CTI Jelentés

A VPN működése és alkalmazása a modern internetes környezetben

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996

Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

A virtuális magán hálózatok (Virtual Private Network - VPN) rendkívül fontos eszközei a mai informatikai életnek. Ez igaz a vállalati szektorra és a magáncélú felhasználásra is. Éppen ezért rengeteg reklám kering az interneten, amelyek különféle VPN szolgáltatásokat hirdetnek, ezért biztosan sok olvasónk ismeri már a kifejezést.

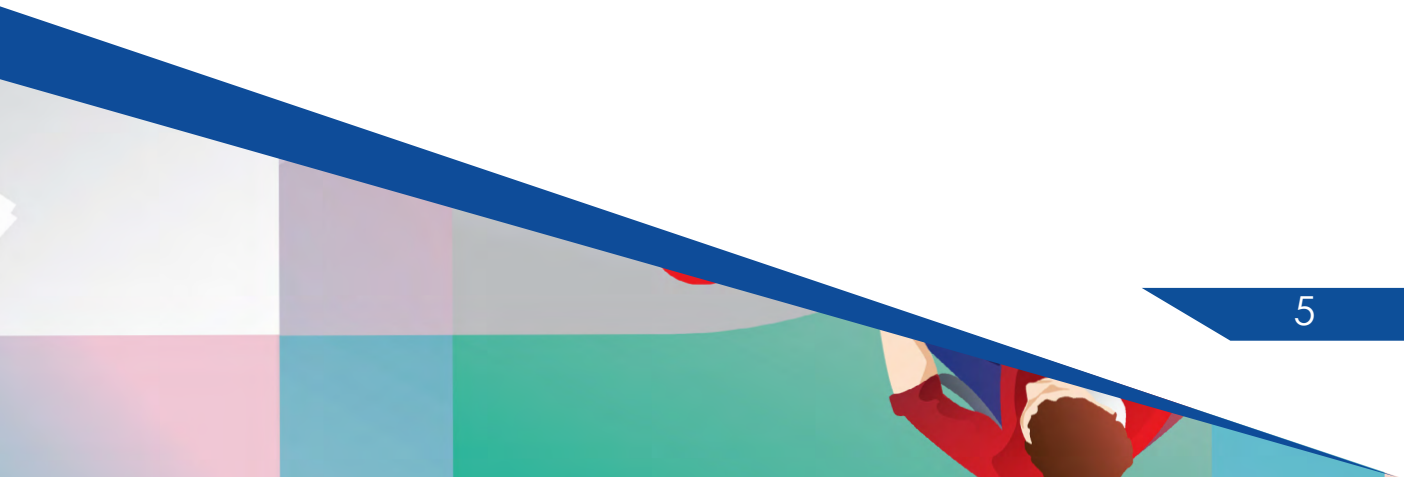
De mi az a VPN? Hogyan működik, és mire jó? Minden esetben nagyobb biztonságot tudunk vele elérni, vagy vannak helyzetek, amikor célszerű kerülni őket? Szükségünk van egyáltalán rá? Ez ugyan az, mint a proxy? Jelen kiadványunk célja a virtuális magán hálózatok működésének bemutatása, és az előzőekben feltett kérdések megválaszolása.

A kiadvány átfogó képet ad a VPN-ek biztonsági kockázatairól is, így reméljük, hogy az elolvasása után mindenki tudatos döntést tud hozni azzal kapcsolatban, hogy van-e szüksége rá, és ha igen, akkor hogyan alkalmazza azokat.

Mi az a VPN?

A VPN a „**virtuális magánhálózat**" rövidítése. Ez a technológia lehetőséget ad egy védett hálózati kapcsolat létrehozására nyilvános hálózatokon keresztül. A VPN-ek valós időben titkosítják az internetes forgalmat, és igyekeznek elrejteni az online identitást. Ezáltal a harmadik felek számára megnehezül az online tevékenységek nyomon követése, és szinte ellehetetlenül az adatlopás.

Ezt lényegében nagyon leegyszerűsítve úgy lehet elképzelni, mintha ugyanabba a routerbe vagy switch-be lennének bekötve a VPN-t használó eszközök, így képesek a hálózat minden előnyét kihasználni úgy, hogy valójában az adatforgalmuk a nyílt interneten keresztül folyik. Láthatják egymást, fileokat tudnak egymással megosztani, kommunikálni tudnak. Amennyiben a munkahelyünkön engedélyezett a home office, úgy a legtöbb esetben - bár léteznek más megoldások is - VPN-nel valósítják meg a munkahelyi környezet és hálózati elérést.



Magáncélú felhasználásnál azonban a legtöbbször egy másféle szolgáltatásról beszélhetünk. Hogyha egy VPN szolgáltató hálózatához kapcsolódunk, akkor ezen a hálózaton különféle előnyöket élvezhetünk. Ilyenek például, hogy megkerülhetünk geolokációs korlátozásokat, cenzúrákat, illetve a weblapok, szerverek elől rejtve marad a privát IP címünk, ezáltal valamelyest a valódi identitásunk anonimizálva van.

Ennek a működéséről egy későbbi fejezetben részletesebben beszámolunk.

A VPN története

Az 1990-es évek elején a HTTP megjelenése lehetővé tette az átlag felhasználók számára, hogy könnyedén böngésszék az internetet hyperlinkeken keresztül. Ekkor kezdett népszerűsödni a „world wide web", és ezzel együtt növekedni kezdett az igény a biztonságos és privát online kommunikációra. Így született meg az IP-layer titkosítás, amely valamelyest a VPN-ek előfutára volt.

Pár évvel később az AT&T Bell laboratórium bemutatta a SwIPe-ot, ami megmutatta, mire képes az IP-layer titkosítás. Ez az innováció nagy befolyással volt a még ma is használatos IPsec-re. Az IPsec-et az 1990-es évek közepén mutatták be, és end-to-end biztonságot nyújtott végpontok között, úgy, hogy az adatforgalom minden egyes IP csomagját titkosította.

Az évtized végén a Microsoft bemutatta a Point-to-Point Tunneling Protocolt (PPTP). A PPTP jelentős előrelépés volt a VPN technológiák fejlődésében, ugyanis az már PPP csomagokat enkapszulált, és virtual data tunnel-eket (virtuális adat alagutakat) hozott létre a végpontok között – csak úgy, mint a mai VPN-ek. Röviddel ezután a Cisco bemutatta az L2F protokollt, ami a PPTP hiányosságait kezelte úgy, hogy többféle internetes forgalmat is támogatott és fejlettebb titkosítási módszereket használt.

A 2000-es évek elején változás történt, ugyanis az internet a magánélet, de főleg az üzleti élet központi elemévé lépett elő. A nagy tőkékkel működő cégek motiválták a szoftvermérnököket, hogy minél újabb, korszerűbb és megbízhatóbb megoldásokat hozzanak létre az internetes biztonság tekintetében, ezért ebben az időszakban több, ma is használt VPN protokoll született meg, úgy, mint az OpenVPN, vagy az SSL VPN.

Internet *VPN* *Az Ön eszköze*

A VPN alapjai

Hogyan működik az internet?

Ahhoz, hogy megértsük hogyan működnek a VPN-ek, először valamelyest tisztáznunk kell a hálózatok, és tágabb értelemben véve az internet működését.

Az internetet úgy lehet elképzelni, mint egy hatalmas vezetéket, amihez csatlakozik minden rajta kommunikáló eszköz . Egyes eszközök közvetlenül a „vezetékhez" vannak csatolva, más eszközöknek pedig egy hosszabb utat kell bejárniuk ahhoz, hogy az interneten kommunikálni tudjanak. Az internet szolgáltatók (ISP) szerverei például közvetlenül az internethez csatlakoznak.

Hogyha egy személyi számítógépről, vagy okoseszközről szeretnénk egy üzenetet küldeni valakinek, vagy meg szeretnénk nyitni egy weblapot, akkor az eszközünknek először rá kell kapcsolódnia az internetre. Ez az internet szolgáltató szerverein keresztül tud megtörténni. Minden információ, ami áthalad az interneten, lebontásra kerül, és csomagokká (packets) alakul. Az elküldött csomagok az úton „gócpontok", a routerek segítségével kerülnek először az internet szolgáltatóhoz, majd ők küldik tovább az internetre, ahol egy hosszú út, és még több router után elérnek a célállomásukhoz. Ott a packetek előre meghatározott szabványok alapján újra összeépítésre kerülnek, és így érkezik meg sértetlenül az adat.

Routing

De honnan tudják az ISP szerverek, és a routerek hogy merre kell tovább küldeni ezeket az adatokat? Minden eszköz, ami az internetre csatlakozik, rendelkezik egy egyedi azonosító számmal. **Ez az IP cím**. Az IP cím belekerül minden elküldött csomagba, mintha egy borítékra ráírt cím lenne. Ez a cím alapján mindenki, aki a kommunikációban részt vesz tudja, hogy merre kell tovább küldenie az adott csomagot.

Fontos megjegyezni, hogy a kommunikáció során elküldött csomagok nem feltétlenül kell, hogy ugyan azt az utat járják be az interneten, sőt, még az sem szükséges, hogy a megfelelő sorrendben érkezzenek be a „célállomásra".

Mivel minden gócpont látja a címzettet, dinamikusan el tudja dönteni, melyik útvonal a legoptimálisabb, a legkevésbé leterhelt abban az adott pillanatban, és arra tudja tovább küldeni a csomagokat. A sorrendbeli összeállításért pedig a korábban említett szabványok, az internet protokollok a felelősek. Az ISP az egész folyamatot látja, és lejegyezheti, logolhatja. Hogyha egy adott weblap HTTPS előtaggal elérhető, akkor miután az eszközünk felvette a szolgáltatással a kapcsolatot, egy úgynevezett kulcspárt cserél, amivel titkosításra kerülnek az elküldött csomagok.

Ettől a ponttól kezdve a csomagok pontos tartalmát már csak mi tudjuk megérteni, azonban a cél és forrás közti kommunikáció a feljegyzett IP címek miatt minden „külső szemlélő" számára publikus.

Ha egy weblap nem titkosított, akkor a csomagok tartalma is értelmezhető bárki számára, aki hálózati forgalmat figyel. Éppen ezért nem javasoljuk például a nyílt WI-FI-k használatát, ezek forgalmát ugyanis nem tudjuk ki figyelheti.

TUDTAD?

Hogyan működnek a VPN-ek szolgáltatásként?

A VPN-ek, azaz a virtuális magán hálózatok szolgáltatás formájában az interneten keresztül érhetők el. A packetek elküldésének menetét közbeékelődve megbonyolítják, így téve a kommunikációt biztonságosabbá. De hogyan is történik ez? Térjünk vissza az előző példánkhoz azzal a különbséggel, hogy most VPN szolgáltatást is használunk!

Az üzenetünk ugyan úgy, ahogy eddig, packetekre bomlik szét, aminek feladó és címzett IP címe is van, azonban az eszközünkről távozó csomagok már titkosítva érkeznek a routerhez, amelyet az eszközön telepített VPN kliens végez el. Ez azt is jelenti többek között, hogy VPN használata közben jelentősen csökken a nyílt wi-fi hálózatok használatának veszélye. Az üzenet tovább utazik az ISP-hez, aki a csomagok tartalmát már nem tudja értelmezni.

Innentől kezdve a packetek a VPN saját szerverére, a saját hálózatára kerülnek. A VPN szerver megváltoztatja a forrás IP címét (a mi eszközünket) a saját IP címére, és így halad tovább az útján az adat.

Ez azt jelenti, hogy amikor egy szerver, vagy tűzfal a csomagjaink útjába kerül, azok azt fogják hinni, hogy a valódi feladó a VPN szerver. Később, ha a cél válaszolni szeretne, szintén a VPN-nel fog egyenes úton kommunikálni, a VPN belső hálózata pedig tudni fogja, hogy a neki küldött adatot mi kértük, ezért tovább küldi számunkra. A titkosítás akkor kerül visszafejtésre, amikor a packetek az út végére érnek, és elhagyják a VPN hálózatot. Így végülis egy elszigetelődés alakul ki a célpont, és köztünk, ugyanis közbeékelődik a VPN hálózat. Mi közvetlenül csak a VPN szolgáltatóval kommunikálunk, és a célpontunk is.

Egy jelentős különbség továbbá, hogy a VPN-szolgáltatók állításuk szerint **nem tárolnak adatokat** a rajtuk keresztülhaladó kommunikációról, és az esetlegesen rögzített információkat **nem osztják meg harmadik felekkel**. Mivel az adatok végponttól – végpontig titkosítva vannak, úgy is el lehet képzelni a VPN-en keresztül futó adatfolyamot, mintha egy átjáró lenne, egy biztonságos cső a két végpont között, amibe senki sem lát be. Ezt hívják angol szakszóval **tunneling**-nek.

Ennek köszönhetően lehetséges például a zóna tiltások feloldása is. Néhány ország politikai, vagy gazdasági okokból tilthatja bizonyos típusú tartalmak vagy weboldalak megjelenítését. Hasonlóképpen néhány szolgáltatás megtagadhatja a használatot lokációtól függően. Ebben segítséget nyújthat a VPN szolgáltatások igénybevétele, amelyeknek általában több városban és országban található szervere, amire csatlakozni lehet, és ezzel bármilyen külső szemlélőt megtéveszthetünk a valós geolokációnkról.

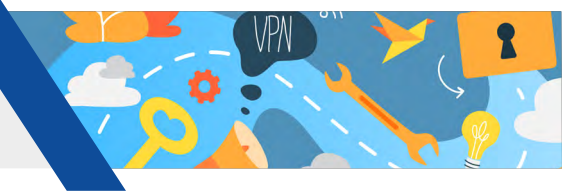
VPN-ek típusai

Site-to-Site

A korábban bemutatott felhasználási módnál a VPN technológia azonban sokkal többre is képes. Például hatalmas segítség lehet egy cégen belüli több telephely számára, amelyek ugyanazokat a közös rendszereket használják. Az úgynevezett Site-to-Site VPN típussal a két helyszín helyi hálózatát „össze lehet olvasztani”. Ebben az esetben effektíve megszűnik a távolság a két létesítmény között, és úgy tudnak üzemelni, mintha minden számítógép egy helyi hálózat lenne.

Ez technikailag megvalósítható az IPsec protokoll segítségével akár hardware-es VPN végpontok használatával, vagy szoftveres eszközök telepítésével és konfigurálásával. Természetesen itt is igaz, hogy a két végpont között egy titkosított tunnel keletkezik, és egy külső fél számára így megismerhetetlen a két végpont közötti kommunikáció tartalma.

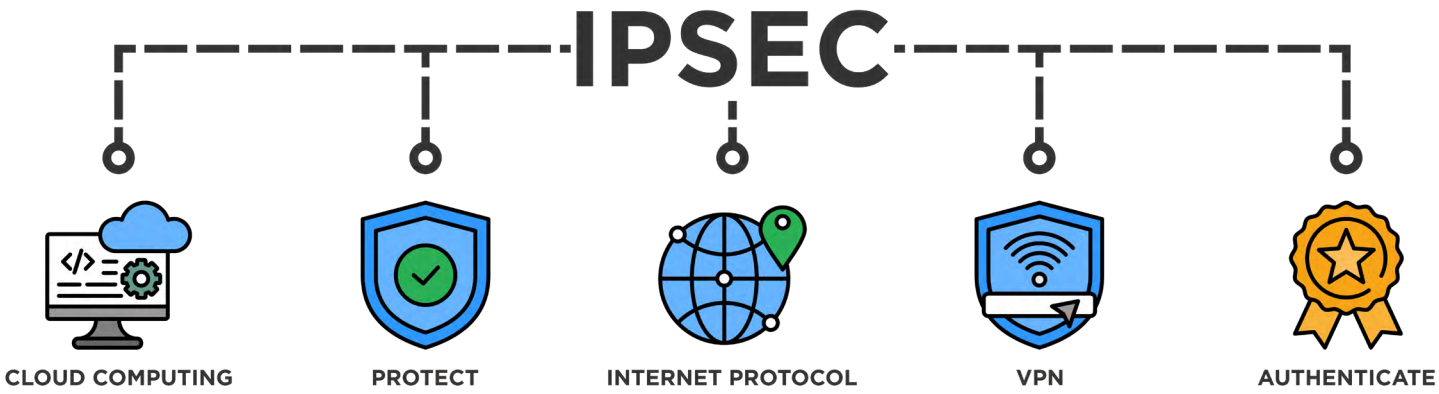
Remote Access



A VPN technológia egy másik gyakori felhasználási módja vállalatok esetében a távoli hozzáférés biztosítása. Ezzel könnyen megvalósítható a munkavállalók otthonról történő munkavégzése. A Site-to-Site megoldáshoz képest a különbség az, hogy ebben az esetben nem két nagy hálózatot kötnek össze virtuálisan, hanem a munkavállaló számítógépét csatolják be a céges hálózatba. Így elérést biztosíthatnak számára a belső rendszerekhez. Az ilyen kapcsolatok egyik jellemzője, hogy a vállalat láthatja az internetes az alkalmazottak forgalmát, ellenőrizheti hogy munkaidőben valóban a munkával foglalkoznak-e, vagy esetleg más internetes tevékenységet végeznek közben.

Ezen felül a VPN-t szolgáltató cég letilthat bizonyos kapcsolatokat, amíg a felhasználó a hálózat része. Így elképzelhető, hogy bizonyos weboldalak nem megnyithatók, néhány internetet igénylő program nem működik megfelelően. Ezzel ideiglenesen sérül bizonyos szolgáltatások elérhetősége.

A remote access VPN megvalósítható az IPsec, SSL/TLS protokollokkal. Lehetőség van böngészőn keresztüli VPN kapcsolat létrehozására, ez azonban kisebb interakcióra ad lehetőséget, mint egy tényleges dedikált kliens használata.



Hardware VPN

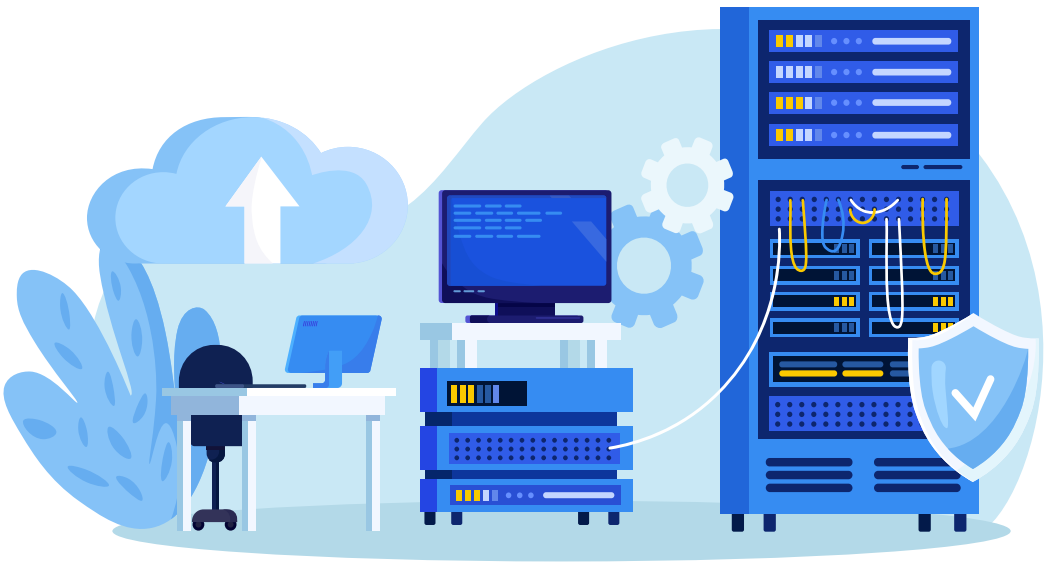
Hardware VPN alkalmazásánál a titkosított tunnel létrehozását, és a routingot, azaz a packetek megfelelő helyre való eljuttatását egy külön erre a célra dedikált fizikai eszköz végzi. Ez leginkább a nagyvállalatok számára ideális megoldás. Előnye, hogy általánosságba véve nagyobb biztonságot adnak, bonyolultabb titkosítási eljárásokat alkalmaznak, mindezt úgy, hogy a sebességük, és a forgalom áteresztő képességük is nagyobb. Ez azért lehetséges, mert a titkosítási eljárásokat az eszköz dedikált komponensei végzik. Így a rendelkezésre állás zavartalanabb lehet, és több szimultán kapcsolat létrehozása válik lehetségessé.

Mindezeken felül a különböző eszközök és operációs rendszerek közti kommunikációt is egységesíti. Hátrányuk viszont, hogy a beüzemelésük bonyolultabb, nehezebben skálázhatók, és drágábbak is szoftveres társaiknál.

Mindezeken felül a különböző eszközök és operációs rendszerek közti kommunikációt is egységesíti.

A nagy teljesítményű hardveres VPN-ek képesek több száz vagy akár több ezer egyidejű kapcsolatot kezelni. Könnyen integrálhatók meglévő hálózati infrastruktúrába, például külön alhálózatok vagy VLAN-ok támogatásával. Ezt a rendszert teljes mértékben a vállalat felügyeli, így nincs szükség a külső szolgáltatók által végzett adatkezelésre, ami fontos lehet az adatvédelem szempontjából.

Hátrányuk viszont, hogy a beüzemelésük bonyolultabb és drágábbak is szoftveres társaiknál. Kiesés esetén teljes szolgáltatásleállás lehetséges valamint kevésbé rugalmasak a frissítések terén a szükséges új eszközbeszerzések miatt.



Gyakori félreértések

[1]

A VPN magának a technológiának a neve, és nem pedig a szolgáltatásé, amiről leginkább hallunk az internetes reklámokban.

*Ezért van úgy, hogy a korábban bemutatott VPN típusokat a **vállalatok saját maguknak készítik el**, saját belső használatra és nem pedig előfizetnek egy internetes VPN szolgáltatásra. Egy saját virtuális hálózatot építenek ki, amit a munkavállalók vagy a vállalat egy másik telephelye igénybe vehet abból a célból, hogy az informatikai rendszereik fizikai távolságtól függetlenül, biztonságosan használhatók legyenek.*

A leggyakrabban havi előfizetéssel elérhető VPN szolgáltatások ugyan ezt a technológiát alkalmazzák, viszont más célra. Ebben az esetben is kialakul egy belső virtuális hálózat, ami a VPN szolgáltató szervereit jelenti. Itt viszont nem az a cél, hogy a felhasználó fontos informatikai rendszereket érjen el, hanem az, hogy a felhasználó a nyílt internetet egy plusz biztonsági „kapun" keresztül használhassa. A felhasználó valódi IP címe elrejtésre és az általa küldött packetek titkosításra kerülnek, így megteremtve a felhasználó biztonságosabb online jelenlétét.

A leggyakrabban, amikor az emberek a VPN-ről beszélnek, akkor erre gondolnak, tehát a VPN szolgáltatásokra, és nem pedig magára a technológiára.

Mi a különbség a VPN-ek és a proxyk között?

Egy másik gyakori félreértés a VPN és a proxy kifejezések **egymás szinonimájaként való használata.** Látszatra hasonlóan működnek, hiszen a proxyk és a VPN hálózatok is a kommunikációba való közbeékelődéssel rejtik el a felhasználó eredeti IP címét és geolokációját. A működési elvük, és a támogatott protokolljaik viszont jelentősen eltérnek.

Amíg a VPN-ek elsődleges célja a biztonság növelése, addig a proxyké a kutatás könnyebbé tétele. Számtalan weboldal figyeli, hogy hány kapcsolatfelvételi kísérlet érkezik egy adott címről, és egy bizonyos szám felett blokkolják ezeket a kísérleteket, ugyanis ezek szolgáltatás megtagadási kísérletre utalhatnak (DoS), vagy pedig adatgyűjtésre (web scraping), és nem pedig egy átlagos felhasználói interakcióra. A proxy szerverek szét tudják osztani különböző IP-címekre az általunk küldött packeteket, így a weboldalt tároló célszerver nem tilt le, hiszen a beérkező kérelmek több külön számítógépről érkeznek. További különbség, hogy a VPN-ek titkosítanak adatot, míg a proxyknál ez nem törvényszerű.

Egy VPN forgalmat lehallgató hacker tehát azt se tudja, hogy mi a hálózaton áthaladó üzenetek tartalma, és azt se, hogy ki a küldője, míg egy proxy forgalmat lehallgató hacker csak az üzenet küldőjének személyét (IP címét) nem ismeri, a tartalmát (hacsak valami más nem titkosítja) igen.

Mindezen felül a VPN-ek használata könnyebb is a proxykénál. Míg egy átlagos VPN szolgáltató kliense csak egy program, amit telepíteni kell, és utána rendszerszintű „védelmet" nyújt az internet irányába – azaz minden kifelé irányuló forgalmat titkosít, és a saját tunnelén keresztül küldi tovább - addig a proxy szervereket manuálisan kell beállítani minden általunk használni kívánt proxyn keresztül.

Mindezen okok miatt elmondható, hogy a VPN egy sokkal felhasználóbarátabb, hétköznapibb és több funkciójú lehetőség, amíg a proxyk inkább az IT profik eszköze.

NEMZETI VIRTUÁLIS TÉR

A magyar állam **2024. január elsejétől ingyenes VPN szolgáltatást biztosít Nemzeti Virtuális Tér néven**. A szolgáltatást minden magyar természetes személy ingyen igénybe veheti, aki magyarországi elektronikus azonosító szolgáltatással (Ügyfélkapu, Ügyfélkapu+, Telefonos azonosítás, Arcképes azonosítás, eSzemélyi) rendelkezik.

A magyar VPN célja, hogy **a jogosult személyek Magyarország határain kívül korlátozás nélkül hozzáférjenek a magyar műsorszolgáltatók által sugárzott, geo-blocking technológiát alkalmazó (földrajzi szűrőrendszerrel védett) médiatartalmakhoz**. Ezen felül azt is biztosítja, hogy a világ bármely pontjáról könnyedén és biztonságosan intézhessük közügyeinket például az ügyfélkapun keresztül.

A VPN használatának hátrányai

Hamis biztonságérzet

Számtalanszor elhangzott már, hogy a VPN-ek célja az internetes forgalmunk anonimizálása, az IP címünk elrejtése és az adataink védelme. Amíg egy általános célú felhasználásnál ez javarészt igaz is, fontos kiemelni, hogy a VPN-ek nem képesek teljes anonimitást biztosítani. Ehhez egyéb kiberhigiéniás technikákat is el kell hogy sajátítsunk, ugyanis léteznek olyan módszerek, amelyekkel az IP címünk megszerzése nélkül is igen nagy bizonyossággal azonosítani tudnak minket. A weboldalak használhatnak sütiket, trackereket, és fingerprinting technikákat az ilyesfajta céljaikra.

Ezen túl a VPN kliensek is számítógépes programok, és mint minden más programban, ezekben is lehetnek sérülékenységek: olyan biztonsági hibák, amelyeket programozók ejtettek, és a biztonsági szakértők figyelmét is elkerülték. Ezeket kihasználhatják hackerek, vagy egy vírusos gép is kompromittálhatja őket. Így elképzelhetővé válik, hogy a VPN szolgáltatón kívül a kliens minden forgalmat továbbít a kiberbűnözők számára is.

Néhány VPN próbálja tiltani az ismerten káros weboldalakat, ezzel valamelyest próbálja védeni a felhasználót. Azonban ez a védelem sem teljeskörű, és egyenesen haszontalan, ha az ember már letöltötte a kártékony programot. Attól, hogy VPN-t használunk, az még nem jelenti azt, hogy teljesen láthatatlanná váltunk a kibertérben. **A VPN nem helyettesít egy jó vírusírtót.**

Ingyenes és megbízhatatlan VPN szolgáltatások

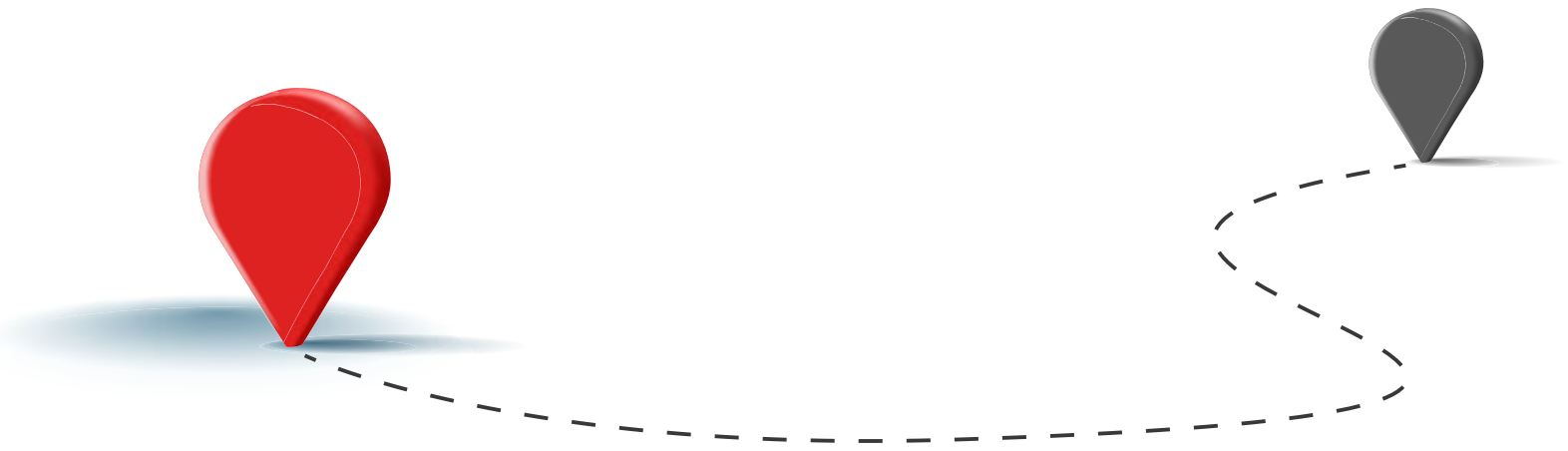
Léteznek ingyenesen használható VPN szolgáltatások, ezekről azonban többnyire elmondható, hogy kevésbé megbízhatóan működnek, mint a fizetős társaik. Sok esetben képtelenek feloldani a geo-blockingot, illetve ha egy adott weboldal vagy szolgáltatás használ VPN szűrőt, akkor esetenként ezek fennakadhatnak rajta, és így teljesen elérhetetlenné válik a kívánt tartalom.

A legrosszabb esetben adatlopás is előfordulhat, például authentikációs adatok megszerzése. A VPN technológiát lehet rossz célokra is használni, hiszen onnantól kezdve, hogy minden forgalmat átirányítunk egy külső félen keresztül, nem tudhatjuk biztosan, hogy ő hogyan kezeli azt. Ez innentől kezdve egy bizalmi kérdéssé válik.

Míg a drágább, fizetős VPN-ek jól szabályozottak, és többnyire megbízhatók, ez nem elmondható az ingyenes verziókról. Ez logikus is, hiszen gondoljunk bele: miért érné meg bárkinek létrehozni egy hatalmas, költséges infrastruktúrát, amit aztán mindenki számára ingyenesen használhatóvá tesz? Ingyenes VPN-eknél gyakran érvényesül az elhíresült mondás: „**Ha nem fizetsz a termékért, akkor te vagy a termék.**" **Mindig járjunk utána a VPN szolgáltatók hitelességének** mielőtt igénybe vesszük őket, legyen az ingyenes vagy fizetős!

Teljesítményproblémák

A VPN-ek természetükből fakadóan minden adatot, ami átfut rajtuk, egy hosszabb úton irányítanak a célhoz, mint ami a sztenderd lenne. Az internet, és a routing protokollok alapvetően úgy működnek, hogy dinamikusan képesek változtatni az egyes csomagok útvonalát attól függően, hogy melyik gócpontok leterheltek, és így összességében a legtöbb internet felhasználó számára a leggyorsabb válaszidőket eredményezik. Egy adott VPN hálózatnak viszont az összes bejövő kérelmet kezelnie kell, ezzel gyakorlatilag fix gócponttá válik, beleszól ebbe a dinamikusan változó útvonalba. Ezen felül a packetek titkosítása és visszafejtése is időt vesz igénybe. Ez összességében azt eredményezi, hogy ha VPN-t használunk, a legtöbb interneten végzett tevékenység észrevehetően lassabbá válik, néhány esetben jelentősen. A legtöbb esetben ez nem zavaró, hibátlanul lehet így híreket, blogokat olvasni, videókat nézni, viszont az olyan felhasználási céloknál, amelyek azonnali reakciókat igényelnek, (például videóhívás vagy online videójátékok) késedelmi gondok jelentkezhetnek.



Továbbá a titkosított tunnel használata miatt az is elmondható, hogy a VPN-en keresztül folyó kommunikáció több adatforgalmat generál. Ez akkor érhet minket kellemetlenül, ha mobilinternetről böngészünk. A rendelkezésünkre álló adatkeret így gyorsabban elfogyhat, vagy nem várt költségek jelenhetnek meg a szolgáltatónknál.

A VPN-ek jogi vonatkozásai

Az európai unió államaiban legális a VPN-ek használata egészen addig, amíg nem kártékony tevékenységekre van felhasználva, azonban ez nem igaz minden EU-n kívüli országra.

A VPN-ek minden formában tiltottak Türkmenisztánban, Ománban, Fehéroroszországban, Irakban és Észak-Koréában. Ezekben az országokban komoly büntetés jár a használatukért, akár szabadságvesztésre is ítélhetik azokat, akik megsértik az ottani törvényeket.

Kínában, Oroszországban, Törökországban, Indiában, Iránban, Egyiptomban, Ugandában és az Egyesült Arab Emírségekben csak azok a VPN-ek használhatók, amelyeket a kormány külön engedélyezett. Ezekben az országokban azonban az állam felügyelheti a VPN hálózatokon keresztülfolyó forgalmat, ami ellentmond a VPN szolgáltatások használatának egyik legfontosabb alapelvének. **Mindig ellenőrizzük a helyi szabályokat** a VPN használattal kapcsolatban!

Különleges funkciók

Néhány VPN szolgáltató különleges funkciókat is biztosít, ezzel valamelyest elkülönülnek a többitől. Ha VPN-t keresünk, ezeket érdemes figyelembe venni a választáskor:

1

RAM-ONLY SERVER

Bizonyos VPN szolgáltatók felhasználóik számára olyan infrastruktúrát építettek ki, ami **teljes mértékben RAM memóriával működik**. Ez azt jelenti, hogy a szervereik csak olvasható image-ről bootolnak. Mivel nincsen HDD, illetve semmilyen egyéb hosszútávú adattárolásra alkalmas eszköz a rendszerben, az ilyen jellegű szolgáltatások még biztonságosabbak, ugyanis egyrészt a hackerek nem tudnak semmilyen olyan programot telepíteni a VPN szerverre, ami később hozzáférést biztosíthatna számukra, mivel az időszerű újraindításoknál ezek törlődnének. Másrészt az ilyen szerverek a működéshez szükséges időn túl **technológiailag képtelenek a felhasználóik adatforgalmait rögzíteni**, ezáltal a VPN szolgáltató semmilyen külső félnek nem tudja utólagosan átnyújtani a felhasználók tevékenységéről készült naplófájlokat, még a hatóságoknak sem. Ezzel egy kicsit kevesebb bizalom szükséges, ugyanis az anonimitást itt a technológia maga garantálja, és nem szimplán a VPN szolgáltató szava.

2 SPLIT TUNNELING

Néhány VPN szolgáltató egy úgynevezett Split Tunneling lehetőséget kínál, aminek lényege, hogy **csak bizonyos típusú forgalmat irányít a titkosított VPN tunnelen keresztül, a többit pedig hagyományos módon a nyílt interneten.** Alapvetően a VPN kliens minden kimenő forgalmat a VPN szerveren keresztül küld, ezzel a szolgáltatással személyre szabhatjuk, hogy mi az a program vagy forgalom típus, aminél fontosabb számunkra az adatok biztonsága, és a többit hagyományos módon a gyorsabb, ámbár kevésbé biztonságos módon tudjuk szimultán használni. Természetesen így a VPN számos előnyéről le kell mondanunk ezen programok esetében.

3 MULTI-HOP VPN - DOUBLE VPN

Multi-hop VPN szolgáltatás esetében (vagy más néven Double VPN) **a VPN szerverre érkező adatforgalom tovább irányul még több VPN szerverre, ezzel az eddiginél is nehezebbé válik az elküldött információk értelmezése az illetéktelen „hallgatózók" számára.** Gyakorlatilag egy plusz védelmi réteget képez az eddigi titkosításon felül azzal, hogy a forgalmat nem egy központi, centralizált szerveren keresztül irányítja, hanem több szerver között szétosztva. Ez azért lehet fontos, mert ha egyetlen egy szerver kezelné, annak kompromittálódása esetén minden rajta keresztül folyó adat veszélybe kerülhetne. Ezen felül a legprofesszionálisabb hackerek, **bizonyos információkat a titkosított adatforgalom figyelésével is meg tudnak szerezni a forgalmi minták elemzésével**. Ezt megnehezíti, ha az információ nem egyetlen fix útvonalat jár be, hanem láncba kötött VPN szervereken keresztül halad.

Kinek javasolt a VPN használata?

A VPN használata szinte bárki számára javasolt, aki fontosnak tartja az online adatvédelmet, ugyanis az a plusz biztonság, amit nyújt a legtöbb ember számára értékesebb, mint a minimális mennyiségű hátrány, ami velük jár.

Különösen ajánlott azoknak, akik:

1. **Gyakran használnak nyilvános Wi-Fi hálózatokat:** Bár ez alapvetően nem ajánlott, vannak olyan élethelyzetek amikor elkerülhetetlen a használatuk. Mivel a nyílt Wi-Fi hálózatok tökéletes eszközei a hackereknek, sokat növel a biztonságon, ha ezeket VPN szolgáltatón keresztül használjuk.
2. **Sokat utaznak:** A VPN-ek segítenek elsimítani a földrajzi korlátozásokból eredő nehézségeket.
3. **Bizalmas információkat kezelnek.**
4. **Adatvédelemre érzékenyek:** A VPN-ek segítenek elrejteni az online tevékenységet az internetszolgáltatók, reklámcégek vagy akár kormányzati megfigyelés elől.
5. **Munkavállalóinak, vagy magának távoli hozzárését szeretne adni a rendszereihez.**

Összefoglaló

A VPN-ek, azaz a virtuális magánhálózatok a mai kiberbiztonság megkerülhetetlen elemei. A név magára a technológiára utal, sok féle módon lehet felhasználni, a köznapi értelemben azonban a lényege az, hogy minden internet irányában elküldött adatot – legyen az üzenet, weblapforgalom vagy bármi – titkosít, illetve elrejti a felhasználó IP címét, ezzel növelve a felhasználó biztonságát és megteremtve anonimitását.

A technológiának akadnak hátrányai is, ezért érdemes átgondolni, hogy van-e értelme számunkra a használatának. Ha úgy döntünk hogy igen, járjunk utána, hogy országunkban milyen szabályok vonatkoznak rájuk, illetve jól fontoljuk meg, melyik VPN szolgáltatót választjuk, ugyanis nem mindegyik egyformán megbízható, illetve néhány különleges funkciókkal kiemelkedik a többi közül.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2024