

Understanding IDP Rulebase Rule Match Settings

IDP inspects the session beginning with the first packet to determine whether the session matches a rule. If the session matches all rule settings for source, destination, service, and VLAN tag ID, IDP decodes the traffic and inspects the session packets for the attack objects specified in the rule. If the session matches only some of the rule settings, the rule is not a match.

Table 1 provides guidelines for setting IDP rulebase match conditions.

Table 1: IDP 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>NOTE: 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>In most cases, to detect incoming attacks that target your internal network, specify Any. Specifying Any means you are not using source as a key to your match.</p> <p>To detect traffic from spyware that has affected hosts in your internal network, specify internal network addresses as the source.</p> <p>To detect attacks between two networks you manage, specify multiple addresses. The more specific you are in defining the source and destination of an attack, the more you reduce false positives.</p>
User Role	<p>Requires one of the specified user roles to match the session for the rule to be applied. If a value for User Role matches, the Source parameter is not consulted.</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>NOTE: Matching based on user role depends on integration with the Juniper Networks IC Series Unified Access Controller (UAC) 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>In most cases, specify the hosts or servers you want to protect.</p> <p>Specify Any to not use destination as a key to your match. For example, it would be impossible to predict the destination IP address for traffic resulting from spyware in your internal network. Specify Any for rules that target spyware attacks.</p>

Table 1: IDP 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. IDP 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>TIP: Specify Default to match the service(s) specified in the rule attack object(s). If the application identification feature is enabled, the IDP process engine identifies services even if they are running on nonstandard ports.</p> <p>If you disable application identification and specify Default, the IDP process engine assumes that standard ports are used for the service.</p> <p>NOTE: If you disable application identification and your service uses nonstandard ports, you must create custom service objects. For procedures, see the <i>IDP Administration Guide</i>.</p> <p>Specify Any to not use service as a key to your match.</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 hosts 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 topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the IDP Rulebase
- User-Role-Based Policy Feature Overview
- Using Application Identification
- IDP Rulebase Example: Specifying the Default Service
- IDP Rulebase Example: Using Application Identification

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

- Specifying Rule Match Conditions (NSM Procedure)

Published: 2010-01-12