VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Tomi Urho

KESKITETTY PALOMUURIJÄRJESTELMÄ

Tekniikka ja liikenne
2013

VAASAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Tomi Urho
Opinnäytetyön nimi	Keskitetty palomuurijärjestelmä
Vuosi	2013
Kieli	suomi
Sivumäärä	33 + 2 liitettä
Ohjaaja	Kalevi Ylinen

Tämä opinnäytetyö on tehty Anvia Yrityspalvelut Oy:n Tuotehallintayksikön Tietoliikenneosastolle. Anvia Yrityspalveluiden tarjoama palomuuripalvelu oli toteutettu erillisillä palomuurilaitteilla, joiden toimitukseen ja ylläpitoon haluttiin helpotusta. Lisäksi haluttiin tuottaa uusia yritysasiakkaille tarjottavia palveluita. Ratkaisuksi valittiin keskitetty palomuurijärjestelmä, joka mahdollistaa palomuuripalveluiden tuottamisen keskitetysti. Hankittu palomuurijärjestelmä mahdollistaa myös UTM-toiminnot, joiden avulla uusia palveluja voidaan tuottaa.

Palomuurilaitevalmistajan valinnassa tehtiin vertailuja monen valmistajan välillä. Laitevalinta perustui valmistajan kykyyn toteuttaa UTM-ratkaisuja sekä laitevalmistajan hyvään maineeseen.

Varsinainen palomuuriklusterin kytkentä operaattoriverkkoon suunniteltiin ja kytkettiin siten, että siinä otettiin huomioon mahdollisimman suuri vikasietoisuus. Palomuurilaitteen mahdollistamat UTM-toiminnot todettiin toimivan hyvin ja ne pystyttiin toteuttamaan Anvian tarjoamiin yritysliittymiin.

Avainsanat palomuuri, keskitetty palomuurijärjestelmä, yhtenäinen tietoturvauhkien hallinta

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikan koulutusohjelma

ABSTRACT

Author	Tomi Urho
Title	Centralized Firewall System
Year	2013
Language	Finnish
Pages	30 + 2 Appendices
Name of Supervisor	Kalevi Ylinen

This thesis is done to Anvia Yrityspalvelut Oy's product management of telecommunication department. Anvia Yrityspalvelut offers firewall services based on distributed firewalls. New centralized firewall system is going to replace the old firewall service and with the new firewall service Anvia is looking more cost efficient model starting with installing and maintenance times. With new firewall system there is also possible to offer new services to the customers. Firewall system is capable of next generation firewall, UTM features.

The Firewall manufacturer selection was done after the comparison between many of the firewall manufacturers. Selection was based on the ability to execute UTM functions and on a good reputation of the manufacturer.

Actual connecting of the firewall cluster to the operator's core network was planned and connected so that there is considered great fault tolerance. Firewall systems UTM functions where tested and stated to function very well and able to implement existing enterprise connections.

Keywords Firewall, centralized firewall system, unified threat management

SISÄLLYS

MERKINNÄT JA LYHENTEET

Application Control	Sovellushallinta -toiminnolla voidaan esimerkiksi rajata tietyn sovelluksen saamaa kaistanmäärää tai estää sen käyttö kokonaan.
AV	Antivirustoiminne palomuurilaitteessa.
CAT6	Category 6, Ethernet-kaapeli.
CPE	Customer Premise Equipment, asiakaspäätelaite.
CLI	Command Line Interface, merkkipohjainen hallintasovellus.
DHCP	Dynamic Host Configuration Protocol, laitteiden dynaaminen osoitteiden määrittely.
HA	High Availability. Tarkoituksena on taata laitteelle tai palvelulle korkea käytettävyys, joka ei ole koskaan pois käytöstä. Ei standardi. Valmistajakohtaisia toteutuksia. Käytetään myös tietojärjestelmien suunnittelussa ja toteutuksessa.
HTTPS	TLS-salattu http-verkkoliikenne.
IETF	Internet Engineering Task Force, internetin standardointia hoitava elin.
IIS	Internet Information Services, Microsoftin web-palvelin.
IPS	Intrusion Prevention System, hyökkäyksenestojärjestelmä. Tunnistaa sovelluksien haavoittuvaisuudet ja estää niiden hyväksikäytön.
IPsec	Internet Protocol Security, määrittelee puitteet tietyille protokollille tietoturvallisten yhteyksien toteuttamiseen.

LACP	Link Aggregation Control Protocol. IEEE 802.3ad -standardi useamman Ethernet-portin yhdistämiseen.
LAG	Link Aggregation Group, looginen porttiryhmä 2 + n kytkinportille.
Loop	Tietoliikenneyhteyksissä syntyvä silmukka, joka aiheuttaa vian ja estää yhteyksien käytön.
MPLS	Multiprotocol Label Switching, MPLS-työryhmän määritelmä etikettien käyttöön pohjautuva protokolla.
NAT	Network Address Translation, yksityisten verkko-osoitteiden muuttaminen julkisiksi verkko-osoitteiksi.
OSI-malli	ISO International Standardization Organization kehittämä hierarkkinen malli tietoliikenneyhteyksille.
PW	Pseudowire, teennäinen johto. VPLS-yhteydestä käytettävä nimitys.
SFP	Small Form-factor Pluggable, moduli yhteyksien kytkemiseen laitteiden välillä.
SHG	Split horizon group, estää verkkosilmukoiden syntymisen.
SSH	Secure shell –protokolla, salattu yhteysmuoto, jota käytetään yleensä merkkipohjaisissa yhteyksissä.
SSL	Secure Sockets Layer, internetyhteyksissä käytettävä salausprotokolla.
TLS	Transport Layer Security, käytetään kahden laitteen välisen yhteyden salaamiseen.

UTM	Unified Threat Management, tietoturvauhkien hallinnasta käytettävä termi. Määritelmä koostuu useista eri tietoturvatoiminteista.
VDOM	Virtual domain. Fyysisen palomuurilaitteen sisällä toimiva virtuaalinen palomuuri, jolla on omat palomuuritoiminteet ja reititysominaisuudet.
VLAN	Virtual Local Arena Network, virtuaalinen lähiverkko.
VoIP	Voice over IP, IP-verkossa kulkeva puheliikenne.
VPLS	Virtual Private LAN Service, MPLS-verkon toiminne. Sillattu L2-tason yhteys 1 + n liittymien välillä.
VPN	Virtual Private Network, virtuaalinen yksityinen verkko.
VRF	Virtual Routing and Forwarding, virtuaalinen reititin.
Web filter	Sisällönsuodatustoiminne. Estää web-liikenteen määritetyille sivustoille tai kategorioidun valinnan mukaan, esimerkiksi aikuisviihde.

KUVIO- JA TAULUKKOLUETTELO

LIITELUETTELO

1 JOHDANTO

Tämä opinnäytetyö on tehty Anvia Yrityspalvelut Oy:lle. Anvia Yrityspalveluiden Tuotehallinta vastaa yrityksille myytävistä yritystuotteista. Palomuuripalvelun tuotteistus- ja tuotevastuu on Tuotehallinnan Tietoliikenneyksiköllä, jossa nähtiin tarpeelliseksi tuoda markkinoille uusia palveluita tavanomaisen palomuuripalvelun tilalle. Palomuuripalvelulla tarjotaan suojausta yritysasiakkaiden sisäverkon laitteille ja sovelluksille. Hankittu palomuurijärjestelmä tarjoaa uusia suojausmekanismeja tietoturvauhkia vastaan, joita kutsutaan toisen sukupolven palomuuritoiminnoiksi. Lisäksi palomuuripalvelulla voidaan toteuttaa tietoturvallisia VPN-etäyhteyksiä.

1.1 Anvia Oyj

Anvian juuret ovat paikallisessa puhelintoiminnassa, josta konserni on laajentunut laaja-alaiseksi viestintäteknologian toimittajaksi. Oy Waasan telefooniyhdistys perustettiin vuonna 1882 ja oli tällöin viides puhelinyhtiö Suomessa Turun, Tampereen, Helsingin ja Viipurin jälkeen. /1/

Anvialla on nykyään kolme liiketoiminta-aluetta; ICT, turva ja TV –liiketoiminta-alue. Anvia muodostuu Anvia Oyj:sta (entinen Vaasan läänin puhelin Oy) ja sen tytäryhtiöistä, joka työllistää noin 700 henkilöä. /2/

Anvia Yrityspalvelut toimittaa ICT-kokonaispalveluja yrityksille ja yhteisöille. Anvia Yrityspalveluilla on toimipisteitä Helsingissä, Kokkolassa, Seinäjoella, Tampereella, Turussa ja Vaasassa.

1.2 Opinnäytetyön sisältö

Tämän opinnäytetyön aiheena on keskitetty palomuurijärjestelmä. Työssä perehdytään palomuurijärjestelmän kytkemiseen operaattorin verkkoon sekä uuden sukupolven palomuuriominaisuuksiin. Opinnäytetyö sisältää myös laitteiden konfiguroinnit, mutta niitä ei tässä työssä tuoda julki, koska ne saattaisivat paljastaa

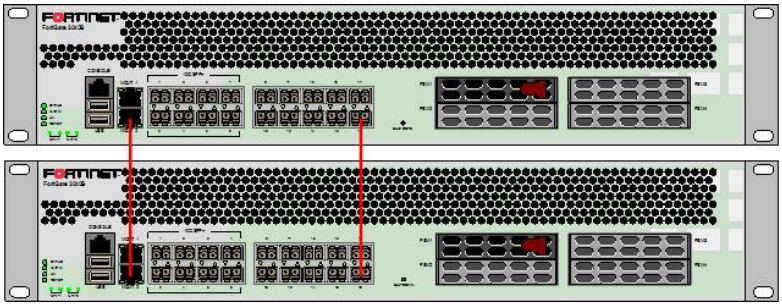
yksityiskohtaista tietoa. Anvia ICT:ssä tehtiin päätös tuottaa palomuuripalvelut keskitetysti sen omasta tietoliikenneverkosta. Palomuuripalveluiden tuottamiseksi on hankittu palomuuriklusteri, jossa on riittävästi suorituskykyä useille yritysasiakkaille. Palomuuriklusteri sisältää kaksi palomuurilaitetta, jotka on sijoitettu ja kytketty operaattorin verkkoon siten, että siinä on pyritty huomioimaan mahdollisimman suuri vikasietoisuus sekä tuotettavien palveluiden kapasiteetin tarve. Lisäksi on hankittu erillinen raportointijärjestelmä, jolla voidaan tuottaa tietoliikenneraportteja palveluun liitetystä asiakkaan yritysliittymästä. Tämän tyyppisistä palveluista, jotka tarjotaan verkosta palveluna, käytetään myös nimitystä pilvipalvelut.

Palomuuriklusteri mahdollistaa tavallisten palomuuritoimintojen lisäksi UTM–toiminnot eli toisen sukupolven palomuuritoiminnot. UTM-toimintoihin sisältyvät muun muassa antivirus, sisällönsuodatus, IPS ja sovellushallinta –toiminteet, joihin tässä työssä perehdytään tarkemmin. Laitteessa on myös mahdollista tehdä virtuaalisia palomuureja.

Anvian aiempi palomuuripalvelu oli toteutettu erillislaitteilla, jolloin jokaiselle yritysasiakkaalle on asennettu erillinen palomuuri asiakkaan laitetilaan, minne operaattorin tietoliikenneyhteydet on myös kytketty. Tämän tyyppisen palvelun tuottaminen ja ylläpito on työlästä ilman keskitettyä hallintajärjestelmää, josta voidaan hallita kaikkia palomuurilaitteita yhdestä järjestelmästä yhden näkymän alta. Palomuurien ohjelmistoversioiden päivittäminen oli hankalaa, koska kaikkia laitteita ei voinut päivittää yhtä aikaa, vaan ne oli tehtävä jokaiseen laitteeseen erikseen. Haasteita oli myös palvelun käyttöönotto- ja vikatilanteissa, kun asentajan täytyy käydä asiakkaan luona fyysisesti toimittamassa laite tai käydä selvittämässä vika paikan päällä. Tällä on suora vaikutus käyttöönotto- ja viankorjausaikoihin. Varastonhallinta pitää myös ottaa huomioon, koska varastossa täytyy pitää tietty määrä laitteita hyllyssä uusia tilauksia varten, ja siitä aiheutuu tilaus- ja varastointikuluja.

2 PALOMUURIKLUSTERIN KYTKENNÄT

Palomuuriklusteri muodostuu kahdesta tai useammasta fyysisestä laitteesta, jota hallitaan yhtenä kokonaisuutena eli se näkyy ylläpitäjälle yhtenä laitteena. Tässä tapauksessa klusteri sisältää kaksi palomuurilaitetta ja ne on kytketty toisiinsa kahden HA-linkin avulla (**Kuvio 1.**)



Kuvio 1. Palomuuriklusterin HA-kytkennät.

HA-linkkien tehtävänä on siirtää laitteiden välistä tietoa. Mikäli toinen palomuurilaite vikaantuu, toimii toinen laite edelleen, eikä vikaantuminen aiheuta haittaa asiakkaiden tietoliikenteelle. Käytännössä aktiivisista tietoliikenneyhteyksistä saattaa kadota muutama IP-paketti, kun yhteydet siirtyvät kunnossa olevalle palomuurilaitteelle.

Palomuuriklusteri voi olla Active-Passive tai Active-Active –tilassa, josta viimeisin on otettu käyttöön. Active-Active –tila mahdollistaa paremman suorituskyvyn, koska palomuuri siirtää tiettyjä IP-sessiota toiselle klusterissa olevalle palomuurille ja näin ollen tasaa resurssien käyttöä. Toinen peruste Active-Active –tilan käytölle on, mikäli laite vikaantuu näkyy se välittömästi toiminnassa, kun taas Active-Passive –tilassa olevan palomuuriklusterin Passive-laitteen tilaa on vaikea todeta. Passive (Slave) –tilassa oleva laite aktivoituu vasta silloin kun Active (Master) –tilassa olevaan palomuurilaitteeseen tulee vika ja se siirtää IP-liikenteen Passive-tilassa olevalle palomuurille ja siitä tulee Master-laite. Slave-tilassa olleen laitteen toiminta todetaan vasta vaihdon yhteydessä. Mikäli Slave-tilassa olevassa palomuurissakin on vika, keskeytyy koko palomuuriklusterin toiminta.

2.1 LACP-protokolla (IEEE 802.1AX-2008)

Palomuuriklusterin kytkemiseksi runkolaitteisiin käytetään LACP-protokollaa, joka mahdollistaa kahden tai useamman fyysisen ethernet-portin yhdistämisen yhdeksi loogiseksi ethernet-linkiksi. LACP on protokolla, joka on toteutettu OSI-mallin siirtoyhteyskerroksella (L2), ja sillä saadaan lisättyä tietoliikenneyhteyksien kapasiteettia tietyin rajoituksin. Kapasiteetin lisäksi LACP:lla saadaan parempi vikasietoisuus kuin yhdellä linkillä, koska LACP toimii vaikka yksi tai useampi fyysistä linkeistä olisi alhaalla olettaen, että yksittäinen LAG (Link Aggregation Group) ei ole kokonaan alhaalla. LACP-protokollalla yhteen liitetyistä porteista (ryhmä) käytetään lyhennettä LAG. /8/ LACP ei paranna yksittäisen yhteyden suorituskykyä eli suurin yksittäisen yhteyden siirtonopeus on sama kuin yhden fyysisen ethernet-linkin nopeus (tässä tapauksessa 1 Gbit/s). /3/

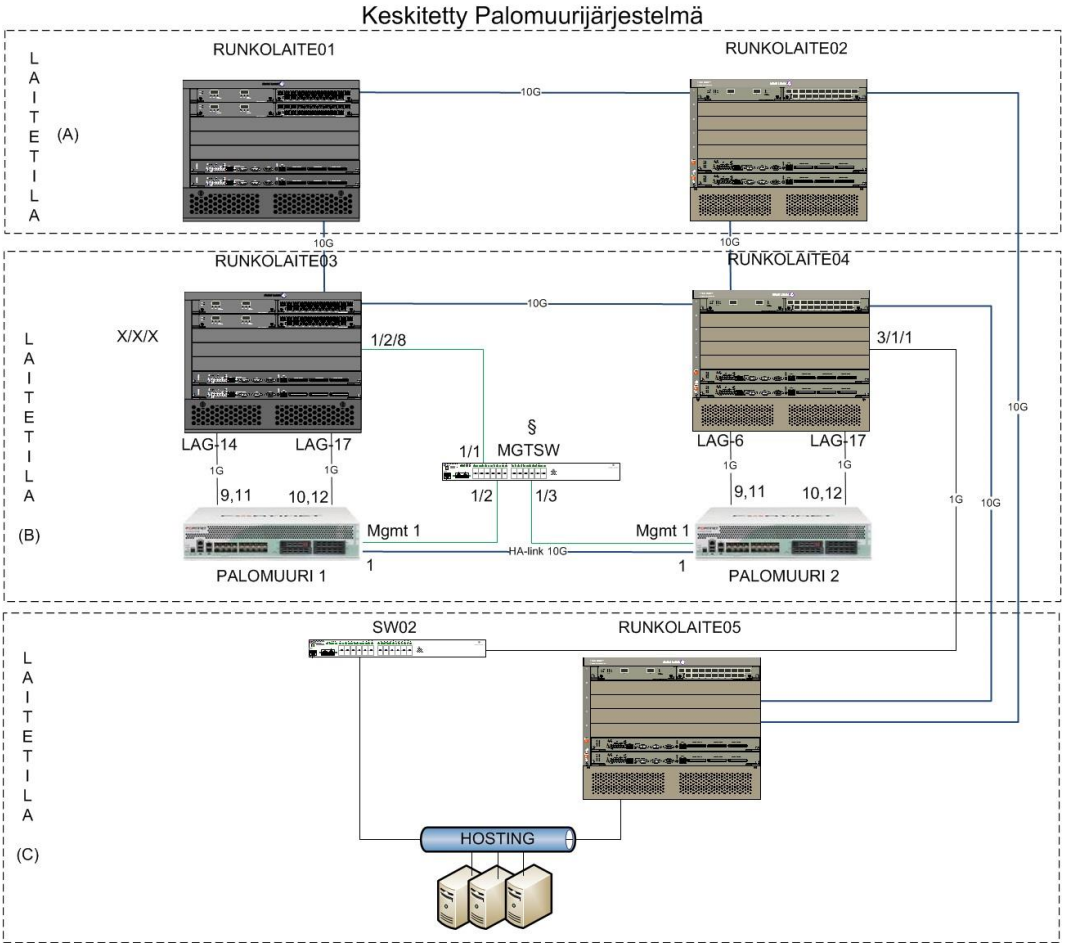
Molemmat palomuurilaitteet ovat kytkettynä 4 x 1 Gbit/s- yhteyksillä runkolaitteeseen eli yhteensä 4 Gbit/s kapasiteetilla (klusterin kokonaiskapasiteetti 8 Gbit/s). 4 Gbit/s kapasiteetti on jaettu vielä erikseen siten, että sisääntulevalle liikenteelle on varattu 2 Gbit/s kaista ja ulos lähtevälle liikenteelle 2 Gbit/s kaista. LACP ei välttämättä skaalaudu lineaarisesti porttimäärien mukaan eli esimerkiksi 1 Gbit/s + 1 Gbit/s –porttien yhdistämisellä ei aina saavuteta 2 Gbit/s kaistannopeutta, vaan todellinen kokonaisnopeus saattaa jäädä hieman sen alle. /3/ Myös erillisten porttien hallinta aiheuttaa ylläpitäjille jonkin verran ylimääräistä ylläpitotyötä.

LACP on hyvä protokolla kaistan lisäämiseksi, silloin kun ei ole saatavilla nopeampaa yksittäistä porttia esimerkiksi 10 Gbit/s, mutta se ei korvaa nopeampaa liityntää. /3/ LACP on suhteellisen helppo toteuttaa sekä laajentaa lisäämällä uusia portteja.

Kun palomuurilaitteita kytkettiin runkolaitteisiin huomattiin, että osa LACP-porteista oli half duplex –tilassa. Tämä aiheutti sen, että half duplex –tilassa oleviin portteihin kohdistuvaan liikenteeseen tuli törmäyksiä (collision) ja tästä syys-

tä liikenne hidastui. Ongelma saatiin ratkaistua vaihtamalla SFP-moduulit molempiin päihin ethernet-kaapeleita, joilla palomuurilaitteet on kytketty runkolaitteisiin. Käytettävät SFP-moduulit ovat kuparityyppiä, jossa käytetään kierrettyä parikaapelia (CAT6).

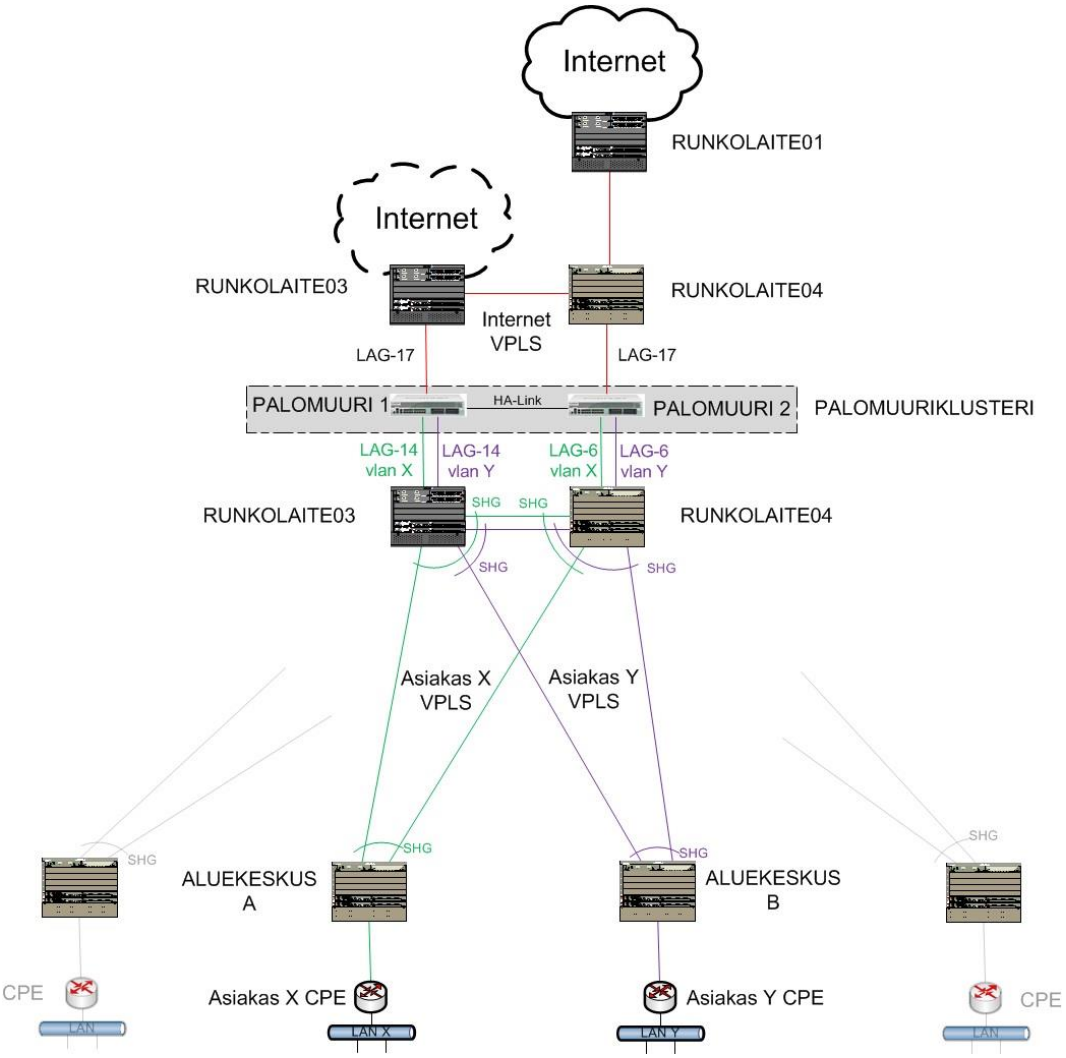
Palomuuriklusterin fyysiset kytkennät runkolaitteisiin näkyvät kuviosta 2. Kuvioon 2 on myös merkitty LAG-ryhmät, jotka on kytketty palomuurilaitteiden runkolaitteiden välille. Runkolaitteet ovat sijoitettuna Anvian eri laitetiloihin ja ne ovat kytkettynä yhteen 10 Gbit/s kapasiteetin linkeillä. Vikasietoisuus on otettu huomioon myös runkolaitteiden kytkennöissä. Mikäli toiseen runkolaitteista tulisi vika, johon palomuurit on kytketty, ei sillä olisi vaikutusta asiakkaan tietoliikenne yhteyksiin. Liikenne kulkisi edelleen toisen runkolaitteen kautta, mutta tällöin vain yhden palomuurilaitteen läpi.



Kuvio 2. Palomuurijärjestelmän fyysiset kytkennät.

2.2 Yritysliittymän kytkeminen palomuurijärjestelmään

Anvia tarjoaa yritysasiakkailleen yritysliittymiä, joihin on mahdollista kytkeä keskitetty palomuurijärjestelmä tuottamaan palomuuripalveluita. Liittymä rakennetaan runkolaitteisiin VPLS-tekniikalla ja verkkosilmukoiden estämiseksi siinä käytetään SHG-toimintoa. Internet-termointi on kahdessa erillisessä runkolaitteessa, jolloin yhden laitteen vikaantuminen ei aiheuta keskeytystä internet-liikenteeseen (**Kuvio 3.**) Kuviossa 3 on kuvattu loogiset yhteydet esimerkiksi, palomuuri 1:n ja 2:n molemmilla puolilla on sama fyysinen runkolaite.



Kuvio 3. Yritysliittymän liittäminen palomuurijärjestelmään.

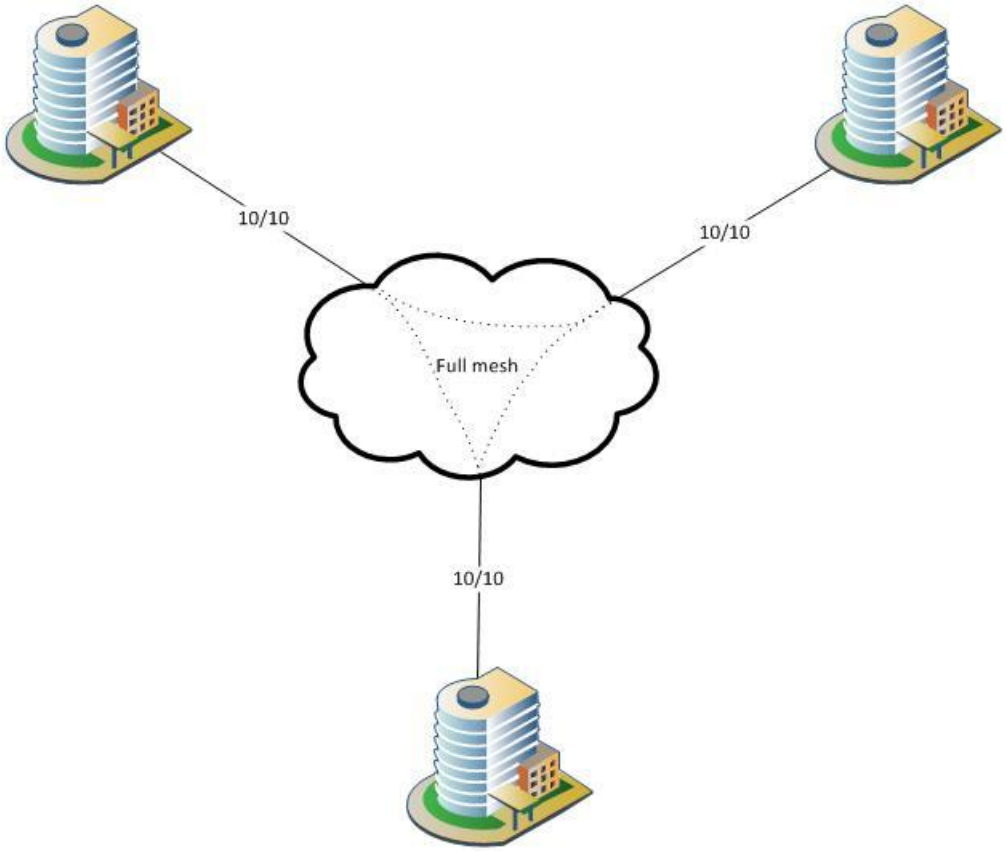
Asiakasyhteydet tuodaan VLANeilla (IEEE 802.1Q) eli OSI-mallin siirtoyhteyskerroksella (L2) palomuurijärjestelmään. /4/ IP-reititys (L3) tehdään palomuurijärjestelmässä sekä asiakaspäätelaitteessa CPE:ssä. Asiakkaan yksityiset (RFC 1918) LAN-verkon osoitteet reititetään palomuurille, jolloin NAT-osoitemuunnokset (RFC 1631) julkisiin IP-osoitteisiin (RFC 791) tehdään palomuurijärjestelmässä. LAN-verkon DHCP-palvelu (RFC 2131) toteutetaan CPE-laitteessa.

2.2.1 VPLS – Virtual Private LAN Services

VPLS on IETF:n määrittelemä käytäntö (RFC 4761 ja RFC 4762). VLPS on yksi MPLS-verkon monista toiminnoista. MPLS (Multi Protocol Label Swicthing)-verkossa toteutettavista palveluista käytetään usein myös VPN (Virtual Private Network) nimitystä. VPLS on OSI-mallin mukainen siirtoyhteyskerroksella (L2) toteutettu toiminne, joka tarjoaa kytkinverkon toiminnot ja se muodostaa yhden broadcast domainin. Yksittäisestä VPLS-yhteydestä käytetään nimitystä: PW (Pseudowire). /5/

VPLS-palvelua ei ole sidottu fyysisiin kytkinportteihin, vaan se on palvelu, joka luodaan MPLS-verkkoon, jossa se kulkee protokollan mukaisesti määriteltyihin laitteisiin full mesh -tyyppisesti. /6/ VPLS:n voi myös kytkeä yhteen tai useampaan fyysiseen porttiin.

Kuviossa 4 on kuvattu tyypillinen full mesh –verkko. Full mesh –verkossa kaikki toimipisteet voivat liikennöidä vapaasti keskenään, liikenteen kiertämättä minkään yksittäisen solmupisteen kautta.



Kuvio 4. Full mesh –tyyppinen tietoliikenneverkko.

2.2.2 SHG – Split Horizon Group

Split Horizon Group –toiminto on osa VPLS:ää ja sillä estetään silmukoiden (loop) syntyminen verkossa. Mikäli silmukka pääsisi syntymään verkkoon, näkyisi se käyttäjälle hidastuneena verkkoliikenteenä tai estäisi sen käytön kokonaan, koska silmukka aiheuttaa sen, että ethernet-verkon broadcast-liikenne lähtee kiertämään verkossa tukkien kaiken muun liikenteen.

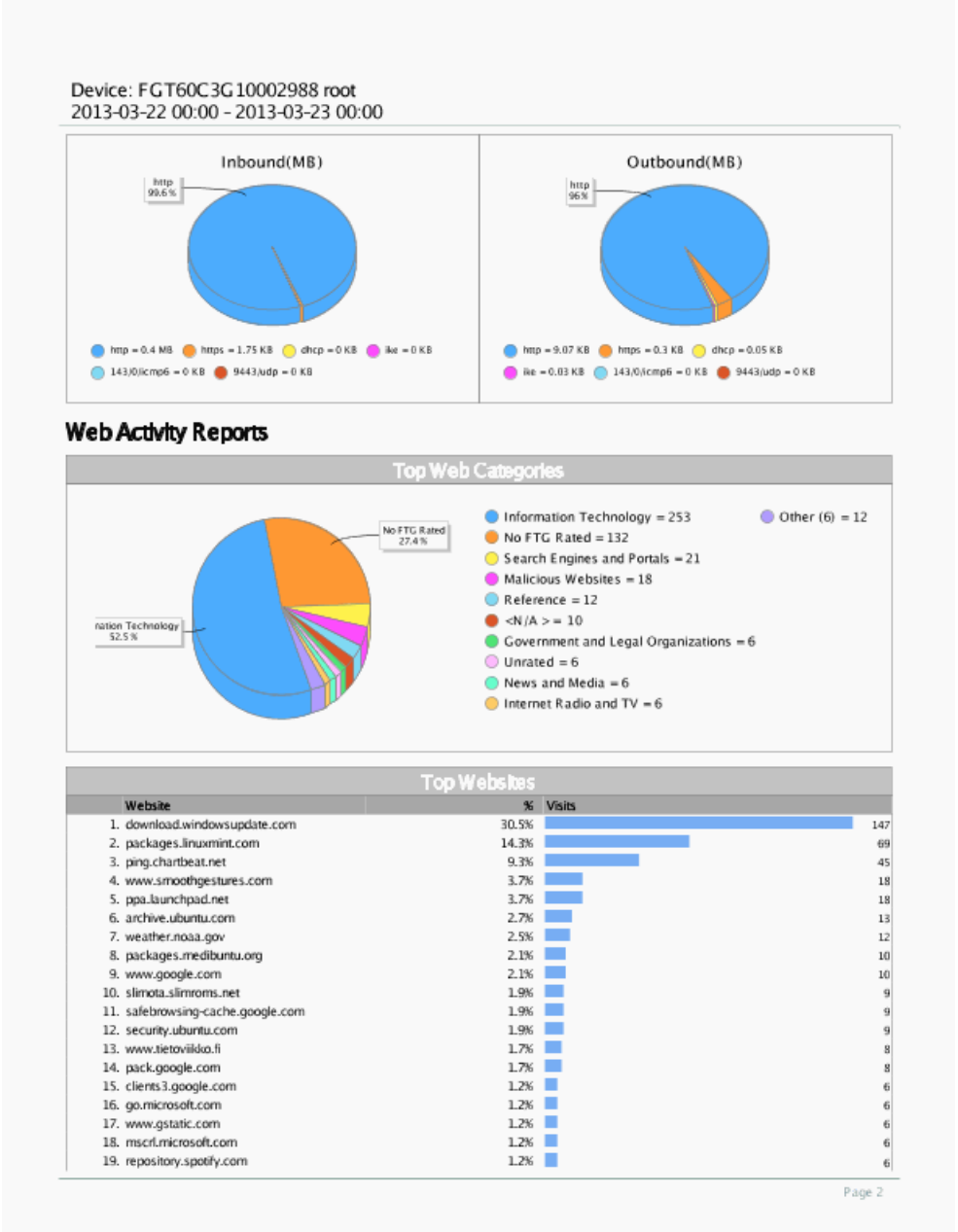
SHG estää liikennevirran kulkemisen useampaa PW:tä pitkin, jolloin silmukkaa ei pääse syntymään. Laite- tai verkkovian sattuessa, kun yhteys katkeaa toiseen laitteeseen, sallii SHG liikenteen kulkemisen aina toista kunnossa olevaa reittiä pitkin. SHG-toiminteella saadaan parannettua palomuurijärjestelmän vikasietoisuutta.

Anvian yritysliittymän toteutustapa on lähes samanlainen vaikka palomuurijärjestelmä ei olisi käytössä, joten sen sovittaminen palomuuriklusteriin ei aiheuttanut suurempia muutoksia. Käytännössä muutokset koskevat NATia, joka tehdään palomuurijärjestelmässä sekä VPLS-toimintoa. Tavallisesti yritysliittymässä ei käytetä VPLS-tekniikkaa, vaan se kytketään VLANilla asiakkaalle.

2.3 Palomuurijärjestelmän hallinta ja liikenneraportointi

Palomuurijärjestelmän hallinta on toteutettu erillisten yhteyksien kautta Anvian sisäverkosta (**Kuvio 2. MGTSW**) Hallintaverkko on nopeudeltaan 1 Gbit/s. Palomuurijärjestelmää on mahdollista hallita, joko CLI:n tai web-rajapinnan kautta. CLI-yhteys on toteutettu salatulla SSH-protokollalla ja myös Web-rajapintaa käytetään salatun https-yhteyden yli.

Hallintaverkkoon on kytketty palomuurijärjestelmän raportointijärjestelmä, joka mahdollistaa yksityiskohtaisen raportoinnin. Raportit voidaan luoda järjestelmään asiakaskohtaisesti ja niihin voi valita erityyppisiä raportteja. Raporttiin voidaan liittää esimerkiksi kohde- ja lähdeosoitteet, joista selviää mistä ja minne asiakas on liikennöinyt. Lisäksi yksityiskohtaisia raportteja saadaan myös UTM-toiminnoista (Antivirus, Web-filter, IPS ja Application control). Esimerkiksi web filter –raportti kertoo muun muassa, mille verkkosivustoille on yritetty mennä, mutta pääsy on estetty ja/tai minne verkkosivustoille on ollut eniten liikennettä. Malliraportissa (**Kuvio 5.**) on jaoteltu liikennejakaumat käytettyjen protokollien mukaan sekä sisään tulevan ja lähtevän suunnan mukaan. Lisäksi raportissa on jakauma (Top Web Categories) www-liikenteestä valmistajan kategorioiden mukaan sekä listaus useimmin käytetyistä www-sivustoista (Top Websites).



Kuvio 5. Malliraportti palomuuriliikenteestä.

3 UUDEN SUKUPOLVEN PALOMUURITOIMMINNOT

UTM (Unified Threat Management) –toiminnoilla varustetut palomuurit tarjoavat huomattavasti paremman tietoturvasuojan kuin perinteiset palomuurit. Perinteiset palomuurit toimivat niin kutsuttuna tilallisena (stateful firewall) palomuurina, joka pystyy selvittämään yhteyden tilan siten, että kukaan ei pääse väliin kaappaamaan olemassa olevaa yhteyttä. Tilallinen palomuuri tunnistaa, IP-paketteja tutkimalla, mistä yhteys on otettu ja minne se on menossa. Tämä suojaustoiminto ei nykypäivänä enää riitä, koska verkkorikolliset ovat kehittäneet huomattavasti nerokkaampia tapoja tunkeutua asiakkaan verkkoon. Tätä varten on jouduttu kehittämään uusia tapoja tunnistaa verkkoon tunkeutujat. UTM pyrkii vastaamaan nykyajan tietoturvauhkiin lähes reaaliajassa.

Perinteisiin palomuuritoimintoihin voidaan myös lukea IPsec VPN ja SSL VPN –toiminteet, jotka mahdollistavat tietoturvalliset etäyhteydet. Vaikka palomuurissa on UTM-toiminnot, sen perustana on edelleen käytössä tuiki tarpeellinen tilallinen palomuuri. Palomuurisäännöstöt pohjautuvat edelleen TCP/IP –porttien avaamiseen liikenteen sallimiseksi.

UTM on vain termi, joka koostuu useasta eri toiminnosta. Toimintoihin kuuluvat muun muassa Antivirus, Application control, Web filter ja IPS-toiminnot. Tässä työssä käsitellään edellä mainittuja UTM-toimintoja. Lisäksi UTM-toimintoihin voidaan myös lukea DDoS, Email filter, VoIP violation ja Data Leak Prevention, näiden toimintojen käsittely rajataan tämän työn ulkopuolelle.

Palomuurijärjestelmässä on virus- ja IPS-tunnistetietokannat, jotka päivittyvät laitevalmistajan käskystä (push update) tai tunnin välein. Lisäksi web filterissä käytettävä tietokanta päivittyy samoin perustein. Tietokannat pitävät sisällään tiedot sillä hetkellä liikkeellä olevista viruksista ja haavoittuvuuksista. Myös yleisimmät virukset ja haavoittuvuudet ovat tietokannoissa. Tietokannat eivät pidä sisällään kaikkia mahdollisia virus- tai IPS-tunnisteita, koska silloin tietokantojen koot kasvavat liian suuriksi ja käytettävyys kärsisi, kun laite joutuisi käymään kaikki mah-

dolliset tunnisteet läpi. Tätä toimintamallia voidaan pitää heuristisena eli pyritään arvioimaan kokemuksen ja tiedon perusteella, mitä on tulossa. Laitetoimittaja päivittää tietokannat automaattisesti, kun uusi virus tai haavoittuvuus löytyy.

Jokainen UTM-toiminto aktivoidaan erikseen palomuurisääntöihin. Sääntöjä rakentaessa on hyvä olla suunnitelma siitä, mitä toimintoja niihin halutaan aktivoida.

3.1 Antivirus

Antivirus-toiminto on yksi osa UTM-toimintoja. Antivirus-toiminto kytketään palomuurissa päälle tiettyyn palomuurisääntöön, jolloin se tulee aktiiviseksi sääntöön valittuihin protokolliin. Sääntöön voidaan valita esimerkiksi http-protokolla, jolloin kaikki http-liikenne tarkistetaan Antivirus-skannerilla. Mikäli liikenteessä havaitaan tunnettu virus, pysäyttää palomuuri liikenteen ja estää viruksen pääsyn asiakaslaitteelle. Asiakaslaitteelle tulee ilmoitus, että sivusto on haitallinen ja tiedosto on laitettu karanteeniin (**Kuvio 6.**)

Kuvio 6. Antivirus-toiminnon ilmoitus viruksesta.

Antivirus-toimintoa ei suositella käytettävän https-protokollan kanssa, koska toiminto joutuu purkamaan TLS-salauksen ennen kuin se pääsee käsiksi ladattavaan tiedostoon ja skannaamaan sen sisällön. Kun TLS-salaus puretaan, näkyy se käyttäjälle rikkonaisena TLS-sertifikaattina, vaikka sertifikaatti olisikin aito. Esimerkiksi, kun mennään jonkun pankin sivuille, jossa on käytössä TLS-sertifikaatti, varoittaa selain rikkoutuneesta varmenteesta. Rikkinäisen varmenteen aiheuttama

varoitus selaimessa saattaa aiheuttaa käyttäjissä hämmennystä ja aiheuttaa turhia yhteydenottoja Anvian asiakaspalveluun.

3.1.1 Palomuurilaitteen antivirus-konsepti

Antivirus-toimintoa voidaan käyttää kahdessa eri tilassa: proxy-based ja flow-based ja ne skannaavat viruksia, matoja, troijalaisia ja haittaohjelmia. Proxy-based antivisrusskannaus toimii siten, että kun käyttäjä lataa tiedoston, bufferoi antivirus proxy ensin tiedoston muistiin, jonka jälkeen se tutkii sen sisällön. Jos virusta ei löydy, lähetetään tiedosto edelleen eteenpäin lataajalle. Mikäli tiedostosta löytyy virus, saa käyttäjä siitä ilmoituksen, että tiedosto on haitallinen eikä sitä päästetä lataajan koneelle. Koska laitteen muisti on rajallinen, on suurin skannattavan tiedoston koko oletuksena 10 Mt, sitä suuremmat tiedostot päästetään automaattisesti antivirusskannerin ohi. Kokoa voidaan kasvattaa muuttamalla laitteen asetuksia, mutta tämä syö palomuurilaitteen resursseja. Lisäksi proxy-based-antivirusskannauksessa voidaan valita käyttöön eri tyyppisiä tietokantoja: normal, extended ja extreme database. Database-valinta vaikuttaa tietokannan virustunnisteiden määrään. /7/

Flow-based tilassa palomuuri käyttää IPS-moottoria tietoliikenteen tutkimiseen viruksilta, madoilta, troijalaisilta ja haittaohjelmilta siten, että tiedostoa ei tarvitse bufferoida laitteen muistiin. Tällä tavoin antivirusskanneri kuluttaa vähemmän palomuurin resursseja, mutta tunnisteiden määrä pienenee verrattuna proxy based-pohjaiseen virusskanneriin.

Liitteessä 2 ja 3 on kuvattu tarkemmin antivirus –toiminteen vaiheita haittaohjelmien löytämiseksi.

3.2 Application control

Application control –toiminteella voidaan rajoittaa sovelluksen käyttöä tai estää sen käyttö kokonaan. Rajoituksella voidaan antaa tietylle sovellukselle käyttöön haluttu kaista. Toiminolla voidaan esimerkiksi rajoittaa youtube.com käyttö 2

Mbit/s, jolloin se ei syö yrityksen koko internetkaistaa, jos sen käyttö ei kuulu yrityksen ydinliiketoimintaan olettaen, että yrityksen internetkaista on suurempi, kuin 2 Mbit/s. Toiminne aktivoidaan samaan tapaan kuin Antivirus –toimintokin eli se valitaan käyttöön tiettyyn palomuurisääntöön.

Application control –toiminnolla voidaan estää esimerkiksi peer-to-peer -liikenne kokonaan tai antaa sille käyttöön vain pieni kaistan määrä. Toinen hyvä estotoiminne on julkisten proxy-palvelinten käytön estäminen. Tämä esto kuuluu olennaisesti yhteen web filter –toiminnon kanssa, vaikka kyseessä onkin application control –toiminne. Kun web filterillä halutaan estää pääsy tietyille sivuille, estää se pääsyn suoraan niille sivuille, jotka on valittu, mutta julkista proxy-palvelinta käyttämällä voidaan esto ohittaa ja mennä sen kautta estetyille sivuille. Kun Application control –toiminteesta on aktivoitu proxy-estotoiminto, ei käyttäjä pääse enää ohittamaan web filter –estoja käyttämällä julkisia proxy-palvelimia.

3.3 IPS (Intrusion Prevention System)

IPS-toiminto estää tunnettuja haavoittuvuuksia käyttäviä haittaohjelmia pääsemästä asiakkaan tietoliikenneverkkoon, josta ne voisivat edetä muille verkossa olevilleen laitteille. Tällainen haavoittuvuus voi olla esimerkiksi linux www-palvelimen php-moduulissa. Jos palvelimen php-moduulia ei ole päivitetty viimeisimpään versioon ja vanhassa versiossa on tunnettu haavoittuvuus, estää palomuuri haavoittuvuutta hyväksikäyttävän haittaohjelman pääsyn palvelimelle eikä se pääse tekemään tuhojaan. Vastaava haavoittuvuus voi olla esimerkiksi Windows-käyttöjärjestelmän selaimessa. Microsoft on voinut julkaista tietoturvapäivityksen kyseiseen haavoittuvuuteen, mutta käyttäjä ei ole vielä viimeisintä päivitystä tehnyt. Tällöin jo palomuurissa havaitaan kyseistä haavoittuvuutta hyväksikäyttävät haittaohjelmat ja estetään niiden pääsy asiakaslaitteelle.

Uusien tietoturvauhkatunnisteiden päivitys tapahtuu palomuurilaiteeseen automaattisesti. Tunnisteet päivittyvät, yleensä huomattavasti nopeammin kuin itse sovelluksen kehittäjän julkaisema tietoturvapäivitys. Tämä toiminne tarjoaa mo-

nessa tapauksessa nopeamman suojan tietoturvahaavoittuvuuksille kuin sovelluksen kehityksestä vastaava pystyy tekemään tieturvapaikkauksen sille. Vaikka tietoturvapäivitys olisi saatavilla kyseessä olevalle sovellukselle, käyttäjän tai ylläpitäjän on viime kädessä tehtävä päivitys itse. Esimerkiksi palvelinkäytössä ei palvelimia voi yleensä päivittää heti kun tietoturvapäivityksiä tulee, vaan ne täytyy tehdä sovittuna ajankohtana, jolloin käyttökatkos ei aiheuta suurta haittaa itse palvelun käytölle. Sama koskee tavallisia tietokoneen käyttäjiä. Monikaan käyttäjä ei varmasti ole koko ajan tarkistamassa onko tietoturvapäivityksiä tullut, jonka jälkeen olisi heti päivittämässä niitä, koska senhetkiset työt täytyy keskeyttää ja käynnistää käyttöjärjestelmä uudelleen.

Tietoturvauhkiin reagoiminen vaatii laitetoimittajalta nopeaa toimintaa. Lisäksi heillä täytyy olla suuret resurssit, että niihin saadaan rakennettua oikeanlainen tunniste ja vielä toimitettua se kaikkiin palomuurilaitteisiin.

IPS-toiminto aktivoidaan myös palomuurisääntökohtaisesti. Palomuurin resurssien kannalta ylläpitäjän kannattaa rajata kohdelaitteet käyttöjärjestelmäkohtaisesti, koska mitä pienempi määrä tunnisteita, sitä vähemmän resursseja se syö palomuurilaitteesta. Esimerkiksi palvelinkäytössä, kun tiedetään mikä käyttöjärjestelmä halutaan suojata, valitaan vain sille käyttöjärjestelmälle tunnetut tietoturvatunnisteet. Lisäksi, jos tiedetään, että esimerkiksi palvelimessa on Windows-käyttöjärjestelmä ja se tarjoaa web-palveluja (IIS), päästään edelleen pienempiin tunnistemääriin, jolloin palomuurin resurssien käyttö edelleen pienenee.

IPS-toiminnossa on kaksi erilaista tekniikkaa tunnistaa hyökkäyksiä verkon ulkopuolelta; anomaly- ja signature-based. Anomaly-based suojausta käytetään, kun verkkoliikennettä yritetään hyväksikäyttää tunkeutumiseen. Host-konetta vastaan voidaan hyökätä siten, että sille lähetetään niin paljon liikennettä, että sen resurssit eivät enää riitä ja se menee tukkoon. Yleisen tapa tähän on denial of service attack (DoS), jossa hyökkääjä lähettää liikennettä host-koneelle useista eri lähteistä sen tarjoamiin palveluihin. Mikäli hyökkäys jatkuu edelleen, host-kone ei enää pysty

palvelemaan oikeita asiakkaita. Tässä tapauksessa hyökkääjä ei saa pääsyä host-koneelle, mutta host-koneen palvelut eivät ole tarjolla muille käyttäjille. /7/

Laitevalmistajan DoS-toiminto estää edellä kuvatun liikennehyökkäyksen antamalla sille threshold-arvon, jolloin aidot käyttäjät saavat edelleen palvelua kyseiseltä host-koneelta. /7/

Signature-based suojausta käytetään tunnettuja hyökkäyksiä ja haavoittuvuuksia hyödyntäviä hyökkäyksiä vastaan. Usein tällaisissa hyökkäyksissä hyökkääjä yrittää päästä asiakkaan verkkoon. Hyökkääjä yrittää kommunikoida host-koneen kanssa siten, että se saa pääsyn host-koneelle. Kommunikointi pitää sisällään tiettyjä komentoja tai sekvenssejä komennoista ja muuttujista. IPS-tunnisteet pitävät sisällään nämä komennot ja niiden sekvenssit, jolloin palomuurilaite tunnistaa ja estää tämän tapaiset hyökkäykset. /7/

IPS-tunnisteet ovat perusta signature-based hyökkäyksen estosuojaukselle. Jokainen hyökkäys pystytään katsomaan tietyn komentojonon tai komentosekvenssin ja muuttujien perusteella. IPS-tunnisteet pitävät sisällään nämä tiedot ja palomuurilaite tietää mitä etsiä verkkoliikenteestä. /7/

Tunnisteet pitävät myös sisällään tunnusomaisia tietoja hyökkäyksistä. Tunnusomaiset tiedot sisältävät verkkoprotokollat, joihin hyökkäykset kohdistuvat haavoittuvan käyttöjärjestelmän ja haavoittuvan sovelluksen osalta. /7/

3.4 Web filter

Web filter –toiminnolla voidaan rajoittaa www-sivustojen käyttöä. Web filter –toiminnossa on valmiita kategorioita, joiden perusteella www-sivut luokitellaan (**Taulukko 1.**) Monilla yrityksillä ja julkissektorin toimijoilla on tarve rajoittaa käyttäjien pääsy tietyille sivuille. Esimerkiksi kouluilla voi olla tarve rajata pääsy aikuisviihdesivustoille tai muuten sellaisille sivustoille, joista voi olla haittaa sen katselijoille. Tähän tarpeeseen pystytään vastaamaan web filter –toiminnolla.

Taulukko 1. Web filter –toiminnon oletuskategoriat.

Potentially Liable	Controversial	Potentially Non-productive	Potentially Bandwidth Consuming
Drug Abuse	Abortion	Advertising	File Sharing and Storage
Occult	Adult Materials	Brokerage and Trading	Streaming Media
Hacking	Advocacy Organizations	Freeware and Software Downloads	Peer-to-peer File Sharing
Illegal or Unethical	Gambling	Games	Internet Radio and TV
Racism and Hate	Extremist Groups	Web-based Email	Internet Telephony
Violence	Nudity and Risque	Web Chat	
Marijuana	Pornography	Instant Messaging	
Folklore	Tasteless	Newsgroups and Message Boards	
Proxy Avoidance	Weapons	Digital Postcards	
Web Translation	Sex Education		
Phishing	Alcohol		
Plagiarism	Tobacco		
Child Abuse	Lingerie and Swimsuit		
	Sports Hunting and War Games		

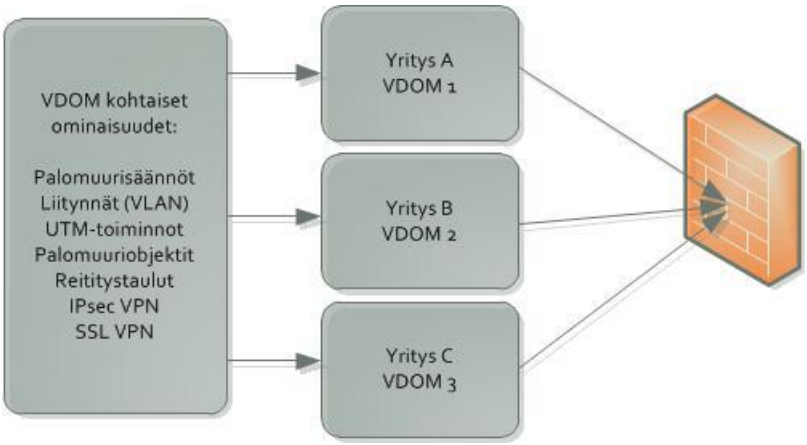
Kuten edellisetkin UTM-tominnot Web filter aktivoidaan tiettyyn palomuurisääntöön. Web filteriin valitaan valmiista kategorioista ne kategoriat, jotka katsotaan tarpeellisiksi ottaa käyttöön. Huomioitavaa on, että Web filter –toiminne tulee aktivoida sellaiseen palomuurisääntöön, jossa on vain siihen käyttöön tarkoitetut protokollat: http, https, ftp, ja ftps. Web filter osaa myös poimia www-liikenteen vaikka se ei olisi standardiportissa esimerkiksi portista 8080. Protokollan valinta on sikäli tärkeä, että sillä säästetään huomattavasti palomuuriresursseja. Jos web filter –toiminne valittaisiin palomuurisääntöön, joka olisi määritelty kuvion 7 mukaan eli kaikki ulos lähtevä liikenne ajettaisiin web filter –moottorin läpi, aiheuttaisi se turhaa resurssien käyttöä palomuurissa. Kuvitellaan, että käyttäjä soittaa VoIP –puhelun, joka käyttää SIP-signaloinnissa porttia 5060, kaikki SIP-liikenne käy web filter –moottorilla aiheuttaen turhaan ylimääräistä palomuuriresurssien käyttöä.

Kuviossa 7. on esimerkki palomuurisäännöstä, jossa on web filter –toiminne aktivoituna. Serviceen pitäisi olla valittuna ALL:in sijaan; http, https, ftp ja ftps, jolloin vältytään turhien palomuuriresurssien käytöltä.

Kuvio 7. Huono esimerkki palomuurisäännöstä web filter käytössä.

3.5 VDOM – Virtuaalinen palomuuri

VDOM ei itsessään kuulu UTM-toimintoihin. Virtuaalisella palomuurilla voidaan rakentaa fyysiseen palomuurilaitteeseen erillisiä virtuaalisia palomuureja, jotka eivät ole mitenkään tekemisissä toistensa kanssa, ellei niin haluta. Virtuaalinen palomuuri sisältää kaikki ne samat toiminnot kuin fyysinen palomuurilaite. Virtuaalisella palomuurilla on omat palomuurisäännöstöt, liitynnät (VLAN), UTM-toiminnot, palomuuriobjektit, reititystaulut, IPsec VPN ja SSL VPN –toiminteet, jotka ovat fyysisessäkin palomuurilaitteessa (**Kuvio 8.**)

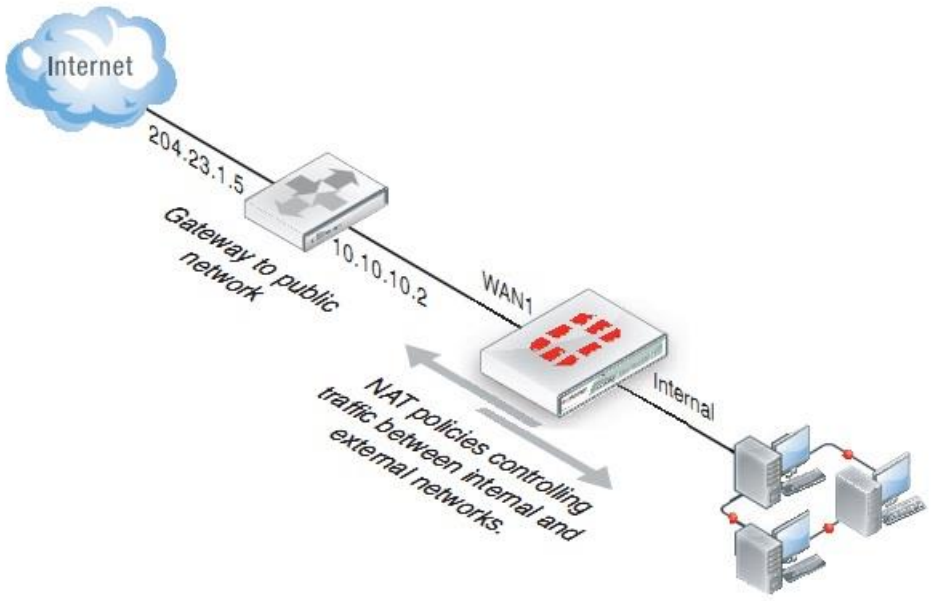


Kuvio 8. Periaatekuva virtuaalisesta palomuurista.

Palomuuriobjekteihin kuuluvat esimerkiksi IP-osoitteet, servicet eli TCP/IP- ja UDP-portit sekä NAT-osoitteet. Objektit valitaan käyttöön palomuurisääntöihin.

Virtuaalista palomuuria voi verrata VRF-toimintoon, jolla fyysiseen reitittimeen voidaan rakentaa useita virtuaalisia reitittimiä. Virtuaalisilla reitittimillä on omat reititystaulut, jotka mahdollistavat päällekkäisten IP-osoitteiden käytön samassa reitittimessä. Virtuaalisessa palomuurissa on edellisen toiminnon lisäksi myös palomuuritoiminnot.

Virtuaalinen palomuuri voidaan määritellä, joko routed (reitittävään) tai transparent (läpinäkyvään) tilaan. Transparent-tilassa oleva virtuaalinen palomuuri ei näy muille verkkolaitteille. Tyypillinen käyttö transparent-tilassa olevalle palomuurille on sellainen, että verkossa on jo olemassa palomuuri tai jokin muu IP-terminoinnista vastaava laite ja siihen väliin halutaan palomuuri, jolla toteutetaan esimerkiksi UTM-toimintoja. Tällöin olemassa olevaan verkkotopologiaan ei tarvitse tehdä muutoksia (**Kuvio 9.**) Vaikka palomuuri on transparent-tilassa, täytyy siihen kuitenkin tehdä palomuurisäännöt liikennöinnin sallimiseksi, kuten normaalissa palomuurissakin. Transparent-tilassa oleva palomuuri mahdollistaa myös NAT-toiminnot.



Kuvio 9. Esimerkki transparent-tilassa olevan palomuurin verkkoon kytkemisestä.

4 JOHTOPÄÄTÖKSET JA YHTEENVETO

Tämän opinnäytetyön aiheena oleva keskitetty palomuurijärjestelmä mahdollistaa Anviaa tuottamaan uusia tietoturvapalveluita kustannustehokkaasti yritysasiakkailleen. Projekti oli Anvian kokoisessa yrityksessä mittava ja laiteinvestoinnit ovat kohtalaisen suuria. Projektiin on käytetty paljon työtunteja, että halutut palvelut voidaan toteuttaa toimivalla tavalla. Projektin tavoitteet saatiin täytettyä, kun palvelut testattiin toimiviksi ja ne pystyttiin toteuttamaan suunnitelmien mukaan.

Palvelun luotettavuus on erittäin tärkeää, kun palveluja tuotetaan suoraan verkosta ja vastuu niiden tuottamisesta on itse operaattorilla. Palomuuriklusterin kytkentä suunniteltiin ja toteutettiin Anvian runkoverkkoon alusta lähtien vikasietoiseksi. Vikasietosuus on todettu toimivan käytännössä erittäin hyvin eikä sen osalta ole tarpeita tehdä muutoksia. Jatkon kannalta olisi hyvä, kun liittymänopeudet kasvavat, että palomuuriklusteri kytkettäisiin runkolaitteisiin 10 Gbit/s liitännöillä. Tällöin asiakkaille voidaan tarjota 1 Gbit/s suurempia nopeuksia.

Laitevalmistajan UTM-ominaisuuksiin perehtyminen on vaatinut suuren määrään tunteja itse laitteeseen tutustumalla ja käytännössä testaamalla. Laitevalmistajan järjestämistä koulutuksista on ollut suuri apu, kun on tarvittu yksityiskohtaista tietoa. Lisäksi apua sai laitevalmistajan hyvistä teknisistä dokumenteista. UTM-toiminnot testattiin ja todettiin toimivan pääsääntöisesti erittäin hyvin. Kaikkia UTM-toimintoja ei voitu kuitenkaan ottaa käyttöön, koska ne näyttäytyvät käyttäjälle virheilmoituksina, aiheuttaen turhaa hämmennystä.

Kokonaisuudessaan voidaan todeta, että palomuuriklusteri tarjoaa juuri niitä ominaisuuksia mitä siltä oltiin alun perin hakemassa. Palomuurijärjestelmän käyttöönotolla on ollut myös myönteinen vaikutus asennus- ja huoltoaikoihin. Jatkokehityksen kohde voisi olla palomuuripalveluiden automatisointi niin, että asiakas voisi itse valita käytettävän palvelun ja aktivoida sen suoraan verkosta.

LÄHTEET

/1/ http://www.anvia.fi/fi-FI/Konserni/tietoakonsernista/historia/Sivut/default.aspx Viitattu 10.3.2013.

/2/ http://www.anvia.fi/fi-FI/Konserni/tietoakonsernista/perustietoa/Sivut/default.aspx Viitattu 10.3.2013.

/3/ IEEE 802 LAN/MAN Standards Committee. Viitattu 14.3.2013. http://www.ieee802.org/3/hssg/public/apr07/frazier_01_0407.pdf

/4/ About.com, OSI Model Reference Guide. Viitattu 24.3.2013. http://compnetworking.about.com/cs/designosimodel/a/osimodel.htm

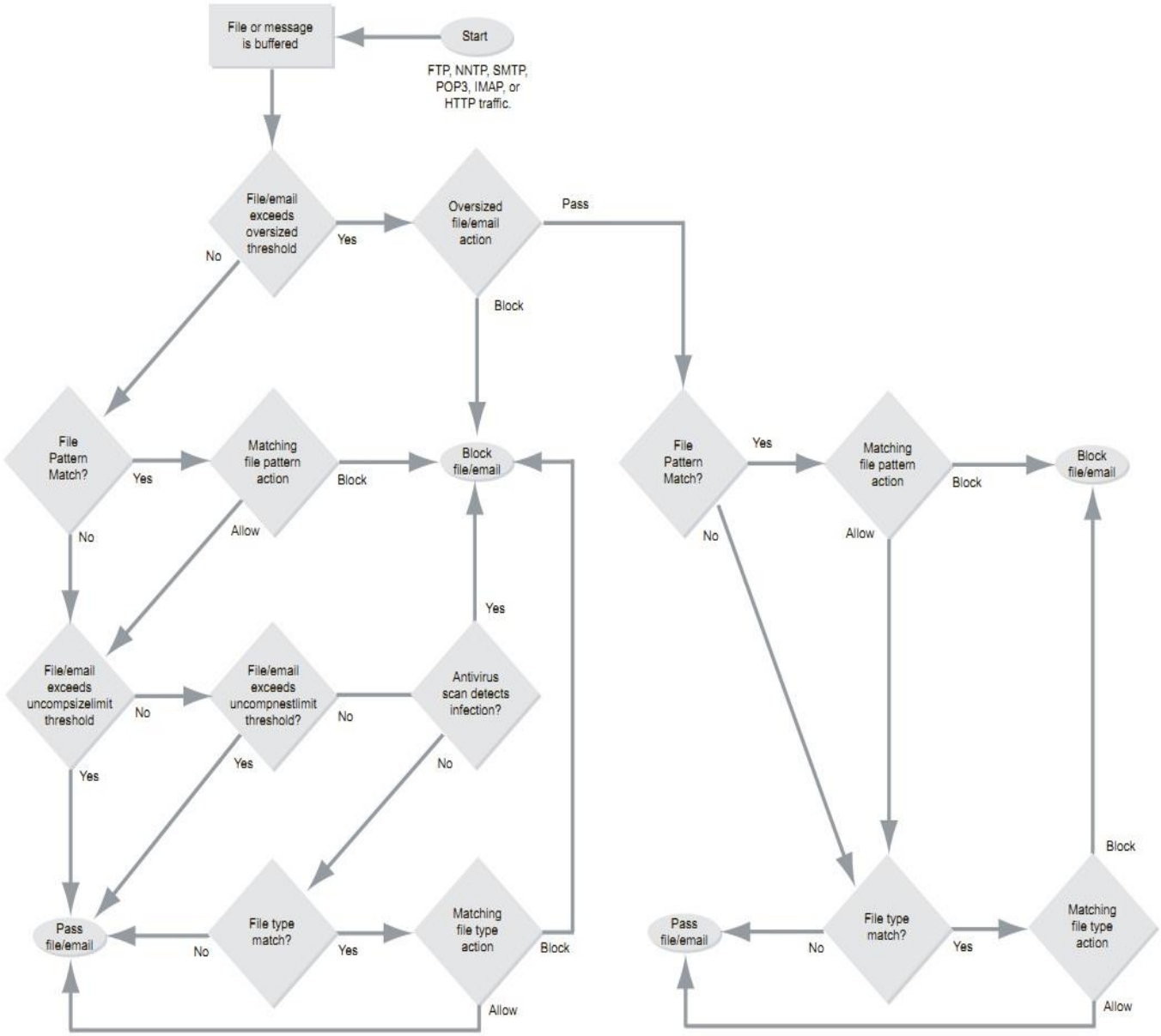
/5/ IETF RFC 4762. Viitattu 23.3.2013. http://tools.ietf.org/html/rfc4762

/6/ Networkworld.com. Viitattu 24.3.2013. http://www.networkworld.com/details/6222.html

/7/ UTM Guide, FortiOS Handbook v4.3

/8/ IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation (IEEE 802.1AX-2008)

Proxy-based antivirus scanning order when using the normal, extended, or extreme database



Antivirus scanning order when using the flow-based database