POHJOIS-KARJALAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

Sami Kallinen

TUTKIMUS TIETOTURVAYHTIÖ CHECK POINTIN TUOTTEISTA

Opinnäytetyö
Toukokuu 2011

POHJOIS-KARJALAN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Toukokuu 2011
Tietotekniikan koulutusohjelma
Karjalankatu 3
80200 JOENSUU
p. (013) 260 6800

Tekijä
Sami Kallinen

Nimeke
Tutkimus tietoturvayhtiö Check Pointin tuotteista

Toimeksiantaja
Pohjois-Karjalan Ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tehdä tutkimus tietoturvayhtiö Check Pointin tuotteista. Tarkoituksena oli käsitellä yhtiön palomuuria hieman tarkemmin.

Check Pointilla on käytössä Software Blade-arkkitehtuuri, jossa jokainen ohjelma eli blade on yksi osa arkkitehtuuria. Asiakas voi rakentaa ohjelmista itselleen sopivan paketin. Kaikkia ohjelmia voidaan hallita yhden hallintakonsolin avulla. Check Pointin tuotteet voidaan jakaa kolmeen pääryhmään: Security Gateways, Endpoint Security ja Security Management. Security Gateways sisältää tuotteita, jotka on tarkoitettu koko verkon suojaamiseen, Endpoint Security-tuotteet on suunnattu verkon asiakaskoneiden suojaamiseen ja Security Management sisältää ohjelmia, joilla hallitaan ja valvotaan kahden muun tuoteryhmän ohjelmia. Check Pointin tuotteisiin kuuluu myös laitteita, joihin on valmiiksi asennettu ohjelmia.

Check Pointin tuotevalikoima on monipuolinen, ja järjestelmä on joustava. Vaatii kuitenkin harjaantumista ennen kuin järjestelmää oppii käyttämään. Palomuuri on Check Pointin ykköstuote ja se on erittäin suosittu yritysten keskuudessa. Sen suorituskyky ja luotettavuus ovat huippuluokkaa.

Kieli
suomi

Sivuja 43

Asiasanat
tietoturva, palomuuri, check point

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2011
Degree programme in
Information technology
Karjalankatu 3
80200 JOENSUU
FINLAND
Tel. +358 (13) 260 6800

Author
Sami Kallinen

Title
Research about the products of the information security company Check Point

Commissioned by
North Karelia University of Applied Sciences

Abstract

The aim of this thesis was to conduct a research about the products of the information security company Check Point. The purpose was to examine Check Point's firewall a little more thoroughly.

Check Point uses an architecture called Software Blade where each piece of software, or blade, is one part of the architecture. Customers can build a suitable bundle from the software. The whole bundle of software can managed from a single management console. Check Point's products can be divided in three main categories. These categories are Security Gateways, Endpoint Security and Security Management. Security Gateways contains products which are designed for protecting the whole network. Endpoint Security focuses on protecting the endpoints of the network and Security Management contains software for monitoring and managing the software of the other two categories. There is also appliances with pre-installed software in Check Point's product range.

Check Point's product range is diverse and the system is flexible. However, it requires some training before one learns to utilize the system. Firewall is Check Point's number one product and it is vastly used among companies. The performance and reliability of the firewall are top class.

Language
Finnish

Pages 43

Keywords
information security, firewall, check point

Lyhenteet

AD	Active Directory, käyttäjätietokanta ja hakemistopalvelu sisältäen tietoa käyttäjistä, tietokoneista ja muista verkon resursseista.
DNS	Domain Name System, järjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi.
FTP	File Transfer Protocol, TCP-protokolla käyttävä tiedonsiirtotekniikka kahden tietokoneen välillä.
GPRS	General Packet Radio Service, GSM-verkkoa käyttävä tiedonsiirtotekniikka.
HTTP	Hypertext Transfer Protocol, WWW-selainten ja -palvelinten käyttämä tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure, salattu versio HTTP:stä.
ICMP	Internet Control Message Protocol, TCP/IP:n kontrolliprotokolla viestien lähettämiseen nopeasti koneelta toiselle.
IKE	Internet Key Exchange, protokolla, jolla luodaan turvallinen yhteys Ipsec:ssa.
IM	Instant Messaging
IP	Internet Protocol, TCP/IP-protokolla, joka toimittaa IP-datapaketit lähettäjältä vastaanottajalle.
IPsec	IP Security Architecture, joukko TCP/IP-protokollia, joilla turvataan Internet-yhteydet.
LAN	Local Area Network, tietoliikenneverkko, joka toimii rajatulla maantieteellisellä alueella.
LDAP	Lightweight Directory Access Protocol, hakemistopalvelujen käyttämä protokolla, jolla hakemistoja luetaan ja muokataan.
OTP	One Time Password, salasana, joka on voimassa vain yhden kirjautumiskerran.
P2P	Peer to Peer, verkko, joka ei sisällä palvelin- ja asiakaskoneita vaan kaikki verkon jäsenet ovat tasavertaisessa asemassa toisilleen ja toimivat sekä palvelimena että asiakkaana.
POP3	Post Office Protocol version 3, TCP/IP-protokolla, jota käytetään sähköpostin noutamiseen etäpalvelimelta.

SMTP	Simple Mail Transfer Protocol, protokolla, jota käytetään sähköpostin siirtämiseen IP-verkkojen halki.
SNX	SSL Network Extender.
SSL	Secure Sockets Layer, salausprotokolla Internet-liikenteen suojaamiseen.
TCP	Transmission Control Protocol, tiedonsiirtoprotokolla, jolla siirretään dataa koneelta toiselle Internetin yli.
UDP	User Datacgam Protocol, yhteydetön protokolla, jonka avulla tietokone voi lähettää tietoa toiselle koneelle IP-verkon kautta ilman, että koneiden välille tarvitsee luoda erillistä yhteyttä.
VPN	Virtual Private Network, mahdollistaa turvallisen ja salatun yhteyden yksityiseen verkkoon Internetin tai muun julkisen verkon yli.
WEB 2.0	Termi, jolla viitataan sosiaalisen median sovelluksiin.
WLAN	Wireless Local Area Network, toimii samankaltaisesti kuin LAN, mutta langattomasti

Sisältö

1 Johdanto

Tämän opinnäytetyön tarkoituksena on tutkia tietoturvayhtiö Check Pointin tuotteita ja tarkastella yrityksen tarjoamaa palomuuria hieman tarkemmin. Työtä pohjustetaan aluksi kertomalla tietoturvasta yleisesti.

Pohjois-Karjalan ammattikorkeakoululla tietoliikennetekniikan opettajilla olisi kiinnostusta ottaa Check Pointin palomuuri mukaan opetukseen. Tämä ei kuitenkaan ole niin yksinkertaista, sillä Check Pointin järjestelmä vaatii jonkin verran perehtymistä, eikä aiheesta ole saatavilla kovin paljon valmista informaatiota. Tässä työssä tutustutaan palomuuriin ja samalla myös muihin tuotteisiin ja näin työ voisi toimia pohjustuksena sille jos koululla tulevaisuudessa tullaan ottamaan Check Point käyttöön.

Tarkoituksena ei ole tehdä mitään Check Pointin mainosesitettä, vaan tarkastella yritystä ja tuotteiden ominaisuuksia puolueettomasti. Lopuksi aion toki kertoa hieman omia mielipiteitäni tutkimusteni ja kokemusteni pohjalta.

2 Tietoturva

Tietoturva on ollut yrityksille tärkeä asia jo pitkään. Yritykset kasvavat ja yrityksen sisäinen kommunikaatio nousee suureen rooliin. Turvallisen kommunikaation takaamiseksi täytyy myös yrityksen tietoturvan olla kunnossa. Nykyään yritykset ottavat tietoturvan erittäin vakavasti ja satsaavat siihen paljon.

Tietoturvalla tarkoitetaan yrityksen tärkeiden tietojen suojaamista, niin että ulkopuoliset eivät pääse niihin käsiksi. Toisin sanoen tietoturva on toimenpiteitä, joilla taataan yrityksen tietojen koskemattomuus. [1.]

Tietoturvalle asetettuja tavoitteita ovat tietojen luottamuksellisuus, eheys, kiistämättömyys, pääsynvalvonta, saatavuus ja tarkastettavuus. Luottamuksellisuus tarkoittaa sitä, että tiedot ovat vain niiden käytössä, joilla niihin on oikeus. Kaikelle dokumenteille ja tiedolle määritellään kenellä on oikeus käyttää, säilyttää ja tuhota niitä. Eheys tarkoittaa sitä, että tieto pysyy muuttumattomana kun tietoa luodaan, käsitellään ja siirretään. Kiistämättömyys on tiedon siirtoon tai käsittelyyn osallistuvien käyttäjien tunnistamisen valvomista. Pääsynvalvonta on käyttäjien tietoon käsiksi pääsyn valvomista ja rajoittamista. Saatavuus tarkoittaa tiedon viiveetöntä ja helppoa käyttöä sellaisille käyttäjille, joilla on siihen oikeus. Tarkastettavuudella tarkoitetaan sitä, että tieto on pystyttävä tarkastamaan ja sen oikeellisuus pitää pystyä osoittamaan, sen jälkeen kun tietoa on käsitelty. [1.]

Tietoturva pitää sisällään erilaisia suojausmenetelmiä, jotka voidaan jakaa kolmeen osaan. Nämä osat ovat fyysinen, hallinnollinen ja tekninen tietoturva. Fyysisellä tietoturvalla tarkoitetaan sitä, että laitteet pidetään turvassa ulkopuolisilta esimerkiksi säilyttämällä niitä lukitussa tilassa. Hallinnollinen tietoturva tarkoittaa yrityksen työntekijöiden riittävää osaamista tietoturvan suhteen. Tähän sisältyy esimerkiksi tieto siitä miten salasanoja ja käyttäjätunnuksia pitää käsitellä. Teknisessä tietoturvassa pyritään siihen, että käytössä olevissa laitteissa ja ohjelmissa ei olisi puutteita tietoturvassa. Tätä asiaa on syytä miettiä jo siinä vaiheessa kun uusia laitteita tai ohjelmia hankitaan. [1.]

3 Check Point

3.1 Yhtiö

Check Point Software Technologies Ltd. on maailmanlaajuinen yritys, joka tuottaa tietotekniseen tietoturvaan liittyviä ohjelmia, laitteita ja palveluita. Laajaan kirjoon kuuluu tietoverkkoa, dataa ja tietokoneita suojaavia tuotteita. Tuotteet on suunniteltu ammattikäyttöön ja yrityksille. Tuotteet ovat kaupallisia, mutta joista-

kin tuotteista on saatavilla 30 päivän ilmaisia kokeiluversioita. Check Pointin tuotteet voidaan jakaa kolmeen osaan: Security Gateways, Security Management ja Endpoint Security [2].

Check Pointilla on käytössä Software blade-arkkitehtuuri. Software bladet ovat itsenäisiä ja modulaarisia ohjelmia ja ne toimivat Software blade-arkkitehtuurin rakennuspalikoina. Kaikkia bladeja hallitaan yhden hallintaohjelman kautta. Asiakas voi vapaasti valita itselleen sopivat bladet. Mitään rajoituksia ei ole. Bladeja voidaan jälkeen päin myös lisätä olemassa olevaan systeemiin. Software blade-arkkitehtuuri on siis varsin joustava ja se on ohjelmistopohjainen, joten uusien laitteiden hankinta ei ole tarpeen, kun bladeja halutaan lisätä. Bladet voidaan asentaa Check Pointin laitteisiin, virtuaaliympäristöön tai jo valmiiksi yritysverkossa olevaan laitteeseen. [3.] Check Pointin tarjoamista bladeista ja laitteista kerrotaan myöhemmin tarkemmin.

3.2 Security Gateway Software Blades

Security Gateway bladeista asiakas voi koota itselleen sopivan paketin tietoturvaohjelmia. Nämä bladet ovat koko verkkoa suojaavia ohjelmia. Seuraavissa luvuissa kerrotaan Security Gateway bladeista tarkemmin. Myös palomuuri kuuluu tähän ryhmään, mutta siitä kerrotaan myöhemmässä luvussa tarkemmin.

3.2.1 IPsec VPN

IPsec VPN on ohjelmisto, joka turvaa tietoliikenneyhteydet asiakkaan tietoverkon, etä- ja mobiilikäyttäjien, sivukonttoreiden ja yrityksen yhteistyökumppaneiden välillä. Tässä ohjelmassa yhdistyy autentikointi, salaus ja käyttäjien käyttöoikeuksien hallinta. Verkon ylläpitäjä voi luoda ja hallita VPN:iä käyttäen mesh- tai tähtirakennetta ja oman harkinnan mukaan turvata koko VPN:än salatun liikenteen, osan salatusta liikenteestä tai antaa liikenteen kulkea turvaamatta.

IPsec VPN tukee sekä verkkoalueisiin perustuvaa VPN:ää, jossa määritellään ne verkon osat, joihin pääsee ainoastaan salatun VPN:än kautta, että reititykseen perustuvaa VPN:ää, jossa määritellään liikenne, joka salataan VPN:än määrittelyjen mukaan. [4.]

IPsec VPN suojaa palvelunestohyökkäyksiltä käyttäen mekanismia, jossa tuntemattomasta yhdyskäytävästä tulevaa yhteyttä pyydetään ratkaisemaan laskennallisesti vaativa pulma ennen kuin verkosta varataan yhteydelle resursseja. Tämä mekanismi on erityisen tehokas suojautuessa IKE-palvelunestohyökkäyksiltä. [4.]

Etäkäyttäjille on tarjolla kolme eri käytäntöä, joilla he voivat liittyä edustamansa yrityksen verkkoon käyttäen VPN:ää. Toimistokäytäntö kapseloi IP-paketit käyttäen etäkäyttäjän alkuperäistä IP-osoitetta, ja näin he ikään kuin näyttävät olevan toimistossa. Toimistokäytäntöön kuuluu myös tehostettu suoja identiteettihuijauksia vastaan varmistamalla, että käyttäjän IP-osoite on autentikoitu ja nimetty käyttäjälle. [4.]

Vierailijakäytäntö on suunniteltu työntekijöille, jotka ovat paikassa, jossa yhteys Internetiin on rajattua. Esimerkiksi asiakkaan toimistossa saattaa olla käytössä vain verkkoselaaminen HTTP- ja HTTPS-porttien kautta. [4.]

Keskitinkäytännössä kaikki liikenne tutkitaan tarkasti ja keskitetysti. Näin jokaisessa toimistossa ei tarvitse erikseen ottaa käyttöön turvallisuustoimintoja ja silti työntekijöille saadaan turvalliset yhteydet tietokoneelta toiselle. [4.]

3.2.2 Mobile Access

Mobile Access-ohjelma tarjoaa liikkuvien käyttäjien älypuhelimille ja kannettaville tietokoneille etäyhteyden yrityksen verkkoon Internetin kautta käyttäen SSL VPN:ää. Mobiilikäyttäjällä on yhteyden luontiin käytössä työkalut Check Point

Mobile Client, SSL VPN Portal ja SNX, joista käyttäjä voi valita itselleen sopivimman vaihtoehdon. [4.]

Check Point Mobile Client on yksinkertainen ja turvallinen ratkaisu yrityksen verkkoon yhdistämisessä. Kyseessä on asiakasohjelma, joka asennetaan älypuhelimeen tai tietokoneeseen ja sen avulla saadaan luotua VPN-yhteys. [4.]

SSL VPN Portal luo portaalin työntekijän ja yritysverkon välille Internet-selaimen avulla. Yhteyden ollessa käytössä, selaimen välimuistin tiedot salataan ja kun yhteys päättyy, kaikki tiedot välimuistista poistetaan. SSL VPN Portal voidaan konfiguroida niin, että se lähettää OTP:n esimerkiksi käyttäjän puhelimeen tekstiviestinä. Saatavilla on myös valinnainen haittaohjelmien skannaaja, joka paikantaa haitalliset ohjelmat ja ohjaa käyttäjiä haittojen poistamiseen. [4.]

SNX on ratkaisu niille mobiilikäyttäjille, joiden tarvitsee päästä käsiksi sellaisiin verkkosovelluksiin, jotka eivät ole WWW-pohjaisia. SNX on Internet-selaimen laajennus, jonka avulla IP-pohjaiset sovellukset voivat luoda yhteyden yritysverkkoon. SNX tukee kaikkia IP-sovelluksia kuten ICMP:tä, UDP:tä ja TCP:tä. Tämä laajennus ladataan automaattisesti mobiilikäyttäjien laitteille SSL VPN Portalin kautta. [4.]

3.2.3 Identity Awareness

Identity Awareness on ohjelma, jonka avulla hallitaan käyttäjiä ja sovelluksia luomalla identiteettiin perustuvia käytäntöjä. Käytäntöihin voidaan lisätä käyttäjiä, käyttäjäryhmiä laitteita. Jokaiselle käytännölle voidaan asettaa erilaiset oikeudet ja näin verkon ylläpitäjä voi kontrolloida mihin verkon osiin milläkin käyttäjällä on oikeus päästä. [4.]

Identity Awarenessin avulla voidaan selvittää käyttäjien identiteetti ja hyödyntää tätä tietoa lisätessä käyttäjää käytäntöihin. Identiteetin selvittämiskeinoja ovat asiakasohjelmaton tunnistus, captive portal ja identiteettiagentti. [4.]

Asiakasohjelmaton tunnistus tapahtuu AD:tä hyödyntäen. Tämä tapa on helppo ja nopea, sillä käyttäjän laitteelle tai AD-palvelimelle ei tarvitse asentaa mitään. Lisäksi tämä tapa on avoimesti käyttäjän nähtävillä. [4.]

Captive portal on keino selvittää identiteetti tunnistamattomilta käyttäjiltä. Käyttäjän pitää autentikoida itsensä web-käyttöliittymän kautta ennen kuin hänellä on oikeus päästä käsiksi tietoihin, joihin pääsy on kyseiselle käyttäjälle sallittu. [4.]

Identiteettiagentti on ohjelma, joka asennetaan käyttäjän tietokoneelle. Sieltä käsin se selvittää käyttäjän identiteetin ja välittää sen yhdyskäytävään. Näin käyttäjä tunnistetaan heti kun hän kirjautuu verkkoalueelle. Agentti lisää myös merkinnän käyttäjän lähettämään dataan ja näin suojaa identiteettihuijauksilta. [4.]

Selvitettyjä identiteettitietoja voidaan myös jakaa tietylle yhdyskäytävälle tai koko verkon alueelle. Tämä mahdollistaa sen, että käyttäjän tarvitsee autentikoida itsensä vain kerran vaikka hänen tarvitsisi päästä käsiksi toisen yhdyskäytävän alueella oleviin tietoihin. Vähemmän autentikointikertoja tarkoittaa myös vähemmän rasitusta verkolle. [4.]

3.2.4 Application Control

Application Control-ohjelma tarjoaa keinon tunnistaa, sallia, estää tai rajoittaa Web 2.0-sovelluksia. Esimerkiksi yritys voi halutessaan estää työntekijöiden pääsyn tietyille Internet-sivuille tai joidenkin Internetin kautta toimivien sovellusten käytön. Käyttäjille ja käyttäjäryhmille on mahdollista antaa erilaisia pääsyoikeuksia. Check Pointilla on laaja tietokanta Internet-sovelluksista. Tästä tietokannasta verkon ylläpitäjä voi valita sovellukset ja pääsyoikeudet eri käyttäjille. [4.]

Application Control kertoo työntekijälle häntä koskevista sovellusten pääsyoikeuksien rajoituksista ja ohjeistaa työpaikan käytäntöjä Internet-sovellusten suhteen. Ylläpitäjä voi myös asettaa ohjelman kysymään työntekijältä käyttääkö hän sovellusta työhön vai huviin ja näin saada paremman kuvan yrityksen verkon resurssien käytöstä. Voidaan myös tarkastella koko yrityksen työntekijöiden Internetin käyttöä yhtenä suurena tilastona. [4.]

3.2.5 Intrusion Prevention System

Intrusion Prevention System on ohjelma, joka estää luvattomat tunkeutumiset yritysverkkoon. Tämä ohjelma täydentää Check Pointin palomuurin suojausta. Intrusion Prevention System suojaa haitallista ja ei-toivottua liikennettä, kuten haittaohjelmien hyökkäyksiä, palvelunestohyökkäyksiä, sovellusten ja palvelimien heikkouksien hyväksikäyttöä, yritysverkon sisältä tulevia uhkia ja ei-toivottujen sovellusten liikennettä vastaan. Tietoliikennettä voidaan myös estää tai sallia datan maantieteellisen lähteen tai kohteen perusteella. Tietyltä maantieteelliseltä alueelta liikenne voidaan esimerkiksi sallia täysin ja toiselta alueelta estää kokonaan. [4.]

Verkon ylläpitäjän on mahdollista käyttää ohjelmaa hiekkalaatikkoympäristössä ja näin tehdä kokeiluja vaikuttamatta verkon suorituskykyyn. Intrusion Prevention System on mahdollista asettaa aktivoimaan uudet suojauskäytännöt automaattisesti. Suojausten käyttöönottoa voidaan kontrolloida erilaisia parametrejä käyttäen. Näin jatkuva ja yksilöllinen suojausten hallinnointi vähenee. Kaikkien suojauskäytäntöjen tapahtumia voidaan tarkastella lokeista ja näin jäljittää jokin tietty tapahtuma. [4.]

3.2.6 Data Loss Prevention

Data Loss Prevention on verkossa liikkuvan, arkaluontoisen datan tahatonta häviämistä ennalta ehkäisevä ohjelma. Tähän sisältyy myös datan vääriin käsiin

joutuminen. Tämän ohjelman avulla käyttäjän on mahdollista korjata datan häviämisen uhat, ilman että muun henkilöstön, kuten mikrotuen, tarvitsee käyttää työaikaa asiaan. Ohjelma ilmoittaa käyttäjälle, kun arkaluontoisen tiedon havaitaan olevan vaarassa ja käyttäjä voi reagoida tilanteeseen reaaliajassa. [4.]

Data Loss Prevention voidaan asettaa valvomaan tiettyjen protokollien tai sovellusten liikennettä. Voidaan myös määritellä millaisen datan häviämistä halutaan ehkäistä. Valvontakäytännöt voidaan määritellä käyttäjäryhmä-, yhdyskäytävä- ja verkkokohtaisesti. [4.]

3.2.7 Web Security

On olemassa haittaohjelmia, jotka on ohjelmoitu niin, että ne keskittävät hyökkäyksensä web-palvelimia kohtaan. Check Pointin Web Security on ohjelma, joka suojaa näitä hyökkäyksiä vastaan. Ohjelma tunnistaa web-palvelimen liikenteestä datan osat, jotka sisältävät haittaohjelman koodia ja osaa päätellä kuinka suuresta uhasta on kyse. Web Securitylla on neljä toimenpidettä, joita se suorittaa jatkuvasti. Ensinnäkin se tarkkailee liikennettä exe-tiedostojen koodin varalta. Toiseksi se vahvistaa, että exe-tiedoston koodia todella on datassa. Kolmanneksi se tunnistaa onko löydetyn exe-tiedoston koodi haitallista, ja neljänneksi se estää haitallisen exe-tiedoston pääsyn kohteeseensa. [4.]

Web Securityyn kuuluu teknologia nimeltä Advanced Streaming Inspection. Tämä osa ohjelmasta käsittelee web-liikennettä kokonaisvaltaisesti, eikä keskity ainoastaan exe-tiedostoihin. Advanced Streaming Inspection voi muokata web-yhteyden sisältöä lennossa. Esimerkiksi HTTP-otsikon tietoja voidaan ikään kuin vääristää niin, että otsikon tiedot web-ympäristöstä ovat piilossa. Piilotettavia tietoja ovat käyttöjärjestelmän ominaisuudet sekä web-palvelinten ja backend-palvelinten identiteetit. Nämä tiedot ovat erittäin tärkeitä tietomurtojen kannalta. Web-palvelimen lähettämä data voidaan pysäyttää ja ylläpitäjän on mahdollista piilottaa tärkeät tiedot kokonaan tai käyttää aiemmin mainittua tietojen vääristämistä ja näin hämätä mahdollista tietomurron tekijää. [4.]

3.2.8 URL Filtering

URL Filtering on ohjelma, joka estää pääsyn haitalliseksi määritellyille Internet-sivuille. Ohjelma sisältää esikonfiguroituja käytäntöjä, jotka estävät Internet-sivuja niiden sisällön mukaan. Käytännöt päivittyvät automaattisesti sitä mukaa kun uusia sivuja tulee ilmi. [4.]

Ohjelma ilmoittaa käyttäjälle kun estetylle sivulle pääsyä yritetään ja ohjaa lisätietoon käyttäjän niin halutessa. Käytössä on myös white list ja black list. Tämä tarkoittaa sitä, että tietyille käyttäjille tai palvelimille voidaan antaa tavallista suuremmat (white list), tai tavallista pienemmät (black list) pääsyoikeudet Internet-sivuille. [4.]

3.2.9 Antivirus & Anti-Malware

Tämä on varmasti se kaikista tutuin tietoturvaohjelma keskiverto käyttäjälle. Antivirus & Anti-Malware suojaa HTTP:n, FTP:n, SMTP:n ja POP3:n kautta kulkevia viruksia, matoja ja troijanhevosia vastaan. Ohjelma pysäyttää virukset ja muut uhat jo yhdyskäytävässä ennen kuin ne ehtivät työntekijöiden tietokoneille. [4.]

Antivirus & Anti-Malware tarkastaa tietokoneelle ladattavat tiedostot ja virustartunnan löytyessä estää tiedonsiirron. Näin estetään tartunnan leviäminen tietokoneelle. Ohjelmalla voidaan valvoa datan kulkua molempiin suuntiin. Esimerkiksi yritysverkosta lähtevää dataa tai yritysverkkoon saapuvaa dataa. Verkossa kulkevat pakatut tiedostot puretaan ja tarkistetaan reaaliajassa. Myös tiettyjen liitäntöjen kautta kulkeva data voidaan ottaa erityistarkkailuun. [4.]

3.2.10 Anti-Spam & Email Security

Anti-Spam & Email Security on ohjelma, joka suodattaa yrityksen sähköpostista roskapostin ja suojaa sähköpostin kautta leviäviltä haittaohjelmilta. Tämä ohjelma voi suodattaa roskapostia lähettäjän IP-osoitteen perusteella. Jos IP-osoite on todettu uhaksi, ohjelma estää tästä osoitteesta saapuvat sähköpostit. Ohjelma osaa tunnistaa myös kuvaan pohjautuvat roskapostit ja ulkomaan kielellä kirjoitetut roskapostit. [4.]

Anti-Spam & Email Security tarkastaa kaikki sähköpostit virusten ja muiden haittaohjelmien varalta. Sähköpostiviestin sisältö, kuten myös viestin sisältämät liitteet tutkitaan. Myös sähköpostijärjestelmän kautta tapahtuvat tietoturvahyökkäykset, kuten palvelunestohyökkäykset pystytään estämään. [4.]

3.2.11 Advanced Networking

Advanced Networking-ohjelma useita ominaisuuksia, jotka helpottavat tietoturvan käyttöönottoa suurissa tietoverkoissa. Näitä ominaisuuksia ovat dynaaminen reititys, tuki monilähetykselle (multicast), QoS (Quality of Service), Internet-palveluntarjoajien redundanssi ja sovellusten kuormituksen tasaaminen. Tästä ohjelmasta on eniten hyötyä suuryrityksille, joille verkon suorituskyky ja tiedon nopea saatavuus ovat tärkeitä. [4.]

Advanced Networking tukee dynaamisia reititysprotokollia, kuten BGP:tä, OSPF:ää RIPv1:tä ja RIPv2:ta. Näistä kolme jälkimmäisintä mahdollistavat dynaamisen reitityksen yksittäisen autonomisen järjestelmän, kuten yrityksen osaston, yrityksen tai palveluntarjoajan yli. Tällä voidaan estää tietoverkon häiriöitä. BGP mahdollistaa dynaamisen reitityksen monimutkaisempien, useista autonomisista järjestelmistä koostuvien tietoverkkojen halki. Kahden palveluntarjoajan käyttö ja verkon jakaminen osiin, niin että verkolla on useita ylläpitäjiä ovat esimerkkejä BGP:n käytöstä. Advanced Networking tukee myös multicast-protokollia, kuten IGMP:tä, PIM-DM:ää ja PIM-SM:ää. [4.]

QoS:n avulla voidaan yrityksen kannalta tärkeälle tietoliikenteelle antaa korkeampi prioriteetti kuin tavalliselle liikenteelle. Sen avulla on myös mahdollista varata osa kaistanleveydestä pysyvästi videokokoussovellukselle ja vastaaville korkean prioriteetin sovelluksille. Lisäksi tietyille käyttäjille voidaan antaa tavallista korkeampi prioriteetti, jopa silloin kun he ovat etäkäyttäjiä VPN-tunnelin kautta. [4.]

Internet-palveluntarjoajien redundanssi takaa luotettavan yhteyden Internetiin. Jos käytössä olevan palveluntarjoajan yhteydessä on vikaa, voidaan ottaa käyttöön varalla oleva palveluntarjoaja. Myös molempien palveluntarjoajien yhtäaikainen käyttö on mahdollista. Näin liikenne voidaan tasata palveluntarjoajien kesken ja kummankin rasitus jää vähäiseksi. [4.]

Sovellusten kuormituksen tasaamisella tarkoitetaan sitä, kun jokainen yhteyspyyntö verkossa ohjataan tietylle palvelimelle määrättyjen sääntöjen mukaan. Näin sovellusten tuottamaa rasitusta voidaan tasata palvelimien kesken. Yhteyspyyntö ohjataan palvelimelle, joka on pienimmän rasituksen alla ja näin mitään palvelinta ei rasiteta kohtuuttomasti. [4.]

3.2.12 Acceleration & Clustering

Acceleration & Clustering-ohjelma pitää sisällään kaksi korkean suorituskyvyn verkon suorituskykyä ja turvallisuutta tehostavaa teknologiaa. SecureXL on Check Pointin patentoima teknologia, joka luo erityisen laitekerroksen, jonka avulla turvallisuuspäätökset voidaan tehdä OSI-mallin sovelluskerroksen alatasolla ja näin ollen myös aikaisemmin. Menettelemällä näin, laitteiden suorituskyvyn aiheuttama viive vaikuttaa päätöksiin mahdollisimman vähän. Jos lähetyksen ensimmäistä datapakettia tarkastetaan tavallisin keinoin ja todetaan turvalliseksi, niin SecureXL:n luoma kerros vastaa lähetyksen jäljellä olevien pakettien tarkastuksesta. [4.]

Toinen Acceleration & Clusteringin sisältämä teknologia on ClusterXL. Tämä teknologia tarjoaa mahdollisuuden jakaa dynaamisesti tietoliikennettä useiden yhdyskäytävien kesken. Tämä takaa datan nopean ja luotettavan siirron. [4.]

3.2.13 Voice over IP

Check PointinVoice over IP-ohjelma (VoIP) tarjoaa useita eri VoIP-protokollia. Ohjelma pystyy myös havaitsemaan ja pysäyttämään haitallisen VoIP-toiminnan ilman ylläpitäjän asiaan puuttumista. Lisäksi Voice over IP sisältää QoS-mekanismeja, joilla taataan äänen korkea laatu. [4.]

Usein VoIP ja NAT on hankala saada toimimaan keskenään. Check Pointin Voice over IP ratkaisee tämänkin ongelman tarjoamalla useita vaihtoehtoja VoIP:n asentamiselle NAT-ympäristöön. [4.]

3.3 Endpoint Security Software Blades

Endpoint Security sisältää tuotteita, jotka on tarkoitettu suojaamaan verkon tietokoneita. Seuraavissa luvussa kerrotaan näistä tuotteista tarkemmin.

3.3.1 Full Disk Encryption

Full Disk Encryption on ohjelma, joka kryptaa automaattisesti tietokoneen kiintolevyn kaikki tiedot. Tämä ohjelma myös estää tiedostojen kopioinnin ja huijausohjelmien asennusyritykset jopa silloin kun kiintolevy siirretään toiseen tietokoneeseen. [5.]

Full Disk Encryption tarjoaa ominaisuuden, joka estää tietokoneen käyttöjärjestelmän lataamisen ennen kuin käyttäjä todistaa olevansa oikeutettu käyttäjä. Tämä tapahtuu esimerkiksi käyttäjätunnuksen ja salasanan avulla tai älykortilla. [5.]

3.3.2 Media Encryption

Media Encryption on ohjelma, jonka avulla voidaan kryptata USB-muistit, DVD-levyt ja muut siirrettävät laitteet, jotka ovat tietokoneessa vain väliaikaisesti. Pääsyä tietokoneen portteihin, kuten USB, bluetooth ja firewire voidaan myös rajoittaa. [5.]

Tämä ohjelma lisää digitaalisen allekirjoituksen jokaiseen kryptattuun laitteeseen ja ilmoittaa käyttäjälle mikäli laitteen tietoihin on tehty luvattomia muutoksia. Jos muutoksia havaitaan, täytyy laitteen käyttöoikeudet määritellä uudelleen ennen kuin laitetta voi käyttää uudestaan yrityksen suojatussa ympäristössä. [5.]

3.3.3 Anti-Malware & Program Control

Anti-Malware & Program Controlin toinen osa on tietokoneen haittaohjelmien havaitsemiseen ja poistamiseen tarkoitettu ohjelma ja toinen osa on ohjelma, joka sallii tietokoneella vain sellaisten ohjelmien käytön, joille on annettu siihen oikeus. Ohjelma pystyy havaitsemaan kaikenlaiset haittaohjelmat, mukaan lukien virukset, ja poistamaan ne. [5.]

3.3.4 Remote Access VPN

Remote Access VPN-ohjelma tarjoaa etäkäyttäjille turvallisen yhteyden yritysverkkoon. Ohjelma tukee IPSec VPN:ää, joten autentikointi, datan koskematto-

muus ja luottamuksellisuus ovat taatut. Ohjelma voidaan myös asettaa estämään yhteys jos käyttäjän laitteeseen ei ole asennettu tiettyä ohjelmaa, kuten esimerkiksi käyttöjärjestelmän viimeisimpiä päivityksiä. [5.]

Remote Access VPN osaa vaihtaa yhteystyyppiä automaattisesti jos käyttäjä liikkuu eri verkkotyyppien (LAN, WLAN, GPRS) alueilla. Näin käyttäjän ei tarvitse autentikoida itseään uudestaan kun yhteystyyppi vaihtuu. [5.]

3.3.5 WebCheck

WebCheck on ohjelma suojaa käyttäjää Internetistä tulevilta uhilta. Ohjelma luo virtuaalisen Internet-selaimen ja eristetyn hiekkalaatikkoympäristön selaimelle. Näin yrityksen verkko ja Internet saadaan eristettyä toisistaan. [5.]

WebCheck myös estää käyttäjän pääsyn sivuille, jotka on todettu tietourkintasivuiksi (phishing). Se osaa tunnistaa tietoa urkkivat sivut, jotka tekeytyvät oikeiksi, laillisiksi sivuiksi. [5.]

3.3.6 Check Point Abra

Check Point Abra ei ole ohjelma, vaan USB-porttiin kytkettävä laite, joka luo tietokoneeseen virtuaalisen työympäristön, joka on erillään muusta tietokoneesta. Näin käyttäjä pystyy olemaan turvallisesti yhteydessä yrityksen verkkoon missä tahansa, mukaan lukien turvattomatkin paikat, kuten hotellin tietokoneet. Abra käyttää yhteyden luomiseen VPN:ää. [5.]

3.4 Security Management Software Blades

Security Management bladet ovat ohjelmia, joilla verkon ylläpitäjän on mahdollista hallita tapahtumia, asettaa turvallisuuskäytäntöjä ja ottaa käyttöön suojauk-

sia koko verkon alueella. Tähän kaikkeen ylläpitäjän tarvitsee käyttää vain yhtä käyttöliittymää. [6.] Näillä ohjelmilla hallitaan aiemmin esiteltyjä Security Gateway bladeja ja Endpoint Security bladeja.

3.4.1 Network Policy Management

Network Policy Management tarjoaa ylläpitäjälle SmartDashboard-konsolin, jolla hallita kaikkia yrityksen käytössä olevia Security Gateway bladeja. Konsolin avulla kaikille Security Gateway bladeille voidaan asettaa sama turvallisuuskäytäntö yhdellä kertaa. Ylläpitäjällä on käytössään graafinen käyttöliittymä, jonka avulla kaikki mahdollinen konfigurointi onnistuu. [6.]

3.4.2 Endpoint Policy Management

Endpoint Policy Management on periaatteessa hyvin samanlainen kuin Network Policy Management, mutta tällä ohjelmalla hallitaan Endpoint Security bladeja. Käytetty konsoli on myös hieman erilainen, mutta toiminnot ovat suurin piirtein samat. [6.]

3.4.3 Logging & Status

Logging & Status on ohjelma, joka kokoaa kaikkien Check Pointin tietoturvaohjelmien lokitiedostot yhteen. Ohjelmille voidaan määritellä verkko-osoite, johon lokitiedostot lähetetään ja Logging & Status kokoaa tiedot kyseisestä osoitteesta. Ylläpitäjän on helppo etsiä haluamaansa tietoa kun kaikki lokit ovat samalla kertaa saatavilla. [6.]

3.4.4 SmartWorkflow

SmartWorkflow on ohjelma, jonka avulla ylläpitäjä voi jäljittää esimerkiksi palomuurin sääntöihin tai käyttäjäryhmiin tehtyjä muutoksia. Tämä on hyödyllistä jos jokin muutos on virheellinen. Muutoksia jäljitetään loogisista yksiköistä, jotka sisältävät kokoelman SmartDashboard-konsolilla tehdyistä muutoksista. [6.]

Ylläpitäjä voi selata muutoksia kronologisessa järjestyksessä tai luoda yksityiskohtaisen listan sen hetkisen session aikana tehdyistä muutoksista. Tietoa saadaan siitä, kuinka jokin kohde muuttui, kuka sitä muutti ja milloin viimeisin muutos on tehty. [6.]

3.4.5 Monitoring

Monitoring on ohjelma, joka valvoo kaikkia verkon laitteita ja näyttää kokonaiskuvan verkosta ja muutoksista joita on tehty laitteisiin, VPN-tunneleihin ja etäkäyttäjiin sekä turvallisuustoimenpiteistä. Yksittäisestä laitteesta on myös mahdollista tarkastella yksityiskohtaisempaa tietoa, kuten käyttöjärjestelmän tietoja, tietoa verkkotoiminnasta ja lisenssitiedot. [6.]

Monitoringin avulla on myös mahdollista luoda kaavioita ja taulukoita joista voidaan analysoida verkon tietoliikenteen käyttäytymistä, tarkistaa ja arvioida verkon käytön kustannuksia, tunnistaa osastoja ja käyttäjiä, jotka luovat verkkoon eniten liikennettä sekä valvoa epäilyttävää käyttäytymistä. [6.]

3.4.6 Management Portal

Management Portal-ohjelmalla voidaan antaa tietyille käyttäjille oikeus nähdä verkon turvallisuuskäytännöt, laitteet ja muut tiedot tavallista yksityiskohtaisemmin. Näillä käyttäjillä ei kuitenkaan ole oikeutta tehdä muutoksia. Esimerkiksi johtajille ja tilintarkastajille voidaan antaa tällaiset oikeudet. [6.]

3.4.7 User Directory

User Directory on ohjelma, jonka avulla Security Gateway-ohjelmat voivat käyttää hyödyksi LDAP-tekniikkaa ja noutaa verkon käyttäjien identiteetin ja turvallisuustiedot palvelimelta. Näin useita, redundanttisia, käyttäjätiedot sisältäviä palvelimia ei tarvitse pitää yllä manuaalisesti. [6.]

3.4.8 SmartProvisioning

SmartProvisioningin avulla verkon ylläpitäjä voi ottaa käyttöön turvallisuuskäytäntöjä ja kokoonpanoasetuksia useaan verkon laitteeseen samaan aikaan, vaikka laitteet olisivat maantieteellisesti laajalla alueella. Ylläpitäjä voi myös tallettaa valmiita konfiguraatioita ja ottaa ne sitten käyttöön uusissa verkon laitteissa. Tämä kaikki tapahtuu yhden käyttöliittymän avulla ja näin ylläpitäjän työ helpottuu. [6.]

SmartProvisioning voi hallita useita laitteita samaan aikaan erilaisten, luotujen profiilien avulla. Näitä profiileja on kahdenlaisia, turvallisuusprofiili ja SmartProvision-profiili. Turvallisuusprofiiliin määritellään turvallisuuskäytännöt halutulle määrälle laitteita, joilla on samat ominaisuudet. Turvallisuuskäytännöt voidaan ottaa käyttöön kaikissa määritellyissä laitteissa samaan aikaan. SmartProvisioning-profiilissa määritellään muita asetuksia, joita halutaan ottaa käyttöön. Näitä asetuksia ovat tavallisesti esimerkiksi DNS, aikavyöhyke, verkkoalueiden nimet ja reititystiedot. [6.]

3.4.9 SmartReporter

SmartReporter-ohjelman avulla verkkolaitteilta kerätyt valtavat määrät tietoa saadaan muutettua ymmärrettäväksi tiedoksi. Tämän tiedon pohjalta yritys voi tarkistaa turvallisuuskäytäntöjen tehokkuuden, suunnitella verkon kapasiteettia ja maksimoida turvallisuusinvestoinnit. [6.]

SmartReporter sisältää runsaasti valmiiksi määriteltyjä raportteja, joista voidaan valita haluttu ja tuottaa raportti tietyltä osa-alueelta. Raportteja voidaan tuottaa esimerkiksi verkon aktiivisuudesta, palomuurin turvallisuudesta, virustorjunnasta ja tiettyyn tuotteeseen liittyvistä tiedoista. Kaikki raportit myös jaetaan osioihin, joista voidaan eritellä vaikkapa tietyntyyppinen liikenne tai toiminta verkossa. Ylläpitäjä voi aikatauluttaa säännölliset raportit tapahtumaan automaattisesti ja raportit voidaan sitten lähettää tietyille käyttäjille esimerkiksi sähköpostilla. [6.]

3.4.10 Multi-Domain Security Management

Multi-Domain Security Managementin avulla olemassa oleva verkon turvallisuushallinnointi voidaan jakaa useisiin virtuaalisiin hallinta-alueisiin. Näitä hallinta-alueita voidaan luoda sijaintiin, yrityksen osastoon tai turvallisuusfunktioon perustuen. Näin ylläpito ja hallinnointi yksinkertaistuu ja myös turvallisuus vahvistuu. [6.]

Jokainen virtuaalinen hallinta-alue on itsenäinen hallinnointiyksikkö ja jokaisella yksiköllä on oma tietokanta, lokipalvelin ja omat turvallisuussäännöt. Hallinta-alueita voi luoda, hallita ja tarkastella yhdeltä hallintakonsolilta. [6.]

3.5 Laitteet

Check Pointilla on tarjolla runsas valikoima laitteita erilaisiin käyttötarkoituksiin. Kaikkiin laitteisiin on asennettu tietty kokoelma Check Pointin ohjelmia. Vaikka ohjelmat on asennettu ennakkoon, niin asiakas voi halutessaan hankkia lisää ohjelmia laitteseensa. Monet laitteet sisältävät myös redundanttisia komponentteja, joten vialliset komponentit voidaan vaihtaa ilman että laitetta tarvitsee kytkeä pois päältä.

3.5.1 Power-1

Power-1 on tuoteperhe laitteita, jotka sisältävät Check Pointin palomuurin, IP-Sec VPN:än, Intrusion Prevention Systemin, Advanced Networkingin ja Acceleration & Clusteringin. Osaan laitteista kuuluu näiden lisäksi Identity Awareness ja Application Control. Tämän tuoteperheen laitteiden sisältämät ohjelmat ovat pitkälti samat, mutta laitteet eroavat toisiltaan fyysisiltä ominaisuuksiltaan ja suorituskyvyltään. Ominaista näille laitteille on korkea suorituskyky. [7.] Laitteiden ominaisuuksia on esitelty tarkemmin taulukossa 1.

Taulukko 1. Power-1-laitteiden ominaisuuksia

	Power-1 5077	Power-1 9077	Power-1 11067	Power-1 11077	Power-1 11088
10/100/ 1000 Mb/s-portit	10/14	14/18	14/18	14/18	14/18
10 Gb/s-portit (valinnainen)	4	4	4	4	4
Palomuurin läpäisy (Gb/s)	9	16	15	20	30
VPN:än läpäisy (Gb/s)	2,4	3,7	3,7	4	4,5
Rinnakkaisia sessioita	1,2 miljoonaa				
IPS:n läpäisy (Gb/s)	7,5	10	10	12	15
VLAN:ien määrä	1024				
Tallennuskapasiteetti (GB)	160	2x160	2x250	2x250	2x250
Mitat (mm)	431 x 509.5 x 88	431 x 509.5 x 88	431 x 580 x 88	431 x 580 x 88	431 x 580 x 88
Massa (kg)	14,5	16,5	23,4	23,4	23,4
Käyttöolosuhteet	Lämpötila:5-40°C, Ilmankosteus:10-85%				

Maksimi tehonkulutus (W)	164,1	200,7	253,2	253,2	253,2

3.5.2 Series 80

Series 80 on suunniteltu yrityksen sivukonttorin käyttöön. Suorituskyky ja koko on mitoitettu paremmin sivukonttoriin sopivaksi kuin suuret, korkean suorituskyvyn laitteet. Tämä laite sisältää valmiiksi palomuurin ja IPSec VPN:än. Lisäksi mahdollisuus on ottaa käyttöön Intrusion Prevention System, Antivirus & Anti-Malware, Anti-Spam & Email Security ja URL Filtering. [7.] Series 80:n ominaisuuksia on esitelty taulukossa 2.

Taulukko 2. Series 80-laitteen ominaisuuksia

10/100/1000 Mb/s-portit	10
Mitat (mm)	220 x 152,5 x 44
Massa (kg)	1,085
Maksimi tehon kulutus (W)	16,68
Palomuurin läpäisy (Mb/s)	1500
VPN:än läpäisy (Mb/s)	220
IPS:n läpäisy (Mb/s)	720
Antiviruksen läpäisy (Mb/s)	100
Rinnakkaisia sessioita	150000
VLAN:ien määrä	1024
Käyttöolosuhteet	Lämpötila:0-40°C, Ilmankosteus:5-95%

3.5.3 VSX-1

VSX-1 on joukko laitteita, joihin voidaan luoda virtuaalisia toteutuksia tavallisista fyysisistä topologioista. Laitteisiin on mahdollista luoda virtuaalisia kytkimiä ja reitittimiä, jotka ohjaavat tietoliikennettä virtuaalisten verkkojen välillä. Virtuaaliset laitteet toimivat hyvin pitkälti samalla tavalla kuin fyysisetkin laitteet. VSX-1-

tuotteet sisältävät palomuurin, VPN:n, URL Filteringin, Intrusion Prevention Systemin, SecureXL:n ja ClusterXL:n. [7.] Laitteiden muita ominaisuuksia on kuvattu taulukossa 3.

Taulukko 3. VSX-1-laitteiden ominaisuuksia

	VSX-1 3070	VSX-1 9070	VSX-1 11060	VSX-1 11070	VSX-1 11080
Virtuaalisten järjestelmien määrä	10	150	250	250	250
Palomuurin läpäisy (Gb/s)	4,5	14	15	20	25
VPN:n läpäisy (Gb/s)	1	3,6	3,7	4	4,5
Rinnakkaisia sessioita	1 000 000	1 100 000	1 200 000	1 200 000	1 200 000
GbE-portit	10	14	14	14	14
Tallennuskapasiteetti (GB)	160	2x160	2x250	2x250	2x250
Mitat (mm)	443 x 381 x 44	431 x 509.5 x 88	431 x 580 x 88	431 x 580 x 88	431 x 580 x 88
Massa (kg)	6,5	16,5	23,4	23,4	23,4
Maksimi tehonkulutus (W)	78	201	253	253	253
Käyttöolosuhteet	Lämpötila:5-40°C, Ilmankosteus:10-85%				

3.5.4 IPS-1

IPS-1 on laite, joka sisältää Intrusion Prevention Systemin. Laite ei sisällä muita Security Gateway-ohjelmia, joten se on vahvasti erikoistunut yhteen tehtävään. Laitteessa on graafinen käyttöliittymä, ja erillinen hallintaportti, joka on normaali

ethernet-portti. IPS-1-laitteita on olemassa useita, jotka eroavat toisistaan ominaisuuksiltaan. [7.] Ominaisuuksia on esitelty taulukossa 4.

Taulukko 4. IPS-1-laitteiden ominaisuuksia

	IPS-1 2070	IPS-1 4070	IPS-1 5070	IPS-1 9070
läpäisy (Mb/s)	50	200	500	1000
10/100/1000 Mb/s-portit	4	8	12	16
Mitat (mm)	44 x 432 x 355	88 x 454 x 510	88 x 454 x 510	88 x 454 x 510
Massa (kg)	6,4	14,4	16,5	16,5
Käyttöolosuhteet	Lämpötila:0-40°C, Ilmankosteus:5-95%			

3.5.5 DLP-1

DLP-1 on laite, joka sisältää Data Loss Prevention-ohjelman. Tästä laitteesta on olemassa kahta eri versiota, joista toinen on ominaisuuksiltaan selvästi ”järeämpi”. [7.] Ominaisuuksista kerrotaan tarkemmin taulukossa 5.

Taulukko 5. DLP-1-laitteiden ominaisuuksia

	DLP-1 2571	DLP-1 9571
Käyttäjien määrä	1000	5000
Viestien käsittelykapasiteetti tunnissa	70000	350000
läpäisy (Mb/s)	700	2500
GbE-portit	6	10
Tallennuskapasiteetti (GB)	500	2x1000 (peilattu)
Mitat (mm)	443 x 381 x 44	431 x 509.5 x 88
Massa (kg)	6,5	16,5
Maksimi tehonkulutus (W)	77,5	200,7
Käyttöolosuhteet	Lämpötila:5-40°C, Ilmankosteus:10-85%	

3.5.6 IP-sarja

IP-laitteita on useita erilaisia ja niiden sisältämät ohjelmat vaihtelevat jonkin verran. Yksi laitteista sisältää ainoastaan palomuurin ja IPSec VPN:än. Toisiin kuuluu lisäksi Intrusion Prevention System, Acceleration & Clustering ja Advanced Networking. On myös olemassa laitteita, joihin sisältyy kaikkien mainittujen lisäksi Application Control ja Identity Awareness. [7.]

Osaan IP-sarjan laitteista on mahdollista asentaa ADP-moduuli (Accelerated Data Path), joka lisää laitteen suorituskykyä. Moduuli vapauttaa resursseja laitteen suorittimelta ja näin läpäisy paranee ja tietoliikenteen viive vähenee. [7.] Laitteiden muita ominaisuuksia on esitelty taulukossa 6.

Taulukko 6. IP-sarjan laitteiden ominaisuuksia

	IP282	IP297	IP397	IP567	IP697	IP1287	IP2457
10/100/1000Mb/s-portit	6	6/8	4/8	4/12	4/16	4/28	4/32
Tallennuskapasiteetti (GB)	40	40	80	80	80	80	80
Mitat (mm)	216 x 457 x 44	216 x 457 x 44	432 x 406 x 44	438 x 559 x 44	438 x 610 x 44	438 x 613 x 88	438 x 613 x 88
Massa (kg)	5,1	5,1	7,71	11,84	12,38	19,6	20,57
Palomuurin läpäisy (Gb/s)	1,5	1,5	3	6,3	11,7	17,5	30
VPN:än läpäisy (Gb/s)	1	1	0,667	1,7	3,3	8,3	8,3
IPS:n läpäisy (Gb/s)	1,4	1,4	2,9	2,9	4	7	9
Rinnakkaisia sessioita	900 000		1 000 000				

VLAN:ien määrä	1024						
ADP-moduuli saatavilla					x	x	x

3.5.7 UTM-1

UTM-1 tuoteperheeseen kuuluu paljon laitteita erilaisilla ohjelmistokokoonpanoilla ja suorituskyvyillä varustettuina. Kaikille laitteille yhteiset ohjelmat ovat palomuuri, IPSec VPN, Network Policy Management, Endpoint Policy Management ja Logging & Status. [7.] Taulukossa 7 on esitelty tuotteiden ominaisuuksia.

Taulukko 7. UTM-1-laitteiden ominaisuuksia

	UTM-1 132/134/138	UTM-1 272/274/278	UTM-1 574/578	UTM-1 1075/1078	UTM-1 2075/2078	UTM-1 3075/3078
10/100/1000Mb/s-portit	4	4	6	6	8	10
Palomuurin läpäisy (Gb/s)	1,5	1,5	2,5	3	3,5	4,5
VPN:än läpäisy (Mb/s)	120	120	300	350	450	1100
IPS:n läpäisy (Gb/s)	1	1	1,7	2,2	2,7	4
Rinnakkaisia sessioita	600 000	600 000	650 000	650 000	1 100 000	1 100 000
VLAN:ien määrä	1024					
Tallennuskapasiteetti (GB)	80	160				
Mitat (mm)	270 x 145 x 40	429 x 255 x 44	429 x 255 x 44	429 x 255 x 44	443 x 381 x 44	443 x 381 x 44

Massa (kg)	1,6	3,7	3,7	3,7	6,5	6,5
Maksimi tehonkulutus (W)	46,9	26,2	41,1	40,1	63,1	77,5
Käyttöolosuhteet	Lämpötila:5-40°C, Ilmankosteus:10-85%					

3.5.8 UTM-1 Edge

UTM-1 Edge-laitteet sisältävät palomuurin, IPSec VPN:än, Intrusion Prevention Systemin, URL Filteringin, Antivirus & Anti-Malwaren ja Anti-Spam & Email Securityn. Tämä tuoteryhmä sisältää uusimpia standardeja tukevan ADSL-modeemin, kytkimen ja osa myös USB-portteja ja WLAN-tukiaseman. UTM-1 Edge-laitteet käyttävät ADSL-tekniikkaa luodessaan yhteyden esimerkiksi sivukonttorista yritysverkkoon. Jos ADSL ei jostain syystä ole käytettävissä, voidaan yhteys muodostaa myös tavallisella puhelinyhteydellä. Lisäksi laitteet sisältävät QoS-ominaisuuden. [7.]

3.5.9 Safe@Office

Safe@Office-laitteet on tarkoitettu pienille yrityksille ja ne ovat melko yksinkertaisia verrattuna muihin Check Pointin laitteisiin. Laitteisiin kuuluu palomuuri, IPSec VPN, Intrusion Prevention System, URL Filtering, Antivirus & Anti-Malware ja Anti-Spam & Email Security. Integroituna ovat ADSL-modeemi, kytkin ja osassa malleista WLAN-tukiasema. Periaatteessa nämä laitteet muistuttavat kotikäytössä suosittuja ADSL-modeemin, reitittimen ja kytkimen yhdistäviä laitteita. Safe@Office sisältää kuitenkin enemmän ominaisuuksia ja takaa paremman tietoturvan. [7.]

3.5.10 Smart-1

Smart-1 on joukko laitteita, jotka sisältävät Check Pointin Security Management-ohjelmia. Laitteiden ja niiden ohjelmien hallintaan käytetään SmartDashboard-konsolia. Kaikkiin Smart-1-laitteisiin kuuluu vakiona Network Policy Management, Endpoint Policy Management, Logging & Status ja SmartProvisioning. Osaan laitteista on mahdollista asentaa vaikka kaikki Security Management-ohjelmat. Nämä laitteet on tarkoitettu keskisuurille ja suurille yrityksille. [7.] Taulukossa 8 on esitelty laitteiden ominaisuuksia.

Smart-1-laitteista on olemassa myös muunnella Smart-1 SmartEvent. SmartEvent-laitteet kuuluu SmartEvent, SmartReporter ja Logging & Status. Näihin laitteisiin ei ole mahdollista asentaa muita ohjelmia vaan sisältö on aina sama. Siinä mielessä siis SmartEvent on muista poikkeava kokonaisuus. Laitteita on kolmea erilaista, joista jokainen on suunnattu hieman erikokoiselle yritykselle. [7.] SmartEvent-laitteiden ominaisuuksia on esitelty taulukossa 9.

Taulukko 8. Smart-1-laitteiden ominaisuuksia

	Smart-1 5	Smart-1 25	Smart-1 50	Smart-1 150
GbE-portit	5	5	4	4
Tallennus-kapasiteetti (GB)	500	4x500 (RAID 10)	4x1000 (RAID 10)	4x1000 (RAID 10, mahdollisuus 12TB asti)
Mitat (mm)	431 x 277 x 44	431 x 551 x 44	580 x 442 x 88	632 x 442 x 131
Massa (kg)	6	13	23,5	29,5
Lokien käsittelykapasiteetti sekunnissa	7500	14000	30000	30000
Maksimi tehonkulutus (W)	70,5	135,8	503,3	399,6
Käyttöolosuhteet	Lämpötila:0-40°C, Ilmankosteus:5-95%			
LCD-näyttö	x		x	x

Taulukko 9. Smart-1 SmartEvent-laitteiden ominaisuuksia

	SmartEvent 5	SmartEvent 25	SmartEvent 50
GbE-portit	5	5	4
Tallennuskapasiteetti (GB)	500	4x500 (RAID 10)	4x1000 (RAID 10)
Lokiin kirjaamisen kapasiteetti (GB/d)	2	10	25
Mitat (mm)	431 x 277 x 44	431 x 551 x 44	580 x 442 x 88
Massa (kg)	6	13	23,5
Keskimääräinen tehonkulutus (W)	61,7	122	350,8
Käyttöolosuhteet	Lämpötila:0-40°C, Ilmankosteus:5-95%		
LCD-näyttö	x		x

4 Check Pointin palomuuri

4.1 Ominaisuudet

Tässä luvussa kerrotaan Check Pointin palomuurista, eikä palomuurista yleisesti. Check Pointin palomuuri on erittäin suosittu ja se onkin yksi yrityksen päätuotteista. Palomuuri on voittanut useita tietotekniikan alan palkintoja. Palomuuri käyttää tilatietoista liikenteensuodatusta (stateful inspection), jonka Check Point aikoinaan keksi. Nykyään käytännössä kaikki palomuurit käyttävät tätä tekniikkaa.

Tilatietoisessa liikenteensuodatuksessa palomuuri jäljittää jokaisen palomuurin läpi kulkevan yhteyden ja varmistaa että yhteydet ovat sallittuja. Palomuuri tutkii kulkevat paketit saadakseen niistä yksityiskohtaisempaa tietoa kuin vain lähde- ja kohdeosoitteen. Tilatietoinen palomuuri valvoo myös yhteyden tilaa ja kerää sen tiedot tilataulukkoon. Tilataulukon mukaan palomuuri päättää pakettien suodattamisesta. Esimerkiksi palomuuri osaa tunnistaa mikäli saapuva paketti ei ole odotettu tai jos paketti on vastaus sisäverkosta lähetetylle pyynnölle. [8.]

Check Pointin palomuuri mahdollistaa pääsyn kontrolloimisen asiakaskoneisiin, palvelimiin ja sovelluksiin. Palomuurin avulla verkon ylläpitäjällä on yksityiskohtainen näkymä käyttäjiin, käyttäjäryhmiin, sovelluksiin, laitteisiin ja yhteystyyppeihin. Näiden tietojen perusteella tehdään päätökset pääsyn kontrolloimisesta. Käyttäjien identiteetti saadaan tietoon tiedustelemalla käyttäjätietokannasta, captive portalin avulla tai asentamalla asiakaskoneelle kerran käytettävä agentti, joka hoitaa identiteetin selvittämisen. Identiteetin selvittämisen jälkeen käyttäjälle voidaan sallia pääsy niihin tietoihin, joihin hänelle on annettu oikeudet. [9.]

Palomuuri tukee Network Address Translationia (NAT), jonka avulla IP-osoitteet voidaan salata niin, että verkon ulkopuolelle osoitteet näkyvät erilaisina kuin verkon sisällä. Osoitteet voidaan salata myös niin, että ne näkyvät yrityksen verkon toisessa osassa salattuina. Verkon ulkopuoliset eivät siis voi nähdä oikeaa IP-osoitetta ja näin verkon turvallisuus parantuu. [9.]

Palomuuri on mahdollista asettaa siltaavaan tilaan niin, että tietystä liitännästä sisään tuleva liikenne voidaan aina ohjata ulos samasta liitännästä tai liitännöistä. Tämä ominaisuus ei vaikuta alkuperäiseen reititykseen. [9.] Lisää Check Pointin palomuurin ominaisuuksia on esitelty taulukossa 10.

Taulukko 10. Check Pointin palomuurin ominaisuuksia

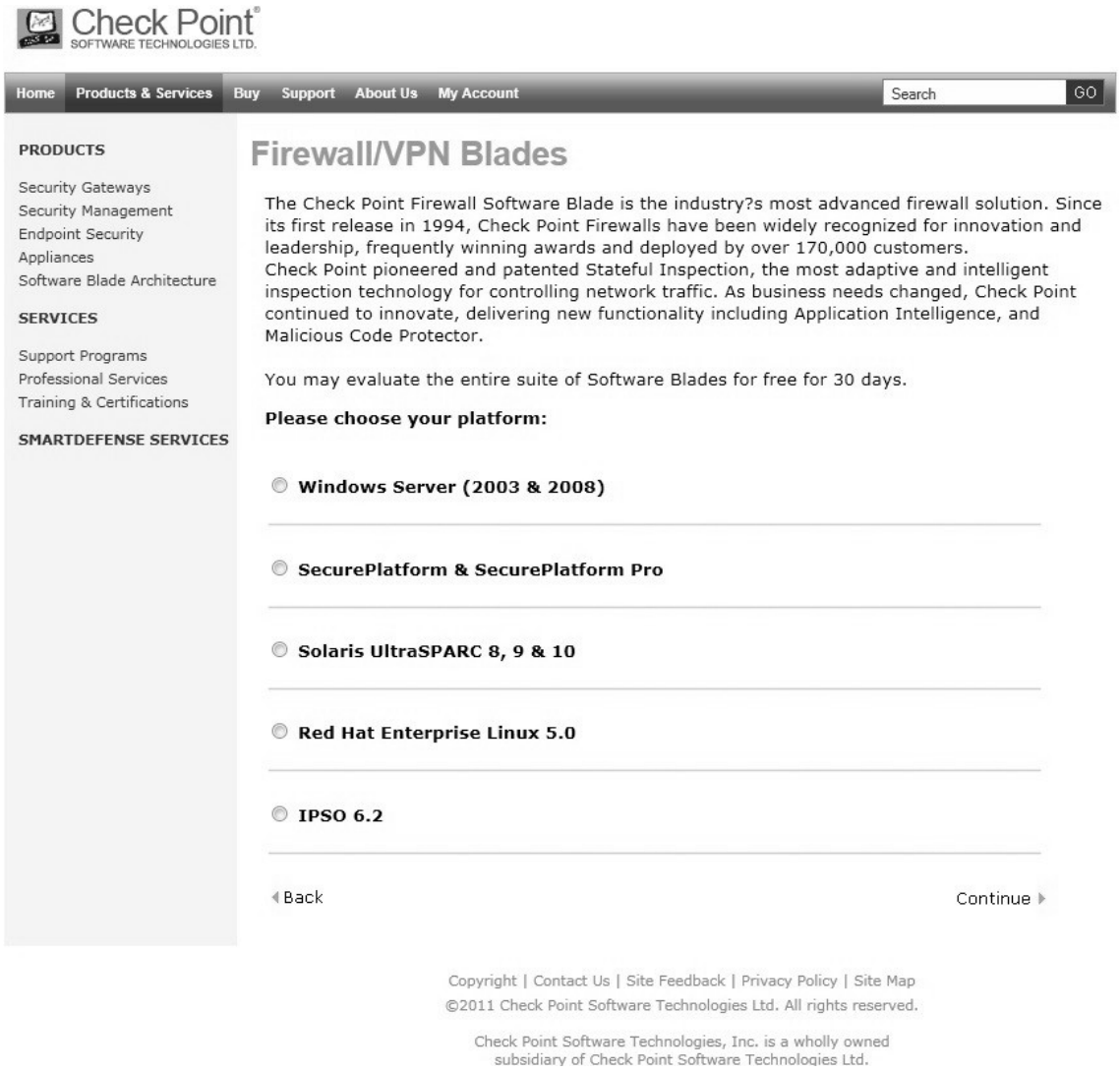
Ominaisuus	Tiedot
Protokolla-/sovellustuki	Yli 500 protokollatyyppiä
VoIP-suojaus	SIP, H.323, MGCP ja SIP NAT-tuella
NAT	Staattinen ja PAT manuaalisilla tai automaattisilla säännöillä
DHCP-yhdyskäytävät	Mahdollista antaa dynaamiset IP-osoitteet
VLAN	256 jokaista liitäntää kohti
Linkkien yhdistäminen (aggregation)	Passiivinen ja aktiivinen 802.3ad
IP-versiot	IPv4, IPv6
Secure Internet Communications (SIC)	Turvallinen kommunikaatiokanava kaikille Check Pointin komponenteille, jotka kuuluvat samaan hallinta-alueeseen

4.2 Palomuuriohjelman lataaminen

Latasin palomuurista 30 päivän ilmaisen kokeiluversion. Palomuuria ei kuitenkaan ollut mahdollista asentaa, joten asennukseen tai käyttöön liittyvistä asioista ei kerrota. Sen sijaan latausprosessi on kuvattu tässä luvussa.

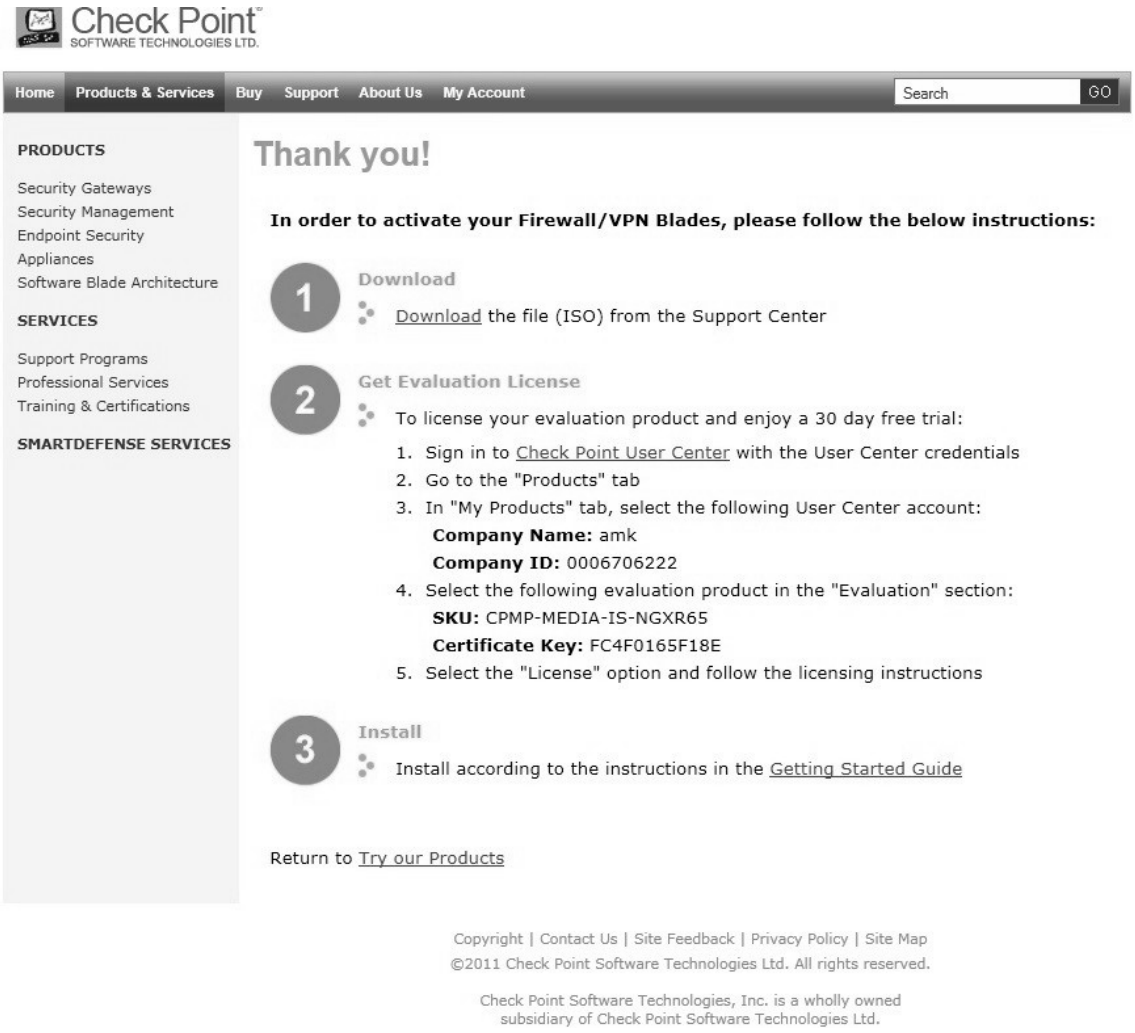
Palomuuri ladataan Check Pointin kotisivuilta osoitteesta www.checkpoint.com (kuva 1). Etusivulta valitaan try our products, josta valitaan firewall/VPN bladeskohdasta try now. Seuraavaksi valitaan käyttöjärjestelmä, jolla palomuuria on tarkoitus käyttää (kuva 2). Vaihtoehtoina on Windows server 2003 ja 2008, SecurePlatform ja SecurePlatform pro, Solaris UltraSPARC 8, 9 ja 10, Red Hat Enterprise Linux 5.0 sekä IPSO 6.2. Samalla myös ilmoitetaan, että tuotetta on oikeus käyttää 30 päivää ilmaiseksi. Alustan valinnan jälkeen painetaan continue, jolloin päästään tilanteeseen, jossa rekisteröityneillä asiakkailla on mahdollisuus kirjautua sisään ja uusilla asiakkailla mahdollisuus rekisteröityä. Rekisteröityminen on pakollista ohjelman lataamiseksi. Rekisteröityessä asiakkaalta vaaditaan joitakin tietoja itsestään. Näihin tietoihin kuuluu etu- ja sukunimi, sähköpostiosoite ja puhelinnumero. Tämän lisäksi asiakkaalta vaaditaan tietoja edustamastaan yrityksestä. (Check Point tarjoaa yrityksille suunnattuja ohjelmistoja) Yrityksestä sivusto pyytää nimeä, osoitetta, kaupunkia, maata, postinumeroa, kuinka monessa paikassa yritys toimii, millä alalla yritys toimii ja työntekijöiden määrää. Lisäksi kysytään haluaako asiakas, että Check Pointin edustaja ottaa yhteyttä. Kun tiedot on annettu, painetaan continue ja sivusto pyytää kirjautumaan sisään. Tunnukset kirjautumiseen lähetetään asiakkaan antamaan sähköpostiosoitteeseen. Tunnukset saapuvat hyvin nopeasti.

Kuva 1. Check Pointin etusivu



Kuva 2. Käyttöjärjestelmän valinta

Käyttäjätunnuksen ja salasanan antamisen jälkeen painetaan jälleen continue ja ruutuun tulee ohjeistusta palomuurin käyttöönotosta (kuva 3). Samat ohjeet tulevat myös sähköpostiin. Ohjeissa on kolme kohtaa.



Kuva 3. Ohjeet palomuurin käyttöönottoon

Ensimmäisessä kohdassa tarjotaan linkki sivulle, josta palomuurin saa ladattua. Ohjelma on iso-muodossa ja se sisältää muutakin kuin pelkästään palomuurin. Tiedoston voi latauksen jälkeen polttaa DVD-levylle. Saman linkin takaa löytyy myös mahdollisuus ladata Check Pointin-ohjelmistoon liittyviä PDF-dokumentteja.

Toisessa kohdassa on linkki, jossa ladatulle tuotteelle hankitaan lisenssi. Linkin takaa löytyvälle sivulle pitää kirjautua sisään samoilla tunnuksilla kuin aiemmin, ellei edellinen kirjautuminen ole edelleen voimassa. Kirjautumisen jälkeen valitaan sivun yläreunan valikosta välilehti Products. Tämän jälkeen avautuvasta pudotusvalikosta valitaan aiemmin luotu tili ja toisesta pudotusvalikosta löytyy tuote, joka halutaan lisensoida. Valikossa voisi olla useita tuotteita jos asiakas

olisi useampia tilannut. Oikean tuotteen kohdalta valitaan pudotusvalikosta license, jolloin sivusto kysyy seuraavia tietoja: lisenssin tyyppi (tästä sivusto antaa lisätietoa), sen tietokoneen IP-osoite, miltä ohjelmistoa tullaan käyttämään, käytetyn tietokoneen merkki sekä käyttöjärjestelmä, jolla ohjelmaa tullaan käyttämään. Kun tiedot on annettu, painetaan License ja tulee ruutuun ilmoitus, että sähköpostiin on lähetetty tarpeelliset tiedot ja ohjeet lisenssistä. Tästä kohdasta käyttäjä voi ladata lisenssitiedoston sekä tarkastella ohjeita tiedoston asentamiseen. Täsmälleen samat tiedot lähetetään myös sähköpostiin.

Kun kahdessa ensimmäisessä kohdassa neuvotut toimenpiteet on suoritettu, voidaan siirtyä kolmanteen kohtaan, jossa yksinkertaisesti kehotetaan asentamaan ohjelma annettujen ohjeiden mukaan. Mukana on toki myös linkki asennusohjeisiin.

5 Tulokset

Voidaan todeta, että Check Pointilla on laaja valikoima monenlaisia tietoturvatuotteita. Tuotteita tutkiessa jäi sellainen kuva, että Software blade-arkkitehtuuri on varsin joustava systeemi. Bladejen lisääminen ja poistaminen Check Pointin laitteisiin tai asiakkaan tietokoneisiin on varsin helppoa. Tosin harvemmin kai mitään halutaan poistaa ja näin heikentää tietoturvaa. Vaikea sanoa onko asia ihan niin yksinkertainen kuin annetaan ymmärtää. Asiakas voi hyvin pitkälti valita haluamansa tuotteet vapaasti. Check Pointin kauppaamissa laitteissa tuntuisi olevan hyvin huomioitu erilaisten yritysten tarpeet. Ominaisuuksiltaan ja ohjelmistoiltaan laitteet vaihtelevat paljon. Security Gateways on selvästi Check Pointin päätuotealue. Se sisältää joitakin yrityksen ydintuotteita. Tähän ryhmään kuuluu myös palomuuri, joka on Check Pointin ykköstuote. Kyseessä onkin ilmeisen hyvä tuote, sillä se on ilmeisesti suosituin palomuuri yritysten keskuudessa. Tuote on saanut paljon tunnustusta. Palomuuri ei tuntunut tarjoavan

sinänsä mitään uutta ja ihmeellistä, mutta se hoitaa tehtävänsä hyvin. Check Pointilla on pitkä kokemus palomuurinsa kehittämisestä.

Check Pointin järjestelmä Software Blade-arkkitehtuureineen on hieman hankala hahmottaa. Security Gateway bladet ja niiden hallintaohjelmat asennetaan monesti eri laitteisiin ja mahdollisesti eri käyttöjärjestelmille. Aloittelijan on vaikea ymmärtää kaikkea ilman asiantuntijan neuvoja. Toki Check Point myös tarjoaa asiantuntijapalveluita. Itse sain tätä työtä tehdessäni jonkinlaisen peruskäsityksen siitä miten järjestelmä toimii mutta paljon lisää pitäisi oppia ennen kuin ohjelmia osaisi käyttää.

Palomuurin kokeiluversion lataaminen ei ollut mikään aivan yksinkertainen prosessi, mutta ei siinä myöskään mitään ylitsepääsemätöntä ollut. Ohjeita seuraamalla pääsee pitkälle. Ohjelman latauksen osalta Check Pointin kotisivut voisivat olla hieman selkeämmät. Välillä oli hieman hankaluuksia löytää sitä mitä halusi. Tuotteet esitellään kyllä selkeästi. Sivuilla, joihin pääsee rekisteröimisen jälkeen, olisi toivomisen varaa. Myös se on hieman hämäävää kun lataa palomuuria, niin saa mukana paljon muutakin. Ladattu paketti oli kooltaan melko suuri ja se sisälsi ainakin SecurePlatform-käyttöjärjestelmän. Ilmeisesti mukana oli myös hallintaohjelmia.

6 Pohdinta

Idea tähän opinnäytetyöhön lähti tarpeesta tutkia Check Pointin palomuuria. Mukaan päätettiin ottaa myös muiden tuotteiden tutkiminen, pääpainon pysyessä palomuurissa. Tähän tavoitteeseen päästiin. Työssä on esitelty Check Pointin tuotteita kattavasti. Palomuurin osuus jäi hieman pienemmäksi kuin olin suunnitellut, mutta ei siinäkään mitään suurempia puutteita ole.

Työssä selvästi eniten aikaa vei osa, jossa kerrotaan muista tuotteista kuin palomuurista. Oli yllättävän työlästä lukea suuria määriä tekstiä englanniksi ja

miettiä sitten järkevää suomennosta. Joillekin termeille on hyvin hankala löytää järkeviä suomenkielisiä vastineita. En osannut aavistaa, että siihen kuluisi niin paljon aikaa. Työn muut osat ehkä hieman kärsivät siitä, että tuotteiden tutkiminen oli niin iso homma.

Opinnäytetyön suunnitelmassa mainittu Check Pointin tuotteiden vertailu Cisco Systemsin tuotteisiin toteutunut. Ciscon tuotteisiin tutustuminen olisi niin paljon aikaa, että katsoin parhaaksi luopua siitä. Valitettavasti ajan rajallisuus vaikutti työn lopputulokseen.

Työssä saatiin tutkittua Check Pointin tuotteita ja erityisesti palomuuria niin kuin oli tarkoitus. Sain myös jonkinlaisen näkemyksen Check Pointin järjestelmästä ja palomuurin käyttöönotosta.

Jatkossa Check Pointin palomuurin käyttöönottoa Pohjois-Karjalan ammattikorkeakouluun suunnitellessa, tämä työ voisi toimia pohjana jatkotutkimukselle. Asioita tarvitsee selvittää paljon ja voi tarjota vastauksia peruskysymyksiin. Näin syvällisempää tutkimusta olisi helpompi lähteä tekemään.

Lähteet

1. Kontaktia Media. 2011. Tietoturva. Suomen Intertopas. http://www.internetopas.com/yleistietoa/tietoturva. 24.5.2011.
2. 2011. Check Point. Wikipedia. http://en.wikipedia.org/wiki/Check_Point. 19.5.2011.
3. Check Point Software Technologies Ltd. 2010. Check Point Software Blade Architecture. Check Point Software Technologies Ltd. Http://www. checkpoint.com /products/softwareblades/architecture/index.html. 20.5.2011.
4. Check Point Software Technologies Ltd. 2010. Security Gateways. Check Point Software Technologies Ltd. http://www.checkpoint.com/ products/index.html#gateways. 16.5.2011.
5. Check Point Software Technologies Ltd. 2010. Endpoint Security. Check Point Software Technologies Ltd. http://www.checkpoint.com/ products/index.html#endpoint. 18.5.2011.
6. Check Point Software Technologies Ltd. 2010. Security Management. Check Point Software Technologies Ltd. http://www.checkpoint.com/ products/index.html#management. 19.5.2011.
7. Check Point Software Technologies Ltd. 2010. Security Appliances. Check Point Software Technologies Ltd. http://www.checkpoint.com/ products/appliances/index.html. 21.5.2011.
8. QuinStreet Inc. 2011. stateful inspection. QuinStreet Inc. http://www.webopedia.com/TERM/S/stateful_inspection.html. 26.5.2011.
9. Check Point Software Technologies Ltd. 2011. Check Point Firewall Software Blade. Check Point Software Technologies Ltd. Http://www. checkpoint.com/products/firewall-software-blade/index.html. 26.5.2011.