Harri Rantala

Next generation -palomuurin tarkastelu ja konfigurointi

Opinnäytetyö
Kevät 2016
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikan koulutusohjelma

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Harri Rantala

Työn nimi: Next generation -palomuurin tarkastelu ja konfigurointi

Ohjaaja: Alpo Anttonen

Vuosi: 2016 Sivumäärä:40

Tässä opinnäytetyössä käydään läpi tietoturvan ja tiedonsiirron perusteet sekä käsitellään ensimmäisen sukupolven palomuureja. Lisäksi työssä syvennytään next generation -palomuurin ratkaisuihin ulkoverkon uhkia vastaan ja tiedon siirtoon salatusti ulkoverkon yli. Työn loppu puolella tarkastellaan laitepalomuurin perusasetuksien konfigurointi tekstipohjaisella käyttöliittymällä.

Avainsanat: palomuuri, tietoturva, IPS, VPN.

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Networking Technology

Author: Harri Rantala

Title of thesis: Consideration and configuration of next-generation firewall

Supervisor: Alpo Anttonen

Year: 2016 Number of pages: 40

This thesis focused in the fundamentals of information security and data transfer. Also the first generation of firewalls was presented. The next-generation firewall solutions with external network threats and encrypted data transfer over the Internet were studied in depth. At the end the configuration of the basic settings of a firewall with a text-based user interface was introduced.

Keywords: firewall, information security, IPS, VPN, next-generation firewall.

SISÄLTÖ

Kuva- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

3DES	Triple Data Encryption Standard.
AES	Advance Encryption Standard.
AET	Advance Evasion Technique, vapaa suomennos kehittänyt kiertojärjestelmä. Tietoverkkoon tunkeutuminen kehittyneemmillä tavoilla joita IPS ei havaitse.
DDoS	Distributed Denial of Service, hajautettu palvelunenestohyökkäys.
DES	Data Encryption Standard.
DoS	Denial of Service, palvelunestohyökkäys.
FAILOVER	Tekniikka, jossa varalaite aktivoituu, kun päälaite vikaantuu.
GRE	Generic Record Examinations.
IDS	Intrusion Detection Systems, suomeksi tunkeutumisen havaitsemisjärjestelmä.
IP	TCP/IP-mallin internet-kerroksen protokolla.
IPS	Intrusion Prevention Systems, suomeksi tunkeutumisen estäjärjestelmä.
IPsec	Internet Protocol Security.
IPX	Internetwork Packet Exchange
L2F	Layer 2 Forwarding.
L2TP	Layer 2 Tunneling Protocol.

NAT	Network Address Translation, osoitteenmuunnostekniikka, jossa sisäverkon osoite käännetään ulkoverkoon sopivaksi osoitteeksi.
NetBeui	Network Basics Input/Output System.
OSI	Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PPTP	Point-to-Point Tunneling Protocol.
PuTTY	Telnet- ja SSH-asiakasohjelma ja pääte-emulaattori.
SSH	Secure Shell on salattuun tietoliikenteeseen tarkoitettu protokolla. Yleisin SSH:n käyttötapa on ottaa etäyhteys SSH-asiakasohjelmalla SSH-palvelimeen, jotta päästään käyttämään toista konetta merkkipohjaisen konsolin kautta.
SSL	Secure Sockets Layer, on salausprotokolla, jolla voidaan suojata internet-sovellusten tietoliikenne IP-verkkojen yli.
SYN	Transmission Control Protocol.
TCP	Tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille, joilla on pääsy internettiin.
TCP/IP	Tarkoittaa usean internetliikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmää.
Tunnelointi	VPN-tekniikassa käytetty protokolla, joka salaa IP-paketin niin että siitä ei ole luottavissa kuin vastaanottajan osoite.
UDP	Yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron.
VPN	Virtual Private Network, on tapa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

1 JOHDANTO

1.1 Työn tausta

Tämä opinnäytetyö tehtiin osana Seinäjoen Ammattikorkeakoulun toimeksiantoa. Projektina oli tietoliikennetekniikan luokan palomuurin konfigurointi. Tietotekniikan luokka toimii tietoliikennelaboratoriona, jokaisessa tietokoneyksikössä on kaksi verkkokorttia. Perusopetuksessa toinen verkkokortti on liitetty Seinäjoen ammattikorkeakoulun sisäverkkoon ja sitä kautta ulkoverkkoon. Toisella verkkokortilla voisi liittyä suoraan ulkoverkkoon, näin voidaan demonstroida tai testata eri tietoliikenteeseen liittyviä tehtäviä tai opetusta, ilman liittymistä SeAMK:in sisäverkkoa, näin luokasta pääsisi suoraa liittymään ulkoverkkoon ilman sisäverkolle asetettuja palomuurisääntöjä.

1.2 Työn tavoite

Työn tavoitteena oli konfiguroida SeAMK:in tarjoamaan palomuuriin perusasetukset. Perusasetuksilla päästään sisäverkosta ulkoverkkoon ja ulkoverkosta sisäverkon palvelimelle. Koska palomuuri on tietoturva- ja verkkolaite tarkastellaan opinnäytetyössä tietoturvaa, tietoliikennettä ja ulkoverkon tietoturvauhkia.

1.3 Työn rakenne

Johdannon jälkeen käsitellään Tietoturvan perusteita ja muutamia tietoturvauhkia. Kolmannessa kappaleessa käydään tietoliikenteen perusteet. Neljännessä kappaleessa luetellaan ensimmäisen sukupolven palomuurit. Viidennessä kappaleessa tarkastellaan tietoturvauhkien torjuntaa ja ratkaisuja esim. tietoliikenteen salaamista ulkoverkossa. Kuudennessa kappaleessa tarkastellaan konfiguroitavan palomuurin ominaisuudet. Mitkä perusasetukset asetetaan, testaus ja päätelmät.

2 TIETOTURVA

2.1 Tietoturvallisuus

Tietoturva kattaa kolme pääasiallista näkökohtaa: luottamuksellisuus, saatavuus ja eheys. Tietoturvallisuuden tavoitteena on varmistaa liiketoiminnan kestävä menestys ja jatkuvuus sekä pitää haittavaikutukset mahdollisemman vähäisinä. Se pitää sisällään asianmukaisen turvamekanismin soveltamisen ja hallitsemisen. Tähän sisältyy monien erilaisten uhkien huomioon ottamien. (ISO 27000 2010, 12.)

Tietoturvallisuus saavutetaan toteuttamalla soveltuva joukko turvamekanismeja, jotka on valittu riskien hallintaprosessin avulla ja hallitaan toteuttamalla tietoturvaan soveltuva hallintajärjestelmä. Järjestelmään sisältyy prosesseja, menettelyjä, organisaatiorakenteita, ohjelmistoja ja laitteistoja, näillä suojataan tunnistettua tietoomaisuutta. Nämä turvamekanismit tulee määritellä ja ottaa käyttöön ja niitä tulee valvoa, katselmoida ja tarvittaessa parantaa, jotta organisaation määrittelemien turvallisuus- ja liiketoimintatavoitteiden saavuttaminen varmistetaan. Asianmukaisten tietoturvallisuuteen liittyvien turvamekanismien odotetaan olevan saumattomasti yhdistetty organisaation liiketoimintaprosesseihin. (ISO 27000 2010, 12.)

2.1.1 Luottamuksellisuus

Jos tieto on luokiteltu tai muuten salassa pidettävää, sen voivat saada käyttöön vain sellaiset tahot, jolla on tiedonsaanti- ja käyttöoikeus siihen. Tietojärjestelmissä luottamuksellisuus toteutetaan normaalisti käyttöoikeuksien hallinnalla; käyttäjälle annetaan sekä vapaa-ajalla käytettäviin että työtehtävissä käytössä oleviin järjestelmiin sellaiset oikeudet, jotka ovat tarpeen tehtävien hoitamisen kannalta. (Rousku 2014, 48.)

2.1.2 Eheys

Tiedon eheydellä tarkoitetaan, että tieto ei saa muuttua hallitsemattomasti. Työtehtävissä tämä tarkoittaa sitä, että tietoa saavat muuttaa vain sellaiset käyttäjät, joilla on siihen tarvittava käyttöoikeus ja vain sallituilla keinoilla. Turvallisuuden näkökulmasta esimerkiksi henkilö-, väestö-, potilashenkilötiedot, julkishallinnon johtamisessa tarvittavat järjestelmät, pankkijärjestelmät, verotus, maanomistus, kiinteistötiedot sekä vakuutustiedot ovat sellaisia järjestelmiä ja tietoja, jotka eivät saa muuttua hallitsemattomasti ja joiden pitää kaikissa olosuhteissa olla palautettavissa. (Rousku 2014, 49.)

2.1.3 Saatavuus

Tietojen ja palveluiden saatavuus liittyy tietojärjestelmien toiminnan turvaamiseen. Verkkoyhteyksien pitää toimia ja palvelimien pitää olla toiminnassa, aina silloin kuin tietoa halutaan käyttää. Esimerkiksi internetissä toimivien palveluiden pitää olla saavutettavissa, mihin vuorokaudenaikaan tahansa. (Järvinen 2002. 24)

2.2 Tietoverkkorikollisuus

Tietoverkkorikollisuus on tietoliikenteen, tietokoneiden, tietojärjestelmien sekä näihin kytkettyjen oheislaitteiden ja tietoverkkojen tarjoamien palveluiden häiritsemistä tai niiden hyväksikäytöllä saatua taloudellista tai muuta hyötyä. Tämä toteutetaan murtautumalla, muuttamalla tai häiritsemällä tietoliikennettä. Toiminta voi kohdistua yksittäiseen henkilöön, yritykseen, yhteisöön tai valtioon (Kuusimäki 2009).

2.2.1 Identiteettivarkaus

Identiteettivarkaudella rikollinen pyrkii esim. samaan haltuunsa yrityksen rahaliikennettä joko esiintymällä yrityksen jäsenenä tai jonkun toisen yrityksen luotettavana henkilönä ja tekaisemalla perättömiä saatavia (Kuusimäki 2009).

Konecranesin ulkomainen tytäryhtiö joutui petoksen uhriksi. Rikoksen tekijät saivat identiteettivarkautta hyödyntämällä ja muilla petostoimilla yrityksen suorittamaan maksuja noin 17,2 miljoonalla eurolla. (Eskola 2015.)

2.2.2 Yritys- ja tietosalaisuuksiin kohdistuvat hyökkäykset

Tieto on elinkeinoelämän keskeinen tekijä. Yrityksen tiedosta ovat kiinnostuneet muut yritykset tai yritysvakoojat. Yritysvakoojat voivat myydä tietonsa ja näin vahingoittaa yritystoimintaa. Yrityksellä voi olla arkistoituna, rahaksi muunnettavaa tietoa, kuten asiakkaisen luottokorttitietoja. (Kuusimäki 2009.)

Yhdysvaltalaisen turvallisuusyhtiö Stratforin järjestelmään murtauduttiin ja viettiin tuhansien ihmisten asiakas- ja luottokorttitietoja. Tietomurron ilmoitti tehneensä Anonymous hakkeriryhmä, joka todisteeksi julkaisi yli 17000 henkilön luottokorttitiedot. (Vaalisto 2011.)

2.3 National Seucurity Agency

NSA on yhdysvaltalainen signaalitiedusteluun keskittyvä valtiohallinnon virasto. Se toimii Yhdysvaltojen puolustusministeriön alaisuudessa. NSA toimii vain sähköisissä ympäristöissä, käytännössä se toimii kyberympäristöissä etsien keinoja suojata ja puolustaa maan kasallisia tietojärjestelmiä ja tietoja. Lisäksi kerää ja tuottaa tietoja ulkomaalaisista tiedustelulähteistä. Tavoitteiden toteuttaminen edellyttää, että NSA kehittää keinoja, joilla se pystyy murtamaan muiden valtioiden tai organisaatioiden suojauskeinona. NSA:ssa työskentelee arviolta 40 000 henkilöä. Mukana on huippumatemaatikkoja ja salausalgoritmien parhaita asiantuntijoita. Entinen NSA työntekijä Edward Snowden paljasti että NSA pystyy katselemaan ja kuuntelemaan mitä tahansa sähköpostiviestejä, puhelinkeskusteluita, www-selaimen selaushistorioita ja Word-asiakirjoja, siihen ei tarvita tuomioistuimen eikä esimiehen lupaa. (Rousku 2015, 82,97.)

2.4 Ruotsin signaalitiedustelu

Ruotsin sotilastiedustelu saa seurata kaikkea internet liikennettä, joka Ruotsin verkossa liikkuu. Tiedustelu saa siis seurata kaiken dataliikenteen mikä siirtyy Suomesta Eurooppaan Ruotsin kautta. (Salminen 2009.)

2.5 Yrityksen tietoturva

Tieto on yrityksen keskeinen voimavara ja menestystekijä. Siksi tieto on myös suojattava samalla tavalla kuin yrityksen fyysistä omaisuutta, työntekijöitä tai brändiä. Huonosti hoidettu tietoturva voi kostautua vahingonkorvauksina ja sopimussakkoina. Lähes kaikki tietoturvaa parantavat toimet ovat työntekijöiden kannalta epämukavia ja lisäävät työtä. Ohjeiden laatiminen jää usein IT-osaston vastuulle, vaikka tietoturvasta huolehtiminen on yrityksen johdon vastuu. (Järvinen 2002. 111)

2.5.1 Johdon tehtävä

Johdon tulisi hyväksyä tietoturvapolitiikka, määrätä turvatehtävät ja koordinoida ja katselmoida turvallisuuden toteutus koko organisaatiossa. Tarvittaessa tulisi organisaation käyttöön hankkia tietoturvallisuuden asiantuntija-apua. Apua tulisi käyttää, jotta pysyttäisiin perillä alan kehityksestä, standardeista ja arviomenetelmistä, jotta saataisiin hyvä yhteistyö tietoturvahäiriöiden käsittelemiseksi. Johdon tulisi edellyttää, että työntekijät, yhteistyökumppanit ja ulkopuoliset käyttäjät noudattavat turvallisuutta organisaatioon luotujen periaatteiden ja menettelytapojen mukaisesti. (ISO 27002 2006, 17,31.)

2.5.2 Yrityksen tietoturvaa käsitteleviä lukuja

Yrityksissä heikoimmin on hoidettu henkilöstön tietoturvakoulutus, yhteistyökumppanien tietoturvan tason varmistaminen ja ohjeistus paikasta riippumattoman työn tietoturvasta. Henkilöstön tietoturvakoulutus on järjestelmällistä vain 13 prosentissa

yrityksistä. Jos satunnaiset koulutukset lasketaan mukaan, luku nousee noin 50 prosenttiin. Lähes 40 prosenttia yrittäjistä ei varmista yhteistyökumppanin tietoturvan tasoa. Tutkimukseen vastanneista kolme prosenttia tiesi joutuneensa tietomurron kohteeksi. Epävarmojen osuus on 13 prosenttia. Tietomurron uhreja voi olla Suomessa tuhansia. Parhaiten yrittäjät ovat hoitaneet virustorjunnan ja palomuurit. Vastaajista 96 prosenttia sanoo, että tietokoneiden virustorjuntaa seurataan joko järjestelmällisesti tai satunnaisesti. Vastaavasti palomuuri oli hankittuna 94 prosentilla vastanneista. (Koivikko 2015.)

2.5.3 Koulutus

Parhain tapa ehkäistä sisäisiä tietoturva rikkomuksia lienee koulutus, jatkuvaan koulutukseen tulisi sisältyä turvallisuusvaatimukset, lailliset liiketoiminnan turvamekanismit sekä tietojenkäsittelypalveluiden oikealainen käyttö. Koulutustoimien tulisi olla sopivia ja olennaisia henkilön rooliin vastuiden ja taitojen kannalta. Niihin tulisi sisältyä tietoa tunnetuista uhkista ja luoda yhteishenkilö, jolta voi pyytää lisätietoa turvallisuutta koskevissa asioissa. (ISO 27002 2006, 3.)

3 TIETOLIIKENTEEN PERUSTEET

3.1 OSI-malli

Vuonna 1977 luotiin OSI-malli, jonka tarkoituksena oli luoda tietoliikenteen toimintamalli. Tämä viitemalli muodosti perustan sille, miten tietokoneita liitettään toisiinsa hajautetuissa tietojärjestelmässä. Tavoitteena oli aikaansaada arkkitehtuuri, jossa tietoliikennejärjestelmät jaettiin kerroksiin. Kerrosten määrittelyssä käytettiin seuraavia lähtökohtia:

1. Rajoitetaan kerrosten lukumäärä siten, että niiden kuvaaminen ja integrointi on mahdollisemman yksinkertainen.
2. Muodostetaan kerrosten väliset rajapinnat sellaisiin kohtiin, joissa kerrosten väliset yhteydet ovat minimissään.
3. Sijoitetaan eri kerroksiin sellaiset aiheet, joiden tekniikka poikkeaa toisistaan.
4. Yhdistetään samanlaiset toiminnot samaan kerrokseen,
5. Mahdollistetaan muutokset kerroksiin ilman, että ne vaikuttavat alapuolella ja yläpuolella oleviin kerrosiin.
6. Muodostetaan kerrosten rajapinnat siten, että kerros liittyy vain ja ainoastaan ylä- ja alapuolella oleviin kerroksiin. (Comer 2002, 181.)

3.1.1 OSI-kerrosarkkitehtuuri

OSI-kerrosarkkitehtuuri laadittiin edellä mainittujen seikkojen perusteella ja tuloksena syntyi 7-tasoinen malli, jota lähes kaikki noudattavat edelleen.

OSI-viitemallin kerrokset ovat seuraavat:

1. Fyysinen kerros määrittelee siirtoyhteyden mekaaniset, fyysiset ja toiminnalliset mallit.
2. Siirtoyhteyskerroksen tehtävä on huolehtia virheettömästä yhteydestä kahden pisteen välillä verkossa.

3. Verkkokerroksen tehtävänä on tarjota ylemmille kerroksille verkon yli sellaisia siirtoyhteyksiä, jotka eivät ota kantaa alla olevan verkon rakenteeseen tai kytkentätekniikkaan.
4. Kuljetuskerroksen tehtävänä on tarjota luotettava tiedonsiirtoyhteys kahden päätepisteen välillä.
5. Istuntokerroksen tehtävä on huolehtia sovellusten välisistä ohjaustoiminnoistaa.
6. Esitystapakerros on kerros, jossa sovitaan yhteisen tiedon esitystavasta päätelaitteiden välille.
7. Sovelluskerros tarjoaa sovellukselle rajapinnan OSI-järjestelmään. (Granlund 2003, 9.)

3.2 TCP/IP

Toinen tärkeä kerrosmalli ei ole standardikomitean laatima, se on tulos tutkimuksesta, joka johti TCP/IP-protokollaperheen syntymiseen. TCP/IP-kerrosmalli voidaan helposti kuvata myös ISO-mallin avulla. Mutta niissä on niin paljon eroja, että eri mallien käyttäminen on perusteltua. TCP/IP-ohjelmisto käsittää viisi kerrosta. Alimmaisella on laitetason kerros, jonka päällä neljä ohjelmakerrosta. (Comer 2002, 183.) Kerrokset ja niiden välillä siirrettävien tietojen muoto on esitettynä taulukossa 1.

Taulukko 1. TCP/IP-kerrosmalli

Sovellu
Kuljetus
Internet
Verkkoliitäntä

Sovelluskerros. Käyttäjät käynnistävät ylimmällä tasolla sovelluksia, jotka käyttävät hyväkseen TCP/IP-yhteisverkon palveluita

Kuljetuskerros. Kerroksen tärkein tehtävä on siirtää tietoja kahden sovelluksen välillä.

Internet-kerros. Kerros hoitaa laitteiden välisen kommunikoinnin. Se vastaanottaa kuljetuskerroksesta paketin lähettämispyynnön ja vastaanottavan tietokoneen osoitteen. Se kapseloi IP-paketin, lisää otsikkotiedot ja määrittää reititysalgoritmin avulla, onko IP-paketti lähetettävä reitittimelle vai suoraan vastaanottajalle.

Verkkokerros. TCP/IP-ohjelmiston alin kerros on verkkokerros, jonka tehtävänä on vastaanottaa verkosta tulevat IP-paketit ja siirtää lähetettävät paketit oikeaan verkkoon. (Comer 2002, 183,184.)

3.3 IP-protokolla

Protokolla, joka määrittää epäluotettavan ja yhteydettömän kuljetusmenetelmän. On nimeltään internet protokolla, tavallisesti kutsuttuna IP. IP määrittää kolme tärkeää asiaa. Ensiksi se määrittää TCP/IP-verkossa tapahtuvan kuljetuksen. Toiseksi IP-ohjelmat suorittavat reititystoiminnot eli valitsevat reitin, jota pitkin tiedot kulkevat. Kolmanneksi IP sisältää joukon sääntöjä, jotka määrittävät epäluotettavan paketin kuljetuksen perusteet. (Comer 2002, 97.)

3.4 TCP-protokolla

Vaikka TCP-protokolla esitellään osana TCP/IP-protokollaperhettä, se on itsenäinen, yleiskäyttöinen protokolla, joka voidaan sovittaa myös muihin kuljetusjärjestelmiin. Koska TCP asettaa vain vähän erityisvaatimuksia käytettävälle verkolle, sitä voidaan käyttää esim. Ethernetissä yhtä hyvin kuin monimutkaisissa yhteisverkoissa. (Comer 2002, 215.)

TCP on protokolla, joka määrittää kahden tietokoneen toisilleen lähettämän datan ja kuittausten muodon ja toiminnan, jota käyttämällä tietokoneet varmistavat, että tiedot on kuljetettu oikein. Se määrittää kuinka samassa tietokoneessa olevat eri kohteet erotetaan toisistaan ja kuinka selvitetään virhetilanteet. (Comer 2002, 215.)

Taulukko 2. TCP/IP-kerrosrakenne

Sovellus
TCP-protokolla
Internet (IP)
Verkkoyhteys

3.4.1 TCP-segmentin rakenne

TCP-ohjelmistojen lähettämiä siirtoyksiköitä kutsutaan segmenteiksi. Segmenttejä lähettämällä muodostetaan ja puretaan yhteyden sekä kuljetetaan dataa, kuittaukset ja ikkunan kokoa koskevat ilmoitukset. (Comer 2002, 221.) TCP-segmentin rakenne on esitetty taulukossa 3.

Taulukko 3. TCP-segmentin rakenne

<table>
<tr><td colspan="3">Lähdeportti</td><td>Kohdeportti</td></tr>
<tr><td colspan="4">Järjestysnumero</td></tr>
<tr><td colspan="4">Kuittausnumero</td></tr>
<tr><td>Otspit</td><td>Varattu</td><td>Koodibitit</td><td>Ikkuna</td></tr>
<tr><td colspan="3">Tarkistussumma</td><td>Urgent-osoitin</td></tr>
<tr><td colspan="3">Optiot</td><td>Täyttö</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Segmentit käsittävät kaksi osaa: otsikon ja data-osan. Otsikko, jota kutsutaan TCP-otsikoksi, sisältää tunniste-ja ohjaustiedot. Lähdeportti- ja Kohdeportti-kentät sisältävät TCP-porttiosoitteet, joilla tunnistetaan yhteyden päissä olevat sovellusohjel-

mat. Järjestysnumero-kenttä ilmaisee segmentin sisältämän datan paikan lähettäjän tavuvirrassa. Numero-kenttä sisältää sen oktetin numeron, jota lähettäjä odottaa ennen seuraavan segmentin lähettämistä. Otspit-kenttä sisältää kokonaisluvun, joka ilmaisee segmentin otsikon pituuden 32-bittisinä lohkoina. Optiot-kentän pituus vaihtelee sen mukaan, mitä optiota on määritetty. Varattu kenttä on tulevaa käyttöä varten. Koodibitit-kentän kuusi bittiä määrittävät, kuinka otsikon muut kentät tulee tulkita. Ikkuna-kenttään tulee arvo, joka määrittää paljonko dataa lähettäjä saa lähettää. (Comer 2002, 221.)

3.5 UDP-protokolla

UPD-protokolla tarjoaa tärkeimmät toiminnot, joita käyttämällä sovellukset voivat lähettää tietosähkeitä toisilleen. UDP-protokolla tarjoaa epäluotettavan yhteydettömän kuljetuspalvelun. Se sitoo sanomat tietokoneiden välillä IP-protokollaa käyttäen, mutta tarjoaa lisäksi menetelmät, joilla tietokoneessa olevat kohteet erotetaan toisistaan. Se ei lähetä kuittauksia saapuneista tietosähkeistä ja eikä lajittele saapuvien sanomien järjestystä. (Comer 2002, 198.)

3.5.1 Sanoman rakenne

UDP-sanomia kutsutaan tietosähkeiksi. Käsitteellisesti käyttäjän tietosähke käsittää kaksi osaa: otsikon ja data-alueen. (Comer 2002, 199.) Taulukossa 4 on kuvattu UDP-sanoman rakenne.

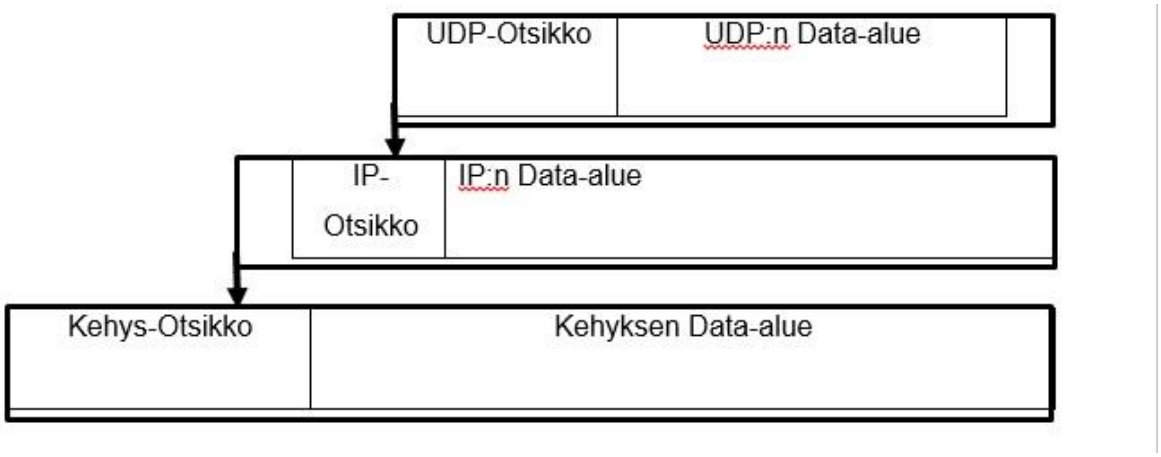
Taulukko 4. UDP-sanoma

Lähdeportti	Kohdeportit
Sanoman pituus	Tarkistussumma
Data	

Lähdeportti- ja Kohdeportti-kentät sisältävät 16-bittisen UDP-protokollaportin numeron, jonka perusteella protokollaohjelmisto tietää, mille prosessille tietosähke lähetetään. Lähdeportti-kenttä on valinnainen. Kun se on määritelty, sen ilmaisee portin, johon vastaus tulee lähettää. Sanoman pituus -kenttä on valinnainen. Sen sisältämä arvo ilmoittaa, montako oktettia UDP-tietosähke sisältää. Tarkistussumma-kenttä on valinnainen, jota ei tarvitse käyttää. Jos arvo on nolla, se tarkoittaa, että tarkistussummaa ei ole laskettu. (Comer 2002, 199.)

3.5.2 Kapselointi

Kapselointi tarkoittaa sitä, että UDP-protokolla liittää käyttäjän datan eteen otsikon ja siirtää tietosähkeen internet-kerrokseen. Internetkerros lisää otsikon UDP-tietosähkeen alkuun. Lopuksi verkkokerros asettaa tietosähkeen kehykseen, enne kuin se lähettää paketin toiselle koneelle. Kehyksen rakenne määräytyy käytettävän verkkotekniikan mukaan. Tavallisesti verkkokehyksetkin sisältävät otsikon. (Comer 2002, 201.)



Kuva 1. Kapselointi

4 PALOMUURI

4.1 Ensimmäisen sukupolven palomuurit

Palomuuri on tekninen järjestely, joka rajoittaa luvatonta pääsyä sisäverkoon, mutta sallii liikenteen sisäverkosta ulkoverkkoon. Palomuuri ohjaa liikennettä kahden verkon välillä, liikenteelle määritellään oikeudet kuten esim. Allow, Block, Encrypt, jne. Yleisesti palomuuri sijoitetaan sisäverkon ja internetin väliin. . (TECH-FAQ 2016.)

Palomuuri tarkastaa kaiken liikenteen, joka kulkee sisään ja ulos. Jos jotkin tiedot eivät täytä tarvittavia kriteerejä, palomuuri evää pääsyn verkkoon. Palomuurin keskeinen tehtävä on todentaa liikenteen turvataso eri tietoverkkojen välillä. (TECH-FAQ 2016.)

4.1.1 Laitepalomuuri

Laitepalomuuri on yleensä sijoitettu lähiverkon ja ulkoverkon väliin. Fyysisellä palomuurilla voi olla samoja ominaisuuksia kuin muillakin verkkolaitteilla, kuten esim. reititys. Laitepalomuuri tarjoaa korkea tasoista suojaa ulkoista tunkeutumista vastaan, koska niissä on oma laitteisto ja käyttöympäristö. Next generation -palomuuri on yleensä laitepalomuuri. (TECH-FAQ 2016.)

4.1.2 Palomuuriohjelma

Palomuuriohjelma asennetaan tietokoneeseen. Toimiakseen se käyttää tietokoneen prosessoria ja muistia. Ohjelmistopalomuuri suojaa vain tietokonetta, johon se on asennettu. Ohjelmistopalomuuri ei suojaa muuta verkkoa, ja ohjelma pitää asentaa jokaiseen tietokoneeseen erikseen. Nykyisin käyttöjärjestelmissä on itsessään ohjelmallinen palomuuri. Ohjelmiston voi ostaa, ja ohjelmistojen tarjoajia on useita. Ohjelmallinen palomuuri on huomattavasti halvempi kuin laitteistopalomuuri. (TECH-FAQ 2016.)

4.1.3 Pakettisuodatus

Yksi palomuuriratkaisu on pakettisuodatus. Palomuuri tarkistaa viisi IP-paketin kenttää:

- Lähde-IP-osoite
- Lähdeportti
- Päämäärän IP-osoite
- Päämäärän portti
- IP-protokolla. (TECH-FAQ 2016.)

Perustuen palomuurin sääntöihin, paketit joko päästetään läpi tai rajoitetaan niitä tai tiputetaan. Jos palomuuri rajoitta paketin kulkua se lähettää viestin lähettäjälle viestin, että paketti rajoitettiin. Jos paketti tuhotaan, palomuuri ei lähetä viestiä lähettäjälle, paketin tuhoamisesta. Pakettisuodatus toimii OSI-mallin kolmannella tasolla, sen toiminta on hyvin samankaltainen kuin reitittimellä. (TECH-FAQ 2016.)

4.1.4 Sovellustason yhdyskäytävä Proxy-palomuuri

Proxy-palomuurissa jokainen paketti pysähtyy Proxy-palomuuriin. Paketti tutkitaan ja verrataan palomuurin sääntöihin. Jos paketit täyttävät säännöt, ne uudelleen luodaan ja lähetetään eteenpäin. Kaikki liikenne kulkee Proxy-palomuurin kautta niin, että suora kommunikaatio sisäisen ja ulkoisen verkon koneiden välillä on mahdotonta. Tästä johtuen Proxy-palomuuri antaa parempaan suojausta kuin pakettisuodatus. Proxy-palomuuri toimii OSI-mallin tasolla seitsemän. (TECH-FAQ 2016.)

5 NEXT GENERATION -PALOMUURI

5.1 Muutamia next generation -palomuurin ominaisuuksia.

Ensimmäisen sukupolven palomuuri kykenee vain “joko/tai”-sääntöihin. Next generation -palomuuri kykenee protokollan sallimaan esim. portti 80, mutta estämään tiettyä liikennettä, joka käyttää porttia 80. Next generation -palomuuria voi kuvailla, että se on verkonuhkien käsittelyyn tarkoitettu työkalu. Next generatio -palomuuriin on lisätty eri ominaisuuksia, jotka aikaisemmin olivat itsenäisiä kokonaisuuksia. Nyt palomuuriin voidaan lisätä esim. virus- ja roskapostitunnistus, QoS-palvelu, IPS, VPN-tunnelointi ja Active Directory. (QuinStreet inc 2011.)

Seuraavissa kappaleissa esitellään next generation -palomuurin tietoturvaratkaisuja ulkoverkon mahdollisia hyökkäyksiä vastaan. Lisäksi esitellään salausmenetelmiä, jos luottamuksellista tietoa siirretään ulkoverkon yli.

5.2 Tunkeutumisen estojärjestelmä

Tunkeutumisen estojärjestelmä tunnetaan myös lyhenteestä IPS. Tunkeutumisen estojärjestelmä on tietoverkon tietoturvan uhan estoteknologia, joka tarkastaa tietoverkon liikennettä, havaitsee ja estää haavoittuvuuksien hyödyntämisen. Yleensä haavoittuvuutta hyödynnetään siten, että hyökkääjä lähettää syötteen, jonka kohteena on ohjelma tai palvelu. Hyökkääjä yrittää kaapata ja saada ohjelman, palvelimen tai tietokoneen käyttöönsä. Onnistuneessa murrossa hyökkääjä voi sulkea kohteen ohjelmia tai yrittää saada kaikki hallintaoikeudet palvelimelle ja pääsyn muuttamaan ohjelmien ominaisuuksia. (Palo Alto Networks inc. 2016.)

Tunkeutumisen estojärjestelmä takaa täydentävän analytiikan tason, joka estää haitallisen syötteen pääsyn sisäverkkoon. Se on erilainen kuin tunkeutumisen havaintojärjestelmä, joka on passiivinen järjestelmä. Se skannaa liikennettä ja raportoi tietoturvapoikkeamat. Tunkeutumisen estojärjestelmä analysoi aktiivisesti liikennettä ja tarkistaa kaiken liikenteen, joka siirtyy ulkoverkosta sisäverkkoon. Jos tunkeutumisyritys havaitaan, tunkeutumisen estojärjestelmä tekee seuraavat toimenpiteet:

- Lähettää hälytyksen verkon valvojalle.
- Tuhoaa vaaralliset paketit.
- Estää liikenteen saapuneesta osoitteesta.
- Uudelleenasettaa yhteyden. (Palo Alto Networks inc. 2016.)

Tunkeutumisen estojärjestelmän täytyy toimia tehokkaasti alentamatta tietoverkon suorituskykyä. Sen täytyy myös toimia nopeasti, koska tunkeutuminen voi tapahtua reaaliajassa. Tunkeutumisen estojärjestelmän pitää tunnistaa uhat ja toimia tarkasti, jotta se eliminoi uhat. (Palo Alto Networks inc. 2016.)

5.2.1 Havaitseminen

Tunkeutumisen estojärjestelmässä on erilaisissa tapoja löytää haavoittuvuudet, mutta allekirjoitetut ja staattiset poikkeama-pohjaiset havainnot ovat kaksi hallitsevaa mekanismia.

Allekirjoituspohjaiset havainnot perustuvat uniikkien tunnistettavien mallien sanakirjaan tai allekirjoituksiin. Kun haittakoodi on löydetty, sen allekirjoitus tallennetaan ja arkistoidaan allekirjoituksien sanakirjaa. Allekirjoitus-havainto jakautuu kahteen tyyppiin:

Haittasyöteallekirjoitus hyödyntää SQL-kyselyn haavoittuvuuksia. Tunkeutumisen estojärjestelmä pystyy tunnistamaan tiettyjä haavoittuvuuksia etsimällä vastaava kyselyn liikenteestä. (Palo Alto Networks inc. 2016.)

Haavoittuvuus-tason allekirjoitus, suojaa tietoverkkoja erilaisilta haavoittuvuuksilta, jotka ovat järjestelmissä. Niitä ei suoraan tarkkailla. Mutta nostaa riskiä hylätä turvallisia paketteja, koska tulkitsee ne vahingollisiksi.

Tilastollisen poikkeaman havaitseminen ottaa näytteitä tietoverkon liikenteestä satunnaisesti ja vertaa niitä esilaskettuun vertailukohtaan. Kun tietoverkon liikenteen näyte ei täsmää vertailukohtaan, tunkeutumisen estojärjestelmä tekee tarvittavat toimenpiteet. (Palo Alto Networks inc. 2016.)

5.3 Advance Evasion Technique

AET on tietoverkkohyökkäys, joka yhdistää muutamia erilaisia kiertämistapoja, joilla voi hyökätä tietoverkkoon niin että omistaja ei sitä huomaa. AET-koodi itsesään ei välttämättömästi ole haitallista, vaan vaara on siinä että se takaa hyökkääjälle huomaamattoman pääsyn tietoverkkoon. (TechTarget 2016a.)

On olemassa noin 200 tiedettyä kiertotekniikkaa, jotka ovat tunnistettavissa kaupallisissa tuotteissa. AET pystyy luomaan miljoonia “uusia” kiertotekniikkoja vain muutamasta yhdistelmästä. Murron havaitsemisjärjestelmä (IDS) ei havaitse tämän tyyppistä murtautumista. Jos kaikki 200 tapaa ovat käytössä, muunnelmia syntyy lähes ääretön määrä. (TechTarget 2016a.)

5.3.1 Kuinka AET toimii

Kun IDS tunnistaa haittasyötteen yhteyspyynnöstä, järjestelmä hylkää kyselyn ja estää pääsyn tietoverkkoon. Hyökkääjä voi muokata sanoja lisäämällä satunnaisia kirjaimia.

Nyt haittasyötteeseen on lisätty satunnaisia kirjaimia. Järjestelmä ei tunnistakaan haittakoodia, mutta murtautuminen onnistuu satunnaisista kirjaimista huolimatta. IDS ei tunnista hyökkäystä ja päästää sen tietoverkkoon. (TechTarget 2016a.)

Suomalainen tietoturvayritys Stonesoft oli ensimmäinen, joka tunnisti ja raportoi AET-uhasta. CERT työskentele Suomessa Stonesoftin ja muiden tietoturvayritysten kanssa ja yrittää löytää haavoittavuuksia. (TechTarget 2016a.)

5.4 Denial of Service

DoS-hyökkäys on yritys tehdä palvelu tai tietoverkko toimintakyvyttömäksi. Yksi yleisimmistä tavoista on, että hyökkääjä kyllästää palvelun ulkoa tulevilla pyynnöillä niin että tavalliset käyttäjät eivät saa yhteyttä palveluun. Dos-hyökkäykset voidaan toteuttaa monilla tavoilla. (Sophos Ltd 2016.)

5.4.1 ICMP-tulva

ICMP-tulvassa hyökkääjä lähettää suuren määrän IP-paketteja, joiden lähdeosoite on sama kuin vastaanottajan eli kohteen. Näin palvelin lähettää itse itselleen paketteja, jolloin liikenne kasvaa niin isoksi että palvelu ei kykene käsittelemään asiakkaiden yhteyspyyntöjä. (Sophos Ltd 2016.)

SYN/TCP-tulva on hyökkäystapa, jossa hyökkääjä lähettää monta TCP/SYN-pakettia, joista puuttuu lähettäjän osoite. Jokainen paketti käsitellään kuten yhteyspyyntö. Tämä aiheuttaa sen, että yhteys jää auki odottamaan kuittausta lähettäjältä. Yhteys on auki niin kauan kunnes se aikakatkaistaan. Kun kaikki yhteydet on varattu, ei tavallinen asiakas saa yhteyttä palveluun. (Sophos Ltd 2016.)

5.4.2 UDP-tulva

UDP-hyökkäys on hyökkäys, jossa hyökkääjä lähettää monia UDP-paketteja palvelun satunnaisiin portteihin. Tämä aiheuttaa sen, että palvelu joutuu lähettämään monta ICMP-vastauspakettia. Tämä kuormittaa palvelun tietoliikennettä niin, että palvelu on saavuttamattomissa. (Sophos Ltd 2016.)

5.5 Distributed Denial of Service

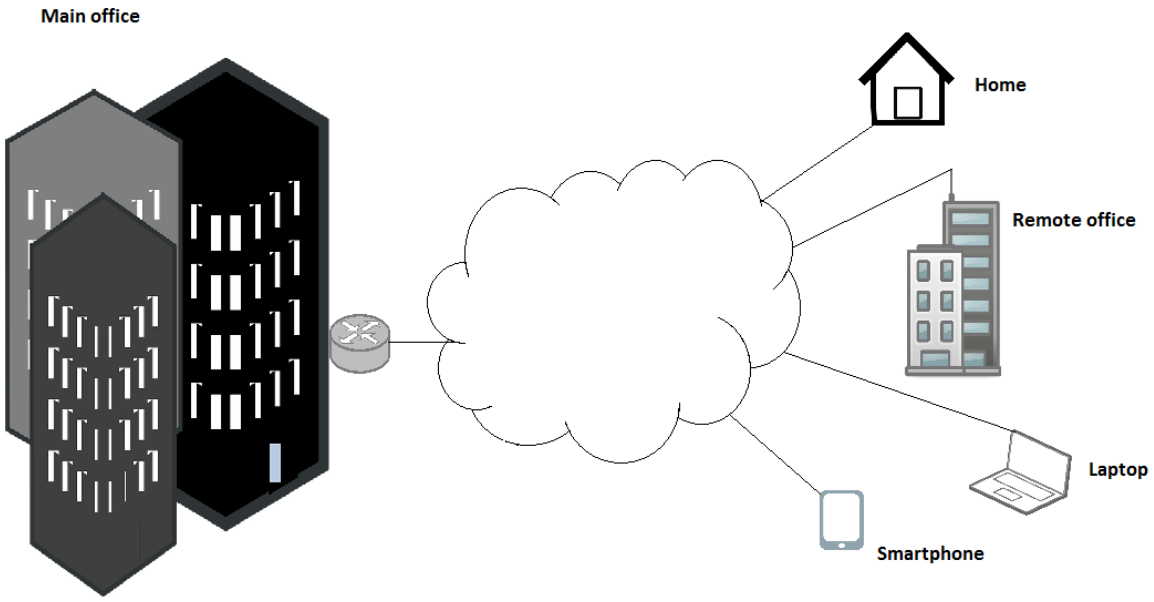
DDoS on palvelimenestohyökkäys, jossa hyökätään usealla samanaikaisella DoS-hyökkäyksellä useasta eri lähteestä, tai luodaan vain tarpeeksi liikennettä, jolloin palvelu ei pysty palvelemaan muita käyttäjiä. (Sophos Ltd 2016.)

Vaikka palomuurissa olisi ominaisuus, joka torjuu palvelunestoehyökkäyksiä, palomuuria ei ole varsinaisesti suunniteltu palvelunestohyökkäyksien torjuntaan. Palvelu saadaan pois toiminnasta, jos hyökkäys on tarpeeksi massiivinen esim. bottiverkon avulla. Tällöin hyökkäysliikenteen määrä on niin suuri että hyökkäyksen kohteelta loppuu kaistanleveys ja resurssit käsitellä yhteyspyyntöjä. (Sophos Ltd 2016.)

Betfair on internetissä toimiva maailman suurin vedonlyöntipörssi. Huhtikuussa 2015 järjestettiin Britanniassa yksi suurimmista laukkakilpailuista, samalle viikon lopulle osui myös Golf's Master -turnauksen loppuhuipennus. Betfairin palveluun tehtiin massiivinen palvelunestohyökkäys, jossa dataliikenteen määräksi laskettiin 45 GBt sekunnissa. Hyökkääjät pyysivät hyökkäyksen lopettamiseksi 10 Bitcoinia, joka tuolloin oli arvoltaan noin 2200 dollaria. (Amsel 2015.)

5.6 VPN-arkkitehtuuri

VPN-arkkitehtuuria käytetään yleisesti turvamaan tietoverkon liikenne, kun sitä siirretään ulkoverkon yli. VPN tarjoaa turvamekanismeja myös sisäverkossa tapahtuvaan liikenteen salaukseen, kapselointiin ja siirtämiseen verkon läpi. Tieto salataan luotettavalla tavalla, koska tietoliikennettä voidaan salakuunnella sisä- tai ulkoverkossa. Salauksen ansiosta paketteja ei voida lukea ilman oikeaa salausavainta, joten tieto voidaan lähettää turvallisesti ulkoverkon yli. User-to-LAN tekniikalla voivat yrityksen työntekijät liittyä yrityksen tietoverkkoon internetin kautta. Site-to-site-tekniikalla yrityksen eri lähiverkot voivat liittyä toisiinsa internetin kautta. Myös sisäverkon sisällä voidaan käyttää site-to-site-ominaisuutta ja liittää siihen yhteistyöyritys ulkoverkosta. (Cisco Systems inc. 2008.)



Kuva 2. VPN-esimerkki

5.6.1 Muutamia VPN-arkkitehtuurin tarjoamia salausprotokollia

IPsec on joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia internet-yhteyksien turvaamiseen. IPsec tarjoaa tehostettuja turvaominaisuuksia, kuten vahvan salausalgoritmin ja kattavan autentikoinnin. IPsecillä on kaksi salaustapaa, tunnelointi ja kuljetus. Tunnelointi salaa paketin otsikon ja datan. Vain järjestelmät, jotka käyttävät IPseciä, voivat hyödyntää tätä protokollaa. Kaikkien laitteiden, jotka vaihtavat tietoja keskenään, täytyy käyttää samaa yleisavainta tai sertifikaattia ja täyttää samanlaiset turvaehtosäännöt. (Cisco Systems inc. 2008.)

Etäkäyttöä varten tietyt laitteet, kuten kannetavat tietokoneet ja älypuhelimet, tarvitset kolmannen osapuolen ohjelmistoja, jotta etäyhteys saadaan muodostettua. IPsec tukee 56 bittistä DES-salausta tai 168 bitin 3DES-salausta. (Cisco Systems inc. 2008.)

Point-to-Point tunnelointi protokolla joka on tarkoitettu organisaation ulkopuolisiin Windows-työasemien kytkeytymiseen Windows-palvelimelle ulkoverkon yli. PPTP tukee monia VPN-protokollia. Microsoft Point-to-Point Encryption tukee 40 bitin ja 128 bitin salausta. On tärkeää muistaa, että PPTP itsessään ei salaa mitään. (Cisco Systems inc. 2008.)

L2TP/IPsec on tunnelointiprotokolla, joka toimii OSI 2 -tasolla. Tätä käytetään yleensä etäyhteydessä, asiakkaan ja palvelimen välillä. (Cisco Systems inc. 2008.)

5.6.2 Tiedon eheys

Tiedon salaminen on tärkeää julkisissa verkoissa. Yhtä tärkeää on varmistetaan se, että tieto ei, muuttunut lähetyksen aikana. Esimerkiksi IPsecillä on mekanismi, jolla varmistetaan se että paketin salattu osa, otsikko ja data-osa eivät ole vahingoittuneet. Jos vahingoittumista ilmenee, paketti hylätään. (Cisco Systems inc. 2008.)

On tärkeää varmistua ja tarkistaa lähteen identiteetti, mistä data on lähetetty. Datan alkuperän autetikonti suojaa hyökkäyksiltä, joissa lähettäjä on väärennetty.

Anti Replay tunnistaa ja rajoittaa uudelleen lähetetyt paketit, mikä auttaa estämään huijauksen. (Cisco Systems inc. 2008.)

5.7 Tunnelointi

Tunnelointi on kapselointiprosessi jossa, koko paketti paketoidaan uudeksi paketiksi ennen lähettämistä verkon yli. Datan tunnelointi on kätevä tapa, jos halutaan piilottaa laitteen alkuperäinen identiteetti. Esimerkiksi laite, joka käyttää IPseciä, kapseloi IP-paketit lisäämällä siihen oman otsikon. Salaamalla alkuperäisen paketin ja otsikon tunnelointilaite piilottaa oikean paketin lähettäjän. Vain luotettu vastaanottaja pystyy lukemaan datan. (Cisco Systems inc. 2008.)

Kaikki edellä mainitut protokollat käyttävät tunnelointia lähettääkseen salattua dataa julkisessa verkossa. Pelkästään tunnelointi itsessään ei tarjoa datan suojaa. Pelkästään paketin kapselointi ei riitä, myös data pitää salata. (Cisco Systems inc. 2008.)

Tunnelointiin tarvitaan kolme protokollaa:

- **Kuljetusprotokolla,** joka on alkuperäinen kuljetettava data, esim. IPX, NetBeui, IP.
- **Kapseloitiprotokolla,** joka käärii alkuperäisen datan, esim. GRE, IPsec, L2F, PPTP, L2TP.

- **Kantajaprotokolla**, jota käytettään tiedon kuljettamiseen verkon yli. Salattuna voidaan lähettää myös protokollat IPX ja NetBeui, joita ei normaalisti kuljeteta julkisissa verkoissa. (Cisco Systems inc. 2008.)

Kapseloitiprotkolla sisältää yleensä tiedon, minkä tyyppistä pakettia ollaan kapseloimassa, ja tiedottaa yhteydestä palvelimen ja asiakkaan välillä (Cisco Systems inc. 2008).

5.7.1 Autentikointi

Ilman käyttäjän autentikointia, kuka tahansa voi käyttää tietokoneeseen asennettua VPN-asiakasohjelmaa ja ottaa etäyhteyden tietoverkkoon. Käyttäjän autentikoinissa pitää käyttäjän kirjauta ensin käyttäjätunnuksella ja salasanalla, jonka jälkeen vasta etäyhteys voidaan muodostaa. Käyttäjätunnus ja salasana voidaan tallettaa VPN-laitteeseen tai ulkoiselle AAA-palvelimelle. (Cisco Systems inc. 2008.)

5.8 SSL-VPN

SSL-VPN on VPN-muoto jota voidaan käyttää verkkoselaimella. Jos verrataan IP-seciä ja SSL-protokollaa, niin SSL ei vaadi erillistä hallintaohjelmistoa käyttäjän tietokoneessa. Sisäverkkoon voidaan liittyä käyttämällä selainpohjaista asiakas-palvelin-ohjelmaa, jolla liikenne salataan. (TechTarget 2016b.)

SSL-VPN koostuu yhdestä tai useammasta VPN-laitteesta, joihin käyttäjä ottaa yhteyttä verkkoselaimella. Liikenne verkkoselaimen ja SSL-VPN:n välissä salataan käyttäen SSL-protokollaa tai TLS-protokollaa. SSL-VPN tarjoaa monipuolista ja helppokäyttöisyyttä käyttäjille riippumatta tietokoneesta ja yhteydenottopaikasta. On olemassa kaksi yleistä SSL-VPN-tyyppiä:

SSL-Portal. Tämä VPN-tyyppi sallii yhden SSL-yhteyden verkkosivustoon, jolla käyttäjä voi turvallisesti kirjauta lukuisiin tietoverkkoihin. Sivustoa kutsutaan portaaliksi, koska se on yksi sivusto ja johtaa moniin resursseihin. Etäkäyttäjä pääsee käyttämään SSL-VPN-yhdyskäytävää millä tahansa modernilla verkkoselaimella. Etäkäyttäjä identifioi itsensä yhdyskäytävään ja yhdyskäytävä autentikoi sen annetulla tavalla ja antaa pääsyn porttaaliin.

SSL-Tunnel. Tämä VPN sallii verkkoselaimella turvallisen pääsyn tietoverkkopalveluihin SSL-tunnelin läpi, sisältäen ohjelmat ja protokollat, jotka eivät ole selainpohjaisia. SSL-Tunnel-VPN edellyttää, että verkkoselain pystyy käyttämään aktiivisia sisältöjä, jotka sallivat sellaisia tekniikkoja. Näitä tekniikkoja ovat esim. Java, JavaScript, Active X, Flash tai verkkoselaimen plug-init. (TechTarget 2016b.)

6 PALOMUURIN KONFIGUROINTI

6.1 Halutut ominaisuudet

Työnä oli konfiguroida palomuuriin 3 ominaisuutta, jotka olivat NAT, Access List ja active/standby failover. Myös etäyhteys konfiguroidaan Telnetille ja SSH:lle käytettäväksi sisäverkosta. Testaus suorittaan, kun konfigurointi on tehty ja kaikki laitteet on saatu paikoilleen ja kytketty verkkoon.

6.2 Laite

Laitteena toimi Ciscon PIX 525 -palomuuri, joka on next generation -palomuuri. Kyseessä on Cisco PIX 500 -sarjan palomuuri, joka sopii keskisuurien yrityksien tietoverkkoihin luotettavaksi tietoturva- ja tietoverkkolaitteeksi. Sen koko on kaksi räkkiyksikköä korkea (2RU) ja siinä on kaksi 10/100 Fast Ethernet -porttia. Se voidaan laajentaa kahdeksalla 10/100 Fast Ethernet -portilla tai kolmella Gigabit Ethernet -portilla. Se sisältää myös verkko-ohjelmistoja ja reititysominaisuuksia. (Systems inc. 2004.)

Kuva 3. Cisco PIX 525 -palomuuri

Palomuurin mitat ja paino ovat:

- 2 RU, standard 19 tuuma, räkkiin asennettava
- mitat 8,89 x 44,45 x 46,36 cm
- paino 14,5 kg

Palomuurin suorituskyky on:

- selväkieliteksit ulostulo: 330 Mbps

- yhtäaikaiset yhteydet: 280,000
- 168-bit 3DES IPSec VPN -ulostulo: 145 Mbps VAC+ tai 72 Mbps VAC
- 128-bit AES IPSec VPN -ulostulo: jopa 135 Mbps VAC+
- 256-bit AES IPSec VPN -ulostulo: jopa 135 Mbps VAC+
- samanaikaista VPN-tunnelia: 2000

Palomuurin tekniset tiedot ovat:

- prosessori: 600-MHz Intel Pentium III -prosessori
- muisti: 128 tai 256 MB SDRAM-muistia
- Flash-muisti: 16 MB
- välimuisti: 256 KB 600 MHz
- järjestelmäväylä: 32-bit, 33-MHz PCI

Palomuurin laajennukset ovat:

- kolme 32-bit/33-MHz:in PCI paikkaa
- kaksi 168-pin DIMM RAM paikkaa

Palomuurin liitännät ovat:

- konsoliportti: RS-232, 9600 bps, RJ-45
- Failover-portti: RS-232, 115 Kbps, DB-15
- kaksi 10/100 Fast Ethernet -porttia, RJ45
- kaksi gigabit Ethernet –valokuituporttia. (Systems inc. 2004.)

6.2.1 Laitteen ominaisuudet ja edut

Laitteen etuja ovat mm. seuraavat:

- VPN-laitteiston nopeuttaminen
  - VPN kiihdytin kortti tai VPN kiihdytin kortti+
  - Failover ja Failover-aktiivinen/aktiivinen

- Protokollatarkistukset
  - HTTP-protokolla
  - FTP-protokolla

- ESMT-protokolla
- DNS
- SNMP-protokolla
- ICMP-protokolla
- SQL*Net
- NFS
- GPRS-tunnelointi protokolla

- Integroidutpalvelut
  - näkymätön sillatussa tilassa
  - DoS-hyökkäyksen esto
  - IPS
  - AAA-palvelin

- VPN-palvelut
  - 2000 yhtäaikaista etäkäyttäjää
  - 56-bittinen DES-salaus
  - 168-bittinen 3DES-salaus
  - 256-bittinen AES-salaus
  - etäyhteyden autentikointi

- Tietoverkkopalvelut
  - Vlan-virtuaaliportit
  - QoS-palvelut
  - OSPF dynaaminen reititys
  - IPv6
  - DHCP-palvelin
  - NAT- ja PAT tuki. (Systems inc. 2004.)

6.3 Konfigurointi

Työ aloitettiin salasanan nollauksella, seuraava vaihe oli NAT-toiminnon ja Access-listin konfigurointi. Palomuuriin kirjautumista helpotettiin konfiguroimalla siihen Telnet- ja SSH-asiakasohjelmalla kirjautuminen sisäverkosta. Testauksessa tarkastetaan yhteys ulkoverkkoon, sisäverkon toimivuus ja pienimuotoinen hajautettu palvelinestohyökkäys.

6.3.1 Salasanan nollaus

Koska laite oli käytetty, oli siihen asetettu kirjautumiseen edellyttävä salasana. Salasanan nollaamiseen tarvittiin yksi reititin, TFTP-palvelin, binääritiedosto, suora RJ45-kaapeli, yksi ristiin kytketty RJ45-kaapeli, konsolikaapeli ja itse palomuuri. Konsolikaapeli kytkettiin tietokoneen konsoliporttiin ja kaapelin toinen pään palomuurin konsoliporttiin. Palomuurin käynnistyessä yhteys otettiin PuTTY-ohjelmalla. Palomuurin käynnistyessä ESC-näppäimen painaminen keskeyttää lautauksen ja binääritiedoston voi ladata palomuurin Flash-muistiin. Binääritiedosto ladattiin Cisco Systemsin verkkosivuilta TFTP-palvelimella ja TFTP-palvelimelta palomuuriin.

Palomuurille annettiin seuraavat komennot:

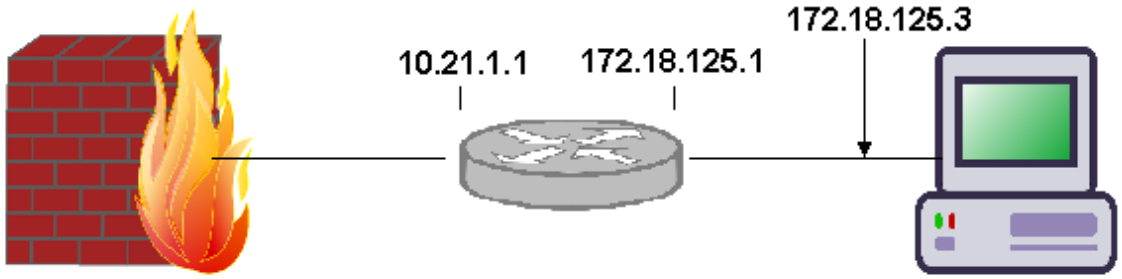
```
monitor>interface 0
0: i8255X @ PCI(bus:0 dev:13 irq:10)
1: i8255X @ PCI(bus:0 dev:14 irq:7 )

Using 0: i82559 @ PCI(bus:0 dev:13 irq:10)
monitor>address 10.21.1.99
address 10.21.1.99
monitor>server 172.18.125.3
server 172.18.125.3
monitor>file np70.bin
file np52.bin
monitor>gateway 10.21.1.1
gateway 10.21.1.1
monitor>ping 172.18.125.3
Sending 5, 100-byte 0xf8d3 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor>tftp
tftp np52.bin@172.18.125.3 via 10.21.1.1.................................
Received 73728 bytes

Cisco Secure PIX Firewall password tool (3.0) #0: Tue Aug 22 23:22:19 PDT 2000
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000
```

```
Do you wish to erase the passwords? [yn] y
Passwords have been erased.

Rebooting....
```



Kuva 4. Salasanan resetointi

Tämän jälkeen kytkennät purettiin ja palomuuriin päästiin kirjautumaan käyttämällä palomuurin oletussalasanaa.

6.3.2 NAT-konfigurointi

Seuraava konfigurointi oli palomuuriin osoitteenmuunnos ja protokolla sääntöjä Access-listaan. Konfigurointi tehtiin alla olevilla käskyillä, jotka sallivat pääsyn FTP-palvelimelle. Esimerkissä olevat IP-osoitteet poikkeavat konfiguroitavan laitteen palomuurin IP-osoitteista.

NAT ja Access-List:

```
hostname(config)#nat (inside) 1 10.1.6.0 255.255.255.0
hostname(config)#global (outside) 1 175.1.1.3-175.1.1.64 netmask 255.255.255.0
hostname(config)#static (inside, outside) 175.1.1.254 10.200.1.254
Määritellään ketkä voivat yhditää web/FTP palvelimen porttiin
hostname(config)#access-list 101 permit tcp any host 175.1.1.254 eq www
hostname(config)#access-list 101 permit tcp host 199.199.199.24 host 175.1.1.254 eq
ftp
hostname(config)#access-list 101 permit tcp host 199.199.199.24 host 175.1.1.254 eq
ftp-data
hostname(config)#access-group 101 in interface outside
```

6.3.3 Failover-konfigurointi

Koska Ciscon omaa failover-kaapeli ei ollut, niin Active/Standby-Failover toteutettiin liittämällä palomuurin gigabitin Ethernet-portit toisiinsa valokuidulla.

Failover active/standby:

```
hostname (config)# interface Gigabitethernet 0
hostname(config-if)# ifname active
hostname(config-if)# exit
hostname(config)# failover lan
hostname(config)# failover lan unit primaryble
hostname(config)# failover interface ip actice 192.168.10.1 255.255.255.255 standby
192.168.20.1
hostname(config)# interface active
hostname(config-if)# no shutdown
hostname(config)# failover
hostname(config)# copy running-config startup-config
toisen yksikön konfigurointi
hostname (config)# interface Gigabitethernet 1
hostname(config-if)# ifname
hostname(config-if)# exit
hostname(config)# failover lan enable
hostname(config)# failover lan interface passive Gigabitethernet 1
hostname(config)# failover interface ip passive 192.168.20.1 255.255.255.255 standby
192.168.10.1
hostname(config)# failover
hostname(config)# copy running-config startup-config
```

6.3.4 Etäyhteyden konfigurointi

Etäyhteyden muodostamiseksi pitää luoda käyttäjä AAA-palvelimelle lisäksi pitää konfiguroida sallitut yhteysprotokollat, kuten Telnet ja SSH. Tietoturvasyistä vain sisäverkosta voi muodostaa yhteyden ja vain yhdestä tietystä IP-osoitteesta. Etäyhteys katkeaa, jos sitä ei käytetä 30 minuuttiin.

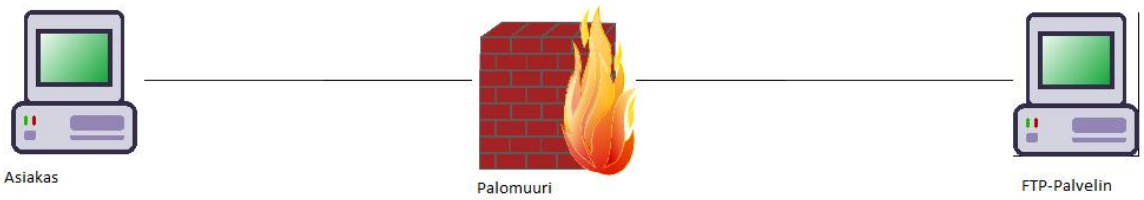
Käyttäjän luominen AAA-palvelimelle.

```
hostname(config)#username username password password
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write mem
Etäkäyttäjien autentikointi
hostname(config)# aaa authentication ssh console LOCAL
hostname (config)# aaa authentication telnet console LOCAL
```

```
Etäyhteyden protokolla ja ip-osoite sisäverkosta
hostname (config)#ssh 10.1.1.2 255.255.255.255 inside
hostname (config)#telnet 10.1.1.2 255.255.255.255 inside
jos yhteys on käyttämättä 30 minuuttia istunto katkaistaan
hostname(config)# telnet timeout 30
hostname(config)# ssh timeout 30
```

6.4 Testaus

Ensimmäisenä testauksena oli testata palomuuria sisäverkossa. Asennettuun FTP-palvelimeen otettiin yhteyttä FTP-asiakasohjelmalla ja ladattiin testitiedosto. Palomuuri oli sijoitettu kahden sisäverkon väliin.



Kuva 5. FTP-tiedonsiirto sisäverkossa

Palomuuri liitettiin sisäverkon ja ulkoverkon väliin. Testaustietokone latasi SeAMK:in verkkosivuston onnistuneesti.

Koska palomuurissa on IPS-järjestelmä, testiin kuului pienimuotoinen DDoS-hyökkäyksen simulointi. FTP-palvelinta vastaan olisi hyökätty viidellä tietokoneella, mutta testiympäristön virustorjuntaohjelma eväsi hyökkäysohjelman käytön, eikä testaamiseen tarkoitettujen tietokoneiden virustorjuntaohjelmaa ollut mahdollista kytkeä pois päältä.

6.5 Päätelmät

Vaikka konfiguroitava palomuuri oli valmistettu vuonna 2006, siitä löytyvät tietoturva-ominaisuudet olivat samat kuin nykyisistä palomuureista löytyvät. Vaikka fyysiset portit olivat nopeudeltaan vanhentuneita, palomuurissa oli mahdollisuus laajentaa portit gigabit Ethernet -valokuituporteiksi. Palomuurin käyttöliittymä oli tekstipohjainen, joka aiheutti sen että vian etsintä oli todella haastavaa verrattuna graafisiin käyttöliittymiin.

LÄHTEET

Amsel, P, 14.4.2015. Online gambling sites targeted by fresh round of DDOS attacks. [Verkkosivuartikkeli]. Calvin Ayre Foundatation [Viitattu 6.3.2016]. Saatavana: http://calvinayre.com/2015/04/14/business/online-gambling-sites-targeted-ddos-attacks/

Cisco Systems inc. 2004. Cisco PIX 525 Security Appliance. [Verkkosivu]. [Viitattu 16.4.2016]. Saatavana: http://www.cisco.com/c/en/us/products/collateral/security/pix-525-security-appliance/product_data_sheet09186a0080091b09.html

Cisco Systems inc. 2008. How VPN works. [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#vpn_tech

Comer, D. E. 2002. TCP/IP. Suomentaja: Suominen, Erkki.

Eskola, H. 21.8.2013. Konecranes joutui suuren petoksen uhriksi. [Verkkolehtiartikkeli]. Kauppalehti. [Viitattu 6.3.2016]. Saatavana: http://www.kauppalehti.fi/uutiset/konecranes-joutui-suuren-petoksen-uhriksi---rikolliset-huijasivat-17-2-miljoonaa-euroa/G44Y66fT

Granlund, K. 2003. Tietoliikenne. 1. p. Porvoo: WS Bookwell.

ISO 27000. 2010. Informaationtegnologia. Turvallisuus.Tietoturvallisuuden hallinta-järjestelmät. Yleiskatsaus ja sanasto. Suomen Standardisoimisliitto SFS.

ISO 27002. 2006. Informaationtegnologia. Turvallisuus.Tietoturvallisuuden hallinta-järjestelmät. Yleiskatsaus ja sanasto. Suomen Standardisoimisliitto SFS.

Järvinen, P. 2002. Tietoturva & yksityisyys. 1. p. Porvoo: WS Bookwell.

Koivikko, K. 2014. Tietoturvassa isoja aukkoja. [Verkkoartikkeli]. Suomen Yrittäjät. [Viitattu 6.3.2016]. Saatavana: http://www.yrittajat.fi/fi-FI/uutisarkisto/a/ya/tietoturvassa-isoja-aukkoja-vain-palomuurit-kunnossa

Kuusimäki, M. 23.9.2009. Hämähäkkejä verkossa: Tietoverkkorikollisuuden torjunta syyttäjän näkökulmasta. [Verkkojulkasu]. ECT FORUM 09. [Viitattu 6.3.2016]. Saatavana: http://www.eis.fi/ect/fp/ECT09_230909_Plenary_Kuusimaki.pdf

QuinStreet inc. 2011. Intro to Next Generation Firewalls. [Verkkosivu]. [Viitattu 6.3.2016]. Saatatava: http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html

Palo Alto Networks inc. 2016. What is an intrusion prevention system? [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips

Rousku, K. 2014. Kybertuvaopas: Tietoturvaa kotona ja työpaikalla. 1. p.

Salminen, J. 2009. Ruotsi aloitti tietoliikenteen salakuuntelun. [Verkkolehtiartikkeli]. Suomen kuvalehti. [Viitattu: 6.3.2016]. Saatavana: http://suomenkuvalehti.fi/jutut/kotimaa/talous/ruotsi-aloitti-verkkoliikenteen-salakuuntelun-mita-pitaa-tehda-ja-tietaa/

Sophos, 2016. How to Prevent DoS and DDoS Attacks using Sophos Firewall. [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: https://www.sophos.com/en-us/support/knowledgebase/123182.aspx

TECH-FAQ. 2016. Firewalls. [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: http://www.tech-faq.com/firewall.html

TechTarget, 2016a. Advanced Evasion Technique (AET). [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: http://searchsecurity.techtarget.com/definition/advanced-evasion-technique-AET

TechTarget, 2016b. SSL VPN. [Verkkosivu]. [Viitattu 6.3.2016]. Saatavana: http://searchsecurity.techtarget.com/definition/SSL-VPN

Vaalisto, H. 2011. Amerikkalaiseen turvayhtiöön tehdyssä hakkeri-iskussa vietiin useiden kymmenien suomalaisten tietoja. [Verkkolehtiartikkeli]. Iltalehti. [Viitattu 6.3.2016]. Saatavana: http://www.iltasanomat.fi/digi/art-2000000462718.html