



Cisco Network Planning Solution Design and Analysis NetDoctor User Guide for IT Guru

Software Release 11.0

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7543-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco Network Planning Solution

Design and Analysis

NetDoctor User Guide for IT Guru

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Copyright

Document Copyright

Title: NetDoctor User Guide for IT Guru
Part Number: D00187
Version: 11

© 1987-2005 OPNET Technologies, Inc.
All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

Software Copyright

Product Name: IT Guru
Product Release: 11.0

© 1987-2005 OPNET Technologies, Inc.
All Rights Reserved.

Documentation Conventions

OPNET documentation uses specific formatting and typographic conventions to present the following types of information:

- Objects, examples, and system I/O
- Object hierarchies, notes, and warnings
- Computer commands
- Lists and procedures

Objects, Examples, and System I/O

- Directory paths and file names are in plain Courier typeface:

```
opnet\release\models\std\ip
```

- Function names in body text are in italics:

```
op_dist_outcome()
```

- The names of functions of interest in example code are in bolded Courier typeface:

```
/* determine the object ID of packet's creation module */  
src_mod_objid = op_pk_creation_mod_get (pkptr);
```

- Variables are enclosed in angle brackets (< >):

```
<opnet_user_home>/op_admin/err_log
```

Object Hierarchies, Notes, and Warnings

Menu hierarchies are indicated by right angle brackets (>); for example:

```
Open File > Print Setup > Properties...
```

Attribute hierarchies are represented by angled arrows (▲) that indicate that you must drill down to a lower level of the hierarchy:

Attribute level 1 ▶ Attribute level 2 ▶ Attribute level 3

Note—Notes are indicated by text with the word Note at the beginning of the paragraph. Notes advise you of important supplementary information.

WARNING—Warnings are indicated by text with the word WARNING at the beginning of the paragraph. Warnings advise you of vital information about an operation or system behavior.

Computer Commands

These conventions apply to Windows systems and navigation methods that use the standard graphical-user-interface (GUI) terminology such as click, drag, and dialog box.

- Key combinations appear in the form “press <button>+x”; this means press the <button> and x keys *at the same time* to do the operation.
- The mouse operations *left-click* (or *click*) and *right-click* indicate that you should press the left mouse button or right mouse button, respectively.

Lists and Procedures

Information is often itemized in bulleted (unordered) or numbered (ordered) lists:

- In bulleted lists, the sequence of items is not important.
- In numbered lists, the sequence of items is important.

Procedures are contained within procedure headings and footings that indicate the start and end of the procedure. Each step of a procedure is numbered to indicate the sequence in which you should do the steps. A step may be followed by a description of the results of that step; such descriptions are preceded by an arrow.

Procedure FM-1 Sample Procedure Format

- 1 Procedure step.
 - ➔ Result of the procedure step.

- 2 Procedure step.

End of Procedure FM-1

For more information about using and maintaining OPNET documentation, see the OPNET IT Guru Documentation Guide.

Document Revision History

Release Date	Product Version	Chapter	Description of Change
February 2005	11.0 PL3	Using NetDoctor	<ul style="list-style-type: none"> Added section for template checker rules. (Device Configuration Imports (DCI) on page MVI-2-2 of the MVI User GuideVNE Server Import on page ITU-10-12 of the Guru User GuideVNE Server Import on page ISU-10-2 of the Sentinel User Guide). New Table of Contents. Added concise/detail rule page views for web report.
		Customizing NetDoctor	<ul style="list-style-type: none"> New Table of Contents. Reorganized chapter around workflow. Included content from OPNK Session 1306 in NetDoctor Reports section.
		Rules/Suites	<ul style="list-style-type: none"> Updated Rules appendix.
		NetDoctor APIs	<ul style="list-style-type: none"> Added 11.0 PL3 APIs.
November 2004	11.0 PL1	Customizing NetDoctor	<ul style="list-style-type: none"> Enhanced section on notifications. Reordered sections and modified some figures Added NetDoctor Reports. Added Rule Creation Examplet.
		NetDoctor APIs	Added 11.0 PL1 APIs.
		Rules/Suites	Updated Rules appendix.
August 2004	11.0	NetDoctor APIs	Reimported section for this release.
		Using NetDoctor	Added sections on auto-generate report template and report on selected objects. Separated template section into sub-headings.
		Customizing NetDoctor	Added sections on creating charts and multi-language report output. Updated rest of document, screenshots, etc.
January 2004	10.5	NetDoctor APIs	Grouped Reporting APIs together in its own section.
		Using NetDoctor	Added sections on notification and report comparison.
September 2003	10.0	Revision History	Section added to this manual.

Contents

	<i>Copyright</i>	ND-FM-iii
	<i>Documentation Conventions</i>	ND-FM-iv
	<i>Document Revision History</i>	ND-FM-vii
	<i>List of Figures</i>	ND-FM-xi
	<i>List of Tables</i>	ND-FM-xii
	<i>List of Procedures</i>	ND-FM-xiii
<hr/>		
1	Overview	ND-1-1
	System Requirements	ND-1-2
	How Does NetDoctor Work?	ND-1-3
	Types of NetDoctor Messages	ND-1-4
	Available Rule Suites	ND-1-4
	How This User Guide Is Organized	ND-1-6
<hr/>		
2	Administration	ND-2-1
	Adding and Activating a NetDoctor License	ND-2-1
	Using the NetDoctor Tutorial	ND-2-2
<hr/>		
3	Using NetDoctor	ND-3-1
	The NetDoctor Menu	ND-3-2
	Configuring NetDoctor	ND-3-4
	Creating Report Templates	ND-3-6
	Auto-Generate a Report Template	ND-3-7
	Manually Create a Report Template	ND-3-8
	Settings Tab	ND-3-10
	Generating a Report From a Template	ND-3-11
	Configuring Notifications	ND-3-13
	Viewing NetDoctor Reports	ND-3-16
	Report Formats	ND-3-16
	Web Report	ND-3-18
	Microsoft Word Report.	ND-3-21
	Comparing NetDoctor Reports.	ND-3-22
	Configuring Report Comparison	ND-3-22
	Analyzing a Comparison Report	ND-3-23
	Suppressing Messages	ND-3-24
	Configuring Global Options	ND-3-27
	Modeling Network Security.	ND-3-29
	Configuring Security Demands	ND-3-30
	Reusing Security Demand Configuration Information	ND-3-33
	Visualizing Network Security Configuration	ND-3-34
	Using Security Demands in Simulations Studies	ND-3-35

Generating Security Reports	ND-3-36
-----------------------------------	---------

Index

ND-IX-1

List of Figures

Figure 1-1	NetDoctor Workflow	ND-1-3
Figure 3-1	NetDoctor Menu	ND-3-2
Figure 3-2	Configure/Run NetDoctor Dialog Box: Rules Tab	ND-3-4
Figure 3-3	NetDoctor Web Report: Sample Output.	ND-3-6
Figure 3-4	Available Templates.	ND-3-6
Figure 3-5	Auto-Generate Report Template Dialog Box	ND-3-7
Figure 3-6	Parameter Description Tooltip	ND-3-9
Figure 3-7	Configure/Run NetDoctor Dialog Box: Settings Tab	ND-3-10
Figure 3-8	Run NetDoctor Dialog Box	ND-3-12
Figure 3-9	Notifications in the Configure/Run NetDoctor Dialog Box	ND-3-13
Figure 3-10	NetDoctor Notifications	ND-3-15
Figure 3-11	View Recent NetDoctor Reports Dialog Box	ND-3-16
Figure 3-12	NetDoctor Web Report.	ND-3-18
Figure 3-13	NetDoctor Web Report.	ND-3-18
Figure 3-14	Rule Output - Concise	ND-3-19
Figure 3-15	Rule Output - Detail	ND-3-20
Figure 3-16	NetDoctor Report in Microsoft Word	ND-3-21
Figure 3-17	Report Comparison Options.	ND-3-22
Figure 3-18	A Web Comparison Report	ND-3-23
Figure 3-19	Edit Suppressions Dialog Box	ND-3-25
Figure 3-20	Suppressed Message Count	ND-3-26
Figure 3-21	NetDoctor Options Dialog Box	ND-3-27
Figure 3-22	The Demands Object Palette	ND-3-30
Figure 3-23	Security Demand Attributes	ND-3-31
Figure 3-24	Create Security Demands Dialog Box	ND-3-32
Figure 3-25	Create Security Demands Dialog Box—With and Without Selection.	ND-3-33
Figure 3-26	Security Demand Configuration File	ND-3-34
Figure 3-27	Network Security Configuration Visualization	ND-3-34
Figure 3-28	Selecting Tables for Security Web-Report.	ND-3-36
Figure 3-29	Network Security Web Report	ND-3-37

List of Tables

Table 1-1	User Guide Contents	ND-1-6
Table 3-1	NetDoctor Menu Operations	ND-3-2
Table 3-2	Configure/Run NetDoctor Dialog Box: Settings	ND-3-10
Table 3-3	Email Notification Parameters	ND-3-14
Table 3-4	NetDoctor Report Organization	ND-3-17
Table 3-5	NetDoctor Options	ND-3-27

List of Procedures

Procedure 2-1	Adding a NetDoctor License	ND-2-1
Procedure 2-2	Activating a NetDoctor License	ND-2-1
Procedure 2-3	Opening the NetDoctor Tutorial	ND-2-2
Procedure 3-1	Running NetDoctor (Basic Configuration)	ND-3-5
Procedure 3-2	Auto-Generating a Report Template	ND-3-7
Procedure 3-3	Creating a Report Template Manually	ND-3-8
Procedure 3-4	Running NetDoctor from a Template	ND-3-12
Procedure 3-5	Viewing a Previous Report	ND-3-16
Procedure 3-6	Creating a Suppression File	ND-3-24
Procedure 3-7	Applying a Suppression File to a Template	ND-3-26
Procedure 3-8	Creating Security Demands	ND-3-30
Procedure 3-9	Creating Multiple Security Demands Simultaneously	ND-3-31
Procedure 3-10	Viewing Security Configuration in the Workspace	ND-3-34
Procedure 3-11	Viewing Security Reports	ND-3-36

1 Overview

NetDoctor is a powerful rules-based engine that proactively identifies incorrect device configurations, including policy violations and inefficiencies. NetDoctor exposes hidden problems that can be difficult to discover due to the sheer volume of configuration information distributed throughout the network. With NetDoctor's customizable environment, you can create your own rules to validate network configurations, verify network security policies, and assess how well a network conforms to defined policies.

NetDoctor rules are run against model attributes, which are set from device configurations you can import from a production network. Also, some NetDoctor rules use simulation data to identify inconsistencies in the operation or performance of the network.

Network managers and operators can use NetDoctor to

- locate network problems caused by misconfigurations
- identify latent problems that might affect the network in the future
- validate the network configuration against the policies of your organization

NetDoctor facilitates the task of checking your device configurations for errors before the configurations are deployed. This can prevent costly errors that would otherwise create problems in the production environment. NetDoctor identifies problems such as

- OSPF Area Border Routers that are not connected to the backbone area
- IBGP neighbors that are not fully meshed—including confederations and route reflectors
- ACLs that contain ineffective statements
- inconsistent interface parameters for OSPF that preclude the formation of adjacencies

With the addition of the Automation module, you can schedule NetDoctor to run at regular intervals, performing proactive analyses, generating reports, and sending optional notifications to you. Although you can still run NetDoctor manually, as needed, automating the process frees you to take care of other business.

NetDoctor produces its results in a customizable report, which you can view in a web browser or in Microsoft Word. Web reports offer support for multiple languages. NetDoctor includes built-in support for English and Japanese web reports—you can customize NetDoctor to generate reports in other languages, too.

System Requirements

To run NetDoctor, you need

- OPNET software (version 8.1 or later)
- a NetDoctor module license
- a Web browser (Netscape 7.0, Mozilla 1.4, or Internet Explorer 5.5 or later) or Microsoft Word

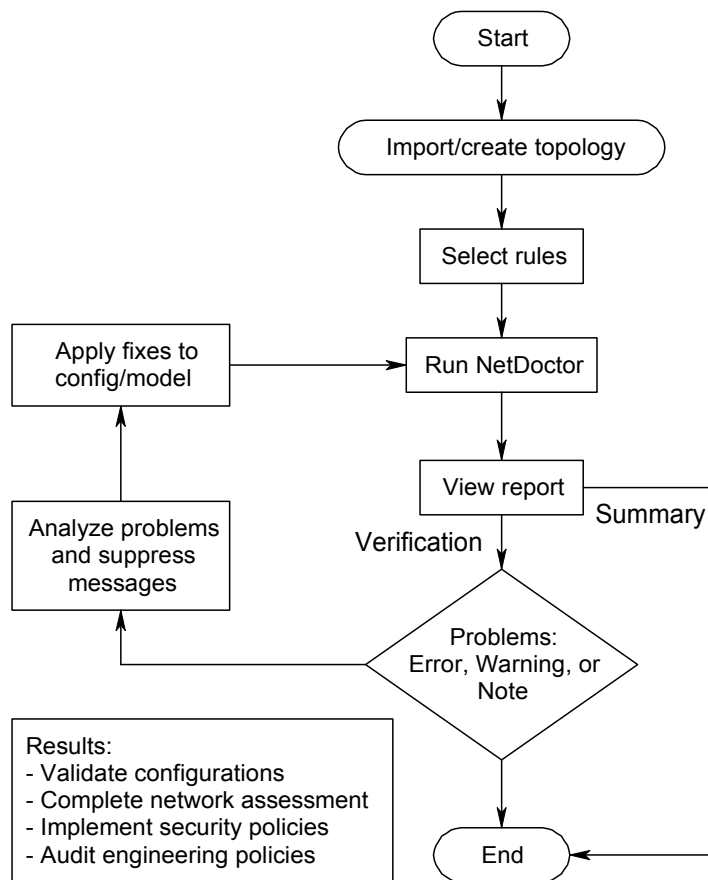
How Does NetDoctor Work?

When NetDoctor runs, it checks the current network model against a list of rules and generates a report with the results. There are two types of NetDoctor rules:

- Verification rules—These rules generate error, warning, or note messages to report on misconfigurations and other problems.
- Summary rules—These rules provide information about the configuration and operation of the network. For example, a summary rule could generate a report on the distinct OS versions deployed in the network, determine the number of routers running a given protocol, or generate a list of routes for all IP flows in the network.

The standard NetDoctor installation includes a variety of rule suites that you can use immediately and includes a development API that can be used to codify the expertise and policies of your organization into NetDoctor rules. You may also use NetDoctor’s template auto-generation feature to quickly analyze your network and intelligently select rules based on brief input from you. For example, the network operations group in a company can verify all proposed changes against rules that were created by the company’s design and planning group. Figure 1-1 shows a typical NetDoctor workflow.

Figure 1-1 NetDoctor Workflow



The rules that drive the NetDoctor analysis generate messages about existing or potential problems in the network configuration. After each run, NetDoctor organizes the messages into an easy-to-navigate report. NetDoctor can generate reports in Microsoft Word (.rtf) or as a web report.

Types of NetDoctor Messages

The verification messages generated by NetDoctor are given one of three severities:

- **Error**—A violation specifying that the severity of the reported problem is critical. It indicates the configuration might result in major network problems if it is deployed. These problems should be fixed to ensure the network is fully operational.
- **Warning**—A violation specifying that the reported problem is not considered critical. These problems should be fixed to prevent transient problems and degraded network performance.
- **Note**—Supplementary information about items in the NetDoctor analysis that you may find helpful.

You can configure NetDoctor to limit its reporting to messages that meet or exceed the severity level in which you are interested. See App A Suites and Rules on page ND-A-1 for a description of all available rules.

Available Rule Suites

NetDoctor comes with the following rule suites:

- AAA
- Administration
- ATM
- BGP
- DLSw
- EIGRP
- HSRP
- IGRP
- IP Addressing
- IP Multicast

- IP Routing
- IPSec
- IPX
- IS-IS
- Kerberos
- Link Aggregation
- MPLS
- MPLS VPNs
- NAT
- Organizational Policies
- OSPF
- PIX
- QoS
- RADIUS
- RIP
- Route Maps and ACLs
- RSRB
- Security
- SNMP
- Spanning Tree
- Static Routing
- System Logging
- TACACS+
- Tunnel Interfaces
- VLANs
- Voice over IP

NetDoctor can support additional protocols through custom rules.

How This User Guide Is Organized

This user guide is organized as follows.

Table 1-1 User Guide Contents

Chapter	Description
Overview	Gives general information about the functions and features of the NetDoctor module
Administration	Describes how to add and activate a NetDoctor license in your OPNET environment
Using NetDoctor	Describes about the menus and procedures for configuring and running NetDoctor, and for viewing NetDoctor output
End of Table 1-1	

2 Administration

This chapter describes how to ensure that the working environment is set up correctly and how to get started in NetDoctor.

- Adding and Activating a NetDoctor License
- Using the NetDoctor Tutorial

Adding and Activating a NetDoctor License

The NetDoctor module is automatically installed when you install OPNET. To use the module, you need to add a NetDoctor license to the local system and activate the license, as described in Procedure 2-1 and Procedure 2-2.

Procedure 2-1 Adding a NetDoctor License

- 1 Start OPNET.
- 2 Choose **License > License Management**.
- 3 Click the **Add License** button and follow the steps on the screen.

End of Procedure 2-1

Procedure 2-2 Activating a NetDoctor License

- 1 In the main OPNET window, choose **License > Product Modules**.
- 2 Select the **NetDoctor** check box if it is not already selected.
- 3 Click OK.

End of Procedure 2-2

Using the NetDoctor Tutorial

The documentation includes a tutorial on NetDoctor that is designed to familiarize you with NetDoctor features and the NetDoctor workflow. Procedure 2-3 describes how to access this tutorial.

Procedure 2-3 Opening the NetDoctor Tutorial

- 1 In the OPNET window, choose **Help > Tutorials**.
 - ➔ The complete list of OPNET tutorials appears.
- 2 From the Module Lessons field, choose **NetDoctor**.
 - ➔ The NetDoctor tutorial appears.

End of Procedure 2-3

3 Using NetDoctor

This chapter describes how to configure and use NetDoctor. Most of this chapter describes the operations used in the rules-based NetDoctor analysis. The last section of this chapter describes how to configure and run security analyses using security demands.

This chapter is organized as follows:

Workflow	Topic	Subtopics
Understanding and Using NetDoctor	The NetDoctor Menu	
	Configuring NetDoctor	<ul style="list-style-type: none"> • Creating Report Templates • Generating a Report From a Template • Device Configuration Imports (DCI) on page MVI-2-2 of the MVI User Guide • VNE Server Import on page ITU-10-12 of the Guru User Guide • VNE Server Import on page ISU-10-2 of the Sentinel User Guide
Understanding Templates	Creating Report Templates	<ul style="list-style-type: none"> • Auto-Generate a Report Template • Manually Create a Report Template
Understanding NetDoctor Reports	Viewing NetDoctor Reports	<ul style="list-style-type: none"> • Report Formats • Comparing NetDoctor Reports • Generating Security Reports
	Modifying NetDoctor Reports	<ul style="list-style-type: none"> • Suppressing Messages • Configuring Global Options
Understanding Network Security Models and Reports	Modeling Network Security	<ul style="list-style-type: none"> • Configuring Security Demands • Visualizing Network Security Configuration • Using Security Demands in Simulations Studies • Generating Security Reports • Reusing Security Demand Configuration Information

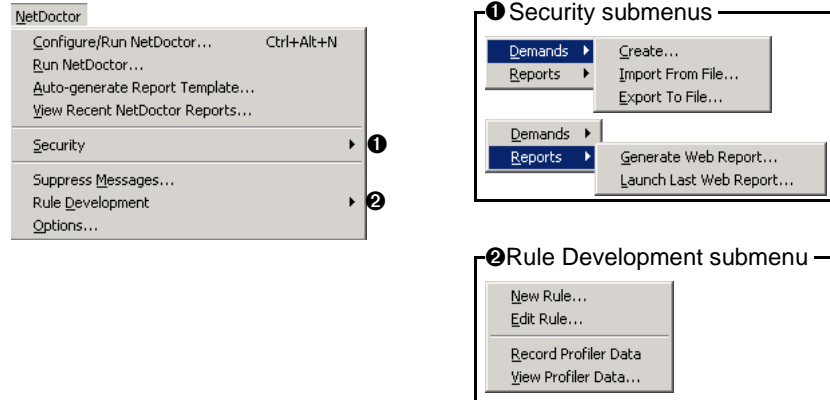
The NetDoctor Menu

From the NetDoctor menu, you can

- configure and run NetDoctor
- create new NetDoctor templates
- view NetDoctor reports
- create security audit reports
- suppress messages in NetDoctor reports
- create new and edit existing rules
- set NetDoctor specific options

Figure 3-1 NetDoctor Menu

NetDoctor main menu



The following table describes the operations of the NetDoctor menu.

Table 3-1 NetDoctor Menu Operations (Part 1 of 2)

Use this menu item...	To...
Configure/Run NetDoctor...	Configure, save, and run NetDoctor report templates.
Run NetDoctor...	Run NetDoctor using an existing report template.
Auto-Generate Report Template...	Create a new NetDoctor template based on the current network model and on the type of analysis you would like NetDoctor to perform.
View Recent NetDoctor Reports...	Choose a recently run NetDoctor report and open it in the appropriate viewer.
Security	Create security demands and run reports that analyze the security configuration of a network.

Table 3-1 NetDoctor Menu Operations (Part 2 of 2)

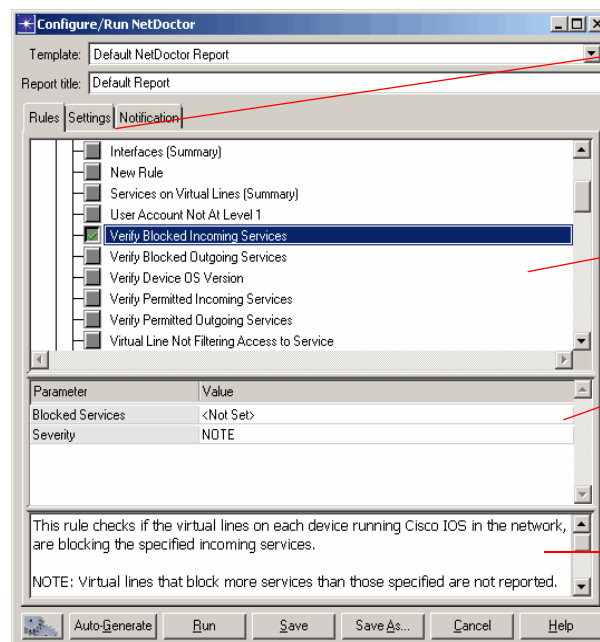
Use this menu item...	To...
Suppress Messages...	Create or edit suppression files.
Rule Development	Create new NetDoctor rules or edit existing rules. See Chapter 4 Customizing NetDoctor on page ND-4-1 for more information on rule development.
Options...	Set NetDoctor-specific options like the web and Word logos, colors for message types, etc.
End of Table 3-1	

Configuring NetDoctor

You can customize NetDoctor to report on the type of information in which you are interested. This includes choosing individual rules or suites of related rules, selecting the language, look, and file type of the report and configuring notification for particular results. The following list is a brief overview of the configuration options:

- Rules:
 - Report on any combination of rules.
 - Specify rule parameters.
- Report Content—Specify the types of messages that are reported, prevent certain messages from being reported, add a diagram of the network to the report, and add appendices to the report.
- Report Format—Generate the report as a web document, Microsoft Word (.rtf) document, XML document, or in a custom format.
- Report Language—Generate the report in English or another language. Language option only applies to web reports; all other report formats are available in English only.
- Notification—Configure NetDoctor to notify you of specified events via Email or pager (requires the optional Automation Module).

Figure 3-2 Configure/Run NetDoctor Dialog Box: Rules Tab



Additional configuration parameters appear on the **Settings** tab.

(A **Notification** tab also appears if you have the optional Automation module enabled.)

Rules pane. All available rules are grouped by suite and listed here.


Parameters table. If a rule has configurable parameters, they appear here. Change the value of a parameter by clicking in the Value column.

Description pane. This section contains a description of the selected rule.

When you configure NetDoctor, you can save the configuration settings as a template. Several example templates are included with NetDoctor. You can use these templates as configured or as a starting point when creating your own templates. You can also run NetDoctor without saving the report configuration as a template.

- To run NetDoctor using the default template and minimal configuration, use Procedure 3-1.
- You can let NetDoctor intelligently select rules and generate a template for you (see Procedure 3-2 on page ND-3-7).
- You can save sets of NetDoctor configuration settings in templates:
 - save configuration settings as a template (see Procedure 3-3 on page ND-3-8)
 - run NetDoctor using a saved template (see Procedure 3-4 on page ND-3-12)

Procedure 3-1 Running NetDoctor (Basic Configuration)

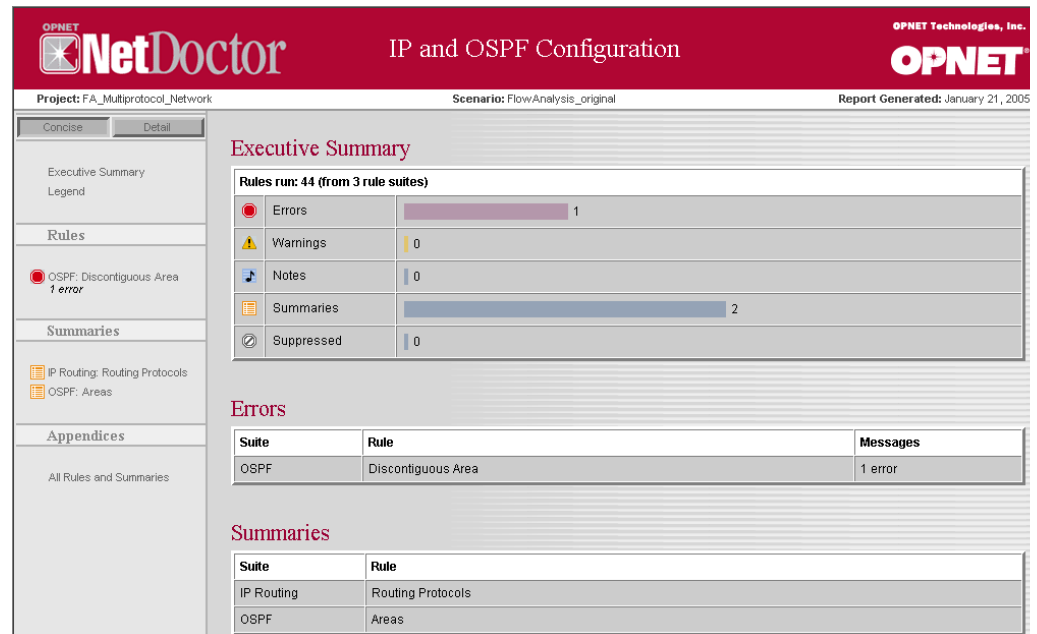
- 1 Open the project and scenario that you want NetDoctor to analyze.
- 2 Open the Configure/Run NetDoctor dialog box. Use one of the following methods:
 - From the NetDoctor menu, choose **Configure/Run NetDoctor**.
 - On the toolbar, click the Configure/Run NetDoctor button. 

➔ The Configure/Run NetDoctor dialog box opens.
- 3 If it's not already selected, select the Default NetDoctor Report in the Template pop-up menu.
- 4 In the Report title text box, enter a name for the report. This name appears in the final report and does not need to correspond to the name of the template.
- 5 Select the suites or individual rules you want to include in the analysis.

Note—You can select (or deselect) an entire rule suite by clicking on the name of the suite.
- 6 Click Run.

➔ NetDoctor analyzes the network and generates a report.

Figure 3-3 NetDoctor Web Report: Sample Output

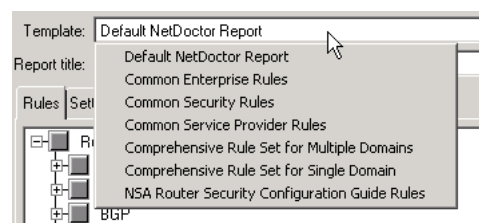


End of Procedure 3-1

Creating Report Templates

NetDoctor templates let you reuse NetDoctor configuration settings. This reduces the amount of time needed to configure NetDoctor for subsequent reports and ensures that your reports are consistent across multiple sessions and multiple projects. NetDoctor includes several templates, as shown in Figure 3-4.

Figure 3-4 Available Templates



You can experiment with the example templates and use them as a basis for your own templates. There are two ways to create report templates. You can

- let NetDoctor automatically generate a template
- manually select the individual rules and suites that make up the template you are creating

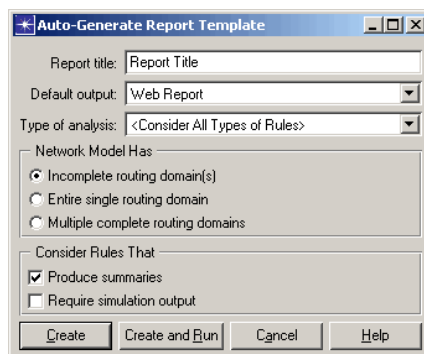
Auto-Generate a Report Template

The Auto-Generate Report Template feature creates new templates based on the current network model and on the type of analysis that you would like to do. The template that is created will include only the rules that meet the criteria you specify and apply to the current scenario. Procedure 3-2 describes how to use the Auto-Generate Report Template feature to create a report template.

Procedure 3-2 Auto-Generating a Report Template

- 1 From the NetDoctor menu, choose Auto-Generate Report Template.
 - ➔ The Auto-Generate Report Template dialog box opens. You can also access this box by clicking the Auto-Generate button in the Configure/Run NetDoctor dialog box.

Figure 3-5 Auto-Generate Report Template Dialog Box



- 2 In the Report title field, specify the title that NetDoctor should use for all reports generated from this template. This name appears on the final report and can be different from the name of the template.
- 3 In the Default output field, specify the default format (web, MS Word, or XML) of the generated report.

Note—Although a default is saved with the template, you can create reports in alternate formats when you run the template.
- 4 Select the type of analysis. Each rule in the library is associated with one or more types of analysis.
- 5 Specify if the scenario includes all devices in the network being modeled. This will minimize false messages produced by rules designed for use in a network with multiple routing domains, for example, in scenarios that include only a single complete routing domain.
- 6 Specify if NetDoctor should consider rules that will produce summary reports (e.g., management reports with summary information).
- 7 Specify if NetDoctor should consider rules that require simulation output from Flow Analysis or discrete event simulation.


- 8 Click **Create** or **Create and Run**.
 - ➔ The **Save As** dialog box opens for you to specify the name of the template and where it should be stored.
- 9 In the **Save As** dialog box, provide a name for the new template.
 - 9.1 In the **Model** directories pane, select the directory in which you want to store the new template.
 - 9.2 In the **File name** field, enter a name for the new template.
 - 9.3 Click **Save**.
 - ➔ The template is created in the location you specified. If you selected **Create** in step 8, the **Configure/Run NetDoctor** dialog box displays the new template. If you selected **Create and Run** in step 8, NetDoctor immediately generates a report based on the new template.

End of Procedure 3-2

Manually Create a Report Template

Procedure 3-3 describes how to manually create a report template using parameters that you specify.

Procedure 3-3 Creating a Report Template Manually

- 1 Open the **Configure/Run NetDoctor** dialog box using one of the following methods:
 - From the NetDoctor menu, choose **Configure/Run NetDoctor**
 - From the toolbar, click the **Configure/Run NetDoctor** icon. 
 - ➔ The **Configure/Run NetDoctor** dialog box opens.
- 2 From the **Template** list, choose a template to use as a starting point for this template. Select a template that is similar to the one you want to create; this will reduce the number of changes you must make.
- 3 Save the template with a new name.
 - 3.1 Click **Save As**.
 - ➔ The **Save As** dialog box displays.
 - 3.2 In the **Model** directories pane, select the directory in which you want to store the new template.
 - 3.3 In the **File name** field, enter a name for the new template.
 - 3.4 Click **Save**.
 - ➔ The template is saved and the **Configure/Run NetDoctor** dialog box reopens.

- 4 In the Report title field, specify the title that NetDoctor should use for all reports generated from this template. This name appears on the final report and can be different from the name of the template.
- 5 Click on the Rules tab and configure the rules used in this template.
 - 5.1 Select the suites or individual rules you want to include in the template. You can select any combination of rules and rule suites.
 - To select all of the rules in a suite, select the checkbox next to the rule suite.
 - To select specific rules in a suite, expand a suite by clicking the + sign (Windows) or > sign (Solaris) and choose the rules you want to include.

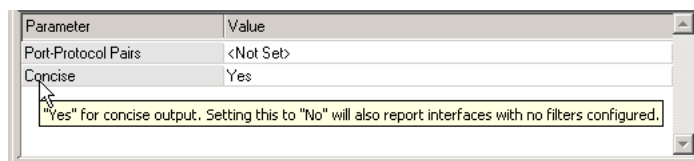
Note—When you select a rule or rule suite, its rule description appears in the Description pane.

- 5.2 Set the rule parameters, if needed.

Some rules have configurable parameters that govern how the rule works. When you select one of these rules, its parameters are displayed in the Parameters table. The values you set are stored in the report template and used when NetDoctor is run using this template.

Note—For a description of a parameter, display its tooltip by positioning the pointer anywhere in that row of the table.

Figure 3-6 Parameter Description Tooltip



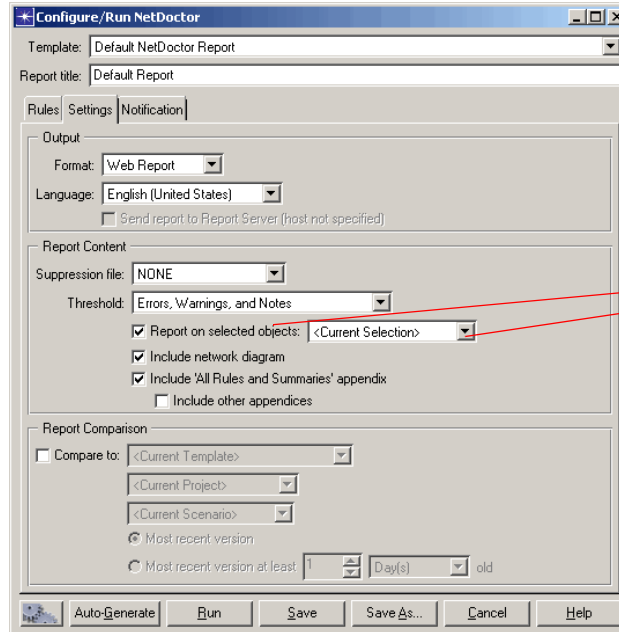
- 6 Click on the Settings tab to configure the format and content of the report. See Table 3-2 Configure/Run NetDoctor Dialog Box: Settings on page ND-3-10 for a description of the available options.
- 7 Click on the Notification tab to enable notifications and to configure their content and format. See Table 3-3 Email Notification Parameters on page ND-3-14 for a description of the available options. (Skip this step if you do not have the optional Automation module.)
- 8 Click **Save**.
 - ➔ The template is saved. You can click **Close** to close the dialog box or you can click **Run** to generate a report using this template.

End of Procedure 3-3

Settings Tab

Some NetDoctor parameters must be configured from the Settings tab of Configure/Run NetDoctor. More information on each parameter is shown in Table 3-2

Figure 3-7 Configure/Run NetDoctor Dialog Box: Settings Tab



You can report on currently selected objects or object selections saved previously in an object selection set.

The following table describes the parameters available on the Settings tab shown in Figure 3-7.

Table 3-2 Configure/Run NetDoctor Dialog Box: Settings (Part 1 of 2)

Item	Description
Format	Specifies the default format of the generated report. Although a default is saved with the template, you can create reports in alternate formats when you run the template. Procedure 3-4 Running NetDoctor from a Template on page ND-3-12 describes how to do this.
Language	Specifies the language in which this report should be generated. Additional language options require customization, as described in the Customizing NetDoctor chapter, NetDoctor Reports on page ND-4-27.
Send report to report server	Sends a copy of the report to the specified Report Server (requires the optional Report Server module).
Suppression File	Specifies a suppression file to use when generating reports with this template. See Suppressing Messages on page ND-3-24 for more details on message suppression.

Table 3-2 Configure/Run NetDoctor Dialog Box: Settings (Part 2 of 2)

Item	Description
Threshold	Specifies the type of messages included in the reports generated with this template. See Types of NetDoctor Messages on page ND-1-4 for a description the available message types.
Report on selected objects	When this box is selected, the NetDoctor report focuses on the objects that were selected in the project workspace when NetDoctor was run (default). You may also save a selection as an object selection set and call up the set later, using the drop-down box. NetDoctor might consider other objects when analyzing the network but will focus on the selected objects in the report. See Save Object Selection Set on page ITU-4-33 of the <i>Guru User Guide</i> for instructions on creating an object selection set.
Include network diagram	Adds an image of the network to the report.
Include 'All Rules and Summaries' appendix	Lists the rules included in the NetDoctor run and a summary of their results as an appendix in the generated report.
Include other appendices	Adds the following lists as appendices to the generated report: All Errors, All Warnings, All Notes, and All Summaries
Compare to	Specifies if this report should be compared to a previously generated report. Use the template, project, and scenario drop-down lists to specify the report that you want to compare to the current report. Use the Most Recent Version radio buttons to specify if you want the latest report or an older report. See Comparing NetDoctor Reports on page ND-3-22.
End of Table 3-2	

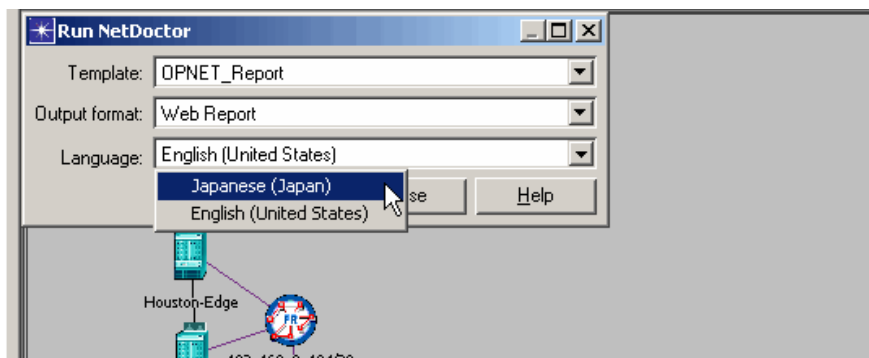
Generating a Report From a Template

After you have configured a template, you can use the template to generate a NetDoctor report for any network topology. You may find this useful for running the same rules and parameters against a variety of network topologies. You can use one of the following methods to generate a report based on a saved template:

- Click Run in the Configure/Run NetDoctor dialog box after selecting, configuring and saving a template. Procedure 3-3 on page ND-3-8 describes how to configure and save a template.
- Use the **Run NetDoctor** menu option to run NetDoctor using an existing template. Procedure 3-4 describes this approach.

Procedure 3-4 Running NetDoctor from a Template

- 1 From the NetDoctor menu, choose **Run NetDoctor**.
➔ The Run NetDoctor dialog box appears.

Figure 3-8 Run NetDoctor Dialog Box

- 2 From the Template list, choose the template you want to use for this analysis.
- 3 From the Output format list, specify the type of report you want NetDoctor to create: Web Report, MS Word Report (.rtf), or XML.
- 4 From the Language drop-down list, choose the language in which you want the report generated.
- 5 Click **Run**.
➔ NetDoctor analyzes the network and generates the report in the specified format.

End of Procedure 3-4

|

Configuring Notifications

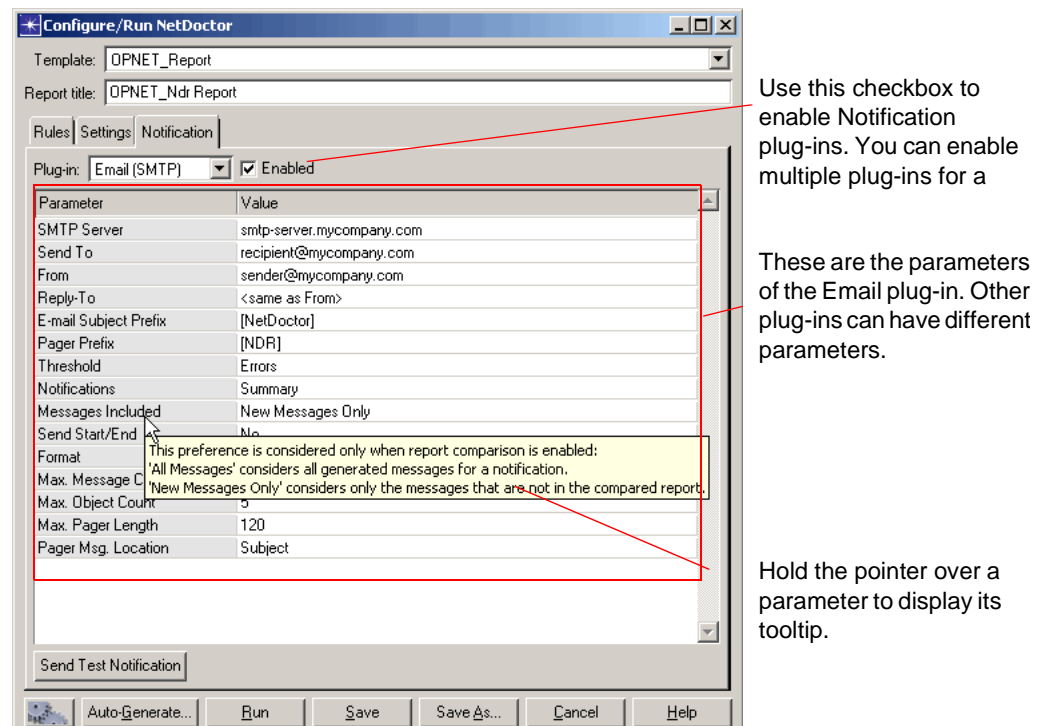
You can configure NetDoctor to send notifications (e.g. via Email) while it is generating a report. The notifications can be customized to include specific information. For example, you might want to know whenever NetDoctor detects an error, or you might only want to know when the NetDoctor run starts and ends. You might want NetDoctor to give you only a summary report on the errors and warnings it detected.

Note—You need the optional Automation module to use the Notification feature.

This section describes the default Email (SMTP) plug-in that ships with NetDoctor. If you want additional types of notifications, you can create additional plug-ins that can send different notifications in alternate formats. For example, you might want to create plug-ins that send notifications as an SNMP trap, via a direct connection to a database, or as an HTML-formatted email. See NetDoctor Reports on page ND-4-27 for more information.

Notifications are configured on the Notification tab of the Configure/Run NetDoctor dialog box. Figure 3-9 shows the parameters available for the Email (SMTP) notification plug-in.

Figure 3-9 Notifications in the Configure/Run NetDoctor Dialog Box



Use this checkbox to enable Notification plug-ins. You can enable multiple plug-ins for a

These are the parameters of the Email plug-in. Other plug-ins can have different parameters.

Hold the pointer over a parameter to display its tooltip.

Table 3-3 describes the parameters of the Email (SMTP) notification plug-in.

Table 3-3 Email Notification Parameters (Part 1 of 2)

Preference	Description
SMTP Server	DNS name or IP address of the email server to use when sending messages.
Send To	A comma separated list of the recipient email addresses.
From	Address that NetDoctor specifies in the From header of its notifications.
Reply-To	Address that NetDoctor specifies in the Reply-To header of its notifications. If this is set to “<same as From>”, then the Reply-To header will not be included.
Email Subject Prefix	The first characters that should appear in the subject field of all notifications when the Format parameter is set to Email.
Pager Prefix	The first characters that should appear in the subject field of all notifications when the Format parameter is set to Pager. Since the message length for pager notifications is often limited, a shorter prefix is usually preferred.
Threshold	The types of messages that are included in the notifications. See Types of NetDoctor Messages on page ND-1-4 for a description the available message types.
Send Start/End	Specifies if NetDoctor should send notifications when a run starts and when a run ends. These are short messages that are sent in addition to other notifications.
Notifications	Specifies the types of notifications sent. NetDoctor can send a notification for each rule (per the Threshold), or it can send a summary notification that covers all of the rules in the run (per the Threshold), or it can do both.
Format	Specifies if notifications should be formatted for viewing in an email client or on a pager. Because pagers, and devices such as text-enabled wireless phones, often limit the number of characters per message, NetDoctor can format its notifications to suit those devices.
Max. Message Count	Limits the number of messages in a rule notification. A message is generated in the notification for each error, warning, and note generated by a rule, subject to the specified threshold. See Figure 3-10 on page ND-3-15 for an example of how this attribute works.

Table 3-3 Email Notification Parameters (Part 2 of 2)

Preference	Description
Max. Object Count	The maximum number of objects associated with a report entry that are included in a message.
Max. Pager Length	Maximum number of characters to include in pager notifications.
Pager Msg. Location	Location of the content of pager notifications: subject-line or body.
End of Table 3-3	

Figure 3-10 shows two notifications from a NetDoctor run and the configuration parameters that were used. The configuration actually generated many messages, but only two are shown.

Figure 3-10 NetDoctor Notifications

Plug-in: Email (SMTP) <input checked="" type="checkbox"/> Enabled	
Parameter	Value
SMTP Server	smtp-server.mycompany.com
Send To	recipient@mycompany.com
From	sender@mycompany.com
Reply-To	<same as From>
E-mail Subject Prefix	[NetDoctor] ①
Pager Prefix	[NDR] ②
Threshold	Errors ③
Notifications	Summary
Messages Included	New Messages Only
Send Start/End	No
Format	E-mail
Max. Message Count	5 ④
Max. Object Count	5
Max. Pager Length	120
Pager Msg. Location	Subject

③ Summary Notification

```

Date: Tue, 25 Nov 2003 00:46:50 -0500 (EST)
To: recipient@mycompany.com
From: sender@mycompany.com
Reply-To: sender@mycompany.com
Subject: [NetDoctor] Summary Report: Default NetDoctor Report

Template: Default NetDoctor Report
Report Title: Comprehensive Report
Project-Scenario: FA_Multiprotocol_Network-FlowAnalysis_original
Summary: 239 rules run, 7 rules tripped (1 error, 67 warnings)
Rules with at least one error or warning: 7
-----
* OSPF: Discontiguous Area (1 error)
* Administration: Verify Router OS Version (35 warnings)
* BGP: IBGP Neighbor Not Loopback Address (20 warnings)
* RIP: Nonoptimal Holddown Timer Values (8 warnings)
* OSPF: Inconsistent Metric (2 warnings)
* OSPF (Advanced): Inconsistent Reference Bandwidth (1 warning)
* OSPF: Inconsistent Reference Bandwidth (1 warning)
                
```

③ A Rule Notification

```

Date: Tue, 25 Nov 2003 00:46:45 -0500 (EST)
To: recipient@mycompany.com
From: sender@mycompany.com
Reply-To: sender@mycompany.com
Subject: [NetDoctor] RIP: Nonoptimal Holddown Timer Values (WARNING)

Template: Default NetDoctor Report
Report Title: Comprehensive Report
Project-Scenario: FA_Multiprotocol_Network-FlowAnalysis_original
Messages: 8 warnings
First Two Messages:
-----
WARNING
- Tested: Holddown timer on router: CR10
- Object: Timers on router: CR10
The holddown timer is 130 seconds while the invalid timer is 180 seconds.
-----
WARNING
- Tested: Holddown timer on router: CR11
- Object: Timers on router: CR11
The holddown timer is 130 seconds while the invalid timer is 180 seconds.
                
```

There are 8 messages, but since the Max. Message Count is 2, only the first two appear in the notification.

Viewing NetDoctor Reports

After a NetDoctor run, the generated report is displayed. NetDoctor keeps a configurable number of previous reports generated for each template in case you want to view any one of them later. Use the preference `netdoctor.keep_prior_reports_count` to set the number of previous reports you would like to retain. You can view a previous report generated for a template in the original output format or in a new output format. Follow Procedure 3-5 to view a NetDoctor report.

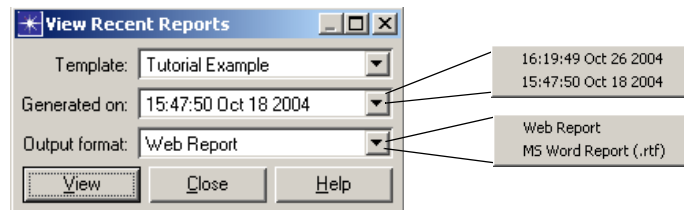
Note—You can change the format in which to view a report without re-running NetDoctor (see Procedure 3-5).

Procedure 3-5 Viewing a Previous Report

- 1 From the NetDoctor menu, choose **View Recent NetDoctor Reports**.

➔ The View Recent Reports dialog box opens.

Figure 3-11 View Recent NetDoctor Reports Dialog Box



- 2 In the Template list, select the template for which you want to view previous reports.
- 3 In the Generated on list, choose the date/time on which the report of interest was run.
- 4 In the Output format list, choose **Web Report or MS Word Report (.rtf)**.
- 5 Click **View**.

➔ The specified report appears in the output format you selected.

End of Procedure 3-5

Report Formats

NetDoctor generates reports in the following formats:

- Web reports (HTML)

- MS Word (.rtf)
- XML

You can also configure NetDoctor to generate reports in alternate formats. This is described in Customizing NetDoctor on page ND-4-1.

This section describes the Web and MS Word reports formats. NetDoctor uses the XML report to generate the other report formats. Since report formats are based on the same information, they include the same content and share a similar structure. The web report is more interactive and is easier to navigate, whereas the MS Word report is easier to edit and is more suitable for printing.

Table 3-4 NetDoctor Report Organization

Report Element	Location	
	Web Report	MS Word Report
Report title, project name, scenario name, and the date the report was generated	Top banner	Cover page
Concise/Detail buttons allowing you to control the verbosity of the display	Navigation frame	
A list of the report contents (list items are links in both reports)	Navigation frame	Table of contents
The messages reported organized by rule	Content frame ¹	Rule sections
Additional data	Appendices ² (a list of available appendices is at the bottom of the navigation frame, the appendices appear in the content frame)	Appendices
End of Table 3-4		

1. Content varies as you navigate through the report.

2. Appendices are listed in the Navigation frame. The contents of an appendix appear in the Content frame.

Web Report

Figure 3-12 shows a NetDoctor report in the web report format. Each web page consists of the top banner, the navigation frame, and the content frame.

Figure 3-12 NetDoctor Web Report

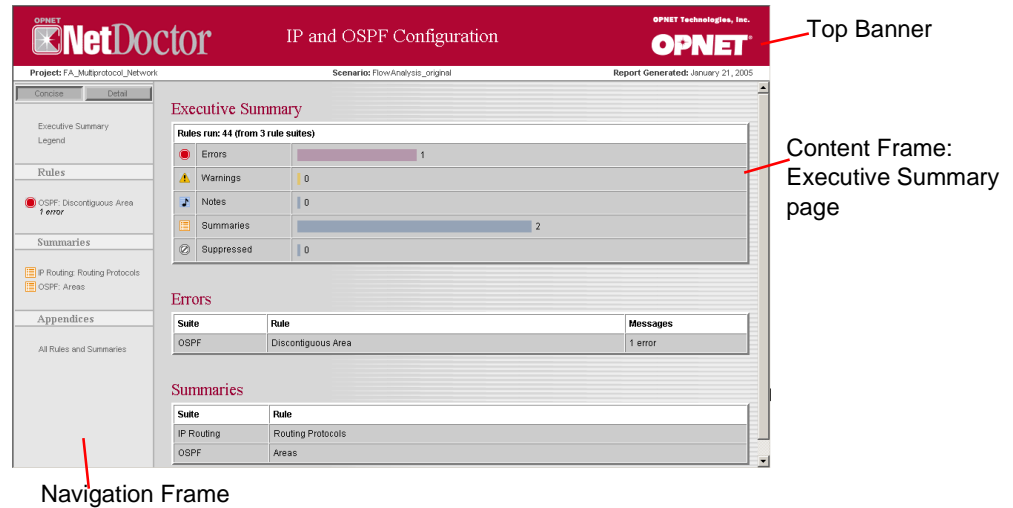
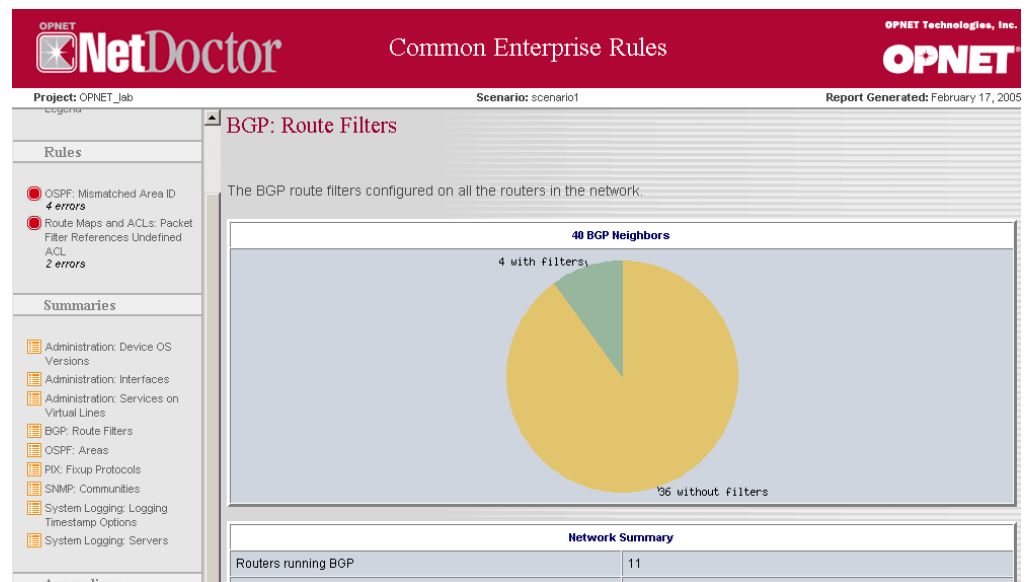


Figure 3-13 shows a NetDoctor web report that includes charts. Bar and pie charts have been added to some summary reports as of release 11.0 and offer another view of the information gathered by NetDoctor. Custom rules can also include charts, as described in the Customizing NetDoctor chapter, Understanding Charts on page ND-4-45.

Figure 3-13 NetDoctor Web Report



Concise and Detail buttons appear in both the navigation frame and the content frame of the NetDoctor web report. If you specify Concise or Detail in the navigation frame, it changes the view of each rule you select in the list. If you select Concise or Detail in the content frame, it changes the view for that rule.

The buttons operate as follows:

- Concise—used to display a concise version of the rule page, as shown in Figure 3-14.
- Detail—used to display a detailed version of the rule page, as shown in Figure 3-14.

Figure 3-14 Rule Output - Concise

The screenshot displays the NetDoctor web interface for an IP and OSPF Configuration report. The header includes the NetDoctor logo, the title 'IP and OSPF Configuration', and the OPNET logo. The report details are as follows:

- Project: dep_ospf_analysis
- Scenario: reconfiguration4
- Report Generated: January 21, 2005

The main content area shows the 'OSPF: Inconsistent Metric' rule. It includes a description: 'Connected interfaces should have a consistent OSPF cost metric. Inconsistent cost metrics may cause asymmetric routing.' Below this, a yellow box highlights the detected warnings:

Detected: 2 warnings

- Atlanta-Access [Serial1/0], Dallas-Edge [Serial1/0] and Houston-Edge [Serial0/1]
- LA-Edge [Serial0], SanDiego-Edge [Serial0/0] and SF-Access [Serial0/0]

The left navigation pane shows a list of rules with their respective warning and note counts:

- IP Addressing: Overlapping Subnets: 1 warning
- IP Routing: Inconsistent Metric Components: 2 warnings
- OSPF: Inconsistent Metric: 2 warnings
- OSPF: Network Statement References Invalid Interface: 1 warning
- OSPF: Redundant Network Statement: 2 warnings
- OSPF: Potential Stub Area: 2 notes
- OSPF: Reference Bandwidth Too Low: 13 notes

Figure 3-15 Rule Output - Detail

The screenshot displays the NetDoctor interface for an IP and OSPF Configuration report. The top header includes the NetDoctor logo, the title "IP and OSPF Configuration", and the OPNET Technologies, Inc. logo. Below the header, the report details are shown: Project: dep_OSPF_Analysis, Scenario: reconfiguration4, and Report Generated: January 21, 2005. The main content area is titled "OSPF: Inconsistent Metric" and contains two warning messages. The first warning, titled "Tested: OSPF cost of interfaces in subnet: 192.168.0.104/29", states that there is an inconsistency in the OSPF cost metric among the interfaces in area 0.0.0.4. It lists the following interfaces and their costs: Dallas-Edge[Serial1/0] (auto calculated) with a cost of 64, Houston-Edge[Serial0/1] (auto calculated) with a cost of 25, and Atlanta-Access[Serial1/0] (auto calculated) with a cost of 25. The second warning, titled "Tested: OSPF cost of interfaces in subnet: 192.168.0.88/29", states that there is an inconsistency in the OSPF cost metric among the interfaces in area 0.0.0.3. It lists the following interfaces and their costs: LA-Edge[Serial0] (auto calculated) with a cost of 64, SanDiego-Edge[Serial0/0] (auto calculated) with a cost of 25, and SF-Access[Serial0/0] (auto calculated) with a cost of 25. Both warnings include a note that some or all of the interfaces have their interface cost set to auto-calculate, which may lead to inconsistencies if the reference bandwidth is changed on some of the routers. A left-hand navigation pane shows a list of rules, with "OSPF: Inconsistent Metric" selected. The bottom of the screen shows a "Summaries" section with a link to "IP Routing: Routing Protocols".

Comparing NetDoctor Reports

You can compare the results of a NetDoctor run with the results generated in previous runs. This is useful for identifying changes that have occurred in the network since the last time you ran NetDoctor.

Note—The report comparison feature in NetDoctor does not require the Report Server. No additional license is needed to use report comparison.

Configuring Report Comparison

The Report Comparison configuration options appear on the Settings tab of the Configure/Run NetDoctor dialog box.

Figure 3-17 Report Comparison Options

Select this checkbox to enable the Report Comparison feature.

Use the pull-down lists to compare this report to a previous report for this template, project, and scenario, or any other template, project, or scenario.

Analyzing a Comparison Report

When you enable Report Comparison, the report generated by NetDoctor highlights changes between the current report and the specified report. Throughout the report, NetDoctor highlights any differences between the two reports in the Differences section of the report. Figure 3-18 shows the web version of a comparison report.

Figure 3-18 A Web Comparison Report

The links in the Differences section let you view all of the changes in one place.

+ signs on the icons indicate that there are new messages

Messages No Longer Detected indicates if there were messages in the earlier report that were not found in this report.

New messages are highlighted in the Executive Summary and throughout the report.

Suite	Rule	Messages
IP Routing	Inconsistent Metric Components	2 warnings
OSPF	Inconsistent Metric	2 warnings
OSPF	Network Statement References Invalid Interface	1 warning
OSPF	Redundant Network Statement	2 warnings

Suppressing Messages

You can suppress messages for specific issues on specific elements in a network without restricting NetDoctor from checking other elements in the network for the same issue. For example, you can suppress messages from the rule “Too Many SNMP Servers” for a single router, and NetDoctor will continue to report warnings for the same rule on other routers in the network. NetDoctor does this by applying a specified suppression file during a run.

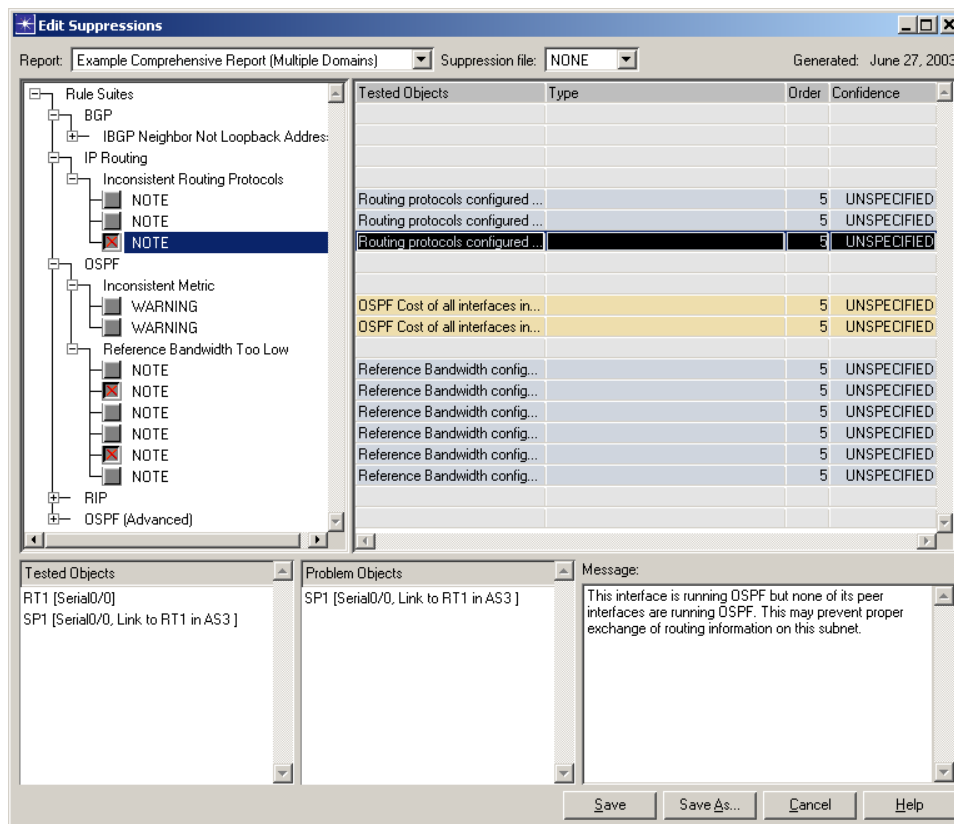
You can use message suppression when you want NetDoctor to check a network against a rule for all objects in the network except a selected few. If you do not want NetDoctor to report on a rule for any of the objects in the network, do not use message suppression. Instead, omit the rule.

You cannot proactively suppress a message. You can only suppress messages after they have been generated in a NetDoctor run. When you enable message suppression, NetDoctor suppresses the exact message for the exact object and rule specified in the suppression file. If you have configured NetDoctor to suppress a particular warning from a rule for an object, NetDoctor will still notify you if it detects an error for that rule.

Procedure 3-6 Creating a Suppression File

- 1 Run NetDoctor to identify the messages that you want to suppress in subsequent NetDoctor reports.
- 2 From the NetDoctor menu, choose **Suppress Messages**.
 - ➔ The Edit Suppressions dialog box appears.

Figure 3-19 Edit Suppressions Dialog Box



- 3 From the Report list, select the template that contains the messages you want to suppress.

Note—You can only suppress messages that have been generated in a report.

- 4 If you want to edit an existing suppression file for this template, select it from the Suppression file pull-down menu. Otherwise, skip this step.
- 5 Find the messages you identified in step 1 and select them in the Rule Suites treeview.

When you select a message, additional information about the rule appears in the lower panes of the dialog box. You can use this information to help you confirm that you have selected the correct message and device.

- 6 Save the suppression information in a suppression file.

When creating a new suppression file:

- 6.1 Click **Save As...**
- 6.2 Give the Suppression file a name and specify where NetDoctor should store it.
- 6.3 Click **Save**.
 - ➔ The new filename appears in the Suppression file list.

When editing an existing suppression file:

- 6.1 Click **Save**.

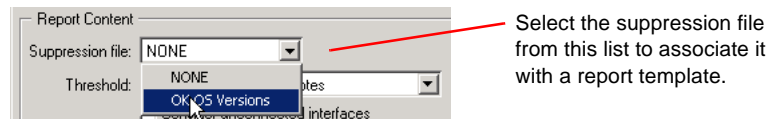
- 7 Click Cancel to close the Edit Suppressions dialog box.

End of Procedure 3-6

After you create a suppression file, you can apply it to a template so that NetDoctor will suppress the messages specified in the suppression file the next time it generates a report from that template.

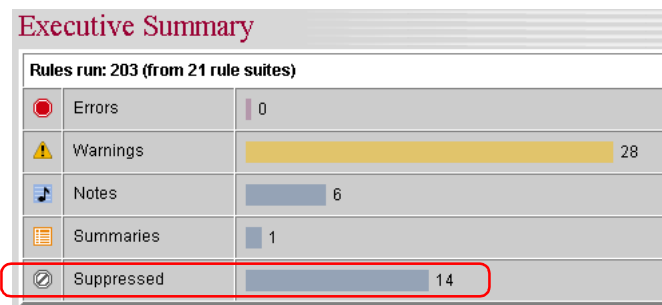
Procedure 3-7 Applying a Suppression File to a Template

- 1 Open the Configure/Run NetDoctor dialog box.
- 2 Select a template that will use the suppression file.
- 3 Click on the Settings tab.
- 4 Under Report Content, select a suppression file from the list.



- 5 Save the template.
 - The next time you run this template, the suppressed messages will not be included in the generated report. You can view the number of messages that were suppressed in the Executive Summary.

Figure 3-20 Suppressed Message Count



End of Procedure 3-7

Configuring Global Options

The NetDoctor Options dialog box lets you configure high-level aspects of NetDoctor operation and report generation. All of the settings in the Options dialog box are global and apply to all future runs of NetDoctor.

Figure 3-21 NetDoctor Options Dialog Box

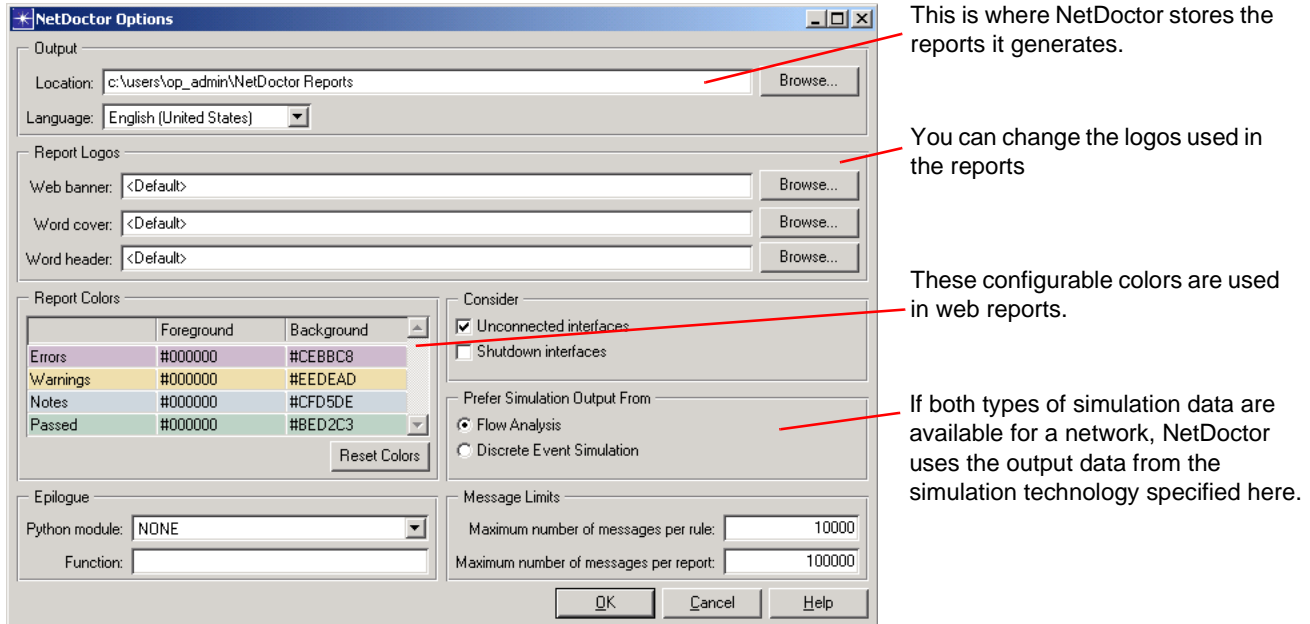


Table 3-5 NetDoctor Options (Part 1 of 2)

Option	Description
Output Location	Sets the location in the file system where NetDoctor reports are placed. Additional folders are created within this location for each project and report type. Created folders using the following naming scheme: <project-scenario\template_name-Web_Report> and <project-scenario\template_name-RTF_Report>
Output Language	This is the default language that NetDoctor uses when generating reports. The output language can be changed from this default when a template is created or edited, or when a report is generated.
Report Colors	Sets the foreground and background colors associated with Errors, Warnings, and Notes and Passed objects. Four user-specified parameters (Users 4-8) are also available. These configurable colors are used only in Web versions of reports.
Report Logos	Lets you to replace the standard NetDoctor and OPNET logos with your own logos. The Web banner logo supports JPEG, GIF, and PNG images. The Microsoft Word cover and Microsoft Word header logo support JPEG or PNG images.

Table 3-5 NetDoctor Options (Part 2 of 2)

Option	Description
Consider unconnected interfaces	Includes unconnected interfaces in the network analysis. By default (selected) NetDoctor looks at unconnected interfaces when it analyzes the network.
Consider shutdown interfaces	Includes shutdown interfaces in the network analysis. By default (not selected) NetDoctor does not look at shutdown interfaces when it analyzes the network.
Prefer Simulation Output From	Some NetDoctor rules need simulation output (from a flow analysis or discrete event simulation). If both types of simulation data are available for a network, NetDoctor uses the output data from the simulation technology specified in this preference.
Epilogue	The Epilogue setting lets rule developers to run additional code at the end of the NetDoctor run. For more information about this setting, see Epilogue Handler on page ND-4-25.
Message Limits	Message limits restrict the number of messages that NetDoctor includes in its report. You can limit the number of messages for each rule and for the entire report.
End of Table 3-5	

Modeling Network Security

In addition to its rules-based analyses that can check rules on security configuration, NetDoctor also has a Security Analysis feature that lets you create and analyze specific security scenarios in a network. For example, device in the network may have security policies configured that are designed to restrict access to all but authorized users. NetDoctor lets you create security demands that represent an unauthorized user trying to access that device. When you run a security analysis, NetDoctor checks these security demands against the access policies configured on the devices in the network. If the configured policies on the device and in the network prevent the unauthorized users that are represented by the security demand from accessing the restricted machine, NetDoctor passes the security demand.

There are two types of security demands:

- **Permit demands**—Represent authorized access, such as employees accessing their company's network from home. A permit demand will pass a security analysis if the demand can be routed. That is, if a user at the source can access the destination. If a user at the source cannot access the destination, the security demand fails.
- **Deny demands**—Represent unauthorized access, such as an intruder hacking into a secured server. A permit demand will pass a security analysis if the demand *cannot* be routed—that is, if a user at the source cannot access the destination. If a user at the source can access the destination, the security demand fails.

All of the security operations available in NetDoctor appear on the NetDoctor > Security submenu. These options let you create security demands, import and export the security demands in the network, run a security analysis, and view security analysis reports. Remember that the intent of a security analysis is to verify if the security policies configured in the network (using access control list, route filters, and so on) implement the access requirements and access restrictions you need. Because of this, the network topologies created using device configuration import and VNE Server import are excellent baselines for security analyses.

You can use the following workflow to analyze the security configuration in a network topology.

- 1) Add security demands to the network. See [Configuring Security Demands](#) on page ND-3-30.
- 2) Visualize the configured security demands. See [Visualizing Network Security Configuration](#) on page ND-3-34.
- 3) Run the NetDoctor Security Analysis to make sure that all security demands pass given the security configuration in the network.

The NetDoctor security analysis verifies if the security configuration meets the objectives modeled by the security demands. A security analysis might reveal that a valid security configuration is unduly restrictive because permit demands can not get through to their destination.

Configuring Security Demands

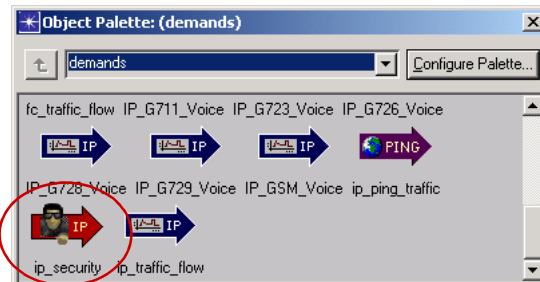
Validating security policies against actual network configuration involves creating security demands in the network and running simulations to verify the intended behavior of the demand. You can configure permit and deny security demands that represent end-to-end requirements to test the security configuration in a network. The NetDoctor Security Analysis feature generates web reports that contain the results of its security audit.

Security demands are created in the project editor using the same drag-and-drop procedure used to create links. NetDoctor also has a utility that lets you create multiple, identical security demands in one operation.

Procedure 3-8 Creating Security Demands

- 1 Open the “demands” object palette:

Figure 3-22 The Demands Object Palette

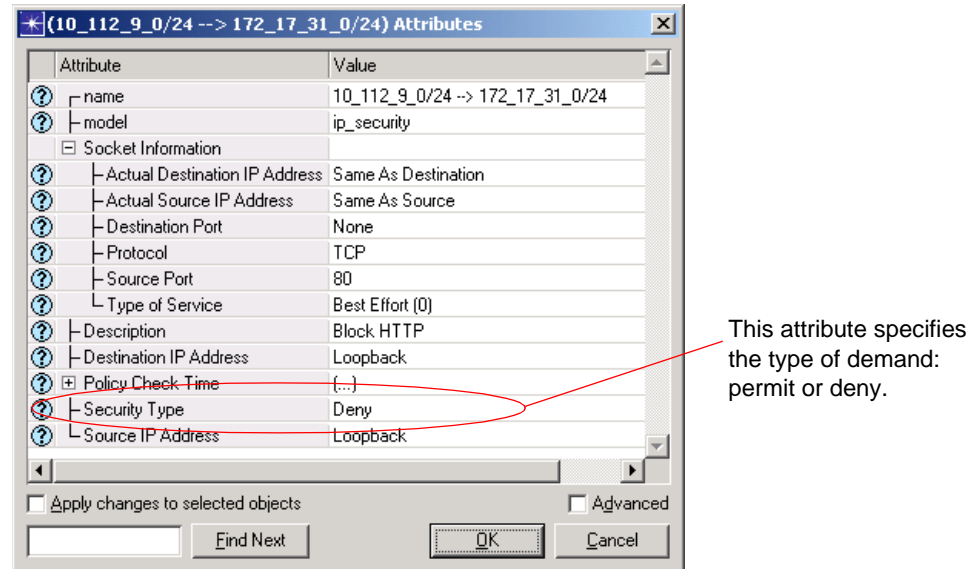


- 2 Click on the **ip_security** demand (see Figure 3-22) in the object palette.
- 3 In the Project Editor workspace, click on the source node of the security demand, then click on the destination node.
 - ➔ A new permit security demand appears in the workspace. Security demands are permit demands by default and are colored green in the workspace. You can edit the attributes of the demand to change it to a deny demand, which are red by default.
- 4 Repeat the previous step to create other security demands.
- 5 When you have finished creating demands, exit demand-definition mode (right-click and select **Abort Demand Definition**).

End of Procedure 3-8

After you create a security demand, you can configure it by editing its attributes. These attributes govern the intentions of the demand: whether the access is authorized or not, routing protocol and type of service used, when the demand is tested, and exact source and destination addresses. Figure 3-23 shows the configurable attributes on a security demand.

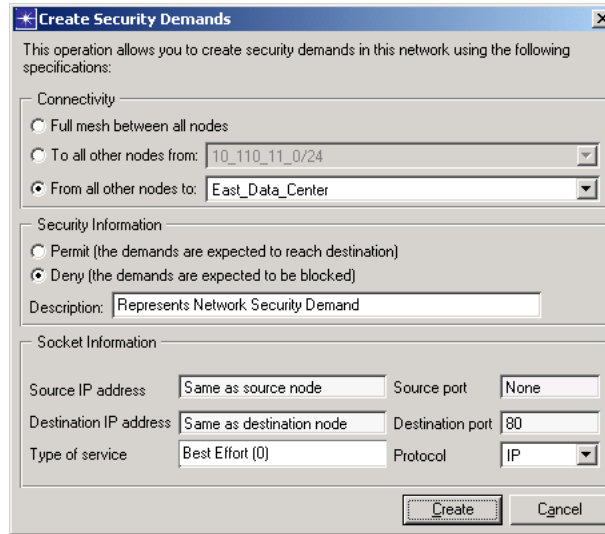
Figure 3-23 Security Demand Attributes



You can create and configure multiple, identically-configured security demands in one operation. The resulting demands can be a full-mesh between all routers, workstations, LANs, and server nodes in the network. Similarly, you can configure the demands from all routers, workstations, LANs, and server nodes in the network to a specified node or from a specified node in the network to all routers, workstations, LANs, and server nodes. This method of adding security demands to a network combines demand creation and configuration into a single step.

Procedure 3-9 Creating Multiple Security Demands Simultaneously

- 1 From the NetDoctor menu, select **Security > Demands > Create...**
 - ➔ The Create Security Demands dialog box displays.

Figure 3-24 Create Security Demands Dialog Box

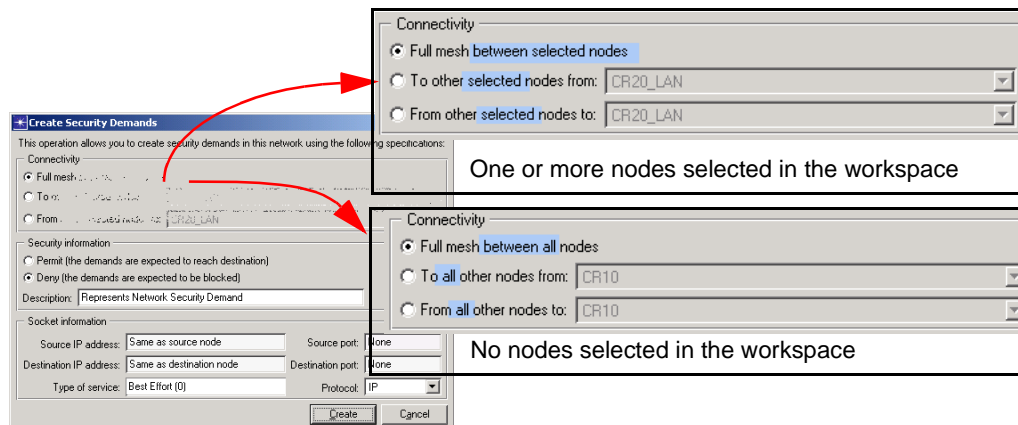
- 2 Under Connectivity, specify the nodes to use as demand endpoints:
 - Full-mesh creates two demands (one in each direction) between each pair of nodes in the network
 - To other nodes from... creates a demand between the specified node and every other node in the network, with this node as the source.
 - From other nodes to... creates a demand between the specified node and every other node in the network, with this node as the destination.
- 3 Under Security Information, specify the type of demand. If you also provide a description, it appears as a tooltip for the demands but does not affect analysis or simulation results.
- 4 Under Socket Information, specify the source and destination IP addresses, ports, as well as the type of service and protocol used. This information is used for policy routing.

End of Procedure 3-9

You can repeat Procedure 3-9 several times, if needed to achieve the desired configuration of security demands. The effects of each of each Create Security Demands operation is added to the existing security configuration.

The Create Security Demands dialog box differs slightly depending on whether or not nodes are currently selected in the project workspace. Figure 3-25 highlights these differences. The available Connectivity options reflect the current node selection in the workspace. You can narrow the scope used when creating multiple demands by selecting the nodes you want to work with before launching the Create Security Demands dialog box.

Figure 3-25 Create Security Demands Dialog Box—With and Without Selection



Reusing Security Demand Configuration Information

After you are satisfied with the security demand configuration in the network, you can preserve the configuration in an external text file that you can reuse in other projects.

- To export security demands to an external file, select NetDoctor > Security > Demands > Export To File and specify where you want to store the file.
- To import security demands from an external file, select NetDoctor > Security > Demands > Import From File and specify the location where you want to retrieve the file.

If you want to configure security demands outside of the user interface, you can export a simple security demand configuration and open the resulting file in any text editor. You can use this file as a template to add additional security demands.

Figure 3-26 shows part of a file used to configure security demands.

Figure 3-26 Security Demand Configuration File

```
# This file contains the security information configured
# in the network model. This file can be modified and can
# be used to import the security demands into the network models

# Fields are described in the order in which they appear.
# Fields should be delimited by comma separator as shown in sample entry.

# Fields Legend
# -----
#1) Security Demand Name
#2) Security Type
#3) Actual Source IP Address
#4) Actual Destination IP Address
#5) Source Port
#6) Destination Port
#7) Protocol
#8) Type of Service
#9) Description
#10) Policy Check Time(s)
#11) Source Node
#12) Source IP Address
#13) Destination Node
#14) Destination IP Address
#-----
CR26_LAN --> CR10,Permit,Same As Source,Same As Destination,-1,-1,IP,0,Access all,200.000000,Logical Network.CR26_LAN,Auto
Assigned,Logical Network.CR10,Auto Assigned

CR26_LAN --> CR11,Permit,Same As Source,Same As Destination,-1,-1,IP,0,Access all,200.000000,Logical Network.CR26_LAN,Auto
Assigned,Logical Network.CR11,Auto Assigned

CR26_LAN --> CR12,Permit,Same As Source,Same As Destination,-1,-1,IP,0,Access all,200.000000,Logical Network.CR26_LAN,Auto
Assigned,Logical Network.CR12,Auto Assigned
```

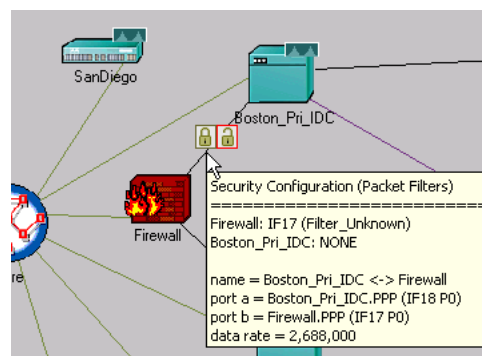
Visualizing Network Security Configuration

In a routed network, data-plane network security is usually implemented using packet filters and route maps. A visualization feature lets you see—in the project workspace—which interfaces are configured to use packet filters.

Procedure 3-10 Viewing Security Configuration in the Workspace

- 1 From the View menu, choose **Visualize Protocol Configuration > IP Security Configuration**.
 - ➔ The links on the network topology are annotated with special icons that indicate the packet filter configuration at both ends of the link.

Figure 3-27 Network Security Configuration Visualization



In this example, the locked padlock indicates that a filter is configured on the Firewall and that no filter is configured on Boston_Pri_IDC. The tooltip indicated that the filter configured on the firewall is named Filter_Unknown.

End of Procedure 3-10

Using Security Demands in Simulations Studies

After configuring security demands in a network topology, you can run simulations on the network using flow analysis or discrete event simulation. For discrete event simulations, you can use the Policy Check Time attribute on the security demands to specify when the security demands should be checked in the simulation. For example you might want to check the policies before, during, and after a failure event.

Generating Security Reports

There are two types of reports available to describe security configuration and behavior in the network:

- Configuration summary report
- Security demand conformance and violation check report

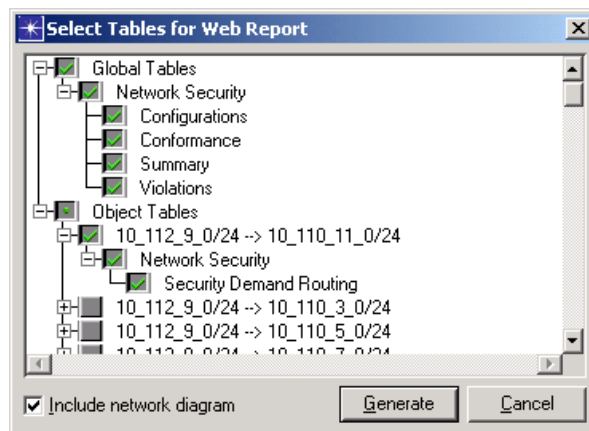
Both reports are available in a unified web report that can be launched from the NetDoctor > Security > Reports menu.

Procedure 3-11 Viewing Security Reports

- 1 Using the NetDoctor menu, choose **Security > Reports > Generate Web Report...**

➔ The Select Tables for Web Report dialog box comes up.

Figure 3-28 Selecting Tables for Security Web-Report



- 2 Select reports of interest under the “Global Tables” and “Object Tables” groups.
- 3 Click **Include Network Diagram** to include a picture of the network topology in the web report.
- 4 Click **Generate**.
- 5 Specify where you want to store the web report.
 - ➔ The web report opens in the default browser

Figure 3-29 Network Security Web Report



- 6 View the Executive Summary to see the number of policy checks and the list of conformances and violations.
 - ➔ The individual conformance and violation reports show how the various security demands conformed or violated the security intention.
- 7 Browse through the reason for success or failure of security checks using the **Status** link available for each security demand report.

End of Procedure 3-11

The Executive Summary lists the number of policy checks and reports on conformance and violations. The individual conformance and violation reports show how the various security demands conformed or violated the security intention. Use the Status link in each security demand report to see why a security check succeeded or failed.

Index

A

A Web Comparison Report, [ND-3-23](#)
Analyzing a Comparison Report, [ND-3-23](#)
Applying a Suppression File to a Template, [ND-3-26](#)
Auto-Generate a Report Template, [ND-3-7](#)
Auto-Generate Report Template Dialog Box, [ND-3-7](#)
Auto-Generating a Report Template, [ND-3-7](#)
available rule suites, [ND-1-4](#)
Available Templates, [ND-3-6](#)

C

Comparing NetDoctor Reports, [ND-3-22](#)
Configure/Run NetDoctor Dialog Box
 Rules Tab, [ND-3-4](#)
 Settings (Part 1 of 2), [ND-3-10](#)
 Settings Tab, [ND-3-10](#)
Configure/Run NetDoctor dialog box, [ND-3-4](#), [ND-3-10](#)
Configuring Global Options, [ND-3-27](#)
Configuring NetDoctor, [ND-3-4](#)
Configuring Notifications, [ND-3-13](#)
Configuring Report Comparison, [ND-3-22](#)
Configuring Security Demands, [ND-3-30](#)
Create Security Demands Dialog Box, [ND-3-32](#)
Create Security Demands dialog box, [ND-3-32](#)
Create Security Demands Dialog Box—With and Without Selection, [ND-3-33](#)
Creating a Report Template Manually, [ND-3-8](#)
Creating a Suppression File, [ND-3-24](#)
Creating Multiple Security Demands Simultaneously, [ND-3-31](#)
Creating Report Templates, [ND-3-6](#)
Creating Security Demands, [ND-3-30](#)

D

Device Configuration File Validation, [ND-3-12](#)

E

Edit Suppressions Dialog Box, [ND-3-25](#)
Edit Suppressions dialog box, [ND-3-25](#)
Email Notification Parameters (Part 1 of 2), [ND-3-14](#)

G

Generating a Report From a Template, [ND-3-11](#)
Generating Security Reports, [ND-3-36](#)

L

license
 activating in NetDoctor, [ND-2-1](#)
 adding in NetDoctor, [ND-2-1](#)

M

Manually Create a Report Template, [ND-3-8](#)
Match/No Match Commands, [ND-3-12](#)
messages
 suppressing, [ND-3-24](#)
 viewing the suppressed message count, [ND-3-26](#)
Microsoft Word Report, [ND-3-21](#)
Microsoft Word report, [ND-3-21](#)
Modeling Network Security, [ND-3-29](#)

N

NetDoctor
 adding and activating a license, [ND-2-1](#)
 configuring, [ND-3-4](#)
 creating a template, [ND-3-8](#)
 understanding NetDoctor operations, [ND-1-3](#)
 understanding the workflow, [ND-1-3](#)
 using, [ND-3-1](#)
NetDoctor administration, [ND-2-1](#)
NetDoctor license
 adding and activating, [ND-2-1](#)
NetDoctor Menu, [ND-3-2](#)
NetDoctor menu, [ND-3-2](#)
NetDoctor Menu Operations (Part 1 of 2), [ND-3-2](#)
NetDoctor Notifications, [ND-3-15](#)
NetDoctor options
 setting, [ND-3-27](#)
NetDoctor Options (Part 1 of 2), [ND-3-27](#)
NetDoctor Options Dialog Box, [ND-3-27](#)
NetDoctor quick start, [ND-3-5](#)
NetDoctor report
 running, [ND-3-11](#) to [ND-3-12](#)
 viewing recent, [ND-3-16](#)
NetDoctor Report in Microsoft Word, [ND-3-21](#)
NetDoctor report organization, [ND-3-17](#)
NetDoctor Report Organization , [ND-3-17](#)
NetDoctor Reports dialog box
 viewing recent, [ND-3-16](#)
NetDoctor tutorial, [ND-2-2](#)
 opening, [ND-2-2](#)
 using, [ND-2-2](#)
NetDoctor User Guide
 contents, [ND-1-6](#)
 organization, [ND-1-6](#)
NetDoctor Web Report, [ND-3-18](#)
 Sample Output, [ND-3-6](#)
NetDoctor administration, [ND-2-1](#)
network security
 generating the Web report, [ND-3-37](#)
 modeling, [ND-3-29](#)
 visualizing the network configuration, [ND-3-34](#)

Network Security Configuration Visualization, [ND-3-34](#)
Network Security Web Report, [ND-3-37](#)
Notifications in the Configure/Run NetDoctor Dialog Box,
[ND-3-13](#)

O

Options dialog box, [ND-3-27](#)
overview, [ND-1-1](#)

P

Parameter Description Tooltip, [ND-3-9](#)
parameter description tooltip, [ND-3-9](#)

R

report
 generating report output, [ND-3-16](#)
Report Comparison Options, [ND-3-22](#)
Report Formats, [ND-3-16](#)
reports
 generating Microsoft Word report in NetDoctor, [ND-3-21](#)
 using report templates in NetDoctor, [ND-3-6](#)
 viewing in NetDoctor, [ND-3-16](#)
Reusing Security Demand Configuration Information,
[ND-3-33](#)
rule description
 viewing, [ND-3-4](#)
Rule Output - Concise, [ND-3-19](#)
Run NetDoctor Dialog Box, [ND-3-12](#)
Run NetDoctor dialog box, [ND-3-12](#)
Running NetDoctor (Basic Configuration), [ND-3-5](#)
Running NetDoctor from a Template, [ND-3-12](#)

S

security demand
 creating, [ND-3-30](#)
 creating attributes, [ND-3-31](#)
 creating demands using the object palette, [ND-3-30](#)

 creating multiple demands simultaneously, [ND-3-31](#)
 exporting and importing, [ND-3-33](#)
 running simulations, [ND-3-35](#)
 selecting tables for security Web report, [ND-3-36](#)
Security Demand Attributes, [ND-3-31](#)
Security Demand Configuration File, [ND-3-34](#)
security report
 viewing, [ND-3-36](#)
Selecting Tables for Security Web-Report, [ND-3-36](#)
Settings Tab, [ND-3-10](#)
Suppressed Message Count, [ND-3-26](#)
Suppressing Messages, [ND-3-24](#)

T

Template Specification File, [ND-3-12](#)
The Demands Object Palette, [ND-3-30](#)
The NetDoctor Menu, [ND-3-2](#)

U

Using NetDoctor, [ND-3-1](#)
Using Security Demands in Simulations Studies, [ND-3-35](#)
Using Specified Commands, [ND-3-12](#)

V

View Recent NetDoctor Reports Dialog Box, [ND-3-16](#)
Viewing a Previous Report, [ND-3-16](#)
Viewing NetDoctor Reports, [ND-3-16](#)
Viewing Security Configuration in the Workspace, [ND-3-34](#)
Viewing Security Reports, [ND-3-36](#)
Visualizing Network Security Configuration, [ND-3-34](#)

W

Web Report, [ND-3-18](#)
Web report, [ND-3-18](#)
 generating, [ND-3-18](#)
 viewing sample output, [ND-3-6](#)