LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

SEURAAVAN SUKUPOLVEN PALOMUURI YRITYKSESSÄ

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
31.5.2012
Janne Rissanen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

RISSANEN, JANNE: Seuraavan sukupolven palomuuri yrityksessä

Tietoliikennetekniikan opinnäytetyö, 48 sivua, 1 liitesivu

Kevät 2012

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli vaihtaa yrityksen vanha Check Point -palomuuri seuraavan sukupolven Palo Alto -palomuuriin. Uutta palomuuria varten yritykseen rakennettiin laboratorioympäristö, jossa Palo Alto -palomuuria voitiin testata ja konfiguroida erillään yrityksen omasta sisäverkosta. Seuraavan sukupolven palomuurilla saavutettiin suurempi tiedonkäsittelykyky ja tietoturvallisempi ympäristö, sillä Palo Alto Networks:n valmistamat palomuurit sisältävät tehokkaat suorittimet ja pystyvät tunnistamaan haittaohjelmia jopa salatusta SSL-liikenteestä. Tämä opinnäytetyö tehtiin lahtelaiselle energia-alan yritykselle Lahti Energia Oy:lle.

Palomuuri on yksi tärkeimmistä verkkoa suojaavista komponenteista, jonka tehtävänä on estää haitallisen liikenteen pääsy verkon tai järjestelmän sisälle. Palomuurin viisi perustoimintoa ovat verkkoliikenteen hallinta, autentikointi, verkkoliikenteen välittäminen, resurssien suojaaminen ja tapahtumien taltiointi. Tavalliset palomuurit hallitsevat liikennettä IP-osoitteiden, protokollien ja käytettävien porttien mukaan. Nykyään dataliikenteen sisältöä ei voida kuitenkaan päätellä käytettävän portin ja protokollan mukaan, sillä ohjelmat osaavat piilottaa itsensä erilaisten piiloutumistekniikoiden avulla. Internet pakotti luomaan palomuureihin seuraavan sukupolven, jotta tietoverkkoja voitaisiin jälleen suojata luotettavasti.

Seuraavan sukupolven palomuuri pystyy tunnistamaan liikennöivän ohjelman riippumatta käytettävästä portista, protokollasta, piiloutumistekniikasta tai SSL-salauksesta. Seuraavan sukupolven palomuuri pystyy myös tunnistamaan verkon käyttäjän ja käyttämään tunnistetietoja palomuurisäännöissä. Uuden palomuurin käyttäminen LDAP-hakemistojen, kuten Microsoft AD:n kanssa helpottaa palomuurisääntöjen luomista, sillä palomuurisääntöjä voidaan tehdä AD:n käyttäjän tai käyttäjäryhmän mukaan.

Opinnäytetyössä vanhan Check Point -palomuurin asetukset siirrettiin Palo Alto -palomuuriin käyttäen hyödyksi seuraavan sukupolven palomuurien ominaisuuksia. Uuteen palomuuriin luotiin palomuurisäännöt, osoitemuunnokset, verkko-objektit ja VPN-yhteydet käyttäen vanhan palomuurin asetuksia pohjana. Seuraavan sukupolven palomuuri tarjosi lisää tietoturvaa, tarkempaa hallintaa ja nopeampaa tiedonkäsittelyä. Tuloksena saatiin tietoturvallisempi ympäristö, joka on helpommin hallittavissa.

Avainsanat: tietoturva, seuraavan sukupolven palomuurit, Palo Alto Networks, NGFW

Lahti University of Applied Sciences
Degree Programme in Information Technology

RISSANEN, JANNE: Next-generation firewall in a corporate network

Bachelor's Thesis in Telecommunications, 48 pages, 1 appendix

Spring 2012

ABSTRACT

The aim of this thesis was to change the client company's old Check Point Firewall to a next-generation Palo Alto firewall. This study was carried out for an energy company Lahti Energia Oy.

A new laboratory environment was built in which the Palo Alto firewall could be tested and configured separated from the company's own internal network. Due to powerful processors and new technology the next-generation firewall reached a higher data throughput and more secure environment. Palo Alto Networks' firewalls can detect malware even from an encrypted SSL traffic.

A firewall is one of the most important protective components of a network. The task of a firewall is to prevent malicious traffic to the network or the system. The five basic functions of a firewall are network traffic management, authentication, traffic forwarding, resource protection and event recording. Common firewalls control traffic through IP-addresses, protocols and ports. Today, data traffic content cannot be inferred from the port and protocol, as the programs can hide themselves by means of various hiding technologies. Because of the Internet a next generation had to be created to the firewalls, so computer networks could again be reliably protected.

The next-generation firewall is capable of detecting the program regardless of the used port, protocol, hiding technology or SSL encryption. The next-generation firewall is also able to identify the user and to use the identifying information in the firewall rules. Using LDAP directories, such as Microsoft AD, eases the creation of new firewall rules.

In this study the settings of an old Checkpoint firewall were moved to the new Palo Alto Firewall using the next-generation firewall features. On the new firewall were created the firewall rules, NAT, network objects, and VPN connections using the old base. The next-generation firewall offered more security, more precise control and faster data processing. The result of using a next-generation firewall was a more secure environment that is more easily manageable.

Key words: data security, next-generation firewalls, Palo Alto Networks, NGFW

LYHENNELUETTELO

AD	Active Directory. Microsoftin valmistama hakemistopalvelu Windows-toimialueille.
API	Application Programming Interface. Ohjelmointirajapinta, jonka mukaan ohjelmat voivat vaihtaa tietoa keskenään.
CLI	Command-line Interface. Komentoliittymä, jonka avulla ihminen ja kone voivat kommunikoida keskenään.
DLP	Data Loss Prevention. Tietoturvaohjelmistojen ominaisuus, joka pyrkii estämään yksityisen tiedon leviämisen ulkopuolisille.
DMZ	Demilitarized Zone. Fyysinen tai looginen aliverkko, joka yhdistää luotetun verkon epäluotettavaan verkkoon.
DNS	Domain Name System. Nimipalvelujärjestelmä, jonka avulla verkkotunnukset voidaan muuttaa IP-osoitteiksi.
DPI	Deep Packet Inspection. IP-paketin tutkimismenetelmä, jossa paketista tutkitaan osia datasisällöstä ja otsikosta.
ESP	Encapsulating Security Payload. IPSec-yhteyksien datavirtojen salausprotokolla.
FTP	File Transfer Protocol. Tiedonsiirtoprotokolla.
HA	High Availability. Tietojärjestelmien käytäntö, jossa pyritään takaamaan palvelun jatkuva toiminta.
HTTP	Hypertext Transfer Protocol. Protokolla Internet-selaimien ja WWW-palvelimien tiedonsiirtoon.

HTTPS	Hypertext Transfer Protocol Secure. HTTP- ja SSL-protokollien yhdistelmä salattuun tiedonsiirtoon.
ICMP	Internet Control Message Protocol. TCP/IP-protokollapinon kontrolliprotokolla.
IDS	Intrusion Detection System. Järjestelmä, jolla pyritään tunnistamaan tunkeutumisyritykset järjestelmään tai verkkoon.
IP	Internet Protocol. Protokolla, jolla laitteet kommunikoivat pakettikytkentäisessä verkossa.
IPS	Intrusion Prevention System. Järjestelmä, jolla pyritään estämään tunkeutumisyritykset järjestelmään tai verkkoon.
IPSec	IP Security Architecture. Joukko tietoliikenneprotokollia, joilla turvataan datavirtoja.
ISO	International Organization for Standardization. Standardisoimisjärjestö.
ISP	Internet Service Provider. Internet-palveluntarjoaja.
IT	Information Technology. Tietotekniikka.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen verkkoprotokolla.
MTU	Maximum Transmission Unit. Suurin protokollan tietoyksikön koko tavuina.
NAT	Network Address Translation. Osoitteenmuunnos.

OSI-malli	Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien kuvaus seitsemässä kerroksessa.
P2P	Peer to Peer. Vertaisverkko.
POLP	Principle of Least Privilege. Pienimpiden mahdollisten oikeuksien käytäntö.
PSK	Pre-Shared Key. Esijaettu avain.
QoS	Quality of Service. Tietoliikenteen priorisointi.
SMTP	Simple Mail Transfer Protocol. Protokolla, jolla sähköpostipalvelimet välittävät tietoa keskenään.
SNMP	Simple Network Management Protocol. TCP/IP-verkkojen hallintaprotokolla.
SSH	Secure Shell. Tietoliikenteen suojausprotokolla, jota käytetään yleensä pääte- ja FTP -yhteyksissä.
SSL	Secure Sockets Layer. IP-verkkojen salausprotokolla.
SSL-VPN	SSL Virtual Private Network. VPN-yhteys, joka salataan SSL-protokollalla.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla tiedonsiirtoon, jossa data lähetetään luotettavasti perille.
UDP	User Datagram Protocol. Tiedonsiirtoprotokolla, jossa paketin perillemenoa ei varmisteta kuten TCP:ssä.
VoIP	Voice over IP. Protokolla äänen siirtämiseen IP-verkoissa.

VPN	Virtual Private Network. Näennäinen yksityinen verkko.
WWW	World Wide Web. Maailmanlaajuinen hypertekstijärjestelmä.
XML	Extensible Markup Language. Tekstimuotoinen merkintäkieli.

SISÄLLYS

1 JOHDANTO

1.1 Työn tausta

Tietoteknisiä laitteita kehitetään hurjalla vauhdilla, ja markkinoille tuodaan koko ajan toinen toistaan hienompaa tekniikkaa. Vanhemmat laitteet jäävät väkisinkin uudempien laitteiden jalkoihin niin nopeudessa kuin ominaisuuksissa. Myös tietoliikenneyhteyksien nopeudet ovat kasvaneet huimaa vauhtia. Tekniikan kehitys asettaa myös yrityksen IT-osaston (Information Technology) harkitsemaan laitteistojen päivittämistä nykyaikaisemmiksi. Yrityksen sisäverkon ja julkisen verkon (Internet) välissä käytetään lähes poikkeuksetta palomuuria, jonka suorituskyvyn on vastattava yrityksen tarpeita. Tietoliikenneyhteyksien nopeuksien kasvaessa myös palomuurin on pystyttävä käsittelemään lisääntynyt dataliikenne.

Uuden palomuurin käyttöönotto yrityksessä voi tuoda mukanaan suuren työurakan, varsinkin jos palomuuriin on määritelty satoja erilaisia palomuurisääntöjä. Saman valmistajan palomuurituotteiden välillä palomuuriasetukset voivat olla helppo siirtää jopa yhden asetustiedoston avulla, mutta entä jos valmistaja vaihdetaankin toiseen? Lahti Energia Oy vaihtoi Nokian laitteistoalustalla toimineen Check Point -palomuuriohjelmiston Palo Alto Networks:n valmistamaan seuraavan sukupolven palomuuriin. Seuraavan sukupolven palomuurin käyttöönoton tavoitteena on mahdollistaa käyttäjä- ja ryhmäkohtainen palomuurisääntöjen luominen ja uhkien tunnistaminen luotettavammin. Uuden palomuurin tulisi myös pystyä käsittelemään yrityksen lisääntynyt dataliikenne ja suojaamaan sisäverkkoa ulkoisilta uhilta. Tämä opinnäytetyö kertoo Check Point -palomuurin korvaamisesta Palo Alto Networks -palomuurilla ja siihen liittyvistä työvaiheista.

1.2 Toimeksiantajan esittely

Lahti Energia Oy on Lahden ja Lahden lähikuntien alueella toimiva energia-alan yritys, jonka tuotteita ovat sähkö ja lämpö. Yhtiön juuret ulottuvat vuoteen 1907, jolloin Lahden kaupungin sähkölaitos perustettiin. Vuonna 1990 Lahden kaupunki yhtiöitti Lahden Energialaitoksen, jolloin syntyi Lahti Energia Oy. Lahti Energia -

konserni koostuu Lahti Energia Oy:stä ja vuonna 2007 perustetusta LE-Sähköverkko Oy:stä, jonka toimialana on verkkoliiketoiminta. Lahti Energia on tunnettu vuonna 2012 valmistuneesta Kymijärven jätteitä polttavasta voimalaitoksesta, joka on ympäristöystävällisesti toimiva jätevoimalaitos. (Lahti Energia Oy 2012a)

Lahti Energian toimipiste sijaitsee Lahden keskustassa Kauppakadulla. Voimalaitoksia Lahti Energialla on kolme: Kymijärven ja Teivaanmäen voimalaitokset Lahdessa, sekä Heinolassa sijaitseva sähkö- ja höyryvoimalaitos. Heinolan voimalaitos tuottaa energiaa vain teollisuuden tarpeisiin. (Lahti Energia Oy 2012c.) Vuonna 2010 Lahti Energia -konsernin liikevaihto oli 180,0 miljoonaa euroa ja liikevoitto 51,2 miljoonaa euroa. Henkilöstöä vuoden 2010 lopussa oli yhteensä 237. Asiakkaita Lahti Energia Oy:llä oli yhteensä yli 80000 (Lahti Energia Oy 2012b).

2 TIETOTURVA YRITYKSESSÄ

2.1 Tietoturvan määrittely

Turva on jatkuva toimenpide, jossa suojataan kohdetta hyökkäyksiltä. Kohde voi olla yritys, omaisuus tai vaikkapa ihminen. Tietokonejärjestelmistä puhuttaessa turvallisuus kattaa järjestelmän fyysisen turvallisuuden, kuten prosessorin, näppäimistön tai muun komponentin. Fyysisen laitteiston lisäksi tietokonejärjestelmä sisältää myös dataa, joka ei ole aineellisesti näkyvissä. Myös tämä aineeton tieto täytyy suojata. Tietoliikenneverkoissa suojauksen kohteena ovat reitittimet, kytkimet ja palvelimet, jotka ovat fyysisiä komponentteja verkon sisällä. Myös näiden välillä kulkeva liikenne ja palvelimien sisältämä data täytyy suojata. Tietoturva käsittää siis näiden resurssien turvaamisen luvattomalta pääsyltä, käytöltä, muokkaamiselta, varkaudelta ja fyysiseltä vahingonteolta. (Kizza 2005, 49.)

Tietoturva jaetaan kolmeen osaan:

- luotettavuus: estetään luvaton tiedon leviäminen kolmansille osapuolille.
- eheys: estetään luvaton resurssien ja tiedon muokkaaminen.
- saatavuus: estetään järjestelmän luvaton hallussapito ja taataan järjestelmän resurssit niitä tarvitsevien käyttöön.

Luotettavuudella tarkoitetaan jotain salaista, jonka ei haluta leviävän ulkopuolisten käyttöön. Nykyään lähes kaikki organisaatioiden salaiset tiedot säilytetään tietojärjestelmien tietokannoissa, joten niiden suojaaminen on ensiarvoisen tärkeää. Eheydellä pyritään takaamaan tietojen oikeellisuus, jottei niitä pääsisi luvattomasti tuhoamaan tai muokkaamaan. Vaikka aineellista vahinkoa tietojen kadotessa ei tapahtuisikaan, voivat kustannukset olla kuitenkin erittäin kalliit. Tietokantojen ja järjestelmien palauttaminen vaatii aikaa ja asiantuntemusta, mutta auttaako se jos asiakkaiden ja käyttäjien luottamus on jo menetetty? Saatavuudella taataan, että järjestelmän kaikki mahdolliset vapaat resurssit ovat aina käytössä, eikä tunkeutujille tai luvattomille käyttäjille tarjota prosessorin laskentatehoa tai levytilaa. (Zwicky, Cooper & Chapman 2001, 28-30.)

2.2 Mitä suojataan ja miksi?

Yrityksellä tai organisaatiolla on järjestelmiä ja resursseja, jotka täytyy suojata luvattomalta käytöltä. Luvaton käyttö voi tapahtua joko ulkopuolelta tai organisaation sisältä, joten molempiin tilanteisiin on varauduttava. Suojaamiseen ja tietoturvaan kuuluvat verkkolaitteistojen ja ohjelmistojen suojaus. Laitteistoihin kuuluvat järjestelmien näppäimistöt, hiiret ja muut hallintalaitteet. Suojattavia verkkolaitteita ovat kaikki verkkoon liitetyt laitteet, kuten palomuurit, kytkimet ja reitittimet. Myös tiedonsiirtokanavat on suojattava salakuuntelulta. Ohjelmistoihin kuuluvat järjestelmien käyttöjärjestelmät, palvelinprotokollat, selaimet, ohjelmat ja muut palvelimissa tai tietokoneissa säilytettävät tiedot. (Kizza 2005, 53.)

Resurssien lisäksi tietoturvalla pyritään suojaamaan myös organisaation maine. Yrityksen WWW-sivuille (World Wide Web) murtautunut henkilö voi tahrata yrityksen maineen lisäämällä sivustolle asiaankuulumatonta sisältöä. Myös sähköpostiin murtautumalla voidaan lähettää yrityksen nimissä viestejä, jotka voivat vahingoittaa yrityksen mainetta. Tunkeutujat voidaan poistaa ja WWW-sivut korjata mutta organisaation maineeseen voi jäädä pysyvä tahra. (Zwicky, Cooper & Chapman 2001, 31-32.)

Hyökkäyksiä on erilaisia: tunkeutuminen, palvelunestohyökkäys ja tietovarkaus. Tunkeutuminen on yksi yleisimmistä hyökkäyksen tyypeistä. Tunkeutumisen tarkoituksena on saada järjestelmä haltuun ja esittäytyä sen luvallisena käyttäjänä. Palvelunestohyökkäyksissä pyritään nimensä mukaisesti estämään palveluiden käyttäminen esimerkiksi täyttämällä järjestelmä tai verkko viesteillä, verkkopyynnöillä ja prosesseilla. Järjestelmä ei enää palvele käyttäjiään vaan käyttää aikansa pyrkimällä vastaamaan kaikkiin viesteihin ja prosesseihin. Tietovarkauksissa pyritään saamaan järjestelmästä tietoa, joka ei oikeasti olisi saatavissa. Salakuuntelemalla verkkoa voidaan saada selville esimerkiksi salasanoja, joiden avulla tietovarkauksia on mahdollista tehdä. (Zwicky, Cooper & Chapman 2001, 32-37.)

2.3 Tietoturvallisen ympäristön luominen

Tietoturvallinen ympäristö voidaan luoda monella eri tapaa, joten yhtä ja oikeaa tapaa ei ole olemassa. Jokainen ympäristö on erilainen, ja niihin tulee soveltaa parhaaksi todettua tietoturvastrategiaa ja menetelmää. Tämän kappaleen jälkeen on esitetty muutamia perusprinsiipejä, jotka pitäisi jokaisessa tietoturvallisessa ympäristössä ottaa huomioon.

Verkkolaitteiden tietoturvan tulisi olla kerrosteinen, eli jokaisessa verkkoon kytketyssä laitteessa otetaan huomioon tietoturvan vaatimukset. Kerrosteisella tietoturvalla saavutetaan se, että jonkin puolustuksen komponenteista vikaantuessa koko verkko ei altistu hyökkäyksille tai väärinkäytöksille. Esimerkiksi yrityksen verkossa ei riitä, että tietoturva-asetukset ovat kunnossa palomuurissa, vaan myös reitittimet, kytkimet, palvelimet ja työasemat täytyy suojata. (Thomas 2005, 86.)

Pääsynvalvonta ja roolit ovat myös osa tietoturvapolitiikkaa. Pääsynvalvonnalla pyritään estämään tarpeeton verkkoliikenne ja sallimaan vain toiminnan kannalta tarpeellinen liikenne. Pääsynvalvontaan on olemassa erilaisia käytäntöjä, kuten pienimpiden mahdollisten oikeuksien käytäntö POLP (Policy of Least Privilege), jossa vain tarpeellinen liikenne sallitaan ja kaikki muu on kielletty. Rooleilla voidaan määrittää käyttäjäkohtaisesti pääsystä ja oikeuksista tiettyihin resursseihin. Esimerkiksi tietoliikenneverkon ylläpitäjällä täytyy olla oikeudet konfiguroida kytkimiä mutta normaalilla käyttäjällä ei. (Thomas 2005, 86-87.)

Käyttäjien tietoisuus on iso osa yrityksen tietoturvaa. Käyttäjille tulisi opastaa tietoturvan tarkoitus, jotta esimerkiksi salasanat pidettäisiin turvallisina. Käyttäjät eivät tarkoituksellisesti luo tietoturvariskejä, vaan he eivät täysin ymmärrä tietoturvan tärkeyttä. Paras keino parantaa käyttäjien tietoturvallista käyttäytymistä on pitää tietoturvakoulutuksia. (Thomas 2005, 87.)

Järjestelmien tarkkailu ja järjestelmäpäivitykset ovat perusasia luodessa tietoturvallista ympäristöä, mutta ne unohtuvat helposti. Verkkoa tarkkaillessa saadaan tärkeää tietoa tunkeutumisyrityksistä ja hyökkäyksistä. Tunkeutumisen havaitsemisjärjestelmä IDS (Intrusion Detection System) on hyvä työkalu verkon tarkkai-

luun. Järjestelmäpäivitykset ovat tietoturvan perusasioita mutta saattavat jäädä muiden kiireiden ohella sivuun. Suurin osa järjestelmäpäivityksistä on juurikin tietoturvapäivityksiä, joten niiden asentaminen on ensiarvoisen tärkeää. (Thomas 2005, 87.)

Jos vahinko tapahtuu tai järjestelmä joutuu hyökkäyksen kohteeksi, on yrityksellä hyvä olla jonkinlainen toimenpidesuunnitelma. Toimenpidesuunnitelman tulisi sisältää tiedot siitä, miten yritys reagoi hyökkäyksen tapahtuessa ja kuinka tilanne korjataan. Kuivaharjoittelu tuo esille toimenpidesuunnitelman heikot kohdat, joten niihin voidaan puuttua ennen kuin todellinen uhka tapahtuu. (Thomas 2005, 88.)

Verkon kannalta tärkein tietoturvakomponentti on palomuuri, johon tämä opinnäytetyö keskittyy. Palomuurin oikeaoppinen konfiguroiminen ja palomuurisääntöjen luominen on tärkeä perusta tietoturvallisen ympäristön luontiin. Tämän opinnäytetyön kappaleissa 3 ja 4 käydään läpi erilaisten palomuurien toimintatapaa ja ominaisuuksia.

3 TAVALLISET PALOMUURIT

Palomuuri on yrityksen tietoliikenneverkon tietoturvan kulmakivi ja yksi tärkeimpiä verkkoa suojaavista komponenteista. Sanasta palomuuri saattaa tulla ensimmäisenä mieleen rakennuksissa käytettävä palon leviämistä estävä seinä. Tietoverkoissa ajatus on sama: pyritään estämään haluamattoman liikenteen pääsy verkon tai järjestelmän sisälle.

Kotikäyttäjälle tutuin palomuuri on tietokoneelle asennettu ohjelmisto, joka toimii yhdessä käyttöjärjestelmän kanssa. Tällaisesta palomuurista käytetään nimitystä isäntä-pohjainen palomuuri (host-based firewall). Jos palomuuri toimii itsenäisenä komponenttina verkon sisällä ja kontrolloi verkkojen välistä liikennettä, on kyseessä verkko-pohjainen palomuuri (network-based firewall). Suomen kielessä puhutaan yleensä ohjelmistopalomuureista ja laitteistopalomuureista. (Noonan & Dubrawsky 2006, 5.)

3.1 Tavallisen palomuurin toimintaperiaate

Palomuuri on verkkolaite tai ohjelmisto, joka valvoo ja hallinnoi verkkoliikennettä. Palomuurilta oletetaan viisi perustoimintoa, joista sen tulisi suoriutua:

- verkkoliikenteen hallinta ja kontrollointi
- autentikointi
- verkkoliikenteen välittäminen
- resurssien suojaaminen
- tapahtumien taltiointi ja raportointi.

(Noonan & Dubrawsky 2006, 5–6.)

Verkkoliikenteen hallinta ja kontrollointi tarkoittaa liikenteen ohjaamista turvattomasta verkosta turvalliseen verkkoon esimerkiksi internetistä yrityksen sisäverkkoon. Verkkoliikenteen kontrolloinnissa palomuuri joko päästää liikenteen läpi tai estää sen. Tämä tapahtuu tutkailemalla paketteja sekä yhteyksiä ja suodat-

tamalla liikennettä palomuuriin asetettujen sääntöjen mukaisesti. (Noonan & Dubrawsky 2006, 6–7.)

Jokainen IP-paketti (Internet Protocol) sisältää otsikkotietoja, joiden mukaan verkkoliikennettä voidaan suodattaa. Tärkeimpiä otsikkotietoja IP-paketista ovat:

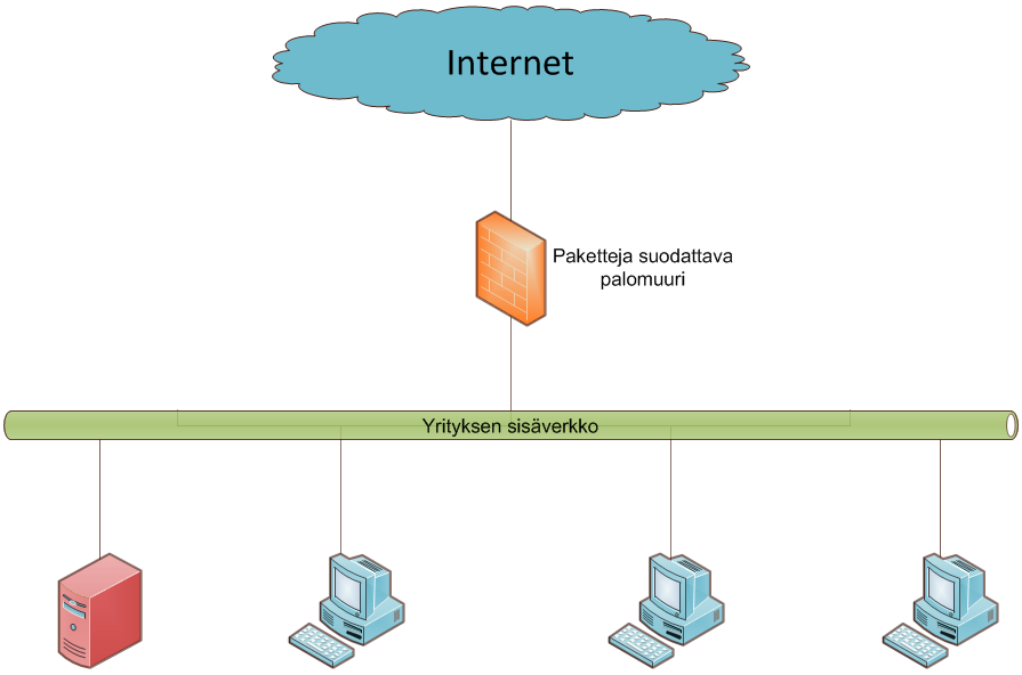
- lähteen IP-osoite
- kohteen IP-osoite
- protokolla
- lähdeportti
- kohdeportti
- viestityyppi
- paketin koko.

Palomuuri voi tutkia IP-paketista myös muita tietoja kuin otsikkotiedot. HTTP-yhteyksien (Hypertext Transfer Protocol) WWW-sivun nimi on mahdollista selvittää IP-paketin sisältä, joten suodatussääntöjä voidaan tehdä myös domainnimien perusteella. Paketin koon mukaan suodatettava liikenne on tehokas estämään palvelunestohyökkäyksiä, sillä usein palvelunestohyökkäyksissä käytetään hyväksi väärin muotoiltuja paketteja. (Zwicky, Cooper & Chapman 2001, 155.) Eräs palvelunestohyökkäystapa on lähettää ylipitkiä ICMP echo request -viestejä (Internet Control Message Protocol), joilla pyritään tukkimaan koko verkon kaistanleveys (CERT, 2001).

Paketteja suodattava palomuuri (kuvio 1) voi tehdä seuraavia tehtäviä saapuvalle paketille:

- lähettää paketti kohteeseen
- hylätä paketti
- hylätä paketti ja ilmoittaa siitä käyttäjälle
- kirjata paketista tietoja lokiin
- lähettää hälytys
- muokata pakettia (esimerkiksi NAT (Network Address Translation))
- lähettää paketti toiseen määränpäähän, johon se oli alun perin menossa.

Palomuuri voi myös muokata suodatussääntöjä tulevien pakettien mukaan. Esimerkiksi havaittuaan palvelunestohyökkäyksen palomuuri voi kieltää kaiken liikenteen vihamielisestä IP-osoitteesta. (Zwicky, Cooper & Chapman 2001, 157.)

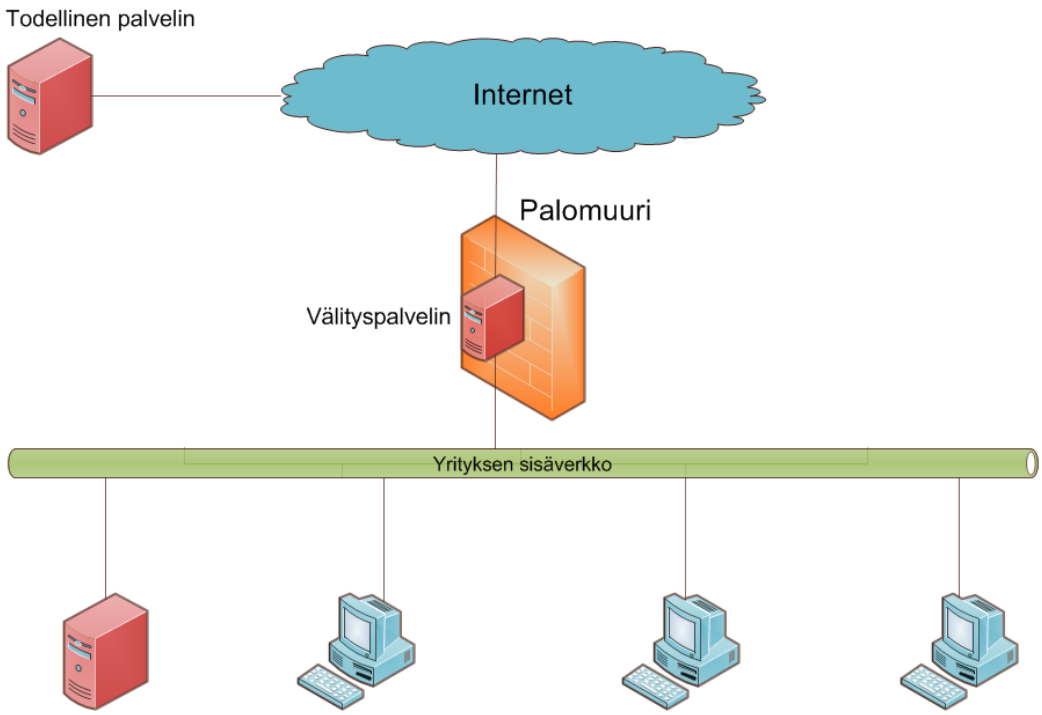


KUVIO 1 Paketteja suodattava palomuuri

Pelkkä verkkoliikenteen suodatus porttien tai IP-osoitteen perusteella ei riitä, sillä tiettyjä palveluita ei haluta tarjota kaikille. Tämän takia palomuurin täytyy tukea yhteyden autentikointia, jotta palveluja voidaan tarjota vain valtuutetuille käyttäjille. Autentikointi voidaan suorittaa esimerkiksi perinteisellä käyttäjätunnuksen ja salasanan kyselyllä. Muita menetelmiä ovat muun muassa sertifikaatit, julkiset avaimet ja PSK (Pre-Shared Key). (Noonan & Dubrawsky 2006, 9–10.)

Verkkoliikenteen välittämisessä voidaan ajatella palomuurin toimivan välityspalvelimena eli proxyna. Proxy-palvelimen tehtävänä on olla kahden isäntäkoneen välissä ja estää niiden suora liikennöinti keskenään. Isäntäkoneet eivät tiedosta keskustelevansa välityspalvelimen kautta, vaan ne kommunikoivat aivan kuten suorassakin verkkoyhteydessä. Proxy-palvelin vastaanottaa kohteelle saapuvan datan, parsii siitä halutun informaation itselleen ja muodostaa siitä paketin uudelleenlähetettäväksi kohteelle. Kun palomuuri toimii tällä tavoin, palomuuri voi

tutkia pakettien sisällön ennen lähettämistä kohteelle ja näin ollen päästää vain sallitun datan kohteelle. Jos paketti sisältää vahingollista dataa, palomuuri pudottaa paketin eikä lähetä sitä vastaanottajalle. Palomuurin toimiessa välityspalvelimena, käytetään palomuurista nimitystä sovellusvälityspalvelin (application proxy) (kuvio 2). (Noonan & Dubrawsky 2006, 10.)



KUVIO 2 Palomuuri välityspalvelimena

Resurssien suojaaminen saavutetaan käyttöoikeuksien määrittelyllä, yhteyksien ja pakettien seurannalla sekä liikenteen välittämisellä. Resursseiksi määritellään palvelut ja laitteistot, jotka ovat kytkeytyneet verkkoon. Menetelmät ovat siis aiemmin todetut palomuurin perusominaisuudet ja näiden yhdistelmät. Vaikka palomuurin tehtävänä on suojata verkossa olevia laitteita, se ei pysty vielä takaamaan resursseille täysin turvallista toimintaympäristöä. Esimerkiksi julkinen HTTP-palvelin, johon ei ole asennettu viimeisimpiä tietoturvapäivityksiä, on altis verkon ulkopuolelta tuleville hyökkäyksille. Hyökkääjä voi ottaa yhteyden porttiin 80 (HTTP), koska se on palomuurisäännöissä sallittu ja käyttää hyväkseen palvelinohjelmistossa olevaa tietoturva-aukkoa esimerkiksi estämällä palvelun toiminnan. Tämän takia verkon sisällä olevien laitteiden ohjelmistojen tietoturvapäivitykset täytyy olla ajan tasalla. (Noonan & Dubrawsky 2006, 10–11.)

Tapahtumien raportointi ja tallentaminen lokitiedostoon on tärkeää, jotta järjestelmänvalvoja voi tarkastella muodostuneita yhteyksiä ja menneitä tapahtumia. Palomuurilla pitäisi olla myös hälytysmekanismi, joka antaa ilmoituksen esimerkiksi sähköpostitse, kun jotakin asetettua sääntöä rikotaan. Lokitiedoston tulisi sisältää saapuneet ja lähteneet paketit sekä palomuuriohjelmiston omat ilmoitukset, jotka liittyvät järjestelmään. Järjestelmän ilmoituksia ovat esimerkiksi muistin täyttyminen tai järjestelmän vikaantuminen. (Noonan & Dubrawsky 2006, 11–12.)

3.2 Palomuurin käyttöönotto ja palomuurisäännöt

Palomuurin käyttöönoton ensimmäinen vaihe on valmistelu ja suunnittelu. Perusasioita suunnittelussa on kartoittaa, mitä palveluja tarjotaan Internetiin ja mitä palveluja Internetistä käytetään. Näin luodaan jo hieman pohjaa, kuinka palomuurisäännöt tulee toteuttaa. Suunnittelussa tulee ottaa myös huomioon, kuinka suorituskykyinen palomuurilaitteisto vaaditaan ja täytyykö verkkoliikenteen kasvuun varautua. Muita pohdittavia asioita ovat vaadittavat oheislaitteet (näytöt, näppäimistöt, hiiret), varmistus, fyysinen tilanvaraus, jatkuva sähkönsyöttö ja kaapelointi. Palomuurin hallinta täytyy myös suunnitella: ketkä saavat muuttaa palomuurin asetuksia ja miten hallinta toteutetaan? Palomuurissa voi olla esimerkiksi etähallinta SSH-yhteyden (Secure Shell) kautta tai pelkkä konsolihallinta. (Allen 2002, 124, 139–140.)

Palomuuriratkaisun suunnittelun jälkeen on hyvä piirtää kaavio tai topologiakuva verkosta ja verkon laitteistosta. Dokumentoinnin jälkeen on helppo katsoa verkossa olevia laitteita ja suunnitella uusien laitteistojen sijoittelua. (Allen 2002, 127.)

Kun suunnittelu ja dokumentointi on tehty valmiiksi, täytyy luoda palomuurisäännöt. Palomuurisääntöjen luomiseen käytetään erilaisia tekniikoita, joista yleisimmät ovat pakettisuodatus ja sovellusvälityspalvelin. Muita tekniikoita ovat muun muassa tilallinen pakettisuodatus (Stateful Packet Inspection) ja läpinäkyvä välityspalvelin (Transparent Proxy). (Allen 2002, 127–131.)

Pakettisuodatus toteutetaan tutkimalla saapuvien ja lähtevien pakettien otsikkotietoja. Säännöt voidaan tehdä lähettäjän tai vastaanottajan IP-osoitteen, protokollan tai käytettävän portin mukaan. Pakettisuodatusta käyttämällä saavutetaan paras suorituskyky, haittapuolena kuitenkin sääntöjen työläs luominen. Pakettisuodatus toimii ISO (International Organization for Standardization) OSI -mallin (Open Systems Interconnection Reference Model) kolmannella kerroksella, eli verkkokerroksella (Network Layer). (Noonan & Dubrawsky 2006, 34–35.)

Sovellusvälityspalvelinta käytettäessä palomuurilta vaaditaan toimintaan soveltuva palvelinohjelmisto. Tässä menetelmässä asiakas, joka haluaa muodostaa yhteyden, ottaa ensin yhteyden palomuurin välityspalvelinohjelmistoon. Yhteyttä muodostava asiakas pyytää välityspalvelinta muodostamaan yhteyden kohteeseen. Jos palomuurin välityspalvelinohjelmisto hyväksyy pyynnön, muodostuu kaksi yhteyttä: yksi asiakkaalta välityspalvelimeen ja toinen kohteelta välityspalvelimeen. Tämän jälkeen välityspalvelin välittää kaiken liikenteen asiakkaan ja kohteen välillä. Toiminto on huomattavasti raskaampi kuin pelkkä pakettisuodatus ja vaatii enemmän suorituskykyä palomuurilta. Sovellusvälityspalvelin on kuitenkin tietoturvallisempi ratkaisu kuin pelkkä pakettisuodatuksen käyttö. Sovellusvälityspalvelin toimii ISO OSI -mallin tasolla seitsemän, eli sovelluskerroksella (Application Layer). (Noonan & Dubrawsky 2006, 37–38)

3.3 Nokia IP390 palomuurialusta

Nokia IP390 palomuurialusta on Check Point -palomuuriohjelmistoa käyttävä palomuurilaite keskisuurille ja suurille yrityksille. Palomuuri sisältää neljä sisäänrakennettua 1 Gbps verkkoliitäntää ja kaksi lisäkorttipaikkaa, joihin voidaan lisätä toiset neljä 1 Gbps verkkoliitäntää.

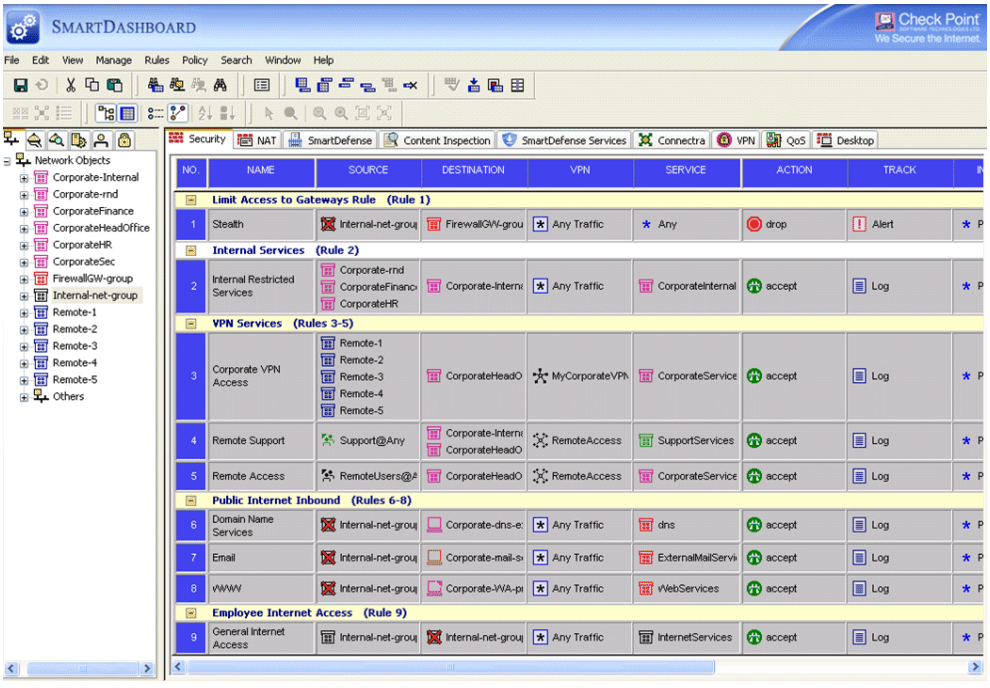
Nokia IP390 varustettuna Check Point -palomuuriohjelmistolla tarjoaa 3 Gbps tiedonsiirtonopeuden ja 36 000 samanaikaista yhteyttä. Palomuurialustan käyttöjärjestelmänä käytetään Nokia IPSO -käyttöjärjestelmää. Nokia IP390 palomuurialustan ominaisuuksiin kuuluvat palomuuritoiminnot, VPN-yhteydet (Virtual

Private Network), IDS, IPS (Intrusion Prevention System), web-suodatus ja virustentorjunta. (Nokia 2008)

3.4 Check Point -palomuuriohjelmisto

Check Point on Yhdysvaltalainen tietoturvayhtiö, joka tarjoaa tietoturvaohjelmia ja laitteita yrityksille. Check Pointin tuotteisiin kuuluvat Nokian palomuurialustalle suunnitellut palomuuriohjelmistot, kuten Check Point R75. Palomuuriohjelmisto asennetaan Nokia IPSO -käyttöjärjestelmän päälle, jonka jälkeen palomuurilaite on käyttövalmis. (Check Point 2012)

Check Point -palomuurien hallintapalvelimen ohjelmistona käytetään SmartCenter-ohjelmaa, joka säilyttää ja välittää palomuurisäännöt ja asetukset halutulle palomuurille. Palomuurisäännöt luodaan työasemalla Check Point Smartdashboard -ohjelmalla, joka lähettää tehdyt muutokset hallintapalvelimelle. Smartdashboard-ohjelman (kuvio 3) avulla voidaan määrittää palomuurille erilaisia asetuksia, kuten palomuurisäännöt, VPN-yhteydet, verkko-objektit ja NAT-asetukset. Keskitetty hallintapalvelin auttaa palomuurien ylläpidossa, kun palomuureja on useita kappaleita. (Check Point 2012)



KUVIO 3 SmartDashboard-ohjelman päänäkymä (Check Point 2010)

4 SEURAAVAN SUKUPOLVEN PALOMUURIT

Tavalliset palomuurit toimivat IP-osoitteiden, porttien ja protokollien mukaan joko estäen liikenteen tai päästäen liikenteen läpi. Tavallinen palomuuri tutkii IP-paketin otsikoita ja tulkitsee verkkoliikenteen esimerkiksi HTTP-liikenteeksi (TCP (Transmission Control Protocol) portti 80) tai SMTP-liikenteeksi (Simple Mail Transfer Protocol) (TCP portti 25). Useimmat palomuurit ovat konfiguroitu toimimaan niin, että luotetusta sisäverkosta sallitaan yhteydet epäluotettuun ulkoverkkoon, ellei liikennettä erikseen estetä palomuurisäännöllä. Tilalliset palomuurit luovat väliaikaisia sääntöjä, jotka sallivat yhteydenmuodostuksen jälkeen paketteja epäluotettavasta verkosta luotettuun verkkoon. (Miller 2011, 6-7.)

Tavalliset palomuurit toimivat hyvin, jos kaikki pelaavat sääntöjen mukaan, mutta Internetin käyttäjistä kaikki eivät kuitenkaan ole hyväntahtoisia. Nykyään Internetissä on monia uuden sukupolven Web 2.0 Internet-ohjelmia yksityiseen ja yritysten käyttöön. Monet ohjelmat ovat hyödyllisiä yrityksen toiminnan kannalle, mutta osa voi vain kuormittaa verkkoa ja altistaa tietoturvauhkille. Esimerkkejä Web 2.0 -ohjelmista ovat SharePoint, Facebook, YouTube, Skype ja Twitter. (Miller 2011, 7, 13.)

Nykyään tietovuodot ovat yleisiä. Tietovuodoissa leviää yleensä organisaation arkaluontoista tai yksityistä tietoa esimerkiksi luottokorttien numeroita sekä sosiaaliturvatunnuksia. Tietovuotoja vastaan on tehty erilaisia DLP-ohjelmistoja (Data Leakage Prevention), joilla voidaan estää tietovuotojen tapahtumista. DLP-ohjelmistot ovat kuitenkin liioiteltuja turvajärjestelmiä monille pienemmille yrityksille ja maksavat todella paljon. Perinteiset palomuurit eivät pysty estämään tietovuotojen tapahtumista, sillä ne ovat tiedottomia ohjelmista, käyttäjistä ja datan sisällöstä. (Miller 2011, 8-9.)

Hyökkäykset OSI-tason seitsemänteen kerrokseen (application layer) ovat yleistyneet, joten tällaiset hyökkäykset olisi tärkeä tunnistaa. Ohjelmia ei voida enää tunnistaa käytettävän portin ja protokollan mukaan, sillä ohjelmat osaavat piilottaa itsensä erilaisten tekniikoiden avulla. Tavalliset palomuurit eivät siis varmasti

tiedä minkä ohjelman liikenne kulkee palomuurin läpi. Yleisimpiä piiloutumistekniikoita ovat:

- porttihyppely, jossa porttia tai protokollaa vaihdetaan satunnaisesti yhteyden aikana
- epästandardien porttien käyttö, kuten Yahoo! Messengerin käyttäminen TCP portin 80 (HTTP) kautta alkuperäisen TCP portin 5050 sijaan
- tunnelointi
- piilottaminen liikenne SSL-salauksella (Secure Socket Layer)

(Miller 2011, 17,21.)

Mitä tapahtui tavalliselle palomuurille? Internet pakotti luomaan palomuureihin uuden sukupolven. Yritysten WWW-liikenteestä on tyypillisesti 20–30% SSL-suojattua liikennettä, jonka sisällä voidaan kuljettaa erilaisten ohjelmien liikennettä ilman, että palomuuri tunnistaa sitä haitalliseksi. Haittaohjelmat eivät pelaa enää sääntöjen mukaan vaan ujuttavat itsensä sisään palomuurin läpi erilaisia piiloutumistekniikoita käyttäen. Tavalliset palomuurit ovat siis tulleet sokeiksi uusille Internetiä käyttäville ohjelmille. Tavallisiin palomuureihin on kehitetty erilaisia DPI-ominaisuuksia (Deep Packet Inspection), joiden avulla voidaan tutkia IP-paketteja tarkemmin. DPI-ominaisuudet ovat kuitenkin epäkäytännöllisiä, sillä kaikkia tarpeellisia IP-paketteja ei pystytä tutkimaan tarkemmin. DPI:n käyttö kuormittaa myös palomuurin prosessoria ja muistia.(Miller 2011, 26, 29.)

4.1 Seuraavan sukupolven palomuurin toimintaperiaate

Seuraavan sukupolven palomuurin tulisi suoriutua seuraavista toiminnoista:

- tunnistaa ohjelmat riippumatta käytettävästä portista, protokollasta, piiloutumistekniikasta tai SSL-salauksesta
- mahdollistaa ohjelmien hallinta yksilöllisesti palomuurisäännöillä
- tunnistaa käyttäjät ja käyttää tunnistetietoja palomuurisäännöissä
- tarjota laajaa reaaliaikaista suojausta myös sovelluskerroksella
- yhtenäistää perinteisen palomuurin toiminta ja tunkeutumisenestojärjestelmä.

(Miller 2011, 36.)

Ohjelmien tunnistaminen seuraavan sukupolven palomuurissa tapahtuu useita eri tekijöitä tutkimalla. Yksi tapa tunnistaa ohjelma on tunnistaa käytettävä protokolla ja purkaa datapaketit. Jos käytetään SSL-suojausta, pitää datapaketin sisältö purkaa, jotta paketti voidaan tutkia tarkemmin. Liikenne salataan uudelleen, kun ohjelma on tunnistettu. Toinen tapa tunnistaa ohjelma, on purkaa protokolla, jotta voidaan tarkastaa käyttääkö ohjelma ”oikeaa protokollaa” vai onko se tunneloitunut jonkin toisen protokollan sisään. Kolmas tapa on tutkia pakettien tunnisteita, joiden avulla voidaan tunnistaa esimerkiksi pikaviestinistunnossa tapahtuva tiedonsiirto. Neljäs tapa on heuristiikka, jonka avulla voidaan tunnistaa esimerkiksi P2P- (peer-to-peer) tai VoIP-ohjelmia (Voice Over IP), jotka käyttävät omaa salaustapaansa. (Miller 2011, 37-38.)

Käyttäjien tunnistaminen yhdistää IP-osoitteen tiettyyn käyttäjään, jonka avulla voidaan hallita verkkoliikennettä käyttäjän perusteella. Käyttäjien tunnistaminen yhdistetään LDAP-hakemistojen (Lightweight Directory Access Protocol), kuten Microsoft AD:n (Active Directory) kanssa. LDAP-hakemisto tarkastaa käyttäjän ja IP-osoitteen suhteen tietyin väliajoin esimerkiksi tarkkailemalla verkkoon kirjautumisia. Käyttäjien tunnistaminen helpottaa IT-osaston toimintaa, sillä palomuurisääntöjä voidaan nyt tehdä tietyn käyttäjäryhmän mukaan. Käyttäjäryhmälle voidaan sallia esimerkiksi jonkin sosiaalisen median käyttö, vaikka muille sosiaalinen media estetään. (Miller 2011, 39.)

Verkkoliikenteen sisällön tunnistamisella voidaan estää reaaliaikaisesti haittaohjelmien pääsy yrityksen sisäverkkoon. Palomuuri tutkii datavirtojen sisältöä ja etsii uhkia tunnisteiden mukaan. Palomuuri voi myös tutkia siirrettävän tiedoston ilman, että se lataa koko tiedoston ensin omaan muistiinsa ja tarkastaa tiedoston vasta sitten. Jatkuvan skannauksen avulla maksimoidaan tiedonsiirtonopeus ja saavutetaan pienin viive. Seuraavan sukupolven palomuurit pystyvät myös tutkimaan ja estämään liikennettä sisällön mukaan. Tiedostopäätteen lisäksi palomuuri voi tutkia paketin sisältä tiettyjä datavirtoja, kuten luottokortin numeroita, ja estää näiden tietojen pääsy ulkoverkkoon. Sisällön tunnistamisen avulla IT-osasto pystyy estämään uhkia, vähentämään Internetin sopimatonta käyttöä ja ehkäisemään tietovuotoja. (Miller 2011, 40-41.)

Seuraavan sukupolven palomuuriin voidaan tehdä palomuurisääntöjä perustuen käyttäjien ja verkkoliikenteen tunnistamiseen. Esimerkkiominaisuuksia palomuurisääntöihin ovat:

- salli tai estä liikenne
- salli liikenne mutta tutki haittaohjelmilta, viruksilta ja muilta uhilta
- salli liikenne aikataulun, käyttäjän tai käyttäjäryhmän mukaan
- pura liikenteen salaus ja tutki sisältö
- liikennevirtojen hallinta QoS:n (Quality of Service) mukaan
- salli ohjelman tietyt toimenpiteet
- mikä vain yllä olevien yhdistelmä.

(Miller 2011, 42.)

4.2 Palo Alto -palomuurit

Palo Alto Networks on Yhdysvaltalainen seuraavan sukupolven palomuurien valmistaja. Palo Alto -palomuurien ominaisuuksiin kuuluvat palomuurisääntöjen luominen liikennöivän ohjelman, käyttäjän ja sisällön mukaan. Palo Alto -palomuurit jaetaan viiteen eri sarjaan:

- PA-200 – pienille toimistoille
- PA-500 – keskikokoisille ja suurille toimistoille
- PA-2000 – isoille toimistoille ja keskikokoisille yrityksille
- PA-4000 – suurille yrityksille
- PA-5000 – palveluntarjoajille ja suurille datakeskuksille.

(Palo Alto Networks 2012)

Palo Alto PA-4020 on tarkoitettu suurille yrityksille. Palomuurin tiedonsiirtonopeus on 2 Gbps ohjelmientunnistusominaisuus päällä. Palomuurin tiedonsiirtonopeus IPSec VPN -yhteyksille on 1 Gbps. PA-4020 pystyy käsittelemään 500 000 samanaikaista yhteyttä ja 60 000 uutta yhteyttä sekunnissa. Palomuuriin pystytään lisäämään 2000 VPN-tunnelia ja 20 virtuaalireitintä. (Palo Alto Networks 2012.)

Palo Alto PA-2050 on tarkoitettu keskisuurille yrityksille ja palomuurin tiedonsiirtonopeus on 1 Gbps ohjelmientunnistusominaisuus päällä. Tiedonsiirtonopeus IPSec VPN -yhteyksille on 300 Mbps. PA-2050 pystyy käsittelemään 250 000 samanaikaista yhteyttä ja 15 000 uutta yhteyttä sekunnissa. VPN-tunneleita palomuuriin voidaan määritellä 2000 ja virtuaalireitittimiä 10. (Palo Alto Networks 2012.)

Palo Alto PA-500 on tarkoitettu keskikokoisille ja suurille toimistoille. Palomuurin tiedonsiirtonopeus on 250 Mbps ohjelmientunnistus päällä ja 50 Mbps IPSec VPN -yhteyksille. Palomuuri pystyy käsittelemään 64 000 samanaikaista yhteyttä ja 7500 uutta yhteyttä sekunnissa. Palomuuriin voidaan lisätä 250 VPN-tunnelia ja 3 virtuaalireititintä. (Palo Alto Networks 2012.)

Palo Alto Networks:n kehittämät palomuurit sisältävät useita ominaisuuksia, kuten SSL-VPN (Secure Socket Layer Virtual Private Network), HA (High Availability) ja GlobalProtect. SSL-VPN on virtuaalinen lähiverkkoyhteys, jossa yhteys salataan joko IPSec- (IP Security Architecture) tai SSL-protokollalla. VPN-yhteys luodaan työasemalta VPN-asiakasohjelman avulla, jonka jälkeen käyttäjä tunnistautuu palomuurille käyttäjätunnuksen ja salasanan avulla. HA on ominaisuus, jonka avulla palomuurilaitteet voidaan kahdentaa. HA:n avulla toinen palomuureista voi menettää toimintakykynsä ilman, että verkon toiminta häiriintyy. GlobalProtect on Palo Alto Networks:n kehittämä ominaisuus, jonka avulla kotona tai työmatkalla oleva työntekijä voi kuljettaa kaiken verkkoliikenteensä yrityksen palomuurin kautta. Käyttäjä voidaan siis suojata yrityksen palomuurin avulla ilman, että käyttäjä ja työasema ovat yrityksen toimitiloissa tai sisäverkossa. (Palo Alto Networks 2011d, 61, 245, 257.)

5 PALO ALTO PALOMUURIEN HALLINTA

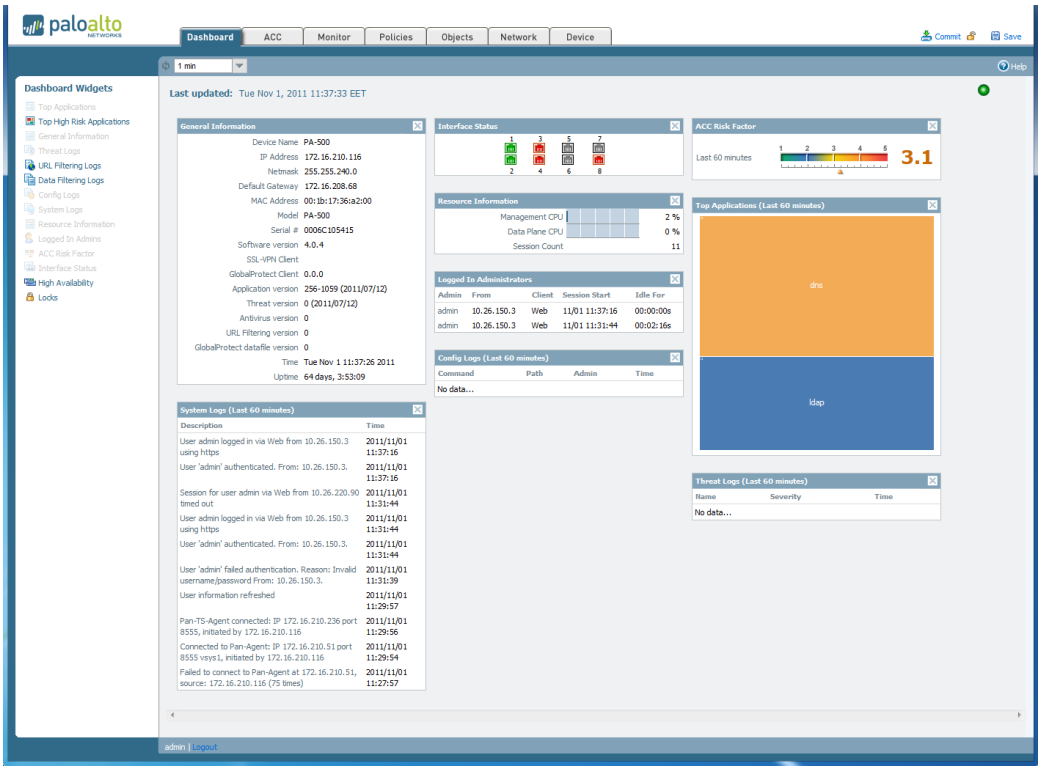
5.1 CLI

Palo Alto -palomuurin komentorivi, eli CLI (Command Line Interface) on merkkipohjainen hallintanäkymä. CLI toimii kahdessa erilaisessa tilassa: Toimintatila (operational mode) ja asetustila (configuration mode). Merkkipohjaiseen hallintaan päästään esimerkiksi sarjalinkkiyhteydellä tai SSH-yhteydellä. Kirjautumisen jälkeen oletustilana on toimintatila, jossa voidaan tutkia palomuurin tilaa ja lokia. Toimintatilassa ei voi tehdä muutoksia asetuksiin. Asetustilaan päästään antamalla toimintatilassa komento *configure*, minkä jälkeen palomuuriin voidaan tehdä muutoksia. Muutokset ajetaan palomuuriin komennolla *commit* ja tallennetaan komennolla *save*. Tallentamattomat asetukset nollautuvat palomuurin uudelleenkäynnistyksen yhteydessä. CLI on laajin ja monipuolisin työkalu palomuurin hallintaan. (Palo Alto Networks 2011a, 15-16, 21.)

Alla muutama esimerkki CLI-komennoista:
admin@paloalto# rename zone dmz to dmz1 muuttaa verkkoalueen dmz nimeksi dmz1 (asetustila).
admin@paloalto> show system info tulostaa näytölle järjestelmätiedot (toimintatila).

5.2 Web-hallinta

Palo Alto -palomuurin Web-hallinta on hyvä vaihtoehto, jos hallittavia palomuureja on vähän. Web-hallinnan kautta voidaan tehdä palomuurin ylläpidon kannalta kaikki tarvittavat asetukset, kuten palomuurisäännöt, NAT-asetukset, verkkoobjektit ja VPN-yhteydet. Web-hallinta ei vaadi erillistä hallintasovellusta, vaan hallinta toimii suoraa Internet-selaimen kautta. Yksinkertaisen graafisen käyttöliittymän ansiosta palomuurin hallinta on helppoa ja merkkipohjaista CLI:tä ei välttämättä tarvita kuin vikatilanteiden selvittämisessä. Kuviossa 4 on esitetty Web-hallintanäkymän etusivu.



KUVIO 4 Palo Alto -palomuurin Web-hallintanäkymä

5.3 Panorama

Panorama on hallintapalvelinohjelmisto Palo Alto -palomuurien hallintaan. Panorama toimitetaan virtuaalijärjestelmänä VMWare-levykuvana, joten hallintapalvelinohjelmistoa voidaan ajaa useissa eri käyttöjärjestelmissä.

Panoraman käyttöliittymä muistuttaa Palo Alto -palomuurien Web-hallintanäkymää, joten siirtyminen keskittyneeseen hallintajärjestelmään on helppoa. Palomuurilaitteet lisätään Panoramaan sarjanumeron ja IP-osoitteen perusteella, minkä jälkeen lisättyä palomuuria voidaan hallinta hallintapalvelimen kautta. Panorama mahdollistaa sääntöjen luomisen useille palomuureille samaan aikaan. (Palo Alto Networks 2011b.)

5.4 MigrationTool OS

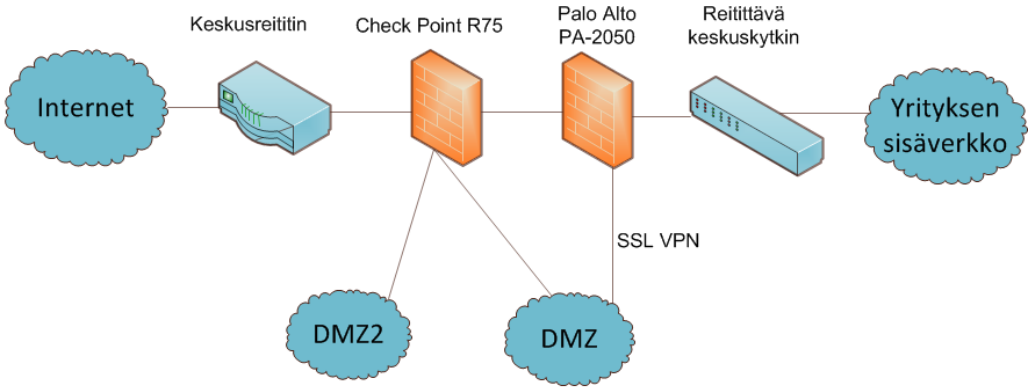
MigrationTool OS on Palo Alto Networks:n kehittämä työkalu, jonka avulla voidaan siirtää verkko-objektit, palvelut ja palomuurisäännöt Cisco PIX/ASA/FWSM, Juniper ScreenOS ja Check Point palomuureista Palo Alto -palomuureihin. MigrationTool OS toimitetaan VMWare-levykuvana, joka sisältää Linux-käyttöjärjestelmän Apache-palvelinohjelmistolla.

MigrationTool OS -työkalu on web 2.0 -ohjelma, joten työkalua käytetään Internet-selaimen kautta. Työkalu kääntää palomuurin asetukset XML-muotoon, joka voidaan ladata Palo Alto -palomuurin asetustiedostoksi. MigrationTool OS ei siirrä NAT-asetuksia, eikä verkkoliityntöjen asetuksia. (Palo Alto Networks 2011c.)

6 SEURAAVAN SUKUPOLVEN PALOMUURIN KÄYTTÖÖNOTTO

6.1 Tietoliikenneverkon rakenne

Lahti Energia Oy:n tietoliikenneverkon rakenne oli varsin tyypillinen yritysverkoille. Julkisen verkon palveluntarjoajan, eli ISP:n (Internet Service Provider), kaapeli oli kytketty yrityksen pääreitittimeen, josta yhteys eteni yritysverkon palomuuriin. Yritysverkon palomuurina toimi Check Point R75 -palomuuri, josta yhteys jakaantui kahteen DMZ-verkkoon (Demilitarized Zone) ja yrityksen sisäverkkoon. Työn aloitushetkellä Check Point -palomuurin ja keskuskytkimen välissä oli myös Palo Alto -palomuuri (PA-2050), jonka kautta kulkivat vain SSL-VPN -yhteydet. Lahti Energia Oy:n verkkotopologia on esitetty kuviossa 5.



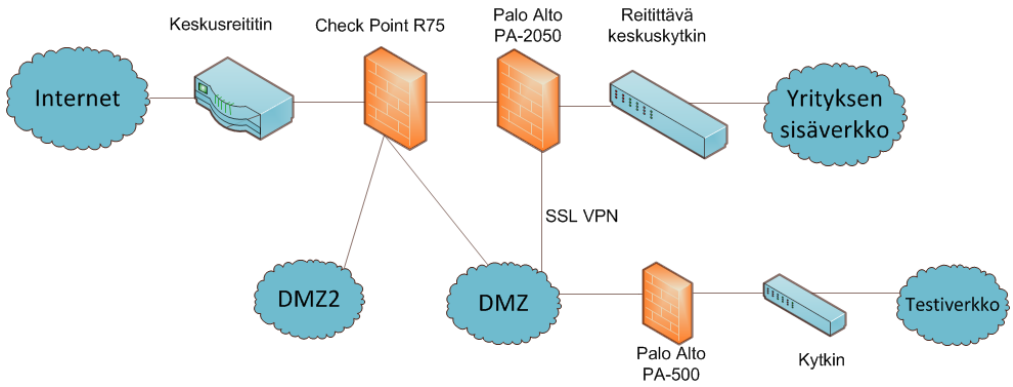
KUVIO 5 Lahti Energia Oy:n verkkotopologia

Testiympäristöä varten verkkoon tulisi kytkeä uusi Palo Alto PA-500 -palomuuri, jonka ulkoverkon liityntä olisi DMZ-alueella ja testiverkon luotettava sisäverkko erillään Lahti Energia Oy:n omasta sisäverkosta. Testiverkon Palo Alto PA-500 -palomuuriin tehtäisiin samat palomuurisäännöt kuin yritysverkon Check Point R75 -palomuurissa, joten lopputuloksena olisivat toimintatavaltaan lähes identtiset palomuurilaitteet. Palo Alto -palomuurien asetustiedostoja voitiin vaihtaa laitteesta toiseen, joten PA-500 palomuuriin tehdyt säännöt ja määritykset oli mahdollista ottaa myöhemmin käyttöön yrityksen pääpalomuurissa (Palo Alto PA-2050).

6.2 Palomuurilaitteen esiasennus

Palomuurin asentaminen aloitettiin sijoittamalla uusi palomuurilaite laitetilaan. Palomuuri sijoitettiin samaan laitekaappiin vanhan Check Point -palomuurin, pääreitittimen ja keskuskytkimen kanssa. Laitekaapissa oli valmiina sähköpistoke palomuurilaitteelle, ja tietoliikenneyhteydet ulkoverkkoon saatiin ethernet-kaapelilla. Tämän jälkeen palomuurin ympärille aloitettiin luoda laboratorioympäristöä, jossa voitaisiin konfiguroida ja testata palomuurilaitetta.

Laboratorioympäristöä varten palomuurista kytkettiin yksi ethernet-liitäntä kytkimeen ja yksi Internetiin. Internet-liityntä saatiin kytkemällä palomuurin ethernet-liitin yrityksen DMZ-verkkoon. Kytkimeen tuleva liitäntä edusti yrityksen luotettavaa sisäverkkoa ja Internet epäluotettavaa ulkoverkkoa. Palomuurin hallinta-liitäntä kytkettiin myös samaan verkkoon sisäverkon kanssa, jotta kytkimeen liitettävillä työasemilla voitiin konfiguroida palomuurin asetuksia. Laboratioympäristö oli nyt valmis, ja laitteeseen asetettiin virrat päälle. Uusi verkkotopologia on esitetty kuviossa 6.



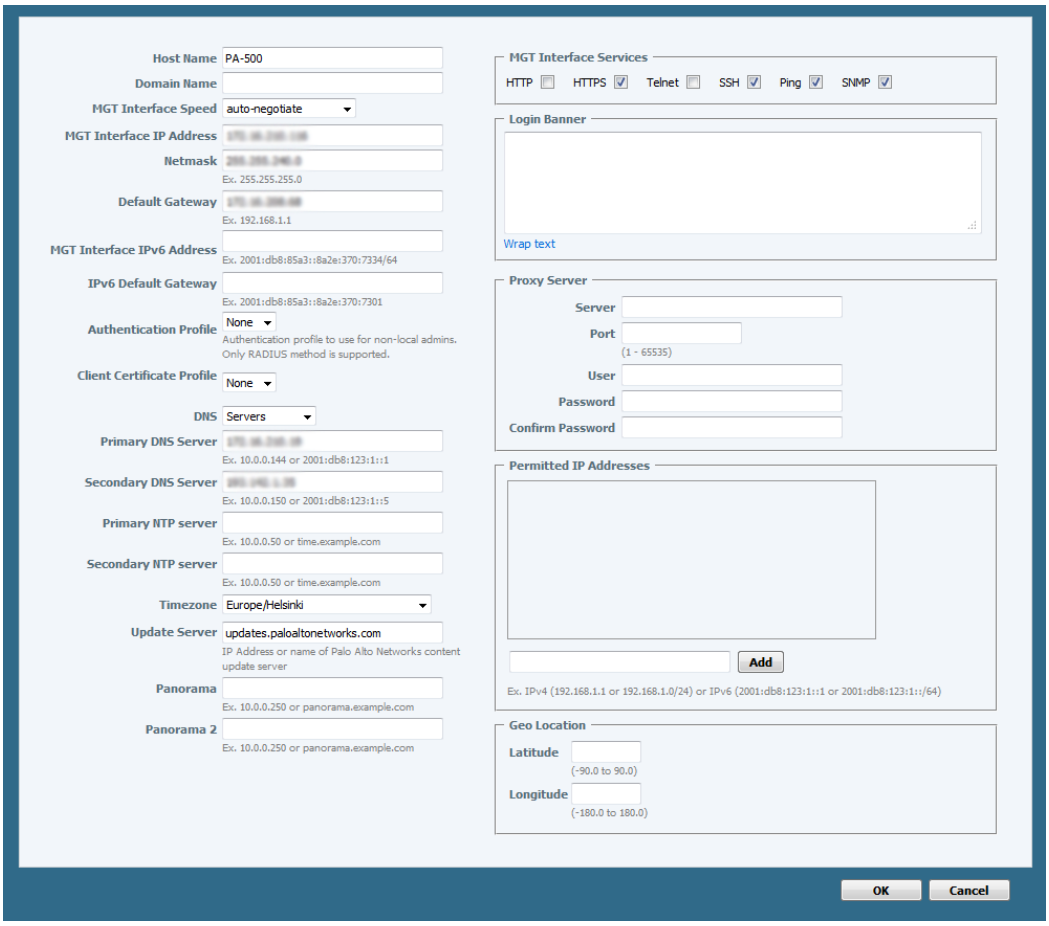
KUVIO 6 Testiverkon sijoittaminen

Ensimmäisen käynnistyksen yhteydessä Palo Alto -palomuuri tulisi rekisteröidä Palo Alto Networks:n kotisivuilla, jotta palomuuriin saataisiin viimeisin ohjelmistoversio, ohjelmatunnisteiden päivitykset ja tuki. Toimittaja oli rekisteröinyt valmiiksi palomuurin, joten päivitykset olivat heti saatavilla. Palo Alto -palomuurin hallintaa varten täytyi hallitsevan työaseman IP-osoitteeksi määritellä jokin 192.168.1.0/24 verkon IP-osoite. IP-osoitteeksi valittiin 192.168.1.2, jolla voitiin

yhdistää internet-selaimella palomuurin hallintaliitynnän IP-osoitteeseen https://192.168.1.1. Selaimeen aukesi kirjautumisikkuna, johon syötettiin käyttäjätunnukseksi ja salasanaksi admin. Kirjautumisen jälkeen selaimeen aukesi palomuurilaitteen yleisnäkymä, jossa esitettiin palomuurin perusasetukset, tiedot ja laitteistoloki.

Ensimmäiseksi palomuuriin määritettiin verkkoasetukset hallintaliitynnälle. Yleisnäkymässä valittiin päävalikosta Device-välilehti, jonka alta valittiin Setup-osio. Setup-osiossa voitiin muokata halutut asetukset hallintaliitynälle. Asetussivu on esitetty kuviossa 7. Asetuksiksi asetettiin seuraavat määritteet:

- isäntänimi: PA-500
- hallintaliitynnän nopeus: automaattinen
- hallintaliitynnän IP-osoite: xxx.xxx.xxx.xxx
- aliverkon peite: xxx.xxx.xxx.xxx
- oletusyhdyskäytävä: xxx.xxx.xxx.xxx
- ensisijainen DNS-palvelin (Domain Name System): xxx.xxx.xxx.xxx
- toissijainen DNS-palvelin: xxx.xxx.xxx.xxx
- aikavyöhyke: Eurooppa/Helsinki
- päivityspalvelin: updates.paloaltonetworks.com
- hallintaliitynnän palvelut: HTTPS (Hypertext Transfer Protocol Secure), SSH, Ping, SNMP (Simple Network Management Protocol).



KUVIO 7 Palo Alto -palomuurin asetussivu

Palomuurin perusasetukset ajettiin laitteeseen painamalla hallintasivulta Commit -painiketta. Palomuurin hallinta-IP-osoite muuttui, joten seuraavalla kerralla Web-hallintaan päästiin osoitteella https:// xxx.xxx.xxx.xxx. Palomuurilla oli tämän jälkeen myös yhteys Internetiin, joten palomuurilaitteen ohjelmisto ja ohjelma-tunnisteet voitiin päivittää.

6.3 Ohjelmistopäivitys

Ohjelmistopäivitysten avulla taattiin, että palomuurin tietoturva ja suorituskyky ovat ajan tasalla. Uusia päivityksiä julkaistiin useita kertoja vuodessa, joten palo-muurin päivittäminen ja uuden version testaaminen täytyi ottaa yrityksen IT-osastolla huomioon. Palo Alto -palomuurin ohjelmistopäivitys tapahtui Device-

välilehden alta löytyvästä Software-osiosta. Software-osio listasi mahdolliset ohjelmistoversiot, jotka laitteeseen voitiin asentaa tai ladata. Uusien ohjelmistoversioiden lataus tapahtui painamalla halutun versionumeron kohdalle Download -painiketta.

Palomuuri toimitettiin ohjelmistoversiolla 3.1.4, joten palomuuri päivitettiin uudempaan 4.0.3 versioon. Ohjelmistoversiota 4.0.3 ei pystynyt asentamaan suoraan, vaan uudempi versio vaati vanhemman 4.0.1 version asennettavan ensin. Päivitys aloitettiin painamalla versionumeron 4.0.1 kohdalla Download.

Latauksen valmistuttua latausohjelma esitti yhteenvedon latauksen onnistumisesta. Yhteenveto ilmoitti mahdollisista latauksen aikaisista häiriöistä ja uuden ohjelmistopäivityksen tuonnista ohjelmistohallintaan. Tämän jälkeen uuden ohjelmistopäivityksen asennus voitiin käynnistää painamalla oikean versionumeron kohdalla Install. Ohjelmistopäivityksen asennuksen aikana palomuuri näytti tietoja päivityksen edistymisestä ja lopuksi ilmoitti päivityksen onnistuneen. Palomuurilaite piti käynnistää uudelleen, jotta ohjelmistopäivitys tulisi voimaan.

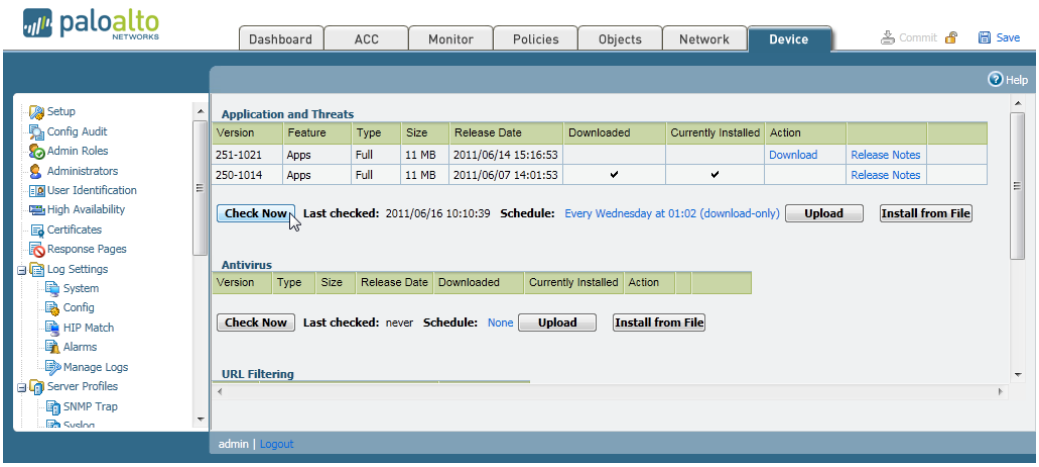
Palomuurin päivityshetkellä uusimman versionumeron 4.0.3 lataaminen ei onnistunut suoraan ohjelmistohallinnan kautta, vaan ohjelmistopäivitys piti tuoda manuaalisesti. Päivitystiedoston pystyi lataamaan Palo Alto Networks:n tukisivustolta ja tuomaan ohjelmistohallintaan painamalla Upload-painiketta. Päivitysohjelma kysyi polkua, josta päivitystiedosto ladataan. Browse-painikkeella päästiin valitsemaan Palo Alto Networks:n tukisivuilta ladattu päivitystiedosto.

Uusimman 4.0.3 version asennus aloitettiin painamalla Install From File -painiketta ja valitsemalla haluttu ohjelmistoversio alasvetovalikosta. Palomuuri asensi päivitetyn ohjelmiston ja otti sen käyttöön uudelleenkäynnistyksen yhteydessä. Päivityksen valmistuttua palomuuri käynnistettiin uudelleen. Palomuurissa oli nyt uusin ohjelmistoversio ja seuraavaksi voitiin siirtyä ohjelmatunnisteiden päivittämiseen.

6.4 Ohjelmatunnisteiden päivitys

Palo Alto -palomuurin ohjelmatunnisteet voitiin päivittää Device-välilehden Dynamic-Updates -osiosta. Ohjelmatunnisteiden päivittämisellä taattiin, että palomuurisäännöissä käytettävät ohjelmat ovat ajan tasalla. Ohjelmatunnisteiden päivityksen mukana tuli usein myös kokonaan uusia ohjelmia, joita voitiin hyödyntää palomuurisäännöissä.

Päivitys aloitettiin etsimällä saatavilla olevat päivitykset (kuvio 8). Päivitysohjelma latasi päivitetyn ohjelmatunnistetiedoston palomuurilaitteeseen, joka asennettiin painamalla latauksen jälkeen Install-painiketta. Asennus kesti muutamia minuutteja ja uudet ohjelmatunnisteet olivat heti käytettävissä. Palomuurilaitetta ei tarvinnut käynnistää uudelleen päivityksen jälkeen. Ohjelmatunnisteiden päivitys eteni hyvin samalla tavalla kuin ohjelmistopäivitys luvussa 6.1.



KUVIO 8 Ohjelmatunnisteiden päivitykset

6.5 Verkkoalueiden määrittäminen

Ennen verkkoliityntöjen määrittelemistä määritettiin palomuurissa käytettävät verkkoalueet, eli zonet. Lahti Energia Oy:n verkkoon määriteltiin viisi erilaista verkkoaluetta, jotka olivat DMZ, DMZ_2, External, Internal ja site-to-site. DMZ ja DMZ_2 olivat demilitarisoituja alueita, joissa sijaitsivat yrityksen palvelimia

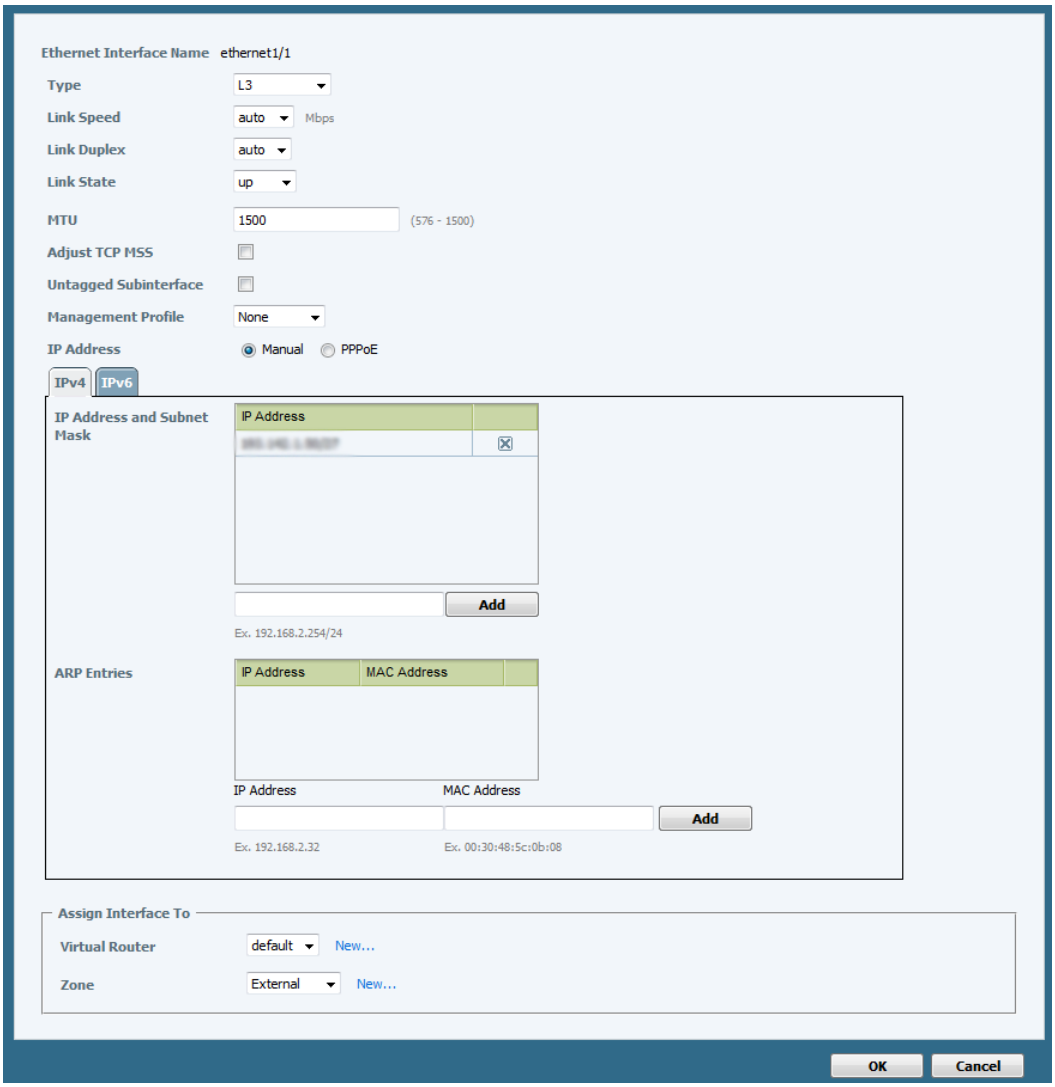
julkisilla IP-osoitteilla. External oli ulkoverkon alue (Internet), Internal luotetun sisäverkon alue ja site-to-site VPN-yhteyksien verkkoalue.

Verkkoalueet lisättiin palomuurin Web-hallinnan Network-välilehden Zones-osiossa painamalla New -painiketta. Uuden verkkoalueen määrittelyihin annettiin verkkoalueen nimi, tyyppi ja siihen liitettävät verkkoliitynnät. Asettamalla Enable User Identification -määrite aktiiviseksi voitiin verkkoalueessa käyttää käyttäjäntunnistusta. Käyttäjäntunnistus otettiin käyttöön verkkoalueessa Internal, joten sisäverkosta liikennöiville käyttäjille voitiin tehdä käyttäjäkohtaisia palomuurisääntöjä.

6.6 Verkkoliityntöjen määrittäminen

Palomuurissa olevat verkkoliitynnät voitiin konfiguroida Web-hallinnan Network -välilehden Interfaces-osiosta. Interfaces-osio listasi kaikki käytettävissä olevat verkkoliitynnät ja niiden ominaisuudet. Listasta nähtiin linkin tilan, liitynnän IP-osoite, käytettävä virtuaalireititin ja verkkoalue, johon verkkoliityntä kuului. Verkkoliityntää pääsi konfiguroimaan painamalla verkkoliitynnän nimeä. Verkkoliitynnän asetuksissa määritettiin liitynnän tyyppi, linkin nopeus, duplex, linkin tila, MTU:n (Maximun Transmission Unit) koko, IP-osoite, virtuaalireititin ja verkkoalue.

Verkkoliityntä ethernet1/1 valittiin ulkoverkon (Internet) liitynnäksi, joten verkkoliitynnälle määritettiin julkinen IP-osoite xxx.xxx.xxx.xxx/27. Verkkoliitynnän ethernet1/1 tyypiksi asetettiin L3 (Layer 3), linkin nopeudeksi ja duplexiksi automaattinen, linkin tila ylös, MTU:n kooksi 1500 (oletus), virtuaalireititttimeksi default ja verkkoalueeksi External. Verkkoliitynnän ethernet1/1 asetukset on esitetty kuviossa 9.



KUVIO 9 Ulkoverkon liitynnän ethernet1/1 asetukset

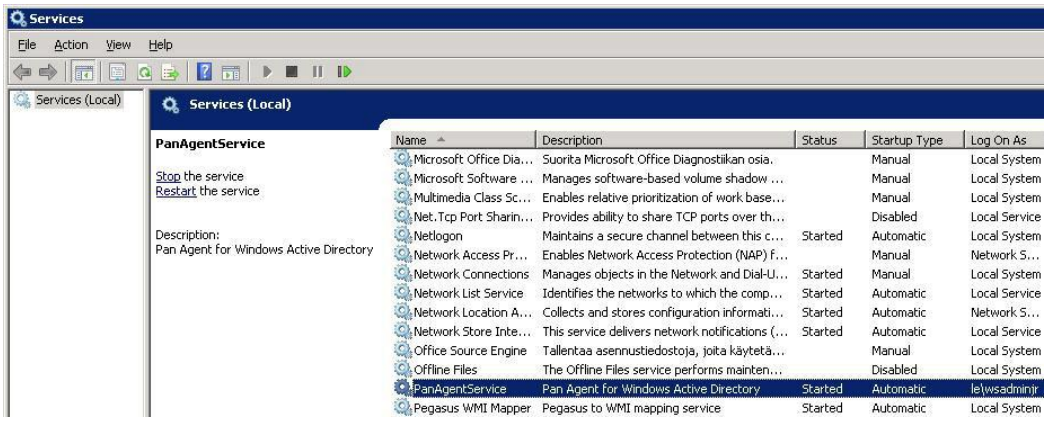
Verkkoliityntä ethernet1/2 valittiin sisäverkon liitynnäksi ja sille konfiguroitiin IP-osoite testiverkosta 192.168.0.0/24, joka oli erillään Lahti Energia Oy:n todellisesta sisäverkosta. Testiverkossa voitiin tutkia palomuurin toimintaa ja palomuurisääntöjä turvallisesti. Verkkoliitynnälle ethernet1/2 asetettiin IP-osoite 192.168.0.253/24, tyypiksi L3, linkin nopeudeksi ja duplexiksi automaattinen, linkin tila ylös, MTU:n kooksi 1500 (oletus), virtuaalireitittimeksi default ja verkkoalueeksi Internal. Kaikki tarvittavat liitynnät olivat nyt konfiguroitu testiverkkoa varten valmiiksi.

6.7 Käyttäjien tunnistaminen

6.7.1 User Identification Agent

Yksi suurimmista uudistuksista vanhaan Check Point -palomuuriin verrattuna oli verkon käyttäjien tunnistaminen ja hyödyntäminen palomuurisännöissä. Palo Alto -palomuuri pystyi tunnistamaan AD-käyttäjän Microsoft Windows -palvelimelle asennettavan tunnistusagentin (User Identification Agent) avulla. Tunnistusagentti yhdisti IP-osoitteen käyttäjään tutkimalla AD-palvelimen kirjautumislokia, lähettämällä kyselyitä pääteasemalle ja käyttämällä Captive Portal -tekniikkaa. Palomuuriin voitiin luoda sääntöjä esimerkiksi siten, että tietyllä AD:n käyttäjäryhmällä on oikeus tiettyyn verkkopalveluun. Näin ollen uuden käyttäjän salliminen verkkopalveluun ei vaatinut uutta palomuurisääntöä, vaan käyttäjä voitiin vain lisätä AD:ssa oikeaan käyttäjäryhmään. Ominaisuus yksinkertaisti palomuurisäännöstöä ja nopeutti IT-osaston toimintaa.

Lahti Energia Oy:n hallintapalvelimelle ladattiin Palo Alto Networks:n tukisivustolta tunnistusagentin asennuspaketti, joka asennettiin palvelimelle oletusasetuksilla. Ennen agentin konfigurointia varmistettiin, että agentti oli käynnissä Windows-palvelimen palveluissa vaadittavan oikeustason tunnuksilla. Agentin tarkistaminen tapahtui avaamalla hallintapalvelimella Services-työkalu, joka listasi kaikki käynnissä olevat palvelut (kuvio 10). Listalta etsittiin PanAgentService ja varmistettiin, että PanAgentService:n tila oli Started ja käynnistystyyppinä automaattinen. Properties-ikkunan Log On -välilehdellä voitiin määrittää käyttäjätunnus, jolla PanAgentService -palvelu käynnistetään. Käyttäjätunnuksen oikeustasona oli oltava vähintään Server Operator, joten käyttäjätunnukseksi valittiin henkilökohtainen AD-verkon pääkäyttäjätunnus. Tunnistusagentti voitiin nyt konfiguroida.



KUVIO 10 Hallintapalvelimen Services -työkalu

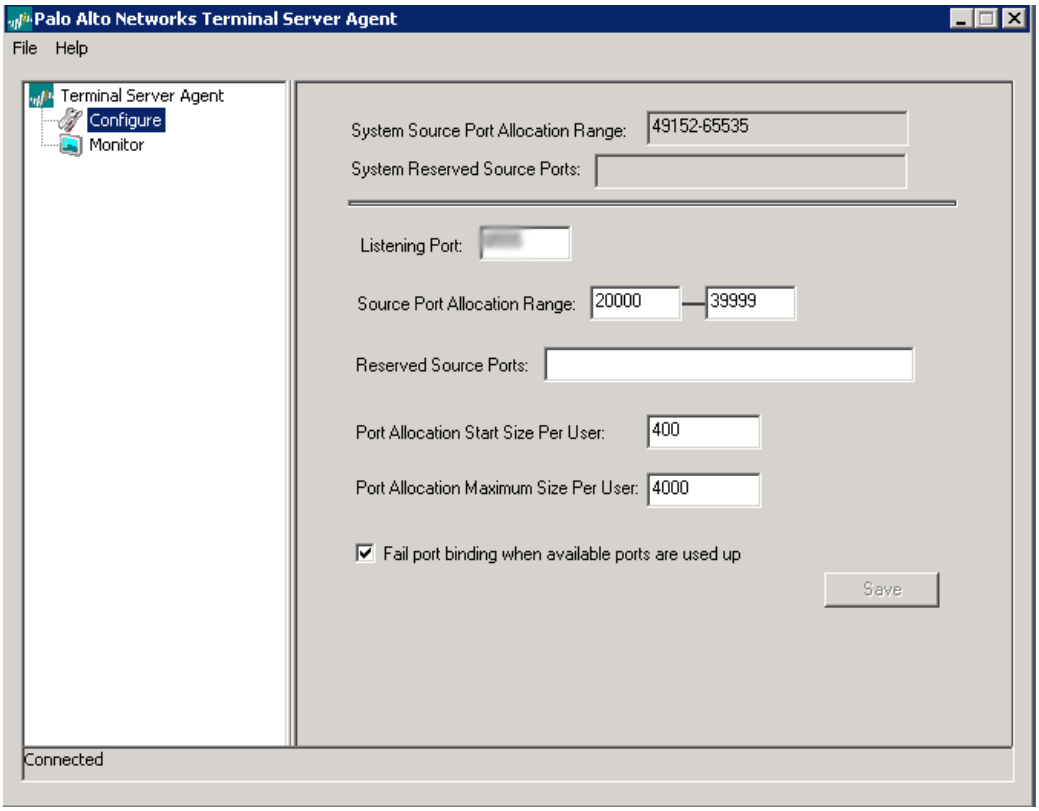
Tunnistusagentin konfigurointi tapahtui avaamalla hallintapalvelimella Palo Alto Networks User Identification Agent -ohjelma ja painamalla avautuvasta ikkunasta Configure. Asetusikkunaan määritettiin AD-toimialueen nimi, agentin porttinumero, AD-toimialueen ohjauskoneiden IP-osoitteet ja sallittu IP-avaruus. AD-toimialueen nimi Lahti Energia Oy:n verkossa oli le.konserni ja agentin porttinumerona käytettiin xxxxx. Toimialueen ohjauskoneiden IP-osoitteet olivat xxx.xxx.xxx.xxx ja xxx.xxx.xxx.xxx. Sallituksi IP-avaruudeksi määritettiin xxx.xxx.xxx.xxx/16. Työasemien käyttäjät voitiin tunnistaa, jos käyttäjän työaseman IP-osoite oli sallitusta IP-avaruudesta. Muut asetukset jätettiin oletusasetuksille.

Tunnistusagentin konfiguroinnin jälkeen määritettiin käyttäjäntunnistusasetukset palomuuriin. Palomuurin Device-välilehden User Identification -osiosta lisättiin tunnistusagentin sijainti. Palomuurille syötettiin tunnistusagentin nimeksi LE_AGENT, IP-osoitteeksi xxx.xxx.xxx.xxx ja portiksi aiemmin määritetty xxxxx.

6.7.2 Terminal Server Agent

Microsoft Windows -terminaalipalvelimilla käyttäjät voitiin tunnistaa asentamalla palvelimelle terminaaliagentti (Terminal Server Agent). Terminaaliagentti ladattiin Palo Alto Networks:n tukisivustolta Lahti Energia Oy:n terminaalipalvelimel-

le ja asennettiin oletusasetuksilla hakemistoon C:\Program Files\Palo Alto Networks\Terminal Server Agent. Terminaaliagentille määritettiin kuunteluportiksi xxxxx ja muut asetukset jätettiin oletusasetuksille. Lähdeporttien allokointialue oli 20000 – 39999, joka varattiin etäkäyttäjien istuntoja varten. Jokaiselle käyttäjälle varattiin minimissään 400 porttia ja maksimissaan 4000 porttia. Terminaaliagentin asetukset on esitetty kuviossa 11.



KUVIO 11 Terminaaliagentin asetukset

Terminaaliagentin asetukset määritettiin palomuuriin vastaavasti kuin tunnistusagentinkin. Device-välilehden User Identification -osiossa voitiin palomuuriin lisätä Terminal Server Agent -palvelun sijainti. Terminaaliagentille asetettiin nimeksi TS_AGENT, IP-osoitteeksi xxx.xxx.xxx.xxx ja portiksi xxxxx. Kaikki asetukset käyttäjien tunnistamista varten olivat nyt valmiit ja verkko-objektien luominen voitiin aloittaa.

6.8 Verkko-objektit

Verkko-objektien avulla palomuurisääntöjen luominen helpottui, sillä palomuurisäännöissä ei tarvinnut muistaa palvelimien ja laitteiden IP-osoitteita, vaan kaikki verkkolaitteet voitiin esittää objekteina. Verkko-objektien, palomuurisääntöjen ja NAT-asetusten siirtäminen olisi ollut mahdollista Palo Alto Networks MigrationTool OS -työkalulla Check Point -palomuurista Palo Alto -palomuuriin, mutta työkalun huonon saatavuuden takia kaikki asetukset tehtiin käsin. Palo Alto palomuurin verkko-objektit luotiin Web-hallinnan Objects-välilehden Addresses-osiossa. Addresses-osio listasi kaikki palomuuriin luodut verkko-objektit ja uusia objekteja voitiin luoda add-painikkeella. Verkko-objektin luonti-ikkunaan syötettiin verkko-objektin nimi, verkko-objektin kuvaus ja IP-osoite tai verkko.

Check Point -palomuurin verkko-objektit löytyivät Check Point SmartDashboard -ohjelman Network Objects -osiosta. Check Point -palomuuri eritteli verkko-objektit päätelaitteisiin (nodes) ja verkkoihin (networks). Palo Alto -palomuurissa sekä päätelaitteet että verkot lisättiin Addresses-osioon. Check Point -palomuurin verkko-objektit sisälsivät samat tiedot kuin Palo Alto -palomuurin verkko-objektit, joten tietojen kopioiminen sujui vaivatta. Verkko-objekteja oli yhteensä lähemmäs 200, joten Palo Alto Networks MigrationTool OS -työkalu olisi säästänyt käsin kopioimisessa kuluneen ajan. Verkko-objekteista kopioitiin kaikki palvelimet, verkot ja verkkolaitteet lukuun ottamatta käyttäjien työasemia. Jokaiselle työasemalle oli luotu vanhassa Check Point -palomuurissa oma verkko-objekti mutta Palo Alto -palomuurissa käyttäjäkohtaiset palomuurisäännöt luotiin käyttäjäntunnistuksen avulla.

Sekä Palo Alto -palomuuri, että Check Point -palomuuri sisälsivät molemmat osoiteryhmiä, joihin kuului yksi tai useampi verkko-objekti. Osoiteryhmät määritettiin Palo Alto -palomuurin Address Groups -osiossa ja osoiteryhmiin määritettiin sinne kuuluvat verkko-objektit osoiteryhmäikkunan Add-painikkeella. Check Point -palomuurissa osoiteryhmät sijaitsivat Groups-osiossa, josta tiedot kopioitiin käsin Palo Alto -palomuuriin. Osoiteryhmiä oli huomattavasti vähemmän kuin verkko-objekteja, joten osoiteryhmien tekoon kului vähemmän aikaa. Verkko-

objektit olivat nyt valmiit ja palomuurisäännöt voitiin kopioida Check Point -palomuurista Palo Alto -palomuuriin.

6.9 Palomuurisäännöt

Palomuurisäännöt kopioitiin käsin Check Point -palomuurista Palo Alto -palomuuriin, joten samalla pystyttiin myös karsimaan vanhat ja käyttämättömät palomuurisäännöt pois. Työ aloitettiin generoimalla Check Point -palomuurilla raportti, josta nähtiin palomuurisääntöjen osumat viimeisimmän puolen vuoden ajalta. Palomuurisääntö poistettiin automaattisesti, jos siihen ei ollut kertynyt puolen vuoden aikana yhtäkään osumaa. Poistettavia sääntöjä tuli yhteensä noin 20.

Palomuurisäännöt luotiin Palo Alto -palomuuriin Web-hallinnan Policies-välilehden Security-osiossa. Check Point -palomuurissa palomuurisäännöt sijaitsivat SmartDashboard -ohjelman Firewall-välilehdellä. Molemmissa palomuureissa palomuurisääntöjen esittämistapa oli hyvin samanlainen, joten palomuurisääntöjen kopioiminen käsin onnistui helposti. Sääntöjä oli yhteensä 240, joten palomuurisääntöjen kopioiminen oli yksi työläimmistä prosesseista. Alla esimerkki palomuurisäännöstä, joka salli ping-paketin palomuurilaitteen julkisen verkon verkkoliitynnälle:

- palomuurisäännön nimi: Firewall_ping
- tunniste: Palomuurihallinta
- lähteen verkkoalue: any
- lähteen verkko-osoite: any
- lähdekäyttäjä: any
- kohteen verkkoalue: DMZ
- kohteen verkko-osoite: FW1
- ohjelma: Ping
- palvelu: Oletus.

Uuden palomuurin käyttöönoton ensimmäisessä vaiheessa tarkoituksena oli luoda lähes identtinen palomuuri vanhan Check Point -palomuurin kanssa, joten esimer-

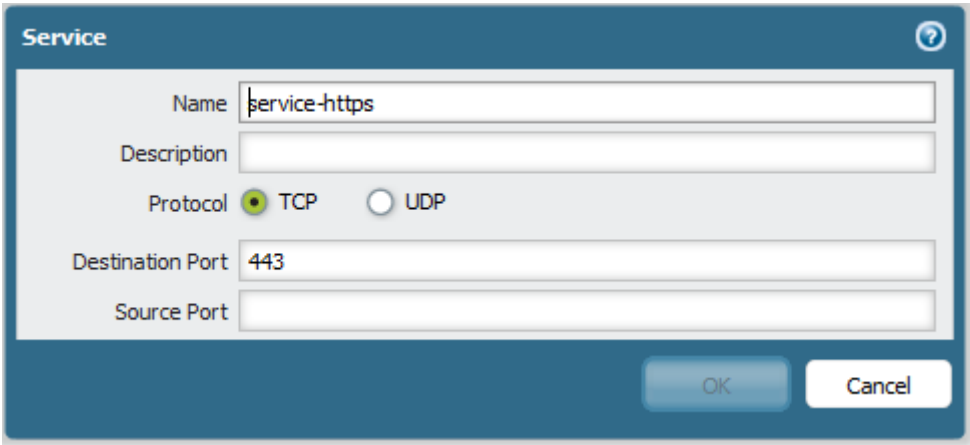
kiksi käyttäjäntunnistusta ei hyödynnetty tässä vaiheessa täysin. Käyttäjäntunnistuksen käyttöönotto olisi vaatinut paljon muutoksia AD-toimialueen käyttäjäryhmiin, joten muutokset jätettiin myöhemmäksi. Vanhassa Check Point -palomuurissa käyttäjäkohtaisia palomuurisääntöjä varten oli luotu verkko-objekti, joka oli määritetty käyttäjän työaseman mukaan. Verkko-objekti oli nimetty työaseman nimen mukaan, ja sille oli määritetty työaseman IP-osoite. Palo Alto -palomuurissa käyttäjä- ja käyttäjäryhmäkohtaiset säännöt luotiin käyttäjäntunnistuksen avulla, joten työasemista ei tehty omia verkko-objekteja. Muutos helpotti palomuurisääntöjen luontia ja käyttäjällä olivat oikeudet eri verkkopalveluihin, vaikka käyttäjä vaihtaisi työasemasta toiseen.

Lähes kaikki palomuurisäännöissä tarvittavat ohjelmat löytyivät suoraan palomuurin ohjelmatunnisteista, mutta joitakin ohjelmia lisättiin käsin. Palomuurin Web-hallinnan Objects-välilehden Applications-osiosta voitiin tarkastella palomuurista löytyviä valmiita ohjelmia ja luoda uusia ohjelmia. Uuden ohjelman luominen onnistui painamalla Add-painiketta ja syöttämällä uudelle ohjelmalle vaadittavat tiedot. Alla on esimerkki luodusta ohjelmasta:

- ohjelman nimi: rtip
- kategoria: networking
- alakategoria: general-business
- teknologia: client-server
- protokolla: TCP, UDP (User Datagram Protocol)
- portti: 771.

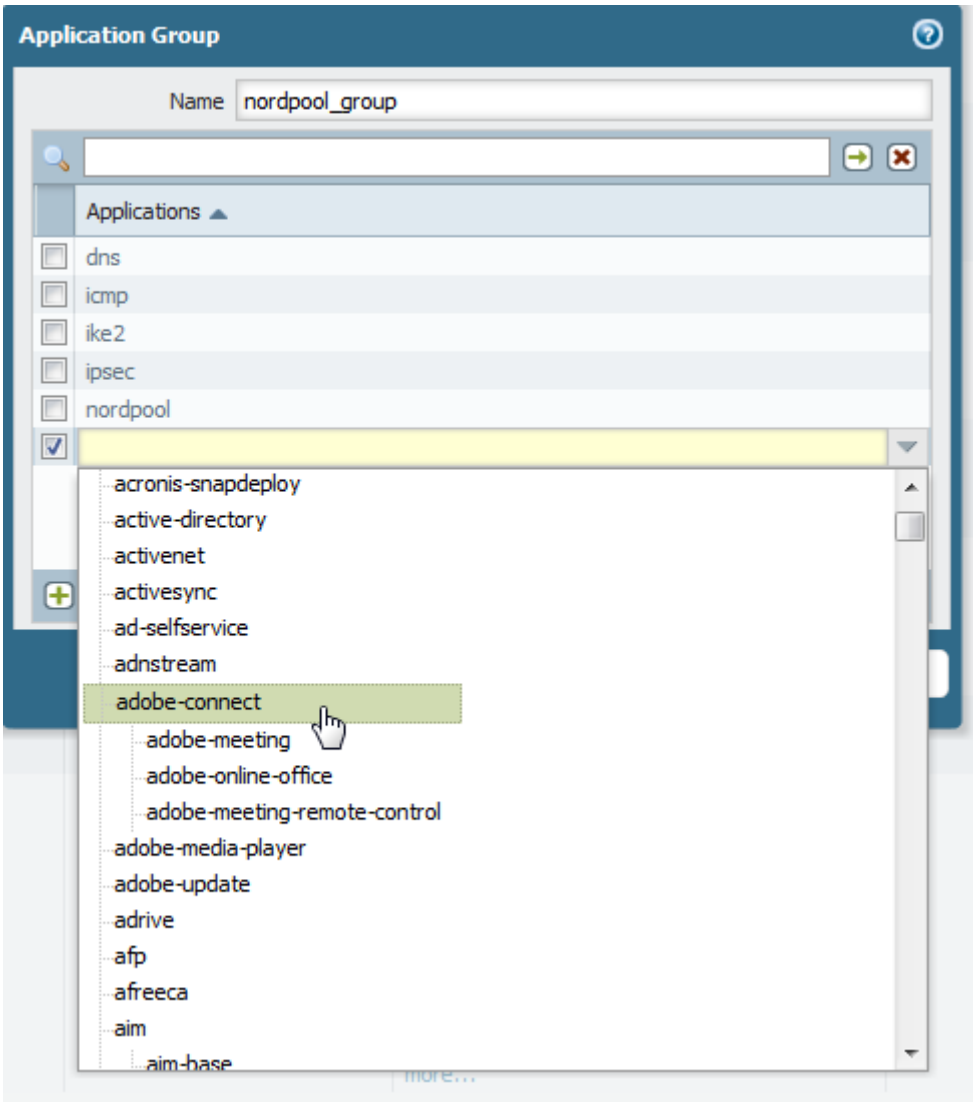
Ohjelmien lisäksi tarvittiin palveluja, joiden avulla voitiin tarkentaa palomuurisäännössä käytettävää ohjelmaa. Palveluja voitiin myös käyttää sellaisenaan ilman, että ohjelmaa määritettiin palomuurisäännössä ollenkaan. Palvelu on yksinkertaisempi kuin ohjelma, sillä palvelulle määritetään vain yksi protokolla (TCP tai UDP), sekä kohde- ja lähdeportti. Palveluja voitiin tarkastella ja luoda palomuurin Web-hallinnan Objects-välilehden Services-osiossa. Uuden palvelun luonnissa palvelulle syötettiin palvelun nimi, kuvaus, protokolla, kohde- ja lähdeportti. Kuviossa 12 on esitetty palvelu ”sevice-https”, joka käyttää TCP-

protokollaa ja kohdeporttia 443. Palvelu määrittää siis HTTPS-protokollan oletusportin.



KUVIO 12 service-https -palvelun asetukset

Palveluiden ja ohjelmien lisäksi palomuuriin määritettiin erilaisia ohjelmaryhmiä, joiden avulla voitiin nopeuttaa ja selkeyttää palomuurisääntöjen luomista. Ohjelmaryhmään voitiin lisätä useita ohjelmia, joten samoja palveluita käyttävien palomuurisääntöjen ohjelmat voitiin lisätä yhteen ohjelmaryhmään. Ohjelmaryhmiä luotiin Application Groups -osiossa syöttämällä ohjelmaryhmän nimi ja siihen kuuluvat ohjelmat. Ohjelmaryhmän luonti on esitetty kuviossa 13.



KUVIO 13 Uuden ohjelmaryhmän luonti

6.10 NAT-asetukset

NAT-säännöissä käytettiin dynaamisia ja staattisia osoitteenmuunnoksia. Dynaamisessa osoitteenmuunnoksessa useat asiakasohjelmat käyttivät samaa julkista IP-osoitetta mutta eri lähdeportin numeroa. Staattisessa osoitteenmuunnoksessa lähdeportti pysyi samana. NAT-asetuksista suurin osa oli yhteistyökumppaneille meneviä yhteyksiä varten. Sääntöjä luotiin 40 ja säännöt kopioitiin käsin Check Point -palomuurista Palo Alto -palomuuriin. Check Point -palomuurin NAT-säännöt löytyivät Check Point SmartDashboard -ohjelmiston NAT-välilehdeltä. Palo Alto -palomuuriin NAT-säännöt voitiin lisätä Policies-välilehden NAT-osiossa. Ensimmäiseksi NAT-sääntöä kokeiltiin Palo Alto -palomuurin hallintatyöasemaan. NAT-säännölle asetettiin seuraavat määritykset:

- nimi: hallintatyöasema
- lähdeverkkoalue: Internal
- kohdeverkkoalue: External
- lähdeosoite: 192.168.0.2
- kohdeosoite: any
- palvelu: any
- lähdeosoitteen muunnos: dynamic-ip-and-port, ethernet1/1, xxx.xxx.xxx.xxx/27
- kohdeosoitteen muunnos: none.

NAT-sääntö teki dynaamisen osoitteenmuunnoksen sisäverkosta ulkoverkkoon IP-osoitteella 192.168.0.2 liikennöivälle laitteelle. Osoitteenmuunnos tehdään palomuurin ethernet1/1-liitynnän IP-osoitteeseen, eli hallintatyöasema liikennöi ulkoverkossa julkisella IP-osoitteella xxx.xxx.xxx.xxx. Hallintatyöaseman NAT-säännön testaamisen jälkeen NAT-säännöt tehtiin myös muille tarvittaville verkoille ja palvelimille.

6.11 IPSec-tunnelit

Lahti Energia Oy:n yhteistyökumppaneille menevät VPN-yhteydet toteutettiin IPSec-tunneleilla. Vanhassa Check Point -palomuurissa VPN-yhteydet olivat myös luotu IPSec:ä käyttäen, joten uuteen palomuuriin lisättiin VPN-yhteydet samoja protokolloja käyttäen. VPN-yhteyksien salausmenetelmät olivat ennestään vahvoja, joten muutoksia yhteyksiin ei tarvinnut tehdä. Samojen yhteysmääritysten johdosta VPN-yhteyksien luominen oli helpompaa, sillä yhteyden luominen ei vaatinut vastapuolelta toimenpiteitä.

Check Point -palomuurin ja Palo Alto -palomuurin VPN-yhteyksien määritystavat erosivat huomattavasti toisistaan, joten yhteyksien määrittäminen vaati tarkempaa perehtymistä asiaan. IPSec-tunnelit luotiin Palo Alto -palomuurin Web-hallinnan Network-välilehdellä, jossa yhteyden määritykset oli jaettu neljään eri osioon: IPSec tunnels, IKE Gateways, IPSec Crypto ja IKE Crypto. IPSec-tunneleiden

luominen aloitettiin määrittämällä IKE Crypto- ja IPSec Crypto -profiilit. Esimerkeissä on käytetty yhden IPSec-tunnelin määrityksiä.

IKE Crypto -profiiliin syötettiin profiilin nimi, Diffie-Hellman-ryhmä, salausalgoritmi, tiivistealgoritmi ja kestoaika. Esimerkin VPN-yhteyden IKE Crypto -profiilin määritykset olivat seuraavat:

- nimi: KK_VPN
- Diffie-Hellman-ryhmä: group2
- salausalgoritmi: aes256
- tiivistealgoritmi: sha1
- kestoaika: 1440 minuuttia.

IPSec Crypto -profiiliin määritettiin profiilin nimi, ESP:n (Encapsulating Security Payload) todennus- ja salausalgoritmi, Diffie-Hellman-ryhmä ja kestoaika. Esimerkkiyhteyden määritykset olivat seuraavat:

- nimi: KK_VPN
- ESP todennusalgoritmi: md5
- ESP salausalgoritmi: aes128
- Diffie-Hellman-ryhmä: no-pfs
- kestoaika: 3600 sekuntia.

IKE-yhdyskäytävään määritettiin yhdyskäytävän nimi, paikallinen IP-osoite, kohteen IP-osoite, esijaettu avain, paikallinen tunniste, kohteen tunniste, IKE (phase 1) käytäntö ja IKE Crypto -profiili. Esimerkkiyhteyden IKE yhdyskäytävän asetukset olivat seuraavat:

- yhdyskäytävän nimi: KK_VPN
- paikallinen IP-osoite: ethernet1/1 xxx.xxx.xxx.xxx
- kohteen IP-osoite: dynaaminen
- paikallinen tunniste: IP-osoite xxx.xxx.xxx.xxx
- kohteen tunniste: IP-osoite xxx.xxx.xxx.xxx
- IKE-käytäntö: auto
- IKE Crypto -profiili: KK_VPN

Viimeisenä VPN-tunnelin luomisessa tehtiin IPSec-tunneli. IPSec-tunnelin määrityksiin asetettiin tunnelin nimi, liitäntä, tyyppi, IKE-yhdyskäytävä, IKE Crypto -profiili ja IPSec Crypto -profiili. Tunnelin liitäntä voitiin luoda IPSec-tunnelin luontivaiheessa. Tunnelin liitännälle annettiin jokin nimi esimerkiksi tunnel.100 ja se liitettiin verkkoalueeseen site-to-site. Muut asetukset tulivat IPSec-tunnelille automaattisesti valinnoista riippuen. Esimerkkiyhteyden IPSec-tunnelin määritykset olivat seuraavat:

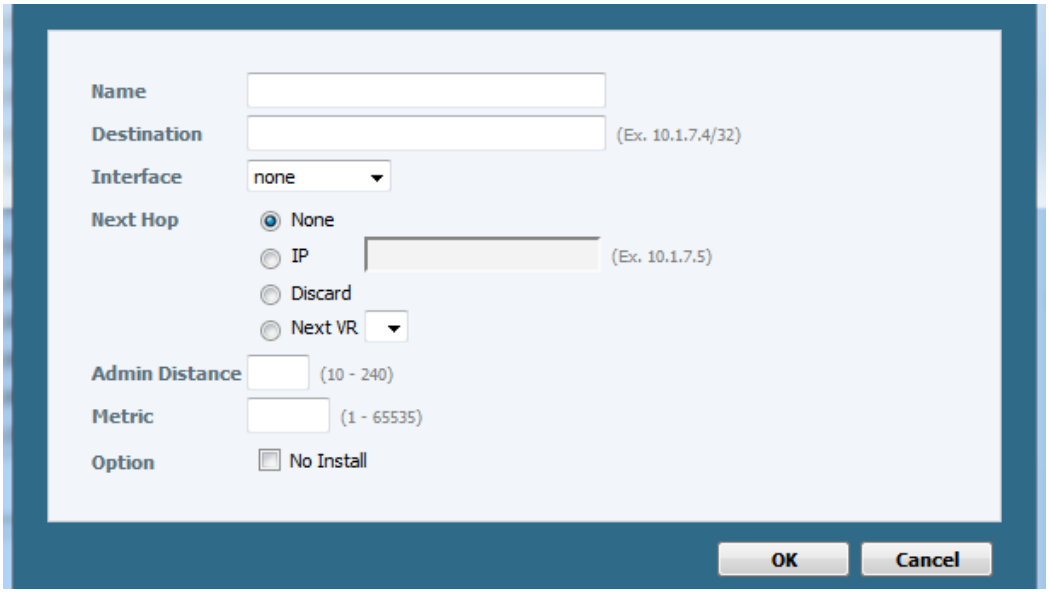
- nimi: KK_VPN
- tunnelin liitäntä: tunnel.111
- tyyppi: Auto Key
- IKE-yhdyskäytävä: KK_VPN
- IKE Crypto -profiili: KK_VPN
- IPSec Crypto -profiili: KK_VPN

6.12 Virtuaalireititin

Palo Alto -palomuurin virtuaalireitittimen avulla voitiin reitittää liikennettä palomuurin sisällä kohdeosoitteen mukaan. Virtuaalireitittimenä käytettiin Palo Alto -palomuurin oletusvirtuaalireititintä (default). Palomuuriin olisi voinut lisätä myös useita muita virtuaalisia reitittimiä. Virtuaalireitittimen asetuksia voitiin määrittää Web-hallinnan Network-välilehden Virtual Routers -osiossa. Virtuaalireitittimen verkkoliitännöiksi valittiin käytössä olevat ethernet-liitännät (ethernet1/1, ethernet1/2) sekä kaikkien VPN-yhteyksien tunneliliitännät.

Verkkoliityntöjen määrityksen jälkeen luotiin staattiset reitit VPN-yhteyksiä varten Static Routes -osiossa. Jokaiselle staattiselle reitille määritettiin nimi, kohdeosoite, verkkoliitäntä ja seuraava reititin (Kuvio 15). Muut asetukset jätettiin oletusasetuksille. Alla esimerkki yhdestä staattisesta reitistä:

- Nimi: teliasonera_vpn
- Kohdeosoite: xxx.xxx.xxx.xxx /32
- Verkkoliitäntä: tunnel.109
- Seuraava reititin: xxx.xxx.xxx.xxx



KUVIO 14 Uuden staattisen reitin luonti-ikkuna

6.13 Palomuurilaitteen varmuuskopiointi

Palo Alto -palomuurien versionumerossa 4.0.3 ei ollut automaattista ominaisuutta palomuurilaitteen varmuuskopiointiin, joten varmuuskopiointi täytyi tehdä jollakin toisella tavalla. Palo Alto -palomuurit tukivat ohjelmointirajapintaa, eli API:a (Application Programming Interface), jonka avulla palomuurilaitteen asetukset voitiin lukea XML-muodossa (Extensible Markup Language). Varmuuskopiointipalvelin piti saada lukemaan palomuurilaitteen asetustiedosto ja tallentamaan tiedosto paikallisesti XML-muodossa.

Varmuuskopiointi ja asetustiedoston lukeminen vaati API-yhteydelle avaimen, jonka avulla varmuuskopiointipalvelin todentaisi itsensä palomuurilaitteelle. API-yhteyden avain saatiin ottamalla yhteys selaimella palomuurilaitteeseen osoitteella https://xxx.xxx.xxx/esp/restapi.esp?type=keygen&user=admin&password=X, jossa X oli palomuurilaitteen pääkäyttäjän (admin) salasana. Selaimelle tulostui seuraavanlainen sivu:

```
<response status="success">
    <result>
                <key>LsKDJR93KFD35LK9klHB%4l==</key>
     </result>
</response>
```

Varmuuskopiointi suoritettiin palvelimella, jonka käyttöjärjestelmänä oli Microsoft Windows Server 2008 R2. Palvelimelle ladattiin wget-ohjelma, jonka avulla voitiin helposti ladata tiedostoja HTTP-, HTTPS- tai FTP (File Transfer Protocol) -protokollaa käyttäen. Varmuuskopiointipalvelimelle luotiin batch-tiedosto, joka latasi palomuurin asetustiedoston palvelimelle ja nimesi tiedoston varmuuskopiointipäivämäärän mukaan. Batch-tiedoston sisältö on esitetty liitteessä 1.

LsKDJR93KFD35LK9klHB%4l== oli aiemmin saatu avain API-yhteyttä varten. Huomioitavaa oli, että batch-tiedostossa komennot tarvitsivat avaimeen kaksi prosenttimerkkiä yhden sijaan Microsoft Windows komentokehotteen toimintaperiaatteen vuoksi. Batch-tiedoston komennot latasivat varmuuskopiointipalvelimelle Palo Alto -palomuurin asetustiedoston pan-cfg.xml ja nimesi asetustiedoston tämän jälkeen varmuuskopiointipäivän mukaan esimerkiksi pan-cfg-20120316.xml.

6.14 Laitetila

Palo Alto -palomuuri sijoitettiin Lahti Energia Oy:n palvelinsaliin, jossa sijaitsivat suurin osa yrityksen palvelimista ja tärkeimmät tietoliikenneverkon aktiivilaitteet. Palvelinsali oli lukittu, ja laitetilaan pääsivät vain sinne oikeutetut henkilöt.

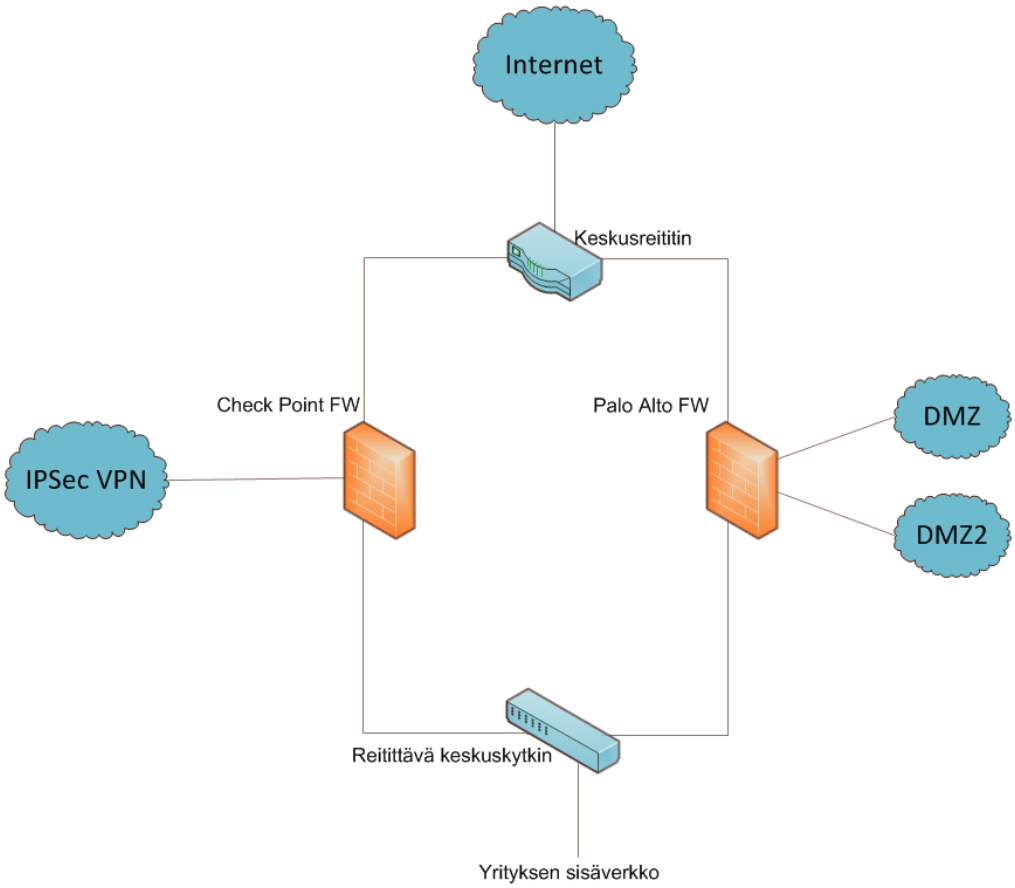
Palvelinsalin lattia oli korotettu asennuslattia, joten verkkolaitteiden kaapelointi laitetilan sisällä voitiin tehdä helposti lattian alla. Laitetilan jäähdytyksestä vastasi tehokas ilmastointi- ja ilmanvaihtojärjestelmä, joka hälytti laitetilan ilman lämpötilan noustessa liian korkeaksi.

6.15 Uuden palomuuriratkaisun edut ja käyttöönotto

Tärkeimmät ominaisuudet uudessa Palo Alto -palomuurissa olivat ohjelmien ja käyttäjien tunnistus. Vanha Check Point -palomuuri ei tunnistanut ohjelmia luotettavasti, eikä Check Point:iin voinut luoda palomuurisääntöjä käyttäjäkohtaisesti. Uusi palomuuriratkaisu helpotti palomuurisääntöjen luomista, sillä pelkillä AD:n muutoksilla käyttäjille voitiin sallia erilaisia verkkopalveluja. Käyttäjäntunnistuksen myötä myös palomuurin hallinta helpottui, ja palomuurisääntöjen määrää voidaan tulevaisuudessa vähentää optimoinnin myötä.

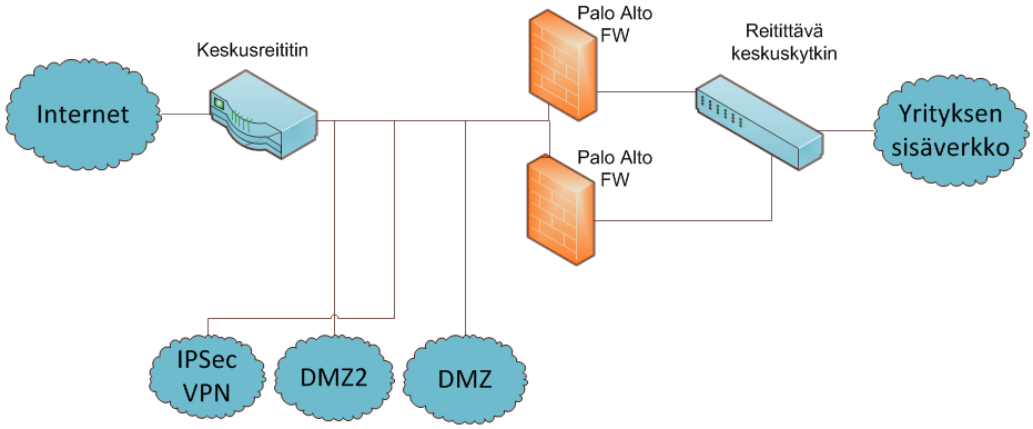
Uusi palomuuri sisälsi myös monia lisäominaisuuksia, jotka omina järjestelminään olisivat kalliita hankkia. Palo Alto -palomuuri sisälsi esimerkiksi sisäänrakennetun virustorjunnan, tunkeutumisenestojärjestelmän ja tietovuodonestojärjestelmän. Erilleen hajautetut järjestelmät heikentäisivät verkon suorituskykyä ja vaikeuttaisivat hallintaa, joten sisäänrakennettujen ominaisuuksien takia verkon ylläpito on helpompaa ja suorituskyky pysyy hyvänä.

Uuden palomuurin käyttöönotossa VPN-yhteyksiä ei vaihdettu yhdellä kerralla uuteen palomuuriin, vaan yhteydet siirrettiin yksi kerrallaan kulkemaan Palo Alto -palomuurin kautta. Käyttöönoton ensimmäisessä vaiheessa verkko oli kuvion 15 mukainen, jossa VPN-yhteydet kierrätettiin vanhan Check Point -palomuurin kautta ja muu liikenne uuden Palo Alto -palomuurin kautta. Siirtämällä VPN-yhtydet yksi kerrallaan uuteen palomuriin säästyttiin vaihdoksesta johtuvista pidempiaikaisista katkoksista.



KUVIO 15 Verkkotopologia käyttöönoton ensimmäisessä vaiheessa

Tulevaisuudessa verkko tulee olemaan kuvion 16 mukainen, jossa kaikki liikenne ohjataan Palo Alto -palomuurien kautta. Palomuurit kahdennetaan, jotta palomuurien toiminta taataan toisen laitteen vikaantuessa. Myös kaikki VPN-yhteydet kulkevat uusien palomuurien kautta.



KUVIO 16 Yksinkertaistettu verkkotopologia käyttöönoton jälkeen

7 YHTEENVETO

Tässä opinnäytetyössä tutustuttiin seuraavan sukupolven palomuurien ominaisuuksiin ja toimintaan. Teoriaosuudessa kerrottiin yritysverkkoihin kohdistuvista tietoturvauhista ja tietoturvallisen ympäristön rakentamista. Teoriaosuus sisälsi myös tavallisen palomuurin toimintaperiaatteen ja uudistukset, joita seuraava sukupolvi toi mukanaan tietoturvaratkaisuihin palomuurien osalta. Palomuurien toimintaperiaatteista huomattiin, että perinteinen palomuuri ei suojaa yrityksen verkkoa enää tarpeeksi hyvin, joten palomuureihin oli kehitettävä uusi sukupolvi.

Tämän opinnäytetyön käytännön osuudessa tavoitteena oli rakentaa toimintatavaltaan lähes identtinen seuraavan sukupolven palomuuri vanhan palomuuriratkaisun tilalle. Uudessa palomuurissa otettiin käyttöön palomuurin tarjoamat lisäedut, kuten käyttäjien ja sisällön tunnistaminen. Palomuurisäännöt tehtiin uusien ominaisuuksien mukaisesti, joten palomuurin läpi menevää liikennettä oli helpompi hallita ja seurata. Uuden palomuurin VPN-yhteydet toteutettiin samoilla protokollilla ja suojausmenetelmillä kuin aiemminkin, sillä yhteyksien tietoturvataso oli ajan tasalla. Kaikkia VPN-yhteyksiä ei siirretty yhdellä kerralla uuteen Palo Alto -palomuuriin, vaan yhteydet siirrettiin yksi kerrallaan vanhasta palomuurista uuteen. Toimimalla näin estettiin yhteyksien vaihdosta johtuvat pidempiaikaiset katkokset.

Tulevaisuudessa Palo Alto -palomuurin ominaisuuksia voidaan hyödyntää paremmin, sillä palomuurissa voidaan ottaa enemmän käyttöön Microsoft AD:n käyttäjäryhmien mukaan tehtyjä palomuurisääntöjä. Käyttäjälle voidaan siis sallia tiettyjä verkkopalveluja vain lisäämällä käyttäjä tarvittavaan käyttäjäryhmään AD:ssa. Myös reaaliaikainen virustorjunta ja palomuurilaitteiden kahdennus parantaisivat tietoturvaa ja toimintavarmuutta. Yksi lupaava lisäominaisuus on myös Palo Alto Networks:n kehittämä GlobalProtect, jonka avulla kotona tai työmatkalla tietokonetta käyttävä henkilö voi kuljettaa verkkoliikenteensä palomuurin läpi, vaikkei olisi yrityksen toimitiloissa tai kytkettynä yrityksen sisäverkkoon.

Uuden palomuurin avulla yrityksen tietoturva on uudella tasolla ja käyttäjien verkkoliikenteen hallinta on helpompaa ja tarkempaa. Käyttäjien ja ohjelmien tunnistaminen luo mahdollisuudet tarkasti säädettyyn tietoturvapolitiikkaan ja tämän myötä tietoturvallisempaan ympäristöön.

LÄHTEET

CERT, 2001. Denial of Service Attacks. CERT [viitattu 27.2.2012]. Saatavissa: http://www.cert.org/tech_tips/denial_of_service.html

Check Point Ltd., 2010. SMART. Check Point [viitattu 13.3.2012]. Saatavissa: http://www.checkpoint.com/products/technologies/smart.html

Check Point Ltd., 2012. Products & Services. Check Point [viitattu 13.3.2012]. Saatavissa: http://www.checkpoint.com/products/index.html

Kizza, J. M. 2005. Computer network security. New York: Springer Science+Business Media, Inc.

Lahti Energia Oy. 2012a. Historia. Lahti Energia Oy [viitattu 23.2.2012]. Saatavissa: http://www.lahtienergia.fi/lahti-energia/50

Lahti Energia Oy. 2012b. Avaintiedot. Lahti Energia Oy. Lahti Energia Oy [viitattu 23.2.2012]. Saatavissa: http://www.lahtienergia.fi/lahti-energia/502

Lahti Energia Oy. 2012c. Energian hankinta ja tuotanto. Lahti Energia Oy [viitattu 23.2.2012]. Saatavissa: http://www.lahtienergia.fi/lahti-energia/energian-hankinta-ja-tuotanto

Lawrence, C.M. 2011. Next-Generation Firewalls For Dummies. Indianapolis: Wiley Publishing

Nokia Inc, 2008. Nokia Network Security. Nokia [viitattu 13.3.2012]. Saatavissa: http://business.nokia.fi/NOKIA_BUSINESS_FINLAND_45/Products/Security_Products/Security_Product_Summary_Guide.pdf

Noonan, W. & Dubrawsky, I. 2006. Firewall Fundamentals. Indianapolis: Cisco Press.

Palo Alto Networks, 2012. Palo Alto Networks' Next-Generation Firewalls. Palo Alto Networks [viitattu 13.3.2012]. Saatavissa: http://www.paloaltonetworks.com/products/

Palo Alto Networks, 2011a. PAN-OS Command Line Interface Reference Guide. Palo Alto Networks.

Palo Alto Networks, 2011b. Management. Palo Alto Networks.

Palo Alto Networks, 2011c. Palo Alto Networks Migration Tool User's Guide. Palo Alto Networks.

Palo Alto Networks, 2011d. Palo Alto Netoworks Administrator's Guide. Palo Alto Networks.

Thomas, T. 2005. Verkkojen tietoturva. Helsinki: IT Press.

Zwicky, E.D., Cooper, S. & Chapman, D.B. 2001. Palomuurien rakentaminen. Helsinki: Satku.

LIITTEET

LIITE 1

VARMUUSKOPIOINTIPALVELIMEN BATCH-TIEDOSTON SISÄLTÖ

```
wget --no-check-certificate
"https://xxx.xxx.xxx.xxx/esp/restapi.esp?type=config&action=show&key=
LsKDJR93KFD35LK9klHB%4l==" --output-document=pan-cfg.xml

for /f "tokens=1-5 delims=/ " %%d in ("%date%") do rename "pan-cfg.xml"
pan-cfg-%%e-%%f-%%g.xml
```