MASOFAVIY KIRISHDA ASOSIY XAVFSIZLIK TEXNOLOGIYASINI TANLASH

A.A. Muradova [1], I. L. Kudratov [2]
[1,2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

https://doi.org/10.5281/zenodo.7856596

Abstract. *The article presents the main security technologies and scientific innovation in remote access. Remote access allows the user to use the resources of another computer located at a great distance. In this case, the choice of the main security technology in remote access was considered important and was written using the literature on the subject and information obtained from the Internet.*

Keywords: *Security, IPsec, protocol, VPN.*

Maqolaning ilmiy yangiligi shundan iboratki, masofaviy kirish uchun asosiy xavfsizlik texnologiyalarini tahlil qilish zarur. Kompaniyalarning masofaviy ish rejimlariga ommaviy va shoshilinch o'tishi axborot xavfsizligi muammolarini sezilarli darajada kuchaytirdi. Aksariyat kompaniyalar birinchi marta bunday vazifaga duch kelishdi, shuning uchun "masofadan ishlash" ga o'tish ularga juda ko'p qiyinchiliklar tug'dirdi. Turli kompaniyalarning statistik ma'lumotlari va hisobotlari bilan tasdiqlangan ma'lumotlar mavjudki, buzg'unchilarning faolligi uzoq vaqt davomida o'sgan. Buzg'unchilar, ayniqsa, foydalanuvchilarning shaxsiy qurilmalari va onlayn xizmatlariga ko'chirilgan maxfiy ma'lumotlarni nishonga olishadi. Mutaxassislarning fikricha, masofaviy ishchilar eng yuqori xavf ostida.Uy tarmoqlari korporativ tarmoqlarga qaraganda ancha xavfsizroq, bu ularga ulangan kompyuterlarni jiddiy potentsial muammolar manbaiga aylantiradi. Masofaviy ish bilan bog'liq axborot xavfsizligi xavflari orasida trafikni o'zgartirish, parollar va maxfiy ma'lumotlarni ushlab qolish, shuningdek, marshrutizatorlarni buzish va foydalanuvchilarni zararli saytlarga yo'naltirish kiradi.

Masofaviy kirish sizga katta masofada joylashgan boshqa kompyuterning resurslaridan foydalanish imkonini beradi va uni mahalliy tarmoqqa kabel orqali ulashning hech qanday usuli yo'q. Bunday holda siz masofaviy tarmoq yaratishingiz mumkin. Masofaviy tarmoq telefon tarmog'i orqali ikkita kompyuterni ulash orqali yaratilgan. Bunday holda, kompyuterlardan biri mahalliy tarmoqqa kiritilishi mumkin. Bunday tashkilot masofaviy kirish masalan, uy kompyuteridan ofisdagi kompyuterlarga ulanish imkonini beradi. Albatta, ulanadigan ikkala kompyuter ham modemlar bilan jihozlangan bo'lishi kerak. U ishlab chiqarilgan kompyuter masofaviy ulanish server deb ataladi. U maxsus sozlangan bo'lishi kerak. Agar, masalan, uzoq tarmoqdagi server mahalliy tarmoqqa ulangan bo'lsa, u holda masofaviy foydalanuvchi nafaqat server resurslariga, balki butun mahalliy tarmoq resurslariga ham kirishini ta'minlash mumkin. shuningdek, barcha tarmoq foydalanuvchilariga o'z resurslarini taqdim eting.

Shunday qilib, masofaviy tarmoq yaratish uchun siz bitta kompyuterni server sifatida sozlashingiz kerak. 1. Masofaviy foydalanuvchi foydalanishi mumkin bo'lgan resurslarga kirishni tashkil qilish. Ushbu protsedura Sec-da batafsil tavsiflangan. "Mantiqiy qurilmalarga kirishni tashkil etish". 2. Masofaviy tarmoq bilan ishlash dasturini - "Microsoft Plus!" dasturiy paketiga kiritilgan Dial-Up Networking Server dasturini o'rnatish zarur. 3. Dial-up Networking dasturiga kiring (Start | Programs | Aksessuarlar | Dial-up Networking). 4. "Ulanishlar" menyusida "Remote Access Server" buyrug'ini tanlang. 5. Qo'ng'iroq qiluvchiga kirishga ruxsat berish radio tugmasini tanlang, shundan so'ng server kiruvchi qo'ng'iroqlarga javob beradi va masofaviy

foydalanuvchilarga tarmoq resurslariga kirishni ta'minlaydi. Bu resurslar xuddi kompyuterlar mahalliy tarmoqqa ulangandek taqdim etiladi. Agar kerak bo'lsa, tarmoqqa kirish uchun parol o'rnatishingiz mumkin.

Shuningdek, siz Dial-up Networking dasturidan foydalanib serverga qo'ng'iroq qilishingiz va uning resurslaridan foydalanishingiz mumkin. 1. Ulanishlar menyusidan Yangi ulanish buyrug'ini tanlang, bu erda tarmoqqa kirish uchun ulanish nomini, server telefon raqamini va parolni ko'rsatishingiz kerak. 2. Shundan so'ng, Dial-up Networking oynasida serverga ulanish uchun yangi belgi paydo bo'ladi. 3. Kursorni ushbu belgi ustiga olib boring va ikki marta bosing. Bog'lanishni o'rnatish oynasi paydo bo'ladi. 4. Keyin modemni yoqishingiz va "Ulanish" tugmasini bosishingiz kerak. Shundan so'ng, modem serverni chaqiradi, bu sizga masofaviy tarmoqqa kirish imkonini beradi. Keyin mahalliy tarmoq uchun yuqorida tavsiflangan barcha tarmoq imkoniyatlaridan foydalanishingiz mumkin.

Masofaviy tarmoq va Ethernet mahalliy tarmog'i o'rtasidagi yagona kamchilik va farq modemlarning yuqori tezlikdagi imkoniyatlari bilan cheklangan kirish tezligidir. o'tkazish qobiliyati telefon tarmog'i. Masofaviy kirish sizga katta masofada joylashgan boshqa kompyuterning resurslaridan foydalanish imkonini beradi va uni mahalliy tarmoqqa kabel orqali ulashning hech qanday usuli yo'q. Bunday holda siz masofaviy tarmoq yaratishingiz mumkin. Masofaviy tarmoq ikkita kompyuterni telefon tarmog'i orqali ulash orqali yaratiladi. Bunday holda, kompyuterlardan biri mahalliy tarmoqqa kiritilishi mumkin. Masofaviy kirishning bunday tashkil etilishi, masalan, uy kompyuteridan ofisdagi kompyuterlarga ulanish imkonini beradi. Albatta, ulanadigan ikkala kompyuter ham modemlar bilan jihozlangan bo'lishi kerak. Masofadan ulanayotgan kompyuter server deb ataladi. U maxsus sozlangan bo'lishi kerak. Agar, masalan, uzoq tarmoqdagi server mahalliy tarmoqqa ulangan bo'lsa, u holda masofaviy foydalanuvchi nafaqat server resurslariga, balki butun mahalliy tarmoq resurslariga ham kirishini ta'minlash mumkin. shuningdek, barcha tarmoq foydalanuvchilariga o'z resurslarini taqdim eting.

Xavfsizlik - har kuni biz to‘qnashadigan hayotimizning jihati: eshikni qulflaymiz, qimmatbaho narsalarni begona ko‘zlardan berkitamiz va ham-yonni duch kelgan joyda qoldirmaymiz. Bu “raqamli dunyoga” ham rasm bo‘lishi shart, chunki har bir foydalanuvchining kompyuteri qaroqchi hujumi obyekti bo‘lishi mumkin [1].

Bugungi kunda tarmoq (IPsec) va transport (SSL/TLS) qatlamlari xavfsizligi texnologiyalari masofaviy kirishni himoya qilish sohasida juda qattiq raqobatlashmoqda. Ushbu yechimlar orasidagi farqlarning mohiyatini aniqlash uchun ba'zi tasniflarni kiritish kerak. Uchta tubdan farq qiladigan tizim arxitekturasini ko'rsatadi: IPsec VPN; SSL yoki TLS protokollari asosida transport qatlami xavfsizligini qo'llash uchun "klassik" stsenariy; SSL (TLS) VPN.

Qanday farqlar bor? Avvalo shuni ta'kidlash kerakki, har uchala arxitektura taxminan bir xil kuchga ega kriptografik algoritmlardan foydalanadi. Shunday qilib, kriptografik kuch mezoniga ko'ra, echimlarni taxminan bir xil deb hisoblash mumkin [2, 3, 4].

Aloqa protokoliga kelsak, IPsec yechimi amalga oshirishda ham, ishlashda ham ancha moslashuvchan va murakkabroq. IPsec arxitekturasida: dastur trafigi tarmoq sathiga paketlar ko'rinishida uzatiladi, paketlar ushlanadi, shifrlanadi va imzolanadi. Maxsus protokol, Internet Key Exchange, IKE, kalitlarni boshqarish va xavfsizlik siyosati bo'yicha muzokaralar olib boradi.

The Burton group konsalting kompaniyasi o'zining analitik hisobotlaridan birida VPN yechimlari asoslanganligini ta'kidladi. IPsec protokoli yuqori xavfsizlik talablari bo'lgan tizimlar uchun SSL/TLS VPN-dan afzalroqdir.

SSL/TLS protokollaridan foydalanishning "klassik" sxemasiga kelsak, bu umuman VPN emas. Eng so'nggi nashr etilgan IETF lug'atlaridan biriga ko'ra, VPNlar “davlat yoki xususiy tarmoqlardan shunday foydalanish usulidirki, VPN foydalanuvchilari boshqa foydalanuvchilardan ajratilgan va xuddi bitta yopiq tarmoqda bo'lgandek bir-birlari bilan muloqot qilishlari mumkin edi”.

Klassik SSL/TLS yechimi bu ta'rifga mos kelmaydi. U bitta transport aloqasining yaxlitligi va konfidensialligini ta'minlaydi. Boshqa ilovalar ochiq trafikni uzatadi va hech kim ularning "shifrlanmagan" portlariga kirishni nazorat qilmaydi. SSL/TLS-da kompyuterni himoya qilish sxemasining bunday ochiqligi meni doimo chalkashtirib yubordi. Ammo bu yechimning o'ziga xos, deyarli raqobatbardosh bo'lmagan "ekologik joy" bor.

Masofaviy (korporativ bo'lmagan) masofaviy kirish uchun xavfsizlik tizimlarida, biz har bir foydalanuvchi uchun "o'zimizning" VPN mijozimizni o'rnatolmasak, SSL yoki TLS ulanishlarini qo'llab-quvvatlaydigan veb-brauzerga alternativa yo'q. Shu sababli, elektron tijorat, jismoniy shaxslarning bank resurslariga kirish tizimlari va foydalanuvchilar katta va nazoratsiz parkiga ega bo'lgan boshqa tizimlar Web-brauzer - xavfsiz SSL/TLS ulanish - portal sxemasi bo'yicha qurilgan.

Bundan farqli o'laroq, IPsec - bu VPN funksiyalarini har tomonlama qamrab oladigan arxitektura. Bu erda ular tomonidan "o'z" transport portlari orqali uzatiladigan barcha ilovalarning trafigi IP-paketlarga aylanadi, ular shifrlangan, imzolangan va ishonchsiz tarmoqlar orqali tunnel qilingan. "Izolyatsiya" IPsec xavfsizlik siyosati bilan, umumiy IP-trafik to'liq himoyalanganda, shaxsiy kalit egalarining qat'iy belgilangan doirasi tarmoqqa kirish huquqiga ega bo'ladi. Bu “zirh”ga begona odamning kirib kelishi mumkin emas.

SSL/TLS VPN texnologiyalari nisbatan yaqinda tarqaldi. Transportga asoslangan VPN mahsulotlarining motivi ishlash uchun oddiyroq va arzonroq VPN yechimini yaratish edi. Biroq, bu erda, "ular eng yaxshisini xohlashdi" syujetida tez-tez sodir bo'lganidek, nuanslar paydo bo'ldi. Yechim ikkita butunlay boshqa arxitekturaga “tadqiq qildi”: “psevdo-VPN” va “halol VPN”, ular o‘z xususiyatlaridan sezilarli darajada farq qiladi.

Pseudo-VPN oddiy veb-brauzer bilan VPN mijozi sifatida ishlaydi. Korporativ tarmoqning tashqi chetidagi xavfsizlik shlyuzi VPN mijozlariga himoyalangan tarmoq resurslarini veb-resurslar shaklida “ko'rsatadigan” xavfsiz veb-serverdir. Shu bilan birga, himoyalangan resurslar Web sahifalar bo'lishi shart emas. Bu fayl tizimlari, hatto suhbat, ovozli va video bo'lishi mumkin. Ushbu resurslarni brauzer orqali taqdim etish uchun veb-serverning "orqasida" proksi-server mavjud bo'lib, u ushbu resurslarni HTTP-ga va HTTP-dan tarjima qiladi. Bunday yechimning go'zalligi nimada? Gap shundaki, mijoz tomonida VPN qurish uchun umuman hech narsa kerak emas.

Har qanday mashinada brauzer mavjud. SSL yoki TLS deyarli har bir brauzerda mavjud. Sertifikat (kalit) shart emas: SSL ham, TLS ham vaqtinchalik seans kalitini tezda yaratishi mumkin. Siz foydalanuvchini keyinchalik seans kaliti himoyasi ostida, masalan, parol yordamida autentifikatsiya qilishingiz mumkin.

Yuqorida keltirilgan ta'rifga ko'ra, bu erda foydalanuvchilar "bir-birlari bilan xuddi bitta yopiq tarmoqda bo'lgandek muloqot qila olmaydilar". Ular faqat himoyalangan tarmoqdagi tanlangan resurslarga kirish funksiyasiga ega bo'ladilar. Bundan tashqari, "tanlangan resurslar" tarkibi VPN shlyuzining bir qismi sifatida proksi-serverlarning imkoniyatlari bilan cheklangan. Kirish "proksi" bo'lmagan resurslar abadiy mavjud bo'lmaydi. Ikkinchidan, mijoz parki ham faqat qisman himoyalangan bo'lishi mumkin. Mijoz tomoni veb-brauzer emas, balki boshqa narsa bo'lgan ilovalar himoyasizdir. Web-VPN shlyuziga kirish hodisalaridan tashqari foydalanuvchi faoliyati esa butunlay nazoratdan tashqarida.

Endi muhim resurslarni himoya qilish uchun IPsec-ni tavsiya qilgan Burton guruhi tahlilchilarining tashvishi aniq bo'lib bormoqda - u istisno qilmaydi.

Ushbu kamchiliklarni tan olgan holda, SSL/TLS VPN sanoati "halol" VPN-larni taklif qilish orqali arxitekturani murakkablashtirishga kirishdi. Bunday yechimning eng yorqin misoli yaxshi ishlab chiqilgan va bir nechta kitoblarda tasvirlangan OpenVPN loyihasidir (http://openvpn.net). Ilova trafigi ochiq transport protokoliga, so'ngra IP-paketlarga to'planadi, ular SSL yoki TLS xavfsizligidan foydalangan holda ushlanadi va transport qatlami protokoliga qayta qadoqlanadi. To'liq xususiyatli "halol" VPN IPsec yechimiga juda o'xshaydi. Biroq, ushbu yechim uchun to'lanadigan narx VPN mijozini o'rnatish zarurati hisoblanadi. Siz hech qaerga borolmaysiz - brauzer IP-paketlarni tutib, transport protokoliga joylashtira olmaydi.

"Adolatli" SSL/TLS VPN ning qanday afzalliklari bor? Ushbu texnologiya bo'yicha mahsulot ishlab chiqaruvchilari u IPsec-ga qaraganda "juda engilroq" ekanligini aytishadi. IPsec-da bo'lgani kabi, VPN mijozi masofaviy foydalanuvchining mashinasiga o'rnatilishi kerak. Foydalanuvchilarga sertifikatlarni tarqatish kerak bo'ladi. IPsec-da bo'lgani kabi, siz xavfsizlik siyosatingizni sozlashingiz kerak.

Darhaqiqat, VPN mijozini o'rnatish va sozlash IPsec-ni masofaviy foydalanuvchilar parkida joriy etishdagi asosiy qiyinchilik hisoblanadi. Protokol va xavfsizlik siyosatining soddaligida biroz yengillik bor. Narxda biroz yengillik bor: SSL/TLS VPN mahsulotlari biroz arzonroq. Ammo, boshqa tomondan, ushbu mahsulotlarning texnik imkoniyatlari torroq. Xavfsiz masofaviy kirish tizimini yaratishga qiziqqan mijoz qanday texnologiyalarni tanlashi kerak? Bu savolga javob yuqorida aniq aytilgan: Ommaviy kirish portallarida - "sof" SSL / TLS, bu aslida VPN emas. Xavfsizlik talablari past bo'lgan va foydalanuvchilar ko'p va ular malakasiz bo'lgan joylarda SSL yoki TLS asosidagi "pseudo-VPN" dan foydalanish yaxshidir. Qat'iylik haqida gap ketganda korporativ yechim va muhim resurslarga kirish haqida - aniq faqat "adolatli" VPN arxitekturasidan foydalanish kerak. IPsec yoki SSL/TLS VPN? Bu erda - havaskor uchun tanlov.

Yechimni yaratish bo'yicha quyidagi bo'limlar, agar boshqacha ko'rsatilmagan bo'lsa, har qanday "adolatli" VPN yechimiga nazariy jihatdan qo'llaniladi.

REFERENCES

1. S.K.Ganiev, M.M.Karimov va K.A. Toshev, "Axborot xavfsizligi," Toshkent, 2008.
2. RFC 4026, L. Andersson, T. Madsen and A.B. Acreo, "Provider-Provided Virtual Private Network (VPN) Terminology", March 2005.
3. SAFE "VPN IPSec virtual private networks," *Cisco Systems*, Inc., 2004 y.
4. D. Dyuks, and R. Pereyra, " ISAKMP configuration method," draftietf-ipsec-isakmp-cfg-03.txt.