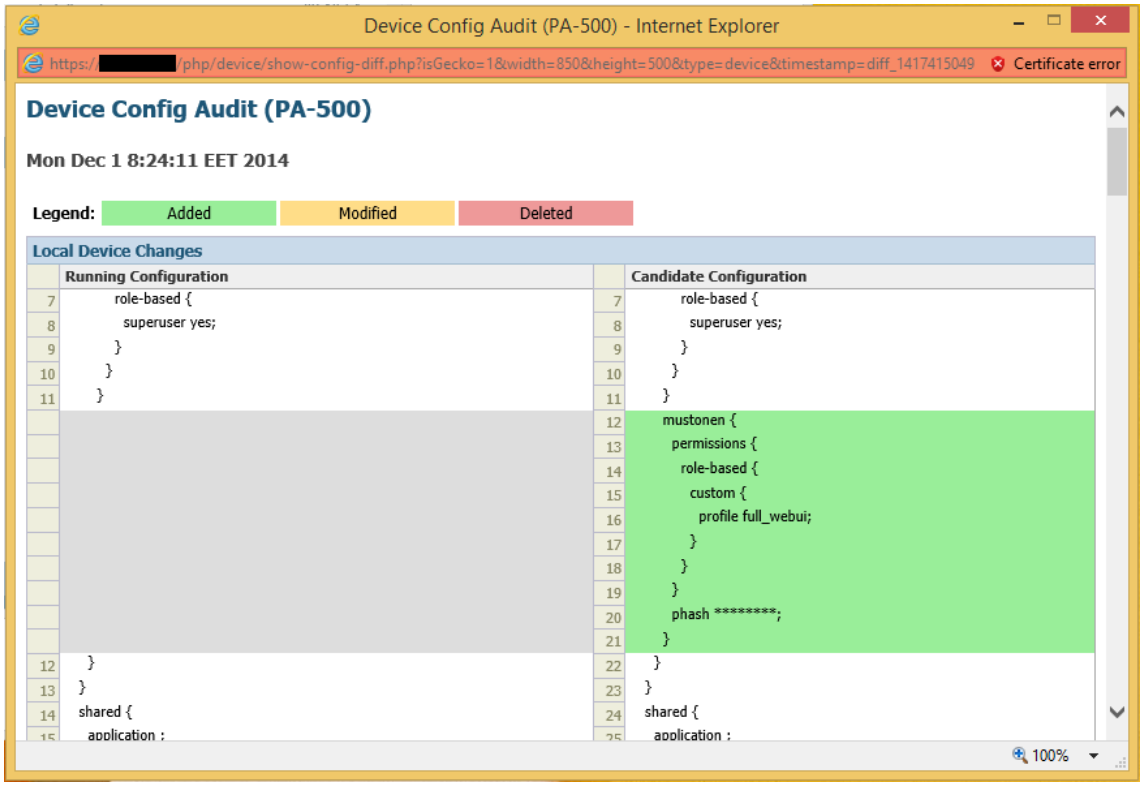
KUVIO 16. Roolin luominen ylläpitäjän oikeuksia varten

Tämän jälkeen määriteltiin uusi ylläpitäjä Device-välilehdeltä löytyvästä kohdasta Administrators. Ylläpitäjälle tulee määritellä nimi, salasana sekä roolipohjaiset oikeudet. Tämän jälkeen Profile-kenttään valittiin aiemmin luotu profiili (kuvio 17).



KUVIO 17. Uuden ylläpitäjän luominen ja profiilin määrittäminen

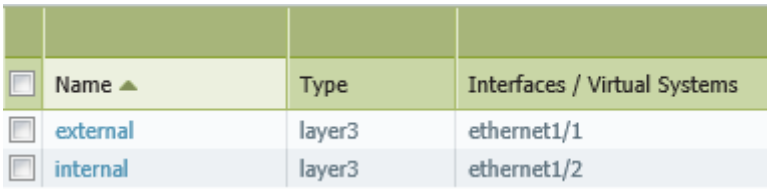
Huomioitavaa palomuurin konfiguroinnissa on, että palomuurille tehdyt muutokset tulevat käyttöön vasta kun C*ommit*–toiminto on suoritettu. Palomuuri on mahdollista myös lukita konfiguraatiomuutoksia varten, tästä ominaisuudesta on hyötyä esimerkiksi silloin kun ylläpitäjiä on useita ja on olemassa riski, että henkilöt tekevät muutoksia samanaikaisesti. Sekä Commit-painike että lukituspainike löytyvät ikkunan oikeasta yläreunasta. Commit-painikkeen painaminen avaa uuden ikkunan, jossa varoitetaan muutosten ylikirjoittavan nykyiset asetukset. Suoritettavia muutoksia voi tarkastella etukäteen valitsemalla Preview Changes. Tämä avaa ikkunan, jossa vertaillaan nykyisiä ja uusia asetuksia rinnakkain (kuvio 18).



KUVIO 18. Vanhan ja uuden konfiguraation vertaaminen rinnakkain

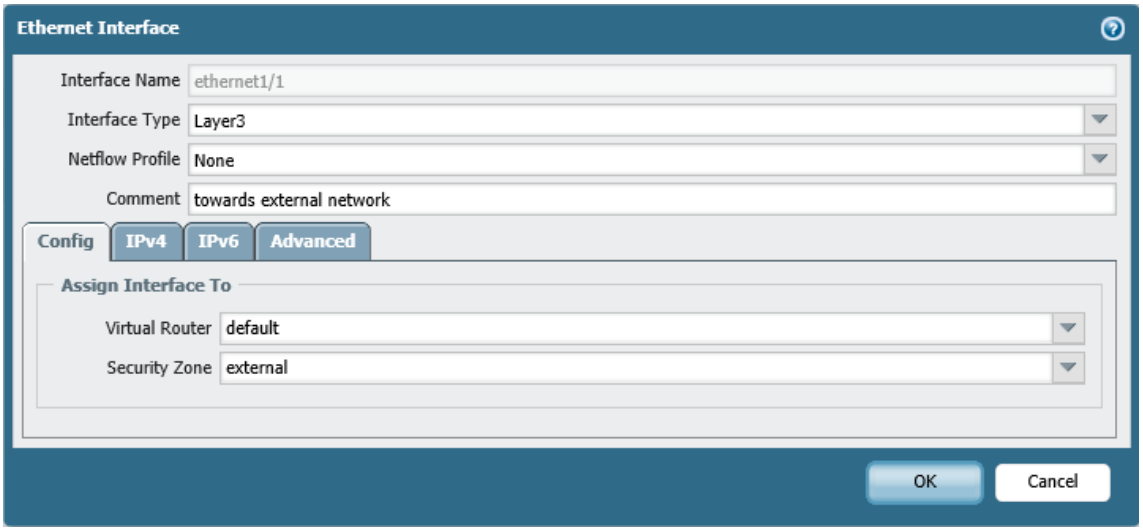
Vyöhykkeet, rajapinnat ja virtuaalinen reititin

Seuraavaksi palomuurille määriteltiin vyöhykkeet (zones) sekä rajapinnat (interfaces). Vyöhykkeillä tarkoitetaan kaikki palomuurin toiminnan kannalta oleellisia verkkoja. Tässä tapauksessa perustettiin omat vyöhykkeet ulkoiselle liikenteelle (external) sekä sisäverkolle (internal). Vyöhykkeiden määritys tapahtuu Network-välilehden alta kohdasta Zones. Vyöhykkeet määriteltiin palomuurin fyysisiin portteihin, tässä tapauksessa 1 ja 2 (kuvio 19).



KUVIO 19. Vyöhykkeiden määrittely palomuurin fyysisiin portteihin

Tämän jälkeen palomuurille määriteltiin rajapinnat Network-välilehdeltä löytyvällä Interfaces-valinnalla (kuvio 20). Tässä tapauksessa ulospäin lähtevä verkkokaapeli oli kytketty palomuurilla ethernet1/1 porttiin. Palomuuri asennettiin toimivaksi OSI-mallin kolmannella tasolla (Layer3) eli verkkokerroksella koska se tulee reitittämään liikennettä verkkojen välillä. Rajapinnalle piti määritellä myös virtuaalinen reititin kohtaan Virtual Router ja siihen valittiin oletusarvo default. IPv4-välilehden alla määriteltiin vielä ulospäin lähtevän liikenteen IP-osoitte sekä verkon peitto (mask).



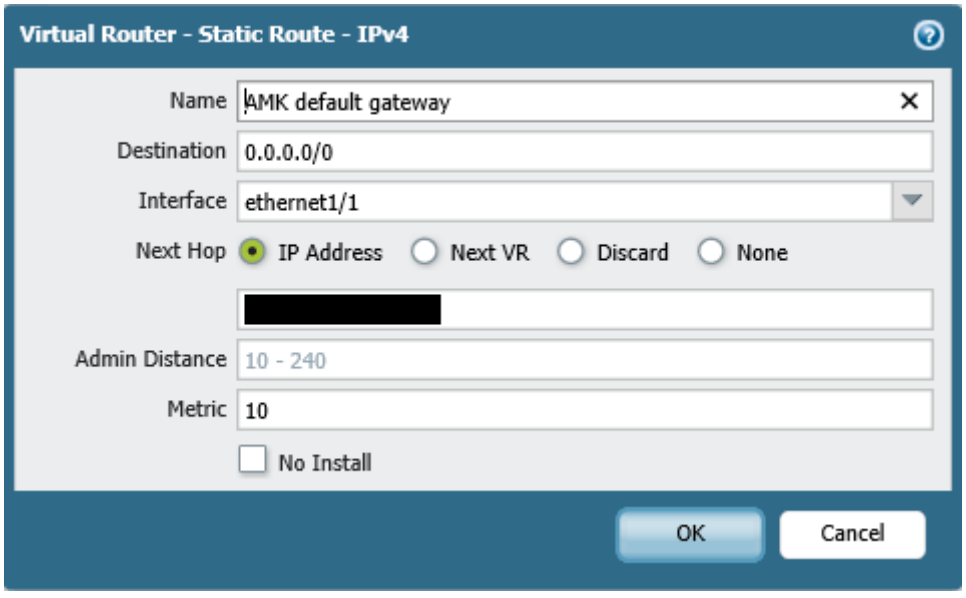
KUVIO 20. Rajapinnan määrittely palomuurilla

Tämän jälkeen edellä mainitut toimenpiteet piti toistaa sisäverkon rajapinnalle, jonka jälkeen määritellyt rajapinnat näkyivät Network-välilehden alla Interfaces-kohdassa (kuvio 21). Rajapinnat näkyivät vihreinä, koska niihin oli kytketty fyysinen kaapeli kun taas muut rajapinnat olivat edelleen harmaina.

Interface	Interface Type	Link State	IP Address	Virtual Router	VLAN / Virtual-Wire	Security Zone	Comment
ethernet1/1	Layer3		[redacted]	default	none	external	towards external network
ethernet1/2	Layer3		[redacted]	default	none	internal	Towards internal network
ethernet1/3			none	none	none	none	
ethernet1/4			none	none	none	none	
ethernet1/5			none	none	none	none	
ethernet1/6			none	none	none	none	
ethernet1/7			none	none	none	none	
ethernet1/8			none	none	none	none	

KUVIO 21. Listaus palomuurin rajapinnoista sekä niiden tilat

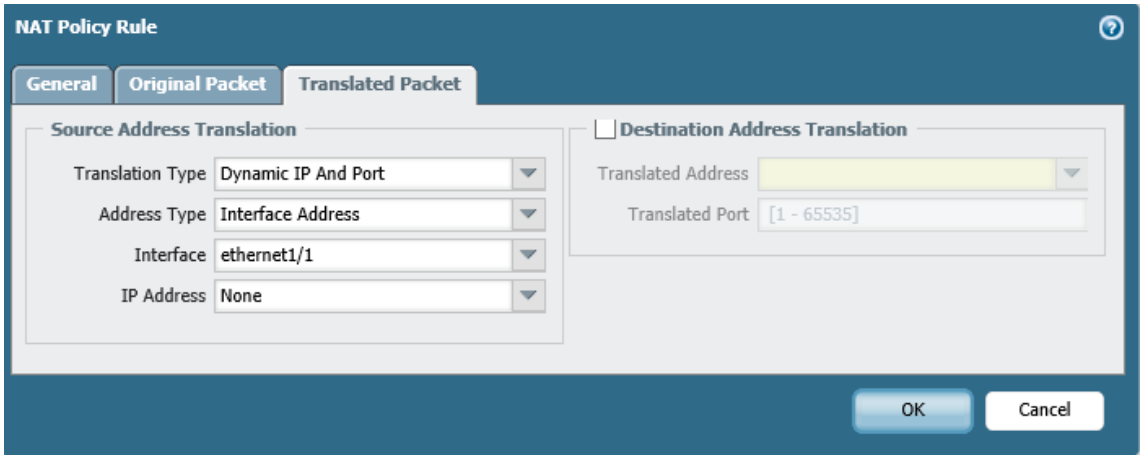
Tämän jälkeen virtuaaliselle reitittimelle täytyi määritellä seuraavan reitittimen osoitteen eli mihin ulos lähtevä liikenne seuraavaksi ohjataan. Tämä tapahtuu Network -välilehdeltä kohdasta Virtual Routers ja valitsemalla virtuaalinen reititin nimeltä default. Static Routes –välilehden alta luotiin uusi staattinen reitti palomuurilta ulos. Reitille piti määritellä nimi, kohde, rajapinta sekä antaa seuraavan hypyn IP-osoite (kuvio 22). Valitsemalla kohteeksi 0.0.0.0/0 reitittyy kaikki ulos lähtevä liikenne määritellyn reitin kautta.



KUVIO 22. Staattisen reitin määritteleminen virtuaaliselle reitittimelle

Osoitteenmuunnos (Network Address Translation, NAT)

Tämän jälkeen palomuurilla tuli tehdä osoitteenmuunnos, jotta sisäverkossa olevat laitteet pääsevät ulos julkiseen verkkoon. Osoitteenmuunnos löytyy Policies-välilehdeltä kohdasta NAT. Ensimmäiseksi General-välilehdellä osoitteenmuunnokselle annettiin nimi ja valittiin tyypiksi IPv4. Tämän jälkeen Original Packet –välilehdellä valittiin lähdeveyöhykkeeksi sisäinen verkko (internal) ja kohdevyöhykkeeksi ulkoinen verkko (external). Translated Packet –välilehdellä kännöksen tyypiksi asetettiin Dynamic IP And Port, osoitteen tyypiksi Interface Address ja vyöhykkeeksi ethernet1/1, joka siis on ulospäin lähtevä rajapinta (kuvio 23).



KUVIO 23. NAT-politiikan luonti sisäverkon laitteille

Turvallisuuspolitiikat ja testaus

Seuraavaksi täytyi määritellä turvallisuuspolitiikat tietoliikenteelle eri vyöhykkeiden välillä. Turvallisuuspolitiikat voidaan määritellä Policies –välilehden alta kohdasta Security. Ensimmäiseksi sallittiin kaikki liikenne sisäverkosta ulkoverkkoon eli luotiin sääntö, jossa lähde on sisäinen vyöhyke ja kohteena on ulkoinen vyöhyke. Liikennettä ei rajoitettu tietyille käyttäjille tai sovelluksille vaan kaikki liikenne sai päästä ulkoverkkoon.

Toiseksi turvallisuuspolitiikaksi luotiin sääntö, jossa määriteltiin mikä liikenne pääsee ulkoverkosta eli julkisesta internetistä sisäverkon puolelle. Tässä tapauksessa määriteltiin lähteeksi ulkoinen vyöhyke ja kohteeksi sisäinen vyöhyke. Turvallisuussyistä johtuen sallituiksi sovelluksiksi määriteltiin ainoastaan DNS-kyselyt (dns) sekä RDP-protokolla (ms-rdp) (kuvio 24). Tässä yhteydessä

ei tarvitse määritellä erikseen VPN-liikennettä, koska se ei itseasiassa läpäise palomuuria vaan se terminoidaan palomuurille.

		Source				Destination				
	Name	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	int_to_ext	internal	any	any	any	external	any	any	application-d...	✓
2	ext_to_int	external	any	any	any	internal	any	dns ms-rdp	application-d...	✓

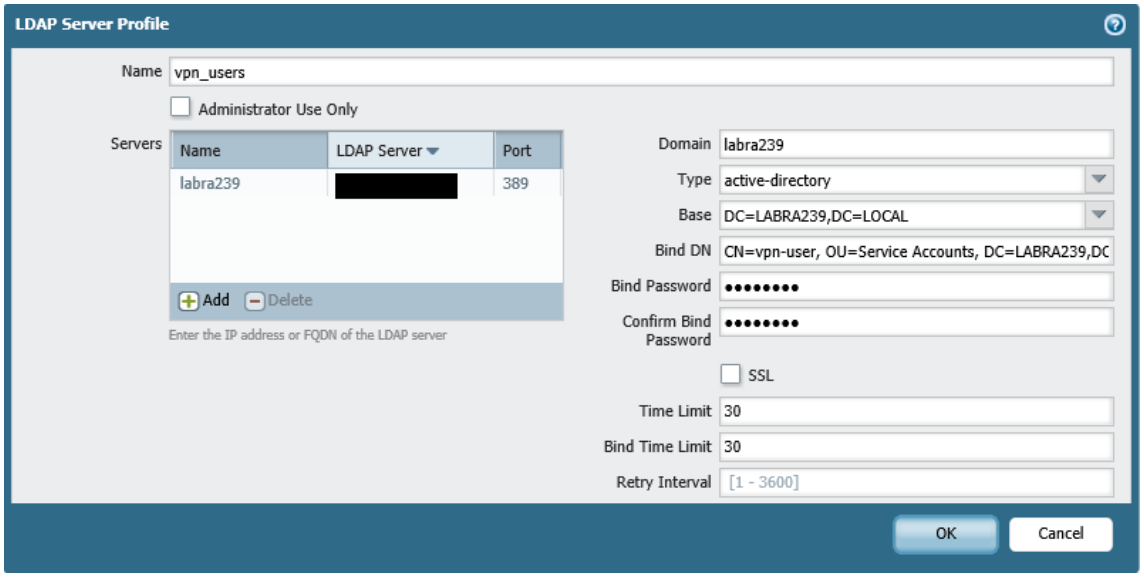
KUVIO 24. Turvallisuuspolitiikat sisäverkosta ulkoverkkoon ja päin vastoin

Tässä vaiheessa palomuurin konfigurointia suoritettiin ensimmäiset testaukset sisäverkosta määrittelemällä sisäverkossa olevalle työasemalle oletusyhdyskäytäväksi (default gateway) palomuurin sisäverkon rajapinnan. Tietoliikenne kulki palomuurin läpi julkiseen internettiin, joka näkyi sivujen aukeamisena. Kyseinen tietoliikenne myös tallentui palomuurille Monitor –välilehden alle. Huomioitavaa on, että Palo Alto Networksin palomuurilla ei tarvitse erikseen sallia aktiivisen yhteyden paluupaketteja kuten esimerkiksi Ciscon palomuurilla. Tästä syystä sivut aukenivat, vaikka http tai https ei ollut sallittuna sovelluksena ulkoisesta verkosta sisäänpäin.

Käyttäjät ja käyttöoikeudet

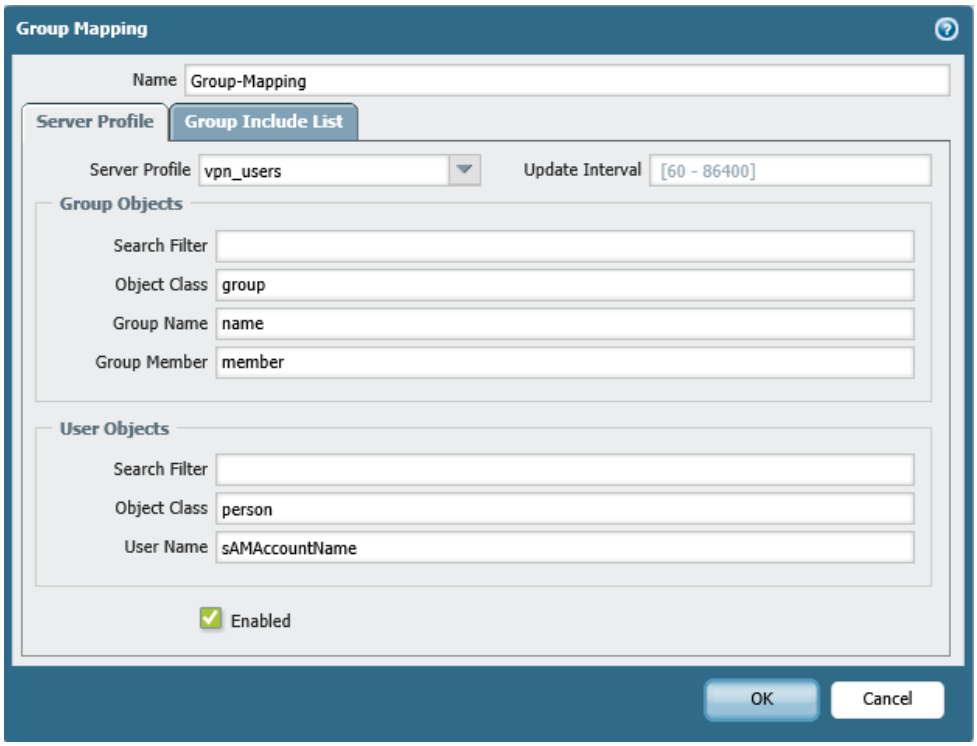
VPN-käyttäjien tunnistuksessa käytettiin erillistä samassa verkossa sijaitsevaa aktiivihakemistopalvelinta, johon luotiin LDAP-integraatio palomuurilta. Kyseiseen aktiivihakemistoon oli kuitenkin ensin luotava ryhmä ja lisättävä ratkaisua käyttävät tunnukset ryhmän sisään. Alussa luotiin palomuurille myös paikallinen (local) käyttäjä, jonka avulla myöhemmin pystyttiin helposti testaamaan sekä VPN-yhteys että varmistamaan LDAP-integraation toimivuus. Uusi käyttäjä luodaan Device-välilehdeltä kohdasta Local User Database / Users.

LDAP-integraatio puolestaan luotiin kohdasta Server Profiles / LDAP. Yhteyttä varten tarvitsi määritellä toimialue johon kytkeydytään, LDAP-palvelimen IP-osoite sekä käyttäjätunnus (kuvio 25). Määritellyllä käyttäjätunnuksella täytyy olla riittävät oikeudet hakea LDAP-hakemistosta tietoa. Portiksi LDAP-yhteydelle määriteltiin 389, jos käytettäisiin SSL-yhteyttä niin portiksi pitäisi määritellä 636.



KUVIO 25. LDAP-integraation luominen palomuurilta

Tämän jälkeen konfiguroitiin automaattinen ryhmien päivitys LDAP-integraation kautta ja tämä tapahtuu Device-välilehdeltä kohdasta User Identification / Group Mapping Settings (kuvio 26). Ensimmäiseksi täytyi antaa tälle automaattiselle päivitykselle nimi sekä valita aiemmin luotu LDAP-integraation profiili kohtaan Server Profile. Automaattinen päivitys voidaan määritellä tapahtuvaksi joko kerran minuutissa, kerran vuorokaudessa tai jotain tältä väliltä, oletusarvoisesti päivitys tapahtuu kerran tunnissa (arvo 3600). Group Include List-välilehden kautta voidaan määritellä ne ryhmät, jotka päivitetään LDAP-integraation kautta automaattisesti. Näin voidaan nopeuttaa päivitystä ja verkon kuormitusta, varsinkin laajemmissa järjestelmissä päivitettäviä ryhmiä voi olla syytä rajata.



KUVIO 26. Ryhmien automaattinen päivitys LDAP-integraation kautta

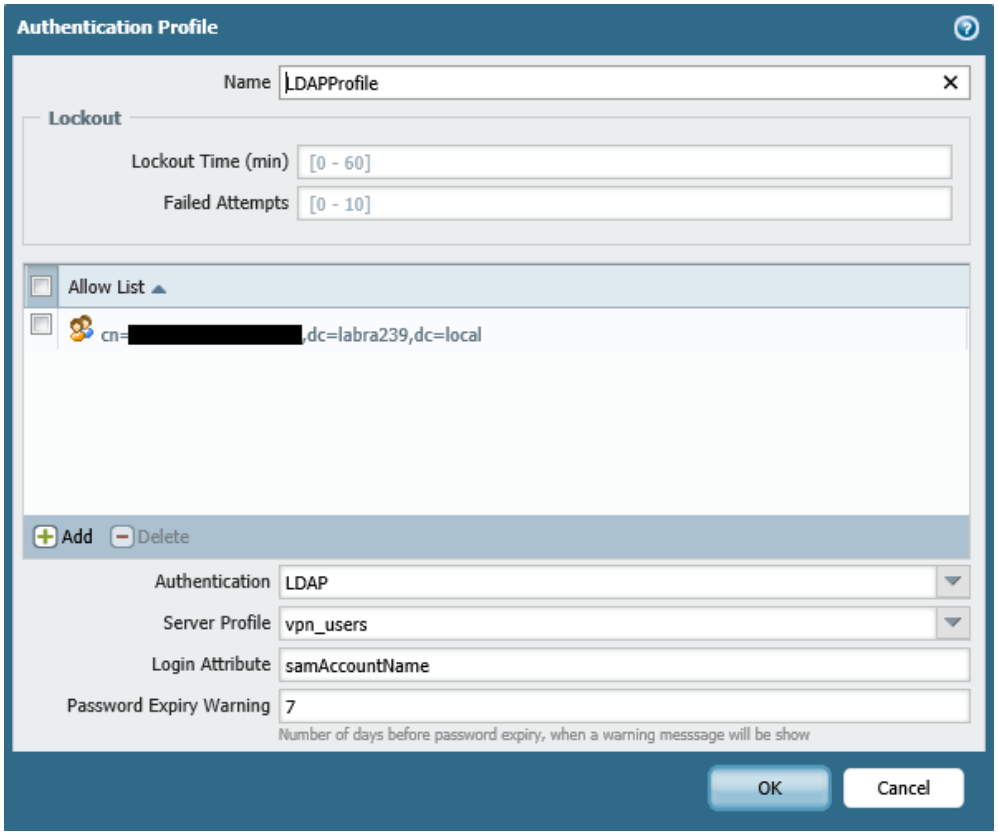
LDAP-integraation toimivuus voidaan helposti testata käyttäen komentopohjaista käyttöliittymää (Command Line Interface, CLI). Alla lista komennoista, jotka listaavat ryhmät, niihin kuuluvat käyttäjät sekä tiedot automaattisesti päivittyvistä ryhmistä (kuvio 27).

Komento	Käyttötarkoitus
show user group list	Listaa kaikki käytettävissä olevat ryhmät
show user group name ryhmän_nimi (* *) käytä koko nimeä samassa muodossa kuin yllä oleva komento listasi	Listaa kyseisen ryhmän sisällä olevat käyttäjät
show user group-mapping statistics	Listaa kaikki automaattisesti päivittyvät ryhmät, milloin edellinen päivitys tapahtui ja milloin seuraava päivitys tulee tapahtumaan

KUVIO 27. Käyttäjien, ryhmien ja automaattisesti päivittyvien ryhmien tarkistus käyttäen CLI-käyttöliittymää

Tämän lisäksi VPN-yhteyttä varten tarvittiin profiili todennusta varten ja se luotiin Device-välilehdeltä kohdasta Authentication Profile. Profiilit täytyi luoda erikseen LDAP-integraatiota sekä paikallisia käyttäjätunnuksia varten. Profiiliin lisättiin ne käyttäjät ja ryhmät, jotka tulevat käyttämään VPN-ratkaisua. Autentikointi tapahtuu LDAP-hakemistosta, palvelinprofiiliksi valittiin aiem-

min luotu vpn_users ja oleellista oli lisätä Login Attribute –kenttään arvo samAccountName (kuvio 28).



KUVIO 28. Profiilin luominen VPN-yhteyksien todennusta varten

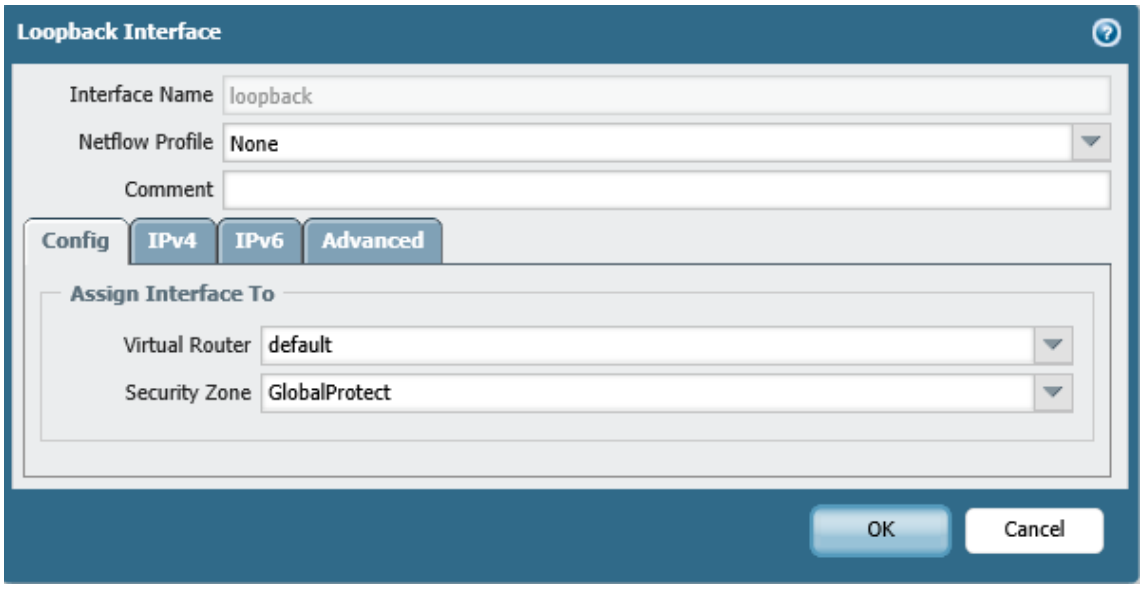
VPN-yhteyden määritteleminen

Palo Alto Networks tuotteilla on mahdollista toteuttaa niin site-to-site VPN kuin remote access VPN. Koska tarve oli mahdollistaa oppilaiden kirjautuminen omilla tunnuksillaan virtuaalikoneisiin julkisen internetin ylitse, toteutimme remote access VPN-ratkaisun. Ratkaisu tukee sekä IPSec- tai SSL-pohjaista VPN-yhteyttä. Oppilas voi käyttää joko palomuurilta ladattavaa GlobalProtect asiakasohjelmistoa tai kolmannen osapuolen ohjelmistoa, joka tukee IPSec-yhteyttä.

Ensimmäiseksi luotiin sertifikaatti GlobalProtect portaalia ja yhdyskäytävää varten, joka tapahtui Devices-välilehdeltä kohdasta Certificate Management / Certificates. Uusi sertifikaatti luodaan Generate-painikkeella ruudun alareunasta. Sertifikaatin nimen voi vapaasti valita, sen sijaan Common Name –kenttään tuli syöttää se IP-osoite, johon käyttäjät ottavat yhteyttä.

GlobalProtect asiakasohjelmisto piti myös ladata palomuurille, josta loppukäyttäjä voi VPN-yhteyttä luodessaan sen ladata ja asentaa omalle koneelleen. Asiakasohjelmiston voi ladata Device-välilehdeltä kohdasta GlobalProtect Client ja valitsemalla uusimman version kohdalta Download. Huomioitavaa tässä on se, että ensiksi kannattaa painaa alareunasta löytyvää Check Now –painiketta, joka tarkistaa löytyykö ohjelmistosta uudempaa versiota. Jos asiakasohjelmistosta on olemassa uudempi versio, vanhempi versio ei lataudu, vaikka se onkin listattuna. Latauksen jälkeen piti ladattu asiakasohjelmisto myös aktivoida painikkeesta Activate.

Seuraavaksi määriteltiin palomuurille uusi vyöhyke VPN-yhteyttä varten ja tämä nimettiin nimelle GlobalProtect. Tähän vyöhykkeeseen luotiin uusi loopback-liitäntä, jolle myös määriteltiin aiemmin määritelty virtuaalinen reititin (kuvio 29). Tämän lisäksi IPv4-välilehden alta kyseiselle rajapinnalle määriteltiin myös oma IP-osoite /32 verkkomaskilla.



KUVIO 29. Loopback-liitännän luominen

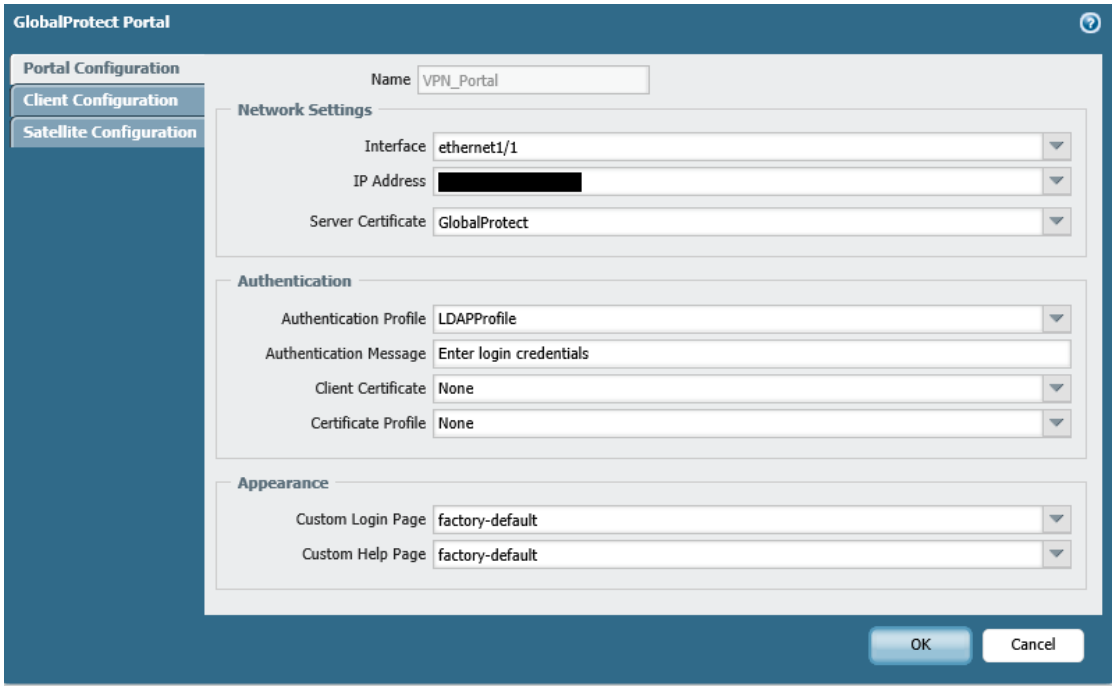
Lopoback-liitännän lisäksi luotiin Network-välilehdeltä kohdasta Interfaces / Tunnel uusi tunneli, jolle annettiin nimeksi tunnel.1. Myös tämä liitettiin vyöhykkeeseen GlobalProtect ja määriteltiin käyttämään samaa default-nimistä virtuaalista reititintä. Edellä mainittujen muutoksien jälkeen palomuurilla siis oli kolme vyöhykettä ja niihin liitettynä neljä rajapintaa (kuvio 30).

Name	Type	Interfaces / Virtual Systems
external	layer3	ethernet1/1
GlobalProtect	layer3	tunnel.1
		loopback
internal	layer3	ethernet1/2

KUVIO 30. Vyöhykkeet ja niihin määritellyt rajapinnat

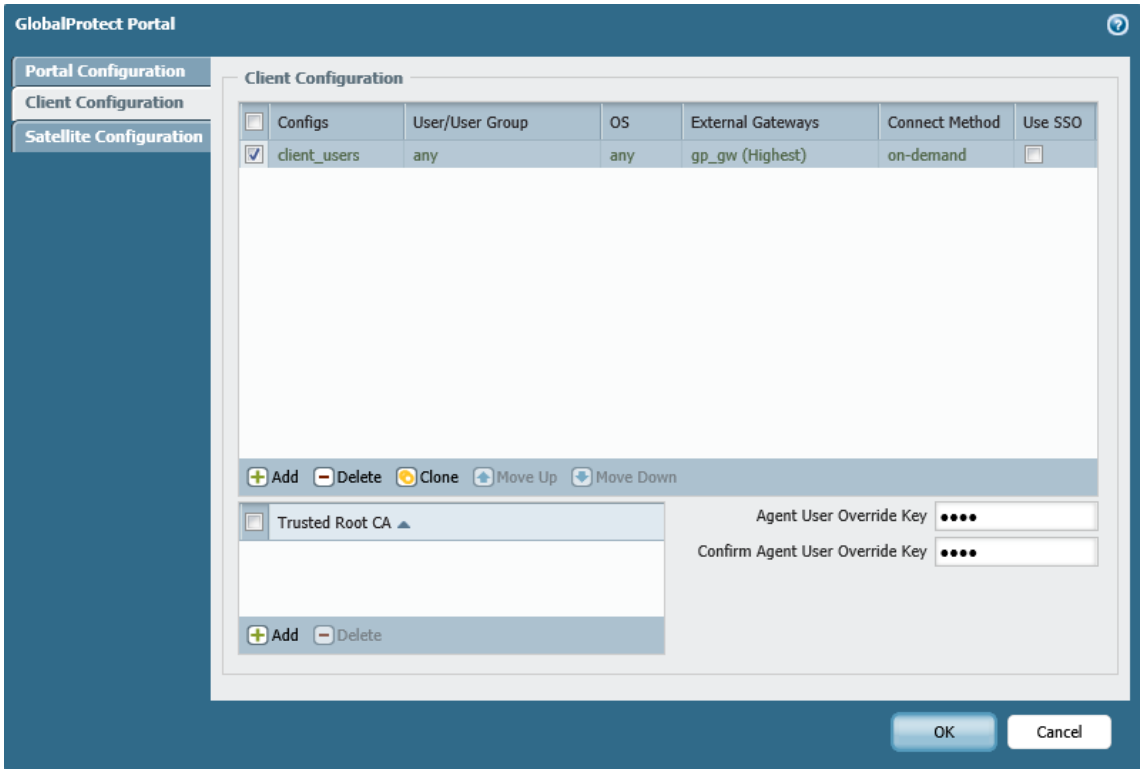
GlobalProtect koostuu kolmesta osasta: portaalista (portal), yhdyskäytävästä (gateway) sekä asiakasohjelmistosta (agent / client). Portaali ylläpitää listaa esimerkiksi yhdyskäytävistä sekä tunnistamiseen käytetyistä sertifikaateista. Yhdyskäytävä puolestaan huolehtii turvallisesta tiedonsiirrosta asiakasohjelmiston ja palomuurin välillä. Asiakasohjelmisto puolestaan on käyttäjän koneelle asennettava ohjelmisto, joka konfiguroidaan ottamaan VPN-yhteys palomuurille.

Ensimmäiseksi konfiguroitiin GlobalProtect portaali valitsemalla GlobalProtect / Portals Network-välilehdeltä. Portaalille määriteltiin rajapinta (interface), palvelimen sertifikaatti (server certificate) sekä käyttäjätunnukseen perustuva tunnistautuminen valitsemalla aiemmin luotu LDAPProfile Authentication Profile –kenttään (kuvio 31). Toinen vaihtoehto olisi käyttää sertifikaatteihin perustuvaa tunnistautumista.



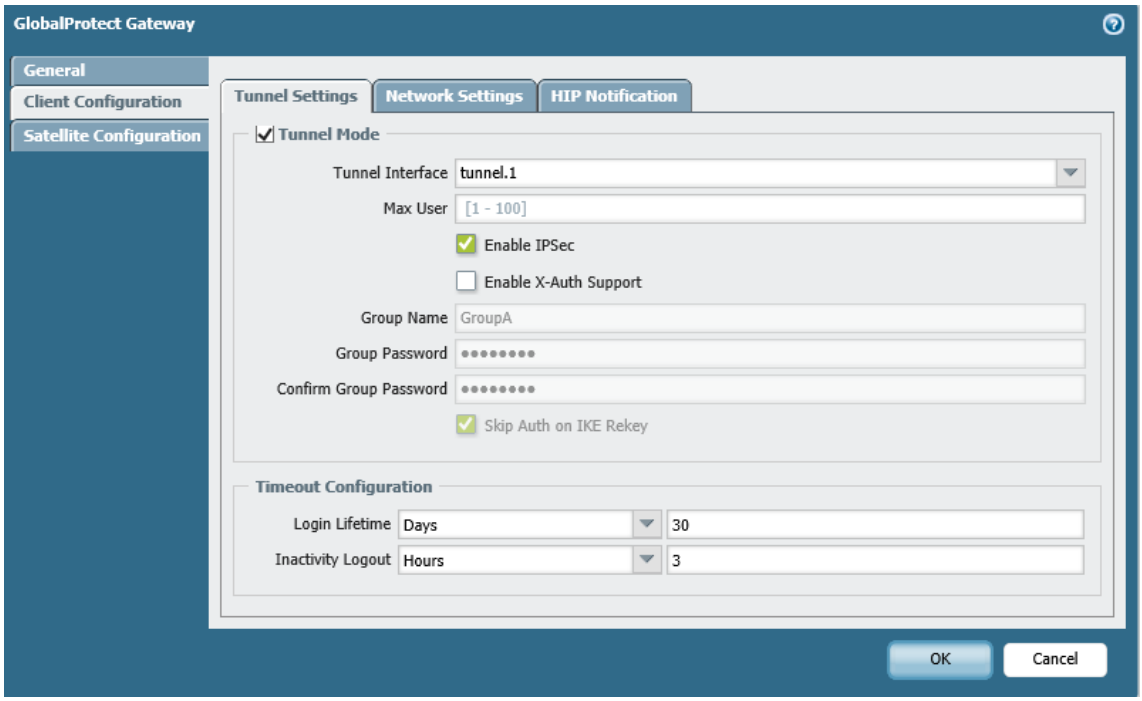
KUVIO 31. GlobalProtect portaalin määritteleminen

Asiakasohjelmiston asetukset määriteltiin Client Configuration –välilehdeltä ja sitä varten luotiin uusi profiili Add-painikkeella (kuvio 32). Tunnistautumismenetelmäksi valittiin 'tarvittaessa' (on-demand) ja yhdyskäytäväksi (External Gateways) määriteltiin julkinen IP-osoite, johon asiakasohjelmisto ottaa yhteyden.



KUVIO 32. GlobalProtect asiakasohjelmiston asetusten määrittely

GlobalProtect yhdyskäytävä määriteltiin Network-välilehdeltä löytyvästä kohdasta GlobalProtect / Gateways. General-välilehdelle tehtiin samat määritykset kuin edellä portaalille eli rajapinnaksi ethernet1/1 ja siihen liitetty IP-osoite. Sertifikaatiksi valittiin sama aiemmin luotu sertifikaatti nimeltä GlobalProtect. Käyttäjien tunnistamiseksi määriteltiin profiiliksi LDAPProfile. Tämän jälkeen valittiin Client Configuration –välilehti ja valittiin tunnelitila (tunnel mode) ja tunnelin rajapinnaksi (tunnel interface) määriteltiin aiemmin luotu tunnel.1. Muutoin asetuksien annettiin olla oletusarvoisesti (kuvio 33).



KUVIO 33. GlobalProtect yhdyskäytävän asetusten määrittely

Network Settings –välilehdellä vielä määriteltiin DNS-palvelin (primary DNS), IP-osoiteavaruus asiakasohjelmistoja varten (IP pool) sekä liikenne, joka reitittyy (access route) luotavan VPN-tunnelin ylitse.

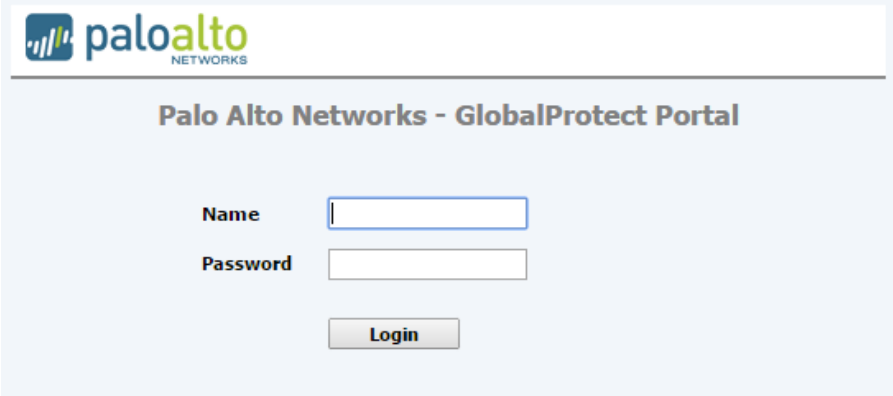
Viimeiseksi määriteltiin turvallisuuspolitiikat myös aiemmin luodulle GlobalProtect vyöhykkeelle Policies –välilehdeltä kohdasta Security. Ainoastaan DNS ja RDP lisättiin sallituiksi sovelluksiksi kun liikennöidään ulkoverkosta GlobalProtect vyöhykkeelle ja sieltä edelleen sisäverkkoon (kuvio 34).

		Source				Destination				
	Name	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	int2ext	internal	any	any	any	external	any	any	application-d...	✓
2	ext2int	external	any	any	any	internal	any	dns ms-rdp	application-d...	✓
3	gp2int	GlobalProtect	any	any	any	internal	any	dns ms-rdp	application-d...	✓
4	ext2gp	external	any	any	any	GlobalP...	any	dns ms-rdp	application-d...	✓

KUVIO 34. Päivitetyt turvallisuuspolitiikat uudelle GlobalProtect vyöhykkeelle

4.2 Testaus

Tämän jälkeen yhteys testattiin julkisen internetin ylitse. Ensimmäiseksi mentiin verkkoselaimella palomuurin julkiseen IP-osoitteeseen, joka kysyi käyttäjätunnuksen sekä salasanan (kuvio 35).

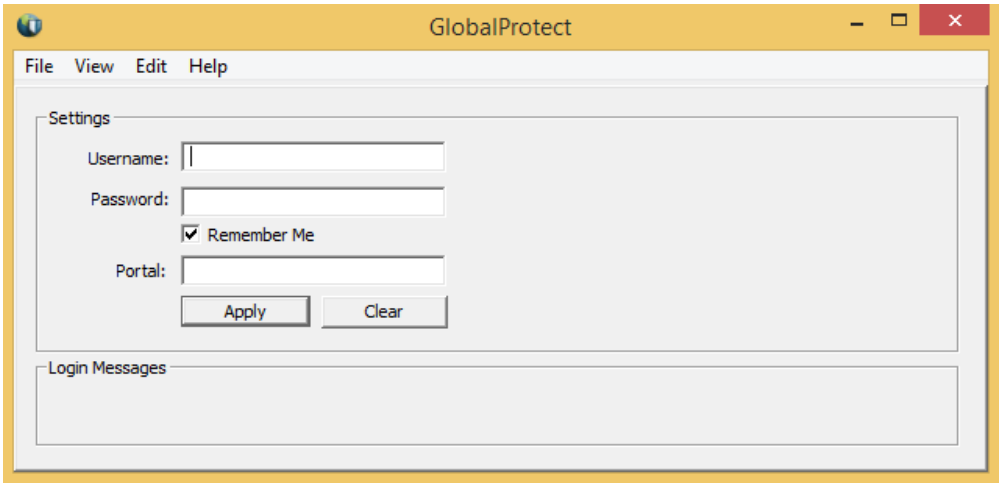


KUVIO 35. GlobalProtect portaalin tunnistautuminen

Verkkosivulle kirjauduttiin käyttämällä aktiivihakemistosta löytyvää käyttäjätunnusta ja salasanaa. Tämän jälkeen avautui ikkuna, josta voitiin ladata GlobalProtect asiakasohjelmisto. Valittavissa oli joko 32- tai 64-bittinen Windows- tai Mac-versio (kuvio 36).

KUVIO 36. GlobalProtect asiakasohjelmiston lataaminen

Kun asiakasohjelmisto oli ladattu koneelle ja asennus suoritettu, käynnistyi GlobalProtect asiakasohjelmisto tietokoneen ruudulle (kuvio 37). Käyttäjätunnukset, salasanan ja IP-osoitteen syöttämisen jälkeen painettiin Apply-painiketta, jonka jälkeen asiakasohjelmisto ilmoitti VPN-yhteyden olevan luotu (connected).



KUVIO 37. GlobalProtect asiakasohjelmiston käyttöliittymä

Tämän jälkeen avattiin Windowsin oma RDP-protokollaa tukeva ohjelmisto Etätyöpöytäyhteys (Remote Desktop Connection). Etätyöpöytäyhteydelle määriteltiin sisäverkon IP-osoite ja painettiin yhdistä-painiketta, jonka jälkeen ohjelma kysyi vielä käyttäjän tunnusta ja salasanaa toimialueelle. Yhteyden voitiin todeta toimivan ja sama voitiin todeta palomuurilta Monitor-välilehden alta liikennettä tarkasteltaessa (kuvio 38).

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	By...
12/09 07:40:04	end	internal	external	[redacted]		[redacted]	80	ms-update	allow	int2ext	13.8 K
12/09 07:40:03	end	internal	external				80	web-browsing	allow	int2ext	1.2 K
12/09 07:40:03	end	internal	external				80	web-browsing	allow	int2ext	2.8 K
12/09 07:40:03	end	internal	external				80	web-browsing	allow	int2ext	4.1 K
12/09 07:40:01	end	internal	external				80	ms-update	allow	int2ext	7.3 K
12/09 04:14:03	end	GlobalPr...	internal		labra239 \mustonen		3389	ms-rdp	allow	gp2int	1.2 M
12/09 04:13:59	end	GlobalPr...	internal		labra239 \mustonen		3389	ms-rdp	allow	gp2int	14.3 K
12/09 02:56:47	end	GlobalPr...	internal		labra239 \mustonen		3389	ms-rdp	allow	gp2int	2.2 M
12/09 02:56:47	end	GlobalPr...	internal		labra239 \mustonen		3389	ms-rdp	allow	gp2int	16.6 K
12/08 18:14:40	end	GlobalPr...	internal		labra239 \mustonen		3389	ms-rdp	allow	gp2int	535.8 K
12/08 18:13:23	end	GlobalPr...	internal		labra239 \mustonen		53	dns	allow	gp2int	192
12/08 18:12:32	end	GlobalPr...	internal		labra239 \mustonen		53	dns	allow	gp2int	208

KUVIO 38. Tallentunut liikenne Palo Alto Networksin palomuurilla

Palomuurilla näkyy DNS-kyselyitä, etätyöpöydän RDP-protokollan mukaista liikennettä sekä myös sisäverkon puolelta ulospäin olevaa verkkoliikennettä.

5 TULOKSET JA JOHTOPÄÄTÖKSET

Oulun Ammattikorkeakoululle saatiin onnistuneesti otettua käyttöön uusi etäopetuksen mahdollistava ratkaisu käyttäen Palo Alto Networksin VPN-ominaisuudet sisältävää fyysistä palomuurituotetta. Ratkaisu mahdollistaa VPN-tunnelin luomisen julkisen internetin ylitse ja etätyöpöytäyhteyden luodun VPN-tunnelin ylitse oppilaiden omilta työasemilta. VPN-yhteys terminoidaan asennetulle palomuurille ja sen kautta päästään Oulun Ammattikorkeakoulun intranetissä sijaitsevaan virtuaaliympäristöön ja sinne asennettuihin työasemiin.

Opinnäytetyön tietoperustassa on laajasti käsitelty tietoverkkoihin ja VPN-ratkaisuihin olennaisesti kuuluvia asioita. Tietoperusta koostui juuri niistä asioista, joita käytännön toteutuksessa vaadittiin ja hankittu tietoperusta oli hyvin ajantasaista. Tietoperustaa jouduttiin täydentämään käytännön toteutuksen aikana ainoastaan hyvin pieniltä osin. Tietoperustan laajuus ja ajantasaisuus mahdollistivat palomuurin käyttöönoton ilman aiempaa kokemusta verkkolaitteiden käytännön asennuksista. Palomuurin konfiguroiminen onnistui graafisella käyttöliittymällä, joka helpotti omalta osaltaan käyttöönottovaihetta. Palo Alto Networksin palomuurin konfigurointi eroaakin monelta osin esimerkiksi Ciscon vastaavien palomuurien konfiguroinnista.

Graafisen käyttöliittymän lisäksi Palo Alto Networks palomuurit pitävät sisällään joukon nykyaikaisia ja mielenkiintoisia ominaisuuksia. Liikennettä voidaan rajoittaa perinteisten IP-osoitteiden, porttien ja protokollien lisäksi esimerkiksi sovelluksien ja käyttäjien perusteella. HIP-ominaisuus (Host Information Profile) antaa mahdollisuuden rajoittaa pääsyä yrityksen tietoverkkoon esimerkiksi asiakaskoneen vanhentuneen virustorjunnan vuoksi. Palomuurit tarjoavat lähes rajattomat mahdollisuudet liikenteen monitorointiin ja raportointiin. Wildfire-ominaisuus mahdollistaa tietoisuuden levittämisen uusista uhkatekijöistä maailmanlaajuisesti viidessätoista minuutissa.

Tulevaisuudessa edellä mainittuja ominaisuuksia voitaisiinkin hyödyntää Oulun Ammattikorkeakoulussa enemmän. Esimerkiksi tietoliikenteen rajaus liikenteen perusteella voitaisiin toteuttaa varmasti paremmin pidemmän aikavälin seurannan pohjalta. Myös palvelimen sertifikaatit voitaisiin asentaa varmenneyritykseltä paikallisesti luotujen sertifikaattien sijaan ja käyttäjien tunnistaminen voitaisiin myös toteuttaa sertifikaatteja käyttäen. Myös mahdollisuus IPSec-protokollan käyttöönottoon nykyisen SSL pohjaisen VPN-ratkaisun sijaan kannattaisi tulevaisuudessa kartoit-

taa. Tämä mahdollistaisi kolmannen osapuolen asiakasohjelmistojen käytön GlobalProtect asiakasohjelmiston sijaan.

Luotua ympäristöä ei ehditty tämän opinnäytetyön puitteissa testata kovin kattavasti, joten ratkaisu on syytä testata esimerkiksi varsinaisessa opetuskäytössä ennen kuin aiemmin käytössä ollut VPN-ratkaisu poistetaan käytöstä.

6 POHDINTA

Opinnäytetyö toteutettiin keräämällä ensin monipuolinen tietoperusta, jossa käytettiin ajantasaisia lähteitä ja tämän jälkeen itse käytännön toteutus, dokumentointi kulki koko opinnäytetyön ajan rinnalla. Lähteet koostuivat niin kirjoista, lehdistä, artikkeleista kuin tuotteiden verkkosivuista. Lähteinä käytin niin suomen- kuin englanninkielisiäkin julkaisuja. Lähtökohtana tietoperustan luomiselle oli lähteiden ajantasaisuus, koska varsinkin tietoverkoista materiaalia oli runsaasti saatavilla. Lähteet olivatkin Microsoftin Technetiä lukuunottamatta kaikki 2010-luvulta.

Harmittavasti paras lähde löytyi viimeisenä, jonka takia jouduin palaamaan osin jo aiemmin luomaani tietoperustaan. Paras lähde tämän opinnäytetyön näkökulmasta oli Stewart, J. Michaelin englanninkielinen kirja tietoverkoista, tietoturvasta, palomuureista ja VPN-yhteyksistä. Kyseistä kirjaa ei alun perin löytynyt minkään oppilaitoksen tai julkisen kirjaston valikoimista, mutta se ystävällisesti ostettiin Oulun Ammattikorkeakoulun valikoimaan.

Verkkosivuja pyrin välttämään lähteinä, mutta varsinkin Palo Alto Networksin tuotteista informaatiota oli hyvin heikosti tarjolla muualla kuin heidän omilla verkkosivuillaan. Tämän lisäksi viittasin muutamassa kohdassa Microsoftin Technetiin. Palo Alto Networksin tuotteiden osalta tukeuduin vahvasti myös puhelinkeskustelusta saamaani informaatioon sekä heidän kanssaan käymään sähköpostikeskusteluun. Ennen puhelinkeskustelua listasin paperille asioita, jotka tahdoin puhelun aikana selvittää (liite 1). Täytyykin todeta, että Palo Alto Networks tarjosi hyvää ja helposti saatavilla olevaa asiakaspalvelua. Edellä mainittujen menetelmien lisäksi osallistuin Palo Alto Networksin webinaariin 27.11.2014, katsoin lukuisia videoita sekä heidän omilta internetsivuiltaan että myös videopalvelu Youtubesta.

Opinnäytetyön loppuvaiheessa oli jonkin verran haasteita itse käytännön toteutuksen kanssa, lähinnä siitä syystä etten ollut aiemmin vastaavanlaisia verkkoratkaisuja käytännössä toteuttanut. Palo Alto Networksin konfigurointimahdollisuudet ovat lähes rajattomat, joten minulle oli aluksi vaikea hahmottaa mitkä asiat ovat oleellisia VPN-yhteyden luomiseen. Toisaalta minulla ei myöskään ollut historian painolastia esimerkiksi Ciscon tuotteista, koska joiltain osin logiikka niissä eroaa Palo Alto Networksin tuotteista. Myös graafinen käyttöliittymä helpotti hahmottamaan laitteessa jo olevia asetuksia ja nopeutti varmasti laitteen käyttöönottoa huomattavasti. Jälkikäteen

tosin voi todeta, että ongelmien selvittely auttoi hahmottamaan asian paremmin ja sen varmasti tulee muistamaan tulevaisuudessa myös varmemmin.

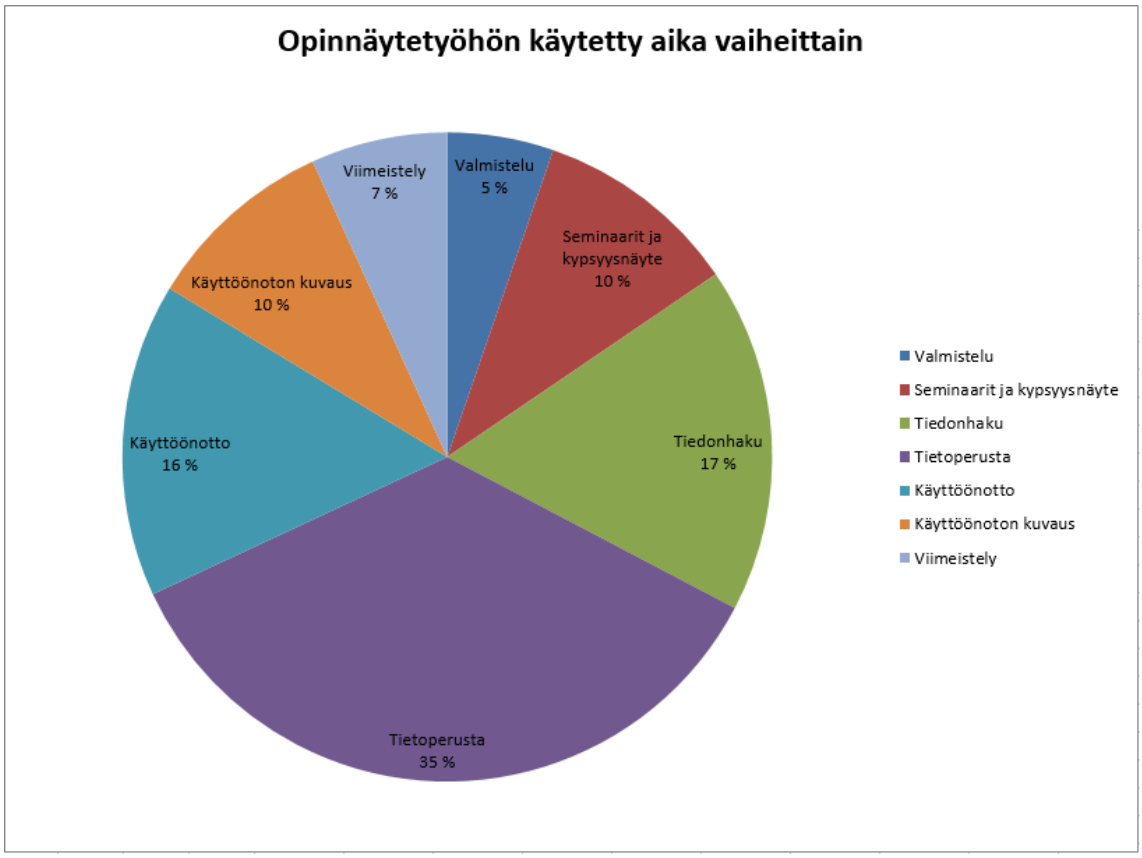
Jo alun perin oli tiedossa, että opinnäytetyön aikataulu on haasteellinen, itse käyttöönottovaihetta helpotti ja nopeutti mahdollisuus hyödyntää aiempaa etäkäyttöratkaisua, jonka ylitse pääsin palomuuria konfiguroimaan. Joiltain osin minun piti itse käytännön toteutuksessa palata takaisin täydentämään tietoperustaa, esimerkiksi osoitteenmuunnoksesta (NAT) alun perin en ollut luonut tietoperustaa.

Opinnäytetyö toteutettiin pääosin reilun kahden kuukauden aikana, koska opinto-oikeuteni oli loppumassa vuoden 2014 lopussa. Onneksi olin tietojenkäsittelyn opintoni jo muilta osin saattanut loppuun, jolloin pystyin keskittymään hyvin täysipainoisesti opinnäytetyön tekemiseen. Pidin opinnäytetyön etenemisestä tarkkaa kirjanpitoa (kuvio 39).

19.11.2014	60min	OHJAUSSEMINAARI: Valmistelua ohjausseminaariin
21.11.2014	**75min**	**OHJAUSSEMINAARI**
22.11.2014	90min	KIRJOITTAMINEN: Ohjausseminaarissa tulleiden kommenttien pohjalta tehtäviä muutoksia
23.11.2014	120min	KIRJOITTAMINEN: Ohjausseminaarissa tulleiden kommenttien pohjalta tehtäviä muutoksia
24.11.2014	60min	TIEDONHAKU: Microsoft DirectAccess
24.11.2014	180min	KIRJOITTAMINEN: YSA, Microsoft DirectAccess
25.11.2014	150min	KIRJOITTAMINEN: Aktiivihakemisto
26.11.2014	180min	KIRJOITTAMINEN: Ratkaisun valinta, käyttöönotto ja korjaukset/täydennykset
27.11.2014	120min	KIRJOITTAMINEN: korjaukset/täydennykset, johdannon uusiksi kirjoittaminen
27.11.2014	60min	TIEDONHAKU: Palo Alto Networks webinaari

KUVIO 39. Ote opinnäytetyön etenemisen kirjanpidosta

Tämä mahdollisti myös tarkastella omaa ajankäyttöäni kriittisesti ja näin ollen pysyä alkuperäisessä tavoiteaikataulussa. Tarkka kirjanpito mahdollisti myös erinäiset raportit opinnäytetyön edistymisestä kuten esimerkiksi opinnäytetyöhön käytetty aika vaiheittain (kuvio 40).



KUVIO 40. Opinnäytetyöhön käytetty aika vaiheittain

Opinnäytetyöstä on tietoturvasyistä poistettu viittaukset sisäiseen tietoverkkorakenteeseen peittämällä esimerkiksi kuvankaappauksista IP-osoitteet. Prosessi palomuurin konfiguroinnista on kuvattu liitteessä (liite 2) ja tämän lisäksi opinnäytetyön toimeksiantajalle eli Oulun Ammattikorkeakoululle on erikseen toimitettu palomuurille konfiguroidut asetukset erillisenä dokumenttina.

Jos opinnäytetyöprosessia miettii kokonaisuutena, niin huomasin että minulle tärkeää oli kerätä kaikki saatavilla oleva tieto, muistiinpanot ja esimerkiksi alustava lähdeluettelo yhteen dokumenttiin. Näin ollenkin loin omia väliaikaisia otsakkeita opinnäytetyöpohjaan, esimerkkinä mainittakoot juuri kyseiset *alustava lähdeluettelo* sekä *muistiinpanot*. Näin sain pidettyä kaiken tarpeellisen tiedon yhdessä paikassa ja opinnäytetyöprosessin hallinnassani.

LÄHTEET

Andreasson, A & Koivisto J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

Beasley, J & Nilkaew, P. 2012. Networking Essentials. Indianapolis: Pearson IT Certification.

Cisco. 2014. User Guide for Cisco Security Manager 4.7. Viitattu 31.10.2014. http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/user/guide/CSMUserGuide.pdf

Desmond, B., Richards, J., Allen, R. & Lowe-Norris, A. 2013. Active Directory. 5th Edition. Sebastopol: O'Reilly Media, Inc.

Horley, E. 2013. Practical IPv6 for Windows Administrators. New York: Apress.

Karinen, I. 2014. Asiantuntijalta: Nimipalvelukaappaus on uhka internetille. Tietosuoja 2/2014.

Krause, J. 2013. Microsoft DirectAccess Best Practices and Troubleshooting. Birmingham: Packt Publishing

Lobo, L. & Lakshman, U. 2014. CCIE Security v4.0 Quick Reference. Third Edition. Indianapolis: Cisco Press.

Lowe, D. 2010. Networking For Dummies. 9th edition. Indianapolis: Wiley Publishing, Inc.

Microsoft Technet. 2007. Active Directory Domain Services Overview. Viitattu 29.10.2014. http://technet.microsoft.com/library/cc731053%28WS.10%29.aspx

Microsoft Technet. 2008. VPN Tunneling Protocols. Viitattu 03.11.2014. http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx

Microsoft Technet. 2009. DirectAccess. Viitattu 24.11.2014. http://technet.microsoft.com/en-us/library/dd637821%28v=WS.10%29.aspx

Microsoft Technet. 2014a. Remote Desktop Services Overview. Viitattu 06.11.2014. http://technet.microsoft.com/library/hh831447.aspx

Microsoft Technet. 2014b. What Are Domains and Forests?. Viitattu 25.11.2014. http://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx

Minasi, M., Greene, K., Booth, C., Butler, R., McCabe, J., Panek, R., Rice, M. & Roth, S. 2013. Mastering Windows Server 2012 R2. Hoboken: Sybex.

Mäkelä, H. 2014. Tietotekniikan peruskirja. Jyväskylä: Docendo Oy.

Palo Alto Networks. 2014a. PA-500 Overview. Viitattu 26.11.2014. https://www.paloaltonetworks.com/products/platforms/firewalls/pa-500/overview.html

Palo Alto Networks. 2014b. VPN. Viitattu 19.11.2014. https://www.paloaltonetworks.com/products/features/networking-vpn.html

Palo Alto Networks. 2014c. Wildfire – Next Generation Firewall Technology. Viitattu 28.11.2014. https://www.paloaltonetworks.com/products/technologies/wildfire.html

Pogue, D. 2013. Windows 8.1: The Missing Manual. Sebastopol: O'Reilly Media, Inc.

Rao, U.H & Nayak, U. 2014. The InfoSec Handbook. New York: Apress Media LLC.

Shrivastava, A. & Rizvi, M.A. 2014. External authentication approach for virtual private network using LDAP. Networks & Soft Computing (ICNSC), 2014 First International Conference19-20.8.2014. 50-54.

Stewart, J. Michael. 2014. Network Security, Firewalls, and VPNs. Burlington: Jones & Bartlett Learning.

Tanenbaum, A & Wetherall, D. 2014. Computer networks. 5th Edition. Essex: Pearson Education Limited.

PUHELINHAASTATTELUN RUNKO LIITE 1

Puhelinhaastattelun suunniteltu runko ennen keskustelua Palo Alto Networks teknisen henkilön kanssa

- *Saatavilla olevat tuotteet (niin fyysiset kuin virtuaalisetkin palomuurit) ja niiden eroavaisuudet?*
- *Termistö: onko GlobalProtect yhteinen nimitys käyttöliittymäohjelmistolle ja yhteinen kaikille tuotteille?*
- *Asiakasohjelmisto: tuleeko tuotteet mukana ja voidaanko käyttää mitä tahansa muuta VPN asiakasohjelmistoa*
- *Protokollat: mitä protokollia Palo Alto Networks tuotteet käyttävät?*
- *Minkälaisiin käyttötarkoituksiin voidaan implementoida?*
- *Hyyödyt ja haitat: mikä erottaa tuotteen kilpailijoiden tuotteista ja esimerkiksi avoimen lähdekoodin VPN-tuotteista?*
- *Asennus: kuinka asennetaan ja onko ohjeita saatavilla? Entä virtuaaliset?*
- *Käyttäjätunnuksien hallinta ja integroituminen esimerkiksi aktiivihakemistoon?*
- *Käyttöjärjestelmät: Windows/Linux/Mac?*
- *Mikä on HIP (Host Information Profile)?*
- *Ohjelmistotuotteen ominaisuudet, esimerkiksi raportointimahdollisuudet?*
- *Saatavilla olevat lisenssit ja niiden hinta?*

PALO ALTO NETWORKS PALOMUURIN KONFIGUROINTI LIITE 2

YLEISET

- IP-osoite
- Oletusyhdyskäytävä (default gateway)
- DNS-palvelin
- Web-palvelin
- Päivityksien asentaminen
- Laitteen rekisteröinti ja lisenssi
- Ylläpitäjien ja heidän rooliensa määrittely
- Paikallisten käyttäjien ja ryhmien luominen
- Vyöhykkeiden (zones) määrittely
- Rajapintojen (interfaces) määrittel
- Virtuaalireititttimen (virtual router) määrittely
- Osoitteenmuunnoksen (NAT) määrittely
- Turvallisuuspolitiikkojen määrittely (security policies)
- LDAP-integraation luominen ja sen automaattinen päivitys (group-mapping)
- Todennusprofiilin luominen (authentication profile)

VPN

- GlobalProtect asiakasohjelmiston lataaminen palomuurille
- Tunnelin luominen (tunnel)
- Loopback-liitännän luominen
- Sertifikaatin luominen palvelimelle
- Uuden vyöhykkeen luominen palomuurille
- Turvallisuuspolitiikkojen uudelleenmäärittely
- GlobalProtect portaalin määrittely (portal)
- GlobalProtect yhdyskäytävän määrittely (gateways)

TESTAUS