GIGACLOUD

Налаштування firewall в S-Cloud

Посібник користувача послугою

версія 1.1 6_2020

03022, Україна, м. Київ,
вул. Васильківська, 37-В

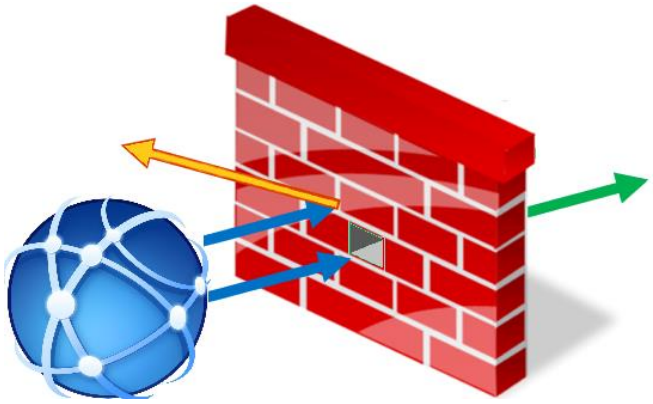
+38 (044) 233-71-70
sales@gigacloud.ua

www.gigacloud.ua

Зміст

Призначення мережевого екрану в S-Cloud

Призначення та принцип роботи мережевого екрану (також «**firewall**», «**файєрвол**» або «**брандмауер**» – «протипожежна стіна») подібні в мережах віртуальних та фізичних серверів, тому адміністрування локальної віртуальної мережі в S-Cloud не повинне викликати складнощів. Термін «**firewall**» позначає програмний чи програмно-апаратний елемент комп'ютерної мережі, який виконує контроль та фільтрацію трафіку через нього, згідно зі встановленими правилами.

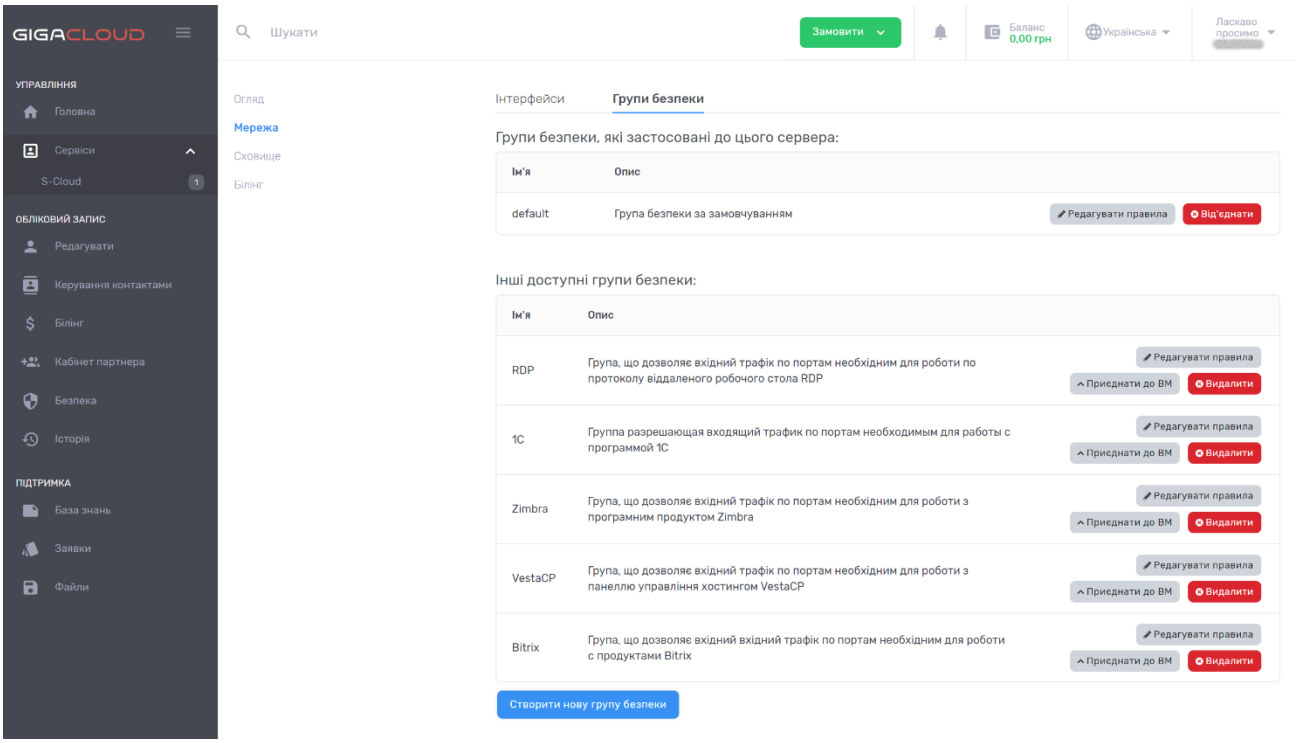


Завдяки налаштуванням **firewall**, дозволений трафік Інтернету пропускається через екран між мережами. **Решта з'єднань блокується** для захисту локальної мережі від небажаного трафіку та зловмисників.

Налаштування файєрвола віртуального серверу S-Cloud

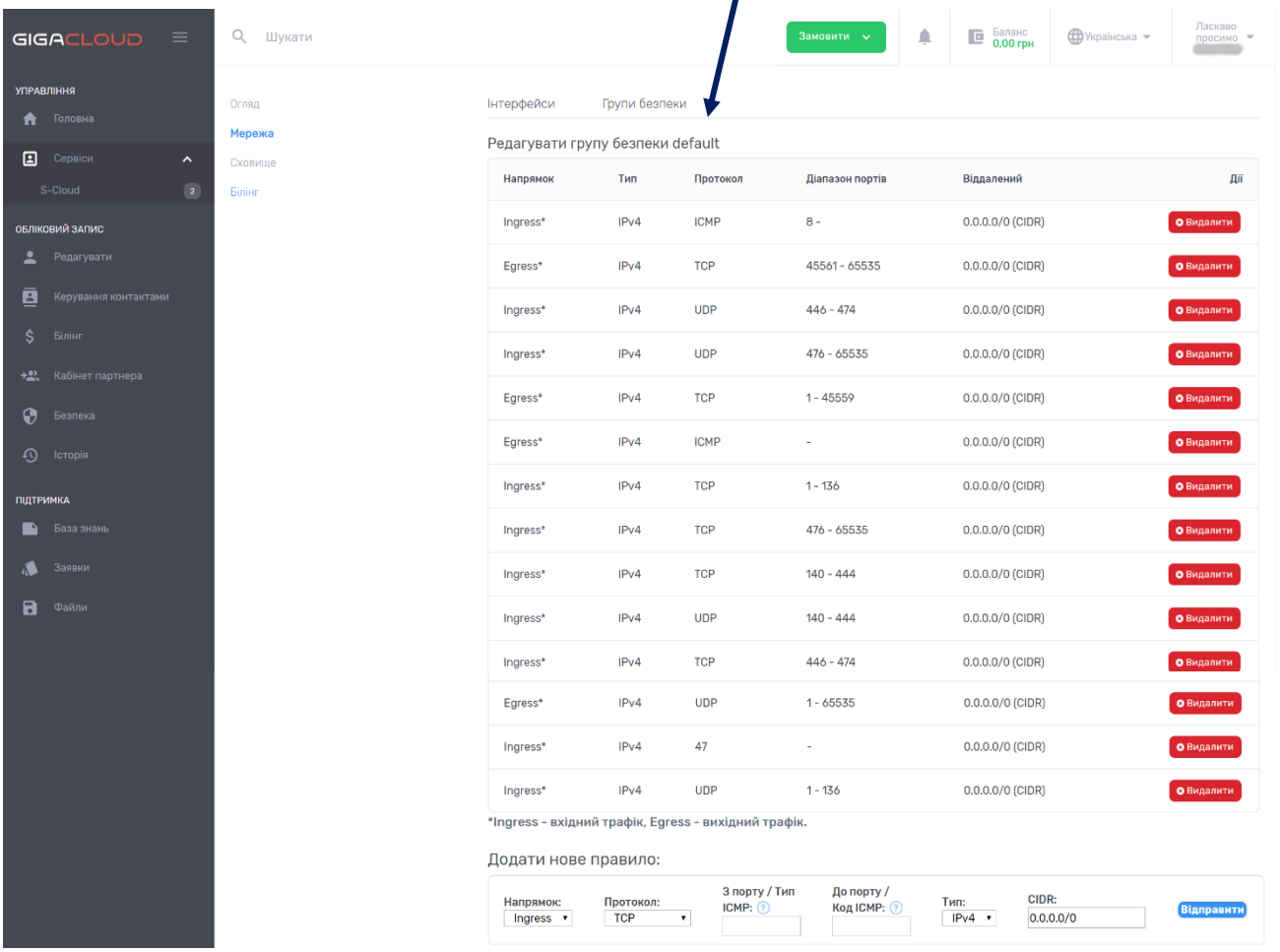
У Клієнтському порталі оберіть меню сервісу **S-Cloud** та потрібний віртуальний сервер.

Користуючись панеллю керування, оберіть розділ "**Групи безпеки**" вкладки "**Мережа**":



Інтуїтивно зрозумілий інтерфейс дозволяє швидко **приєднати до сервера готові шаблони груп безпеки**, що мають стандартні налаштування для роботи поширених сервісів (RDP, 1С та ін.) або **створити нову групу безпеки**.

Для створення та налаштування **firewall**, оберіть дію «**Редагувати правила**» групи безпеки «**default**», що містить початкові налаштування правил:



Згідно рекомендованої **політики безпеки** у мережі, виконайте наступні налаштування:

- видаліть всі наявні у переліку правила **Ingress** (вхідний трафік);
- додайте нові правила, що дозволяють трафік лише для забезпечення роботи необхідних служб.

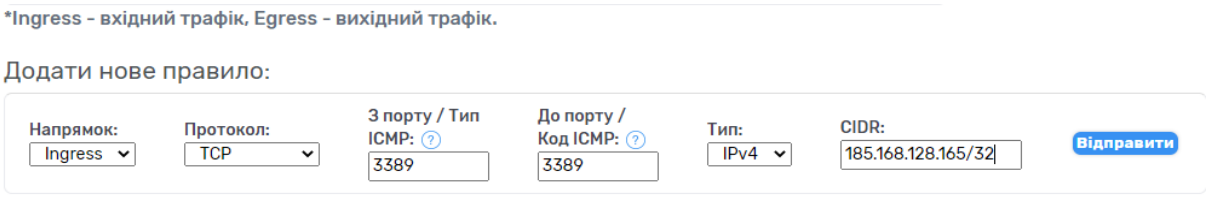
Увага! Для максимальної безпеки замість початкового налаштування «0.0.0.0/0» («дозволяються всі IP-адреси») у полі налаштувань CIDR вкажіть власну IP-адресу, з якої ви дозволяєте встановити з'єднання під час підключення до віртуального сервера.

Наприклад, для роботи панелі керування хостінгом **VestaCP** потрібно відкрити додаткові порти:

- 25 – SMTP;
- 143 – IMAP;
- 8083 – Веб-інтерфейс панелі VestaCP.

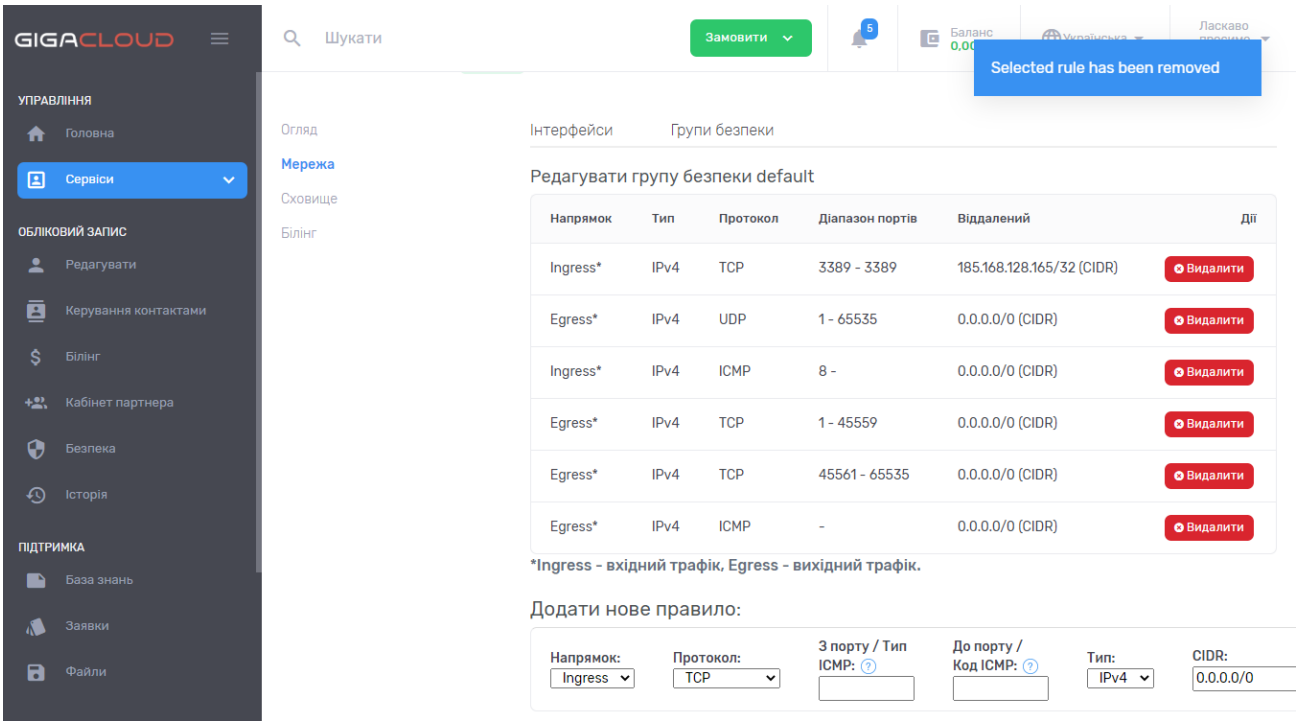
Приклад налаштування підключення по RDP

Окрім автоматизованого використання готового шаблону групи безпеки RDP, можливо налаштувати групи «**default**» власноруч:



Порт 3389 є стандартним для підключення по RDP (значення 3389 може бути змінено на нестандартне з метою підвищення безпеки з'єднання). У полі «**CIDR**» (Classless Inter-Domain Routing або «безкласова адресація») вкажіть ваше власне значення дозволеної адреси IP.

Переконайтеся, що налаштування після **видалення зайвих** вхідних правил (**Ingress**) та дозволу роботи **тільки необхідних вам служб** подібні наведеному нижче (за винятком адреси IP):

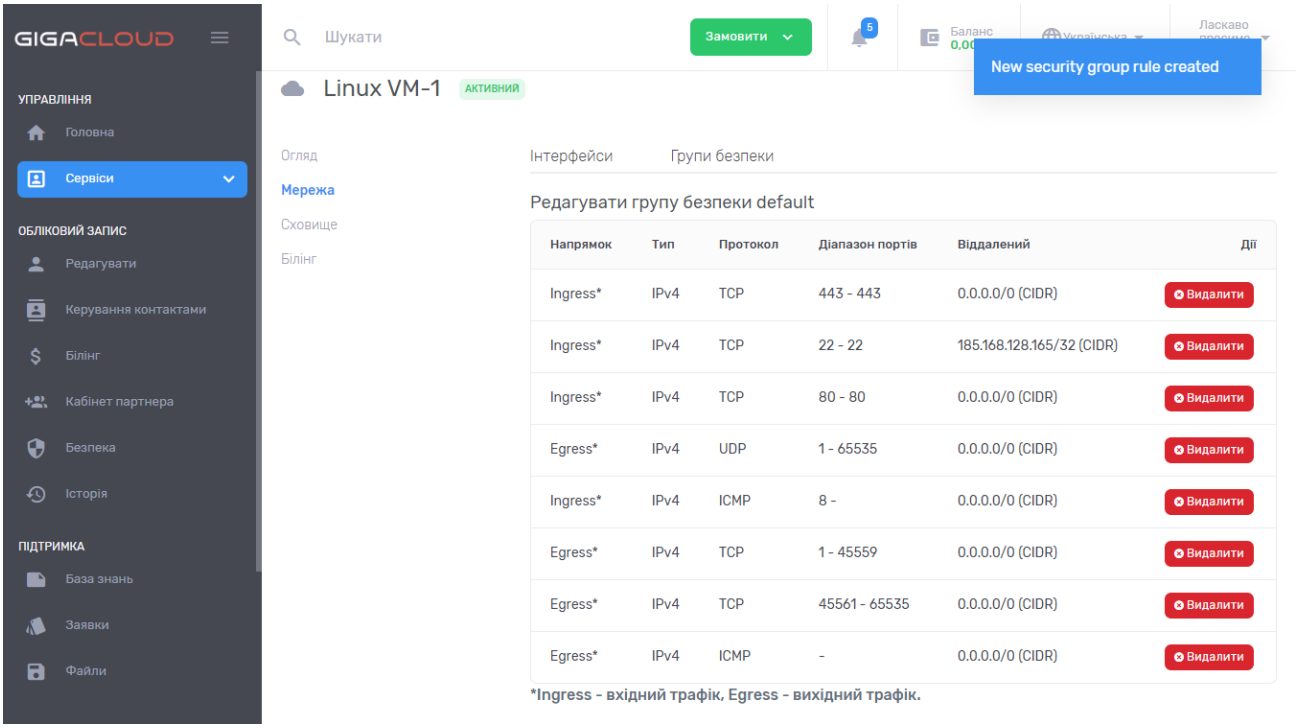


Правила групи безпеки «**default**» (див. 6 послідовних рядків таблиці на зображенні вище) встановлюють наступне:

1 – Ingress, визначає IP-адресу і порт, з яких дозволене підключення по RDP до сервера;
2 – Egress, визначає діапазон дозволених UDP портів;
3 – Ingress, дозволяє з'єднання за вхідним міжмережевим протоколом керуючих повідомлень (Ping та Traceroute);
4 та 5 – Egress, визначають діапазони дозволених TCP портів;
6 – Egress, дозволяє з'єднання за вихідним міжмережевим протоколом керуючих повідомлень (Ping та Traceroute).

Приклад налаштування підключення по SSH

У випадку необхідності підключення до віртуального сервера по SSH, виконайте налаштування згідно наведеного (вкажіть у полі CIDR ваше значення дозволеної адреси IP):



Правила групи безпеки «**default**» (див. 8 послідовних рядків таблиці на зображенні вище) встановлюють наступне:

1 – Ingress, визначає вхідний порт протоколу HTTPS;
2 – Ingress, визначає IP-адресу і порт, з яких дозволене підключення по SSH до сервера;
3 – Ingress, визначає вхідний порт протоколу HTTP;
4 – Egress, діапазон дозволених UDP портів;
5 – Ingress, дозволяє з'єднання за вхідним міжмережевим протоколом керуючих повідомлень (Ping та Traceroute);
6 та 7 – Egress, визначають діапазон дозволених TCP портів;
8 – Egress, дозволяє з'єднання за вихідним міжмережевим протоколом керуючих повідомлень (Ping та Traceroute).