Secure the Network Edge against the DDoS Attacks!

cisco Live!

Raja Kolagatla
Engineering Product Manager, @kraja80

BRKMSI-1001

Cisco Webex App

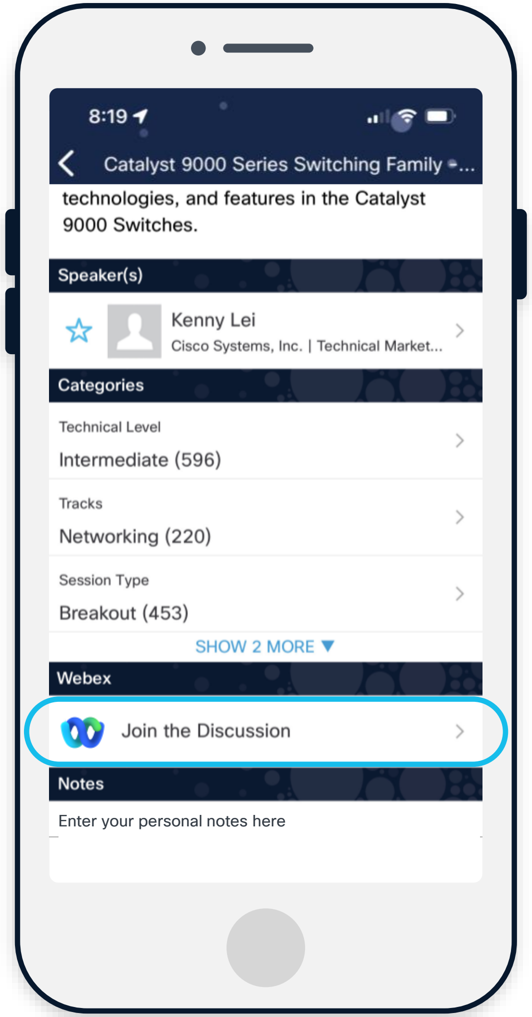
Questions?

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 13, 2025.



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

Do not edit

How to change the design

Can we have a split of audience here?

The Slido app must be installed on every computer you're presenting from

Do not edit

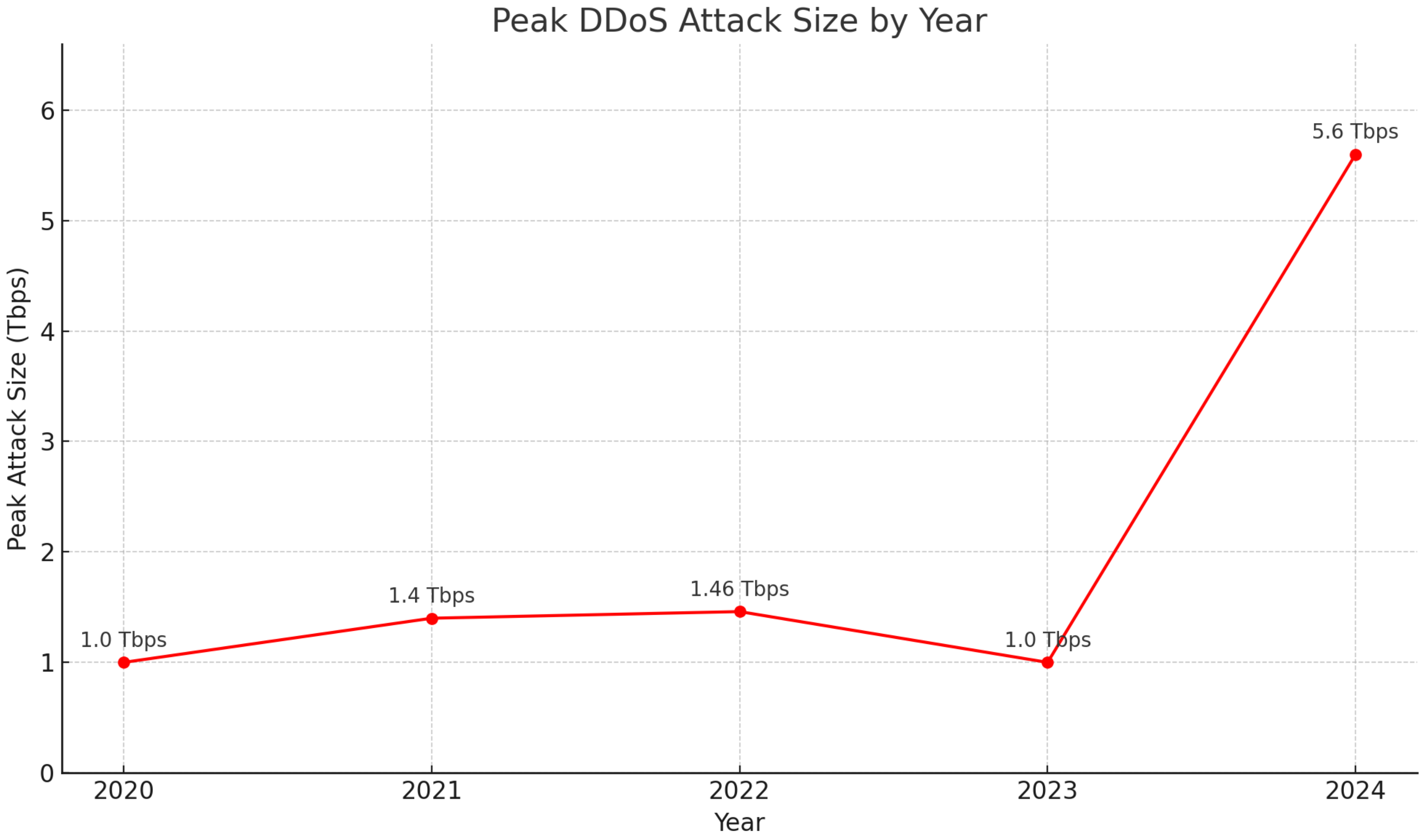
How to change the design

How many significant DDoS attacks have seen/recorded in your network?

The Slido app must be installed on every computer you’re presenting from

Peak DDoS attacks increasing YoY!

Is your network designed to handle them?



Agenda

01 Evolving DDoS attacks

02 Edge Protection – Architecture, Usecases

03 Solution Workflows & Key features

04 Two-Layered DDoS Protection

05 Customer case study

The DDoS Threat continues to grow and evolve. Are you protected?

DDoS attacks can have a long-lasting negative impact on Service Provider/Large Organization’s business

Direct financial impact

- Service disruptions can lead to lost revenues.
- Missed SLAs can result in penalties.
- Cybercriminals use DDoS for extortion.

Customer churn

- Poor quality of experience encourages customers to move to competition.

Brand damage

- Negative publicity can cause reputational damage.
- A tarnished brand reduces shareholder confidence.

Fines

- Regulators can impose hefty fines on organizations with inadequate security measures.

DDoS Attack Trends

Increasing L3/L4 Attack Frequency

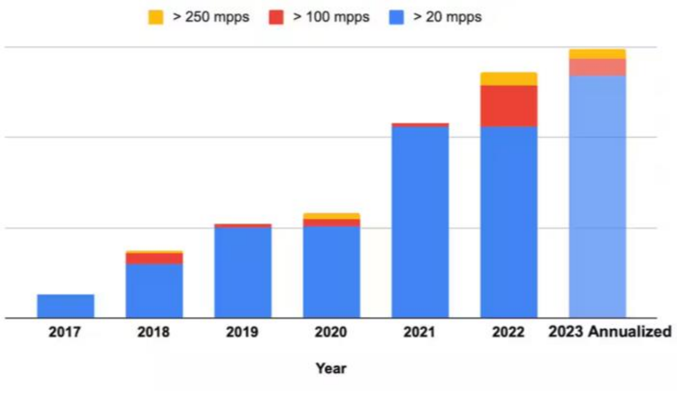
Attack time reduction

Attack orchestration using AI

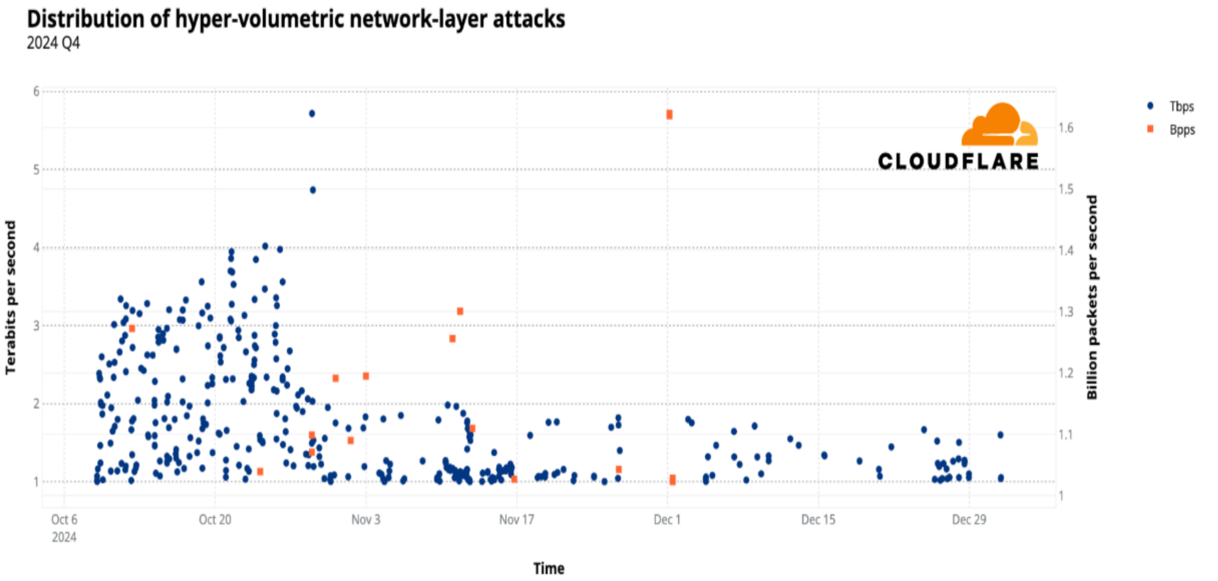
Growth of DDoS-for-Hire Services

Geopolitical and Hacktivist Influence

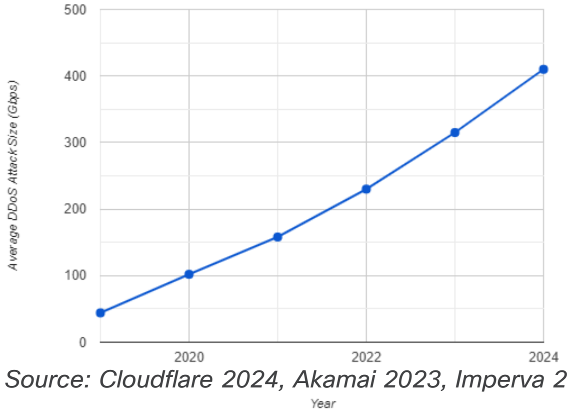
Increasing L3/L4 attack frequency



Source: Akamai 2023



Hyper-volumetric DDoS Attacks



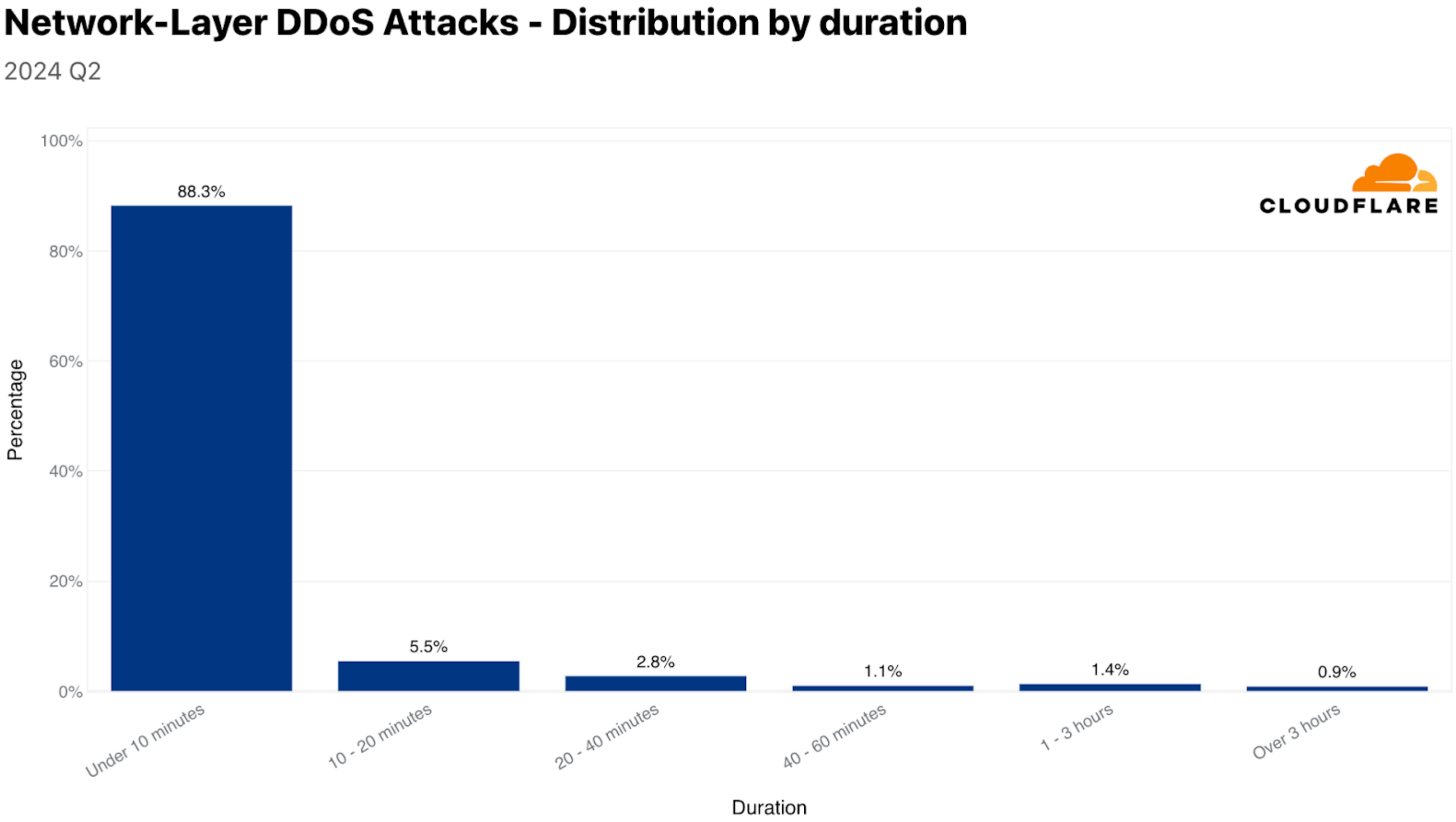
Source: Cloudflare 2024, Akamai 2023, Imperva 2023

Largest attack mitigated in Q4 2024 is 5.6Tbps of Mirai DDoS attack.

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



Attack orchestration using AI

Enhanced Attack Precision with AI

Example: GitHub DDoS Attack (February 2018) – 1.35 Tbps

Analyzes network traffic data to identify optimal times and methods for launching attacks

AI-Driven Botnets

Example: Mirai Botnet Evolution

AI-driven botnets can dynamically adjust their behavior to evade detection and maintain the intensity of the attack.

Adaptive Evasion Techniques

Example: Pulse Secure VPN Exploitation (2020)

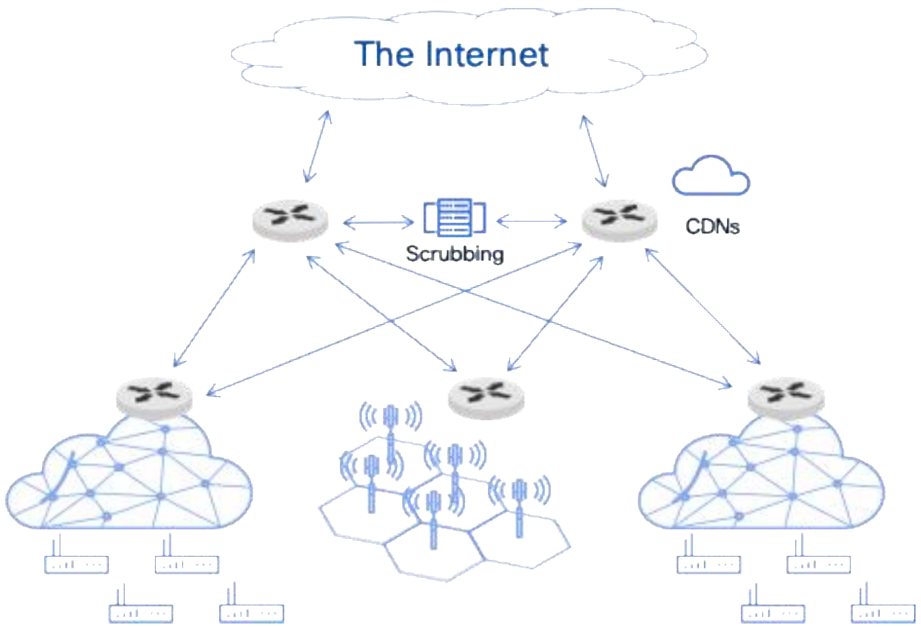
Difficult for defenses to recognize a consistent attack signature

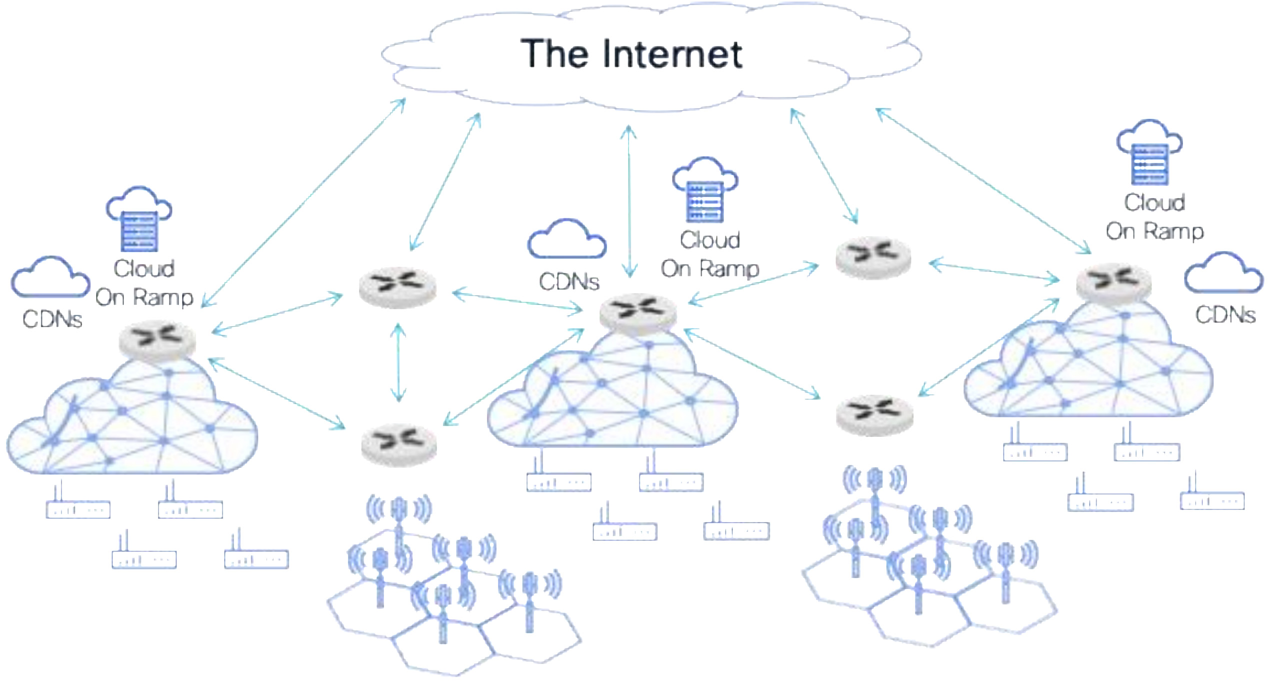
Increased Vectors in the DDoS attacks, AI-Powered Coordination

Simulates different DDoS attack vectors (e.g., volumetric, protocol-based) to identify the most effective ones

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 solutions cannot scale with attack trends

Cost

Centralized scrubbing is prohibitively expensive to keep up with network bandwidth growth (3x,5x,10x).

Latency

Longer, impractical scrubbing routes adds unwanted delays to traffic, potentially breaking SLAs.

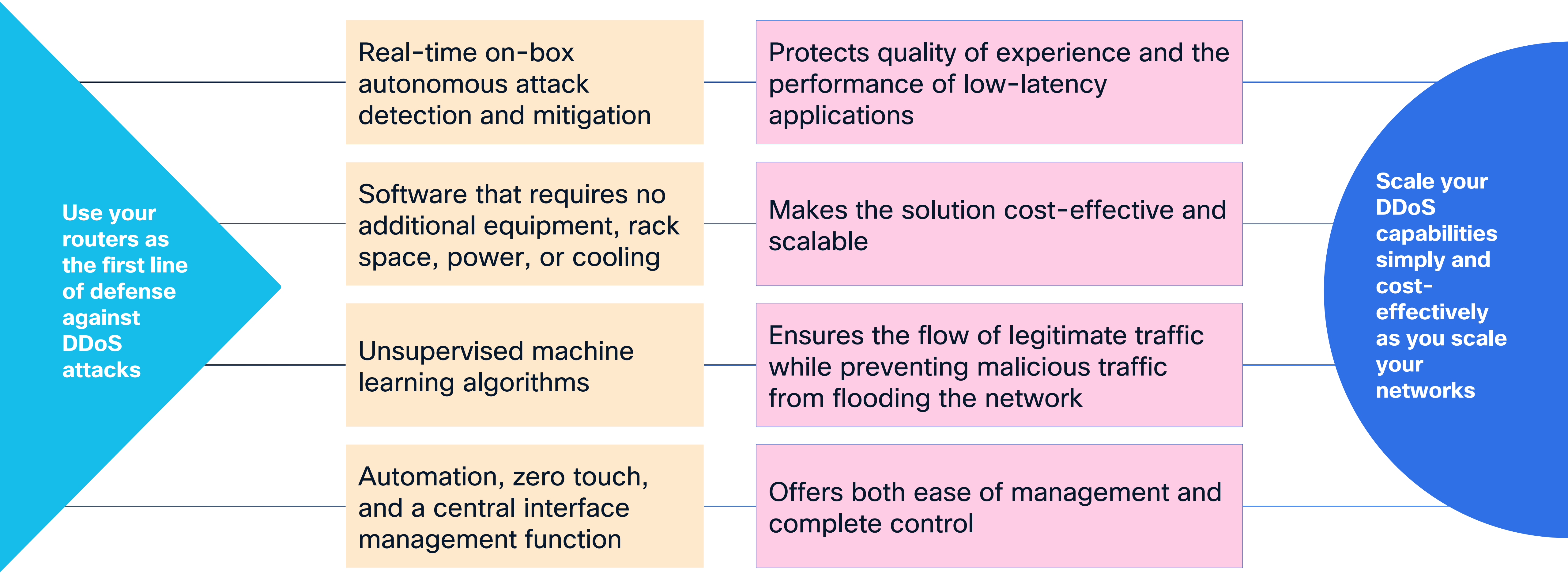
Security

Due to cost and latency issues, operators often only protect a selection of routes, leaving them vulnerable to dynamic, multi-vector nature of today's threats.

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

Industry's true on-box solution designed for SP's and Larger enterprises.

Keep attack traffic off your network by using your routers as the first line of defense

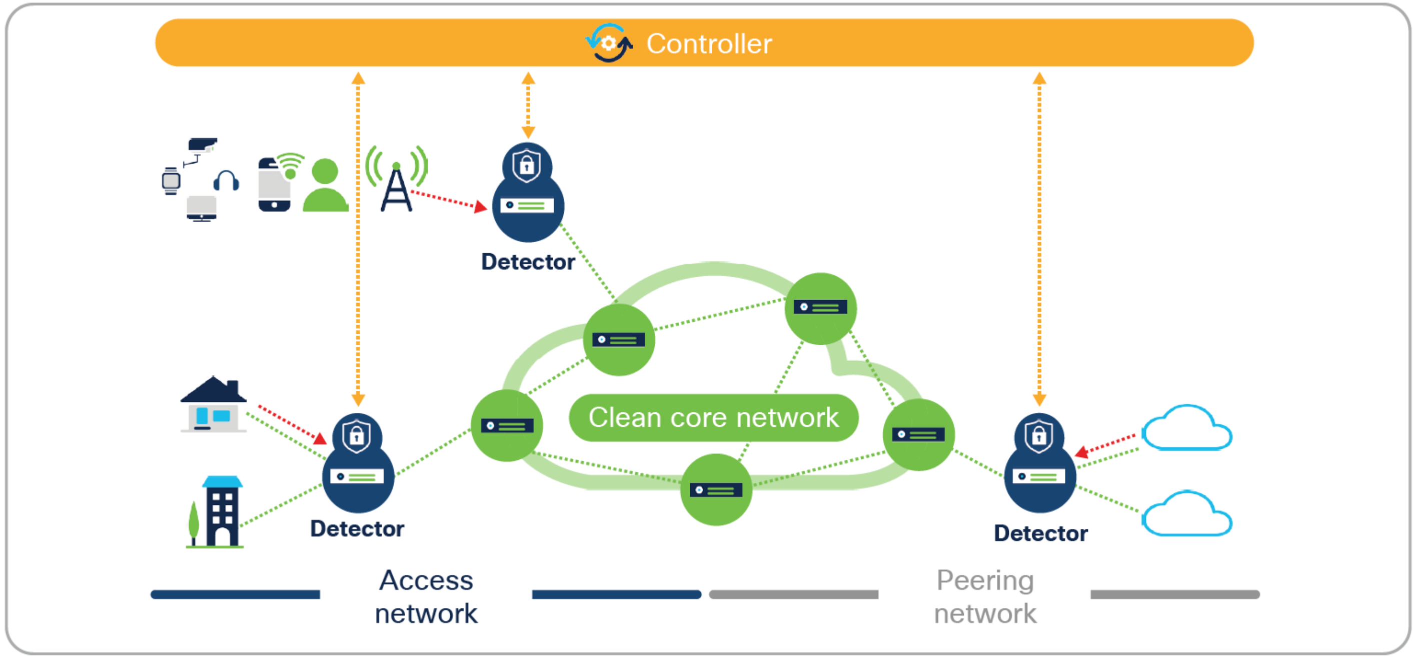


Use your routers as the first line of defense against DDoS attacks

Real-time on-box autonomous attack detection and mitigation	Protects quality of experience and the performance of low-latency applications
Software that requires no additional equipment, rack space, power, or cooling	Makes the solution cost-effective and scalable
Unsupervised machine learning algorithms	Ensures the flow of legitimate traffic while preventing malicious traffic from flooding the network
Automation, zero touch, and a central interface management function	Offers both ease of management and complete control

Scale your DDoS capabilities simply and cost-effectively as you scale your networks

Solution architecture



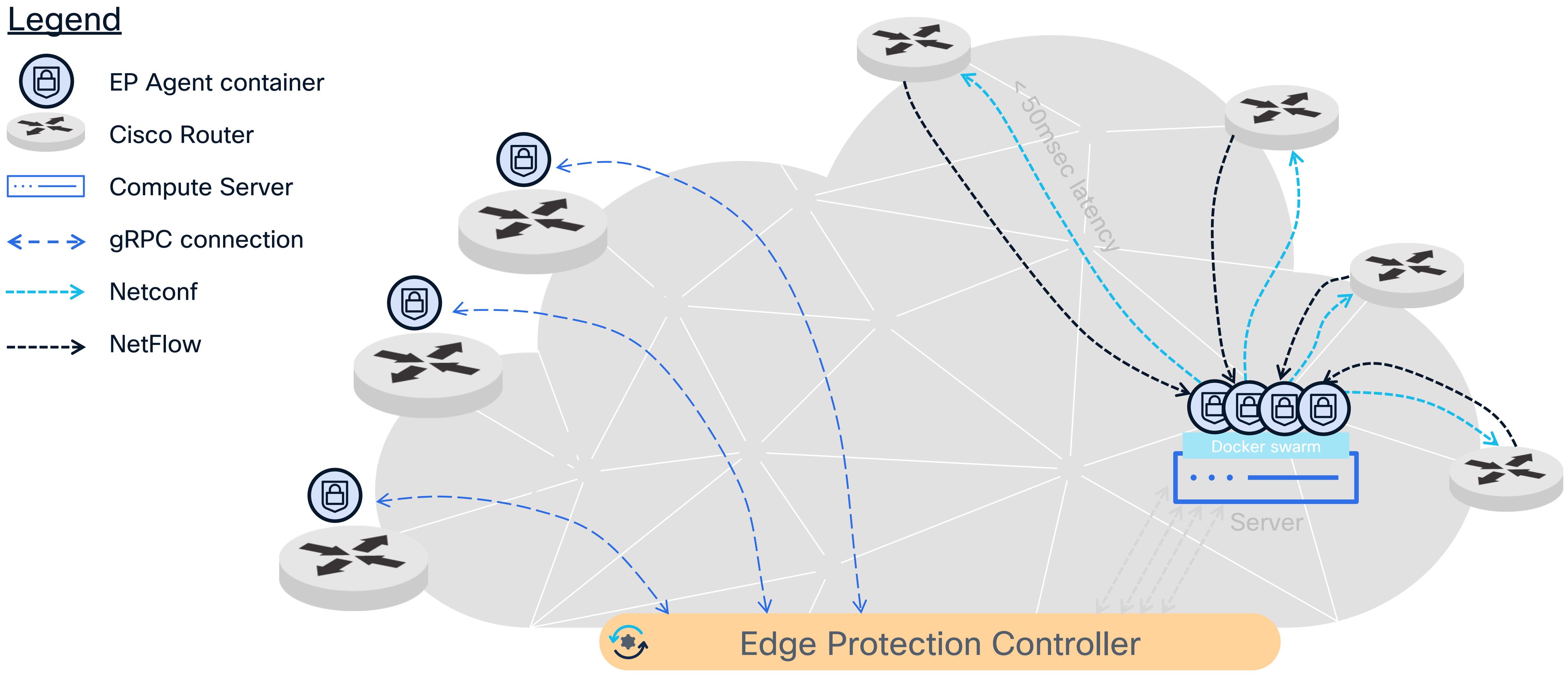
Controller

- 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

Agents / Detector

- A container deployed on a router, utilizing dedicated CPU and memory resources, collecting and analysing network telemetry.
- Employs *advanced ML 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.

Edge Protection deployment architecture On/Off Box



On-box: For Cisco Hardware
Off-box: Multi-vendor & Older Cisco hardware

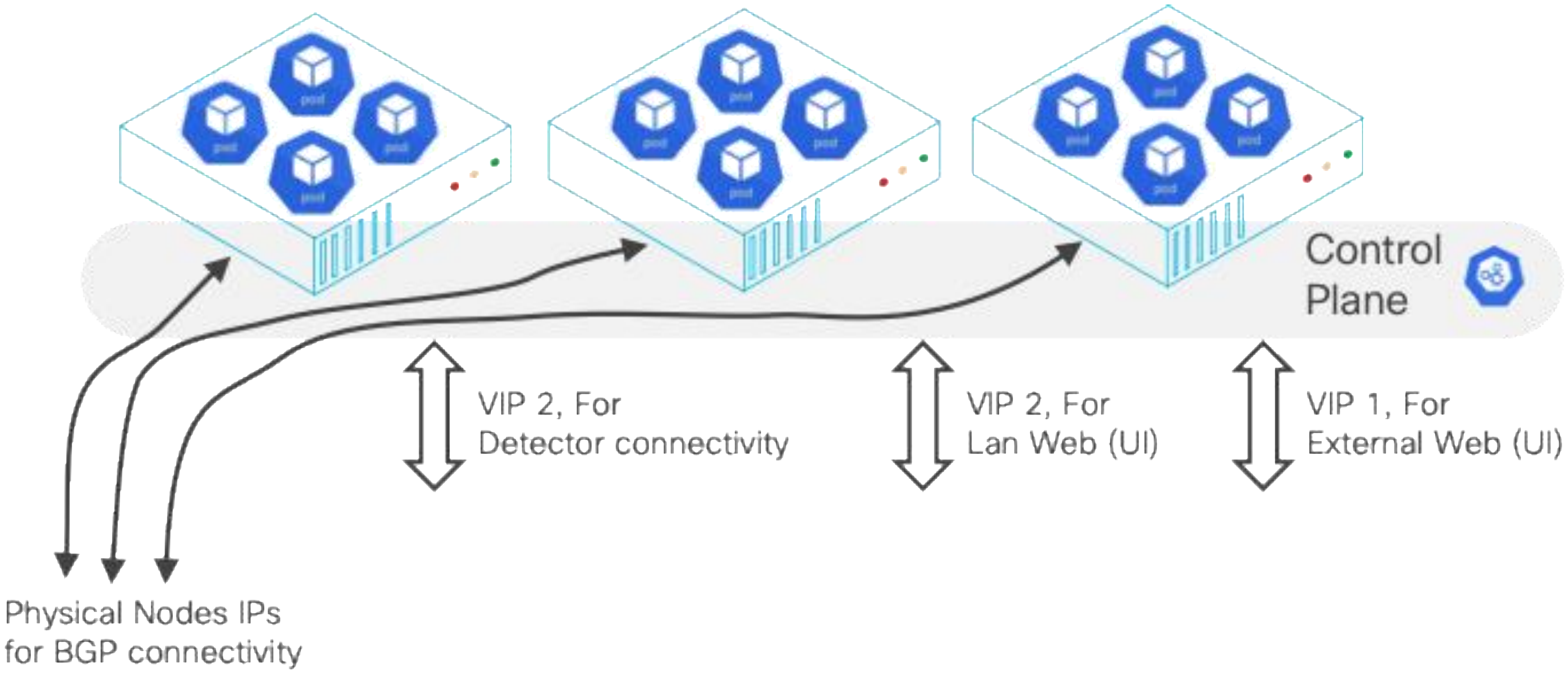
Edge Protection Controller design

- 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 Virtual IP Address (VIP)
- Connectivity to BGP using physical IP addresses of Nodes

Controller deployment contd...

Inter-node connectivity requirements for Geo HA:

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


pod
Control Plane
VIP 2, For Detector connectivity
VIP 2, For Lan Web (UI)
VIP 1, For External Web (UI)
Physical Nodes IPs for BGP connectivity

Peering

Ensure the availability of services despite constantly evolving threats

The challenge

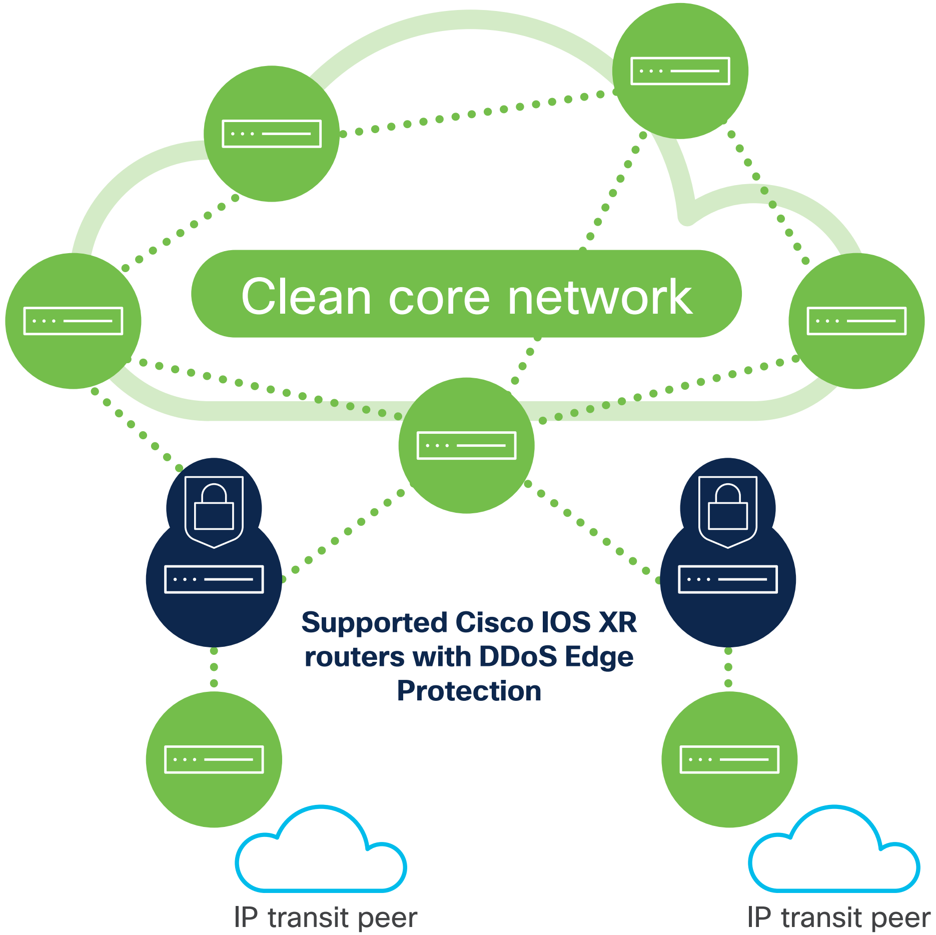
- Protecting peering against DDoS attacks is complex because *of the volume of traffic handled by peering nodes* and the range of protocols that perpetrators can exploit to target different services.
- Current approaches using *static misuse lists* are unable to identify zero-day attacks and protect 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.



Broadband

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

The challenge

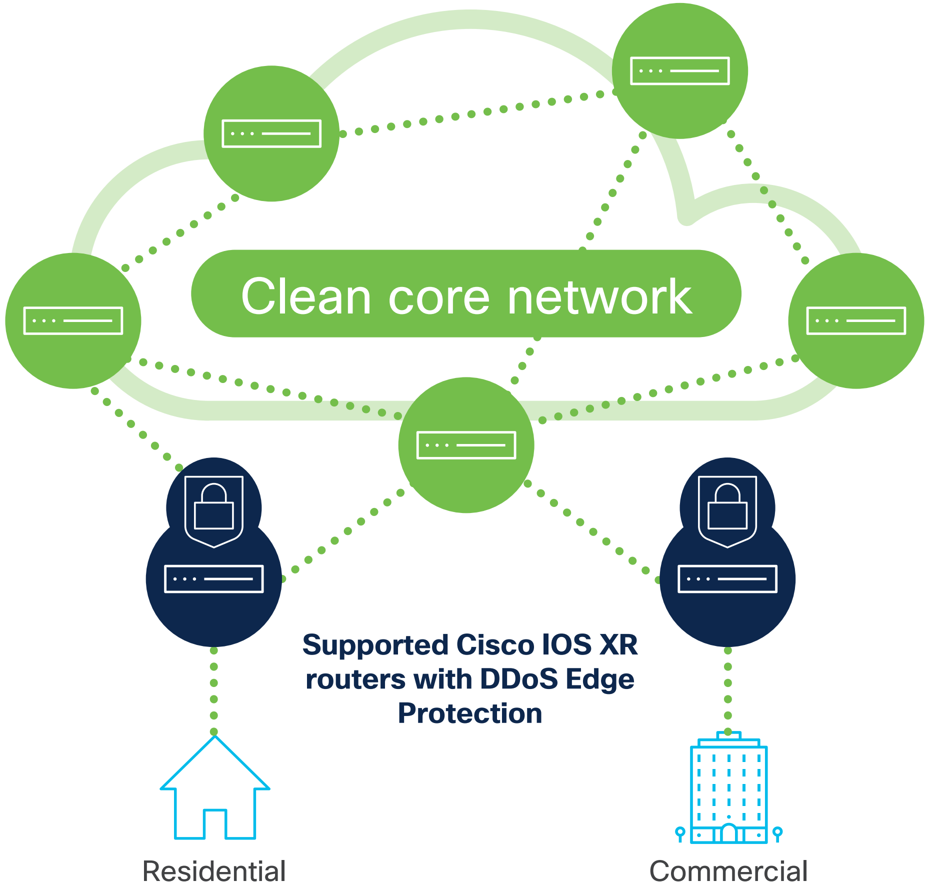
- New super-fast fiber-to-the-home networks *increase opportunities for perpetrators to exploit high-bandwidth CPE* and different end-user devices.
- The development of more distributed broadband architectures increases the risks of *DDoS attacks using local internet break-outs*.
- Users expect *flawless 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.

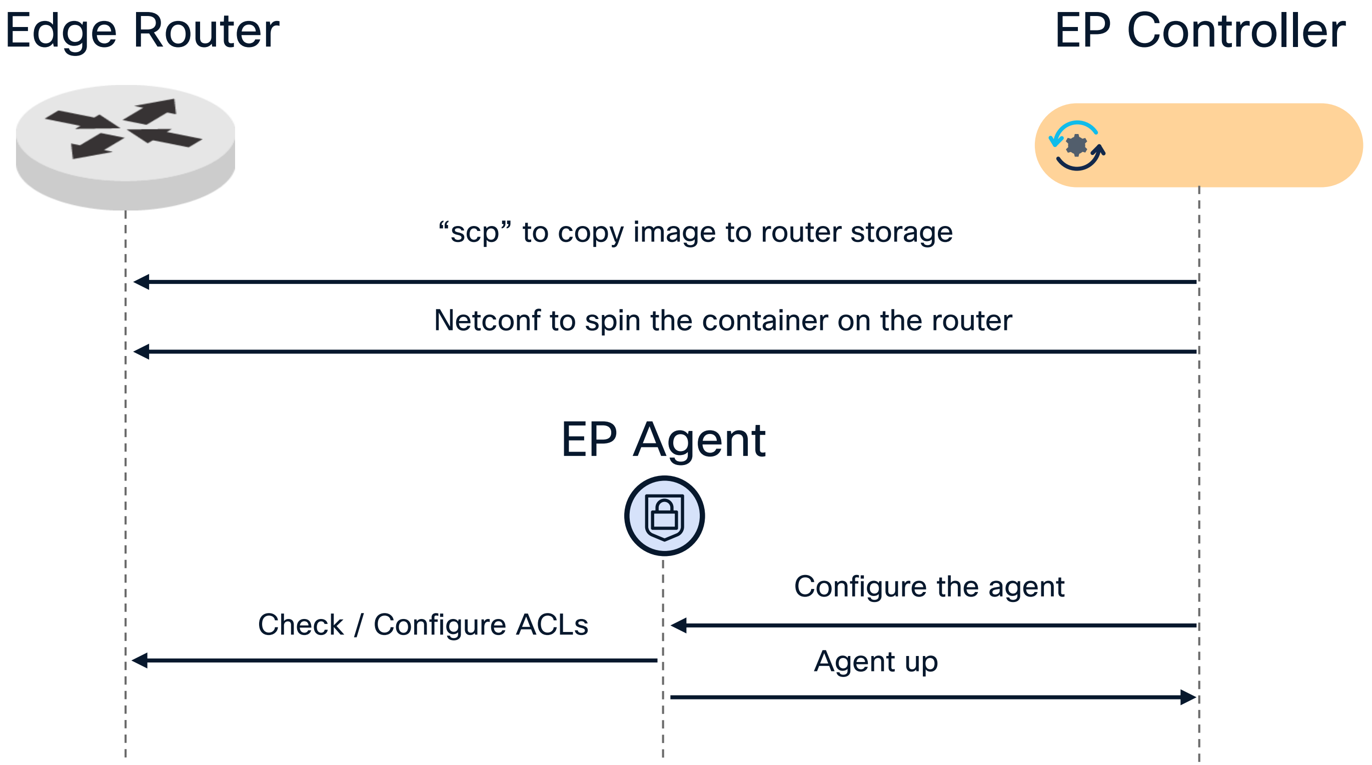


Comparison with traditional DDoS mitigation systems

Feature	Cisco Edge Protection	On-prem Scrubbing	Cloud DDoS Service
Time to Mitigation	Below 20 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 ACEs	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 & key features

Deployment and provisioning



Edge Router

EP Controller

“scp” to copy image to router storage

Netconf to spin the container on the router

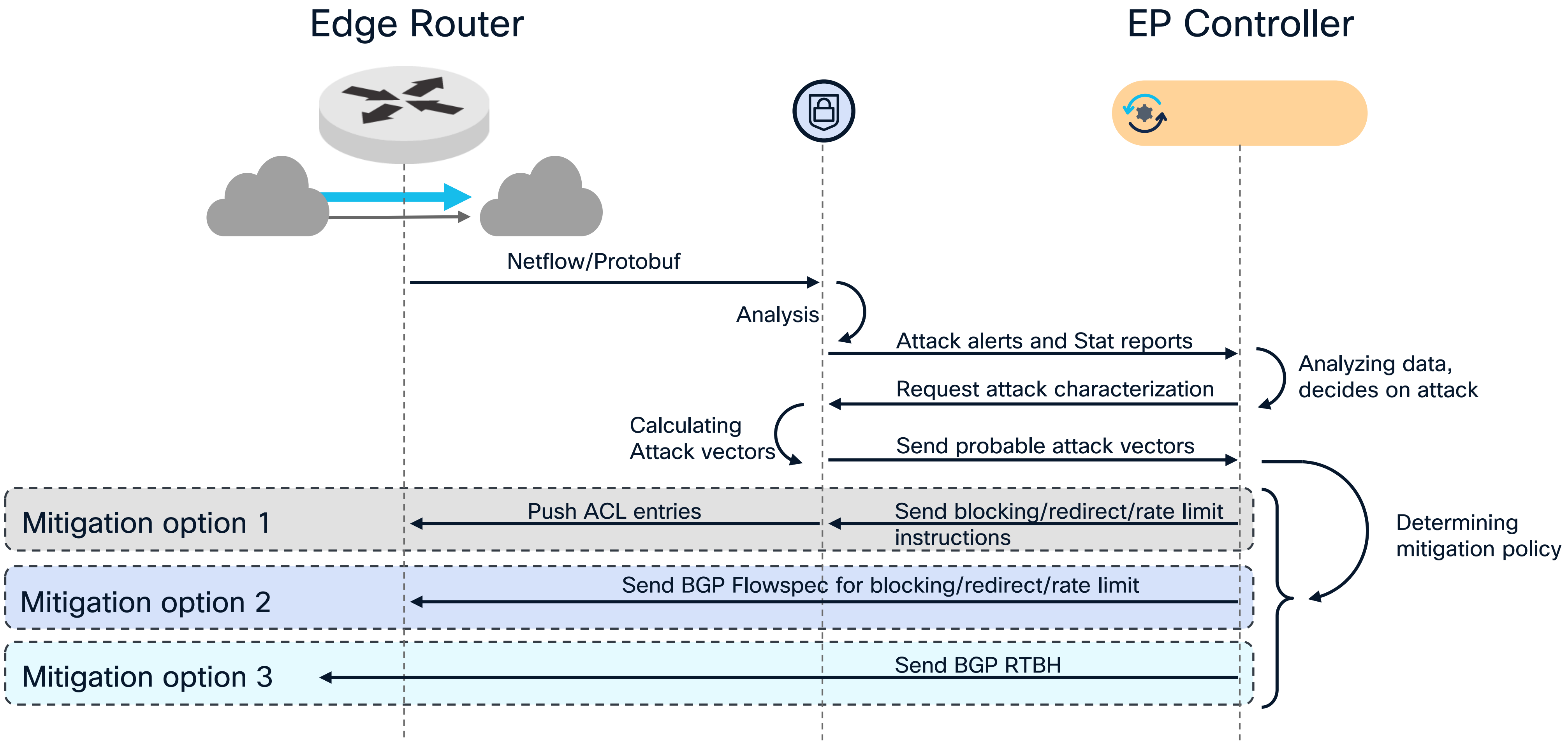
EP Agent

Configure the agent

Check / Configure ACLs

Agent up

Workflow With Edge Protection


Edge Router
EP Controller
Netflow/Protobuf
Analysis
Attack alerts and Stat reports
Analyzing data, decides on attack
Request attack characterization
Calculating Attack vectors
Send probable attack vectors
Determining mitigation policy
Mitigation option 1
Push ACL entries
Send blocking/redirect/rate limit instructions
Mitigation option 2
Send BGP Flowspec for blocking/redirect/rate limit
Mitigation option 3
Send BGP RTBH

Detection algorithm overview

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

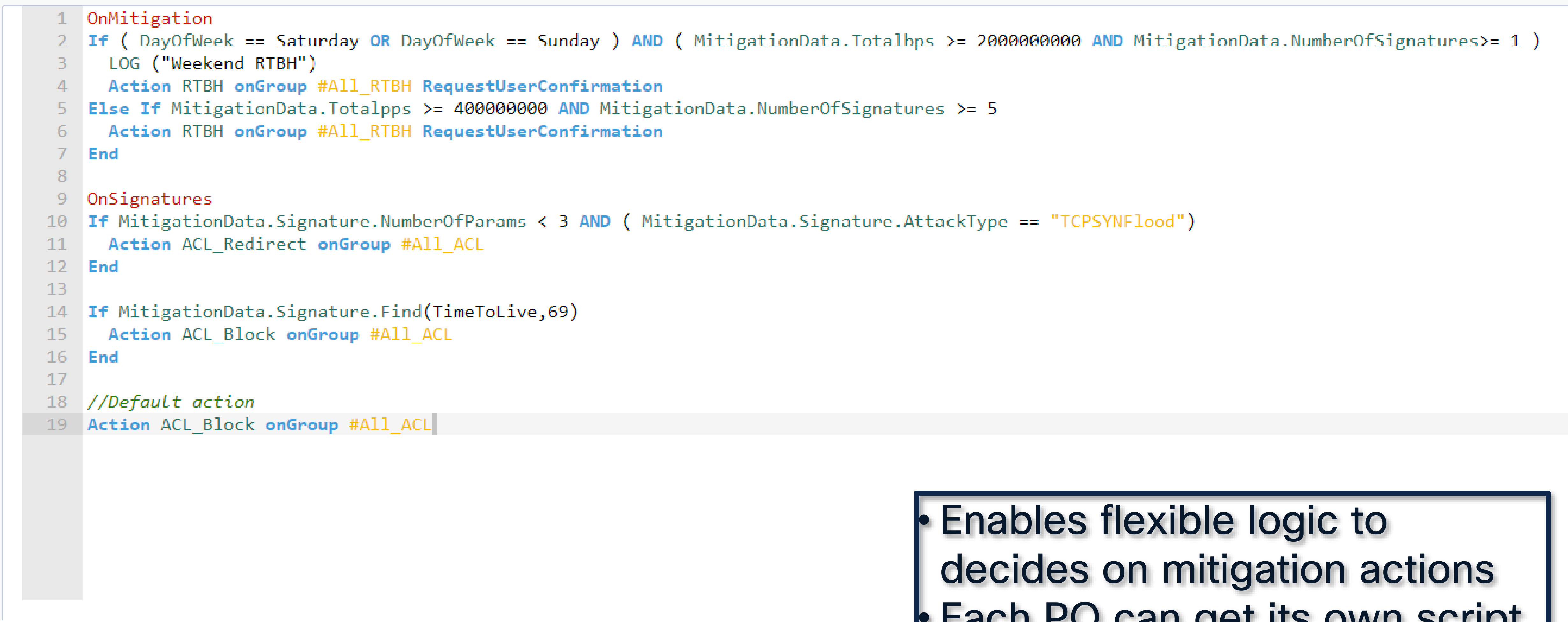
4. Learning scheduler
   - Set the learning duration (per PO) recommended 24 hours
   - Set the periodic learning intervals (daily, weekly...) recommended busy day once a week
   - Un-learnt hosts that appear between learnings learned as they appear

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

*Protected Object

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

Benefits of DDoS Edge Protection to Operators

Upto 83% of TCO savings

No dedicated Scrubbers & Backhauling

Fastest detection in market

~30 sec on average and ~10 sec mitigation helps meet SLAs

DDoS unique technology

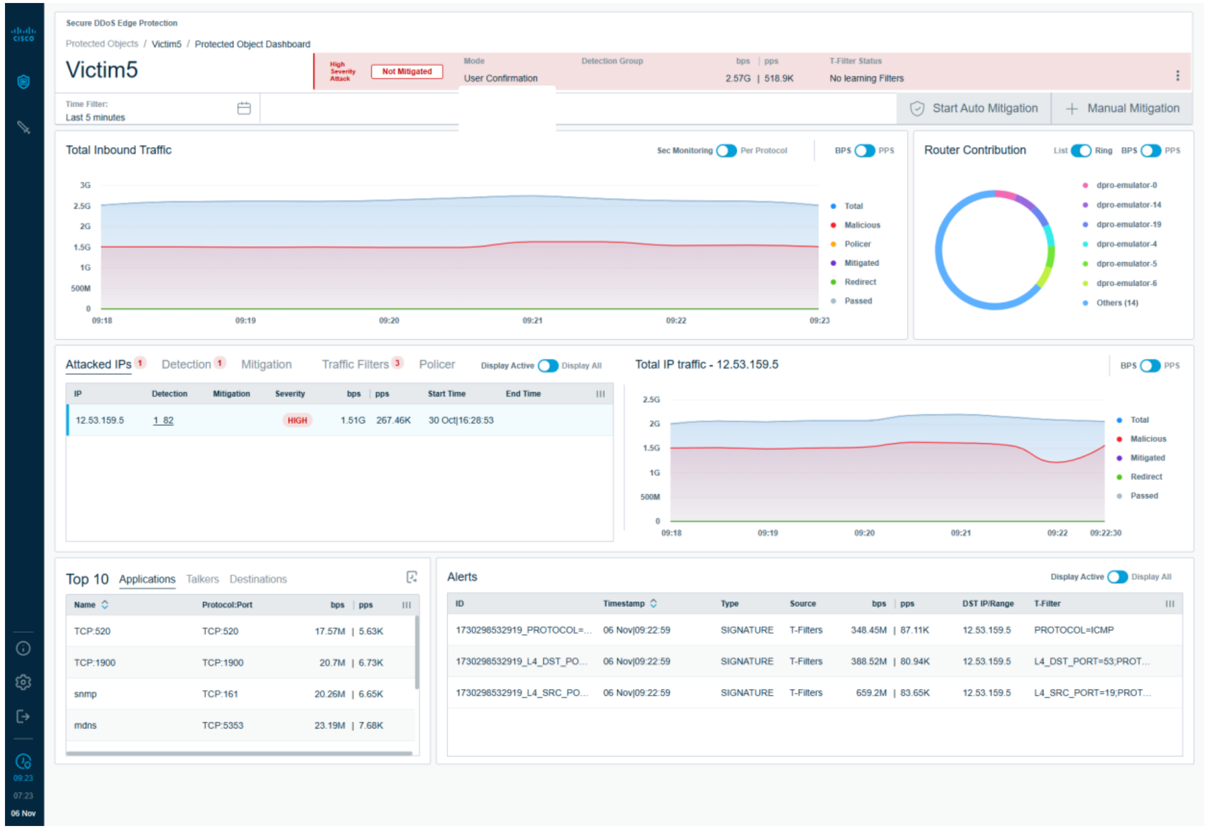
Dynamic Thresholds, Scripting Languages

Monetize the services

Creates additional revenue streams with the MSSP capability

MSSP Feature

MSSP (Managed Security Service Provider)



Victim5

High Severity Attack | Not Mitigated

Mode	Detection Group	bps | pps	T-Filter Status
User Confirmation		2.57G | 518.9K	No learning Filters

Time Filter: Last 5 minutes

IP	Detection	Mitigation	Severity	bps | pps	Start Time	End Time
12.53.159.5	1 82		HIGH	1.51G 267.46K	30 Oct|16:28:53	

Name	Protocol:Port	bps | pps
TCP:520	TCP:520	17.57M | 5.63K
TCP:1900	TCP:1900	20.7M | 6.73K
snmp	TCP:161	20.26M | 6.65K
mdns	TCP:5353	23.19M | 7.68K

ID	Timestamp	Type	Source	bps | pps	DST IP/Range	T-Filter
1730298532919_PROTOCOL=...	06 Nov|09:22:59	SIGNATURE	T-Filters	348.45M | 87.11K	12.53.159.5	PROTOCOL=ICMP
1730298532919_L4_DST_PO...	06 Nov|09:22:59	SIGNATURE	T-Filters	388.52M | 80.94K	12.53.159.5	L4_DST_PORT=53;PROT...
1730298532919_L4_SRC_PO...	06 Nov|09:22:59	SIGNATURE	T-Filters	659.2M | 83.65K	12.53.159.5	L4_SRC_PORT=19;PROT...

Real-time Visibility

Policy Management & Control

Reporting & Dashboards

Integration to existing systems

Key highlights of the MSSP feature

Creates a source of potential revenues

Supports tiering policies (Bronze, Silver, Gold)

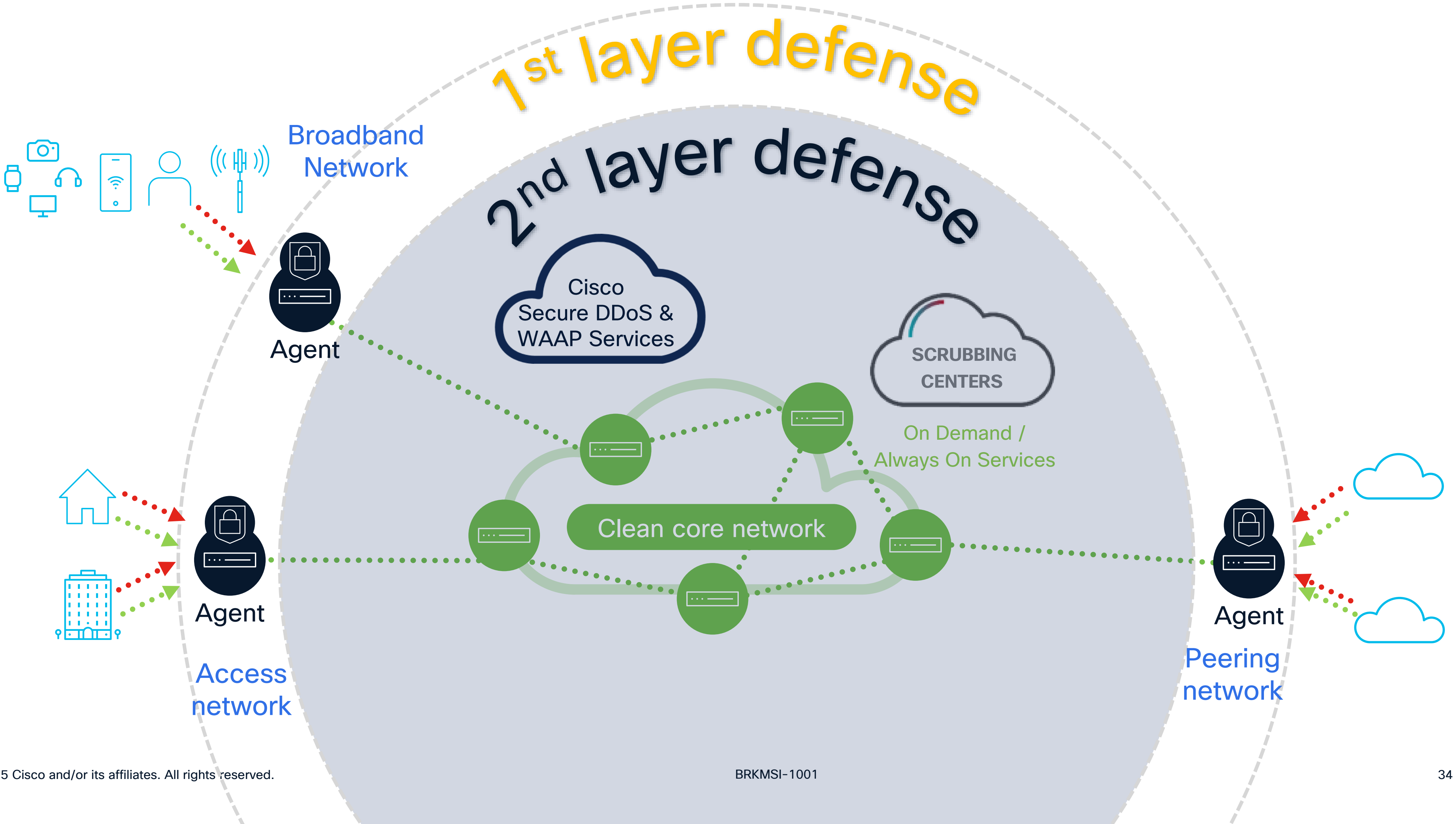
Allows to onboard up to 10K protected Customers

Brand awareness and reduces churn

Built-in support for MSSP, included with the License

Two-Layered DDoS Protection (for large networks)

Cisco DDoS Protection



Two-layered approach to secure a large-scale network

1

1st layer defence

Cleaning as much as possible on the edge of the network

- Turn your edge routers into security platforms
- Block 95% of the malicious traffic on the edge of the network – volumetric attacks etc.
- Software solution – leveraging available compute power in the routers

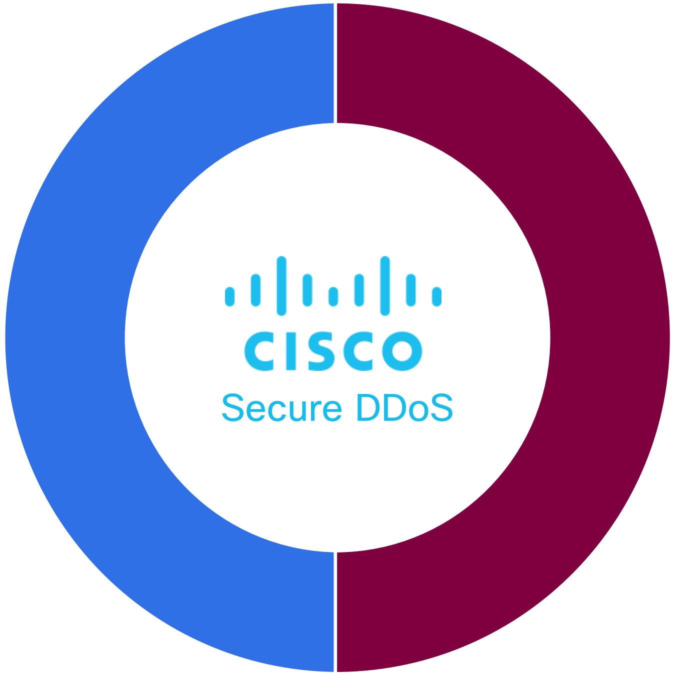
2

2nd layer defense

Addressing sophisticated attacks and specific security threats and protecting specific assets

- Addressing threats that require Layer 7 analysis
- Using pinpoint hardware-based solutions for specific threats or specific assets, such as DNS attacks.

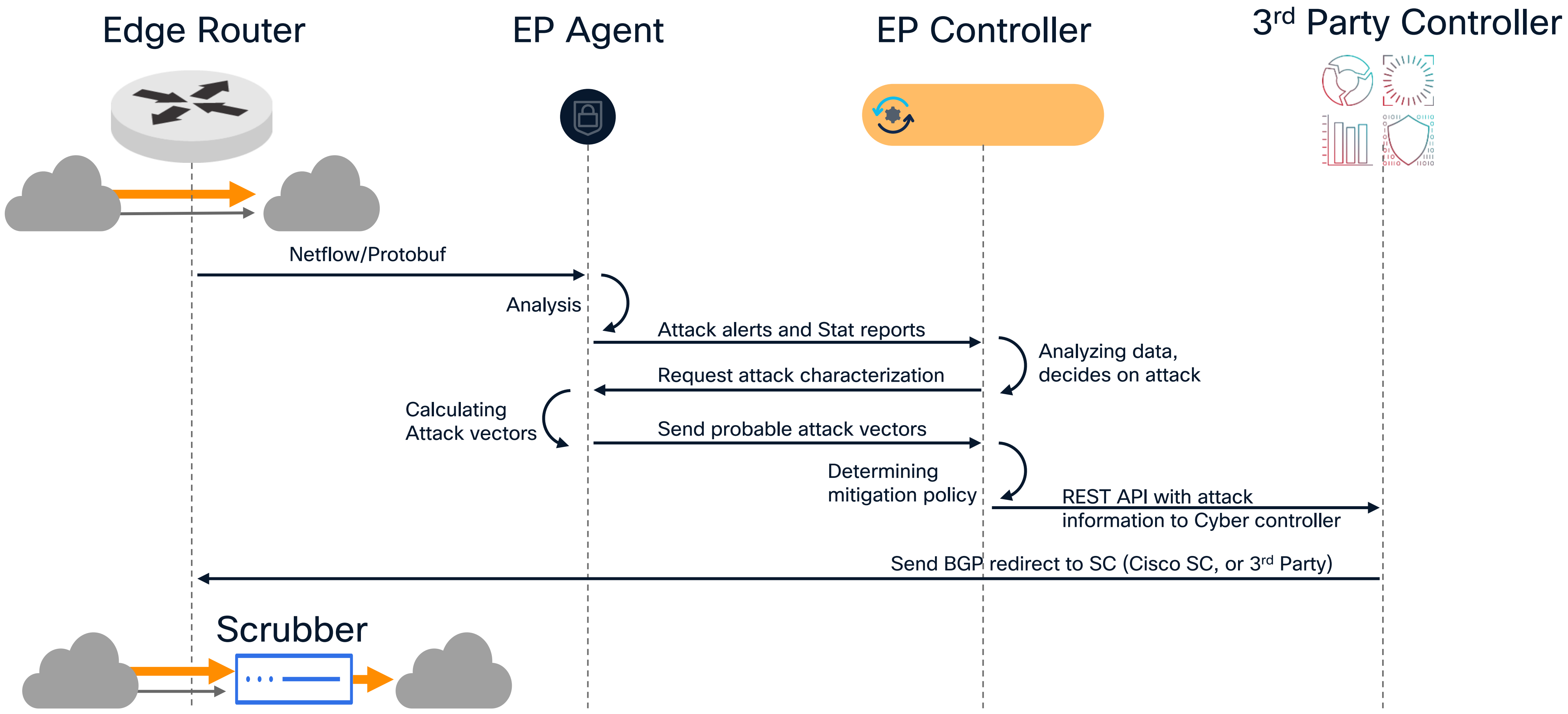
Edge Protection
Using edge routers
as first line of defense, creating a "clean
pipes" on the internal network



On-prem hardware
Using on-prem HW for specific attacks
on critical infrastructure like DNS, local
applications etc.

Workflow With Edge Protection –

Integration Into Cisco Secure Scrubbing Center + 3rd Party SC



Edge Router

EP Agent

EP Controller

3rd Party Controller

Netflow/Protobuf

Analysis

Attack alerts and Stat reports

Analyzing data, decides on attack

Request attack characterization

Calculating Attack vectors

Send probable attack vectors

Determining mitigation policy

REST API with attack information to Cyber controller

Send BGP redirect to SC (Cisco SC, or 3rd Party)

Scrubber

Customer Case Study

Edge Protection for B2B Services for UK Customer

Managed DDOS Protection
MSecure
Firewalls
Content Filtering

About customer

UK based SP focusing on enhancing the business transformation journey of handers of enterprises and public sector organizations in the new digital economy through service innovation and robust technology partners.

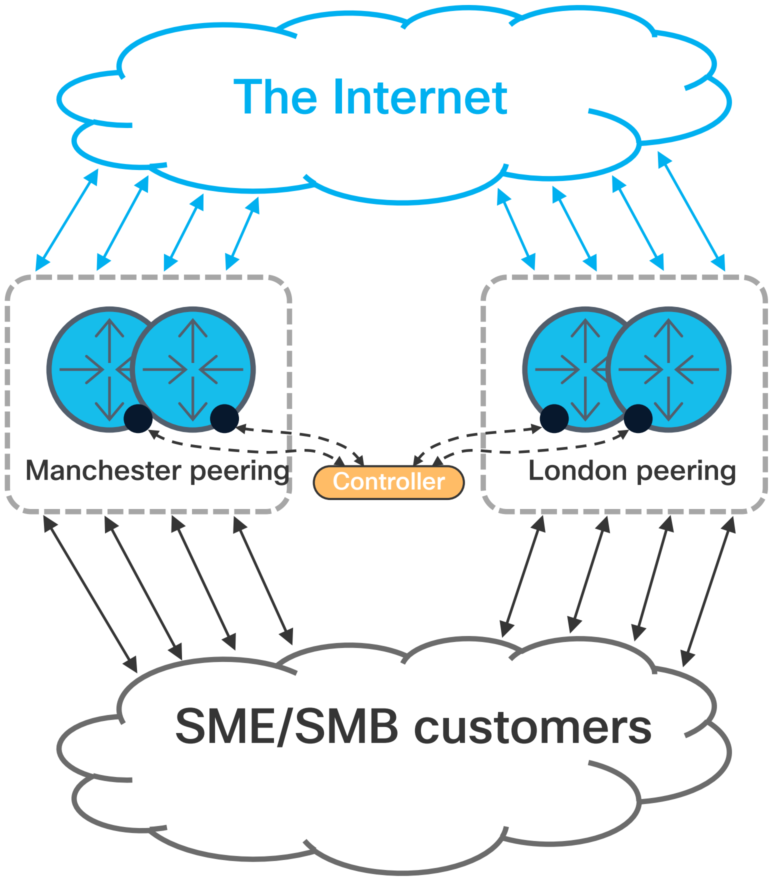
Customer Challenge

Customer faced a scale issue with existing DDoS inline scrubbing, the dilemma was to either add few more appliances and to existing architecture, or to look for a highly scalable modern cost-effective solution

Edge Protection for B2B Services for UK Customer

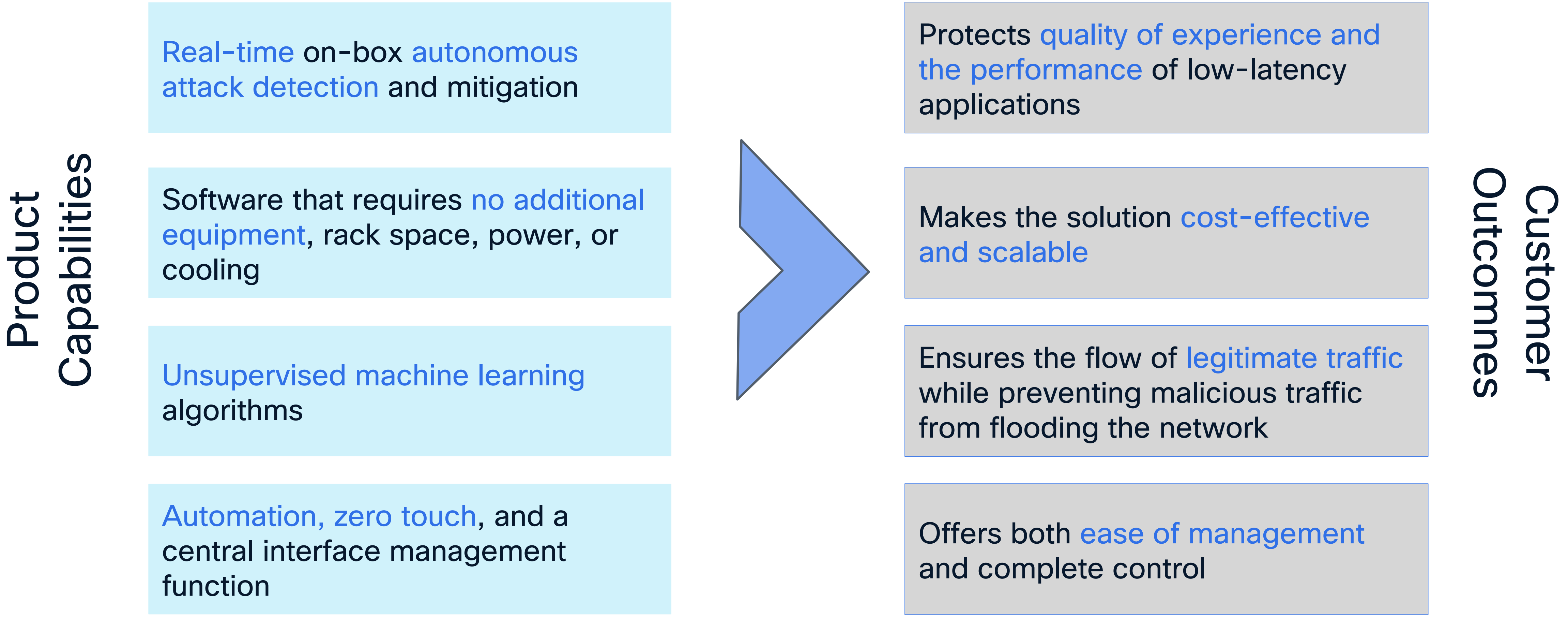
After evaluating multiple options, customer selected Cisco Edge Protection. This solution stood out for its unique integration with Cisco routers, offering robust DDoS defense capabilities as an add-on rather than requiring standalone appliances. Key advantages of Cisco's solution:

- **Scalability**: Seamless integration with customer's growing network infrastructure.
- **Flexibility**: Simplified creation of customized MSSP service packages to meet diverse client requirements.
- **Performance:** Near-instantaneous detection and mitigation of DDoS threats, ensuring minimal service interruptions.
- **Cost Efficiency**: Eliminating the need for separate appliances, significantly reducing capital and operational expenses.



Conclusion

Double up the router as defense against the defense attacks



Product Capabilities

- Real-time on-box autonomous attack detection and mitigation
- Software that requires no additional equipment, rack space, power, or cooling
- Unsupervised machine learning algorithms
- Automation, zero touch, and a central interface management function

Customer Outcomnes

- Protects quality of experience and the performance of low-latency applications
- Makes the solution cost-effective and scalable
- Ensures the flow of legitimate traffic while preventing malicious traffic from flooding the network
- Offers both ease of management and complete control

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 2026.

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: rakolaga@cisco.com

Thank you

cisco Live!