The bridge to possible

Cisco Secure DDoS Edge Protection Datasheet

Contents

Product overview

Cisco® Secure DDoS Edge Protection is an innovative software solution that stops cyberattacks at the service provider (SP) network edge. The Edge Protection solution consists of a controller and one (1) or more detectors across the network.

When deployed on supported Cisco IOS® XR–based routers, Edge Protection detects and mitigates distributed-denial-of-service (DDoS) attacks directly on the routers of an SP network. By moving DDoS protection to the network edge, service providers can mitigate DDoS attacks at the most efficient and lowest risk location, the ingress points. This minimizes the impact that DDoS attacks have on the network and applications, reduces core bandwidth requirements, and ensures customer quality of experience (QoE). DDoS detection at the network edge enables SPs to mitigate attacks at the source, eliminating the need to backhaul traffic to scrubbing centers.

The Edge Protection solution consists of two components:

1. Centralized controller – A service that manages a distributed network of detectors, analyzes trends across the network, and orchestrates cross-network visibility and mitigation. The controller also delivers a full system management lifecycle for the entire service.
2. A collection of detectors – An Edge Protection detector is a Docker container that runs on a Cisco IOS XR–based router.

Features and customer benefits

- Stop DDoS attacks at the ingress of the network
- No additional hardware required
- No changes to the architectures
- No need to overprovision network facilities such as links and routers to account for attack traffic
- No backhauling of malicious traffic
- Minimizes customer outages and optimizes the end-user experience
- No additional facilities requirements such as power, rack space, and cooling
- Allows SPs to meet low-latency application requirements

The diagram below depicts the use of Cisco Secure DDoS Edge Protection to detect and mitigate DDoS attacks at the network edge.

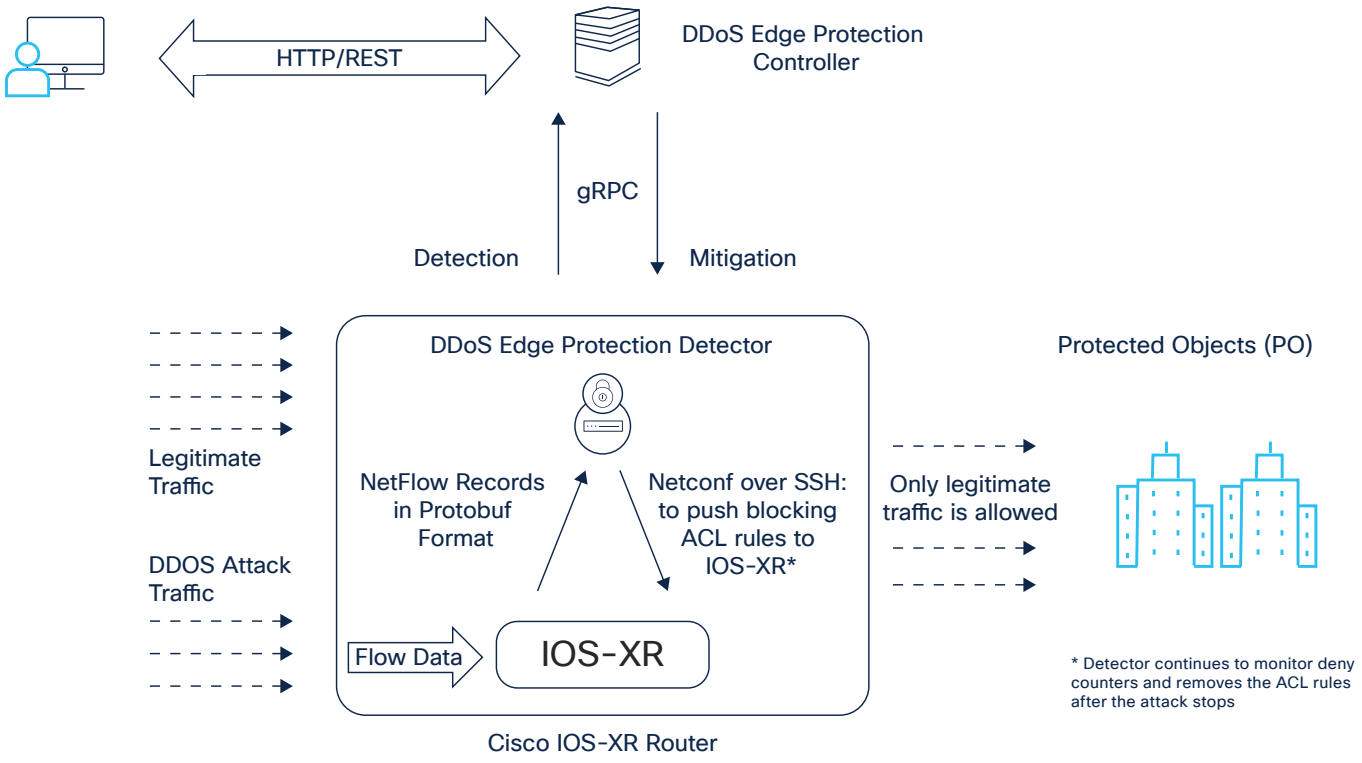

Figure 1. Secure DDoS Edge Protection solution components and traffic flow

Controller

The Edge Protection controller is highly available central management software that manages a collection of detectors that have been deployed on the edge or peering routers. The controller is designed in a modular and containerized architecture to be deployed on a highly scalable Kubernetes cluster, allowing for containers to expand and be replicated in order to manage and support thousands of detectors.

The bridge to possible

Controller functions

Key features and functions of the controller include the following:

- Manages container lifecycle for a fleet of detectors
- Configures and edits detector profiles and security settings
- Checks the health of detectors
- Displays information about real-time attack forensics and threat intelligence analyses
- Controls the mitigation of DDoS attacks at the ingress point of the network
- Provides real-time reporting of events as well reporting on past events
- Provides operational control and incident response

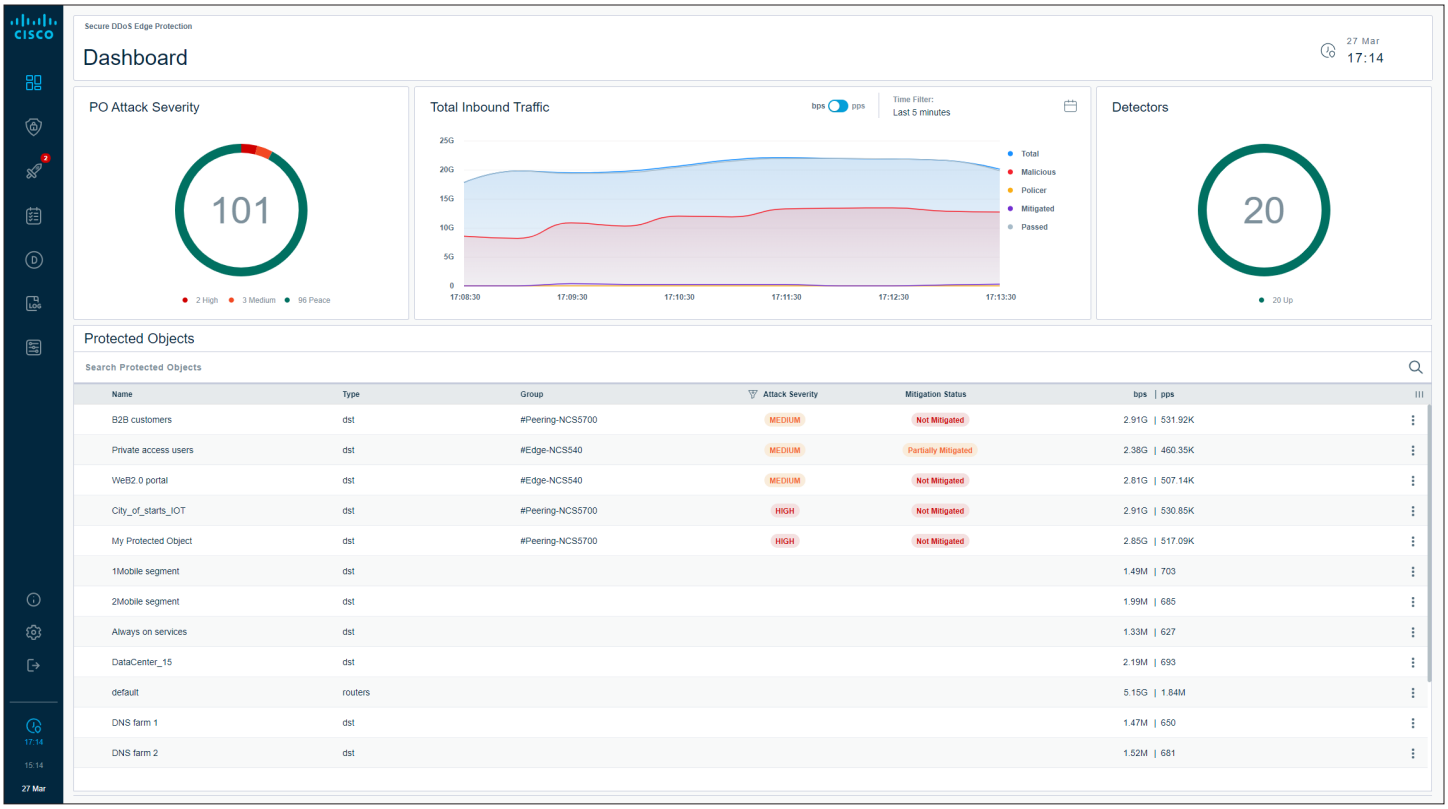

Figure 2. Controller main dashboard. High-level status of the network, protected objects, and detectors.

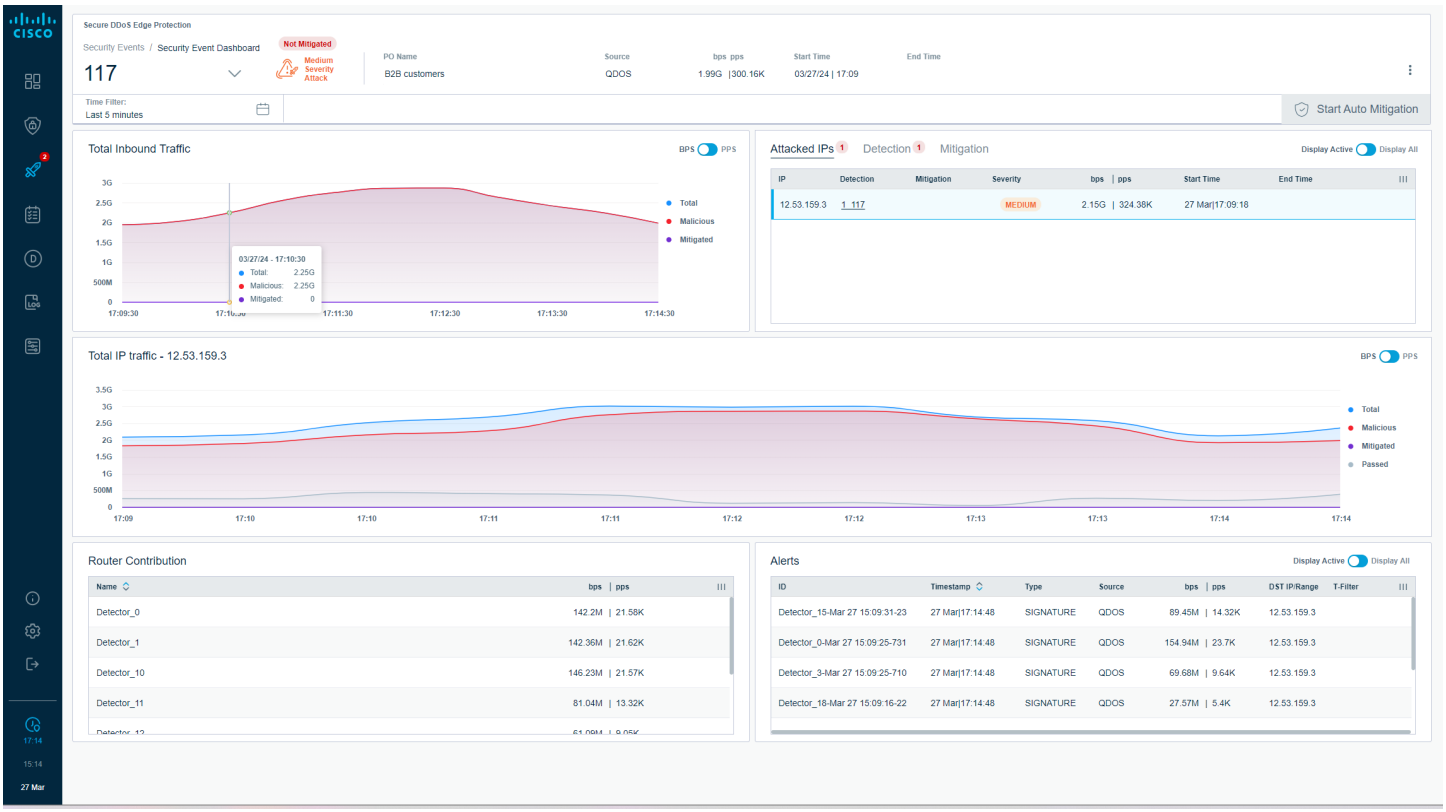

Figure 3. Detailed attack view. Attack detection events, deployed mitigation ACL rules, and attack traffic.

Controller specifications

The controller can be deployed using a provided OVA or on a customer-deployed Ubuntu Linux machine that meets the system requirements below and required software dependencies.

Provided OVA virtual machine minimum requirements:

- OVA: VMWare
- vCPU: 4 cores
- Memory: 8 GB
- Disk: 100 GB (7200 RPM or better)
- 1 network interface

Customer-deployed virtual machine minimum requirements:

- OS: Ubuntu Linux 20.04
- vCPU: 4 cores
- Memory: 8 GB
- Disk: 100 GB (7200 RPM or better)
- 1 network interface

Software packages required:

- Minimum Kubernetes v1.18.20 installed

Maximum detectors per controller: 50,000[1]

Management protocol: SSH, HTTP, HTTPS, REST API

Controller to/from detector communication protocol: gRPC

High availability: Yes, using Kubernetes clustering technology

Detector

The detector is a container deployed on Cisco IOS XR–based routers that utilizes spare management CPU and memory to avoid any negative impact on the performance of the router or traffic flow through the router. The detector analyzes flows received from the router and uses patented technology to determine whether the traffic is legitimate or a DDoS attack. Once an attack is detected, the mitigation can be implemented on the router ingress port either automatically or manually depending on the service provider's preference.

Having all the flows inspected locally on each router provides better visibility, quicker response, and a more optimized network as malicious traffic is blocked at the source rather than being redirected to a centralized scrubbing center. Additionally, no additional hardware is required to be deployed for the detection and mitigation as they leverage the existing technology already installed at these ingress points into the service provider's network.

Deployment of the detectors is controlled and managed by the Edge Protection centralized controller.

Detector specifications

Router requirements:

Supported NCS 540[1], NCS 55xx/57xx, and Cisco 8000 routers running IOS-XR

Management protocols: SSH and NETCONF over SSH

NetFlow v9 support

Docker container support for third-party applications

Minimum 2 CPU cores and 1 GB RAM

1 For the Edge Protection controller to support 50,000 detectors, additional memory and CPU cores will be required above the minimum required resources to deploy the controller. Example: To support 1000 detectors, the recommended number of resources required is 8 CPU cores and 16 GB memory.

Although there are no specific versions of CPU or memory specified, the performance and response of the application will be reflective of the quality and performance of these components.

Detector scalability

The scalability of the Edge Protection detector is based on the number of flows ingested, not on the bandwidth consumed by the router. A single detector can ingest tens of thousands of flows per second (FPS) without impacting the data or management plane of the router. Flows forwarded to the Edge Protection detector are based on a sampling rate. The sampling rate used is usually dependent on the volume of traffic and flows on a device to provide good visibility into data without losing attack accuracy. Higher sampling results in more flows being forwarded to the detector and thereby increasing the total number of FPS received by the detector.

With ingress traffic on the router at 1.2 Tbps and a sampling rate of 1024:1, the 50,000 FPS received by the detector required less than 65% of available detector CPU cores and less than 200 MB of the allocated 1 GB detector RAM.

The figures below shows the increase in the detector's CPU utilization as the number of flows per second increase for both GTP (Figure 4) and non-GTP traffic (Figure 5).

Table 1. GTP traffic use case on NCS 540

UE FPS	Sampling rate	Detector FPS	CPU
100,000	10:1	10,000	20%
100,000	100:1	1000	<5%
1,000,000	100:1	10,000	20%
10,000,000	1000:1	10,000	20%
50,000,000	1000:1	50,000	65%
100,000,000	4000:1	25,000	38%
250,000,000	4000:1	62,500	80%
1,000,000,000	20,000:1	50,000	65%

1 Refer to Cisco Network Convergence System 540 Medium Density Routers Data Sheet and Cisco Network Convergence System 540 Large Density Router Data Sheet for a list of supported models.

Table 2. Non-GTP traffic use case on Cisco NCS 55xx/57xx

Unique user traffic @ Flows Per Second (FPS)	Total throughput (Ingress traffic)	NetFlow Sampling Rate	Unique Flows Per Second (FPS) on Detector	CPU(%)
100,000	1200 Mbps	1024:1	100	1
100,000	1200 Mbps	2048:1	120	1
1 million	1200 Mbps	1024:1	1000	3
1 million	1200 Mbps	2048:1	600	3
1 million	1200 Mbps	4096:1	500	3
10 million	1200 Mbps	1024:1	10000	25
10 million	1200 Mbps	2048:1	5000	20
10 million	1200 Mbps	4096:1	2000	10
50 million	1200 Mbps	1024:1	48000	130
50 million	1200 Mbps	2048:1	24000	70
50 million	1200 Mbps	4096:1	12000	30
100 million	1200 Mbps	2048:1	49000	130
100 million	1200 Mbps	4096:1	24000	63

Licensing

- The Edge Protection detector is licensed per router for a 3- or 5-year period.
- The controller is part of the overall solution package and therefore not licensed separately.

More information

For more information about Cisco Secure DDoS Edge Protection, please see:

- Secure DDoS Protection webpage: www.cisco.com/go/secure-ddos
- Edge Protection on DEVNET: developer.cisco.com/docs/secure-ddos-edge-protection
- Edge Protection DEVNET Demo Guide: www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protection/secure-protection-devnet-demo-guide.pdf
- Edge Protection AAG: www.cisco.com/c/en/us/products/collateral/security/secure-ddos-edge-protection-aag.pdf
- Edge Protection technical white paper: www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protection/secure-edge-protection-tech-wp.pdf