Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2020

Jari Vienola

NGFW-PALOMUURIEN SÄÄNTÖKANTOJEN OMINAISUUDET JA YLLÄPITO

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2020 | 44 sivua

Jari Vienola

NGFW-PALOMUURIEN SÄÄNTÖKANTOJEN OMINAISUUDET JA YLLÄPITO

Yritykset hyödyntävät päivittäisessä toiminnassaan yhä enemmän tietoverkkoja ja internet-pohjaisten palveluiden käyttöä, minkä vuoksi on tärkeää, että yritykset suojaavat sisäiset resurssinsa ulkoisilta uhilta. Tämän takia yritysten on panostettava vahvan tietoturvan ylläpitoon ja uuden sukupolven palomuurit toimivat tämän suojauksen perustana.

Opinnäytetyössä perehdytään kolmen eri palomuurivalmistajan seuraavan sukupolven palomuurilaitteisiin ja esitellään laitteiden toimintaa erityisesti sääntökantojen ylläpidon näkökulmasta. Sääntökannat ovat palomuureille rakennettavia palomuurisääntöjen joukkoja, joiden avulla määritetään minkä tyyppinen liikenne sallitaan kulkevan palomuurin läpi. Lisäksi työssä esitellään yleisellä tasolla palomuurien toimintaperiaatteet ja käydään läpi palomuurien historiaa.

Opinnäytetyön tavoitteena oli esitellä tärkeimmät palomuurien sääntökantojen ylläpitoon liittyvät tehtävät ja tuoda esiin kyseisissä tehtävissä ilmaantuvia eroavaisuuksia eri laitevalmistajien laitteiden välillä.

Työhön valikoitui kolme palomuurivalmistajaa, jotka ovat Check Point Software Technologies, Forcepoint ja Palo Alto Networks. Palomuurien hallintaan liittyvät toimenpiteet toteutettiin ensisijaisesti graafisen käyttöliittymän avulla työn havainnollisuuden parantamiseksi.

Opinnäytetyön tuloksena saatiin sääntökantojen hallintaan painottuva vertailu kolmen eri palomuurivalmistajan palomuurilaitteista esimerkkien avulla esitettynä. Opinnäytetyössä tuotettua vertailua voidaan hyödyntää palomuurilaitteiden hallintaan tutustumisessa ja yrityksen tarpeisiin sopivan palomuurilaitteen valinnassa.

ASIASANAT:

ylläpito, internet, palomuuri, tietoturva, tietoverkot

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Infromation and Communications Technology

2020 | 44 pages

Jari Vienola

ADMINISTRATION AND PROPERTIES OF RULE BASES ON NGFW FIREWALLS

As companies rely more and more on the use of networks and internet-based technologies in their daily operations, it has become increasingly important to secure internal resources from external threats. This requires companies to maintain strong network security with modern firewalls working as the foundation of this security.

This bachelor's thesis introduces the next-generation firewalls produced by three different firewall manufacturers and presents the operation of the devices, focusing especially on the perspective of maintaining rule bases. Rule bases are sets of firewall rules that are built on firewalls to determine which type of traffic can traverse through the firewall. Additionally, this work explains the main principles of firewalls in general and reviews the history of firewalls.

The aim of the thesis was to introduce the most important tasks related to the administration of firewall rule bases and highlight any differences present in these operations between different manufacturers devices.

The three different firewall manufacturers that were selected for this thesis were Palo Alto Networks, Check Point Software Technologies and Forcepoint. The administration of the firewalls was presented primarily through a graphical user interface to improve the illustration of the work.

As a result of the thesis, a comparison on basic firewall administration on the different manufacturers devices was provided with the help of examples taken from real production environments. The comparison provided in this thesis can be used by IT administrators to gain basic knowledge about next-generation firewalls and help companies choose a suitable firewall product to be used in their environment.

KEYWORDS:

administration, internet, firewall, information security, networking

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

ACL	Access-control List. Pääsylista, jonka avulla voidaan suodattaa tietoliikenteen kulkua tietoverkojen välillä.
AD	Active Directory. Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu.
CLI	Command-line Interface. Komentorivi.
FQDN	Fully Qualified Domain Name. Kokonainen verkkotunnus, joka sisätää kaikki verkkotunnuksen osat.
GUI	Graphical User Interface. Graafinen käyttöliittymä, esimerkiksi palomuurien hallintaa varten.
IP	Internet Protocol. Yksi TCP/IP protokollapinon protokollista, joka vastaa siitä että tietoliikennepaketit pääsevät kulkemaan tietoverkoissa ja löytävät perille päätepisteeseensä.
IPS	Intrusion Prevention System. Tunkeilijan havaitsemisjärjestelmä joka pyrkii havaitsemaan ja estämään tietoverkkoon kohdistuvat hyökkäysyritykset.
ICMP	Internet Control Message Protocol. Protokolla, jonka avulla verkkolaitteet voivat lähettää viestejä toisilleen.
NAT	Network Address Translation. Tietoverkoissa käytössä oleva osoitteenmuunnostekniikka, joka mahdollistaa useiden yksityisten IP-osoitteiden kääntämisen julkiseksi IP-osoitteeksi.
NGFW	Next-Generation Firewall. Uuden sukupolven palomuuri, jossa on huomattavasti perinteistä palomuuria enemmän toiminnallisuuksia.
OSI-malli	Open Systems Interconnection Reference Model. Tietoliikennejärjestelmien suunnittelussa ja kuvaamisessa käytetty viitemalli.
PAN-OS	Palo Alto Networksin palomuureissa käytössä oleva käyttöjärjestelmä.
TCP	Transmission Control Protocol. Päätelaitteiden välisen luotettavan tiedonsiirron mahdollistava protokolla.
TCP/IP	Protokollapino, jossa yhdistyy useita internet-liikennöinnissä käytettäviä tietoliikenneprotokollia.
UDP	User Datagram Protocol. Tietoliikenneprotokolla, joka mahdollistaa yhteydettömän tiedonsiirron laitteiden välillä.
URL	Uniform Resource Locator. Viittaus resurssin sijaintiin verkossa, yleiskielellä verkko-osoite.

VPN	Virtual Private Network. Tapa yhdistää paikallisia verkkoja julkisen internetin ylitse turvallisesti.

1 JOHDANTO

Yritykset hyödyntävät päivittäisessä toiminnassaan yhä enemmän tietoverkkojen yli tapahtuvaa tietoliikennettä. Tietoliikenteen käytön kasvaessa myös yrityksen tietoturvasta huolehtiminen nousee yhä suurempaan rooliin. Myös julkisten pilvipalveluiden käyttö on kasvanut valtavasti, esimerkiksi AWS (Amazon Web Services), Google Cloud ja Microsoft Azure ovat yhä useampien yritysten käytössä ja tämä osaltaan lisää tarvetta vahvan suojauksen ylläpitämiselle kaikenkokoisissa yrityksissä. Vahvaa palomuureilla toteutettua suojausta voidaankin pitää yritysten tietoturvan perustana.

Palomuurien avulla yritykset voivat hallita sisäverkosta ulospäin ja ulkoverkosta sisäverkkoon kulkevaa liikennettä, ja estää epätoivotusta lähteestä tai epätoivottuun kohteeseen kulkeva liikenne. Tässä toiminnassa tärkeimmässä roolissa ovat palomuureille tehtävät palomuurisäännöt, joiden avulla määritellään sallittu ja ei-sallittu tietoliikenne yrityksen tietoverkoissa. Palomuurisäännöt kootaan sääntökantoihin, joiden ylläpito on yleensä yrityksen IT -osaston vastuulla. Palomuurivalmistajat kehittävät palomuurejaan jatkuvasti ja myös sääntökantojen hallinta pyritään tekemään mahdollisimman yksinkertaiseksi ja tehokkaaksi erilaisten toiminnallisuuksien ja ominaisuuksien avulla. Palomuurit tarjoavat nykyisin kehityksensä myötä myös paljon muita toiminnallisuuksia kuin pelkästään tietoliikenteen suodatusta ja tarkkailua, mutta näihin toiminnallisuuksiin ei tässä opinnäytetyössä oteta juurikaan kantaa.

Opinnäytetyössä esitellään lyhyesti palomuurien historiaa ja käydään läpi palomuurien toimintaperiaatteet. Tämän lisäksi työssä käsitellään uuden sukupolven palomuurilaitteiden (NGFW) sääntökantoja ja niiden ominaisuuksia. Työn tarkoituksena on vertailla kolmen eri laitevalmistajan palomuureja ja perehdyttää lukija palomuurien sääntökantoihin, niiden toimintaan ja ylläpitoon liittyviin ominaisuuksiin. Työhön valittiin kolme eri valmistajaa, jotka ovat Palo Alto Networks, Checkpoint Software Technologies ja Forcepoint. Opinnäytetyössä keskitytään käsittelemään vain palomuurien sääntökantoja, eikä palomuurien muita toiminnallisuuksia käydä työssä juurikaan läpi. Tästä syystä työtä ei sellaisenaan voida käyttää valittujen valmistajien palomuurien kokonaisvaltaiseen vertailuun, mutta työn tuloksia voidaan kuitenkin käyttää apuna yritykselle sopivan palomuurilaitteen valinnassa sekä sääntökantojen ominaisuuksien ja toiminnallisuuksien vertailussa.

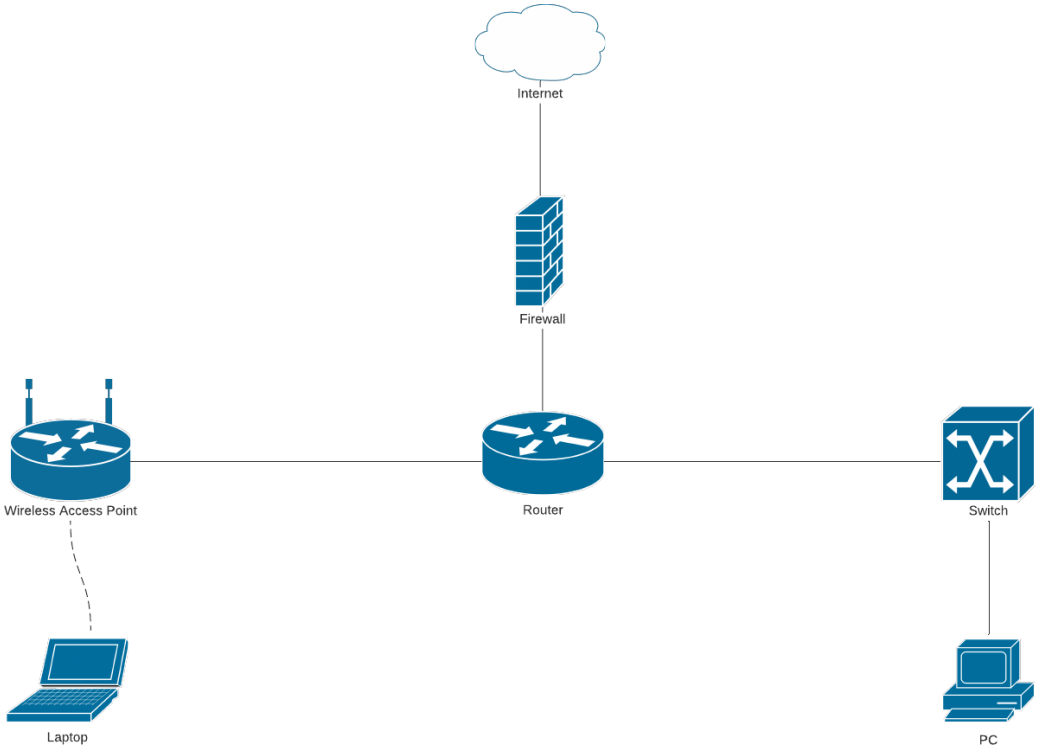
Opinnäytetyön luvussa 2 esitellään palomuurien historiaa ja kerrotaan palomuurien kehityksestä. Luvussa 3 esitellään työhön valikoituneet tuotevalmistajat ja niiden historia lyhyesti. Luvussa 4 keskitytään erikseen jokaisen valmistajan NGFW palomuurilaitteiden sääntökantojen ylläpitoon ja ominaisuuksiin. Luvussa 5 kootaan yhteenveto eri valmistajien palomuureista ja analysoidaan opinnäytetyön tuloksia.

2 PALOMUURIEN HISTORIAA

Tässä luvussa esitellään palomuurin toimintaperiaate yleisesti. Lisäksi käsitellään palomuurien historiaa ja esitellään eroavaisuuksia ensimmäisten käytössä olleiden palomuurien ja nykyisten uuden sukupolven palomuurilaitteiden välillä.

2.1 Palomuurin toimintaperiaate

Palomuurin pääasiallinen toimintaperiaate on lyhyesti ilmaistuna hyvin yksinkertainen: tarkkailla ja hallita tietoliikenteen kulkua tietoverkkojen välillä. Tietoverkkojen välillä kulkeva tietoliikenne ohjataan kulkemaan palomuurin lävitse, kuten kuvassa 1 on esitetty, jolloin palomuuri voi tarkastaa liikenteen sisällön ja suojata näin sisäverkkoa ulkoapäin tulevilta hyökkäyksiltä ja uhilta. (Oppliger 1997.)

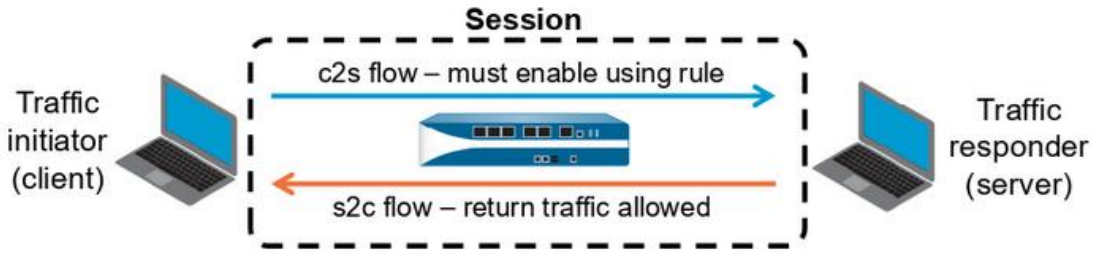


Kuva 1. Palomuurin sijanti tietoverkossa (Lucidchart 2020).

Yksityisen tietoverkon ja ulkoverkkoihin johtavan yhteyden väliin kytketty palomuuri kytketään usein kumpaankin päähän yhdellä liitännällä. Ulkoverkkoon tai internetiin

johtavaa kytkentää kutsutaan ulkoiseksi verkkoliitännäksi ja sisäverkkoon johtavaa kytkentää sisäiseksi verkkoliitännäksi. Muita käytettyjä nimityksiä ovat mm. suojaamaton verkkoliitäntä ja suojattu verkkoliitäntä, sekä luotettu verkkoliitäntä ja epäluotettu verkkoliitäntä. Palomuurin suojauksesta johtuen nimitystä ”suojaamaton verkkoliitäntä” voidaan pitää toisaalta harhaanjohtavana, sillä palomuurin suojauspolitiikka toimii usein molempiin suuntiin: sekä sisäverkosta ulospäin että ulkoverkosta sisäänpäin, eikä ulkoverkkoon johtavaa liitäntää voida näin ollen pitää täysin suojaamattomana. (Scarfone ja Hoffman 2009, 2-2.)

Palomuurit voidaan jakaa IP-pakettien käsittelytavan perusteella kahdentyyppisiin palomuureihin: tilattomiin palomuureihin ja tilallisiin palomuureihin. Tilattomat palomuurit tarkastelevat kaikkia palomuurin lävitse kulkevia IP-paketteja yksittäisinä, kun taas tilalliset palomuurit huomioivat myös aikaisemmat samojen kohteiden välillä kulkeneet paketit (Liu 2010). Kun tietoliikenne on päässyt hyväksytysti tilallisen palomuurin läpi, lisätään tieto aktiivisesta tietoliikenneyhteydestä muistiin, jolloin kyseisten päätepisteiden välillä kulkeva tietoliikenne pääsee kulkemaan vapaammin (kuva 2). Tilalliset palomuurit pystyvät siis valvomaan kokonaisia liikennevirtoja yksittäisten pakettien sijaan (Solarwinds MSP 2019). Tilalliset palomuurit tallentavat tiedon liikennevirroista erilliseen sessiotauluun, joka sisältää tiedon kaikista palomuurin läpi kulkevista aktiivisista tietoliikennesessioista. Kun tietoliikennesessio tulee päätökseensä ja yhteys suljetaan, poistuu tieto myös palomuurin sessiotaulusta. Palomuurin ylläpitäjällä on mahdollisuus tarkastella palomuurin sessiotaulua ja tarvittaessa sulkea aktiivisia sessioita.



Kuva 2. Havainnekuva aktiivisesta tietoliikennesessiosta (Palo Alto Networks 2020, M4-6).

Liikenteen suodattamista varten palomuureille rakennetaan sääntökanta, joka määrittää sen mitä liikennettä palomuurin lävitse sallitaan kulkevan, ja toisaalta minkä liikenteen palomuuri hylkää estäen täten liikenteen kulkemisen. Uudemmissa palomuurilaitteissa sääntökantaan voidaan lisätä mm. käyttäjätietokantoja (esim. Microsoft AD) ja applikaatioiden käyttöä hyödyntäviä palomuurisääntöjä, joiden avulla palomuurisäännöistä

saadaan tarkempia ja turvallisempia. Esimerkiksi Microsoft AD:n käyttäjätietokantaa hyödyntämällä voidaan luoda palomuurisääntöjä, joissa tietyt kohteet sallitaan vain tietyille käyttäjille. Mikäli markkinointiosastolla tarvitaan pääsy Facebookiin, voidaan markkinointiosastolla työskenteleville henkilöille sallia pääsy Facebookiin luomalla palomuurisääntö, joka sallii pääsyn vain sellaisille henkilöille, jotka ovat Microsoft AD:ssa liitettynä markkinointiosaston AD-ryhmään. Edellä mainitussa esimerkkitilanteessa voidaan myös hyödyntää sovellustunnistusta käyttämällä Facebookille räätälöityä applikaatioon pohjautuvaa palomuuriavausta. Tällöin on mahdollista sallia esimerkiksi pelkkä facebookin selaaminen, mutta estää facebookin sisäisten toimintojen, kuten Facebook-chatin tai Facebook-julkaisujen käyttö. Sovellustunnistuksen avulla palomuurisäännöistä saadaan entistä tarkempia ja tietoverkkojen turvallisuutta parannettua, sillä vain tarpeellisten ominaisuuksien ja toiminnallisuuksien käyttö voidaan sallia yrityksen tietoverkossa.

Ennen sääntökannan rakentamista on huomioitava muutamia asioita. Turvallista tietoverkkoympäristöä luodesssa on hyvä aloittaa rakentamalla palomuurille sääntökanta, joka estää kaiken liikennöinnin, tosin uudemmissa palomuureissa ulospäin suuntautuvan liikennöinnin estävä sääntö on käytössä jo valmiiksi. Näin voidaan varmistua siitä, ettei palomuurille jää ylimääräisiä ”aukkoja”, vaan ainoastaan haluttu ja tarpeellinen tietoliikenne voidaan sallia sääntökantaan lisättävien palomuurisääntöjen perusteella (Kuva 4). Sääntökannan rakentamista varten on selvitettävä ja tehtävä analyysi siitä, minkälaista tietoliikennettä yrityksen tietoverkossa kulkee ja miten palomuurin halutaan käsittelevän liikennettä. Palomuurisääntöjen tulisi sisältää vähintään seuraavat kohdat liikenteen suodattamista varten:

- IP-paketin lähdeosoite
- IP-paketin kohdeosoite
- liikenteen tyyppi (tietoliikenneprotokolla)
- portti
- toimenpide (paketin salliminen, hylkääminen tai pudottaminen).

Palomuuri vertaa liikenteestä kerättyjä tietoja sääntökannassa oleviin palomuurisääntöihin, aloittaen ensimmäisestä palomuurisäännöstä. Liikenne sallitaan tai estetään ensimmäisen sellaisen palomuurisäännön mukaisesti, joka täsmää kyseessä olevan liikenteen tietoihin. Tästä syystä palomuuripolitiikan viimeisen säännön tulisi aina olla sellainen, joka estää kaiken liikenteen, jottei mitään ylimääräistä liikennettä päästetä kulkemaan palomuurin läpi. (Scarfone & Hoffman 2-2, 2-3, 2-4.)

			Source				Destination						
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Addr...	Application	Service	Action	Profile	Options
1	Rule B	none	Trust	192.168.1.3	any	any	Untrust	any	dns ftp web-browsing	application-default		none	
2	Rule C	none	Trust	192.168.1.3	any	any	Untrust	any	any	any		none	
3	Rule A	none	Trust	any	any	any	Untrust	any	any	any		none	
4	Rule D	none	Untrust	any	any	any	any	any	any	any		none	

Kuva 3. Neljä erillistä palomuurisääntöä Palo Alto Networksin NGFW palomuurilla (Palo Alto Networks 2020).

2.2 Ensimmäiset palomuurit

Ennen varsinaisten erillisten palomuurilaitteiden yleistymistä, tietoverkoissa kulkevan liikenteen suodattamiseen käytettiin verkkolaitteille rakennettavia pakettisuodattimia. Pakettisuodatin asennettiin tietoverkossa usein reitittävälle laitteelle ja täten tietoverkkojen välillä kulkevaa liikennettä voitiin suodattaa. Esimerkkinä yksinkertaisesta pakettisuodattimesta voidaan käyttää tietoverkkoon asennettua reititintä, jolle on luotu pääsylista. Yksinkerataisimmillaan pääsylista kiinnittää huomiota vain pakettien lähde- ja kohdeosoitteisiin sekä käytettävään tietoliikenneprotokollaan ja porttitietoon. (Scarfone ja Hoffman 2009, 2-2,2-3.)

Pääsylistojen avulla voidaan suodattaa liikenteen kulkua sekä sisäverkosta ulospäin että ulkoverkosta sisäänpäin. Pääsylistoilla toteutettua suojausta voidaan kutsua myös tilattomaksi pakettisuodatukseksi, joka on toinen yleisistä palomuurin suodatustyypeistä. Pääsylistoilla luotua suojausta ei voida nykyisin pitää enää kovinkaan turvallisena, sillä ne eivät ota mitään kantaa verkossa kulkevien pakettien sisältöön (Scarfone ja Hoffman 2009, 2-2,2-3). Pääsylistat muodostavat kuitenkin perustan uudemmissa palomuureissa käytössä oleville sääntökannoille ja niiden sisältämille palomuurisäännöille.

2.3 Seuraavan sukupolven palomuurit

Lokakuussa 2009 Yhdysvaltalainen tutkimus- ja konsultointiyritys Gartner julkisti ”Defining the Next-Generation Firewall” -nimisen dokumentin, jossa listattiin minimivaatimukset uusille NGFW palomuureille. Gartnerin listauksen mukaan NGFW palomuureissa täytyy olla vähintään seuraavat toiminnallisuudet:

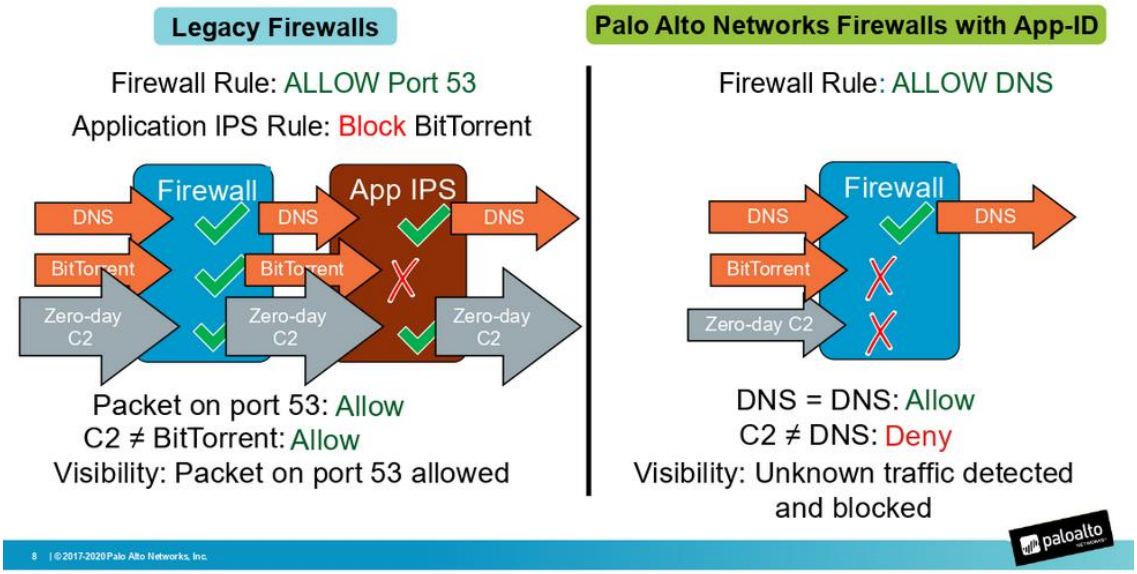
- Tuki yhdenmukaiselle bump-in-the-wire konfiguraatiolle ilman että verkkotoiminnoille aiheutuisi häiriöitä konfiguraation seurauksena.

- Toimia alustana tietoliikenteen tarkkailua ja tietoverkon turvallisuuspolitiikan toimeenpanoa varten.
- Standardinmukaiset ensimmäisen sukupolven palomuurien toiminnallisuudet, mm. pakettisuodatus, NAT toiminnallisuus, tilallinen protokollasuodatus ja kyky VPN-yhteyksien luomiseen
- Integroitu tunkeilijan havaitsemisjärjestelmä (IPS). Palomuuri on kykenevä reagoimaan hyökkäyksiin ja tietoturvauhkiin esimerkiksi ehdottamalla haitallista sisältöä levittävien verkkosivujen tai tietyistä IP-osoiteavaruuksista tulevan liikenteen suodattamista IPS:n tarjoaman datan perusteella.
- Kyky seurata ja tunnistaa sovellusten käyttöä ja mahdollistaa liikenteen suodattamista ja palomuuripolitiikan käyttöä applikaatioiden perusteella, ennemmin kuin pelkän protokollan, palvelun tai portin perusteella. Esimerkiksi palomuuri voi sallia Skype sovelluksen liikenteen, mutta estää tiedostojen jakamisen Skypen sisällä.
- Sisältää ”palomuurin ulkopuolista älyä”, eli mahdollisuus tuoda tietoa palomuurin ulkopuolisista lähteistä palomuurin sääntökannan optimointia ja parempaa liikenteen suodatusta varten. Esimerkiksi ulkoisten käyttäjätietokantojen käyttö liikenteen suodattamisessa.
- Tuki uusien tietolähteiden ja uusien tekniikoiden hyödyntämiseen tulevaisuuden uhkia varten.

Gartnerin ennusteen mukaan vuonna 2009 vain alle 1 % internetyhteyksistä suojattiin NGFW palomuurien avulla, mutta vuoden 2014 loppuun mennessä tämä luku nousisi aina 35 % asti. Lisäksi ennusteen mukaan vuonna 2014 hankituista palomuurilaitteista 60 % olisi sellaisia, jotka voitaisiin luokitella NGFW palomuureiksi (Pescatore & Young 2009).

Yhtenä NGFW-palomuurilaitteiden tärkeimmistä ominaisuuksista voidaan pitää kykyä suorittaa tarkkaa ja syvällistä analyysiä applikaatiotasolla (OSI-malli 7. kerros). NGFW-palomuureilla voidaan tehdä sääntökantaan palomuuriavauksia applikaatioiden perusteella, jolloin ei tarvitse käyttää pelkkää protokollaan ja porttiin pohjautuvaa avausta. NGFW palomuuri kykenee analysoimaan applikaatioiden liikennettä ja estämään sellaisten applikaatioiden liikenteen, joita ei ole erikseen sallittu applikaation perusteella tehdyllä palomuuriavauksella. Tällä tavoin voidaan välttyä myös haitallisten 0-päivä haavoittuvuuksien ja muun haitalliseksi luokitellun liikenteen pääsyn sallimiselta.

Esimerkiksi DNS-liikenteen tapauksessa perinteisellä palomuurilla voidaan tehdä palomuurisääntö, joka sallii DNS-liikenteen käyttämän TCP-protokollan portin 53 liikenteen. Tällöin palomuuri sallisi myös kaiken muunemmis sellaisen liikenteen, joka käyttää TCP-protokollaa ja porttia 53, samoin kuin oikea DNS-liikenne. Erillisellä ohjelmistopohjaisella IPS-suojauksella haitallista liikennettä voi päästä läpi, mikäli IPS ei tunnista liikennettä haitalliseksi. Tämä korostuu erityisesti 0-päivä haavoittuvuuksissa, kun IPS-järjestelmät eivät vielä tunnista haavoittuvuutta. NGFW-palomuureilla tehdyillä applikaatiopohjaisilla palomuuriavauksilla ei kuitenkaan sallita portin 53 TCP-liikennettä mikäli liikennettä ei tunnisteta oikeaksi DNS-liikenteeksi, jolloin myös haitallinen 0-päivä haavoittuvuutta hyödyntävä liikenne saadaan pysäytettyä ennen sen pääsyä yrityksen sisäverkkoon (Palo Alto Networks 2020, M5-8).



Kuva 4. Havainnekuva palomuuriavausten eroista (Palo Alto Networks 2020, M5-8).

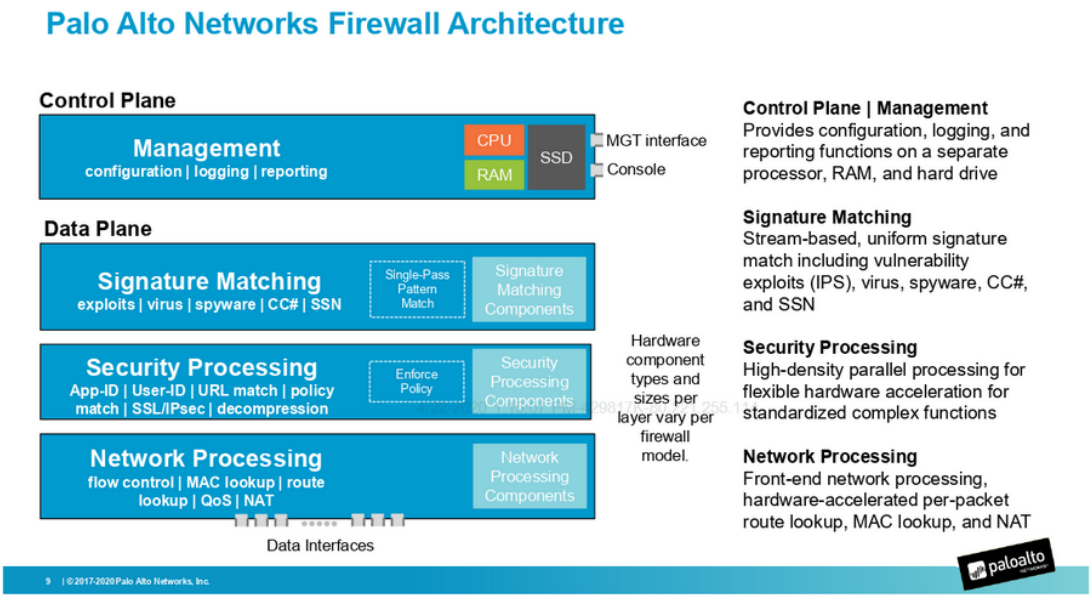
2.4 NGFW-palomuurien ominaisuuksien ja termien esittely

NGFW-palomuurien sääntökantojen ominaisuuksien ja ylläpidon esittelyä ja vertailua varten käydään läpi sellaiset yleiset ominaisuudet ja tekniikat, mitkä liittyvät olennaisesti NGFW-palomuurilaitteisiin ja ovat käytössä kaikissa työhön valikoiduissa palomuureissa. Sääntökantoihin liittyvät valmistajakohtaiset toiminnallisuudet ja ominaisuudet

esitellään erikseen myöhemmissä yksittäisten valmistajien laitteita käsittelevissä kappaleissa.

2.4.1 Control plane ja data plane -alustat

Palomuurin hallinta, liikenteen valvonta ja kyky käsitellä tietoliikennettä on normaalisti jaoteltu palomuurilla sisäisesti kahden eri alustan välille (kuva 5). Control planen avulla suoritetaan palomuurin hallintaan, lokitietojen keräämiseen ja reittitietojen päivitykseen liittyvät tehtävät. Data planen avulla suoritetaan palomuurin pääasiallisia tehtäviä, mm. liikenteen analysointia, liikenteen suodatusta palomuurisääntöjen perusteella ja antivirus- ja tunkeilijanestojärjestelmien käyttöä. Toimintojen segmentointi kahdelle erilliselle alustalle helpottaa resurssien keskittämistä ja lisää palomuurin vikasietoisuutta esimerkiksi palvelunestohyökkäyksiä vastaan. Järeämmillä palomuurilaitteilla voi olla data planella ja control planella allokoituna omat prosessorit ja keskusmuistit jotta resurssien riittävyydestä voidaan varmistua (Palo Alto Networks 2020; Forcepoint 2017).



Kuva 5. Palo Alto Networksin NGFW-palomuurin arkkitehtuuri (Palo Alto Networks 2020, M1-11).

2.4.2 Security zone -verkkoalue

Security zonet ovat palomuureille määriteltäviä verkkoalueita joiden avulla virtuaalisia ja fyysisiä verkkoliitäntöjä (interface) voidaan koota yhdeksi loogiseksi kokonaisuudeksi.

Security zoneen voidaan lisätä useampia verkkoliitäntöjä ja jokainen verkkoliitäntä tulee liittää johonkin security zoneen. Yksittäinen fyysinen tai virtuaalinen verkkoliitäntä voi kuulua vain yhteen security zoneen. NGFW palomuurit hyödyntävät security zoneja liikenteen suodattamisessa, sillä palomuurisäännöt käyttävät security zonen tietoja tarkastaessaan liikenteen lähde- ja kohdetietoja (Palo Alto Networks 2020; Check Point 2020; Forcepoint 2018).

2.4.3 Security policy -säännöstö

Security policyllä tarkoitetaan sitä kokonaisuutta, jonka perusteella palomuuri säätelee liikenteen kulkua tietoverkoissa. Tärkeimmässä roolissa on palomuurille rakennettu sääntökanta, jonka sääntöjä vasten palomuuri vertaa vastaanottamaansa liikennettä ja toteuttaa säännöstössä määrättyjä toimenpiteitä. Kaikki palomuurin data plane alustan läpi kulkeva liikenne tarkastetaan ja sallitaan tai estetään sääntökannan mukaisesti. Palomuuri aloittaa liikenteen tietojen vertailun ensimmäisestä palomuurisäännöstä ja lopettaa vertailun ensimmäisen täsmäävän säännön kohdalla suorittaen liikenteelle säännössä määritetyt toimenpiteet eli yleensä joko sallien tai estäen kyseisen liikenteen kulkemisen.

3 VALMISTAJIEN ESITTELY

Seuraavassa luvussa esitellään kolme opinnäytetyöhön valikoitunutta palomuurivalmistajaa: Palo Alto Networks, Checkpoint Software Technologies (jäljempänä Check Point) ja Forcepoint, ja käydään lyhyesti läpi kyseisten yritysten historiaa. Työhön valittujen palomuurivalmistajien valintaan vaikutti ennen kaikkea oma osaaminen ja mahdollisuus päästä työni yhteydessä käsittelemään kyseisten valmistajien palomuureja.

Palo Alto Networks, Check Point ja Forcepoint ovat kaikki vahvasti edustettuina yrityksille suunnattujen palomuurilaitteiden markkinoilla. Useat arvostetut ICT-alaa seuraavat julkaisut ovat listanneet kaikki työhön valitut valmistajat ja näiden palomuurilaitteet parhaimpien markkinoilla tarjolla olevien laitteiden joukkoon. Esimerkiksi ICT-alaan keskittyvän tutkimus- ja konsulttiyhtiö Gartnerin julkaiseman ”Magic Quadrant for Network Firewalls” -raportin mukaan (Kaur ym. 2019). Forcepoint, Check Point ja Palo Alto Networks sijoittuvat kaikki vuoden 2019 listauksessa kymmenen parhaimmaksi arvioidun palomuurivalmistajan joukkoon Palo Alto Networksin ollessa koko listauksen ensimmäisenä. (Kuva 4.)

Kuva 6. Gartnerin ”Magic Guadrant for Network Firewalls” -listaus 2019 (Kaur ym. 2019).

3.1 Palo Alto Networks

Palo Alto Networks perustettiin Maaliskuussa 2005 ja sen perustivat Nir Zuk, Rajiv Batra ja Yuming Mao. Nir Zuk työskenteli ennen Palo Alto Networksin perustamista Check Pointilla ja oli heidän mukanaan kehittämässä maailman ensimmäistä tilallista pakettisuodatusta hyödyntävää palomuuria. (Forbes 2020; Blacharski 2010.)

Palo Alto Networksin tilikauden 2019 liikevaihto oli 2,9 miljardia Yhdysvaltain dollaria. Asiakkaita Palo Alto Networksillä on oman ilmoituksensa mukaan 70 000 yli 150:ssä eri maassa. Palo Alto Networksin tuoteportfolio on jaettu kolmen erillisen tavaramerkin alle: Strata, Prisma ja Cortex. Strata käsittää fyysiset NGFW palomuurilaitemallistot ja niiden oheistuotteet, kuten lisenssit. Prisma tavaramerkin alle on keskitetty pilvipalveluiden ja pilvialustojen suojaukseen tarkoitetut tuotteet, esimerkiksi virtuaaliset VM-palomuurimallistot. Cortex-tavaramerkin alle kuuluvat Palo Alto Networksin keskitetyt tietoturvauhkien hallinta- ja valvontapalvelut, mm. Cortex XDR sovellusalusta. (Palo Alto Networks 2020.)

Palo Alto Networksin NGFW palomuurit ovat saatavilla sekä fyysisinä laitteina, että virtuaalialustoille asennettavina virtuaalisina palomuureina. Fyysisten palomuurilaitteiden tuoteperhe on nimetty PA-malliksi ja tällä hetkellä myynnissä olevat mallistot ovat PA-220, PA-220R, PA-800, PA-3200, PA-5200 ja PA-7000. Myynnistä jo poistuneita mallistoja ovat PA-200, PA-500, PA-2000, PA-3000, PA-4000 ja PA-5000. Virtuaalisten palomuurien tuoteperhe on nimetty VM-malliksi, jonka myytävät mallistot ovat VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000-HV. Palomuurilaitteiden keskitettyä hallintaa varten Palo Alto Networksin tuoteportfoliossa on Panorama niminen laite. Panorama on verkkoon asennettava erillinen fyysinen laite, jonka kautta palomuurien hallinnointi ja lokien seuranta onnistuu keskitetysti. Panoramasta saatavilla olevat mallit ovat M-200, M-500 ja M-600. Fyysiset NGFW palomuurimallistot, virtuaaliset NGFW palomuurimallistot ja Panorama käyttävät kaikki Palo Alto Networksin kehittämää PAN-OS käyttöjärjestelmää, jonka uusin julkaistu versio on PAN-OS 9.1. (Palo Alto Networks 2020.)

3.2 Check Point

Check Point, koko nimeltään Check Point Software Technologies, on monikansallinen tietoturvaratkaisuja ja laitteita toimittava yritys. Check Pointin perusti vuonna 1993

israelilainen insinööri Gil Shwed. Hän toimii yhä yhtiön toimitusjohtajana. Yhtiöllä on pääkonttorit Israelin Tel Avivissa ja San Carlosissa, Kalifornian osavaltiossa, Yhdysvalloissa. Check Point tuli tunnetuksi maailman ensimmäisestä tilallista pakettisuodatusta hyödyntävästä palomuuristaan, FireWall-1:stä, joka julkistettiin vuonna 1994. Nykyisin Check Point työllistää yli 5200 ihmistä maailmanlaajuisesti ja Check Pointin tuotteet suojaavat yli sadantuhannen yrityksen toimintaa ja yli miljoonaa käyttäjää tietoturvauhilta ympäri maailman. (Check Point Software Technologies 2020.)

Check Point uudisti palomuuritarjontaansa vuoden 2020 aikana ja uudet NGFW palomuurit kantavat nimeä Quantum Security Gateway. Check Point tarjoaa asiakkailleen erikokoisiin ympäristöihin tarkoitettuja mallistoja, jotka poikkeavat toisistaan lähinnä suorituskyvyn perusteella. Pienemmille sivutoimipisteille suunnatut mallistot ovat Quantum 3600 ja Quantum 3800. Pienille ja keskisuurille yrityksille tarkoitetut mallistot ovat Quantum 6200, Quantum 6400, Quantum 6600 ja Quantum 6700. Suuremmille yrityksille on tarjolla Quantum 7000 ja Quantum 16200 -mallistot, ja datakeskusten suojausta varten Quantum 26000 ja Quantum 28000 -mallistot. Kaikkien Check Point NGFW palomuurien käyttöjärjestelmä on Check Pointin oma Gaia järjestelmä, jonka uusin julkaistu versio on R80.40. (Check Point 2020.)

3.3 Forcepoint

Tammikuussa 2016 yhdysvaltalainen puolustusteollisuuden suuryritys Raytheon hankki omistukseensa Stonesoftin seuraavan sukupolven palomuurituotteet ja Sidewinderin proxy palomuurit teknologiayritys Inteliltä. Uudet omistukset integroitiin jo aikaisemmin Raytheonin hankkiman Websensen kanssa ja kokonaisuus uudelleenbrändättiin Forcepointiksi (Helmick 2016). Vaikka Forcepoint ei brändinä olekaan kovin vanha, on yritys toiminut eri nimillä kyberturvallisuuden ja tietoturvan parissa jo yli 20 vuotta. Nykyisin Forcepoint työllistää yli 2 700 ihmistä maailmanlaajuisesti ja sillä on yli 14 000 asiakasta 150 eri maassa. Forcepointin tunnetuimpiin asiakkaisiin lukeutuvat mm. IBM, Microsoft, Walmart ja Toyota. (Forcepoint 2020.)

Forcepointin NGFW palomuureja on saatavilla useissa eri mallistoissa. Yritysten pienemmille sivutoimipisteille tarkoitettuja NGFW malleja ovat N51, N51LTE, N110, N115, N330, N331, N335 ja N335W. Keskisuurille toimipisteille tai pienille datakeskuksille tarkoitettuja malleja ovat N1101 ja N1105. Suuremmille toimipisteille tarjonnasta löytyvät mallit N2101, N2105, N3301, N3305. Suurille toimipisteille ja kampusalueille

suunniteltuja malleja ovat N3401, N3405 ja N3410. Lisäksi todella suurille kampusalueille ja suurille datakeskuksille on tarjolla vielä oma mallinsa, Forcepoint N6205, joka on yhtiön tehokkain NGFW palomuurilaite. Forcepoint käyttää NGFW palomuuriensa käyttöjärjestelmänä erityistä ”kovennettua” versiota Linux ytimestä. Uusin NGFW palomuureille saatavilla oleva käyttöjärjestelmäversio on NGFW 6.7.2. (Forcepoint 2020.)

4 SÄÄNTÖKANTOJEN YLLÄPITO

Kappaleessa käsitellään Palo Alto Networksin, Check Pointin ja Forcepointin NGFW palomuurien sääntökantoja ja perehdytään sääntökantojen ylläpitoon ja ominaisuuksiin todellisten laiteympäristöistä hankittujen esimerkkien avulla. Palomuurilaitteiden hallinta suoritetaan käyttämällä graafista käyttöliittymää (GUI), sillä graafisen käyttöliittymän kautta palomuurin hallinta ja operointi on huomattavasti komentoriviltä tehtävää hallintaa selkeämpää ja havainnollistavampaa. Kaikkien työssä esiteltyjen palomuurilaitteiden hallinta onnistuu myös komentorivin (CLI) kautta. Palomuurien hallinnassa pyrittiin hyödyntämään myös keskitettyä hallintajärjestelmää, sillä keskitetty hallintajärjestelmä yksinkertaistaa usein palomuurien hallintaa ja mahdollistaa monia sellaisia ominaisuuksia ja toiminnallisuuksia joiden avulla palomuurien hallinnasta saadaan paljon tehokkaampaa.

4.1 Palo Alto Networks next-generation firewall

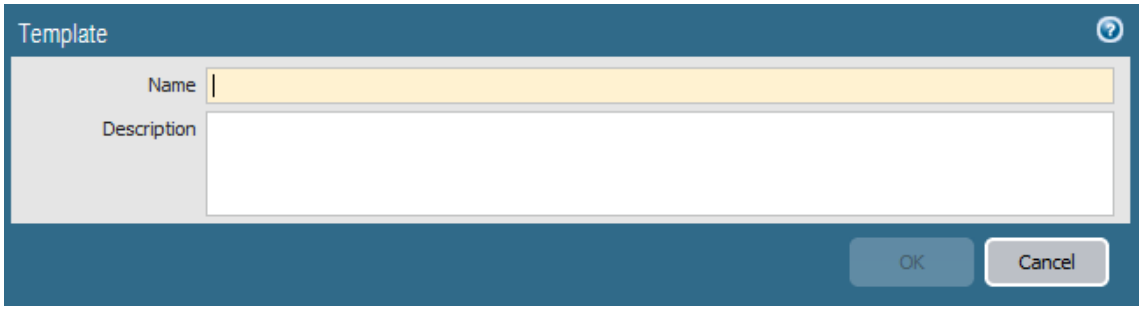
Palo Alton NGFW palomuurien hallinta esitetään työssä pääasiassa graafisen käyttöliittymän (GUI) kautta. Palomuureja voidaan hallita verkkoselaimella graafisen käyttöliittymän kautta suoraan palomuurille määritetyn management IP-osoitteen tai julkisen IP-osoitteen yli, mikäli hallintayhteys lähdeosoitteesta on sallittu. Lisäksi palomuurien hallintaan voidaan käyttää komentoriviä (CLI) tai keskitettyä hallintajärjestelmää. Palo Alton tapauksessa keskitetty hallintajärjestelmä Panorama käyttää samaa käyttöjärjestelmää kuin palomuuritkin, joten Panoraman GUI:n ulkoasu on samanlainen kuin yksittäisen palomuurin GUI:lla.

4.1.1 Panorama keskitetty hallintajärjestelmä

Palo Alto NGFW -palomuureja voidaan hallita Palo Alto Networksin keskitetyn hallintajärjestelmä Panoraman kautta. Panorama on erillinen yrityksen verkkoon asennettava laite, jonka avulla voidaan kerätä lokeja palomuureilta, analysoida liikennettä, sekä hallita palomuurien konfiguraatioita ja sääntökantoja keskitetysti. Panoraman kautta voidaan myös siirtyä suoraan yksittäisen Panoramaan yhdistetyn palomuurin omalle graafiselle käyttöliittymälle. Palomuurit liitetään Panoramaan sarjanumeron perusteella.

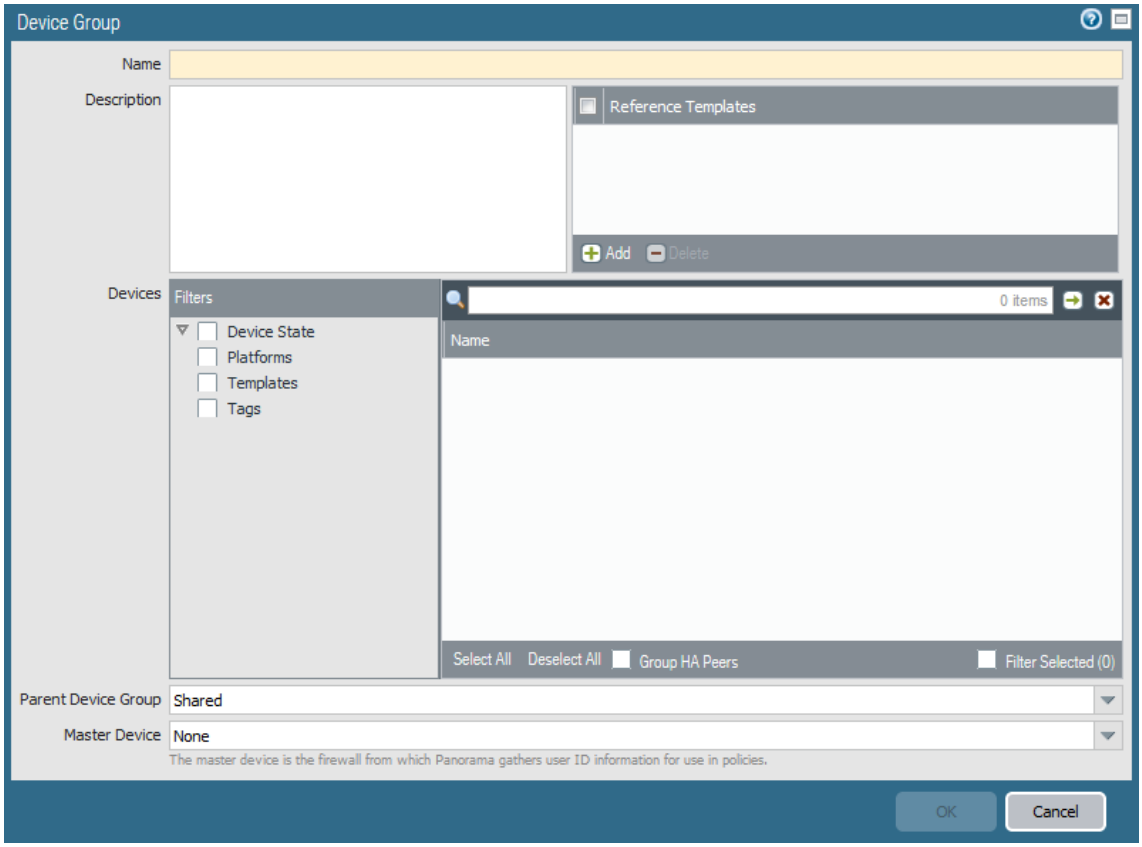
Liitettävälle palomuurille täytyy myös määrittää Panoraman IP-osoite ja muurin tulee pystyä kommunikoimaan Panoraman kanssa. Panoramalle asennetut lisenssit määrittävät sen kuinka monta palomuuria Panoraman keskitettyyn hallintaan voidaan liittää.

Panoraman avulla voidaan luoda konfiguraatio sapluunoita (template) ja sapluuna pinoja (template stack), joiden avulla haluttuja laite- ja verkkokonfiguraatioita voidaan tehdä samanaikaisesti useammille palomuureille (kuva 7). Templatet mahdollistavat useiden palomuurien hallinnan loogisena kokonaisuutena helpottaen suuren laitemäärän hallintaa. Useampia templateja voidaan yhdistää rakentamalla niistä pino, eli template stack ja yhdistämällä halutut templatet sekä palomuurit kyseisen template stackin alle. Template stackien avulla valmiita konfiguraatioita voidaan puskea Panoramasta suoraan laitteelle, jolloin konfiguraatio kirjoitetaan valittujen laitteiden aktiiviseen konfiguraatioon ja muutokset tulevat voimaan. Jotta konfiguraatiomuutokset voidaan tehdä templatejen avulla panoramasta, tulee palomuurin kuulua johonkin template stackiin. (Palo Alto 2020.)

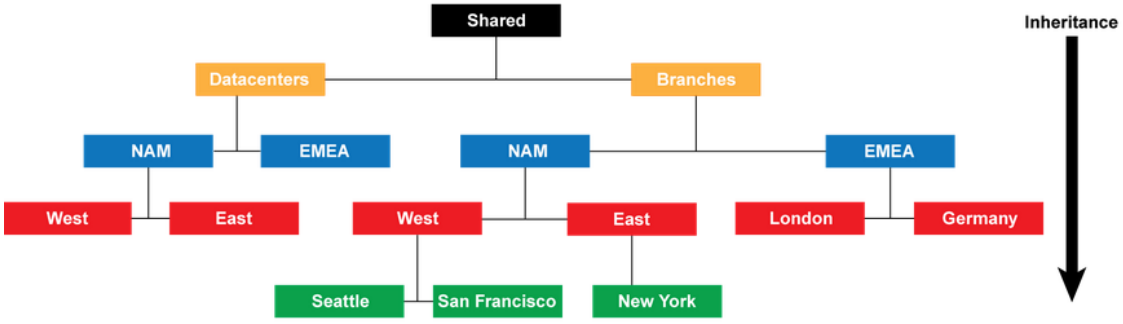


Kuva 7. Uuden templaten luonti Panoramassa

Panoramassa voidaan rakentaa myös laiteryhmiä (device group), joiden avulla voidaan hallita palomuureille tehtäviä palomuurisääntöjä ja niihin liittyviä objekteja (kuva 8). Laiteryhmiin voidaan liittää useita palomuureja ja laiteryhmät voidaan rakentaa puumaiseen muotoon hierarkisesti (kuva 9). Ylimmällä tasolla olevan laiteryhmän konfiguraatiot periytyvät kaikille alemman tason laiteryhmille ja niiden sisältämille laitteille, kun taas alemmilla tasoilla olevien laiteryhmien konfiguraatiot periytyvät vain oman ryhmänsä laitteille ja oman ryhmänsä alapuolella oleville laitteille. (Palo Alto Networks 2020.)



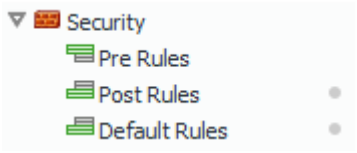
Kuva 8. Uuden device groupin luonti Panoramassa.



Kuva 9. Device groupien hierarkia (Palo Alto Networks 2020).

Device groupit helpottavat palomuurien sääntökantojen ylläpitoa mahdollistamalla keskitetyn sääntökantojen hallinnan useammille palomuureille kerralla. Device groupien avulla voidaan myös helpottaa uusien palomuurien käyttönottoa, sillä tarvittavat palomuurisäännöt voidaan tuoda laitteen konfiguraatioon device groupien avulla. Hierarkisen rakenteen ansiosta device groupien ylemmille tasoille voidaan luoda sääntöjä, jotka ovat käytössä kaikilla yrityksen toimipisteillä, kun taas alemmilla tasoilla voidaan luoda esimerkiksi toimistokohtaisia tai maanosakohtaisia palomuurisääntöjä.

Panoramassa palomuurien sääntökanta koostuu pre-rules-, post-rules- ja default-rules-osioista (kuva 10). Sääntökannan osioinnilla voidaan helpottaa ylläpitoa ja selkeyttää sääntökannan tarkastelua. Osiointi on mahdollista vain Panoramassa device groupeille tehydyillä sääntökannoilla.



Kuva 10. Sääntökannan osiointi

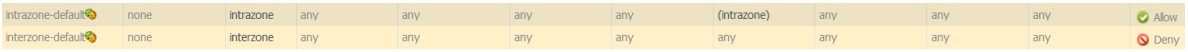
Sääntökantojen osiointi ja mahdollisuus luoda palomuurisääntöjä Panoraman kautta tai paikallisesti palomuurilla itsessään vaikuttaa luonnollisesti myös sääntöjen vertailujärjestykseen. Palomuurisääntöjen vertailujärjestys on esitetty kuvassa 11.

Kuva 11. Palomuurisääntöjen vertailujärjestys (Palo Alto Netoworks 2020).

4.1.2 Sääntökannan hallinta

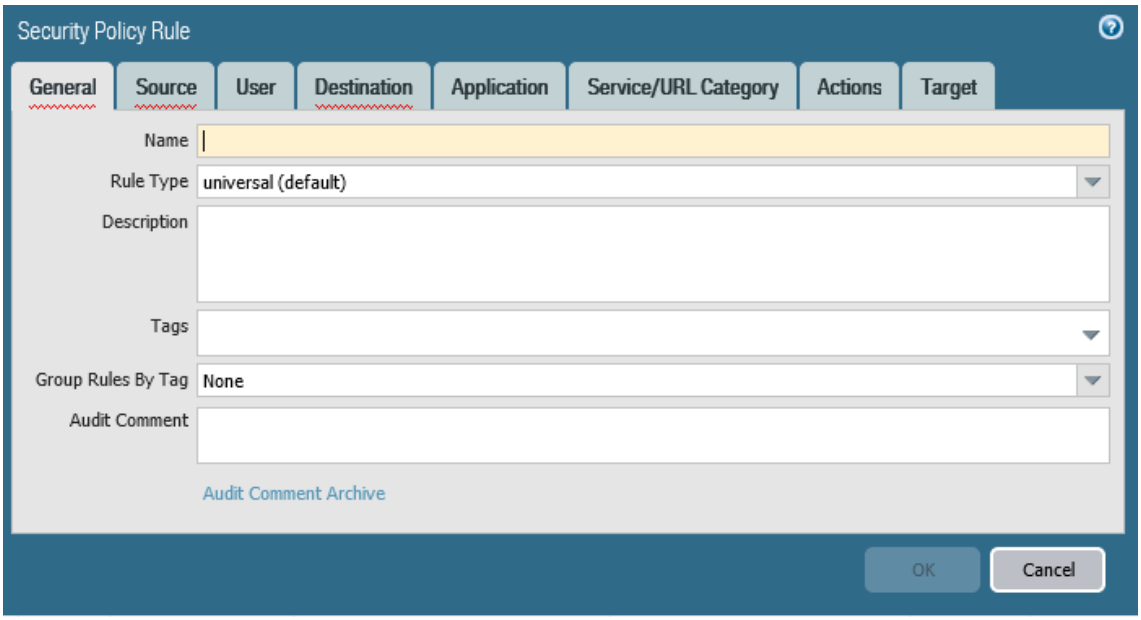
Palo Alto Networksin NGFW palomuureilla on aina valmiiksi lisättynä 2 erillistä sääntöä: intrazone-default ja interzone-default. Intrazone-default sallii oletuksena kaiken security zonejen sisäisen liikenteen, kun taas interzone-default estää kaiken liikenteen joka kulkisi security zonesta toiseen (kuva 12). Näitä sääntöjä kutsutaan ehdottomiksi palomuurisäännöiksi eikä palomuurin ylläpitäjä voi poistaa niitä. Ylläpitäjällä on kuitenkin mahdollisuus tehdä rajoitetusti muutoksia kyseisiin sääntöihin. Ehdottomat palomuurisäännöt on tehty tarkoituksellisesti niin kattaviksi, että kaikki sellainen liikenne, joka ei ole osunut vielä yhteenkään aikaisempaan palomuurisääntöön, tulee osumaan varmasti

jompaankumpaan näistä säännöistä. Tällä tavoin voidaan varmistaa ettei mitään liikennettä pääse kulkemaan palomuurin läpi ilman säännöstön mukaista liikenteen tarkastusta.



Kuva 12. Intrazone-default ja interzone-default säännöt.

Uuden palomuurisäännön lisääminen Palo Alto NGFW palomuureilla avaa hallintanäkymässä ikkunan, joka sisältää seuraavat välilehdet: General, Source, User, Destination, Application, Service/URL Category, Actions ja Target (kuva 13). Mikäli sääntö tehdään suoraan palomuurille, Target kenttä ei ole käytössä.



Kuva 13. Uuden palomuurisäännön lisääminen Palo Alto NGFW palomuurilla

Seuraavassa listauksessa käydään läpi kaikki palomuurisäännön määrityksessä käytettävissä olevat vaihtoehdot. Kuvassa 14 on kuvattu palomuurin käyttämät liikenteen suodatuskriteerit havainnollistavan esimerkin kautta.

- General
- Source
- User
- Destination
- Application

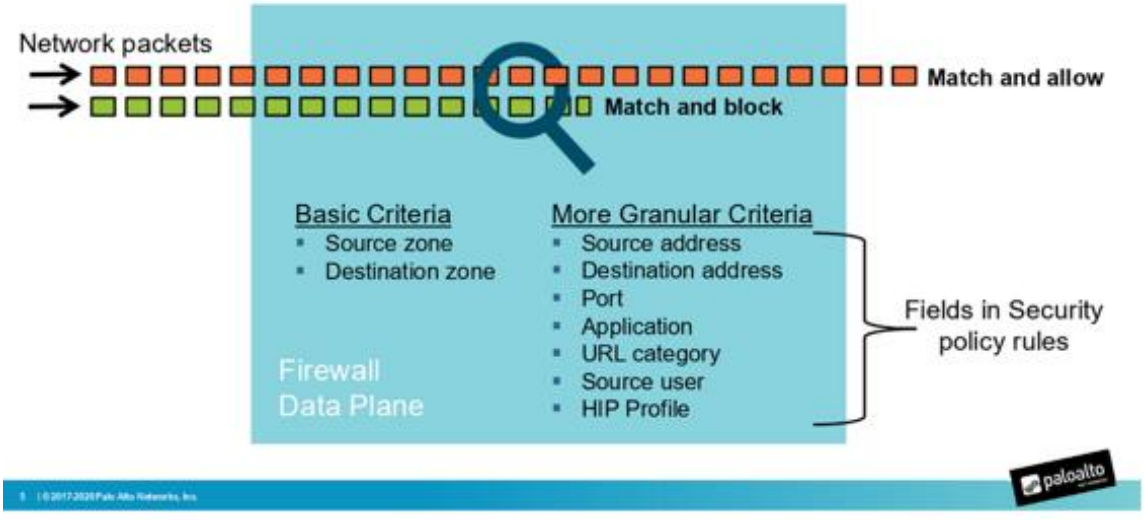
- Service/URL category
- Actions
- Target

General-välilehdellä määritetään säännölle yleiset tiedot. Nimi ja säännön tyyppi ovat ainoat pakolliset kentät. Säännön tyyppi tulee valita kolmesta valmiista vaihtoehdosta: universal(oletuksena käytössä), intrazone tai interzone. Intrazone tarkoittaa vain yhden alueen sisällä kulkevaa liikennettä, interzone yhdeltä alueelta toiselle ja universal näiden yhdistelmää (kuva 15). Lisäksi General-välilehdellä voidaan määrittää säännölle tagi, kuvaus ja kommentti sääntökannan ylläpitoa helpottamaan. Nämä eivät kuitenkaan ole pakollisia. Source-välilehdellä annetaan säännölle lähdetiedot, eli lähteenä käytettävä verkkoalue (source zone) ja lähdeosoite (source address). Verkkoalueeksi voidaan määrittää joko yksi alue, useampia alueita tai ”any”, jolloin kaikki lähdealueet ovat sallittuja. Lähdeosoitteena voidaan käyttää IP-osoitteita, kokonaisia verkkoja maskeineen, verkkotunnuksia (FQDN) tai maantieteelliseen sijainnin mukaan (region). Näiden lisäksi voidaan käyttää any kenttää, jolloin kaikki lähdeosoitteet kelpaavat.

User-välilehdellä voidaan määrittää sallitut käyttäjät tai käyttäjäryhmät. Tämän käyttö edellyttää, että User-ID toiminto on käytössä palomuurilla. Edellä mainittujen lisäksi voidaan valita ”any”, jolloin käyttäjärajoitusta ei ole. User välilehdellä voidaan ottaa käyttöön HIP profiilin (Host information profile) tarkastus. HIP-profiililla voidaan varmistaa päätelaitteen tietoturvan taso määrittämällä vaatimukset esimerkiksi virustorjunnalle, levyn kryptaukselle tai käyttöjärjestelmäversioille. Destination-välilehdellä määritetään kohdetiedot, joiden määritys toimii täysin samalla tavalla kuin lähdetietojenkin. Application-välilehdellä valitaan käytettävät applikaatiot. Applikaatiot valitaan valmiista listasta, johon on kerätty kaikki Palo Alto NGFW palomuurin tunnistamat applikaatiot. Palo Alto Networksin vastuulla on listauksen ylläpito ja tarvittavat muutokset viikottaisten päivitysten avulla. Service/URL category-välilehdellä voidaan määrittää haluttu protokolla (TCP tai UDP) ja portti. Jos liikenteen tyyppiä ei haluta määrittää, voidaan valita any. Mikäli palomuurisäännössä käytetään applikaatioita, voidaan serviceksi määrittää application-default, jolloin palomuuri hyväksyy applikaatioille vain standardinmukaisen liikenteen (esimerkiksi DNS = TCP 53). URL categoryn avulla voidaan hyödyntää Palo Alton verkko-osoitteiden kategorisointia ja esimerkiksi estää liikennöinti uhkapelikategorian alle luokitelluille sivustoille. Palo Alto Networks ylläpitää listaa sivustoista ja sivustojen uudelleenkategorisointia voi pyytää suoraan Palo Altolta.

Actions-välilehdellä valitaan toimenpide joka ko. sääntöön osuvalle liikenteelle halutaan tehtävän. Allow-vaihtoehto päästää liikenteen läpi hyväksytysti, kun taas deny estää liikenteen kulkemisen ja lähettää vastapäälle ilmoituksen liikennöinnin päättymisestä applikaatiolle määritetyn oletustavan mukaisesti. Drop-vaihtoehto estää liikenteen kulkemisen, mutta ei lähetä vastapäähän ilmoitusta liikennöinnin päättämisestä. Lisäksi voidaan käyttää reset-client, reset-server tai reset-both vaihtoehtoja, joista kaikki estävät liikenteen kulkemisen ja lähettävät ilmoituksen liikennöinnin päättymisestä, joko päätelaitteelle (client), palvelimelle (server) tai molemmille (both). Toimenpiteiden lisäksi actions-välilehdellä voidaan määrittää hyväksytylle liikenteelle käyttöön ylimääräisiä turvallisuutta parantavia tarkastuksia, esimerkiksi virustarkastukset ja haavoittuvuustarkastukset. Actions-välilehdllä on mahdollista valita myös halutaanko sääntöön osuvasta liikenteestä tehdä merkintä lokiin liikennesession alkaessa, liikennesession loppuessa tai ei ollenkaan, ja halutaanko mahdollinen loki lähettää esimerkiksi panoramaan, erilliselle syslog palvelimelle tai tietyille henkilöille sähköpostilla. Viimeisenä valintana voidaan säännölle vielä määrittää valinnainen aikataulu, joka määrää milloin sääntö on voimassa.

Target-välilehdellä määritetään minkä palomuurien konfiguraatioon tehty palomuurisääntö halutaan lisätä. Target-välilehti on käytössä vain Panoraman avulla device groupeihin määritetyillä palomuurisäännöillä. Suoraan palomuureilla tehdyt palomuurisäännöt tulevat käyttöön vain sille palomuurille, johon sääntö tehdään.



Kuva 14. Liikenteen suodatuskriteerit (Palo Alto Networks 2020, M4-5).

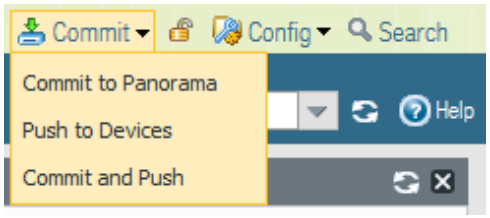
Kuva 15. Sääntötyypit (Palo Alto Networks 2020, M4-8).

Olemassa olevia palomuurisääntöjä voidaan poistaa kokonaan (delete), poistaa käytöstä (disable), ottaa uudelleen käyttöön (enable) ja kloonata (clone). Lisäksi palomuurisääntöjä voidaan vapaasti liikutella sääntökannassa ja usein tällaiselle saattaakin tulla tarvetta palomuurisääntöjen määrän kasvaessa suuremmaksi.

4.1.3 Muutosten tallentaminen laitteille

Kaikki Palo Alton NGFW palomuureilla ja Panoramassa tehdyt konfiguraatio- ja sääntökantamuutokset pitää tallentaa erikseen laitteiden aktiiviseen konfiguraatioon. Graafisella käyttöliittymällä tämä onnistuu oikean yläkulman commit painikkeen avulla (kuva 16). Yksittäisellä palomuurilla suoritettuna commit avaa näkymän, jossa voidaan valita halutaanko aktiiviseen laitekonfiguraatioon tallentaa kaikki odottavat muutokset, vai vain tietyn ylläpitäjän tekemät muutokset. Commit näkymässä on lisäksi mahdollista tarkastaa ja validoida tehdyt muutokset. Ylläpitäjä voi halutessaan lisätä myös kommentin konfiguraation tallennuksen yhteyteen.

Panoramalla suoritettuna commit tarjoaa kolme eri vaihtoehtoa: Commit to Panorama, Push to Devices ja Commit and Push (kuva 16). Commit to Panorama tallentaa konfiguraation Panoramaan myöhempää laitteille tallentamista varten. Push to Devices synkronoi Panoramaan tallennetun konfiguraation laitteiden aktiiviselle konfiguraatiolle ja Commit and push suorittaa molemmat aikaisemmin mainitut toiminnot yhdellä komennolla.



Kuva 16. Commit vaihtoehdot Panoramassa

4.1.4 Liikenteen monitorointi

Palomuurin sääntökannan toiminnan kannalta on tärkeää pystyä seuraamaan, miten palomuuri käsittelee liikennettä. Tätä toimintaa varten Palo Alton palomuurien läpi kulkevaa liikennettä voi seurata graafiselta käyttöliittymältä Monitor näkymän avulla. Kaikki palomuurille tuleva liikenne, joka osuu johonkin lokia keräävään palomuurisääntöön, jättää siitä merkinnän palomuurin liikennelokiin. Liikennelokiin jää merkintä kaikista liikennesessioiden alkamisista ja päättymisistä. Lokista nähdään mm. lähde- ja kohdeosoitteen tiedot, käytetty tietoliikenneprotokolla, portti, applikaatio, palomuurin liikenteelle suorittama toiminto, käytetty palomuurisääntö ja aikaleima. Monitorointi välilehdeltä nähdään käytännössä kaikki palomuurin liikenteestä keräämä tieto ja ylläpitäjä voi valita näkymäänsä vain haluamansa tiedot. Lokien näkyvyyttä voidaan rajata myös ylläpitäjien käyttöoikeuksien mukaan.

4.2 Forcepoint next-generation firewall

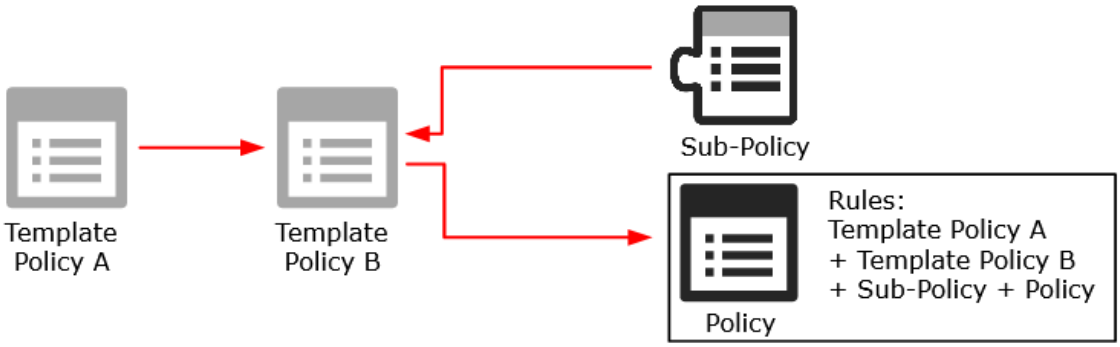
Forcepointin NGFW-palomuurien hallinta voidaan suorittaa graafisen käyttöliittymän kautta verkkoselaimen yli, etä- tai konsoliyhteydellä komentoriviltä tai keskitetyn hallintajärjestelmän kautta. Aivan kuten Palo Altonkin palomuureissa, hallintayhteyden muodostaminen vaatii laitteen alkukonfiguraatiota, mutta tätä ei aiheen rajauksen vuoksi käsitellä työssä. Tässä opinnäytetyössä pyrittiin hyödyntämään ensisijaisesti Forcepointin keskitettyä hallintaa sen tuomien etujen, helppokäyttöisyyden ja havainnollisuuden vuoksi.

4.2.1 Forcepoint NGFW Security Management Center

Forcepointin palomuureja voidaan hallita keskitetysti Forcepointin Security Management Centerin (SMC) avulla. Security management centeriä voidaan käyttää selaimella verkkopohjaisena tai paikallisesti asentamalla Security Management Center client työasemalle. Tässä opinnäytetyössä security management centeriä käytettiin verkkoselaimen avulla. Keskitetyn hallinnan avulla voidaan tarkkailla palomuurien läpi kulkevaa liikennettä, tehdä muutoksia laitekonfiguraatioon ja sääntökantoihin, ja suorittaa laitteiden ohjelmistopäivityksiä.

4.2.2 Sääntökannan hallinta

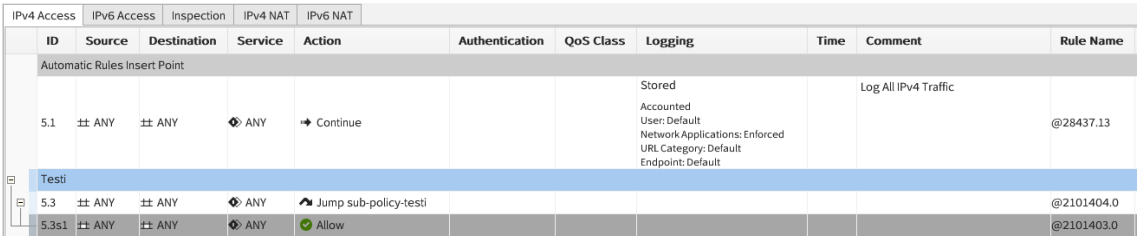
Forcepoint NGFW-palomuureilla sääntökanta rakentuu puumaiseen malliin erillisten sääntökantaan luotavien policy osioiden alle. Policy-osiot voidaan jakaa kolmeen luokkaan: Template policies, policies ja sub-policies. Policyt toimivat hierarkisesti ja ylemmillä tasoilla luodut policyt periyttävät omat sääntönsä alemman tason policyille (kuva 17). Uusi policy tulee luomisvaiheessa liittää aina jonkin olemassa olevan template policyn alle, jolloin myös kaikki template policyssä olevat säännöt periytyvät uudelle policylle. Template policyjen avulla voidaan helpottaa sääntökantojen ylläpitoa, sillä saman template policyn alle voidaan rakentaa useita erillisiä policyjä.



Kuva 17. Policyjen välinen hierarkia (Forcepoint 2019).

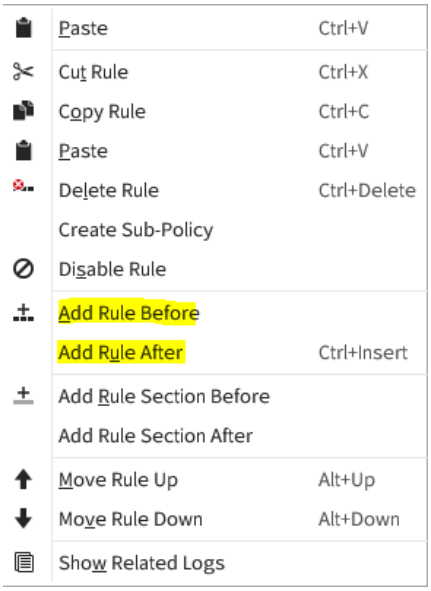
Sub-policyt ovat policyjen, template policyjen tai toisten sub-policyjen sisälle rakennettavia sääntöosioita. Sub-policy lisätään toisen policyn sisään lisäämällä nk. hyppysääntö (jump rule) halutun policyn sisälle. Hyppysäännöllä ohjataan siihen täsmäävä liikenne sub-policyyn, jossa palomuuri suorittaa liikenteelle sub-policyn sisältämien sääntöjen

mukaisen tarkastuksen (kuva 18). Sub-policyjen avulla voidaan yksinkertaistaa sääntökantanäkymää, kun kaikki palomuurisäännöt eivät ole automaattisesti näkyvillä, vaan ne ovat puumaisessa rakenteessa, josta haluttuja policyjä tai sub-policyjä voi avata tarkasteltavaksi yksitellen. Sub-policyjä rakentamalla voidaan myös nopeuttaa palomuurin toimintaa, sillä vain sub-policyä edeltävään hyppysääntöön osuva liikenne voidaan ohjata sub-policyyn, kun taas kaiken muun liikenteen annetaan jatkaa normaalisti sääntökannassa eteenpäin siihen asti kunnes liikenteelle löytyy täsmäävä palomuurisääntö. Sub-policyjä voidaan luoda sääntökantaan kahdella tavalla, joko tekemällä uusi sub-policy ja luomalla sen alle uusia palomuurisääntöjä tai valitsemalla olemassa olevia palomuurisääntöjä ja luomalla näistä uusi sub-policy. (Forcepoint 2019.)



Kuva 18. Sääntökantaan lisätty sub-policy

Uusia palomuurisääntöjä voidaan lisätä valitsemalla sääntökannasta jokin aikaisempi palomuurisääntö ja lisäämällä uusi tyhjä sääntö ko. palomuurisäännön eteen tai taakse (kuva 19).



Kuva 19. Palomuurisäännön lisääminen Forcepoint NGFW palomuurilla.

Uuden palomuurisäännön luomisessa käytetään useita kenttiä, jotka on lueteltu seuraavassa listauksessa:

- ID
- Source
- Destination
- Service
- Action
- Authentication
- Qos Class
- Logging
- Time
- Comment
- Rule Name
- Source VPN
- Hits.

ID-kentässä näkyvä numero on säännölle automaattisesti luotu tunnistenumero, jota ylläpitäjä ei voi muokata. Tunnistenumero määräytyy sen mukaan, mille paikalle sääntö on policyssä tehty. Source-kenttää käytetään lähdetietojen määrittämiseen. Source-kentässä voidaan käyttää käyttäjätietoa (user), IP-osoitetietoa (source address), verkkotunnusta (domain name), verkkoaluetta (zone), päätelaitteen käyttämää applikaatiota (endpoint application) tai päätelaitteen asetuksia (endpoint settings). Destination kentässä tehdään kohdetietojen määritys. Kohdetietojen määritykseen käytetään samoja kenttiä kuin lähdetietojenkin määritykseen, eli user,destination address, domain name, zone, endpoint application ja endpoint settings. Service kohdassa määritetään käytetty protokolla tai applikaatio. Halutessaan voi hyödyntää myös verkkosivun luokitukseen perustuvaa URL suodatinta (URL situation). Action-kenttä määrittää palomuurin liikenteelle tekemät toimenpiteet. Vaihtoehdot ovat:

- allow
- continue
- discard
- refuse

- jump
- apply blacklist.

Allow sallii liikenteen kulkemisen palomuurin läpi. Continue ohjaa liikenteen jatkamaan kulkuaan sääntökannan läpi. Discard hylkää liikenteen lähettämättä ilmoitusta liikennesession katkeamisesta lähettäjälle. Refuse hylkää liikenteen ja lähettää tiedon vastapäälle ICMP viestinä. Jump siirtää liikenteen jatkamaan suodatusprosessia määritettyyn sub-policyyn. Mikäli liikenne ei täsmää mihinkään sub-policyssä määritettyyn sääntöön, tarkastus jatkuu seuraavasta säännöstä aktiivisessa policyssä. Apply blacklist vertaa liikennettä nk. mustalle listalle lisättyihin tietoihin. Jos liikenne täsmää johonkin näistä tiedoista, liikenne hylätään, mutta jos liikenne ei täsmää mustalla listalla oleviin tietoihin, jatkuu liikenteen suodatusprosessi seuraavasta säännöstä.

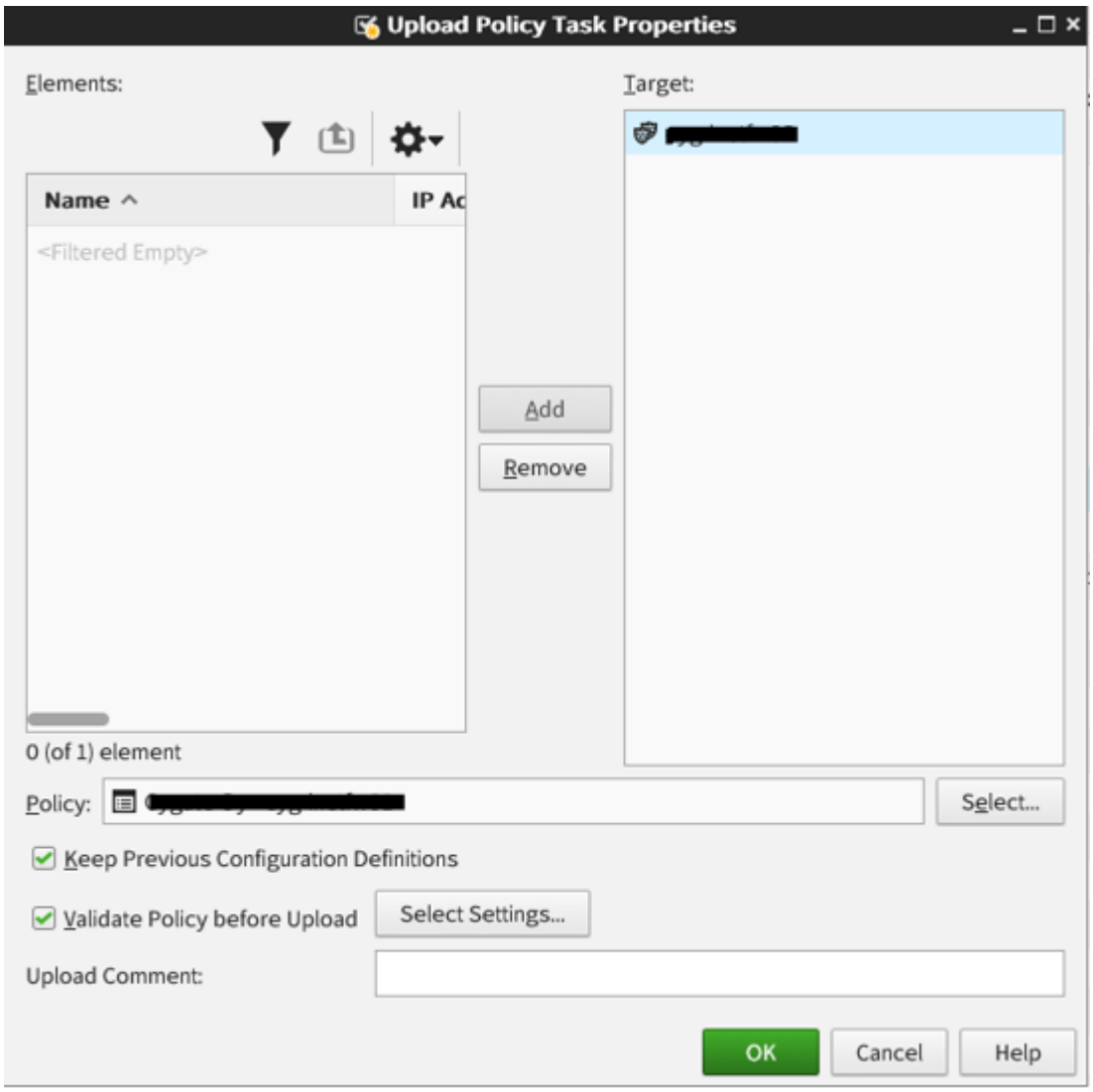
Authentication-kenttää voidaan käyttää sallimaan vain autentikoituneet käyttäjät. Ylläpitäjä voi valita sallittavat autentikaatiomenetelmät. Qos Class-kentän avulla liikenteelle voidaan määrittää haluttu QoS-luokka. Valittavina on high priority, normal priority ja low priority. Logging-kentässä määritetään minkälaista lokia säännöstä halutaan kerätä, vai halutaanko sääntöön osuva liikenne jättää kokonaan merkkaamatta liikennelokiin. Time-kentässä voidaan määrittää säännölle rajoitettu voimassaoloaika. Comment-kenttä on tarkoitettu säännölle kirjoitettavan vapaamuotoisen kommentin jättämistä varten. Kommenttia voidaan käyttää esimerkiksi säännön tarkoituksen selittämistä varten. Rule Name-kenttässä voidaan merkitä säännölle nimi. Säännöt saavat valmiiksi nimikenttään määritetyn uniikin tägin, jota ei voi poistaa, mutta nimen voi tallentaa tägin rinnalle. Source VPN-kenttään voidaan määrittää halutaanko suodatuksessa käyttää lähteenä tiettyä VPN yhteyttä. Hits-kentässä näkyy laskuri, joka laskee kuinka monta kertaa sääntöön on osunut liikennettä.

Yllämainituista kentistä ainoastaan Source, Destination, Service ja Action kentät ovat pakollisia. Palomuurisääntöjen paikkaa voidaan muuttaa sääntökannassa vapaasti niiden luomisen jälkeen. Sääntöjä voidaan myös ottaa pois käytöstä (disable) tai takaisin käyttöön (enable) tai poistaa kokonaan (delete). (Forcepoint 2019.)

4.2.3 Muutosten tallentaminen laitteille

Kun palomuurisääntöjä muokataan policyjen sisällä, tulee policyt asentaa uudelleen palomuureille muutosten voimaan saattamiseksi. SMC:llä toiminto voidaan suorittaa ensin

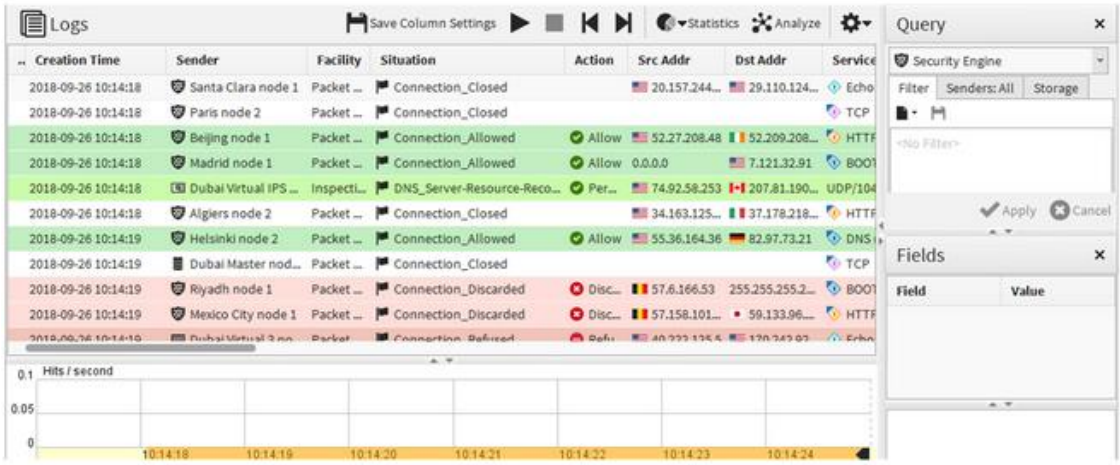
valitsemalla haluttu policy listasta ja sen jälkeen valitsemalla install policy vaihtoehto. Policyn asentaminen avaa uuden ikkunan, jossa voidaan varmistaa, mille palomuureille uusi policy halutaan tallentaa, ja lisäksi voidaan kirjoittaa vapaamuotoinen kommentti (kuva 20). SMC validoi asennettavan konfiguraation ennen sen tallentamista palomuureille ja ilmoittaa mikäli policyn asentamisessa on ongelmia. Ylläpitäjä voi vielä peruuttaa policyn asentamisen ja palata korjaamaan virheet. Virheilmoituksen voi myös ohittaa ja asentaa policyn varoituksista huolimatta, mutta tällöin on riskinä että jokin palomuurin konfiguraatiossa voi mennä rikki.



Kuva 20. Policyn asennus palomuureille.

4.2.4 Liikenteen monitorointi

Forcepoint Security Management Centerissä palomuurin keräämää liikennelokia voi tarkastella logs välilehdeltä (kuva 21). Liikennettä voi tarkastella reaaliajassa sen kulkiessa palomuurin läpi tai suodattamalla lokia haluttujen parametrien mukaisesti. Lokinäkymässä voi myös valita tiettyyn palomuurisääntöön osunutta liikennettä ja siirtyä tarkastelemaan kyseisen palomuurisäännön ominaisuuksia. Tämä on erityisen hyödyllistä, jos palomuuri estää sellaista liikennettä, mitä ei haluttaisi estettävän. Ylläpitäjä voi siirtyä suoraan säännön konfigurointiin lokinäkymästä ja tehdä tarvittavat muutokset sääntöön, jotta liikenne saadaan jatkossa kulkemaan palomuurin läpi ongelmitta.



Kuva 21. Forcepoint SMC lokinäkymä (Forcepoint 2019).

4.3 Check Point Software Systems next-generation firewall

Check Pointin seuraavan sukupolven palomuureista käytetään nimitystä Security Gateway (SG). Palomuurien hallinta voidaan suorittaa komentorivillä, käyttämällä graafista käyttöliittymää web-selaimella, tai keskitetyn hallintajärjestelmän kautta. Työssä hyödynnettiin vaihtoehdoista viimeiseksi mainittua, eli keskitettyä hallintajärjestelmää.

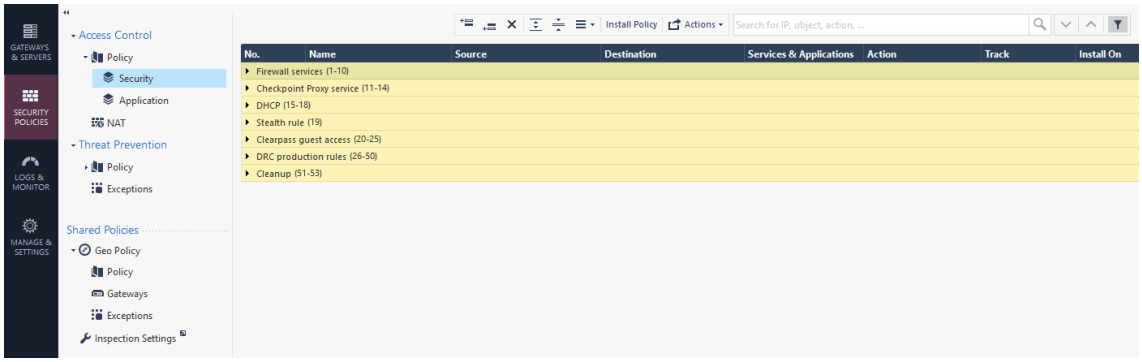
4.3.1 Check Point Security Management Server

Check Pointin NGFW palomuurien keskitetty hallinta tapahtuu yrityksen verkkoon asennettavan erillisen hallintapalvelimen, Check Point Security Management Serverin,

kautta. Hallintapalvelin voidaan asentaa fyysiselle koneelle tai virtuaalikoneelle. Kun Check Point Security Management Server on asennettu ja otettu käyttöön, voidaan asentaa hallintaohjelmisto, Check Point SmartConsole. Uusin ohjelmisto on ladattavissa Check Pointin verkkosivuilta. SmartConsole muodostaa yhteyden Security Management Serverin kanssa, minkä jälkeen kaikkia Security Management Serveriin liitettyjä palomuureja voidaan hallita SmartConsolen kautta.

4.3.2 Sääntökannan hallinta

Check Point Smart Console hallinta-alustalla sääntökantojen hallinta tapahtuu Security Policies välilehdellä. Security Policies välilehdellä on listaus kaikkien hallinta-alustalle lisättyjen palomuurien tai palomuuriklustereiden sääntökannoista. Sääntökantaa pääsee muokkaamaan valitsemalla haluamansa sääntökannan listalta. Sääntökannnan avaaminen muokkausta varten avaa kuvan 22 kaltaisen näkymän.



Kuva 22. SmartConsole sääntökannan muokkausnäkymä.

Sääntökantaan voidaan rakentaa osioita, joiden alle palomuurisäännöt on helppo jaotella esimerkiksi tyypin mukaan. Sääntökantaosiot on mahdollista avata näkyville tai piilottaa, mikä helpottaa sääntökannan lukemista ja hallintaa. Sääntöosioden käyttö ei kuitenkaan ole pakollista ja sääntökanta toimii täysin normaaliin tapaan riippumatta siitä onko osiointi käytössä vai ei. Osiointi ei vaikuta sääntöjen järjestykseen, vaan säännöt numeroidaan järjestysnumerolla niiden luontivaiheessa ja sääntöjä voi liikutella sääntökannassa haluamilleen paikoille.

Uusi palomuurisääntö voidaan lisätä sääntökantaan valitsemalla joku olemassaolevista palomuurisäännöistä tai sääntöosioista ja käyttämällä toimintoa add rule above tai add rule below. Uusi palomuurisääntö syntyy sääntökantaan valitun säännön edelle tai

valitun säännön jälkeen, riippuen siitä kumpaa toimintoa käytettiin. Check Point käyttää palomuurisäännöissä seuraavia kenttiä:

- No.
- Name
- Source
- Destination
- Services & Applications
- Action
- Track
- Install On

No.-kenttä täyttyy automaattisesti säännön luomishetkellä liukuvalla järjestysnumerolla, joka kertoo palomuurisäännön järjestyksen sääntökannassa. Name-kenttää käytetään vapaavalintaisen nimen määrittämiseen säännölle. Source-kentässä määritellään lähdetiedot. Lähdetietoina voi käyttää yksittäisiä IP-osoitteita, IP-verkkoja, verkkoalueita (zone), dynaamisia objekteja, verkkotunnuksia, tunnistettuja käyttäjiä tai itsestään päivittyviä objekteja (esimerkiksi julkisten pilvipalveluiden päivittyvää IP-osoite listaa). Destination-kentässä määritettäviin kohdetietoihin voidaan käyttää samoja tietoja kuin source-kentässäkin (ks. edellinen kohta). Services & Applications-kentässä määritellään halutut palvelut tai applikaatiot. Määritys voidaan tehdä palveluiden, applikaatioiden, mobiiliapplikaatioiden, verkkosivujen, internet-liikenteen oletuskategorioiden tai itsetehtyjen mukautettujen ryhmien tai kategorioiden mukaan.

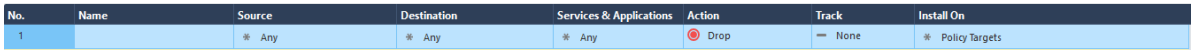
Action-kentässä määrätään palomuurin toimenpiteet liikenteelle. Vaihtoehdot ovat:

- Accept
- Drop
- Ask
- Inform
- Reject

Accept sallii liikenteen kulkemisen. Drop pudottaa liikenteen lähettämättä ilmoitusta liikenteen aloittaneelle osapuolelle ja liikenne näkyy aloittajalle vain aikakatkaisuna ilman vastausta. Ask-toiminnon avulla voidaan kysyä käyttäjältä kysymys ja lisätä mukaan mahdollisuus vastaukselle, eli esimerkiksi valintaruutu, jolla käyttäjä ilmoittaa tiedostavansa mahdolliset riskit. Inform-toiminto lähettää käyttäjälle viestin, mutta ei pyydä

vastausta tai hyväksyntää. Reject estää liikenteen ja lähettää TCP reset paketin liikenteen aloittaneelle osapuolelle, minkä jälkeen liikennesessio sulkeutuu.

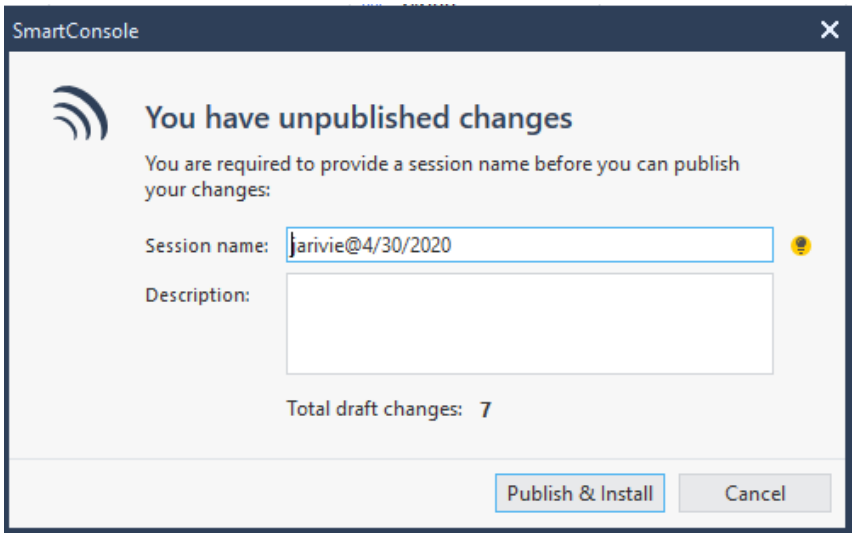
Track-kentässä määritellään miten tieto liikennesessiosta halutaan tallentaa. Oletuksena tieto tallennetaan palomuurin liikennelokiin, mutta vaihtoehtoisesti voidaan lähettää myös sähköposti-ilmoituksen tai jättää liikenteen tiedot kokonaan tallentamatta lokiin. Install On-kenttää käytetään määrittämään palomuurit, joille sääntö tullaan asentamaan. Oletuksena sääntö asennetaan vain sille palomuurille tai palomuuriklusterille, jonka sääntökantaa ollaan muokkaamassa.



Kuva 23. Kentät palomuurisäännössä.

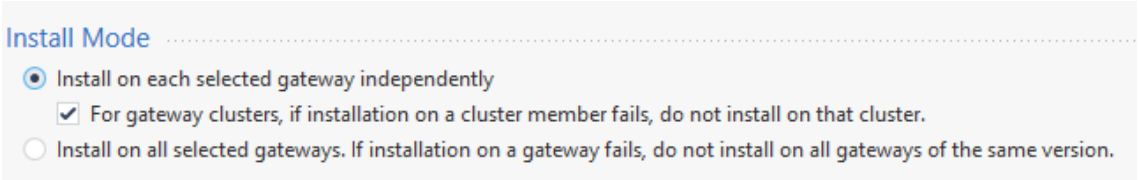
4.3.3 Muutosten tallentaminen laitteille

Palomuureille tehdyt muutokset tulee tallentaa laitteille, jotta muutokset tulevat voimaan palomuurien aktiivisessa kongifuraatiossa. Keskitetyn hallinnan kautta tehdyille muutoksille voidaan käyttää päävalikosta avautuvaa Install policy toimintoa. Tämä avaa kuvan 24 mukaisen ikkunan, jossa ylläpitäjää pyydetään julkistamaan tehdyt muutokset ja nimeämään istunto, jolla muutokset tehtiin. Istunto nimetään oletuksena ylläpitäjän käyttäjänimen ja päivämäärän mukaan. Julkistetut muutokset tallentuvat muutoslokiin josta kaikkien ylläpitäjien on helppo seurata, kuka muutoksia on tehnyt. Lisäksi voidaan kirjoittaa valinnainen kuvaus tehdyistä muutoksista.



Kuva 24. Policyn julkistaminen.

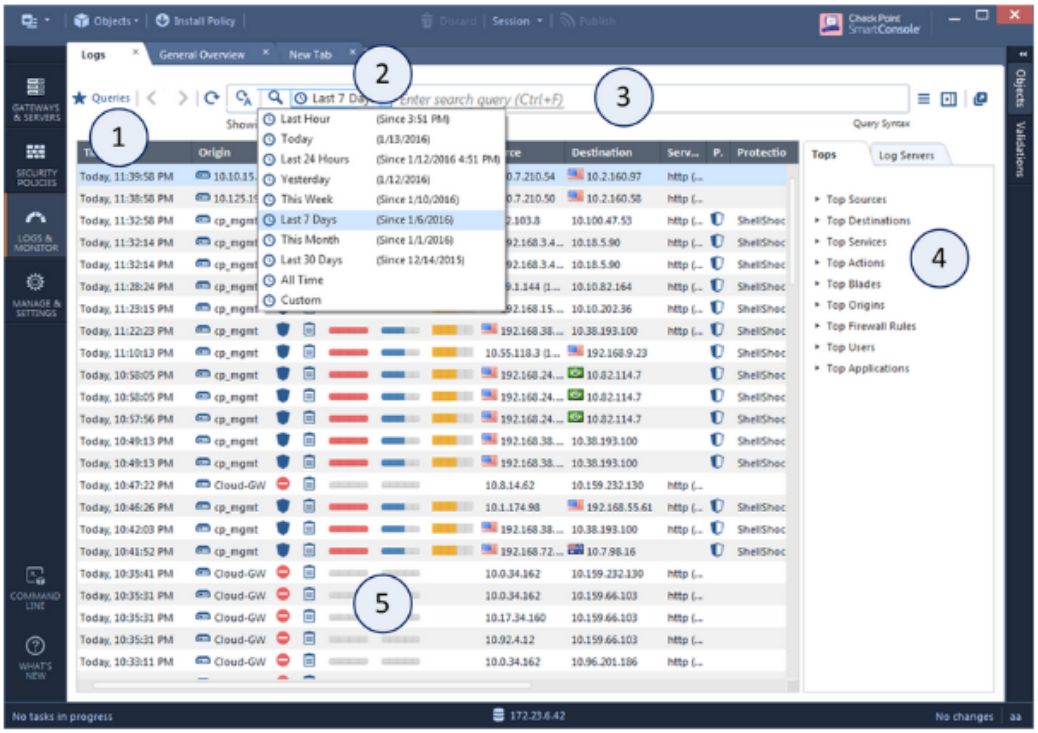
Kun tiedot julkistamista varten on täytetty, voidaan muutos julkistaa ja uusi Policy asentaa palomuureille. Julkistamisen jälkeen avautuu policyn asennusikkuna, josta valitaan haluttu asennustapa ja haluttu policy. Policyn asennukseen on kaksi vaihtoehtoa. Joko asennetaan policy erikseen kaikille valituille palomuureille, tai sitten asennetaan policy kaikille palomuureille samanaikaisesti (kuva 25). Policyn asennuksesta voi seurata virheitä (warning) tai se voi epäonnistua kokonaan, jos policyssä on sellaisia virheitä, jotka voivat rikkoa palomuurin toiminnan.



Kuva 25. Policyn asennusvaihtoehdot.

4.3.4 Liikenteen monitorointi

Liikenteen monitorointi Check Point SmartConsolessa tapahtuu omalla Logs&Monitor-välilehdellään (kuva 26). Check Point tarjoaa lukuisia erilaisia tapoja lokien suodattamiseen, mutta useimmiten on helpointa rajata liikennelokeja kohde- ja lähdeosoitteiden perusteella. Liikennelokiin osuvasta liikenteestä voidaan avata myös ykistyiskohtaisempi näkymä, josta nähdään mm. mihin palomuurisääntöön kyseinen liikenne osuu. Lokinäkymästä voidaan myös siirtyä suoraan muokkaamaan sitä palomuurisääntöä, johon liikenne osuu.



Item	Description
1	**Queries** - Predefined and favorite search queries.
2	**Time Period** - Search with predefined custom time periods.
3	**Query search bar** - Define custom queries in this field. You can use the GUI tools or manually enter query criteria. Shows the query definition for the most recent query.
4	**Log statistics pane** - Shows top results of the most recent query.
5	**Results pane** - Shows log entries for the most recent query.

Kuva 26. Check Point SmartConsole lokinäkymä (Check Point 2019).

5 YHTEENVETO JA TULOSTEN ANALYSOINTI

Opinnäytetyön aiheena oli perehtyä kolmen eri palomuurivalmistajan NGFW palomuurilaitteisiin ja vertailla niiden sääntökantoja erityisesti ominaisuuksien ja ylläpidon näkökulmasta. Työn suorituksessa hyödynnettiin mahdollisuutta päästä suorittamaan oikeita hallinnollisia tehtäviä asiakasympäristöissä oman työn yhteydessä.

Palomuurien hallinta perustui pääasiassa samoihin periaatteisiin kaikkien valmistajien laitteilla, mutta hallinnointiin liittyviä eroavaisuuksia löytyi silti runsaasti. Palo Alton ja Check Pointin palomuureilla sääntökannat rakentuvat suoraviivaisemmin ja kaikkea palomuurille saapuvaa liikennettä kuljetetaan sääntökannan läpi täsmäävän säännön löytymiseen asti. Forcepointin palomuureilla pyritään helpottamaan palomuurin taakkaa rakentamalla puumaiseen rakenteeseen perustuva sääntökanta, jossa liikennettä pyritään ohjaamaan erillisiin alikantoihin, eli sub-policyihin, joissa liikenteen suodatus suurimmaksi osaksi tapahtuu. Kaikki laitevalmistajat hyödyntävät hallintatehtävissä omia alustojaan ja pyrkivät jatkuvasti kehittämään järjestelmiään helppokäyttöisemmiksi ja selkeämmiksi. Oman käyttökokemuksen perusteella Palo Alton palomuurit tuntuvat mieluisimmilta käyttää selkeän käyttöliittymän ja kattavien ominaisuuksien vuoksi, mutta paremmuusjärjestykseen palomuureja ei voi työn perusteella asettaa.

Uuden sukupolven palomuurilaitteet tarjoavat nykyisin niin suuren määrän ominaisuuksia ja toiminnallisuuksia, ettei kaikkien ominaisuuksien perinpohjainen vertailu yhden opinnäytetyön pohjalta ole mahdollista. Työssä kuitenkin onnistuttiin tuomaan hyvin esille NGFW-palomuurien toimintaperiaate ja esittelemään tärkeimmät sääntökantojen ylläpitoa koskevat tehtävät oikeiden esimerkkien pohjalta. Työtä olisi helppo jatkokehittää perehtymällä yhä syvällisemmin sääntökantojen ominaisuuksiin ja esittelemällä myös vähemmän käytettyjä toimintoja ja ominaisuuksia tarkemmin.

LÄHTEET

Blacharski, D. 2010. How I Got Here: Nir Zuk, CTO, Palo Alto Networks. Viitattu 10.4.2020. https://www.itworld.com/article/2756415/how-i-got-here--nir-zuk--cto--palo-alto-networks.html

Check Point Software Technologies 2020. Security Zone. Viitattu 11.4.2020. https://sc1.checkpoint.com/documents/R80.20/SmartConsole_OLH/EN/html_frameset.htm?topic=documents/R80.20/SmartConsole_OLH/EN/TE5TdfvLDUAMRJmWiaUeKw2

Check Point Software Technologies 1994-2020. Company Overview. Viitattu 11.4.2020. https://www.checkpoint.com/about-us/company-overview/#

Check Point Software Technologies 2020. Quantum Appliance Comparison Chart. Viitattu 13.4.2020. https://www.checkpoint.com/downloads/products/check-point-appliance-comparison-chart.pdf

Check Point Software Technologies 2019. Security Management Administration Guide. Viitattu 23.4.2020. https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_SecurityManagement_AdminGuide/html_frameset.htm

Check Point Software Technologies 2019. Logging. Viitattu 24.4.2020. https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/131914

Forbes Media LLC 2020. Palo Alto Networks (PANW). Viitattu 11.4.2020. https://www.forbes.com/companies/palo-alto-networks/#19604a19f564

Forcepoint 2020. About Us. Viitattu 11.4.2020. https://www.forcepoint.com/company/about-us

Forcepoint 2020. NGFW Appliance. Viitattu 11.4.2020. https://www.forcepoint.com/appliance/forcepoint-ngfw-appliances

Forcepoint 2017. Forcepoint Next Generation Firewall. Viitattu 10.4.2020. https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_en_0.pdf

Forcepoint 2019. Creating and managing policy elements. Viitattu 20.4.2020. https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.7.0/GUID-6B798A15-C5BE-4A06-B7EA-B1FB1C6CA17C.html

Forcepoint 2019. What the Logs view shows. Viitattu 23.4.2020. https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.7.0/GUID-8B3B9B63-CBA1-47C5-848F-0C9AA3B3D041.html

Helmick, S. 2016. Raytheon|Websense Is Now Forcepoint™. Viitattu 14.4.2020. https://www.forcepoint.com/newsroom/2016/raytheonwebsense-now-forcepoint

Kaur, R., Hils, A., D'Hoinne, J., Watts, J. 2019. Magic Quadrant for Network Firewalls. Viitattu 7.4.2020. https://www.gartner.com/doc/reprints?id=1-1OIMIBCY&ct=190919&st=sb

Liu, A.X. 2010. Firewall Design and Analysis. Viitattu 5.4.2020. https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=731297

Lucidchart 2020. Using network diagrams for diagnosis and troubleshooting. Viitattu 4.4.2020. https://www.lucidchart.com/blog/how-to-diagram-your-network-for-diagnosis-and-troubleshooting

Oppliger, R. 1997. Internet security: firewalls and beyond. Viitattu 4.4.2020. https://dl.acm.org/doi/pdf/10.1145/253769.253802

Palo Alto Networks 2020. About Us. Viitattu 10.4.2020. https://www.paloaltonetworks.com/about-us

Palo Alto Networks 2020. Viitattu 11.4.2020. https://www.paloaltonetworks.com/products/product-selection

Palo Alto Networks 2020. Add a Template. Viitattu 18.4.2020. https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/add-a-template

Palo Alto Networks 2017-2020. Approved Partner Student Kit - Firewall 9.1 Essentials: Configuration and Management Version A (APSK-PAN-EDU-210 9.1 Version A).

Palo Alto Networks 2020. Security policy fundamentals. Viitattu 7.4.2020. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClWZCA0

Palo Alto Networks 2020. Device Group Hierarchy. Viitattu 20.4.2020. https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy.html

Palo Alto Networks 2020. Evaluation order of Panorama pushd security policies. Viitattu 20.4.2020. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CljVCAS

Pescatore, J. Young, P. 2009. Defining the Next-Generation Firewall. Viitattu 5.4.2020. http://img1.custompublish.com

Scarfone, H. & Hoffman, P. Guidelines on Firewalls and Firewall Policy Viitattu 4.4.2020. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Solarwinds MSP 2019. Stateful vs. Stateless Firewall Differences. Viitattu 5.4.2020. https://www.solarwindsmsp.com/blog/stateful-vs-stateless-firewall-differences