

Using the Recommended Security Policy

The highly respected Juniper Networks Security Center team (J-Security Center) provides the default IDP security policy—named Recommended. We advise that you use this policy (or customize it) to protect your network from the likeliest and most dangerous attacks.

Table 1 summarizes the properties of the Recommended security policy.

Table 1: Recommended Security Policy Definition

Property	Value
Rulebase	IDP rulebase
Rules	Nine rules, distinguished by attack object
Source	Any
Service	Default, meaning the matching property is based on the service bindings of the attack object specified by the rule
Destination	Any
Attack objects	Recommended IP, Recommended TCP, Recommended ICMP, Recommended HTTP, Recommended SMTP, Recommended DNS, Recommended FTP, Recommended POP3, Recommended IMAP, Recommended Trojan, Recommended Virus, Recommended Worm
Action	Recommended, meaning the action is specified by the attack object
Notification	Logging

If you prefer, you can copy this security policy and use it as a template for a custom security policy tailored for your network.

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

- Understanding the IDP Rulebase
- IDP Rulebase Example: Specifying the Default Service
- IDP Rulebase Example: Using Application Identification
- IDP Rulebase Example: Using Recommended Attack Objects
- IDP Rulebase Example: Using Recommended Actions
- Example: Fine-Tuning a Security Policy

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

- Developing Security Policies Task Summary

Published: 2010-01-12