



Preface

This guide describes the Cisco Traffic Anomaly Detector (Detector), how it functions, and how to perform administration tasks.

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

This preface contains the following sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

Audience

The *Cisco Traffic Anomaly Detector Configuration Guide* is intended primarily for the following audiences:

- Network administrators
- Engineers
- Operators
- Network security professionals

This guide assumes a thorough knowledge of networking and networking security.

How to Use This Guide

This guide is organized as follows:

Chapter	Description
Chapter 1, “Product Overview”	Describes the Cisco Traffic Anomaly Detector (Detector) and outlines the Detector operation states and components.
Chapter 2, “Initializing the Detector”	Describes the initial procedures required to connect and configure the Detector. The chapter outlines the Detector CLI environment and authentication methods.
Chapter 3, “Configuring the Detector”	Describes how to configure Detector services and access control.
Chapter 4, “Configuring Zones”	Describes how to create and manage zones.
Chapter 5, “Configuring Zone Filters”	Describes the zone filters and how to configure them.
Chapter 6, “Configuring Policy Templates and Policies”	Describes the zone policies and policy templates and how to configure them.
Chapter 7, “Learning the Zone Traffic Characteristics”	Describes the learning process and how to use the learning process to construct and tune the policies that the Detector uses for zone anomaly detection.
Chapter 8, “Detecting Zone Traffic Anomalies”	Describes how to configure and activate the Detector to detect anomalies in the zone traffic and to activate a Cisco Guard to protect a zone.
Chapter 9, “Using Interactive Detect Mode”	Describes the Interactive detect mode and the recommendations, the user decision options, and the policy interactive status.
Chapter 10, “Using Attack Reports”	Describes the attack reports, the report structure, and viewing options.
Chapter 11, “Using Detector Diagnostic Tools”	Describes the Detector diagnostic tools.
Chapter 12, “Performing Maintenance Tasks”	Describes how to perform tasks that are required for Detector maintenance.

Symbols and Conventions

This guide uses the following conventions:

Style or Symbol	Description
boldface font	Boldface text indicates commands and keywords that you must enter exactly as shown.
<i>Italics font</i>	Italic font indicates arguments for which you supply the values.

Style or Symbol	Description
Screen font	Screen font indicates the screen display, such as a prompt, and information that the Detector displays on the screen. Do not enter screen font as part of the command.
[x]	Square brackets indicate an optional element (keyword or argument).
[x y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
[x {y z}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to select one. If you do, you have some required choices.

This guide uses the zone name *scannet* and the prompt *user@DETECTOR-conf-zone-scannet#* in examples.

This guide uses the following symbols and conventions to identify different types of information:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Tip

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.



Timesaver

Means the described action saves time. You can save time by performing the action described in the paragraph.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

