SANGFOR

VDI

Distributed Firewall Rules Configuration Guide

Version 5.4.2

Change Log

Date	Change Description
May 31, 2020	Distributed Firewall Rules Configuration Guide.

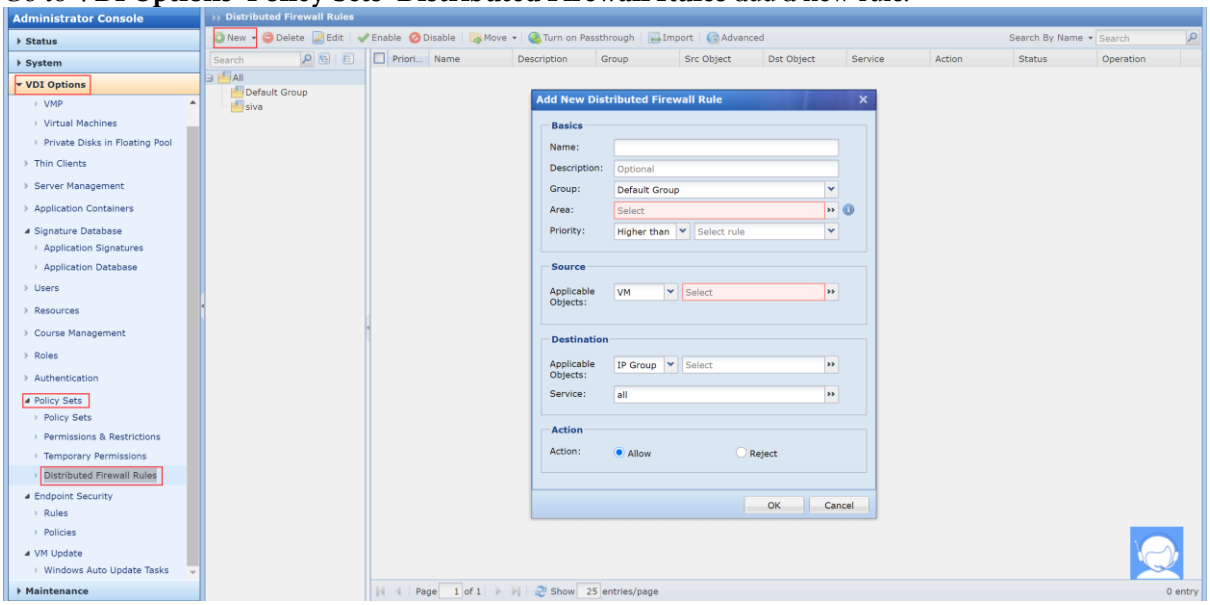
CONTENT

Chapter 1 Application Scenario

VDC can achieve the purpose of restricting the virtual machine network without any third-party devices. Distributed firewall Rules supports configuration for ip range, vdc local users/user groups/ldap external users mapped to local groups/imported from ldap to local users/user groups, virtual machines/resources/resource groups.

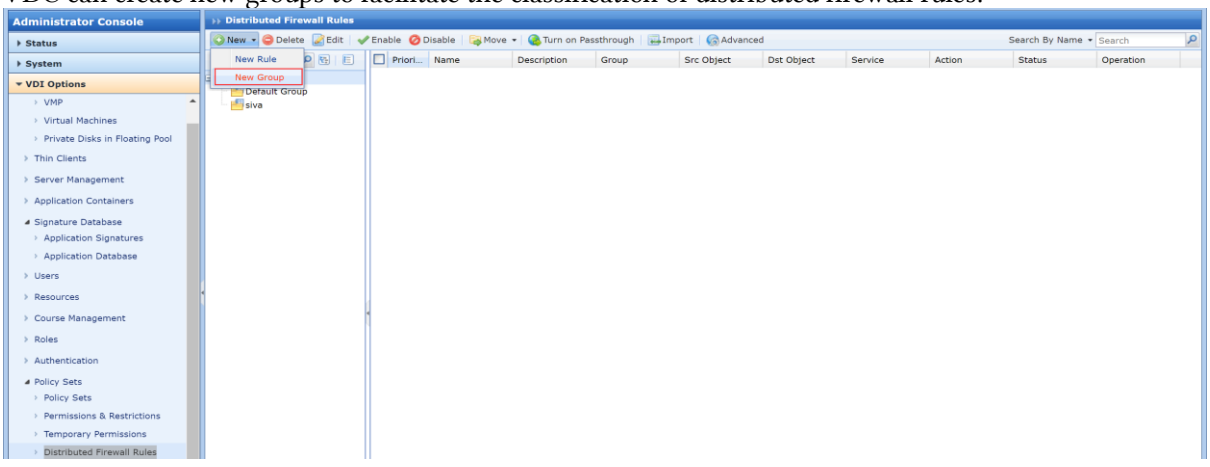
Chapter 2 Instructions for distributed firewall rules

1. Go to **VDI Options>Policy Sets>Distributed Firewall Rules** add a new rule.

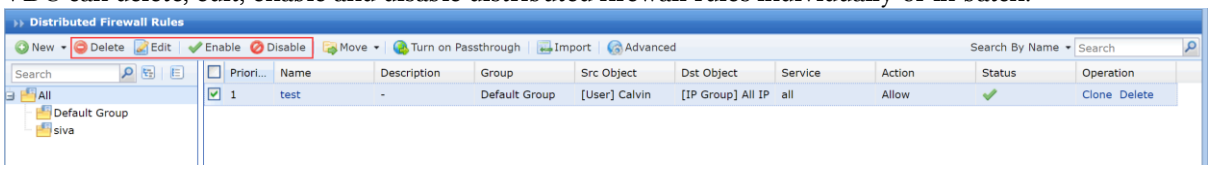


To add a new distributed firewall rules, you need to fill in the **name**, **description**, select the **group**, **area**, and **priority** (priority determines the order in which this firewall takes effect. The lower the priority number, the higher the priority). Both **source** and **destination** objects support IP groups , User, virtual machine configuration, according to the distributed firewall policy configured by the user, if the user is a local user, it will take effect immediately. If it is an external user, it is implemented through group mapping. If the object is configured as a user group, you must log in next time to take effect. Configure distributed firewall policies based on IP groups and virtual machines to take effect immediately. Services can choose built-in services or custom services. Effective conditions can be set to allow or deny access from source to destination

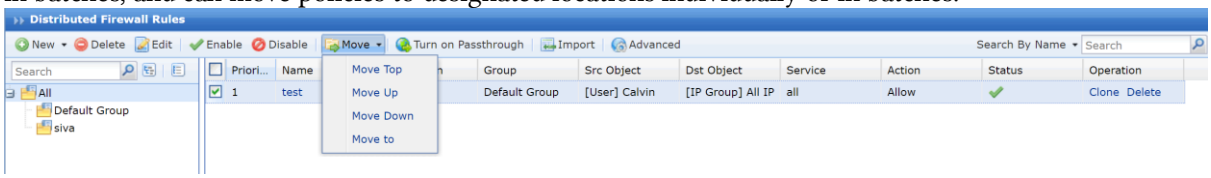
2. VDC can create new groups to facilitate the classification of distributed firewall rules.



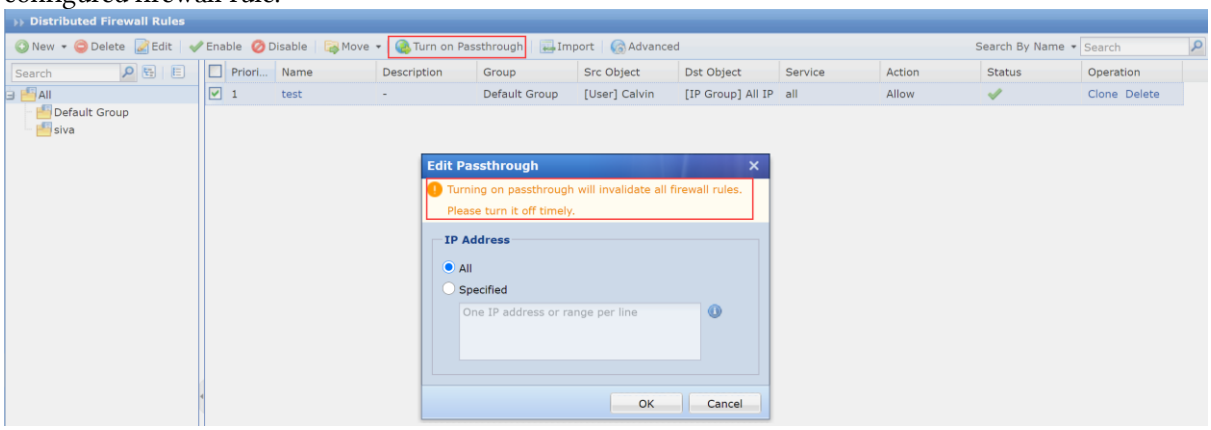
3. VDC can delete, edit, enable and disable distributed firewall rules individually or in batch.



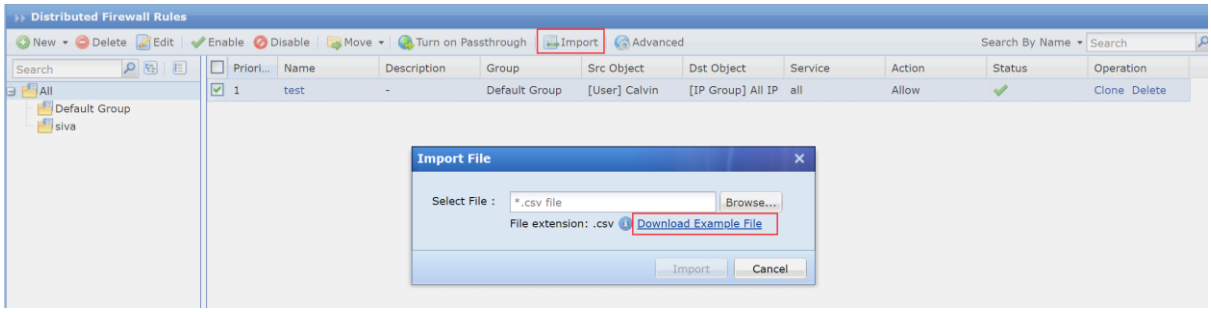
4. VDC can move top, move up, move down and move to the distributed firewall rules individually or in batches, and can move policies to designated locations individually or in batches.



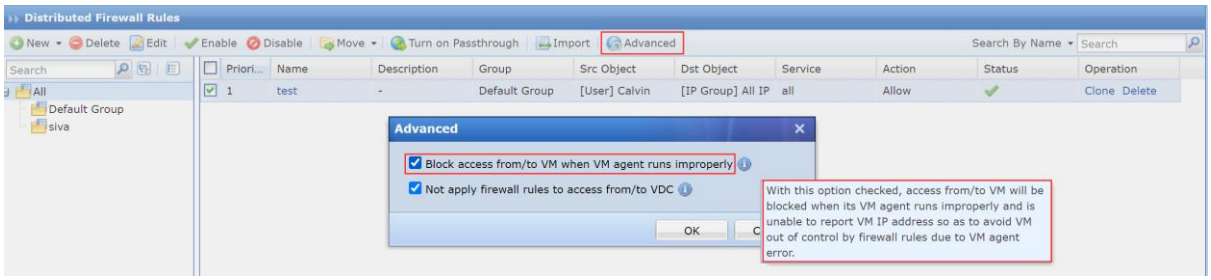
5. When the distributed firewall rule does not take effect, the service of the user virtual machine is interrupted. You can set the user virtual machine to pass through, you can set up a single or multiple IP pass-through, or set up all virtual machine pass-through The machine is not controlled by the configured firewall rule.



6. VDC supports both IP source and destination objects for IP rules import. Before import the rule, you need to download example file.

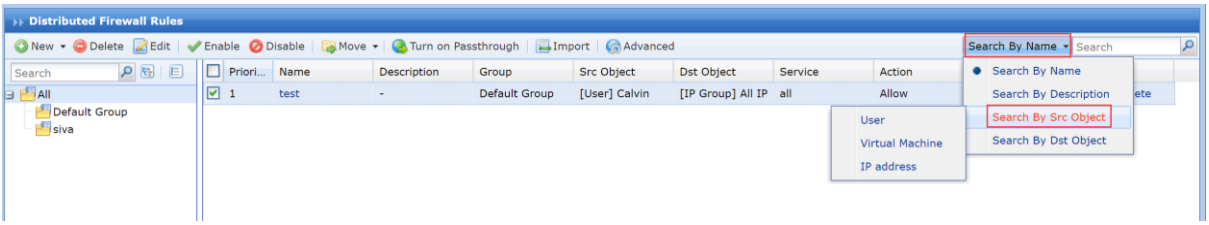


7. In the advanced settings, you can enable **[Block access from/to VM when VM agent runs improperly]**, enable this function, with this option checked,access from/to VM will be blocked when its VM agent run improperly and is unable to report VM IP address so as to avoid VM out of control by firewall rules due ti VM agent error.



8. All the distributed firewall rules configured by the IP of the user-associated virtual machine can be

searched out, which is convenient for the administrator to analyze the rule conflicts and troubleshoot.



Chapter 3 Precautions

1. If "Block access from/to VM when VM agent runs improperly" is enabled on VDC, when the virtual machine cannot report IP to VDC because of agent abnormality, the virtual machine is isolated after 5 minutes and cannot access any network. Firewall policy It will not take effect until five minutes after the machine is power on again.

2. For external users who have not imported VDC, the firewall rules will be cleared after the user logs out. In this scenario, it is recommended to configure firewall rules for virtual machines or IP groups.

3. The firewall rule of a floating pool virtual machine will take effect when the user enters the virtual machine.

4. Virtual machine policy will be cleaned up within ten minutes of virtual machine power off.

5. The distributed firewall rules does not support Linux virtual machines.

6. The distributed firewall rules of Windows virtual machines will not take effect until the agent is installed.

7. The number of users or user groups selected by a single distributed firewall rules cannot exceed 200.