

WINDOWS SERVERDA MASOFAVIY KIRISH. DA, VPN YOKI AOVPN

Farg'ona davlat texnika universiteti
ATT kafedrası assistenti o'qituvchisi:
Nazirkulov Jamoldin Davlatjon o'g'li
FDTU 4-bosqich 55A-22 guruh
Sayidaliyev Muhammadiyor

Annotatsiya: Windows Server operatsion tizimida masofaviy kirishni tashkil etish usullari, jumladan DirectAccess (DA), Virtual Private Network (VPN) va Always On VPN (AOVPN) texnologiyalari ko'rib chiqiladi. Mazkur texnologiyalar foydalanuvchilarga korporativ tarmoqlarga xavfsiz va qulay masofaviy ulanish imkonini beradi. Ish davomida ushbu yechimlarning ishlash prinsipi, afzalliklari, kamchiliklari hamda amaliy qo'llanilish sohalari tahlil qilinadi.

Аннотация: В данной работе рассматриваются способы организации удалённого доступа в операционной системе Windows Server, включая технологии DirectAccess (DA), Virtual Private Network (VPN) и Always On VPN (AOVPN). Эти технологии обеспечивают безопасное и удобное подключение пользователей к корпоративным сетям из удалённых мест

Abstract: This paper examines remote access solutions in the Windows Server operating system, including DirectAccess (DA), Virtual Private Network (VPN), and Always On VPN (AOVPN) technologies. These solutions provide secure and reliable

remote connectivity to corporate networks. The study analyzes the working principles, advantages, disadvantages, and practical applications of each technology.

Kalit so'zlar: Windows Server, masofaviy kirish, DirectAccess, VPN, Always On VPN, tarmoq xavfsizligi, masofaviy ish.

Ключевые слова: Windows Server, удалённый доступ, DirectAccess, VPN, Always On VPN, сетевая безопасность, удалённая работа.

Keywords: Windows Server, remote access, DirectAccess, VPN, Always On VPN, network security, remote work.

Kirish

Hozirgi kunda global raqamli iqtisodiyot sharoitida tashkilotlar va kompaniyalar xodimlari turli joylardan ishlash imkoniyatiga ega bo'lishadi. Shu sababli korporativ tarmoqlarga masofaviy va xavfsiz kirishni ta'minlash muhim ahamiyat kasb etadi. Windows Server operatsion tizimi masofaviy kirish uchun bir nechta yechimlarni taqdim etadi, jumladan **DirectAccess (DA)**, **Virtual Private Network (VPN)** va **Always On VPN (AOVPN)** texnologiyalari. DirectAccess foydalanuvchilarga avtomatik va doimiy korporativ tarmoqqa ulanish imkonini beradi, VPN esa xavfsiz shifrlangan tunnel orqali internet orqali ulanishni ta'minlaydi. Always On VPN esa ushbu ikki yechimning eng zamonaviy ko'rinishi bo'lib, mobil va statik qurilmalarda barqaror va xavfsiz masofaviy ulanishni kafolatlaydi. Ushbu ishning maqsadi – Windows Server muhitida masofaviy kirish texnologiyalarini tahlil qilish, ularning afzalliklari va kamchiliklarini aniqlash hamda tashkilotlar uchun amaliy tavsiyalar ishlab chiqishdir. Tadqiqot natijalari korporativ tarmoqlarda xavfsiz va samarali masofaviy ish muhitini tashkil etishga xizmat qiladi. So'nggi o'n yilliklarda axborot texnologiyalari va global tarmoqlar tez sur'atlar bilan rivojlanib, xodimlar ish faoliyatini faqat ofis bilan cheklash emas, balki turli joylardan amalga oshirish imkoniyati paydo bo'ldi. Shu bilan birga, tashkilotlar va kompaniyalar uchun **masofaviy kirish** tizimlarini xavfsiz, barqaror va samarali tashkil etish dolzarb

muammo sifatida yuzaga chiqdi. Masofaviy kirish nafaqat ish jarayonlarining uzluksizligini ta'minlaydi, balki xodimlar ish unumdorligini oshirish, resurslardan samarali foydalanish va ish muhitini raqamlashtirish imkoniyatini yaratadi. Windows Server operatsion tizimi korporativ tarmoqlarga masofaviy ulanishni tashkil etish uchun bir nechta yechimlarni taklif qiladi. Ularning eng ko'p qo'llaniladiganlari quyidagilardan iborat. **Virtual Private Network (VPN)** – internet orqali xavfsiz va shifrlangan ulanishni tashkil qiladi. VPN korporativ tarmoqni himoya qiladi, tashqi foydalanuvchilar va filiallarni markaziy server bilan bog'lash imkoniyatini beradi. VPNning asosiy afzalligi uning moslashuvchanligi va keng tarqalganligi bo'lib, u ko'plab tashkilotlar tomonidan qo'llaniladi.



1. **DirectAccess** — Windows Enterprise bilan ishlaydigan, foydalanuvchi kompyuteri avtomatik tarzda korporativ tarmoq bilan ulanadigan texnologiya. Foydalanuvchi harakat qilmasa ham avtomatik ulanadi, doimiy ulanishni ta'minlaydi, IPv6 asosida ishlaydi va xavfsiz IPsec tunneli bilan ishlaydi. Kamchiligi shundaki, faqat Windows Enterprise/Ultimate bilan ishlaydi, konfiguratsiyasi murakkab va AD hamda PKI bilan integratsiya talab qiladi. Ishlatish maqsadlari — korporativ kompyuterlar va foydalanuvchilar Windows Enterprise ishlatadi, har doim ulanadigan va administrator nazoratida bo'lishi kerak bo'lgan tarmoq.
2. **2.VPN** — foydalanuvchining masofaviy joylashgan qurilmasini korporativ tarmoqqa xavfsiz ulanadigan tunneldan o'tkazadi. Windows Serverda

PPTP, L2TP/IPsec, SSTP va IKEv2 kabi turlari mavjud. Platformaga moslashuvchan, oddiy va tez sozlanadi. Kamchiligi foydalanuvchi har safar ulanadi yoki ulanishni avtomatlashtirish kerak, Always On imkoniyati yo‘q. Ishlatish maqsadlari — ko‘p turdagi qurilmalar mavjud bo‘lsa, oddiy, tezkor va universal masofaviy kirish kerak bo‘lsa.

3. **Always On VPN (AOVPN)** — Windows 10/11 va Windows Server 2016+ bilan ishlaydigan yangi VPN texnologiyasi, DirectAccess’ning zamonaviy alternativasi hisoblanadi. Doimiy ulanadi, foydalanuvchi interaktiv bo‘lmasa ham tarmoq bilan ulanadi, xavfsiz IKEv2/IPsec yoki SSTP tunnellari orqali ishlaydi. Device tunnel va User tunnel orqali tarmoq resurslariga qulay kirish ta’minlaydi. Kamchiligi faqat Windows qurilmalari uchun qulay, qo‘shimcha konfiguratsiya va sertifikat talab qiladi. Ishlatish maqsadlari — har doim avtomatik ulanadigan, xavfsiz va modern VPN kerak bo‘lsa, Windows 10/11 Enterprise muhitida.

4. **Qisqacha taqqoslash** DirectAccess foydalanuvchi uchun avtomatik, doimiy ulanish beradi, faqat Windows bilan mos, xavfsizligi yuqori. VPN foydalanuvchi uchun qo‘lda ulanadi, universal platformalarda ishlaydi, xavfsizligi turlicha, doimiy ulanish yo‘q. AOVPN foydalanuvchi uchun avtomatik, doimiy ulanish beradi, Windows qurilmalari uchun mos, xavfsizligi yuqori. DirectAccess Windows Enterprise bilan ishlaydi foydalanuvchi kompyuteri avtomatik tarzda korporativ tarmoq bilan ulanadi Harakat qilmasa ham ulanadi doimiy ulanishni ta’minlaydi IPv6 va IPsec orqali xavfsizlanadi Kamchiligi faqat Windows Enterprise bilan ishlaydi konfiguratsiyasi murakkab AD va PKI bilan integratsiya talab qiladi Ishlatish maqsadi korporativ kompyuterlar va foydalanuvchilar Windows Enterprise ishlatadi har doim ulanadigan va administrator nazoratida bo‘lgan tarmoq VPN foydalanuvchining masofaviy qurilmasini korporativ tarmoqqa xavfsiz ulanadigan tunneldan o‘tkazadi Windows Serverda PPTP L2TP/IPsec SSTP va IKEv2 turlari mavjud Platformaga moslashuvchan oddiy va tez sozlanadi Kamchiligi foydalanuvchi har safar ulanadi yoki avtomatlashtirish kerak Always On imkoniyati yo‘q Ishlatish maqsadi ko‘p turdagi qurilmalar mavjud bo‘lsa oddiy tezkor va universal

masofaviy kirish kerak bo'lsa Always On VPN AOVPN Windows 10 11 va Windows Server 2016+ bilan ishlaydi DirectAccess zamonaviy alternativasi Doimiy ulanadi foydalanuvchi interaktiv bo'lmasa ham tarmoq bilan ulanadi Xavfsiz IKEv2/IPsec yoki SSTP tunnellari orqali ishlaydi Device tunnel va User tunnel orqali tarmoq resurslariga qulay kirish Kamchiligi faqat Windows qurilmalari uchun qulay qo'shimcha konfiguratsiya va sertifikat talab qiladi Ishlatish maqsadi har doim avtomatik ulanadigan xavfsiz va modern VPN kerak bo'lsa Windows 10 11 Enterprise muhitida.



Windows Server muhitida masofaviy kirish tashkil qilishda asosiy maqsad foydalanuvchilarning korporativ resurslarga xavfsiz va qulay ulanishini ta'minlash hisoblanadi Masofaviy kirish uchun turli usullar mavjud jumladan DirectAccess VPN va Always On VPN AOVPN Har bir texnologiya o'z afzallik va cheklovlariga ega DirectAccess Windows Enterprise muhitida ishlaydi foydalanuvchi qurilmasi avtomatik ravishda tarmoqqa ulanadi foydalanuvchi hech narsa qilmaydi doimiy ulanishni ta'minlaydi IPsec xavfsizligi bilan ishlaydi Kamchiliklari konfiguratsiyasi murakkab Active Directory va PKI bilan integratsiya talab qiladi va faqat Windows qurilmalari uchun mos Ishlatish maqsadi korporativ kompyuterlar va foydalanuvchilar uchun avtomatik va xavfsiz ulanishni ta'minlash VPN esa keng tarqalgan va turli

platformalarda ishlaydi Windows macOS Linux va mobil qurilmalarda moslashuvchanlikni ta'minlaydi Foydalanuvchi ulanishni qo'lda ishga tushiradi VPN turli protokollar orqali ishlashi mumkin PPTP eski va xavfsiz emas L2TP IPsec va IKEv2 xavfsizroq SSTP esa HTTPS orqali firewall orqali oson o'tadi Kamchiliklari foydalanuvchi har safar ulanadi va Always On rejimi standartda yo'q Ishlatish maqsadi tez va universal masofaviy kirishni ta'minlash Qo'shimcha yondashuvlar sifatida masofaviy kirishni boshqarish uchun **Network Policy Server NPS, Routing and Remote Access Service RRAS va Azure AD integratsiyasi** ham ishlatiladi NPS yordamida foydalanuvchilar va qurilmalar autentifikatsiyalanadi RRAS esa VPN va DirectAccess xizmatlarini boshqaradi Azure AD bilan integratsiya masofaviy qurilmalarni bulut orqali xavfsiz boshqarish imkonini beradi Xulosa qilib aytganda masofaviy kirish yechimi tanlashda asosiy mezonlar foydalanuvchi platformasi xavfsizlik darajasi avtomatik ulanish talablari va boshqaruv soddaligidir DirectAccess doimiy va avtomatik ulanishni Windows Enterprise muhitida ta'minlaydi VPN universal va tezkor yechimdir AOVPN esa DirectAccess ning zamonaviy va xavfsiz alternativasi hisoblanadi

Xulosa

Windows Server muhitida masofaviy kirish tashkil qilish uchun uch asosiy yo'nalish mavjud DirectAccess VPN va Always On VPN AOVPN Har biri o'ziga xos afzallik va cheklovlarga ega DirectAccess Windows Enterprise muhitida doimiy va avtomatik ulanishni ta'minlaydi lekin faqat Windows qurilmalari bilan mos va konfiguratsiyasi murakkab VPN universal va turli platformalarda ishlaydi tez sozlanadi lekin foydalanuvchi har safar ulanadi va Always On rejimi standartda yo'q Always On VPN AOVPN esa DirectAccess ning zamonaviy alternativasi hisoblanadi doimiy va xavfsiz ulanish beradi lekin faqat Windows qurilmalari uchun qulay Masofaviy kirish yechimini tanlashda asosiy mezonlar foydalanuvchi platformasi xavfsizlik darajasi avtomatik ulanish talablari va boshqaruv soddaligidir Qo'shimcha yondashuvlar sifatida Network Policy Server NPS Routing and Remote Access Service RRAS va

Azure AD integratsiyasi ishlatiladi bu yechimlar foydalanuvchilarni autentifikatsiya qilish va masofaviy qurilmalarni xavfsiz boshqarish imkonini beradi

Foydalanilgan adabiyotlar va manbalar

- 1 Windows Server Documentation Microsoft Docs
- 2 Remote Access Overview Microsoft Learn
- 3 Always On VPN Deployment Guide Microsoft Docs
- 4 DirectAccess Planning and Deployment Microsoft Technet
- 5 VPN Types and Configuration in Windows Server Microsoft Docs
- 6 Network Policy Server NPS Overview Microsoft Docs
- 7 Routing and Remote Access Service RRAS Overview Microsoft Docs
- 8 Azure AD Integration for VPN Microsoft Learn