

Az SSL VPN alkalmazása

A **VPN lényege**, hogy a távolról bejelentkező felhasználót ellátja egy „helyi” IP címmel, így olyan mintha a belső hálózat szereplője lenne. Miután bejelentkezett, hozzáférhet a vállalatban belül található erőforrásokhoz, adatokhoz. Lehetőség van arra is azonban, hogy a VPN-szerveren olyan szabályokat határozzunk meg, amelyekkel a user-eket tudjuk korlátozni.

Hátránya: - minden esetben szükség van speciális kliens szoftver telepítésére
- bonyolultsága révén, hiba esetén problémás a kapcsolat javítása
- amikor a kapcsolat nem működik a felhasználók segítségére várnak

Ezen problémák kiküszöbölésére fejlesztették ki az új típusú SSL (Secure Sockets Layer) VPN-eket, amelyek rendkívül könnyen telepíthetők és nem kell bonyolult beállításokat végezni rajtuk.

A hagyományos IPsec VPN olyan biztonságos csatornák létrehozására alkalmas, ahol az adatok titkosítva továbbítódnak, valamint a felhasználók csatlakoznak a helyi hálózathoz. Ilyenkor ugyanazon a csatornán bármennyi felhasználónak lehetősége van csatlakozni. Az egyik nagy különbség, hogy az **SSL VPN esetében** az egyes felhasználók a szolgáltatásokhoz és alkalmazásokhoz csatlakoznak a helyi hálózatban és nem válnak annak részévé. A csatornát egyetlen felhasználó és szerver/hálózat között hozza létre.

A Juniper készülék képes leválasztani a belső hálózatot a külsőtől, ezáltal védi az erőforrásokat az illetéktelen hozzáférésektől. A felhasználó kap egy olyan eszközt, amelyre csatlakoztatjuk a belső hálózatot valamint a külső internetkapcsolatot, és nem kell rajta különleges beállításokat végezni annak érdekében, hogy a VPN kapcsolatot felépítsük. Tehát lehetőségünk van Web alkalmazásokat illetve szolgáltatásokat biztonságosan és egyszerűen elérni. Ebben az esetben, a cégen belüli egyéb erőforrásoknak is biztonságos távoli elérést biztosít.



A Juniper **Secure Access** termékcsalád két fontos funkciója az Access Control és az Endpoint Security. Az első szerint három különböző hozzáférési módszer alapján irányíthatjuk a felhasználók hozzáférését az erőforrásokhoz.

Core Access: Hozzáférést biztosít Web alapú alkalmazásokhoz, fájl megosztókhoz, Telnet/SSH host alkalmazásokhoz és Outlook Web eléréséhez.

Segítségével a felhasználók, bármilyen eszközről, bármilyen hálózaton tudnak csatlakozni (pl: vállalati laptop, otthoni vagy partner számítógép, kiosk, PDA).

Secure Application Manager: Kliens/szerver alkalmazások elérése (pl: Windows és Java alkalmazások). Egy kattintásos hozzáférés, olyan alkalmazásokhoz, mint a Citrix, Microsoft Outlook, Lotus Notes.

Szükséges azonban, hogy az alkalmazási szoftver fel legyen telepítve a felhasználók számítógépére.

Network Connect: Az IPsec VPN-hez hasonló megoldás, amely a teljes IP forgalmat két pont között képes küldeni. Támogatja a kliens és erőforrás igényű alkalmazásokat (pl: streaming media, VoIP).

Abban az esetben ajánlott amikor az alkalmazottak teljes hálózati hozzáférést kapnak.

Az Endpoint Security két végpont között biztonságos kapcsolatot épít fel. Először leellenőrzi az eszközt amiről a felhasználó VPN csatlakozást szeretne létesíteni és biztosítja, hogy az eszköz megfeleljen a vállalati politikának, majd csak ezután hozza létre a kapcsolatot.

Host Checker: megvizsgálja a folyamatokat és szolgáltatásokat a kliens számítógépén majd eldönti, hogy ha kapcsolódhat az internethez hogyan teheti meg ezt. Amennyiben nem teljesül a szabályzat, a következők történhetnek

- átirányítja a felhasználót egy előre meghatározott oldalra és tájékoztatja a problémáról, vagy esetleg milyen lépéseket kell tennie az elhárítás érdekében.
- megpróbál egy másik policy-t engedélyezni (pl. ha valamilyen okból kifolyólag a víruskereső nem működik)
- leállít futó folyamatokat vagy letöröl fájlokat a kliens gépéről, amennyiben erre szükség van

Cache Cleaner: eltávolítja a visszamaradt adatokat a felhasználó gépéről, mint pl. Temporary Internet Files, Application Cashes.

Az SSL VPN **előnyeit** tekintve

- ✓ Bárhol, bármikor hozzáférést biztosít, legyen akár otthon PC, vállalati laptop, mobiltelefon
- ✓ Nincs szükség szoftver telepítésre, konfigurációra, hibajavításra
- ✓ Csak egy Internetes böngésző és internet kapcsolat kell hozzá
- ✓ Növeli a biztonságot azáltal, hogy titkos és hiteles hozzáférést biztosít, valamint speciális alkalmazásokat, erőforrásokat tudunk felhasználónként korlátozni
- ✓ Rugalmas abból a szempontból, hogy nincs szükség külön kliens szoftver telepítésére és hozzáférhető bármilyen internetezésre alkalmas eszközről
- ✓ Olyan helyen is használható ahol az IPsec VPN nem működik, mert esetleg le vannak tiltva a kommunikációjához szükséges portok (pl: hotel esetében, stb...)
- ✓ Abban az esetben ha az IPsec VPN nem működne, az SSL VPN automatikusan átveszi a helyét.



Az Juniper eszközök előnye, hogy a célnak kifejlesztett hardveren titkosított fájlrendszer található. Ezáltal a JUNOS szoftvert futtató környezetben korlátozható a belépés az OS alá. A legtöbb esetben a legkisebb eszközök is ugyanazt tudják menedzselhetőség szempontjából mint a nagyobbak.