

Intrusion Detection and Prevention Devices and Security Policies Overview

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

For a detailed explanation of security policy features and components, and for examples, see the *IDP Concepts & Examples Guide*.

To create an effective security policy, follow these basic steps:

1. Run the New Policy wizard to create a new security policy object. The new security policy can be based on a predefined template.
2. Use the Security Policy editor to add 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
Application Rulebase	Enables you to limit bandwidth for specified users and applications and thus helps to manage network traffic. APE rules do not use attack objects..
IDP Rulebase	Protects your network from attacks by using attack objects to detect known and unknown attacks. Juniper Networks provides predefined attack objects that you can use in IDP rules. You can also configure your own custom attack objects.
Exempt Rulebase	You configure rules in this rulebase to exclude known false positives or to exclude a specific source, destination, or source/destination pair 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.
Backdoor Rulebase	Protects your network from mechanisms installed on a host computer that facilitates 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.
SYN Protector Rulebase	Protects your network from SYN-floods by ensuring that the three-way handshake is performed successfully for specified TCP traffic. If you know that your network is vulnerable to a SYN-flood, use the SYN-Protector rulebase to prevent it.
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).
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.

3. Within rulebases, configure rules.

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

- A source/destination/service match condition that determines which traffic to inspect
- Attack objects that determine what to look for (IDP rulebase and Exempt rulebase)
- Actions that determine what to do when an attack is detected
- Notification options, including logs, alerts, and packet captures

Each rulebase can contain up to 40,000 rules.

4. Fine-tune your security policy as you learn more about your network and security requirements and IDP capabilities.

Related Topics

- Configuring Predefined Security Policies (NSM Procedure)
- Creating a New Security Policy (NSM Procedure)
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)
- Troubleshooting Security Policy Validation Errors (NSM Procedure)