Jani Roukka

SEURAAVAN SUKUPOLVEN PALOMUURI

Tietojenkäsittelyn koulutusohjelma

2015

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

Seuraavan sukupolven palomuuri

Roukka, Jani
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Marraskuu 2015
Ohjaaja: Grönholm, Jukka
Sivumäärä: 26
Liitteitä: 0

Asiasanat: Seuraavan sukupolven palomuurit, palomuurit

Opinnäytetyön aiheena oli seuraavan sukupolven palomuurit ja mitä ne tuovat tietoverkon suojaamiseen. Työssä käsiteltiin mikä on perinteinen palomuuri ja mitä sen tarkoitus on ja mitkä ovat sen heikkoudet.

Työssä tuotiin esille, mitä tarkoitetaan seuraavan sukupolven palomuurilla ja miksi se on parempi, kuin perinteinen palomuuri. Tämän jälkeen käytiin läpi muutama eri seuraavan sukupolven palomuurilaite ja mitä siihen kuuluu.

Tämän jälkeen pohdittiin, mitä yrityksen pitäisi tietää ennen seuraavan sukupolven palomuurin hankkimista. Työssä käyttiin myös läpi IT-strategian tarpeellisuus tietoturva tarpeiden määrittelyssä.

Next-generation firewall

Roukka, Jani
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
November 2015
Supervisor: Grönholm, Jukka
Number of pages: 26
Appendices: 0

Keywords: Next-generation firewalls, firewalls

The subject of this thesis was next-generation firewalls and what they bring to network security. In the thesis I studied what is a traditional firewall and what is its purpose and what are its weaknesses.

In the thesis I also went through what next-generation firewall means and why is it better than a traditional firewall. After this I showcased a few next-generation firewalls and what they were all about.

After this I went through what a business needs to know before deciding on getting a next-generation firewall. In the thesis I also went through why an IT-strategy is essential for the measurement of the company needs in term of security.

SISÄLLYS

1 JOHDANTO

Nykytekniikka kehittyy valtavalla nopeudella ja nopea kehitys tuo mukanaan myös erilaisia vaaroja, jopa tietojenkäsittelyn puolelle. Näihin ongelmiin on monia erilaisia ratkaisuja ja yksi niistä on seuraavan sukupolven palomuurit, jota on tämän opinnäytetyön aiheena. Perinteiset palomuurit ovat tosin melko heikkoja vastustamaan kaikkia niitä uhkia, joita netistä voi tulla yrityksen verkkoon. Palomuurin toimintoina on vain estää liikenne määriteltyihin portteihin sulkemalla ne. Tämä tosin ei riitä enää, sillä on olemassa tapoja, joilla voidaan ohittaa perinteinen palomuuri täysin. Tämä on johtanut siihen, että markkinoille on tullut useita erilaisia verkon suojaratkaisuja tukemaan palomuurin toimintoja.

Näitä laitteita on useita ja yleensä hidastavat verkkoliikennettä joko minimaalisen tai suuren määrän, sillä verkkoliikenne joutuu käymään näiden laitteiden läpi, jotta voidaan tarkistaa onko liikenne sitä mitä sen pitäisikin olla, jolloin voidaan olla varmoja, että verkkoliikenne on turvallista. Kun verkkoon liitetään useita erilaitteita, tulee myös niiden hallinnasta ja ylläpidosta vaikeampaa. Tämä nostaa yrityksien kustannuksia, joka ei ikinä ole hyvä asia liiketoiminnan kannalta, mutta yritykset pyrkivät silti pitämään suojaus ja budjetti suhteen hyvänä.

Yhtenä ratkaisuna tähän on ollut unified threat management (UTM). UTM-laitteet tarjoavat useita ominaisuuksia mitä verkon tietoturvaan vaaditaan, kuten gateway antivirus, intrusion prevention ja muita. Seuraavan sukupolven palomuurit tosin tarjoavat suuremmassa osassa tapauksia suurempia kaistanopeuksia, jonka takia niitä on alettu käyttää enenmmän suurissa organisaatioissa.

Tähän ongelmaan on tosin olemassa ratkaisu ja se on seuraavan sukupolven palomuurit. Seuraavan sukupolven palomuurit hoitavat usean eri verkkoa suojaavan laitteen toiminnot yhdessä laitteessa. Tämä tarkoittaa sitä, että verkon tietoturvan hallinta on parempi ja helpommin hallittavissa. Tämä myös vähentää aikaa, jota kuluu jokaisen laitteen ylläpitämiseen, jolloin saadaan aikaiseksi säästöjä.

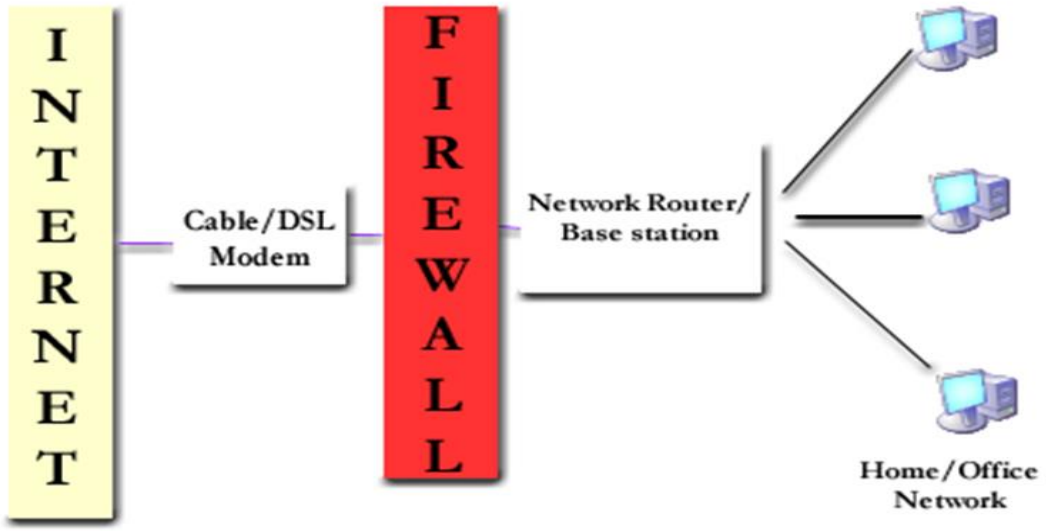
Seuraavan sukupolven palomuuria hankkiessa tulee myös kartoittaa, mitkä ovat yrityksen tarpeet tietoturva mielessä, jotta saadaan mahdollisimman hyvä laite tähän tehtävään. Markkinoilla on useita eri laitevalmistajia, joista valita mikä on juuri sopiva yrityksen tarpeeseen.

2 PALOMUURITYYPIT

2.1 Perinteinen palomuuri

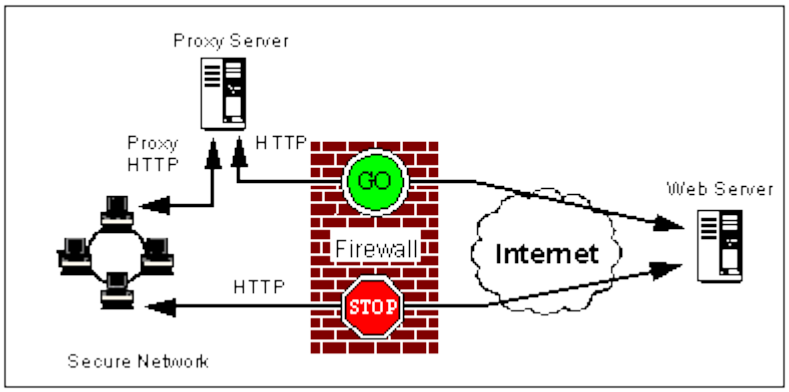
Perinteisellä palomuurilla tarkoitetaan yleensä verkossa olevaa laitetta, joka valitsee mitä verkkoon pääsee ja mitä ei. Perinteinen palomuuri hoitaa tämän tarkastamalla liikennettä, joko tilaton taikka tilallinen tiloilla. Tilattomalla palomuurilla tarkoitetaan, että palomuuri tarkastaa jokaisen paketin erillään, jolloin ei saada kuvaa miten liikenne kokonaisuudessaan liikkuu.

Tilallisessa palomuurissa palomuuri pystyy tarkastamaan pakettiliikennettä tiettyyn pisteeseen saakka seuraamalla sille asetettua protokollaa ja selvittämään missä kohtaa elinkaartaan tietty pakettikeskittymä on. (Wilkins, 2014)



Kuva 1. Erittäin yksinkertainen kuva perinteisen palomuurin toiminnasta.(Oversite sentry, 2015)

Perinteisen palomuurin voi myös toteuttaa proxy-palomuurina, joka tarkoittaa sitä että se on ainoa verkossa oleva piste, joka keskustelee ulkoverkon kanssa. Tällä mahdollistetaan se, että data voidaan tarkastaa proxyssä ennen kuin se välitetään sen todelliselle vastaanottajalle, jolloin saadaan mahdollinen haitallinen liikenne leikattua pois ennen kuin se pääsee vastaanottajalle. Tämä tarkoittaa myös sitä, että sisäverkosta ei pääse ulkoverkkoon käsiksi muuta kuin proxy-palomuurin kautta.



Kuva 2. Kaavio proxy-palomuurin toiminnasta. (Medialab, ei pvm.)

Proxy-palomuureilla on tosin haittansa, sillä jokainen ohjelmisto vaatii oman proxyn ohjelmistotasolla. Proxy-palomuurilliset verkot kärsivät myös heikosta liikenteen nopeudesta ja ohjelmistotuen rajoituksista ja toiminnoista. Tämä johtaa siihen, että tämä toteutus ei ole kovin hyvin laajennettavissa. Tämä on yksi syy siihen, miksi proxy palomuurit eivät ole kovin laajasti käytössä. (Palo alto Networks, 2015)

Yleisiä ominaisuuksia, joita saattaa löytyä palomuurilaitteesta, ovat network access translation (NAT), port address translation (PAT) ja virtual private network (VPN). Näiden ominaisuuksien lisäksi perinteinen palomuuri tarjoaa paljon saatavuutta ja käytettävyyttä. (Wilkins, 2014)

Perinteistä palomuuria on usein tukemassa useita erilaisia verkon tietoturvalaitteita. Näihin laitteisiin kuuluu intrusion prevention järjestelmät (IPS), intrusion detection järjestelmät (IDS), anti-virus skannerit ja spämmi filtterit. IPS-järjestelmän tarkoituksena on on suodattaa verkkoliikennettä ennalta määrätyillä säännöillä. Tämän jälkeen se ilmoittaa siitä eteempäin tai tekee ennalta määrätyn toiminnon, kuten estää liikenteen. IDS-järjestelmä on periaatteltaan melkein kuin IPS, mutta se vain tarkastaa ja raportoi eteenpäin kohdatessaan epäilyttävää liikennettä. Anti-virus

scannauksella tutkitaan käyttäjien levyjä virusten varalta. Spämmi filtterin tarkoituksena on estää verkossa liikkuva liikenne, joka ei vastaa sille annettuja määritelmiä taikka liikenne toimii muuten epänormaalisti. (Beal, 2005)

Unified threat management(UTM) -laitteet ovat myös yksi ratkaisu palomuuritoimintoihin. UTM-laitteet ovat ominaisuuksiltaan erittäin saman tapaisia, kuin seuraavan sukupolven palomuurit, sillä ne sisältävät paljon samoja toimintoja. Suurin asia mikä on ajamassa seuraavan sukupolven palomuureja UTM-laitteiden edelle on se, että UTM-laitteet ovat hitaampia tietoliikenteen liikuttamisessa ja prosessoinnissa kuin seuraavan sukupolven palomuurit. Tämä tosin ei ole haittana pienille tai keskisuurille yrityksille, joilla on pienemmät tietoliikenne tarpeet kuin suuremmilla yrityksillä taikka organisaatioilla. (Casey, 2014)

2.2 Seuraavan sukupolven palomuuri

Seuraavan sukupolven palomuurit (NGFW) nimikettä voivat laitevalmistajat käyttää vapaasti, joka mahdollistaa, että markkinoilla on useita erilaisia laitteita, jotka hoitavat eri asiat paremmin tai huonommin kuin toiset.
Yleensä NGFW-laitteet sisältävät ainakin seuraavat ominaisuudet:

- Ohjelmistokohtainen erotteleminen
- Aktiivinen seuranta
- Integroitu Intrusion Protection System (IPS)
- Käyttäjien seuranta (Käyttäjä- ja ryhmähallinta)
- Bridged- ja routed-tilat
- Kyky käyttää ulkoisia resursseja.

(Wilkins, 2014)

2.2.1 Ohjelmistokohtainen erotteleminen

Yksi suuri asia perinteisen palomuurin ja uuden sukupolven palomuurin välillä on se, että uuden sukupolven palomuurilla on mahdollista erotella ohjelmistokohtaisesti tietoliikennettä. Perinteiset palomuurit ovat riippuvaisia yleisistä porteista, joiden

avulla perinteiset palomuurit pystyvät erottelemaan mikä taikka mitkä ohjelmistot olivat käytössä, taikka minkälaisen hyökkäyksen alaisena verkko on. NGFW-laite ei ole riippuvainen porteista, vaan itse palomuuri pystyy selvittämään minkälaisesta liikenteestä on kyse tutkimalla ip-paketin tasoja kahden ja seitsemän välillä.

Hyvä esimerkki tämän toiminnon tärkeydestä on portin 80 kautta liikkuva HTTP-liikenne. Perinteisesti tätä porttia ei ole käytetty kuin HTTP-liikenteelle, mutta nykyään on useita erilaisia sovelluksia, jotka hyödyntävät tätä porttia tietoliikenteensä liikuttamiseen päätelaitteelta palvelimelle. On olemassa useita erilaisia tapoja piilottaa liikenne portin 80 kautta menevän liikenteen sekaan, mutta yleisin on tunnelointi.

Tunneloinnissa data on tunneloitu HTTP-dataan, joka mahdollistaa sen että data voidaa purkaa loppukäyttäjällä. Tavalliselle palomuurille tämä liikenne ei eroa mitenkään muusta vastaavasta liikenteestä ja se päästetään läpi, mutta NGFW pystyy erottamaan tämän mahdollisesti haitallisen liikenteen ja pysäyttämään kyseiset liikenteen etenemisen, jos se on ohjeistettu niin tekemään. (Wilkins, 2014)

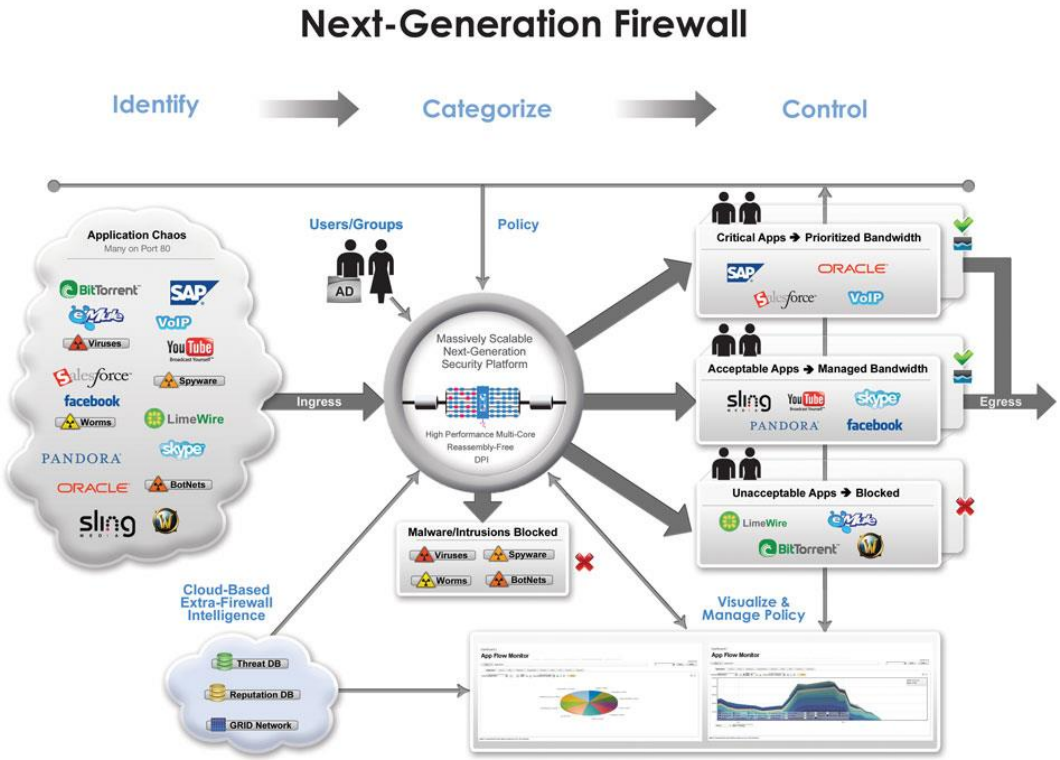
2.2.2 Aktiivinen seuranta

Tällä termillä viitataan siihen, että NGFWn tulee tarkastaa tietoliikennettä syvällisemmin kuin perinteisen palomuurin, sillä sen tulee käydä OSI-mallin tasot kahdesta seitsemään, kun taas perinteinen palomuuri tarkastaa vain kahdesta neljään välillä. Tämä mahdollistaa sen että tietoliikennettä voidaan suodattaa tarkemmin, joka johtaa parempaan tietoturvaan. (Wilkins, 2014)

Tämän tapainen liikenteen tutkinta ei kuitenkaan ole ilman mitään haittoja, sillä se hidastaa tietoliikennettä hieman, sillä liikennettä ei skannata välittömästi. Onneksi NGFW on kuiteinkin nopeampi ratkaisu kuten esimerkiksi unified threat management (UTM) ratkaisut. (Ohlhorst, 2013)

2.2.3 Käyttäjien seuranta

Käyttäjien liikenteen seuranta on yksi suuri ominaisuus, mikä erottaa NGFWn perinteisistä palomuureista. NGFW hoitaa tämän käyttämällä jo olemassa olevaa käyttäjien autentikointia, kuten esimerkiksi active directory tai LDAP. Kun käyttäjät ovat tiedossa, on tiettyjen käyttäjien liikenteen hallinta helppoa. (Wilkins, 2014)
Tätä voidaan kuvan 2. esimerkin tapaisesti hyödyntää siten, että rajoitetaan työaikana käytettävän ei töihin liittyvän liikenteen kaistaa tai estetään se vallan, jolloin jää enemmän kaistaa yritystoiminnoille. (Ohlhorst, 2013)

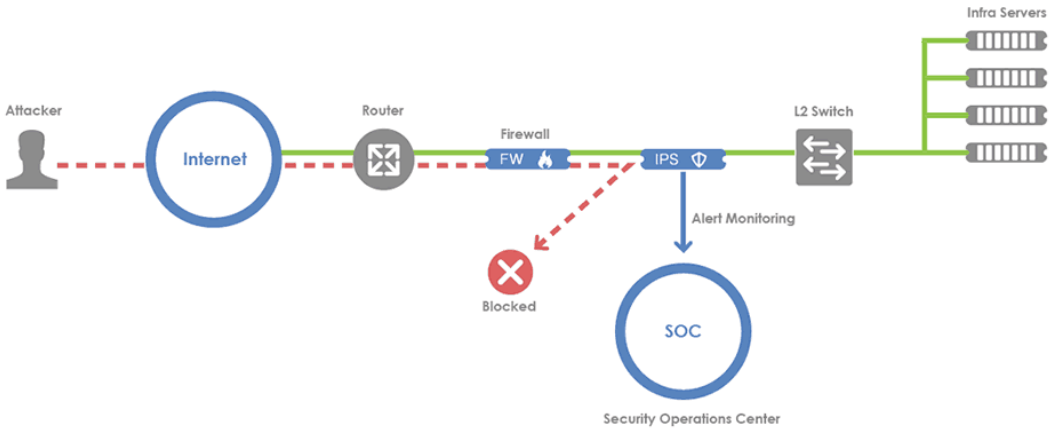


Kuva 3. Esimerkki miten ohjelmistojen liikenteen sekasotku selvitetään(Oversite sentry, 2015)

2.2.4 Integroitu Intrusion Protection System

IPS-järjestelmän tarkoituksena on huomata useita erilaisia hyökkäystekniikoita ja estää niiden vaikuttaminen verkkoon. Yleensä yrityksissä, joissa on käytössä perinteinen palomuuri, on myös käytössä Intrusion Detection System (IDS) tai IPS.

Nämä ovat yleensä erillisiä laitteita, kun taas NGFWssä ne ovat integroitu järjestelmään.



Kuva 4. Esimerkki miten erillinen IPS-laite estää hyökkäykset ja mihin se tulisi sijoittaa verkossa(Colt, 2015)

Tällä ei ole suurta eroa erilliseen laitteeseen paitsi se, että IPS saa paljon suuremman määrän dataa mistä tarkastaa mahdollisten hyökkäysten varalta. Integrointi lisää myös IPSn toimintanopeutta. (Ohlhorst, 2013)

IPS- ja IDS-laitteille tulee myös vastaan salattua dataa, jolle ne eivät voi mitään itsekseen, sillä ne eivät osaa purkaa suojausta. Tähän tarvitaan erillinen lisälaite, joka purkaa tai ei pura liikennettä riippuen siitä, miten se on ohjeistettu toimimaan. Tälläinen laite voi olla, joko passiivisena kuuntelijana, joka vain tarkistaa onko liikenne suojattua vai ei ja kirjaa sen lokiin. Tarkastuslaite voi myös olla aktiivisena osana verkkoa, joka tarkoittaa sitä, että se purkaa suojatun liikenteen, jos se on ohjeistettu tekemään niin ja siirtää sen tarkastuslaitteelle kuten IPS. (SANS instituutio, 2013)

2.2.5 Bridged- ja routed-tilat

Bridged- tai routed-tilojen käyttäminen ei ole uusi ominaisuus, mutta NGFWn toiminnan kannalta se on tärkeä ominaisuus. Nämä tilat ovat tärkeitä, sillä useasti yrityksissä on vielä käytössä perinteisiä palomuureja ja NGFW siirtyminen ei tapahdu kerralla, jonka takia NGFW tulee olla käytössä bridged-tilassa, jolloin NGFW itsessään ei näy osana reittiä ja menettää osan toiminnoistaan. Kun yrityksen

kaikki laitteet ovat saatu vaihdettua NGFW-pohjaiseen ratkaisuun, voidaan niiden tila vaihtaa routed-tilaan, mutta tämä ei tapahdu ihan niin helposti, sillä se vaatii uudelleen configurointia. (Ohlhorst, 2013)

3 NGFW-LAITTEIDEN VERTAILU

Markkinoilla on useita erilaisia NGFW-ratkaisuja. Niissä on useimmiten pieniä eroja, joilla ne markkinoivat itseään parempana kuin muut. Useimmin seuraavat asiat ovat ne, jotka eroavat eniten laitteiden välillä ja tulisi tarkastaa, että ne ovat juuri ne, jotka täyttävät niille asetetut tarpeet.

1. Suojaako NGFW palvelin- ja client-pohjaisia hyökkäyksiä vastaan ja mikä on sen onnistumisprosentti?
2. Onko mahdollista ohittaa NGFW-laite jotenkin?
3. Onko NGFW-laite luotettava ja tasapainoinen?
4. Ylläpitääkö NGFW-laite sisään- ja ulostulevien ohjelmistojen käytänteitä?
5. Ylläpitääkö NGFW-laite sisään- ja ulostulevien identiteettien käytänteitä?
6. Mikä on NGFW-ratkaisun suorituskyky.

(Wilkins, 2014)

3.1 Cisco FirePOWER 8350

Ciscon FirePOWER sarja on tullut tarjolle, kun Cisco hankki Sourcefiren. Ciscon FirePOWER 8300 sarjan laitteet voidaan asettaa olemaan joko NGFW, next generation intrusion protection järjestelmä (NGIPS) tai advanced malware protection (AMP) erikseen taikka itsenäisesti. Tämän sarjan laitteista 8350 on alin malli ja sen yläpuolella ovat 8360, 8370 ja 8390. 8300-sarjan alapuolella on myös 8200- ja 8100-sarjat sekä Ciscon alkuperäinen Adaptive Security Appliance (ASA). ASA-sarjan laitteet ovat ensimmäisen sukupolven NGFW-laitteita, jonka takia ne tarvitsevat päivityksen, jotta niitä voi käyttää kunnon NGFW-laitteena. (Cisco, 2015)

Cisco FirePOWER 8350	
Palvelinhyökkäysten esto %	99.5%
client-hyökkäysten esto %	99%
Ohitettavissa	Ei ole
Luotettava toiminta	Kyllä
Ohjelmistokäytänteiden ylläpito	Kyllä
Identiteettikäytänteiden ylläpito	Kyllä
IPS-läpäisynopeus	15 Gbps
Verkon läpäisynopeus	30 Gpbs
Suojauksen hinta per Mbps	20.03$
Kahdennettu virransyöttö	Kyllä
Virrankulutus	635-1000W
Pinottava	Kyllä neljään saakka
Räkkitila per yksikkö	2U

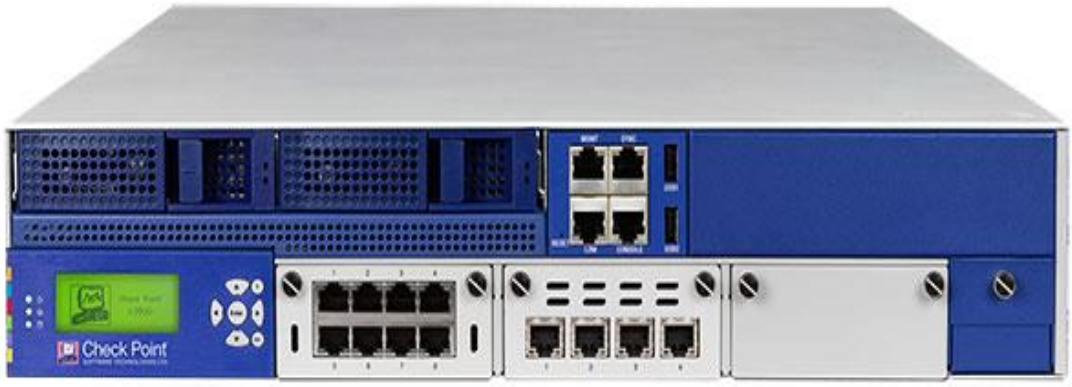
Kuva 5. Cisco FirePOWER 8350-laitteen etupaneeli. (Cisco, 2015)

3.2 CheckPoint 13500

CheckPointin 13500-laite on osa 13000-sarjaa, tähän sarjaan kuuluu myös 13800-laite. CheckPoint on pitkän historian omaava yritys, joka tarjoaa luotettavia tietoturvaratkaisuja. CheckPointin palomuurit kuuluvat yksiin eniten käytössä olevista palomuuriratkaisuista. (Wilkins, 2014)

13000-sarjan laitteet voidaan ottaa käyttöön neljässä eri toiminnossa riippuen tarpeesta. Toiminnot ovat NGFW, next generation threat prevention (NGTP), next generation secure web gateway (NGSWG) ja next generation data protection (NGDP). Nämä toiminnot voidaan ottaa käyttöön erikseen taikka itsenäisesti riippuen valitusta blade-paketista. (Check Firewalls, 2015)

CheckPoint 13500	
Palvelinhyökkäysten esto %	97.1%
client-hyökkäysten esto %	95.9%
Ohitettavissa	Ei ole
Luotettava toiminta	Kyllä
Ohjelmistokäytänteiden ylläpito	Kyllä
Identiteettikäytänteiden ylläpito	Kyllä
IPS-läpäisynopeus	5.7 Gbps
Verkon läpäisynopeus	23.6 Gpbs
Suojauksen hinta per Mbps	21.45$
Kahdennettu virransyöttö	Kyllä
Virrankulutus	431W
Pinottava	Ei ole
Räkkitila per yksikkö	2U



Kuva 6. CheckPoint 13500-laitteen etupaneeli (Check Firewalls, 2015)

3.3 Fortinet FortiGate-3600C

Fortinetin FortiGate-3600C on osa Fortigate 3000-sarjaa. FortiGate 3000-sarjaan kuuluvat seuraavat laitteet FortiGate-3040B, FortiGate-3140B, FortiGate-3240C, FortiGate-3600C, FortiGate-3700D, FortiGate-3810A ja FortiGate-3950B. FortiGate-3600C voidaa ottaa käyttöön NGFWnä, perinteisenä palomuurina, virtual private network (VPN) terminoijana ja next generation intrusion protection järjestelmänä. (Fortinet, 2015)

Fortinet FortiGate-3600C	
Palvelinhyökkäysten esto %	97%
client-hyökkäysten esto %	91.8%
Ohitettavissa	Ei ole
Luotettava toiminta	Kyllä
Ohjelmistokäytänteiden ylläpito	Kyllä
Identiteettikäytänteiden ylläpito	Kyllä
IPS-läpäisynopeus	15 Gbps
Verkon läpäisynopeus	60 Gpbs
Suojauksen hinta per Mbps	8.30$
Kahdennettu virransyöttö	Kyllä
Virrankulutus	615W
Pinottava	Ei ole
Räkkitila per yksikkö	3U

Kuva 7. Fortinet FortiGate-3600C-laitteen etupaneeli (Fortinet, 2015)

3.4 WatchGuard XTM1525

WatchGuardin XTM1525 on osa 1500-sarjan laitteita, johon kuuluu myös 1520 ja 2520. XTM1525 voidaan ottaa käyttöön NGFWnä, virtual private network terminaattorina, next generation Intrusion Protection järjestelmänä tai unified threat management (UTM) laitteena (WatchGuard, 2015)

Kuva 8. WatchGuard XTM1525-laitteen etupaneeli (WatchGuard, 2015)

WatchGuard XTM1525	
Palvelinhyökkäysten esto %	96.7%
client-hyökkäysten esto %	98.7%
Ohitettavissa	Ei ole
Luotettava toiminta	Kyllä
Ohjelmistokäytänteiden ylläpito	Kyllä
Identiteettikäytänteiden ylläpito	Kyllä
IPS-läpäisynopeus	13 Gbps
Verkon läpäisynopeus	25 Gpbs
Suojauksen hinta per Mbps	11.87$
Kahdennettu virransyöttö	Kyllä
Virrankulutus	130W
Pinottava	Ei ole
Räkkitila per yksikkö	1U

3.5 Dell SonicWALL SuperMassive E10800

Dell SonicWALL SuperMassive E10800 on osa SuperMassive-sarjaa johon kuuluu niin 9000-sarjan laitteet kuin 10000-sarjan laiteet. Dell sai nämä omistukseensa, hankittuaan SonicWALLin. SuperMassive E10800 voi ottaa käyttöön NGFWnä, virtual private network terminaattorina, next generation intrusion protection järjestelmänä taikka unified threat management laitteena. (Dell, 2015)

Dell SonicWALL SuperMassive E10800	
Palvelinhyökkäysten esto %	96.4%
client-hyökkäysten esto %	99.1%
Ohitettavissa	Ei ole
Luotettava toiminta	Kyllä
Ohjelmistokäytänteiden ylläpito	Kyllä
Identiteettikäytänteiden ylläpito	Kyllä
IPS-läpäisynopeus	28 Gbps
Verkon läpäisynopeus	40 Gpbs
Suojauksen hinta per Mbps	15.046$
Kahdennettu virransyöttö	Kyllä
Virrankulutus	750W
Pinottava	Ei ole
Räkkitila per yksikkö	4U

Kuva 9. Dell SonicWALL SuperMassive E10800 -laitteen etupaneeli (Dell, 2015)

4 YRITYKSEN TARPEIDEN MÄÄRITTELY

4.1 NGFW-laitteen hankinnan kannattavuus

Ennen NGFW-laitteen hankintaa tulee ottaa huomioon yrityksen tarpeet. Joillekin yrityksille perinteiset palomuurit, intrusion prevention järjestelmät ja niitä tukevat reitittimet ja kytkimet ovat tarpeeksi. Tämän tason suoja tosin ei ole tarpeeksi kaikille, jolloin tulee arvioida onko perinteiset palomuurit tarpeeksi, vai tulisiko hankkia verkonsuojalaitteita taikka NGFW-laitteita.

Alan asiantuntijat ovat sitä mieltä, että minimi mitä yritys tarvii tietosuojan osalta on palomuuri, intrusion prevention-järjestelmä, anti-virus-ohjelmisto, haittaohjelmasuoja, intrusion detection-järjestelmä ja jonkinlainen langaton suojaus. NGFW-laite täyttää nämä kaikki vaatimukset ja hieman enemmän.

Tapauksessa jossa yritys valitsee hankkia jokaiseen näistä tarpeista erillisen laitteen tarkoittaa sitä, että laitteita tulee olemaan useita, jolloin niiden kaikkien yksittäinen hinta, huolto ja suojaus tulee laskea yhteen ja vasta sitten verrata vastaan ratkaisua, jossa on vain yksi ylläpidettävä suojaratkaisu usean sijaan. Jokaiselle suojamuodolle erillistä laitetta käytettäessä tulee myös huomioida, että tämä vaatii enemmän työtä integroida, ylläpitää ja kouluttaa, jotta saadaan tarvittava tietosuojataso jokaisen laitteen kohdalle.

Yrityksien tulee myös tarkastaa tämän hetkinen tietoverkko-infrastruktuurinsa ja riskianalyysinsä, jotta yritys voi päättää onko yksittäiset laitteet vai keskitetty NGFW oikeampi ratkaisu. NGFW:llä on myös etunaan se, että se tarjoaa yhden laitevalmistajan kautta koko arkkitehtuurin ja hallintakäyttöliittymän. Tämä tuo säästöjä vähemmän työn muodossa, sillä kun kaikki raportointi ja hallinta on yhdennetty tarkoittaa se sitä, että data on helposti luettavaa ja tulkattavaa, jolloin kuluu vähemmän aikaa raporttien lukemisessa ja tulkkaamisessa.

Kaikki tosin ei ole parempaa NGFW-laitteiden kannalta, sillä yhteen laitteeseen koko verkontietoturvan integrointi tuo mukanaan tietynlaisia ongelmiakin ainakin alussa. Verkon tietoturvan siirtäminen NGFW-laitteelle ei ole halpaa ja verkon infrastruktuurin uusiminen on suurta vaivaa vaativa työ. Tämä voi joissain tapauksissa olla liian suuri hinta verkon tietoturvan yhdistämiselle, varsinkin jos vaihdettaviin laitteisiin on sijoitettu kohtuullisia summia rahaa.

Mikäli yritys pystyy ylittämään kaikki nämä haasteet, on sillä edessään huomattavia säästöjä ei vaan rahallisesti, mutta myös ajallisesti. Tämä tarkoittaa sitä, että ainoa estävä tekijä on sitoutumiskyky ratkaisun hankintaan ja yrityksen resurssit. (Villegas, 2015)

4.2 IT-strategia

Yrityksen IT-strategian tavoitteena on helpottaa tietohallinnon johtamista ja luoda selvät toimintamallit. IT-strategian tarpeellisuus korostuu, kun tietohallinto saa eteensä suuren muutoksen, kuten tulisiko yrityksen hankkia NGFW-laite vai pitää tarpeelliset toiminnot erillisissä laitteissa. Ilman selkeää IT-strategiaa saattaa yrityksen kehitystä heikentäväksi tekijäksi jäädä tietohallinto. IT-strategian sisältämien periaatteiden, toimintamallien ja kokonaisarkkitehtuuria koskevien kohtien ja tietohallinnon kustannuksien hallussapito mielessä pitäen tulee valita, onko NGFW-laitteen hankinta oikea ratkaisu, vai kykeneekö yritys toiminaan jollain pienemmällä ratkaisullakin. (Tietomalli.fi, 2012)

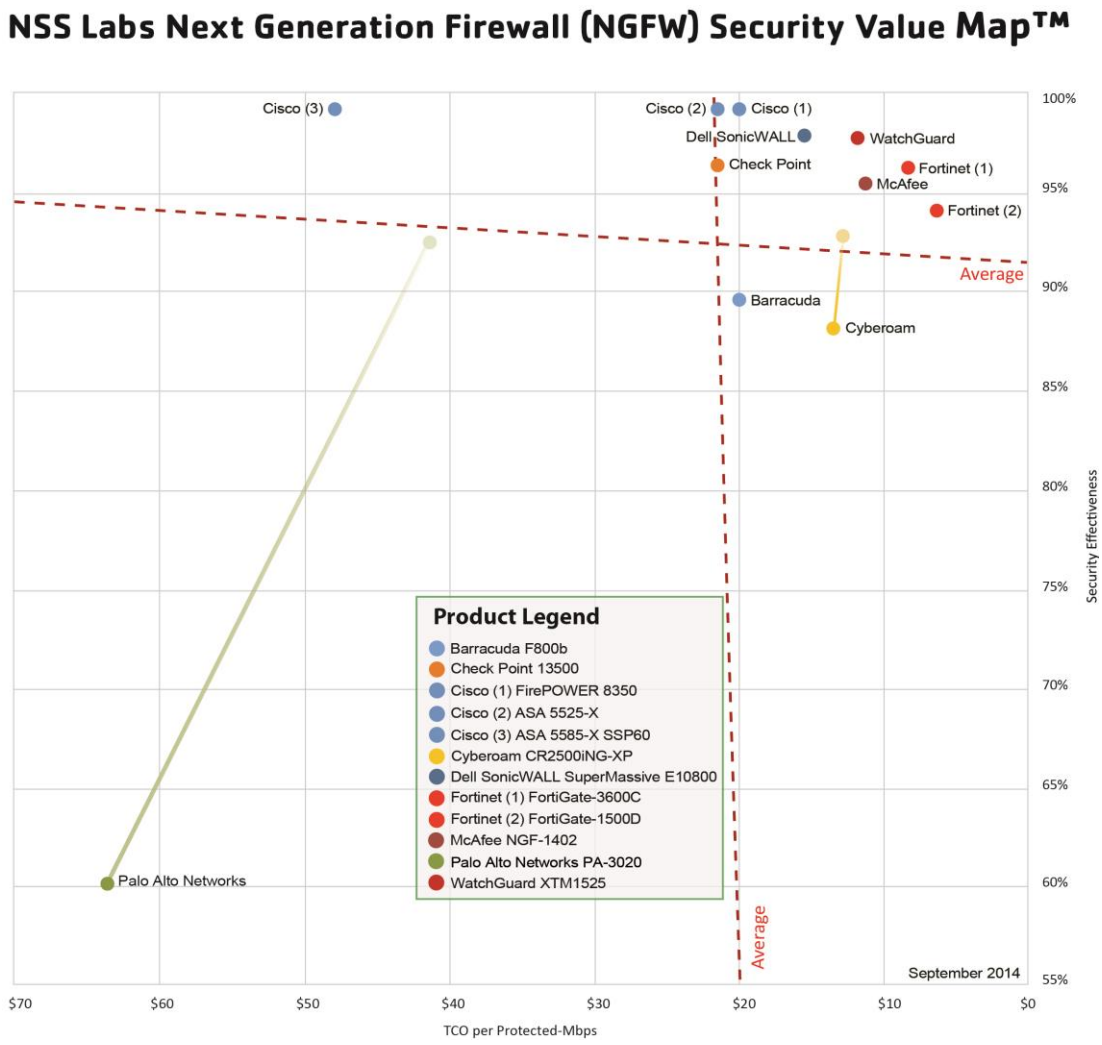
IT-strategiaa hyödyntäen tulee myös päättää onko kaikki NGFW-laitteen tarjoamat ominaisuudet tarpeellisia vai sisältääkö se joitakin ominaisuuksia, joita yritys ei tarvitse. Tapauksissa, joissa yritys ei tarvitse kaikki NGFW-laitteen tarjoamia palveluita, kannattaa harkita NGFW-laitteen hankintaa, jossa on kaikki tyypilliset ominaisuudet, joita NGFW-laitteella tulee olla, mutta ominaisuuksien aktivointi maksaa erikseen tuotteessa, jolloin voidaan luoda säästöjä jättämällä hankintahetkellä turhat ominaisuudet aktivoimatta. (Villegas, 2015)

4.3 NGFW-laitteen valintakriteerit

NGFW-laitetta valitessa yritykselle valinta yleensä päätetään pienten eroavaisuuksien avulla. Tämä johtuu siitä, että suurin osa NGFW-laitteista on melko samanlaisia ja hoitavat samat toiminnot. Tästä johtuen yleensä NGFW-laitteen valinta tehdään omien tottumuksien ja kokemuksien pohjalta. Nämä kokemukset ovat joskus fakta-pohjaisia ja joskus ne ovat ihan vaan puhepohjaisia, mutta silti ne vaikuttavat laitetta valittaessa.

Tuotetta valittaessa tärkeitä tekijöitä ovat tuotteen tehokkuus hyökkäysten estämisessä, mikä on nähtävissä edellä olevissa tauluissa kahdessa ensimmäisessä kentässä. Vaikka näiden arvojen ero on pieni, saattaa tämä pienikin ero olla erottava tekijä onnistuneen ja epäonnistuneen hyökkäyksen välillä.

Yksi tärkeä tekijä tehokkuuden lisäksi on myös, että laitteella on tarpeeksi suuri läpäisynopeus. Tämä tekijä ei ole suoraan verrattavissa laitteiden välillä, sillä laitteiden kapasiteettierot ovat erittäin suuriakin välillä. Parempi mittari tähän vertailuun on kuvan 9. tapainen esitys, josta nähdään paljonko laite maksaa per suojattu Mbps. Tämän tapaista vertailua käyttäessä on helppo verrata kalliita ja halpojakin laitteita toisiinsa, jolloin on helpompi päättää mikä laitteista sopii parhaiten sille tarkoitettuun ympäristöön ja budjettiin. (Wilkins, 2014)



Kuva 10. Graafi eri yrityksien NGFW-laitteiden hinnasta per suojattu Mbps. (WatchGuard, 2014)

Näiden lisäksi tulee vielä ottaa huomioon, kuinka paljon laite vie tilaa ja energiaa. Tässäkään kohdassa tuotteet eivät ole suoraan verrattavissa, jolloin on hyödynnettävä erilaista vertaustapaa, kuten jaetaan laitteen kuluttama energian määrä laitteen koolla. (Wilkins, 2014)

5 NGFW-LAITTEEN TULEVAISUUS

Kun proxy palomuurien suosio alkoi laskea 90-luvun jälkeen tarvittiin jotain, joka tarjoaisi saman tason suojaa, kuin proxy palomuurit, mutta olisi laajennettavampi ja älykkäämpi. Tämä tarve toi markkinoille NFGW-laitteet, jotka olivat parempia ja laajennettavia, kuin sen hetken suosituin ratkaisu.

Tällä vuosituhannella tosin on tullut uusi trendi, jolla on etunsa ja haittansa. Tämä uusi trendi on palveluiden ulkoistaminen. Nykyään yritykset voivat ulkoistaa melkein kaiken, mihin se ennen tarvitsi laitteistoa, kuten verkkosivut ja tiedostojen varmistus ja varastointi. Tätä voidaan myös käyttää tietoturvan ulkoistamiseen, jolloin kaikki liikenne ohjataan palveluntarjoajan pilven läpi, jossa he hoitavat samat toiminnot kuin NGFW-laite ja muut verkon suojauslaitteet.

Tämän tavan hyötyihin kuuluu se, että laitteilla on toiminta takaus palveluntarjoajalta, jolloin ne ovat melkein sataprosenttisesti kokoajan tarjolla. Tämä myös vähentää alustavia hankinta kustannuksia, sillä laite hankintoja ei tarvitse suorittaa. Tämä myös on mahdollista siirtää vallan palveluntarjoajan hallintaan, jolloin saadaan säästöjä ajallisesti.

Tämän tapaisella ratkaisulla on myös haitta puolensa. Näitä haittoja ovat esimerkiksi se, että olet sidottuna internet yhteytesi tarjoavan tahon tukemiin palveluihin. Yhtenä ongelmana tulee myös se, että yrityksen liikenne ei ole ainoa, mitä tämä pilventarjoaja hoitaa. Tämä johtaa siihen, että he eivät ole niin tutustuneita yrityksesi sisäisiin tapoihin ja menettelyihin, jotka saattavat vaikuttaa verkkoliikenteeseen. Tämä johtaa siihen, että he eivät voi tarjota niin hyvää palvelua, kuin yrityksen oma IT-henkilöstö.(Burke, 2011)

6 YHTEENVETO

Palomuurit ovat olleet ja ovat tärkeä osa verkon tietoturvaa. Palomuuritekniikoita on useita erilaisia ja kun tekniikka kehittyy tulee todennäköisesti niiden muoto muuttumaan useaan kertaan jatkossakin. Perinteisesti palomuurit ovat olleet vain yksi osa verkko, joka estää haitallisen liikenteen sisään tai ulospääsyn portteja sulkemalla tai avaamalla ne halutulle liikenteelle.

Perinteisistä palomuureista onkin helppo siirtyä aikajanassa seuraavaan ratkaisuun eli seuraavan sukupolven palomuureihin. Seuraavan sukupolven palomuurit ovat ominaisuuksiltaan ja toiminnoiltaan erittäin houkutteleva ratkaisu, mutta ovat hintava sellainen. Tutkiessani olen huomannut, että markkinoilla on useita eri ratkaisuja, melkein jokaisen niin pienenkin kuin suurenkin yrityksen taikka organisaation tarpeisiin. Tutkiessani sain myös selville, että IT-strategian olemassa olo, on erittäin tärkeää, sillä se auttaa yrityksen laitetarpeiden määrittelyssä. Mikäli IT-strategia ei ole olemassa, saattaa tarpeiden kartoituksesta tulla erittäin vaikeaa.

Aihetta tutkiessani löysin myös uusia ideoita, kuten pilveen palomuurilaitteiden ulkoistamisen. Tämän tapainen ratkaisu tuo yrityksille mahdollisuuden ulkoistaa melkein kaikki toimintonsa verkkoon. Tämä on erittäin hyvä toteutus tapa nyky maailmassa, sillä tekniikka kehittyy kokoajan ja laitteet vanhenee entistä nopeammin.

LÄHTEET

Check Firewalls. (2015) Check Point 13500 Appliance Viitattu 14.11.2015
http://www.checkfirewalls.com/13500.asp

Cisco. (2015). Cisco FirePOWER 8000 Series Appliances Data Sheet Viitattu 14.11.2015
http://www.cisco.com/c/en/us/products/collateral/security/firepower-8000-series-appliances/datasheet-c78-732955.html

Dell. (2015). Sonic WALL SuperMassive E10000 Series. Viitattu 14.11.2015
http://www.sonicwall.com/products/sonicwall-supermassive-e10000/

Fortinet. (2015). FortiGate 3600C Viitattu 14.11.2015
http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-3600C.pdf

Ohlhorst, F. (1.3.2015). Next-Generation Firewalls 101. Viitattu 6.11.2015
http://www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097

Tietomalli.fi. (11.11.2012). Strategia ja Hallinto. Viittattu 15.11.2015
https://www.tietohallintomalli.fi/malli/strategia-ja-hallinto/johdanto

WatchGuard. (2014). Kuva 9. Viitattu 15.11.2015
http://www.watchguard.com/news/press-releases/nss-2014.jpg

WatchGuard. (2015). WatchGuard® XTM 1520, 1525 and 2520. Viitattu 14.11.2015
http://www.watchguard.com/docs/datasheet/wg_xtm1500-2500_ds.pdf

Wilkins, S. (23.11.2014). A Guide to Choosing a Next-Generation Firewall. Viitattu 2.11.2015
http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html

Villegas, M. O. (2.2015). Three things to consider before deploying a next-generation firewall. Viitattu 15.11.2015
http://searchsecurity.techtarget.com/feature/Three-things-to-consider-before-deploying-a-next-generation-firewall

Palo alto Networks(2015).What is a firewall?. Viitattu 18.11.2015
https://www.paloaltonetworks.com/resources/learning-center/what-is-a-firewall.html

SANS instituutio(2013).Finding Hidden Threats by Decrypting SSL. Viitattu 18.11.2015
https://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840

Oversite sentry. (2015). Kuva 1. Viitattu 7.11.2015
http://oversitesentry.com/wp-content/uploads/2015/05/basic-networkdiagram.png

Medialab. (ei pvm.) Kuva 2. Viitattu 21.11.2015
http://medialab.di.unipi.it/web/doc/JNetSec/jns_ch12-18.gif

Oversite sentry. (2015). Kuva 3. Viitattu 8.11.2015
http://oversitesentry.com/wp-content/uploads/2015/06/ngfw_large-sonicwall.jpg

Colt. (2015). Kuva 4. Viitattu 8.11.2015
http://www.kvhasia.com/images/intrusion_prevention_system.gif

Cisco. (2015). Kuva 5. Viitattu 14.11.2015
http://www.cisco.com/c/dam/en/us/products/security/firepower-8000-series-appliances/product-large.jpg

Check Firewalls. (2015). Kuva 6. Viitattu 14.11.2015
http://www.checkfirewalls.com/images/13500/13500.jpg

Fortinet. (2015). Kuva 7. Viitattu 14.11.2015
http://www.fortinet.com/sites/default/files/productimages/FG-3600C.png

Watchguard. (2015). Kuva 8. Viitattu 14.11.2015
http://www.247watchguard.com/wp-content/uploads/2014/09/xtm1500_rt.jpg

Dell. (2015). Kuva 9. Viitattu 14.11.2015
http://www.sonicguard.com/images/SuperMassive/E10000-side.jpg

John Burke. (11.11.2011). The Pros and Cons of a Cloud-Based Firewall. Viitattu 19.11.2015
http://www.networkworld.com/article/2221089/infrastructure-management/the-pros-and-cons-of-a-cloud-based-firewall.html

Vangie Beal (28.11.2005) Network Security Appliances Explained Viitattu 21.11.2015
http://www.webopedia.com/quick_ref/network_appliance.asp

Brad Casey. (4.2014). UTM vs. NGFW: Comparing unified threat management, next-gen firewalls. Viitattu 21.11.2015
http://searchsecurity.techtarget.com/answer/UTM-vs-NGFW-Comparing-unified-threat-management-next-gen-firewalls