Using Layer 3 Firewall Rules

Layer 3 Firewall rules provide an administrator granular access control of outbound client traffic. With the MR series, outbound traffic refers to client traffic originating from the wireless network that is destined for the wired LAN or Internet. On the MX, outbound traffic refers to traffic originating from one VLAN that is destined for another VLAN or traffic originating from the LAN that is destined for the Internet or a remote network that is located over a static LAN route. This article discusses how to use Layer 3 Firewall rules on MR series access points, MX Security Appliance or Z-series Teleworker gateways.

A layer 3 firewall rule on the MX or Z-series appliance is stateful and can be based on protocol, source IP address and port, and destination IP address (or FQDN) and port. Layer 3 firewall rules on the MR are stateless and can be based on destination address and port. Dashboard presents the rules in numeric order, they are evaluated from top to bottom beginning with rule number 1. The first rule that matches is applied, and subsequent rules are not evaluated. If no rules match, the default rule (allow all traffic) is applied.

An explanation of the fields in a Layer-3 firewall rule is shown below.

- **#**: The sequence number of a particular firewall rule.
- **Policy**: Specifies the action the firewall should take when traffic matches the rule. Matching traffic can be allowed or denied.
- **Protocol**: Specifies the protocol to match in outbound traffic i.e. TCP, UDP, ICMP, ANY.
- **Source (MX/Z-series only)**: Specifies the source IP address or network address using CIDR notation to match in outbound traffic. "Any" can also be used to specify all networks.
- **Src port (MX/Z-series only)**: Specifies the source port number to match in outbound traffic. This can be a single port, port range, multiple comma-separated ports, or "any".
- **Destination**: Specifies the destination FQDN, IP address or network address using CIDR notation to match in outbound traffic. "Any" can also be used to specify all networks. Note that, on a network with an MX handling inter-VLAN routing, the IP address of the MX on the destination subnet may still be accessible via ping even if the rule is set to block traffic. This is due to the nature of software routing on the MX and does not pose a security risk; host devices on the destination subnet will still be blocked according to the rule.
- **Dst port**: Specifies the remote port number to match in outbound traffic. On the MX, this can be a single port or multiple comma-separated ports. On the MR, this can be a single port or port range.
- **Comment**: A description of the rule.
- **Hits (MX/Z-series only)**: A counter reflecting the number of times the rule was applied. The counter starts each time the page is accessed.
- **Actions**: Options to delete or change the order of a rule.
- **Logging**: If syslog reporting is enabled, denotes whether or not to report on a given rule.

In MX 13.4 firmware and higher, fully qualified domain names can be configured in the Destination field. For more details, please read the FQDN Support section of Firewall Settings.
Example Configurations

Use Case 1: In the example below we want to block all IP traffic originating from network 10.0.0.0/8 that is destined for network 192.168.1.0/24. However, we do not want to block traffic originating from network 192.168.1.0/24 that is destined for 10.0.0.0/8 or block either network from accessing other remote networks such as the Internet.

Based on the rules shown below, any traffic originating from the 10.0.0.0/8 network destined for the 192.168.1.0/24 network matches rule 1 which is evaluated first. Because the "Policy" for this rule specifies a "Deny" action, the firewall will block all traffic when the rule is hit. The second rule evaluated which is the default rule, enforces an implicit allow all. All other traffic will match this rule. Hosts on either network can send data to any other remote network.

Note: When selecting "ANY" from the Protocol menu, the choice for Src port and Dst port become grayed out because this setting matches all IP traffic.

Use Case 2: In the example below, we want to allow any host in the network 10.0.0.0/8 to access a web server 192.168.1.254 that is listening on TCP port 80. However, we want to block any other outbound traffic from hosts in 10.0.0.0/8 or host 192.168.1.254.
Based on the rules shown below, traffic originating from any host on the 10.0.0.0/8 network that is destined for web server 192.168.1.254 on TCP port 80 is allowed. When the local host communicates with a service on a remote host, it normally picks an ephemeral source port and sends traffic to the port used by the service on the remote host. This is why the source port in this rule is set to "Any." Because there is an implicit allow rule processed last and we want to perform a "Deny" action on all other outbound traffic from hosts on the 10.0.0.0/8 network and the web server, a deny all rule is required. This rule needs to be evaluated right after rule 1. Because the firewall is stateful, replies from the web server to hosts on the 10.0.0.0/8 network are allowed the bypass the deny rule due to the connection is already being established. The deny will rule which is processed second will match all other traffic besides traffic to the web server.

**Note:** Cisco Meraki firewalls implement an inherent Allow All rule which can't be modified and is the last rule processed. Firewall rules are processed from the top down.

<table>
<thead>
<tr>
<th>#</th>
<th>Policy</th>
<th>Protocol</th>
<th>Source</th>
<th>Src port</th>
<th>Destination</th>
<th>Dist port</th>
<th>Comment</th>
<th>Hits</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Allow</td>
<td>TCP</td>
<td>10.0.0</td>
<td>Any</td>
<td>192.168.1.254/32</td>
<td>80</td>
<td>Allow web</td>
<td>0</td>
<td>✗: X</td>
</tr>
<tr>
<td>2</td>
<td>Deny</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny all</td>
<td>0</td>
<td>✗: X</td>
</tr>
<tr>
<td></td>
<td>Allow</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Resources**

- [MR Firewall Rules](#)
- [MX Firewall Settings](#)
- [Creating a Layer 7 Firewall Rule](#)
- [Layer 3 and 7 Firewall Processing Order](#)
Blocking Websites with Content Filtering and Layer 7 Firewall Rules