Tampereen ammattikorkeakoulu

Palo Alto PA5060 palomuurin ominaisuudet ja käyttöönotto

Jouni Parkki

OPINNÄYTETYÖ
Toukokuu 2019

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

PARKKI, JOUNI:
Palo Alto PA5060 -palomuurin ominaisuudet ja käyttöönotto

Opinnäytetyö 30 sivua, joista liitteitä 4 sivua
Toukokuu 2019

Tämän opinnäytetyön tarkoituksena oli luoda virtuaalipalomuuriympäristöjä kyberturvallisuuden opetus- ja tutkimuskäyttöön. Ympäristöjen toteuttamiseen käytettiin Palo Alto Networksin kolmannen sukupolven PA5060-palomuuria. Varsinaisten virtuaalipalomuurien lisäksi työn tarkoituksena oli myös luoda kirjallinen dokumentaatio mahdollisia uudelleenasennuksia varten. Lisäksi tutustuttiin muihin palomuurin ominaisuuksiin ja mahdollisuuksiin hyödyntää niitä verkkojen suojauksessa ja valvonnassa.

Virtuaaliympäristöt saatiin toteutettua annettujen määritysten mukaisesti kohtuullisen helposti. Palo Alto tarjoaa laitteisiinsa kattavan dokumentaation, jonka pohjalta palveluiden käyttöönotto on yksinkertaista. Työssä tutkittuja lisäominaisuuksia saatiin myös implementoitua verkkojen valvontaa tehostamaan. PA5060 tarjoaa muiden kolmannen sukupolven palomuurien tavoin useita tietoturvaa ja verkonvalvontaa parantavia ominaisuuksia.

Työn lopputuloksena saatiin luotua käytännöllinen opetusympäristö, jonka avulla voidaan helposti simuloida palomuurien toimintaa, lisäksi palomuurin ominaisuuksia hyödynnettiin toisten verkkojen valvonnassa. Asennusdokumentaation pohjalta ympäristön käyttöönotto voidaan tehdä uudestaan aivan alusta saakka.

Asiasanat: Palo Alto, palomuuri, tietoverkot, NGFW

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

PARKKI JOUNI:
Palo Alto PA5060 Firewall Features and Installation

Bachelor's thesis 30 pages, appendices 4 pages
May 2019

The purpose of this thesis was to create virtual firewall environments for cybersecurity study and for research purposes. The virtual environments were created using Palo Network's third generation PA-5060 firewall. In addition to creating the virtual firewalls, the purpose was to write installation guide for later reinstallations.

The virtual environments were implemented with the given specifications. Palo Alto offers comprehensive set of documentation, which facilitates installations. The additional features presented in this thesis were also implemented to improve network monitoring. Third generation firewalls, including the PA5060 offers several security and network monitoring features.

The result of this thesis was a practical learning environment, which can be used for simulating operations and behaviour of firewalls. Step-by-step installation guide helps through reinstallation from the very beginning.

Key words: palo alto, firewall, networks, NGFW

SISÄLLYS

LYHENTEET JA TERMIT

ACL	Access Control List Pääsylista
AD	Active Directory Microsoftin valmistama hakemistopalvelu
BGP	Border Gateway Protocol Reititysprotokolla
CLI	Command Line Interface Komentorivipohjainen käyttöliittymä
DPI	Deep Packet Inspection IP-paketin tutkimismenetelmä
DNS	Domain Name System Nimipalvelujärjestelmä
DMZ	Demilitarized Zone Demilitarisoitu vyöhyke
FTP	File Transfer Protocol Tiedostonsiirtoprotokolla
HA	High Availability. Tietojärjestelmien suunnittelussa käytettävä käytäntö
IDS	Intrusion Detection System Tunkeilijan havaitsemisjärjestelmä
IP	Internet Protocol Internet protokolla
IPS	Intrusion Prevention System Tunkeutumisen estojärjestelmä
IT	Information Technology Tietotekniikka
LDAP	Lightweight Directory Access Protocol Verkkoprotokolla hakemistopalveluiden käyttöön
NAT	Network Address Translation Osoitteenmuunnos
NGFW	Next Generation Firewall Seuraavan sukupolven palomuuri
OSI-malli	Open Systems Interconnection Reference Model

	Malli, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
OSPF	Open Shortest Path First. Reititysprotokolla.
OSPFv3	Open Shortest Path First v3 Uudempi versio OSPF-reititysprotokollasta
PAT	Port Address Translation Porttimuunnos
RIP	Routing Information Protocol Reititysprotokolla
SPI	Stateful Packet Inspection Tilallinen pakettien suodatus
SSH	Secure Shell Tietoliikenteen suojausprotokolla
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla
TAP	Test Access Point Verkkomonitorointityökalu
TCP	Transmission Control Protocol. Kuljetuskerroksen yhteydellinen tiedonsiirtoprotokolla.
TLS	Transport Layer Security Salausprotokolla
UDP	User Datagram Protocol Kuljetuskerroksen yhteydetön tiedonsiirtoprotokolla
VLAN	Virtual Local Area Network Virtuaalilähiverkko

1 JOHDANTO

Palomuuri on kriittinen osa tietoverkkoa. Käytännössä aina, kun sisäverkosta ollaan yhteydessä ulkoverkkoon, tarvitaan yhteyden välille palomuuri. Palomuurit voidaan jakaa karkeasti joko laite- tai sovelluspalomuureihin, tai toimintaperiaatteen mukaan tilattomiin, tilallisin ja seuraavan, eli kolmannen sukupolven palomuureihin, joissa on uusia ominaisuuksia helpottamaan verkon valvontaa ja uhkien tunnistamista aikaisempien sukupolven palomuurien ominaisuuksien lisäksi.

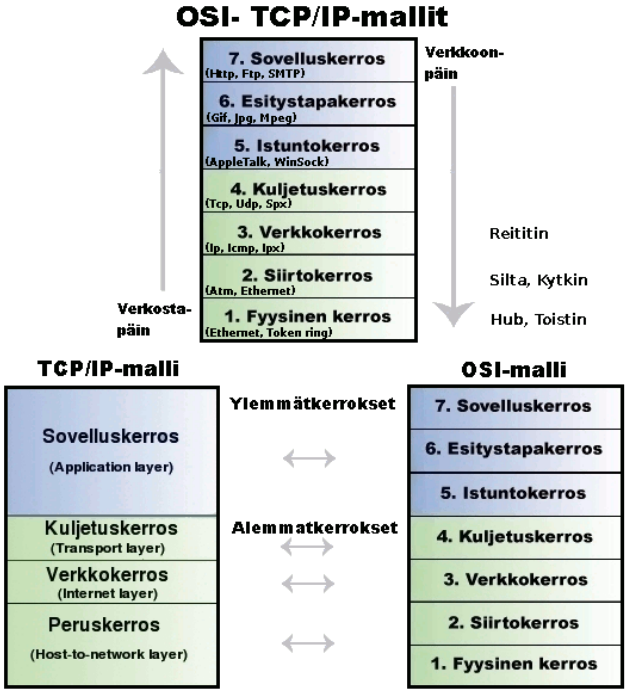
Tämä opinnäytetyö on tuotettu Tampereen ammattikorkeakoulun tieto- ja viestintätekniikan lehtorin toimeksiantona. Tarkoituksena oli ottaa käyttöön ja konfiguroida opetuskäyttöön saatu seuraavan sukupolven Palo Alto PA-5060 –palomuuri siten, että sen avulla voidaan luoda testiympäristö kyberturvallisuuden opetuksen käytännön töihin.

Tässä opinnäytetyössä käydään ensin hieman läpi eri tyyppisiä palomuureja ensimmäisen sukupolven tilattomista palomuureista aina uusimman, eli kolmannen sukupolven palomuureihin asti. Lisäksi työssä esitellään käytännöntyössä hyödynnetyn PA-5060 –palomuurin keskeisimmät ominaisuudet, joita itse työssä käytettiin, sekä eri työvaiheita palomuurin ympäristön luomisessa.

2 PALOMUURI

Palomuuri on tietoverkossa toimiva laite, joka valvoo verkkoon tulevaa ja verkosta lähtevää liikennettä. Palomuurin tehtävänä on estää asiaton pääsy verkosta toiseen, eli suojautua verkkohyökkäyksiltä, hallita ulospäin suuntautuvaa liikennettä sekä rajoittaa verkkoympäristön liikennettä.

Palomuurin, kuten tietoverkkojen yleensäkin, toimintaa ymmärtääkseen on hyvä ymmärtää ainakin perusasiat OSI-mallista ja TCP/IP-protokollista. OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa, malli perustuu siihen, että kukin kerros käyttää yhtä alemman kerroksen palveluja ja vastaavasti tarjoaa palveluja yhtä kerrosta ylemmäs. OSI-mallissa rajapinnat, palvelut ja protokollat on pidetty erossa toisistaan. TCP/IP-malliin ei ole tehty samanlaista erottelua, vaan se muodostaa hierarkian, jossa sekä verkkokerros, että kuljetuskerros ovat näkyvissä sovelluksille. Arkkitehtuurin keskeinen ajatus on, että on yksi kaikille yhteinen protokolla IP. Paketteja voidaan lähettää minkä vain protokollan päällä, joka toimii peruskerroksella ja kaikki muut sovellukset, palvelut ja protokolla käyttävät IP:tä. (Krimaka.net, 2019). Alla kuvassa 1 on esitetty TCP/IP-protokollat sekä OSI-malli.



KUVA 1 TCP/IP-protokollat ja OSI –malli (krimaka.net, 2019).

2.1 Aikaisemmat sukupolvet

2.1.1 Tilaton palomuuri

Tilaton pakettisuodatinpalomuuri on palomuurityypeistä vanhin ja myös toimintatavaltaperiaatteeltaan yksinkertaisin. Tilaton palomuuri kehiteltiin 1990-luvun alkupuolella. Suodatukseen tilaton palomuuri käyttää pääsylistaan tehtyjä sääntöjä. Määritettyjen sääntöjen perusteella palomuuri joko päästää lävitse tai estää lähetetyn paketin.

OSI-mallissa tilaton palomuuri toimii kolmannella ja neljälle kerroksella. Palomuuri tarkastelee paketin otsikkotiedoista kohdeosoitetta ja –porttia, lähdeosoitetta ja –porttia sekä IP-protokollaa. Itse paketin sisältöä palomuuri ei tarkasta ollenkaan. Sääntölistaa palomuuri käy läpi ylhäältä alaspäin, jos sääntö pätee, paketti päästetään läpi, eikä listaa käydä enää pidemmälle.

Tilattoman palomuurin etuna on sen yksinkertaisuus, koska palomuuri ei tarkasta sisältöä ollenkaan, on käsittely nopeaa. Hinnaltaan tilattomat palomuurit ovat myös halvin ratkaisu. Tilattoman palomuurin heikkous on sama yksinkertaisuus, palomuurin tietoturva on merkittävästi heikompi tilalliseen ja sovelluspalomuurin verrattaessa.

2.1.2 Tilallinen palomuuri

Toisen sukupolven palomuurit, eli niin kutsutut tilalliset palomuurit eroavat tilattomista siten, että tilallinen pitää yllä taulukkoa avatuista TCP-yhteyksistä ja hyväksyy näihin yhteyksiin kuuluvat myöhemmät paketit. Täten tilallinen muuri sallii paluuliikenteen automaattisesti, eikä sitä varten tarvitse erikseen luoda sääntöä, kuten tilattomalla palomuurilla tarvitsisi. (Yeo, 2003). OSI-mallissa tilallinen palomuuri toimii tilattoman palomuurin tavoin kerroksilla kolme ja neljä, sekä erona tilattomaan palomuuriin, myös kerroksella viisi, eli istuntokerroksella.

Tilallinen palomuuri sisältää myös tilattomasta palomuurista tutun pääsylistan, jonka pohjalta saapuva liikenne käydään ensin lävitse. Paketin saapuessa palomuurille yhteys avataan, jos yhteys on sallittu ja jatkossa kaikki saapuvat paketit

päästetään lävitse, kunnes yhteys katkaistaan. Yhteyden katkaisun jälkeen paketteja ei enää päästetä läpi, ennen kuin uusi yhteys on avattu.

2.2 Seuraavan sukupolven palomuurit

Seuraavan sukupolven, eli järjestyksessään kolmannen teknologiasukupolven, palomuurien toimintaperiaate on yhdistelmä aikaisempien palomuurisukupolvien tekniikoita, kuten pakettisuodatukseen, osoitteenmuunnokseen (NAT) ja porttiosoitteen muunnokseen (PAT). Vanhojen tekniikoiden lisäksi kolmannen sukupolven palomuurit sisältävät uusia ominaisuuksia, kuten pakettien syvätarkistuksen ja tunkeutumisenestojärjestelmän.

OSI-mallissa seuraavan sukupolven palomuurit toimivat kerroksilla 4-7, eli kuljetus-, istunto-, esitystapa- sekä sovelluskerroksella. Web-pohjaisista haittaohjelmista sekä sovelluskerroksen että kohdennetuista hyökkäyksistä onkin tullut ongelma vanhemmille palomuurisukupolville, sillä ohjelmat kykenevät piilottamaan itsensä, esimerkiksi porttihyppelyn, SSL-salauksen tai epästandardin portin käytön avulla. Vanhempiinkin palomuureihin on kehitetty DPI-ominaisuuksia, mutta ne ovat epäkäytännöllisiä, koska kaikkia paketteja ei kuitenkaan kyetä tutkimaan tarkasti, jonka lisäksi ne vielä kuormittavat palomuuria.

Seuraavan sukupolven palomuurilla voidaan tarkoittaa joko sovelluspalomuuria tai laitepalomuuria. Seuraavan sukupolven palomuureista käytettyä lyhennettä NGFW yritykset voivat käyttää vapaasti, joten toiminnot ja ominaisuudet eri valmistajien välillä saattavat hieman vaihdella. Seuraavan sukupolven palomuurit ovat myös kehittyneet termin käyttöönoton alkuajoista jo jonkin verran. Pääsääntöisesti seuraavan sukupolven palomuurien tulisi kuitenkin pystyä tunnistamaan ohjelmat riippumatta käytettävästä protokollasta, portista, piiloutumistekniikasta tai SSL-salauksesta, tarjota laajaa reaaliaikaista suojaa sovelluskerroksella, tunnistaa käyttäjät ja käyttää tunnistetietoja palomuurisäännöissä sekä mahdollistaa eri ohjelmien hallinta sääntöjen avulla. (Miller, 2011).

Kolmannen sukupolven palomuureilla ohjelman tunnistus perustuu useaan eri tekijään. Tapoja voi olla esimerkiksi tunnistaa käytettävä protokolla ja purkaa sitten

datapaketit, tunnistaa protokolla ja tarkistaa sitten, että hyödyntääkö sovellus oikeaa protokollaa, vai onko se tunneloitu jonkin muun protokollan sisään. Muita tapoja ovat paketin tunnisteiden tutkiminen, joiden avulla voidaan tunnistaa käytetty tiedonsiirto, sekä heuristiikka, jonka avulla voidaan käyttää tiettyjen ohjelmien omat salaustavat. (Miller, 2011).

Kolmannen sukupolven palomuurit tarkastelevat myös liikennettä syvällisemmin kuin aikaisemmat palomuurit ja reaaliajassa. Jatkuvan skannauksen avulla tiedonsiirtonopeudesta saadaan kaikki irti, eikä viive pääse nousemaan liiaksi. Palomuurit pystyvät myös tutkimaan ja estämään liikennettä sen sisällön mukaan, muuri pystyy tutkimaan paketin sisällä olevia datavirtoja ja estämään esimerkiksi tiettyjen tietojen päätymisen ulkoverkkoon. (Miller, 2011)

3 PALOALTO PA-5060 PALOMUURIN OMINAISUUKSIA

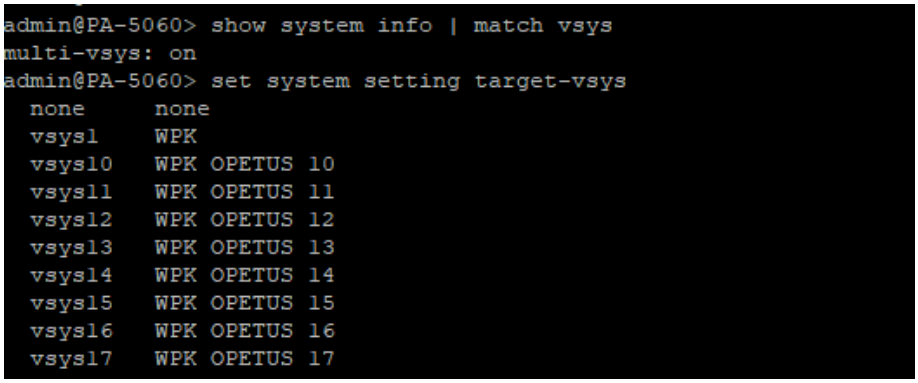
3.1 Perusominaisuudet

Palo Alto Networks on yhdysvaltalainen tietoturvayhtiö, jonka pääkonttori on Santa Clarassa, Kaliforniassa. Palo Alto valmistaa pääasiassa palomuureja sekä pilvipohjaisia tietoturvaratkaisuja. Palo Alton PA-5060 kuuluu ominaisuuksiensa puolesta kolmannen sukupolven huippumuureihin. Ominaisuuksiltaan palomuuri on omiaan suurien yritysten tai jopa datakeskusten tarpeisiin.

Yhtäaikaisia istuntoja palomuurilla voi olla neljä miljoonaa ja palomuuri pystyy käsittelemään 120 000 uutta yhteydenluontia sekunnissa. Sovellustunnistuksen ollessa päällä, PA-5060 kykenee jopa 20 Gb/s läpäisykyvyn. Tarkemmin palomuurin ominaisuudet ja tekniset tiedot on lueteltu liitteessä 1.

3.2 Hallinta

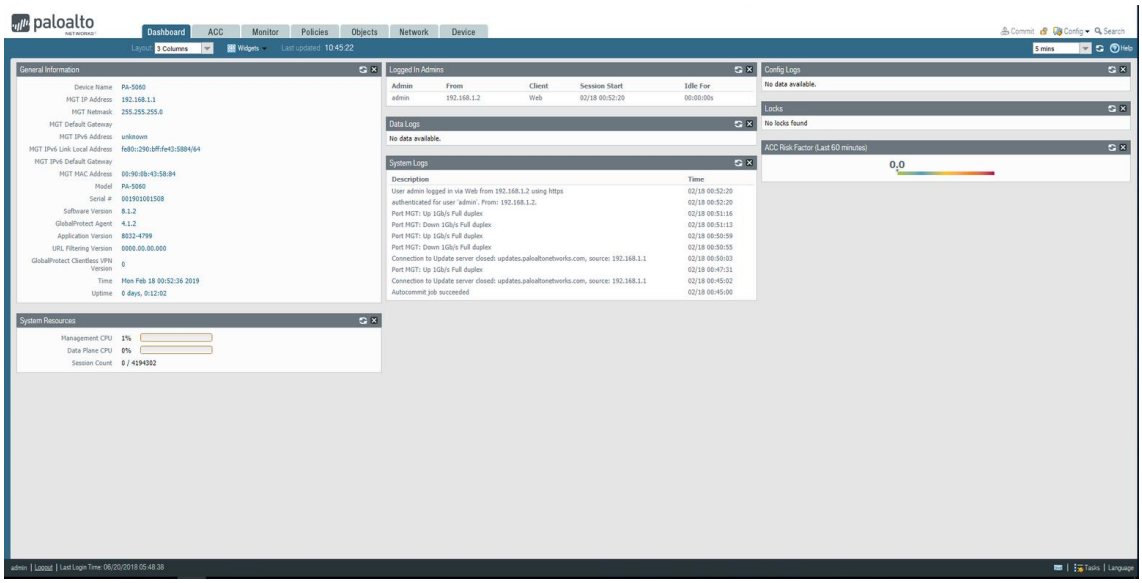
Palo Alton palomuurien hallintaan on kaksi eri vaihtoehtoa. Ensimmäinen vaihtoehto on komentorivi, eli CLI-hallintanäkymä. Yhteys muodostetaan joko SSH-yhteydellä tai sarjalinkillä. Komentorivillä on kaksi eri tilaa, joko toimintatila (operational mode) tai asetustila (configuration mode). Oletustilana on toimintatila, jossa voidaan tutkia palomuurin tilaa ja lokeja. Mikäli palomuurin asetuksiin halutaan tehdä muutoksia, pitää käyttää asetustilaa. Esimerkki komentorivinäkymästä on esitelty alla. Kuvassa on listattu työssä luotuja virtuaalipalomuureja.



KUVA 2 Komentorivikäyttöliittymä

Toinen vaihtoehto palomuurin hallintaan on web-hallinta. Käyttöliittymän ulkoasu on kuvattu alla kuvassa 3**.** Web-käyttöliittymän kautta voidaan tehdä käytännössä

kaikki tarvittavat asetukset. Web-käyttöliittymä on kätevä työkalu, varsinkin jos hallittavia palomuureja on vain muutamia. Muutoksien ajaminen laitteeseen tapahtuu web-käyttöliittymässä oikean yläkulman ”commit”-näppäimellä. Mikäli jokin määritys on virheellinen, kuten vaikkapa sama IP-osoite kahdessa eri portissa, eivät asetukset tallennu. Web-käyttöliittymä on ollut pääpiirteittäin samanlainen jo vuosia, riippuen käytettävästä lisenssistä, joten vanhatkin ohjeet pätevät melko hyvin.



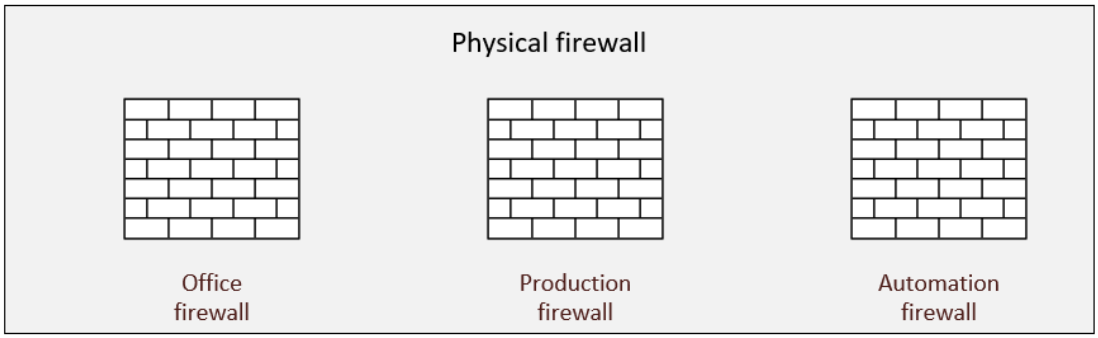
KUVA 3 Web-käyttöliittymä

Sekä web-käyttöliittymä, että terminaalipohjainen käyttöliittymä ovat hyviä tapoja hallita palomuureja, kun hallittavia kohteita on vähän. Laajemmille kokonaisuuksille Palo Alto tarjoaa Panorama hallintapalvelinohjelmistoa. Panorama on keskitetty hallintajärjestelmä uuden sukupolven palomuureille. Keskitetyn hallinnan kautta palomuurisäännöt ja –käytännöt voidaan implementoida useisiin laitteisiin samalla kertaa ja myös verkon valvonta helpottuu. (Palo Alto Networks, 2019).

3.3 Virtuaaliset palomuurit

Käytännön työn kannalta oleellinen ominaisuus Palo Alton palomuureissa on mahdollisuus luoda omia virtuaalisia palomuureja. Virtuaalisella palomuurilla tarkoitetaan fyysisen laitteen sisällä toimivia itsenäisiä loogisia palomuureja. Virtuaalisen palomuurin liikenne voidaan pitää erillään saman fyysisen palomuurin

muista virtuaalisista palomuureista. Kuvassa neljä on esitetty tilanne, jossa fyysiseen palomuurin on luotu erikseen virtuaaliset palomuurit toimisto-, tuotanto- sekä automaatioverkoille, joka voisi olla hyvinkin tyypillinen tilanne tehdasympäristössä. Virtuaalipalomuurin edut tulevat esille esimerkiksi tilanteessa, jossa kahden erillisen yksikön verkkoliikenne tarvitsee eriyttää toisistaan kokonaan, koska virtuaalipalomuurien avulla yksi fyysinen laite riittää.



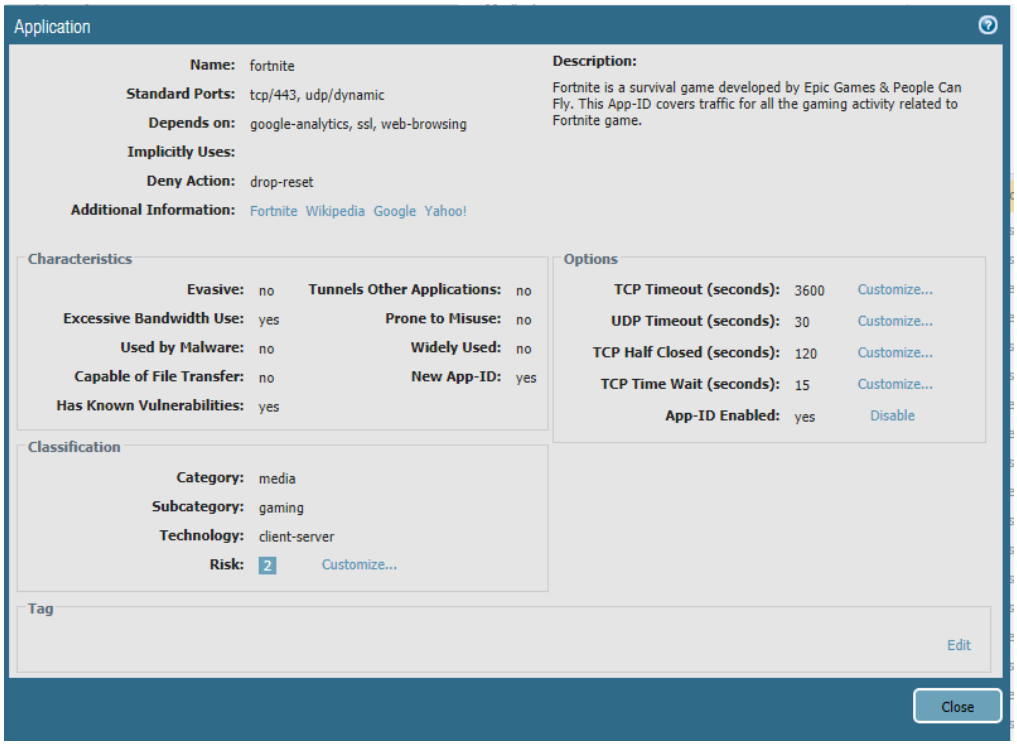
KUVA 4 Esimerkki virtuaalisista palomuureista

Virtuaalijärjestelmiä tukevat Palo Alton PA-3000, PA-5000 ja PA-7000 –sarjojen palomuurit. Tässä työssä käytetyllä PA-5060 palomuurilla voi luoda 25 virtuaalista yksikköä ilman lisenssiä ja lisenssillä määrää on nostettavissa 225 kappaleeseen.

3.4 Sovellussuodatus

Sovellussuodatus on yksi uusista ominaisuuksista, jotka tulivat mahdollisiksi uuden sukupolven palomuurien myötä. Aikaisemmilla laitteilla sovellustunnistukseen ei kyetty, koska tunnistus perustui porttitunnistukseen ja useat sovellukset käyttävät samaa porttia, kuten vaikkapa Skype ja selaimet hyödyntävät molemmat TCP-porttia 80 (Snyder, 2011).

Palo Alton laitteissa sovellustunnistus perustuu App-ID teknologiaan, jonka avulla voi nähdä eri sovellukset verkossa, oppia kuinka ne käyttäytyvät ja niiden ominaisuuksia. Sovelluksille pystyy tekemään myös erilaisia sääntöjä, kuten sallia vain tiettyjen tiedostotyyppien lähetys Slackissa, tai kuten kuvassa 5**,** estää jokin sovellus kokonaan. Tässä tapauksessa estetty sovellus oli nuorison suosiossa oleva Fortnite-peli.



KUVA 5 Sovellustunnus

3.5 Käyttäjätunnistus

Käyttäjätunnistusta ei tässä työssä otettu käyttöön, mutta se on mahdollista LDAP-hakemistojen avulla eli esimerkiksi Windowsin Active Directoryä hyödyntäen. Käyttäjätunnistuksen avulla käyttäjäprofiili saadaan yhdistettyä tiettyyn verkon IP-osoitteeseen.

Käyttäjätunnistus mahdollistaa entistä tarkempien palomuurisääntöjen luomisen tietyille käyttäjäryhmille, jolloin tietyille käyttäjille tai käyttäjäryhmille voidaan sallia palveluja, jotka ovat muille estettyjä, tai toisinpäin.

3.6 Tunkeilijan havaitsemis- ja estojärjestelmät

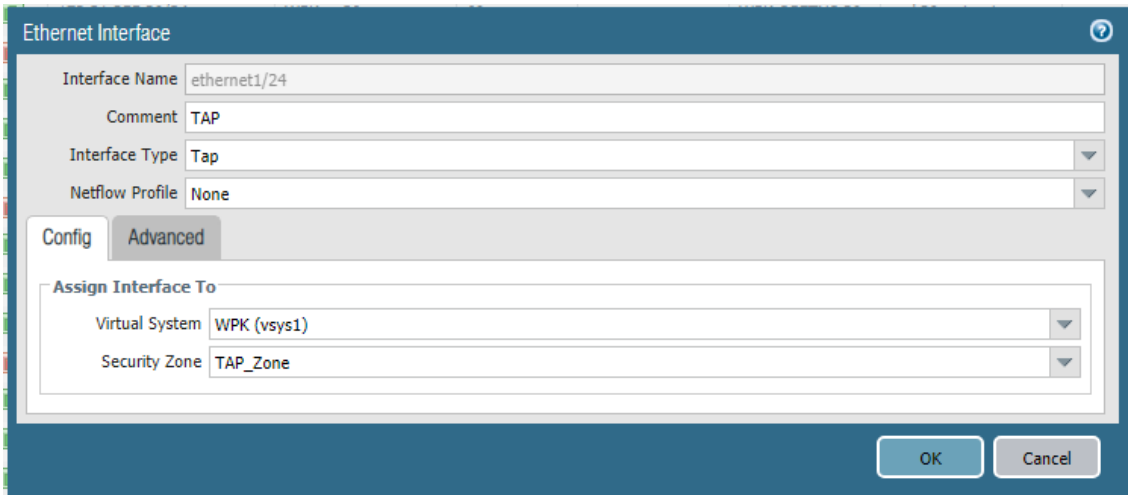
Tunkeutumisen havaitsemis- ja estojärjestelmät ovat molemmat tärkeitä palomuurin ominaisuuksia. Havaitsemisjärjestelmän toimintaperiaate on tarkkailla järjestelmää automaattisesti ja hälyttää, mikäli poikkeavaa käytöstä havaitaan, havaitsemisjärjestelmät ovat suunniteltu huomaamaan sekä ihmisten tekemät hyökkäykset, että haittaohjelmien ominaiskäytös verkossa.

Tunkeutumisen estojärjestelmällä on monia samoja ominaisuuksia kuin tunkeutumisen havaitsemisjärjestelmällä, mutta estojärjestelmä voi myös nimensä mukaisesti yrittää estää hyökkäyksen. Halutessaan hyökkäysien eston voi ottaa pois päältä, jolloin järjestelmä toimii havaitsemisjärjestelmän tavoin.

3.7 TAP-liikenteenkaappauspiste

TAP-liikenteenkaappauspisteen avulla voidaan valvoa ja analysoida verkon läpi kulkevaa liikennettä tietyn portin kautta. TAP-pisteestä palomuuri näkee kaiken portin kautta kulkevan liikenteen, mutta ei osallistu muuten liikenteeseen.

Palomuurilla TAP-pisteen konfigurointi tapahtuu Interfaces-välilehden kautta, halutun portin liitäntätyyppi asetetaan TAP-tilaan. Lisäksi liitännälle tulee määritellä oma verkkoalue. Alla kuvassa on esimerkki TAP-portin määrityksestä.



KUVA 6 TAP-pisteen määritys

3.8 DNS Sinkhole

DNS Sinkhole on tekniikka, jota käytetään estämään DNS-palvelinta ratkaisemaan tiettyjen URL-osoitteiden isäntänimiä. Tekniikka perustuu siihen, että DNS-palvelin palauttaa saastuneeksi tiedetylle osoitteelle väärän IP-osoitteen. (Infosec, 2018).

Palo Alton muurit tukevat sinkhole-tekniikkaa. Kaikki kyselyt, jotka tulevat osoitteista, jotka kuuluvat Palo Alto Networks DNS signatures-listaan, ohjataan Palo

Alton sinkhole-palvelimelle. Login avulla voidaan seurata tälle sinkhole-palvelimelle ohjattuja kyselyitä (Palo Alto Networks, 2019).

4 TOIMEKSIANNON ESITTELY JA SUUNNITTELU

4.1 Työn tarkoitus

Käytännön työssä tarkoitus oli selvittää palomuurin ominaisuuksia ja luoda niitä hyväksikäyttäen laboratorioympäristö kyberturvallisuuden opetus- ja tutkimuskäyttöön. Työssä luodaan lisäksi tarvittavat palomuuriasetukset TAMKin WPK-, Kyber- ja Titenet-verkon suojaukseen. Lisäksi palomuurin ominaisuuksia pyritään hyödyntämään mahdollisuuksien mukaan. Suunnitelma on esitetty kaaviona liitteessä 2.

Opetuskäyttöä varten luodaan yhteensä 15 itsenäistä loogista palomuuria. Jokaiseen loogiseen palomuurin tulee kolme aliverkkoa ja hallinnointiliittymä.

4.2 Suunnittelu

Koska opetuskäyttöön tarvittiin yhteensä 15 toisistaan erillä olevaa virtuaalista palomuuria ja jokaiseen palomuurin tuli vielä kolme aliverkkoa, todettiin, että työ vaatii yhteensä 45 erilaista virtuaalista aliverkkoa. Jokaiselle palomuurille piti luoda luotettu verkkoalue, epäluotettu sekä demilitarisoitu alue.

Virtuaaliset lähiverkot nimettiin siten, että luotetut verkot saivat numerot 10-25, demilitarisoitu alue 30-45 ja epäluotettu alue numerot 50-65. IP-osoitteet jaettiin alla taulukossa 1 olevan esimerkin mukaisesti. Sisäverkolle luotiin DHCP-palvelin ja muille verkoille laitettiin kiinteä verkko-osoite.

Taulukko 1 WPK-opetus 10 virtuaalipalomuurin virtuaaliverkot

Luotettu / Trusted	Osoiteavaruus 192.168.10.0/24
DMZ	192.168.100.10
Epäluotettu / Untrusted	172.31.255.10

5 KÄYTTÖÖNOTTO JA KONFIGUROINTI

5.1 Alkuvalmistelut

Oletusasetuksilla ensimmäinen kirjautuminen palomuurin hallintapaneeliin tapahtui palomuurin hallintaportin kautta. Oletuksena palomuurin IP-osoite on 192.168.1.1/24, kirjautumiseen vaaditut admin-tunnukset löytyivät laitteen ohjeista. Kirjautumiseen käytetyn koneen IP-osoite tulee asettaa käsin samaan aliverkkoon palomuurin kanssa, jotta kirjautuminen onnistui.

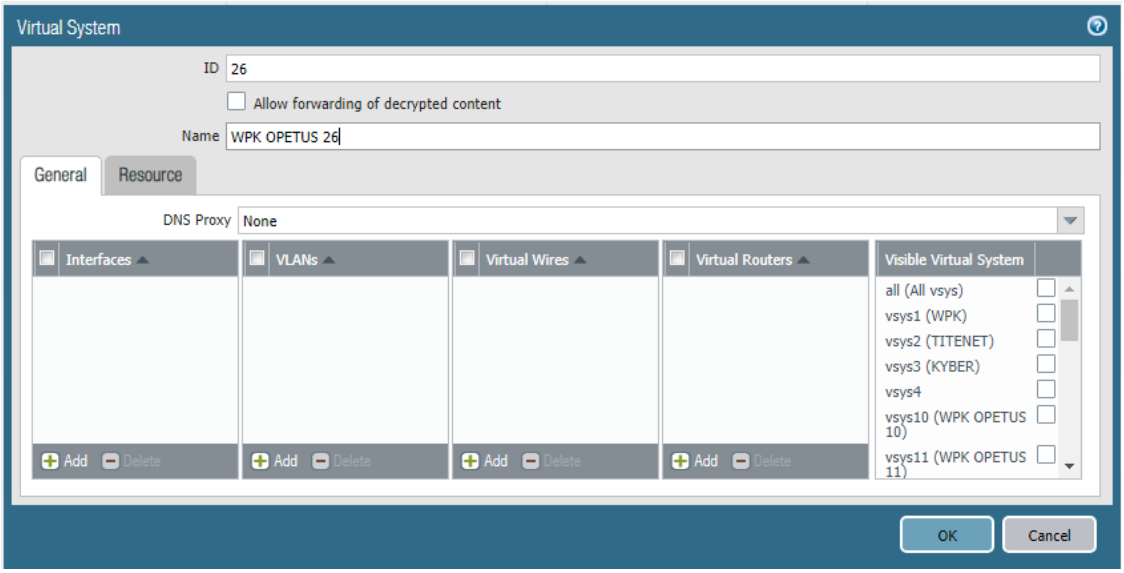
Ensimmäiseksi järkevintä on vaihtaa admin-tunnuksen salasana johonkin muuhun oletusvaihtoehdosta jo ihan tietoturvankin kannalta. Salasanan muuttaminen onnistuu kuvassa 3 näkyvästä ”Device” –valikosta.

Admin-tunnuksen vaihtamisen jälkeen seuraavaksi ladattiin päivitykset palomuurin käyttöjärjestelmään. Palo Alton palomuurit hyödyntävät omaa Palo Alto Networksin kehittämää PAN-OS –käyttöjärjestelmää. PA-5060 -palomuurille tuorein käyttöjärjestelmä on versio 8.1, jota tässä työssä myös käytettiin. Versio 8.1 jää myös tämän palomuurin viimeiseksi käyttöjärjestelmäversioksi (Palo Alto Networks, 2019).

5.2 Virtuaalipalomuurin luominen

Ennen kuin virtuaalipalomuureja pääsee luomaan, tulee ominaisuus ottaa käyttöön. Mahdollisuuden luoda virtuaalipalomuureja saa käyttöön ”Device” –välilehden ”Setup” –valikon ”Management” –kohdasta klikkaamalla rastin ruutuun kohdassa ”Multi Virtual System Capability”.

Itse virtuaalipalomuurien luonti tapahtuu samalta ”Device” –välilehdeltä kohdasta ”Virtual systems”. Virtuaalipalomuuri tarvitsee itselleen luontivaiheessa tunnuksen, joka voi olla mikä tahansa luku väliltä 1-255 sekä nimen. Tässä kohtaa jätettiin vielä muut kohdat tyhjiksi. Halutessaan tässä kohtaa pääsisi ”Resource” –valikon takaa määrittelemään sääntöjä juuri luodulle palomuurille. Esimerkkikuvassa luodaan virtuaalipalomuuria WPK-verkon opetuskäyttöön.



KUVA 7 Virtuaalipalomuurin luominen

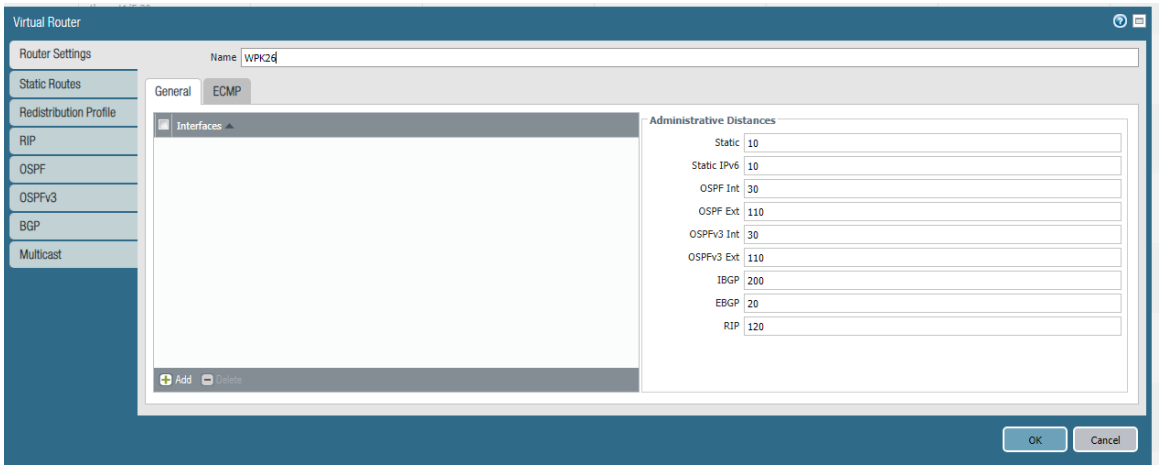
5.3 Virtuaalireititin

Virtuaalireititin on palomuurin toiminto, joka osallistuu kolmannen verkkokerroksen reititykseen. Palomuuri käyttää virtuaalireititintä hankkiakseen reitit muihin aliverkkoihin joko manuaalisesti määritettyjä staattisia reittejä tai dynaamisia reittejä hyödyntäen.

Kaikille niille aliverkoille, joiden halutaan olevan yhteydessä toisiinsa, tulee määrittää yhteinen virtuaalireititin. Yksi rajapinta voi kuulua vain yhteen virtuaaliseen reitittimeen, mutta reititysprotokollia ja staattisia reittejä voi yhdellä reitittimellä olla käytössä useampia. Kolmannen verkkokerroksen reitityksessä virtuaalireititin tukee dynaamisista protokollista BGP-, OSPF-, OSPFv3- ja RIP-protokollia. (Palo Alto, 2019).

Oletuksena palomuurissa on valmiiksi luotu virtuaalireititin nimeltään ”default”. Tähän työhön luodaan kuitenkin 15 erillistä virtuaaliympäristöä, joten oletusreititintä ei voida käyttää, vaan reitittimet pitää luoda.

Reitittimet luodaan ”Network” –välilehden ”Virtual Routers” –alavalikosta. Alla olevassa kuvassa luodaan uutta virtuaalireititintä. Työssä ei määritelty erikseen reitityksiä.



KUVA 8 Virtuaalireitittimen luominen

Virtuaalireitittimille luodaan yksi staattinen reitti. Reitin luominen tapahtuu kuvassa 7 esitetyn näkymän ”Static Routes” -valikosta. Reitti luodaan siten, että kaikki liikenne ohjataan oletusyhdyskäytävälle, eli lähdeosoitteeksi asetetaan 0.0.0.0/0, joka kattaa kaikki verkon osoitteet ja Next Hop -osoitteeksi oletusyhdyskäytävän IP-osoite.

5.4 Verkkoalueet

Verkkoalueet ovat looginen kokonaisuus, joka koostuu yhdestä tai useammasta liitynnästä. Tähän työhön verkkoalueita luotiin kolme yhtä virtuaalipalomuuria kohden. Palomuureille luotiin luotettu sisäverkko, demilitarisoitu DMZ-alue sekä epäluotettu ulkoverkko.

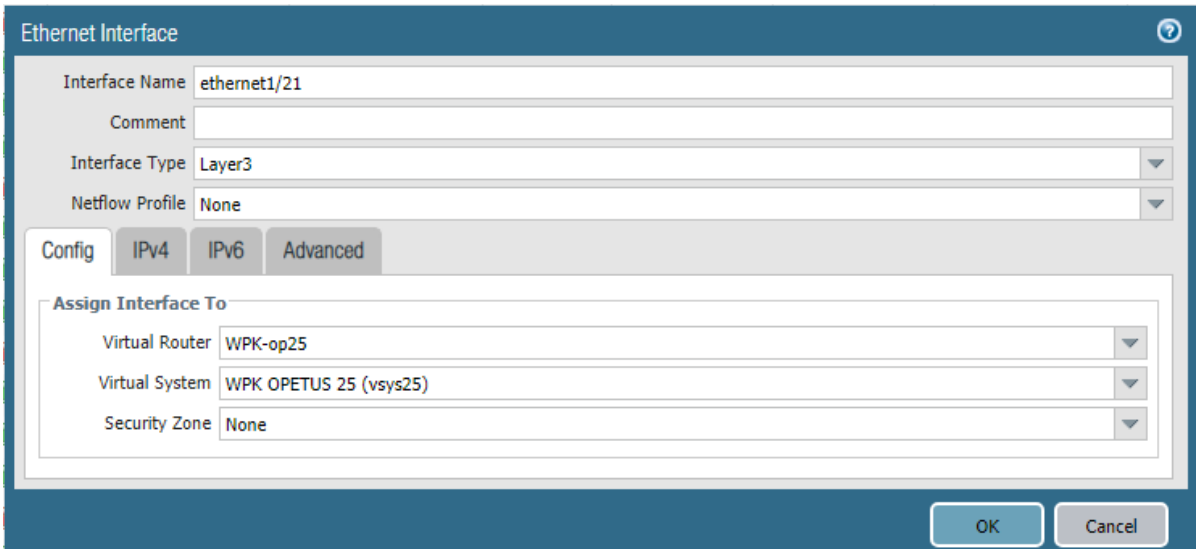
Verkkoalueet luotiin Network-välilehden Zones-valikosta. Luontivaiheessa uudelle verkkoalueelle määritettiin nimi, tyyppi ja liitynnät, joissa tätä aluetta hyödynnettiin.

5.5 Verkkoliitännät

Palo Alto PA-5060 -palomuurin liityntöjen konfigurointi tapahtuu Network -välilehden Interfaces -valikosta. Valikosta voidaan konfiguroida liitynnän tyyppi.

PA-5060-palomuuri liitynnät voidaan konfiguroida joko Layer2 tai Layer3-liitynnöiksi, Virtual Wire -liitynnäksi, HA-liitynnäksi tai TAP-liitynnäksi. Määritykset eroavat hienoisesti toisistaan sen mukaan, minkä liitännän valitsee.

Tässä työssä verkkoliitynnät WPK-verkolle luotiin Layer3-liityntöinä. Layer3 eroaa Layer2-liitynnästä siten, että Layer3 kykenee reitittämään liikennettä useiden porttien välillä, jonka takia se myös valittiin tähän työhön. Alla kuvassa 9 on esitelty liitynnän luominen. Liitynnälle määritettiin reititin, virtuaalijärjestelmä sekä verkkoalue.



KUVA 9 Verkkoliitynnän luominen

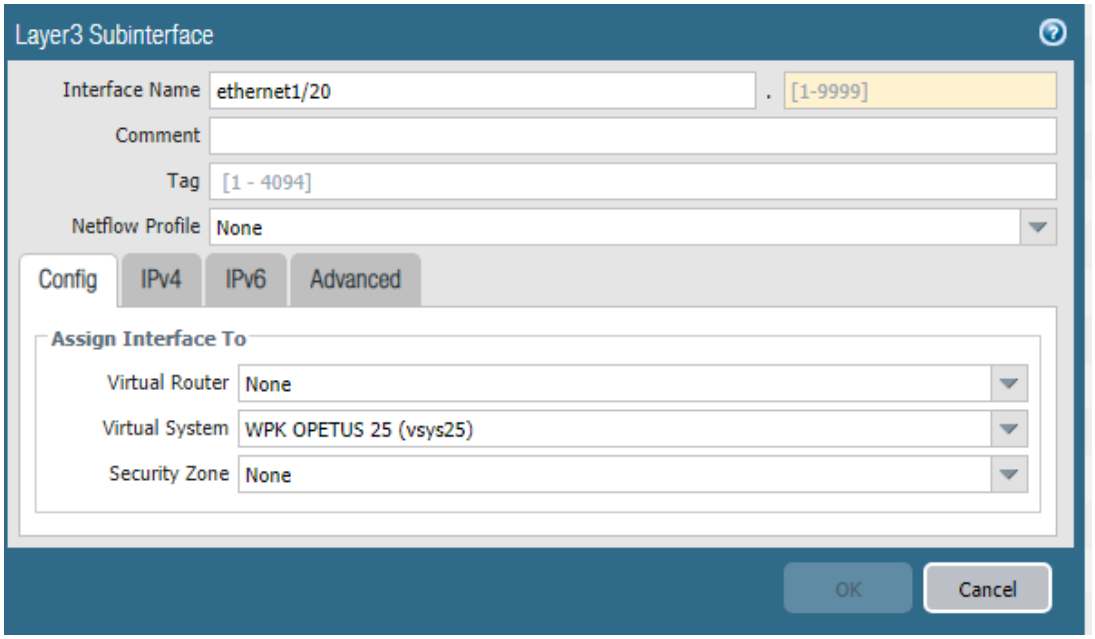
Lisäksi palomuurin luotiin kahden portin välille toisen kerroksen liitynnät. Tämän ratkaisun pohjalta laite voidaan kytkeä minkä tahansa kahden verkkolaitteen väliin ja liikenne kulkee laitteen läpi, muttei vaikuta siihen mitenkään.

5.5.1 Alirajapinnat

Koska jokainen virtuaalipalomuuri määritettiin omaan verkkoliitäntäänsä, tuli liitäntöihin määrittää kaikki palomuurin tarvitsemat verkot, eli trusted, untrusted ja DMZ. Näin yhteen liitäntään saadaan luotua looginen kokonaisuus.

Alirajapinnan luominen tapahtui samasta Interfaces-välilehdestä. ”Add Subinterface” –napista avautuu kuvan 10 –mukainen valikko. Jokainen uusi liityntä vaatii itselleen oman yksilöllisen ID:n. Lisäksi uudelle liitynnälle tulee määrittää reititin,

järjestelmä sekä verkkoalue. Lisäksi liitynnälle tuli määrittää IP-osoite, tässä kohtaa käytettiin taulukossa 1. esitettyjä määritteitä.



KUVA 10 Alirajapinnan määritys

5.6 NAT

NAT-tekniikalla tarkoitetaan osoitteenmuunnosta, jolla saman sisäverkon koneet voivat käyttää yhtä julkista IP-osoitetta. Tekniikan avulla IP-osoitteita voidaan säästää, kun sisäverkon koneille ei tarvita julkisia osoitteita. Samalla sisäverkon laite saadaan piilotettua.

Työssä NAT-asetukset täytyi määrittää siten, että trusted-alueesta saatiin yhteys untrusted-alueeseen. Määritys tapahtui käyttöliittymän Policies-välilehden NAT-valikosta.

5.7 Säännöt

Virtuaalipalomuuria luodessa luodaan automaattisesti kaksi sääntöä jokaista uutta palomuuria kohden. Luodut säännöt ovat intrazone-default ja interzone-default. Nämä säännöt määrittelevät alueiden sisäistä ja ulkoista liikennettä. Näitä valmiita sääntöjä ei juurikaan pysty itse muokkaamaan, ainoat hyväksytyt muokkauskohteet ovat liikenne, suojausprofiilit ja lokiasetukset.

Oletussäännöt suoritetaan aina viimeisenä, eli vain, jos mikään muu sääntö ei päde. Muita sääntöjä ei tässä kohtaa luotu ollenkaan, vaan muurit jätettiin odottamaan opetuskäytön alkua.

6 POHDINTA

Opinnäytetyö vaati paljon uuden opettelemista, vaikka Palo Alton tuoteperhe olikin jo entuudestaan hieman tuttua töiden kautta, mutta lähinnä liikenteen seurannan ja muun valvonnan osalta. Uusia palomuureja en ollut päässyt itse pystyttämään. Omat haasteensa toi myös käytännössä täysin uusi verkkoympäristö, jonka selvittely vei hetken aikaa, ennen kuin työtä pääsi tekemään täydellä vauhdilla.

Alkuhaasteiden ja muutaman erehdyksen ja oppimisen jälkeen työ lähti sujumaan hyvin. Palo Alton laitteisiin löytyy erittäin hyvä manuaali, jossa käydään perusteellisesti kaikki eri asetukset lävitse. Lisäksi löysin muutaman videon, joissa käytiin itseäni arveluttaneet asiat selkeästi lävitse.

Työ osoittautui erittäin opettavaiseksi, työtä tehdessä tuli opittua paljon uusia asioita ja samalla kerrattua sellaisia, jotka olivat jo osin päässeet unohtumaan. Työstä opittuja asioita voin varmasti hyödyntää tulevaisuudessa työelämässä, mikäli tarvetta on.

Jatkokehityksenä työhön voisi ottaa käyttäjätunnistuksen käyttöön. Nyt siihen ei ajanpuutteen vuosi ollut mahdollisuutta. Lisäksi Palo Alton muitakin ominaisuuksia voisi hyvin implementoida olemassa olevaan ympäristöön.

LÄHTEET

Infosec. 2018. Understanding DNS Sinkholes – A weapon against malware. Tulostettu 8.4.2019. https://resources.infosecinstitute.com/dns-sinkhole/#gref

Krimaka.net. 2019. OSI ja TCP/IP-malli. Tulostettu 8.4.2019. http://www.krimaka.net/tietotekniikka/verkko-ja-ethernet/osi-ja-tcp-ip-mallit.html

Miller, Lawrence C. 2011. Next-Generation Firewalls for Dummies.

Newman David. 2011. Palo Alto PA-5060 is one fast firewall. Network World. Tulostettu 26.2.2019. https://www.networkworld.com/article/2179971/network-security/palo-alto-pa-5060-is-one-fast-firewall.html

Palo Alto Networks. 2019. App-ID. Tulostettu 1.3.2019. https://www.paloaltonetworks.com/technologies/app-id

Palo Alto Networks. 2019. DNS Sinkholing. Tulostettu 8.4.2019. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/dns-sinkholing.html

Palo Alto Networks. 2019. Hardware End-of-Life Dates. Tulostettu 28.2.2019. https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates.html

Palo Alto Networks. 2019. Panorama Datasheet. Tulostettu 28.2.2019. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/panorama-centralized-management-datasheet

Palo Alto Networks. 2019. Virtual Routers. Tulostettu 4.3.2019. https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers

Rouse, Margaret. 2013. Network TAP. Tulostettu 1.3.2019. https://searchnetworking.techtarget.com/definition/Network-tap

Rouse, Margaret. 2018. Next-generation firewall (NGFW). Tulostettu 28.2.2019. https://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW

Snyder, Joel. 2011. Palo Alto earns short list status. Tulostettu 1.3.2019. https://www.networkworld.com/article/2179973/palo-alto-earns-short-list-status.html

Yeo, Lisa. 2003. Choosing a Personal Firewall. Tulostettu 25.3.2019. http://www.informit.com/articles/article.aspx?p=31945&seqNum=3

LIITTEET

Liite 1. Palo Alto PA5060 tekniset tiedot

PALO ALTO NETWORKS: **PA-5000 Series Specsheet**

PA-5000 Series

Key PA-5000 Series next-generation firewall features:

CLASSIFY ALL APPLICATIONS, ON ALL PORTS, ALL THE TIME WITH APP-ID™.

- Identify the application, regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Use the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, apply traffic shaping.
- Categorize unidentified applications for policy control, threat forensics, custom App-ID creation, or packet capture for further investigation.

EXTEND SAFE APPLICATION ENABLEMENT POLICIES TO ANY USER, AT ANY LOCATION, WITH USER-ID™ AND GLOBALPROTECT™.

- Agentless integration with Active Directory, LDAP, eDirectory Citrix and Microsoft Terminal Services.
- Integrate with NAC, wireless, and other non-standard user repositories with an XML API.
- Deploy consistent policies to users running Microsoft Windows, Mac OS X, Linux, Android or iOS platforms, regardless of location.

PROTECT AGAINST ALL THREATS—BOTH KNOWN AND UNKNOWN—WITH CONTENT-ID™ AND WILDFIRE™.

- Block a range of known threats including exploits, malware, and spyware—across all ports, regardless of common threat evasion tactics employed.
- Limit unauthorized transfer of files and sensitive data, and control non-work-related web surfing.
- Identify unknown malware, analyze for more than 100 malicious behaviors, automatically create and deliver protection in the next available update.

paloalto NETWORKS
the network security company™


PA-5060


PA-5050


PA-5020

The Palo Alto Networks™ PA-5000 Series is comprised of three high performance models, the PA-5060, the PA-5050 and the PA-5020, all of which are targeted at high speed datacenter and Internet gateway deployments.

The PA-5000 Series delivers up to 20 Gbps of throughput using dedicated processing and memory for the key functional areas of networking, security, threat prevention and management. To ensure that management access is always available, irrespective of the traffic load, the data and control planes are physically separated. The controlling element of the PA-5000 Series is PAN-OS™, a security-specific operating system that allows organizations to safely enable applications using App-ID, User-ID, Content-ID, GlobalProtect and, WildFire.

PERFORMANCE AND CAPACITIES[1]	PA-5060	PA-5050	PA-5020
Firewall throughput (App-ID enabled)	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps
Max sessions	4,000,000	2,000,000	1,000,000
New sessions per second	120,000	120,000	120,000
IPSec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
GlobalProtect (SSL VPN) concurrent users	20,000	10,000	5,000
SSL decrypt sessions	90,000	45,000	15,000
SSL inbound certificates	1,000	300	100
Virtual routers	225	125	20
Virtual systems (base/max[2])	25/225*	25/125*	10/20*
Security zones	900	500	80
Max. number of policies	40,000	20,000	10,000

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 5.0.
[2] Adding virtual systems to the base quantity requires a separately purchased license.

For a complete description of the PA-5000 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

HARDWARE SPECIFICATIONS

I/O

- PA-5060, PA-5050: (12) 10/100/1000, (8) Gigabit SFP, (4) 10 Gigabit SFP+
- PA-5020: (12)10/100/1000, (8) Gigabit SFP

MANAGEMENT I/O

- (2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console port

STORAGE OPTIONS

- Single or dual solid state disk drives

STORAGE CAPACITY

- 120GB, 240GB SSD, RAID 1

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- PA-5060: Redundant 450W AC (330W/415W)
- PA-5050, PA-5020: Redundant 450W AC (270W/340W)

MAX BTU/HR

- PA-5060: 1,416
- PA-5050, PA-5020: 1,160

INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz); -40 to -72 VDC

MAX CURRENT CONSUMPTION

- 8A@100VAC, 14A@48VDC

MAX INRUSH CURRENT

- 80A@230VAC; 40A@120VAC; 40A@48VDC

MEAN TIME BETWEEN FAILURE (MTBF)

- 6.5 Years

RACK MOUNTABLE (DIMENSIONS)

- 2U, 19" standard rack (3.5"H x 20"D x 17.5"W)

WEIGHT (STAND ALONE DEVICE/AS SHIPPED)

- 41lbs/55lbs

SAFETY

- UL, CUL, CB

EMI

- FCC Class A, CE Class A, VCCI Class A

CERTIFICATIONS

- NEBS Level 3, FIPS level 2, ICSA

ENVIRONMENT

- Operating temperature: 32° to 122° F, 0° to 50° C
- Non-operating temperature: -4° to 158° F, -20° to 70° C

NETWORKING

INTERFACE MODES

- L2, L3, Tap, Virtual wire (transparent mode)

ROUTING

- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 64,000/64,000
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Jumbo frames: 9,210 bytes max frame size
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

HIGH AVAILABILITY

- Modes: Active/Active, Active/Passive
- Failure detection: Path monitoring, Interface monitoring

ADDRESS ASSIGNMENT

- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

IPV6

- L2, L3, tap, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 4,096 (PA-5060, PA-5050), 2,048 (PA-5020)
- Aggregate interfaces (802.3ad)

NAT/PAT

- Max NAT rules: 8,000 (PA-5060), 4,000 (PA-5050), 1,000 (PA-5020)
- Max NAT rules (DIPP): 450 (PA-5060), 250 (PA-5050), 200 (PA-5020)
- Dynamic IP and port pool: 254
- Dynamic IP pool: 32,000
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 8 (PA-5060, PA-5050), 4 (PA-5020)
- NAT64

VIRTUAL WIRE

- Max virtual wires: 2,048 (PA-5060, PA-5050), 1,024 (PA-5020)
- Interface types mapped to virtual wires: physical and subinterfaces

L2 FORWARDING

- ARP table size/device: 32,000 (PA-5060, PA-5050), 20,000 (PA-5020)
- MAC table size/device: 32,000 (PA-5060, PA-5050), 20,000 (PA-5020)
- IPv6 neighbor table size: 5,000 (PA-5060, PA-5050), 2,000 (PA-5020)

SECURITY

FIREWALL

- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

WILDFIRE

- Identify and analyze targeted and unknown files for more than 100 malicious behaviors
- Generate and automatically deliver protection for newly discovered malware via signature updates
- Signature update delivery in less than 1 hour, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

FILE AND DATA FILTERING

- File transfer: Bi-directional control over more than 60 unique file types
- Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN
- Drive-by download protection

USER INTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

URL FILTERING (SUBSCRIPTION REQUIRED)

- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking
- Physical interfaces supported for QoS: 12

SSL VPN/REMOTE ACCESS (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama)
- Multi-language user interface
- Syslog, Netflow v9 and SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter and export traffic, threat, WildFire, URL, and data filtering logs
- Fully customizable reporting

For a complete description of the PA-5000 Series next-generation firewall feature set, please visit www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054
Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

Liite 2. Käytännön työn topologiat