Tommi Kauppinen

Yhdistetty uhkien hallinta seuraavan sukupolven palomuurilla

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
1.5.2017

Metropolia

Tekijä Otsikko Sivumäärä	Tommi Kauppinen Yhdistetty uhkien hallinta seuraavan sukupolven palomuurilla 45 sivua + 2 liitettä
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli perehtyä nykyaikaisen seuraavan sukupolven palomuurin (NGFW) yhdistetyn uhkien hallinnan teknologioiden (UTM) teknisiin toimintaperiaatteisiin ja siihen, kuinka näillä ominaisuuksilla saadaan useampi suojauskerros yrityksen verkkotietoturvalle.

Työssä tutkittiin tyypillisimpiä tietoverkoissa esiintyviä uhkia yrityksen tietoturvalle ja niiden pohjalta uhkien torjuntaan tarjolla olevia palomuuriteknologioita. Tarkoituksena oli tutkia kunkin teknologian teknisiä toimintaperiaatteita ja sitä, kuinka ne pystyvät havaitsemaan ja eristämään yrityksen tietoverkosta haittaohjelmia ja muita tietoturvauhkia IP-paketeista sovellustasolla.

Työssä kytkettiin päälle useita UTM-suodatusprofiileja seuraavan sukupolven palomuurille ja havainnollistettiin myös lyhyesti UTM-ominaisuuksien vaikutusta tietoliikenteen käsittelyaikaan palomuurilla. Suoritetuissa testauksissa näytettiin myös, kuinka estetyn liikenteen käsittely palomuurilla ilmenee loppukäyttäjälle.

Testitulosten perusteella voitiin päätellä, että UTM-ominaisuuksilla varustettu palomuuri pystyy tehokkaasti toimimaan yrityksen tietoverkon uhkien ja sisällön suodattimena. Lisäksi voitiin todeta, että yhdistetyn uhkien hallinnan käyttöönotto lisää viiveitä IP-liikenteessä.

Avainsanat	UTM, NGFW, palomuuri, FortiGate, tietoturva

Author	Tommi Kauppinen
Title	Unified threat management on next-generation firewall
Number of Pages	45 pages + 2 appendices
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Erik Pätynen, Senior Lecturer

The goal of this final year project was to investigate in detail the technical principles of Unified Threat Management (UTM) technologies on a modern next-generation firewall (NGFW) and how properly implemented UTM features provide an additional layer of security to modern enterprise networks.

The project aimed to briefly analyze most commonly encountered threats on modern IP networks and how UTM technologies on NGFW can counter these threats. Each technology was examined in terms of how it operates on technical level and how to prevent threats on protocol basis.

Security and performance balance was also analyzed in this project. The goal was to investigate how UTM features on a firewall affect the performance of most common applications such as HTTP and how the traffic scanning can cause issues from the end user's perspective.

Based on the test results, it can be conducted that Unified Threat Management technologies on a next-generation firewall can act as a cost-effective threat and content filtering service without the need to invest in numerous security appliances. The test results also indicate that enabling UTM scanning on a firewall increases the latency in IP-traffic.

Keywords	UTM, NGFW, firewall, FortiGate, network security

Sisällys

Lyhenteet

AC	Application Control. Sovellusten hallinta.
AD	Active Directory. Microsoftin Windows-toimialueen käyttäjätietokanta.
APT	Advanced Persistent Threat. Edistynyt pitkäkestoinen hyökkäys. Kokonaisuus monimutkaisia ja huomaamattomia haittaohjelmia sekä prosesseja, jotka on suunniteltu jotakin tiettyä entiteettiä vastaan.
ASIC	Application Specific Integrated Circuit. Sovelluskohtainen mikropiiri.
AV	Anti-virus. Virustentorjunta.
BYOD	Bring your own device. Yrityksen tietoturvapolitiikka, joka sallii työntekijöiden omien päätelaitteiden käytön yritysverkossa.
DLP	Data Loss Prevention. Tietovuotojen esto.
DMZ	Demilitarized Zone. Yrityksen lähiverkosta eristetty alue, joka tarjoaa palveluita turvattomaan verkkoon kuten Internetiin.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
DPI	Deep Packet Inspection. IP-pakettien sisältämän datan tutkiminen.
DTLS	Datagram Transport Layer Security. Tietoliikenteen salaamisprotokolla.
FTP	File Transfer Protocol. TCP-protokollaa käyttävä tiedostonsiirtomenetelmä.
HTTP	Hypertext Transfer Protocol. Muun muassa selaimien käyttämä hypertekstin siirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure. Salauksella suojattu HTTP-protokolla.

IoT	Internet of Things. Esineiden Internet tai teollinen Internet.
IP	Internet Protocol. Pakettikytkentäisissä verkoissa tietoliikenteen toimittamiseen käytetty protokolla.
IPS	Intrusion Prevention System. Tunkeutumisestojärjestelmä.
NGFW	Next-generation firewall. Seuraavan sukupolven palomuuri.
OSI	Open Systems Interconnection. Viitemalli, joka kuvaa tiedonsiirtoprotokollien toimintaa seitsemässä kerroksessa.
POP3	Post Office Protocol version 3. Sähköpostin hakemiseen tarkoitettu protokolla.
SDN	Software-defined networking. Ohjelmallisesti määritelty verkkoarkkitehtuuri.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
SSL/TLS	Secure Sockets Layer/Transport Layer Security. Tietoliikenteen salaamiseen käytetty protokolla.
TCP	Transmission Control Protocol. Tilallinen tietoliikenneprotokolla yhteyksien luomiseen ja tiedon siirtämiseen.
UDP	User Datagram Protocol. Tilaton tietoliikenneprotokolla tiedon siirtämiseen.
URL	Uniform Resource Locator. Merkkijono, jolla viitataan tiedon sijaintiin, kuten www-osoitteeseen.
UTM	Unified Threat Management. Yhdistetty uhkien hallinta.
WF	Web Filter. Web-suodatin.

1 Johdanto

Yritysten ja organisaatioiden tietoturva on nykypäivänä yksi suurimmista huolenaiheista. Tietoverkkoihin kytketään nykyään lukemattomia päätelaitteita, ja yhä kiihtyvällä tahdilla verkkoon ilmestyy myös teollisen Internetin (IoT) myötä mitä yksinkertaisimpia laitteita verkkoyhteydellä varustettuna. Yritysten IT-asiantuntijoiden ja ulkoistettujen palveluiden tuottajien on vaikeaa ylläpitää tarkkaa kirjaa kaikista verkkoon kytkeytyvistä päätelaitteista ja niiden tietoturvasta. Äärimmillään verkkoon kytkeytyvä laite voi olla LTE-yhteyden varassa oleva mitta-anturi, johon ei saada asennuksen jälkeen tietoturvapäivityksiä. Lukemattomat päätelaitteet, yhä lisääntyvät pilvipalvelut ja jatkuvasti muuttuvat virukset ja muut haittaohjelmat asettavat haasteita yrityksen verkkotietoturvan ensimmäiselle ja kenties tärkeimmälle komponentille, palomuurille.

Takavuosina yrityksen täytyi budjetoida erilliset tietoturvalaitteet erilaisia hyökkäystyyppejä vastaan. Virustorjuntaan tarvittiin oma laite, tunkeutumisuhkia vastaan sekä havainnointi- että torjuntalaite ja web-liikennettä varten oma välityspalvelin. Nykyään yrityksen tarvitsee investoida parhaimmillaan vain yhteen palomuuriin, jonka lävitse kaikki yrityksen tietoliikenne ohjataan keskitetysti. Seuraavan sukupolven palomuuri yhdistää virustorjunnan, tunkeutumisuhkien estämisen, web-liikenteen rajoittamisen ja erilaisten sovellusten hallinnan. Säästöjä syntyy niin investointi- kuin ylläpitokuluissakin.

On hyvin tärkeää, että seuraavan sukupolven palomuureja hallinnoivat asiantuntijat ymmärtävät yrityksen käyttämät sovellukset, yritykseen kohdistuvat tietoturvauhat ja -teknologiat, jotta yrityksen tietoliikenteestä voidaan suodattaa tarpeeton ja haitallinen liikenne pois.

Tämän insinöörityön tarkoituksena on perehtyä nykyaikaisten palomuurien yhdistetyn uhkien hallinnan (Unified Threat Management, UTM) teknologioihin ja niiden teknisiin toimintaperiaatteisiin. Työssä tutkitaan, miltä UTM-suodatus näyttää loppukäyttäjän näkökulmasta tietoturvauhan esiintyessä tai kiellettyä sovellusta käytettäessä. Tarkoituksena on myös lyhyesti esitellä liikenteen skannaamisen aiheuttamia suorituskykyvaikutuksia HTTP- ja HTTPS-liikenteen toimintaan.

Ohjaavana tekijänä tämän työn tekemiseen on ollut oma päivittäinen tietoturvan asiantuntijuus erilaisten yritysasiakkaiden verkkojen parissa, joissa palomuuri on keskiössä. Työssäni olen huomannut, että on tärkeää tuntea yrityksen käyttämät sovellukset ja niiden tietoturvavaatimukset. Sovellusten käyttämillä IP-osoite- ja portti-protokollayhdistelmillä luodaan varsinainen palomuuriavaus tarvittaviin verkkoihin, ja tämän lisäksi liikenteelle voidaan antaa oma UTM-profiili, joka skannaa liikenteen virusten ja muiden hyökkäysten varalta sekä tunnistaa käytetyn sovelluksen.

Palomuurin sääntökannassa tarvitaan hienojakoisuutta, sillä palomuurille aiheutuu suorituskykyongelmia, mikäli kaikki mahdolliset tietoturvaprofiilit kytketään päälle kaikelle mahdolliselle tietoliikenteelle. Myös liikenteen ja tietoturvatapahtumien lokituksen vuoksi on tärkeää, että palomuurilla on tarkasti rakennettu sääntökanta.

Insinöörityön osana luodaan yksinkertainen palomuurisääntökanta, johon yhdistetty uhkien hallinta kytketään päälle. Jokaisen UTM-teknologian toiminta testataan, ja lopuksi suoritetaan suorituskykytestauksia HTTP- ja HTTPS-liikenteellä. Palomuurisääntökannan ja UTM-profiilien käyttöönotto tehdään Fortinetin FortiGate-palomuurilla. Fortinet on Palo Alto Networksin lisäksi johtavia seuraavan sukupolven palomuurin valmistajia.

2 Yrityksiin kohdistuvat uhat tietoverkoissa

2.1 Ulkoiset uhat

Yrityksiin kohdistuvista ulkoisista tietoturvauhista puhuttaessa tarkoitetaan lähes yksinomaan Internetistä saapuvia haittaohjelmia ja toisinaan myös palvelunestohyökkäyksiä. Helsingin seudun kauppakamarin ja elinkeino-, liikenne- ja ympäristökeskuksen rahoittaman DigiCyber-hankkeen mukaan [1] suomalaisista yrityksistä 47 % pitää tietojenkalastelu- ja haittaohjelmahyökkäyksiä suurimpina yritykseen kohdistuvina tietoturvauhkina. Riskitekijöinä ovat myös tunkeutumisyritykset yrityksen julkisia palveluita tarjoaviin palvelimiin esimerkiksi DMZ-eteisverkossa, jossa voi olla puutteelliset suojaukset joko ohjelmistossa tai sallitun tietoliikenteen osalta.

CyberEdge Group-tutkimusyhtiön julkaiseman globaalin raportin mukaan noin 1 000 kyselyyn vastanneesta yrityksestä 51,9 % epäili joutuneensa vähintään kerran onnistuneen kyberhyökkäyksen kohteeksi vuoden 2016 aikana [2]. Yleisimmät hyökkäystavat vaihtelevat tietojen kalastelusta (phishing), malwareen (virukset, troijalaiset) ja palvelunestohyökkäyksiin. Raportin mukaan yksi suurimmista kasvavista uhista ovat SSL-salattuina verkossa kulkevat haittaohjelmat, joiden estämiseen kyselyyn vastanneista yrityksistä 52 % oli ainakin osittain kykeneviä.

Itse hyökkäystyypit eivät juurikaan ole muuttuneet sitten vuosituhannen vaihteen, mutta hyökkäyksistä on tullut monimutkaisempia ja jopa valtiotasolla kehitettyjä uhkia. Vaikeimmissa tapauksissa puhutaan niin sanotuista ”Advanced persistent threat” -uhista (APT), jotka ovat tarkkaan räätälöityjä haittaohjelmia jotakin tiettyä järjestelmää tai ympäristöä vastaan ja joiden toimintaa tarkasti seurataan ne kehittäneen entiteetin toimesta. Esimerkiksi Suomessa Suojelupoliisin julkaisemassa vuosikertomuksessa vuodelle 2016 todetaan, että Suomeen kohdistuneet verkkovakoilut lisääntyivät merkittävästi ja suurin osa havainnoista liittyi APT28 (Fancy Bear) -nimiseen hyökkäykseen [3].

UTM-suodatusominaisuuksia harvemmin otetaan käyttöön liikenteelle, joka käynnistetään yritysverkon ulkopuolelta. Oletuksena tämänkaltainen liikenne on estetty tavallisilla palomuurisäännöillä. Poikkeuksena voi olla esimerkiksi yrityksen julkinen web-palvelin, jolle voidaan lisätä UTM-skannaus esimerkiksi SQL-injektioita ja WordPress-haavoittuvuuksia vastaan. Arkaluontoisille palvelimille pääsy yritysverkon ulkopuolelta voidaan

sallia esimerkiksi yrityskumppaneille tai palveluiden tuottajille joko Internetin kautta vain tietystä lähde-IP-osoitteesta tai tarjoamalla kumppaneille VPN-yhteyksiä, joiden lävitse liikenne kulkee salatusti palvelimille.

2.2 Sisäiset uhat

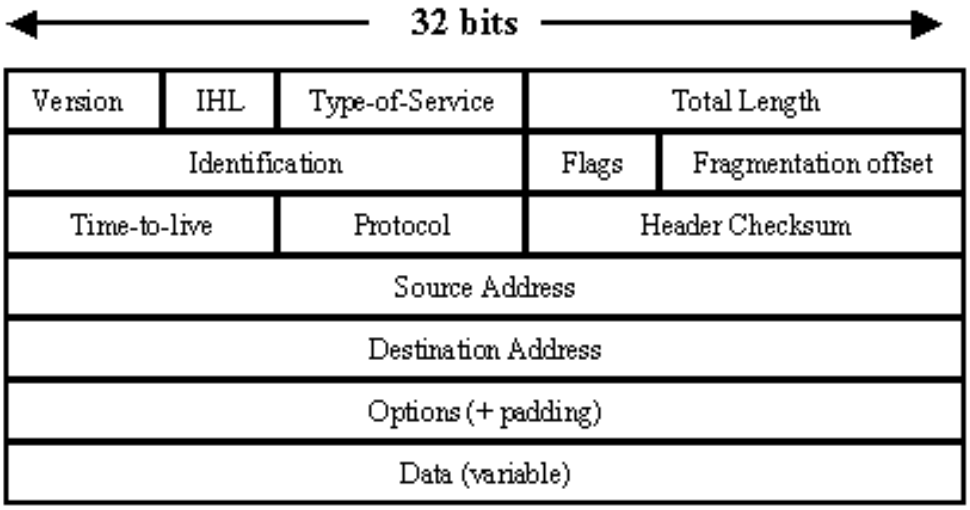
Yritysten suurimpia sisäisiä tietoturvauhkia on työntekijöiden tahallinen ja tahaton luottamuksellisen tiedon jakaminen yrityksen ulkopuolelle, haitallisten sähköpostien avaaminen ja vierailu haitallisilla verkkosivustoilla. UTM-teknologiat yleensä keskittyvät analysoimaan liikennettä, joka käynnistetään yrityksen sisältä ja kun kohteena on tietoturvaton verkko kuten Internet.

CyberEdge Groupin raportin [2] mukaan mobiliilaitteet, kuten älypuhelimet ja tabletit, muodostavat yhden suurimmista riskeistä yrityksen sisäverkolle. Viime vuosina kasvaneessa BYOD (bring-your-own-device) -ilmiössä yrityksen työntekijöille on sallittu enemmän oikeuksia kytkeä omia mobiililaitteitaan esimerkiksi yrityksen langattomaan verkkoon. Ongelmana on työntekijöiden yksittäisten mobiililaitteiden tietoturvasta huolehtiminen, sillä muualla saastuneen laitteen kytkeminen yritysverkkoon voi altistaa sen muun muassa matojen leviämiselle. Yrityksen työntekijöille pitäisikin aina antaa tarpeellinen tietoturvakoulutus.

3 Palomuurin rooli nykyaikaisessa yritysverkossa

3.1 Seuraavan sukupolven palomuurin määritelmä

Seuraavan sukupolven palomuurin (next-generation firewall, NGFW) määritelmään [4] kuuluu, että palomuurin on ominaisuuksien puolesta kyettävä tekemään liikenteen suodatusta IP-osoitteiden sekä protokollaporttien lisäksi myös IP-pakettien sisältämästä sovellusdatasta OSI-verkkomallin tasolla 7. IPv4-paketin rakenne on esitelty kuvassa 1. Markkinoilla on myöhemmin käytetty myös käsitettä UTM-palomuuri, mutta käytännössä eroa NGFW-termiin ei ole; molemmat määritelmät käsittävät palomuurin kyvyn tunnistaa ja suodattaa sovellustasolla muun muassa viruksia, haavoittuvuuksia, bottiverkkoja ja tietovuotoja.



Kuva 1. IPv4-paketin rakenne [5]. NGFW-palomuuri tarkistaa paketista lähde- ja kohdeosoitteiden lisäksi myös datan, johon sisältyy TCP/UDP lähde- ja kohdeportit OSI-verkkomallin tasolla 4 sekä varsinaisen protokollan kantaman sisällön tasolta 7.

Seuraavan sukupolven palomuurit ovat ominaisuuksiensa puolesta kehittyneet valtavasti kuluneen 15 vuoden aikana. Ydinfilosofia NGFW-palomuurissa ja erityisesti sen tarjoamissa UTM-ominaisuuksissa on ollut keskittää useita erilaisia yrityksen tietoturvalle olennaisia komponentteja yhteen laitteeseen.

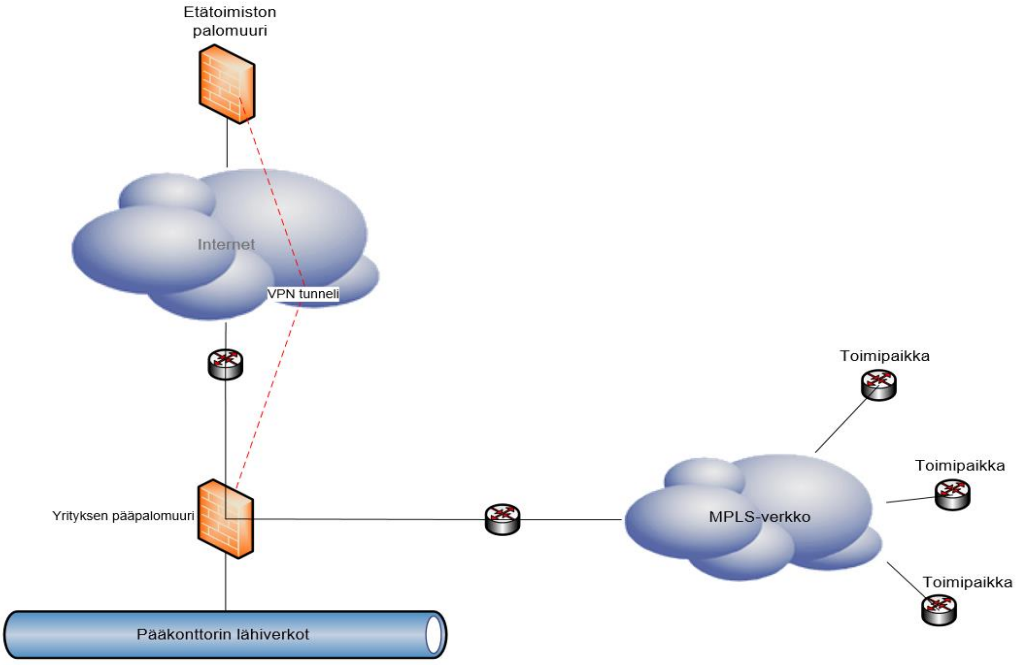
Vuosituhanteen vaihteessa oli vielä yleistä, että suurissa ja keskisuurissa yritysverkoissa tietoturvassa jouduttiin investoimaan erillisiin laitteisiin havainnoimaan ja estämään tietynlaisia uhkia. Yritysverkossa saattoi olla perinteisen palomuurin lisäksi laite torjumaan viruksia, toinen laite havaitsemaan tunkeutumisia, kolmas laite estämään tunkeutumiset ja neljäs laite lokeja varten. Lisäksi yrityksen sallima verkkoliikenne saatettiin kierrättää erikseen välityspalvelimen kautta, jolla oli erikseen lista sallituista verkkosivustoista. Yritykseltä, joka halusi pitää huolta tietoturvastaan, vaadittiin mittavia investointeja laitteiden ja lisenssien ostamiseen ja ylläpitokustannuksiin.

Kaikki nämä ominaisuudet löytyvät nyt yhdestä seuraavan sukupolven palomuurista, mikä vähentää huomattavasti investointi- ja ylläpitokustannuksia.

3.2 Verkkotopologia

Palomuuri on yrityksen tietoturvallinen yhdyskäytävä, joten on tärkeää saada kaikki liikenne ohjattua sen lävitse. Enenevissä määrin on nähtävissä ympäristöjä, joissa yritykset investoivat yhteen suuren kokoluokan palomuuriin, jolle kaikki liikenne ohjataan pääkonttorilta ja etätoimistoilta joko VPN-tunneleilla tai esimerkiksi suljetussa MPLS-verkossa. Itse palomuuri sijaitsee joko yrityksen omassa konesalissa tai se voi olla esimerkiksi tuotettuna pilvipalveluna kolmannen osapuolen hallinnoimana.

Tällä lähestymistavalla säästytään ylimääräisiltä ylläpito- ja lisenssikustannuksilta. Koko yrityksen tietoliikenne kiertää keskitetysti pääpalomuurin kautta, jossa on rakennettuna tarkka palomuurisääntökanta ja uhkien hallintaan optimoidut tietoturvaprofiilit. Kuvassa 2 on havainnollistettu verkkotopologia, jossa kaikki yrityksen Internet-liikenne kulkee pääpalomuurin kautta.



Kuva 2. Esimerkki verkkotopologiasta, jossa kaikki yrityksen Internet-liikenne pakotetaan kiertämään pääpalomuurin kautta.

3.3 Keskitetty uhkien hallinta ja paketin kulku palomuurissa

Kun palomuurille on rakennettu sääntökanta sallittujen lähde- ja kohde-IP-osoitteiden sekä protokollaporttien perusteella, on luotuihin sääntöihin mahdollista lisätä UTM-skannausprofiileja. Itse profiilit koostuvat erilaisista teknologioista, jotka pyrkivät tekemään muun muassa seuraavaa:

- haittaohjelmasuodatus
- sovellusten tunnistus ja hallinta
- haavoittuvuuksien, hyväksikäytön tunnistus ja esto (IPS)
- botnet-liikenteen tunnistus ja esto
- selauksen suojaus
- SSL/TLS-salauksen purkaminen liikenteestä
- roskapostin esto
- tietovuotojen estäminen [6].

Pakettien käsittelyjärjestys palomuurilla on itse laitteen ja loppukäyttäjän näkökulmasta tärkeää. Palomuurit ovat niin sanottuja tilallisia laitteita, eli ne pitävät kirjaa tulevasta ja lähtevästä IP-liikenteestä omassa sessiotaulussaan [7]. Näin palomuuri pysyy perillä olemassa olevasta liikenteestä, jolle on jo tehty liikenteen perustarkistukset.

Esimerkkinä asiakaskone lähettää HTTP-pyynnön yrityksen sisäverkosta Internetissä sijaitsevalle web-palvelimelle. Palomuuri analysoi TCP-kättelystä ensimmäisen paketin ja tekee sille reititys- ja palomuurisääntötarkistuksen. Palomuurisäännössä tarkistetaan, ovatko lähde- ja kohde-IP-osoitteet sekä käytetyt lähde- ja kohdeprotokollaportit sallittuja. Mikäli ovat, palomuuri tarkistaa onko säännössä käytössä UTM-profiileja ja ovatko kyseiset profiilit virtaus- vai puskurointitilassa.

Mikäli liikenne on sallittu, palomuuri luo liikenteestä sessiotauluun merkinnän ja ohjaa liikenteen tarpeen vaatiessa sovelluskohtaiselle mikropiirille (ASIC). Web-palvelimen palauttaessa asiakaskoneelle TCP SYN ACK -viestin palomuuri automaattisesti sallii paluuliikenteen, sillä liikenne osuu muodostettuun sessioon eikä reititys- tai palomuurisääntötarkistusta enää tässä vaiheessa tehdä.

Palomuuri luo itselleen sessiot myös kuljetuskerroksen tilattomasta UDP-protokollasta.

Palomuurin sallimille sessioille suoritetaan jatkuvasti UTM-tarkistuksia, ja näiden tarkistuksien osalta suoritusjärjestyksellä on merkitystä. Nopeimmat sovellustason tarkistukset tehdään ensin. Session paketit ajetaan ensin IPS- ja sovellushallinnan tarkistusten läpi, joissa liikennettä verrataan tunnettuihin tunnisteisiin. Tämän jälkeen siirrytään raskaampien UTM-profiilien käsittelyyn [32].

Huomionarvoista UTM-profiileissa on, että useimpia ominaisuuksia on lähes kaikilla NGFW-palomuureilla mahdollista suorittaa joko niin sanotuissa puskuroiduissa (proxy) tai virtaus (flow)-tiloissa. Termit vaihtelevat valmistajasta riippuen, mutta ero näiden kahden tilan välillä on sama.

Puskuroidussa tilassa asiakaskoneen avaamat sessiot palvelimen kanssa tapahtuvat itse asiassa palomuurin kanssa eli palomuuri toimii eräänlaisena näkymättömänä välityspalvelimena. Idea puskuroidussa tilassa on, että palomuuri pystyy rakentamaan lähetetystä liikenteestä kokonaiskuvan puskurimuistiinsa ja tekemään tarvittavat suodatukset tiedostoille ja muulle sisällölle, ennen kuin lähettää datan eteenpäin asiakaskoneelle.

Virtaustilassa palomuuri ei muodosta erillisiä sessioita asiakkaan ja palvelimen välille, vaan yhteys tapahtuu koneiden välillä suoraan ja palomuuri skannaa tietoja jokaisesta

lähetetystä paketista puskurimuistiinsa ja siirtää paketit viipymättä eteenpäin. Mahdolliset haittaohjelmat tunnistetaan, kun muistiin on saatu tarpeeksi tunnistetietoja IP-paketeista. Virtaustila on nopea ja kevyt palomuurin suorituskyvylle, mutta ei kykene yhtä tarkkaan ja monipuoliseen havainnointiin ja datan muokkaamiseen kuin puskuroidussa tilassa.

Liitteessä 1 on esitelty prosessikaavio palomuurivalmistaja Fortinetin FortiGate-palomuurin IP-pakettien käsittelyjärjestyksestä, kun UTM-profiilit ovat puskurointitilassa.

Sekä virtaus- että puskurointipohjaisissa tarkistuksissa molemmissa tehdään yleensä viimeisenä toimenpiteenä virusten tarkistus. Syynä tähän on, että palomuurin pitää verrata pakettia tai muistiin ladattua tiedostoa tunnettuihin virustunnisteisiin ja mahdollisesti tehdä sille heuristisia tarkistuksia, joilla voidaan havaita viruksiin viittaavaa sisältöä. Tämä toimenpide on raskas, ja mikäli virustarkistus tehtäisiin heti ensimmäisenä toimenpiteenä, se hidastaisi olennaisesti liikenteen kulkua. Viruksentorjuntaa olisi turha tehdä liikenteelle, jos esimerkiksi nopeasti toimiva web-suodatin estäisi liikenteen joka tapauksessa skannauksen jälkeen.

4 UTM-teknologiat

4.1 Tunkeutumisestojärjestelmä

Tunkeutumisestojärjestelmä eli IPS (Intrusion Prevention System) perustuu karkeasti jo vuonna 1986 julkaistun uhkien havaitsemismallin pohjalle [8]. Vuosikymmenien myötä mallin pohjalta on rakennettu havaitsemisen lisäksi myös estojärjestelmiä.

IPS-järjestelmä toimii purkamalla IP-paketin sisältö OSI-mallin tasolla 7 protokolladekooderilla ja vertaamalla sovelluksen sisältöä tunnettuihin hyökkäystunnisteisiin. IPS-järjestelmän tarkoitus on estää tunnettuja haavoittuvuuksia sovellustasolla. Nykyaikaiset seuraavan sukupolven palomuurit pystyvät myös havaitsemaan poikkeuksia sovelluksen toiminnassa ja tämän perusteella tunnistamaan potentiaalisia uusia hyökkäystapoja. Kuvassa 3 on esitetty muutamia tunnettuja hyökkäystunnisteita.

Applications	Name	Severity	Target	OS
Adobe	Adobe.Flash.ATF.Length.Field.Handling.Heap.Overflow	Critical	Server, Client	Other, Windows, Linux, MacOS
Adobe	Adobe.Flash.ATF.Length.Field.Value.Parsing.Heap.Overflow	Critical	Server, Client	Other, Windows, Linux, MacOS
Adobe	Adobe.Flash.ATF.Textures.Memory.Corruption	Critical	Server, Client	Windows, Linux, MacOS
Adobe	Adobe.Flash.AttachMovie.Memory.Corruption	Critical	Server, Client	Windows, Linux, MacOS
Adobe	Adobe.Flash.Audio.Handling.Out.Of.Bound.Remote.Code.Execution	Critical	Server, Client	Windows, Linux, MacOS
Adobe	Adobe.Flash.AVC.Decoder.Memory.Out.Of.Bounds.Access	Critical	Server, Client	Windows, Linux, MacOS
Adobe	Adobe.Flash.AVM2.Remote.Code.Execution	Critical	Server, Client	All
Adobe	Adobe.Flash.AVSegmentedSource.Class.Memory.Corruption	Critical	Server, Client	Windows, Linux, MacOS
Adobe	Adobe.Flash.Bitmap.Object.JXR.Memory.Corruption	Critical	Server, Client	Windows, MacOS

Kuva 3. Esimerkki FortiGate-palomuurin IPS-tunnisteista Adobe Flash -sovelluksen haavoittuvuuksia vastaan.

Palomuurin IPS-järjestelmä mahdollistaa ylläpitäjälle myös käsintehtyjen tunnisteiden luonnin. Käsintehdyillä tunnisteilla voidaan monipuolisesti tarvittaessa estää tunnistettuja tietoturvariskejä, joille ei ole vielä olemassa virallisia valmistajan tekemiä tunnisteita. Mahdollista on myös rakentaa sellaisia tunnisteita, joilla rajoitetaan jonkin sovelluksen toimintaa estämällä tiettyjä ominaisuuksia.

Teknisellä tasolla IPS-järjestelmä voi tunnistaa uhkia kolmella tavalla.

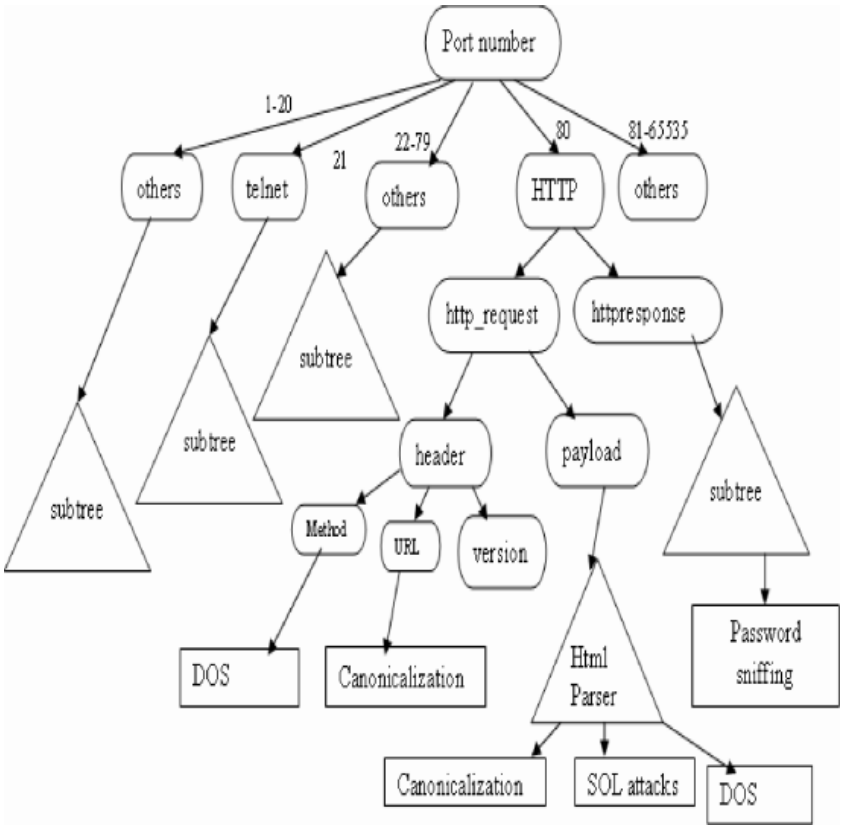
Tunnistepohjaisissa ratkaisuissa IP-paketin otsikkoa ja sisältöä skannataan ennalta määriteltyjä kuvioita vasten [9]. Kuviot voivat esimerkiksi perustua tietynlaiseen bittijonoon tai tunnistettujen haittaohjelmien tapaan suorittaa ohjelmakoodinsa.

Tunnisteet voidaan jakaa edelleen tilattomiin ja tilallisiin [9]. Tilattomat tunnisteet analysoivat yksittäisiä IP-paketteja joko otsikon tai sisällön perusteella. Tilaton tunniste voi olla esimerkiksi sellainen, jossa jokaisen IP-paketin sisältö avataan ja luetaan tekstin ” /etc/passwd” varalta. Mikäli teksti löytyy paketista, se estetään.

Tilalliset tunnisteet seuraavat esimerkiksi muodostettua TCP-sessiota, ja mikäli tietyt ehdot täyttyvät, liikenne estetään. Hyökkäys voi esimerkiksi jakaantua useampaan IP-pakettiin tai TCP-segmenttiin, ja kun tarpeeksi todisteita haittaohjelman olemassaolosta on saatu, liikenne estetään.

IPS-järjestelmän toinen tapa tunnistaa uhkia on niin sanottu anomaliapohjainen tunnistaminen, jossa IPS-järjestelmään määritellään sovellusten tavallisesti sisältämän datan perusteella vertailukohta. Heuristiikkaa ja erilaisia sääntölausekkeita hyödyntämällä palomuuri voi havaita poikkeamat esimerkiksi sovelluksen kantaman sisällön pituudesta ja estää liikenteen [10]. Anomaliapohjaisessa tunnistuksessa on suurena riskinä, että järjestelmä tuottaa vääriä hälytyksiä, mikäli määriteltyä vertailukohtaa ei ole tarpeeksi tarkasti määritelty.

Kolmas vaihtoehto ja modernein tapa palomuurin IPS-järjestelmän uhkien estämiseen on kontekstiperustainen suodattaminen [11]. Kontekstipohjaisessa suodatuksessa palomuurin IPS-moottori purkaa pakettien sisällön protokolladekooderilla ja seuraa yhteydessä muodostettuja sessioita ja liikenteen tapahtumia. Erona tilallisen tunnisteen toimintaan kontekstipohjaisessa suodatuksessa IPS-järjestelmä kykenee yhdistelemään sovelluksen liikenteen tapahtumista mahdollisiin hyökkäyksiin johtavia viitteitä ja tarvittaessa estämään liikenteen. Kuvassa 4 on esimerkki prosessikaaviosta kontekstipohjaiselle suodatukselle.



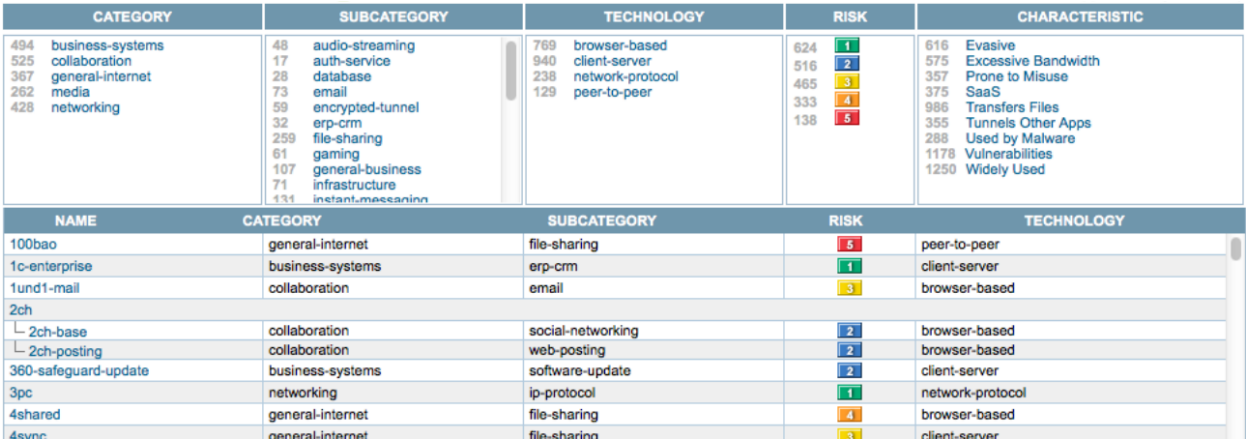
Kuva 4. Kontekstipohjaisen IPS-järjestelmän prosessikaavio hyökkäysten havaitsemiseen [11].

4.2 Sovellusten hallinta

Sovellusten hallinta (AC, Application Control) pohjautuu yleensä ainakin osittain palomuurin IPS-tietokantaan ja näin ollen käyttää samoja tunnisteita erilaisten sovellusten tunnistamiseen. Perinteinen palomuuri pystyy tunnistamaan liikenteen IP-osoitteen ja käytettävän kuljetuskerroksen protokollan ja portin perusteella, mutta ei ota kantaa paketin sovellusdataan. Seuraavan sukupolven palomuuri analysoi edellä mainittujen tietojen lisäksi OSI-mallin tasolla 7 IP-paketin datasisältöä ja tunnistaa käytetyn sovelluksen tai palvelun.

Esimerkiksi kun käyttäjä avaa selaimellaan YouTube-videon, perinteinen palomuuri tunnistaa, että kohdeportti on TCP 80 tai TCP 443 ja IP-osoite 216.58.211. Seuraavan sukupolven palomuuri pystyy myös tunnistamaan, että kyseessä on HTTP-protokolla ja käytetty palvelu on YouTube. Tämän tiedon perusteella voidaan palomuurilla tehdä toimenpiteitä, kuten estää liikenne, sallia liikenne, estää vain tiettyjä toiminnallisuuksia (ku-

ten HD-tasoisen kuvan katselu tai videoiden kommentointi) tai rajoittaa sovelluksen verkossa käyttämää nopeutta. Kuvassa 5 on esitelty esimerkkinä Palo Alto Networksin palomuurin lokidataa verkossa havaituista sovelluksista.



Kuva 5. Palomuurin tunnistamia sovelluksia [12].

Teknisellä tasolla sovellushallinta hyödyntää palomuurin valmistajan valmiita tunnisteita erilaisten sovellusten tunnistamiseen sovellustasolta riippumatta siitä, missä protokollaportissa liikennettä kulkee. Tunnisteiden lisäksi hyvin tunnetuille protokollille, kuten HTTP:lle, FTP:lle ja POP3:lle, on olemassa omat protokolladekooderit.

Dekoodereilla voidaan tunnisteen lisäksi havaita minkälaisesta sovelluksen toiminteesta on kyse. On esimerkiksi mahdollista sallia Facebookin käyttö sen kattavalla tunnisteella, mutta erikseen kieltää Facebookin ”tykkää”-napin käyttö. Lisäksi joillakin valmistajilla on käytössä heuristiikkaa ja sovelluksen sekä käyttäjän käyttäytymistä seuraavia ominaisuuksia, joiden pohjalta sovellus voidaan tunnistaa [12]. Heuristisia skannauksia voidaan suorittaa esimerkiksi sovellukselle, jonka epäillään osallistuvan vertaisverkkoon mutta jolle ei ole olemassa vielä tunnistetta. Heuristiikka analysoi esimerkiksi sovelluksen lähettämien IP-pakettien pituutta ja sitä, kuinka monta sessiota sovellus muodostaa, ja tämän perusteella se voi kyetä päättelemään, että kyse on vaikkapa BitTorrent-asiakasohjelmasta.

Sovellustunnisteet luokitellaan usein kuuluvaksi johonkin kategoriaan. Palomuurin ylläpitäjä voi halutessaan estää kokonaisia palvelukategorioita, joihin sisältyy tietyntyyppisiä tunnisteita. Esimerkiksi YouTube voidaan luokitellaan ”Video/Audio”-kategoriaan ja

VoIP-puhelut ”Network-Protocol”-kategoriaan. Kategoriapohjainen suodatus on hyödyllinen, koska sillä voidaan suoraan estää kaikki haitallisiksi luokitellut sovellukset. Palomuurivalmistajilla on lisäksi olemassa omat jatkuvasti päivittyvät pilvipalvelunsa, joista palomuurit käyvät päivittämässä sovellustunnisteensa ja kategoriat.

On kuitenkin hyvin mahdollista, että palomuurin lävitse kulkeva sovellus on niin harvinainen tai muuten vain tuntematon, että palomuuri ei pysty sitä tunnistamaan. Tällaisessa tilanteessa sovellus luokitellaan usein kuuluvaksi ”muut sovellukset” -kategoriaan, jolle voidaan antaa oma tietoturvapolitiikka, kuten estää kaikki tuntemattomiksi jääneet sovellukset.

Kuten IPS-järjestelmässä, on sovellushallinnan sensoreille mahdollista luoda käsin tehtyjä tunnisteita. Useimmissa tapauksissa palomuurivalmistajille on myös mahdollista lähettää pyyntö määritellä uusi tunniste tuntemattomalle sovellukselle. Usein isot ohjelmistotalot ovat kuitenkin haluttomia luovuttamaan esimerkiksi lähdekoodiaan palomuurivalmistajille analysoitavaksi tunnisteen luomista varten, joten valmiit tunnisteet usein luodaan niin sanotulla takaisinmallinnusmenetelmällä [13]. Menetelmässä sovelluksen toimintaa analysoidaan niin paljon, että tunnistetta varten saadaan tarpeeksi dataa.

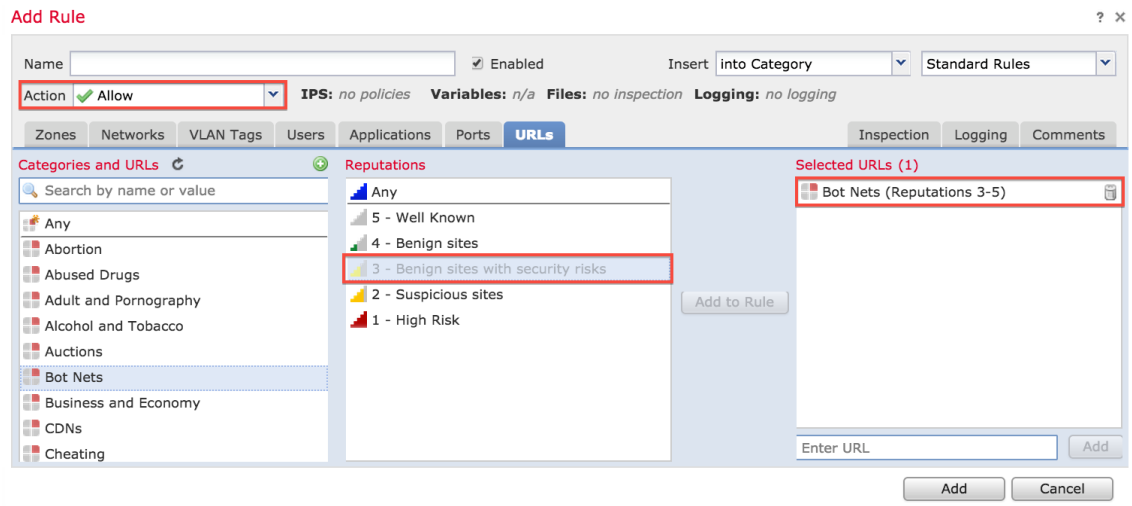
4.3 Web-suodatus

Web-liikenteen suodatus on yksi tärkeimpiä palomuurin UTM-ominaisuuksia, joilla saadaan ehkäistyä yrityksen työntekijöiden aiheuttamia tietoturvariskejä. Joissakin tapauksissa saadaan myös työntekijöiden tuottavuutta lisättyä estämällä turhat ajanvietepalvelut. Nykyaikainen palomuuri tunnistaa HTTP- ja HTTPS-liikenteen sovellustasolta riippumatta käytetystä protokollaportista. Riippuen konfiguraatiosta web-suodatin voi estää liikenteen, sallia sen, antaa käyttäjälle varoituksen tai vaatia käyttäjältä tunnistautumista ennen sivustoille siirtymistä.

Web-liikenteen suodattamiseen on useita eri tapoja. Yksi käytetyimmistä on sallia liikennettä verkkosivujen kategorian pohjalta. NGFW-valmistajien palvelut käyttävät hakurobotteja, jotka analysoivat verkkosivujen sisältöä ja luokittelevat ne erilaisiin kategorioihin. Tämä tieto siirretään valmistajan palveluiden tietokantaan, johon palomuurit tekevät kyselyjä tarkistaakseen luokituksia verkkoliikenteelle.

Web-luokituksista esimerkiksi YouTube voidaan luokitella kategoriaksi ”Streaming Media and Download”, ja palomuurin suodatusprofiilissa kyseinen kategoria voidaan lisätä estetyksi. Verkkosivuja luokitellaan myös niiden alla olevien URL-osoitteiden perusteella. Esimerkiksi sivusto www.reddit.com luokitellaan ”Newsgroups and Message Boards” -kategoriaan, mutta alasivusto www.reddit.com/r/networking puolestaan ”Information Technology” -kategoriaan. Näin ollen kategoriapohjaisella suodatuksella on mahdollista automaattisesti estää sivustoilta semmoisia kokonaisuuksia, joiden on todettu olevan saastuneita tai muuten kuuluvan erikseen kiellettyihin kategorioihin.

Toinen tapa on lisätä verkkosivut estetyksi tai sallituksi käsin URL-osoitteen perusteella. Esimerkkinä URL-suodatuksessa voidaan estää kokonainen domain tai vain tietty osa sivustosta yksinkertaisella määrityksellä, kuten lisäämällä niin sanottu villikorttimääritys *.example.com, joka estäisi muun muassa osoitteet test.example.com ja dev.example.com. Kuvassa 6 on esimerkki Ciscon ASA-palomuurin FireSIGHT-web-suodattimesta.



Kuva 6. Ciscon ASA-palomuurin web-suodatus, jossa on kategoriapohjaisen suodatuksen lisäksi mahdollista sallia tai estää sivusto sen maineen perusteella [14].

Kolmas vaihtoehto on suodattaa web-osoitteita DNS-pohjaisesti eli estää tunnetut haitalliset sivustot nimipalvelutietokannasta. Asiakaskoneen yhdistäessä web-sivustolle palomuuri tekee DNS-kyselyn valmistajan ylläpitämille nimipalvelimille, jotka luokittelevat sivustoja domainin perusteella kategorioihin. Tämä suodatustapa on nopea, mutta siitä puuttuu hienojakoisuus; kokonainen sivusto on joko sallittu tai estetty eikä suodatus ota kantaa sivuston alta löytyviin tarkempiin URL-osoitteisiin.

Web-suodatukseen liittyy osittain myös ominaisuus nimeltä ”Web Application Firewall” eli WAF, joka on kohdistettu web-palvelimien suojaamiseen [15]. WAF käsittää osittain samoja toiminnollisuuksia kuin IPS-järjestelmä esimerkiksi tunnistamalla ja estämällä SQL-injektioita, mutta tämän lisäksi se voi tarkasti analysoida HTTP-liikenteen poikkeamia palvelimen ja asiakaskoneen välillä muun muassa tarkkailemalla sessiossa siirrettyjen evästeiden määrää, syötettyjä URL-parametreja ja siirrettyjen sisältöjen pituuksia.

Hieman valmistajasta riippuen on kategoria- ja URL-suodatusta mahdollista suorittaa puskurointi- ja virtaustiloissa. Puskurointitilassa palomuuri kerää web-palvelimelta saapuvan liikenteen kokonaisuudessaan, tarkistaa sivuston luokituksen ja mahdolliset käsin tehdyt URL-ohitukset, minkä lisäksi datasta on mahdollista suodattaa pois esimerkiksi Java Applet- ja ActiveX-komponentteja. Puskurointitila sallii myös pienimuotoisen datan manipuloinnin, kuten Googlen SafeSearch-ominaisuuden päälle pakottamisen tehtyihin Google-hakuihin riippumatta siitä, miten loppukäyttäjä on SafeSearch-asetuksen selaimessaan määritellyt. Palomuuri tarkistaa myös verkkosivuston tekemät uudelleenohjaukset ja URL-osoitteet sivuston sisältämille kuville, jotka korvataan tyhjällä tilalla, mikäli yksittäisen kuvan URL kuuluu estettyyn kategoriaan.

Virtaustilassa kategoria- ja URL-suodatus on edelleen mahdollista, mutta palomuuri ei kykene manipuloimaan verkkosivun sisältöä samalla tarkkuudella kuin puskurointimallissa, sillä liikenne ohjataan eteenpäin välittömästi palvelimelta asiakaskoneelle.

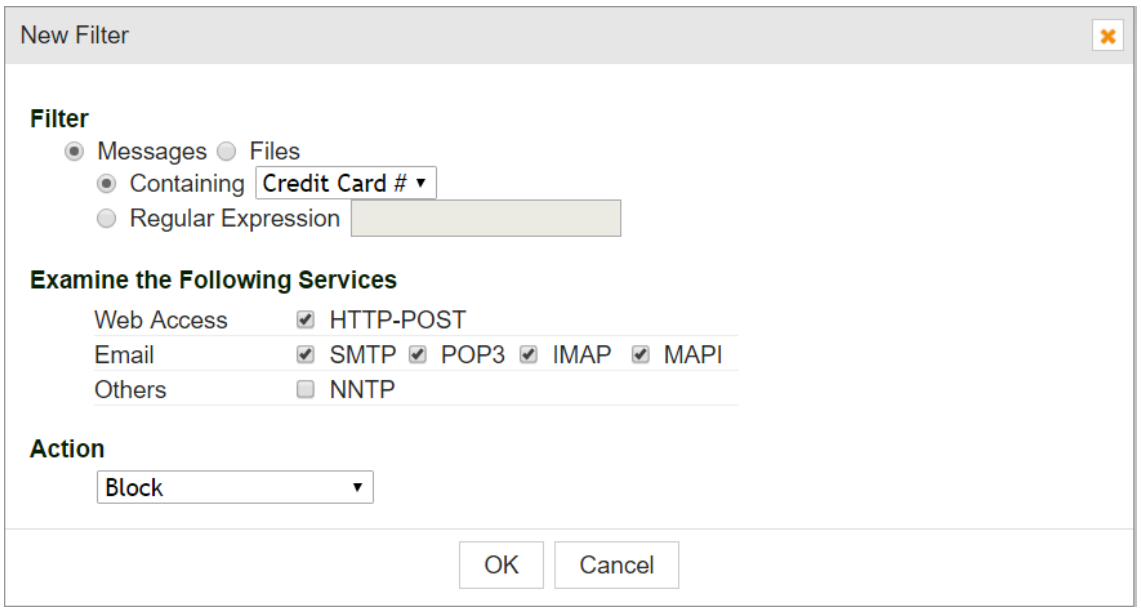
4.4 Tietovuotojen estäminen

Tietovuotojen estämisellä (Data Loss Prevention, DLP) viitataan joko tiedon tahalliseen vuotamiseen organisaation ulkopuolelle jollekin sellaiselle taholle, jolle nämä tiedot eivät kuulu, tai tiedon menettämistä niin, että se ei ole enää yrityksen hallussa. Suojeltavia tietoja voi olla esimerkiksi henkilötiedot, luottokorttitiedot ja erilaiset yrityssalaisuudet. Erityisesti julkisissa organisaatioissa on yleistä, että niiden tietojenkäsittelyä ohjaa myös lainsäädäntö, kuten Yhdysvalloissa olevat HIPAA- ja PCI-DSS-asetukset [16]. Esimer-

kiksi terveydenhuollossa on erittäin tärkeää, että potilaskertomukset ja muut henkilötiedot eivät vahingossa päädy vääriin käsiin ja että näiden tietojen vuotamista voidaan verkkotasolla ehkäistä DLP:llä.

Seuraavan sukupolven palomuuri pystyy havaitsemaan tietoliikenteestä ylläpitäjän määrittelemät arkaluonteiset tiedot ja estämään ne tarvittaessa. Esimerkiksi organisaation käyttämä pohja kaikille dokumenteille voidaan lisätä palomuurin tietokantaan niin, että organisaation dokumenttipohjassa toistuvista elementeistä (logo, allekirjoitukset) luodaan palomuurille niin sanottu vesileima, jonka perusteella palomuuri voi estää dokumenttien siirron yritysverkon ulkopuolelle [17].

DLP:ssä palomuurin ylläpitäjän pitää määritellä, minkälainen aineisto on luokiteltava tietovuototarkistuksen piiriin. Konfiguraatiomäärityksissä voi olla, että erilaisissa viesteissä esiintyvät tekstipohjaiset merkkijonot laukaisevat estomekanismin tai erikseen kielletyt tiedostomuodot estetään jakamasta. Kuvassa 7 on esitelty konfiguraatioesimerkki FortiGate-palomuurilla, jossa palomuuri tunnistaa HTTP- ja sähköpostiprotokollista luottokorttinumeroiden formaatin ja estää tiedon jakamisen.



Kuva 7. Esimerkki tietovuodon estämisestä. Konfiguraatio estää luottokorttinumeroiden lähettämisen joko web-selaimesta tai sähköpostista.

4.5 Virustorjunta

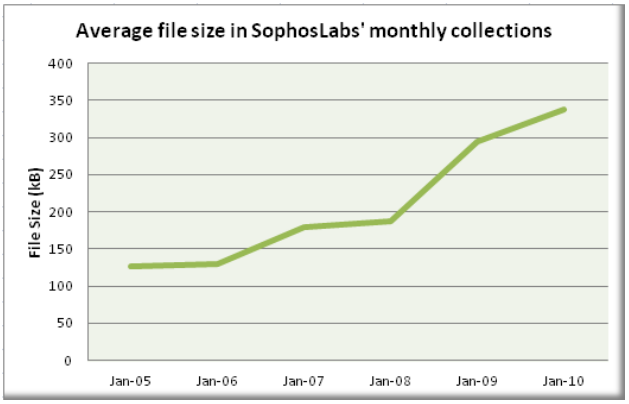
Virusten torjunta on seuraavan sukupolven palomuurin tärkeimpiä tehtäviä.

Palomuuri tutkii web- ja sähköpostiliikenteestä sekä FTP-liikenteestä sisällön ja vertaa sisältöä tunnettuihin virustunnisteisiin ja myös mahdollisiin poikkeaviin sisältöihin, joita epäillään viruksiksi. Seuraavan sukupolven palomuureilla on yleensä kaksi erilaista tapaa skannata viruksia.

Puskurointimallissa palomuuri toimii eräänlaisena välityspalvelimena asiakaskoneen ja palvelimen välillä, jossa palomuuri ohjaa asiakaskoneen avaaman liikennesession itselleen ja luo uuden session palvelimen kanssa. Tässä tilassa palomuuri lataa TCP-sessioista palvelimelta saapuvat tiedostot kokonaisuudessaan puskurimuistiin ja vertaa kokonaisuutta tunnettuihin virustunnisteisiin ja tekee myös heuristisia skannauksia, joilla voidaan havaita virukseen viittaavaa haittaohjelmakoodia [18]. Skannauksen jälkeen palomuuri lähettää tiedoston eteenpäin asiakaskoneelle, mikäli viruksia ei havaittu. Mikäli virus havaittiin liikenteestä, annetaan asiakaskoneelle ilmoitus viruksen löytymisestä ja sessio palvelimen kanssa katkaistaan.

Jos skannattava tiedosto on iso, esimerkiksi yli 10 Mt kooltaan, on palomuurilla mahdollisuus konfiguraatiosta riippuen joko sallia tiedosto ilman skannausta tai estää se. Perusteluna ison tiedoston sallimiseen voi olla tieto siitä, että tyypillinen virus on kooltaan joitakin satoja kilotavuja ja suurien tiedostojen lataaminen muistiin veisi palomuurilta kohtuuttomasti resursseja. Puskurointimenetelmä on paras keino havaita uusia viruksia ja niin sanottuja polymorfisia viruksia, jotka voivat muuttaa ohjelmakoodiaan ajan saatossa.

Virtaustilassa palomuuri skannaa siirrettävää sisältöä sitä mukaa, kuin sitä palvelimen ja asiakaskoneen välillä liikkuu [18]. Esimerkiksi 5 Mt:n tiedostoa skannataan lennosta niin pitkään, kunnes palomuuri havaitsee liikenteestä EOF (end of file) -ilmoituksen tai kunne virus havaitaan. Virtaustilan voi lisäksi asettaa skannaamaan yksittäiset paketit kokonaisuudessaan tai vain paketin sovellusdatan ensimmäiset rivit, joissa virukset suurella todennäköisyydellä sijaitsevat. Tyypillisen viruksen koko on havainnollistettu kuvassa 8.



Kuva 8. SophosLabsin raportti tyypillisen haittaohjelman koosta [19].

Hyvänä puolena virtaustilassa on skannauksen nopeus. Liikennettä siirretään suoraan asiakaskoneelle sitä mukaa, kuin sitä palvelimelta saadaan, eikä palomuurin tarvitse varata yhtä paljon resursseja liikenteen käsittelyyn. Haittapuolina voi olla väärien hälytysten syntyminen, sillä palomuurin pitää saaduista yksittäisistä IP-paketeista verrata sisältöä tietokantaan ilman kokonaiskuvaa varsinaisesta tiedostosta.

Esimerkiksi zip-tiedostojen sisältö voi olla vaikeasti skannattavissa, sillä palomuurin pitäisi pystyä kokoamaan ja purkamaan zip-tiedosto kokonaisuudessaan sisällön tarkkaa tarkistusta varten. Virtaustila on myös käyttäjäepäystävällinen, sillä virushavainnon tapahtuessa palomuuri saattaa katkaista yhteyden palvelimelle heti ilman minkäänlaista ilmoitusta loppukäyttäjälle.

Palomuurivalmistajilla on usein saatavilla erikseen palveluna myös niin sanottu sandboxing-ominaisuus [20]. Sandboxiin palomuuri voi epävarmoissa tilanteissa lähettää skannauksen yhteydessä tiedoston tarkempaa analysointia varten. Suljetussa sandboxing-ympäristössä tiedosto suoritetaan ja sen käyttäytymistä verrataan haittaohjelmien tyypillisesti suorittamiin toimiin. Palomuurin on näin mahdollista havaita verkosta polymorfisten- ja APT-virusten uusia iteraatioita sekä myös ”zero-day”-hyökkäyksiä uusien virusten ja muiden haitakkeiden ilmestyessä ensimmäistä kertaa.

Sandboxing-ominaisuudessa on myös se hyöty, että mikäli tarkistettavaksi toimitettu tiedosto luokitellaan virukseksi, valmistaja lisää siitä tunnisteen tietokantaansa ja näin tunniste leviää päivityksenä globaalisti kaikkiin valmistajan palomuurien tietokantoihin.

4.6 Sähköpostisuodatus

Seuraavan sukupolven palomuurit pystyvät estämään roskaposteja ja muita haitallisia sähköposteja erilaisin menetelmin [21]. Yksinkertaisin menetelmä on lisätä käsin lähettäjän IP-osoite tai aliverkko mustalle listalle estetyksi. Mustalle listalle voi lisätä myös lähettäjän sähköpostiosoitteen tai rakentaa niin sanotulla säännöllisellä lausekkeella tarkan funktion, jolla estetään lähettäjä. Ylläpitäjällä on myös mahdollisuus lisätä suodatusprofiiliin kiellettyjen sanojen tarkistuslista. Jos esimerkiksi sähköpostiviestin otsikosta löytyy kielletty sana, viesti estetään välittömästi.

Roskapostien dynaamisen sisällön vuoksi palomuurien on hankala torjua niitä pelkillä ylläpitäjän käsin tekemillä määrityksillä. Valmistajilla onkin usein myytävänä erillisiä sähköpostien suodatukseen tarkoitettuja lisenssejä, jotka voidaan aktivoida palomuurilla. Näin palomuuri saadaan kytkettyä valmistajan tai kolmannen osapuolen reaaliaikaiseen suodatuspalveluun. Palveluun kytkettynä palomuurilla on konfiguraatiosta riippuen mahdollisuus lähettää lukuisia tarkistuspyyntöjä sähköpostiskannauksen aikana. Näihin palveluihin lukeutuvat sähköpostin lähettäjän IP-osoitteen tarkistus globaalilta mustalta listalta, sähköpostin sisältämien URL-osoitteiden ja hyperlinkkien tarkistus sekä sähköpostin tarkistussumman vertailu. Kuvassa 9 on esimerkki käsin luodusta suodattimesta.

```
security {
    utm {
        custom-objects {
            url-pattern {
                permit {
                    value [ "bob@domain-abc.net" "joe@domain-abc.net" 150.150.150.10 ];
                }
                deny {
                    value "domain-xyz.net";
                }
            }
        }
        feature-profile {
            anti-spam {
                address-whitelist permit;
                address-blacklist deny;
                sbl {
                    profile spam-email {
                        no-sbl-default-server;
                        spam-action block;
                    }
                }
            }
        }
    }
}
```

Kuva 9. Anti-Spam-suodatuskonfiguraatio Juniperin SRX-palomuurin komentoriviltä tehtynä.

4.7 SSL-salauksen purkaminen

NSS Labs -tutkimuslaitoksen mukaan SSL/TLS salatun liikenteen määrä kasvoi vuosien 2015 ja 2016 välillä jopa 90 % ja 40,5 % verkkosivuista käytti salausta liikenteelle heinäkuussa 2016 [22]. Lisäksi tutkimusyhtiö Gartnerin mukaan vuonna 2017 yli 50 % kaikista verkkohyökkäyksistä hyödyntää salattuja yhteyksiä [23] ja esimerkiksi kuuluisa Zeus-bottiverkko hyödyntää salattuja yhteyksiä komentokeskuksen kanssa kommunikointiin.

Seuraavan sukupolven palomuurin UTM-ominaisuudet ovat hyödyttömiä, mikäli palomuurin lävitse kulkeva liikenne on salattua, sillä protokolladekooderit eivät pysty lukemaan sovellusdataa ja tunnisteiden vertailu on tuloksetonta. Jotta liikenne voidaan skannata, on palomuureille kehitetty erikseen SSL-liikenteen purkaminen.

SSL-salauksen purkamiseen liittyy teknisiä ja lainsäädännöllisiä haasteita. Suomessa lainsäädännön näkökulmasta SSL-salauksen purkamista osittain estää laki yksityisyyden suojasta työelämässä ja sen pykälä 21, yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä [24]. Myös lähtökohtaisesti verkkoliikenteestä kertyvät yksilöivät teletunnistetiedot ovat luottamuksellisia ja perustuslain mukaisia perusoikeuksia viestinnän koskemattomuudesta [25; 26].

Työnantajan näkökulmasta työntekijöiden verkkoliikenteestä saatuja tietoja, jotka eivät suoraan liity työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, ei saa käyttää työnjohto-oikeudelliseen toimiin, kuten työntekijöiden seurantaan tai tarkkailuun. Tunnistetietojen koskemattomuus koskee niin salattua kuin salaamatontakin liikennettä, mutta SSL-salauksen purkamisen yhteydessä yrityksen työntekijöiden pitäisi olla tietoisia siitä, että myös salattu tietoliikenne tullaan tarkistamaan. Yritys voi tiedottaa työntekijöilleen salatun liikenteen purkamisesta esimerkiksi tietoturvaohjeistuksessaan [24].

Seuraavan sukupolven palomuureilla on myös joissakin tapauksissa teknisesti mahdollista kertoa käyttäjälle salatulle HTTPS-sivustolle siirtymisen yhteydessä, että liikenne tullaan purkamaan ja tarkistamaan. Työntekijöiden yksityisyydensuojaa voidaan teknisellä tasolla kunnioittaa myös purkamalla salattua liikennettä vain osittain tarkoin määritellyllä palomuurisääntökannalla, kuten sallimalla sosiaalisen median sivustot omassa palomuurisäännössään ilman salauksen purkamista. Joissakin tapauksissa palomuurin SSL-salauksen purkamiseen käytetyssä konfiguraatiossa on mahdollista hyödyntää

web-suodatuksen kategorioita, joilla voidaan automaattisesti poistaa purkamisen piiristä esimerkiksi terveydenhoitoon ja finanssiasiointiin liittyvät sivustot.

Teknisellä tasolla palomuuri toimii välityspalvelimena asiakaskoneen ja palvelimen välillä tapahtuvassa SSL-kättelyssä niin, että varmenteiden vaihdon aikana palomuuri tarjoaa omaa varmennettaan sekä asiakaskoneelle että palvelimelle. Käytännössä syntyy kaksi SSL-salattua sessiota: yksi palomuurin ja palvelimen välille ja toinen palomuurin ja asiakaskoneen välille. Liikenteen saapuessa SSL-salattuna palvelimelta palomuurille SSL-salaus puretaan, liikenne skannataan läpi haittaohjelmista UTM-profiileilla ja kryptataan uudelleen palomuurin omalla varmenteella. Tämän jälkeen liikenne siirretään eteenpäin asiakaskoneelle [27].

Huomioitavaa on, että mikäli palomuurin omaa varmennetta ei ole allekirjoitettu tunnetun varmentajan toimesta (certificate authority), saa asiakaskone aina varoituksen epäkelvosta varmenteesta. Palomuurin itsensä allekirjoittamaa varmennetta on mahdollista käyttää, mikäli asiakaskoneille on kyseinen varmenne asennettu esimerkiksi Windowsin AD-ryhmäpolitiikan avulla ja palomuuri merkitty luotetuksi varmentajaksi.

Koska palomuuri SSL-purkamisen aikana käytännössä toimii niin sanotulla ”Mies välissä” (man-in-the-middle) -periaatteella, on salauksen purkamisessa paljon teknisiä haasteita. Osa verkkosivuistoista ja muista sovelluksista tarkistaa myös asiakaskoneen tarjoaman varmenteen oikeellisuuden niin sanotulla HTTP Public Key Pinning (HPKP)- tai HTTP Strict Transport Security (HSTS) menetelmillä [28], joilla palvelin voi varmistua liikenteen koskemattomuudesta. Käytännön esimerkkinä kyseisiä tarkistuksia tekevistä sovelluksista on Googlen Chrome-selain.

Lisäksi palomuurin täytyy tukea SSL-kättelyssä käytettyjen varmenteiden salaustapoja ja varsinainen purkaminen voi rajoittua vain tietyille protokollille kuten, HTTPS:lle, SSH:lle, FTPS:lle sekä salatuille sähköpostiprotokollille. Erityisen ongelmallisia ovat myös yksinoikeudella patentoidut salausprotokollat, joita palomuuri ei pysty käsittelemään. Myös UDP-kuljetuskerroksella toimivan Datagram Transport Layer Securityn (DTLS) purkaminen voi olla palomuurin kannalta vaikeaa tai mahdotonta salauksen dynaamisen vuoksi. DTLS:ää on ehdotettu erityisesti teollisen internetin laitteiden salausprotokollaksi [29].

4.8 Käyttäjien hallinta ja UTM-ominaisuudet

Käyttäjien hallinnalla viitataan palomuurin näkökulmasta siihen, että palomuuri pystyy yhdistämään verkossa jo tunnistautuneen käyttäjän käytössä olevaan IP-osoitteeseen tai päätelaitteeseen. Käyttäjien hallintaa voidaan hyödyntää myös UTM:ssä esimerkiksi vaatimalla tunnistautumista tietyissä olosuhteissa suodatusprofiilin laukaisemana.

Jo lokituksen vuoksi on tärkeää, että verkossa olevat käyttäjät pystytään yhdistämään IP-osoitteisiin lokien myöhempää tarkastelua varten. Tämän lisäksi palomuurille avautuu uusia mahdollisuuksia sallia tietynlaisia resursseja ainoastaan esimerkiksi tiettyyn Active Directory -ryhmään kuuluville käyttäjille. Tällainen single-sign-on-menettely on tehokas tapa estää luvattomien käyttäjien verkon käyttö kokonaan.

Tulevaisuudessa NGFW-palomuurien on ennustettu muuntuvan yhä enemmän kontekstipohjaisiksi ohjelmistopohjaisten verkkojen (SDN) ja koneoppimisen myötä [30], jolloin myös UTM-ominaisuuksilla saadaan tarkkaa dataa verkossa olevista käyttäjistä ja sovelluksista.

Jo nyt sovellusten hallinta on mahdollista kytkeä yhteen käyttäjien hallinnan kanssa. Palomuuri voi käydä hakemassa tiedot yrityksen verkossa kirjautuneena olevista käyttäjistä AD-palvelimelta ja sovellusten hallinta tarkkailee yksittäisten käyttäjien käyttämien sovellusten normaalia toimintaa ja pystyy havaitsemaan poikkeamia sovelluksen tai käyttäjän toiminnassa [31]. Palomuurien on mahdollista myös yksilöidä sisäverkossa olevat päätelaitteet valmistajan mukaan muun muassa MAC-osoitteen ja sovelluksen hallinnan kaappaamaan datan perusteella esimerkiksi HTTP-GET-pyynnöistä, joissa käyttäjien selaimet ilmoittavat käyttöjärjestelmänsä web-palvelimelle. Näin on mahdollista rajoittaa vaikkapa tiettyjen valmistajien laitteiden liikennöintiä.

5 Palomuurin sääntökannan rakentaminen ja UTM-suodatusten lisääminen

5.1 Työn lähtökohdat

Insinöörityön osana rakennettiin laboratorioympäristössä seuraavan sukupolven FortiGate-palomuurille palomuurisääntökanta, johon kytketään päälle yleisimmin käytetyille sovelluksille yksilöidyt UTM-profiilit. Perusteluina tarkoin eritellylle sääntökannalle on se, että kaikelle liikenteelle ei tarvita kaikkia mahdollisia suodatusominaisuuksia. Sovellus- ja protokollakohtaisilla palomuurisäännöillä ja UTM-skannauksilla säästetään palomuurin rajallista suorituskykyä ja ehkäistään skannausten mahdollisia negatiivisia vaikutuksia yksittäisten sovellusten toimivuuteen.

Varmin tapa saada yrityksen tietoliikenne ja samalla liiketoiminta jumiin on lisätä kaikki mahdolliset UTM-ominaisuudet kaikelle mahdolliselle lähtevälle liikenteelle. Vaikka nykyaikainen palomuuri ohjaakin liikennettä sovelluskohtaisille mikropiireille (ASIC) käsiteltäväksi, on esimerkiksi keskitetyssä palomuuriratkaisussa jopa suuren kokoluokan palomuuri nopeasti jumissa suoritustehon osalta, mikäli kaikki liikenne pitää suorittaa useamman syväskannausvaiheen läpi.

Työssä rakennettiin yleisimmille protokollille, kuten HTTP:lle, HTTPS:lle, FTP:lle ja sähköpostiprotokollille, omat UTM-profiilit, jotka skannaavat vain kyseisen protokollan liikenteen sisällön. Lisäksi SSL-salauksen purkaminen lisättiin aluksi HTTPS-liikenteelle ja myöhemmin myös kaikelle muulle liikenteelle sovellusten tunnistamiseen tarkoitetulla AC-profiililla.

Työn lopuksi vertailtiin lyhyesti verkkoliikenteeseen aiheutuvia viiveitä, kun palomuuri skannaa liikennettä puskurointi- ja virtaustiloissa ja ilman suodatusprofiileja.

5.2 Suunnittelu

Palomuurisääntöjen luominen alkoi ensiksi sen suunnittelulla, mitä sovelluksia yrityksellä voisi olla käytössä ja onko liikenteen tarkoitus kulkea vain yrityksen omassa sisäverkossa vai tarvitseeko sovellus pääsyn Internetiin. Monet palvelut on nykypäivänä tuotettu pilvipalveluna, joten esimerkiksi sellaiset sovellukset kuin Salesforce ja Microsoft Office

365 tarvitsevat pääsyn Internetiin. Pilvipalveluiden luonteen vuoksi on käytännössä todella työlästä sallia kyseisiä palveluita perinteisillä lähde -ja kohde IP-osoitteisiin pohjautuvilla palomuurisäännöillä. joten pilvipalvelut otettiin erityiseen tarkasteluun sen varalta, että voitaisiin sallia omilla sovelluskohtaisilla AC-profiileilla.

Mitä tulee suuriin ja keskisuuriin yrityksiin, on niillä omina tuotettuina palveluina useimmiten ainakin Active Directory-, DNS- ja DHCP-palvelimet ja kyselyt näille palvelimille kulkevat joko suoraan suljetussa sisäverkossa, eristetyssä WAN-yhteydessä kuten MPLS tai salatussa VPN-tunnelissa, joten liikenne näihin tunnettuihin palvelimiin voitiin sallia palomuurilla saman tien.

Internet-liikenteelle päädyttiin siihen lähtökohtaan, että perinteisillä palomuurisäännöillä voidaan sallia esimerkiksi tiedostonsiirto tunnetun kumppanin palvelimelle, mikäli liikenne on lähtökohtaisesti salattua esimerkiksi SFTP- tai SSH-protokollilla. Muussa tapauksessa kumppanille rakennetaan mahdollisuuksien mukaan VPN-tunneli ja salaamaton liikenne kuljetaan salatussa tunnelissa kumppanin palvelimelle.

HTTP- ja HTTPS-liikenteelle, jotka eivät suoraan liity yrityksen liiketoimintaan luotiin omat palomuurisäännöt sekä molemmille niin, että IPS-profiili skannaa yleisimmät tunnetut hyökkäykset web-selaimessa. Lisäksi virustentorjunta-profiili lisättiin skannaamaan ainoastaan HTTP-protokollasta virukset ja web-suodattimeen merkattiin päälle kategoriapohjainen suodatus, jossa estettiin ainakin alustavasti aikuisviihde ja FortiGuard-palvelun tunnistamat haitalliset verkkosivut ja URL-osoitteet.

5.3 Verkkotopologia

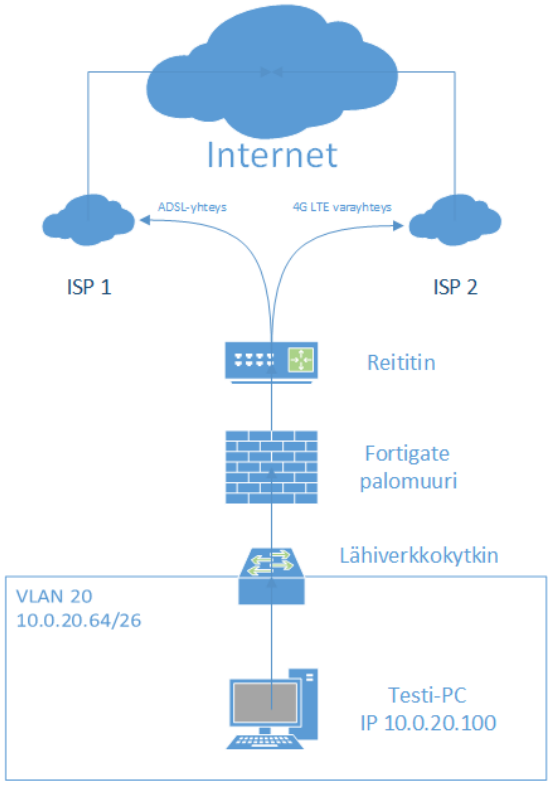
Työ tehtiin laboratorioympäristössä, jossa oli olemassa kaksi Internet-liittymää. Koska palomuurilla harvoin on tarvittavia moduuleja WAN-teknologioita varten, on topologiassa Internetiä vasten sijoitettu yksi reititin. Reititin muodostaa yhteyden Internetiin sekä ADSL- että 4G LTE -yhteyksillä. Itse reitittimelle ei konfiguroitu mitään tietoturvaominaisuuksia control plane securityä lukuun ottamatta, eli reitittimen hallinta sallittiin vain sisäverkosta.

FortiGate-palomuuri kytkettiin fyysisesti suoraan kiinni reitittimeen kahdella RJ45-Ethernet-kaapelilla, ja palomuurilla otettiin käyttöön kuormantasausominaisuus, jolla Internet-liikennettä jaetaan sessiokohtaisesti tarvittaessa 4G-varayhteydelle, jos pääyhteyden

käyttöaste ylittää 90 %. Palomuurin näkökulmasta molemmat Internet-yhteydet sidottiin yhteen ”wan-load-balance”-liitäntään, mikä helpotti palomuurisääntöjen luontia.

Palomuurin omiin liitäntöihin kytkettiin lähiverkkokytkin, johon puolestaan laboratorioympäristön tietokoneet aliverkosta 10.0.20.0/24 kytkettiin. Lähiverkossa on käytössä neljä virtuaalista lähiverkkoa (VLAN), ja jokaisen aliverkon maski on /26. Näin koko /24-aliverkko on jaettu tasan neljään osaan ja jokaisella yrityksen osastolla on oma aliverkko. Myös WLAN-vierasverkolle on oma VLAN.

Laboratorioympäristössä VLANit on nimetty seuraavasti: VLAN 10 on vierasverkolle, VLAN 20 sisäiselle IT-osastolle, VLAN 30 myynnille ja markkinoinnille ja VLAN 40 kehitys- ja tuotanto-osastolle. Varsinainen testaus suoritettiin VLAN 20:ssa sijaitsevalla koneella. Verkkotopologia on kuvattu kuvassa 10.



Kuva 10. Laboratorioympäristön verkkotopologia.

5.4 Palomuurisääntökannan määrittely

Verkkokytkentöjen ja alustavien tietoturvasääntöjen suunnittelun jälkeen aloitettiin palomuurin konfigurointi. Tässä vaiheessa palomuurilla oli jo reititys sekä sisäverkkoon että Internetiin kunnossa, joten tehtäväksi jäi sääntöjen luominen. Sisäverkossa on käytössä

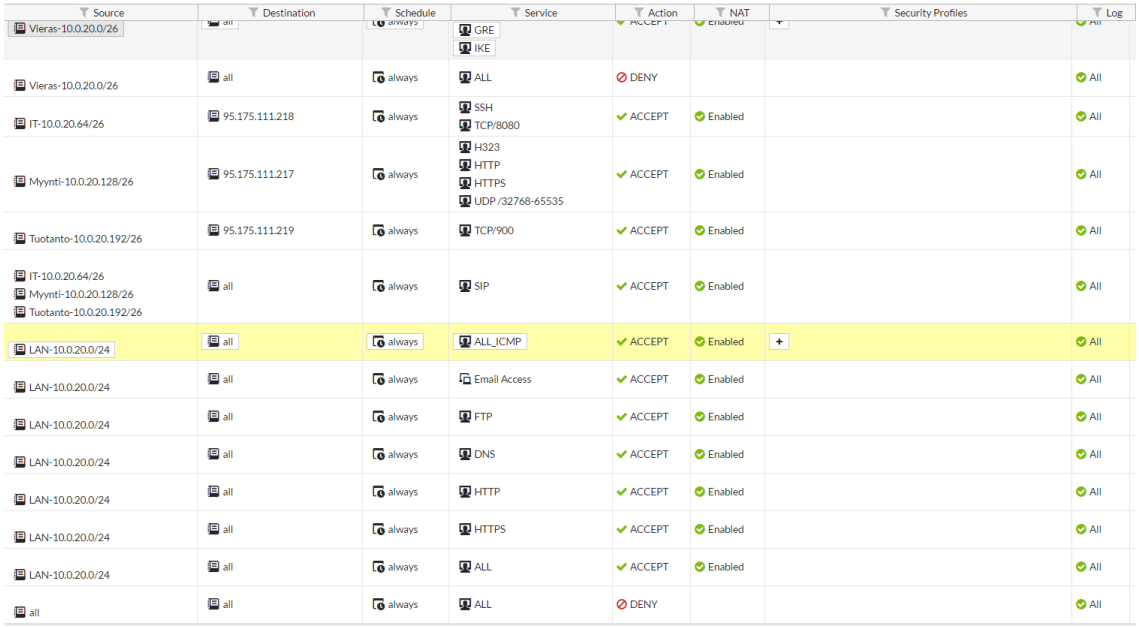
neljä VLAN-verkkoa, joten palomuurille luotiin uusi tietoturva-alue (security zone) nimeltään ”LAN”, johon kaikki VLAN-liitännät lisättiin. Tietoturva-alueen tarkoituksena on helpottaa ja yhdenmukaistaa palomuurisääntöjen konfigurointia niputtamalla samanlaisilla tietoturvavaatimuksilla olevia verkkoja yhdeksi kokonaisuudeksi. Itse tietoturva-alueen alle määriteltiin myös VLAN-kohtaisia sääntöjä.

Palomuurisäännöissä sallittiin alustavasti eri osastojen tarvitsemia yhteyksiä kumppaniyritysten ja palveluiden tarjoajien palvelimille IP-osoitteiden ja TCP/UDP-porttien perusteella. Esimerkkeinä näistä säännöistä oli IT-osaston tarvitsema pääsy etäpalvelimen hallintaan SSH-protokollalla ja valvontastatistiikan lukemiseen epästandardilla HTTP-portilla 8080. Erityistä huomiota kiinnitettiin VoIP-puhelimien liikennöintiin, ja SIP-protokollalle luotiin tässä vaiheessa oma palomuurisääntö sallimaan kaikki liikenne ulospäin, jotta puhelut yhdistyvät.

Vierasverkoksi tarkoitettu VLAN 10 eristettiin muusta sisäverkosta kokonaan ja pääsy Internetiin sallittiin hyvin rajatusti. Käytännössä tavallinen verkkoselaaminen ja VPN-tunnelointiprotokollat sallittiin, sillä vierailla on usein tarve käyttää oman yrityksensä VPN-yhteyttä töiden tekemiseen.

Yrityksen kaikille VLAN-verkoille sallittiin kaikki verkkoselaaminen HTTP- ja HTTPS-protokollilla, joille molemmille tehtiin omat säännöt UTM-profiilien käyttöönottoa silmällä pitäen. Myös nimipalvelukyselyt DNS-protokollalla sallittiin omassa säännössään.

Palomuurisäännöissä pohjimmaiseksi lisättiin sääntö, joka erikseen estää kaiken muun verkossa kulkevan liikenteen. Tämä kuitenkin havaittiin hyvin nopeasti toimimattomaksi ratkaisuksi, sillä esimerkiksi Microsoft Office 365:n palvelut käyttävät laajalti myös niin sanottuja TCP/UDP-yläportteja ja käytännössä sääntö esti esimerkiksi videopuheluiden toiminnan kokonaan. Ratkaisuksi otettiin lopulta käyttöön sääntö, jossa sallitaan kaikki portit kaikkiin IP-osoitteisiin. Tähän sääntöön kytkettiin päälle myöhemmin UTM-profiilit, joilla suodatetaan sallittu liikenne halutun laiseksi. Kuvassa 11 näytetään osa luoduista palomuurisäännöistä ennen UTM-profiilien päälle kytkemistä.



Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Vieras-10.0.20.0/26	all	always	GRE IKE	ACCEPT	Enabled		All
Vieras-10.0.20.0/26	all	always	ALL	DENY			All
IT-10.0.20.64/26	95.175.111.218	always	SSH TCP/8080	ACCEPT	Enabled		All
Myynti-10.0.20.128/26	95.175.111.217	always	H323 HTTP HTTPS UDP /32768-65535	ACCEPT	Enabled		All
Tuotanto-10.0.20.192/26	95.175.111.219	always	TCP/900	ACCEPT	Enabled		All
IT-10.0.20.64/26 Myynti-10.0.20.128/26 Tuotanto-10.0.20.192/26	all	always	SIP	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	ALL_ICMP	ACCEPT	Enabled	+	All
LAN-10.0.20.0/24	all	always	Email Access	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	FTP	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	DNS	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	HTTP	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	HTTPS	ACCEPT	Enabled		All
LAN-10.0.20.0/24	all	always	ALL	ACCEPT	Enabled		All
all	all	always	ALL	DENY			All

Kuva 11. Alustavasti luotuja palomuurisääntöjä.

5.5 UTM-profiilien määrittely ja käyttöönotto

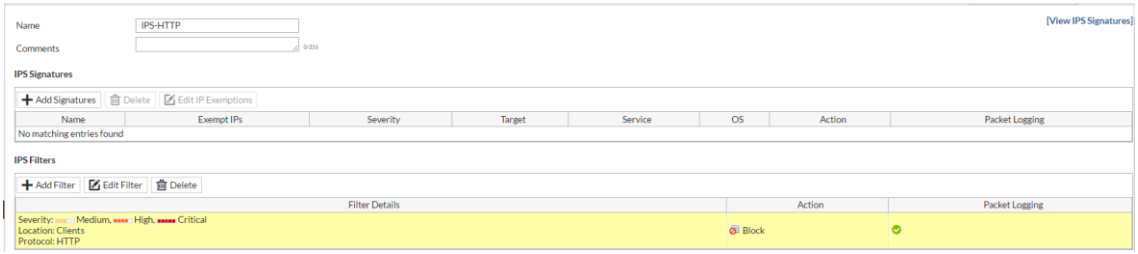
Palomuurisääntöjen luomisen jälkeen otettiin yhdistetty uhkien hallinta eli UTM käyttöön luotuihin sääntöihin. FortiGate-palomuurilla prosessi alkoi rekisteröimällä UTM-lisenssit FortiGuard-palvelussa, ja aktivoinnin jälkeen tarkasteltiin sääntökantaa uudelleen. Erityisenä painopisteenä on HTTP- ja HTTPS-liikenne, joka on ylivoimaisesti eniten käytetty protokolla, ja aiemmin luotu sääntö, joka sallii kaiken tuntemattoman liikenteen ulos palomuurilta.

Tunkeutumisestojärjestelmään määriteltiin omat profiilit erikseen HTTP-, DNS-, SIP- ja FTP-protokollille sekä profiili muille tuntemattomille protokollille. HTTP-profiilille otettiin käyttöön Fortinetin oma IPS-tietokanta, ja suodattimeen lisättiin kaikki keskitasoiset ja sitä korkeammin luokitellut hyökkäykset.

Lisäksi suodatinta hienosäädettiin niin, että IPS-skannaus tehdään vain tunnisteille, jotka kohdistuvat suoraan asiakaskoneille (clients) ja kun tunnistettu protokolla on HTTP. Lisäksi määriteltiin, että vain Windows- ja Linux-käyttöjärjestelmiin kohdistuvat hyökkäykset estetään, sillä laboratorioympäristössä ei esimerkiksi ole Mac-koneita.

Näillä määrityksillä tunnistekantaa saatiin rajattua 2 496 kappaleeseen, joten palomuuri ei käytä ylimääräisiä resursseja tunnisteiden analysointiin, jotka eivät koske sisäverkon päätelaitteita. DNS-, SIP- ja FTP-protokolille luotiin vastaavanlaiset profiilit, joissa vain

kyseiseen protokollaan kohdistuvat hyökkäykset estetään. Kuvassa 12 näytetään palomuurin graafisella käyttöliittymällä HTTP:lle luotu IPS-sensori.



Kuva 12. HTTP-liikenteelle rakennettu IPS-sensori.

HTTP-profiilin yhteydessä luotiin myös testausta varten käsin tehty tunniste, jolla estetään HTTP-POST-viestien lähetys TCP-portissa 8088.

Luotu sisältötunniste ”Block.HTTP.Post” lisättiin konfiguraatioon seuraavanlaisena FortiGaten syntaksia noudattaen:

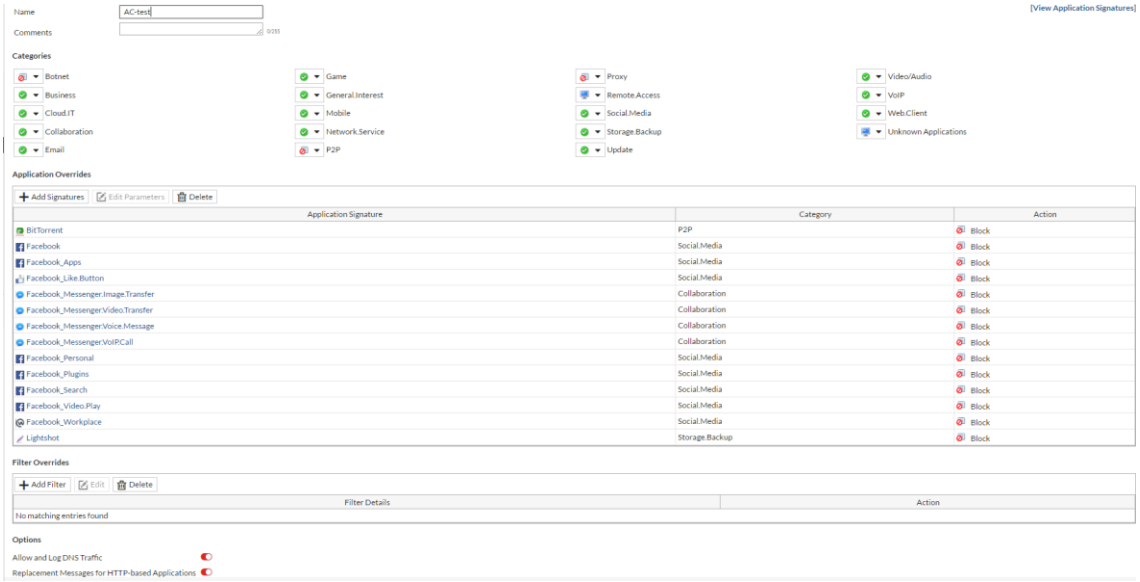
```
F-SBID(
 --attack_id 8479;
 --name "Block.HTTP.Post";
 --protocol TCP;
 --dst_port 8088;
 --pattern "|50 4f 53 54|";
)
```

Tunniste etsii jokaisesta IP-paketin sisällöstä heksadesimaaliarvoa 50 4f 53 54, mikäli kyseessä on muodostettu TCP-sessio kohdepalvelimen porttiin 8088. Heksadesimaaliarvo 50 4f 53 54 kääntyy ASCII-merkintätavalla sanaksi POST, ja mikäli kyseessä on HTTP-liikennettä, estää IPS-järjestelmä esimerkiksi täytettyjen web-lomakkeiden lähettämisen web-palvelimelle.

Sovellusten hallinnassa otettiin alustavasti käyttöön profiili, jossa estetään kategoriapohjaisesti yhteydet tunnistettuihin bottiverkkoihin, vertaisverkkoihin (peer-to-peer) ja välityspalvelinsovelluksiin, kuten kuluttajille tarkoitetut VPN-yhteydet (esim. Astrill, CyberGhost).

Lisäksi käsin lisättiin kaikki Facebookiin liittyvät tunnisteet estetyiksi, jotta Facebookin selaaminen työajalla saadaan estetyksi. Tarpeen vaatiessa Facebookin käyttö voidaan

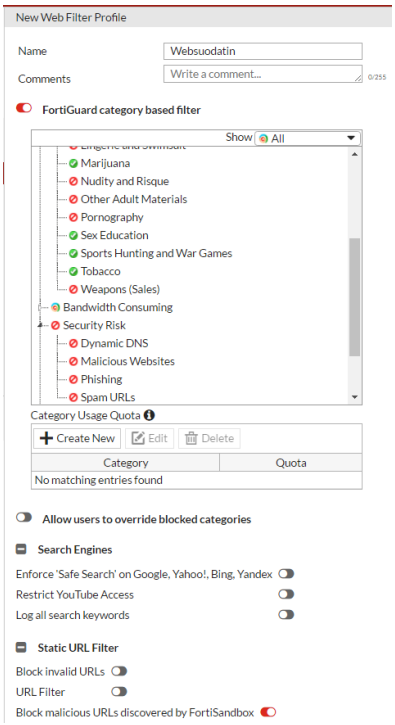
sallia rajoitetusti esimerkiksi markkinoinnin käyttöön. Varmuuden vuoksi myös BitTorrent-tunniste lisättiin käsin estetyksi, vaikka se kuuluukin jo P2P -kategoriaan. Kuvassa 13 listataan AC-profiilin estämät kategoriat ja tunnisteet.



Kuva 13. Sallitut sovelluskategoriat ja tunnisteet.

Web-suodattimessa otettiin käyttöön FortiGuard-palvelun kategoriapohjainen suodatus verkkosivustoille. Kategorioita on lukuisia, ja niistä räikeimmät kategoriat, kuten aikuisviihde ja tunnetut phishing- ja muut haitalliset sivustot, lisättiin estetyksi kuvan 14 esittämällä tavalla.

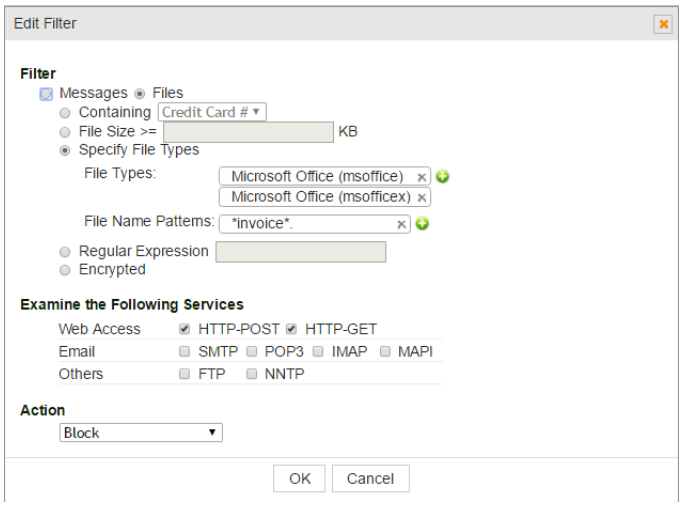
Käyttöön otettiin myös FortiGuardin FortiSandbox-ominaisuus, jossa palomuuri lähettää epävarmoissa tapauksissa verkkosivun sisällön analysoitavaksi Fortinetin palvelimille.



Kuva 14. Web-suodattimen kategoriat.

Tietovuotojen estämisessä otettiin aluksi käyttöön yksinkertainen profiili, jossa estetään .doc- ja docx-tiedostojen siirtäminen HTTP:llä Internetissä sijaitseville palvelimille, mikäli tiedoston nimestä löytyy ”invoice” eli lasku. Alun perin tarkoituksena oli luovuttaa FortiGatelle analysoitavaksi yrityksen dokumenttipohja, jossa on yrityksen logo ja nimi vesileimatunnistusta varten. Tämä ei kuitenkaan onnistunut, sillä toimenpide olisi vaatinut erillistä tallennustilaa palomuurilla, jota ei FortiGate 60E -palomuurimallissa ollut saatavilla.

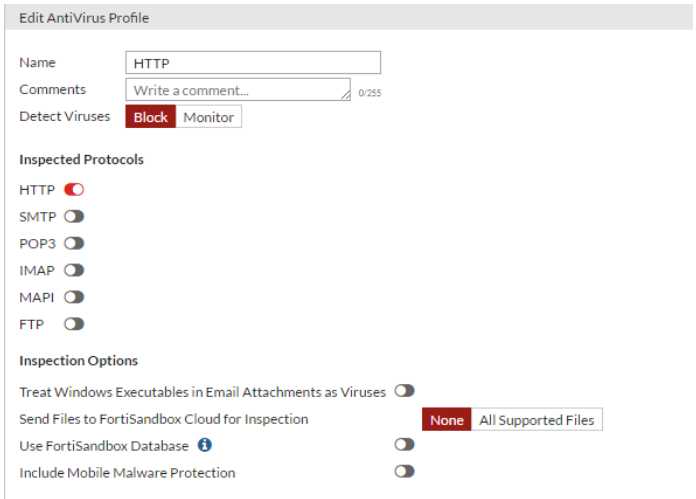
DLP-profiili konfiguroitiin käyttämään ”msoffice”-tiedostomuotoja, joihin doc- ja docx-tiedostomuodot sisältyvät, ja tämän lisäksi määritykseen lisättiin ehtolause ”*invoice*”, jolla laskutusdokumentit tunnistetaan. Konfiguraatio on esitetty kuvassa 15.



Kuva 15. Tietovuotosuojan määritelty konfiguraatio.

Virustorjuntaprofiilit jaettiin kolmeen osaan: HTTP:lle, FTP:lle ja sähköpostiprotokollille omansa. Profiileissa kytkettiin päälle kaikki FortiGuardin tavallisen tietokannan sisältämät virustunnisteet. Lisäksi sähköpostiprotokollien profiilissa kytkettiin päälle ominaisuus, joka lähtökohtaisesti käsittelee .exe-tiedostoja viruksina sähköpostien liitetiedostoissa.

Profiileissa olisi ollut vaihtoehtona ottaa käyttöön myös laajennettu virustietokanta, joka sisältää hyvin vanhoja ja muita viruksia, joita ei ole nähty globaalissa verkkoliikenteessä pitkään aikaan. Tätä tietokantaa ei tässä vaiheessa nähty tarpeelliseksi. FortiSandbox-ominaisuutta ei virustorjunnassa kytketty päälle, koska tarpeellinen lisenssi puuttui. Kuvassa 16 näytetään FortiGaten graafisen käyttöliittymän vaihtoehdot antivirusprofiilin määrittämiseen.



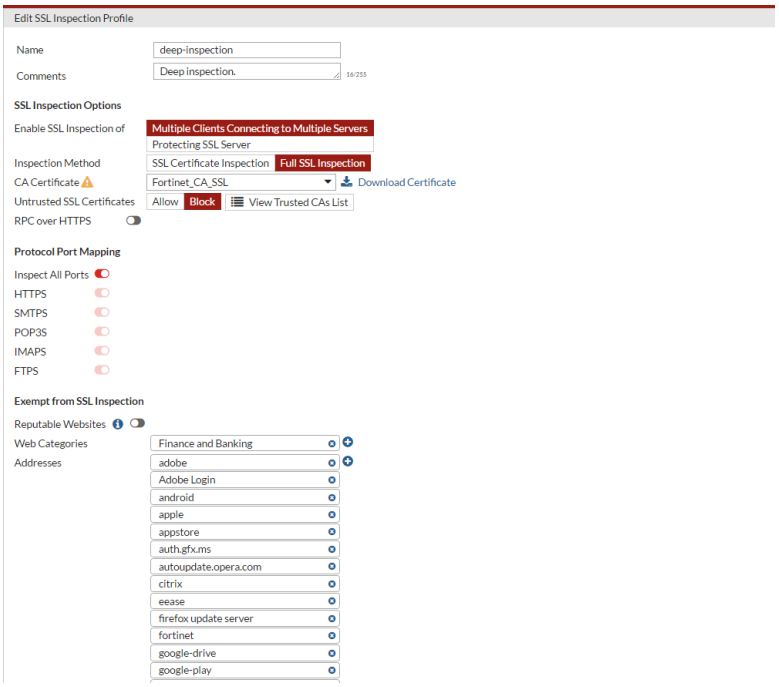
Kuva 16. Määritelty virustorjuntaprofiili HTTP-protokollalle.

SSL-salauksen purkamisessa otettiin käyttöön kaksi mallia. Yksinkertaisemmassa mallissa palomuuri tarkistaa SSL-salatuista yhteyksistä palvelimen tarjoaman varmenteen oikeellisuuden ja muut tiedot. Tämä tarkistus otettiin käyttöön yhdessä web-suojauksen kanssa vierasverkon lähtevälle HTTPS-liikenteelle. Syynä tähän oli se, että vierasverkkoon kytkeytyville koneille ei ole mahdollista lisätä palomuurin omaa varmennetta luotetuksi varmentajaksi.

Varmenteen tarkistus web-suojauksen kanssa mahdollistaa web-suojauksen kategoriapohjaisen estämisen, sillä palomuuri ei tässä mallissa toimi ”mies-välissä”-periaatteella. SSL-kättelyvaiheessa kohdepalvelimen tarjoamasta varmenteesta löytyvien tietojen perusteella web-suodatin pystyy estämään tai sallimaan liikenteen.

Toisessa mallissa SSL-salattu liikenne purettiin kokonaisuudessaan palomuurilla niin, että palomuuri tarjoaa omaa varmennettaan asiakaskoneille. Laboratorioympäristössä palomuurin varmenne asennettiin käsin testauskoneelle, mutta varmenne olisi mahdollista levittää myös esimerkiksi Microsoftin AD GPO -ryhmäsetuksella yrityksen tietokoneille.

Mikäli varmennetta ei olisi asennettu koneille, käyttäjät saisivat selaimessaan aina ilmoituksen virheellisestä varmenteesta, sillä palomuurin omaa varmennetta ei ole allekirjoitettu minkään virallisen varmentajan toimesta. Kuvassa 17 näytetään SSL-salauksen purkamiseen käytetty konfiguraatio.



Kuva 17. SSL-salauksen purkamiseen käytettävä profiili. Palomuuri tarjoaa asiakaskoneille palomuurin itsensä allekirjoittamaa varmennetta ”Fortinet_CA_SSL”.

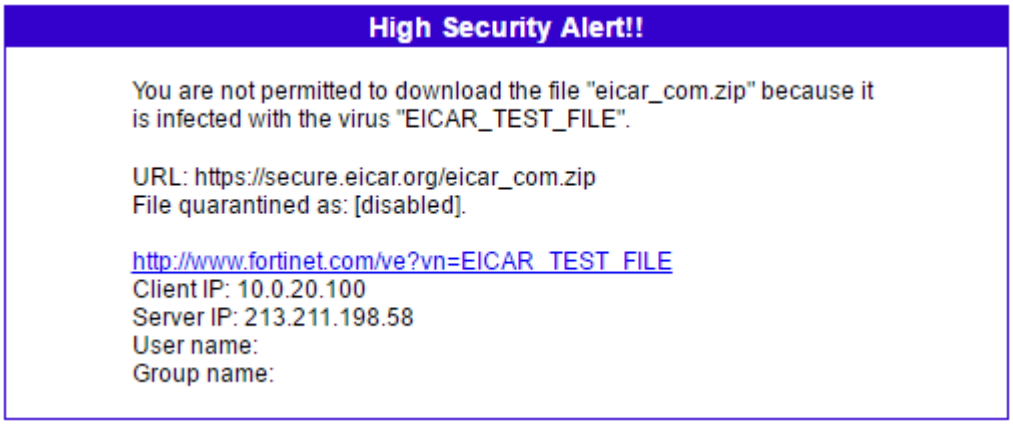
5.6 Testaus ja havaitut ongelmat

UTM-profiilien konfiguroinnin ja palomuurisääntökantaan liittämisen jälkeen siirryttiin testausvaiheeseen.

Työn testauksessa selvitettiin HTTP- ja HTTPS-protokollilla, että UTM-profiilit toimivat oikein ja estävät haitallisen ja ei-toivotun liikenteen. Lisäksi tutkittiin käsin luodun IPS-tunnisteen toimivuutta ja UTM-profiilien suorituskykyvaikutuksia verkkosivujen lataamiseen.

Profiilien testaus aloitettiin kokeilemalla, estääkö virustorjunta EICAR-testiviruksen. EICAR on yleisesti käytetty testivirus, joka on kokonaisuudessaan 68 merkkiä pitkä ASCII-teksti. Virusta yritettiin ladata selaimella osoitteesta http://www.eicar.org/anti_virus_test_file.htm ja puskurointitilassa toiminut virustorjuntaprofiili havaitsi ja eristi viruksen sekä antoi selaimessa ilmoituksen zip-tiedoston lataamisen estämisestä viruksen vuoksi (kuva 18).

Testaus suoritettiin myös salatulla HTTPS-yhteydellä, ja tämäkin koe onnistui, eli tässä vaiheessa voitiin myös alustavasti todeta SSL-purkamisen toimivan.

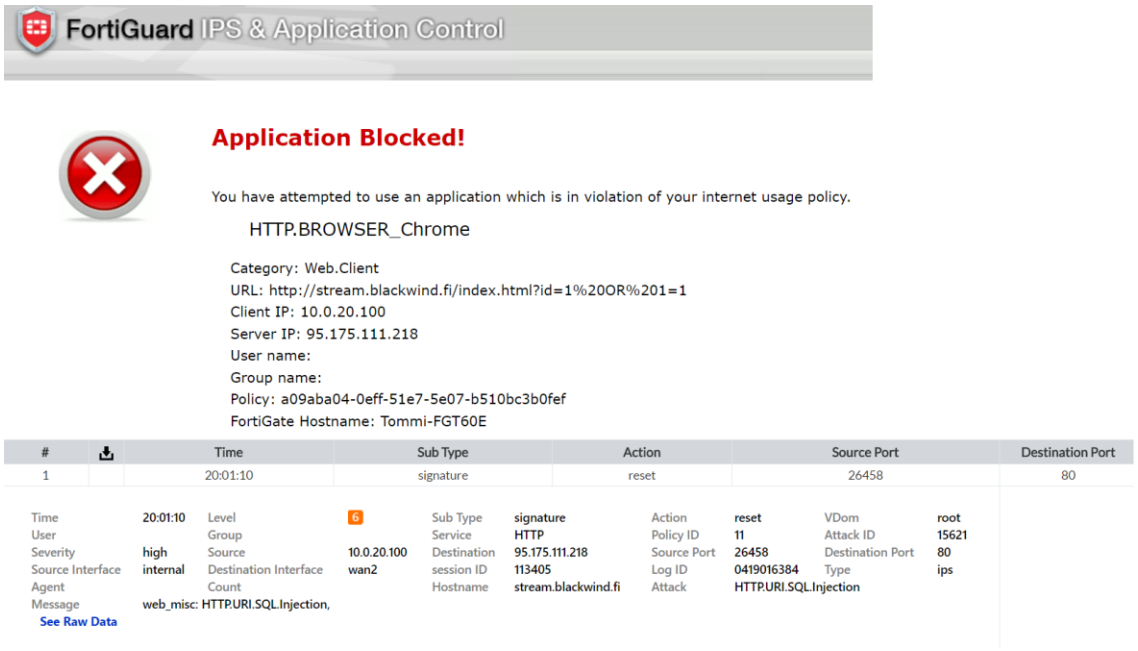


Kuva 18. Palomuuri on estänyt viruksen sisältäneen tiedoston.

Virustorjuntaa testattiin myös Fortinetin ”Test Your Metal” -kokeella osoitteessa http://metal.fortiguard.com/tests/, jossa samaa EICAR-virusta yritetään ladata selaimessa tehtävällä 18 erilaisella tavalla. Tavat vaihtelivat esimerkiksi salasanasuojatusta zip-tiedostosta zip-tiedostoon, joka sisältää useita zip-tiedostoja. Myös tässä testissä kaikki 18 koetta menivät onnistuneesti läpi, joten virustorjunnan voitiin olettaa toimivan halutulla tavalla.

Tunkeutumisestojärjestelmää muokattiin kokeen ajaksi koskemaan myös palvelimiin kohdistuvia hyökkäyksiä. Toiminnallisuutta testattiin suorittamalla hyvin yksinkertainen SQL-injektio hallinnoimalleni palvelimelle osoitteessa stream.blackwind.fi. Hyökkäysyritys suoritettiin selaimessa syöttämällä URL-osoitteeksi http://stream.blackwind.fi/index.html?id=1 OR 1=1.

Lauseke ” OR 1=1” voi hyvin huonosti suojatussa SQL-tietokannassa palauttaa esimerkiksi koko käyttäjä-salasanataulukon nähtäväksi. Testissä IPS-järjestelmä onnistuneesti esti tämän yrityksen ja palautti jälleen selaimessa käyttäjälle ilmoituksen, että yritys on estetty kuvan 19 mukaisesti.

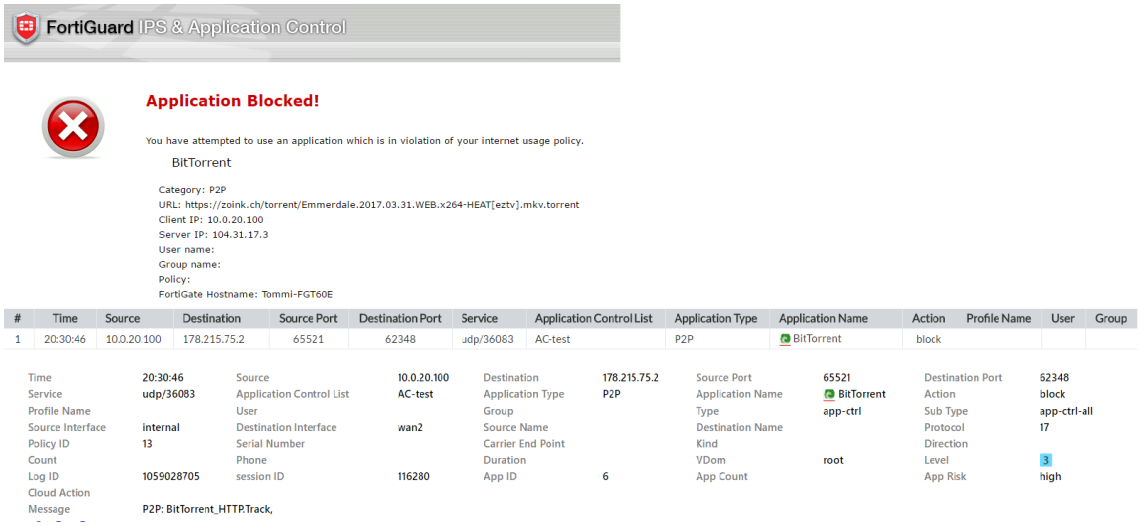


Kuva 19. Käyttäjän saama ilmoitus IPS-järjestelmän estämästä hyökkäysyrityksestä ja palomuurin lokimerkintä tapahtumasta.

Aikaisemmin käsin tehdyn tunnisteen ”Block.HTTP.Post” testaamisessa oli aluksi haasteita, sillä syötetty syntaksi ei luonut oikein toimivaa tunnistetta HTTP-POST-viestien estämiseen. Tunniste saatiin lopulta toimimaan tutkimalla tarkemmin Fortinetin dokumentaatiota aiheesta, ja kirjautumisyritys palvelimen http://stream.blackwind.fi:8088 hallintakonsoliin lopulta saatiin estetyksi, mikä ilmeni käyttäjän näkökulmasta vain yhteyden aikakatkaisuna. Palomuurin lokeja tarkastelemalla kuitenkin saatiin varmuus siitä, että yhteys todella oli estetty.

Tunkeutumisestojärjestelmän perään suoritettiin testaus sovellusten estämisestä. Aikaisemmin luodussa profiilissa on estetty muun muassa BitTorrent-liikenne, jonka toimintaa testattiin ensin lataamalla torrent-tiedosto Internetistä ja sen jälkeen yrittämällä jakaa torrentia asiakasohjelmalla.

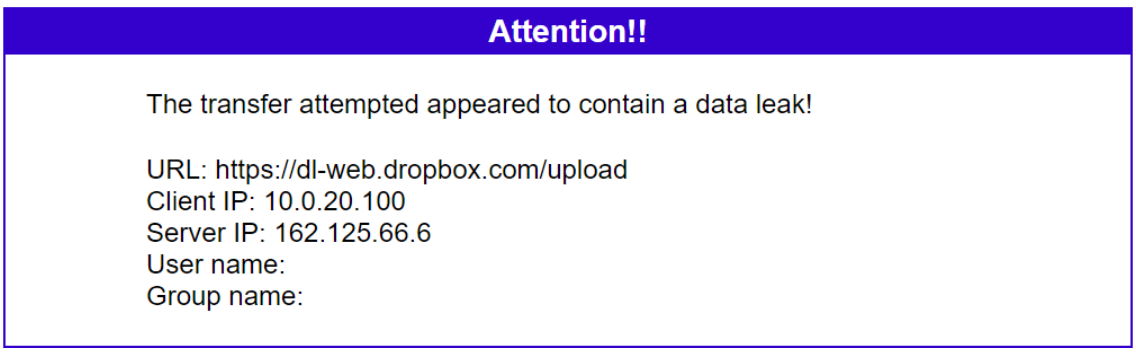
Testauksessa ilmeni, että myös web-suodatin saattoi joissakin tapauksissa estää pääsyn torrent-sivustoille, koska kategoria ”peer-to-peer file sharing” oli estetty. Kategorian sallimisen jälkeen .torrent-tiedostot laukaisivat AC-profiilin eston virheilmoituksella. Ongelmaksi muodostui, että aikaisemmin tehty konfiguraatio kuitenkin salli niin kutsutut magneettilinkit, jotka torrent-asiakasohjelma pystyy avaamaan välittömästi. Torrentien jakaminen asiakasohjelmalla pystyttiin silti estämään onnistuneesti. Kuvassa 20 näytetään selaimessa saatu virheilmoitus, kun .torrent-tiedostoa yritettiin ladata, ja lokimerkinnässä näkyy torrent-asiakasohjelman estetty sessio.



Kuva 20. Torrentien lataaminen ja jakaminen estetty onnistuneesti.

Tietovuotojen estämiselle suoritettiin koe, jossa yritettiin siirtää ”invoice1422017.docx”-nimistä tiedostoa Dropbox-pilvipalveluun. Määritelty DLP-profiili oli hyvin yksinkertainen, ja käytännössä se olisi mahdollista kiertää esimerkiksi muuntamalla .docx-tiedosto PDF-tiedostoksi, mutta toiminnallisuuden kokeilua varten konfiguraatio oli riittävä.

Web-suodatin tai sovellustenhallinta ei estä pääsyä Dropboxiin, mutta tiedostoa siirrettäessä DLP-suodatin sai konfiguraation hienosäädön jälkeen onnistuneesti testitiedoston siirron estettyä HTTPS-liikenteestä kuvan 21 mukaisesti.



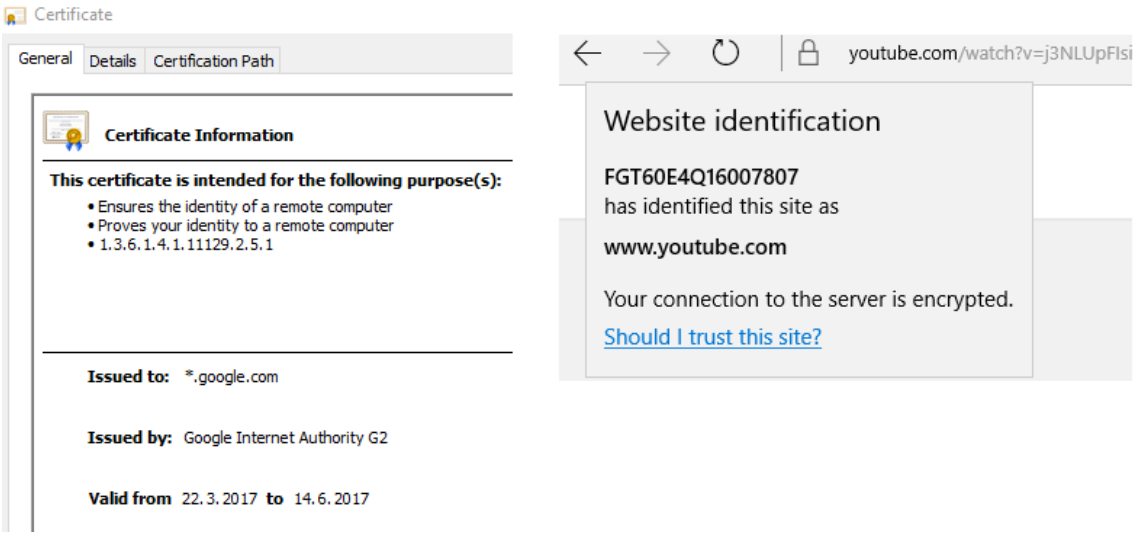
Kuva 21. Tiedoston siirtäminen estetty DLP-käytännön mukaisesti.

SSL-salauksen purkamiseen liittyvät testit osoittautuivat mielenkiintoisiksi, sillä salauksen purkamisen onnistumisesta palomuurilla ei ollut aina täyttä varmuutta. Käytetty var-

menne täytyi erikseen tarkistaa selaimen omista verkkoyhteystiedoista. Yleensä salauksen purkaminen onnistui hyvin monenlaisilla sivustoilla vierailtaessa, mutta muutamia ongelmia ilmeni.

Selvisi, että SSL-purkamiseen tarkoitetussa profiilissa oli jäänyt päälle purkamisen ohittavia poikkeuksia, kuten finanssi- ja pankkialaan liittyvät kategoriat. Lisäksi monet isot pilvipalvelut, kuten Appstore, YouTube ja Windows-päivitykset, olivat valmiina lisättyinä poikkeuksina.

Poikkeuksien poistamisen jälkeen yhteydet esimerkiksi YouTubeen Microsoftin Edge-selaimella saatiin salattua palomuurin omalla varmenteella. Ongelmalliseksi muodostui Chrome-selain, joka Googlen palveluihin yhdistäessä hyväksyi SSL-kättelyssä Googlen varmenteen palomuurin varmenteen sijaan. Erot selaimilla on esitelty kuvassa 22. Chromen käyttäytyminen johtunee HSTS- ja HPKP-varmenteiden tarkistusmenetelmästä.



Kuva 22. Käytettyjen varmenteiden ero Chrome- ja Edge-selaimilla YouTubeen yhdistettäessä. Vain Edgellä on käytössä palomuurin käyttämä varmenne.

Suorituskykytestit tehtiin kolmessa osassa käyttämällä hyväksi Chrome-selaimen debug-konsolia, joka näyttää kokonaisajan verkkosivuston sisällön lataamiselle. Tarkoituksena oli havainnollistaa palomuurin lisäämää käsittelyaikaa sivujen lataamisessa, kun yhdistetty uhkien hallinta on kytketty päälle palomuurisäännöissä.

HTTP- ja HTTPS-liikenteen kokeet suoritettiin kolmella eri palomuurin toimintamallilla, ja jokaisella toimintamallilla verkkosivun lataaminen suoritettiin 10 kertaa ja sivun lataamiseen käytetty aika kirjattiin. Lisäksi kolmannessa kokeessa ainoastaan SSL-salauksen

purkaminen kytkettiin päälle HTTPS:lle ja muut UTM-profiilit poistettiin käytöstä. HTTP-liikenteeltä poistettiin käytöstä kaikki UTM-ominaisuudet. Tällä kokeella haluttiin tutkia salauksen purkamisen nopeutta verkkosivustolle, joka hyväksyy sekä salaamatonta että salattua liikennettä.

Testauksen ajaksi kahdennetusta Internet-yhteydestä kytkettiin pois 4G-yhteys, jolloin kaikki yhteydet kulkivat 16 Mb/s -nopeuksista ADSL-yhteyttä pitkin. Lisäksi verkosta kytkettiin pois kaikki muut päätelaitteet ja varmistettiin, ettei testauskoneella ole muita sovelluksia liikennöimässä. Näillä toimenpiteillä haluttiin minimoida itse verkkoyhteyksistä aiheutuvia viivepoikkeamia.

Jokaisen sivun lataamiskerran jälkeen Chrome-selaimen välimuisti ja palomuurilla olleet sessiot tyhjennettiin. Tällä pyrittiin siihen, että sekä palomuuri että selain joutuivat käsittelemään koko prosessin uudestaan alkaen TCP- ja SSL-kättelyistä SSL-salauksen purkamiseen, UTM-profiilien tarkistukseen ja uuden session muodostamiseen. Lisäksi nimenselvityksen DNS-välimuistia ei tyhjennetty testien välissä, joten tuloksiin ei sisälly nimenselvityksestä johtuvaa viivettä. Ensimmäinen ja toinen testaus suoritettiin palomuurilla kolmessa eri toimintamallissa:

1. yksinkertaisella palomuurisäännöllä, joka sallii kaiken uloslähtevän liikenteen ilman minkäänlaisia UTM-profiileja
2. HTTPS-palomuurisäännöllä, jossa oli kytkettynä päälle puskurointitilassa seuraavat UTM-profiilit: virustorjunta, web-suodatin, sovellusten hallinta, IPS-järjestelmä, tietovuotojen esto ja SSL-salauksen purku
3. HTTPS-palomuurisäännöllä, jossa oli kytkettynä päälle virtaustilassa seuraavat UTM-profiilit: virustorjunta, web-suodatin, sovellusten hallinta, IPS-järjestelmä, ja SSL-salauksen purku; tietovuotosuoja ei toimi virtaustilassa, joten se kytkeytyi pois automaattisesti.

Ensimmäinen koe suoritettiin avaamalla suomenkielisestä Wikipediasta artikkeli Suomesta https://fi.wikipedia.org/wiki/Suomi. Tämä yhteys oli SSL-salattua, ja Wikipedia-sivun sisällössä ei ollut mitään, mitä UTM-profiilit olisivat estäneet.

Toinen koe suoritettiin avaamalla Helsingin Sanomien etusivu http://www.hs.fi/, joka ei ole SSL-salattua. Tässä tapauksessa web-suodattimessa oli lisätty ”Advertising”-kategoria estetyksi, mikä käytännössä poisti mainokset Helsingin Sanomien etusivulta.

Kolmannessa kokeessa ainoastaan SSL-salauksen purkaminen jätettiin päälle palomuurisäännöissä ja HTTPS-liikenteen purkamisen nopeutta verrattiin, kun sivu ladattiin salaamattomalla HTTP:llä ilman UTM-suodatuksia. Testaus suoritettiin kuvasivusto imgur.com:iin.

Testaustulokset on esitetty liitteessä 2.

Ensimmäisessä testauksessa voidaan nähdä suoraan, että puskurointitilassa toimivat profiilit lisäävät sivun lataamisaikaan noin yhden sekunnin. Mielenkiintoisesti SSL-salauksen purkaminen ei juurikaan nostanut viiveitä, sillä virtaustilassa päästiin lähes samoihin lukemiin kuin ilman suodatuksia.

Toisessa testauksessa erot eivät olleet yhtä huomattavia. Testissä pitää ottaa huomioon web-suodattimen estämien mainosten vuoksi muodostettujen yhteyksien vähäisempi määrä ja ladatun sisällön pienempi koko kuin ilman suodatusta, minkä ansiosta käsittelyaika oli samaa luokkaa.

Kolmannessa testissä SSL-salauksen purkaminen lisäsi imgur.com:n latausaikaa huomattavasti. Tässä testissä käytetty sivusto oli tarkoituksella sisällöltään monimutkaisempi kuin HTTPS-testissä käytetty Wikipedia. Salauksen purkamisen hitaus tässä testissä selittyy muun muassa imgur.com:n sisältämillä Javascriptien tekemillä ristiviittauksilla. Palomuuri joutui purkamaan samaan aikaan useita SSL-salattuja sessiota muun muassa Facebookiin viitatuissa yhteyksissä.

6 Yhteenveto

Insinöörityön tekemisen lähtökohtana oli oma päivittäinen asiantuntijatyöskentely ulkoistettuja tietoturvapalveluita myyvässä tietoliikenneyrityksessä. Usein asiakkaille tehtyjä muutoksia ja uusia käyttöönottoja on vaikea testata itse, koska pääsyä asiakkaan sisäverkossa oleville päätelaitteille ei ole. Yksi suurimpia motiiveja työn tekemiseen olikin, että pääsen itse testaamaan loppukäyttäjän näkökulmasta UTM-profiilien toimivuutta.

Palomuurien UTM-ominaisuudet luovat korvaamatonta lisäarvoa yrityksen tietoturvalle, mutta ylläpitäjien täytyy olla perillä yrityksen tietoturvavaatimuksista. Ulkoistettujen palveluiden tarjoajien ja asiakkaan välisessä kommunikaatiossa voi tulla virheitä, ja valitettavan usein näkeekin palomuurin konfiguraatiossa tehottomia tai väärin määriteltyjä suodatuksia. Insinöörityön aikana laboratorioympäristössä käytössä ollut palomuuri toimi myös oman kotiverkkoni yhdyskäytävänä, ja kahden kuukauden aikana UTM:n toiminnallisuudessa tuli toisinaan ihmeellisyyksiä vastaan. Toisinaan verkkosivustot eivät suostuneet latautumaan ollenkaan tai latautuivat hyvin pitkällä viiveellä. Epäilyksenä oli, että jokin suodatusprofiileista vastaava prosessi palomuurilla hidasteli tai web-suodatin odotti pitkään vastausta jonkin sivuston muualle viittaamaan osoitteeseen.

Tarkoituksella vierailin myös haitallisilla verkkosivuilla testatakseni suodatusta, mutta hieman yllättäen esimerkiksi web-suodatin päästi minut toisinaan semmoisille sivustoille, jotka testauskoneelle asennettu F-Secure-tietoturvaohjelmisto osasi estää. Tämä toimi hyvänä muistutuksena siitä, että päätelaitteen tietoturvasta ei voida luopua kokonaan eikä palomuuri ole tietoturvan kokonaiskuvassa kuin ensimmäinen puolustuslinja.

Omassa asiantuntijatyöskentelyssäni FortiGate-palomuurien UTM-prosesseja joudutaan toisinaan käynnistämään kokonaan uudestaan, sillä ohjelmistokoodissa tuntuu olevan virheitä, jotka syövät esimerkiksi palomuurin muistia kohtuuttomasti. Palomuureilla on yleensä suojausmekanismeja tilanteisiin, joissa joko fyysisen muistin tai suorittimen käyttöaste on huipussa. FortiGate-palomuurilla tämä tunnetaan käsitteenä ”conserve mode”, ja käytännössä asiakkaan näkökulmasta tietoliikenne estyy ainakin osittain, kunnes käyttöaste on laskenut tietyn rajan alle.

Suorituskykytesteissä puskurointitilan lisäämä latenssi liikenteeseen ei tullut yllätyksenä, koska muuri joutuu keräämään tiedostojen datan puskurimuistiinsa. SSL-salauksen pur-

kamisen voitiin todeta lisäävän sivustojen latausaikoja huomattavasti, mikäli sivuston sisällössä on paljon SSL-salattuja ohjauksia ja muita viittauksia muihin sivustoihin. Tämä yhdistettynä useita kategorioita estävään web-suodattimeen voi toisinaan tehdä sivujen lataamisesta hyvin hidasta.

Tämän työn tarkoituksena oli perehtyä nykyaikaisen palomuurin keinoihin analysoida yritysverkossa esiintyvien uhkien torjuntaa ja sovellusten tunnistamista. UTM-teknologiat ovat seuraavan sukupolven palomuureilla vain yksi osa kokonaisuutta. Palomuurit suorittavat lukuisia muita toiminnallisuuksia, joilla yritysverkon tietoturvasta saadaan kokonaisvaltaisesti tietoturvallisempi. Näihin toiminnallisuuksiin voidaan muun muassa laskea esimerkiksi Unicast Reverse Path Forwarding -reititystarkistukset, VPN-tunnelit ja rajoitetussa määrin palvelunestohyökkäysten torjuntaan tarkoitetut DoS-sensorit.

Tietoturva on vuodesta toiseen kuuma puheenaihe, ja jatkuvasti muuttuvassa kehityksessä UTM-palomuurit pystyvät vielä toistaiseksi pysymään kehityksessä mukana. Lähitulevaisuudessa SDN-verkkojen yleistyessä myös nykyaikainen palomuuri todennäköisesti integroituu osaksi virtualisoidun verkon toiminnanohjausta, jossa palomuureista tulee yhä enemmän tietoisia verkon, sovellusten ja käyttäjien toiminnasta.

Lähteet

1 Yrityksiin kohdistuvat kyberuhat. 2016. Verkkodokumentti. Helsingin seudun kauppakamari. <https://issuu.com/kauppakamari/docs/yrityksiin_kohdistuvat_kyberuhat_20>. Luettu 21.3.2017.

2 Cyberthreat Defence Report. 2016. Verkkodokumentti. CyberEdge Group. <https://webroot-cms-cdn.s3.amazonaws.com/4814/5954/2435/2016_cyberedge_group_cyberthreat_defense_report.pdf>. Luettu 21.3.2017.

3 Vuosikertomus. 2016. Verkkodokumentti. Suojelupoliisi. <http://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/72827_SUPO_2016_FIN.pdf?571b125d7376d488>. Luettu 22.3.2017.

4 Defining the Next-Generation Firewall. 2009. Verkkodokumentti. Gartner, Inc. <http://img1.custompublish.com/getfile.php/1434855.1861.sqqycbrdwq/Defining+the+Next-Generation+Firewall.pdf>. Luettu 1.5.2017.

5 Exploring the anatomy of a data packet. 2001. Verkkodokumentti. TechRepublic. <http://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/>. Luettu 1.5.2017.

6 What is Unified Threat Management (UTM)? 2017. Verkkodokumentti. Kaspersky Lab. <https://usa.kaspersky.com/resource-center/definitions/utm>. Luettu 26.4.2017.

7 Li, Xin; Ji, Zheng-Zhou & Hu, Ming-Zeng. 2005. Stateful Inspection firewall session table processing. International Journal of Information Technology, Vol. 11 No. 2.

8 Denning, Dorothy. 1986. An Intrusion-Detection Model. IEEE Symposium on Security and Privacy.

9 Carter, Earl & Hogue, Jonathan. 2006. Intrusion Prevention Fundamentals. Cisco Press.

10 Wang, Ke & Stolfo, Salvatore. 2004. Anomalous Payload-Based Network Intrusion Detection. RAID 2004: Recent Advances in Intrusion Detection, s. 203–222.

11 Anitha, A & Vaidehi, V. 2006. Context based Application Level Intrusion Detection System. International conference on Networking and Services (ICNS'06).

12 APP-ID. 2015. Verkkodokumentti. Palo Alto Networks. <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief>. Luettu 27.3.2017.

13 Antunes, Joao; Neves, Nuno & Verissimo, Paulo. 2011. Reverse Engineering of Protocols from Network Traces. 18th Working Conference on Reverse Engineering (WCRE).

14 Troubleshoot Issues with URL Filtering on a FireSIGHT System. 2016. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118852-technote-firesight-00.html>. Luettu 26.4.2017.

15 Web Application Firewalls. 2015. Verkkodokumentti. SANS Institute. <https://www.sans.org/reading-room/whitepapers/application/web-application-firewalls-35817>. Luettu 28.3.2017.

16 Best Practices for DLP Implementation in Healthcare Organizations. 2015. Verkkodokumentti. Code Green Networks. <https://www.codegreennetworks.com/resources/downloads/HealthcareDLPBestPractices.pdf>. Luettu 30.3.2017.

17 Technical Note: Example of FortiGate DLP Watermarking using FortiExplorer. 2015. Verkkodokumentti. Fortinet Inc. <http://kb.fortinet.com/kb/documentLink.do?externalID=FD36722>. Luettu 28.4.2017.

18 Don’t Compromise on Visibility, Speed or Security. 2012. Verkkodokumentti. Infosecurity Magazine. <https://www.infosecurity-magazine.com/opinions/comment-dont-compromise-on-visibility-speed-or/>. Luettu 1.5.2017.

19 How large is a piece of Malware? 2010. Verkkodokumentti. SophosLabs. <https://sophosnews.files.wordpress.com/2010/07/malwaresize1.png>. Luettu 2.4.2017.

20 Greamo, Chris & Ghosh, Anup. 2011. Sandboxing and Virtualization: Modern Tools for Combating Malware. IEEE Security & Privacy 9/2011, s. 79–82.

21 Anti-Spam techniques. 2017. Verkkodokumentti. Fortinet Inc. <http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Anti_Spam/Anti-Spam%20techniques.htm>. Luettu. 26.4.2017.

22 The Encrypted Web - An Upward Trajectory. 2017. Verkkodokumentti. NSS Labs. <http://www2.nsslabs.com/l/46762/2016-10-17/4fy6lv>. Luettu 20.3.2017.

23 Protecting from a Growing Attack Vector: Encrypted Attacks. 2016. Verkkodokumentti. Radware Ltd. <https://www.gartner.com/imagesrv/media-products/pdf/radware/Radware-1-2Y7FR0I.pdf>. Luettu 2.4.2017.

24 Laki yksityisyyden suojasta työelämässä. 13.8.2004/759.

25 Sähköisen viestinnän tietosuojalaki. 16.6.2004/516.

26 Suomen perustuslaki. 11.6.1999/731.

27 Finding Hidden Threats by Decrypting SSL. 2017. Verkkodokumentti. SANS Institute. <https://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840>. Luettu 1.5.2017.

28 HTTP Strict Transport Security (HSTS). 2012. Verkkodokumentti. Internet Engineering Task Force (IETF). <https://tools.ietf.org/html/rfc6797>. Luettu 1.4.2017.

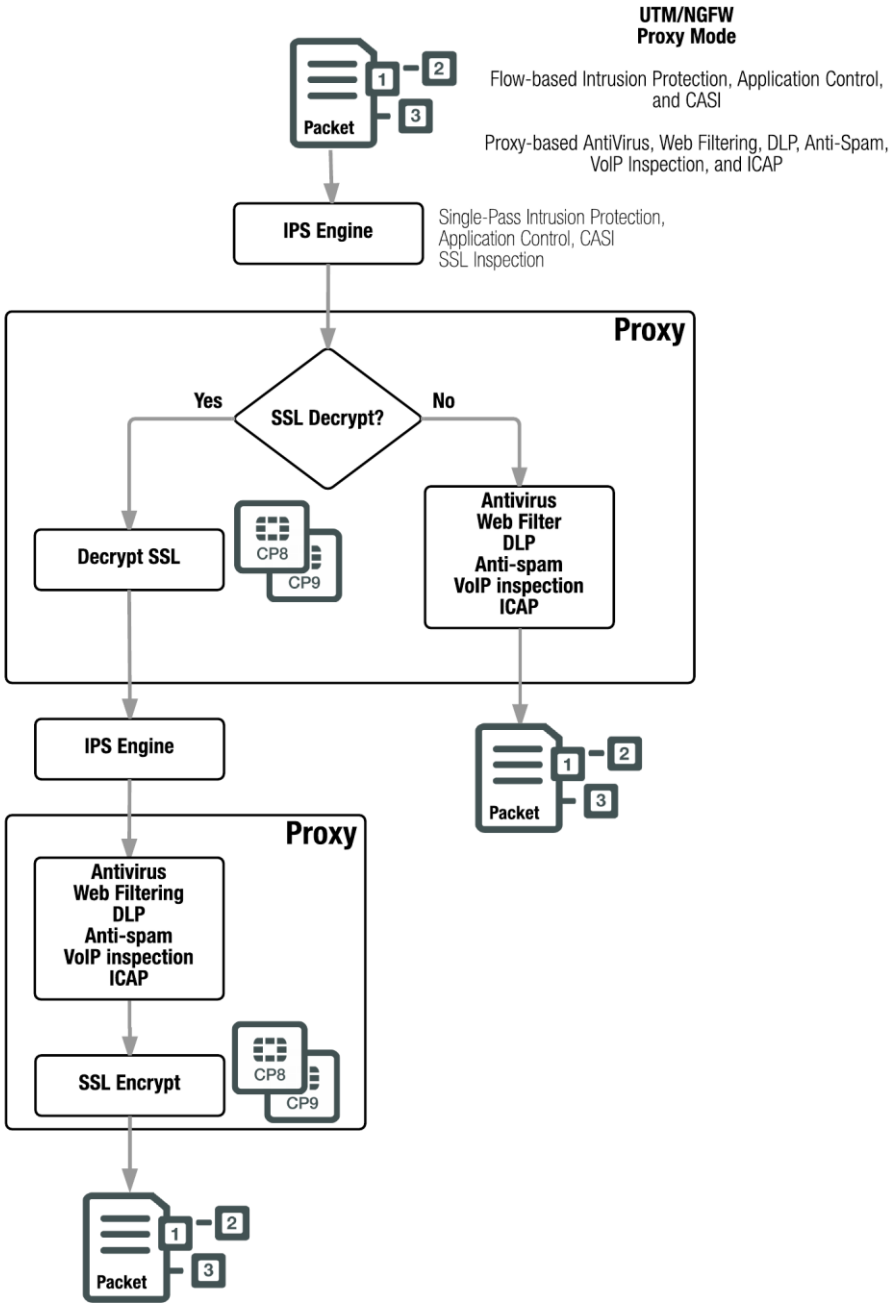
29 Kumar, Sye; Tschofenig, Hannes & Kumar, Sandeep. 2014. Securing the Internet of Things: A Standardization Perspective. IEEE Internet of Things Journal 6/2014, s. 265–275.

30 2020 Vision: What's the Future for Firewalls, SDN and the Cloud? 2016. Verkkodokumentti. Garland Technology. <https://www.garlandtechnology.com/blog/2020-vision-whats-the-future-for-firewalls-sdn-and-the-cloud>. Luettu 3.4.2017.

31 PAN-OS Administrator’s Guide, User-ID. 2017. Verkkodokumentti. Palo Alto Networks Inc. <https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/70/pan-os/pan-os/section_7.pdf>. Luettu 26.4.2017.

32 Parallel Path Processing (Life of a Packet). 2017. Verkkodokumentti. Fortinet Inc. <http://docs.fortinet.com/uploaded/files/2795/fortigate-optimal-life-54.pdf>. Luettu 4.4.2017.

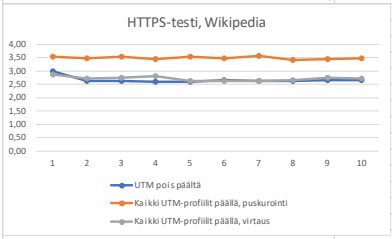
FortiGate-palomuurin prosessikaavio



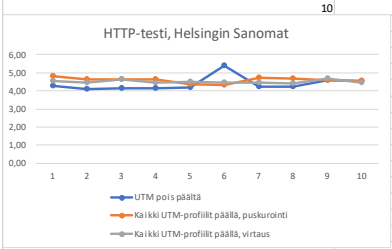
IP-Paketin kulku Fortigate-palomuurissa, kun UTM-skannaukset ovat päällä. Kaikki virtaus-pohjaiset profiilit suoritetaan ensin, minkä jälkeen siirrytään tarkempaan puskurointitilaan [32].

Suorituskykytestien tulokset

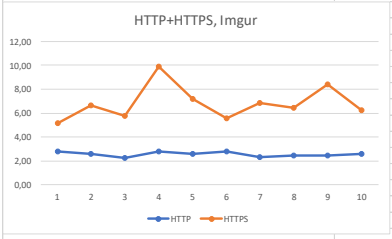
Testi 1			
Kohdesivu: https://fi.wikipedia.org/wiki/Suomi			
Ladatun websisällön koko: 3,4 Mt UTM:llä ja 3,6 Mt ilman			
IP-osoitteet: 91.198.174.208 ja 91.198.174.192	Websivun lataamiseen käytetty aika, sekunteina		
Suorituskerta	UTM pois päältä	Kaikki UTM-profiilit päällä, puskurointi	Kaikki UTM-profiilit päällä, virtaus
1	2,99	3,53	2,88
2	2,62	3,49	2,73
3	2,62	3,53	2,76
4	2,61	3,46	2,80
5	2,60	3,55	2,64
6	2,67	3,49	2,62
7	2,62	3,57	2,64
8	2,64	3,43	2,66
9	2,65	3,44	2,76
10	2,66	3,48	2,71



Testi 2			
Kohdesivu: http://www.hs.fi/			
Ladatun websisällön koko = 1,8 Mt UTM:llä ja n. 2,3 Mt ilman			
IP-osoitteet: lukuisia viittauksia mm. mainossivuille			
	Websivun lataamiseen käytetty aika, sekunteina		
Suorituskerta	UTM pois päältä	Kaikki UTM-profiilit päällä, puskurointi	Kaikki UTM-profiilit päällä, virtaus
1	4,28	4,80	4,56
2	4,08	4,62	4,45
3	4,14	4,65	4,63
4	4,13	4,62	4,47
5	4,18	4,38	4,48
6	5,38	4,32	4,47
7	4,24	4,72	4,46
8	4,23	4,68	4,42
9	4,61	4,61	4,67
10	4,56	4,55	4,46



Testi 3		
Kohdesivu: http://imgur.com/ ja https://imgur.com/		
Ladatun websisällön koko = n. 2 Mt		
IP-osoitteet: lukuisia		
	Websivun lataamiseen käytetty aika, sekunteina	
Suorituskerta	HTTP	HTTPS
1	2,78	5,13
2	2,56	6,62
3	2,21	5,79
4	2,75	9,90
5	2,57	7,19
6	2,75	5,58
7	2,29	6,84
8	2,44	6,46
9	2,42	8,41
10	2,60	6,21



UTM-profiilien vaikutus websivujen lataamisaikaan.