STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**VPN**

ročníkový projekt

**Jakub Žák**

**II.D**

2024

Obsah

Obsah 2

Anotácia 3

1 VPN 4

1.1 Princíp a funkcia VPN 4

1.1.1 Účel a funkcie VPN 5

1.1.2 Bezpečnostné aspekty a súkromie v súvislosti s VPN 6

1.1.3 Bezpečnosť VPN 6

1.1.4 Princíp šifrovacieho tunela vo VPN 7

2 Záver 9

Zoznam použitej literatúry 10

Anotácia

**Annotation**

1. VPN

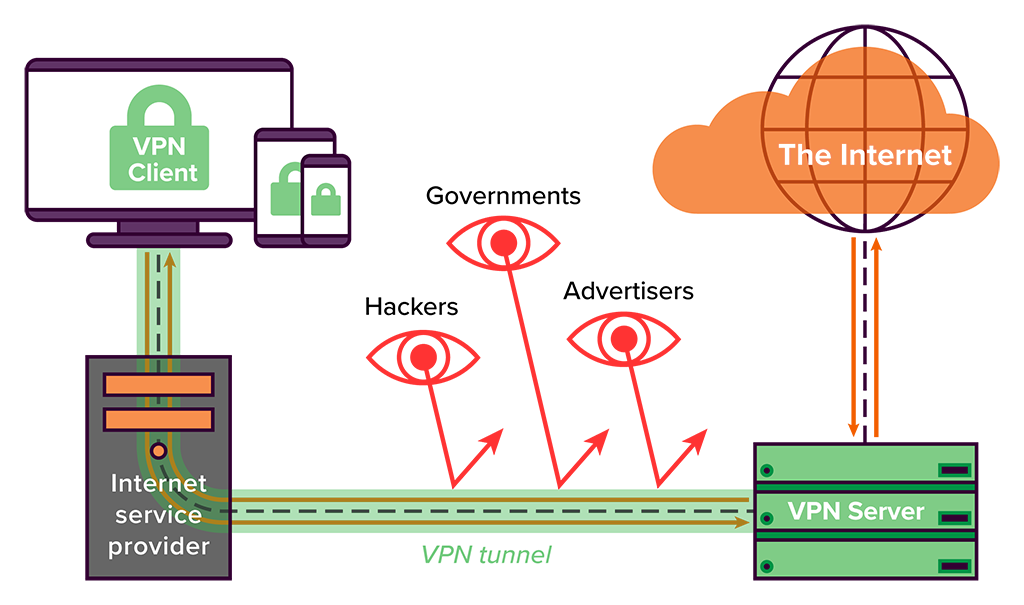
VPN je skratka pre „virtuálnu súkromnú sieť“. Je to služba, ktorá vám poskytuje bezpečný a súkromný prístup na internet. Šifrovaním vášho pripojenia VPN skryje vašu IP a online aktivitu pred špionážnymi očami a ochráni vaše údaje pred kyberzločincami.

* 1. Princíp a funkcia VPN

Sieť VPN funguje tak, že internetové pripojenie zariadenia smeruje cez súkromnú službu a nie cez bežného poskytovateľa internetových služieb (ISP) používateľa. VPN funguje ako sprostredkovateľ medzi tým, že sa používateľ dostane online a pripojí sa na internet skrytím svojej IP adresy.

Pomocou VPN sa vytvorí súkromný, šifrovaný tunel, cez ktorý môže zariadenie používateľa pristupovať na internet a zároveň skryť svoje osobné informácie, polohu a ďalšie údaje. Všetka sieťová prevádzka sa odosiela cez zabezpečené pripojenie cez VPN. To znamená, že všetky údaje prenášané na internet sú presmerované do siete VPN a nie z počítača používateľa.

Keď sa používateľ pripojí na web pomocou svojej siete VPN, jeho počítač odošle informácie webovým stránkam prostredníctvom šifrovaného pripojenia vytvoreného sieťou VPN. VPN potom prepošle túto požiadavku a odošle odpoveď z požadovanej webovej stránky späť do pripojenia.



Obr. 1 Zjednodušený VPN diagram

* + 1. Účel a funkcie VPN

Namiesto odosielania vášho internetového prenosu (vyhľadávania, navštívené stránky, nahrávanie, sťahovanie) priamo vášmu poskytovateľovi internetových služieb (ISP), VPN najprv nasmeruje váš prenos cez server VPN. Týmto spôsobom, keď sa vaše údaje konečne prenesú na internet, zdá sa, že pochádzajú zo servera VPN, nie z vášho osobného zariadenia.

Bez VPN je vaša IP adresa – špeciálne číslo jedinečné pre vašu sieť – viditeľná pre web. Sieť VPN maskuje vašu IP adresu tým, že pôsobí ako sprostredkovateľ a presmeruje vašu komunikáciu. Pridáva tiež šifrovanie alebo tunel okolo vašej identity, keď sa pripájate. Kombinácia servera VPN a šifrovacieho tunela blokuje vášho poskytovateľa internetových služieb, vlády, hackerov a kohokoľvek iného, ​​aby vás pri navigácii na webe špehovali.

Akú máte IP adresu? Správny druh môže znamenať rozdiel, pokiaľ ide o online bezpečnosť. Naučte sa detaily svojej IP adresy pomocou našich sprievodcov pre verejné a súkromné ​​adresy IP a statické a dynamické adresy IP.



Obr. 2 Vpn na celom svete

* + 1. Bezpečnostné aspekty a súkromie v súvislosti s VPN

Sieť VPN šifruje vašu komunikáciu a skryje vašu IP adresu. Vďaka tomu skryje aj vašu polohu, históriu prehliadania, vyhľadávania, sťahovanie a akékoľvek ďalšie aktivity, ako je hranie alebo streamovanie. Sieť VPN skrýva tieto informácie pred zlými hercami, poskytovateľmi internetových služieb, webovými stránkami a dokonca aj utláčajúcimi vládami.

IP adresa: VPN skryje vašu skutočnú IP adresu a nahradí ju IP adresou servera VPN, ku ktorému ste pripojení. To bráni ostatným sledovať vašu online aktivitu späť k vašej skutočnej polohe alebo identite.

Poloha: Zamaskovaním vašej IP adresy VPN skryje aj vašu fyzickú polohu. Aj keď sa webové stránky alebo aplikácie pokúšajú sledovať vašu polohu inými spôsobmi, ako je GPS, VPN im bráni presne určiť, kde sa nachádzate.

História a aktivita prehliadania: VPN šifruje váš internetový prenos, vďaka čomu je nečitateľný pre každého, kto sa ho pokúša zachytiť. To zaisťuje, že vaša história prehliadania, vyhľadávania, sťahovanie a ďalšie online aktivity zostanú súkromné ​​a bezpečné.

Ochrana osobných údajov: Keď používate sieť VPN, všetky údaje prenášané medzi vaším zariadením a internetom sú šifrované. To chráni citlivé informácie, ako sú prihlasovacie údaje, heslá a osobné údaje, pred zachytením hackermi alebo škodlivými subjektmi.

Prevencia obmedzovania šírky pásma: Niektorí poskytovatelia internetových služieb obmedzujú internetové pripojenia na základe typu online aktivity, ako je streamovanie videí alebo hranie hier. Sieť VPN skryje vašu online aktivitu pred poskytovateľom internetových služieb, čím im bráni obmedziť vaše pripojenie a zabezpečiť konzistentné rýchlosti.

* + 1. Bezpečnosť VPN

Odosielanie údajov na server tretej strany sa môže zdať strašidelné, najmä ak ste to nikdy predtým neurobili. Ako zistíte, či poskytovateľ plní svoje sľuby? Aká bezpečná je VPN?

Aj keď to môže znieť ako niečo, čo by ste našli na dark webe, technológia VPN je úplne legálna, bezpečná a prístupná každému, kto by mohol chcieť chrániť svoje údaje. Organizácie používajú VPN na pridanie ďalšej vrstvy súkromia do svojej siete, zatiaľ čo jednotliví používatelia ju môžu použiť, aby zabránili podvodníkom ukradnúť ich informácie, najmä cez verejnú sieť Wi-Fi. S nárastom krádeží identity a iných foriem počítačovej kriminality nie je táto ďalšia vrstva len príjemným bonusom – je nevyhnutná na udržanie ochrany.

VPN služby a poskytovatelia

VPN služby a poskytovatelia sú dôležitým aspektom pre tých, ktorí hľadajú spoľahlivý a bezpečný spôsob, ako využívať VPN technológiu. Existuje mnoho komerčných VPN služieb, ktoré ponúkajú rôzne funkcie a cenové modely pre jednotlivcov aj pre firmy. Tieto služby často zahŕňajú rôzne servery umiestnené po celom svete, rôzne protokoly, možnosť použitia na rôznych zariadeniach a rôzne úrovne šifrovania a anonymizácie. Okrem toho existujú aj firemné VPN riešenia, ktoré sú navrhnuté pre špecifické potreby podnikových používateľov a často zahŕňajú možnosti ako riadenie prístupu, monitorovanie aktivít a rozšírené bezpečnostné funkcie. Pri výbere VPN služby alebo poskytovateľa je dôležité zvážiť niekoľko faktorov, vrátane úrovne bezpečnosti, dostupnosti serverov, rýchlosti pripojenia, ceny a zákazníckej podpory, aby ste našli najvhodnejšie riešenie pre vaše potreby.



Obr. 3 Vpn zabezpečenie

* + 1. Princíp šifrovacieho tunela vo VPN

Tunel VPN je bezpečné, šifrované spojenie medzi zariadením používateľa a internetom prostredníctvom virtuálnej súkromnej siete.

Tunel VPN šifruje internetový prenos používateľa a smeruje ho na vzdialený server VPN. Odtiaľ sú údaje dešifrované a doručené na určené miesto.

Šifrované pripojenie umožňuje bezpečnú, súkromnú cestu pre internetový prenos používateľa. V dôsledku toho zostávajú online aktivity používateľa skryté pred zvedavými očami a kybernetickými hrozbami. Tunel VPN tiež pomáha zabezpečiť dôvernosť, integritu a autentickosť všetkých údajov pri ich prenose cez verejné siete.

Tunelovanie VPN vytvára bezpečné a šifrované spojenie medzi zariadením používateľa a vzdialeným serverom VPN.

Pozrime sa, ako funguje proces tunelovania VPN:

Krok 1: Používateľ získa službu VPN a pripojí sa k požadovanému serveru prostredníctvom svojho zariadenia.

Krok 2: Klient alebo aplikácia VPN vytvorí šifrovaný tunel pre internetový prenos používateľa. Odtiaľ je prevádzka smerovaná na vzdialený server VPN cez internetové pripojenie používateľa.

Krok 3: Údaje, ktoré prechádzajú tunelom VPN, sú šifrované pomocou protokolu. Týmto spôsobom nikto nemôže zachytiť alebo získať prístup k údajom. Údaje sú tiež transformované do „šifrovaného textu“, vďaka čomu sú nečitateľné.

Krok 4: Vzdialený server VPN prijíma a dešifruje šifrovaný prenos, čo umožňuje, aby internetová prevádzka používateľa prešla do zamýšľaného cieľa. Klient a server VPN používajú na dešifrovanie údajov kľúče alebo reťazec čísel.

Krok 5: Údaje používateľa sú smerované späť zo šifrovaného tunela do jeho zariadenia, ku ktorému majú pristupovať.

Väčšina sietí VPN má prepínač zabíjania, ktorý odpojí internetové pripojenie používateľa od tunela VPN. Táto funkcia zabraňuje tomu, aby bola IP adresa používateľa pri prerušení spojenia odhalená tretím stranám.

Bez prepínača zabíjania by sa zariadenie používateľa automaticky vrátilo k svojmu bežnému internetovému pripojeniu, čím by potenciálne odhalilo svoje online aktivity poskytovateľovi internetových služieb alebo iným zvedavým očiam. Ak sa používateľ zúčastňuje citlivých online aktivít (napr. online bankovníctvo), nemusí byť schopný zabezpečiť svoje dôverné informácie.

1. Záver

Zoznam použitej literatúry