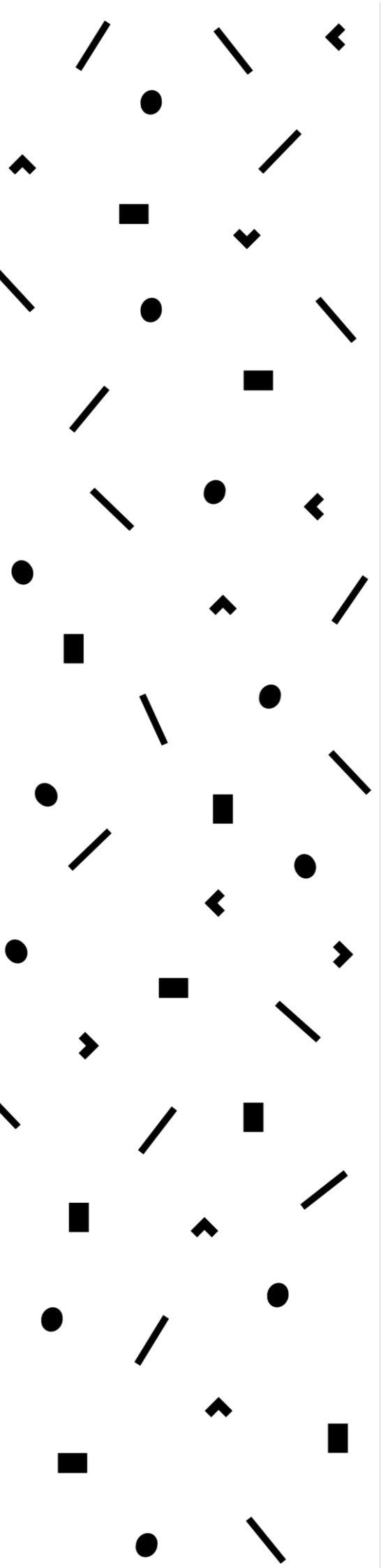


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Palomuurien ominaisuudet ja niiden soveltuvuus Lahden ammattikorkeakoulun ympäristöön

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Miika Äijälä

Lahden ammattikorkeakoulu
Tietotekniikka

ÄIJÄLÄ, MIIKA:

Palomuurien ominaisuudet ja niiden soveltuvuus Lahden ammattikorkeakoulun ympäristöön

Tietoliikennetekniikan opinnäytetyö, 47 sivua, 1 liitesivu

Kevät 2017

TIIVISTELMÄ

Tutkimuksen tavoitteena oli selvittää ja kartoittaa markkinoilla olevien palomuurijärjestelmien soveltuvuutta Lahden ammattikorkeakoulun tulevaksi palomuurijärjestelmäksi. Työ tehtiin Lahden ammatti-korkeakoulun tietohallinnolle.

Tutkimuksessa keskityttiin palomuurijärjestelmän hallintaan, käyttöönottoon ja testattiin olemassa olevien järjestelmien yhteensopivuutta valitun palomuurin kanssa. Työssä testattiin myös etäkäyttäjän tunnistamista ja pääsyä sisäverkkoon.

Palomuurijärjestelmän tehtävänä on mahdollistaa VPN-yhteys erityisesti MAC-käyttäjille, jotka eivät pysty hyödyntämään olemassa olevaa DirectAccess -ominaisuutta. VPN-tunneli suojaa etäkäyttäjän yhteyden ja mahdollistaa käyttäjän tunnistamisen avulla pääsyn organisaation sisäverkkoon.

Tutkimuksessa keskitytään Sophos-palomuurin käyttöönottoon ja konfigurointiin, koska kyseisen valmistajan laite on hankittu testattavaksi ja koekäytön aikana pystytään selvittämään järjestelmän soveltuvuus Lahden ammattikorkeakoulun järjestelmien kanssa. Vertailuna testattiin Palo Alton vastaavaa järjestelmää ja mahdollisuuksia etäyhteyden mahdollistamiseksi.

Tutkimuksessa vertailtiin Palo Alton ja Sophoksen eroja, hallintaa ja käyttöönottoa. Työn aikana saadaan yleiskuva järjestelmien hallinnasta ja perehdytään syvemmin laitteiden VPN-mahdollisuuksiin sekä mahdollisuuksia laajentaa toimintaa pilvipalveluihin. Tutkimuksen tulosten perusteella pystytään suosittelemaan valittua palomuuria Lahden ammattikorkeakoulun tulevaksi palomuurijärjestelmäksi.

Asiasanat: palomuuri, tietoturva, Sophos, Palo Alto

Lahti University of Applied Sciences
Degree Programme Information Technology

ÄIJÄLÄ, MIIKA:

Technical features of firewalls and their suitability to the Lahti University of Applied Sciences environment

Bachelor's Thesis in Telecommunications, 47 pages, 1 page of appendix

Spring 2017

ABSTRACT

The aim of this thesis was to study the firewalls available on the market and their suitability for the new firewall system of Lahti University of Applied Sciences. The thesis was executed for the information management of Lahti University of Applied Sciences.

The thesis concentrated especially on managing and deploying a firewall while, also testing the compatibility of the chosen firewall with other systems in the university's network. Remote user identification and accessibility to the network were also examined in the thesis.

The main task of firewalls is to enable Mac users to use a VPN connection when establishing connection to a network. Mac users cannot utilize existing the DirectAccess method when connecting to a network. The VPN tunnel protects the user's connection and allows the user to connect to the network after the user is identified.

The thesis mainly focused on the deployment and configuration of the Sophos firewall since it had been acquired for testing. A test run gave a better perspective about the system's compatibility with other systems in the network. The firewall's main objective is to handle VPN connection between networks. Palo Alto's firewall was also tested to examine differences in functionality and usability.

Differences between the Sophos and Palo Alto firewalls were examined. The thesis gives an overview of the system's management and VPN connection possibilities, as well as potential opportunities to expand operations to cloud computing. Based on the results of the study, it was possible to recommend the chosen firewall to be the next firewall system for Lahti University of Applied Sciences.

Key words: firewall, information security, Sophos, Palo Alto

SISÄLLYS

LYHENNELUETTELO

AD	Active Directory. Käyttäjätietokanta ja hakemistopalvelu.
AWS	Amazon Web Service. Amazonin pilvipalvelu, joka tarjoaa erilaisia työvälineitä verkkopalveluiden rakentamiseen.
DMZ	Demilitarized zone. Aliverkko, joka yhdistää luotetun verkon epäluotettavaan verkkoon.
DNS	Nomain Name System. Nimipalvelujärjestelmä, jonka avulla verkkotunnukset muutetaan IP-osoitteiksi.
DoS	Denial of Service. Verkkohyökkäys, jolla pyritään estämään verkkosivuston käyttö.
DPI	Deep Packet Inspection. IP-paketin tutkimismenetelmä, jossa paketista tutkitaan osia sisällöstä ja otsikosta.
HA	High Availability. Tietojärjestelmien käytäntö, jossa pyritään takaamaan palvelun jatkuva toiminta.
IP	Internet Protocol. Protokolla, jonka avulla laitteet kommunikoivat pakettikytkentäisessä Internet-verkossa.
IPS	Intrusion Prevention System. Järjestelmä, jolla pyritään järjestelmään kohdistuvat tunkeutumisyritykset.
LAN	Local Area Network. Rajoitetulla alueella toimiva tietoliikenneverkko.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
NAT	Network Address Translation. Osoitteenmuunnos.
NGFW	Next-Generation Firewall. Monia ominaisuuksia sisältävä palomuuri.

OSI-Layer	Open Systems Interconnection Reference Model. Tiedonsiirtoprotokollien kuvaus seitsemässä kerroksessa.
SCCM	System Center Configuration Manager. Microsoftin kehittämä ohjelma, jonka avulla voidaan hallita suuria määriä laitteita.
SQL	Structured Query Language. Standardoitu kyselykieli, jolla tietokantaan voi tehdä erilaisia hakuja.
SSL	Secure Sockets Layer. IP-verkkojen salausprotokolla.
SSL-VPN	SSL Virtual Private Network. SSL-protokollalla salattu VPN-yhteys.
VLAN	Virtual Local Area Network. Fyysinen tietoliikenne verkko, joka jaetaan loogisiin osiin.
VPN	Virtual Private Network. Näennäinen yksityinen verkko.

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on selvittää ja kartoittaa markkinoilla olevien palomuurijärjestelmien soveltuvuutta Lahden ammattikorkeakoulun (LAMK) tulevaksi palomuurijärjestelmäksi. Työssä valitaan kaksi palomuurijärjestelmää ja vertaillaan laitteiden ominaisuuksia toisiinsa Vertailtavia ominaisuuksia ovat järjestelmien toiminta, hallinta, tekniset tiedot ja yhteensopivuus muiden käytössä olevien järjestelmien kanssa. Opinnäytetyö tehdään Lahden ammattikorkeakoulun tietohallinnon toimeksiannosta, ja laite tulee valvomaan käyttäjien liikennettä ulkoverkosta yrityksen sisäverkkoon.

Tässä opinnäytetyössä selvitetään aluksi tietoturvaa yleisesti ja tarvetta yrityksen tasolla. Tämän jälkeen selvitetään eri palomuurityyppien toimintoja ja ominaisuuksia. Lisäksi selvitetään seuraavan sukupolven palomuurin keskeisiä ominaisuuksia ja isoimpia eroja perinteiseen palomuuriin. Työssä tarkastellaan myös Gartner-konsulttiyhtiön tutkimustyötä valittujen palomuurivalmistajien osalta.

Tässä opinnäytetyössä valitaan kaksi palomuuria, jotka asennetaan laboratorioverkkoon. Työssä tarkastellaan palomuurin yleistä hallintaa ja käyttöä. Palomuurin keskeisin ominaisuus on mahdollistaa Virtual Private Network (VPN) -liikenne sisäverkkoon ja yhteensopivuus Active Directoryn (AD) kanssa. Testiympäristönä käytetään koulun tietoverkkolaboratoriota.

Lopuksi selvitetään palomuurien mahdollisuuksia muodostaa site-to-site VPN-yhteys Azuren pilvipalveluun. Site-to-Site VPN-yhteyden avulla pystytään yhdistämään sisäverkon ja virtuaaliverkon palvelut, jolloin saadaan vikasietoisuutta ja paljon hyödyllisiä ominaisuuksia käyttöön. Työssä selvitetään tärkeimmät vaatimukset yhteyden muodostamiseksi ja palomuurijärjestelmän yhteensopivuuksia pilvipalveluiden kanssa.

2 TIETOTURVA

2.1 Tietoturva yleisesti

Tietoturva on ympäristö, jossa palvelut, järjestelmät ja data on suojattu erilaisilta uhilta. Mahdollisia uhkia ovat esimerkiksi tiedon urkinta, tahaton- ja tahallinen vahingonteko.

Tietoturvaa pyritään kehittämään jatkuvasti uusien menetelmien tullessa käyttöön. Pilvipalveluiden yleistyessä tarve uudenlaiseen tietoturvaan kasvaa. (Woody 2013, 23.)

Tietoturvalla tarkoitetaan sitä, että tieto ei joudu sellaisen käsiin, jolla ei ole oikeuksia niiden käsittelyyn. Tietoturvalle on annettu tavoitteet: luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa henkilötietojen ja salassa pidettävän datan estämistä joutua vääriin käsiin. Eheys tarkoittaa tiedon muuttumattomuutta luomisen, käsittelyn ja siirron aikana. Saatavuus mahdollistaa tiedon helpon saatavuuden ja käytön. (Viestintävirasto 2013.)

Fyysisen laitteen hajoamiset ja inhimilliset virheet ovat myös uhkia tietoturvalle. Dataa häviää virheen sattuessa, jos sitä ei ole ennakoitu. Huonosti suojattu verkko mahdollistaa hyökkääjän vahingoittaa verkkoa ja antaa mahdollisuuden käyttää dataa omiin tarkoituksiinsa.

Tietoturvaa tulee miettiä myös tekniikan ulkopuolella. Tekniset ongelmat on helpompi ratkaista kuin muuttaa ihmisten käyttäytymistä. Erilaiset huijausviestit ja kalastelut mahdollistavat henkilön pääsyn dataan, johon ei ulkopuolisella olisi oikeutta, tai jokin ulkopuolinen taho saa huijaamalla salasanat tai omaisuutta itselleen.

2.2 Tietoturvan tarve yrityksessä

Yrityksen tietoturvan päätavoitteena on suojella sisäverkon laitteistoa ja sisältöä ulkoverkon monilta uhilta. Verkkoa suojellaan yleensä sijoittamalla palomuuri verkon reunalle, jolloin estetään hyökkääjän pääsy

sisäverkkoon, mutta jos suojaus murretaan, niin hyökkääjällä on vapaa pääsy kaikkiin verkon sisäisiin palveluihin ja tietokantoihin. Tietoturvaa voi parantaa esimerkiksi päivittämällä laitteisto, ohjeistamalla henkilökunta salasana vaatimuksilla, lukemalla lokeja ja lisäämällä palomuurit myös sisäverkkoon. (Ford 2003, 1.)

Demilitarized Zone (DMZ) sallii yrityksen lisätä palveluja näkyville ulkoverkkoon ja samalla suojelee sisäverkkoa mahdollisilta uhilta. DMZ:n tarkoitus on toimia väylänä sisäverkkoon, jonka kautta käyttäjä voi tunnistautua. DMZ voi myös toimia testialueena verkkomuutoksille tai uusille palvelin testeille. (Tech-FAQ 2017.)

2.3 Verkon tietoturva

Yksittäisen verkon tietoturvaa voidaan parantaa monin eri keinoin. Verkon luotettavuutta voidaan parantaa tekemällä verkosta vikasietoinen ja turvallisuutta voidaan parantaa jakamalla verkot segmentteihin ja estämällä pääsy ei-halutuilta tahoilta.

Verkkoon voidaan myös luoda DMZ, jonka tehtävänä on toimia ulko- ja sisäverkon välissä rajoittaen sisään tulevaa liikennettä, mutta ulosmenevä liikenne on vapaampaa. ”Luotetaan enemmän siihen, mitä lähetetään kuin mitä vastaanotetaan.” Sisäisen verkon monitorointi ja hallinta verkon koon kasvaessa voi heikentää verkon turvallisuutta, jos luotetaan sisäiseen verkkoon sokeasti. Myös mahdollisuus virhekonfigurointeihin kasvaa. (Woody 2013, 117 – 118.)

Hyvän tietoturvan saavuttamiseksi tarvitaan huolellista suunnittelua ja pitää ottaa huomioon lainsäädännön vaatimukset ja rajoitukset. Erilaisia keinoja ja malleja on monia, ja verkon ylläpitäjän on hyvä tietää tietosuojaa koskevat perusasiat ja kehittää verkon turvallisuutta ja käytettävyyttä.

2.4 Virukset ja haittaohjelmat

Viruksia ja haittaohjelmia on monenlaisia. Virukset yleensä leviävät koneesta toiseen internetin verkkojen välillä tarkoituksena saastuttaa mahdollisimman monta laitetta. Torjunta on yleensä automatisoitua erilaisilla viruksentorjuntaohjelmilla ja alan yritykset jakavat löytämänsä virukset keskenään.

Haittaohjelmat jaetaan eri kategorioihin toimintansa perusteella. Viruksen toiminta perustuu tietokoneen toimintojen muokkaamiseen tai estämiseen. Virus voi tyhjentää levyn tilanvarastaulukon, jolloin informaatio on hävinnyt mutta data on kuitenkin saatavilla palautustyökaluilla. Virus voi myös kirjoittaa roskakoodia dataan aiheuttaen järjestelmään toimintahäiriöitä. (Oulun kauppaoppilaitos 2004b.)

Troijalainen on ohjelma, joka ei leviä, mutta voi aiheuttaa silti mittavia vahinkoja. Troijalainen pyörii toisen ohjelman taustalla, ja sen tehtävänä on porttien avaus, tiedostojen poisto tai tiedostojen uudelleennimeäminen. Ohjelma on poistettava manuaalisesti. (Kaspersky 2016.)

Kaikkia haittaohjelmia vastaan paras keino suojautua on ennaltaehkäisy. Viruksentorjuntaohjelman virustietokanta on pidettävä ajan tasalla, palomuuri päällä ja vältettävä tuntemattomien tiedostojen ja ohjelmien asentamista. Tiedostopäätteet on hyvä myös pitää näkyvissä, jolloin test.txt.pif-tuplapäätteiset huomataan helpommin. Varmuuskopioiden ottaminen säännöllisesti helpottaa palautumista ei-toivotusta tilanteesta.

3 PALOMUURITYYPIT

3.1 Palomuuri lyhyesti

Palomuurin tehtävä on suojella sisäverkkoa ulkoverkosta tulevilta tunkeilijoilta ja haitallisilta ohjelmilta. Perinteisen palomuurin toimintoihin kuuluu liikenteen suojaus, VPN, Network Address Translation (NAT), DMZ ja vikasietoisuus. (Oulun kauppaoppilaitos 2004.)

Pakettisuodatteinen palomuuri suodattaa paketteja muun muassa lähde- ja kohdeosoitteen, protokollan ja porttinumeron perusteella. Tilapohjainen pakettisuodatus pitää kirjaa istunnoista ja yhteyksistä ja tarvittaessa reagoi tapahtumiin. Tilallinen palomuuri pitää kirjaa muodostetuista yhteyksistä ja sallii vain yhteyteen kuuluvat paketit. Sovellustason palomuurin toiminta perustuu datan tarkkailuun ja liikenteen suodatukseen sisällön perusteella. (Oulun kauppaoppilaitos 2004.)

Liikenteen suodatuksen lisäksi palomuurin tehtäviin kuuluu muitakin tehtäviä. NAT estää sisäverkon osoitteita näkymästä ulospäin, ja kaikki sisäverkon liikenne kulkee yhden osoitteen kautta eikä paljasta verkon rakennetta ulkopuolisille. VPN luo salatun tunnelin kohteiden välille verkon yli, jolloin ulkopuoliset eivät pääse näkemään informaatiota siirron aikana.

3.2 Perinteinen palomuuri

Eri sukupolven palomuurit eroavat huomattavasti toimintaperiaatteiltaan ja ominaisuuksiltaan. Jokaisella on kuitenkin oma käyttötarkoitus ja rooli organisaation turvallisuuden takaamisessa. Pakettisuodatteinen palomuuri suodattaa liikennettä verkko- ja kuljetuskerroksessa. Järjestelmä tarkastelee liikennettä Internet Protocol (IP) -osoitteen ja porttien numeron perusteella.

Sovellustason palomuuri osaa tutkia sovellustasolla kulkevaa liikennettä ja osaa estää erilaisia Structured Query Language (SQL) injection -hyökkäyksiä tehokkaasti. Deep Packet Inspection (DPI) tarkistaa

saapuvan liikenteen kohde- ja lähdeosoitteet, paketin eliniän ja dataosuuden. Taulukossa 1 kerrotaan lyhyesti palomuurien toiminnasta. (Adbel-Aziz 2009, 4 - 6.)

TAULUKKO 1. Palomuurien toiminta (Adbel-Aziz 2009, 5.)

Tyyppi	Pakettisuodatteinen	Tilapohjainen pakettisuodatus	Sovellustason palomuuri	Deep packet inspection
OSI Layer	Kuljetuskerros	Kuljetuskerros	Sovellustaso	Sovellustaso
Sukupolvi	First generation	second generation	Third generation	Fourth Generation
Toiminta	Tutkii kohde ja lähde osoitetta, porttia ja kutsuttuja palveluja.	Pitää kirjaa istunnoista ja yhteyksistä ja tarvittaessa reagoi	Sovellustason palomuurin toiminta perustuu datan tarkkailuun ja liikenteen suodatukseen sisällön perusteella	Tutkii saapuvan paketin otsakkeet ja dataosuuden etsien mahdollisia viruksia ja haittaohjelmia.

3.3 Seuraavan sukupolven palomuuri

Seuraavan sukupolven palomuuri -käsite vaihtelee ja ominaisuudet voivat vaihdella eri valmistajilla. Seuraavan sukupolven palomuurin keskeiset ominaisuudet ovat kuitenkin seuraavat:

- sovellusten tunnistaminen
- aktiivinen seuranta
- integroitu tunkeutumisen estojärjestelmä
- identiteetin tunnistaminen
- bridged- ja routed-tilat
- kaikki peruspalomuurin ominaisuudet.

(Wilkins 2014.)

Seuraavan sukupolven palomuuri valvoo liikennettä sovellustasolla hyödyntäen DPI-menetelmää, jonka avulla pystytään valvomaan koko verkkoliikenteen sisältöä. Sisällön perusteella palomuuri päästää läpi,

estää tai reitittää liikennettä. DPI-palomuuria hyödyntämällä voidaan suojautua paremmin Denial of Service (DoS) -hyökkäyksiltä ja pystytään tehokkaammin havaitsemaan viruksia ja troijalaisia. Palomuurilla on myös mahdollista rajata verkkosivuilla vierailua ja voidaan määritellä ohjelmistokohtaisesti eri sovelluksille pääsy sisäverkkoon. Järjestelmä pystyy estämään haittaohjelmien leviämistä yrityksen sisäverkossa. (Rouse 2017.)

Next Generation Firewall (NGFW) -palomuuri tarkastaa liikennettä OSI (Open Systems Interconnection Reference Model) -mallin 2-7 tasoilla ja suodattaa haitallista liikennettä. Organisaation sisällä voidaan myös rajata käyttäjän käyttämien sovelluksien liikenteen kaistaa siten, että työhön liittyvät asiat ovat korkealla prioriteetilla ja muun liikenteen kaistaa rajoitetaan tai estetään kokonaan. Sääntöjä voidaan asettaa esimerkiksi verkon, portin, Virtual Local Area Network (VLAN), sovelluksen ja käyttäjän perusteella. (Wilkins 2014.)

3.3.1 Sovellusten tunnistaminen

Ohjelmistokohtainen tunnistaminen on palomuurin ominaisuus, jonka avulla pystytään havaitsemaan haitallista liikennettä. Järjestelmä pystyy tunnistamaan sallitun liikenteen seasta poikkeavaisuuksia, jotka muuten olisivat päässyt sisäverkkoon huomaamatta. (Ohlhorst 2013.)

Järjestelmällä pystytään rajoittamaan liikennettä sisäverkossa, jotta pystytään priorisoimaan käyttäjän liikennettä. Liikenne pystytään erittelemään esimerkiksi rajoittamalla suoratoistopalveluiden liikennettä ja priorisoidaan omaan työnkuvaan liittyvä liikenne. Rajoitus pystytään myös asettamaan kellonajan mukaan niin, että työajan jälkeen ei ole rajoituksia. Rajoitukset ja hallinta tehdään käyttäjä- ja ryhmäkohtaisesti. (Ohlhorst 2013.)

3.3.2 Käyttäjien seuranta

Käyttäjien seuranta on yksi NGFW-palomuurin ominaisuuksista, joka hyödyntää käytössä olevaa AD tai Lightweight Directory Access Protocol (LDAP) -tietokantaa IP-osoitteen sijaan. Käyttäjien liikenteen hallinta helpottuu ja pystytään priorisoimaan kaistankäyttöä yritystoiminnalle ja jopa estämään työhön liittymätöntä liikennettä. Ominaisuuden periaatteena on suojata yrityksen resursseja käyttäjän tahalliselta ja tahattomalta toiminnalta. (Firth 2014, 6.)

Palomuuri pystyy valvomaan erittäin tarkasti käyttäjän liikennettä, joka tekee ominaisuudesta haasteellista käyttäjän yksityisyyden oikeuksien noudattamiseen. Seuranta pystyy esimerkiksi näkemään työntekijän käyttämiä hakusanoja hakukoneilla ja tallentamaan sivuja, joilla on vierailtu. Ennen ominaisuuden käyttöönottoa selvitettäviä asioita ovat seuraavat:

- minkälaista käyttäjästä tallennetaan
- kuinka tietoa käytetään
- miksi tietoa kerätään ja miten sitä hyödynnetään
- kuinka kauan tieto pidetään tallessa
- kuka pääsee tietoon käsiksi.

(Firth 2014, 20-22.)

3.3.3 Integroitu tunkeutumisen estojärjestelmä

Intrusion Prevention System (IPS) -järjestelmä valvoo verkkoliikennettä ja vertaa liikennettä määriteltyyn tietokantaan sekä etsii poikkeuksia normaalista liikenteestä. IPS kirjoittaa tapahtumat lokiin ja valvoo verkossa epäilyttävää ja tunkeutumiseen viittaavaa liikennettä. IPS kirjoittaa lokiin hälytyksistä ja tapahtumista sekä voidaan määrittää estämään liikennettä haluttujen parametrien mukaisesti. (McMillan 2009.)

IPS on suunniteltu tunnistamaan ja estämään tietynlaista liikennettä, mutta järjestelmä ei ymmärrä sovellustason liikennettä. Järjestelmä on

suunniteltu lisäsuojaksi ja tarjoaa suojaa muiden järjestelmien pettäessä. (McMillan 2009.)

4 PALOMUURIN TARVE JA ANALYSOINTI

4.1 Palomuurien valinta

Markkinoilla on erilaisia NGFW laitteita monilta eri valmistajilta. Työn tarkoituksena on vertailla kahden eri palomuurivalmistajan tuotteita ja soveltuvuutta LAMK:n tulevaksi palomuurijärjestelmäksi. Selvitettäviä asioita ovat palomuurin tekniset ja hallinnalliset ominaisuudet sekä yhteensopivuus muiden järjestelmien kanssa.

Vertailuun valittuina kohteina ovat Palo Alto PA-820- ja Sophos SG 230-palomuurit. Palomuurit ovat toiminnoiltaan vertailtavissa, mutta Sophoksen SG 230 -malli on huomattavasti tehokkaampi.

Palo Alto ja Sophos ovat Gartner-taulukon eri tauluissa, joten työn tuloksena nähdään järjestelmien eroavaisuus ja toimintojen hallinta. Vertailun tarkoituksena on saada selville, kuinka Gartner-taulukon alapäässä oleva Sophos palomuuri soveltuu vaadittavista tehtävistä.

4.2 Palomuurin tarve Lahden ammattikorkeakoulussa

Tulevan palomuurin tarkoitus on mahdollistaa etäkäyttäjän yhteys sisäverkkoon hyödyntäen AD-käyttäjätietokantaa ja VPN-tunnelointia. Tarkoituksena on mahdollistaa eri tuoteryhmien VPN-yhteydet, jotka eivät pysty hyödyntämään käytössä olevaa DirectAccess (DA) -ominaisuutta.

VPN-menetelmänä käytetään Secure Sockets Layer Virtual Private Network (SSL-VPN) -yhteyttä, joka edellyttää käyttäjän tietokoneelle asennettavan VPN-ohjelman. Käyttäjällä tulee olla aktiivinen tili luotuna AD-palveluun, josta haetaan käyttäjän kirjautumistiedot.

Palomuurijärjestelmän yhteensopivuus pilvipalveluihin on tulevaisuudessa tarpeellinen palvelu. Palomuurin soveltuvuutta tutkitaan tunnettujen pilvipalveluiden osalta. Palomuurijärjestelmän valinnassa selvitetään myös VPN-ohjelman asentamista automatisoidusti ja sertifikaattien jakamista

yksilöidysti eri käyttäjille, ilman että tietokoneen käyttäjän tarvitsee itse tehdä mitään.

4.3 Gartner-raportti valituista palomuureista

Gartner on markkinatutkimusyhtiö, joka raportoi ohjelmistoja ja julkaisee vuosittain Business Intelligence ja analytiikka – analyysinsä. Raportissa keskitytään Gartnerin raportteihin palomuuriohjelmista vuosilta 2015 ja 2016.

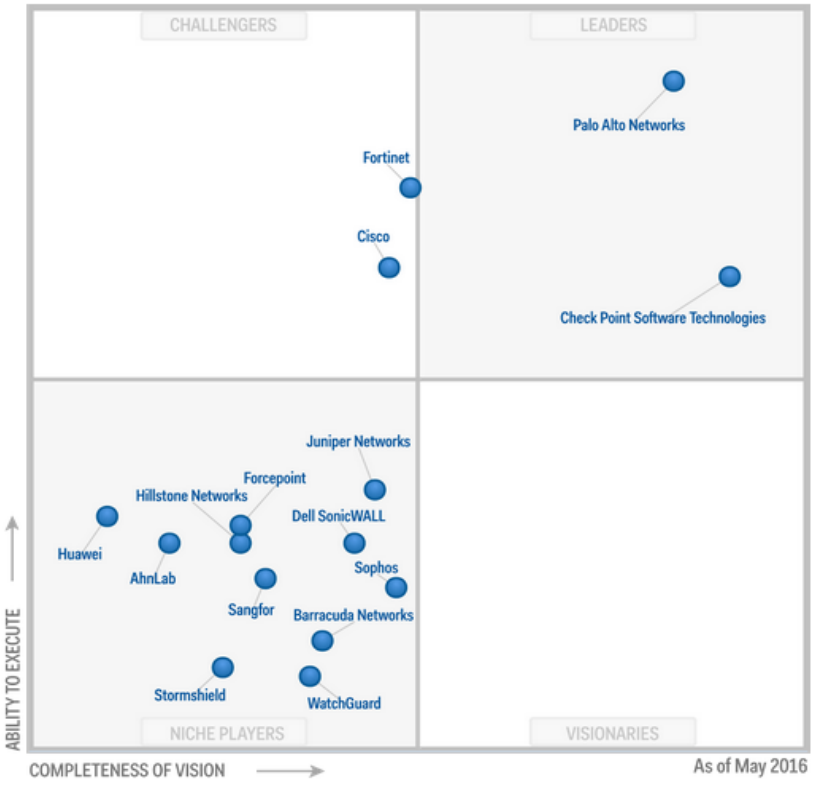
Tulokset koostuvat kahdesta osasta. Ensimmäisessä osassa keskitytään ohjelmiston kykyyn suoriutua tehtävistä, asiakastyytyväisyyteen ja suorituskykyyn. Testien toisessa osassa tarkastellaan yrityksen tuotekehitystä, reagointia markkinoihin ja uusia innovaatiota. Tulokset jaetaan 4 ryhmään: niche, haastajat, visionäärit ja johtajat. Jokaiselle valmistajalle, jälleenmyyjälle ja asiakkaalle tehdään samanlaiset kyselyt ja testit. Raportti koostuu monesta eri kokonaisuudesta eikä keskity pelkästään laitteen ominaisuuksiin. (Gartner 2015.)

Ability to execute tarkoittaa organisaation kykyä ylläpitää tuotetta, yrityksen taloudellista tilannetta, asiakkaita ja myyntiä. Asteikon korkeimpina tarkastelukohteita ovat yleinen tyytyväisyys tuotteisiin ja valmistajan tarjoamiin palveluihin. Muita korkean tason kriteereitä tutkimuksessa ovat laitteen toiminta, luotettavuus ja organisaation kyky reagoida uhkiin sekä yrityksen henkilöstön asiantuntevuus. Asteikossa tarkastellaan myös yrityksen yleistä taloudellista tilannetta ja tuotteiden kilpailukykyä markkinoilla. Arvioitaviin kohteisiin kuuluu myös laitteen hinta ja kyky kehittää tuotetta. (Gartner. 2015.)

Completeness of Vision tarkoittaa yrityksen kykyä reagoida markkinoihin, tuotteen kehitystä ja innovatiivisuutta. Arvioitavia kohteita ovat organisaation kyvyt tuoda markkinoille uusia innovaatioita, laitteiden ominaisuudet ja tuotekehitys. Asteikossa arvostellaan myös organisaation kykyä toimia monikansallisen yrityksen partnerina. (Gartner. 2015.)

Gartner asettaa valmistajat neljästä ryhmästä koostuvaan taulukkoon, jossa on vertailtuna eri valmistajia keskenään. Työn kannalta keskitytään Palo Alton ja Sophoksen vertailuun ja seuraavissa kuvioissa nähdään valmistajien sijoitus Gartnerin analyysitaulukossa (kuviot 1 ja 2).

KUVIO 1. Gartner Magic Quadrant for Enterprise Network Firewalls 2015 (Gartner. 2015.)



KUVIO 2. Gartner Magic Quadrant for Enterprise Network Firewalls 2016 (Gartner. 2016.)

Palo Alto keskittyy seuraavan sukupolven palomuurien kehitykseen ja tarjoaa tuotteitaan virtuaalisesti ja pilveen. Palo Alto oli myöhään liikkeellä pilvipalveluiden tarjonnassa, joten sekin oli otettu huomioon. Palo Alto -tuotteet ovat myös helppokäyttöisiä ja tukevat monia ympäristöjä, kuten Azure ja Hyper-V. (Gartner. 2016.)

Sophos sijoittuu taulukon Niche-ryhmään, koska yritys keskittyy tuotteillaan pieniin ja keskikokoisten yritysten palomuuriratkaisuihin. Arviointiin vaikuttaa yrityksen tuotetarjonta datacenter ja isojen yritysten palomuuriratkaisuihin, joka on pieni tai olematon. Yrityksen vahvuuksiin lasketaan yrityksen pilviratkaisu, jonka avulla voidaan yhdistää verkkoja ja laitteita pilvipalveluiden avulla. Sophos on myös tarjolla Amazon Web Service (AWS) -pilvipalvelussa palomuurina ja tuotetta valitaan nykyään useammin yrityksen pilvipalvelun palomuuriksi. (Gartner. 2016.)

5 PALOMUURIN HALLINTA JA TESTAUS

5.1 Laboratorioympäristön suunnittelu

Tässä osiossa perehdytään palomuurin käyttöönottoon, hallintaan ja tutustutaan järjestelmän toimintoihin. Palomuurin tehtävänä on mahdollistaa käyttäjän VPN-yhteys organisaation sisäverkkoon, joten työssä simuloidaan käyttäjän pääsyä sisäverkkoon käyttäen palomuurin VPN-ominaisuuksia.

Palomuuri hyödyntää käyttäjän tunnistamisessa AD-käyttäjätietokantaa. AD asennetaan Windows Server 2016 -palvelimelle. AD-palveluun luodaan kolme ryhmää, ja näihin ryhmiin lisätään vähintään yksi käyttäjä. Käytettävän ryhmät ovat jumala, hallinto ja kayttajat. Jumala-ryhmä on tarkoitettu ylläpitäjille, jotka hallinnoivat verkkoa ja palveluja. Hallinto on keskitason käyttäjille, jotka ovat tietyn palvelun ylläpitäjiä. Kayttajat ryhmällä on rajallinen pääsy palveluihin ja verkkoon.

Työssä on valittu vertailtaviksi Palo Alto ja Sophos -palomuurijärjestelmät. Sophos on valittu koekäyttöön edullisen hinnan ja nopeuden vuoksi, mutta laite sijoittuu Gartner-taulukon alapäähän. Palo Alto sijoittuu taulukon kärkipäähän ja työssä tutkitaan järjestelmien yhteensopivuuksia vaadittavien toimintojen kanssa ja kuinka taulukon häntäpäässä oleva laite pärjää kärkipäässä olevalle järjestelmälle. Työssä tehdyt vaiheet koostuvat seuraavista testeistä:

- järjestelmän käyttöönotto laboratorioympäristöön
- lisenssien päivitys
- sisä- ja ulkoverkon IP-osoitteiden määritys
- palomuurisääntöjen luonti ja testaus
- AD-integraatio
- VPN-yhteyden testaaminen
- site-to-site ominaisuudet teoriassa.

5.2 Palo Alto -palomuurin käyttöönotto

Työssä testattavana on Palo Alto PA-500, joka on ominaisuuksiltaan kevyt ja järjestelmällä pystytään tekemään tarvittavat testit ja hallinnalliset vertailut. Palo Alton PA-800-sarjan laite olisi ominaisuuksiltaan ja nopeuksiltaan riittävä VPN-liikenteen välittämiseen ja suodattamiseen. PA-800-sarjan laitteet ovat tarkoitettu keskikokoisille yrityksille ja kyseisten laitteiden tiedonsiirtonopeus VPN-yhteyksille on 400 - 500 Mbps.

Testiympäristössä käytetty PA-500-palomuuri sisältää samat hallinnalliset ominaisuudet kuin tehokkaammat mallit. Työssä otetaan palomuuri käyttöön ja liitetään AD-järjestelmän kanssa. Lisäksi työssä tutkitaan PA-800-sarjan Site-to-site VPN-ominaisuuksia.

Taulukossa 2 esitetään Palo Alton testien aikana käytetyt IP-avaruudet. Julkista osoitetta käytetään vain laitteen lisenssien päivitykseen ja testit tehdään suljetussa laboratorioympäristössä. Taulukossa 3 esitetään käytetyt IP-osoitteet harjoituksen aikana. Lisäksi työssä käytetään Windows 2016 -palvelinta, jonka IP-osoite on 192.168.90.2/24.

TAULUKKO 2. Palo Alto harjoituksen IP-avaruudet ja staattiset osoitteet

	IP osoite	subnet mask
Sisäverkko	192.168.90.0	255.255.255.0
Windows Server 2016	192.168.90.2	255.255.255.0
Simuloitu Ulkoverkko	192.168.50.0	255.255.255.0

5.2.1 Tekniset ominaisuudet

Palo Alto PA-500 on yhden räkkiyksikön kokoinen laite. Laitteessa on 160 Gb HDD-levy tiedon tallentamista varten ja laitteen etupaneelissa on 8 I/O

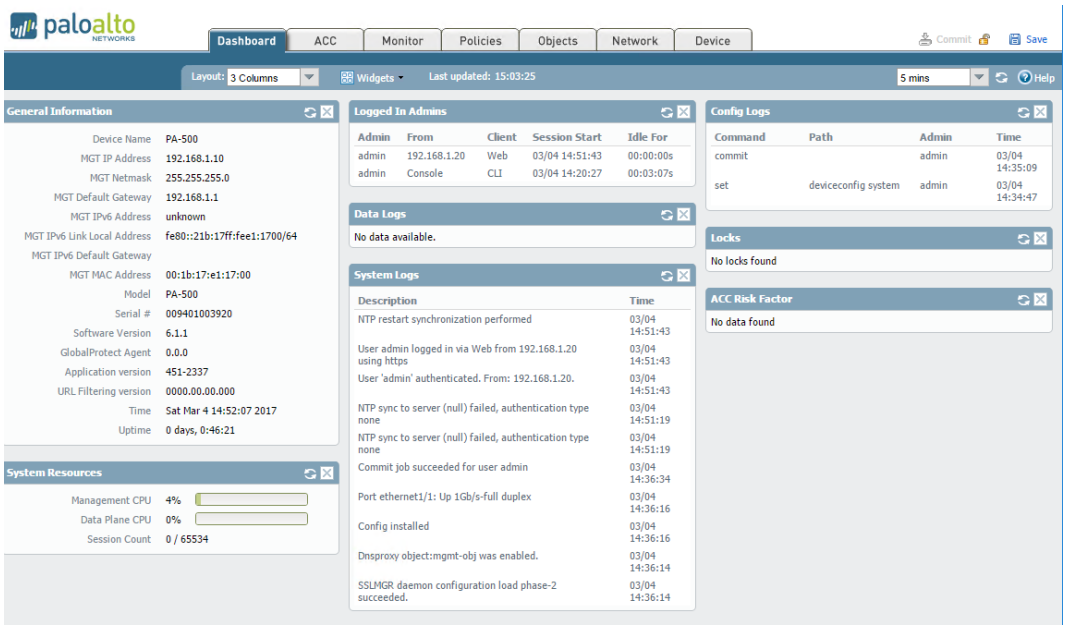
porttia, jotka voidaan määrittää haluamalla tavalla. Lisäksi etupaneelissa on yksi Management I/O ja RJ-45-konsoliportti, jotka ovat nähtävissä kuvassa (kuva 1).

KUVA 1. Palo Alto PA-500

PA-500 on tarkoitettu pienille yrityksille. Palomuurin tiedonsiirtonopeus on 250 Mbps. VPN-yhteyksien tiedonsiirtonopeus on 50 Mbps. Palomuuri pystyy käsittelemään 64 000 samanaikaista yhteyttä ja 7 500 uutta yhteyttä sekunnissa. (Palo alto Networks 2016b.)

5.2.2 Ensimmäinen käyttöönotto ja hallintanäkymä

Palo Alto PA-500:n ensimmäinen konfigurointi tehdään konsolinäkymässä, jolloin määritellään management portin IP-määritykset. Asetukset annetaan komennolla *set deviceconfig system ip-address x.x.x.x netmask y.y.y.y default-gateway z.z.z.z dns-setting servers primary v.v.v.v*, jonka jälkeen hyväksytään asetukset komennolla *commit*. Laite tekee tarvittavat muutokset, jotta päästään jatkamaan konfigurointia web-hallinnassa. Kuviossa nähdään Palo Alton hallintanäkymä (kuvio 3).



KUVIO 3. Palo Alto hallintanäkymä

Palo Alton hallintanäkymä on helposti muokattavissa omien tarpeiden mukaisesti. Sivun ylälaidasta navigoidaan laitteen yleisiin asetuksiin ja asetukset otetaan käyttöön *commit*-valinnalla. Palo Alton -välilehdet selitettynä lyhyesti:

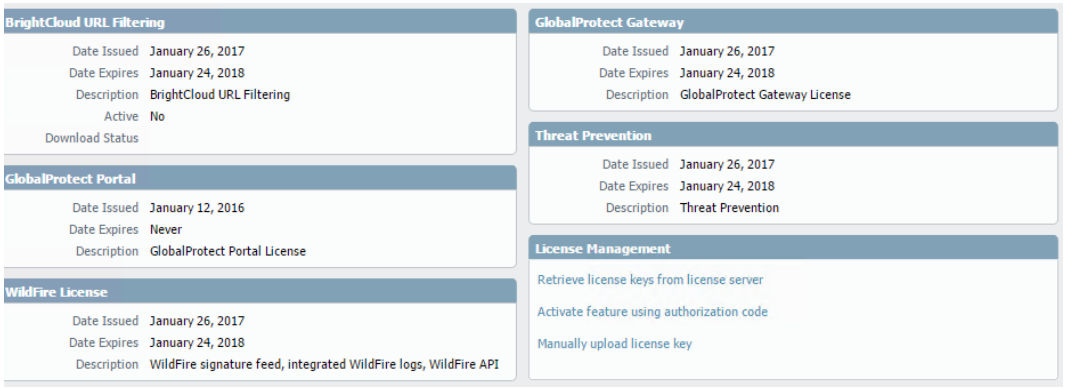
- Dashboard-välilehdellä näkee palomuurin yleiset tiedot, kuten versio ja liitännän toimintatila. Dashboardille voidaan myös lisätä eri tauluja tarpeen mukaan ja tietojen päivitysväli on 1 min, 2 min, 5 min tai käsin valittu.
- ACC-välilehdellä nähdään verkossa tapahtuva liikenne, joka kerätään lokeista ja näytetään visuaalisina graafeina.
- Monitor-välilehdellä tarkastellaan laitteen keräämä tieto verkosta lokien muodossa.
- Policies-välilehdellä määritellään laitteen palomuuri säännöt, NAT reititys ja suojaus.
- Objects-välilehdellä määritellään laitteelle menettelytavat.
- Network-välilehdellä asetetaan laitteen sisä- ja ulkoverkon tiedot, VLAN, VPN-tunnelit ja mahdolliset DHCP määritykset.

- Device-välilehdellä tehdään laitteelle muutoksia, kuten asetetaan vikasietoinen High Availability (HA), linkittäminen AD-palveluun, käyttäjätunnistaminen, lisenssien ja virustietokantojen päivitys.

5.2.3 Lisenssin päivitys

Lisenssi haetaan oletuksena Palo Alton omalta lisenssipalvelimelta, jolloin palomuurin tulee olla yhteydessä ulkoverkkoon. Käytettävät lisenssit voidaan hakea suoraan palvelimelta tai vaihtoehtoisesti laitteeseen voidaan syöttää lisenssiavain manuaalisesti.

Lisenssit välilehdellä nähdään aktiivisena olevat palvelut, jotka lisenssillä on saatu käyttöön. Kuviossa nähdään aktiiviset lisenssit (kuvio 4).



KUVIO 4. Palo Alto lisenssi

5.2.4 Verkon määritykset ja sääntöjen testaus

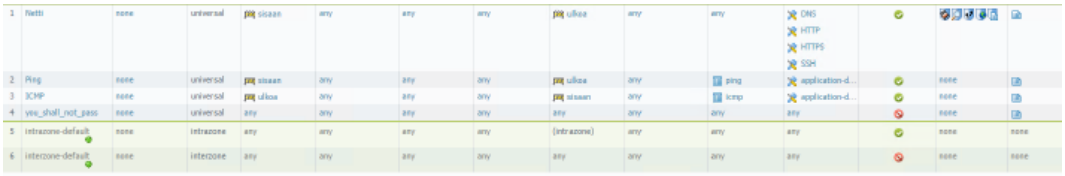
Testeissä tehdään kaksi verkkoa, jossa ensimmäinen verkko simuloi ulkoverkkoa ja toinen määritellään sisäverkoksi. Sisä- ja ulkoverkko määritellään taulukon 2 mukaisesti. Sisäverkossa on kytkin, PC ja Windows Server 2016 -palvelin. Lisäksi palomuuriin määritellään liitäntä, joka on yhteydessä Internetiin.

Työssä määritellään lisäksi kaksi tunnel-interfacea, joita tarvitaan etäkäyttäjän tunnistamiseen ja pääsynhallintaan. Kuviossa 5 on määritelty tunnelit 1 ja 2, joiden tehtävänä on sallia pääsy sisäverkkoon.

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	none	none		
tunnel.1		none	default	Trust		LOCAL
tunnel.2		none	default	Trust		ADUC

KUVIO 5. Palo Altoon luodut tunnelit

Palomuurin toimintojen testaamiseksi sallitaan sisäverkosta ulkoverkkoon HTTPS, HTTPS, SSH, PING, DNS ja kielletään kaikki muu liikenne. Palomuurin sääntö lisätään valikosta policies -> Security -> Add tai muokkaa jo valmiina olevaa sääntöä. Säännöt luetaan ylhäältä alas, joten ensin sallitaan haluttu liikenne, jonka jälkeen kielletään kaikki muu. Kuviossa nähdään palomuurin näkymä säännöistä (kuvio 6).

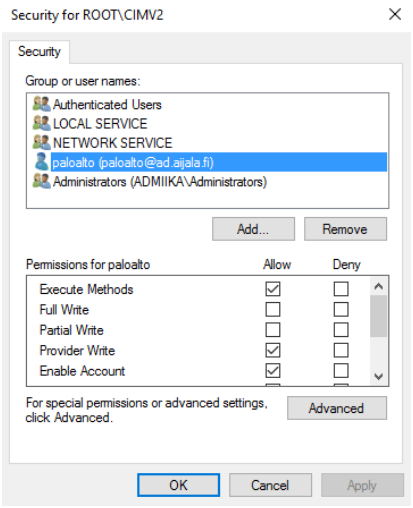


KUVIO 6. Palo Alto sääntö aktivoituna

WWW-suodatus luodaan Objects -> Security Profiles -> URL Filtering, jonka avulla voidaan kieltää haluttu sivusto. Aktivoidaan palomuurin säännöissä objecti, joka lisätään Security Policy rule > actions välilehdellä. Suodatus todettiin toimivaksi.

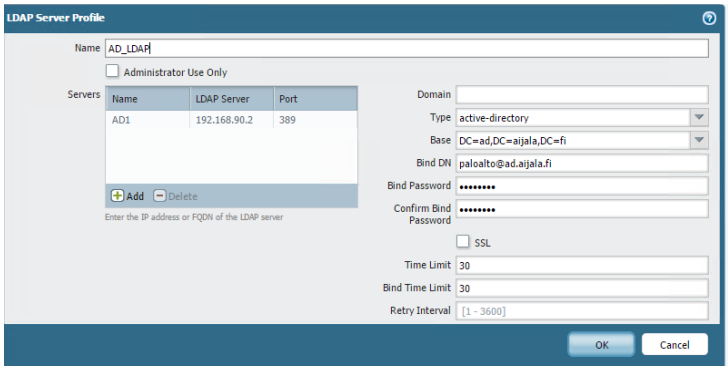
5.2.5 Palo Alton AD-integraatio

Palo Alto palomuurin AD-integraatio vaatii käyttäjän, jolla on kuviossa määritetyt oikeudet Root/CIMV2 kansioon (kuvio 7). Oikeudet määritellään Windows-palvelimella WmiMgmt hallintanäkymässä.



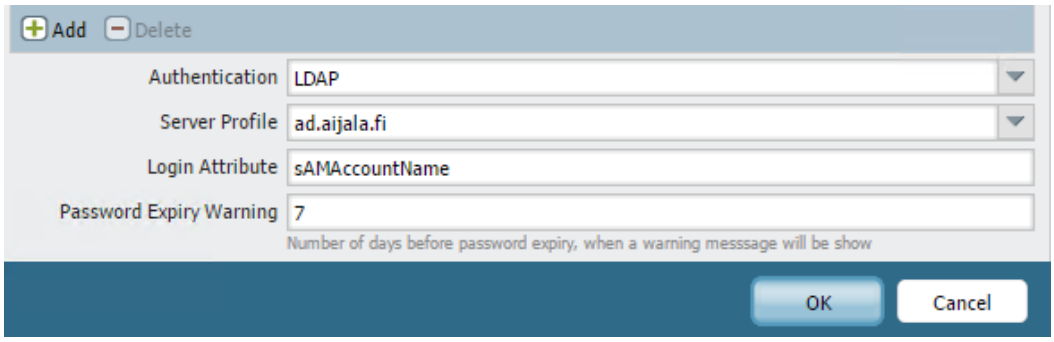
KUVIO 7. Palo Alto käyttäjän oikeudet

Palo Alto -palomuurin integraatio aloitetaan device-välilehdellä, minkä jälkeen valitaan server profiles -> LADP. Seuraavaksi lisätään profiilin tiedot kuvion mukaisesti ja määritellään server listalle palvelimen IP-osoite ja portti 389 (kuvio 8).



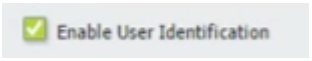
KUVIO 8. AD-profiilin luonti

Seuraavaksi määritellään autentikointiprofiili, jonka avulla voidaan linkittää profiili palomuuriin. Profiiliin lisätään domain, autentikointimenetelmä ja attribuutit käyttäjän kirjautumiselle kuvion mukaisesti (kuvio 9). Profiilin luonnin aikana määritellään myös sallitut käyttäjät. Testeissä sallitaan kaikki käyttäjät.



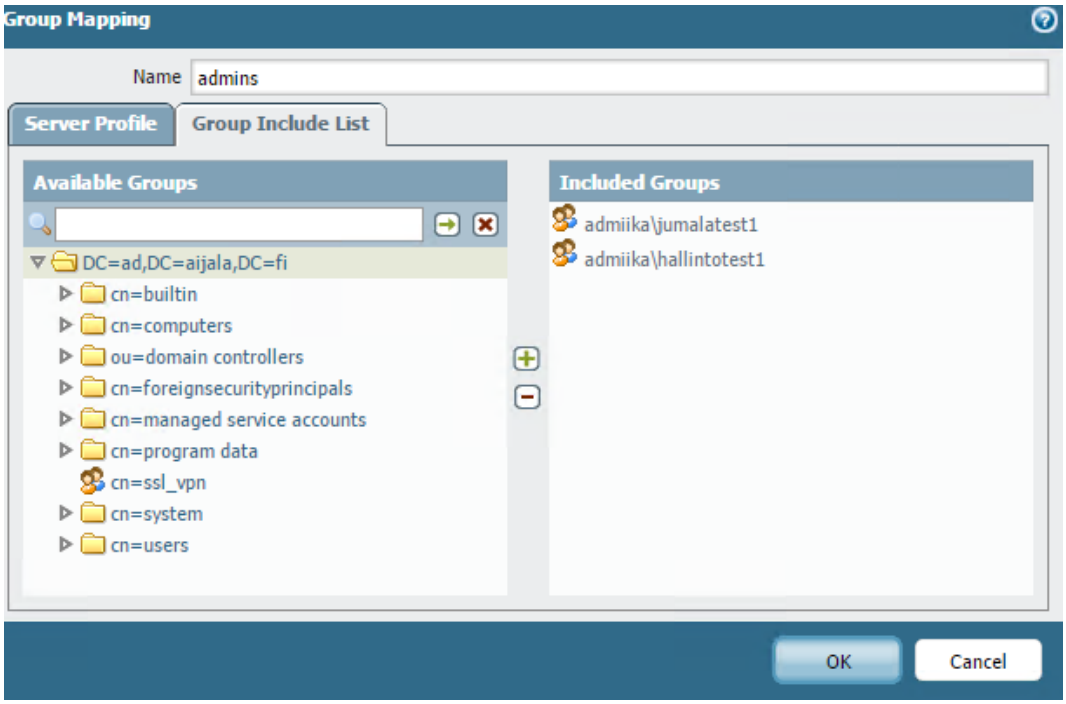
KUVIO 9. Autentikointiprofiili

Seuraavaksi aktivoidaan käyttäjän tunnistaminen jokaiseen palomuurin -zoneen, josta halutaan käyttäjän kirjautuvan AD-autentikoitumisen avulla. Kuviossa nähdään haluttu asetus (kuvio 10).



KUVIO 10. Käyttäjän tunnistaminen zone-asetuksissa

User identification -välilehdellä määritellään group mapping -asetukset, joiden avulla palomuuri hakee käyttäjätiedot AD-tietokannasta. Listaan lisätään jumalatest1 ja hallintotest1 -ryhmät. Kuviossa nähdään, että yhteys toimii AD:n ja palomuurin välillä (kuvio 11).

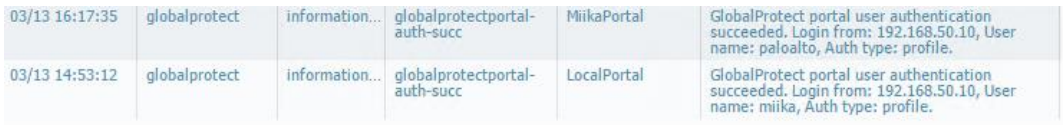


KUVIO 11. Ryhmätietojen lisäys palomuuriin

5.2.6 Etäyhteys palomuuriin

Palomuuriin ja AD:n välille on nyt luotu toimiva yhteys ja yhteyden avulla palomuuri varmistaa käyttäjän oikeudet kirjautuessaan sekä sallii pääsyn sisäverkkoon. Testiä varten on luotu palomuurin sisäiseen muistiin yksi käyttäjä, jotta voidaan nähdä kirjautumistapojen eroavaisuus lokeissa.

Kuviossa nähdään onnistunut kirjautuminen LocalPortal profiilista, joka on palomuurin sisäinen käyttäjälista (kuvio 12). Onnistunut kirjautuminen kirjataan lokeihin auth-succ merkinnällä. MiikaPortal on AD:sta haettu käyttäjälista, joka hakee käyttäjätiedot kirjatuessa. VPN-yhteys ulkoverkon ja sisäverkon välillä todetaan toimivaksi.



03/13 16:17:35	globalprotect	information...	globalprotectportal-auth-succ	MiikaPortal	GlobalProtect portal user authentication succeeded. Login from: 192.168.50.10, User name: paloalto, Auth type: profile.
03/13 14:53:12	globalprotect	information...	globalprotectportal-auth-succ	LocalPortal	GlobalProtect portal user authentication succeeded. Login from: 192.168.50.10, User name: miika, Auth type: profile.

KUVIO 12. Lokitiedot käyttäjän kirjatuessa ulkoverkosta

5.2.7 Käyttäjän toimenpiteet

Palo Alto -järjestelmät käyttävät GlobalProtect lisäosaa, joka mahdollistaa käyttäjän kirjautumisen palomuurin käyttäjäportaaliin. Sovellus pystytään asentamaan monin eri tavoin käyttäjälle riippuen organisaation toimintatavoista. Sovellus pystytään asentamaan MAC OS ja Windows -tietokoneille. Ohjelma pystytään myös asentamaan Windows 10 käyttöjärjestelmällä olevaan puhelimeen sekä iOS- ja Android-laitteille. (Palo Alto Networks 2016a, 85 - 86.)

Sertifikaatti voidaan asentaa käyttäjäkohtaisesti jokaisen käyttäjän laitteelle. Sertifikaatti ladataan Windowsin sertifikaatti tietokantaan tai MAC OS-laitteen keychainiin. GlobalProtect sovellus voidaan asentaa käyttäjille käyttäen seuraavia tapoja:

- GlobalProtect asennus tehdään suoraan web-portaalista. Käyttäjä kirjautuu palomuurin web-portaaliin ja asentaa itse sovelluksen laitteelleen. Toimenpide vaatii käyttäjälle asennusoikeudet käytössä olevalle laitteelle.
- Verkkoympäristössä oleva erillinen web-server, josta käyttäjä voi asentaa tiedoston itselleen. Tällä tavalla pystytään vähentämään palomuuriin kohdistuvaa kuormaa.
- Asetukset haetaan komentoriviltä käyttäen Msiexec-sovellusta. Käyttäjälle asennetaan sovellus ja tarvittavat asetukset määritellään Windows rekisteriin tai Mac plistiin kyseisen ohjelman osalta.
- AD-ympäristössä voidaan mainostaa sovellus käyttäen ryhmä käytäntöjä.

(Palo Alto Networks 2016a, 33 - 35, 85 - 86.)

5.3 Sophos-palomuurin käyttöönotto

Sophos SG 230 on otettu Lahden ammattikorkeakoulussa testattavaksi laitteeksi edullisen hinnan ja korkean nopeuden vuoksi. Palomuurin tehtävänä on mahdollistaa käyttäjien VPN-yhteys sisäverkkoon. Palomuuri

on Sophos tuoteryhmän Medium kokoluokan laite, joka on yhden räkkiyksikön kokoinen laite. Tuote on tarkoitettu pieni- ja keskikokoisille yrityksille ja laite voidaan kahdentaa vikasietoisesti toisella samanlaisella laitteella.

Sophos otetaan käyttöön hyödyntämällä High Availability failover vikasietoisuutta. LAMK:lla palomuurit sijoitetaan fyysisesti eri sijainteihin ja HA-linkki muodostetaan sisäverkon yli. Linkin muodostaminen vaatii kaksi identtistä laitetta ja voimassa olevan lisenssin vain toiselle laitteelle. Työssä tutkitaan myös SG-200 sarjan Site-to-site VPN-ominaisuuksia ja sertifikaattien sekä VPN-ohjelman automatisoitua jakamista käyttäjille.

Taulukossa 3 esitetään Sophoksen testien aikana käytetyt IP-osoitteet. Julkista osoitetta käytetään vain laitteen päivitykseen ja URL-filtering ominaisuuden testaamisen aikana. Työssä käytetty Internal-verkko on väliaikainen verkko, joka luotiin automaattisen asennuksen yhteydessä.

TAULUKKO 3. Sophos harjoituksen aikana käytetyt IP-avaruudet

	IP osoite	subnet mask
Internal (Väliaikainen)	192.168.0.0	255.255.255.0
user	192.168.10.0	255.255.255.0
VPN pool	192.168.80.0	255.255.255.0
Management	192.168.90.0	255.255.255.0
Ulkoverkko	192.168.100.0	255.255.255.0

5.3.1 Tekniset ominaisuudet

Fyysisessä laitteessa on 6 I/O liitäntää ja laitteeseen on mahdollista lisätä korkeintaan 8 liitäntää lisää erillisellä moduulilla, jolloin laitteen porttien

yhteenlaskettu määrä on 14 kappaletta. Lisäksi etupaneelissa on 2 USB 3.0 I/O -liitäntää ja RJ-45-liitäntä konsoliyhteyttä varten, jotka ovat nähtävissä kuvassa (kuva 2). Laitteen takana on 1 USB 2.0 I/O -liitäntä ja 1 VGA-liitäntä. Laitteessa on sisäinen 120 GB SSD paikallisen lokien ja tietojen tallentamista varten.

KUVA 2. SG 230 etupaneeli

Sophos 230 on tarkoitettu pienille ja keskikokoisille yrityksille. Palomuurin teoreettinen tiedonsiirtonopeus on 13 Gbps. VPN-yhteyksien tiedonsiirtonopeus on 2 Gbps. Palomuuri pystyy käsittelemään 4 miljoonaa samanaikaista yhteyttä ja 70 000 uutta yhteyttä sekunnissa. (Sophos 2016b.)

5.3.2 Sophos-palomuurin käyttöönotto

Sophos palomuurissa ensimmäinen konfigurointi tehdään web-hallinnan kautta osoitteesta https://192.168.0.1:4444. Web-hallinnassa aloitetaan laitteen konfigurointi laitteen asennusvelhon avulla. Sophoksen asennusvelhon vaiheet:

1. Määritellään laitteen nimi, yrityksen tiedot ja pääkäyttäjän salasana.
2. Määritellään laitteelle lisenssi ja jos lisenssiä ei ole, niin laitteella on 30 päivän kokeilujakso.
3. Asetetaan palomuurin Local Area Network (LAN) -verkon IP, mask ja mahdolliset DHCP-asetukset. Laboratoriotesteissä otin palomuurin sisäisen DHCP-palvelun käyttöön ja määritin internal-

verkon osoitteeksi 192.168.0.1 255.255.255.0 ja DHCP-osoitteita jaetaan välillä 192.168.0.20-254.

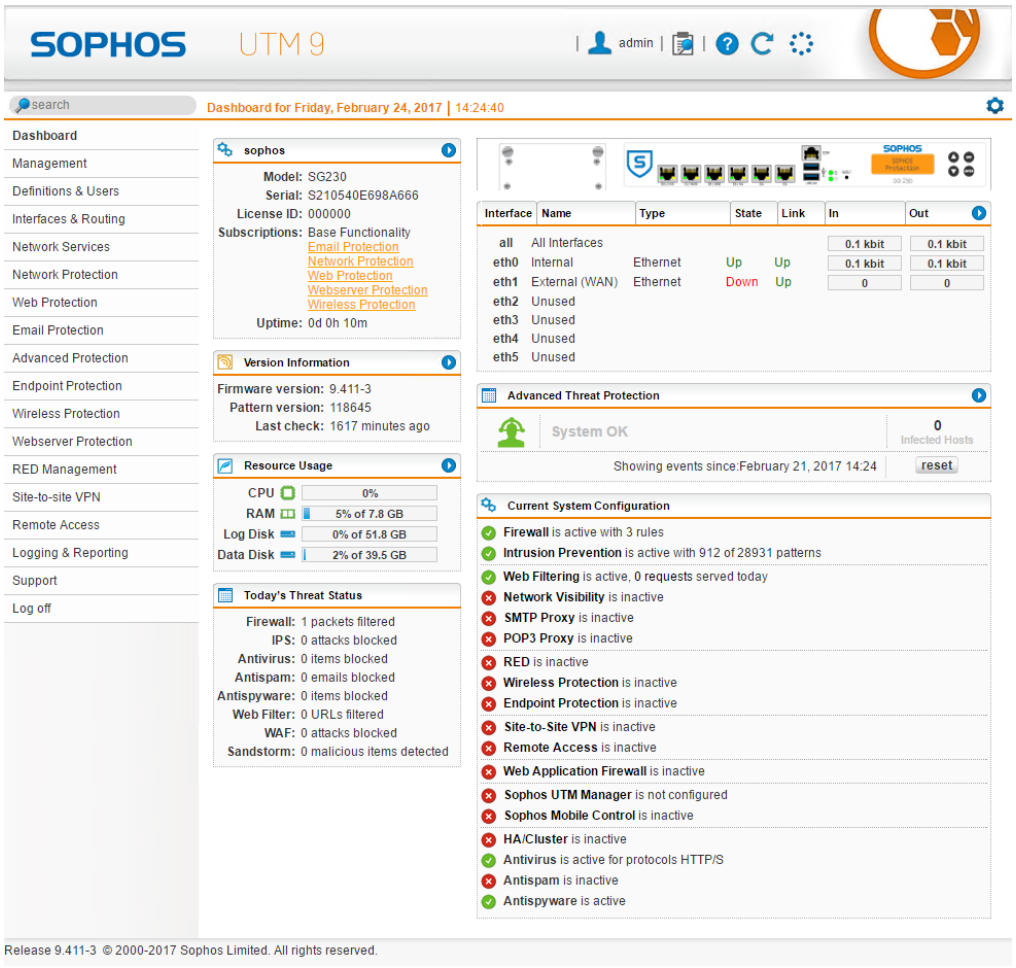
4. Seuraavaksi määritellään ulkoverkon liitäntä ja mahdollisesti ulkoverkon osoitetyyppi. Työssä ulkoverkko tulee eth1-liitäntään ja verkon IP-avaruus on 193.166.74.0 ja osoitetyyppi on DHCP.
5. Määritetään ulosmenevän liikenteen säännöt ja tarkoituksena on sallia HTTP ja HTTPS, terminal ja ulosmenevä DNS liikenne. Asetuksessa voidaan myös määrittää Ping-asetukset, jolloin Palomuuri vastaa tai välittää ping-kyselyjä.
6. Seuraavaksi määritetään kehittyneet IPS ja C&C/Botnet asetukset, mutta kumpaakaan ei oteta käyttöön.
7. Määritetään verkkosivujen suodatus, jotta pystytään estämään haitallinen sisältö sisäverkossa. Estettävien listalla on rikolliset sivut, huume, alastomuus ja epäilyttävät sivut. Asetuksissa voidaan myös määrittämään palomuuri skannaamaan sivu virusten varalta.
8. Email protection ei ole käytössä.

Lopuksi tarkastellaan asennusvelhon yhteenveto kuvion mukaisesti ja tarvittaessa voidaan tehdä vielä muutoksia ennen hyväksymistä (kuvio 13). Sophoksen hallintaan voidaan näillä asetuksilla kirjautua osoitteesta https://192.168.0.1:4444. Kirjautumisessa käytetään luotua admin tunnusta ja salasanaa. Asennusvelho ilmoittaa asennuksessa aktivoitavat palvelut.

KUVIO 13. Asennusvelhon yhteenveto

5.3.3 Sophos WebAdmin

Palomuurissa ei ole vielä määritelty muita asetuksia, kuin asennusvelhon aikana määritetyt asetukset. Kuviossa nähdään yhteenveto käytettävissä olevista palveluista, palomuurin käyttötase, tietoturva poikkeukset ja linkkien tila (kuvio 14).



KUVIO 14. WebAdmin

Palomuurin 30 päivän kokeilujaksossa on paljon ominaisuuksia käytössä ja osa näistä on otettu käyttöön, mutta työssä ei testata kaikkien palveluiden toimivuutta. Osa toiminnoista on otettu käyttöön vain, jotta voidaan tarkastella lokeja ja palomuurin hallintaa. Sophoksen 30 päivän kokeilujaksoon sisältyy seuraavat ominaisuudet:

- network Protection
- email Protection
- wireless Protection
- sandstorm
- endpoint Antivirus
- basicGuard
- support Services.

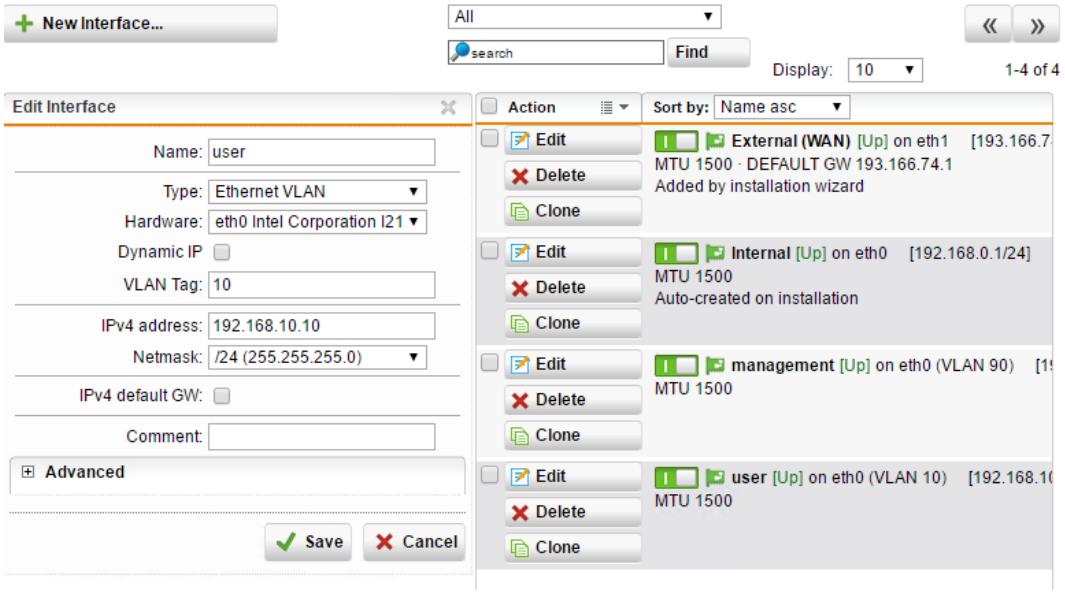
Palomuurissa on yksityiskohtaiset lokit, jotka ovat helposti löydettävissä WebAdmin-näkymän ylälaidasta käyttäjänimen oikealta puolelta. Lokilistalla on kaikki palvelut listattuna, vaikka palvelua ei ole otettu käyttöön. Lokitiedot antavat yksityiskohtaisesti tietoa käyttäjästä, palvelusta ja käytetystä metodista. Liitteenä 1 olevasta tiedostosta nähdään eriteltynä palomuurin lista

5.3.4 Verkon luonti

Luodaan laboratorioympäristöön testiverkko Sophoksen ympärille, niin että palomuurista on yhteys ulkoverkkoon ETH0-liitännän kautta ja ETH1-liitännästä on yhteys sisäverkkoon. Sisäverkkoon luodaan käyttäjille ja hallinnolle omat sisäverkon osoiteavaruudet. Palomuurin DHCP-palvelulla jaetaan IP-osoitteet halutuille verkoille.

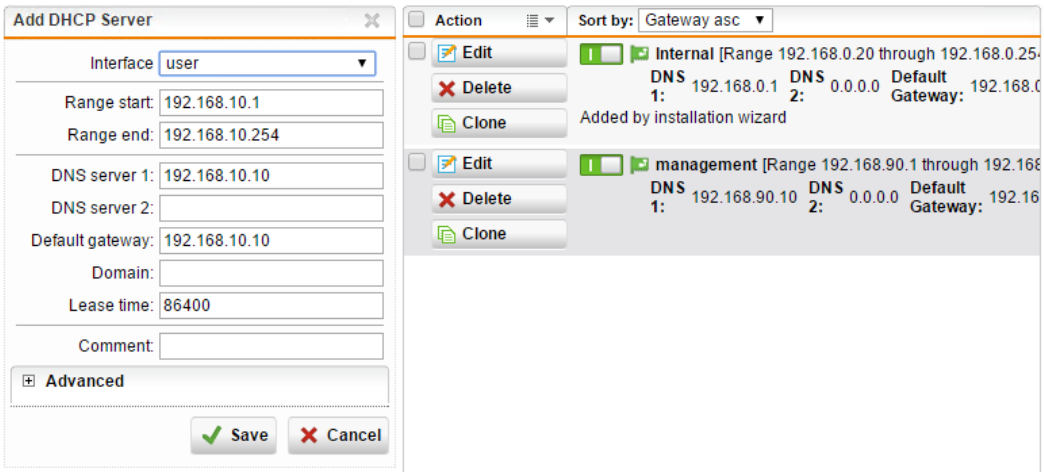
E4-liitynnän kautta muodostetaan virtuaalisesti ulkoverkko, jotta voidaan testata palomuurin läpikulkevaa liikennettä ja määrittää palomuurisääntöjä. Palomuurin verkot luodaan taulukon mukaisesti (taulukko 4).

Verkon määritys ja virtuaalisten verkkojen luonti tehdään interface-asetuksissa. Uuden liitännän luonnin yhteydessä määritetään verkon luonnille VLAN, jolle annetaan staattinen IP-osoite. Verkon luonnin yhteydessä määritellään VLAN, IP-avaruus, verkon nimi ja käytettävä liitäntä. Kuviossa näytetään Sophoksen näkymä verkon luonnista (kuvio 15).



KUVIO 15. VLAN määritys

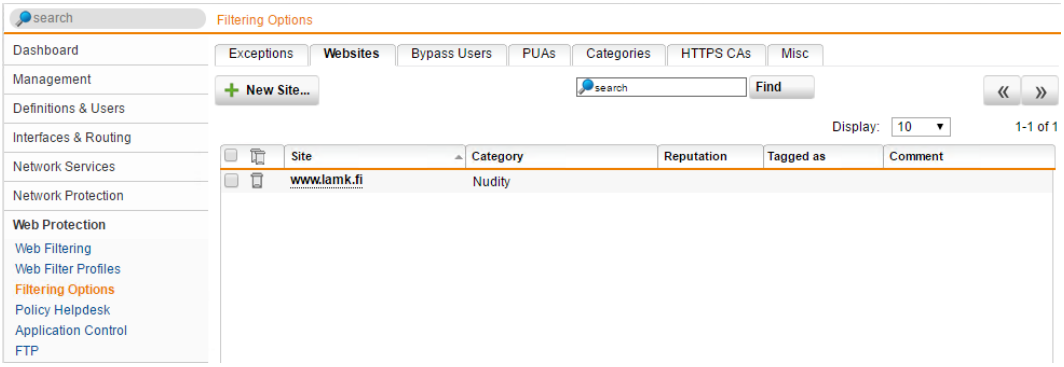
Seuraavaksi lisätään DHCP-palvelulle IP-osoitteet ja avaruudet. Kuvion esimerkissä luodaan user verkolle DHCP ja valmiina on jo luotu internal ja management verkot (kuvio 16). Internal -verkko on väliaikainen ja tarkoitus poistaa käytöstä.



KUVIO 16. DHCP määritykset verkoille

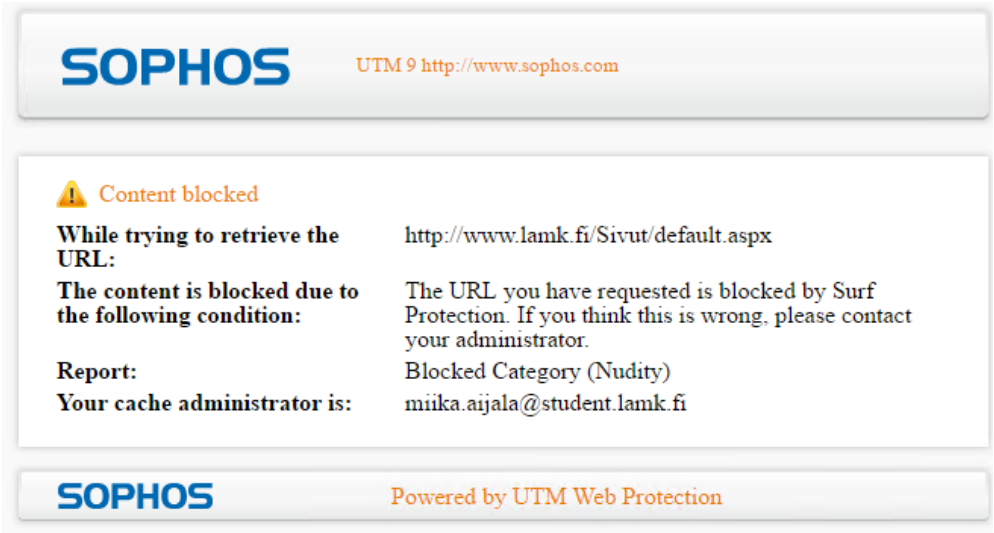
5.3.5 Web-suodatus

Web-suodatus testataan estämällä yhteys www.lamk.fi osoitteeseen. Manuaalinen suodatus tehdään WebAdmin asetuksissa Filtering Options, jossa lisätään sivu kiellettyjen osoitteiden listalle (kuvio 17).



KUVIO 17. palomuurilla estetyt verkkosivut

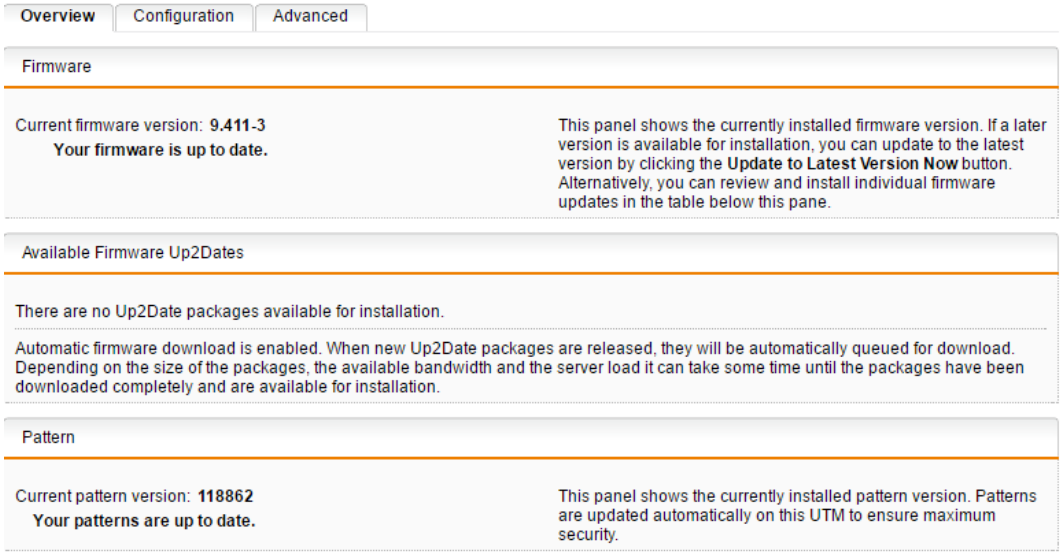
Seuraavaksi testataan suodatuksen toimivuutta sisäverkosta. Tuloksena saadaan Sophoksen näkymä estosta, kun yritetään ottaa yhteys juuri kiellettyyn lamk.fi osoitteeseen (kuvio 18).



KUVIO 18. käyttäjälle tulostettu näkymä estetystä sivusta

5.3.6 Päivitys ja backup

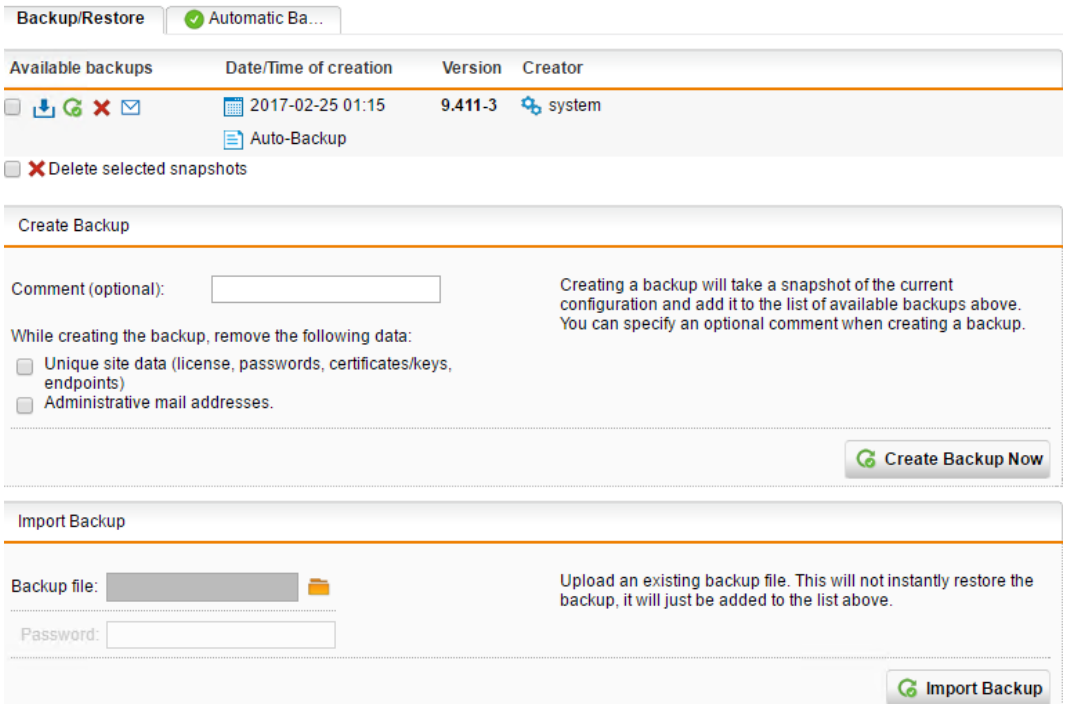
Sophos firmwaren päivitys tehdään Management -> Up2Date WebAdmin hallinnan valikosta. Päivitykset tarkistetaan oletuksena 15 minuutin välein. Kuviossa nähdään, että palomuurin ohjelmisto on ajan tasalla (kuvio 19).



KUVIO 19. Sophos Up2Date näkymä

Palomuurissa on automaattinen varmuuskopiointi, joka tekee varmuuskopioita viikoittain. Laite ottaa varmuuskopiot oletuksena viikoittain, mutta aikaväliä voidaan vaihtaa päivittäiseksi tai kuukausittaiseksi.

Varmuuskopio voidaan ottaa myös manuaalisesti ja antaa kyseiselle kopiolle kuvaava nimi. Kuvion palomuuri on ottanut automaattisen varmuuskopion ja nimennyt tiedoston ajanjakson mukaan (kuvio 20). Laitteeseen voidaan ladata myös asetukset varmuuskopiosta import backup -toiminnolla.



KUVIO 20. Sophos palomuurin varmuuskopiointi

5.3.7 Sophos AD -integraatio

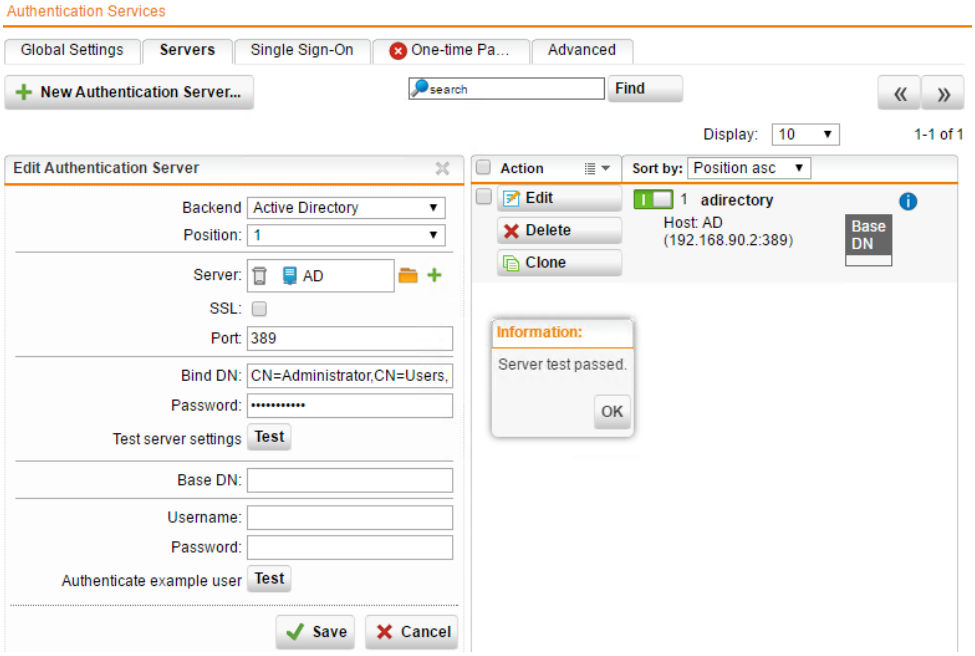
SSL-VPN kirjautuminen AD-tunnuksilla vaatii toimivan AD-integraation palomuurin ja palvelimen välillä. AD-autentikointi otetaan käyttöön Sophoksen WebAdmin hallintaliittymän Definitions and users -välilehdeltä. Navigoidaan autentication servers asetuksiin ja aktivoidaan käyttäjien luonti automaattisesti (kuvio 21).

KUVIO 21. Käyttäjien luonti automaattisesti kirjautuessa

AD-palvelu liitetään Sophoksen Authentication Services -> Servers, jossa määritellään käytettävä AD-palvelin ja tarvittavat asetukset. Liitokseen tarvitaan DN-linkki admin tason käyttäjästä, joka saadaan palvelimelta helpoiten komentorivillä komennolla *dsquery user –name A** Komentorivi tulostaa listan A kirjaimella alkavista käyttäjistä. Työssä käytettävä tunnus

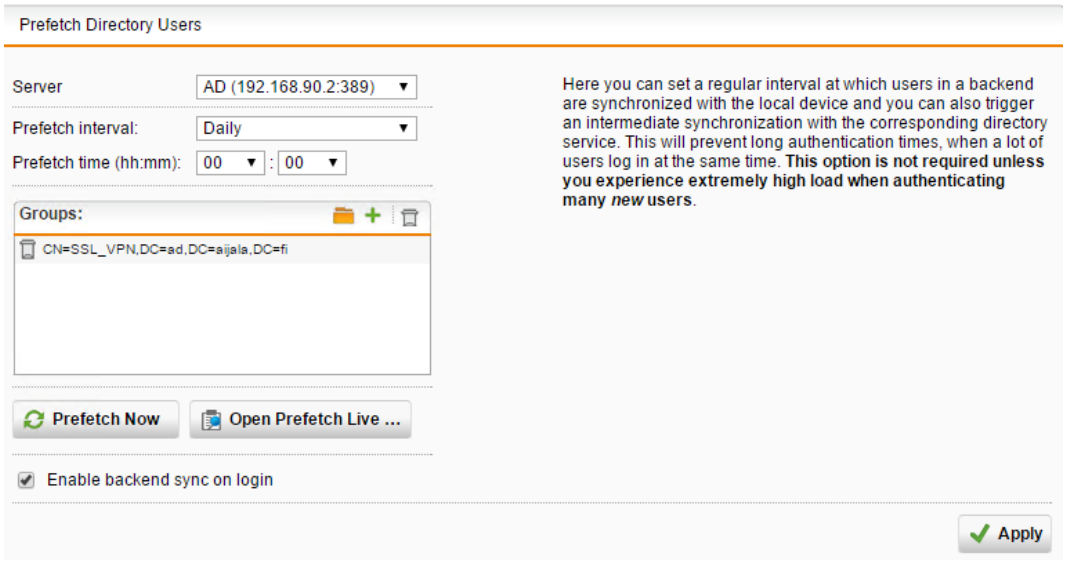
on nimeltään Administrator, jolloin vastaus on *CN=Administrator,CN=Users,DC=ad,DC=aijala,DC=fi.*

Komentoriviltä saadulla DN-linkillä voidaan liittää palomuuri AD-palveluun. Test painikkeella voidaan todeta yhteys ja linkki palomuurin ja AD-palvelimen kanssa toimivaksi (kuvio 22).



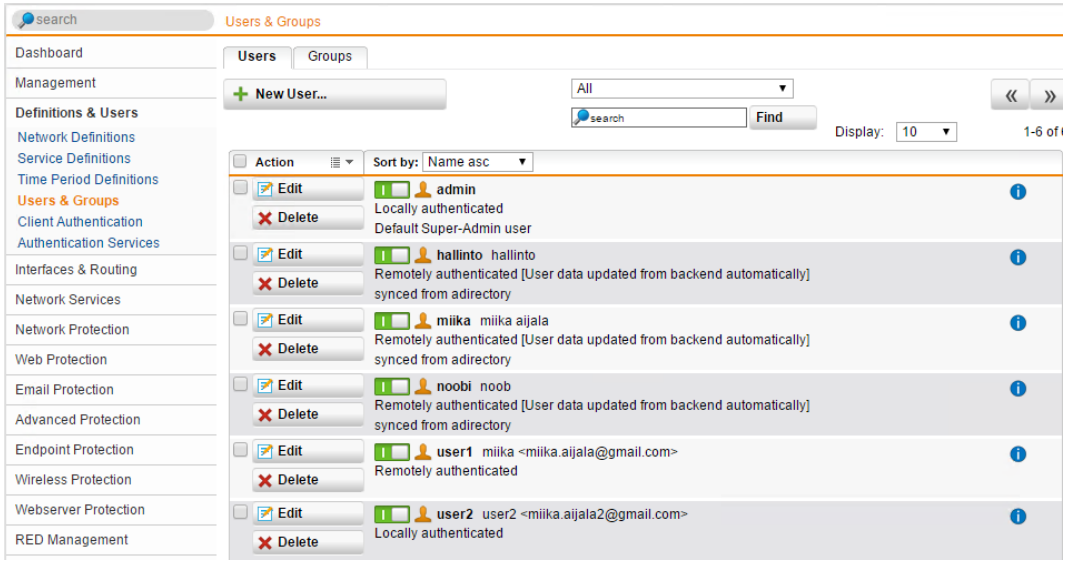
KUVIO 22. Sophos palomuurin ja AD:n välinen linkki testattu toimivaksi

Oletuksena Sophos ei luo käyttäjälle kirjautumistunnusta palomuuriin, joten automatic user creation tulee olla päällä tai prefetch-toiminto ajettu kerran. Prefetch-toiminto ruuhkauttaa palomuuria paljon, joten toimintoa ei suositella, jos käyttäjiä on paljon. Palomuuri kuitenkin lisää käyttäjän palomuurin käyttäjätietoihin, kun käyttäjä kirjautuu ensimmäisen kerran. Kuviossa on määritelty AD-polku päivittäin päivitettävälle ryhmälle, joka haetaan käyttäjätietokannasta (kuvio 23).



KUVIO 23. AD-käyttäjäryhmän päivitysväli Sophoksen käyttäjälistaan

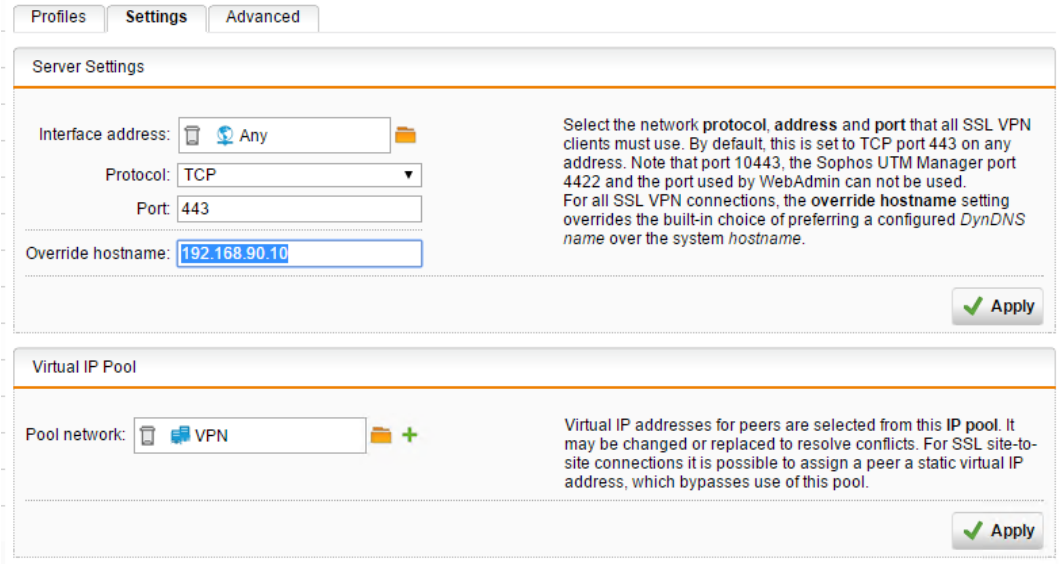
Sophokseen luodaan automaattisesti käyttäjät aikaisempien asetusten perusteella ja voidaan nopeasti hallita oikeuksia ja pääsyä suoraan palomuurista. Kuviossa User1 ja User2 on käsin tehtyjä tunnuksia. AD:sta on haettu käyttäjät miika, hallinto ja noobi, jotka synkronoituvat päivittäin (kuvio 24).



KUVIO 24. Lista tunnetuista käyttäjistä

5.3.8 SSL VPN -määritykset

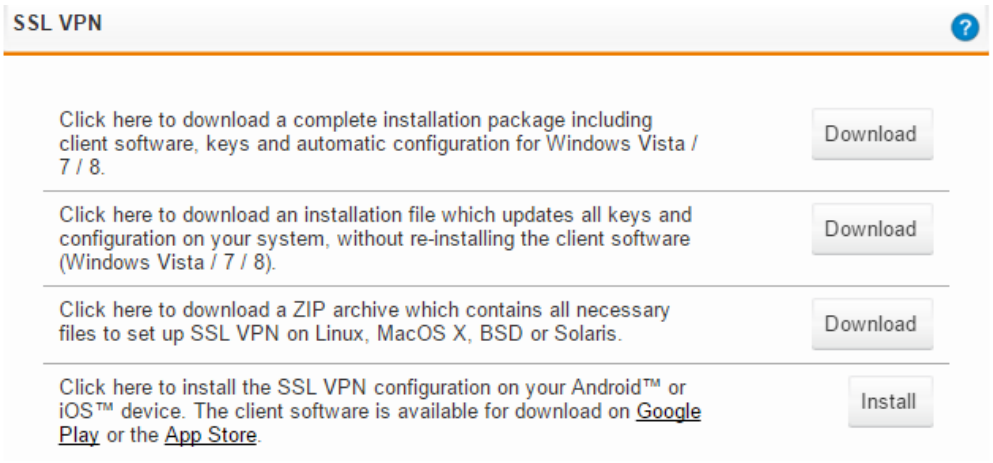
Käyttäjien etäyhteyksiä varten määritellään SSL VPN -yhteyksille oma sisäverkkoavaruus, josta käyttäjät saavat osoitteen. Työssä määritellään VPN-verkko taulukon 4 mukaisesti ja tarvittavat salausmääritelmät annetaan advanced-välilehdellä. Profiles-välilehdellä lisätään käyttäjät ja ryhmät, jotka saavat käyttää SSL VPN -yhteyttä.



KUVIO 25. SSL VPN IP-asetukset

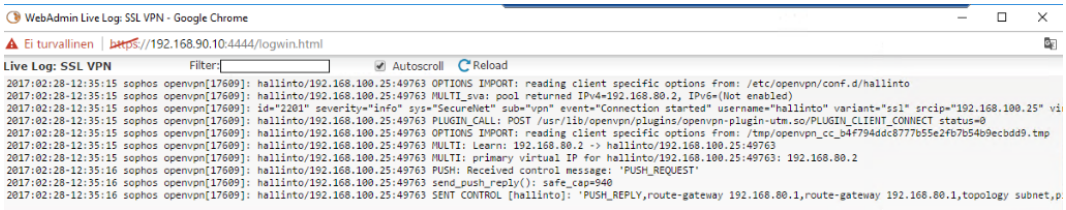
5.3.9 Etäyhteys käyttäen SSL VPN -yhteyttä

Palomuurin SSL VPN -yhteyttä testataan kirjautumalla simuloidun ulkoverkon osoitteeseen https://192.168.100.10. Käyttäjän kirjautuessa palomuuri luo tilin, jonka jälkeen on mahdollista ladata asennustiedosto etäyhteyden muodostusta varten. Käyttäjä kirjautuu palomuuriin omilla tunnuksilla, jotta käyttäjä saa asennettua omat salaustiedot sisältävän VPN-ohjelman. Kuviossa nähdään käyttäjän vaihtoehdot tiedoston lataamiseen (kuvio 26).



KUVIO 26. Käyttäjäportaalissa asennettavissa olevat tiedostot

Kun tiedosto on ladattu ja asennettu laitteelle, niin tämän jälkeen voidaan käynnistää sovellus. Sovellus kysyy käyttäjänimeä ja salasanaa, johon syötetään AD-tunnistetiedot. Kirjautuminen näkyy palomuurin lokitiedostoissa. Kuviossa nähdään onnistunut VPN-yhteys palomuurin kautta SSL VPN -yhteydellä (kuvio 27).



KUVIO 27. Lokitiedosto onnistuneesta VPN-yhteydestä

5.3.10 Käyttäjän toimenpiteet

Sophoksen web-portaaliin kirjautuessa käyttäjä voi ladata Sophos VPN-ohjelman, joka mahdollistaa käyttäjän kirjautumisen palomuuriin. Kirjautumisen jälkeen käyttäjä voi asentaa ohjelman laitteelleen ja asennuksen jälkeen VPN-ohjelmaan kirjaudutaan omilla tunnuksilla. VPN-ohjelma muodostaa yhteyden organisaation sisäverkkoon ja käyttäjällä on pääsy sisäverkon palveluihin.

Monissa yrityksissä on keskitetty hallinta kaikilla IT-laitteilla, jolloin käyttäjä ei voi itse asentaa mitään ohjelmia itsenäisesti. Sophos ei tarjoa selkeitä

toimintatapoja VPN-ohjelman ja käyttäjän sertifikaattien jakamiseen organisaation sisällä. Ohjelma on kuitenkin mahdollista jakaa käyttäjälle System Center Configuration Manager (SCCM) -ohjelman avulla, jonka jälkeen haetaan käyttäjän sertifikaatti palomuurista. Sertifikaatit jaetaan käyttäjille Group policy:llä jokaiselle käyttäjälle erikseen.

5.4 Site-to-site -yhteys

Työn kuluessa tuli tarve Site-to-Site VPN-yhteyksien muodostamiseen, joten seuraavaksi käydään läpi, mitä se tarkoittaa ja selvitetään mahdollista laitetukea valmistajien välillä. Site-to-Site tarkoittaa, organisaation sisäverkon ja virtuaalisen pilvipalvelun verkon yhdistämistä. Virtuaalinen verkko laajentaa nykyistä käytössä olevaa verkkoa ja käyttötarkoituksia on monia. Virtuaaliverkko voi toimia fyysisen järjestelmän varmuuskopiona, jolloin vikatilanteessa pilvipalvelussa oleva järjestelmä toimii varajärjestelmänä. Virtuaaliverkko voi myös laajentaa nykyistä palvelintarjontaa, jolloin tarvittavat järjestelmät voidaan asentaa pilvipalveluun nopeasti ja vaivattomasti.

VPN-yhteys muodostetaan hyödyntämällä staattista tai dynaamista VPN-yhteyttä. Yhteydet selitetään lyhyesti seuraavasti:

- Static Routing tarkoittaa Staattisesti reititettyä VPN:ää, jota kutsutaan myös Policy pohjaiseksi VPN-yhteydeksi. Policy pohjainen VPN salaa ja reitittää paketit asiakkaan määrittämän rajapinnan kautta. Staattinen reititys ei tue Multi-Site VPN, Vnet to Vnet tai Point-to-Site reititystä.
- Dynamic Routing tarkoittaa Dynaamisesti reititettyä VPN:ää ja on riippuvainen tunnel-liitännästä, joka on luotu erityisesti pakettien välittämiseksi. Kaikki Tunnel-liitäntään saapuvat paketit ohjataan suoraan VPN-yhteyteen. Tukee Multi-Site VPN, Vnet to Vnet ja Point-to-Site reitityksiä.

(Slaten 2014.)

Amazon AWS Site-to-Site ominaisuus on yhteensopiva Sophoksen palomuurijärjestelmien kanssa. Sophos palomuurilla voidaan muodostaa Site-to-Site VPN-yhteys Amazonin virtuaalisen verkon ja organisaation sisäverkon kanssa dynaamisesti ja staattisesti. VPN-yhteys määritellään Amazonin virtuaalisen sisäverkon konfiguraatioissa, jossa annetaan palomuurin ulkoverkon osoite. VPN-yhteys on mahdollista luoda staattisesti ja dynaamisesti. VPN-tunnelin luonnin jälkeen AWS luo asennustiedoston, jossa määritellään palomuurin valmistaja, alusta ja versio. Lopuksi asennustiedosto lisätään Sophos palomuuriin ja palomuuri määrittää asetukset automaattisesti. (Sophos 2016a.)

Microsoft Azure ei ole suoraan yhteensopiva suoraan Sophoksen palomuurijärjestelmän kanssa. Site-to-Site VPN-yhteys on mahdollista luoda vain käyttäen staattisesti luotua VPN-gatewaytä. Sophos ei tue IKEv2 protokollaa, jota käytetään dynaamisessa reitityksessä ja laite hyödyntää vain IKEv1 protokollaa. IKEv1 heikkoutena on Site-to-Site-yhteyksien lukumäärä, joka on rajoitettu yhteen. (Techbast 2015.)

5.5 Testien tulokset ja analysointi

Alla olevassa taulukossa 4 esitetään taulukkomuodossa Sophos SG 230- ja Palo Alto PA-820 -palomuurien vertailu teknisistä ominaisuuksista. Taulukossa on tiivistettynä laitteiden tekniset tiedot, ominaisuudet ja hintatiedot. Sophoksen ja Palo Alton hintavertailussa jokainen ominaisuus on erikseen tilattavissa ja ominaisuudet ovat seuraavasti:

- Sophos Essential, eli jokainen moduuli ostetaan erikseen ja hinta määräytyy hinnaston mukaan.
- Sophos Totalprotect sisältää laitteen, kaikki lisenssit ja ympärivuorokautisen tuen vuodeksi. Hinta 4587$
- Palo Alton lisenssit ovat noin 900$ per lisenssi. Lisenssit ovat Threat Prevention, Decryption Mirroring, URL Filtering, Virtual Systems, WildFire, GlobalProtect ja AutoFocus

TAULUKKO 4. Palomuurien vertailu

Palomuuri	Sophos SG 230	Palo Alto PA-820
palomuurin läpäisykyky	13 Gbps	940 Mbps
samanaikaisten yhteyksien korkein lukumäärä	4000000	128000
yhteyksiä per sekunti	70000	8300
VPN-liikenteen läpäisykyky	2 Gbps	400 Mbps
IPS Läpäpisykyky	3 Gbps	780 Mbps
Hardware		
Muisti (RAM)	8 Gb	x
Tallennustila	120GB SSD	240GB SSD
Verkkoliitännät	6	8 Gigabit Eth
Laajentaminen	8 port GBE or 2 port 10Gbe	-
Virrankulutus	34W	45W
Hinta		
hinta per laite	2045 $	4500 $
Laitteiston ominaisuuksien hinta per yksi lisenssi	385 - 1019 $ / vuosi	900$ / vuosi

Testikäytössä oleva Sophos selviytyy hyvin vaaditusta AD-integraatiosta ja käyttäminen on helppoa. Palomuurin hyviä puolia on järjestelmän

helppokäyttöisyys ja sääntöjen luonti oli hyvin yksinkertaista. Järjestelmään voi ostaa palveluita yksittäin tai pakettina ja hinta vaihtelee tarvittavan lisenssin mukaan. SG 230 on hinta/nopeus suhteeltaan hyvä valinta. Lokitiedot ovat helposti löydettävissä ja hyvin selkeitä luettavia.

Sophoksen heikkoudet tulee vastaan, kun halutaan saada VPN-käyttäjille asennuspaketti ja sertifikaatit automatisoidusti organisaation sisällä. Sophos ei tarjoa selkeitä ohjeita toiminnan suorittamiseen ja kyseistä toimintoa ei myöskään testattu työn aikana. Järjestelmän voidaan integroida Azuren pilvipalveluihin vain käyttäen staattista reititystä, koska järjestelmä ei tue IKEv2-protokollaa.

Palo Alton järjestelmä oli helppo asentaa ja käyttöönotto oli yksinkertaista. Järjestelmässä määritellään trust- ja untrust-zonet, joiden avulla pystytään määrittämään palomuurisäännöt ja estämään läpikulkevaa liikennettä. AD-integraatio toimii järjestelmien välillä ja palomuuri pystyy hyödyntämään olemassa olevaa AD-tietokantaa. Etäyhteys testattiin ja todettiin toimivaksi.

6 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli selvittää Palo Alton ja Sophoksen seuraavan sukupolven palomuurien soveltuvuutta Lahden ammattikorkeakoulun seuraavaksi palomuuriksi. Palomuurien toimintaa testattiin yleisellä tasolla ja tarkasteltiin hallintanäkymää ja toimintoja.

Sophos SG 230 oli huomattavasti helpompi asentaa käyttökuntoon ja laitteen hallinta ja sääntöjen luonti oli tehty hyvin yksinkertaiseksi. Sophos palomuurin yleisilme oli myös hyvin selkeä ja tarvittavat ominaisuudet löytyivät suhteellisen helposti. Sophos heikkoudet tulivat vastaan Site-to-Site VPN-yhteyksien luomisessa, jos järjestelmä haluttiin saada yhdistettyä pilvipalveluihin. Sophos järjestelmä ei tue IKEv2:ta, joka on vaatimuksena dynaamisesti reititettyihin Azuren Site-to-Site yhteyksiin. Vaihtoehtona on IKEv1, mutta tämä rajaa yhteyksien määrän yhteen ja toiminto ei tue mobiililaitteiden yhdistämistä virtuaalisen verkon palveluihin.

Palo Alto PA-500 ensimmäinen asennus tehdään aluksi konsolinäkymästä, jossa määritellään hallintaosoite ja aliverkon osoite. PA-500 ei käytä asennusvelhoa. Hallintanäkymä oli vapaasti muokattavissa tarpeen mukaan. Kun palomuuri on saatu käyttöön ja tarvittavat asetukset määriteltyä, niin hallinta oli hyvin selkeää. Laite on myös hyvin yhteensopiva monien järjestelmien kanssa, joten laitetta voi suositella kasvavaan yritykseen, jossa eri järjestelmiä voidaan yhdistää palomuurijärjestelmän kanssa.

Molemmat järjestelmät ovat yhteensopivia AD-hakemistopalvelun kanssa, joten järjestelmien integraatio ei tuottanut ongelmia ja toimintaa pystyttiin testaamaan. Palomuureissa oli myös mahdollisuus lisätä käyttäjiä laitteen sisäiseen muistiin. VPN-yhteyden muodostamisessa hyödynnettiin AD:sta haettuja käyttäjä- ja ryhmätietoja. Tietojen avulla pystyttiin määrittelemään käyttäjien oikeuksia verkon eri osa-alueille. Palo Alton -järjestelmällä on mahdollista asentaa erillinen agent-ohjelma sisäverkkoon, joka yhdistää palomuurit yhteen AD-käyttäjätietokantaan. Ominaisuus on hyödyllinen,

jos useampi palomuuri hakee samaa tietoa tietokannasta ja agentin avulla pystytään vähentämään AD-palveluun kohdistuvaa kuormaa.

Selkeimmät erot järjestelmien välillä ovat kuitenkin laitteiden hinta ja nopeuserot. Sophoksen laite on helppokäyttöinen ja tarjoaa vaativat etäkäyttäjän VPN-yhteydet kilpailukykyiseen hintaan. Jos palomuuri-järjestelmän toimintaa halutaan laajentaa, niin kannattaa tarkistaa laitteen yhteensopivuus muiden järjestelmien kanssa. Palo Alton järjestelmä tarjoaa laajasti ohjeita ja on hyvin yhteensopiva monien eri järjestelmien kanssa.

Testissä oleva palomuuri ei tällä hetkellä ole suunniteltu koko verkon kattavaksi palomuuriksi, vaan järjestelmän tehtävänä on valvoa VPN-liikennettä. Testikäytössä oleva Sophos SG 230 täyttää liikenteen-suodattamisen vaatimukset ja on hyvin helppokäyttöinen sekä hallinta on sujuvaa. Järjestelmän hankinnassa tulee ottaa huomioon käytettävien ominaisuuksien hyödyntäminen ja tarve. Työssä käytetty Sophos SG 230 mahdollistaa käyttäjien VPN-yhteydet sisäverkkoon eikä vaadi suuria investointeja ja asennus on helppoa.

Palo Alto PA-800-sarjan tuotteet eivät yllä Sophoksen tarjoamien nopeuksien tasolle ja hintasuhde on huomattavasti korkeampi verrattuna Sophoksen SG 230 -tuotteeseen. Palo Alton vahvuudet raportissa tulee esiin, kun halutaan hallita organisaation sisällä VPN-ohjelman automaattista asennusta ja sertifikaattien jakamista automatisoidusti käyttäjille. Palo Alto tukee myös IKEv2, jonka avulla järjestelmä pystyy hyödyntämään dynaamista reititystä Azure-palveluun.

Työn aikana olisi voinut testata käytännössä laitteiden site-to-site ominaisuuksia. Pääpainona olisi ollut verkkojen liittäminen Azuren ja AWS-pilvipalveluihin, joka mahdollistetaan palomuurin Site-to-site VPN-yhteyden avulla. Raportin kirjoittamisen aikana tuli tarve laajentaa verkko Azuren pilvipalveluihin, mutta testikäytössä oleva Sophos SG 230:lla on mahdollista luoda vain staattisesti reititetty yhteys. Työssä olisi pitänyt tutkia myös VPN-ohjelman automatisoitua levitystä käyttäjille, niin että

käyttäjän toimenpiteet olisivat mahdollisimman vähäiset. Sertifikaattien jakaminen automatisoidusti olisi pitänyt myös testata erityisesti Sophos laitteella, koska valmistaja ei tarjoa minkäänlaisia ohjeita toiminnan suorittamiseksi omalla laitteellaan. Laitteiden testaamista jatketaan Sophoksen kanssa paljastuneiden haasteiden vuoksi.

Nykypäivänä lähes kaikki tieto on tallennettu sähköisesti ja tietoturvan tarve vain kasvaa. Luotettavan palomuurin huolellinen konfigurointi ja hallinta auttavat suurelta osin verkon suojaamisessa hyökkääjiltä, mutta käyttäjistä johtuvia virheitä sattuu ja nämä skenaariot on otettava huomioon tietoturvaa suunniteltaessa. Tietoturvan tarve kasvaa joka päivä ja uusia uhkia ilmaantuu jatkuvasti, mutta uhat eivät koske vain yrityksen verkkoja. Tietoturvaa tulee miettiä myös henkilökohtaisesti oman laitteiston kannalta, koska Bring Your Own Device (BYOD) on kasvava trendi nykypäivänä. Huolellisesti suunniteltu ja hallittu verkko mahdollistaa tiedon luotettavuuden ja eheyden. Tulevaisuudessa uhat vain kasvavat, joten aktiivisuus tietoturva-alalla on todella tärkeää.

LÄHTEET

Adbel-Aziz, A. 2009. Intrusion Detection & Response Leveraging Next Generation Firewall Technology. SANS Institute [viitattu 22.2.2017]. Saatavissa: https://www.sans.org/reading-room/whitepapers/firewalls/intrusion-detection-response-leveraging-generation-firewall-technology-33053

Firth, R. 2014. Next-Generation Firewalls and Employee Privacy in the Global Enterprise. SANS Institute [viitattu 1.3.2017]. Saatavissa: https://www.sans.org/reading-room/whitepapers/legal/generation-firewalls-employee-privacy-global-enterprise-35467

Ford, D. 2003. Simple rules for securing your internal network. SANS Institute [viitattu 20.2.2017]. Saatavissa: https://www.sans.org/reading-room/whitepapers/bestprac/8-simple-rules-securing-internal-network-1254

Gartner 2015. Magic Quadrant for Enterprise Network Firewalls. Innetworktech [viitattu 20.2.2017]. Saatavissa: http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf

Gartner 2016. Magic Quadrant for Enterprise Network Firewalls. Dataway [viitattu 20.2.2017]. Saatavissa: http://www.dataway.com/pdf/2016_Gartner_Firewall.pdf

Kaspersky Lab 2017. What is a Trojan Virus [viitattu 20.2.2017]. Saatavissa: http://www.kaspersky.com/internet-security-center/threats/trojans

McMillan, J. 2009. What is the Difference Between an IPS and a Web Application Firewall. SANS Institute [viitattu 25.2.2017]. Saatavissa: https://www.sans.org/security-resources/idfaq/what-is-the-difference-between-an-ips-and-a-web-application-firewall/1/25

Ohlhorst, F. 2013. Next-Generation Firewalls 101. NetworkComputing [viitattu 6.3.2017]. Saatavissa:

http://www.networkcomputing.com/careers/next-generation-firewalls-101/1861967701

Oulun kauppaoppilaitos 2004. Tietoturvajärjestelmät [viitattu 20.2.2017]. Saatavissa: http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/palomuurit/palomuurit.htm

Palo Alto Networks 2016b. PA-500. Palo Alto Networks [viitattu 2.3.2017]. Saatavissa: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-500-specsheet

Palo Alto Networks 2016a. GlobalProtect Administrator's Guide. [viitattu 20.2.2017]. Saatavissa: https://www.paloaltonetworks.it/content/dam/paloaltonetworks-com/en_US/assets/pdf/framemaker/71/globalprotect/globalprotect-admin-guide.pdf

Sophos 2016b. Sophos SG Series Appliances. [viitattu 2.3.2017]. Saatavissa: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-sg-series-appliances-brna.pdf?la=en

Sophos 2016a. Site-to-site VPN configurations for Amazon VPC. [viitattu 17.3.2017]. Saatavissa: https://community.sophos.com/kb/zh-cn/120922

Rouse, M. 2017. Deep Packet Inspection (DPI). TechTarget [viitattu 5.3.2017]. Saatavissa: http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI

Slaten, R. 2014. Static vs Dynamic Routing Gateways in Azure. Microsoft [viitattu 18.3.2017]. Saatavissa: https://blogs.msdn.microsoft.com/rslaten/2014/12/08/static-vs-dynamic-routing-gateways-in-azure

Techbast, P. 2015. Step by step Site to site VPN Microsoft Azure and Sophos UTM configuration. Techbast [viitattu 17.3.2017]. Saatavissa: http://techbast.com/2015/02/step-by-step-site-to-site-vpn-microsoft-azure-and-sophos-utm-configuration.html

Tech-FAQ, 2017. DMZ (DeMilitarized Zone). [viitattu 1.3.2017]. Saatavissa: http://www.tech-faq.com/dmz.html

Viestintävirasto, 2016. Ohjeita viestinnän suojaamiseen. [viitattu 15.2.2017]. Saatavissa: https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohjeitaviestinnansuojaamiseen.html.

Woody, A. 2013. Enterprise Security: A data-centric Approach to securing the enterprise. Packt Publishing Ltd [viitattu 10.2.2017]. Saatavissa: http://site.ebrary.com.aineistot.lamk.fi/lib/lamk/reader.action?docID=10672332

Wilkins, S. 2014. A Guide to Choosing a Next-Generation Firewall. Tom's IT Pro [viitattu 5.2.2017]. Saatavissa: http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html

LIITTEET

Liite 1. Sophos palomuurin Lokitiedostot

Admin notifications
Advanced Threat Protection
Application Control
Boot messages
Client Authentication
Configuration daemon
DHCP server *
DNS proxy
Device Agent
Directory user prefetch
Dynamic Routing
Endpoint Protection
Endpoint Web Protection
FTP Proxy
Fallback messages
Firewall
HTML5 VPN Portal
HTTP daemon
High availability
Hotspots
IPsec VPN
IPv6
Ident daemon
Intrusion Prevention System
Kernel messages
Local logins
Logging subsystem
MiddleWare
Multicast (PIM-SM) routing daemon
POP3 proxy
PPP daemon
PPPoA
PPPoE
PPTP daemon
RED
Remote Configuration Manager
Restd
SMTP proxy
SOCKS proxy
SSH server
SSL VPN
Selfmonitoring
Service Monitor daemon
Sophos Mobile Control
Support Access daemon
System messages
Up2Date messages
User authentication daemon
Web Application Firewall
Web Filtering
Wireless Protection