

## Using Attack Objects

---

If the session matches rule settings for source, destination, service, and VLAN tag ID, the IDP engine decodes the traffic and inspects the session packets for the attack objects specified in the rule. The following topics provide guidelines for using attack objects in IDP rulebase rules:

- Attack Objects Overview on page 1
- Understanding Predefined Attack Objects and Attack Object Groups on page 2
- Using Custom Attack Object Groups on page 2
- Using Custom Attack Objects on page 3

### Attack Objects Overview

When traffic matches an IDP rulebase source/destination/service condition, the IDP engine inspects the traffic for the attack objects you specify.

A *signature attack object* detects known attacks using stateful attack signatures. An attack signature is a pattern that always exists within an attack; if the attack is present, so is the attack signature. With stateful signatures, the IDP engine can look for the specific protocol or service used to perpetrate the attack, the direction and flow of the attack, and the context in which the attack occurs. Stateful signatures produce few false positives because the context of the attack is defined, eliminating huge sections of network traffic in which the attack would not occur.

A *protocol anomaly attack object* identifies unusual activity on the network. It detects abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used. Protocol anomaly detection works by finding deviations from protocol standards, most often defined by RFCs and common RFC extensions. Most legitimate traffic adheres to established protocols. Traffic that does not, produces an anomaly, which may be created by attackers for specific purposes, such as evading an IPS.

A *compound attack object* combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the compound attack object; you can specify the order in which signatures or anomalies must match. Use compound attack objects to refine your IDP policy rules, reduce false positives, and increase detection accuracy. A compound attack object enables you to be very specific about the events that need to occur before the IDP engine identifies traffic as an attack. You can use **And**, **Or**, and **Ordered and** operations to define the relationship among different attack objects within a compound attack and the order in which events occur.

Attack object definitions also include data fields to help you group and manage attack objects and use them in security policies. These data fields include category, severity, keywords, and a recommended flag.

*Predefined attack objects* provided by the Juniper Networks Security Center (J-Security Center) team also contain a recommended action for the IDP appliance to take against the attack session.

*Custom attack objects* are ones you create, if your security policy requires more or less protection, or more or less accounting than what the predefined attack objects provide.

Both predefined and custom attack objects are stored in the attack object database.

When you add attack objects to an IDP rulebase rule, you can add attack objects by group or individually.

## **Understanding Predefined Attack Objects and Attack Object Groups**

The Juniper Networks Security Center (J-Security Center) team has developed more than 600 attack objects and these are included in the attack object database used in IDP security policies.

Table 1 describes the attack object groups provided by the J-Security Center.

**Table 1: Predefined Attack Object Groups**

<b>Group</b>	<b>Contents</b>
Attack Type	Contains two subgroups: anomaly and signature. Within each subgroup, attack objects are grouped by severity.
Category	Contains subgroups based on category. Within each category, attack objects are grouped by severity.
Operating System	Contains the following subgroups: BSD, Linux, Solaris, and Windows. Within each operating system, attack objects are grouped by services and severity.
Severity	Contains the following subgroups: Critical, Major, Minor, Warning, Info. Within each severity, attack objects are grouped by category. Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).
Web Services	Contains subgroups based on Web services. Within services, attacked objects are grouped by severity.
Miscellaneous	Contains attack objects that have a significant affect on IDP performance.
Response	Contains attack objects where the attack is detected in the server-to-client direction. This group contains a hierarchy of subgroups that includes all of the above categories.

J-Security Center updates the attack object database to provide new attack objects, to revise severities or recommendations, or to remove obsolete attack objects. We recommend you schedule routine, automatic updates.

## **Using Custom Attack Object Groups**

A *dynamic group* contains members that match properties you specify for the group. You use dynamic groups so that an attack database update automatically populates the group with relevant members. This eliminates the need to review each new signature to determine if you need to use it in your existing security policy. A

predefined or custom dynamic group can only contain attack objects and not attack groups. Dynamic group members can be either predefined or custom attack objects.

A *static group* is not automatically updated with new members. It contains only the attack objects or groups you have added. Use static groups when you do not want your attack group dynamically populated during NSM updates. For example, if you customize the action for predefined attack objects to meet your company's security policy guidelines, you can create one or more static groups to contain these attack objects. When you perform an NSM attack object update, your static group will not be affected.

There are two types of static groups: predefined static groups and custom static groups. Predefined static groups are categories of groups provided by default.

A custom static group can include the same members as a predefined static group (predefined attack objects, predefined static groups, and predefined dynamic groups), plus the following members:

- Custom attack objects
- Custom dynamic groups
- Other custom static groups

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to manage the members. However, you can include a dynamic group within a static group to automatically update some attack objects. For example, the predefined attack object group Operating System is a static group that contains four predefined static groups: BSD, Linux, Solaris, and Windows. The BSD group contains the predefined dynamic group BSD-Services-Critical, to which attack objects can be added during an attack database update.

## **Using Custom Attack Objects**

The attack objects provided by the Juniper Networks Security Center (J-Security Center) team cover most cases for small business, enterprise, and service provider networks. Your business might encounter cases where you must modify a predefined attack object or create a new one. For example:

- You read a security advisory about a known attack and want to create an attack object that detects the malicious traffic described in that advisory.
- You need to update or improve an existing third-party signature (such as a Snort signature).
- You want to customize an existing signature or protocol anomaly attack object for your local environments. For example, you might need to customize a signature to prevent false positives generated by a specific application running on your network.
- You want to detect specific activity on your network. For example, you might want to detect abnormal traffic (possibly malicious), remote log-ins, or brute force attacks that attempt to guess usernames and passwords.

For a complete tutorial on creating custom attack objects, see the *IDP Custom Attack Objects Reference and Examples Guide*.

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

- J-Security Center Updates Overview
- Understanding the IDP Rulebase
- IDP Rulebase Example: Using Recommended Attack Objects
- Exempt Rulebase Example: Exempting an Attack Object

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

- Attack Objects Task Summary

---

Published: 2010-01-12