

---

## Mitigating DDoS Using Cisco Guard and Traffic Anomaly

**Duration: 2**    **Course Code: DDOS**

---

### Overview:

This course *Mitigating DDoS Using Cisco Guard and Traffic Anomaly Detector* (DDOS) v1.0, is an introductory end-user course focused on the basic deployment and configuration of the Cisco Guard (Guard) and Cisco Traffic Anomaly Detector (Detector) distributed denial of service (DDoS) mitigation solutions. On completing the course, delegates will be able to recognize threats posed by DDoS attacks, select the appropriate mitigation strategies, and successfully deploy Cisco DDoS mitigation solutions. This course includes hands-on lab practice in setting up and configuring Guard and Detector devices, creating zones and protection policies, and analyzing Guard attack reports for various DDoS attack scenarios.

---

### Target Audience:

The Primary audience for this course are: Network designers, Network Administrators, Network Engineers, Network Managers, Program Managers, Project Managers and System Engineers.

---

### Objectives:

- Describe how the Cisco DDoS defence solution protects network devices from suspect traffic generated during a DDoS attack.
  - Describe the operation of the Cisco Guard and Cisco Traffic Anomaly Detector, including zone traffic learning, zone traffic protection, and the Guard protection cycle.
  - Configure network connectivity for the Guard and Detector for operation in a given customer network.
  - Select the appropriate DDoS mitigation traffic diversion and injection methods for a given customer network.
  - Configure the appropriate zones in the Guard and Detector for a given customer scenario.
  - Configure the appropriate optional zone filters in the Guard and Detector for a given customer scenario.
  - Adjust the Guard to optimize performance for a given customer scenario.
- 

### Prerequisites:

The skills and knowledge required from a delegate before they take this course are as follows

- Delegates must hold a valid CCNA
  - Foundation-level network knowledge and skills necessary to install, configure, operate, and troubleshoot network devices and applications.
  - Basic knowledge of Cisco IOS networking and concepts
  - Foundation-level network security knowledge and skills necessary to install, configure, operate and troubleshoot network security devices and applications including firewalls, intrusion detection systems and intrusion prevention systems.
  - Basic knowledge of the Windows operating system
-

## Content:

### **Mitigating DDoS Attacks**

- What is a DDoS Attack
- Impact of a DDoS Attack
- Types of DDoS Attack
- Deficiencies of Common DDoS Defences
- Designing a complete DDoS Protection Program
- Cisco Guard
- Cisco Guard Core Processes
- Cisco Traffic Anomaly Detector
- Cisco DDoS Defence Deployment

### **Understanding the Cisco Guard and the Cisco Traffic Anomaly Detector**

- Cisco Guard and Traffic Anomaly Detector Operation
- What is a Zone
- Zone Traffic Diversion
- Zone Traffic Learning
- Zone Traffic Protection
- The Cisco Guard Protection Cycle
- Cisco Guard Interactive Recommendations
- Cisco Guard Attack reports
- Optional Features

### **Configuring Network Connectivity for the Cisco Guard and Traffic Anomaly Detector**

- Installing the Cisco Guard and the Traffic Anomaly Detector
- Cisco Guard and Traffic Anomaly Detector CLI
- Basic Setup tasks
- Configuring the Cisco Guard and Traffic Anomaly Detector Interfaces
- Configuring the Cisco Guard and Traffic Anomaly Detector Network Connections
- Enabling Cisco Guard and Traffic Anomaly Detector Services
- Configuring AAA

### **Diverting and Injecting Traffic**

- What is IP Traffic Diversion
- Common Traffic Injection Methods
- Policy –based Routing Method
- VPN Routing Forwarding Method
- Tunnel Diversion Method

### **Configuring Zones**

- Zone Configuration Process
- Creating a Zone
- Configuring Zone Traffic Diversion and Injection
- Configuring Remote Activation of Cisco Guard
- Learning Zone Traffic Characteristics
- Zone Configuration Example

### **Configuring Optional Zone Filters**

- Zone Filters
- Flex Filters
- Bypass Filters
- User Filters

### **Managing the Cisco Guard and Traffic Anomaly Detector**

- Managing the Cisco Guard and Cisco Traffic Anomaly Detector
- Reloading, Rebooting, and shutting Down the Cisco Guard and Cisco Traffic Anomaly Detector
- Protecting the Zone
- Cisco Guard and Cisco Traffic Detector Attack Reports
- Interpreting Cisco Guard Attack Reports
- Viewing Dropped Traffic Statistics

## Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 01924 377489

[info@globalknowledge.co.uk](mailto:info@globalknowledge.co.uk)

[www.globalknowledge.co.uk](http://www.globalknowledge.co.uk)

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK