Republika e Shqipërisë
Universiteti i Tiranës
Fakulteti i Ekonomisë
Departamenti i Statistikës
dhe Informatikës së Zbatuar
Grupi: IE 304

Mikrotezë

Datë: 02/10/2018

VIRTUAL PRIVATE NETWORK- IMPLEMENTIMI I SIGURISË NË RRJET

Punoi:
Egli Menkshi

Pedagogu Udhëheqës:
Prof. Dr. Fatmir MEMAJ

"Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security."
—John Allen Paulos

Hyrje

Duke qënë se Interneti po i bën gjithmonë e më të parëndesishme distancat ndërmjet njerëzve, fenomeni i privatësise po bëhet gjithmone e më shqetësues.

Sot, siguria është një ndër prioritet kryesore që merret në shqyrtim kur bëhet fjalë për dizajnimin dhe implementimin e rrjeteve kompjuterike.

Siguria e informacionit është një element i rëndësishëm i një organizate. Informacioni është një aset dhe si cdo aset tjeter i një organizate ai ka vlerën e vet. Format e reja te biznesit dhe ato ekzistuese jane maturuar dhe jane te pirua te pranojne faktin se risqet e sigurisë së informacionit mund të kenë një ndikim negativ në procesin e vazhdimësisë te biznesit, të imazhit publik, të marrëdhënieve midis organizatave, mund të shkaktojnë humbje financiare, të ndikojnë në marrëdhëniet me klientët, partnerët si dhe të krijojnë probleme me Konfidencialiteti, integriteti dhe disponueshmëria e informacionit janë tre karakteristikat kryesore të sigurisë.

Kështu që, në këtë mikrotezë, materiali është përgatitur në mënyrë të tillë që të japë një ide sa me të qartë rreth rrjetave privatë virtualë dhe firewalleve, duke i përshkruar ato nga ana teknike dhe funksionale.

I. Kapitulli 1 - Siguria në rrjeta

1. Njohja me Sulmuesit

Kercenuesit e sigurise ne rrjet mund te kategorizohen si me poshte :

- **Sulmuesit e jashtem**: Persona te cilet nuk kane te drejte aksesi ose leje ne rrjetin tone por perpiqen te perdorin Internetin ose menyra te tjera per te fituar akses.
- **Sulmuesit e brendshem** : Zakonisht jane punonjes te pakenaqur, keqdashes ose ndonje pale kontraktuese e cila nuk eshte shperblyer sipas kushteve te paracaktuara.
- **Sulmuesat fillestare** (Script Kiddie Threats): Persona pa eksperience te cilet perdorin mjete (tools) te gatshme te ofruara ne site pirate Interneti (black hat).
- **Sulmuesat eksperte** (Expert Threats): Hackers te afte ne programim te cilet krijojne kercenime shume me serioze (viruse, worms, Trojan apo tipe te ndryshme spyware-esh). Ne se motivohen nga keqdashja apo nga konkurrenca, keto sulmues mund te realizojne qellimet ne menyre te suksesshme ne rrjet dhe te krijojne probleme. Zakonisht skriptet e shkruajtura nga keto eksperte i jepen “fillestareve” per ekzekutim.

2. Procesi i sulmit ne rrjet

Sulmet ne rrjet perfshijne proceset e meposhtme :

- **Reconnaissance** (studimi, njohja e terrenit): Fillimi i çdo sulmi eshte zbulimi i sa me shume informacioni rreth viktimes. Per shembull ne se deshirojme qe te aksesojme resurset e nje kompanie, nje fillim i mire do te ishte te vizitonim faqen e internetit te saj per te marre informacion te pergjithshem. Ne se duam te infiltrohemi ne rrjetin e brendshem te saj ne mund te kryejme nje skanim portash TCP dhe UDP per te pare se cilat porta jane te lejuara dhe cilat jane te bllokuara.
- **Exploitation** (shfrytezimi): Pasi kryejme studimin, duhet te veprojme pra te infiltrohemi ne rrjet. Nje gje e tille mund te kryhet me menyrat e meposhtme :
  - Vjedhja e passworde-ve
  - Inxhinieri sociale
  - Perdorimi i sistemeve te pastandartizuar
  - Nxjerrje e informacionit
- **DoS** (Denial of Service) : Mohimi i sherbimi ndalon resurset e rrjetit qe te vendosen ne dispozicion te perdoren

3. Fazat e mbrojtjes

Siguria eshte nje cikel i perbere nga shume procese dhe jo nje aktivitet te vetem, është një grumbull i rregullave, udhëzuesve dhe listave të kontrollit. Fazat e sigurise ndahen ne:

- **Parandalimi:** Stopimi i kercenimeve. Eshte utopike realizimi i nje rrjeti plotesisht te sigurte por ajo qe mund te arrijme eshte arritja e nje niveli te pranueshem josigurie. Sa me shume mbrojtje vendoset ne nje rrjet aq me shume kohe i duhet nje hacker-i qe te infiltroje ne te dhe aq me e madhe eshte koha per zbulimin e tij.
- **Zbulimi:** Procesi i percaktimit qe nje sulm eshte duke ndodhur. Eshte shume e rendesishme matja e politikave te ndjekura veçanerisht ne rastin e politikave te sigurise.
- **Vleresimi dhe pergjigja:** Vleresimi i problemit dhe i situates. Duhet t'i pergjigjemi pyetjeve ne vazhdim: Çfare ndodhi? Si ndodhi? Kur ndodhi? Sa ishte kostoja e sulmit? Pasi bejme vleresimin duhet te percaktojme pergjigjen pra masat qe duhen marre per te parandaluar qe nje sulm i tille te perseritet.
- **Korrigjimi:** Rregullimi i problemit. Ne shume raste zgjidhja nuk eshte e dukshme por eshte nje proces intuitiv. Integrimi i korrigjimit ne procesin e sigurise e ben ate nje cikel te mbyllur.

Pasi veprimi korrigjues eshte kryer, parandalimi ka te beje me aplikimin e rregullave te reja te sigurise ne firewall ose nje ACL (access control list) e re ne router. IDS (intrusion detection systems) na ndihmojne ne identifikimin e sulmeve qe mund te ndodhin. Si firewall-et ashtu dhe IDS mbajne shenime (logs) te cilat na ndihmojne ne vleresimin e problemeve eventuale.

Mjetet e sigurise jepen si me poshte :

- Parandalimi → Firewall dhe ACL e router-ave
- Zbulimi → IDS
- Vleresimi → Logging

4. Politikat e Sigurisë

Nje politike sigurie eshte hapi i pare kritik drejt sigurimit te rrjetit te nje organizate apo institucioni. Ne te bazohen te gjitha menyrat se si kjo organizate trajton çeshtjet e sigurise dhe se kush prej resurseve qe ofron ajo jane me te rendesishmet.

• Faktorët që duhen marr parasysh kur vendosim për komponentët e sigurisë
– Avantazhet dhe dis-avantazhet e komponentëve
– Tiparet dhe funksionet
– Kërkesat për ngritjen dhe mirëmbajtjen e tyre
– Kufizimet buxhetore
– Kërcënimet reale

Perveç perdorimit te pranueshem te politikave te sigurise, enkriptimit nje menaxhim i mire nevojitet per aplikimin e politikave specifike per firewall-in. Keto politika udhezojne konfigurimin e nje sistemi operativ sa me pavarur nga gabimet dhe te forcuar (duken

çaktivizuar sherbimet jo esenciale dhe duke lene vetem ato te domosdoshme), portat qe duhen hapur dhe proceduren per te hapur porta te reja. Gjithmone eshte e dobishme te aplikohet principi i *privilegjit minimal* i cili thote qe vetem resurset te cilat jane te domosdoshme per te kryer punen duhet te jene te aksesueshme.

II. Kapitulli 2 – VPN dhe karakteristikat e tyre

1. Çfarë është VPN ?

Për aq kohë sa interneti ka ekzistuar, ka pasur nevojë për protokolle për të mbajtur të dhënat private dhe të sigurta. Historia e teknologjisë VPN (rrjeti privat virtual) daton në vitin 1996, kur një punonjës i Microsoft-it zhvilloi protokollin e tunelimit peer-to-peer, ose PPTP. Teorikisht dhe mbase edhe në mënyrë abstrakte një VPN është një Rrjet Privat Virtual.

Fillimisht, VPN-të përdoreshin pothuajse ekskluzivisht në biznese. Megjithatë, fenomeni i shkeljeve të sigurisë në nivel të lartë që ndodhi në fillim të viteve 2000 ishte një moment kyç në historinë e teknologjisë VPN. Në këtë kohë, përdoruesit e përditshëm të internetit u bënë në dijeni të rreziqeve të vërteta të punës në internet dhe filluan të kërkonin mënyra më të sigurta për ta bërë këtë.

Sot, VPN-të përdoren për të siguruar lidhjet e internetit, për të parandaluar malware dhe hacking, për të siguruar privatësinë dixhitale, për të zhbllokuar përmbajtjen e kufizuar dhe për të fshehur vendndodhjet fizike të përdoruesve. Më e lehtë për t'u përdorur dhe më e përballueshme se kurrë, sot një VPN është një mjet thelbësor për të qëndruar i sigurt në internet.

2. Elementët e ndërtimit të një VPN-je

Meqënëse siguria është problemi kryesor, është në dorën tonë të merremi dhe ta mbrojmë atë nëpërmjet kriptimit duke e konfiguruar sipas qëllimeve tona. Duhet te kihet parasysh që një VPN nuk të ofron fleksibilitetin e kërkuar nqs. hasen shërbime kritike gjatë funksionimit të saj, gjithashtu edhe kur ajo përbëhet nga lidhje dial-up të cilat nuk janë shumë të shpjeta.

Standartet e tunelizimit të përdorura nga VPN-të Cisco janë: IPSec., L2TP dhe GRE, ndërsa në teknologjitë e kriptimit mund të përfshihen DES dhe 3DES.

Një VPN përbëhet nga një tunel privat dhe i sigurtë midis një pike të largët dhe një porte. Natyra e "ndjeshme" dhe disi problematike e disa komunikimeve bën të mundur që të perdorim **IPSec**. për të siguruar: 1) Integritetin 2) Konfidencialitetin dhe 3) Autentikimin.

a) Çfarë bëjnë këto sherbime:

Konfidencialiteti
Nëse dërgohet dicka, atëherë personi i dëshiruar mund ta lexojë atë, ndërkohe që pjesëtarë të tjerë mund ta kapin atë por nuk mund ta lexojnë. Kjo realizohet me anë të algoritmave të kriptimit si DES.

Integriteti
Ka të bëjë me sigurinë që të dhënat e transmetuara nga burimi në destinacionin e dëshiruar arrijnë pa gabime dhe deformime. Kjo sigurohet nga algoritma të përzjerjes si MD5.

Autentikimi
Ka të bëjë me njohjen që të dhënat e marra janë të njëjta me të dhënat e dërguara dhe që dërguesi që pretendon se i ka derguar është në fakt dërguesi i vërtetë. Kjo realizohet nga mekanizma siç është shkëmbimi i çertifikatave dixhitale.

b) Nje VPN e dizenjuar mire duhet te kete:

- Siguri
- Besueshmeri
- Mundesi Zgjerimi
- Menaxhim te rrjetit
- Menaxhim te politikave

3. Teknologjite e ndryshme VPN

VPN-të mund të paraqiten në forma të ndryshme dhe të implementohen në një varietet të ndryshëm rrugësh. VPN-të mund të klasifikohen jo vetëm duke u bazuar në shtresën e modelit OSI të cilën ato implementojnë por edhe mbi bazën e cilës model VPN-je ato mbështeten dhe paraqesin.

Modeli Peer

Modeli *peer* i VPN-së është ai model në të cilin përcaktimi i rrugës (path-it) në shtresën e rrjetit kryhet duke u bazuar në parimin e "kërcimit", kërcim-pas-kërcimi (hop-by-hop). Nyjet e anës ose të skajit (ana e "klienit") formojnë një lidhje ose marrëdhënie peer të lidhur me shtresën e rrjetit, me një VPN service provider dhe zgjedhin rrugën më të mirë në rrjet për në destinacionin final, ndryshe nga një mënyrë tjetër në të cilën rruga në rrjet është e parapërcaktuar.

Modeli Overlay

Modeli VPN-së *overlay* do të quhet ai model në të cilin përcaktimi i rrugës në shtresën e rrjetit për tek një nyje skaji bëhet në bazë të parimit "cut-through" (kalim-mes-përmes). Shtresa e rrjetit nuk ka "dijeni" për infrastrukturën bazë. Të gjitha nyjet e "skajit" (ana e "klientit") janë efektivisht një hop-kërcim larg nga njëra-tjetra, pavarësisht se sa kërcime (hop-e) ekzistojnë fizikisht ndërmjet tyre.

VPN-të e shtresës së linjës (Link Layer VPNs)

VPN-të e shtresës së linjës implementohen në shtresën e dytë (shtresa e data link-ut) të modelit referues OSI. Kjo shtresë siguron platformën e përgjithshme të rrjetëzimit, ndërkohë që rrjetat diskrete ndërtohen në shtresën e rrjetit. VPN-të e ndryshme ndajnë të njëjtën ifrastrukturë, por ato nuk kanë dallueshmëri nga njëra-tjetra. Ndryshimi midis këtij modeli dhe atij të qarqeve te dedikuara është se nuk ekziston asnjë orë (clock) e sinkronizuar e të dhënave midis dërguesit dhe marrësit, si dhe nuk ekziston asnjë rrugë (path) transmetimi e siguruar nga rrjeti bazë. Rjetet Frame Relay dhe ATM janë shembuj të VPN-ve të shtresës së linjës.

VPN-të e shtresës së rrjetit

Këto lloj VPN-sh janë të implementuara në shtresën e tretë (shtresa e rrjetit) të modelit OSI. Do të paraqesim dy tipet e VPN-ve që implementohen në shtresën e rrjetit: Rjetat "Tunneling" dhe Rrjetat Privatë Virtualë "Dial" (VPDN).

VPN-të "Tunneling"

VPN-të "Tunneling" po bëhen shumë të përhapura dhe zgjerimi më i madh i VPN-ve parashikohet në këtë drejtim. Tunelet mund të krijohen një router-i burim dhe një router-i destinacion, mund të jënë gjithashtu edhe të tipit router-me-router (router-to-router), ose hot-me-host (host-to-host). Tunelimi ("tunneling") mund të jetë "point-to-point", ose "point-to-multipoint", por tunelimi point-to-point është më i shkallëzueshëm se ai point-to-multipoint. Kjo gjë vjen sepse tunelimi point-to-point kërkon më pak menaxhim "nga lart", duke e parë nga pikëvështrimi i mirëmbajtjes.

Një nga avantazhet më të mëdha të *"tunneling"* (tunelimit) është se lidhja **"backbone"** e VPN-së dhe subnet-et e lidhur VPN nuk patjetër të kenë adresa unike rrjeti. Kjo është shumë e rëndësishme nqs do të konsiderojmë numrin e madh të organizatave që përdorin një hapësirë adresash private.

Një VPN që përdor tunelimin mund të ndërtohet me dijen ose jo të network provider-it (siguruesit të rrjetit) dhe mund të përfshijë disa network provider-a. Natyrisht që performanca do të rrezikohej disi nqs service provider-i (siguruesi i shërbimit) nuk është në dijeni të tunelimit të përdorur dhe nuk siguron kualitet shërbimi adekuat.

Enkapsulimi i përgjithshëm Cisco i routimit (Generic Routing Encapsulation – GRE) përdoret për tunelimin midis router-it burim dhe atij destinacion, si dhe për router-me-router. Tunelet GRE sigurojnë një rrugë specifike brënda një WAN-i të shpërndarë duke enkapsuluar trafikun me "header-a" të rinj paketash për të siguruar arritjen në destinacionin specifik. Një tunel GRE konfigurohet midis një router-i burimi (ingress) dhe një router-i destinacion (egress). Paketat e caktuara për tu dërguar nëpër tunel enkapsulohen me një header GRE, transportohen nëpër tunel drejt adresës destinacion, dhe më pas i hiqet header-i GRE. Protokollet L2TP (Layer 2 Tunneling Protocol) i IETF dhe PPTP (Point-to-Point Tunneling Protocol) i Microsoft-it përdoren për tunelimin host-to-host. PPTP-ja nuk mund të funksionojë efektivisht pa disa gjëra sigurie shtesë (features), si psh. ato të siguruara nga IPSec. meqënëse dihet që ky protokoll ka probleme dhe cënueshmëri në sigurinë. Disa nga këto cënueshmëri (vulnerabilities) janë pakësuar me forcimin e mekanizmit të autentikimit PPTP, por përsëri mekanizmat e sigurisë sigurojnë një mbrojtje të dobët dhe janë të cënueshëm nga sulmet.

Tunelimi host-to-host është shumë më i sigurtë se ai router-to-router, për vetë faktin që tunelimi host-to-host mund ta enkriptojë të gjithë shkëmbimin e mesazheve. Kjo gjë nuk ndodh në tunelimin router-to-router, sepse në këtë lloj tunelimi vetëm tuneli enkriptohet, ndërkohë që anët ose pjesët host-router dhe router-host në të dy anët e "konversacionit" ngelen të paenkriptuara. Tunelimi konsiderohet si një model VPN-je *overlay*.

Rrjetat Private Virtualë "Dial"

VPDN-të që përdorin Internetin si një bartës të trafikut të aksesit në distancë
janë bërë shumë "popullore". Këto lloj VPN-sh jo vetëm që ulin koston në mënyrë reale, por por sigurojnë edhe një fleksibilitet të dukshëm. Çdo pikë prezence e ISP-së (PoP – Point of Presence) përdoret për të siguruar shërbime të sigurtë aksesi RAS me një kosto sa më të vogël. L2TP-ja dhe PPTP-ja janë fondamentale për design-in VPDN dhe sigurojnë feature-at e tunelimit nëpërmjet të cilave trafiku RAS "arrin" shërbimin e dëshiruar. Një VPDN mund të përfshihet në modelin *overlay* të VPN-ve.

VPN-të e shtresës së Transportit dhe Aplikacionit

Këto VPN implementohen në shtresën e transportit dhe aplikacionit (Shtresat 4 dhe 5) të modelit referues OSI. Këto lloj implementimesh kërkojnë që aplikacioni të jetë në dijeni të VPN-së dhe kështu që duhet tën ndërtohen me duke pasur parasysh këtë gjë. Megjithatë sigurisht që kjo lloj forme e VPN-së nuk është e zakonshme.

Intranet VPN-të

Një VPN intranet i lidh zyrat qëndrore të një ndërmarrjeje, zyrat në distancë dhe zyrat e degëve në një rrjet të brendshëm nën një infratrukturë të shpërndarë duke përdorur lidhje të dedikuara. Intranet VPN-të ndryshojnë nga extranet VPN-të sepse ato sigurojnë vetëm akses-in tek klientët e punësuar të ndërmarrjes. Në figurën më poshtë jepet një skenar në të cilin një klient VPN komunikon dhe lidhet me router-in VPN me mënyrën Dial-up.

Extranet VPN-të

Një VPN extranet lidh klientë të jashtëm, furnitorë, partnerë dhe grupe interesi në një rrjet klientësh të ndërrmarrjes nën një infrastrukturë të shpërndarë duke përdorur lidhje të dedikuara. Extranet VPN-të ndryshojnë nga Intranet VPN-të sepse ato sigurojnë akses tek përdorues qe janë jashtë ndërmarrjes.

Access VPN-të

Një *access* VPN siguron akses në distancë, të largët në intranetin ose extranet-in e klientëve të një ndërmarrjeje, nën nje infrastrukturë të shpërndarë. Access VPN-të përdorin linjë analoge me dial-up, ISDN, DSL, IP të lëvisshme dhe teknologji kabujsh të ndryshëm. Ato lidhin në mënyrë të sigurtë përdorues të lëvizshëm, zyrat e degëve etj.

Përdoruesit në distancë

Interneti ofron një alternativë me kosto të ulët për ti dhënë mundësi përdoruesve të largët të aksesojnë rrjetin e korporatës. Në vend që të mbajë një sasi të madhe modem-ash dhe fatura telefoni me kosto të lartë, një sipërmarrje mund tu japi mundësi përdoruesve të largët të aksesojnë rrjetin përmes internetit. Vetëm me një thirrje telefonike lokale të ISP-së, një perdorues mund të aksesojë rrjetin e korporatës.

Çfarë është një tunel?

Një tunel është një tip kriptimi që e bën lidhjen nga një pikë në pikën tjetër të sigurt. Tuneli quhet virtual sepse ai nuk mund të aksesohet nga pjesa tjetër e lidhjes në internet.

4. Vështrimi funksional

Nga pikëvështrimi funksional VPN-të kategorizohen si VPN të aksesit në distancë ose si site-to-site.

VPN të aksesit në distancë u referohen implementimeve në të cilën përdorues individual në distancë, të referuar si punonjësit mobile, aksesojnë rrjetin e korporatës nëpërmjet PC-ve të tyre. Punonjësit mobile mund të përdorin lidhjet tradicionale dial-in në një service provider lokal, dhe më pas të inicializojnë tunelin deri te korporata.

VPN-të site-to-site u referohen implementimeve në të cilat rrjeti në një vendndodhje lidhet me një rrjet në një vendndodhje tjetër nëpërmjet një VPN. Paisjet e rrjetave autentikojnë njëra-

tjetrën dhe më pas vendosin lidhjen VPN midis siteve. Këto paisje më pas veprojnë si porta, duke e kaluar në mënyrë të sigurt trafikun në sitin e destinuar. Router-at ose firewall-et që suportojnë VPN-në dhe koncentratorët e dedikuar VPN, të gjithë e ofrojnë këtë funksion.

Ky dallim midis VPN-ve të aksesit në distancë dhe site-to-site bëhet gjithmonë e më i zbehur, ndërkohë që paisje të reja, si klientet hardëare VPN, bëhen gjithmonë e më të përhapur në përdorim. Paisje të tilla mund të shfaqen sikur janë një paisje e vetme që e akseson rrjetin, megjithëse mund të kemi një rrjet me disa paisje mbrapa kësaj.

III. Kapitulli 3 – Designet e perdoruesit ne distance

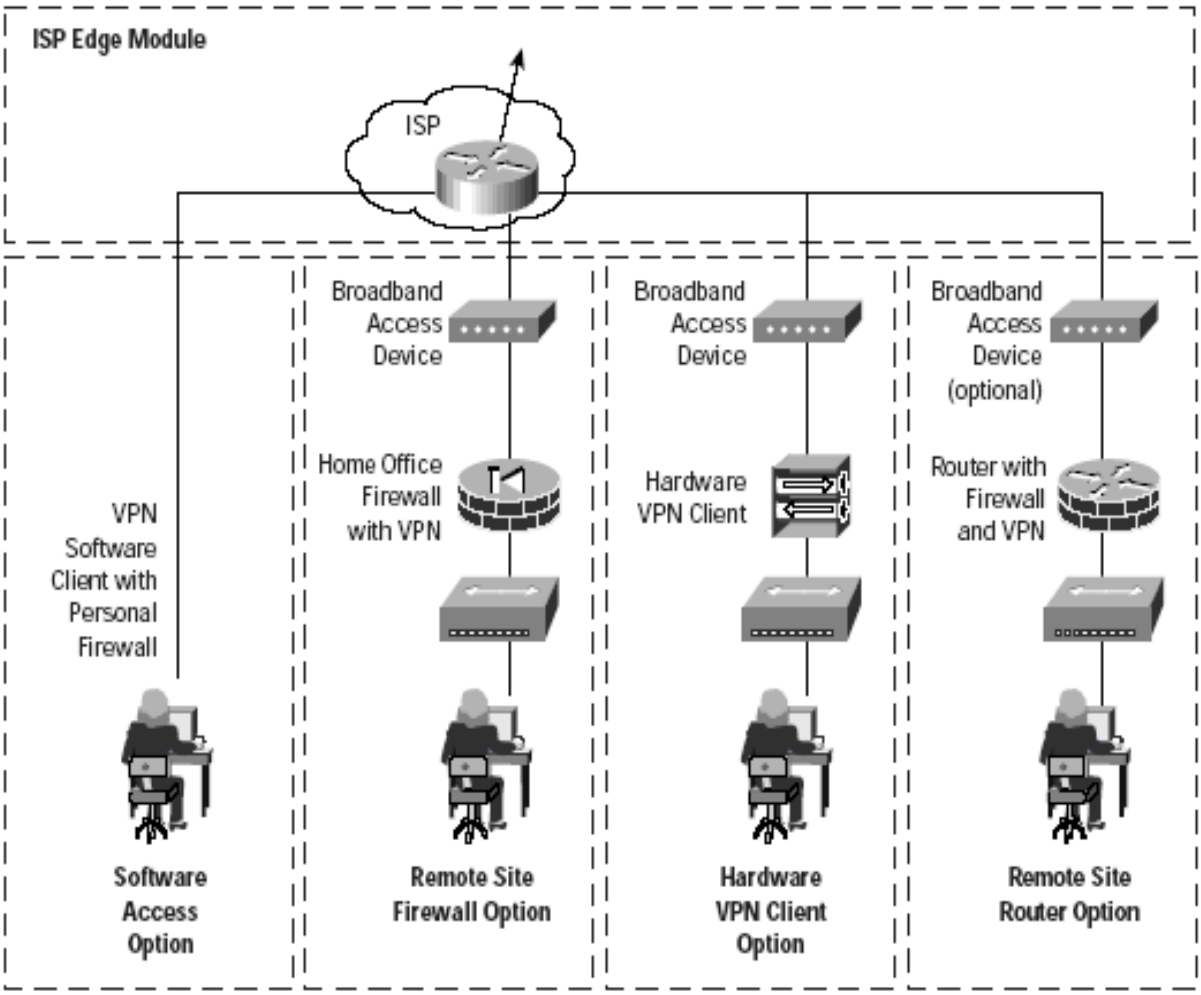
Ekzistojnë katër opsione për të siguruar lidhjet VPN të përdoruesve të largët me sitet e korporatës. Lidhjet në distancë aplikohen si në punonjësit mobile (të lëvizshëm) ashtu edhe në punonjësit shtëpi-zyrë. Qëllimi kryesor i këtij design-i është që të sigurojë lidhje nga site-i në distancë te zyrat qëndrore të korporatës nëpërmjet ndonjë mjeti si interneti. Janë të vlefshme katër opsionet në vazhdim:

- *Opsioni me akses software* – përdoruesi në distancë me një klient VPN software dhe software personal firewalli në PC.

- *Opsioni remote-site firewall* – site-i në distancë i mbrojtur me një firewall të dedikuar që siguron “firewalling” dhe lidhje IPSec VPN me zyrat qëndrore të korporatës. Lidhja WAN sigurohet nëpërmjet një ISP-je, nëse zotëron paisje të aksesit me brez të gjerë (dmth DSL ose modem kabëll)

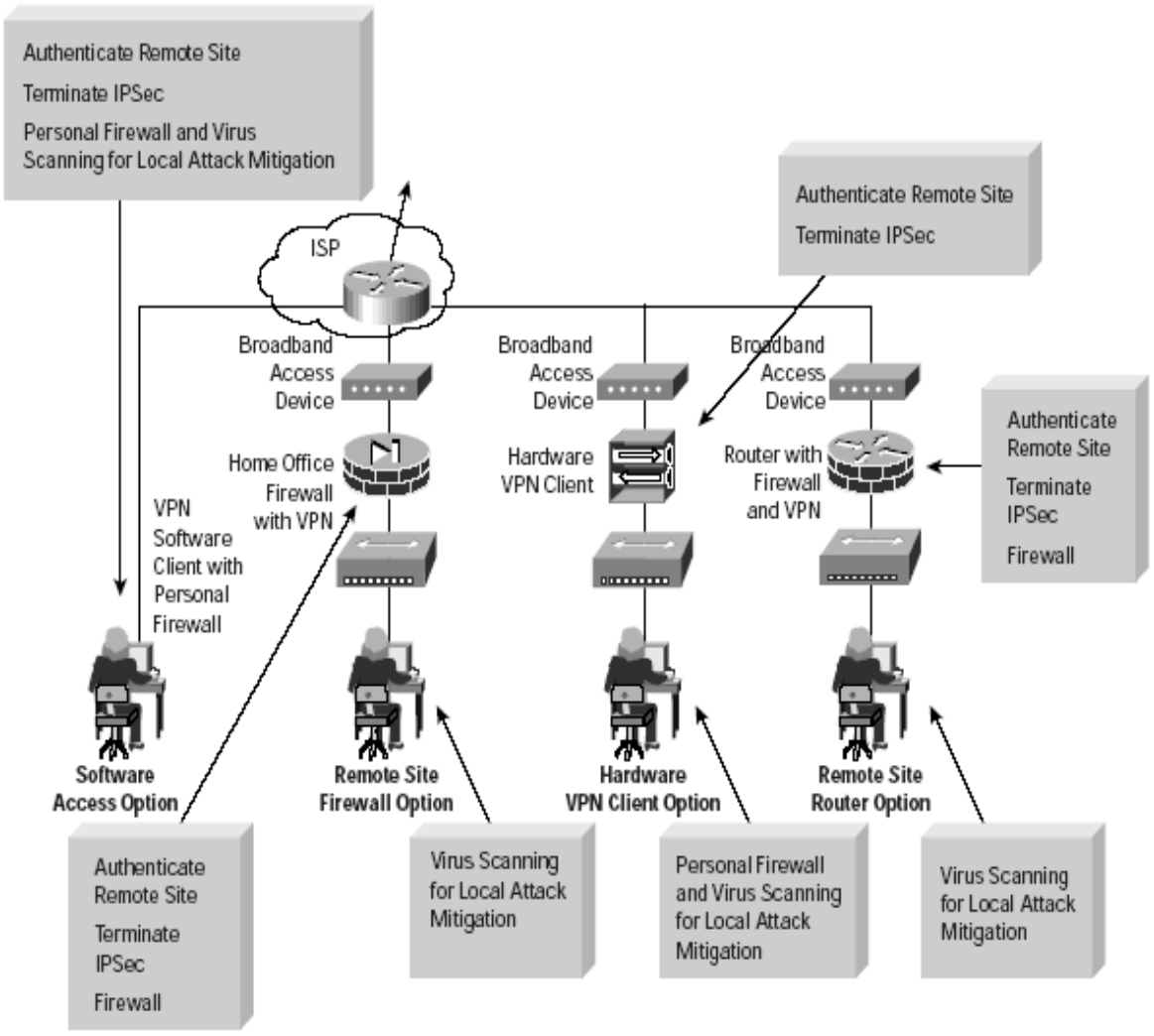
- *Opsioni hardware VPN client* – sitet në distancë që përdorin hardware VPN client të dedikuar, i cili siguron lidhje IPSec VPN me zyrat qëndrore të korporatës; lidhje WAN sigurohen nëpërmjet nje ISP-je, nëse zoteron paisje aksesi me brez të gjerë.

- *Opsioni remote-site router* – siti në distancë që përdor një router i cili siguron firewalling dhe lidhje IPSec VPN me zyrat qëndrore të korporatës. Routeri mund të sigurojë akses broadband të drejtpërdrejt ose të kalojë permes një ISP-je, nëse zotëron paisje aksesi broadband



1. Paisjet VPN kryesore

- *Paisjet e aksesit broadband* – siguron akses në rrjetin broadband (DSL, kabëll, etj.)
- *VPN firewall* – siguron tunele të sigurtë të kriptuar end-to-end midis site-it në distancë dhe zyrave qëndrore të korporatës; siguron mbrojtje në shtresën e rrjetit të burimeve të sitit në distancë dhe filtrim të plotë të trafikut.
- *Software firewall personal* – siguron mbrojtje në nivelin e paisjeve për PC individual
- *Opsioni router VPN me firewall* – siguron tunele të sigurtë të kriptuar fund-me-fund midis PC-ve individualë dhe zyrave qëndrore të korporatës.
- *VPN hardware client* – siguron tunele të sigurtë të kriptuar fund-me-fund.



2. Opsioni me akses software

Opsioni i aksesit me software është e lidhur me punonjësit mobile dhe shtëpi-zyrë. Ajo që i nevojitet përdoruesit në distancë është një PC me softëare VPN dhe lidhje me internetin ose me rrjetin e një ISP nëpërmjet një lidhje dial-in ose Ethernet. Funksioni kryesor i softwarit VPN klient është të vendosi një tunel të sigurtë të kriptuar nga paisja e klientit të një paisje VPN e zyrave qëndrore të korporatës. Aksesi dhe autorizimi janë të kontrolluara nga mjedisi i zyrave qëndrore kur filtrimi ndodh në firewall dhe në vetë klientin nëse të drejtat e aksesimit janë refuzuar nga polica e sigurisë. Përdoruesi i largët në fillim autentikohet, e më pas merren parametrat e IP, si adresën IP virtuale që përdoret për të gjithë trafikun VPN dhe vendndodhjen e serverave të emrave (DNS dhe WINS). Tunelizimi i ndarë mund gjithashtu të aktivizohet dhe çaktivizohet përmes sitit qëndror. Në këtë dizajn, tunelizimi i ndarë është çaktivizuar, duke e bërë të nevojshme për të gjthë përdoruesit në distancë të aksesojnë internetin përmes lidhjes së korporatës kur kanë vendosur një tunel. Duke qënë se përdoruesit në distancë mund të mos e

duan gjithmonë të aktivizuar tunelin kur lidhen me internetin ose me rrjetin e ISP, software firewall personal rekomandohet për të zvogeluar infektimet e PC nga viruset.

3. Opsioni remote-site firewall

Opsioni remote-site VPN firewall është e lidhur me punonjësit shtëpi-zyrë ose mundësisht një degë e vogël zyre. Me këtë opsion supozohet që siti në distancë ka një lloj aksesi broadband nga service provideri. Firewall-i VPN është instaluar pas një DSL apo modem kabell. Firewalli VPN krijon një tunel të një paisje VPN e zyrës qëndrore dhe siguron akses në internet përmes NAT dhe inspektim dhe filtrim të plotë. PC-të individual në rrjetin e sitit në distancë nuk kanë nevojë për një software VPN për të aksesuar burimet e korporatës, vec në mos udhëtojnë dhe të kenë nevojë për të aksesuar intranetin e korporates përmes internetit. Në këtë konfigurim është aktivizuar tunelizimi i ndarë. Software për skanimin e viruseve rekomandohet për të zvogëluar rreziqet e tunelizimit të shpërndarë.

Përmbledhja e adresave vetjake duhet të implementohet në mënyrë që të lehtësohet ngarkesa administrative dhe të lejohet ndërkomunikimi i siteve në distancë nëse nevoitet. Aksesi dhe autorizimi në rrjetin e korporatës dhe internetin kontrollohen nga konfigurimi i firewallit të sitit në distancë dhe të paisjes VPN të zyrës qeëdrore. Konfigurimi dhe menaxhimi i sigurisë të firewallit të sitit në distancë mund të arrihet përmes një tuneli IPSec nga ana publike e firewallit deri te zyrat qëndrore të korporatës. Ky kuadrim siguron që perdoruesve të sitit në distancë të mos u kerkohet të kryejnë ndonjë ndryshim në konfigurim të firewallit shtëpi-zyrë. Përdoruesit individual të sitit në distancë që aksesojne rrjetin e korporatës nuk kryejnë autentikimin e përdoruesit në këtë opsion. Supozohet që mjedisi është i kontrolluar. Nëse mjedisi nuk është i kontrolluar, duhet marrë në konsideratë autentikimi i përdoruesit në firewallin e zyrës qëndrore. VPN-ja përdor autentikimin e paisjeve me çelësa të ndarë. Në një shpërndarje të madhe rekomandohen çertifikatat dixhitale.

4. Opsioni klient hardware VPN

Ky opsion është identik me opsionin remote-site firewall me ndryshimin që klienti hardware VPN nuk ka një firewall të plotë të vendosur. Ky opsion kërkon përdorimin e një firewall-i personal në hostet individuale, veçanërisht kur tunelizimi i ndarë është i aktivizuar. Pa firewallin personal, siguria e hosteve individual pas paisjes VPN varet nga sulmuesi nëse është në gjëndje të shmang NAT. Kjo varësi rezulton nga fakti se kur tunelizimi i ndarë aktivizohet, lidhjet me internetin kalojnë përmes një përkthimi adresash shumë-në-një dhe nuk kalojnë përmes ndonjë filtrimi në shtresën e katërt apo më sipër. Me tunelizimin e ndarë të çaktivizuar, i gjithë aksesi me internetin duhet të jetë përmes zyrave qëndrore të korporatës. Ky kuadrim pjesërisht zvogëlon kërkesat për firewallet personal në sistemet fundor.

Një klient hardware VPN ofron dy avantazhe kryesore. E para, ashtu si me klientin VPN software aksesi dhe autorizimi në rrjetin e korporatës dhe në internet kontrollohen në mënyrë qëndrore nga mjediset e zyrave qëndrore të korporatës. Konfigurimi dhe menaxhimi i sigurisë

së paisjes VPN hardware bëhet përmes një lidhje *Secure-Sockets-Layer (SSL)*, nga siti qendror. Ky kuadrim nuk u kerkon përdoruesve në distancë të kryejnë ndonjë ndryshim në konfigurim në klientin hardware VPN. Avatntazhi i dytë i opsionit hardware VPN client, është që PC-të individual në rrjetin e sitit në distancë, pavarësisht se çfare sistemi operativ është instaluar, nuk kanë nevojë për një VPN client software për të aksesuar burimet e korporatës. Megjithatë, përdoruesit individual në sitin në distancë që aksesojnë rrjetin e korporatës nuk autentikohen me këtë opsion. Klienti hardware vepron në dy mënyra të mundshme. Në të parën, të gjithë përdoruesit pas klientit hardware duken si një përdorues i vetëm në intranetin e korporatës përmes përdorimit të NAT shumë-në-një. Në të dytën, të gjitha paisjet aksesojnë intranetin e korporatës pa NAT, dhe hostet në intranet mund të fillojnë lidhjet me hostet pas klientit hardware sapo vendoset tuneli. Mënyra e parë është më thjeshtë për tu menaxhuar dhe në këtë mënyrë më e shkallëzueshme, e dyta është me fleksibël. Niveli i sigurisë i ofruar nga të dyja mënyrat është i njejtë. Klienti hardware VPN kalon përmes autentikimit të paisjes me koncentratorin VPN të zyrës qëndrore, duke përdorur një grup të konfiguruar çelesash të ndarë. Supozohet se mjedisi është i kontrolluar. Nëse mjedisi nuk është i kontrolluar duhet marrë në konsideratë autentikimi në firewallin e zyrave qëndrore. Në rastin kur kemi një përhapje të madhe, rekomandohet përdorimi i çertifikatave dixhitale.

5. Opsioni remote-site router

Opsioni remote-site router është pothuajse identik me opsionin remote-site firewall me pak ndryshime. E para, duke qënë se kemi të bëjmë me një router me tipare të plota, mund të suportohen aplikime të avancuara si QoS. QoS mund të përdoret për të përcaktuar përparësinë në aksesimin e intranetit të korporatës mbi navigimin në Webin e Internetit. E dyta, ekziston një opsion për të integruar funksionet e një firewalli VPN dhe një paisje e aksesit broadband në një paisje të vetme. Ky opsion kërkon që ISP-ja juaj t'iu lejoj të menaxhoni routerin broadband, diçka kjo që nuk është e zakonshme.

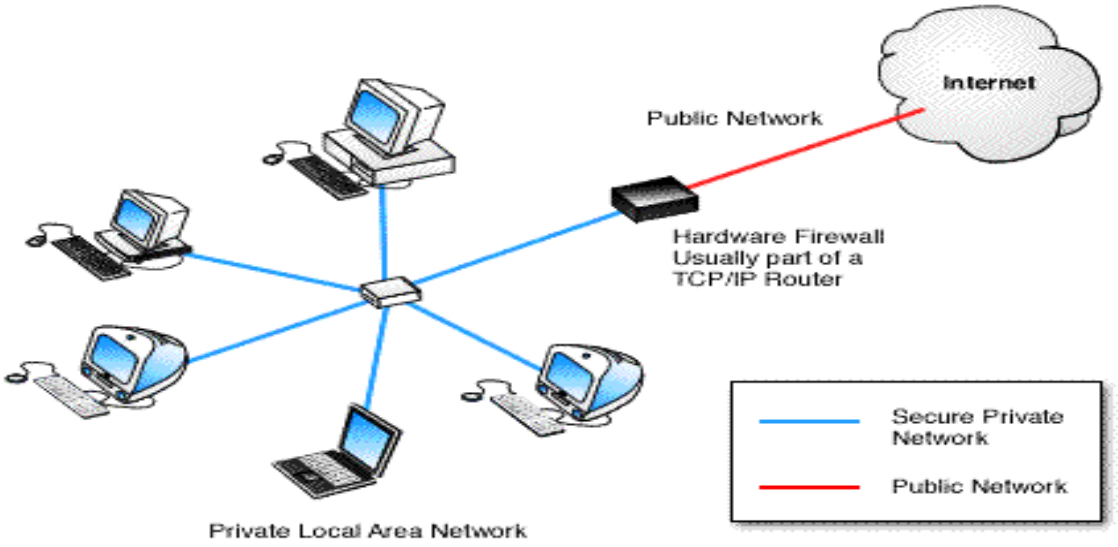
IV. Kapitulli 4 – Firewall-et funksionet dhe klasifikimi i tyre.

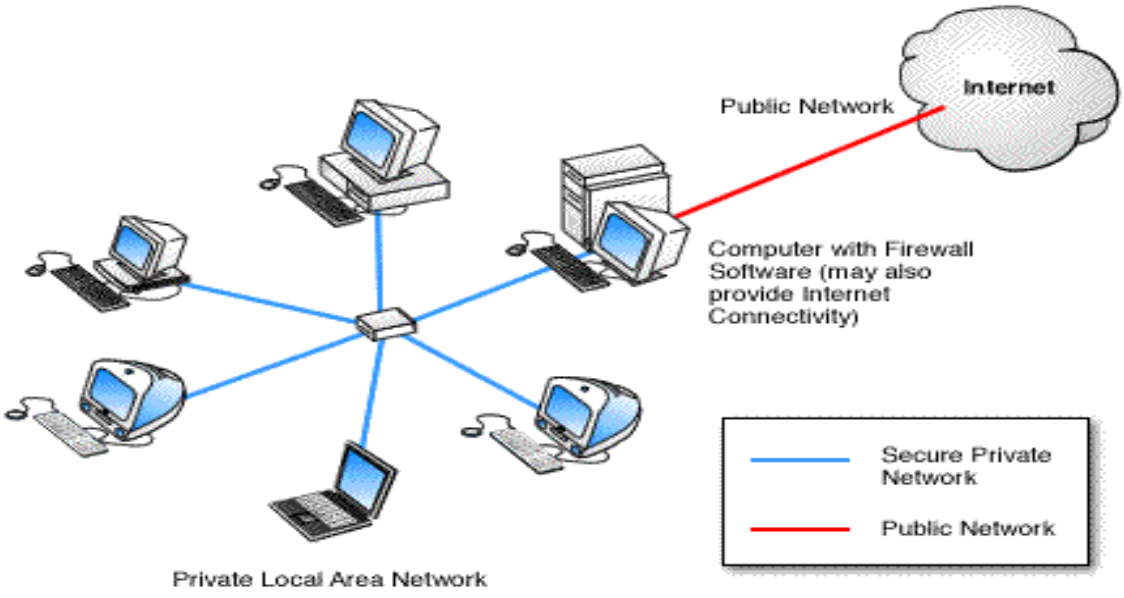
1. Çfarë është një Firewall

Një firewall është një software ose një hardware ASIC që vlereson dhe analizon trafikun në rrjet dhe e filtron ate duke u bazuar ne nje set rregullash të percaktuara nga politika e sigurise. Ne kete kendveshtrim firewall-et jane te ngjashem me router pasi dhe router-at sherbejne për të kontrolluar trafikun e paketave TCP/IP. Per çdo pakete firewalli krahason komponentet e njohur te paketes me setin e rregullave te sigurise dhe vendos nese paketat do te lejohen te kaloje.

Siç thame nje firewall mund te jete nje pajisje hardware ose nje program software qe ekzekutohet ne nje komputer host te sigurte. Ne secilin rast duhet te kete te pakten dy nderfaqe,nje per rrjetin e brendshem qe do te mbroje te konsideruar si te sigurite dhe nje per rrjetin publik te jashtem te konsideruar si jo te sigurte.

Ne figurat e meposhtme jepen dy rastet kur firewall-i eshte nje hardware ASIC apo thjesht nje software i cili ekzekutohet ne nje komputer normal.





Me poshte po japim avantazhet dhe disavantazhet e te dy tipeve te firewall-eve.

a) Firewall-et Hardware

- Tentojne te sigurojne nje mbrojtje me te plote se firewallet software
- Nje firewall hardware mund te mbroje me shume se nje sistem ne nje kohe te caktuar.
- Ato nuk ndikojne ne performancen e sistemit duke qene se nuk ekzkekutohen ne sistemin tone Jane te pavarur nga sistemi operativ dhe aplikacionet te perdorura ne rrjetin tone.
- Jane te kushtueshem, vetem nese kemi nje numer te madh makinash qe ne duam te mbrojme mund te kushtoje me pak te kemi nje firewall hardware sesa nje numer kopjesh te nje firewalli sotware per cdo makine. Duke qene se nuk ekzekutohen ne komputerin tone mund te jene te veshtire te konfigurohen.

b) Firewall-et Software

- Zakonisht jane shume te lire
- Jane shume te thjeshte per tu konfiguruar
- Duke qene se ekzekutohen ne kompjuterin tone ato kerkojme burime te sistemit tone (CPU,memorje, hapesire te harddiskut).
- Shpesh mund te konfliktoje me sistemin tone operativ
- Duhet te instalojme versionin korrekt per sistemin tone operativ ne menyre qe te jete kompatibel me te.

2. Funksionet e një firewall-i

Nje firewall eshte nje pajisje mbrojtese pra qe ne se konfigurohet ne menyren e duhur e ul pasigurine ne nje nivel te kenaqshem. Nese duhet te ndertojme nje firewall, gjeja e pare per te cilen duhet te shqetesohemi eshte se cfare po perpiqemi te mbrojme. Kur lidhemi me rrjetin e jashtem pra ne Internet ne rrezikojme informacionin qe kemi ne kompjuter, resurset dmth kompjuterin ne teresi dhe gjithashtu dhe reputacionin tone apo te kompanise :

Nje firewall ekzaminon te gjitha paketat qe routohen ndermjet 2 ose me shume rrjeteve te lidhur tek nderfaqet e firewall-it per te pare nese keto paketa permbushin kriteret e specifikuara . Nese ky kusht plotesohet paketat lejohen te kalojne, ne te kundert ato hidhen poshte(discard). Firewallet mund te filtrojne paketat duke u bazuar ne adresat e tyre IP te burimit dhe te desinacionit si dhe numrit te portes se perdorur. Kjo eshte e njohur dhe si address filtering. Firewallet mund te filtrojne tipe te ndryshme trafiku rrjeti. Nje gje e tille njihet dhe si protokoll filtering sepse vendimi per te kaluar apo jo nje pakete behet ne baze te protokollit qe perdoret, psh HTTP ,TELNET,FTP etj. Pra qellimi kryesor i perdorimit te firewall-it eshte imponimi i sigurise ne komunikimin midis rrjetit te brendshem dhe atij te jashtem. Nje firewall mund te beje dhe autentikimin e perdorueseve te cilet jane te autorizuar per te komunikuar nepermjet tij sipas nje politike sigurimi te paracaktuar.

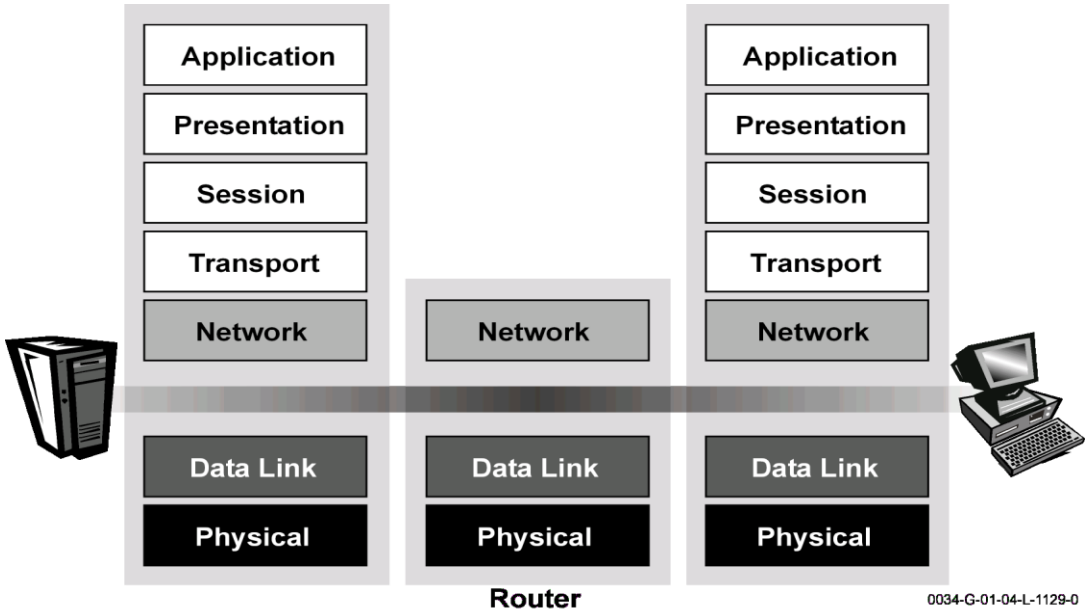
3. Klasifikimi i Firewalle-ve

Duke pasur parsysh modelin OSI per komunikimin ne rrjet , lidhur me shtresen ne te cilen operojne firewall-et mund t'i ndajme ne tre grupe kryesore:

- Packet Filters
- Application Layer Firewalls
- Stateful Inspection Firewalls

a) Packet Filters

Firewall-et *Packet Filters* e bazojne vendimin e tyre mbi filtrimin e paketave ne analizimin e adresave IP burim dhe destinacion te paketave ose ne numrin e portave te perdorura. Meqenese keto tipe firewall-esh operojne ne shtresen e rrjetit ato jane te pavarur nga aplikacionet, dhe mund te sigurojne performance dhe shkallezueshmeri optimale. Megjithate *Packet Filters* jane firewallet me pak te sigurte. Arsyeja kryesore eshte se ata nuk jane te orientuar nga aplikacionet dhe nuk analizojne permbajtjen e paketave dhe as formatin e protokollit te perdorur. Me poshte jepet nje figure qe shpjegon operimin e packet filter nga pikepamja e modelit OSI.



Avantazhet e packet filters :

- Te pavarur nga aplikacionet
- Performance e larte
- Shkallezueshmeri

Disavantazhet e packet filters

- Siguri e ulet
- Asnje analize siper shtreses se rrjetit
- Konfigurim dhe menaxhim i veshtire

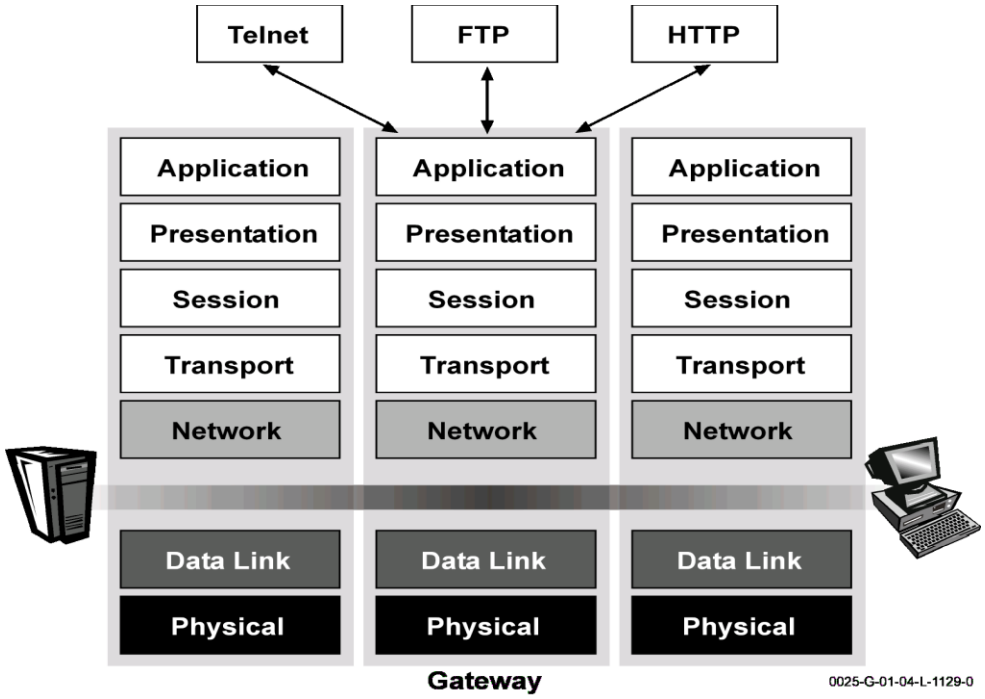
Shembull: Lista e aksesit

ACL e meposhtme i perket nje routeri Cisco te serise 2514 dhe eshte nje shembull i qarte i nje packet filter. Me anen e saj ne bllokojme te gjithe trafikun TCP perveç atij HTTP (porta 80), HTTPS (443), FTP(21 dhe 20), dhe DNS(53).

```
access-list 101 permit tcp any any eq 21
access-list 101 permit tcp any any eq 20
access-list 101 permit tcp any any eq 80
access-list 101 permit tcp any any eq 443
access-list 101 permit tcp any any eq 53
access-list 101 permit tcp any any gt  1023
```

b) Firewall-et e shtresës së aplikacionit (Proxies)

Ne ekstremin tjeter te klasifikimit te firewall-eve qendrojne *application gateways* ose siç njihen ndryshe me emrin *Proxies*. Keto tipe firewall-esh implementojne sigurine ne rrjet duke ekzaminuar te gjithe shtresen e aplikacionit. Ata e realizojne kete duke thyer modelin klient-server. Ne kete rast çdo komunikim klient-server do te kete nevoje per dy lidhje: e para nga klienti tek firewalli dhe e dyta nga firewall-i per tek serveri. **Çdo proxy do te kete nevoje per nje daemon ose proces aplikative** duke e bere shkallezueshmerine dhe suportin nje problem te vertete. Ne figuren e meposhtme jepet funksionimi i nje Application gateway e pare nga pikepamja e modelit OSI



Avantazhet e application gateways:

- Konsiderohen si metoda me e sigurte per kontrollin e lidhjeve ne rrjet
- Firewall-i punon ne shtresen e aplikacionit dhe kupton plotesisht protokollin qe po perdoret.
- Ata sigurojne aktivitet te mire *log* si dhe informacion mbi protokollet.
-

Disavantazhet e application gateways :

- Mund te shnderrohen ne piken e dobet ne transmetime me gjeresi te madhe brezi.
- Shpeshhere jane te ngadalte dhe nuk mund te pershtaten per streame te dhenash me shpejtesi te larte si psh VoIP.
- Proxiet mund te jene te disponueshme vetem per sherbimet TCP.
- Numri i proxies te suportuara eshte i kufizuar.
- Çdo lidhje ka nevoje per procesin e saj daemon. Nje gje e tille mund te ezauroje resurset e makines duke perfshire ketu CPU dhe memorien.

- Mund te kemi ekspozim te sistemit operativ ne nivel te ulet dhe kompromentim te stack-ut TCP/IP

c) Stateful Inspection Firewalls

Keto tipe firewall-esh, te cilet jane patentuar nga *Check Point Firewall Technologies*, eshte standarti industrial per zgjidhjet e sigurise ne rrjet ne kompanite e medha. **Ne keto tipe firewall-esh paketat interceptohen ne shtresen e rrjetit per performance me te larte (si ne rastin e packet filters), por te dhenat e derivuara nga te gjitha shtresat e komunikimit aksesohen dhe analizohen per siguri me te larte**. Keshtu keto tipe firewall-esh na ofrojne nje nivel me te larte sigurie duke inkorporuar komunikimin dhe informacionin mbi kontekstin e paketave, i cili ruhet dhe rinovohet vazhdimisht ne nje tabele gjendjeje dhe ne nje tabele komunikimi.

Avantazhet e stateful inspection firewalls jane:

- Jane me te shpejte se application proxies.
- Mund te kontrollojne te gjithe paketen TCP/IP.
- Mund te kuptojne detajet e protokolleve.
- Jane te lehte per tu administruar me nje terminal GUI.
- Sigurojne regjistrim ngjarjesh mjaft te mire.

Disavantazhet e stateful inspection firewalls permbledhin:

- Jane me pak te sigurte se application proxies.
- Jane me te ngadalte se firewall-et packet filtering.
- Administrimi i firewall-it mund te duket i lehte me nje terminal GUI, duke lejuar qe administratore pak te kualifikuar te aksesojne firewall-in
- Per disa protokolle keto firewalle ofrojne te njejtin nivel sigurie si packet filters.

4. Demilitarized Zones (DMZ)

Nje zone e demilitarizuar (DMZ) izolon hostet qe jane te aksesueshme nga jashte rrjetit (web server ose FTP server) nga serverat e brendshem . Hostet e jashtem jane vendosur ne nje zone te ndare te lidhur me firewallin. Kjo krijon DMZ. Çdo subnetwork eshte konfiguruar gjithashtu me zonen e tij te sigurise duke e lidhur ate ne firewall. I gjithe trafiku ndermjet zonave dhe i gjithe trafiku mes Internetit dhe te gjithe zonave eshte kontrolluar nga firewalli. Ne kete menyre çdo zone eshte izoluar dhe sistemet ne çdo zone besojne vetem sistemet brenda se njejtes zone. Prandaj nese nje hacker arrin te aksesoje nje host, hostet e tjera ne rrjet jane akoma te sigurte. DMZ shpesh here jane perdorur per servera te caktuar si web server qe duhet te jete te aksesueshem nga 2 rrjeta te ndare, nga ai i brendshem i konsideruar si i sigurte dhe nga ai i jashtem i konsideruar si i pasigurte. Zakonisht nje organizate e organizon intranetin e saj ne menyre te tille qe serverat qe permbajne informacion te rezervuar vendosen ne rrjetin e brendshem nderkohe qe serverat te cilet aksesohen si nga rrjeti i brendshem dhe nga ai i

jashtem si psh webserver-at, mailserver-at vendosen ne DMZ duke eliminuar mundesine qe te ndodhen ne te njejtin subnet me serverat e brendshem te kompanise. Me pas percaktohet dhe trafiku i lejuar drejt ose nga rrjetit te jashtem, atij te brendshem dhe DMZ.

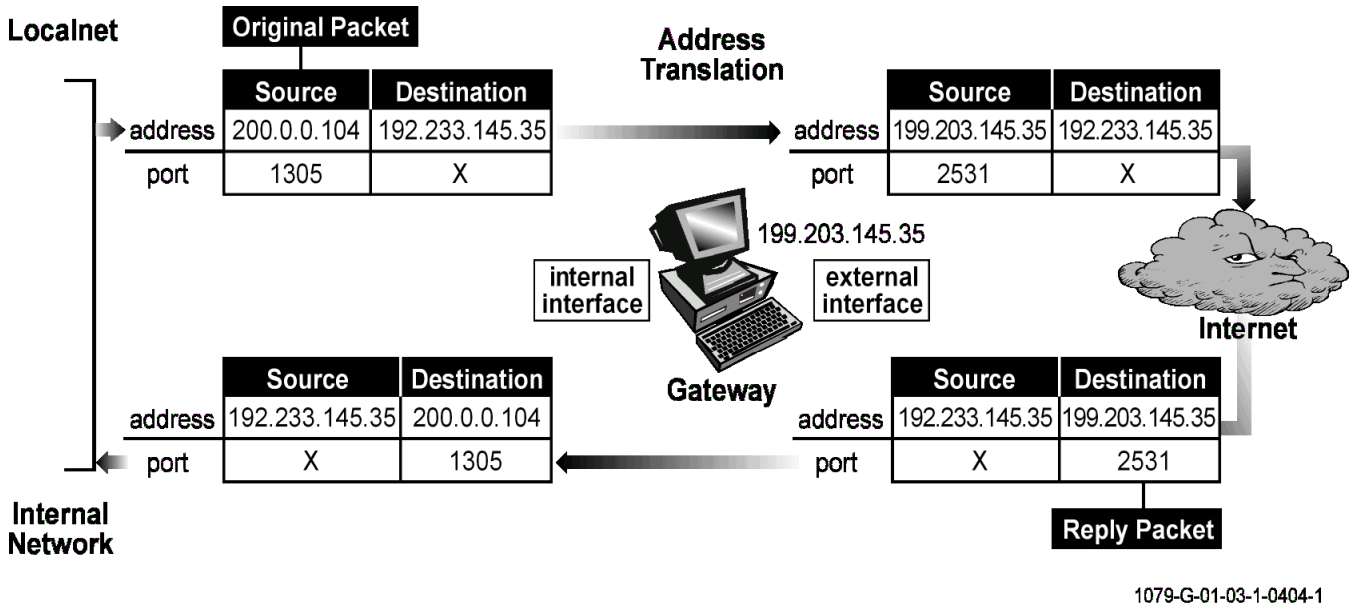
5. Network Address Translation (NAT)

Nje menyre tjeter per te mbrojtur rrjetin tone prapa firewall-it eshte duke i caktuar subneteve apo tere rrjetit adresa IP te konsideruara si private. Ne ditet e sotshme kjo eshte bere nje gje me se e domosdoshme si pasoje e procesit te ezaurimit te adresave IP. Me pas kur dalin nga rrjeti i brendshem keto adresa IP private perkthehen ne adresat IP publike te rezervuara pra te blera nga ne. Nje gje e tille behet e mundur nga mekanizmi i perkthimit te adresave NAT. Praktikisht si pasoje e NAT adresat e rrjetit tone te brendshem jane te padukshme dhe e vetmja adrese qe shihet eshte adresa publike qe i eshte caktuar kompanise sone. Adresat e meposhtme jane caktuar si private pra per perdorim te brendshem nga organi vendimarres i Internetit IANA (Internet Assigned Numbers Authority).

- **10.0.0.0 /8**
- **172.16.0.0 /12**
- **192.168.0.0 /16**

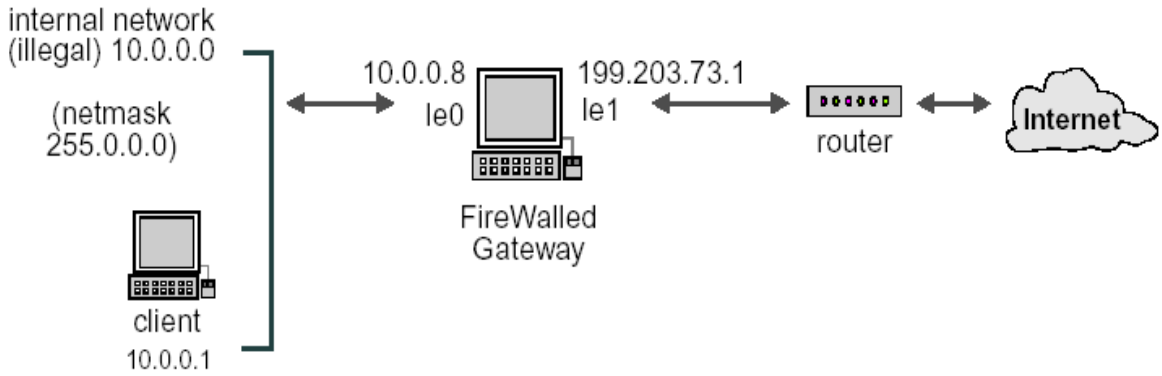
NAT mund te operoje ne dy menyra:

- **Hide:** Adresat e brendshme te rrjetit perkthehen ne nje adrese te vetme publike. Per te dalluar midis adresave te brendshme te rrjetit perdoret numri i portes i cili ndryshon ne menyre dinamike per te identifikuar adresen e brendshme nga erdhi paketa. Ky lloj NAT-i nuk funksionon ne rastet kur numri i portes se protokollit nuk mund te ndryshoje dhe atehere kur serveri i jashtem duhet te njohe klientin ne baze te adreses IP te tij.



- **Static:** Çdo adrese private perkthehet ne nje adrese korresponduese publike duke lene te pandryshuar tipin e portes qe perdoret. Ka dy nentipe te NAT-it statik:

    - Menyra statike burim
    - Menyra statike destinacion



V. Kapitulli 5 – Check-Point si paketë firewall VPN

Paketa Check Point Next Generation (NG) perbehet nga disa produkte te konceptuar per te krijuar nje zgjidhje totale mbi çeshtjen e sigurise. Siguria ne rrjet nuk shihet nen kendveshtrime individuale te instalimit te nje firewall-i apo te konfigurimit te nje lidhjeje VPN. Arkitektura **SVN** (Secure Virtual Network) e ofruar nga CheckPoint i perfshin gjithe aspektet e sigurise ne rrjet ne nje produkt te vetem dhe te lehte per tu perdorur, per me teper me nderfaqe GUI

Arkitektura SVN shikon te gjithe rrjetin e ndermarrjes ne teresi duke mos perfshire vetem rrjetin lokal LAN si dhe lidhjet WAN te tij por duke trajtuar dhe me perdoruesin VPN te lidhur ne distance.
Paketa e produkteve Check Point Next Generation (NG) eshte projektuar per te permbushur nevojat e sigurise dhe te menaxhimit te kerkuara nga arkitektura SVN. Keshtu perdorimi i Firewall 1/VPN 1 si mbrojtes i rrjetit te brendshem dhe si pike fundore e sigurte per te gjithe trafikun VPN ploteson nevojat primare te sigurise per te gjithe kompanite. Pasi kemi siguruar zemren e sistemit, SecuRemote i shtohet paketes NG si nje aplikacion GUI qe na ofron nje konfigurim VPN shume te thjeshte. **Secure Client** eshte projektuar per te ndertuar funksionalitetin e SecuRemote duke lejuar Menaxheret e Sigurise per te vendosur dhe per te imponuar Politikat e Sigurise per platformat klient qe lidhen me sherbimin VPN. Ne versionin NG, paketes se produkteve CheckPoint ju shtuan dhe dy aplikacione te reja per te lejuar menaxheret e sigurise te menaxhojne user-at si dhe account-et. Komponenti Account Management u shtua per te menaxhuar account-et e perdoruesve te ruajtura ne serverat LDAP (Lightweight Directory Access Protocol), dhe User Authority (UA) u integrua per te bere te disponueshem informacionin e autentifikimit te marre nga Firewall-1/VPN-1, ndaj aplikacioneve te tjera. Per te ndihmuar ne menaxhimin e rrjetit, dy mjete te reja u integruan ne suiten e produkteve NG. Meta IP lejon menaxhimin e serverave DNS dhe DHCP, nderkohe qe FloodGate-1 siguron menaxhimin e Quality of Service (QoS), shume i nevojshem ne Internet dhe ne lidhjet VPN. Se fundmi per te siguruar informacion te deatajuar mbi sigurine dhe per perdorimin jo vetem te produkteve te pakets NG por dhe te aplikacioneve te tjera te pales se trete (third-party), CheckPoint ka integruar Reporting Module.

1. Arkitektura e CheckPoint

Paketa Check Point Firewall-1/VPN-1 perfshin produktet e meposhtme:

- **SmartClient**
- **SmartCenter Server**
- **Enforcement Module**
- **SVN foundation**
- **OPSEC**

a) SmartClient

SmartClient eshte aplikacioni GUI qe lejon administratorin e sistemit te konfiguroje dhe te monitoroje modulin e perforcimit (CheckPoint Firewall-1/VPN-1). Ne perberje te tij jane keto aplikacione kryesore:

SmartDashboard permban komandat dhe mjetet e duhura per analizimin dhe menaxhimin e sigurise se rrjetit tone me anen e krijimit dhe menaxhimit te politikave te sigurise. Eshte mjeti kryesor per konfigurimin e serverit SmartCenter. Lehtesi ne perdorim dhe eliminimi i menuve te njepasnjeshme per te gjetur objektet.

SmartUpdate eshte utiliteti kryesor qe sherben per te rinovuar liçensat e leshuara nga CheckPoint, menaxhimin e instalimeve software ne menyre remote duke leshuar liçensat perkatese si dhe per update-imin e disa moduleve CheckPoint ne menyre te njekohshme.

SmartView Tracker eshte programi kryesor qe menaxhon log-et e marra nga modulet e perforcimit. Ky program na ofron mundesine per te aplikuar filtra te ndryshem ose queries ne rekordet e afishuara.

SmartView Status na ndihmon per te monitoruar ne kohe reale te gjithe produktet CheckPoint te instaluara si dhe produktet OPSEC. Ne mund te vendosim alarme (alerts) si dhe paralajmerime (warnings) ne baze te gjendjes se produkteve. Keto mund te gjenerohen ne varesi te kushteve te caktuara si psh perdorimi i CPU, hard disk gati plot, politike jo e instaluar apo humbje sinkronizimi.

SmartView Monitor sherben per diagnostifikimin e rrjetit. Eshte programi kryesor qe na lejon per te analizuar trafikun ne rrjet dhe lidhjet si dhe per te siguruar informacion ne kohe reale per performancen e rrjetit dhe gjendjen e sigurise.

SmartView Reporter eshte programi qe gjeneron reportet.

b) Smart Center Server

Serveri SmartCenter ose i quajtur ndryshe ne versionet e meparshme te Check Point serveri i menaxhimit eshte pika qendrore e arkitektures Check Point. Ai perdoret per te shperndare politikat e sigurise drejt moduleve te perforcimit dhe per te ruajtur skedaret log qe me pas i upload-ohen stacioneve menaxhuese (SmartClient). Perveç ketyre moduli i

menaxhimit ruan bazen e te dhenave te user-ave si dhe objektet e ndryshme te rrjetit te perdorur ne politikat e sigurise. Serveri i Menaxhimit gjithashtu kontrollon ne se Politika e Sigurise eshte e percaktuar ne menyre te sakte dhe eshte e kompiluar ne formatin qe i nevojitet modulit te inspektimit. Serveri i Menaxhimit SmartCenter eshte kompatibel dhe me pajisje te pales se trete pasi me te mund te konfigurojme dhe ACL e router-ave.

Serveri SmartCenter permban:

- **Databasen e objekteve**
- **Databasen e user-ave**
- **Rregullat e sigurise**
- **Databasen e log-eve**

Ne qender te arkitektures Check Point qendron pikerisht Moduli i Menaxhimit**. Ky modul i cili ndodhet ne serverin SmartCenter konfigurohet duke perdorur klientet GUI (SmartClient) te cilet mund te jene te instaluar ne te njejten platforme ku eshte instaluar SmartCenter ose ne nje platforme tjeter.** Nje konfigurim i tille na lejon qe te menaxhojme te gjithe sigurine e rrjetit nga nje Server Menaxhimi i vetem.

c) Moduli i përforcimit

Moduli perforcimit permbledh modulin e inspektimit si dhe serverat e sigurise Firewall-1 dhe VPN-1. Ai instalohet ne nje gateway Interneti ose ne pikat e aksesit te rrjetit. Me perkufizim nje pike aksesi do te quajme piken ku rrjeti lokal eshte i lidhur pra i aksesueshem me rrjetin e jashtem. Moduli i perforcimit permbledh:

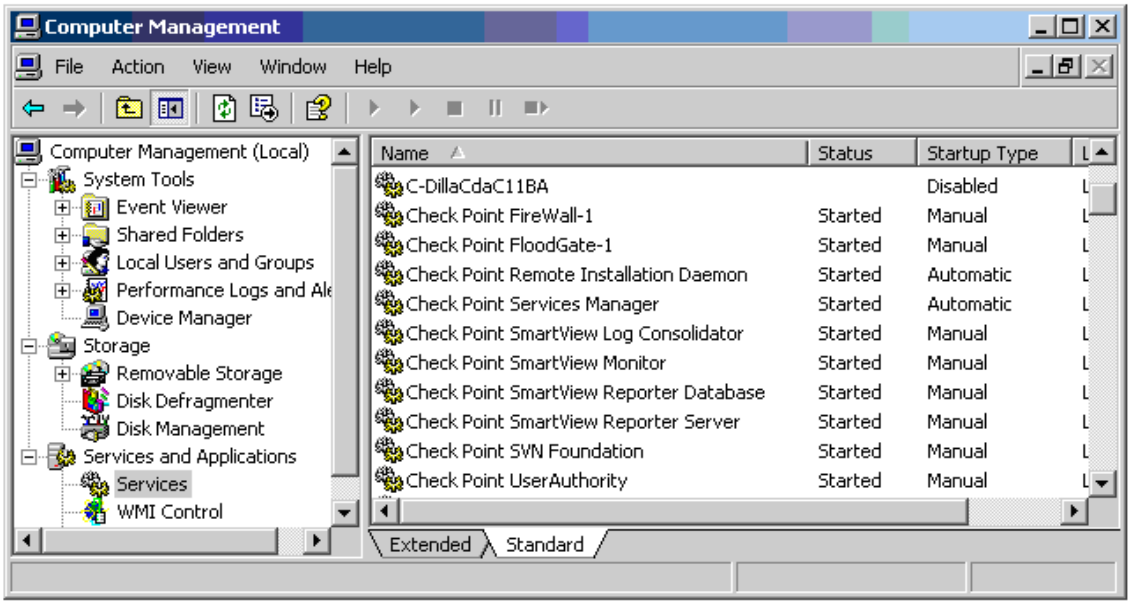
- **Modulin e Inspektimit** i cili ekzaminon te gjitha komunikimet
- **Serverat e Sigurise** te cilet sigurojne autentifikim si dhe veti te sigurise ne permbajtje ne nivelin aplikativ per SMTP, Telnet, FTP, HTTP dhe rlogin.
- **Moduli i Firewall-it** i cili eshte i vendosur midis shtreses se data-link dhe asaj te rrjetit ne modelin OSI

d) SVN Foundation

Baza SVN konsiderohet si sistemi operativ Check point (CPOS). SVN ka aftesine qe te konfiguroje dhe te menaxhoje sigurine e firewall-it, rrjetet VPN, alokimin e bandwidth-it, adresimin IP etj. Te gjithe produktet CheckPoint perveç SmartConsole perdorin sherbimet CPOS:

- Komandat **cpstart** dhe **cpstop**
- Daemonin Check Point (**cpd**)
- Rojtarin (watchdog) per sherbimet kritike
- Utilitetin **cpconfig**
- Utilitetin e licensave

- Daemonin **snmp**



e) OPSEC (Open Platform for Security)

Asgje nuk mund te konsiderohet perfekte, keshtu qe Check Point krijoi nje program per te lejuar firmat te tjera zhvilluese dhe prodhuese qe te plotesojne paketen standarte me produkte dhe sherbime shtese. Pra OPSEC siguron kompatibilitetin e paketes Check Point me aplikacione te tjera te pales se trete. Shembuj te OPSEC jane:

- **CVP (**Content Vectoring Protocol**)** server: Ky server perdoret per te ekzaminuar permbajtjen e paketave TCP/IP dhe zakonisht perdoret per skanim virusesh.
- **UFP** (URL Filtering Protocol) server: Perdoret ne percaktimin e resurseve URI. Perdoret zakonisht per te pare dhe per te ndryshuar permbajtjen HTTP.
- **SAMP (**Suspicious Activity Monitoring Protocol**)**: Eshte nje protokoll ne te cilin sistemet e dedektimit IDS te paleve te treta mund te lidhen me modulet Check Point per te bllokuar sulmet.
- **LEA** (Log Export API): Ky protokoll lejon produktet shtese qe te aksesojne skedaret log te firewall-it (fw.log) ne menyre qe te gjenerojne reporte ose te bejne analizimin e ngjarjeve.
- **OMI (**Object Management Interface**)**: Perdoret per te siguruar nje nderfaqe te sigurte drejt bazave te te dhenave te Serverave te Menaxhimit Check Point.
- **SAA (**Secure Application API**)**: Kjo eshte nje nderfaqe per programim aplikacionesh (API) qe suporton krijimin e produkteve qe autentifikojne user-at me modulet Check Point. Produktet e certifikuara OPSEC ne kete kategori permbledhin PKI (public key infrastructure), kartat smart, serverat e autentifikimit dhe serverat e direktorive.

- **UAA (**User Authority API**)**: Perdoret per te ofruar informacion mbi sigurine ne rrjet ndaj aplikacioneve te pales se trete.

VI. Kapitulli 6 –Realizimi i VPN me Check Point

VPN perdorin procedura te ndryshme kriptografike per te autentikuar userat dhe per te siguruar qe te dhenat do te mbeten private. Shume protokolle jane zhvilluar per te arritur qellimet e meposhtme:

- **Fshehtesia (privacy):** Asnje person nuk duhet te jete ne gjendje te lexoje mesazhin e derguar perveç derguesit dhe marresit te vertete per te cilin ky mesazh eshte derguar.
- **Verifikimi (authenticity):** Marresi i mesazhit te enkriptuar duhet te jete i afte te verifikoje me siguri se kush eshte derguesi i mesazhit.
- **Integriteti i te dhenave (data integrity):** Marresi i mesazhit duhet te jete i afte te verifikoje ne se mesazhi eshte alternuar apo modifikuar gjate transmetimit.

Nje VPN eshte nje rrjet qe ndertohet duke perdorur nje infrastrukture publike te perbashket dhe qe alokon ne menyre dinamike qarqe virtuale per te lidhur nyjet dhe per te transmetuar te dhena private. VPN perdorin autentikimin per te siguruar qe vetem personat e autorizuar lejohen per te aksesuar resurset e rrjetit. Me nje fjale VPN eshte nje tunel i enkriptuar. Keto tunele mund te krijohen ne nje nga tre menyrat e meposhtme:

- **Klient – Klient**
- **Gateway – Gateway**
- **Klient – Gateway**

1. Protokollet VPN

Protokollet e perdorur ne lidhjet VPN perfshijne:

- **PPTP:** Point to Point Tunneling Protocol eshte implementimi Microsoft i nje protokolli qe ngjan me nje protokoll point-to-point por qe transmeton te dhena ne internet.
- **L2TP:** Layer 2 Tunneling Protocol eshte zgjidhja RFC per lidhjet VPN
- **L2F:** Layer 2 Forwarding Protocol eshte standarti VPN i implementuar nga Cisco
- **IPSec:** Konsiston ne nje bashkesi protokollesh dhe standartesh qe sigurojne integritet dhe konfidencialitet me anen e proceseve te meposhtme:
  - **Autentikim:** Procesi i verifikimit te derguesit dhe i sigurimit qe te dhenat nuk jane modifikuar gjate kalimit ne rrjet.
  - **Enkriptim:** Procesi i transformimit te te dhenave ne nje forme te palexueshme nga asnjeri pervec marresit te vertete per te cilin te dhenat jane derguar.

- **Menaxhim i çelesave:** Procesi i krijimit, administrimit dhe shkembimit te celesave te perdorur per autentikim dhe enkriptim.

- **SSL:** Nje protokoll qe u zhvillua fillimisht nga Netscape dhe qe perdoret per komunikim te autentikuar dhe te enkriptuar midis klienteve dhe serverave. Perdorimi me i zakonshem eshte ne HTTP e sigurte (HTTPS). Protokolli Check Point SIC (Secure Internal Communications) qe sherben per komunikime te sigurta ne rrjet, bazohet tek SSL.

2. Kriptimi

Kriptografia ne pergjithesi eshte procesi i transformimit te te dhenave ne nje forme te palexueshme. Sistemet kriptografike perdorin algoritma qe ndahen ne dy grupe te medha: algoritma simetrike dhe algoritma josimetrike.

Algoritmat simetrike perdorin nje çeles sekret i cili eshte i njejte si ne pajisjen kriptuese ashtu dhe ne ate dekriputese. Algoritmat me te perdorshem simetrike jane:

- **DES:** Algoritmi enkriptues me i perdorur.
- **3DES:** Triple DES eshte me i sigurte se DES sepse perdor tre çelesa te veçante duke ulur keshtu mundesine e crack-imit te algoritmit.
- **CAST:** Algoritem kriptimi i bazuar ne RFC 2144.
- **AES:** AES eshte standarti i avancuar i kriptimit i bazuar ne algoritmin Rijndael. Ka tre gjatesi çelesash: 128, 192 dhe 256 bit.

Algoritmat asimetrike perdorin dy çelesa te veçante: nje per kriptim dhe nje per dekriptim. Keto çelesa njihen me emrin çelesa publike dhe private. Algoritmat me te perdorur asimetrike jane:

- **DH:** DH eshte nje algoritem asimetrik i bazuar ne logaritme diskrete.
- **RSA:** Eshte nje algoritem qe perdoret per transmetimin e çelsave dhe bazohet ne dy numra te medhenj.
- **PGP:** PGP u zhvillua fillimisht si nje aplikacion i lire per sigurine ne e-mail.

Algoritmat simetrike perdorin nje çeles te vogel dhe jane te shpejte. Problemi i tyre qendron ne shkembimin e çelsit. Ne kontrast algoritmat asimetrike perdorin nje çeles te madh por jane te ngadalte. Zakonisht perdoren ne fazen e pare te transmetimit per shkembim çelesash.

3. Algoritmat e Hashit

Nje algoritem hashi merr nje mesazh me nje gjatesi arbitrare dhe prodhon ne dalje nje mesazh me gjatesi fikse te njohur si *fingerprint* ose *digest*. Funksionet hash mund te perdoren per aplikacionet e firmave digitale, ku nje skedar i madh duhet te kompresohet ne nje menyre te sigurte perpara se te kriptohet me nje çeles privat (sekret). Algorimet me te perdorur hash jane **HMAC-SHA** dhe **HMAC-MD5.** Funksionet hash me te perdorur ne kriptografine e çelsave publike jane:

- **MD2:** funksion hash 128 bit
- **MD5:** funksion hash 128 bit
- **SHA-1:** funksion hash 160 bit

6.6.4 – IP Security

IPSec konsiston ne disa protokolle:

- **SA:** Security Association siguron nje lidhje virtuale midis entiteteve peer IPSec per te percaktuar se kush prej sherbimeve IPSec jane te disponueshme midis ketyre entiteteve.
- **AH:** Authentication Header siguron integritet per paketat duke perfshire nje checksum hashi ne pakete. Ne se marrim nje pakete me AH dhe veprimi checksum rezulton i suksesshem, mund te sigurohemi qe paketa eshte ne gjendjen e saj origjinale. AH i ben hash te gjithe paketes qe nga koka IP deri ne fundin e paketes.
- **ESP:** Encapsulating Security Payload siguron konfidencialitet per paketat duke i enkriptuar ato me nje algoritem enkriptues. Ne se marrim nje pakete me ESP dhe e dekriptojme ate atehere ne e dime qe ndajme te njejtin password sekret me entitetin tone peer dhe se paketa nuk eshte lexuar gjate transmetimit.
- **IPComp:** IP Payload Compression siguron nje menyre per te kompresuar paketat perpara enkriptimit me ESP.
- **IKE:** Internet Key Exchange perdoret per te transmetuar sekretin simetrik (çelesin simetrik).

4. Skemat e Kriptimit

Nje skeme kriptimi konsiston ne elementet e meposhtem:

- **Nje protokoll i menaxhimit te celesave─** per te gjeneruar dhe ndryshuar celesat
- **Nje algoritem kriptimi ─** per kriptimin e mesazheve
- **Nje algoritem autentikimi─** per te siguruar integritetin

Skemat e kriptimit qe suportohen nga VPN-1/FireWall-1

- **Manual IPSec**
- **IKE**
- **SKIP**
- **FWZ**

a) Skema e kriptimit ‘Manual IPSec’

Paketat IP kriptohen ne perputhje me standartin ESP (Encapsulating Security Payload) sipas te cilit paketa origjinale enkriptohet dhe enkapsulohet brenda nje pakete me te madhe.

Ka dy menyra per te bere enkapsulimin:

- Tunel Mode
- Transport Mode

Tunel Mode

Ne Tunel Mode, e gjithe paketa (perfshire edhe koken IP) kriptohet ne perputhje me SA (Security Asociation). Nje koke ESP qe permban SPI dhe te dhena te tjera, shtohet ne fillim te paketes,dhe ndertohet nje IP e re.

Paketa e re permban:

- Koken e re IP
- Koken ESP
- Paketen origjinale te kriptuar

Me pas paketa e re dergohet ne destinacion. E mira e kesaj menyre eshte se destinaconi i specifikuar ne header-in e ri IP mund te jete i ndryshem nga ai i specifikuar ne header-in origjinal IP. Keshtu eshte e mundur te dergosh paketen ne nje host i cili ben deskriptimin ne interes te nje numri tjeter hostesh; deskriptori host deskripton paketen, heq header-at ESP dhe IP pastaj dergon paketen origjinale ne destinacionin e caktuar.

Transport Mode (nuk suportohet nga VPN-1/FireWall-1)

Ne Transport Mode, header-I IP nuk kriptohet. Nje header ESP futet midis header-it IP dhe header-it te shtreses se transportit. Header-i i shtreses se transportit dhe cdo gje pas saj kriptohet.
Kjo metode nuk e rrit gjatesine e paketes aq sa Tunnel Mode. Paketa e ekriptuar duhet derguar ne destinacionin origjinal.

Te Metat:

Celesat jane te fiksuar gjate kohezgjatjes se lidhjes.
Nuk ka mekanizma per shkembimin e celesave.

b) Skema e Kriptimit IKE

IKE eshte nje standart per kalimin SA midis dy hosteve qe do te perdorin IPSec, dhe eshte skema e menaxhimit te celesave qe eshte zgjedhur per IP Version 6.

Shkembimi i celesave IKE eshte i ndare ne dy faza:

Faza 1 (Agresive Mode)
Ne kete faze peers vendosin nje IKE Security Association qe do te perdoret per enkriptimin dhe autentikimin.

Faza 2
Duke perdorur SA te vendosur ne fazen 1, peers vendosin nje SA per kriptimin e trafikut IPSec. Celesat mund te modifikohen sa here te jete e nevojshme gjate kohezgjatjes se lidhjes duke permbushur fazen 2.

c) Skema e Kriptimit SKIP

SKIP, e zhvilluar nga Sun Microsystems, shton dy tipare ne manualin IPSec

- Celesa te permiresuar—Manuali IPSec perdor celesa fiks, SKIP perdor nje hierarki celesash
- Menaxhimi i celesave—SKIP implementon nje protocoll te menaxhimit te celesave per Manual IPSec.

SKIP siguron nje hierarki celesash te ndryshueshem ne kohe, qe perdoren per kriptimin e lidhjes po aq mire sa edhe implementimi i nje protokolli te menaxhimit te celesave. SKIP gjithashtu perfshin ESP dhe AH, dhe i shton header-in e tij paketes.
Celesi i kriptimit dhe celesi i autentikimit jane te ndare nga celesi i sesionit, i cili ndyshon ne intervale te caktuara, ose kur nje sasi te dhenash kalon nje prag te vene.
Se fundmi celesi i sesionit i ndryshuar komunikohet duke e kriptuar ate me celesin Kijn i cili ndryshon cdo ore.Celesi Kijn derivohet nga bashkesia e celesave sekrete Deffie-Hellman, duke perdorur nje funksion hash. Cdo korrespondent pajiset me pjesen publike te celesit Deffie-Hellman te korrespondentit tjeter qe ben transmetimin me celesin e saj RSA.
SKIP perfshin nje protokoll pre kete shkembim te celesave publik.

d) Skema FWZ

Sipas kesaj skeme nje mesazh kriptohet me nje celes sekret te derivuar ne menyre te sigurte nga korresponduesit Diffie-Hellman.
Numri I celesave qe mund te menaxhohen eshte propocional me numrin e koresponduesve. Kjo eshte ne kontrast me disa skema te tjera, ne te cilat numri I celesave te menaxhuar eshte propocional me katrorin e numrit te koresponduesve.

Header-at e paketave TCP/IP nuk kriptohen, perte siguruar qe protokolli do te marre dhe dergoje paketat ne menyre korrekte. Header-i i tekstit TCP/IP kombinohet me celesin e sesionit per te kriptuar pjesen e te dhenave te cdo pakete, keshtu qe dy paketa te ndryshme nuk mund te kriptohen me te njejtin celes. Nje checksum kriptografik fute ne cdo pakete per te siguruar intregritetin e te dhenave.

e) Skemat Public Key

VPN-1/FireWall-1 suporton dy tipe celesash publik:

- Deffie-Hellman

  Nje cift celesash, publik-private, Deffie-Hellman perdoret per te llogaritur nje celes sekret i cili do te perdoret me pas per kriptimin dhe deskriptimin e mesazheve. Gjate shkembimit te celesave nuk shkembehet asnje informacion sekret keshtu qe nuk kerkohet nje kanal i sigurte.

- RSA Public Keys

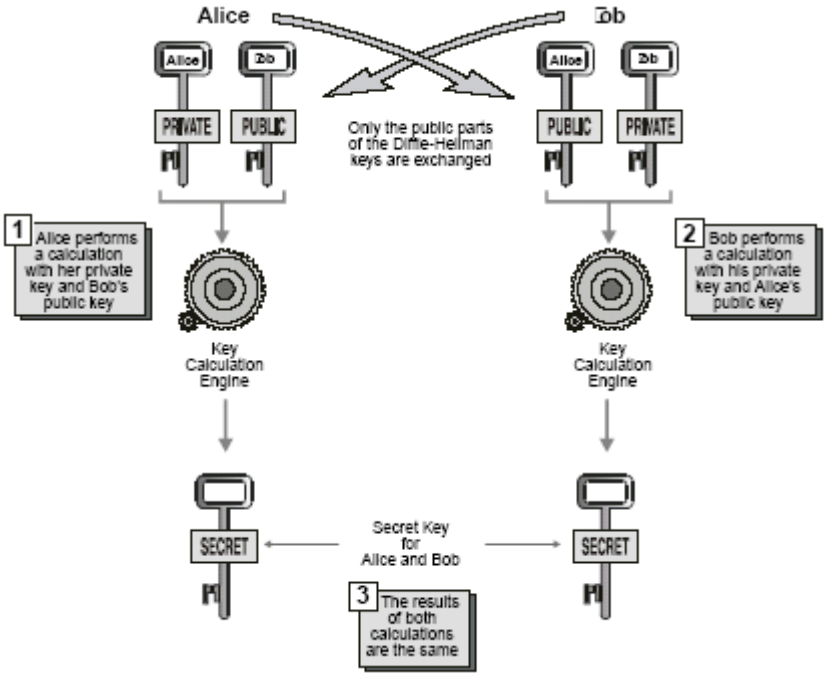
  Ne kontrast me ciftin e celesave Deffie-Hellman, cifti i celesave publik-privat RSA perdoret per te kriptuar mesazhe. Nje mesazh i kriptuar me nje celes publik mund te deskriptohet vetem me nje celes privat dhe anasjelltas. Shkembimi i celesave perfshin edhe shkembimin e iformacionit sekret, keshtu qe duhet ruajtur duke perdorur deshmi.

Figura e meposhtme ilustron skemen Deffie-Hellman, pjeset publike dhe private te celesave te dy personave Alice dhe Bob. Procesi i shkembimit eshte si me poshte:

1. Bob merr celesin publik te Alice dhe ben disa llogaritje duke perfshire celesin e tij privat dhe celesin publik te Alice.

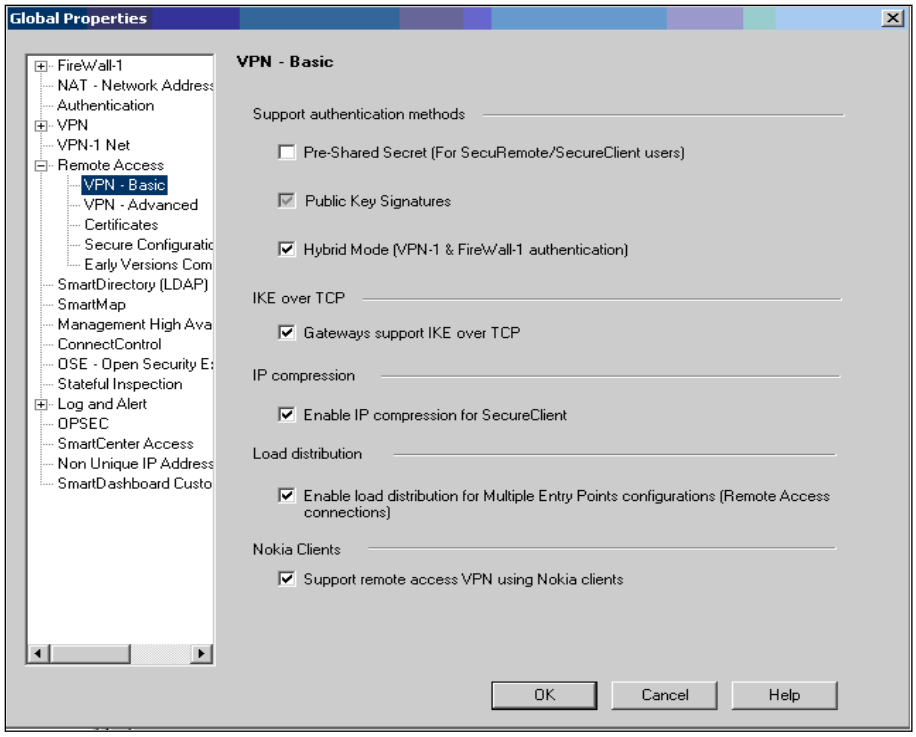
2. Alice merr celesin publik te Bob dhe ben disa llogaritje duke perfshire celesin e saj privat dhe celesin publik te Bob.

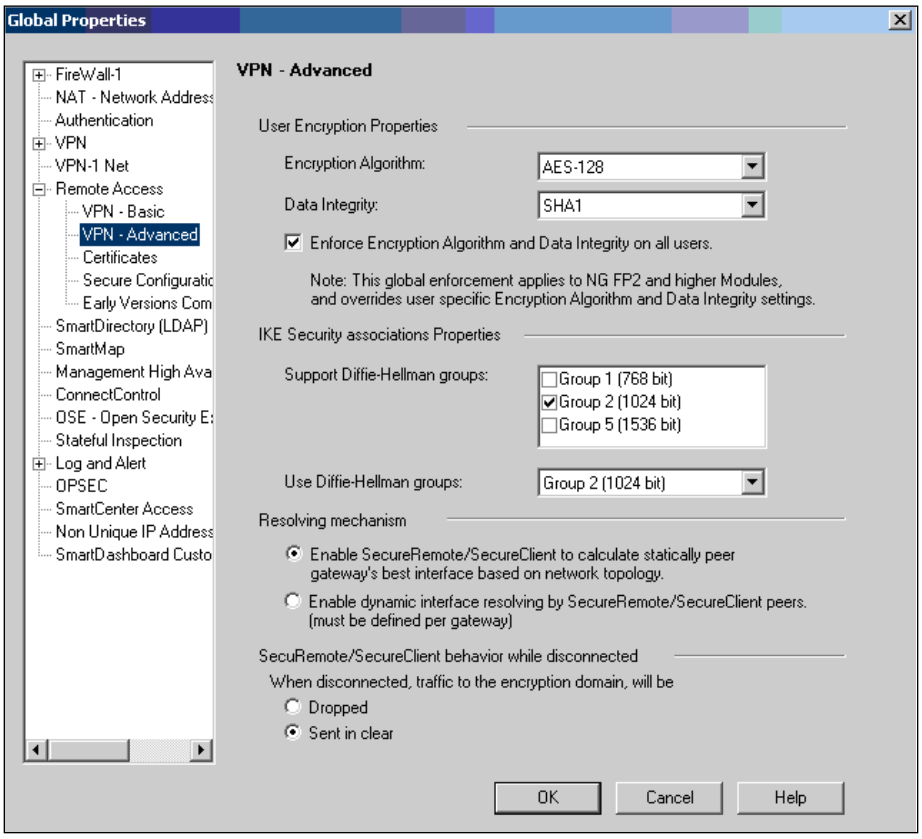
Rezultati i te dy llogaritjeve eshte i njejti, dhe ky rezultat eshte celesi sekret. Asnje informacion sekret nuk shkembehet, keshtu qe nuk ka mundesi qe nje pergjues te pervetesoje celesin sekret.



f) SecuRemote

VPN SecuRemote eshte aplikacioni klient qe krijon nje tunel VPN midis nje useri remote dhe rrjetit te brendshem qe menaxhohet nga nje modul Checkpoint ,duke e lejuar userin remote qe te aksesoje informacionin dhe serverat me anen e dial-up apo lidhjeve te dedikuara LAN. Per te vendosur nje lidhje te tille klient – gateway duhet specifikuar ne serverin e menaxhimit SmartCenter, userat qe kane te drejte aksesi ne rrjetin e brendshem. Keshtu fillimisht duhet krijuar profili i userit remote ne bazen e te dhenave te userave ne serverin e menaxhimit. Hapi i dyte do te jete konfigurimi i firewallit per te realizuar lidhjen me klientin VPN. Ky konfigurim perfshin percaktimin e komunitetit VPN ne te cilin do te marre pjese firewalli, çertifikatat apo çelesat sekrete qe do te perdoren etj. Per te pare konfigurimet e VPN japim komanden **Global Properties** tek menuja **Policy.** Ne dritaren qe na shfaqet hapim direktorine **Remote** dhe klikojme tek **VPN Basic** dhe me pas tek **VPN Advanced** per te pare konfigurimin e gateway tone lokal. Ne figurat e meposhtme shihet ky konfigurim per nje lidhje VPN. Hapi i fundit qe duhet bere do te jete krijimi i nje rregulle ne Bazen e Rregullave per grupin e userave SecuRemote qe do te aksesojne rrjetin tone. Ne kete rregull fusha **Source** duhet te permbaje grupin e userave SecuRemote nderkohe qe fusha destinacion do te permbaje nje rrjet, nje server apo nje grup serverash. Veprimi do te jete Client Encrypt.


Global Properties
FireWall-1
NAT - Network Address
Authentication
VPN
VPN-1 Net
Remote Access
VPN - Basic
VPN - Advanced
Certificates
Secure Configuratic
Early Versions Com
SmartDirectory (LDAP)
SmartMap
Management High Ava
ConnectControl
OSE - Open Security E
Stateful Inspection
Log and Alert
OPSEC
SmartCenter Access
Non Unique IP Address
SmartDashboard Custo
VPN - Basic
Support authentication methods
Pre-Shared Secret (For SecuRemote/SecureClient users)
Public Key Signatures
Hybrid Mode (VPN-1 & FireWall-1 authentication)
IKE over TCP
Gateways support IKE over TCP
IP compression
Enable IP compression for SecureClient
Load distribution
Enable load distribution for Multiple Entry Points configurations (Remote Access connections)
Nokia Clients
Support remote access VPN using Nokia clients
OK
Cancel
Help


Global Properties
FireWall-1
NAT - Network Address
Authentication
VPN
VPN-1 Net
Remote Access
VPN - Basic
VPN - Advanced
Certificates
Secure Configuratic
Early Versions Com
SmartDirectory (LDAP)
SmartMap
Management High Ava
ConnectControl
OSE - Open Security E
Stateful Inspection
Log and Alert
OPSEC
SmartCenter Access
Non Unique IP Address
SmartDashboard Custo
VPN - Advanced
User Encryption Properties
Encryption Algorithm:
AES-128
Data Integrity:
SHA1
Enforce Encryption Algorithm and Data Integrity on all users.
Note: This global enforcement applies to NG FP2 and higher Modules, and overrides user specific Encryption Algorithm and Data Integrity settings.
IKE Security associations Properties
Support Diffie-Hellman groups:
Group 1 (768 bit)
Group 2 (1024 bit)
Group 5 (1536 bit)
Use Diffie-Hellman groups:
Group 2 (1024 bit)
Resolving mechanism
Enable SecureRemote/SecureClient to calculate statically peer gateway's best interface based on network topology.
Enable dynamic interface resolving by SecureRemote/SecureClient peers. (must be defined per gateway)
SecuRemote/SecureClient behavior while disconnected
When disconnected, traffic to the encryption domain, will be
Dropped
Sent in clear
OK
Cancel
Help

g) SecureClient

VPN-1 SecureClient ka te njejtin funksion si SecuRemote por permban veçori shtese per sigurine si psh siguri ne permbajtje, regjistrimi i aktivitetit ne te dhena log dhe alerte. Me pak fjale SecureClient eshte SecuRemote i pajisur me firewall personal. Firewalli eshte i konfiguruar me rregullat Desktop Security te cilat shkarkohen nga Baza e Rregullave ne serverin e menaxhimit SmartCenter ne momentin e logimit te klientit.

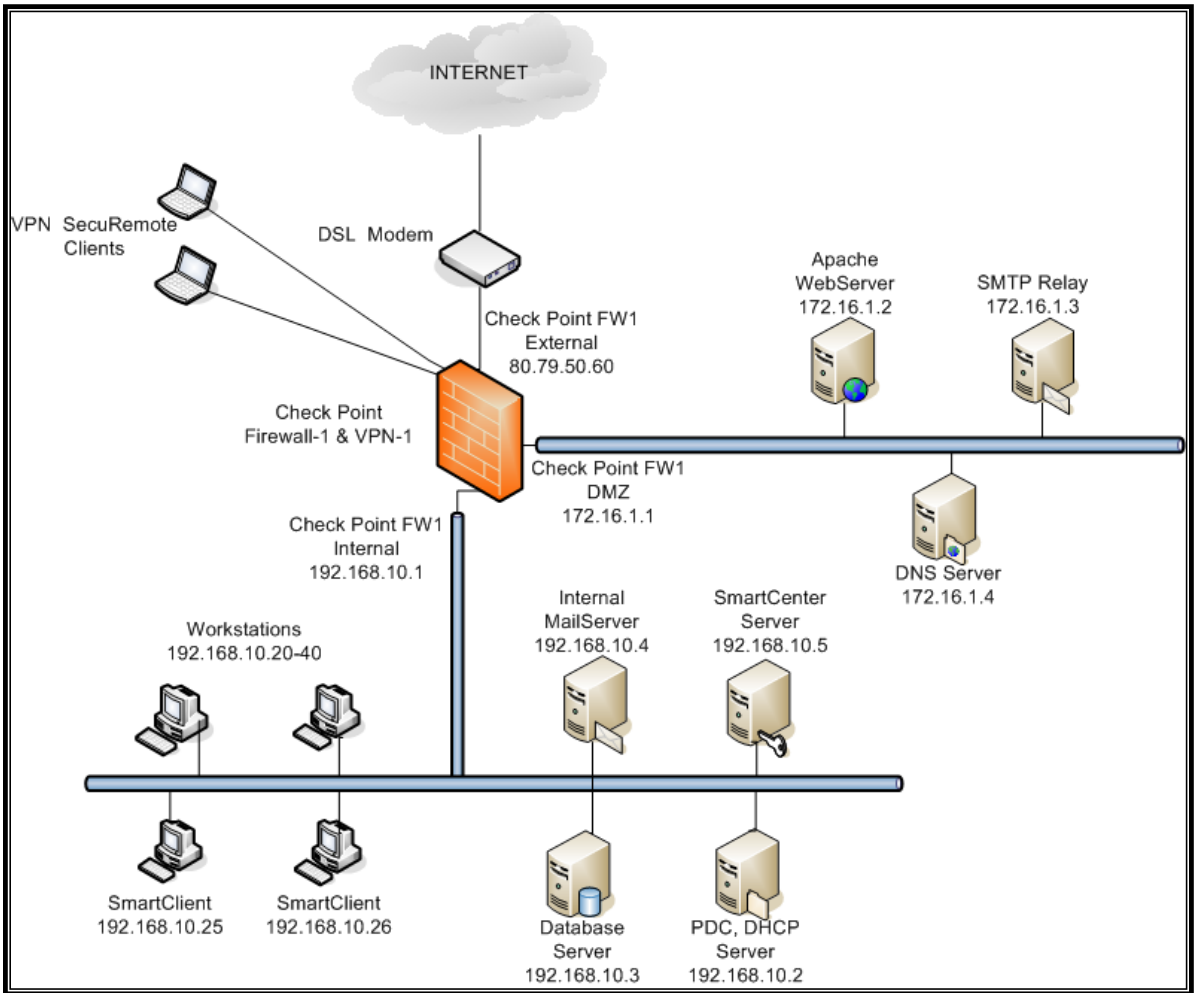
h) VPN pa klientë (Clientless VPN)

VPN pa kliente jane zgjedhja me e mire per tu perdorur per akses remote kur trafiku pra te dhenat qe duhet te aksesojme jane faqe Web apo e-mail. Nga vete emri ato nuk kane nevoje per program klient si SecuRemote apo SecureClient pasi perdorin nje web browser te zakonshem. Protokolli i perdorur eshte SSL pra kemi te bejme me HTTPS (HTTP te sigurte).

Perveç konfigurimeve normale te firewallit ne rastin e VPN pa kliente na duhet te krijojme dhe nje objekt Web Server dhe te specifikojme ne te sherbimin HTTPS. Per te krijuar objektin Web Server krijojme nje host te ri dhe e quajme Web_Server dhe i caktojme adresen IP. Me pas tek ky host qe krijuam do te percaktojme sherbimin HTTPS.

VII. Kapitulli 7 –Implementimi i Check Point

Bashkengjitur eshte nje rrjet praktik te cilin e kemi zgjedhur si model te rrjetit te nje kompanie apo biznesi:



1. Infrastruktura e rrjetit

Rrjeti eshte konceptuar te ndertohet sipas skemes se meposhtme. Per arsye sigurie serverat te cilet jane te aksesueshem nga interneti si psh WebServi Apache, SMTP Relay i cili menaxhon e-mailet inbound dhe outbound si dhe DNS severi jane vendosur ne nje DMZ pra duke i izoluar nga subneti i brendshem i kompanise ku jane vendosur serverat me te rendesishem si DB server qe mund te kene informacione konfidenciale dhe qe nuk duhet te dalin jashte kompanise. Ne rrjetin e brendshem eshte vendosur dhe Serveri i Menaxhimit te firewallit SmartCenter si dhe klientet GUI SmarClient qe do te administrojne firewallin te cilet

do te jene ne qender te vemendjes sone. Le te shohim me ne detaj pjeset perberese te rrjetit te brendshem.

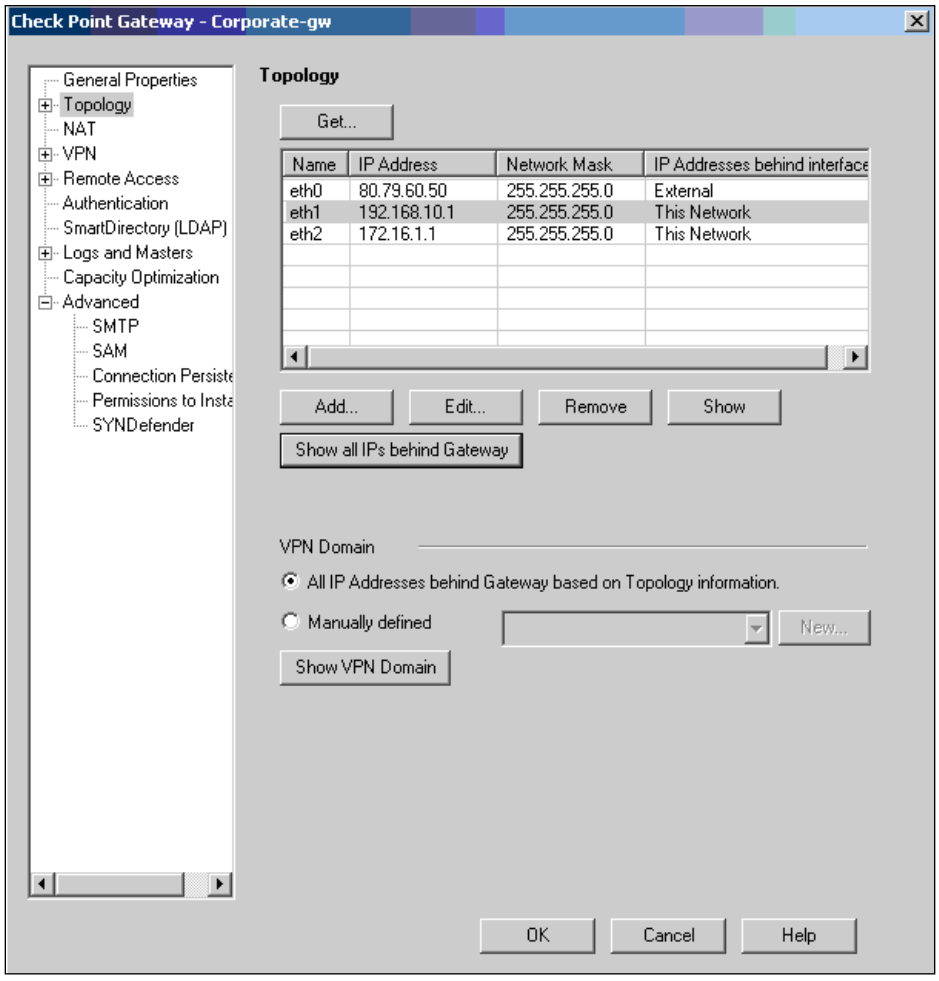
- **Internal Mail Server:** Eshte serveri qe menaxhon sistemin e postes elektronike te brendshme te kompanise. Ne te eshte instaluar Microsoft Exchange 2000.
- **PDC, DHCP Server:** Kontrolleri i Domainit te kompanise. Ne te eshte instaluar Active Directory ku jane te specifikuar te gjithe komputerat si dhe userat e kompanise. Sherben dhe si DHCP server per te pajisur me adrese IP te gjithe komputerat te konfiguruar me adrese IP dinamike.
- **Database Server:** Ne te ruhet baza e te dhenave e kompanise qe permban gjithe informacionin mbi operimin e saj. Ne te ruhen dhe te gjithe dokumentat qe perdoren nga punonjesit e kompanise.
- **SmartCenter Server:** Eshte serveri qe menaxhon firewallin dhe qe ruan te dhenat log te regjistruara nga moduli i perforcimit.
- **Web Server:** Serveri qe menaxhon faqen e internetit te kompanise.
- **SMTP Relay:** Eshte serveri qe menaxhon trafikun inbound dhe outbound te e-mailit pra qe menaxhon e-mailet qe jane te drejtuar brenda dhe jashte rrjetit te brendshem te komanise.
- **DNS Server:** Serveri qe ofron sherbimin DNS per kompjuterat e brendshem te kompanise.

Interneti ne rrjetin e brendshem sigurohet nga ISP me anen e nje linje te dedikuar DSL. Mund te perdorim dhe nje linje backup dial-up ne rast difekti te linjes kryesore. Me anen e VPN resurset e rrjetit te brendshem do te aksesohen nga disa usera remote qe mund te jene partneret e kompanise apo punonjesa mobile.

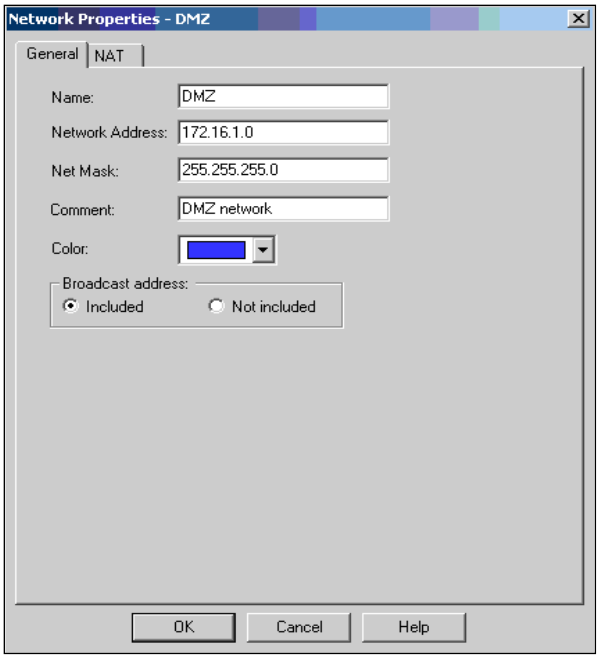
Moduli qendror i perforcimit Firewall-1 & VPN-1 mund te jete nje kompjuter ose nje platforme hardware si psh Nokia IS500. Per thjeshtesi kemi zgjedhur rastin kur ky modul eshte nje platforme Windows 2000 ku jane aktive vetem sherbimet e domosdoshme per operimin e tij si firewall. Duhet te kete tre nderfaqe rrjeti te konfiguruara si ne figure. Maska e perdorur do jete ajo default 24 qe i korrespondon subnet mask 255.255.255.0. Pasi i kemi konfiguruar te treja nderfaqet e rrjetit te modulit te perforcimit aktivizojme *IP-forwarding* dhe me pas mund te fillojme instalimin e Firewall-1 & VPN-1 tek ky kompjuter, te SmartClient tek serveri menaxhimit dhe te klienteve GUI sipas hapave te pershkruara me pare. Gjate instalimit te SmartClient do te na kerkohet te bejme regjistrimin e licensave per produktin tone Check Point, percaktimin e klienteve GUI duke dhene adresat IP te kompjuterave ne rrjet ku kemi instaluar SmartClient perkatesisht 192.168.10.25 dhe 192.168.10.26 si dhe krijimin e entiteteve me te drejta administrative mbi serverin e menaxhimit SmartCenter. Ne fund do te behet dhe inicializimi i autoritetit te brendshem certifikues. Te gjitha keto procedura jane shpjeguar ne kapitullin tre per instalimin dhe konfigurimin e Check Point NG.

2. Krijimi i objekteve të rrjetit

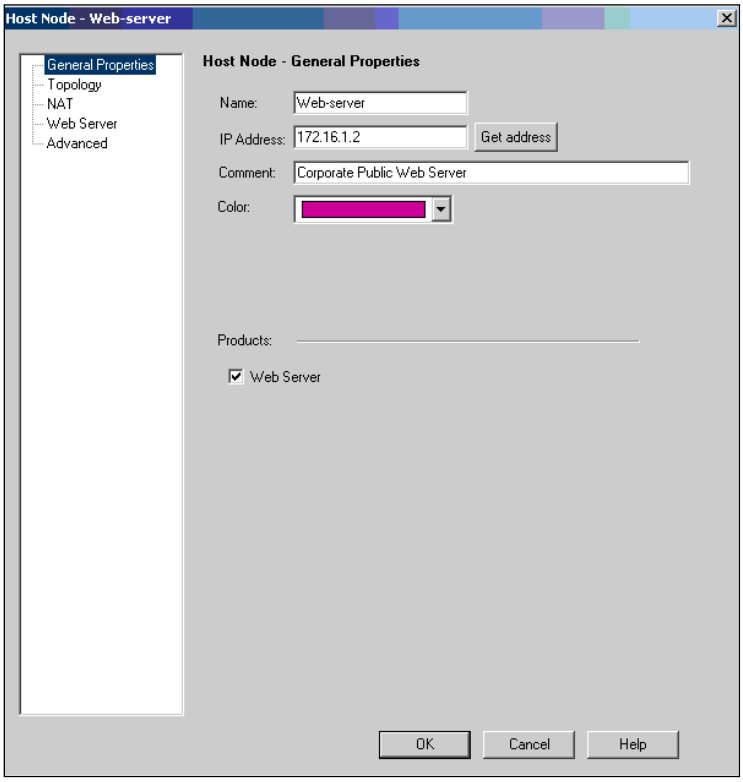
Perpara se te konfigurojme Bazen e Rregullave duhet qe te krijojme objektet e rrjetit tek serveri menaxhimit. Gjithashtu tek objekti qe perfaqeson firewallin duhet te konfigurojme nderfaqet e rrjetit me adresat IP perkatese. Per ta realizuar zgjedhim komanden **Network Objects** tek menuja **Manage.** Zgjedhim objektin *corporate-gw* qe perfaqeson firewallin ne rrjetin tone dhe i japim **Edit.** Ne ekran do shfaqet dritarja me karakteristikat e firewallit e cila paraqitet ne figuren e meposhtme. Shkojme tek **Topology** dhe aty shtojme te tre nderfaqet e firewallit.



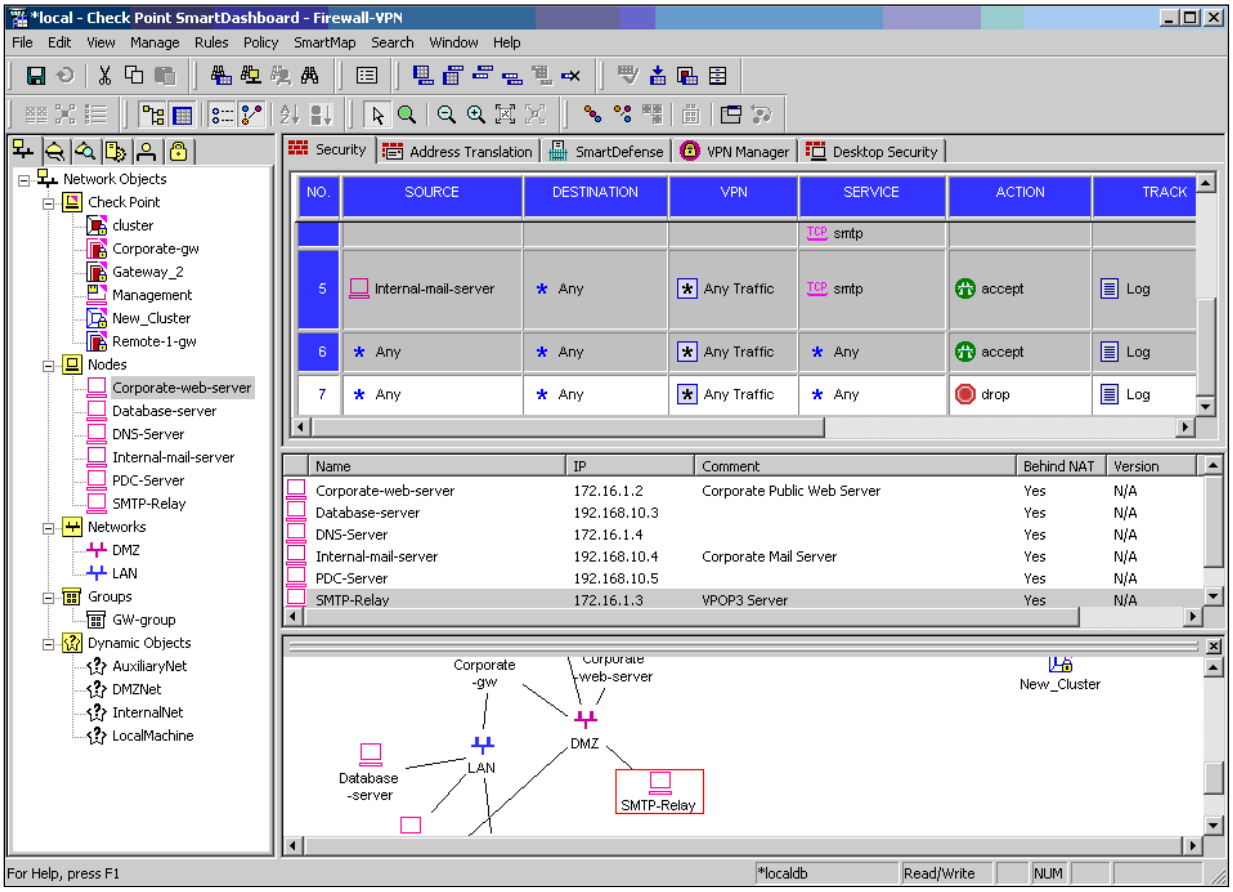
Duhet te krijojme objekte per te gjithe serverat qe bejne pjese ne rrjetin tone te brendshem dhe qe do te perfshihen ne bazen e rregullave. Do te krijojme dy objekte **Networks** te cilat do t'i emerojme *Internal* dhe *DMZ.* Shembullin e krijimit te DMZ jepet me poshte.



Tek te dy objektet kemi lejuar NAT ne modalitet *hide* dhe te gjitha adresat e brendshme jane te fshehura pas adreses IP te nderfaqes se jashtme. Pervec dy objekteve qe perfaqesojne dy subnetet tona duhet te krijojme objektet qe perfaqesojne hostet ne rrjet. Krijimi i ketyre objekteve eshte i ngjashem me krijimin e objekteve te subneteve. Shembulli i krijimit te objektit qe perfaqeson **WebServerin** jepet ne figuren e meposhtme.



Tek **General Properties** do te japim emrin e WebServer-it si dhe adresen IP te tij. Tek **Topology** do te krijojme nderfaqen e rrjetit te Web Serverit duke shenuar dhe njehere adresen IP si dhe Subnet Maskun. Ne se do te aplikojme mekanizmin NAT atehere nje gje e tille duhet te konfigurohet tek menuja **NAT** si dhe modaliteti *Hide* apo *Static* qe do te perdoret. Tek menuja **Web Server** duhet te zgjedhim modulin e perforcimit qe do te sherbeje si mbrojtje dhe qe ne rastin tone eshte firewalli i quajtur Corporate_gw. Te njejten procedure do te ndjekim dhe per hostet e tjere qe bejne pjese ne rrjetin tone dhe qe do te perfshihen ne politiken e sigurise. Ne fund pamja e pemes se objekteve ne dritaren kryesor te SmarDashboard do te jete si me poshte:

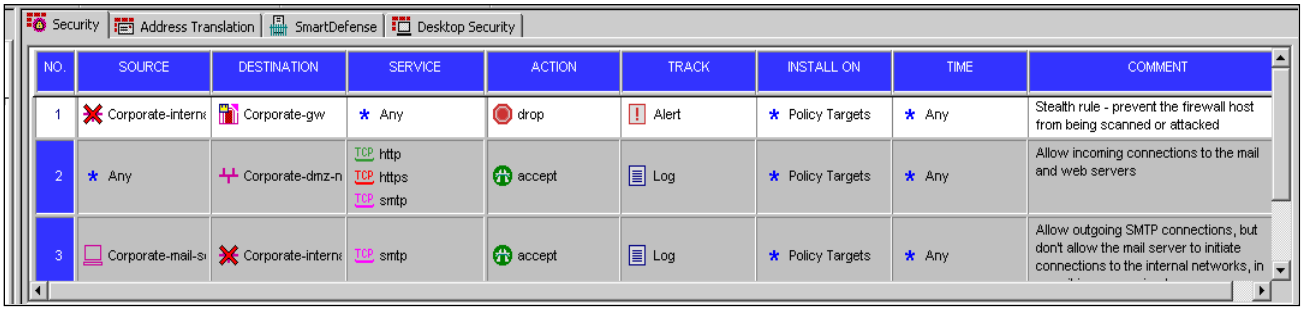


3. Krijimi i Bazës së Rregullave

Pasi kemi krijuar objektet e rrjetit mund te fillojme me konceptimin e bazes se rregullave qe do jete implementimi i politikes se sigurise ne firewall. Gjeja e pare qe duhet bere eshte identifikimi i trafikut te lejuar dhe me pas gjithcka tjeter do te jete e palejuar. Nje gje e tille varet nga shume faktore si psh nga sherbimet qe do te ofroje kompania, veprimtaria e stafit te IT etj. Ne tabelen e meposhtme eshte percaktuar trafiku i lejuar.

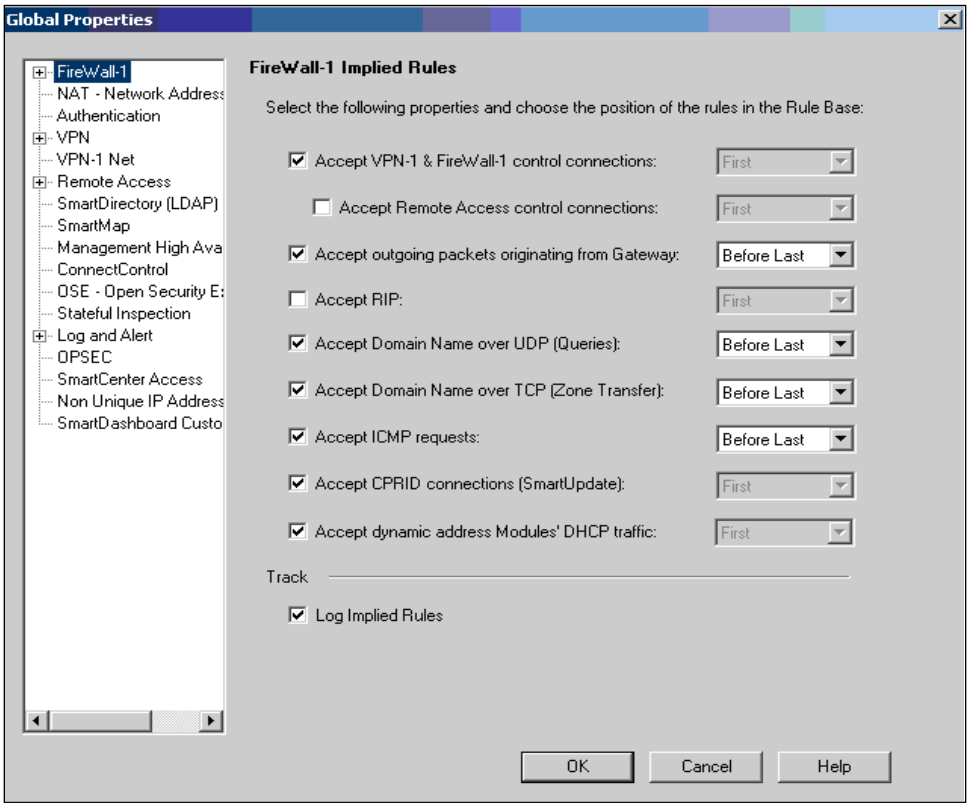
Burimi	Vendndodhja e Burimit	Destinacioni	Vendnodhja e Destinac.	Numri i Portes
X	X	***SMTP Relay***	Rrjeti DMZ	25 TCP
X	X	***Web Server***	Rrjeti DMZ	80 TCP (http) 443 TCP(https)
X	X	***DNS Server***	Rrjeti DMZ	53 TCP 53 UDP
SMTP Relay	Rrjeti DMZ	***Internal Mail Server***	Rrjeti i brendshem	25 TCP
Internal Mail Server	Rrjeti i brendshem	***SMTP Relay***	Rrjeti DMZ	25 TCP
X	Rrjeti i brendshem	***X***	X	80 TCP 443 TCP
Web Server	Rrjeti DMZ	***X***	X	53 TCP 53 UDP
Sektori IT	Rrjeti i brendshem	***X***	X	20 TCP 21 TCP
Sektori IT	Rrjeti i brendshem	***X***	X	23 TCP
Sektori IT	Rrjeti i brendshem	***X***	X	23 TCP
Sektori IT	Rrjeti i brendshem	***X***	X	161 UDP

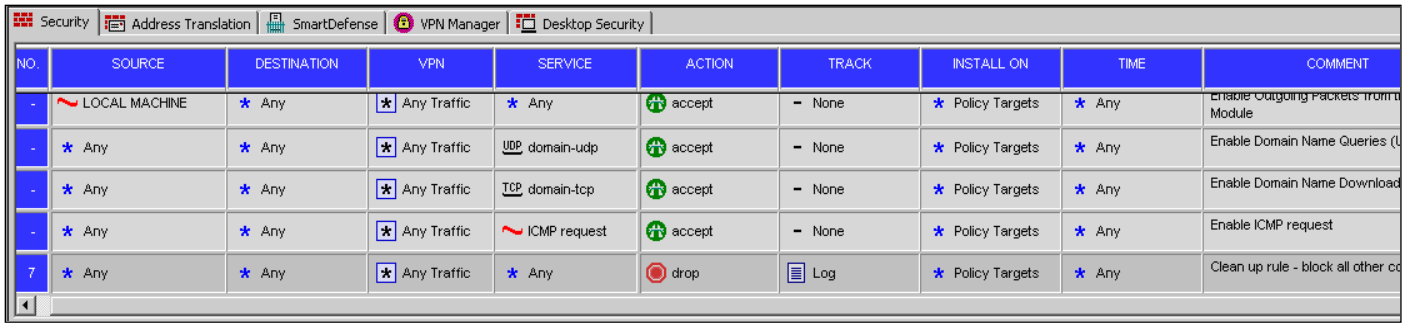
Tani qe kemi vendosur se cili do te jete trafiku i lejuar ne rrjet mund te fillojme te konfigurojme Bazen e Rregullave. Si rregull fillimisht do te vendosim dhe rregullat Stealth dhe Clean Up qe do te jene perkatesisht rregulla e pare dhe e fundit e bazes. Sic e kemi thene rregulla Stealth eshte rregulla qe hedh poshte dhe regjistron ne skedaret log trafikun qe eshte i destinuar per Firewall-1. Duhet te jete gjithmone rregulla e pare ne Bazen e Rregullave pasi eshte rregulla qe mbron firewall-in. Ndersa rregulla Clean-Up eshte rregulla e fundit ne Bazen e Rregullave dhe hedh poshte te gjithe trafikun qe nuk eshte lejuar ne rregullat e mesiperme.



Pasi kemi perpiluar gjithe rregullat duhet t'i ruajme ato ne databasen e rregullave qe ndodhet ne serverin e menaxhimit. Per te realizuar kete tek menuja **Policy** zgjedhim komanden **Install.**

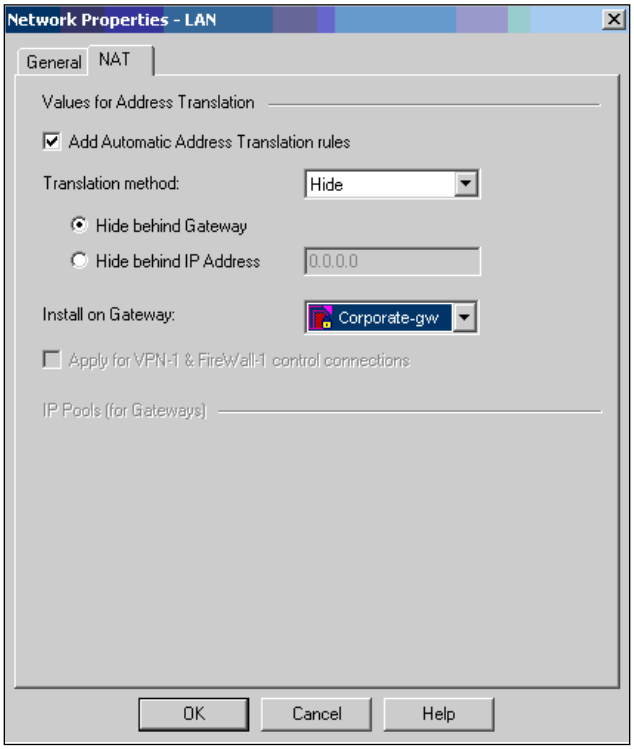
Per te lejuar komandat ICMP drejt firewallit shkojme tek menuja **Policy** dhe japim komanden **Global Properties.** Ne tabin qe i korrespondon Firewall-1 shohim ne se eshte i checkuar opsioni **Accept ICMP requests.** Po ne kete dritare duhet te checkojme dhe dy opsionet **Accept Domain Name over UDP** dhe **Accept Domain Name over UDP** per te lejuar serverin DNS qe te kryeje funksionin e tij dhe te lidhet me serverat e tjere DNS. Ne te djathte te çdo opsioni specifikojme renditjen e rregulles perkatese te implikuar ne bazen e rreguullave. Mund t'i japim tre vlera **First, Last** dhe **Before Last.** Ne te tre rregullat e mesiperme qe checkuam zgjedhim opsionin *Before Last* qe e vendos rregullen e mesiperme para rregulles se fundit qe eshte rregulla Clean Up. Pasi klikojme OK mund te shohim rezultatet ne bazen e rregullave. Ne fund japim serish komanden **Install** tek menuja **Policy.**

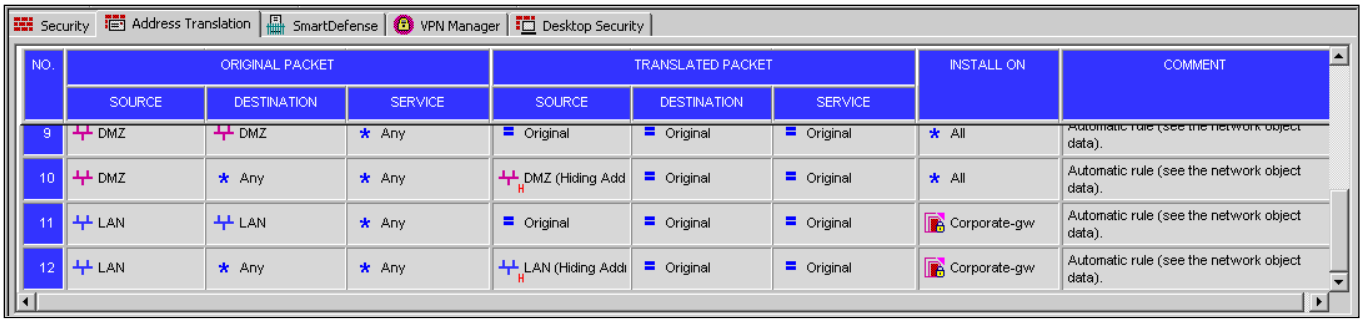




4. Aplikimi i NAT-it automatik

Ne subnetin e brendshem dhe ne ate DMZ do te aplikojme mekanizmin NAT. Do et perdorim modalitetin **Hide** dhe te gjithe paketat qe dalin jashte rrjetit tone do t'i fshihen adreses se nderfaqes se jashtme te firewallit. Per te realizuar mekanizmin NAT zgjedhim objektet qe perfaqesojne rrjetin e brendshem dhe DMZ dhe i japim komanden Edit. Tek menuja NAT specifikojme modalitetin qe do te perdorim si dhe adresen IP qe do te perdoret. Ne se zgjedhim opsionin **Hide Behind Gateway** do perdoret nderfaqja e jashtme e firewallit. Me pas shohim efektet ne bazen e rregullave.

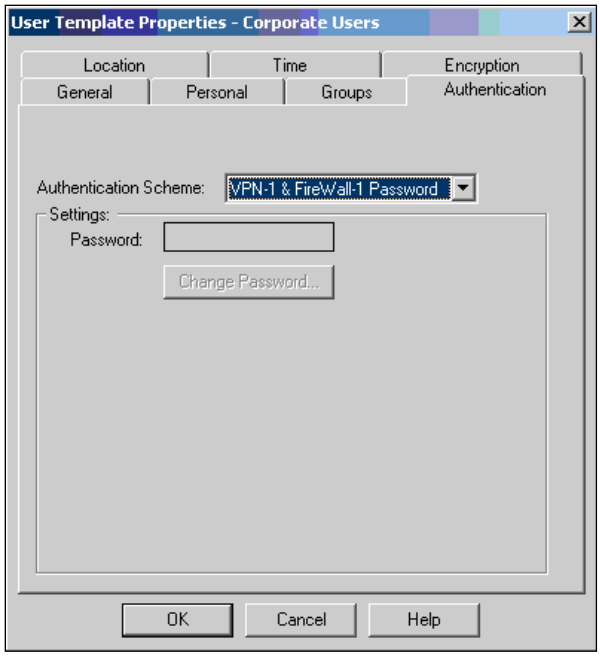




5. Autentikimi i përdoruesve

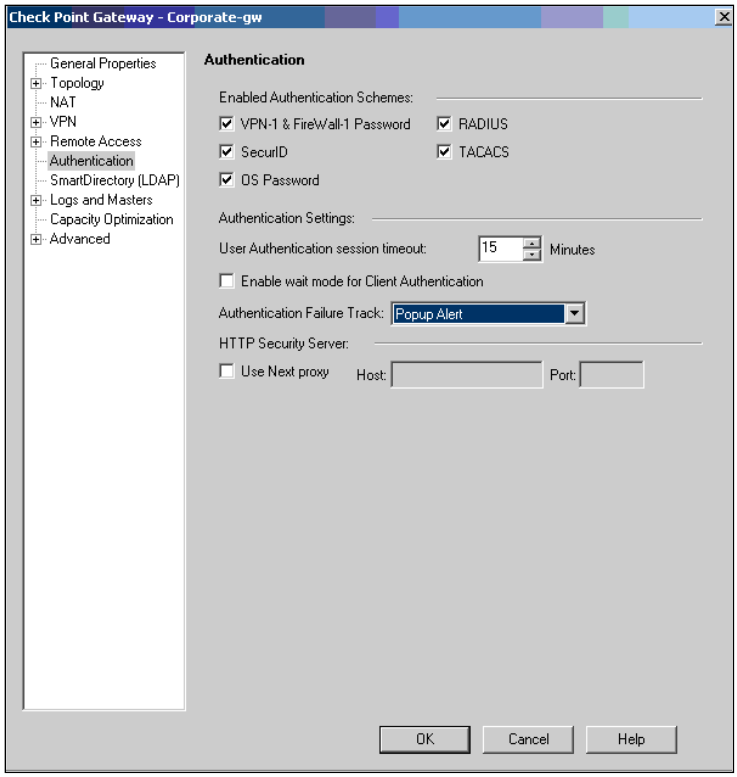
Pasi kemi aplikuar NAT-in automatic eshte momenti qe te konfigurojme procesin e autentikimit te userave. Kemi zgjedhur te perdorim autentikimin e tipit user meqenese ai eshte i pavarur nga komputeri klient qe perdoret por eshte i orientuar ndaj profilit te userit. Nje gje e tille eshte shume e pershtatshme per userat e domainit te cilet mund te logohen ne çdo komputer qe ben pjese ne domain. Autentikimi mund te perdoret per shume arsye. Psh ne mund te perdorim autentikimin per te kufizuar aksesin e perdoruesve ndaj resurseve te ndryshme te rrjetit duke e ndare ate sipas departamenteve. Gjithashtu autentikimi mund te perdoret per te regjistruar trafikun ne internet per secilin perdorues pasi ne skedaret log do te shfaqet dhe emri i perdoruesit te loguar. Keshtu mund te kuptojme se kush perdor internetin ne menyre te sigurte dhe se kush futet ne web site te konsideruara si te “rrezikshme” per sigurine ne rrjet.

Meqenese rregullat e autentikimit perdorin grupe userash dhe jo usera individuale, duhet te percaktojme fillimisht grupet qe do perdorim dhe me pas te krijojme userat ne to. Mund te krijojme nje template specific per userat qe do te krijojme. Ne kete menyre krijimi i userave te rinj behet me i thjeshte. Per krijimin e userave, templateve apo grupeve te userave mjafton te shkojme tek ikona **User** ne pemen e objekteve ose tek menuja **Manage, Users and Administrators, New.** Krijojme nje template per userat e firewall-it.

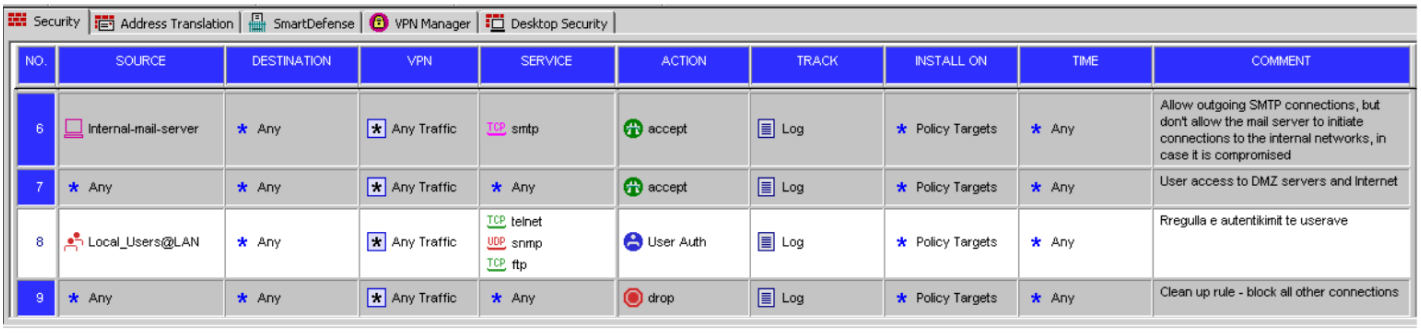


Tek menuja **General** japim emrin e template-it qe po krijojme. Nderkohe qe tek menuja **Groups** specifikojme se ne cilin grup do te bejne pjese userat qe do te krijohen nga ky template. Per userat kemi krijuar dy grupe: Local_Users qe perfaqeson punonjesit e brendshem te kompanise dhe Mobile_Users qe perfaqeson userat mobile qe aksesojne rrjetin me anen e lidhjeve VPN. E rendesise te veçante per ne eshte menuja **Authentication** pasi aty specifikohet skema e autentikimit qe do te perdoret. Nje skeme e preferuar do te ishte ajo RADIUS por ne mungese te nje serveri RADIUS kemi zgjiedhur skemen qe realizon autentikimin me anen e passwordit te modulit Firewall-1 siç tregohet dhe ne figure. Ne fund japim komanden **Install Database** tek menuja **Policy** ne menyre qe te gjithe ndryshimet e bere te ruhen tek database i perdoruesve qe ndodhet ne serverin e menaxhimit.

Pasi kemi mbaruar procesin e krijimit te userave duhet te konfigurojme modulin Firewall-1 qe te suportoje skemen e autentikimit qe do te perdorim. Per kete tek menuja **Manage** zgjedhim **Network Objects.** Tek lista qe do te na shfaqet zgjedhim objektin qe perfaqeson Firewall-1 dhe japim komanden **Edit.** Tek **Authentication** checkojme skemen e autentikimit qe do te perdorim. Nderkohe qe opsionet e tjera nuk i ndryshojme.

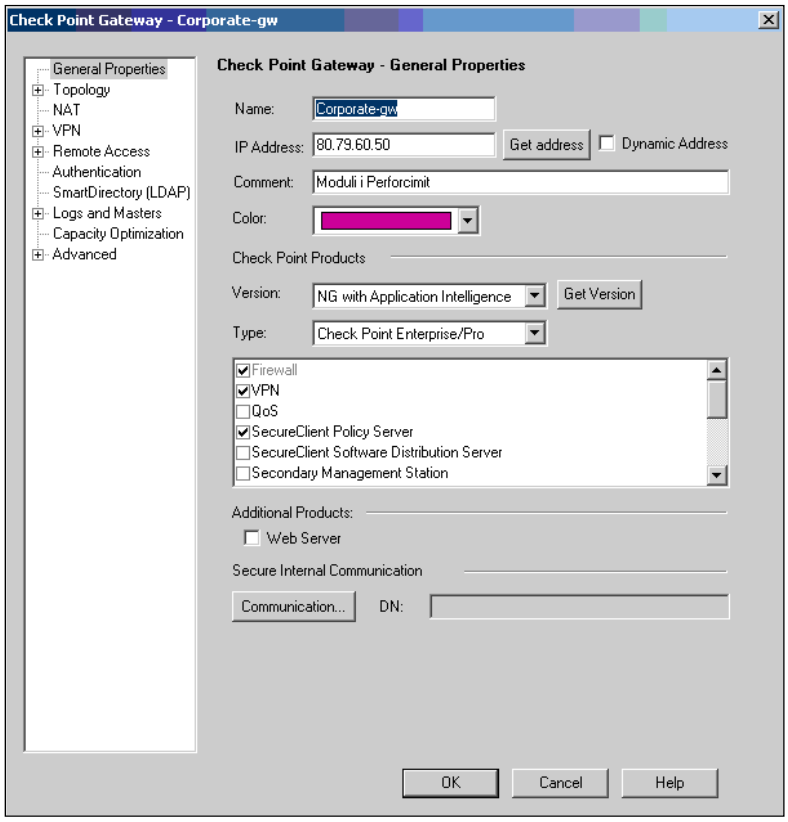


Hapi i fundit eshte krijimi i rregulles se autentikimit ne bazen e rregullave. Ne fushen **Source** klikojme me butonin e djathte, japim komanden **Add User Access** dhe zgjedhim grupin qe do te autentikohet. Gjithashtu mund te specifikojme dhe vendndodhjen ne terma komputerash te rrjetit nga deshirojme qe te realizohet ky autentikim. Tek fusha **Service** specifikojme sherbimin apo sherbimet qe deshirojme te autentikojme nderkohe qe tek fusha **Action** do zgjedhim **User_Auth** qe perfaqeson veprimin e autentikimit user.



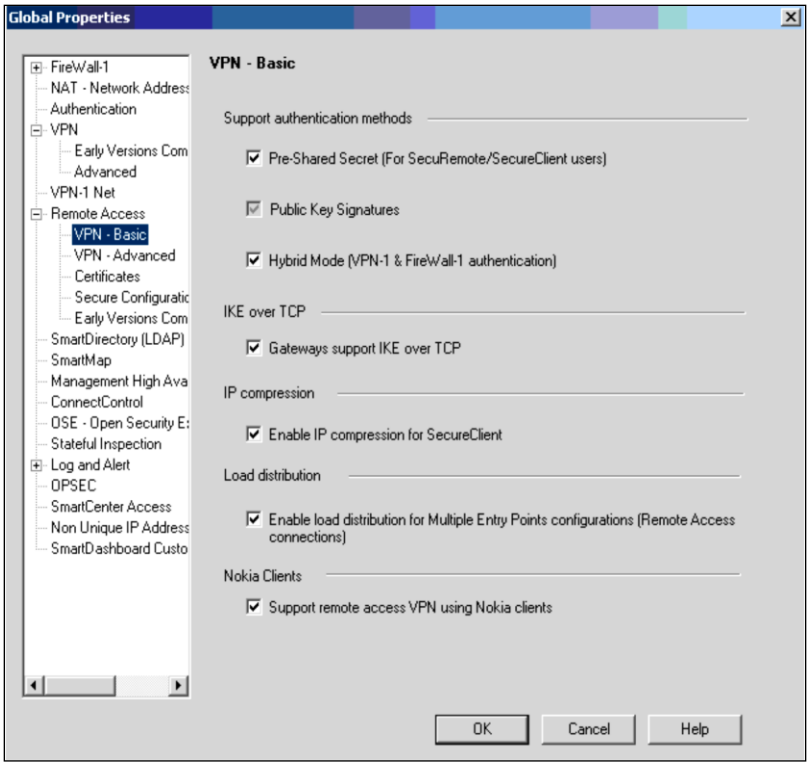
6. Realizimi i VPN

Tani eshte momenti qe te konfigurojme lidhjen VPN per userat remote te cilet mund te jene partneret e kompanise ose agjentet mobile te saj. Lidhja VPN do te jete e tipit klient-gateway. Per te realizuar lidhjen VPN duhen konfiguruar se pari moduli i perforcimit i kompanise sone si dhe duhen instaluar programet klient te VPN: SecuRemote ose SecureClient. Per te konfiguruar firewallin japim komanden **Edit** tek objekti i rrjetit qe e perfaqeson ate.

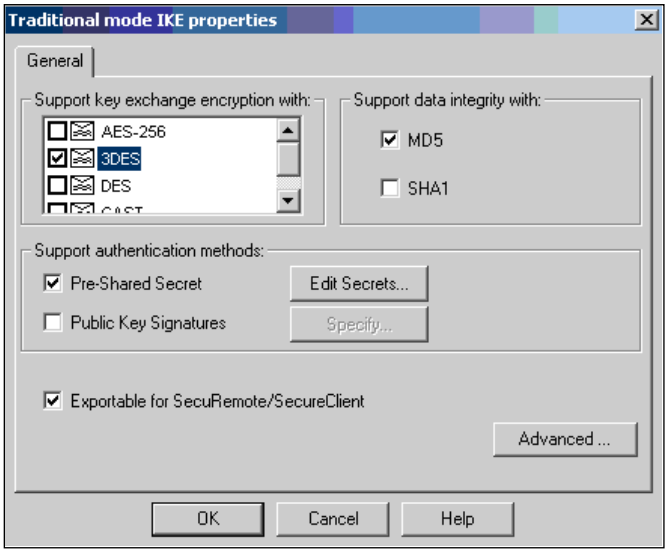


Tek **General Properties** zgjedhim **SecureClient Policy Server.** Kjo i lejon te gjithe klientet VPN qe perdorin SecureClient qe te shkarkojne nga Serveri i Menaxhimit rregullat e sigurise Desktop Security per tu perdorur nga firewalli personal i SecureClient. Tek menuja **VPN** klikojme tek **Traditional Mode Configuration.** Ne dritaren qe hapet zgjedhim opsionin **Exportable for SecuRemote/SecureClient.** Japim **OK.**

Tani duhet te konfigurojme **Global Properties** tek menuja **Policy.**

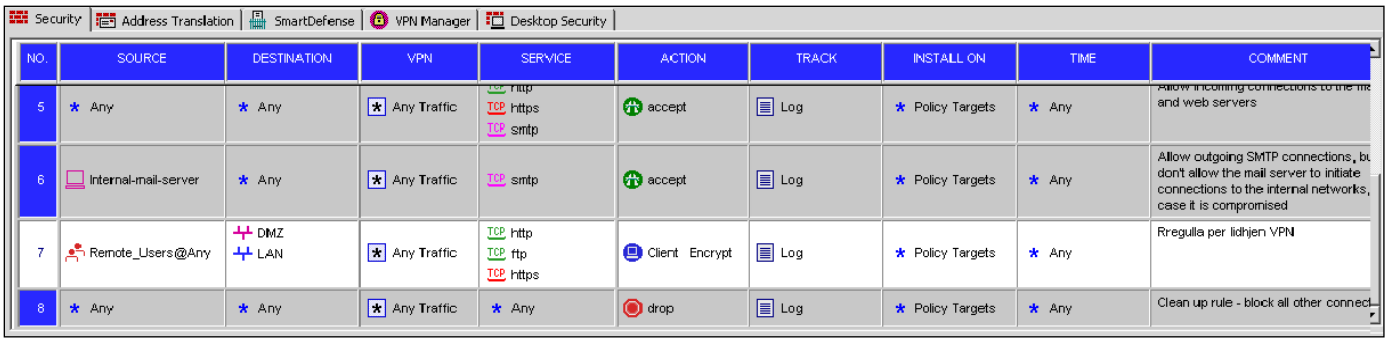


Tek **Remote Access** hapim menune **VPN-Basic** dhe aktivizojme opsionin **Pre-Shared Secret** si dhe opsionet e tjera te treguara ne figure. Opsionit **Pre-Shared Secret** lejon perdorimin e nje sekreti (passwordi) te perbashket per autentikimin e klientit. Ky çeles do te transmetohet me anen e protokollit IKE i cili ne firewallin tone eshte konfiguruar si ne figuren e meposhtme. Keshtu shkembimi i çelesave do te realizohet me skemen e enkriptimit **3DES** meqenese po perdorim çeles simetrik nderkohe qe per te verifikuar integritetin e te dhenave do te perdorim funksionin hash **MD5.**

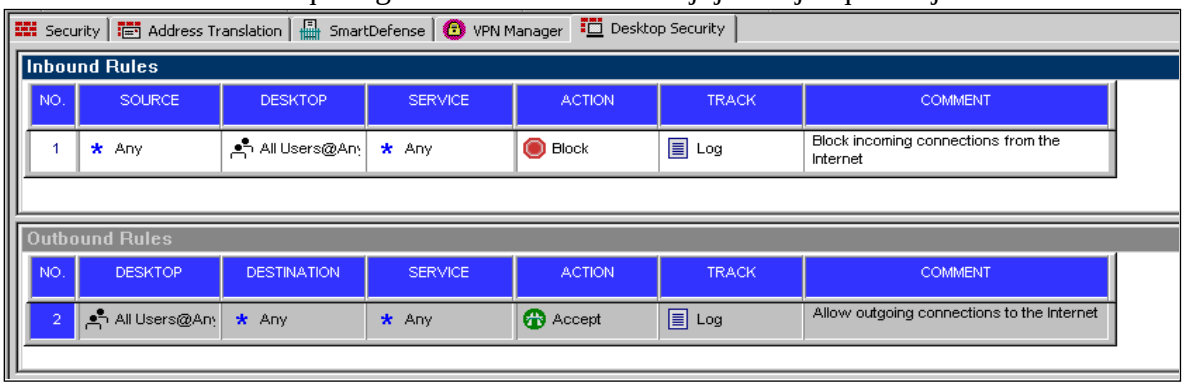


Tani duhet te percaktojme rregullen qe do te perdoret per lidhjen VPN si dhe rregullat qe do te perdoret nga firewalli i SecureClient. Ne rregullen e lidhjes VPN fusha **Source** do te

permbaje grupin e userave remote nderkohe qe fusha **Destination** mund te permbaje nje rrjet, nje server apo nje grup serverash ne varesi te resurseve te rrjetit qe duhet te aksesojne userat remote. Fusha **service** do te plotesohet sipas nevojave nderkohe qe fusha **Action** do te permbaje veprimin **Client Encrypt.** Rregulla e lidhjes VPN jepet ne figuren e meposhtme



Nderkohe qe rregullat e Desktop Security do te percaktohen si me poshte. Perkatesisht rregulla **Inbound** do te bllokoje lidhjet qe vijne nga Interneti ne komputerin ku eshte instaluar SecureClient nderkohe qe rregulla **Outbound** do te lejoje lidhjet qe i drejtohen Internetit.



Pasi kemi mbaruar pune me konfigurimin e modulit VPN duhet te vazhdojme me instalimin dhe konfigurimin e klienteve SecuRemote dhe/ose SecureClient. Te dy keto programe gjenden ne CD e paketes CheckPoint dhe do t'i instalojme ne kompjuterat qe do te perdoren nga userat mobile per tu lidhur me rrjetin tone. Pasi programi klient eshte instaluar do te vazhdojme me konfigurimin e lidhjes nga ana e klientit. Duhet qe te shtojme modulin VPN ndaj te cilit do te realizohet lidhja. Per kete shkojme tek menuja **File, Name, IP** dhe japim adresen IP te nderfaqes se jashtme te firewallit tone. Do te na kerkohet qe te japim nje username dhe password te cilet mund te jene userat qe krijuam gjate procesit te autentikimit te perdoruesve. Ne fund duhet te krijojme nje rregull te re sigurie qe do t'i lejoje userat te aksesojne rrjetin. Kjo rregull do te jete e njejte me rregullen e sigurise qe krijuam tek firewalli. Ne kete moment lidhja VPN eshte gati dhe mund te kontrollojme te dhenat log per te pare ne se tuneli eshte krijuar.

VIII. Ankronime

3DES - Triple DES
ACL - Access Control List
AES - Advanced Encryption Standart
AI - Application Intelligene
AIX - Advanced Interactive Executive
AH - Authentication Header
API - Application Programming interface
ARP - Address Resolution Protocol
ASIC - Application Specific Integrated Circuit
ATM - Asynchronous Transfer Mode
BGP - Border Gateway Protocol
CA - Certificate Authority
CPOS - Check Point Operating System
CPU - Central Processing Unit
CVP - Content Vectoring Protocol
DES - Data Encryption Standart
DMZ - Demilitarized Zone
DN - Distinguished Name
DNS - Domain Name System
DoS - Denial of Service
DSL - Digital Subscriber Line
ELA - Event Logging API
ESP - Encapsulating Security Payload
FDDI - Fiber Distributed Data Interface
FTP - File Transfer Protocol
FW - Firewall
GCC - GNU Compiler Collection
GPL - General Public License
GUI - Graphical User Interface
HDLC - High Level Data Link Control
HTTP - HyperText Transfer Protocol
HTTPS - HTTP over SSl
ICA - Internal Certificate Authority
ICF - Internet Connection Firewall
ICMP - Internet Control Message Protocol
IDS - Intrusion Detection System
IKE - Internet Key Exchange
IP - Internet Protocol
IPComp - IP Payload Compression
IPSec - Internet Protocol Security
IPSO - Internet Protocol Security Option
IPX - Internetwork Packet Exchange
IPv4 - Internet Protocol version 4

IPv6 - Internet Protocol version 6
ISO - International Organization for Standartization
ISP - Internet Service Provider
LAN - Local Area Network
LDAP - Lightweight Directory Access Protocol
MAC - Media Access Control
MD2 - Message Digest 2
MD5 - Message Digest 5
NAT - Network Address Translation
NG - Next Generation
OPSEC - Open Platform for Security
OS - Operating System
OSPF - Open Shortest Path First
PAT - Port Address Translation
PC - Personal Computer
PIN - Personal identification Number
PKI - Public Key Infrastructure
PPTP - Point-to-Point Tunneling Protocol
QoS - Quality of Service
RA - RegistrationAuthority
RADIUS - Remote Authentication Dial-In User Service
RDP - Reliable Datagram Protocol
RFC - Request For Comments
RIP - Routing Information Protocol
SA - Security Association
SCTP - Secure Control Transmission Protocol
SCV - Secure Configuration Verification
SHA - Secure Hash Algorithm
SIC - Secure Internal Com,munications
SNMP - Simple Network Management Protocol
SSL - Secure Sockets Layer
SVN - Secure Virtual Network
TACACS - Terminal Access Controller Access Control System
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
VoIP - Voice Over IP
VPN - Virtual Private Network

IX. Referencat

- Virtual Private Networks-Charlie Scott, Paul Wolfe, and Mike Erwin
- Privacy-Enhanced Business
- Check Point NG Security Administration – Syngress
- Check Point Firewall -1 VPN Manual – Check Point Technologies

- https://www.computerworld.com/article/2546283/networking/what-you-need-to-know-about-vpn-technologies.html
- https://hacked.com/virtual-private-network-vpn-everything-you-need-to-know/
- www.checkpoint.com
- http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en#contenu
- https://www.globalknowledge.com/us-en/
- www.syngress.com