The bridge to possible

Cisco Secure DDoS Edge Protection Use Cases Overview

March 2024

Contents

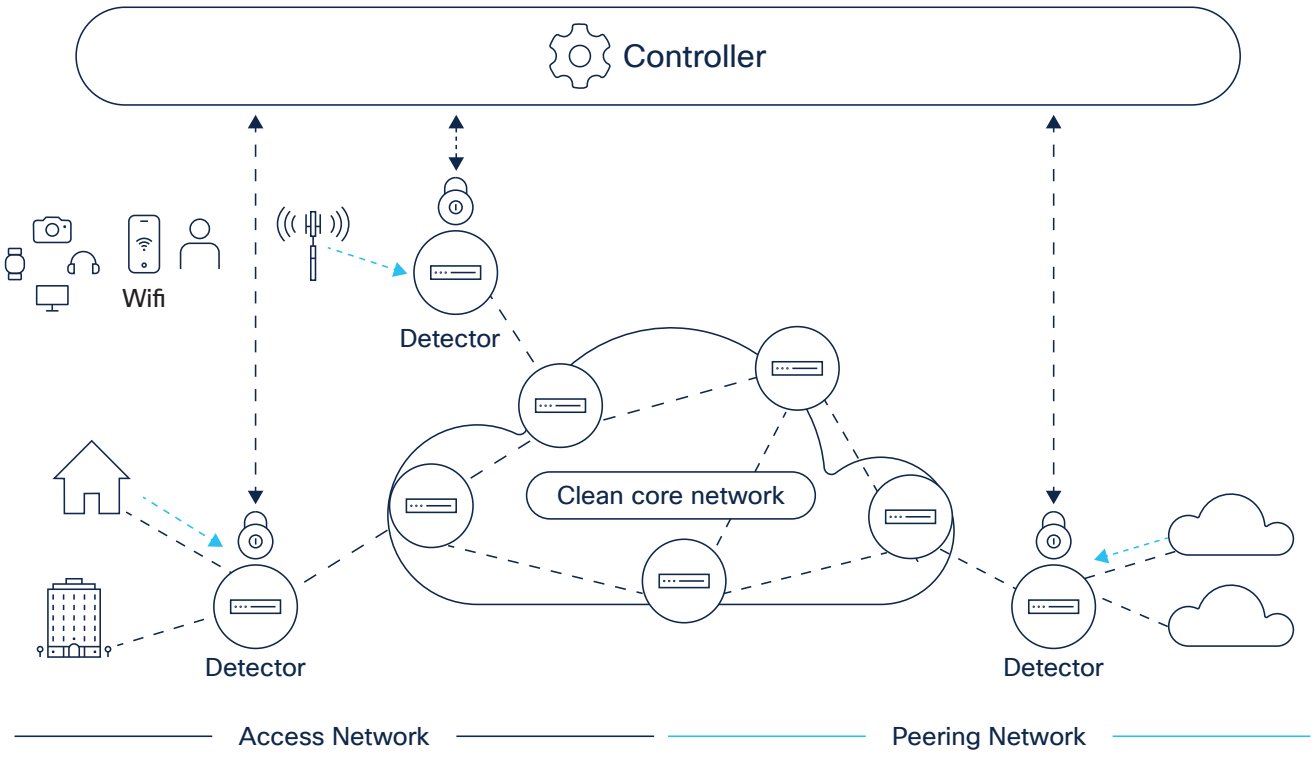
The bridge to possible

1. Introduction

Cisco® Secure DDoS Edge Protection enables communication service providers and others with critical network infrastructure to keep attack traffic off their network by using routers as the first line of defense against DDoS attacks. It is the world's first true on-box distributed-denial-of-service (DDoS) protection solution. It integrates detection and mitigation for zero-day and known attacks with Cisco IOS® XR–based routers. This way, customers can extend DDoS defenses at scale while significantly reducing the cost of DDoS protection compared to traditional solutions. Cisco Secure DDoS Edge Protection enables network operators to scale their DDoS capabilities simply and cost-effectively, as they scale their networks.

1.1 Use cases

Cisco Secure DDoS Edge Protection consists of two software components: detectors on each router and a controller that is hosted on a server (on-prem or in the cloud) to manage up to 50,000 detectors and share protective DDoS signatures across all detectors. The solution can be deployed in different places across the network to ensure the availability and performance of services.



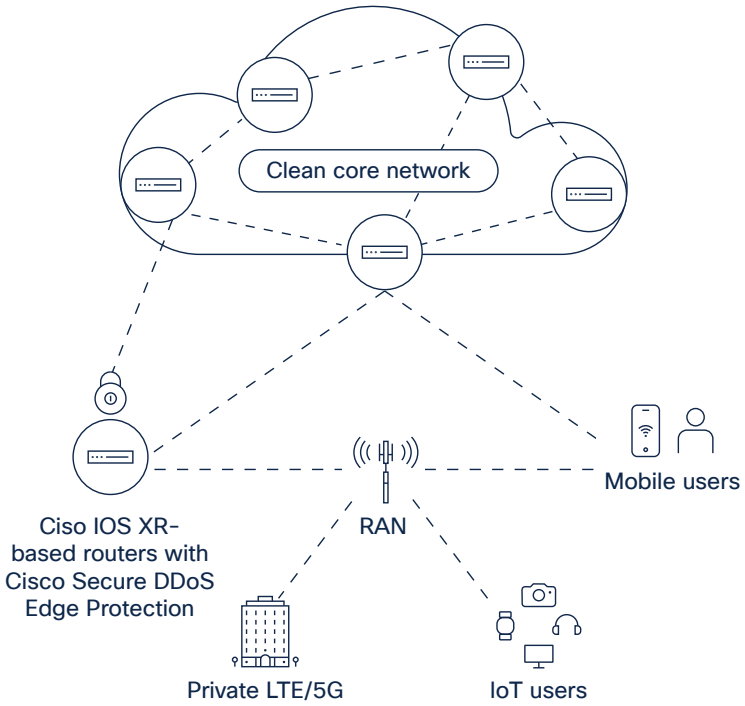
2. Mobile access: protect the performance of low-latency applications

2.1 The challenge

The industry is operationalizing 5G standalone architectures, and mobile networks are becoming highly distributed. Delivering low-latency services at the edge calls for portions of the packet core to be moved as close to the user as possible. Simultaneously, the proliferation of mobile and IoT devices creates new opportunities for cybercriminals to launch massive DDoS attacks, which compromises communication service providers' ability to deliver services securely and with the low-latency user experience that customers have come to expect. This means that security must be moved out to the edge too, so that attacks can be detected and mitigated as close to the source as possible.

2.2 How Cisco Secure DDoS Edge Protection addresses it

Cisco Secure DDoS Edge Protection protects the network from attacks originating from mobile end-user equipment (UE) such as cellphones and IoT sensors with unprecedented depth and efficacy. Deployed on cell site routers, the solution sees inside the GTP tunnel for mobile traffic and inspects UE sessions represented by their tunnel endpoint identifier (TEID). It then blocks an attacking UE based on its TEID using a ternary content addressable memory (TCAM)–based access control list.



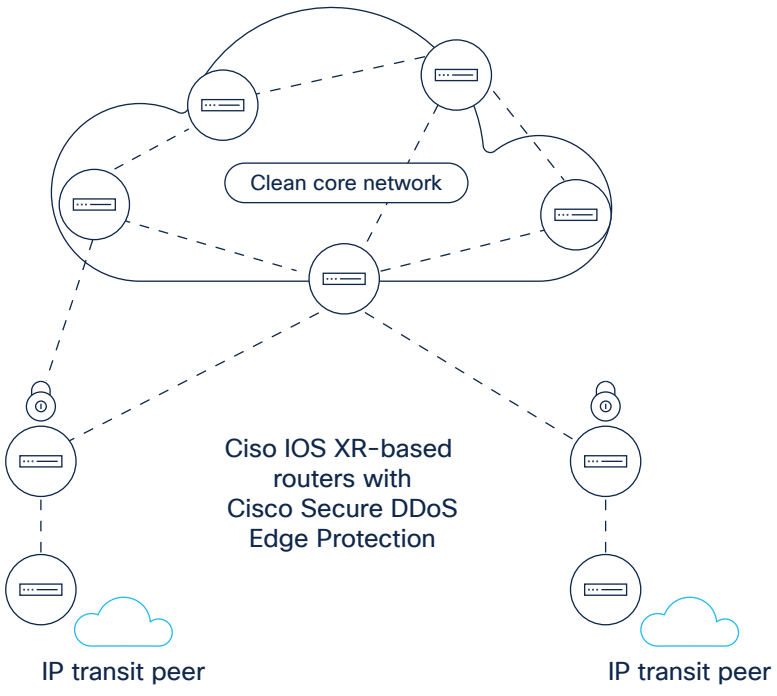
The machine learning capabilities of Cisco Secure DDoS Edge Protection ensure that only traffic from malicious UEs is blocked. By autonomously detecting and mitigating DDoS attacks at the network edge, the solution protects the performance of low-latency mobile and IoT services and prevents attacks from infiltrating applications in the MEC or the packet core.

Applying security in the cell site router to protect the N3 (the path from the cell site router to the user plane function (UPF)) or to protect at the aggregation layer when the N3 is encrypted requires scalability. The centralized controller of Cisco Secure DDoS Edge Protection correlates aggregated telemetry from all cell site routers to scale defenses when an attack occurs and deliver network-wide visibility, detector fleet control, and attack lifecycle management.

3. Peering: ensure the availability of services despite constantly evolving threats

3.1 The challenge

Protecting peering against DDoS attacks is complex because of the volume of traffic handled by peering nodes and the range of protocols that perpetrators can exploit to target different services. Traditional approaches using static misuse lists and telemetry gathered from NetFlow are no longer fit for purpose, because they are unable to identify zero-day attacks and adapt to constantly evolving threats. Additionally, the cost of traditional DDoS defense to keep pace with growing node traffic volumes is becoming unaffordable. That is why communication service providers need a new, highly scalable, and cost-effective approach to protect peering against both known and unknow threats.



3.2 The solution

Cisco Secure DDoS Edge Protection transforms DDoS mitigation and detection by scaling it for the peering edge in a cost-effective way. It gives network operators full visibility over known and unknown threats by characterizing attacks and their signatures in real time. Thanks to Protobuf, Cisco Secure DDoS Edge Protection is able to detect different threat attributes more effectively and mitigate attacks with greater depth. So, as attack vectors change, the solution dynamically adapts the mitigation.

To scale peering policy across the network (and to address issues with BGP flowspec used in traditional DDoS defense), the solution uses Netconf/Yang. Once it detects an attack on a router, its access control list instantly updates, and the controller shares that malicious DDoS signature with all other routers. And, once the attack is over, the access control list is automatically updated to allow access for the blocked traffic. The access control lists of Cisco Secure DDoS Edge Protection are the most sophisticated in the industry, and they are augmented by a user-defined field (UDF), which enables a customized DDoS protection experience for communication service providers.

Cisco Secure DDoS Edge Protection helps communication service providers ensure the availability of services as the volume of traffic handled by peering nodes grows and new threats emerge.

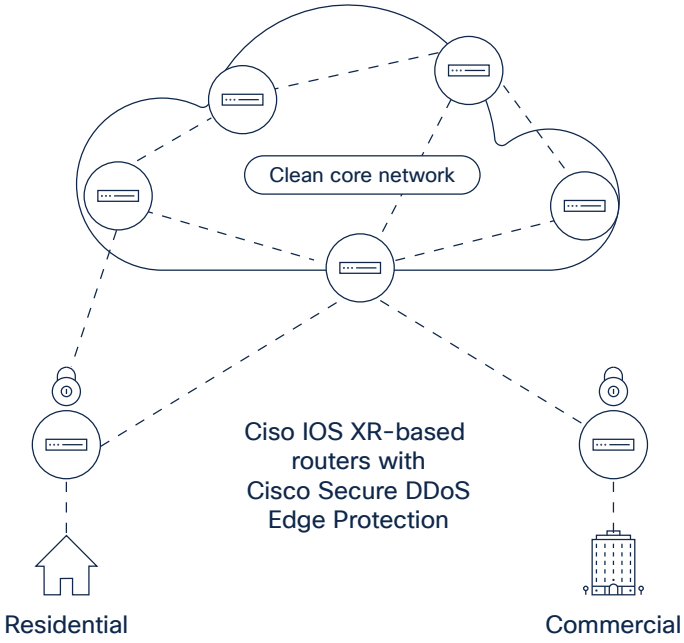
4. Broadband: improve customer retention by ensuring quality of experience

4.1 The challenge

As quality of experience becomes critical for customer retention and a competitive differentiator, communication service providers must prevent network downtime so that they can offer their customers flawless connectivity for gaming, content streaming, collaboration, and other services. Yet, new super-fast fiber-to-the-home (FTTH) networks increase opportunities for perpetrators to exploit high-bandwidth CPE and different end-user devices.

At the same time, the risk of DDoS attacks using local internet breakouts is growing. So, communication service providers need to tackle threats from two directions:

- Attacks originating from CPE and end-user devices and
- Attacks originating from the internet



4.2 How Cisco Secure DDoS Edge Protection addresses it

Cisco Secure DDoS Edge Protection offers bidirectional detection and mitigation against attacks targeting broadband networks. Like with the peering use case, it gives communication service providers full visibility over threats emerging at internet breakouts and mitigates them in real time by adapting to constantly changing attack vectors. Additionally, it prevents perpetrators from exploiting high-bandwidth customer devices to stage attacks. As the solution is deployed on a Cisco IOS XR-based router, one hop away from the broadband network gateway (BNG) shelf where subscribers terminate, it ensures that threats leveraging CPE and end-user devices won't spread into the rest of the network.

As services at the edge become more important and broadband networks continue to grow at breakneck speed, the bidirectional detection and mitigation capabilities of Cisco Secure DDoS Edge Protection ensure a flawless experience for residential and business customers and help prevent attrition.

To learn more about Cisco Secure DDoS Edge Protection,

visit www.cisco.com/go/ddos-edge-protection