

## **ЗАБЕЗПЕЧЕННЯ МОБІЛЬНОСТІ ТА ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ РІШЕНЬ PALO ALTO GLOBAL PROTECT**

У сучасному світі мобільність та віддалений доступ до корпоративних ресурсів стали невід'ємною частиною ведення бізнесу. Сучасні працівники все частіше працюють за межами офісу, перевіряючи електронну пошту з дому, оновлюючи корпоративні документи в подорожах, або виконуючи завдання з будь-якого місця, де є доступ до Інтернету. Така мобільність робочої сили підвищує продуктивність і гнучкість, але водночас створює значні ризики для безпеки. Кожного разу, коли користувачі залишають будівлю компанії зі своїми ноутбуками чи смартфонами, вони обходять корпоративний брандмауер та відповідні політики, які розроблені для захисту як користувача, так і мережі.

У цьому контексті, безпека і конфіденційність даних стають важливими аспектами, що потребують уваги. Існує багато різних рішень для забезпечення мобільності та віддаленого доступу. Одним з найпопулярніших сьогодні є Global Protect від Palo Alto Networks. Саме цей продукт стає ключовим для забезпечення захищеного та ефективного доступу до інформації.

Palo Alto Global Protect дозволяє організаціям захищати своїх мобільних співробітників, поширюючи платформу безпеки наступного покоління для всіх користувачів, незалежно від їх місця знаходження. За допомогою різноманітних функцій Global Protect забезпечує захист трафіку, здійснюючи аналіз програмного забезпечення, ідентифікацію користувачів та пристроїв, а також впроваджує передові технології для забезпечення реалізації політик безпеки.

Global Protect – це універсальне рішення, яке надає можливість різних сценаріїв свого використання [2], а саме:

- віддалений доступ з використанням технологій VPN;
- розширене запобігання загрозам;
- фільтрація URL-адрес;
- підтримка BYOD;
- реалізація концепції Zero Trust.

Global Protect надає безпечний шлюз для доступу до внутрішніх і хмарних додатків на гарантує, що конфіденційні дані залишаються захищеними під час передавання. Для інтернет-трафіку Global Protect діє як механізм захисту, що перехоплює та нейтралізує загрози, перш ніж вони зможуть проникнути в кінцеву точку. Він блокує доступ до шкідливих веб-сайтів, запобігає фішингу та крадіжці облікових даних, тим самим забезпечуючи захист кінцевих точок;

Global Protect контролює доступ до веб-сайтів та контенту в мережі. Це дозволяє організаціям ефективно виконувати політику безпеки та обмежувати ризики, пов'язані з некоректним використанням мережі; Підтримуючи VPN на рівні додатка для конфіденційності користувачів, Global Protect забезпечує безпечне підключення для різноманітних пристроїв, у тому числі керованих і некерованих. Він також дає змогу налаштовувати механізми автентифікації, адаптовані до конкретних типів пристроїв;

Застосовуючи модель безпеки нульової довіри Zero Trust, Global Protect забезпечує надійну ідентифікацію користувачів і надає детальний контроль над доступом до ресурсів, а також впроваджує багатофакторну автентифікацію для доступу до конфіденційних ресурсів, що підвищує рівень безпеки.

Global Protect забезпечує безперебійне застосування політики незалежно від місця розташування користувача. Ця платформа надає адміністраторам повний набір можливостей для ефективної боротьби з кіберзагрозами. Використовуючи такі технології, як App-ID і User-ID, організації можуть адаптувати політику на основі використання програми та профілів користувачів, забезпечуючи точний контроль над доступом до мережі. Крім того, такі функції, як розшифровка SSL і захист від зловмисного програмного забезпечення WildFire, дозволяють перехоплювати загрози та пом'якшувати їх у реальному часі, зміцнюючи захист від нових кіберзагроз.

Використання Palo Alto Global Protect надає значні переваги організаціям, які прагнуть покращити мобільність користувачів і можливості віддаленого доступу, а саме:

- покращена безпека;
- підвищена продуктивність;
- дотримання нормативних вимог;
- економічність.

Покращена безпека здійснюється за рахунок використання надійних протоколів шифрування Global Protect, багатофакторної автентифікації та заходів забезпечення безпеки кінцевих точок.

Розширене запобігання загрозам зменшує ризики безпеки, пов'язані з віддаленим доступом, захищаючи критичні активи від потенційних порушень або викрадання даних.

Підвищення продуктивності забезпечує безперебійний і безпечний доступ до корпоративних ресурсів з будь-якого місця чи пристрою, Global Protect підвищує продуктивність робочої сили, полегшуючи співпрацю та безперервність операцій незалежно від географічних обмежень.

Дотримання нормативних вимог допомагає організаціям дотримуватися нормативних вимог, запроваджуючи суворий контроль доступу, перевіряючи дії користувачів і ведучи повні журнали для звітування про відповідність.

Функції централізованого управління та масштабованості Global Protect мінімізують адміністративні накладні витрати та витрати на інфраструктуру, пов'язані з наданням віддаленого доступу, створюючи економічно ефективне рішення для організацій різного розміру.

Одним з основних сценаріїв використання Palo Alto Global Protect є забезпечення мобільності та віддаленого доступу користувачів до корпоративних ресурсів [1].

Основні кроки цього процесу:

1. Розгортання і конфігурація.
2. Аутентифікація та авторизація.
3. Шифрування трафіку.
4. Моніторинг та аналіз.
5. Підтримка мобільних пристроїв.

Розгортання та налаштування Global Protect в корпоративній мережі включає в себе встановлення серверів, налаштування політик безпеки та інтеграцію з існуючими інфраструктурними рішеннями. Платформа може бути розміщена в хмарі, на власному обладнанні або в гібридній конфігурації, що робить її ідеальним рішенням для організацій будь-якого розміру та потреб. Процес розгортання може бути значно спрощений завдяки автоматизації за допомогою скриптів та інструментів оркестрування.

Для забезпечення безпеки доступу, Global Protect використовує різні методи аутентифікації, такі як аутентифікація за допомогою логіну та пароля, сертифікатів, а також двофакторну аутентифікацію. Крім того, адміністратор може встановлювати правила доступу до різних ресурсів мережі, контролювати час та обсяги з'єднань, а також відслідковувати активність користувачів для виявлення потенційних загроз.

Однією з ключових функцій Global Protect є шифрування трафіку між клієнтом та сервером, що забезпечує конфіденційність інформації, яка передається по мережі. Global Protect використовує стійкі алгоритми шифрування для захисту даних, що передаються між клієнтом та сервером. Залежно від конфігурації, може бути зашифровано весь трафік або лише трафік до корпоративних ресурсів. Це гарантує конфіденційність інформації та захищає її від перехоплення та несанкціонованого доступу.

Global Protect надає адміністраторам потужні інструменти для моніторингу та аналізу активності користувачів та трафіку. Детальні журнали та звіти дають уявлення про те, хто, коли, як і до яких ресурсів отримує доступ. Моніторинг у реальному часі дозволяє негайно реагувати на будь-які підозрілі дії.

Global Protect розширює свою функціональність, надаючи безпеку не лише для користувачів настільних комп'ютерів, але і для мобільних пристроїв, таких як смартфони та планшети. Ця можливість дозволяє користувачам з легкістю отримувати доступ до корпоративних ресурсів навіть у русі, не обмежуючи їхньої продуктивності та забезпечуючи безпеку даних.

Таким чином, Global Protect стає життєво важливим компонентом операційної платформи безпеки Palo Alto Networks, що дає можливість організаціям розширювати надійну безпеку кінцевих точок і можливості віддаленого доступу для мобільних працівників. Використовуючи комплексні функції Global Protect і гнучкі варіанти розгортання, організації можуть ефективно пом'якшувати кіберризики та захищати критично важливі активи в дедалі динамічнішому середовищі загроз.

#### Список використаних джерел

1. Global Protect Overview. Palo Alto Networks | Tech Docs Home. URL: <https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview>
2. Palo Guard – Enterprise Security Platforms. Palo Alto Networks Products & Solutions | PaloGuard.com. URL: <https://www.paloguard.com/GlobalProtect.asp>