#CiscoLiveAPJC

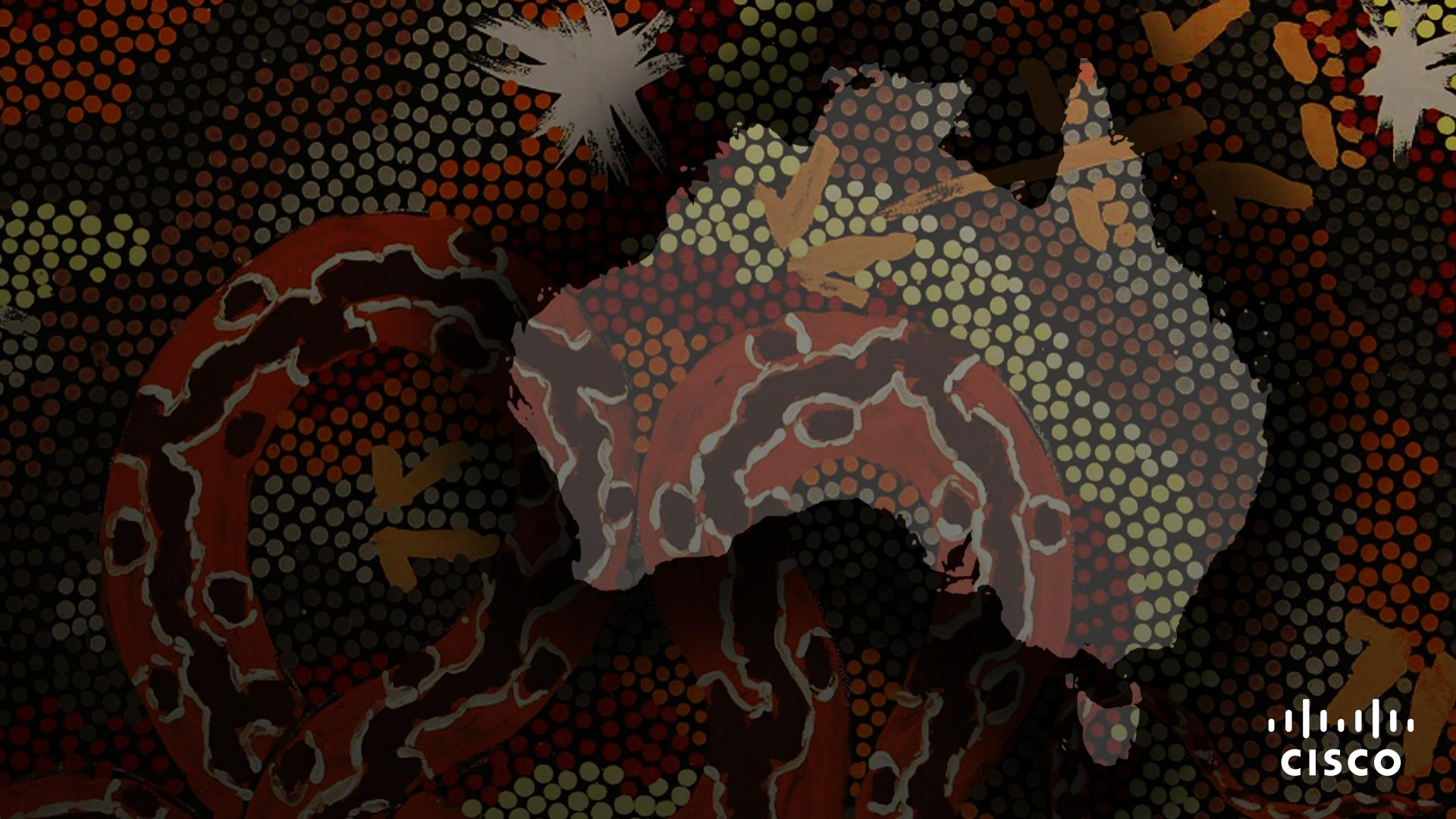
The bridge to possible

Cisco Secure Edge Protection

Protecting the (5G) Edge Against DDoS Attacks

Michael Geller – Distinguished Architect
@michaelge11er

BRKSPM-2363


CISCO

Cisco Webex App

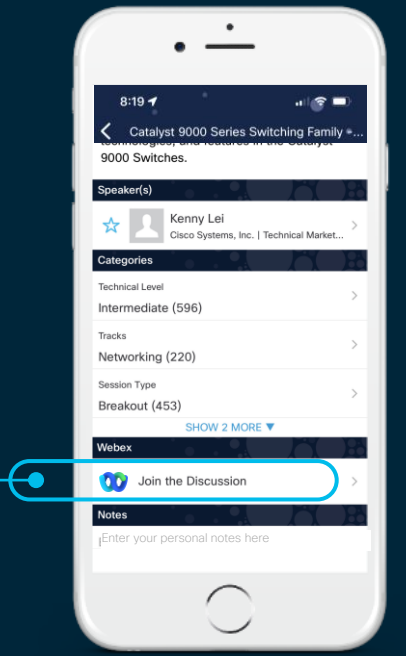
Questions?

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 Thursday 22 December, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSPM-2363

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- DDoS Attacks in 5G Networks
- Cisco Secure DDoS Edge Protection
- Cisco Secure Edge Protection Demo
- What To Do Next
- Conclusion

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

DDoS Attack Protection at the 5G Network Edge
Setting the Stage

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

5G Operator's Greatest Security Challenges

INFRASTRUCTURE CHALLENGES

- Compromised Users, Partners and Platforms
- Distributed Operations for 5G use-cases – UPP/CPP
- Public Cloud Shared Responsibility Model

SERVICE AVAILBILITY CHALLENGES

- Software Model
- Low Latency SLAs
- Local Breakouts
- Critical Interface and API Exposure

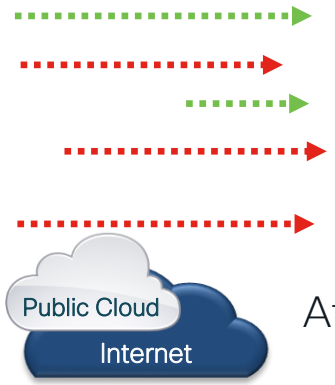
SECURITY OPS CHALLENGES

- Explosion of Security Events
- Visibility and Control
- Time-to-Action
- Cost at Scale

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Typical DDoS Attack Source & Targets

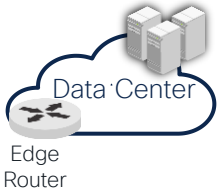
Typical Attack Source

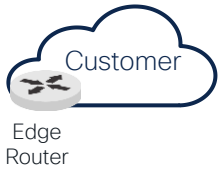


Inbound Attacks

Attacks originate from outside to inside

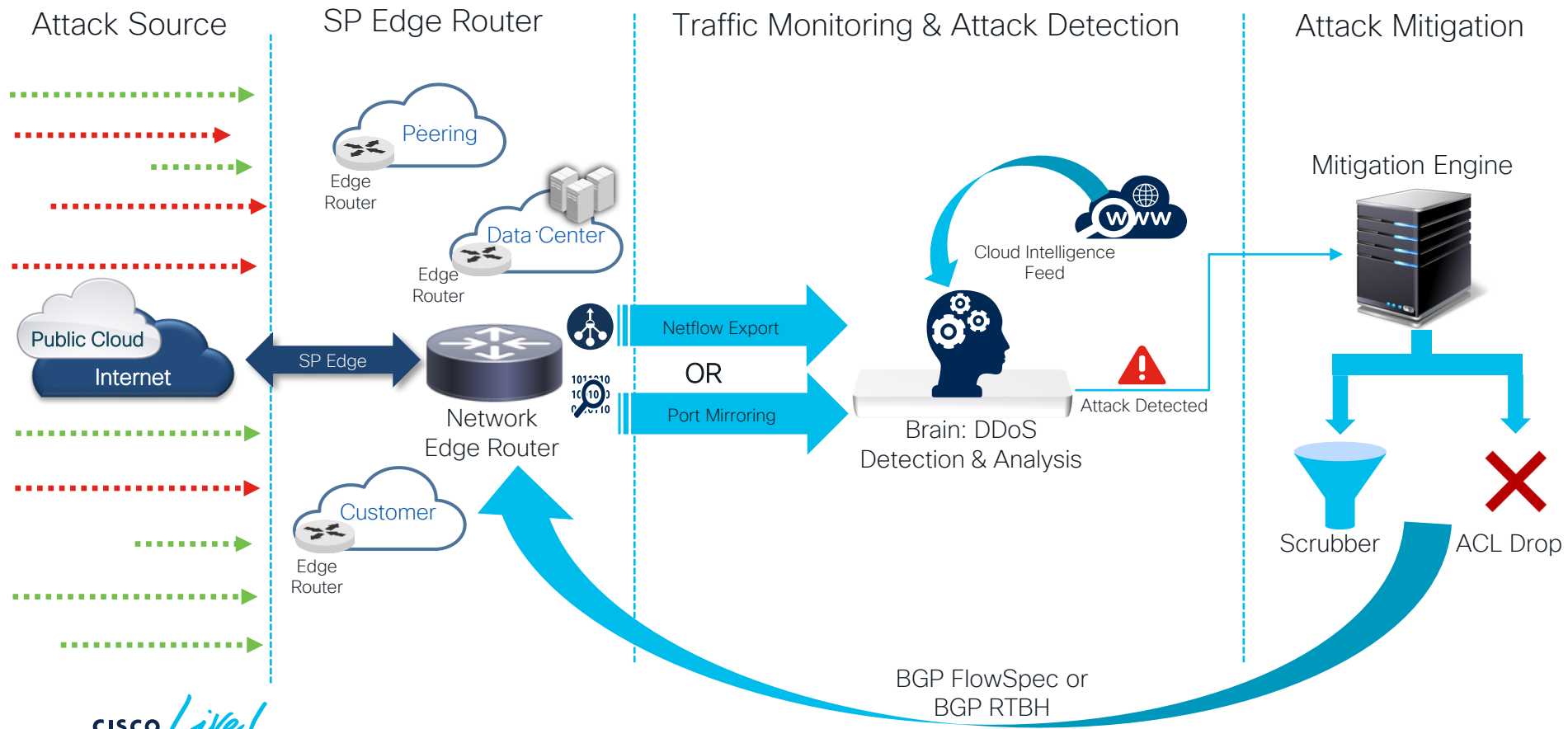
Typical Attack Targets





© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

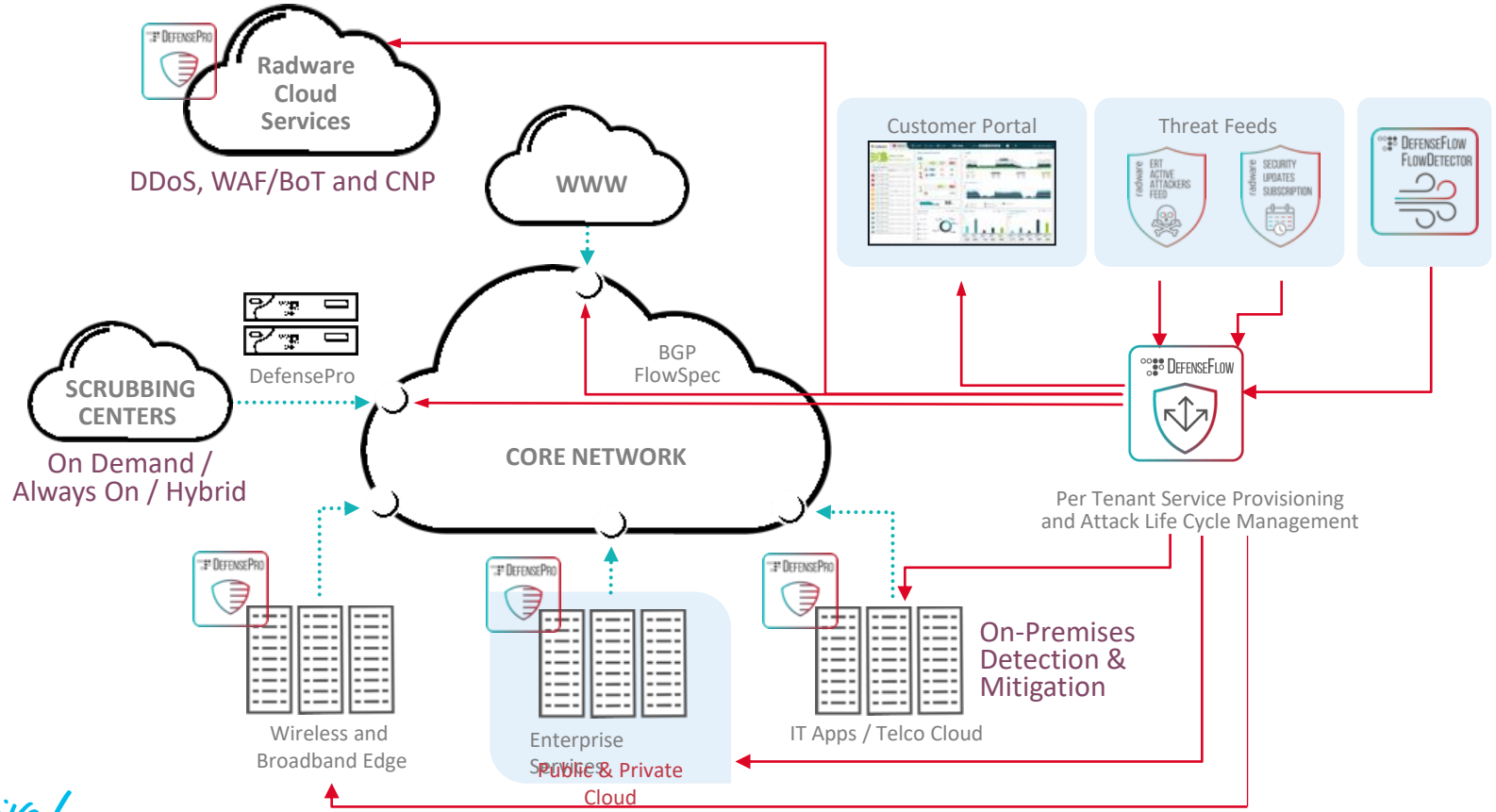
Typical DDoS Solution Deployment



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protecting The Network End to End

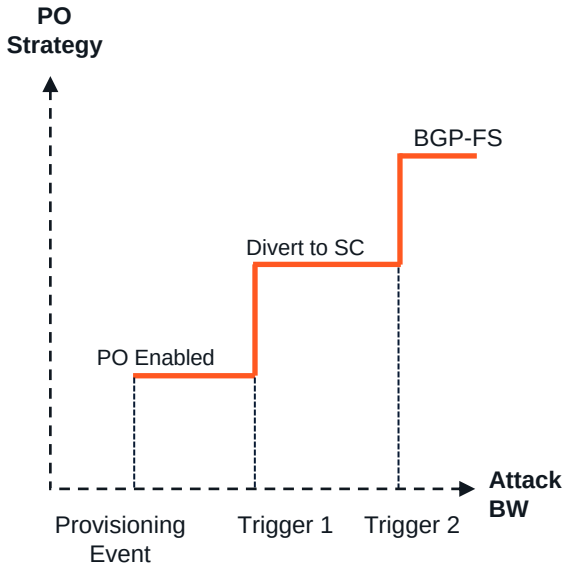
Current Recipe and Ingredients

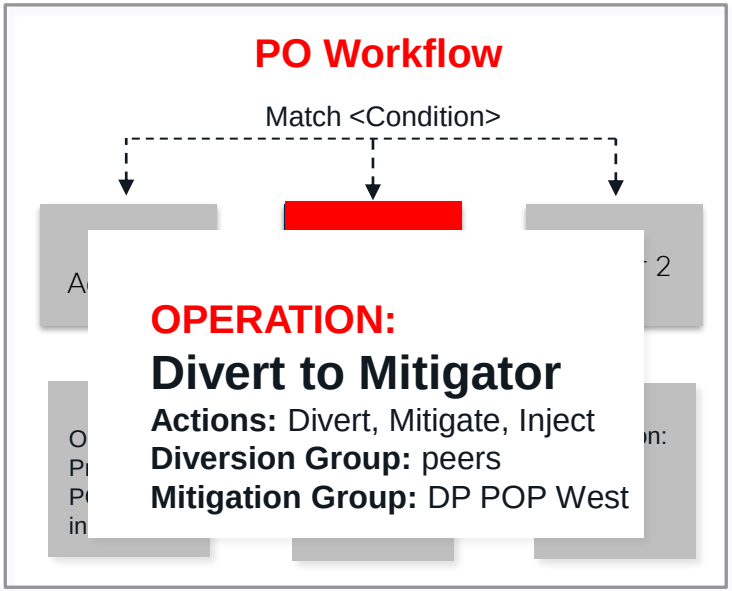


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protected Objects – SecOps

Automation Based on Workflows

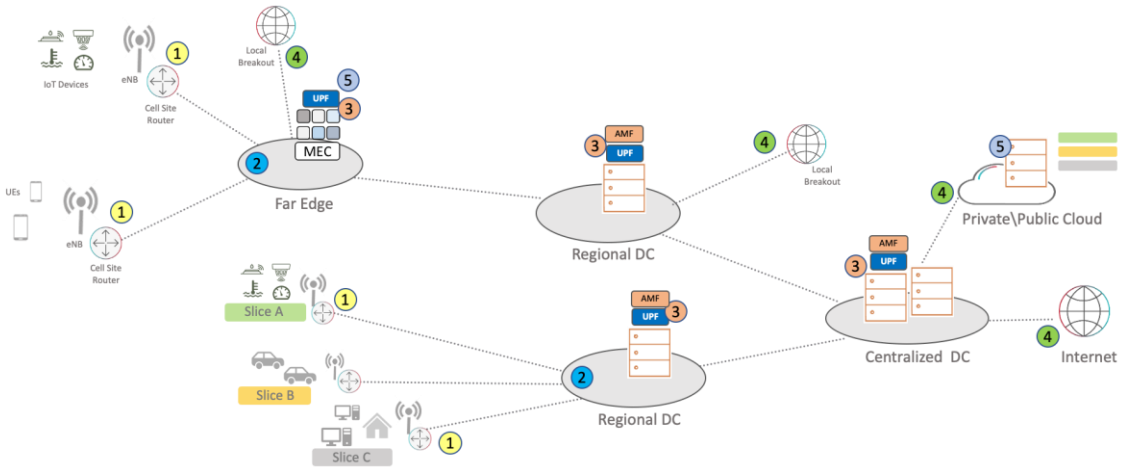




© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

5G Security Use Cases

Today, We Focus on Use Case 1



1. Use Case: UE/IOT Anomalies Detection. Risk: Attacks Originating from User Equipment (N3)
2. Use Case: MEC Infrastructure & 5GC Availability. Risk: Infrastructure & Services availability (N1/N2/N3)
3. Use Case: Network Peering Protection. Risk: Distributed Internet Access (N6/N9)
4. Use Case: 5GC Control Plane API Protection. Risk: APIs & Applications (SBI)
5. Use Case: Security as a Service for 3rd Party Apps & SASE

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where Else In The Network Does This Make Sense?

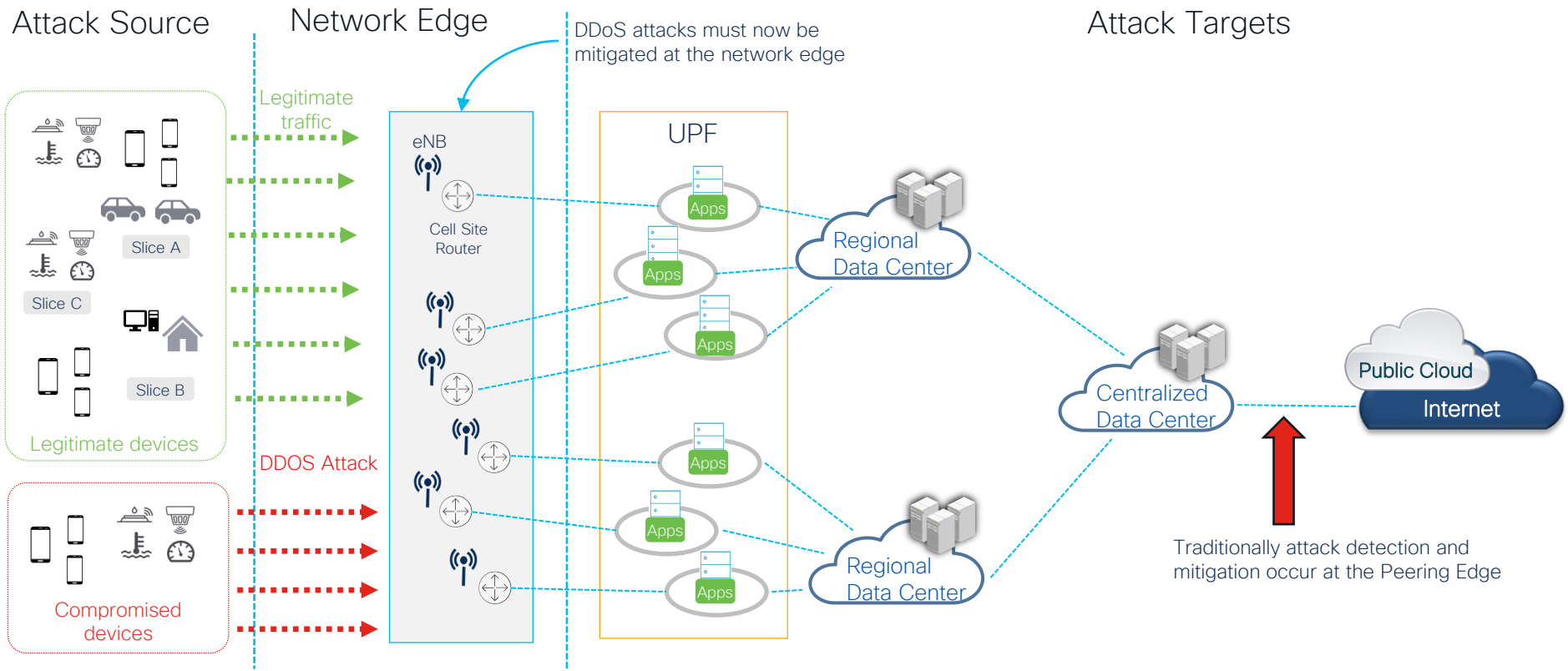
- Evolution of Peering – Avoid “tromboning of traffic” & reduction of network over build for DDoS mitigation services
- Broadband Aggregation Edge
- Protection of critical services at the MEC
- Private Enterprise or IoT based “edge” services (example – private 5G)

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

DDoS Attacks in 5G Networks

cisco Live!

Mobility/5G Use case

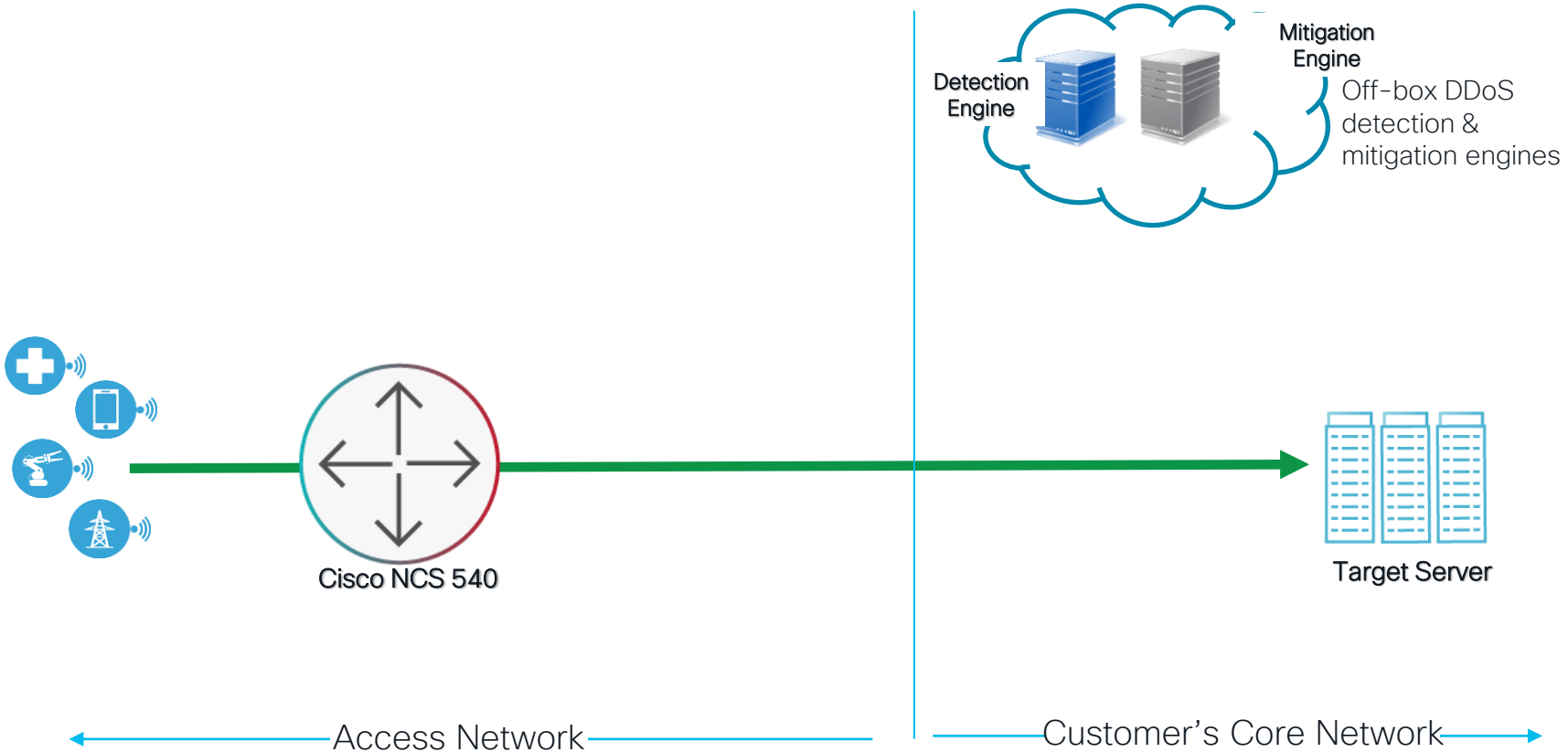


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure DDoS Edge Protection

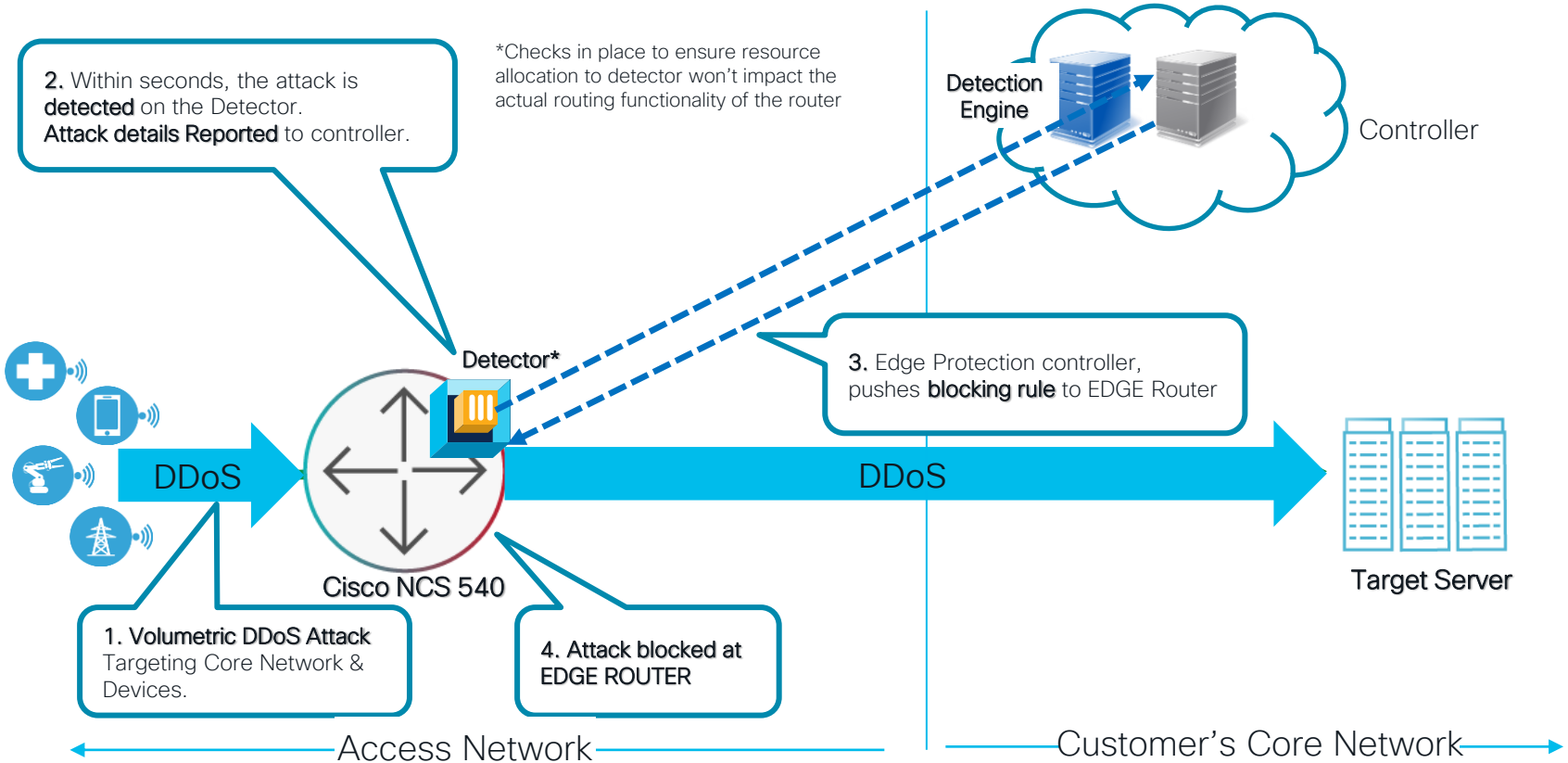
cisco Live!

Traditional DDoS Solution on NCS540



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

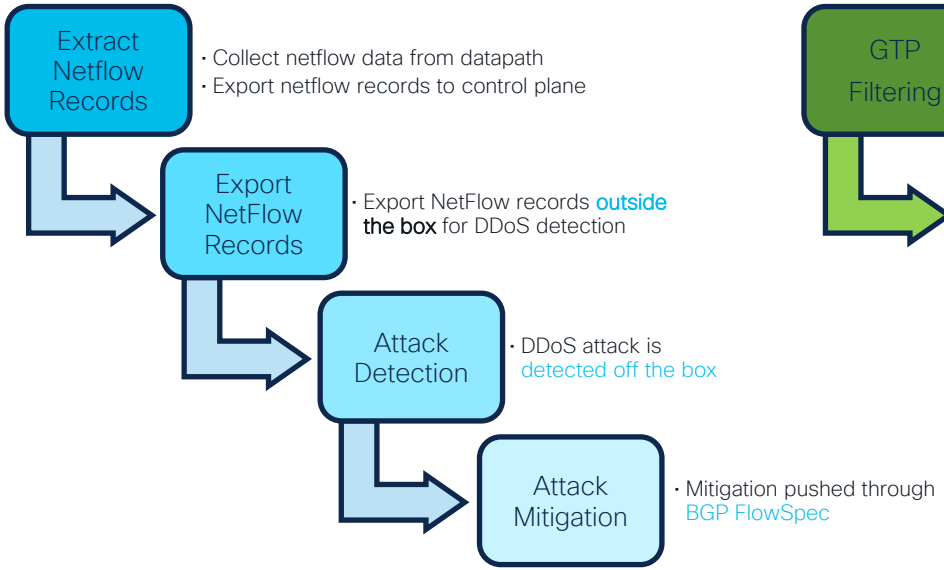
Edge Protection Solution on NCS540



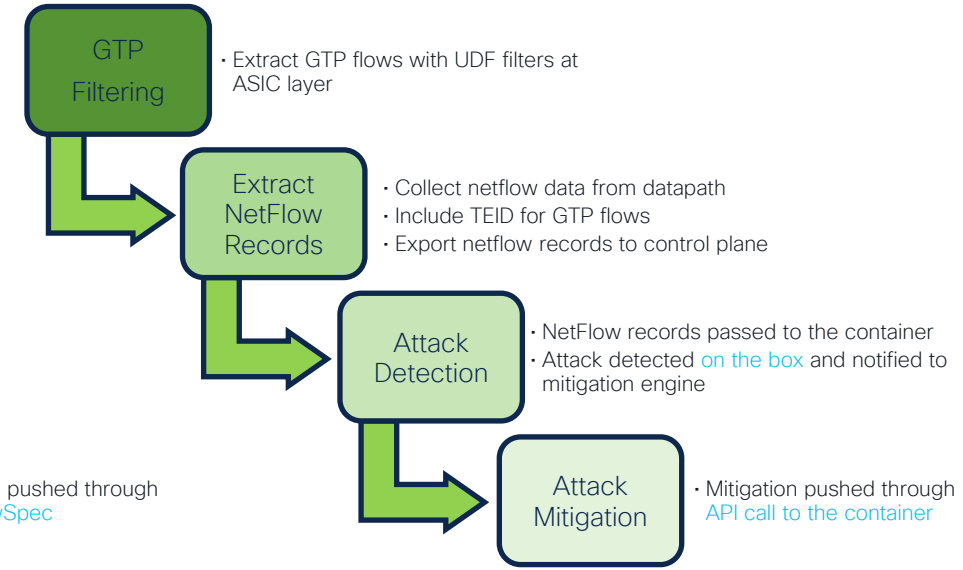
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

DDoS Workflow Comparison

Existing Workflow



Improved Workflow with Edge Protection

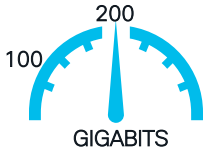


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

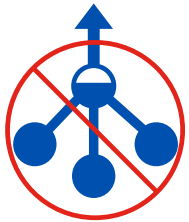
Highlights of Cisco Secure DDoS Edge Protection

Unique Solution for Mobility

Faster Detection



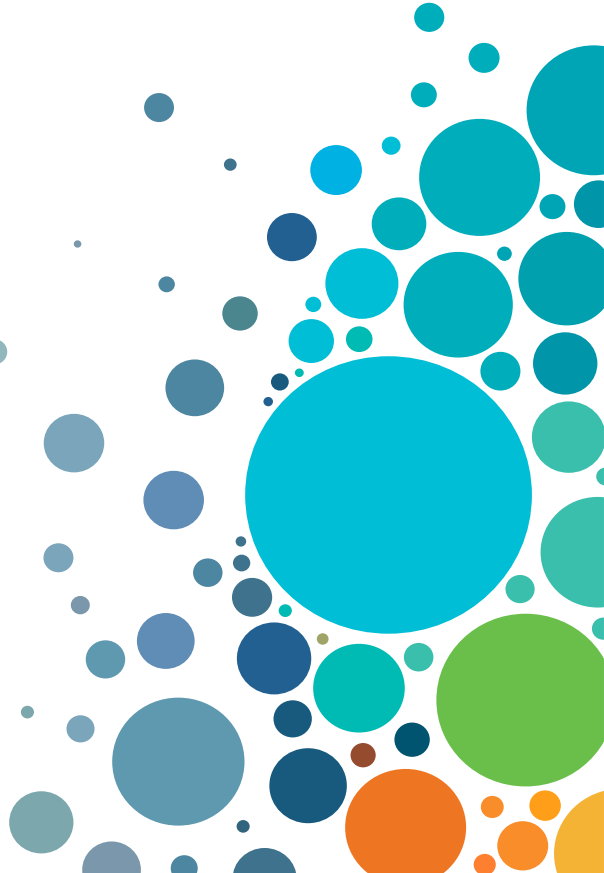
Higher Throughput Protection



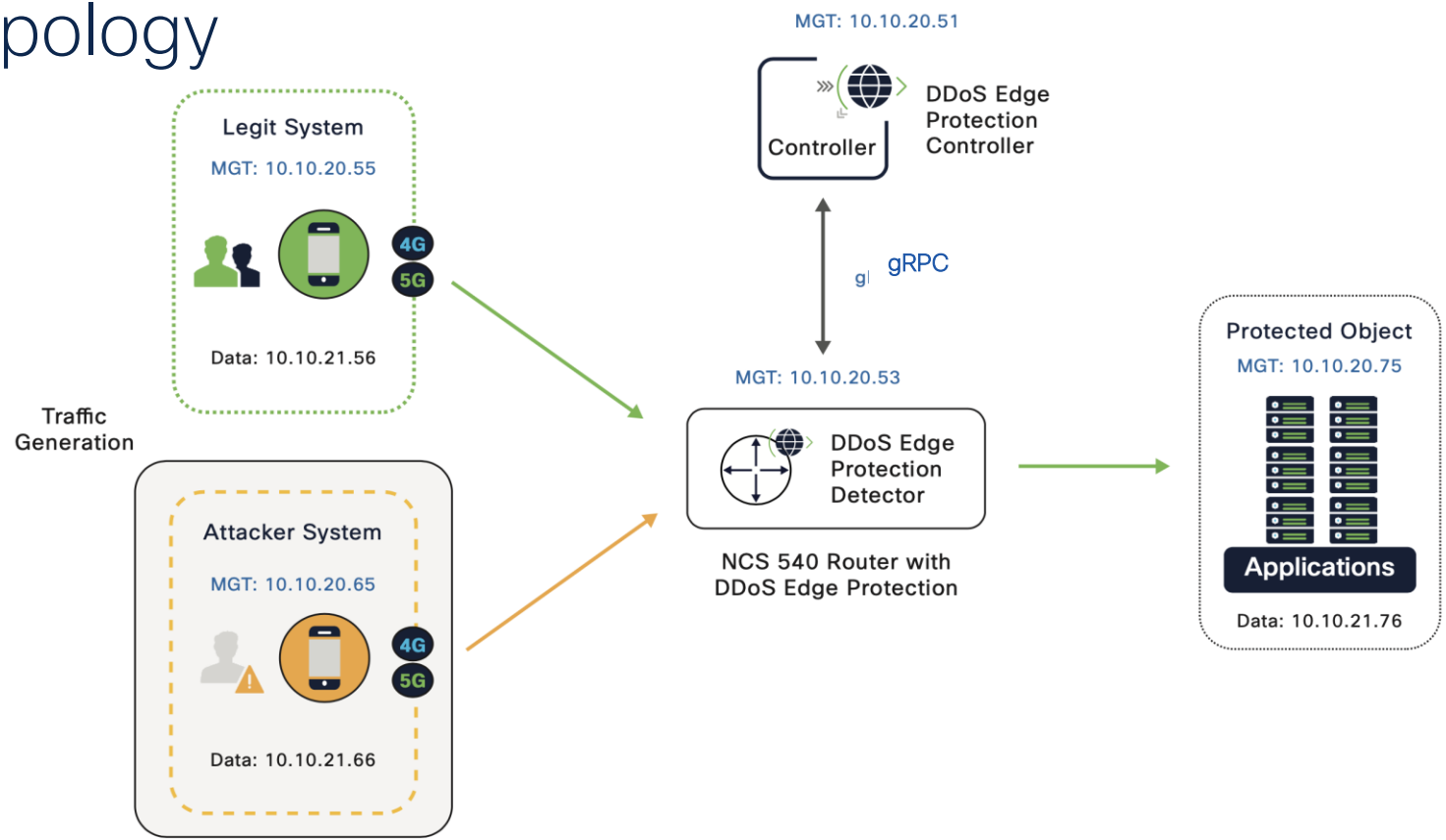
No NetFlow Export For DDoS

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Protection Demo



Topology



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Protection Demo

What To Do Next

Try It Out!! Edge Protection Demo on DevNet

To learn more, visit us on Cisco DEVNET

- Cisco Secure DDoS Edge Protection on Devnet: https://developer.cisco.com/docs/secure-ddos-edge-protection
- Need a development lab to learn what's possible? Visit the DevNet Sandbox and search for "DDoS Edge Protection" https://developer.cisco.com/site/sandbox/

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resources & Next Steps

Learn more

- Download the Cisco Edge Protection AAG (At-A-Glance) - https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-edge-protection-aag.pdf
- Download the Edge Protection White Paper - https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protction/secure-edge-protection-tech-wp.pdf
- Download the Edge Protection DevNet Demo Guide - https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protection/secure-protection-devnet-demo-guide.pdf
- NCS 540 Product web page - https://www.cisco.com/c/en/us/products/routers/network-convergence-system-540-series-routers/index.html

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

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Want To Learn More About 5G Security?

More on 5G Security:
Edge Protection @ World of Solutions
Rakesh Kandula & Nitin Singla

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Reference Architecture

CISCO SECURE

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt: Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- ISE TrustSec
- Cisco DNA Center
- Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Expert 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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

#CiscoLiveAPJC