Lauri Hållfast

Palvelunestohyökkäyksen vaikutusten pienentäminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

18.11.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Lauri Hållfast Palvelunestohyökkäysten vaikutusten pienentäminen 54 sivua + 1 liite 18.11.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Lehtori Harri Ahola Service Support, Manager Sauli Vainio

Palvelunestohyökkäysten vaikutusten pienentämisellä pyritään puolustautumaan volyymi- ja ohjelmistopohjaisilta -palvelunestohyökkäyksiltä. Tätä vaikutusten pienentämistä kutsutaan englanniksi termillä ”mitigate”. Työssä tutkittiin palvelunestohyökkäyksen tekniikkaa ja verrattiin sitä eri kybersodankäynnin keinoihin. Työssä pyrittiin myös määrittelemään palvelunestohyökkäyksen tekijän taktiikkaa hyökkäyksen käynnistyksessä ja tutkimaan eri mahdollisuuksia palvelunestohyökkäysten vaikutusten pienentämiseen olemassa olevin keinoin.

Työssä tutkittiin palvelunestohyökkäyksen vaikutusta laboratorio-olosuhteissa eri palomuurikonfiguraatioihin. Tutkimuksissa todettiin, että palvelunestohyökkäysten vaikutusten lieventäminen on ilman etukäteisvalmistautumista vaikeata tai mahdotonta. Havaittiin myös, että palvelunestohyökkäys voi lamauttaa palomuurin ja estää näin kohteen kaiken tietoliikenteen laitteen läpi. Lamautuneen palomuurin hallinta oli hyökkäyksen aikana mahdotonta.

Työn tuloksien pohjalta todetaan, että kriittisen verkkopalvelun ylläpitäjän kannattaa varautua palvelunestohyökkäyksiin ennakkoon. Varmin tapa on investoida automaattiseen palvelunestohyökkäysten torjuntaan erikoistuneisiin laitteisiin ja palveluihin tai hajauttaa verkkopalvelun ylläpitoa mahdollisimman laajalle. Näin varmistetaan, ettei yhteen kohteeseen käynnissä oleva hyökkäys lamauta kaikkia palveluita.

Avainsanat	DOS, mitigointi, kybersota, palvelunesto

Author Title Number of Pages Date	Lauri Hållfast Denial of Service mitigation 54 pages + 1 appendix 18 September 2014
Degree	Bachelor of Engineering
Degree Programme	Computer Science
Specialisation option	Networking
Instructors	Harri Ahola, Principal Lecturer Sauli Vainio, Service Support, Manager

Denial of service (DoS) mitigation is the means of defending against volume or software based denial of service attacks. The objective of this thesis is to study the technology behind a denial of service attack, and compare it to other weapons of cyber warfare. In addition, the thesis investigates the different tactics behind launching a denial-of-service attack and the possibilities of mitigating these attacks with current means available.

The effects of denial of service attacks on firewall devices were observed in laboratory conditions. During these tests, it was concluded that mitigation of these attacks without preparation is difficult or impossible. Furthermore, it was noticed that a denial of service attack can paralyze a firewall completely and thus block all penetrating traffic. When paralyzed, even the management of a firewall was found impossible.

Based on the findings of this thesis, it can be concluded that the administrator of a highly critical network service must prepare for denial of service attacks. The best way is to invest in automatic mitigation devices or services or decentralize the network service as extensively as possible. This will ensure that when under an attack, not all network services will become unavailable.

Keywords	DOS, mitigation, cyber warfare, denial of service.

Sisällys

Lyhenteet

ARP	Address Resolution Protocol. Käytetään verkkotason osoitteiden yhdistämiseen loogisiin (siirtokerros) osoitteisiin.
CMS	Content Management System. Järjestelmä jonka tarkoituksena on huolehtia verkkosivuston sisällöstä ja mahdollistaa sen ylläpitäjälle helppokäyttöisyys sivuston päivitykseen.
DDOS	Distributed Denial Of Service. Hajautettu palvelunestohyökkäys.
DOS	Denial Of Service. Palvelunesto. Estetään jonkin verkkopalvelun toiminta lamauttamalla sen resurssit.
DNS	Domain Name System. Nimipalvelujärjestelmä joka muuntaa IP-osoitteen domain nimeksi.
HTTP	Hypertext Transfer Protocol. Yleisin verkkosivujen siirtämiseen palvelimen ja internet-selaimen välillä käytetty protokolla.
ICMP	Internet Control Message Protocol. Verkkokerroksella käytetty protokolla kohdeverkkojen tilan selvitykseen.
IDMS	Intelligent Mitigation System. Järjestelmä, joka osaa automaattisesti mitigoida havaittuaan palvelunestohyökkäyksen.
IDS	Intrusion Detection System. Järjestelmä, joka seuraa tietoverkon sisällä ja sen ulkorajoilla tapahtuvaa liikennettä ja raportoi poikkeamista ja tunkeutumisyrityksistä.
IP	Internet Protocol.
IPS	Intrusion Prevention System. Järjestelmä, jonka avulla on tarkoitus estää tietoverkkoon tunkeutuminen reagoimalla poikkeamiin
IPV4	Internet Protocol version 4.
IPV6	Internet Protocol version 6.
LCC	Logical Link Layer. OSI-mallin 2. kerroksen siirtokehyksen nimi.
MAC	Media Access Control. OSI-mallin 2. kerroksen siirtokehyksen nimi.
NAT	Network Address Translation. IP-osoitteen osoitemuunnos.
NTP	Network Time Protocol. Aikatiedon välittämiseen tietokoneiden välillä käytetty protokolla.
NOC	Network Operations Control. Verkonvalvontakeskus palvelu – ja internet operaattorilla. Vastuullaan on verkon ja mahdollisesti siihen liitettyjen palveluiden valvonta ja vikatilanteisiin reagointi.

OODA	Observation, Orientation, Decision, Action. Johtamisen vaiheiden silmukka.
OSI	Open System Interconnection. Tietoliikenteen eri tasojen kuvaus
SNMP	Simple Network Managment Protocol, Verkkolaitteiden tilan ja kunnon valvontaan käytetty protokolla.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan yhteydellisiä yhteyksiä laitteiden välille tietoverkoissa.
TCP-ACK	Acknoweldge. TCP protokollassa käytetty yhteyden avaukseen liittyvä hyväksyntä, kohdekone hyväksyy lähteen avaaman yhteyden.
TCP-SYN	Synchronize. TCP protokollassa käytetty uuden yhteyden avauksessa käytettävä paketti.
UDP	User Datagram Protocol. Tietoliikenneprotokolla, jolla luodaan yhteydettömiä yhteyksiä laitteiden väillle tietoverkoissa.
UTM	Unified Thread Management. Perinteisestä palomuurista laajennettu tietoturvalaite, joka pyrkii valvomaan jokaisella OSI-mallin kerroksella tapahtuvaa liikennettä.

1 Johdanto

Palvelunestohyökkäyksen mitigointi tarkoittaa palvelunestohyökkäyksen vaikutusten vähentämistä ja lievennystä. Hyökkäystä ei voi estää tai pysäyttää sen ollessa käynnissä. Tässä työssä tutkin eri palvelunestohyökkäysten tekniikoita ja sitä, mitä mahdollisuuksia on hyökkäyksen kohteella varautua hyökkäyksiin. Tutkin myös eri hyökkäyksen käynnistäjän motiiveja verkkohyökkäyksiin.

Palvelunestohyökkäykset ovat hyvin mediaseksikäs tietoverkkotekniikan ala. Ne saavat Suomessa aikaan räikyviä otsikoita onnistuessaan. Kohteena ovat olleet suomalaiset mediatalot ja julkisuudessa olevat yritykset. Yritykset yleensä kiinnostuvat hyökkäysten vaikutusten lieventämisestä otsikoiden myötä tai huomatessaan olevansa hyökkäyksen kohteena.

Helpoin keino suojautua palvelunestohyökkäyksiltä etukäteen on huolehtia palvelun hajauttamisesta maailmanlaajuisesti ja automaattisesta lievennyksestä. Hyökkäyksen jatkuessa se voi nimittäin laajentua saman palveluntarjoajan muihin palveluihin ja aiheuttaa ennakoitua suurempaa tuhoa. Hajauttaminen on kuitenkin kallista ja vaatii suunnittelua etukäteen.

Pääsin itse tutustumaan tarkemmin palvelunestohyökkäyksiin Maanpuolustuskoulutusyhdistyksen järjestämällä Kyberturvallisuus kurssilla 20. -22.9.2013 Santahaminassa Helsingissä. Kurssilla toimittiin valvotuissa olosuhteissa kyberhyökkäyksen kohteena olevassa organisaatiossa. Palvelunestohyökkäykset toimivat osana kyberhyökkäyksessä käytettäviä keinoja.

Eri laitevalmistajien toimittamissa ratkaisuissa on tutustuttu hyökkäysten vaikutusten lieventämiseen niin pilvipohjaisissa, kuin laitteistopohjaisissa ratkaisuissakin. Näiden toimivuudesta ja sopivuudesta on haastateltu DNA Oy:ssä työskenteleviä asiantuntijoita. Lisäksi rakensin laboratorioympäristön, jossa testasin normaalin palomuurin toimintaa hyökkäyksessä, ja sen mahdollisuuksia selviytyä sellaisesta.

Internetissä esillä olevan yrityksen tulisi varautua mahdollisiin verkkouhkiin tietoturvastrategiassaan ja mahdollisesti harjoitella hyökkäyksen väistöä käytännössä.

2 Tietoverkkotekniikan palvelurakenne

2.1 Verkkopalvelun koostumus

Nykyinen internet näkyy normaalille käyttäjälle verkkosivuina. Sivustojen kautta voidaan hoitaa pankkiasioita, työasioita tai vain noutaa verkosta tietoa vapaa-ajalla. Harvoin normaali verkkoselaaja joutuu ajattelemaan eri palveluita, jotka toimivat yhteen tuottaen hänelle hänen näkemänsä verkkosivun. Tällöin käyttäjältä saattaa unohtua, että jokaisen verkko-sivun taustalla on sitä tuottava tietokone.

Verkkosivu voi koostua useista palveluista: sen sisältämä tieto voidaan hakea eri tietokannoista, kuvat toisaalta ja verkkosivun jäsentely kolmannesta paikasta. Jokaista tällaista tiedon lähdettä kutsutaan palveluksi. Näistä tausta palveluista koostetaan verkkopalveluna käyttäjälle näkyvä verkkosivu.

Internet on pullollaan käyttäjälle näkymättömiä palveluita. Esimerkiksi nimipalvelut (DNS, Domain Name system) huolehtivat verkko-osoitteiden käännöstä ja aikapalvelut (NTP, Network Time Protocol) tietokoneen kellonajasta. Tausta-palvelut on automatisoitu nykyään niin paljon, ettei niiden toiminta näy juuri lainkaan peruskäyttäjälle.

Verkkopalvelu koostuu IP-osoitteesta ja avoimesta portista. Esimerkiksi verkko-osoite http://www.metropolia.fi kertoo että ip-osoitteessa ”www.metropolia.fi” on avoinna tcp portti 80 http-liikenteelle. DNS nimi metropolia.fi selvitetään selaimessa automaattisesti ip-osoitteeksi 195.148.144.10. Yhteyden avaaminen Metropolian verkkosivupalveluun onnistuu näin helposti olemassa olevien rajapintojen avulla. Rajapintoja kuvaamaan on luotu OSI-malli.

2.2 OSI-Malli

2.2.1 Yleisesti

OSI-mallia (Open System Interconnection) käytetään yleisesti tiedonsiirron kuvaamiseen internetissä ja muissa tieto-verkoissa. OSI-malli on yksi automaattisen tietoliikenteen vanhimmista käsitteistä (sen kehitys on alkanut jo 1970-luvulla), mutta se onnistuu yhä kuvaamaan tietoliikenteen verkkorakennetta ja rajapintoja. OSI-mallia käytetään

myös työkaluna palvelunesto-hyökkäysten laadun tunnistamisessa, siksi tutkimme sitä tässä työssä tarkemmin.

Kuva 1. OSI-malli kuvattuna graafisesti (Wikipedia, 2005).

OSI-malli on jaettu seitsemään verkkokerrokseen (ks. kuva 1). Jokainen verkkokerros tukeutuu allaan olevan kerroksen tuottamaan palveluun ja näin tarjoaa valmiin rajapinnan ylempien kerrosten käytettäväksi. Näin ylempien kerrosten ei tarvitse huolehtia alempien kerrosten tehtävistä, ja päinvastoin. Kärjistettynä: verkkoselaimen (layer7) ei tarvitse huolehtia bitin kapseloinnista modeemin soittosarjaan (layer1-2).

Käyttäjälle näkyvät palvelut pyörivät OSI-mallin seitsemännellä kerroksella, eli sovelluskerroksella. Toimiakseen verkkopalvelun kaikkien palveluiden pitää toimia kaikkien OSI-mallin kerrosten läpi, niin palvelinpäässä kuin asiakaspäässä.

Rajapinnat mahdollistavat jokaisen kerroksen viestinnän ylemmän ja alemman kanssa. Viestintä koostuu pyynnöistä, ilmoituksista, vasteista ja vahvistuksista. Koska rajapinnat on määritelty tarkasti, voi niiden kautta välittää vain tarkasti sovittuja pyyntöjä. Tämä mahdollistaa eri laitevalmistajien välisen tiedonsiirron: kaikki kun käyttävät samoja standardeja. Kuitenkin joskus vihamielinen toimija hyödyntää raajapintojen suunnitteluun jääneitä heikkouksia luoden haittaohjelmia, ja saa täten kerrokset toimimaan toisiaan vastaan. Yhtenä mainittavana heikkoutena on TCP-protokollan (Transmission Control Protocol) ominaisuus istunnon (engl. session) muodostuksessa. (Granlund 2007: 7–8).

Koska nykyään tiedonsiirtokanavien tarjonta on lisääntynyt ja tiedonsiirto nopeutunut, OSI-mallia täydentämään on luotu ns. TCP/IP-malli. Vaikka internet on yleisin tunnettu tietoverkkojen yhteenliittymä (ja se toimii pääosin TCP/UDP/IP -protokollapinon päällä), voidaan OSI-mallia käyttää myös muiden tiedonsiirtoratkaisujen kuvaukseen.

2.2.2 Fyysinen ja siirtokerros

OSI-mallin kaksi alinta kerrosta, fyysinen ja siirtokerros, huolehtivat tiedon siirrosta laite- ja bittitasoilla. Tällöin ylempien kerrosten toteutuksessa ei tarvitse ottaa kantaa siihen, miten eri tiedonsiirtokanavaa (sähkökaapelia, radiotietä, valokuitua yms.) pitkin tieto lopulta siirretään. Ylemmät kerrokset huolehtivat nopeimman reitin valinnasta, fyysinen ja siirtokerros huolehtivat reitistä itsestään.

Nimensä mukaan OSI-mallin alin, eli fyysinen kerros on tiedonsiirron fyysisen kanavan huolehtimista. Täällä varmistetaan, että tietopaketti paketoidaan oikein, siirretään oikein ja puretaan oikein. Fyysisellä kerroksella on ainoastaan tarkoituksena tarjota toimiva siirtotie, se ei ota kantaa tiedon pirstoutumiseen, kokoon taikka sisältöön. Toki isommalla tietopaketilla kestää joitain siirtoteitä pitkin kauemmin siirtyä, mutta fyysinen kerros siirtää sitä aina bitti kerrallaan eteenpäin.

Siirtokerros, layer 2, toimii yhdessä fyysisen kerroksen kanssa luoden jatkuvasti eri reittejä laitteiden välille. Näissä kahdessa kerroksessa tapahtuvan logiikan ansiosta ylemmät reitityspäätökset voidaan tehdä nopeasti. Kun fyysinen kerros vain siirtää bitti kerrallaan tietoa eteenpäin, on siirtokerroksen tehtävänä huolehtia siirtotien varaamisesta (fyysiseltä kerrokselta) ja virheiden havainnoista, virheiden korjauksesta sekä tietovuodosta (bit overflow). Näitä kahta siirtokerroksen tehtävää nimitetään MAC- (Medium Access Control) ja LCC (Logical Link Control)-kerroksiksi.

Siirtokerroksella huolehditaan laitteiden ylempien kerrosten yhdistämisestä loogisiin yhteyksiin. ARP-taulua eli (Address Resolution Protocol) ylläpitämällä ja kyselyitä suorittamalla siirtokerroksella voidaan yhdistää verkkokerroksen IP-osoitteet loogisiin MAC-osoitteisiin. Näin nopeutetaan tiedonsiirtoa siirtokerroksella ja ylläpidetään taulukkoa toimivista loogisista yhteyksistä. (Granlund 2007: 6–9.)

2.2.3 Verkkokerros

OSI-mallin kolmas kerros eli verkkokerros huolehtii tietopaketin siirrosta verkkojen välillä. Alempia kerroksia hyödynnettäessä voidaan verkkokerroksella toimiessa viestiä suoraan loogisten verkkojen välillä, IP- tai muuta vastaavaa protokollaa hyödyntäen.

Loogiset verkkoyhteydet tarkoittavat, että samassa verkossa olevat koneet voivat keskustella (vaihtaa paketteja) nopeammin ja etsiä myös muita samassa verkossa olevia koneita esim. ARP-kyselyitä hyödyntämällä. Verkosta on myös reititystieto muihin verkkoihin, eli paketti löytää lopulta tiensä reitityksen ansiosta seuraavaan kohteeseensa.

Verkkokerroksella toteutetaan myös ip-pakettien reititys. Internetissä on käytössä useita eri reititysprotokollia, joita yhdistelemällä saadaan mahdollisimman kattava ja hyvä reitti varmistettua paketille. Toisin kuin piirikytkentäisessä, pakettikytkentäisessä ei löydettyä reittiä varata yhdelle yhteydelle, vaan se voi olla useiden yhteyksien käytössä. Samoin pakettien reitti voi muuttua kesken mahdollisten verkkovikojen seurauksena, ilman että yhteyden käyttäjän tarvitsee reagoida tähän mitenkään.

Verkkokerroksella on yleensä käytössä IP-protokolla tiedonsiirtoa varten. IP-protokollalla kommunikoidaan IP-osoitteiden avulla, joista tunnistetaan kohde ja lähdekoneet. Verkkokerroksella voidaan siirtää myös ICMP-protokollan viestejä. ICMP (Internet Control Message Protocol) on tarkoitettu nopeaan kohdelaitteen testaukseen, eikä sitä ole suunniteltu sisältämään tietoa. Aktiiviverkkolaitteet vastaavat ICMP-viestiin oletuksena, ja sen avulla voikin selvittää, mihin asti verkkokerroksen yhteydet on luotu reitillä lähteestä kohteeseen. Käytettyjä ICMP-paketin lähettäviä komentoja ovat ping ja traceroute. (Granlund 2007: 9.)

2.2.4 Kuljetuskerros

OSI-mallin neljäs kerros eli kuljetuskerros hyödyntää muiden OSI-mallin kerrosten mukaan alempien kerrosten rajapintoja. Alemmalla verkkokerroksella tapahtuneet reititysmuutokset näkyvät viiveinä ylemmille kerroksille. Paketit voivat tulla myös muutoksista johtuen aivan eri järjestyksessä perille, kuin ne on lähetty. On neljännen kerroksen tehtävänä huolehtia pakettien oikeasta järjestyksestä ja siirrosta ylempien kerrosten käyttöön. Tähän OSI-mallin neljäs kerros ottaa käyttöön istunnot (engl. Session).

Tietoliikennettä on kerroksella kahta eri tyyppiä; yhteydellistä ja yhteydetöntä. Yhteydellisessä liikenteessä varmistetaan jokaisen paketin tulo kuittaamalla se takaisin lähettäjälle, yhteydettömässä tätä ilmoitusta ei tehdä / tarvita. Yhteydellisestä tiedonsiirrosta mainittakoon esimerkkinä TCP, yhteydetön puolestaan UDP (User Datagram Protocol).

TCP-protokollassa vastaanottaja avaa aina uuden istunnon saadessaan ensimmäisen paketin lähettäjältä. Tätä istuntoa protokolla käyttää järjestämään pirstoutunutta pakettijonoa oikeaan järjestykseen. Vasta kun paketit on saatu oikein koottua ja järjesteltyä, lähettää vastaanottaja kuittauksen lähettäjälle.

UDP protokollassa paketit lähetetään viiveettä eteenpäin ilman kuittauksia vastaanottajan ja lähettäjän välillä. UDP sopiikin välittömän tiedon (esimerkiksi anturin lähettämän tiedon) välitykseen. TCP puolestaan on hyödyllinen, kun halutaan siirtää suurempia määriä tietoa ja varmistaa sen eheys. (Ruohonen 2002: 14–38.)

2.2.5 Yhteys-, istunto- ja sovelluskerros

OSI-mallin ylemmät kerrokset, 5. 6. ja 7.kerros, toimivat käyttöjärjestelmän osana. Kun alempia kerroksia hyödynnetään yksinkertaisimmissa verkkolaitteissa (kytkimet, reitittimet, palomuurit), ovat nämä ylemmät kerrokset päätelaitteiden hyödyntämiä. Yksittäisellä reitittimellä ei ole tarvetta purkaa tietoa hankalasti esityskerroksiin vain sen eteenpäin välitykseen. Reititystä varten riittävät vain kerrokset 1–3 (joskus myös 4).

Tähän sääntöön tuovat poikkeuksen viime aikoina yleistyneet UTM- (Unified Thread Management) -laitteet. Nämä palomuuri- ja IPS (Intrusion Prevention System) -laitteet huolehtivat yritysten tietoverkkojen reunojen tietoturvasta ja simuloivat käyttäjän toimia toimessaan. Aikaisemmin riitti, että estettiin ei-toivotut ulkopuoliset yhteydet järjestelmällisesti (sulkemalla tietyt portit yms.) ja sallittiin sisäverkosta lähtevät pyynnöt ja niihin vastaukset. Oli päätelaitteen vastuulla huolehtia omasta tietoturvastaan. Nykyään UTM-laitteet keräävät, purkavat, avaavat ja tutkivat kaikki laitteen läpi liikkuvat tietopaketit. Näin niidenkin tarvitsee hyödyntää ylempien OSI-mallin kerrosten rajapintoja.

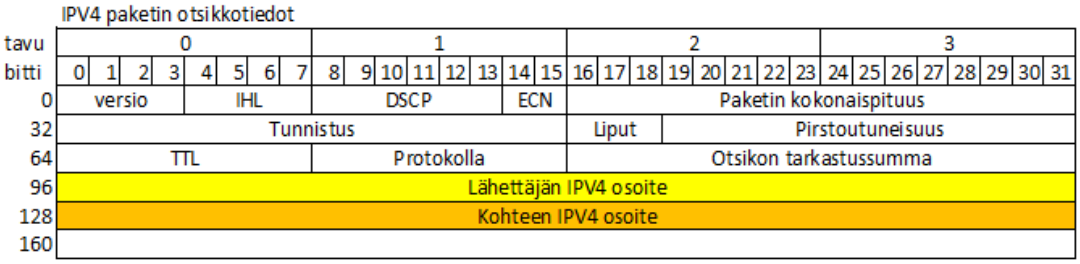
Käyttöjärjestelmä tarjoaa ohjelmille usein automaattisesti mahdollisuudet tiedonsiirtoon – riippuu siis käyttöjärjestelmän logiikasta, kuinka ylempiä kerroksia käytetään. Tiedonsiirron kanssa esiintyvä ongelma voi hyvinkin olla ohjelmallinen – eli käyttöjärjestelmän ja ohjelman välinen vikatilanne luo käyttäjälle tunteen, että ohjelma on rikki eikä tieto-

verkko toimi. Käyttöjärjestelmien tavoissa huolehtia tietopaketista on havaittu myös heikkouksia – tällöin pahimmassa tapauksessa käyttöjärjestelmä suorittaa verkosta latautunutta haittaohjelmakoodia kysymättä lainkaan käyttäjältä.

Ylemmät OSI-mallin kerrokset on luotu mahdollistamaan eri käyttöjärjestelmien välistä tiedonsiirtoa. Kun kaikki järjestelmät hyödyntävät samoja rajapintoja samalla tavoin, tiedonsiirto onnistuu. Muiden kerrosten tavoin ylimmät kerrokset ovat riippuvaisia alemmista ja niiden rajapinnoista viestinnässään. (Ruohonen 2002: 14–52. ; Granlund 2007: 6–11.)

2.2.6 IP-osoite

Laajalti käytössä on Internet Protocol-osoitteisto – versio 4, lyhyemmin IPV4. IPV4 toimii OSI-mallin verkkokerroksella ja huolehtii valtaosan internetiin liitettyjen koneiden reitityksestä. Käytännössä jokaisella tietokoneella, joka on liitetty internetiin, on oma yksilöllinen IP-osoitteensa. Koneen internetiin lähettämät paketit merkitään lähettävällä IP-osoitteella ja paketteihin merkitään kohdekoneen IP-osoite.



Kuva 2. Ipv4-paketin osoitteisto.

IPV4 osoitteisto koostuu useista toisiaan tukevista osista (ks. kuva 2):

- *Versio* kertoo käytettävän IP-version.
- *IHL: Internet Header Lenght* kertoo otsikkotietojen pituuden.
- *DSCP ja ECN* (Differentiated Services Code Point, Explicit Congestion Notification) ovat paketin palveluluokka, millä kiireellä paketti kuuluu reitittää.
- Paketin kokonaispituus tavuina. Mikäli kaikki lähetettävä data ei mahdu yhteen pakettiin, tarvitsee paketteja pilkkoa.

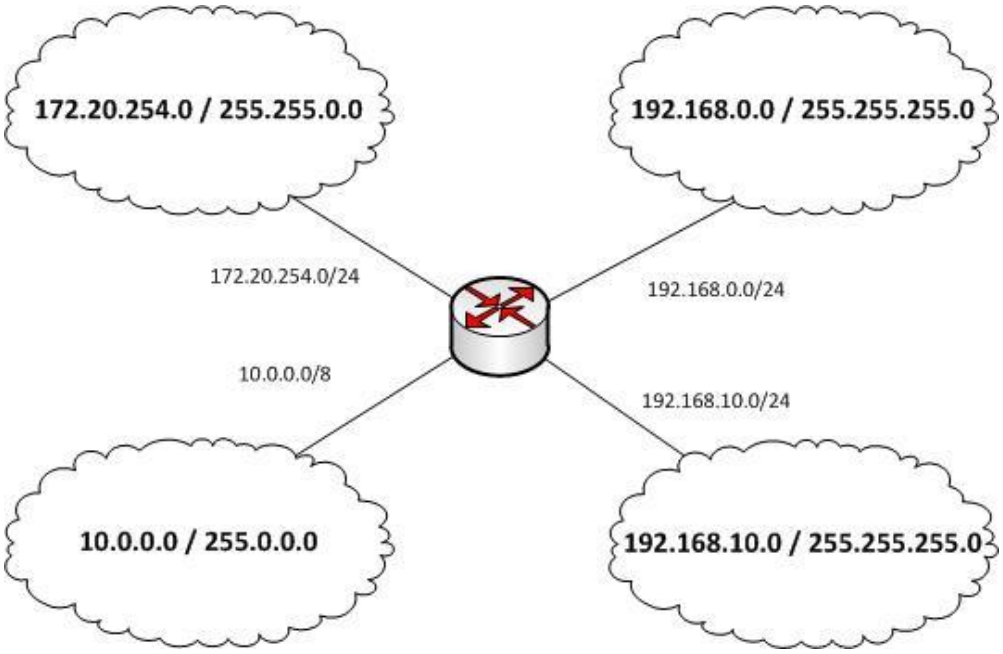
- Tunnistus. Mikäli paketteja on jouduttu siirron aikana pilkkomaan, käytetään tunnistuskentän tietoa niiden kokoamiseen.
- Liput. Ovat bittejä, jotka kertovat, mikäli paketti on pirstoutunut tai mikäli sitä ei saa pirstoa.
- Pirstoutuneisuus, kertoo, mihin kohtaan pilkottua pakettia tämä paketti kuuluu.
- *TTL*, Time To Live, kertoo kuinka kauan paketilla on elinaikaa. Tämä tavu määrää, kuinka kauan pakettia lähetetään eteenpäin.
- Protokolla. Mitä protokollaa käytetään Kuljetuskerroksella (esimerkiksi ICMP, TCP, UDP, IP).
- Otsikon tarkastussumma on summa jonka avulla voidaan varmistaa, ettei otsikkotieto ole muuttunut paketin matkan aikana.
- Lähettäjän ja Kohteen IPV4-osoitteet bitteinä.

IP-osoitteisto koostuu 32-bittisistä osoitteista (4 tavua). Tämä rajoittaa käytössä olevat osoitteet 4 294 967 296 yksilölliseen osoitteeseen. Nämä IPV4-osoitteet loppuivat helmikuussa 2011. Tällöin osoitteistusta hallinnoiva IANA (Internet Assigned Numbers Authority) jakoi viimeisen vapaan olleen IPV4-verkkoavaruuden.

IPV4 osoite koostuu itse osoitteesta ja osoitteen aliverkon peitteestä. Tällöin osoite voi olla esimerkiksi (desimaalimuodossa):

172.20.254.1 ja aliverkon peite *255.255.0.0*.

Jokaisesta aliverkosta on oletusyhdyskäytävä seuraaviin verkkoihin, joita kautta liikenne ohjataan, jos konetta tai verkkoa ei löydy nykyisestä. Näin samassa lähiverkossa toimivat laitteet voivat kommunikoida keskenään vaivattomasti suoraan koneelta koneelle ilman, että liikenne kiertää internetin tai reunareitittimen kautta (kuva 3). (Granlund 2007: 269–280.)



Kuva 3. 4 eri aliverkkoa yhdistettynä toisiinsa.

IP-verkot on jaettu aliverkkoihin. Jaetun verkon viimeinen osoite on varattu verkon mainostukseen (BROADCAST) ja ensimmäinen osoite aliverkon osoitteeksi (NETWORK). Verkon mainostukseen varattuun osoitteeseen lähetetyt pakettiin vastaavat oletuksena kaikki samassa verkossa olevat laitteet. Aliverkon osoitteeseen lähetetyt paketit reitittyvät, mutta mikään laite verkosta ei vastaa niihin oletuksena.

IPV4-osoitteiden loppumisen takia on kehitetty IPV6-osoitteistus, joka on 128-bittinen osoitteistus. Tällöin käytössä on 340 sekstiljoonaa yksilöllistä osoitetta. Näiden loppuminen ei ole lähiaikoina ajankohtaista.

IPV4-osoitteiden loppumista on hidastettu aliverkottamalla ns. lähiverkkoihin ja käyttämällä NAT (Network Address Translation) -tekniikkaa. Tällöin yhden julkisen IP-osoitteen takaa voi liikennöidä isokin aliverkko. Lähettävä IP-osoite vaihdetaan NAT-muunnoksessa sisäverkon osoitteesta julkisen verkon osoitteeseen automaattisesti ja NAT-muunnoksen toteuttava laite pitää kirjaa osoitemuutoksistaan ja osaa reitittää paluupaketit oikeaan sisäverkkoon / oikeaan koneeseen. (Ruohonen 2007: 22–23., 80–85.)

Internet on suunniteltu IPV4-osoitteiden varaan. Alun perin suljetuksi tarkoitettu protokolla luottaa, että käyttäjä on rehellinen eikä väärennä mitään osioita lähettämästään

paketista. IPV4 liikenteessä ei tarvitse varmentaa lähettäjän ip-osoitetta erikseen vaan luotetaan lähettäjän olevan se, joka merkitsee pakettiin. Väärentäessään paketin lähettäjä-osoitteen vihamielinen taho voi näin luoda näennäisesti eri lähteestä tulevaa liikennettä. (Ruohonen 2002: 14–28.)

2.3 TCP- ja UDP-portti

Liikennöitäessä TCP/UDP-protokollilla tulee lähetettävään IP-pakettiin kirjata myös lähtevän liikenteen lähetysportti ja kohdeportti. TCP- ja UDP- liikenne toimii OSI-mallin kuljetuskerroksella, joten porttitieto lisätään alemman IP-kerroksen tuottamaan pakettitietoon. UDP-paketin osoitekentät ovat lyhyempiä ja täten kevyempiä, vaikka IPV4-protokollassa siihen lisätäänkin lähde- ja kohde-osoitteet.

TCP paketin otsikkotiedot

Bitti	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Lähdeportti (65535 eri porttia)																Kohdeportti (65535 eri porttia)															
32	paketin järjestysnumero																															
64	Kuittausnumero																															
96	Otsikon pituus				Varaus						Liput						Ikkunan koko															
128	Tarkistussumma (checksum)																Kiireellisyysosoitin															
160	Optiot ja täyte																															
192	Data alkaa																															

UDP paketin otsikkotiedot

Bitti	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Lähdeosoite (ipv 4)																															
32	Kohdeosoite (ipv4)																															
64	Tyhjänä								Protokolla (portti)								UDP paketin koko															
96	Lähdeportti (65535 eri porttia)																Kohdeportti (65535 eri porttia)															
128	Pituus																Tarkistussumma (checksum)															
160	Data alkaa																															

Kuva 4. TCP-portti ja UDP-portti ip-paketin otsikkokentässä (Ruohonen 2007: 30–35)

Jokaisella TCP- ja UDP-paketilla on lähettävä portti ja kohdeportti (ks. kuva 4). Porttinumero on 16-bittinen, eli desimaalina välillä 1 ja 65 535. Portit voidaan jaotella kolmeen kategoriaan:

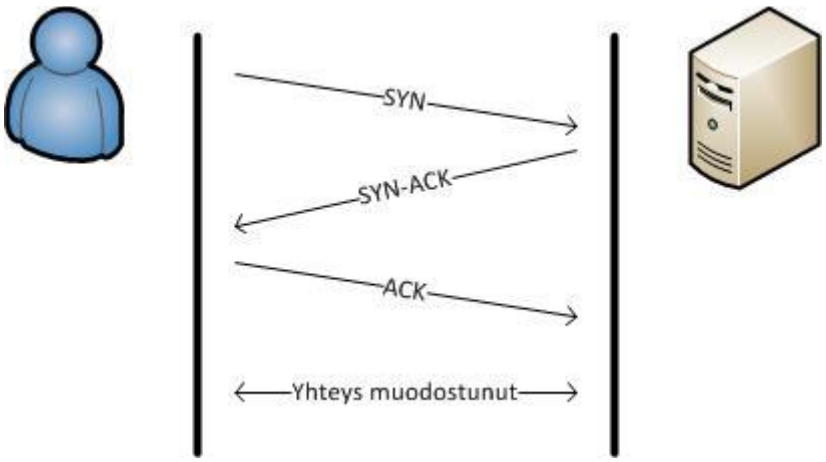
- tunnetut portit (1–1023)
- rekisteröidyt portit (1024–49 151)
- dynaamiset tai yksityiset portit (49 152–65 535).

Tunnetuista porteista ja niiden rekisteröinnistä vastaa IANA. Tunnettuja portteja ovat esimerkiksi:

- 22 & 21 – FTP (File Transfer Protocol)
- 22 – SSH (Secure Shell)
- 80 – HTTP (Hypertext Transfer Protocol)
- 443 – HTTPS (HTTP Secure)

Näihin kohdeportteihin on siis sovittu liikennöitävän vain tietyn tyyppistä liikennettä. http-verkkosivu vastaa yleensä portista 80 – näin esim. internetselain osaa ottaa automaattisesti siihen porttiin yhteyden ja hakea verkkosivun onnistuneesti.

IP-osoite ja portti muodostavat uniikin parin. Kun lähettävä kone varaa lähettävän portin liikenteelle, tulee sen pitää sama portti liikennöinnissä koko liikenteen ajan. Palvelin vastaa samalle portille koko liikenteen ajan. TCP-liikenteessä tehdään myös niin sanottu TCP-kättely jokaisen paketin kohdalla. Liikenne alkaa TCP -SYN ja -ACK viesteillä kuvassa 5 esitettyyn tapaan.



Kuva 5. TCP-kättely. Yhteyden muodostuttua voidaan lähettää dataa laitteiden välillä.

Näin varmistetaan jokaisen paketin eheys ja perillepääsy. Istunto, jonka kohdekone ja lähdekone avaavat, sisältää tiedot käytössä olevista IP-osoite-porttipareista. Näin varmistetaan, että liikenne ohjautuu oikeaan paikkaan, eikä jollekin muulle asiakaskoneelle.

TCP-protokollaan kuuluu määrittelynä paketin elinikä (kuinka kauan paketti kiertää etsien kohdettaan) sekä paketin maksimikoko. TCP:ssä on myös määritelty toimet, sille mitä tehdä, jos paketti häviää matkalle. Tämä näkyy asiakkaalle yleensä siten, ettei SYN-ACK-viesti koskaan saavu palvelimelta vahvistamaan kättelyä. Tällöin asiakas lähettää SYN-viestin uudelleen kohteeseen.

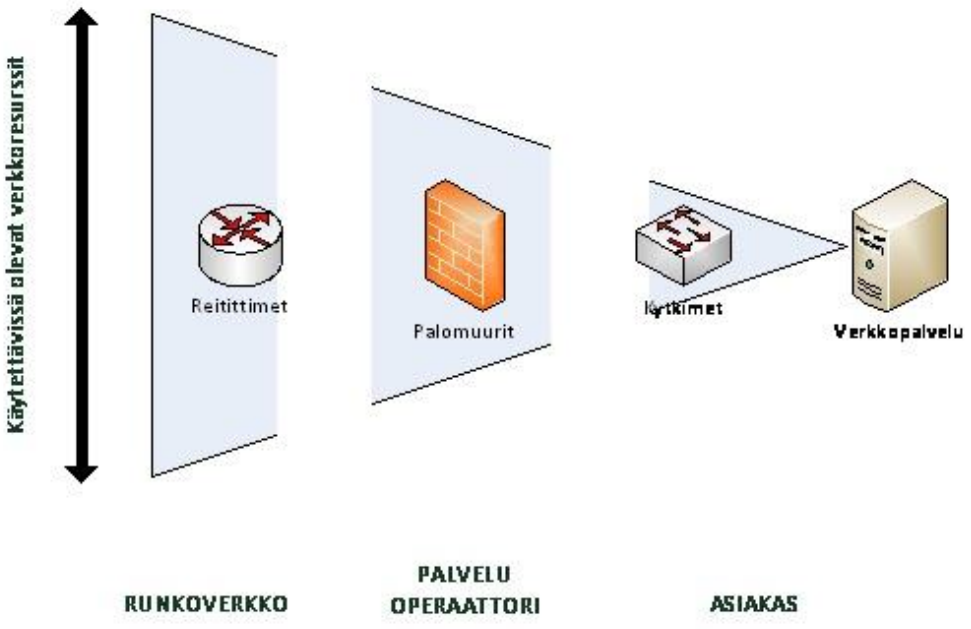
UDP:n yhteydettömässä liikennöinnissä edestakaista kättelyä ei joka paketille tehdä mutta siinäkin on käytössä portti- ja IP-parit.

Palvelinkoneella tulee olla ohjelmisto, joka kuuntelee tiettyä porttia. Esimerkiksi HTTP (Hypertext Transfer Protocol)-nettisivuliikenteelle tulee olla ohjelmisto päällä, joka kuuntelee ja käsittelee porttiin 80 tulevia HTTP-pyyntöjä. HTTP- ja muilla sovelluskerroksen protokollilla on oma yksilöivä tapansa välittää tietoa. Nämä protokollat paketoidaan TCP liikenteeseen kuorman sisään, ja näin niitä ei avata alemmissa (Layer 3,4) kerroksen reitityspäätöksissä. (Ruohonen 2002: 106–115.)

3 Tietoverkkoturvallisuus

3.1 Tietoturva-ajattelu

Tietoturvallisuus muodostuu useasta tasosta: Internet-palveluntarjoajasta (ISP), organisaation aktiivilaitteista (palomuurit, reitittimet), organisaation palveluista (tiedosto- yms. palvelimet /palvelut) sekä organisaation työasemasta / käyttäjästä (ks. kuva 6).



Kuva 6. Kolmitasoinen tietoturva.

Tietoverkkoturvallisuuteen kuuluu myös erottamana osana fyysinen turvallisuus. Fyysisen turvallisuuden tulee olla ajan tasalla niin toimipisteiden kuin palveluiden ja verkon osalta. Fyysistä turvallisuutta on kulunvalvonta tiloissa, joissa verkkolaitteet toimivat ja tarvittaessa verkkolaitteiden, ja -yhteyksien fyysinen turvaaminen.

Tietoverkkoturvallisuuden rinnalla mainitaan myös kyberturvallisuus. Nykyajan yhteiskunnassa, jossa myös monet kriittiset yhteiskunnalliset laitokset (vesi-, sähkölaitokset, liikenteenohjaus yms.) on kytketty tietoverkoin toisiinsa, tulee tietoverkkoturvallisuudesta kyberturvallisuutta.

Nykyajan käsitteen mukaan tällainen tietoverkko, johon on kytketty myös tuotannollisia järjestelmiä on kyberverkko. Käsitteen mukaan yhteen internetpalveluun kohdistuva hyökkäys on tietoverkkohyökkäys – koko verkostoon kohdistuva hyökkäys on kyberhyökkäys. (Hyppönen 2013.)

Maailmalla ei ole vielä koettu aitoa kybersotaa, sodan käsitteenä on kuitenkin ”kahden tai useamman järjestön välistä aseellista konfliktia”. Lähimmäksi aitoa kybersotaa onkin päästy Viron pronssipatsaskiistojen 2007 ja Georgian konfliktin 2008 yhteydessä. Myös Ukrainan kriisistä 2014 on ollut nähtävissä kybersodan aineksia. Myös informaatiosodan voidaan lukea kuuluvaksi kybersotaan. (Hyppönen 2013.)

3.2 Verkkohyökkäyksen käynnistäjä

Verkko- tai kyber-hyökkäyksen käynnistäjä voidaan luokitella seuraavasti (Hyppönen 2013):

- Valtiollinen
  - Poliisi / syyttäjä
  - Suomessa poliisi saa vuoden 2014 alusta suorittaa verkkohyökkäyksiä rikostutkinnan yhteydessä.
- Rikollinen
  - Tarkoituksena rahallinen hyöty
  - Myyvät botnet-verkkoja, joita voi käyttää palvelunestohyökkäyksiin.
- Sotilaallinen
  - Valtion sotilasstrategiaan voi kuulua tietoverkkosodankäynti.
  - Aktiivisia ohjelmia ainakin Yhdysvalloilla, Venäjällä sekä Kiinalla.
  - Suuret toimijat ja valtavat budjetit – ammattimainen toiminta
- Aktivisti, terroristi, amatööri
  - Tarkoituksena kiusan aiheutus tai näkyvyyden hankinta
  - Yleisin palvelunestohyökkäyksen käynnistäjä
  - Pienin rahoitus – amatööritason toimintaa
  - Script-kiddiet – kokeilunhalu

Eri toimijoilla on luonnollisesti eri tarkoitukset toimilleen. Tässä työssä tutustutaan ensisijaisesti aktivistien käynnistämiin palvelunestohyökkäyksiin. Mainituista toimijoista aktivisti kaipaa eniten näkyvyyttä toimelleen – motiivina voi toimia epäonnistunut asiakaspalvelu, koetun vääryyden korjaaminen tai vain kokeilunhalu.

Verkkohyökkäyksen käynnistämiseen ei nykyään tarvita juurikaan osaamista. Internetin hakukoneita käyttämällä voi löytää siistit käyttöohjeet ja valmiit asennuspaketit hyökkäyksen käynnistämiseen. Näin kynnys hyökkäyksen tekemiseen voi olla hyvinkin matala. (Hyppönen 2013.)

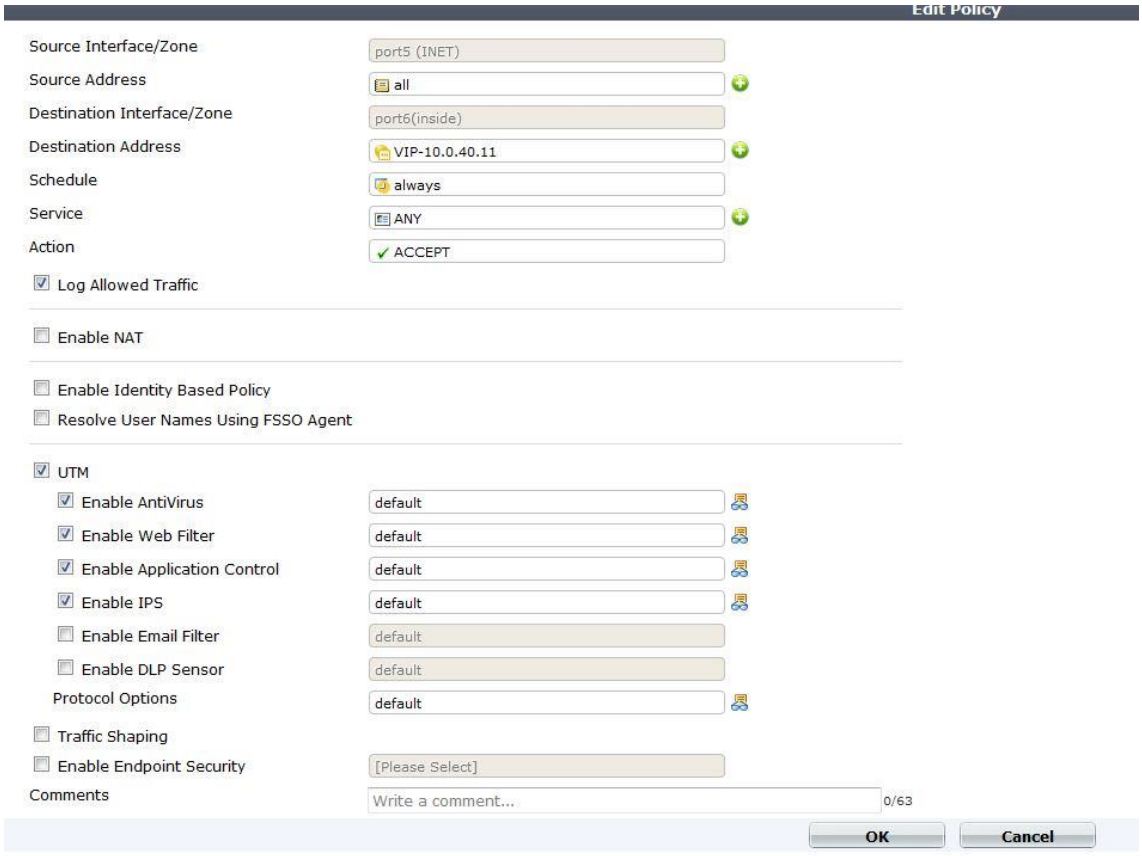
3.3 UTM-palomuurit

Perinteisesti verkkohyökkäyksiltä on suojauduttu palomuurein ja IPS/IDS-järjestelmin oman tietoverkon ulkoreunalla. Usein yrityksestä on vain yksi reitti internetiin jolloin tämän reitin turvaaminen on ollut tarpeeksi. Ulkoverkoista tulevat yhteydet on rajoitettu palomuurein tarkasti vain haluttuihin avoimiin palveluihin, sisäverkosta sallitaan kaikki yhteydet ulkomaailmaan. Näin verkkohyökkäykselle on ollut vain yksi kanava tunkeutumiselle, joka on ollut verrattain helppo torjua.

Tilanne on kuitenkin muuttunut; vihamieliset ohjelmistot leviävät usb- ja muiden muistien avulla, internet-yhteyksiä voi yrityksen sisäverkosta olla useita (wlan, 3g/4g) , ja vihamielinen koodi osataan nykyään pakata sallitun liikenteen sekaan. Näin sen rajoittaminen vanhalla yksinkertaisella palomuuritekniikalla on vaikeaa. Lisäksi käyttäjät olettavat nykyään saavuttavansa internet-palvelut helposti ja nopeasti kaikkialta.

UTM (Unified Threat Management)-ratkaisut yrittävät vastata uusien haittaohjelmien ja virusten piiloutumiseen normaalin liikenteen sekaan. 2000-luvulla yleistyneet ratkaisut voivat sisältää perinteisen palomuurin lisäksi IPS-ominaisuudet, virustorjuntaa (AV), roskapostisuodattimia, sisällönsuodatusta (www-sivujen), tietovuotojen hallinnointia (DLP) sekä sovelluspohjaista raportointia. Perinteisen palomuuritoiminnan lisäksi UTM-muuri avaa IP-paketin OSI-mallin sovelluskerroselle asti. Näin UTM-muurissa voidaan valvoa myös paketin sisällön perusteella tietoliikennettä.

UTM-skannaukset integroidaan palomuurisääntöihin, joissa voidaan määritellä lähde ja kohde tarkasti protokollan tarkkuudella (Kuva 7).



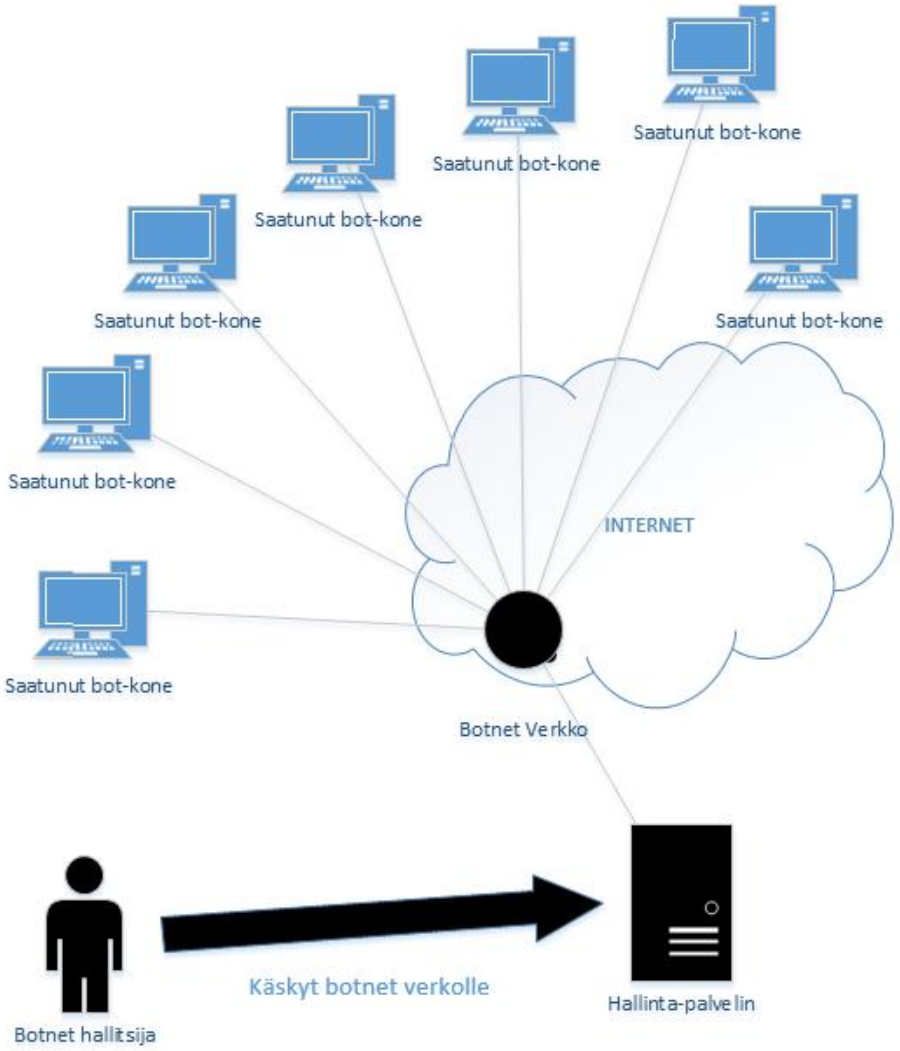
Kuva 7. UTM-palomuurisääntö. Käytössä on virustutka, websivujen luokitus sekä rajoitus ja ohjelmistojen tarkkailu- ja tunkeutumisenestojärjestelmät (IDS/IPS).

UTM-ratkaisut ovatkin muodostuneet palomuurien seuraavaksi kehityssuunnaksi. Yksittäinen UTM-palomuuri ei kuitenkaan takaa aukotonta tietoturvaa, muuri valvoo vain yhtä yhdyskäytävää lähiverkon ja internetin välillä. Mikäli haittaohjelman liikenne ei kulje UTM-laitteen kautta, ei siitä voida luoda hälytytystä tai rajoittaa sitä. Siksi tulee huolehtia myös oman lähiverkon asiakaslaitteiden paikallisesta tietoturvasta. (Fortinet UTM Solution Guide. 2014)

3.4 Verkkohyökkäysten vertailua

Valtaosa internetissä leviävistä haittaohjelmista on automatisoituja, ne tekevät omaa toimintaansa tietyn kaavan mukaan. Haittaohjelmilla on oma tarkoituksena; osa luo kohdekoneesta osan bot-verkkoa, osa aloittaa kohdekoneelta roskapostituksen ja osa jää vain seuraamaan käyttäjän toimia. (Hyppönen 2013.)

Riippuu hyökkäyksen käynnistäjästä, millainen haittaohjelma on tarkoitukseen varattu. Rikollisille tärkeintä on saavuttaa mahdollisimman laaja määrä saastuvia koneita liitettäväksi omiin botnet-verkkoihinsa. Valtiollisille sekä sotilaallisille toimijoille puolestaan tärkeintä voi olla saada kohdejärjestelmästä tietoja, ilman että järjestelmänvalvojat huomaavat vierailua. Aktivistien ja amatöörien tarkoituksena on puolestaan luoda mahdollisimman paljon näkyvyyttä toimillaan.



Kuva 8. Botnet-verkon toiminta

Botnet-verkossa haittaohjelman saastuttama kone ottaa yhteyttä verkon hallintapalvelimeen. Verkon hallitsija voi tuon hallintapalvelimen kautta jakaa käskyt koko verkolle samaan aikaan (kuva 8). Viestit menevät huomaamattomina saastuneen koneen normaalin verkkoliikenteen seassa. Tällöin myös botnetin hallitsija voi myös sijaita missä

vain internetissä, ilman että häntä saadaan koskaan paikallistettua. Botnet-verkon koneita taitava hallitsija voi käskyttää jopa aivan samoin kuin olisi kirjautuneena paikallisesti. (Defecting DDOS Attacks 2014.).

Nykyään hyvin suojattuun kohdejärjestelmään tunkeutuminen vaatii haittaohjelman ujuttamista järjestelmän sisään. Yksinkertaisimmillaan tämä on internet-sivun linkki, joka ohjaa käyttäjän selaimen lataamaan haittaohjelman. Haittaohjelma luo tällöin takaportin järjestelmään ja alkaa viestiä oman ohjauskoneensa kanssa.

Tällaiset isoa määrää tavoittelevat haittaohjelmat huomataan suhteellisen nopeasti. Ohjelma toimii aina samalla logiikalla – usein samalla ohjelmistokoodilla. Näin sen tunnistaminen helpottuu. Verkkoselainten toimittajat reagoivat selaimensa heikkouksiin päivityksin ja antivirustoimittajat päivittävät omat virustietokantansa tunnistamaan uuden haittaohjelman. Tästä syystä tuleekin pitää niin paikallisen koneen virustorjunta kuin aktiivilaitteiden (UTM) päivitykset ajan tasalla.

Verkkohyökkäys voidaan kohdistaa internetin suuntaan avoimeen palveluun esim. http-sivuun. Jos palvelu toimii palomuurin takaa, tulee siihen sallia yhteydenotot internetin puolelta. Tällöin tulee palvelua ylläpitävän järjestelmän olla ajan tasalla. Varsin usein sivuston taustalla toimiva julkaisupalvelu (CMS, Content Management System) sisältää tunnetun heikkouden, joka altistaa järjestelmän hyökkääjälle.

CMS-järjestelmät ja yritysten verkkosivut on usein eristetty itse yrityksen tuotantoverkosta. Näin turvataan yrityksen tuotannon jatkuvuus, vaikka julkiset verkkosivut joutuisivatkin hyökkäyksen kohteeksi. Hyvin usein verkkosivut ovat kuitenkin tärkein viestintäkanava yrityksen ja asiakkaiden välillä. Viestinnän katkeaminen johtaa helposti siihen harhaluuloon, että koko yrityksen toiminta on lamaantunut, vaikka vain yksi verkkopalvelu estynyt. Siksi on hyvä, että yrityksissä on varauduttu myös toissijaisten viestintäkanavien käyttöön (esimerkiksi Twitter, Facebook, Sähköposti) tällaisen tilanteen tapahtuessa.

Riippuu hyökkääjän tavoitteista, millaista hyökkäystyyppiä hän käyttää. Huomaamattoman tunkeutumisen mahdollistavat räätälöidyt haittaohjelmat ovat työläitä valmistaa ja käyttää. Niiden luomiseen vaadittavat resurssit voivat olla reilusti yli mahdollisten hyötyjen. (Hyppönen 2013.)

Aktivistien tarkoituksena on usein saada mahdollisimman paljon näkyvyyttä toimilleen. Tällöin vaivihkainen tunkeutuminen kohteen järjestelmään ei välttämättä ole helpoin keino. Aktivistit pyrkivätkin murtamaan sivustojen julkaisuohjelmia haavoittuvuuksien kautta ja toteuttamaan palvelunestoja saadakseen näkyviä reaktioita.

4 Palvelunestohyökkäys ja hajautettu palvelunestohyökkäys

4.1 Palveluneston tavoite

Palvelunesto on verkkohyökkäyksistä näkyvin. Verrattaessa perinteiseen sodankäyntiin, palvelunestohyökkäys on kuin aluepommitus. Hyökkäyksen tavoitteena on halvaannuttaa kohteen toiminta (palvelu). Tämä on hyvin näkyvä toimi, varsinkin jos uutismediat reagoivat tapahtumaan.

Palvelunestohyökkäyksen suuren näkyvyyden vuoksi sitä voidaan myös käyttää harhauttamiseen. Mikäli järjestelmään tunkeutunut hyökkääjä havaitsee esimerkiksi kohteen IT-osaston aloittaneen puolustustoimet, voidaan palvelunestohyökkäyksellä siirtää kohteen huomio toisaalle. IT-osastot keskittyvät tällöin mitigoimaan ja torjumaan palvelunestoa antaen hyökkääjälle lisäaikaa huomaamattomalle toiminnalleen.

Palvelunestolla tavoitellaan lamauttavaa vaikutusta. Kohteen näkyvää toimintaa lamautetaan ja luodaan kuvaa kohteen koko toiminnan epävarmuudesta. Usein aktivistien ollessa kyseessä julistautuvat he hyökkäyksen tekijöiksi jostain tietystä syystä.

Kybersodassa voidaan palvelunestoilla pyrkiä lamauttamaan suurempia kokonaisuuksia. Tällöin kohteena ovat yhteiskunnan toimilta kriittiset järjestelmät ja tietojärjestelmät. Yleensä tällainen systemaattinen hyökkäys liittyy suurempaan kriisiin, jolloin yhteiskuntakin reagoi siihen. Teoriassa palvelunestohyökkäyksellä on mahdollista lamauttaa ainakin osa yhteiskunnan tietoverkosta toimimattomaksi. (Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks. 2002.)

4.2 Palveluneston vaikutukset

Palvelunestohyökkäyksen tavoite on saada estettyä jonkin tietyn palvelun käyttö käyttäjiltä. Tällöin hyökkääjä käyttää palvelua tarjoavan osapuolen kaikki resurssit omaan liikenteensä, estäen aitojen asiakkaiden liikenteen palveluun.

Palvelun resursseja ovat:

- internetyhteyden kapasiteetti (kaistan leveys)
- palomuuripalvelun resurssit (sessiot eli istunnot, UTM ominaisuuksien resurssit)
- palvelimen fyysiset resurssit (kuorma, muistinkäyttö, tallennustilat)
- palvelimen ohjelmistot (ohjelmointivirheet, haavoittuvuudet).

OSI-Layer 3- ja 4-hyökkäykset kuluttavat palvelimen, palomuurin ja palveluntarjoajan (ISP:n) fyysisiä resursseja. OSI-Layer 7 -hyökkäykset on suunnattu erityisesti palvelimen ohjelmistojen ohjelmointivirheisiin ja haavoittuvuuksiin. (Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks. 2014. ; Fortinet 2014.)

Kun verkkopalvelun toiminta ja ainoa tiedotuskanava saadaan lamautettua, aiheuttaa se käyttäjissä paniikkia ja huolestumista. Tämä huoli voi esimerkiksi pankin sivujen ollessa nurin näkyä pankin puhelinpalveluun huolestuneiden asiakkaiden tiedustellessa talletustensa perään. Verkkopalvelun toiminnan horjuttaminen heijastuu myös sitä ylläpitävän organisaation julkisuuskuvaan. Yleisö ja yhteistyökumppanit voivat todeta kohteen olevan epäluotettava kumppani ja siirtää toimintonsa toiselle palveluntarjoajalle.

Palvelunestohyökkäyksen noustessa julkisuuteen ruokkii se myös itseään. Kiinnostuneet käyttäjät yrittävät kirjautua myös kohdepalveluun lisäten sen kuormaa entisestään. Vaikutukset palvelunestosta ovatkin ensisijaisesti imagollisia. Yleensä yritys investoi hyökkäyksen jälkeen mitigointiin ja varatoimenpiteisiin, mutta menetettyä mainetta investoinnit eivät enää pelasta.

Mikäli estettävä palvelu on jokin rahaliikenteen tms. tuotannon kautta kriittinen, voidaan palveluneston vaikutuksia mitata myös rahassa. Esimerkiksi pörssitoiminnan onnistu-

nut lamauttaminen aiheuttaa niin välittömiä tappioita menetettynä kauppoina kuin välillisiä menetettynä luottamuksella.

4.3 Palveluneston kohteet

Yleisin palvelunestonyökkäyksen kohde on verkkosivu. Sen näkyvyyden esto on yksinkertainen toimi hyökkääjälle, ja se on hyvin näkyvää yleisölle. Verkkosivu kohteen kulissina toimii ilmiselvänä kohteena, vaikkei se vaikuttaisikaan kohteen tuotannon toimintaan. Lisäksi hyökkääjä voi helposti varmentaa hyökkäyksensä onnistumisen.

Palvelunesto voidaan kohdistaa kaikkiin avoimiin internetin palveluihin, mutta hyökkäyksen tavoite pysyy kaikissa samana; estää tai häiritä palvelun toimintaa. Muiden näkymättömien palveluiden häirintä voi johtaa välillisesti verkkosivun tavoittamattomuuteen (esimerkiksi DNS-nimipalveluiden häirinnällä verkkosivu www.metropolia.fi ei aukea automaattisesti käyttäjän selaimeen). Oikeaan paikkaan kohdistettu palvelunesto voi näin lamauttaa useampia verkkopalveluita.

Hyökkääjän ammattitaidosta riippuu, miten hyvin kohde saadaan tiedusteltua. Mitä tarkemmat tiedot kohteen järjestelmistä on käytössä, sitä lamauttavampi palvelunesto voidaan toteuttaa. Useimmat palvelunestot keskittyvät kuitenkin vain julkisen verkkosivun kaatoon.

Huonosti suunniteltu verkko ja hyvin toteutettu kohteen tiedustelu voivat teoriassa tarjota mahdollisuuden lamauttaa operaattorin koko runkoverkon tai osia siitä. Hyökkäyksellä voidaan pyrkiä estämään verkon operoinnin korjaustoimenpiteet, jolloin pahimmillaan verkko-operointi joutuu lähtemään korjaustoimenpiteitä varten fyysisesti paikan päälle. Nykyään kun palvelut on hajautettu maantieteellisesti, voi se olla aikaavievää ja jopa mahdotonta.

Yleisin Suomeen kohdistunut palvelunestohyökkäys on kohdistunut mediataloihin, vuoden 2007 Euroviisujen aikaan YLE:n verkkosivuihin ja Tapaninpäivänä 2012 useisiin mediataloihin (Nelonen, MTV, iltalehti) kohdistunut palvelunesto puhuvat tämän puolesta. Hyökkäyksen kohteilla on haettu näkyvyyttä lamauttamalla suosituimpia verkkopalveluitamme. Osa hyökkäyksistä torjuttiin ja niiden vaikutuksia vähennettiin (mitigoitiin).

Palvelunestohyökkäys ei etene automaattisesi kohteesta toiseen verkkomadon tavoin, vaan se täytyy aina kohdistaa tiettyyn palveluun.

Muita potentiaalisia kohteita Suomessa voivat olla esimerkiksi mielipiteitä nostattavien poliittisten toimijoiden verkkopalvelut, uskonnolliset järjestöt, tekijänoikeuksia valvovat tahot ja valtion toimielimet (ministeriöt, poliisi, oikeuslaitokset). Riskiä nostavat suuremmat tapahtumat yhteiskunnassa, kuten esimerkiksi vaalit, yt-neuvottelut ja suuremmat oikeusjutut. Koska verkkopalveluiden ylläpitäjät eivät raportoi torjutuista palvelunestoista julkisesti, emme tiedä, kuinka laajaa tämän aseen käyttö lopulta on maassamme.

Maailmalta on esimerkkejä, joissa palvelunestohyökkäystä on käytetty kiristyksen välineenä. Rikollisjoukko estää palvelunestolla verkkosivuston käytön ja lupaa sopivaa korvausta vastaan vapauttaa sivuston takaisin käyttöön. Tämä edustaa varainhankintakeinoa rikolliselle toimijalle. Suomeen vastaavat kiristyshyökkäykset eivät julkisuudessa olevien tietojen mukaan ole vielä rantautuneet. Osaltaan tämän mahdollistaa syrjäinen maantieteellinen sijaintimme, suurten operaattoreiden on helppo rajoittaa muualta maahamme kohdistuvia palvelunestohyökkäyksiä maan rajoilla, osaltaan puolestaan ainutlaatuinen kielialueemme ja toimiva yhteiskuntajärjestelmämme. (Hyppönen 2013.)

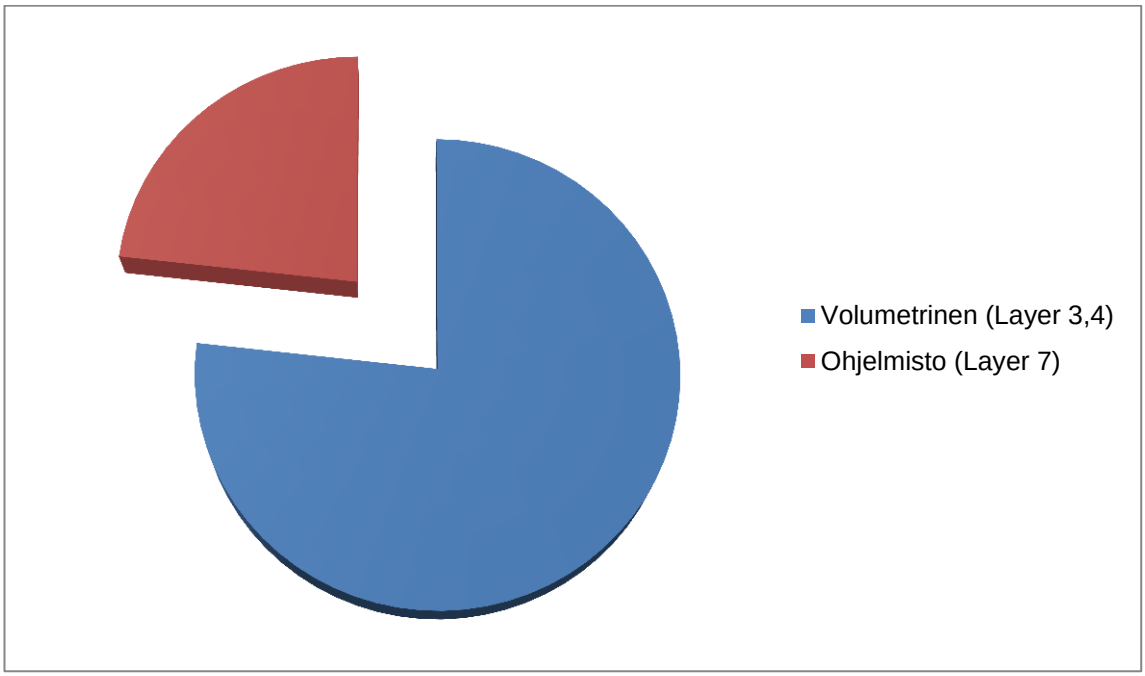
Palvelunestohyökkäys on Suomessa aina rikollinen toimi.

4.3.1 Volumetrinen palvelunestohyökkäys

Layer 3- ja 4-tason palvelunestohyökkäykset tähtäävät resurssien näännyttämiseen kohdejärjestelmistä. Verkko- ja kuljetuskerroksella toimittaessa hyökkääjän ei tarvitse ottaa kantaa, millaista palvelua hän on kaatamassa. 3- ja 4-tasojen hyökkäykset ovat puhtaasti resurssipeliä. Se kumpi osapuoli pystyy luomaan enemmän käytettävää resurssia, yleensä onnistuu tavoitteessaan. Volumetrinen palvelunesto (DOS, Denial of Service) näkyy selvänä piikkinä valvottaessa verkkopalvelun fyysisiä resursseja, erityisesti verkkoliikenteen käyttäytymistä.

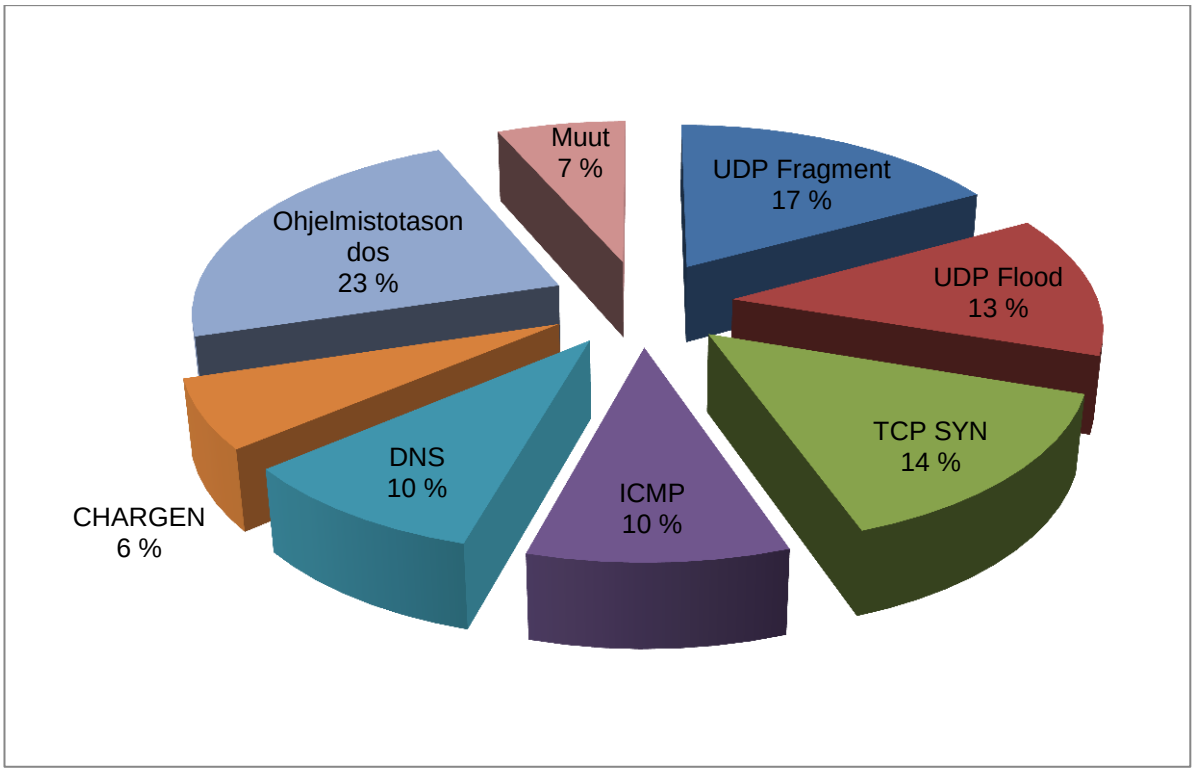
Huolimatta volumetrisen palveluneston suuresta verkkoliikenteen käytöstä, internetpalveluntarjoaja (ISP) ei usein huomaa omaan asiakkaaseensa kohdistuvaa hyökkäystä. ISP ei seuraa niin aktiivisesti omien asiakkaidensa liikennettä, jotta se havaitsisi runko-

verkossaan tapahtuvan suuren lisäyksen. Liikenne palveluntarjoajan runkoverkossa on kuitenkin niin paljon suurempaa, että suuretkin DOS-hyökkäykset häviävät muun liikenteen sekaan.



Kuvio 1. Palvelunestohyökkäysten jakauma volumetrisen (verkko- ja kuljetuskerros) ja ohjelmistotason hyökkäysten välillä. (Prolexic 2014.)

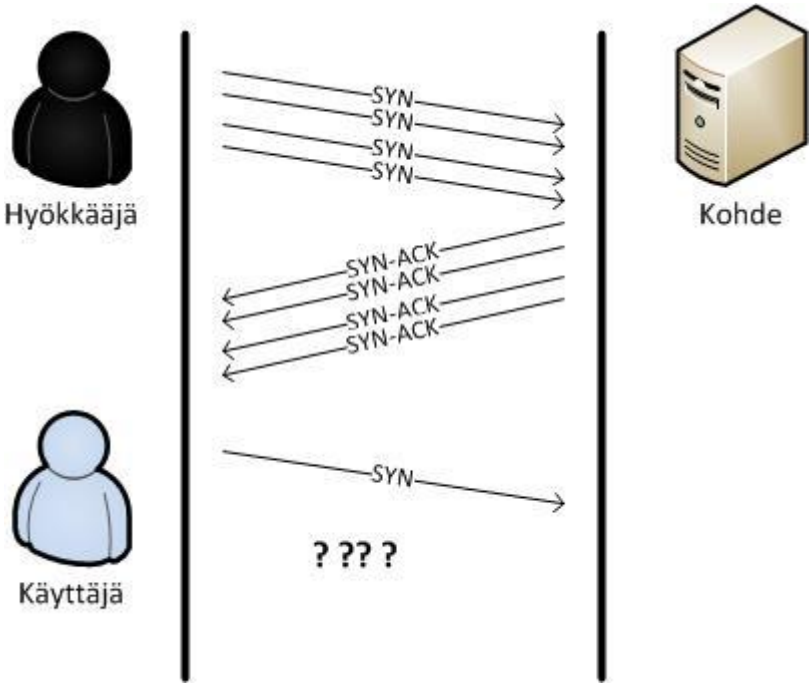
Prolexic:n havaintojen (kuvio 1.) mukaan arviolta 2/3 kaikista palvelunestohyökkäyksistä kohdistuu juuri verkko- ja kuljetuskerroksiin. Palveluneston ja hajautetun palveluneston kohdistaminen verkko- ja kuljetuskerroksiin on teknisesti helpompaa kuin ohjelmistotason hyökkäys. Myös hyökkääjän henkilöllisyyden salaaminen onnistuu tällä tasolla helpommin. Kuviossa 2 on esitelty eri tekniikat joita verkko- ja kuljetuskerroksien hyökkäysten toteutuksessa on käytetty. (Prolexic 2014.)



Kuvio 2. Havaitut palvelunestotekniikat Q4 2013 (Prolexic 2014.)

Kuljetuskerroksella valtaosa hyökkäyksistä toteutetaan UDP-protokollalla (30 %) UDP palveluihin kohdistuviin heikkouksiin. Vaikka UDP on tilaton yhteysmuoto, voidaan myös sillä luoda ylivuotohyökkäyksiä. Kohdelaite joutuu UDP-paketin saadessaan käymään läpi oman sääntötaulunsa tarkistaen, onko paketin kohdeportissa avoimia palveluita. Tämä lisää kuormaa kohdelaitteelle. UDP-ylivuoto on uhka erityisesti palvelinkoneille, jotka ovat suoraan yhteydessä internetiin ilman palomuuria.

TCP-SYN-ylivuotohyökkäykset ovat käytössä noin 15 %:ssa hyökkäyksistä. Näissä hyökkääjä avaa kohdekoneeseen TCP-yhteyden lähettämällä SYN-paketin. Kohdekone avaa hyökkääjälle istunnon ja vastaa SYN-ACK-paketilla. Kohde joutuu pitämään istuntoa auki odottaen hyökkääjältä ACK-viestiä. TCP-istunnon muodostus jää odottamaan kuluttaen kohteen resursseja ja estäen oikeisiin SYN-viesteihin vastaamisen.



Kuva 9. TCP SYN flood. Käyttäjä ei saa vastausta kohteelta, koska hyökkääjä on varannut kaikki verkkoresurssit.

TCP SYN-hyökkäyksessä on kyse siitä, että hyökkääjä pystyy luomaan tarpeeksi pyyntöjä kohdepalvelimelle. Yleensä hyökkääjä väärentää oman lähettävän ip-osoitteensa, jolloin SYN-ACK-viestit katoavat, eivätkä häiritse hyökkääjää. Kohdekone jää SYN-ACK-viestit lähetettyään odottamaan TCP-protokollan mukaista ACK-viestiä. Näin myöskään uusi käyttäjä ei saa avattua yhteyttä, koska kohde odottaa yrittää muodostaa yhteyksiä hyökkääjään kuten kuvassa 9.

Volumetristä palvelunestoa mitataan Gbit/s-mittarilla. Suurin mitattu palvelunestohyökkäys on mitattu 300 Gbit/s ja normaalien hyökkäystenkin voima on kasvamassa. Yleisimmät hyökkäykset tällä hetkellä ovat noin 100 – 150 Gbit viestiliikennettä sekunnissa. Tämäkin on jo tavanomaisen yritysinternetliittymän (1-10 Gbit/s) kaatava datamäärä. (Prolexic 2014.)

Palvelunestohyökkäyksistä mitataan myös sen kestoa. Tyypillinen hyökkäys on alle kuuden tunnin pituinen. Mikäli kyseessä on kriittinen verkkopalvelu, on siihen tässä ajassa yleensä päästy vaikuttamaan ja mitigoimaan. (Prolexic 2014.)

4.3.2 Ohjelmistotason palvelunesto

Ohjelmistotason palvelunesto (DOS) iskee verkkopalvelun ohjelmiston, eli tason 7 heikkouksiin. Jotta ohjelmistotasolle asti OSI-mallissa päästään, tulee lähteen ja kohteen väliin luoda toimiva TCP-istunto. Tämä vaatii SYN-ACK-pakettiin vastaamisen aidosta IP-osoitteesta ja jo luodun session hyödyntämistä.

Valtaosa ohjelmistotason hyökkäyksistä on kohdistunut HTTP-sivuihin ja HTTP-GET-tyypillä toteutetusti. Tässä hyökkäyksessä hyökkääjä lähettää HTTP-GET hakuja ja pyytää toistuvasti kohdetta lataamaan ja lähettämään jonkin verkkosivun tietyn objektin. Tämä objekti voi vaatia palvelimelta tietokantakyselyitä tai muuta paljon laskentatoimea vaativaa toimenpidettä. Näiden kyselyiden tulva lopulta hidastaa verkkosivun toimintaa ja mahdollisesti kaataa sen.

Ohjelmistotason palvelunestohyökkäykset vaativat tarkempaa suunnittelua ja kohteen tuntemusta. Verkkosivun etusivu on yleensä ylläpitäjän puolelta optimoitu vastaamaan suuriin määriin kyselyitä, mutta taustapalvelut välttämättä eivät. Jotta ohjelmistotason palvelunestosta saadaan parhain hyöty, tulee se kohdistaa johonkin tällaiseen taustajärjestelmään. (Arbor Networks Webinars 2014.)

4.3.3 Palveluneston (DOS) ja hajautetun palveluneston erot (DDOS)

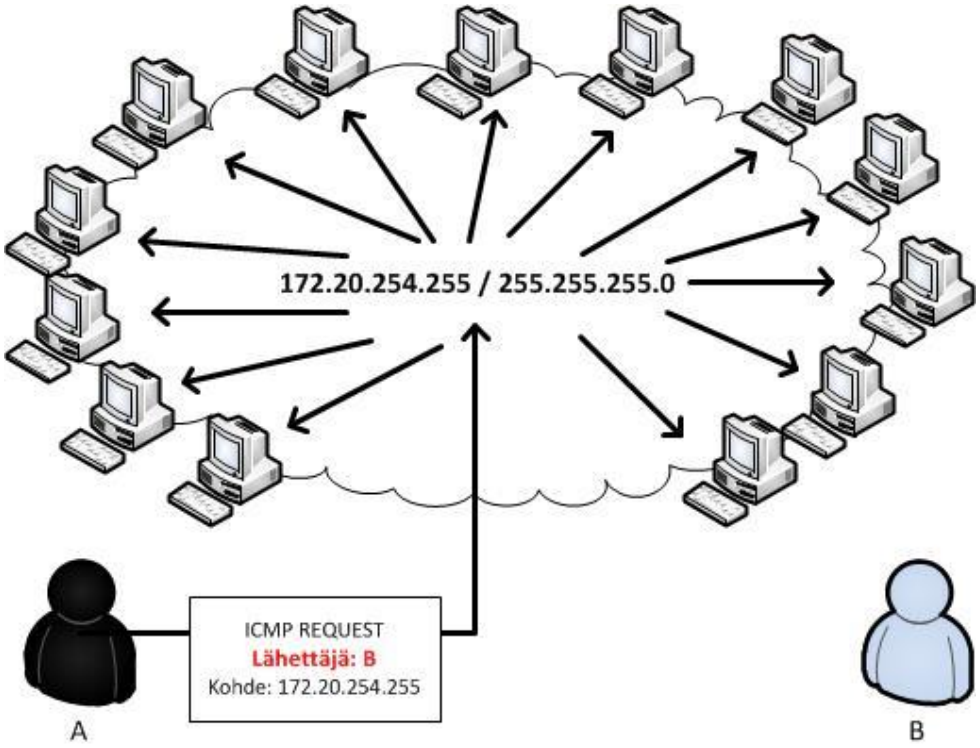
Palvelunesto ja hajautettu palvelunesto pyrkivät molemmat samaan lopputulokseen: estämään palvelun toiminnan. Kun normaali palvelunesto hyödyntää vain yhden lähettäjän resursseja, hyödyntää hajautettu palvelunesto useita internetissä avoimena olevia resursseja. Näin yksittäistä hyökkääjää ei saada selville ja palveluneston vaikutusten lieventäminen (mitigointi) vaikeutuu.

Varsinkin suomalaiset internet operaattorit rajoittavat lisäksi asiakkaidensa lähtevien pakettien osoitekenttien väärennystä. Mikäli havaitaan, että asiakkaan verkkoliittymästä lähtee liikennettä eri ip-osoitteella, kuin asiakkaalle on allokoitu, puuttuvat operaattorin reitittimet automaattisesti asiaan ja pudottavat paketit. Näin suomalainen internetin käyttäjä ei voi väärentää omaa lähettäjän osoitettaan ja käynnistää laajaa palvelunestoa vain yhdestä kohteesta. Ulkomailla toimivat operaattorit ovat kokemusten mukaan väljempiä lähettäjän paketin identiteetin tarkastuksessa ja voivat sallia eri lähteistä tulevia paketteja. Mikäli liikenne sallitaan operaattorin toimesta myös operaattorien ja eri

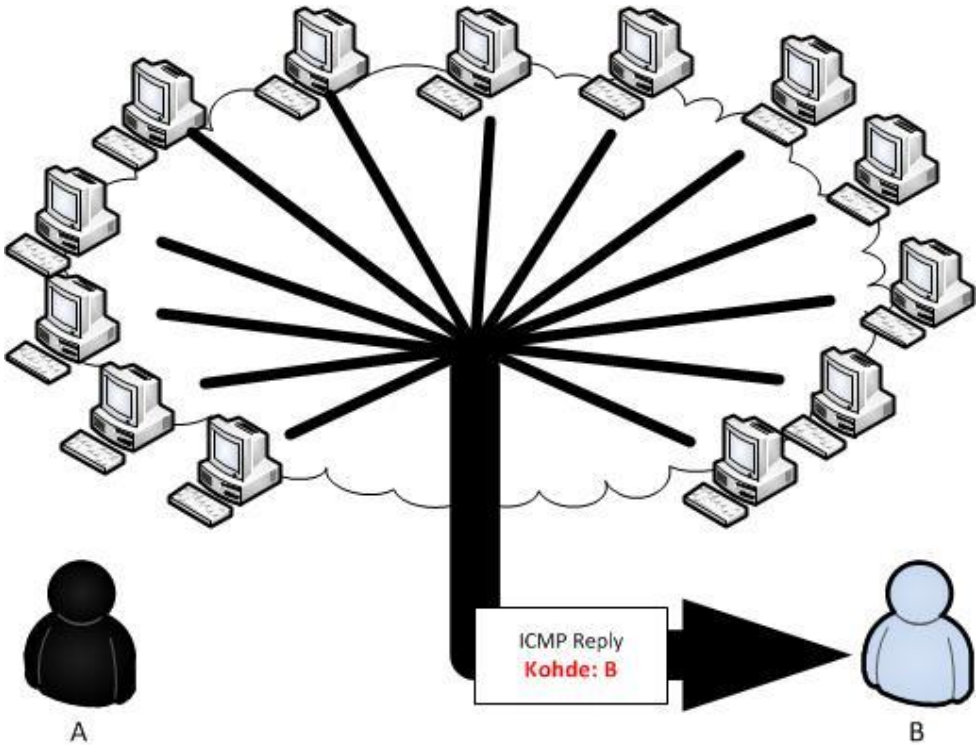
maiden välisiin verkkoihin, on sen aitouden tunnistaminen jo huomattavasti vaikeampaa.

Hajautettuun palvelunestoon voidaan käyttää internetiin kytkettyjä palveluita ja botnet-verkkoja. Ajatuksena on, että lähettäjä voi pienellä lähetyksellä saada aikaan moninkertaisen tulvan kohdekoneeseen. Koska ip-paketin osoitetietoa voidaan muokata lähettäjän toimesta, voidaan siitä vaihtaa lähettävän laitteen ip-osoite. Näin vastausviestit menevät aivan eri kohteeseen kuin lähettääjlle, kuten on kuvattu kuvissa 10. ja 11. (F-Secure 2014).

ICMP-protokollaa on käytössä noin 10 % hyökkäyksistä. IP-protokollan määritykset mahdollistavat oletuksena verkkojen mainostusosoitteen käytön ICMP-viesteille. Mainostusta käytetään heijastamaan hyökkäys väärentämällä ICMP-viestiin lähettäjän osoite ja lähettämällä ICMP-viesti ison aliverkon mainostusosoitteeseen. Tällöin aliverkossa olevat kaikki laitteet vastaavat ICMP-viestin lähetystiedoissa olevalle lähettäjälle. Viaton väärennetty vastaanottaja saa yhtäkkiä käsiinsä huiman määrän ICMP-reply-viestejä (ks. kuvat 10 ja 11).



Kuva 10. A lähettää väärennetyn ICMP-paketin aliverkkoon.



Kuva 11. B saa ICMP Reply viestit kaikilta aliverkon koneilta, joille A on lähettänyt Request pyynnön.

DNS-nimipalveluita käytetään noin 9,5 % hyökkäyksistä. Internetissä on mahdollista käyttää avoimia nimipalvelimia. Näiltä nimipalvelimilta voi kuka tahansa tehdä nimipalvelutietokyselyn (DNS Request). Palvelimet vastaavat kyselyyn kyselyn lähettäjätiedon mukaan. Kuten ICMP-hyökkäyksessä, voidaan DNS-nimikyselynkin lähettäjätieto väärentää ja ohjata kaikki nimipalvelu-vastaukset viattomalle kohteelle kuluttaen sen verkkokaistaa.

DNS-nimipalvelun käyttö palvelunestoon vaatii sen olevan ns. open resolver -tilassa. Tällöin palvelu ei vaadi nimitietoa kysyvältä lainkaan todennusta, eikä kysyjien määrää tai kyselyn tyyppiä rajoiteta. Näin palvelu vastaa kaikille, jotka kysyvät siltä DNS-nimitietoja. Internetissä on avoimia nimipalvelimia noin 20 miljoonaa, Suomessakin jopa 20 000. Näiden kaikkien hyödyntäminen yhteen kohteeseen hyökkäyksessä on mahdollista ja luo oikein suunniteltuna suuren määrän liikennettä. Yksittäinen kysely moninkertaistuu ja paisuu kohdistuen lopulta yksittäiseen kohteeseen. Myös muita internetin avoimia TCP-palveluja voidaan käyttää hyökkäyksen moninkertaistamiseen samalla periaatteella kuin ICMP- ja DNS-protokollia. (Arbor Networks Webinars 2014.)

Hajautetussa palvelunestossa hyödynnetään myös botnet-verkkoja. Hallituista orjakoneista voidaan lisätä DNS-kyselyitä tai lähettää suoria TCP Flood -hyökkäyksen viestejä. Koneiden lähettämien pakettien sisältöä voidaan myös väärentää ja aiheuttaa näin entistä enemmän hämmennystä kohteelle.

5 Palvelunestohyökkäyksen vaikutusten lieventäminen

5.1 Palveluneston havaitseminen

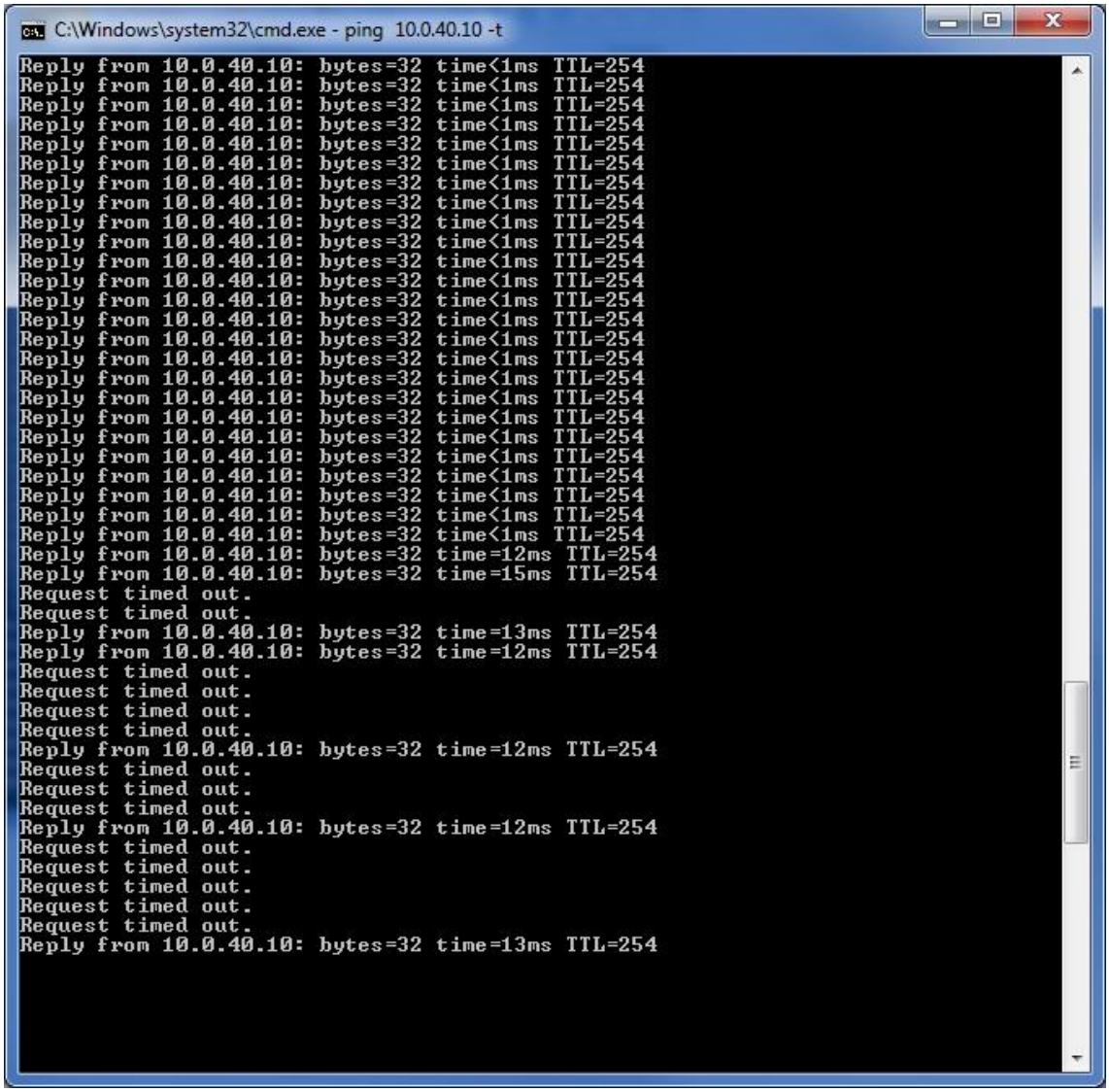
Palvelunestohyökkäyksen havaitseminen on monivaiheinen prosessi. Mikäli kyseessä on voluumipohjainen, eli layer -3 tai 4 -tason hyökkäys, näkyy se kasvavana verkkoliikenteenä ISP:n tasolta reitittimellä, palveluntarjoajan kohdalta palomuurissa ja lopulta itse päätelaitteella. Kuitenkin hyökkäyksen tunnistaminen normaalista verkkoliikenteestä voi tässä tilanteessa olla vaikeaa.

Palvelunestohyökkäys voi lamauttaa verkon aktiivilaitteita ja samalla estää niiden hallinnan. Tämä on erityisen totta varsinkin valmistelemattomien laitteiden kanssa. Hyökkääjä saa näin lamautettua verkkoa valvovan tahon kaikki keinot toimia hyökkäystä vastaan (kuva 12).

Kuva 12. Palvelunestohyökkäys on lamauttanut FortiGate palomuurijärjestelmän ja sen hallinnan.

Volyymipohjainen hyökkäys syö resursseja kohdelaitteilta samaan tapaan kuin normaali sivustolla vierailu. Näin normaalikin liikenne voi aiheuttaa tilapäisen palveluneston kohdepalveluun. Tämä tapahtuu varsinkin, jos palveluun käytettäviä fyysisiä (laskentateho, muisti) resursseja on karsittu. Mikäli verkkopalvelun kanssa samaa verkkokaistaa käyttää esimerkiksi yrityksen normaali verkkoliikenne, voi palvelunesto lamauttaa kaiken verkkoliikenteen yrityksestä.

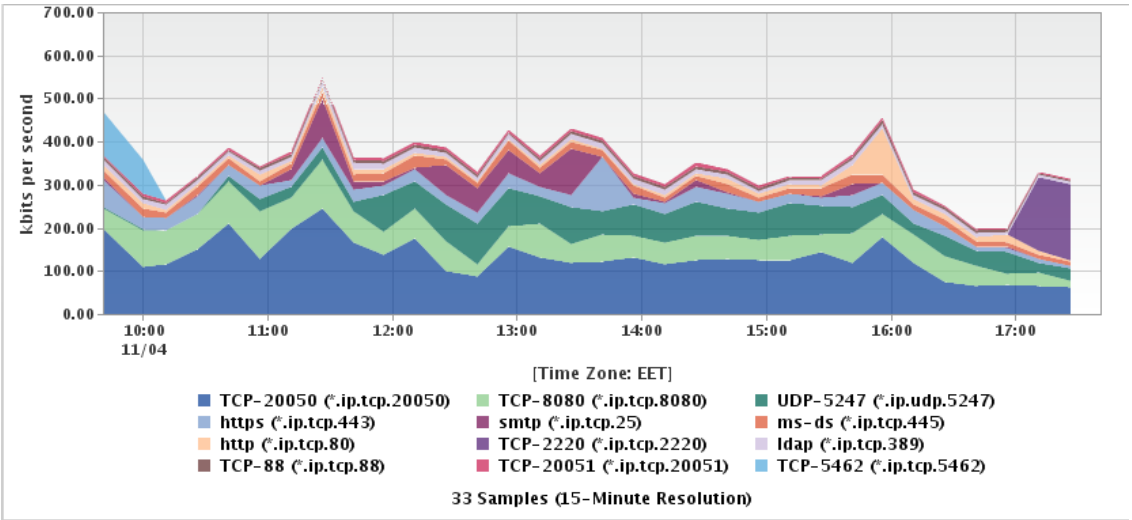
Hyökkäyksen havaitseminen omasta lähiverkosta voi olla vaikeaa. Volyymipohjainen hyökkäys voi kuluttaa internetin suuntaan olevat resurssit palvelulta, mutta se voi yhä vastata ongelmitta sisäverkkoon. Myöskään itse palvelimen suorituskyvyssä ei välttämättä havaita mitään muutoksia. Yleensä verkkopalvelusta valvotaan kohdepalvelimen verkkoyhteyttä ping-komennoin ICMP:llä sekä palvelimen fyysisiä resursseja SNMP (Simple Network Management Protocol)-viestein. Samoin periaattein valvotaan myös muita palvelun verkkopolun laitteita. Kohdepalvelin voi vastata ICMP-viesteihin normaalisti sisäverkosta tulevaan kyselyyn, ja voi olla, ettei mikään sen SNMP-valvonnoista hälytä. Näin verkkopalvelua valvova ei välttämättä tiedä kyseessä olevan palvelun käytön olevan estetty.



Kuva 13. Palvelunestohyökkäys aiheuttaa katkoksia ICMP valvontaan. Normaali vasteaika on <1ms.

Mikäli palvelua valvotaan vain ICMP:llä, tulee valvoa aktiivisesti myös vasteaikoja ICMP vastauksissa. Laiteen vastausta suurella viiveellä ei tule automaattisesti tulkita normaaliksi toiminnaksi, mikäli kyseisen palvelun kohdalla ei ole odotettavissa tällaisia katkoksia (kuva 13).

Nykyaikaiset reitittimet ja palomuurit tarjoavat myös mahdollisuutta valvoa tietoliikennettä laitteen läpi. Tätä kutsutaan ns. NetFlow – valvonnaksi (Kuva 14). Tällöin valvottavat laitteet tuottavat tietoa kaistan käytöstä valvontaan. NetFlow valvonnalla voidaankin tehokkaasti havaita muutokset tiedonsiirrossa ja tarvittaessa hälyttää valvontaa aiheesta.



Kuva 14. Netflow -tiedolla voidaan tutkia, kuinka paljon kaistaa on käytössä ja mihin kaistaa kuluu.

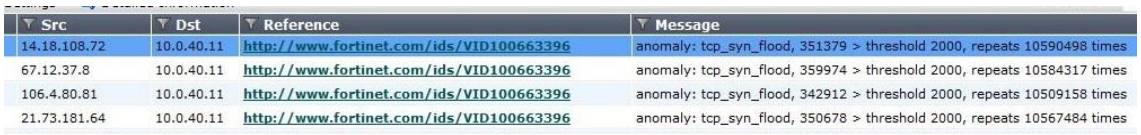
NetFlow-dataa ei kuitenkaan lähetetä, jos laitteen toimintaa on häiritty. Myös muunkin valvontatiedon saaminen laitteelta hyökkäyksen aikana voi olla haastavaa. Siksi tuleekin kehittää verkon valvontakeskuksen (NOC, Network Operations Control) kykyä havaita ja tunnistaa palvelunestohyökkäys. Hallintoihin tila voi näkyä normaalina verkkokatkoksena, jonka käsittely ei välttämättä aiheuta erityisiä toimia. Näin menetetään arvokkaita hetkiä torjuntatoimien käynnistämisessä.

Internet-palveluntarjoaja ei oletuksena seuraa taikka havaitse muutoksia verkkokaistan käytössä yksittäisen asiakkaan kohdalla. Tällainen havainnointi syö resursseja optimoiduilta runkoverkon reitittimiltä, joten se kytketään päälle vain tapauskohtaisesti. Tällöin NetFlow – ym. valvontatiedon saaminen onkin usein arvokas lisäpalvelu ISP:ltä.

Ohjelmistopohjaisen palveluneston havaitsemiseen ei normaali SNMP-valvonta riitä. Hyökkäys kohdistuu palvelimella pyörivään ohjelmistoon, eikä tällöin estä palvelinta vastaamasta valvontaansa. Myöskään NetFlow-monitorointi ei paljasta syyksi hyökkäystä, sillä Layer7-hyökkäys ei kuluta kaistaa kuten volumetrinen hyökkäys.

Hyvin usein palvelunestohyökkäyksen havaitsee ensimmäisenä palvelun käyttäjä, joka ei hyökkäyksen vuoksi pääse käyttämään verkkopalvelua. Käyttäjän vikailmoituksesta lähtee tällöin vianselvitys. Tällöin kestääkin huomattavan kauan, kunnes vian syy selviää palvelunestohyökkäykseksi, ja siihen päästään reagoimaan oikein. Käyttäjän kokemuksia voidaan simuloida koneellisesti ns. Application Monitoring -palvelun kautta. Tässä tekniikassa tietokoneella ladataan verkkosivu ja tarkastetaan sen toimivuus. Näin valvonta huomaa, mikäli sivu ei latautukaan oikein ja varoittaa siitä valvonnassa.

Havainnointia suorittaessa tulee myös muistaa kerätä lokitietoa kaikista tapahtumista myöhempää käyttöä varten. Palvelunestohyökkäys on aina rikos, ja siitä tulee tehdä rikosilmoitus poliisille. Rikostutkintaa helpottaa kaikki mahdollinen lokitieto tapahtumalta (esim. kuva 15). Lokitiedon saaminen hyökkäyksen kohteena olevasta laitteesta voi olla vaikeaa, joten sitä tulee kerätä mahdollisimman laajalti kaikilta verkkoon liittyvistä laitteista. Myös hajanaisen lokitiedon keskitettyä keruuta ja tulkintaa tulee harjoitella aktiivisesti NOC:in henkilöstön kanssa.



Src	Dst	Reference	Message
14.18.108.72	10.0.40.11	http://www.fortinet.com/ids/VID100663396	anomaly: tcp_syn_flood, 351379 > threshold 2000, repeats 10590498 times
67.12.37.8	10.0.40.11	http://www.fortinet.com/ids/VID100663396	anomaly: tcp_syn_flood, 359974 > threshold 2000, repeats 10584317 times
106.4.80.81	10.0.40.11	http://www.fortinet.com/ids/VID100663396	anomaly: tcp_syn_flood, 342912 > threshold 2000, repeats 10509158 times
21.73.181.64	10.0.40.11	http://www.fortinet.com/ids/VID100663396	anomaly: tcp_syn_flood, 350678 > threshold 2000, repeats 10567484 times

Kuva 15. Kerättyä lokitietoa palvelunestohyökkäyksestä. Tiedossa on tarkat kellonajat, hyökkäyksen tyyppi ja hyökkääjän lähde-osoite.

Palvelua valvottaessa sovelletaan niin sanottua OODA (Observation, Orientation, Decision, Action) -silmukkaa:ia. Tällöin palvelua ja sen vikatilanteita

- havainnoidaan
- arvioidaan
- päätetään reaktio
- reagoidaan.

Riippuu verkonvalvonnan kyvyistä ja sillä olevista resursseista, kuinka nopeasti palvelunesto arvioidaan oikein ja milloin siihen päästään reagoimaan. Reagointia, eli palvelunestohyökkäyksen vaikutusten lievennystä kutsutaan mitigoinniksi.

Mikäli käytössä on IDMS-järjestelmä (Intelligent Mitigation system), osaa järjestelmä tarkkailla ja arvioida verkkohyökkäykset ensitilassa. Tällöin voidaan valita mikäli hyökkäystä mitigoidaan automaattisesti vai vasta järjestelmää valvovan kehotteesta. (Arbor Networks Webinars. 2014.)

5.2 Palveluneston vaikutusten lieventäminen

Kun palvelunestohyökkäys on tunnistettu ja siihen on päätetty reagoida, tulee reaktio päättää. Reaktio riippuu hyökkäyksen tyypistä. Vaikutusten lievennyksen keinot kolmella eri tietoturvan tasolla vaihtelevat. Mitä lähempänä hyökkääjää päästään hyökkäykseen vaikuttamaan, sitä suuremmat mahdollisuudet hyökkäyksen onnistuneeseen lieventämiseen ovat olemassa.

Yksinkertaisen palveluneston pysäyttämiseen riittää jo hyvin lähelle lähdettä sijoitettu accesslist-sääntö. Näin esimerkiksi reitittimellä voidaan estää hyökkäyksen lähteen liikennöinti kohteeseen. Tätä operaattori voi tehdä jo tarkistamalla asiakkaidensa lähtevien pakettien osoitetiedot ja pudottamalla väärennetyt (reverse path checkup).

Mikäli reitittimillä ja palomuureilla ei ole lainkaan varauduttu palvelunestohyökkäykseen, ei palvelimen hallinnassa voida tehdä paljoakaan toimia palvelun pelastamiseksi. Jos hyökkäys onnistuu lamauttamaan palvelimen hallinnan (esimerkiksi jos palvelin on kytketty suoraan internetiin, ilman palomuureja yms.), ei palvelinta voida etätoimin pelastaa. Kohdepalvelun uudelleenkäynnistys ei auta, sillä hyökkääjä tulee samasta yhdyskäytävästä kuin muut palvelun käyttäjät. Hyökkäys jatkuu yhä uudelleenkäynnistyksestä riippumatta, ja lamauttaa sen jälkeen palvelun.

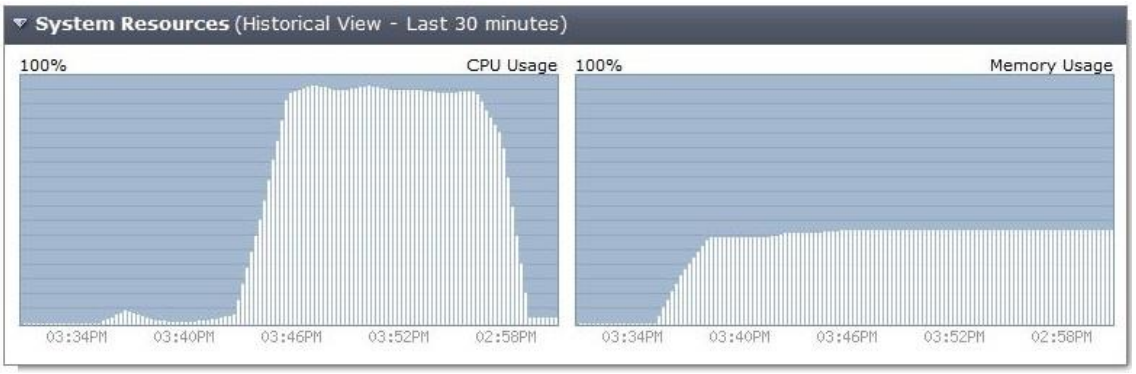
Palvelimen ylläpitäjällä on mahdollisuuksina hyökkäykseen joutuessaan lisätä laitteen fyysisiä resursseja (muistia ja prosessoritehoa) ja olla yhteydessä internetpalveluntarjoajaan. Paikallisesti palvelu saadaan palautettua irrottamalla palvelin internetistä mutta silloin palvelu ei ole enää käytettävissä internetin puolelta.

Palvelimen toimintaa voidaan tehostaa luomalla klusteroituja palvelimia ja jakamalla kuormaa (engl. Load Balance) eri palvelimien kesken. Myös palvelimen ohjelmistokoodin syvällinen testaus voi ennaltaehkäistä suorituskyvystä johtuvia palvelunestoja. Näiden toimien käyttöönottaminen hyökkäyksen aikana on kuitenkin monimutkaista ja myöhäistä.

Palvelimen kohdalla palvelunestohyökkäysten vaikutusten lieventäminen perustuu etukäteissuunnitteluun. Palvelun kaikki osat tulee testata huolellisesti ohjelmistotason hyökkäyksen torjumiseksi. Erityisesti raskaiden tietokantakyselyiden ja muiden palvelinta kuormittavien tehtävien optimointi vaikeuttaa onnistuneen ohjelmistotason hyökkäyksen toteutusta.

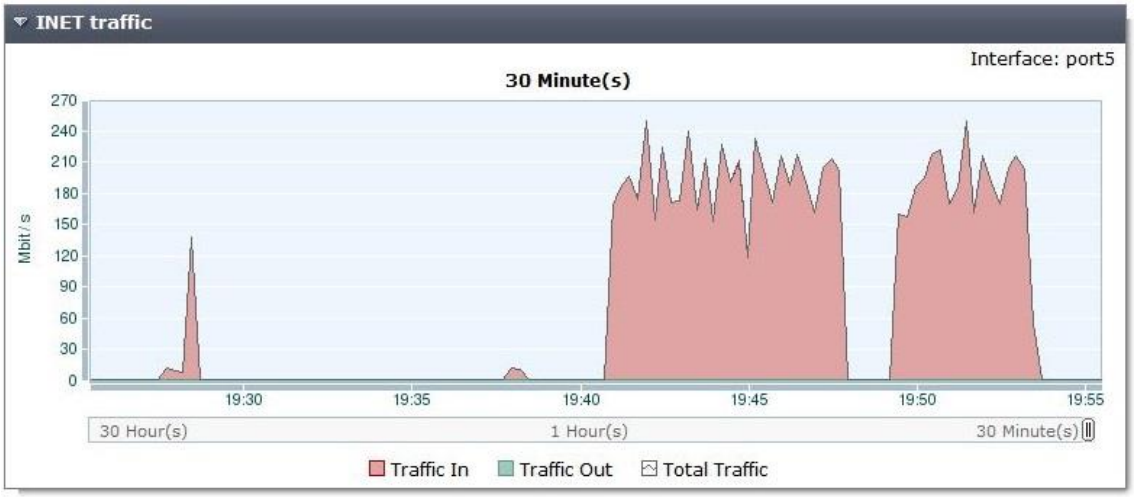
Mikäli palvelimelle on käytössä palomuuripalvelu, voi palvelun ylläpitäjä olla yhteydessä heihin. Palomuuripalvelun ylläpitäjä voi havaita poikkeuksen myös itse omasta valvonnastaan. Hyvin usein automaattiset hyökkäyksen lievennystoimet ovat kuitenkin lisäpalveluna eivätkä aina asiakkaan välittömässä käytössä.

Uudemmissa palomuureissa voi olla integroituna palvelunestohyökkäysten lievennykseen käytettäviä työkaluja. Nämä toimivat rajoittaen laskurien kautta eri liikennemääriä. Mikäli muuri havaitsee raja-arvon ylittävän määrän liikennettä tiettyyn kohteeseen, alkaa se rajoittaa yhteyksiä (ks. kuva 18). Muuri ei erittele normaalia liikennettä eikä hyökkäävää liikennettä vaan rajoittaa kaikkia yhteyksiä. Tämä näkyy palvelun käyttäjälle hitautena palvelun käytössä. (Arbor Networks Webinars. 2014.)



Kuva 16. FortiGate laitteen prosessorikuorma ja muistin käyttö hyökkäyksen aikana. Palvelunestoon torjuminen on lähes kuluttanut prosessorin resurssit loppuun (>90 %).

Integroidut ominaisuudet syövät kuitenkin laitteelta sen resursseja. Tämä hidastaa palomuurin muita toimintoja. Palvelunestohyökkäyksen lievennyksessä on tärkeää saada toteutettua se tarkoitukseen suunnatulla resurssilla. Mikäli jo resursseistaan karsittu verkkolaite joutuu toimimaan myös palveluneston mitigoijana, loppuvat siltä kaikki käytettävissä olevat keinot ja palvelunesto onnistuu (kuva 16). Tästä syystä on tarjolla erityisesti tähän tehtävään suunniteltuja verkkolaitteita. Palvelunestohyökkäyksen vaikutuksia torjuvan laitteen täytyy käytännössä pystyä vastaamaan kasvavaan määrään viestejä, puskuroimaan niiden aiheuttamaa kuormaa ja näillä keinoin lieventää itse palveluun kohdistuvaa painetta.



Kuva 17. FortiGate palomuurilaitetta vastaan on tehty palvelunestohyökkäys joka on havaittavissa sen grafiikassa.

Maiden ja operaattorien väliset runkoverkot on yleensä toteutettu massiivisella verkkokaistalla. Tämä tarkoittaa että resursointi tähän verkkoon täytyy pakostakin olla laadukasta. Näin runkoverkon reunareitittimillä voidaan rajata palveluneston aiheuttamia harmeja jo ennen kuin hyökkäys pääsee kuluttamaan resursseja sisemmältä operaattorin infrastruktuurista. Reitittimelle rajoituslistat tekevät internetpalveluntarjoajat. Nämä rajoituslistat ovat käsityönä tehtäviä ja väliaikaisia. ISP yleensä poistaa rajoitukset muutaman päivän tai viikon kuluttua hyökkäyksen vaimentumisesta. Mikäli hyökkäyksen lähdettä ei saada täydellä varmuudella selville, ISP rajoittaa myös verkkokaistan käyttöä oman runkoverkkonsa laidalla. Näillä toimin saadaan rajoitettua kohteeseen osuvaa hyökkäystä.

Internetpalveluntarjoajat eivät aktiivisesti seuraa asiakkaidensa verkkoliikennettä. Tällöin pyyntö palvelunestohyökkäyksen rajoittamiseen tulee asiakkaalta, ja kun asiak-

kaalla ei välttämättä ole tietoa olevansa hyökkäyksen kohteena, voi lievennystoimen käynnistyksessä kestää. Myös sen käyttöönotto ISPn verkkoon kestää, koska palveluntarjoajan pitää varmistaa, etteivät heidän tekemänsä muokkaukset vaikuta muiden asiakkaiden palvelutasoon, tämä tarkoittaa että palveluntarjoajan toimet tulevat usein hyvinkin pitkällä viiveellä.

Volyymipohjaisen palveluneston vaikutusten lieventämiseen on internetissä tarjolla useita pilvipohjaisia ratkaisuja. Näihin palveluihin voidaan verkkoliikenne reitittää joko koko ajan, jolloin pilvipalvelu seuraa ja reagoi havaitsemiinsa poikkeamiin automaattisesti tai manuaalisesti, kun kohdeorganisaatio huomaa olevansa hyökkäyksen kohteena. Pilvipalvelussa etuna on skaalautuvuus, palvelua voidaan helposti tehostaa torjumaan isojakin volumeja hyökkäysliikennettä.

Pilvipohjaisen palvelun ostaminen on kuitenkin pidemmällä aikavälillä kallista ja sen perustelu talouspuolelta hankalaa, varsinkin jos hyökkäyksiä ei satu useita. Pilvipalvelun kautta reititettynä liikenne hidastuu. Liikenteen reititys hyökkäyksen alla voi myös vaatia toimia ISP:ltä ja on hidasta ottaa käyttöön.

TCP-hyökkäystä torjuttaessa mitigointi tapahtuu seuraamalla luotuja sessioita ja paketin muotoa. Mikäli aidon TCP-SYN-viestin lähettävä asiakas ei saa tiettyyn aikaan SYN-ACK-viestiä lähettää asiakas uudestaan SYN-viestin. Palvelunestoa torjuva palvelu kerää SYN-viestit pitkään listaan ja jää odottamaan toista SYN-viestiä. Asiakkaan aidon SYN-viestin tullessa se päästetään läpi. Näin haitallinen liikenne jää odottamaan aikakatkaisua vaikutusta lieventävään laitteeseen.

Anomalies Configuration:

Name	Enable	Logging	Action	Threshold
tcp_syn_flood	☑	☐	Block	2000
tcp_port_scan	☐	☐	Pass	1000
tcp_src_session	☐	☐	Pass	5000
tcp_dst_session	☐	☐	Pass	5000
udp_flood	☑	☐	Block	2000
udp_scan	☐	☐	Pass	2000
udp_src_session	☐	☐	Pass	5000
udp_dst_session	☐	☐	Pass	5000
icmp_flood	☑	☐	Block	250
icmp_sweep	☐	☐	Pass	100
icmp_src_session	☐	☐	Pass	300
icmp_dst_session	☑	☐	Block	1000
ip_src_session	☐	☐	Pass	5000
ip_dst_session	☑	☐	Block	5000

OK Cancel

Kuva 18. FortiGate-laitteen AntiDos-suodatin.

SYN-paketeista voidaan tarkkailla kaikkia sen sisältämiä tietoja IP-osoitteiden maantieteellisistä sijainneista bittitasolla oleviin merkkeihin paketin alkuperästä (kuva 18). Myös kellonaikaan verrataan tulevia paketteja ja tarkkaillaan outoihin ajankohtiin tulevaa liikennettä.

Mitigointipalveluita vertaillessa puhutaan läpäisyarvoista, eli siitä kuinka paljon tarkastamatonta liikennettä pystytään vastaanottamaan, ja yhä säilyttämään palvelun laatu. (Palvelunestohyökkäyksiltä suojautuminen, Nixu 2003.)

5.3 Hajautetun palveluneston vaikutusten lieventäminen

Hajautetussa palvelunestohyökkäyksessä hyökkäävää osapuolta ei pystytä varmentamaan. Hyökkääjä myös hyödyntää internetissä olevia avoimia palveluita hyökkäyksen vaikutusten vahventamiseen. Nämä palvelut voivat olla suojaamattomia DNS-

palvelimia tai muita aivan sinänsä laillisia ja aitoja palveluita, joita ei normaalioloissa haluta estää.

Hajautettuun palvelunestohyökkäykseen kuuluu erityisesti hyökkääjän ip-osoitteen väärennys. Tällöin mahdollisesti kerätty lokitieto hyökkääjän ip-tiedoista ei ole yksilöivä eikä käyttökelpoinen.

Hyökkäyksen suurin haaste on aidon liikenteen tunnistaminen haittaliikenteen seasta. Jos hajautettu hyökkäys on saatu onnistumaan ohjelmistotasolle, tarvitaan sen mitigointiin erikoistuneita ohjelmistoja ja laitteita. Muutoin hajautetun hyökkäyksen torjunta toimii samoin periaattein kuin hajauttamattoman.

Palvelunestohyökkäyksen torjumisen siirtäminen pilvipalveluun, eli pakettipesuriin, on hyvin toimiva tapa vähentää hajautetun hyökkäyksen vaikutusta palveluun. Pakettipesuri sijaitsee poikkeuksetta jo internet verkossa tai palveluntarjojan verkossa jossa saapuvaan hyökkäykseen päästään tehokkaammin vaikuttamaan kuin palvelun oman yhdyskäytävän varrella. Pakettipesurin optimointi ohjelmistotason hyökkäyksiä varten voi kuitenkin olla työläs ja kallis prosessi, varsinkin jos palvelun rakenne muuttuu aktiivisesti. Näin palvelua lähempänä toimiva palvelunestohyökkäyksen vaikutuksia lieventävä laite on helpompi optimoida juuri senhetkiseen ohjelmistoon ja palveluun.

Markkinoilla on laitteita jotka yhdistävät paikallisen- ja pilven pakettipesurien hyvät puolet. Asiakkaan yhdyskäytävässä toimiva laite valvoo reaaliaikaisesti liikennettä ja ilmoittaa mahdollisista muutoksista palvelutasossa. Laite voidaan käskyttää eskaloimaan pakettipesua myös pilveen mikäli laitteen oma suorituskyky on vaarassa.

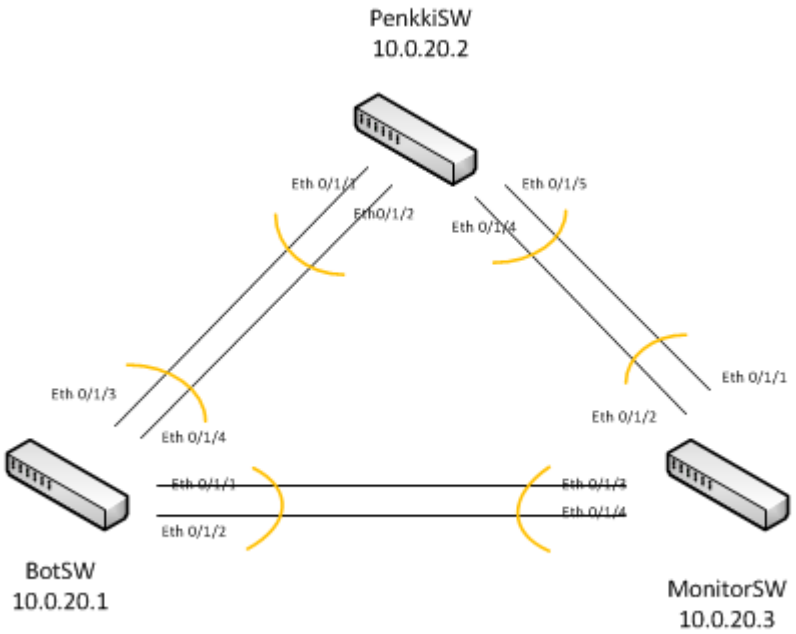
Kuten yleensä it-ratkaisuissa, eivät eri laitevalmistajan ratkaisut toimi toistensa kanssa hyvin. Eli valmistaja A:lta tilattu palomuuri ja reititys ei välttämättä toimi ideaalilla tavalla valmistaja B:n pakettipesurin ja kuormantasauksen kanssa. Myöskin automaattiset toimet eri laitevalmistajien välillä jäävät minimiin. (Teleyrityksen mahdollisuudet rajoittaa verkkohyökkäyksiä. 2014; Arbor Networks Webinars 2014).

6 Palvelunestohyökkäysten vaikutusten torjuminen laboratoriossa UTM-palomuurein

Palvelunestohyökkäyksen vaikutuksia on mahdollista simuloida laboratorio-ympäristössä ns. pakettigeneraattorin avulla. Tällöin ohjelmallisesti luodaan palvelunestohyökkäystä simuloiva määrä paketteja ja reititetään ne osumaan testattavaan ympäristöön. Rakensin oman laboratorio-ympäristön Fortigate valmistajan palomuurilaitteilla. Tarkoituksena oli selvittää, kuinka hyvin palomuurilaitteet pystyvät selviytymään palvelunestohyökkäyksistä erilaisin konfiguraatioin. Laitteet ovat jo hieman vanhentuneet, joten ajantasaista kuvaa laitevalmistajan tuotteiden kyvyistä testauksessa ei saatu.

6.1 Laboratorioympäristön kuvaus

Testaukseen käytettävän rungon verkko on luotiin Foundry FLS648-kytkimiä hyödyntäen. Kytkinportit ovat 1000 Gbit/s ja kytkinten välit on toteutettu port-channel-ominaisuudella (Foundry vastaava TRUNK). Näin on käytettävissä 2 x 1000 Gbit/s:n linkit kytkinten väliseen liikenteeseen (ks. kuva 19).



Kuva 19. Kytkinten väliset kytkennät.

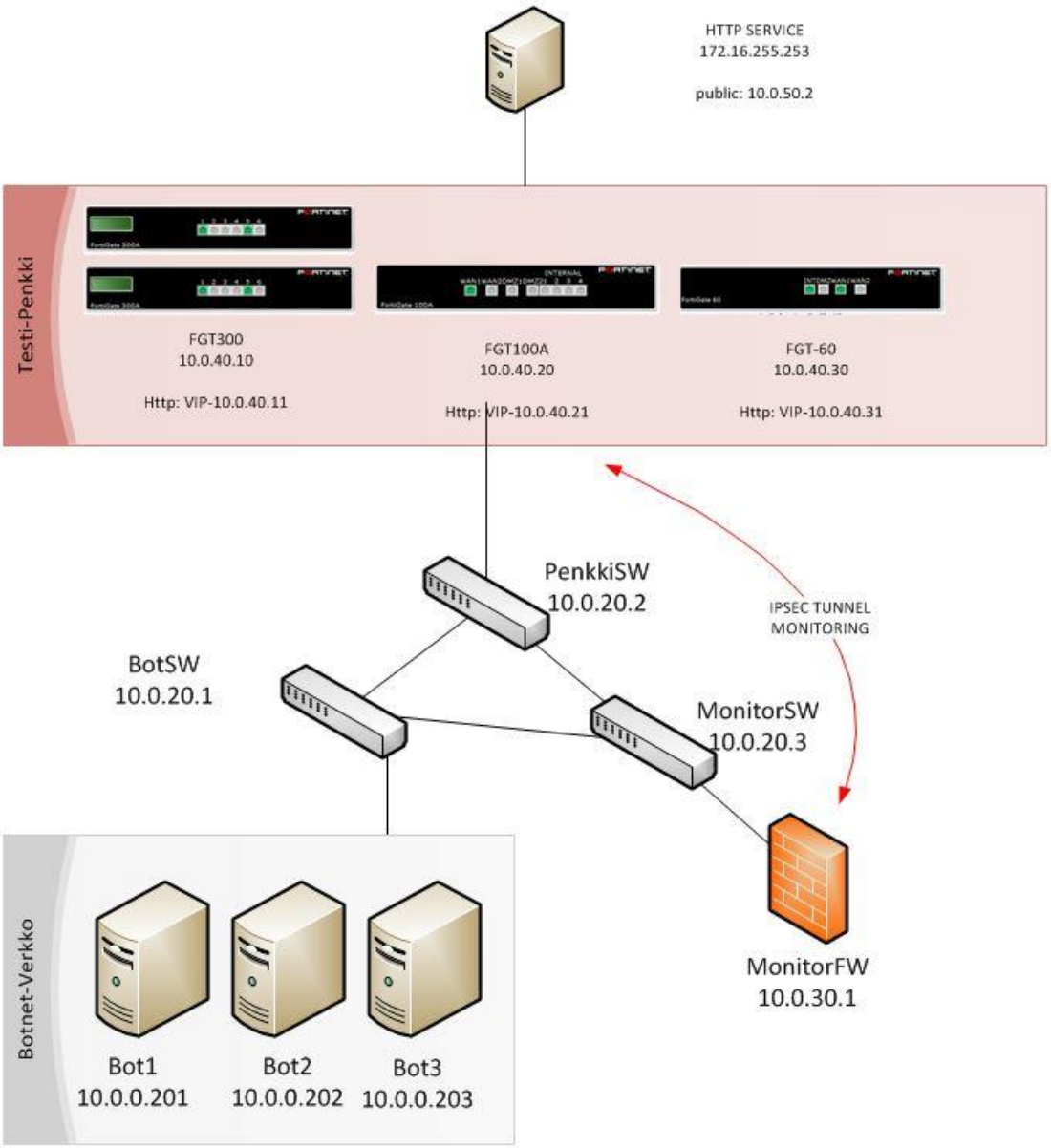
Kytkimet on nimetty nimillä ”MonitorSW”, ”BotnetSW” ja ”PenkkiSW” vastaamaan laitteeseen kytkettäviä fyysisiä laitteita. MonitorSW-laitteeseen kytketään valvontaan käytettävä palomuuri, jonka takaa simuloidaan palvelun valvontaa. BotnetSW-kytkimeen kytketään palvelunestohyökkäystä tekeviä laitteita ja PenkkiSW-kytkimeen testattavat palomuurit.

Tarkoituksena oli simuloida internetistä tulevaa palvelunestohyökkäystä, joiden kohteena ovat testattavat palomuurit (kuva 20, *Test-Penkki*) ja niiden takana oleva http-palvelu (kuva 20, *HTTP SERVICE)*. Testauksessa keskityttiin palomuurin toimintaan hyökkäyksen alla. Ympäristön takia palomuureista tuli poistaa käytöstä ”reverse path check”-ominaisuus, joka pudottaa väärennetyn ip-osoitteen paketin. Käytännössä internetiä testausympäristössä simuloi aliverkko 10.0.0.0/16, johon hyökkäyskoneet tuottivat liikennettä.

Ympäristön toimintaa varten Rapid spanning tree (RSTP) kytkettiin käyttöön kytkimiin. Testattaviin muureihin asetettiin oletusyhdyskäytävä osoittamaan kohteeseen 10.0.0.210. Tätä kohdetta ei valvottu eikä sen toimintaa seurattu. Kytkennät on selitetty omassa dokumentissaan (Liite 1).

Hyökkäyskoneina käytettiin kolmea Ubuntu 12.04.4 LTS -konetta, joissa ajettiin ”t50”-pakettigenerointiohjelmaa luomaan palvelunestohyökkäys kohde-ip:hen. T50 ohjelma väärentää oletusasetuksilla lähettäjän ip-osoitteen. Ohjelmaan voi määrittää myös tarkasti eri protokollat mitä testataan. Ohjelmalla voidaan testata mm, OSPF-reititystä ja IPSEC-liikennettä.

Testausympäristö on rakennettu niin, ettei liikenne missään tilanteessa pääse vuotamaan internetiin. Testauksen valvontaliikenne toteutettiin paikallisesti tai valvontaan käytettävän palomuurin (kuva 20, *MonitorFW.*) lävitse.



Kuva 20. Testausympäristön yleiskuvaus. Botnet-Verkosta suoritetaan hyökkäys Testi-Penkissä olevaa palomuuria vastaan. Vuorollaan testattavana olevaa palomuuria valvotaan IPSEC-VPN tunnelin avulla MonitorFW laitteelta.

Laitteita testattiin yksitellen. Hyökkäys kohdistettiin aina yhteen testilaitteeseen kerrallaan ja sen takana olevaan HTTP-sivua ylläpitävään palvelimeen (kuva 20, *HTTP SERVICE*). Hyökkäys käynnistettiin käsin jokaiselta Botnet-Verkon koneelta, ja hyökkäys kulki lyhintä reittiä (BotSW-PenkkiSW) testivuorossa olevaan palomuuriin. HighAvailability cluster:in vaatimat kaapeloinnit, sekä testauksen sisäverkkoa kuvaavat kaapeloinnit oli toteutettu kytkimessä MonitorSW. Näin niiden sisäinen liikenne ei vaikuttanut testattavaan palvelunestohyökkäyksen liikenteeseen.

6.2 Testattavat laitteet

Testilaite 1. Fortigate 300 A

Fortigate 300A laite yksittäin on tavanomaisin laite-asennus, jossa yksittäinen laite huolehtii yksinään palomuuritoiminnoista. Tällöin laite on myös kahdentamaton yhteyspiste, jonka vikaantuminen estää koko verkon toiminnan. Yksittäisen laitteen resurssit ovat rajalliset, mutta yksittäinen laite on kustannustehokkain ja yksinkertaisin kytkettävä.

Testilaite 2. Fortigate 300A – HighAvailability Cluster, Active-Passive mode

Fortigate HighAvailability cluster on kahdennettu palomuuripalvelu. Kahdennuksen tarkoituksena on laitehäiriön yhteydessä säilyttää verkon toiminta. Active-Passive-tilassa toinen palomuurilaitteista on aktiivinen ja toinen passiivinen osapuoli. Passiivinen osapuoli tarkkailee aktiivisen toimintaa ja havaitessaan häiriön toiminnassa se ottaa aktiivisen roolin ja rupeaa huolehtimaan verkkoliikenteestä.

Testilaite 3. Fortigate 300A – HighAvailability Cluster, Active-Active mode

Active-Active-tilassa molemmat klusterin laitteet huolehtivat liikenteestä yhdessä. Pääroolin omaksunut laite jakaa tehtävät klusterin kaikille laitteille. Tässä kokoonpanossa on vain kaksi laitetta, mutta klusteriin voidaan liittää myös useampia laitteita. Kaapeloinnin ja verkon muiden aktiivilaitteiden täytyy olla konfiguroitu oikein , jotta kaikille klusterin laitteille saadaan identtiset yhteydet.

Active-Active-klusterin pitäisi teoriassa olla tehokkain mahdollinen laitekokoonpano. Tällöin kaikki laitteiden fyysiset resurssit ovat puhtaasti verkkoliikenteen käytössä.

Testilaite 4. Fortigate 100A

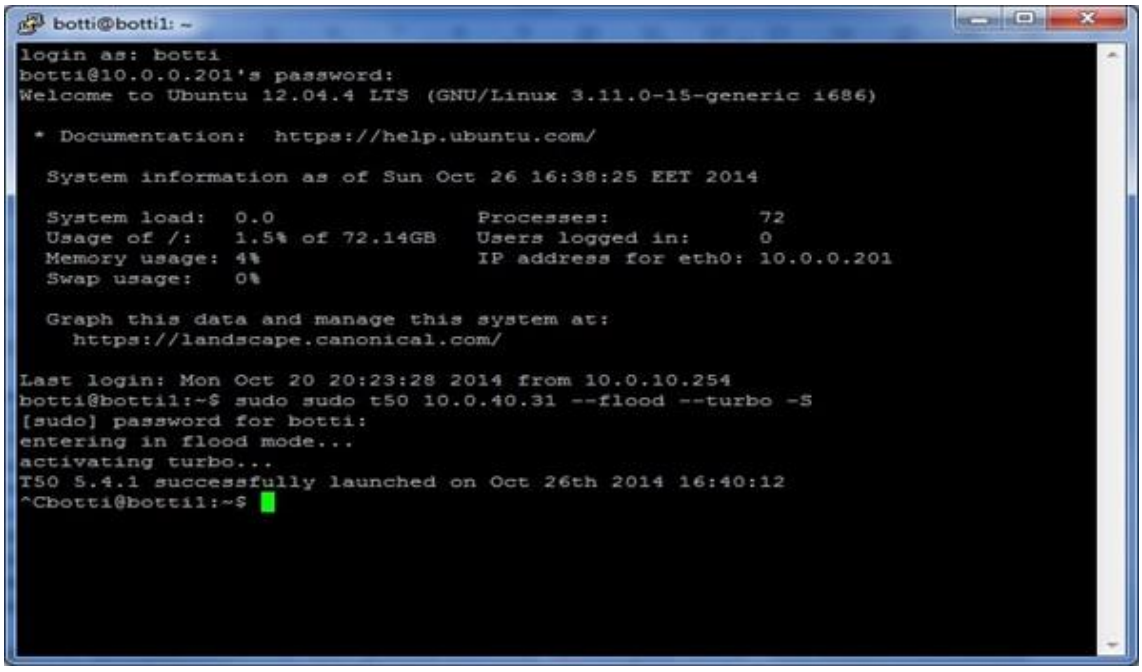
Fortigate 100A on pienempi palomuurilaite kuin 300A. Sen ominaisuudet on mitoitettu pienempään yritykseen, ja sen tekniikka on hieman vanhempaa. 100A:ssa on esimerkiksi vain 100 mb/s nopeuksiin kykenevät ethernet-portit. Laite onkin tarkoitettu etäkonttorin tai vastaavan internetyhteyspisteeksi. Fortigate 100A on jo 300A:n kanssa poistunut tuotannosta.

Testilaite 5. Fortigate 60

Fortigate 60 on testauksen vanhin laite. Poistumassa, ellei jo poistunut aktiivikäytöstä. Tarkoitettu pienten konttorien vpn-yhteyspisteeksi eikä enää nykyään sovellu kuormittavaan palomuuritoimintaan.

6.3 Testauksen kulku

Testauksessa käynnistin palvelunestohyökkäyksen SYN-FLOOD menetelmällä hyökkäyskoneista yhtäaikaisesti. T50 pakettigeneraattori määriteltiin luomaan oletusasetuksin TCP-SYN-liikennettä niin paljon kuin mahdollista (kuva 21). Käytännössä tämä tarkoittaa maksimissaan liikennettä 100 mb/sekunnissa johtuen käytettävän laitteiston porttinopeuksista.



Kuva 21. T50 ohjelman käynnistys. Ohjelman ollessa käynnissä se simuloi palvelunestohyökkäystä kohteeseen, tässä tapauksessa ip-osoitteeseen 10.0.40.31.

Valvonnan toteuttaminen testilaitteisiin osoittautui haastavaksi – palvelunesto kaatoi muurin oman hallinnan odottamatta, jolloin SNMP ja muut valvontapalvelut eivät saaneet muurista dataa. Edes muurien sisäpuolen porttiin hallintayhteyden avaaminen ei onnistunut hyökkäyksen ollessa käynnissä. Muurien oma lokitus toimi vaihtelevasti – varsinkin 300A:n variaatiot (testilaitteet 1–3), jotka joutuivat suurimman hyökkäyksen

kohteeksi johtuen suuresta porttinopeudestaan, kärsivät katkoista myös paikalliseen lokitukseen. Havainnot testauksesta perustuvat muurien omiin lokitietoihin.

Palomuureja kuormitettiin ja testattiin seuraavin asetuksin:

- Destination NAT (Kohde NAT), päällä / pois
- UTM ominaisuudet, päällä / pois
- Anti-DOS ominaisuudet, päällä / pois

Eri asetukset kuvaavat palomuurin ylläpitäjän ennakointia hyökkäykseen. Oletusasetuksilla UTM-ominaisuudet olivat palomuureista pois päältä, samoin kuin Anti-DOS-suodattimet. Riippuen organisaation julkisten ip-osoitteiden suunnittelusta muurissa voidaan ajaa NAT-osoitemuunnosta, muureja testattiin myös ilman osoitemuutoksia.

Hyökkäystä ajettiin verrattain lyhyen aikaa (5–30 minuuttia). Jo lyhyessäkin testauksessa saatiin odotettuja tuloksia, joilla voitiin muurin toimintaa arvioida.

Valmistautumaton palomuurikonfiguraatio kohde-NAT-osoitemuunnoksella oli vaikeuksissa palvelunestohyökkäyksen alla. Muurin hallintaan käytetty vpn-tunneli kytkeytyi hyökkäyksen alkaessa pois päältä. Hyökkäyksen ollessa käynnissä verkkosivuun ei päässyt lainkaan internetverkon puolelta kiinni. Sivusto vastasi normaalisti omasta sisäverkostaan eikä palvelimen kuormituksessa näkynyt muutoksia. Muurin jähmettyminen tulpaksi tietoliikenteelle pelasti tässä tapauksessa sisäverkon palvelimen suurimmalta hyökkäykseltä (kuva 22).

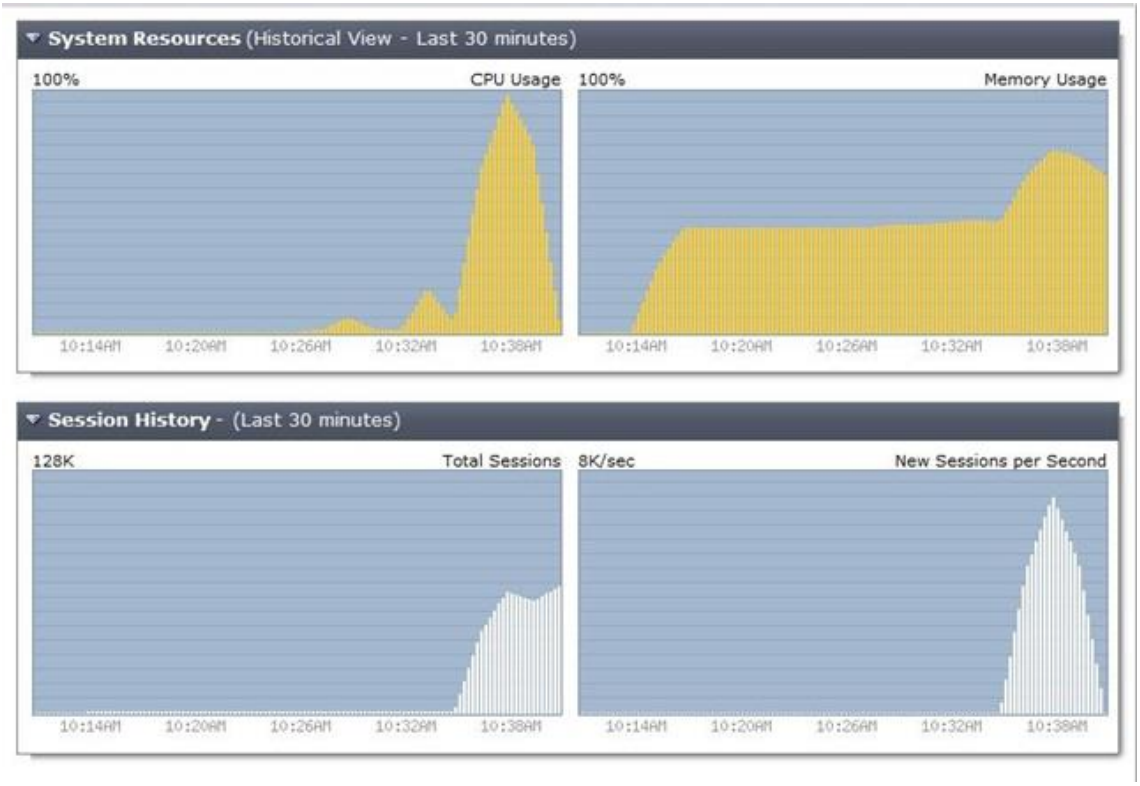
Kuva 22. FortiGate palomuuri on hyökkäyksellä lamautettu.

Kun kohde-NAT otettiin pois päältä oli palvelin suoraan kytkettynä internetiin. Suoran osoitteen avaaminen tarkoitti, ettei palomuurin tarvitse tehdä osoitemuutosta liikenteelle. Tämä vähentää palomuurin kuormaa, kun liikenne reititetään suoraan kohdelaitteelle. Vaikka muurin tehtävänä tässä testissä oli vain välittää liikennettä eteenpäin, hyökkäys sai silti aikaan järjestelmän resursseille mahdottoman tehtävän. Suojatakseen

muurin toimintaa, tiputti se käyttöjärjestelmänsä ns. Conserve modeen (vastaava kuin Linuxin kernel panic) jonka tehtävänä on suojella järjestelmän itsensä toimintaa ja ylläpitää hallittavuutta.

Suoran osoitteen käyttö on testatuista kokoonpanoista vaarallisin, sillä hyökkäys pääsi osittain Conserve mode:een siirtyneen palomuurin ohitse. Näin hyökkäys lamauttaa sekä palomuurin, valvonnan, että sisäverkon palvelimen. Voidaankin todeta, että kyseistä verkkoratkaisua ei ole optimoitu lainkaan palvelunestohyökkäysten varalta.

Hyökkäyksen tyyppi testauksessa oli TCP-flood – eli hyökkäystä ei kohdistettu vain tiettyyn palveluun tai porttiin vaan itse laitteiden verkkoyhteyksiin ja fyysisiin resursseihin. Hyökkäyksessä luotiin suuri määrä TCP-SYN-paketteja, jotka vastaanotettiin ja palomuuri muodosti jokaiselle paketille oman istuntonsa. Testauksessa luotu kuorma osui näin raskainten aina palomuurilaitteeseen (kuva 23), huolimatta siitä oliko palomuurissa käytössä NAT-osoitteenmuutos vai ei.



Kuva 23. Palomuurin järjestelmä-resurssit olivat kovilla hyökkäyksen aikana. Hyökkäysliikennettä pyrittiin käsittelemään ja tämä vaati tehoja prosessorilta ja välimuistilta. Hyökkäyspakettien luomat istunnot näkyvät myös grafiikassa.

UTM-ominaisuuksien tarkoituksena on luodata palomuurin lävistävää liikennettä haitta-ohjelmien ja tietovuotojen varalta. Fortigaten UTM-ominaisuuksiin kuuluu myös AntiVirus-skannaus, jossa kaikkea palvelimen ja asiakaskoneen välistä liikennettä tarkkaillaan ja haitalliset yhteydet tarvittaessa estetään.

Fortigate toteuttaa tämän tutkimalla sen lävistävien pakettien sisältöä. Jokainen paketti avataan ja tutkitaan, ja mikäli tarvetta on, pudotetaan. Tämä vie palomuurilta paljon muistia ja prosessoritilaa. Testissä kytkettiin käyttöön oletus UTM-suodattimet – niitä ei siis lainkaan optimoitu palvelunestohyökkäysten varalta.

UTM-suodatus on tarkoitettu löytämään normaalin liikenteen seasta haitallisia ohjelmapätkiä, ei torjumaan laajaa palvelunestoon tarkoitettua hyökkäystä. Kun liikenteen määrä ylittää laitteen raja-arvot, kytkeytyvät UTM-ominaisuudet automaattisesti toiminnasta suojellakseen palomuurilaitteen ydintoimintoja. Muuriin kohdistunut hyökkäys teki juuri näin, eli sammutti UTM-ominaisuudet hyökkäyksen käynnistyessä. Tämä ei kuitenkaan riittänyt hyökkäyksen laajuuden vuoksi – muurin toiminta pysähtyi, eivätkä UTM-ominaisuudet tuoneet mitään lisäarvoa palveluneston torjumiseen. Muurit käyttäytyivät hyökkäyksessä siis samoin kuin ilman UTM-ominaisuuksia.

Fortigate Anti-DOS-suodattimen tarkoitus on pysäyttää palvelunestohyökkäys pakettipesurin tavoin, ennen kuin haitallinen määrä paketteja pääsee kuormittamaan palomuurin reititys ja pääsylistoja. Tällöin Fortigate pyrkii pysäyttämään paketin välittömästi fyysisen portin käsittelyn jälkeen, ennen kuin siitä luodaan muuriin omaa istuntoaan ja ennen kuin muuri on ehtinyt varata siihen resursseja. Fortigate-palomuuri jättää tässä kohtaa TCP-istunnon odottamaan, hyödyntäen TCP-protokollaan kuuluvaa uudelleenlähetystä. SYN-ACK-viestiä ei lähetetä ennen vahvistavaa TCP-SYN-viestiä.

Mikäli asiakaskone ei tässä kohtaa lähetä uutta TCP SYN viestiä ja näin vahvista istunnon aitoutta, yhteys hylätään. Fortigate Anti-DOS valmistellaan määrittämällä jokaiselle liikenteelle raja-arvot. Näiden arvojen tulisi olla mahdollisimman lähellä verkkosivun oikeaa käyttöä sujuvoittaakseen palvelun käyttöä. Liikenteen ylittäessä raja-arvon Fortigate ryhtyy estämään sitä. Raja-arvot voidaan määritellä liikennetyypin mukaan kuten kuvassa 24. (FortiGate DoS Protocetion. 2014.)

Anomalies Configuration:

Name	Enable	Logging	Action	Threshold
tcp_syn_flood	☑	☐	Block	2000
tcp_port_scan	☐	☐	Pass	1000
tcp_src_session	☐	☐	Pass	5000
tcp_dst_session	☐	☐	Pass	5000
udp_flood	☑	☐	Block	2000
udp_scan	☐	☐	Pass	2000
udp_src_session	☐	☐	Pass	5000
udp_dst_session	☐	☐	Pass	5000
icmp_flood	☑	☐	Block	250
icmp_sweep	☐	☐	Pass	100
icmp_src_session	☐	☐	Pass	300
icmp_dst_session	☑	☐	Block	1000
ip_src_session	☐	☐	Pass	5000
ip_dst_session	☑	☐	Block	5000

OK Cancel

Kuva 24. FortiGaten Anti-Dos määritykset.

Raja-arvoja ja Anti-Dos-ominaisuutta käyttöön otettaessa kannattaa muistaa, että palomuurilaitteen resursseja on rajoitetusti. Voimakkaan ja pitkäkestoisen hyökkäyksen kohdalla voimakkaallekin palomuurilaitteelle rasitus voi olla liikaa. Anti-Dos-sensori ei kuitenkaan sisällä paljoakaan logiikkaa – se on vain yksinkertainen estolista, joka toimii, kun raja-arvot ylittyvät. Ohjelmistotason palvelunestohyökkäyksiin sillä ei voida vaikuttaa.

Kuva 25. Palvelunestohyökkäyksen aiheuttamaa liikennettä. Huippuliikenne ollut noin 190 Mbit/s.

Anti-Dos-ominaisuus onnistui torjumaan testiympäristössä ajetun hyökkäyksen. Hyökkäyksen taso ja teho olivat verrattain pieniä, maailmalla on havaittu useita satoja gb/s hyökkäyksiä (kuva 25). Anti-Dos-ominaisuus kuitenkin kuormitti jo tälläkin hyökkäyksellä muureja rankasti, joten muurit eivät selviäisi raskaammasta hyökkäyksestä yhtä hyvin.

Testauksessa todettiin, että Layer 3- ja 4-tason voluumipohjainen palvelunesto iskee verkon aktiivilaitteista eniten palomuuriin. Volumitasoiset hyökkäykset eivät testeissä läpäisseet palomuuria ja vaarantaneet täten palvelimen tai sisäverkon tietoturvaa, mikäli NAT-osoitteenmuunnos oli käytössä. Ilman NAT-osoitemuunnosta, palvelunestohyökkäys onnistui paikoin lamauttamaan myös kohdepalvelimen. Palvelunesto oli aina tehokas valmistelemattomaan kohteeseen ja onnistui lamauttamaan sen odotettua tehokkaammin.

Palvelunestohyökkäyksistä Layer 7, eli ohjelmistotason hyökkäys on suunniteltu enemmän palvelimien toimintaa lamauttamaan. Ohjelmistotason hyökkäystä ei voi pelkällä pakettigeneraattorilla testaamaan laboratorioympäristössä.

7 Johtopäätökset

Palvelunestohyökkäykset jotka johtuvat internetin suunnittelun yhteydessä olleesta luottamuksen ajatuksesta ovat tulleet jäädäkseen. IPv6-ratkaisussa ei ole poistettu

hyökkäysten mahdollisuutta, ja teknisesti aukottoman järjestelmän rakentaminen voikin osoittautua mahdottomaksi.

Internetin tietoturvassa palvelunesto on äänekäs ja aggressiivinen keino vaikuttaa. Sen käynnistys ja vaikutus on poikkeuksetta laajaa ja havaittavissa. Mikäli kohdeverkkoon halutaan siis vaikuttaa huomaamatta ja kohteen tietämättä, on palvelunesto siihen huonoin mahdollinen keino.

Mikäli kuitenkin halutaan siirtää kohteen huomio toisaalle tai saada suurta näkyvyyttä toimilleen on palvelunestohyökkäys hyödyllinen ase. Myös kohteen eri verkkolaitteita sillä saadaan tehokkaasti häirittyä ja samalla onnistuessaan estettyä kohteen verkkoliikenne kokonaan.

Hyvin suunniteltu palvelunestohyökkäys voi lamauttaa myös suurempia osia verkkorakenteesta. Yhdistettynä huonosti suunniteltuun verkkoratkaisuun oikeaan paikkaan kohdistettu hyökkäys voi eskaloitua isoksikin ongelmaksi. Mikäli hyökkäys pystyy lamauttamaan isompiakin verkkoja, voi se kohdistua myös internetin reunalla toimiviin yhteiskunnallisiin palveluihin. Näin yksinkertaisella palvelunestohyökkäyksellä voidaan lamauttaa jopa yhteiskunnan perusrakenteita vesihuollosta sähköverkkoihin. Paras keino suojautua tältä uhkakuvalta on tehdä verkkosuunnitelmat hyvin ja varautua ennakkoon mahdollisiin hyökkäyksiin ja prosesseihin hyökkäyksen ollessa käynnissä. Myös kriittisten palveluiden eriyttäminen internetistä on suositeltavaa.

Mitä lähempänä hyökkäyksen lähdettä päästään hyökkäykseen vaikuttamaan, sitä suuremmat todennäköisyydet palvelunestohyökkäysten vaikutusten vähentämiseen tähtäävillä toimilla on onnistua. Pilvessä toimivat palvelut ovat hyvin tehokkaita ja käyttökelpoisia suurten hyökkäysten torjunnassa. Pilvessä toimittaessa hyökkäyksen lieventämiseen voidaan määrittää automaattisesti lisää resursseja ja täten lieventää hyökkäystä itse kohdelaitteeseen.

Ohjelmistotasolla toimittaessa tulee tietää tarkkaan palvelun rakenne ja toimintaperiaate. Ohjelmistotason hyökkäys ei näy liikenteen kasvuna eikä kuormita verkon aktiivilaitteita samoin kuin voluumipohjainen, joten sen havaitseminen operaattoriverkossa toimittaessa voi olla haastavaa. Ohjelmistotason hyökkäyksen torjuntaan palvelun oletusyhdyskäytävässä toimiva laite on siis parhain.

Laboratoriotesteissä havaittiin, ettei valmistautumaton palomuuri pysty selviytymään minkäänlaisesta palvelunestohyökkäyksestä. Palomuurit tukkeutuivat liikenteestä täysin, eikä niiden hallinta onnistunut edes paikallisesti. Testeissä havaittiin, että palomuurien AntiDos-sensori parantaa palomuurin toimintaa palvelunestohyökkäyksessä, mutta ei pysty lieventämään kaikkia palvelunestohyökkäyksen vaikutuksia verkkopalveluun.

Verkon reitittimien ja palomuurien käyttöä palveluneston vaikutusten lieventämiseen kannattaa välttää. Mikäli laitteiden resursseja allokoidaan muihin kuin sen omiin tehtäviin liikaa, voi oma päämääräinen tehtävä siitä vaarantua. Lisäksi laitteiden kyky yksilöidä hyökkäävää liikennettä aidosta on kyseenalainen ja karkea. Vahingossa voidaan torjua myös hyödyllistä liikennettä. Mikäli muita laitteita ei ole käytettävissä, voidaan palomuurien omilla ominaisuuksilla (AntiDos-sensorilla) hetkellisesti lieventää palvelunestohyökkäyksen vaikutuksia.

Suomessa toimittaessa internetverkon runkorakenne pelastaa paljon. Sijaintimme internetin maantieteellisellä laidalla tarkoittaa, että yksittäinen operaattori voi tehokkaasti oman verkkonsa maantieteellisellä laidalla rajoittaa siihen tulevaa liikennettä. Näin esimerkiksi voidaan rajoittaa yhteyksiä muualta maailmasta kohteeseen www.metropolia.fi, mutta samalla säilyttää optimipalvelutaso suomalaisille käyttäjille.

Palvelunestohyökkäykset on mahdollista torjua ja niiden vaikutukset vähentää minimiin. Mikäli kyseessä on kriittinen palvelu, jonka toiminta ei saa hetkeksikään heikentyä on suositeltavaa investoida jo ennalta tehokkaisiin laitteisiin ja ohjelmistoihin, jotka kykenevät palveluneston torjumaan. Yleinen trendi maailmalla on hyökkäysten siirtyminen ohjelmistopohjaisiksi. Tämä tuo haasteen torjuntaan, kun enää ei riitä vain resurssin lisääminen verkkolaitteisiin hyökkäyksen torjuntaan.

Hyökkäyksen havaitsemista ja siihen reagointia tulee harjoitella kaikkien verkkoa valvovien kanssa. Yhteistyö eri palveluntarjoajien välillä tulee hioa saumattomaksi, jolloin toimien ja vastuiden jakautuminen on vastuullista. Tavoitteena tilanne, jossa kaikki tietävät mitä kuuluu tehdä ja kuka tekee. Mikäli kyseessä on todella kriittinen palvelu, hukataan hyökkäyksen tunnistamisessa usein paljon arvokasta aikaa, kun vastuuta pallotellaan palveluntarjoajalta toiselle eikä kukaan oikeasti vaikuta hyökkäykseen.

Palvelunestohyökkäys voi vaikuttaa myös ei julkisten verkkopalveluiden käytettävyyteen. Mikäli verkkolaiteita ja palomuureja ei ole optimoitu esimerkiksi selviämään vää-

rennetystä liikenteestä, voi se lamauttaa laitteen toiminnan vaikkei sen kautta mitään julkista palvelua ylläpidettäisikään. Hyökkäyksen voi esimerkiksi naamioida tulevaksi IPSEC-VPN tunneliliikenteeksi. Valmistautumaton laite saadaan näin epäkuntoon ja toimintakyvyttömäksi hyökkäyksen ajaksi.

Lähteet

Arbor Networks Webinars. 2014. Useita verkkodokumentteja. <http://www.arbornetworks.com/resources/media-library/service-provider-webinars>. Luettu 19.11.2014.

Defeating DDOS Attacks. 2014. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.pdf>. Luettu 19.11.2014.

Denial of service (DOS). 2014. Verkkodokumentti. F-Secure. <http://www.f-secure.com/en/web/labs_global/articles/about_denialofservice>. Luettu 19.11.2014.

FortiGate DoS Protocetion. Whitepaper. Verkkodokumentti. Fortinet <http://www.fortinet.com/sites/default/files/whitepapers/WP-DOS.pdf>. Luettu 19.11.2014.

Fortinet UTM Solution Guide. 2014. Verkkodokumentti. Fortinet. <http://www.fortinet.com/sites/default/files/solutionbrief/UTMSolutionBrief.pdf>. Luettu 27.11.

Granlund Kaj. 2007. Tietoliikenne. Jyväskylä: WSOYpro/Docendo-tuotteet.

Heinonen Arsi. 2003. Verkkohyökkäysinformaation keskitetty analysointi. Diplomityö. <http://www.tml.tkk.fi/Publications/Thesis/heinonen.pdf>. Luettu 19.11.2014.

Hyppönen, Mikko. 2013. F-Secure Oy. Tutkimusjohtaja. Luento Helsinki 13.5.2013

Matthew Tanase: Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks. 2002. Verkkodokumentti. <http://www.symantec.com/connect/articles/barbarians-gate-introduction-distributed-denial-service-attacks>. Luettu 19.11.2014.

Mellin Jorma. 2014. Teleyrityksen mahdollisuudet rajoittaa verkkohyökkäyksiä. Verkkodokumentti . TDC Oy. <https://www.viestintavirasto.fi/attachments/esitykset/Jorma_Mellin_DDoS-mitigation.pdf>. Luettu 19.11.2014.

Palvelunestohyökkäyksiltä suojautuminen. 2013. Verkkodokumentti. Nixu Oy. <http://www.nixu.com/fi/julkaisut/palvelunestohy%C3%B6kk%C3%A4ykselt%C3%A4-suojautuminen>. Luettu 19.11.2014.

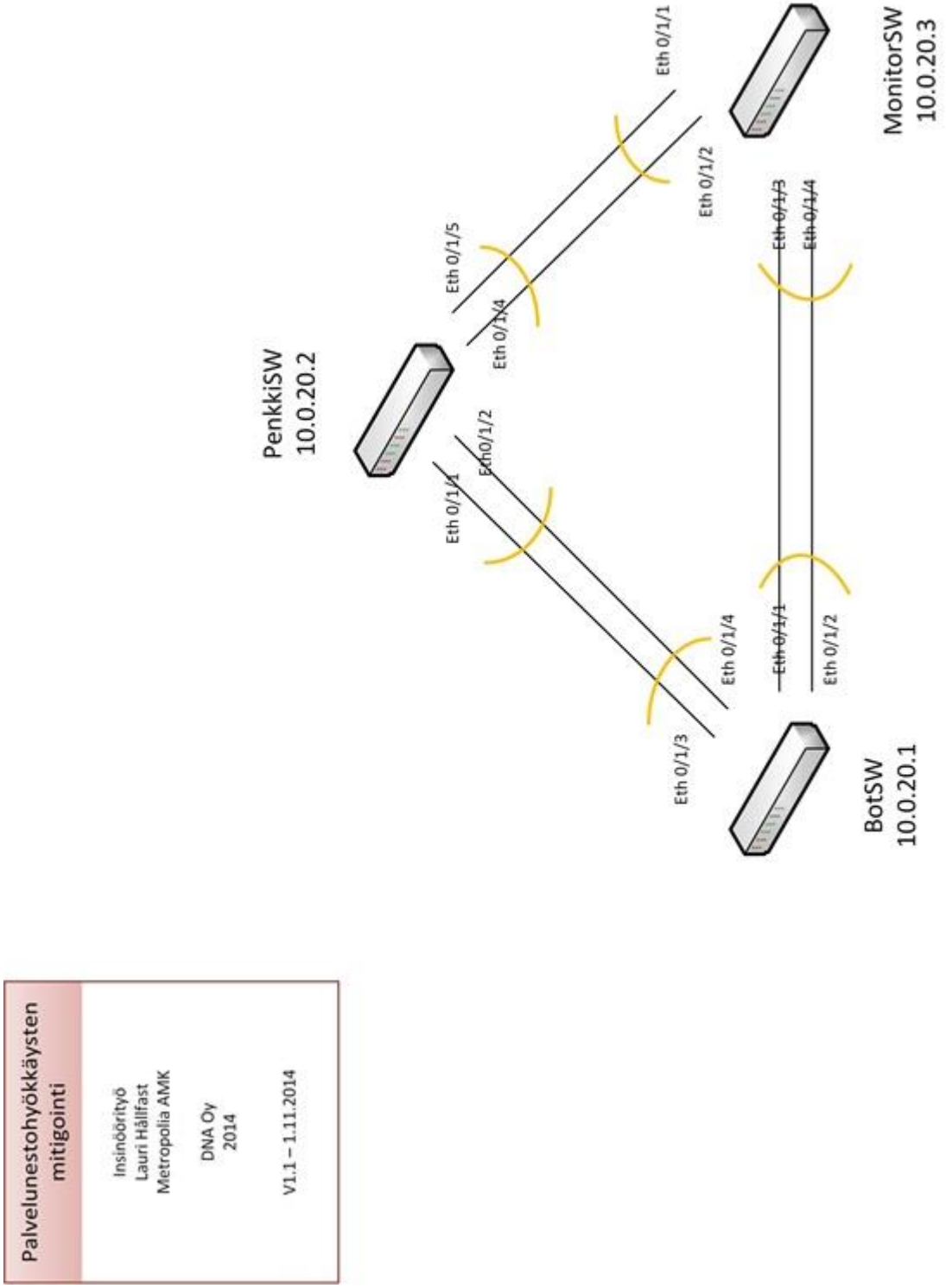
Ruohonen Mika. 2002. Tietoturva. Jyväskylä: WSOYpro/Docendo-tuotteet.

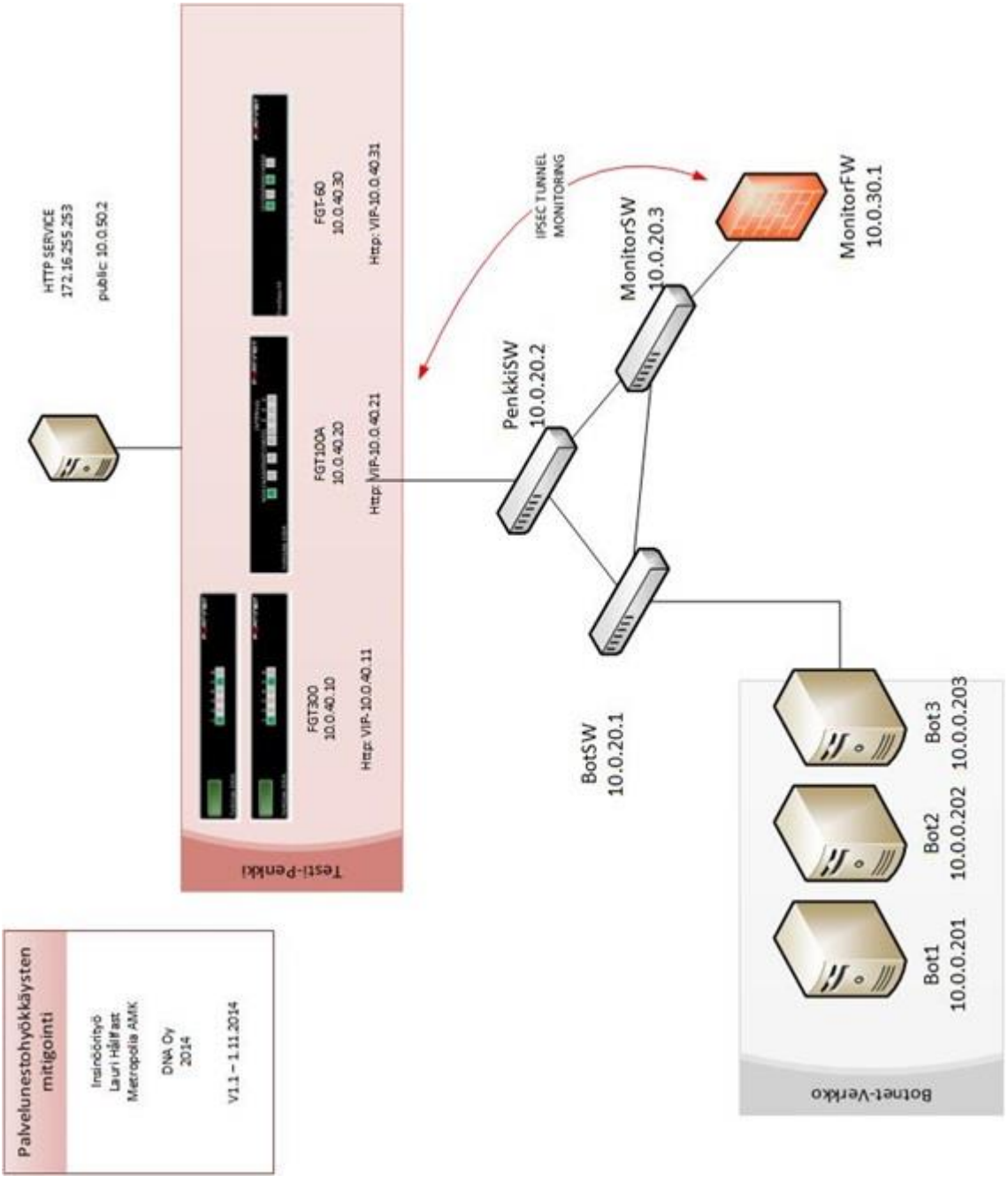
Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks. 2008. Verkkodokumentti. Cisco Systems.
<http://www.cisco.com/image/gif/paws/13634/newsflash.pdf>. Luettu 19.11.2014

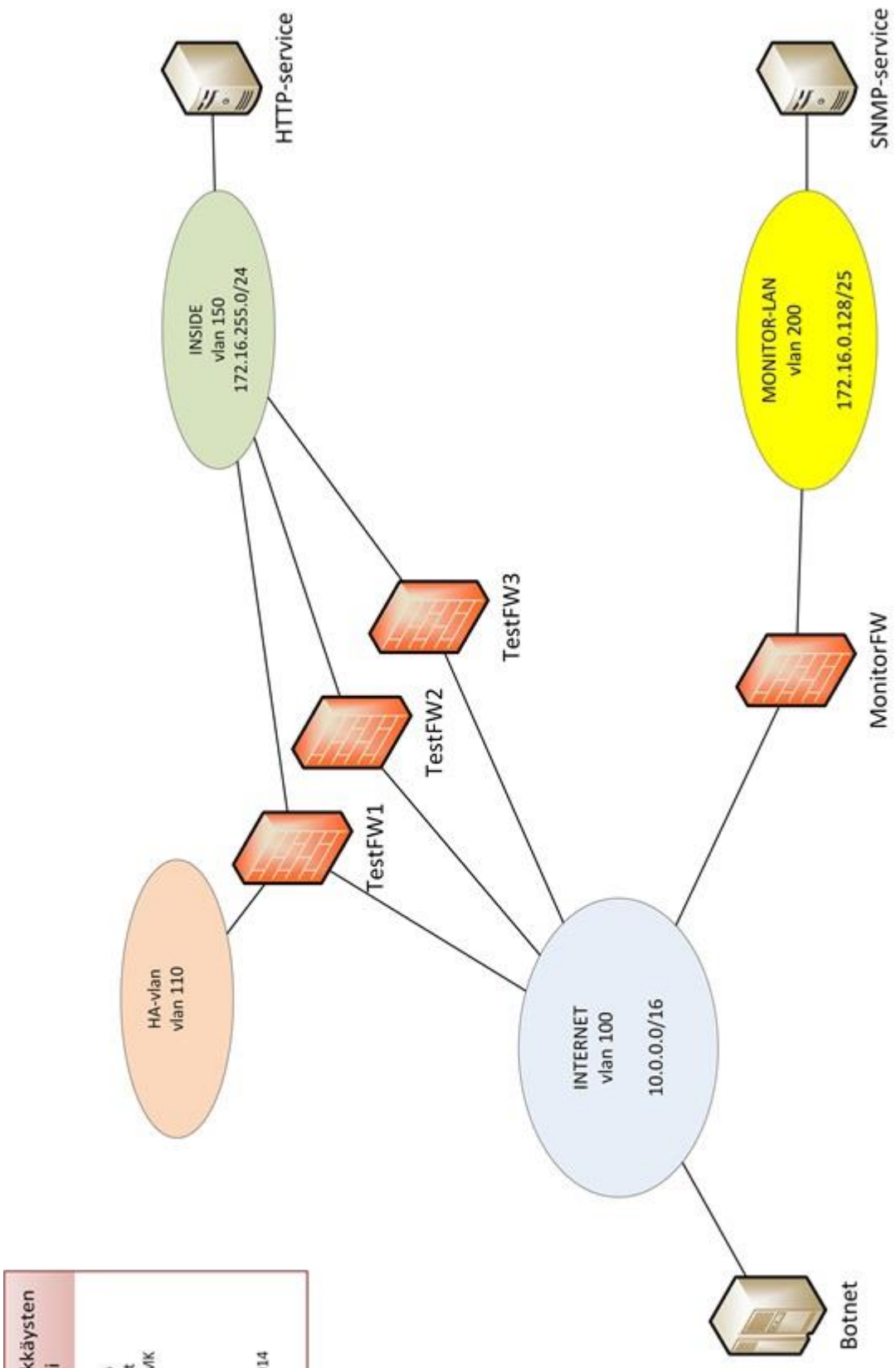
The Top 10 DDoS Trends for 2013. 2014. Verkkodokumentti. Prolexic.
<http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-top-ten-10-ddos-trends-infographic.html>. Luettu 19.11.2014.

Wikipedia, OSI-malli. 2005. Verkkodokumentti
<http://fi.wikipedia.org/wiki/Tiedosto:OSI-malli.jpg>. Luettu 19.11.2014

Liite 1: Testausympäristön graafinen kuvaus




Palvelunestohyökkäysten mitigointi
Insinöörityö
Lauri Hälfast
Metropolia AMK
DNA Oy
2014
V1.1 – 1.11.2014
Testi-Penkki
HTTP SERVICE
172.16.255.253
public 10.0.50.2
FGT300
10.0.40.10
Http: VIP-10.0.40.11
FGT100A
10.0.40.20
Http: VIP-10.0.40.21
FGT-60
10.0.40.30
Http: VIP-10.0.40.31
IPSEC TUNNEL
MONITORING
PenkkiSW
10.0.20.2
MonitorSW
10.0.20.3
MonitorFW
10.0.30.1
BotSW
10.0.20.1
Botnet-Verkko
Bot1
10.0.0.201
Bot2
10.0.0.202
Bot3
10.0.0.203


Palvelunestohyökkäysten mitigointi
Insinöörityö
Lauri Hällfast
Metropolia AMK
DNA Oy
2014
V1.1 – 1.11.2014
HTTP-service
SNMP-service
INSIDE
vlan 150
172.16.255.0/24
MONITOR-LAN
vlan 200
172.16.0.128/25
TestFW3
TestFW2
TestFW1
MonitorFW
HA-vlan
vlan 110
INTERNET
vlan 100
10.0.0.0/16
Botnet

Palvelunestohyökkäysten mitigointi

Insinöörityö
Lauri Hällfast
Metropolia AMK

DNA Oy
2014

V1.1 – 1.11.2014