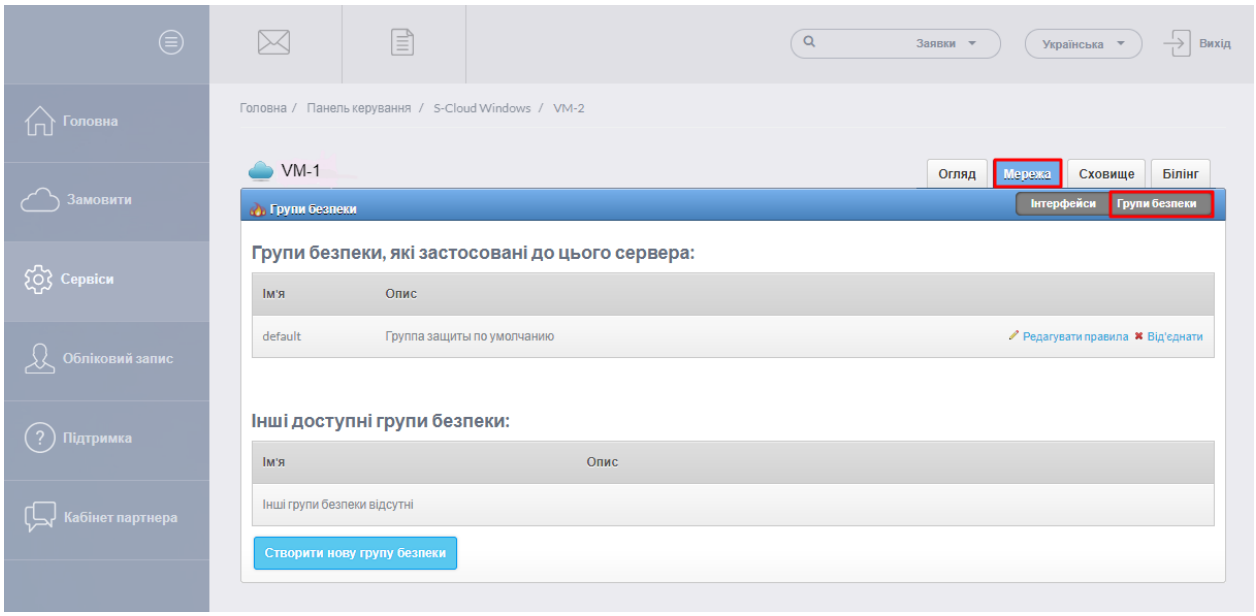
S-Cloud. Групи безпеки.

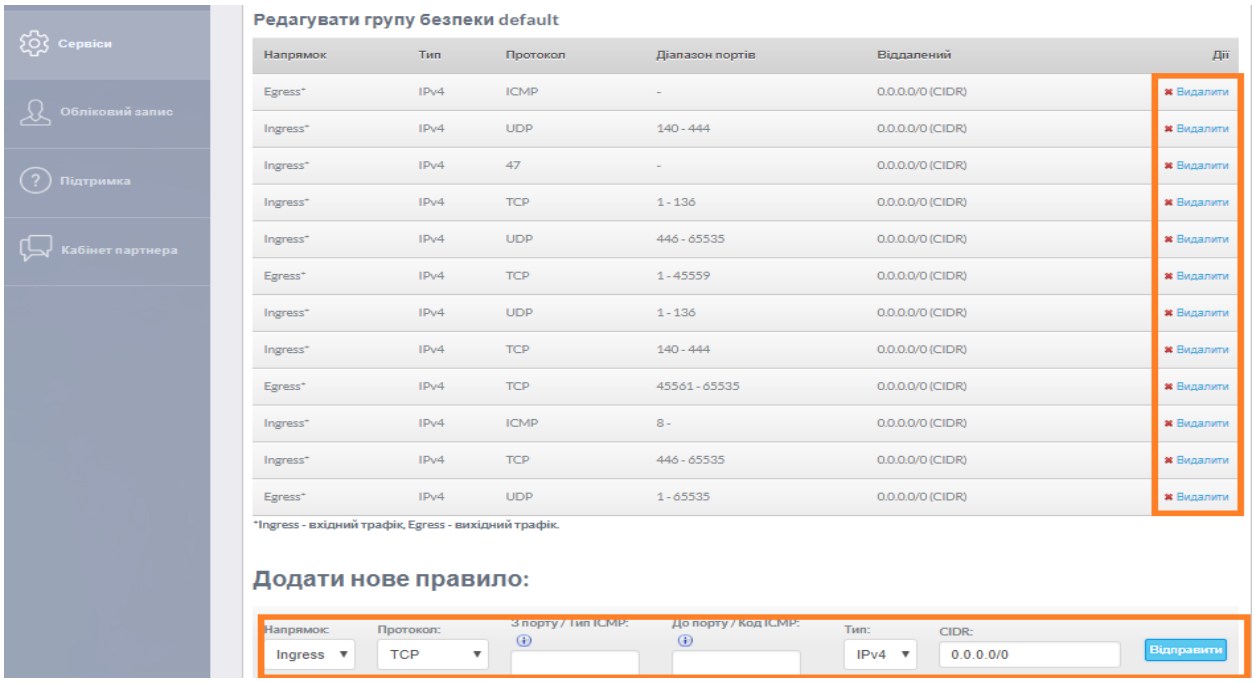
У вкладці “Мережа” ви можете налаштувати файєрвол на сервері (розділ “Групи безпеки”), натиснувши «Редагувати правила»:



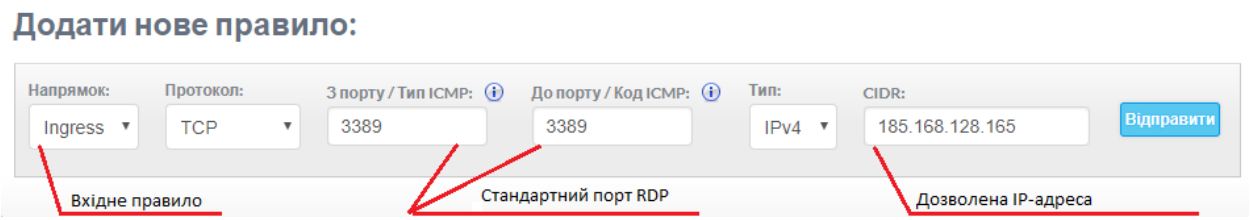
Налаштування Firewall

Створення firewall'а починається з визначення політики безпеки в тій мережі, для якої він розроблюється. Для цього:

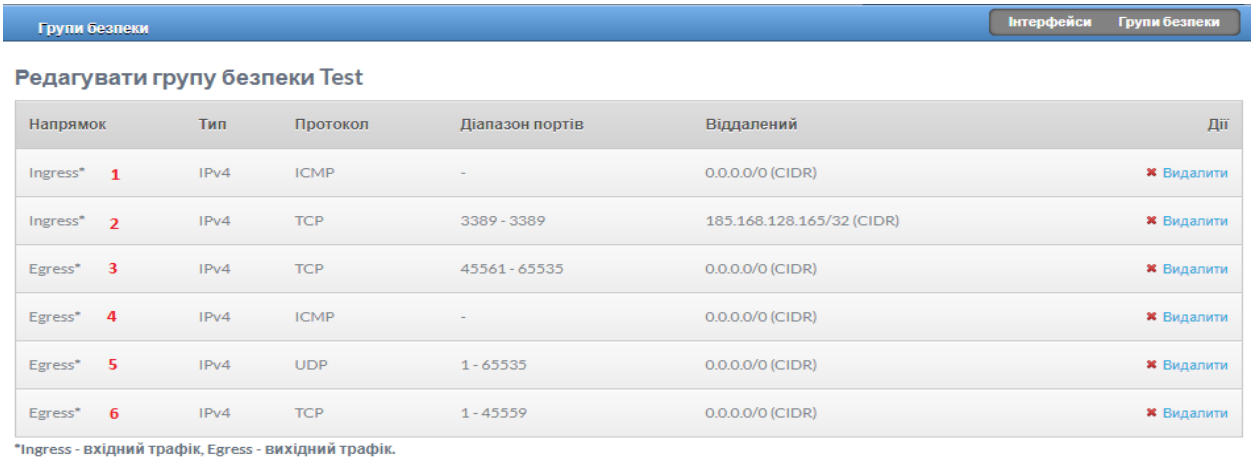
- видаліть <u>всі</u> правила **Ingress** (вхідні),
- дозвольте службі, що використовуються.



Для максимальної безпеки завжди рекомендуємо вказати IP-адресу, з якої Ви підключаєтеся до ВМ.



Приклад 1. Налаштування підключення по RDP



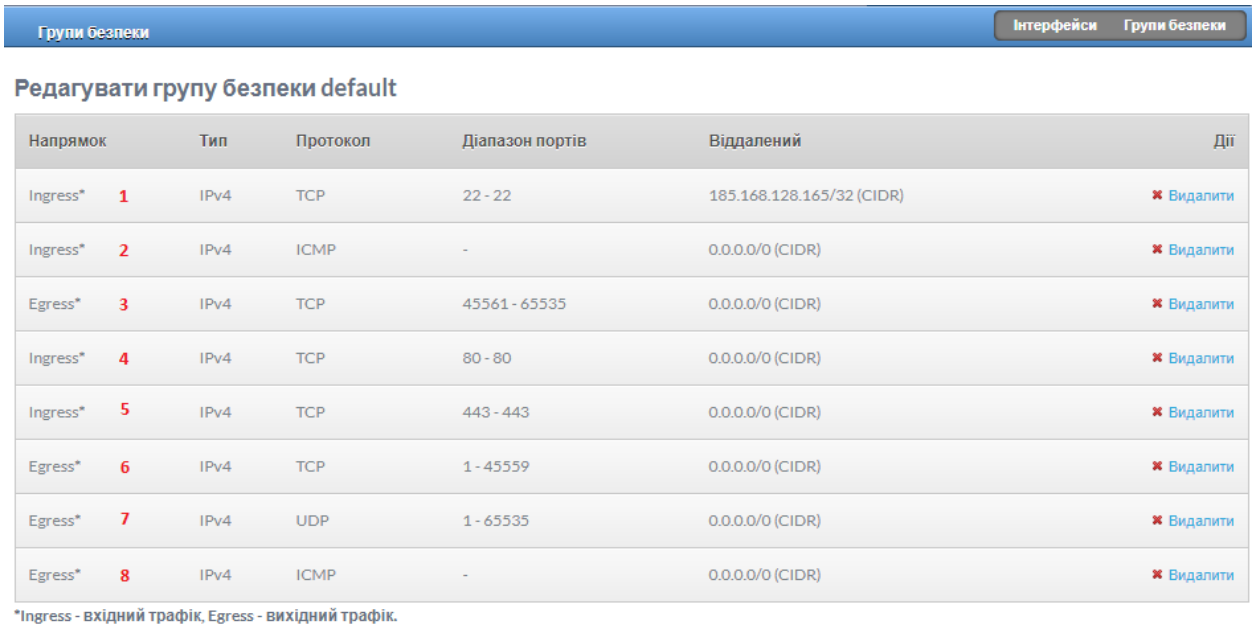
Напрямок	Тип	Протокол	Діапазон портів	Віддалений	Дії
Ingress* 1	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити
Ingress* 2	IPv4	TCP	3389 - 3389	185.168.128.165/32 (CIDR)	Видалити
Egress* 3	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress* 4	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити
Egress* 5	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress* 6	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	Видалити

*Ingress - вхідний трафік, Egress - вихідний трафік.

Правила:

1) (Вхідний) міжмережевий протокол керуючих повідомлень (Ping та Traceroute).
2) IP-адреса і порт з яких дозволене підключення до VM по RDP.
3) Діапазон дозволенних TCP портів.
4) (Вихідний) міжмережевий протокол керуючих повідомлень (Ping та Traceroute).
5) Діапазон дозволенних UDP портів.
6) Діапазон дозволенних TCP портів.

Приклад 2. Налаштування підключення по SSH



Напрямок		Тип	Протокол	Діапазон портів	Віддалений	Дії
Ingress*	1	IPv4	TCP	22 - 22	185.168.128.165/32 (CIDR)	Видалити
Ingress*	2	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити
Egress*	3	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	4	IPv4	TCP	80 - 80	0.0.0.0/0 (CIDR)	Видалити
Ingress*	5	IPv4	TCP	443 - 443	0.0.0.0/0 (CIDR)	Видалити
Egress*	6	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	Видалити
Egress*	7	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress*	8	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити

*Ingress - вхідний трафік, Egress - вихідний трафік.

1) IP-адреса і порт з яких дозволене підключення до VM по SSH.
2) (Вхідний) міжмережевий протокол керуючих повідомлень (Ping та Traceroute)
3) Діапазон дозволенних TCP портів.
4) Вхідний порт протоколу HTTP.
5) Вхідний порт протоколу HTTPS.
6) Діапазон дозволенних TCP портів.
7) Діапазон дозволенних UDP портів.
8) (Вихідний) міжмережевий протокол керуючих повідомлень (Ping та Traceroute)

Наприклад для VestaCP потрібно відкрити додаткові порти:

1) 25 – SMTP
2) 143 - IMAP
3) 8083 – Веб-інтерфейс VestaCP.