
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Cisco Secure Edge Protection

Protecting the 5G Edge & other “Edges” against DDoS attacks

Michael Geller – Distinguished Architect
@michaelge11er

BRKSPG-2401

Cisco Webex App

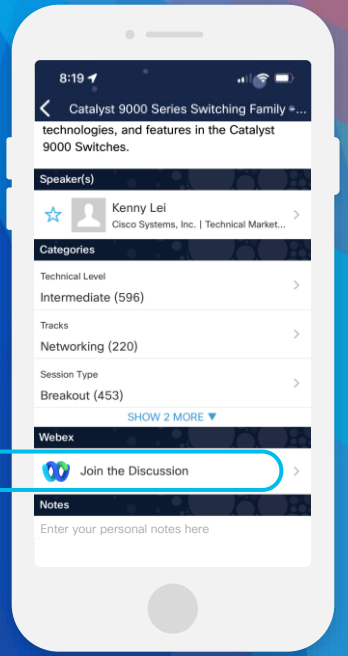
Questions?

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 9, 2023.



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

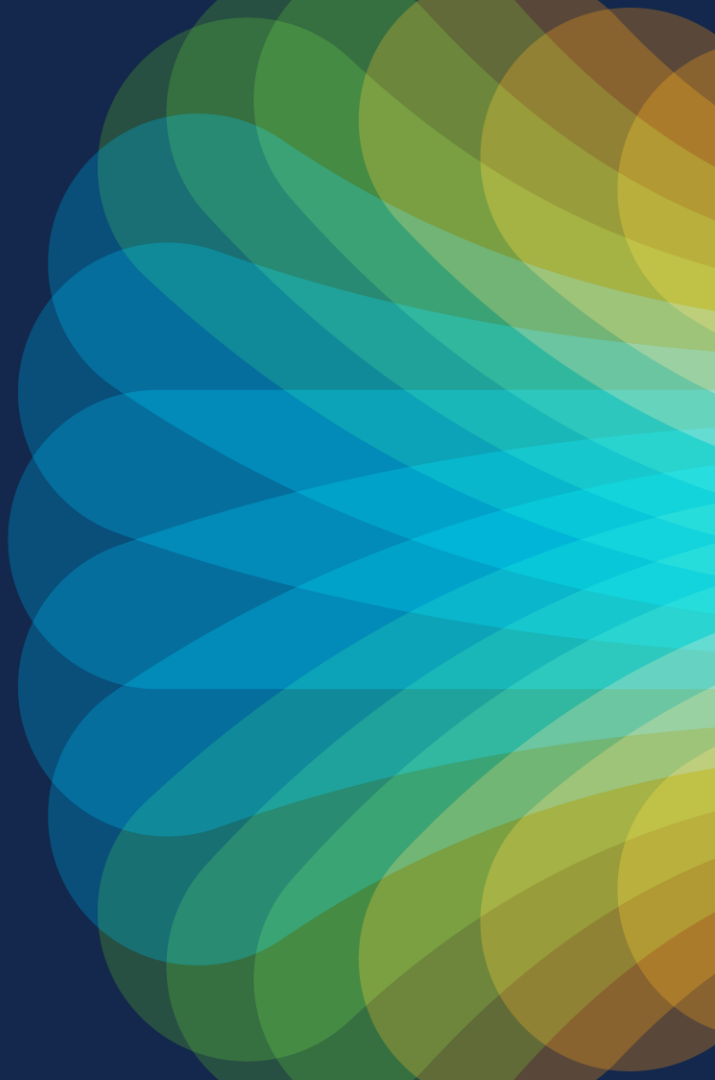
Agenda

- Introduction
- Which Edge?
- Cisco Secure DDoS Edge Protection
- Cisco Secure Edge Protection Demo
- What To Do Next

My Personal & Professional Life

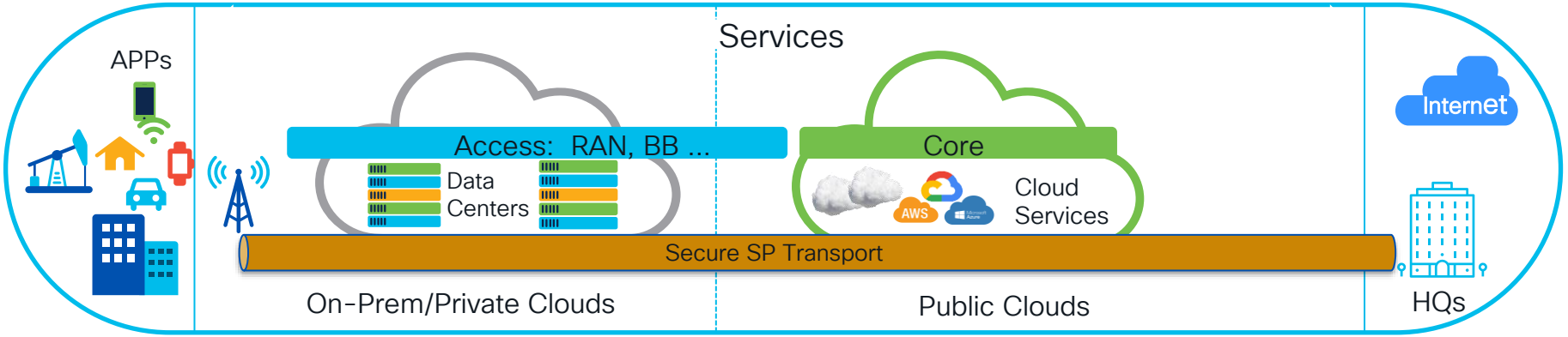
- Distinguished Architect @ Radware
- 25 Years in Cisco
- Distinguished Speaker
- Cloud and SP Security
  - “Securing critical apps and the networks that deliver them”
- Areas of focus: DDoS, 5G, AppSec, SecOPS
- 2 kids, 1 wife
- 4th Degree Black Belt, TKD

Introduction



Which Edge? Where Do I Start? - Availability

Simply: Protect the Control Plane, the Data Plane & the Services Plane



Device Threats

- Malware
- Bots DDoS
- Firmware Hacks
- Device Tampering
- Sensor Susceptibility
- TFTP MitM attacks
- Client side vuls

Air Interface & RAN Threats

- MitM attack
- Jamming
- Rogue Nodes Insecure S1, X2
- Insecure Xx, Xn
- Insecure F1x
- Encryption

MEC & Backhaul Threats:

- DDoS attacks
- LI Vulnerabilities
- Insecure Sx & N6
- MEC Backhaul sniff
- Side Channel attacks
- NFVi Vulnerabilities
- K8s & API Security
- Automation

Cloud & Cloud Edge Threats

- Permission Sprawl & Identity Policy Management – cross cloud
- Event management – cross cloud
- Application vulnerabilities
- API vulnerabilities

Infrastructure & OAM Threats

- Virtualisation
- LI Vulnerabilities
- Access Control
- Network Slice security
- API vulnerabilities NEF vulnerabilities
- Roaming Partner DDoS & DoS attacks
- Trust / Zero Trust
- Routing / BGP / RPKI

Problem Statement

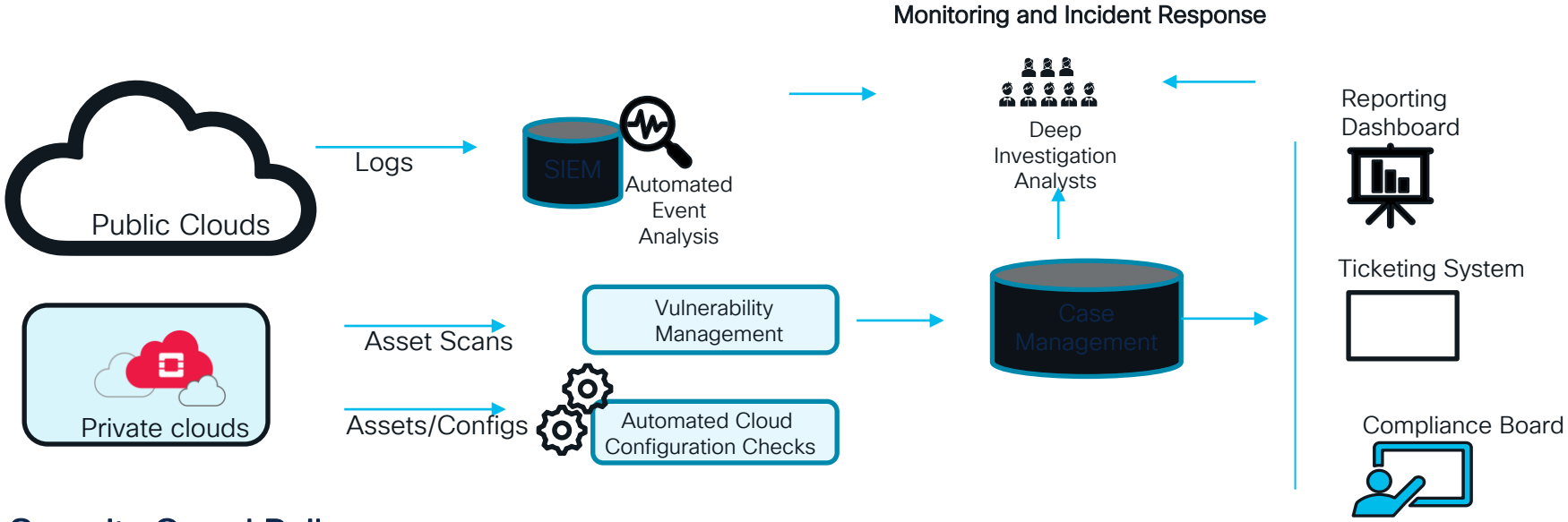
- 5G is about the user experience – outcome based
- To deliver the desired user experience → Low latency focus
- To deliver low latency outcomes, implement at “the edge”
- Agile security for 5G & requires autonomy – Optimizes 5G Networks

DDoS Attack Protection at the 5G Network Edge
What Does This Mean for Security?

- Security moves to the edge too
- Solves for new threat vectors in 5G → Higher power UE and IoT
- What are the “outcomes?”:
  - Fixed mobile broadband, Connected X (Cars, stadiums, …), Gaming, Virtual reality

The SecOps Perspective

What's Missing? – DDoS Protection for Applications and the Network

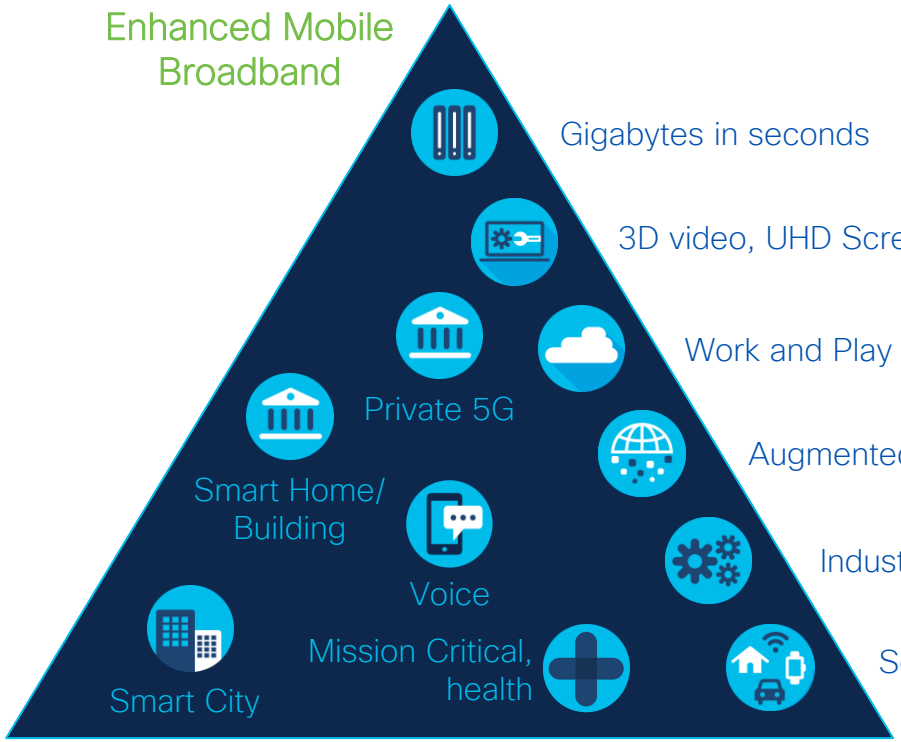


Security Guard Rails

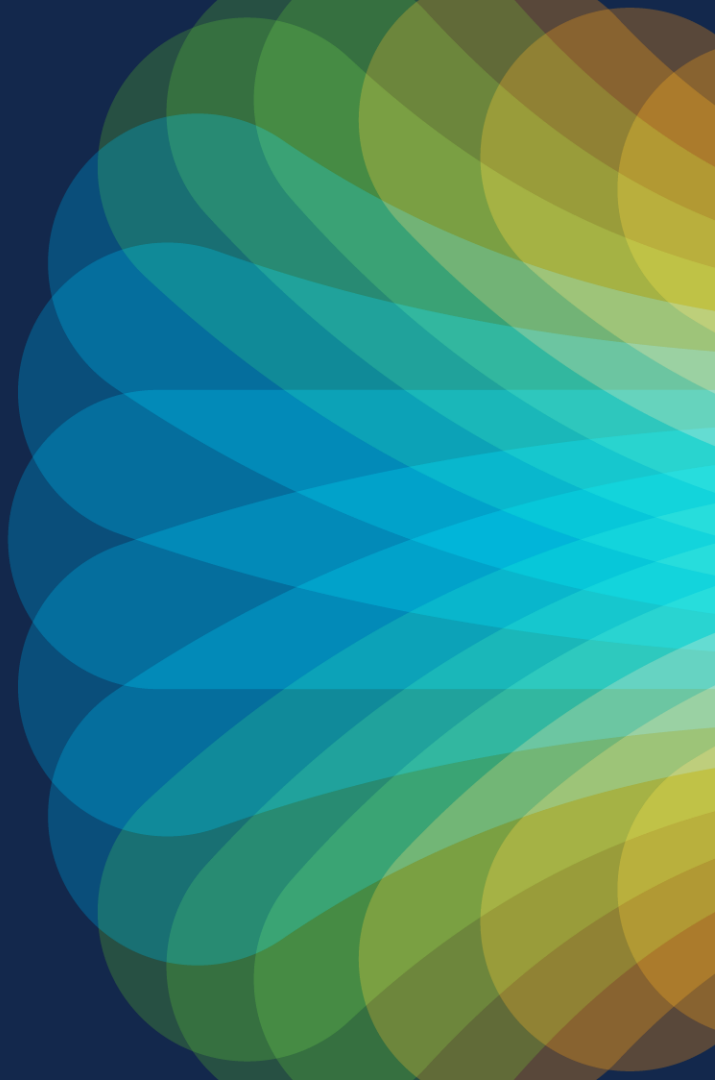
- Enforce Strong Identity
- Set Up Bastion/Jump Host for Secure Access
- Harden Base OS for VMs
- Network Zoning (VPC) to restrict external exposure
- Enable Vulnerability Scanning
- Enable Security Logging And Monitoring
- Create Account Level Encryption Key
- Harden/Securely Configure all AWS Components
- Tagging of resources and Asset Attribution
- Automated Security Audits

Use Cases –Business View

[Munib Shah's Session - BRKSPM-2027]

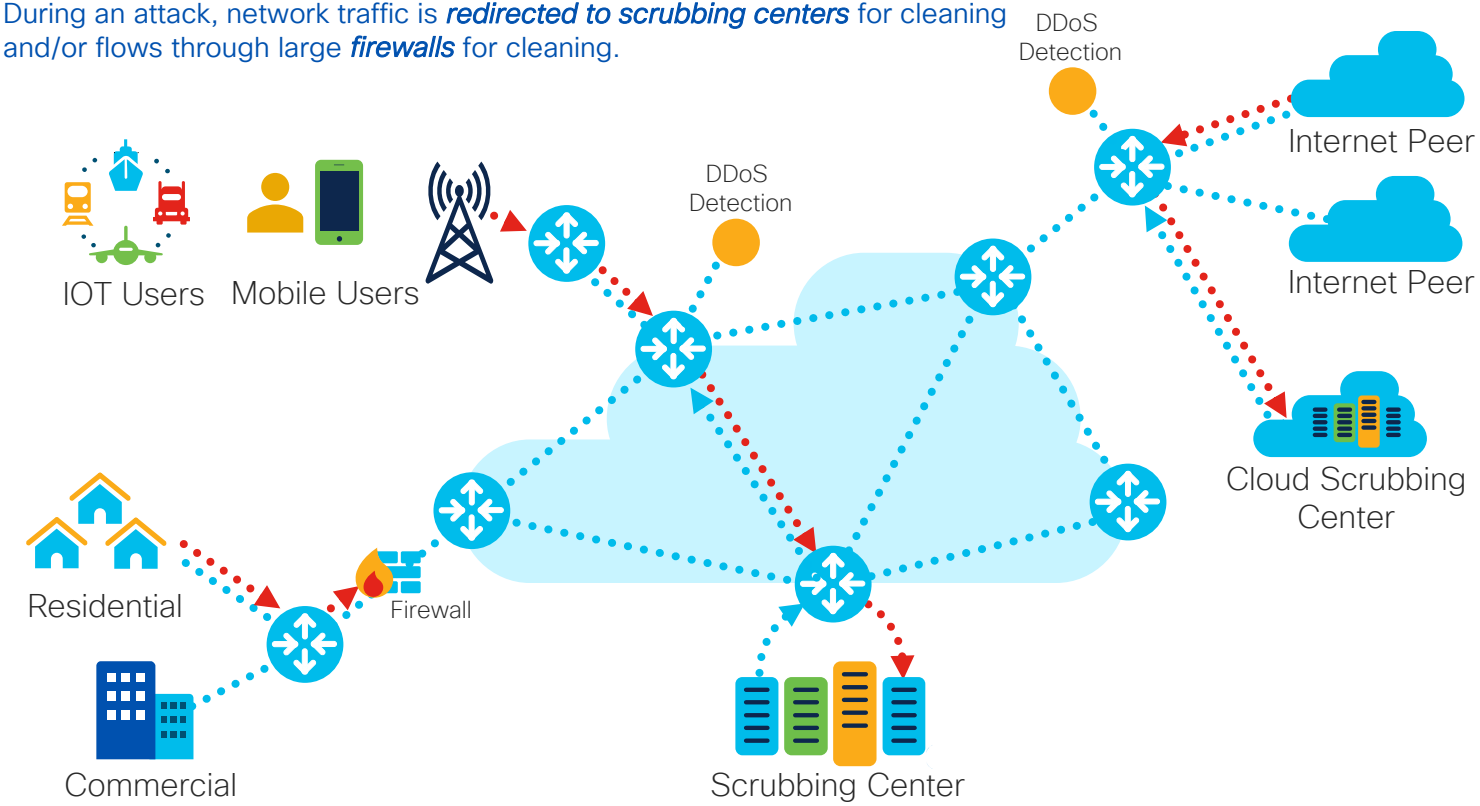


Which Edge?



Present mode of operation

During an attack, network traffic is ***redirected to scrubbing centers*** for cleaning and/or flows through large ***firewalls*** for cleaning.

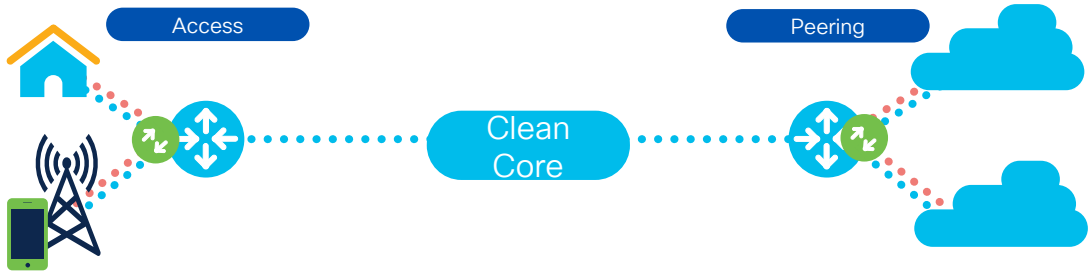


DDoS Edge Protection operation

Routers at the network edge detect and clean DDoS traffic.

EdgeProtect DDoS Benefits

EdgeProtect DDoS delivers customers the ability to build a ***self-defending network***. Combining the power of Cisco's edge routing portfolio and RadWare's expertise in the DDoS protection, EdgeProtect DDoS enables a Cisco router to ***detect and mitigate DDoS traffic*** at the network edge without the need for dedicated firewalls, DDoS detection infrastructure or scrubbing centers.



Efficacy

- 99% efficacy rate
- Eliminate DDoS at network edge
- Protect against infected subscribers
- Integrated into network

User Experience

- Line speed scrubbing
- 0 ms latency vs. 30+ ms ++
- Increased reliability and uptime
- Improved user experience

Lower Costs

- Remove DDoS traffic from network
- Simplified operational model
- Reduce power and cooling costs
- No dedicated infrastructure

Mobile access

Protect the performance of low-latency applications

The challenge

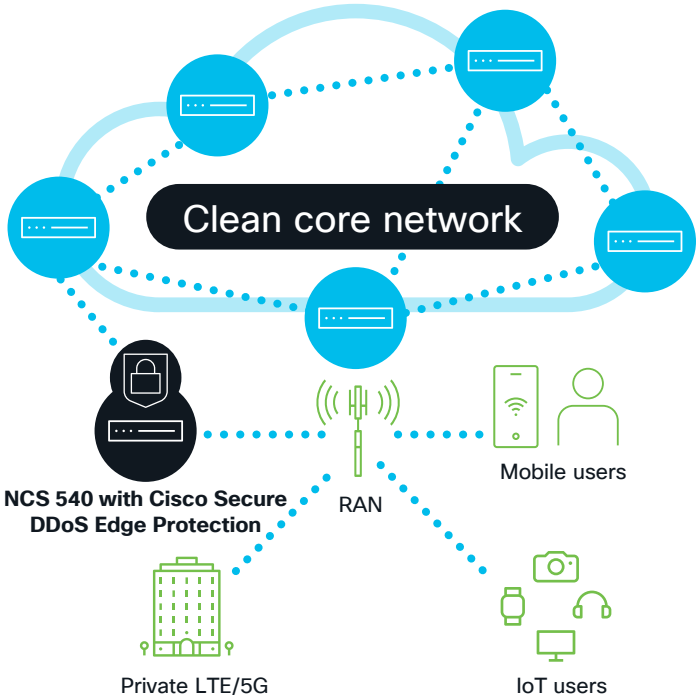
- The proliferation of mobile and IoT devices creates new opportunities for cyber criminals to launch DDoS attacks.
- Traditional DDoS solutions can only detect attacks once the traffic exits the encrypted GTP-U tunnel – when it is too late.
- Backhauling mobile and IoT traffic to scrubbing centers is 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, on the cell site router at the network edge, before they spread to applications in the MEC or in the packet core.
- 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).



Peering

Ensure the availability of services despite constantly evolving threats

The challenge

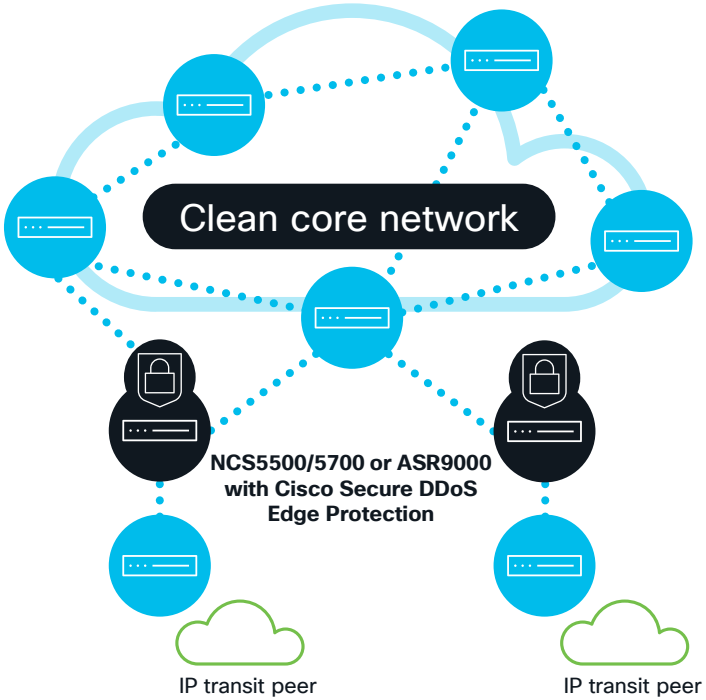
- Protecting peering against DDoS attacks is complex because of the volume of traffic handled by peering nodes and the range of protocols that perpetrators can exploit to target different services.
- Current approaches using static misuse lists are unable to identify zero-day attacks and protect the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

The challenge

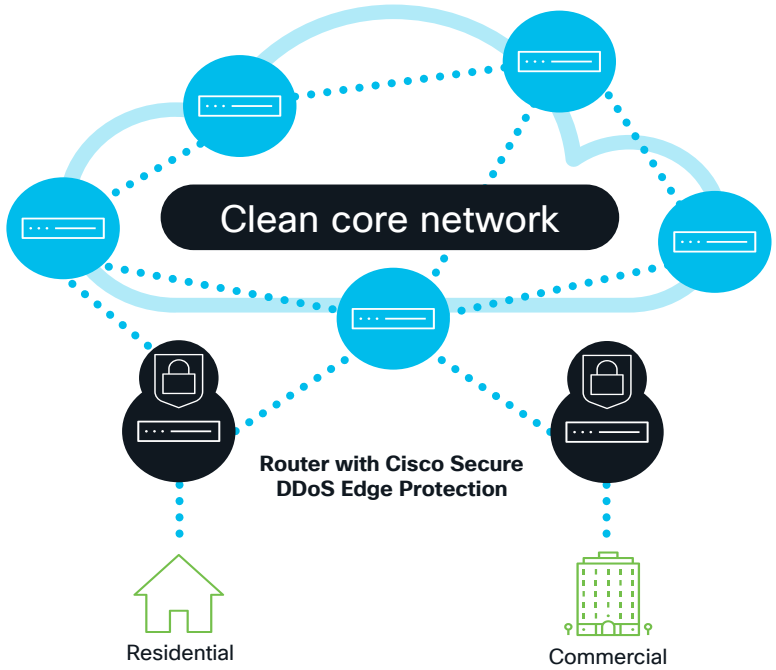
- New super-fast fiber-to-the-home networks increase opportunities for perpetrators to exploit high-bandwidth CPE and different end-user devices.
- The development of more distributed broadband architectures increases the risks of DDoS attacks using local internet break-outs.
- Users expect flawless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

- Gives full visibility over threats emerging at Internet breakouts by characterizing attacks and their signatures in real-time, and by dynamically adapting 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.

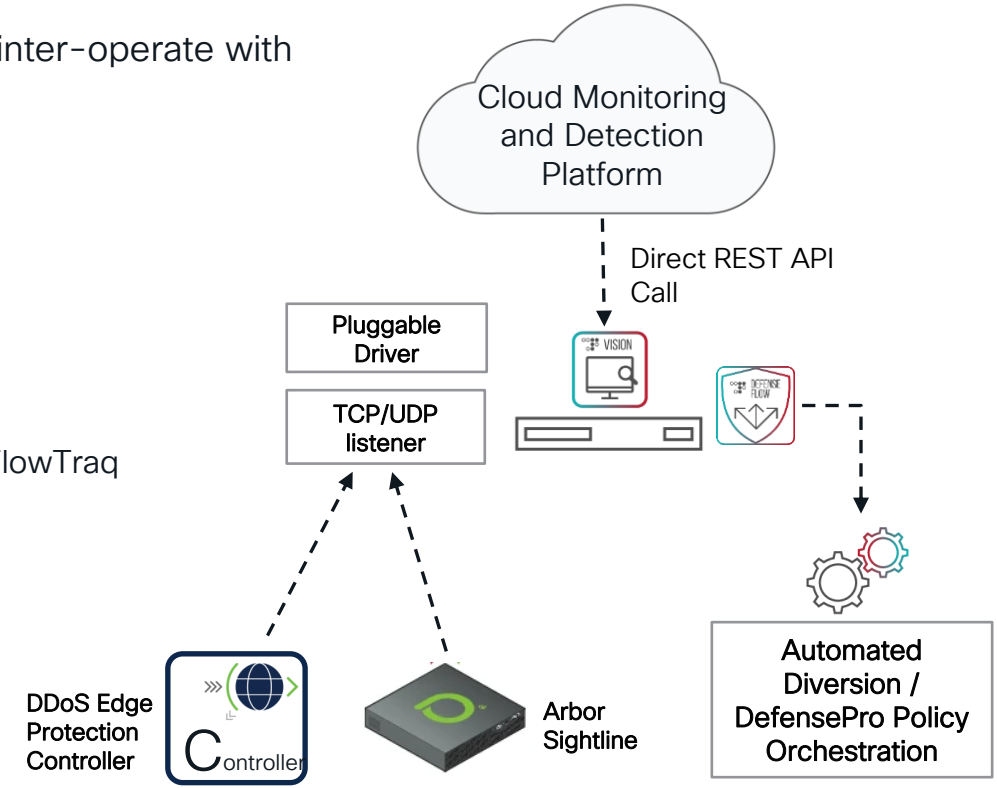
The outcome

- 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.

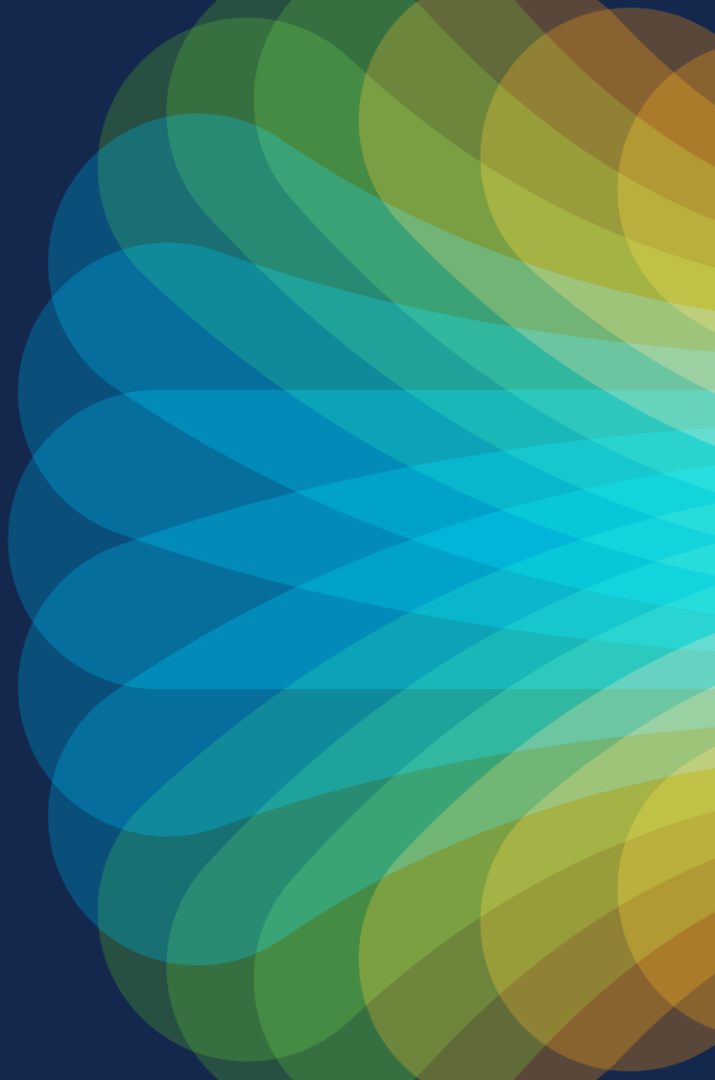


What If I Already Have DDoS Protection?

- **DefenseFlow Cyber Security Controller** can inter-operate with other detection devices:
- Two methods:
  - Third party Detection Driver
    - StealthWatch, Genie, FastNetMon, Sightline
  - Detection REST API
    - Singularity (Crossworks…) , Kentik, Deepfield, FlowTraq
- Device Drivers on Radware Portal

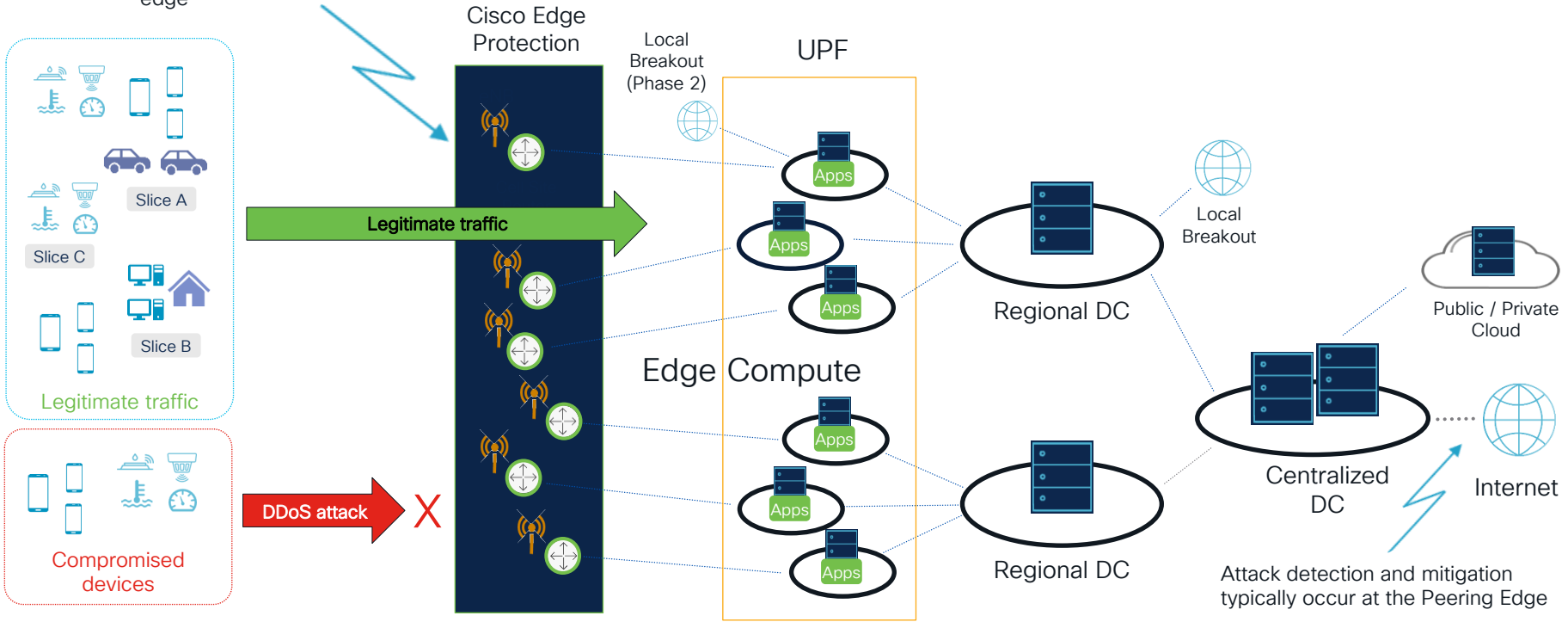


Cisco Secure DDoS Edge Protection

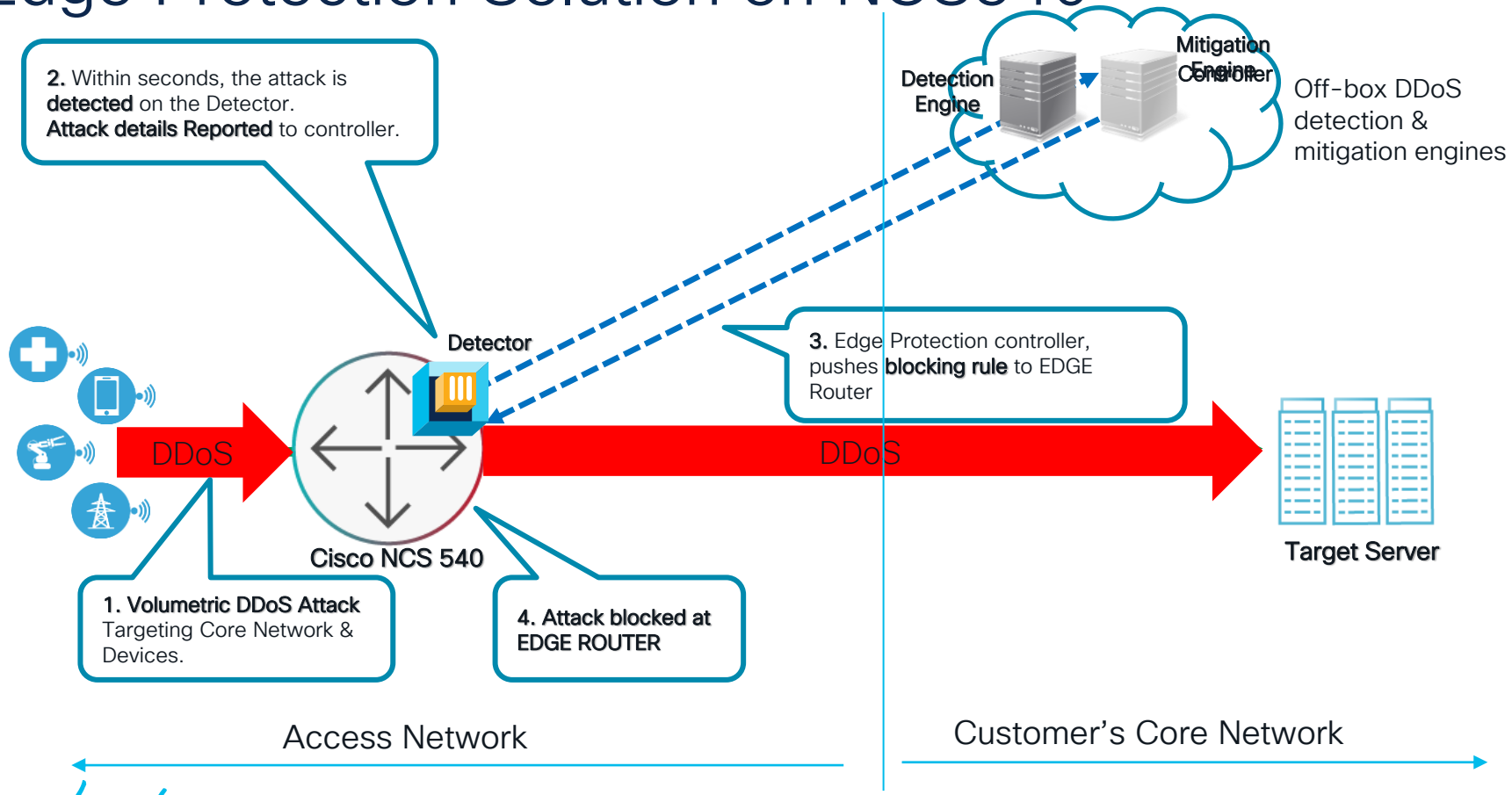


DDoS Attack Protection at the 5G Network Edge

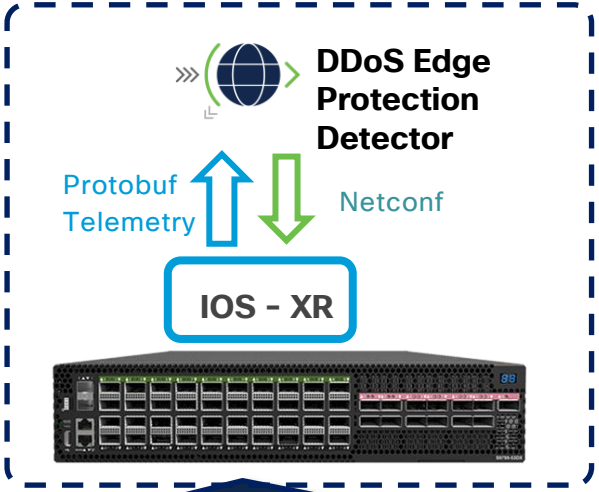
Cisco Secure DDoS Edge Protection stops DDoS attacks at the network edge



Edge Protection Solution on NCS540



DDoS Edge Protection Software Components



gRPC

Controller

DDoS Edge Protection Controller

Detectors. Key features & functions:

- Installed by Controller, authenticated via mTLS.
- Deployed as a docker container on IOS-XR.
- Telemetry managed via templates. Multiple usecases.
- Detects attacks locally.
- Enforces mitigation locally on the router “ingress” port.
- Reports every 2 sec to the controller.

Controller. Key features & functions:

- Manages container lifecycle for a fleet of detectors.
- Configures and edits detector profiles and security settings via template library.
- Health checks detectors.
- SecOps dashboard displays real-time attacks info, forensics and threat intelligence.
- Controls DDoS attack lifecycle from a single perspective.
- Provides real-time and historical reporting of events.
- Provides operational control and incident response.

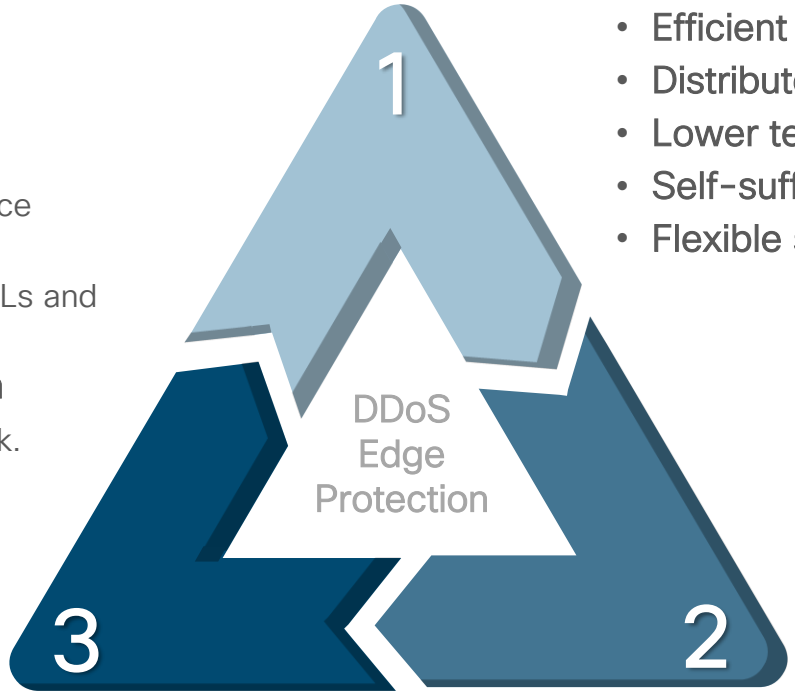
Improvements In All Three Dimensions

DETECTION

- **Efficient Telemetry.** Protobuf.
- **Distributed** across edge routers.
- **Lower telemetry overhead.**
- **Self-sufficient** Quantile DDoS Algorithm.
- **Flexible sampling rates** per use case.

MITIGATION

- **Granular** rules for service restoration.
- **Wire speed** TCAM ACLs and Quota management.
- **Network optimization**
- **Scales** with the network.
- **Fully automated.**

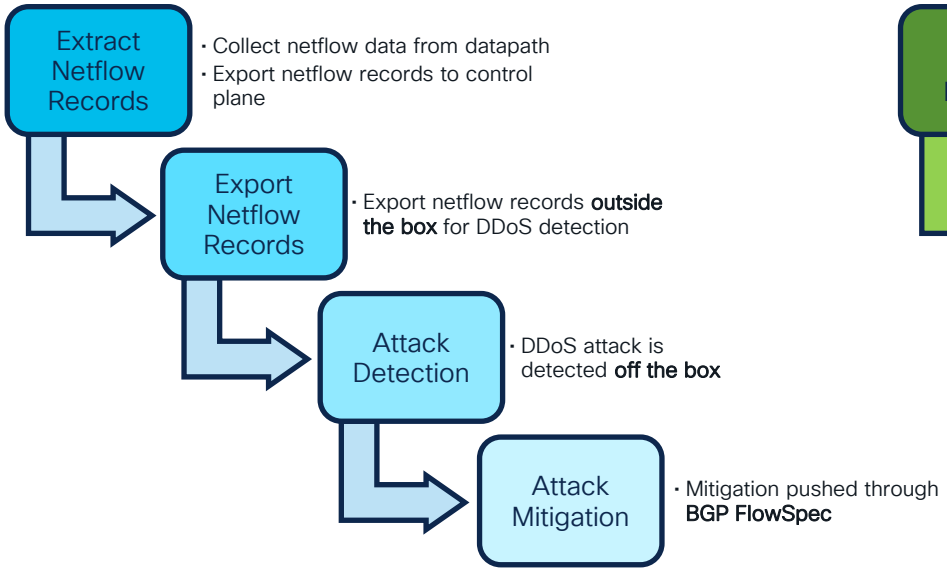


INSPECTION

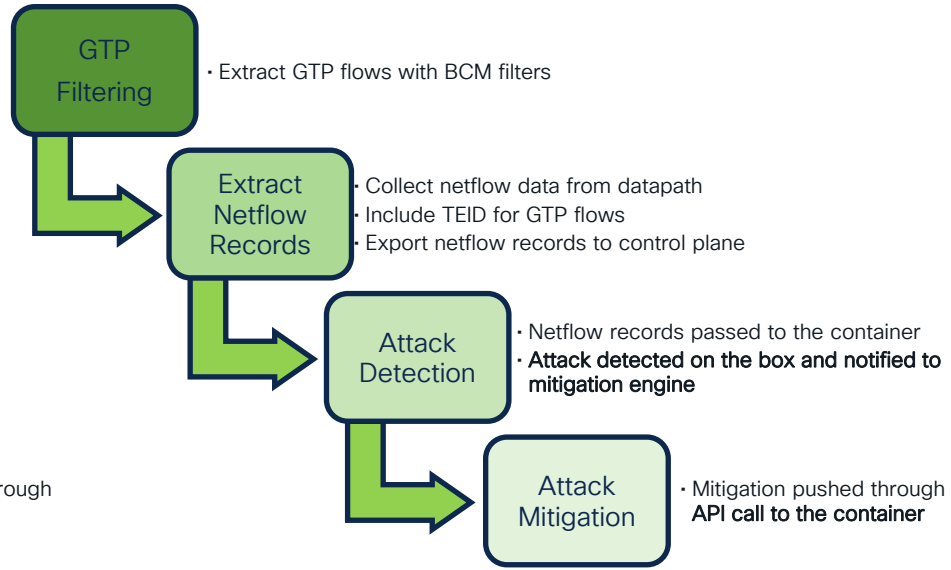
- **Localized** attack characterization.
- **Machine learning** Real Time Signature
- **Fully automated** attack life-cycle.
- **Advanced** protocol attributes can be added to protobuf template

DDoS Workflow Comparison

Existing Workflow



Improved Workflow with Edge Protection



Cisco Secure DDoS Edge Protection Demo

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

Real-time on-box autonomous attack detection and mitigation

To protect quality of experience and the performance of low-latency applications

Software that requires no additional equipment, rack space, power, or cooling

For cost-effectiveness and scalability

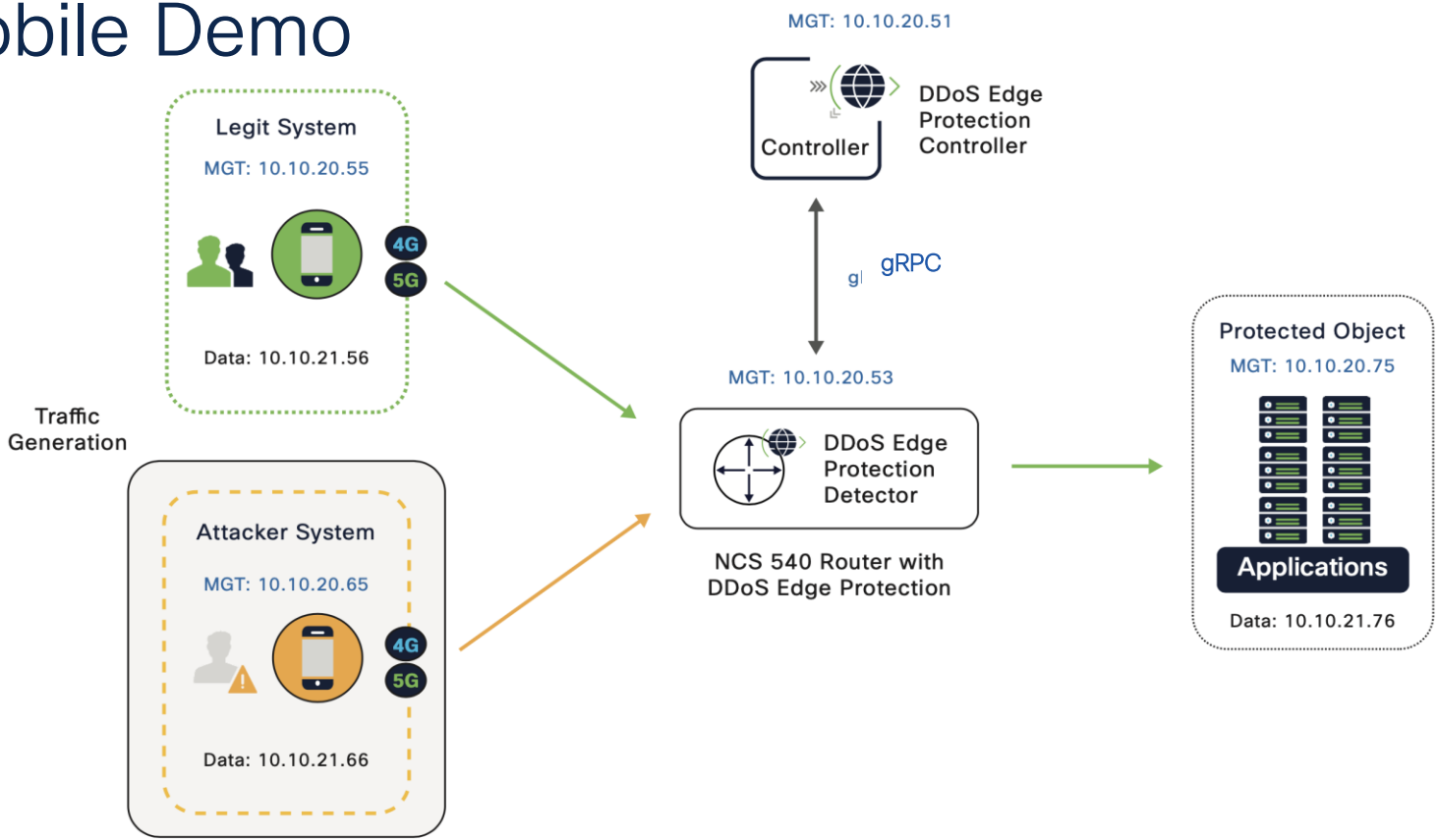
Unsupervised machine learning algorithms

To ensure the flow of legitimate traffic while preventing malicious traffic from flooding the network

Automation, zero touch, and a central interface management function

For ease of management and complete control

Mobile Demo



Dpro Controller

10.10.20.51.nip.io/detectors/61726460521ca65a2ffbca06/dashboard?quantilesChart=A&quantilesType=bps&timeFilter=5

cisco

Dashboard

Detectors

Attacks

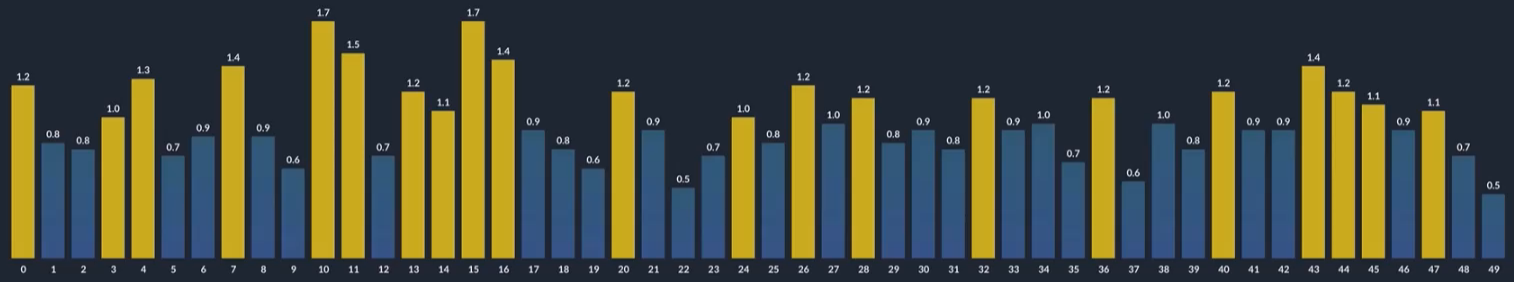
Protected Objects

No alerts to display

Quantiles Traffic Percentage BPS A

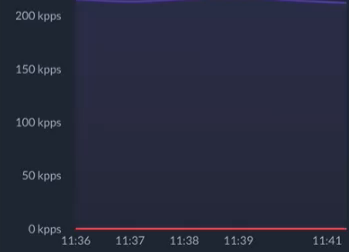
PPS

VIEW 50-99 >

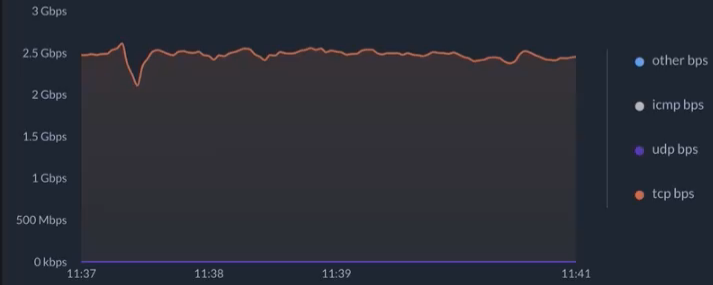


Total Traffic BPS

Total Traffic PPS



Traffic by Protocol

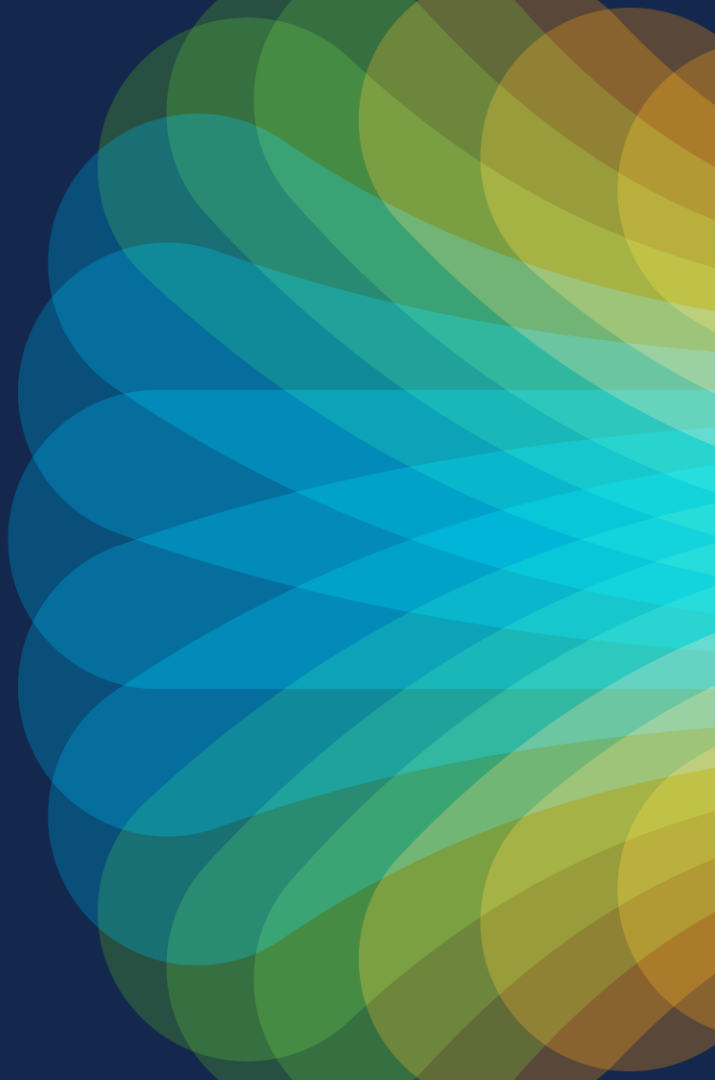


Logs

Export Log File

TIME	TYPE	DEBUG LEVEL	MODULE	MESSAGE

What To Do Next!



Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Learn More About The Solution

Cisco Secure DDoS Protection web page
https://www.cisco.com/go/secure-ddos

Cisco “What is a DDoS Attack?” web page,
https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

Cisco Secure DDoS Protection AAG
https://salesconnect.cisco.com/open.html?c=4a832942-96ff-4953-9953-65aa6970baa0

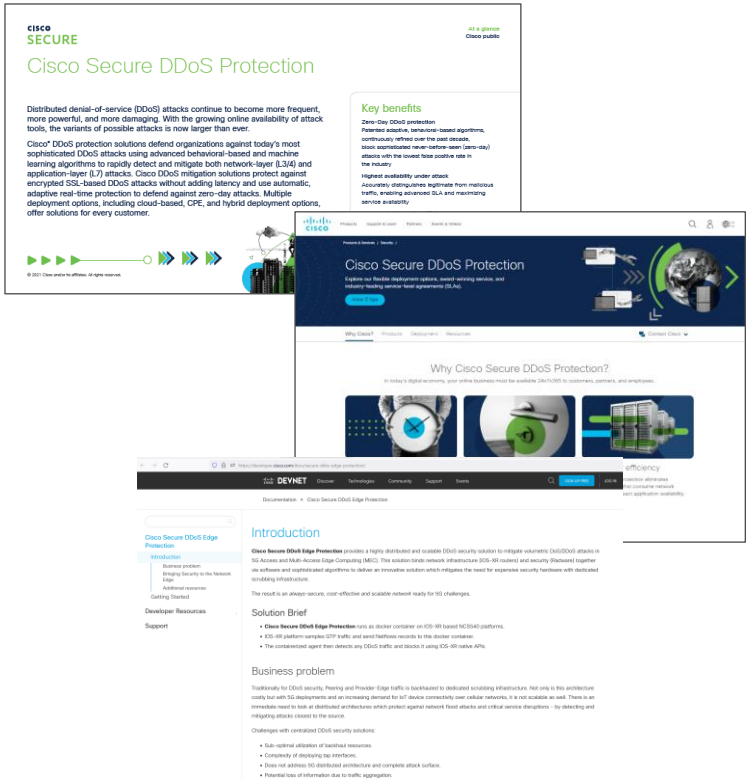
Download the Cisco Edge Protection AAG
https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-edge-protection-aag.pdf

NCS 540 security web page,
https://www.cisco.com/c/en/us/products/routers/network-convergence-system-540-series-routers/index.html

DDoS Edge Protection on DEVNET,
https://developer.cisco.com/docs/secure-ddos-edge-protection

To schedule a Demo or request a Proof of Value (POV)

Contact your Cisco sales representative or reach us at
secure-ddos-edge-protection@external.cisco.com



Want To Learn More About Security for SPs?

Holistic Security in 5G deployments - BRKSPM-2027

Munib Shah, Principal Architect, Cisco Systems, Inc.

As 5G provides service providers with more opportunities in sectors such as healthcare or manufacturing, it also considerably increases the extent of damage that can be caused by adversaries. Service provider networks are thus becoming an attractive target for cyber criminals to exploit. In this session attendees will be provided with a holistic view of security in large scale 5G deployments. The presenter will provide real-world examples of how operators are taking an embedded security approach to reduce risk and accelerate their time to market.

Want To Learn More About Security for SPs?

FULL CONFERENCE IT LEADERSHIP

Building & Maintaining Trust in Service Provider Networks - BRKSPG-2868

Rakesh Kandula, Technical Marketing Engineer, Cisco Systems, Inc.

FULL CONFERENCE IT LEADERSHIP

Let's Talk Security: A Service Provider's Perspective - IBOSPG-2000

Rakesh Kandula, Technical Marketing Engineer, Cisco Systems, Inc.

Joe Malcolm, DSE CSO, Cisco Systems, Inc.

Nitin Singla Singla, Engineering Product Manager, Cisco Systems, Inc.

Cisco Private 5G Learning Map

Start

June 4 | 2:00 pm
TECSPG-2432
New Adventures in Wireless: The Journey of WiFi6 and Private 5G Networks for the Enterprise

June 5, | 8:00 am
BRKSEC-2085
Architecting Enterprise Security in a Wi-Fi plus Private 5G World

June 5 | 8:30 am
BRKSPG-2042
Architecting Private 5G for resiliency, security, and enterprise network convergence

June 5 | 10:30 am
BRKSPM-1006
The 5G System as a Spectrum Management Solution

June 5 | 11:00 am
BRKENS-2950
Is your Enterprise Network Ready for P5G

June 5 | 11:30 am
PSOSPG-1002
Leading Your Digital Transformation with Cisco Private 5G Network Offer

June 6 | 3:00 pm
BRKEWN-2030
WiFi6 and Private 5G for the Enterprise – a 'Better Together' Journey

June 7 | 2:30 pm
PSOGEN-1033
Unlock business outcomes from connectivity with a Private 5G solution

June 7 | 4:00 pm
BRKSPG-3004
Monolithic or Polylithic packet cores? The case for specialized use-case-based mobile packet cores

June 8 | 09:30 am
BRKSPG-2044
5G Use Cases Flight Line of the Future and Smart Warehouse

June 8 | 01:00 pm
IBOSPG-2007
Getting Started with Private 5G

June 8 | 1:00 pm
BRKGEN-2001
Cisco P5G - A Robust and Secure Architecture

Finish

Cisco 5G Learning Map

Start

June 4 | 9:00 am
TECIOT-2584
Designing IoT Wireless Networks

June 5, | 8:30 am
BRKNWT-2203
Automation-first Approach to Network Infrastructure Modernization for 5G & Beyond

June 5 | 1:00 pm
BRKSPG-2063
Design, Deploy and Manage Transport Slicing using SDN Controller and Assurance

June 5 | 1:00 pm
BRKARC-2094
Hiking the Band Canyon with 5G: New Use Cases, New Business Outcomes

June 5 | 2:30 pm
BRKSPG-1002
Don't Just Connect, Grow your IoT Business with Cisco IoT Cellular Connectivity Management

June 5 | 3:00 pm
BRKIOT-1126
Connecting Moving Assets with Cisco IoT Solutions

June 6 | 10:30 am
BRKSPG-2315
Cloud-Ready Converged SDN Transport

June 6 | 1:00 pm
BRKSPG-2401
Cisco Secure Edge Protection – Protecting the 5G Edge against DDoS Attacks

June 6 | 2:30 pm
IBOSPM-2030
5G Transport Design Considerations Combining Onsite and Cloud-Based Deployments

June 6 | 4:00 pm
BRKSPM-2027
Holistic Security in 5G Deployments

June 7 | 10:30 am
BRKSPG-2133
Evolution of the Transport Network Architecture in the Context of 5G and Open RAN

June 8 | 8:30 am
BRKSPG-3050
Synchronizing 5G Mobile Networks

Cisco 5G Learning Map

June 8 | 9:30 am

IBOSPG-2006

DISH Wireless, World's first 5G Network with a Hybrid Cloud

June 8 | 10:30 am

BRKNWT-2301

DevNetOps Automation Approach to Network Infrastructure Modernization for 5G and Beyond

June 8, | 11:00 am

BRKSPG-2040

Troubleshooting 5G Architectures

June 8 | 1:00 pm

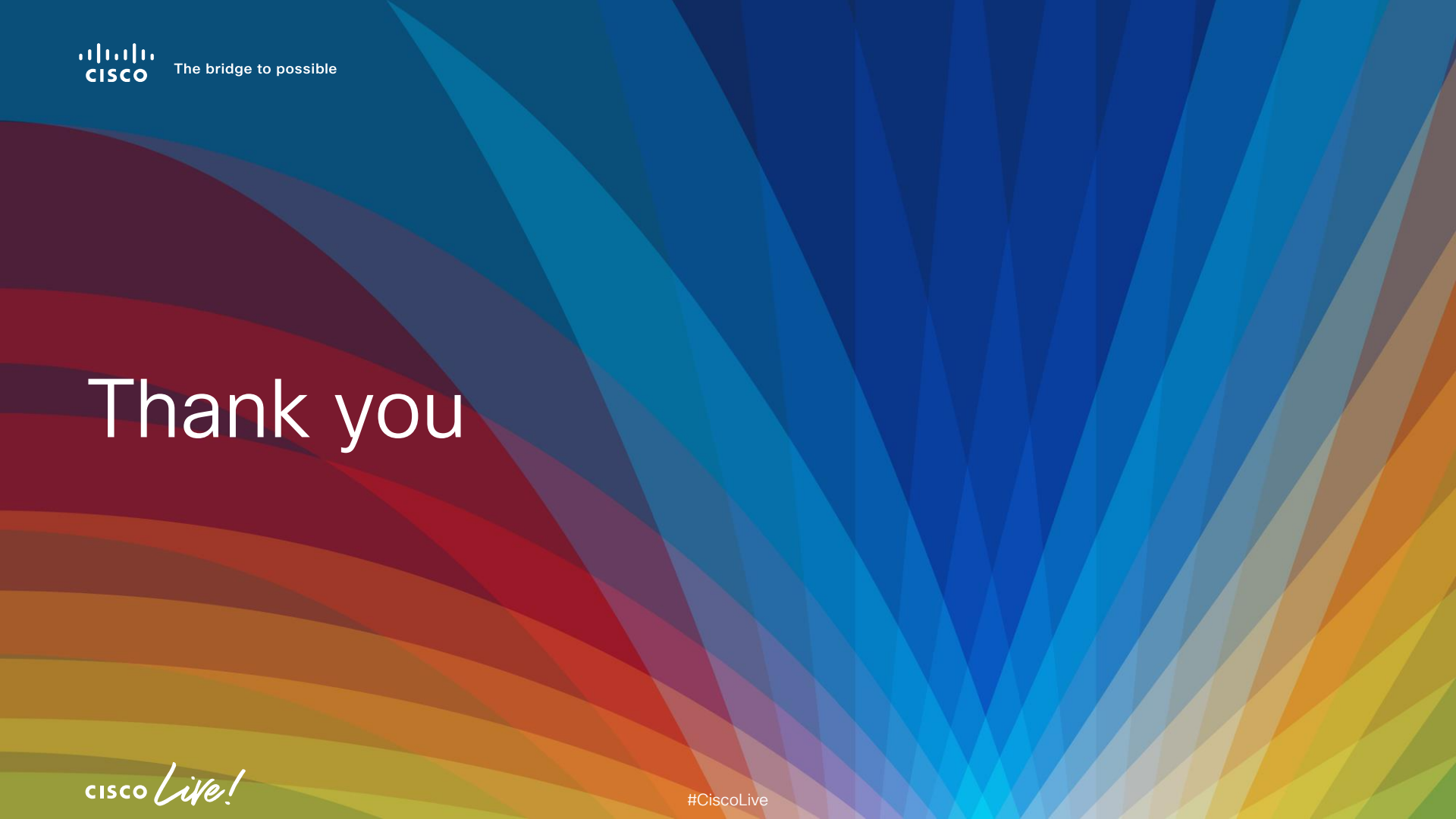
BRKMER-2001

Postcards from the 5G Edge: Meraki Cellular Gateways

Finish

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive


cisco Live!
Let's go
#CiscoLive

Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code: