Tallinna Ülikool

Informaatika Instituut

Microsoft DirectAccess ja OpenVPN võrdluses

Bakalaureusetöö

Autor: Toomas Väärt

Juhendaja: Meelis Karp

Autor: …….. “…...“ …… 2013. a.

Juhendaja: ……... “…...“ …… 2013. a.

Instituudi direktor: ……. “…...“ …… 2013. a.

Tallinn 2013

Autorideklaratsioon

Deklareerin, et käesolev bakalaureusetöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....
(kuupäev) (autor)

Sisukord

Sissejuhatus

Infotehnoloogia jõuline areng võimaldab tänapäeva arvutikasutajatel olla tunduvalt mobiilsemad, kui see oli võimalik varasemalt. Antud seisukohta kinnitab ka tõsiasi, et *IDC*[1] andmetel on müügi eesmärgil ülemaailmselt hakatud eksportima rohkem sülearvuteid kui lauaarvuteid, võimaldades inimestel olla tunduvalt liikuvamad. Seejuures on ka ülemaailmsete mobiilsete töötajate populatsioon oodatud kasvama 919,4 miljonilt 2008. aastal kuni 1,19 miljardile 2013. aastal, moodustades 34,9 % ülemaailmselt töötajaskonnast (Drake, Jaffe, Boggs, 2010, *Worldwide Mobile Worker Population 2009-2013 Forecast*, lk 1). Viimast aga soodustab paljuski just interneti kiire areng, mis arvutite kasutamise väljaspool kontorit kasutajatele võimalikuks teeb.

Tänapäeval on seega üpriski tavaliselt nähtuseks, kui töötaja viibib tööasjus väljaspool kontorit, olles näiteks töölähetusel. Sellest tingituna võib juhtuda, et töötajal on vaja ligi pääseda ettevõtte sisevõrgule, asudes ise samal ajal näiteks lennujaamas, kodus, kohvikus, kliendi juures või muudes kohtades, kus on olemas juurdepääs internetile. Seejuures pole aga ettevõtte turvalisuse huvides see, et kõikidel isikutel on võimalik pääseda ligi ressurssidele, mis ettevõtte sisevõrgus asuvad, kuna sageli on need mõeldud üksnes kitsale kasutajaskonnale ehk oma töötajatele. See aga tekitab erinevaid administreerimise probleeme, sest ka ettevõtte töötajatel endil on erinevad ligipääsuvõimalused ettevõtte siseinfole, mis võib olla konfidentsiaalne ning mille sattumine valedesse kätesse võib rikkuda oluliselt ettevõtte ärilisi huve. Tähtis on ka see, et kasutajate arvutid, millel on ligipääs ettevõtte sisevõrku, oleksid kaugelt hallatavad IT-administraatori poolt ja seeläbi kaitstud ning viirustest vabad. Et antud probleeme edukalt lahendada kasutavad organisatsioonid virtuaalse privaatvõrgu tehnoloogiat (edaspidi tekstis ka kui VPN[2]).

Antud bakalaureusetöö eesmärgiks ongi keskenduda virtuaalsete privaatvõrkude lahendustele. Pidades silmas bakalaureusetööle esitatud mahunõuet võrdleb töö autor omavahel Microsoft DirectAccessi ja OpenVPN-i omadusi, toob välja nende positiivsed ja negatiivsed küljed, ning püüab leida vastust küsimusele, kumb antud lahendustest on ettevõtete jaoks mõistlikum. Käesoleva bakalaureusetöö teema on aktuaalne, kuivõrd Eestis pole antud teemal koostatud veel ühtegi seesugust uurimust.

1 International Data Corporation
2 Virtual Private Network

Huvi Microsoft DirectAccessi vastu tekkis käesoleva töö autoril Ian McLeani ning Orin Thomase poolt kirjutatud raamatu “Configuring Microsoft® Windows 7” lugemise ajal, kus selgitati DirectAccessi laialdasi ning kasulikke omadusi. Seejuures puutub autor oma igapäevases töös kokku erinevate VPN-i ühendustega, kuid autorile pole töö kirjutamise hetkel teada ühtegi sellist Eestis asuvat ettevõtet, mis kasutaks DirectAccessi, seevastu leidub aga hulgaliselt neid, kes kasutavad OpenVPN-i tehnoloogiat.

Eeltoodust tulenevalt otsib autor ühtlasi oma töös vastust küsimusele, miks on OpenVPN-i kasutatavus Eestis laialdasem, kui on see Microsoft DirectAccess puhul. Nimetatud eesmärgi saavutamiseks on autor teinud vastava küsitluse ning esitanud need erinevate ettevõtete IT-juhtidele, süsteemiadministraatoritele, võrguadministraatoritele ning projektihalduritele. Küsitluse eesmärgiks on peaasjalikult saada informatsiooni selle kohta, millist virtuaalse privaatvõrgu tehnoloogiat ettevõttetes kasutatakse, millised eelised või puudused on DirectAccessil OpenVPN-iga võrreldes, kas DirectAccessil nähakse lähitulevikus potentsiaali ning kas ühe VPN-i eelistamine teisele on üldse põhjendatud.

Eeltoodud eesmärkide saavutamiseks on autor püstitanud järgmised hüpoteesid:

1) Microsoft DirectAccessi tarkvaralised lahendused on ettevõtetele mõistlikumad, kui on seda OpenVPN-i omad

2) Küsitlusele vastanud isikud eelistavad ühte virtuaalse privaatvõrgu tehnoloogiat teisele põhjendatult.

Käesoleva bakalaureusetöö kirjutamisel on autor kasutanud peamiselt võõrkeelseid allikaid, kuivõrd eestikeelseid antud teemakohaseid materjale ning teoseid leidub küllaltki vähe. Uurimismeetodina DirectAccessil ja OpenVPN-i omavahelisel kõrvutamisel on töös kasutatud võrdlevat meetodit. Autor eeldab, et antud diplomitöö lugejal on arusaam põhilistest infotehnoloogia-alastest, eeskätt just võrgundust ning virtuaalseid privaatvõrke puudutavatest erialastest terminitest.

Antud bakalaureusetöö on struktuuriliselt jaotatud kolmeks peatükiks. Bakalaureusetöö esimeses pooles võrdleb autor omavahel DirectAccessi ja OpenVPN-i tarkvara omadusi. Töö teises osas keskendub autor aga läbiviidud küsitlusele, kus toob välja küsitluse taustandmed, märgib üles saadud tulemused ning analüüsib saadud vastuseid. Bakalaureusetöö viimases, kolmandas peatükis, esitab autor antud teemakohase kokkuvõtte koos omapoolse arvamusega.

1. Microsoft DirectAccessi ja OpenVPN-i võrdlus

1.1 Virtuaalse privaatvõrgu tehnoloogiast üldiselt

Interneti levikuala on võrreldes minevikuga tunduvalt mastaapsem, olles kasutajatele kättesaadav ülemaailmselt. See on aga omakorda toonud endaga kaasa hulgaliselt nutikaid lahendusi tarkvaraarendajate poolt. Eelkõige just interneti laiaulatuslik kasutus on tekitanud huvi IP-põhiste virtuaalsete privaatvõrkude ehk VPN-ide vastu, mis on aja jooksul muutunud aina populaarsemaks (Andresson, Madsen, 2005, *Provider Provisioned Virtual Private Network (VPN) Terminology*, lk 6).

Terminit – virtuaalne privaatvõrk – on varasemalt seostatud selliste kaugühenduse teenustega nagu avalik telefonivõrk ja “Frame Relay PVC” ehk permanentne virtuaalühendus, kuid tänapäeval seostatakse seda peamiselt IP-põhiste andmevõrkudega. Enne seda kui seesugune kontseptsioon üldse tekkis, kulutasid suured korporatsioonid märkimisväärseid ressursse sellele, et ehitada üles komplekssseid privaatvõrke, mida tänapäeval teatakse kui intranetti. Kuna aja jooksul muutus internet aina rohkem kättesaadavamaks, siis hakkasid ettevõtted oma privaatvõrke jagama veebis ning lõid nn ekstraneti, et ühendada oma sise- ja väliskasutajaid (AnexGATE homepage, 2010, *VPN history*, lk 1).

Kuigi interneti kasutamine privaatvõrgu loomiseks on tasuv aga ka kiire viis, esineb üks oluline fundamentaalne probleem – turvalisus. Tänapäeva VPN lahendus aga ületab selle takistuse, kasutades spetsiaalseid tunneli protokolle ja komplekssseid krüpteerimise ja andmete terviklikkuse protseduure. Privaatsus on saavutatud enamjaolt nn punktist punkti ühendusega. Kuna antud operatsioonid leiavad aset avalikus võrgus, siis VPN-i rakendamine võib maksta oluliselt vähem kui eraomandis olevad või renditud teenused/võrgud.

VPN tähistab seega üldist terminit, mis hõlmab enda alla avalikke ja privaatseid võrke, luues kasutajagruppe, kes on eraldatud teistest internetikasutajatest ja kes saavad üksteisega suhelda nagu nad oleksid privaatses võrgus. Lühidalt öeldes on VPN viis privaatvõrguga (nt kontori võrk) ühenduse loomiseks avaliku võrgu (interneti) kaudu. Internetiühenduse kasutamine

võimaldab luua ühenduse eri allikatega üle kogu maailma ning olla ühenduses oma töökontoriga. Virtuaalse privaatvõrgu tehnoloogia abil saavad ka ettevõtted ise luua ühenduse oma harukontorite või teiste ettevõtetega avaliku võrgu (interneti) kaudu, säilitades samal ajal ühenduse turvalisuse (Microsoft Corporation, 2010, *Support*).

1.1.1 Microsoft DirectAccessi lühitutvustus

Windows Server 2008 R2 ja Windows 7 on tutvustanud DirectAccessi kui võimalust, mis asendab olemasolevat VPN-i infrastruktuuri. Microsoft DirectAccessi on reklaamitud kui lahendust, mis pakub kasutajatele kogemust, mille läbi kaugtöö tundub nii nagu inimene töötaks kontoris, sest DirectAccessi abil loob internetiga ühendatud klientarvuti IP ühenduse asutuse sisevõrgu ressurssidega (nt failiserver) kasutaja jaoks täpselt samamoodi, nagu ta asuks oma arvutiga asutuse sisevõrgus. Seega koos DirectAccessiga pääsevad kaugkasutajad ligi vajalikele ettevõtte failidele, veebilehtedele ja rakendustele ilma, et nad oleksid lisaks ühenduses virtuaalse privaatvõrgu – VPN-iga (Microsoft Corporation, 2010, *DirectAccess Technical Overview for Windows 7 and Windows Server R2*, lk 5).

Lühidalt öeldes loob DirectAccess nn kahepoolse ühenduse kasutaja ettevõtte võrguga iga kord kui kasutaja DirectAccessi toega arvuti ühendab end internetiga ja seda isegi enne, kui kasutaja ennast reaalselt sisse logib. Sellest tulenevalt ei pea kasutaja ise vaeva nägema, et ettevõtte võrguga ennast ühendada ning IT administaatorid saavad hallata arvuteid väljaspool kontorit. Kuid selleks, et Microsoft DirectAccess üldse toimida saaks, peavad ettevõtte serverid olema konfigureeritud nii, et nad DirectAccessi toega kliente ka toetaksid (Wright, Plesniarski, 2011, *MCTS Guide to Microsoft Windows 7: Exam #70-680*, lk 653).

Uurides Microsoft DirectAccessi ei saa aga jätta mainimata seda, et kui Microsofti serverile on lisatud spetsiaalne tarkvaralahendus - Unified Access Gateway ehk UAG - lihtsustab ja annab see lisavõimalusi DirectAccessi kasutamiseks. Koos UAG DirectAccessiga on võimalik hallata nii Apple, Linuxi kui ka Microsoft Windowsi operatsioonsüsteeme. Ühtlasi pakub UAG tuge suhtemiseks IPv6 kui ka IPv4 võrkudega (Kopczynski T., CISSP, GSEC, GCIH, MCTS; 2010, *DirectAccess and UAG DirectAccess Deployment Guide*, lk 31).

1.1.2 OpenVPN-i lühitutvustus

OpenVPN-i peetakse silmapaistvaks tarkvaraliseks lahenduseks, mis leiutati James Yonani poolt 2001.aastal ning mida on aja jooksul püsivalt edasi arendatud (Feilner; Graf, 2009, Preface). Ühtlasi peetakse OpenVPN-i üheks maailma populaarseimaks paketiks, mille abil virtuaalne privaatne võrk üles seada. OpenVPN-i kasutatakse laialdaselt paljude indiviidide ja ettevõtete poolt ning mõned teenusepakkujad pakuvad OpenVPN-ile ligipääsu kui teenust kaugkasutajatele ebaturvalistes oludes (Keijser, 2011, *OpenVPN 2 Cookbook*, Preface).

OpenVPN hõlmab endas laiaulatuslikku VPN-i raamistikku, mis on kavandatud lihtsustama kohaspetsiifilisi vajadusi, näiteks võimaldades klientidele jagada kohandatud installatsiooni pakette või pakkuda alternatiivseid autentimismeetodeid läbi OpenVPN-i tarkvaramooduli liidese (Keijser, 2011, Preface). OpenVPN-i ligipääsu server omab hulgaliselt installatsiooni ja konfiguratsiooni vahendeid, mis võimaldavad lihtsat ja kiiret VPN-i kaugjuurdepääsu lahenduste kasutuselevõttu, kasutades OpenVPN-i avatud lähtekoodi projekti (OpenVPN Technologies Inc., 2010,*OpenVPN Access Server System Administrator Guide*, lk 2).

1.2 Paigaldamiseks esitatavad nõuded

1.2.1 Microsoft DirectAccessi paigaldamiseks esitatavad nõuded

Microsoft DirectAccessi üheks nõudeks võib välja tuua selle, et ühel või enamal serveril peab peale olema installeeritud operatsioonsüsteem Windows Server 2008 R2 või sellest uuem versioon. Lisaks on vajalik, et serveril oleks olemas kaks võrguadapterit: üks, mis on ühenduses otse välisvõrguga ning teine, mis on otse ühenduses sisevõrguga. DirectAccessi serveri võrguadapteril tuleb seejuures määrata vähemalt kaks järjestikust avaliku IPv4 aadressi, mis on ühenduses internetiga. DirectAccessi kasutajate arvutite nõudeks on aga see, et kasutusel oleks operatsioonsüsteem Microsoft Windows 7 Enterprise või Microsoft Windows 7 Ultimate. Ühtlasi peavad kliendid olema AD DS[3] domeeni liikmed (Microsoft Corporation, 2010, *DirectAcces Requirements*).

Eeltoodust mitte vähemoluliseks nõudeks võib välja tuua ka selle, et Microsoft DirectAccessi puhul peab eksisteerima üks domeenikontroller (Microsoft Windows serverites nimetatakse domeenikontrolleriks serverit, mis käitleb autentimisnõudeid ehk võimaldab sisselogimist Windows Serveri domeenis) ning DNS server (ehk domeeninimede süsteem: internetiteenus, mis tõlgib domeeninimed IP aadressideks), mis kasutab Windows operatasioonsüsteemi Server 2008 SP2-e või Windows Server 2008 R2-e. Nimetatud nõuet on lihtsam aga täita, kui serveris on alternatiivina kasutusel UAG (Forefront Unified Access Gateway). UAG abil on DirectAccessi võimalik paigaldada ka DNS serveri ning domeenikontrolleriga, mis töötavad Windows Server 2003 peal, kuid seda vaid juhul, kui NAT64 funktsioon on lubatud (Microsoft Corporation, 2010, *DirectAcces Requirements*).

DirectAccessi puhul on tähtis ka PKI ehk nn avaliku võtme infrastruktuur, mis väljastab arvuti sertifikaate ning valikuliselt kiipkaardi sertifikaati kiipkaardi autentimiseks ja ka tervise sertifikaati NAPi jaoks (Microsoft Corporation, 2010, *DirectAcces Requirements*). NAP ehk Network Access Protection tähistab funktsiooni Windows Server 2008 R2-e ja Windows 7-e juures, mis jälgib süsteemi miinimumnõudeid, hinnates kliendi arvuti tervist, kui nad üritavad ühenduda või suhelda võrgus. Kliendi arvutid, mis ei ole kooskõlas süsteemi tervishoiu

3 Active Directory Domain Service

miinimumnõuetega, saavad üksnes piiratud juurdepääsu võrgule kuniks nende konfiguratsioon on uuendatud (Microsoft Corporation, 2010, *DirectAccess with Network Access Protection (NAP))*.

Veel üheks DirectAccessi kasutamise tingimuseks võib välja tuua ka selle, et kui kliendid tahavad omavahel suhelda IPv4 tehnoloogial põhinevatel ressurssidel, on tarvis NAT64 funktsiooni, mis ei ole DirectAccessi standardpaketi osaks. Kui aga Windowsi Server on varustatud UAG-ga, siis sisaldab see endas sisseehitatud NAT64 funktsiooni (Microsoft Corporation, 2010, *DirectAcces Requirements*). Täpsemalt võimaldab NAT64 funktsioon suhelda IPv6 võrkudel IPv4 võrkudega ja vastupidi (Microsoft Corporation, 2012, *IPv6 – Technology Overview*).

1.2.2 OpenVPN-i paigaldamiseks esitatavad nõuded

OpenVPN-i kasutamise üheks nõudeks võib välja tuua selle, et kui kasutaja soovib paigaldada Windowsi platvormil olevat OpenVPN-i serverit, siis peaks serverile olema installeeritud spetsiaalne tarkvara, millisteks on VMware Workstation, VMware Server, VMware Player või VMware Fusion (OpenVPN Technologies Inc., *Using the OpenVPN Access Server Virtual Appliance VMware Version*). Teine võimalus, kuidas Windowsi serveri keskkonnas OpenVPN-i Serverit kasutada, on Windowsi serverile installeerida Hyper-V või Virtual PC, näiteks täpsemalt Hyper-V 2008 R2, Hyper-V 2008 R2 (OpenVPN Technologies Inc., *Using the OpenVPN Access Server Windows (VHD) Virtualization Version*). Samas on aga OpenVPN-il olemas ka kommertsverisoon, mille installeerimiseks pole vaja eraldi eelpool kirjeldatud virtualiseerimise tarkvara ega osta ka litsentse. Kuid antud versiooni negatiivseks küljeks on see, et kommertsversioonil puudub ülevaatlik ja mugav OpenVPN-i graafiline administraatori kasutajaliides (OpenVPN Technologies Inc., *Community Project Overview*).

Lisaks on OpenVPN-i serverit võimalik ka installeerida RedHat, Fedora, CentOS, Debian ning Ubuntu värskematele versioonile. Olenevalt protsessori arhitektuurist on olemas versioone nii 32bit kui ka 64bit-seid operatsioonsüsteemile (OpenVPN Technologies Inc., *OpenVPN Access Server Quick Start Guide).* Oluline on veel ka teada, et Linuxi installeerimisel serveris oleks

funktsioon nimega SELinux välja lülitatud. Lisaks tuleb veenduda, et võrgu sätted lubaksid OpenVPN-i klientidel siseneda ligipääsuserverisse ning et serveri domeeninimi vastaks ikka õigele aadressile (OpenVPN Technologies Inc. *How to prepare for the deployment of openVPN Access Server?).*

Selleks, et viimati mainitud protsess edukalt lõpetada, tuleks teha ka üks järgnevatest valikutest: serveril on kas siis staatiline IP-aadress, mis on kättesaadav klientidele internetis (vähemalt TCP port, mis on kasutusel Access Serveri poolt) ning eelduslikult on serveril olemas ka FQDN (Fully Qualified Domain Name) ehk täielik domeeninimi või serveril on dünaamiline IP-aadress, mis on klientidele kättesaadav internetist ning dünaamiline DNS server, mis jälgib muutuvat IP-aadressi (OpenVPN Technologies Inc. *How to prepare for the deployment of openVPN Access Server?).*

1.2.3 Kokkuvõte

Lähtudes eeltoodust võib selgelt välja tuua asjaolu, et Microsoft DirectAccessi on võimalik installeerida üksnes Windowsi serveri operatsioonsüsteemi keskkonnas, mis muudab OpenVPN-i tarkvara kasutamise DirectAccessiga võrreldes palju paindlikumaks, kuivõrd OpenVPN-i on võimalik installeerida nii Windowsi aga ka Linuxi keskkonnas.

DirectAccessi negatiivseks küljeks võib autori hinnangul nimetada ka seda, et DirectAccessi saavad kasutada ainult Windows Enterprise ja Windows Ultimate-i kasutajad, mis aga piirab oluliselt kasutajaringi.

Suuremaks erinevuseks uuritavate objektide vahel saab välja tuua ka selle, et OpenVPN ühenduse jaoks pole tarvis kahte võrguadapterit, mida on aga vaja DirectAccessi puhul. Tegemist on seega lisanõudega, mis muudab DirectAccessi kasutuselevõtu nõudlikumaks kui OpenVPN-i puhul, selle vajalikkust ning põhjendatust uurib autor aga täpsemalt järgnevas alapeatükis. Kuid uurides kahe virtuaalse privaatvõrgu paigaldamise nõudeid, selgus ka asjaolu, et Microsoft DirectAccess vajab töös olekuks ilmtingimata domeenikontrollerit. Küll aga saab OpenVPN-i kasutada ilma domeenikontrollerita.

Tehes kokkuvõttet peatükist „Paigaldamiseks esitatavad nõuded“, soovib autor suuremat tähelepanu pöörata sellele, et Microsoft DirectAccess ilma UAG-ta on palju nõudlikum. UAG aga lihtsustab kasutamist, kuigi selle peab eraldi serverile peale installeerima, mis on kahtlemata lisatööks. OpenVPN seevastu on palju paindlikum, seda on võimalik paigaldada nii erinevate Linuxite kui ka Windowsi serveri operatsioonsüsteemidele. Autori hinnangul on OpenVPN-il seega tunduvalt väiksemad nõuded, kui on neid Microsoft DirectAccessil.

1.3 Ühenduse spetsiifika

1.3.1 Microsoft DirectAccessi ühendus

DirectAccess on üles ehitatud standarditel põhineval tehnoloogial: IPsec-il[4] ja IPv6-l[5]. DirectAccess kasutab IPsec-i, et autentida mõlemat, nii kasutajat kui arvutit, lubades administraatoril seadistada arvutit enne, kui kasutaja üldse sisse logib. DirectAccessi abil loovad kliendid IPv6 liikluse IPsec tunnelis DirectAccessi serverini, mis moodustab justkui värava sisevõrgu ja klientide arvutite vahel (Microsoft Corporation, 2010, *DirectAccess Connections*).

Täpsemalt loob DirectAccessi klient kaks IPsec tunnelit, kasutades selleks IPsec tunneli režiimi ja ESP[6] funktsiooni ehk nn sõnumi kapselturve, mis tagab IP-datagrammide terviklikkuse, autentimise ja konfidentsiaalsuse. Ühte neist tunnelitest võib kutsuda nn infrastruktuuri ning teist sisevõrgu tunneliteks. Infrastruktuuritunnel annab juurdepääsu sisevõrgu - Domain Name System (DNS) - serverile ning domeenikontrollerile, lubades arvutil alla laadida Group Policy ehk rühmapoliitika konfiguratsioone ning küsib autentimist kasutaja poole pealt. Sisevõrgu tunnel aga autentib kasutajat ja annab juurdepääsu sisevõrgu ressurssidele ja serveritele (Microsoft Corporation, 2010, *DirectAccess Connections*).

IPv6 osas on seejuures aga oluline teada, et kuigi DirectAccess töötab IPv6 platvormil, siis on DirectAccessi teatud juhul võimalik kasutada ka IPv4 tehnoloogial. Nimelt juhul kui kohalik

4 Internet Protocol Security
5 Internet Protocol version 6
6 Encapsulating Security Payload

IPv6 võrk pole kättesaadav, saab klient kasutada 6to4 või Teredo IPv6-e ülemikutehnoloogiat, mis võimaldab edasi saata IPv4 kapseldatud IPv6-e põhist liiklust. Kui aga näiteks tulemüür takistab kliendi arvutil 6to4-l või Teredo-l DirectAccessi serveriga ühendust saada, siis üritab kliendi arvuti automaatselt ühenduda IP-HTTPS[7] abil. Protokoll IP-HTTPS kasutab nimelt IPv4-põhist SSL[8] ühendust, et kapseldada IPv6 liiklust (Microsoft Corporation, 2010, *The DirectAccess Connection Process*).

Nagu eelpool mainitud on DirectAccessi abil võimalik omavahel eraldada välisvõrk ja sisevõrk. Täpsemalt suudab DirectAccess eraldada sisevõrgu liiklust välisvõrgu liiklusest, et vähendada mittevajalikku liiklust ettevõtte võrgus. Enamus VPN-sid aga saadavad kogu liikluse, isegi liikluse, mis on suunatud välisvõrgu poole, läbi VPN-i ühenduse. Antud asjaolu võib muuta liikluse aeglaseks ettevõtte sise- ja välisvõrgus. Interneti liiklus välisvõrguga ei pea aga seejuures liikuma läbi sisevõrgu, vaid liiklus, mis on suunatud välisvõrku, läheb otse välisvõrku, ilma sisevõrku läbimata. Lühidalt öeldes ei saada nn vaikimisi liiklusvool DirectAccessis interneti liiklust läbi DirectAccessi serveri (Microsoft Corporation, 2010, *Separating Internet and Intranet Traffic*).

Ühenduse osas võib DirectAccessi puhul välja tuua ka selle, et IT-administraatoritel on võimalus suunata kogu liiklus, välja arvatud kohaliku alamvõrgu liiklus, läbi DirectAccessi serveri ning intranetti ehk sisevõrkku. Kui see valik on võimaldatud, siis kasutab DirectAccessi klient IP-HTTPS-i IPv6 ühenduseks DirectAccess serveriga, vaatamata sellele, kas DirectAccessi klient on tulemüüri või välisliiklust vahendava komponendi - proxy - ehk puhverserveri taga. Kombineerides selle võimaluse aga Windowsi tulemüüriga ning Windowsi lisarakenduse ja arvuti kaitsemehhanismi Advanced Security-iga, saavad IT-administraatorid täieliku kontrolli selle üle, millised rakendused võivad ühendust kasutada ning millistesse alamvõrkudesse klientide arvutid ligi pääsevad (Microsoft Corporation, 2010, *Separating Internet and Intranet Traffic*).

Näiteks saavad IT-administraatorid seadistada Windowsi tulemüüri reegleid, et need: lubaksid arvutidel ühenduda kogu internetiga, kuid ainult ühe spetsiifilise alamvõrguga sisevõrgus;

7 Internet Protocol - Hypertext Transfer Protocol Secure
8 Secure Sockets Layer

lubaksid arvutitel ühenduda otse internetiga kasutades selleks Internet Explorerit aga et kõikide teiste aplikatsioonide ühendus liiguks läbi sisevõrgu; hoiaksid ära sisevõrgu programmide suhtluse internetiga, piirates nende suhtlemist ainult kindlate serveritega sisevõrgus (Microsoft Corporation, 2010, *Separating Internet and Intranet Traffic*).

1.3.2 OpenVPN-i ühendus

Open VPN-i ühenduse osas on oluline esmalt teada, et OpenVPN-i versioonides, mis on vanemad kui 2.2-RC2, on piiratud IPv6 tugi. Kui OpenVPN 2.0 töötab nn serveri režiimina, siis on IPv6 toetatud ainult läbi TAP mooduse aga mitte TUN-i abil. Lisaks peavad VPN-i kandvad ühendused kasutama IPv4 lõpp-punkte. OpenVPN 2.2-RC2-s IPv6-t TUN-režiimis aga rakendati Windows TAP draiveri jaoks. Täielik IPv6 tugi on nüüdseks olemas "kõike ühendavas" ja uusimat koodi kasutavas Git-is[9] ning mis on lisatud ka OpenVPN 2.3-e (OpenVPN Technologies Inc, 2011, *Is IPv6 support planned/in the works?).*

OpenVPN-ile on iseloomulik ka see, et üle interneti andmete edastamine toimub läbi turvalise SSL[10] protokolli. Kuivõrd OpenVPN kasutab SSL-i, ei saa OpenVPN-i kasutada koos IPsec, L2TP[11] või PPTP[12]-ga. Ajalooliselt on aga IPsec-i eelis olnud erinevate tootjate tugi, kuid see on aga tasapisi hakanud muutuma, kuna OpenVPN-i tuge on järk-järgult suurendatud teatud riistvara seadmetele (OpenVPN Technologies Inc, *Why SSL VPN?).*

OpenVPN Access Server ehk OpenVPN-i pöördusserver koosneb komplektist installatsiooni ja konfiguratsiooni tööriistadest, mis võimaldavad kiiret VPN-i kaugjuurdepääsu lahendust, kasutades OpenVPN-i avatud lähtekoodiprojekti. OpenVPN-i pöördusserveri kasutuselevõtt sisaldab endas ühte serverit aga palju kliente ning palju kasutajaid. Iga kliendi seade kasutab avalikku IP-võrku (internetti), et suhelda OpenVPN pöördusserveriga ja saavutab seeläbi VPN-kaitstud sissepääsu privaatsele IP-võrgule (OpenVPN Technologies Inc, 2010, *OpenVPN Access Server System Administrator Guide*, lk 2).

9 http://git-scm.com/
10 Secure Socets Layer
11 Layer 2 Tunneling Protocol
12 Point-to-Point Tunneling Protocol

OpenVPN Access Server sisaldab kokku kolme võrguteenust: VPN Server; Connect Client (HTTPS) ning Admin Web UI (HTTPS). 1) VPN Server on süsteemiagent, mis loob VPN tunnelid VPN-i klientidega. Kui TCP[13] protokoll on seadistatud VPN-i serveriga suhtlemiseks, võib VPN Server samuti suunata teenused Connect Clienti või/ja Admin Web UI-le. 2) The Client Web Service ehk kliendi veebiteenus on kaitstud veebiteenus, mis sisaldab SSL-kaitstud HTTP prokotolli. Kasutajad logivad „Connect Client"-i, et allalaadida eelkonfigureeritud OpenVPN-i kliendi installifaili või kliendi konfiguratsioonifaili. Tavapärane ühendus sellise liikluse jaoks on TCP võrguport (liides, mille kaudu saab üle võrgu pöörduda konkreetse programmi poole) 443. 3) VPN Tunnel service-it ehk nn VPN-i tunnelteenust on võimalik konfigureerida nii, et see kasutaks kas TCP või UDP[14] võrguporti. TCP puhul on võimalik seda konfigureerida veel ka nii, et see edastaks Connect Client-i ja/või „Admin Web UI" teenuseid. Kui teenuse edastamine on kasutusel, siis peab vaid üks TCP port interneti klientidele avatud olema. Kui rakendusi, mis vajavad UDP kommunikatsiooni (nagu näiteks VoIP[15]), kasutatakse VPN-is, siis OpenVPN-i Access Serveri-i seadistamine selliselt, et see kasutaks UDP protokolli VPN-i „tunneldamiseks" viib tulemuseni, et VPN-i tunnelis toimuv kommunikatsioon on märksa efektiivsem. Sellisel juhul peab serveris interneti klientidele olema avatud ka UDP port (tavaliselt nr 1193) (OpenVPN Technologies Inc, 2010, *OpenVPN Access Server System Administrator Guide*, lk 5).

OpenVPN-il on kolm kõige tüüpilisemat võrgukonfiguratsiooni. Neist esimene on: üks võrguliides privaatsel võrgul tulemüüri taga. Selline konfiguratsioon on kõige levinum, kui Access Server asub ettevõtte sisevõrgus, võimaldades VPNi sisenemist kasutajatel, kes on väljaspool ettevõtte võrku. Sellisel konfiguratsioonil Access Server omab ühte võrguliidest, mis on ühendatud privaatse võrguga. Sellise konfiguratsiooni puhul on vajalik, et interneti võrguvärav oleks seadistatud edastama soovitud TCP/UDP võrgupordi liiklust avalikust IP-aadressist Access Serveri privaatsele IP-aadressile. Minimaalselt üks TCP port (tavaliselt 443) on vajalik suunata. See suudab kanda nii VPN tunneli liiklust kui ka Web Client Server/Connect Client-i liiklust. Valikuliselt on võimalik VPN tunnelit eraldada Web Client Server-i liiklusest, sellisel juhul tuleks lisaks avada üks TCP või UDP liides (tavaliselt 1193) (OpenVPN Technologies Inc, 2010, *OpenVPN Access Server System Administrator Guide*, lk 5-6).

13 Transmission Control Protocol
14 User Datagram Protocol
15 Voice over Internet Protocol

Teiseks tüüpiliseks OpenVPN-i võrgukonfiguratsiooniks on: kaks võrguliidest, üks avalikus ja teine privaatses võrgus. Sellist konfiguratsiooni on kõige sagedamini näha siis, kui Access Server asub ettevõtte sisevõrgus aga omab seejuures isiklikku avalikku IP-aadressi. Access Server suhtleb klientidega väljaspool ettevõtte sisevõrku läbi oma avaliku IP-liidese. See kasutab teist võrguliidest, et suhelda võrku ühendatud arvutitega privaatses IP-võrgus ja saadab andmepakette VPN tunneli ja privaatvõrgu vahel (OpenVPN Technologies Inc, 2010, *OpenVPN Access Server System Administrator Guide*, lk 6).

Kolmandaks tüüpiliseks OpenVPN-i võrgukonfiguratsiooniks võib nimetada järgmist: üks võrguliides avalikus võrgus. Selline konfiguratsioon on aga kõige tihedamini näha siis, kui Access Server asub andmeserveris ja selle eesmärk on luua virtuaalne IP-võrk, milles kõik VPN-i kliendid saavad ühenduda selleks, et hoida end ühenduses teenustega, mis on paigaldatud serverisse (OpenVPN Technologies Inc, 2010, *OpenVPN Access Server System Administrator Guide*, lk 7).

1.3.3 Kokkuvõte

Eeltoodust tulenevalt võib DirectAccessi ning OpenVPN-i ühenduse erinevuseks välja tuua selle, et DirectAccessi ühendused on loodud ühenduma automaatselt, kui kasutaja arvuti siseneb internetti. OpenVPN-i ühendusele on iseloomulik aga asjaolu, et ühendus tuleb alustada ja lõpetada kindla kasutajapoolse toiminguga. OpenVPN-i kasutaja saab ühineda VPN-i ühendusega kasutades selleks „Connect Client“-it. Ühtlasi peitub DirectAccessi mugavus ka selles, et administraator saab arvutit administreerida enne, kui kasutaja sinna end sisse logib. Seega võib DirectAccessi plussiks tuua asjaolu, et see on automaatne ehk ei nõua eraldi käivitamist nagu nõuab seda standardne OpenVPN-i pakett.

Vastavalt eelnevates alapeatükkides käsitletule, saab oluliseks erinevuseks antud virtuaalsete privaatvõrkude puhul välja tuua ka selle, et DirectAccessi ja OpenVPN-i on omavahel võimalik eristada ka IPv6 tehnoloogia kasutamise põhjal. Nimelt on DirectAccess valmistatud juba uue tehnoloogiaga, mis omab täielikku valmisolekut IPv6 võrkude jaoks. Võrdluseks võib aga tuua, et OpenVPN lubab pakkuda täielikku tuge IPv6 jaoks alles OpenVPN 2.3 versioonis, milline

väljaanne on tänaseks avalikkusele kättesaadavaks tehtud alles 2013. aasta märtsikuu lõpuks. Samas ei saa aga IPv6 kasutamisvõimalust nimetada niivõrd DirectAccessi plussküljeks ja OpenVPN-i miinuspooleks, kuivõrd IPv6 on küllaltki uus protokoll, mis jõudis laialdasemalt kasutusele alles 6.juunil 2012.aastal (Microsoft Corporation, 2012, *IPv6).* Seega on antud protokolli kasutatavus autori hinnangul veel üsna väike. IPv6 protokoll pole näiteks ka „Google"-i kasutajate seas eriti populaarne, kuna sealseid IPv6 kasutajaid 20.aprilli 2013.a. seisuga oli vaid 1.34% (Google, 2013, *Statistics*). Kuigi ka DirectAccessi puhul on loodud lisavõimalus IPv4 kasutamiseks, nõuab see omaette seadistamist. Seetõttu võiks öelda, et DirectAccess on ühenduse poole pealt pigem tulevikku suunatud, kuivõrd see on loodud eeskätt IPv6 platvormile. Siinkohal tahab aga autor rõhutada, et ühenduse osas on DirectAccessi oluliseks eeliseks OpenVPN-i ees see, et juhul kui DirectAccessi kasutaja ei saa mingil põhjusel kasutada IPv6 võrku, siis kasutab DirectAccess automaatselt 6to4 või Teredo IPv6 üleminekutehnoloogiat. Kui aga ka 6to4 või Teredo ei saa DirectAccessi serveriga ühendust, siis püüab kliendi arvuti DirectAccessi serveriga automaatselt ühenduda IP-HTTPS-i abil. Eeltoodust tulenevalt on autori hinnangul DirectAccessi ühenduse protsess väga hästi läbimõeldud ja kasutaja jaoks töökindlam, sest omab tagavara alternatiive ühendumaks ettevõtte sisevõruga.

Veel üheks erinevuseks OpenVPN-i ning DirectAccessi ühenduse osas võib välja tuua selle, et OpenVPN-il on palju erinevaid võrgukonfiguratsiooni mooduseid, kuidas ühendus kasutajate jaoks luua. Kõige tüüpilisemad konfiguratsioonimoodused, mida OpenVPN-i puhul kasutatakse, on nimetatud eespool, täpsemalt peatükis 1.3.2 ning kõige sarnasem neist DirectAccessiga on teine võrgukonfiguratsioon - kaks võrguliidest, üks avalikus ja teine privaatses võrgus. Seega on DirectAccessi võrgukonfiguratsioone vaid üks, OpenVPN pakub aga laia valikut, olles seeläbi kasutajate jaoks tunduvalt paindlikum ning võimaldab ettevõttetel valida endale sobivaima variandi.

Ühenduse puhul võib välja tuua asjaolu, et DirectAccess on disainitud eraldama sisevõrgu liiklust interneti liiklusest, mistõttu väheneb mittevajalik liiklus sisevõrgus. DirectAccessi oskab seega vahet teha andmepakettidel, mis on seotud internetiga ning mis ettevõtte sisevõrguga. Antud asjaolu aga võimaldab ühendusel olla tõhusam ning kiirem. Seevastu enamik VPN-e ei filtreeri andmepakette ning edasi saadetakse kogu liiklus, sealhulgas ka kõik see, mis on mõeldud internetis liikumiseks. Kuivõrd eelpool sai tuvastatud, et DirectAccessile kõige

sarnasemaks OpenVPN-i võrgukonfiguratisooniks on kaks võrguliidest, üks avalik ja teine privaatses võrgus, siis sarnaselt DirectAccessile omab ka OpenVPN võimalust eraldada mittevajalikku liikust sisevõrgu liiklusest. Antud moodus on aga üks paljudest OpenVPN-i ühendamise võimalustest. Autori hinnangul on aga just see OpenVPN-i ühendamise võimalus kõige tõhusam, sest see võimaldab olla samaaegselt kiire aga esmapilgul ka turvaline moodus, kuivõrd sise- ning välisvõrgu liikluse andmepaketid on üksteisest tõhusalt lahutatud. Turvalisusele keskendub autor täpsemalt aga järgnevas peatükis.

Ühenduse osas leiab autor vajalikuks veel juhtida tähelepanu 2011. aasta teaduslikule uurimustööle „Performance Comparison of IPsec and TLS Based VPN Technologies“, mis põhineb IPsec-i ja TLS protokollide jõudluse omavahelisel võrdlusel. Antud uurimus keskendus VPN tehnoloogiatele, mis võrdles neid kahte tehnoloogiat, baseerudes nende parameetritele nagu näiteks läbilaskevõime ja reaktsiooniaeg. Uurimuses jõuti järeldusele, et raske on täpsemalt valida, milline neist kahest protokollidest on parem, kui analüüsida nende kõiki tulemusi korraga. Siiski otsustati paremaks valida OpenVPN selle lihtsuse ning kiire ja otsekohese rakendamise tõttu. Leiti, et SSL lahenduse installeerimine ja konfigureerimine võrreldes IPseciga on justkui „lapsemäng“. Teisest küljest toodi välja aga asjaolu, et IPsec on mõnevõrra kiirem ja on olnud turul kauem aega, kui on seda SSL VPN-i võimalused, mistõttu on sel tehnoloogial palju rohkem tuge riist- ja tarkvara tootjatelt (I. Kotuliak, P. Rybár, P. Trúchly, 2011, *Performance Comparison of IPsec and TLS Based VPN Technologies*, lk 220-221).

1.4 Kasutajate autentimine ja turvalisus

1.4.1 Microsoft DirectAccessi autentimine ja turvalisus

DirectAccessile on iseloomulik asjaolu, et DirectAccess autentib arvuti enne, kui kasutaja üldse sisse logib, muutes privaatse sisevõrgu tehnoloogia kasutamise väga mugavaks, kuivõrd kasutaja ei pea autentimiseks eraldi aega planeerima ning füüsiliselt arvuti taga olema. Kuid üldjuhul tagab arvuti autentimine siiski ligipääsu ainult domeenikontrolleri ja DNS serveri vahel. Alles pärast kasutaja sisselogimist autentib DirectAccess kasutajat, misjärel saab kasutaja ühenduda ressurssidega, millele tal siseneda on lubatud (Microsoft Corporation, 2010, *DirectAccess Authentication*).

Seejuures toetab DirectAccess standardset kasutaja autentimist, kasutades selleks arvuti sertifikaate, kasutajakonto nime ning parooli isikutunnistust. Suurema turvalisuse huvides on võimalik juurde lisada autoriseerimise kiipkaardiga (näiteks ID-kaardiga). Selline konfigureerimise viis võimaldab kasutajatel siseneda interneti ressursidesse ilma kiipkaardita, kuid vajab kiipkaarti vahetult enne seda, kui kasutaja soovib ühenduda sisevõrgu ressurssidega. Lisaks peab kasutaja sisestama kiipkaardile oma kasutajapoolsed tunnused täiendavaks kaitseks (Microsoft Corporation, 2010, *DirectAccess Authentication*).

Ühtlasi kasutab Microsoft DirectAccess autentimise jaoks IPv6/IPsec tunnelit, et ühendada DirectAccessi kliente DirectAccessi serveritega ja sisevõrgu resurssidega. Lisaks on serverile võimalik paigaldada Microsoft Forefront UAG, DirectAccessi hõlbustusrakendusprogramm (wizard), mis konfigureerib Windowsi tulemüüri koos Advanced Security ühenduse turvalisuse eeskirjadega järgnevalt:

1. Infrastruktuuri tunneli (antud tunnel on loodud enne, kui kasutaja sisse logib) puhul DirectAccessi kliendid autentivad arvuti sertifikaadi ja arvuti kontopõhistel NTLMv2 (täiustatud seansiturbemehhanism, mis on mõeldud sõnumite konfidentsiaalsuse ehk krüpteerimise ja terviklikkuse, st allkirjastamise, tagamiseks) isikutunnistuste alusel. Edukal autentimisel luuakse ühendus vajalikule infrastruktuuri serverile, mis annab võimaluse infrastruktuuri serveritel kaugelt DirectAccessi kliente juhtida.

2. Sisevõrgu tunnel (antud tunnel on kasutusel, et lubada DirectAccessi klientidel siseneda ülejäänud sisevõrguga). Kui eelpool kirjeldatud arvuti isikutunnistuse valideerimine on edukas, siis samal ajal kui DirectAccessi klient proovib saata liiklust sisevõrgu serverile, loob klient automaatselt teise IPsec ESP[16] sessiooni, olenevalt tunneli IPsec poliitikast. Tunnel ise on loodud pärast seda, kui arvuti sertifikaadi ja sisselogitud kasutaja konto on valideeritud. Peale edukat sisselogimist saab DirectAccessi klient ühenduda ükskõik millise sisevõrgu ressurssiga, milleks on talle õigused antud (Microsoft Corporation, 2010, *Client authentication*).

DirectAccessi puhul on võimalik kasutada ka nn tugeva autentimise meetodit. Sellisel juhul toetab standardne Forefront UAG DirectAccessi klientide autentimist, kasutades selleks

16 Encapsulating Security Payload

kasutajanime ja parooli. Tagamaks veelgi tugevamat turvet on võimalik lisada kahest tegurist koosnevat autentimist kiipkaardi ja ühekordse parooli abil (Microsoft Corporation, 2010, *Client authentication*).

Turvalisuse täiendamiseks on võimalik lisada seega kiipkaardi autentimist. Kiipkaardi autentimist saab kasutada mitmel erineval viisil:

Kasutaja autentimine – kiipkaardi autentimine on vajalik spetsiifilistel kasutajatel, olenevalt sellest, mis arvutit nad kasutavad.

Arvuti autentimine – kiipkaardi autentimine on vajalik spetsiifilistele arvutitele, olenevalt sellest, kes on kasutaja.

Sissepääsu autentimine – IPsec sissepääs vajab kiipkaardi autentimist enne ühenduse lubamist. Selline viis lubab kasutajatel ligi pääseda interneti ressurssidele ilma kiipkaardita, kuid vajab kiipkaardi autentimist enne kui kasutaja või arvutid saavad ühenduda sisevõrgu ressurssidega. Eelpool kirjeldatud viise võib ka omavahel kombineerida (Microsoft Corporation, 2010, *Client authentication*).

DirectAccessi üheks turvalahenduseks on ka OTP[17] ehk ühekordse salasõna rakendamise lahendus. OTP kasutusega on võimalik luua nn kahefaktoripõhine autentimine. Lühidalt öeldes põhineb OTP autentimine kasutaja ja arvuti sertifikaadi olemasolul. Seejuures nõuavad IPsec-i reeglid seda, et DirectAccessi klient omaks sertifikaati, mis on määratud serveri CA[18] poolt, et sisevõrku pääseda (Microsoft Corporation, 2010, *Client authentication*).

Peatudes aga turvalisusel, saavad DirectAccessi kliendid ühenduda sisevõrgu ressurssidele kahe erineva IPsec kaitse - „end-to-end“ ja „end-to-edge“- abil. Esimese, „end-to-end“, kaitsega saavad DirectAccessi kliendid luua IPsec-i sessiooni läbi DirectAccessi serveri igale serverirakendusele, millega neil ühendus on. Antud viis tagab kõrgeima kaitse taseme, kuna see võimaldab seadistada ligipääsu sätteid DirectAccessi serveris. Siinkohal on aga oluline märkida seda, et antud serveri rakendus peab töötama Windows Server 2008-s või Windows Server 2008 R2-s ning ühtlasi, et need kasutaksid IPv6 ja IPsec tehnoloogiat.

17 One Time Password Solution
18 Certificate Authority

Seevastu „end-to-edge“ kaitse abil saavutavad DirectAccessi kliendid IPsec sessiooni IPsec-i „gateway“ ehk serveri väravaga. IPsec-i serveri värav edastab kaitsmata liikluse, mis suundub edasi sisevõrgu tarkvara serveriteni. Kirjeldatud võimalus ei vaja seejuures IPsec-i sisevõrgus ja töötab IPv6-t võimaldavates rakenduste serverites. Et aga tagada kõige turvalisem ühendus, tuleks terves ettevõttes juurutada IPv6 ja IPsec-i tehnoloogiat, uuendada tarkvara serverid Windows Server 2008 või Windows Server 2008 R2-ni. See omakorda võimaldab autentimist ja ka krüpteerimist DirectAccessi kliendist sisevõrgu ressurssideni. Alternatiivina võibki kasutada aga „end-to-edge“ kaitset, kui on soov vältida IPv6 ja IPsec-i kasutamist terves ettevõtte võrgus (Microsoft Corporation, 2010, *DirectAccess Connections*).

1.4.2 OpenVPN-i autentimine ja turvalisus

OpenVPN Access Serverile on iseloomulik, et sellega on võimalik juhtida sisemisi andmebaase ning see on võimeline töötama erinevate populaarsete autentimismeetoditega. Sellisteks meetoditeks on: Local: Internal Database autentimine; PAM: süsteem autentimiseks kasutajatele, kellel on kontod Access Server Linuxi serveris; Active Directory/LDAP Server; RADIUS Server(s). Kasutaja autentimise teenus võib asetseda samas serveris, kus asub ka Access Server, samas võib teenus aga paikneda täiesti eraldi serveris, senikaua kuni server on kättesaadav Access Serveri poolt, kas siis privaatse või avaliku võrgu läbi (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administration Guide*, lk 8). Seejuures on OpenVPN-ile võimalik lisada ka kiipkaardiga autentimist, kuid selle jaoks on vajalik kasutusele võtta lisatarkvara OpenSC (Viktor Tarasov, 2012, *OpenSC – tools and libraries for smart cards*). Ka on OpenVPN-il olemas võimalus kasutada OTP funktsiooni, tänu millele saab kasutaja ettevõtte sisevõrku sisselogimisel kasutada ühekordseid paroole, suurendades seeläbi oluliselt ühenduse turvalisust.

OpenVPN-ile on omanäoline see, et OpenVPN ei autenti arvutit enne kui kasutaja sinna sisse logib ning klientide konfiguratsioonifailid ja Windowsi tarkvara paigaldamise pakett on igale kasutajale automaatselt loodud. Selleks peab kasutaja aga edukalt Connect Clienti sisse logima. See protsess toimub ilma administraatori sekkumiseta, kuivõrd antud toiming on eelnevalt seadistatud administraatori poolt, kes Access Serveri installeeris. Oluline on seejuures aga teada, et kui kasutaja on andmebaasist välja lülitatud või kasutajate hulgast kustutatud, siis ei saa

OpenVPN-i kasutaja enam luua ühendust OpenVPN-i serveriga, kuna ta ei saa enam ennast autentida. Eeltoodust tulenevalt pole administraatoril vajadust kustutada Access Serveris kasutaja jaoks loodud konfiguratsioonifaili. Ühtlasi peab aga silmas pidama, et iga genereeritud kliendi konfiguratsioon on kasutaja-lukustatud ning seda on võimalik kasutada ainult spetsiifilise kasutaja poolt. Kui kasutaja jagab oma kliendi konfiguratsioonifaili, ei saa seda teine kasutaja kasutada (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administration Guide*, lk 8). Selleks, et kasutajad saaksid serverist iseendale alla laadida VPN-i konfiguratsioonifaili on neil võimalik kasutada (kui see on eelnevalt seadistatud) Client Web Service-it. Client Web Service on turvaline veebiteenus, mis kasutab SSL-i - kaitstud HTTP protokolli veebibrauserites (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administration Guide*, lk 5).

Turvalisuse kohapealt võib OpenVPN-i puhul välja tuua selle, et vaikimisi Access Serveri Admin Web UI ja Client Web Serveri komponendid toetavad SSL/TLS[19] võimalusi, mis sisaldab ka nn SSLv2[20] šiffrit (teksti krüpteerimisemeetod teksti loetavuse ja tähenduse varjamiseks) komplekti. Paraku on aga SSLv2 protokoll muutunud vähem turvalisemaks versiooniks võrreldes SSL/TLS protokollidega. Et ühendust paremini turvata, tuleks seega välja lülitada SSLv2 koos selle juurde kuuluvate nõrkade šiffrite komplektidega. Seejuures uuendab Access Server regulaarsete ajavahemike järel VPN kliendi TLS sessiooni. See on vajalik, et hoida TLS-i ühenduse turvalisuse tõhusust. Sessiooni aega ennast saab administraator ka ise seadistada (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administration Guide*, lk 24).

OpenVPN-i on aga võimalik muuta turvalisemaks, kasutades selleks TLS-auth funktsiooni. TLS-auth funktsioon lisab HMAC[21] allkirja kõigile SSL/TLS pakettidele, tänu millele on võimalik kontrollida nende usaldusväärsust ja tõsta turvalisust. Näiteks aitab see kaitsta DoS[22] rünnakute vastu ning peita avatud võrguseadme ühenduskohti. Vajadusel suudab TLS-auth kahe seadme ebaturvalist andmevahetuse alustusprotesessi (kätlusprotsess) katkestada palju varasemas staadiumis (OpenVPN Technologies Inc., *HOWTO*).

19 Transport Layer Security protocol
20 Secure Socket Layer version 2 protocol
21 Hash-based message authentication code
22 Denial of Service (Attack)

1.4.3 Kokkuvõte

Oluliseks erinevuseks Microsoft DirectAccessi ja OpenVPN-i vahel on see, et Microsoft DirectAccessi puhul autentitakse arvuti enne, kui kasutaja üldse sisse logib, kuid see tagab sissepääsu ainult domeenikontrolleri ja DNS-i serveri vahel. Automaatne arvuti autentimine on autori hinnangul hea lahendus, kuivõrd traditsionaalselt on raske kontrollida, kas ja kuidas kasutajad virtuaalse privaatvõrguga ühenduvad. Lisaks on nii võimalik tagada, et arvuti operatsioonsüsteem oleks uuendatud enne, kui kasutaja loob ühenduse ettevõtte sisevõrguga. Lisaks saab antud moodusega vähendada tõenäosust, et sisenetakse arvutiga ettevõtte võrku, mis võib olla nakatanud mõne potentsiaalselt ohtliku arvutiviirusega.

Üldjoontes on aga OpenVPN-i ja DirectAccessi autentimisvõimalused küllaltki sarnased, mõlemad privaatvõrgud kasutavad kasutajate autentimiseks arvuti sertifikaate, kasutajakontosid ning paroolide isikutunnistusi. DirectAccess toetab seejuures kiipkaardiga autentimist, samas on seda võimalik implementeerida ka OpenVPN-ile lisatarkvara OpenSC abiga. Erinevuseks võib aga välja tuua selle, et OpenVPN-il on OTP funktsioon, mille abil on võimalik arvutite autentimise turvalisust muuta tunduvalt suuremaks, kuid standardsel DirectAccessil see puudub. OTP funktsiooni on DirectAccessi puhul võimalik kasutada siis, kui serveril on kasutusel UAG.

Tegelikkuses pakub aga Microsoft DirectAccess OpenVPN-ist turvalisemat kaitset, sest see kasutab IPv6 ja IPsec protokolli. Nimelt oli IPv4 algselt disainitud väheste turvalisuse meetmetega ning hiljem on IPv4-le lisatud juurde erinevaid turvalisuse lisasid. Samas on aga IPv6 disainimisel juba algselt arvestatud turvalisusega. Teadaolevalt on näiteks IPv6-e aadresside hulk ja nende pikkused tunduvalt suurem, kui on seda IPv4-l, tänu sellele on teiste võrkude skaneerimine ning ka viiruste paljunemine teistesse võrkudesse raskendatud, sest alamvõrkude arv on palju suurem (IPv4 or IPv6 – *Myths and Realities*, lk 49). Et tagada tugev ning kõige turvalisem ühendus, tuleks seega terves ettevõttes juurutada IPv6 ja IPsec-i tehnoloogiat. Samas võib aga IPv6-le üleminek ettevõttele kulukaks minna, olenevalt sellest, missugused seadmed parasjagu kasutusel on.

Eeltoodust tulenevalt selgus, et DirectAccessi kasutamiseks peab kasutaja arvuti olema

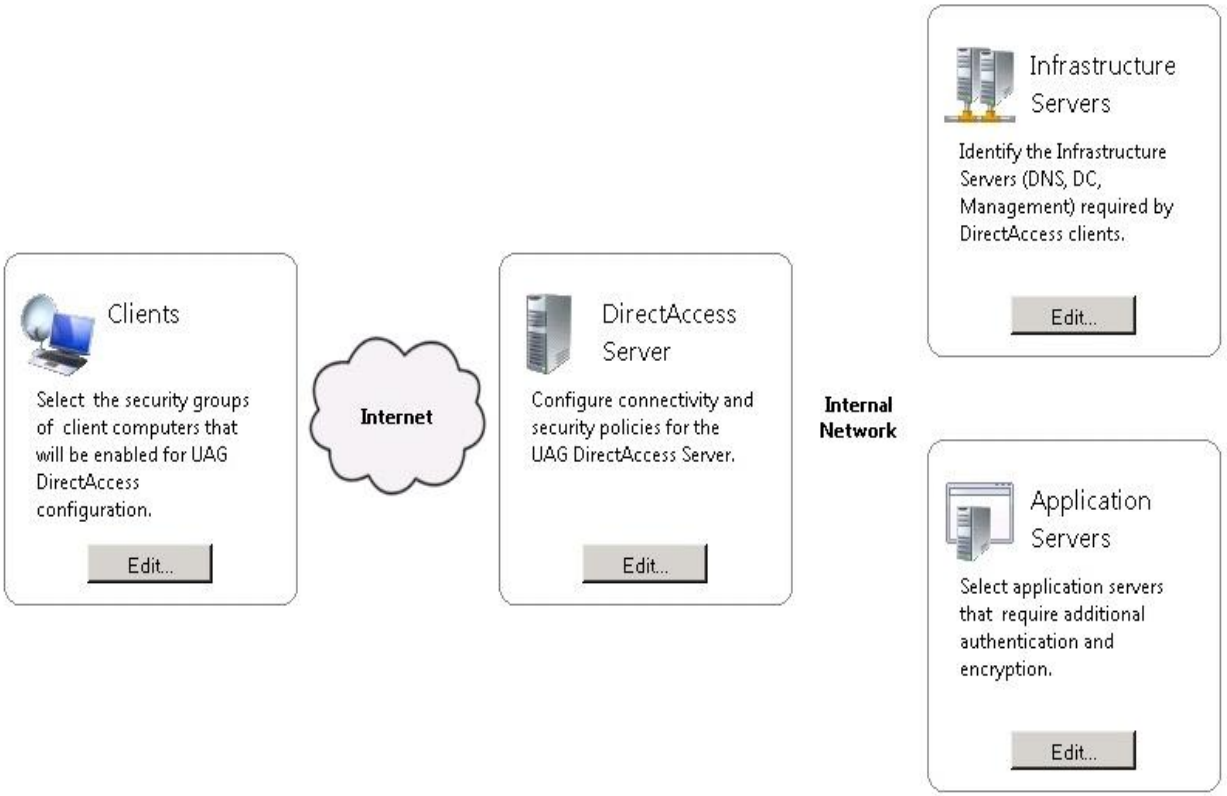
domeenis. See tähendab, et suure tõenäosusega on arvutit seadistanud IT-administraator, kellel on olnud võimalus arvutile paigaldada ettevõtte jaoks spetsiifilise tarkvara. OpenVPN-i kasutajal on seevastu VPN-i ühendust kergem luua, selleks ei pea kasutaja olema domeenis. Autentimiseks on kasutajal vaja sisse pääseda Connect Clienti, kus ta saab endale ühenduse loomiseks vajaliku rakenduse. Viimasel juhul võib aga tekkida probleeme siis, kui kasutaja ei ole piisavalt arvutiteadlik, kuid sellise kasutaja puhul tekitab üldse küsitavusi virtuaalse privaatvõrgu kasutamine.

Üheks erinevuseks vaadeldavate objekti vahel on ka asjaolu, et Microsoft DirectAccess kasutab algselt IPv6 protkolli ning kui see ei toimi, siis läheb varuvariandina tööle NAT6to4 funtsioon suhtlemaks IPv4-ja seadmetega. Kui ka see ei tööta (näiteks tulemüüri pärast), siis võetakse kasutusele IP-HTTPS protkoll. See kõik muudab DirectAccessi ühenduse komplekssemaks ning nutikamaks.

1.5 Graafiline kasutajaliides

1.5.1 Microsoft DirectAccessi kasutajaliides

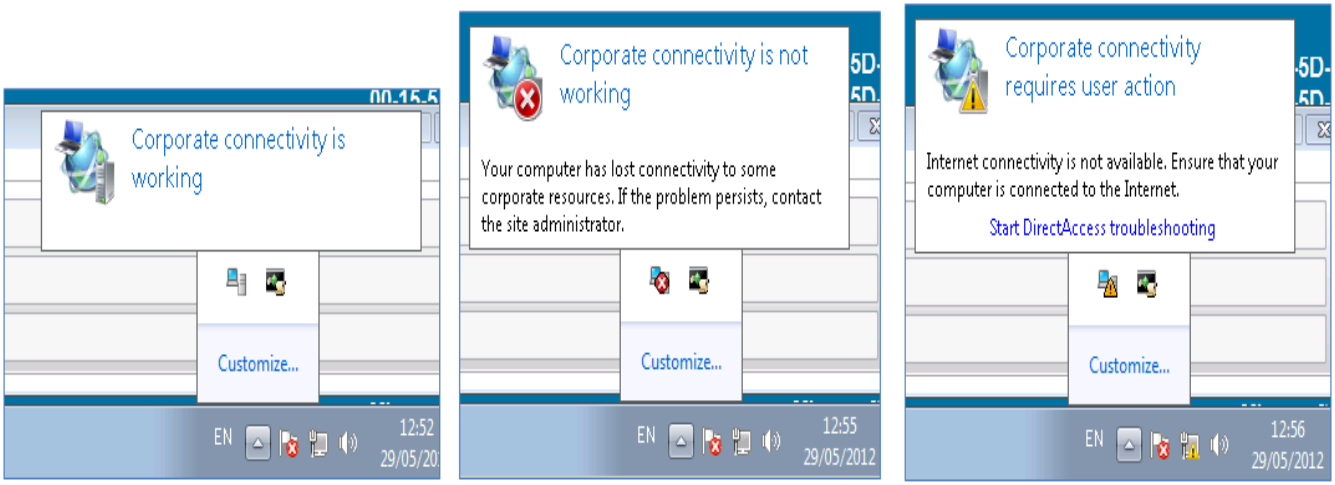
Esmapilgul tundub Microsoft DirectAccessi administraatori kasutajaliides üsna kasutajasõbralik. Valikud on oma funktsioonilt jaotatud nelja alamlõiku: Clients; DirectAccess Server; Infrastructure Servers; Application Servers (Joonis 1). Visuaalselt annab see parema ülevaate, näiteks sellest, mis valikud jäävad sisevõrku ja mis jäävad välisvõrku. Tegemist on seega küllaltki lihtsa ja arusaadava ülesehitusega. Alamlõigu „Clients“ abil on võimalik valida kasutajagruppe, kellel on õigus kasutada DirectAccessi. „DirectAccess Server“-i alt on aga võimalik konfigureerida ühenduse ja turvalisuse poliitikat, nagu näiteks ühenduse sätteid, sertifikaadi komponente ja kiipkaardi eeskirju. „Infrastructure Servers“ alt saab seevastu konfigureerida infrastruktuuri servereid. „Application Server“ võimaldab täiendada autentimist ja krüpteerimist, näiteks valida „end-to-end“ autentimist, millest oli juttu eelmises peatükis.



Joonis 1 - DirectAccessi administraatori kasutajaliides (MeirM [MSFT], 2010, *UAG DirectAccess Test Lab Guide CRL Check Update*).

„Microsoft Download Center"-ist[23] on võimalik alla laadida lisapakett DCA[24] Microsoft DirectAccessi kasutajale (Joonis 2). Tegemist on rakendusega, mis aitab organisatsioonidel vähendada IT-toele kuluvaid kulusid. Nimelt informeerib DCA mobiilset kasutajat jooksvalt selle ühenduse staatusest. Lisaks omab see võimalust kasutajal ühendust luua. DCA-l on ka diagnostika lisafunktsioon, et aidata mobiilsel kasutajal anda vajalikku infot IT-toele (Microsoft Corporation, 2010, *Microsoft DirectAccess Connectivity Assistant*).

23 http://www.microsoft.com/en-us/download/details.aspx?id=29039
24 DirectAccess Connectivity Assistant



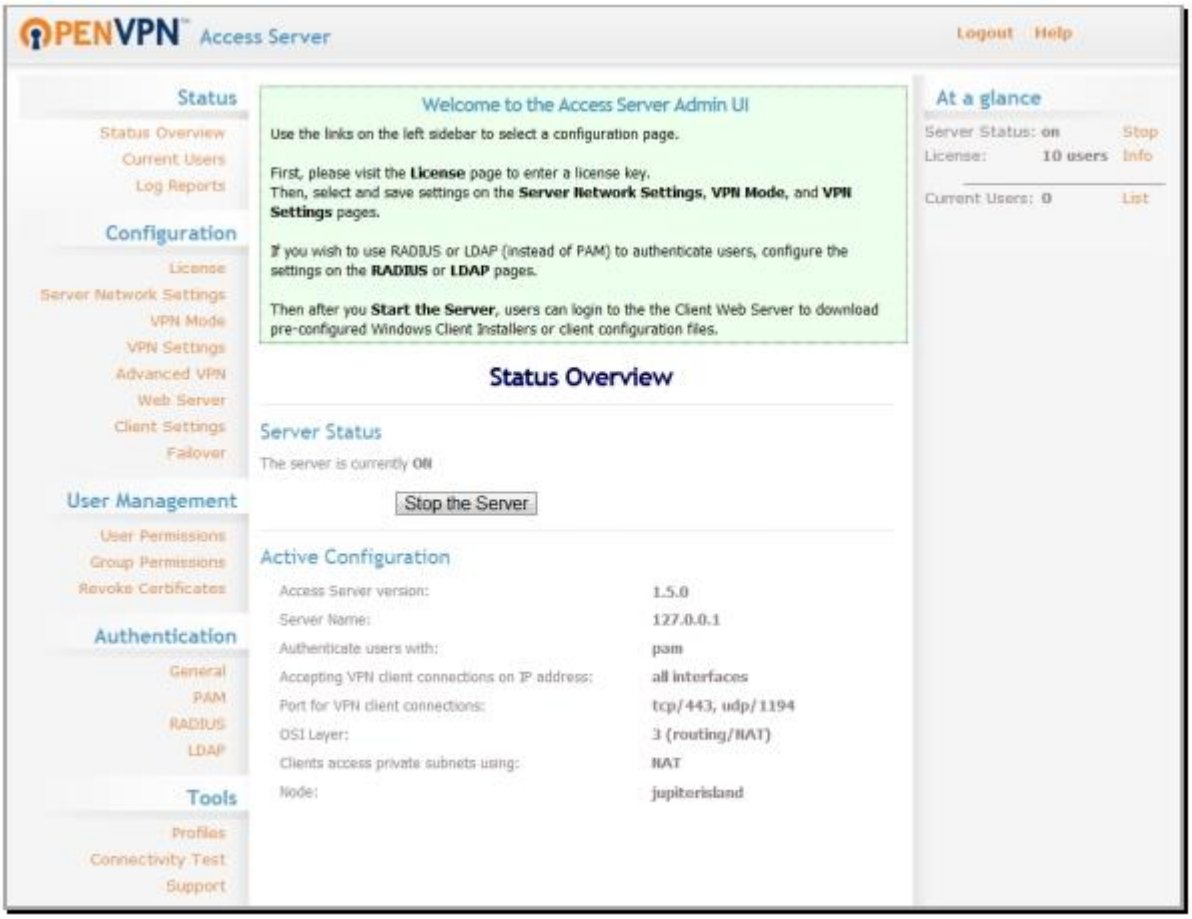
Joonis 2 - DirectAccessi Connectivity Assistant ehk ühenduse assistent (*Microsoft Corporation, DirectAccess Connectivity Assistant 2.0 is available*)

1.5.2 OpenVPN-i kasutajaliides

Administraatori sisselogimiseks on OpenVPN-il kasutusel Admin Web UI. Veebilehitseja võib administraatorit hoiatada olenevalt sellest, kas serveri sertifikaat on antud veebilehitsejas usaldusväärne. Pärast seda, kui veebilehitsejale antakse luba jätkata, ilmub ekraanile OpenVPN-i Admin Web UI sisselogimise aken (Joonis 3). Järgnevalt on antud aknasse vaja sisestada kasutajanimi ning parool. Sellega on OpenVPN-i sisselogimine kasutaja jaoks igati arusaadavaks ning lihtsaks tehtud.

Joonis 3 – Admin Web UI sisselogimise aken (*OpenVPN Technologies Inc., 2010, OpenVPN Access Server System Administrator Guide*, lk 14)

Access Server-isse sisselogimisel avaneb laiem veebipõhine vaade (Joonis 4), kus vasakul pool lehe ääres on järjestatud suur hulk võimalike funktsioonide pealkirju. Kui neile hiirega klõpsata, siis on lehe keskosas võimalik nende funktsioonide parameetreid täpsemalt muuta. Paremal pool akna ääres on pealkiri „At a glance“, kus on jooksev info selle kohta, kas server on sees, mitu litsentsi on olemas ja kui palju kasutajaid on antud hetkel ennast sisse loginud.

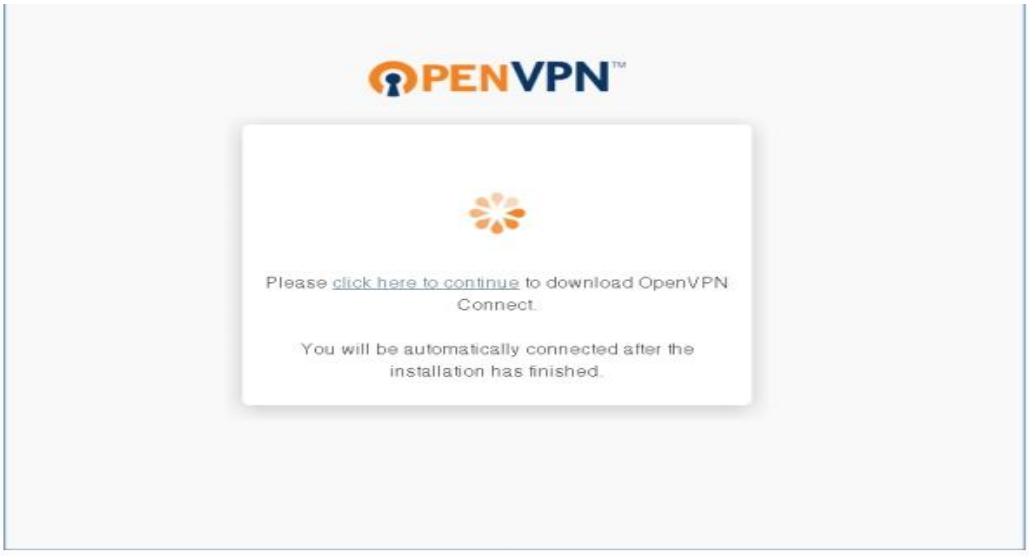


Joonis 4 – Admin Web UI, OpenVPN-i graafiline administraatori kasutajaliides (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 15)

Tavakasutaja saab OpenVPN-i Access Serverile ligi Connect Clienti kasutades. Selleks peab kasutaja minema teatud aadressile oma veebilehitsejas. Veebilehitseja võib tavakasutajat hoiatada selle eest, kas serveri sertifikaat antud veebilehitsejas on ikka usaldusväärne. Pärast seda, kui veebilehitsejale antakse tavakasutaja poolt luba jätkata, ilmub ekraanile sisselogimise aken (Joonis 5).

Joonis 5 - Connect Client-i sisselogimise leht (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 44)

Sisselogimise aknas on kasutajale antud kaks valikut - kas sisse logida või ühenduda. Kui kasutaja valib ühendumise („Connect“), siis esimesel korral on kasutajal võimalik allalaadida OpenVPN Connect-i paigaldamise rakendus. Sellisel juhul küsitakse kasutajalt uuesti, kas ta ikka soovib installeerimisega jätkata (Joonis 6). Kui jah, siis tuleb kasutajal aktiivsele tekstile hiirega vajutada.



Joonis 6 – Installeerimiseks kasutajalt kinnituse küsimine (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 45)

Kui installeerimine on valmis, siis jätkab veebilehitseja ühenduse loomist VPN Serveriga. Juhul, kui ühendus on edukalt loodud, näeb kasutaja OpenVPN-i staatust, näiteks seda, kui kaua on kasutaja ühenduses olnud ning kui palju andmeliiklust on saadetud ning kätte saadud (Joonis 7).

Joonis 7 - Ühenduse staatus (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 46)

Ühtlasi on OpenVPN-i Connect Clientil olemas kasutajaliidese tegumiriba, kus kuvatakse OpenVPN-i Connect Clienti programmi ikoon (Joonis 8). Selle abil on kasutajal võimalik ühenduda ja lõpetada ühendus OpenVPN-i Access Serveriga. Lisaks on seal ka otselink, mis käivitab veebilehitsejas Connect Clienti-liidese.

Joonis 8 – Connect Clienti tegumirea ikoon (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 46)

Kui kasutaja aga valib sisselogimise (vt joonist 5), siis on tal võimalik alla laadida erinevaid installeerimisvariante vastavalt oma operatsioonsüsteemile (Joonis 9). Ühtlasi saab kasutaja sealt alla laadida erinevaid administraatori poolt eelseadistatud profiile, näiteks serveripõhiseid profiile, kasutajapõhiseid profiile ning kasutaja automaatset sisselogimise profiili vastava kasutaja jaoks. Mõned neist profiilidest ei ole kõikide kasutajate jaoks kättesaadavad, see nimelt oleneb sellest, millised on nende kasutajate õigused. Lisaks on kasutajal sisselogimisel olemas nupp „Connect“, mis asub sisselogimislehe ülemises vasakus nurgas, ühendumaks antud isikut Access Serveriga. Veel on kasutajatel, kellele on omistatud administraatori õigused, lisanupp „Admin“, mille abil saab antud kasutaja ligi Access Serverile. Paremal üleval on ka väljalogimise nupp „Logout“.

Joonis 9 – Sisselogimisel järgnev aken (OpenVPN Technologies Inc., 2010, *OpenVPN Access Server System Administrator Guide*, lk 47)

1.5.3 Kokkuvõte

Autori hinnangul jätab Microsoft DirectAccessi administreerimispaneel professionaalse mulje, arusaadavalt on ära näidatud, mis sätted jäävad ettevõtte seisukohast sisevõrku ning mis välisvõrku. Põhifunktsioonid on jaotatud nelja suuremasse rühma ning kasutajal on lihtne mööda ettenäidatud juhiseid liikuda. Samas on funktsioonidele lisatud ka graafiline pilt ja täpsustav tekst, mis aitab kasutajal paremini aru saada antud funktsiooni olemusest.

OpenVPN-i serveri administeerimisliides on aga üsna erinev Microsoft DirectAccessiga. Esmapilgul tundub autorile OpenVPN-i administraatoriliides veidi keerukas, kuna sisaldab väga palju infot ning erinevaid pealkirju. Täpsemalt pole ära märgitud, mis etapi kaupa tuleks serverit seadistada. Vaid esmakordsel sisselogimisel on tervitusaknas lühidalt selgitatud, milliseid menüüosi tuleb administraatoril külastada ning mida seal seadistada. Autor leiab, et tegemist on vägagi pealiskaudse juhendiga. Kuna algne menüüvalik on suur, siis jõuab funktsiooni muutmiseni kiirelt vaid sel juhul, kui administraator juba teab, mida teha on vaja. Seega võiks ka OpenVPN olla rohkem Microsoft DirectAccessi stiilis, kus on rohkem graafilisi pilte ning selgitusi. OpenVPN-i administraatori kasutajaliidest kasutades tekkis autoril küsimus, miks on Access Serveri paremal pool, „At a glance“ pealkirja all, niivõrd palju vaba ruumi jäetud. Lisaks võiks seal olla võimalus üldse ära peita kogu „At a glance“ menüüosa, mille tulemusel oleks keskmises aknas oleva teksti jaoks rohkem ruumi. Samas võiks administraatoril olla võimalik „At a glance“ tulpa lisada või eemaldada elemente nagu näiteks info aktiivsete kasutajate IP-aadressite, serveri töösolekuaja ning administraatori sessiooniaja kohta. Väljanägemiselt tundub autorile, et OpenVPN-i Access Server sarnaneb mõne vanema ruuteri administraatori paneeliga.

Seevastu OpenVPN-i Connect Client jätab autorile märksa parema mulje, sest väljanägemisele on rohkem rõhku pööratud näiteks varjutekitamise efektiga. Ka on antud sisselogimise aken kasutaja jaoks igati lihtne ning loogiline. Kasutaja võib endale sobivalt valida, kas ta soovib kohe OpenVPN-i ühendusega ühenduda või tahab ta selle asemel hoopis kasutajakontosse sisse logida. Samas on kasutajal ka sisselogides väga lihtsalt virtuaalse privaatvõrguga koheselt ühenduda, kuna avanenud akna ülaääres on olemas „Connect“ nupp. Seega kui kasutaja näiteks ekslikult sattus sisselogimislehele, siis võib ta seal koheselt ettevõtte võrguga ühenduda ning ta ei pea seejuures eelnevale lehele tagasi minema või ennast sisselogimislehelt välja logima.

Lisaks toob autor välja, et kui OpenVPN-i tarkvara on arvutile peale installeeritud, siis peaks Windowsi tegumireal oleval Tray ikoonil võimalik kasutajal valida, kas tarkvara käivitatakse automaatselt või mitte. Seega võiks OpenVPN-i Connect Clientil olla näiteks „linnukese“ koht, kus saaks valida, kas OpenVPN käivitub automaatselt, kui Windows-isse sisse logitakse.

Microsoft DirectAccessi Connectivity Assistanti osas leiab autor, et igal DirectAccessi kasutajal peaks olema installeeritud antud lisatarkvara, kuna see võimaldab kasutajal saada kiiret ülevaadet sellest, kas ühendus ettevõtte sisevõrguga on aktiivne või mitte. Tehes aga tööd virtuaalse privaatvõrguga omab ühendus kriitilist tähtsust, mida võiks võrrelda sellise vajaliku abimehega nagu on seda ka Internet Accessi riba, mis näitab, kas interneti ühendus on arvutis olemas. Lisaks aitab see vähendada IT-administraatori tööd, kuna antud rakendus omab nn tõrkeotsingu funktsiooni, mille läbi võib kasutaja ise tekkinud probleemist jagu saada.

1.6 Maksumus

1.6.1 Microsoft DirectAccessi maksumus

Käesoleval ajal on Microsoft DirectAccessi kasutamiseks vajalik endale soetada Microsoft Windows Server 2012 litsents. Microsoft Windows Server 2012 soetamiseks pakub Microsoft nelja erinevat versiooni:

1) Datacenter – täielikult Windows Serveri poolt tagatud funktsionaalsus koos piiramatu virtuaalse operatsioonsüsteemide arvuga. Antud verisooni on võimalik soetada jaehinnaga 4809 dollarit (3675,20 eurot), kuid lõplik hind sõltub konkreetsest partnerist.
2) Standard – erinevuseks eeltoodud versiooniga on see, et standardversioon on mõeldud madala või mittevirtuaalse keskkonna jaoks. Nimetatud versioon omab täielikku Windows Serveri funktsionaalsust koos kahe virtuaalse operatsioonsüsteemi võimalusega. Standard versiooni jaehind on ligi 882 dollarit (674,05 eurot).
3) Essentials – käesolev versioon on mõeldud väikeettevõtete keskkondade jaoks. Tegemist on lihtsama liidesega, mis on eelhäälestatud ühendumaks pilveteenustega ning ei oma virtuaaliseerimisõigusi. Antud versiooni omapäraseks on ka see, et see on mõeldud kuni 25-le kasutajale. Versiooni jaehind on ligikaudu 501 dollarit (382,88 eurot).
4) Foundations - tegemist on serveriga, millel on eelinstalleeritud Windows Server 2012 ning mille litsents kehtib ainult teatud riistvarale. Antud versioon omab üldotstarbelise serveri funktsionaalsust ning virtualiseerimisõigusi. Erinevuseks teistest versioonidest on see, et selle limiidiks on 15 kasutajat (Microsoft Corporation, 2013, *Windows Server 2012 How to Buy*).

Eeltoodust tulenevalt oleneb Microsoft Windows Server 2012 maksumus suuresti selle kasutajate arvust ning virtualiseerimise vajadusest. Lisaks pakub Microsoft võimalust Standardi või Datacenteri versiooni tasuta 180 päeva vältel proovida (Microsoft Corporation, 2013, *Download Windows Server 2012*). Selleks, et välja selgitada Microsoft Windows Server 2012 edasimüügihind Eestis, esitas käesoleva töö autor vastava hinnapäringu Eestis tegutsevale Microsofti partnerile, IT-haldusteenuse osutamist pakkuvale ettevõttele. Hinnapakkumiseks tehti autorile Microsoft Windows Server 2012 Standard versiooni litsentsi eest 842.66 eurot, millele omakorda lisandub käibemaks. Seega on Standard versiooni edasimüügihind võrreldes jaehinnaga märkimisväärselt kõrgem.

Huvipakkuvaks siinjuures on aga ka asjaolu, et Microsoft Windows Server 2012 on suhteliselt uus serveri tarkvara. Nimelt sai see alguse 30.10.2012. a. Tavatuge antud versioonile pakutakse kuni 09.01.2018. a (Microsoft Corporation, 2013, *Support*). Sellest tulenevalt leiab autor, et antud versiooni litsentsi ei tasuks võtta kauemaks kui viieks aastaks, kuivõrd suure tõenäosusega tuleb Microsoft Corporation siis välja uue tarkvaralahendusega.

1.6.2 OpenVPN-i maksumus

OpenVPN Access Serveri litsentsi maksumuseks on 5 dollarit iga kliendi ühenduse eest aastas. Soetatavate litsentside arv ettevõtte poolt on minimaalselt 10. Seega peab OpenVPN Access Serveri litsentsi ostja arvestama vähemalt 50 dollarilise kulutusega. OpenVPN Access Serveri litsentse saab osta rohkem kui üheks aastaks. Kulusid saab kokku hoida sellega, kui litsents osta pikemaks ajaks kui üks aasta. Näiteks kui litsentsi kasutustähtajaks on 2 aastat, on litsentsi hinnaks 9.50 dollarit ühe kliendi litsenti eest, mis annab seega 5% soodustust. Kui osta OpenVPN Access Serveri litsents 3 aastaks on ühe kliendi litsentsi tasu 13.50 dollarit, mille puhul on allahindluseks 10%. Kui osta OpenVPN Acces Serveri litsents 4 aastaks, on ühe kliendi litsentsi tasu 17 dollarit, mis teeb allahindluseks 15%. Samas, kui OpenVPN Access Serveri litsents osta kokku 5 aastaks, tasutakse selle eest 20 dollarit ühe kliendi litsentsi eest. Allahindlus sellisel juhul on 20% ning moodustab ettevõtte minimaalseks kuluks 200 eurot (OpenVPN Technologies Inc., 2013, *Pricing Guide*).

Seejuures on OpenVPN Access Serverit võimalik kasutada tasuta kahe kliendi ulatuses. Tegemist on võimalusega, mis on mõeldud antud serveri testimiseesmärgil (OpenVPN Technologies Inc., 2013, *Pricing Guide*). OpenVPN Community versioon on aga kasutajatele tasuta, kuid see ei anna administraatorile kõiki neid võimalusi, mida pakub OpenVPN Access Server.

1.6.3 Kokkuvõte

Antud teema kokkuvõtteks võib öelda, et kuigi Microsoft Corporation pakub küll 180-päevast Microsoft Server 2012 testimise võimalust, siis OpenVPN-i eeliseks on autori hinnagul just suuresti see, et sellel on olemas Community versioon, mille eest tasu ei nõuta ning millele ajalist piirangut seatud ei ole.

Open VPN-i Access Serveri tasulise versiooni litsentsi on aga autori arvates mõistlik võtta pikemaks ajaks, kuna lähtuvalt eelpool kirjeldatust on hind sellisel juhul tunduvalt soodsam. Näiteks 5-aastase kasutusajaga on litsents tunduvalt odavam, kui võrrelda seda üheaastase litsentsiga. Microsoft Server 2012 puhul ei sõltu hind kasutusajast vaid kasutajate ja virtuaalse operatsioonsüsteemide arvust, mis on lähtuvalt vajadustest jaotatud erinevateks tarkvarapakettideks. Samas on oluline aga märkida, et Microsoft Server 2012 puhul kestab põhitugi kuni 2018. aastani. Seega kui antud versioon võtta viieks aastaks, usub autor, et tõenäoliselt on selleks hetkeks kättesaadavaks tehtud juba uus Microsoft Serveri versioon.

Kui OpenVPN Access Server võtta kasutusele kokku viieks aastaks, maksab ühe kliendi litsents 20 dollarit ehk 15.31159 eurot. Kui võrrelda seda Microsoft Server 2012 Standard jaehinna maksumusega, saab 882 dollari ehk ligi 675.24115 euro eest 44 OpenVPN-i litsentsi viieks aastaks. Samas kui võtta arvesse Eestis oleva partneri pakutavat hinda, siis saab ostja endale antud rahasumma eest 55 OpenVPN Access Serveri litsentsi. Datacenteri versiooni hinna, 4809 dollari ehk 3681.672025 euro, eest saab aga ligikaudu 240 Access Serveri litsentsi. Microsoft Server 2012 Essentialsi maksumuseks on 501 dollarit, seega saab antud raha eest ostja ligikaudu 25 litsentsi ehk siis sama palju, kui palju on Essentialsi maksimaalne kasutajate arv.

Võrreldes Microsoft Server 2012 ning OpenVPN versioonide maksumust, võib kokkuvõtteks öelda, et autori hinnangul pakub OpenVPN ettevõttele tunduvalt soodsamat lahendust, kui teeb seda Microsoft Corporation, kuivõrd OpenVPN-il on olemas tasuta Community versioon, millele pole kehtestatud ajalist piirangut.

1.7 Esimese peatüki vahekokkuvõte

Bakalaureusetöö esimeses pooles selgus, et Microsoft DirectAccess on VPN-i taoline tehnoloogia, mis hõlmab enda alla avalikke ning privaatseid võrke, luues kasutajagruppe, kes on eraldatud teistest internetikasutajatest ja kes saavad üksteisega suhelda nagu nad oleksid privaatses võrgus. Eeltoodud kirjeldus vastab ka OpenVPN-ile. Nagu aga töös selgus, esineb neil kahel virtuaalsel privaatvõrgul teatud erisusi. Näiteks nõuab Microsoft DirectAccess Windows 7 Ultimate ja Windows 7 Enterprise versiooni ning Windows Server 2008 R2-te või sellest uuemat serveritarkvara. Lisaks on ühenduse loomise jaoks tarvis kahte võrguadapterit ning kahte avalikku ja järjestikust IP-aadressi. Antud nõuded pole aga vajalikud OpenVPN-i puhul, mistõttu on viimane palju paindlikum, sest OpenVPN-i on võimalik installeerida nii Windowsi kui Linuxi keskkonnas. Seejuures ei saa aga jätta märkimata, et 2010. aastast on administraatoritel võimalik serverile lisada serveri täienduspakett UAG. Samas tuleb aga UAG serverile eraldi peale installeerida, mis on administraatori jaoks lisatööks ning ka lisakulutuseks. Kuivõrd UAG näol on tegemist niivõrd olulise lisapaketiga, siis leiab autor, et see peaks DirectAccessiga kohe algusest peale kaasas olema.

Ühenduse kohapealt aga selgus, et oluliseks erinevuseks OpenVPN-i ja Microsoft DirectAccessi vahel on see, et viimane on loodud ühenduma automaatselt, kui kasutaja arvuti internetti siseneb. Ka annab DirectAccess administraatoritele võimaluse enne kasutaja sisselogimist muuta arvuti ettevõtte reeglitele vastavaks. DirectAccessi plusspoolele võib seega nimetada, et see on automaatne ja ei nõua eraldi seadistamist, mida seevastu nõuab standardne OpenVPN-i pakett. OpenVPN-i ja Microsoft DirectAccessi on võimalik eristada veel ka IPv6 tehnoloogia kasutamise põhjal, DirectAccess nimelt omab täielikku valmisolekut IPv6 jaoks, OpenVPN pakub aga täielikku tuge IPv6 jaoks alles OpenVPN 2.3 versioonis, mis tähendab, et täielik IPv6 tugi on kasutajatele kättesaadav alates 2013. märstikuu lõpust. Siinkohal on aga oluline märkida, et IPv6 tehnoloogiat veel laialdaselt ei kasutata, mistõttu ei saanud seda varasemalt pidada OpenVPN negatiivseks küljeks. On aga ilmselge, et aja jooksul IPv6 protokolli populaarsus suureneb, mistõttu märgib selle kasutusvõimalus tulevikus kindlasti oluliselt suuremat rolli. Ilmselt on sellele on mõelnud OpenVPN-i tarkvaraarendajad, kui lisasid OpenVPN-ile täieliku IPv6 toe. Samas on aga DirectAccess niivõrd leidlik lahendus, et kui DirectAccessi kasutaja ei saa mingil põhjusel IPv6 võrku kasutada, siis kasutab DirectAccess automaatselt NAT6to4 või

Teredo IPv6 üleminekutehnoloogiat ning kui ka see ei aita, siis püüab kliendi arvuti serveriga automaatselt IP-HTTPS-i abil ühenduda. Eeltoodust tulenevalt on DirectAccessi ühenduse protsess väga töökindel ning see on hästi läbimõeldud. Just viimati nimetatud omaduste tõttu leiab autor, et Microsoft DirectAccessi ühenduse protsess mõistlikum ja parem, kui on seda OpenVPN-i oma, sest see on varasemalt olnud ja on ka praegu rohkem läbinägelikum.

Nagu eelnevalt nimetatud on DirectAccessile iseloomulik see, et arvuti autentitakse enne, kui kasutaja üldse sisse logib. Antud lahendus on autori hinnangul hea, kuna traditsiooniliselt on raske kontrollida, kas ja kuidas kasutajad virtuaalse privaatvõrguga ühenduvad. Ühtlasi on sellisel juhul võimalik tagada, et arvuti operatsioonsüsteem oleks uuendatud enne, kui kasutaja ettevõtte sisevõrguga ühenduse loob. Nii saab aga vähendada ka tõenäosust, et ettevõtte võrku sisenetakse arvutiga, mis on nakatanud mõne arvutiviirusega ning kätkeb endas seeläbi olulist turvariski. Autentimise juures on oluline aga välja tuua, et DirectAccessil puudub OTP ehk ühekordse parooli kasutamise funktsioon, selline võimalus on aga OpenVPN-il, muutes seeläbi arvutite autentimise turvalisuse oluliselt suuremaks. Samas on OTP funktsiooni DirectAccessil võimalik kasutada siis, kui server kasutab UAG-d. Üldiselt pakub aga Microsoft DirectAccess autori hinnangul OpenVPN-ist turvalisemat kaitset, sest see kasutab IPv6 ning IPsec protokolli. Seejuures peab DirectAccessi puhul kasutaja arvuti olema domeenis, mis tähendab, et arvutit saab eelnevalt seadistada IT-administraator, kellel on võimalik arvutile spetsiaalne, ettevõttele sobilik, tarkvara paigaldada.

Välisilmelt jätab autori hinnangul Microsoft DirectAccessi administreerimisepaneel professionaalsema mulje ning seal on väga selgelt ära näidatud, millised sätted jäävad ettevõtte seisukohast sisevõrku ning mis välisvõrku. Põhifunktsioonid on jaotatud nelja suuremasse rühma ning kasutajal on lihtne mööda etteantud juhiseid liikuda. Seejuures on funktsioonidel ka graafiline pilt ja täpsustav tekst, mis aitavad väga hästi funktsioonide olemusest aru saada. OpenVPN-i välisilme on aga käesoleva töö autori hinnangul korrapäratu, sest see sisaldab endas palju infot ja erinevaid pealkirju. Ühtlasi annab OpenVPN vaid pealiskaudse juhendi sellest, kuidas serverit seadistada. Ka on autori arvates Access Serveri parempoolses menüüosas liialt palju vaba ruumi, mida võiks täita vajaliku informatsiooniga näiteks selle kohta, kui pikk on serveri töösolekuaeg ning administaatori sessiooniaeg. Ühtlasi leiab autor, et kui OpenVPN-i tarkvara on arvutile peale installeeritud, siis peaks Windowsi tegumireal oleval Tray ikoonil

võimalik valida, kas tarkvara käivitatakse automaatselt või mitte. Seejuures võiks ka OpenVPN Connect Clientil olla mingisugune märkimise koht, kust valida, kas OpenVPN käivitub automaatselt, kui kasutaja Windowsi sisse logib. Eeltoodud põhjustel eelistab käesoleva töö autor välisilme poolest Microsoft DirectAccessi, kuid ka DirectAccessi puhul peab autor vajalikuks arvutile installeerida lisatarkvara - Connectivity Assistant, mis annab kiire ning mugava ülevaate sellest, kas ühendus ettevõtte sisevõrguga on aktiive või mitte.

Maksumuse osas on aga autori hinnangul mõistlikum OpenVPN-i lahendus, kuna OpenVPN-il on olemas tasuta Community versioon, millele pole kehtestatud ajalist piirangut. See aga võimaldab ettevõttel oluliselt oma kulutusi kokku hoida. Microsoft DirectAccessi jaoks vajalik Microsofti Server 2012 serverilahendus on tasuta kasutatav üksnes 180-päeva vältel, mistõttu pole sellisel juhul tegemist toimiva ning jätkusuutliku lahendusega ettevõtte jaoks.

2. Küsitlus

Käesoleva bakalaureusetöö küsitlus (Lisa 1) on viidud läbi erinevate Eesti riigiasutuste ning eraettevõtete IT-juhtide, süsteemiadministraatorite, võrguadministraatorite ning projektihaldurite seas aastatel 2012 ja 2013. Küsitlus viidi läbi võimalikult erinevate ettevõtete ja organisatsioonide töötajate vahel.

Küsitlus ise oli anonüümne ning sellele vastamine võttis aega 15-20 minutit. Küsimustikus oli kokku 4 küsimust. Esitatud küsimustikule vastati kirjalikult, e-posti vahendusel. Enne küsitluse saatmist aadressaadile võttis käesoleva töö autor isikutega ühendust ka telefoni teel, pidades vajalikuks ennast ja oma töö teemat eelnevalt tutvustada ning küsida isikutelt nõusolekut neile küsitluse edastamiseks. Mõlemal juhul, nii telefoni teel kui e-posti vahendusel, sai isikutele selgitatud, et küsitlus on anonüümne ning kui mõnele küsimusele vastata ei osata, siis palus autor sinna kirjutada vastuseks „ei tea“. Küsitlus esitati kokku 10-le isikule, oma vastused tagastas neist 5 küsitletut.

Üheks küsitlusele vastajaks oli riigile kuuluva äriühingu, kus töötab kokku ligi 60 inimest, IT-projektijuht. Teiseks vastajaks oli töötaja, kelle ametinimetuseks on juhtivspetsialist. Antud isik töötab riigiasutuses, kus on kokku üle 400 töötaja. Küsitlusele vastas ka IT teenuste projektijuht, kes töötab ministeeriumis, mille valitsemisalasse kuulub mitmeid ameteid ja inspektsioone ning kus töötajaid on kokku 5000. Neljandaks vastajaks oli IT-osakonna juhataja ning ettevõtte, kus ta töötab kuulub Eesti Vabariigile, töötajaid on seal ligikaudu 150. Viiendaks vastajaks on ühe Eesti telekommunikatsioonіettevõtte vanem võrguadministraator. Viimase asutuse näol on tegemist eraettevõttega, kus on kokku pea 2000 töötajat.

2.1 Küsitluse tulemused

2.1.1 Esimene küsimus – kas hetkel on firmas kasutusel mõni VPN lahendus, kui jah, siis milline?

Küsitluse esimene küsimus – kas hetkel on firmas kasutusel mõni VPN lahendus, kui jah, siis milline? - on vajalik, et selgitada välja see, milliseid lahendusi vastavad ettevõtted kasutavad ning seeläbi ka eelistavad. Ühtlasi võimaldab antud vastustest näha, kas küsitletute ettevõttetes on kasutusel näiteks DirectAccess või OpenVPN.

Esimene küsitluses osalenud isik vastas, et nende ettevõttes on kasutusel OpenVPN. Teise küsitletu ettevõttes kasutatakse aga Juniper SRX VPN lahendust erinevate büroode ühtse võrgu loomiseks. Kolmas isik märkis, et tema ei oska kindlat lahendust öelda, sest asutuse poolt on antud sülearvutid, mis on eelnevalt seadistatud IT-osakonna poolt ning virtuaalsetesse privaatvõrkudesse saab ainult nende seadmetega. Neljas küsitluses osalenu vastas, et nende ettevõttes kasutatakse OpenVPN-i ja Win7 IKEv2-e, mobiilide jaoks aga L2TP/IPsec-i. Viies osalenu vastas, et nende ettevõttes on kasutusel Fortinet SSL ja IPsec VPN.

2.1.2 Teine küsimus - miks on valitud antud VPN tehnoloogia?

Küsitluse teine küsimus – miks on valitud antud VPN tehnoloogia – on autori hinnangul vajalik selleks, et selgitada välja, kas vastava virtuaalse privaatvõrgu lahendus on üldse põhjendatud või võiks selle asemel või selle kõrval kasutada hoopiski mingit muud privaatvõrgu lahendust nagu näiteks Microsoft DirectAccessi või OpenVPN-i.

Esimene küsitlusele vastanu leidis, et OpenVPN-i tarkvara on valitud seepärast, et see on vabavaraline, sobib kõikidele platvormidele ja toetab mitut autentimisviisi. Teine küsitletu vastas, et Juniper SRX VPN eeliseks on, et selline lähenemine annab võimaluse hallata kõiki seadmeid, mis vajavad võrku (tööjaamad, printerid jne). Kolmandal küsitluses osalenul puudub aga teave selle kohta, miks on nende ettevõttesse vastav VPN tehnoloogia üldse valitud. Neljas isik vastas, et OpenVPN-i tehnoloogia on valitud seepärast, et see on tasuta ning selle kasutuselevõtt oli lihtne; IKEv2 on kasutusel, kuna OpenVPN vajab Win7-ga administraatori

õigusi ning L2TP/IPsec seetõttu, et see on IOS ja Androidi poolt vaikimisi toetatud. Viies isik vastas, et Fortinet toodab UTM (Unified Threat Management) seadmeid, mis sisaldavad ka VPN piiramatu kasutajatearvu litsentsiga. Ettevõttel on seda mugav kasutada, kuna on üks turvaseade, mida hallata.

2.1.3 Kolmas küsimus - millised on hetkel kasutusel oleva VPN tehnoloogia puudused?

Kolmas küsimus – millised on hetkel kasutusel oleva VPN tehnoloogia puudused – on autori hinnangul vajalik selleks, et selgitada välja antud virtuaalse privaatvõrgu miinuspooled ning kas neid oleks võimalik kõrvaldada näiteks Microsoft DirectAccessi või OpenVPN-i kasutuselevõtuga.

Esimene küsitlusele vastanu, kelle ettevõttes kasutatakse OpenVPN-i, leidis, et vastava privaatvõrguga on raske hallata domeeni mittekuuluvaid seadmeid ning selle autentimist ei anna kuidagi automatiseerida. Teine isik, kelle asutuses on Juniper SRX VPN, vastas, et antud riistvaraline VPN võimaldab ainult kindlate asukohtade vahelist liiklust. Kolmas isik vastas, et tal puudub teave vastava VPN tehnoloogia puuduste kohta. Neljas vastanu, kelle ettevõttes on kasutusel samuti OpenVPN, leidis, et selle puuduseks on administraatori õiguste vajamine Win7-e ja 8 puhul; IKEv2 miinuseks on, et WinXP ning mobiilsed seadmed seda ei toeta. Viies vastaja leiab, et hetkel häirivaid puudusi ta märganud ei ole.

2.1.4 Neljas küsimus - kas oled mõelnud olemasolevat VPN lahendust vahetada OpenVPN-i või Microsoft DirectAccessiga, miks?

Neljas küsimus – kas oled mõelnud olemasolevat VPN lahendust vahetada OpenVPN-i või Microsoft DirectAccessiga, miks? - on käesoleva töö autori arvates vajalik selleks, et analüüsida, kas vastanud ise arvavad, et hetkel kasutatava VPN-i miinuseid saaks nimetatud lahendustega kõrvaldada või leiavad nad, et nende poolt kasutusel olev VPN on neile sobilik.

Esimene küsitluses osalenu märkis, et nad kasutavadki juba OpenVPN lahendust. Teine isik aga

vastas, et nende ettevõttel ei ole kindlasti plaanis hetkel kasutatavat VPN lahendust välja vahetada, kuid neil on lisaks olnud plaanis kasutusele võtta Microsoft DirectAccessi VPN lahendus mobiilsetes töökohtades. Kolmas küsitletu vastas, et tal puudub teave VPN-i vahetamise kohta. Neljas vastanu märkis, et OpenVPN on ca kolmekümnes WinXP sülearvutis kasutusel, kõik uued Win7, Win8 sülearvutid kasutavad IKEv2-e, kuna see on operatsioonsüsteemiga vaikimisi kaasas ning see on piisavalt turvaline. DirectAccessi on antud ettevõttes testitud Win7-e ja UAG-ga, kuid see ei toiminud olukorras, kus nii sise- kui välisvõrgus on "native" IPv6. Viies küsitletu vastas, et ei ole mõelnud vahetamise peale. Olemasolev lahendus on ühtne seade (tulemüür, VPN, antiviirus, veebifilter, rakenduste kontroll), mida on mugav ja lihtne hallata. Teiste alternatiivide kasutuselevõtuks ei näe antud isik praegu mingeid eeliseid.

2.2 Küsitluse analüüs

Esimese küsimuse järgi on näha, et vastanute hulgas kasutavad kaks ettevõtet OpenVPN tehnoloogiat. Microsoft DirectAccessi aga üheski asutuses kasutusel ei ole. Üks küsitlusele vastanu ei teadnud , mis VPN-i lahendus neil kasutusel on. Samas on aga näha, et OpenVPN-i ja Microsoft DirectAccessi kõrval kasutatakse ka teisi virtuaalse privaatvõrgu lahendusi, näiteks riistvaralist Juniper SRX VPN-i, mobiilide jaoks L2TP/IPsec protokolli ja Windows 7 jaoks IKEv2 protokolli, lisaks kasutatakse ka Fortinet SSL-i. Seega on antud küsitlusele vastanute hulgas OpenVPN kõige populaarsemaks lahenduseks.

Teise küsimuse vastuste järgi on näha, et kahel asutusel on valitud OpenVPN ning selle põhjuseks on ühel juhul toodud, et see on vabavaraline ning teisel juhul, et tegemist on tasuta rakendusega. Siinkohal peab aga autor nõustuma, et OpenVPN-i Community versiooni suureks eeliseks on just see, et selle eest ei nõuta litsentsi tasu. Lisaks on üks vastanutest veel selgitanud, et OpenVPN sobib paljudele platvormidele ning toetab mitut autentimisviisi. Käesoleva töö autor nõustub antud seisukohaga, sest OpenVPN-iga on tõesti võimalik autentida mitut erinevat moodi ning selle plussküljeks on ühtlasi asjaolu, et see sobib ka nii Windowsi aga ka Linuxi operatsioonsüsteemidele. Üks küsitletutest tõi seejuures välja, et tema ettevõte kasutab IKEv2 protkolli, kuna OpenVPN-i kasutamine Windows 7-s vajab administraatori õigusi.

Kolmanda küsimuse ühes vastuses tuuakse välja, et ettevõttes kasutatakse OpenVPN-i, kuid sellega on raske hallata seadmeid, mis ei kuulu domeeni. Autor leiab, et seadmeid, mis ei kuulu domeeni ei peakski olema kerge hallata. Siinkohal tekib küsimus, et miks antud seadmed domeenis ei ole, kui neid soovitakse administraatori poolt kergelt ja kaugelt hallata. Teine kasutaja aga kasutab hoopiski riistvaralist VPN-i, mis võimaldab ainult kindlate asukohtade vahelist liiklust. Käesoleva töö autori soovituseks olekski liikuvamatele seadmetele/sülearvutitele paigaldada, kas siis OpenVPN või DirectAccessi VPN lahendus, mis antud probleemi kõrvaldaks. Üks vastanu tõi ettevõttes kasutatava OpenVPN-i miinuseks taaskord välja selle, et Windows 7 ja Windows 8 puhul on tarvis administraatori õigusi. Siinkohal rõhutab autor uuesti, et OpenVPN-i installeerimiseks on tõesti vaja administraatori õigusi, kui see on vastavalt seadistatud ei ole käivitamiseks tarvis administraatori õigusi. Seega tegelikkuses sobiks kõikides antud ettevõtetes nii OpenVPN kui Microsoft DirectAccess kasutusele võtta. Ühel juhul kõrvaldaksid need koguni hetkel kasutuses oleva riistvaralise VPN-i puudused.

Neljanda küsimuse vastuste hulgas ilmnes, et üks küsitlusele vastanu ei soovi olemasolevat OpenVPN-i lahendust välja vahetada ning jääb mulje, et ta on sellega üldjoontes rahul. Teine vastanu leidis, et näeb tulevikus ette vajadust Microsoft DirectAccess VPN-i lahendust mobiilsetes töökohtades kasutusele võtta. See on autori hinnangul igati tervitatav, kuivõrd DirectAccessi kasutuselevõtt võimaldab antud juhul kõrvalda vastava riistvaralise VPN-i puudused. Neljanda küsitluses osalenu ettevõttes oli proovitud DirectAccessi koos UAG-ga, kuid ühendust mingil põhjusel ei saadud. Autori hinnangul tasuks seda varianti aga uuesti proovida ja ametlikes veebilehtedes asuvaid juhiseid järgida, sest alates 1. veebruarist 2010. aastast on olemas ametlik info selle kohta, et DirectAccessi UAG toetab "native" IPv6 protokolli (Microsoft Corporation, 2012, *Choosing an intranet IPv6 connectivity design*). Vahetust ei soovi viies vastaja, kellele meeldib, et kasutatav lahendus sisaldab tulemüüri, VPN-i, antiviirust, veebifiltrit, rakenduste kontrolli, mida on lihtne ja mugav hallata. Kuivõrd viimatise VPN lahenduse, Fortinet SSL-iga, pole autor varasemalt kordagi kokku puutunud, tekitas see autorile huvi ning hilisemat soovi selle tehnoloogia omadustega lähemalt tutvuda.

3. Kokkuvõte

Käesolevas bakalaureusetöös võrdles autor omavahel kahte virtuaalse privaatvõrgu tarkvara - Microsoft DirectAccessi ja OpenVPN-i. Töös sooviti leida vastust küsimusele, kumb antud lahendustest on ettevõtete jaoks mõistlikum ning ühtlasi, miks on OpenVPN-i kasutatavus Eestis laialdasem, kui on see Microsoft DirectAccess puhul. Nimetatud eesmärgi saavutamiseks kõrvutas autor Microsoft DirectAccessi ning OpenVPN-i tarkvaralisi omadusi ja lahendusi. Bakalaureusetöö eesmärkide saavutamiseks koostas autor lisaks ka küsitluse, mille esitas erinevate ettevõtete IT-juhtidele, süsteemiadministraatoritele, võrguadministraatoritele ning projektihalduritele.

Struktuuriliselt jagas autor bakalaureusetöö kolmeks suuremaks peatükiks. Esimeses peatükis võrdles autor omavahel Microsoft DirectAccessi ja OpenVPNi omadusi ning analüüsis aspekte, mis on virtuaalse privaatvõrgu valimisel olulised. Iga tarkvaralist omadust käsitletava peatüki järgi esitas autor kokkuvõtte, kus tõi välja antud virtuaalsete privaatvõrkude erinevused ning esitas sellest lähtuvalt omapoolse subjektiivse hinnangu. Bakalaureusetöö esimese peatüki lõpus esitas autor erinevate omaduste kõrvutamise tulemustest vahekokkuvõtte.

Esimese peatüki võrdluse põhjal osutus ühenduse, turvalisuse ning graafilise kasutajaliidese osas autori hinnangul paremaks Microsoft DirectAccessi tarkvaralised lahendused. OpenVPN oli aga mõistlikum nõuete ja maksumuse osas. Sellest tulenevalt on autor veendumusel, et mõlemal privaatvõrgu tehnoloogial on oma tugevad ning nõrgad küljed. Näiteks võib OpenVPN-i positiivseks küljeks nimetada Community versiooni, mida on ettevõtetel võimalik kasutada tasuta. Autor on arvamusel, et just seetõttu ongi OpenVPN Eestis laialdasemat kasutust leidnud, kui näiteks Microsoft DirectAccess, mis pakub 180-päevast tasuta prooviversiooni, mis pole pikemat perspektiivi silmas pidades ettevõtete jaoks otstarbekas lahendus. Samas võib Community versioonile ette heita selle kasutajaliidese mõningast keerukust administraatori jaoks. Microsoft DirectAccessi administreerimispaneel jätab autori hinnangul professionaalsema mulje ning administraatoril on seal kergem aru saada erinevate funktsioonide olemusest ja toimimisest. Oluline on juhtida ka tähelepanu sellele, et kui varem oli Microsoft DirectAccessi plussiks see, et sellel on IPv6 tugi, siis alates 29.03.2013 pakub ka OpenVPN antud tuge.

Kokkuvõtlikult leiab autor, et mõlemad antud virtuaalse privaatvõrgu tehnoloogiad täidavad efektiivselt oma ülesandeid, mistõttu võib öelda, et mõlemad tehnoloogiad on lähtuvalt erinevate ettevõtete vajadusi ning soove arvestades mõistlikud. Usutatavasti on aga eelarvepoliitika nii mitmegi ettevõtte jaoks primaarne, mistõttu ollakse valmis tegema järelandmisi teiste omaduse, näiteks graafilise kasutajaliidese suhtes, mis lõppkokkuvõttes ei oma ettevõtte jaoks määravat rolli. Sellest tulenevalt ei leidnud autori hinnangul kinnitust bakalaureusetöö esimene hüpotees, millest tulenevalt on Microsoft DirectAccessi tarkvaralised lahendused ettevõtete jaoks mõistlikumad, kui on seda OpenVPN-i omad.

Töö teises pooles keskendus autor bakalaureusetöö raames läbiviidud küsitlusele. Antud peatüki eesmärgiks on peaasjalikult saada informatsiooni selle kohta, millist virtuaalse privaatvõrgu tehnoloogiat ettevõttetes kasutatakse, missugused eelised või puudused on DirectAccessil võrreldes OpenVPN-iga, kas DirectAccessis nähakse üldse lähitulevikus potentsiaali olevat ning kas ühe VPN-i eelistamine teisele on üldse põhjendatud. Küsitluse tulemustest selgus, et viiest vastanust kahel on ettevõttes kasutusel OpenVPN, kuid ükski vastanute ettevõtetest ei kasuta DirectAccessi. Sellest tulenevalt on näha, et pigem eelistatakse OpenVPN-i Microsoft DirectAccessile. Küsitlusest selgus ka asjaolu, et OpenVPN-i ja Microsoft DirectAccessi kõrval kasutatakse ka teisi virtuaalse privaatvõrgu lahendusi, näiteks riistvaralist Juniper SRX VPN-i või Fortinet SSL tehnoloogiat.

Läbiviidud küsitluse raames otsis autor kinnitust bakalaureusetöö teisele hüpoteesile, mille kohaselt eelistavad küsitlusele vastanud ühte virtuaalse privaatvõrgu tehnoloogiat teisele põhjendatult. Küsitluse tulemuste põhjal saab teha järelduse, et vastavad virtuaalsed privaatvõrgud on ettevõtetele valitud põhjendatult ja nad täidavad üldjoontes neilt nõutavaid ülesandeid. Näiteks selgus küsitlustest see, et OpenVPN-i kasutatakse just sellepärast, et see on tasuta ja sobib paljudele platvormidele ning toetab mitut autentimisviisi. Eeltoodust tulenevalt peab paika autori poolt püstitatud hüpoteesi, mille kohaselt eelistasid küsitlusele vastanud isikud ühte virtuaalse privaatvõrgu tehnoloogiat teisele põhjendatult. Võttes arvesse hinnanguid ning bakalaureusetöö küsitluse tulemusi, jõudis bakalaureusetöö autor tõdemuseni, et OpenVPN on hetkel laialdasemalt kasutusel ja populaarsem, kui on seda Microsoft DirectAccess.

Comparison of Microsoft DirectAccess and OpenVPN

Resume

The purpose of this bachelor´s thesis is to give a thorough comparison between Microsoft DirectAccess and OpenVPN. The aim is to bring out the positive and negative sides of these two objects and finally to answer the question, which of these solutions are more reasonable for companies. To achieve the goal of this thesis, author also carried out a survey on the present subject.

This bacherlor´s thesis consists of three major chapters. The first chapter compares Microsoft DirectAccess and OpenVPN software. In order to reach the goal of the bachelor´s thesis, the author divided the comparison part of the work into 7 individual sections. The first section gives brief introduction of the Microsoft DirectAccess and OpenVPN, following sections represent the functionality that author believes are the main points what administrators seek when they choose between Microsoft DirectAccess and OpenVPN. After each section the author analyzes compared functionalities and sums up all the noticed negative and positive sides of these two virtual private networks. The second chapter focuses on the performed inquiry, brings out the background data, points up the results and analyzes the responses. Third and also the last chapter gives overview of the results obtained in the first and second chapter. In this chapter the Author gives his opinion which virtual private network – Microsoft DirectAccess or OpenVPN - is more reasonable for the companies. Author then announces the so-called winner, the one VPN that made the best impression and turned out to be the most versatile in the functionality sections.

As a result Microsoft DirectAccess has succeeded in being the best in following sections: Connection, Interface, Authentication & Security. OpenVPN on the other hand has shown itself as the better choice in these following sections: Requirements, Cost. Concluding from the above, author has decided that both are versatile and more function wise. Taking into consideration author’s personal opinion, the results of the survey and all of the conclusions named above, author presumes that OpenVPN right now is used more widely and it is more popular for consumers group in general because it has free Community version. The author of this

bacherlor´s thesis belives that Microsoft DirectAccess and OpenVPN solutions are more modern for the long turn, because they both support future-oriented tehnologies and solutions for example IPv6, which right now is not so widely used.

Kasutatud kirjandus

Andersson L., Madsen T (2005) *Provider Provisioned Virtual Private Network (VPN) Terminology.* Saadud (06.10.2012) veebiaadressilt http://www.rfc-editor.org/rfc/pdfrfc/rfc4026.txt.pdf

AnexGATE (2010). *VPN history.* Saadud (06.10.2012) veebiaadressilt http://www.anexgate.com/downloads/whitepapers/vpnprimer.pdf

Drake, S.-D.,Jaffe, J., Boggs, R. (2010) *Worldwide Mobile Worker Population 2009-2013 Forecast*. Saadud (06.10.2012) veebiaadressilt: http://img.en25.com/Web/CitrixOnline/IDC_2009-2013_Forecast.pdf

Feilner M.; Graf N. (2009) *Beginning OpenVPN 2.0.9. Build and integrate Virtual Private Networks using OpenVPN.* Packt Publishing Ltd, UK.

Git (2012). Saadud (08.10.2012) veebiaadressilt: http://git-scm.com/

Google (2013). *Statistics.* Saadud (22.04.2013) veebiaadressilt: http://www.google.com/intl/en/ipv6/statistics.html

Grossetete P.; Popoviciu C-P.; Wettling F. IPv4 or Ipv6 – Myths and Realities. Saadud (16.03.2013) veebiaadressilt: http://media.techtarget.com/searchNetworking/downloads/IPv4_or_IPv6.pdf

Keijser J-J. (2011) *OpenVPN 2 Cookbook.* Packt Publishing Ltd, UK.

Kopczynski T., CISSP, GSEC, GCIH, MCTS (2010) *DirectAccess and UAG DirectAccess. Deployment Guide.* Saadud (07.10.2012) veebiaadressilt: http://www.cco.com/portals/0/downloads/DirectAccessDeploymentGuide-Morimoto.pdf

Kotuliak I., Rybár P., Trúchly P (2011). *Performance Comparison of IPsec and TLS Based VPN Technologies.* Saadud (07.12.2012) veebiaadressilt: http://www.iceta.sk/_archiv/2011/proceedings/iceta2011_truchly.pdf

MeirM [MSFT] (2010). *UAG DirectAccess Test Lab Guide CRL Check Update*. Saadud (18.12.2012) veebiaadressilt: http://blogs.technet.com/b/edgeaccessblog/archive/2010/05/20/uag-directaccess-test-lab-guide-crl-check-update.aspx

Microsoft Corporation (2010). *Choosing an intranet IPv6 connectivity design.* Saadud (18.12.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/ee406201.aspx

Microsoft Corporation (2010). *Client authentication.* Saadud (10.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/ee809064.aspx

Microsoft Corporation (2010). *DirectAccess Authentication.* Saadud (10.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/dd637823(v=ws.10).aspx

Microsoft Corporation (2010). *DirectAccess Connections.* Saadud (08.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/dd637767(v=ws.10).aspx

Microsoft Corporation. *DirectAccess Connectivity Assistant 2.0 is available.* Saadud (07.12.2012) veebiaadressilt: http://support.microsoft.com/kb/2666914

Microsoft Corporation (2010). *DirectAccess Requirements.* Saadud (07.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/dd637797(v=ws.10).aspx

Microsoft Corporation (2010). *DirectAccess Technical Overview for Windows 7 and Windows Server R2.* Saadud (07.10.2012) veebiaadressilt: http://www.microsoft.com/en-us/download/confirmation.aspx?id=17039

Microsoft Corporation (2010). *DirectAccess with Network Access Protection (NAP).* Saadud (07.10.2012) veebriaadressilt: http://technet.microsoft.com/en-us/library/ff528477(WS.10).aspx

Microsoft Corporation (2013). *Download Windows Server 2012.* Saadud (20.04.2013) veebiaadressilt: http://technet.microsoft.com/en-us/evalcenter/hh670538.aspx

Microsoft Corporation (2012). *IPv6.* Saadud (08.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/network/bb530961.aspx

Microsoft Corporation (2012). *IPv6 - Technology Overview.* Saadud (07.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/hh831730.aspx

Microsoft Corporation (2010). *Microsoft DirectAccess Connectivity Assistant*. Saadud (07.12.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/ff384241.aspx

Microsoft Corporation (2010). *Separating Internet and Intranet Traffic.* Saadud (08.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/dd637769(v=ws.10).aspx

Microsoft Corporation (2013). *Support.* Saadud (07.04.2013) veebiaadressilt: http://support.microsoft.com/lifecycle/search/?sort=PN&alpha=Windows+server

Microsoft Corporation (2010). *The DirectAccess Connection Process.* Saadud (10.10.2012) veebiaadressilt: http://technet.microsoft.com/en-us/library/dd637792(v=ws.10).aspx

Microsoft Corporation (2010). *Virtuaalse privaatvõrgu ühenduse konfigureerimine Windows XP-s (artikli ID: 314076).* Saadud (06.10.2012) veebiaadressilt: http://support.microsoft.com/kb/314076/et

Microsoft Corporation (2013). *Windows Server 2012 How to Buy.* Saadud (20.04.2013) veebiaadressilt: http://www.microsoft.com/en-us/server-cloud/windows-server/buy.aspx

OpenVPN Technologies Inc. Community Project Overview. *Introduction.* Saadud (21.03.2012) veebiaadressilt: http://openvpn.net/index.php/open-source/245-community-open-source-software-overview.html

OpenVPN Technologies Inc. *HOWTO. Introduction.* Saadud (07.12.2012) veebiaadressilt: http://openvpn.net/index.php/open-source/documentation/howto.html

OpenVPN Technologies Inc. *How to prepare for the deployment of openVPN Access Server?* Saadud (07.10.2012) veebiaadressilt: http://openvpn.net/index.php/access-server/docs/admin-guides/122-how-to-install-and-configure-openvpn-access-server-software.html

OpenVPN Technologies Inc. (2011). *Is IPv6 support planned/in the works?* Saadud (08.10.2012) veebiaadressilt: http://openvpn.net/index.php/open-source/faq/77-server/287-is-ipv6-support-plannedin-the-works.html

OpenVPN Technologies Inc. *Pricing Guide.* Saadud (20.04.2013) veebiaadressilt: http://openvpn.net/index.php/access-server/pricing.html

OpenVPN Technologies Inc. *OpenVPN Access Server Quick Start Guide.* Saadud (07.10.2012) veebiaadressilt: http://openvpn.net/index.php/access-server/docs/229.html

OpenVPN Technologies Inc. (2010). *OpenVPN Access Server System Administrator Guide.* Saadud (07.10.2012) veebiaadressilt: http://openvpn.net/images/pdf/OpenVPN_Access_Server_Sysadmin_Guide_Rev.pdf

OpenVPN Technologies Inc. *Using the OpenVPN Access Server Virtual Appliance VMware Version.* Saadud (07.10.2012) veebiaadressilt: http://openvpn.net/index.php/access-server/download-openvpn-as-vm/164.html?osfamily=Virtual%20Appliance%20(VMWare)&ex=1

OpenVPN Technologies Inc. *Using the OpenVPN Access Server Windows (VHD) Virtualization Version.* Saadud (07.10.2012) veebiaadressilt: http://openvpn.net/index.php/access-server/download-openvpn-as-vm/202.html?osfamily=Virtual%20Appliance%20Windows%20(VHD)&ex=1

OpenVPN Technologies Inc. *Why SSL VPN?* Saadud (10.10.2012) veebiaadressilt: http://openvpn.net/index.php/open-source/339-why-ssl-vpn.html

Tarasov V. (2012). *OpenSC – tools and libraries for smart cards*. Saadud (07.12.2012) veebiaadressilt: http://www.opensc-project.org/opensc

Wright B., Plesniarski L (2011) *MCTS Guide to Microsoft Windows 7: Exam #70-680.* Course Technology, Cengage Learning, USA.

Lisad

Lisa 1

Küsitlus

Kas hetkel on firmas kasutusel mõni VPN lahendus, kui jah, siis milline?

Miks on valitud antud VPN tehnoloogia?

Millised on hetkel kasutusel oleval VPN tehnoloogia puudused?

Kas oled mõelnud olemasolevat VPN lahendust vahetada OpenVPN-i või Microsoft DirectAccessiga, miks?

Parimate soovidega ja ette tänades

Toomas Väärt