Firewall Rule Actions.mobile.phone

Armor Knowledge Base

Armor Knowledge Base / Armor Complete / Firewall Rules

Firewall Rule Actions

Topics Discussed

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

- Read Virtual Data Centers
- Read Firewall
- Write Firewall

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 **IP Group Name**, enter a descriptive name.
   - Armor recommends that you add **Source** or **Destination** into the name of the IP Group to help you identify the IP Group as the **Source** or **Destination** IP group.
7. In **Add Members To Group**, 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 **Apply**.
   - 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 **Service Group Name**, enter a descriptive name.
7. In **Add Members To Group**, 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 **Apply**.
    - 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. Click **Actions**, and then click **New Rule**.

    - If you do not see **Actions**, then click **Create a Firewall Rule**.
5. In **Name**, enter a descriptive name.
6. In **Action**, select **Allow** to allow specified traffic to access your virtual machine or **Block** to block specified traffic.
7. Under **Service**, enter and select the name of the desired Service Group.
    - To learn how to create a Service Group, see Create a service group.
8. Under **Source**, enter and select the name of the desired IP Group.
    - To learn how to create an IP Group, see Create an IP group.
9. Under **Destinations**, in the field, enter and select the name of the desired IP Group.
10. Click **Save Rule**.

To reorder a rule:

1. Under Rule, in the numbered fields, enter a number to move the rule to a different position.
    - If you have more than 25 rules, the additional rules will be placed in a secondary section within the **Firewall** screen. To reorder and move these additional rules into a higher position, enter a number under the **Order** column, and then press **Enter** on your keyboard.
2. In the top menu that appears, click **Save**.

⚠ 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.

To disable a rule:

1. Locate and hover over the desired rule.
2. Click the vertical ellipses.
3. Click **Disable Rule**.
4. Click **Disable Rule** again.
5. In the top menu that appears, click **Save**.

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

Use these instructions to create a new firewall rule with an existing IP Group and Service Group.

⚠ 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, you have the option to disable the rule. This rule will be saved, and you can enable the rule at a later time.

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. Click **Actions**, and then click **New Rule**.
    - If you do not see **Actions**, then click **Create a Firewall Rule**.
5. In **Name**, enter a descriptive name.
6. In **Action**, select **Allow** to allow specified traffic to access your virtual machine or **Block** to block specified traffic.
7. Under **Service**, enter and select the name of the desired Service Group.
    - To learn how to create a Service Group, see Create a service group.
8. Under **Source**, enter and select the name of the desired IP Group.
    - To learn how to create an IP Group, see Create an IP group.
9. Under **Destinations**, in the field, enter and select the name of the desired IP Group.
10. Click **Save Rule**.

> ⓘ After you create a rule, Armor recommends that you place the rule in the correct order.

To reorder a rule:

1. Under Rule, in the numbered fields, enter a number to move the rule to a different position.
    - If you have more than 25 rules, the additional rules will be placed in a secondary section within the **Firewall** screen. To reorder and move these additional rules into a higher position, enter a number under the **Order** column, and then press **Enter** on your keyboard.
2. In the top menu that appears, click **Save**.

> ⚠ 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.

To disable a rule:

1. Locate and hover over the desired rule.
2. Click the vertical ellipses.
3. Click **Disable Rule**.
4. Click **Disable Rule** again.
5. In the top menu that appears, click **Save**.

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. Several options are available to edit. Follow the appropriate sub-steps below.

To edit the name of a firewall rule:

1. Under **Name**, edit the name.
2. Click **Save Rule**.
3. In the top menu that appears, click **Save**.

To add a source:

1. Under **Source**, enter and select:
    - an IP address
    - an IP address range
    - a CIDR
    - an existing IP Group
2. Click **Save Rule**
3. In the top menu that appears, click **Save**.

> ⚠ You cannot create a new IP Group from this window. To learn how to create an IP group, see Create an IP group.

To remove a source:

1. Under **Source**, hover over the desired source.
2. Click the trash icon.
3. Click **Save Rule**
4. In the top menu that appears, click **Save**.

> ⚠ You cannot save a rule without a source. You must have an entry in the **Source** section.

To add a destination:

1. Under **Destination**, enter and select:
    - an IP address
    - an IP address range
    - a CIDR
    - an existing IP Group
2. Click **Save Rule**
3. In the top menu that appears, click **Save**.

> ⚠ You cannot create a new IP Group from this window. To learn how to create an IP group, see Create an IP group.

To remove a destination:

1. Under **Destination**, hover over the desired source.
2. Click the trash icon.
3. Click **Save Rule**
4. In the top menu that appears, click **Save**.

> ⚠ You cannot save a rule without a source. You must have an entry in the **Destination** section.

1. Under **Action**, select **Allow** or **Block**.
2. Click **Save Rule**.
3. In the top menu that appears, click **Save**.

1. Under **Service**, enter and select:
    - a service
    - a subprotol
    - an existing service group
2. Click **Save Rule**
3. In the top menu that appears, click **Save**.

> ⚠ You cannot create a new Service Group from this window. To learn how to create a service group, see Create a service group.

1. Under **Source**, hover over the desired source.
2. Click the trash icon.
3. Click **Save Rule**
4. In the top menu that appears, click **Save**.

> ⚠ You cannot save a rule without a source. You must have an entry in the **Source** section.

> ⚠ After you create a rule, you have the option to disable the rule. This rule will be saved, and you can enable the rule at a later time.

To enable or disable a firewall rule:

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.
8. In the top menu that appears, click **Save**.

To delete 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. Hover over the desired firewall rule.
5. Click the vertical ellipses.
6. Click **Delete Rule**.
7. Click **Delete Rule** again.
8. In the top menu, click **Save**.

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**.

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