GIGACLOUD

Distributed Firewall (DFW) у хмарі GigaCloud

Посібник адміністратора

версія 1.2 10_2023

+380 44 233 7170
www.gigacloud.ua

Зміст

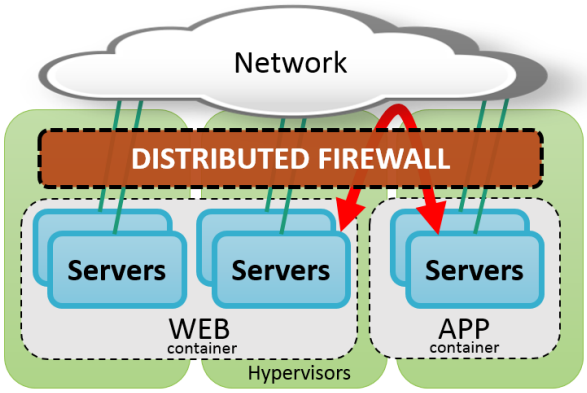
Особливості розподіленого файєрвола (DFW) у групах ЦОДів (DCG) 3
Створення групи ЦОДів (Data Center Group) 4
Створення правил розподіленого файєрвола 7
Редагування правил DFW 12

Особливості розподіленого файєрвола (DFW) у групах ЦОДів (DCG)

Впровадження рішення NSX-T програмно-визначеної мережевої платформи віртуалізації та системи безпеки мережевих сервісів надає принципово нові можливості: **об'єднання одного або декількох віртуальних дата-центрів VDC одного орендаря в групи ЦОДів (Data Center Group, DCG)** – до 16 VDC в одній DCG. Створення таких DCG передбачає розширені мережеві функції для об'єднаних ними VDC:

- централізоване мережеве адміністрування;
- утворення централізованої точки виходу;
- внутрішній трафік «East-West» між окремими вузлами в DCG;
- розподілений файєрвол (Distributed Firewall, DFW), що може застосовуватися в динамічних групах – тепер у правилах можна використовувати мітки безпеки, імена ВМ або назви ОС, а не лише статичні групи та набори IP-адрес.

Політика безпеки розподіленого файєрвола (брандмауера) визначається централізовано через API за допомогою поняття логічних "контейнерів" (робочі навантаження розміщуються в контейнерах програмно, а функції забезпечення безпеки програмується в ядрах гіпервізора). Правила безпеки базуються на приналежності до контейнера, а не на IP-адресах (наприклад, об'єкти в контейнері "WEB" можуть спілкуватися з контейнером "APP" через певний TCP-порт X, див. схему на мал. нижче):



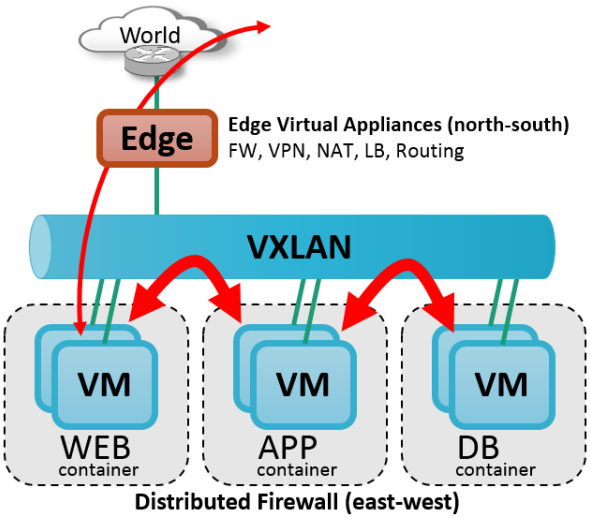
Приналежність ВМ до контейнера може бути статичною або динамічною, запрограмованою на спрацьовування певних метаданих про робоче навантаження, наприклад:

- ідентифікатор користувача;
- наявність вірусу;
- характеристики операційної системи та застосунків, що використовуються та ін.

Внаслідок, адміністратор мережі може обмежувати трафік між окремими групами ВМ, не потребуючи доступу ззовні до операційних систем кожної з цих ВМ, а правила DFW будуть автоматично розповсюджуватись і на майбутні нові ВМ у групах, що відповідають параметрам правила. **Таким чином, за своїми можливостями DFW суттєво відрізняється від традиційних фізичних або віртуальних файєрволів (брандмауерів):**

- реалізація безпеки відокремлена від мережевої архітектури – DFW присутній вже у ядрі гіпервізора та підключається безпосередньо до робочих навантажень;
- кожний надісланий або отриманий ВМ пакет проходить через брандмауер зі збереженням стану та перевіряється ще до потрапляння в мережу;
- політика безпеки мігрує разом із ВМ при міграції робочого навантаження на інший гіпервізор, а правила безпеки відокремлені від IP-адресації (IP-адреса ваших віртуальних машин може змінюватися без зміни політики безпеки).

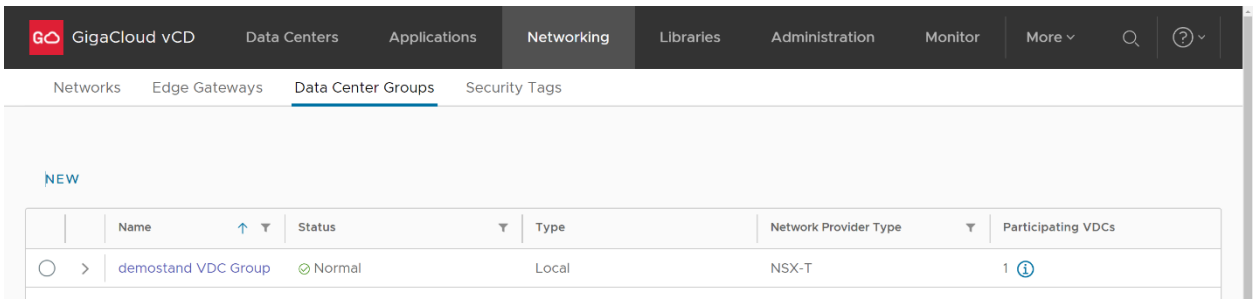
Водночас, DFW може поєднуватися в загальному рішенні з іншими файєрволами (брандмауерами), де правила застосовуються на портах фізичних або віртуальних маршрутизаторів – наприклад, на роутері Edge (див. схему на мал. нижче):



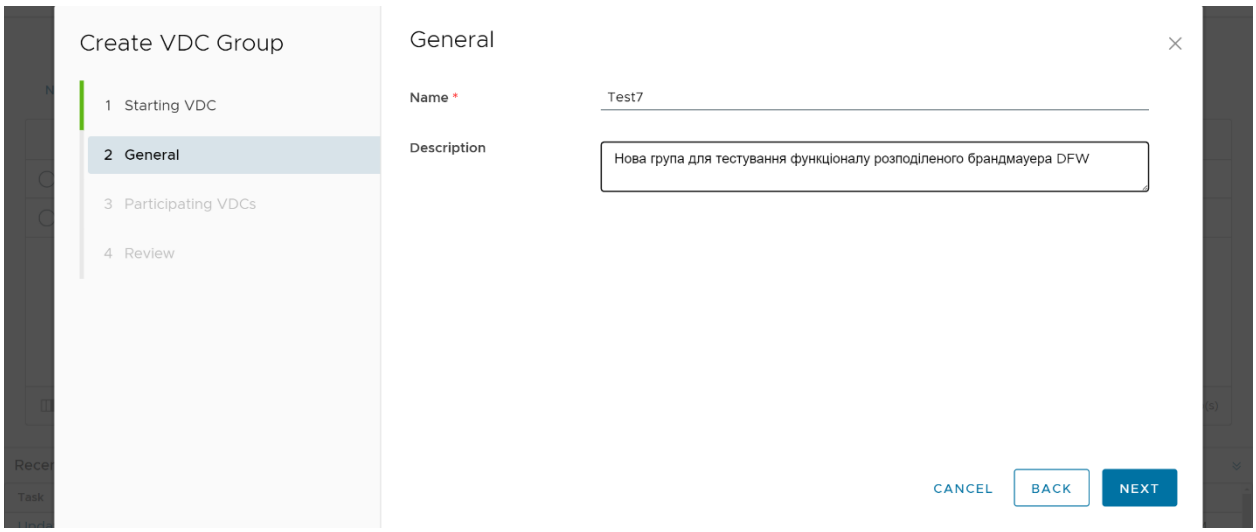
Створення групи ЦОДів (Data Center Group)

Для початку роботи з DFW, орендар хмарної інфраструктури повинен перейти до веб-інтерфейсу VMware Cloud Director (VCD) і створити щонайменше одну групу ЦОДів.

У верхній панелі навігації VCD оберіть вкладку «Networking» і перейдіть на вкладку меню «Data Center Groups» (групи ЦОДів):

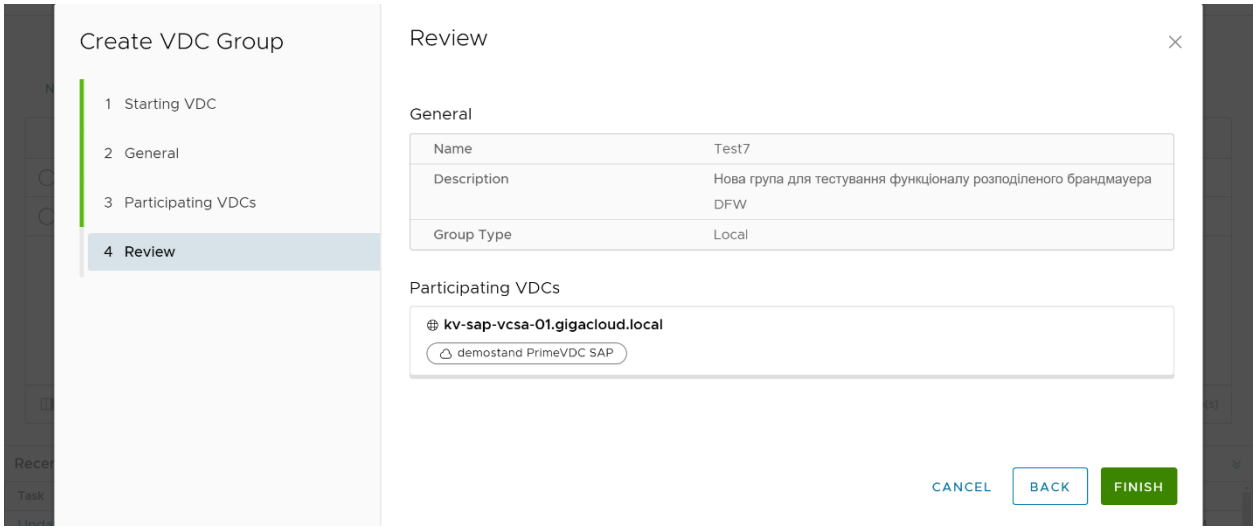


Натисніть кнопку «NEW» для створення нової групи та пройдіть послідовність кроків, користуючись інтуїтивно зрозумілим екранним інтерфейсом:

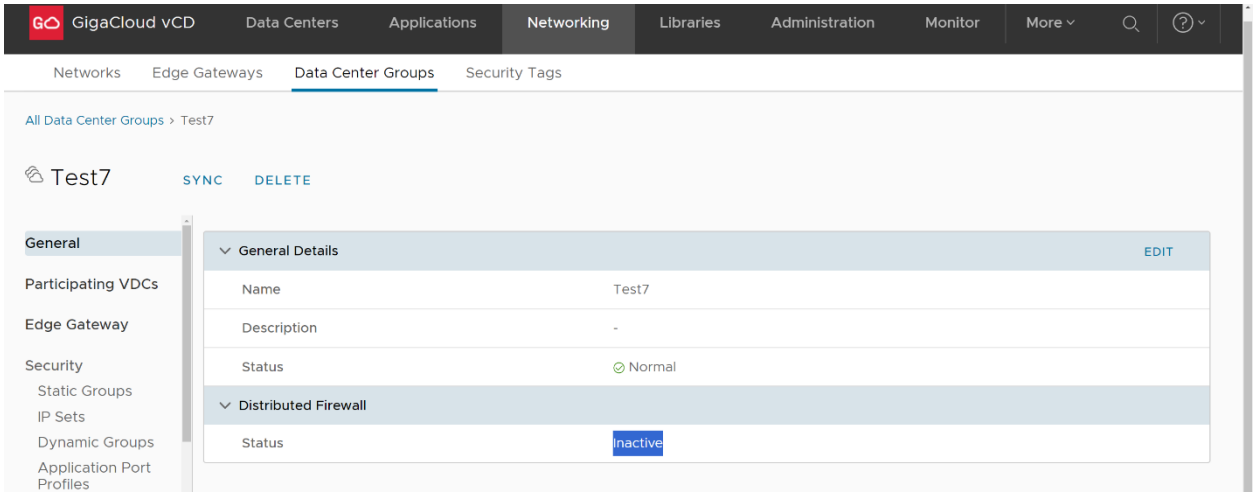


Екранна кнопка «NEXT» призначена для переходу до наступного вікна, а кнопка «BACK» – для повернення до попереднього кроку (з метою зміни налаштувань параметрів).

Пересвідчіться у вірності введених значень та завершіть створення групи натисканням кнопки «FINISH»:

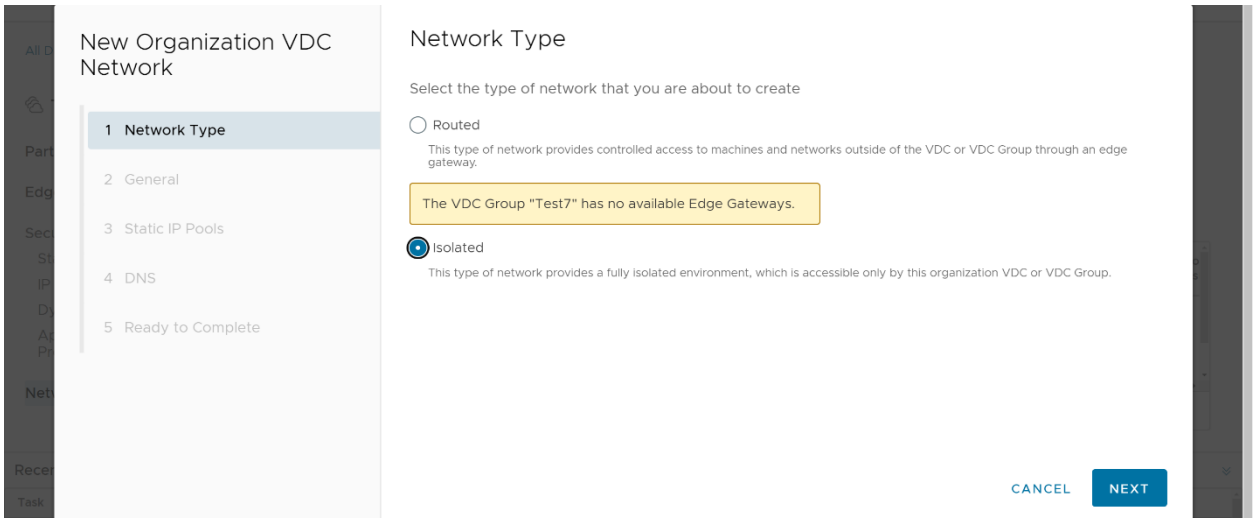


Обов'язковою дією є активація провайдером DFW у новій групі центру обробки даних, оскільки за використання функції DFW з орендаря може стягуватися додаткова плата.



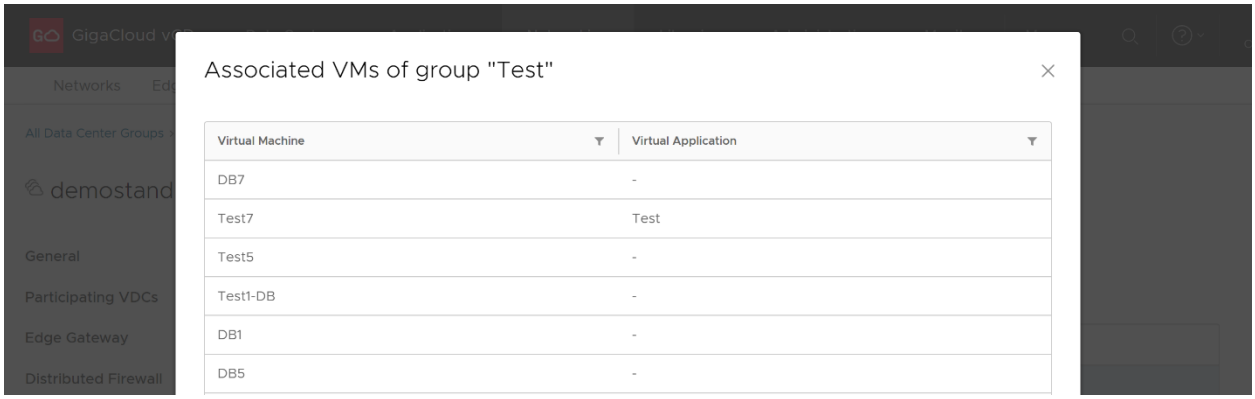
Після активації DFW провайдером, додайте мережі до DCG, що діє як межа сфери дії (або досяжності правил) DFW. Якщо ВМ підключена до мережі, що не додана до DCG, правила DFW не застосовуватимуться до цієї віртуальної машини.

За допомогою панелі керування, додайте мережу до DCG – створіть нову мережу або імпортуйте вже існуючу мережу Org VDC.

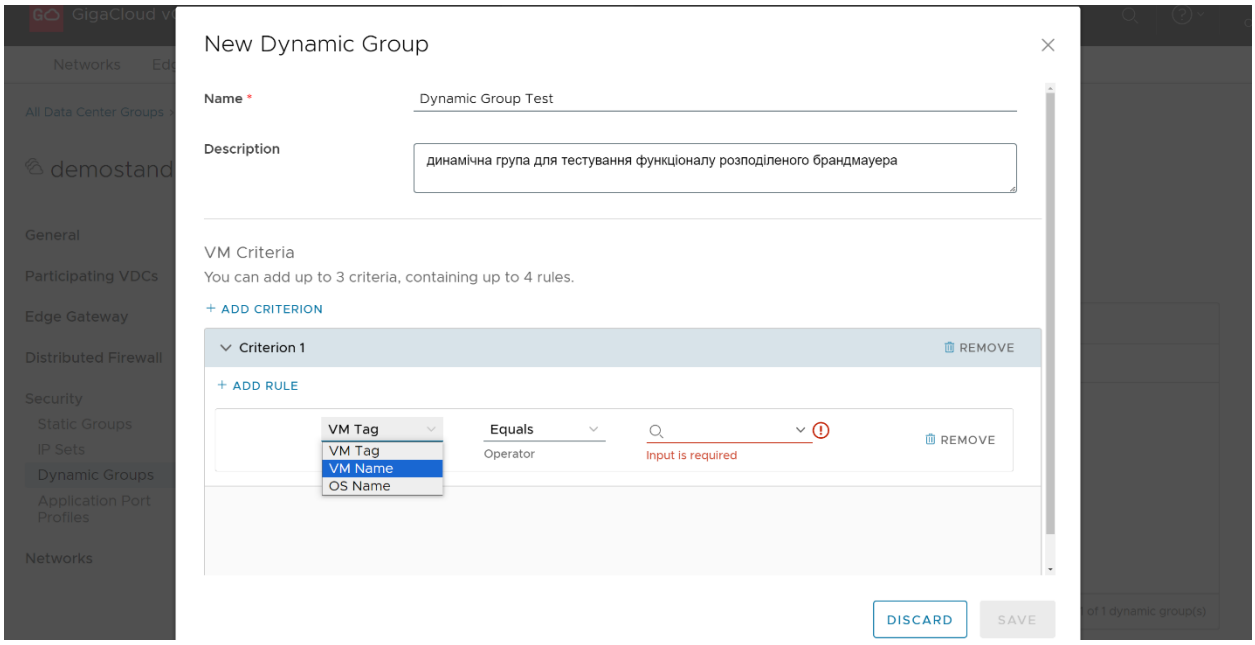


Перед створенням правил DFW, необхідно попередньо створити групи ВМ або набори IP-адрес. Використовуючи панель керування VCD, групування можна виконати декількома способами:

- на основі статичних груп (Static Groups), до яких додається одна або декілька мереж. При використанні статичної групи в правилі DFW – таке правило застосовується до всіх ВМ, що приєднані до мереж в групі. За допомогою пункту меню "ASSOCIATED VMS" можна перевірити, які віртуальні машини підключено до мереж у статичній групі;



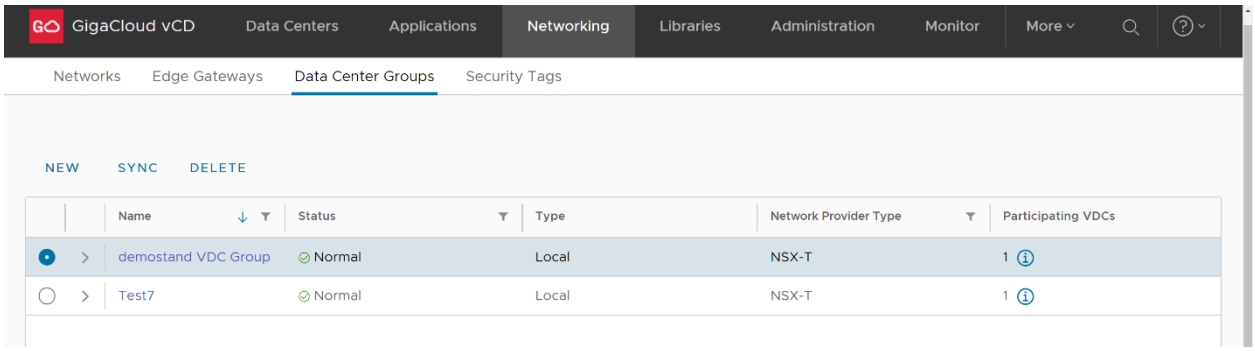
- на основі наборів IP-адрес (IP Sets) – для групування ресурсів поза межами організації VCD (наприклад, у глобальній мережі компанії, коли додавання IP-адрес або підмереж є єдиним способом їх групування);
- на основі динамічних груп (Dynamic Groups) для групування ВМ на основі певної ключової ознаки – мітки безпеки, імені ВМ або назви OS (операційної системи). При створенні динамічної групи, на початку вона має один критерій і правило належності до групи. За потреби, це можна розширити до 3 критеріїв, із 4 правилами для кожного (кілька критеріїв діють як оператор OR, кілька правил в межах одного критерію діють як оператор AND);



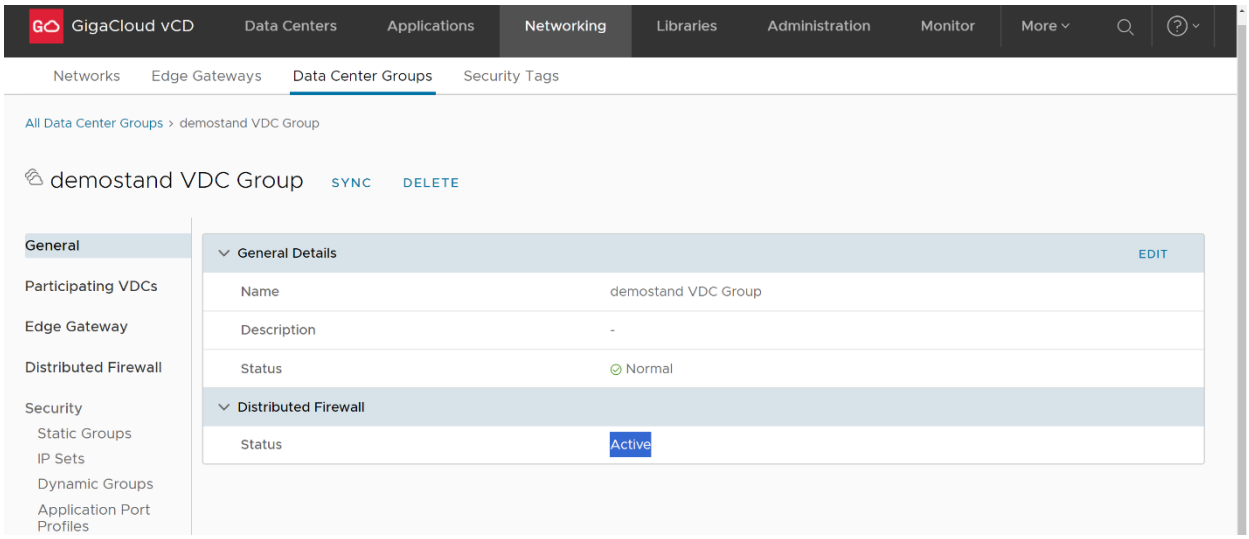
- за допомогою профілів портів застосунків та програм (Application Port Profiles), що є комбінаціями протоколу і порту (або групи портів), що використовуються для служб розподіленого файєрвола. Окрім користування набором попередньо налаштованих типових профілів портів, ви також можете створювати власні профілі портів додатків.

Створення правил розподіленого файєрвола

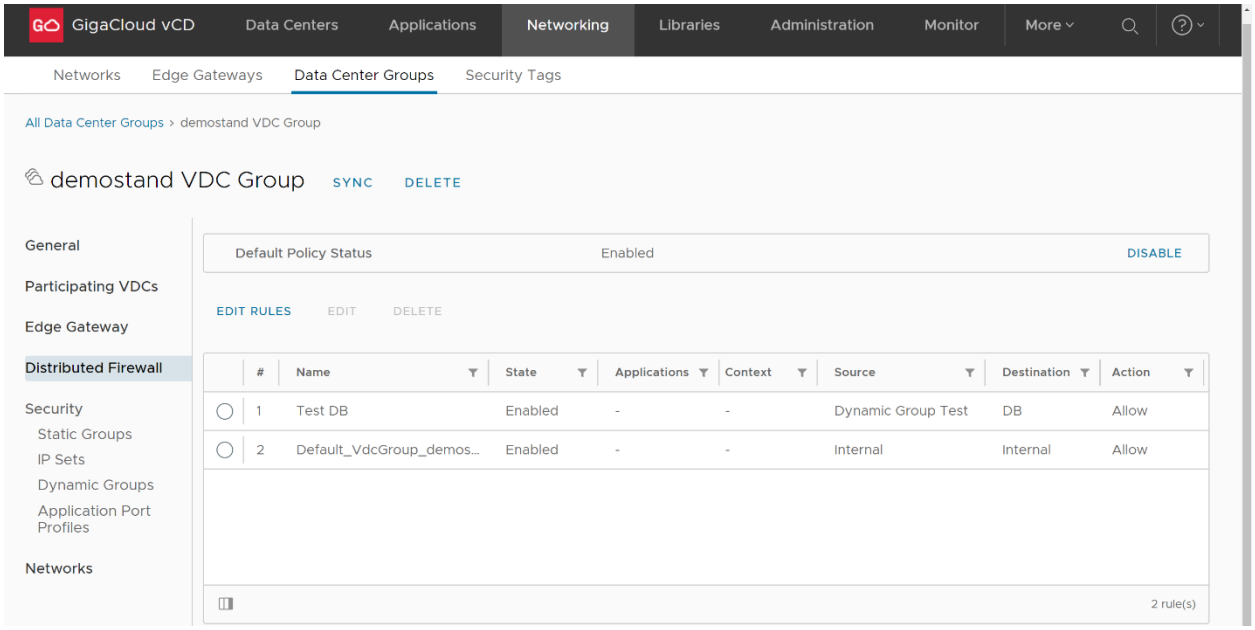
У верхній панелі навігації оберіть вкладку «Networking» і перейдіть на вкладку «Data Center Groups» (групи ЦОДів):



Із переліку груп ЦОДів оберіть потрібну вам групу. Переконайтеся, що служба Distributed Firewall для цієї групи ЦОДів – увімкнена (в стані «Active»).



Перейдіть до розділу меню «Distributed Firewall» ліворуч, натисніть напис «EDIT RULES».

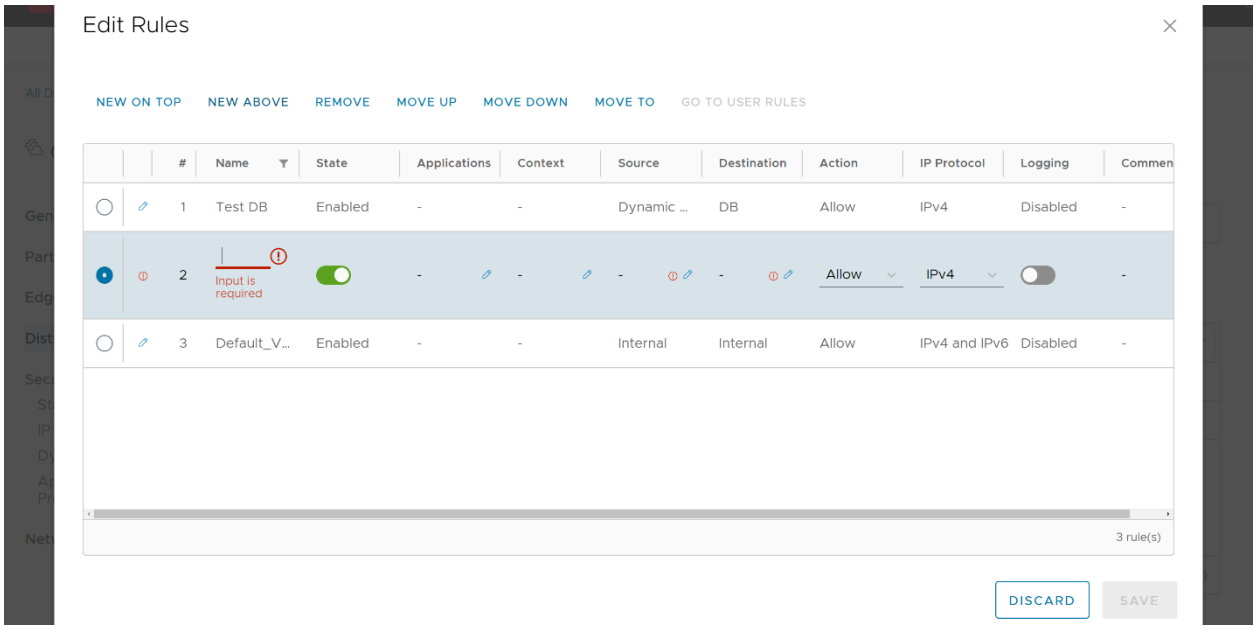


Як зазвичай при використанні файєрволів, доцільно першим правилом у списку дозволити весь можливий трафік, а решта правил буде обмежувати його відповідно до потреби.

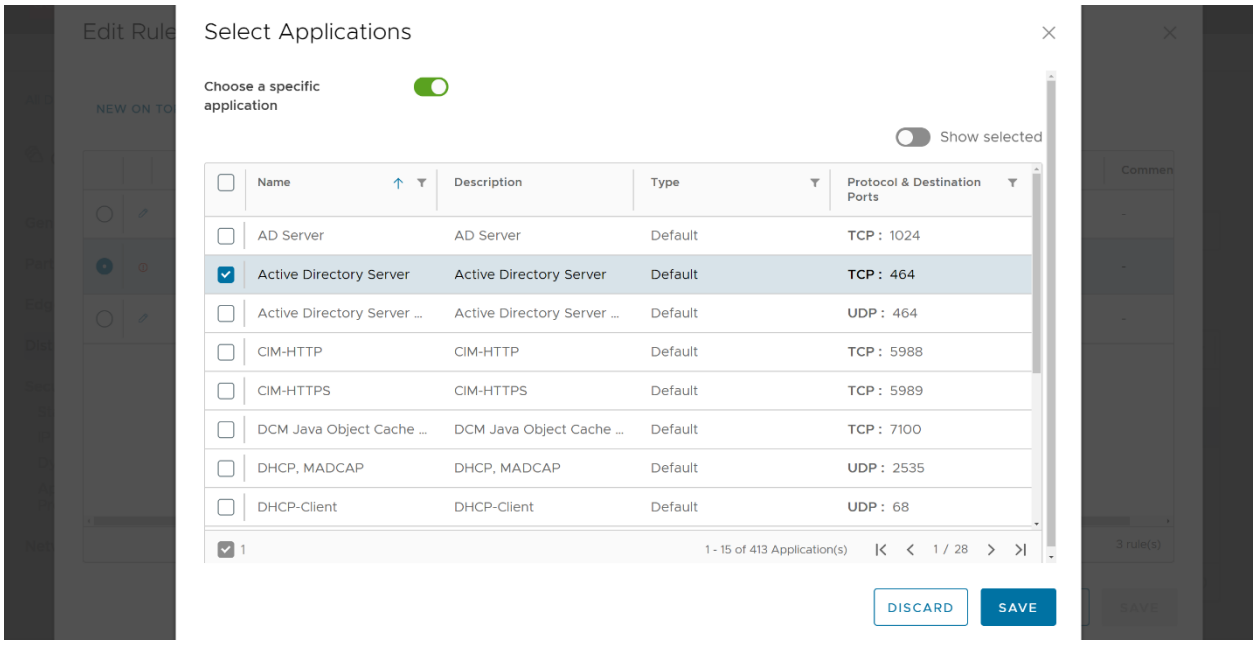
Натисніть кнопку «NEW ON TOP», щоб нове правило файєрвола було доданим першим у списку або позначте потрібне місце в списку та натисніть кнопку «NEW ABOVE».

Налаштуйте параметри нового правила:

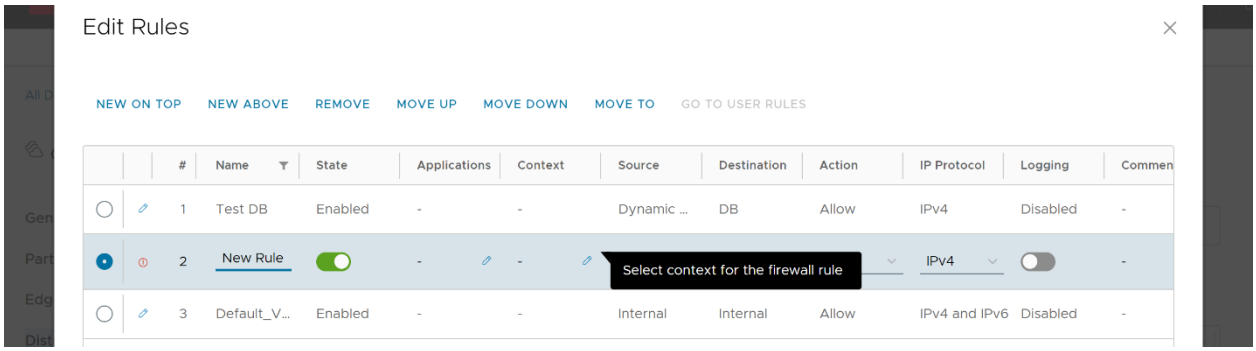
- введіть назву правила у полі параметру «Name»;



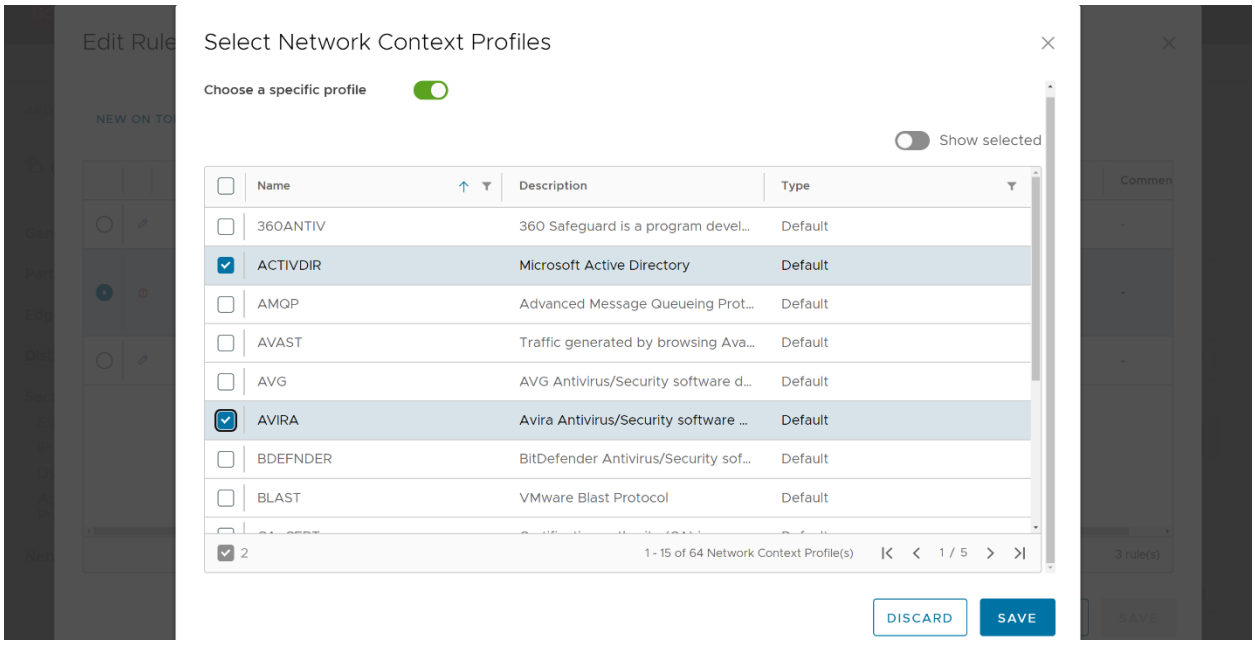
- увімкніть екранний перемикач стану в полі «State», щоб правило почало працювати після створення;
- введення параметрів для допоміжного поля «Applications» – не є обов'язковим (призначене для зручності врахування типових застосунків/програм, що використовують стандартні мережеві порти та протоколи для своєї роботи і потребуватимуть дозволу відповідного трафіку). Позначте всі необхідні застосунки та натисніть кнопку «SAVE»;



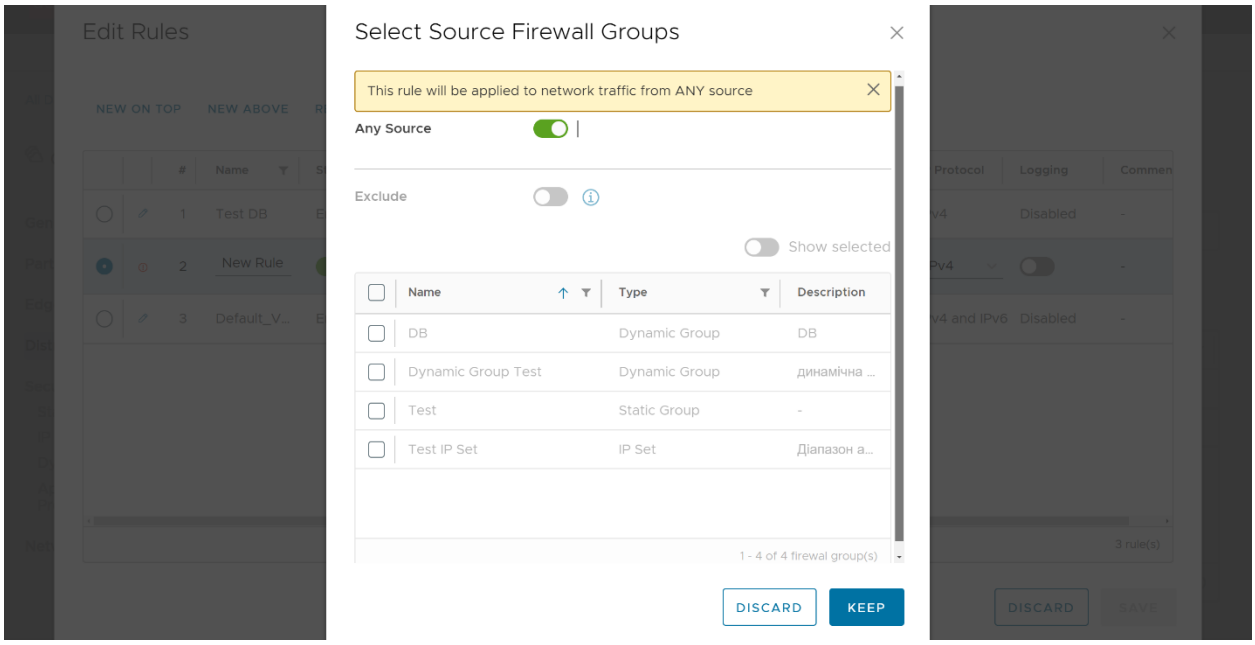
- аналогічним чином, введення параметрів для допоміжного поля «Context» – не є обов'язковим (призначене для вибору та позначення типових профілів мережевого контексту NSX-T, що відповідають даному правилу DFW).



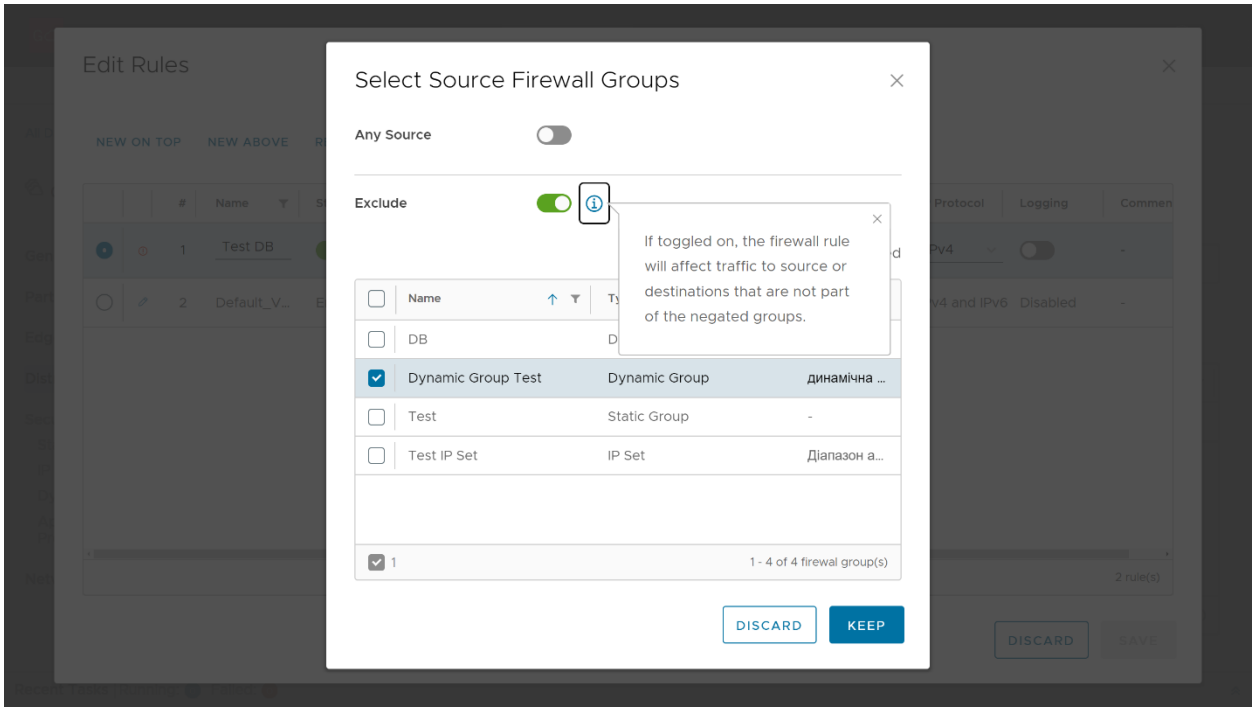
Якщо потрібно, позначте всі необхідні профілі та натисніть кнопку «SAVE»:



- оберіть джерело трафіку (набори IP-адрес та/або групи безпеки зі списку) в полі «Source». Щоб дозволити або заборонити трафік з будь-якої адреси джерела, активуйте екранний перемикач «Any Source».

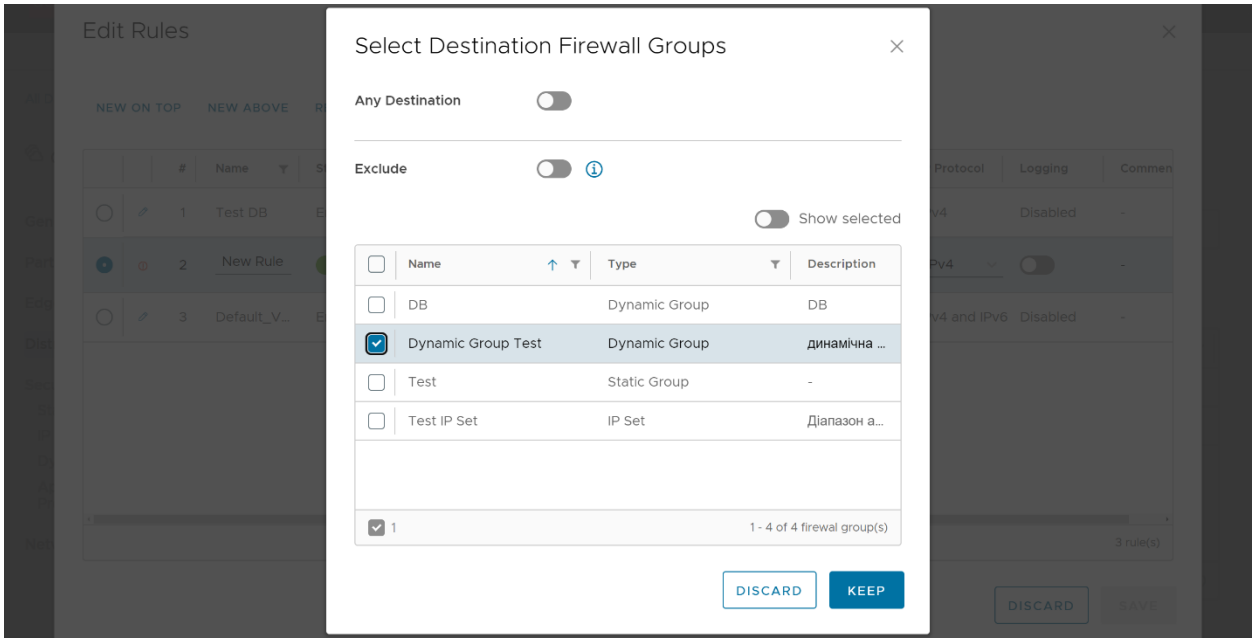


Щоб дозволити/заборонити трафік з певних наборів IP-адрес/груп безпеки, виберіть потрібне. Можливо також дозволити/заборонити трафік для всіх наборів IP-адрес/груп безпеки, окрім обраних зі списку (для цього активуйте екранний перемикач «Exclude»).



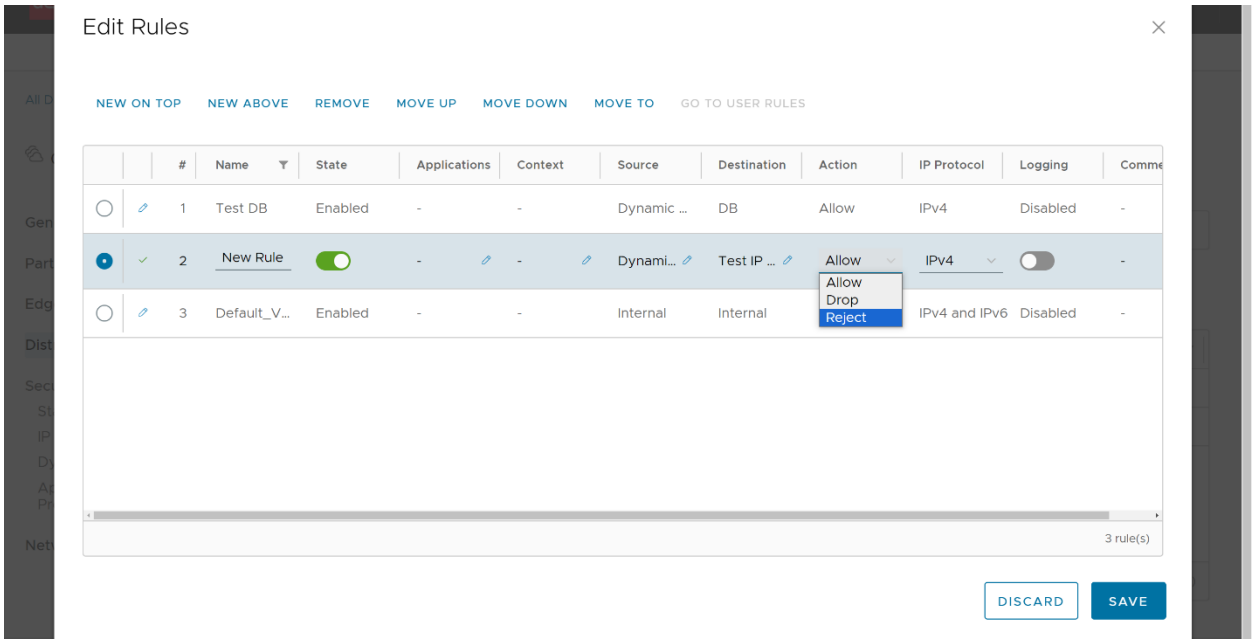
На завершення редагування параметрів поля «Source», натисніть екранну кнопку «KEEP»;

- оберіть пункт призначення трафіку в полі «Destination» (аналогічним чином, можливо дозволити/заборонити трафік на певні набори IP-адрес/груп безпеки, на всі адреси або на всі адреси, окрім обраних).



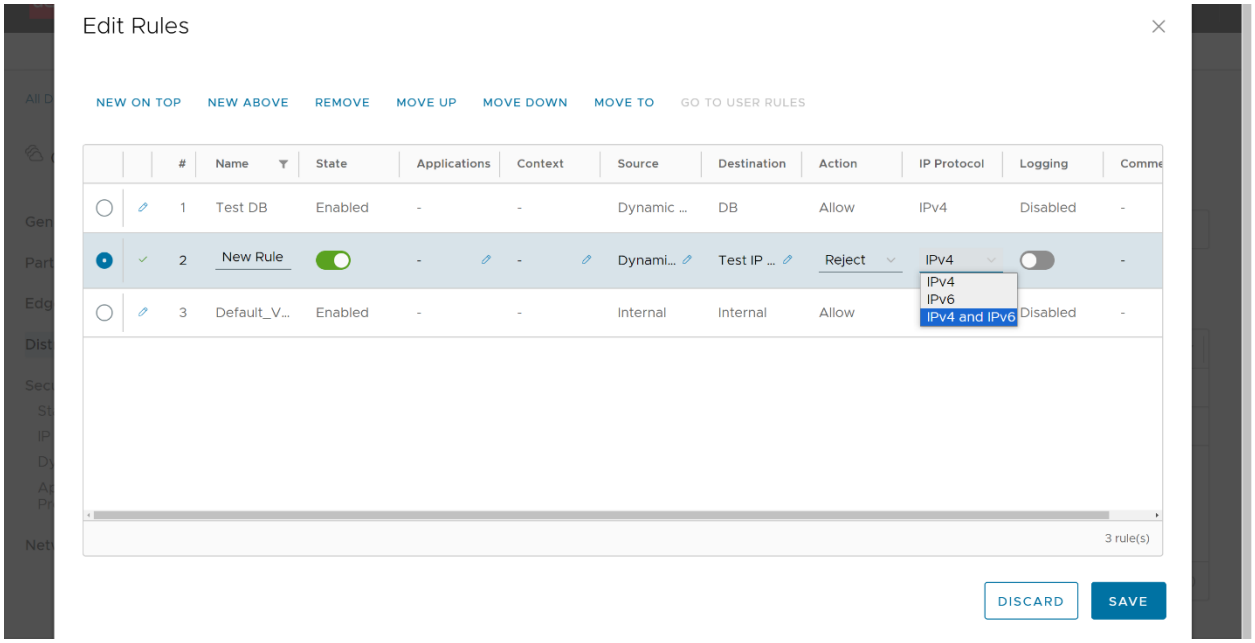
На завершення редагування параметрів поля «Destination» – натисніть екранну кнопку «KEEP».

- оберіть дію «Allow/Drop/Reject» у спадаючому меню поля «Action» для дозволу чи заборони трафіку від певних джерел/пунктів призначення/служб – або до них:



Трафік за цим правилом вже дозволено дією «Allow». Оберіть дію відхилення пакетів «Reject» для блокування трафіку між зазначеними джерелами та пунктами призначення (з відправкою у відповідь ICMP-пакетів із інформацією про недоступність порту призначення). Відкидання пакетів «Drop» зазвичай використовують для протидії алгоритмам сканування (шляхом «поглинання» отриманих пакетів, тобто ілюзії для відправника щодо наявності там вільної IP-адреси та отримання ним великих значень часу відповіді мережі – до 100 сек.);

- оберіть протоколи IP, до трафіку яких буде застосовано правило (IPv4 або IPv6 або обидва одночасно);

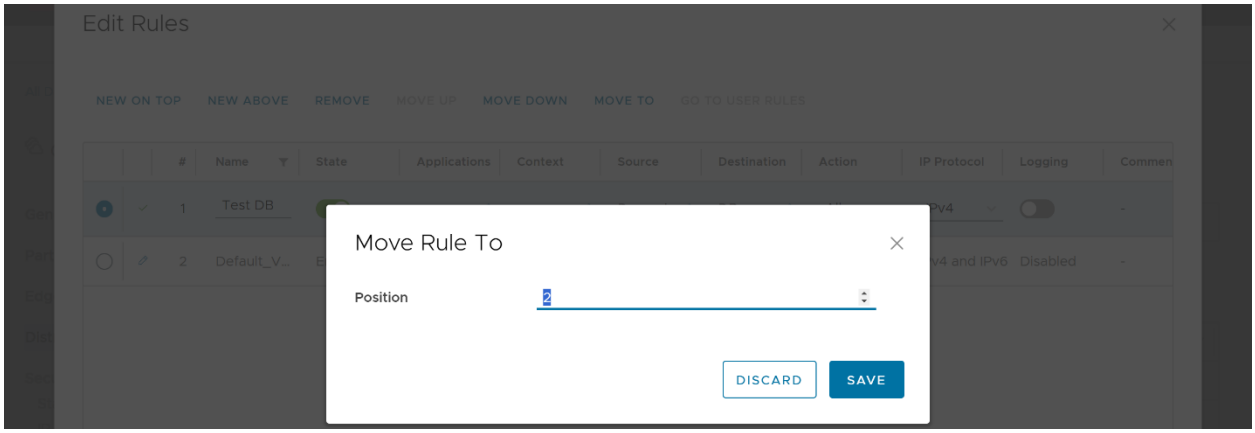


- у разі потреби у веденні записів до журналу подій перетворення мережевих адрес за цим правилом – увімкніть екранний перемикач у полі «Logging».

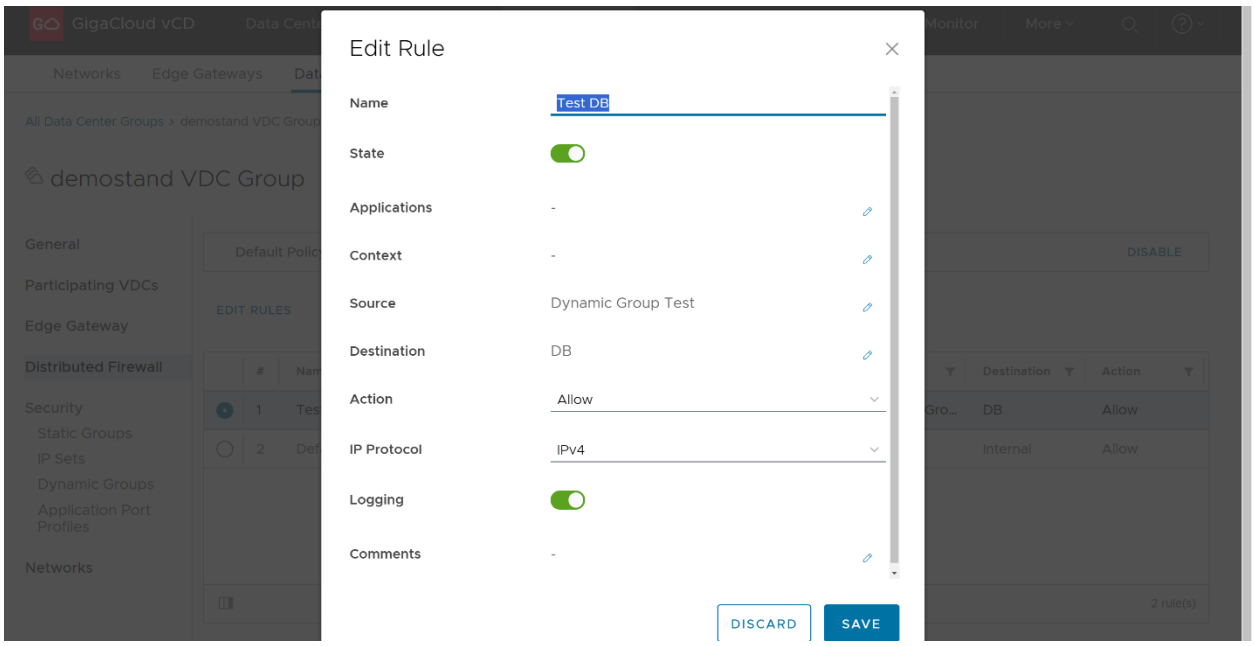
На завершення, натисніть екранну кнопку «SAVE». Для налаштувань інших правил DFW повторіть наведені вище кроки (після створення нових правил їх буде додано до обраного вами місця списку).

Редагування правил DFW

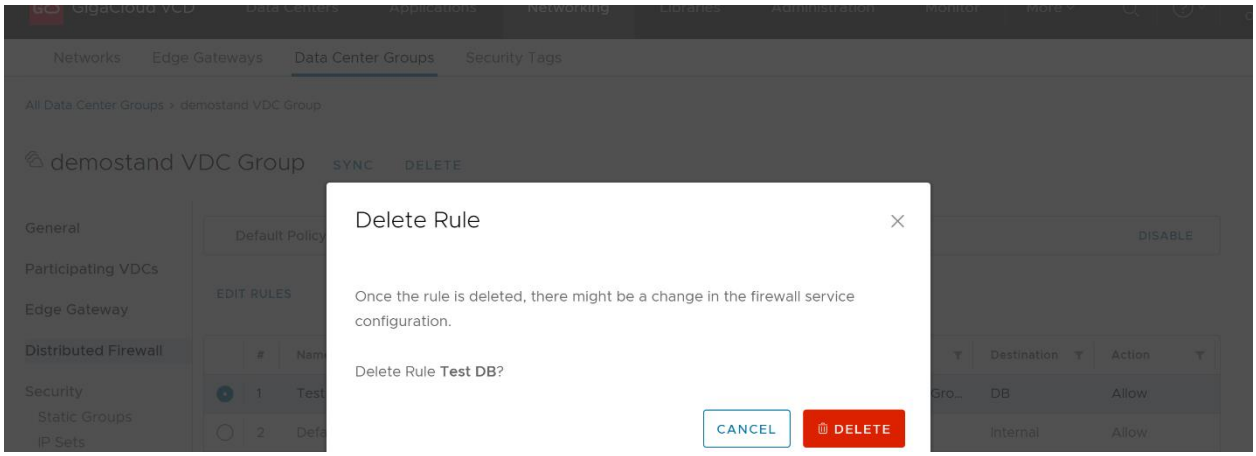
Користуючись екранними кнопками «MOVE UP / MOVE DOWN / MOVE TO» меню розділу «Edit Rules» панелі керування, ви можете переміщати вже існуючі правила розподіленого файєрвола вгору та вниз списку, змінюючи логіку фільтрації трафіка.



Натискання кнопки «EDIT» дозволяє редагувати налаштування обраного правила:



Натискання кнопки «DELETE» дозволяє у разі потреби видалити обране правило.



Якщо необхідно, звертайтесь до фахівців СТП провайдера за консультацією та користуйтесь послугою Gigacloud Admin.