

## **БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА БЕЗПЕКА: РОЛЬ PFSense У ВИСОКОДОСТУПНИХ МЕРЕЖАХ**

Сучасні високодоступні мережі вимагають ефективного управління трафіком та високого рівня безпеки для забезпечення стабільності та надійності функціонування. PFSense виконує ключову роль у досягненні таких цілей, поєднуючи балансування навантаження та високий рівень безпеки.

Балансування навантаження є важливою функцією для високодоступних мереж, оскільки воно дозволяє розподіляти трафік між декількома серверами. Це може допомогти підвищити продуктивність мережі, оскільки трафік не надходить лише на один сервер. Балансування навантаження також може допомогти підвищити доступність мережі, оскільки якщо один сервер вийде з ладу, інший сервер зможе продовжувати обробляти трафік.

Основна мета балансування навантаження – це оптимізація використання ресурсів, максимізація пропускної здатності, зменшення часу відгуку і запобігання перевантаження будь-якого одного ресурсу. Використання декількох компонентів балансування навантаження, замість одного компонента, може значно підвищити надійність і доступність за рахунок резервування. Саме балансування навантаження передбачає, зазвичай, наявність спеціального програмного забезпечення або апаратних засобів, таких як багаторівневий комутатор або система доменних імен, серверний процес [1].

PFSense підтримує кілька методів балансування навантаження. Статичне балансування розподіляє трафік між серверами на основі статичного правила, наприклад, на основі IP-адреси або номера порту. Динамічне балансування розподіляє трафік між серверами на основі динамічних факторів, таких як навантаження на сервер або час відгуку. Балансування за допомогою IP-адрес розподіляє трафік між серверами на основі IP-адреси клієнта.

Безпека також є важливою для високодоступних мереж, оскільки вони є більш привабливими для хакерів. Зловмисники можуть використовувати високодоступні мережі для запуску атак на велику кількість користувачів.

PFSense надає широкий спектр функцій безпеки, які можуть допомогти захистити високодоступні мережі від атак. Фільтрація пакетів може блокувати несанкціонований трафік, який може використовуватися для запуску атак. PFSense підтримує широкий спектр правил фільтрації пакетів, які можна використовувати для блокування різних типів несанкціонованого трафіку. Системи виявлення та запобігання вторгненням (IDS/IPS) можуть виявляти та запобігати атакам, використовуючи різні методи. Віртуальні приватні мережі (VPN) можуть шифрувати трафік між пристроями, що перешкоджає зловмисникам відстежувати та атакувати його.

Для підвищення безпеки мережі за допомогою мережевого екрану PFSense рекомендується регулярно оновлювати програмне забезпечення, перевіряти журнали безпеки PFSense на наявність ознак атак, створювати резервні копії конфігурації PFSense.

Таким чином, PFSense – це потужний інструмент підвищення ефективності функціонування та безпеки високодоступних мереж.

В доповіді буде показано, як використовувати функції балансування навантаження та безпеки PFSense в процесі створення стійкої та захищеної мережі [2].

### **Список використаних джерел**

1. Динамічне балансування трафіку між декількома провайдерами. URL: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/12-7.pdf>
2. pfSense® – World's Most Trusted Open Source Firewall. URL: <https://www.pfsense.org/>