



CHAPTER 1

Product Overview

This chapter provides a general overview of the Cisco Guard (Guard) including its major components and how they work together to protect network elements from malicious attack traffic.

The chapter contains the following sections:

- [Understanding the Guard](#)
- [Understanding DDoS Attacks](#)
- [Understanding Zones, Zone Policies, and the Learning Process](#)
- [Understanding Zone Protection](#)
- [Understanding the Protection Cycle](#)

Understanding the Guard

The Guard is a Distributed Denial of Service (DDoS) attack mitigation device that diverts suspect traffic from its normal network path to itself for cleaning. During the traffic cleaning process, the Guard identifies and drops the attack packets and forwards the legitimate packets to their targeted network destinations.

Typically, you deploy the Guard in a distributed upstream configuration at the backbone level.

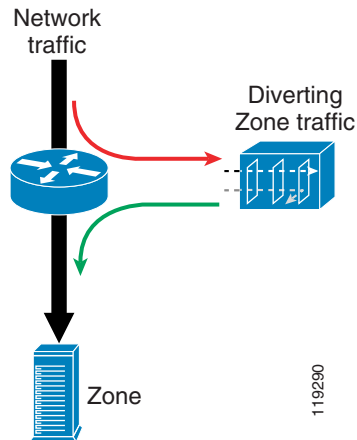
You define the network elements, or *zones*, that the Guard protects against DDoS attacks. When a zone is under attack, the Guard diverts only the network traffic that is destined for the targeted zone, identifies and drops specific attack packets, and forwards legitimate traffic packets to the zone. The Guard constantly filters the zone traffic and stays on the alert for evolving attack patterns. When the Guard determines that the attack on the zone has ended, it stops diverting the zone traffic to itself. By diverting network traffic only when needed, the Guard can assume its protective role when there is an attack but remain unobtrusively in the network background for the rest of the time.

The Guard allows you to do the following tasks:

- **Traffic learning**—Learn the characteristics (services and traffic rates) of normal zone traffic using an algorithm-based process. During the learning process, the Guard 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 Guard uses to determine when the zone traffic is normal or abnormal (indicating an attack on the zone).
- **Traffic protection**—Distinguish between legitimate and malicious traffic and filter the malicious traffic so that only the legitimate traffic is allowed to pass on to the zone.
- **Traffic diversion**—Divert the zone traffic from its normal network path to the Guard learning and protection processes and then returns the legitimate zone traffic to the network.

Figure 1-1 shows a sample network application in which the Guard diverts zone traffic to itself so it can learn the zone traffic or protect the zone from an attack.

Figure 1-1 Cisco Guard 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.

To overcome spoofed attacks, the Guard performs anti-spoofing processes that use challenge-response algorithms that can distinguish spoofed traffic from nonspoofed traffic. The Guard considers the traffic that passes the anti-spoofing mechanisms as authenticated traffic.

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.

The Guard initially activates an anti-spoofing mechanism to block all spoofed packets. The Guard then performs a statistical analysis on the traffic to detect and block anomalies in the traffic that are not spoofed, such as an unusual number of SYN packets, a large number of concurrent connections, or a high traffic rate.

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. The Guard anti-zombie processes mitigates such HTTP attacks by using a challenge response authentication process to differentiate between legitimate browsers and zombie programs that access the attacked site.

Understanding Zones, Zone Policies, and the Learning Process

This section describes what a Guard zone represents, how zone policies detect traffic anomalies, and how the Guard 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 Guard protects 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 Guard configures the zone with a default set of policies and policy thresholds to detect anomalies in the zone traffic.

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

For more information about zones, see [Chapter 5, “Configuring Zones.”](#)

Understanding the Zone Policies

When the Guard protects a zone, the policies associated with the zone configuration enable the Guard to detect anomalies in the zone traffic and mitigate attacks on the zone. When the traffic flow exceeds a policy threshold, the Guard identifies the traffic as abnormal or malicious and dynamically configures a set of filters to apply the appropriate protection level to the traffic flow according to the severity of the attack.

For more information about zone policies, see [Chapter 7, “Configuring Policy Templates and Policies.”](#)

Understanding the Learning Process

The learning process enables the Guard to analyze normal zone traffic and create a set of zone-specific policies and policy thresholds that are based on the analyzed traffic. The zone-specific policies and policy thresholds enable the Guard 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 Guard might not be able to detect traffic anomalies (attacks). When policy thresholds are set too low, the Guard 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 Guard 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 8, “Learning the Zone Traffic Characteristics.”](#)

Understanding Zone Protection

You can activate zone protection on the Guard by using one of the following methods:

- **Manually**—You can manually access the Guard and activate protection for a zone.
- **Automatically**—You can configure the Guard to accept a protection activation message from a network attack detection device, such as the Cisco Traffic Anomaly Detector (Detector).



Note

The Detector is the companion product of the Guard. The Detector is a DDoS attack detection device that can analyze a copy of the zone traffic and activate the Guard attack mitigation services when the Detector determines that the zone is under attack. The Detector can also synchronize zone configurations with the Guard. For more information about the Detector, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* and *Cisco Traffic Anomaly Detector Configuration Guide*.

This section contains the following topics:

- [Understanding Traffic Filters](#)
- [Understanding the Different Protection Modes](#)
- [Understanding the Protect and Learn Function](#)
- [Understanding On-Demand Protection](#)
- [Understanding Attack Reports](#)

Understanding Traffic Filters

The Guard uses four types of traffic filters to apply the required protection level to the zone traffic. You can configure these filters to customize the traffic flow and control the DDoS protection operation.

The Guard uses the following types of filters:

- User Filters—Apply the required protection level to the specified traffic flows.
- Bypass filters—Prevent the Guard from applying DDoS protection measures to specific traffic flows.
- Flex-Content filters—Count or drop a specified traffic flow and filter according to fields in the IP and TCP headers and content bytes.
- Dynamic filters—Apply the required protection level to the specified traffic flows. The Guard creates dynamic filters only when it detects an attack on the zone and configures them based on its analysis of the traffic flow. The Guard continuously modifies this set of filters based on the the zone traffic, type of DDoS attack, and changes to the attack characteristics.

The Guard has three protection levels that enable it to apply different processes to the traffic flows:

- Analysis protection level—Allows the traffic to flow monitored, but unhindered, during zone protection if no anomalies are detected. Once the Guard detects an anomaly, it applies the appropriate protection level to the traffic.
- Basic protection level—Activates anti-spoofing and anti-zombie functions to authenticate the traffic by inspecting the suspicious traffic flow to verify its source.
- Strong protection level—Activates severe anti-spoofing functions that inspect the traffic flow packets to verify the legitimacy of the flow.

The Guard analyzes the traffic and coordinates the efforts of the zone policies that monitor the zone traffic for anomalies with the zone filters. In addition, it limits the rate of traffic that it injects on to the zone to prevent traffic overflow.

For more information about filters, see [Chapter 8, “Learning the Zone Traffic Characteristics.”](#)

Understanding the Different Protection Modes

You can activate the Guard to perform zone protection as follows:

- Automatic protect mode—Automatically activates the dynamic filters that it creates during an attack.
- Interactive protect mode—Creates dynamic filters during an attack but does not activate them. Instead, the Guard groups the dynamic filters as recommended actions for you to review and decide whether to accept, ignore, or direct these recommendations to automatic activation.

For more information about the protection modes, see [Chapter 10, “Using Interactive Protect Mode.”](#)

Understanding the Protect and Learn Function

You can activate the threshold tuning phase of the learning process and activate zone protection simultaneously (the protect and learn function) to enable the Guard to learn the zone policy thresholds and at the same time monitor the traffic for anomalies. When the Guard detects an attack, it stops the learning process and begins mitigating the attack. The Guard resumes the learning process when the attack ends. This process prevents the Guard from learning malicious traffic thresholds during an attack.

For more information about the protect and learn function, see the [“Enabling the Protect and Learn Function”](#) section on page 8-11.

Understanding On-Demand Protection

You can use the default zone templates and associated default policies to protect a zone without enabling the Guard to learn the zone traffic characteristics. The default policies and filters in the Guard zone templates can protect a zone that has traffic characteristics that are unknown to the Guard.

For more information about on-demand protection, see the [“Activating On-Demand Protection”](#) section on page 9-2.

Understanding Attack Reports

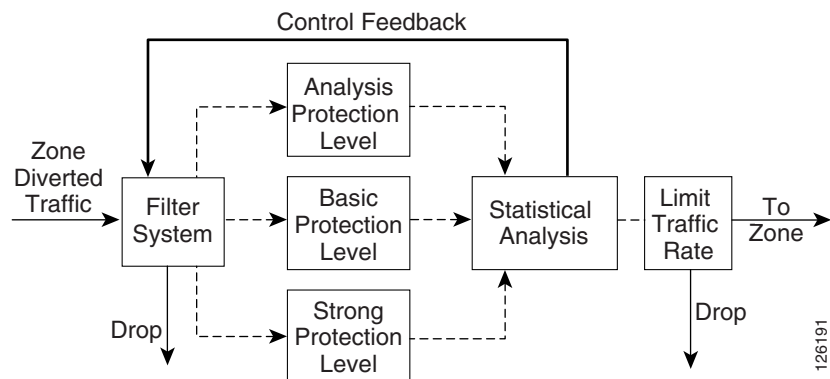
The Guard provides an attack report for every zone that provides zone status information and details of the attack, starting with the production of the first dynamic filter and ending with protection termination.

For more information about the attack reports, see [Chapter 11, “Using Attack Reports.”](#)

Understanding the Protection Cycle

The Guard protection cycle applies the zone filters, zone policies, and the Guard protection levels to the traffic flow to analyze and clean the zone traffic and inject legitimate traffic only to the zone. [Figure 1-2](#) shows the Guard protection cycle.

Figure 1-2 Guard Protection Cycle



Once zone protection is activated by you or by an anomaly detection device such as the Detector, the Guard diverts the zone traffic to itself where the policies of the zone configuration monitor the traffic flow. A policy executes an action against a particular traffic flow when the flow exceeds the policy threshold. Policy actions can range from issuing a notification to creating new filters (dynamic filters) that direct the traffic to the appropriate protection level. The Guard analyzes the traffic flow, drops the traffic that exceeds the defined rate that the zone can handle, and then injects the legitimate traffic back to the zone.

During the attack, the Guard performs a closed-loop feedback cycle in which it adjusts the zone protection measures to the dynamically changing zone traffic characteristics. The Guard adjusts the protection strategies to handle any changes to the DDoS attack and traffic flow. The Guard stops zone protection if no dynamic filters are in use, the traffic to the zone has not been dropped, or no new dynamic filters have been added over a predefined period of time.

