

Understanding APE Rulebase Actions

Actions are responses to sessions that match the source/destination/service or source/destination/application condition.

Table 1 describes the actions you can specify for APE rulebase rules.

Table 1: IDP Rulebase Actions

Action	Description
Rate Limit	<p>Rate limits set an aggregate limit for all matching sessions. If a session matches an APE rule where a rate limit has been set, the IDP engine performs a rate-limit check. If the limit has not been reached, the IDP appliance forwards the packets. If the limit has been reached, the IDP appliance behaves as if no bandwidth is available: it drops packets until the aggregate bandwidth falls below the limit. When the IDP appliance drops packets, the TCP or UDP endpoints identify the packet loss and slow down the transmission rate.</p> <p>The rate limits that make sense for your business case depend on the bandwidth for your links. If you have a 1-Gbps link, and want no more than 10% available to peer-to-peer traffic, the sum of the rate limits you specify for all peer-to-peer rules should be less than 102.4 Mbps (in each direction).</p> <p>You configure separate rate limits for client-to-server and server-to-client directions. For peer-to-peer traffic, we recommend you set the same rate for each direction.</p> <p>NOTE: For TFTP traffic, all traffic is counted as client-to-server traffic. A TFTP server responds to get requests by establishing an ephemeral port from which to send the reply. In this case, both directions appear to the IDP appliance as client-to-server flows. We recommend you set the same rate for each direction.</p> <p>Logs generated for traffic that match this rule display Rate Limit and traffic direction (c2s or s2c).</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, the rate limiting action has no effect in sniffer mode.</p>
None	<p>Does not perform rate limiting. Logs generated for traffic that match this rule display Accepted.</p>
Close Client and Server	<p>Closes the connection and sends an RST packet to both the client and the server.</p> <p>Logs generated for traffic that match this rule display Close.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p>
Close Client	<p>Closes the connection to the client but not to the server.</p> <p>Logs generated for traffic that match this rule display Close Client.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p>

Table 1: IDP Rulebase Actions (continued)

Action	Description
Close Server	<p>Closes the connection to the server but not to the client.</p> <p>Logs generated for traffic that match this rule display Close Server.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. However, if you use ACM to configure a sniffer mode reset interface, the IDP device can send an RST packet to both the client and server but does not close the connection.</p>
DiffServ Marking	<p>Assigns the DiffServ value you specify to the packet.</p> <p>Logs generated for traffic that match this rule display DiffServ.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, this action has no effect in sniffer mode.</p>
Drop Connection	<p>Drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</p> <p>Logs generated for traffic that match this rule display Drop Connection.</p> <p>NOTE: In sniffer mode, the IDP appliance is not in the path of network traffic. Therefore, this action has no effect in sniffer mode.</p>

Related Topics The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the APE Rulebase

The following related topic is included in the *IDP Administration Guide*:

- Configuring the APE Rulebase (NSM Procedure)

Published: 2010-01-12