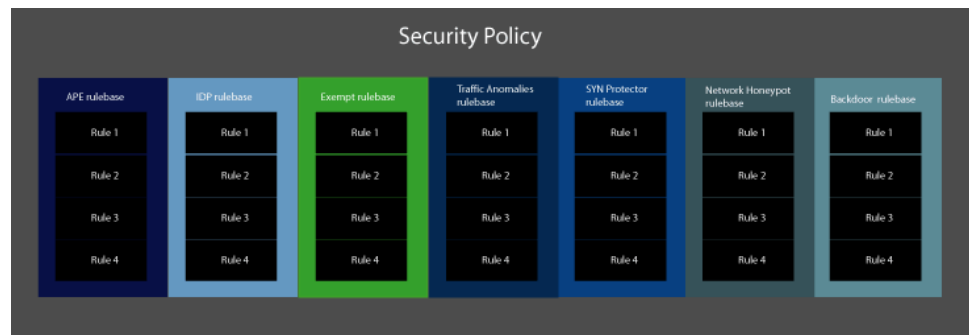


Understanding the Components of an IDP Security Policy

An IDP security policy defines how an IDP appliance handles network traffic. It allows you to enforce various attack detection and prevention techniques on traffic that traverses your network.

Figure 1 illustrates the components of an IDP security policy.

Figure 1: Security Policy Components



A security policy is made up of one or more rulebases. A *rulebase* is an ordered set of rules that use a particular detection method to identify and prevent attacks.

Table 1 describes the IDP security policy rulebases. A security policy can contain only one instance of any rulebase type.

Table 1: IDP Security Policy Rulebases

Rulebase	Description
APE rulebase	Enables you to implement application policy enforcement rules. You can use APE rules to manage sessions based on application and/or user role. You can terminate matching sessions or limit bandwidth available to them. See Understanding the APE Rulebase.
IDP rulebase	Protects your network from attacks by using attack objects to detect known and unknown attacks. Juniper Networks Security Center (J-Security Center) provides predefined attack objects that you can use in IDP rules. You can also configure your own custom attack objects. See Understanding the IDP Rulebase.
Exempt rulebase	You configure rules in this rulebase to exclude known false positives or to exclude a specific source, destination, or attack object from matching an IDP rule. If traffic matches a rule in the IDP rulebase, IDP attempts to match the traffic against the Exempt rulebase before performing the action specified. See Understanding the Exempt Rulebase.

Table 1: IDP Security Policy Rulebases (continued)

Rulebase	Description
Traffic Anomalies rulebase	Protects your network from attacks by using traffic flow analysis to identify attacks that occur over multiple connections and sessions (such as scans). See Understanding the Traffic Anomalies Rulebase.
SYN Protector rulebase	Protects your network from SYN-floods by ensuring that the three-way handshake is performed successfully for specified TCP traffic. If your network is vulnerable to SYN-flood attacks, use the SYN-Protector rulebase to prevent it. See Understanding the SYN Protector Rulebase.
Network Honeypot rulebase	Protects your network by impersonating open ports on existing servers on your network, alerting you to attackers performing port scans and other information-gathering activities. See Understanding the Network Honeypot Rulebase.
Backdoor rulebase	Protects your network from mechanisms installed on a host computer that facilitate unauthorized access to the system. Attackers who have already compromised a system typically install backdoors (such as Trojans) to make future attacks easier. When attackers send and retrieve information to and from the backdoor program (as when typing commands), they generate interactive traffic that IDP can detect. See Understanding the Backdoor Rulebase.



NOTE: Firewall rulebases, visible in NSM, do not apply to standalone IDP appliances.

Rules are instructions that provide context to detection methods. Rules specify:

- A match condition that determines which traffic to inspect
- Attack objects that determine what to look for (IDP rulebase and Exempt rulebase)
- Actions and operation modes that determine what to do when traffic matches a rule
- Notification options, including logs, alerts, and packet captures

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

- Understanding the Number of Available and Installed Policies
- Understanding the Rule-Matching Algorithm
- Example: Fine-Tuning a Security Policy

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

- Developing Security Policies Task Summary

Published: 2010-01-12