corero

Surgical DDoS Attacks

Deployment Models for Effective Protection

Sean Newman
Director Product Management

DDoS Continues to Grab the Headlines!...

500 Gbps Hong Kong attack
France swarmed after terror attack
PlayStation & Xbox hit at Christmas

Anon hits Church of Scientology

Spamhaus attack:

Reported to reach 310 Gbps

Rio Olympics 540

Mirai Botnet
OVH / Krebs / DYN
600 Gbps -> 1Tbps

Spammers discover botnets

ProtonMail attack

First Hacktivists:
Zapatista National Liberation Army

Estonia:
Parliament, banks, media, Estonia Reform Party

Coordinated US bank attacks:
Grew to 200 Gbps, and continue today

DoS for Notoriety

1993　…　2005　2007　2009　2011　2013　2015　2016　2017

The Internet of Things is Coming to get Us!

13+ Billion IoT Devices By 2020
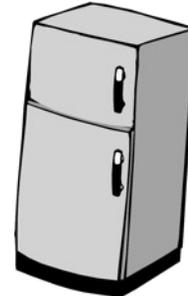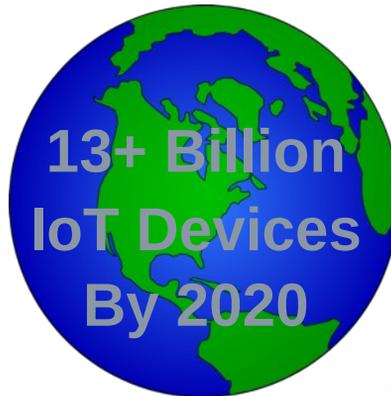
DDoS as a Smokescreen

Surgical Attacks Evade Conventional Defenses

Large attack, but short in duration - triggers detection but too short to mitigate

Ongoing low-level attacks "under the radar"

Inbound Traffic
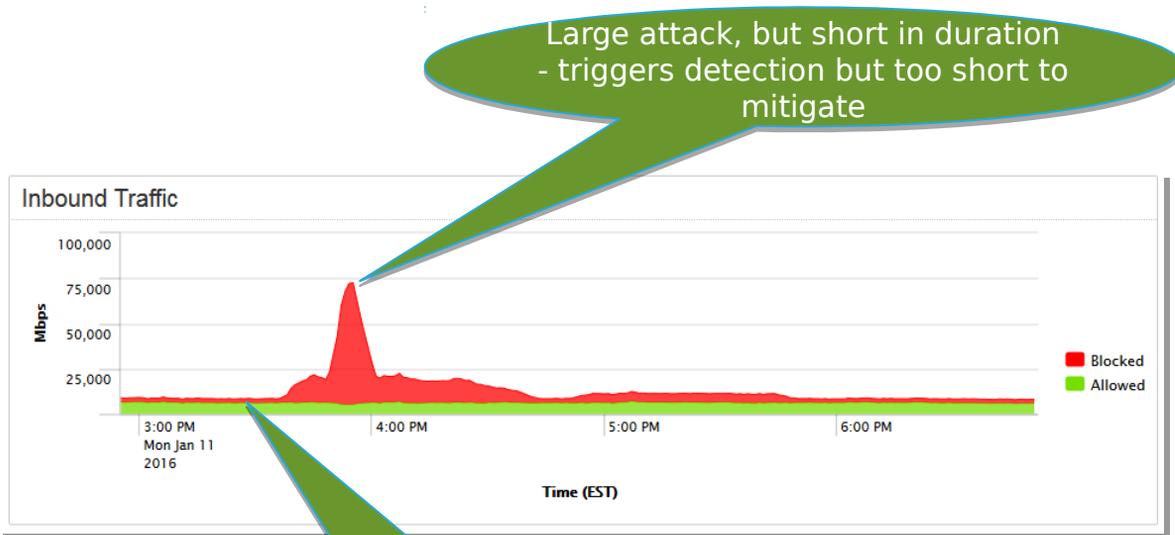
Defending against Surgical DDoS Attacks

DDoS Defense 1.0 – Null Route

Basic DDoS Detection

(NetFlow Collector/Analyzer)

NetFlow

Native Traffic Path

Attack Traffic
Normal Traffic

Null Route
on Destination IP

Customers Offline

All traffic discarded = Attacks perfected
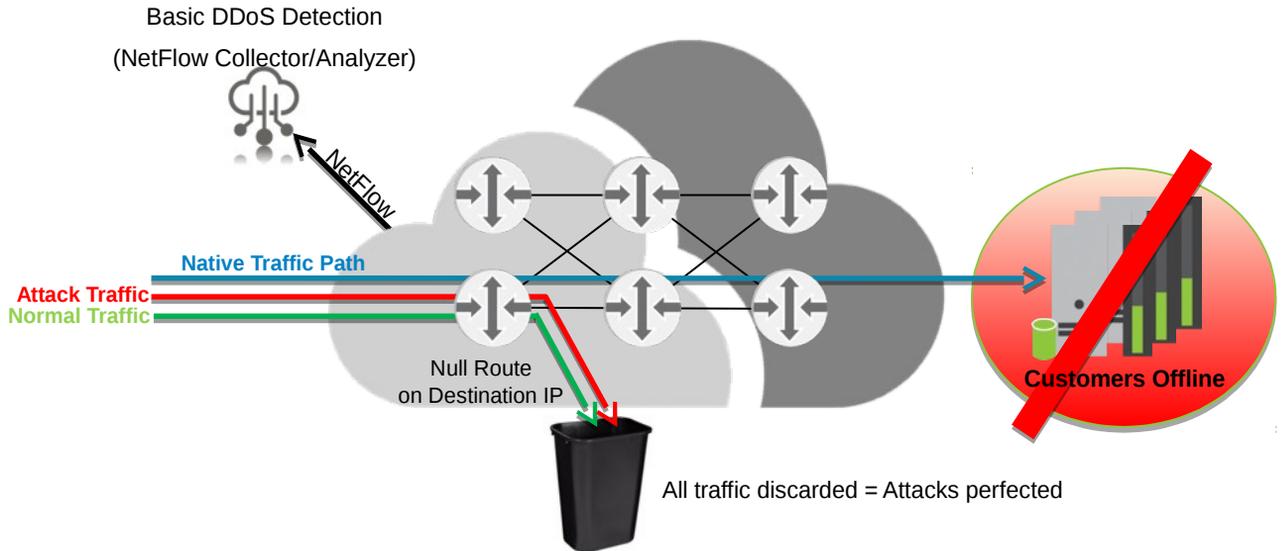
DDoS Defense 2.0 – Out-of-Band Scrubbing

Enhanced DDoS Detection

(NetFlow Collector/Analyzer)

NetFlow

Native Traffic Path

Attack Traffic
Normal Traffic

New Route via BGP

Diverted Traffic Path

GRE Tunnel to Customer

Mixed Traffic

Partially Protected Customers

Offline DDoS Scrubbing
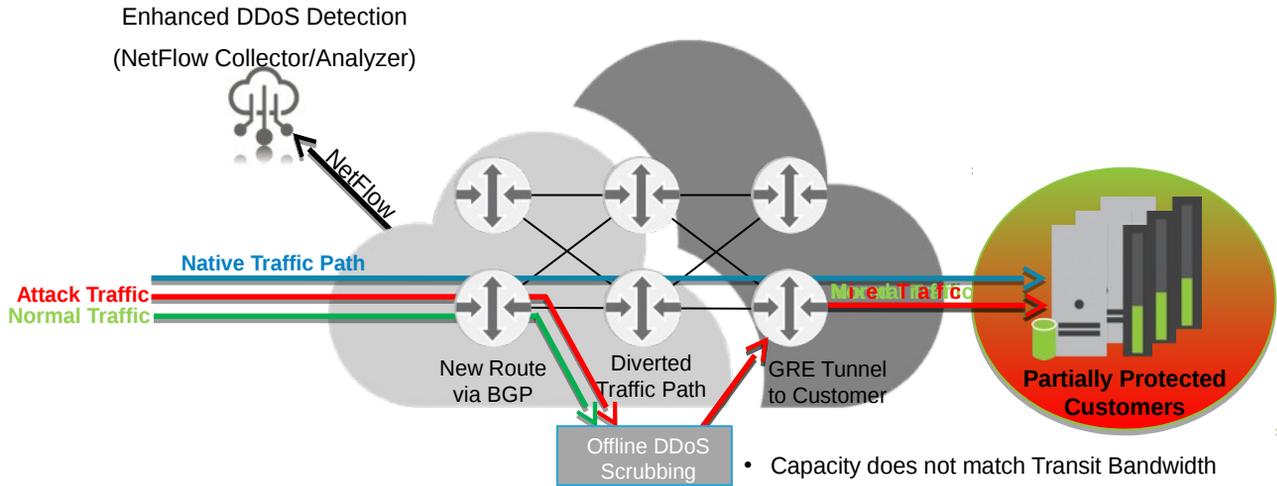
- Capacity does not match Transit Bandwidth
- Delayed Mitigation capability
  - Collector/Analyzer must Alert
  - Typically Manual Intervention Required
  - High False Positive and Negative Rates

DDoS Defense 3.0 – Direct Inline, Always-On

Comprehensive DDoS Analytics

Real-time Alerting and Reporting

Attack Traffic
Normal Traffic

Always-On DDoS

Normal Traffic

Fully Protected Customers

DDoS Traffic

Blocked

Inline

- No Customer Impact from DDoS Attacks
- Near-Instantaneous Mitigation
- Capacity matches Transit/Service bandwidth
- Distributed protection from saturating Attacks
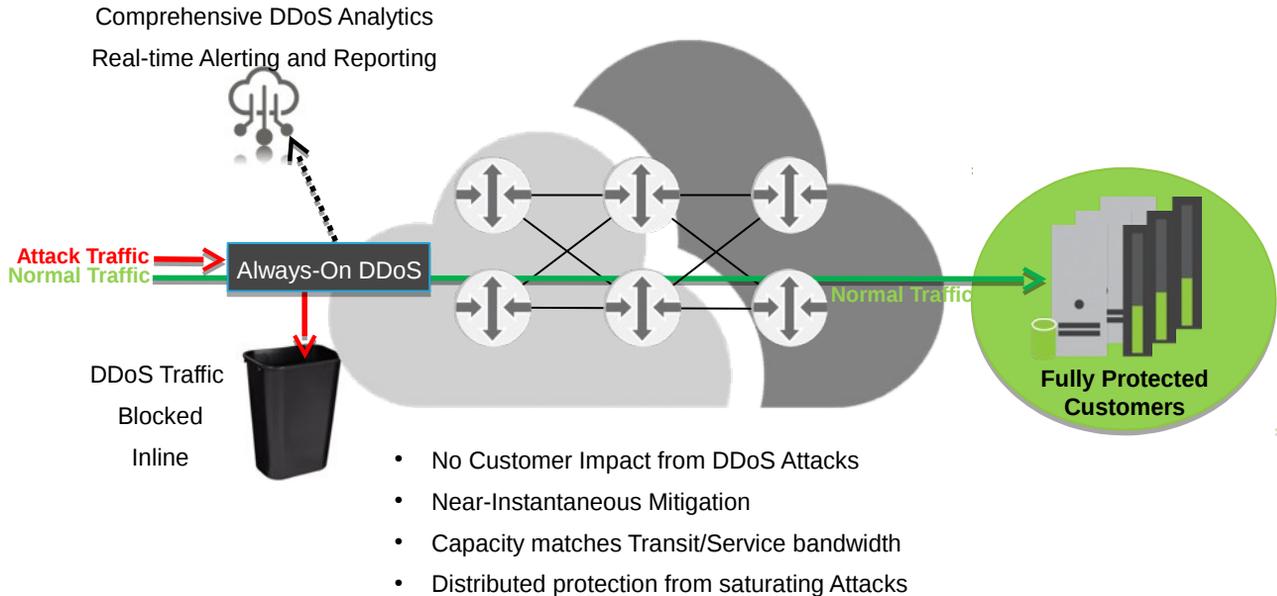
DDoS Defense 3.0 – Virtual Inline, Always-On

Router Redirect =
Forward "All" inbound traffic to dirty VRF

Peering IX

PE Router

"Dirty" VRF Default Route

Global Routing Table

DDoS Protection Array

Egress Traffic routed directly out of interface

Protected Customers
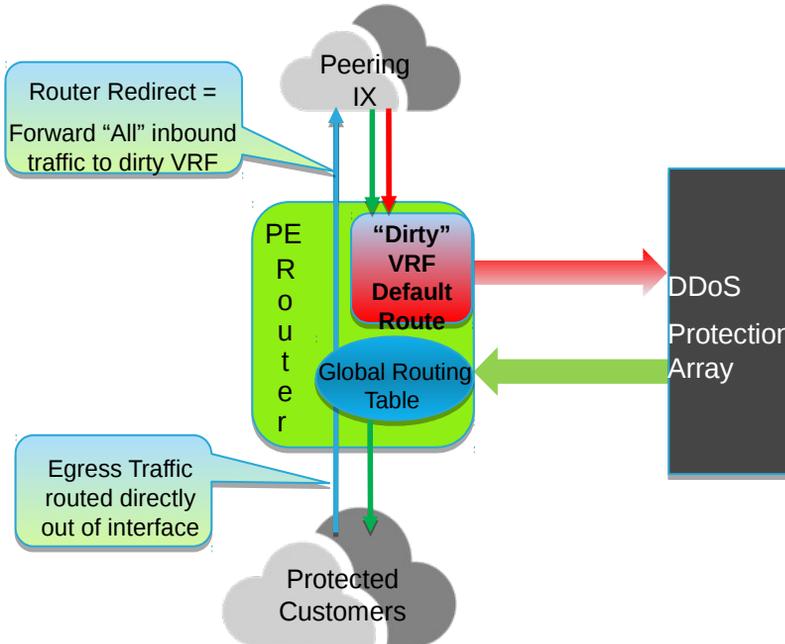
- Inbound Traffic diverted for DDoS Inspection/Mitigation

- Transparent Deployment

- Scales Easily for DDoSaaS

- Redundancy provided via Network LAG – N+1

- Virtual Router Forwarding Instance (VRF) Supported by most L3 Switch Router Vendors

- VRF prevents routing loops

Summary

- **It's not all about the massive DDoS Saturation Attacks**
  - They're less than 2% of all DDoS
- **'Surgical' Attacks are constant threat to online availability**
  - Basic Null-Route detection is blind to low-level attacks
    - And leaves customers completely offline for duration of attack
  - Traditional Out-of-Band Scrubbing is too slow for short sharp attacks
    - Damage is done before mitigation engages, leaving customer offline
- **Always-On, Real-time, DDoS Protection is a reality**
  - Protect your infrastructure, as well as your customers'
  - Sell to customers 'as a service' and generate incremental revenue
  - Easy to scale as you and your customer base grows

Questions?

Thank You!