

Using Application Identification

The application identification feature enables the IDP engine to detect applications running on standard ports or nonstandard ports. Port independent application identification enhances both security and manageability by eliminating the need to manually and comprehensively configure application-port mapping for the service objects used in the IDP rulebase and APE rulebase rules.

The application identification feature uses application signatures provided by the Juniper Security Center team (J-Security Center) to identify the session application. J-Security Center updates signatures and develops new ones as necessary. Updates are provided to customers during routine detector engine updates. You cannot create custom signatures.

When the application identification feature identifies a new application, it caches the result (the destination address, port, protocol, and service) to reduce processing required for subsequent sessions.

When the IDP engine processes security policy rules, it examines the session beginning with the first packet to determine a match. To match service or application, the IDP engine first tries to match the session against the application identification cache to determine the application. If the session does not match the application identification cache, the IDP engine processes the session against the application signatures to determine the application. If the IDP engine is still unable to determine the application, it uses the standard application protocol and port.

In IDP rulebase rules, with application identification enabled, you set the service object in rules to **Default** to allow the application identification feature to determine the correct service. If you set service to a specific service object, application identification is not applied and the rule is processed using the service object properties.

In APE rulebase rules, you can specify a match based on application or service. With the application identification feature enabled, you should specify a match based on application. If you disable application identification and specify a match based on application, the IDP engine uses the standard application protocol and port for the application. If your application is not supported by the application identification feature, you can specify a match based on service and configure a custom service object.

The application identification feature is enabled by default. You have the option to disable the feature and to tune the following parameters (if necessary):

- Maximum number of sessions utilizing application identification
- Maximum memory used by application identification
- Maximum memory for saving TCP or UDP packets per session

For complete procedures on tuning these parameters, see the *IDP Administration Guide*.

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

- IDP Rulebase Example: Using Application Identification
- Understanding the IDP Rulebase
- J-Security Center Updates Overview

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

- Specifying Rule Match Conditions (NSM Procedure)

Published: 2010-01-12