cisco The bridge to possible

Cisco Secure Edge Protection

How Cisco is Reimagining DDoS Defense

Mike Geller – Distinguished Architect
@michaelge11er
BRKSPG-2401

cisco Live!

#CiscoLive

Cisco Webex App

Questions?

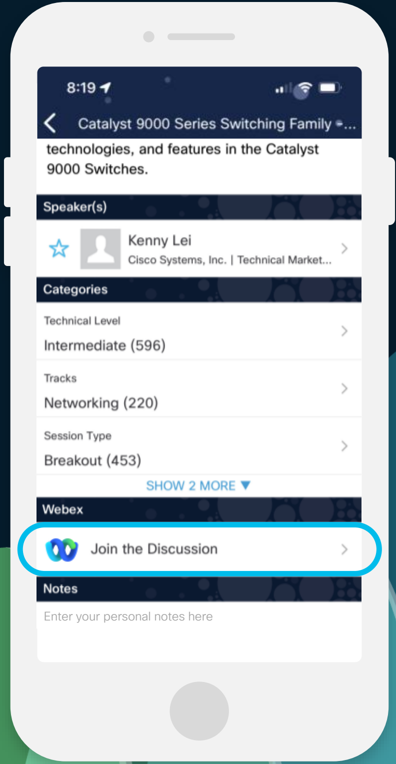
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKSPG-2401



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

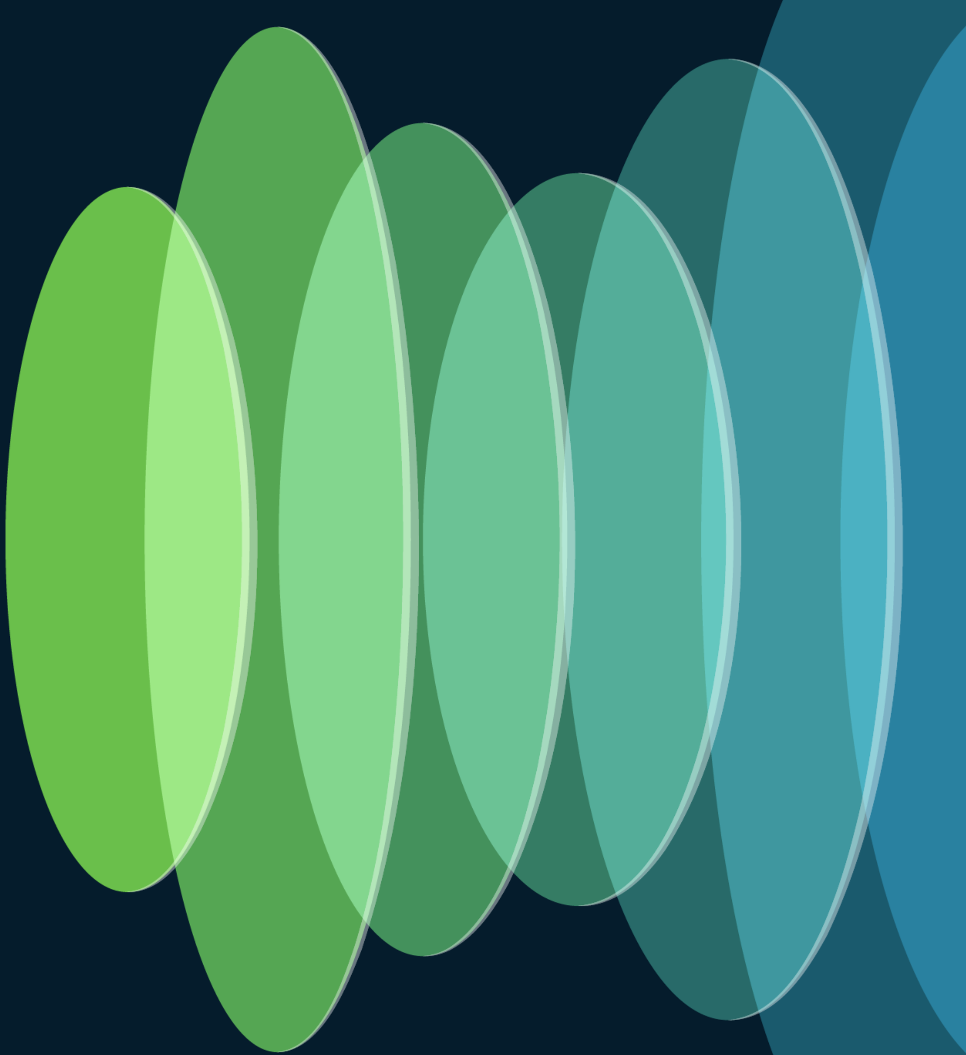
Enter your personal notes here

cisco Live!

Agenda

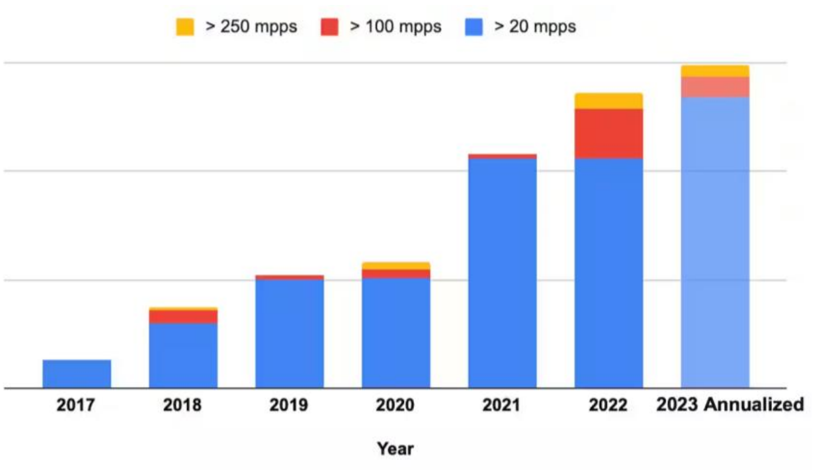
- DDoS and Network Trends
- Why existing solutions fall short for service providers
- What is Cisco Secure DDoS Edge Protect
- How Cisco Secure DDoS Edge Protect solves for Service Providers
- Even more innovation
- Conclusion

DDoS and Network Trends



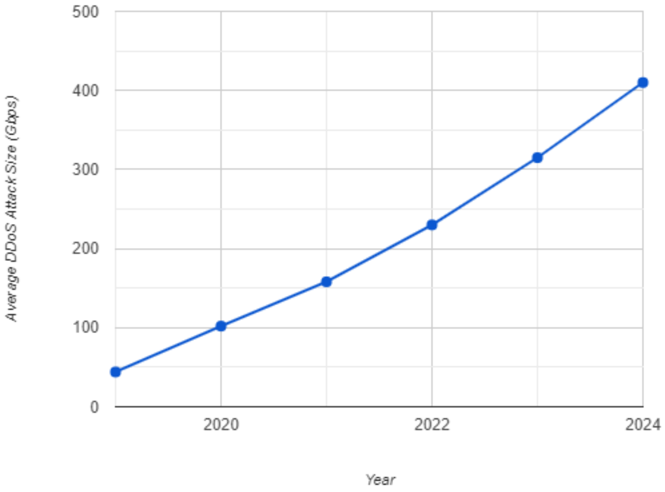
DDoS attacks are growing in bandwidth and frequency

Growth in L3/4 attack frequency



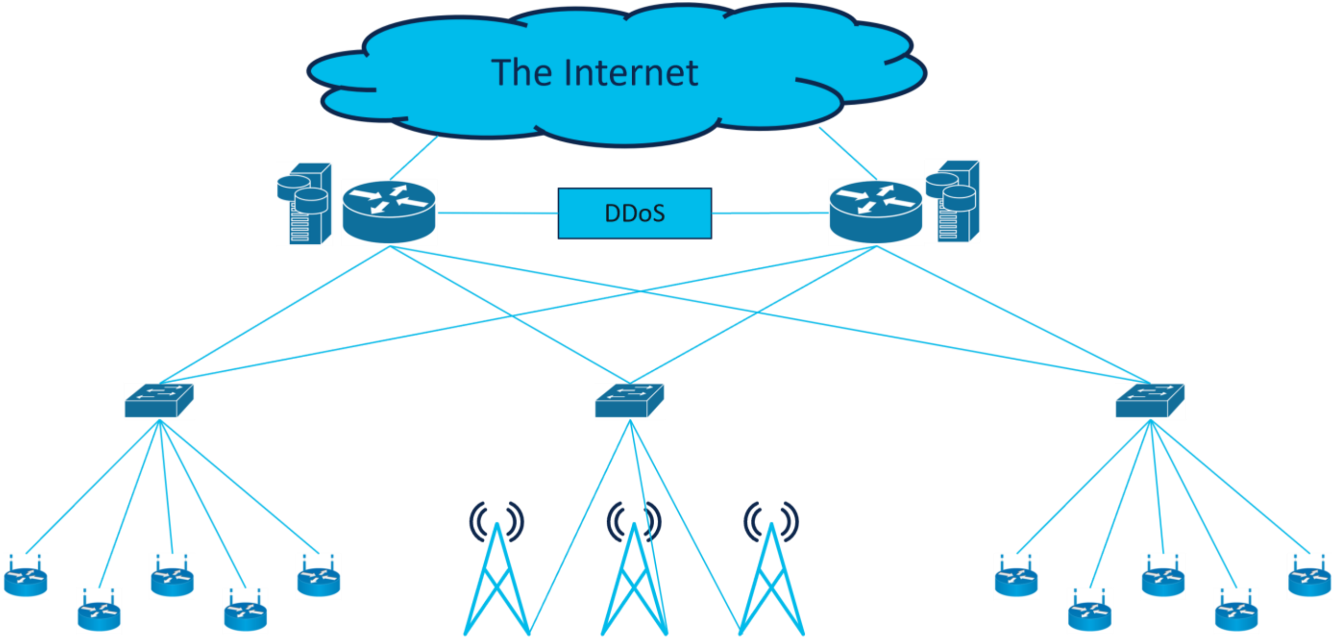
Source: Akamai 2023

Growth in L3/4 attack size



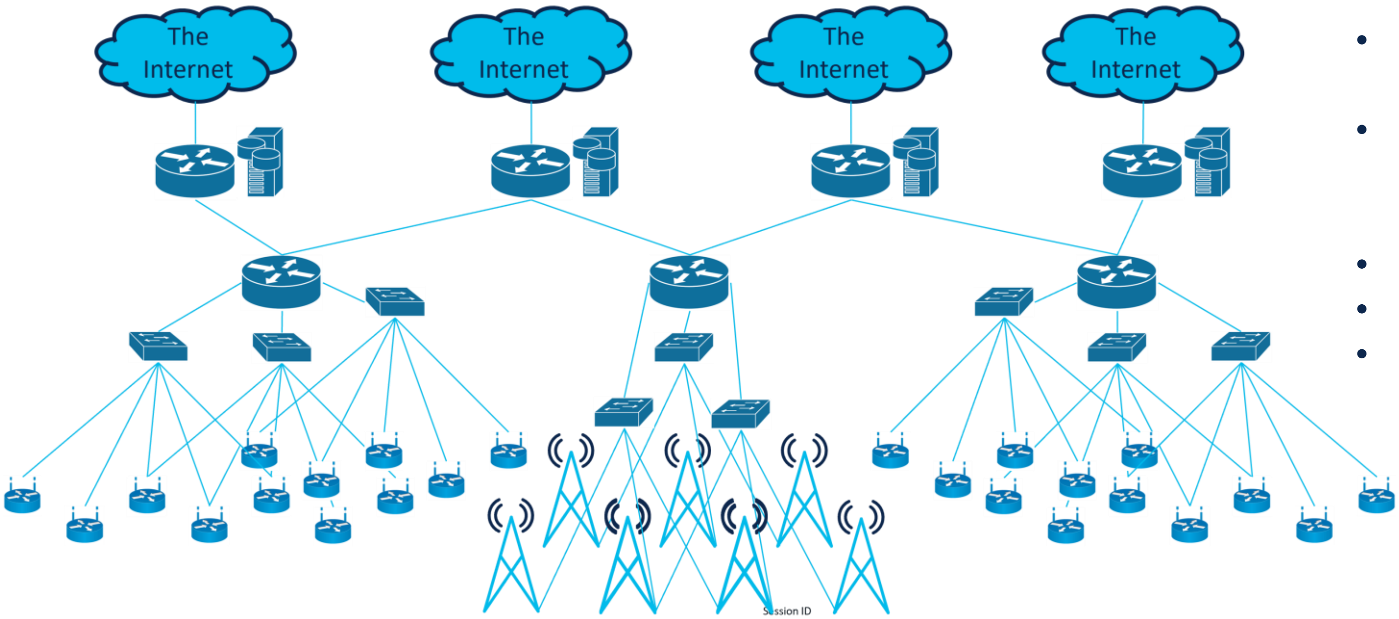
Source: Cloudflare 2024, Akamai 2023, Imperva 2023

Changes in Service Provider Network Architecture



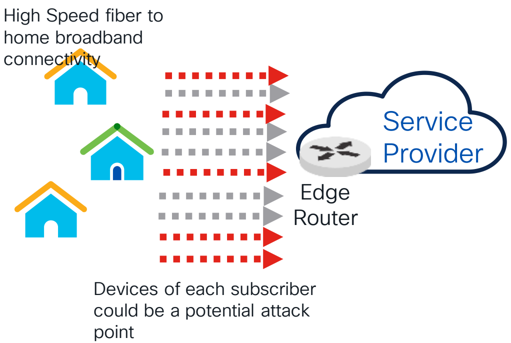
- Network is Central
- Sometimes Local CDN
- Few internet connections

Changes in Service Provider Network Architecture

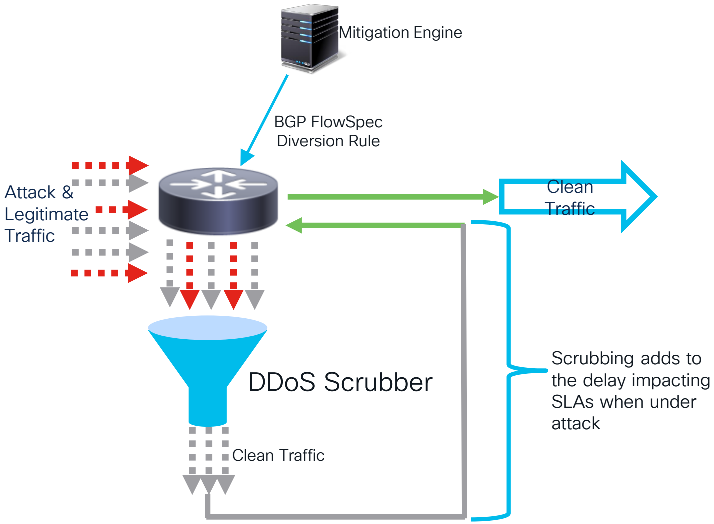


- Network is becoming distributed
- Multiple internet connections and Local breakouts
- New local applications
- Cloud on ramp
- CDNs

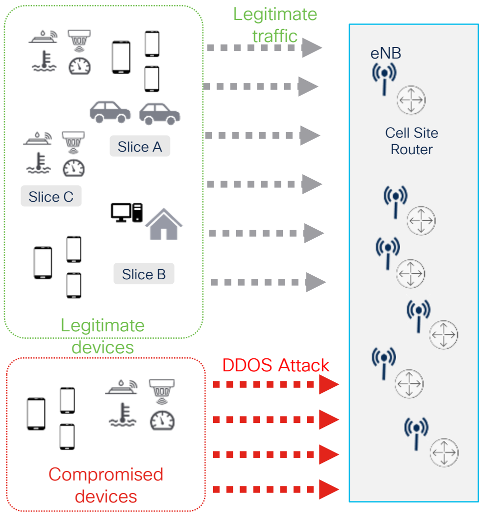
Evolving DDoS Threats & Requirements


High Speed fiber to home broadband connectivity
Service Provider
Edge Router
Devices of each subscriber could be a potential attack point

Protection from attacks originating from SP's own customers/subscribers

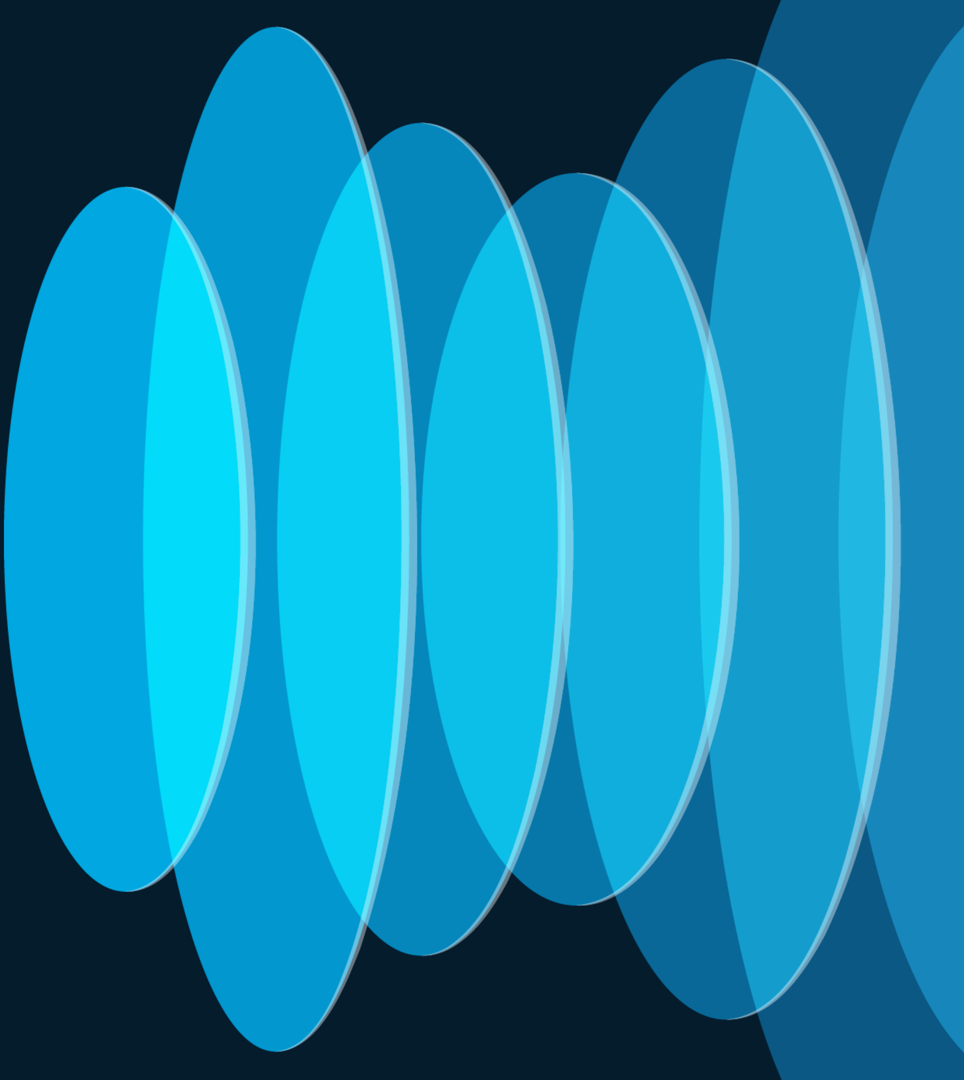

Mitigation Engine
BGP FlowSpec Diversion Rule
Attack & Legitimate Traffic
Clean Traffic
DDoS Scrubber
Clean Traffic
Scrubbing adds to the delay impacting SLAs when under attack

Ultra-low latency requirements for 5G applications must be met even under an active DDoS attack



Increased attack surface due to more IoT and mobile end points connecting to the network

Why existing solutions fall short for service providers



DDoS Defense with Scrubbing

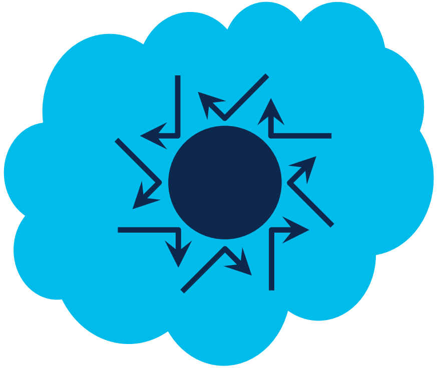
- Detection
  - As networks becomes more distributed collecting Telemetry is more challenging, and central processing is hard to scale, resulting in reducing sampling rates
- Mitigation
  - As DDoS attack grows, scalability becomes a challenge required more hardware, space, power and cooling
  - As networks are becomes more distributed, traffic tromboning adds latency, and requires additional overhead to carry the attack traffic

DDoS Defense with Flowspec

- Detection
  - As networks becomes more distributed collecting Telemetry is more challenging, and central processing is hard to scale, resulting in reducing sampling rates
- Mitigation
  - It is hard to monitor Flowspec rules making it hard to monitor attack lifecycle
  - Flowspec enters BGP tables and act on all packets, making it had to differentiate between different ports on the same router
  - It mandates BGP routing, which in some network segments or topologies is not used
  - Flowspec rules adds additional load into BGP routing engine and consumes routing table memory

DDoS Defense with Cloud based solution

- Detection
  - As networks becomes more distributed collecting Telemetry is more challenging, and central processing is hard to scale, resulting in reducing sampling rates
- Mitigation
  - Per incident business model, is not scalable as attack frequency grows
  - Always-on solution is not practical for service providers and adds latency
  - To and back from cloud traffic should be accounted as well



Traditional DDoS solutions cannot scale with attack trends

Scaling traditional DDoS defense across more distributed networks, carrying exponentially growing volumes of traffic, is cost prohibitive.

Traditional DDoS defense negatively impacts the performance of low-latency applications on the edge.

Protecting networks is becoming increasingly difficult due to the dynamic, multi-vector nature of today’s threats.

What is Cisco Secure DDoS Edge Protect

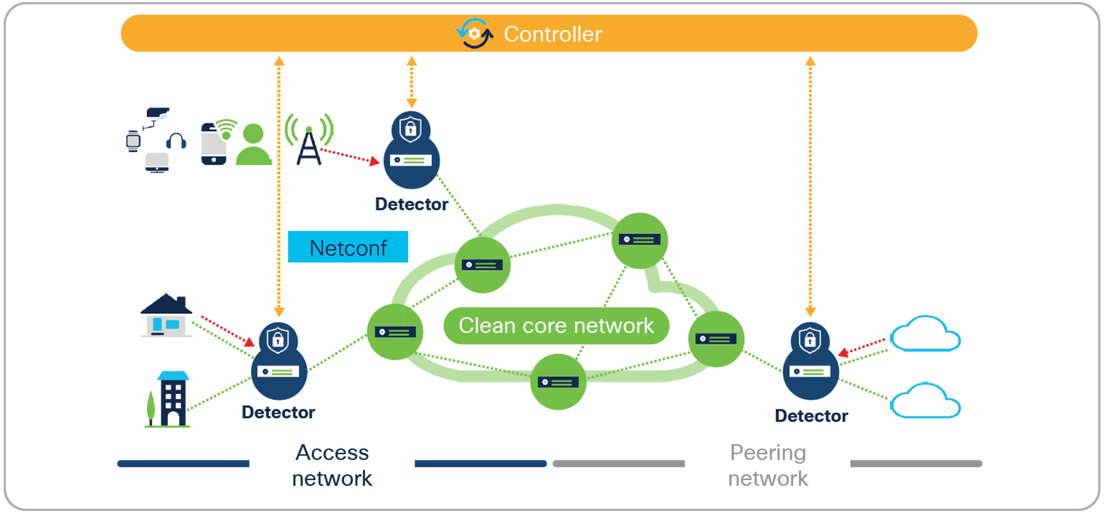
Solution Overview

Detectors

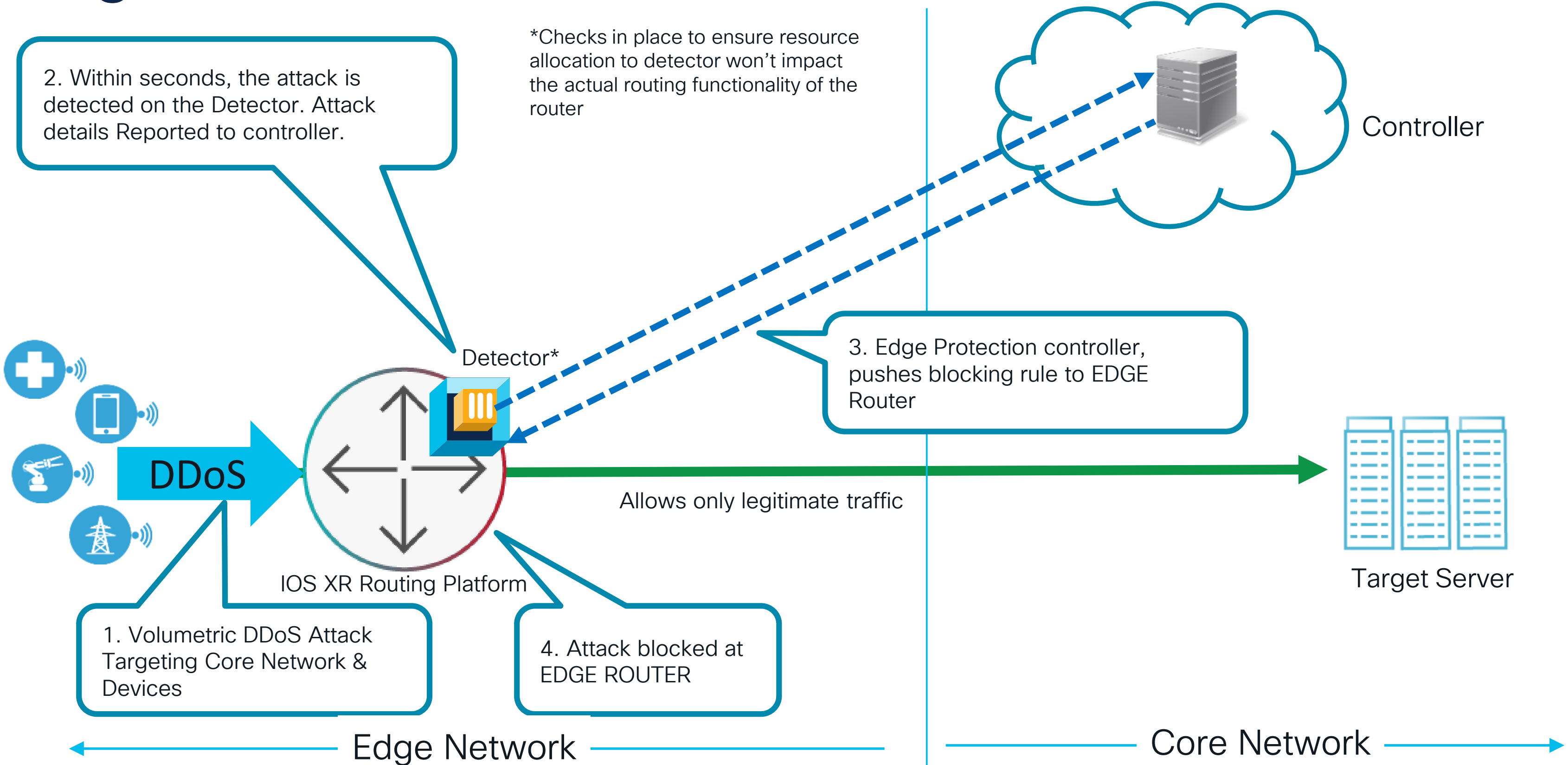
- A container deployed on a router, utilizing dedicated CPU and memory resources, collecting and analyzing network telemetry.
- Employs advanced AI algorithms to detect and mitigate network-borne attacks (DDoS attack, scanning etc.), both at the node level and across the entire network.
- When an attack is detected, a mitigation policy is applied to the router by ACL rules.

Controller

- A modular, containerized design, centrally manages detectors.
- Manages thousands of Detectors/network nodes
- Manages automatically detector’s life cycle – installations, upgrades, security settings and health monitoring
- Manages security functions across the network with a centralized global view - mitigation orchestration, event reporting
- APIs for simple integration with other security management platforms



Edge Protection Solution On IOS XR Routers



2. Within seconds, the attack is detected on the Detector. Attack details Reported to controller.

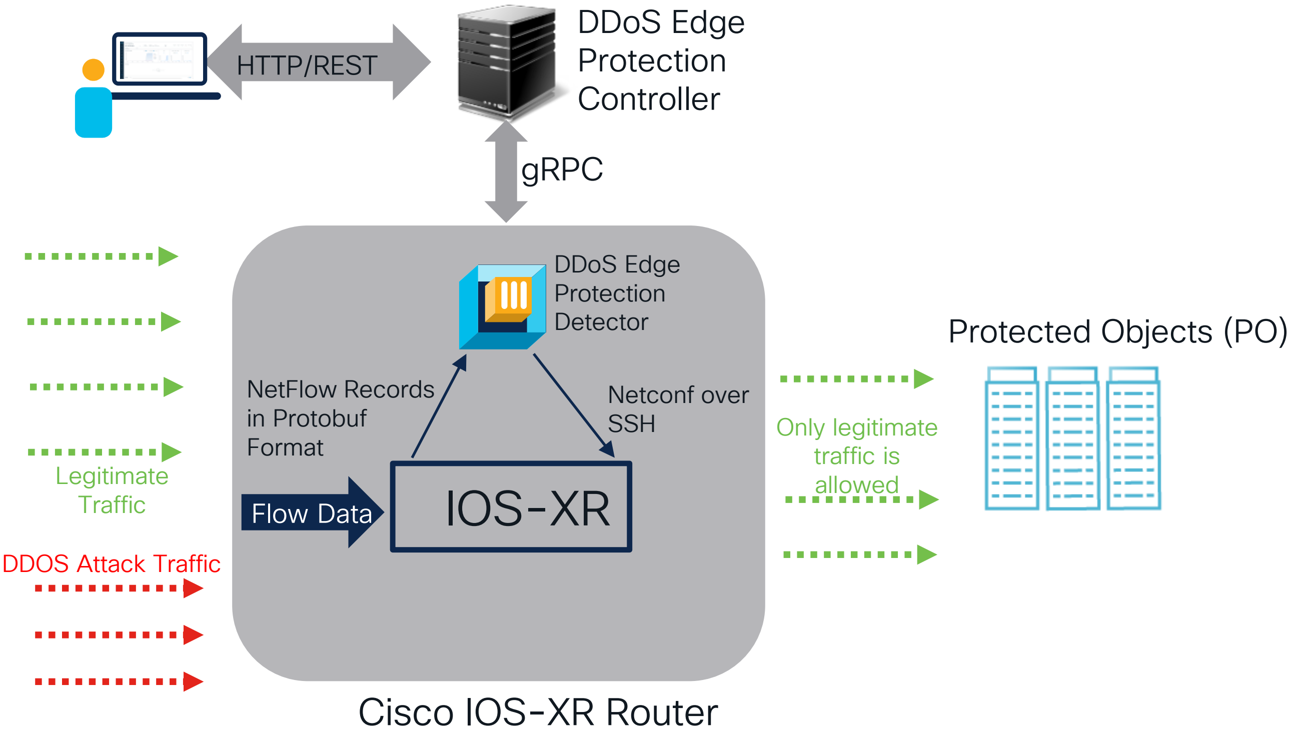
*Checks in place to ensure resource allocation to detector won't impact the actual routing functionality of the router

3. Edge Protection controller, pushes blocking rule to EDGE Router

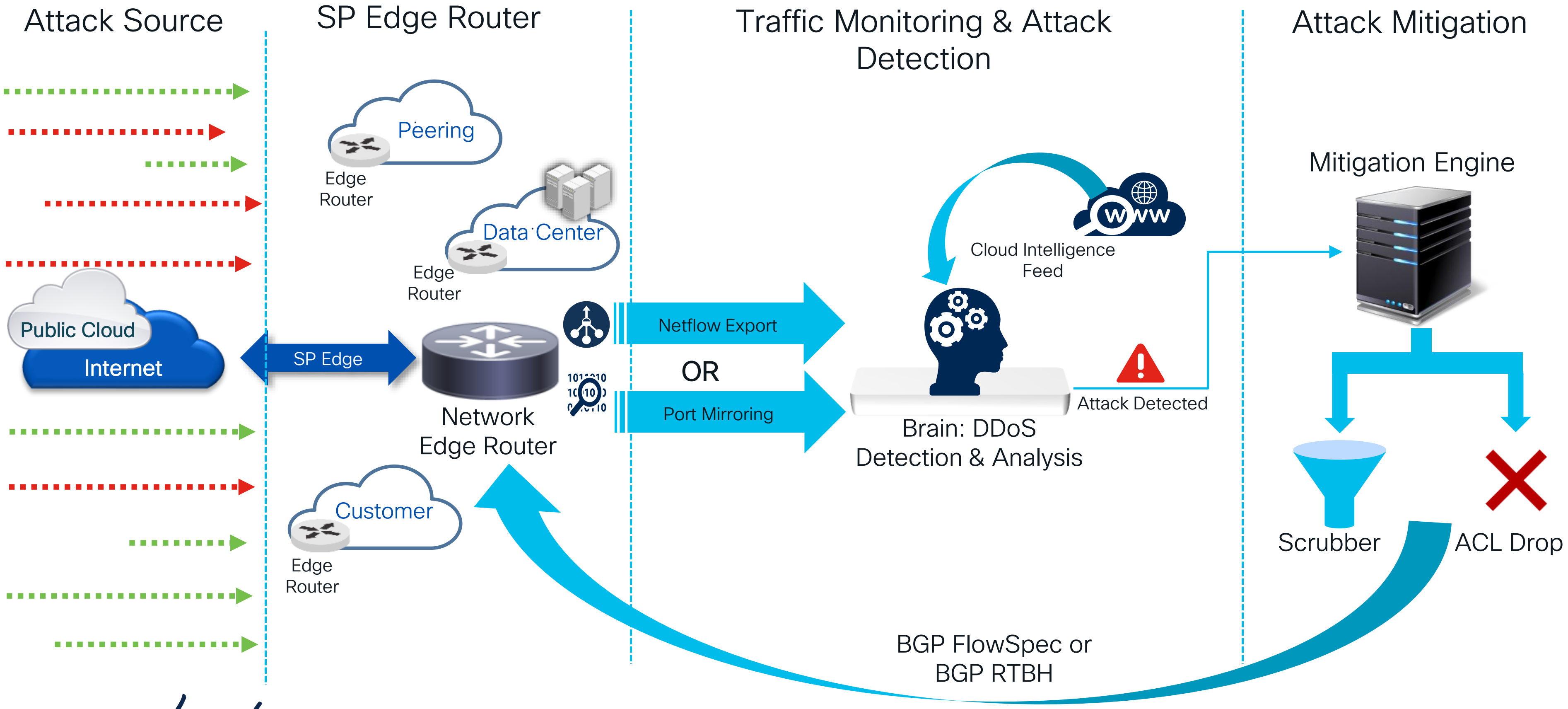
1. Volumetric DDoS Attack Targeting Core Network & Devices

4. Attack blocked at EDGE ROUTER

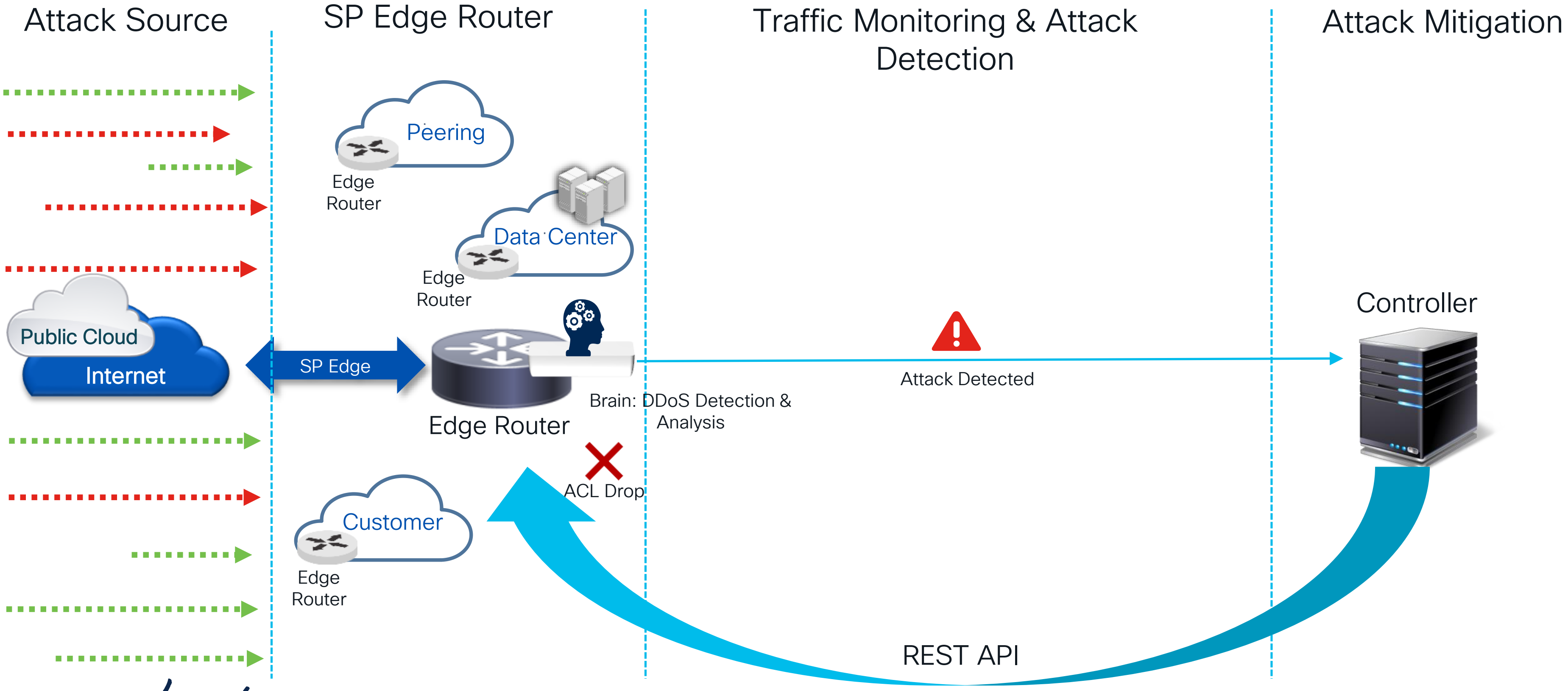
End-to-End Workflow – Router View


HTTP/REST
DDoS Edge Protection Controller
gRPC
DDoS Edge Protection Detector
NetFlow Records in Protobuf Format
Netconf over SSH
Flow Data
IOS-XR
Legitimate Traffic
DDOS Attack Traffic
Only legitimate traffic is allowed
Protected Objects (PO)
Cisco IOS-XR Router

Traditional DDoS Deployment Architecture

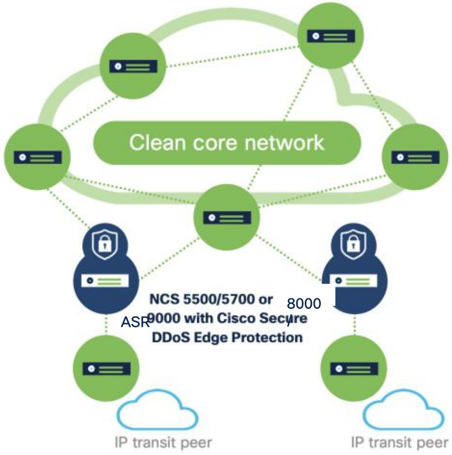


High Level Architecture



Peering Use Case

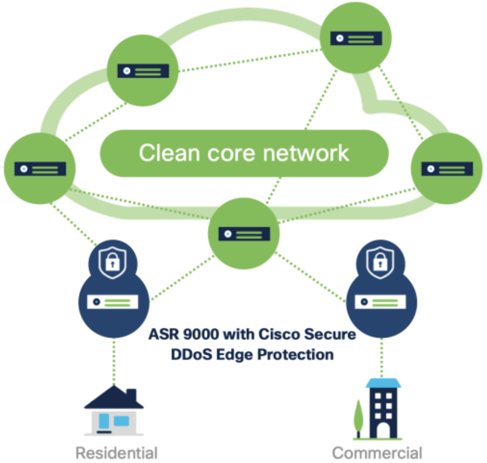
Protect from external threats to ensure availability of services



1. Traditional approaches using static misuse lists, static thresholds, etc. won't scale and results in increased scrubbing costs.
2. With Edge Protection, zero-day attacks can be detected, thresholds can adapt dynamically and reduce the scrubbing costs too.

Broadband use case

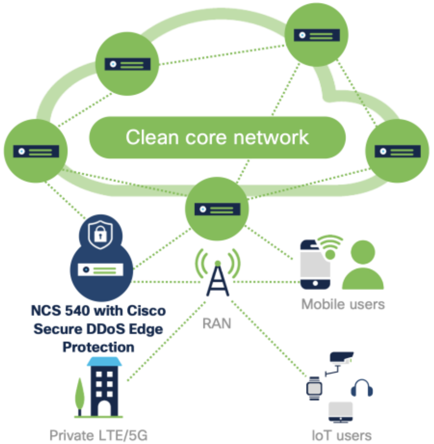
Protect from threats arising out of broadband subscribers & ensuring quality of experience



1. Edge Protection helps in mitigating attacks in both directions as mentioned below.
   a) Service providers can deploy the solution at internet breakouts to protect from external threats like peering use case.
   b) By deploying the same solution on IOS-XR routers next to BNG gateway, threats from subscribers can also be mitigated.

Mobile Use Case

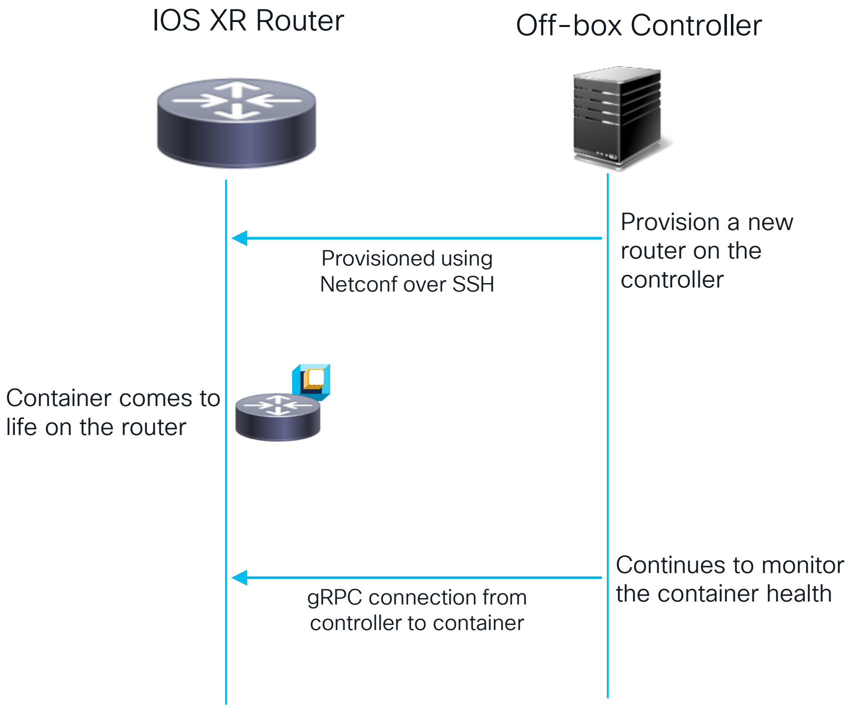
Protect from mobile end point threats to support ultra-low latency requirements



1. Traditional approaches to handle threats from mobile & IoT end points would impact the ultra-low latency requirements for 5G.
2. Edge Protection solution can be deployed on cell-site routers helping with faster detection & mitigation needed for ultra-low latency applications. It also helps in blocking the attackers based on the TEIDs.

Detailed Flows

Provisioning Phase



IOS XR Router

Off-box Controller

Provision a new router on the controller

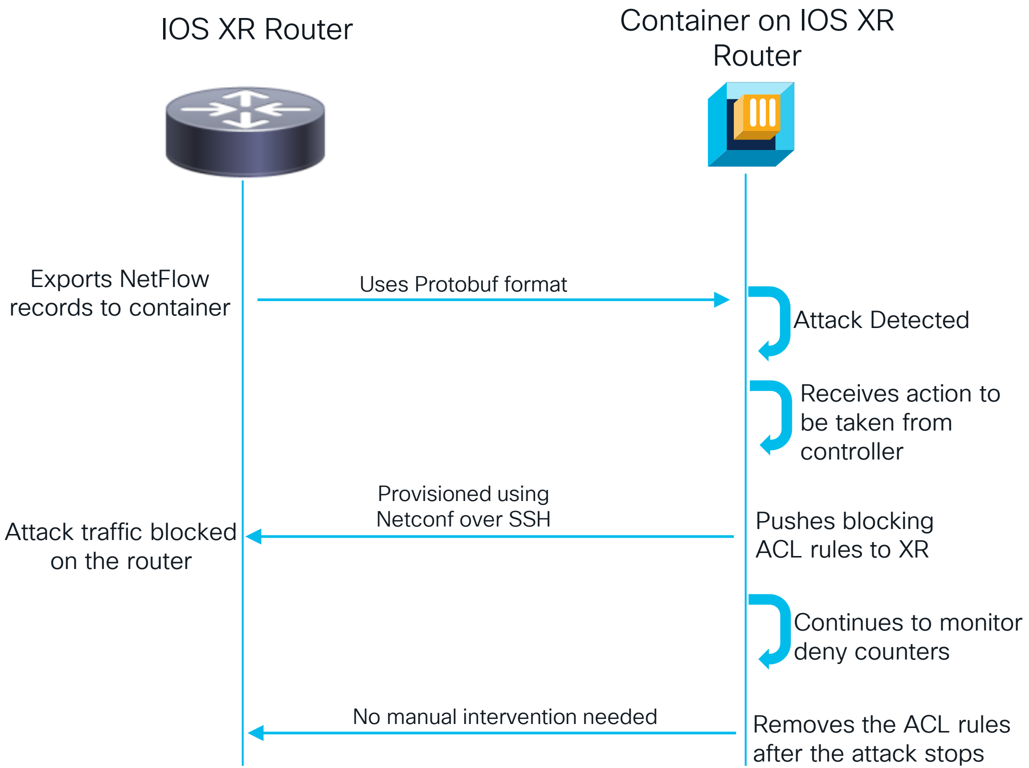
Provisioned using Netconf over SSH

Container comes to life on the router

Continues to monitor the container health

gRPC connection from controller to container

Detection & Mitigation Flows



IOS XR Router

Container on IOS XR Router

Exports NetFlow records to container

Uses Protobuf format

Attack Detected

Receives action to be taken from controller

Provisioned using Netconf over SSH

Attack traffic blocked on the router

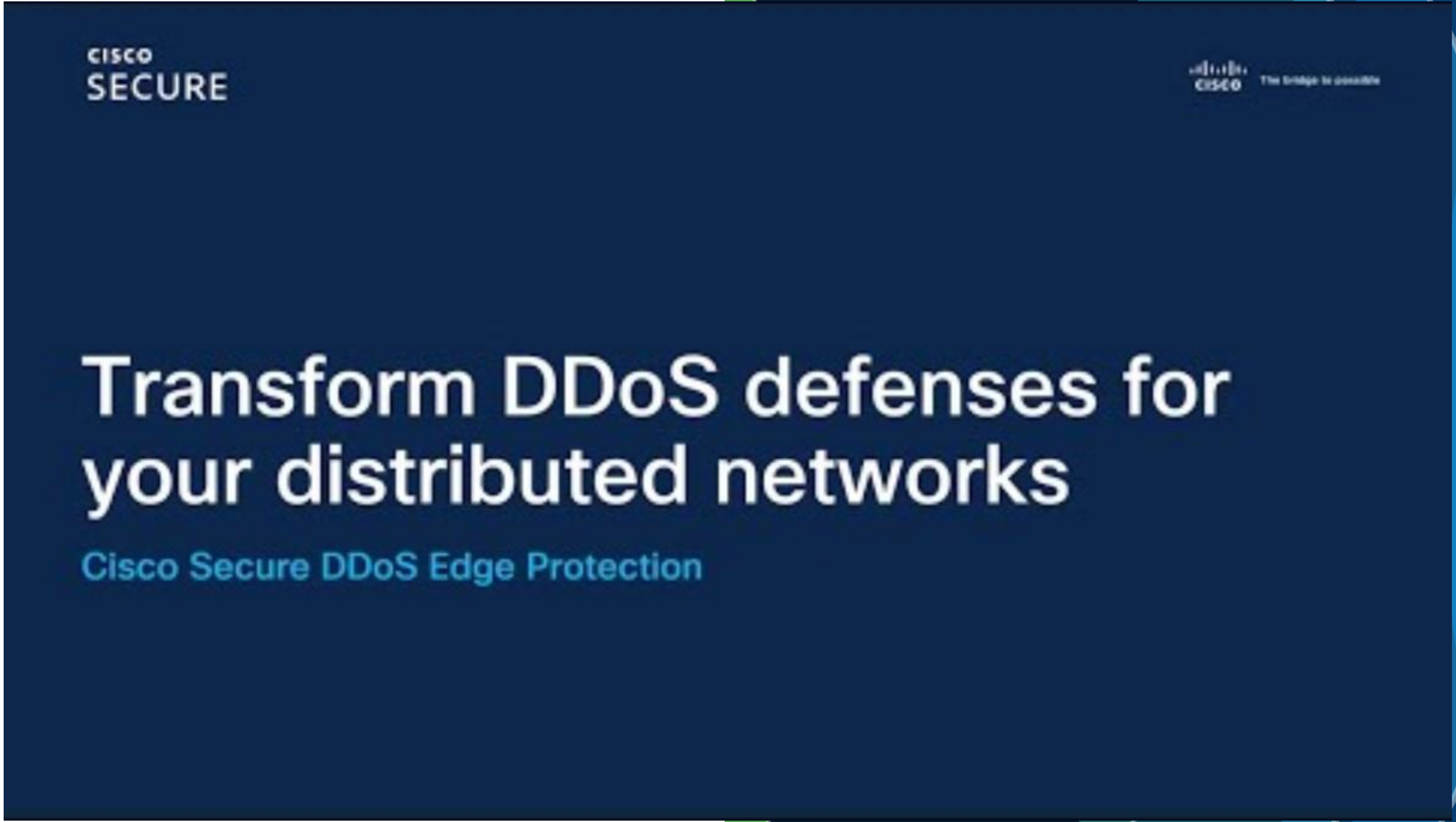
Pushes blocking ACL rules to XR

Continues to monitor deny counters

No manual intervention needed

Removes the ACL rules after the attack stops

Live Demo



cisco SECURE

cisco The bridge to possible

Transform DDoS defenses for your distributed networks

Cisco Secure DDoS Edge Protection

Detection Algorithm Overview
Self Learning Thresholds (Learning)

1. Learning is at the controller level on all data from detectors
2. PO can have a mix of learning and pre-configured filters
3. Learning – Per host within PO, Per PO, both, Parent/Child
4. Learning scheduler – duration, intervals
5. What to expect after learning

Additional Controller Details
Attack Lifecycle Management

1. Helps in detection using the self learning thresholds by aggregating the data from multiple detectors.

2. Supports grouping of detectors across the network based on the deployment scenario.

3. Co-ordinates orchestration of the mitigation policy across multiple detector groups.

4. When a single detector in a group sees an attack, the attack signature is sent to the controller. The controller pushes the mitigation actions to all other detectors that are part of the same group.

5. When an attack stops, the mitigation rule is removed from the group of routers only when the controller ensures the attack has stopped on all the routers that are part of the same group.

6. The detection of attack stop is done by individual detectors monitoring the deny counters of the mitigation rule and sending the stats to the controller.

Additional Controller Details
System Management

1. Provisions the detectors on each of the routers and monitors the detector health.
2. Performs the lifecycle management of all detectors.
3. Supports upgrade of the detectors.
4. Performs user and tenant management.
5. Performs management of the protected objects, setting the thresholds, etc.
6. Supports creation of specific templates for each router or a group of routers.
7. Supports customization to select the number of ACEs that can be used overall for mitigation and the range of ACEs.
8. Once detector is deployed, interface discovery feature can be activated.

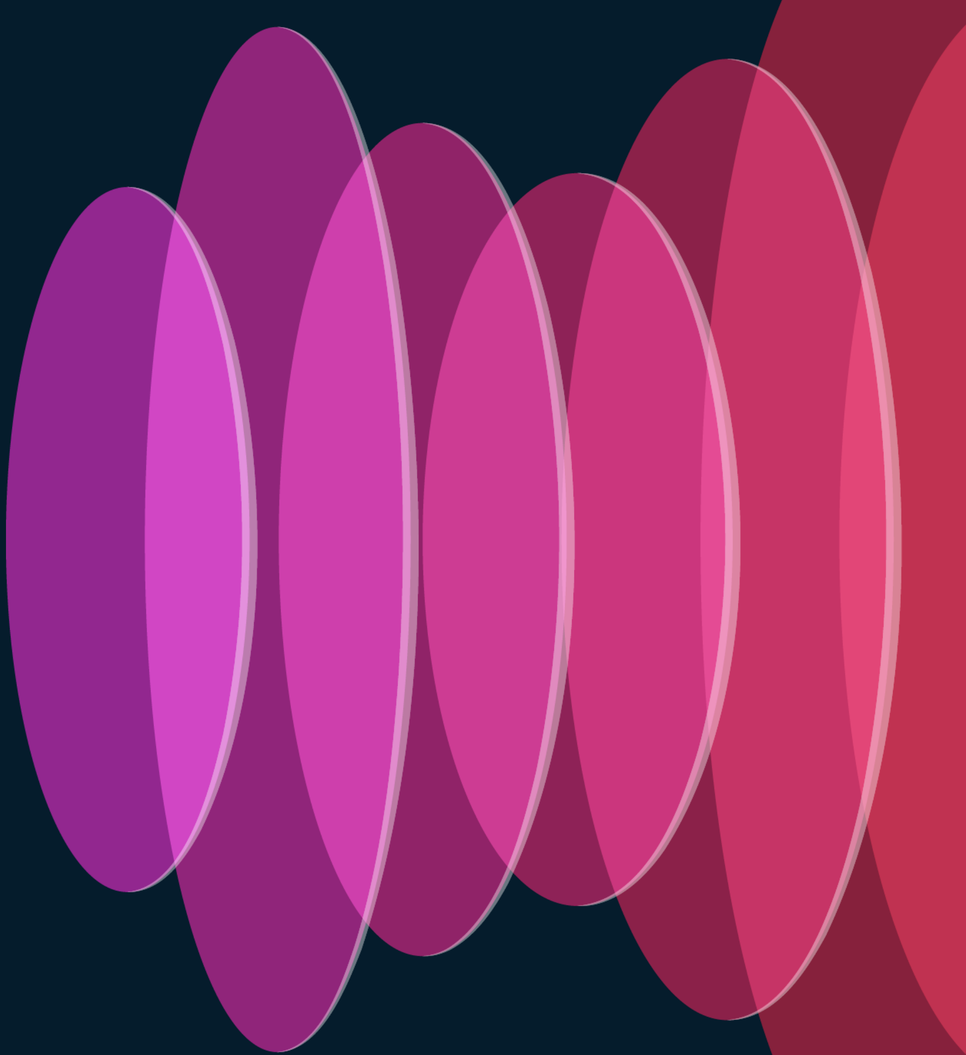
Throughput Test Results

1. Below table shows the test results on a NCS 5508 setup running 7.11.1 IOS-XR image.
2. Traffic was injected through IXIA with traffic ingressing through one LC and egressing through a different LC.
3. Net traffic (ingress + egress together) passing through the system was 2.4 Tbps.
4. The test was carried out with 100% traffic as legitimate and then repeating for 100% attack traffic with similar test results.
5. The RAM used was < 200MB out of 1GB available and CPU utilization didn't exceed 130% out of 200% available.

Flows Per Second (FPS)	Total throughput (Ingress traffic)	NetFlow Sampling Rate	Flows Per Second (FPS) on Detector	CPU(%)*	RAM(MB)
10 million	1200 Mbps	1024:1	10000	25	90
10 million	1200 Mbps	2048:1	5000	20	95
10 million	1200 Mbps	4096:1	2000	10	75
50 million	1200 Mbps	1024:1	48000	130	180
50 million	1200 Mbps	2048:1	24000	70	130
50 million	1200 Mbps	4096:1	12000	30	90
100 million	1200 Mbps	2048:1	49000	130	180

* 2 cores are available for the detector implying we have 200% available for CPU utilization

How Cisco Secure DDoS Edge Protect solves for Service Providers



Benefits of Cisco DDoS Edge Protection

More efficient network operations

- Keep network architecture as is
- Quick and automatic deployment and operation
- Clear separation between network operation and security protection tools – no need for NetFlow or other traffic rerouting

✓

More economical, with lower TCO

- No need for additional hardware, leverages available compute resources on the router
- No need for traffic reroutes to dedicated hosting facilities
- Using Kubernetes and Docker containers to achieve zero touch life-cycle management

✓

Better protection, application performance and QoE

- Block attacks on the edge of the network
- Scales across distributed networks
- Faster response to attacks: the only viable solution for protecting low-latency applications
- Advanced algorithms to deal with zero-day attacks, including multi-vector attacks

✓

Extends telcos’ security posture with a two-layered approach

Extends security posture

- Creating a clean pipe into the telco’s infrastructure
- First line of defense: protecting distributed perimeters from volumetric attacks at the edge
- Protecting flow-based/stateful security components

Complements existing DDoS solutions

- Effectively removing volumetric attacks, cleaning 90% of bad traffic
- Working together with other DDoS solutions
- Integrates fully with Radware DDoS offerings

Summary

The Cisco Secure DDoS Edge Protection Advantage

- Stops DDoS attacks at the ingress of the network
- Reuse existing hardware at no additional cost
- Keep your network architecture as is
- 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 facilities requirements such as power, rack space, and cooling
- Allows service providers to meet low-latency requirements of modern broadband communication

What sets Cisco Secure DDoS Edge Protection apart

- True on-box DDoS protection: **a world first**
- Highest DDoS protection efficacy: **99.49%**
- Fastest time to service restoration: **8-10 seconds**
- Largest number of simultaneous multi-vectors attack: **500**
- **20** years of DDoS defense experience combined with almost **40** years of routing experience

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: mike.geller@radware.com

The bridge to possible

Thank you

#CiscoLive