Firewall Rules

Armor Knowledge Base

Topics Discussed

- Review Supported Services and Sub-Protocols

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

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

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** IP 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
Rule	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 learn how to reorder and move these additional rules into a different page, see Reorder a firewall rule. 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 Armor Support.
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 **IP 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. This can be an IP address, an IP address range, or a CIDR. Each **Source** IP address must be associated with an **IP Group**. An **IP Group** can contain one IP address or several IP addresses.
Destination	This column displays the **IP Group** that contains the **Destination** IP address (or addresses). The **Destination** IP address is the server or virtual machine that you want to protect. This can be an IP address, an IP address range, or a CIDR. Each **Destination** IP address must be associated with an **IP Group**. An **IP Group** can contain one IP address or several IP addresses.
Services	This column displays the type of protocol for the configured ports in the firewall rule.
Status	This column displays the status of the firewall rule: • **Enabled** indicates that the firewall rule has been enabled. • **Disabled** indicates that the firewall rule has been disabled. • **Pending** indicates that the firewall rule is waiting to be enabled. • **Error** indicates that the firewall rule has encountered an error.

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

Troubleshooting

For rules or groups in an **Error** state, you can click **Retry** to troubleshoot the issue. You can only click **Retry** once. If this action does not resolve the issue, then you must contact Support.

Related Documentation

- Firewall Rules
- IP Address
- Virtual Machines
- Workloads

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★½ 18 rates