VPN típus és hardver kiválasztása

VPN típusok összehasonlítása

Fölmerülhet benned a kérdés, hogy miért pont IPSEC/IKEv2 protokollt kellene használnod? Sokféle VPN megoldás létezik. Ennek a leírásnak az elkészítésében sokat segített Nikita Tarikin előadásának megtekintése. Az általa előkészített ábrák nagyon kifejezőek. Az egyik ilyen ábra ami azt mutatja, hogy melyik VPN protokol milyen előnyökkel és hátrányokkal rendelkezik.

Compare VPN types (RouterOS)

	L2TP	L2TP/IPSEC + psk	OpenVPN	PPTP	SSTP	IPSec IKE2
Protocol	UDP	UDP over UDP/ESP	TCP	GRE	TCP	UDP, ESP
Performance	Fast	Medium	Slow	Fast	Slow	**Very fast**
Connection establishment	Medium	Slow	Slow	Medium	Medium	**Very fast**
Requires strong CPU for encryption	No	Yes	Yes	No	Yes	Yes
Multicore CPU load balance	Yes	Yes	No	Yes	Yes	Yes
Security	Low	Strong	Strong	Low	Strong	**Very strong**
Push routes	No	No	Yes	No	No	Yes
Bypass NAT	Yes	Yes	Yes	Yes	Yes	Yes
Has interface	Yes	Yes	Yes	Yes	Yes	No
OS popularity	High	Very high	High	Very high	Low	High

Nikita Tarikin / nikita@tarikin.com

Az látható, hogy a "biztonságos" és az "alacsony CPU igény" egymást kizáró dolgok. Ami biztonságos ahhoz erős CPU kell. Amihez nem kell erős CPU, az nem biztonságos. Ebből a dilemmából a kiutat az jelenti, hogy bizonyos eszközökben külön hardver van a titkosításra. Cél hardver alkalmazásával viszonylag alacsony költségen nagy teljesítményt lehet elérni. Erről alább még írok.

A táblázatot áttekintve elég egyértelműen látszódik, hogy ha az erős titkosítás és a megbízhatóság a célunk, és mindezt viszonylag nagy sebességgel szeretnénk elérni, akkor az IPSEC + IKEv2 a

legjobb megoldás. Manapság nagyon elterjedt és favorizált az OpenVPN. A fenti táblázatban ez azért van lassúnak jelölve, mert a MikroTik/RouterOS OpenVPN megoldása nem mondható optimálisnak. Más rendszereken az OpenVPN egész gyors tud lenni, legalábbis ami az adatforgalmat illeti. (A csatlakozás sebessége ott is elég lassú.) Mivel mi itt MikroTik/RouterOS eszközökkel szeretnénk megoldani a kapcsolatot, ezért az OpenVPN-t nem tudjuk használni. Plusz az OpenVPN-ről tudni kell, hogy alapból layer 3 protokoll fölött, layer 4-ben van implementálva. Az IPSEC-hez képest egyel magasabb szinten van, és ebből fakad néhány hátránya.

Néhány további dolog ami a táblázatból nem látszódik:

- A régi számítógépek és operációs rendszerek nem, vagy nem teljesen jól támogatják az IPSEC/IKEv2 VPN-t.
- Az IPSEC/IKEv2 beállítása általában nagyobb szakértelmet igényel, mint mondjuk egy L2TP szerver beállítása. Ez a cikk azért íródott, hogy átsegítsen a beállítás nehézségein. Ezért remélhetőleg ez sem okoz majd problémát.

Hardver kiválasztása

Ahogy föntebb említettem, nem mindegy hogy milyen eszközt használunk. Ilyen célra kizárólag olyan típust érdemes használni, amibe bele van építve a titkosítási algoritmusok hardveres támogatása. A specifikációk áttanulmányozása után bárki ki tudja választani a neki megfelelőt.

A MikroTik router-ek esetében erről van egy nagy táblázat itt:

https://wiki.mikrotik.com/wiki/Manual:IP/IPsec#Hardware_acceleration

Íme néhány általam favorizált típus.

HAP AC2

Az általam javasolt legkisebb/legolcsóbb MikroTik router a HAP AC2 típus. Ajánlott fogyasztói ára e cikk írásakor 69 USD. Ez nagyon alacsony ár a tudásához képest.

RB750Gr3

Ha nincsen szükség WiFi-re, vagy ha a Wifi-t külön eszközökkel szeretnéd megoldani, akkor esetleg szóba jöhet az RB750Gr3 is. CPU teljesítményben ez egy kicsit alulmarad a HAP AC2-höz képest, és várhatóan a HAP AC2 által alkalmazott arm architektúra a jövőben nagyobb támogatásra számíthat. (A memóriája több, de IPSEC site-to-site alagutazásnál ez nem igazán számít.) Minimálisan olcsóbb (59 USD). Én személy szerint akkor is inkább a HAP AC2-őt venném, ha a wifi részére nincsen szükségem.

HAP AC3

A HAP AC3 típus pontosan ugyan azt az IPQ-4019 processzort használja mint a HAP AC2. Bár a memóriája több, de VPN kapcsolat kiépítéshez erre nincs szükség. Ha csak a VPN alagút kiépítését nézzük, akkor nem jobb mint a HAP AC2, viszont drágább (99 USD). A Wifi képességei sokkal jobbak 5Ghz-en a specifikáció szerint, de erről én inkább itt nem mondanék véleményt mivel sosem próbáltam.

A fenti eszközök megfelelő beállítás esetén akár 300-400Mbps sebességel képesek IPSEC titkosításra. (Az IPSEC teljesítményt a hivatalos honlapon a "test results" fülön lehet megtalálni.) Kis céges és otthoni felhasználásra azért érdemes MikroTik-et használni, mert ezt a teljesítményt ilyen konfigurálhatóság és felügyelet mellett más cég termékeivel nem nagyon lehet elérni. (Hasonló tudású Cisco termékek többszörösébe kerülnek. Bár az igaz hogy ott a támogatás is jobb.)

RB4011

Ha ennél is nagyobb teljesítményre van szükség, akkor a RB4011 lehet jó megoldás. Ez nagyobb csomagméretnél 2Gbps IPSEC átvitelre képes, de még 512byte csomagméret esetén is kb. 800Mbps-t tud. Ennek van egy Wifi-vel ellátott változata is.

x86

Ha még ennél is nagyobb teljesítményre van szükséged, akkor sem kell lemondani a RouterOS-ről. A RouterOS elérhető x86 platformon. Egy gyors géppel és QSFP kártyákkal jóval nagyobb teljesítmény is elérhető. Bár az az igazság, hogy ha 1Gbp fölötti IPSEC teljesítményre van szükséged, akkor nem biztos, hogy ebből a cikkből kellene tájékozódnod, és akkor egyáltalán nem biztos, hogy a MikroTik lesz a megfelelő megoldás. :-)

Revision #5
Created 2 January 2021 18:11:55 by Gandalf
Updated 9 January 2021 12:20:34 by Gandalf