

High-Speed Packet Processing & Programmable DDOS filtering

Ta Ngoc Huy Phuong

Agenda

Realities of DDoS Attacks

HPE Integral Security with Corero SmartWall One

HPE Advanced Silicon Product

Customer References



Realities of DDoS Attacks – 2025



5%
increase daily attacks

86%
of attack
< 10 minutes

13%
Increase in multi-vector
attacks
60 sec vector changes

The Hacker News [Subscribe – Get Latest News](#)

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Expert Insights Contact

AppOmni Don't Be the Next SaaS Breach
Protect Salesforce from UNC6395-style attacks. [Secure It Now](#)

Cloudflare Blocks Record-Breaking 11.5 Tbps DDoS Attack

Sep 03, 2025 Ravie Lakshmanan Threat Intelligence / Network Security

WIZ

“Cloudflare's defenses have been working overtime. Over the past few weeks, we've autonomously blocked hundreds of hyper-volumetric DDoS attacks, with the largest reaching peaks of 5.1 Bpps and 11.5 Tbps. The 11.5 Tbps attack was a UDP flood that mainly came from Google Cloud.... pic.twitter.com/3rOys7cfGS”

AISURU is linked to some of the largest DDoS attacks recorded, frequently leveraging extremely high-rate UDP floods.

- 22.2 Tbps DDoS Attack (Record-Breaking):** Cloudflare mitigated an attack that peaked at a record-breaking 22.2 terabits per second (Tbps) and 10.6 billion packets per second (Bpps) in September 2025. While Cloudflare did not share details about this specific attack, AISURU has been active in setting new records.
- 15.72 Tbps DDoS Attack on Azure:** On October 24, 2025, Azure DDoS Protection neutralized a multi-vector attack measuring 15.72 Tbps and nearly 3.64 billion packets per second (bpps), which was the largest DDoS attack ever observed in the cloud and targeted a single endpoint in Australia. This attack originated from the Aisuru botnet.
- 11.5 Tbps DDoS Attack:** Cloudflare mitigated a massive 11.5 Tbps and 5.1 Bpps attack in September 2025. XLab research attributed this attack to the Aisuru botnet.

Source:
2025 Corero DDoS Threat Intelligence Report - <https://www.corero.com/threat/>
<https://thehackernews.com/2025/09/cloudflare-blocks-record-breaking-115.html>
<https://unwire.pro/2025/09/03/cloudflare-blocks-record-breaking-11-5-tbps-ddos/security/>
<https://techcommunity.microsoft.com/blog/azureinfrastructureblog/defending-the-cloud-azure-neutralized-a-record-breaking-15-tbps-ddos-attack/4470422>

Realities of DDoS Attacks – 2026



BY THE NUMBERS

Thirty seconds. The headlines.
Everything else is in the pages that follow.

262%

Year-over-year increase in peak attack sizes

2.7 Tbps

Largest observed
peak attack
volume in 2025

50+

Unique attack
vector combinations
in a single campaign

12.3 per
day

Average DDoS attacks per customer in 2025,
the sharpest annual rise in a decade

1.3 BILLION

Packets per second in a single TCP SYN event, February 2026

:06
seconds

Shortest observed attack
wave in pulse campaigns

90.9
percent

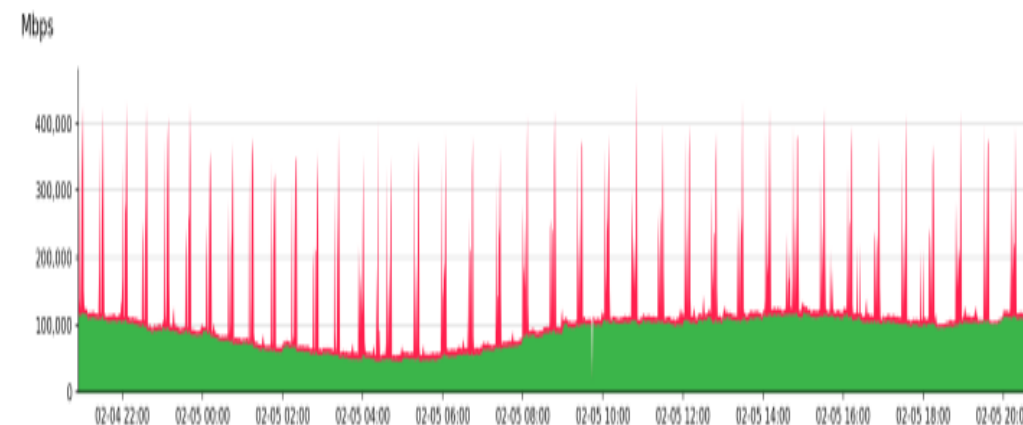
Attacks now lasting less than
10 minutes, up from 80.7% in 2021

56
percent

Sub-1G attacks under 200 Mbps,
small enough to be invisible on
most dashboards

30.5
percent

Attacks followed by a repeat
within seven days



Need a solution which is real-time, high scale and cost-effective

Cost of Damaging DDoS Attacks



Cost of Damaging DDoS Attacks in 2025: Annual Trends Report

Alongside the holiday spirit and festive decorations, this season has been marked by a series of high-profile DDoS attacks that made the headlines. Some of the more striking examples that took place around New Year's Day included:

- **Japan's largest telco NTT Docomo disrupted by DDoS attack** – 90+ million subscribers lost access to their website, news platforms, and mobile payment systems.
- **Ukraine's intelligence disrupts Lukoil services with cyberattack** – Lukoil customers could not make payments at gas stations via the mobile application.
- **Internet sites of several French cities hit by cyber attacks** – Hackers used DDoS attacks to protest French support for Ukraine.
- **Mizuho Bank and Resona Bank may have been hit by cyberattack** – Two of the largest banks in Japan were hit, impacting the availability of online banking services.
- **NIPOST's website down, suffers DDoS attack** – The Nigerian Postal Service's site was down.



GTT EDITORIAL TEAM

The GTT editorial team is comprised of technology experts from product, marketing and development. Our mission is to create quality content and thought leadership for all levels of technology readers with an interest in networking, security, and telecom services.

Distributed Denial of Service (DDoS) attacks continue to pose a significant threat to organizations worldwide, with a notable increase in frequency and sophistication from January 2025 to March 2025. During this period, the number of DDoS attacks surged by **137% compared to the previous year**. On average, each DDoS attack costs a company approximately **\$1.1 million USD**, underscoring the substantial financial impact these incidents can have. Cybercriminals are becoming increasingly bold, targeting organizations of all sizes and across various industries. They are leveraging advanced tools such as artificial intelligence (AI), machine learning (ML), and automation, **which are also used by organizations to defend against these threats**. To mitigate the risks associated with DDoS attacks, **it is crucial for organizations to implement robust security measures** including **continuous network monitoring, adaptive threat detection and scalable DDoS mitigation strategies**.

corero

[NETWORK SECURITY]

Error fetching data.

SPEAK WITH A SPECIALIST

PRODUCTS ▾ SOLUTIONS ▾ SERVICES RESOURCES ▾ PARTNERS ▾ INVESTORS ▾ ABOUT ▾ SUPPORT

Loss of Revenue

Perhaps the most obvious and recognized impact of a DDoS attack is the loss of revenue resulting from disrupted online services or e-commerce transactions. During an attack, businesses may experience downtime, leading to missed sales opportunities, reduced customer engagement, and tarnished brand reputation (see #2). Research suggests that the average cost of a DDoS attack for businesses can range from thousands to **hundreds of thousands of dollars per hour**, depending on the industry and scale of the attack.

Damage to Brand Reputation

DDoS attacks can severely damage a company's brand reputation and erode customer trust and loyalty, which will ultimately cause long-term damage to a company's bottom line that extends far beyond the duration of the DDoS attack.

Customers may perceive prolonged service disruptions as a sign of incompetence or negligence on the part of the business, leading to customer churn and negative word-of-mouth publicity. Rebuilding trust and repairing brand reputation in the aftermath of a DDoS attack can be a challenging and time-consuming process, impacting long-term profitability and competitiveness. PR firms cost a lot of money, especially when you are in a time of crisis and in urgent need of their services.

Operational Disruption

Beyond financial losses, DDoS attacks can disrupt critical business operations, including communication systems, supply chain management, and employee productivity. IT teams are often forced to divert resources and manpower to mitigate the attack, leading to increased operational costs and decreased efficiency in other areas of the business. Extended downtime can also result in missed deadlines, delayed projects, and contractual penalties, further exacerbating the impact on business operations.

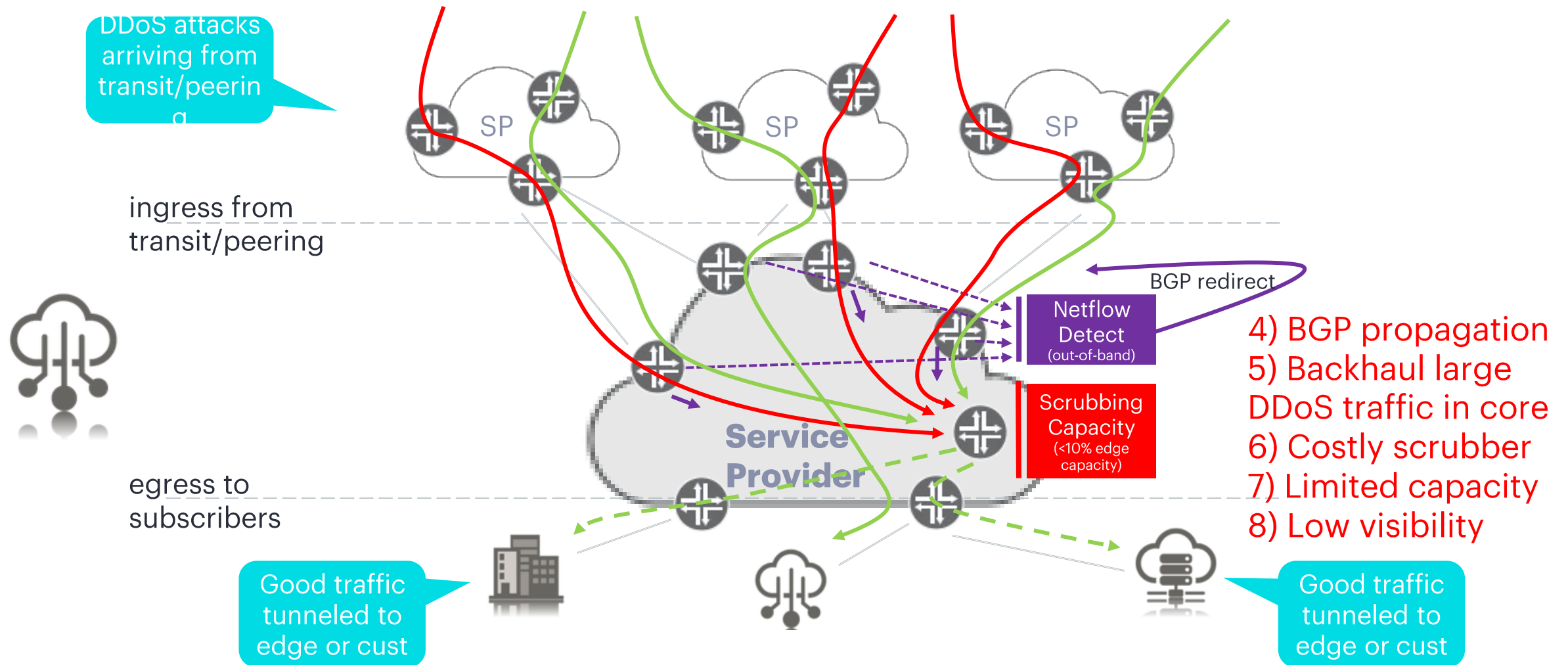
Legal and Regulatory Ramifications

DDoS attacks may expose businesses to legal and regulatory liabilities, particularly if sensitive customer data is compromised or if the attack violates industry-specific compliance standards (e.g., GDPR, HIPAA). Organizations may face lawsuits, fines, or regulatory sanctions for failing to protect customer data or maintain adequate cybersecurity measures. Compliance failures and data breaches resulting from DDoS attacks can also tarnish a company's reputation and undermine investor confidence, leading to long-term financial repercussions.

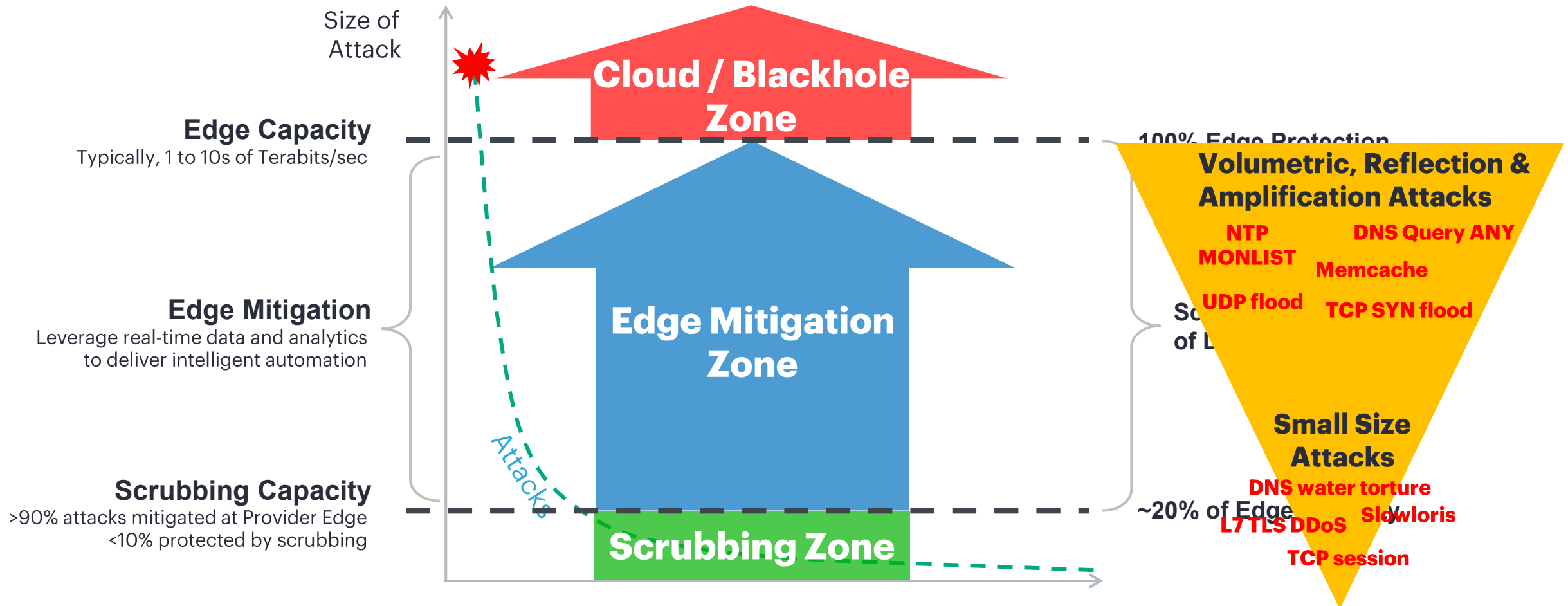
Stopping DDoS attacks in real time starts here—
ready to see how?
Powered by AI

https://mazedbolt.com/blog/cost-of-damaging-ddos-attacks-in-2025-annual-trends-report?utm_source=substack&utm_medium=email
<https://www.gtt.net/us-en/resources/blog/navigating-the-surge-effective-strategies-for-ddos-mitigation-in-2025-and-beyond/>

Problems of legacy 'detect and redirect' solution (cont)



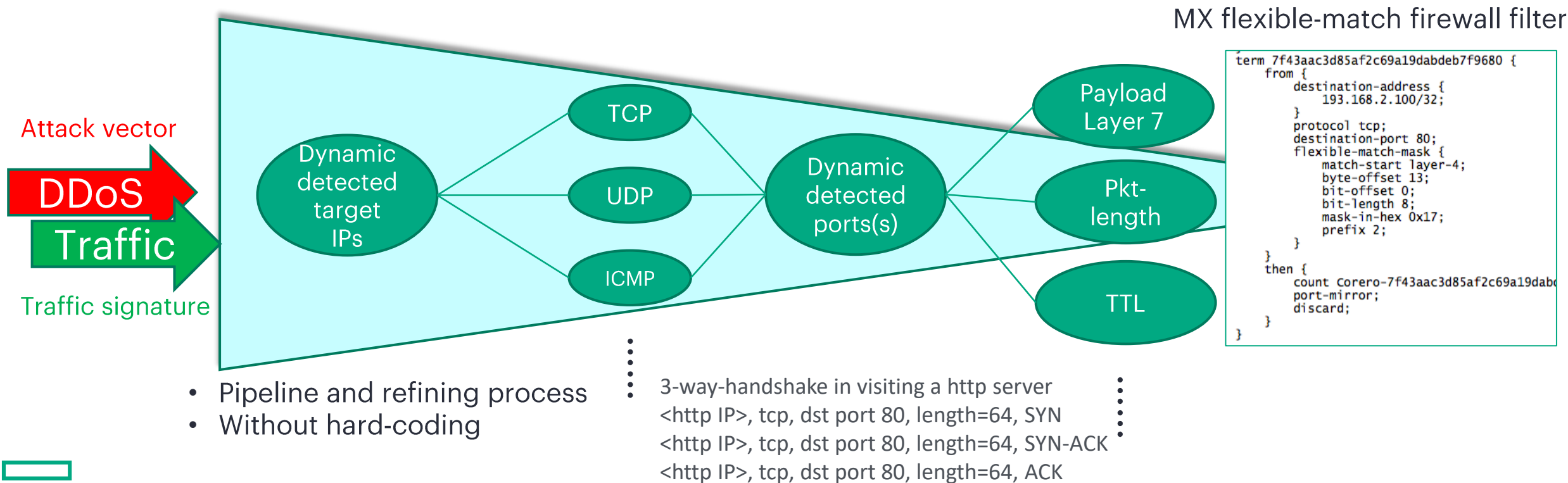
Scrubbing vs Attack Size & Network Capacity



Inspection Pipeline

Fully dynamic and programmatic detection without the need of signature update. The basic principle is as follow:

Traffic signature (pattern) = (1) destination IP + (2) protocol + (3) port + (4) payload + ...

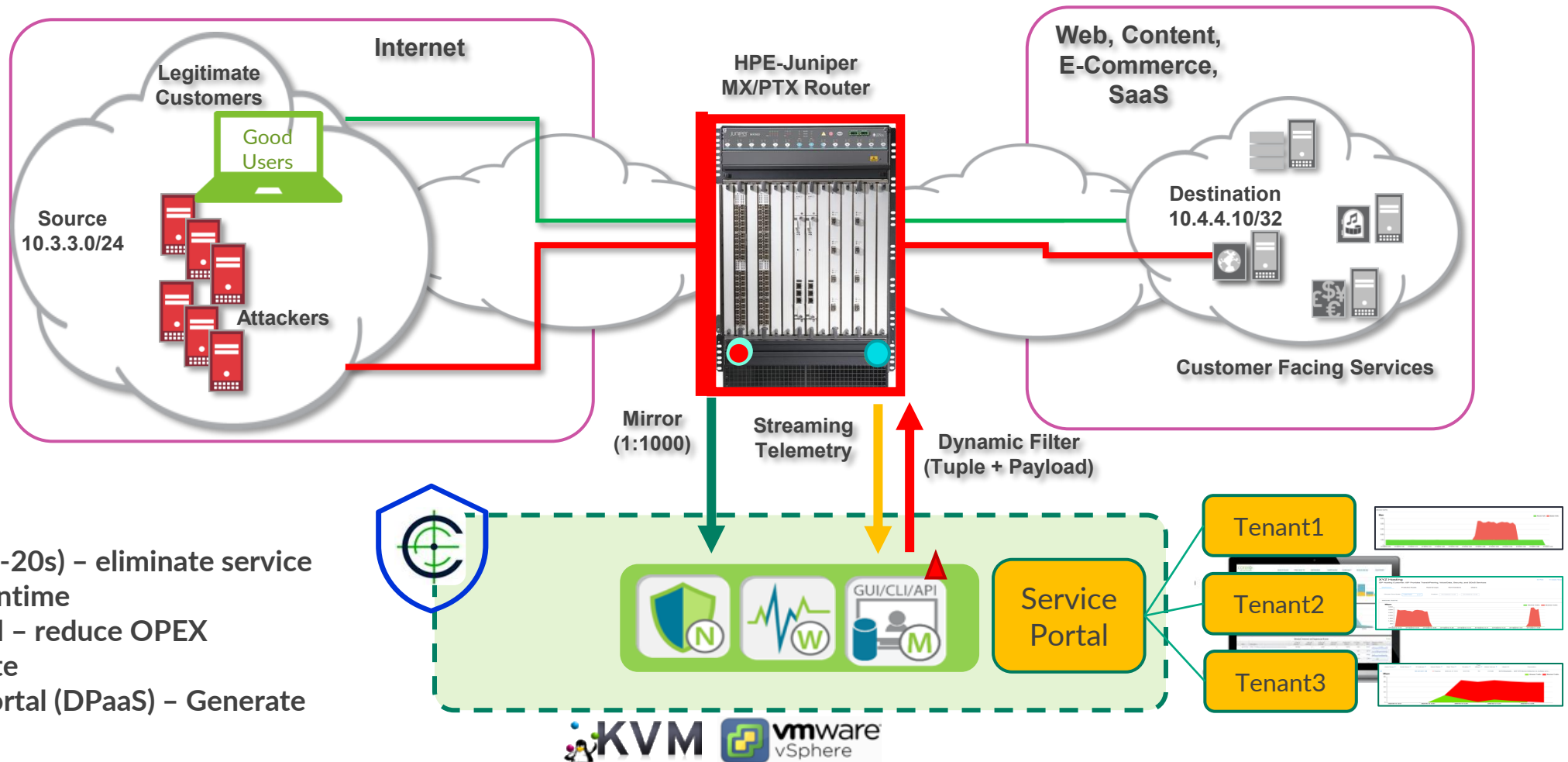


HPE Integral Security with Corero SmartWall One



SmartWall One (SWO) – Remote Mitigation Deployment

Fully Automated Anti-DDoS Solution



SWO benefits

1. Real-Time (~15s-20s) – eliminate service impact and downtime
2. Fully-automated – reduce OPEX
3. Simple to operate
4. Multitenancy Portal (DPaaS) – Generate revenue

Enhanced Accuracy + Speed of DDoS Detection/Mitigation

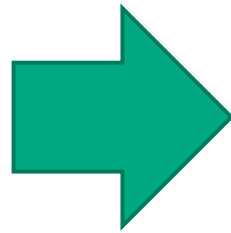
Netflow

- aggregation delay
- header only
- attack overload

Flowspec/RTBH

- BGP propagation
- header only
- limited visibility

Legacy

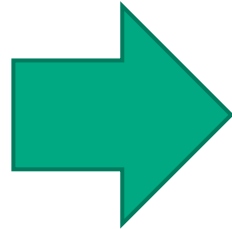


Sampled Mirror

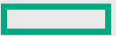
- immediate forwarding
- header and payload
- scales with attack

Firewall Filter

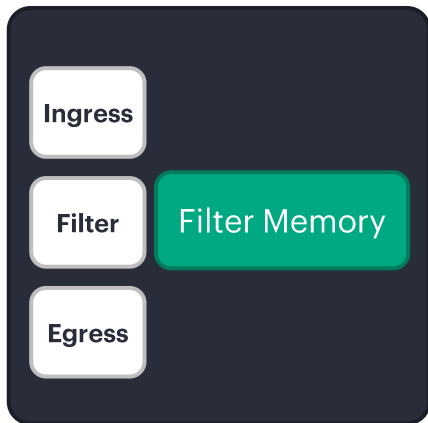
- Advanced silicon w/ flexible-match lookup
- header and payload
- streaming telemetry



HPE Silicon Advantages

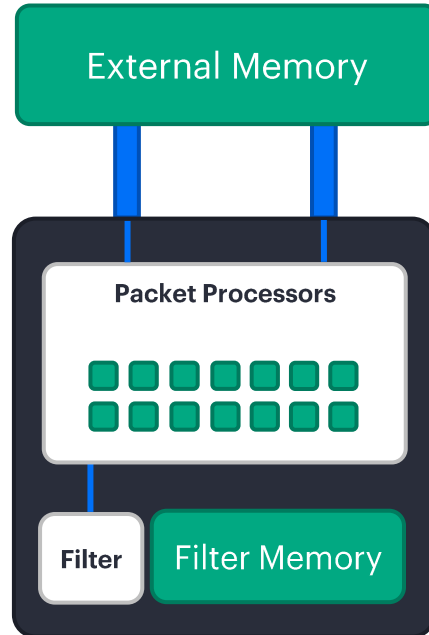


ASICs, Memory and Filter Implementation



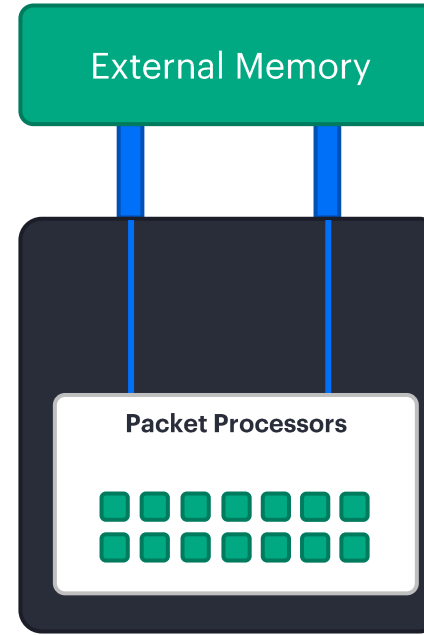
Express

Higher Performance
Limited Scale



Trio [XL and beyond]

Combination of both



Trio (Original)

Moderate Performance
Very Large Scale

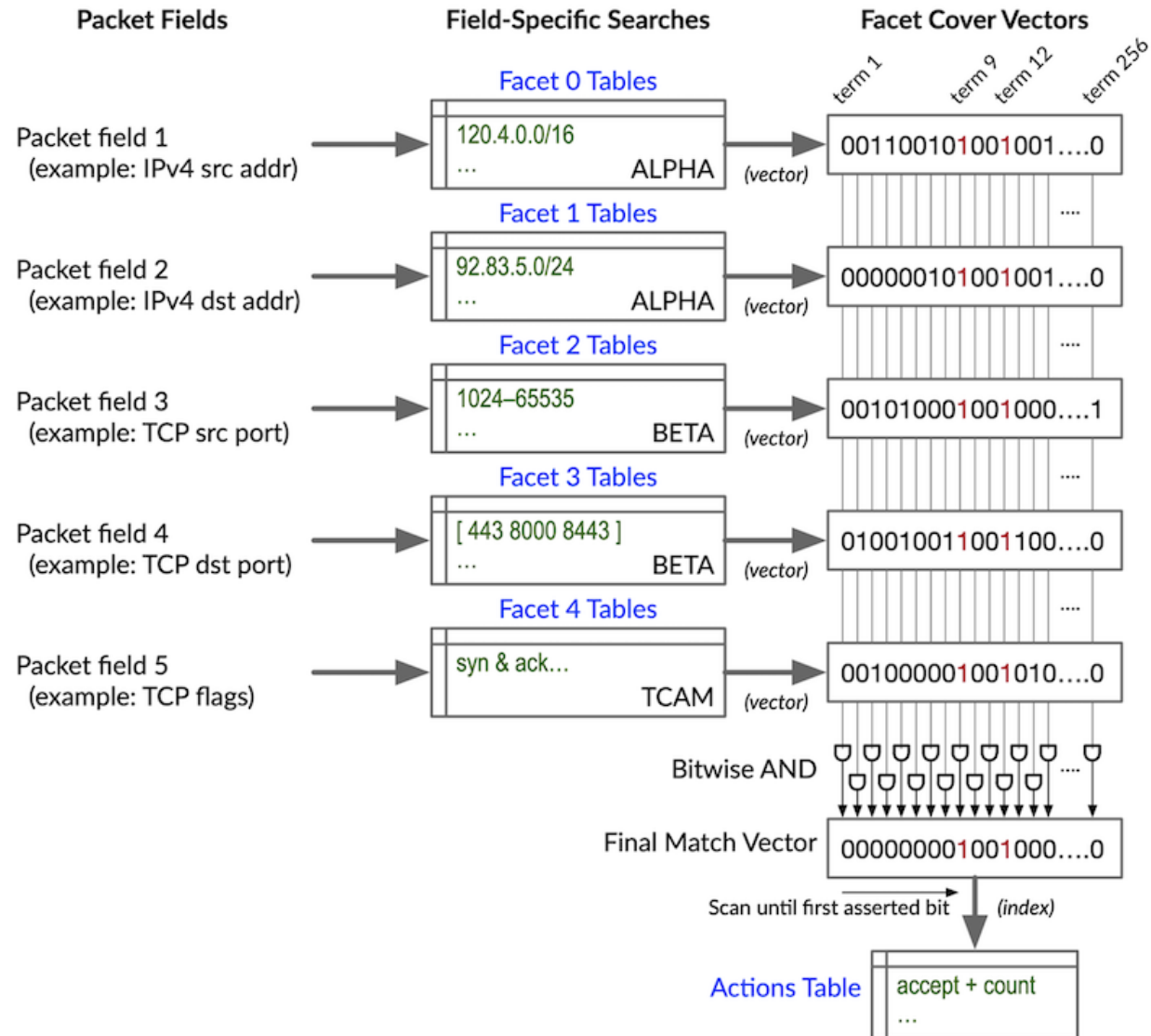
Features

Wider search keys (>320bit)
Range, prefix and exact match
Combinations of the above
Negate matches
Next term action
Count action





PTX ASIC Filter Implementation



**O(1) search time target, TCAM-like
Combination of tree,
hash-table and associative arrays (TCAM)**

Search keys are configured per filter

[Express 4 Filters - Foundation](#)



MX/PTX Firewall Filter Flexible Match

e.g. NTP MONLIST

```
lab@MX10003-2> show ephemeral-configuration instance Corero
## Last changed: 2019-02-14 17:15:25 UKT
firewall {
  family inet {
    filter CORERO-MITIGATE {
      term b003e993f5bbe929ea7cce09b58f5cde {
        from {
          destination-address {
            193.168.1.123/32;
          }
          protocol udp;
          source-port 123;
          flexible-match-mask {
            match-start layer-4;
            byte-offset 11;
            bit-offset 0;
            bit-length 8;
            mask-in-hex 0xFF;
            prefix 42;
          }
        }
        then {
          count Corero-b003e993f5bbe929ea7cce09b58f5cde;
          port-mirror;
          discard;
        }
      }
    }
  }
}
```

Flex match:

start from layer 4 (UDP)

Byte-offset 11 means the 12th Byte

Match for 8 bits

Mask = 0xFF = 1111 1111 (compare all bits)

Pattern = DEC 42 = HEX 2a

1st byte of UDP

12th byte of UDP

+ Frame 127 (201 bytes on wire, 201 bytes captured)															
+ Ethernet II, Src: JuniperN_bf:d4:b4 (00:1f:12:bf:d4:b4) Dst: Gould_d2:69:8c (00:00:dd:d2:69:8c)															
+ Internet Protocol, Src: 94.211.215.80 (94.211.215.80), Dst: 202.202.202.2 (202.202.202.2)															
+ User Datagram Protocol, Src Port: ntp (123), Dst Port: sdo-tls (3896)															
- Network Time Protocol															
- Flags: 0xef															
1... = Response bit: Response (1)															
.1.. = More bit: 1															
..10 1... = Version number: reserved (5)															
.... .111 = Mode: reserved for private use (7)															
- Auth, sequence: 133															
1... = Auth bit: 1															
.000 0101 = Sequence number: 5															
Implementation: Unknown (209)															
Request Code: MON_GETLIST_1 (42)															
0020	ca	00	00	7b	0f	38	00	a3	4e	4a	ef	85	d1	2a	00
0030	00	00	00	00	00	00	00	00	b1	d7	bd	8c	b5	1d	08
0040	49	78	69	60	20	00	00	04	10	11	12	13	04	e9	df
0050	00	71	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26
0060	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36
0070	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46
0080	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56
0090	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66
00a0	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76
00b0	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86

MX/PTX firewall filter flexible match (cont)

example: TCP SYN ACK FLAG set

```
term 31a178cd4a556f7b75fbbbcfa5877745 {  
  from {  
    destination-address {  
      193.168.4.124/32;  
    }  
    protocol tcp;  
    destination-port 80;  
    flexible-match-mask {  
      match-start layer-4;  
      byte-offset 13;  
      bit-offset 0;  
      bit-length 8;  
      mask-in-hex 0x17;  
      prefix 18;  
    }  
  }  
  then {  
    count Corero-31a178cd4a556f7b75fbbbcfa5877745;  
    port-mirror;  
    discard;  
  }  
}
```

Flex match:

start from layer 4 (TCP)

Byte-offset 13 means the 14th Byte

Match for 8 bits

Mask = 0x17 = 0001 0111 (only to compare the set position)

Pattern = DEC 18 = HEX 12 = 0001 0010

1st byte of TCP

14th byte of TCP

0001 0010

```
# Ethernet II, Src: 20:d8:0b:84:a3:f1 (20:d8:0b:84:a3:f1), Dst: 00:00:78:05:d7:60 (00:00:78:05:d7:60)  
# Internet Protocol Version 4, Src: 80.167.55.85 (80.167.55.85), Dst: 201.201.201.2 (201.201.201.2)  
# Transmission Control Protocol, Src Port: 49877 (49877), Dst Port: 80 (80), Seq: 0, Ack: 0, Len: 0  
  Source port: 49877 (49877)  
  Destination port: 80 (80)  
  [Stream index: 0]  
  Sequence number: 0 (relative sequence number)  
  Acknowledgment number: 0 (relative ack number)  
  Header length: 20 bytes  
  # Flags: 0x012 (SYN, ACK)  
    000. .... = Reserved: Not set  
    ...0 .... = Nonce: Not set  
    .... 0... = Congestion Window Reduced (CWR): Not set  
    .... .0.. = ECN-Echo: Not set  
    .... ..0. = Urgent: Not set  
    .... ...1 = Acknowledgment: Set  
    .... .... 0... = Push: Not set  
    .... .... .0.. = Reset: Not set  
    # .... .... .1. = Syn: Set  
    .... .... .0 = Fin: Not set  
  window size value: 65535  
  [calculated window size: 65535]  
0000  00 00 78 05 d7 60 20 d8 0b 84 a3 f1 08 00 45 00  ..X... ..E.  
0010  00 28 16 78 40 00 3f 06 2a 8f 50 a7 37 55 c9 c9  .(.x@.?.*.P.7U..  
0020  c9 02 c2 05 00 50 5c fa 9c 29 5f 46 83 a6 50 12  .....P\.)_F..P.  
0030  ff ff f5 d3 00 00 00 00 00 00 00 00 da df 00 c1  ....c1
```

MEMCACHED ATTACKS and say “SORRY” TO PHUNUONLINE.COM.VN

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Time to live	Time to live	Info
114	0.000113	212.48.74.97	120.72.100.198	MEMCAC	200	11211	45571	55	55	MEMCACHE Continuation
115	0.000114	222.168.27.117	120.72.100.198	MEMCAC	200	11211	53976	114	114	MEMCACHE Continuation
116	0.000115	223.84.214.223	120.72.100.198	MEMCAC	200	11211	8090	115	115	MEMCACHE Continuation
117	0.000116	186.67.61.246	120.72.100.198	MEMCAC	200	11211	5717	114	114	MEMCACHE Continuation
118	0.000117	120.77.23.112	120.72.100.198	MEMCAC	200	11211	3496	46	46	MEMCACHE Continuation
119	0.000118	223.84.214.223	120.72.100.198	MEMCAC	200	11211	11252	113	113	MEMCACHE Continuation
120	0.000119	61.41.79.50	120.72.100.198	MEMCAC	200	11211	30792	116	116	MEMCACHE Continuation
121	0.000120	212.48.74.97	120.72.100.198	MEMCAC	200	11211	26123	55	55	MEMCACHE Continuation
122	0.000121	120.25.157.186	120.72.100.198	MEMCAC	60	11211	59013	111	111	MEMCACHE Continuation
123	0.000122	61.41.79.50	120.72.100.198	MEMCAC	200	11211	36095	115	115	MEMCACHE Continuation
124	0.000123	113.53.228.43	120.72.100.198	MEMCAC	60	11211	24972	55	55	MEMCACHE Continuation
125	0.000124	140.238.182.138	120.72.100.198	MEMCAC	66	11211	48508	57	57	MEMCACHE Continuation
126	0.000125	116.62.224.169	120.72.100.198	MEMCAC	60	11211	40643	47	47	MEMCACHE Continuation
127	0.000126	125.77.26.138	120.72.100.198	MEMCAC	200	11211	64713	52	52	MEMCACHE Continuation
128	0.000127	61.41.79.50	120.72.100.198	MEMCAC	200	11211	13814	116	116	MEMCACHE Continuation
129	0.000128	186.67.61.246	120.72.100.198	MEMCAC	200	11211	1750	113	113	MEMCACHE Continuation
130	0.000129	218.201.154.106	120.72.100.198	MEMCAC	200	11211	20801	113	113	MEMCACHE Continuation
131	0.000130	186.67.61.246	120.72.100.198	MEMCAC	200	11211	1750	113	113	MEMCACHE Continuation
132	0.000131	218.201.154.106	120.72.100.198	MEMCAC	200	11211	4456	112	112	MEMCACHE Continuation
133	0.000132	61.41.79.50	120.72.100.198	MEMCAC	200	11211	25023	115	115	MEMCACHE Continuation
134	0.000133	61.41.79.50	120.72.100.198	MEMCAC	200	11211	25023	115	115	MEMCACHE Continuation

<

▶ Frame 132: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface unknown, id 0

▶ Ethernet II, Src: JuniperN_fe:f0:b0 (f4:b5:2f:fe:f0:b0), Dst: VMware_a7:62:85 (00:50:56:a7:62:85)

▶ Internet Protocol Version 4, Src: 218.201.154.106, Dst: 120.72.100.198

▶ User Datagram Protocol, Src Port: 11211, Dst Port: 4456

Memcache Protocol

0000 00 50 56 a7 62 85 f4 b5 2f fe f0 b0 08 00 45 20 PV·b··· /·····E

0010 05 94 25 d8 40 00 70 11 8d 1e da c9 9a 6a 78 48 ··%@p·····ixH

0020 64 c6 2b cb 11 68 05 80 05 47 00 01 06 f0 08 d4 d···h··· ·G·····

0030 00 00 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 SorryS orrySorr

0040 79 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 ySorrySo rrySorry

0050 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 SorrySor rySorryS

0060 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 6f orrySorr ySorrySo

0070 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 rrySorry SorrySor

0080 72 79 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 rySorryS orrySorr

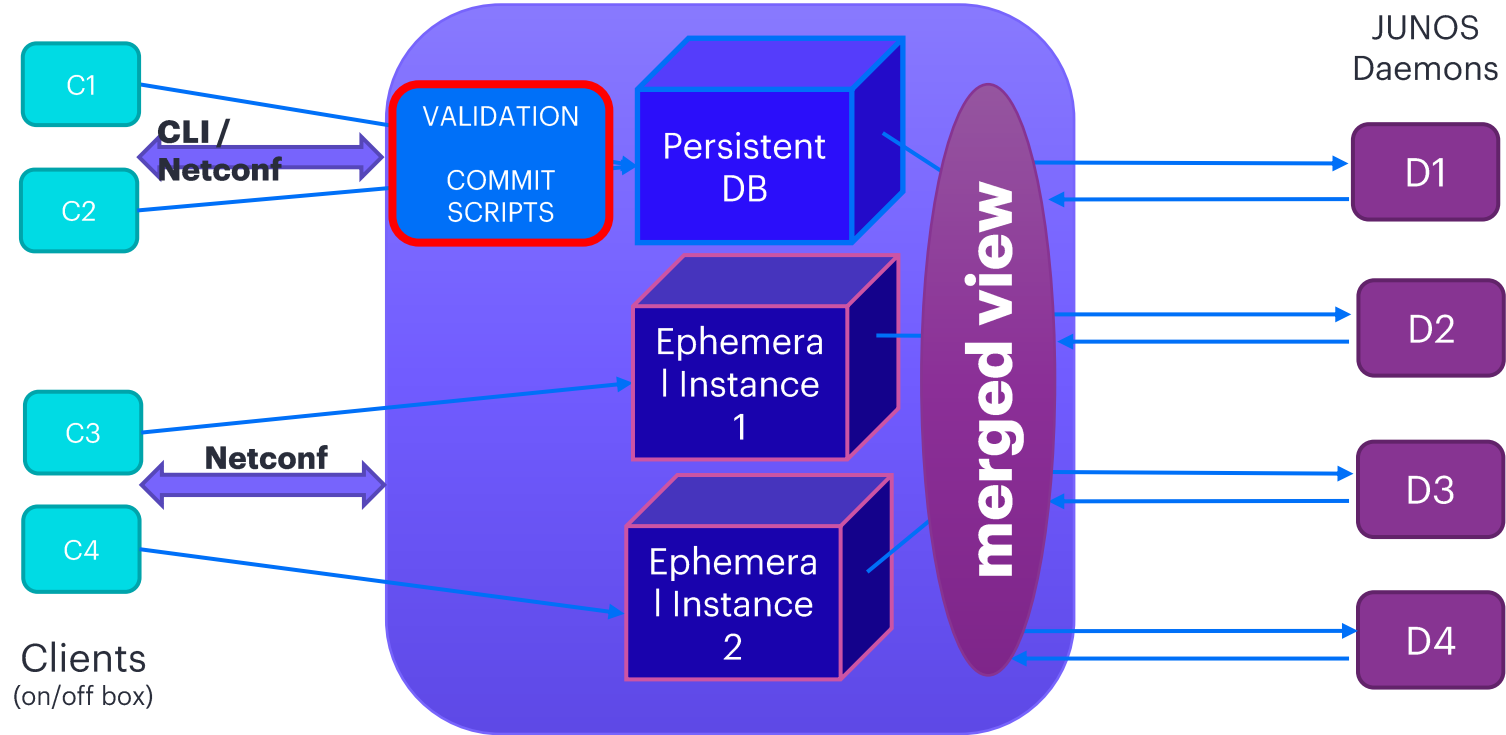
0090 79 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 ySorrySo rrySorry

00a0 53 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 SorrySor rySorryS

00b0 6f 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 6f orrySorr ySorrySo

00c0 72 72 79 53 6f 72 72 79 53 6f 72 72 79 53 6f rrySorry

ephemeral database model



example: programming ephemeral via netconf in pyez

This will make 100 commits to firewall filter with random IP addresses:

```
from jnpr.junos import Device
from getpass import getpass
from jnpr.junos.utils.config import Config
import sys
import random

#hostname = input("Device hostname: ")
hostname = "e2-e11"
#username = input("Device username: ")
username = "aelita"
password = getpass("Device password: ")

# NETCONF session over SSH
dev = Device(host=hostname, user=username,
passwd=password)

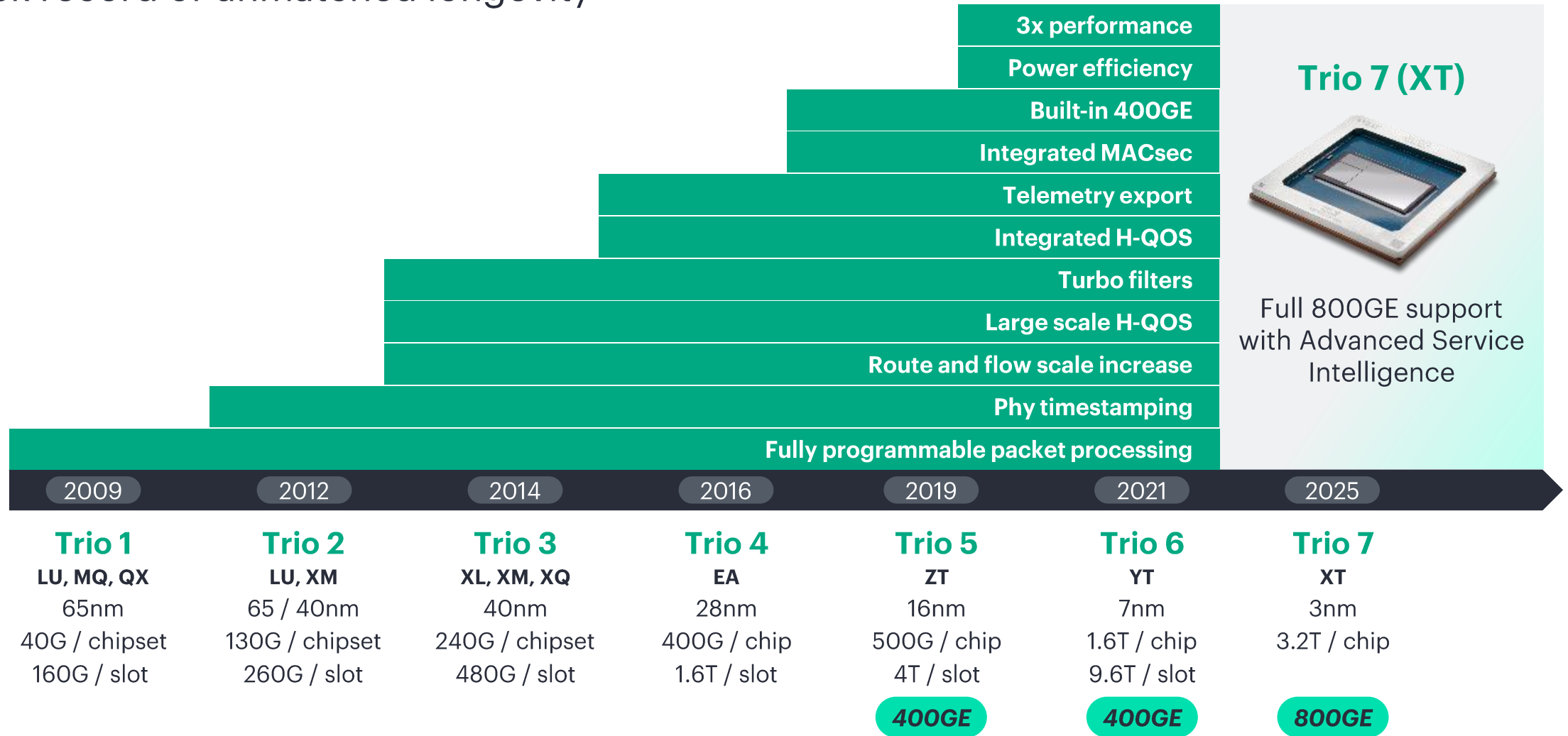
try:
    dev.open()
except Exception as err:
    print (err)
    sys.exit(1)

with Config(dev, mode='ephemeral',
ephemeral_instance='inst1') as cu:
    set_string = ''
    for K in range(1,100):
        a = str(random.randint(1,223))
        b = str(random.randint(0,255))
        c = str(random.randint(0,255))
        d = str(random.randint(0,255))
        set_string += 'set firewall family inet filter
eph term A From source-address
'+a+'.'+b+'.'+c+'.'+d+'/32\n'
    cu.load(set_string, format='set')
    cu.commit()

dev.close()
```

Trio ASIC evolution

Track record of unmatched longevity



Introducing Trio 7 (XT)

Continuing Juniper's legacy of silicon leadership



Superior flexibility higher and flexible fan out (64 interfaces per XT)



320 processing cores
for massive parallelism

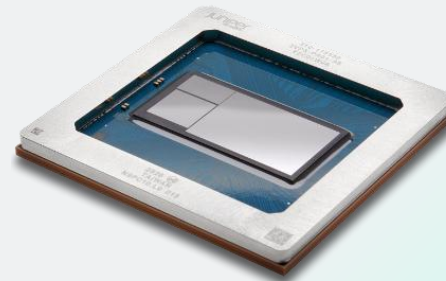


Inline MACsec
at 800G and IPsec support



Flexible filters
with real integrated DDoS protection

Trio 7 (XT)



Full 800GE support
3nm technology

3.2 Tbps packet forwarding engine
1GE to 800GE on one ASIC



Rich telemetry
highest sampling and export rates



~33% Power efficiency improvement
Better TCO



Proven performance
12M FIB, 80M RIB, 16K VRF, 4M flow,
256K FILTERS, 64K SUBS, 512K queues



Investment protection | backward compatibility | fully programmable processing



Future-proof MX portfolio

1G / 10G / 100G / 400G generation powered by Trio

Compact



Trio 4



MX204

1RU, Compact

400G
8 x 10GE
4 x 100GE



Trio 6



MX301*

1RU, Compact

1.6T
4 x 400GE
16 x 100GE



MX304

2RU, Compact

1.6T-4.8T
12 x 400GE
48 x 100GE

Classic



Trio 3-5



MX240/480/960

5RU – 16RU, Modular

12T
120 x 100GE
528 x 10GE



MX2008/2010/2020

24RU - 45RU, Modular

80T
160 x 400GE
800 x 100GE

Modular



Trio 4/6



MX10004, MX10008

7RU – 21RU, Modular

38.4-76.8T
192 x 400GE
768 x 100GE

Next Gen MX portfolio

1G / 10G / 100G / 400G generation

Compact



Trio 6



Trio 6



2H2026
MX304-LMIC20S



NEW



MX301	MX304
1RU, Compact	2RU, Compact
1.6T 4 x 400GE 16 x 100GE	4.8T 12 x 400GE 48 x 100GE

Modular MX10000



Trio 4/6



NEW
MX10K - RE3



MX10004, MX10008
7RU - 13RU, Modular
38.4-76.8T 192 x 400GE 768 x 100GE

MX10000 Line Cards



Trio 6



Trio 6



Trio 6



Trio 7







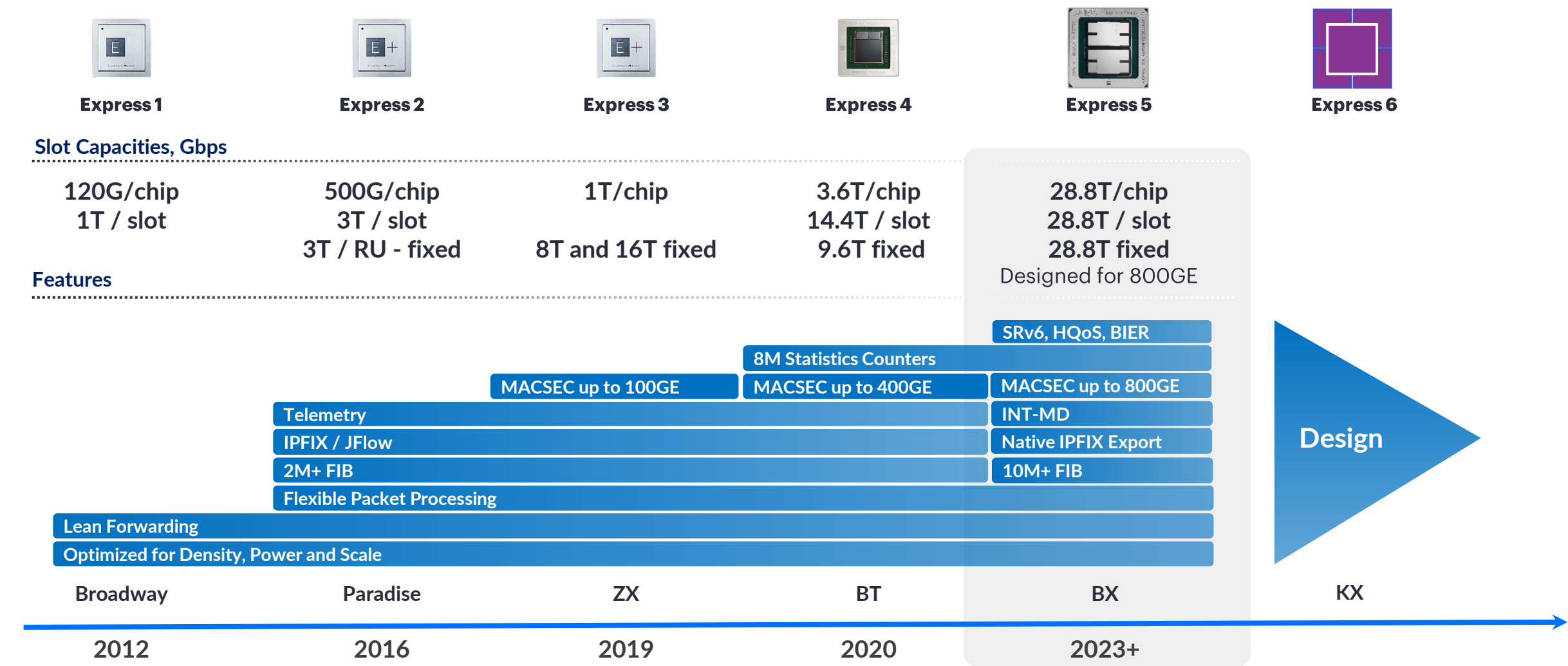
NEW



1H 2027

LC9600	LC4800	LC4802	LC3200
24 x 400GE	48 x 100GE SFP	48 x 100GE QSFP	Multiple MICs
9.6T 24 x 400GE 96 x 100GE	4.8T 4 x 400GE 44 x 100GE	4.8T 4 x 400GE 44 x 100GE	3.2T 4 x 800GE/8 x 400GE, or 32 x 100GE

Express ASICs, Silicon Powering PTX Routers

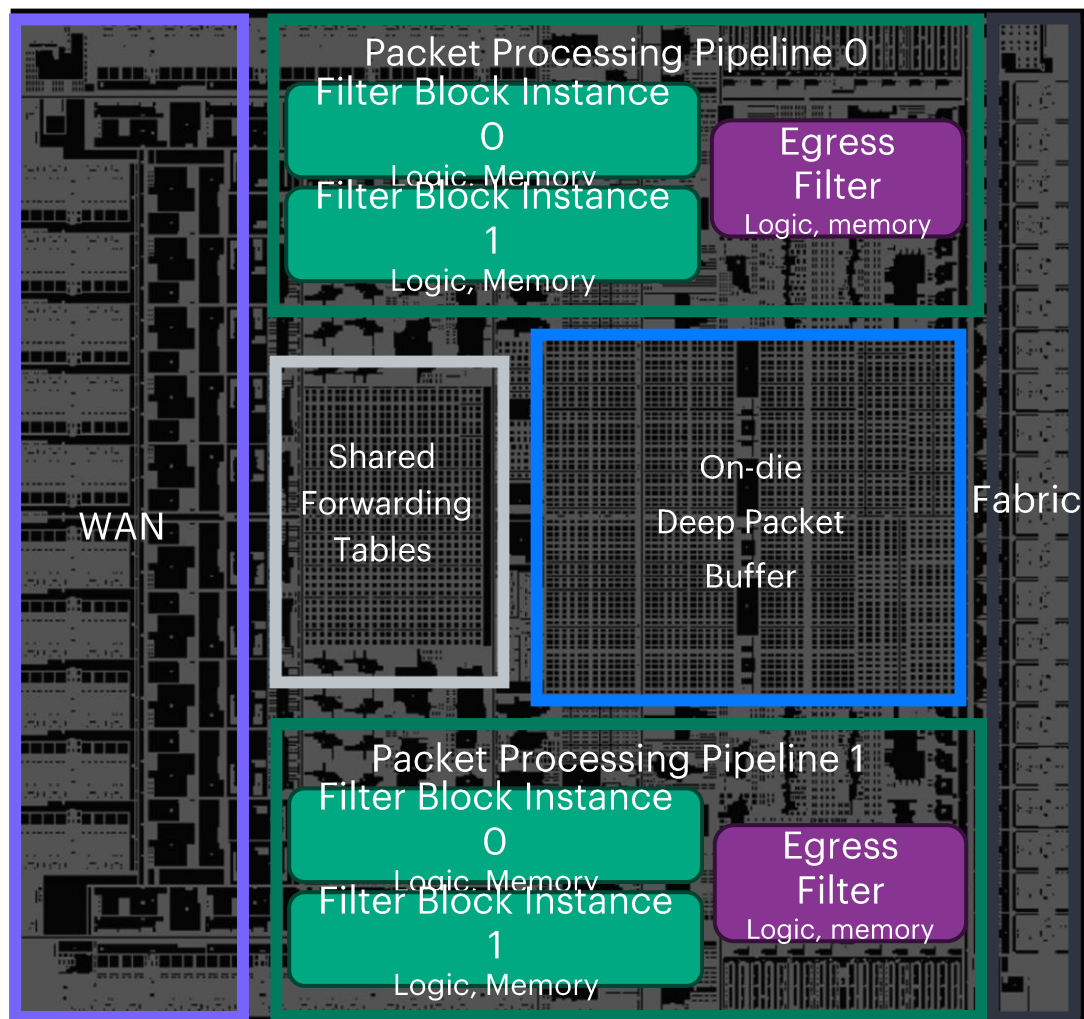


BX / Express 5 Taxonomy

System

Package

Die



4.96 Bpps per chip
total
2.48 Bpps per packet
processor
1.24 Bpps per filter instance

Assuming two filter operations per packet

Filter Block Instance 0
Logic and Memory

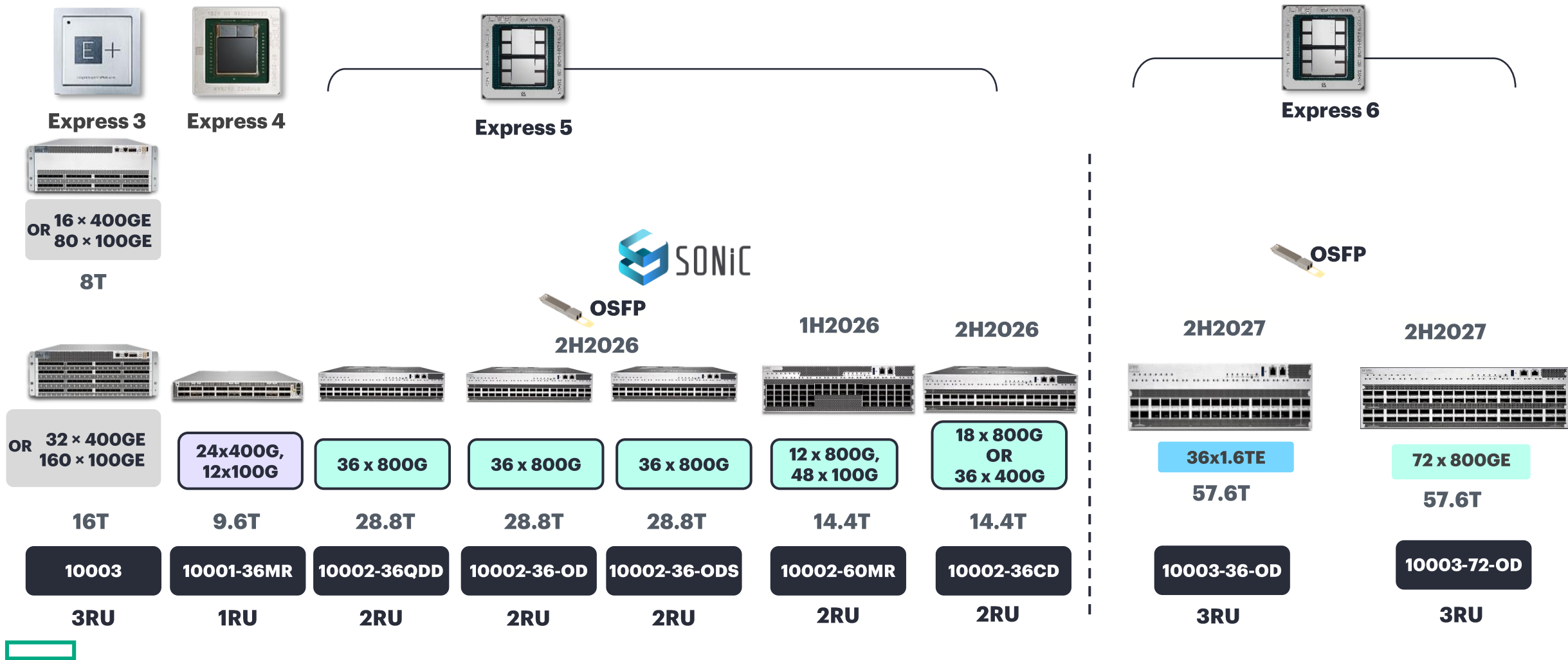
High-scale, feature-rich
Shared between ingress and egress

Egress Filter
Logic, memory

Low-scale, high-performance
Egress only

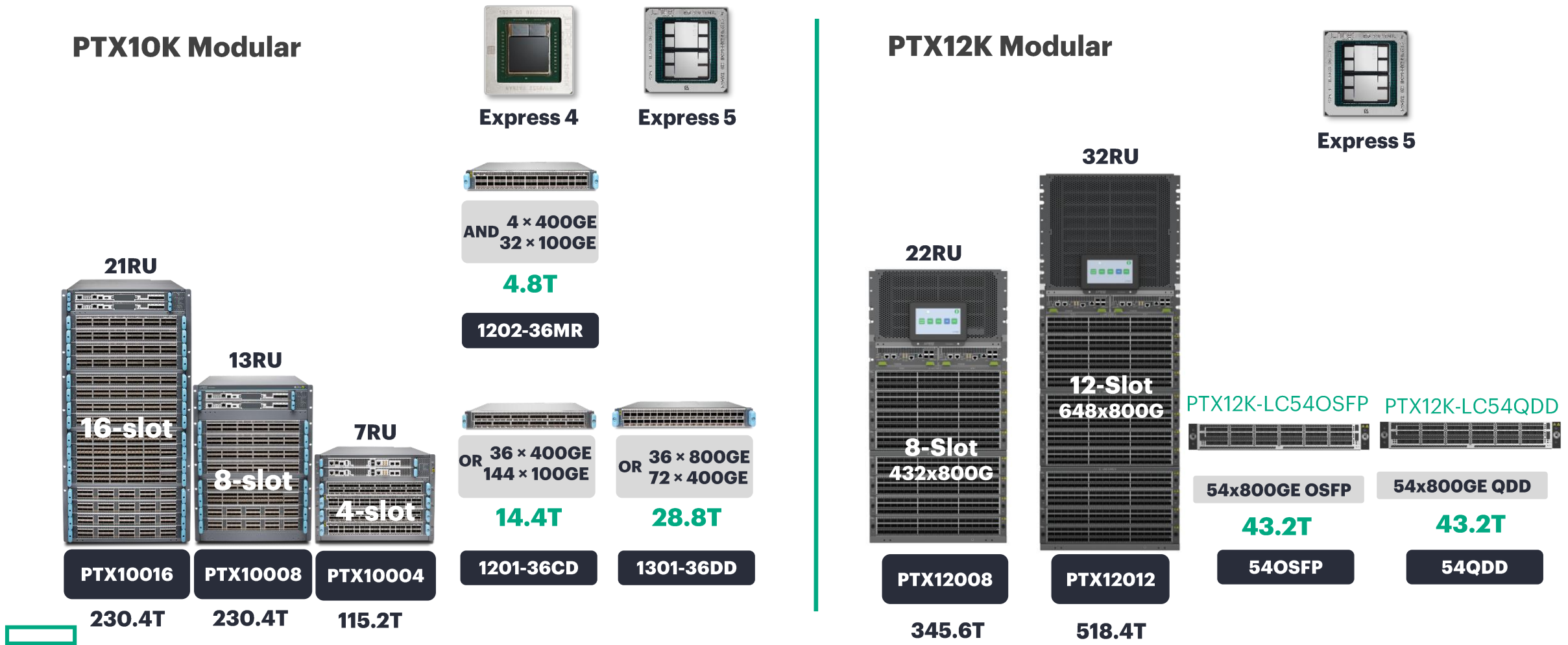
Full PTX Fixed Portfolio, 2020-2028

100GE, 400GE, 800GE and 1.6TE Generation



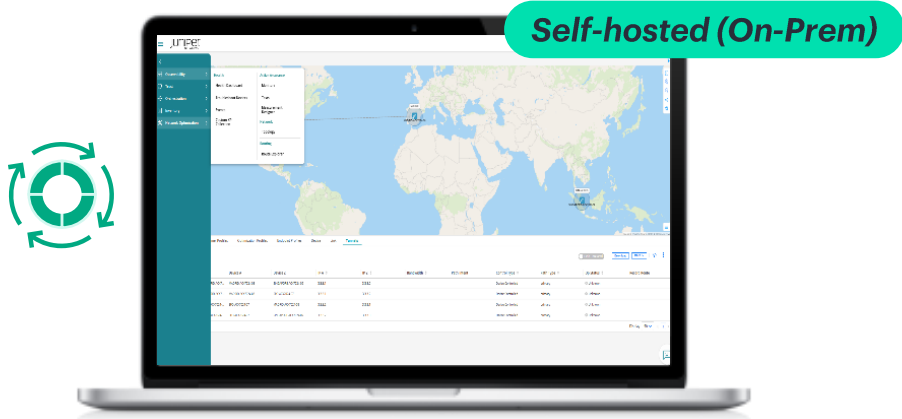
PTX Modular Portfolio

Industry's largest density of 800GE with 648 x 800GE OSFP/QSFP ports



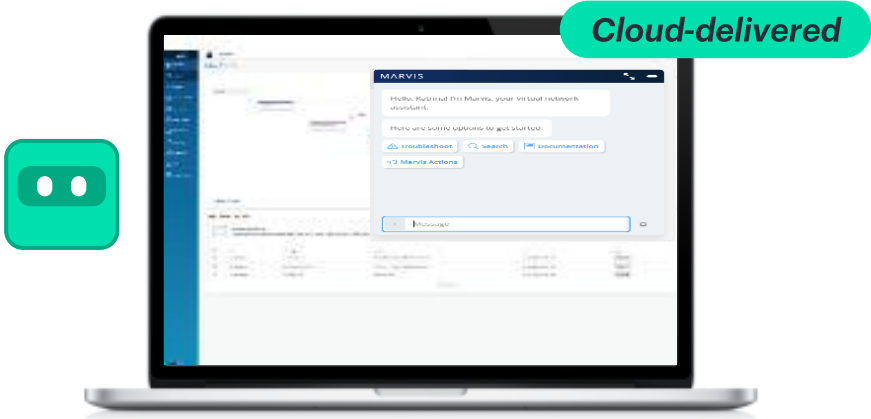
AI-Native, intent-based automation

Routing Director



Plan	Orchestrate	Assure	Optimize
Simple and intuitive for operators			
Granular device control			
Network planning, advanced traffic engineering and orchestration			
Multivendor and customizable			
Real-time network status visibility and analytics			

Routing Assurance



Assure	Optimize
Proactively detect and remediate routing issues	
Simplify and automate operations	
AI-based fault detection and root cause analysis	
AI-assisted troubleshooting (LLM Connector)	
Reliable performance for the AI era	



Mist Routing Assurance with AIOPs

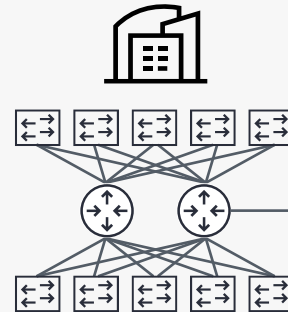
Juniper Mist Routing Assurance

- Easily adopt industry leading MXs for routing
- Proactively detect and remediate WAN issues before they impact users
- Simplify and automate operations, boosting productivity
- Reduce MTTR with root cause analysis and actionable insights



Official product launch June 5, new features added weekly

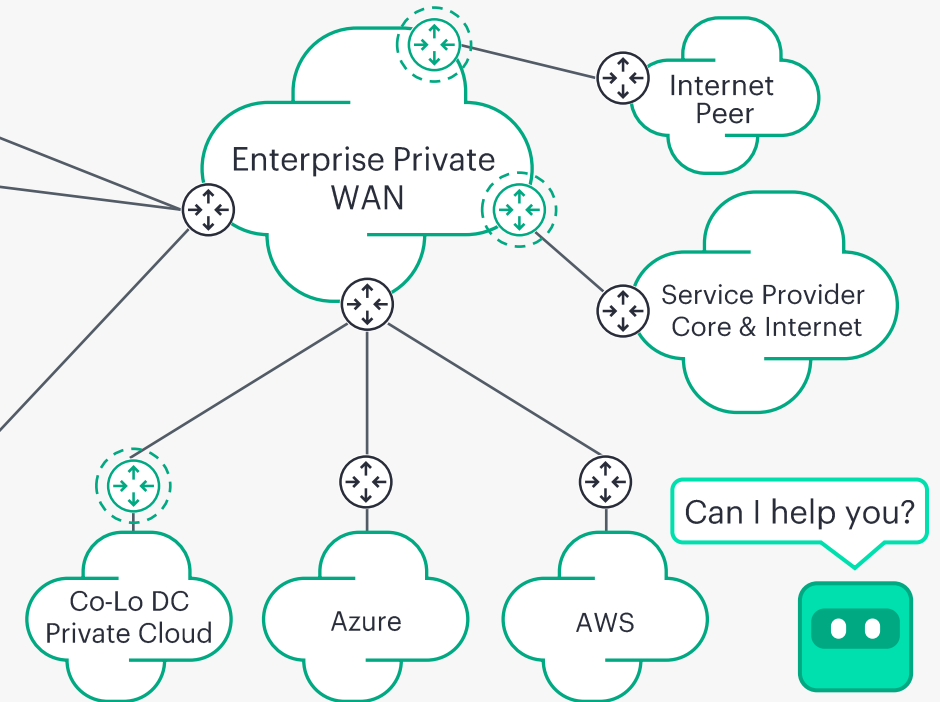
Campus Branch



Data center

Campus and Branch Edge (CPE)

WAN



Private WAN Edge | Internet Edge/Peering | Cloud Connect

Demo – DNS Flood Mitigation

slab-mx240-01_re0 SSeSSeconds: 313 TttTime

Interface	Link	Input packets	(pps)	Output packets	(pps)	Description
gr-1/0/0	Up	0	(0)	0	(0)	
ip-1/0/0	Up	0	(0)	0	(0)	
lc-1/0/0	Up	0	(0)	0	(0)	
lt-1/0/0	Up	0	(0)	0	(0)	
mt-1/0/0	Up	0	(0)	0	(0)	
pd-1/0/0	Up	0	(0)	0	(0)	
pe-1/0/0	Up	0	(0)	0	(0)	
pFh-1/0/0	Up	0	(0)	0	(0)	
ud-1/0/0	Up	0	(0)	0	(0)	
ut-1/0/0	Up	0	(0)	0	(0)	
vt-1/0/0	Up	0	(0)	0	(0)	
xe-1/0/0:0	Down	0	(0)	0	(0)	
xe-1/0/0:1	Down	0	(0)	0	(0)	
xe-1/0/0:2	Down	0	(0)	0	(0)	
xe-1/0/0:3	Down	0	(0)	0	(0)	
gr-1/1/0	Up	0	(0)	0	(0)	
ip-1/1/0	Up	0	(0)	0	(0)	
lc-1/1/0	Up	0	(0)	0	(0)	
lt-1/1/0	Up	0	(0)	0	(0)	
mt-1/1/0	Up	0	(0)	0	(0)	
pd-1/1/0	Up	0	(0)	0	(0)	
pe-1/1/0	Up	0	(0)	0	(0)	
pFe-1/1/0	Up	0	(0)	0	(0)	
ud-1/1/0	Up	0	(0)	0	(0)	
ut-1/1/0	Up	0	(0)	0	(0)	
vt-1/1/0	Up	0	(0)	0	(0)	
xe-1/1/0:0	Up	7907747266	(16230)	37056317094	(81105)	EXTERNAL -...
xe-1/1/0:1	Up	37156412255	(81083)	7601144435	(16230)	INTERNAL -...
xe-1/1/0:2	Up	2377752	(0)	115170586	(0)	ROUTING AN...
xe-1/1/0:3	Up	577679	(1)	79168820	(145)	SERVICES -...
mams-2/0/0	Up	0	(0)	0	(0)	
vms-2/0/0	Up	0	(0)	0	(0)	
mams-2/1/0	Up	0	(0)	0	(0)	
vms-2/1/0	Up	0	(0)	0	(0)	

root@dd-source101: ~ (ssh)

root@dd-source101:~# sh attack_dns_flood_response_to_target.cns-002067.sh

corero

Home

Policy

- Detection
- Protection
- Remote Mitigation
 - DIP Thresholds
 - Rule Triggers
- Address Groups
- Rule Groups

Network

- Clusters
- Devices
- Segments
- Operating Modes
- Tunnel Termination
- BGP
- Routers

Services

System

CMS14

Units: pps 2/2 2/2 6 Version: 14.0.1.0012 Uptime: 60d 17h 53m Commit ? admin

Detection Cluster All Device All

Status OK

Operating Modes Detector: detect

Network Clusters: 1 Devices: 1 Segments: 2 Interfaces: 2

Traffic

Rules Rule Definitions

Attacks Current Attacks

Protection Cluster All Device All

Status OK

Operating Modes Bypass: automatic Defense: mitigate

Network Clusters: 2 Devices: 1 Segments: 1 Interfaces: 2

Traffic

Rules Rule Definitions

Attacks Current Attacks

Remote Mitigation

Status OK

Routers Juniper Enabled: 1

Router Telemetry

Remote Mitigations

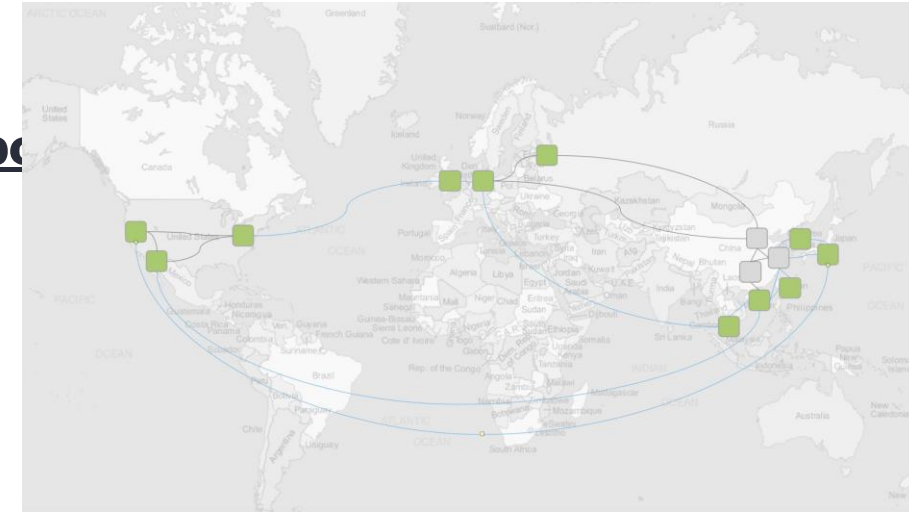
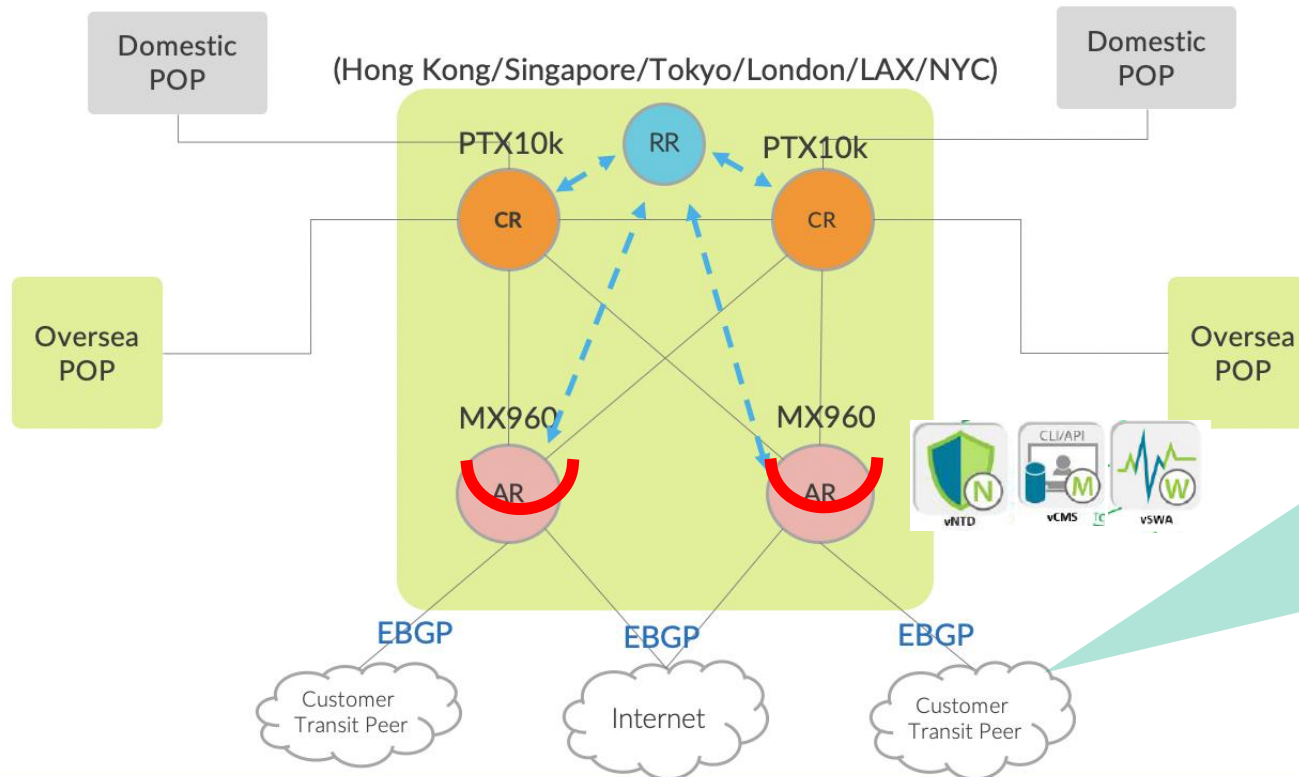
Actions

Customer References

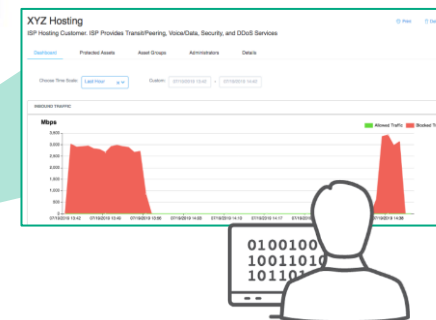


China Top3 sp international backbone

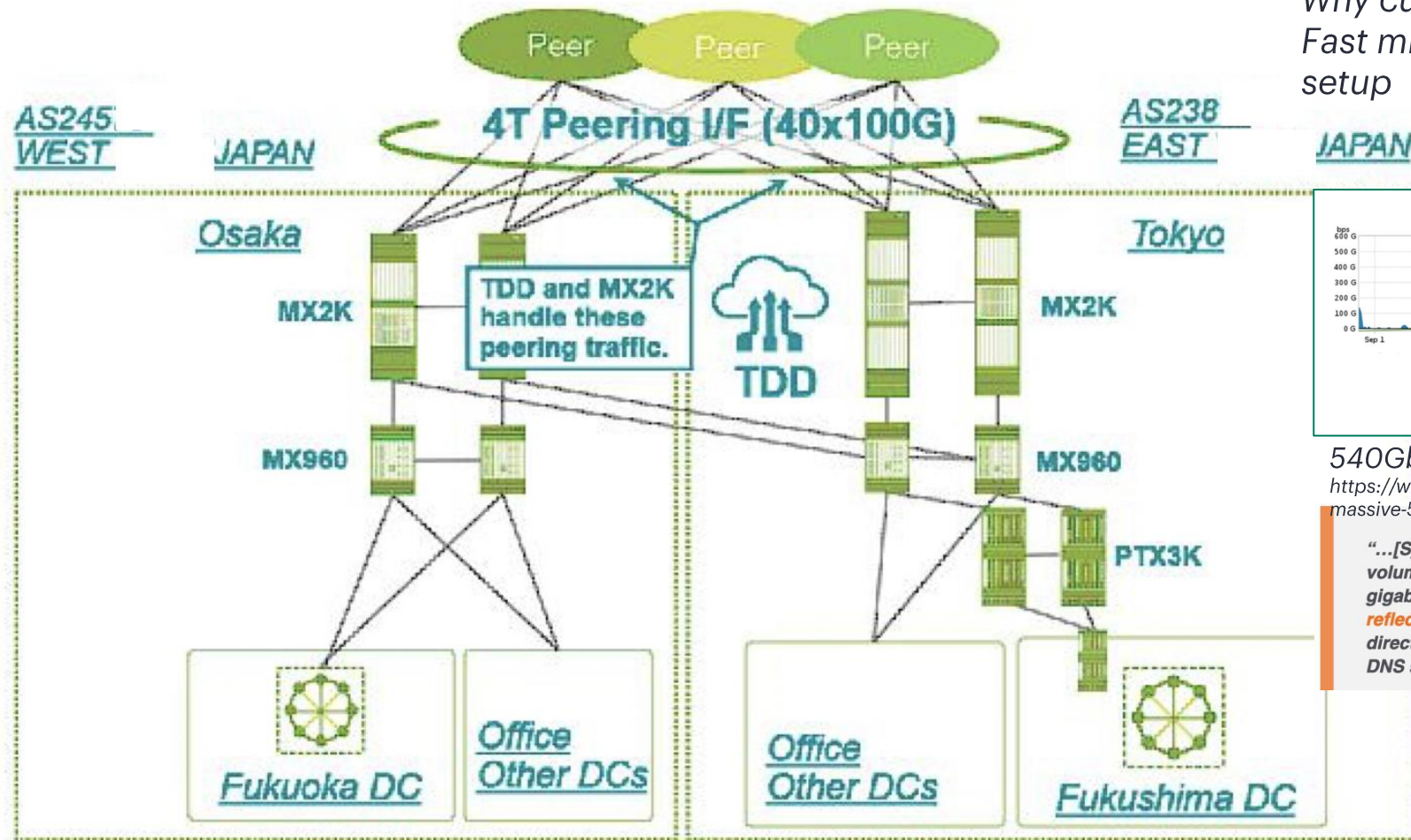
- 12 international POPs
- DDoS protection as a service to customers by **multitenancy po**
- End-to-end solution offering by Juniper



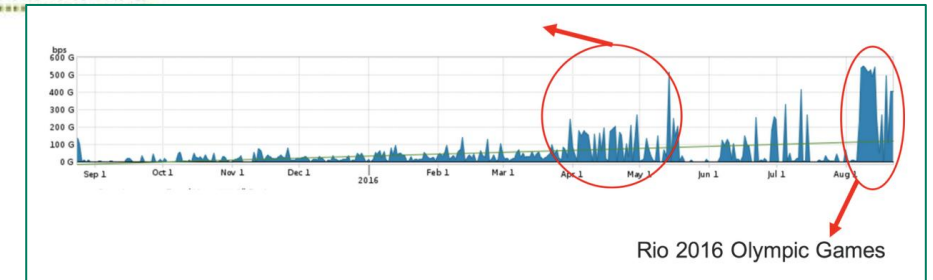
Why customer chooses TDD?
Create MX differentiation and single vendor solution
(Cisco needs to partner with Arbor), fast mitigation and
simple in operation (no change in data flow)



Large ott in japan (official supporter of Tokyo olympic)



Why customer chooses TDD?
Fast mitigation, scalable, ease of use and simple setup



540Gbps DDoS attack in Rio 2016

<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/>

"...[S]everal organizations affiliated with the Olympics... [came] under large-scale volumetric DDoS attacks ranging from the tens of gigabits/sec up into the hundreds of gigabits/sec. A large proportion of the attack volume consisted of **UDP reflection/amplification attack** vectors such as DNS, chargen, ntp, and SSDP, along with direct UDP packet-flooding, SYN-flooding, and application-layer attacks targeting Web and DNS services."

Official supporter of Tokyo Olympic Internet-based information and navigation services (including: Web/App or internet search engine systems and services, Weather information)

Large research network in AUSTRALIA

Internet services provider to Australian education and research partners

- Protect network infrastructure and offer anti-DDoS service to universities and research partners via **multitenancy portal**
- **Flexible config tool** to whitelist the giant UDP compute data transfer between DCs



SEATH SP

Protect Networking Infrastructure & Save Expensive Submarine Cables Resource

Internet & cloud service provider with submarine cables across ASEAN POPs

Pain points

- Legacy (Cloudflare) solution is **too slow and complex** in operations
- **Manual** operations, e.g. submit tickets to Cloudflare to announce customer prefixes for mitigation
- Volumetric DDoS from overseas PoPs consumes a lot of BW causing **service impact**

Why do we win?

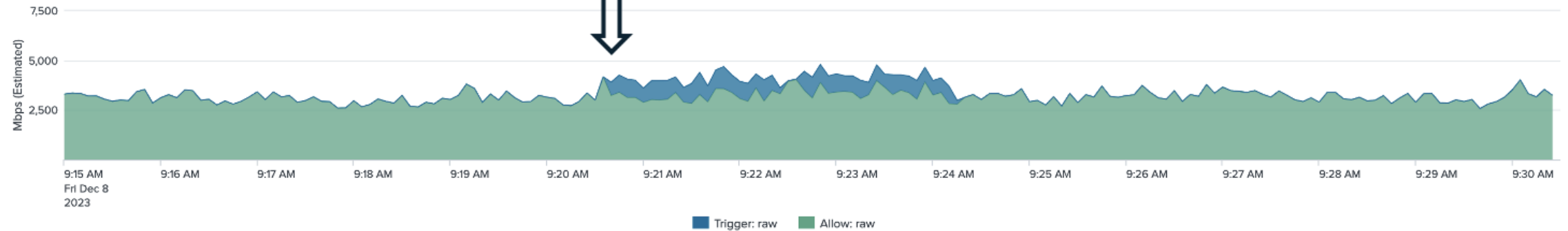
- Full **automation and fast** reaction time
- **Ease to deploy** in overseas PoPs
- Block volumetric DDoS before entering submarine cable network
- **Save** expensive submarine cable resource for customer's real traffic



Top Service Provider in APJ

Real-time Mitigation in 15s

Traffic seen on NTD index=securewatch type=sflow dir=inbound



Modified Telemetry data in table format (unsummarized, 50K records max) index=securewatch_tdd sourcetype=corero_juniper_telemetry_table

Telemetry Interval (seconds)

2

Mitigation filter in action at 9:20:55s



Public References

Sure Telecom

<https://www.sure.com/guernsey/latest-news/2020/sure-begins-multimillion-pound-network-upgrade-project/>



Linode (North America)

<https://www.juniper.net/content/dam/www/assets/case-studies/us/en/linode.pdf>
<https://www.youtube.com/watch?v=E3C74d3hC5c>



GARR (Italy)

<https://www.juniper.net/gb/en/company/press-releases/2020/pr-2020-10-26-00-00.html>
<https://go.corero.com/hubfs/3.%20Website%20Content/1.%20Asset%20Downloads/2.%20Case%20Studies/Corero-Juniper-GARR-Case-Study.pdf>



Plusnet (Germany)

<https://newsroom.juniper.net/news/news-details/2021/Plusnet-Chooses-Juniper-Networks-and-Corero-Joint-Security-Solution-to-Stop-DDoS-Attacks-in-Seconds/default.aspx>
<https://www.sourcesecurity.com/news/corero-network-security-juniper-networks-provide-co-7165-ga-co-1602672655-ga.1625218166.html>



THANK YOU

