5G Security: Why & How?

Oussama Naffati – SP Security Technical Solutions Architect
onaffati@cisco.com

BRKSEC-2763

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

About your speaker

Oussama NAFFATI
onaffati@cisco.com
EMEA SP Cybersecurity TSA
12 years in cybersecurity
Last 3 years with Cisco

- Based in Paris
- Father of a lovely 3 years daughter
- Other sessions here at Cisco Live: [LTRCLD-2230] Hands-On Security and Visibility in 5G Mobile Networks
- Passionate about: Bug Bounties, Ethical hacking, Security Architectures, Mobility..

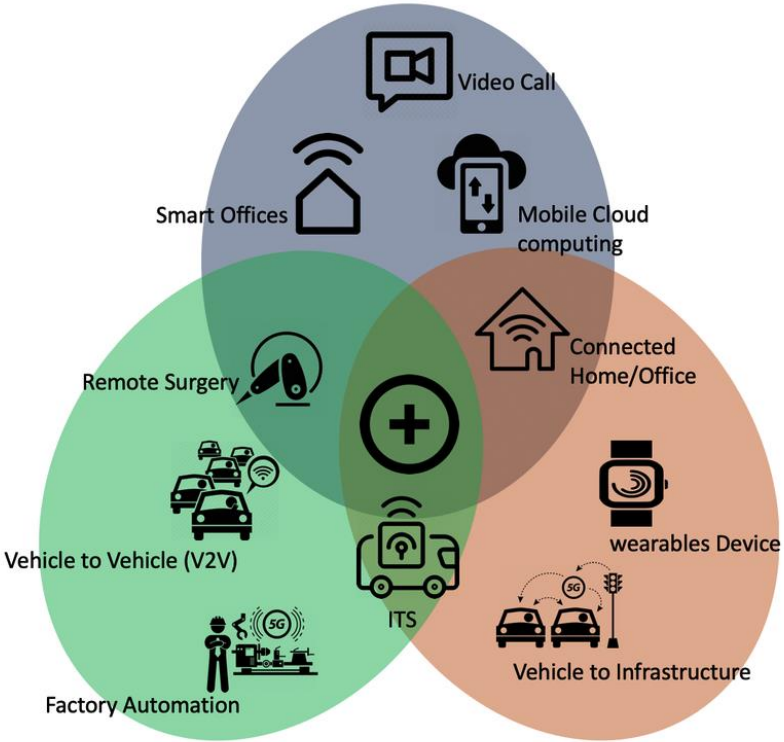
What should you expect … and not expect

- 5G security only (no residual, no fixed..)
- No specific focus on Private 5G
- No Mobile Architecture deep dive

- Real Life 5G security Challenges
- Concrete Use cases
- Holistic view of 5G security

5G Use Cases

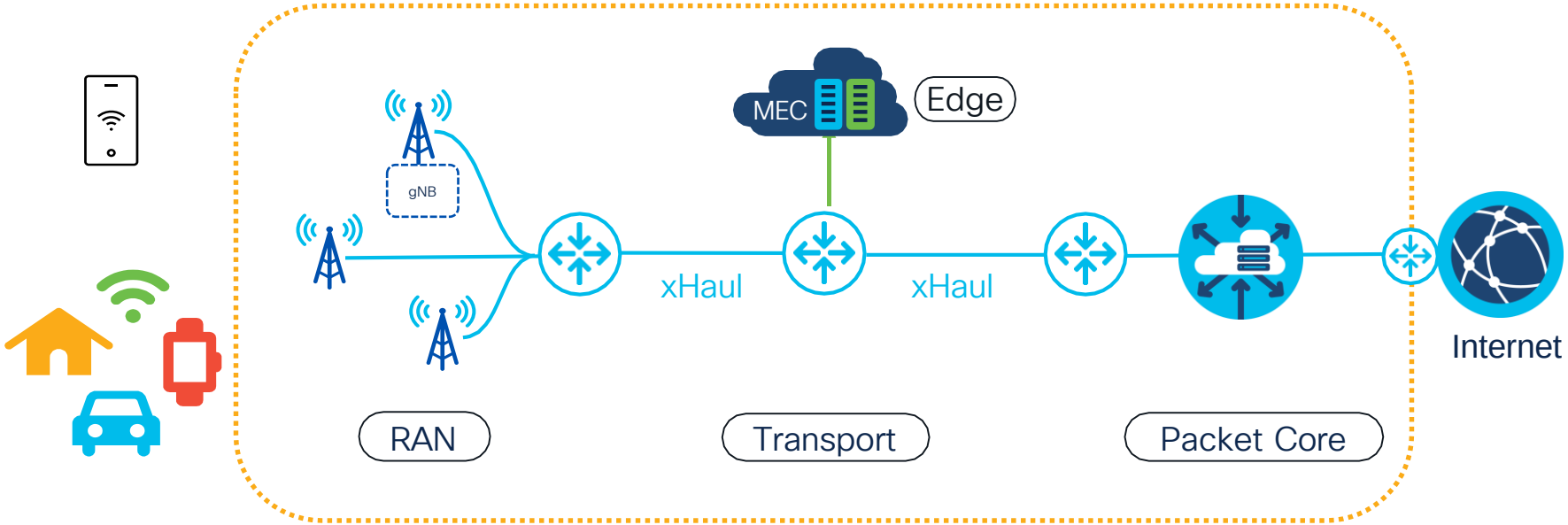
Enhanced Mobile Broadband



Ultra Reliable and low latency communications

Massive Machine types communications

Space View of 5G Deployment

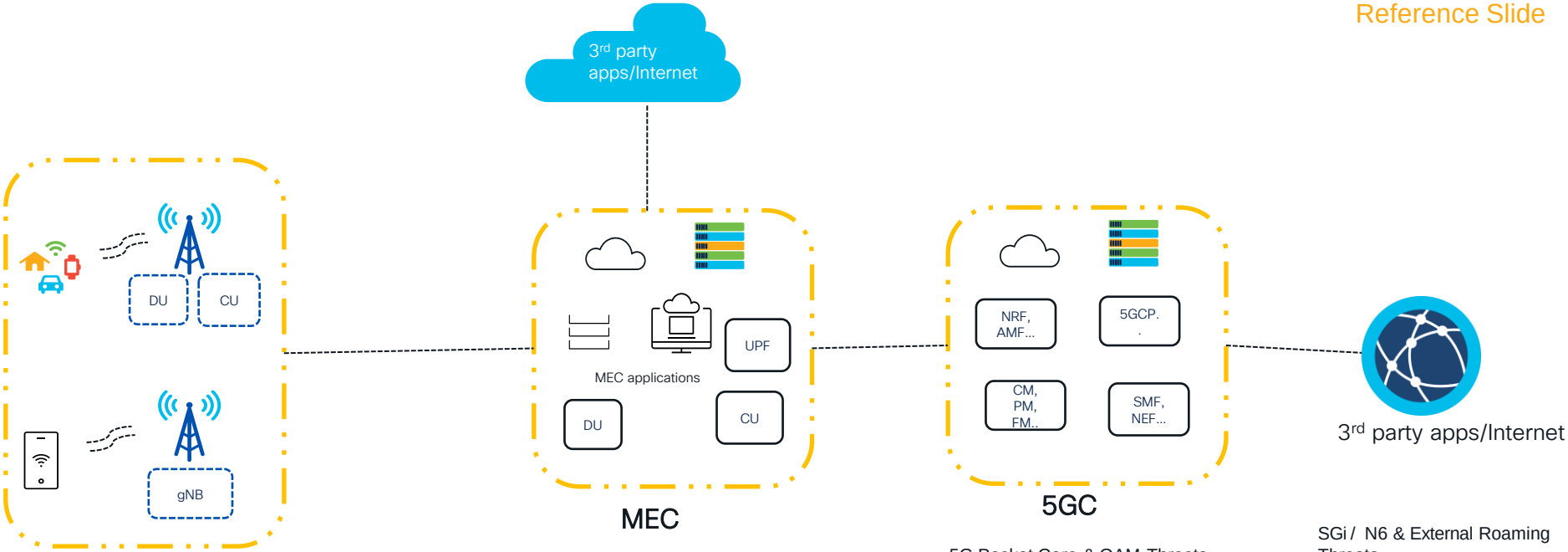


RAN: Radio Access Network

MEC: Multi-access Edge Compute

End to End threats in 5G

Reference Slide



Device Threats

Malware
Bots DDoS
Firmware Hacks
Device Tampering
Sensor susceptibility

Air Interface Threats

Man in the middle

Jamming

RAN Threats

Node Impersonation
Device Tampering
Forced reject during - UE Attach Request
Rogue gNB UE Attach
Forced Downgrade - using Rogue gNB

MEC & Backhaul Threats

DDoS attacks
Side Channel attacks
NFVi Vulnerabilities
Forced Attack on - Unsecured Backhaul
Eavesdropping due to - unsecured Backhaul

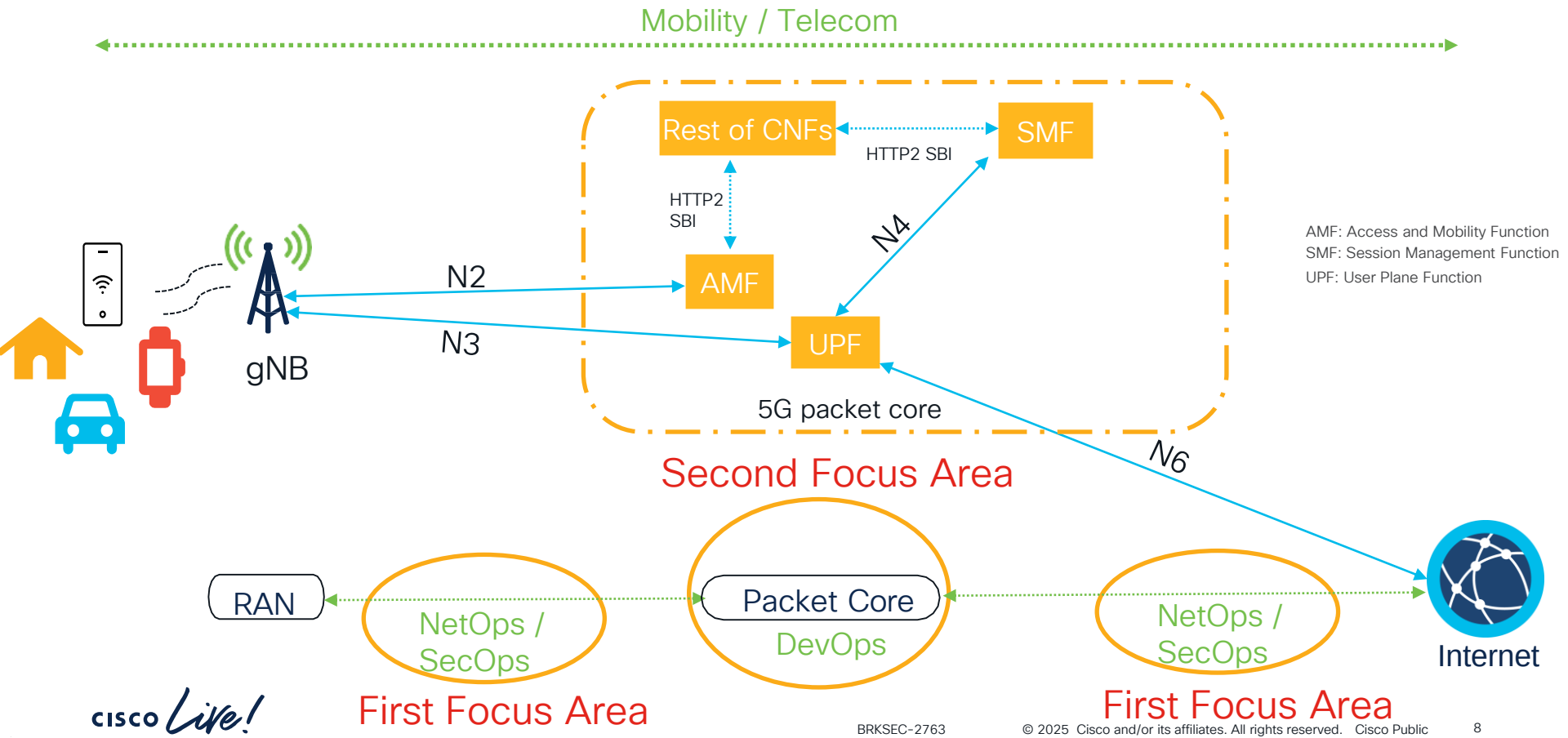
5G Packet Core & OAM Threats

Virtualisation
LI Vulnerabilities
Improper Access Control
Network Slice security
API vulnerabilities
NEF vulnerabilities
Roaming Partner

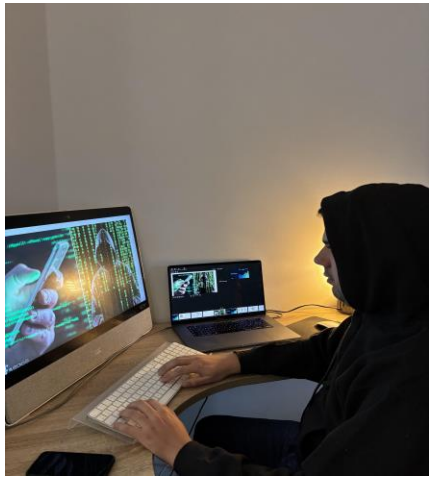
SGi / N6 & External Roaming Threats

Attack from external - MNO
Port and Protocol - Scanning Attacks
SGi Penetration attacks
App server vulnerabilities
Application vulnerabilities API vulnerabilities

5G Security: A Symphony of Teams

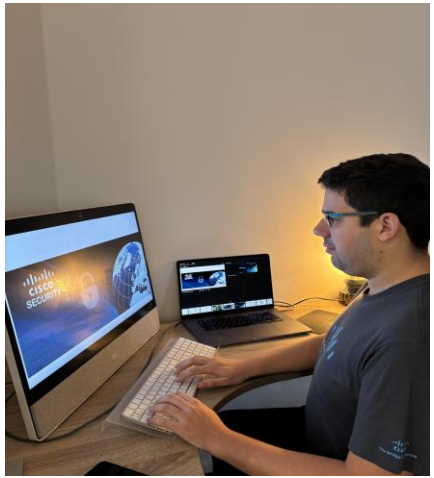


Battle between two very different personas…



5G_Hacker

- Explore and exploit hidden 5G vulnerabilities
- Fluent in hacking tools

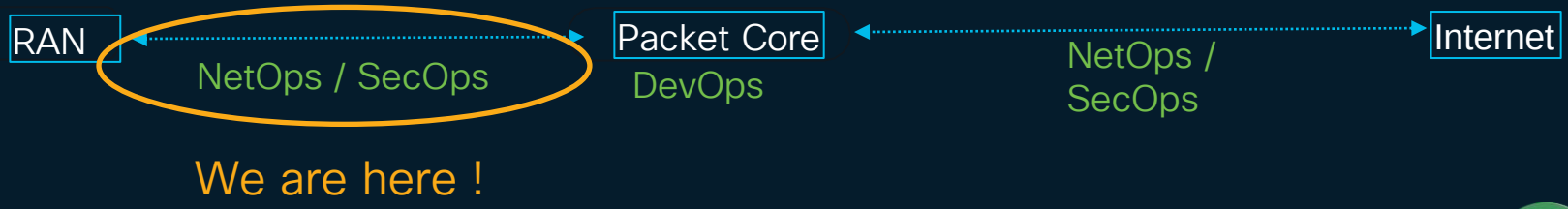


5G_Protector

- Fixes every vulnerability before attackers can strike
- Cisco Security black belt

Agenda

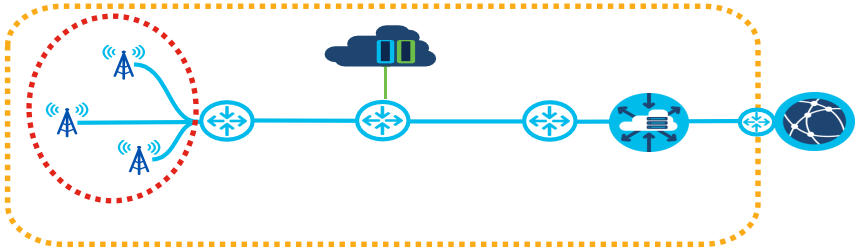
- Introduction
- Security Gateway use case
- N6 (Gi) FW use case
- 5G Packet Core protection use case
- Conclusion



SecGW Use Case

cisco Live!

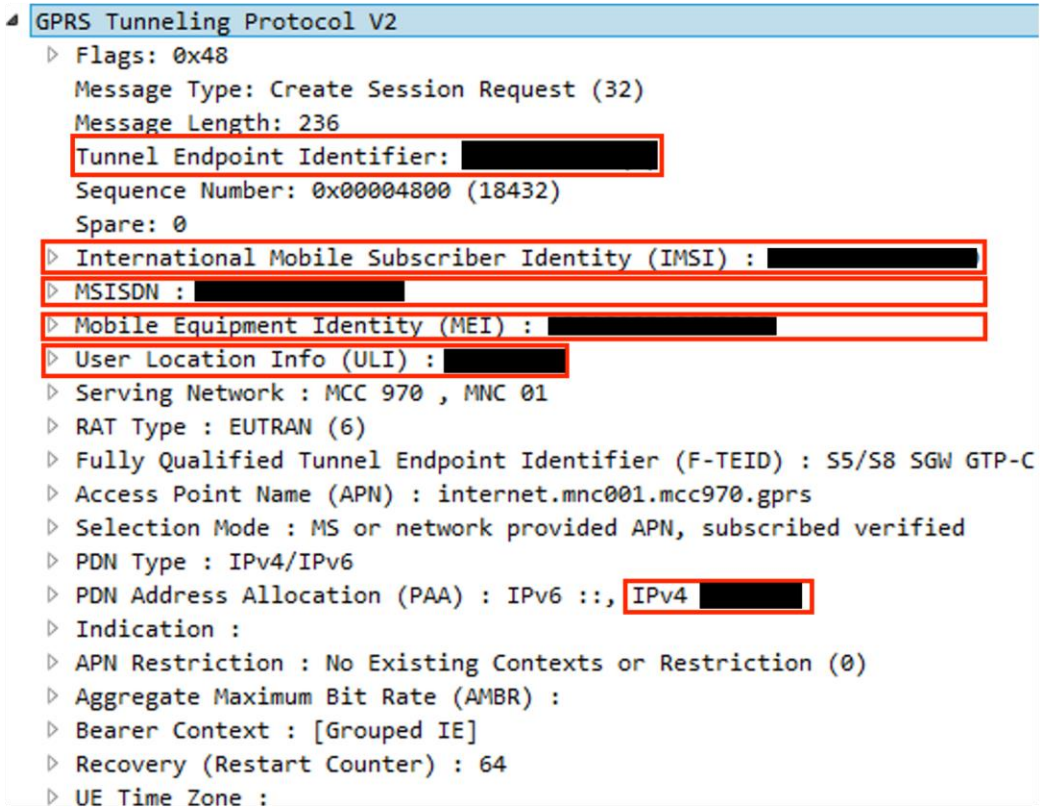
Cell sites



- More than 10000 for a medium sized city (~1 million population)
- In Theory: We should have some security : port security, Dynamic ARP inspection, secure DHCP..
- Reality is different: hard to configure at large scale, very few have this level of granularity

Which protocol are used between RAN and Core?

- GTP-U for User Plane and GTP-C for Control Plane traffic for users
- Other signaling protocols
- All clear text
- GTP is old (late 1990) and was never designed with security in mind
- GTP attack vectors are well known by the industry (GSMA FS.20)



5G_hacker Rogue gNodeB Attack

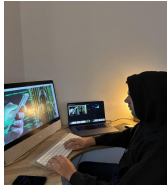
Cell site with weak security

Rogue gNodeB 192.168.1.100

```
from scapy.all import sniff

def packet_handler(packet):
    """
    Callback function to process each captured packet.
    Prints a summary of the packet.
    """
    print(packet.summary())

# Define the core address and capture filter
core_address = "192.168.1.200"
# Filter for UDP packets on port 2152 and one of the endpoints equals the core address.
capture_filter = f"udp port 2152 and host {core_address}"

print(f"[*] Starting to sniff GTP-U traffic with core address {core_address} (UDP
print("[*] Press CTRL+C to stop.")

try:
    sniff(filter=capture_filter, prn=packet_handler, store=False)
except KeyboardInterrupt:
    print("\n[*] Stopped sniffing.")
```

Sniff some legitimate traffic towards Packet Core: 192.168.1.200

5G_hacker Rogue gNodeB

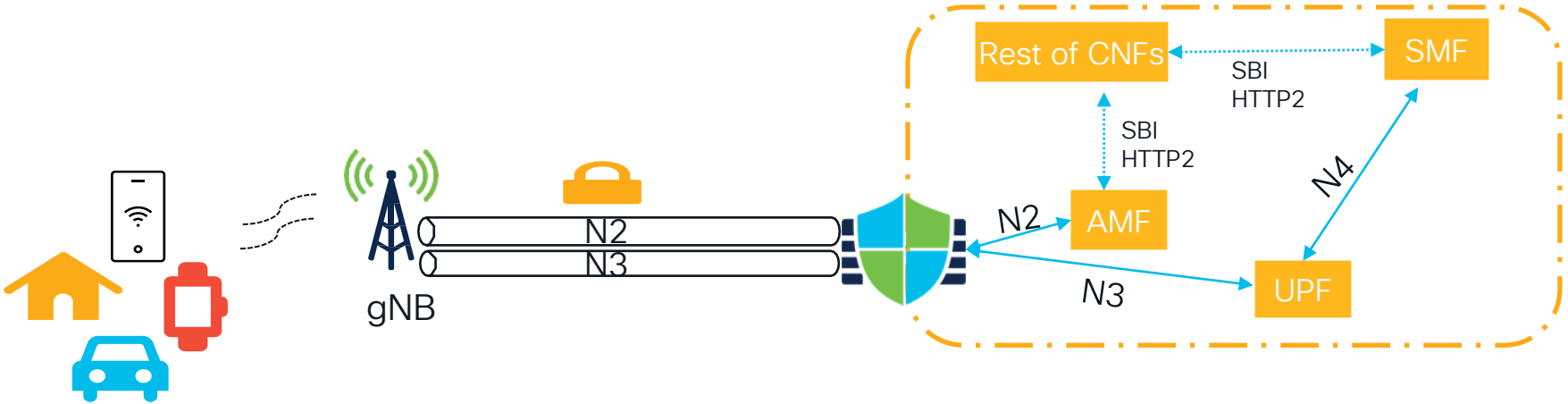


```python
from scapy.all import *
# Load the GTP module (requires Scapy 2.4.0+)
load_contrib("gtp")

# Define the source and destination IP addresses
src_ip = "192.168.1.100"   # Example UE gateway address
dst_ip = "192.168.1.200"   # Example Core Network address

# Build the IP layer
ip_layer = IP(src=src_ip, dst=dst_ip)

# Build the UDP layer (GTP-U typically uses port 2152)
udp_layer = UDP(sport=2152, dport=2152)

# Craft the GTP-U header.
# Here, flags are set to 0x30 to indicate a G-PDU in GTPv1-U without optional fields.
# TEID is set to a sample value (0x12345678) that should be replaced by a legitimate one.
gtp_layer = GTP_U_Header(teid=0x12345678, flags=0x30, msgtype=255)
# Note: In GTPv1-U, the G-PDU message type is typically 255. Verify against your specific
implementation.

# Create a payload to simulate legitimate user data
payload = Raw(load="Legitimate GTP-U user payload.")

# Stack all layers together: IP / UDP / GTP-U / Payload
packet = ip_layer / udp_layer / gtp_layer / payload

# Display the crafted packet details
packet.show()

# Optionally, send the packet on the network.
# Depending on your setup and permissions, you may need to run this with elevated privileges.
send(packet)
```

```python
# 3GPP TS 29.274 v12.12.0 section 8.22
INTERFACE_TYPES = {
    0: "S1-U eNodeB GTP-U interface",
    1: "S1-U SGW GTP-U interface",
    2: "S12 RNC GTP-U interface",
    3: "S12 SGW GTP-U interface",
    4: "S5/S8 SGW GTP-U interface",
    5: "S5/S8 PGW GTP-U interface",
    6: "S5/S8 SGW GTP-C interface",
    7: "S5/S8 PGW GTP-C interface",
    8: "S5/S8 SGW PMIPv6 interface",
    9: "S5/S8 PGW PMIPv6 interface",
    10: "S11 MME GTP-C interface",
    11: "S11/S4 SGW GTP-C interface",
    12: "S10 MME GTP-C interface",
    13: "S3 MME GTP-C interface",
    14: "S3 SGSN GTP-C interface",
    15: "S4 SGSN GTP-U interface",
    16: "S4 SGW GTP-U interface",
    17: "S4 SGSN GTP-C interface",
    18: "S16 SGSN GTP-C interface",
    19: "eNodeB GTP-U interface for DL data forwarding",
    20: "eNodeB GTP-U interface for UL data forwarding",
    21: "RNC GTP-U interface for data forwarding",
    22: "SGSN GTP-U interface for data forwarding",
    23: "SGW GTP-U interface for DL data forwarding",
    24: "Sm MBMS GW GTP-C interface",
    25: "Sn MBMS GW GTP-C interface",
    26: "Sm MME GTP-C interface",
    27: "Sn SGSN GTP-C interface",
    28: "SGW GTP-U interface for UL data forwarding",
    29: "Sn SGSN GTP-U interface",
    30: "S2b ePDG GTP-C interface",
    31: "S2b-U ePDG GTP-U interface",
    32: "S2b PGW GTP-C interface",
    33: "S2b-U PGW GTP-U interface",
    34: "S2a TWAN GTP-U interface",
    35: "S2a TWAN GTP-C interface",
    36: "S2a PGW GTP-C interface",
    37: "S2a PGW GTP-U interface",
}
```

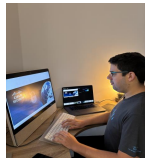
- Big number of 3GPP interfaces can be easily exploited
- Replay Attacks, Impersonation, Fraud..

3GPP highly recommended Security Gateway !



- Protects both user and control plane traffic from eavesdropping through encryption
- Confirms gNodeB identities: Preshared Keys or certificate based authentication
- Encrypts Control plane or user plane or both
- Protects against impersonation

5G_Protector SecGW use cases



Enhanced Mobile Broadband (eMBB)

Streaming 4K Video

- 5G_Protector Key challenges:

Latency: Moderate
Supports streaming

Availability: Very High
Enable media

Throughput: Extremely high
Handle gigabit-level data rates

Ultra-Reliable Low-Latency Communications (URLLC)

Example: Self-Driving Cars

- 5G_Protector Key challenges:

Latency: Ultra-low
<1 ms for near-instantaneous control

Availability: Extremely high
Guarantee mission-critical operations without interruptions

Throughput: Low
focused on reliable, small, and critical data packets

Massive Machine Type Communications (mMTC)

Tool: Smart Home Devices

- 5G_Protector Key challenges:

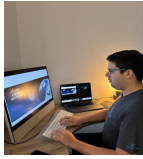
Latency: Moderate
sufficient for sensor data

Availability: Very high
support thousands of devices reliably across the network

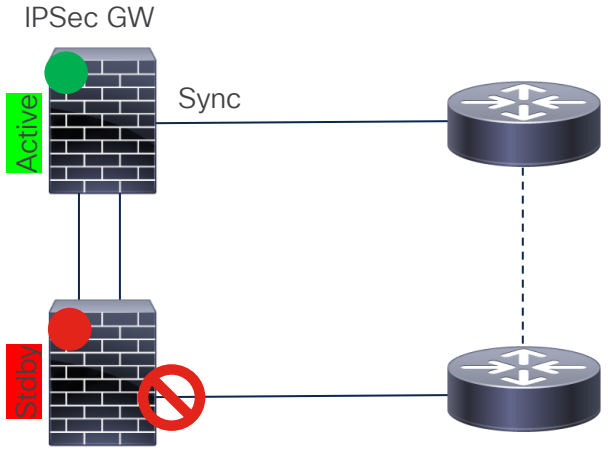
Throughput: moderate
each device sends minimal data, but there are many devices overall

Smart Home Devices Use case: Centrally deployed

Moderate Latency Very high availability Moderate throughput

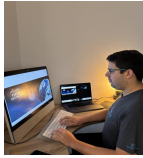


- An IPSec GW Pair in Active/Backup mode
- Backup node does not accept any traffic
- Active and Standby nodes are in same L2 broadcast domain
- FTD supports static VTI, Dynamic VTI and crypto Maps
- To detect a failure and re-route traffic, L3 protocols like BFD and BGP are required
- No session synchronisation (statefullness) between sites (intersite)
- FTD 7.3+: Use Performance profile called VPN heavy with prefilter fastpath, this allocates 90% of cores to data plane and 10% to snort

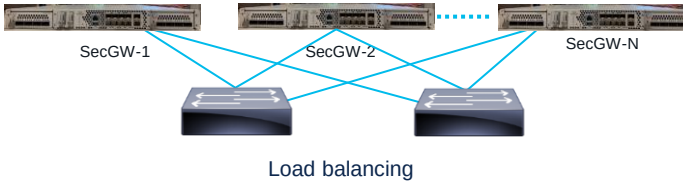


Streaming 4K videos use case: Deployed centrally

Moderate Latency Very high Availability Extremely high throughput

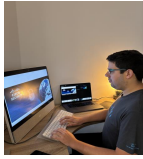


- Distributed VPN clustering in FTD7.7 for 4200 platforms
- Support up to 16 nodes for 4200. Around 30% Penalty for overall IPSEC performance
- All SecGW clustered appliances being active, achieving N+1 resiliency
- gNB's target one single SecGW cluster IP address
- Stateful solution: all IPSec sessions state is replicated from the session owner to other backup units via Clustering

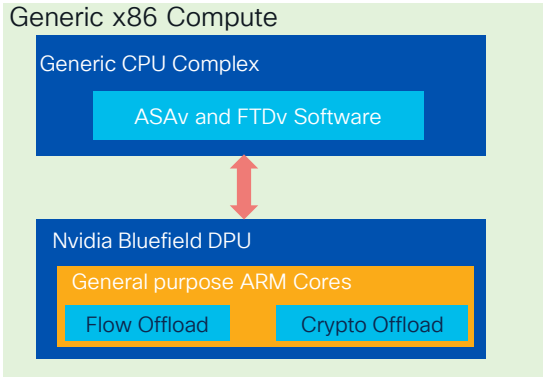


Self-Driving cars use case: Edge Deployed

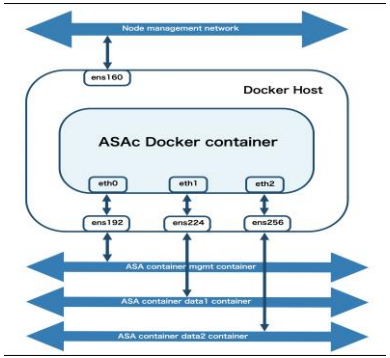
Ultra low Latency Extremely high availability Low throughput



- Support of SR-IOV, DPDK, VPP for performance enhancement
- Individual mode clustering
- Need for external load balancer
- Distributed VPN is not supported

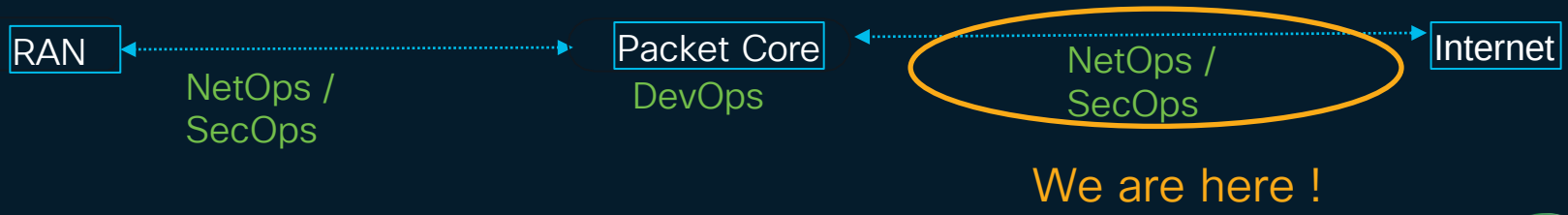


- If NVIDIA DPU is present, Additional ARM software components program offer inline acceleration for IPSEC encryption & flow offload
- Targetting 30 to 50% for IPSEC and 80 to 100% for flow offload performance improvement



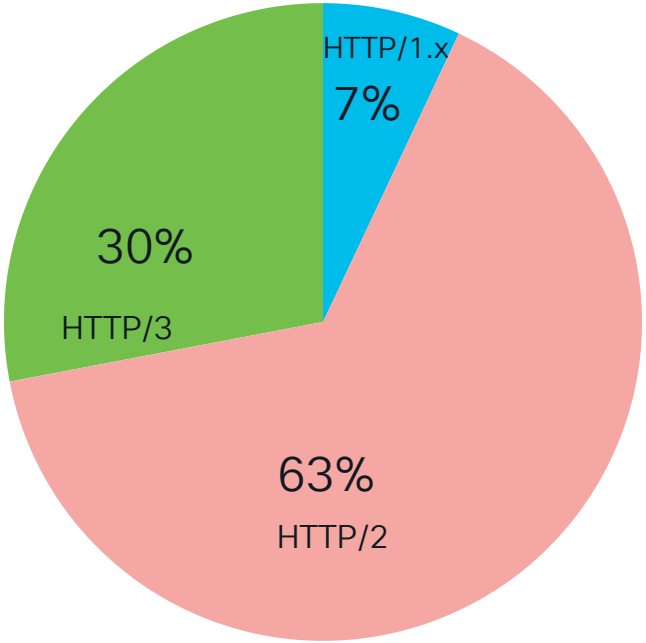
- Standalone Container solution With Infrastructure-as-Code (IaC) on K8S and Docker environment
- HA and Clustering are not supported in this release

cisco Live!



N6 (Gi) FW Use Case

2025 : Internet is fully encrypted

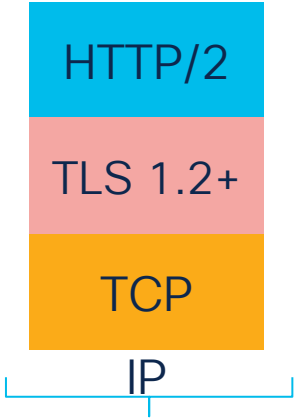


Source : Cloudflare Radar (November 2024) : [Cloudflare Radar]

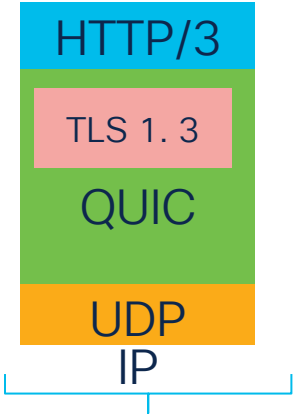
HTTP Evolution

Reference Slide

Your web traffic can be encrypted



Your traffic divided into multiple-streams in same session, encrypted



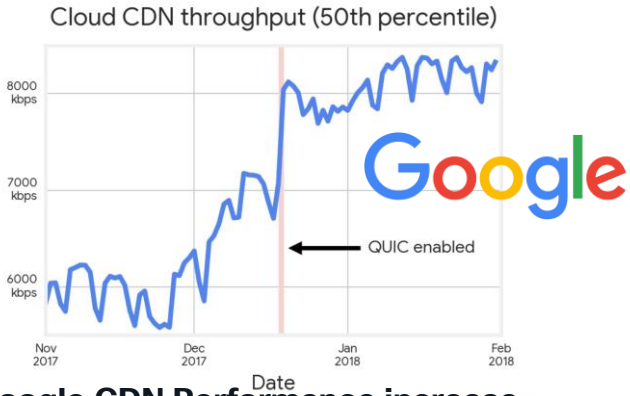
Your web traffic divided into multiple-streams & encrypted

The consumers are observing benefits : BRKSPG-2583

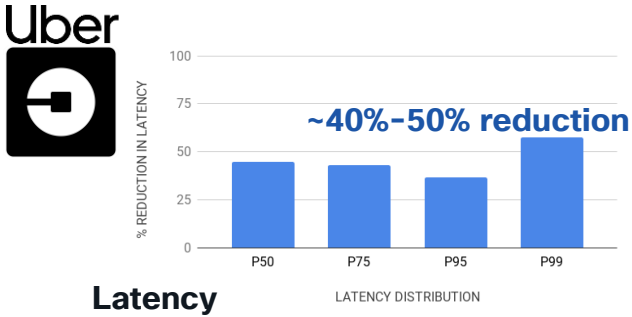
QoE Drives QUIC Adoption

Reference Slide

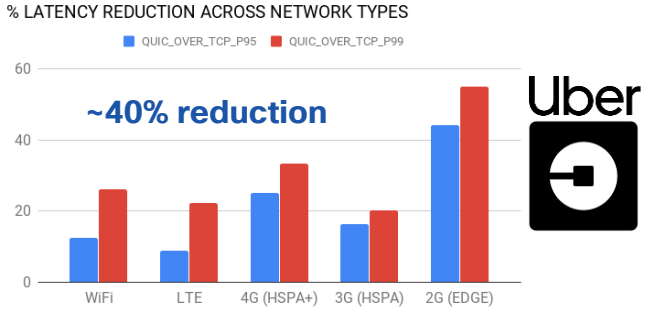
1.8B Daily Active Users – 3B Monthly
QUIC and H/3 are protocols of choice*



Google CDN Performance increase



Latency reduced significantly**



The more fragile the network, the more QUIC excels**

*source Facebook engineering

** source Uber engineering

IETF Standards

Reference Slide

TLS 1.3

RFC 8446

2018

QUIC

RFC 9000

2021

MASQUE

Charter-ietf-masque-2

2023

2018

Secure DNS Standards

DoT – RFC7858
DoH – RFC8484

2020

eSNI via ECH

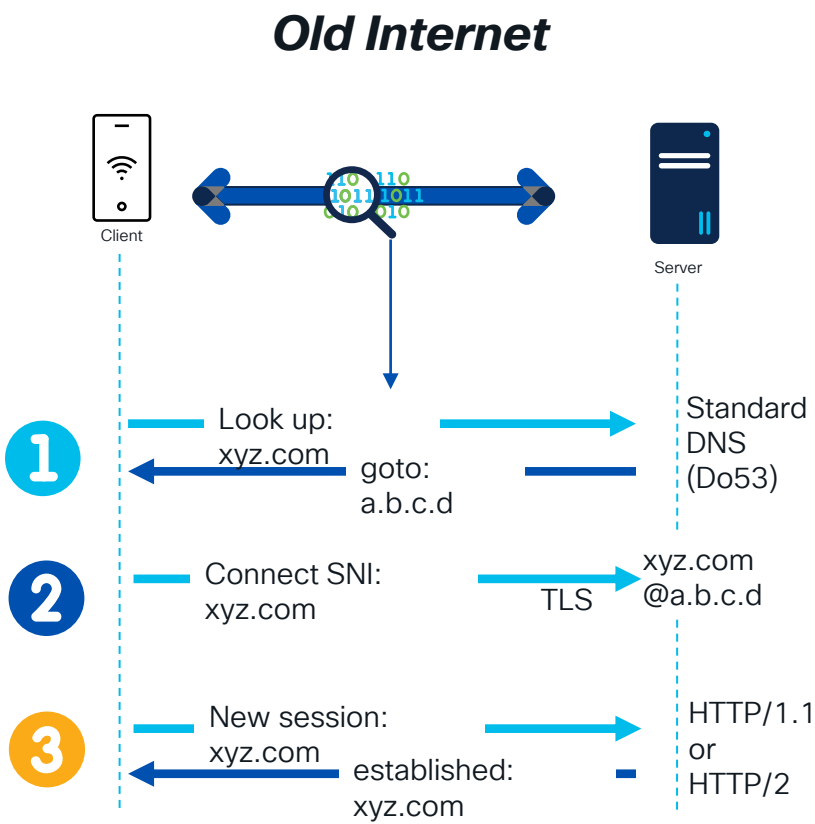
RFC8744
Draft-ietf-tls-esni-17

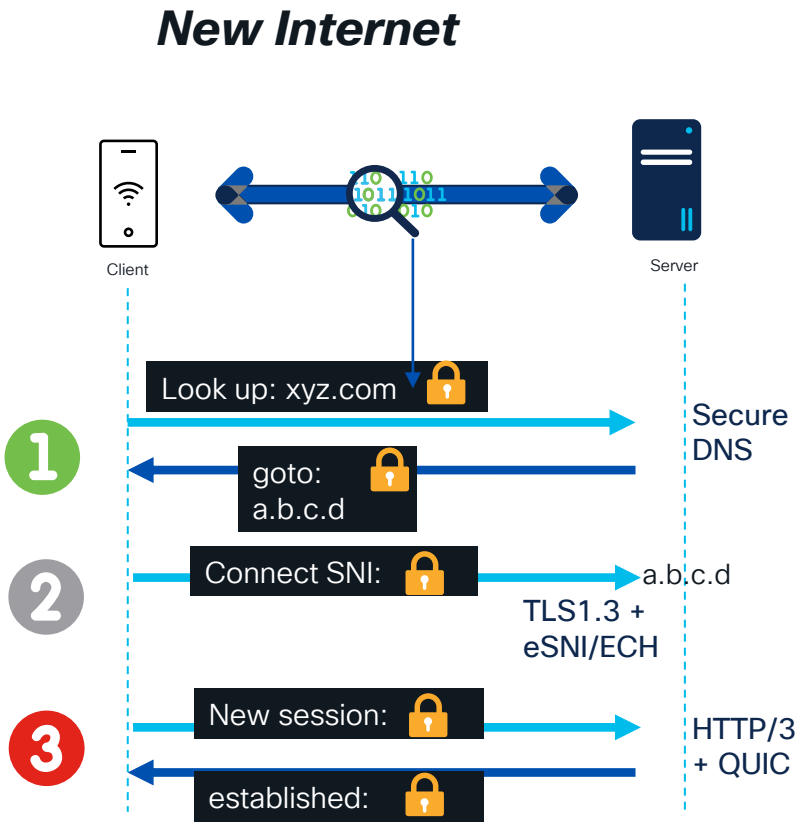
2022

HTTP/3

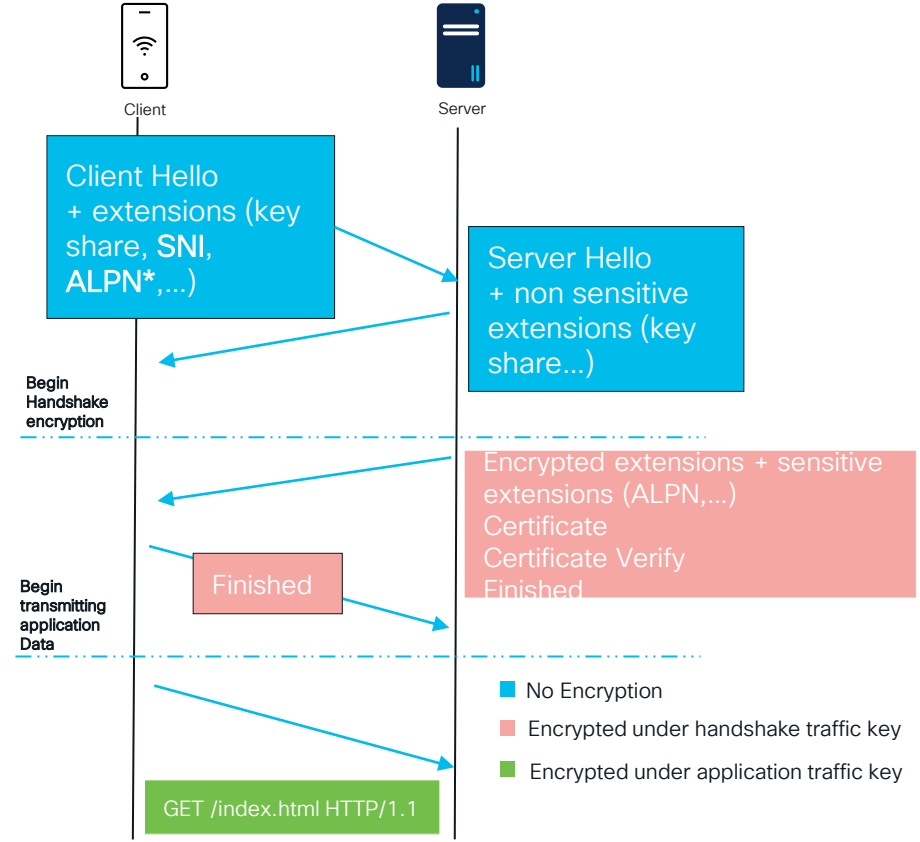
RFC9194

Visibility is lost in N6 interface

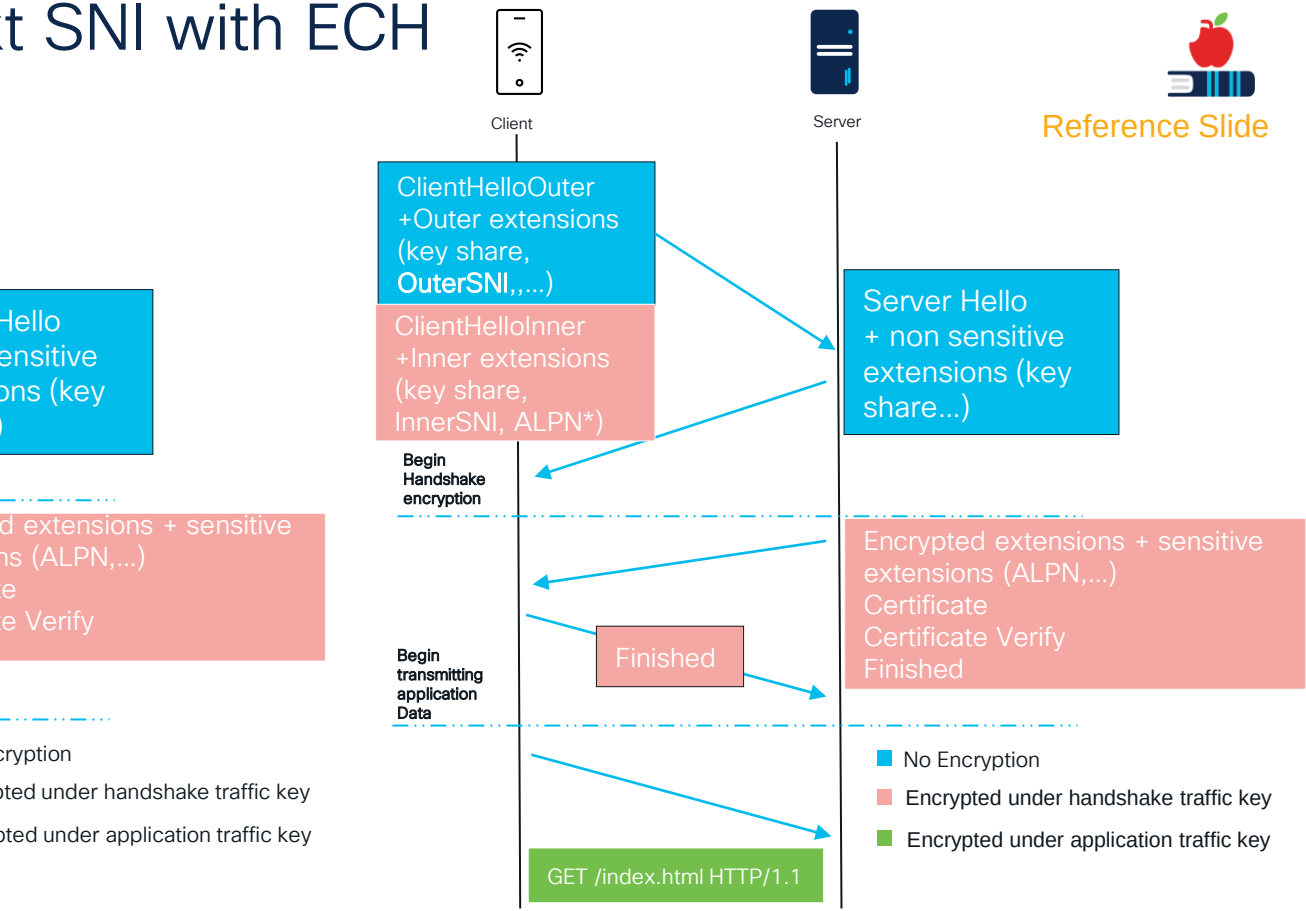




No more cleartext SNI with ECH



RFC 6066
Destination (SNI*) & capabilities in clear



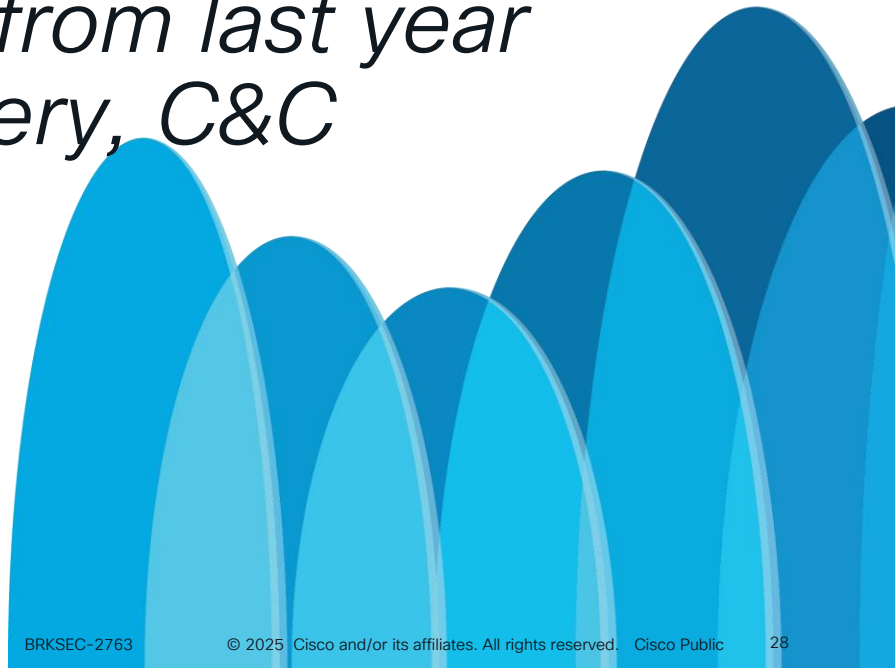
Draft-ietf-tls-esni-17
DNS over HTTPS
Destination (SNI*) & capabilities fully encrypted

SNI : server name identifier
ECH : Encrypted client Hello
ALPN : Application layer protocol negociation

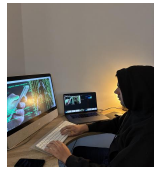
Reference Slide

*"More than 85% of attacks now use encrypted channels **across various stages of the kill chain**, up 20% from last year (Phishing, Malware Delivery, C&C activities, and more .)"*

Annual State of Encrypted Attacks Report, ThreatLabz, Q4 2024



5G_Hacker: Attack User plane devices through encrypted channels



Reconnaissance & Scanning

Tools: NMAP/ Shodan..

- 5G_hacker uses NMAP to Identify active hosts, open ports, and services.
- 5G_hacker uses Shodan to locate exposed vulnerable IoT devices running outdated firmware.

Vulnerability Identification & Exploitation

Tools: Metasploit / Exploit-DB..

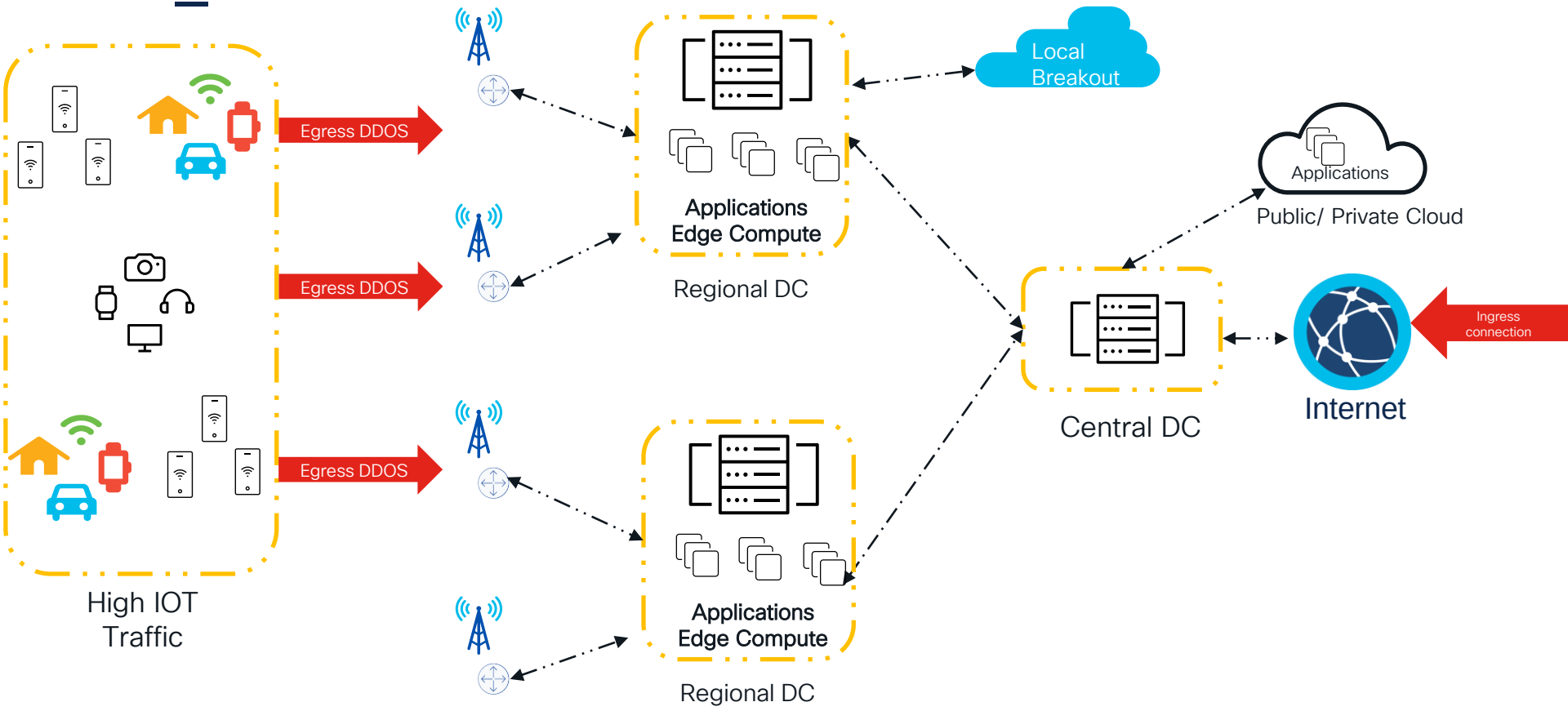
- 5G_hacker uses Exploit-DB repository of known exploits to learn about discovered IOT devices vulnerabilities
- 5G_hacker uses Metasploit Framework for developing and executing exploit code against target system

Initial access & Persistance

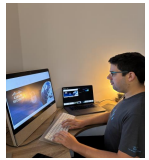
Tool: Hydra / Medusa / custom backdoors..

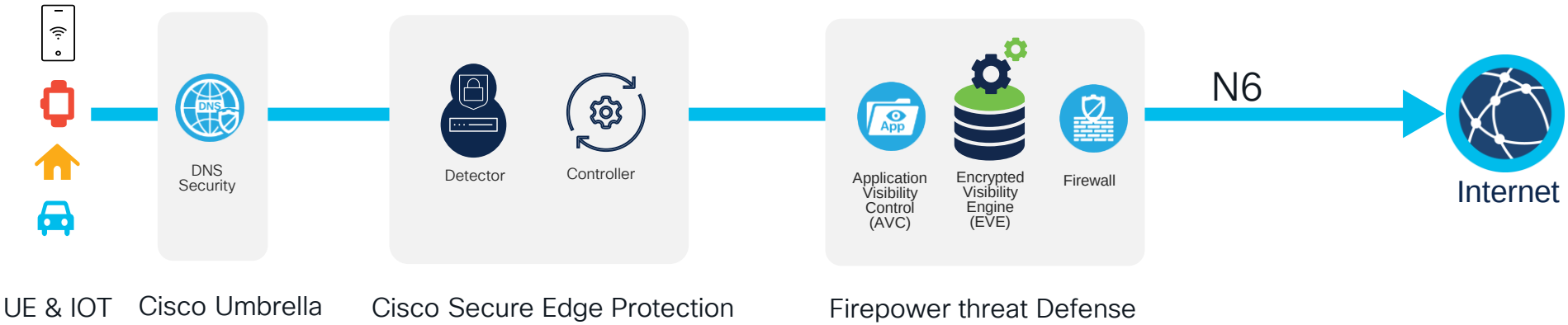
- 5G_Hacker will gain initial access by scanning for devices with default passwords or dictionary vulnerable devices using Hydra and Medusa
- 5G_hacker may use techniques such as HTTP(S) beacons or DNS tunneling to communicate with a Command-and-Control server using encrypted channels

5G_Hacker Attack Plan !



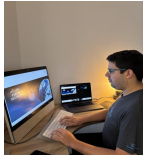
5G_Protector Proposal to secure User Plane



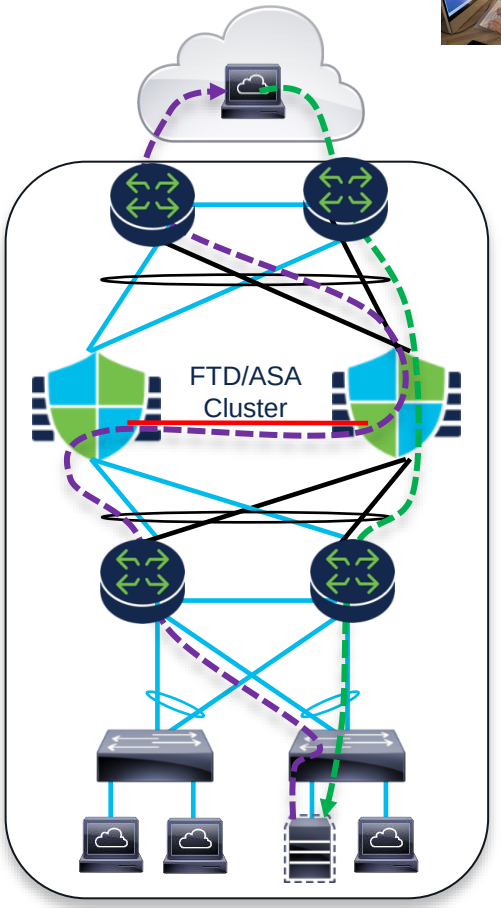


UE & IOT | Cisco Umbrella | Cisco Secure Edge Protection | Firepower threat Defense

Gi/N6 Firewall: Clustering

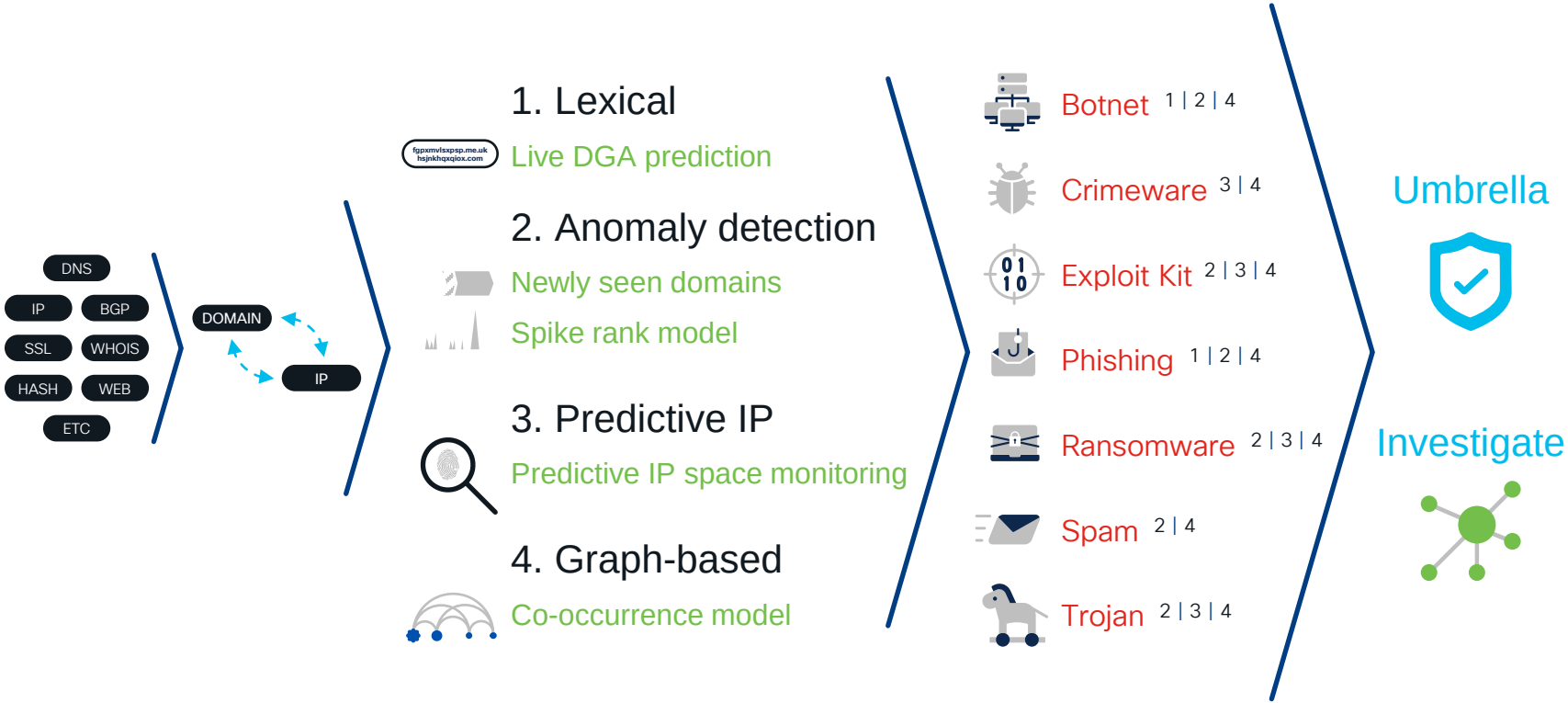


- Combines multiple Cisco Secure Firewalls into a single logical device with configuration shared among all units in the cluster
- Same configuration shared among all units in the cluster
- Allows pay as you grow sizing – nodes can be added to existing clusters up to 16 nodes. This is crucial for 5G disaggregation
- EtherChannel with LACP provides resilience distribution of traffic towards the cluster
- Resolves routing asymmetry
- All packets in a bidirectional flow are redirected to the *flow owner*

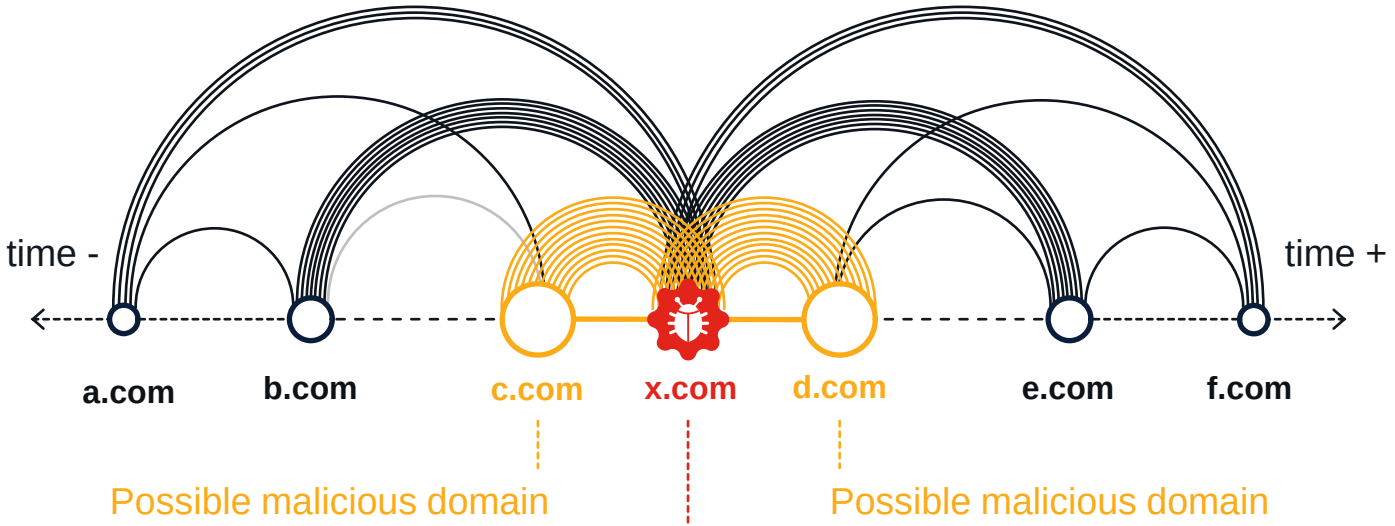


90% of malwares use DNS in attacks

Cisco Umbrella: Multi-faceted threat intelligence



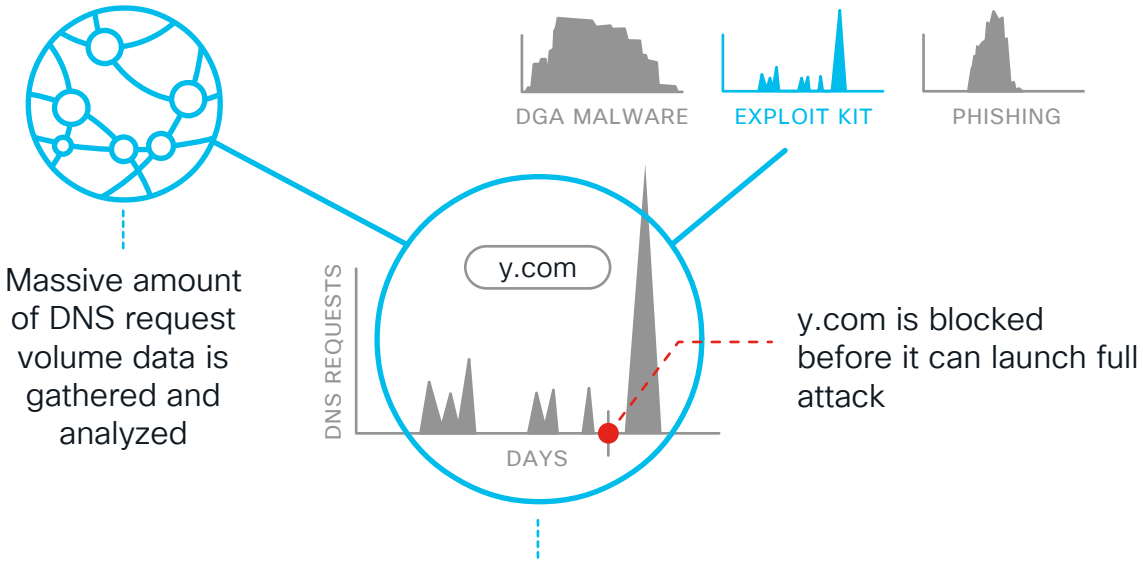
Co-occurrence Model: Domains guilty by inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

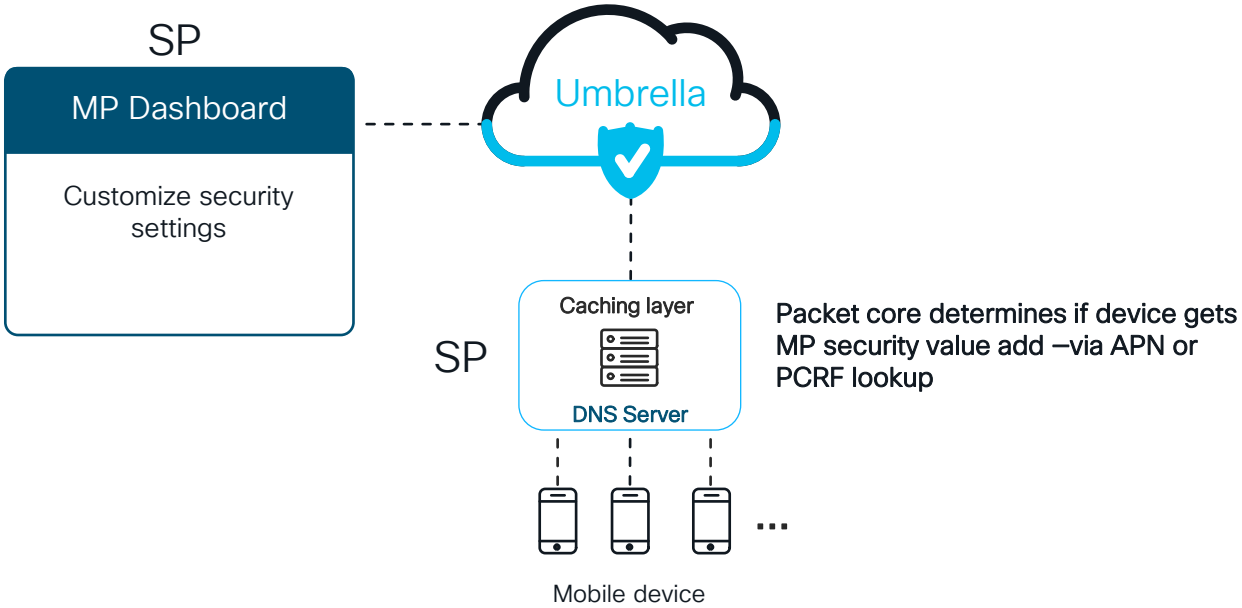
Spike Rank Model : Patterns of guilt

Reference Slide



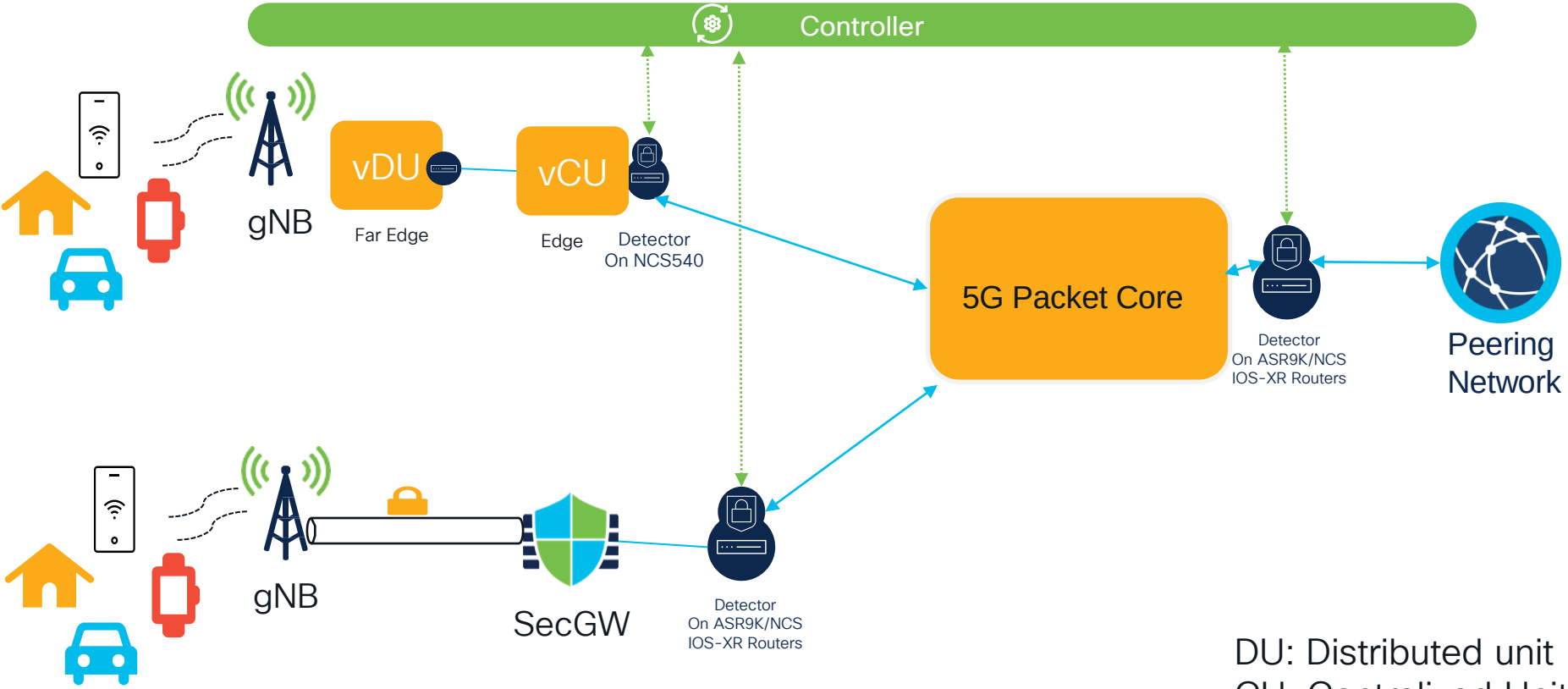
Umbrella for SP: Mobile Protect

Reference Slide



APN : Access Point Name
PCRF : Policy & Charging Rule function

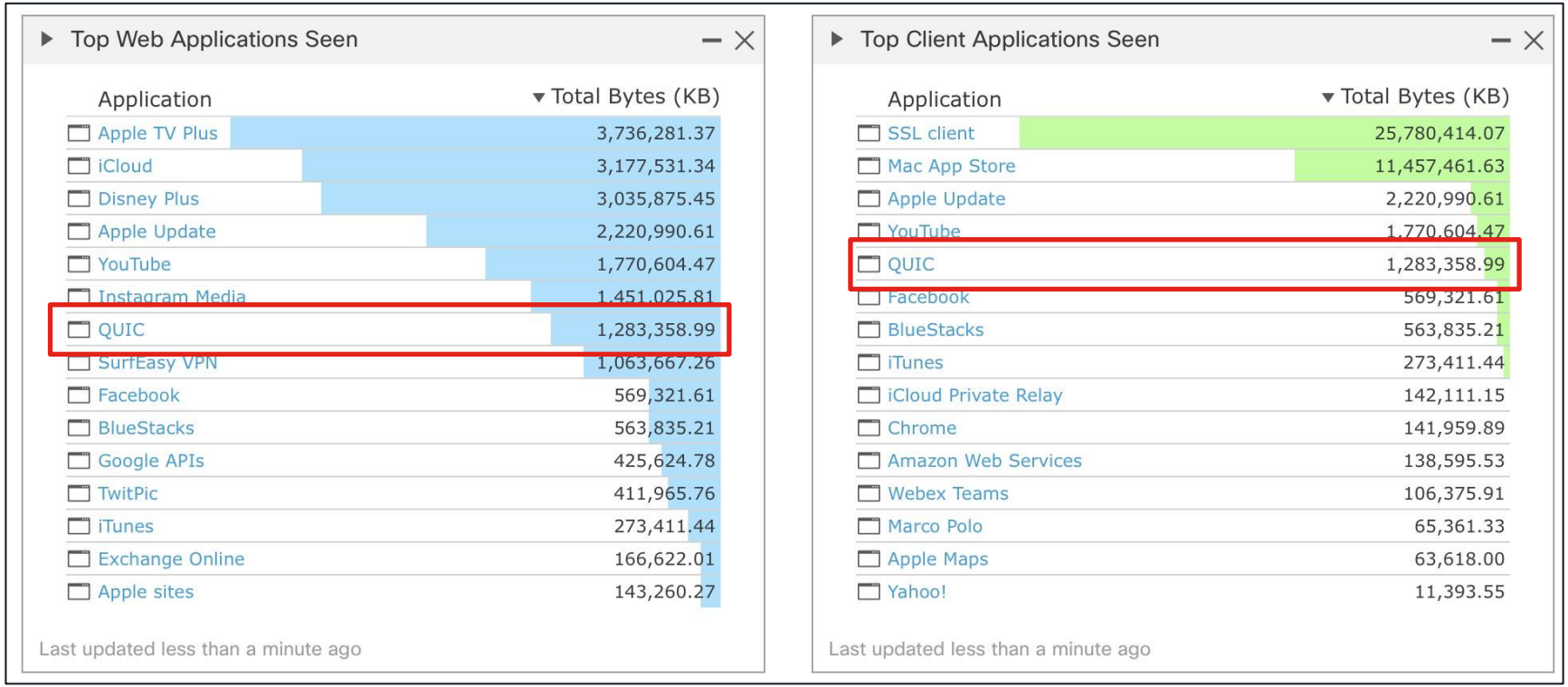
Cisco secure edge DDOS: BRKSPG-2401



DU: Distributed unit
CU: Centralized Unit

How to figure out if my subscribers are infected ?

Secure Firewall Encrypted Visibility Engine : OFF



Top Web Applications Seen

Application	Total Bytes (KB)
Apple TV Plus	3,736,281.37
iCloud	3,177,531.34
Disney Plus	3,035,875.45
Apple Update	2,220,990.61
YouTube	1,770,604.47
Instagram Media	1,451,025.81
QUIC	1,283,358.99
SurfEasy VPN	1,063,667.26
Facebook	569,321.61
BlueStacks	563,835.21
Google APIs	425,624.78
TwitPic	411,965.76
iTunes	273,411.44
Exchange Online	166,622.01
Apple sites	143,260.27

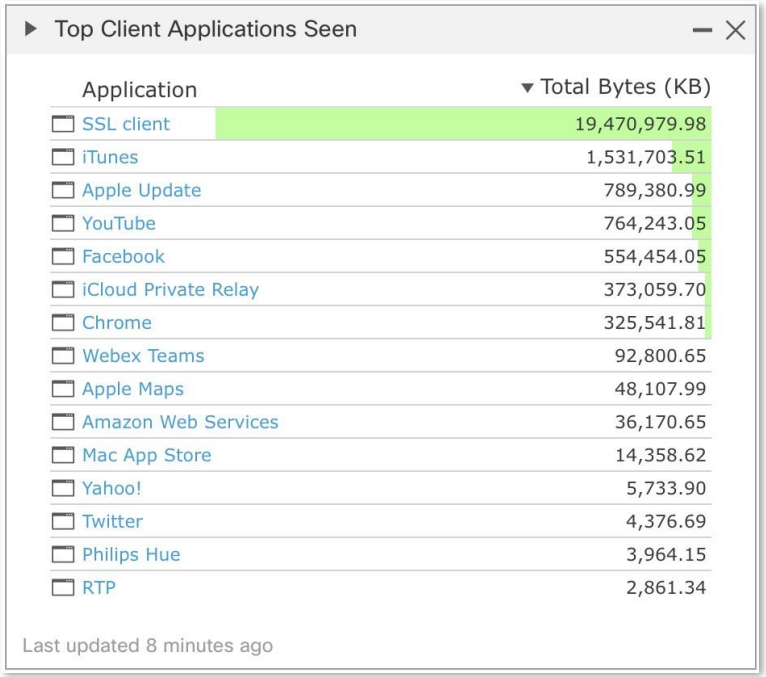
Last updated less than a minute ago

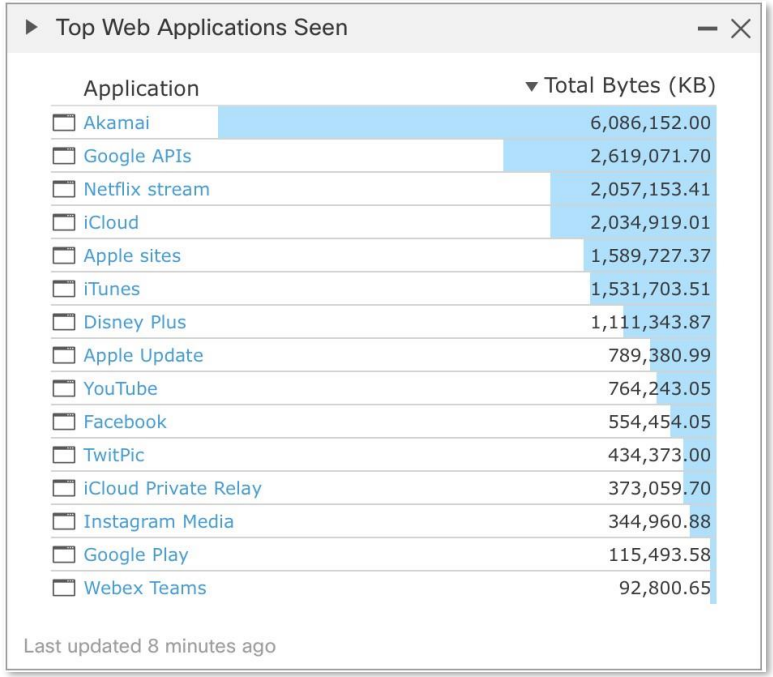
Top Client Applications Seen

Application	Total Bytes (KB)
SSL client	25,780,414.07
Mac App Store	11,457,461.63
Apple Update	2,220,990.61
YouTube	1,770,604.47
QUIC	1,283,358.99
Facebook	569,321.61
BlueStacks	563,835.21
iTunes	273,411.44
iCloud Private Relay	142,111.15
Chrome	141,959.89
Amazon Web Services	138,595.53
Webex Teams	106,375.91
Marco Polo	65,361.33
Apple Maps	63,618.00
Yahoo!	11,393.55

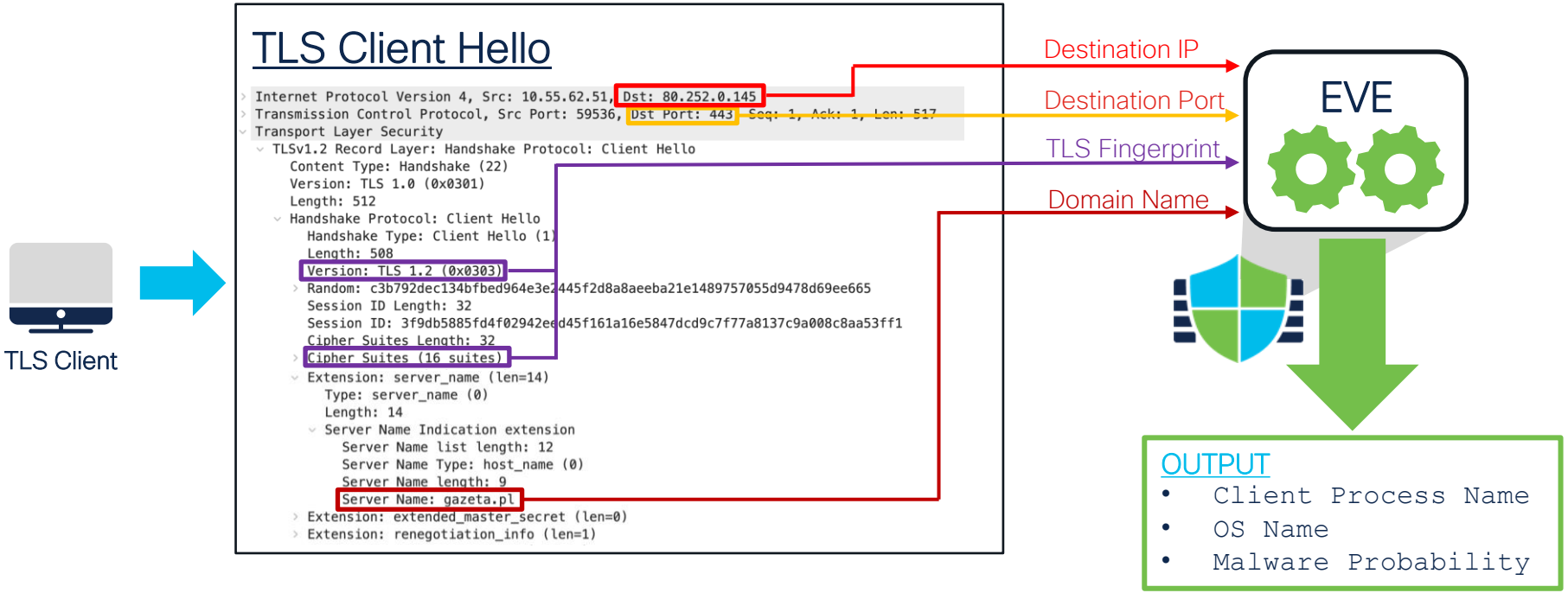
Last updated less than a minute ago

Secure Firewall Encrypted Visibility Engine : ON

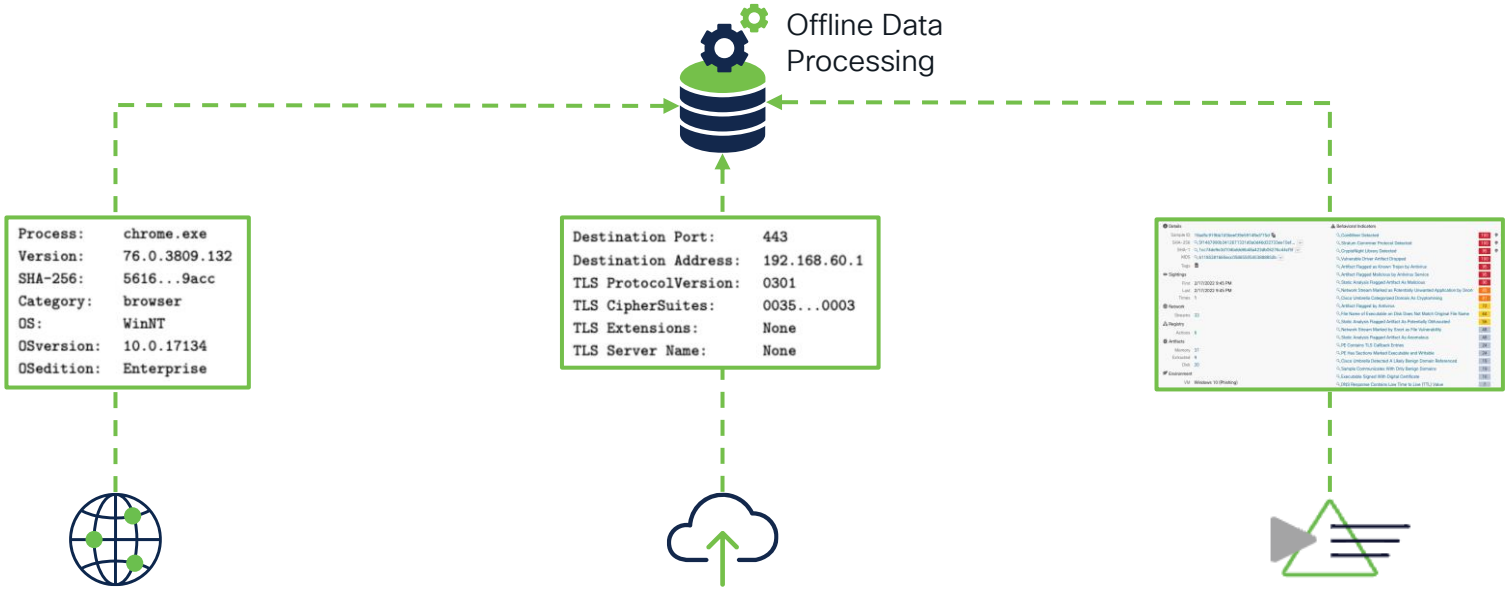




Encrypted Visibility Engine Output



How is EVE dataset Powered?

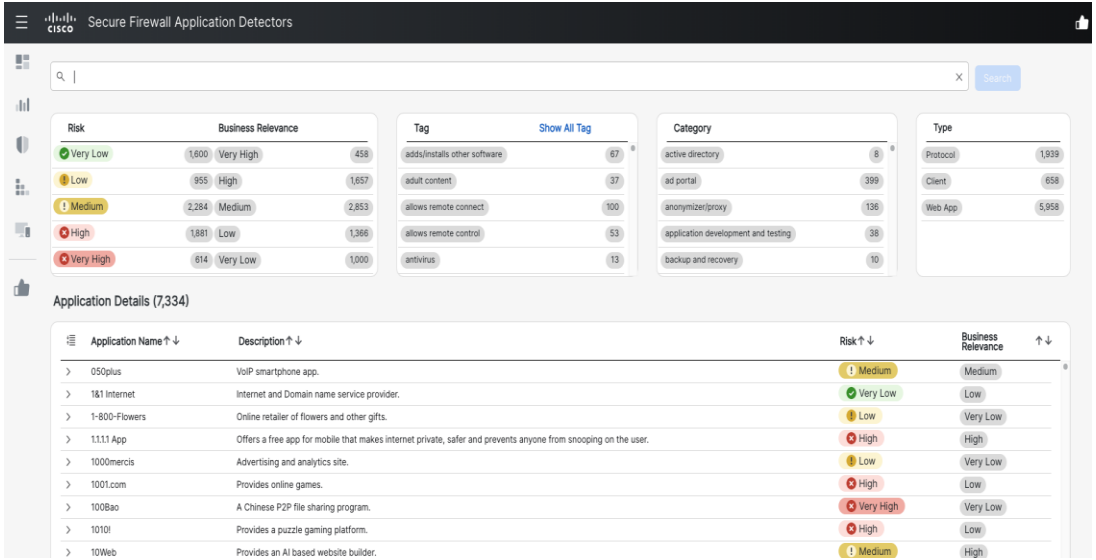


Process data from 80,000 Secure Client (AnyConnect) endpoints **everyday**

Over 30 DCs around the globe collecting 1B TLS fingerprints **daily**

10,000 samples sandboxed by Secure Malware Analytics **everyday**

Appid.cisco.com




```
stats:
  general:
    total fingerprints:          10,000
    total labeled fingerprints: 4,934
    total connections:           11,004,470,612
    fingerprints per protocol:
         tls: 2,902
        http: 1,885
        quic: 146
      tofsee: 1
    connections per protocol:
         tls: 8,662,691,963
        http: 1,980,055,863
        quic: 361,722,785
      tofsee: 1

  Threat Grid:
    total fingerprints: 784
    total connections:  5,530,102
    fingerprints per protocol:
        http: 607
         tls: 176
      tofsee: 1
    connections per protocol:
         tls: 3,640,195
        http: 1,889,906
      tofsee: 1
```

- Details, release notes for each application supported for cisco secure firewall
- Over 300 encrypted applications are recognized by EVE

EVE in action

1, Process Confidence denotes how certain we are with EVE judgement on the source process.

3, Threat Confidence and Score provide calculated likelihood of a flow being sourced by malware.

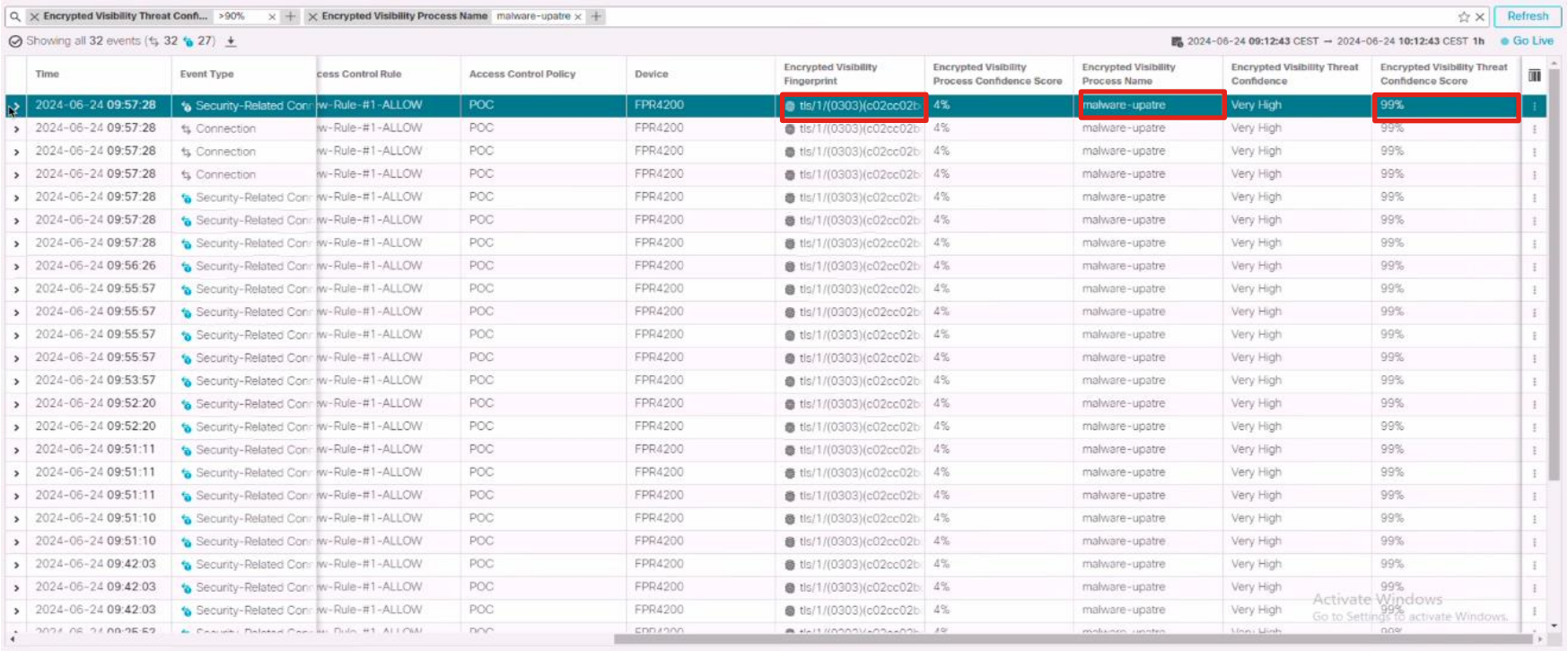
Time	Action	Event Type	Destination IP	Destination Port / ICMP Code	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score	Client Application	Detection Type
2022-05-04 17:14:10	Allow	Connection	199.58.81.140	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:53	Allow	Connection	163.172.21.117	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:49	Allow	Connection	45.66.33.45	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:32	Allow	Connection	131.188.40.189	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:27	Allow	Connection	45.14.233.149	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint

2, Process Name denotes the name of the process on the host that generated this flow.

4, Client Application detected by EVE and added to the source Host Profile.

5, Detection Type is marked as TLS Fingerprint.

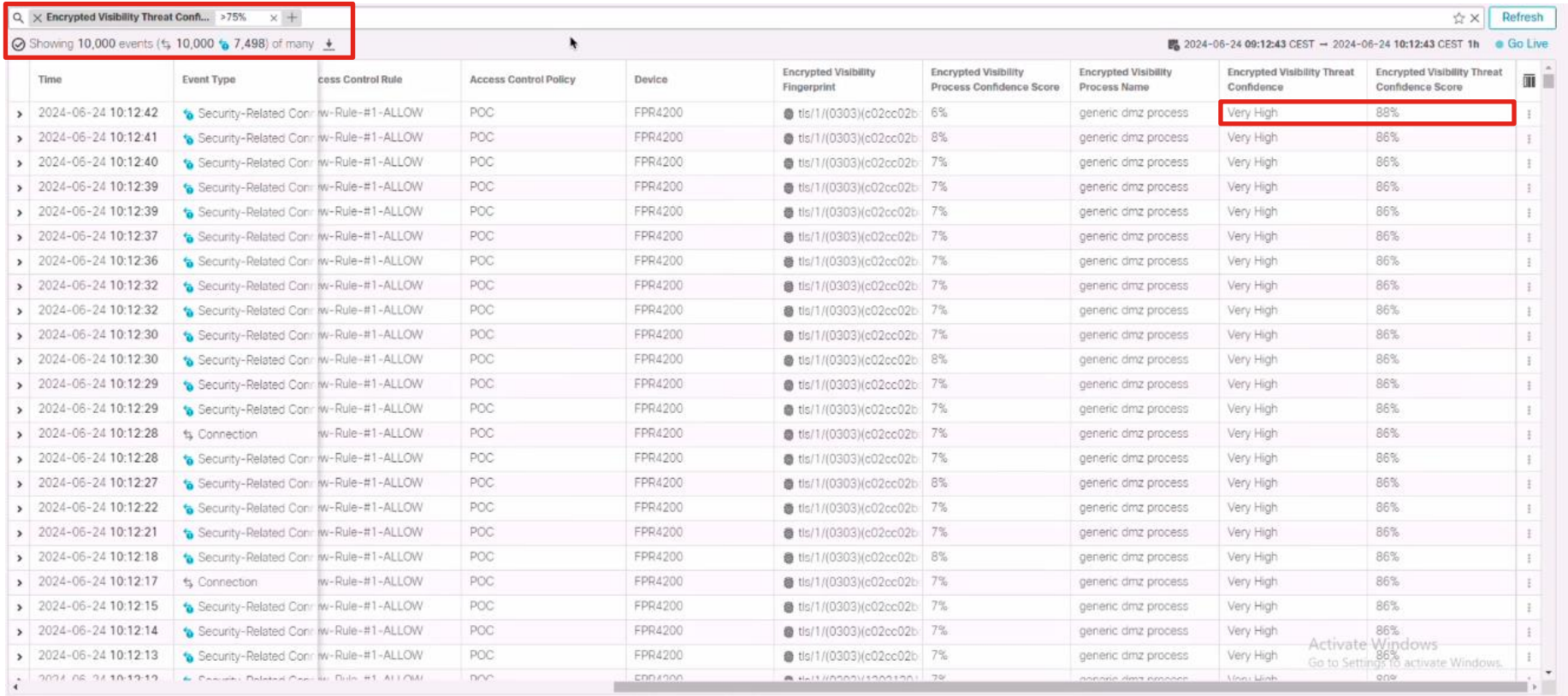
EVE in action



- EVE performance impact is minimal

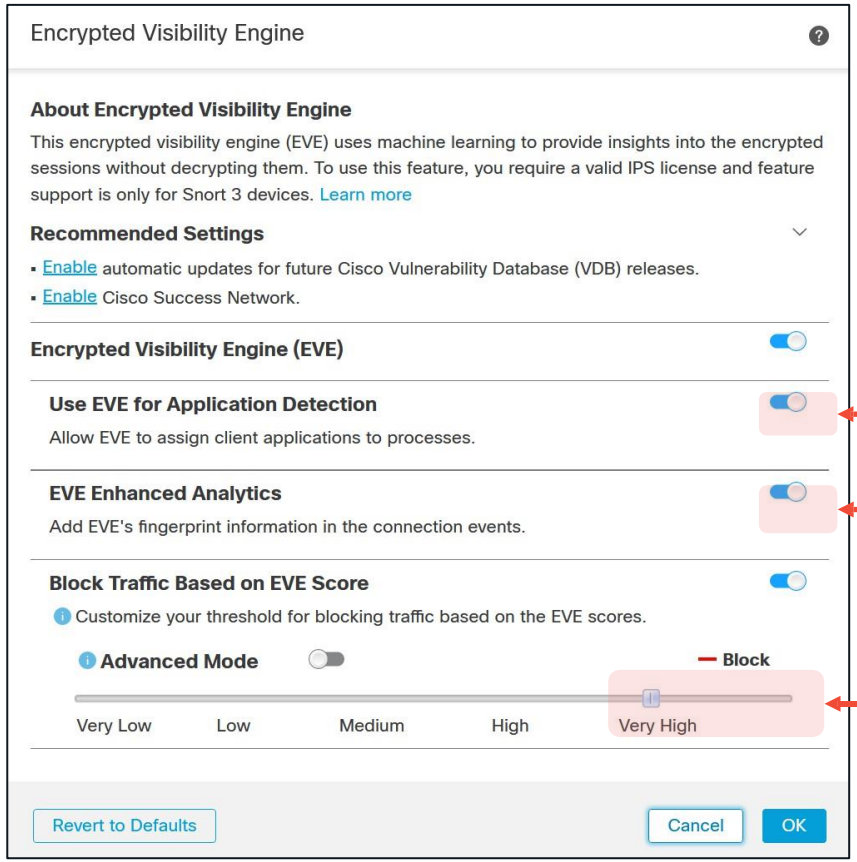
EVE in action

Reference Slide



Time	Event Type	cess Control Rule	Access Control Policy	Device	Encrypted Visibility Fingerprint	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
2024-06-24 10:12:42	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	6%	generic dmz process	Very High	88%
2024-06-24 10:12:41	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	8%	generic dmz process	Very High	86%
2024-06-24 10:12:40	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:39	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:39	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:37	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:36	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:32	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:32	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:30	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:30	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	8%	generic dmz process	Very High	86%
2024-06-24 10:12:29	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:29	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:28	Connection	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:28	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:27	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	8%	generic dmz process	Very High	86%
2024-06-24 10:12:22	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:21	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:18	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	8%	generic dmz process	Very High	86%
2024-06-24 10:12:17	Connection	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:15	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:14	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%
2024-06-24 10:12:13	Security-Related Con	w-Rule-#1-ALLOW	POC	FPR4200	tls/1/(0303)(c02cc02b	7%	generic dmz process	Very High	86%

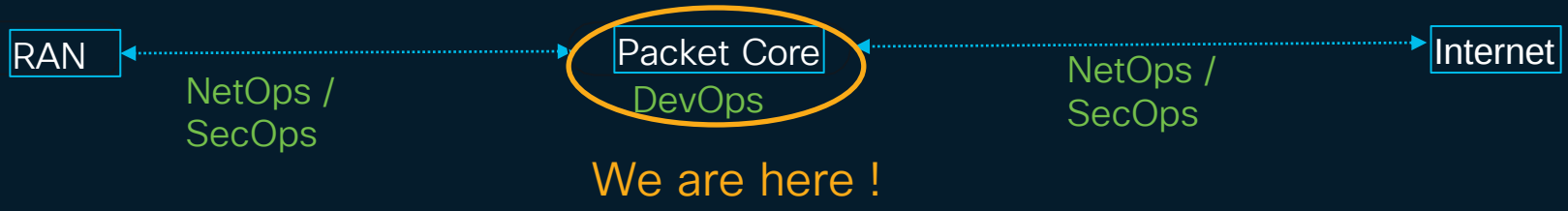
Encrypted Visibility Engine (EVE) 2.0



Inference-based AppID enrichment.

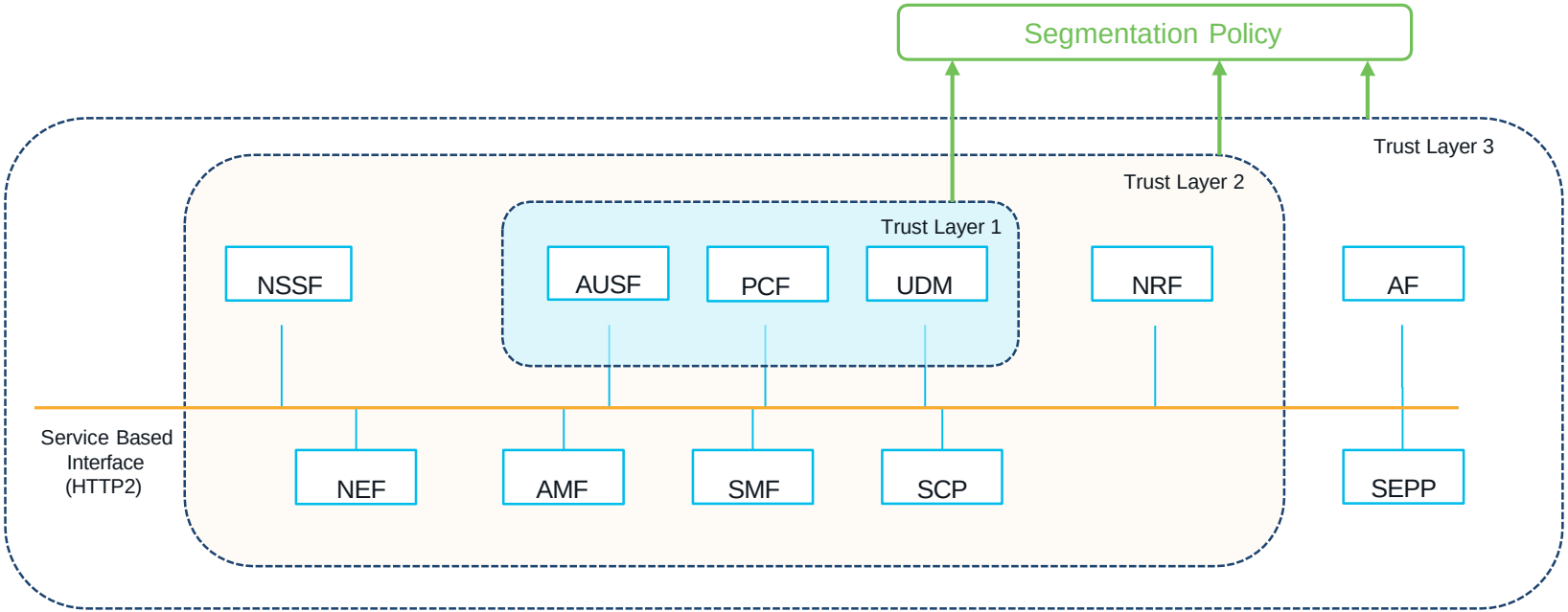
Detailed fingerprint data for third-party use.

Connection filtering based on malware confidence scores.



Packet Core Protection Use Case

5G Core Trust Model



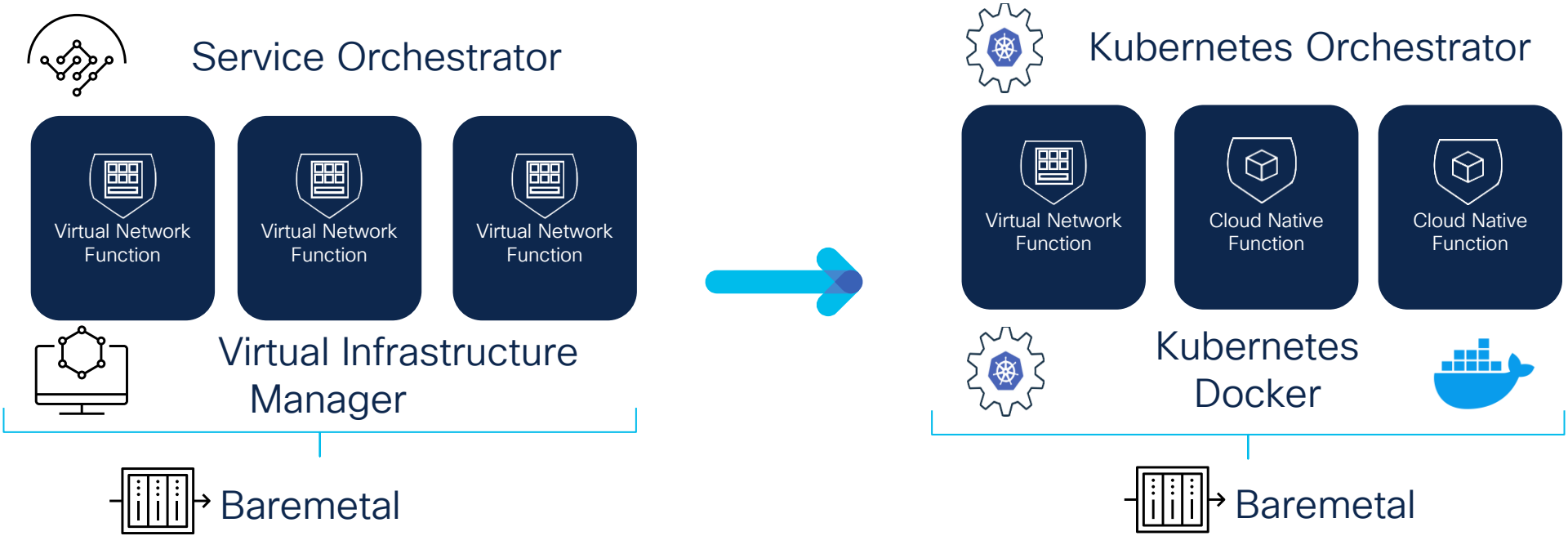
NSSF: Network Slice Selection Function
AUSF: Authentication Server Function
PCF: Policy Control Function
UDM: Unified Data management
NRF: Network Repository Function

AF: Application Function
AMF: Access and Mobility Function
SMF: Session Management Function
SCP: Secure Communication Proxy NEF: Network Exposure Function

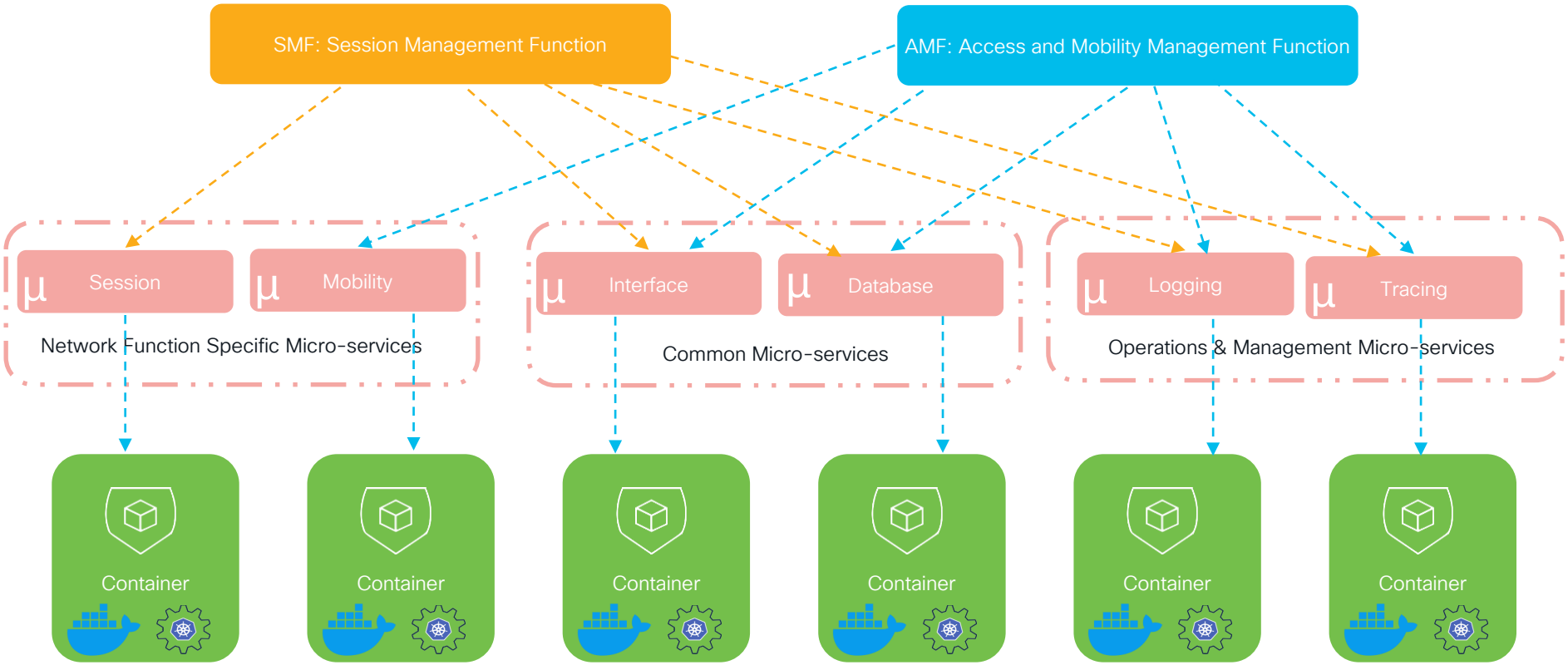
SEPP: Secure Edge Protection Proxy
UPF: User Plane Function
vDU: Distributed Unit
vCU: Centralized Unit

Source: 3GPP 1975-sec_5g

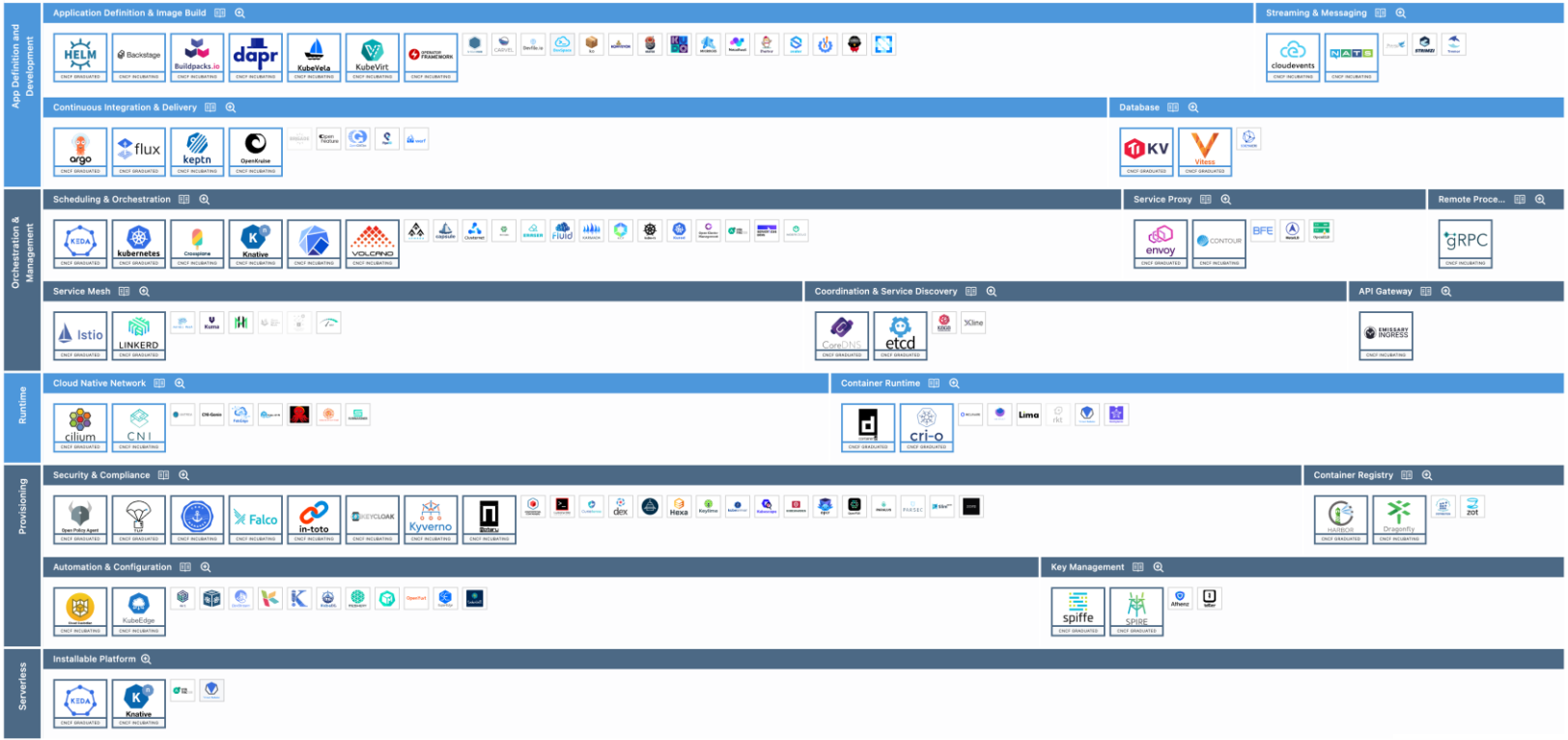
5G: Cloud Native Infrastructure transition



How does Virtual Network Function look like?



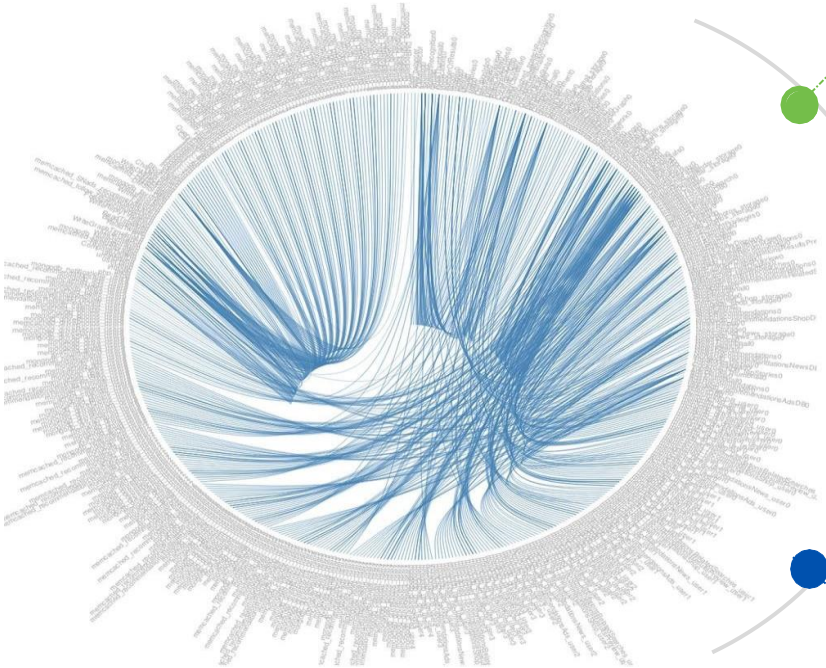
Cloud Native Computing Foundation



Source : [CNCF Landscape](#)

CLOUD NATIVE LANDSCAPE

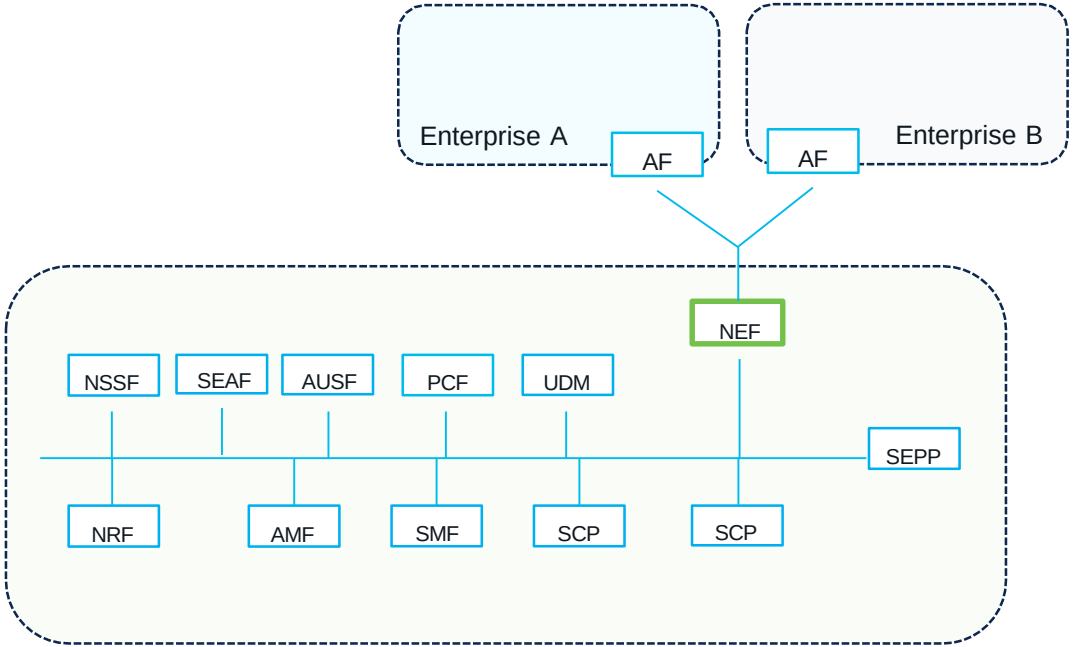
Security Challenges in Service Based Interface



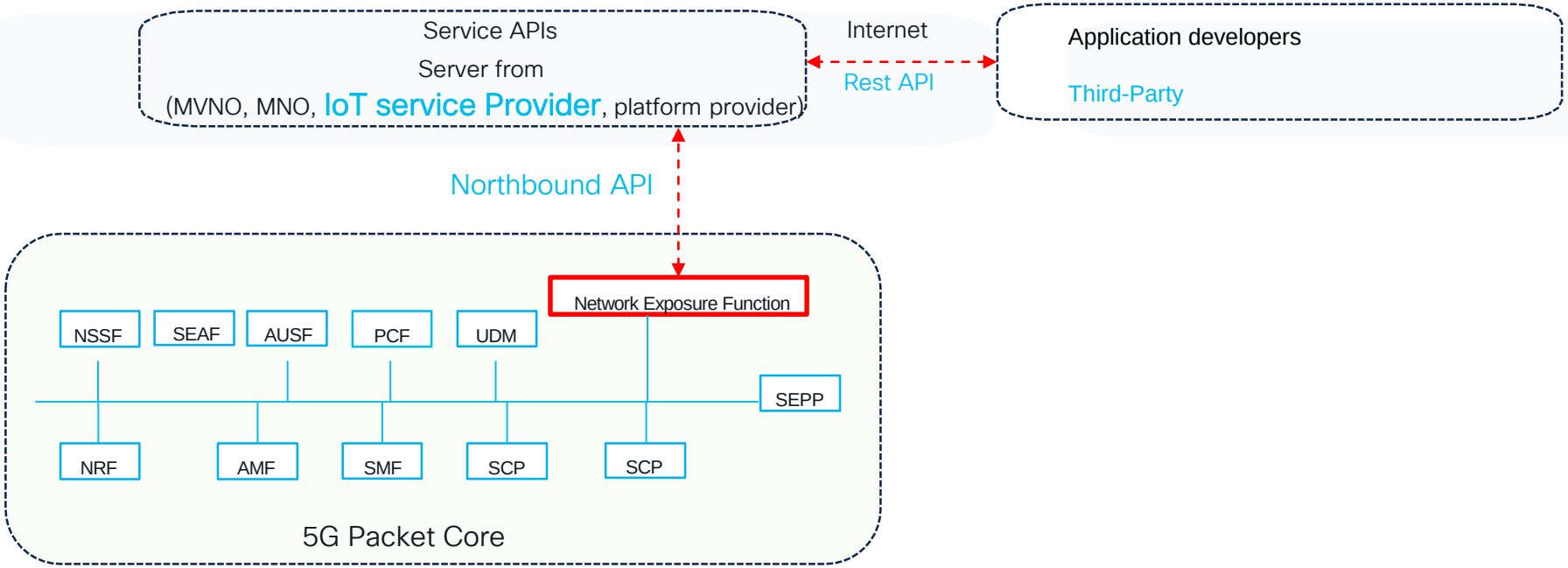
- OAUTH on the Service Based Interface?
- mTLS on the Service Based Interface?
- API Rate limiting?
- Do I see all my images and their interactions?
- Do I have Pod security Measures ? Like RBAC?

Came with 5G: Exposing the core: NEF

Reference Slide



Network Exposure Function



- Used for applications like : Smart Factories, Virtual realities, Vehicle tracking and monitoring…
- Provides access to the mobile core for third party services

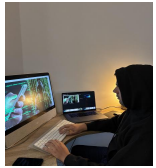
IoT Service Platforms

- The Service APIs portal is a platform where users can interact with different APIs
- APIs use Swagger or OpenAPI, which are tools that make it easy to see and use the APIs

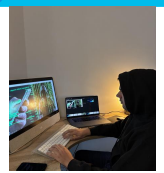
SIM

GET	/api/v1/sim	List SIMs
GET	/api/v1/sim/status	List SIM Statuses
GET	/api/v1/sim/{sim_id}	SIM Details
DELETE	/api/v1/sim/{sim_id}	Delete a SIM
PATCH	/api/v1/sim/{sim_id}	Update a SIM
GET	/api/v1/sim/{sim_id}/stats	SIM Usage and Costs Statistics
GET	/api/v1/sim/{sim_id}/stats/daily	SIM Usage and Costs Statistics per day
GET	/api/v1/sim/{sim_id}/event	List SIM Events
GET	/api/v1/sim_batch/bic/{bic}	Validate if a given batch can be registered by BIC
PATCH	/api/v1/sim_batch/bic/{bic}	Register a given batch by BIC

5G_Hacker Plan to Access network exposure services



5G_Hacker registers with a fake company tax ID and a spoofed email address. Many providers have weak verification processes



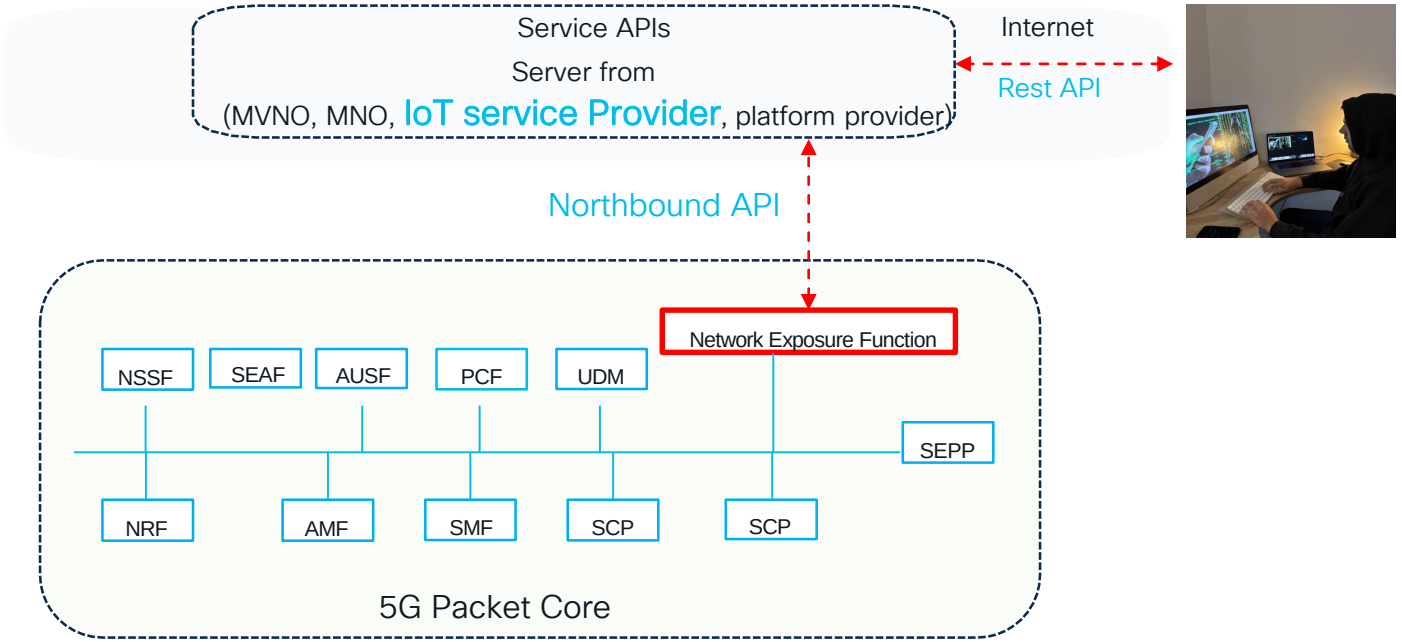
5G_Hacker Receives SIM cards at a private (random) address and gains access to service APIs via email

5G_hacker activates SIM Card and validates credentials

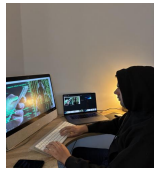
5G_Hacker has Access to IOT service platform APIs and masquerades as a target company while accessing the platform

5G_Hacker can perform API operations and probing to find vulnerabilities.

5G_hacker got access to Packet Core



What can 5G_attacker accomplish with such access ?



5G Hacker attack

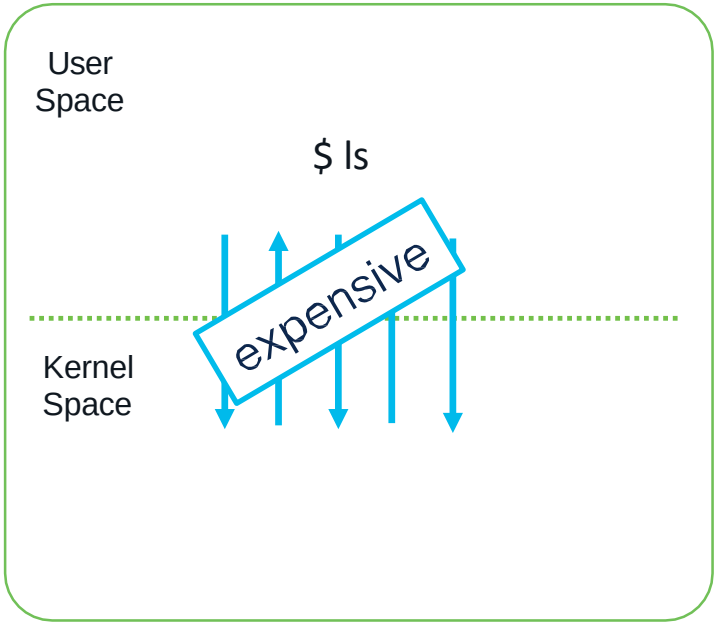
- Inject Malicious payloads, strings, characters, files
- Uses Guidelines from OWASP web security testing
- Uses REST security cheat sheets

BURPSUITE

5G Hacker findings

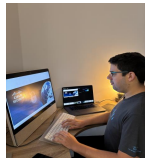
- No OAuth token generation on several platforms
- Static API tokens (which don't expire)
- Few rate limits for API requests
- No mTLS within service Based Interface
- No IP ban was observed from the API gateway
- Verbose error messages

User to Kernel space communication

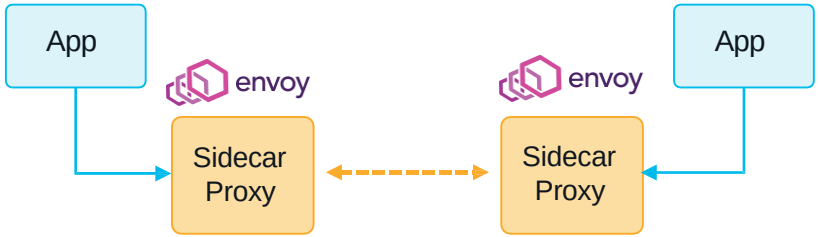


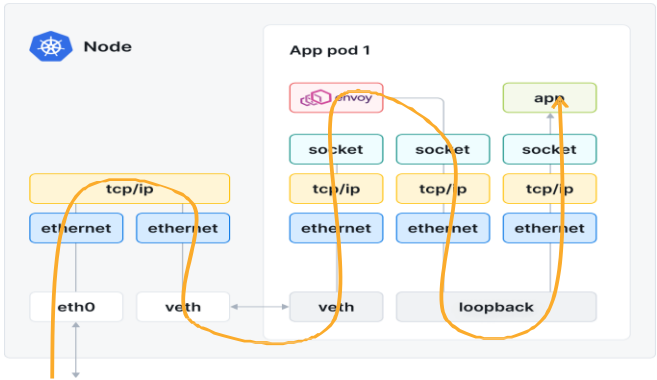

```
ansiblecontroller@worker02:~/Documents$ strace -c ls
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 38.57    0.000712          26        27           mmap
 32.56    0.000601         601         1           execve
  6.12    0.000113          16         7           read
  5.85    0.000108          13         8           pread64
  5.31    0.000098          12         8           mprotect
  4.50    0.000083           9         9           openat
  1.73    0.000032           3         9           fstat
  1.68    0.000031          31         1           munmap
  1.35    0.000025           2        11           close
  0.70    0.000013           6         2         2 access
  0.38    0.000007           3         2           rt_sigaction
  0.33    0.000006           3         2         1 arch_prctl
  0.22    0.000004           4         1           set_tid_address
  0.22    0.000004           4         1           prlimit64
  0.16    0.000003           1         3           brk
  0.16    0.000003           3         1           rt_sigprocmask
  0.16    0.000003           3         1           set_robust_list
  0.00    0.000000           0         2           ioctl
  0.00    0.000000           0         2         2 statfs
  0.00    0.000000           0         2           getdents64
------ ----------- ----------- --------- --------- ----------------
100.00    0.001846                   100         5 total
```

Service Mesh



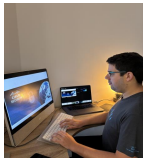
- mTLS and Authentication
- Ingress
  - Load Balancing
  - Protocol Parsing
  - Path-based routing
- L7 traffic management
  - Service load balancing East West
  - Rules





- Performance Impact

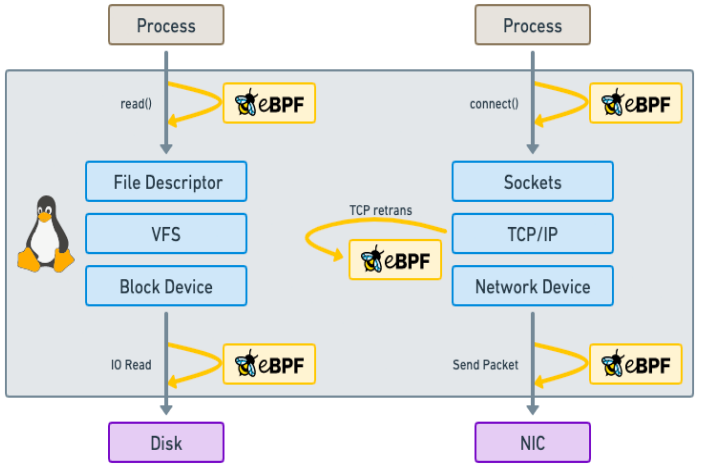
eBPF can resolve the equation !



- eBPF is a technology that can run sandboxed programs in the operating system kernel
- Enables high performance and low CPU overhead infrastructure tools

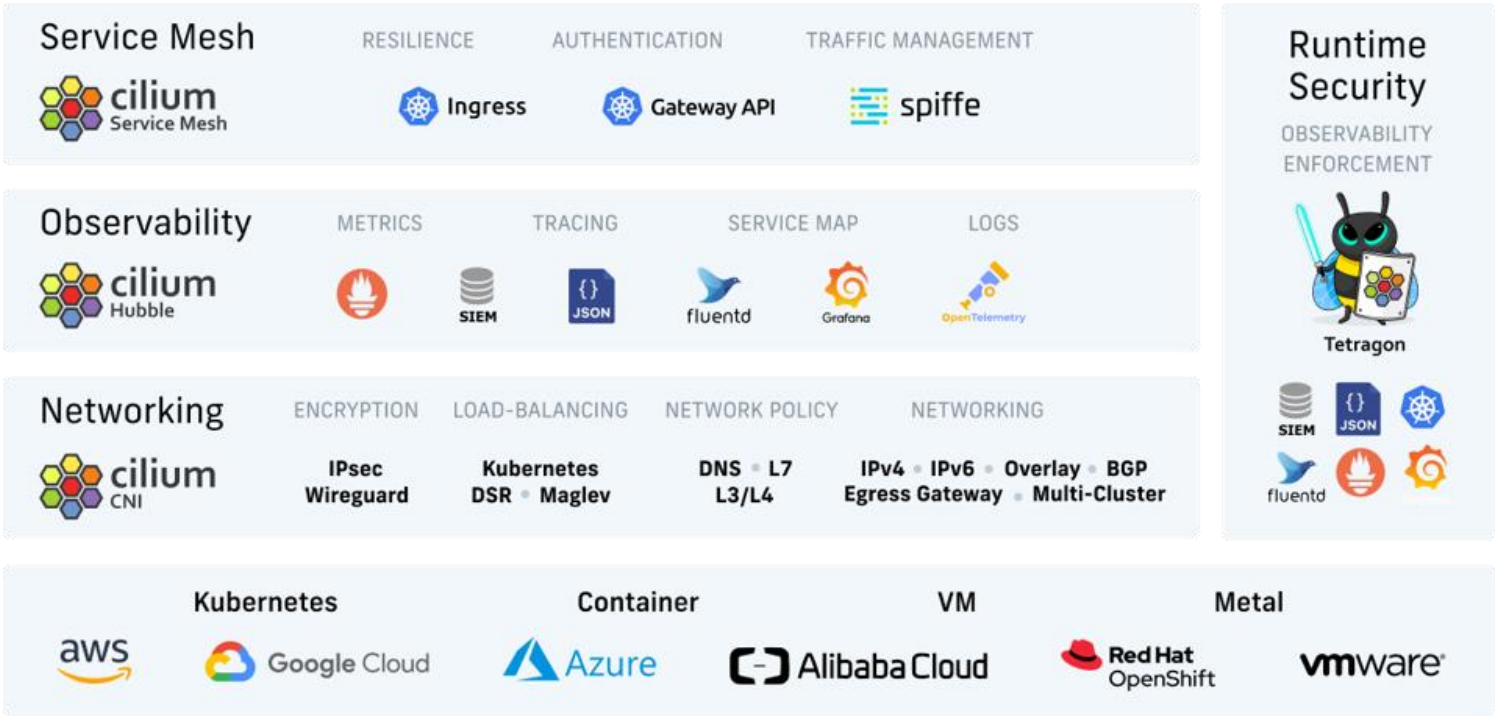
BUT

- Requires kernel knowledge to build advanced capabilities
- Most users will leverage existing tools rather than writing eBPF themselves



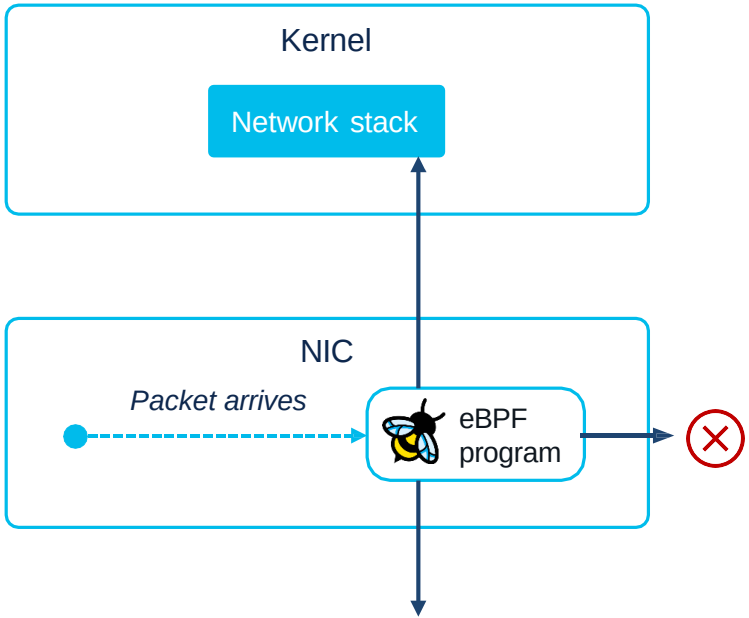
Attachment points: Kernel functions, userspace functions, system calls, sockets, packet level...

Cloud-Native Security with eBPF: Cilium, Hubble and Tetragon

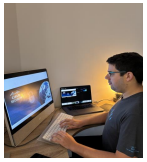


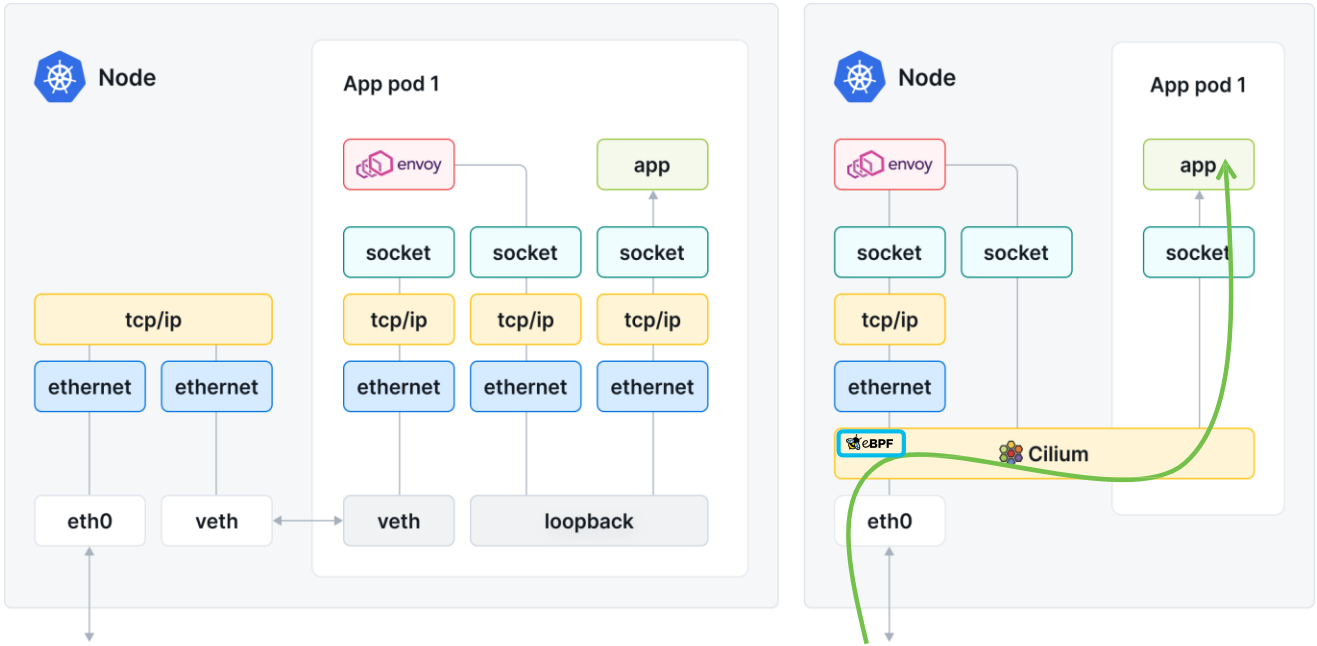
eXpress Data Path

Reference Slide



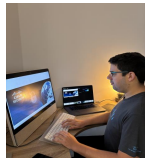
Cilium: Reduces performance impact !



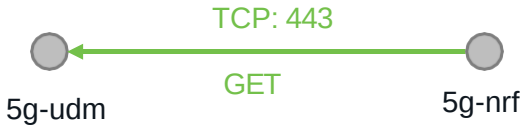


- **Cilium** is an open-source project based on eBPF to provide networking and security for cloud native environments such as Kubernetes clusters

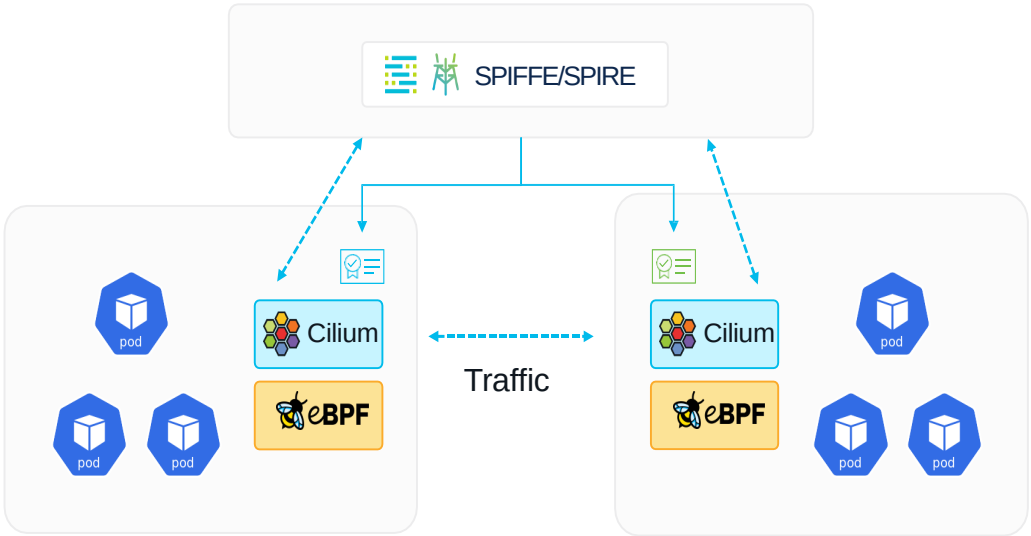
Identity aware Network Policy for 3GPP segmentation



```yaml
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  name: sba-rule
  namespace: 5g
spec:
  description: "Allow HTTP2 Get from app=5g-udm to app=5g-nrf"
  endpointSelector:
    matchLabels:
      app: 5g-udm
  ingress:
  - fromEndpoints:
    - matchLabels:
        app: 5g-nrf
      toPorts:
      - ports:
        - port: "443"
          protocol: TCP
        rules
          http:
          method: "GET"
```



Mutual Authentication with cilium

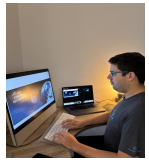


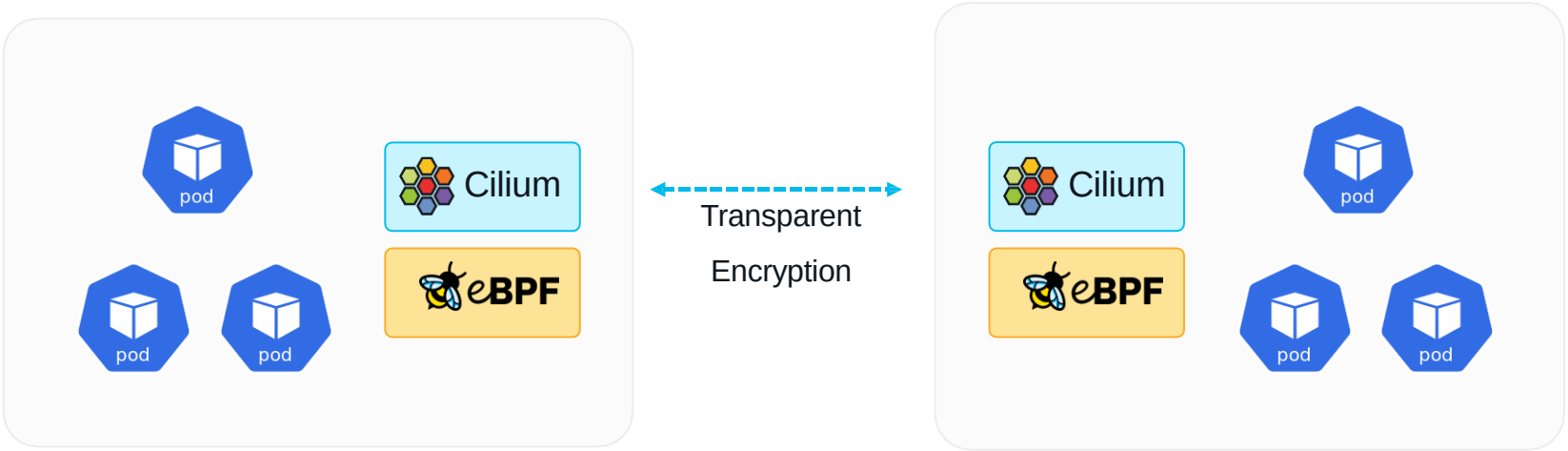

```
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  name: mutual-auth-echo
spec:
  endpointSelector:
    matchLabels:
      app: echo
  ingress:
  - fromEndpoints:
    - matchLabels:
        app: pod-worker
    authentication:
      mode: "required"
    toPorts:
    - ports:
      - port: "8080"
        protocol: TCP
```

$authentication.mutual.spire.install.enabled=true
$authentication.mutual.spire.enabled=true

- SPIFFE is a simple standard for giving unique IDs to software services so they can securely talk to each other
- SPIRE is a tool that implements SPIFFE, managing those IDs and ensuring secure service interactions

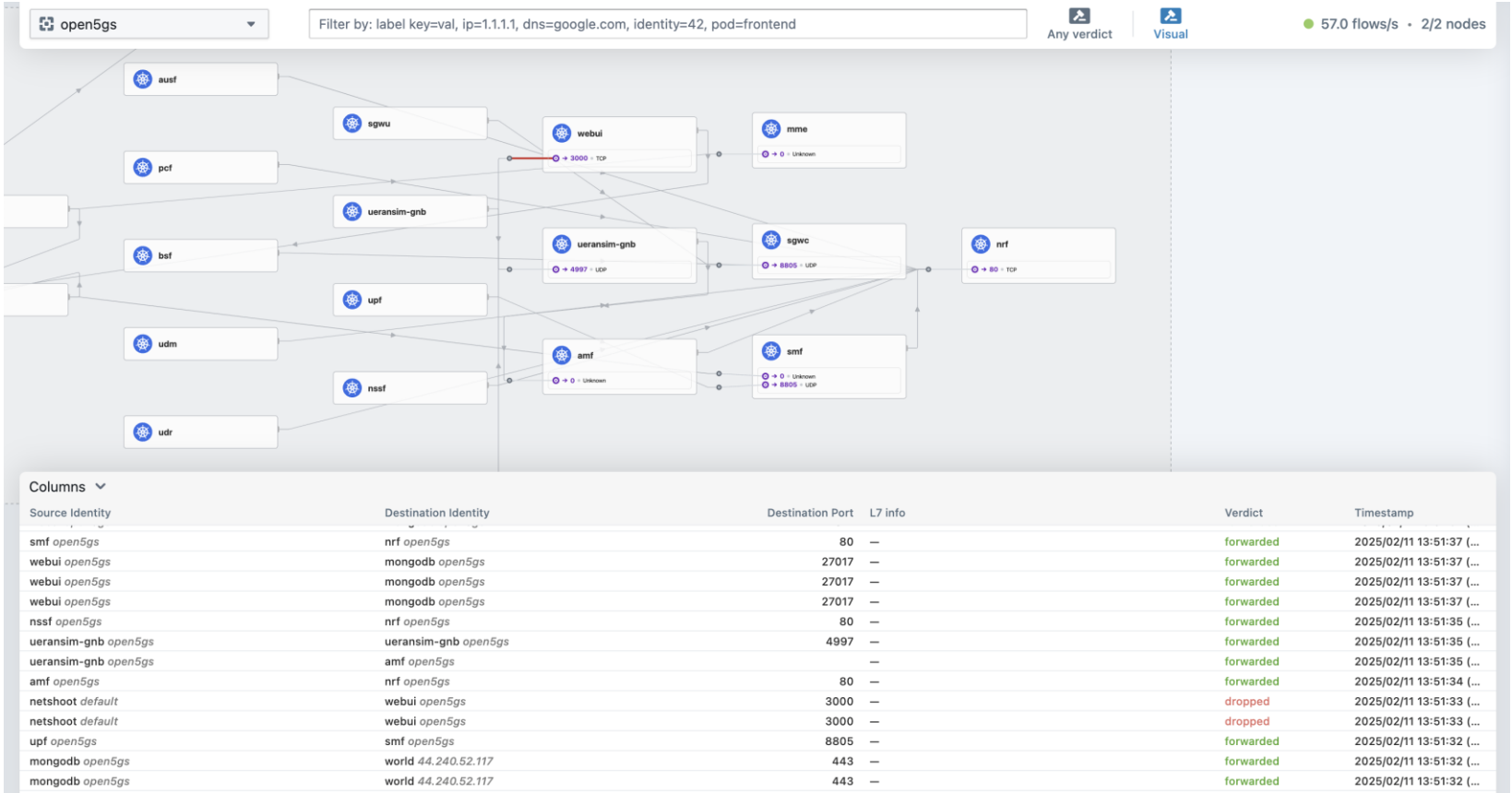
Encryption with cilium: IPSEC & Wireguard



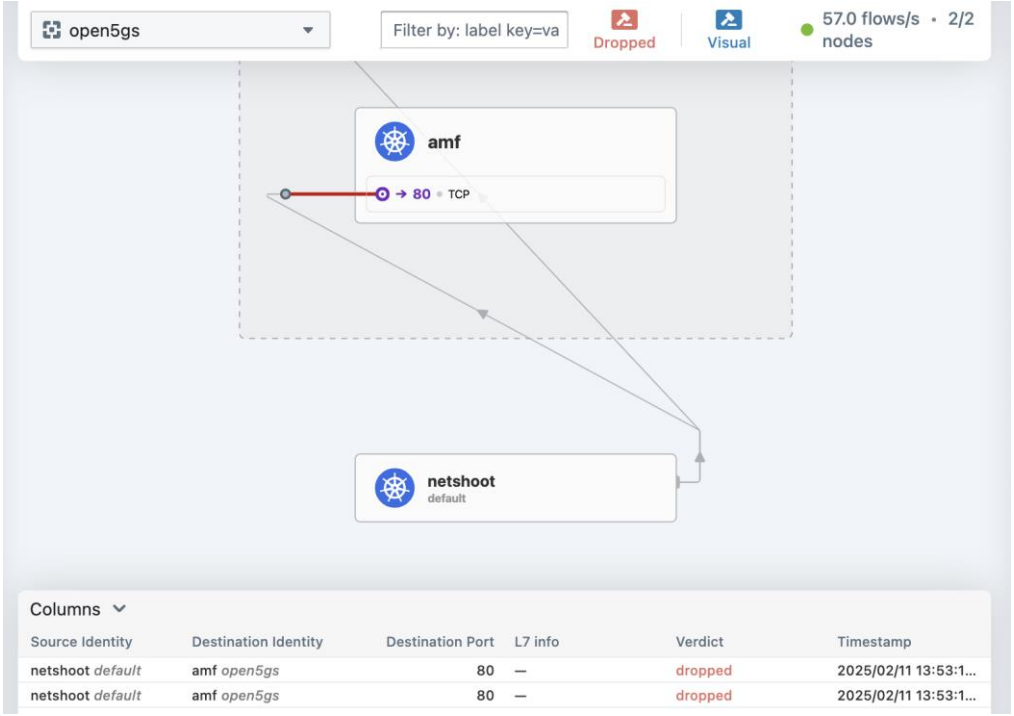



```
$ cilium install --version 1.15.5 --set encryption.enabled=true  -set encryption.type=ipsec
```

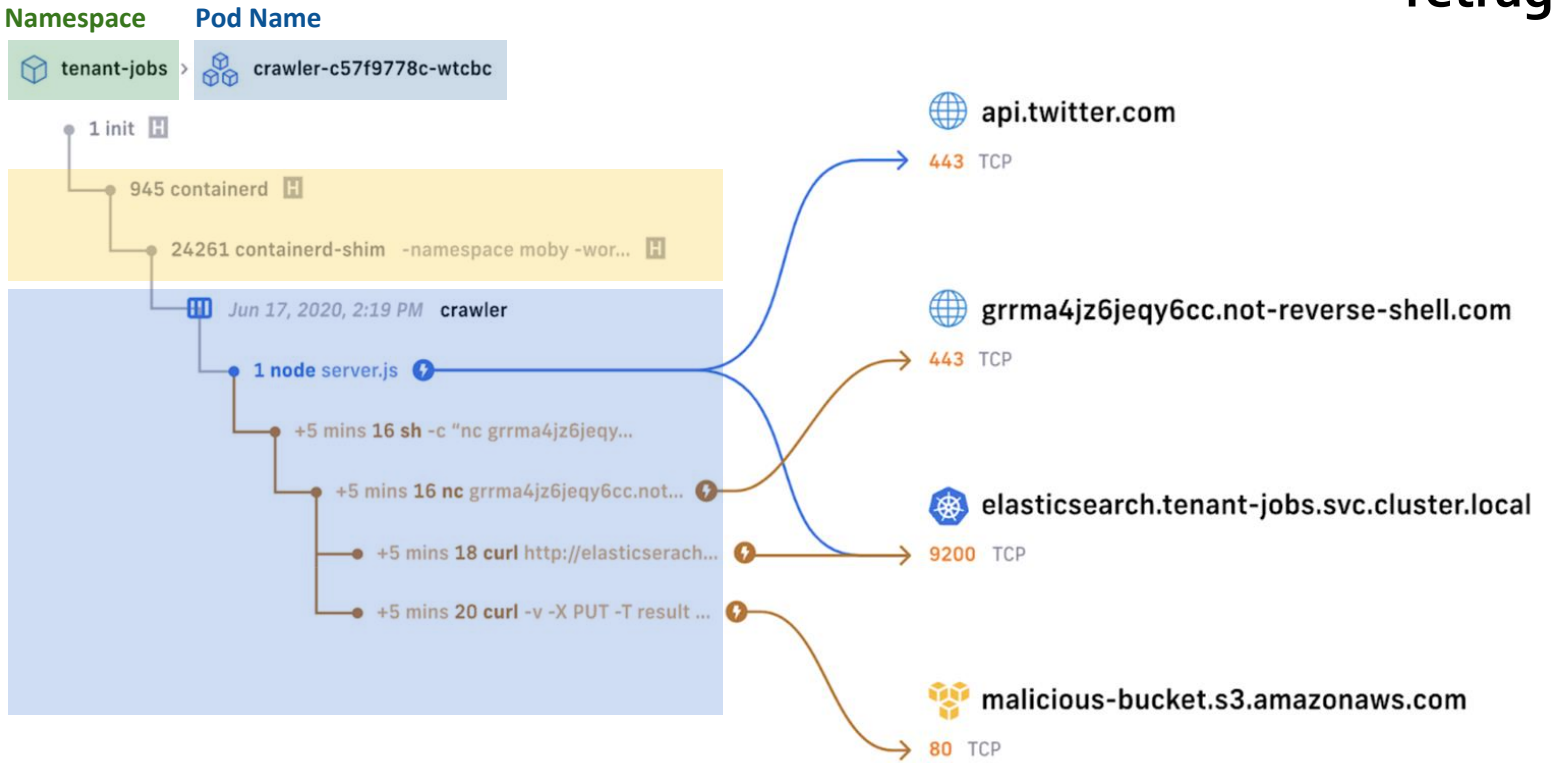
Visualize your traffic with hubble



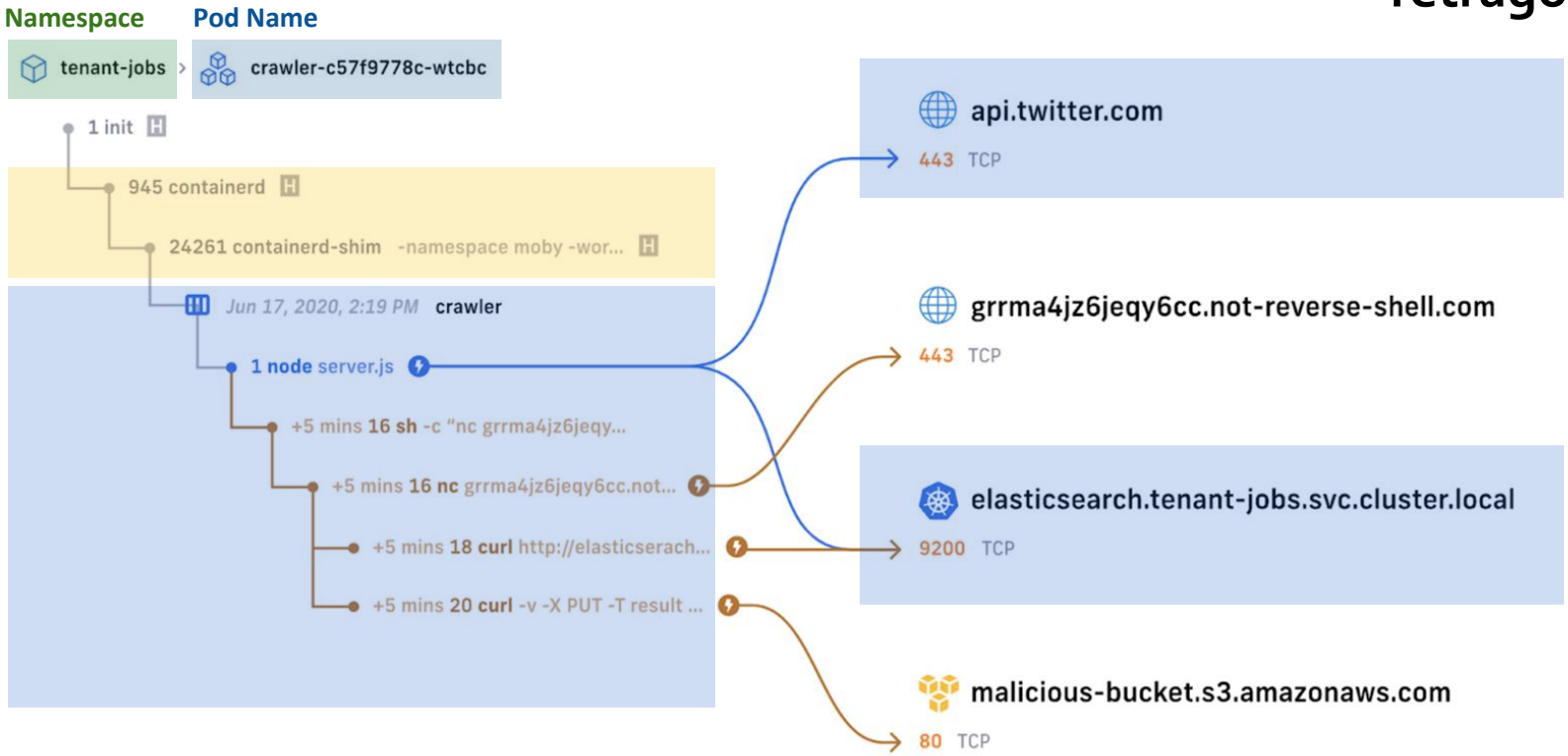
Visualize Blocked traffic with hubble



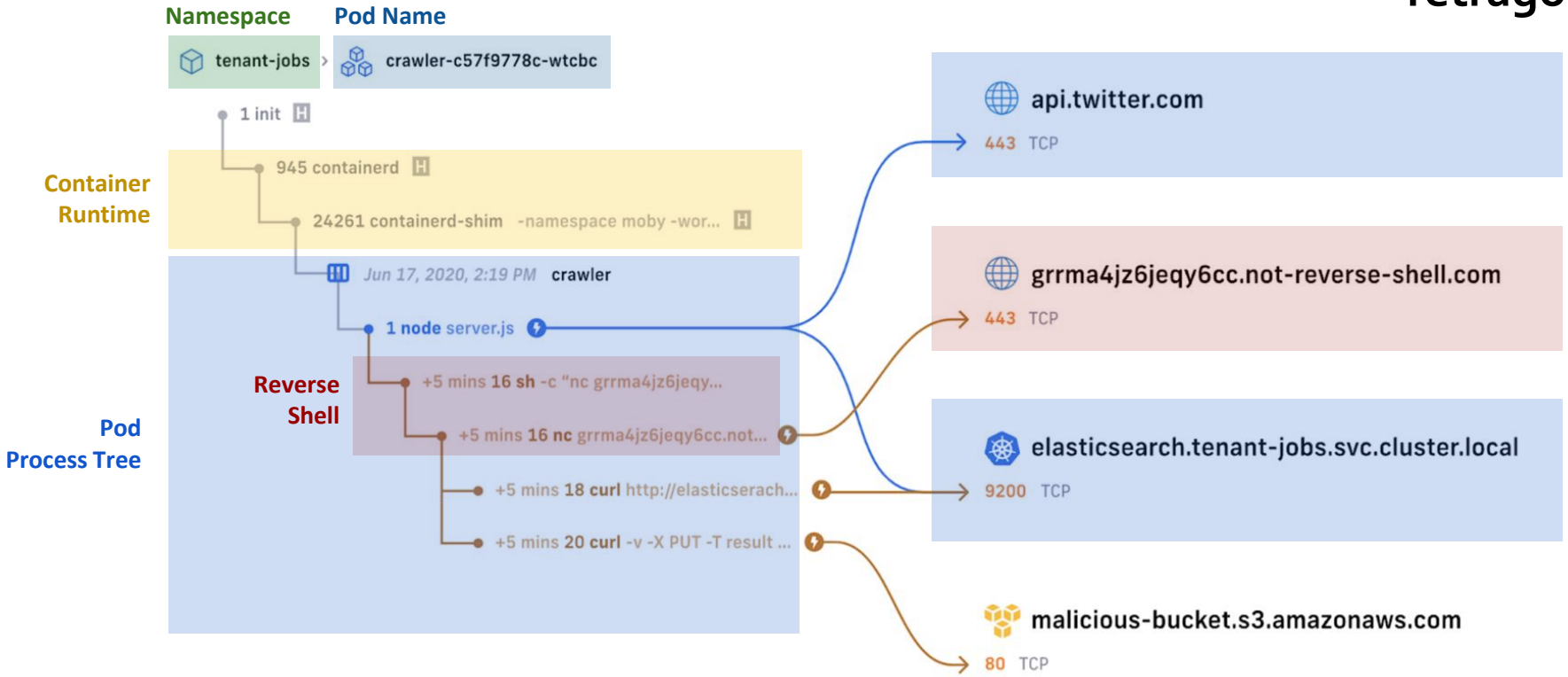
Tetragon in Kubernetes: Deep Visibility & Runtime Security



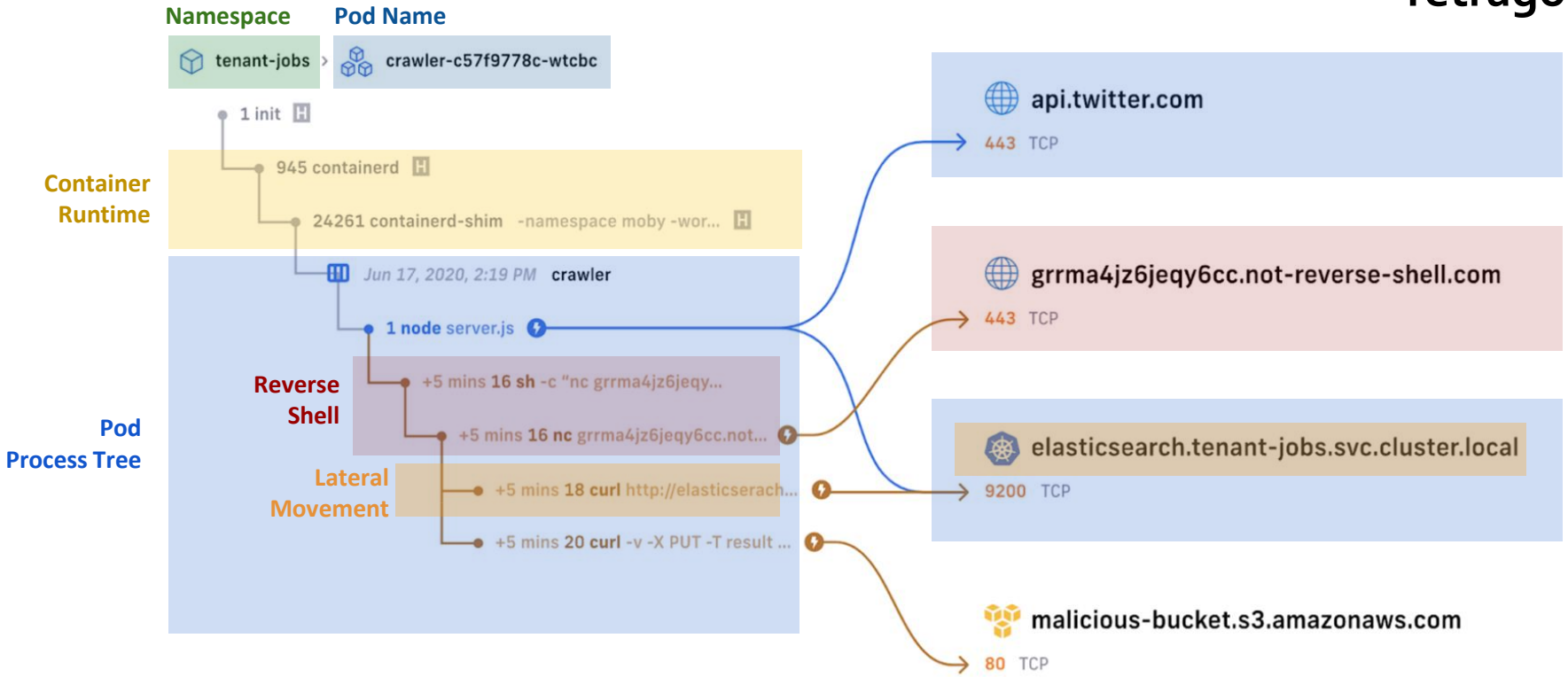
Tetragon in Kubernetes: Deep Visibility & Runtime Security



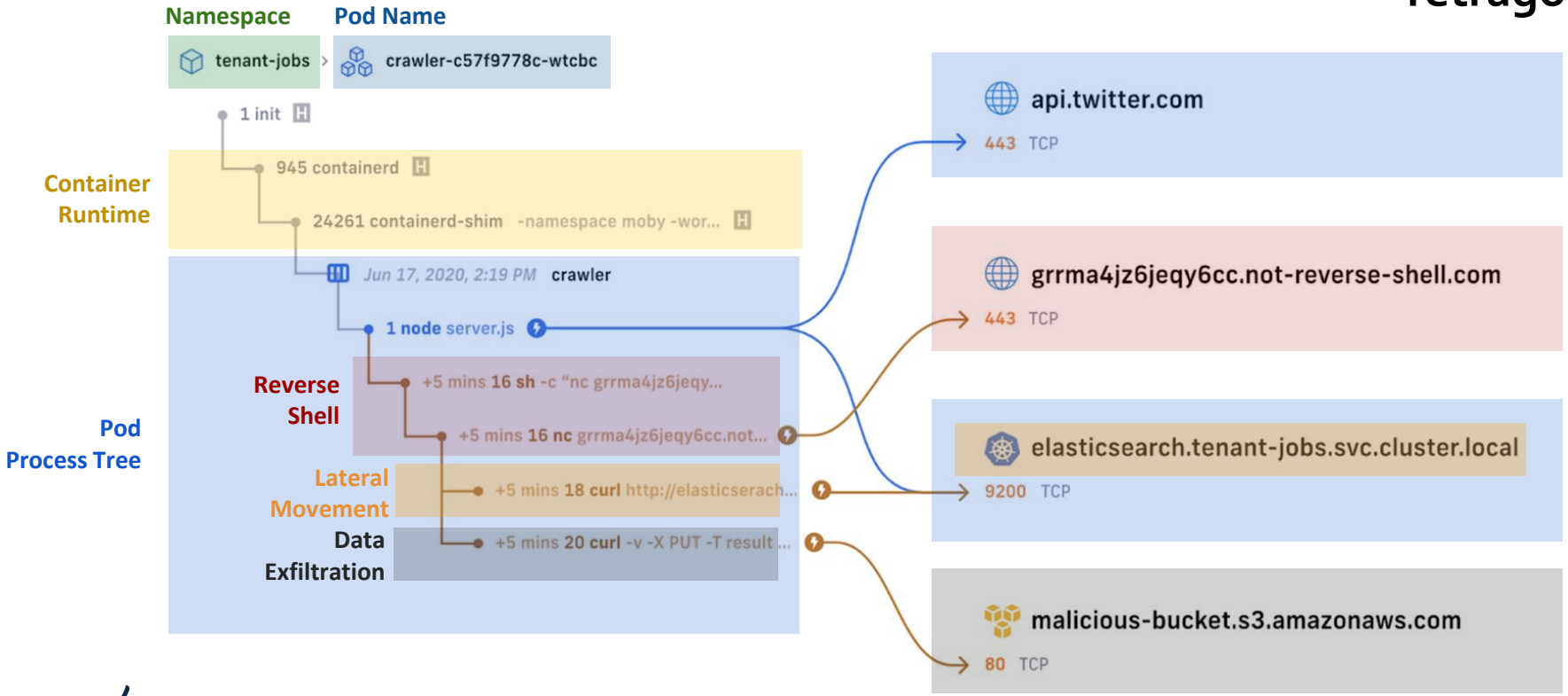
Tetragon in Kubernetes: Deep Visibility & Runtime Security



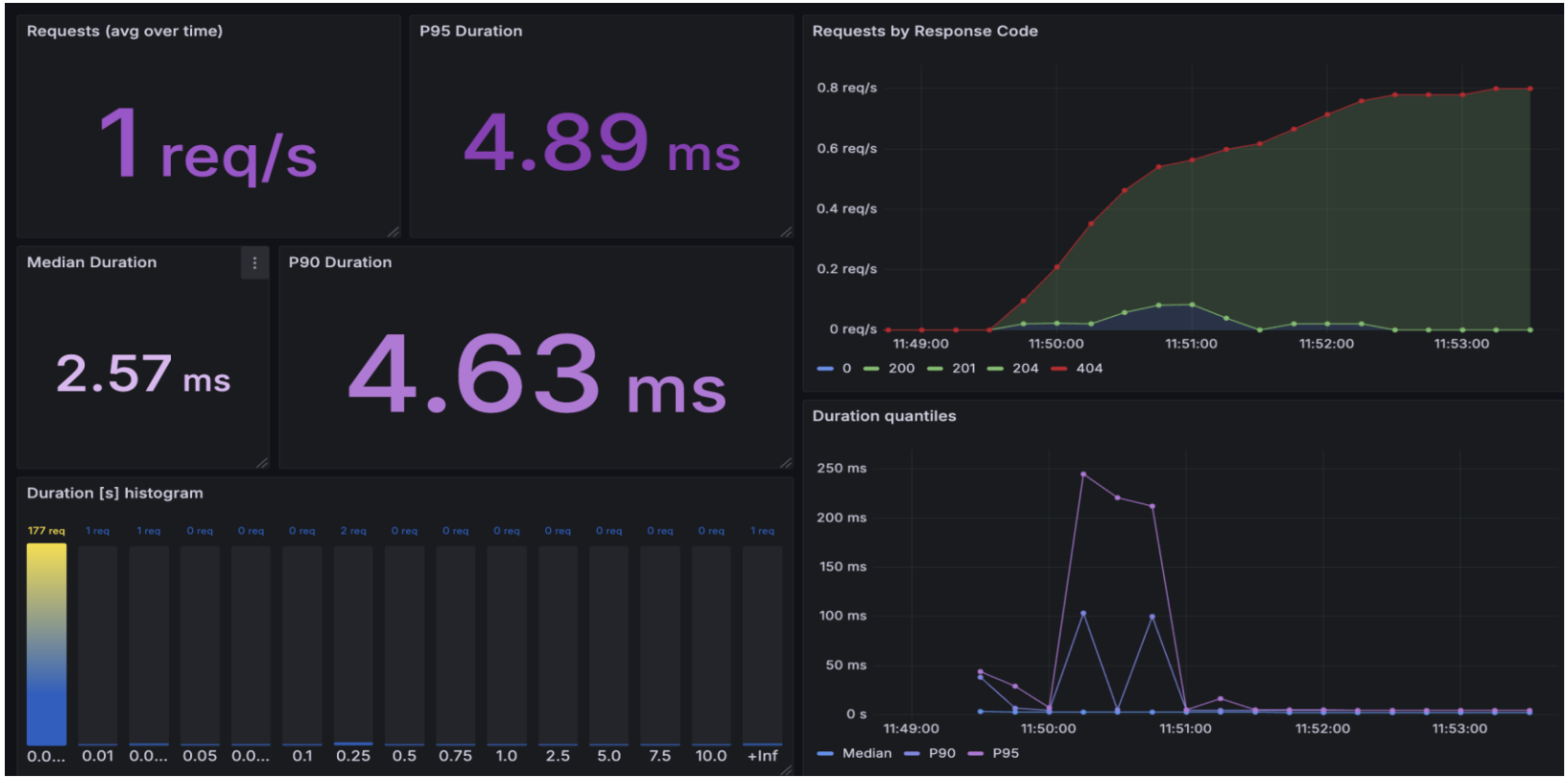
Tetragon in Kubernetes: Deep Visibility & Runtime Security



Tetragon in Kubernetes: Deep Visibility & Runtime Security

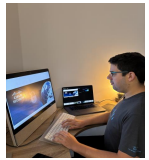


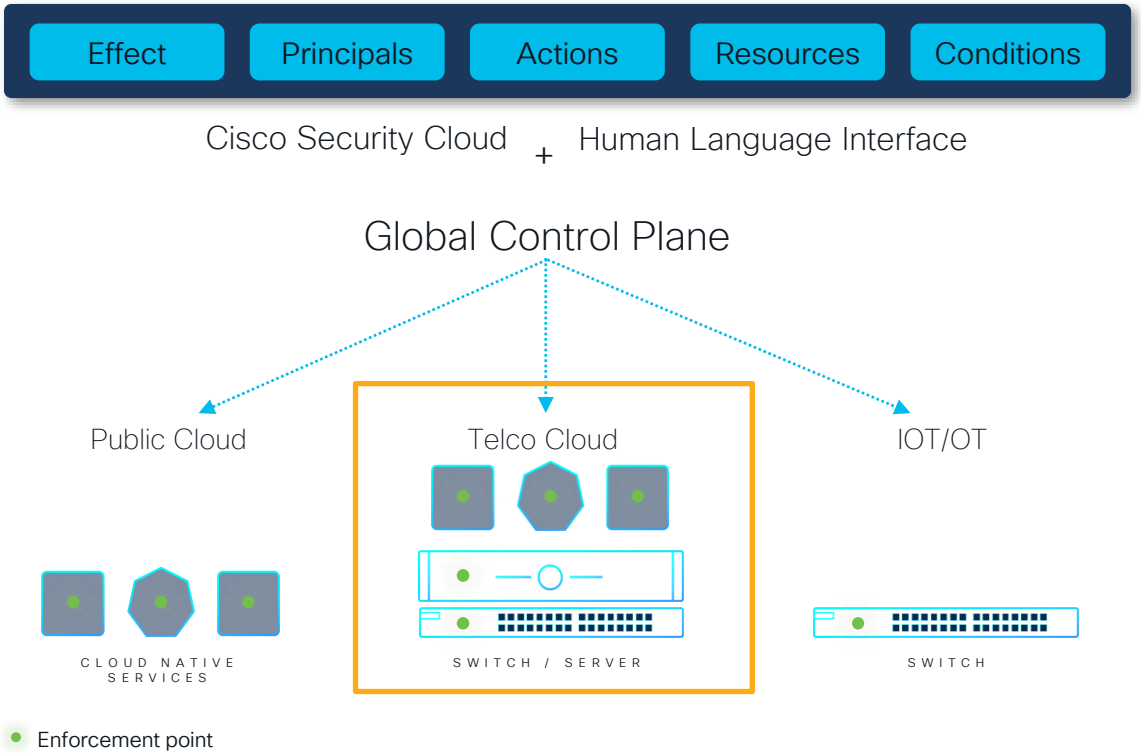
Performance metrics exported to Graphana



Hypershield

Hypershield: Benefits of isovalent products & more...



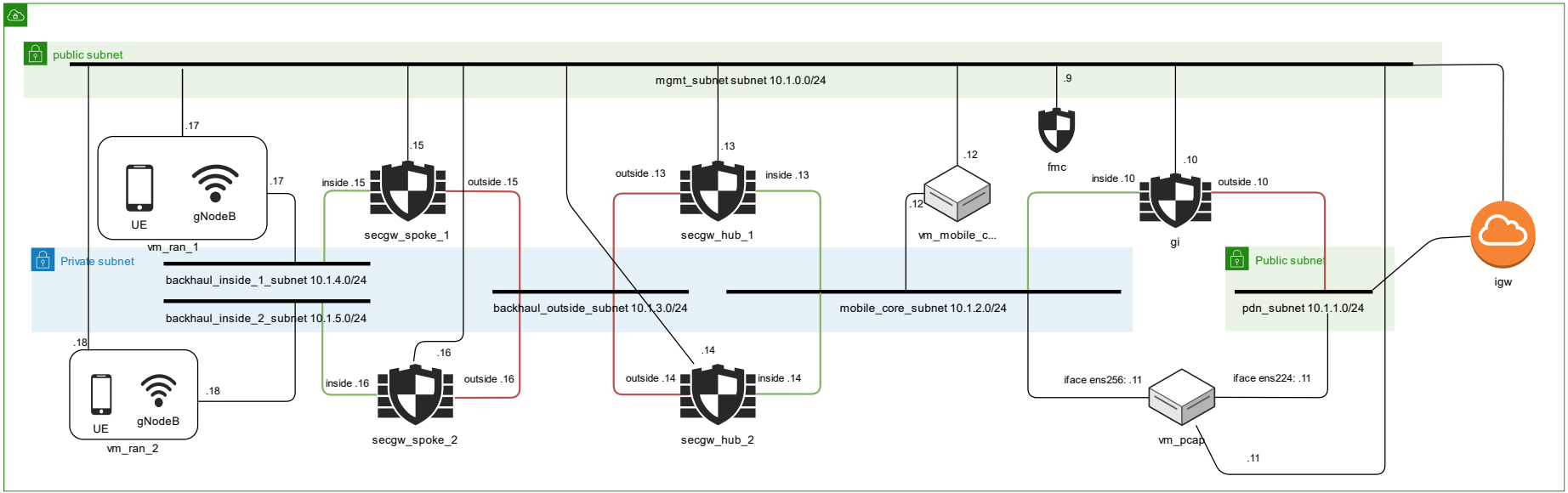


- Unified management
- Single global policy
- Different enforcement points
- Kernel level enforcement (based on isovalent)
- Autonomous segmentation
- Distributed exploit protection

That’s a wrap!

cisco Live!

Get your hands Dirty !



Lab Technologies

- Security Gateway
- GI Firewall
- Cloud-Native Security

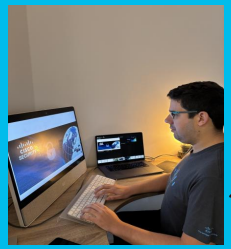
- EVE
- eBPF

- Secure Firewall
- Tetragon
- Cilium
- Hubble

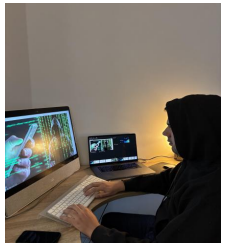
Key Takeaways

- Deploy Security Gateways whenever possible
- Encrypted traffic on the N6 interface is a security risk
- eBPF makes life easier for segmentation, visibility & enforcement

Game Over



So, what do you think Dear 5G_Hacker ? Hein ?



Well.. I should admit you're too strong… white flag..

for now..

Complete your Session Survey

Before leaving the room please share your feedback on this session!

- If you want to see a new round of this battle !
- It is very important for me personally and … … based on previous feedback, I included new attacks and changed a lot of content

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

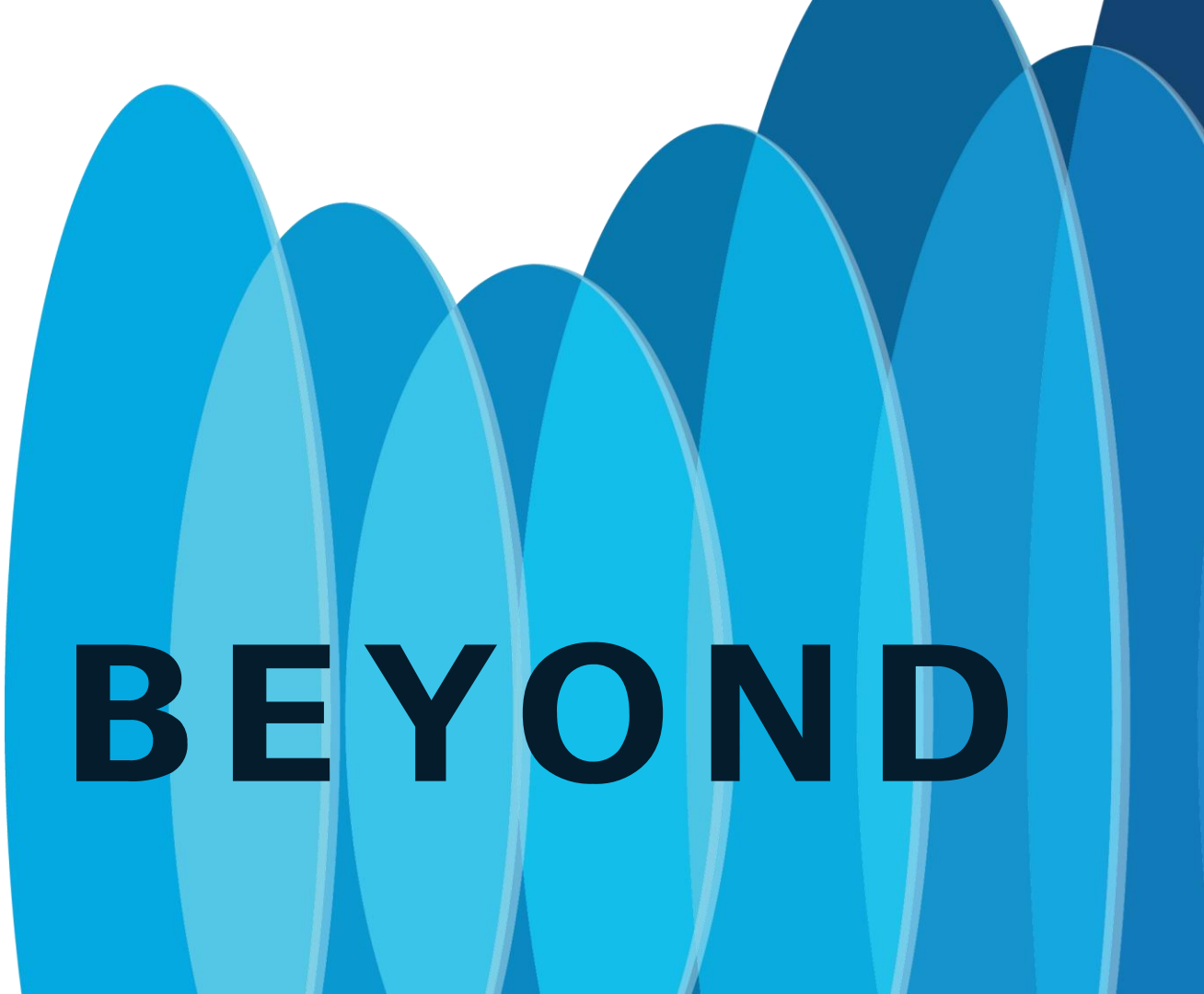
Continue your education

- 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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Thank you

cisco Live!

cisco Live!



GO BEYOND