

GIGA CLOUD

# 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

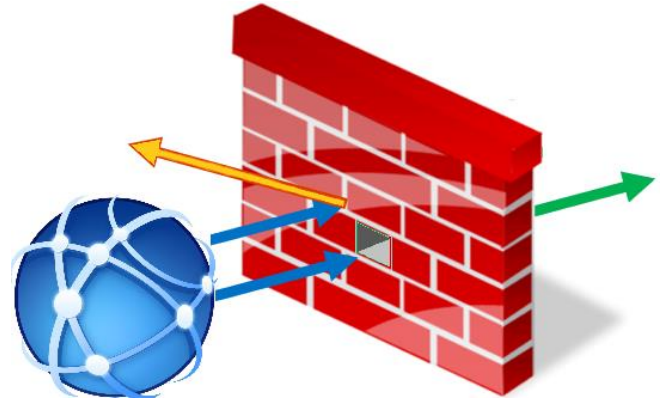
[www.gigacloud.ua](http://www.gigacloud.ua)

## Зміст

Призначення мережевого екрану в S-Cloud.....	3
Налаштування файрвола віртуального серверу S-Cloud .....	3
Приклад налаштування підключення по RDP .....	5
Приклад налаштування підключення по SSH.....	6

## Призначення мережевого екрану в S-Cloud

Призначення та принцип роботи мережевого екрану (також «**firewall**», «**файєрвол**» або «**брандмауєр**» – «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**»:

Інтерфейси **Групи безпеки**

Групи безпеки, які застосовані до цього сервера:

Ім'я	Опис	Дії
default	Група безпеки за замовчуванням	Редагувати правила   Відєднати

Інші доступні групи безпеки:

Ім'я	Опис	Дії
RDP	Група, що дозволяє вхідний трафік по портам необхідним для роботи по протоколу віддаленого робочого стола RDP	Редагувати правила   Приєднати до VM   Видалити
1C	Група разрешающая входящий трафик по портам необходимым для работы с программой 1C	Редагувати правила   Приєднати до VM   Видалити
Zimbra	Група, що дозволяє вхідний трафік по портам необхідним для роботи з програмним продуктом Zimbra	Редагувати правила   Приєднати до VM   Видалити
VestaCP	Група, що дозволяє вхідний трафік по портам необхідним для роботи з панеллю управління хостингом VestaCP	Редагувати правила   Приєднати до VM   Видалити
Bitrix	Група, що дозволяє вхідний трафік по портам необхідним для роботи з продуктами Bitrix	Редагувати правила   Приєднати до VM   Видалити

Створити нову групу безпеки

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

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

Скріншот інтерфейсу управління фаєрволом у GIGACLOUD. Ліва панель містить меню: УПРАВЛІННЯ (Головна, Служби, S-Cloud), ОБЛІКОВИЙ ЗАПИС (Редагувати, Керування контактами, Білінг, Кабінет партнера), БЕЗПЕКА (Безпека, Історія), ПІДТРИМКА (База знань, Заявки, Файли). Основна частина екрана показує налаштування групи безпеки 'default'. Таблиця правил:

Напрямок	Тип	Протокол	Діапазон портів	Віддалений	Дії
Ingress*	IPv4	ICMP	8 -	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	UDP	446 - 474	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	UDP	476 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	1 - 136	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	476 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	140 - 444	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	UDP	140 - 444	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	446 - 474	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	47	-	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	UDP	1 - 136	0.0.0.0/0 (CIDR)	Видалити

\*Ingress - вхідний трафік, Egress - вихідний трафік.

Додати нове правило:

Напрямок: Ingress, Протокол: TCP, З порту / Тип ІСМР: [ ], До порту / Код ІСМР: [ ], Тип: IPv4, CIDR: 0.0.0.0/0, Відправити

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:

\*Ingress - вхідний трафік, Egress - вихідний трафік.

Додати нове правило:

Напрямок: Ingress	Протокол: TCP	З порту / Тип ICMP: ? 3389	До порту / Код ICMP: ? 3389	Тип: IPv4	CIDR: 185.168.128.165/32	<b>Відправити</b>
----------------------	------------------	----------------------------------	-----------------------------------	--------------	-----------------------------	-------------------

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):

Напрямок	Тип	Протокол	Діапазон портів	Віддалений	Дії
Ingress*	IPv4	TCP	3389 - 3389	185.168.128.165/32 (CIDR)	<b>Видалити</b>
Egress*	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	<b>Видалити</b>
Ingress*	IPv4	ICMP	8 -	0.0.0.0/0 (CIDR)	<b>Видалити</b>
Egress*	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	<b>Видалити</b>
Egress*	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	<b>Видалити</b>
Egress*	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	<b>Видалити</b>

\*Ingress - вхідний трафік, Egress - вихідний трафік.

Додати нове правило:

Напрямок: Ingress	Протокол: TCP	З порту / Тип ICMP: ?	До порту / Код ICMP: ?	Тип: IPv4	CIDR: 0.0.0.0/0
----------------------	------------------	--------------------------	---------------------------	--------------	--------------------

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 міжмережєвим протоколом керуючих повідомлень (Ping та Traceroute);
- 4 та 5 – Egress, визначають діапазони дозволених TCP портів;
- 6 – Egress, дозволяє з'єднання за вихідним міжмережєвим протоколом керуючих повідомлень (Ping та Traceroute).

## Приклад налаштування підключення по SSH

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

Напрямок	Тип	Протокол	Діапазон портів	Віддалений	Дії
Ingress*	IPv4	TCP	443 - 443	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	22 - 22	185.168.128.165/32 (CIDR)	Видалити
Ingress*	IPv4	TCP	80 - 80	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	ICMP	8 -	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити

\*Ingress - вхідний трафік, Egress - вихідний трафік.

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).

