



CHAPTER 1

Product Overview

This chapter provides a general overview of the Cisco Traffic Anomaly Detector (Detector) including its major components and how they work together to help protect network elements by detecting malicious attack traffic

The chapter contains the following sections:

- [Understanding the Detector Module](#)
- [Understanding DDoS Attacks](#)
- [Understanding Zones, Zone Policies, and the Learning Process](#)
- [Understanding the Anomaly Detection Process](#)

Understanding the Detector Module

The Detector monitors a copy of the network traffic, continuously looking for indications of a Distributed Denial of Service (DDoS) attack against a network element, or *zone*, such as a server, firewall interface, or router interface.

Using port mirroring or a fiber optic link splitter, you configure the switch or router to capture the traffic sent to the zone and pass a copy of it to the Detector.

The Detector can operate as an independent DDoS detection and alarm component; however, it works optimally with the Cisco Guard (Guard), the companion product of the Detector.



Note

The Guard is a DDoS attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector can also synchronize zone configurations with the Guard. For more information about the Guard, see the *Cisco Anomaly Guard Module Configuration Guide* or the *Cisco Guard Configuration Guide*.

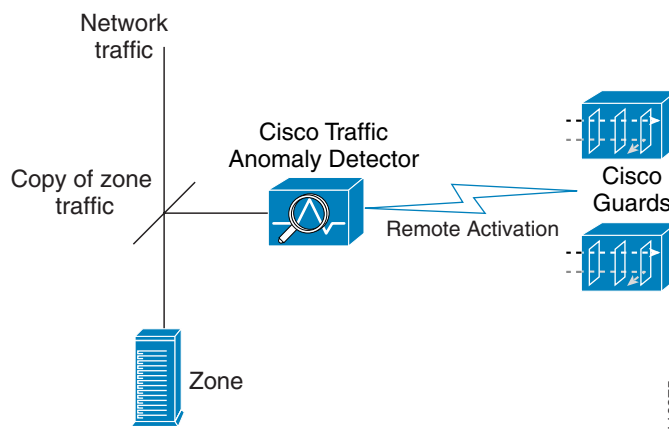
The Detector uses a set of zone policies to analyze a copy of all inbound zone traffic. The zone policies enable the Detector to identify traffic anomalies that indicate an attack on the zone. When the Detector identifies a traffic anomaly, it can issue a syslog message to notify you of the attack or it can activate a Guard to mitigate the attack.

The Detector allows you to do the following tasks:

- **Traffic learning**—Learns the characteristics (services and traffic rates) of normal zone traffic using an algorithm-based process. During the learning process, the Detector modifies the default zone traffic policies and policy thresholds to match the characteristics of normal zone traffic. The traffic policies and thresholds define the reference points that the Detector uses to determine when the zone traffic is normal or abnormal (indicating an attack on the zone).
- **Traffic anomaly detection**—Detects anomalies in zone traffic based on normal traffic characteristics.

Figure 1-1 shows a sample network application in which the Detector receives a copy of the network traffic for analysis.

Figure 1-1 Cisco Traffic Anomaly Detector Operation



Understanding DDoS Attacks

DDoS attacks deny legitimate users access to a specific computer or network resource. These attacks are launched by individuals who send malicious requests to targets that degrade service, disrupt network services on computer servers and network devices, and saturate network links with unnecessary traffic.

This section contains the following topics:

- [Understanding Spoofed Attacks](#)
- [Understanding Nonspoofed Attacks](#)

Understanding Spoofed Attacks

A spoofed attack is a type of DDoS attack in which the packets contain an IP address in the header that is not the actual IP address of the originating device. The source IP addresses of the spoofed packets can be random or have specific, focused addresses. Spoofed attacks saturate the target site links and the target site server resources. It is easy for a computer hacker to generate high volume spoofed attacks even from a single device.

Understanding Nonspoofed Attacks

Nonspoofed attacks (or client attacks) are mostly TCP-based with real TCP connections that can overwhelm the application level on the server rather than the network link or operating system.

Client attacks from a large number of clients (or zombies) may overwhelm the server application even without any of the individual clients creating an anomaly. The zombie programs try to imitate legitimate browsers that access the target site.

Understanding Zones, Zone Policies, and the Learning Process

This section describes what a Detector zone represents, how zone policies detect traffic anomalies, and how the Detector learns the zone traffic characteristics.

These sections contain the following topics:

- [Understanding Zones](#)
- [Understanding the Zone Policies](#)
- [Understanding the Learning Process](#)

Understanding Zones

A zone that the Detector monitors for traffic anomalies can be one of the following elements:

- A network server, client, or router
- A network link, subnet, or an entire network
- An individual Internet user or a company
- An Internet Service Provider (ISP)
- Any combination of these elements

When you create a new zone, you assign a name to it and configure the zone with network addresses. The Detector configures the zone with a default set of policies and policy thresholds to detect anomalies in the zone traffic.

The Detector can protect multiple zones at the same time if the network address ranges do not overlap.

For more information about zones, see [Chapter 4, “Configuring Zones.”](#)

Understanding the Zone Policies

The policies associated with the zone configuration enable the Detector to detect anomalies in the zone traffic. When the traffic flow exceeds a policy threshold, the Detector identifies the traffic as abnormal or malicious and dynamically configures a set of filters (dynamic filters) to apply the appropriate detection level to the traffic flow according to the severity of the attack.

For more information about zone policies, see [Chapter 4, “Configuring Zones.”](#)

Understanding the Learning Process

The learning process enables the Detector to analyze normal zone traffic and create a set of zone-specific policies and policy thresholds that enable the Detector to more accurately detect zone traffic anomalies.

You enable the learning process to replace the default set of zone policies or to update the current set of zone policies that may not be configured properly to recognize current normal traffic services and volume. When policy thresholds are set too high compared to the current normal traffic volume, the Detector might not be able to detect traffic anomalies (attacks). When policy thresholds are set too low, the Detector may mistake legitimate traffic for attack traffic.

The learning process consists of the following two phases:

- **Policy Construction Phase**—Creates the zone policies for the main services that the zone traffic uses. To create zone policies, the Detector follows the rules established by the policy templates that each zone configuration contains.
- **Threshold Tuning Phase**—Tunes the thresholds of the zone policies to values that are appropriate for recognizing the normal traffic rates of the zone services.

For more information about the learning process, see [Chapter 7, “Learning the Zone Traffic Characteristics.”](#)

Understanding the Anomaly Detection Process

This section describes how the Detector detects zone traffic anomalies and generates attack reports.

This section contains the following topics:

- [Understanding Traffic Filters](#)
- [Understanding the Different Anomaly Detection Modes](#)
- [Understanding the Detect and Learn Function](#)
- [Understanding Attack Reports](#)

Understanding Traffic Filters

The Detector uses three types of traffic filters to apply the required anomaly detection level to the zone traffic. You can configure these filters to customize the traffic flow and control the DDoS detection operation.

The Detector uses the following types of traffic filters:

- **Bypass filters**—Prevent the Detector from applying DDoS detection measures to specific traffic flows.
- **Flex-Content filters**—Count a specified traffic flow and filter according to fields in the IP and TCP headers and content bytes.
- **Dynamic filters**—Apply the analysis detection level to the traffic flow. When the Detector detects an anomaly during the analysis process, the dynamic filters instruct the Detector to either record the event in the syslog or activate a Guard to protect the zone.

The Detector coordinates the actions of the zone policies that monitor the zone traffic for anomalies with the zone filters.

For more information about filters, see [Chapter 5, “Configuring Zone Filters.”](#)

Understanding the Different Anomaly Detection Modes

You can activate the Detector anomaly detection operation in the following ways:

- Automatic detection mode—The Detector automatically activates the dynamic filters that it creates.
- Interactive detect mode—The Detector builds a queue of the dynamic filters that it creates and then groups the filters as recommended actions. You review the recommendations and decide whether to accept, ignore, or direct these recommendations to automatic activation.

For more information about the interactive detect mode, see [Chapter 9, “Using Interactive Detect Mode.”](#)

Understanding the Detect and Learn Function

You can activate the threshold tuning phase of the learning process and activate zone anomaly detection simultaneously (the detect and learn function) to enable the Detector to learn the new zone policy thresholds and at the same time monitor the traffic for anomalies using the current thresholds. When the Detector detects an attack, it stops the learning process but continues to monitor the traffic for anomalies. This process prevents the Detector from learning malicious traffic thresholds during an attack.

For more information about the detect and learn function, see the [“Enabling the Detect and Learn Function”](#) section on page 7-11.

Understanding Attack Reports

The Detector provides an attack report for every zone that provides zone status information and details of the attack, starting with the production of the first dynamic filter, and ending with anomaly detection termination.

For more information about the attack reports, see [Chapter 10, “Using Attack Reports.”](#)

