# VPN ORQALI MASOFADAN XAVFSIZ KIRISHNI TASHKIL ETISH

**[1]A. A. Muradova, [2]I. L. Kudratov**
[1]Muhammad al-Xorazmiy nomidagi TATU, PhD, dotsent
[2]Muhammad al-Xorazmiy nomidagi TATU, 2-kurs magistranti

***https://doi.org/10.5281/zenodo.7856605***

***Annotatatsiya.*** *Maqolada VPN orqali masofadan xavfsiz kirishni tashkil etish xususiyatlari keltirilgan. Maqola VPN (Virtual Private Network) texnologiyasi, VPN turlari va qo‘llanilishi, VPN ishlash tartibi bo‘yicha ma’lumotlar mavzuga oid adabiyotlar va internetdan olingan ma’lumotlardan foydalangan holda yozildi.*

***Kalit so'zlar:*** *Internet, TCP/IP, protokol, Intranet, Ekstranet, VPN.*

Internetning gurillab rivojlanishi natijasida dunyoda axborotni tarqatish va foydalanishda sifatiy o‘zgarish sodir bo‘ldi. Internet foydalanuvchi lari arzon va qulay kommunikatsiyaga ega bo‘ldilar. Korxonalar Internet kanallaridan jiddiy tijorat va boshqaruv axborotlarini uzatish imkoniyatlariga qiziqib qoldilar. Ammo Internetning qurilishi prinsipi niyati buzuq odamlarga axborotni o‘g‘irlash yoki atayin buzish imkoniyatini yaratdi. Odatda, TCP/IP protokollar va standart lnternet-ilovalar (e-mail, Web, FTP) asosida qurilgan korporativ va idora tarmoqlari suqilib kirishdan kafolatlanmaganlar. lnternetning hamma yerda tarqalishidan manfaat ko‘rish maqsadida tarmoq hujumlariga samarali qarshilik ko‘rsatuvchi va biznesda ochiq tarmoqlardan faol va xavfsiz foydalanishga imkon beruvchi virtual xususiy tarmoq yaratish ustida ishlar olib borildi. Natijada, 1990-yilning boshida virtual xususiy tarmoq konsepsiyasi yaratildi. «Virtual» iborasi VPN atamasiga ikkita uzel o‘rtasidagi ulanishni vaqtincha, deb ko‘rilishini ta’kidlash maqsadida kiritilgan. Haqiqatan, bu ulanish doimiy, qat’iy bo‘lmay, faqat ochiq tarmoq bo'yicha traflk o‘tganida mavjud bo‘ladi. Virtual tarmoq VPNlarni qurish konsepsiyasi asosida yetarlicha oddiy g‘oya yotadi: agar global tarmoqda axborot almashinuvchi ikkita uzel bo‘lsa, bu uzellar orasida ochiq tarmoq orqali uzatilayotgan axborotning konfidensialligini va yaxlitligini ta’minlovchi virtual himoyalangan tunnel qurish zarur va bu virtual tunneldan barcha mumkin bo‘lgan tashqi faol va passiv kuzatuvchilarning foydalanishi haddan tashqari qiyin bo‘lishi lozim [1].

**VPN o‘zi nima?** VPN Virtual Private Network (Virtual shaxsiy tarmoq) so'zlarining qisqartmasi bo'lib, unda siz ochiq tarmoqdagi ikkita kompyuterni bir-biriga ulab, shaxsiy va maxfiy bog'lanishni yaratasiz. VPNlar dastlab uylaridan turib nozik ish hujjatlarini internet orqali ko'rishni xohlagan kompaniya ishchilari uchun yaratilgan. Shundan beri u mashhur bo'lib, oddiy foydalanuvchilar qo'liga ham yetib bordi. VPN foydalanuvchiga har qanday ma'lumotni "internet tunneli" deb ataladigan tarmoq orqali jo'natish va olish imkoniyatini beradi.

**VPN turlari va qo‘llanilishi.** VPN’ning uchta asosiy ko‘rinishi qabul qilingan: masofadan turib foydalanish imkoniyati mavjud bo‘lgan VPN (Remote Access VPN), tashkilot ichidagi VPN (Intranet VPN) va tashkilotlararo VPN (Extranet VPN) [2].

• masofadan turib foydalanish imkoniyati mavjud bo‘lgan VPN ba’zan Dial VPN deb ham nomlanadi. Ular mustaqil dial-up-foydalanuvchilarga xavfsiz tarzda Internet yoki boshqa umumiy foydalanish tarmog‘i orqali markaziy ofis bilan bog‘lanish imkonini beradi.

• Intranet VPN «nuqta-nuqta» yoki LAN-LAN VPN deb ham ataladi. Bu tur VPN butun Internet yoki boshqa umumiy foydalanish tarmog‘i orqali xavfsiz xususiy tarmoqlar yaratadi.

• Ekstranet VPN bo‘lsa, elektron tijorat uchun ideal muhit vazifasini bajaradi. Bu VPN bog‘lanish yordamida biznes hamkorlar, xom ashyo yetkazib beruvchilar va mijozlar bilan xavfsiz bog‘lanish imkoniyati mavjud. Ekstranet VPN — bu Intranet VPN’ning kengaytirilgan ko‘rinishi bo‘lib, unda ichki tarmoqni himoya etish maqsadida fayrvoldan foydalaniladi.

**Uning ishlash tartibi quyidagicha**. Masalan, qayerdadir kompyuter tarmog'i bor va unga ulanish huquqi faqat ayrim odamlarga berilgan. Siz ulardan birisiz va bu tarmoqqa xavfsiz yo’l bilan ulanishingiz kerak. Shunda siz VPNdan foydalansangiz, u kompyuteringiz va siz kirmoqchi bo'lgan tarmoqning haqiqiy va xavfsiz ekanini tasdiqlab beradi. Shundan so'ng VPN siz jo'natmoqchi bo'lgan ma'lumotni shifrlab, uni ikkinchi tomonga ham shifrlangan holatda yetkazib beradi. Kimdir tarmoqqa kirib ma'lumotlaringizni o'qishga urinsa, ularga turli raqamlardan iborat kodlangan ma'lumot ko'rinadi, xolos.

VPN imkonyatini taqdim etuvchi xizmatlar ko'p. Ular "PureVPN", "AirVPN" yoki "VPN4All" kabi nomlar bilan ataladi. Ularning har biri o'ziga xos xizmatlarni taqdim etib, ayrimlari bepul, boshqalari esa yiliga 80 yoki 100 dollargacha pulli bo'lishi mumkin.

**VPN qanday ishlaydi?** VPN ma'lum bir kompyuter yoki tarmoqqa xavfsiz bog'lanish imkoniyatini bersa ham, undan shaxsiy ma'lumotlaringizni himoyalash va bloklangan saytlarga kirish vositasi sifatida ham foydalanishingiz mumkin [3].

Qaysidir bir VPN xizmatini sozlab, o'rnatib olganingizdan so'ng, kompyuteringiz shu xizmatga aloqador VPN tarmoqlariga xavfsiz ulanadi. Shundan so'ng, masalan, bloklangan YouTube saytiga kirmoqchi bo'lsangiz, bu sayt uchun murojaatingiz VPN serveriga yuboriladi va bu server YouTube saytini bloklanmagan manzildan olib sizga jo'natadi. Shu yo'l bilan xuddi YouTubega to'g'ridan to'g'ri ulanayotgandek bo'lasiz, lekin aslida siz VPN orqali boshqa bir yashirin manzil va ma'lumotlar bilan saytni ochayotgan bo'lasiz.

Ammo shu yerda bir lekini bor. Agar hukumat VPN kompaniyasi ishlatayotgan biror serverdan xabar topsa, shu serverni bloklab qo'yishi mumkin va natijada u orqali siz bloklangan saytlarni ocha olmaymiz. Shuning uchun VPN kompaniyalari ko'plab serverlar bilan ishlashadi va ularni aniqlab bloklash qiyin bo'ladi.

**VPN menga qanday yordam berishi mumkin?** Internet markazlashmagan boshqaruv tizimiga asoslangani bois hukumatlar uchun VPNlarni aniqlash va bloklash juda qiyin. Ular sizning onlayn va shaxsiy ma'lumotlaringizni himoya qilishda ham samarali ishlaydi. Internetga ko'p ma'lumot joylash yoki ko'chirib olish bilan shug'ullansangiz va bu faoliyatingiz uchun jazolanishdan qo'rqsangiz, VPN sizga qo’l kelishi mumkin.

Turli VPN tanlovlari mavjudligi boshida sizni biroz chalg'itishi mumkin. Har bir tarmoqning ishlash uslubi va texnik qoidalari har xil bo'ladi va bir VPNning imkoniyatlari boshqasiniki bilan bir xil bo'lmasligi mumkin. Shuningdek, texnik bilimi cheklangan odamlar uchun uni ishlatish murakkab tuyuladi. Mavzuni biroz tadqiq qilsangiz va bunday dasturlarni yaxshi tushunadigan ishonchli do'stlaringizdan yordam olsangiz, qanday VPN tanlash bo'yicha bir qarorga kelishingiz osonlashadi.

**Ehtimoliy kamchiliklari.** Hukumatlar saytlarni bloklashda turli xil vositalardan foydalanishini hisobga olsak, ba'zan VPNning sizga to'g'ri kelish yoki kelmasligi qaysi davlatda yashashingizga ham bog'liq bo'ladi.

Eron, masalan, ayrim saytlarni bloklashda ulkan va o'zgaruvchan bloklash usullaridan foydalanadi. Yuqorida tilga olingan sabablarga ko'ra, bu holatda bloklarni aylanib o'tish uchun

VPN qo'l kelishi mumkin. Ammo Xitoyning internetni kuzatish usullari farqli va bu holatda VPNdan boshqa dasturlarni ishlatish samaraliroq bo'lishi mumkin.

VPN bilan bog’liq yana ikki noqulaylik bor. Birinchidan, uni ishlatish uchun maxsus fayllar va dasturlarni VPN kompaniyasidan ko’chirib olishingiz kerak. Agar siz bu kompaniyaga internet orqali bog’lana olmasangiz yoki uning sayti davlatingizda bloklangan bo’lsa, bu ishingizni qiyinlashtirishi mumkin.

Ikkinchidan, sizning ma’lumotlaringiz turli noma’lum joylardagi har xil serverlar orqali o’tayotgani bois VPN internet tezligini sekinlashtirishi mumkin. Bundan achchiqlangan ayrim foydalanuvchilar dasturni internetda ishlayotgan paytlari o’chirib qo’yadilar. Bu usa ularning onlayn faoliyatlari endi ochiq tarmoqlarga o’tdi, degani.

**Masofaviy foydalanuvchi "kirish erkinligi".** Masofaviy kirish tarmog'ini loyihalashda keyingi eng muhim masala - foydalanuvchining Internetga kirish muammosi. Ushbu dizaynning xavfli tomoni shundaki, foydalanuvchi internetda viruslar va boshqa kirlarni, masalan, josuslik dasturlarini qabul qilib, korporativ tarmoqqa tranzit hujum agentiga aylanishi mumkin.

Bunday tahdidning oldini olish uchun Cisco’dagi hamkasblar qo‘shimcha xavfsizlik choralarini qo‘llashni tavsiya qiladilar: antivirus (bugungi kunda bu yerda josuslarga qarshi dastur qo‘shilishi kerak), mijoz kompyuteridagi shaxsiy xavfsizlik devori va kirish konsentratorida kengaytirilgan xavfsizlik boshqaruvi (IDS). Men VPN-ning yuqori izolyatsiyalash qobiliyatiga ega ekanligiga asoslanib, biroz boshqacha yondashuvni ko'rib chiqishni taklif qilaman (bu faqat yaxlitlik va maxfiylik mexanizmlariga tayanib, sanoat odatda kam baholaydi).

Misol uchun, an'anaviy perimetr qurilmasini, xavfsizlik devorini ko'rib chiqing. Xavfsizlik devorining xavfsizlik siyosatini u orqali o'tayotgan trafikni passiv kuzatish yoki faol skanerlash orqali aniqlash juda oson. Xavfsizlik devori xavfsizlik siyosatini tushunganimdan so'ng, korporativ tarmoq ichiga noqonuniy paketni osongina kiritishim mumkin. VPN bu imkoniyatni butunlay yo'q qiladi. Xavfsizlik shlyuzidan faqat shaxsiy kalit egasi tomonidan chiqarilgan paket o'tadi. Buni "taxmin qilish" mumkin emas, shuning uchun begona odam hech qachon tarmoqqa kirmaydi.

Masofaviy kirish segmentida faqat izolyatsiya VPN siyosatini qo'llash tavsiya etiladi, unga ko'ra masofaviy foydalanuvchi faqat korporativ tarmoqqa kirishi mumkin, boshqa hech qanday joyda. Bir qarashda bu yondashuv bir qancha savollar tug‘diradi. Birinchisi: agar masofaviy foydalanuvchi Internetga kirishga muhtoj bo'lsa-chi?

Javob oddiy: masofaviy foydalanuvchilarga xavfsiz kanal orqali korporativ tarmoqqa chiqishga ruxsat bering, keyin esa oddiy mahalliy foydalanuvchilar uchun xavfsizlik choralarini qo‘llagan holda masofaviy foydalanuvchilarni Internetga “umumiy asosda” qo‘yib yuboring (2-rasm).

Ushbu yechim ikkita asosiy afzalliklarni beradi:

✓ Masofaviy kirish tarmog'ining xavfsizlik siyosati oddiy, bir xil va mustahkamdir. Faqat qattiq izolyatsiyalash VPN siyosati bizga agressiv ochiq tarmoq muhitidan tartibsiz, malakasiz va sodiq masofaviy foydalanuvchilar kelishi shart bo'lmagan muhitda nisbatan xavfsizlikni va'da qilishi mumkin.

Administratorlarning barcha kuchi va texnik xavfsizlikka investitsiyalari barcha foydalanuvchilar uchun yagona Internetga kirish nuqtasini ta'minlashga qaratilishi mumkin.

Ushbu sxemaning nochorligi aloqa uchun qo'shimcha xarajatlardir, chunki masofaviy foydalanuvchilarning trafigi Internet orqali ikki marta o'tadi: himoyalangan shaklda va ochiq shaklda. Biroq, foydalanuvchilarning masofaviy trafiki odatda korporativ aloqalarning umumiy narxining nisbatan kichik qismini tashkil qiladi. Internet arzon va uzoq foydalanuvchilardan Internet-trafikning ikki baravar narxi korporativ tarmoqning yuqori xavfsizligi uchun to'lash uchun maqbul narx bo'lib tuyuladi.

Umuman olganda, shaxsingizni yashirish va bloklangan saytlarni ochishda VPN yaxshi qurol vazifasini o’taydi. Ammo qayerda yashashingiz, qaysi kompaniya yoki xizmatdan foydalanishingizga qarab siz ishlatadigan VPNning imkoniyatlari har xil bo’lishi mumkin.

**REFERENCES**

1. S.K.Ganiev, M.M.Karimov va K.A. Toshev, “Axborot xavfsizligi,” Toshkent, 2008.
2. "Different Types of VPNs and When to Use Them," *VPN Mentor*. Retrieved October 16, 2020.
3. R.Younglove, "Virtual Private Networks - How They Work," *Journal of Computational Control Engineering*, ISSN 0956-3385, 11 (6),2000,pp. 260–262. doi:10.1049/cce: 20000602.