

Understanding APE Rulebase Match Conditions

IDP inspects the session beginning with the first packet to determine whether it matches an APE rulebase rule. If the session matches all of the rule settings for source or user role, destination, service or application, and VLAN tag ID, IDP takes the action specified by the rule. If the session matches only some of the rule settings, IDP does not apply the rule action.

The APE rulebase is a terminal rulebase. Rules are evaluated in numerical order. The first rule to match is applied and subsequent rules are not processed.

If an APE rule matches but the action does not drop the connection, IDP also processes additional rulebases to inspect for attacks. If an attack rule determines the connection be closed or dropped, that action is taken and the rate-limiting action is not required.

Table 1 provides guidelines for setting IDP rulebase match conditions.

Table 1: APE Rulebase Match Condition Guidelines

Setting	Guideline
From zone/To zone	Not applicable for standalone IDP appliances.
Source	<p>Requires one of the specified source IP addresses to match the session for the rule to be applied. You can add address objects for hosts, groups, or network address ranges.</p> <p>You must choose between source IP address or user role as match criteria for a rule. You cannot configure both for one rule.</p> <p>Specify Any to not use source as a key to your match.</p> <p>NOTE: If a value for user role matches, the source parameter is not used.</p>
User Role	<p>Requires one of the specified user roles to match the session for the rule to be applied.</p> <p>You must choose to configure either source IP address or user role as match criteria for a rule. User role-based rules are evaluated before IP address-based rules. If a user-role based rule matches, the rule is applied and IP address-based rules are not consulted.</p> <p>Matching based on user role depends on integration with a Juniper Networks IC Series Unified Access Control appliance.</p>
Destination	<p>Requires one of the specified destination IP addresses to match the session for the rule to be applied. You can add address objects for hosts, groups, or network address ranges.</p> <p>Specify Any to not use destination as a key to your match.</p>

Table 1: APE Rulebase Match Condition Guidelines (continued)

Setting	Guideline
Service	<p>Requires one of the specified services to match the session for the rule to be applied. Services are Application Layer protocols that define how data is structured as it travels across the network. The IDP engine can inspect services that use TCP, UDP, RPC, and ICMP Transport Layer protocols. If the application running on the destination server uses standard ports, you can select from predefined services. If the application running on the destination server uses nonstandard ports, you must create a custom service object.</p> <p>If you specify named values for both service and application, only the application value is used.</p> <p>We recommend you specify Default for the service parameter and configure the application parameter instead.</p> <p>Specify Any to not use service as a key to your match.</p> <p>NOTE: To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to Any.</p>
Application	<p>Requires one of the specified applications to match the session for the rule to be applied. The predefined list of applications is populated by the application identification feature. The application identification feature identifies the application regardless of port. Port-independent application identification simplifies rule configuration and ensures you do not miss applications running on nonstandard ports. For this reason, we recommend you use the application parameter instead of the service parameter whenever possible.</p> <p>If you specify named values for both service and application, only the application value is used.</p> <p>Specify Any to not use application as a key to your match.</p> <p>NOTE: To apply an APE action to all traffic matching source and destination parameters, set both the service parameter and the application parameter to Any.</p>
VLAN	<p>Requires one of the specified VLAN tags to match the session for the rule to be applied.</p> <p>Specify Any to not use VLAN tag as a key to your match.</p>



TIP: You can use Profiler to identify the destination servers and services that are included in your network. In NSM, you can create address objects and service objects to facilitate configuration. One benefit of using objects is that you can configure them once and then use them in multiple rules. For details, see the NSM online Help.

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

- Understanding the Rule-Matching Algorithm
- Understanding the APE Rulebase
- User-Role-Based Policy Feature Overview
- Using Application Identification

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

- Configuring the APE Rulebase (NSM Procedure)

Published: 2010-01-12