

Using Other Security Policy Templates

NSM includes security policy templates you can use as the basis for a custom security policy tailored for your network. Template rules include a set of attack objects and logically associated IDP actions. If you choose to use these templates, we advise you to 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.

Table 1 describes IDP security policy templates.

Table 1: IDP Security Policy Templates

Template	Description
all_with_logging	Includes all attack objects and enables packet logging for all rules. This policy is provided for lab use and is not recommended in production.
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.
idp_default	Contains a set of attack groups that balances security and performance.
web_server	Protects HTTP servers from remote attacks.

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

- Using the Recommended Security Policy

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

- Developing Security Policies Task Summary

Published: 2010-01-12