VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Petteri Rantala

MPLS-VERKON KUSTANNUSTEHOKAS KORVAAMINEN VIKASIETOISELLA MULTI-LINK VPN -RATKAISULLA

CASE STONESOFT

Liiketalous ja matkailu
2013

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Petteri Rantala
Opinnäytetyön nimi	MPLS-verkon kustannustehokas korvaaminen vikasietoisella Multi-Link VPN -ratkaisulla - Case Stonesoft
Vuosi	2013
Kieli	suomi
Sivumäärä	47 + 4 liitettä
Ohjaaja	Jarmo Laasanen

Tässä opinnäytetyössä tarkastelen kahta eri tapaa toteuttaa PK-yrityksen monipisteverkko, sekä niihin liittyviä ominaispiirteitä. Työn tarkoituksena on löytää vastaus kysymykseen, voisiko Stonesoftin Multi-Link VPN olla kustannustehokkaalla tavalla korvaava ratkaisu perinteiselle tietoliikenneoperaattorin MPLS-tekniikkaan pohjautuvalle VPN ratkaisulle.

Käsittelen näihin ratkaisuihin liittyvät keskeiset teknologiat pintapuolisesti ja pyrin keskittymään yritysten kannalta olennaisiin seikkoihin. Case-osiossa vertaan näitä tekniikoita kolmen eri muuttujan kautta. Nämä ovat vikasietoisuus, tietoturva ja kustannukset. Aineistona olen käyttänyt erään suomalaisen yrityksen tietoliikennekustannuksia ja kokemuksia, sekä Stonesoftin laitehinnaston mukaisia hintoja.

Lopuksi käsittelen tutkimuksen keskeisiä havaintoja sekä esittelen niiden pohjalta syntyneet johtopäätökset.

Avainsanat tietoliikenne, MPLS, Multi-Link VPN

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Petteri Rantala
Title	Cost-efficient Replacement of MPLS a Network with Multi-Link VPN –Technology. Case Stonesoft.
Year	2013
Language	Finnish
Pages	47 + 4 Appendices
Name of Supervisor	Jarmo Laasanen

In this thesis two different ways to implement a multipoint network for a small enterprise were examined. In addition, the related characteristics were studied. The aim was to answer the question of whether Stonesoft's Multi-Link VPN could offer a cost-effective solution to the traditional internet service providers' Multi-protocol Label Switching (MPLS) technology based a VPN solution. The related essential technologies, the main focus being on their business-critical issues, were also discussed.

In the case study these techniques were compared through three different variables; redundancy, security and cost-efficiency.

The used source material consists of the telecommunication costs and experiences of a certain Finnish company, as well as the current Stonesoft price list. Finally, the key findings of the study and the conclusions based on them were discussed.

Keywords telecommunication, MPLS, Multi-Link VPN

SISÄLLYS

KÄSITELUETTELO

ADSL	Asymmetric Digital Subscriber Line, asymmetrinen laajakaistatekniikka
AES	Advanced Encryption Standard, lohkosalausjärjestelmä, jota käytetään tietotekniikassa
AET	Advanced Evasion Techniques, kehittyneet evaasiotekniikat
CRM	Customer Relationship Management, asiakkuudenhallintajärjestelmä
ERP	Enterprise Resource Planning, toiminnanohjausjärjestelmä
IPS	Intrusion Prevention System, tunkeutumisen estojärjestelmät
IPsec	Internet Protocol Security, kokoelma protokollia, joita käytetään salattujen yhteyksien muodostamiseen
IP VPN	TDC Oy:n käyttämä termi MPLS-pohjaisesta verkkoratkaisusta
ISP	Internet Service Provider, tietoliikenneoperaattori
MPLS	Multiprotocol Label Switching, lippumerkintöihin perustuva pakettien kytkentätekniikka
QOS	Quality of Service, termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia
SMC	Stonesoft Management Center, Stonesoft-tuotteiden hallintaohjelmisto
SPOF	Single Point of failure, yksittäinen vikaantumispiste
SSL-VPN	Secure Sockets Layer - Virtual Private Network, tekniikka, jossa VPN-yhteys muodostetaan SSL-yhteyden yli työasemalta suljettuun verkkoon tai verkkojen välille

VDI	Virtual Desktop Infrastructure, virtuaalinen työpöytä
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
VOIP	Voice over Internet Protocol, protokolla, jolla voidaan siirtää ääntä IP-verkossa
VPN	Virtual Private Network, virtuaalinen erillisverkko
VRF	Virtual Routing and Forwarding, reititystekniikka
WLAN	Wireless Local Area Network, langaton lähiverkko

KUVIO- JA TAULUKKOLUETTELO

LIITELUETTELO

1 JOHDANTO

Viime vuosina tietoliikenneverkkojen merkitys yritysten liiketoiminnassa on kasvanut huomattavasti, sillä lähes kaikki yrityksen toimintaan liittyvät sovellukset vaativat tietoliikenneverkon toimiakseen. Ilmiö näyttää vahvistuvan vuosi vuodelta ja nykypäivänä yrityksen tietoliikenneverkkoa voidaan kriittisyytensä puolesta verrata esimerkiksi teolliseen tuotantolaitteeseen. Kehityksen tärkeimpiä moottoreita ovat olleet viime vuosien suurimmat IT-trendit kuten virtualisointi, pilvipalvelut sekä erilaiset yhdistetyn viestinnän ratkaisut. Merkittäväksi trendiksi voidaan katsoa myös IT-ratkaisuihin liittyvät kustannuspaineet ja kasvaneet tehokkuusvaatimukset.

Edellä mainitut tuottavuutta ja tehokkuutta lisäävät teknologiat ovat täysin riippuvaisia toimivasta tietoliikenneverkosta ja tästä johtuen monissa yrityksissä on jouduttu tilanteeseen, jossa verkkoratkaisut täytyy miettiä uudelleen. Mielenkiintoiseksi asian tekee näkökulman muuttuminen aiemmasta pakollisesta pahasta aidosti liiketoimintalähtöiseksi. Hyvin tyypillinen tilanne nykyään on, että verkko ei tarjoa ainoastaan yrityksen liiketoimintaa tukevia sovelluksia, kuten intranet ja matkalaskuohjelma, vaan se tarjoaa edellä mainittujen sovellusten lisäksi kaikki liiketoiminnan kannalta kriittiset sovellukset, kuten esimerkiksi puhelinsovellukset, taloushallinnon sovellukset ja tuotannonohjauksen sovellukset.

Nykyään voidaankin katsoa, että verkkoratkaisujen suunnittelu ja vaatimusten määrittely lähtee suoraan liiketoiminnan tarpeista eikä IT:n tarpeista. Verkkoratkaisua mietittäessä budjetointia ei enää ohjaakaan yrityksen IT-budjetti, vaan keskeinen tekijä on verkon merkitys yrityksen liiketoiminnalle. Hyvin usein IT-osasto esittelee vaihtoehdot, mutta liiketoiminnasta vastaavat ihmiset määrittelevät tarpeet ja tekevät lopulliset päätökset. Tämä on johtanut kahteen asiaan: vaatimusten kasvuun ja siitä johtuen myös jossain määrin kustannusten kasvuun.

Tässä työssä on tarkoitus etsiä korvaavaa ratkaisua tänä päivänä yleisesti käytössä oleville tietoliikenneoperaattoreiden toimittamille MPLS-teknologiaan pohjautuville VPN-ratkaisuille. Korvaavan ratkaisun tulisi palvella paremmin tämän päi-

vän yritysten liiketoimintaa ja sen asettamia vaatimuksia niin kustannustehokkuuden, vikasietoisuuden kuin tietoturvankin osalta.

Olen valinnut vaihtoehtoiseksi teknologiaksi suomalaisen Stonesoftin kehittämän Multi-Link VPN -ratkaisun. Teknologian tekee mielenkiintoiseksi sen ainutlaatuisuus ja skaalautuvuus erikokoisten yritysten tarpeisiin. Kyseessä ei ole kustannusten puolesta niin sanottu enterprise-tuote, joka on vain suuryritysten saatavilla, vaan se on hinnallisesti myös PK-yritysten ulottuvilla.

Tutkimuksessa tarkastelen edellä mainittuja MPLS- ja Multi-Link VPN-teknologioita kolmesta eri näkökulmasta. Valitut näkökulmat ovat käytännössä samat kuin liiketoiminnan yleisimmät vaatimukset tietoverkolle eli kustannustehokkuus, vikasietoisuus ja tietoturva.

Opinnäytetyöllä ei ole varsinaista toimeksiantajaorganisaatiota. Konkreettisten tulosten saamiseksi olen laatinut case-esimerkin, jossa tarkastelen Stonesoftin ratkaisun soveltuvuutta erään suomalaisen yrityksen tarpeisiin. Kustannustehokkuuden tarkasteluun käytän kyseisen yrityksen todellisia tietoliikennekustannuksia 36 kuukauden ajanjaksolta. Koska työssä käsitellään yrityksen tietoturvan kannalta arkaluontoisia asioita, en yrityksen edustajan toiveesta johtuen paljasta kyseessä olevaa yritystä, vaan käytän siitä nimitystä Firma.fi ja yrityksen edustajasta käytän nimitystä IT Manager.

Lopputuloksena on melko kattava vertailu näistä kahdesta edellä mainitusta teknologiasta. Vertailun pohjalta yritys voi pohtia Stonesoftin Multi-Link VPN -teknologian soveltuvuutta itselleen. Esimerkkilaskelma antaa myös mahdollisuuden miettiä, minkä suuruisia kustannussäästöjä olisi mahdollista vaihtoehtoisella ratkaisulla saavuttaa.

2 YRITYSVERKOT

Tässä kappaleessa kuvaan karkealla tasolla yleisimpiä suomalaisten yritysten käytössä olevia monipisteverkkoratkaisuja. Ratkaisut on jaettu kolmeen kategoriaan. Nämä ovat erilaiset tietoliikenneoperaattoreiden toteuttamat MPLS-teknologiaan pohjautuvat VPN-ratkaisut, laitevalmistajien perinteiset IPsec VPN -ratkaisut, sekä näiden yhdistelmät, joista käytän nimitystä hybridimalli. Operaattoreiden toimittamat MPLS-ratkaisut eroavat toisistaan jonkin verran ja yhtälailla myös eri valmistajien VPN-ratkaisut eroavat toisistaan. Tästä syystä esittelen varsinaiset teknologiat melko karkealla tasolla ja keskityn sen sijaan valittuihin näkökulmiin.

2.1 Nykytilanne

”Nykyisin hyvin monen yrityksen toiminta on erittäin riippuvaista tietoverkkojen toiminnasta, minkä tähden tietoverkkojen luotettavuuden on oltava korkealla tasolla. Internet-operaattoreiden asiakkaina olevat yritykset osaavat vaatia nykyisin hyvin korkeaa saatavuutta eli verkossa ei saa olla katkoksia juuri ollenkaan. Jos yrityksen runkoverkon toiminta keskeytyy, se vaikuttaa välittömästi verkon kaikkiin käyttäjiin ja kaikkiin verkon kautta saataviin palveluihin.”
(Kettunen 2009.)

Hyvä esimerkki voisi olla tilanne, jossa yrityksen tuotantoa ohjaavat palvelimet on keskitetty palveluntarjoajan konesaliin ja yhteydet konesalin ja tuotantolaitoksen välillä katkeavat. Pahimmassa tapauksessa koko tuotanto katkeaa ja siitä johtuvat taloudelliset menetykset voivat olla huomattavia. Puhumattakaan tilanteesta, jossa tietoverkon häiriöt saattavat johtaa pahimmillaan jopa ihmishenkien menetykseen.

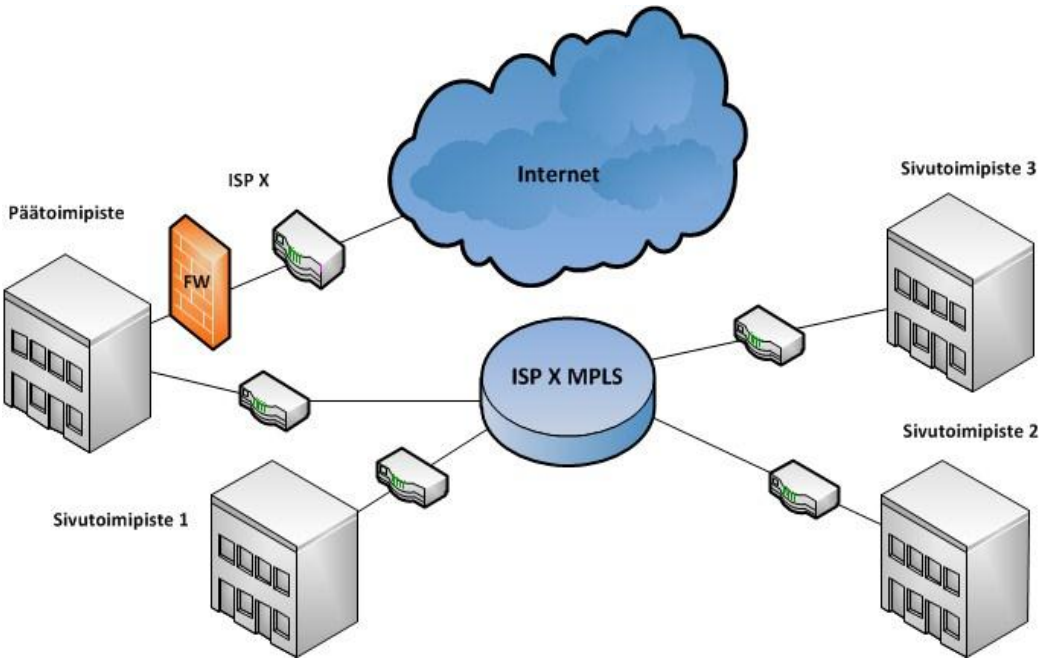
”Tästä syystä yritysten tietoverkoissa kaikki tärkeät laitteet, järjestelmät ja linkit kahdennetaan. Mahdollisessa vikatapauksessa syntyvän katkoksen on oltava myös kestoltaan mahdollisimman lyhyt, enintään muutaman sekunnin mittainen.”
(Kettunen 2009.)

2.2 MPLS-teknologiaan pohjautuvat verkot

MPLS on protokolla, joka yhdistää kytkentäisten verkkojen suorituskyvyn ja reititettyjen IP-verkkojen skaalautuvuuden. (Darukhanawalla & Bellagamba 2009, 19)

MPLS-teknologiaan pohjautuvat verkot ovat tyypillisesti tietoliikenneoperaattoreiden toimittamia. Tekniikan tarkoituksena on yhdistää yrityksen eri toimipistei-

den verkot loogiseksi kokonaisuudeksi. Tällä tavoin toteutetusta verkosta käytetään nimitystä VPN-verkko eli virtuaalinen yksityisverkko. Verkko toimii tietoliikenneoperaattorin runkoverkon sisällä omana yksityisenä verkkonaan. Tietoliikenneoperaattorin aktiivilaitteet huolehtivat siitä, että oikeat paketit löytävät tiensä oikeaan verkkoon ja toisaalta myös huolehtivat siitä, että paketit eivät pääse väärään verkkoon. Tietoliikenneoperaattorit käyttävät verkkoratkaisustaan useita eri nimiä, kuten yritysverkko (DNA), IP VPN (TDC) ja Yritysinternet (Elisa) jne. Yhteistä näille kaikille on standardoitu teknologia, jonka päälle ne on rakennettu.



Kuvio 1. MPLS-verkko.

MPLS-verkko toteutetaan tyypillisesti niin sanotulla ”Full-Mesh” –reititysperiaatteella, jolloin kukin toimipiste voi liikennöidä vapaasti keskenään lyhimmän reitin kautta. Kuviossa 1 esimerkiksi sivutoimipiste 3:n liikenne ei kierrä päätoimipisteen kautta määränpään ollessa sivutoimipiste 2, vaan se valitsee aina lyhyimmän reitin. Ainoastaan internetliikenne kulkee aina päätoimipisteen palomuurin läpi. Verkossa kulkevaa dataa ei oletuksena salata, mutta se on kuitenkin täysin näkymätöntä muille verkon käyttäjille. Reititystaulut ovat myös asiakaskohtaisia, joten niiden tiedot eivät myöskään näy muille verkon käyttäjille.

Verkkoratkaisu on mahdollista toteuttaa yhdellä tai useammalla virtuaaliverkolla, jotka erotellaan toimipisteissä VLAN:n avulla. Useita virtuaaliverkkoja käytettäessä on syytä huomioida niiden vaikutus verkkoratkaisun hintaan, sekä niiden asettamat vaatimukset muille verkon aktiivilaitteille. Virtuaaliverkot tulee määritellä myös sivutoimipisteiden aktiivilaitteille. Tyypillinen käyttökohde erillisille virtuaaliverkoille on esimerkiksi yrityksen VOIP-liikenteelle varattu oma virtuaaliverkko ja sille taattu tietoliikennekaista. Tällä tavoin voidaan varmistua, että puhelut verkossa toimivat, vaikka verkossa olisikin paljon muuta liikennettä.

Tietoliikenneverkko koostuu seuraavista komponenteista: tietoliikenneoperaattorin runkoverkko, asiakkaan keskitetty internetyhteys, toimipistekohtaiset päätelaitteet sekä asiakasliittymät. Edellä mainittujen lisäksi tietoliikenneoperaattorit tarjoavat lukemattoman määrän erilaisia lisäpalveluja ratkaisuihinsa, kuten esimerkiksi liikenteenpriorisointi (QoS) ja erilaiset verkon toimintaan liittyvät valvontapalvelut. Tyypillisesti tietoliikenneoperaattori vastaa VPN-verkon toimivuudesta kokonaisuudessaan. Toimipistekohtaiset päätelaitteet ovat pääsääntöisesti tietoliikenneoperaattorin omaisuutta ja se myös vastaa niiden toiminnasta. Loppuasiakkaalla ei ole yleensä pääsyä laitteiden hallintakonsoliin. Internetyhteys sen sijaan on mahdollista hankkia myös toisen tietoliikenneoperaattorin kautta. Palomuuripalvelut voidaan toteuttaa joko omilla laitteilla tai tietoliikenneoperaattorin tarjoamana palveluna. (TDC Nordic IP VPN - palvelukuvaus ja erityisehdot 2011.)

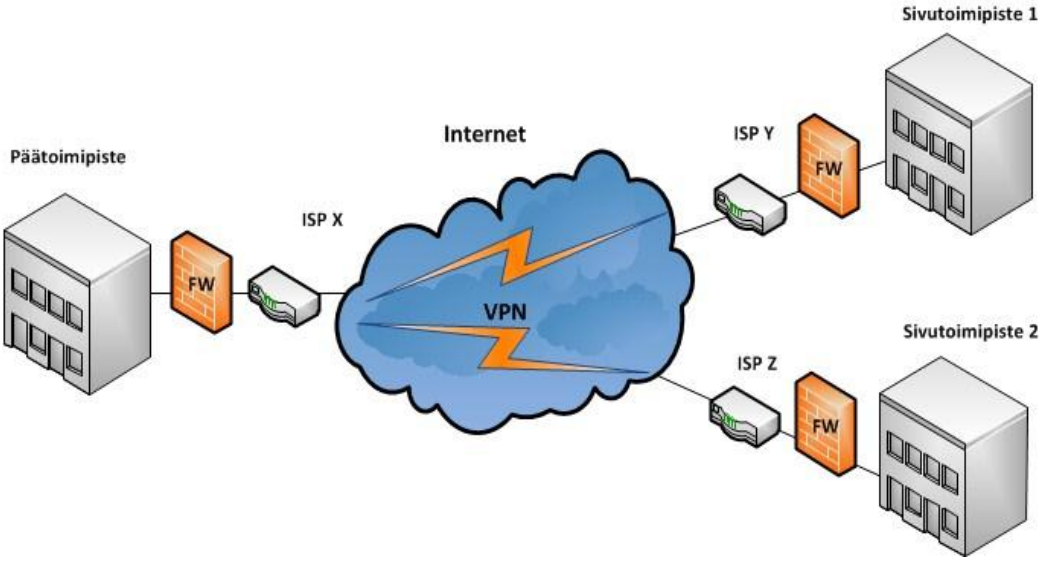
2.3 IPsec VPN -verkot

VPN-tunnelit ovat jo vuosia tarjonneet yrityksille kustannustehokkaan tavan yhdistää eri toimipisteitä tietoturvallisella tavalla. Tällä tavoin on saavutettu ainakin hetkellisiä kustannussäästöjä verrattuna operaattoreiden toimittamiin MPLS-teknologiaan pohjautuviin yritysverkkoratkaisuihin. Ongelmana on kuitenkin ollut ratkaisujen toimintavarmuus. Tästä johtuen ne onkin katsottu monessa yrityksessä riskitekijöiksi. (Stonesoft Whitepaper ISP Redundancy 2006.)

Perinteisiin IPsec VPN -ratkaisuihin liittyvät riskit ja haasteet ovat johtuneet useista eri tekijöistä, kuten eri laitevalmistajien yhteensopivuusongelmista, tunneleiden kahdentamisen vaikeudesta ja ratkaisujen hankalasta hallittavuudesta. Han-

kalasti hallittava ympäristö syntyy helposti, kun sekoitetaan eri sukupolvien laitteita tai eri valmistajien laitteita keskenään. Pahimmillaan jokaista laitetta hallitaan eri hallintatyökalulla, jolloin myös verkkoa ylläpitävältä henkilöstöltä vaaditaan osaamista niistä kaikista. Hankaluuksia aiheuttavat myös useat eri ohjelmistoversiot ja niihin liittyvät päivitykset ja tukisopimukset.

Edellä mainituista haasteista huolimatta PK-yrityksissä suosittu tapa toteuttaa usean toimipisteen verkkoratkaisu on kuitenkin ollut palomuurilaitteiden avulla muodostetut VPN-tunnelit, joilla eri toimipisteet on yhdistetty toisiinsa. Palomuurien tehtävänä on huolehtia internetliikenteestä, tietoturvasta, sekä reitittää VPN-tunneliin tai VPN-tunneleihin menevät paketit kulloinkin oikeaan verkkoon. Haasteita aiheuttaa tyypillisesti reititys sekä monimutkainen säännöstö. Useimmiten nämä molemmat seikat johtuvat ainakin osittain siitä, että jokaisen toimipisteen internetliikenne reititetään suoraan internetiin. Perusteluna tälle on kaistantarpeen pieneneminen päätoimipisteessä. Nykyisten tietoliikenneyhteyksien kapasiteetti on sen verran suuri ja hinnat alhaiset, joten mielestäni tälle perustelulle ei ole enää pohjaa. Vaihtoehtoisesti verkossa voisi olla yksi piste, josta liikennöitäisiin keskitetysti ulos, kuten MPLS-ratkaisussa. Käytettäessä useita eri reittejä julkiseen verkkoon tarvitaan useita erilaisia paikkakuntakohtaisia palomuurisäännöstöjä sekä reitityksiä. Nämä lisäävät verkon kompleksisuutta merkittävästi tuomatta kuitenkaan mitään erityistä lisäarvoa verkon toiminnallisuuden tai tietoturvan kannalta. Yritysten ja niiden yhteistyökumppaneiden tai asiakkaiden välisiä VPN-tunneleita on hyvin usein myös terminoitu paikkakuntakohtaisesti ja ne on määritelty erilaisilla tunnelikohtaisilla säännöstöillä. Tietoturvan näkökulmasta on ongelmallista, jos yrityksen verkkoon on pääsy monia eri reittejä pitkin. Useimmiten tämänkaltaisissa tietoliikenneverkoissa myös tunneleiden käyttöön liittyvä lokitieto on hajallaan eri puolilla verkkoa.

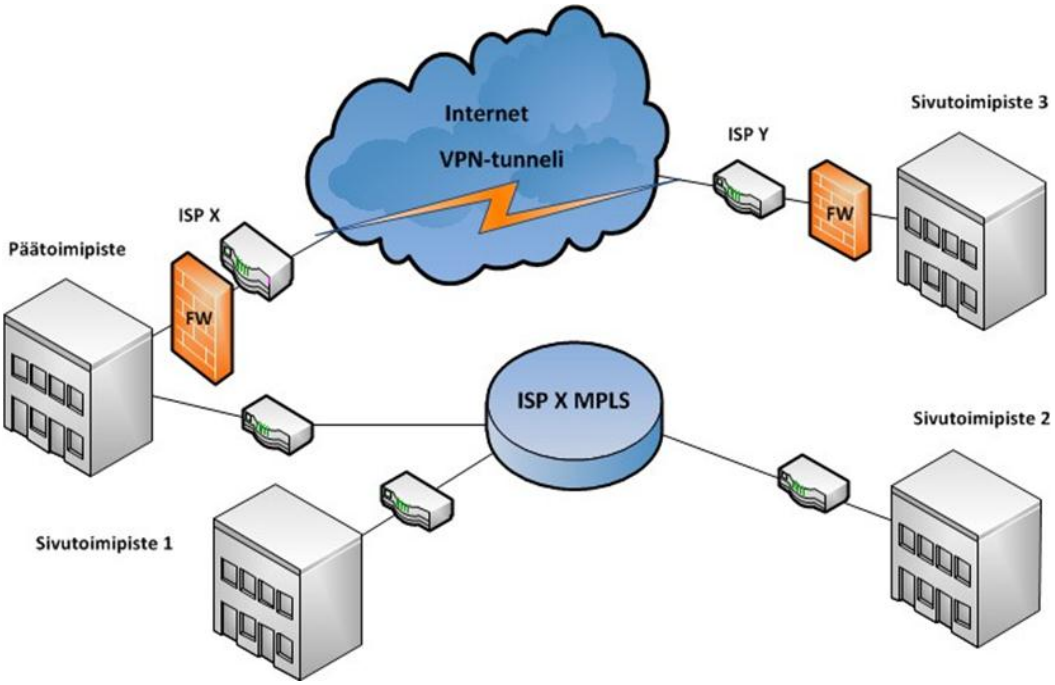


Kuvio 2. Perinteinen IPsec VPN -verkko.

Tällä tavoin toimittaessa pienikin yritys saa muutamassa vuodessa aikaiseksi erittäin monimutkaisen tietoliikenneverkon. Monimutkaisuus aiheuttaa suoria kustannuksia lisääntyneinä ylläpitokustannuksina ja välillisiä kustannuksia syntyy, kun verkkoratkaisu ei tue yrityksen varsinaista liiketoimintaa parhaalla mahdollisella tavalla. Liiketoiminnan kannalta voi olla erittäin tärkeää pystyä reagoimaan nopeasti erilaisiin muutospyyntöihin. Nämä voivat liittyä esimerkiksi yrityskaupasta johtuvaan migraatioon, sähköiseen laskutukseen tai erilaisiin alihankintaketjun yhteyksiin. Monimutkainen ja vaikeasti hallittava kokonaisuus aiheuttaa sen, että nopea reagointi on mahdotonta. Jopa pienienkin muutosten tekeminen verkkoon vaatii huolellista testausta ja runsaasti aikaa. Erittäin merkittävänä uhkatekijänä voidaan pitää myös mahdollisten tietoturvapuutteiden vaikutusta yrityksen imagoon ja kilpailukykykyyn. Tietoturvapuutteista johtuva tunkeutuminen yrityksen järjestelmiin saattaa pahimmillaan ajaa yrityksen vararikkoon, mikäli asiakkaat menettävät luottamuksensa yritykseen.

2.4 Hybridimallin mukaiset verkot

Ehkä yleisin tapa toteuttaa yritysverkko on yhdistelmä edellä mainituista MPLS- ja IPsec VPN -teknologioista (ks. kuvio 3).



Kuvio 3. Hybridimallin mukainen verkko.

Hyvin usein yritykset aloittavat verkkoprojektit kartoituksilla, tarvemäärittelyillä ja erilaisten teknologioiden vertailulla. Yritysten apuna näissä projekteissa on yleensä jälleenmyyjiä, päämiehiä ja ulkopuolisia konsultteja. Tältä pohjalta yritys valitsee teknologian ja aloittaa sen implementoinnin. Monessa tapauksessa käy kuitenkin niin, että varsinaisen projektin jälkeen ilmenee uusia tarpeita, henkilöitä vaihtuu tai teknologia kehittyy ja päädytään alkuperäisestä päätöksestä poiketen valitsemaan esimerkiksi IPsec VPN -ratkaisu osaksi MPLS-ratkaisua. Syynä tähän saattaa olla esimerkiksi kustannuspaineet tai MPLS-liittymän pitkä toimitusaika, joka saattaa olla jopa kahdeksan viikkoa. Toimitusajan pituuteen vaikuttaa ensisijaisesti liittymän maantieteellinen sijainti. Mikäli liittymä asennetaan alueelle, josta löytyy tietoliikenneoperaattorin omaa verkkoa, on asennus nopeampi kuin vaihtoehdossa, jossa liittymä asennetaan toisen tietoliikenneoperaattorin verkkoon Suomessa tai ulkomailla.

Tyypillinen esimerkki on yritys, joka toteuttaa Suomen sisäisen verkon MPLS-teknologialla ja avatessaan ensimmäistä ulkomaan toimipistettä, huomaa tietoliikenneyhteyden hinnan olevan moninkertainen aiempiin yhteyksiin verrattuna. Tässä kohtaa päätöksentekijä arvioi usein asiaa vain yhden toimipisteen kustan-

nusten kautta ja päätyy hankintahinnaltaan halvempaan ratkaisuun eli perinteiseen IPsec VPN -ratkaisuun. Lopputuloksena on hybridimallin mukainen verkko, jossa on käytössä sekä MPLS-teknologiaa että perinteistä IPsec VPN -teknologiaa.

Tämän kaltaisen verkon keskitetty hallinta ei käytännössä ole mahdollista, koska osa laitteista on tietoliikenneoperaattorin hallinnassa ja osa yrityksen omassa hallinnassa. Verkon aktiivilaitteet ovat useimmiten myös eri valmistajien tuotteita, jolloin hallintakonsoleita tarvitaan useita. Sama ongelma koskettaa myös lokitietojen keskitettyä keräämistä. Markkinoilla on kolmansien osapuolien tuotteita, joilla voidaan hallita eri valmistajien laitteita sekä kerätä niistä lokitiedot. Nämä ohjelmistot ovat useimmiten melko kalliita ja hyvin harvoin ne toimivat yhtä hyvin kuin alkuperäiset.

Hybridimallin mukaan toteutetussa verkossa on omat hyvät ja huonot puolensa. Hyvänä puolena mainitaan usein kustannustehokkuus ja huonona puolena hallinnan hankaluus. Näennäinen kustannustehokkuus syntyy, kun kallis MPLS-yhteys esimerkiksi Aasiaan korvataan perinteisellä IPsec VPN -yhteydellä. Vaihtoehtojen hankintahintoja vertailemalla säästö on ilmeinen, mutta kokonaiskustannuksia tarkastellessa tilanne ei välttämättä olekaan enää sama. Kokonaiskustannusten kasvu syntyy verkon topologian monimutkaistumisesta ja sitä kautta ylläpidon kulujen kasvamisesta. Tällä tavoin toteutetussa usean toimipisteen verkossa saattaa olla moninkertaiset kulut verrattuna tietoliikenneoperaattorin toimittamaan MPLS-verkkoon. Kuluja syntyy, kun jokainen pieni muutos verkkoon joudutaan tekemään moneen kertaan johtuen verkon arkkitehtuurista, erimerkkisistä laitteista sekä useista yhteistyökumppaneista.

3 STONESOFT OYJ

Stonesoft Oyj on suomalainen puhtaasti tietoturvaan keskittynyt maailmanlaajuisesti toimiva yhtiö. Yrityksen pääkonttori on Helsingissä ja sen lisäksi yrityksellä on useita myyntikonttoreita eri puolilla maailmaa. Yritys on perustettu vuonna 1990 ja tänä päivänä se työllistää noin 200 henkilöä eri puolilla maailmaa. Vuonna 2011 yrityksen liikevaihto oli noin 30 miljoonaa euroa, mutta tulos oli tappiollinen. Stonesoft Oyj:n osakkeet noteerataan NASDAQ OMX Helsingin päälistalla. Yrityksen toimitusjohtajana toimii Ilkka Hiidenheimo. (Stonesoft vuosikertomus 2011.)

3.1 Historia

Stonesoftin liiketoiminta oli alkujaan tietoturvaratkaisujen jälleenmyyntiä ja se olikin 90-luvun alkupuolella yksi Euroopan suurimpia Checkpoint-jälleenmyyjiä. Hyvin pian yhtiö aloitti kuitenkin oman teknologian kehittämisen. Sen seurauksena julkaistiin StoneBeat-tuoteperhe vuonna 1996. StoneBeat oli markkinoiden ensimmäisiä korkean käytettävyyden tietoturvaratkaisuja. Kyseessä oli niin sanottu aktiivi/passiivi -klusteri. Vuonna 1999 julkaistiin StoneBeat FullCluster, joka piti sisällään patentoidun klusterointi- ja kuormantasausteknologian. Ensimmäinen varsinainen palomuurituote eli StoneGate julkaistiin vuonna 2001. (Siuro 2008, 7.)

Taloudellisesta näkökulmasta katsottuna yrityksen historia listautumisen jälkeen on ollut erittäin vaiherikas. Yritys listautui Helsingin pörssiin vuonna 1999 niin sanotun IT-kuplan ollessa suurimmillaan. Tällöin Stonesoftin liikevaihto oli n. 27 miljoonaa euroa ja yrityksen markkina-arvo moninkertainen. Yrityksen markkina-arvo oli korkeimmillaan vuonna 2000, jolloin se kävi 880 miljoonassa eurossa. Kuplan puhjettua kurssi kääntyi jyrkkään laskuun ja vuoden lopussa 2012 yrityksen markkina-arvo oli vain noin 88 miljoonaa euroa.

3.2 Tuoteportfolio

Tässä kappaleessa esittelen tämän työn kannalta keskeisimmät tuotteet Stonesoftin tuoteportfoliosta. Tuotteet ovat StoneGate Management Center (SMC), StoneGate-palomuurit ja Stonesoft IPS. Nämä kolme tuoteperhettä liittyvät olennaisesti työssä käytettyihin näkökulmiin: kustannustehokkuus, vikasietoisuus ja tietoturva. Case-osiossa esiteltävä ratkaisu muodostuu näiden kolmen edellä mainitun tuoteperheen jäsenistä.

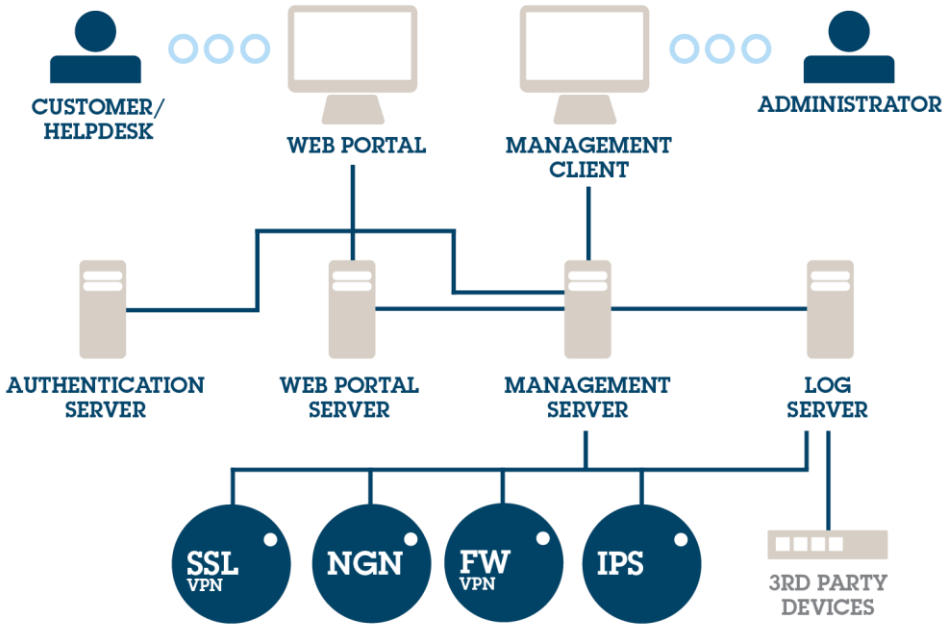
Stonesoft kertoo tuotteistaan päivitetyssä strategiassaan vuosille 2013–2014 seuraavasti:

”Stonesoftin tuotteet suojaavat tietoverkkoja ulkoisia uhkia vastaan, mahdollistavat suurtenkin verkkotietoturvajärjestelmien tehokkaan keskitetyn hallinnan, muodostavat turvattuja ja luotettavia tietoyhteyksiä toimipaikkojen ja yhteistyökumppaneiden välille, sekä parantavat tietoverkon vikasietoisuutta.

Stonesoftin kilpailuetuja vaativassa asiakassegmentissä ovat tutkimukseen perustuvat edistyneiden verkkohyökkäysten (advanced evasion techniques) torjuntaratkaisut, tehokas keskitetty hallintajärjestelmä sekä korkean käytettävyyden ratkaisut. Stonesoftin vahvuuksia on myös edistynyt tekninen toteutus, mikä mahdollistaa nopean dynaamisen reagoinnin uhkakuvien muuttuessa.” (Stonesoft Oyj Pörssitiedote 12.11.2012.)

3.2.1 StoneGate Management Center

StoneGate Management Center -hallintaohjelmiston (SMC) avulla voidaan hallita keskitetysti muun muassa StoneGate-palomuuria, IPS- sekä SSL VPN -ratkaisua.



Kuvio 4. SMC-arkkitehtuuri (SMC Architecture 2013.)

Arkkitehtuuri koostuu hallintapalvelimesta, lokipalvelimesta ja hallintaohjelmistosta (ks. kuvio 4). Järjestelmää voidaan laajentaa erillisillä autentikointi- ja portaalipalvelimilla. Kaikki kuviossa 4 olevat palvelimet voivat olla joko fyysisiä tai virtuaalisia.

SMC on suunniteltu isojen ja maantieteellisesti hajallaan olevien ympäristöjen hallintaan. Tästä syystä siinä onkin huomioitu korkean käytettävyyden asettamat vaatimukset eli hallintapalvelin ja lokipalvelin voidaan kahdentaa sekä hajauttaa myös maantieteellisesti. Palvelimien kahdentaminen mahdollistaa järjestelmän täydellisen hallinnan myös mahdollisessa vikatilanteessa, sekä hallinta- ja lokipalvelimien huoltotyöt ilman katkoksia.

Kuvio 5. Stonesoft Management Center hallintaliittymä (Stonesoft Management Center 2012.)

Koko verkon kattava keskitetty hallinta tuo useita merkittäviä etuja niin hallinnan kuin tietoturvankin kannalta. Näitä ovat muun muassa yhteiset monitorointi-, loki- ja raportointipalvelut sekä käyttäjää helpottava yksi graafinen käyttöliittymä, jolla hoidetaan kaikkien laitteiden hallinta (ks. kuvio 5). Esimerkiksi useilla paikkakunnilla toimivan yrityksen verkossa leviävä virusepidemia on helppo pysäyttää, kun vain tiedetään sen leviämistapa. Tällöin voidaan keskitetysti estää tämä tietty verkkoliikenne koko yrityksen verkosta ja sen jälkeen monitoroida estämisen onnistuminen. Tämän jälkeen voidaan aloittaa saastuneiden koneiden puhdistaminen.

SMC:n piiriin on mahdollista kytkeä myös muiden valmistajien tuotteita. Näin mahdollistetaan esimerkiksi kytkimien tai reitittimien lokitietojen keräys SMC:n lokitietokantaan. Tällä tavoin toimittaessa saadaan yhdestä järjestelmästä erittäin hyvä yleiskuva koko verkon tapahtumista. (Stonesoft Management Center datasheet 2012.)

3.2.2 StoneGate Firewall /VPN

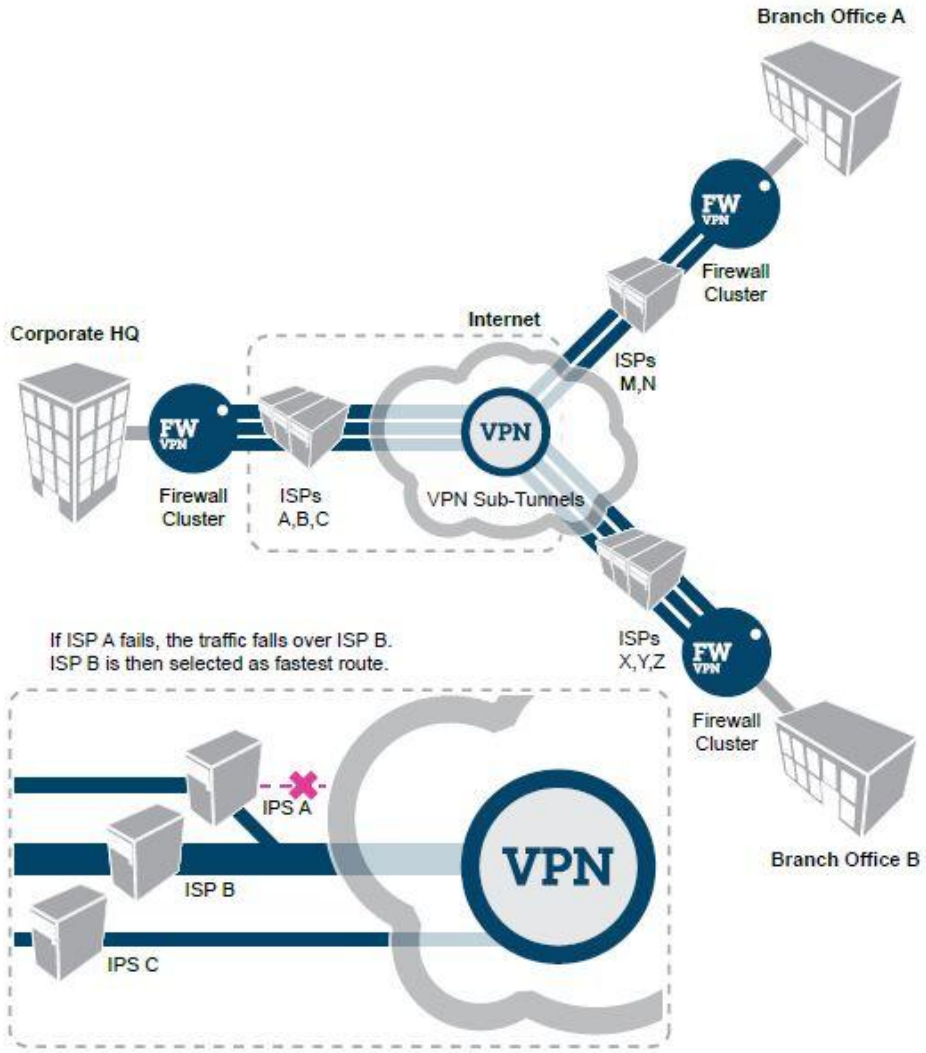
Stonegate-palomuuriratkaisun juuret ovat vuodessa 2001, jolloin Stonesoft julkaisi ensimmäisen version palomuuri- ja VPN-ohjelmistostaan. Viimeisen kymmenen vuoden aikana tietoturvauhat ja niihin liittyvät ratkaisut ovat kehittyneet merkittävästi. Tästä syystä ensimmäisen sukupolven palomuurien ei katsota enää tarjoavan riittävää suojaa verkon uhkia vastaan.

StoneGate on niin sanottu toisen sukupolven palomuuriratkaisu. Ratkaisu koostuu seuraavista osa-alueista: palomuuri, VPN, IPS (tunkeutumisen havainnointi- ja estojärjestelmä) sekä turvallisen etäkäytön mahdollistava SSL VPN. StoneGate-ratkaisun tehtävänä on yhdistää verkkotietoturva, korkea käytettävyys sekä kuormantasausteknologia yhtenäiseksi, keskitetysti hallittavaksi järjestelmäksi.

”Stonesoft on löytänyt merkittävän verkon tietoturvaa koskevan uhkakategorian, kehittyneet evaasiotekniikat (Advanced Evasion Techniques, AET). Kehittyneet evaasiotekniikat pystyvät kuljettamaan jo tunnetun hyökkäyksen kohteeseen nykyisten tietoturvalaitteiden huomaamatta. Voidakseen suojella kriittistä tietopääomaansa organisaatiot tarvitsevat dynaamisen, ohjelmistopohjaisen tietoturvajärjestelmän. Kehittyneiden evaasiotekniikoiden tuoma uhka kehittyy jatkuvasti, joten verkon suojauksen tulee olla keskitetysti päivitettävissä, kuten StoneGate verkon tietoturvaratkaisu.” (Stonesoft Oyj Vuosikertomus 2010.)

3.2.3 Stonesoft Multi-Link VPN

Stonesoft Multi-Link -teknologia tarjoaa yksinkertaisen tavan toteuttaa vikasietoiset internetyhteydet. Multi-Link-teknologiaa käytettäessä yrityksen ei tarvitse hankkia kalliita kolmannen osapuolen laitteisto- ja ohjelmistoratkaisuja yhteyksien kahdentamiseen, vaan toiminnallisuus on integroituna jokaiseen StoneGate-palomuuriin.



Kuvio 6. Stonesoft Multi-link VPN (ISP Redundancy 2006.)

Multi-Link-teknologia mahdollistaa useiden eri tietoliikenneoperaattoreiden ja yhteystyyppien samanaikaisen käytön. Kuvion kuusi esimerkissä yrityksen verkko on muodostettu kahdeksan eri tietoliikenneoperaattorin yhteydellä. Mikäli yksi linkki katkeaa, siirtyy kaikki liikenne automaattisesti kulkemaan jäljellä olevien linkkien kautta. Teknologia tukee kaikkia IP-pohjaisia tietoliikenneyhteystyyppejä, kuten ADSL, 4G tai vaikka sateliittiyhteyksiä. Tällä tavoin saadaan yksinkertaisesti ja kustannustehokkaasti varmistettua tietoliikenneverkon häiriötön toiminta ja poistettua verkosta niin sanottuja SPOF-pisteitä.

Vikasietoisuuden lisäksi Multi-Link-teknologia mahdollistaa myös kuormantasauksen eri tietoliikenneyhteyksien välillä. Tietoliikenneyhteyksien tehokkuus kasvaa, kun laite valitsee aina nopeimman tai parhaiten soveltuvan käytössä olevan yhteyden. Verkon maksimikapasiteetti on käytössä olevien tietoliikenneyhteyksien summa.

Kriittisissä ympäristöissä voidaan verkon toimintavarmuutta nostaa vielä yhdistämällä Multi-Link-teknologia ja klusteroidut StoneGate-laitteet. Tämä mahdollistaa kuormantasauksen myös palomuurinoodien välillä. Yhden noodin vikaantuessa sen hoitama liikenne siirtyy automaattisesti toiselle noodille. Toimenpide on täysin läpinäkyvä loppukäyttäjille eli kaikki palvelut pysyvät toiminnassa, vaikka verkossa onkin yksittäisen laitteen vikaantumisesta johtuva vikatilanne. StoneGate-laitteita voidaan klusteroida jopa 16 kappaletta.

Multi-Link-teknologia tarjoaa myös kustannussäästöjä mahdollistamalla kalliiden MPLS-ratkaisujen korvaamisen kustannustehokkaammalla vaihtoehdolla. Migraatio teknologiasta toiseen on tehty helpoksi eli vanhoja ja uusia yhteyksiä voidaan käyttää rinnakkain. Tämä mahdollistaa erittäin joustavan aikataulun ja palvelut voidaan migroida uuteen ratkaisuun jopa yksitellen, mikäli niin halutaan.

Multi-Link-teknologiaa voidaan internetyhteyksien kahdentamisen lisäksi hyödyntää vastaavalla tavalla rakennettaessa yritykselle monipisteverkkoa IPsec VPN -tunneleiden avulla. VPN-tunnelit voidaan rakentaa vikasietoisesti, kun kahden toimipisteen välillä on useampia aktiivisia tunneleita, jotka käyttävät eri tietoliikenneyhteyksiä. Esimerkiksi yritys voisi yhdistää kaksi toimipistettä ADSL-liittymän ja 4G-liittymän päälle rakennetuilla VPN-tunneleilla. Tällöin toimipisteiden välillä olisi neljä aktiivista VPN-tunnelia, joissa liikenne kulkisi ennalta määritettyjen kuormantasaussääntöjen mukaan. Mikäli toisen toimipisteen ADSL-liittymä vikaantuisi, niin kaikki liikenne siirtyisi automaattisesti ja täysin läpinäkyvästi 4G-yhteyden päällä toimivien VPN-tunneleiden varaan. ADSL-yhteyden korjaantuessa liikenne palautuisi automaattisesti normaalitilaan ja alkaisi jälleen toimia ennalta määritettyjen kuormantasaussääntöjen mukaan. Tällä tavoin voidaan rakentaa vikasietoisempia ja tietoturvallisempia yhteyksiä huomat-

tavasti edullisemmin kuin normaaleilla MPLS-teknologian pohjautuvilla toteutuksilla.

Multi-Link-teknologia helpottaa myös viiveille herkkien tai paljon tietoliikennekaistaa vaativien sovellusten toimintaa. Tyypillisesti esimerkiksi VOIP-puheluille halutaan varata tietty määrä laadukasta tietoliikennekaistaa, mutta esimerkiksi www-liikenne sen sijaan voidaan reitittää edullisen kuluttajaliittymän kautta internetiin.

Kaiken kaikkiaan Multi-Link-teknologia mahdollistaa yritykselle hyvin yksinkertaisen ja kustannustehokkaan tavan rakentaa vikasietoiset ja tietoliikenneoperaattorista riippumattomat internetyhteydet. Yrityksen eri toimipisteet on yhtä lailla mahdollista yhdistää tietoturvallisesti ja operaattoririippumattomasti samaa teknologiaa hyödyntäen. Teknologian käyttö ei vaadi operaattoreiden välisiä peering-sopimuksia, ei erityisosaamista eikä enterprise-tason laitteita. Teknologian käyttöön riittää Stonegate-palomuurilaitteet ja palomuuritekniikan perustuntemus. Stonesoft suosittelee kuitenkin aina muutaman päivän peruskurssia ennen käyttöönottoa. Yrityksen liiketoiminnan kannalta kyseessä on kuitenkin kriittiset asiat eli tietoliikenneverkon toiminta ja tietoturva. Multi-Link on Stonesoftin patentoima uniikki teknologia. (Stonesoft Management Center datasheet 2012.)

3.2.4 Stonesoft IPS

IPS-laitteen tarkoituksena on havainnoida ja estää erilaisia verkosta tulevia hyökkäyksiä ja uhkia sekä raportoida näistä. Laite asennetaan tyypillisesti palomuurin taakse, jolloin kaikki palomuurin läpäissyt liikenne kulkee vielä IPS-laitteen läpi ennen varsinaiseen sisäverkkoon pääsyä. Laite analysoi liikennettä useilla eri metodeilla ja havaittuaan uhkia se pyrkii estämään ne ja raportoimaan niistä eteenpäin. Nykyaikaiset IPS-laitteet ovat proaktiivisia eli ne ottavat kantaa myös tuntemattomiin uhkiin. Palomuuri- ja IPS-laitteet lähestyvät ominaisuuksiensa puolesta toisiaan koko ajan ja välillä rajanveto niiden välille onkin melko vaikeaa. Useimmiten palomuureissa on IPS-laitteiden ominaisuuksia ja toisaalta myös IPS-laitteissa on ominaisuuksia, joita on totuttu näkemään palomuureissa.

Stonesoftin IPS-ratkaisu integroituu täysin SMC-hallintajärjestelmään ja on keskeinen osa Stonesoftin kerroksellista suojautumisjärjestelmää. IPS:n tärkeimpiä tehtäviä on suojata yrityksen verkko kehittyneiltä evaasiotekniikoilta. Stonesoft on tehnyt uraa uurtavaa tutkimustyötä juuri kehittyneiden evaasiotekniikoiden parissa.

3.2.5 Markkinatilanne

Stonesoft on alle 30 miljoonan eron liikevaihdollaan erittäin pieni tekijä globaalissa tietoturvamarkkinassa. Markkinaa hallitsevat globaalisti toimivat suuryritykset, kuten Cisco, Check Point ja HP. Stonesoftin edistyksellisestä teknologiasta kertoo kuitenkin paljon se, että Gartner on valinnut yrityksen tuotteet mukaan vuosittain julkaisemiinsa tutkimuksiin Magic Quadrant for Enterprise Network Firewalls ja Magic Quadrant for Intrusion Prevention systems.

Gartner kuvailee tutkimuksessaan Magic Quadrant for Enterprise Network Firewalls 2011 Stonesoftin vahvuuksia seuraavasti:

- Stonesoftin tutkimustyö koskien evaasiotekniikoita on lisännyt yhtiön ja sen tuotteiden uskottavuutta ja näkyvyyttä.
- Stonesoft on tietoturvaan keskittynyt toimittaja, joka on osoittanut laitteessaan erittäin hyvää suorituskykyä niin ohjelmistojen kuin läpäisykyvyn osalta.
- Stonesoft tarjoaa myös virtualisoidun version palomuuristaan, joka on sertifioitu VMwarelle ja jota voi hallita SMC:n avulla.
- Stonesoft tarjoaa tuotteissaan tuen klusteroinnille, erittäin korkeaa käytettävyyttä ja mahdollisuuden 3G-varayhteyksille.
- Tuen hinta on hieman alle alan keskiarvon ja yrityksellä on uskollinen asiakaskunta.

Heikkoudet:

- Stonesoftilla on rajallinen näkyvyys EMEA-alueen ulkopuolisilla markkinoilla. Näkyvyys on heikkoa myös Gartnerin asiakkaiden piirissä, vaikkakin yrityksen liikevaihto kasvanut.

- Vaikka Stonesoftin palomuureissa on paljon uuden sukupolven ominaisuuksia, niin siitä huolimatta sen näkyvyys on ollut heikko Gartnerin asiakkaiden piirissä (Young & Pescatore. 2011.)

Gartner kuvailee tutkimuksessaan Magic Quadrant for Intrusion Prevention Systems 2012 Stonesoftin vahvuuksia seuraavasti:

Vahvuudet

- Stonesoftin hyvät toisen sukupolven IPS-ominaisuudet ylittävät ensimmäisen sukupolven laitteiden ominaisuudet.
- Stonesoftin palomuureilla ja IPS-laitteilla on yhteinen laitteisto- ja ohjelmistoalusta, joka tarjoaa mahdollisuuden tuoda IPS-ominaisuuksia palomuuriin tai toisinpäin.
- Stonesoftin tutkimus edistyneiden evaasiotekniikoiden osalta sekä sen kyky suojata näitä tekniikoita vastaan on lisännyt sen näkyvyyttä yritysten parissa, jotka ovat kokeneet edistyneet ja kohdennetut hyökkäykset uhiksi.

Heikkoudet

- Stonesoft ei kuulu viiden suurimman IPS-tuotteisiin erikoistuneen yrityksen joukkoon (Market Share: Enterprise Network Security Equipment and Routers, Worldwide 2011).
- Stonesoftin näkyvyys on tällä hetkellä maantieteellisesti heikko Gartnerin asiakkaiden parissa (Young & Pescatore. 2012.)

Pienestä koostaan huolimatta Stonesoft on viime aikoina saanut erittäin paljon julkisuutta koskien kehittyneitä evaasiotekniikoita. Stonesoft julkaisi tiedotteen kehittyneistä evaasiotekniikoista jo vuonna 2010, mutta keskustelu niiden ympärillä jatkuu edelleen. Monet valmistajat ovat sitä mieltä, että Stonesoft liioittelee niiden merkitystä. Stonesoft itse on täysin vakuuttunut niiden aiheuttamista tietoturvariskeistä ja onkin antanut markkinoinnissaan niille erittäin suuren painoarvon.

Tulevaisuuden näkymistään Stonesoft kertoo osavuosikatasauksessaan seuraavasti:

”Vuonna 2011 alkoi kehitys, jossa Stonesoft ja muut verkon tietoturvaan erikoistuneet yritykset kasvoivat voimakkaasti. Stonesoft olettaa tietoturvauhkien kehittyvän huolestuttavampaan suuntaan, mikä luo yhtiölle uusia liiketoimintamahdollisuuksia.
Stonesoftin kattava tuotetarjonta vastaa nopeasti kehittyviin ja muuttuviin tietoturvahaasteisiin, mukaan lukien pilvipalveluiden, virtualisoinnin ja tietoturvan ulkoistuksen mukanaan tuomat vaatimukset.” (Stonesoft Oyj Pörssitiedote 19.10.2012 klo 9.15.)

4 CASE: FIRMA.FI

Tässä kappaleessa tarkastelen esimerkinomaisesti erään suomalaisen yrityksen (jatkossa Firma.fi) nykyisen TDC:n toimittaman IP VPN -tietoliikenneratkaisun korvaamista Stonesoftin vaihtoehtoisella ratkaisulla. Firma.fi:n nykyistä tietoliikenneratkaisua koskevat tiedot mukaan lukien sen hyvät ja huonot puolet, ovat peräisin minun ja Firma.fi:n IT Managerin välisestä puhelinhaastattelusta. Tarkastelen ratkaisuja kolmesta eri näkökulmasta. Nämä ovat kustannustehokkuus, vikasietoisuus ja tietoturva. Valitsin nämä kolme näkökulmaa, koska ne ovat mielestäni yrityksen kannalta kolme keskeisintä asiaa. Lisäksi ne ovat myös melko helposti mitattavia. Tekniikoita vertaillessani jätän vertailun ulkopuolelle muun muassa hallintaan liittyvät asiat, koska ne ovat ihmisten tottumuksiin ja mielipiteisiin liittyviä asioita. Lopputuloksena syntyy melko kattava arvio Stonesoftin teknologian soveltuvuudesta ko. yrityksen käyttöön. Arvio ei luonnollisesti kerro absoluuttista totuutta, mutta toimii ohjenuorana tietoliikenneratkaisua mietittäessä.

4.1 Firma.fi

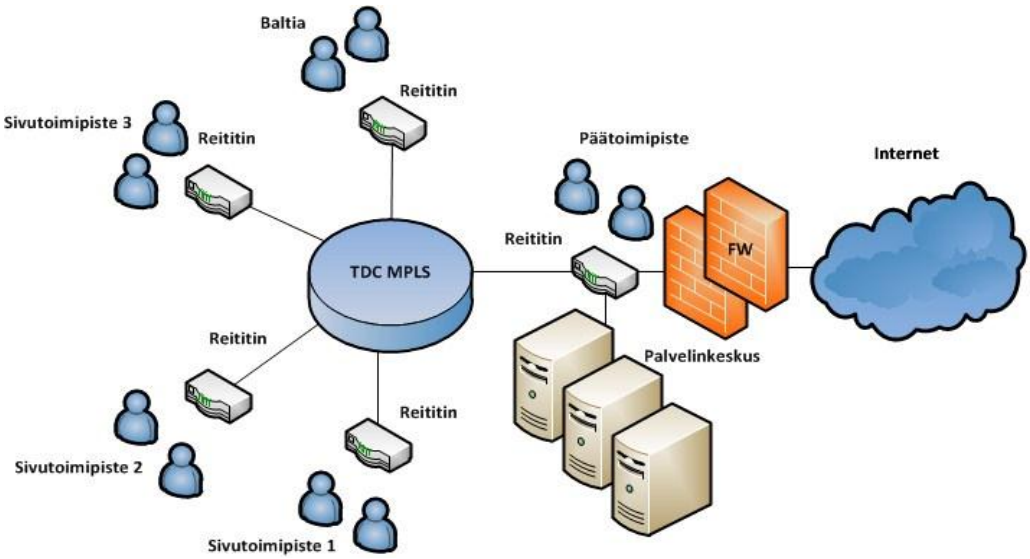
Firma.fi toimii Suomessa neljällä paikkakunnalla ja niiden lisäksi yrityksellä on toimipiste Baltiassa. Yrityksen henkilöstömäärä on noin 150 henkilöä. Yrityksen liiketoiminnan luonteesta johtuen tietoverkot ovat erittäin keskeisessä roolissa. Yrityksen tietojärjestelmät sijaitsevat keskitetyssä konesalissa, joka on tähtimäisesti toteutetun verkon keskipiste. Täältä käsin tuotetaan peruspalveluiden, kuten Active Directory ja tiedosto- ja tulostuspalveluiden lisäksi mm. ERP-, CRM-, VDI- ja VOIP-palvelut. Yrityksellä on käytössä myös videoneuvotteluratkaisu toimipisteiden väliseen kommunikointiin. Verkkoratkaisuna on tietoliikenneoperaattorin toimittama MPLS-tekniikkaan pohjautuva yritysverkko. MPLS-tekniikkaan perustuva ratkaisu on ollut yrityksen käytössä jo useita vuosia. Verkon toiminta on ollut luotettavaa ja valittuun ratkaisuun on oltu päällisin puolin tyytyväisiä. Huonona puolena ratkaisussa on operaattorisidonnaisuus sekä melko korkea kustannustaso. Tämän tyyppistä ratkaisua on melko vaikea kilpailuttaa ja vaihtaa, koska tietoliikenneoperaattorin vaihto toiseen aiheuttaa erittäin suuria muutoksia verkkoon. Verkon muutokset taas puolestaan aiheuttavat katkoksia lii-

ketoimintaan. Lisäksi dataverkon ja puhepalveluiden hinnoittelu on osittain sidottu toisiinsa, jolloin muutettaessa datapalveluiden toimittajaa saattaa myös puhepuolen hinnoittelu muuttua. Vikasietoisuuden parantaminen ilman kustannuksien merkittävää nousua on myös havaittu haasteelliseksi. Syynä tähän on lähinnä ollut tietoliikenneoperaattorin korkeahko hinnoittelu.

4.2 Nykyinen tietoliikenneratkaisu

Yrityksen nykyinen tietoliikenneratkaisu on TDC:n (Pohjoismainen tietoliikenneoperaattori) toimittama MPLS-teknologiaan pohjautuva IP VPN -ratkaisu. Ratkaisu on ollut yrityksen käytössä jo useita vuosia (ks. kuvio 7).

”TDC IP VPN on lähiverkkojen yhdistämispalvelu, joka yhdistää yrityksen eri toimipisteiden lähiverkot. TDC IP VPN luo lähiverkkojen välille yhtenäisen verkkokokonaisuuden johon voidaan liittää esimerkiksi mobiiliverkoissa toimivia päätelaitteita, kiinteitä yritysliittymiä sekä muita palveluverkkoja.” (TDC IP VPN 2012.)



Kuvio 7 Firma.fi:n nykyinen tietoliikenneratkaisu

Firma.fi:n verkko on toteutettu siten, että IP VPN -palvelu yhdistää lähiverkot eri paikkakunnilla yhdeksi loogiseksi kokonaisuudeksi. Kaikki yrityksen oman verkon ulkopuolelle suuntautuva liikenne reititetään päätoimipisteeseen ja sieltä keskitetyn asiakkaan omistaman ja hallinnoiman palomuurin läpi internetiin. TDC toimii tietoliikenneoperaattorina myös internetliikenteen osalta. Lisäpalveluna yri-

tys on hankkinut TDC:ltä Multi-VPN -palvelun, joka mahdollistaa useamman asiakaskohtaisen virtuaalisen lähiverkon. Virtuaalisia lähiverkkoja hyödynnetään muun muassa VOIP-liikenteessä ja koko yrityksen kattavassa langattomassa vierailijaverkossa.

”Multi-VPN lisäpalvelu tarjoaa asiakkaalle useampia asiakaskohtaisia virtuaaliverkkoja (VPN). Multi-VPN lisäpalvelussa TDC ylläpitää liikenteen erottelua alkaen asiakaspäätelaitteen liityntärajapinnasta asiakasliittymien ja TDC:n runkoverkon yli aina kohdetoimipisteen asiakaspäätelaitteen liityntärajapintaan asti. Kohteena olevassa toimipisteessä liikenne ohjataan kyseiseen VPN-verkkoon liitettyyn virtuaaliseen lähiverkkoon (Virtual LAN, VLAN). Asiakaspäätelaitteessa liikenteen erottelu toteutetaan käyttäen virtuaalisia reitittimiä (VRF).” (TDC IP VPN Lisäpalvelut: Palvelutasot 2011.)

Verkko on toteutettu siten, että kaikki lähiverkkojen yhdistämiseen tarvittavat verkon aktiivilaitteet ovat tietoliikenneoperaattorin omaisuutta ja se vastaa niiden hallinnasta ja ylläpidosta. TDC on toteuttanut verkon kauttaaltaan Ciscon teknologialla. Kuviossa 7 olevat palomuurilaitteet ovat yrityksen omaisuutta ja yritys hallinnoi niitä itse. Palomuurilaitteet ovat Stonesoftin teknologiaa ja niistä on muodostettu aktiivi/aktiivi -klusteri.

Ratkaisun hyvänä puolena on, että yrityksen ei tarvitse investoida laitteisiin eikä yrityksellä myöskään tarvitse olla osaamista kyseessä olevista laitteista palomuurilaitteitta lukuun ottamatta. Huonoksi puoleksi voidaan katsoa, että yritys ei voi tehdä itse mitään muutoksia tai vikatilanteessa korjaavia toimenpiteitä laitteille. Verkon ongelmatilanteiden ratkaisua helpottaa ja myös nopeuttaa, koska jokaisella paikkakunnalla on sama tietoliikenneoperaattori. Tällöin vikatilanteista voidaan ilmoittaa yhteen paikkaan ja myös korjaavat toimenpiteet tehdään yhdestä paikasta. Näin vältetään valitettavan yleinen tilanne, jossa eri osapuolet syyttelevät tosiaan ja pyrkivät siirtämään ongelman eteenpäin. On tärkeää kuitenkin huomata, että tietoliikenneoperaattorin vastuu ulottuu ainoastaan reitittimelle ja jokaisella paikkakunnalla on verkossa myös muita aktiivilaitteita. Mahdolliset internetliikenteeseen liittyvät ongelmat ovat myös asia erikseen, koska palomuurit ovat yrityksen omassa hallinnassa. Tästä syystä IP VPN -ratkaisu ei ole täysin poistanut yritykseltä oman verkko-osaamisen tarvetta.

4.2.1 Vikasietoisuus

Firma.fi:n IP VPN -ratkaisussa vikasietoisuus ja tarvittavat kahdennukset on toteutettu lähinnä TDC:n runkoverkon osalta. Asiakkaan tiloissa olevia laitteita ei ole kahdennettu päätoimipisteen keskitettyä palomuuriklusteria lukuun ottamatta. Tämä on hyvin tyypillinen tapa toteuttaa tämänkaltaiset ratkaisut PK-yrityksissä. Asiakkaan tiloissa olevan laitteen vikaantuessa vasteaika sen vaihtamiseen on seuraava työpäivä. Yritys on miettinyt toimittajan kanssa lisäpalveluna saatavaa palvelutason nostoa mahdollisten vikatilanteiden varalle. TDC kertoo IP VPN -palveluun lisäpalveluna saatavista palvelutasoista seuraavasti:

”Vian ollessa vähäinen palveluaika Standard-tasolla on arkisin klo 08.00—16.00, Premium- ja Exclusive-tasolla klo 08.00—22.00. Suuremmassa vikatilanteessa, eli silloin, kun liittymän käyttö on kokonaan estynyt, Exclusive-asiakkaita palvellaan vuorokauden ympäri viikon jokaisena päivänä.”

”Vasteaika on enimmäisaika, joka kuluu asiakkaan yhteydenotosta vianselvityksen aloittamiseen. Vasteajat vaihtelevat palvelutasosta riippuen yhdestä tunnista neljään tuntiin. Exclusive-palvelutaso takaa vianselvityksen aloittamisen jopa tunnin kuluessa palvelupyynnöstä vian laajuudesta huolimatta.” (TDC IP VPN 2012.)

Palvelutason nostaminen on kuitenkin todettu toistaiseksi tarpeettomaksi, koska sen ei ole katsottu lisäävän verkon toimivuutta palvelun hintaan nähden riittävästi. Ongelmana on lähinnä, että runkoverkon ongelmat korjautuvat kyllä nopeasti, koska ne koskettavat pääsääntöisesti useita asiakkaita. Asiakaskohtaiset ongelmat sen sijaan johtuvat useimmiten päätelaitteen vikaantumisesta, jolloin palvelutason nosto ei merkittävästi nopeuta vikatilanteesta palautumista. Vikatilanteessa suurin osa ajasta kuluu kuitenkin uusien laitteiden lähettämiseen, konfigurointiin ja yrityksen verkkoon kytkemiseen. Tähän ongelmaan käytännössä ainoa ratkaisu olisi laitteiden kahdentaminen tai varalaitteiden säilyttäminen yrityksen toimipisteissä.

4.2.2 Tietoturva

IP VPN -ratkaisussa yritys on ulkoistanut tietoturvan sisäverkon osalta tietoliikenneoperaattorille. Tällöin tietoturva on juuri niin vahva kuin tietoliikenneoperaattori sen haluaa olevan. On tärkeää huomata, että lähtökohtaisesti tietoturvan ulkoistaminen ei paranna sitä, vaan ainoastaan vastuu siitä siirtyy. MPLS-

tekniikkaan pohjautuvissa IP VPN -toteutuksissa data ei ole salattua, vaan tietoliikenneoperaattorin verkon sisällä liikkuessaan se on täysin lukukelpoista. Halutessaan tietoliikenneoperaattorin henkilökunnalla on mahdollisuus päästä käsiksi yrityksen verkossa liikkuvan dataan. Kyseessä on erittäin olennainen seikka, kun käsitellään esimerkiksi tärkeää tuotekehitysdataa tai vaikka valtion turvallisuuteen liittyvää aineistoa. Firma.fi ei käsittele tämänkaltaista aineistoa.

TDC kertoo IP VPN -ratkaisun tietoturvasta ja tekniikasta seuraavasti

”TDC IP VPN muodostaa yritykselle oman suljetun verkon. Yhdistettyjen lähiverkkojen liikenne ei missään vaiheessa kulje julkisen Internetin kautta, eivätkä verkossa liikennöivät asiakkaat näe toisiaan. TDC monipalveluverkon varmennetut yhteydet ja verkon MPLS-tekniikka takaavat että liikenne ohjautuu verkossa automaattisesti aina suorinta ja nopeinta tietä haluttuun pisteeseen.” (TDC IP VPN 2012.)

Toisaalta verkon riskejä kartoitettaessa on syytä miettiä, missä suurimmat riskit ovat. Ovatko ne tietoliikenneoperaattorin hallinnoimassa sisäverkossa vai esimerkiksi yrityksen hallinnoimassa palomuurissa tai loppukäyttäjien päätelaitteissa. Palomuuri on yrityksen sisäverkon ja julkisen verkon välissä ja se toimii myös alustana, jonka läpi julkaistaan erilaisia palveluita julkisen verkon puolelle kuten esimerkiksi ekstranet-palvelut. Nämä palvelut ovat tyypillisesti jatkuvien hyökkäysyritysten kohteena, jolloin niiden kunnollinen suojaaminen on erityisen tärkeää. Loppukäyttäjien päätelaitteiden suojaaminen on taas jatkuvaa tasapainoilua tietoturvan ja käytettävyyden välillä ja tästä syystä päätelaitteisiin liittyen on aina tiettyjä uhkia olemassa.

”Turvallisuus on tärkeää, mutta käytettävyys on kaiken A ja O.” (Firma.fi IT-Manager 2012.)

Tietoturva koostuu useista kerroksista ja mikään yksittäinen kerros ei takaa yritykselle absoluuttista turvaa. Toisaalta minkään yksittäisen kerroksen vahvistaminen ei myöskään heikennä kokonaisuutta.

4.2.3 Kustannukset

Firma.fi:n nykyisen tietoliikenneratkaisun kustannuksia tarkastellessa on syytä huomioida, että kustannukset eivät välttämättä ole täysin läpinäkyviä. Tämä joh-

tuu siitä, että yrityksellä on käytössä useita eri ratkaisuja samalta tietoliikenneoperaattorilta, jolloin jonkin tietyn palvelun hintaa on saatettu kompensoida jollain toisella. Vertailussa käytän niitä lukuja, jotka yrityksen laskulta löytyvät. Tässä laskelmassa ei huomioida mahdollisesta ratkaisun vaihdosta johtuvia käyttöönottokustannuksia. Päätoimipisteen kustannukset sisältävät myös internet-liikenteen ja tarpeellisen määrän julkisia IP-osoitteita. Asiakkaan pyynnöstä verkkoon tehtävät muutokset laskutetaan kulloinkin vallitsevan hinnaston mukaan.

Toimipiste	**Nopeus mbs**	**Hinta € per kk**
Päätoimipiste	200	1 300,00
Sivutoimipiste 1	100	590,00
Sivutoimipiste 2	10	250,00
Sivutoimipiste 3	10	250,00
Baltia	10	1 000,00
Hinta yhteensä:		**3 390,00**

Taulukko 1. Firma.fi:n tietoliikenneyhteyksien kuukausikustannukset.

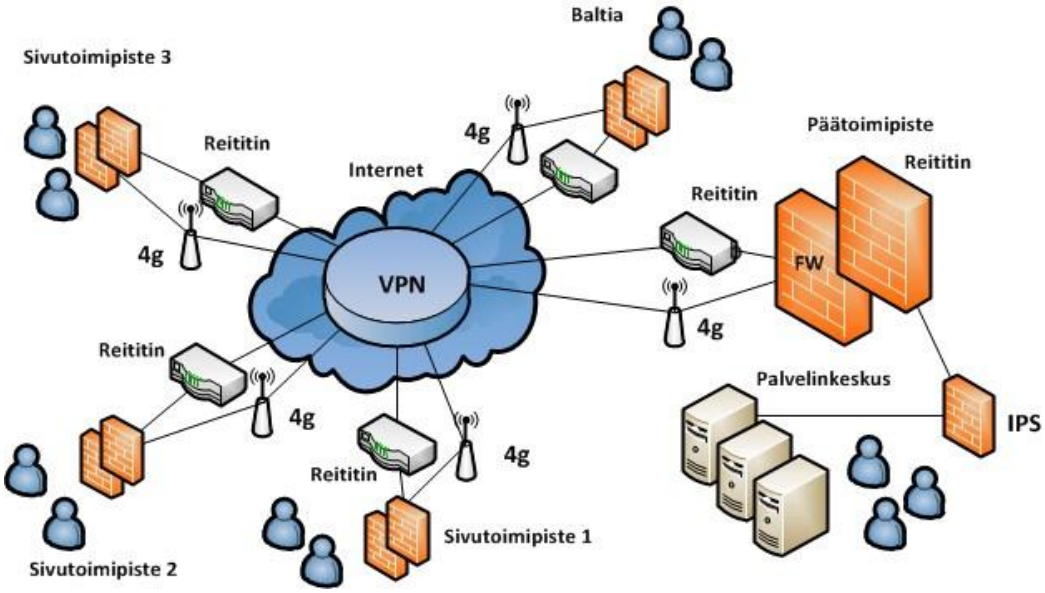
Kuten yllä olevasta taulukosta huomaa niin kokonaiskustannuksiin vaikuttaa erittäin paljon toimipisteiden maantieteellinen sijainti. Firma.fi:n verkon toiminnan kannalta on täysin merkityksetöntä sijaitseeko toimipiste Suomessa vai ulkomailla, mutta kustannusten kannalta sillä on erittäin suuri merkitys. Hyvänä esimerkkinä toimii Baltian toimipiste, jonka tietoliikenneyhteyden kuukausihinta on nelinkertainen verrattuna Suomessa sijaitseviin toimipisteisiin. Paineita kustannusten laskuun on, koska yritys on laajentamassa toimintaansa muun muassa Ruotsiin. Toimipisteen maantieteellinen sijainti voi vaikuttaa myös palvelutasoihin ja palveluiden saatavuuteen sekä toimitusaikoihin. Yritys pitää kuitenkin erittäin tärkeänä verkon säilymistä eheänä kokonaisuutena ja pyrkii välttämään hybridiver-

kon tuomat ongelmat. Tästä syystä mahdollisiksi vaihtoehdoiksi jää nykyinen TDC:n toimittama ratkaisu tai sitten sen korvaaminen kokonaisuudessaan Stonesoftin teknologialla.

4.3 Ratkaisuna Stonesoft Multi-Link VPN

Tässä kappaleessa esittelen Firma.fi:n tarpeisiin sopivan Stonesoftin teknologiaan pohjautuvan ratkaisuehdotuksen. Ratkaisulla voidaan korvata nykyinen TDC:n toimittaman ratkaisu sekä myös tuottaa huomattavaa lisäarvoa verrattuna nykyiseen ratkaisuun. Lisäarvo syntyy vikasietoisuuden ja tietoturvan paranemisesta sekä kustannusten laskusta. Yrityksen kannalta keskeisin asia on, että samoilla tai pienemmillä kustannuksilla voidaan tuottaa vastaavat tai paremmat palvelut. Kokonaiskustannuksia katsottaessa on syytä huomioida nykyisen ratkaisun korvaamisen aiheuttamat käyttöönottokustannukset.

Ratkaisuehdotus koostuu Stonesoft Management Center -hallintalisenssin laajennuksesta, sivutoimipisteisiin hankittavista palomuurilaitteista, IPS-laitteesta sekä kahdennetuista tietoliikenneyhteyksistä (ks. Kuvio 8. Stonesoft-verkko). Yrityksellä ei ole tällä hetkellä IPS-laitteita käytössä, joten se aiheuttaa hieman lisäkustannuksia nykyiseen ratkaisuun verrattuna. IPS-laitteen tehtävänä olisi kasvattaa tietoturvan tasoa nykytilanteeseen verrattuna ja sitä kautta varmistaa verkon häiriötön toiminta. Kokoonpano on laadittu kolmen vuoden tukisopimuksilla. Laitteet on mitoitettu nykyisten internetliittymien kapasiteetin mukaan. Verkon topologia säilyy ratkaisuehdotuksessa keskeisiltä osiltaan ennallaan, jolloin uuden ratkaisun implementointi olisi mahdollisimman helppoa. IP-osoitteiden säilyessä ennallaan uusi verkko olisi mahdollista rakentaa lähes valmiiksi vanhan verkon rinnalle, jolloin käyttöönottovaiheessa tuotantoverkon katkokset jäisivät mahdollisimman lyhyeksi.



Kuvio 8. Stonesoft-teknologialla toteutettu verkko.

Kustannussäästöjä syntyisi, kun nykyiset tietoliikenneyhteydet korvattaisiin edullisilla niin sanotuilla kuluttajaliittymillä. Alueellisesta saatavuudesta johtuen liittymät voisi olla toteutettu useilla eri tekniikoilla. Yleisimpiä kuluttajaliittymätoteutuksia ovat ADSL-, kaapelimodeemi- ja valokuitupohjaisettoteutukset. Erittäin mielenkiintoinen vaihtoehto on matkapuhelinverkossa toteutettu 4G-yhteys. Ratkaisun kannalta ei ole merkitystä, mikä tai mitkä edellä mainituista teknologioista olisivat käytössä. Yhteistä näille kaikille on halpa hinta, hyvin rajoitetut ominaisuudet ja pääsääntöisesti dynaamiset IP-osoitteet. Multi-Link VPN -teknologia mahdollistaa virtuaalisen yksityisverkon muodostamisen, vaikka sivutoimipisteissä olisikin käytössä ainoastaan dynaamisia IP-osoitteita.

Ratkaisuehdotuksessa ainoastaan yrityksen päätoimipisteeseen jäisi nykyinen 200 megabitin nopeudella toimiva niin sanottu yritysliittymä, johon olisi kytketty nykyiset julkiset IP-osoitteet. Sivutoimipisteet toteutettaisiin saatavuudesta riippuen joko kaapelimodeemilla tai vaihtoehtoisesti kuituyhteyksillä. Niiden lisäksi jokaiseen toimipisteeseen tulisi 4G-yhteys. Kussakin toimipisteessä olisi tällöin kahdennettu yhteys, joka olisi kapasiteetiltansa huomattavasti nykyistä suurempi. Multi-Link -teknologia huolehtisi kuormantasauksesta liittymien välillä.

Firma.fi:n päätoimipisteen internetliittymä säilyisi ennallaan ja se toimisi myös jatkossa kaikkien toimipisteiden keskitettynä reittinä internetiin. Asiakkaille, toimittajille ja yhteistyökumppaneille luodut VPN-tunnelit terminoitaisiin edelleen kaikki päätoimipisteeseen, jolloin myös niiden liikenne kulkisi IPS-laitteen läpi. Tällä tavoin voitaisiin varmistua myös yrityksen ja sen yhteistyökumppaneiden välisen liikenteen turvallisuudesta.

4.3.1 Vikasietoisuus

Stonesoftin ratkaisussa vikasietoisuus on erittäin korkealla tasolla. Valitsin esimerkkikokoonpanoon jokaiseen toimipisteeseen klusteroidun StoneGate-palomuurilaitteen. Yrityksen päätoimipisteessä on jo Stonesoftin valmistama aktiivi/aktiivi-klusteri. Sivutoimipiste 1:n valitsin käyttäjämäärästä johtuen myös aktiivi/aktiivi-klusterin. Toisen klusterin jäsenen vikaantuessa toinen klusterin jäsen ottaa toisen tehtävät haltuun ilman katkosta. Muihin toimipisteisiin valitsin niin sanotun aktiivi/passiivi -klusterin. Aktiivisen laitteen vikaantuessa passiivinen laite ottaa sen tehtävät haltuun, mutta yhteydet katkeavat muutamaksi sekunniksi. Syynä erityyppisten klustereiden valintaan oli toimipisteiden kokoero. Kustannustehokkuus paranee hieman käytettäessä aktiivi/passiivi-klusteria pienimmissä toimipisteissä ilman, että käytettävyys kärsii merkittävästi.

Huomattava parannus vikasietoisuuteen syntyy myös aktiivisten toimipistekohtaisten varayhteyksien kautta, jotka mahdollistaa Stonesoftin Multi-Link VPN -teknologia. Nykyisessä ratkaisussa tietoliikenneyhteyden vikaantuminen eristää toimipisteen yrityksen verkosta ja samalla estyy lähes kaikkien tietojärjestelmien käyttö. Stonesoftin teknologiaan pohjautuvassa ratkaisussa vastaavassa vikatilanteessa siirrytään automaattisesti käyttämään varayhteyttä. Varayhteyden nopeuden tulee kuitenkin olla riittävä, jotta halutut sovellukset toimivat myös vikatilanteessa. Tyypillisesti vikatilanteissa priorisoidaan sovelluksia eli käytännössä esimerkiksi videoneuvottelut voivat estyä, mutta ERP-järjestelmän tulee toimia. Mikäli mahdollista, niin toimipisteen tietoliikenneyhteydet kannattaa toteuttaa eri teknologioilla. Yhdistämällä kiinteän verkon ja mobiiliverkon yhteyksiä saadaan aikaiseksi erittäin vikasietoinen kokonaisuus. Yhteydet on mahdollista hankkia myös

eri tietoliikenneoperaattoreilta, mutta tällöin on riskinä ratkaisun monimutkaistuminen. Suosittelenkin hankkimaan kaikki liittymät yhdeltä valtakunnalliselta tietoliikenneoperaattorilta.

Vikasietoisuuden osalta on syytä huomioida myös yrityksen resurssit. Nykyisessä mallissa tietoliikenneoperaattori vastaa toimipisteiden välisistä yhteyksistä ja niihin liittyvistä ongelmista. Lähtökohtaisesti voimme olettaa, että tietoliikenneoperaattorilla on riittävä tekninen osaaminen ja riittävät resurssit mahdollisten vikatilanteiden korjaamiseksi. Vaihtoehtoisessa mallissa yritys vastaa itse tai yhteistyökumppanin kanssa laitteista, jolloin on tärkeä miettiä toimintamallit ja vastuumatriisit mahdollisia vikatilanteita varten valmiiksi. Yrityksen tulee myös huomioida käytössä olevien resurssien riittävyys ja tekninen osaaminen. Hyvä ratkaisu on tehdä jonkinasteista yhteistyötä jonkin tietoturvaan erikoistuneen yrityksen kanssa, joka voi tarpeen vaatiessa antaa osaavia resursseja yrityksen käyttöön.

4.3.2 Tietoturva

Firma.fi katsoo nykyisen tietoliikenneratkaisun tietoturvatason olevan nykytilanteessa riittävä.

”Mikäli tietoturvatasoa haluttaisiin nostaa, se tehtäisiin todennäköisesti verkon ulkolaidalla olevan palomuurin säännöstöä tiukentamalla ja verkon sisäpuolelle asennettavalla IPS-laitteella.” (Firma.fi IT-Manager 2012.)

Näiltä osin kumpikin, niin nykyinen kuin Stonesoftin tietoliikenneratkaisu, on yhtenevä. Sillä kummassakin ratkaisussa liikennöidään internetiin asiakkaan hallinnoiman palomuurin läpi. Vaatimukset tietoturvaa kohtaan kasvavat kuitenkin koko ajan. Vaatimusten kasvu johtuu uhkien lisääntymisestä, yrityksen kasvusta ja asiakkaiden vaatimusten tiukentumisesta. Tästä johtuen tietoturvatason proaktiivinen nostaminen voidaan katsoa yrityksen kannalta erittäin hyödylliseksi.

Tietoturvan kannalta merkittävin ero syntyy toimipisteiden välisessä liikenteessä. Nykyisessä ratkaisussa data kulkee eristetyssä verkossa, mutta se ei ole salattua. Stonesoftin-ratkaisussa data on salattua, mutta se kulkee julkisessa verkossa.

Stonesoftin-ratkaisussa on lisäksi mahdollista rajoittaa toimipisteiden välistä liikennettä juuri niin kuin yritys haluaa. Lähtökohtaisesti sallitaan vain tarpeellinen liikenne ja muu liikenne estetään. Keskitetty hallinta mahdollistaa myös nopean reagoimisen esimerkiksi internetissä leviävään virusepidemiaan. Kun tiedetään, mitä liikennettä halutaan estää, niin esto voidaan tehdä muutamissa minuuteissa ja se kattaa koko yrityksen verkon. Tällä tavoin voidaan edellä mainitun kaltainen epidemia tehokkaasti eristää ja minimoida sen aiheuttamat vahingot.

4.3.3 Kustannukset

Tässä kappaleessa vertailen kahden edellä mainitun ratkaisun kustannuksia siltä osin kuin se on mahdollista. Tämä tarkoittaa käytännössä nykyisiä tietoliikenneratkaisun kuukausikustannuksia verrattuna vaihtoehtoisen ratkaisun hankintakustannuksiin. Vertailujaksona on toimialalle tyypillinen 36 kuukautta. Vertailun tarkoituksena ei ole kertoa absoluuttista totuutta investoinnin kannattavuudesta, vaan sen tehtävänä on kertoa mahdollisesta säästöpotentiaalista. Lisäksi nostan esiin muutamia oheiskustannusten kannalta tärkeimpiä seikkoja. Näitä ovat muun muassa transitiokustannukset, koulutuskustannukset ja ylläpitokustannukset.

Stonesoft-ratkaisun ylläpidon ja hallinnan voi myös ulkoistaa kumppanille. Tällöin saavutettaisiin toki teknologiahyöty, mutta esimerkiksi joustavuus ja reagointinopeus todennäköisesti kärsisivät jonkin verran. Firma.fi:llä on omaa korkealla osaamistasolla varustettua IT-henkilöstöä, joilla on kokemusta nykyisen Stonesoft –palomuuriratkaisun ylläpidosta, joten tämä näkökulma jätetään epätodennäköisyytensä vuoksi käsittelemättä. Koulutuskustannuksia ei myöskään synny tässä vaiheessa, koska yrityksen IT-henkilöstöllä on riittävä osaaminen ratkaisusta.

Ylläpitokustannuksia aiheutuu jonkin verran esimerkiksi laitteiden vaatimista ohjelmistopäivityksistä johtuen. Karkea arvio vuotuisesta työmäärästä on noin 0,5—1 henkilötyöpäivää per toimipiste.

Vaihtoehtoisen ratkaisun kustannukset muodostuvat hankittavista laitteista sekä nykyisten tietoliikenneyhteyksien kustannusten ja korvaavien tietoliikenneyhteyksien kustannusten välisestä erotuksesta.

	Stonesoft hallintapalvelin (viisi toimipistettä)	**Hinta €**
1	StoneGate Management Center, 5 licenses + 3-year Basic support	6 200,00
	Päätoimipiste	
2	StoneGate Firewall FW-1030 –appliance + 3-year Basic Support for FW-1030-C2(8/5) (laitteet jo olemassa)	0
	Sivutoimipiste 1	
2	StoneGate FW-315 firewall + 3-year Basic support	3 300,00
	Sivutoimipiste 2	
2	StoneGate FW-315L firewall + 3-Year Basic Support	2 200,00
	Sivutoimipiste 3	
2	StoneGate FW-315L firewall + 3-Year Basic Support	2 200,00
	Sivutoimipiste Baltia	
2	StoneGate FW-315L firewall + 3-Year Basic Support	2 200,00
	Optiona	
1	StoneGate IPS-1030 –appliance + 3-Year Basic Support	4 900,00
	Hinta yhteensä	**21 000,00**

Taulukko 2. Stonesoft-ratkaisun laitteet hintoineen.

Taulukkoon 2 olen koonnut tarvittavat laitteet 36 kuukauden tukisopimuksineen. Hinnat ovat suuntaa antavia ja perustuvat Stonesoftin vuoden 2013 Q1-hinnastoon. Tarvittavien laitteiden kokonaishinta on noin 21 000 euroa. Tämä summa sisältää sivutoimipisteiden palomuurilaitteet sekä koko verkon suojaamiseen mitoitetun IPS-laitteen. Vertailukelpoisen luvun kuukausikustannuksista saa hyödyntämällä leasing-rahoitusta. Kyseisen kokoonpanon leasing-rahoitus 36 kuukauden sopimuksella on noin 600 euroa kuukaudessa alv 0%.

Taulukkoon 3 olen koonnut suuntaa antavat liittymähinnat sekä niiden teoreettiset maksiminopeudet. Hinnat ovat peräisin Soneran sekä Soneran tytäryhtiön EMT:n www-sivuilta. Hinnoissa ei ole huomioitu liittymien mahdollisia avausmaksuja. Varsinaisia saatavuuskyselyitä liittymille ei ole tehty. Yhteydet on laskettu ADSL- ja 4G-tekniikalla toteutetuille liittymille. Hinnat sisältävät tarpeelliset päätelaitteet. ADSL-tekniikka on valittu toteutustavaksi, koska se on saatavilla varmasti jokaiseen toimipisteeseen.

Toimipiste	**Yhteystyyppi**	**Nopeus mbs**	**Hinta €/kk**
Päätoimipiste	Kuitu (TDC) / 4G	200/200 ja 100/50	1 330,00
Sivutoimipiste 1	Sonera Laajakaista/ 4G	10/5 ja 100/50	47,50
Sivutoimipiste 2	Sonera Laajakaista/ 4G	10/5 ja 100/50	47,50
Sivutoimipiste 3	Sonera Laajakaista/ 4G	10/5 ja 100/50	47,50
Sivutoimipiste Baltia (EMT)	EMT ADSL + 4G	24/3 ja 100/50	130,00
Yhteensä			**1 602,50**

Taulukko 3 Yhteyksien hinnat 23.1.2013 (Sonera ja EMT)

Mikäli Firma.fi päättäisi vaihtaa ratkaisua, niin lähtökohtaisesti pyrittäisiin käyttämään kaapelimodeemiyhteyksiä johtuen niiden halvasta hinnasta ja korkeasta kapasiteetistä. ADSL-tekniikkaa hyödynnettäisiin ainoastaan niissä toimipisteissä, missä kaapelimodeemiyhteyksiä ei olisi saatavilla.

On syytä huomioida, että kummankin teknologian todellinen nopeus on alhaisempi kuin teoreettinen maksiminopeus. Yrityksen toimipisteet sijaitsevat isojen kaupunkien keskustoissa, joten uskon toteutuvien nopeuksien olevan vähintäänkin samansuuruisia kuin nykyiset nopeudet. Kiinteiden yhteyksien osalta huomattavasti suurempiakin nopeuksia on saatavilla niin kuitu- kuin kaapeliverkon toteutuksilla hinnan säilyessä ennallaan.

4.4 Yhteenveto

Yhteenvetona voidaan todeta, että Firma.fi:n kannalta vaihtoehtoinen ratkaisu on erittäin mielenkiintoinen. Se tuottaa merkittäviä etuja kaikilla keskeisillä osa-alueilla niin verkon käytettävyyden kuin tietoturvankin paranemisena ja kustannusten laskuna. Lisäetuna ratkaisussa on myös suurempi kapasiteetti sivutoimipisteiden tietoliikenneyhteyksissä. Tietoliikennekapasiteettia tarvitaan koko ajan enemmän johtuen sovellusten vaatimusten kasvusta. Hyvänä esimerkkinä on videoneuvotteluiden kuvanlaadun muuttuminen teräväpiirto-tasoiseksi.

Edellä mainitut edut on mahdollista saada käyttöön ilman kustannusten kasvua, pikemminkin kustannusten laskiessa. Nykyisten tietoliikennekustannusten ollessa noin 3 400 euroa kuukaudessa ja vaihtoehtoisen ratkaisun kuukausikustannusten jäädessä noin 2 200 euroon kuukaudessa voidaan investointia katsoa perusteltuna ainakin hankintakustannusten osalta. Tämä tarkoittaa 36 kuukauden jaksolla noin 43 000 euron säästöpotentiaalia. Tästä summasta kuluu toki osa käyttöönottoon (arvio 5 henkilötyöpäivää) ja ratkaisun ylläpitoon (0,5—1 henkilötyöpäivää vuodessa per toimipiste). Yritys on laajentamassa toimintaansa ulkomaille, jolloin ratkaisujen välinen hintaero korostuu entisestään johtuen ulkomaisten yhteyksien huomattavasti korkeammista hinnoista.

Strategiselta kannalta katsottuna vastuu verkosta siirtyisi toimipisteiden välisten yhteyksien osalta tietoliikenneoperaattorilta yrityksen IT-henkilöstön vastuulle. Tällöin on tärkeää miettiä valmiiksi mahdolliset päivystykset ja erilaiset lomajärjestelyt, jotta mahdolliset vikatilanteet verkossa saadaan aina hoidettua haluttujen vasteaikojen puitteissa. Riskitekijänä voidaan nähdä myös henkilöstön pysyvyys ja mahdollinen tietotaidon menetys avainhenkilön vaihtaessa työpaikkaa. Tämänkaltaisia riskejä vastaan on kuitenkin helppo suojautua osaavilla kumppaneilla ja huolellisella dokumentoinnilla.

5 JOHTOPÄÄTÖKSET

Maailma yritysten ympärillä muuttuu koko ajan. Muutama vuosi sitten kukaan ei tuntenut esimerkiksi käsitettä pilvipalvelut. Tänä päivänä se on yksi nopeimmin kasvavia IT-markkinoita. Muutoksen nopeudesta johtuen yritysten IT-infrastruktuurit ovat jatkuvien muutospaineiden alla. Muutaman vuoden takaisten parhaiden käytäntöjen mukaan toteutetut ympäristöt eivät välttämättä olekaan enää liiketoiminnan näkökulmasta parhaita mahdollisia. Liiketoiminnan vaatimukset ovat muuttuneet ja monissa yrityksissä myös IT-osastojen rooli on muuttunut. Päätöksiä ei tehdä enää IT:n näkökulmasta, vaan liiketoiminnan näkökulmasta. Tästä johtuen myös tietoverkkoja tulee tarkastella uudesta näkökulmasta.

Perinteisten verkkoratkaisujen korvaamisessa Stonesoft osoittautui erityisen mielenkiintoiseksi vaihtoehdoksi. Heidän kehittämänsä Multi-Link Vpn -teknologia mahdollistaa nykyisten MPLS-ratkaisujen korvaamisen siten, että verkkojen käytettävyys paranee ja tietoturvan taso nousee, kustannusten pysyessä ennallaan tai jopa laskiessa. Olennaisena osana tässä kehityspolussa on mobiiliverkkojen kehittyminen. Nykyiset 4G-verkot ovat äärimmäisen kustannustehokas keino niin tietoliikennekapasiteetin lisäämiseen kuin yhteyksien kahdentamiseen. Tässä työssä esitellyn teknologian hyödyt ovat niin ilmeiset, että hyvin todennäköisesti tietoliikenneverkkojen puolella tulee tapahtumaan muutoksia. Asiakkaat tulevat olemaan entistä kiinnostuneempia vaihtoehtoisista ratkaisuista ja tästä johtuen tietoliikenneoperaattorit ovat pakotettuja kehittämään tuoteportfoliotansa tai vaihtoehtoisesti laskemaan hintoja.

Firma.fi oli yllättynyt teknologian nopeasta kehityksestä ja sen tarjoamista uusista mahdollisuuksista. Yrityksen liikevaihto on kasvanut useita kymmeniä prosentteja vuosittain ja henkilöstön määrä noin 20 prosenttia vuodessa. Tästä johtuen tietoliikenneverkolle asetetut tarpeet ja vaatimukset ovat osittain muuttuneet muun muassa vikasietoisuuden osalta. Erilaisten verkkohyökkäysten lisääntyminen ja niiden sama laaja näkyvyys mediassa on aiheuttanut yrityksessä keskustelua.

Erityisen suurta mielenkiintoa herätti kaksi seikkaa: Multi-Link-teknologia sekä sen mahdollistamat nopeat ja kahdennetut yhteydet. Ratkaisun nopea takaisin-

maksuaika oli myös positiivinen yllätys. Uuden teknologian helppo käyttöönotto nähtiin myös tärkeänä tekijänä. Vanhan ratkaisun etuna koettiin yksi ja sama tietoliikenneoperaattori ja heidän palvelualttiutensa. Firma.fi miettii vakavasti nykyisen ratkaisun korvaamista voimassa olevan sopimuskauden päättyessä.

Henkilökohtaisesti uskon tämän tyyppisten ratkaisujen yleistyvän kalliiden ja kankeiden MPLS-ratkaisujen kustannuksella. Teknologia voi olla joko Stonesoftin tai jonkun muun valmistajan vastaavaa teknologiaa, mutta suunta on varmasti kohti kustannustehokkaampia ratkaisuja. Muutoksen nopeutta kasvattaa varmasti mobiiliverkkojen suorituskyvyn kasvu. Toinen asia on sitten, kuka tämänkaltaiset ratkaisut toteuttaa. Toteuttavatko ratkaisut yritykset itse, tietoliikenneoperaattorit vai ulkoistuskumppanit? Lopputulos on kuitenkin yritysten kannalta sama eli ratkaisut kehittyvät ja hinnat laskevat.

LÄHTEET

Kirjat ja elektroniset julkaisut

Darukhanawalla, N. & Bellagamba, P. 2009. Interconnecting Data Centers Using VPLS. Indianapolis. Cisco Press.

ISP Redundancy Stonesoft Whitepaper. 2006. A Practical Guide to ISP Redundancy and Uninterrupted Internet Connectivity
Viitattu 27.1.2013. http://whitepaper.talentum.com/whitepaper /view.do;jsessionid=3eedf34b30d7d48738c79afe4d30bb5c98f8b4d815d7.e34KaNeLb3aNe3eKchmKbx8Lai0?id=4051

Kettunen, M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana.
Viitattu 27.1.2013. http://papaya.ictlab.kyamk.fi/~amake/SimuNet /SimuNet%20artikkeliv6a.pdf

Siuro, J. 2008. Opinnäyte Verkonvalvonta Stonesoftin testiverkkoon
Viitattu 27.1.2013. http://publications.theseus.fi/bitstream/handle/10024/10031 /Siuro.Jussi.pdf?sequence=2

Stonesoftin päivitetty strategia: tavoitteena vahva kasvu vuosina 2013—2014, Stonesoft Oyj Pörssitiedote 12.11.2012 klo 11.59
Viitattu 27.1.2013. http://www.stonesoft.com/en/company/press_and_media /releases/fi/2012/12112012.html

Stonesoft Management Center Architecture
Viitattu 11.3.2013. http://www.stonesoft.com/opencms/export/system /galleries/pics /technical_illustrations/Stonesoft_Architecture_1440.png

Stonesoft Management Center datasheet. 2012.
Viitattu 27.1.2013 http://www.stonesoft.com/opencms/export/system/galleries /download/datasheets/smc.pdf

Stonesoft Oyj osavuosikatsaus tammi-syyskuu 2012, Stonesoft Oyj Pörssitiedote 19.10.2012 klo 9.15
Viitattu 27.1.2013. http://www.stonesoft.com/en/company/press_and_media /releases/fi/2012/19102012.html

Stonesoft tuotehinnasto jälleenmyyjille.
Viitattu 27.1.2013. https://www.stonesoft.com/partner/pricing/pricelist_EUR /EUR-price-list-Excel-January-15th-2013.xlsx

Stonesoft Vuosikertomus 2010
Viitattu 27.1.2013. http://www.stonesoft.com/opencms/export/system/galleries /download/financial_documents/annual_reports/Stonesoft_Vuosikertomus_2010_FI.pdf

Stonesoft Vuosikertomus 2011
Viitattu 27.1.2013. http://www.stonesoft.com/opencms/export/system/galleries/download/financial_documents/annual_reports/Stonesoft_VUOSIKERTOMUS_2011_FI_web.pdf

TDC IP VPN
Viitattu 27.1.2013. http://tdc.fi/element.php?dogtag=tdcf_ratkaisut_data_ipVPN

TDC IP VPN Lisäpalvelut: Palvelutasot
Viitattu 27.1.2013. http://tdc.fi/element.php?dogtag=tdcf_ratkaisut_data_ipvpn_pt

Viestintävirasto: Tunkeutumisen havaitsemis- ja estojärjestelmät
Viitattu 27.1.2013. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/tunkeutuminen.html

Young, G & Pescatore, J. 2012. Magic Quadrant for Enterprise Network Firewalls. Gartner

Young, G & Pescatore, J. 2012. Magic Quadrant for Intrusion Prevention Systems. Gartner

Haastattelut

Firma.fi IT-manager 2012. Puhelinhaastattelu 20.12.2012.

TDC Nordic IP VPN

Palvelukuvaus ja erityisehdot

TDC Nordic IP VPN

Sisällysluettelo

1. Sopimusliitteen tarkoitus

Tämä tuotekohtainen sopimusliite käsittää TDC Oy:n (jäljempänä TDC) toimittaman TDC Nordic IP VPN –palvelun (jäljempänä palvelu) palvelukuvauksen ja siihen liittyvät erityisehdot. Tämä sopimusliite liitetään osaksi TDC:n ja asiakkaan välistä toimitussopimusta.

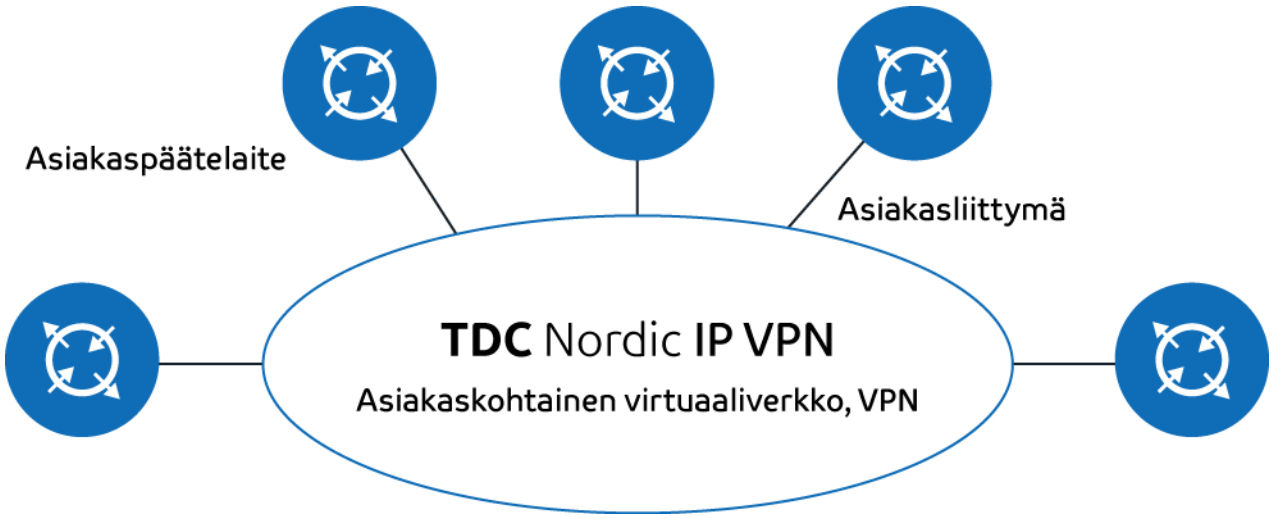
2. Palvelukuvaus

2.1 Palvelun yleiskuvaus

TDC Nordic IP VPN tarjoaa tietoverkkoratkaisun asiakkaan toimipisteiden välisen liikenteen välittämiseksi. Palvelu yhdistää asiakkaan eri toimipisteet loogiseksi kokonaisuudeksi, johon voidaan liittää muun muassa etäyhteyspalvelu, lähiverkkopalveluita, yhteyksiä palveluntarjoajien konesaleihin sekä internetpalveluita.

2.2 Palvelun toiminnallisuudet

TDC Nordic IP VPN palveluun kuuluvat seuraavat toiminnallisuudet, jotka sisältyvät palvelun kuukausihintaan.



Kuva 1: TDC Nordic IP VPN –palvelun peruskomponentit

2.2.1 Asiakaskohtainen virtuaaliverkko

Palvelussa luodaan asiakkaan käyttöön asiakaskohtainen virtuaalinen yritysverkko (Virtual Private Network, VPN) TDC:n runkoverkon sisälle. Luotu VPN-verkko toimii ”full-mesh” -reititysperiaatteella, eli jokaisesta VPN-verkkoon kytketystä toimipisteestä voi liikennöidä kaikkiin muihin samaan asiakaskohtaiseen VPN:ään liitettyihin toimipisteisiin. Asiakaan VPN-verkkoon luodaan asiakaskohtainen reititystaulukko, eikä asiakkaan verkon reititystieto tai asiakasverkossa kulkeva liikenne näy muille TDC:n runkoverkon VPN-verkoille.

Palvelu sisältää yhden asiakaskohtaisen virtuaaliverkon.

2.2.2 Toimipistekohtainen asiakasliittymä

Asiakkaan toimipisteet liitetään asiakaskohtaiseen virtuaaliverkkoon tilaajajohdolla. Tilaajajohtoon määritetään toimipistekohtainen sovittu kahdensuuntainen, symmetrinen tiedonsiirtokapasiteetti, joka yhdistää toimipisteen asiakaskohtaiseen VPN-verkkoon.

Tilaajajohto ja sille määritetty tiedonsiirtokapasiteetti muodostavat asiakasliittymän. Asiakasliittymä välittää IPv4-protokollan mukaisen liikenteen toimipisteen ja TDC:n runkoverkkoon luodun asiakaskohtaisen VPN-verkon välillä.

Asiakasliittymän kapasiteetti on mukautettavissa asiakkaan tarpeen mukaan symmetrisestä 512 kbps nopeudesta aina 1 Gbps nopeuteen asti. Erityisjärjestelyin TDC voi toteuttaa toimipistekohtaisesti liittymänopeuksia aina 10 Gbps asti. Fyysinen tilaajajohto voidaan toteuttaa metallijohtimisena -, kuituoptisena- tai radiotieyhteytenä. Toteutustapa riippuu liittymätyyppien saatavuudesta sekä asiakasliittymältä vaadittavasta kapasiteetista.

2.2.3 Asiakaspäätelaite

TDC toimittaa palvelun mukana asiakaspäätelaitteen. Asiakaspäätelaitteen merkki ja malli riippuu asiakasliittymän kapasiteetista, valituista lisäpalveluista sekä sovitusta asiakkaan liityntärajapinnasta.

Asiakaspäätelaite tarjoaa asiakkaan liityntärajapinnaksi 10/100BaseT tai 10/100/1000BaseT Ethernet -rajapinnan RJ45-liitynnällä. Erikseen sovittaessa liityntärajapinnaksi voidaan tarjota optinen 1000BASE-SX tai 1000BASE-LX/LH -liityntä joko LC- tai SC-mallin liittimellä.

Asiakkaan perustellusta pyynnöstä liittymä voidaan toimittaa myös ilman TDC:n toimittamaa asiakaspäätelaitetta. Tällöin TDC ei pysty toimittamaan kaikkia tässä palvelukuvauksessa kuvattuja valvonta-, raportointi- ja lisäpalveluja.

2.2.4 Verkko-osoitteet

Asiakasliittymän linkin IP-osoitteet allokoidaan TDC:n julkisesta osoiteavaruudesta. Verkon valvonta ja liittymien varmennus perustuu TDC:n julkisiin IP-osoitteisiin.

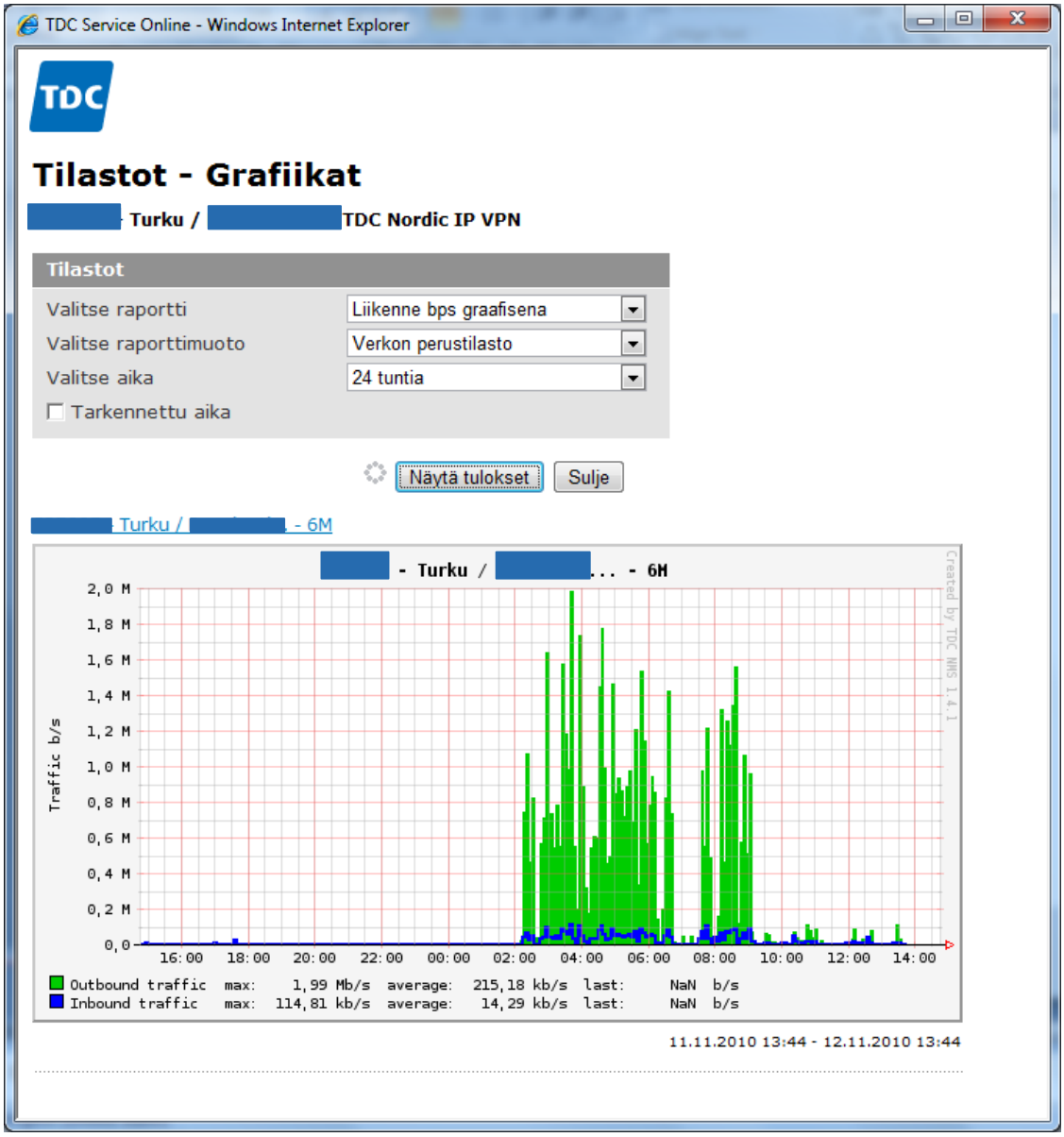
Asiakkaan toimipisteissä voidaan käyttää asiakkaan valinnan mukaan joko yksityisiä RFC 1918:n mukaisia, tai vaihtoehtoisesti joko julkisia, asiakkaalle rekisteröityjä (Provider Independent, PI) tai TDC:lle rekisteröityjä (Provider Assigned, PA) IPv4–osoitteita.

2.2.5 Raportointi

TDC tarjoaa asiakkaan yhteyshenkilön käyttöön TDC Service Online -palvelun, jonka kautta tuotetaan palvelun tila- ja liikenteen kapasiteettiraportteja. TDC Service Online tarjoaa muun muassa seuraavat raportit palveluun liittyen:

- Liikennemäärät graafisena tai numeerisena
- Liittymän käyttöaste graafisena tai numeerisena
- Palvelun käytettävyys
- Liikenteen kumulatiivinen määrä

Raportteja on mahdollista tarkastella eri aikajaksoilta kuten kuluva vuorokausi, viikko, kuukausi tai vuosi.



Kuva 2: TDC Service Online liikennemääräraportti

TDC Service Online -palvelun kautta asiakas saa myös uusimman ja ajantasaisen tuotedokumentaation sekä asiakastiedotteet. TDC Service Online palveluportaalin kautta voi myös raportoida mahdollisia vikoja sekä tilata palvelun muutostöitä.

2.3 Maksulliset lisäpalvelut

Alla mainittujen lisäpalveluiden lisäksi palveluun voidaan liittää myös muita TDC:n tarjoamia maksullisia lisäpalveluita, joista on saatavilla oma palvelukuvauksensa, kuten:

- Keskitetty internetliittymä
- Liikenteen priorisointi, QoS
- Asiakasliittymän varmennus

2.3.1 Dynaaminen reittitaulun välitys (BGP-4)

Liittymän liikenteenohjaus käyttää oletusasetuksin staattista reititystä TDC:n asiakaspäätelaitteen sekä asiakkaan toimipisteen verkkoinfrastruktuurin välillä. Kaikki toimipisteen sisäverkosta sovituilla lähdeosoitteilla saapuva liikenne välitetään asiakaskohtaiseen VPN-verkkoon ja kaikki VPN-verkosta toimipisteen sisäverkkoon saapuva liikenne välitetään asiakkaan verkkoon.

Toimipistekohtaisesti voidaan sopia asiakaskohtaisen VPN-verkon reittitaulun dynaamisesta välittämisestä asiakkaan reitittimen ja TDC:n asiakaspäätelaitteen välillä käyttäen IETF RFC 4271-standardin mukaista BGP-4 –protokollaa.

Käytettäessä dynaamista reittitaulunvälitystä asiakkaan tulee minimoida mainostamiensa reittien määrä. TDC rajoittaa toimipistekohtaisesti vastaanottamiensa reittien määrän maksimissaan 4000 reittiin toimipistettä kohti.

Dynaaminen reittitiedon välitys on maksullinen lisäpalvelu, jonka avauksesta peritään toimipistekohtainen, kertaluontoinen avausmaksu.

2.3.2 Dynaaminen IP-osoitepalvelu (DHCP Server)

Dynaaminen IP-osoitepalvelu voidaan toteuttaa TDC:n toimittamassa asiakaspäätelaitteessa käyttäen IETF RFC2131 -standardin mukaista Dynamic Host Configuration Protocol (DHCP) –yhteyskäytäntöä. IP-osoitepalvelun avulla voidaan välittää seuraavat IP-parametrit toimipisteen työasemille:

- IPv4-osoite
- aliverkkomaski
- yhdyskäytävän IPv4-osoite (default gateway)
- nimipalvelun palvelimien (DNS- palvelu) IPv4-osoitteet
- laitteen oletuksena käyttämä verkkotunnus
- aikapalvelimen IPv4-osoite
- WINS-palvelimien IPv4-osoite
- TFTP-palvelimen IPv4-osoite

Dynaaminen verkko-osoitepalvelu (DHCP Server) on maksullinen lisäpalvelu, jonka avauksesta peritään toimipistekohtainen, kertaluontoinen avausmaksu.

2.3.3 Keskitetty verkko-osoitepalvelu (DHCP Forwarding)

TDC:n toimittama asiakaspäätelaite voi reitittää toimipisteen sisäverkon DHCP-kyselyt asiakaskohtaisen VPN-verkon yli asiakkaan osoittamalle keskitetylle DHCP-palvelimelle. Asiakaspäätelaitteet tukevat IETF RFC3046 -standardin mukaista DHCP-viestien välitystoimintoa.

Dynaaminen verkko-osoitepalvelu (DHCP Forwarding) on maksullinen lisäpalvelu, jonka avauksesta peritään toimipistekohtainen, kertaluontoinen avausmaksu.

2.3.4 Asiakaspäätelaitteen lukuoikeus (SNMP Read)

Asiakas voi saada koneellisen lukuoikeuden asiakaspäätelaitteen keräämään liikenteen tilastolliseen informaatioon. Lukuoikeus toteutetaan käyttäen IETF RFC 3416 -standardin mukaista Simple Network Management Protocol (SNMP) versio 2 -yhteyskäytäntöä.

Koneellinen lukuoikeus sallitaan vain asiakkaan ennalta nimeämiltä laitteilta ja niille määritellyistä IP-osoitteista. TDC allokoi lukuun tarvittavan avaimen (community string). Perustellusta syystä voidaan käyttää myös asiakkaan allokoimia avaimia.

TDC rajoittaa asiakaspäätelaitteen lukuoikeuden koskemaan ainoastaan tiettyjä yksilöintitunnuksia (Object Identifier, OID), jotka tarjoavat liikenteen välitykseen liittyvää tilastollista informaatiota. Perustellusta syystä TDC voi antaa koneellisen lukuoikeuden myös muihin yksilöintitunnuksiin. TDC voi kuitenkin estää pääsyn näiden yksilöintitunnusten informaatioon, mikäli valittu yksilöintitunniste saattaa paljastaa vain TDC:n sisäiseen käyttöön tarkoitettua informaatiota, tai mikäli asiakaspäätelaitteen käytössä oleva käyttöjärjestelmä ei tue ehdotettua yksilöintitunnusta.

Asiakaspäätteen lukuoikeus on maksullinen lisäpalvelu, jonka avauksesta peritään toimipistekohtainen, kertaluontoinen avausmaksu.

2.3.5 Multi-VPN

Multi-VPN lisäpalvelu tarjoaa asiakkaalle useampia asiakaskohtaisia virtuaaliverkkoja (VPN). Multi-VPN lisäpalvelussa TDC ylläpitää liikenteen erottelua alkaen asiakaspäätelaitteen liityntärajapinnasta asiakasliittymien ja TDC:n runkoverkon yli aina kohdetoimipisteen asiakaspäätelaitteen liityntärajapintaan asti. Kohteena olevassa toimipisteessä liikenne ohjataan kyseiseen VPN-verkkoon liitettyyn virtuaaliseen lähiverkkoon (Virtual LAN, VLAN). Asiakaspäätelaitteessa liikenteen erottelu toteutetaan käyttäen virtuaalisia reitittimiä (VRF).

Multi-VPN on toimipistekohtainen lisäpalvelu. Saman asiakkaan eri VPN-verkkojen topologioiden ei tarvitse olla yhteneväisiä. Eri toimipisteisiin voidaan aktivoida vain siellä tarvittavat asiakaskohtaiset VPN-verkot.

Multi-VPN perustoteutuksessa kaikki toimipisteen VPN-verkot jakavat asiakasliittymän kapasiteetin. Koko asiakasliittymän kapasiteetti on yhden VPN-verkon käytettävissä, mikäli muissa VPN-verkoissa ei ole liikennettä samaan aikaan. Kun useat VPN-verkot välittävät liikennettä samanaikaisesti, kaikkea liikennettä kohdellaan tasa-arvoisesti. VPN-verkkojen yhteenlasketun liikennemäärän ylittäessä asiakasliittymän kapasiteetin, määräytyy välittämättä jäävä liikenne satunnaisesti, mikäli asiakas ei ole erikseen hankkinut käyttöönsä liikenteen priorisointia, QoS.

Vaihtoehtoisesti asiakasliittymän kapasiteetti voidaan jakaa kiinteästi eri VPN-verkkojen välillä, mikäli kyseinen toiminnallisuus on saatavissa kyseiseen toimipisteeseen. Tällöin kullekin VPN-verkolle allokoidaan asiakasliittymään kiinteä kapasiteetti eikä yhden VPN-verkon liikenne voi ylittää sille allokoitua kapasiteettia, vaikka muissa VPN-verkoissa ei kulkisi liikennettä samaan aikaan. VPN-verkoille allokoitujen kapasiteettien summa ei voi ylittää asiakasliittymän kapasiteettia.

Multi-VPN -palvelun avauksesta peritään kertaluonteinen avausmaksu sekä kuukausittain toistuva palvelumaksu. Toimipisteeseen saatavilla olevien asiakaskohtaisten VPN-verkkojen määrä vaihtelee riippuen asiakasliittymän toteutustavasta. Metallijohtimisilla yhteyksillä toteutettuihin toimipisteisiin on saatavilla enintään seitsemän (7) ja kuituoptisilla yhteyksillä toteutettuihin toimipisteisiin enintään kaksikymmentä (20) virtuaaliverkkoa.

2.3.6 Multi-VRF (Hub & Spoke)

Multi-VRF lisäpalvelulla voidaan muuttaa asiakkaan VPN-verkon topologia niin kutsutun ”hub and spoke” -mallin mukaiseksi.

Tällöin asiakkaalle voidaan luoda yksi tai useampia toimipistekohtaisia ”spoke”-asiakasverkkoja. Yhteen tai useampaan keskitettyyn toimipisteeseen luodaan niin kutsuttuja ”hub”-asiakasverkkoja. Liikenteen välitys on aktivoitu vain ”spoke” ja ”hub”-verkon välillä. Liikenteen välitys on estetty eri ”spoke”-verkkojen välillä.

Multi-VRF -palvelulla voidaan luoda asiakaskohtaisesti useita eri ”hub and spoke” -topologian mukaisia verkkoja, joiden topologioiden ei tarvitse olla yhtenevä.

Multi-VRF on maksullinen lisäpalvelu, jonka aktivoinnista peritään toimipistekohtainen avausmaksu. Toimipisteeseen saatavilla olevien ”hub” tai ”spoke”-verkkojen määrää koskevat samat asiakasliittymätyypistä johtuvat rajoitukset, jotka mainittiin kohdassa 2.3.5 Multi-VPN.

2.3.7 Raportoinnin laajennus (Extended Network Statistics)

Raportoinnin laajennus on lisäpalvelu, joka tarjoaa palveluun kiinteästi kuuluvan raportoinnin lisäksi tilastointia kahden eri toimipisteen välisen verkkoyhteyden laatuparametreistä.

Raportoinnin laajennus aktivoidaan toimipistekohtaisesti. Tilattaessa asiakkaan tulee määritellä toinen toimipiste ja mittaus. Raportointi aktivoidaan koskemaan vain näiden kahden toimipisteen välistä liikennettä. Yhdestä toimipisteestä voidaan aktivoida mittauksia yhteen tai useampaan toimipisteeseen.

Laajennettu raportointi tarjoaa seuraavat liikenneparametrit:

- Kahden toimipisteen välisen liikenteen siirtoviipe
- Kahden toimipisteen välisen liikenteen siirtoviipeen vaihtelu
- Kahden toimipisteen välisen liikenteen pakettihävikki

Raportoinnin laajennus on toimipistekohtainen lisäpalvelu, jonka aktivoinnista peritään avausmaksu sekä toimipistekohtainen, kuukausittainen palvelumaksu.

2.3.8 Tapahtumailmoitus (Incident Notification Service, INS)

Tapahtumailmoitus voidaan aktivoida asiakasliittymäkohtaisesti. TDC:n verkonvalvontajärjestelmä valvoo asiakasliittymän asiakaspäätelaitetta säännöllisesti. Järjestelmä aiheuttaa hälytyksen, mikäli asiakaspäätelaite ei vastaa kolmeen peräkkäiseen valvontaviestiin. Mikäli hälytyksen aiheuttaneessa asiakasliittymässä on tapahtumailmoitus aktivoituna, luodaan hälytyksen tapahtuessa myös vikailmoitus TDC:n pohjoismaiseen vianhallintajärjestelmään. Asiakasta informoidaan tapahtumasta myös sähköpostitse ja/tai tekstiviestillä.

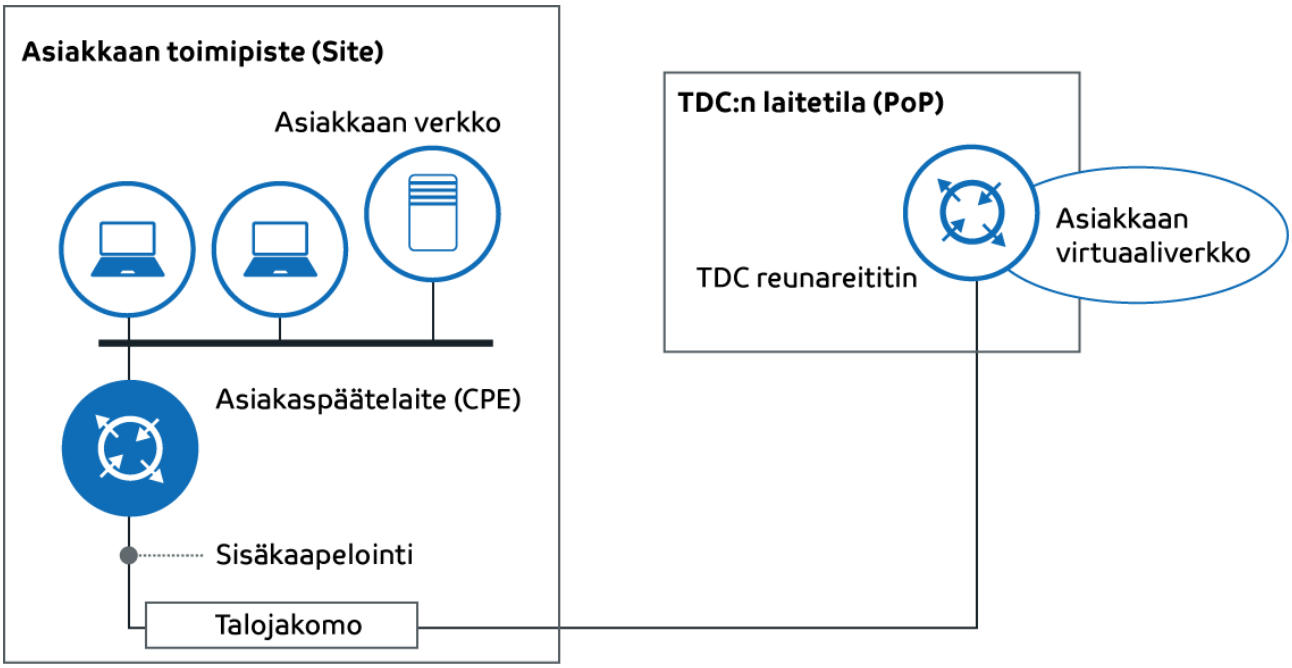
Viestin saatuaan asiakas voi olla yhteydessä TDC:n asiakaspalveluun aktivoidakseen vikailmoituksen ja viankorjauksen.

Tapahtumailmoitus on toimipistekohtainen lisäpalvelu, jonka aktivoinnista peritään avausmaksu sekä toimipistekohtainen, kuukausittainen palvelumaksu.

2.4 Palvelun tekninen kuvaus

2.4.1 Asiakasliittymän tekninen toteutus

Palvelun asiakasliittymä toteutetaan toimittamalla fyysinen tilaajajohto asiakkaan kiinteistön talojakamon ja TDC:n laitetilan välille. Talojakamosta asiakkaan tulee hoitaa sisäkaapelointi omiin tiloihinsa, jonne TDC toimittaa palveluun sisältyvän asiakaspäätelaitteen. TDC:n laitetilassa yhteys kytketään TDC:n aktiivilaitteeseen ja se välitetään sovitun kapasiteetin mukaisena loogisena yhteytenä TDC:n reunareitittimeen. TDC:n reunareitin välittää asiakkaan liikenteen yhteen tai useampaan asiakaskohtaiseen VPN-verkkoon.



Kuva 3: TDC Nordic IP VPN asiakasliittymän tekninen toteutus

2.4.2 TDC:n pohjoismainen runkoverkko

TDC Nordic IP VPN -palvelun asiakaskohtaiset VPN-verkot toteutetaan TDC:n pohjoismaisessa IETF RFC4364 -standardin mukaisessa Multi Protocol Label Switching (MPLS) runkoverkossa.

Runkoverkossa palvelun siirtokapasiteettia ei ole rajoitettu, vaan se on maksimissaan sovitun asiakasliittymänopeuden suuruinen TDC:n runkoverkosta asiakkaan toimipisteeseen ja asiakkaan toimipisteestä TDC:n runkoverkkoon. Palvelun siirtokapasiteettia ei myöskään ole rajoitettu koti- tai ulkomaiden välillä, vaan se tarjoaa optimoidut yhteydet kaikkialle TDC:n oman runkoverkon alueelle. TDC:n pohjoismainen runkoverkko koostuu yhdestä autonomisesta reititysverkosta ja se ulottuu myös yhdysliikennepisteisiin Länsi-Euroopassa ja Pohjois-Amerikassa.

TDC:n Nordic IP VPN -palvelu on laajennettavissa maailmanlaajuiseksi useiden muiden operaattoreiden kanssa toteutettujen varmennettujen yhdysliikennekäytävien kautta.

TDC:n runkoverkon aktiivilaitteet on sijoitettu laitetiloihin, jotka on suunniteltu palvelimien ja tietoliikennelaitteiden ylläpitoon. Laitetilat täyttävät korkeat tietoturva- ja käytettävyysvaatimukset. Tilat on liitetty TDC:n runkoverkkoon suurikapasiteettisilla, varmennetuilla tietoliikenneyhteyksillä. Laitetilojen aktiivilaitteiden sähkönsyöttö on varmennettu.

2.5 Ylläpito- ja valvontapalvelut

Palvelun sisältyy TDC:n pohjoismainen standard-palvelutaso. Toimipistekohtaisesta palvelutason korotuksesta voidaan sopia kirjallisesti TDC:n ja asiakkaan välillä. Asiakaspalvelu tapahtuu TDC Yritysasiakkaan käsikirjan mukaisesti.

TDC valvoo asiakaspäätelaitteita sekä asiakasliittymiä koneellisesti 24/7/365.

2.6 Hinnoittelu

Palvelusta veloitetaan kertaluontoinen toimipistekohtainen maksu (asennusmaksu) ja toistuva toimipistekohtainen palvelumaksu (kiinteä kuukausimaksu).

Yksittäisen toimipisteen laskutus alkaa kyseisen osatoimituksen valmistumispäivämäärästä.

Lisäpalveluiden hinnoittelu on kuvattu erikseen kappaleessa 2.3.

2.7 Toimitus

2.7.1 Toimitusaika

Toimipistekohtaisen asiakasliittymän arvioitu toimitusaika on noin kahdeksan (8) viikkoa sopimuksen syntymisestä. Kuituoptisella paikallisyhteydellä toteutetuilla liittymillä arvioitu toimitusaika on 12 viikkoa. Toimitusaika alkaa kulua siitä, kun asiakas on toimittanut TDC:lle kaikki toimitusta varten tarvittavat tiedot.

Mikäli yhden osatoimituksen toimitus viivästyy asiakkaasta johtuvasta syystä ja tällä on vaikutusta muiden liittymien toimittamiseen, TDC:llä on oikeus siirtää muiden osatoimitusten toimitusaikoja vastaavasti.

Toimitus tehdään normaalin työajan puitteissa, ellei asiakkaan kanssa ole kirjallisesti toisin sovittu.

2.7.2 Toimituksen edellytykset

Asiakkaan tulee ilmoittaa kaupallisen ja teknisen yhteyshenkilönsä yhteystiedot RIPE NCC -tietokantaa varten, kun palveluun otetaan käyttöön julkisia, TDC:lle rekisteröityjä IP-osoitteita.

Asiakkaan tulee osoittaa asiakaspäätelaitteelle tila, joka täyttää tässä dokumentissa kuvatut asiakaspäätelaitteen ympäristövaatimukset.

Asiakkaan tulee huolehtia sovitun tyyppisen sisäkaapeloinnin toteutuksesta asiakaspäätelaitteen sijoituspaikan ja talojakamon välillä.

TDC:llä tai sen alihankkijalla tulee olla esteetön pääsy toimipisteen talojakamoon sekä asiakaspäätelaitteen sijoituspaikalle. Talojakamon sekä asiakaspäätelaitteen sijoituspaikan tulee täyttää tässä dokumentissa kuvatut huoltotyön ympäristövaatimukset.

Toimipisteeseen tulee olla saatavilla metallijohtiminen- tai kuituoptinen tilaajajohto, jolla asiakasliittymä on tarkoituksenmukaista toteuttaa. Mikäli asiakkaan talojakamoon ei ole saatavilla tarkoituksenmukaista tilaajajohtoa, TDC voi rakentaa tilaajajohdon. Tällöin TDC:llä on oikeus periä korotettu avausmaksu. Mikäli asiakaspäätelaitteen sijoituspaikalta löytyy tarkoituksenmukainen radiopeitto, voidaan siirtotienä käyttää vaihtoehtoisesti myös radiotietä.

2.7.3 Toimituksen sisältö

Toimitus koostuu osatoimituksista. Jokainen osatoimitus koostuu asiakkaan tiettyyn toimipisteeseen toimitettavista yhteyksistä, jotka muodostavat osan asiakkaalle toimitettavasta laajemmasta VPN-verkosta.

Päätelaite, päätelaitteen vaatimat ohjelmistolisenssit, paikallisyhteys, yhteyden liittäminen asiakaskohtaiseen VPN-verkkoon TDC:n runkoverkossa, sekä sovittujen lisäpalveluiden avaaminen sisältyvät toimitukseen.

Metallijohtimin toteutettu paikallisyhteys toimitetaan asiakkaan osoittamaan puhelinrasiaan ja kuituoptinen paikallisyhteys talojakamoon.

2.8 Palvelun rajaukset

Palvelun välittää vain IPv4-protokollan mukaista unicast-liikennettä. IPv4-multicast sekä IPv6-unicast liikenteen välitys voidaan aktivoida tapauskohtaisesti erityistoimenpitein. IPv4-multicast ja IPv6-unicast liikenteen välitys hinnoitellaan tapauskohtaisesti erikseen.

TDC:lle rekisteröidyt (PA) ja asiakkaalle allokoidut julkiset IP-osoitteet ovat asiakkaan käytettävissä vain tämän palvelukuvauksen mukaisen palvelusopimuksen voimassaoloaikana. TDC:llä on oikeus ottaa osoitteet muuhun käyttöön välittömästi palvelusopimuksen päätyttyä. TDC ei tällöin vastaa asiakkaan palveluiden uudelleen määrittelystä tai siitä aiheutuneista kustannuksista. Asiakas ei voi antaa TDC:lle rekisteröityjä PA-osoitteita eteenpäin yhteistyökumppaninsa käyttöön ilman TDC:n kirjallista suostumusta.

Palvelu tukee enimmillään 4000 IP-reittitietoa asiakaskohtaista VPN-verkkoa kohti. Mikäli raja ylittyy, ei rajan ylittäviä reittejä huomioida, jolloin kyseisiin verkkoihin ei voi liikennöidä muista toimipisteistä. Tuettujen reittien määrän nostamisesta voidaan sopia kirjallisesti erikseen. Reittimäärän kasvattaminen hinnoitellaan aina tapauskohtaisesti erikseen.

2.9 Asiakkaan vastuut

Toimittaessaan palvelua asiakkaalle TDC edellyttää asiakkaan noudattavan seuraavia palvelun piirissä olevien laitteiden sijoituspaikkaa koskevia laitetilavaatimuksia (jäljempänä ympäristövaatimukset):

TDC:n määrittelemät ympäristövaatimukset laitteistolle:

- Laitetta ympäröivän ilmatilan lämpötila ei saa nousta yli +28 ºC tai laskea alle +10 ºC .
- Ilman suhteellinen kosteusprosentti ei saa ylittää 85 %.
- Laitteelle on taattava riittävä vapaa tila jäähdytykseen sekä ilmanvaihtoon.
- Laite ei saa sijaita pölyisessä tilassa tai lähellä sellaista tilaa, josta mahdollinen pöly voi kulkeutua laitteeseen.
- Laitteen päälle ei saa sijoittaa muita laitteita.
- Laitteen sähkönsyötön tulee olla maadoitettu.
- Laite ei saa sijaita tilassa, jonka läheisyydessä on vahvavirtakoneita.

Asiakkaan on huolehdittava siitä, että laitetilat täyttävät TDC:n ympäristövaatimukset 24 tuntia vuorokaudessa, koko sopimuskauden ajan.

TDC:n huolto- ja asennustyön edellyttämät ympäristövaatimukset:

- Vähintään kaksi sähköpistorasiaa (230V) huoltotöitä varten.
- Laitetilan valaistuksen on oltava riittävä huoltotyön suorittamiseksi.

Asiakkaan on huolehdittava laitteiden sijoittamisesta TDC:n ympäristövaatimusten mukaisesti. Asiakas vastaa laitteiden laitetila-, sähkö- ja ilmastointikustannuksista sekä muista laitteiden sijoituspaikkaan liittyvistä kustannuksista.

Asiakas vastaa tiloissaan tarvittavista kiinteistön sisäisistä kaapelointitöistä sekä niiden kustannuksista. Asiakas vastaa itse verkkoonsa kytkettyjen laitteidensa (esim. työasema, palvelin, kytkin, reititin tai langattoman lähiverkon tukiasema), järjestelmien ja sisäverkon tietoliikenteen tietoturvasta sekä toiminnasta kaikissa tapauksissa. Asiakas voi parantaa tietoturvaansa käyttämällä TDC:n tietoturva-palveluita.

Asiakkaan tulee huolehtia verkkosuunnittelussaan, ettei asiakaskohtainen VPN-verkon 4000 kappaleen reittitiedon määrä ylity palvelussa.

Asiakas vastaa muutostöistä ja niiden kustannuksista, mikäli asiakkaan toimipistekohtainen VPN-verkkojen määrä ylittää metallijohtimisilla asiakasyhteyksillä tuettujen VPN-verkkojen enimmäismäärän.

TDC ei lähtökohtaisesti toimita laitteita, varaosia tai ohjelmistolisenssejä ulkomaille. Mikäli palvelun toimitus edellyttää laitteiden, niiden varaosien tai ohjelmistolisenssien toimittamista ulkomaille asiakkaan nimenomaisesta vaatimuksesta, asiakas vastaa niiden tarvitsemista paikallisista viranomaismaksuista, -hyväksynnöistä sekä -luvista.

2.10 Palvelun muutokset ja lisätilaukset

Asiakaspalvelusta tilattavat muutostyöt ja lisätilaukset laskutetaan kulloinkin voimassa olevan hinnaston mukaan. Lisätilaukset ja palvelua koskevien määritysten muutokset tilataan TDC:n Yritysasiakkaan käsikirjassa esitetyllä tavalla. TDC Yritysasiakkaan käsikirja sisältää myös TDC:n asiakastuen yhteystiedot.

3. Erityisehdot

TDC:llä tai sen alihankkijalla on oikeus tarkastaa asiakkaan laitetila ennen vuokralaitteen ja asiakasliityntälaitteen toimittamista asiakkaalle sekä tarvittaessa vuokra- tai käyttöaikana.

TDC Nordic IP VPN -palvelun asiakasverkko välittää kaiken liikenteen palveluun kytkettyjen toimipisteiden välillä. TDC ei suodata asiakkaan VPN-verkon sisäistä liikennettä ilman nimenomaista kirjallista sopimusta. Tämä koskee myös tietoverkkojen tietoturvauhkien toteutumista, kuten haittaohjelmien tai ulkopuolisten palvelunestohyökkäysten aiheuttamia suuria liikennemääriä tai palveluiden estymistä. TDC ei vastaa näiden uhkien toteutumisesta asiakkaalle aiheutuneista välittömistä tai välillisistä vahingoista tai kustannuksista.

Mikäli toimitettu asiakasliittymä ei tilaajajohdon pituuden tai sen laadun takia toimi tilatulla nopeudella, TDC varaa mahdollisuuden toimittaa liittymä hitaammalla nopeudella ko. hitaampaa nopeutta vastaavalla hinnalla, tai sopia asiakkaan kanssa muusta menettelystä.

Mikäli toimipistekohtaista asiakasliittymää ei voi toteuttaa liittämällä tilaajajohto TDC:n runkoverkkoon, se voidaan toteuttaa vaihtoehtoisesti vuokraamalla tietoliikennekapasiteettia toiselta operaattorilta asiakkaan toimipisteen ja TDC:n runkoverkon välille. Mikäli kapasiteetin tarjoavalta operaattorilta ei ole saatavilla tilaajayhteydelle asiakkaan tilaamaa kapasiteettivaihtoehtoa, TDC varaa mahdollisuuden toteuttaa asiakasliittymän tilattua kapasiteettia lähinnä olevalla kapasiteetilla.

TDC toimittaa 10 Mbit/s ja sitä pienemmät kapasiteetit ensisijaisesti käyttäen metallijohtimisia tilaaja-yhteyksiä. Mikäli toimitusvaiheessa käy ilmi, ettei kohteeseen olekaan saatavilla metallijohtimista tilaaja-yhteyttä, TDC:llä on oikeus perääntyä sopimuksesta ja tarjota yhteyttä uudelleen hinnoiteltuna toteutettuna optisella tilaajayhteydellä, langattomalla laajakaistayhteydellä tai kapasiteettipohjaisena

vuokrapalveluna. Vastaavasti TDC:llä on oikeus perääntyä sopimuksesta, mikäli asiakkaan talojakamoon ei ole saatavilla asiakkaan tilaaman liittymätyypin vaatimaa tilaajajohtoa, eikä asiakas suostu maksamaan korotettua avausmaksua tilaajayhteyden rakentamisesta.

Pohjoismaiden ulkopuolelle toimitettujen kansainvälisten yhteyksien osalta TDC käyttää alihankkijoita. Mikäli alihankkija ei kykene toimittamaan sopimuksen mukaista palvelutasoa, TDC:llä on oikeus perääntyä sopimuksesta tai tarjota yhteyttä uudelleen hinnoiteltuna ja/tai alemmalla palvelutasolla.

TDC Nordic IP VPN –palvelu välittää liikenteen ilman salausta, ellei asiakkaan kanssa ole asiasta erikseen kirjallisesti sovittu. Salaamaton liikenne saattaa ylittää valtioiden maantieteelliset rajat TDC:n pohjoismaisen runkoverkon tai TDC:n kumppanin verkon alueella. Valtiot seuraavat eri tasoin sähköistä viestintää alueellaan ja salaamaton liikenne saattaa päätyä eri maiden viranomaisten tietoon.

TDC Nordic IP VPN Palvelutaso

Tuotekohtaiset erityisehdot

Tuotekohtaiset erityisehdot - TDC Nordic IP VPN Palvelutaso

Sisällysluettelo

1. Sopimusliitteen tarkoitus

Nämä TDC Nordic IP VPN –palvelun palvelutason tuotekohtaiset erityisehdot (jäljempänä myös SQA) ovat TDC Pohjoismaisen palvelutason (jäljempänä myös yleinen SLA) liite, joka sisältää TDC Nordic IP VPN –palvelun tuotekohtaiset laatuparametrit. Yhdessä nämä dokumentit muodostavat TDC Nordic IP VPN Palvelutason, joka on TDC Nordic IP VPN -palvelun maksullinen lisäpalvelu.

Tämä SQA liitetään osaksi yleistä SLA:ta, koska yleinen SLA ei sellaisenaan sisällä tuotekohtaisia laatuparametreja. Jos yleisen SLA:n ja tämän SQA:n sanamuodoissa on eroa, tämän SQA:n sanamuoto korvaa yleisen SLA:n sanamuodon TDC Nordic IP VPN Palvelutason tapauksessa. TDC Nordic IP VPN Palvelutasoon liittyviä ehtoja tulkittaessa noudatetaan seuraavaa etusijajärjestystä:

1. TDC Nordic IP VPN - palvelukuvaus ja erityisehdot
2. TDC Nordic IP VPN Palvelutaso - tuotekohtaiset erityisehdot (tämä dokumentti)
3. TDC Pohjoismainen palvelutaso - palvelukuvaus ja erityisehdot

2. Määritelmät

Asiakaspäätelaite – Asiakaspäätelaite, joka toimitetaan asiakkaalle osana palvelua.

Verkkoviive - Aika, joka tarvitaan datapaketin siirtoon palveluliitäntöjen välillä.

Jitter - Verkkoviiveen vaihtelu.

Pakettihävikki - Paketit, jotka eivät pääse perille palveluliitäntöjen välisessä pakettien siirrossa olevan siirtovirheen tai laitteiston ylikuormittumisen takia.

Hävikki – Pakettihävikki.

Paikallisyhteys – Asiakaskohtainen palveluun käytettävä tietoliikenneyhteys palveluliitännän A ja palveluliitännän B välillä.

Palvelu - Tämän SQA:n tapauksessa palvelu on TDC:n toimittama TDC Nordic IP VPN -palvelu, josta on sovittu sitovalla toimitussopimuksella.

Palveluliitäntäpiste A - TDC:n reunareitittimen tarjoama asiakasrajapinta TDC:n laitetilan ja asiakkaan toimipisteen väliseen paikallisyhteyteen. (Performance Guarantee Point A)

Palveluliitäntäpiste B - Ethernet RJ-45 tai optinen rajapinta asiakaspäätelaitteessa, jonka toimittamisesta ja hallinnasta TDC vastaa osana palvelua (Performance Guarantee Point B).

Laitetila, PoP - Point of Presence. TDC:n hallinnoima laitetila verkon solmuille, joita käytetään asiakasyhteyksien yhdistämiseen niiden edelleen siirtämiseksi TDC:n runkoverkkoon.

Reunareititin - TDC:n reunareititin (PE), joka sijaitsee PoP:ssä.

Priorisoidut liikenneluokat - TDC QoS -lisäpalvelu mahdollistaa kolme (3) priorisoitua liikenneluokkaa: puhe (voice), video ja data. Muu liikenne, joka ei kuulu mihinkään näistä luokista, luokitellaan ei-priorisoiduksi.

Runkoverkko - TDC:n siirtoverkko, joka yhdistää TDC:n laitetilat ja niihin sijoitetut aktiivilaitteet.

QoS - Quality of Service. TDC Nordic IP VPN –palvelun maksullinen lisäpalvelu (ks. kohta priorisoidut liikenneluokat).

SLA - Service Level Agreement, palvelutaso. TDC:n palvelutasosopimus muodostuu kahdesta (2) osasta: TDC Pohjoismainen palvelutaso (yleinen SLA) ja tuotekohtainen SQA, jossa kuvataan tiettyyn tuotteeseen liittyvät palvelun laatuparametrit. TDC Pohjoismainen palvelutaso ei sisällä yksin riittäviä laatuparametrejä millekään tuotteelle, vaan se yhdistetään aina SQA:han.

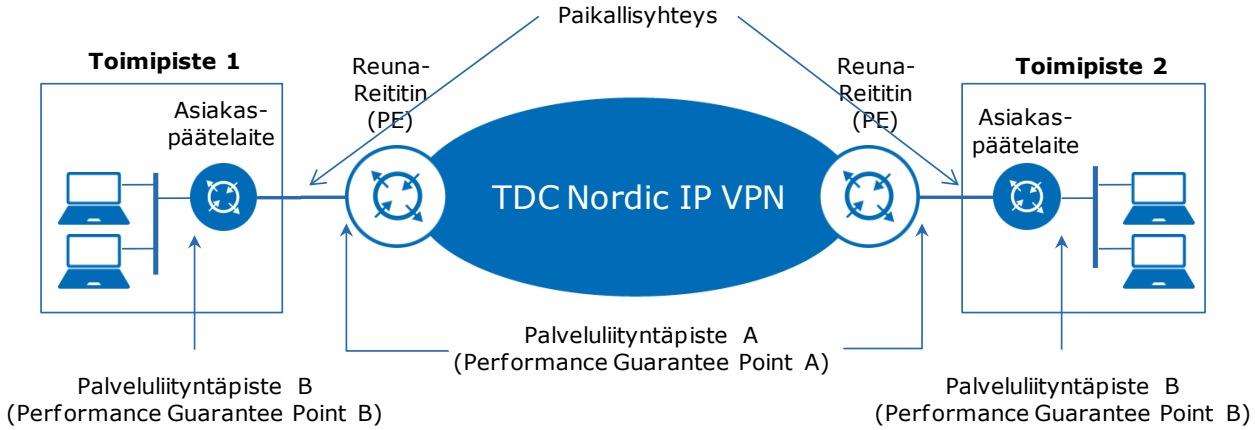
SQA - Service Quality Appendix, palvelutason tuotekohtaiset erityisehdot. SQA on osa TDC Pohjoismaista palvelutasoa.

Toimipiste - Asiakkaan kiinteistö, joka toimii myös palvelun toimitusosoitteena.

DSL - Digital Subscriber Line. Digitaalinen metallijohtimisilla tilaajayhteyksillä käytettävä tiedonsiirtotekniikka, josta käytetään erilaisia muunnelmia kuten ADSL, SHDSL ja VDSL.

2.1 TDC Nordic IP VPN Palvelutason kattavuus

TDC Nordic IP VPN Palvelutaso kattaa TDC:n hallinnoimat verkon osat palveluliitäntäpisteiden B välillä. Palvelutason kattamat verkon osat on esitetty seuraavassa kuvassa.



3. Palvelun suorituskyky

3.1. TDC Nordic IP VPN –palvelun suorituskyky

Tässä kappaleessa on kerrottu TDC Nordic IP VPN -palvelun suorituskykyä kuvaavien mittareiden raja-arvot verkkoviiveen, verkkoviiveen vaihtelun ja pakettihävikin osalta. Lisäksi määritellään tekniset edellytykset, joiden on toteuduttava, jotta annetut arvot pätevät.

Taulukossa A kappaleessa 3.1.3 ja taulukossa B kappaleessa 3.1.4 määritetään palvelun suorituskyvyn raja-arvot. Normaalin toiminnan aikana palvelun suorituskyky on vähäiselle vialle annettuja raja-arvoja parempi.

Mikäli asiakkaan mielestä palvelun suorituskyky on annettuja raja-arvoja heikompi, asiakas voi ottaa yhteyttä TDC asiakastukeen avatakseen palvelupyynnön. Tämän jälkeen TDC suorittaa verkon suorituskyvyn mittauksia tutkiakseen onko palvelussa vikaa ja onko mahdollisesti havaittu vika vähäinen vai vakava.

Mikäli vika luokitellaan vakavaksi viaksi, liittymäkohtaisena palveluaikana kulunut aika palvelupyynnön avaamishetkestä palvelupyynnön ratkaisuhetkeen tulkitaan käyttökatkokseksi. Mikäli vika luokitellaan vähäiseksi viaksi, TDC korjaa vian normaalien tapahtumanhallintaprosessiensa mukaisesti.

3.1.1. Suorituskyvyn mittaaminen

Tässä SQA:ssa annetulla verkkoviiveellä tarkoitetaan edestakaista verkkoviivettä. Edestakaisella verkkoviiveellä tarkoitetaan aikaväliä, joka kestää datapaketin siirtämiseen lähettäjältä vastaanottajalle ja toisen datapaketin siirtämiseen vastaanottajalta lähettäjälle. Verkkoviiveen vaihtelulle ja pakettihävikille annetut arvot koskevat vain yhdensuuntaista tiedonsiirtoa.

TDC Service Online –palveluportaalin kautta annetut laajennettujen raportointipalvelujen (Extended Network Statistics ja Extended Network Statistics for Quality of Service) antamat arvot ovat viitteellisiä, eikä TDC käytä niitä vianmäärityksen perusteena. TDC suorittaa erilliset kahden toimipisteen väliset päästä-päähän mittaukset silloin, kun se on välttämätöntä vian luokittelemiseksi ja vian selvittämiseksi.

Verkkoviive (edestakainen viive)

TDC Nordic IP VPN -palvelun verkkoviiveen raja-arvot on määritelty taulukoissa A ja B. Jos verkkoviive ylittää jossakin taulukossa annetun arvon, vikaluokitus tehdään kyseisten taulukoiden mukaan. Verkkoviiveen mittaukset suoritetaan kyseisen liittymän toimipistekohtaisena palveluaikana, ja viive ilmoitetaan taulukossa mainitun mittausjakson keskiarvona. Yhden suunnan viive on noin puolet edestakaisesta viiveestä.

Verkkoviiveen vaihtelu (Jitter)

TDC Nordic IP VPN -palvelun raja-arvot verkkoviiveen vaihtelulle on määritelty taulukoissa A ja B. Jos verkkoviiveen vaihtelu ylittää jossakin taulukossa annetun arvon, vikaluokitus tehdään kyseisten taulukoiden mukaan. Verkkoviiveen vaihtelun mittaukset suoritetaan priorisoiduille luokille kyseisen liittymän toimipistekohtaisena palveluaikana ja verkkoviiveen vaihtelu ilmoitetaan taulukossa mainitun mittausjakson keskiarvona.

Pakettihävikki

TDC Nordic IP VPN -palvelun pakettihävikin raja-arvot on määritelty taulukoissa Aja B. Jos hävikki ylittää jossakin taulukossa annetun arvon, vikaluokitus tehdään kyseisten taulukoiden mukaan. Pakettihävikin mittaus suoritetaan kyseisen liittymän toimipistekohtaisena palveluaikana ja hävikki ilmoitetaan taulukossa mainitun mittausjakson keskiarvona.

3.1.2. Tekniset edellytykset

Tämän SQA:n taulukoissa A ja B määritetään TDC Nordic IP VPN -palvelun suorituskyvyn raja-arvot verkkoviiveelle, verkkoviiveen vaihtelulle ja pakettihävikille kahdessa eri tilanteessa.

- Palvelun suorituskyky TDC:n runkoverkon alueella (taulukko A)
- Palvelun päästä-päähän suorituskyky kahden TDC:n hallinnoiman asiakaspäätelaitteen välillä (taulukko B)

Taulukoiden A ja B määrittelemät raja-arvot TDC Nordic IP VPN -palvelun suorituskyvylle pätevät kyseisen liittymän palveluaikana, kun seuraavat yleiset tekniset edellytykset toteutuvat:

- Yhteysnopeus ≥ 1 Mbit/s
- Keskimääräinen pakettikoko tunnin mittausjaksolla 350–1000 tavua (tietoliikenteen yleinen keskimääräinen pakettikoko)
- Liittymäkohtaisen kaistanleveyden kapasiteetista on käytössä alle 75%

Taulukossa B annettujen raja-arvojen pätemiselle on lisäksi erityisehtoja, jotka on kuvattu taulukon B yhteydessä.

3.1.3. TDC Nordic IP VPN –palvelun suorituskyky runkoverkossa

Taulukossa A annettuja raja-arvoja sovelletaan palveluihin, joissa asiakkaan liityntärajapintana on palveluliitäntäpiste A. Näissä palveluissa TDC ei toimita asiakaspäätelaitetta osana TDC Nordic IP VPN –palvelua. Tällöin palvelun suorituskyvyn mittaamiseen pätee taulukko A ja mittaukset tehdään kahden TDC:n runkoverkon reunareitittimen (palveluliitäntöjen A) välillä.

Taulukko A. TDC Nordic IP VPN -palvelun suorituskyky runkoverkossa

Liikenneluokka	Suorituskyky-parametrit	Pohjoismaissa[3]		Kunkin maan sisällä		Mittausjakso palveluaikana
		Vähäinen vika	Vakava vika	Vähäinen vika	Vakava vika	
Puhe (Voice)	Viive (ms)[1]	30	45	18	40	1 tunti
	Jitter (ms)[2]	4,5	12,5	3,5	8,5	
	Hävikki (%)[2]	0,01	0,2	0,01	0,2	
Video	Viive (ms)[1]	35	50	20	45	1 tunti
	Jitter (ms)[2]	6	17	4,5	12,5	
	Hävikki (%)[2]	0,01	0,2	0,01	0,2	
Data	Viive (ms)[1]	35	50	20	45	1 tunti
	Hävikki (%)[2]	0,01	0,2	0,01	0,2	
Ei-priorisoitu liikenne	Viive (ms)1	50	75	25	65	1 tunti
	Hävikki (%)[2]	0,05	0,5	0,05	0,5	

1) Edestakainen verkkoviive

- Ruotsin alueella verkkoviiveen raja-arvot pätevät vain yhteyksillä, joiden maantieteellinen etäisyys on enintään 900 km. Pidemmillä etäisyyksillä 10 ms lisäviive tulee lisätä taulukossa annettuihin raja-arvoihin.
- Norjan alueella annetut verkkoviiveen raja-arvot eivät ole voimassa Nordlandin, Tromsin eikä Finnmarkin läänien alueilla. Näiden läänien alueilla 10 ms lisäviive tulee lisätä taulukossa annettuihin raja-arvoihin.

2) Yhdensuuntainen raja-arvo.

3) Tanska, Ruotsi, Norja ja Suomi.

3.1.4. TDC Nordic IP VPN –palvelun päästä-päähän suorituskyky

Taulukossa B annettuja raja-arvoja sovelletaan palveluihin, joissa asiakkaan liityntärajapintana on palveluliitäntäpiste B. Näissä palveluissa TDC toimittaa ja hallinnoi asiakaspäätelaitetta osana TDC Nordic IP VPN –palvelua. Tällöin palvelun suorituskyvyn mittaamiseen pätee taulukko B ja mittaukset tehdään kahden TDC:n hallinnoiman asiakaspäätelaitteen (palveluliitäntöjen B) välillä.

Taulukko B. TDC Nordic IP VPN -palvelun suorituskyky päästä-päähän.

Liikenne-luokka	Suorituskyky-parametrit	Optinen yhteys / Leased Line				DSL				Mittaus-jakso palvelu-aikana
		Pohjois-maissa[3]		Kunkin maan sisällä		Pohjois-maissa[3]		Kunkin maan sisällä		
		Vähäinen vika	Vakava vika	Vähäinen vika	Vakava vika	Vähäinen vika	Vakava vika	Vähäinen vika	Vakava vika	
Puhe (Voice)	Viive (ms)[1]	35	55	23	50	40	70	28	65	1 tunti
	Jitter (ms)[2]	6	14	5	10	8,5	20	7	15	
	Hävikki (%)[2]	0,01	0,4	0,01	0,4	0,01	0,4	0,01	0,4	

Video	Viive (ms)[1]	40	60	25	55	45	75	30	70	1 tunti
	Jitter (ms)[2]	7,5	18,5	6	14	10	25	8,5	20	
	Hävikki (%)[2]	0,01	0,4	0,01	0,4	0,01	0,4	0,01	0,4	
Data	Viive (ms)[1]	40	60	25	55	45	75	30	70	1 tunti
	Hävikki (%)[2]	0,01	0,4	0,01	0,4	0,01	0,4	0,01	0,4	
Ei-priorisoitu	Viive (ms)1	55	85	30	75	60	100	35	90	1 tunti
	Hävikki (%)[2]	0,1	0,8	0,1	0,8	0,1	0,8	0,1	0,8	

1) Edestakainen verkkoviive

- Ruotsin alueella verkkoviiveen raja-arvot pätevät vain yhteyksillä, joiden maantieteellinen etäisyys on enintään 900 km. Pidemmillä etäisyyksillä 10 ms lisäviive tulee lisätä taulukossa annettuihin raja-arvoihin.
- Norjan alueella annetut verkkoviiveen raja-arvot eivät ole voimassa Nordlandin, Tromsin eikä Finnmarkin läänien alueilla. Näiden läänien alueilla 10 ms lisäviive tulee lisätä taulukossa annettuihin raja-arvoihin.
- Annettuja raja-arvoja sovelletaan kahden toimipisteen välillä, joista toisen paikallisyhteys on aina toteutettu optisella yhteydellä tai leased line -tekniikalla. Kahden DSL-yhteydellä toteutetun toimipisteen välillä 10 ms lisäviive tulee lisätä yllä mainittujen ehtojen lisäksi taulukossa annettuihin raja-arvoihin.
- Asymmetrisellä DSL-yhteydellä (ADSL) toteutettuihin paikallisyhteyksiin tulee taulukossa annettuihin raja-arvoihin lisätä yllä mainittujen ehtojen lisäksi 5 ms lisäviive.

2) Yhdensuuntainen raja-arvo

3) Tanska, Ruotsi, Norja ja Suomi.

Taulukon B arvot pätevät vain, jos yleisten teknisten ehtojen lisäksi myös seuraavat ehdot täyttyvät:

- TDC Nordic IP VPN -palveluun sisältyy TDC:n toimittama ja hallinnoima asiakaspäätelaite.
- Priorisoidut liikenneluokat puhe (voice), video ja data ovat käytössä vain, mikäli palveluun on liitetty ne mahdollistava TDC QoS -lisäpalvelu.
- Priorisoitu liikenne vie korkeintaan 75% yhteyden kaistanleveydestä.

Palvelun paikallisyhteytenä mahdollisesti käytettävä langaton laajakaistaratkaisu lisää palvelun viivettä ja sen vaihtelua. Mitään taulukossa B annetuista SQA-arvoista ei sovelleta palveluun, jossa liikenne välitetään langattoman laajakaistaratkaisun yli, eikä tällaiselle palvelulle anneta erillisiä suorituskykyparametreja eikä niiden raja-arvoja.

3.2. TDC Nordic IP VPN -palvelun käytettävyys

Jokaiselle asiakkaan TDC Nordic IP VPN –palvelun piirissä olevalle toimipisteelle voidaan määrittää sovellettava palvelutaso erikseen. Käytettävyys- ja käyttökatkoslaskelmat tehdään palvelu- ja toimipistekohtaisesti toimipisteelle sovitun palvelutason perusteella. Käytettävyys- ja käyttökatkoslaskelmat tehdään TDC Pohjoismaisen palvelutaso palvelukuvauksen mukaisesti. Taulukosta C käy ilmi, kuinka palvelun käytettävyys määräytyy sovitun palvelutason ja käytössä olevan laitteiston mukaisesti.

Jos TDC Nordic IP VPN –palvelun piirissä olevassa toimipisteessä on käytössä varmennettu ratkaisu, palvelun katsotaan olevan käyttämättömissä vain, jos molemmat yhteydet ovat pois käytöstä.

Taulukko C. Palvelun käytettävyys

Palvelun käytettävyys neljännesvuosittain			
	SLA-taso standard	SLA-taso premium	SLA-taso exclusive

Toimipisteessä varmentamaton palvelu	99,63 %	99,81 %	99,90 %
Korvaustaso[1]	S1	P1	E1
Toimipisteessä linkin, asiakaspäätelaitteen tai reunareitittimen varmennus[2]	99,81 %	99,86 %	99,95 %
Korvaustaso[1]	S2	P2	E2
Toimipisteessä täysin varmennettu palvelu[2]	99,86 %	99,90 %	99,99 %
Korvaustaso[1]	S3	P3	E3

1) Korvaustasot on esitetty korvauksia käsittelevän kohdan taulukossa D.

2) Nämä vaihtoehdot ovat mahdollisia silloin, kun käytössä on paremman käytettävyyden takaava varmennettu ratkaisu, eli jokin tai kaikki palvelun komponenteista (asiakaspäätelaite, paikallisyhteys, runkoverkon reunareititin) on varmennettu.

4. Kompensaatiot

Asiakas on oikeutettu korvaukseen, mikäli TDC ei pysty tarjoamaan taulukossa C määritettyä käytettävyyttä. Korvauksen määrä käy ilmi taulukosta D. Jos palvelun käytettävyys ei jonkin TDC Nordic IP VPN –palveluun liitetyn toimipisteen osalta yllä määritetylle tasolle, korvauksen määrä lasketaan sen perusteella, mitkä ovat palvelun neljännesvuosittaiset maksut kyseisessä toimipisteessä.

Neljännesvuosittaiset maksut määritetään laskemalla yhteen vikaantuneen palvelun kuukausimaksut kyseisessä toimipisteessä neljännesvuoden ajalta.

Jos TDC ei palvelun suorituskyvyn osalta pysty toteuttamaan tämän SQA:n mukaista palvelutasoa kolmen (3) perättäisen neljännesvuosijakson aikana;

- Asiakas ja TDC voivat neuvotella korkeammista raja-arvoista vakavan vian luokittelun osalta (Customized SQA),
- TDC voi selvittää, onko palvelun tuottaminen mahdollista jonkin toisen teknisen ratkaisun avulla (esim. kuituverkko), mikäli Asiakas on halukas neuvottelemaan uudesta hinnasta palvelulle.
- Mikäli Osapuolet eivät pääse sopimukseen edellä esitetyistä ratkaisuista, kummallakin Osapuolella on oikeus irtisanoa sopimus päättymään kyseessä olevan toimipisteen osalta 20 päivän irtisanomisajalla.

Taulukko D. Korvaukset

Palvelun käytettävyys	Korvauksen määrä								
	SLA-taso standard			SLA-taso premium			SLA-taso exclusive		
	S1	S2	S3	P1	P2	P3	E1	E2	E3
< 99,99 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	15 %
< 99,95 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	15 %	25 %
< 99,90 %	0 %	0 %	0 %	0 %	0 %	15 %	15 %	25 %	25 %
< 99,86 %	0 %	0 %	15 %	0 %	15 %	25 %	15 %	25 %	50 %
< 99,81 %	0 %	15 %	25 %	15 %	25 %	50 %	25 %	50 %	50 %
< 99,73 %	0 %	25 %	50 %	25 %	50 %	50 %	25 %	50 %	100 %
< 99,63 %	15 %	50 %	50 %	50 %	50 %	100 %	50 %	100 %	100 %

Magic Quadrant for Intrusion Prevention Systems

5 July 2012 ID:G00222572

Analyst(s): Greg Young, John Pescatore

VIEW SUMMARY

The network intrusion prevention system market is undergoing a period of dynamic evolution. Next-generation IPSs are available for the best protection, and first-generation IPSs are increasingly being absorbed by new next-generation firewall placements.

Market Definition/Description

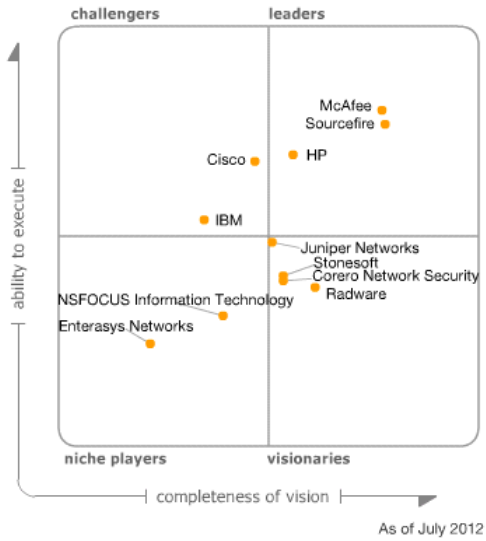
The network intrusion prevention system (IPS) appliance market is composed of stand-alone appliances that inspect all network traffic that has passed through frontline security devices, such as firewalls, Web security gateways and email security gateways. IPS devices are deployed in line and perform full-stream reassembly of network traffic. They provide detection via several methods — signatures, protocol anomaly detection, behavioral or heuristics. By being in-line, IPSs can also use various techniques to block attacks that are identified with high confidence. The capabilities of IPS products need to adapt to changing threats, and next-generation IPSs (NGIPSs) have evolved in response to advanced targeted threats evading first-generation IPSs (see "Defining Next-Generation Network Intrusion Prevention").

This Magic Quadrant focuses on the market for stand-alone IPS products; however, IPS capabilities are also delivered as functionality in other network security products. Network IPSs are also provided within a next-generation firewall (NGFW), which is the evolution of enterprise-class network firewalls to include application awareness and policy control, as well as the integration of network IPS (see "Magic Quadrant for Enterprise Network Firewalls"). IPS capability is also available in unified threat management "all in one" products used by small businesses (see "Magic Quadrant for Unified Threat Management").

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Intrusion Prevention Systems



Source: Gartner (July 2012)

Return to Top

Vendor Strengths and Cautions

Cisco

Cisco (www.cisco.com) is a very large network infrastructure vendor, with a broad network security product portfolio. Cisco has stand-alone IPS available in the 4300 (350 Mbps to 2 Gbps) and 4200 (up to 4 Gbps) Series appliances, as well as the IDS Services Module 2 switch blade when loaded with its IPS Sensor Software. Cisco also has IPS available for the Adaptive Security Appliances (ASAs) 5500-X

EVIDENCE

Gartner used these inputs for developing this Magic Quadrant:

- Results, observations and selections of IPSs, as reported via inquiries by multiple analysts with Gartner clients
- A formal survey of IPS vendors
- Formal surveys of end-user references
- Product demonstrations
- Product briefings

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance

Series firewalls (via an add-in hardware module for the 5500 Series), and software-based IPS within Internetwork Operating System (IOS)-based and Integrated Services Routers (ISRs). However, this analysis is focused on the stand-alone devices. Cisco has Web and email security gateway products as part of its security product line. The IPS Manager Express is for smaller deployments (up to 10 devices), and Cisco Security Manager (CSM) for larger or enterprise deployments.

Strengths

Enterprises already using Cisco network infrastructure or firewall products are familiar with the management and monitoring model, and can leverage a single console management for multiple Cisco products.

Cisco has wide international support, an extremely strong channel and broad geographic coverage. Enterprises that already have a significant investment in Cisco security products or that use CSM are good shortlist candidates for Cisco IPS.

Cisco IPS includes a Risk Rating feature that can be set to adjust alerts based on factors, such as the sensitivity of the asset being protected, providing context for detection and blocking. Reputation correlation services are provided by the Cisco Security Intelligence Operations (SIO).

Cisco had the largest market share for specialized IPS appliance market share in 2011, according to Gartner (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Cautions

Cisco was the vendor second-most-often listed as the product competing vendors claim to have replaced in 2011, according to our research. The most often cited reasons for Cisco IPS being replaced were signature quality and manageability.

The current Cisco IPS management consoles do not score well in shortlist competitions against most leading IPS products, and Gartner observes consistently low scores on this aspect in customer evaluations. This is less of an issue where enterprises already use Cisco security products.

Cisco IPS revenue declined 2.2% from 2010 to 2011 (again, see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011"). In our assessment, this is attributable to factors including increased pressure from NGIPS competitors, lack of focus on network security by Cisco (later addressed by an internal reorganization of the security unit), and replacement by NGFW.

Return to Top

Corero Network Security

In 2010, Corero (www.corero.com) acquired Boston-based IPS vendor Top Layer Security. Its single multigigabit-capable IPS appliance is based on Tilera 64 core processors, and is soft-licensed in 10 model sizes. Corero also has a specialized network load balancer and distributed denial of service (DDoS) and DDoS defense system (DDS) products. Corero does not have its own firewall, secure Web gateway or secure email gateway products.

Strengths

Enterprises looking for good DDoS defense capabilities within their IPS can shortlist Corero.

It has low-latency performance and focuses on protocol normalization, especially for advanced targeted threats.

Corero has high client satisfaction with pre- and postsales relationships.

Cautions

Prior to the acquisition by Corero, Top Layer Security was limited in resources and fell behind the competition. While Corero brings more resources, it does not yet have a track record in the network security space.

Virtual machine versions, content-aware data loss prevention (DLP) or reputation services were not yet available at the time of this report.

No vendor identified Corero as a top three competitive threat, and Gartner rarely sees Corero on client IPS shortlists. Corero is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Return to Top

Enterasys Networks

Headquartered in the northeast U.S., Enterasys Networks (www.enterasys.com) is a networking infrastructure company that is an arm of Siemens Enterprise Communications, with security products that include IPS, security information and event management (SIEM), and network access control (NAC). The Enterasys Intrusion Prevention System (also known as Dragon IPS) has in-line sensors that range from 100 Mbps to 10 Gbps of throughput. Enterasys also has a virtual version of the network IPS, host sensors, an event flow manager used to consolidate event information from large numbers of Enterasys sensors, and its Distributed IPS. For large or complex deployments, the Enterasys Event Flow Processor (EFP) can be used to aggregate event information and report it up to the Enterprise Management Server (EMS). Enterasys does not have its own firewall, secure Web gateway, or secure email gateway products.

Strengths

The Enterasys IPS is well-suited for internal deployments or where other Enterasys networking products are in place.

Its management features include log compression.

Customers rate its technical and overall support highly.

Cautions

Gartner continues to see the Dragon product rarely used for in-line blocking, and mostly used in

those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

IDS detect-only mode.

Gartner rarely sees Enterasys on IPS shortlists, and no vendor listed Enterasys as a competitive threat. Enterasys is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Return to Top

HP

HP (www.hp.com) is a large, global, broad-based IT and service vendor. HP has retained the TippingPoint brand name from the hardware IPS product line, also referred to as the S-series products, and has IPS blades that run in HP networking switches. The software version is the HP TippingPoint Secure Virtualization Framework. HP does not have its own secure Web gateway or secure email gateway products. HP has firewall products, but has a very small market share.

Strengths

HP has strong channel support. The TippingPoint IPS products have a broad model range of purpose-built appliances, and are known for low latency and high throughput. HP has a good strategy for IPS in virtualized environments.

Customers often cite ease of installation as a positive in product evaluations, especially for deployments with many devices. The product line includes Core Controller, which load-balances multiple appliances.

HP had the fourth-greatest market share for specialized IPS appliances in 2011, according to Gartner (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Cautions

Gartner does not believe HP has expressed a clear strategy for network security beyond IPS — in particular, details of its NGFW strategy.

Gartner believes that HP's placement of TippingPoint in its software security business unit (as opposed to in the HP Networking business unit) shows a lack of focus on the network security market.

In the Magic Quadrant survey to vendors, HP and one other company were named most often as the company they claim to have most frequently replaced.

Return to Top

IBM

IBM (www.ibm.com) is one of the largest IT hardware, software and service vendors. The former Internet Security Systems (ISS) and Proventia brands are now known as IBM Security Network Intrusion Prevention System. IPS is available in nine models of appliance within the GX Series, with inspected throughput ranging from 200 Mbps to 20 Gbps. The virtual network security platform is available in a VMware software version. IBM does not have its own firewall or secure Web gateway. During 4Q11, IBM acquired Q1 Labs, a developer of SIEM and network behavior analysis technology. IBM has implemented a reorganization that consolidates most security products into a single business unit headed by the former Q1 Labs CEO.

Strengths

IBM is benefiting from the early ISS leadership with the Protocol Analysis Module (PAM) deep inspection engine, which has more easily enabled the addition of new protocol inspection capabilities and a strong foundation for protection against emerging threats for which no signatures have yet been developed.

IBM has a wide sales and distribution network, and access to customers that already have a strong relationship with IBM. Gartner has seen increased IBM IPS buying for our clients in India.

IBM had the third-largest market share for specialized IPS appliances in 2011, according to Gartner (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Cautions

IBM ISS presence on IPS shortlists of Gartner customers has been low. Many Gartner clients do not see IBM as a strategic supplier of network security products.

In the Magic Quadrant survey to vendors, IBM and one other company were named most often as the company they claim to have most frequently replaced.

Return to Top

Juniper Networks

Juniper (www.juniper.net) is a large network infrastructure vendor with a security product portfolio that includes firewall, IPS, IPsec and Secure Sockets Layer (SSL) VPN, unified threat management (UTM), and NAC products. The Juniper Intrusion Detection and Prevention (IDP) IPS appliance line consists of four models that range from 150 Mbps to 10 Gbps throughput. The new Juniper Virtual Gateway (vGW) for VMware has IDS capabilities, but no IPS. Juniper does not have its own secure Web gateway or secure email gateway products. IPS functionality is available as part of the Juniper firewall product lines (see "Magic Quadrant for Enterprise Network Firewalls"). Security Design, as part of the new Junos Space management platform, is the new IPS management platform. The Juniper IDP IPS appliances are not based on the Junos Network OS.

Strengths

Juniper Networks' IDP supports a high number of virtual IPS instances and six third-party vulnerability assessment engines, has rate limiting, and integrates with Juniper SSL VPN products so that threat information can be linked to VPN sessions and user identity for action.

In February 2012, Juniper acquired a small Web application security company, Mykonos Software, which brought Juniper a number of skilled security researchers to enhance its threat R&D.

Juniper IPS is a good shortlist candidate for enterprises where other Juniper security or

networking equipment is in place.

Cautions

Juniper IPS has low visibility with Gartner clients, which is likely due to Juniper having focused on advancing its SRX Series integrated IPS/firewall products versus stand-alone IPS products.

During the Magic Quadrant evaluation period, Juniper appeared to focus more on broader security, as related to data center infrastructure and mobility competition, rather than on a specific network security field.

Juniper is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Return to Top

McAfee

McAfee (www.mcafee.com) had been a pure-play security vendor with a large product portfolio across network and desktop security, but is now a subsidiary of Intel, following its acquisition in 2011. The McAfee Network Security Platform (NSP) is the stand-alone IPS model line, with models that range from 100 Mbps to over 80 Gbps (via load-balanced cluster) throughput. McAfee also has IPS within the McAfee Firewall Enterprise; however, this is primarily legacy IPS from Secure Computing, and not within the scope of this Magic Quadrant. McAfee does not have a virtualized soft appliance version of the NSP IPS product.

Strengths

Its strong NGIPS capabilities that go beyond first-generation IPS, along with NSP, can make a good shortlist contender for enterprises using other McAfee security products.

It has the ability to leverage the larger threat research capabilities of its IPS threat research team.

McAfee is highly visible on Gartner client IPS shortlists, especially in government markets. McAfee was the vendor listed most often in the survey to vendors regarding their greatest IPS competitor. McAfee had the second-greatest market share for specialized IPS appliances in 2011 (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Its hardware investments in purpose-built appliances are a strength. Its IPS console scores well in competitive selections and independent tests.

Cautions

Gartner perceives the Intel acquisition has been a significant distraction for McAfee. Intel does not have a track record in network security appliance markets.

The McAfee brand is known more for desktop security offerings, and often isn't considered widely by enterprises and channel partners as a strong network security provider.

Return to Top

NSFOCUS Information Technology

Headquartered in Beijing, China, NSFOCUS (www.nsfocus.com) also has wholly owned subsidiaries in the United States and Japan. It has been selling IPS in Asia/Pacific since 2005, and also has products in the Web application firewall, anti-DDoS, and vulnerability management categories. The company has seven models ranging from 200 Mbps to 10 Gbps. NSFOCUS does not have its own firewall, secure Web gateway, or secure email gateway products.

Strengths

It had an early and strong focus on Internet Protocol version 6 (IPv6) traffic handling, and vulnerabilities specific to Asia/Pacific applications and products.

Enterprises based in China and other Asia/Pacific countries are good candidates to shortlist NSFOCUS IPS.

Gartner observes NSFOCUS IPS often is selected when cost-effectiveness is weighted highly.

Cautions

NSFOCUS is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011"). Current sales are all within Asia/Pacific.

Features seen in other IPSs, such as virtual versions, are on the NSFOCUS road map, but not currently in the product.

Many countries outside Asia/Pacific are hesitant to buy security technology from Chinese vendors, fearing interference by the Chinese government. NSFOCUS has addressed this by committing to having a U.S. application testing vendor inspect each version of its code for vulnerabilities or backdoor capabilities.

Return to Top

Radware

Headquartered in Israel, Radware (www.radware.com) is a data center infrastructure vendor offering IPS, network behavior and anomaly detection (NBAD), anti-DoS and Web Application Firewall products. The DefensePro IPS supports throughput up to 12 Gbps. Radware does not have its own firewall, secure Web gateway or secure email gateway products.

Strengths

The company's focus on R&D is evidenced with innovative features including non-signature-based detection capabilities and integration with other Radware components.

Enterprises that already have an investment in other Radware products are good shortlist candidates for Radware IPS.

Gartner clients that selected DefensePro IPS did so when additional measures versus advanced threats were weighted highly.

Cautions

Radware is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Radware visibility with Gartner clients is low, and it has limited channel support compared to most competitors in the IPS market.

Return to Top

Sourcefire

Headquartered in Maryland, pure-play security vendor Sourcefire (www.sourcefire.com) has IPS as its primary market, and is well-known for being the commercial manager for the Snort open-source security products. The Sourcefire IPS has appliance models that provide up to 40 Gbps of throughput. Virtual IPS is available for the VMware, Red Hat KVM and Xen platforms. The new FirePOWER hardware can be a transition to recently introduced NGFW capabilities for incumbent Sourcefire IPS customers.

Strengths

It has good NGIPS capabilities that go beyond first-generation IPSs.

Its new FirePOWER hardware platform scores well in client shortlists. The Sourcefire firewall and IPS share a common hardware and software platform, providing an easier migration path and means to transform a placement from IPS to NGFW or the reverse.

Its former RUA and RNA products are now included as part of the FireSIGHT management console. Its new console scores well in competitive selections and independent tests. Sourcefire is highly visible on Gartner client IPS shortlists, especially in the government market.

Sourcefire had the fifth-greatest market share for specialized IPS appliances in 2011 (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Cautions

Sourcefire may dilute its resources while trying to compete in the crowded endpoint protection market, and launch an NGFW product and compete in the IPS market at the same time.

The multiple Sourcefire brands are confusing to customers.

Return to Top

Stonesoft

Headquartered in Finland, Stonesoft (www.stonesoft.com) is a pure-play security company with NGFW, IPS and SSL VPN products. Stonesoft IPS appliances support throughput from 200 Mbps to 20 Gbps. Stonesoft IPS is available in software, a virtual edition to run on the VMware ESX Server and the appliance version. New features and updates are included as part of support and maintenance.

Strengths

Its good NGIPS capabilities go beyond first generation.

The Stonesoft firewall and IPS share a common hardware and software platform, providing a means to transform a placement from IPS to NGFW or the reverse.

Stonesoft's advanced evasion of threats research, as well as the capabilities to protect against these threats, has increased its presence on shortlists for enterprises where advanced targeted threats are of concern.

Cautions

Stonesoft is not one of the top five vendors for specialized IPS appliance market share (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011").

Stonesoft's visibility with Gartner clients is currently low for some geographies.

Return to Top

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Return to Top

Added

NSFOCUS Information Technology

Return to Top

Dropped

Check Point has focused on sales of IPS within the firewall platform.

NitroSecurity was acquired by McAfee (see "McAfee Enters the SIEM Market With NitroSecurity Acquisition").

StillSecure no longer actively markets stand-alone IPS products. It is focused on its other security

products.

Return to Top

Inclusion and Exclusion Criteria

Only products that met these criteria were included:

Meet Gartner's definition of network IPS:
- Operate as an in-line network device that runs at wire speeds
- Perform packet normalization, assembly and inspection
- Apply rules based on several methodologies to packet streams, including (at a minimum) protocol anomaly analysis, signature analysis and behavior analysis

Drop malicious sessions — they don't simply reset connections. The drop must not be a block of all subsequent user traffic.

Have achieved network IPS product sales during the past year of more than $9 million within a customer segment that is visible to Gartner, and have at least 400 devices deployed under paid support with customers.

Sell the product primarily as a stand-alone IPS.

Products and vendors were excluded if:

They are in other product classes or markets (such as network behavior assessment [NBA] products or NAC products), are not IPS, and are covered in other Gartner research.

They host IPS software on servers and workstations, rather than an in-line device on the network.

Return to Top

Evaluation Criteria

Ability to Execute

The Ability to Execute criteria (see Table 1) are:

Product service and customer satisfaction in deployments. Performance in competitive assessments and having best-in-class detection and signature quality are highly rated. Competing effectively to succeed in a variety of customer placements.

Overall business viability, including overall financial health and prospects for continuing operations.

Sales execution and pricing including dollars per Gbps, revenue, average deal size, installed base and use by managed security service providers (MSSPs).

Market responsiveness and track record. Delivering on planned new features.

Market execution, including delivering on features and performance, customer satisfaction with those features, and those features winning out over competitors in selections. Delivering products, which are low-latency and multi-Gbps, have solid internal security, behave well under attack, have high availability, and are available ports that meet demands, are rated highly. Speed of vulnerability-based signature production, signature quality and dedicating internal resources to vulnerability discovery are highly rated.

Customer experience and operations, including management experience and track record, and depth of staff experience, specifically in the security marketplace. Also important is low latency, rapid signature updates, overall low false-positive and false-negative rates, and how the product fared in attack events. Postdeployment customer satisfaction, where the IPS is actively managed, is a key criterion.

Winning in highly competitive shortlists versus other IPS vendors is highly weighted.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Source: Gartner (July 2012)

Completeness of Vision

The Completeness of Vision criteria (see Table 2) are:

Market understanding and strategy. This includes providing the correct blend of detection and blocking technologies that meet and are ahead of the requirements for IPS. Innovation, forecasting customer requirements, having a vulnerability rather than exploit product focus, being ahead of competitors on new features and integration with other security solutions are highly rated. Also included is understanding and commitment to the security market and, more specifically, the network security market. Vendors that rely on third-party sources for signatures or have weak or "shortcut" detection technologies score lower.

Sales strategy includes pre- and postproduct support, value for pricing, and providing clear explanations and recommendations for detection events.

Offering strategy, with emphasis on product road map, signature quality, NGFW integration and performance. Successfully completing third-party testing, such as the NSS Group IPS tests and Common Criteria evaluations, are important. Vendors that reissue signatures, are over-reliant on behavioral detection and are slow to issue quality signatures do not score well.

The business model includes the process and success rate for developing new features and innovation, and R&D spending.

Vertical, industry and geographic strategy includes the ability and commitment to service geographies and vertical markets (for example, MSSP and the financial sector).

Innovation, including R&D, and quality differentiators, such as performance, management interface and clarity of reporting. Features that are aligned with the realities of network operators, such as those that reduce "gray lists" (for example, reputation and correlation) are rated important. The road map should include moving IPS into new placement points and better-performing devices. NGIPS features are highly weighted.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Low
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Standard

Source: Gartner (July 2012)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain Leaders, vendors must demonstrate a track record of delivering successfully in enterprise IPS deployments and in winning competitive assessments. Leaders produce products that embody NGIPS capabilities, provide high signature quality and low latency, are innovating with or ahead of customer challenges (such as using endpoint intelligence to make more-efficient detections) and have a range of models. Leaders continually win selections and are consistently visible on enterprise shortlists. However, a leading vendor is not a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant.

Return to Top

Challengers

Challengers have products that address the typical needs of the market, with strong sales, large market share, visibility and clout that add up to higher execution than Niche Players. Challengers often succeed in established customer bases, but do not yet fare well in competitive selections or do not have robust NGIPS capabilities.

Return to Top

Visionaries

Visionaries invest in leading-/"bleeding"-edge features that will be significant in next-generation products, and that give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, especially new NGIPS or novel anti-threat capabilities, but they lack the execution skills to outmaneuver Challengers and Leaders.

Return to Top

Niche Players

Niche Players offer viable solutions that meet the needs of some buyers, such as those in a particular geography or vertical market. Niche Players are less likely to appear on shortlists, but they fare well when given the right opportunities. Although they generally lack the clout to change the course of the market, they should not be regarded as merely following the Leaders. Niche Players may address subsets of the overall market (for example, the small and midsize business [SMB] segment or a vertical market), and they often do so more efficiently than Leaders. Niche Players frequently are smaller enterprises, produce only software appliances and/or do not yet have the resources to meet all enterprise requirements.

Return to Top

Context

Current users of network IPSs highly prioritize next-generation network IPS capabilities at refresh time.

Current users of NGFWs look at a next-generation network IPS as an additional defense layer.

Enterprises evaluating network IPS and firewall offerings for deployment in 2012 or later should develop migration strategies to products that can identify and mitigate advanced threats.

Return to Top

Market Overview

According to Gartner market research, the worldwide IPS market in 2011 for stand-alone appliances grew approximately 4.7% to $1.19 billion, whereas, overall, the network security equipment market grew by 6.3% (see "Market Share: Enterprise Network Security Equipment and Routers, Worldwide, 2011"). Data collected from vendors for this Magic Quadrant (independently from the market report we have cited) validates this range. This is below our previous estimates. Factors driving those estimates:

- The threat landscape is currently aggressive, but major IPS vendors were slow to address botnet and advanced target threats. Some spending that would have gone to IPS products went to advanced threat detection and network forensics products (see "Network Security Monitoring for Lean Forward Organizations").
- NGFWs are starting to impact the stand-alone IPS market as less innovative first-generation IPSs are absorbed into firewall refreshes, becoming part of NGFWs.
- As market penetration advances, growth as a percentage will flatten.

Considering these factors, Gartner forecasts that the end-user total spending for the 2012 IPS market will grow by approximately 4% over 2011, with a compound annual growth rate (CAGR) for 2011 through 2016 of 2.5%.

NGIPS Is Here

IPS has had two primary performance drivers — the handling of the network traffic at near wire speeds, and the deep inspection of the traffic based on the signatures, rules and policy. The first generation of IPS was effectively a binary operation of "threat or no threat" based on signatures of known vulnerabilities. Rate-shaping and quality of service (QoS) were some of the first aspects that brought context to otherwise single-event views. As inspection depth has increased, digging deeper into the same silo of the traffic yields fewer benefits. This next generation of IPS does apply fuller stack inspection, but also applies new sources of intelligence to existing techniques:

- Correlation — Relating events to one another, internal and external to the IPS
- Context — Bringing information to bear to better understand the observations
- Content — Classifying executables

These advances are discussed in detail in "Defining Next-Generation Network Intrusion Prevention." Best-of-breed NGIPS is still found in stand-alone appliances, rather than NGFW. However, the gap is closing as NGFW IPS quality increases rapidly, and IPS vendors move to introduce NGFW.

More IPS Gets Absorbed by NGFW; However, the Stand-Alone IPS Market Will Persist

With the improvement in availability and quality of the IPS within NGFW, NGFW adoption reduces the need for network IPS in many enterprises. However, the stand-alone IPS market will persist to serve several scenarios:

1. The incumbent firewall does not offer a viable NGFW option.
2. Separation of the firewall and IPS is desired for organizational or operational reasons.
3. A best-of-breed IPS is desired, meaning a stand-alone NGIPS is required.
4. Niche designs for a placement where IPS is desired, but without a firewall.

Strategic Planning Assumptions

- Less than 10% of Internet connections today are secured using NGFWs. By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.
- Today, 60% of enterprises have some stand-alone network IPS deployed. By year-end 2016, this will decline to 45% due to increased adoption of NGFW.

Return to Top

G00219235

Magic Quadrant for Enterprise Network Firewalls

Published: 14 December 2011

Analyst(s): Greg Young, John Pescatore

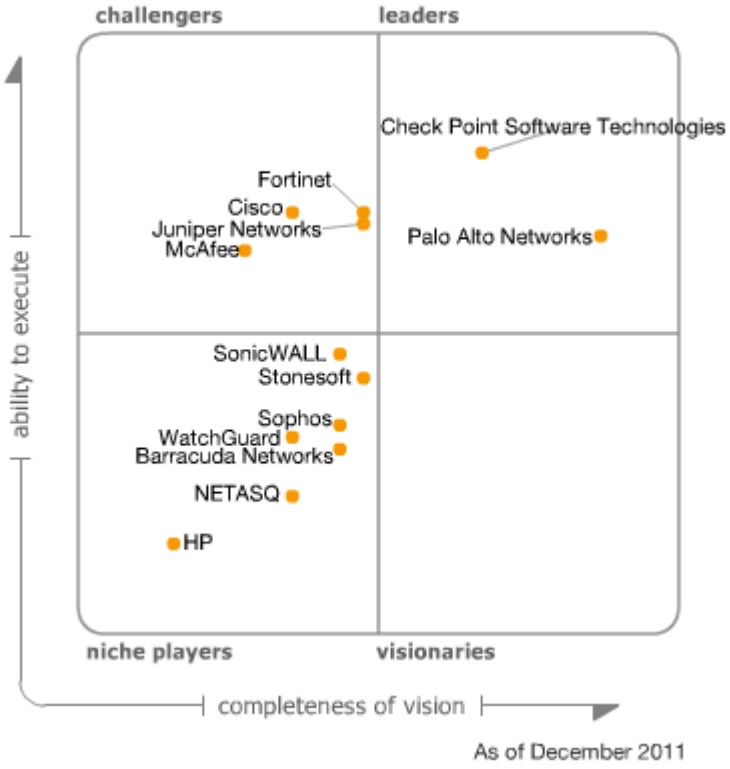
The enterprise network firewall market is undergoing a period dynamic evolution, as effective next-generation firewalls are now increasingly necessary. Vendors that have addressed advanced targeted threats have seen gains in the market.

What You Need to Know

The enterprise firewall market is one of the largest and most mature security markets. It is populated with both mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization and use of the cloud, have increased demand for new firewall features and capabilities. Organizations' final product selection decisions must be driven by their specific requirements, especially in the relative importance of management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, and integration with the established security and network infrastructure.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (December 2011)

Market Overview

Firewalls are generally the first line of defense between untrusted networks (such as the Internet or connections to business partners). They limit the attack aperture for vulnerable PCs, servers and other infrastructure elements. Firewalls long ago became a "check the box" requirement in most compliance regimes for securing trust boundaries. Throughout the years, firewalls have continued to evolve to add deeper and more flexible inspection and enforcement capabilities as threats advanced, and to run at faster and faster throughput rates as network speeds increased.

In 2010 and 2011, Gartner saw market pressures accelerate the demand and available offerings for next-generation firewall (NGFW) platforms (see "Defining the Next-Generation Firewall") that provide the capability to detect and block sophisticated attacks, as well as enforce granular security policy at the application (versus port and protocol) level. As enterprises increase the use of Web-based applications — with more complex connections within applications, more complex data centers and more data being presented to customers — firewalls have had to keep up with features and performance to meet these changing needs. Gartner also saw increased enterprise demands for

aggregate throughput rates of 5Gbps and higher, as well as demand for the ability to partition higher-capacity firewall platforms into multiple virtual firewalls.

Gartner also observed an acceleration of the trend for large distributed businesses moving away from backhauling or "home running" all branch-office Internet connectivity back through the headquarters firewall and toward allowing direct branch-office connectivity to the Internet for user Web surfing and the like. The majority of enterprises still look to their primary firewall vendors to provide the branch-office devices. With few exceptions, a single brand of firewall vendor is the best practice (see "Q&A: Is It More Secure to Use Firewalls From Two Different Vendors?"). However, many enterprises are moving their Web security gateway tier to cloud-based or as-a-service delivery to deal with mobile employee Web use, and are finding that this is also a very attractive approach for providing low-cost secure Web access to branch offices without requiring customer premises equipment. For simple branch offices, this enables the branch's point-of-presence router to be used for connectivity back to headquarters and the Internet without an additional firewall product.

Branch office firewalls and small or midsize business (SMB) firewalls continue to diverge as increasingly distinct products, along with relatively simple management tools to deploy and operate them (see "Magic Quadrant for Unified Threat Management"). In that midsize market, Gartner sees managed security service providers (MSSPs) as having increased influence over firewall and intrusion prevention system (IPS) product selection, as small businesses limit their hiring of expensive security personnel.

Acquisitions and initial public offerings were limited in 2010 and 2011 to the purchase of Astaro by Sophos (see "Astaro Acquisition Will Extend Sophos' Midmarket Security Offerings"). McAfee, which had acquired Secure Computing, was acquired by Intel, and SonicWALL was acquired by Thoma Bravo, an investment firm that owns several other security companies, such as Entrust and Tripwire. IBM ceased production of its Proventia product, but stated that it will enter the NGFW market at some point in the future. Sourcefire also announced plans to add NGFW capabilities to its product line, which had previously been dominated by IPS offerings. Gartner believes that 2012 will bring some additional acquisition activity, as larger vendors that are trying to compete in the network infrastructure markets against Cisco look to add network security products to their portfolios.

The firewall market remains a large market, with firewall/VPN revenue of approximately $5.9 billion in 2010, an approximate 10% increase over the $5.4 billion of 2009. Gartner estimates that total 2011 firewall revenue will be approximately $6.3 billion. Most firewall vendors saw strong revenue growth over this period, as delayed firewall refresh from previous pent-up demand, and increased use of video and social networking drove up network bandwidth demands. As NGFW capabilities have dominated feature comparisons (as shown by Palo Alto Networks' rapid growth), price pressure has been reduced to some degree. However, the trends we identified last year of cloud and virtualization still continue to impact the market. Gartner saw increased demand for software-only versions of firewalls for use inside virtualized data centers, but most of this demand was directed toward incumbent firewall vendors. We do not see openings for virtual-only firewall vendors.

As NGFW products become more widely used, focus will shift toward manageability and scalability — until the next threat wave. 2012 will be the year most mainstream firewall vendors catch up to the smaller innovative vendors in feature count. The innovative vendors must show that they have the same management tools, as well as third-party ecosystem support and scale, as the larger vendors. Enterprises should continue to focus on threat-facing capabilities, throughput and manageability as key evaluation criteria for firewalls, with technical criteria typically weighted two times to three times cost criteria.

Firewall policy management (FPM) products (see Note 1) are a distinct, adjacent market. Gartner recommends FPM tools be considered where the complexity of the environment exceeds the firewall console capability, where the firewall rule base is exceptionally large or dynamic, where there is more than one brand of firewall in use, if a complex transition to another brand of firewall is planned, or if workflow tools are required as part of firewall rule management.

The Strategic Planning Assumptions for the enterprise firewall market are:

- Virtualized versions of enterprise network safeguards will not exceed 2% of the market through 2012, or 20% through 2016.
- Through 2015, more than 75% of enterprises will continue to seek security from a vendor different from their infrastructure vendor.
- Less than 5% of Internet connections today are secured using NGFWs. By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built appliances for securing corporate networks. Products must be able to support single enterprise firewall deployments and large deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles and products.

As the firewall market evolves from stateful firewalls to NGFWs, other security functions (such as network IPSs) and full-stack inspection, including applications, will also be provided within an NGFW. The NGFW market will eventually subsume the majority of the stand-alone network IPS appliance market at the enterprise edge. This will not be immediate, however, because many enterprise firewall vendors have IPSs within their firewall products that are competitive with stand-alone IPS appliances, and are resisting truly integrating the functions and instead colocate them within the appliance. Although firewall/VPN and IPS are converging (and sometimes URL filtering), other security products are not. All-in-one or unified threat management (UTM) products are suitable for SMBs but *not* for the enterprise: Gartner forecasts that this separation will continue until at least 2015. Branch office firewalls are becoming specialized products, diverging from the SMB products.

As part of increasing the effectiveness and efficiency of firewalls, firewalls will need to add more blocking capability as part of the base product, to go beyond port/protocol identification and to move toward a service view of traffic.

Gartner has successively increased the Magic Quadrant evaluation weighting for NGFW features. This edition reflects a significant increase in the weighting of NGFW capabilities reflecting the changing markets and enterprise needs.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet the market definition and description were considered for this report under the following conditions:

- Gartner analysts assess that the company has an ability to effectively compete in the enterprise firewall market.
- Gartner clients generate inquiries about the company.
- The company regularly appears on shortlists for selection and purchases.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than $10 million and within a customer segment that is visible to Gartner.

Exclusion Criteria

Network firewall companies that were not included in this report may have been excluded for one or more of the following conditions:

- The company did not meet the inclusion criteria.
- The company has minimal or negligible apparent market share among Gartner clients, or is not actively shipping products.
- The company is not the original manufacturer of the firewall product. That includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and Internet service providers (ISPs) that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and do not rate platform providers separately.
- The company's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs, such as UTM firewalls or those for small office/home office placements, are not targeted at the market this Magic Quadrant covers (enterprise) and are excluded.
- The company has primarily a network IPS with a non-enterprise-class firewall.

- The company has personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls — all of which are distinctly separate markets.

Stand-alone network IPS appliances are a distinct market and are covered in Gartner's Magic Quadrant for Network Intrusion Prevention Systems.

Added

No vendors were added.

Dropped

No vendors were dropped; however, name changes did occur. The 3Com/H3C entry has been renamed to HP. Astaro has been renamed to Sophos, and phion has been renamed to Barracuda Networks, to represent the acquiring companies. Gartner examined several vendors that did not meet the inclusion criteria, or were nonresponsive and did not have any significant visibility within the market. Sourcefire was not shipping a firewall at the time of the analysis of this report.

Evaluation Criteria

Ability to Execute

- *Product or service:* This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continuously deployed in enterprises, and the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a company's ability to execute. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is foremost over revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and being able to support complex deployments and modern demilitarized zones. Having a low rate of vulnerabilities in the firewall is important. Logistical capabilities for managing appliance delivery, product service and port density matters. Support is rated on quality, breadth and value of offerings through the specific lens of enterprise needs.
- *Overall viability:* Overall business viability includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security market. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (which is compared to Gartner data on such competitions held by our customers), and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Instead, we consider use of

these firewalls to protect the key business systems of enterprise clients and presence on competitive shortlists.

- *Sales execution/pricing:* We evaluate the company's pricing, deal size, installed base and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. Pre- and post-sales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, including the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains. Cost of ownership over a typical firewall life cycle (three to five years) was assessed, as was the pricing model for (1) conducting a refresh while staying with the same product and (2) replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.
- *Market responsiveness and track record:* This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in the firewall market and how enterprises deploy network security.
- *Market execution:* Competitive visibility is a key factor, including which vendors are most commonly considered top competitive solutions, during the RFP and selection process, and which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking looks at which vendors consider each other to be direct competitive threats, such as driving the market on innovative features copackaged within the firewall, or offering innovative pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and the inability of a product to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.
- *Customer experience and operations:* This includes management experience and track record, as well as the depth of staff experience specifically in the security marketplace. The greatest factor in this category is customer satisfaction throughout the sales and product life cycle. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	Standard
Operations	Standard

Source: Gartner (December 2011)

Completeness of Vision

- *Market understanding and strategy:* This includes providing a track record of delivering on innovation that precedes customer demand rather than an "us too" road map. We also evaluate the vendor's overall understanding and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning road maps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put a plan in place, show that they are following their plan and modify their plan as they forecast the market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive road map and delivery of NGFW is weighted very highly. The NGFW capabilities are expected to be integrated both to achieve improved correlation and functional improvement.
- *Sales strategy:* Sales strategy includes pre- and post-product support, value for pricing, and providing clear explanations and recommendations for detection events. Building loyalty through credibility with full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and to do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.
- *Offering strategy:* This criterion focuses on a vendor's product road map, current features, NGFW integration, virtualization and performance. Credible independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integrating with other security components is also weighted, as well as product integration into

other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office. Innovation such as introducing practical new forms of intelligence that the firewall can apply policy to are highly rated.

- *Business model:* This includes the process and success rate for developing new features and innovation, and R&D spending.
- *Vertical, industry and geographic strategy:* This includes the ability and commitment to service geographies and vertical markets, such as complex enterprise international deployments, MSSPs, carriers or governments.
- *Innovation:* This includes R&D and quality differentiators, such as:
  - Performance, which includes low latency, new firewall mechanisms and achieving high IPS throughput and low appliance latency
  - Firewall virtualization and securing virtualized environments
  - Integration with other security products
  - Management interface and clarity of reporting — the more a product mirrors the workflow of the enterprise operation scenario, the better the vision
  - "Gives back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity

Products that are not intuitive in deployments or operations are difficult to configure or have limited reporting, and they are scored accordingly.

The more a product mirrors the workflow of the enterprise operation scenario, the better the vision. Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner (December 2011)

Leaders

The Leaders quadrant contains a mix of large and midsize vendors, with the common element of making products that are built for enterprise requirements. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rules/policy minimization. An NGFW capability is an important element as enterprises move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safeguarding features, providing expert capability, rather than treating the firewall as a commodity, and having a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss and options for hardware acceleration.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not leading with features. Many Challengers are slow to work toward or do not plan for an NGFW capability, or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challenger products are often well-priced and, because of their strength in execution, vendors can offer economic security product bundles that others cannot. Many Challengers hold themselves back from becoming leaders because they are obligated to place security or firewall products as a lower priority in their overall product sets. Firewall market challengers will often have significant market share but trail smaller market share leaders in the release of features.

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with leaders and challengers. Most visionary products have a good NGFW capability but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations willing to update products more frequently and switch vendors if required. Where firewalling is a competitive element for an enterprise, visionary vendors are good shortlist candidates. There are no Visionaries in this edition. Vendors that did not have NGFW capabilities are adding them in a defensive move, while those with strong NGFW offerings focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better identification of malicious protocols at multi-Gbps rates.

Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls, makers of multifunction firewalls for SMBs, or branch-office-only product makers attempting to break into the enterprise market. Many Niche Players are making larger SMB products, with the mistaken hope that this will satisfy enterprises. Some enterprises that have the firewall needs of an SMB (for example, some Type C "risk-averse" enterprises) may consider niche products, although other models from Leaders and Challengers may be more suited. If local geographic support is a critical factor, then Niche Players can be shortlisted.

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks (www.barracudanetworks.com) acquired European firewall vendor phion in 2009. Barracuda has been primarily focused on selling to the low end of the midsize enterprise market at very aggressive price points. The former phion firewall is now branded as the Barracuda NG Firewall family across a range of appliances and a virtual version. Barracuda is assessed as a Niche Player for enterprises, mostly because it serves a set of placements well, usually in portions of EMEA or when the Leaders are otherwise not welcome. We do not see the Barracuda NG Firewall frequently displacing Leaders otherwise.

Strengths

- The Barracuda NG Firewall is a good option for Barracuda customers who want to get a firewall product from the same vendor, especially those organizations that are outgrowing their current UTM and/or moving into point products.
- The Barracuda NG Firewall unit support staff offer good local language support, especially in Germany, Switzerland and Austria.
- Often, users comment that VPN tunnel setup was very easy and that they like the central management features.

Cautions

- Barracuda customers are primarily SMBs that do not yet have well-established enterprise network security channels.
- No vendor we surveyed listed Barracuda as a significant enterprise competitive threat.
- Barracuda has not been seen competing in the NGFW shortlists of Gartner customers because of low visibility outside Europe.
- Some users have commented that the initial setup can be more complex than needed, and that the availability of training is limited when compared with competitors.

Check Point Software Technologies

Check Point Software Technologies (see www.checkpoint.com) is a well-known, pure-play security company with the second largest firewall installed base (when support is included), and strong and broad channel support. Check Point has continued to expand its software "blade" strategy (that is, preloaded software modules enabled through subscription keys), as introduced in version R70. Check Point has recently undertaken a period of considerable product feature enhancement, and has introduced new blades and new performance levels. Gartner views this as a response to the significant threat posed by Palo Alto Networks. The indirect result of this R&D by Check Point has been significantly increased competitiveness versus other firewall competitors, such as Cisco and Juniper Networks.

The majority of enterprises choose to use Check Point-branded appliances, although options are also available for a software install on self-sourced servers, a virtual machine install (Secure Gateway Virtual Edition [VE]), or the remaining partners, such as Crossbeam. Check Point firewalls are essentially divided into three classes listed in increasing performance: UTM-1 for SMB or branch, the IP line legacy from the Nokia acquisition, and the high-end Power-1 appliance line. Check Point has not yet blended the IPSO and SmartCenter on Secure Platform OSs into a single OS under the announced Project Gaia. With the Direct Support option, customers can now receive all support directly from the company. Check Point is assessed as a leader for enterprises, because we continuously see the vendor competing and winning in demanding selections, following an NGFW development path that customers are asking for, and displacing competitors based on its features and channel strength.

Strengths

- Check Point scored high as a significant enterprise competitive threat by all vendors Gartner surveyed.
- Check Point firewall management capabilities are valued highly by customers with a large number of firewalls with differing configurations. Check Point firewalls are most often seen in large and complex networks because of the capabilities of the SmartCenter management platform. Check Point usually scores the highest in console quality for selections that Gartner observes. Check Point has invested and continues to invest considerable intellectual property into the management console, in recognition of the importance configuration has to

administrators in enterprise deployments. Provider-1 users we surveyed generally report a high level of satisfaction. Gartner sees premium-support-level customers, especially at the Diamond level, renewing their support at those same levels in recognition of the customized and easy access to support.

- Check Point has a strong field of product options, such as VSX for virtualized firewalling, VE for running in virtualized environments, and its Eventia correlation product. SecurePlatform allows for a loading of the firewall, along with a hardened OS onto off-the-shelf server hardware. The wide availability of appliance and software options enables Check Point to meet the requirements for complex enterprise networks. Blade pricing has been priced less when compared with stand-alone or point solutions, especially IPS. The R75 release had a significant number of features and improvements, which increased competitive pressure significantly across the firewall market. Check Point has raised the quality of the IPS in the product significantly over that of SmartDefense and IPS-1, and performed favorably on third-party IPS testing by NSS Labs.
- Check Point has good capability for servicing large enterprises with the combination of its Power-1 appliance line, having a VMware-certified version (VPN-1 VE) and VPN-1 UTM running in a container on ESX.
- Check Point has the strongest third-party ecosystem of security products that integrate easily with Check Point's management platform.

Cautions

- High price is a common reason provided by Gartner customers for replacing or considering replacing Check Point firewalls. This is not an issue where a premium firewall function is required and justifies the investment. In firewall selections and support renewals, Gartner often hears that support pricing is complex, and price negotiations are difficult.
- The Check Point Software Blade architecture has short-term attractiveness, but is a difficult long-term strategy option for enterprises. Enterprises are cautious about adding new functions to firewalls. With more than 13 blades now available, charging for features that are included by competitors is challenging. The Check Point 3D Security messaging is too abstract and does not align with or resonate with the firewall-buying market.
- The vendor remains challenged in producing competitive network security products outside the firewall market.
- Project Gaia has not yet been delivered (it is in beta with selected customers), meaning many clients must maintain two Check Point OSs and the associated complexity in licensing. Provider-1, which is popular with larger customers, has not been notably advanced or marketed.

Cisco

Cisco (see www.cisco.com) has an exceptionally broad network security product portfolio. It has strong product offerings across the network security, Web security and email security tiers.

Although not outwardly visible to most customers, Cisco is going through a period of significant change in its firewall offerings. Cisco has continued to consolidate its security products into a single business unit, and Gartner believes Cisco has had a significant effort under way to develop an NGFW product (and accompanying appliances) as a successor to the Adaptive Security Appliance (ASA) firewall. Gartner believes that Cisco is in a strong position to launch data-center-specific security offerings, should Cisco choose to make this a key strategy. Cisco firewalls have not seen any noteworthy changes this year. An exception is that Cisco introduced new high-end models this year, including the 5585-X, which has been well-accepted by incumbent Cisco firewall users. Cisco is assessed as a Challenger for enterprises over the evaluation period, because we did not see it frequently displacing Leaders based on vision or feature, and it does not compete in the NGFW field. Instead, Cisco mostly wins competitive procurements through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not highly weighted evaluation criteria. ASA is available in four editions, which clearly define what safeguards are being purchased.

Strengths

- Cisco has significant market share in security (including having the largest market share for firewall appliances), has wide geographic support and is viewed as a significant (second-highest) enterprise competitive threat by the vendors we surveyed.
- Gartner clients consistently rate the Cisco support network as excellent, and the most often cited reason for selecting or staying with Cisco security products. The vendor has strong channels, broad geographic support and the availability of other security products.
- Its ASA has the option to add an IPS module (AIP-SSM) to replace a stand-alone IPS.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, with firewalls also available via the Firewall Services Module blade for Catalyst switches, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router.
- The integration of reputation features across Cisco security products is a highly significant feature differentiator that is often missed in enterprise selections. Although many companies have reputation features, the breadth of the reputation feed is a critical quality factor.

Cautions

- Cisco firewall products are selected more often when security offerings are added to Cisco's infrastructure, rather than when there is a shortlist with competing firewall appliances. Cisco was listed by competitors as the product they most often replace.
- Where Cisco firewalls were shortlisted, but not selected, the difficulty of using the management console, Cisco Security Manager (CSM), for basic configuration and management was consistently the factor most often cited.
- The requirement to add a hardware module (the AIP-SSM) to add IPS capability to the ASA firewall appliance remains a barrier to deployment and a competitive disadvantage for branch-office deployments. The add-in module does, however, provide processing help with the deep

inspection load. If the SSM module is used for IPS, then it cannot be used for other content inspection.

- The ASA line is becoming somewhat dated, although Gartner expects Cisco to ship new models and software in 2012.

Fortinet

California-based Fortinet (see www.fortinet.com) has long focused on using purpose-built hardware to produce UTM appliances at strong price/performance points. Although the firewall features in its UTM products met most of the needs of firewall-focused large enterprise buyers, Fortinet's approach and philosophy continue to be focused on "everything in one box," which has caused its brand and channel support to be slow to evolve from its SMB base. However, Fortinet continues to make progress within the Gartner customer base, usually by expanding out from branch-office or retail deployments, and is seen winning some data center implementations. Fortinet is a significant threat to competitors in this market because of the company's hardware expertise, competitive pricing and steady revenue growth. Fortinet is a viable shortlist contender for most of the enterprise firewall market. It is assessed as a Challenger mostly because we see it displacing competitors on value and performance, but not often beating Leaders in mainstream enterprise selections. Fortinet has steadily been expanding its support offerings to be better aligned to the enterprise, including options for dedicated technical account managers.

Strengths

- Fortinet continues to get positive reviews for the delivery of new features and products, and clients report easy deployments. Fortinet has a large R&D team and uses this to outmaneuver competitors that often rely on OEM arrangements. This has enabled Fortinet to maintain road map agility, get to market quickly with both a new feature and one that is fully console-integrated, and better integrate features and avoid the pitfalls of partners that are acquired or change direction. This also has enabled Fortinet to expand its portfolio of nonfirewall network security offerings, which provides increasing cross-selling opportunities.
- Fortinet continues to increase its wins against the larger firewall incumbents, and it gained additional footholds in emerging areas, such as in-the-cloud firewalls and with carriers/ISPs where high-end performance is required. Fortinet is price-competitive, especially when using multiple virtual domains, and appliance reliability is reported as very high. Fortinet has invested substantially in obtaining and completing certifications and testing suites (Common Criteria, Federal Information Processing Standard [FIPS], NSS Labs and ICSA Labs) that are appealing to a wide array of customers.
- Its firewalls have high-end performance from purpose-built hardware and a wide model range (more than 20 appliance models), including bladed appliances for large enterprises and carriers, as well as SMB and branch office solutions. Although many competitors are increasing their reliance on Intel for their future performance gains, Fortinet (much as in its software development) maintains control of its own dual processors — one application-specific integrated circuit (ASIC) for network security operations and the second for content inspection.

The Advanced Mezzanine Card (AMC) expansion slot options for the enterprise-class models include an onboard security ASIC with additional ports or a hard drive providing investment preservation without having to resort to only appliance replacement, like many competitors. The AMC port options also minimize appliance replacement by being able to upgrade without replacing the whole box.

Cautions

- Where Fortinet was shortlisted but not selected in enterprises, the management capabilities were most often listed as the reason. However, where aggressive console use is not required, or where multiple firewalls share the same policy, the Fortinet console is highly competitive.
- Post-sales service and support do not win Fortinet selections over competitors; however, support and enterprise sales have been steadily improving in the enterprise, especially for premium-level support.
- Fortinet does not have a dedicated NGFW, but instead presents its UTM product, expecting a subset to be used. Fortinet's marketing that is focused on using UTM for enterprises undervalues Fortinet's enterprise offerings and steers away larger customers. Fortinet has historically defined enterprises as 500 users — about half the number used by Gartner and competitors. The UTM messaging also has enterprises excluding Fortinet from NGFW shortlists, even when the necessary capabilities (such as application control) are present.
- Fortinet does not have a strong third-party security vendor ecosystem compared with the major enterprise firewall incumbents.

HP

Acquired in 2009 as part of HP's acquisition of 3Com, China-based H3C was formed as a joint partnership between Huawei and 3Com, and has been shipping firewalls since 2003. Now as part of HP (see www.hp.com), it is leveraging this technology mostly in its current customer base. The HP F5000 and F1000, also called the A Series Firewalls, will be of most interest to China-based enterprises, especially where other H3C, 3Com or Huawei networking equipment is used. An add-in module for switches, the HP Threat Management Services zl module, is also available for the HP E5400 zl and E8200 zl series switches. HP is assessed as a Niche Player vendor primarily because of its geographic sales and presence, and the current absence of NGFW features, such as IPS and application control.

Strengths

- HP and legacy H3C have a strong regional presence in China and the Asia/Pacific region, and sales are increasing for incumbent HP networking customers.
- There is a wide range of models (including a high-throughput, blade-based chassis), branch office models and enterprise models, all with a flat-fee URL model.
- It has broad IPv6 support.

Cautions

- The former SecPath firewalls are not visible outside the Asia/Pacific region and have to address concerns from many geographies about relying on technology developed in China.
- The firewall lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation, which is usually seen in enterprise contenders.
- HP's corporate changes, which include four CEOs in 13 months. The inclusion of the network security business in a software division continues to show that HP does not yet have a coherent network security strategy.

Juniper Networks

Gartner sees Juniper Networks' firewalls (see www.juniper.net/us/en) mostly selected as an adjunct to the network infrastructure business by enterprises that are already Juniper customers. The move to Junos from ScreenOS and the SRX model line have been the most significant changes in the Juniper firewalls. Juniper also introduced AppSecure for application control and visibility. Juniper is assessed as a Challenger for enterprises, because we see Juniper selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features. During the evaluation period, Juniper appeared to focus more on other areas of its business and did not make significant advances with its firewall products. Juniper is, however, often shortlisted and/or selected in carrier, service provider and data center deployments, primarily because of price and high throughput on its largest appliances.

Strengths

- Appliance performance and range of models were most often listed by users as what they like about Juniper firewalls. Clients often comment on its positive performance and the reliability of its products, including responsiveness of support, and the global support channel.
- Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, and Juniper expresses a clear road map for firewall and security customers. Juniper has shown development and security discipline in keeping the rate of vulnerabilities in the product low.
- Juniper has strong branch office firewalls, complementing the enterprise products. Its branch-office firewalls include WAN optimization controller and an Avaya voice gateway.
- Having routing in the firewall is of interest to a very narrow segment of customers.

Cautions

- Problems using Juniper's Network and Security Manager to manage SRX products were the most common criticism by Gartner clients since the last version of this Magic Quadrant. Secure Design is the planned new management product to replace Network and Security Manager.

- As a network infrastructure vendor, Juniper is at a disadvantage selling into Cisco networks, where buying any Juniper security equipment can be resisted as a Cisco network equipment replacement.
- Like most competitors, integration between IPS and the firewall is limited, and Juniper is rarely considered by customers looking for an NGFW.
- During the evaluation period, Gartner observed an increase in complaints about Juniper firewall support — usually related to resolving complex configurations.

McAfee

McAfee (see www.mcafee.com/us) was acquired by Intel in early 2011 (see "Making Sense of Intel's Acquisition of McAfee"). It obtained its firewall products through the acquisition of Secure Computing in late 2008. The Sidewinder product has been renamed to the McAfee Firewall Enterprise (MFE). There are seven product models and a virtualized version. The MFE is certified for use on Crossbeam X Series blades and Riverbed Steelhead appliances. Application control has been added under the AppPrism feature name in v.8.0. Users report improvements in the firewall console quality under McAfee.

The road map for MFE is more important for consideration than the current features in the product. A re-engineered MFE integrated with the McAfee IPS on a purpose-built hardware platform will be the milestone for which to watch and a road map toward an NGFW. McAfee is assessed as a Challenger for enterprises, because we do not see it continuously displacing Leaders based on vision or feature, but instead through sales execution or value.

Strengths

- The TrustedSource feature blocks known bad IP addresses (from a dynamically updated list source) from connecting to the firewall, and is a significant differentiating feature. Although many companies have reputation features, the breadth of the reputation feed is a critical quality factor. The vendor's integration of reputation services across network, Web and email security product lines provides a strong cross-selling opportunity. The larger McAfee sales and channels have already increased MFE's presence in the market, while changes to the product are under way.
- The McAfee Firewall Profiler provides guidance on firewall configuration and is included with the product. MFE has identity and geolocation options.
- The Sidewinder firewall had a reputation for high security, making the MFE popular with some government-sector customers.
- McAfee has more network security products across multiple markets than almost any competitor. The prospect of integrating these products represents potential "glue" between silo products, which few competitors can promise.

Cautions

- The Intel acquisition presents a significant risk of distraction for the McAfee network security unit. Although an arm's-length relationship has been established, other acquisitions of network security products by nonsecurity or non-network companies have been generally unsuccessful. Intel already collaborates and supports many other network security vendors that compete with McAfee, putting in place a potential conflict.
- The McAfee IntruShield IPS engine, available in the stand-alone IPS appliances, is not yet integrated into the MFE. The current MFE IPS capabilities are not very competitive with leading NGFW vendors, especially for configuration and performance.
- McAfee has a small range of models and models that are generally not suitable for the high end or data center deployments. The MFE has been primarily available on general-purpose servers, which is met with skepticism by network operations buying centers. McAfee is transitioning to purpose-built hardware, with the likely eventual goal of merging the MFE onto the McAfee IPS hardware, which is highly competitive.
- MFE is rarely seen on Gartner client firewall shortlists; however, when it is, the time taken to navigate the general McAfee support system is the most often listed criticism heard from Gartner clients during the selection process.

NETASQ

NETASQ (see www.netasq.com) has been a pure-play network security vendor headquartered in France for more than a decade, selling firewalls, vulnerability management and messaging security gateways. NETASQ products mostly appeal to midsize companies and EU-based enterprises. All NETASQ firewall products are in two product lines. The U Series has eight models, and two appliances in the enterprise-labeled NG line. Virtual versions are also available in the V line. NETASQ is assessed as a Niche Player for enterprises, mostly because it best serves SMBs, and agencies in portions of EMEA or when the Leaders or Challengers do not have the usual advantages.

Strengths

- By not using traditional signatures and, instead, focusing on heuristics, NETASQ has innovated on an IPS path that is different from mainstream UTM vendors, which has positioned it more uniquely for countering new kinds of attacks. Users report that they like its policy-based management and real-time policy warning.
- It is VPN-certified for "EU restraint" use in the EU, which is of interest to governments and agencies looking for simpler procurement.
- NETASQ gets good marks from midsize enterprises for features and ease of use, and has good channel support in EMEA.
- NETASQ users comment to Gartner that the branded training and EU support are very good.

Cautions

- The majority of NETASQ's penetration, visibility and channel is focused in EMEA, especially France.
- Although having a good feature set, NETASQ has not been part of NGFW selections as seen by Gartner because of the company's low visibility outside France.
- Some users have commented to Gartner that managing large numbers of devices and VPN configurations is difficult within the interface.

Palo Alto Networks

Palo Alto Networks (see www.paloaltonetworks.com) has been selling enterprise firewalls for four years. A privately held company, Palo Alto Networks has been a significant disruptive influence in the firewall market during the evaluation period. This disruption was a result of focusing on replacing incumbent firewalls by closely integrating firewalls and IPSs of high quality, while adding application identification and inspection to meet emerging needs, all in a unified and tightly integrated engine. The company founder and CTO also has credibility as a co-inventor of the stateful firewall, and part of the founding team of a leading competitor, Check Point Software Technologies. Palo Alto Networks started in the market with behind the firewall placements to add application control; however, almost all deployments Gartner sees are firewall replacements.

Palo Alto Networks' high-performance NGFW functionality continues to drive competitors to react in the firewall market. It is assessed as a Leader mostly because of its NGFW design, redirection of the market along the NGFW path, consistent displacement of Leaders and Challengers, and market disruption forcing Leaders to react. With a unified single-pass inspection engine, rather than a design of passing traffic to submodules, Palo Alto Networks has maintained performance with relatively few models.

Strengths

- Palo Alto Networks continues to demonstrate effective application identification (App-ID), allowing for categorizing, blocking and rate-shaping of applications, particularly within HTTP and HTTPS. In the competitive situations that Gartner observes, Palo Alto Networks usually scores highest for application categorization and ease of configuration in the management console.
- Gartner customers report that Palo Alto Networks' appliance performance in most deployments is as advertised in specification sheets, and the management console is improving at a rate faster than competitors.
- The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream, obviating unnecessary IPS deep inspection or "hairpinning" — inefficiently passing traffic between modules. The IPS rated well in third-party testing by NSS Labs.

- Palo Alto Networks generated the most firewall inquiries among Gartner customers in 2010 and 2011 — almost more than all other firewall vendors combined — essentially dominating the enterprise conversation in NGFW. High customer loyalty and satisfaction are observed from early adopters.

Cautions

- The PA series of firewalls does not yet have Common Criteria EAL-4+ for Information Technology Security Evaluation for the firewall; however, EAL-2 certification was recently received.
- Palo Alto Networks has a limited number of models when compared with competitors. The company does not have products in adjacent security markets, which would allow for cross-selling opportunities. Fast growth has challenged its support infrastructure, which the company responded to with opening another U.S. support center. The company has room to develop a third-party product support ecosystem.
- Opportunistic selling into the secure Web gateway (SWG) and URL-filtering market can confuse some customers that Palo Alto Networks is not a firewall company, or allow it to be considered for UTM selections, for which it will not compete well in (for example, small businesses).
- Gartner has heard anecdotal performance issues, with appliances at the highest end, that customers deploy advanced NGFW policies on high-speed heterogeneous traffic.

SonicWALL

SonicWALL (see www.sonicwall.com) is a California-headquartered security company. In 2010, SonicWALL was acquired by Thoma Bravo, an investment firm that owns other security companies, such as Entrust and Tripwire. Although the majority of SonicWALL's business has been selling UTM to midsize businesses, it has introduced the SuperMassive line, which is squarely aimed at the high end at very competitive price/performance points. Other SonicWALL security products include Secure Sockets Layer (SSL) VPN, email security gateways, clean wireless and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class NSA, NSA and TZ. SonicWALL is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well (for example, retail and upper-midsize businesses), and we do not see it often displacing Leaders.

Strengths

- SonicWALL's competitive prices have resulted in strong solutions for wide remote-office deployments (such as in retail outlets) and SMBs.
- The company has the reputation and track record of strong channel support. SonicWALL has improved its enterprise go-to-market ability, rather than attempting to push an SMB UTM upmarket, by aligning product lines specifically to the horizontal — SuperMassive for data centers, service providers and ISPs, and the E-Class NSA for enterprises.

- The SuperMassive line has achieved market traction in high-end deployments, such as carriers and service providers, where firewall throughput, low latency and price are foremost. Historically, SonicWALL has been more focused on software. This move to hardware engineering has given it credibility in more enterprise selections. These gains are also evident in the performance shown in the E-Class platform using a purpose-built, stream-based deep inspection microprocessor design.
- SonicWALL recently enhanced application identification/inspection, under the name Application Intelligence and Control. Performance monitoring by core provides good device capacity management.
- The move to private company status after being acquired by Thoma Bravo (see "Thoma Bravo Buy to Boost SonicWALL Stance in Security Market") has allowed SonicWALL the flexibility to plan R&D and hardware engineering efforts that will have longer-term benefits. Greater collaboration with other Thoma Bravo companies could, however, be a future lever to better compete with vendors that have broader product portfolios.

Cautions

- Most of SonicWALL's firewall and other security product lines have been primarily SMB-focused and not competitive in most enterprises. SonicWALL does not yet have a broad enough enterprise channel, support and management console features to be considered in competition with Leaders and become a bigger part of the NGFW conversation.
- Gartner rarely sees SonicWALL in most Type A and Type B enterprise firewall selections.
- SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in the Gartner customer base. Although it has a good NGFW feature set, SonicWALL has not been part of NGFW selections as seen by Gartner. Keeping the NSA brand on the E-Class line has created some customer confusion as to whether the product is an SMB UTM or an enterprise-class firewall.

Sophos

Acquired by desktop security software vendor Sophos (www.sophos.com) this year (see "Astaro Acquisition Will Extend Sophos' Midmarket Security Offerings"), German firewall vendor Astaro has been shipping firewall products since 2001. Astaro takes a unique approach by leveraging open-source components and focuses primarily on software. Upper midsize businesses (for example, 250 to 999 employees) are most suited to use the Astaro Security Gateway. Gartner believes that Sophos will be the primary go-to-market channel for the Astaro Security Gateway, focusing on current Sophos customers that are starting to outgrow a UTM but do not yet have large enterprise firewall needs. Gartner observes Astaro usually scoring highly where price is the primary factor, Sophos products are already in place, and the throughput requirements are not at the higher end (for example, large enterprises). Sophos is assessed as a Niche Player for enterprises, mostly because it wins over Leaders in some selections based on features or with a very specific channel.

Strengths

- Astaro's leverage and integration of a wide range of open-source components provide an attractive price point. There is no extra charge for the management product, and of great interest, it offers a free basic firewall version for use in VMware.
- Users like Astaro's clustering features and price, and ease of installation is reported as a strong point.
- The Astaro Security Gateway is available as an appliance or software load, and as a certified Amazon Virtual Private Cloud connector. Astaro now has application control.
- Subsequent to the Sophos acquisition, strong growth in its firewall business has been experienced, and Astaro has SWG and email security gateway offerings. Customer satisfaction is generally high, especially with postsale technical support. Deployments in North America have increased.

Cautions

- The Astaro firewall has limited visibility outside of EMEA and is not often seen in enterprise selections in the Gartner client base. Its UTM focus is less a match for enterprises and better for SMBs. Astaro is short on enterprise features (such as supporting multiple firewall instances in the same appliance) and usually competes with other SMB firewall vendors.
- Users would like improved reporting, and the most voiced criticism was the difficulty of use and slow responsiveness of the of the management interface. The Astaro VPN does not have FIPS 140-2 certification.
- Sophos was not listed by any vendor we surveyed as a significant enterprise competitive threat, and has not been highly visible on NGFW shortlists among Gartner clients.

Stonesoft

Headquartered in Finland, Stonesoft (see www.stonesoft.com) has been expanding its operations into North America and other geographies, especially Eastern Europe. Stonesoft is focused on network security and has been very innovative in analyzing threat evasion techniques. Introduced in 2011, the Stonesoft NextGen Firewall product is offered across a wide range of appliances. Stonesoft is assessed as a Niche Player for enterprises, because it serves a set of placements well — usually for strong central management or where protection against evasive attacks is key. Stonesoft also provides stand-alone IPS and SSL VPN products. StoneGate v.5.3 introduced application awareness and user identity.

Strengths

- Stonesoft's threat research concerning evasive attacks has increased security credibility and visibility for the company and products.

- It is a security-focused vendor, and has demonstrated very good appliance performance and throughput. This year, Stonesoft introduced the FW-315, a smaller device for branch offices and environments such as process control locations.
- Stonesoft offers a virtualized firewall version that is certified for VMware. Both can be run under the Stonesoft Management Center.
- It offers support for clustering, very robust high availability and 3G backup connection capability.
- Support pricing is slightly lower than the industry average, and it has a loyal customer base.

Cautions

- Stonesoft has limited market visibility and channel strength outside of EMEA, and it has low visibility within the Gartner customer base, although its firewall and company revenue has increased.
- Although Stonesoft NGFW has many next-generation features, it has not been very visible in Gartner client NGFW shortlists.

WatchGuard

WatchGuard (www.watchguard.com) is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM series of products span performance and feature ranges demanded by large enterprises, but WatchGuard's branding, channel support and management capabilities tend to be more oriented toward smaller businesses. A well-established security-focused company, WatchGuard also has products that include SSL VPN and the XCS SWGs. The XTM-branded firewall models fall into two categories. The XTM 2 Series and XTM 5 Series are UTM, and the XTM 8 Series and the XTM 1050 and 2050 models are targeted for the enterprise. WatchGuard is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing Leaders.

Strengths

- WatchGuard's strong price/performance has enabled it to win price-sensitive competitions across retail, branch-office and remote-office deployments.
- Users report high satisfaction with the reporting function in the WatchGuard management console. WatchGuard has taken steps to better enter the enterprise arena such as achieving FIPS 140-2 certification for the VPN, and adding application control, and user identity features. Enterprise models are correctly targeted at NGFW, rather than UTM functionality.
- It has better-than-market-average integration between the IPS and the firewall, such as having IPS blocks result in subsequent source blocking at the firewall. It has a low rate of product vulnerabilities.

- Channel partners and customers rate the company highly. Having a specific management console for MSSPs is a competitive factor. A software key to unlock appliance performance for some models can minimize appliance downtime when upgrading.

Cautions

- Common Criteria for Information Technology Security Evaluation are not yet in place for all WatchGuard firewalls.
- Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed and has low visibility in the Gartner customer base. Although having a good NGFW feature set, WatchGuard has not been part of NGFW selections as seen by Gartner.
- Having the XTM model brand for all appliances has created enterprise customer confusion as to whether the products are suitable for them.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Network Intrusion Prevention System Appliances, 2010"

"Defining the Next-Generation Firewall"

"The Secure Web Gateway Will Not Converge With Enterprise Firewalls"

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Magic Quadrant for Unified Threat Management"

Acronym Key and Glossary Terms

ASA	Adaptive Security Appliance
ASIC	application-specific integrated circuit
FPM	firewall policy management
FIPS	Federal Information Processing Standard
Gbps	gigabits per second
IPS	intrusion prevention system
ISP	Internet service provider
MFE	McAfee Firewall Enterprise
MSSP	managed security service provider
NGFW	next-generation firewall
SMB	small or midsize business
SSL	Secure Sockets Layer
SWG	secure Web gateway
UTM	unified threat management

Evidence

The analysis in this report was primarily based on (1) interviews and interactions during firewall inquiries with Gartner clients since the last report, (2) surveys completed by vendors, (3) vendor briefings, (4) interviews with references provided by the vendor, and (5) supporting quantitative research on market share.

Note 1 Firewall Policy Management Tools

Third-party FPM vendors (such as AlgoSec, LogLogic, RedSeal Networks, Tufin, FireMon and Skybox Security) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the FPM market is still somewhat small, the customers requiring help with complexity are the very largest, and the market is growing. Additionally, very large enterprises usually have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single vendor solution is usually the best choice. All FPM vendors support multiple firewall products, whereas almost no firewall vendor will manage a competing product and is expanding into managing other network security devices.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/ serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/ partnerships, as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary

tools, customer support programs (and the quality thereof), availability of user groups and SLA.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600