

The background features a central vertical green bar. On either side of this bar, there are grayscale images of fingerprints, with the ridges and valleys clearly visible. The overall composition is clean and professional, emphasizing security and identity.

JUNIPER THREAT DEFENSE DIRECTOR (TDD)

Karel Hendrych

Consulting Engineer, EMEA

khe@juniper.net

AGENDA

- Juniper Threat Defense Director (TDD) Positioning
- Technology Overview, Use Cases
- Scaling and deployment options
- Demo videos



JUNIPER DDoS PROTECTION SOLUTIONS

SRX and MX Series

- Basic DDoS Protection with screens → first protection line for smaller scale
- All SRX series, high end SRX5k series recommended
- MX240/480/960 and MX2K with service pics (MS-MIC, MS-MPC), 16.1R3 and above (so called IDS)

BGP flow specs in routers: MX and PTX

- Allows DDoS protection enforcement in combination with any flow spec compliant DDoS solution, example Arbor

Corero + MX

- **Sophisticated, fast and scalable DDoS protection solution**

CORERO INTRODUCTION

Corero Network Security (CNS)

- London Stock Exchange AIM listed:
- Focus: Real-time DDoS Protection (Detection and Mitigation)
- Target Markets:
 - Service Providers, Cloud/Hosting Providers, Digital Enterprise

SmartWall DDoS Detection and Mitigation

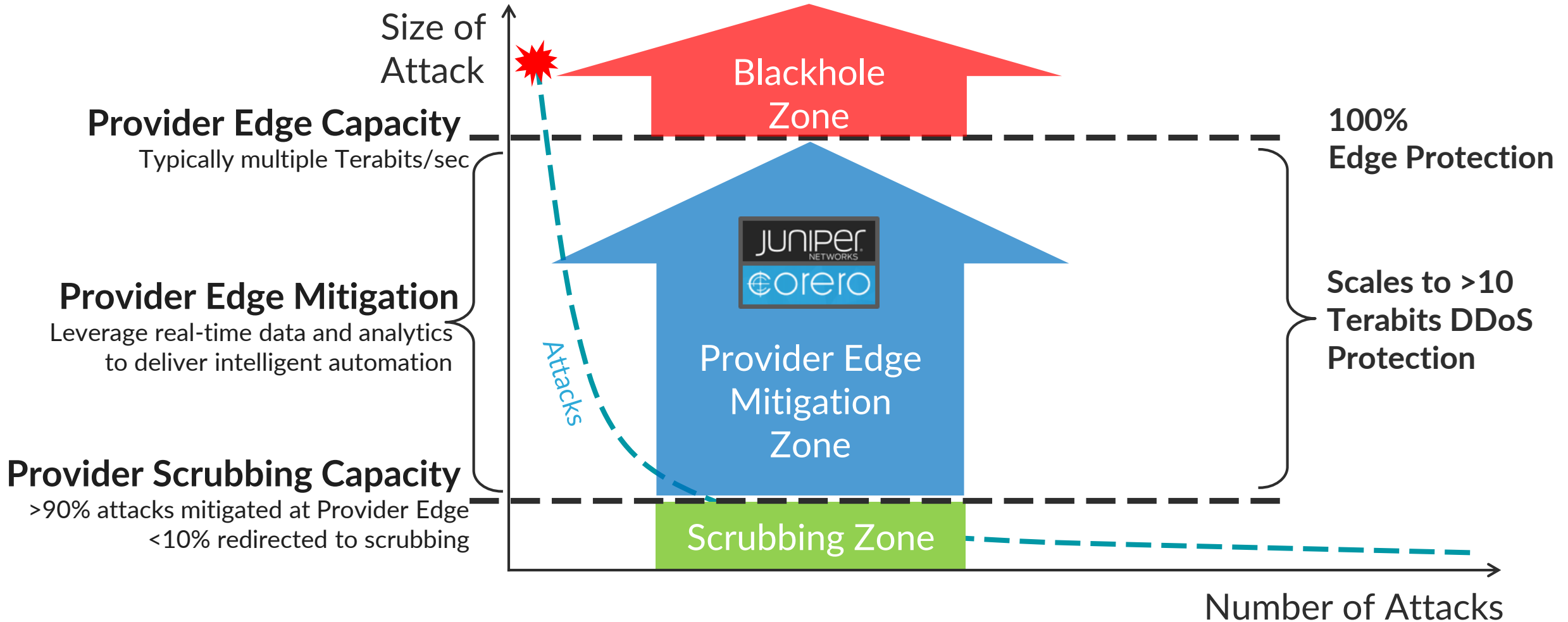
- Products:
 - SmartWall® Threat Defense Director (TDD) with Juniper MX
 - DDoS Detection and Mitigation 500Gb, 1Tb, 10Tb, 40Tb
- Services:
 - DDoS Monitoring, Analytics and SOC
- Available on the Juniper Price List
 - Supported by JTAC

WHAT JUNIPER TDD DOES

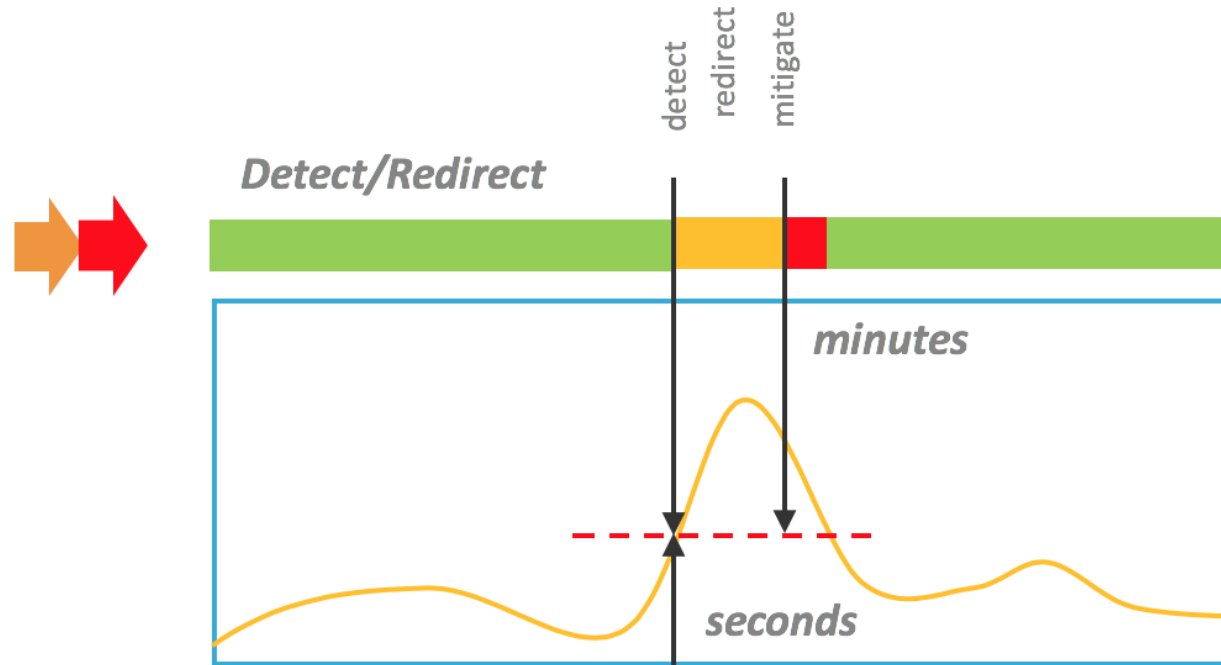





**Juniper TDD is threshold based
volumetric DoS/DDoS protection.**

MITIGATION STYLE VS. ATTACK SIZE AND EDGE CAPACITY



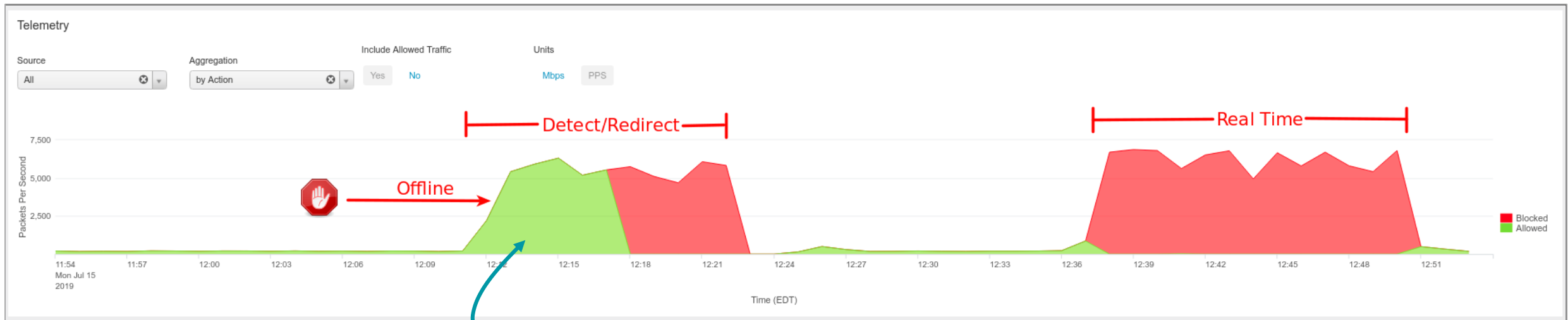
TIME TO MITIGATION (TTM) OF MINUTES = FAIL



-  allowed
-  missed attack
-  blocked



TIME TO MITIGATE COMPARISON USING ANALYTICS



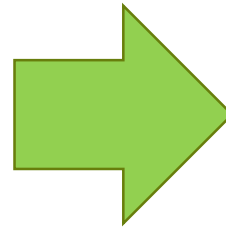
*77% of DDoS
Incidents last less
than <10 minutes*

ENHANCED ACCURACY + SPEED OF DDOS DETECTION/MITIGATION



Netflow

- aggregation delay
- header only
- attack overload



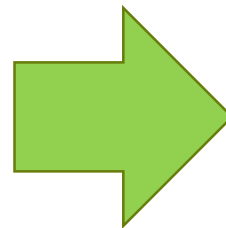
Sampled Mirror

- immediate forwarding
- header and payload
- scales with attack



Flowspec

- BGP propagation
- header only
- limited visibility



NETCONF

- ephemeral configuration
- header and payload
- streaming telemetry

COMPARISON TRADITIONAL NETFLOW/REDIRECT VS MIRROR/NETCONF



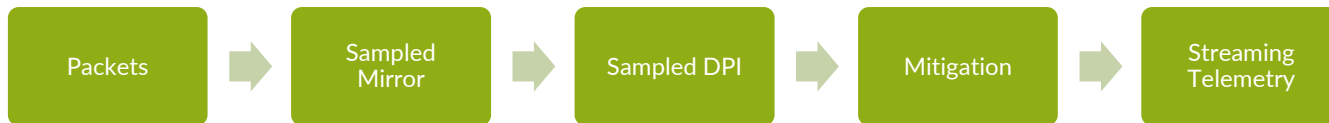
Netflow/Redirect

Typically Minutes



Sampled Mirror / Netconf

Typically < 10 seconds



< 2 second

< 2 second

< 5 seconds



TECHNOLOGY OVERVIEW

Juniper Thread Defense Director



TDD COMPONENTS AND MX FEATURES

Juniper Threat Defense Director (TDD)

- Detection Engine (vDE)

- Detect DDoS attack from sampled packets
- Forwards information to CMS



- Detection Director (DD)

- Central Management Server (vCMS)

- Manage mitigation policy
- Receives and coalesces data from DE(s)



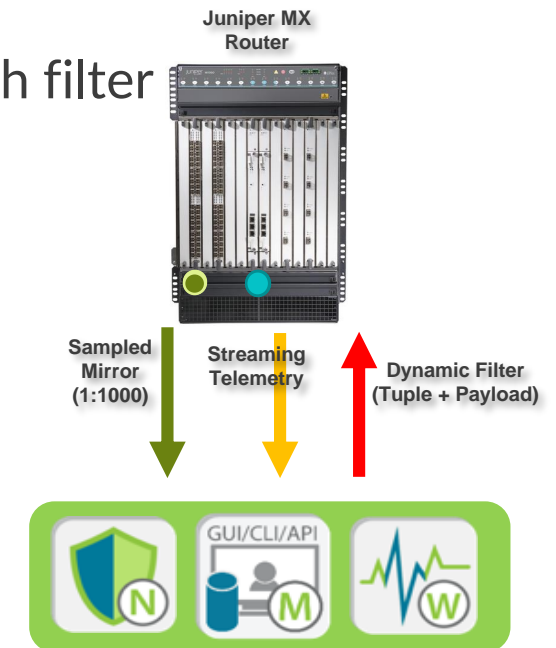
- SecureWatch Analytics (vSWA)

- Receive information from CMS
- FF provisioning
- Receive and display Telemetry
- Rich analytics and visualization

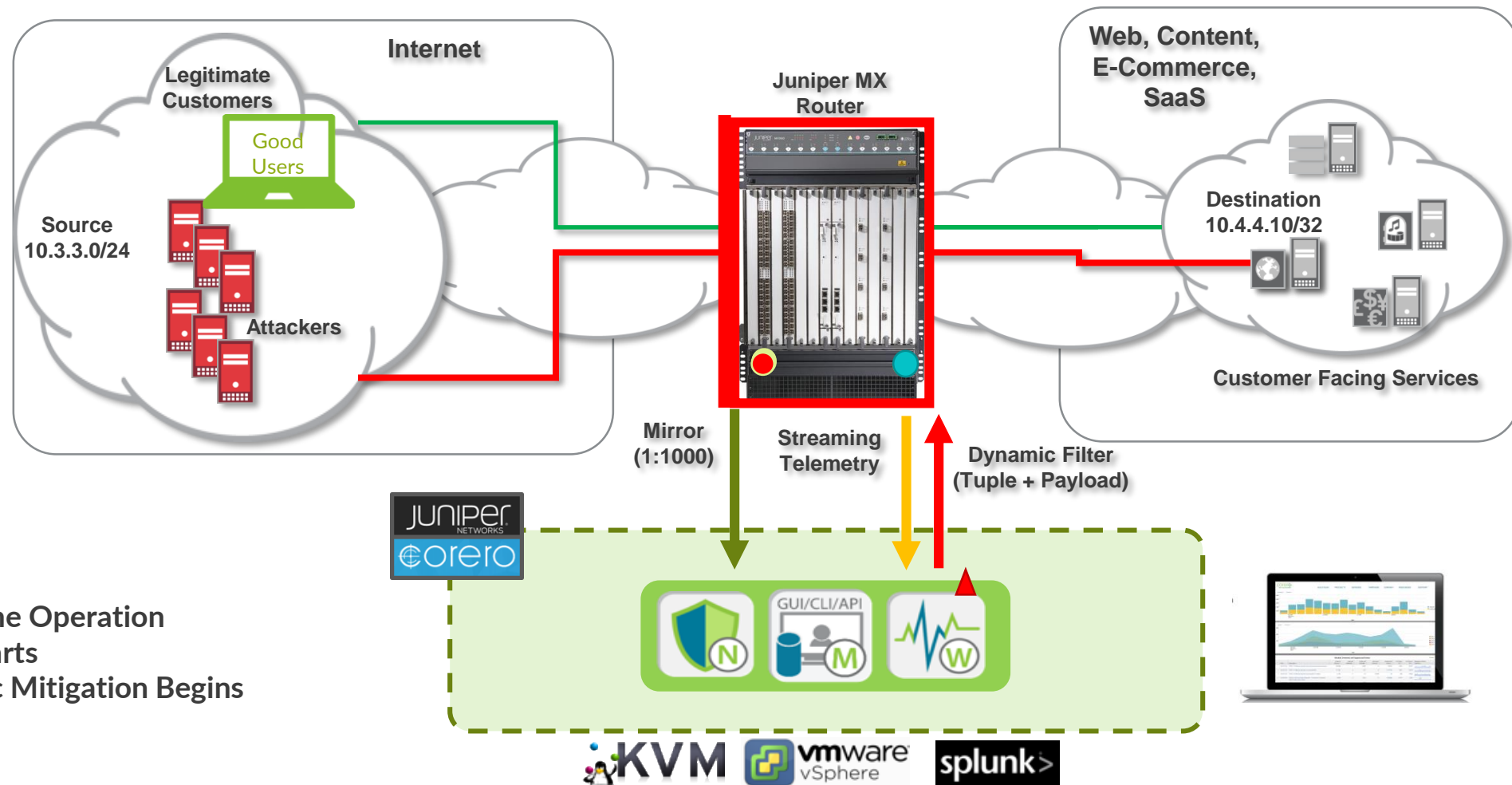


Juniper MX

- Packet mirroring (1:1000)
- NETCONF and ephemeral config database
- FF Telemetry
- Firewall flexible match filter
- Trio MPCs



JUNIPER THREAT DEFENSE DIRECTOR AUTOMATION FLOW



1. Peace-Time Operation
2. Attack Starts
3. Automatic Mitigation Begins

MX FIREWALL FILTER FLEXIBLE MATCH EXAMPLE: NTP MONLIST

```
lab@MX10003-2> show ephemeral-configuration instance Corero
## Last changed: 2019-02-14 17:15:25 HKT
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;
  }
}

```

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 02 00 0b 0f 38 00 a3 4e 4a ef 85 d1 2a 00 00 ...{.8.. NJ...
0030 00 00 00 00 00 00 00 00 b1 d7 bd 8c b5 1d 08 ff .....
0040 49 78 69 60 20 00 00 04 10 11 12 13 04 e9 df c5 Ixi`...
0050 00 71 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 .q.....!"#$%&'
0060 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ()*+,-./ 01234567
0070 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 89:;<=>? @ABCDEFGH
0080 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 HIJKLMNO PQRSTUW
0090 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 XYZ[\]^_ `abcdefg
00a0 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 hijklmno pqrstuvwxyz
00b0 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 xyz{|}~. ....

```

Flex match:

start from layer 4 (UDP)

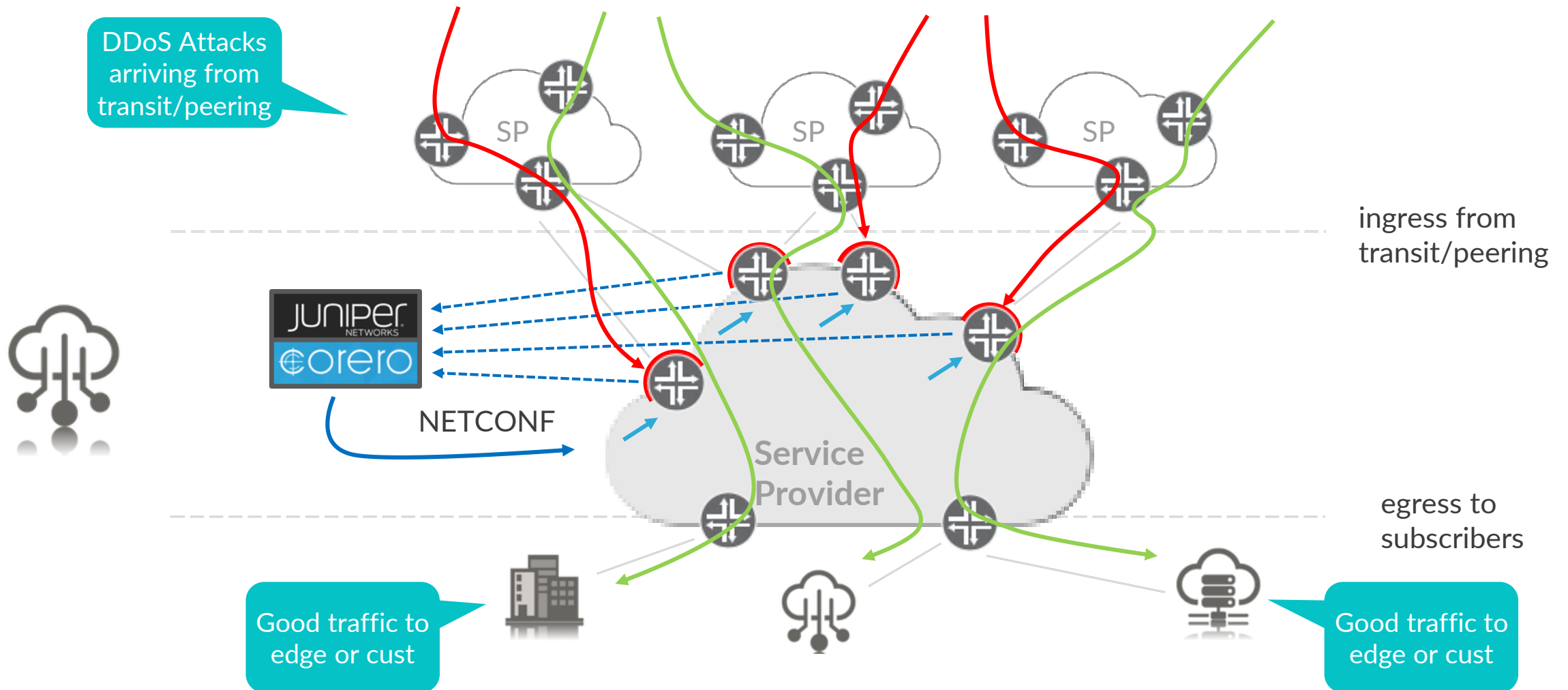
Byte-offset 11 means the 12th Byte

Match for 8 bits

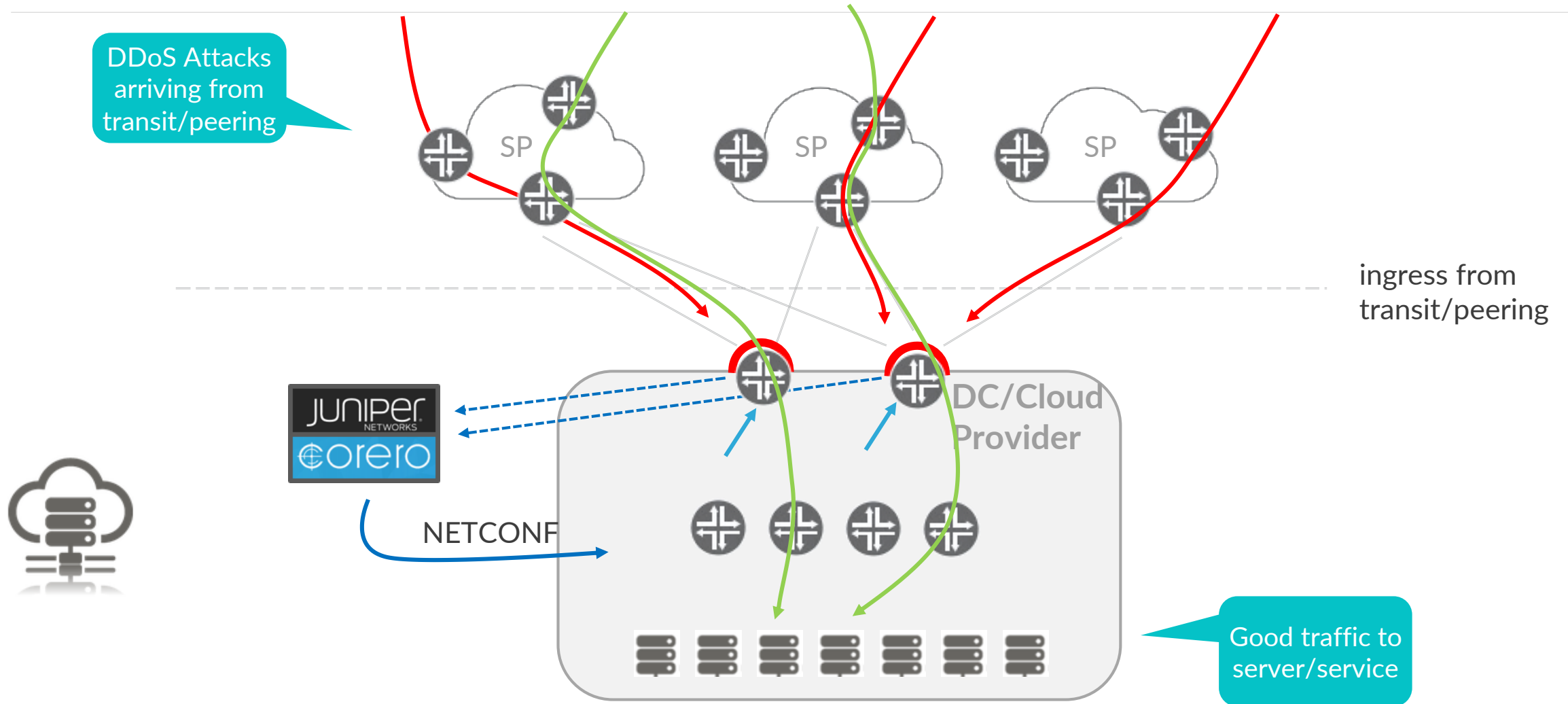
Mask = 0xFF = 1111 1111 (compare all bits)

Pattern = DEC 42 = HEX 2a

PROVIDER EDGE DDoS DETECTION AND MITIGATION



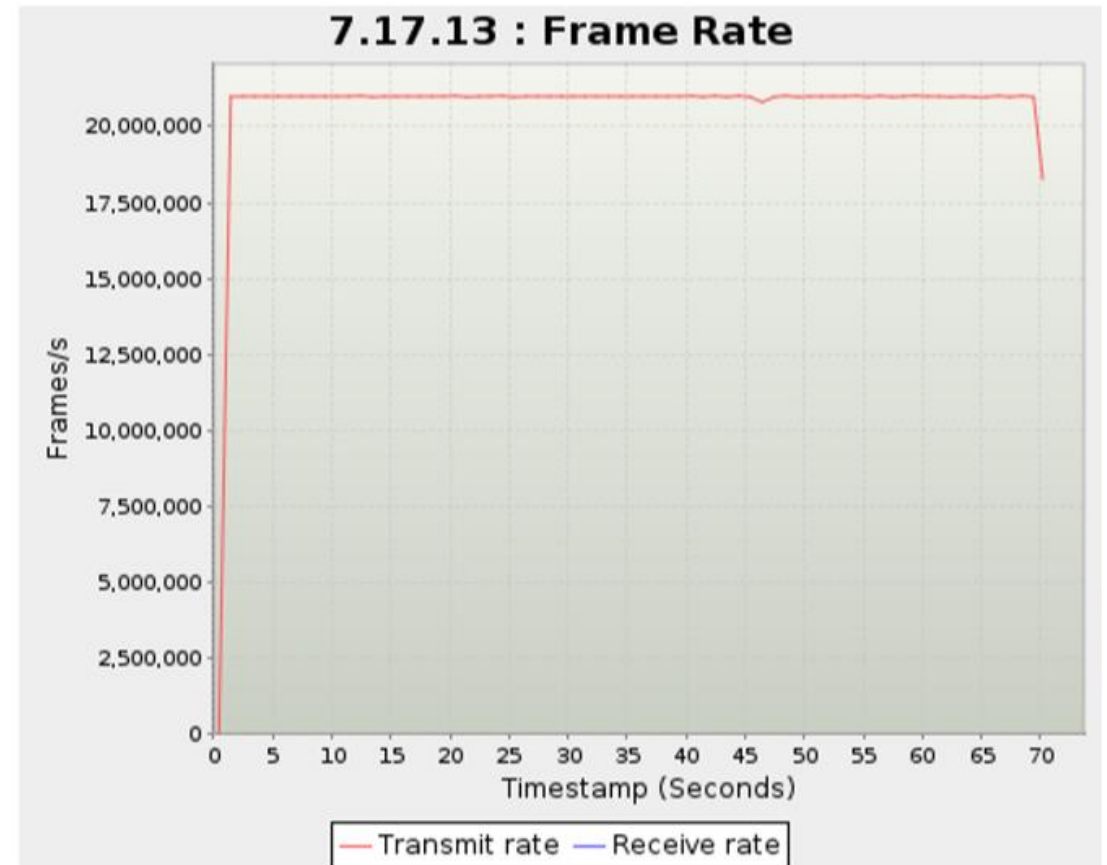
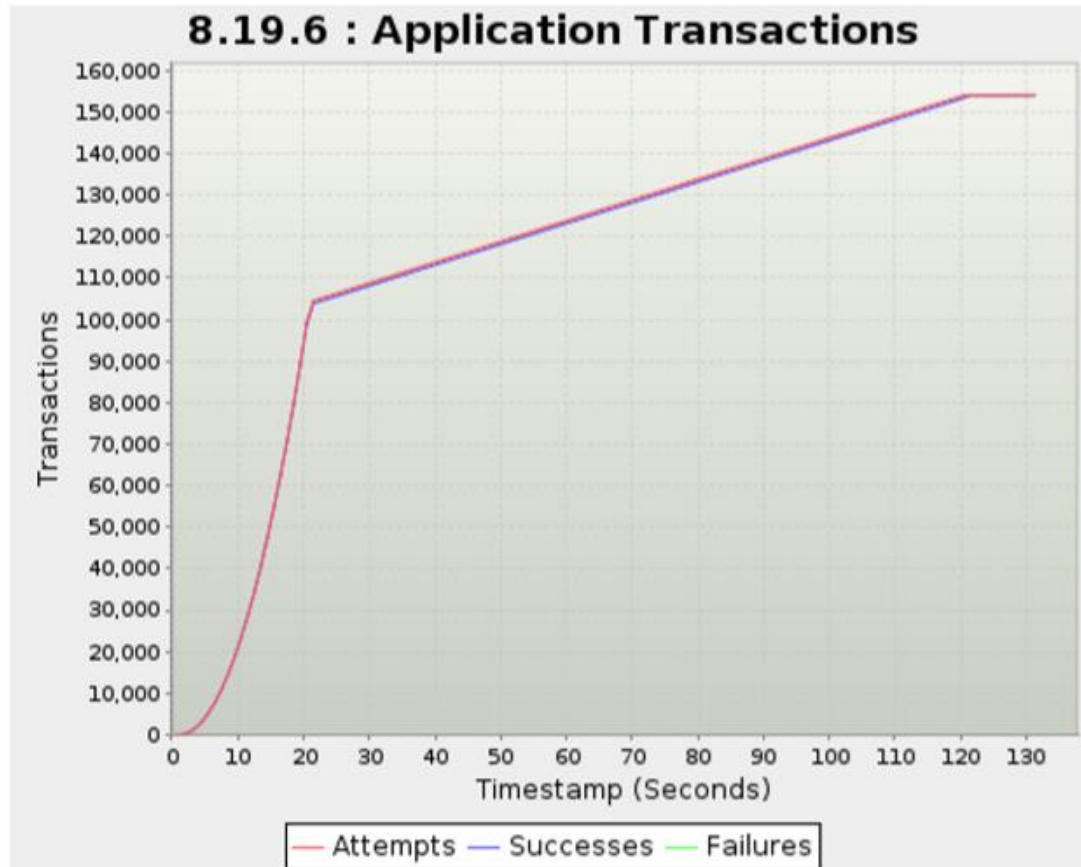
DC/CLOUD EDGE DDoS DETECTION AND MITIGATION



SETTING TDD THRESHOLDS WITH SRX5K + SPC3 SCREENING ?

Successful application transactions over time

Background 21M PPS SYN flood



THOUGHTS ON SRX SOURCE NAT POOLS PROTECTION ?

- Source NAT pools can be high profile targets (impacting subscribers)
- When DDoS is above SRX screening capacity TDD would block destination IP (effectively causing DoS by blocking the source NAT IP address)
- Junos 18.3 SRX can do session scan only for IPs removed from NAT pool
 - Blast zone reduction as the entire session table is not wiped upon NAT pool change
 - Possibilities to automate pool changes based on TDD analytics/actions (REST API, PyEZ...)

SCALING AND DEPLOYMENT OPTIONS

Juniper Thread Defense Director



SCALING DATA / RESOURCE UTILIZATION

SmartWall TDD (Threat Defense Director)

Sampled Mirror (tuple + payload)

TDD



MX Filter Generation (tuple + payload)

Sampled Mirror 1:1000
1Tbps ingress = 1Gbps samples

Streaming Telemetry = few
kB every 10 seconds per
Router

Netconf Configuration = few
kB every second per Router



TDD software VMs on standard 1RU server can
- monitor 10Tbs (10Gbps samples)
- mitigate via NETCONF to 50 MX Routers
Scales linearly beyond that.

Juniper MX

Sampled Mirror (1:1000)

Streaming
Telemetry

Ingress Traffic

Egress Traffic

Dynamic Filter (tuple + payload)

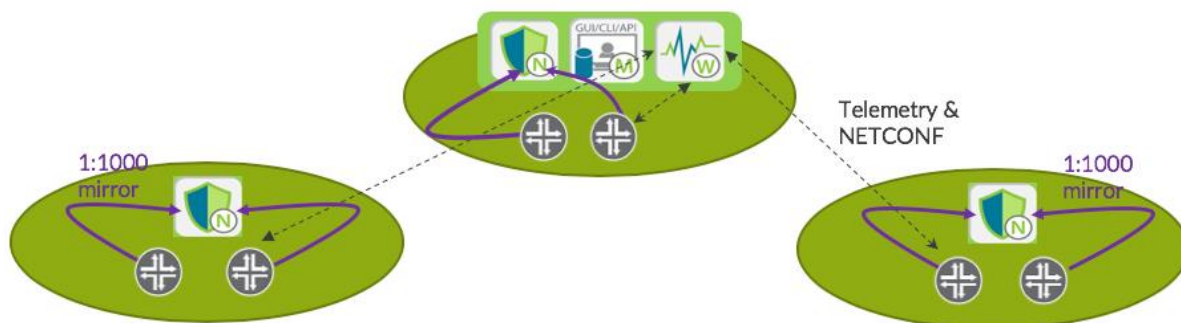
MX Router (MPC/MIC Trio) with negligible overhead
- can sample selected ingress interfaces at 1:1000
- support 100s of dynamic filter terms
- streaming telemetry for each filter term
- ephemeral config update <1 sec, 100 times/minute

OPTION 1: DISTRIBUTED DE (RECOMMENDED)

In this option, the DE is distributed.

Advantages of this Option are:

- **Commercial:** - if cost of international or site interconnection are high, then this option will save on cost of backhauling mirrored traffic to central site
- **Technical:** more simple to operate because customer does not need to setup and maintain L2 / GRE connectivity between sites



SKU configurations requirement:

- **1x J-COR-DOS-DD-1T-1** (capacity license can be shared among multiple sites)
- **2x J-COR-DOS-DE-1P-1** (capacity license comes with 1xDE, thus, 2 additional DE licenses are needed)
- Note: MX mirrors packet to DE at the same site

| Product Number | Description | Quantity |
|-------------------|---|----------|
| J-COR-DOS-DD-1T-1 | Corero SmartWall Threat Defense Director Virt Edi 1 Yr software subsc. Includes 1 Detection Engine lic, max 5, for up to 1Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity | 1 |
| J-COR-DOS-DE-1P-1 | Corero SmartWall Threat Defense Director Detection Engine, 1 pack, Virtual Edition 1 Year software subscription with 10 Gbps of processing capacity. Includes Juniper Care Support, Software Maintenance and Updates. | 2 |

OPTION 2 – CENTRALIZED DE

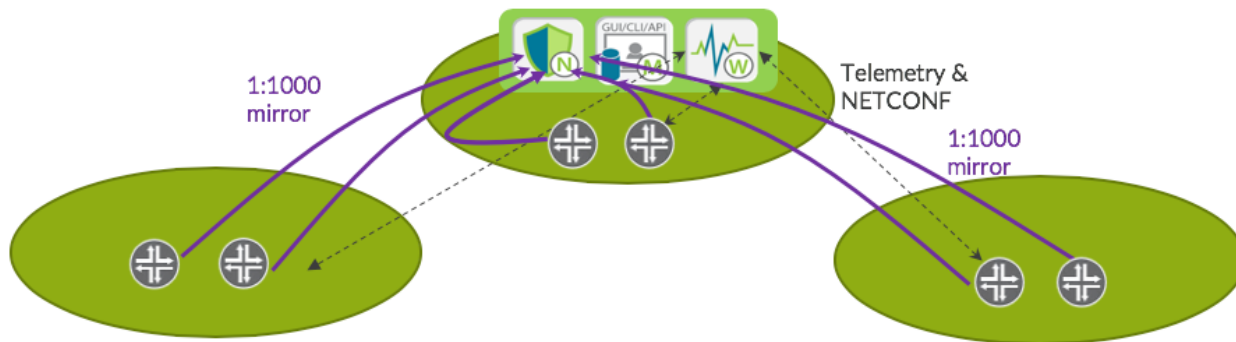
In this option, the TDD components are centralized and so, only the included DE is required.

Advantages of this Options are:

- **Commercial:** if the cost of inter-site bandwidth is not issue, then you save on the cost of having to purchase additional DE
- **Technical:** Only 3 VMs are needed, but customer sends samples to centralized DE

SKU configuration requirement:

- **1x J-COR-DOS-DD-1T-1** (capacity license can be shared among multiple sites)
- Note: MX mirrors packet to DE at the centralized site
 - E.g. if the b/w of each site is 300Gbps, the mirrored b/w is 300Mbps (1:1000)



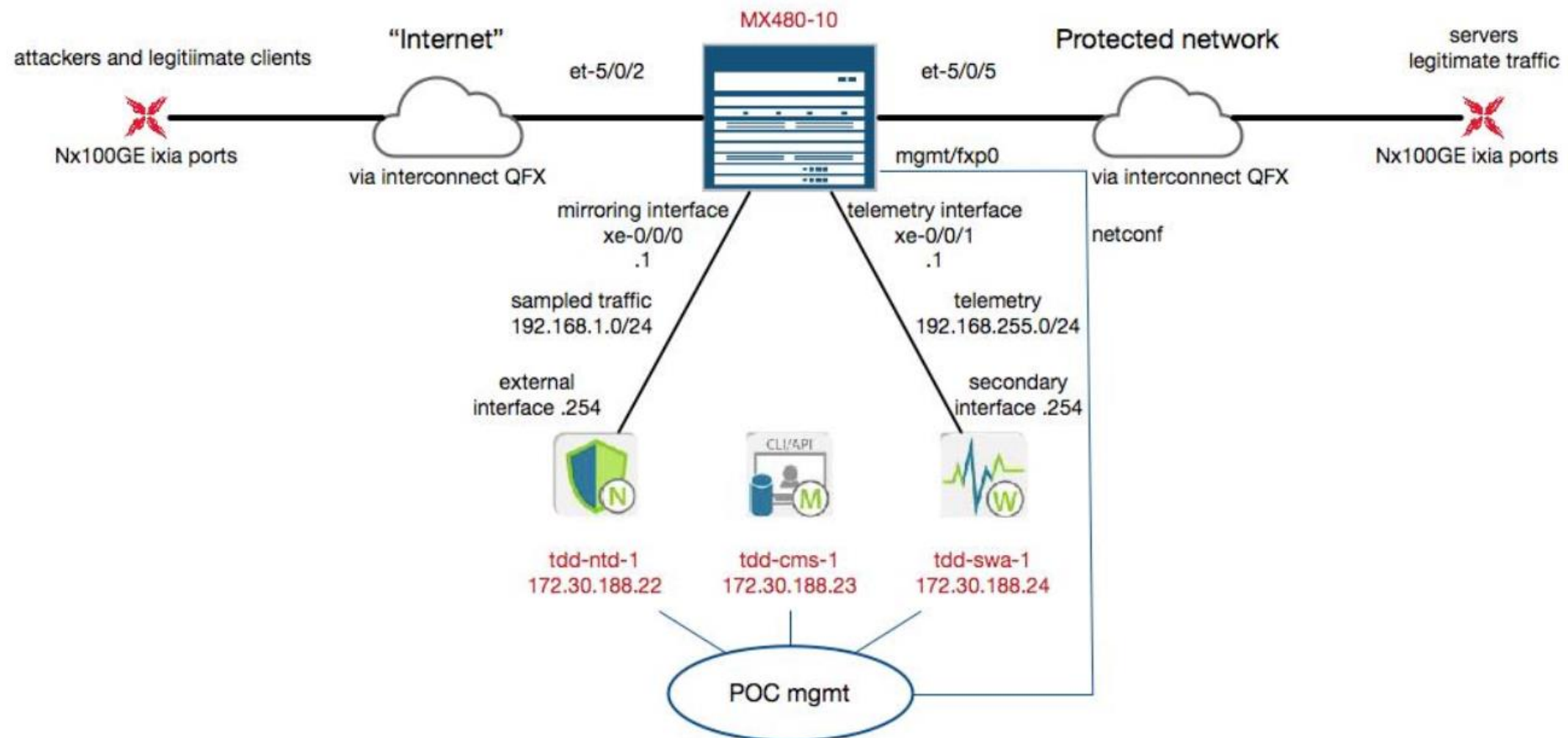
| Product Number | Description | Qty |
|-------------------|--|-----|
| J-COR-DOS-DD-1T-1 | Corero SmartWall Threat Defense Director Virt Edi 1 Yr software subsc. Includes 1 Detection Engine lic, max 5, for up to 1Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity | 1 |

DEMO VIDEOS

Juniper Thread Defense Director



DEMO LAYOUT



The background features a central vertical green bar. On either side of this bar, there are grayscale images of fingerprints, with the ridges and valleys clearly visible. The text is overlaid on the green bar.

Q&A?

THANKS!

Karel Hendrych

Consulting Engineer, EMEA

khe@juniper.net

JUNIPER
NETWORKS

Engineering
Simplicity