

Configuring Predefined Security Policies (NSM Procedure)

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 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	9 rules, distinguished by attack object
Traffic source	Any
Service	Default, meaning the matching property is based on the service bindings of the attack object specified by the rule
Destination	Any
Attacks	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.

Table 2 describes other IDP security policy templates.

Table 2: IDP Security Policy Templates

Template	Description
all_with_logging	Includes all attack objects and enables packet logging for all rules.
all_without_logging	Includes all attack objects but does not enable packet logging.
dmz_services	Protects a typical DMZ environment.
dns_server	Protects DNS services.
file_server	Protects file sharing services, such as SMB, NFS, FTP, and others.
getting_started	Contains very open rules. Useful in controlled lab environments, but should not be deployed on heavy traffic live networks.

Table 2: IDP Security Policy Templates (continued)

Template	Description
idp_default	Contains a good blend of security and performance.
web_server	Protects HTTP servers from remote attacks.

If you use these templates, we advise you customize them for your deployment. At a minimum, you should change the destination IP setting from **Any** to the IP addresses for specific servers you want to protect. For more information, see the *IDP Concepts & Examples guide*.

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Creating a New Security Policy (NSM Procedure)
 - Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)
 - Modifying IDP Rulebase Rules (NSM Procedure)

Published: 2009-08-20