White paper Cisco public

# Cisco Secure DDoS Edge Protection: Security at the Network Edge

October 2024

# Contents

# 1. Introduction

In the ever-evolving digital landscape, the threat of Distributed Denial of Service (DDoS) attacks poses significant challenges for both service providers and network operators. The rapid growth of DDoS attack traffic far exceeds the expansion of internet traffic, exacerbating the urgency of addressing this issue.

Addressing the threat of DDoS attacks is getting more challenging as networks are increasingly decentralized, with local internet breakouts emerging as the standard for connecting cloud infrastructure, Content Delivery Networks (CDNs), and more. In addition, the accessibility and affordability of launching massive DDoS attacks have significantly lowered the barrier of entry for malicious actors, thereby heightening the vulnerability of online infrastructures. The deployment of centralized defense solutions struggles to keep pace with these evolving network dynamics and threats.

In response to these challenges, Cisco® has developed Cisco Secure DDoS Edge Protection, an innovative solution designed to bolster network defenses against DDoS attacks. Embracing the paradigm shift toward distributed, decentralized networks, Cisco Secure DDoS Edge Protection employs docker containers deployed onto edge routers, effectively positioning these routers as the first line of defense. This solution not only prevents attack traffic from infiltrating the network but also addresses the economic constraints often associated with existing solutions by utilizing already deployed hardware.

## 1.1 Cisco Secure DDoS Edge Protection Benefits

Cisco Secure DDoS Edge Protection is an innovative software solution that stops cyberattacks at the 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[1], Edge Protection detects and mitigates Distributed-Denial-of-Service (DDoS) attacks directly on the routers of a network. By moving DDoS protection to the network edge, network operators can mitigate DDoS attacks at the most efficient and lowest risk location, the ingress points.

Moving DDoS protection to the network edge, and keeping malicious traffic out, brings the following advantages:

### 1.1.1 Reduction in the total cost of ownership

Cisco Secure DDoS Edge Protection is designed to use existing router hardware to perform the detection and mitigation. As such, it reduces the need to divert traffic and deploy or add capacity to scrubbing centers. This enables up to 83% in TCO savings[2] including savings in required equipment, floor space, power, and cooling expenses.

[1] For a list of supported routers, refer to Edge Protection Data Sheet

[2] Based on TCO Calculation for 4 Tbps Peering Network, with Edge Protection solution deployed on NCS5500 platforms.

### 1.1.2 Ease of operation

The solution mitigates attacks right on the network edge, thus eliminating the need to transfer traffic from edge locations to scrubbing centers. This eases the burden on the network to transport suspect traffic and simplifies operations.

### 1.1.3 Easy deployment and management

The containerized software uses zero-touch provisioning and enables secure, smooth, and fast life cycle management.

### 1.1.4 No added latency

Malicious traffic is mitigated at the ingress of the edge/peering router and is not redirected into a scrubbing center. This way, network operators avoid adding latency to the legitimate traffic that would normally be processed through a scrubbing center.

### 1.1.5 Native scalability

The solution scales with the network it protects. It runs directly on the router and the DDoS protection capacity grows linearly with router capacity. This reduces the need to build additional scrubbing centers and distribute them across the network.

### 1.1.6 Faster detection and mitigation

Detection and mitigation are done on the router. Therefore, there is no need to send NetFlow records to external collectors, and no need for Border Gateway Protocol (BGP) redirection or BGP Flow spec for mitigation, resulting in a much faster process of detection and mitigation.

### 1.1.7 Future proof investment

Cisco Secure DDoS Edge Protection is designed to support distributed and disaggregated network architectures. Whether to protect 5G edge Multi-access Edge Computing (MEC), or distributed peering, the solution is built for hyperscale distribution of tens of thousands of nodes. This coverage is practically impossible to achieve with current DDOS solutions.

# 2. Solution overview

Cisco Secure DDoS Edge Protection consists of two components: a centralized controller and a collection of detectors.

## 2.1 Controller

The controller is a highly available central management software responsible for overseeing a collection of detectors deployed on Cisco IOS XR routers. Engineered with a modular and containerized architecture, the controller is deployable within a highly scalable Kubernetes cluster. This design enables containers to dynamically expand and replicate, facilitating the management and support of a fleet of detectors. Key functions of the controller include:

- Managing the lifecycle of a fleet of detectors
- Configuring and editing detector profiles and security settings
- Monitoring the health status of detectors
- Presenting real-time insights into attack forensics and threat intelligence analyses
- Orchestrating the mitigation of DDoS attacks at the network's ingress point
- Delivering event reporting and facilitating historical event analysis
- Enabling operational control and incident response

## 2.2 Detector

This is a container deployed on a Cisco IOS XR router, utilizing spare CPU and memory resources to ensure no negative impact on router performance or traffic flow.

The detector analyzes network telemetry received from the router using Protobuf and patented technology to determine the legitimacy of traffic. Upon detecting an attack, a mitigation policy employing Access Control List (ACL) rules will be applied to the router's ingress port. This can be applied automatically or manually, depending on the user's preference.

Inspecting all flows locally on each edge router offers enhanced visibility, quicker response times, and optimized network performance. This approach blocks malicious traffic as close to the source as possible, rather than rerouting it to a centralized scrubbing center, thus eliminating the need for additional hardware for detection and mitigation. The detector sits on existing edge routers already installed at these ingress points within the network.

The deployment and lifecycle of detectors are controlled and managed by the controller.

## 2.3 Attack lifecycle management

The attack lifecycle management process in the system includes identifying (detection), analyzing (characterization), and stopping (mitigation) ongoing attacks. It also includes post-attack actions that allows for reporting and investigation of attacks.

### 2.3.1 Detection

The diagram below illustrates the process of malicious traffic detection.

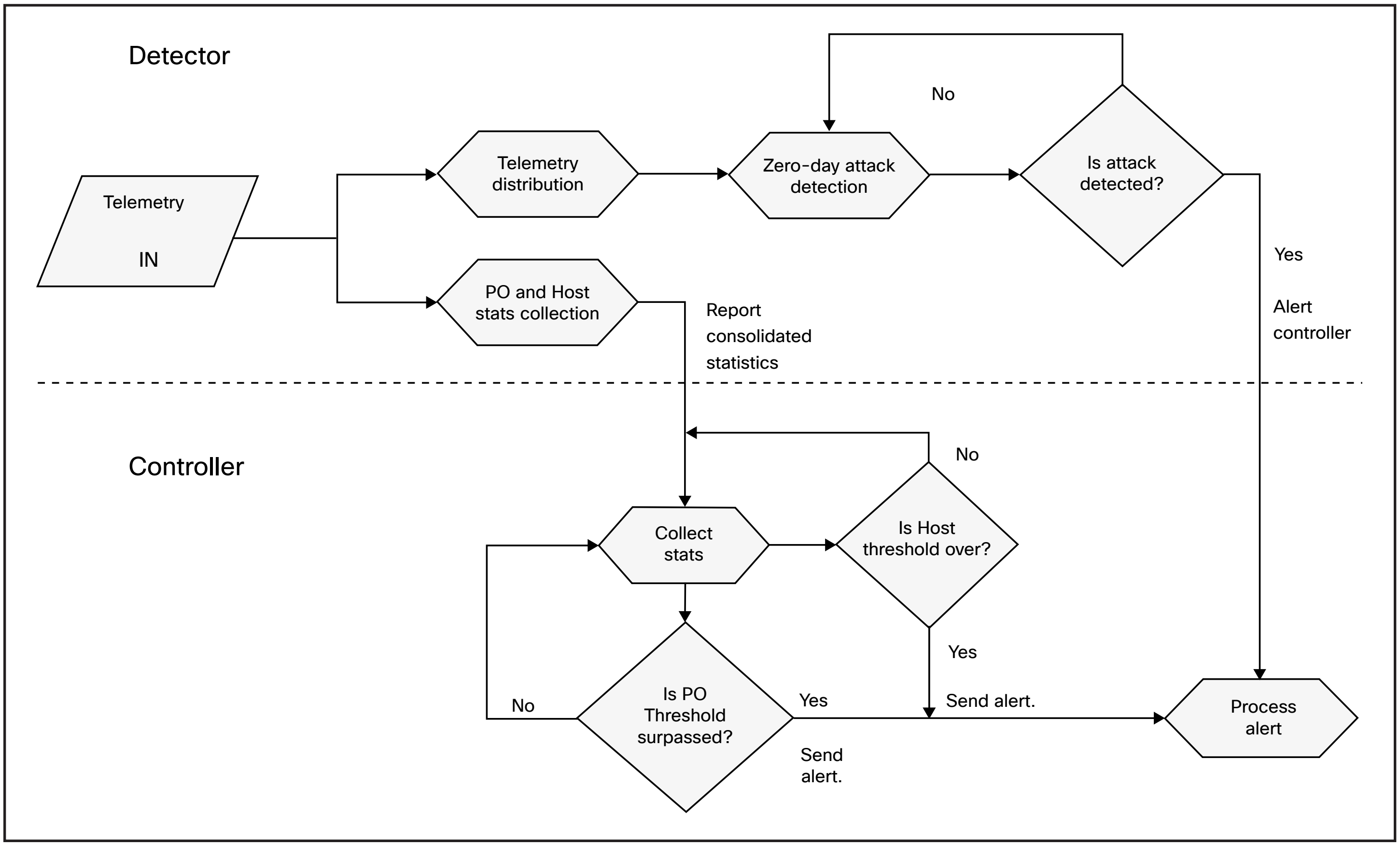


Figure 1. Detecting malicious traffic

The Cisco Secure DDoS Edge Protect employs two distinct attack detection algorithms to safeguard various network segments. In the Edge Protection terminology, these network segments are called Protected Objects or POs. As depicted in the diagram above, detection comprises a Zero-Day Attack Detection algorithm, operating within the context of a single detector, and a Threshold-based Detection algorithm, which aggregates statistical information from all detectors in the system.

#### 2.3.1.1 Zero Day Attack Detection[3]

The system employs an unsupervised machine learning algorithm based on statistical modeling of traffic traversing a router. During normal operation, the system learns statistical parameters, such as the average and standard deviation. An attack triggers detection when certain non-correlated parameters deviate by a few standard deviations from the expected average. The precise parameters and degree of deviation also aid the system in characterizing the attack.

[3] This feature is scheduled for release during the first half of 2025.

#### 2.3.1.2 Threshold-Based Detection

In threshold-based detection, users can set static traffic thresholds for known attack vectors. Alternatively, the system autonomously learns threshold levels for these known attack vectors. These thresholds are defined per protected object and can be applied to the entire protected object or individual hosts within its address range.

Detectors gather requisite statistical information from telemetry data and transmit condensed reports to the controller. Subsequently, the controller computes network-wide statistics and compares them against the static or learned thresholds. If one or more thresholds are surpassed, a detection alarm is triggered, inclusive of information about the threshold vectors and the attacked IP.

### 2.3.2 Attack Characterization and Mitigation

When the controller receives an attack detection alert, whether from the threshold (by the controller) or zero-day attack detection algorithm (by the detector), it triggers the characterization of the attack to identify the most accurate attack vector(s), especially in the case of multi-vector attacks.

The search for potential vectors occurs within the detector, which maintains telemetry-based statistical information about traffic patterns directed to IP addresses within the router. The detector compares traffic patterns before and during the attack, pinpointing significant differences. This data is sent to the controller, which aggregates information from other detectors. The controller then calculates all attack vectors and sends the corresponding ACL rules back to the detector for implementation, blocking the attack.

### 2.3.3 Attack monitoring and post attack actions

After deploying Access Control Entire (ACE) on the target routers, the system continuously monitors several key metrics. First, it tracks the number of packets matching the deployed ACEs. Second, it monitors traffic destined for the attacked IPs to verify that the ACEs are effectively blocking the attack. If the attack persists, the system will take corrective actions. This may involve modifying the existing ACEs or adding new ones to ensure all malicious traffic is blocked.

Once the system observes a decrease to 0 in packet hits on the deployed ACEs, indicating the attack has subsided, it will automatically remove the attack status and clear the corresponding ACEs from the routers. Importantly, all attack details are stored within the system, allowing for the generation of comprehensive reports, also in PDF format.

## 3. Supported use cases

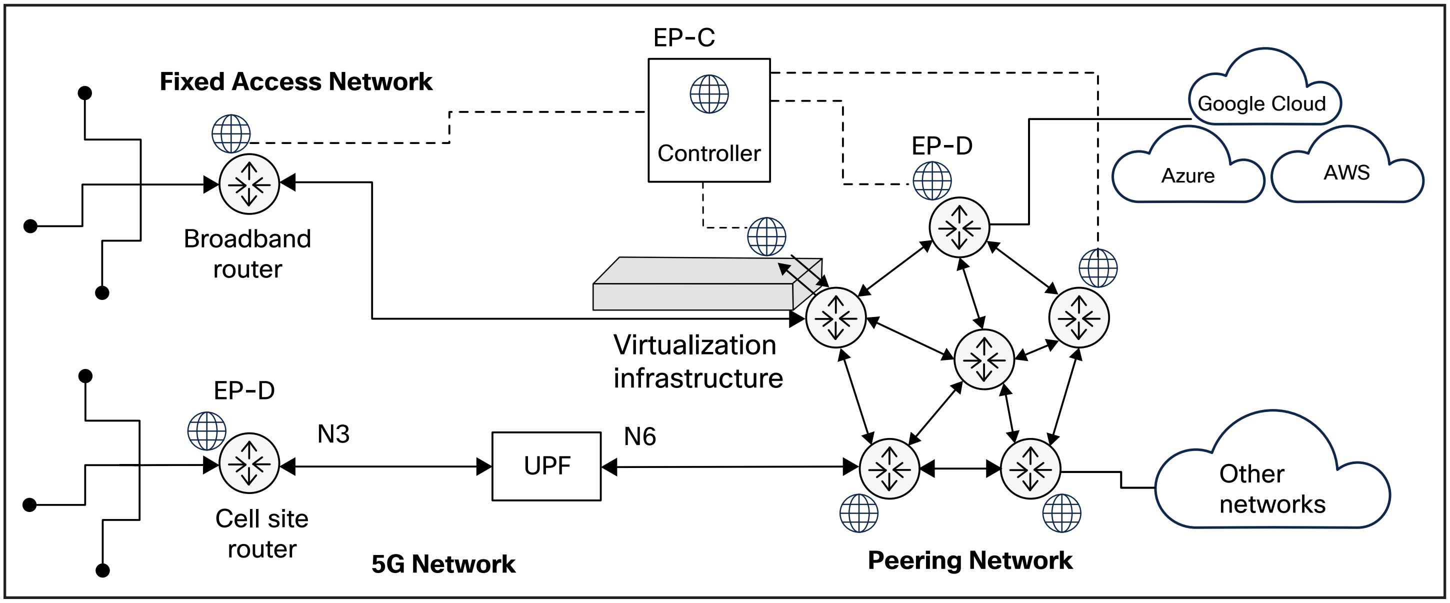


Figure 2. Secure DDoS Edge Protection in the network

The above drawing describes the possible insertion points of the Cisco Secure DDoS Edge Protection into different network locations:

### 3.1 The peering use case

DDoS protection for peering points and internet exchanges isn't new. For almost three decades Communication Service Providers (CSPs) have been using scrubbing centers to clean the "pipes" from malicious traffic. The Cisco Secure DDoS Edge Protection is an innovation brought to scale DDoS protection for the peering edge. The ability to combine both detection and mitigation on the peering routers, for known and unknown attacks, brings an overdue modernization to an ever-increasing challenge.

#### 3.1.1 Problem being solved

In recent years DDoS attacks are growing at a faster rate than internet traffic. According to GCore-Rader report, a quarterly report covering DDoS attacks, volumetric DDoS attack max rates grew at a 66% Compound Annual Growth Rate (CAGR) between January 2021 and January 2023[4]. While according to a TeleGeography report published in 2023, global internet traffic is growing at about 30% CAGR.[5]

This means that in a traditional DDoS defense architecture, scrubbing center capacity should grow about three times faster than the capacity of a network operator's internet exchanges and peering routers. This creates scalability and cost issues. Furthermore, carrying all that malicious traffic into scrubbing centers through the operator network means overprovisioning of the network to accommodate the malicious traffic.

[4] Source: https://gcore.com/library/wp-security-gcore-radar-q3-4-2023

[5] Source: https://www2.telegeography.com/hubfs/assets/product-tear-sheets/product-page-content-samples/global-internet-geography/telegeography-global-internet-geography-executive-summary.pdf

### 3.1.2 Solution

The innovative architecture used by Edge Protection solves the scalability and cost issues for protecting peering edge and internet exchange points. It provides a detection and mitigation capacity that is equal to the routing traffic capacity provided by each router that the solution is installed on. Therefore, network providers no longer need to worry about the mitigation capacity in the scrubbing center. Also, as more peering edge routers are added to the network, detection and mitigation is being added without the need for overdimensioning or creating special routes to and from the scrubbing center.

### 3.1.3 Peering use case infographic

**Peering**

Ensure the availability of services despite constantly evolving threats

**The Challenge**

- Protecting peering against DDoS attacks in complex because of the volume of traffic handled by peering nodes and the range of protocols that perpetrators can exploit to target different services.
- Current approaches using static misuse lists are unable to identify zero-day attacks and protect the network against constantly evolving threats.
- Growing node traffic volumes make traditional DDoS solutions cost-prohibitive.

**How our solution addresses it**

- Gives full visibility over threats by characterizing attacks in real-time.
- Dynamically adapts the mitigation as attack vectors change.
- Offers scalable and cost-effective protection for peering by tackling threats at the edge of the network.

**The outcome**

- Protects peering from attacks and ensures the availability of services, as the volume of traffic handled by peering nodes grows and new threats emerge.

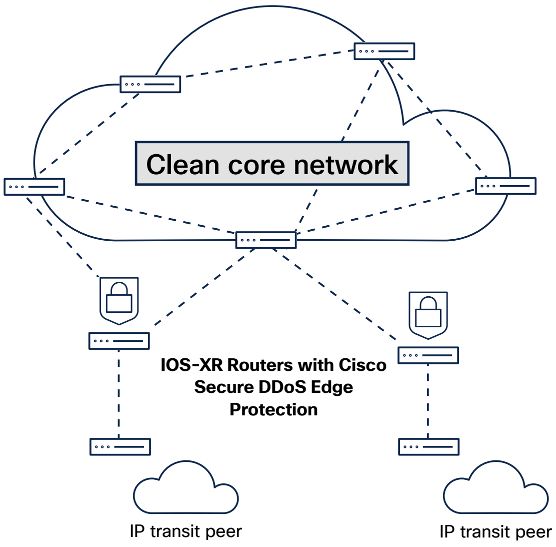


Figure 3. Protecting peering against DDoS attacks

## 3.2 The broadband access use case

The pervasive adoption and continuous growth of streaming TV content over fiber networks in households, coupled with the transition to 4K and 8K content, along with cloud vendors shifting from a highly centralized approach to a “zones” approach, is significantly reshaping the architecture of broadband access networks. This transformation compels network operators to establish local breakouts to accommodate CDNs and localized cloud hosting. Consequently, this necessitates a reevaluation of network security.

### 3.2.1 Problem being solved

The architectural shifts occurring in broadband access networks, wherein novel breakout points emerge with cloud “on-ramp” connectivity on one side and 10Gbps home connection speeds on the other, are altering the attack surface of these networks. Examples of new attack surfaces include:

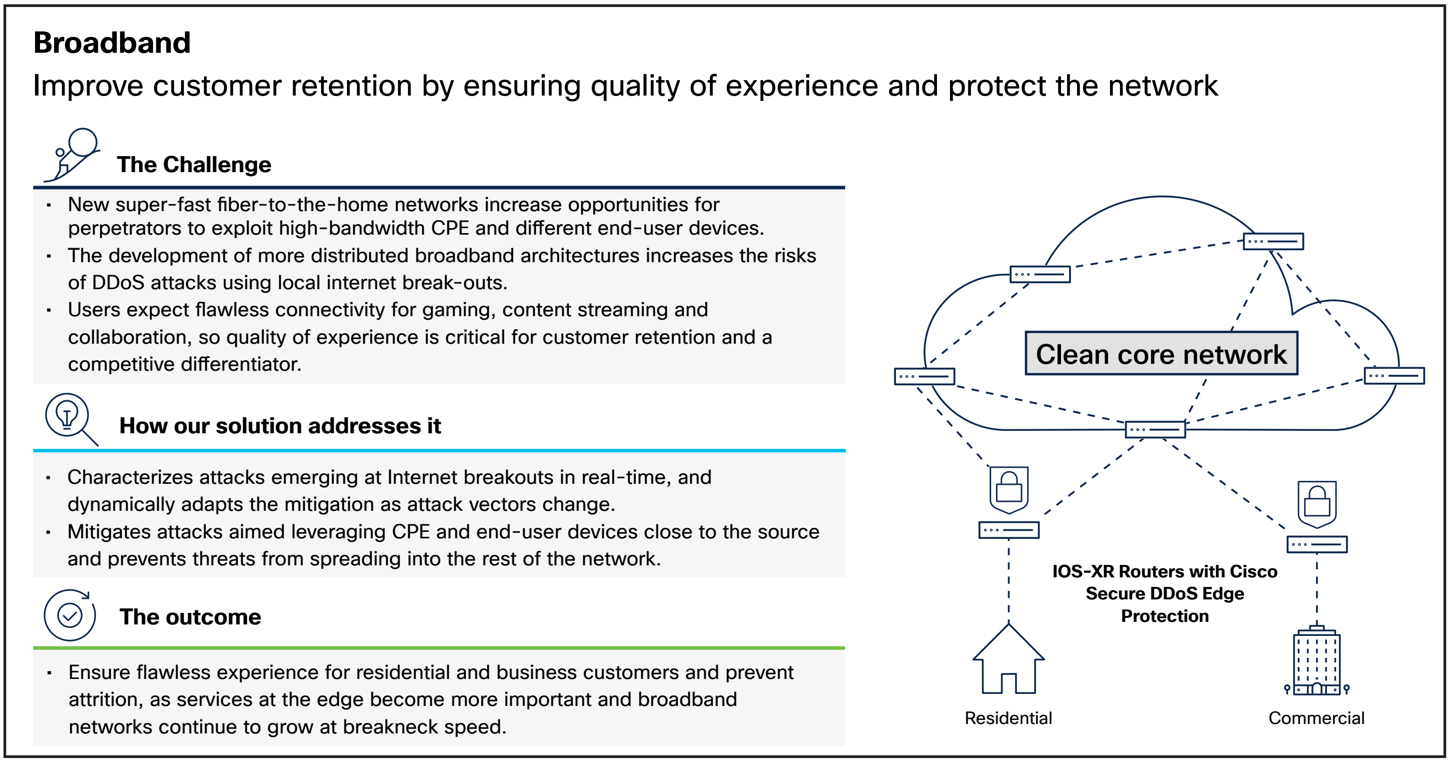
1. Compromised home IoT devices that could be exploited to launch high-volume attacks on network resources or other users.
2. The proliferation of multiple breakout locations with cloud “on-ramp” connectivity and CDN interconnects, resulting in numerous entry points for attackers to initiate assaults, potentially hindering or entirely blocking access to cloud or content services.

Conventional cybersecurity tools developed for broadband access network architectures featuring single or minimal touchpoints with the public internet fall short in addressing the scale required to combat these attack surfaces.

### 3.2.2 Solution

As detailed in the peering use case, the Cisco Secure DDoS Edge Protection solution offers an innovative architecture that tackles scalability and cost concerns. This solution is particularly effective in the context of broadband access networks, where breakout points can number in the hundreds. Moreover, the use of traditional inline appliances not only introduces cost implications but also latency issues. These appliances can become bottlenecks and single points of failure within these networks.

### 3.2.3 Broadband use case infographic



**Broadband**

Improve customer retention by ensuring quality of experience and protect the network

**The Challenge**

- New super-fast fiber-to-the-home networks increase opportunities for perpetrators to exploit high-bandwidth CPE and different end-user devices.
- The development of more distributed broadband architectures increases the risks of DDoS attacks using local internet break-outs.
- Users expect flawless connectivity for gaming, content streaming and collaboration, so quality of experience is critical for customer retention and a competitive differentiator.

**How our solution addresses it**

- Characterizes attacks emerging at Internet breakouts in real-time, and dynamically adapts the mitigation as attack vectors change.
- Mitigates attacks aimed leveraging CPE and end-user devices close to the source and prevents threats from spreading into the rest of the network.

**The outcome**

- Ensure flawless experience for residential and business customers and prevent attrition, as services at the edge become more important and broadband networks continue to grow at breakneck speed.

Figure 4. Protecting broadband access against DDoS attacks

## 3.3 The 5G Network (mobile access) use case

With Cisco Secure DDoS Edge Protection, the security perimeter is pushed beyond the User Plane Function (UPF). This allows the cell site router to become the first line of defense against DDoS attacks from compromised User Equipment (UE) devices.

Deployed on the Cisco NCS 540 router, Edge Protection defends against Internet of Things (IoT) and UE distributed attacks by providing not only full detection, but also granular mitigation capabilities in a small, lightweight containerized package, allowing service providers to ensure access to applications for legitimate users even while under attack.

This is a true on-box solution. The controller simply gives operational control to intervene in an attack and to manage configuration and deployment of the containers. All detection processing and blocking signature creation is done on-box using a containerized DDoS detection engine optimized for the access edge. Only a minimal dataset containing the attack profile and blocking rules are passed to the controller for operator validation/intervention. Once approved, the blocking rule is applied to the router directly for mitigation.

This is a radical departure from how DDoS has been managed in the past. NetFlow no longer needs to be passed to a massive, centralized processing infrastructure. Attack traffic can be blocked in-place and no longer needs to be backhauled to a dedicated scrubbing infrastructure. As we will demonstrate, this is a new approach to DDoS protection, designed to fully meet 5G's hyperscale and latency requirements while also being a lightweight, effective solution.

### 3.3.1 Problem being solved

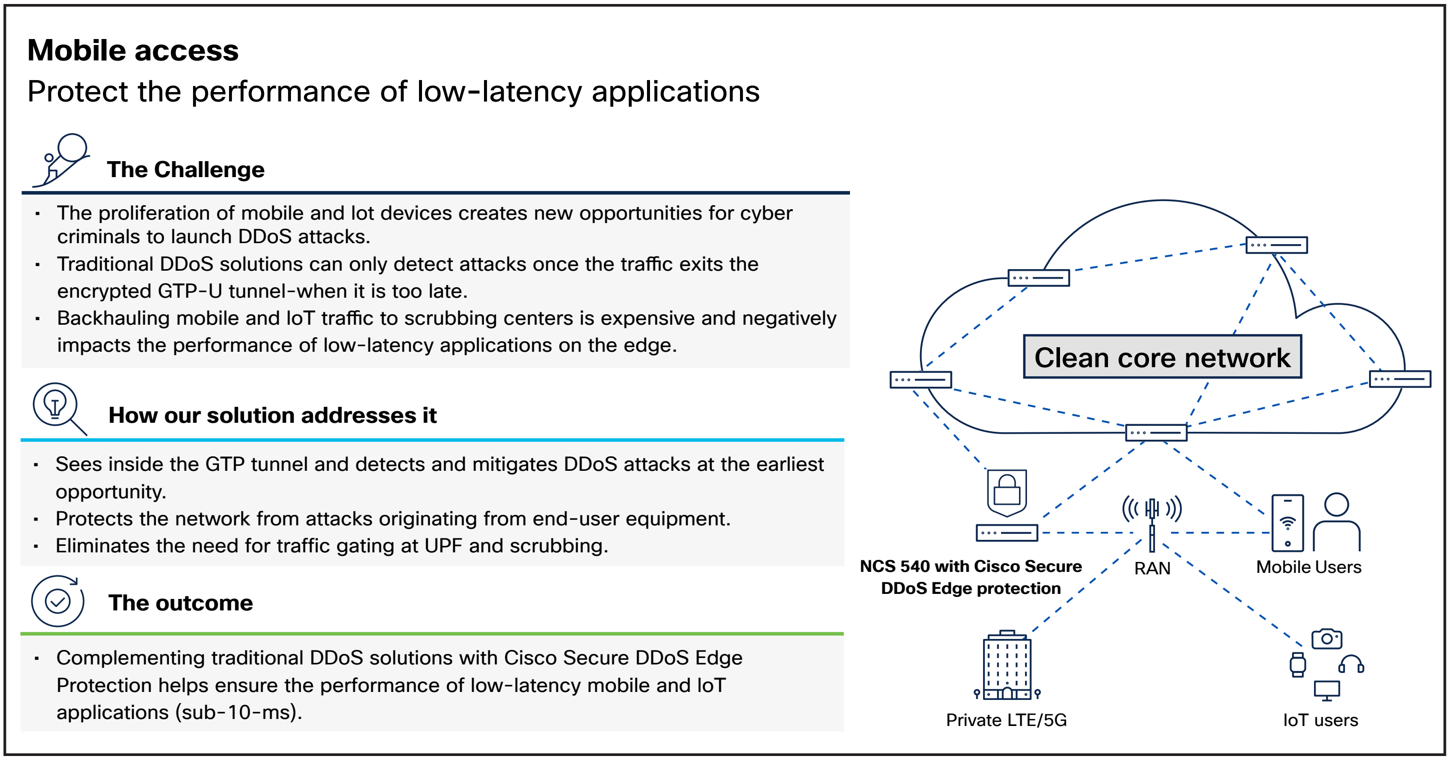
The 5G network includes new features to support new revenue generating applications. For example, a feature like Massive Machine-Type Communications (mMTC) is designed to support high-density IoT connectivity allowing up to a few million IoT sensors per square mile. This creates new opportunities for service providers and enterprises but also brings new hazards because most of the IoT devices lack the capacity to run end-point protection and can be exploited by cybercriminals to launch massive DDoS attack on the network infrastructure.

Ultra Reliable Low Latency Communication (URLLC) is another feature in 5G networks, allowing a round trip time between the user devices and the application of sub-10 milliseconds. To achieve this not only requires enhancements on the radio interface but also creates "local breakouts" using the distributed nature of the 5G network and specifically intermediate User Plane Function (iUPF ); on some occasions the process also uses network slicing. These new architecture enhancements drastically increase the amount of connection points to the internet and to third-party applications and brings with it additional vulnerabilities.

### 3.3.2 Solution

Cisco Secure DDoS Edge Protection for 5G networks is designed to be deployed on N3, N9, or N6 interfaces supporting both GPRS Tunneling Protocol (GTP ) tunneled traffic or regular IPv4/6 traffic. This allows the solution to detected infected UEs, IoT devices, or MEC applications by monitoring traffic patterns and find anomalies. Using the router Access Control List capabilities, the solution can insert dedicated rules to mitigate malicious traffic at the closest point to its origin, thus saving network resources and protecting critical network infrastructure.

### 3.3.3 Mobile access use case infographic



**Mobile access**

Protect the performance of low-latency applications

**The Challenge**

- The proliferation of mobile and Iot devices creates new opportunities for cyber criminals to launch DDoS attacks.
- Traditional DDoS solutions can only detect attacks once the traffic exits the encrypted GTP-U tunnel-when it is too late.
- Backhauling mobile and IoT traffic to scrubbing centers is expensive and negatively impacts the performance of low-latency applications on the edge.

**How our solution addresses it**

- Sees inside the GTP tunnel and detects and mitigates DDoS attacks at the earliest opportunity.
- Protects the network from attacks originating from end-user equipment.
- Eliminates the need for traffic gating at UPF and scrubbing.

**The outcome**

- Complementing traditional DDoS solutions with Cisco Secure DDoS Edge Protection helps ensure the performance of low-latency mobile and IoT applications (sub-10-ms).

Figure 5. Protecting mobile access against DDoS attacks

## 4. Conclusions and next steps

As the adoption of new distributed network architectures continues to expand and the volume of bandwidth and devices on these networks increases rapidly, it opens up opportunities for attackers to exploit vulnerabilities and causes widespread disruptions in critical infrastructure networks. The emergence of new threat vectors underscores the need for a comprehensive, distributed, and adaptive approach to network security.

Cisco Secure DDoS Edge Protection leverages the capabilities of Cisco routers to redefine network security. By harnessing the spare memory and CPU within routers, this solution optimizes resource usage and reduces costs. This approach taps into previously untapped compute resources, enabling the implementation of efficient, cost-effective, and scalable security measures, without the continual addition of extra appliances to the network.

A primary advantage of this innovative approach is its zero-touch deployment capability, which streamlines the setup and management of network security through a unified console. Automation and machine learning reduce the reliance on manual configuration, minimizing operational complexities and resulting in heightened effectiveness, enhanced security, and significant cost savings.

Contact your local Cisco representative today to learn more about how you can begin benefiting from this technology.