UNIVERSITETI I TIRANËS

FAKULTETI I EKONOMISË

DEPARTAMENTI STATISTIKË

DHE INFORMATIKË E ZBATUAR

Temë Diplome

VPN- BENEFITE, KOMPONENT DHE IMPLEMENTIM

Diplomë BACHELOR

Emri/Mbiemri i Studentit:

Bejane Zenjelaj

Emri/Mbiemri i Udhëheqësit:

Prof. Dr. Areti Stringa

Tiranë, Tetor 2018

Nuk pretendoj që në këtë punim të kem arritur të trajtoj në perfeksion VPN, dhe gjithcka rreth tyre, por shpresoj që sado pak të kem arritur të krijoj një punim te plotë dhe gjithpërfshires. Krijimi i këtij punimi ishte një rrugëtim i gjatë të cilin pata fatin të mos e bëj vetëm. Nuk mund të lë pa përmendur profesoren udhëheqese të time, Prof. Areti Stringa, e cila u tregua gjithmonë e gatshme për të më mbështetur dhe përgjigjur cdo pyetjeje të timen. Gjithashtu dëshiroj të permend fakultetin ku unë kalova 3 vitet e Bachelor, që kanë qenë të paharrueshme për mua. Së treti dëshiroj të falemnderoj kompaninë në të cilën unë punoj për lehtësimet e mundura.

Faleminderit të gjithëve!

Abstrakt

Interneti sot është një domosdoshmëri e të gjithëve dhe si i tillë ai ka marrë një zhvillim të gjithanshëm. Por, si me cdo gjë tjetër, një zhvillim i gjithanshëm sjell dhe probleme të pa identifikuara më parë. Një nga problemet kryesore është dhe siguria. Tashmë asnjëherë nuk jemi 100% të mbrojtur kur jemi online dhe ky disavantazh i madh i internetit duhet rregulluar disi. Një nga shumë mënyrat e gjetur janë VPN. VPN është një rrjet privat virtual krijuar brenda një rrjeti publik që me anë të disa teknologjive të caktuara siguron privatësinë dhe sigurinë e të dhënave. Demonstrimi i çka u përmend më sipër është dhe qëllimi i kësaj teme.

Përmbajtja

Tabela e figurave

Hyrje

Jetojmë në shekullin e 21-të, në një kohë kur të qenurit online vjen natyrshëm për këdo. Ajo çka para pak vitesh mendohej si komoditet, sot shihet si domosdoshmëri. Është e domosdoshme prania e internetit gjatë çdo hapi të jetës dhe punës tonë dhe kjo ndonëse na ka lehtësuar shumë, na ka sjellë dhe shumë probleme. Problemi me kryesor dhe më i madhi ngelet siguria. Rrjeti i internetiti është i tillë që ne nuk mund ta kontrollojmë dot dhe si pasojë kjo na lë shume vurnerabël ndaj shulmeve apo 'syve' dashakeq.

Por si mund të mbrohemi ne nga kjo e metë e internetit? Fatmirësisht zhvilluesit dhe shkencëtarët kanë arritur në shumë mënyra dhe pikërisht një prej tyre do të diskutojmë sot. VPN-Virtual Private Netëork është pikërisht një nga këto mënyra. Por cfarë është ajo? VPN është krijmi i një rrugëkalimi të sigurt në rrjetën e madhe të internetit duke na siguruar privatësinë.

Siç u përmend privatësia është pika kyce e kësaj teknologjie dhe për këtë përdoret shumë enkriptimi, protokollet e ndryshme dhe bashkëpunimi me fireëallet për të krijuar atë tunelin e sigurt. Në vazhdimësi të temës do të trajtohen pikërisht këto komponentë.

Teoria na ndihmon shumë të kuptojmë thelbin e çështjes, por është praktika ajo që na e fikson atë në mendje. Duke ndjekur këtë filozofi në përmbajtje të këtij punimi gjendet dhe një implementim praktik i rastit duke treguar hap pas hapi.

Rishikim i literaturës

Implementimi i VPN në rrjetin tonë është një proçes i cili kërkon një studim të mëparshëm të VPN, pasi ndonëse janë teknologji mbizotëruese sot, ato kërkojnë një proçes të mirëstudiuar për t'u implementuar. Implementimi që do të shihet më poshtë është rasti kur ne krijojmë çdo gjë 'from scratch' në kompjuter lokal, por përgjithësisht në profesionet tona në kompani do të na duhet te punojmë shumë me pjesën e fundit të konfigurimit të saj.

Ekzistojnë disa mënyra të ndryshme për të instaluar VPN dhe punime rreth kësaj, por gjithësecila prej tyre fokusohet në një aspekt të veçantë. Në këtë punim synohet të paraqitet mënyra e plotë e instalimit.

Fillimisht do të instalojmë Virtual Machine dhe serverin e zgjedhur në të. Më pas duhet bërë konfigurimi i Active Directory dhe zbatimi i proçedurave pasardhësë. Pasi përfundohet kjo, kalojmë të konfigurimi i NetBios për të komunikuar në rrjetin lokal. Rrjedhimisht kalojmë të Remote Access dhe te vet konfigurimi i VPN.

Në fund të gjithë këtij proçesi na lind e drejta për të krijuar lidhjen me VPN, që është dhe hapi i fundit. Kjo pjesë është shumë e thjeshtë dhe është përgjithësisht ajo çka shumë programues mund t'ju duhet të konfigurojnë në kompjuterat e tyre të punës.

1. Bazat e VPN

1.1 Vështrim i përgjitshëm rreth VPN.

VPN është një mënyrë e sigurt e kalimit të të dhënavë në një rrjet të pasigurt duke mundësuar enkriptimin e të dhënave gjatë kalimit në tunel. VPN ka dy tipe, lidhjen me akses të largët të një përdoruesi të vetëm në rrjetin e kompanise, dhe lidhjen site-to-site që nënkupton lidhjen midis dy rrjëtave të sigurta të kompanise. VPN gjithashtu i jep kompanisë mundësi të ulë kostot e saj me një lidhje të tillë.[1]

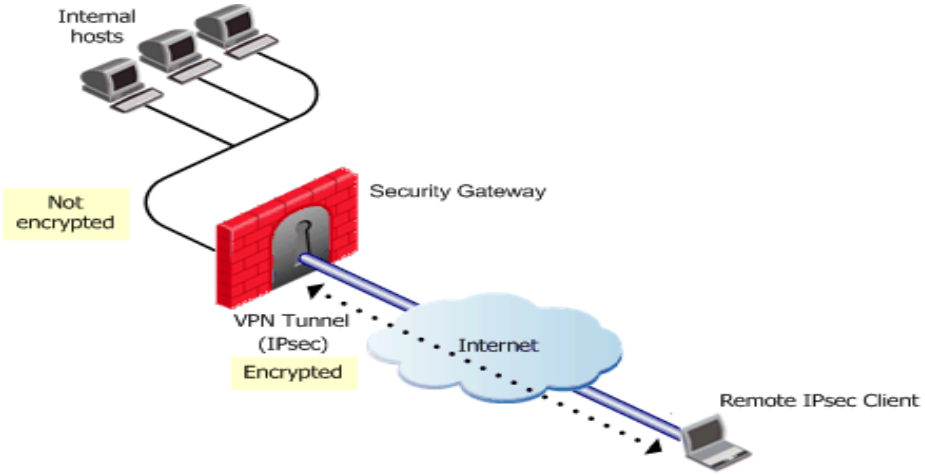

Figura 1 Skema e VPN ndërmjet dy rrjeteve të sigurtë

Tipret bazë për VPN janë:

Është virtuale:
VPN nuk është një rrjet fizik sigurie që mund të zotërohet nga përdoruesi, por është një lidhje në rrjet midis përdoruesve të ndryshëm që me anë të teknikave të protokollit të tunelimit bëhet i dukshëm për përdoruesin.Për të kapërcyer pasojat e mospasjes së një rrjeti fizik, duhet të krijohet marrëveshja e nivelit të shërbimit për të ofruar, në mënyrën më të mirë të mundshme, performancë dhe disponueshmëri të kërkesave që i nevojiten VPN.

Është Private:
Privatësia e VPN qëndron në faktin se ai siguron konfidencialitetin dhe integritetin e të dhënave. Përgjithësisht trafiku i VPN kalon shpesh kalon nëpër rrjete publike dhe kështu ky funksion bëhet i domosdoshëm. Kërkesat e sigurisë përfshijnë:

- Vërtetësia e origjinës së të dhënave
- Ripërtëritja e çelsave kriptografikë në mënyrë ciklike

- Enkriptimin e të dhënave
- Maskimi i adresës.

Është rrjet:
Edhe pse fizikisht jo i tillë, VPN-ja trajtohet si një zgjerim të infrastrukturës së rrjetit të kompanisë. Kjo do të thotë që duhet të jetë në dispozicion të pjesës tjetër të rrjetit, me anë të routerave dhe adresimit.

1.2 Nevojat dhe përfitimet nga VPN

Të gjithë e dimë se interneti është i domosdoshëm në ditët e sotme dhe gjithnjë e më shumë jeta jonë , por dhe e ardhmja e biznesit, po drejtohet drejt tij. Duke trajtuar aspektin e biznesit, sot thuajse çdo kompani ka një ëebsite të vetin ku reklamohet, ka një mënyrë komunikimi të brendshme etj,, dhe kjo gjë ka rritur nevojën për VPN, pasi interneti është si një xhungël ku duhet te mbrohesh nga çdo sulm i mundshëm dhe pikërisht këty hyn teknologjia VPN.
Figura e mëposhtme ilustron kalimin e sigurt të të dhënave në rrjetin e madh të internetit mes degëve apo komponentëve të ndryshëm të një kompanie. Ofruesit e shërbimit në internet (ISPs) ofrojnë shërbimin në internet me kosto efektive (nëpërmjet lidhjeve direkte apo numrave të telefonave), duke eleminuar linjat e dedikuara, kostot e telefonatave të largëta, lidhjet e gjata, etj. [4]

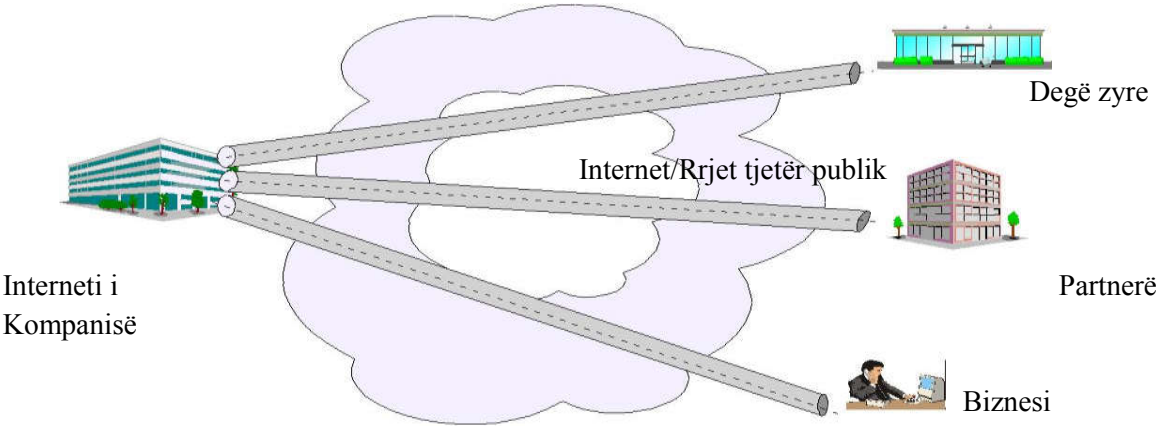

Figura 2 Rrjeti privat virtual (VPN)

Statistikisht është llogaritur një përfitim 47% e kostos së ËAN dhe 8-% e kostos së lidhjes dial-up, nga zvendësimi i linjave të dedikuara VPN; statistikë kjo e marrë nga një raport kërkimor në 1997.
Teknologjitë e VPN po bëhen gjithnjë e më të standartizuara, por jo të gjitha produktet në treg mbështesin të gjitha metodat VPN. Ndërkohë që disa metoda të VPN mund të jenë përdorur në lidhjen me njëra tjetrën, disa të tjera janë zgjidhje alternative. VPN mund të përcaktohet duke patur parasysh nevojat në bazë të pikave të mëposhtme:

- Sigurinë
- Nevojat e biznesit

- Përshtatja me sistemin aktual
- Perfomancën

Zgjidhja ideale do të ishte zhvillimi i një teknologjie VPN nga kompanitë bazuar në nevojat e tuyre. Zgjidhjet e VPN bazuar në IPSEC sot avancojnë kryesisht në mjedisinIPv4, por është e rëndësishme që ato kanë mundësi dhe kapacitet për tu zhvendosur në IPv6 dhe ruajtur kominikimin e brendshëm të kompanisë. Eksperienca me rrjetat luan gjithashtu një rol shumë të rëndësishëm në këtë ekuacion. [4]

1.3 Ndarjet e VPN

1.3.1 Llojet e VPN

VPN mund të kategorizohet si më poshtë: [2]

1. VPN e bazuar në software mundëson më tepër fleksibilitet në atë se si do të manaxhohet trafiku i rrjetit. Ky tip është i përshtatshëm kur pika fundore e VPN nuk është e kontrolluar nga e njëjta palë, dhe ku disa fireëalle të ndryshme apo dhe rutera janë në përdorim. Ajo do të përdoret me përshpejtues të enkriptimit të hardware për të rritur performancën.

2. VPN e bazuar në firewall është një nga llojet e VPN që bazohet në aftësitë e firewall. Ky tip i VPN e bën sigurinë duke përdorur mekanizmat e firewallit për tu futur në aksesin e një rrjeti të brëndshëm. Kjo përfshin përkthimin e adresave, autenticitetin e përdoruesit, alarmet në kohë reale dhe loget e shpeshta.

3. SSL VPN lejon përdoruesit të lidhen me VPN duke përdorur një web browser. Një avantazh në përdorimin e SSL VPN është lehtësia në përdorim, sepse të gjitha standartet që mbështesin web browserat e lejojnë protokollin SSL.

4. VPN të bazuara në hardware ofron shërbim më të gjërë në rrjet, performancë më të mirë dhe më shumë besueshmëri, që kur nuk ka procesor të ngarkuar. Gjithesi është me i shtrenjtë.

1.3.2 Dy tipet më të shpeshta të VPNs.

Remote-Access—E quajtur ndryshe edhe rrjeti privat virtual dial-up (VPDN), është një përdorues i lidhur në një lidhje lokale dhe që ka punonjës që i nevojiten të lidhen me rrjetin privat nga vendndodhje të ndryshme. Tipikisht, një kompani që dëshiron të implementojë një një VPN në distancë disa forma të lidhjes në distancë VPN përdor disa forma të lidhjes dial-up që përdoret nga ISP-të. Përdoruesit në distancë mund të thërrasin një numër 1-800 për të arritur në internet dhe përdorin programin e klientit të VPN për të aksesuar rrjetin e mbrëndshëm të kompanisë. Një shembull i mirë është i një kompanie që i nevojitet një akses në distancë i VPN është një firmë e madhe me qindra shitës. Lidhja në distancë mundëson siguri, enkripton lidhjen ndërmjet kompanisë dhë përdoruesit përmes një ofrues shërbimi si palë e tretë. [3]

Site-to-Site - Përmes paisjeve të dedikuara një kompani mund të lidhet me disa përdorues përgjatë një rrjeti publik të tillë si është interneti. Cdo përdorues i nevojitet vetëm një lidhje lokale me rrjetin publik, duke kursyer shumë para nga ndërtimi i lidhjeve të privatizuara e të kushtueshme. VPN site-to-site ndërton ndërmjet zyrave të të njëjtës kompani dhe quhet intranet VPN, ndërkohë që kur një lidhje përdoret me klientë ose partnerë biznesi jashtë rrjetit të kompanisë quhet ekstranet VPN. [3]

1.4 Veprimet që bën VPN

- Enkapsulimi i IP - kjo përfshin bashkëngjitjen e paketave të të dhënave TCP/IP brënda një pakete me një adresë IP apo të një Fireëall ose një server që vepron si një pikë fundore VPN. Ky enkapsulim fsheh hostin.
- Enkriptimi - bëhet në pjesën e të dhënave të paketës. Enkriptimi mund të bëhet ose në pjesën e transportit që enkripton të dhënat, ose në pjesën e tynelit e cila enkripton dhe dekripton të dhënat përgjatë transmetimit si të trupit të të dhënave ashtu edhe të kokës.
- Autentifikimi - përfshin krijimin e një domaini enkriptimi i cili përfshin autenticitetin e kompjuterit dhe të dhënave të paketës duke përdorur enkriptimin publik.

1.5 Kërkesat e VPN

Tani do të trajtojmë që i atribuohen zakonisht VPN, gjërat që do të meren në konsideratë poarandalojnë nga vënia në rrezik e zgjidhjes së VPN.

1.5.1 Konsiderimet e sigurisë për VPN

Përdorimi i VPN ngre disa shqetësime të sigurisë përtej atyre që ishin të pranishëm në rrjetet më parë .
Një kalim të dhënash end-to-end mund të përmbajë:

- Një segment i jashtëm (Internet) që ku navigojnë dhe burimeve të jashtme.
- Pajisje jashtë kontrollit (për shembull, aksesin e kutisë së ISP në një segment dial-in dhe ruternat në internet).
- Një segment të brëndshëm (intranet) që përmban hoste dhe routera. Disa mund të jenë keqdashës, dhe disa mund të shërbejnë si trafik mes rrjetit të jashtëm dhe të brëndshëm të kompanisë.
- Një portë sigurie (Fireëall ose router) që është i vendosur mes një segmenti të brëndshëm dhe të të jashtëm.

Pra sic kuptohet ka shumë munësit pët të ndryshuar përmbajtjen e datagramës, mundësi për të përgjuar, të bëjë sulme DoS(denial-of-service)etj.[4]

1.5.1.1 Një path tipik end-to-end

Për të kuptuar çështjet me siguri të VPN-së end-to-end, ne shohim elementët përgjatë një pathi end-to-end. Trafiku end-to-end do të kalojë në tre segmenteve bazë: një segment dial-in, një segment të jashtëm (Internet) dhe një segment të brendshëm (intranet).

- **Segmenti Dial-in:** Ky segment zgjatet nga një makinë e përdoruesit në distancë tek një akses boks të mundësuar nga ISP. Protokollet dhe procedurat të përdorur në lidhje janë specifikuar nga ISP. Sot shumë ISP mbështesin protokollin point-to-point (PPP) në këtë segment.

- **Rrjeti i jashtëm (Internet):** Një trafik i një kompanie në internet nuk und të quhet si e izoluar, ashtu si mund të ishte me një rrjet privat të dedikuar, që kur rrjedh nga VPN të ndryshme është e miksuar në backbone të Internetit.

- **Rrjeti i brëndshëm (intranet):** Ky segment është në fund të rrugës së komunikimit. Rrjeti i brëndshëm është nën kontrollin e kompanisë. I gjithë trafiku në rrjetin e brëndshëm të kompanisë gjenerohet nga kompania; shumë pak trafik hyn apo del jashtë saj; bashkë me protokollet ne intranet.

1.5.1.2 Ekspozimet në klientin e dial-in

Klienti dial-in është kur fillon komunikimi kështu që mbrojtja është në aksesin fizik të klientit dial-in. Klienti duhet të mbrojë kur nuk e ka nën mbikqyrje. Një shembull i thjeshtë është vendosja e passëordit, edhe kur e lë vetëm për një kohë të shkurtër. Fikja e kompjuterit dhe mbyllja e dhomës duhet marë në konsideratë.

1.5.1.3 Ekspozimet në segmentin dial-in

Segmenti dial-in dërgon trafikun e të dhënave të përdoruesit direkt tek një ISP. Në rast se të dhënat janë të pa enkriptuara, dhe është mjaft e lehtë për ISP për të shqyrtuar të dhënat sensitive, adhtu dhe për njëhacker. Enkriptimi i shtresës së linkut ndërmjet hostit në distancë dhe ISP mund të bëjë mbrojtjen nga përgjuesit pasivë, por nuk mund të mbrojë nga një ISP keqbërëse. Që kur ISP mund të dekritpjë rrjedhjen e të dhënave të përdoruesit, të dhënat sensitive janë të akoma në ISP në formë të pa ekriptuar.

1.5.1.4 Ekspozimet në internet

Në disa skenarë të qasjes në largësi, një ISP ndërton një tynelim për të zgjatur shtrirjen e lidhjeve PPP kështu që pika fundore mund të bëhet kutia e aksesit dhe porta e sigurisë. Në rast se protokolli i tynelimit nuk përfshin tipare të fuqishme të sigurisë, një ISP keqbërëse mundet që fare lehtë të ndërtojë një tynel që të dërgon diku tjeter. Kështu, të dhënat e përdoruesit mund të dërgohen nga një tynel fals tek një portë e ngritur për qëllime keqbërëse ku të dhënat mund të lexohen apo modifikohen. [4]
Ka gjithashtu rreziqe në kalimin e datagramit brënda tynelit. Në rast se datagramat janë në formë teksti, ndonjë ruter lehtësisht mund të shqyrtojë apo modifikojë datagramën, dhe një sulmues pasiv mund të përgjojë në ndonjë nga lidhjet përgjatë rrugës.Enkriptimi link-pas-linku në secilën hap në backbonet e internetit mundet të pengojë përgjimet, por nuk mbron të dhënat e përdoruesit nga nje ruter keqbërës, pasi çdo ruter përgjatë rrugës do të jetë në gjëndje për të bërë dekriptimin të të dhënave të përdoruesit, as enkriptimi i link-by-link nuk mund të mbrojtë nga tynelet false, pasi pikat fundore false të tynelit mund të kenë akses në teksin e pastër. Edhe protokollet popullore të tynelimit si L2TP nuk mundëson ndonjë siguri të fuqishme. Prandaj, IETF ka rekomanduar që trafiku në tynel duhet të mbrojet me protokolle IPSec.

1.5.1.6 Firewallet dhe ruterat e VPN

Përgjithësisht filtrimi i paketave të IP është i implementuar në Firewalle dhe rutera për të mbrojtur rrjetin privat nga sulmet e internetit. Në situatën ku lidhja e VPN udhëton në Firewalle apo rutera që kryejnë filtrimin e paketave IP si në figurën 5, konfigurimi i Firewallit apo ruterit do të ndryshohet për të lejuar trafikun e VPN përgjatë Firewell apo ruterit.

Specifikisht, ndryshimet në konfigurimet e mëposhtme janë kërkuar për Fireëall apo rutera:

- Aktivizim i përcjelljes së IP
- Lejim të portës UDP 500 për IKE
- Lejim të protokolleve të IP 50 dhe 51 për ESP dhe AH
- Lejim të portës UDP 1701 për L2TP dhe L2F
- Lejim të protokollit të IP 47 (GRE) dhe të portës TCP 1723 për PPTP

1.5.1.7 Ekspozimet në intranet

Përgjithësisht ekziston besimi se rreziqet më të mëdha në internet vijnë nga jashtë, por studime të ndryshme kanë treguar se shumica e sulmeve në fakt lindin nga brënda. Ëështë e mundur për një punonjës keqbërës të modifikojë një kuti të brëndshme duke bërë të mundur për të monitoruar, ndryshuar apo riroutuar datagramat që rrjedhin në rrjetin e kompanisë. Kur të dhëna nga rrjete të ndryshme rrjedhin në intranet (për shembull në rastin kur një lidhje VPN lidh prodhuesit me disa klientë) kërcënimet brënda intranetit duhen ruajtur. Nëse një segment apo një partner nuk e ka rrjetin intranet të sigurt vihet kështu në rrezik siguria e çdo partneri që komunikon me të.

1.6 Performanca e VPN

1.6.1 Konsiderime në performance

1.6.1.1 Numri i logeve (regjistrimeve)

Në mënyrë të ngjashme, regjistrimet e mesazheve dhe eventeve që kanë të bëjnë me trafikun e VPN ka të ngjarë të shkaktojnë një ndikim në performancë. Ky ndikim do të jetë i ndryshëm për klientë, servera dhe porta. Problemi për tu zgjidhur në këtë rast është mjaft delikat:

1. Në rast se braktisen krejt loget, rrezikohet kompromentimi i sigurisë së rrjetit sepse nuk do të jemi në gjëndje për të zbuluar përpjekjet për ndërhyrje dhe sulme të ndryshme. Një zgjidhje e mirë sigurie gjithmonë përfshin një sasi të caktuar të logeve.

2. Nëse bëhen loge të shumta do të humbim një sasi të konsiderushme të përpunimit që do të shkaktojë vonesa e trafikut dhe buffera apo hapësira të logeve të mbingarkuara. Kjo mund të

bëjë që sistemet të jenë të pa-operueshme dhe e tërë zgjidhja e VPN jo praktike.

Praktikë e mirë është të ngrihet dhe të testues për sistemet që do të vendosen më pas për të ndërtuar mjedisin e VPN. Gjatë fazës së testimit, përcaktimi se çfarë do të ruhet nga secila këto sisteme, sa performancë do të humbi gjatë logut dhe cila prej logeve do të tregohen në veçanti. Kjo do të ofrojë me një kuptim se cilat evente janë të rëndësishme për tu regjistruar në mënyrë të përhershme dhe cilat evente duhen vetëm të regjistrohen vetëm në rast se ka ndonjë problem specifik.
Porta e VPN në disa kompani gjithashtu kanë aftësi për të hyrë në një server logesh në mënyrë që të shmangin mbingarkimet e burimeve lokale. Nëë këtë mënyrë do të mblidhen dhe vlerësohen regjistrimet (loget) e informacionit në vendndodhjen qëndrore që do bëjë zbulimin e ndërhyrjeve dhe parandalimin e tëyre më të lehtë.

1.6.1.2 Numri i përpunimeve të enriptimit

Një nga çështjet kyçe në lidhje me performancën do të jetë faktori i enriptimit. Për të përcaktuar impaktin e procesit të enriptimit duhet llogaritur pikat e mëposhtme:

- Serverat me qasje të përhershme në akses VPN njoftojnë disa enriptime në ekzekutim deri në një shkallë kur është dashur të ndahet serveri nga paisja e enriptimit. Kur arrihet kjo pikë nevojitet të përcaktohet për platformadhe nuk mund të përgjithsohet apo të matet në numër lidhjesh apo sasia e trafikut me kalimin e kohës.
- Sistemet fundore, tipikisht klientët VPN dhe serverat me qasje rastësore në VPN, shumicën e kohës nuk njoftojnë për performancën duke përdorur enriptimin sepse ato vetëm ekzekutojnë ose vetëm bëjnë të mundur lidhjen harmonike.
- Portat e VPN në mënyrë të sigurtë thithin shumicën e procesit të enriptimit në shumicën e skenareve VPN. Prandaj, duke shtuar paisje speciale hardëare për enriptim apo shtimin e paisjeve të dedikuara për VPN duhet të konsiderohet si një alternativë para se Fireëall të thyhet apo ruteri nuk bën rrugëzime sepse është mbingarkuar me kryerjen e veprimeve të VPN.

1.7 Enkriptimi në VPN

1.7.1 Objektivi i përgjitshëm i enkrpitmit.

Enkriptimi është një mënyrë efiçente për të bërë të dhëna të palexueshme për marrës të padëshirueshëm. Megjitatë nëse nuk trajtohet si duhet enkriptimi mund të bëhet më tepër një kërcënim për të dhënat sesa ti mbrojë ato. Duhet patur parasysh që enriptimi kërkon çelsa për të transferuar teksin e pastër në një grumbull karakteresh dhe anasjelltas. Në rast se çelsat humbin ose vidhen, për shembull nga një administrator sistemi i cili largohet nga puna pa dorëzimin e çelsave të enriptimit tek eprorët e tij, të dhënat janë kompromentuar dhe, çfarë është më e keqja, mund të mos jetë më e mundshme për ti aksesuar këto të dhëna.Prandaj, si pjesë e rregullave të sigurisë, duhet që përcaktohet qartë nëse enriptimi është i nevojshëm, dhe nëse po, për cilat tipe të dhënash, në cilën pjesë të rrjetit, dhe kush do të autorizohet për të përdorur atë.
Kryesisht janë dy mënyra për mbrojtjen nga humbja apo vjedhja e çelsave të enriptimit:

Rigjenerim i çelsave

Kjo teknikë është projektuar për të lejuar agjencitë e zbatimit të ligjit (LEA) për të rimarrë çelsat për dekriptimin e mesazheve sekrete sipas interesave të tyre. Kjo është një teknikë edhe për rikthimin e çelsave kriptografikë por është një proces mjaft i komplikuar dhe më pak praktik se ruajtja e çelsave.

Një mënyrë për implementimin e gjenerimit të çelsave është nga vendosja e blloqeve të rikuperimit të çelsave në rrjedhën e të dhënave në intervale të rastësishme ose/dhe kur çelsi ndryshon. Këto blloqe të rigjenerimit të çelsave janë të enkriptuar me çelsa publik të një pale të tretë të sigurtë (agjentë të rikuperimit të çelsave). Agjentët e rikuperimit të çelsave mund të dekriptojnë çelsin me çelsat e tyre privat, atëhere çelsat e enkriptimit me çelsat publik të LEA dhe e dërgon atë tek LEA. LEA dekripton çelsat me çelsin e saj privat dhe me pas dekripton mesazhin sheh teksin e pastër

Ruajtja e çelsit.

Kjo teknikë mundëson ruajtjen dhe tërheqjen e çelsave dhe të dhënave në rast se ato vidhen apo humbin. Çelësat janë ruajtur nga një palë të tretë besuar (agjent rikuperimi apo ruajtës çelsash), si një pjesë e tërë apo e ndarë, në vënde të sigurta, në mënyrë që të kthehen kur ato kërkohen. Pala e tretë e besueshme mund të jetë nje administrator i çelsave në kompani i vendosur brënda apo jashtë kompanisë. Kjo siguron që çelsat mbeten në zotërim të kompanisë edhe pasi administratori i sistemit ose kushdo që i përdorte këto çelsa është larguar nga puna.

1.7.2 Rregullimet e eksport/import

Sa herë nevojitet të përdorim enkriptimin duhet të jemi të sigurtë se cili nivel i enkriptimit është i lejuar nga shteti dhe për natyrën e biznesit. Zakonisht bankat mund të vendosin nivele të larta të enkriptimit në krahësim me përdoruesit e zyrave të vogla, dhe në disa shtete janë më kufizuese se të tjerat. Në Shtetet e Bashkuara enkriptimi është i rregulluar nga Departamenti i Tregetise.

1.7.3 Rreziqet nga enkriptimi end-to-end

Kur një enkriptim end-to-end është i lejuar, kjo e hap Fireëall në një zonë të pabesueshme. Kur implementohet, trafiku i enkriptimit end-to-end nuk do të shihet nga klienti ku zbatohet ky përjashtim për dizajnimin klient/server. Kjo nënkupton që vetëm një herë sulmuesi gjen akses në një pikë fundore, ndërhyrësi do të ketë akses në të gjithë intranetin e kopmanisë. Dos mbështet në portën e VPN ose Fireëall gjithashtu nuk do të bëhet e përdorshme, dhe ndërhyrësi do të prishi një shërbim të rëndësishëm klient/server.

2. Teknologjitë e VPN

2.1 Firewall-et

Një Firewall është një sistem i cili qëndron ndërmjet rrjetit të brëndshëm dhe pjesës së jashtme. Firewallet kanë qënë vendosur në një rrjet të madh publik për shumë vjet dhe kanë zënë vend thelbësor në zhvillimin e strategjive të sigurisë. Edhe pse nuk është një strategji e përsosur, firewalli është i lehtë në konfigurim, kërkon modifikim të vetëm një portë të ruterit. Në rast se kemi një lidhje të shumëfishtë WAN me disa pathe për në internet, do të ishte e mira të krijohej një Firewall për çdo pikë të ndërlidhjes. Kompleksiteti i proçesit rritet në mënyrë dramatike nga një pikë e vetme në një portë e shumfishtë. [4]

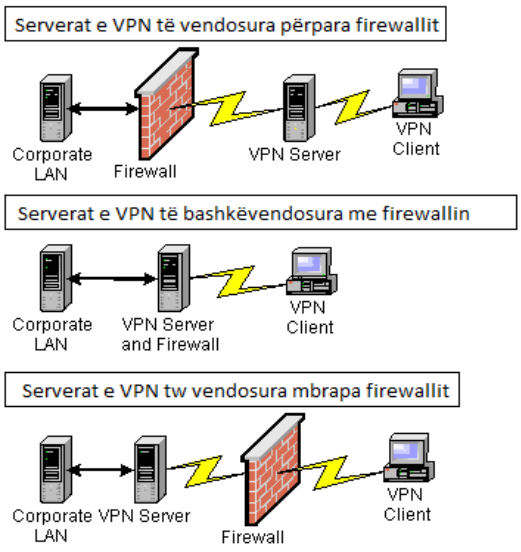

Figure 3 Pozicionimi i firewall-eve

2.1.1 Çfarë është një firewall?

Firewallet zakonisht kanë dy funksione për një administrator rrjeti. E para është të kontrollojnë cilat pjesë mund të shohë një i jashtëm në rrjet dhe shërbimet në këto paisje me cilat ai do të ketë kontakte. E dyta është kontrolli se cilat paisje në Internet një përdorues i Intranetit do të shohi, apo më saktë cilat shërbime ai do ti përdorë. Nje Firewall është më shumë si një polic trafiku, organizon se cilat pathe në trafikun e rrjetit do të kalojnë dhe cilat do ti ndalojë. Fireëallet e internetit zakonisht e bëjnë këtë duke inspektuar çdo pako në portat e ruterit, e cila është arsyeja edhe që atyre i referohen si sisteme të "filtrimit të paketave".

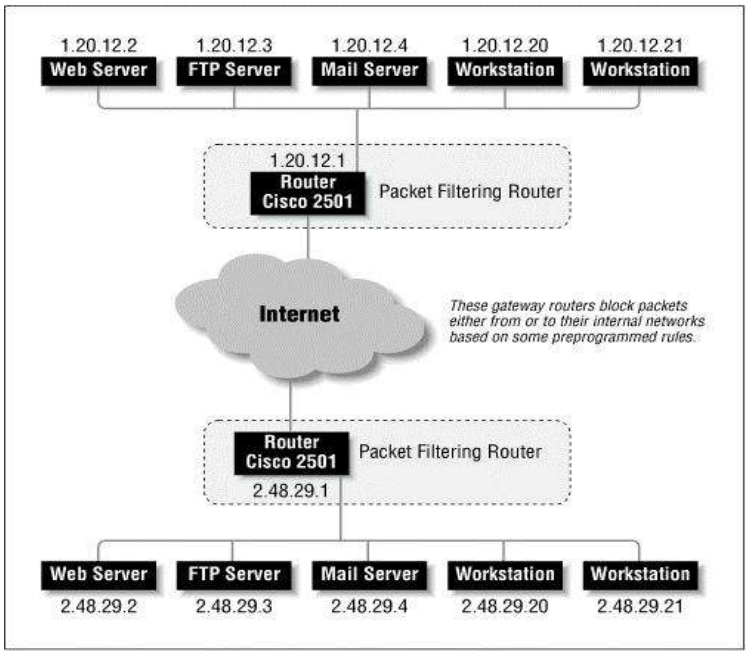

Figure 4 Një Firewall tipik

2.1.2 Cilat janë tipet e firewalleve?

Që kur thuajse të gjitha teknikat e firewallit janë projektuar mbi një model të ngjashëm, një pikë e centralizuar e kontrollit, janë vetëm pak variante në nivel të lartë që nevojiten të eksplorohen. Gjithsej janë katër variante që përdoren më së shumti, dhe sigurisht ne jemi duke lënë jashtë disa arkitektura komplekse dhe të avancuara. [4]

2.1.2.1 Kufizimi apo filtrimi i paketave në rutera.

Ruterat dhe kompjuterat që transmetojne filtrimin e paketave zgjedhin të dërgojnë trafikun në një rret të bazuar me rregulla të paracaktuara. Ruterat nuk veprojnë bazuar në atë që është brënda ngarkesave, por se nga vjen dhe cila është destinacioi i saj. Në konsideratë është se a i përmbush paketa një set parametrash, dhe duhen marë masat për të lejuar apo ndaluar kalimin. Tabelat që bëjnë lejimin dhe ndalimin janë ngritur në përputhje me rregullat e sigurisë së rrjetit të brëndshëm të vendosura nga administratori i rrjetit apo koordinatori i sigurisë.

Një vështrim në funksionimin e filtruesve të paketave tregon se ruterat nuk shohin tek përmbajtja e paketës por tek koka e informacionit TCP/IP, për të bërë shqyrtimin e rastit. Kështu, në rast se ruteri do të pyetet të lejojë të gjithë trafikun nga rrjeti 192.168.1.1/24, do të kontrollojë të gjitha paketat për të parë përputhjen e adresave vurim dhe i tejkalon ato më tej. Ndërkohë që një paketë duhet të kalojë nga një rrjet në një tjetër tjetër filtri do të lejojë tranzitin dhe paketa do të kalojë më tej. Pra, në thelb, kjo tregon se si i gjithë operacioni i këtij firewalli bën sigurinë. [4]

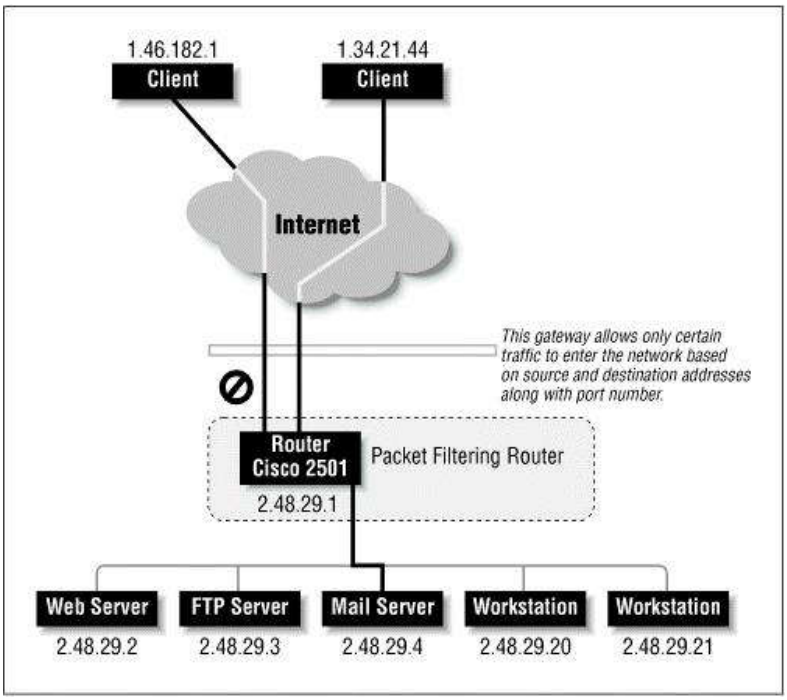

Figure 5 Një paketë filtrimi në ruter

Filtrimi i paketave mund të marë dy forma bazë. E para është një rrjet i hapur me filtrim selektiv të trafikut të padëshiruar. Për secilin tip të sulmit të rrjetit, një filtër i përshtatshëm lihet në vend të ruterit. E dyta është një trafik i mbyllur me filtrim selektiv të trafikut të dëshiruar

Ruterat në ditët e sotme i kërkohet të bëjnë mrekulli, sidomos në garën për shumë e më shumë bandëidth. Puna e ruterit është e dedikuar për të dërguar trafikun, jo për të kapur dhe për të dërguar paketa që kanë rrezik për sigurinë.

Ajo që sygjerohet, natyrisht, është se do të ketë një ndryshim të dukshëm në atë që portat e rrjetit do të duken në të ardhmen. Besohet se do të ketë një ndarje të paisjeve të ruterave dhe filtrimit të paketave (ose edhe të paisjeve të sigurisë, për këtë çështje) në një afat të afërt. Produktet e reja tashmë vijnë nga ata që mbështesin autentifikimin dinamik përmes një filtruesi të paketave në ruter direkt në nivel përdoruesi, madje edhe në një lidhje të enkriptuar.

Një pengesë e fundit është ndryshimet e shpeshta në rrjet mund të kërkojnë rikonfigurim të portave të ruterit dhe filtrimit të paketave në fireëall. Kjo mund të kërkojë kohë dhe prirje të gabuar në rast se një gabim i pakapshëm ndodh më shpesh në rrjet të gjërë të hapur, ose një ndryshim i vogël në ruter të paaftë për të kryer detyrën e tij si një drejtues të trafikut në rrjet. [4]

2.1.2.2 Bastioni i hostit

Nje bastion host përdor si mekanizmin e filtrimit të paketave, të mundësuar nga ruteri dhe një host i sigurtë. Një host i sigurtë është vend që ka sistemin e saj të operimit dhe disa shërbime nën kujdesin e ekspertit të sigurisë. Siguria primare është mundësuar nga një ruter filtrimi i paketave, dhe hosti i sigurtë i përdorur për të drejtuar rrjedhën e informacionit në cilindo drejtim. Hosti bastion është një paisje e sigurisë së kontrolluar që është lidhur me internetin me të njëjtën metodë si paisjet e tjera.. Portat lejojnë

trafikun të kalojë në të në mënyrë më pak të kufizuar. Hostet bastion janë tipikisht të përdorura në kombinim me filtrimin e ruterave sepse filtrimi i paketave të thjeshta nuk mund të bëhet ne protokolle apo në shtresën e aplikimit (Figura 9).

Një host bastion është më i lehtë për tu konfiguruar në krahësim më një server të shpërndarëdhe më i lehtë në mirëmbajtje, sepse sasia më e madhe e trafikut është dërguar në një sistem. Që kur hosti bastion është përqëndruar në shtresën e brëndshme, nuk nevojiten më përjashtues special prej paisjeve të tjera të lidhura lokalisht. Rregullat e sigurisë do të diktojnë se cfarë duhet për të konfiguruar në to ruterat e filtrimit të paketave, të cilat do të bëhen sa më kufizuese të jetë e mundur. Nuk është e pazakontë për administratorin që të përdorë një kombinim të strategjive, duke përdorur si filtrimin e paketave në ruter ashtu dhe hostet bastion.

Një ndër gjërat më thelbësore në konfigurimin e hosteve basion për masat e sigurisë është konfigurimi i filtrit të paketave të bëhet për masat e sigurisë është ai konfigurim i filtrimit të paketave që të bëhet gjenerike gjëndja "blloko gjithcka", pasuar nga disa gjëndje shumë specifike të cilat i përkasin vetëm hostit bastion. Për ndryshimet e mëdha dhe të shpeshta të rrjetit, mund tëshihet që kjo redukton ngarkesën e personelit të sigurisë. Duke shtuar paisje të reja apo duke pasur përdorues të instaluar ose përdorues të instaluar dobët në paisjet e sigurta nuk ndikon në Fireëall dhe mbrojtjen e ofruar nga hosti bastion.

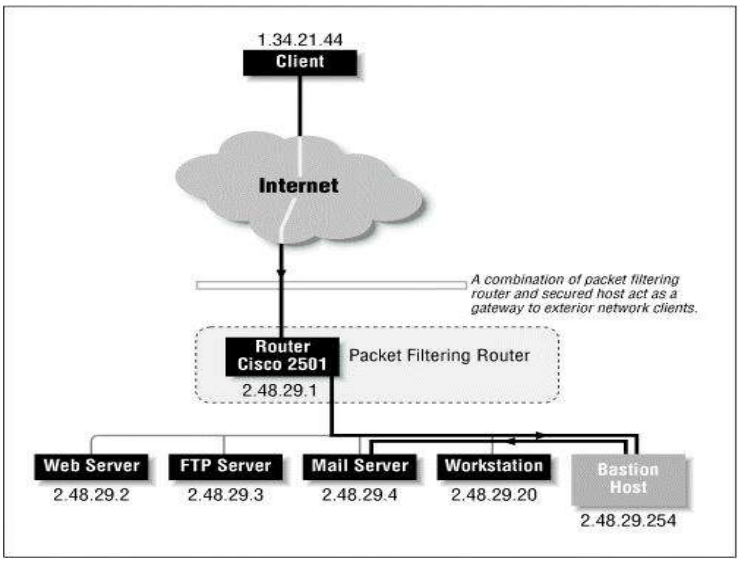

Figure 6 Një Firewall host-bastion

Sigurisht, duke patur një pikë kontrolli të qëndërzuar ka disavantazhet e saj. Për një rrjet të madh dhe të ngarkuar do të duhen disa paisje të aktrojnë si hoste bastion (duke e bërë administrimin e tyre më të shtrirë në kohë), apo më mirë, një perimetër i rrjetit të hostit basion do të nevojitej.. Çdo paisje kërkon seksionin e saj në filtrimin e paketave në fireëall, duke mbledhur kompleksitet, dhe me secilën paisje ka problem me prova dhe prova të dyfishta për pastërtinë. Bashkë me nevojën për Hoste të shumëfishtë për të parandaluar ngjeshjen në rrjet, qëndërzimi i informacionit në bastion mund të tërheqë sulme, pa llogaritur që një pengesë e madhe për këtë llog konfigurimi të Firewallit është se ajo mund të çojë në një rrezik tragjik sigurisë, një sulmues mund të mari privilegjet e operatorit në hostin bastion, Kështu një pikë e vetme e kontrollit është e barabrtë me një pikë të vetme të dështimit.

2.1.2.3 DMZ ose zona e perimetrit në rrjet

Një teknikë e mirë për të ndarë rrjetin e kompanive nga mjedisi i rrezikshëm i internetit është të bëjë "rutimin e rrjetit" në të cilin duhet të kalojë i gjithë trafiku. Instalimet e mëdha zakonisht kanë gati të tillë rrjeta gati për tu ndarë është që në mënyrë efektive mund të ndahet trafiku local nga trafiku i MAN nga WAN apo rrjeti botëror. Ashtu si mund të mendohet, një rutim në rrjet konsiston vetëm në rutera, duke përfshirë lidhjet hyrëse dhe dalëse, dhe zakonisht shkon me termin "backbone." Një konfigurim i tillë shihet në figurën 10. Si fillim janë të paktën dy rutera të përfshirë në mbrojtjen e intranetit. Një ruter shërben si portë për internetin, dhe tjetra shërben si portë për rrjetin e brëndshëm. Rrjeti ndërmjet dy ruterave nuk duhet të ketë paisje tjeter në të me përjashtim të paisjeve të rutimit dhe hosteve të besueshëm.

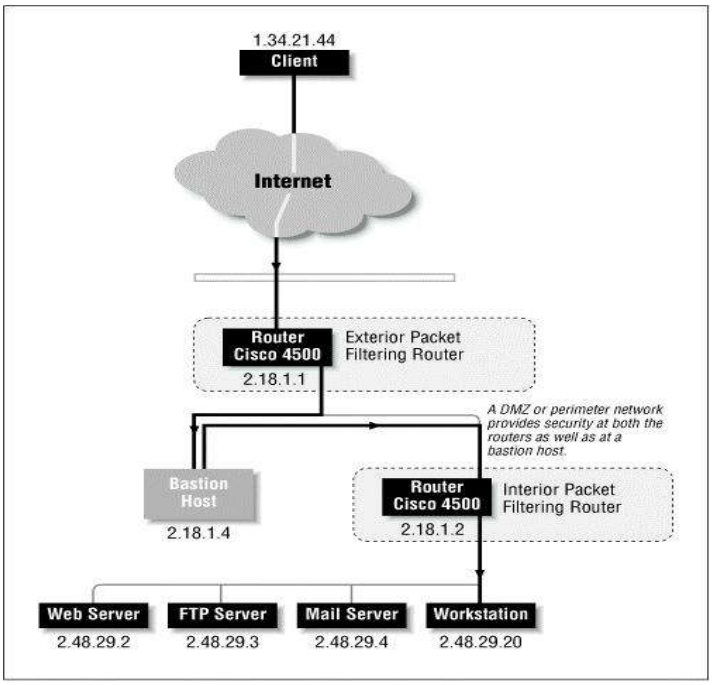

Figure 7 Një zonë perimetri në firewall

Tipi i dytë në sigurinë e arkitekturës DMZ përfshin një degë të sigurisë në pjesën e jashtme të perimetrin në nivel ruteri ose në një host në perimetrin e rrjetit; ndërhyrësit do të shohin vetëm paisjet që janë transit, asgjë më tepër. Për të përfituar akses në një rrjet të brëndshëm, duhet të krakohet perimetri i brëndshëm i ruterit, i cili duhet ti dekurarojë ato deri sa
 të largohen. Një zgjidhje e VPN nga rrjeti i brëndshëm duhet që të përfshijë enkriptimin e paketave, dhe të komplikojë një përpjekje për të rrezikur rrjetin
Në një zoë standarte të perimetrit, kontollet më komplekse janë vendosur në rutera të brënshëm, të cilët janë at që ndajnë rrjetin e brëndsm nga permetri i rrjetit si dhe nga rrjeti i jashëm. Kjo është nj praktikë mjat e mirë pr të ngritur rrjetin DMZ në këtë, sepse ky konfigrim mund të krahësohet me nivlin e qareve koncenrike—secila prej tyre më pas jep më pak siguri. Gjithashu, bëhet nj praktikë e shpeshtë për të

përdorur Netëork Address Translation (NAT) në ruterat e brëndsm që të koplikojë më tej vendnodhjen dhe vjedhjen e infomacionit të brëndshëm në komunikim. NAT ofron siguri nga përkthimi i adresave jo të rutueshm (të tilla si rangu 192.168.0.0) në adresa reale internet në një mjedis dinamik. Nuk është një mënyrë e lehtë për të këmbyer informacion me hoste të brëndshmë më përjashtim të rastit kur anashkalohet përktihimi i adresave.
Siguria më e fortë që mund të bëhet me DMZ do të ishte të mos lejojë të gjithë trafikun të dalë jashtë nga rutera të jashtëm, dhe të mos lejojë të gjithë trafikun të futet në rrjetin e brëndshëm direkt nga interneti.
Në thelb, kjo bën që procesi i trafikut të jetë me dy faza. Klientët në internet mund të kontaktojnë vetëm më makinat që janë të lokalizuara në perimetrin e rrjetit, dhe klientët që janë brënda rrjetit të brëndshëm nuk mundet të shohin internetin direkt; ato gjithashtu do tu nevojitet të përdorin ndërmjetës përgjatë një bastioni host të DMZ. Nje gjë e tillë mund të rrënojë perpjekjet e nje sulmuesi.

2.1.2.4 Serverat proxy

Një shërbim proxy është më shumë se një postobllok "tranzit" në një zonë të informacionit. Proxy shtiret të jetë në fund të lidhjes, por mbron dërguesin e vërtetë apo marrësin nga një trafik i panjohur. Shërbimi që prezanton problemin më të madh tek manaxheri i sigurisë "protokolli standart i shkëmbimit të skedarëve"(FTP). Është e pasigurë sepse përdoret në mënyrë rastësore, në numër të madh portash për të krijuar një sesion peer-to-peer me një klient. Duke pasur një shërbim që vepron në më shumë se një portë, siguron një problem për administratorin e sigurisë.

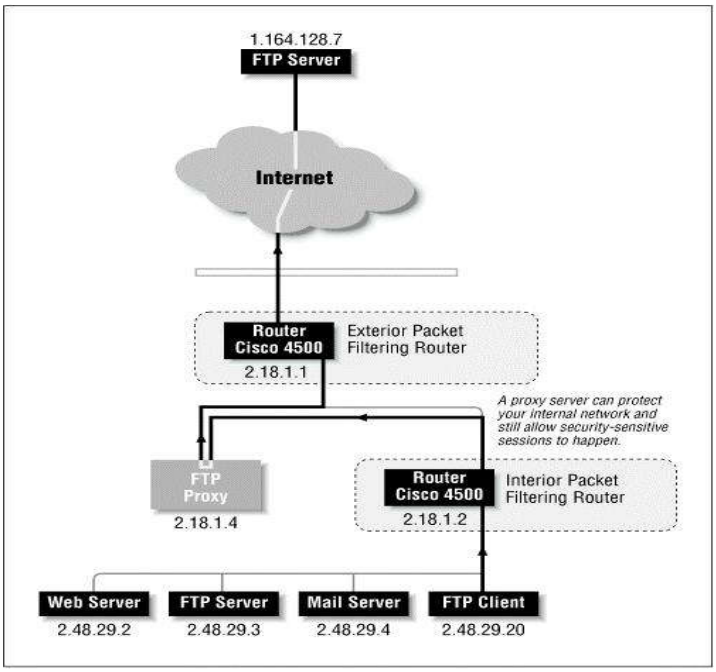

Figure 8 Një server proxy si një fireëall

Për të adresuar këtë një sesion "pasiv" i FTP mund të krijohet por jo të gjithë klientët e mbështesin këtë.
Duke përdor një proxy ashtu si në figurën 11, është një tjetër opsion për të krijuar një lidhje FTP përgjatë Fireëall. Pasi të krijohet një makinë hosti në një perimetër rrjeti që vepron për klientët, që është vendosur

në rrjetin e brëndshëm, një lidhje e plotë do të bëjë që me pak siguri të dorëzohemi.
Proxy FTP është në perimetrin e rrjetit dhe i është dhënë akses përmes fireëallit të jashtëm për të krijuar sesione FTP.

Për arsyen se një proxy server ngjan më shumë më një kompjuter se me llojet e tjerë të fireëalleve, një kujdes special do të përdoret për të siguruar që proxy server është siguruar mirë nga rregullat e sigurisë. Gjithashtu, është e rëndësishme të theksohet që një shërbim proxy është një masë shtesë e mbrojtes dhe nuk duhet të konsiderohet si një zgjidhje e përgjitshme. Mburoja e filtrimit të paketave Firewall mund të ndihmoje për të mbajtur gjëra të ndara, dhe/ose rrjeti mund të segmentohet në subnete të ndryshme, të izoluara nga rreziku më i lartë tek rreziku më i ulët.

2.2 Enkriptimi dhe autentifikimi
Konfigurimi dhe vendosja e një rrjeti privat virtual përfshin jo vetëm një filtrim paketash në ruter.
Enkriptimi mund të përdoret si një metodë për të ndryshuar të dhënat nga një formë normale në një formë të pa-përdorur nga askush përveç marrësit të mesazhit, i cili e ka të nevojshme ta dekriptojë atë. Imputi në një algoritëm enkriptimi është tipikisht një teks i pastër, ndërkohë që autputi është një mal më karaktere të pakuptimta. Procesi i enkrpitmit mbron të dhënat duke e bërë punën e ndërhyrësit shumë të vështirë apo mjaft të gjatë për të gjetur se çfarë nënkuptojnë ato shifra. Rutinat kriptografike përdorin matematikën për të ndryshuar të dhënat që procesi të jetë i nderlikuar.

2.2.1 Kriptografia në rrjetat e komunikimit
Mbrojtja e komunikimit në rrjet është mjaft themelore. Mbrojtja vjen nga nevoja për të dërguar të dhëna në një rrjet të panjohur publik. Kjo shpesh referohet edhe si problem i "transmetimit mbi një kanal të pasigurtë", dhe shpesh zgjidhet nga një apo dy metoda.
Zgjidhja më e thjeshtë është, të bësh komunikimin të sigurtë duke privaizuar kanalin e komunikimit. Në rast se bëjmë që palët e treat të mos kenë akses në rrjet, ndërhyrjet bëhen tmerrësisht të veshtira, kështu që lidhja është solide. Por gjithsesi kjo nuk është zgjidhja më e mirë, për disa arsye. Është mjaft e kushtueshme për të privatizuar një infrastrukturë kaq të madhe komunikimi, të cilat mund të jenë të parealizueshme, si dhe jopraktike për të ndryshuar në kohën e duhur, për të mos përmëndur që do të ishte mjaft e vështirë për të përmbushur pritshmëritë e përdoruesve.
Kjo është edhe arsyeja që VPN po bëhet gjithmonë e më shumë i përdorshëm. Që nga koha që zgjidhja nuk është për të privatizuar një infrastrukturë të tërë, duhet që të sigurohen të dhënat në një kanal të pasigurtë. Me fjalë të tjera, duke e bërë të aksesueshmë për të gjithë, por duke e transferuar në një formë (duke përdorur kriptografi) vetëm një marrës mund ta shohi atë.

2.2.2 Algoritmet Kriptografike

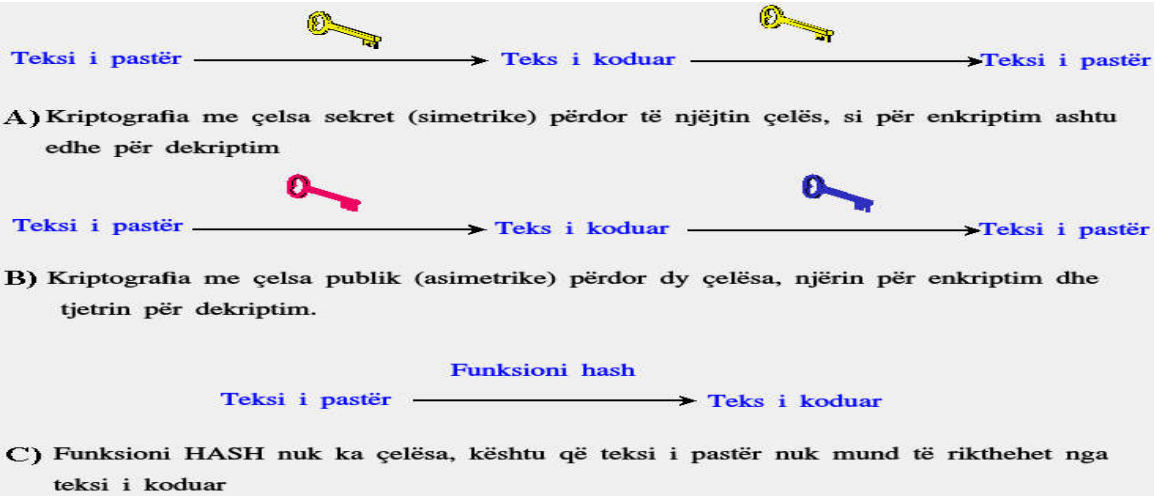

Figure 9 Funksionet kriptografike

2.2.2.1 Kriptografia me çelsat private.

Me kriptografinë me çelsa sekret, një çelës i vetëm përdoret nga të dy palët e komunikimit, si enkriptimi ashtu edhe dekriptimi. Për arsye se një çelës i vetëm përdoret për të dy funksionet, kriptografia me çelsa sekret është quajtur edhe enkriptimi simetrik.

Në këtë formë kriptografie, si dërguesi ashtu edhe marësi duhet të dijnë çelsin, që është sekret. Vështirësia më e madhe në këtë rast është shpërndarja e çelsit.

Algoritmet më të përdorshme për kriptografinë me çelsa sekret janë:

- Standarti i enkriptimit të të dhënave (DES)
- Standarti i avancuar i enkriptimit (AES)
- Algoritmi ndërkombëtar i enkriptimit të të dhënave (IDEA) etj.

2.2.2.2 Kriptografia me çelsat publike

Kriptografia me çelsat publik është mendohet të jetë zhvillimi më i rëndësishëm në fushën e kriptografisë në 300-400 vitet e fundit. Thelbi i kriptografisë me çelsa publikë është që kripto sisteme në të cilën dy pjesë bashkëpunojnë në një komunikim të sigurtë mbi një rrjet komunikimi jo të sigurtë pa patur një çelës sekret. [5]

PKC varet nga ekzistenca e të ashtëquajtura funksione njq mënyrëse, ose funksione matematikore që janë të lehta për tu përllogaritur, ndërsa operacioni invers është mjaft i vështirë.

Dy shembuj për këtë janë:

1. Multipleksimi vs. Faktorizimi: Supozojmë që kemi dy numra primarë, 3 dhe 7, dhe duhet të llogaritim prodhimin; dhe nuk do shume kohë të llogaritësh përfundimin që del 21. Le të mendojmë, në vend të saj, të themi që kemi një numër, 21, dhe duhet të gjejmë se cilët numra primarë janë llogaritur për të gjetur rezultatin. Zgjidhjen do ta gjejmë por sigurisht do të dojë një kohë shumë më të gjatë se gjetja e prodhimit të numrave 3 dhe 7. Problemi do të jetë edhe më i

vështirë nëse do ta bëjmë për numra primarë me mbi 400 shifra e më shumë, sepse produkti mund të ketë rreth 800 shifra. [5]

2. Eksponencialiteti dhe logaritmet. Supozojmë që do të marim numrin 3 në fuqi të 6; përsëri, është e lehtë për tu llogaritur sepse 3 në fuqi të gjashtë është 729. Nëse do të kemi se numrin 729 dhe të gjejmë dy numrat fillestarë që përdorëm, do të gjejmë log x të 729=y, që do të dojë një kohë të gjatë ëpr të gjetur të dy vlerat. Ndërkohë që shembujt më sipër janë të parëndësishëm, atpo prezantojnë 2 nga pjesët funksionale që janë ëprdorur me PKC, lehtësinë e shumëzimit dhe të eksponencialitetit kundrejt vështirësive relative të faktorit dhe të llogaritjes së algoritmeve respektivisht. "Mashtrimi" matematik në PKC është për të gjetur një shteg në funksionin një-mënyrësh kështu që llogaritja e kundërt bëhet e lehtë duke patur parasysh njohurinë e disa elementeve të informacionit. [5]

Gjenerimi i çelsave publik PKC që janë matematikisht të lidhur me njëri tjetrin, gjithsesi nuk do të thotë se në rast se di njërin bën llogaritjet për të gjetur tjetrin. Njëri çelës është ëprdorur për për të enkriptuar teksin e pastër dhe tjetri për të dekriptuar teksin e koduar. E rëndësishme nuk është se cili çelës është përdorur në fillim, por që të dy çelsat duhet për të përmbushur proçesin e punës. Për arsyen se kërkohet një çift çelsash, kjo metodë quhet kriptografia asimetrike.

Në PKC, një nga çelësat është projektuar si çelësi publik dhe mund të reklamohet gjerësisht si dëshiron zotëruesi i saj. Tjetri është i projektuar si çelësi privat dhe nuk i jepet asnjëherë një pale tjetër. Kryesisht mesazhet dërgohen sipas kësaj skeme.Supozojmë që A dërgon mesazhin tek B. A enkripton informacionin duke përdorur çelsin publik. B dekripton mesazhin duke përdorur çelsin privat. Kjo metode mund të përdoret edhe nëse është dërguar mesazhi apo jo. A për shembull mund të enkriptojë teksin e pastër me çelsin e saj privat, dhe kur B dekripton atë duke përdorur çelësin publik, ai e di që A është dërguesi që e ka dërguar mesazhin dhe që A nuk mund ta mohojë që e ka dërguar atë mesazh.

Algoritmet me çelsat public që janë përdorur në ditët e sotme për këmbim të informacionit si dhe për firma dixhitale përfshijnë:

- RSA
- Algoritmi i firmave dixhitale (DSA):
- Kriptografia e kurbës eliptikë (ECC)
- Standarti me çelsa public në kriptogra (PKCS):
- Algoritmi i shkëmbimit të çelsave (KEA)

2.2.2.3 Funksioni hash.

Një funksion kriptografik hash është një funksion hash i cili mer një input (apo mesazh) dhe kthen një vlerë fikse në madhësi e cila quhet vlera hash (shpesh quhet si kodi i mesazhit, etj).

Një funksion ideal hash ka 4 veti kryesore:

- Është e lehtë të llogaritësh vlerën hash të një të dhëne
- .Është tmerrësisht e vështirë të llogaritësh në mënyrë kompjuterike teksin që ka një vlerë hash të caktuar.
- Është tmerrësisht e vështirë të ndryshosh mesazhin pa zbërthyer vlerën Hash

- Është thuajse e pamundur që dy mesazhe të ndryshme të kenë të njejtën vlerë hash.

Funksionet me këto cilësi janë përdorur si funksione hash për një shumëllojshmëri qëllimesh, jo vetëm në kriptografi. Aplikacionet praktike përfshijnë kontrolle të integritetit të mesazhit, firma dixhitale, autenticitetin, dhe një llojshmëri siguri informacionesh të aplikacioneve.

Një funksion hash mer një gjatësi stringu si një imput dhe prodhon një string me një gjatësi fikse që vepron si një tip "firme" për të dhënat. Në këtë mënyrë, një person që di vlerën hash e ka të pamundur për të gjeneruar mesazhin, por vetëm personi që ka mesazhin origjinal mund të vërtetojë që vlera hash është krijuar apo jo nga ai mesazh.

2.2.3 Autenticiteti

Teknikat e autentifikimit janë thelbësore tek VPN, ato sigurojnë pjesët e komunikimit që ato janë duke shkëmbyer të dhëna me përdorues apo hostet e duhur. Autenticiteti është analoge me "loget" në një sistem me emer dhe fjalëkalim. VPN megjithatë do të kërkojë metoda më të rrepta për të vërtetuar identitetin. Shume sisteme autenticiteti të VPN janë të bazuara në një sistem kyç. Çelsat janë drejtuar përmes një algoritmi hash, i cili gjeneron vlera hash. Pala tjetër mban që çelsat do të gjenerojë vlerën e saj hash dhe do ta krahësojë atë me atë që mori nga pala tjetër. Vlera hash e dërguar përgjatë internetit është e pakutpueshme për një mbikqyrës, kështu që askush nuk do të jetë në gjëndje të zbërthejë atë. Protokolli i autentifikimit të "Shtrengimit të duarve"(CHAP) është një shembull i mirë të një metode autenticiteti që përdor këtë skemë. Një shembull tjetër autenticiteti është RSA.

Autenticiteti tipikisht bëhet ne fillim të çdo sesioni, dhe më pas në mënyrë të rastësishmë përgjatë një sesioni sigurohet që nuk ka të shtirur në këtë bashkëkomunikim. Autenticiteti mund të përdoret për të siguruar integritet të dhënash. Të dhënat mund të dërgohen përmes një algoritmi hash për të nxjerrë një vlerë që është në kontrollin e mesazhit. Çdo devijim në kontroll dërgohet nga një palë tek tjetra do të thotë që të dhënat janë korruptuar përgjatë dërgimit soe janë kapur apo modifikuar përgjatë kohës.

2.2.3.1 Përdorimi i kriptosistemeve dhe autentifikimit në VPN

Ashtu si tek të gjithë komunikimet e sigurta, të gjitha sistemet mbrojtëse kanë tre funksione të rëndësishmë. Komunikimet e sigurta si fillim mbrojnë të dhënat tranzit në mënyrë që palët e treta nuk kanë mundësi të kapin apo të lexojnë dërgesën. Teknikat më popullore të enkriptimit të përdorura në VPN përfshijnë DES, Triple DES, RC2 dhe RC4.

Të dyja palët duhet të dinë që janë duke komunikuar me njëri-tjetrin, edhe pse nuk mund të shohin njëri tjetrin. Dërguesi dhe marrësi duhet të jenë në gjëndje nëse një palë e tretë po tenton të ngacmojë mesazhet, apo ndonjë qëllim tjetër dashakeq. Ky është koncepti i integritetit në mesazh.

Kur dërgohet një mesazh, dërguesi e konverton mesazhin në një vlerë unike hash ose një kod të autentifikimit të mesazhit (kodi MAC), i cili enkriptohet me çelësin e tij privat që përfshihet më mesazh, e gjitha enkriptohet me çelsin publik. Pas transmetimit marrësi do të dekriptojë paketën me çelsin privat, përllogarit vlerën e MAC, dekripton të gjithë meszhin me çelësin privat, përllogarit vlerën e MAC për teksin e ri, dekripton kodin MAC të përdoruesit me çelës publik, krahëson kodin MAC, në rast se nuk përputhen dërgesa është ndryshuar.

Protokolli SKIP është një implementim mjaft popullor i enkriptimit dhe autenticitetit. SKIP është i disponueshëm nga ofrues të ndryshëm si në Unix ashtu edhe në Windows. Secili host që përdor SKIP mban lista e kontrollit të aksesit duke specifikuar se cilët hoste është i gatshëm për të marrë nga trafiku dhe çfarë tipe të enkriptimit të përdorë për secilën prej tyre. Kur një paketë IP është dërguar nga një host SKIP në një tjetër, dërguesi enkripton paketën me protokoll SKIP dhe më pas përfundon një tjetër paketë IP rreth saj kështu që mund të kalojë në internet.

Çelsat për të ngritur një rrjet privat të shkëmbimit të të dhënave apo të ruajtjes së të dhënave të sigurta mbështeten në mundësinë për të qënë në gjëndje për të parandaluar të panjohur dhe për të bërë një izolim të asaj që duam të mbrojmë. Pa fireëalle, një VPN mund të ekzistojë, gjithsesi pa të njëjtën filozofi të sigurisë. Por, pa enkriptim, një VPN nuk do të ekzistonte. Kodimi i masterialit zgjidh problemin e madh të sigurisë në komunikim mbi një kanal të pasigurtë në një mjedis armiqesor.

3. Protokollet e tynelimit në VPN

3.1 Protokolli PPTP

Protokolli i tynelimit point-to-point (PPTP) është një protokoll rrjeti që lejon transferimin e të dhënave të sigurta nga një klient në distancë tek një server i kompanisë duke krijuar një lidhje VPN përgjatë rrjetit TCP/IP, normalisht duke përdorur një ISP. PPTP mbështet multi-protokollet, rrjetin privat virtual mbi një rrjet publik të tillë si interneti. [6]

3.2.2 Protokolli PPP

PPP është një protokoll i aksesit në distancë i përdorur nga PPTP për të dërguar të dhëna multi-protokoll përgjatë rrjetit të bazuar në TCP/IP. PPP enkapsulon IP, IPX (Shkëmbimi i paketave në rrjet), dhe NetBEUI (Zgjatim i ndërfaqes së përdoruesit NetBIOS) dhe tipe të tjera paketash në framet PPP. PPP më pas dërgon paketat e enkapsuluara duke krijuar lidhje point-to-point ndërmjet dërguesit dhe marrësit.

3.2 L2TP mbi IPSec VPNs

L2TP mbi IPSec VPNs lejon biznesin të transmetojë të dhëna në internet, ndërsa ende mban një nivel të lartë të sigurisë për të mbrojtur të dhënat. Mund të përdoren tipe të sigurta të lidhjes për zyra të vogla në distancë të klientëve që duan akses në rrjetin e kompanisë. GJithashtu mund të përdorim VPN të L2TP/IPSec për rutera tek site nëpërmjet përdorimit të ISP--ve lokale duke krijuar një lidhje dial në qëndrën e kompanisë.

Kur kemi vendosur se ku dhe si të përdorim n lidhjen L2TP mbi IPSec, kujtojmë që pika e aksesit në internet ose DMZ e rrjetit është vendi ku serveri i VPN do të vendoset. Serveri i VPN është përgjegjës për të bërë që rregullat e aksesit do të konfigurohen në llogarinë e përdoruesit në programin e serverit, në profilin e përdoruesit në rregullat e aksesit në distancë ose në IAS.

L2TP krijon sigurinë e nevojshme IPSec për të siguruar trafikun e të dhënave. Nuk është e nevojshme për të vendosur apo aktivizuar rregullat e IPSec në dy kompjutera. Në rast se kompjuteri ka një rregull të IPSec aktiv, L2TP do të shtojë rregull sigurie të mbrojë të dhënat e tynelimit L2TP është ekzistuesja. [8]

3.3 SSTP

Protokolli i tynelimit të sigurtë SSTP është një përcaktim nga protokolli i shtresës së aplikimit. Ajo është projektuar për të bërë një komunikim sinkron në një rradhë dhe lëvizje ndërmejt dy programeve. Ajo lejon shumë aplikacione fundore përgjatë lidhjes së internetit, ndërmjet nyjeve, duke bërë të mundur përdorimin efikas të burimeve të komunikimit që janë të disponueshme në rrjetProtokolli SSTP i bazuar në SSL në vend të PPTP me IPSec dhe përdor portën TCP 443 për përcjelljen e trafikut SSTP. Edhe pse ajo është mjaft e lidhur me SSL, një krahësim i drejtpërdrejtë nuk mund të bëhet në mes të SSL e SSTP, SSTP është vetëm një protokoll tynelimi ndryshe nga SSL. Shumë arsye janë për zgjedhjen e SSL përpara IPSec si bazë për SSTP. IPSec është në mënyrë direkte mbështetës i idhjes së VPN site-to-site dhe SSL është një bazë më e mirë për zhvillimin e SSTP, dhe e mbështet atë. [10]

Disa arsye për të mos u bazuar në IPSec janë:

- Nuk kërkon autenticitet të fortë,,
- Diferencat që ekzistojnë për klientët që lidhen ngan jë kompani në një tjetër.
- Protokollet jo-IP nuk mbështeten automatikisht,
- Për arsyen se siguria e IPSec është projektaur për lidhjen site-to-site , ka të ngjatë që të krijojë problem për përdorues që lidhen nga vënde të ndryshme me një numër të limituar të adresave IP.

3.3.1 SSL VPN, një bazë më e pajtueshme për zhvillimin e SSTP

SSL VPN adreson këto çështje edhe më shumë. Ndryshe nga bazikja SSL, SSL VPN siguron një sesion të tërë. Nuk kërkohen adresa statike, dhe një klient është i panevojshëm në shumë raste. Që kur lidhjet janë bërë nëpërmjet shfletuesit në internet, protokolli i lidhjes default është TCP/IP. Klientët që lidhen nëpërjmet SSL VPN mun të përdorin në një desktop për përdorim të burimeve të rrjetit. Transparenca tek përdoruesi, trafiku nga laptopi i tyre mund të jetë i kufizuar për burime të caktuara në bazë të kritereve të paracaktuara të biznesit. [10]

3.3.2 SSTP – një zgjatim i VPN

Zhvillimi i SSTP u bë nga mungesa e aftësive të VPN. Mangësia kryesore e VPN ishin lidhjet e saj të paqëndrushme. Kjo është pasojë fushave të saj të pamjaftueshme të mbulimit. SSTP rrit hapësirën e mbulimit të lidhjes VPN, duke e rregulluar këtë problem. SSTP krijon një lidhje përmes një HTTP të sigurtë, kjo lejon klientët të aksesojnë të sigurt në ruterat e NAT, firewalle dhe web proxy, pa rrezikun e bllokimit të portave. SSTP nuk është projektuar për lidhjen VPN site-to-site por ka për qëllim të përdoret për lidhjen e faqeve VPN të klientit.

Suksesi i SSTP mund të gjendet në karakteristikat e mëposhtme:

- SSTP përdor HTTPS për të krijuar një lidhje të sigurtë
- Tyneli SSTP (VPN) do të funksionojë mbi një HTTP të sigurtë. Problemet me lidhjen e VPN bazuar në protokollin e tynelimit point-to-point (PPTP) ose L2TP do të eleminohen. Ëeb proxy, fireëallet dhe ruterat e Adresave të Përkthimit në Rrjet (NAT) protokolli Point-to-Point Tunneling Protocol (PPTP) ose Layer 2 Tunneling Protocol (L2TP) do të eleminohen. Web proxy, firewallet dhe adresat e përkthimit në internet (NAT) të lokalizuara në rrugëzimin mes klientit dhe serverit nuk do të bllokojnë më lidhjen e VPN.
- Ulet numri i portave të bllokuara

- Çështjet e bllokimit përfshijnë lidhjen në raport me bllokimin e portës PPTP GRE ose L2TP ESP nëpërmjet një fireëalli apo ruteri NAT që pengon klientin nga arritja në server, nuk do të jetë më problem. Klientët do të jenë të aftë për tu lidhur nga kudo nëpërmjet internetit.

- SSTP do të ndërtohet në serverat Longhorn
- SSTP nuk do të kërjojë ritrajtim të çështjeve, çështjet e kontrollit të përdoruesit fundor të VPN mbeten të pandryshuara. Tynelimi i bazur në SSTP lidhet direkt në ndërfaqen aktuale për kleintin e VPN Mikrosoft dhe programin e serverit.
- Mbështetje të plotë për IPv6. SSTP VPN.
- Përdor integrimin e mbrojtjes në aksesin e rrjetit për klientë.
- Integrim i fortë në MS RRAS klient dhe server, me aftësi në dy faktorë autenticiteti.
- Rrit mbulimin e VPN nga disa pika në më shumë lidhje internet. Enkapsulim të SSL për udhëtim në përtën 443.
- Mund të kontrollohet dhe të manaxhohet duke përdorur Firewall të shtresës së rrjetit të tillë si ISA.
- Zgjidhje e plotë në rrjetin e VPN, jo vetëm një tynelim për një aplikacion.
- Integrim në NAP.
- Integrim të rregullave dhe konfigurim për të ndihmuar klientët.
- Një session i vetëm i krijuar për tynelim.
- Pavarsia e aplikacionit.
- Autenticitet më i fortë se IPSec
- Mbështetje për protokollet jo-IP, ky është një avantazh i madh në krahësim me IPSec.
- Nuk është e nevojshme të blesh paisje të shtrenjta, të vështira për të konfiguruar firewalle që nuk mbështesin integrimin e Active Directory dhe integrimin e faktorëve të autentictetit

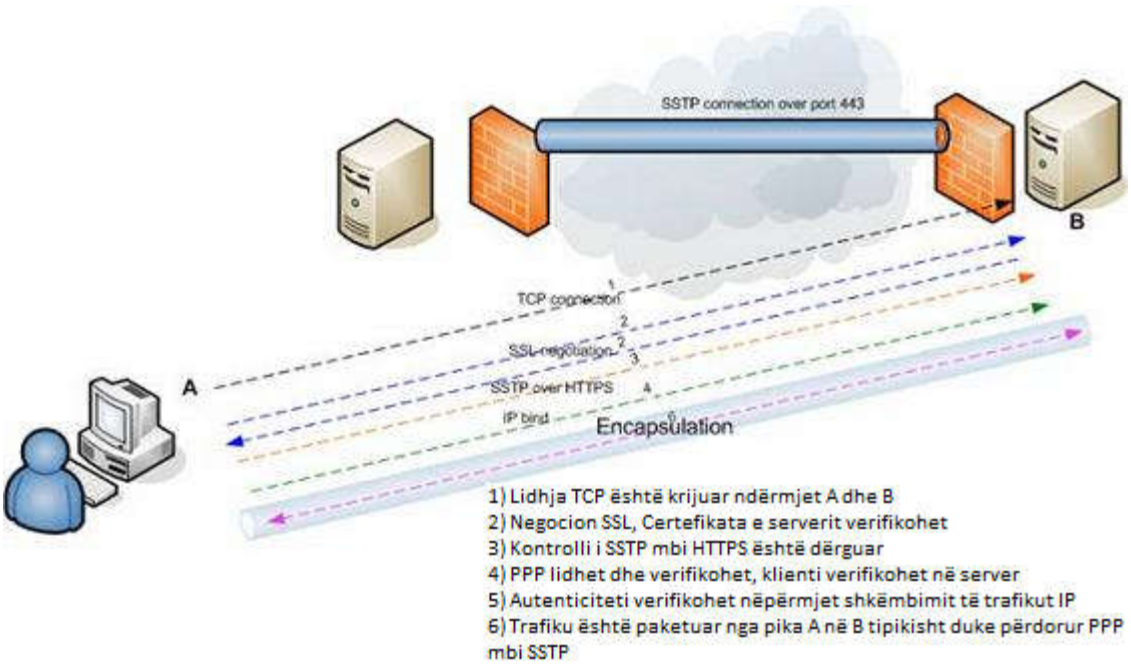

Figure 10 Mekanizmi i lidhjes SSTP.

3.3.2 Hapat e punës së SSTP bazuar në VPN.

Klientëve SSTP i nevojitet lidhje internet. Kur verifikimi i lidhjes është bërë nga protokolli, lidhja TCP/IP vendoset në server në portën 443. Negocimi SSL do të zërë vend në kryje të lidhjes së krijuar TCP, ko do të kontrollohet për vërtetësinë e certefikatës. Në rast se cerfitekata është e saktë, lidhja do të krijohet, në rast se jo, lidhja do të dështojë.

Klienti dërgon një kërkesë HTTPS në krye të sesionit të enkriptimit të SSL në server. Klienti dërgon paketat e kontrollit SSTP në sesionin e HTTPS. Kjo nga ana tjetër krijon një gjëndje të SSTP në të dyja pjesët për qëllime të kontrollit, të dyja anët janë iniciojnë komunikimin në shtresa të PPP.

Negicimi i SSTP duke përdorur SSTP me HTTPS tani gjen vënd në të dy pjesët fundore. Klientit i kërkohet të autetifikohet në server. [10] Ky sesion tani lidhet me ndërfaqet IP në të dy pjesët dhe një adresë IP të caktuar për trafik të rutimit. Trafiku mund të kalojë në lidhjen e krijuar duke qënë trafik IP ose diçka tjetër.

Mikrosofti është i bindur që ky protokoll do të ndihmojë me lehtësimin e çështjeve të VPN. Ekipi i RRAS është duke bërë gati integrimin në SSTP dhe protokolli do të jetë pjesë e zgjidheve të problemeve. i vetmi parakusht për momentin është që klienti shkon nga një sistem p.sh Vista në një server Longhorn. Tiparet e vendosura në këtë protokoll të vogël janë si fleksibël dhe të pasura ashtu edhe protokolli do të rrisë eksperiencën e përdoruesit dhe të administratorit.

3.4IKEv2

Shkëmbimi i çelsave në Internet (version 2) është një protokoll tynelimi i bazuar në IPSec që është zhvilluar nga Mikrosoft dhe Cisco, dhe që është i implementuar në Ëindoës 7 dhe më tej. Ky standrt tynelimi është i përdorur nga paisjet Blackbarry, dhe është zhvilluar në mënyrë të pavarur si implementim open source nga sistemet Linux dhe sisteme të tjera operative. Quajtur si lidhje VPN nga Mikrosoft, IKEv2 është veçanërisht nga ri-krijimi i lidhes së VPN në mënyrë automatike kur humbet përkohësisht lidhja. Përdoruesit e telefonive Mobile, përfitojnë gjithashtu nga përdorimi i IKEv2, kjo për shkak të mbështetjes së saj për to, gjithashtu i bën më elastik në ndryshimin e rrjetave. Ky është një lajm i mirë për përdoruesit e celularëvë gjithashtu, për shembull, lidh telefonat e tyre inteligjentë tek një rrjet Wi-fi ndërkohë që janë në shtëpi dhe zgjedhin të përdorin paketën e internetit të kompanisë celulare, apo kur rregullisht zgjedhin mes hotspoteve. IKEv2 është mjaft i përdorshëm tek telefonat Blackbarry, dhe është ndër të paktët protokollë tynelimi që mbështeten nga paisjet Blackbarry. Nuk është aq i gjithëpranishëm sa IPSec (p.sh. është i përfshirë në pak platforma), por IKEv2 konsiderohet po aq i mirë, në mos më superior se L2TP/IPsec inga ana e sigurisë, performancës (shpejtësisë) dhe stabilitetit. [8]

Avantazhet

- Më i shpejtë se PPTP, SSTP dhe L2TP, kështu që ajo nuk përfshin mbingarkesat me protokollet point-to-point (PPP) (PPP)
- Shumë e qëndrueshme – veçanërisht kur zgjedhim rrjetat ose rilidhjet pas një lidhjeje të humbur internet.
- Mjaft i sigurtë – mbështet AES 128, AES 192, AES 256 dhe 3DES
- I lehtë për tu instaluar (të paktën në nivelin e përdoruesit fundor)
- Është i mbështetur nga paisjet Blackbarry

Disavantazhet

- Nuk mbështetet në shumë platforma
- Përdor të njëjtën portë UTP me IPSec dhe PPTP), e cila është e lehtë për të bllokuar zgjidhet me bazë SSL të tilla si OpenVPN dhe SSTP
- Ne vetëm i besojmë teknologjisë open source

3.5 Open VPN

OpenVPN është një teknologji e re open source që përdor librarinë e protokolleve, bashkë me një amalgamë të teknologjive të tjera, për të mundësuar një zgjidhje të mirë të VPN. Një nga pikat e saj më të forta është sepse është konfigurimi i saj, dhe megjithë se ajo punon mirë në portat e UDP, ajo mund të punojë mirë në cilëndo portë, përfshirë dhe portën TCP 443. Kjo e bën trafikun e saj të komunikojë veç nga trafiku duke përdorur standartin HTTPS mbi SSL (njësoj si në gmail), dhe është mjaftë e vështirë për tu bllokuar. Një tjetër avantazh i OpenVPN është që libraria e OpenSSL është përdorur për të mbështetur enkriptimin më një numër algoritmesh kriptograifk (p.sh. AES, Bloëfish, 3DES, CAST-128, Camellia dhe të tjerë), megjithatë ofruesit e VPN më shumë përdorin AES ose Bloëfish. Bloëfish 128-bit është i ndëertuar default në OpenVPN, dhe që përgjithësisht është konsideruar i sigurtë, ajo ka dobësi të njohura.

AES është një teknologji e re, nuk ka dobësi të njohura, dhe falë adoptimit nga qeveria e Shteteve të Bashkuara, për përdorim të saj për mbrojtje të sigurt të të dhënave, ajo konsiderohet si një ‘standart i artë’

kur bëhet fjala për enkriptim. Fakti që ka një madhësi blloku prej 128-bit më mirë se Blowfish që ka madhësi blloku prej 64-bit gjithashtu ka treguar që për të dhëna me madhësi të mëdha (mbi 1 GB) qëndron më mirë se Bloëfish. Gjithesi, ty dy janë të të çertefikuar nga NIST, të cilat duke e njohur gjërësisht si një problem, ne kemi probleme me të.

OpenVPN është bërë një lidhje default, dhe që nuk përdoret nga ndonjë platformë, është mjaft mirë i përdorur si një palë e tretë softëare (duke përfshirë si iOS edhe Android).

Avantazhet

- I konfiguruar mirë
- Shumë i sigurt (mundësisht edhe ndaj NSA)
- Mund të anashkalojë VPN
- Mund të përdorë një gamë të gjërë të algoritmeve të enkriptimit
- Open source (dhe për këtë arsye mund të verifikohet)

Disavantazhet

- Kërkon një palë të tretë programi
- Mund të jetë i vështirë për tu ndërtuar
- Mbështetja për telefoninë mobile është përmirësuar, por nuk është dhe aq i mirë në desktop.

3.6 L2F

Cisco propozoi një një protokoll tynelimi të shtresës së dytë të quajtur L2TP si një konkuret për PPTP. Ajo përdor PPP për enkriptim dhe autenticitet por shtrin autenticitetin për të mbështetur TACACS+ dhe RADIUS duke përdorur EAP (Protokolli i zgjeruar i autentifikimit). Ajo gjithashtu mbështet autenticitetin e shtresës së dytë, një përdorues në distancë për ISP POP dhe një tjetër nga ISP POP tek portat e rrjetit të kompanisë. Tynelet e shumëfishta të VPN mund të krijohen duke përdorur L2F. Ndërkohë që PPTP mbështet vetëm IP, L2F mund të ekzekutohet në krye te protokollit të shtresës së dytë të tillë si ATM. [9]

4. Implementimi i VPN

Në implementimin e VPN qëllimi është të ndërtojmë një profil klienti dhe një profil server të cilat do të lidhen mes tyre për të simuluar një lidhje të VPN. Për të bërë konfigurimin e klientit dhe të serverit ne do të përdorim Ëindoës Server, në të cilën do të instalojmë disa aplikacione si Active Directory, DNS Server, DHCP Server etj. Pas instalimit të Active Directory krijova një profil me emrin tim që i dhashë gjithashtu kredenciale, të cilin do ta përdor për testim të VPN. Më pas do të konfiguroj VPN server për të aksesuar Active Directory. Për të aksesuar Active Directory me anë të kredencialeve të mia, më duhet të konfiguroj këtë lidhje me krijimin e lidhjes së VPN. Në momentin e konfigurimit dhe të krijimit të lidhjes së VPN, në profiling e Active Directory mund të shoh përdoruesit e loguar, pra mund të shoh që profili im është i aksesuar dhe që aty mundet edhe të bllokoj lidhjen apo ta çaktivizoj atë.

4.1 Konfigurimi i serverit.

4.1.1 Krijimi i mjedisit për instalimin e VPN Server.

Fillimisht instalojmë një makinë virtuale Virtualbox, VirtualMachine etj, në të cilën instalojmë një sistem serveri të cilin unë kam zgjedhur Windoës Server R2 64 bit.

Në këtë sistem serveri instaloj fillimisht Active Directory. Active Directory (AD) është një shërbim direktorie i ofruar nga Mikrosoft për domain të rrjeteve në Ëindoës dhe është i përfshirë në sistemet operative Windows server si një grup procesesh dhe shërbimesh. Një Active Directory kontrollon, autorizon dhe autentifikon të gjithë kompjuterat dhe domainet e Windows në rrjet dhe përforcon rregullat e sigurisë për të gjithë kompjutarat dhe instalimin apo përditësimin e programeve. Për shembull, kur një përdorues logohet në kompjuter që është pjesë e domainit, Active Directory cakton passëordin dhe përcakton nëse përdoruesi është administrator apo përdorues i thjeshtë. Ka të drejta të paracaktuara nga administratori i sistemit.

Fillimisht pas instalimit të Sistemit Windows Server bëhet instalimi i Active Directory që instalohet njëherësh edhe me sisteme të tjera serveri si DNS apo DHCP. Keto konfigurohen në Windows server dhe më pas mund të kryejmë shërbime të tjera me to.

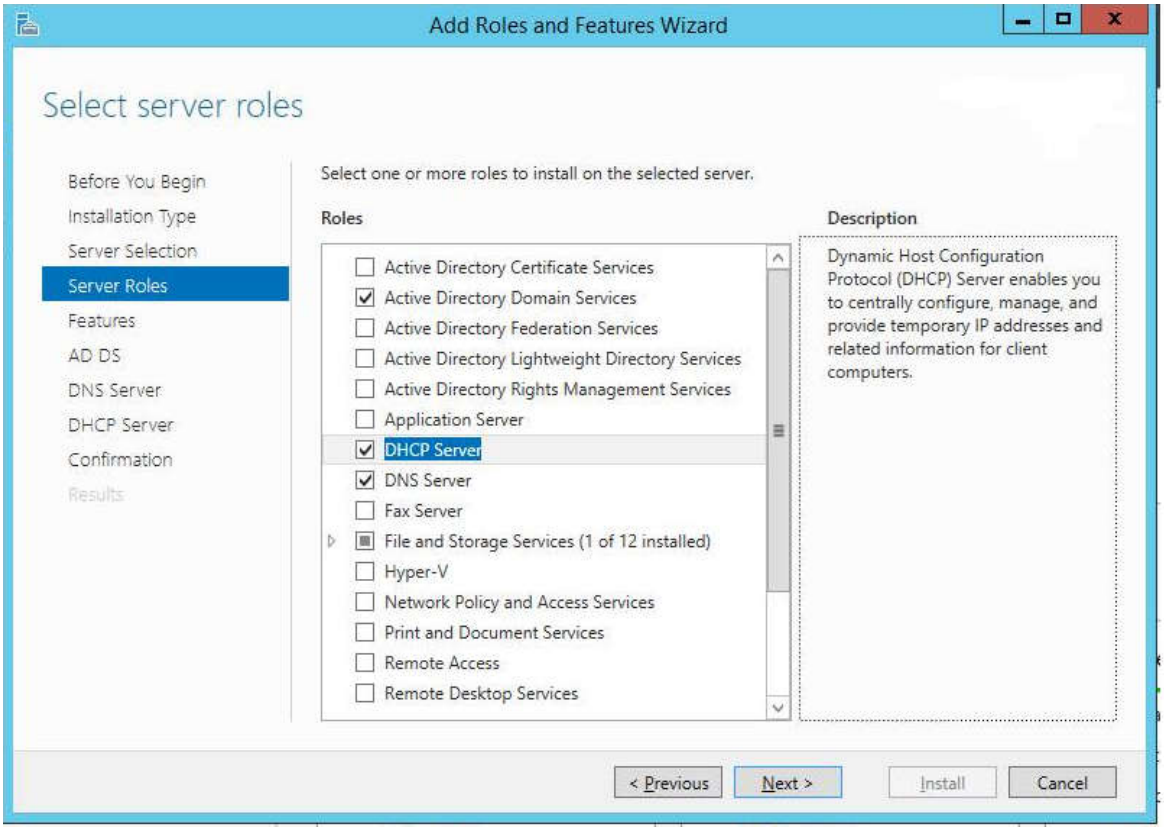

Figure 11 Përzgjedhja për instalim e AD, DHCP dhe DNS.

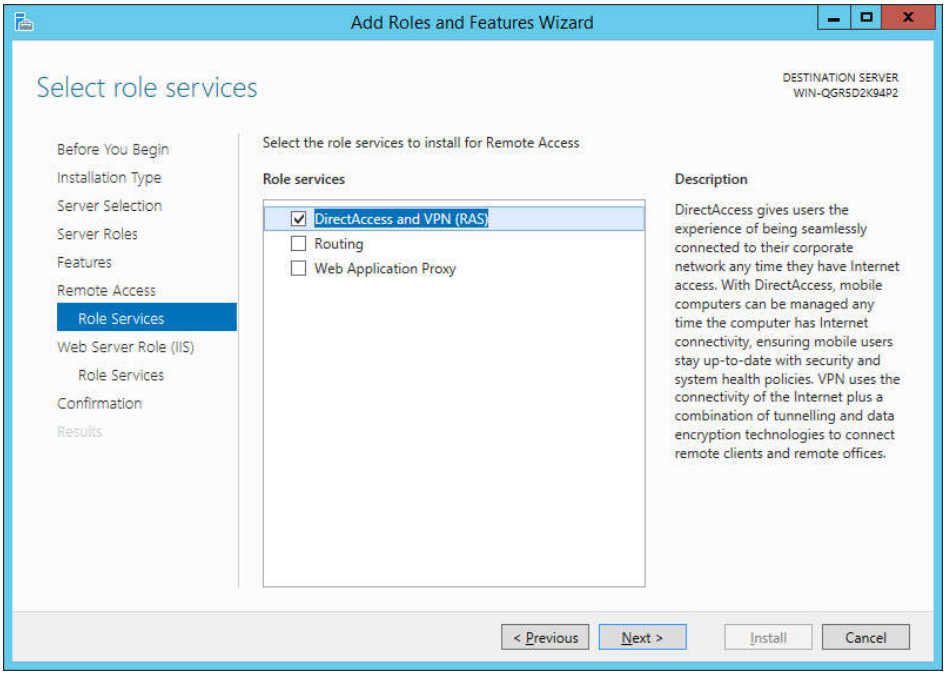

Figure 12 Përzgjedhja e roleve të shërbimit

Më pas vendosim kredenciale të tilla si emri i domain, apo emri NetBios e cila zakonisht është emri root i domain.

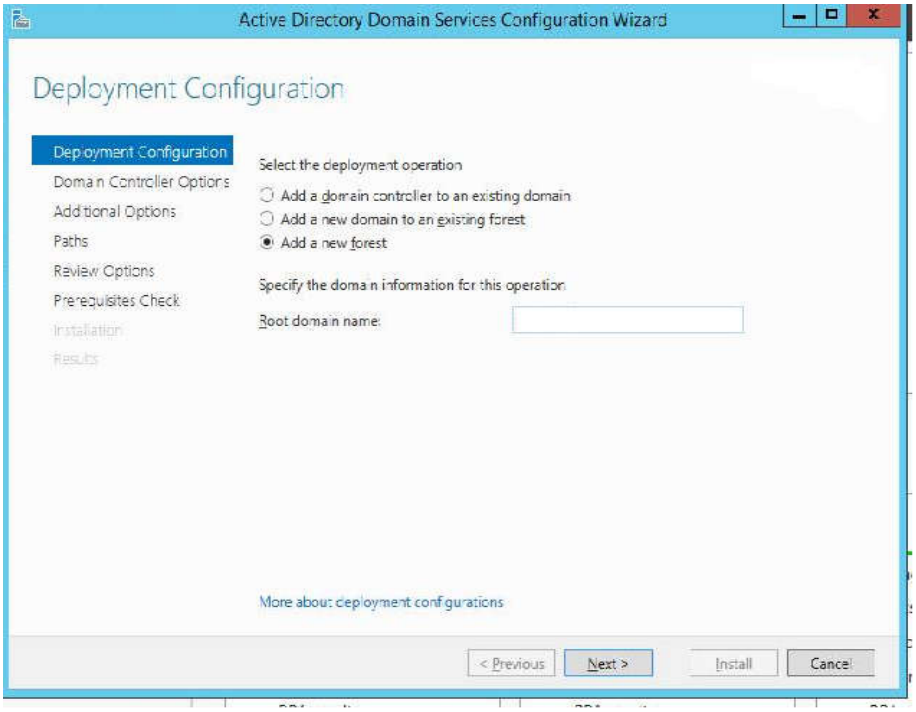

Figure 13 Vendosja e domainit për në direktorinë active

Pasi zgjedhim root.domain name e cila do të na shërbejë si emri root ne Active Directory e cila do të na shërbejë si domain kur të aksesojmë AD nga VPN.

Ne zgjedhim edhe emrin për NetBIOS që kryesisht zgjidhet emri root i Active Directory.

NetBIOS (Network Basic I/O System) mundëson aplikacione në kompjutera të ndarë të komunikojnë përgjatë rrjetit lokal. NetBIOS nuk është një protokoll rrjeti. Sistemet e vjetra e ekzekutojnë NetBIOS me IEE 802.2 dhe IPX/SPX. Në sistemet e reja normalisht NetBIOS ekzekutohet mbi TCP/IP nëpërmjet protokollit NBT (NetBIOS over TCP/IP). Kjo sjell si rezultat në secilin kompjuter në rrjet kemi adresë IP dhe emër BIOS që korespondon me një emër host.

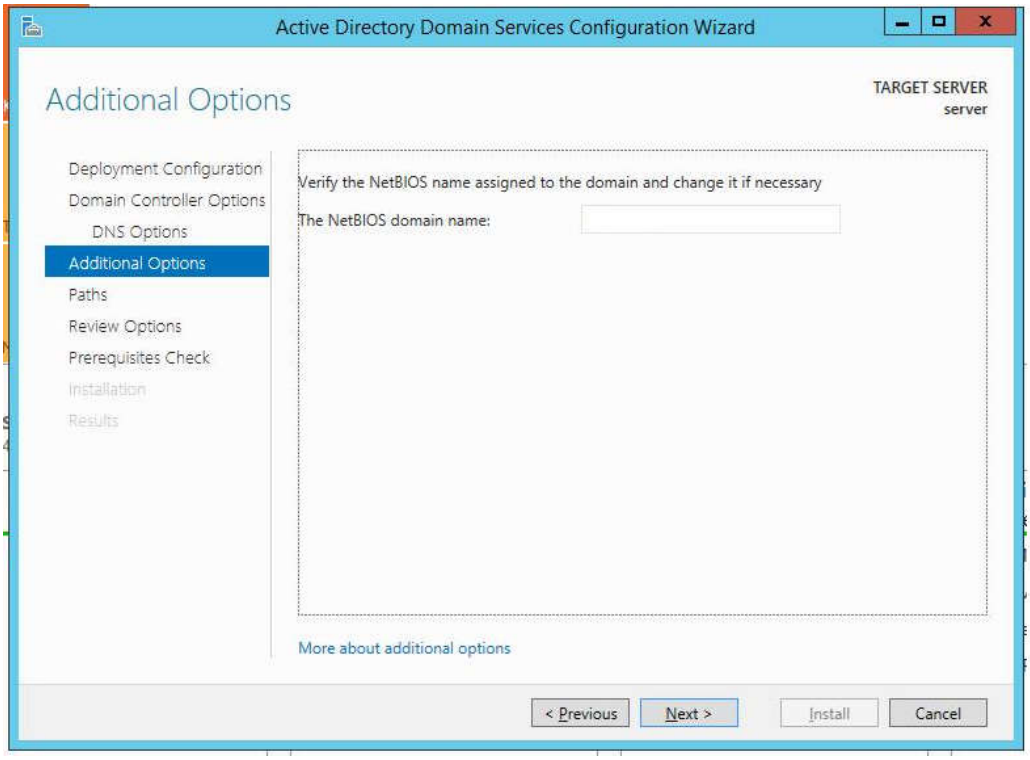

Figure 14 Vendosja e NetBIOS.

Më pas instalohet “Remote Acess” tek serverat e instaluar, e cila do të shërbejë për lidhjen me Active Directory duke ditur që aksesi në distancë është në vetvete qëllimi i VPN.

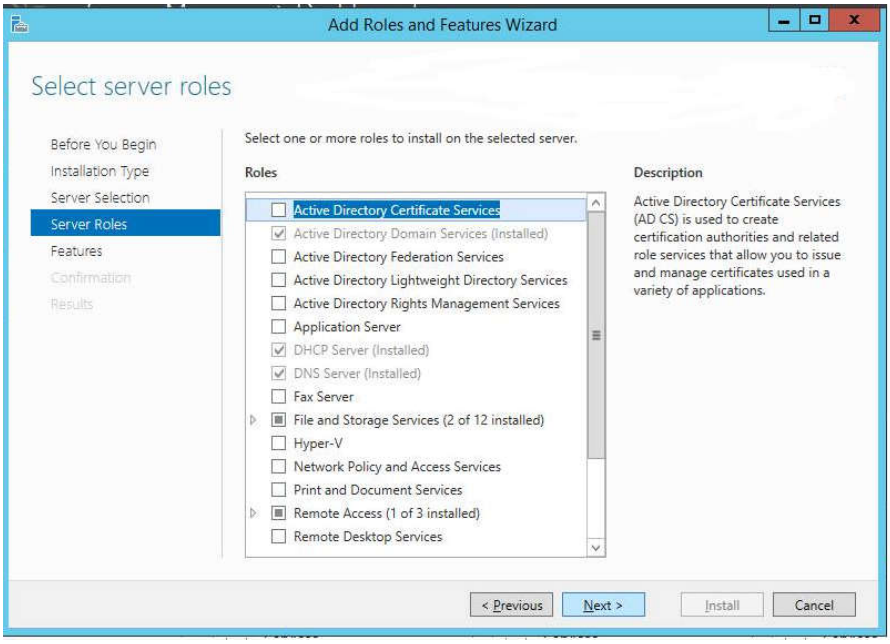

Figure 15 Instalimi i Remote Acess

4.1.2 Konfigurimi i VPN server.

Më pas Remote Acess del tek Server Manager të cilin mund ta konfigurojmë duke shkuar tek "Open Getting Started Wizard" dhe përzgjedhur llojin e lidhjes që do krijojmë DirectAcess, VPN apo të dyja bashkë. Më pas përzgjedhim opsione të konfigurimit të VPN të përzgjedhura si më poshtë.

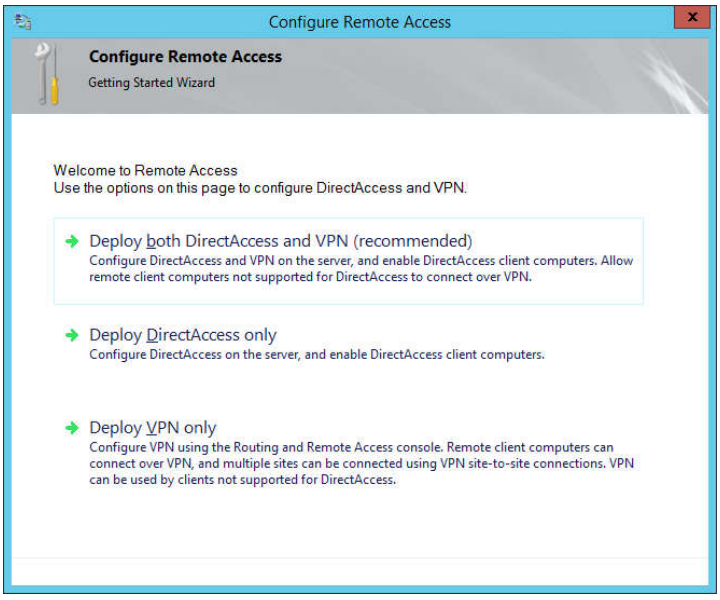

Figure 16 Konfigurimi i aksesit në distancë

Përzgjedhja e shërbimit DirectAcess apo VPN Në ndryshim nga VPN që duhet që klienti të iniciojë lidhjen, në rastin e DirectAcess kjo lidhje qëndron për sa kohë përdoruesi është në internet. Më pas futemi tek profili i Routing dhe Remote Acess për të konfiguruar llojin e veçorive të lidhjes, të cilat tregohen sipas figurave vijuese.

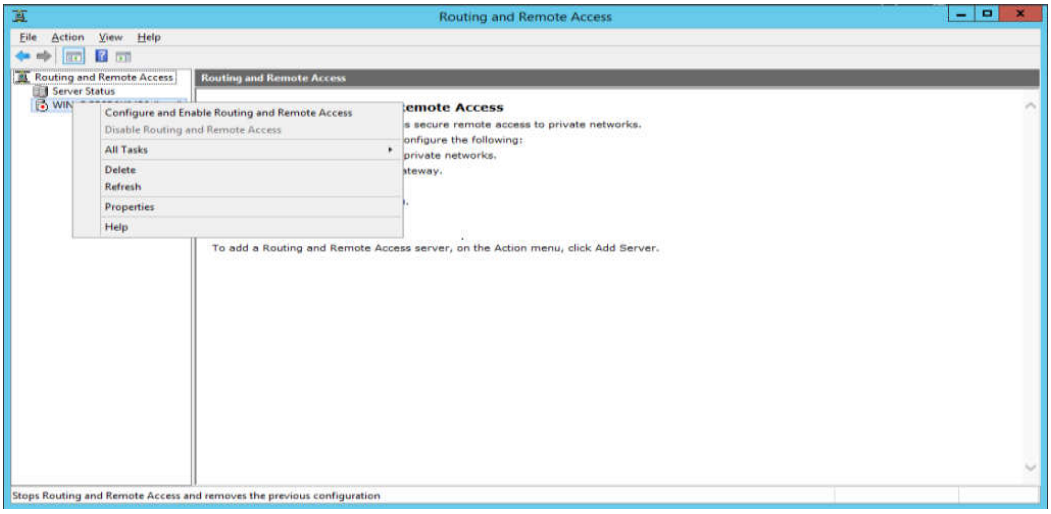

Figure 17 Konfigurimi i acess remote nga Serveri.

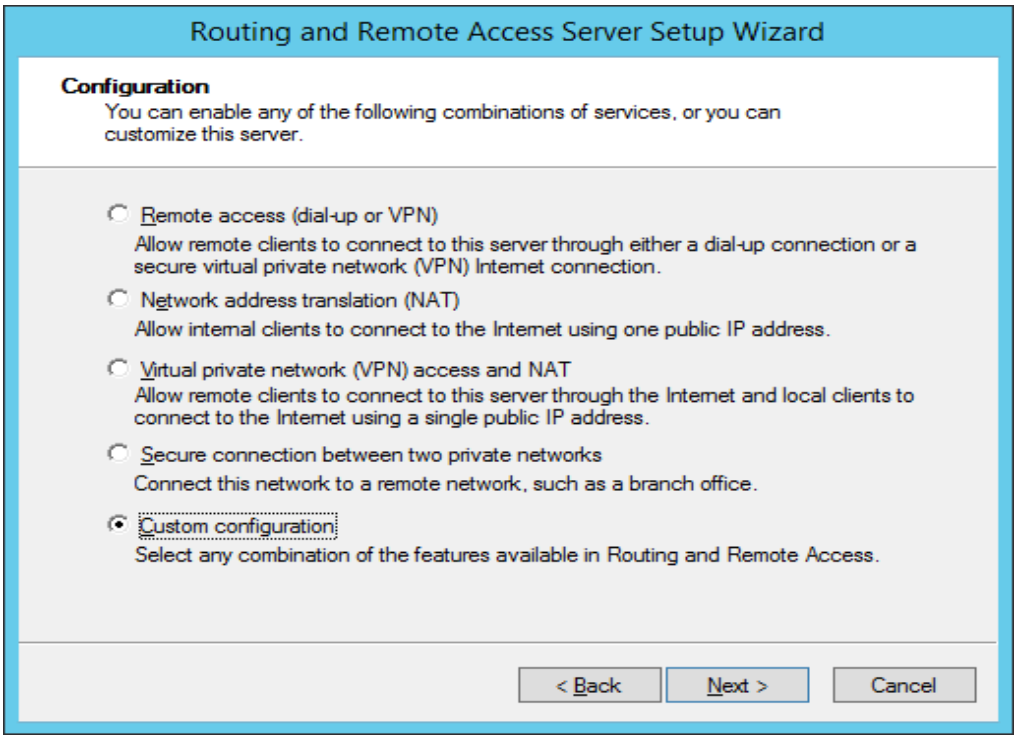

Figure 18 Përshtatja në konfigurimin e serverit të aksesit në distancë.

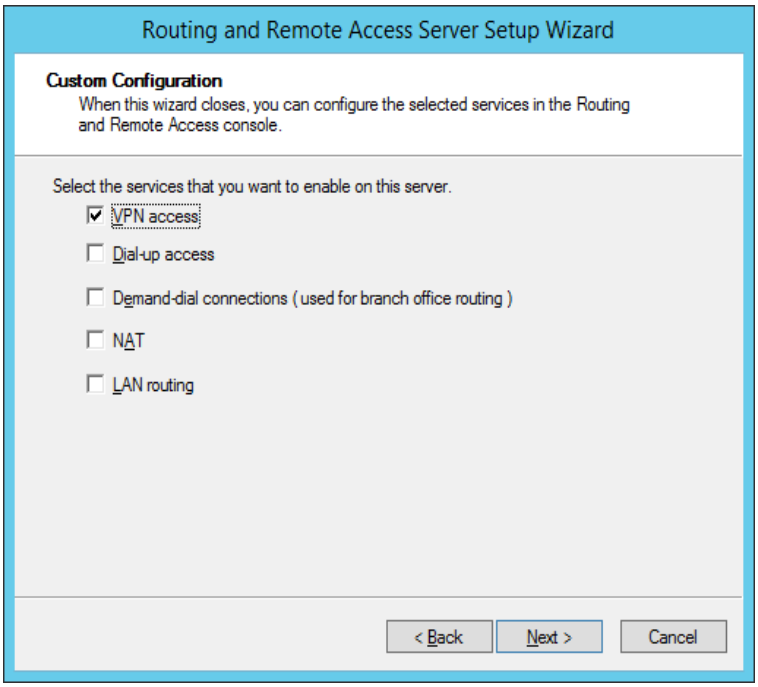

Figure 19 Përzgjedhja e VPN nga llojet e aksesit në distancë.

4.1.3 Konfigurimi i Active Directory

Në foton më poshtë vendoset username e cila lidhet me domain root që u krijua në fillim sapo u instlua AD. Domaini bejane.al do të shërbejë për tu loguar në AD por ky domain shpesh përdoret edhe si domain tek mail serverat të cilat lidhen me AD në kompani të ndryshme për përdorim nga punonjësit e saj. Përdoruesit i vendosim emër/mbiemër/ si dhe përshrime të tjera të tij. Në Active Directory sipas punës dhe hierarkisë së punonjësit i vendosen atribute, por ne nuk e kemi bërë një gjë të tillë sepse qëllimi i krijimit të këtij profile është që të shërbejë për lidhjen e VPN.

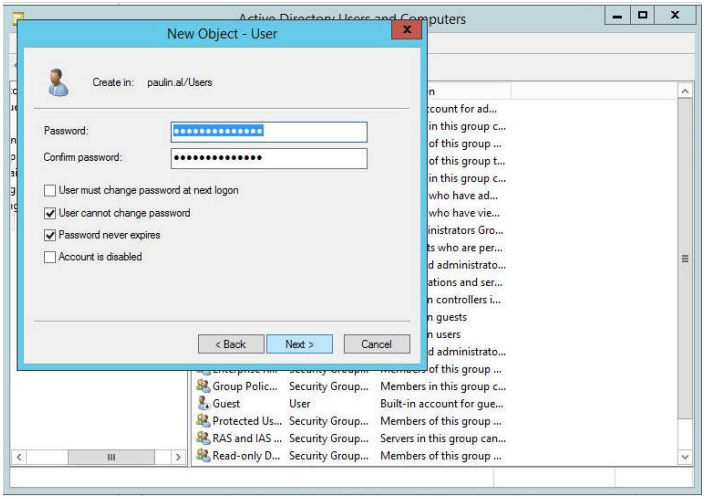

Figure 20 Vendosja e kredencialeve në Acitve Directory

Për arsye testi vendosëm që mos ndryshohet passëord si dhe afati i përdorimit të tij mos të jetë i kufizuar ashtu si ndodh në AD kur për arsye sigurie fjalëkalimet përditësohen shpesh.

Në foton më poshtë vendoset username e cila lidhet me domain root që u krijua në fillim sapo u instlua AD. Domaini bejane.al do të shërbejë për tu loguar në AD por ky domain shpesh përdoret edhe si domain tek mail serverat të cilat lidhen me AD në kompani të ndryshme për përdorim nga punonjësit e saj.

4.2 Konfigurimi I lidhjes klient-server.

Konfigurimi i klientit bëhet duke marë disa të dhëna si IP, dhe duke vendosur saktë të dhënat e mara nga profili i Active Directory, më pas do të përzgjidhet edhe lloji i enkriptimit, tynelit dhe veti të tjera që endihmojnë mjaft VPN të rrisë sigurinë e saj.

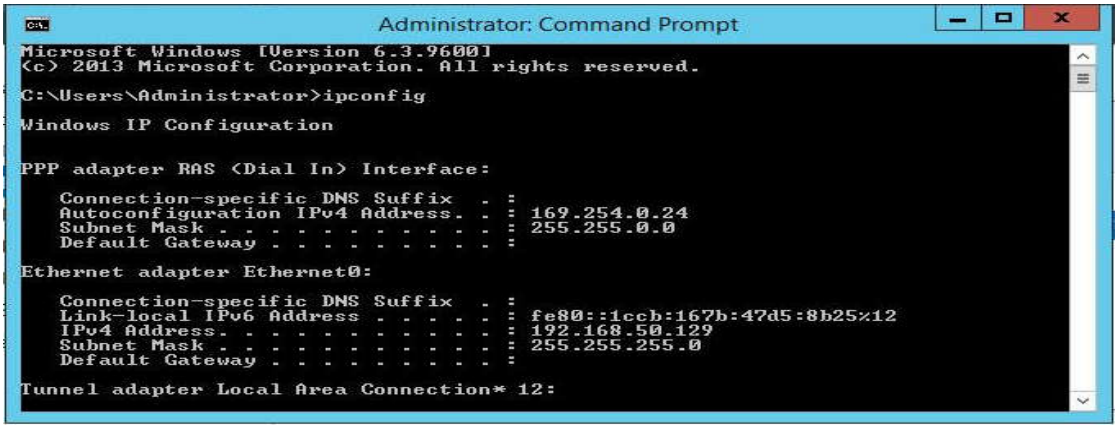

Figure 21 Konfigurimet IP në Windoës

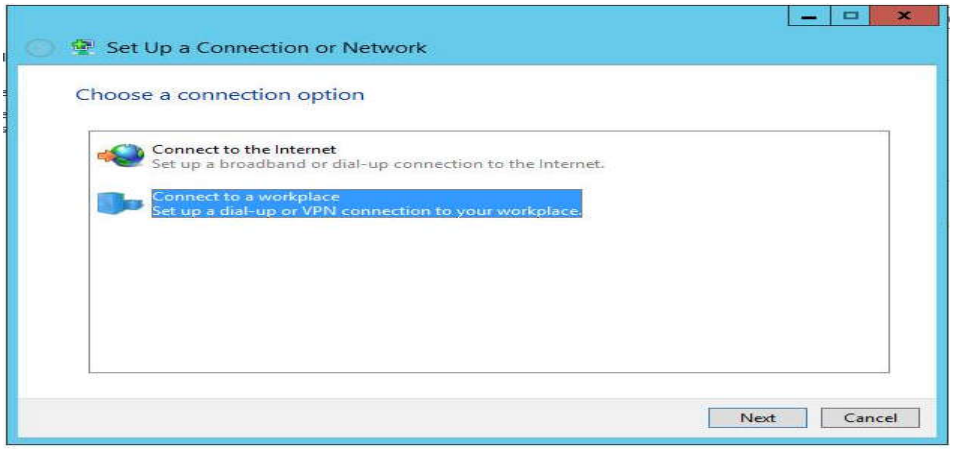

Figure 22 Krijimi i lidhjes sVPN,

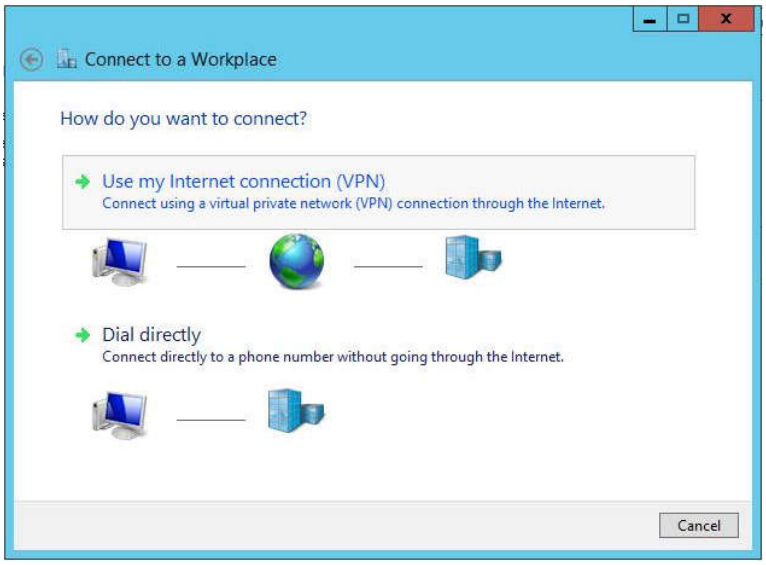

Figure 23 Përzgjedhja e internetit për tu lidhur me serverin AD.

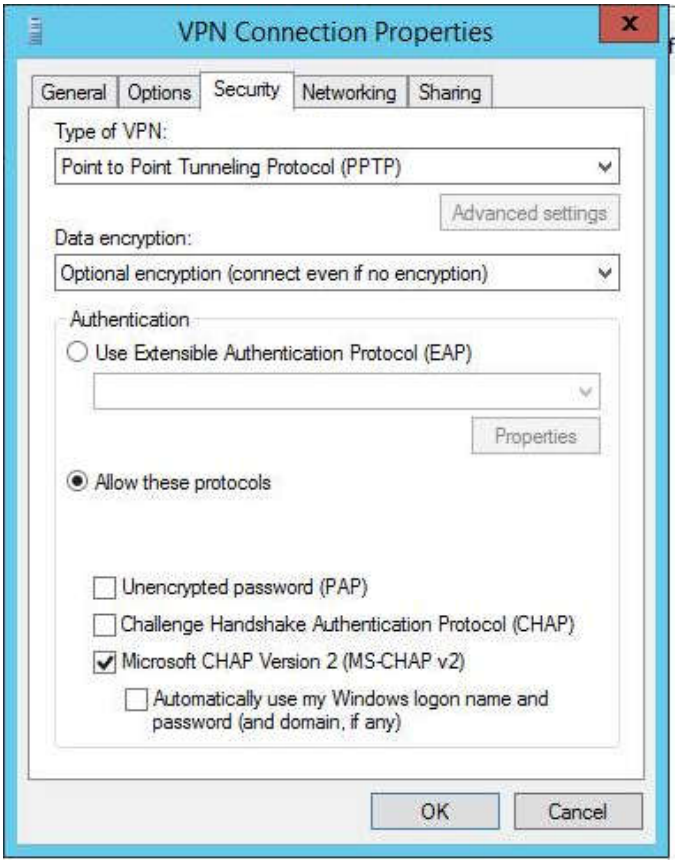

Figure 24 Përzgjedhja e vetive të VPN.

Figure 25 Pamja pas përfundimit

Përdoruesi akseson AD me anë të profilit të tij në VPN duke përdorur username/password dhe domain profilin e tij në Active Directory.

Përfundime

Siguria është një 'hot topic' sot, pra një temë e nxehtë e cila ka sjellë shumë diskutime dhe probleme. Sidomos për kompanitë e ndryshme ky problem dhe kjo çështjë bëhet dhe më aktuale pasi humbja e të dhënave apo interceptimi ose ndryshimi i tyre nga palë të treta nënkupton vdekjen dhe rrënim të saj. Një nga mënyrat e gjetura dhe përdoruara masivisht sot janë dhe VPN, një rrjet virtual privat që siguron komunimim të painterceptuar në rrjet.

Duke demonstruar karakteristikat dhe komponentët e ndryshëm të kësaj teknologjie, duke vijuar me implementimin e saj, është arritur të krijohet një panoramë e plotë dhe bazë për kuptimin dhe zhvillimin e individual.

Referencat

1. **Khiza, Joseph Miga.** *Guide to Computer Netëork Security.* Tennessee : s.n., 2014. ISBN 978-1-4471-6653-5.

2. *VPN Security.* **Infosec.** 2008, Government of Hong Kong, p. 24.

3. Hoë Virtual Private Netëorks Ëork. *CISCO.* [Online] 10 13, 2008. http://ëëë.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-hoë-vpn-ëorks.html.

4. **Charile Scott, Paul Ëolfe, Mike Erëin.** *Virtual Private Netëorks, Second Edition.* 1999. ISBN: 1-56592-529-7.

5. **Kessler, Gary C.** *Gary Kessler.* [Online] 2015. http://garykessler.net/library/crypto.html.

6. **Compaq.** [Online] 1999. ftp://kierer.at/compaq/partners/microsoft/infolib/ecg5150899.pdf.

7. **Microsoft.** [Online] https://technet.microsoft.com/en-us/library/cc977622.aspx.

8. **Craëford, Douglas.** PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2. *Bestvpn.* [Online] May 1, 2013. [Cited: September 14, 2015.] https://ëëë.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/.

9. **Christos Douligeris, Dimitrios Serpanos.** *Netëork Security, Current Status and Future Directions.* 2007. ISBN 978-0-471-70355-6.

10. **M.Maghales, Ricky.** Secure Socket Tunneling Protocol. *ËindoësSecurity.* [Online] April 17, 2007. [Cited: September 16, 2015.] http://ëëë.ëindoësecurity.com/articles-tutorials/fireëalls_and_VPN/Secure-Socket-Tunneling-Protocol.html.

11. CISCO https://www.cisco.com/c/en/us/products/ios-nx-os-software/ethernet-vpn.html