Firewall Rules

This topic only applies to **Armor Complete** users.

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

- Read Firewall
- Write Firewall

Overview

You can use the **Firewall** screen to configure which web traffic can (or cannot) access your virtual machine or server.

Each entry in the table represents a single rule that allows or blocks web traffic from accessing your virtual machine or server. Within a single rule, you can configure several IP addresses or just a single IP address.

You can combine related IP addresses into an **IP Group**. For example, if you want to block traffic from three separate IP addresses, 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**. You can use the same practice for **Destination** I P addresses. For more information, see Create an IP group.

Similar to an **IP Group**, you can create a **Service Group** to combine similar port requirements.

In the **Firewall Rules** screen, each firewall rule entry contains the following information:

Column	Description

Order	You can place firewall rules in a specific order as a way to further filter traffic. Traffic will be tested against each firewall rule, starting with the firewall rule in the top position, followed by the next firewall rule. As a result, Armor recommends that generic rules be placed at the top of the table, with more specific rules towards the bottom of the table. For example, if you have two firewall rules, incoming traffic will be tested against the first rule (the rule in the top position). If the traffic passes the first firewall rule, then the traffic will be tested against the second firewall. If the traffic passes the second firewall rule, then the traffic will be allowed to access your site. In another example, if traffic does not pass the first firewall rule (the rule in the top position), then the traffic will be blocked, even without being tested against the second firewall rule. You cannot change the order of a disabled rule. Each page in the **Firewall** screen only lists 25 rules. If you have more than 25 rules, these additional rules will be placed in another page within the **Firewall** screen. To reorder and move these additional rules into a different page, enter a number under the **Order** column, and then press **Enter** on your keyboard. You cannot drag rules across different pages in the **Firewall** screen. If you are not familiar with how to order firewall rules, Armor recommends that you send a support ticket for assistance. The order of firewall rules is very important to properly filter undesired traffic. To learn how to send a support ticket, see Support Tickets.
Name	This column displays the descriptive name of the firewall rule.
Action	This column displays if the firewall rule is configured to **Allow** or **Block** web traffic to the **Destination**.
Source	This column displays the **Service Group** that contains the **Source** IP address (or addresses). The **Source** IP address is the starting point for the web traffic that you want to allow or block. Each **Source** IP address must be associated with a **Service Group**. A **Service Group** can contain one IP address or several IP addresses. You can enter an IP address, an IP address range, or a CIDR.
Destination	This column displays the **Service Group** that contains the **Destination** IP address (or addresses). The **Destination** IP address is the server or virtual machine that you want to protect. Each **Destination** IP address must be associated with a **Service Group**. A **Service Group** can contain one IP address or several IP addresses. You can enter an IP address, an IP address range, or a CIDR.
Services	This column displays the type of protocol for the configured ports in the firewall rule.

Create a firewall rule with a new IP address group

Step 1: Create an IP 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 the plus (+) icon.
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.

Step 2: Create a Service Group

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 the plus (+) icon.
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.

Step 3: Create a firewall rule

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 the plus (+) icon.
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. Select and drag the newly created rule to the desired position.
    - Under the **Order** column, you can also enter a number to move the firewall 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. You cannot drag these additional rules into the primary section of the **Firewall** screen.
2. In the top window, 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 Support Tickets.

To disable a rule:

1. Locate and hover over the desired rule.
2. Click **Disable Rule**.
3. Click **Disable Rule** again.
4. In the top window, 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 the plus (+) icon.
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. Select and drag the newly created rule to the desired position.
    - Under the **Order** column, you can also enter a number to move the firewall 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. You cannot drag these additional rules into the primary section of the **Firewall** screen.
2. In the top window, 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 Support Tickets.

To disable a rule:

1. Locate and hover over the desired rule.
2. Click **Disable Rule**.
3. Click **Disable Rule** again.
4. In the top window, click **Save**.

Edit 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. 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.

Edit name

To edit the name of the firewall rule:

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

Edit source

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 window, 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.

Remove a source

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

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

Edit destination

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 window, 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.

Remove a destination

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

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

Edit action

1. Under **Action**, select **Allow** or **Block**.
2. Click **Save Rule**.

3. In the top window, click **Save**.

Edit services

Add a service

1. Under **Service**, enter and select:
    - a service
    - a subprotol
    - an existing service group
2. Click **SaveRule**
3. In the top window, 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.

Remove a source

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

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

Enable or disable a firewall rule

> 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), 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, click **Save**.

Delete 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 **Delete Rule**.
7. Click **Delete Rule** again.
8. In the top menu, click **Save**.

Export firewall data

To 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

Create an IP 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 the plus (+) icon.
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 **S ource** 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.

Edit an IP 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 **IP Groups**.
5. Locate and place your cursor over the desired IP group.
6. Click the pencil icon.
7. Make your changes, and then click **Appy** to save.

Delete an IP 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 **IP Groups**.
5. Locate and place your cursor over the desired IP group.
6. Click the trash icon.
7. Click **Delete IP Group**.

Create a service group

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 the plus (+) icon.
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.

Edit a 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. Locate and place your cursor over the desired service group.
6. Click the pencil icon.
7. Make your changes, and then click **Appy** to save.

Delete a Service Group

> You cannot delete a service group that is actively used in a firewall rule.

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. Locate and place your cursor over the desired service group.
6. Click the trash icon.
7. Click **Delete Service Group**.

Review supported services and sub-protocols

Supported services or sub-protocols	List	Notes	Example
Services	• TCP • UDP • ORACLE_TNS • FTP • SUN_RPC_TCP • SUN_RPC_UDP • MS_RPC_TCP • MS_RPC_UDP • NBNS_BROADCAST • NBDG_BROADCAST • L2_OTHERS • This service requires a hexadecimal subprotocol, such as: L2_OTHERS/0x814c • L3_OTHERS	• These services are not case-sensitive. • You must enter a port number.	• TCP/80 • udp/40 • Tcp/80 • udP/40
Additional services	• AARP • AH • ARP • ATALK • ATMFATE • ATMMPOA • BPQ • CUST • DEC • DIAG • DNA_DL • DNA_RC • DNA_RT • ESP • FR_ARP • GRE • IEEE_802_1Q • IGMP • IPCOMP • IPV4 • IPV6 • IPV6FRAG • IPV6ICMP • IPV6NONXT • IPV6OPTS • IPV6ROUTE • IPX • L2TP • LAT • LLC • LOOP • NETBEUI • PPP • PPP_DISC • PPP_SES • RARP • RAW_FR • RSVP • SCA • SCTP • TEB • X25	• These additional services are not case-sensitive. • Do not enter a port number with these additional services.	• AARP • aarp • Aarp

Sub-protocols	• echo-reply • destination-unreachable • source-quench • redirect • echo-request • router-advertisement • router-solicitation • time-exceeded • parameter-problem • timestamp-request • timestamp-reply • address-mask-request • address-mask-reply • network-unreachable • host-unreachable • protocol-unreachable • port-unreachable • fragmentation-needed • source-routing-failed • destination-network-unknown • destination-host-unknown • source-host-isolated • destination-network-prohibited • destination-host-prohibited • network-unreachable-tos • host-unreachable-tos • communication-prohibited • redirect-network • redirect-host • redirect-tos-network • redirect-tos-host • ttl-zero-transit • ttl-zero-reassembly • pointer-to-error • options-missing • bad-length	• You can use these sub-protocols to communicate an error message to a user who attempts to access your site. • Do not enter a port number. • You must enter **icmp**, followed by the specific sub-protocol. • You must enter the sub-protocol in lower-case letters.	• icmp/destination-unreachable • icmp/time-exceeded

Review API calls

- Get Firewall Groups
- Get Firewall Group
- Update Firewall Group
- Create Firewall Group
- Delete Firewall Group
- Get Firewall Services
- Get Firewall Service Detail
- Put Firewall Service
- Create Firewall Services
- Delete Firewall Service
- Get Firewalls
- Get Firewall Rules
- Create Firewall Rules

Related documentation

Page:Firewall Rules

Page:IP Address

Page:Virtual Machines

Page:Workloads