

Understanding the APE Rulebase

The APE rulebase (application policy enforcement) leverages the application identification feature to enable you to manage network traffic based on application. APE rules match source-destination-application criteria. APE rules do not use attack objects.

You can configure rule actions to meet application policy enforcement objectives. For example:

- To use the IDP appliance like an application firewall, you can specify drop or close actions. Matching traffic is terminated at the IDP appliance.
- To set a cap on available bandwidth for disfavored applications or use of certain applications by certain users, you can specify a rate limiting action. When the limit is reached, the IDP appliance begins dropping matching traffic.
- To support deployments where you use your other network equipment to implement quality-of-service (QoS) guarantees, you can specify a DiffServ marker action. The IDP engine applies the DSCP marker to matching applications or user roles.

Any traffic not terminated by APE rules can be inspected subsequently by the IDP rulebase and other rulebases.

When you create rules for the APE rulebase, you specify:

- Match conditions
- An action
- Notification options

Related Topics The following related topics are included in the *IDP Concepts and Examples Guide*:

- Understanding APE Rulebase Match Conditions
- Understanding APE Rulebase Actions
- Understanding APE Rulebase Notification Options
- APE Rulebase Example: Limiting Bandwidth to Instant Messaging and Peer-to-Peer Traffic in the Enterprise
- APE Rulebase Example: Using User-Role-Based Rules to Support Tiered Subscriptions

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

- Configuring the APE Rulebase (NSM Procedure)