Layer 3 and 7 Firewall Processing Order

Firewall rules on MR Series Access Points and MX Series Security Appliances are processed in a top down fashion, with Layer 3 rules being processed, followed by Layer 7 rules. Unless traffic is explicitly blocked by at least one rule, it will be allowed through by a default allow all rule.

Reference L3 and L7 Rules

For the examples to follow, the Layer 3 (L3) and Layer 7 (L7) firewall rules shown below will be used, with a Security Appliance network used for reference.

Traffic Allowed by Default

By default, outbound traffic will be allowed through the firewall unless explicitly blocked by at least one L3 or L7 rule. In this example, SSH (TCP port 22) traffic will be allowed through the firewall because there are no configured L3 or L7 rules that act upon it.

Layer 3 Rules

1. No Match
2. No Match
3. No Match

Layer 7 Rules

1. No Match
Traffic Blocked by Layer 3 Rule

In this example, SMTP traffic (TCP port 25) will be blocked by the L3 firewall, because rule 3 under layer 3 explicitly blocks it. Layer 7 rules would be ignored because the traffic has already been blocked.

Layer 3 Rules

1. No Match
2. No Match
3. Matched - Traffic blocked

Layer 7 Rules

1. Not processed because traffic was already blocked

Traffic Blocked by Layer 7 Rule

The MR access point and MX security appliance differ slightly in their processing of L7 firewall rules after the L3 firewall. On the MR, if traffic matches an allow rule on the L3 firewall, that traffic will bypass the L7 firewall altogether. On the MX, if traffic matches an allow rule on the L3 firewall, it can still be blocked by an L7 firewall rule.

On the **MX**, HTTP traffic (TCP port 80) to Facebook.com will be blocked by the L7 firewall, because rule 1 under layer 7 explicitly blocks it, even though the traffic was allowed through the layer 3 firewall.

Layer 3 Rules

1. Matched - Traffic allowed through L3 firewall
2. Not processed
3. Not processed

Layer 7 Rules

1. Matched - Traffic blocked

On the **MR**, HTTP traffic (TCP port 80) to Facebook.com will be allowed through the firewall, because rule 1 under layer 3 explicitly allows it.

Layer 3 Rules

1. Matched - Traffic allowed through L3 firewall
2. Not processed
3. Not processed

Layer 7 Rules

1. Not processed because traffic was already allowed
Group Policy Behavior

By default for MX L3 and L7 firewalls are processed independently, as illustrated above. Note that L3 and L7 rules in a group policy behave as one logical firewall just like an MR, again as illustrated above. With L3 being processed before L7, meaning that any allowed denied L7 applications (e.g. Netflix) would be allowed if the L3 portion of the rule contained an explicit allow for HTTP/HTTPS.