Mi az a VPN-szolgáltatás?

A VPN, amely virtuális magánhálózatot jelent, digitális kapcsolatot létesít a számítógép és egy VPN-szolgáltató tulajdonában lévő távoli kiszolgáló között, létrehoz egy pontok közötti alagutat, amely titkosítja a személyes adatokat, maszkolja az IP-címét, és lehetővé teszi a webhelyblokkok és tűzfalak blokkolását az interneten. Ez biztosítja, hogy az online élmény privát maradjon, védett és biztonságosabb legyen.

Definíciója szerint a VPN-kapcsolat a következő:

Virtuális, mivel nincsenek fizikai kábelek a csatlakozási folyamatban.

Privát, mert ezen a kapcsolaton keresztül senki más nem látja az Ön adatait vagy a böngészési tevékenységet.

Hálózati, mivel több eszköz – a számítógépe és a VPN-kiszolgáló – működik együtt egy létrehozott kapcsolat fenntartása érdekében.

A biztonságosabb, szabadabb és biztonságosabb online élményt keresők számára a VPN használatának számos előnye van. A VPN az adatok titkosításával és az IP-cím maszkolásával védi a felhasználókat, így a böngészési előzményeik és helyük nem követhető. Ez a nagyobb anonimitás fokozott adatvédelmet, valamint nagyobb szabadságot biztosít azoknak, akik blokkolt vagy régióhoz kötött tartalmakhoz szeretnének hozzáférni.

VPN-kapcsolatok típusai

Ma a számítógépekhez és mobileszközökhöz készült VPN-ek széles választékát találja, mind prémium, mind ingyenes, professzionális és személyes használatra. Íme néhány a leggyakoribb típusok közül:

Név	Type (Típus)	Csatlakozási mód	Használati eset
Távelérési VPN (más néven ügyfél-hely VPN)	Kezdőlap	Csatlakozás privát hálózathoz vagy harmadik féltől származó kiszolgálóhoz SSL/TSL protokollon keresztül	Azon távoli dolgozók számára, akiknek privát kapcsolaton keresztül kell hozzáférniük a céges fájlokhoz és erőforrásokhoz, vagy azoknak a felhasználóknak, akik titkosított kapcsolaton keresztül szeretnének böngészni a nyilvános interneten
Helyek közötti VPN	Privát	A hálózat egy másik hálózathoz csatlakozik LAN- és WAN-kapcsolaton keresztül	Azon nagyvállalatoknak, amelyeknek több különböző helyen kell összekapcsolniuk belső hálózataikat, miközben biztonságos kapcsolatot kell fenntartaniuk
VPN-alkalmazások	Mobil	Csatlakozás magánhálózathoz VPN-alkalmazáson keresztül mobileszközön vagy okostelefonon	Azon mobilfelhasználók számára, akik útközben szeretnék kihasználni a VPN előnyeit, vagy instabil internetkapcsolatot tapasztalnak

Távelérési VPN (más néven ügyfél-hely VPN)

A számítógép leggyakrabban használt VPN-típusainak egyike, a távelérési VPN lehetővé teszi a helyi felhasználók számára, hogy a személyes eszközükről csatlakozzanak a szervezet hálózatához vagy egy távoli kiszolgálóhoz. Ehhez meg kell adnia hitelesítő adatait egy bejelentkezési lapon, amely lehetővé teszi a kapcsolat létesítését webböngészőn keresztül. A felhasználók virtuális asztali ügyfélen vagy VPN-alkalmazáson keresztül is csatlakozhatnak a VPN-hez, amely a hitelesítő adatok megadása után egy hálózathoz vagy kiszolgálóhoz is csatlakozik. Az ügyfél egyszerű felületet biztosít a felhasználóknak a munkához, valamint a kapcsolati információkat és a VPN különböző funkciói közötti váltás lehetőségét. A távelérési VPN professzionális és személyes használatra is megfelelő, ezért ez a VPN egyik leggyakoribb formája. Lehetővé teszi a távmunkában dolgozók számára, hogy anélkül férhessenek hozzá a vállalati fájlokhoz és erőforrásokhoz, hogy az irodában kellene lenniük, és védelmet nyújt a távoli vállalatok privát adatainak, így azok privát jellegűek maradhatnak. Az egyéni felhasználók számára, akik egyszerűen csak nagyobb autonómiával és anonimitással szeretnének böngészni a nyilvános interneten, a távelérési VPN elengedhetetlen a tartalomblokkok, a tűzfalak és az internetszolgáltató általi követés elkerüléséhez.

Helyek közötti VPN

A robusztusabb, egyéni megoldásra szoruló nagy szervezetek a helyek közötti VPN-eket választhatják. A helyek közötti VPN egy privát, belső hálózat, amely egy szervezeten belül több hálózatból áll, amelyek egymás helyi hálózataihoz (LAN) csatlakoznak a nyilvános interneten keresztül. Ez a beállítás lehetővé teszi, hogy a felhasználók a szervezeten belül vagy azzal szomszédos két külön hálózatban oszthassák meg az erőforrásokat egymással, miközben továbbra is korlátozzák az összes erőforrásukhoz való teljes hozzáférést, így biztosítva, hogy a vállalaton belüli kommunikáció a lehető legprivátabb és legbiztonságosabb maradjon. A helyek közötti VPN-ek mérete és összetettsége miatt ez a kapcsolattípus leginkább nagyvállalati szintű, több telephelyen részlegekkel rendelkező vállalatok számára ideális.

A helyek közötti VPN-eken belül két hálózattípus létezik:

Intranet

Az intranetes helyek közötti VPN több telephelyet kapcsol össze egyazon szervezetből helyi hálózaton keresztül. Ez akkor hasznos, ha több részlegnek több helyen kell együttműködnie egymással egy zárt, privát hálózaton belül. A helyek közötti kapcsolaton keresztül ezek a részlegek biztonságosan és hatékonyan cserélhetnek erőforrásokat egymással.

Extranet

Egy extranetes helyek közötti VPN több különböző szervezet webhelyét kapcsolja össze LAN segítségével. Egy olyan szervezetnek, amely gyakran együttműködik külső szállítókkal, partnerekkel vagy üzleti szállítókkal, szükség lehet a hálózat kialakítására. A szervezetek testre is szabhatják az egyes hálózatok közötti hozzáférés hatókörét, így csak bizonyos erőforrások lesznek megosztva, míg mások privátak maradnak.

Mobil VPN

Míg a régi VPN-szolgáltatók jellemzően az asztali felhasználókat szolgálják ki, az okostelefonok jelentős növekedést generáltak a VPN-ek fejlődésében – és nem véletlenül. A menet közben nagyobb biztonságot és védelmet kereső okostelefonos felhasználók számára szükséges a mobil VPN.

A mobil VPN-ek nem csupán a hagyományos VPN előnyeit biztosítják, de akkor is védik az adatokat, ha az internetkapcsolat nem észlelhető vagy instabil, vagy amikor a mobiladat-forgalom és a Wi-Fi között vált. Amíg az alkalmazás fut, a VPN-kapcsolat biztonságos marad, és az eszköz védett marad. A rugalmasság miatt a mobil VPN ideális felhasználóknak utazások során, illetve azok számára, akik nem rendelkeznek hozzáféréssel megbízható internetkapcsolathoz.

Hogyan működik a VPN?

Amikor megkísérel kapcsolatot létesíteni a VPN-szolgáltató távoli kiszolgálójával, a kiszolgáló hitelesíti a felhasználót, és létrehoz egy titkosított alagutat az adatok futtatásához. Az alagúton áthaladó adatok kódolva vannak, és olvashatatlanná válnak bárki számára, aki nem rendelkezik hozzáféréssel a titkosítási kulcshoz, és emiatt az olvasás nem engedélyezett. Amint ezek az adatok elérik a kiszolgálót, a kiszolgáló a saját titkos kulcsával fejti vissza az adatokat, és olvashatóvá teszi azokat. A kiszolgáló visszaküldi a visszafejtett adatokat és egy új IP-címet arra a helyre, amelyhez csatlakozni próbál. A titkosítási folyamat menete – és annak teljes biztonságossága – a kapcsolat létrehozásához használt protokoll típusától vagy az utasítások rendszerétől függ. A VPN-szolgáltatások csak akkor garantálják a biztonságot és a nyugalmat, ha erős protokollt használnak. Ez az a motor, amely működteti a VPN-t. A VPN-szolgáltatók között számos különböző protokollt találhat, mindegyiket saját útválasztási módszerekkel, és mindegyiket saját használati esetekkel. Íme néhány a leggyakoribb lehetőségek közül, amelyekre érdemes figyelni:

OpenVPN

A világ egyik leggyakrabban használt protokollja, az OpenVPN iparági szabványnak számít a biztonság, a stabilitás és a rugalmasság tekintetében. 256 bites titkosítási technológiával rendelkezik, SSL/TSL protokollon keresztüli alagútképzést biztosít, és nyílt forráskódú technológiát használ, ami azt jelenti, hogy bárki megtekintheti a forráskódját, és elháríthatja az esetleges biztonsági réseket. Ez az átláthatósági szint biztosítja, hogy adatait soha ne értékesítsék vagy adják át külső hirdetőknek.

SSTP

Az SSTP, amely a Secure Socket Tunneling Protocol rövidítése, egy másik iparági szabványnak számító protokoll, amely 256 bites titkosítást és SSL/TSL-tanúsítványokat tartalmaz a hitelesítéshez. Natív módon, a Windows operációs rendszerbe van beépítve, és a Microsoft támogatja, így a legjobb választás a Windows-felhasználók számára.

IKEv2 / IPSec

Az IKEv2, amely a Internet Key Exchange 2-es verziójának rövidítése, egy olyan protokoll, amely általában az IPSec, IP-biztonság protokollal van párosítva az optimális biztonság és sebesség érdekében. Az IKEv2/IPSec fenntartja a kapcsolatot még instabil internetkapcsolat esetén is, és még akkor is, ha a mobiladat-forgalom és a Wi-Fi között vált. Ez a legjobb protokoll mobil VPN-ekhez.

L2TP / IPSec

Az L2TP, amely a Layer 2 Tunneling Protocol rövidítése, egy másik protokoll, amelyet gyakran párosítanak az IPSec-kel a fokozott biztonság érdekében. Az SSTP-hez hasonlóan ez is natív módon be van építve a Windows operációs rendszerbe, és általában könnyen beállítható, bár számos szolgáltató már nem támogatja ezt a protokollt, mivel már jobb lehetőségek állnak rendelkezésre.

PPTP

A PPTP, amely a Point-to-Point Tunneling Protocol rövidítése, az L2TP elődje volt, és azóta már elavulttá vált. Egyes ingyenes VPN-ek továbbra is használhatják ezt a protokollt, azonban számos ismert biztonsági hibája miatt már nem tekinthető megbízhatónak a biztonságos kapcsolatokhoz.

WireGuard

A WireGuard egy újabb, folyamatosan bővülő protokoll, amely folyamatosan fejlődik a VPN területén. Egy kisebb kódbázist, modernebb titkosítási technológiát és nagyobb mobilkompatibilitást biztosít. Az OpenVPN-hez hasonlóan ez egy nyílt forráskódú projekt, ami azt jelenti, hogy bárki áttekintheti a forráskódot, hibákat jelenthet be, és a szolgáltatók felelősségre vonhatók.

Hogyan védi a VPN az IP-címet?

A titkosítás mellett a VPN a nyilvános interneten is maszkolja az IP-címet, és maszkolja az identitását. Amikor egy felhasználó sikeresen csatlakoztatja a számítógépet a VPN-kiszolgálóhoz, a VPN nem csupán az adatai védelmét biztosítja, hanem egy új IP-címet is hozzárendel, amely elrejti a valódi IP-címét. Ez egy megosztott IP-cím formájában fordulhat elő, amely több felhasználót egyetlen IP-címhez csoportosít, így az egyes felhasználók tevékenységei nehezen észlelhetővé válnak. Ez az új IP-cím a VPN-kiszolgáló IP-címének is megfelelhet, ami azt jelenti, hogy minél több kiszolgáló található a világon, annál több IP-cím közül választhat. Az igényeitől függően ez a VPN-ügyfél beállításaiban konfigurálható. Amikor egy VPN elrejti az IP-címét, a helyét is megváltoztatja vagy elrejti. Ez azon tartalomblokkokat és tűzfalak elkerülésénél lehet hasznos, amelyek az IP-címére támaszkodva kezdeményezik a blokkolást. Az IP-maszkolás hatékonynak bizonyult a doxing ellen is, ahol a privát identitását online nyilvánossá teszik, valamint DDoS-támadásokat vagy elosztott szolgáltatásmegtagadási támadásokat. Ha senki sem ismeri a valódi IP-címét, senki sem indíthat támadást Ön ellen.