SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Preddiplomski sveučilišni studij računarstva

Završni rad

IMPLEMENTACIJA VPN MREŽA

radna verzija

Rijeka, ožujak 2019. Maja Vrsaljko

Sadržaj

1. Uvod 1

2. VPN 2

2.1. Što je VPN? 2

2.2. Razvoj 3

2.3. Namjena 4

2.4. Osnovni koncept 5

2.5. Zahtjevi 7

2.6. Vrste rješenja 7

2.7. Preduvjeti za ostvarenje VPN mreže 8

2.7.1 Vatrozid 8

2.6.2 Enkripcija podataka 11

2.7. VPN tehnologije 15

2.7.1 SSL 15

2.6.2. SSH 16

2.6.3 IPSec 17

2.6.4 L2TP 18

3. Sofverska implementacija 19

4. Hardverska implementacija 19

1. Uvod

- na kraju

2. VPN

2.1. Što je VPN?

Virtualna privatna mreža (VPN) je proširenje privatne mreže preko određene javne mrežne infrastrukture. Omogućuje klijentima slanje ili primanje podataka preko različitih nesigurnih komunikacijskih kanala poput Interneta ili ATM mreža. VPN je prvenstveno niz tehnologija koje sudjeluju u realizaciji sigurnog kanala između dvije krajnje točke.

Naziva se virtualna jer neposredno spaja dva geografski udaljena klijenta, preciznije, ne postoji potreba za fizičkim vezama, već se povezivanje odvija preko javnog medija. Poseban naglasak stavlja se na privatnost i sigurnost mreže. Podrazumijeva se korištenje istih sigurnosnih pravila koja se primjenjuju u lokalnim mrežama.

Privatna mreža ili intranet je izolirano područje unutar mreže kojoj ima pristup samo definirani broj korisnika i obično je pronalazimo u poslovnim organizacijama. Tipični korporativni primjer je lokalna (LAN) mreža koja povezuje od jednog do nekoliko stotina računala (čvorova) specijaliziranim kablovima u jednu privatnu mrežu. Korisnici međusobno komuniciraju i oni jedini imaju pravo izmjene i pregleda podataka. Ovakvim modelom podaci se nalaze u povjerljivom i zaštićenom okruženju, nedostupnim za ostatak svijeta. Iste uvjete osigurava i VPN mreža; pouzdanost, vjerodostojnost i nekompromitiranost kako podataka tako i korisnika.

2.2. Razvoj

VPN nije prva tehnologija koja je pokušala kreirati privatni prostor na internetu. Do prije svega dvadeset godina najčešći način povezivanja udaljenih računala koristio je tzv. iznajmljene linije.

Iznajmljene linije poput ISDN (eng. Integrated Service Digital Network) i T1 su privatne veze koje telekomunikacijske kompanije mogu iznajmiti svojim korisnicima. One direktno i trajno spajaju dva čvora. Radi se o rezerviranoj vezi koja je u principu uvijek aktivna i spremna za korištenje. Ovim pristupom tvrtke imaju priliku geografski proširiti svoju privatnu mrežu u jednu Wide-Area mrežu (WAN). WAN mreža je širokog dosega i obično spaja više lokalnih mreža u jednu veliku pomoću fizičkih vodova. Međutim, ovaj pristup je poprilično skup, nepraktičan i nefleksibilan i danas se rijetko koristi.

1996. godine Microsoft je razvio PPTP (eng. Point-to-Point Tunneling Protocol) tunelirajući protokol koji se smatra prethodnikom moderne VPN tehnologije. Za PPTP se općenito može reći da stvara sigurnu vezu koristeći TCP kontrolni kanal i GRE (eng. Generic Encapsulation Tunnel) za enkapsulaciju PPP paketa. Danas ne postoji jedan definirani standard za postavljanje VPN tehnologije, već korisnik bira koje protokole i dodatne komponente želi koristiti. Kako je privatnost na internetu jedan od gorućih problema današnjice ne začuđuje da 1 od 4 korisnika upotrebljava neki oblik VPN-a.

2.3. Namjena

Najveću primjenu VPN mreža pronalazimo u velikim poslovnim poduzećima s geografski raširenom mrežom poslovnica i podružnica. Poslovnice međusobno komuniciraju, djelatnici na poslovnim putovanjima pristupaju tvrtkinim resursima itd. U tu svrhu mogu se, naravno, koristiti telefonski pozivi ili elektronička pošta, ali pozivi su skupi i neisplativi, a elektronička pošta se može lako kompromitirati na razne načine. Alternativno, relativno jeftino i efikasno rješenje je implementacija VPN mreže.

Zamislimo poslovnu organizaciju poput Coca Cole koja ima svoje podružnice diljem svijeta. Zaposlenici u zagrebačkoj podružnici imaju svoju privatnu mrežu unutar koje komuniciraju i imaju siguran protok podataka. Međutim, zaposlenici na poslovnim putovanjima moraju pristupiti povjerljivim podacima, a da se pri tome osiguraju isti uvjeti kao i unutar intraneta. VPN tehnologija omogućava upravo to, korisnici razmjenjuju podatke unutar kontroliranog i sigurnog mrežnog okruženja bez obzira na njihovu fizičku udaljenost. Osim putem podataka VPN omogućava i prijenos govora – VoIP (eng. Voice over IP) što je zgodno za inozemne pozive.

2.4. Osnovni koncept

Koristeći jednostavnu analogiju mogu se objasniti osnovni principi VPN tehnologije (u nastavku teksta samo VPN). Zamislimo da se nalazimo na otoku usred oceana okruženi s još tisuću otoka, neki bliži, neki udaljeniji od nas. Za putovanje do ostalih otoka koriste se katamarani koji su javno dostupni svima. Otok predstavlja jednu LAN mrežu, ocean je internet, a putovanje katamaranom je poput spajanja na Web server. Ne postoji kontrola nad vezama i ruterima kojim naš paket putuje. Nadalje, stanovnici otoka ne žele više koristiti javne katamarane, već grade mostove do željenih otoka kako bi putovali sigurnije. Mostovi predstavljaju korištenje iznajmljenih linija, što je praktično za spajanje bližih lokacija, no za udaljenije predstavlja veliki trošak. Gdje se u analogiji uklapa VPN? Kad bi svaki stanovnik imao vlastitu podmornicu (VPN) mogao bi brzo, jednostavno i neovisno putovati do bilo kojeg otoka. Iako bi se kretao oceanom (internetom) imao bi željenu privatnost i sigurnost i upravo je to glavna motivacija za implementaciju VPN mreže.

Analogiju po strani, osnovna ideja VPN-a je osigurati sigurni medij između dviju ili više privatnih mreža preko javne mreže poput Interneta. Virtualna veza između dvije krajnje točke ostvaruje se tuneliranjem pri čemu se provodi enkapsulacija i enkripcija podataka. Jednom kad podaci napuste lokalnu mrežu, na putu do odredišta, postaju dostupni svim potencijalnim uljezima koji ih mogu otuđiti ili izmijeniti, stoga su sigurnosni mehanizmi nužni za održavanje kvalitetnog tunela.

VPN predstavlja značajnu uštedu u odnosu na WAN mreže jer se može uspostaviti brzo i jeftino bilo gdje na svijetu. Korištenje interneta kao posrednika snosi i određene negativne posljedice. Ne postoji garancija konstante dostupnosti kanala pa u tome leži prednost iznajmljenih linija. Također, moguća su i kašnjenja i/ili gubitak paketa. Implementacija VPN-a ima smisla ako se poduzeće prostire na geografski velikom području, dok je za mala poduzeća ipak bolja opcija WAN mreža.

Tehnologije potrebne za ostvarenje VPN mreže se implementiraju ovisno o potrebama i preferencama korisnika, a najčešća su:

Programska rješenja koja se ostvaruju instaliranjem potrebnih aplikacija na klijentskoj i serverskoj strani. Ovo rješenje pogodno je za korisnike koji žele, putem mobilnih uređaja, pristupiti središnjoj mreži (npr. rad od kuće, poslovna putovanja...)

Sklopovska rješenja ostvaruju se ispravnom konfiguracijom mrežnih uređaja. Obično se koristi za trajno povezivanje više lokalnih mreža. [sve cis]

Kombinacija oba pristupa

U nastavku rada pružit će se implementacijski primjeri programskog i sklopovskog rješenja.

2.5. Zahtjevi

Zahtjevi [CIS – osnovi koncepti VPN tehnologije]

Područje okupacije pri razvoju tehnoloških rješenja za VPN stručnjake su definitivno povjerljivost, integritet, autentifikacija i autorizacija klijenata i sadržaja koji izmjenuju. Dva klijenta na udaljenim geografskim lokacijama žele biti sigurni da samo oni razumiju sadržaj poruke, odnosno da je u slučaju presretanja, poruka beskorisna svim potencijalnim uljezima. Nadalje, potrebno je sačuvati integritet poruke odnosno da sadržaj poruke, namjerno ili slučajno, nije moguće izmjeniti na putu od pošiljatelja do primatelja. Iz navedenog proizlaze zahtjevi koje VPN tehnologija mora zadovoljiti [CIS]:

Autentifikaciju korisnika - provjera identiteta korisnika

Upravljanje adresama – dodijeljivanje klijentskih adresa unutar privatnih mreža

Enkripcija

Upravljanje ključevima

Podrška različitim protokolima

2.6. Vrste rješenja

Topološki, VPN rješenja se mogu podijeliti na:

Intranet: koristi se za povezivanje više podružnica tvrtke s njenom središnjice. Komunikacija se ostvaruje uspostavom veze VPN poslužitelja preko Interneta. Riječ je o site-to-site konfiguraciji VPN mreže u kojoj se spajaju dvije udaljene LAN mreže.

Ekstranet: koristi se za povezivanje više različitih tvrtki koje žele dijeliti resurse i surađivati. Veza se ostvaruje spajanjem klijenta na udaljeni VPN poslužitelj.

Udaljeni pristup: model u kojem se pojedinačni korisnik spaja na privatnu mrežu. Koristi se klijentskim VPN programom i obično se radi o vanjskim suradnici, poslovnim putnicima, zaposlenicima koji rade na terenu itd.

Iz konfiguracijske perspektive moguće je podijeliti VPN rješenja:

client-to-server: najčešće se koristi kod udaljenog pristupa, tj. kada se klijent želi spojiti na privatnu mrežu

server-to-server: primjenjuje se kod intranet i ekstranet mreža, tj. kada se podružnice/tvrtke međusobno umrežuju.

2.7. Preduvjeti za ostvarenje VPN mreže

Kako je već rečeno VPN mrežu ne čini jedna jedinstvena tehnologija, već niz drugih samostalnih tehnologija koje su nužne za ostvarenje mreže. Najprisutniji i najkorišteniji su: vatrozidi, enkripcijski algoritimi, autentifikacijski protokoli i tunelirajući mehanizmi.

2.7.1 Vatrozid

Vatrozid (eng. firewall) je sigurnosni sustav koji prati ulazni i izlazni promet mreže. Postavlja se između sigurne, povjerljive mreže i druge nesigurne mreže poput interneta. Radi se o kombinaciji hardvera i softvera koji izolira privatnu mrežu od javne propuštajući određene pakete. Glavni cilj je osigurati da sav promet prolazi kroz vatrozid, a samo se autorizirani propušta. Vatrozid dijelimo u tri generacije: filtri paketa (eng. packet filters), filtri stanja (eng. stateful filters) i filtri aplikacijskoj sloja (eng. application gateways).

Prva generacija: filtri paketa [kurose/web]

Jedna tipična poslovna organizacija povezuje svoju internu mrežu preko izlaznog rutera (eng. gateway router) sa ostatkom interneta. Sav promet koji izlazi/ulazi u mrežu prolazi kroz izlazni ruter i upravo tu se događa filtriranje paketa. Analiziraju se IP datagrami paketa koji stižu na ruter na temelju niza predefiniranih pravila. Odluka o propuštanju paketa donosi se prema: izvorišnoj i odredišnoj IP adresi ili TCP/UDP porta, TCP bitova (SYN, ACK), ICMP poruke itd. Mrežni administrator određuje pravila i obično se radi o kombinaciji više njih npr. propušta se sav promet na portu 23 osim specifičnih IP adresa. Ako organizacija želi svojim zaposlenicima dopustiti spajanje na javnu mrežu, a onemogućiti vanjski pristup, filtiranje se može napraviti preko TCP ACK bita.[Kurose]Pravila za filtriranje paketa implementiraju se na željeni ruter preko ACL lista (eng. Access Control Liste), a mogu postojati različite liste za ulazni i izlazni promet. Filteri paketa djeluju samo na prva tri sloja OSI modela što znači da ne mogu znati sadržaj paketa koji pristiže u mrežu.

Druga generacija: inteligentni filtri paketa

Ako analiziramo svaki paket zasebno ne možemo znati pripada li određeni paket jednom TCP toku (eng. TCP stream). Ako proučimo primjer sa blokiranjem TCP ACK bita 1 može se lako zaključiti da se takvi paketi mogu zloupotrijebiti i iskoristit za napad na mrežu. Filteri stanja riješavaju taj problem prateći TCP veze od početka do kraja analizirajući faze trostrukog rukovanja (eng. three-way handshake). Filteri stanje koriste tablice u kojim su zapisane trenutno aktivne veze pa ih se može blokirati kad završe (detektira se TCP FIN paket) ili nakon nekog vremena. Ovakav pristup je napredniji jer se odluke o filitriranje ne donose samo na temelju pravila, već i temeljem povijesti pristiglih paketa.

Treća generacija: filtri aplikacijskog sloja

Prethodna riješenja mogu filtirati promet na temelju IP adresa, portova, TCP veza itd., no ne mogu prepoznati identitet pošiljatelja i primatelja jer operiraju na trećem sloju OSI modela. Filteri aplikacijskog sloja odlaze korak dalje i filtiraju promet prema podacima same aplikacije. Application gateway je specifičan proxy poslužitelj na kojem se provodi identifikacija korisnika. Sav promet prolazi kroz njega, a zatim kroz gateway ruter. Prednost treće generacije je i razumijevanje FTP, HTTP i DNS protokola pa paketi koji uspiješno prođu gateway ruter mogu biti odbačeni na application gateway-u jer dolaze od neautoriziranih korisnika. Međutim, za svaku aplikaciju potrebno je definirati drugi application gateway. Prolazak kroz gateway može biti i vremenski zahtjevno ako više korisnika koristi istu aplikaciju.

Danas se pretežno koriste hibridne verzije nekih od opisanih rješenja, a mogu biti implementirani sklopovski na nekom posebnom hardveru ili na nekom od operacijskih sustava (npr. Windows, Linux). Poznati komercijalni vatrozidi su Zone Alarm, Kerio Personal itd, a aplikacijskih gateway poslužitelji Squid, WinGate..

U osnovnom obliku vatrozid ima dva sučelja – unutarnje i vanjsko. Unutarnje je vezano za privatnu mrežu, a vanjsko za javnu. Postavlja se pitanje gdje je najbolje postaviti sigurnosni zid i kako poslagati arhitekturu naše mreže. S obzirom na centraliziranu prirodu vatrozida razlikujemo dvije varijacije: vatrozidi implementirani na mreži (eng. network-based) i vatrozidi implementirani na domaćinu (eng. host-based).

Implementacija na mreži [PMF]

Na gateway ruter implementira se jedno od prethodno opisanih rješenja. Ruter ne donosi odluku o propuštanje paketa na temelju sadražaja paketa, već na temelju predefiniranih parametara. Parametre postavlja mrežni administrator i može se dogoditi da ih često mora ažurirati i mijenjati. Ovakva arhitektura može poprimiti dva osnovna oblika: otvorena mreža s filtrima za neželjeni promet ili zatvorena mreža s filtrima za željni promet. Negativne strana ovakve implementacije je nepostajanje autentifikacije za korisnike .

Implementacija na domaćinu

Implementacija na domaćinu koristi mehanizam filtriranja paketa zajedno sa centralnim računalom (bastion-host). Centralno računalo ima svoj operativni sustav i primarna svrha mu je regulirati ulazni i izlazni promet mreže. Promet s javne mreže prolazi kroz gateway ruter i zatim odlazi na centralno računalo gdje se analizira prije propuštanja u ostatak privatne mreže. Dodavanje novih računala ili loše instalirani softveri unutar mreže ne utječu na rad centralnog računala. Međutim, centralizirani sustav predstavlja i veliku ranjivost sustava, u slučaju preuzimanja centralnog računala uljez dobiva kontrolu nad čitavom mrežom. Ovaj problem rješava se implementacijom demilitarizirane zone s dva vatrozida i jednim centralnim računalom. Postavlja se ruter između javne mreže i centralnog računala i zatim još jedan ruter između centralnog računala i lokalne mreže. Postavljanjem dva vatrozida, unutarnjeg i vanjskog vrši se dodatno razgraničenje između dvije mreže. U osnovi to znači da sav promet prolazi kroz kroz dvije faze. Klijenti na internetu komuniciraju samo s centralnim računalom koji dalje preusmjerava promet u unutarnju, a korisnici unutarnje mreže ne mogu vidjeti internet već mu pristupaju preko posrednika. Kao dodatna mjera zaštite unutarnje mreže koristi se NAT (eng. Network Addres Translation) i VPN servisi koji kriptiraju pakete. U slučaju napada na mrežu mrežni administrator može u potpunosti prekinuti komunikaciju vanjske i unutarnje mreže ili blokirati samo jednu od njih dvije.

VPN i vatrozidi

Iako VPN servisi ne implementiraju direktno vatrozide oni su integralni dio privatnih mreža i predstavljaju prvu crtu obrane. Ispravno konfiguriranje VPN servera sa vatrozidom neizostavni je dio postavljanja sigurne privatne mreže. Dva su osnovna pristupa u konfiguracija VPN servera i vatrozida:

VPN server spojen je na internet, a vatrozid se nalazi između VPN-a i intraneta

Vatrozid je spojen na internet, a VPN server se nalazi između vatrozida i intraneta

U prvom slučaju potrebno je dodati filtere paketa koji propuštaju samo IP adrese definirane VPN serverom. Ulazni promet se dekriptira na VPN serverima i zatim prolazi kroz vatrozid do intranet korisnika. U ovom scenariju vatrozid može blokirati pristup intranet resursima određenim VPN klijenitima s obzirom da su oni jedini koji imaju pristup privatnoj mreži. U drugom slučaju, češće korištenom, vatrozid dopušta stvaranje VPN tunela za ulazni i izlazni promet između VPN klijenta i servera. Mogu se implementirati i dodatni filteri za ostale filtere poput Web ili FTP servera.

2.6.2 Enkripcija podataka

Implementacija vatrozida je samo jedan dio VPN jednadžbe. Jednom propušteni podaci u mrežu zahtjevaju dodatnu razinu evaluacije kako ne bi namjerno ili slučajno nanijeli štetu privatnoj mreži. Kako potvrditi integritet pristigle poruke? Kako da budemo sigurni da je poruka stigla s izvora kojeg tvrdi da je? Na ta nam pitanje odgovara kriptografija.

Kriptografija je znanstvena disciplina koja proučava metode šifriranje poruka. Gotovo sve VPN tehnologije integriraju neki oblik enkripcije podataka. Osnovni zadatak kriptografije je zamaskirati poruku na način da je čitljiva samo osobi kojoj je namjenjena. Pošiljatelj i primatelj razmjenjuju poruke preko nesigurnog javnog kanala prilikom čega treća osoba može presresti, nadzirati ili izmjeniti sadržaj iste. Najsigurnija metoda bila bi privatizirati komunikacijski kanal, međutim to je jako skupo i neprakatično. Enkripcijske metode transformiraju sadržaj poruke, koji se u kripotografiji naziva čisti tekst (eng. plaintext) u kriptogram (eng. ciphertext) koristeći unaprijed dogovorene ključeve. Prilikom transformacije koriste se kriptografski algoritmi gdje se, općenito govoreći, radi se o matematičkim funkcijama, jednoj za šifriranje, a drugoj za dešifriranje. Algoritmi se najčešće dijele u tri osnovne kategorije: hash algoritmi, sustav privatnih ključeva i sustav javnih ključeva.

2.6.2.1 Hash algoritmi

Hash funkcija je svaka dobro definirana procedura ili matematička funkcija koja pretvara veliku količinu podataka u mali podatak.[CERT]Hash funkcija uzima ulaz m i transforimira ga u izlaz odnosno hash vrijednost H(m). Od hash funkcije se zahtjeva: brzina, ovisnost isključivo o ključu, ireverzibilnost, otpornost na kolizije i da za slične ulazne ključeve daje vrlo različite rezultate [Lenac]. Za dvije različite poruke m i n ne smiju se dobiti iste hash vrijednosti odnosno H(m)≠H(n) u svakom slučaju. Ovo svojstvo nam garantira da potencijalni presretač ne može zamijeniti originalnu poruku sa malicioznom iste hash vrijednosti. Primjerice, ako za ulaz uzmemo lozinku m =1234 i hash funkciju H(m)=(m\*π)/e za izlaz se dobiva hash vrijednost kojoj je teško pronaći početnu vrijednost m.

Poznatiji hash algoritmi su MD5 (Message Digests 5) i SHA-1 (Secure Hashing Algorithm).

MD5 algoritam uzima za ulaz podatak varijabline duljine kojeg kriptira u hash dužine 128 bitova. Ulazni podatak razdvaja u blokove po 512 bitova pri čemu se zadnji blok nadopunjava do dužine 512[CIS]. Algoritam zatim obrađuje svaki blok u 4 stupnja gdje svaki stupanj sadrži 16 operacija baziranih na različitim matematičkim funkcijama. MD5 se često koristi za provjeru integriteta, pri primitku poruke računa se njen MD5 hash i uspoređuje sa dobivenim pa ako su identični poruka je nepromijenjena.

SHA-1 algoritam, razvijen 90tih godina prošlog stoljeća od strane američke NSA (National Security Agency), jedan je od najpopularnijih kripto algoritama i koristi se u većini današnjih internetskih protokola. Smatra se nasljednikom MD5 algoritma koji također dolazi do hash vrijednosti kroz niz iteracija.

2.6.2.2 Sustav privatnih ključeva

Sustav privatnih ključeva ili simetrična kriptografija baziraju se na principu supstitucije jedne vrijednosti za drugu, čistog teksta za kriptogram. Najjednostavniji algoritam ove metode datira još iz razdoblja Cezara koji se njemu u čast naziva i Cezarova šifra. Cezar se često pri komunikaciji koristio šifrom koja je slova u tekstu zamijenjivala sa slovima udaljenim k mjesta u abecedi. Primjerice, za k = 3 slovo a zamijeni se slovom d (u engleskom alfabetu). Dobivena poruka izgledala bi nečitljivo iako je lako provaljiva s obzirom da imamo samo 26 mogućih vrijednosti varijable k. Varijabla k je ključ i definira način šifriranja poruke. Poboljšanja ove metode nalazimo u monoalfabetskim i polialfabetskim šifriranjima koji koriste različite ključeve za različita slova ili par ključeva u ponavljajućem uzorku. Za razliku od hash algoritama, ključevi su fiksnih veličina i transformiraju poruku varijabilne duljine koja se kasnije može povratiti u izvorno stanje koristeći ključ. U modernoj kriptografiji razmjena sadržaja temelji se na sustavu privatnih ključeva. Zamislimo komunikaciju između dvije osobe, pošiljatelja i primatelja, u kriptrografiji obično nazvani Alice i Bob koji komuniciraju preko nesigurnog kanala pri čemu treća osoba, Oscar može nadzirati njihov razgovor. Alice i Bob koriste standardizirani, javno objavljen i svima dostupan enkripcijski algoritam pa tako i Oscaru. Enkripcijski algoritam kao ulaz prima tajni ključ K\_A (string brojeva ili znakova) i čisti tekst m i kao izlaz šalje Bobu kripitiranu poruku K\_A (m). Po primitku poruke, Bob će morati iskoristi svoj ključ K\_B i dekripcijski algoritam K\_B (K\_A (m) ) ako bi dešifrirao poruku. U simetričnom sustavu oba ključa K\_A i K\_B su identični i tajni. [Kurose], stoga iako je Oscaru može biti poznat enkrpcijski algoritam, bez tajnog ključa sadržaj je beskoristan.

Najpoznatije enkripcijske metode koje koriste privatne ključeve su blok šifre (eng. Block Chipers) i ulančane blok šifre (eng. Cipher-Block Chaining).

Blok šifre koriste se u većini modernih internetskih protokola poput SSL-a i IPsec-a o kojima će biti više govora kasnije. Metoda blok šifra čisti tekst koji treba kriptirati dijeli u blokove po k bitova. Podijeljene blokove zatim kriptira zasebno koristeći varijacije privatnog ključa u obliku tablice šifrata. Primjerice, za k=3 poruka se razbija u dijelove po 3 bita što znači da postoji 2^3 (=8) mogućih ulaza, odnosno, za svaki od 8 mogućih ulaza postoji 8!(=40320) permutacija[Kurose]. Svaki ulaz ima definiran svoj izlaz u tablici šifrata pa ukoliko i Alice i Bob znaju ključ k mogu bez problema dešifirati poruku. Lako se primjećuje da za moderna računala procesuiranje 40320 permutacije i nije neki problem, međutim ako povećamo k=64 to bi značilo da bi obje strane trebale biti u mogućnosti pohraniti tablice veličine 2^64 što je poprilično nepraktično i nefikasno. Umjesto toga, ova metoda koristi funkcije koje simuliraju permutacijske tablice, a čije funkcioniranje izlazi iz okvira ovog rada. Danas postoje mnogi algoritmi koji koriste metode blok šifiranja, a najpoznatiji od njih su DES (Data Encryption Standard) i AES (Advanced Encryption Standrad). Primjerice, DES koristi 64-bitne blokove podataka sa 56-bitnim ključem. Alternativa blok šiframa su šifre tokova (eng. stream chipers) koje mogu kriptirati poruke varijabline duljine, za razliku od blok šifri koje moraju nadopunjavati bitove ukoliko blok nije potpun.

2.6.2.3 Sustav javnih ključeva

Sustav privatnih ključeva odlikuje jedna velika mana, naime za sigurnu komunikaciju nužna je tajnost ključa. Za razmjenu tajnog ključa pošiljatelj i primatelj moraju u nekom trenutku koristiti nesigurni kanal (poželjno je često mijenjati tajni ključ). Posjedovanje jednog identičnog tajnog ključa predstavlja sigurnosni problem. Pioniri sustava javnih ključeva smatraju se Whitfield Diffie i Martin Hellman koji su 1976. godine predstavili rješenje za problem razmjene ključeve.

Njihov protokol sastojao se od grupe G i generatora g [PMF]:

Alice generira slučajan prirodan broj a ∈ {1,2,,…│G|-1} i šalje Bobu element g^a

Bob generira slučajan prirodan broj b ∈ {1,2,,…│G|-1} i šalje Alice element g^b

Alice računa 〖(g^b)〗^a= g^ab

Bob računa 〖(g^a)〗^b= g^ab

Tajni ključ K=g^ab

Sustav javnog ključa zasniva se na ideji da je potrebno definirati funkciju f koju je lako izračunati, a f^(-1) teško. U tom slučaju funkcija za šifriranje e\_K bi mogla biti javno dostupna jer je iz nje teško ili praktički nemoguće izračunati funkciju za dešifiranje d\_K. Ako u danom primjeru uljez iz g i g^a može izračunati a (riješiti problem diskretnog logaritma), onda može izračunati i ostatak potrebnih varijabli. U konačnici to znači da svaki korisnik posjeduje jedan javni i jedan privatni ključ bez ikakve potrebe za razmjenom tajnih ključeva u čemu i leži njegova najveća prednost. Međutim, nedostak ovog sustava je u tome da je ranjivi na napade na odabrani tekst. Najkorišteniji i najpoznatiji algoritam ovog tipa je RSA nazvan prema svojim osnivateljima Ron Rivest-u, Adi Shamir-u i Leonardu Adleman-u.

RSA se zasniva na korištenju osnovnih matematičkih operacija, a posebice na korištenje operatora mod. RSA se sastoji od dva ključna dijela, prvi obuhvaća odabir javnog i privatnog ključa, a drugi enkripcijski i dekripcijski algoritam. Zamislimo ponovno da Alice i Bob komuniciraj, ovaj put koristeći RSA. Imajući na umu da je sadržaj svake poruke zapravo niz bitova koji su ekvivalentni nekom cijelom broju, RSA zapravo šifrira integere.

Za generiranje javnog i privatnog ključa Bob mora pratiti slijedeće korake [KUROSE]:

Odaberi dva prosta broja p i q, ne veća od 1024 bita.

Izračunaj n = pq i z = (p-1)(q-1)

Odaberi cijeli broj e, ne veći od n, koji nema zajedničkih faktora sa z. Vrijednost e će se koristiti u šifriranju

Pronađi cijeli broj d takav da je ed–1 dijeljivo sa z (bez ostataka). Drugim riječima biramo takav d da zadovoljava ed mod z=1

Bobov javni ključ K\_B^+ je par brojeva (n,e), a privatni K\_B^- je par brojeva (n,d)

Recimo da Alice šalje Bobu poruku ekvivalentnu cijelom broju m. Kriptirana poruka označena sa c koja se šalje Bobu jednaka je:

c= m^e mod

gdje su m i e par iz javnog ključa

Za dešifriranje pristigle poruke c Bob računa:

m=c^d mod n

gdje su d i n varijable iz privatnog ključa

Pouzdanost RSA leži u tome da ne postoji poznati algoritam za brzu i efikasnu faktorizaciju brojeva, odnosno u ovom slučaju, ne možemo iz poznatog broja n dovoljno brzo izračunati proste faktore p i q.

Javni ključevi obično se koriste u domeni digitalnih potpisa, dok su privatni ključevi svoju primjenu pronašli u komunikaciji.

VPN i enkripcija

Bez enkripcije teško možemo govoriti o VPN-u. Enkripcija prije svega osigurava integriteta poruka u tranzitu, stoga je ona ključni faktor u implementaciji sigurne virtualne mreže. Najčešće korišteni enkripcijski algoritmi u VPN-u su DES, SHA, RC2 i drugi. //Slijedeći ključni čimbenik u ostvarivanju sigurne komunikacije je autentifikacija korisnika.

2.7. VPN tehnologije

//još malo uvoda

Osnovni principi i metode enkripcije, autentifikacije, autorizacije i vatrozida objedinjeni su internetskim protokolima koji omogućavaju stvaranje virtualne veze (tunela) između dva udaljena mrežna entiteta. Tuneliranje je tehnika prijenosa enkapsuliranih podataka od jedne točke do druge preko trećeg, nepovezanog medija. Protokole koje implementiraju tehniku tuneliranja pronalazimo gotovo u svim slojevima OSI modela, a najpoznatiji su: GRE, IPSec, PPTP, SSL/TLS, PPTP, L2F, L2TP, OpenVPN itd.

2.7.1 SSL [Kurose]

1194. američka tvrtka razvija poboljšani, sigurniji TCP protokol; Secure Socket Layer. SSL je danas široko prihvaćen i korišten protokol baziran na razmjeni sigurnosnih parametara. U mrežnoj hijerarhiji nalazi se između aplikacijskog i transportnog sloja.

Njegovu primjenu pronalazimo u većini novčanih transakcija na internetu. Prilikom online kupnje od korisnika se traži unos osobnih podataka koji uključuju i broj kreditne kartice. Bez enkripcije uljez bi mogao presresti korisnikovu narudžbu i ukrasti osobne podatkem. Bez mehanizma za provjeru vjerodostojnosti podataka ne postoji garancija da je narudžba ispravna i nepromijenjena i u konačnici bez ikakve autentifikacije, korisnik nema garanciju da pristupa ispravnoj stranici. Navedene probleme rješava SSL protokol koji je u osnovi samo produžetak TCP-a. Općenito se može reći da se protokol sastoji od dva podprotokola jedan za uspostavu veze i jedan za razmjenu podataka. Tijekom uspostave veze postoje dvije faze, rukovanje i transformacija ključeva. Tijekom faze rukovanja klijent (Bob) uspostavlja TCP vezu sa serverom (Alice) i provjera komunicira li uistinu sa Alice, zatim šalje Alice kriptirani master ključ koji će obje strane iskoristiti u generiranju simetričnih ključeva za SSL sesiju. U fazi transformacije ključeva obje strane posjeduju master ključ iz kojeg se generiraju četiri različa ključa, dva ključa za enkripciju podataka EA i EB i dva ključa za provjeru ispravnosti podataka, MACA i MACB . Na posljetku, obje strane posjeduju četiri ista ključa i podaci se mogu poslati preko sigurne TCP veze. Poznato je da se podaci u TCP vezi šalju u jednom neprikinutom toku pa se postavlja pitanje u kojem trenutku provjeravati ispravnost istih. SSL rješava taj problem na način da podatke razbije na manje pakete koji se zajedno sa MAC ključem šifriraju i šalju drugoj strani koja ih ponovno dešifrira uz pomoć prethodno definiranog ključa. Veza se prekida u trenutku kada se u dešifriranom paketu pronađe TCP FIN oznaka.

1996. god. provodi se standardizacija SSL-a i kao rezultat se razvija poboljšani protokol TLS. Donešene promjene bile su minimalne, primjerice TLS uz sustav simetričnih ključeva mora koristiti i certifikate. SSL/TLS protokol se prvenstveno koristi u komercijalnim aplikacija poput eBaya i Amazona. Može se prepoznati ukoliko URL počinje sa https: umjesto http što označava da se HTTP protokol provodi preko SSL-a. Iako je 2015. prestala podrška, SSL3.0 idalje ostaje aktivan sudionik mrežnog prometa.

2.6.2. SSH [Computer Networks & CIS]

Jedan od pionira sigurnosnih protokola razvijen je 90-ih godina prošlog stoljeća na sveučilištu Helsinki u Finskoj kao zamjena za postojeće nesigurne protokole. SSH stvara kriptirani tunel između dva domaćina nakon njihove identifikacije.Vrši enkripciju i dekripciju na krajnjim točkama tunela pri čemu pretpostavlja ispravnost istih. Protokol se može koristiti za SSH tuneliranje ili uspostavu VPN mreže preko SSH veze s obzirom da osigurava tajnost, integritet podataka i autentičnost korisnika. Implementira se na aplikacijskom sloju i koristi se kao korisnički program što ga čini privlačnim i jednostavnim za široku uporabu jer je za razliku od ostalih protokola potrebna samo instalacija programa. Mehanizmi koje koristi su simetrična ili asimetrična enkripcija podataka i autentifikacija korisnika na serverskoj i klijentskoj strani uz korištenje digitalnih potpisa. Prvi korak u komunikaciji je uspostava SSL veze pri čemu se dogovaraju algoritmi za razmjenu ključeva i mehanizmi enkripcije, a među najčešće korištenim su simetrični AES, DES, 3DES i asimetrični DSA ili RSA te Diffie-Hellman za razmjenu ključeva. Idući korak je autentifikacija servera i korisnika najjčešće koristeći RSA sustav autentifikacije uključuje javne ključeve i certifikate. Naposljetku, obje strane generiraju ključeve i započinju SSL sesiju. Podaci se šalju u paketima ograničene veličine koji moraju sadržavati četiri bajta nasumice odabaranih podataka koji služe kao dodatna zaštita od eventualnih napada.

2.6.3 IPSec[Kurose i Computer Networks]

IPSec je najpoznatiji standardizirani sigurnosni protokol razvijen i sponzoriran od 1986. do 1991. godine od strane NSA. Implementiran je na mrežnom sloju OSI modela što tuneliranje čini automatskim bez prisustva korisnika. Dodatna prednost je što nema zasebnih konfiguracija aplikacija jer se šifriranje događa nezavisno na nižim raznima. Enkapsulira se sav sadržaj viših raznih OSI modela, što čini kompletan sadržaj paketa poput TCP/UDP segmenta ili sadržaja email-a nevidljivim. Pored enkripcije, IPSec osigurava mehanizme za autentifikaciju, očuvanje integriteta podataka i pouzdanosti čime se svrstao među najpopularnije protokole za kreiranje VPN-a. Kompletni IPSec paket osigurava razne sigurnosne usluge i algoritme koje korisnici biraju prema vlastitim preferencama i financijskim mogućnostima.

Protokol se u osnovi sastoji od dva prodprotokola: AH (eng. Authentication Header) i ESP (eng. Encapsulation Security Payload) protokola. AH protokol osigurava integritet podataka, autentifikaciju izvorišnog klijenta, ali ne i enkripciju podatka, dok ESP osigurava sve od navedenog pa je samim time i korišteniji. IPSec se može koristiti u dva oblika: transportnom (eng. transport mode) i tunelirajućem (eng. tunneling mode) načinu rada. U transportnom način IPSec zaglavlje se umeće između IPv4 i TCP zaglavlja paketa. IPSec zaglavlje u tom slučaju obično sadrži sigurnosne informacije poput SA (eng. Security Association) identifikatora i broja sekvence. U tunelirajućem obliku, pogodnim za VPN mreže, čitavi IP paket zajedno sa zaglavljem se enkapsulira u novi paket s potpuno novim zaglavljem.

Prije slanja IPSec paketa dva mrežna entiteta stvaraju vezu na mrežnom slojum tzv. sigurnosnu asocijaciju (eng. Security Associations) između dvije krajnje točke. SA je jednosmjerna odnosno ukoliko obje strane žele razmjenjivati podatke potrebno je stvoriti dvije SA veze. Informacije o vezama pohranjuju se na ruteru u posebnoj bazi SAD (eng. Security Association Database), a uključuju 32-bitni SA identifikator SPI (eng. Security Parameter Index), izvorišnu i odredišnu IP adresu, enkripcijski i autentifikacijski ključ i algoritam za provjeru integriteta podataka. Nakon uspostavljene veze izvorišni ruter pakira originalni IPv4 paket koristeći ESP protokol na slijedeći način: [kurose opet]

na kraj IPv4 paketa dodaje ESP polje

rezultat se kriptira koristeći ključ i algoritam specificiran SA-om

na početak kriptiranog paketa dodaje se ESP zaglavlje čime se dobiva tzv. enhilada

stvara se autentifikacijski MAC preko cijele enhilade

na kraj ehilade dodaje se stvoreni MAC čime se formira finalni paket

stvara se novo klasično IP zaglavlje koje se dodaje na finalni paket

Konačni IPSec paket je poboljšanja verzija IPv4 paketa koja putuje mrežom kao naizgled obični IP paket dok je zapravo čitav originalni IP paket zamaskiran uključujući i izvorišnu i odredišnu IP adresu, a adrese koje su vidljive su krajnje točke IPSec tunela. Jednom pristigli paket dešifrira se ponovno koristeći algoritme i ključeve definirane SA vezom kako bi se u konačnici ekstrahirao originalni vanilla IPv4 paket. Vidljivo je da IPSec obuhvaća enkapsulaciju podataka i stvaranje sigurno komunikacijskog kanala za prijenos tih podataka. Uspostavom SA veze i razmjenom ključeva i algoritama bavi se ISAKMP (eng. Internet Security Association and Key Management) model, a ključni protokol za razmjenu ključeve je IKE (eng. Internet Key Exchange). Prva faza IKE-a protokol sastoji se od razmjene ključeva i identifikacije entiteta, a u drugoj se uspostavljaju sesijski ključevi i SA veze.

Zaključno, IPSec je trenutno jedno od najboljih i najefikasniji rješenja sigurne host-to-host komunikacije za uspostavu VPN mreža.

2.6.4 L2TP [neki diplomski, CIS, WIKI, IBM]

L2TP je još jedan u nizu tunelirajućih protokola za razvoj VPN mreža. Nasljednik Microsoftovog PPTP protokola i Ciscovog L2F 2000.godine objedinio je njihove najbolje značajke. Implementiran je na podaktnovnom mrežnom sloju i u osnovi enkapsulira PPP okvire za slanje preko IP, X.25 ili ATM mreža. L2TP ne osigurava enkripcijske mehanizme, već se oslanja na podršku ostalih protokola poput IPSec-a.

U slučaju IP mreža, L2TP koristi UDP i nizove poruka za održavanje tunela, valja napomenuti da paketi ne moraju biti kriptirani. Razlikujemo dva načina tuneliranja: dobrovoljni i prisilni tunel [IBM], a razliku pronalazimo u krajnjoj točki. Krajnje točke tunela nazivaju se LAC (eng. L2TP Access Concentrator) i LNS (eng. L2TP Network Server). Kod dobrovoljnog načina, tunel završava kod klijenta, a sa prisilnim kod ISP-a (eng. Internet Service Provider).

Obavezno tuneliranje se provodi na slijedeći način [CIS:

Udaljeni korisnik inicira PPP (eng. Point-to-Point) vezu koju ISP prihvaća

ISP zahtjeva korisničko ime

U ISP-ovoj bazi korisničko ime je povezano sa LNS-om

LAC inicira L2TP tunel prema LNS-u

Ako LNS prihvati vezu, LAC enkapsulira PPP u L2TP i šalje pakate preko tunela

LNS prihvaća okvire, odvaja L2TP zaglavlja i obrađuje ih kao normalne PPP okvire

LNS koristi standardnu PPP autentifikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu

LNS zatim koristi standardnu PPP autentikaciju da bi utvrdio identitet korisnika i dodijelio mu IP adresu

Dobrovoljno:

Modemski korisnik uspostavi vezu sa svojim ISP-om

L2TP klijent (LAC) inicira L2TP tunel prema LNS-u

Ako LNS prihvati vezu, LAC enkapsulira PPP u L2TP i prosljeđuje podatke kroz tunel

LNS prihva ća okvire, odvaja iz njih L2TP zaglavlja i obrađuje ih kao normalne dolazne zahtjeve

L2TP razlikuje dvije vrste poruka kontrolne i podaktovne. Kontrolne se koriste prilikom uspostave, održavanja i zatvaranja tunela, a podaktovne sa enkapsulaciju PPP okvira koji se prenose kroz tunel. Autentifikacija se obično događa na strani ISP-a, a sve druge sigurnosne aspekte najbolje ga je koristiti u kombinaciji sa IPSec-om (L2TP/IPSec).

3. Sofverska implementacija

Danas na tržištu su dostupna razna softverska rješenja za podizanje VPN mreža koja variraju prema cijeni, performansama, kompleksnosti i sl. Softveri u svom programskom paketu dolaze s određenim enkripcijskim metodama, tunelirajućim protokolima i postavkama vatrozida čime znatno olakašavaju implementaciju VPN mreže koja je, još jednom, skup različitih tehnologija, a ne jedna jedinstvena. Najpoznatiji takvi softveri su NordVPN, strongSwan i OpenVPN koji dolaze u različitim paketima s različitim tehnologijama, al im je zajednička karakteristika da zadovoljavaju sve bitne zahtjeve VPN mreže. U moru VPN rješenja ističe se OpenVPN programski paket otvorenog koda koji se, iako poprilično mlad, pokazao kao jedan od najfleksiblnijih i najboljih besplatnih rješenja na tržištu.

3.1. OpenVPN (Cisco)

2002. godine James Yonan osmislio je komercijalni programski paket koji se nastavio razvijati u partnerskom udruženju s Francis Dinhaom u tvrtki OpenVPN Technologies Inc. Zahvaljujući višeplatformnost, visokom stupnju sigurnosti i politici otvorenog koda, ovaj protokol danas uživa veliku popularnost i nametnuo se kao prvi izbor u implementaciji VPN mreža.

OpenVPN protokoli omogućuju stvaranje point-to-point ili site-to-site veza u routing ili bridging konfiguraciji. Koristi SSL/TLS protokol za enkripciju podataka, sposoban je za rekonfiguraciju vatrozida ili NAT-a i omogućuje svojim korisnicima razne autentifikacijske tehnike.

Za korištenje OpenVPN-a potrebno je instalirati paket i na strani poslužitelja i na strani klijenta. Nakon instalacije konfigurira se svaka strana zasebno, a moguće je privremeno ili stalno korištenje. Neke od prednosti korištenja OpenVPN-a su: (ponovno CIS):

jednostavna instalacija i konfiguracija poslužiteljske i klijentske strane.

višeplatformnost – paket je moguće koristiti na raznim operacijskim sustavima (Linux distribucije, Windowsi, Mac itd.)

podaci se usmjeravaju na TCP/UDP 1194 port prema želji korisnika. TCP nudi pouzdanosti, a UDP fleksibilnost i jednostavnost.

koristi virtualna mrežna sučelja TUN ili TAP čime je u stanju prisiliti sve programe da mu proslijeđuju podatke. TUN sučelje je virtualna mrežnau kartica koje se često koristi za point-to-point komunikaciju, dok se TAP sučelje koristi za neke kompleksnije mrežne topologije.

pruža mogućnost prijenosa različitih tipova podataka

razni mehanizmi autentifikacije ovisno o preferencama korisnika

pokreće se u korisničkom prostoru, a ne u jezgri operacijskog sustava kao npr. IPSec.

Pokret otvorenog koda stvorio je veliku zajednicu korisnika koja kontinuirano sudjeluju na unaprijeđenju proizvoda i pomaže novim korisnicima. Također, dostupna je kompletna dokumentacija zajedno sa konfiguracijskim uputama i tehničkom podrškom.

3.1.2 Arhitektura OpenVPN-a

Enkripcija

Za enkripciju i autentifikaciju podataka i tunela koristi se OpenSSL enkripcijskom knjižnicom kojoj prepušta čitav posao. OpenSSL paket se temelji na SSLeay knjižnici a sastoji se od raznih komponenti:

SSL knjižnica za korištenje SSL/TLS protokola

Kripto knjižnica koja sadrži razne kriptografske algoritm (neki od njih opisani u x.y poglavlju):

Simetrične algoritme: DES, AES, IDEA...

Asimetrične algoritme: DSA, RSA, DH...

Hash funkcije: MD5, HMAC...

Osim OpenSSL, OpenVPN u konfiguraciji može koristiti i statički ključ. Tehnika korištenja statičkog ključa je jednostavnija za implementaciju i korištenje, ali i puno nesigurnija. Statički ključ je uvijek isti, a njegova distribucija se obično obavlja preko neisgurnog medija. U slučaju obnove potrebno je obavijestiti sve mrežne entitete. OpenVPN obično koristi 2048 bitni statički ključ kojeg generira pomoću Blowfish algoritma.

Autentifikacija

Postoji nekoliko načina autentifikacije korisnika: pre-shared ključevi, certifikati i autentifikacija korisničkim podacima. Korištenje ključeva je najjednostavniji način, a certifikata najkompleksniji i najrobusniji. U novijim verzijama omogućeno je korištenje raznih kombinacija.

Networking

OpenVPN koristi UDP ili TCP protokole transportnog sloja, točnije kreira SSL tunele na jednom TCP/UDP portu (uobičajeno 1194 port). Tehnički, to znači da je u konfiguraciji dovoljno podesitit Novije verzije (2.3.x nadalje) u potpunosti podržavaju i IPv6 protokole unutar tunela. Može se kreirati IP tunel na mrežnom sloju ili ethernet tunel na podatkovnom sloju, također pruža opciju stvaranja više tunela po procesu (u početku je funkcionirao na principu jedan tunel jedan proces). Opcionalno, može koristiti kompresijske algoritme (LZO kompresijska knjižnica).

4. Hardverska implementacija