Nykyaikaiset palomuurit ja niiden kehityssuunnat

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Teknillinen tiedekunta
Huhtikuu 2025
Julia Kauppinen

TURUN YLIOPISTO
Tietotekniikan laitos

Julia Kauppinen: Nykyaikaiset palomuurit ja niiden kehityssuunnat

TkK-tutkielma, 23 s.
Teknillinen tiedekunta
Huhtikuu 2025

Palomuurit ovat tärkeä osa tietoturvaa. Ne suojaavat käyttäjiä haitallisilta tahoilta estämällä luvattoman pääsyn järjestelmiin ja edistävät samalla internetin turvallisuutta. Palomuurit ovat kehittyneet vuosien varrella hyvin paljon. Kyberuhat ovat tulleet entistä monimutkaisemmiksi ja älykkäämmiksi, jonka takia myös palomuurien on täytynyt kehittyä pysyäkseen ajan tasalla ja tarjotakseen tehokasta suojaa.

Tutkielma tarkastelee nykyaikaisia palomuureja ja niiden kehityssuuntia. Työssä käydään läpi, miten palomuurit ovat kehittyneet historian saatossa, millaisia tekniikoita palomuureissa käytetään ja mihin suuntaan teknologia saattaa olla kehittymässä.

Palomuureilla tapahtuva tietoliikenteen suodatus toteutuu IP-, TCP- ja UDP- protokollien kautta. Palomuuri koostuu useista ominaisuuksista, jotka määrittävät sen toiminnan, kuten säännöt, suodatuskriteerit, kirjautumiskäytännöt, sallittujen ja estettyjen liikennetyyppien määrittely, käyttöoikeuksien hallinta ja liikenteen tarkastustasot.

Palomuureja voidaan jaotella erilaisiin tyyppeihin niiden toimintaperiaatteen ja sijoituspaikan mukaan. Yleisimpiä tyyppejä ovat perinteiset verkko- ja sovellustason palomuurit, pilvipohjaiset palomuurit sekä seuraavan sukupolven palomuurit (NGFW), jotka tarjoavat syvemmän liikenteen analyysin ja parempia suojausratkaisuja. Lisäksi palomuurit voivat olla joko laitteistopohjaisia tai ohjelmistopohjaisia.

Asiasanat: palomuurit, tekoäly, palomuuritekniikat, palomuurien kehitys

UNIVERSITY OF TURKU
Department of Computing

Julia Kauppinen: Nykyaikaiset palomuurit ja niiden kehityssuunnat

Bachelor's Thesis, 23 p.
Tietotekniikan laitos
April 2025

Firewalls are an important part of cybersecurity. They protect users from malicious entities by blocking unauthorized access to systems and simultaneously promote the security of the internet. Firewalls have evolved significantly over the years. As cyber threats have become more complex and intelligent, firewalls have also had to evolve to stay up to date and provide effective protection.

This thesis examines modern firewalls and their development trends. The work covers how firewalls have evolved throughout history, what techniques are used in firewalls, and in which direction the technology may be developing.

The traffic filtering in firewalls occurs through IP, TCP and UDP protocols. A firewall consists of several features that define its operation, such as rules, filtering criteria, and authentication practices. These features include defining allowed and blocked traffic types, access control, and traffic inspection levels.

Firewalls can be classified into different types based on their operating principle and location. The most common types are traditional network and application layer firewalls, cloud-based firewalls, and next-generation firewalls (NGFW), which provide deeper traffic analysis and better security solutions. Additionally, firewalls can be either hardware-based or software-based.

Keywords: firewall, artificial intelligence, firewall technologies, the development of firewalls

Sisällys

Lyhenteiden selitykset

NGFW	Next Generation Firewall, seuraavan sukupolven palomuuri
DPI	Deep Packet Inspection, syväpakettitarkistus
TCP	Transmission Control Protocol, lähetyksen ohjausprotokolla
UDP	User Datagram Protocol, käyttäjän datagrammiprotokolla
DNS	Domain Name System, nimipalvelujärjestelmä
SSL	Secure Sockets Layer, suojattujen yhteyksien kerros
TLS	Transport Layer Security, TLS-salaus

1 Johdanto

Palomuurit ovat olleet tärkeä osa tietoverkkojen turvallisuutta jo useiden vuosikymmenien ajan. Varhaiset palomuurit olivat hyvin yksinkertaisia, ja niiden tarkoituksena oli suodattaa verkkoliikennettä sekä estää ulkopuoliset tunkeutujat pääsemästä verkkoon. Nykyisin palomuurit ovat huomattavasti monipuolisempia ja kehittyneempiä: ne pystyvät paljon muuhunkin kuin pelkkään liikenteen suodatukseen.

Nykyaikaiset palomuurit hyödyntävät tekoälyä ja koneoppimista, joiden avulla ne voivat tehdä älykkäitä päätöksiä ja mukautua nopeasti muuttuviin uhkiin. Tällaisiin nykyaikaisiin ominaisuuksiin kuuluvat esimerkiksi uhkatiedustelu, joka tarjoaa ajantasaista tietoa uusista uhkista. Syväpakettitarkistus mahdollistaa verkkoliikenteen tarkemman analysoinnin, ja salausprotokollien käsittely turvaa tiedonsiirron myös salatulla liikenteellä. Lisäksi koneoppimisen ansiosta palomuurit voivat oppia jatkuvasti ja mukautua itsenäisesti, mikä parantaa niiden tehokkuutta uhkien torjunnassa. Zero trust -periaatteen mukaisesti palomuurit myös valvovat käyttäjiä ja laitteita verkossa entistä tiukemmin sillä oletuksella, ettei kukaan ole automaattisesti luotettava.

Tässä tutkielmassa perehdytään siihen, miten palomuurit ovat kehittyneet ja mitä ominaisuuksia nykyaikaiset järjestelmät tarjoavat tietoverkkojen suojaukseen sekä millaisia kehityssuuntia on odotettavissa tulevaisuudessa. Tutkielma on toteutettu kirjallisuuskatsauksena.

Tutkielmassa tarkastellaan kahta tutkimuskysymystä:

1. Miten palomuuritekniikka on kehittynyt ja mitkä tekniikat ovat nykyisissä palomuureissa keskeisiä?

2. Mitkä ovat keskeiset tulevaisuuden kehityssuunnat palomuuritekniikoille ja mikä on tekoälyn merkitys niissä?

Lähdeaineistoa etsittiin käyttämällä Google Scholar -hakupalvelua ja hyödyntämällä hakusanoja "firewall", "firewall and AI", "next generation firewall"sekä "firewall history". Lisäksi osa lähteistä on löydetty alkuperäisten lähteiden lähdeluetteloiden kautta.

Tutkielma etenee seuraavasti: Lukija ensiksi johdatetaan aiheeseen, mikä auttaa lukijaa ymmärtämään tutkielman sisältöä paremmin. Seuraavassa osiossa käydään läpi, mikä palomuuri on ja sen historiallista kehitystä. Tämän jälkeen syvennymme tutkielman kysymyksiin ja tarkastelemme nykyaikaisia palomuuritekniikoita tarkemmin. Tämän jälkeen siirrytään tarkastelemaan ennakoituja kehityssuuntia, joiden avulla pyritään hahmottamaan mihin suuntaan palomuuriteknologiat saattavat olla kehittymässä tulevaisuudessa.

Tutkielman viimeisessä kappaleessa käydään läpi keskeisimmät havainnot ja vastataan työn alussa esitettyihin kysymyksiin. Lopuksi tehdään yhteenveto koko tutkielman sisällöstä, mikä auttaa lukijaa hahmottamaan aiheen kokonaiskuvaa ja syventämään ymmärrystä palomuurien merkityksestä ja kehityksestä.

Tätä tutkielmaa on korjattu ja viimeistelty tekoälyavusteisesti kielenhuollon osalta.

2 Palomuurit ja niiden kehitys

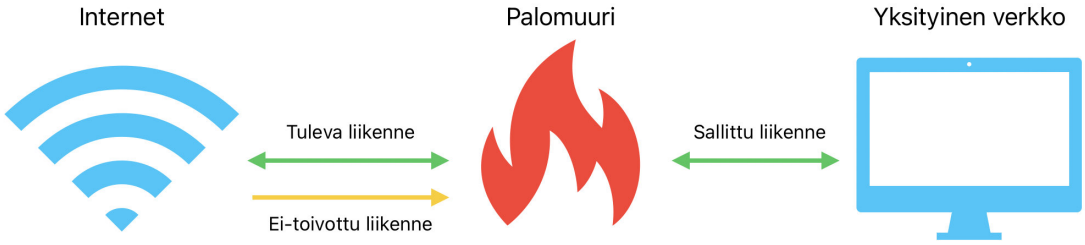
Tässä luvussa käsitellään palomuurien kehitystä ja niihin liittyvää teknologiaa. Ensiksi tarkastellaan mitä palomuuri tarkoittaa ja miten se toimii. Sen jälkeen siirrytään palomuurien kehityshistoriaan, joka loi perustan nykyiselle tietoturvateknologialle. Lopuksi käydään läpi palomuurien eri sukupolvet ja niiden ominaisuudet.

2.1 Palomuuritekniikan perusteet

Palomuurin tehtävä on turvata verkkoliikenteen asemat (eng. network hosts) siten, että se valvoo ja hallitsee liikennevirtaa. Verkkoliikenteen asemat ovat laitteita, jotka kommunikoivat verkon sisällä kuten esimerkiksi tietokoneet ja älypuhelimet. Kuvassa 2.1 näkyy miten palomuuri toimii, toisin sanoen palomuuri toimii portinvartijana.

Tietoturvassa palomuurin rooli on ensisijainen. Se toimii ensimmäisenä puolustuslinjana, tarkkaillen ja halliten verkkoliikennettä estääkseen mahdolliset kyberuhat. Ylläpitämällä esteen (eng. barrier) luotettavien ja epäluotettavien verkkojen välillä palomuurijärjestelmät ovat keskeisiä varmistamaan yrityksien omaisuuden ja datan turvallisuuden [1]. Palomuurit luokitellaan yleisesti viiteen päätyyppiin: paketinsuodatuspalomuuri, sovellustason palomuuri, piiripohjainen palomuuri, tilallinen palomuuri ja seuraavan sukupolven palomuuri [2].

Palomuurit tutkivat ja suodattavat paketteja omien sääntöjensä perusteella. Jos paketti ei täytä asetettuja sääntöjä, sen pääsy kielletään [1]. Kappaleessa 2.3 käydään paketinsuodatusta tarkemmin läpi.



Kuva 2.1: Palomuuri suojaa verkkoa estämällä haitallisen liikenteen ja sallimalla vain luotettavat yhteydet internetistä yksityiseen verkkoon.

2.2 Palomuurien historiaa

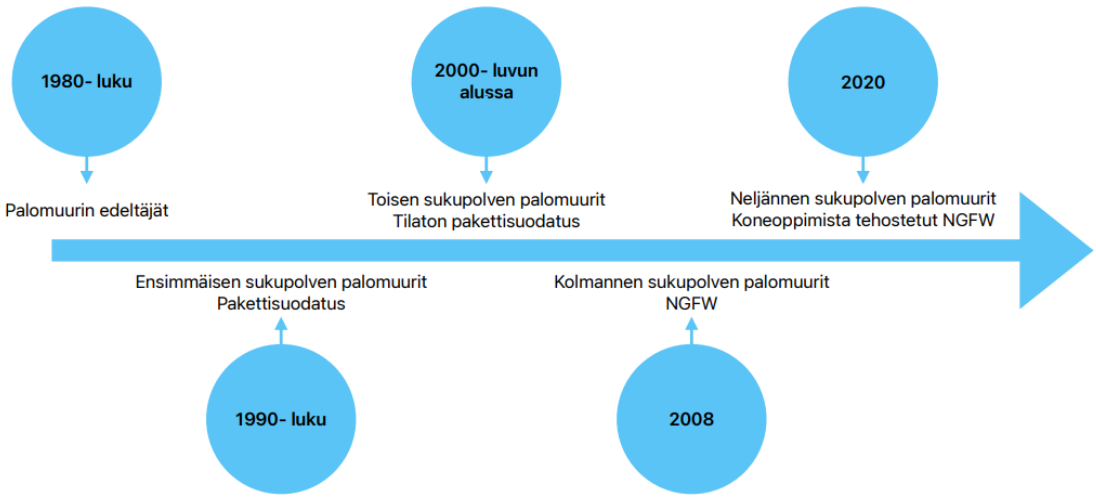
Palomuureille ei ole ollut vain yhtä keksijää, vaan niiden kehityksessä on ollut mukana monia eri tahoja ajan myötä. Palomuurien historia alkoi 1980- luvulla yksinkertaisella pakettisuodatuksella (eng. packet filtering) kehittyen nykyajan uudeksi seuraavan sukupolven palomuuriksi (eng. next generation firewall, NGFW). [3]

Palomuurit olivat aluksi fyysisiä laitteita, jotka pysäyttivät ulkoiset tunkeutujat. Termi "palomuuri"viittasi alun perin rakennuksien väliseiniin, jotka oli suunniteltu rajoittamaan tulipalon leviämistä. Myöhemmin tämä ennaltaehkäisevä idea omaksuttiin myös juniin, joissa käytettiin rautaisia seiniä suojaamaan matkustajaosastoja. [3]

Ennen palomuurien ilmestymistä 1980-luvun loppupuolella verkon reitittimet alkoivat yleistyä. Reitittimien alkumuodot toimivat verkon erottajana. Reititin ylläpiti peruseristystä varmistaen, että ongelmat tai liiallista liikennettä aiheuttavat protokollat eivät siirtyneet verkon toiselta puolelta toiselle [3]. Tämä perusajatus kehittyi myöhemmin palomuuriksi. Ensimmäinen palomuuri keskittyi liikenteen suodatukseen, josta tämä alkoi kehittyä sovelluskerrokseen ja siitä vielä edeten kuljetus- ja verkkokerrokseen. [3]

AT & T Bell Laboratories oli keskeisessä roolissa palomuurien kehityksessä, kun se kehitti ensimmäisen piiritason portin vuosina 1989–1990. Tämä innovaatio loi tär-

keän pohjan tulevalle palomuurien kehitystyölle. Ajan myötä tietoturva-asiantuntijat laajensivat näitä ideoita ja integroitavat ne laajempaan palomuuriteknologiaan. [3]



Kuva 2.2: Aikajana palomuurien kehityksestä

Palomuurien kehityksessä tunnistetaan neljä sukupolvea. Eri kehitysvaiheiden luokittelussa sukupolviin on lähteiden välissä erimielisyyttä. Lähteen [4] mukaan sukupolvet määrittyvät seuraavasti:

- ensimmäisen sukupolven palomuuri on paketinsuodatus
- toisen sukupolven palomuurit ovat syväpakettitarkistus (eng. deep packet inspection, DPI)
- kolmannen sukupolven palomuurit ovat NGFW ja sovelluskerros (eng. layer 7, application layer)
- neljännen sukupolven palomuurit ovat pilvipohjaiset palomuurit (eng. cloud)

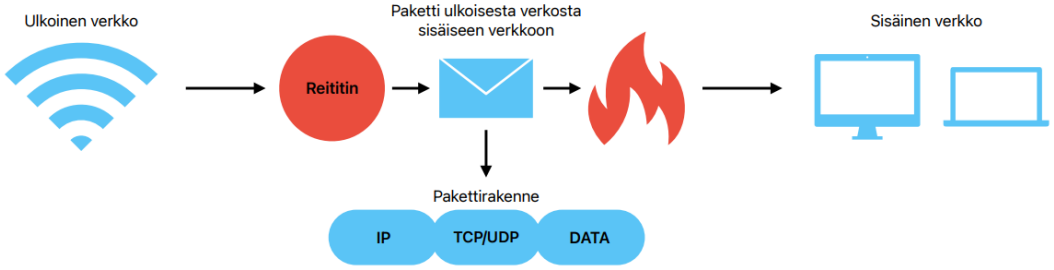
Aikasemman kuvan 2.2 perusteella näemme erilaisen näkemyksen neljästä sukupolvesta, joka on lähteestä [3].

2.3 Palomuuritekniikoiden sukupolvet

Ensimmäisen sukupolven palomuurit perustuivat paketinsuodatukseen [4]. Tarve kasvoi systeemeille, jotka pystyisivät valvomaan tietoturvakäytäntöjä verkon tasolla, kun yhteen liitettyjen verkkojen käyttö suureni.

Pakettisuodatuspalomuurit toimivat OSI-mallin (eng. Open Systems Interconnection Reference Model) verkkokerroksella (eng. layer 3, network layer) siten, että se tarkastelee verkossa kulkevia datapaketteja. Paketteja arvioitiin ennalta määrättyjen sääntöjen perusteella, joissa otettiin usein huomioon paketin lähde- ja kohde-IP-osoitteet, porttinumerot sekä käytetty protokolla joko TCP (eng. Transmission Control Protocol) tai UDP (eng. User Datagram Protocol). Prosessi muistuttaa postin toimintaa, jossa kirjeitä lajitellaan osoitteen perusteella avaamatta niitä itse. Kuvassa 2.3 näkyy miten paketinsuodatus toimii. Kuvan pakettirakenne sisältää seuraavat tarkistukset ja tiedot:

- IP: Tarkistaa lähde- ja kohde-IP-osoitteet
- TCP/UDP: Tarkistaa lähde- ja kohde- porttinumerot. Sisältää myös tiedon käytetystä protokollasta.
- DATA: Paketin varsinainen sisältö



Kuva 2.3: Paketinsuodatuksen toimintaperiaate

Palomuurin kriittinen ominaisuus oli sen tilaton luonne. Aikaisempien pakettien tietoja ei tallennettu. Jokainen paketti käsiteltiin omana tapahtumana. Paketin hyväksyntä tai hylkäys perustui ainoastaan sääntöihin. Tämä oli yksinkertainen, mutta toimiva tapa hallita saapuvaa ja lähtevää verkkoliikennettä. [3]

Yksinkertaisuus aiheutti myös haavoittuvuuksia. Tilaton palomuuri ei ymmärtänyt yhteyden tilaa. Tilattomat palomuurit eivät voineet esimerkiksi varmistaa, että saapuvat paketit kuuluivat olemassa olevaan ja lailliseen yhteyteen. Hyökkääjät kiersivät palomuurit vain muuttamalla liikenteensä portteja ja luomalla tunneleita porttien 80 ja 53 kautta [3], [4].

Toisen sukupolven palomuurit ovat tilallinen pakettisuodatus tai tilallinen palomuuri ja syväpakettitarkistus. Tilallinen palomuuri toimi TCP:n kolmoiskättelyprosessin (eng. threeway handshake) periaatteella [2]. Tilallinen pakettisuodatus erosi tilattomasta siten, että se tarkkaili aktiivisesti yhteyksien tilaa ja määritteli verkkoliikenteen asiayhteyden. Tilallisten palomuurien suunnittelu perustui ajatukseen siitä, että kaikki paketit eivät ole erillisiä yksiköitä vaan, että monet niistä muodostavat osan laajempaa asemien välistä viestintää. Ymmärtämällä yhteyksien asiayhteyden tilalliset palomuurit pystyivät tekemään tietoisempia päätöksiä siitä, mitkä paketit sallitaan ja mitkä estetään. Ne arvioivat paitsi yksittäisiä paketteja myös niiden yhteyttä muihin saman istunnon paketteihin. Tämä oli verrattavissa siihen, että ymmärrettiin yksittäisten lauseiden sijasta koko keskustelun merkitys. [3]

Syväpakettitarkistus taas oli ratkaisu tunnelointiin liittyvissä ongelmissa. Nämä palomuurit kykenivät tunnistamaan yhteyden todellisen protokollan porttivalinnoista riippumatta. Kuitenkaan se ei auttanut uuteen uhkaan: käyttäjät, jotka klikkailivat haitallisia linkkejä ja toivat haittaohjelmia verkkoon. [4]

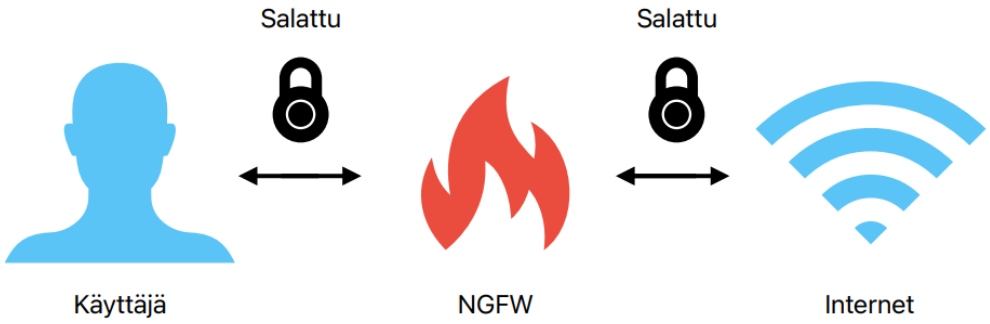
Kolmannen sukupolven palomuurit ovat ensimmäisiä NGFW-palomuureja (eng. Next Generation Firewall). Tämä merkitsi uuden aikakauden alkua verkkotur-

vallisuusteknologiassa. Palomuurit eivät olleet enää vain porttien ja IP-osoitteiden suodattamista, vaan ne pystyivät myös syvempään tarkasteluun [3]. NGFW:llä on kaikki perinteisten palomuurien ominaisuudet, kuten pakettisuodatus, verkko- ja porttiosoitteen muunnos (eng. NAT, network address translation), tilallinen tarkastus ja virtuaalinen erillisverkko (eng. VPN, virtual private network). Lisäksi siinä on edistyneempiä ominaisuuksia, kuten tunkeutumisenestojärjestelmä (eng. IPS, intrusion prevention system), syväpakettitarkastus ja käyttäjätunnistus [2], [5].

NGFW:t erottuivat kyvyllään tunnistaa ja analysoida sovelluksia portista ja protokollasta riippumatta, tarjoten täyden näkyvyyden kaikkiin verkon yli kulkeviin sovelluksiin. Tämä mahdollisti järjestelmänvalvojille kattavien ja tarkkojen turvapolitiikkojen (eng. safety policies) luomisen. Nämä menettelytavat eivät olleet vain verkkoon keskittyneitä, vaan niissä otettiin huomioon liikenteen luonne, mukana olevat sovellukset ja niiden käyttäjät. [3]

Kyvyllä nähdä ja ymmärtää sisältöä NGFW:t lisäsivät uuden ulottuvuuden palomuurin menettelytapoihin, mahdollistaen haitallisen sisällön estämisen ja tukien yrityksen menettelytapoja (eng. policies) tiedonsiirron osalta. Tämä oli erityisen tärkeää aikana, jolloin tietovuodot ja tietomurrot yleistyivät.[3]

NGFW:t pystyivät SSL-salauksen (eng. Secure Sockets Layer) purkuun, jolloin ne pystyivät tarkastamaan salattua liikennettä [6]. Ne myös pystyivät TLS-liikenteen (eng. Transport Layer Security) salauksen purkuun [5]. Palomuuri asettaa itsensä kahden SSL-yhteyden väliin. Jolloin se toimii näiden yhteyksien välityspalvelimena (eng. proxy). Kun käyttäjä haluaa hakea salattua liikennettä, se tekee kyselyn palomuurille, joka taas kysyy internetistä sen omalla salausavaimella halutun salatun liikenteen. Internetistä tulee takaisin salattu viesti, jonka palomuuri purkaa, analysoi, kryptaa (salaa) ja vie sen taas kryptattuna käyttäjälle [6]. Tämä oli hyvin tärkeää, koska ilman sitä salattu liikenne olisi ollut merkittävä sokea alue verkon puolustuksessa [3]. Kuvassa 2.4 näkyy, miten SSL toimii.



Kuva 2.4: SSL/TLS-salauksen purkaminen NGFW:ssä

Kaiken kaikkiaan NGFW:iden kehitys edisti merkittävää siirtymää passiivisista laitteista pois ja käyttämään aktiivisia laitteita. Kun NGFW:stä tuli normi, verkkoturvallisuusjärjestelmät pystyivät suorittamaan syvempää tarkastelua ja tekemään reaaliaikaisia turvapäätöksiä kattavan data-analyysin perusteella. [3]

Neljännen sukupolven palomuurit ovat pilvipohjaisia ja koneoppimista hyödyntäviä [1], [4]. Pilvipalomuuri on palomuuri, joka toteutetaan pilvipalveluiden avulla. Sitä pidetään usein eräänlaisena välityspalvelin-palomuurina, koska pilvipalvelin voi toimia välityspalvelimen tavoin. Välityspalvelin toimii välikätenä käyttäjän ja kohdeverkon välillä, käsitellen ja tarkastaen liikennettä ennen sen välittämistä eteenpäin [7]. Välityspalvelin on välikappale, joka vastaanottaa ja tarkistaa asiakkaan pyynnöt ennen niiden välittämistä eteenpäin. Se toimii suojatun verkon ja ulkopuolisten palveluiden välillä, varmistaen, että liikenne on turvallista ja sallittua [8]. Pilvipalomuurit ovat helposti skaalautuvia, mikä mahdollistaa niiden tehokkaan toiminnan myös kasvavien liikennemäärien myötä. Pilvipohjaisia palomuureja voidaan käyttää tehokkaasti ohjelmistopohjaisissa verkoissa. Ne voidaan hallita vaivattomasti ja ne tarjoavat suojan erilaisia hyökkäyksiä vastaan. [7]

Koneoppimista hyödyntävät palomuurit ovat erityisen tehokkaita tunnistamaan ja suojaamaan tuntemattomia uhkia vastaan. Ne analysoivat verkkoliikenteen käyt-

täytymismalleja ja tunnistavat poikkeavuuksia, jotka voivat viitata uusiin hyökkäyksiin. Näin ne tarjoavat dynaamisen suojamekanismin, joka mukautuu kehittyviin uhkiin ilman, että ne perustuvat pelkästään tunnettuihin uhkakuviin. Lisäksi ne tukevat IoT-laitteiden suojausta luomalla jatkuvaan oppimiseen perustuvia turvallisuuskäytäntöjä, mikä vähentää altistumista uusille uhille. Näiden palomuurien ennakoiva suojausstrategia ja tehokkaat hallintatoiminnot tekevät niistä keskeisiä modernien tietoturvaratkaisujen toteutuksessa.[8]

3 Nykyaikaiset palomuuritekniikat

Tässä luvussa käsitellään nykyaikaisia palomuuritekniikoita, keskittyen erityisesti NGFW:n ominaisuuksiin. Aluksi tarkastellaan NGFW:n ominaisuuksia ja tämän jälkeen Zero Trust -mallia.

3.1 NGFW:n ominaisuudet

NGFW:llä on kolme tärkeää ominaisuutta. Nämä ominaisuudet ovat:

- sovellustietoisuus
- sisällön tarkastus ja heuristinen analyysi
- käyttäjän tunnistus

Perinteiset palomuurit, joita käytiin läpi kappaleessa 2, käyttivät otsikkotietoja, kuten IP-osoitetta, porttinumeroa ja kuljetusprotokollaa, lähettäjän ja paketin tunnistamiseen. Kuitenkin nykyään esiintyy edistyneitä internetuhkia, jotka käyttävät kiertotaktiikoita, kuten porttien vaihtelua (eng. port hopping), epästandardeja portteja (eng. non-standard ports), SSL-salausta ja tunnelointiprotokollia, onnistuen näin ohittamaan perinteiset palomuurit [9]. NGFW pystyy tunnistamaan oikean sovelluksen analysoimalla pakettia otsikkotietojen ulkopuolelta. Perinteiset palomuurit eivät tarkista sisältöä (eng. payload), koska sisältö on suojattu sovellusprotokollalla, kuten HTTPS (eng. hypertext transfer protocol secure). NGFW käyttää TLS-salauksen purkuominaisuutta saadakseen näkyvyyden sovellustason viesteihin. Se

purkaa TLS-yhteyden väliaikaisesti, analysoi sisällön turvallisuusriskejä ja salaa sen uudelleen ennen lähettämistä eteenpäin. Kuvassa 2.4 näkyy tämän toimintaperiaate. [2]

Suurimmalla osalla sovelluksista on tunnetut sovellusallekirjoitukset. Ne ovat ainutlaatuisia transaktiopiirteitä, jotka tunnistavat sovelluksen riippumatta protokollasta ja portista. Kaikki sovellukset, joilla on epäilyttävä allekirjoitus, estetään NGFW:llä, ja sallitut sovellukset tutkitaan tarkemmin. Tällä tavalla voidaan havaita ja käsitellä kiertotaktiikoita, kuten porttien vaihtelua ja epästandardeja portteja. [2]

Lisäksi NGFW:n analysoima sovellus voi olla vain kulissi todelliselle sovellukselle. Toisin sanoen todellinen sovellus käyttää ensimmäistä sovellusprotokollaa tunnelina. Joten, miten NGFW määrittää, kuuluuko sovellusprotokolla todelliselle sovellukselle? Tässä kohtaa sisällön tarkastus ja heuristinen analyysi tulevat hommiin. [2]

Sovelluskerros OSI-mallissa on nykyisin kaikkein haavoittuvaisin ja helpoiten ulkopuolisten hyökkäysten kohteeksi joutuva kerros. Samalla se on myös vaikeimmin puolustettavissa, sillä tämän kerroksen haavoittuvuudet liittyvät usein monimutkaisiin käyttäjän syötetilanteisiin. Yli 70 % verkkohyökkäyksistä kohdistuu sovelluskerrokseen [10]. Siksi sovelluskerroksen suojaus on erittäin tärkeä osa NGFW:tä. Kuten aiemmin mainittiin, NGFW tarkastelee verkkokerrosta ja siirtokerrosta syvemmälle. Se analysoi jokaisen paketin sisällön ja tutkii sovelluksen allekirjoituksen. Tämä riittää estämään useimmat tunnetut hyökkäykset, mutta ei kaikkia. Tässä kohtaa heuristinen (tai käyttäytymiseen perustuva) analyysi astuu mukaan varasuunnitelmana. [2]

Heuristinen analyysi keskittyy monimutkaisiin sovelluksiin, jotka käyttävät tuntemattomia algoritmeja tai omia salausmenetelmiään, kuten vertaisverkkoihin perustuvaa tiedostonjakoa (eng. peer-to-peer file-sharing) tai VoIP-sovelluksia (eng.

Voice over Internet Protocol). Heuristinen analyysi määrittää, onko sovellus haitallinen, tarkkailemalla sen toimintaa. Tyypillisesti heuristinen analyysi käyttää kolmea komponenttia haitallisten sovellusten tunnistamiseen. [2]

Ensimmäinen komponentti on tietojen kerääjä (eng. data collector). Kun sovelluksen protokollasta purettu hyötykuorma on saatu, tietojen kerääjä kerää dynaamisia ja staattisia tietoja suoritettavasta tiedostosta. Toisena tulee tulkki (eng. interpreter), joka muuntaa ensimmäisen komponentin keräämät tiedot välivaiheen esitysmuotoon. Kolmas komponentti, sovittaja (eng. matcher), vertaa näitä välivaiheen esityksiä tietokantaan, joka sisältää tunnettuja haitallisen käyttäytymisen malleja. [2]

Allekirjoituksen tarkastuksen ja heuristisen analyysin lisäksi URL (eng. Uniform Resource Locator)- ja tiedostojen suodatus ovat tehokkaita työkaluja pakettien tarkastuksessa. URL-suodatus estää yhteydet tietyistä verkkotunnuksista. Tiedostojen suodatus puolestaan sallii NGFW:n estää tiedostoja niiden todellisen tyypin perusteella, ei vain tiedostopäätteen mukaan, ja kontrolloida arkaluontoisen datan siirtoa. Yhdistämällä allekirjoitusten tarkastus, heuristinen analyysi sekä URL- ja tiedostosuodatus, sovelluskerrokseen kohdistuvat verkkohyökkäykset voidaan havaita ja torjua. [2]

Viimeisenä ominaisuuksina käymme läpi käyttäjän tunnistuksen. Tilallisen palomuurin tapaan NGFW seuraa liikennevirtoja sekä niiden lähettäjiä ja vastaanottajia. Kuitenkin NGFW vie käyttäjän tunnistuksen askeleen pidemmälle. Sen jälkeen, kun NGFW on saanut peruskäyttäjätiedot paketin otsikosta, kuten määränpään ja lähteen IP-osoitteet ja niiden porttinumerot, se kommunikoi LDAP-hakemistojen (eng. Lightweight Directory Access Protocol), kuten Active Directoryn (AD), kanssa. Active Directory on Microsoftin oma hakemistopalvelu, joka yhdistää käyttäjätiedot käyttäjän IP-osoitteeseen (eng. Internet Protocol). Kommunikoimalla AD:n kanssa NGFW pitää oman käyttäjätaulunsa ajan tasalla vertaamalla sitä säännöl-

lisesti AD:n tietoihin. Kun käyttäjän ja IP-osoitteen välinen yhteys on vahvistettu, NGFW pyytää lisätietoja käyttäjästä, kuten rooli- ja ryhmäjakoja, AD:ltä. Näin NGFW saa selkeyden siitä, kuka vastaa tietyistä paketeista tietoliikennevirrassa, ja mahdollistaa pakettisuodatuksen käyttäjätunnuksen perusteella. [2]

Käyttäjätunnistus on tärkeää verkonvalvojille, sillä se helpottaa vianetsintää ja mahdollistaa nopean reagoinnin hätätilanteissa. NGFW:issä on monia ominaisuuksia, joista kaikkia ei ole tässä tutkielmassa käsitelty.

3.2 Zero Trust -malli

Zero Trust -malli esiteltiin vuonna 2010. Se pyrkii parantamaan verkkojen tietoturvaa kyseenalaistamalla aiemmat oletukset suojatun sisäverkon luotettavuudesta, se ei ole tietty arkkitehtuuri, vaan joukko periaatteita [5], [11]. Perinteisesti palomuureja on käytetty jakamaan verkot luotettuihin ja ei-luotettuihin verkkoihin, mutta Zero Trust -mallissa oletetaan, että sekä ulkoisia että sisäisiä uhkia on aina verkossa [5]. Nykyisten järjestelmien monimutkaisuus ja verkkoyhteyksien tarve vaativat täysin uudenlaista luottamuksen uudelleensuunnittelua jokaisen järjestelmän komponentin ja käyttäjän kohdalla. Zero Trust -malli perustuu siihen, että jokaiselle komponentille suoritetaan jatkuva tunnistus- ja valtuutusprosessi [11]. Zero Trust -verkkojen toteuttaminen edellyttää palomuureilta ja tunkeutumisen havaitsemisjärjestelmiltä kehittyneitä ominaisuuksia [5]. Zero Trust -mallin kehittäminen on tärkeää tietoturvan kannalta, esimerkiksi jos työntekijät käyttävät omia laitteitaan työtehtävissä tai siirtävät työvälineitä kodin ja työpaikan välillä.

Zero Trust -mallin puolustusalueet voidaan jakaa seuraaviin osa-alueisiin:

- Digitaaliset identiteetit
- Päätepisteet ja verkko
- Sovellukset ja tekoälypohjainen kyberturvallisuus

- Infrastruktuuri ja tiedot

Digitaaliset identiteetit suojaavat ja vahvistavat käyttäjätietoja hyödyntämällä vahvaa todennusta [12]. **Päätepisteet** tarjoavat näkyvyyden verkossa käytettäviin laitteisiin ja varmistavat niiden vaatimustenmukaisuuden ja kunnon ennen käyttöoikeuden myöntämistä. **Verkko** puolestaan ei luota laitteisiin tai käyttäjiin ilman tarkistusta, vaan salaa kaiken sisäisen viestinnän, rajoittaa käyttöoikeuksia toimintaperiaatteiden mukaisesti sekä hyödyntää mikrosegmentointia ja reaaliaikaista uhkien havaitsemista. [12]

Sovellukset takaavat asianmukaiset sovelluksensisäiset käyttöoikeudet, avaavat pääsyn reaaliaikaisen analytiikan perusteella sekä valvovat ja hallitsevat käyttäjien toimintaa esimerkiksi tekoälyn avulla. [12]

Infrastruktuuri käyttää telemetriaa hyökkäysten ja poikkeavuuksien tunnistamiseen. Telemetria tarkoittaa tiedonkeruumenetelmää, jossa järjestelmän tai verkon toiminnasta kerätään ja analysoidaan reaaliaikaista tietoa [13]. Lisäksi infrastruktuuri hyödyntää pilvisuojausta, joka tunnistaa ja estää riskialttiit toiminnot automaattisesti. [12]

Lopuksi, **tiedot** suojataan luokittelemalla ne tietojen kontekstin perusteella. Tämä mahdollistaa tietopohjaisen suojauksen, jossa tiedot salataan ja käyttöä rajoitetaan suojauksen ja hallintaperiaatteiden mukaisesti [12]. Suuret yritykset, jotka tarjoavat Zero Trust -mallia voivat erota toisistaan puolustusalueiden suhteen. Esimerkiksi verkkoliikenteen hallinta saattaa puuttua kokonaan tai olla käytössä eri nimellä, kuten Fortinetin tapauksessa [14].

4 Palomuuritekniikoiden ennakoituja kehityssuuntia

Tässä kappaleessa käymme läpi tekoälypohjaisia ja pilvipohjaisia palomuureja. Lopussa käymme läpi palomuurien haasteita ja rajoituksia.

4.1 Tekoälypohjaiset palomuurit

Tekoäly (eng. AI, Artificial Intelligence) on uusi tekninen tieteenala, joka tutkii ja kehittää teorioita, menetelmiä, teknologioita ja sovellusjärjestelmiä, joita käytetään ihmisen älykkyyden jäljittelemiseen, laajentamiseen ja kehittämiseen. Tekoäly on levinnyt lähes kaikille aloille, kuten talouteen, avaruusteknologiaan, automaattiseen säätöön, tietokonesuunnitteluun. Sen sovellukset ovat tuottaneet suuria taloudellisia etuja, mikä on tehokkaasti edistänyt talouden ja yhteiskunnan tieteellistä kehitystä. [15]

Yhä useammat sovellukset altistuvat verkolle internetin kehittyessä. Suurten etujen houkuttelemina kyberhyökkäykset ovat yhä yleisempiä, ja verkon tietoturvatilanne on vakavassa tilassa. Forresterin tutkimuksen mukaan lähes kolmannes vastaajista kertoi kohdanneensa yli kuusi vakavaa tietoturvavälikohtausta kuluneen vuoden aikana. CNCERT torjuu vuosittain yli 100 000 kiristysohjelmahyökkäystä, ja tapauksien määrä on ollut nousussa. Hyökkäyksiin kuuluu monet erilaiset hyökkäysmenetelmät kuten, esimerkiksi verkkourkinta (eng. phising), hakkerointi ja tietojen

varastaminen. [15]

Palomuurien uhkasuojeluteknologia kohtaa vakavia haasteita yhä lisääntyvien ja älykkäämpien verkkohyökkäysten edessä. Nämä haasteet ovat:

- Nopeasti muuttuvat uhkat ovat vaikeita käsitellä
- Moniulotteisia hyökkäyksiä on vaikea käsitellä
- Käyttö- ja kunnossapitotyöt ovat yhä raskaampia

Tekoälypalomuuri käyttää tekoälyteknologiaa verkon uhkien havaitsemiseen, ennustamiseen ja käsittelemiseen. Tekoälypalomuuri eroaa yleisestä palomuurista siten, että sen tavoitteena on havaita tuntemattomia uhkia, mukaan lukien uhan lähde, konteksti, vaaran aste, hyökkäysketju, ennustaa seuraavat hyökkäystoimet ja tehdä vastaavat toimenpiteet näiden tietojen perusteella. [15]

Tekoälypalomuurin älykkyys ei ole pelkästään tietty algoritmi, vaan sopeutuva, automatisoitu ja itse kehittyvä kyky. Tämä ominaisuus voi korvata asiantuntijat, ylittää asiantuntijat monimutkaisissa dataympäristöissä ja toteuttaa tietoturvapuolustuksen nopeammin ja tarkemmin. [15]

Samalla tekoälypalomuuri ei ole vain palomuuri, vaan verkon turvallisuusalusta, joka integroi erilaisia turvallisuuskykyjä, esimerkiksi säännöt, allekirjoitukset, mallit, älykkyys, hyökkäykset ja puolustukset. Se kykenee havaitsemaan uhkia, tunnistamaan niiden vaarat ja lähteet, ennustamaan tarkasti seuraavat toimet, tekemään parhaat päätökset ajallaan ja nopeasti, sekä vastaamaan ja suorittamaan tarvittavat toimenpiteet. [15]

Perinteiseen palomuuriin, joka perustuu määriteltyihin sääntöihin ja allekirjoituksiin, verrattuna tekoälypalomuuri on dataohjattu (eng. data-driven) ja dynaamisempi. Se koulutetaan käyttämällä valtavaa määrää esimerkkidataa koneoppimisen ja syväoppimisen avulla. Tämän vuoksi sillä on vahva yleistämiskyky, ja se pystyy

havaitsemaan uusia uhkia ja haittaohjelmia helpommin ja nopeammin. [15] Tekoälypalomuurilla on seuraavat edut:

Tavallinen palomuuri poimii allekirjoituksia tunnetuista haavoittuvuuksista, kun taas tekoälypalomuuri voi havaita tuntemattomia uhkia ja tunnistaa tunnetut variantit ja tuntemattomat uhkat tarkemmin. [15]

Tavallinen palomuuri voi tarjota vain yksittäistä suojelua, kun taas tekoälypalomuuri voi tehdä tietoyhteistyötä. Se voi tarkemmin tunnistaa ja arvioida uhkia älykkyyden, hyökkäys- ja puolustusosaamisen avulla. Tekoälypohjainen palomuuri on erityisen hyvä lieventämään DDoS-hyökkäyksiä (eng. Distributed Denial-of-Service attack). [15], [16]

Tavallinen palomuuri voi saavuttaa vain sovellustason visualisoinnin, kun taas tekoälypalomuuri voi saavuttaa uhkavision. Se pystyy syvällisemmin ymmärtämään turvallisuustilanteen ja tekemään oikeat toimenpiteet hyökkäysketjun ja APT- organisaation kuvauksen analyysin perusteella. [15]

Lisäksi tekoälypalomuuri voi hyödyntää täysimääräisesti valtavaa dataa, analysoida ja kouluttaa puolustusmallia, päivittää mallia jatkuvasti verkkoiskujen reaaliaikaisen datan perusteella, sopeutua verkkoiskujen uusiin muutoksiin ja ratkaista nykyisin käytössä olevien palomuuritekniikoiden uhkien havaitsemiskyvyn puutteet. [15]

4.2 Pilvipohjaiset palomuurit

Kaksi merkittävää muutosta tietoturvassa heijastavat sitä, että tieto digitalisoituu nopeasti ja pilvilaskenta (eng. cloud computing) yleistyy vauhdilla. Pilvilaskenta on teknologia, joka mahdollistaa tietojen, palveluiden ja sovellusten tallentamisen, käytön ja saatavuuden internetin välityksellä ilman, että käyttäjän tarvitsee omistaa fyysistä infrastruktuuria [17]. Yhä useammat organisaatiot tallentavat tietonsa pilveen ja hyödyntävät sitä suurten tietomassojen käsittelyyn, mikä on hämärtänyt

perinteisen verkon rajoja. Tämä on luonut uudenlaisia haasteita kaikille tietoturva-alalla toimiville sekä digitaalisen ympäristön eheyden turvaamiselle. Perinteisillä tietoturvamekanismeilla, erityisesti perinteisillä palomuureilla, on merkittäviä rajoituksia uusien riskien hallinnassa ja modernien kyberuhkien torjunnassa.[18]

Pilvipalomuuri, kuten nimikin viittaa, toteutetaan pilviteknologian avulla. Pilvipalomuurit toimivat eräänlaisina välityspalomuureina, koska pilvipalvelin voi toimia välityspalvelimena. Pilvipalomuureja on helppo skaalata verkkoliikenteen kasvaessa. [7]

Pilvipalomuuri tarjoaa vahvan suojan pilveen tallennetuille tiedoille ja sovelluksille. Se on erityisen hyvin soveltuva dynaamisiin pilviympäristöihin, joissa verkko-olosuhteet voivat muuttua jatkuvasti [17]. Se estää luvattoman liikenteen pääsyn pilvipohjaisiin järjestelmiin samalla, kun se sallii laillisen liikenteen kulkemisen. Pilvipalomuuri voi olla osa julkista, yksityistä tai hybridipilveä, ja se voi toimia itsenäisesti tai osana laajempaa tietoturvaratkaisua [19].

Pilvipalomuureissa käytetään myös sovellustason suodatusta, joka analysoi verkkoliikennettä syvällisemmin ja estää haitalliset tai epäilyttävät pyynnöt. DDoS-suojaus on olennainen osa pilvipalomuureja, sillä se tunnistaa ja torjuu hajautettuja palvelunestohyökkäyksiä analysoimalla liikennemalleja ja reitittämällä haitallisen liikenteen pois järjestelmästä. Viimeisimpänä, mutta ei vähäisimpänä, pilvipalomuureissa hyödynnetään koneoppimista ja tekoälyä, joiden avulla voidaan tunnistaa ja estää uusia uhkia reaaliaikaisesti. [18], [19].

Pilvipalomuuri analysoi ja suodattaa verkkoliikennettä ennen kuin se saavuttaa pilvi-infrastruktuurin. Se voi sijaita suoraan pilvipalveluntarjoajan infrastruktuurissa, jolloin se toimii osana laajempaa tietoturvaratkaisua. Joissain tapauksissa asiakkaat voivat luoda omia virtuaalipalomuureja, jotka valvovat liikennettä tietyissä verkon osissa. [19].

Pilvipalomuuri tarjoaa monia etuja, kuten skaalautuvuuden, helpon hallinnan ja

kustannustehokkuuden. Se mukautuu automaattisesti liikenteen kasvuun ja laskuun, mikä takaa jatkuvan suojauksen. Keskitetty hallintapaneeli mahdollistaa sääntöjen ja asetusten hallinnan eri sijainneista, ja maksuperusteinen käyttö voi olla edullisempi vaihtoehto kuin fyysisen palomuurin ylläpito. [19].

4.3 Haasteet ja rajoitukset

Palomuurit ovat kehittyneet hyvin paljon lyhyen ajan aikana, mutta niin ovat myös tietoturvan uhat. Vaikka NGFW saattaa puolustaa hyvin kuljetuskerroksessa (eng. layer 4, transport layer), joskus se on puutteellinen kehittyneitä hyökkäyksiä vastaan [14]. Vaikka NGFW tarjoaa tehokasta suojaa sovelluskerroksessa, se rajoittuu vahvasti staattisiin sääntöihin ja allekirjoituksiin. Tämä rajoitus tekee siitä huonomman uusia, tuntemattomia uhkia vastaan, koska se ei ole yhtä dynaaminen kuin, esimerkiksi tekoälypohjaiset järjestelmät.

Myös pilvipohjaisissa palomuuriympäristöissä on havaittu haavoittuvuuksia. Hakanin tekemässä tutkimuksessa [20] huomattiin, että pilvipalveluinfrastruktuuri tallentaa ja siirtää arkaluonteista tietoa internetin kautta, usein monien eri sovellusten kautta. Tämä tekee perinteisistä pakettitasoisista palomuureista tehottomia monimutkaisia hyökkäyksiä vastaan.

Yksi pilviympäristöjen suurimmista haasteista on niiden dynaamisuus, sillä työkuormat eivät ole vakioita ja verkkorakenteet voivat vaihdella. Perinteiset palomuurit eivät kykene tarjoamaan riittävää suojaa pilvi-infrastruktuureille, koska uhkavektorit kasvavat jatkuvasti. Tietoturvaratkaisujen onkin oltava joustavia, helposti saatavilla ja vähän resursseja kuluttavia, jotta ne vastaavat organisaatioiden pilvipohjaisten toimintojen yleistymiseen. [18]

Tekoälypohjaisissa palomuureissa haavoittuvuudet ja haasteet liittyvät koneoppimisen ja syväoppimisen käyttöön uusien uhkien dynaamiseen tunnistamiseen sekä jatkuvaan oppimiseen ja poikkeamien havaitsemiseen [14]. Tekoälypohjaisten palo-

muurien heikkoutena tai rajoituksena on tarve parantaa tekoälypäätösten tulkittavuutta ja läpinäkyvyyttä. Kehityskohteina on skaalaavuus, joustavuus ja luotettavuus.

5 Yhteenveto

Tutkielmassa tarkasteltiin palomuurien kehitystä, nykyisiä teknologioita ja tulevaisuuden suuntauksia. Ensimmäinen tutkimuskysymys käsitteli palomuuritekniikan kehitystä ja nykyaikaisimpia tekniikoita. Palomuurit ovat kehittyneet perinteisistä paketinsuodatukseen perustuvista ratkaisuista kohti seuraavan sukupolven palomuureja, jotka hyödyntävät syväpakettitarkistusta (DPI), sovellustietoisuutta ja käyttäjätunnistusta. Lisäksi Zero Trust -malli on yleistynyt, sillä se edellyttää jokaisen verkkoon liittyvän laitteen ja käyttäjän jatkuvaa tunnistamista ja valvontaa. Palomuurit ovat kehittyneet hyvin paljon, kun miettii, että ensimmäinen palomuuri vain suodatti paketteja.

Toinen tutkimuskysymys käsitteli palomuurien tulevaisuuden kehityssuuntia ja tekoälyn roolia niissä. Tekoälypohjaiset palomuurit mahdollistavat entistä dynaamisemman uhkien tunnistamisen, sillä ne kykenevät oppimaan ja mukautumaan uusiin hyökkäystapoihin ilman, että ne perustuvat pelkästään staattisiin sääntöihin. Pilvipohjaiset palomuurit puolestaan tarjoavat joustavuutta ja skaalautuvuutta, mikä tekee niistä erityisen tehokkaita hajautetuissa verkkoympäristöissä. Toisin sanoen tekoälyn osuus tulevaisuuden palomuureissa on keskeinen.

Palomuurien kehitys on reaktio kyberuhkien jatkuvaan muutokseen ja kehitykseen. Vaikka uudet teknologiat, kuten NGFW, tekoäly ja pilvipalvelut, tarjoavat entistä parempia suojautumiskeinoja, ne tuovat mukanaan myös haasteita, kuten tarvetta kehittää tekoälymallien läpinäkyvyyttä ja varmistaa pilvipalveluiden tieto-

turva. Kyberuhat ja tekoälypohjaiset suojaukset käyvät jatkuvaa kilpajuoksua, jossa hyökkäystavat kehittyvät ja puolustusmekanismit mukautuvat niitä torjumaan. Tulevaisuudessa todennäköisesti tullaan käyttämään enemmän tekoälyä tekoälyhyökkäyksiä vastaan, tekoäly vs tekoäly.

Yhteenvetona voidaan todeta, että palomuurit ovat edelleen keskeinen osa verkkoturvallisuutta, ja niiden kehitys jatkuu yhä monimutkaisempien uhkien torjumiseksi. Hyökkäykset kehittyvät jatkuvasti, joten myös palomuuritekniikoiden on kehityttävä.

Lähdeluettelo

[1] Palo Alto Networks. ”What is a firewall? | firewall definition”, Palo Alto Networks. (2024), url: https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall (viitattu 15. 10. 2024).

[2] J. Liang ja Y. Kim, ”Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall”, teoksessa *Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, tammikuu 2022, s. 0752–0759. DOI: 10.1109/CCWC54503.2022.9720435.

[3] Palo Alto Networks. ”The History of Firewalls | Who Invented the Firewall?”, Palo Alto Networks. (2024), url: https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls (viitattu 15. 10. 2024).

[4] D. Holmes, *FW4: The Fourth Generation Of Firewalls*, en-US, huhtikuu 2020. url: https://www.forrester.com/blogs/fw4-the-fourth-generation-of-firewalls/.

[5] J. Heino, A. Hakkala ja S. Virtanen, ”Study of methods for endpoint aware inspection in a next generation firewall”, *Cybersecurity*, vol. 5, nro 1, s. 25, syyskuu 2022, ISSN: 2523-3246. url: https://doi.org/10.1186/s42400-022-00127-8.

[6] ”More on SSL decryption”. yhteistyössä Palo Alto Networks. Section: Community Blogs. (7. elokuuta 2020), url: https://live.paloaltonetworks.com/t5/community-blogs/more-on-ssl-decryption/ba-p/342598.

[7] P. P. Mukkamala ja S. Rajendran, ”A survey on the different firewall technologies”, *International Journal of Engineering Applied Sciences and Technology*, vol. 5, nro 1, s. 363–365, 31. toukokuuta 2020, ISSN: 24552143. DOI: 10.33564/IJEAST.2020.v05i01.059.

[8] The Open University. ”Network security”, Open Learning. (17. maaliskuuta 2016), url: https://www.open.edu/openlearn/digital-computing/network-security/content-section-9.5.

[9] M. Keil. ”Balancing the risks and benefits of evasive applications”, Palo Alto Networks Blog. (8. syyskuuta 2009), url: https://www.paloaltonetworks.com/blog/2009/09/controlling-evasive-applications/.

[10] R. Koch, ”Towards Next-Generation Intrusion Detection”, teoksessa *Proceedings of the 2011 3rd International Conference on Cyber Conflict*, Tallinn, Estonia, kesäkuu 2011, s. 1–18.

[11] C. Zanasi, F. Magnanini, S. Russo ja M. Colajanni, ”A Zero Trust approach for the cybersecurity of Industrial Control Systems”, teoksessa *2022 IEEE 21st International Symposium on Network Computing and Applications (NCA)*, ISSN: 2643-7929, vol. 21, Boston, MA, USA, joulukuu 2022, s. 1–7. DOI: 10.1109/NCA57778.2022.10013559.

[12] Microsoft. ”Zero Trust -suojausmalli – Moderni suojausarkkitehtuuri | Microsoft Security”. (12. huhtikuuta 2024), url: https://www.microsoft.com/fi-fi/security/business/zero-trust.

[13] L. Tan, W. Su, W. Zhang, J. Lv, Z. Zhang, J. Miao, X. Liu ja N. Li, ”In-band network telemetry: A survey”, *Computer Networks*, vol. 186, s. 107 763,

helmikuu 2021, ISSN: 13891286. DOI: 10.1016/j.comnet.2020.107763. url: https://linkinghub.elsevier.com/retrieve/pii/S1389128620313396.

[14] T. Sarkorn ja K. Chimmanee, "Review on Zero Trust Architecture Apply In Enterprise Next Generation Firewall", teoksessa *2024 8th International Conference on Information Technology (InCIT)*, Chonburi, Thailand, marraskuu 2024, s. 255–260. DOI: 10.1109/InCIT63192.2024.10810611.

[15] Z. Wang, "Research on Feature and Architecture Design of AI Firewall", teoksessa *2021 5th Annual International Conference on Data Science and Business Analytics (ICDSBA)*, Changsha, China, syyskuu 2021, s. 75–78. DOI: 10.1109/ICDSBA53075.2021.00024.

[16] I. Hasanov, S. Virtanen, A. Hakkala ja J. Isoaho, "Application of Large Language Models in Cybersecurity: A Systematic Literature Review", *IEEE Access*, vol. 12, s. 176 751–176 778, 2024, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2024.3505983.

[17] W. J. Wisesa, H. H. Nuha ja R. G. Utomo, "Implementation of Network Security Using a Cloud Computing-Based Firewall on the PukulEnam Company Website", teoksessa *Proceedings of the 2023 3rd International Conference on Intelligent Cybernetics Technology Applications (ICICyTA)*, Denpasar, Bali, Indonesia, joulukuu 2023, s. 432–437. DOI: 10.1109/ICICyTA60173.2023.10428860.

[18] H. Sharma, "Next-generation firewall in the cloud: Advanced firewall solutions to the cloud", *Journal of Emerging Technologies and Applications (JETA)*, vol. 1, nro 1, s. 99–111, 2021. DOI: 10.56472/25832646/JETA-V1I1P112.

[19] G. H. Carvalho, I. Woungang ja A. Anpalagan, "Cloud Firewall Under Bursty and Correlated Data Traffic: A Theoretical Analysis", *IEEE Transactions on*

Cloud Computing, vol. 10, nro 3, s. 1620–1633, heinäkuu 2022. DOI: 10.1109/TCC.2020.3000674.

[20] D. Hakani, "A Survey on Firewall for cloud security with Anomaly detection in Firewall Policy", teoksessa *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, Greater Noida, India, tammikuu 2023, s. 825–830. DOI: 10.1109/AISC56616.2023.10085419.