Millist SSL VPN-i soetada?

21 aastat tagasi - 11.03.2005 Autor: AM

(Arvutimaailm 3/05)

Autor: **Hardy Viilup**

SSL-il põhinevad VPN lahendused koguvad üha enam populaarsust. Selle põhjuseks on nende poolt pakutav funktsionaalsus:

• ligipääs vajalikele ressurssidele igalt poolt;

• end reaalses elus tõestanud turvalisus;

• lihtne integreerimine olemasoleva infosüsteemiga;

• lihtne haldus.

Ligipääs vajalikele ressurssidele on tagatud tänu SSL-võimeliste veebisirvijate laiale levikule, igast võrgustatud arvutist võib leida veebisirvija. Neid võib kohata ka tänapäevastes mobiiltelefonides. Ka on SSL/TLS protokollid on end tõestanud igapäevases elus turvalistena.

SSL VPN lahendused on realiseeritud SSL proksiserverina, kus ühendused sisevõrgu ressurssidega pakendatakse SSL/TLS proksiserveri (edaspidi lihtsustatult proksi) poolt turvalisemasse, SSL/TLS protokolliga kaitstud ühendusse. Kliendi ja proksiserveri vaheline ühendus on krüpteeritud.

Lahendus ei nõua muudatusi sisevõrgu serverite poolel, rakendamiseks on vajalik ainult proksi paigaldamine selliselt, et sellele oleks juurdepääs välisvõrgust ja loomulikult on vajalik ettevõtte turvapoliitikaga sobilike autentimismeetodite, krüptoalgoritmide, sisevõrguressursside ja pääsuõiguste seadistamine.

Kui te olete otsustanud SSL VPN lahenduse kasuks, tahate te loomulikult valida parima lahenduse. Alljärgnevalt toon välja tähtsaimad kriteeriumid, millele tasuks enne lahenduse soetamist tähelepanu pöörata.

Autentimine

Autentimismeetodite mitmekesisus võimaldab lahenduse valutumalt integreerida olemasoleva infosüsteemiga ja kasutada olemasolevat volitatud kasutajate

loendit. Enamlevinud autentimisprotokollid on LDAP, NTLM ja RADIUS, nende tugi peaks tootel olemas olema.

Krüpteerimine

Ühenduse käigus vahetatav informat-sioon on krüpteeritud, kasutades kliendi ja proksi vahel kokku lepitud krüptoalgoritmi. Oluline on, et proksi poolt oleks toetatud tugevad krüptoalgoritmid nagu 3-DES ja AES-256. Kliendi poolel toetatud krüptoalgoritmid olenevad konkreetsest seadmest ja kasutatavast veebisirvijast.

Kliendi masina turvalisus

Kliendid võivad kasutada sisevõrgu ressursside poole pöördumiseks väga erineva turvatasemega seadmeid nagu ettevõtte poolt hallatavad arvutid, koduarvutid, PDA-d, mobiiltelefonid. Selleks, et otsustada, millise tasemega pääsuõigusi kliendile omistada, tuleks kindlaks teha kliendi seadme turvalisuse tase. Selle määramiseks tuleb kontrollida, et seadmesse ei oleks paigaldatud spioonvara, klahvivajutuste logijaid ja masinas oleks aktiivne uusima viirusmustriga viirusetõrje tarkvara ning tulemüür.

SSL VPN peab oskama enda järgi koristada, sest keegi meist ei taha, et ettevõtte tundliku sisuga dokumentide töökoopiad jääks maha avalikult kasutatavatesse seadmetesse ja oleksid teistele kättesaadavad. Et seda ei juhtuks, peab kliendipoolne rakendus oskama eemaldada töö käigus seadmesse tekkinud failid, seda ka juhul, kui seade peaks „kinni jooksma” või ootamatult alglaadimise käivitama.

Rakenduste tugi

Veebipõhised sisevõrgu rakendused on väga laialt levinud ja nende toetamisega probleeme ei esine. Tõsisemaid probleeme valmistavad grupitöö rakendused nagu Lotus Notes ja Microsoft Exchange, nende puhul on vajalik SSL VPN lahendusepoolne tugi. Kui te kasutate ühte nendest, siis jälgige kindlasti, et need rakendused oleksid toetatud.

Kui teie poolt kasutatavad rakendused vajavad UDP protokolli tuge, siis veenduge selle toe olemasolus.

Tootja usaldusväärsus

Tootja peab omama kogemust turvatoodete alal, vastasel korral riskite sellega, et olete soetatud toote beetatester. Oluline on ka ettevõtte tegevuse kestvus. Mida pikem tootmisajalugu, seda väiksem on risk, et toodet ei toetata aastate pärast.

Laiendatavus

Hästi läbimõeldud lahendus kasvab koos ettevõttega. Kui ettevõttel tekkib juurde harukontoreid või suureneb töötajate hulk, siis peab ka lahendus olema hõlpsasti kohandatav.

Haldus ja käideldavus

Reaalses elus esineb olukordi, kus klient ei saa tema poolt kasutatavasse seadmesse paigaldada klienttarkvara, näiteks avalikes internetipunktides. Paljudel juhtudel ei oska klient vajalikku tarkvara paigaldada ja administraatoritel puudub juurdepääs kliendi poolt kasutatavale seadmele, seega on väga oluline, et lahendus oleks kasutatav ka ilma klienttarkvarata.

- Lahendused
- Turvalisus