INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.3 №1 (2025). January
innovativepublication.uz

Sho‘ba nomi: VPN (Virtual Private Network) Yordamida Korporativ Tarmoq Xavfsizligini Ta'minlash

Raxmonqulov Diyorjon Ulug’bek o‘g‘li

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali

coderdiyorjon0624@gmail.com

Annotatsiya: Mazkur maqolada VPN (Virtual Private Network) yordamida korporativ tarmoq xavfsizligini ta'minlashga oid texnologiyalar ko'rib chiqiladi va tahlil qilinadi. VPN ulanishlarida qo'llaniladigan asosiy protokollar, ularning afzalliklari va kamchiliklari tahlil qilinib, ushbu texnologiyaning xavfsizlikni ta'minlashdagi o'rni va istiqbollari yoritiladi.

Kalit so'zlar: VPN, virtual xususiy tarmoq, xavfsizlik, protokollar, masofaviy kirish, jamoat tarmoqlari, ma'lumot uzatish, ochiq aloqa kanallari, shifrlash, tarmoq himoyasi, autentifikatsiya.

Аннотация: В статье рассматриваются и анализируются технологии обеспечения безопасности корпоративной сети с использованием VPN (Virtual Private Network). Основные протоколы VPN, их преимущества и недостатки изучаются с целью выявления роли и перспектив этой технологии в защите данных.

Ключевые слова: VPN, виртуальная частная сеть, безопасность, протоколы, удалённый доступ, публичные сети, передача данных, открытые каналы связи, шифрование, защита сети, аутентификация.

Abstract: This article explores and analyzes technologies for ensuring corporate network security using VPN (Virtual Private Network). The main VPN protocols, their advantages, and disadvantages are examined to highlight the role and prospects of this technology in safeguarding data.

Key words: VPN, virtual private network, security, protocols, remote access, public networks, data transfer, open communication channels, encryption, network protection, authentication.

VPN (Virtual Xususiy Tarmoq) kontseptsiyasi Internet kabi ommaviy aloqa kanallari orqali xavfsiz muloqotni ta'minlash uchun moliyaviy muqobil sifatida yuzaga kelgan va tezda axborotning yaxlitligini, maxfiyligini va haqiqiyligini kafolatlovchi keng tarqalgan xavfsizlik texnologiyasiga aylangan. Bu xizmat foydalanuvchilarga tarmoq orqali xavfsiz aloqalarni amalga oshirishda yordam beradi.

VPN ulanishi yordamida barcha trafik dunyoning boshqa nuqtalarida joylashgan serverlar orqali xavfsiz tarzda yo‘naltirilishi mumkin. Bu esa mahalliy snooping (yashirin kuzatish) va xakerlik urinishlaridan himoya qiladi, shuningdek, foydalanuvchining haqiqiy IP manzilini kirilayotgan veb-saytlar va onlayn xizmatlardan yashiradi. Bu usul internetdagi maxfiylikni ta'minlashda samarali yechim hisoblanadi.

VPN shuningdek, ayrim hududlarda mavjud bo‘lmagan onlayn kontentga kirish imkoniyatini yaratadi, bu esa kontent egalarining cheklovlarni qanday samarali amalga

oshirishi bilan bog‘liq. Xizmat ko‘rsatuvchi provayderlar ko‘plab mamlakatlarda serverlarni boshqaradi va foydalanuvchilarga bu serverlar o‘rtasida osongina almashish imkonini taqdim etadi. Masalan, foydalanuvchilar o‘zlarining yoki boshqa mamlakatdagi cheklangan kontentga kirish uchun VPN serveridan foydalangan holda bir mamlakatda joylashgan server orqali ulanishi mumkin.

Kibertahdidlarning xilma-xilligi va intensivligi ortib borayotganligi sababli, tarmoq ma’murlari tashkilotning ichki tarmoqlarini to‘liq blokirovka qilish istagini muvozanatlashlari kerak, shu bilan birga ichki tarmoqqa masofaviy qurilmalar, xodimlar, mijozlar va IoT orqali kirishni ta’minlash zarur. Ushbu muvozanatni saqlash uchun, internetdan xavfsiz foydalanish imkoniyatini ta’minlash maqsadida, virtual xususiy tarmoq (VPN) orqali virtual tarmoqqa xavfsiz kirishni tashkil qilish mumkin. Bu usul tarmoq xavfsizligini ta’minlash bilan birga, foydalanuvchilarga masofadan ulanish imkoniyatini yaratadi.

Xavflarni bartaraf etish uchun VPN turini tanlashda qo‘shimcha xavfsizlik xususiyatlarini hisobga olish zarur. Bu xususiyatlarga quyidagilar kiradi: kuchli autentifikatsiya qo‘llab-quvvatlash, kuchli shifrlash algoritmlaridan foydalanish, antivirus dasturlari va hujumlarni aniqlash hamda oldini olish vositalaridan foydalanish, boshqaruv va texnik portlar uchun sukut bo‘yicha mustahkam xavfsizlik, raqamli sertifikatni qo‘llab-quvvatlash, ro‘yxatga olish va auditni qo‘llab-quvvatlash, shuningdek, barcha manzillarni maxfiy saqlash bilan shaxsiy tarmoqdagi mijozlarga manzillarni belgilash imkoniyatini ta’minlash. Bu xavfsizlik choralari VPN ulanishlarining xavfsizligini oshirish va muhim ma'lumotlarning himoyasini ta'minlashda muhim rol o'ynaydi.

Himoyalangan korporativ tarmoqlarni qurish uchun VPN yechimlaridan biri – marshrutizatorlar asosidagi VPN. Tashqi dunyo bilan lokal tarmoq o‘rtasidagi barcha

axborot marshrutizator orqali o‘tadi. Bu marshrutizatorlar chiqayotgan paketlarni shifrlash va kiruvchi paketlarni rasshifrovka qilish uchun tabiiy platformaga aylantiriladi. Boshqacha aytganda, marshrutizatorlar, odatda, marshrutlash vazifasini VPN bilan birga bajarishi mumkin.

Bunday yechimning afzalligi shundaki, marshrutlash va VPN vazifalarini birgalikda boshqarish ma’muriyati osonlashadi. Korporativ tarmoqni himoya qilish uchun ekranni ishlatmasdan, faqat tarmoqdan foydalanish va uzatiladigan trafikni shifrlash bo‘yicha xavfsizlik vazifalarini birgalikda hal qilishda marshrutizatorlardan foydalanish samarali va qulaydir.

Biroq, bu yechimning kamchiligi, marshrutlash bo‘yicha asosiy amallar bilan birga, shifrlash va autentifikatsiyalash jarayonlarini bajarishning ko‘p mehnatni talab qilishi natijasida marshrutizatorning unumdorligiga bo‘lgan talabning oshishidir. Marshrutizatorning unumdorligini oshirish uchun shifrlash vazifalarini apparat yordamida amalga oshirish mumkin. Bu orqali marshrutizatorlar xavfsizlikni ta’minlashda yuqori samaradorlikni saqlab qoladi.

Marshrutizatorlar asosida VPN qurishda esda tutish lozimki, bu yondashuv kompaniyaning umumiy axborot xavfsizligini ta’minlash muammosini to‘liq hal qilmaydi. Chunki barcha ichki axborot resurslari tashqaridan hujumlar uchun ochiq qoladi. Shu sababli, bu resurslarni himoyalash uchun, odatda, chegara marshrutizatorlaridan keyin joylashgan tarmoqlararo ekranlardan foydalaniladi.

Cisco 1720 VPN Access Router marshrutizatori kichik va o‘rtacha korxonalarda himoyalangan tarmoqni tashkil etish uchun mo‘ljallangan. Bu marshrutizator Internet va intratarmoqlardan foydalanishni tashkil etish uchun zarur bo‘lgan imkoniyatlarni ta’minlaydi va Cisco IOS dasturiy ta’minoti asosida virtual xususiy tarmoqlarni tashkil etish

vazifalarini bajaradi. Cisco IOS operatsion tizimi VPN vazifalarining keng to‘plamini ta’minlaydi, jumladan, ma’lumotlarni himoyalash, xizmat sifatini boshqarish va yuqori ishonchlilikni ta’minlash.

Cisco 1720 marshrutizatori quyidagi ma’lumotlar himoyasini ta’minlaydi:

- **Tarmoqlararo ekranlash**: Cisco IOS Firewall komponenti lokal tarmoqlarni hujumlardan himoya qiladi. CBAC (Context-based access control) funksiyasi ma’lumotlarni dinamik yoki holatlarga asoslangan ravishda filtrlaydi, bu esa samarali tarmoqlararo ekranlash uchun juda muhimdir.
- **Shifrlash**: IPSec protokolidagi DES va Triple DES shifrlash algoritmlari ma’lumotlar konfidensialligini va yaxlitligini ta’minlaydi, shuningdek, ma’lumotlar manbaini autentifikatsiyalashni (ma’lumotlar global tarmoqdan o‘tgandan so‘ng) ta’minlaydi. Shifrlash algoritmlari ma’lumotlarni ishonchli va standart tarzda himoya qiladi.
- **Tunnellash**: Tunnellashning IPSec, GRE (Generic Routing Encapsulation), L2F va L2TP standartlari ishlatiladi. L2F va L2TP standartlari masofadagi foydalanuvchilarning korxona lokal tarmog‘ida o‘rnatilgan Cisco 1720 marshrutizatorigacha virtual tunnel o‘tkazishga imkon beradi. Bu holatda korxona masofadan foydalanish serveriga ehtiyoj qolmaydi va shaharlararo yoki xalqaro qo‘ng‘iroqlar uchun to‘lovlar tejaladi.
- **Qurilmalarni autentifikatsiyalash va kalitlarni boshqarish**: Marshrutizator qurilmalarining autentifikatsiyasini va VPN kalitlarini boshqarish imkoniyatlarini ta’minlaydi, bu esa tizim xavfsizligini oshiradi.

Bundan tashqari, Cisco 1720 marshrutizatori hujumlarni aniqlash va oldini olish kabi xavfsizlik vazifalarini bajaradi, masalan, "xizmat qilishdan voz kechish" kabi xavfsizlikni

ta’minlash uchun, shuningdek, Java blokirovka qilish, audit va ogohlantirishlarni real vaqtda tarqatish kabi imkoniyatlarni ham taqdim etadi.

Kompaniya Web-texnologiyaga asoslangan va VPN yuklanganligini nazoratlash, yuz beruvchi hodisalar asosida statistika va axborotni yig‘ishga mo‘ljallangan **Transcend Ware Secure VPN Manager** dasturiy ilovasini ishlab chiqdi. Ushbu ilova VPN tarmog‘ini boshqarish va kuzatishni osonlashtiradi, shuningdek, hodisalar asosida tahlil va ma'lumotlarni yig‘ish imkoniyatlarini taqdim etadi.

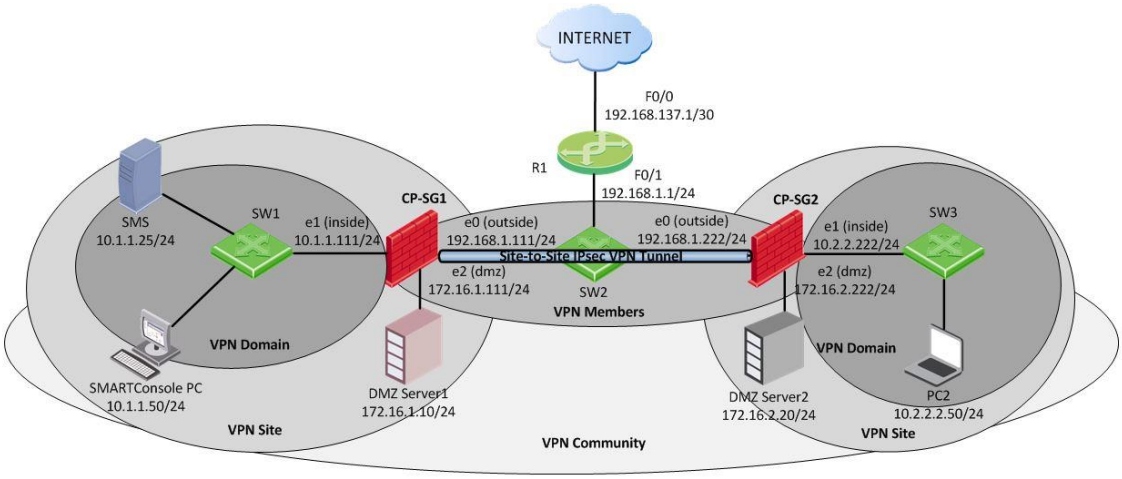
Shuningdek, **3Com** kompaniyasi kriptohimoyalangan tunnellarni osongina yaratishga imkon beruvchi Web asosidagi instrumentariy ishlab chiqadi, bu orqali foydalanuvchilar xavfsiz tunnellarni yaratish va boshqarish uchun qulay vositalarga ega bo‘ladilar.

Internet Devices kompaniyasining **Fort Knox** marshrutizatorlari tezlik va quvvatni uyg‘unlashtirib, yuqori samaradorlikni ta’minlaydi. Fort Knox marshrutizatori IP-trafikni ishlash vazifalari ro‘yxatining kengligi bilan ajralib turadi, bu esa uning afzalliklaridan biridir. Ushbu marshrutizator quyidagi funksiyalarni bajaradi:

- **Tarmoqlararo ekran rejimi**: Fort Knox marshrutizatori tarmoqlararo ekran rejimida ishlaydi, bu esa lokal tarmoqlarni global tarmoqdan himoya qiladi.
- **NAT (Network Address Translation)**: Fort Knox NAT standard bo‘yicha adreslarni translatsiyalashni amalga oshiradi. Bu, ichki IP-adreslarni tashqi dunyodan yashirish va marshrutizatorlar trafigini qayta yo‘naltirish imkonini beradi.
- **Xavfsizlik siyosatini boshqarish**: Marshrutizator xavfsizlik siyosatini boshqarish va tarmoq xavfsizligini ta’minlash uchun zarur funksiyalarni taqdim etadi.
- **Web-sahifalar va DNS xeshlarini saqlash**: Fort Knox Web-sahifalar va DNS jadval yozuvlarini xeshlash orqali tarmoq ish faoliyatini optimallashtiradi.

- **Audit**: Marshrutizator auditni bajarish imkoniyatlarini taqdim etadi, bu esa tarmoqda yuz berayotgan harakatlarni monitoring qilish va tahlil qilish uchun zarurdir.

Fort Knox marshrutizatori ko‘pincha korporativ tarmoq chegarasida, ya’ni global tarmoq bilan korporativ tarmoqni ulovchi marshrutizatorlar orqasida o‘rnatiladi. Bu marshrutizator boshqa lokal tarmoqlar bilan VPN-aloqasini tashkil qilish va tarmoqlararo ekranlar orqali foydalanishni nazorat qilish qoidalarini shakllantirishga imkon beradi.



1-rasm. Check Point FW/VPN asosida korporativ VPN tarmo g‘ini qurish sxemasi.

Check Point VPN-1 mahsulotlari **ochiq standartlar (IPSec)** asosida amalga oshirilgan va foydalanuvchilarni autentifikatsiyalashning rivojlangan tizimiga ega. Ushbu tizim, shuningdek, **ochiq kalitli (PKI)** taqsimlashning tashqi tizimlari bilan o‘zaro aloqani qo‘llab-quvvatlaydi. Bu esa foydalanuvchilarni autentifikatsiyalash, shifrlash va tarmoq xavfsizligini ta’minlashda katta yordam beradi.

Check Point VPN-1 ning asosiy imkoniyatlaridan biri — bu boshqarish va auditning markazlashtirilgan tizimini tashkil etish imkoniyatidir. Bu tizim, tarmoq xavfsizligini boshqarish va kuzatish uchun zarur bo‘lgan barcha ma’lumotlarni markazdan boshqarishga imkon beradi.

Check Point Fire Wall-1/VPN-1 nafaqat **ochiq, balki kriptohimoyalangan trafikni** ham nazoratlaydi. Tarmoqlararo ekran (Firewall) orqali kirgan ma’lumotlar VPN-1 vositalari yordamida **rasshifrovka qilinadi**, so‘ngra axborotlar paketi yana shifrlanadi va o‘tkazib yuboriladi. Bu jarayon, trafikni nafaqat kriptografik tarzda berkitishni, balki axborotlar paketini **autentifikatsiyalash** funksiyasini ham bajaradi.

VPN-1 tizimida trafikni shifrlashda quyidagi mashhur **kriptoalgoritmlar** ishlatiladi:

- **DES** (Data Encryption Standard)
- **3-DES** (Triple DES)
- **CAST**
- **IDEA** (International Data Encryption Algorithm)
- **FWZ1** (Check Point kompaniyasining ishlanmasi)

FWZ1 — bu Check Point kompaniyasining maxsus ishlab chiqilgan kriptotizimi bo‘lib, bu ham trafikni shifrlash va autentifikatsiyalash uchun qo‘llaniladi.

Bu tizimlar Check Point VPN-1 mahsulotlarining tarmoq xavfsizligini ta’minlashdagi ishonchliligini oshirib, foydalanuvchilarning ma’lumotlarini himoya qilishda samarali yechimlarni taqdim etadi.

Ixtisoslashtirilgan apparat vositalari asosidagi VPN tizimlarining asosiy afzalligi — bu **yuqori unumdorlik**. VPN paketlarini ishlashda kerakli hisoblashlar hajmi **oddiy paketlar bilan ishlashdagiga nisbatan 50-100 marta** ko‘proq bo‘ladi. Bu tizimlar, xususan, **shifrlash** jarayonlarini optimallashtirish uchun **ixtisoslashtirilgan mikrosxemalar**dan foydalanish orqali yuqori tezlikka erishadilar.

Ixtisoslashtirilgan apparat vositalari yordamida ishlaydigan VPNlar, shifrlash jarayonlarini apparat darajasida amalga oshiradi, bu esa **dasturiy ta'minot asosidagi**

VPNga qaraganda ancha tezroq ishlashni ta'minlaydi. Mikrosxemalar maxsus maqsadlar uchun ishlab chiqilgan bo‘lib, ular ma'lum bir hisoblash jarayonini optimallashtiradi, masalan, shifrlash va de-shifrlash operatsiyalarini. Bu, o‘z navbatida, VPN tarmog‘ining umumiy ishlash samaradorligini va **tezligini** sezilarli darajada oshiradi.

Bu afzallik, yuqori xavfsizlik va tezlikni talab qiladigan, masalan, katta korporatsiyalar, moliya sohasidagi tashkilotlar va boshqa yuqori tezlikdagi trafikni ishlovchi tizimlarda juda muhimdir.

Apparat shlyuzlarini o‘rnatish dasturiy shlyuzlar va marshrutizatorlar yoki brandmauerlar asosidagi shlyuzlarga nisbatan juda oson va samarali amalga oshiriladi. Bunday qurilmalar o‘rnatish va sozlashda, odatda, **pastroq murakkablikka** ega, chunki ular maxsus ishlab chiqilgan va tezda integratsiyalanishi mumkin.

Bunday tizimlarni boshqarish ikki asosiy masalani hal etishni talab qiladi:

1. **Sertifikatsiya markazi orqali kalitlarni boshqarish**: Apparat shlyuzlarida kalitlarni boshqarishning markazlashgan tizimi, odatda, Windowsga moslashgan dasturiy ilovalar yordamida amalga oshiriladi. Bu yordamida autentifikatsiya va ma'lumotlarni shifrlash uchun zarur bo‘lgan **xususiy va umumiy kalitlarni** boshqarish osonlashadi.
2. **Himoyalangan tunnellashni boshqarish**: Apparat shlyuzlarining asosiy afzalliklaridan biri, tunnellash jarayonlarini markazlashtirish imkoniyatidir. Markaziy boshqaruvdan, bir ish joyidan turib barcha tunnellarni nazorat qilish mumkin. Bu, ayniqsa, ko‘p tunnellarni boshqarish zarur bo‘lgan holatlarda foydalidir.

Boshqaruvchi dasturlar, tunnelning **asosiy himoyalash funksiyalarining** to‘g‘ri bajarilishini ta’minlaydi va tizimda yuzaga keladigan **xatoliklarni aniqlaydi**. Bu dasturlar tunnellarni boshqarish, trafikni yo‘naltirish, va xavfsizlikni ta'minlashni amalga oshiradi.

Ular tarmoqda sodir bo‘ladigan har qanday muammolarni aniqlash va hal qilishni osonlashtiradi.

References:

1. Росляков А.В Виртуальные частные сети. Основы построения и применения, 2006
2. Мезенцев А.В. Технологии защищенной обработки информации, 2013
3. Ибе О. Сети и удаленный доступ: Протоколы, проблемы, решения, 2002; "Is this the same as Ad Hoc mode?". Archived from the original on 2013-08-30
4. "Wireless Distribution System Linked Router Network". DD-WRT Wiki. Archived from the original on June 30, 2017. Retrieved December 31, 2006
5. "How Wi-Fi Roaming Really Works". Archived from the original on 2019-02-23. Retrieved 2008-10-09
6. https://www.geeksforgeeks.org/wlan-full-form/
7. Bekzod, B., & Daeik, K. (2021). Face recognition based automated student attendance system. Turkish Journal of Computer and Mathematics Education, 12(11), 3531-3534
8. Ikromovich, H. O., & Mamatkulovich, B. B. (2023). Facial recognition using transfer learning in the deep cnn. Open Access Repository, 4(3), 502-507
9. Mamatkulovich, B. B. (2022, May). Automatic Student Attendance System Using Face Recogniton. In Next Scientists Conferences (pp. 6-22)
10. Mamatkulovich, B. B., Shuhrat o’g’li, M. S., & Jasurjonovich, B. J. (2023). SPECIAL DEEP CNN DESIGN FOR FACIAL EXPRESSION CLASSIFICATION WITH A SMALL AMOUNT OF DATA. Open Access Repository, 4(3), 472-478
11. Mamatkulovich, B. B. (2023). Alijon o’g’li HA Facial Image-Based Gender and Age Estimation. Eurasian Scientific Herald, 18, 47-50
12. Babakulov, B. (2023). UNİVERSİTET TALABALARİ UCHUN CHUQUR O'RGANİSHGA ASOSLANGAN YUZNİ ANİQLASHDAN FOYDALANGAN HOLDA AVTOMATİK DAVOMAT TİZİMİ. Инновационные исследования в современном мире: теория и практика, 2(3), 74-76