УДК 004.7

Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ GLOBALPROTECT, CISCO SECURE CLIENT ТА FORTICLIENT ДЛЯ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ В УМОВАХ КІБЕРЗАГРОЗ

У сучасних умовах гібридної організації праці та стрімкого зростання кіберзагроз, забезпечення захищеного віддаленого доступу стає критичним елементом корпоративної інформаційної безпеки. Традиційні VPN-рішення еволюціонують у бік Zero Trust Network Access (ZTNA), інтеграції з SASE (Secure Access Service Edge) та безперервної оцінки стану кінцевих пристроїв. Провідні рішення ринку – Palo Alto Networks GlobalProtect, Cisco Secure Client (AnyConnect) та Fortinet FortiClient – пропонують комплексні підходи до шифрованого віддаленого доступу, але відрізняються архітектурою, рівнем інтеграції з екосистемою та рівнем акценту на запобігання загроз.

GlobalProtect становить невід'ємну частину екосистеми Palo Alto Networks і забезпечує тісну інтеграцію з міжмережевими екранами наступного покоління (NGFW) та хмарною платформою Prisma Access. Рішення реалізує принципи Zero Trust Network Access (ZTNA 2.0), передбачаючи безперервну верифікацію ідентичності користувача, стану пристрою та контексту доступу. Архітектура базується на компонентах GlobalProtect Portal та GlobalProtect Gateway, що дає змогу здійснювати централізоване й узгоджене керування доступом у гібридних і хмарних середовищах.

Cisco Secure Client належить до найпоширеніших корпоративних клієнтів захищеного доступу. Рішення підтримує сучасні протоколи SSL/TLS та IPsec IKEv2, забезпечуючи високу сумісність із різноманітним мережевим обладнанням Cisco. Ключовою перевагою є глибока інтеграція з платформою Cisco Identity Services Engine (ISE) для оцінки стану пристроїв і динамічного контролю доступу, а також з Cisco Umbrella – для додаткового захисту на рівні DNS навіть поза активним VPN-з'єднанням.

FortiClient від компанії Fortinet позиціонується як уніфікований агент кінцевої точки (Fabric Agent), який поєднує функції захищеного віддаленого доступу, захисту від шкідливого програмного забезпечення та оцінки відповідності вимогам безпеки. Завдяки тісній інтеграції з екосистемою Fortinet Security Fabric рішення забезпечує наскрізну видимість і контроль загроз у гетерогенних IT-середовищах, дозволяючи динамічно застосовувати політики доступу.

Таблиця 1. Порівняльна характеристика рішень

	GlobalProtect	**Cisco Secure Client**	**FortiClient**
Протоколи	IPsec, SSL/TLS, ZTNA	SSL/TLS, IPsec IKEv2, ZTNA, DTLS	IPsec, SSL/TLS, ZTNA
MFA	SAML, RADIUS, сертифікати	SAML, RADIUS, RSA SecurID, Cisco Duo	SAML, FortiToken, RADIUS, сертифікати
Платформи	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android
Виявлення загроз	Інтеграція з WildFire	Cisco Talos Intelligence	FortiGuard Labs
Інструменти управління	Panorama, Prisma Access	Cisco SecureX, інтеграція з ISE/DNA Center	FortiClient EMS
Ліцензування	Підписка (включено до NGFW / Prisma Access)	Підписка за кількістю користувачів (Advantage / Premier)	Freemium (обмежена версія) + комерційна підписка

Рішення підтримують MFA та інтеграцію з IDP через SAML 2.0. GlobalProtect вирізняється застосуванням профілів стану хоста (HIP), що забезпечує динамічну адаптацію політик доступу на основі безперервного моніторингу кінцевих точок.

У контексті криптографічного захисту GlobalProtect та FortiClient реалізують ZTNA-тунелювання за стандартом TLS 1.3, тоді як Cisco Secure Client використовує протокол DTLS (на базі UDP) для оптимізації затримки та продуктивності.

Ефективність протидії загрозам базується на інтеграції з екосистемами вендорів: GlobalProtect використовує хмарну пісочницю WildFire, Cisco базується на аналітиці Talos Intelligence, а FortiClient акумулює уніфіковану телеметрію в межах Fortinet Security Fabric для наскрізного моніторингу гетерогенних середовищ.

Вибір рішення залежить від існуючої інфраструктури та пріоритетів безпеки. GlobalProtect є оптимальним для організацій, що потребують максимальної видимості трафіку та використовують інструменти аналізу загроз Palo Alto. Cisco Secure Client залишається стандартом для великих корпорацій зі складною мережевою структурою, де критичною є деталізація політик доступу. FortiClient часто представляє найкраще співвідношення "функціональність/вартість" для компаній, які шукають інтегроване рішення, що поєднує VPN та захист кінцевих точок.

Список використаних джерел

1. GlobalProtect. Palo Alto Networks | TechDocs Home. URL: https://docs.paloaltonetworks.com/globalprotect

2. Secure Client (including AnyConnect). Cisco. URL: https://www.cisco.com/site/us/en/products/security/secure-client/index.html

3. FortiClient 7.4. Fortinet Document Library | Home. URL: https://docs.fortinet.com/product/forticlient