Secure the Network Edge against the DDoS Attacks

Raja Kolagatla
Senior Product Manager, Provider Connectivity
@kraja80

BRKMSI-1001

Webex App

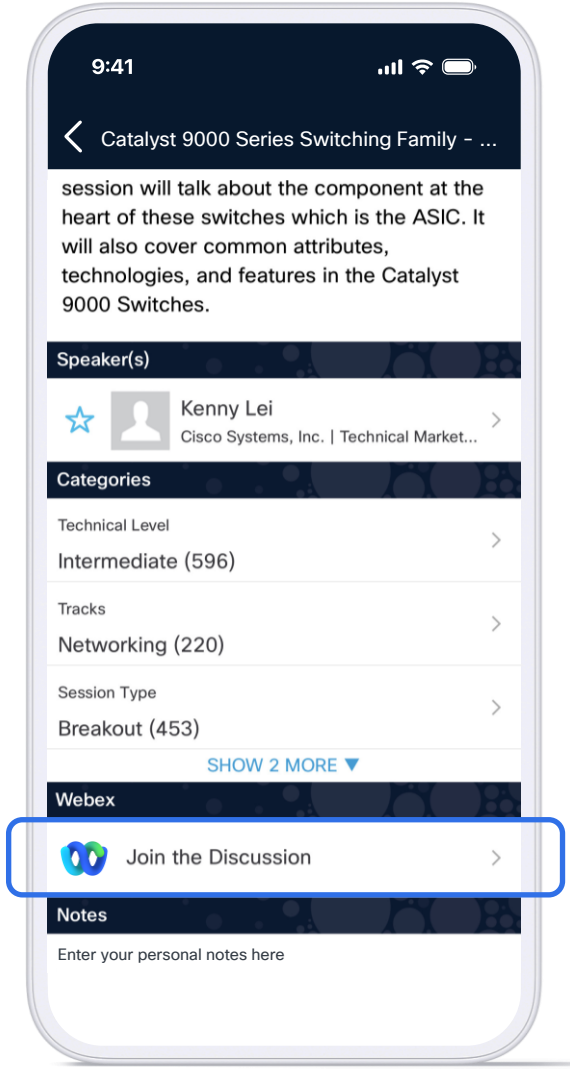
Questions?

Use Webex App to chat with the speaker after the session

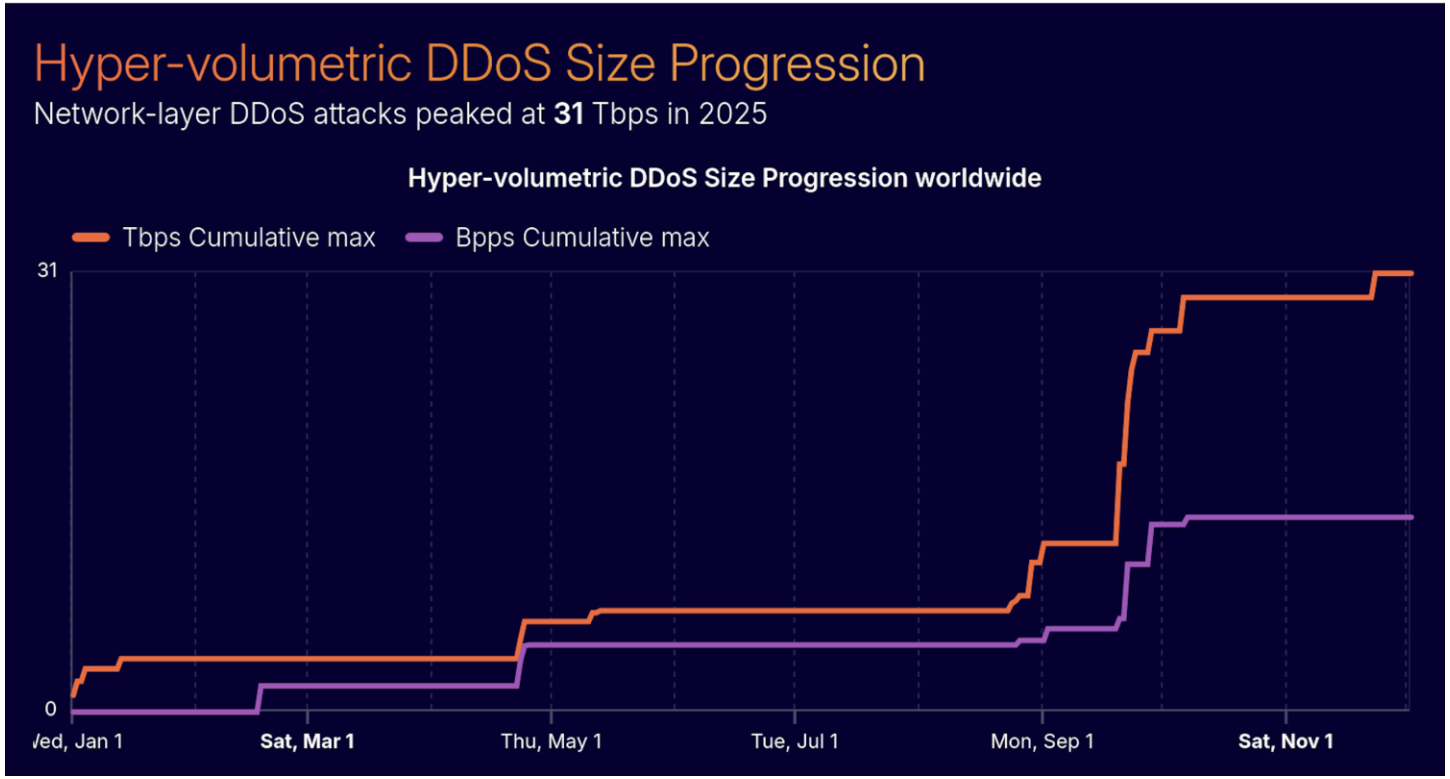
How

1. Find this session in the Cisco Events 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 February 27, 2026.



Why Service Providers need to worry about the DDoS attack(s) now?



DDoS attack traffic against AI companies surged by as much as 347% Month-On-Month in September 2025*

*Source: Cloudflare Reports

Agenda

01 DDoS Attacks Trends – the rise of AISuru botnet

02 Cisco DDoS Edge Protection

03 Work flows, Usecase & the algorithm(s)

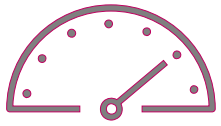
04 MSSP Usecase – Monetize the DDoS Protection offering

05 Customer case study

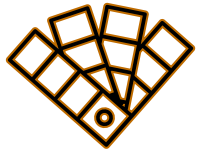
06 Summary

DDoS Attack Trends – the rise of AISuru botnet

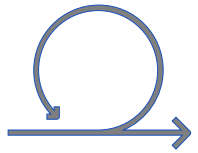
DDoS Attack trends



166% YoY
Increase in DDoS Volume of traffic



Carpet Bombing Attacks
80% DNS-Based
16% Botnets
2% TCP reflection



44%
DDoS attacks observed in 2025 lasted less than five minutes

Residential proxy abuse is on the rise

Surge of AI in DDoS Attacks

Rise in attack traffic volume – Courtesy: AlSuru Botnet

Alsuru

Aug. 2024

- Alsuru **IoT botnet** emerges
- Large-scale DDoS attacks
- Mirai-derived architecture
- Supply chain compromise of IOT

Kitty variant

Oct. 2024

- Simplified protocol
- SOCKS5 proxy support
- Stealth proxying

Alrashi variant

Nov. 2024

- Zero-day exploits
- Proxy services via CPE Routers
- Large infrastructure attacks >6Tbps

Kimwolf variant

Aug. 2025

- Botnet compromising Android devices
- Uses residential proxy SDK architecture
- 2 Million devices infected

Compromised Devices

IOT Devices

IOT Devices

Enterprise/CPE routers

Android devices

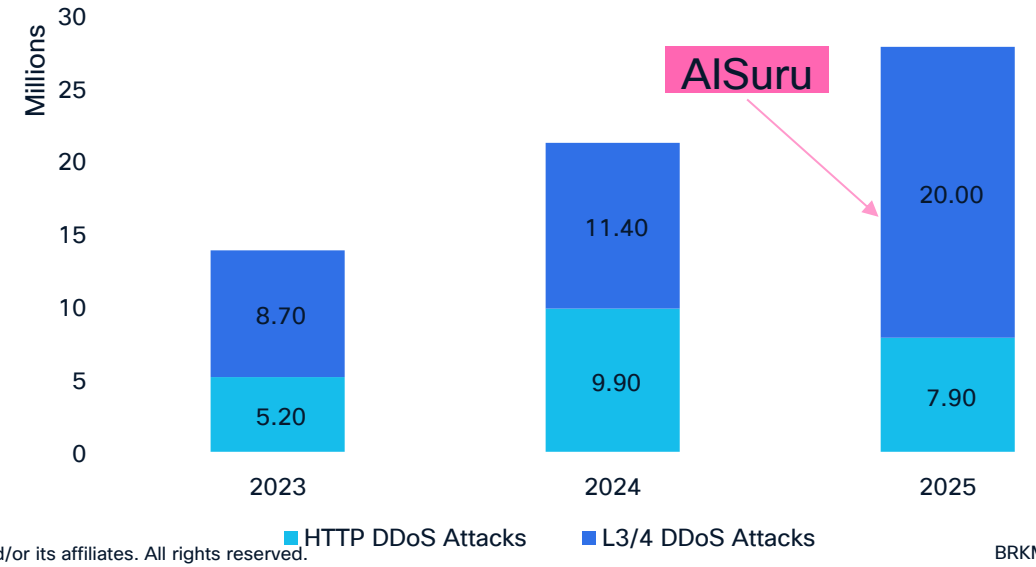
cisco

Why AISuru emergence is seismic shift in the DDoS Landscape?

Normalization of "Hyper-Volumetric" Scale

The "Residential Proxy" Camouflage

Collateral ISP Disruption



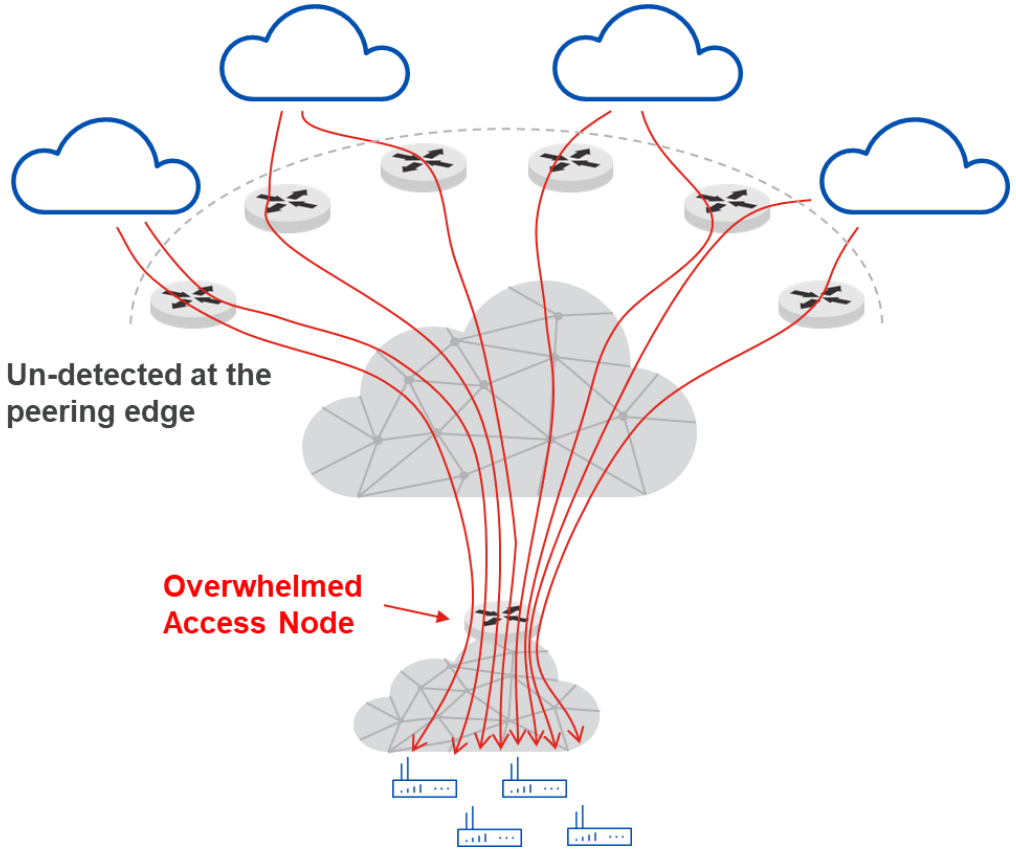
AISuru Havoc

- Largest attack to-date: 31.4 Tbps (Layer 4 DDoS) / 14.1 billion packet-per-second (Bpps)
  - Request rate: 200 Million requests per second (rps)
- Unique attack patterns:
  - Aggressive Pulse Attacks
  - Pernicious Carpet Bombing

Carpet Bombing

Exploiting weaknesses of traditional solutions to create a distractive undetected DDoS attacks

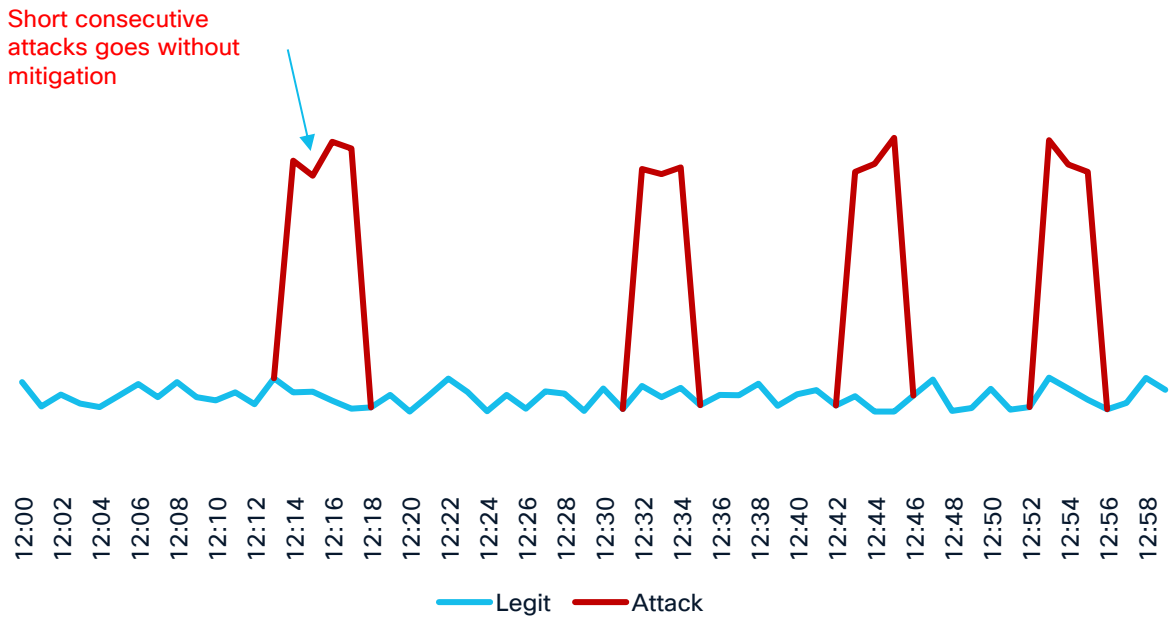
- Targets 100s of IPs in the same prefix with low-rate attack traffic
- Evades detection by avoiding volumetric thresholds
- Traffic aggregates at access routers/nodes, overwhelming them
- Causes collateral damage even if individual hosts seem unaffected
- Can trigger a domino effect, taking down network segments



Pulse attacks

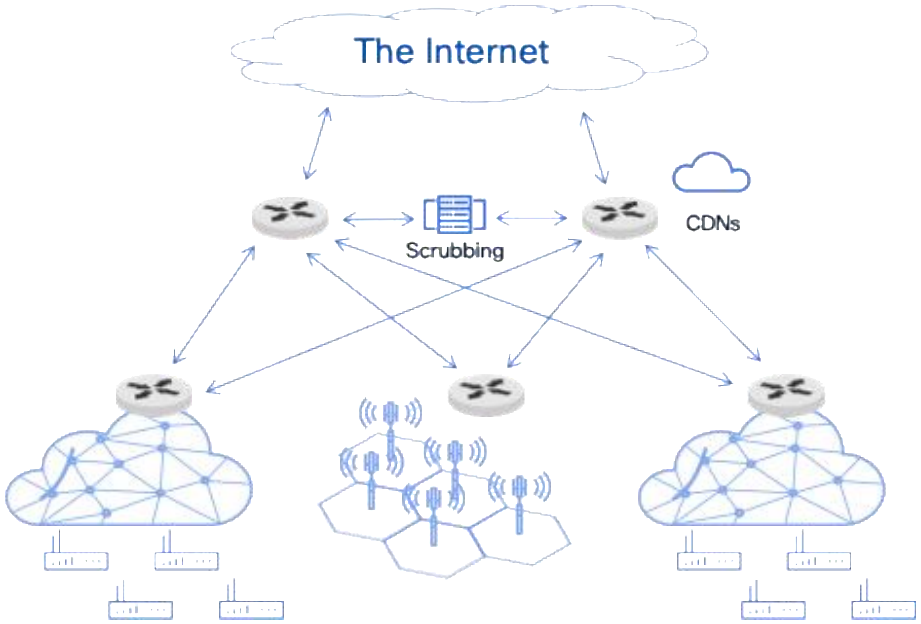
Exploiting weaknesses of traditional solutions to create a distractive undetected DDoS attacks

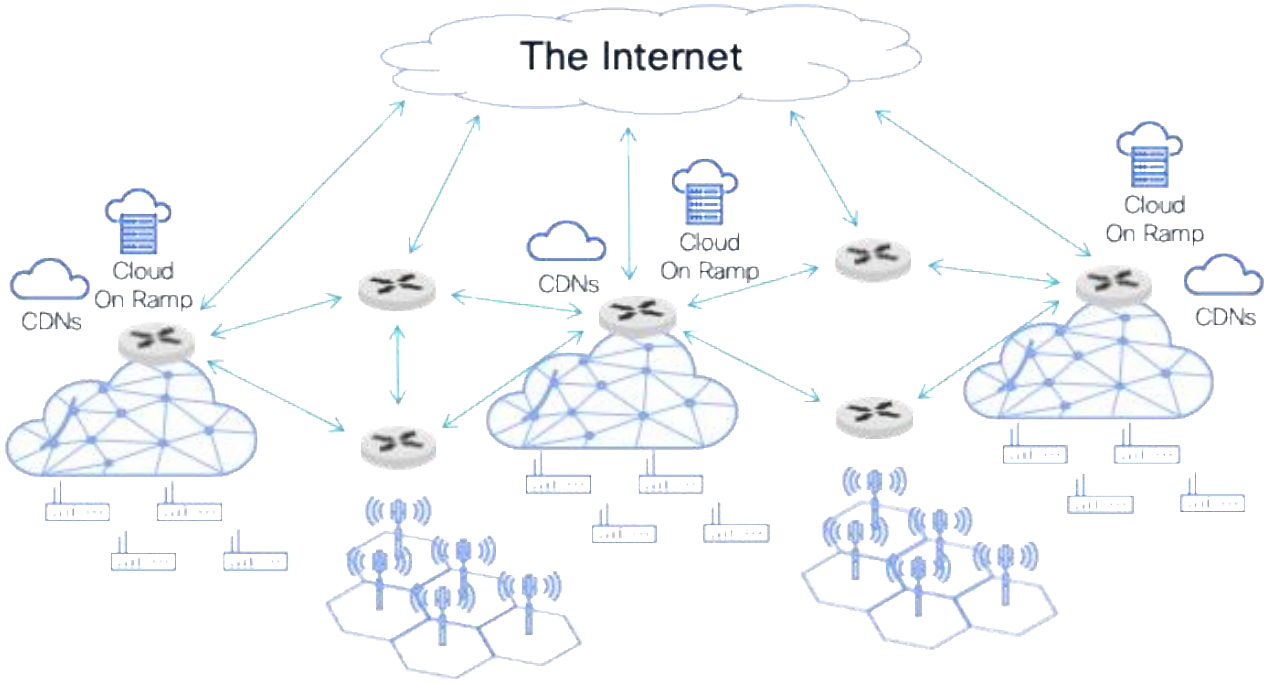
- Sending a short high volume attack traffic to a single host
- Evades mitigation, attack lasts 3 minutes
- Short wait, attack again a different host
- Causes collateral damage to individual hosts and network elements



Evolution of service provider network architecture

From centralized to distributed





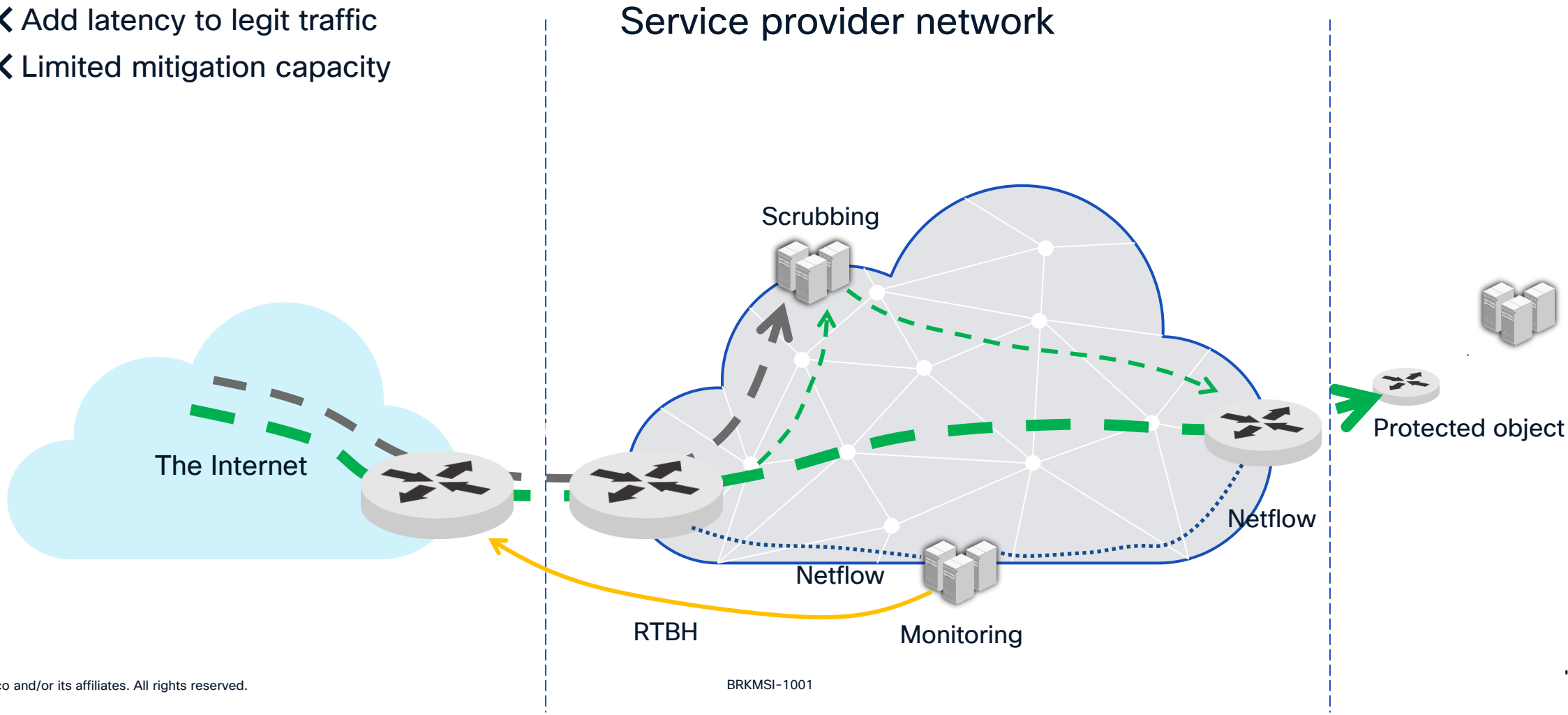
- Network is Central
- Sometimes local CDN
- Few Internet Connections
- Single scrubbing center might be good enough.

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

Traditional DDoS Deployments

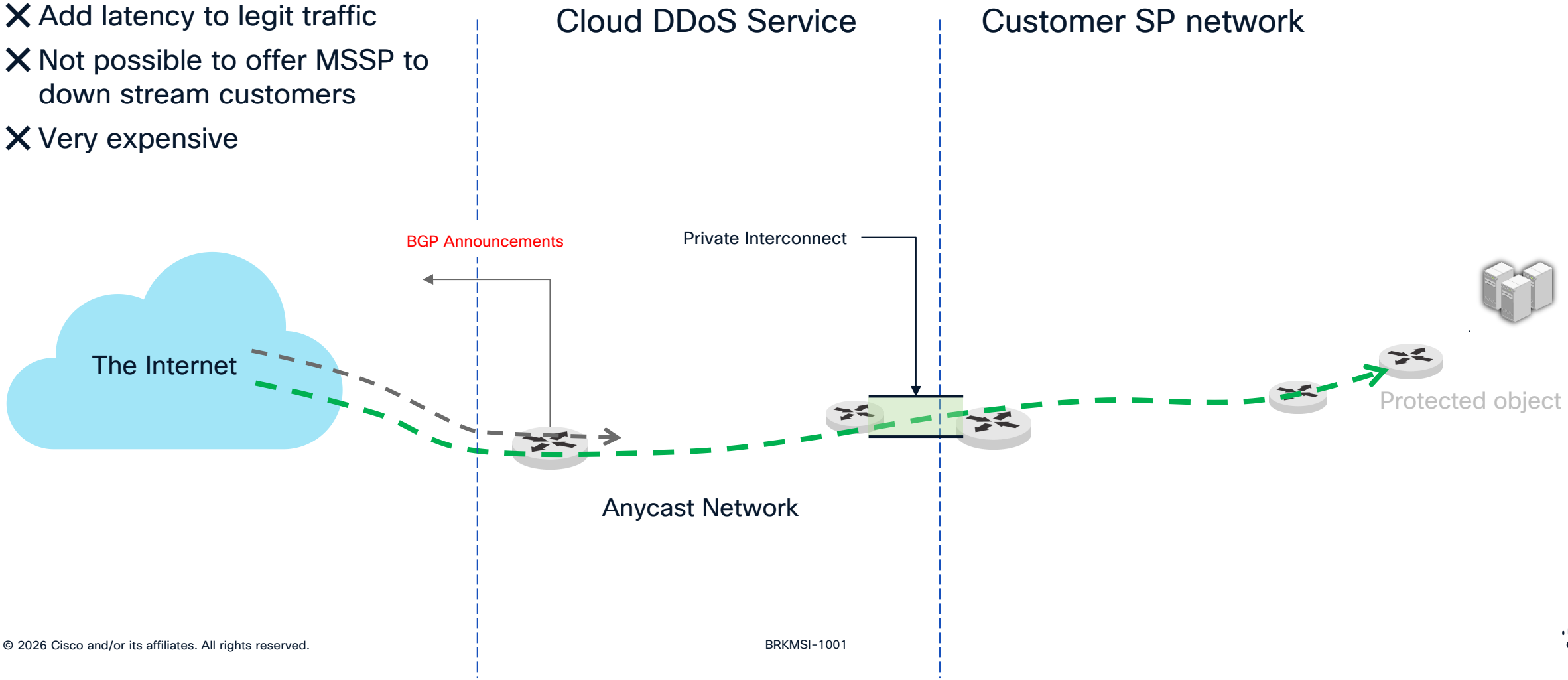
Traditional OnPrem DDoS deployment architecture

- ✕ 1 to 3 minutes time to mitigation
- ✕ High Total Cost Of Ownership
- ✕ Add latency to legit traffic
- ✕ Limited mitigation capacity



Cloud DDoS deployment architecture

- ✕ Very high time to mitigation
- ✕ Could becomes a bottle neck and single point of failure
- ✕ Add latency to legit traffic
- ✕ Not possible to offer MSSP to down stream customers
- ✕ Very expensive



Traditional DDoS Systems can’t scale/mitigate the current attacks

Aggressive Pulse Attacks
Bursts of 30 to 120 seconds

Scrubbers takes 90 seconds or more to start mitigation

Pernicious Carpet Bombing
UDP Flood on 1000s of endpoints <200Mbps

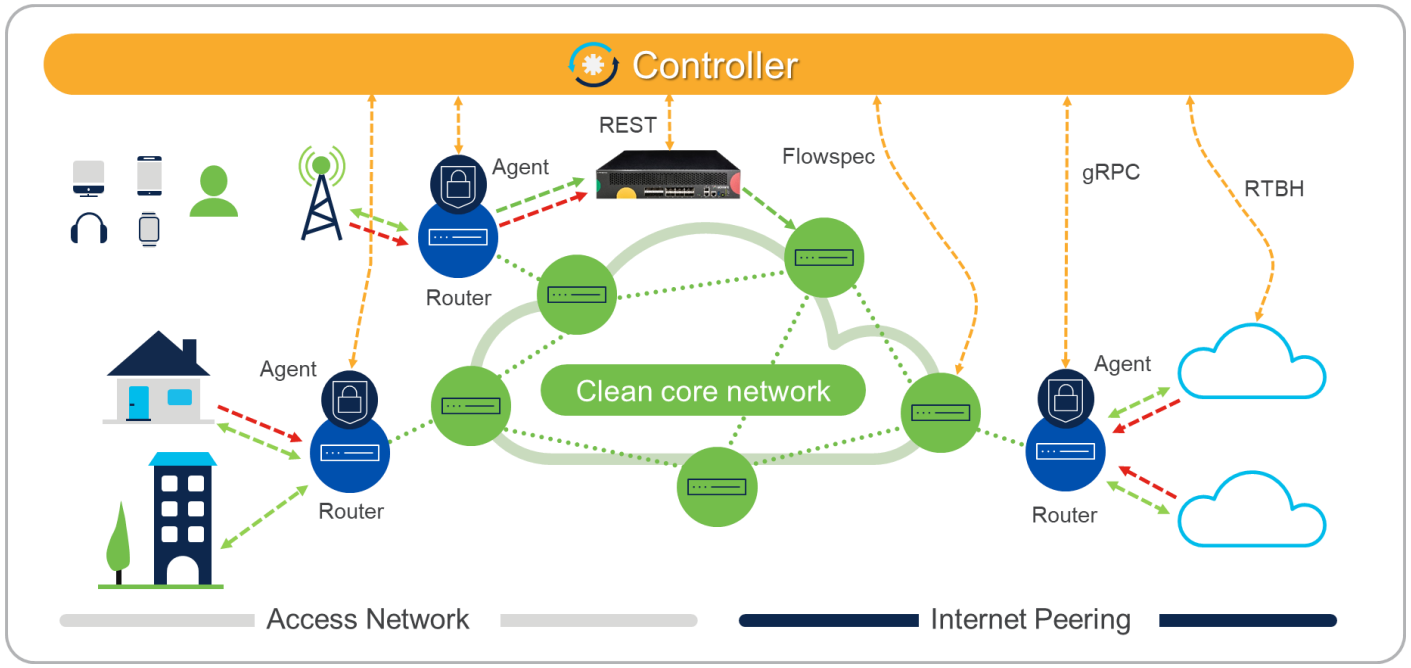
Traditional threshold-based system cannot detect low volume UDP/TCP floods

Outbound attacks
Goes to few Tbps crushing egress interface

Scrubbers are unidirectional scrubs only incoming traffic

Cisco Secure DDoS Edge Protection

Solution architecture



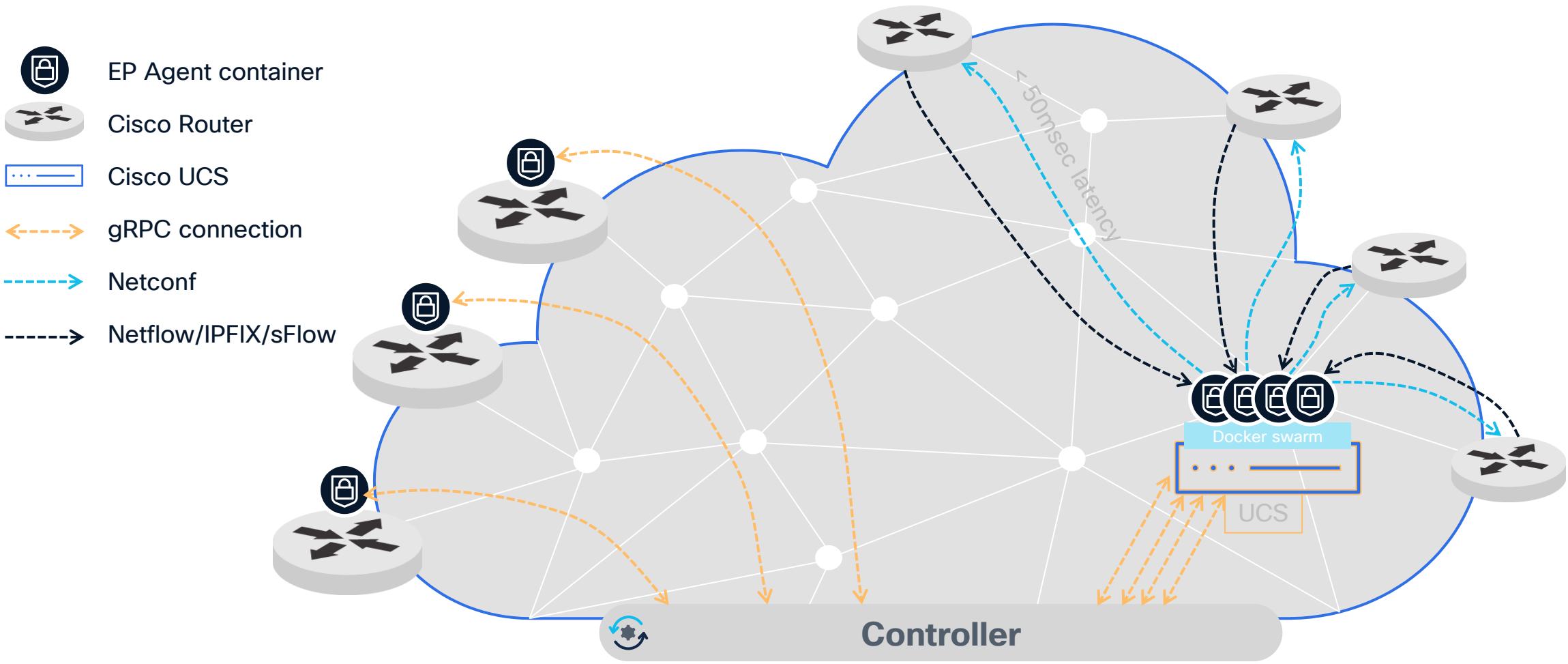
Controller

- 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
- Implements BGP RTBH and Flowspec mitigation
- Integrated over REST APIs with any cloud or scrubbing mitigation device

Agents

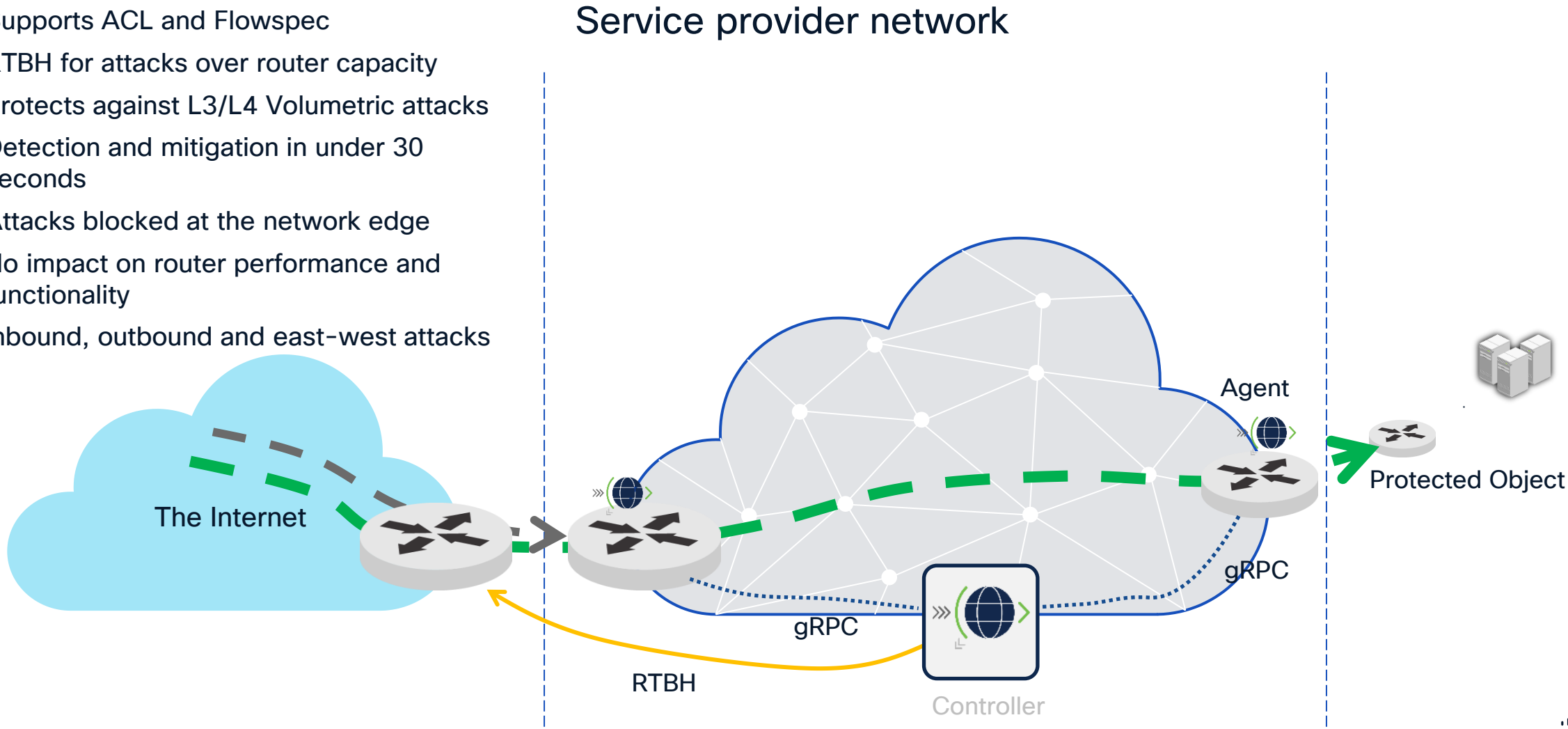
- A container deployed on a router, utilizing dedicated CPU and memory resources, collecting and analysing network telemetry.
- Sends aggregated statistical reports and alerts to the Controller.
- When an attack is detected, a mitigation policy is applied to the router by ACL rules.

Cisco EP deployment architecture On/Off Box



Cisco DDoS Edge Protect deployment architecture

- On Box detection and mitigation
- Supports ACL and Flowspec
- RTBH for attacks over router capacity
- Protects against L3/L4 Volumetric attacks
- Detection and mitigation in under 30 seconds
- Attacks blocked at the network edge
- No impact on router performance and functionality
- Inbound, outbound and east-west attacks



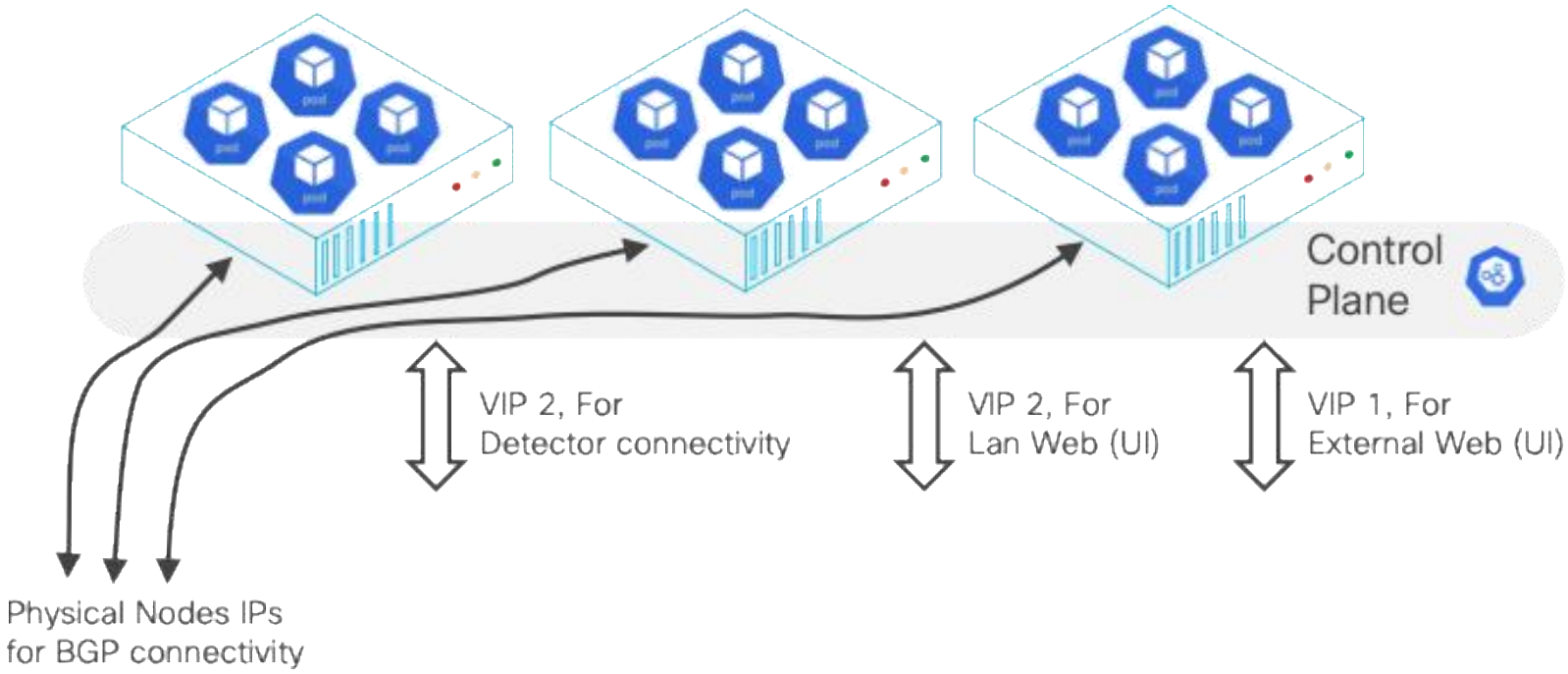
Edge Protection Controller design

- The Controller is a Kubernetes Cluster
- It is built over K3S (reduced size) Kubernetes
- It can support
  - Single node deployment
  - Or multi-node deployment
- Multi-node deployment allow for
  - High availability
  - Redundancy, including GEO redundancy
- Connectivity to Detectors, Web using VIP
- Connectivity to BGP using physical IP addresses of Nodes

Controller Deployment

Inter-node connectivity requirements for Geo HA:

- Latency < 20msec, preferred <10msec
- Bandwidth min 1Gbps, preferred 10Gbps
- It is possible to add interfaces and VIPs for any external connectivity, only 1 VIP is mandatory

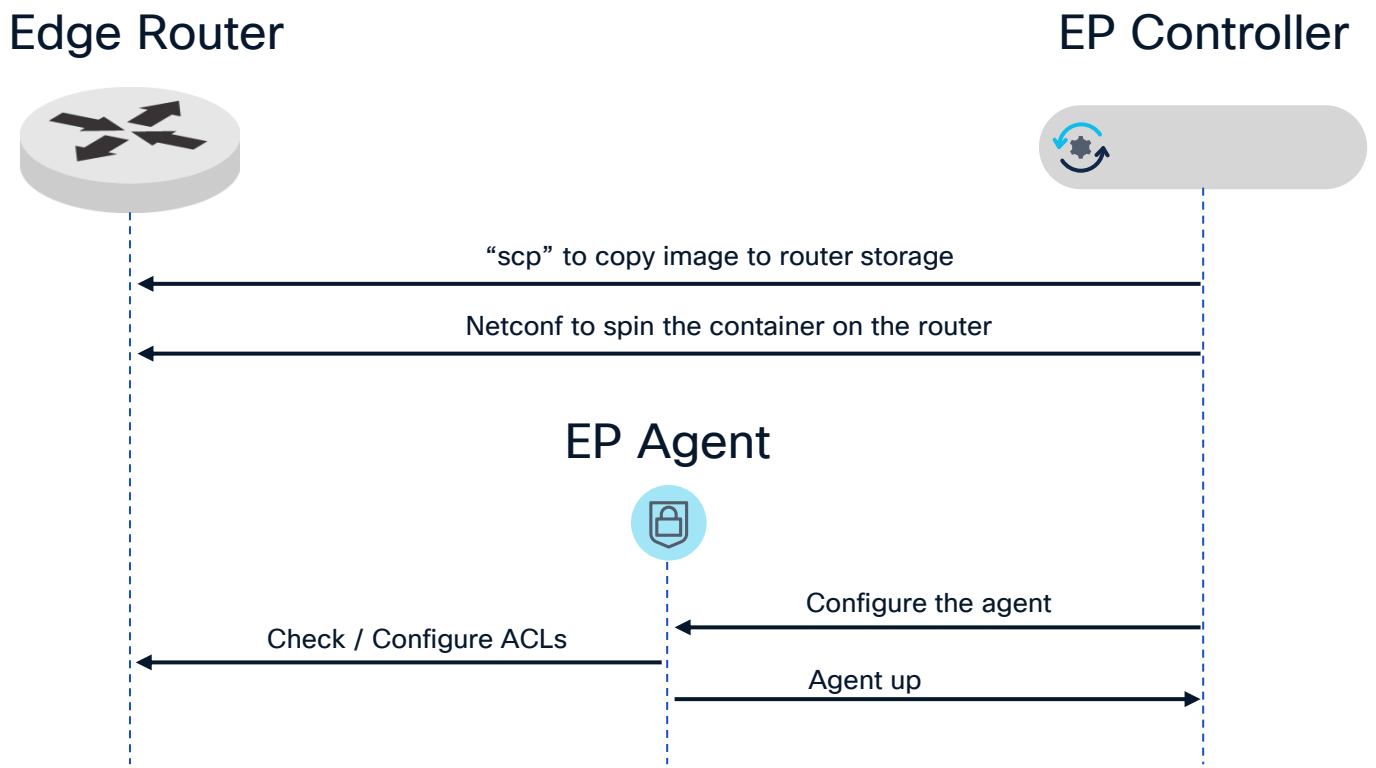


Comparison with traditional DDoS mitigation systems

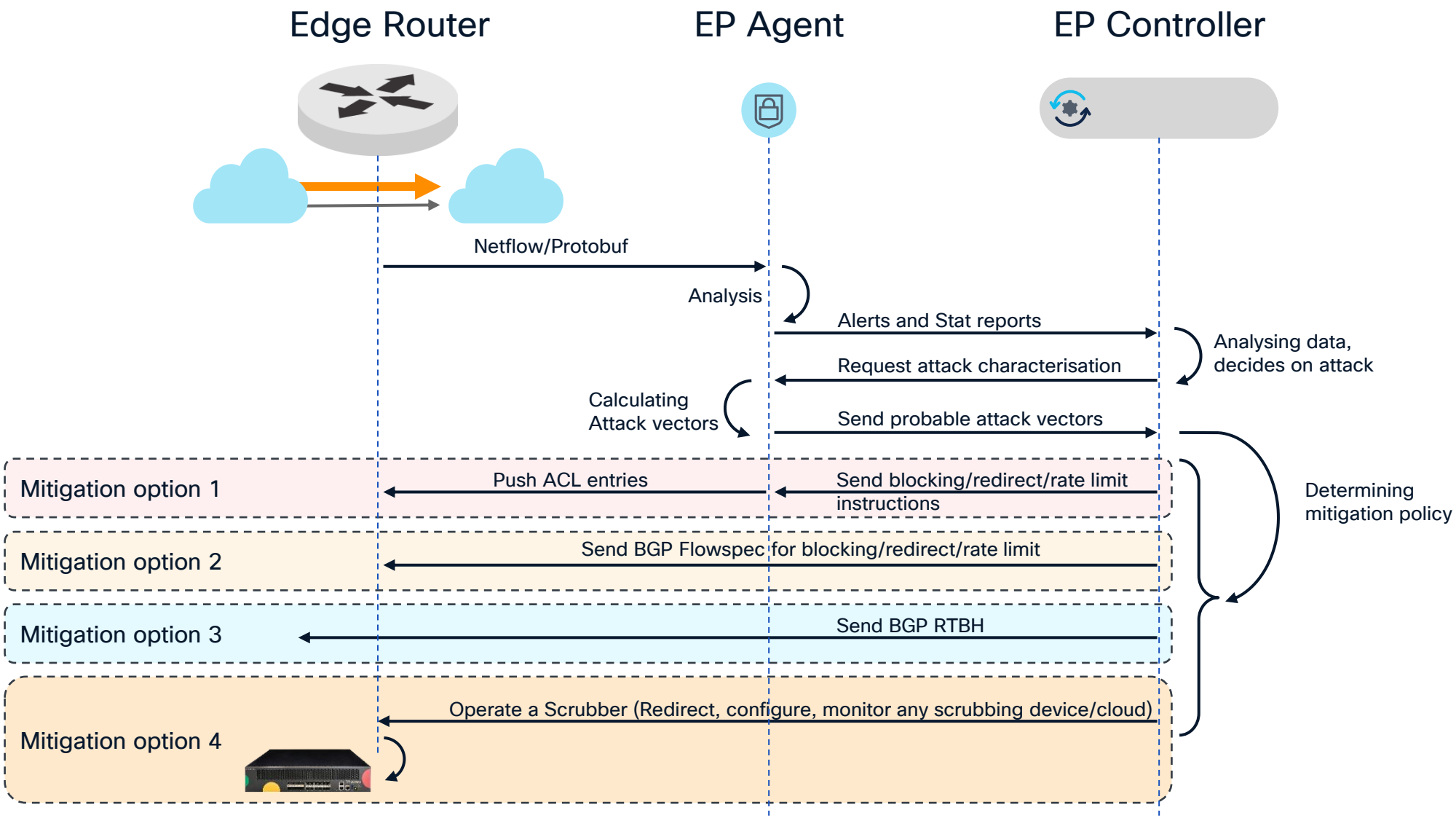
Feature	Cisco Edge Protection	On-prem Scrubbing	Cloud DDoS Service
Time to Mitigation	Below 30 Sec	1-2 Minutes	Very slow
Single point of failure	No Bottlenecks, No latency	Partial, requires addl. Investment for redundancy	Yes, Single vendor network
Stateless Firewall (static ACL's)	Yes with 1000's of ACLs	Yes + BGP FlowSpec	Yes, but limited and expensive
Latency	No added latency	Add latency on mitigated target traffic	100's of msec (depends on how distributed the vendor network is)
Always On	Yes	Yes	Depending on Service Tier (expensive)
MSSP	Yes	Required additional systems & subscription	No
Automation Operations	Yes, Customer programable policies	Simple Playbooks	No
Mitigation Capacity	Max. capacity is Network capacity	Limited by appliance capacity	Depends on the contract

Workflows, Usecases & the algorithm(s)

Deployment and provisioning



Attack Life Cycle Management



Deployment Usecase #1: Peering

Inbound Attack Protection

The challenge

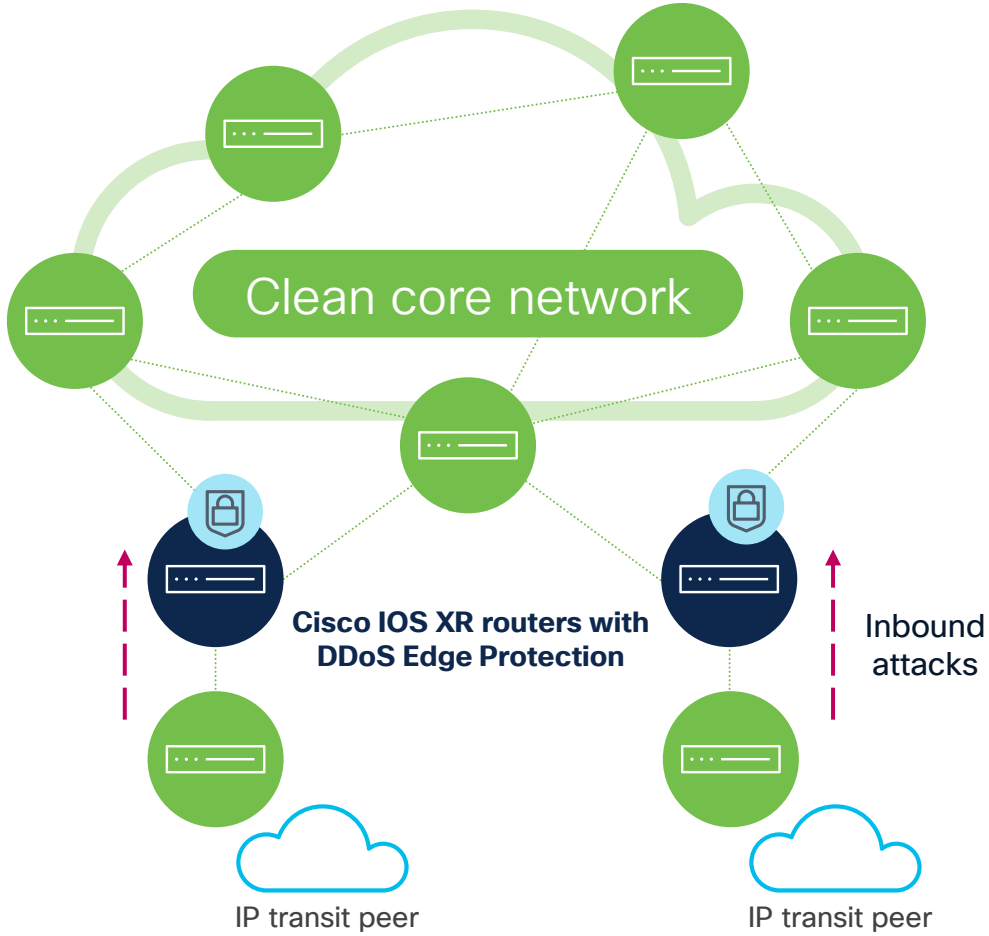
- Massive peering volumes and diverse protocols make ***static filters and "misuse lists"*** ineffective against rapidly evolving threats.
- ***Scaling*** traditional hardware to match modern peering traffic is cost-prohibitive.

How our solution addresses it

- Edge Protection provides real-time visibility and ***dynamic mitigation*** that automatically re-characterizes defense logic as attack vectors change.
- Architecture provides cost-effective, multi-layer protection (L3–L7) to ***keep the core network clean***

Supported Functionality

- Protects against L3/4 DDoS attacks
- Protects against L7 Volumetric attacks
- Advanced protection against carpet bombing and burst attacks



Deployment Usecase #2: Access/Broadband

Outbound Attack Protection

The challenge

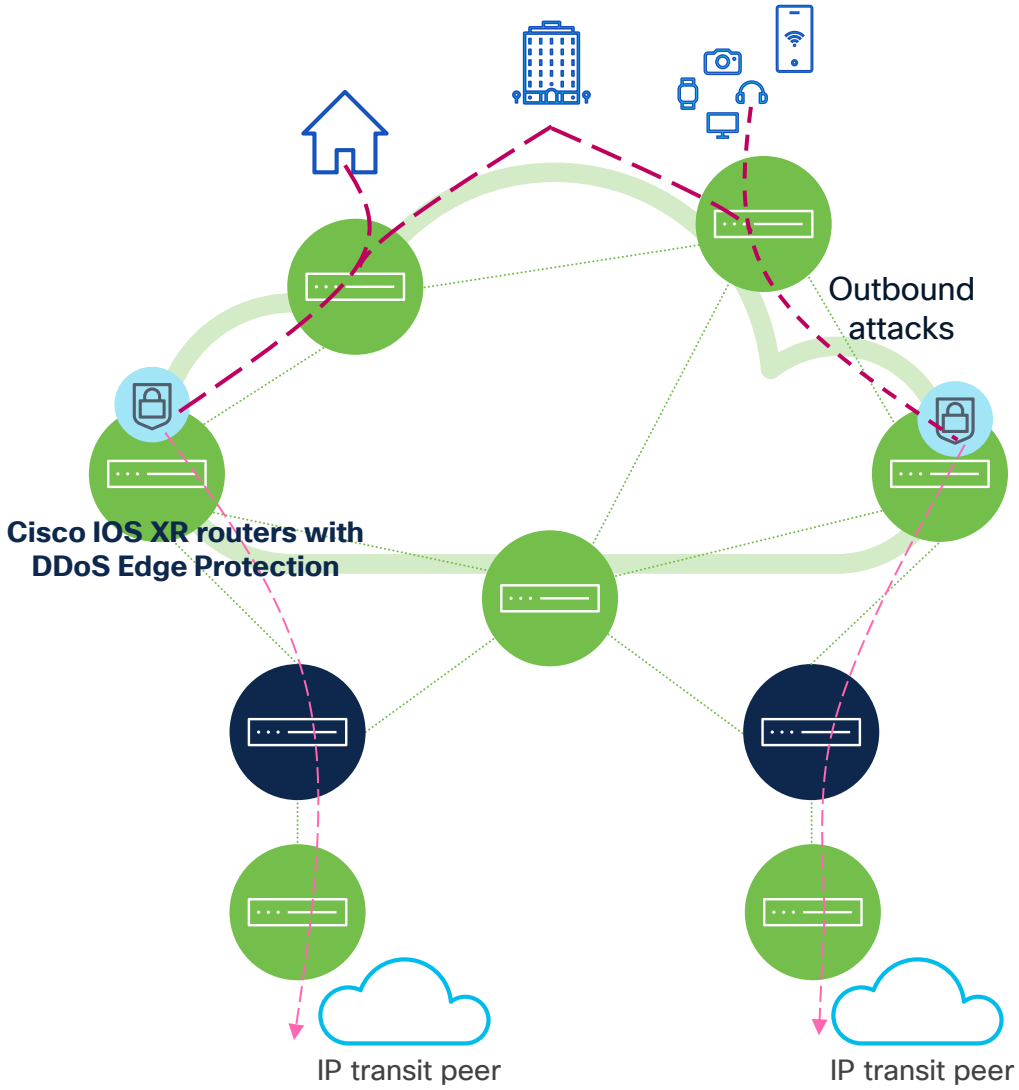
- Botnet-infected CPEs turn provider networks into **"attack launchpads",** causing peering IPs to be blacklisted and preventing legitimate traffic handoff.
- High-volume outbound attacks from infected end-user devices ***overwhelm access nodes*** and degrade service for legitimate subscribers.

How our solution addresses it

- Uses a **multi-pass approach** to identify devices infected with botnets such as Alsuru and Kimwolf
- Detects in real time when a campaign is launched against a specific target or a range of destinations

Supported Functionality

- Protects Botnet infected devices, including latest threat actors like Aisuru and Shadow v2



Deployment Usecase #3: East-West

East-West Attack Protection

The challenge

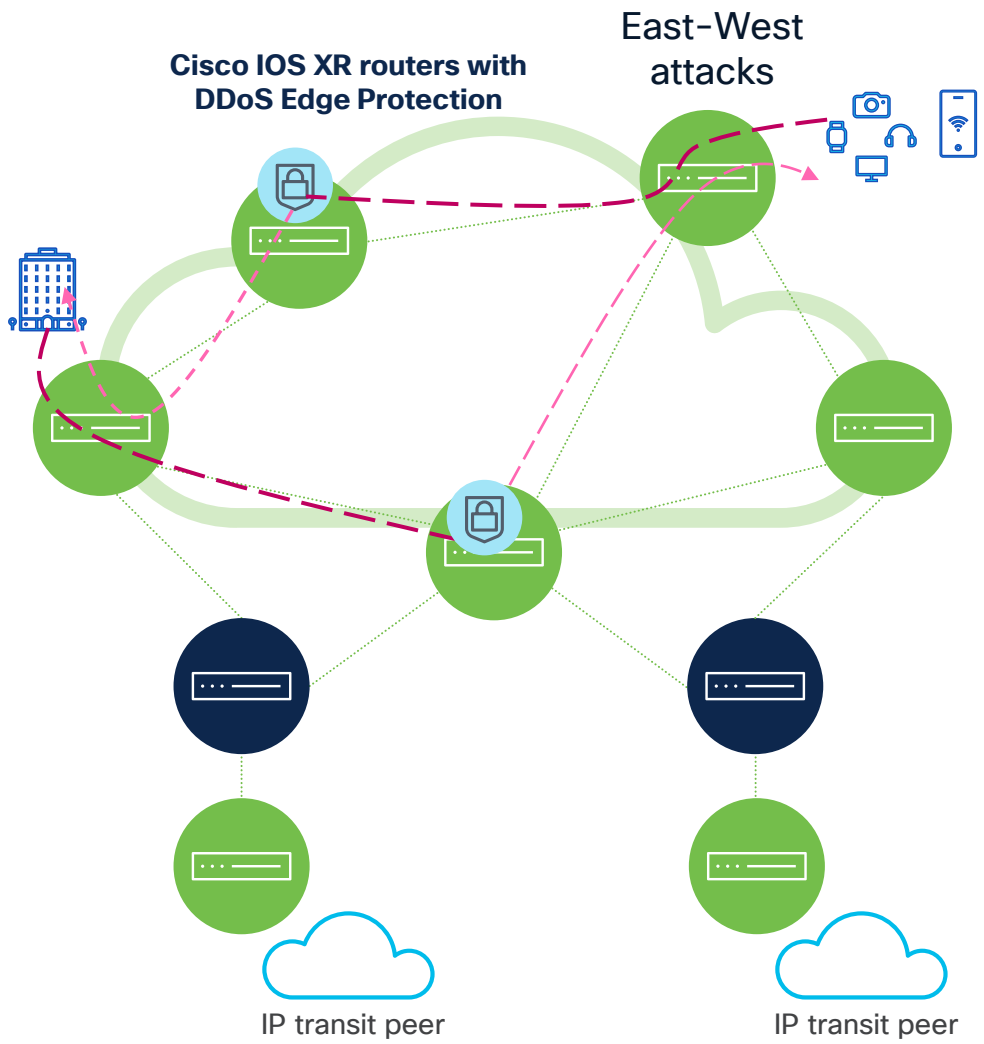
- **Visibility Gaps:** Traditional perimeter-only defenses are blind to internal traffic, allowing malicious flows to spread horizontally between users without detection.
- **Internal Exploitation:** Competitive environments and gaming scenarios often trigger targeted attacks within the network to disrupt specific user sessions or gain unfair advantages.

How our solution addresses it

- Monitors the thresholds, individual endpoints for behavioral anomalies, automatically blocking attack traffic for remediation.

Supported Functionality

- Real-time suppression of targeted peer-to-peer attacks, ensuring service continuity in low-latency, high-stakes(like Gaming) environments.



Detection algorithm overview – In/Out attacks

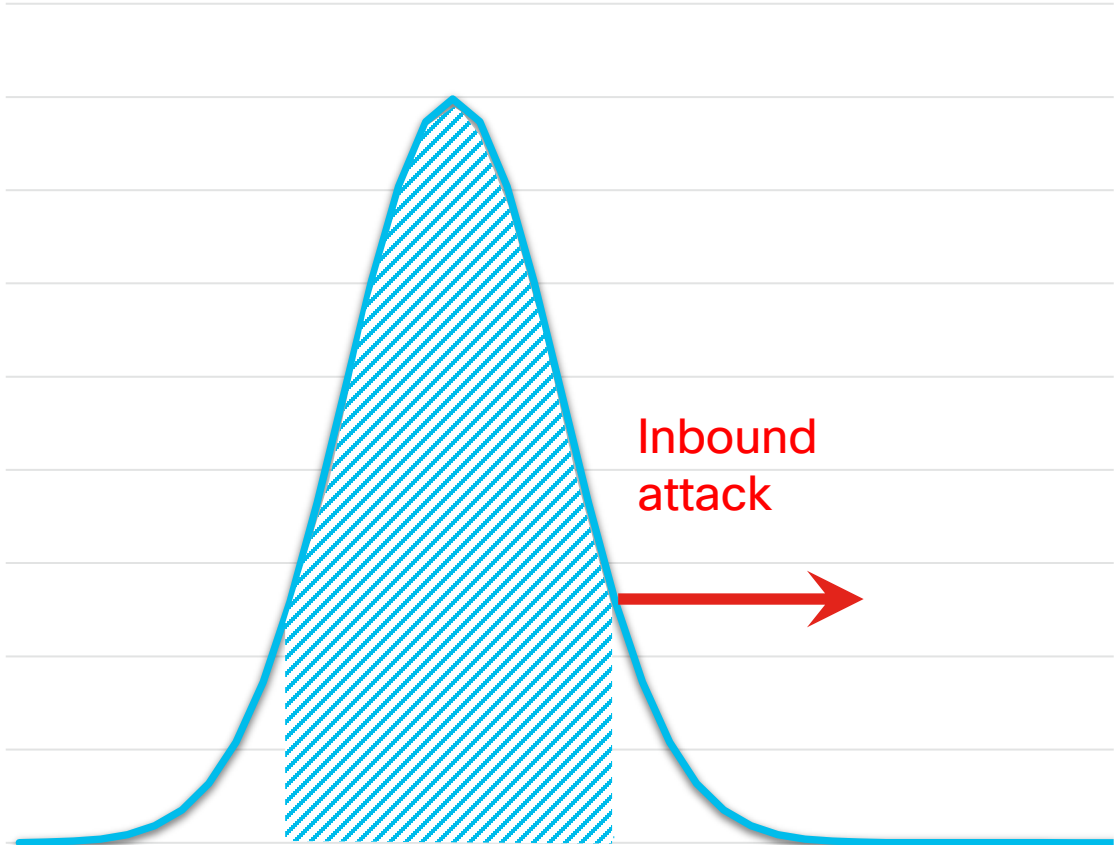
Self-learning thresholds (learning phase)

1. Learning Is at the controller level on all data from all detectors
2. PO Can have a mix of learning filters and pre-configured filters
3. Learning is performed
   - Per Host within a PO
   - Per PO (setting threshold levels) for the entire PO
   - Or both per PO and per host
4. Learning scheduler
   - Set the learning duration (per PO) recommended 160 hours
   - Set the periodic learning intervals (daily, weekly…) recommended weekly
   - Un-learnt hosts that appear between learnings learned as they appear
5. At the end of learning
   - For every filter, hosts are clustered into groups based on K-means with elbow method
   - For every filter, filter thresholds are set per group, with X% (configurable) from learnt value
   - Every filter and filter group can be edited manually
6. User can further divide a PO into child POs to support hosts binning

Attack Condition Validation – SWIFT

ML to learn “normal” behavior per host

Distribution of In / Out number of Flows, for a single host



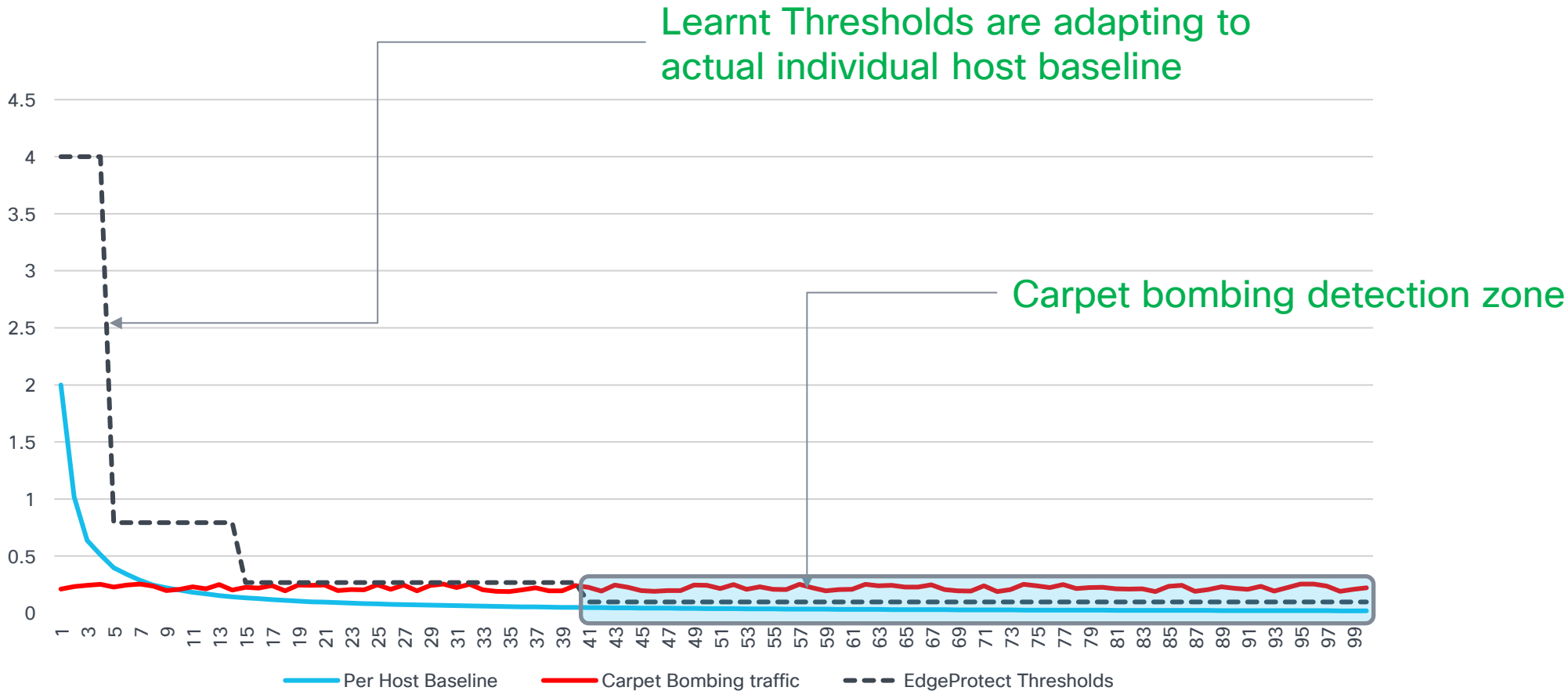
How it works:

1. Constant measurement of In/Out number of flows, measuring Average and Standard deviation
2. DDoS attack by definition is unidirectional
3. When there is “over the threshold event
   - If real attack In/Out is also drastically skewed
4. We are measuring number of flows, to neutralize bias from packet length or number of packets
5. DDoS attack always constitutes from very short flows

cisco

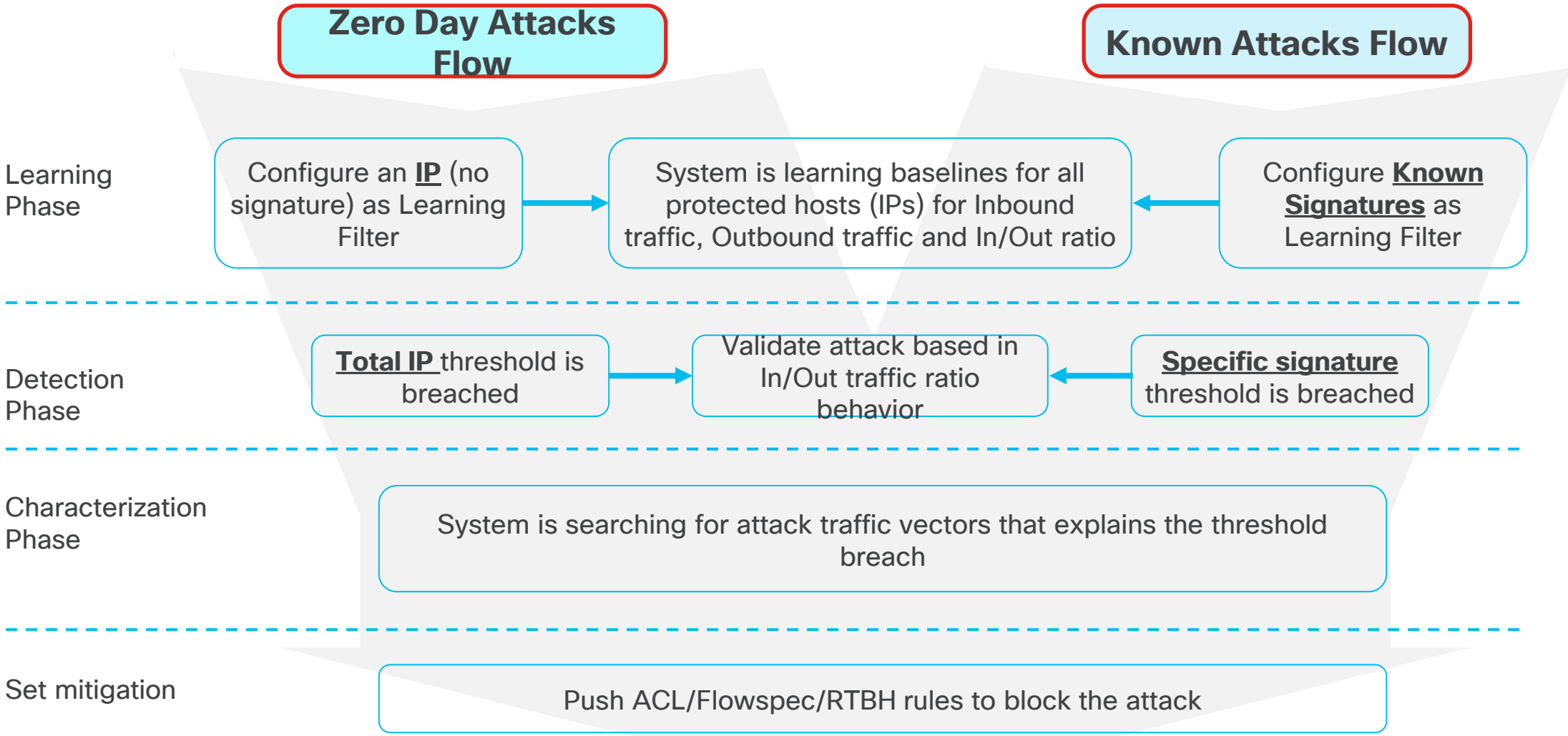
Accurate Carpet-Bombing detection & mitigation

Typical Traffic Patterns and use of ML Thresholds



cisco

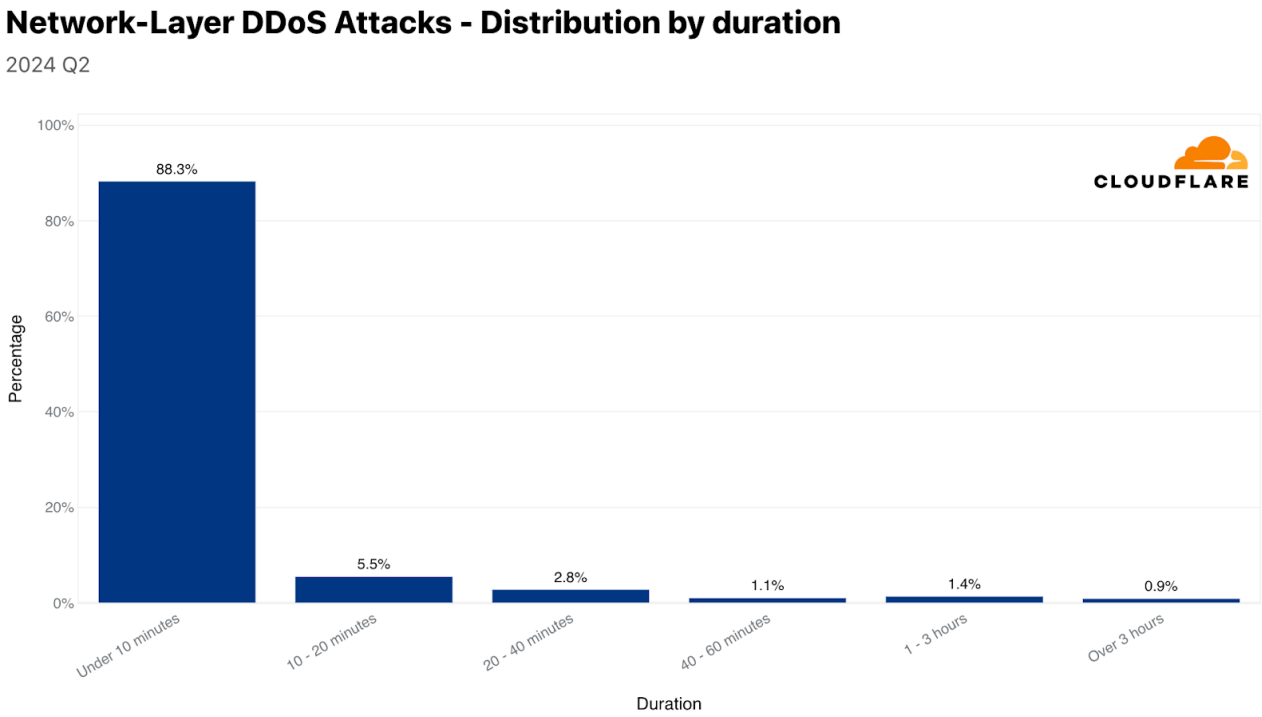
Detection & Mitigation of Attacks



The importance of superfast time to mitigation

Latest data shows that attack are getting shorter and more violent.
Industry standard for time to mitigation is 1 to 3 minutes, meaning up to 30% of attack traffic goes in

About 90% of attacks are below 10 minutes



Cisco Secure DDoS Edge Protect, creates a new industry standard for Time To Mitigation – **30seconds**.

MSSP – Monetize the DDoS offering

MSSP – Monetize DDoS Protection at Scale

- **Included with the License**

  MSSP is part of the basic license package

- **Massive Multi-Tenancy**

  Allow onboarding of 10,000+ customers, each of a different PO

- **Secure role-based access**

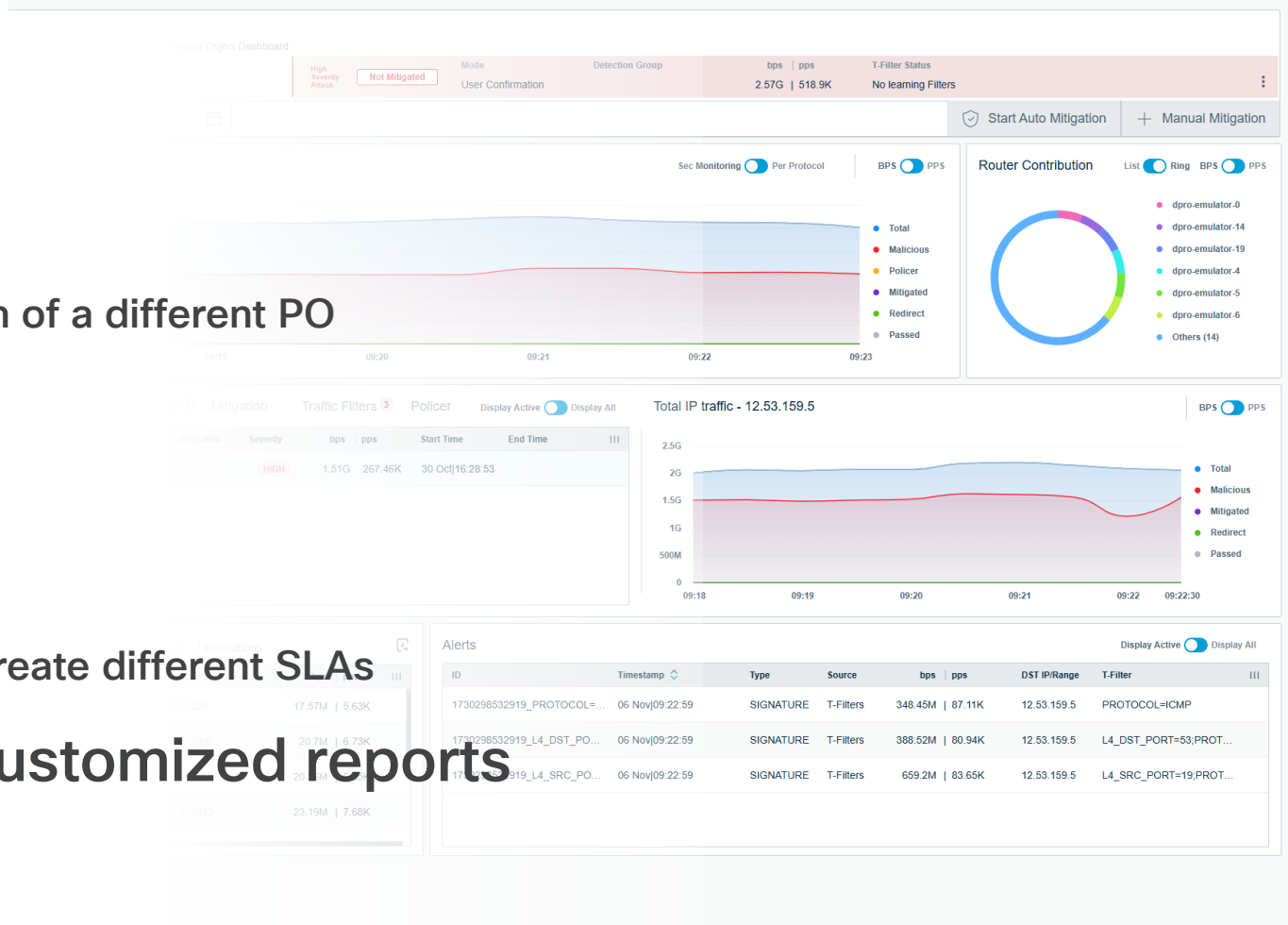
  Full data isolation between tenants

- **Tiered based service models**

  Flexible detection and mitigation policies to create different SLAs

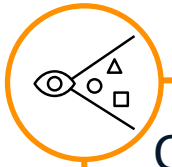
- **Customer facing portal, with customized reports**

  Branded attack reports and trend summaries

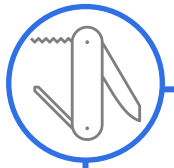


DDoS Edge Protection – Customer benefits

Full customer portal, with reporting



Customer can manage their own policies to some extent



Supports tiering policies (Bronze, Silver, Gold)

Allows to onboard up to 10K protected Customers

Creates a source of potential revenues

Brand awareness and reduces churn

Built-in support for MSSP, included with the License

Scripting language

```
OnMitigation
If ( DayOfWeek == Saturday OR DayOfWeek == Sunday ) AND ( MitigationData.Totalbps >= 2000000000 AND MitigationData.NumberOfSignatures>= 1 )
  LOG ("Weekend RTBH")
  Action RTBH onGroup #All_RTBH RequestUserConfirmation
Else If MitigationData.Totalpps >= 400000000 AND MitigationData.NumberOfSignatures >= 5
  Action RTBH onGroup #All_RTBH RequestUserConfirmation
End

OnSignatures
If MitigationData.Signature.NumberOfParams < 3 AND ( MitigationData.Signature.AttackType == "TCPSYNFlood")
  Action ACL_Redirect onGroup #All_ACL
End

If MitigationData.Signature.Find(TimeToLive,69)
  Action ACL_Block onGroup #All_ACL
End

//Default action
Action ACL_Block onGroup #All_ACL
```

- Enables flexible logic to decides on mitigation actions
- Each PO can get its own script
- Few example scripts are included

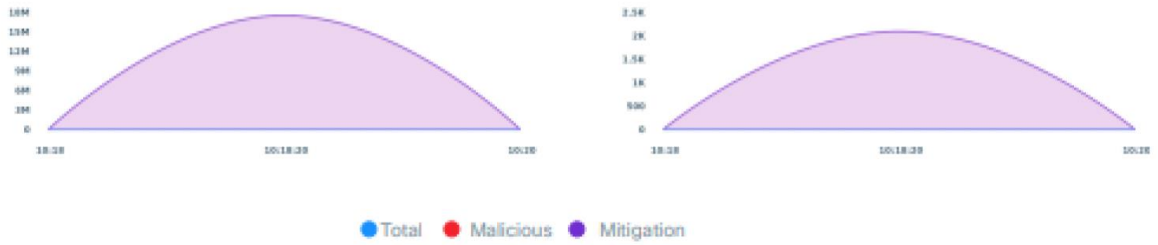
Sample attack report sent to the customers

PO Name: ITS-CUSTOMER
Attack ID: 3356
Attack Severity: MEDIUM
Status: END
Started: 2025-09-17 11:18 Europe - London
Ended: 2025-09-17 11:20 Europe - London
Average attack traffic (bps/pps): 17.53Mbps | 2.09Kpps

Security Event Summary

PO Name: ITS-CUSTOMER
Attack Severity: MEDIUM
Status: END

Max attack traffic(bps/pps): 17.53Mbps | 2.09Kpps
Average attack traffic(bps/pps): 17.53Mbps | 2.09Kpps
Number of attacked IPs: 1
Attack ID: 3356



PO Name: ITS-CUSTOMER
Attack ID: 3356
Attack Severity: MEDIUM
Status: END
Started: 2025-09-17 11:18 Europe - London
Ended: 2025-09-17 11:20 Europe - London
Average attack traffic (bps/pps): 17.53Mbps | 2.09Kpps

Detailed Security Event Information

Attacked IP IP.AD.DR.ESS

Detections

1. Detection ID: 1_3356 Started: 2025-09-17 11:18 Europe - London Ended: 2025-09-17 11:19 Europe - London
Detected vectors:
1. IP.AD.DR.ESS ,SRC_PORT:53;PROTOCOL:UDP
2. ,SRC_PORT:53;PKT_LNGTH:1028;PROTOCOL:UDP;TTL:61

Bps Traffic

Pps Traffic

Customer Case Study

Customer showcase – ITS UK

Hyper-volumetric data floods, some exceeding 1 Tbps and stealthy criminals mimicking legitimate traffic mean that DDoS threats are no longer just inconvenient isolated incidents – they're highly sophisticated campaigns used to scale disruption, data extortion and even geopolitical influence.

The ITS SecureEdge **Promise**

Powered by Cisco, ITS SecureEdge delivers an always-on, Advanced Machine Learning – backed service right at the network edge for 24/7/265 protection that adapts to the changing threat landscape. That means ITS SecureEdge delivers:

Future-proof protection at scale
Constantly adapting to changing attack vectors to keep protection up to the challenge.

Performance-first defence
Our mitigation tactics work within seconds, not minutes. That means less latency and less disruption – keeping your customer experience seamless.

Accuracy driven
ITS SecureEdge is an intelligent solution designed to distinguish between malicious and legitimate traffic with precise accuracy – helping your customers thrive online – even during attacks.

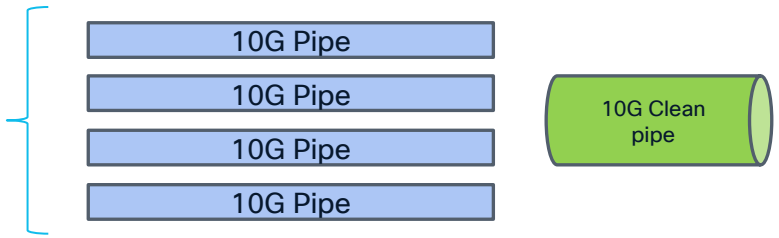
Customer Business scenario & Product details

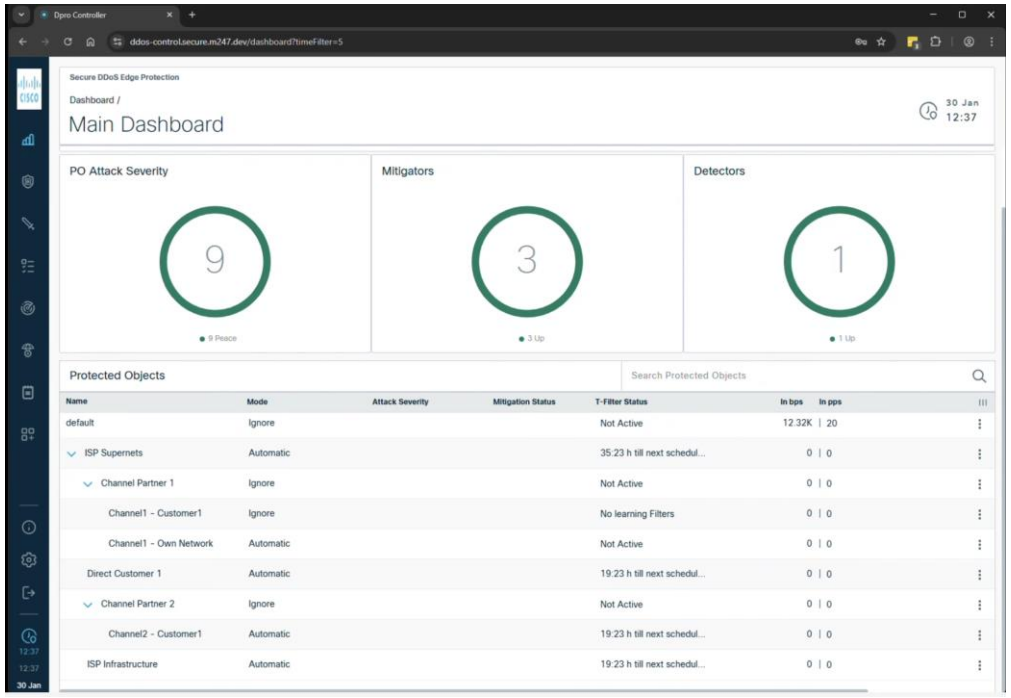
- Monetization Opportunity: Partner led system
  - Wholesale model
- Key Product features:
  - Always-On, Proactive Defense
  - Rapid detection & mitigation of DDoS attacks
  - Minimal impact on Legitimate traffic
  - Detailed reporting & Analytics
  - Equitable Single Tier service
- Pricing Model:
  - Equitable Single Tier Service
- End customer benefits:
  - Secured Business Continuity
  - Cost savings & resource optimization
  - Future proof solution

10-15%

uplift on the connectivity pricing

MSSP package from another UK Tier-2 Service Provider



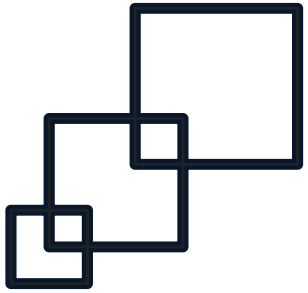


Name	Description
-Prod-1G	1 Gbps Protected Bandwidth

```
1  //      Mitigation Script - Production
2  // Threshold = 1G
3
4  // Network Protection above 20G
5  If MitigationData.Totalbps >= 20G
6    LOG("Attack detected in excess of 20G - REDIRECT (NULL ROUTE)")
7    Action ACL_Redirect onGroup #All_ACL
8    // This will be replaced with RTBH when operable
9  End
10
11 // Attack is sufficiently identifiable, so block attack and rate limit all remaining traffic to IP
12 If MitigationData.Signature.NumberOfParams > 3
13   LOG("Attack detected with sufficient params - BLOCK/RATELIMIT")
14   Action ACL_Block onGroup #All_ACL, Flowspec_Ratelimit(1G,bps) onGroup #All_Flowspec ByDestinationOnly
15 End
16
17 // Attack cannot be sufficiently identified, so just rate limit what we assume to be attack traffic
18 LOG("Attack detected with insufficient params - RATELIMIT")
19 Action Flowspec_Ratelimit(1G,bps) onGroup #All_Flowspec
```

Summary

Cisco Secure DDoS Edge Protection is designed to handle the growing networks.



Distributed & Scaling

- Edge Protection Containers run on distributed nodes, scale well along with the scaled Networks.

Continuous Learning

- Advanced ML algo's in learning mode will adapt to 'your' networks, reducing the false positives
- Ready for newer and evolving DDoS attacks

Monetization

- MSSP features allow you to offer differentiating services, help to increase the ARPU for customers.

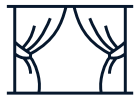
For any further questions or product interest or POCs, please reach out to :
ask-ddos@cisco.com

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact us at: ask-ddos@cisco.com


CISCO