Firewall Rule Actions

Armor Knowledge Base

Topics Discussed

- Create a Firewall Rule
- Reorder A Firewall Rule
- Refresh the Status a Firewall Rule
- Edit a Firewall Rule
- Manage Firewall Rule Notes
- Export Firewall Data

To fully use this screen, you must have the following permissions assigned to your account:

- Read Virtual Data Centers
- Read Firewall
- Write Firewall
- Write Entity Meta Data
- Read Entity Meta Data

Create a Firewall Rule

Create a Firewall Rule with a New IP Address Group

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several IP addresses or just a single IP address.

You can combine related IP addresses into a single **IP Group**. For example, if you want to block traffic from three separate IP address, you do not have to create three separate firewall rules. Instead, you can combine the three separate IP addresses into a single, configurable **IP Group**. Then, when you create a firewall rule, you can pick the newly created **IP Group** as your **Source** or **Destination** IP addresses.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **IP Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **Name of IP Group**, enter a descriptive name.
7. In **IP Addresses**, enter a member, and then click the plus icon.
    - You can enter:
        - A single IP address
        - A range of IP addresses
        - CIDR
    - You must add at least one member.
    - You can add multiple members to a service group.
8. Click **Create Group**.
    - The newly created IP group will appear at the bottom of the table.

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several protocols (and ports).

You can combine related protocols (and ports) into a **Service Group**. For example, if you want to create a firewall rule to block three types of traffic, you do not have to create three separate firewall rules. Instead, you can combine the three types of traffic (protocols and ports) into a single, configurable **Service Group**. Then, when you create a firewall rule, you can pick the newly created **Service Group**.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **Service Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **Name of Service Group**, enter a descriptive name.
7. In **Services**, enter the service or sub-protocol, and then click the plus (+) icon.
    - You must add at least one member.
    - You can add multiple members to a service group.

Service Or Sub-Protocol	Notes	Example
Services (TCP, UDP, Etc.)	You Must Enter A Port Number. These Services Are Not Case-Sensitive.	• Tcp/80 • TCP/80 • Tcp/80 • TCp/80
Additional services (AARP, AH, etc.)	These additional services are not case-sensitive. Do not enter a port number with these additional services.	• ATALK • igmp • Gre
Sub-protocols (echo-reply, redirect, etc.)	You must enter **icmp**, followed by the specific sub-protocol. You must enter the sub-protocol in lower-case letters. Do not enter a port number.	• icmp/source-host-isolated • icmp/time-exceeded

8. Click Create Group.
    - The newly created service group will appear at the bottom of the table.

For a complete list of supported services and sub-protocol, see Review supported services and sub-protocols.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top menu, click the corresponding data center.
4. On the **Rules** tab, click **Actions**, and then click **New Rule**.
    - If you do not see **Actions**, then click **Create a Firewall Rule**.
5. In **Name of Rule**, enter a descriptive name.
6. Under **Action**, select **Allow** to allow specified traffic to access your virtual machine, or **Block** to block specified traffic.
7. Under **Status**, select **Enabled** to create the rule in an enabled status, or **Disabled** to create the rule in a disabled status.
8. In **Source**, select the name of the desired IP Group.
    a. If the desired IP Group is not listed, click **+ New IP Group** to create a new IP Group, then follow the steps outlined in Create an IP group.
9. In **Destination**, select the name of the desired destination.
    a. If the desired destination is not listed, click + **New IP Group** to create a new IP Group, then follow the steps outlined in Create an IP group.
10. In **Services**, select the name of the desired Service Group.
    a. If the desired Service Group is not listed, click + **New Service Group** to create a new Service Group, then follow the steps outlined in Create a service group.
11. Click **Save**.

After you create a rule, Armor recommends that you place the rule in the correct order. To learn more, see Reorder a Firewall Rule.

Create a Firewall Rule with an Existing IP Address Group and Service Group

To create a new firewall rule with an existing IP Group and Service Group, simply follow the instructions outlined in Create a firewall rule.

If you have not created an IP Group or Service Group, and you want to create a new firewall rule, see Create a firewall rule with a new service group and new IP Group.

After you create a rule, Armor recommends that you place the rule in the correct order. To learn more, see Reorder a firewall rule.

Reorder A Firewall Rule

The Armor default rule that displays at the bottom of the table cannot be re-ordered.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.

3. Under **Rule**, in the numbered fields, enter the desired number, then click the check mark to move the rule to a different position. Click **X** to cancel.
    - If you have more than 25 rules, the additional rules will be placed on the next page of the **Firewall** screen.

> ⚠ If you are not familiar with ordering rules, contact Armor Support to help you properly order your firewall rules. It is extremely important to order rules in order to receive desired traffic.
>
> To learn how to send a support ticket, see Armor Support.

Refresh the Status a Firewall Rule

You can manually refresh the status of an individual firewall rule. This will allow you to see the status of the firewall rule transition from a **Pending** status.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Locate and hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Refresh Rule**.

You can also manually refresh the status of all firewall rules at once.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **Actions**, and then click **Refresh Page**.

Edit a Firewall Rule

> ⚠ You cannot edit or delete a rule or group that is in a **Pending** or **Error** state. To make changes, the rule must be in an **Enabled** or **Disabled** state; the group must be in a **Ready To Use** or **In Use** state.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Locate and hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Edit Rule**.
7. Make any desired changes to the firewall rule.
8. Click **Save**.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Locate and hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Edit Rule**.
    a. Hover over the desired **Source**, then click the trash can icon.
    b. Hover over the desired **Destination**, then click the trash can icon.
    c. Hover over the desired **Service Group**, then click the trash can icon.
7. Click **Save.**

> ⚠ In order to save a rule, you must have an entry in the **Source, Destination**, and **Services** section.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Enable Rule** or **Disable Rule**.
7. Click **Enable Rule** or **Disable Rule** again.

> ⚠ You cannot edit or delete a rule or group that is in a **Pending** or **Error** state. To make changes, the rule must be in an **Enabled** or **Disabled** state; the group must be in a **Ready To Use** or **In Use** state.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Delete Rule**.
7. Click **Delete Rule** again.

Manage Firewall Rule Notes

> ⚠ In order to create, view or edit notes for your firewall rules, you must have the following permissions enabled:
>
> - Write Entity Meta Data
> - Read Entity Meta Data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data center, then click the corresponding data center.
4. Locate and hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **View/Edit Notes**.
7. In **Notes**, enter the desired text.
8. Click **Submit**.

> ⓘ A note icon will display next to the **Name** of the firewall rule that was updated. Click the icon to view the note.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data center, then click the corresponding data center.
4. Locate and hover over the desired firewall rule.
5. Next to the **Name,** click the note icon.
    a. Or, click the vertical ellipses, then click **View/Edit Notes**.

Export Firewall Data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data center, then click the corresponding data center.
4. Select **Rules**, I**P Groups,** or **Service Groups** to filter the data.
5. (Optional) Use the filter function to customize the data displayed.
6. In the bottom, right part of the screen, click **CSV**.

- You have the option to export all the data (**All**) or only the data that appears on the current screen (**Current Set**).

Data type	Data displayed
Rules	Order, Name, Sources, Destinations, Services, Action, Enabled, Notes
IP Groups	Name, Ips, Ranges, Cidrs, Notes
Service Group	Name, Udp, Tcp, Icmp, Notes

Was this helpful?

Your Rating:  Results: 0 rates