MR Firewall Rules

Custom firewall rules provide an administrator with more granular access control beyond LAN isolation. An administrator can define a set of firewall rules that is evaluated for every request sent by a wireless user associated to that SSID. Firewall rules are evaluated from top to bottom. 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.

Layer 3 Firewall Rules

As an example, the figure below depicts a sample set of custom firewall rules that will be enforced at layer 3.

Different kinds of requests will match different rules, as the table below shows. For a web request to CNN, rules 1-4 do not match, so rule #5 (the default rule) applies, and the request is allowed. In contrast, for a BitTorrent request over TCP port 6881, rule #1 does not match, but rule #2 matches. The request is denied, and no subsequent rules are evaluated.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(no match)</td>
<td>(no match)</td>
<td>MATCH (deny)</td>
<td>MATCH (deny)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>(no match)</td>
<td>(no match)</td>
<td>(no match)</td>
<td>MATCH (deny)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(no match)</td>
<td>MATCH (allow)</td>
<td>(no match)</td>
<td>(no match)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(no match)</td>
<td>(no match)</td>
<td>MATCH (allow)</td>
<td>MATCH (allow)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>MATCH (allow)</td>
<td>(no match)</td>
<td>(no match)</td>
<td>MATCH (allow)</td>
<td></td>
</tr>
</tbody>
</table>

Create a "Deny Local LAN" firewall rule to easily create secure guest SSID.
Layer 7 Firewall Rules

Using Meraki’s unique layer 7 traffic analysis technology, it is possible to create layer 7 firewall rules to completely block certain applications without having to specify specific IP addresses or port ranges using Meraki’s heuristic application fingerprints. This can be useful when applications use multiple or changing IP addresses or port ranges.

It is possible to block applications by category (e.g. ‘All video & music sites’) or for a specific type of application within a category (e.g. only iTunes within the ‘Video & music’ category). The figure below illustrates a set of layer 7 firewall rules including applications blocked by entire categories and specific applications blocked within a category:

<table>
<thead>
<tr>
<th>#</th>
<th>Policy</th>
<th>Application</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td>Blogging</td>
<td>All Blogging</td>
</tr>
<tr>
<td>2</td>
<td>Deny</td>
<td>HTTP hostname...</td>
<td>facebook.com</td>
</tr>
<tr>
<td>3</td>
<td>Deny</td>
<td>File sharing</td>
<td>All File sharing</td>
</tr>
<tr>
<td>4</td>
<td>Deny</td>
<td>Gaming</td>
<td>Battle.net</td>
</tr>
</tbody>
</table>
Configuration

Firewall rules can be applied for a given SSID or as part of a group policy. The SSID level firewall is configured on the Wireless > Firewall and Traffic Shaping page for each SSID. For a detailed article on group policy configuration click here.