



Cisco Configuration Assurance Solution Audit and Analysis NetDoctor User Guide for IT Sentinel

Software Release 11.5

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-7584-02



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 Configuration Assurance Solution

Audit and Analysis

NetDoctor User Guide for IT Sentinel

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

Copyright

Document Copyright

Document Title: NetDoctor User Guide for IT Sentinel
Document Part Number: D00187
Version: 12

© 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 Sentinel
Product Release: 11.5

© 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 windowing 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 Sentinel Documentation Guide.

Document Revision History

Release Date	Product Version	Chapter	Description of Change
August 2005	11.5	Overview	<ul style="list-style-type: none"> Updated sections with new figures and a table. Moved system requirements to Getting Started.
		Getting Started	<ul style="list-style-type: none"> Renamed Administration to Getting Started. Reorganized sections.
		Using NetDoctor	<ul style="list-style-type: none"> Reorganized sections and updated figures and tables. Updated Comparing NetDoctor Reports. Added SNMP Trap, Syslog, and Trouble Ticket sections (Notification). Added section for device-centric and rule-centric reporting. (Report Formats).
		Customizing NetDoctor	<ul style="list-style-type: none"> Enhanced Tips for Effective Rule Development.
		Rules/Suites	<ul style="list-style-type: none"> Updated Rules appendix.
		NetDoctor APIs	<ul style="list-style-type: none"> Reorganized into four sections (Model Access, IP Graph, Reporting, and Simulation Output). Added examples for all methods and functions.
February 2005	11.0 PL3	Using NetDoctor	<ul style="list-style-type: none"> Added section for template checker rules. (Device Configuration File Validation). 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 Example.
		NetDoctor APIs	Added 11.0 PL1 APIs.
		Rules/Suites	Updated Rules appendix.

Release Date	Product Version	Chapter	Description of Change
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

Copyright ND-FM-iii

Documentation Conventions ND-FM-iv

Document Revision History ND-FM-vii

List of Figures. ND-FM-xi

List of Tables ND-FM-xiii

List of Procedures ND-FM-xiv

1 Overview ND-1-1

How Does NetDoctor Work? ND-1-1

Viewing NetDoctor Reports ND-1-2

NetDoctor Workflow ND-1-2

 Running NetDoctor. ND-1-3

 Viewing Results ND-1-3

 Analyze and Fix ND-1-3

 Typical NetDoctor Workflow. ND-1-4

Types of NetDoctor Messages ND-1-4

Available Rule Suites ND-1-5

How This User Guide Is Organized ND-1-6

2 Getting Started ND-2-1

System Requirements ND-2-1

Adding and Activating a NetDoctor License ND-2-1

The NetDoctor Menu ND-2-2

Using the NetDoctor Tutorial ND-2-3

3 Using NetDoctor ND-3-1

NetDoctor Options ND-3-2

 Run NetDoctor Options ND-3-2

 Configure/Run NetDoctor ND-3-3

 Run NetDoctor. ND-3-3

Configuring NetDoctor ND-3-4

 NetDoctor Templates ND-3-4

 Default Template ND-3-4

 Auto-Generate a Report Template ND-3-6

 Manually Create a Report Template ND-3-7

 Generating a Report from a Template ND-3-9

 Templates and Use Cases ND-3-10

 Report Settings ND-3-11

 Settings Tab ND-3-11

 Notification ND-3-13

 Configuring Notification Plug-ins ND-3-13

- Email ND-3-15
- SNMP Trap ND-3-18
- Syslog ND-3-21
- Trouble Ticket ND-3-24
- Device Configuration File Validation ND-3-27
 - Using Specified Commands ND-3-27
 - Example of a Specified Command Rule ND-3-30
 - Using Template Files ND-3-32
 - Rules for Configuration File Sections ND-3-37
- Viewing NetDoctor Reports ND-3-39
 - Report Formats ND-3-40
 - Web Report ND-3-40
 - Microsoft Word Report ND-3-44
 - Comparing Report Formats ND-3-45
 - Comparing NetDoctor Reports ND-3-46
 - NetDoctor's Report Comparison feature allows you to compare rule output between a current and previous run. When you configure Report Comparison and NetDoctor Notification, you can automatically publish or send critical information about new problems in your network. Configuring Report Comparison ND-3-46
 - Running Report Comparison ND-3-46
 - Report Comparison and Automation ND-3-46
 - Analyzing a Comparison Report ND-3-47
- Modifying NetDoctor Reports ND-3-48
 - Suppressing Messages ND-3-48
 - Configuring Global Options ND-3-51
- Modeling Network Security ND-3-53
 - NetDoctor Security Operations ND-3-53
 - Security Demands ND-3-53
 - Configuring Security Demands ND-3-54
 - Reusing Security Demand Configuration Information ND-3-57
 - Visualizing Network Security Configuration ND-3-58
 - Using Security Demands in Simulations Studies ND-3-59
 - Generating Security Reports ND-3-60

Index

ND-IX-1

List of Figures

Figure 1-1	NetDoctor Web Report.	ND-1-2
Figure 1-2	Typical NetDoctor Workflow.	ND-1-4
Figure 2-1	NetDoctor Menu.	ND-2-2
Figure 3-1	Configure/Run NetDoctor Dialog Box: Rules Tab	ND-3-3
Figure 3-2	Run NetDoctor Dialog Box.	ND-3-3
Figure 3-3	NetDoctor Web Report: Sample Output.	ND-3-5
Figure 3-4	Auto-Generate Report Template Dialog Box	ND-3-6
Figure 3-5	Available Templates.	ND-3-7
Figure 3-6	Parameter Description Tooltip	ND-3-9
Figure 3-7	Run NetDoctor Dialog Box.	ND-3-9
Figure 3-8	Configure/Run NetDoctor Dialog Box: Settings Tab	ND-3-11
Figure 3-9	Notification in the Configure/Run NetDoctor Dialog Box	ND-3-14
Figure 3-10	NetDoctor Email Notification	ND-3-17
Figure 3-11	SNMP Trap Notification in the Configure/Run Dialog Box.	ND-3-18
Figure 3-12	Sample List of SNMP Traps Generated by NetDoctor.	ND-3-20
Figure 3-13	Configure Syslog Notification Plug-in.	ND-3-21
Figure 3-14	Remedy HelpDesk Notification in the Configure/Run Dialog Box	ND-3-24
Figure 3-15	Match/No Match Commands	ND-3-28
Figure 3-16	Report on Match/No Match Commands.	ND-3-29
Figure 3-17	Match/No Match Commands	ND-3-31
Figure 3-18	Report on Match/No Match Commands.	ND-3-31
Figure 3-19	Multi-Layer Switch Test	ND-3-32
Figure 3-20	Match Templates	ND-3-33
Figure 3-21	Template Specification File	ND-3-34
Figure 3-22	Template File Rule.	ND-3-35
Figure 3-23	Folder Contents	ND-3-36
Figure 3-24	Template_file_spec.xml File.	ND-3-36
Figure 3-25	Match Templates for “^hostname”	ND-3-36
Figure 3-26	NetDoctor Results for Template File Check.	ND-3-37
Figure 3-27	Detail of Rule Result	ND-3-37
Figure 3-28	Starting and Ending Sections in the Template Specification File.	ND-3-38
Figure 3-29	View Recent NetDoctor Reports Dialog Box	ND-3-39
Figure 3-30	Web Report	ND-3-40
Figure 3-31	Rules Run in Bar Graph.	ND-3-40
Figure 3-32	Executive Summary: By Rule or By Device	ND-3-41
Figure 3-33	Rule-Centric Display	ND-3-42
Figure 3-34	Device-Centric Display.	ND-3-43
Figure 3-35	NetDoctor Report in Microsoft Word	ND-3-44
Figure 3-36	Report Comparison Options.	ND-3-46
Figure 3-37	A Web Comparison Report	ND-3-47
Figure 3-38	Edit Suppressions Dialog Box	ND-3-49
Figure 3-39	Suppressed Message Count	ND-3-50
Figure 3-40	NetDoctor Options Dialog Box.	ND-3-51
Figure 3-41	The Demands Object Palette	ND-3-54
Figure 3-42	Security Demand Attributes	ND-3-55

Figure 3-43	Create Security Demands Dialog Box	ND-3-56
Figure 3-44	Create Security Demands Dialog Box—With and Without Selection.	ND-3-57
Figure 3-45	Security Demand Configuration File	ND-3-58
Figure 3-46	Network Security Configuration Visualization	ND-3-59
Figure 3-47	Selecting Tables for Security Web-Report.	ND-3-60
Figure 3-48	Network Security Web Report	ND-3-61

List of Tables

Table 1-1	NetDoctor Rule Suites	ND-1-5
Table 1-2	User Guide Contents	ND-1-6
Table 2-1	NetDoctor Menu Operations	ND-2-3
Table 3-1	NetDoctor Options	ND-3-2
Table 3-2	Configure/Run NetDoctor Dialog Box: Settings	ND-3-11
Table 3-3	Email Notification Parameters	ND-3-15
Table 3-4	Email Notification Parameters (Advanced)	ND-3-16
Table 3-5	SNMP Trap Notification Parameters	ND-3-19
Table 3-6	SNMP Trap Notification Parameters (Advanced)	ND-3-19
Table 3-7	Syslog Notification Parameters	ND-3-22
Table 3-8	Syslog Notification Parameters (Advanced)	ND-3-22
Table 3-9	Trouble Ticket Parameters	ND-3-25
Table 3-10	Trouble Ticket Parameters (Advanced)	ND-3-26
Table 3-11	Available Parameters for Vendor-Specific Rules	ND-3-27
Table 3-12	Available Parameters for Generic Rules	ND-3-29
Table 3-13	Available Parameters for Vendor-Specific Rules	ND-3-32
Table 3-14	Available Parameters for Generic Rules	ND-3-33
Table 3-15	NetDoctor Report Organization	ND-3-45
Table 3-16	Running NetDoctor with Automation	ND-3-47
Table 3-17	NetDoctor Options	ND-3-51

List of Procedures

Procedure 2-1	Adding a NetDoctor License	ND-2-1
Procedure 2-2	Activating a NetDoctor License	ND-2-2
Procedure 2-3	Opening the NetDoctor Tutorial	ND-2-3
Procedure 3-1	Running NetDoctor with the Default Template	ND-3-4
Procedure 3-2	Auto-Generating a Report Template	ND-3-6
Procedure 3-3	Creating a Report Template Manually	ND-3-8
Procedure 3-4	Running NetDoctor from a Template	ND-3-9
Procedure 3-5	Configuring a NetDoctor Notification Plug-in	ND-3-13
Procedure 3-6	Viewing a Previous Report	ND-3-39
Procedure 3-7	Creating a Suppression File	ND-3-48
Procedure 3-8	Applying a Suppression File to a Template	ND-3-50
Procedure 3-9	Creating Security Demands	ND-3-54
Procedure 3-10	Creating Multiple Security Demands Simultaneously	ND-3-55
Procedure 3-11	Viewing Security Configuration in the Workspace	ND-3-58
Procedure 3-12	Viewing Security Reports	ND-3-60

1 Overview

NetDoctor is a powerful, rules-based engine that proactively identifies incorrect device configurations, policy violations, and inefficiencies. NetDoctor exposes potential problems that can affect the availability, performance, and security of your network. Use the comprehensive rules provided with NetDoctor or use your own custom rules to

- locate network problems caused by misconfigurations
- identify underlying 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.

How Does NetDoctor Work?

NetDoctor rules are run against configuration data, which are set from device configurations imported from a production network. Some NetDoctor rules use simulation data to identify inconsistencies in the performance of the network. NetDoctor identifies specific problems such as

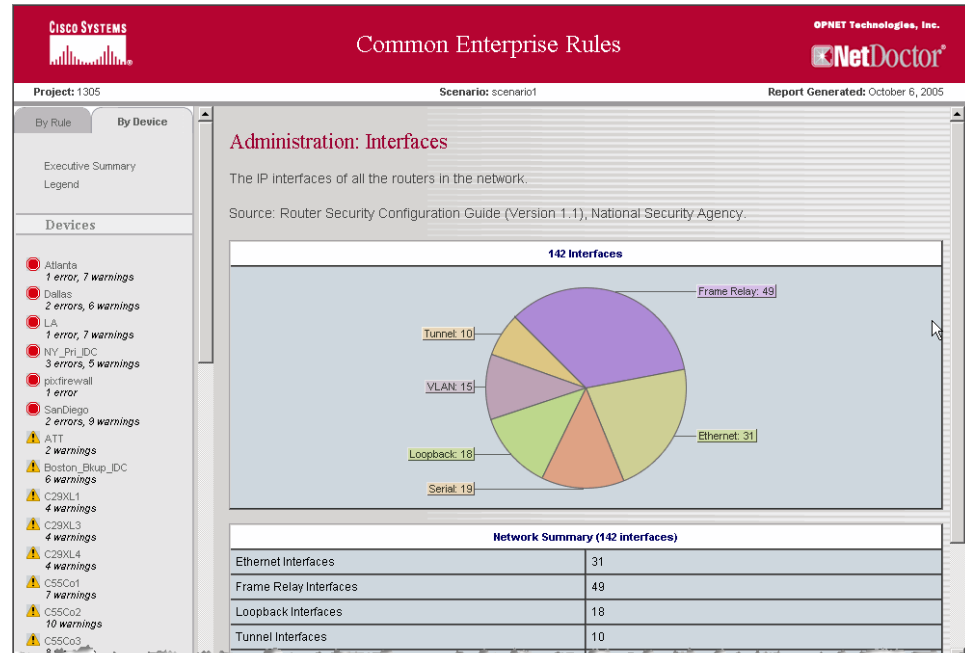
- OSPF area border routers that are not connected to the backbone area
- IBGP neighbors that are not fully meshed—including confederations and route reflectors
- ACLs that contain ineffective statements
- inconsistent interface parameters for OSPF that prevent the formation of adjacencies

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 other users.

Viewing NetDoctor Reports

NetDoctor produces its results in customizable reports, which you can view in a web browser or in Microsoft Word. See Figure 1-1 for a sample web report.

Figure 1-1 NetDoctor Web Report



NetDoctor includes support for languages other than US English. You can install language libraries developed by OPNET or you can customize the report language with your own message library (see Multi-Language Rule Output on page ND-4-33).

Note—Download the available language libraries from the OPNET technical support page (www.opnet.com/support). Check for the latest versions of the libraries after new releases of the OPNET software. The most up-to-date language libraries may lag the most recent OPNET software release.

NetDoctor Workflow

To run NetDoctor, first import configuration data using Device Configuration Imports (DCI) from your network or from an Import from VNE Server. The rules are then run against these sources to uncover issues in your network.

Running NetDoctor

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. For example, a NetDoctor verification rule displays a warning if a network statement references an invalid interface.
- **Summary rules**—These rules provide information about the configuration and operation of the network. For example, a NetDoctor summary rule generates a report on the distinct OS versions deployed in the network.

The standard NetDoctor installation includes a variety of rules organized into suites to use immediately, and an API that supports the development of custom rules to codify the expertise and policies of your organization into new NetDoctor rules.

NetDoctor also provides a template auto-generation feature to quickly analyze your network and intelligently select rules based on brief input from you.

Viewing Results

View NetDoctor results based on the rules or the devices—in concise or detailed formats. 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. You specify whether NetDoctor generates a web (.html) report or a Microsoft Word (.rtf) report. Each time you run NetDoctor, you can view and save the results for further analysis.

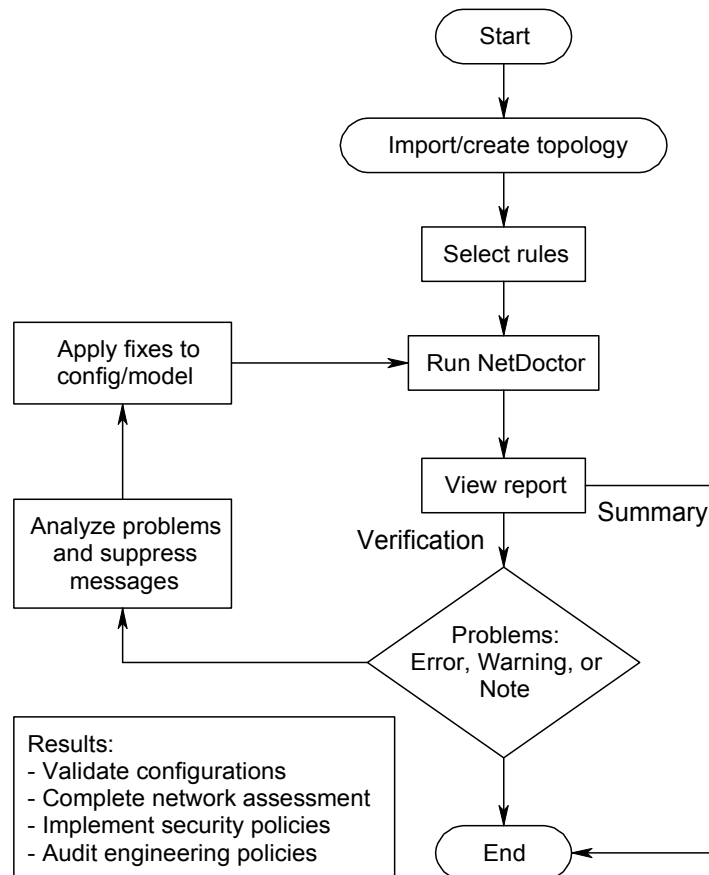
Analyze and Fix

The next step is to analyze your results and fix configuration errors, modify policies, and/or change the template rules or templates you want to use, and then run NetDoctor again.

Typical NetDoctor Workflow

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 1-2 shows a typical NetDoctor workflow.

Figure 1-2 Typical NetDoctor Workflow



Types of NetDoctor Messages

Examples of the messages generated by NetDoctor's verification rules include the following:

- **Error**—A violation specifying that the severity of the reported problem is critical. Determine if these problems should be fixed to ensure the network is fully operational.
- **Warning**—A violation specifying that the reported problem is not considered critical. Determine if these problems should be fixed to prevent potential problems and degraded network performance.

- **Note**—Supplementary information about items in the NetDoctor analysis that you may find helpful.
- **Pass**—A message that a tested object passed the verification rule. Setting NetDoctor to report this message is useful for troubleshooting your NetDoctor configuration in a development environment, particularly if you are receiving no errors or warnings. To save on system resources in a production environment, you will most likely not want to generate a message for every passed node.

Use thresholds to configure NetDoctor to limit its reporting to messages that meet or exceed your required severity levels.

Available Rule Suites

NetDoctor includes the following rule suites:

Table 1-1 NetDoctor Rule Suites

AAA	IPSec	RIP
Administration	IPX	Route Maps and ACLs
ATM	IS-IS	RSRB
BGP	Kerberos	Security
DLSw	Link Aggregation	SNMP
EIGRP	MPLS	Spanning Tree
Firewalls	MPLS VPNs	Static Routing
HSRP	NAT	System Logging
IGRP	Organizational Policies	TACACS+
IP Addressing	OSPF	Tunnel Interfaces
IP Multicast	QoS	VLANs
IP Routing	RADIUS	Voice over IP

NetDoctor can support additional protocols through custom rules. See App A Suites and Rules on page ND-A-1 for a description of all available rules.

How This User Guide Is Organized

The following table describes where to find key features and workflow procedures.

Table 1-2 User Guide Contents

Chapter	Description
Overview	Gives general information about the functions and features of the NetDoctor module.
Getting Started	Describes system requirements, activating a NetDoctor license, menu descriptions, and how to access the tutorial file.
Using NetDoctor	Describes the procedures for configuring and running NetDoctor, and for viewing NetDoctor output.
Customizing NetDoctor	Describes how to edit NetDoctor rules and how to write custom rules for your own business environment. Describes how to create and edit notification plug-ins. Describes how to create and edit charts for your reports. Describes how to extend message libraries to support additional languages for rule output.
Appendix A: Suites and Rules	Lists all NetDoctor rules and their descriptions.
Appendix B: NetDoctor APIs	Lists the NetDoctor APIs. Rules are written in the Python programming language.
End of Table 1-2	

2 Getting Started

This chapter describes the following topics:

- System Requirements
- Adding and Activating a NetDoctor License
- The NetDoctor Menu
- Using the NetDoctor Tutorial

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

Note—Beginning with OPNET release 11.5 and later, NetDoctor Notification no longer requires the Automation module license.

Adding and Activating a NetDoctor License

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

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

Once you have a valid license, you need to activate the license as described in Procedure 2-2.

Procedure 2-2 Activating a NetDoctor License

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

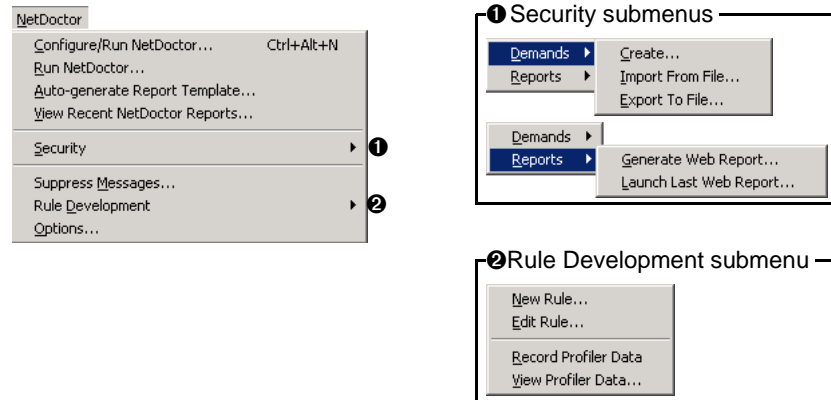
End of Procedure 2-2

The NetDoctor Menu

To use the NetDoctor module, access the main menu and submenus from the Project Editor main window. See Figure 2-1.

Figure 2-1 NetDoctor Menu

NetDoctor main menu



The following table describes the operations of the NetDoctor menu. For a detailed description of how to use these operations, see the Using NetDoctor chapter. For rule development and more advanced configuration and troubleshooting, see the Customizing NetDoctor chapter.

Table 2-1 NetDoctor Menu Operations

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.
Suppress Messages...	Create or edit suppression files.
Rule Development	Create new NetDoctor rules or edit existing rules.
Options...	Set NetDoctor-specific options like the web and Word logos, colors for message types, etc.
End of Table 2-1	

Using the NetDoctor Tutorial

The documentation includes a tutorial 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 NetDoctor’s rules-based analysis. The last section of this chapter describes how to configure and run security analyses using security demands. Use the following table to access topics organized by objective:

Objective	Topic	Subtopics
Running NetDoctor	NetDoctor Options	<ul style="list-style-type: none"> • Configure/Run NetDoctor • Run NetDoctor
Understanding NetDoctor Configuration	Configuring NetDoctor	<ul style="list-style-type: none"> • NetDoctor Templates • Report Settings • Notification • Device Configuration File Validation
Understanding 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"> • NetDoctor Security Operations • Visualizing Network Security Configuration • Using Security Demands in Simulations Studies • Generating Security Reports

Note—See The NetDoctor Menu in the Getting Started section of this user guide for basic operation descriptions.

NetDoctor Options

NetDoctor provides options for displaying the type and format of the report information you need. Choose individual rules or suites of rules for each template along with other configuration settings. See Table 3-1 for a brief overview of the NetDoctor options:

Table 3-1 NetDoctor Options

Configuration Setting	Options
Rules	<ul style="list-style-type: none"> • Report on any combination of rules • Specify rule parameters
Report Content	<ul style="list-style-type: none"> • Specify the severity of messages reported • Prevent messages for certain objects from being reported • Add a diagram of the network • Add appendices to the report
Report Format <ul style="list-style-type: none"> • Device-Centric Concise • Device-Centric Detailed • Rule-Centric Concise • Rule-Centric Detailed 	<ul style="list-style-type: none"> • Web (.html)—all formats in one report • Microsoft Word (.rtf)—one report for each format • XML
Report Language	<ul style="list-style-type: none"> • English • Install language libraries from OPNET Technical Support • Customize others
Notification	<ul style="list-style-type: none"> • Email • SNMP Trap • Syslog • Trouble Ticket • Customize others

Note—Choose other global settings such as the web report logo or report colors by selecting Options from the NetDoctor menu. See Configuring Global Options on page ND-3-51

Run NetDoctor Options

The two options for running NetDoctor are

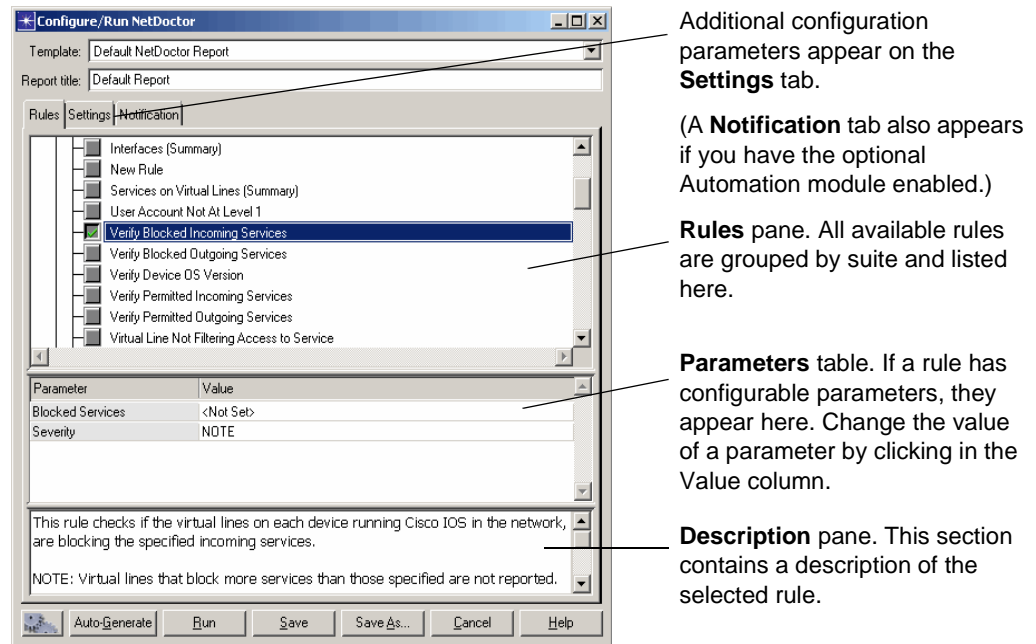
- Configure/Run NetDoctor
- Run NetDoctor

Configure/Run NetDoctor

To specify configuration settings for individual templates before running, select Configure/Run NetDoctor from the NetDoctor menu in the Project Editor main window.

Use the Rules tab in the Configure/Run NetDoctor dialog box to select or preview the rules used for a template. See Figure 3-1.

Figure 3-1 Configure/Run NetDoctor Dialog Box: Rules Tab



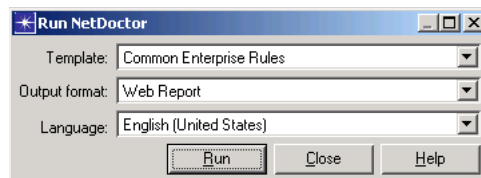
For explanations of the other tabs see the Settings Tab on page ND-3-11 and Notification on page ND-3-13.

Run NetDoctor

To run NetDoctor without specifying individual template settings, select Run NetDoctor from the NetDoctor menu in the Project Editor main window. Specify the template, output format, and language before running. See Figure 3-2.

Note—All other configuration settings are determined by the selected template.

Figure 3-2 Run NetDoctor Dialog Box



Configuring NetDoctor

Configuring NetDoctor requires creating and saving templates. Individual rules or groups of rules organized by rule suites run against your network model using NetDoctor templates. NetDoctor templates also store the format, language, comparison, and notification settings of your report.

NetDoctor Templates

There are two ways to create report templates:

- Let NetDoctor automatically generate a template.
- Manually select the individual rules and suites for the template you are creating from an existing template.

Several example templates are included with NetDoctor. Use these templates as configured or as a starting point when creating your own templates. The main templates for running NetDoctor are:

- Default template
- Auto-generated template
- Manual template

Once a template is saved, it becomes available from the Template drop-down list when you configure and/or run NetDoctor. Edit the title of the generated report in the Report title field. This name appears on the final report and can be different from the name of the template.

Default Template


The default NetDoctor template is called the Default NetDoctor Report. This template contains all of the available NetDoctor rules organized by rule suites. Select the individual rules or suites of rules that you want to use, and then run NetDoctor (see Procedure 3-1 on page ND-3-4).

If you want to save your configuration settings as another template, select the Save As button before running NetDoctor. Save the template with a new name in your Model directory.

When you change settings in the Default NetDoctor Report and run, these settings will be saved to this template. Use the following procedure for running NetDoctor with the Default Template.

Procedure 3-1 Running NetDoctor with the Default Template

- 1 Open the project and scenario that you want NetDoctor to analyze.

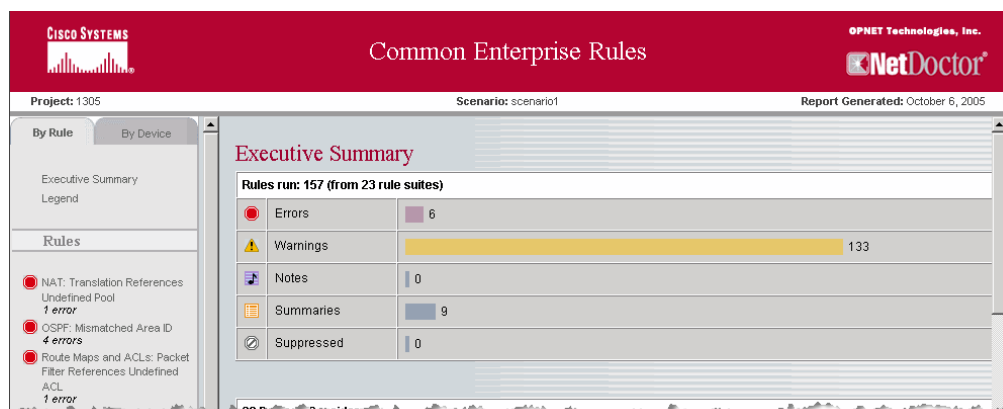
- 2 Open the Configure/Run NetDoctor dialog box. Use one of the following methods:
 - From the NetDoctor menu, choose Configure/Run NetDoctor.
 - On the toolbar, click the Configure/Run NetDoctor button. 

➔ 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

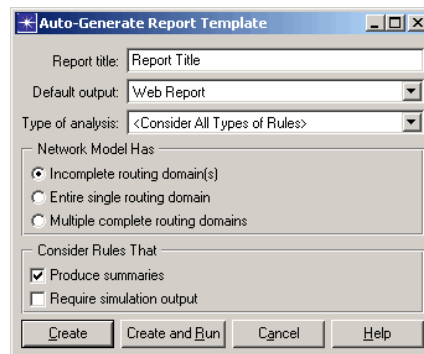
Auto-Generate a Report Template

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. By using the auto-generated template, you let NetDoctor intelligently select rules and generate a template for you. The template that is created will include only the rules that meet the criteria you specify and that 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 3-4 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 after you run the template.

- 4 Select the type of analysis. Each NetDoctor rule is associated with one or more types of analysis.
- 5 Specify the routing domain information.

Note—Match your model configuration with this setting to avoid false positives and to make sure rules that apply to your model are considered.

For example, if your model includes a multiple routing domain, and you select incomplete routing domain here, several rules will not be considered to run against your model. If on the other hand, you select a multiple routing domain and your network model has an incomplete routing domain, you will end up with several false positive messages.

- 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.

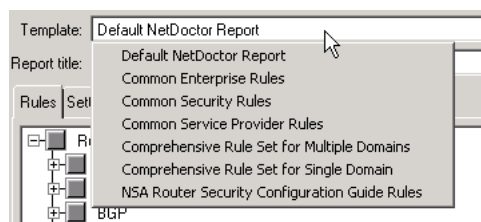
End of Procedure 3-2

Manually Create a Report Template

When you configure NetDoctor, the settings can be saved for reuse in the existing template or as a new template. 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. When you manually create a template with this method, save it in your Model directory (see Procedure 3-3 on page ND-3-8). You can then run NetDoctor with this saved template (see Procedure 3-4 on page ND-3-9).


NetDoctor includes several example templates, as shown in Figure 3-5.

Figure 3-5 Available Templates



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.

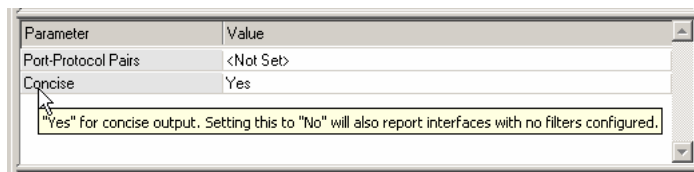
➔ The template is saved and the Configure/Run NetDoctor dialog box reopens.
- 4 In the Report title field, specify the title that NetDoctor should use for all reports generated from this template. This name appears on the final report and can be different from the name of the template.
- 5 Click on the 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-3-11 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-3-15 for a description of the available options.
- 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

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 opens.

Figure 3-7 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 for the report generated.
- 5 Click Run.
 - ➔ NetDoctor analyzes the network and generates the report in the specified format.

End of Procedure 3-4

Templates and Use Cases

By creating a template to match each of your network use cases, you reduce the number of configuration settings that need to change each time you run NetDoctor. The templates you create provide the basis for automating tasks. For example, create templates for more critical daily troubleshooting reports and others for weekly or monthly summary reports.

Report Settings

Report settings include the options for report format, language, suppression, and comparison features. For reports in languages other than English, you must install the associated language library or you can develop your own language library (see Multi-Language Rule Output on page ND-4-33). For more detailed explanations for the other settings, see Report Formats on page ND-3-40, Comparing NetDoctor Reports on page ND-3-46, and Suppressing Messages on page ND-3-48.

Note—Download the available language libraries from the OPNET technical support page (www.opnet.com/support). Check for the latest versions of the libraries after new releases of the OPNET software. The most up-to-date language libraries may lag the most recent OPNET software release.

Settings Tab

The Settings tab from the NetDoctor Configure/Run dialog box gives you access to change reporting options (see Figure 3-8). These options are associated with the selected template. More information on each parameter is listed in Table 3-2.

Figure 3-8 Configure/Run NetDoctor Dialog Box: Settings Tab

The following table describes the parameters available on the Settings tab shown in Figure 3-8.

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-3-9 describes how to do this.
Language	Specifies the language in which this report should be generated (download available language libraries from OPNET Technical Support. Additional language options may require customization, as described in the Customizing NetDoctor chapter, Multi-Language Rule Output on page ND-4-33).
Send report to report server	Sends a copy of the report to the specified Report Server .
Suppression File	Specifies a suppression file to use when generating reports with this template. See Modifying NetDoctor Reports on page ND-3-48 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).
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. Select the Use most recent scenario checkbox to specify if you want compare the current run with the most recent report. See Comparing NetDoctor Reports on page ND-3-46.
End of Table 3-2	

Notification

The NetDoctor Notification feature sends specific information about a NetDoctor run to you, other users, or applications. NetDoctor's notification system supports multiple notification plug-ins. For example, you can configure a notification plug-in to send information about a network problem directly to Remedy's HelpDesk system to open a trouble ticket.

NetDoctor provides the following notification plug-ins:

- Email
- SNMP Trap
- Syslog
- Trouble Ticket

Note—In OPNET release 11.5 and later, the NetDoctor Notification feature does not require an Automation module license or execution within the Sentinel application.

You can add notification plug-ins or customize existing ones. See Notification Plug-ins on page ND-4-66 for more information on adding custom notification plug-ins. Notification plug-ins are written using the Python programming language. For more information on how to use Python, see <http://www.python.org>.

Configuring Notification Plug-ins

Enable notifications from the Notification tab of the Configure/Run dialog box (see Figure 3-9). The configuration settings for each notification plug-in apply to the selected NetDoctor template.

Use Procedure 3-5 to configure a NetDoctor notification plug-in.

Procedure 3-5 Configuring a NetDoctor Notification Plug-in

- 1 Choose Configure/Run NetDoctor from the NetDoctor menu.
- 2 Select a template from the Template drop-down list.
- 3 Choose the Notification tab.
- 4 Select a notification plug-in from the Plug-in drop-down list.
- 5 Select the Enabled checkbox to enable the plug-in.

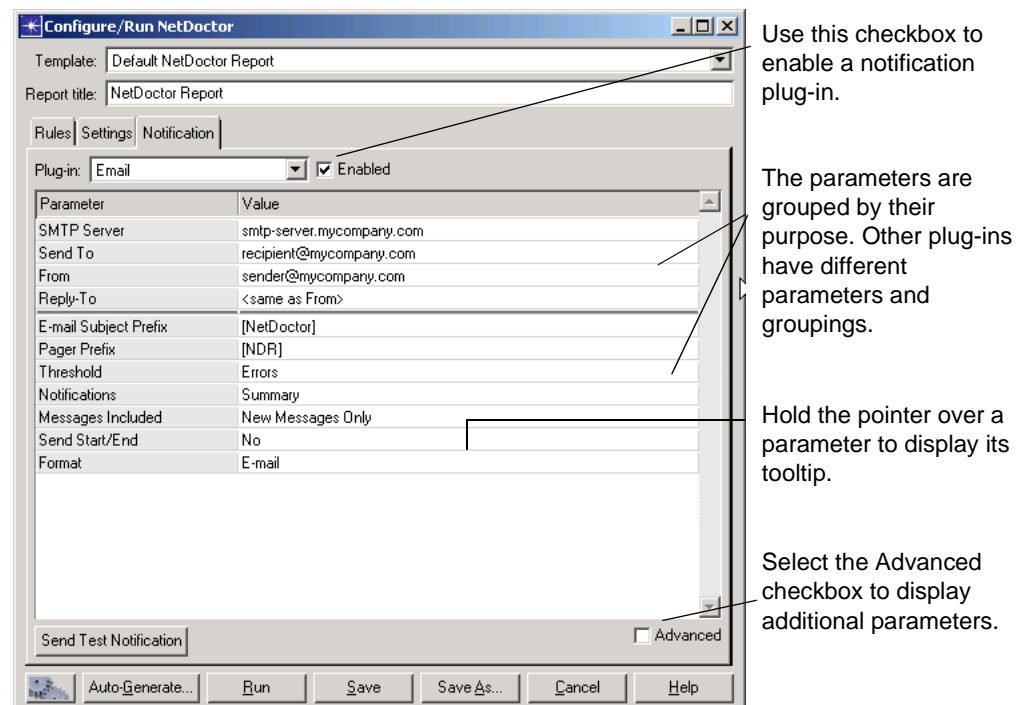
Note—You can enable multiple notification plug-ins for each NetDoctor template.

- 6 Edit the parameter values associated with the notification plug-in (see Figure 3-8 for the Email plug-in).
- 7 Choose Send Test Notifications to test the connectivity of the notification plug-in.
- 8 Continue to configure other plug-ins as needed.

End of Procedure 3-5

Once configured, notification plug-ins and their settings are saved with the selected template. Figure 3-9 shows the parameters available for the Email notification plug-in.

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



Email

Configure the Email notification plug-in to send emails or pages to a list of the recipients. Table 3-3 and Table 3-4 describe the Email notification parameters.

Table 3-3 Email Notification Parameters

Parameter	Description
SMTP Server	DNS name or IP address of the destination SMTP server.
Send To	A comma separated list of the recipient Email addresses.
From	Address to use in the From header of generated emails.
Reply-To	Reply-To header to use in generated emails. If this is set to "<same as From>", then the Reply-To header will not be included.
Email Subject Prefix	Beginning text to use in subject field of all notifications when the Format parameter is set to Email.
Pager Prefix	Beginning text to use in subject field of all notifications when the Format parameter is set to Pager. A shorter prefix is usually preferred; the message length for pager notifications is often limited.
Threshold	Controls the types of messages that are included in the notifications. See Types of NetDoctor Messages on page ND-1-4 for a description of the available message types.
Notifications	NetDoctor can send a notification for each rule (per the Threshold), send a summary notification that covers all of the rules in the run (per the Threshold), or it can do both.
Messages Included	This parameter is considered only when Report Comparison is enabled: All Messages (considers all messages generated for a notification), or New Messages Only (considers only the messages that are not in the compared report).
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.
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.
End of Table 3-3	

Table 3-4 Email Notification Parameters (Advanced)

Parameter	Description
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-3-17 for an example of how this attribute works.
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 3-4	

Figure 3-10 shows the Email notification plug-in configuration parameters and values for a NetDoctor run with samples of the resulting summary and rule notification emails. This configuration generated many messages, but only two are shown.

Figure 3-10 NetDoctor Email Notification

Parameter	Value
SMTP Server	smtp-server.mycompany.com
Send To	recipient@mycompany.com
From	sender@mycompany.com
Reply-To	<same as From>
Email Subject Prefix	[NetDoctor] 1
Pager Prefix	[NDR]
Threshold	Errors 2
Notifications	Summary 3
Messages Included	New Messages Only
Send Start/End	No
Format	Email
Max. Message Count	2 4
Max. Object Count	5
Max. Pager Length	120
Pager Msg. Location	Subject

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.
    
```

4

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

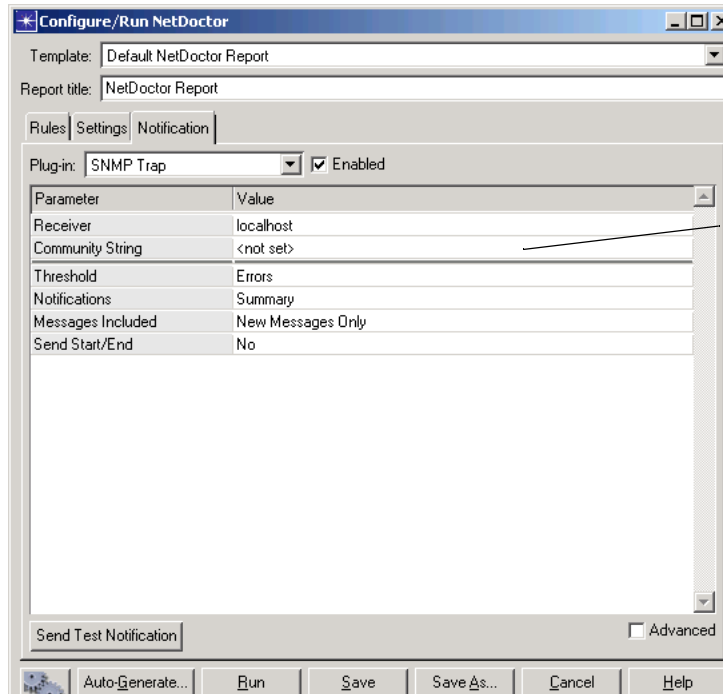
Template: Default NetDoctor Report
Report Title: Comprehensive Report
Project-Scenario: FA_Multiprotocol_Network-FlowAnalysis_original
Summary: 239 rules run, 7 rules tripped (1 error, 67 warnings) 2
Rules with at least one error or warning: 7
-----
* OSPF: Discontiguous Area (1 error)
* Administration: 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)
    
```

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

SNMP Trap

Configure the SNMP Trap notification plug-in to send a trap to a network management system. Depending on changes to your network configuration and how often you run NetDoctor, a trap sends timely alerts of network problems. Figure 3-11 shows the parameters available for the SNMP Trap notification plug-in.

Figure 3-11 SNMP Trap Notification in the Configure/Run Dialog Box



Use these parameters to set the values for the SNMP trap receiver host.

Table 3-5 and Table 3-6 describe the SNMP Trap notification parameters.

Table 3-5 SNMP Trap Notification Parameters

Parameter	Description
Receiver	The DNS name or IP address for trap receiver host.
Community String	Trap community string for trap receiver host.
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.
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.
Messages Included	This parameter is considered only when Report Comparison is enabled: All Messages (considers all messages generated for a notification), or New Messages Only (considers only the messages that are not in the compared report).
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.
Max. Message Length	The maximum number of characters to include in the trap (default 255).
End of Table 3-5	

Table 3-6 SMNP Trap Notification Parameters (Advanced)

Parameter	Description
Receiver Port	Trap listening port number for trap receiver host (default 162).
Max. Message Length	The maximum number of characters to include in the trap (default 255).
End of Table 3-6	

Figure 3-12 shows an example of a sample list SNMP traps generated by NetDoctor.

Figure 3-12 Sample List of SNMP Traps Generated by NetDoctor

Timestamp	Host Name	Event Description	Trap OID and Type	Rule Messages
Thu May 12 18:01:14	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	System Logging: Logging Disabled (17 warnings)
Thu May 12 18:01:14	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	BGP: EBGP Neighbor not Locally Connected (4 errors)
Thu May 12 18:01:17	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	IP Routing: Routing Loops In Network (37 warnings)
Thu May 12 18:01:18	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	ISIS: Incompatible Circuit Type Between Peers (6 warnings)
Thu May 12 18:01:18	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	ISIS: Inconsistent Metrics (1 warning)
Thu May 12 18:01:19	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Area Summary Includes Addresses Outside Area (7 warnings)
Thu May 12 18:01:10	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Discontiguous Area (1 error)
Thu May 12 18:01:11	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Inconsistent Metric (4 warnings)
Thu May 12 18:01:11	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Inconsistent Reference Bandwidth (1 warning)
Thu May 12 18:01:11	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Mismatched Area ID (4 errors)
Thu May 12 18:01:11	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	OSPF: Network Statement References Invalid Interface (1 warning)
Thu May 12 18:01:12	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	Route Maps and ACLs: Ineffective ACL (1 warning)
Thu May 12 18:01:13	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	Route Maps and ACLs: Packet Filter References Undefined
Thu May 12 18:01:13	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	Route Maps and ACLs: Redundant Statement In ACL (4 warnings)
Thu May 12 18:01:13	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	Route Maps and ACLs: Redundant Statement in Route Map (1 warning)
Thu May 12 18:01:13	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	VLANs: Inconsistent VLANs Across Trunk Link (96 warnings)
Thu May 12 18:01:14	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	SNMP: Community Uses Weak Name (65 warnings)
Thu May 12 18:01:14	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	SNMP: Community Without ACL (55 warnings)
Thu May 12 18:01:15	wtn12090.opnet.com	Received NetDoctor Event [1]	private.enterprises.21359.1.9.1.1.0.1.1 (OctetString)	Default: NetDoctor Report: 160 rules run, 18 rules report

Syslog

The Syslog notification plug-in sends NetDoctor rule message data to a syslog server on your network. Figure 3-13 shows the parameters available for the Syslog notification plug-in.

Figure 3-13 Configure Syslog Notification Plug-in

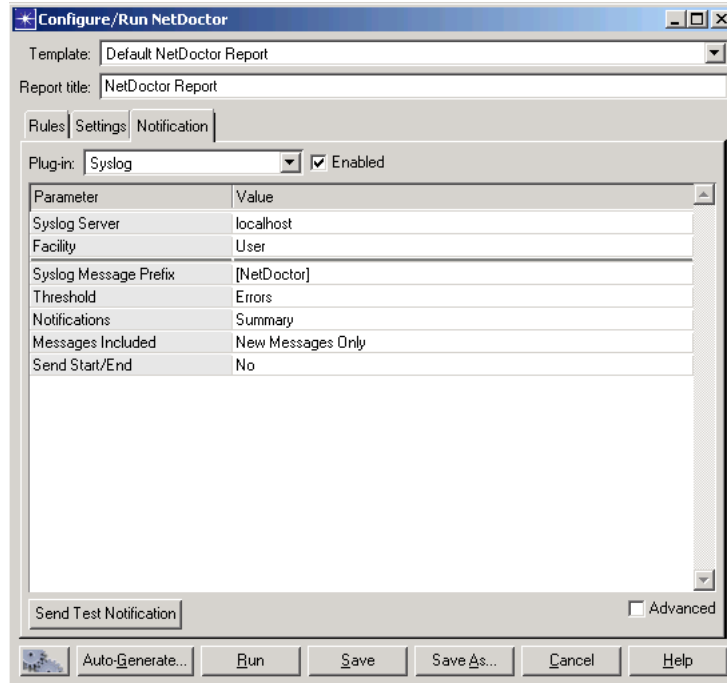


Table 3-7 and Table 3-8 describe the Syslog notification parameters.

Table 3-7 Syslog Notification Parameters

Parameter	Description
Syslog Server	Server name or IP address (default localhost).
Facility	The user access level configured on the syslog server. Values can be local0 - local7.
Syslog Message Prefix	The prefix to use for the syslog message notifications.
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.
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.
Messages Included	This parameter is considered only when Report Comparison is enabled: All Messages (considers all messages generated for a notification), or New Messages Only (considers only the messages that are not in the compared report).
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.
End of Table 3-7	

Table 3-8 Syslog Notification Parameters (Advanced)

Parameter	Description
Port	UDP port number (default 514).
Syslog Severity for NetDoctor Errors	Specify the syslog severity entry for NetDoctor message (default Error).
Syslog Severity for NetDoctor Warnings	Specify the syslog severity entry for NetDoctor message (default Warning).

Table 3-8 Syslog Notification Parameters (Advanced)

Parameter	Description
Syslog Severity for NetDoctor Notes	Specify the syslog severity entry for NetDoctor message (default Note).
Syslog Severity for NetDoctor Passed Messages	Specify the syslog severity entry for NetDoctor message (default Info).
Max. Message Length	The maximum number of characters to include in the syslog (default 255).
End of Table 3-8	

Trouble Ticket

The Trouble Ticket notification plug-in creates Remedy HelpDesk trouble tickets. You can configure the Trouble Ticket Notification plug-in to create a trouble ticket for each rule, each report entry generated by a rule, or one ticket for the entire NetDoctor run.

The Trouble Ticket notification plug-in is written for the standard HelpDesk_Submit_Service that is available with the default installation of Remedy HelpDesk (Mid-Tier Version 6.3).

Note—The Remedy form and web service are fully customizable, including changes to web service fields (required or not), and changes to acceptable values for fields. Some changes to the web service configuration will require you to customize the Trouble Ticket plug-in (see Creating Customized Plug-ins on page ND-4-68).

Figure 3-11 shows the parameters available for the Remedy HelpDesk notification plug-in.

Figure 3-14 Remedy HelpDesk Notification in the Configure/Run Dialog Box

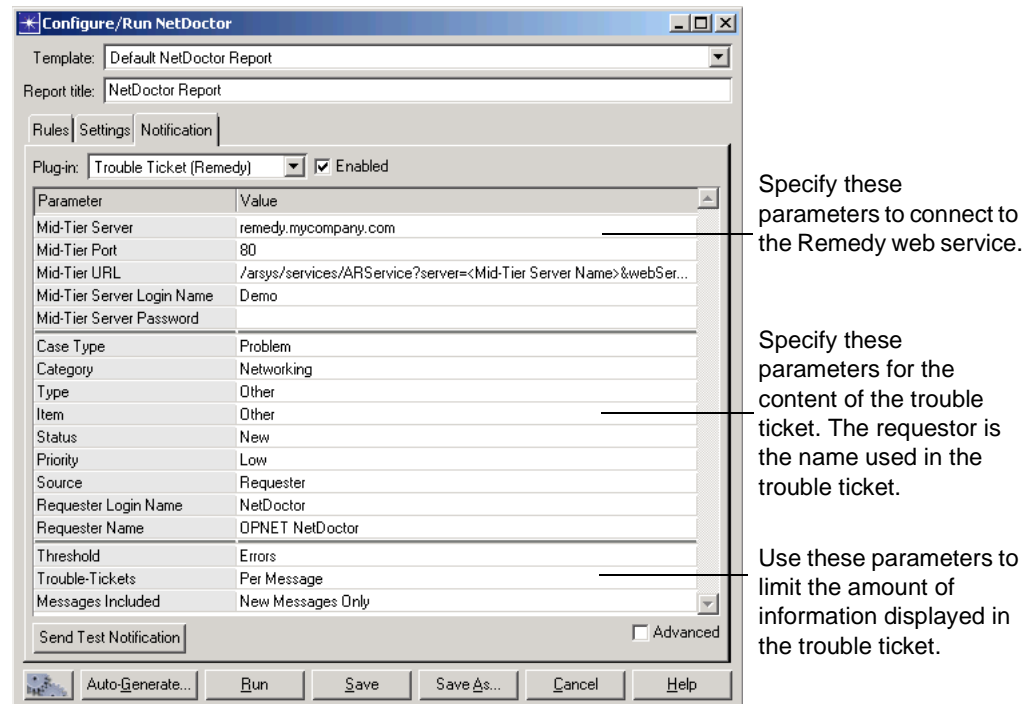


Table 3-9 and Table 3-10 describe the Remedy HelpDesk notification parameters.

Table 3-9 Trouble Ticket Parameters

Parameter	Description
Mid-Tier Server	The DNS name or IP address of the Remedy Mid-Tier Server running the HelpDesk_Submit_Service.
Mid-Tier Port	The HTTP port of the HelpDesk_Submit_Service.
Mid-Tier URL	The complete path including arguments (if any) to the HelpDesk_Submit_Service.
Mid-Tier Server Login Name	The login name of the user account to create the HelpDesk tickets.
Mid-Tier Server Password	The password of the user account to create the HelpDesk tickets.
Case Type	The case type of the HelpDesk tickets (default Problem).
Category	The category of the HelpDesk tickets (default Network).
Type	The type of the HelpDesk tickets.
Item	The item of the HelpDesk tickets.
Status	The status of the HelpDesk tickets.
Priority	The priority of the HelpDesk tickets (default Low).
Source	The source to use as the requestor of the HelpDesk tickets (default Requestor).
Requestor Login Name	The login name of the requestor of the HelpDesk tickets.
Requestor Name	The name of the requestor of the HelpDesk tickets.

Table 3-9 Trouble Ticket Parameters

Parameter	Description
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.
Trouble-Tickets	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.
Messages Included	This parameter is considered only when Report Comparison is enabled: All Messages (considers all messages generated for a notification), or New Messages Only (considers only the messages that are not in the compared report).
End of Table 3-9	

Table 3-10 Trouble Ticket Parameters (Advanced)

Parameter	Description
Max. Message Count	The maximum number of messages in a Per Rule HelpDesk ticket.
Max. Object Count	The maximum number of problem objects in the summary of a Per Message HelpDesk ticket.
Max. Summary Length	The maximum length of the summary field of the HelpDesk ticket.
Max. Description Length	The maximum length of the description field of the HelpDesk ticket. 0 means that the length is unlimited.
End of Table 3-10	

Device Configuration File Validation

NetDoctor includes rules designed to help you validate device configuration files. These rules are contained in the Organizational Policies rule suite and have parameters that let you specify the conditions your device configuration file must match or not match. You can also change the severity of the rule result.

Note—Device configuration file validation rules rely on Python regular expressions. While Python regular expressions are outside the scope of this document, you can find such information at the Python.org website: <http://www.python.org/doc/2.3.4/lib/module-re.html>.

There are two kinds of rules in the Organizational Policies rule suite:

- Specified command rules—let you specify one or more commands in the rule’s parameters to match or not match.
- Template file rules—let you specify a template file or set of template files that contain commands to match or not match in the rule’s parameters.

These rules require the network model to be populated with the device configuration files associated with the network objects. You can either import your device configuration files through Device Configuration Import (DCI) or Import from VNE Server. For information on DCI, refer to Device Configuration Imports (DCI) on page ISU-10-21 of the *Sentinel User Guide*. For information on importing from VNE Server, refer to Import from VNE Server on page ISU-10-2 of the *Sentinel User Guide*.

Using Specified Commands

There are several vendor-specific versions and one generic version of this rule. The vendor-specific versions test devices that run a specific vendor’s operating system. This is indicated in the rule’s name (“Cisco Router IOS Configuration Differs from Specified Commands”, for example). The parameters for these rules are described in Table 3-11.

Table 3-11 Available Parameters for Vendor-Specific Rules

Parameter	Value
Device Name	The Python regular expression used to decide which devices to check. Use “.*” to match all names.

Table 3-11 Available Parameters for Vendor-Specific Rules

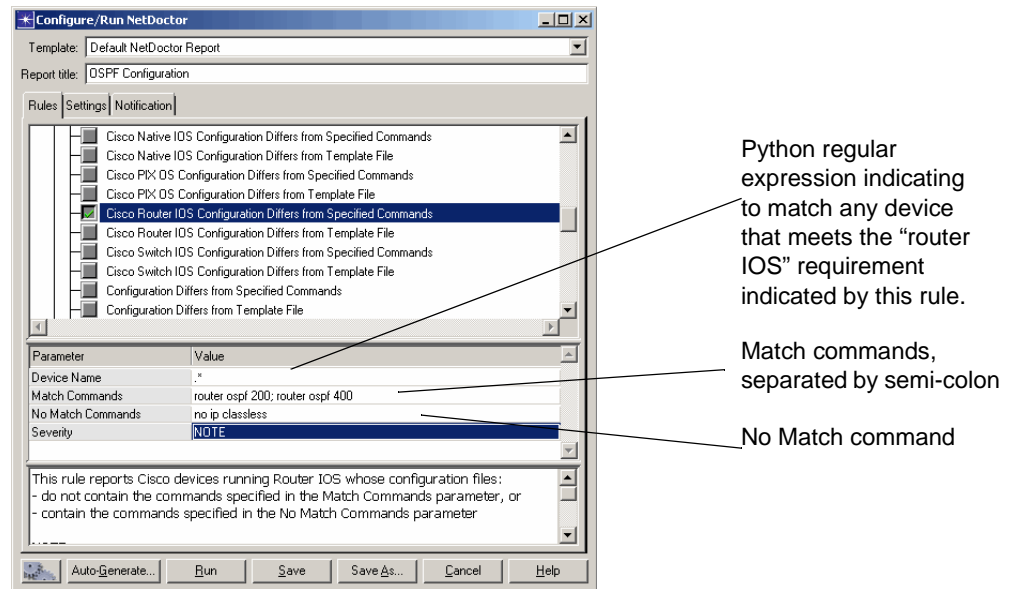
Parameter	Value
Match Commands	Specify a Python regular expression for command(s) that must be found in the device configuration file, separated by semi-colons.
No Match Commands	Specify a Python regular expression for command(s) that must not be found in the device configuration file, separated by semi-colons.
Severity	The severity of messages generated by this rule.
End of Table 3-11	

In the following example, we want to make sure that any Cisco router running IOS in our network has both “router ospf 200” and “router ospf 400” configured and does not have the “no ip classless” statement.

Figure 3-15 shows the configuration of the rule to give the desired result. We specify:

- Match Commands: “router ospf 200;router ospf 400”
 - The configuration file must contain both of these statements.
- No Match Commands: “no ip classless”
 - The configuration file must not contain this statement.

Figure 3-15 Match/No Match Commands



If any of the specified conditions are true, NetDoctor reports on the rule, as shown in Figure 3-16. Notice that the NetDoctor report shows us that router “c1700_Dallas” does not have the “router ospf 200” and “router ospf 400” configurations we expected. In other words, the configuration differed from the commands it should contain.

The router is correctly configured for “ip classless”, since we got no result for our No Match “no ip classless” test. This means that our configuration file did not contain the command “no ip classless”, which is as it should be.

Figure 3-16 Report on Match/No Match Commands

Organizational Policies: Cisco Router IOS Configuration Differs from Specified Commands [Concise] [Detail]

This rule reports Cisco devices running Router IOS whose configuration files:

- do not contain the commands specified in the Match Commands parameter, or
- contain the commands specified in the No Match Commands parameter

NOTE:

- Separate multiple commands with semi-colons in the rule parameters
- In addition to simple strings, the commands can be specified as Python regular expressions.

Severity

Tested Object

Match conditions not found

Tested: Configuration of: c1700_Dallas

NOTE
Configuration

This device does not meet the specified configuration.
Statements not found:

- o router ospf 200
- o router ospf 400

The generic version of the specified commands rules allow you to test devices, independent of vendor or operating system type. The rule’s name (“Configuration Differs from Specified Commands”, for example) does not contain vendor, operating system, or OSI layer specification. The parameters for these rules allow you to specify commands for Layer 2 and Layer 3 and are described in Table 3-12.

Table 3-12 Available Parameters for Generic Rules (Part 1 of 2)

Parameter	Value
Layer 2 Device Name	The Python regular expression used to decide which devices to check. Use “.” to match all names.
Layer 2 Match Commands	Specify a Python regular expression for command(s) that must be found in the Layer 2 configuration file, separated by semi-colons.
Layer 2 No Match Commands	Specify a Python regular expression for command(s) that must not be found in the Layer 2 configuration file, separated by semi-colons.
Layer 3 Device Name	The Python regular expression used to decide which devices to check. Use “.” to match all names.

Table 3-12 Available Parameters for Generic Rules (Part 2 of 2)

Parameter	Value
Layer 3 Match Commands	Specify a Python regular expression for command(s) that must be found in the Layer 3 configuration file, separated by semi-colons.
Layer 3 No Match Commands	Specify a Python regular expression for command(s) that must not be found in the Layer 3 configuration file, separated by semi-colons.
Severity	The severity of messages generated by this rule.
End of Table 3-12	

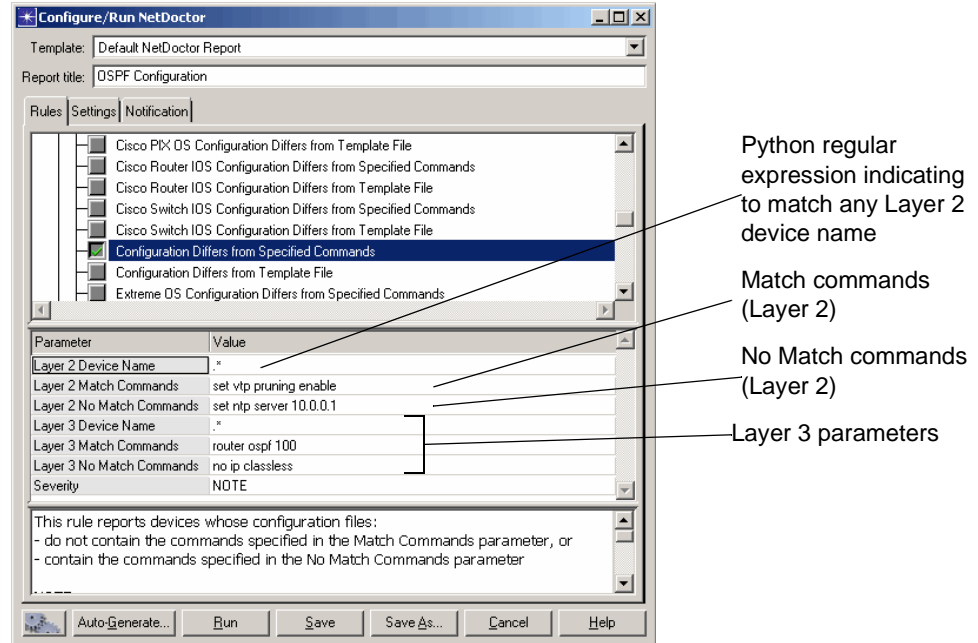
Example of a Specified Command Rule

In the following example, we want to make sure that any Layer 3 device in our network has both “router ospf 100” configured and does not have the “no ip classless” statement. Any Layer 2 device must have the “set vtp pruning enable” command and must not have the “set ntp server 10.0.0.1”. A generic specified commands rule is a good way to test all of the devices, both Layer 2 and Layer 3, at one time.

Figure 3-17 shows the configuration of the rule to give the desired result. We specify:

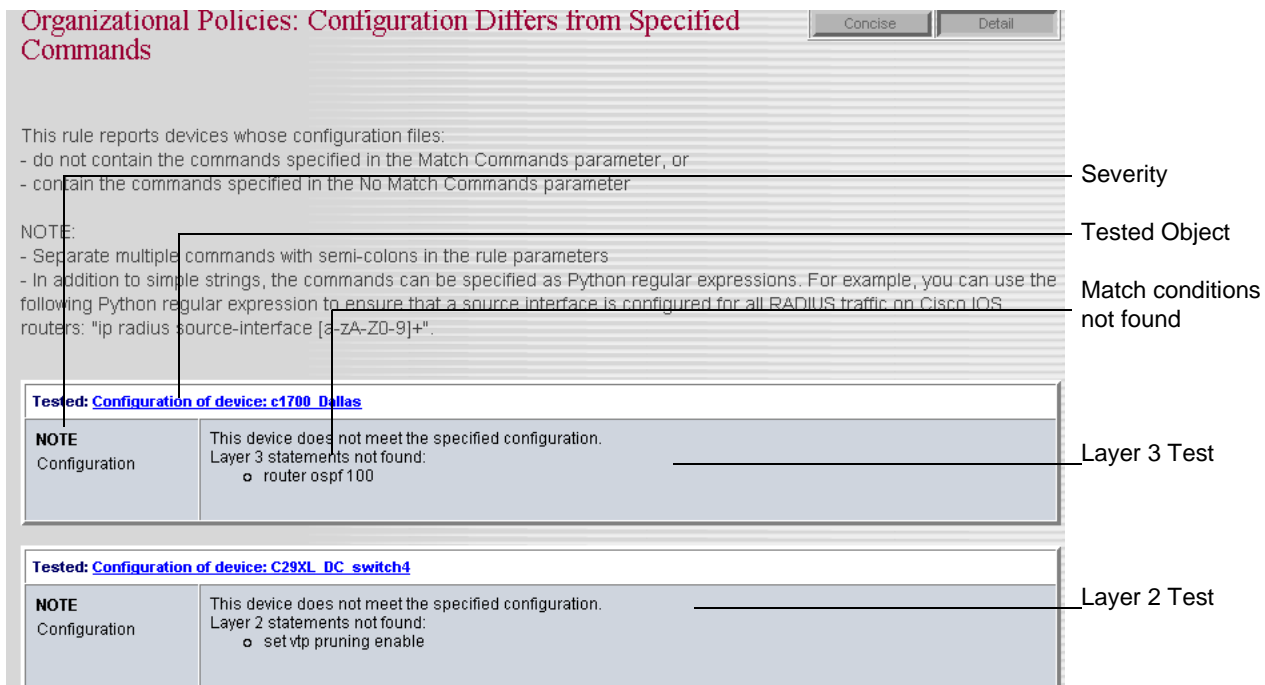
- Layer 2 Match Command: “set vtp pruning enable”
 - The Layer 2 configuration file must contain this statement.
- Layer 2 No Match Command: “set ntp server 10.0.0.1”
 - The Layer 2 configuration file must not contain this statement.
- Layer 3 Match Command: “router ospf 100”
 - The Layer 3 configuration file must contain this statement.
- Layer 3 No Match Command: “no ip classless”
 - The Layer 3 configuration file must not contain this statement.

Figure 3-17 Match/No Match Commands



If any of the specified conditions are true, NetDoctor reports on the rule, as shown in Figure 3-16. Notice that the NetDoctor report shows us that router “c1700_Dallas” does not have the “router ospf 100” configurations we expected. In other words, the configuration differed from the commands it should contain. The router is correctly configured for “ip classless”, since we got no result for our No Match “no ip classless” test. This means that our configuration file did not contain the command “no ip classless”, which is as it should be.

Figure 3-18 Report on Match/No Match Commands



Notice that the Layer 2 device does not have “set vtp pruning enable”, as we expected.

Another type of device in the network model is the multi-layer switch, which has both Layer 2 and Layer 3 components. The result of our test on a multi-layer switch is shown in Figure 3-19. In this case, if both Layer 2 and Layer 3 results are produced, the report is combined.

Figure 3-19 Multi-Layer Switch Test

Tested: Configuration of device: c5500 DC switch1	
NOTE Configuration	This device does not meet the specified configuration. Layer 2 statements found: <ul style="list-style-type: none"> o set ntp server 10.0.0.1 Layer 3 statements not found: <ul style="list-style-type: none"> o router ospf 100

This Layer 2 command is configured and matches.

This Layer 3 command does not match.

Using Template Files

There are several vendor-specific versions and one generic version of this rule.

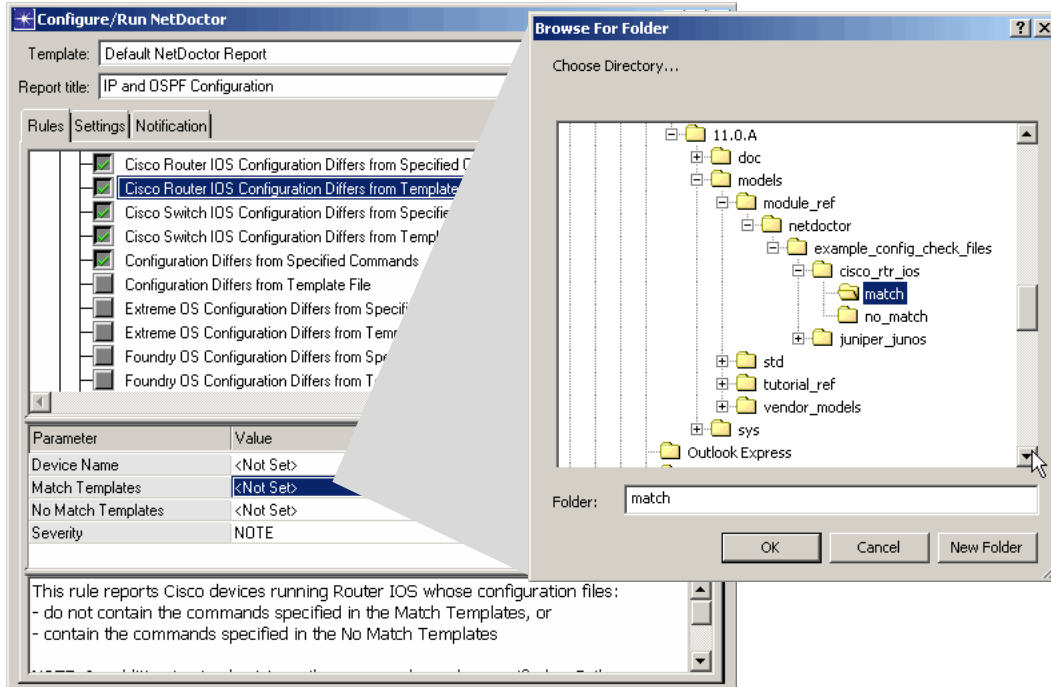
Vendor-Specific Rules The vendor-specific versions test devices that run a specific vendor’s operating system. This is indicated in the rule’s name (“Cisco Switch IOS Configuration Differs from Template File”, for example). The parameters for these rules are described in Table 3-13.

Table 3-13 Available Parameters for Vendor-Specific Rules

Parameter	Value
Device Name	The Python regular expression used to decide which devices to check. Use “.*” to match all names.
Match Template	Specify the folder that contains your match templates through the directory chooser.
No Match Template	Specify the folder that contains your no match templates through the directory chooser.
Severity	The severity of messages generated by this rule.
End of Table 3-13	

You specify the folder containing the template(s) through a directory chooser, as shown in Figure 3-20.

Figure 3-20 Match Templates



When you click on the value field next to "Match Templates", a directory chooser opens. Select the folder containing the match templates you wish to use.

Generic Rules The generic version of a template file rule allows you to test devices, independent of vendor or operating system type. The rule's name ("Configuration Differs from Template File", for example) does not contain vendor, operating system, or OSI layer specification. The parameters for this rule allow you to specify commands for Layer 2 and Layer 3 and are described in Table 3-14.

Table 3-14 Available Parameters for Generic Rules (Part 1 of 2)

Parameter	Value
Layer 2 Device Name	The Python regular expression used to decide which devices to check. Use "." to match all names.
Layer 2 Match Templates	Specify the folder that contains your Layer 2 match templates through the directory chooser.
Layer 2 No Match Templates	Specify the folder that contains your Layer 2 no match templates through the directory chooser.
Layer 3 Device Name	The Python regular expression used to decide which devices to check. Use "." to match all names.

Table 3-14 Available Parameters for Generic Rules (Part 2 of 2)

Parameter	Value
Layer 3 Match Commands	Specify the folder that contains your Layer 3 match templates through the directory chooser.
Layer 3 No Match Commands	Specify the folder that contains your Layer 3 no match templates through the directory chooser.
Severity	The severity of messages generated by this rule.
End of Table 3-14	

Template Specification File The folder you specify for match or no match templates can contain the template specification file (optional) and the template files. The template specification file allows you to apply groups of templates to groups of devices instead of applying all templates to all devices.

Note—If the directory does not contain a *template_file_spec.xml* file, the rule assumes all files in the directory are templates and that each device must match or not match all templates.

The template specification file, *template_file_spec.xml*, contains the listing of the templates to apply to devices whose configuration files have a certain command string. Figure 3-21 shows the anatomy of the template specification file.

Figure 3-21 Template Specification File

The group is "All IOS Routers"

Search for "hostname".

If "hostname" is found, apply the regular expression(s) in these template files to the device configuration file.

```
<?xml version="1.0" encoding="UTF-8"?>
<TemplateGroups>
  <Group name="All IOS Routers">
    <IncludeRegex>^hostname</IncludeRegex>
    <File>router_ios_match.txt</File>
    <File>router_ios_snmp_match.txt</File>
  </Group>
  <Group name="ACL 10">
    <IncludeRegex>^access-list 10</IncludeRegex>
    <File>router_ios_acl_10_match.txt</File>
  </Group>
</TemplateGroups>
```

Group

Referenced Template File(s)

The parameters of the *template_file_spec.xml* file are as follows:

- Group tags—defines the name of the template group and the start and finish of the group within the template file.

The *Group name* is used to identify the group, or command set, that a device matched in the NetDoctor report. For example, the output might read, Layer 3 statements not found for “All IOS Routers”. The group name is listed between double quotes in the output.

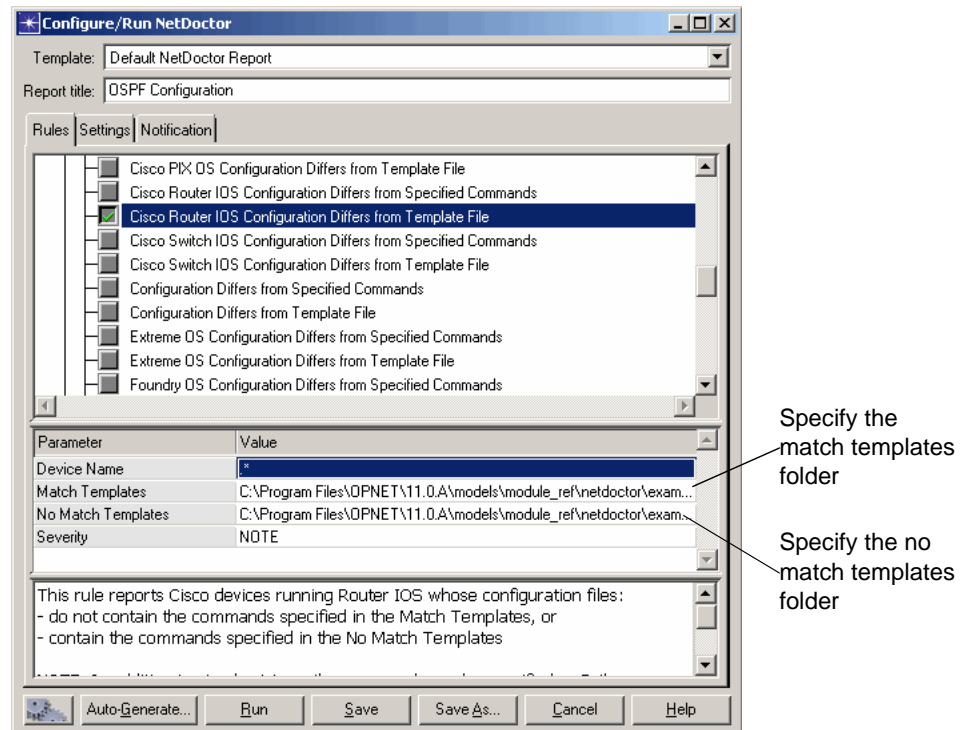
Note—If a device configuration file matches more than one group, it is tested for each group. In the final NetDoctor report, the rule reports inconsistencies for each group distinctly.

- IncludeRegEx—defines the regular expression, that is searched for in the configuration file to match it to the group.
- File—defines the template(s) to apply to devices matching the regular expression.

WARNING—Although you can edit and create template specification files in any text editor, the name must always be *template_file_spec.xml*, as this is how NetDoctor rules identify it. The *template_file_spec.xml* file must be in the same directory as the templates it references. If *template_file_spec.xml* is not found, the device configuration file is checked against all templates in the directory.

Template File Rule Example Let’s take a look at an example in which we want to use the rule “Cisco Router IOS Configuration Differs from Template File”.

Figure 3-22 Template File Rule



Each folder contains the templates and the *template_file_spec.xml* file, as shown in Figure 3-23:

Figure 3-23 Folder Contents

Name ▲	Size	Type	
router_ios_acl_10_match	1 KB	Text Docu...	Match folder contents
router_ios_match	1 KB	Text Docu...	
router_ios_snmp_match	1 KB	Text Docu...	
template_file_spec	1 KB	XML Docum...	

Name ▲	Size	Type	
router_ios_no_match	1 KB	Text Docu...	No Match folder contents
template_file_spec	1 KB	XML Docum...	

The *template_file_spec.xml* file specifies the conditions under which certain templates are applied.

Figure 3-24 Template_file_spec.xml File

```
<?xml version="1.0" encoding="UTF-8"?>
<TemplateGroups>
  <Group name="All IOS Routers">
    <IncludeRegex>^hostname</IncludeRegex>
    <File>router_ios_match.txt</File>
    <File>router_ios_snmp_match.txt</File>
  </Group>
  <Group name="ACL 10">
    <IncludeRegex>^access-list 10</IncludeRegex>
    <File>router_ios_acl_10_match.txt</File>
  </Group>
</TemplateGroups>
```

If "hostname" is found...
then apply these templates.

If "hostname" is found in the device configuration file, the *router_ios_match.txt* and *router_ios_snmp_match.txt* templates are applied to the device configuration file. The device configuration file must match the conditions in each template shown in Figure 3-25 or it is reported as an inconsistency in the rule output.

Figure 3-25 Match Templates for "hostname"

router_ios_match.txt

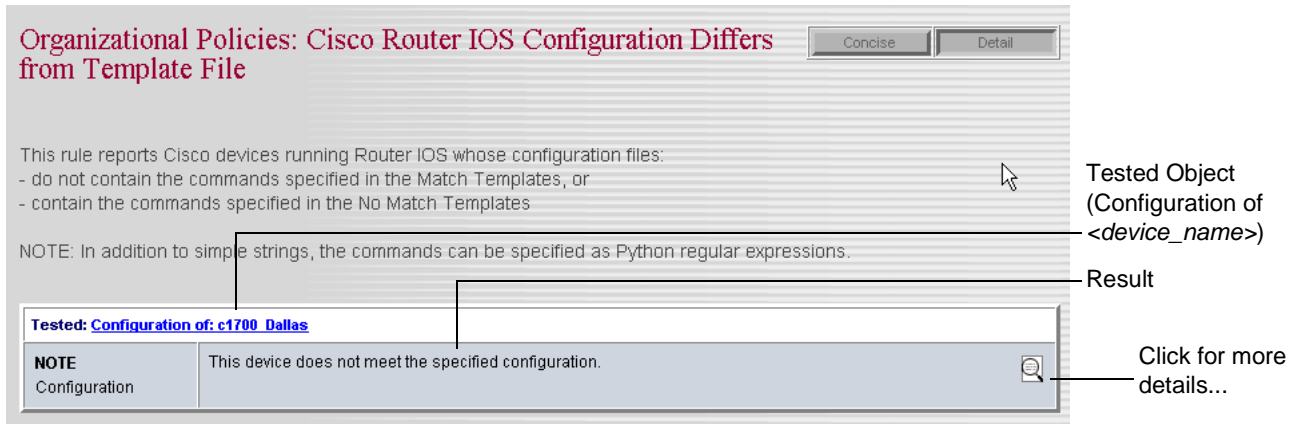
```
^service password-encryption
^(radius source-interface ){[a-zA-Z0-9]}+
^logging on
^radius server-host 10.1.1.1
^(interface Loopback99){\s}+(ip address 10.0.0.1 255.255.255.255){\s}+(ip pim sparse-mode)
```

router_ios_snmp_match.txt

```
^ip access-list 11
^ip access-list 12
^snmp-server community $3cr3t rw 11
^snmp-server community vi3w0nly r 12
^snmp-server enable traps snmp
^snmp-server enable traps envmon
^snmp-server host 10.12.18.192 trapc0mm snmp envmon
```

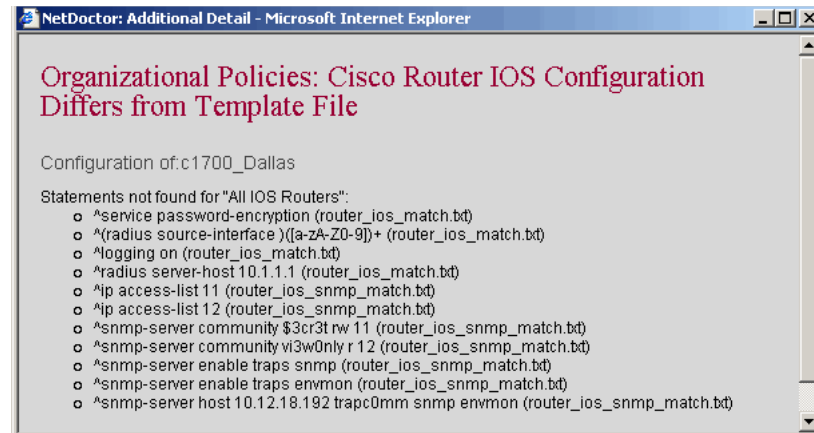
The NetDoctor report that results from our example shows that we have devices in our network model that do not comply with our match and no match rules.

Figure 3-26 NetDoctor Results for Template File Check



If we expand the details on this rule result, notice the line-by-line breakdown of our device configuration file check by the template:

Figure 3-27 Detail of Rule Result



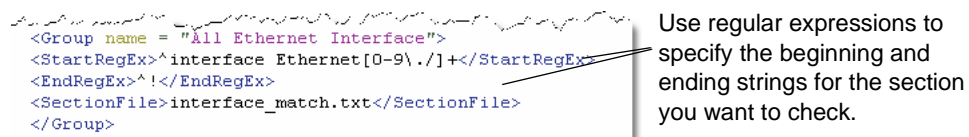
The preceding examples show the Match templates. The No Match templates work the same way.

Rules for Configuration File Sections

You can specify Match or No Match templates for commands in specific sections of your configuration files. For example, you may want to check Serial ports in your network model for protocol-specific information, such as the subinterfaces configured for Frame Relay or ATM.

Using the *template_spec_file.xml*, specify the starting and ending regular expressions to match strings that begin and end a section you want to check in a configuration file (see Figure 3-28).

Figure 3-28 Starting and Ending Sections in the Template Specification File



```
<Group name = "All Ethernet Interface">
<StartRegEx>^interface Ethernet[0-9\\.\\.]+</StartRegEx>
<EndRegEx>^!</EndRegEx>
<SectionFile>interface_match.txt</SectionFile>
</Group>
```

Use regular expressions to specify the beginning and ending strings for the section you want to check.

For this example, NetDoctor checks any Ethernet interface sections in the configuration file against the *interface_match.txt* file. This provides a way to check subsets of the configuration file commands.

Viewing NetDoctor Reports

After each Netdoctor run, a Web Report or an MS Word Report automatically displays; the XML file containing report data is saved to a specific location. NetDoctor keeps a configurable number of previous reports generated for each template in case you want to view any of them later. Use the preference `netdoctor.keep_prior_reports_count` to set the number of previous reports you would like to retain.

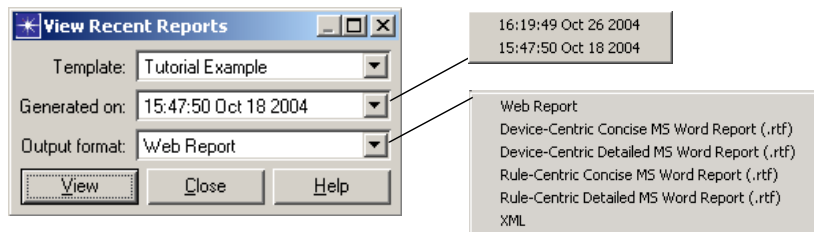
You can view a previous report generated for a template in the original output format or in a new output format. Follow Procedure 3-6 to view a NetDoctor report.

Note—You can view a report in a different format without re-running NetDoctor (see Procedure 3-6).

Procedure 3-6 Viewing a Previous Report

- 1 Choose NetDoctor > View Recent NetDoctor Reports.
 - ➔ The View Recent Reports dialog box opens.

Figure 3-29 View Recent NetDoctor Reports Dialog Box



- 2 In the Template list, select the template for the previous reports you want to view.
- 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, MS Word Report (in any of the four MS Word formats), or XML.
- 5 Click View.
 - ➔ The specified report appears in the output format you selected.

Note—If you choose XML, a window opens to indicate where the XML report format is saved.

End of Procedure 3-6

Report Formats

NetDoctor generates a Web Report or an MS Word report in the following formats:

- Device-Centric Concise
- Device-Centric Detailed
- Rule-Centric Concise
- Rule-Centric Detailed

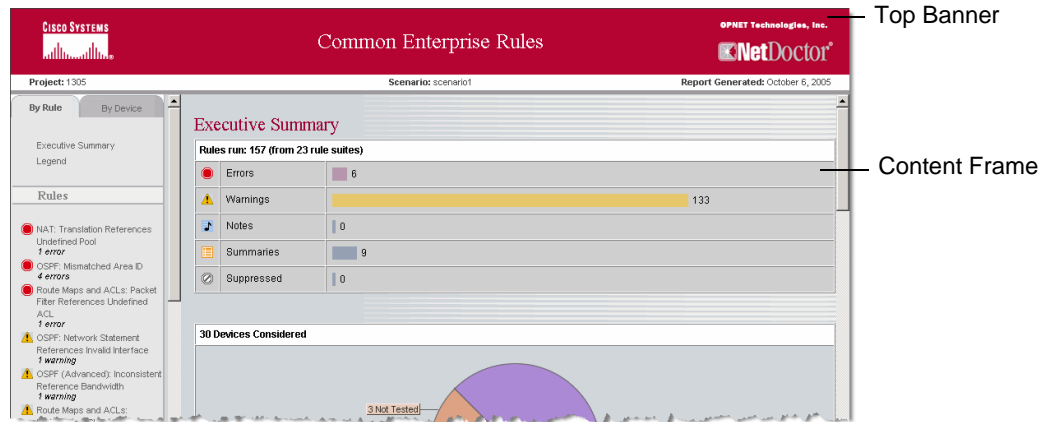
Web Report

The Web Report includes all report formats in one report. Figure 3-32 shows a NetDoctor Web Report. The report consists of a top banner, a tabbed navigation frame, and a content frame.

Figure 3-30 Web Report

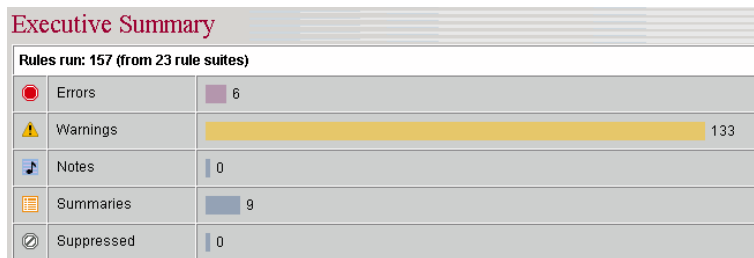
Tabbed Navigation Frame:

- By Rule
- By Device



Executive Summary The Executive Summary displays statistics about the rules run and devices tested. The first bar graph has a summary of all the messages generated (see Figure 3-31).

Figure 3-31 Rules Run in Bar Graph



Executive Summary By Rule or By Device Select the “By Rule” or “By Device” tab in the navigation frame to view rule-centric or device-centric information. The Executive Summary is the default display for both tabs. If you scroll down, you can see summaries based on rules or devices (see Figure 3-33).

Figure 3-32 Executive Summary: By Rule or By Device

The screenshot shows the NetDoctor interface for 'Common Enterprise Rules'. The 'By Rule' tab is selected in the left navigation pane. The main content area is divided into three sections: Errors, Warnings, and Summaries.

Suite	Rule	Messages
NAT	Translation References Undefined Pool	1 error
OSPF	Mismatched Area ID	4 errors
Route Maps and ACLs	PacketFilter References Undefined ACL	1 error

Suite	Rule	Messages
OSPF	Network Statement References Invalid Interface	1 warning
OSPF (Advanced)	Inconsistent Reference Bandwidth	1 warning
Route Maps and ACLs	Ineffective ACL	1 warning
Route Maps and ACLs	Redundant Statement in ACL	4 warnings
Route Maps and ACLs	Redundant Statement in Route Map	1 warning
SNMP	Community Uses Weak Name	56 warnings
SNMP	Community Without ACL	57 warnings
System Logging	Logging Disabled	12 warnings

Suite	Rule
Administration	Device OS Versions
Administration	Interfaces

Select the “By Rule” tab and scroll down in Executive Summary to view rule-centric information.

The screenshot shows the NetDoctor interface for 'Common Enterprise Rules'. The 'By Device' tab is selected in the left navigation pane. The main content area displays a table of error and warning counts for various devices.

Devices	Messages
Atlanta	1 error, 7 warnings
ATT	2 warnings
Boston_Bkup_IDC	6 warnings
C29XL1	4 warnings
C29XL3	4 warnings
C29XL4	4 warnings
C55Co1	7 warnings
C55Co2	10 warnings
C55Co3	8 warnings
C55Co4	6 warnings
C8509_SUP	6 warnings
Dallas	2 errors, 6 warnings
DC	3 warnings
Euro_Partner	5 warnings
FR_Cloud	3 warnings
Genuity	5 warnings
Houston	7 warnings
LA	1 error, 7 warnings
London	5 warnings
NY_Pri_IDC	3 errors, 5 warnings

Select the “By Device” tab and scroll down in Executive summary to view device-centric information.

Viewing Specific Web Report Information Select a rule or device listed by name in the Rules or Devices section of the navigation frame. The specific information about the rule or device displays in the content frame (see Figure 3-33 and Figure 3-34).

Rule-Centric Concise or Detailed Information Use the “Concise” or “Detailed” buttons in the upper right corner of the content frame to display the message information for each violated a rule (see Figure 3-33).

Figure 3-33 Rule-Centric Display

Select a rule.

The screenshot shows a navigation pane on the left with a 'Rules' section. A red circle highlights the rule 'OSPF: Mismatched Area ID' which has '4 errors'. The main content area shows the report for this rule in 'Concise' mode, listing four errors: Dallas [Tunnel0] and NY_Pri_IDC [Tunnel2], Dallas [Tunnel1] and SanDiego [Tunnel1], LA [Tunnel0] and NY_Pri_IDC [Tunnel1], and NY_Pri_IDC [Tunnel0] and SanDiego [Tunnel0].

Executive Summary
Legend

Rules

- NAT: Translation Reference Undefined Pool
1 error
- OSPF: Mismatched Area ID
4 errors**
- Route Maps and ACLs: Packet Filter References Undefined ACL
1 error
- OSPF: Network Statement References Invalid Interface
1 warning
- OSPF (Advanced): Inconsistent Reference Bandwidth
4 warnings

OSPF: Mismatched Area ID Concise Detail

All peer interfaces running OSPF must agree on the OSPF area ID.

Detected: 4 errors

- Dallas [Tunnel0] and NY_Pri_IDC [Tunnel2]
- Dallas [Tunnel1] and SanDiego [Tunnel1]
- LA [Tunnel0] and NY_Pri_IDC [Tunnel1]
- NY_Pri_IDC [Tunnel0] and SanDiego [Tunnel0]

Select “Concise” or “Detailed”.

Concise information about all the messages generated by the rule.

OSPF: Mismatched Area ID Concise Detail

All peer interfaces running OSPF must agree on the OSPF area ID.

Tested: Area IDs of 2 interfaces.

ERROR Configuration	The interfaces in this subnetwork are not configured to operate in the same area. The following interfaces are configured to operate in area 0.0.0.0: <ul style="list-style-type: none">NY_Pri_IDC [Tunnel2] The following interfaces are configured to operate in area 0.0.0.3: <ul style="list-style-type: none">Dallas [Tunnel0] Interfaces in different areas will not form adjacencies with each other.
-------------------------------	--

Detailed information for each message.

ERROR Configuration	The interfaces in this subnetwork are not configured to operate in the same area. The following interfaces are configured to operate in area 0.0.0.3: <ul style="list-style-type: none">Dallas [Tunnel1] The following interfaces are configured to operate in area 0.0.0.2: <ul style="list-style-type: none">SanDiego [Tunnel1] Interfaces in different areas will not form adjacencies with each other.
-------------------------------	--

ERROR Configuration	The interfaces in this subnetwork are not configured to operate in the same area. The following interfaces are configured to operate in area 0.0.0.0: <ul style="list-style-type: none">NY_Pri_IDC [Tunnel1] The following interfaces are configured to operate in area 0.0.0.2: <ul style="list-style-type: none">LA [Tunnel0] Interfaces in different areas will not form adjacencies with each other.
-------------------------------	--

Device-Centric Concise or Detailed Information Use the “Collapse All” or “Expand All” buttons to display information about each of the rules that the device violated. You can toggle between concise or detailed information for each rule by selecting the expand icon to the left of the rule name in the content frame (see Figure 3-34).

Figure 3-34 Device-Centric Display

Select a device.

Executive Summary
Legend

Devices

- Atlanta
1 error, 7 warnings
- Dallas
2 errors, 6 warnings
- LA
1 error, 7 warnings
- NY_Pri_IDC
3 errors, 5 warnings
- pixfirewall
1 error
- SanDiego
2 errors, 9 warnings
- ATT
2 warnings

Dallas (Cisco 3640) Collapse All Expand All
2 errors, 6 warnings

- OSPF: Mismatched Area ID 2 errors
- OSPF (Advanced): Inconsistent Reference Bandwidth 1 warning
- SNMP: Community Without ACL 2 warnings
- SNMP: Community Uses Weak Name 2 warnings
- System Logging: Logging Disabled 1 warning

Dallas (Cisco 3640) Collapse All Expand All
2 errors, 6 warnings

OSPF: Mismatched Area ID 2 errors

All peer interfaces running OSPF must agree on the OSPF area ID.

ERROR Configuration	The interfaces in this subnetwork are not configured to operate in the same area. The following interfaces are configured to operate in area 0.0.0.0: o NY_Pri_IDC[Tunnel2] The following interfaces are configured to operate in area 0.0.0.3: o Dallas[Tunnel0] Interfaces in different areas will not form adjacencies with each other.
ERROR Configuration	The interfaces in this subnetwork are not configured to operate in the same area. The following interfaces are configured to operate in area 0.0.0.3: o Dallas[Tunnel1] The following interfaces are configured to operate in area 0.0.0.2: o SanDiego[Tunnel1] Interfaces in different areas will not form adjacencies with each other.

Select “Collapse All” or “Expand All”.

Concise list of all the rules the device violated.

Toggle expand icon to display detailed or concise information.

Shows all messages for each rule the device violated.

Microsoft Word Report

Figure 3-35 shows a NetDoctor report in Microsoft Word format. The first page is a title page that includes the information that appears in the title banner on the web report. Navigation links to the report content appears on the second page in the table of contents. The executive summary provides a synopsis of the number of rules run, the number of messages suppressed, and the errors, warnings, and notes generated by the NetDoctor run. The rest of the report consists of the information from the rules pages and appendices.

Figure 3-35 NetDoctor Report in Microsoft Word



Comparing Report Formats

NetDoctor uses the same XML to generate all report formats, so they include the same content. The Web Report is easier to navigate; the MS Word report is easier to edit and print. See Table 3-15.

Table 3-15 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
Rule/Device Tab	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	Rule sections (rule-centric versions only)
The messages reported organized by device	Content frame	Device sections (device-centric versions only)
Additional data	Appendices ¹ (a list of available appendices is at the bottom of the navigation frame, the appendices appear in the content frame)	Appendices
End of Table 3-15		

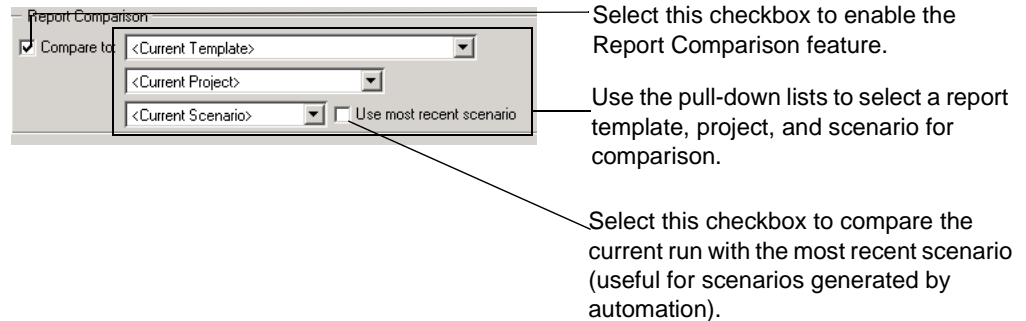
1. Appendices are listed in the Navigation frame. The contents of an appendix appear in the Content frame.

Comparing NetDoctor Reports

NetDoctor's Report Comparison feature allows you to compare rule output between a current and previous run. When you configure Report Comparison and NetDoctor Notification, you can automatically publish or send critical information about new problems in your network. **Configuring Report Comparison**

Access the Report Comparison configuration options from the Settings tab of the Configure/Run NetDoctor dialog box. Select the "Compare to" checkbox to enable Report Comparison. See Figure 3-36 for Report Comparison options.

Figure 3-36 Report Comparison Options



Running Report Comparison

When you run NetDoctor with Report Comparison enabled, NetDoctor compares the results of running the template in use for the existing scenario with the results of the specified template, project, and scenario. The report generated by NetDoctor highlights changes between the rule output of the current run with the rule output of the specified report.

With the default <Current...> selections in the Report Comparison section, you compare the current NetDoctor run using the current template on the current scenario with the most recent report generated using the current template and scenario.

The "Use most recent scenario" checkbox is useful for comparing reports generated from scenarios created by automation.

Report Comparison and Automation

There are two ways to select scenarios when you run NetDoctor with Report Comparison enabled:

"Use most recent scenario" checkbox selected: Choose from a list of scenario baseline names available in the drop-down list to the left of the checkbox (without timestamps). One baseline name for the scenario is listed, even though multiple scenarios of the same project may exist.

“Use most recent scenario” checkbox cleared: Choose from a list of available scenarios. This list will include each timestamped scenario.

See Table 3-16 for a summary of the Report Comparison options using the <Current...> settings with automation.

¹ **Table 3-16 Running NetDoctor with Automation**

Automatically created scenarios?	“Use most recent scenario” selected?	Description of report output with the <Current...> settings:
No	No	Shows differences between the current and most recent previous report.
No	Yes	Same as above.
Yes	No	In most cases, NetDoctor will not find a previous report. This is not recommended.
Yes	Yes	Shows differences between the current report and most recent report generated using the most recent automatically created scenario.
End of Table 3-16		

Analyzing a Comparison Report

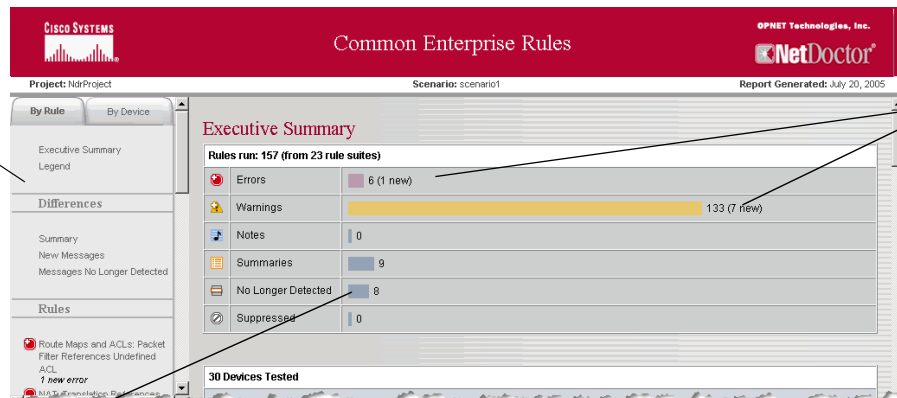
NetDoctor highlights any differences throughout the report. The Differences section in the left navigation frame has links to a Differences Summary, New Messages, and Messages No Longer Detected. These three pages show just differences. Figure 3-37 shows the web version of a comparison report.

Figure 3-37 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.

Modifying NetDoctor Reports

To modify NetDoctor reports, you can suppress messages or configure Global Options.

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.

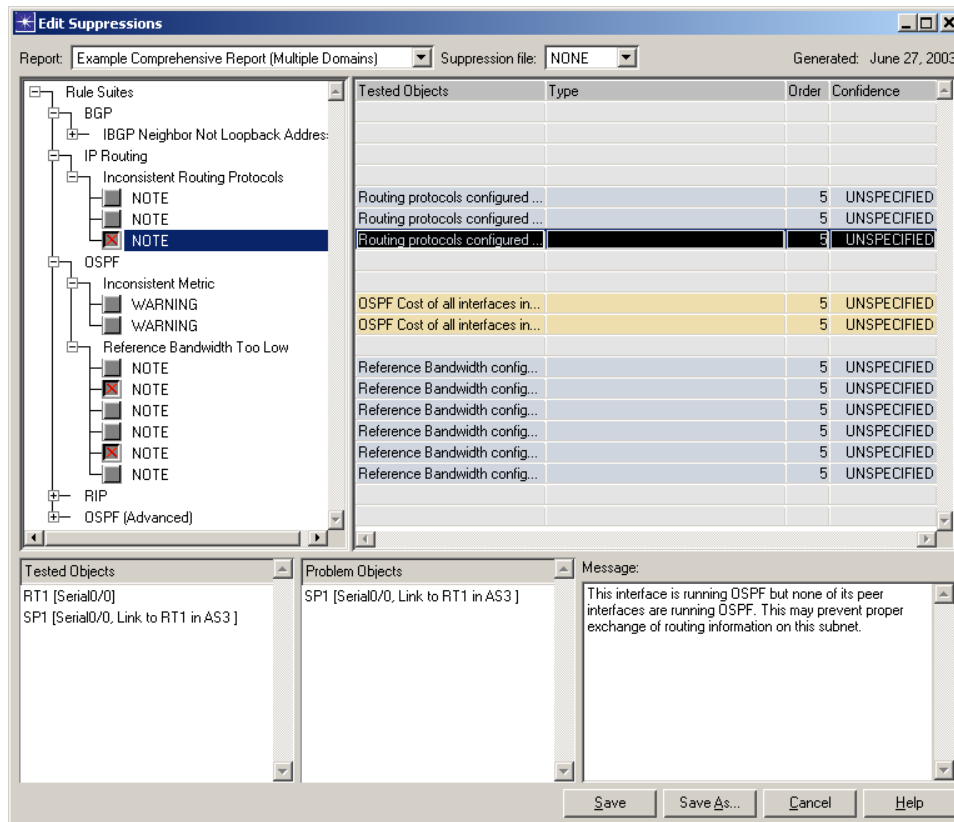
You can use message suppression when you want NetDoctor to check a network against a rule for all objects in the network except a selected few. If you do not want NetDoctor to report on a rule for any of the objects in the network, do not use message suppression. Instead, omit the rule.

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 3-7 Creating a Suppression File

- 1 Run NetDoctor to identify the messages that you want to suppress in subsequent NetDoctor reports.
- 2 Choose NetDoctor > Suppress Messages.
 - ➔ The Edit Suppressions dialog box appears.

Figure 3-38 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 3-7

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.

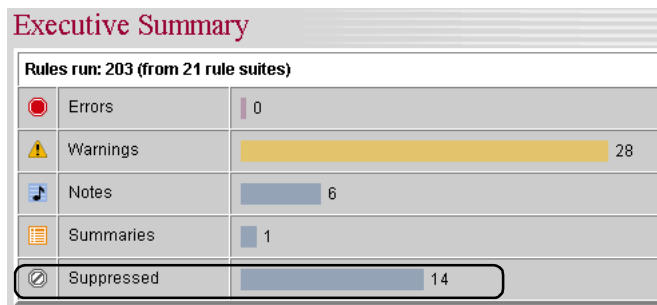
Procedure 3-8 Applying a Suppression File to a Template

- 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 3-39 Suppressed Message Count



End of Procedure 3-8

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 3-40 NetDoctor Options Dialog Box

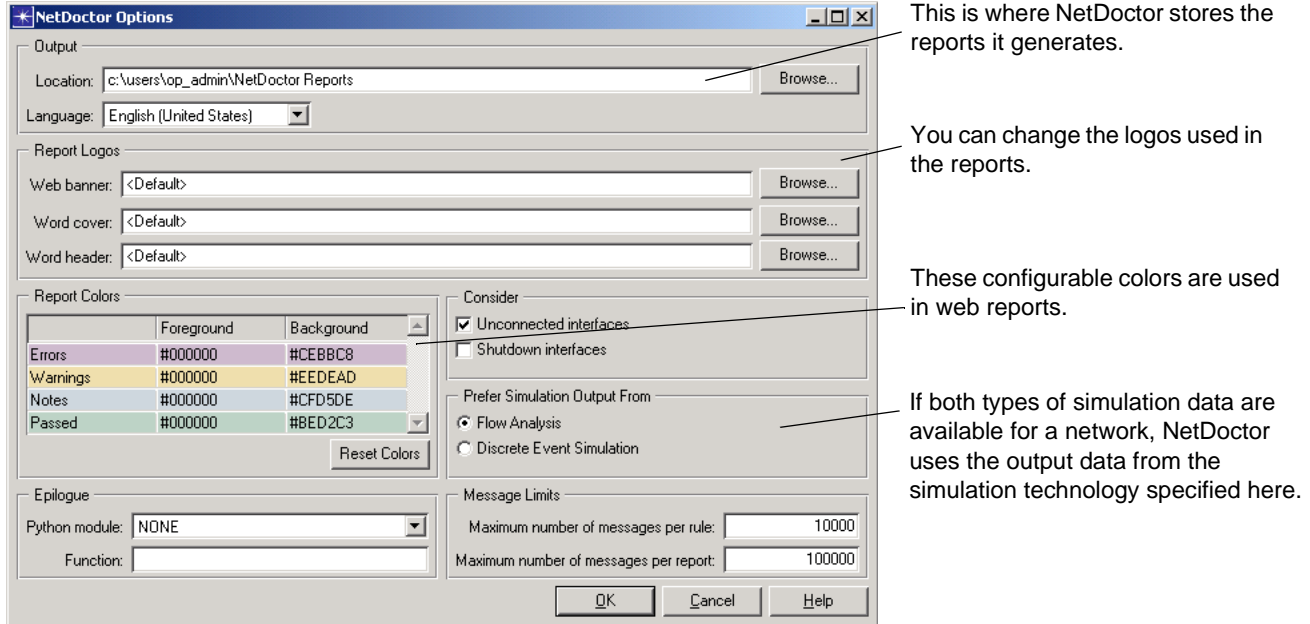


Table 3-17 NetDoctor Options (Part 1 of 2)

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 3-17 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-4-26.
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 3-17	

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, a device in the network may have security policies configured that are designed to restrict access to all but authorized users. NetDoctor analyzes your network and provides information to let you know if your security configuration will work correctly using security demands. 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.

NetDoctor Security Operations

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. The NetDoctor security analysis verifies that the policies configured in the network implement the access requirements and access restrictions you need using access control lists, route filters, and so on. Because of this, the network topologies created using Device Configuration Import (DCI) and VNE Server import are excellent baselines for security analyses.

Security Demands

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.

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-3-54.

- 2) Visualize the configured security demands. See Visualizing Network Security Configuration on page ND-3-58.
- 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

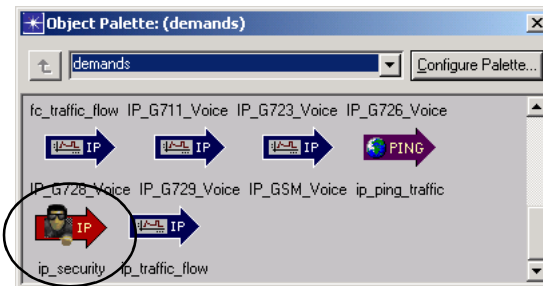
Validating security policies against actual network configuration involves creating security demands in the network and running simulations to verify the intended behavior of the demand. You can configure permit and deny security demands that represent end-to-end requirements to test the security configuration 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 3-9 Creating Security Demands

- 1 Open the “demands” object palette:

Figure 3-41 The Demands Object Palette



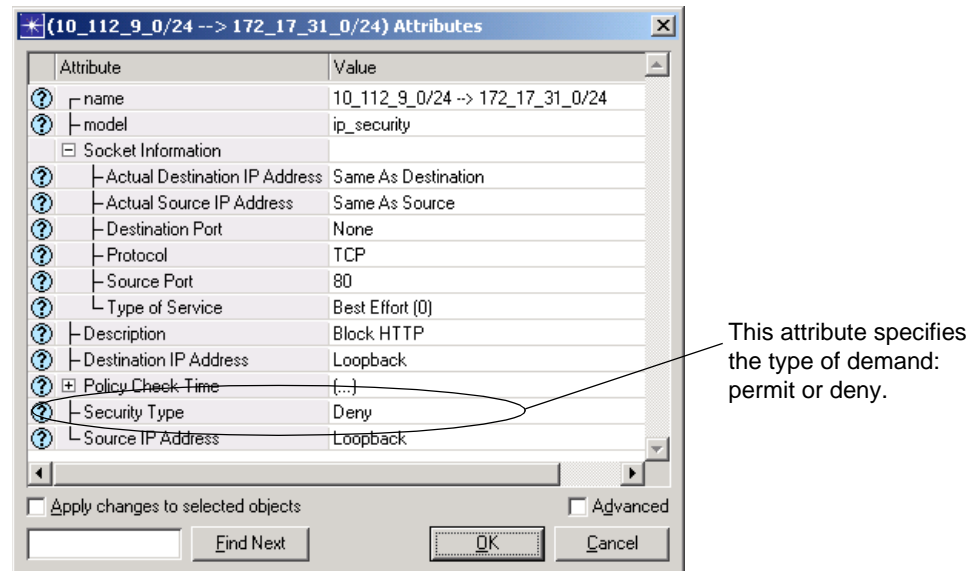
- 2 Click on the ip_security demand (see Figure 3-41) in the object palette.
- 3 In the Project Editor workspace, click on the source node of the security demand, then click on the destination node.
 - ➔ A new permit security demand appears in the workspace. Security demands are permit demands by default 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 3-9

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 3-42 shows the configurable attributes on a security demand.

Figure 3-42 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 3-10 Creating Multiple Security Demands Simultaneously

- 1 Choose NetDoctor > Security > Demands > Create.
 - ➔ The Create Security Demands dialog box displays.

Figure 3-43 Create Security Demands Dialog Box

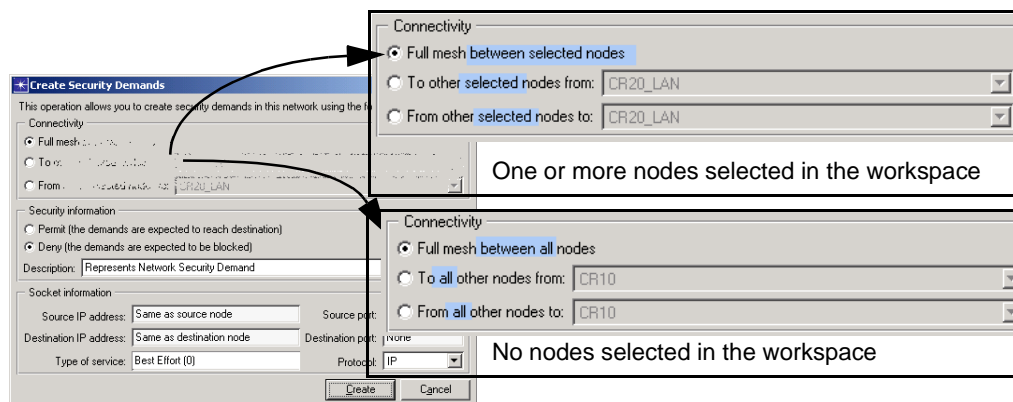
- 2 Under Connectivity, specify the nodes to use as demand endpoints:
 - Full-mesh between all nodes—creates two demands (one in each direction) between each pair of nodes in the network
 - To other nodes from:—creates a demand between the specified node and every other node in the network, with this 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 3-10

You can repeat Procedure 3-10 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 3-44 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 3-44 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 3-45 shows part of a file used to configure security demands.

Figure 3-45 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
```

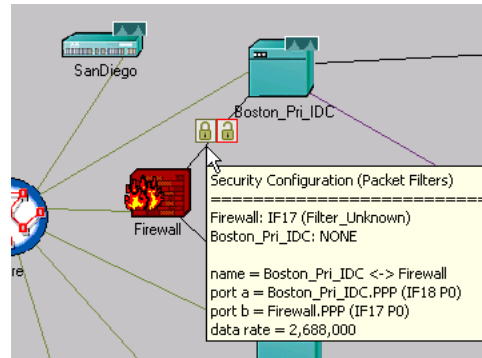
Visualizing Network Security Configuration

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 3-11 Viewing Security Configuration in the Workspace

- 1 Choose View > 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 (see Figure 3-46).

Figure 3-46 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 3-11

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

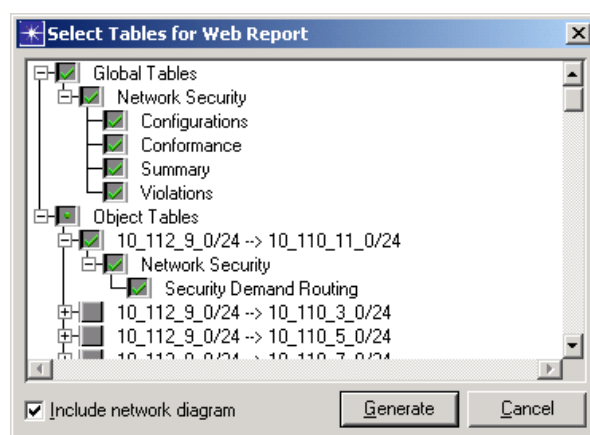
Both reports are available in a unified web report that can be launched from the NetDoctor > Security > Reports menu.

Procedure 3-12 Viewing Security Reports

- 1 Choose NetDoctor > Security > Reports > Generate Web Report...

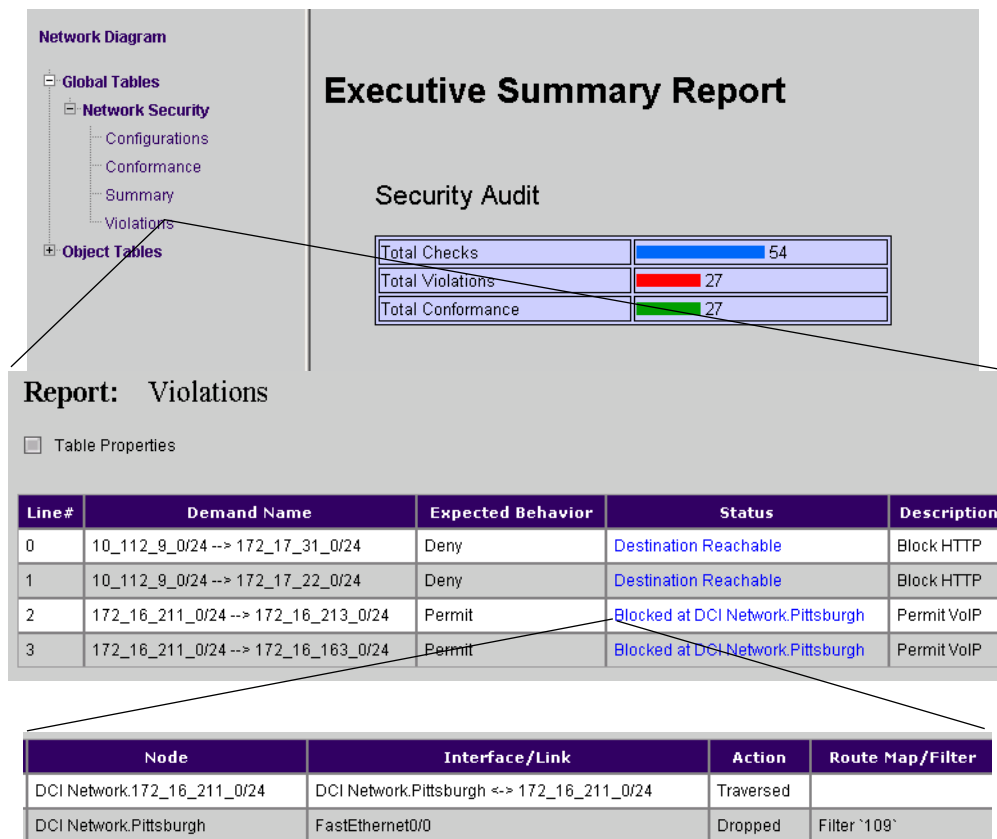
➔ The Select Tables for Web Report dialog box comes up.

Figure 3-47 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 3-48 Network Security Web Report



Line#	Demand Name	Expected Behavior	Status	Description
0	10_112_9_0/24 --> 172_17_31_0/24	Deny	Destination Reachable	Block HTTP
1	10_112_9_0/24 --> 172_17_22_0/24	Deny	Destination Reachable	Block HTTP
2	172_16_211_0/24 --> 172_16_213_0/24	Permit	Blocked at DCI Network.Pittsburgh	Permit VoIP
3	172_16_211_0/24 --> 172_16_163_0/24	Permit	Blocked at DCI Network.Pittsburgh	Permit VoIP

Node	Interface/Link	Action	Route Map/Filter
DCI Network:172_16_211_0/24	DCI Network.Pittsburgh <-> 172_16_211_0/24	Traversed	
DCI Network.Pittsburgh	FastEthernet0/0	Dropped	Filter '109'

- 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.
- Browse through the reason for success or failure of security checks using the Status link available for each security demand report.

End of Procedure 3-12

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

Symbols

.Configure/Run NetDoctor Dialog Box
Settings Tab, [ND-3-11](#)

A

A Web Comparison Report, [ND-3-47](#)
Analyzing a Comparison Report, [ND-3-47](#)
Applying a Suppression File to a Template, [ND-3-50](#)
Auto-Generate a Report Template, [ND-3-6](#)
Auto-Generate Report Template Dialog Box, [ND-3-6](#)
Auto-Generating a Report Template, [ND-3-6](#)
Available Parameters for Generic Rules (Part 1 of 2),
[ND-3-29](#), [ND-3-33](#)
Available Parameters for Vendor-Specific Rules, [ND-3-27](#),
[ND-3-32](#)
available rule suites, [ND-1-5](#)
Available Templates, [ND-3-7](#)

C

Comparing NetDoctor Reports, [ND-3-46](#)
Configure/Run NetDoctor, [ND-3-3](#)
Configure/Run NetDoctor Dialog Box
Rules Tab, [ND-3-3](#)
Settings (Part 1 of 2), [ND-3-11](#)
Configure/Run NetDoctor dialog box, [ND-3-3](#), [ND-3-11](#)
Configuring Global Options, [ND-3-51](#)
Configuring Report Comparison, [ND-3-46](#)
Configuring Security Demands, [ND-3-54](#)
Create Security Demands Dialog Box, [ND-3-56](#)
Create Security Demands dialog box, [ND-3-56](#)
Create Security Demands Dialog Box—With and Without
Selection, [ND-3-57](#)
Creating a Report Template Manually, [ND-3-8](#)
Creating a Suppression File, [ND-3-48](#)
Creating Multiple Security Demands Simultaneously, [ND-3-55](#)
Creating Security Demands, [ND-3-54](#)

D

Detail of Rule Result, [ND-3-37](#)
Device Configuration File Validation, [ND-3-27](#)

E

Edit Suppressions Dialog Box, [ND-3-49](#)
Edit Suppressions dialog box, [ND-3-49](#)
Email Notification Parameters (Part 1 of 2), [ND-3-15](#)
Example of a Specified Command Rule, [ND-3-30](#)

F

Folder Contents, [ND-3-36](#)

G

Generating a Report From a Template, [ND-3-9](#)
Generating Security Reports, [ND-3-60](#)
Generic Rules, [ND-3-33](#)

L

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

M

Manually Create a Report Template, [ND-3-7](#)
Match Templates, [ND-3-33](#)
Match Templates for “^hostname”, [ND-3-36](#)
Match/No Match Commands, [ND-3-28](#), [ND-3-31](#)
messages
suppressing, [ND-3-48](#)
viewing the suppressed message count, [ND-3-50](#)
Microsoft Word Report, [ND-3-44](#)
Microsoft Word report, [ND-3-44](#)
Modeling Network Security, [ND-3-53](#)
Multi-Layer Switch Test, [ND-3-32](#)

N

NetDoctor
adding and activating a license, [ND-2-1](#)
creating a template, [ND-3-8](#)
understanding the workflow, [ND-1-4](#)
using, [ND-3-1](#)
NetDoctor administration, [ND-2-1](#)
NetDoctor license
adding and activating, [ND-2-1](#) to [ND-2-2](#)
NetDoctor Menu, [ND-2-2](#)
NetDoctor menu, [ND-2-2](#) to [ND-2-3](#)
NetDoctor Menu Operations (Part 1 of 2), [ND-2-3](#)
NetDoctor Notifications, [ND-3-17](#)
NetDoctor options
setting, [ND-3-51](#)
NetDoctor Options (Part 1 of 2), [ND-3-51](#)
NetDoctor Options Dialog Box, [ND-3-51](#)
NetDoctor quick start, [ND-3-4](#)
NetDoctor report
running, [ND-3-9](#)
NetDoctor Report in Microsoft Word, [ND-3-44](#)
NetDoctor report organization, [ND-3-45](#)
NetDoctor Report Organization , [ND-3-45](#)
NetDoctor Reports dialog box
viewing recent, [ND-3-39](#)
NetDoctor Results for Template File Check, [ND-3-37](#)
NetDoctor tutorial, [ND-2-2](#)

- opening, [ND-2-3](#)
- using, [ND-2-2](#)
- NetDoctor User Guide
 - contents, [ND-1-6](#)
 - organization, [ND-1-6](#)
- NetDoctor Web Report
 - Sample Output, [ND-3-5](#)
- NetDoctor administration, [ND-2-1](#)
- network security
 - generating the Web report, [ND-3-61](#)
 - modeling, [ND-3-53](#)
 - visualizing the network configuration, [ND-3-58](#) to [ND-3-59](#)
- Network Security Configuration Visualization, [ND-3-59](#)
- Network Security Web Report, [ND-3-61](#)

O

- Options dialog box, [ND-3-51](#)
- overview, [ND-1-1](#)

P

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

R

- report
 - generating report output, [ND-3-40](#)
- Report Comparison Options, [ND-3-46](#)
- Report Formats, [ND-3-40](#)
- Report on Match/No Match Commands, [ND-3-29](#), [ND-3-31](#)
- reports
 - generating Microsoft Word report in NetDoctor, [ND-3-44](#)
- Reusing Security Demand Configuration Information, [ND-3-57](#)
- rule description
 - viewing, [ND-3-3](#)
- Run NetDoctor, [ND-3-3](#)
- Run NetDoctor Dialog Box, [ND-3-9](#)
- Run NetDoctor dialog box, [ND-3-9](#)
- Run NetDoctor Options, [ND-3-2](#)
- Running NetDoctor (Basic Configuration), [ND-3-4](#)
- Running NetDoctor from a Template, [ND-3-9](#)

S

- security demand
 - creating, [ND-3-54](#)
 - creating attributes, [ND-3-55](#)
 - creating demands using the object palette, [ND-3-54](#)
 - creating multiple demands simultaneously, [ND-3-55](#)
 - exporting and importing, [ND-3-57](#)
 - running simulations, [ND-3-59](#)
 - selecting tables for security Web report, [ND-3-60](#)
- Security Demand Attributes, [ND-3-55](#)
- Security Demand Configuration File, [ND-3-58](#)
- security report
 - viewing, [ND-3-60](#)
- Selecting Tables for Security Web-Report, [ND-3-60](#)
- Settings Tab, [ND-3-9](#)
- Suppressed Message Count, [ND-3-50](#)
- Suppressing Messages, [ND-3-48](#)

T

- Template File Rule, [ND-3-35](#)
- Template File Rule Example, [ND-3-35](#)
- Template Specification File, [ND-3-34](#)
- Template_file_spec.xml File, [ND-3-36](#)
- The Demands Object Palette, [ND-3-54](#)

U

- Using NetDoctor, [ND-3-1](#)
- Using Security Demands in Simulations Studies, [ND-3-59](#)
- Using Specified Commands, [ND-3-27](#)
- Using Template Files, [ND-3-32](#)

V

- Vendor-Specific Rules, [ND-3-32](#)
- View Recent NetDoctor Reports Dialog Box, [ND-3-39](#)
- Viewing a Previous Report, [ND-3-39](#)
- Viewing Security Configuration in the Workspace, [ND-3-58](#)
- Viewing Security Reports, [ND-3-60](#)
- Visualizing Network Security Configuration, [ND-3-58](#)

W

- Web report
 - viewing sample output, [ND-3-5](#)