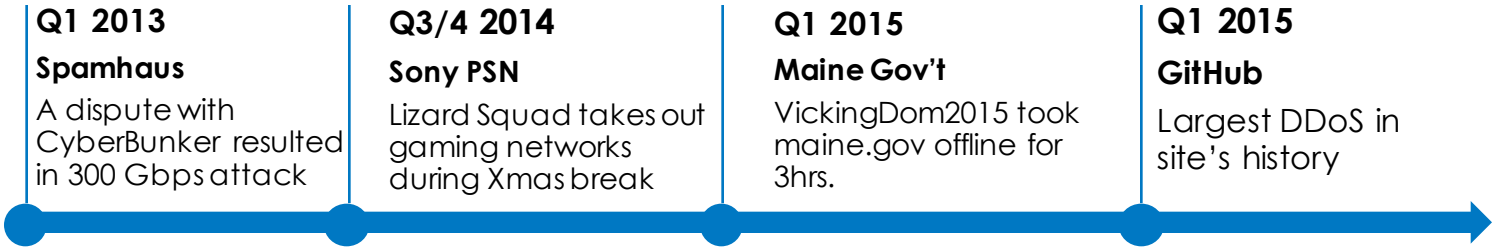
Thunder TPS

Overview

DDoS in the News



"Enterprise and mid-sized hosting provider demand for on-premises DDoS prevention solutions is growing every day"

Source: Infonetics

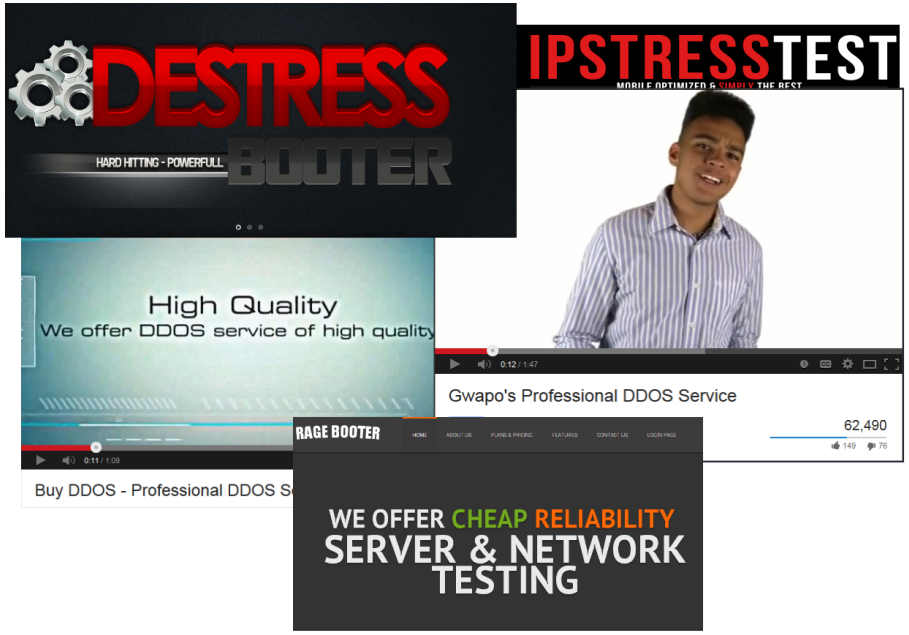
The Line is Going Up

159 attacks >100G in 2014

15% increase in number of attacks against public-sector targets Q4 of 2014

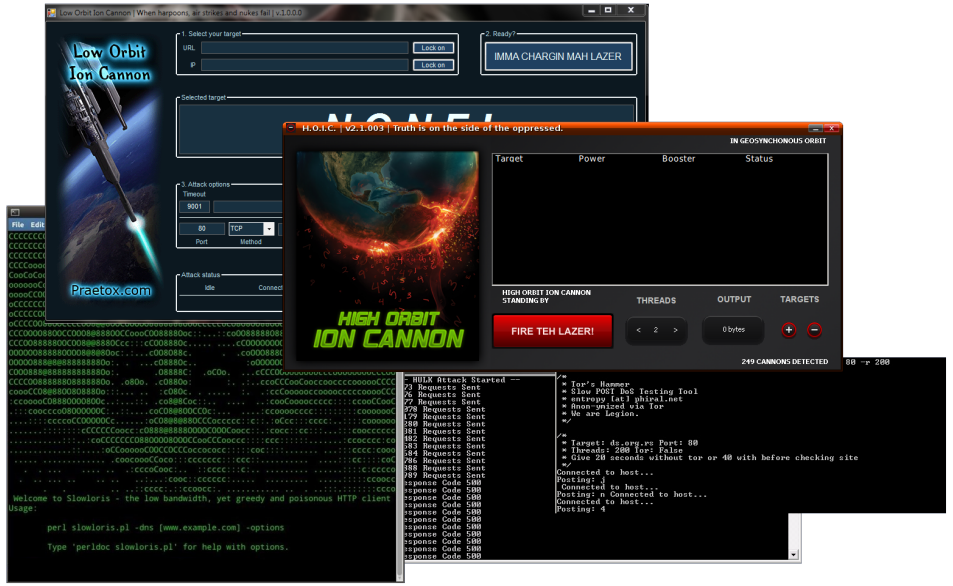
52% increase in average peak bandwidth from Q3

Services and Toolkits Make it Easy to Launch DDoS Attacks



DDoS for hire services, often called "booters," or "Stressers":

- advertise on YouTube & forum posts.
- Services can cost as little as $2 per hour



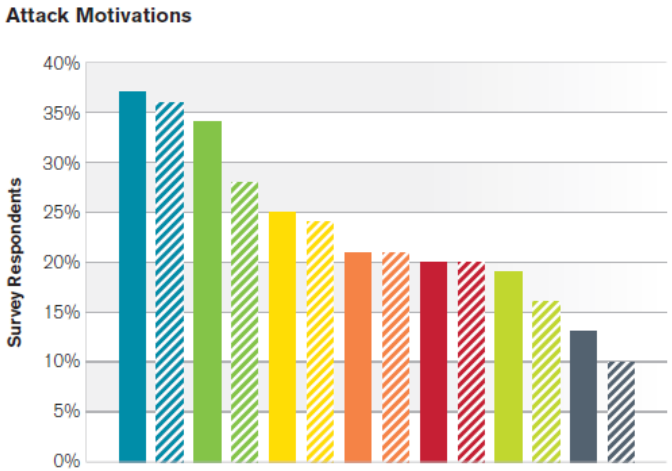
Off-the shelf attack tools allow even unsophisticated attackers and hacktivists to take down websites

- Low Orbit Ionic Canon (LOIC)
- High Orbit Ionic Canon (HOIC)

Evolution of Attacker Motivations

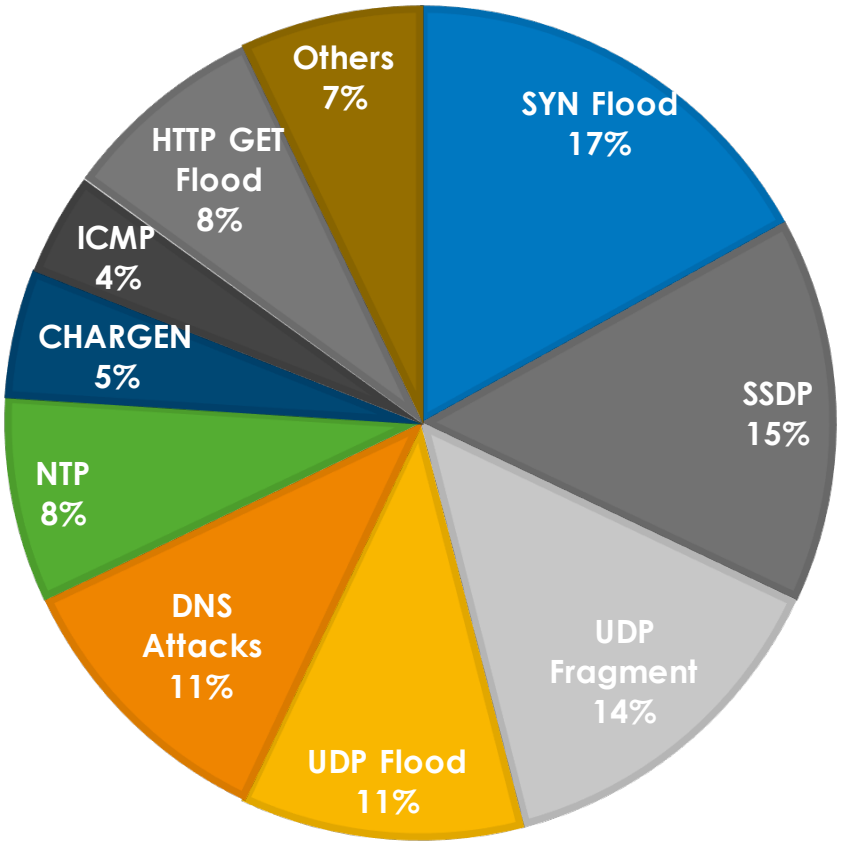
DDoS has evolved into a complex threat with multiple tactics and targets

- Various Attacker Motivations
  - Notoriety, extortion, hactivists, diversionary tactics
  - Organized groups constantly change techniques to attack governments, financial institutions and other online organizations
  - Low Barrier to Entry - Botnets are cheap to rent, readily available and easy to manage[2]



- **37%** Nihilism/vandalism
- **36%** Online gaming-related
- **34%** Political/ideological disputes (i.e., WikiLeaks/Anonymous, nationalism, religious controversy, etc.)
- **28%** Criminals demonstrating DDoS attack capabilities to potential customers
- **25%** Social networking-related (i.e., IRC, chat networks, Facebook, Twitter, Google+, etc.)
- **24%** Online gambling-related
- **21%** Misconfiguration/accidental
- **21%** Inter-personal/inter-group rivalries (i.e., individual disputes, schools, sports teams, etc.)
- **20%** Criminal extortion attempt
- **20%** Financial market manipulation
- **19%** Diversion to cover compromise/data exfiltration
- **16%** Flash crowds
- **13%** Competitive rivalry between business organizations
- **10%** Intra-criminal disputes

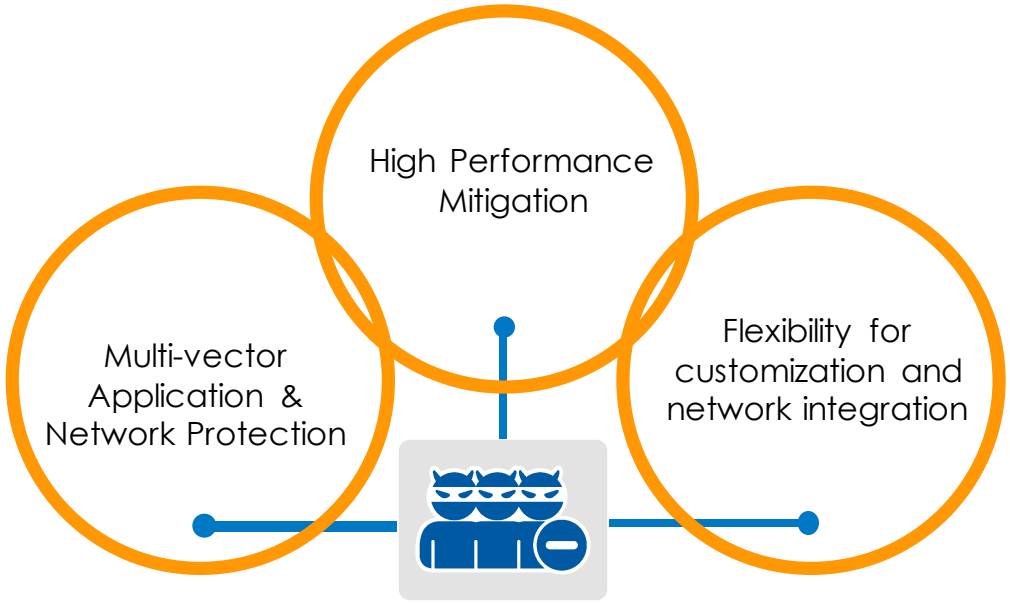
The Usual Suspects Are Still Responsible for Most Attacks



DDoS Trends		
Total Attacks	↑	Up 90% from 2013
Multi-Vector	↔	Roughly half of all attacks
SSDP	↑	New entrant in the DDoS arsenal accounts for 15% of attacks – can amplify attacks up to 30x
App Attacks	↓	Down 16% year-over-year; accounts for ~10% attacks
Attack Duration	↑	Up 28% to 29 hours

Introducing Thunder Threat Protection System (TPS)

Thunder Threat Protection System (TPS)



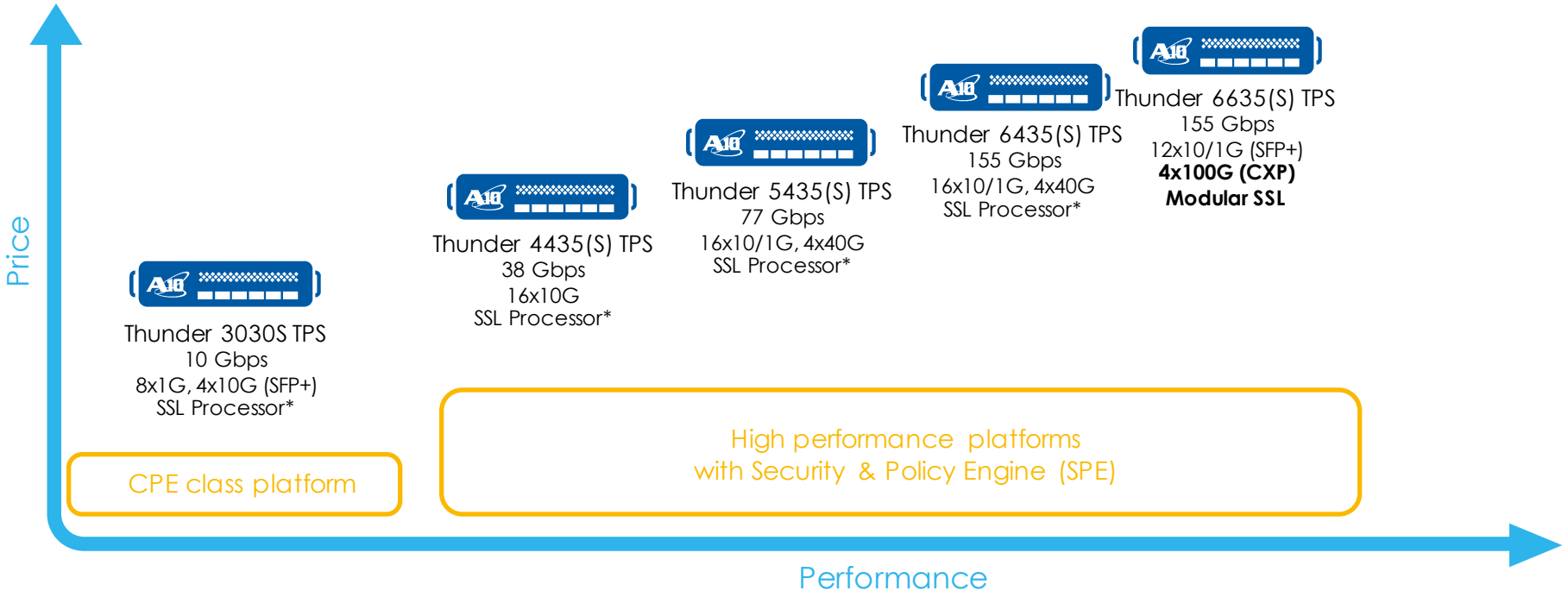
Next Generation DDoS Protection

Multi-vector Protection
- Detect & mitigate application & network attacks
- Multi-level traffic visibility
- **60** Hardware mitigations

High Performance
- Mitigate Up to **155 Gbps** of attack throughput, **223 M** packets per second (pps) in 1 rack unit
- **64k** protected objects
- **8 x 16M** black/white list capacity

Flexibility for customization and network integration
- Programmatic Policy Engine
  - aFleX
  - RegExp
  - BPF
- SDK/RESTful API for 3rd party integration
- Many deployment modes
  - Asymmetric
  - Symmetric
  - TAP mode
  - Hybrid

Mitigation: Thunder TPS Appliances



Thunder TPS Performance

	Thunder 3030S TPS (CPE)	Thunder 4435 TPS	Thunder 5435 TPS	Thunder 6435 TPS	Thunder 6635 TPS
Mitigation Throughput^	10 Gbps	38 Gbps	77 Gbps	155 Gbps	155 Gbps
Cluster Throughput^^	80 Gbps	300 Gbps	600 Gbps	1.2 Tbps	1.2 Tbps
TCP SYN Auth/sec PPS*	6.5 million	35 million	35 million	70 million	70 million
SYN Cookies/sec PPS**	6.5 million	55 million	112 million	223 million	223 million
DDoS Attack Detection and Mitigation	Software	Software + hardware assist	Software + hardware assist	Software + hardware assist	Software + hardware assist

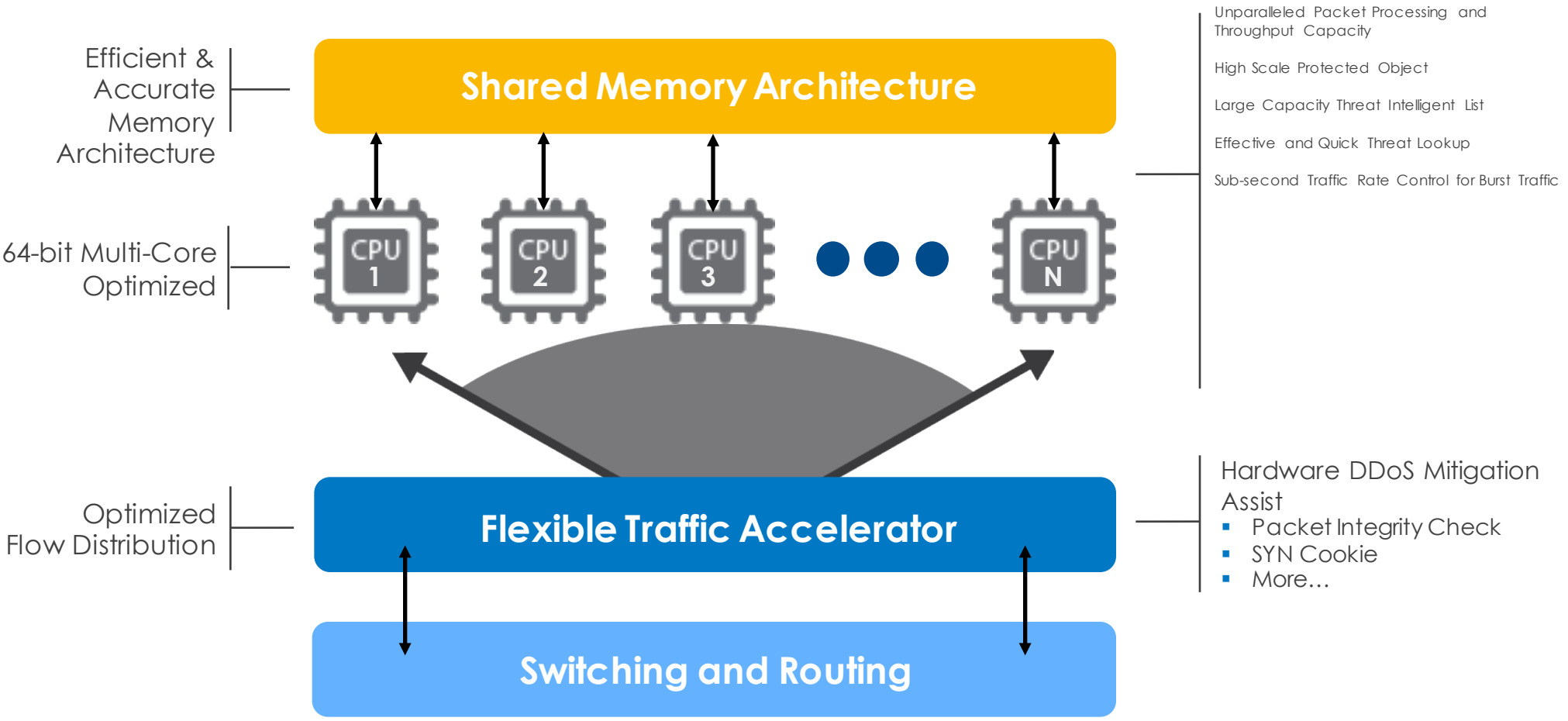
^ All numbers above are measured with DDoS Mitigation enabled, and NOT normal L2/L3 (switching/routing) numbers
^^ List Synchronization Cluster Throughput
* Packets per second - CPU-based performance
** Packets per second - Hardware(FTA)-based performance

Thunder TPS Protected Object Capacity

- Granular mitigation per object by applying specific rules
  - E.g. port, protocols and subnets
- Competitor supports up to 2k managed objects only for example
- Protected object logging

Protected (Watched) Objects	Value
Destination Entry ▪ IPv4 Host / Subnet ▪ IPv6 Host / Subnet (including Source-Destination Pair entry)	64k
Source Entry ▪ IPv4 Host / Subnet ▪ IPv6 Host / Subnet	64k
HTTP URI	128 per template
Destination L4 Port and Protocol	512 per destination IP

ACOS: Optimal Platform for DDoS Mitigation

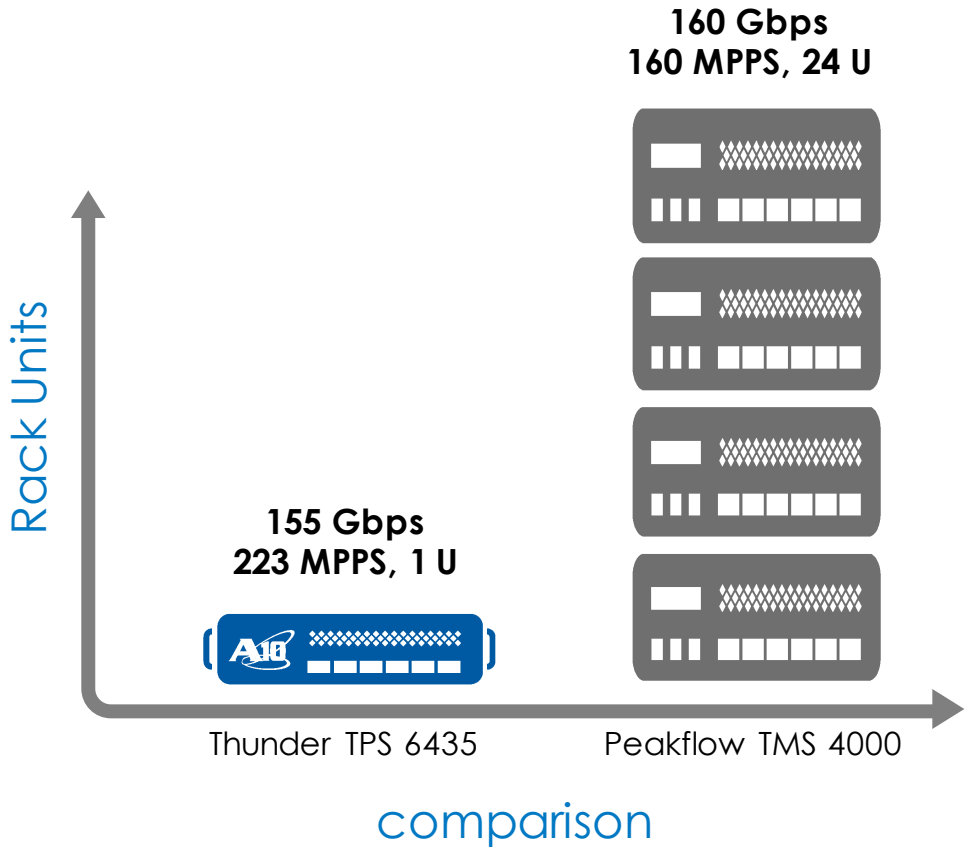


Flexibility, Programmability and Ease of Integration

- Customize with aFleX (TCL-based)
- Pattern matching with
  - Regular Expressions (regexp)
  - Berkeley Packet Filter (BPF)
    - tcpdump, Wireshark
- RESTful API
  - ACOS is 100% API driven
  - 100% parity between CLI and API
- TAP mode for monitoring only, or use in hybrid mode with inline or asymmetric
- Monitoring mode to monitor new policies
- Common Event Logging (CEF) to integrate with 3rd party

Thunder TPS for Top US Service Provider

- Benefits:
  - Higher Mitigation Throughput
    - 155 Gbps (TMS 6435) compared to 40 Gbps (TMS4000)
  - Reduced data center footprint
    - 1RU compared to 6RU (TMS4000)
  - Easily integrated into existing detection system
    - Flowtrack
    - Deepfield
  - Lower Price
    - Arbor - high price and annual S&M costs
  - Inbound and Outbound DDoS Protection
    - Arbor has limited outbound protection.

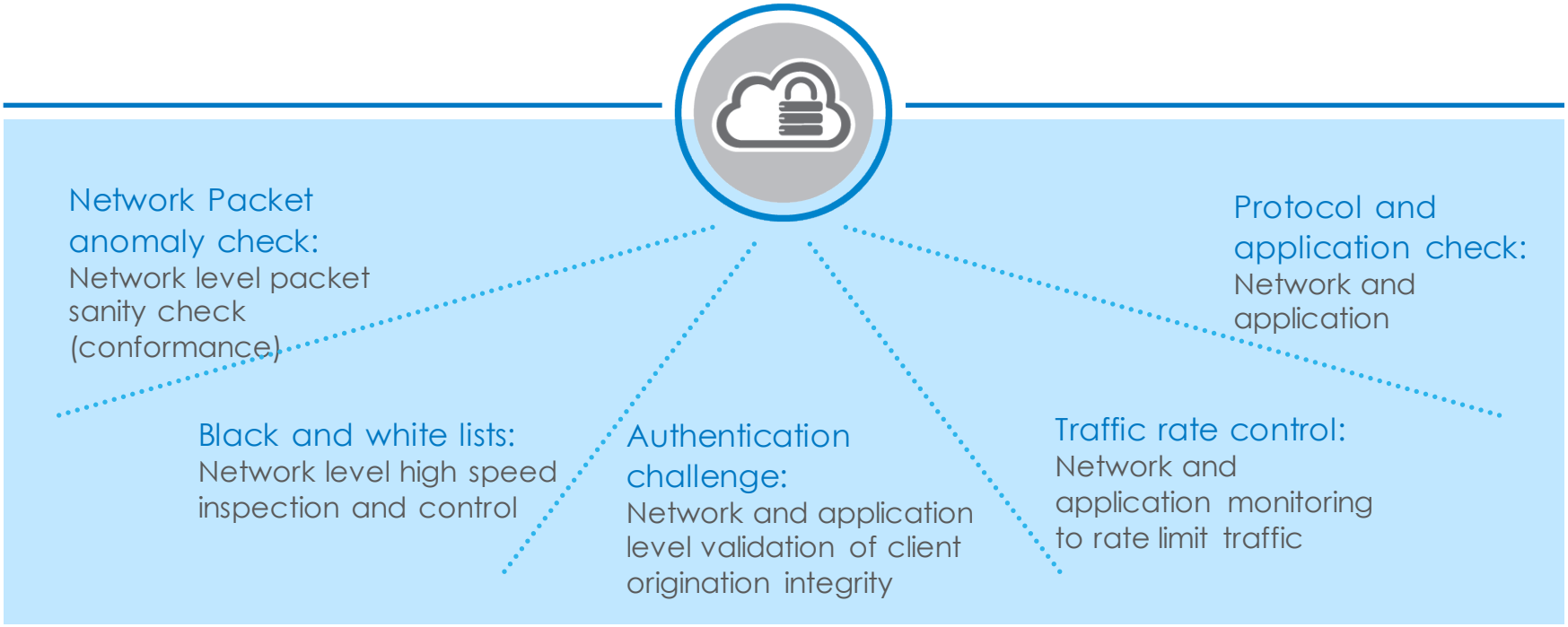


comparison

Multi-vector Application & Network Protection

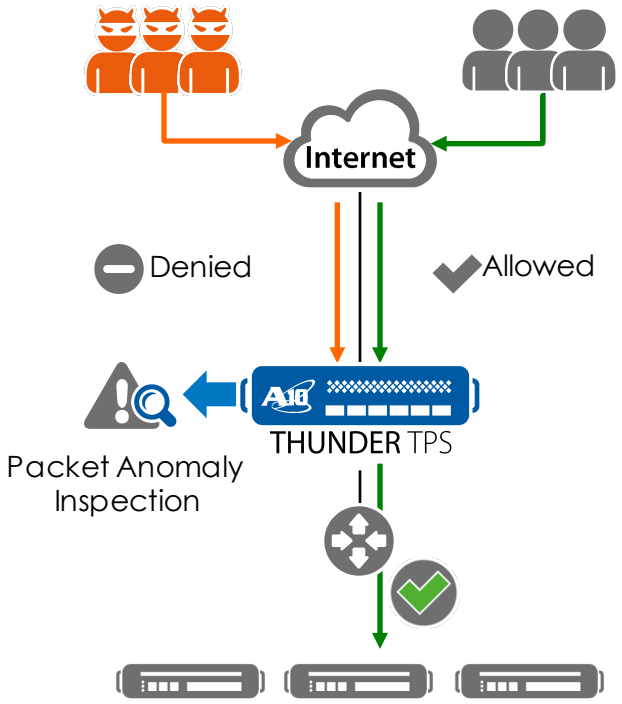
Mitigating DDoS Attacks

Five principal methods for effective mitigation



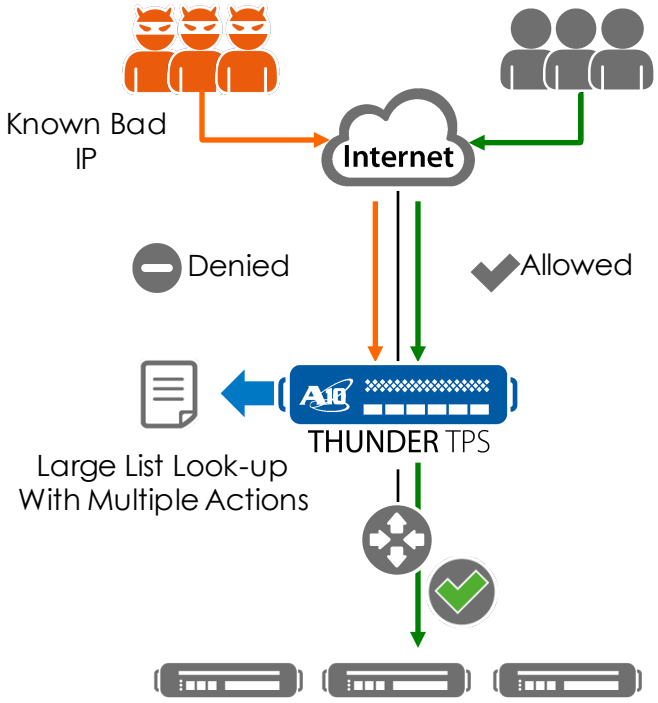
Network Packet Anomaly Check

- Packet sanity check (conformance) in hardware and software
  - Prevents volumetric attacks and protocol attacks
  - Network checks (L3-4) for standard behavior
- Examples
  - TCP SYN & FIN, TCP XMAS, TCP SYN Flag, TCP Bad Checksum, UDP Bad Checksum, Runt Packet, more…



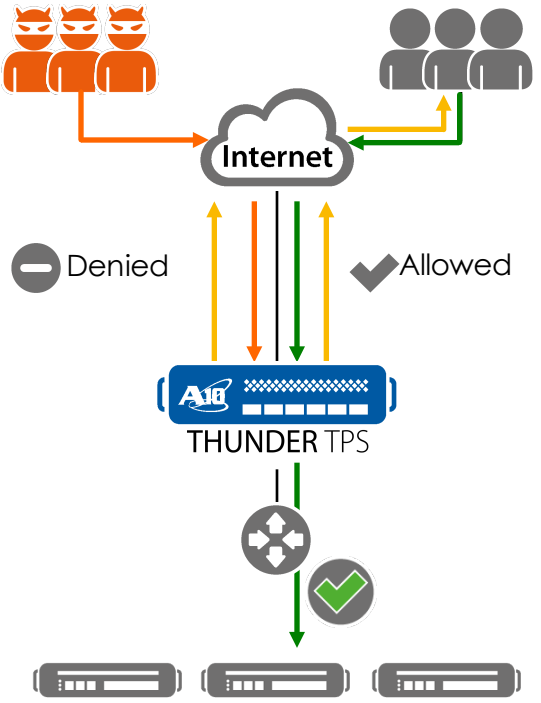
Black and White Lists

- High speed inspection and control of good and bad sources
  - Prevents known bad clients
  - 8 x 16 M entries list capacity
  - Network level enforcement (L3-4)
- Examples
  - Import 3rd Black/White Lists, Dynamic creation from SYN Cookie, SYN authentication & Action-on-ACK, Dynamic White List with DNS authentication & spoof detection, Dynamic Black List with scanning detection, TCP abnormal packets threshold, HTTP header filter, more…



Authentication Challenge

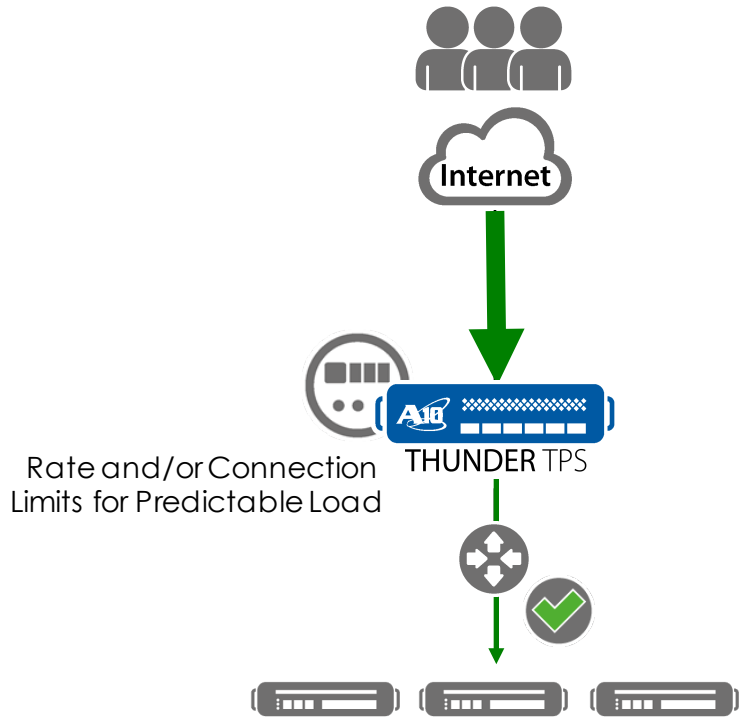
- Validates client origination integrity
  - Bot detection
  - Prevents volumetric and protocol attacks
  - Network and application checks (L3-7)
- Examples
  - TCP SYN authentication, TCP SYN cookie, TCP Action on ACK, UDP authentication, DNS authentication, HTTP Challenge, TCP error packet limit, more…



Traffic Rate

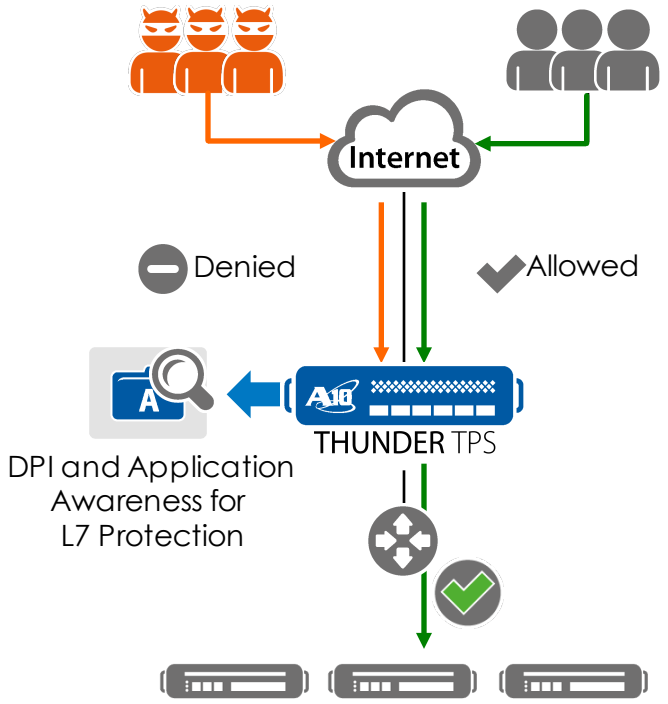
- Monitor and rate limit traffic
  - Network and application level enforcement (L3-7)
  - Configurable over-limit actions for TCP, UDP, HTTP and DNS
  - Rate limit *per connection (*TCP or UDP) for ultra-granular control
  - Bandwidth or packet rate control

- Examples
  - Connection limit, Connection rate limit, Fragment rate limit, Packet rate limit, HTTP Request rate limit, DNS request limit per DNS Record Type, SSL request rate limit, more…



Protocol and Application Behavioral Checks

- Monitor and check traffic behavior
  - 400+ global, destination-specific and behavioral counters
  - All counters available through GUI, CLI, sFlow export
  - Enforce specific values
  - Network and application checks (L3-7)
- Examples
  - TCP template, HTTP template, DNS template, UDP template, SSL-L4 template, Scan detection, aFleX scripting, more…
  - HTTP example Slowloris
  - SSL authentication as bot detection
  - POODLE attack protection

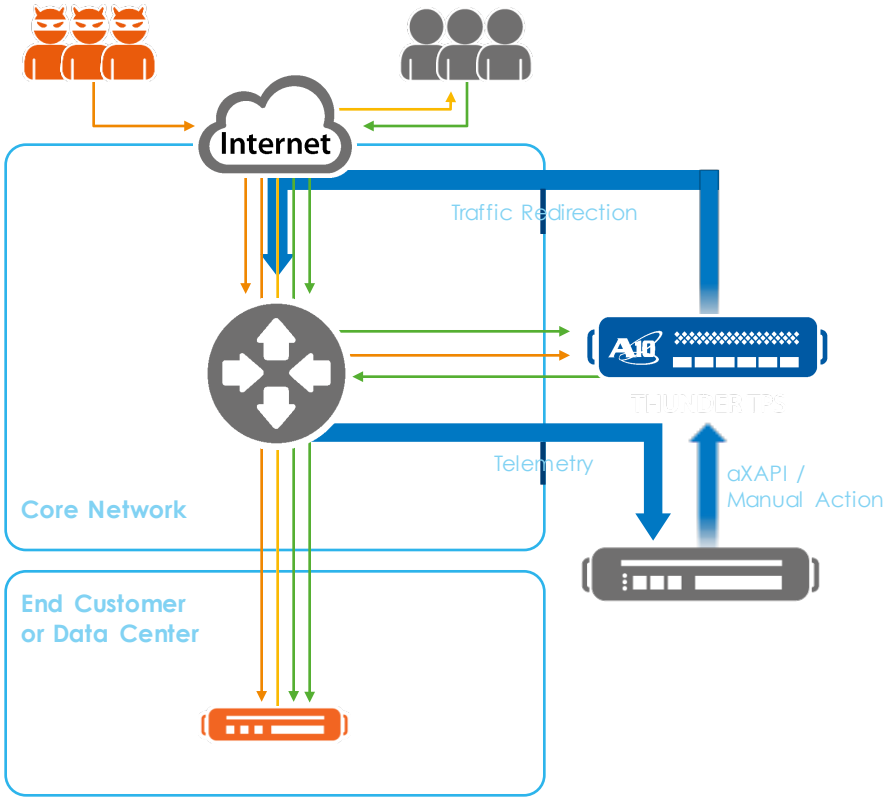


Flexibility for customization and network integration

Flexible and broad deployment options

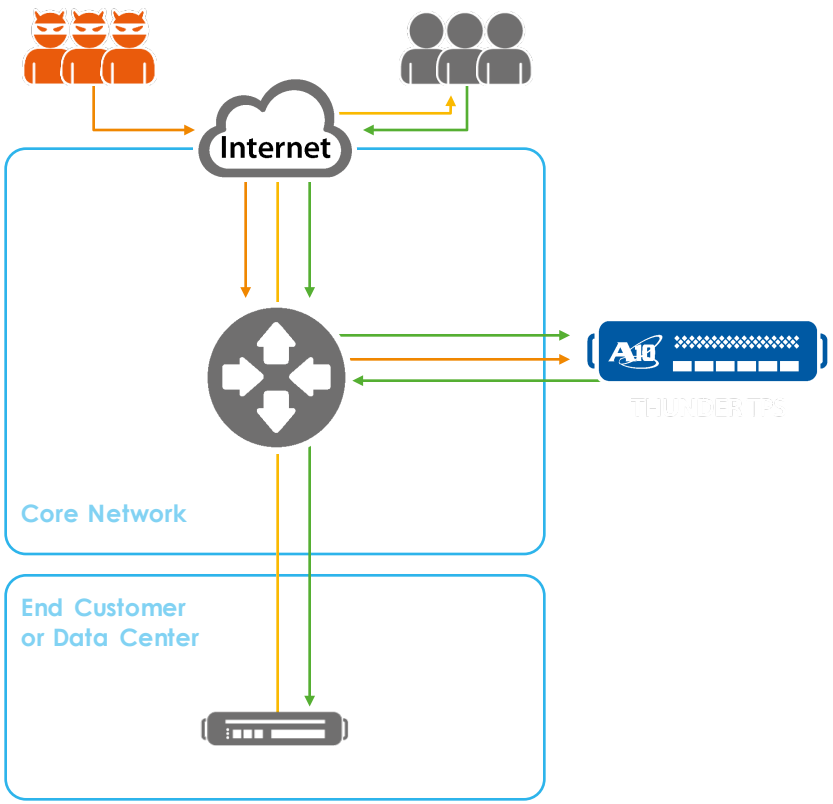
- Asymmetric deployment
  - Reactive
  - Proactive
- Symmetric (inline) deployment
- Out-of-band (TAP) deployment

Asymmetric Reactive Deployment



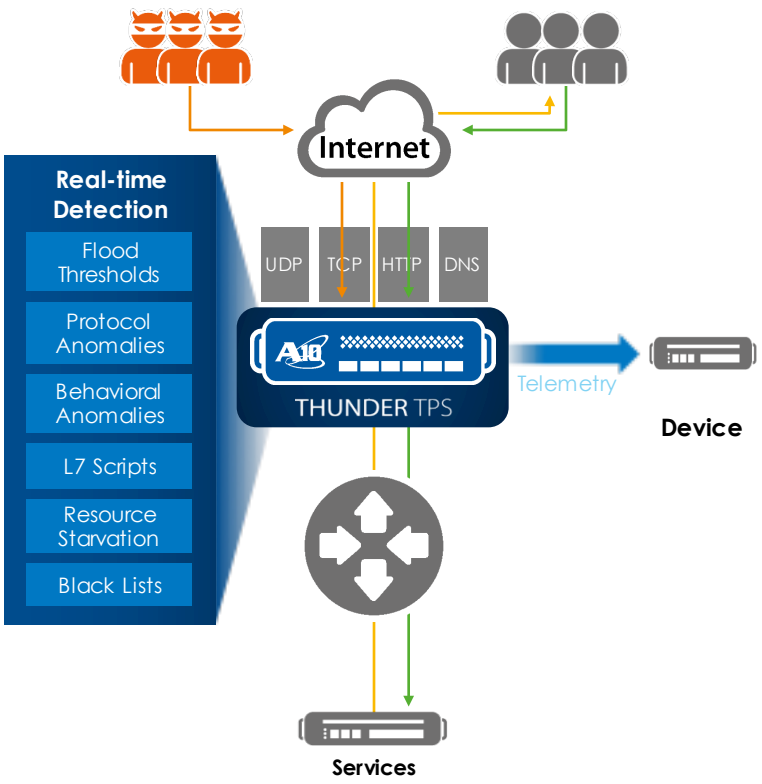
- Asymmetric Reactive deployment
  - Classic deployment model
  - Scalable solution for DDoS mitigation
    - Oversubscribed bandwidth deployment
    - No additional latency in peace time
    - Longer time to mitigate (Flow-based detection)
  - Suitable for Service Providers
    - Protecting select services
    - Large scale core network
- Profile
  - Traffic redirected to TPS for scrubbing as needed
    - Support BGP for route injection
  - Valid traffic forwarded into network for services
    - Support GRE & IP-in-IP tunneling

Asymmetric Proactive Deployment



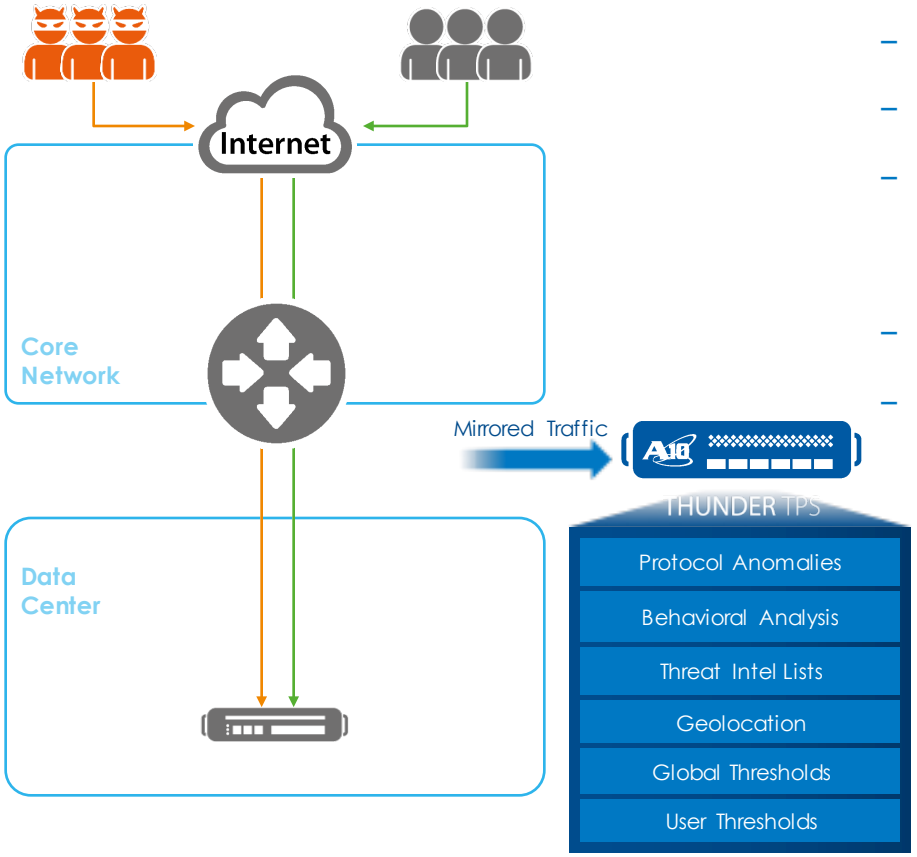
- Asymmetric Proactive Deployment
  - For high performance DDoS detection and mitigation
  - DDoS detection and mitigation in one box
  - Suitable for Large Enterprises and ISPs
    - Protecting own services
    - Protecting end customers
    - Large-mid scale core network
- Profile
  - Inbound traffic always routed toward TPS
    - For high risk customers
  - DDoS detection at sub-second scale

Symmetric Deployment



- Symmetric Deployment
  - Inline DDoS detection and mitigation in one box
  - Inspect both inbound and outbound traffic
  - Suitable for Enterprises
    - Protecting own services
    - Permanent protection
    - Sub-second detection-to-mitigation
- Profile
  - Detect and inspect L3 – L7 traffic for both inbound and outbound traffic
  - Deep statistics sFlow export
  - DDoS detection and mitigation at sub-second scale

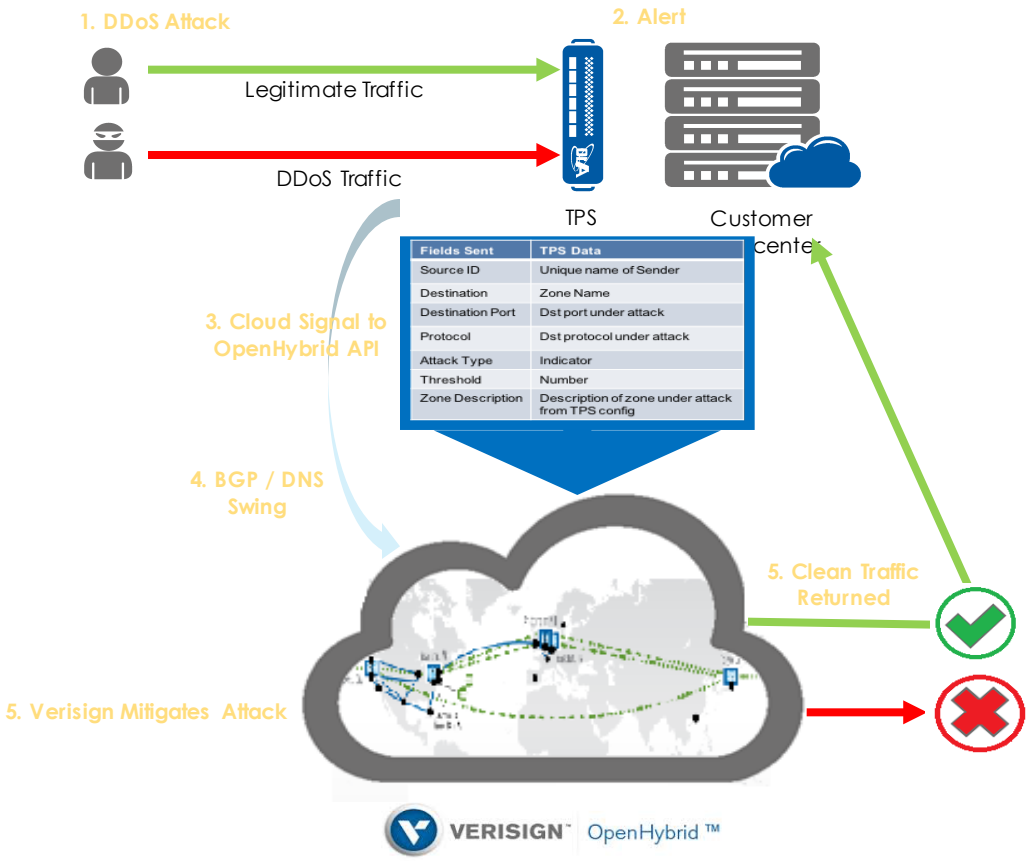
Out-of-Band (TAP) Deployment



- Out-of-Band (TAP) Deployment
  - High Speed DDoS Detection Capability
  - Receive and analyze mirrored traffic data from routers
  - Build dynamic Black/White lists
    - Function as black/white list master
    - Synchronize lists with cluster members
  - Hybrid mode supported
  - DDoS statistics and counters for DDoS detection

A10 TPS + Verisign Integration

ACOS 3.2 Detection/Mitigation + Cloud Signaling

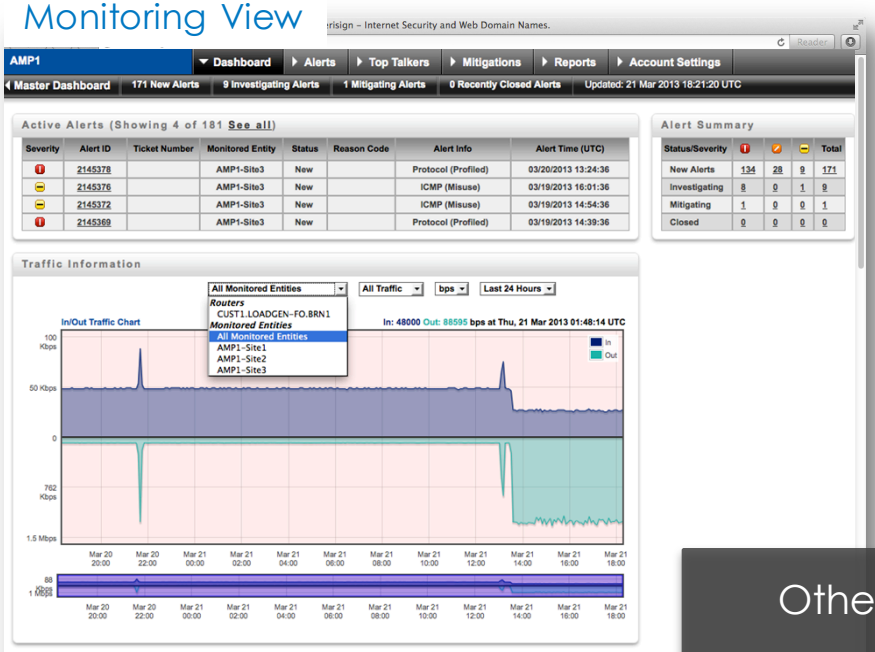


- A10 TPS deployed within customer's network
- TPS learns traffic patterns
- TPS detects incoming attack
- TPS performs on premise mitigation
- Attack is identified – Cloud Signaling initiated
- Verisign's SOC Engineer works with customer to initiate traffic redirect
- Traffic is re-routed via BGP or DNS
  - BGP
    - Must divert a minimum of a /24 subnet
    - Traffic returned via GRE
  - DNS
    - DNS A records are modified to point attack FQDN to Verisign cloud
    - Clean traffic is sent to its destination

VERISIGN CUSTOMER PORTAL

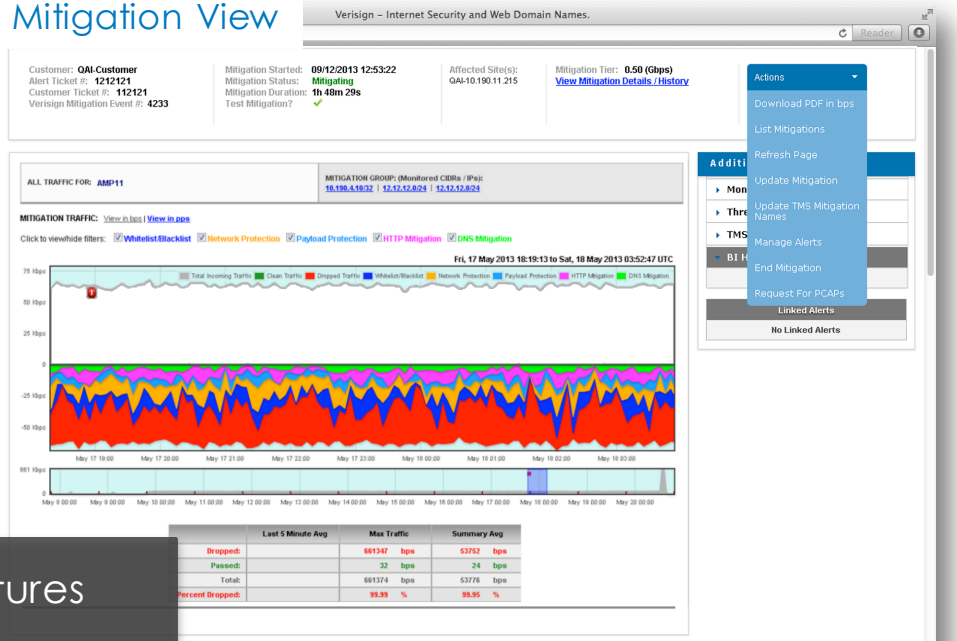
- **An intuitive customer portal with real-time view into traffic and attack protection**

Monitoring View



- Real-time alert reporting on attack activity
- Integration of on-premise and cloud alerts from OpenHybrid sources
- RESTful API to retrieve monitoring alerts in JSON format

Mitigation View



- Track the start time and duration of attack
- Clean and drop traffic by countermeasure
- Drill down into specific time periods of any event

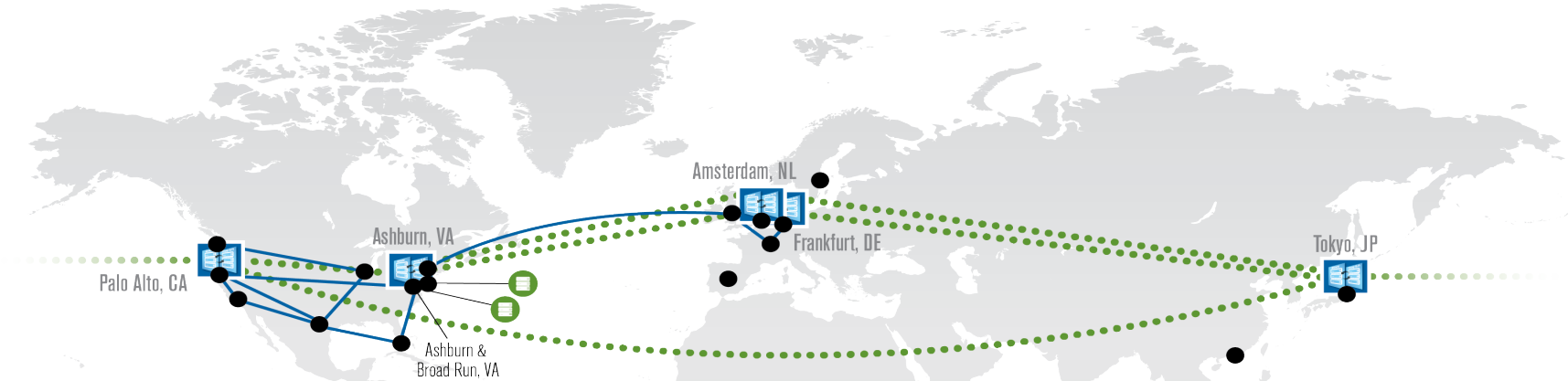
Other Features

- Detailed top talkers
- Hierarchical architecture for global customers
- Downloadable reports

PURPOSE-BUILT GLOBAL NETWORK

VERISIGN

- **High Redundancy, Massive Scale, Minimal Latency**



2+ Tbps Global Capacity & Global Peering

Directly connects with over 700 networks at 1,200 points of interconnection

Flexibility in Returning Clean Traffic

Scrub Centers
Network POP
Monitoring Centers

A10 TPS 3.2 Update

Behavioral Monitoring & Anomaly Detection

Protected Zones

- A new container type for property configuration
- Can group multiple destination IPs/subnets
- Holds the new mitigation policy
  - Destination policy and source-based policies
  - Thresholds and countermeasures for each level of the escalating mitigation policy – for automatic escalation & mitigation
- Helps maintain backward compatibility
  - Protected destinations are retained as is

Multi-Protocol Behavioral Indicators

Packet, session, and ratio metrics enable comprehensive profiling and facilitate detection of anomalies

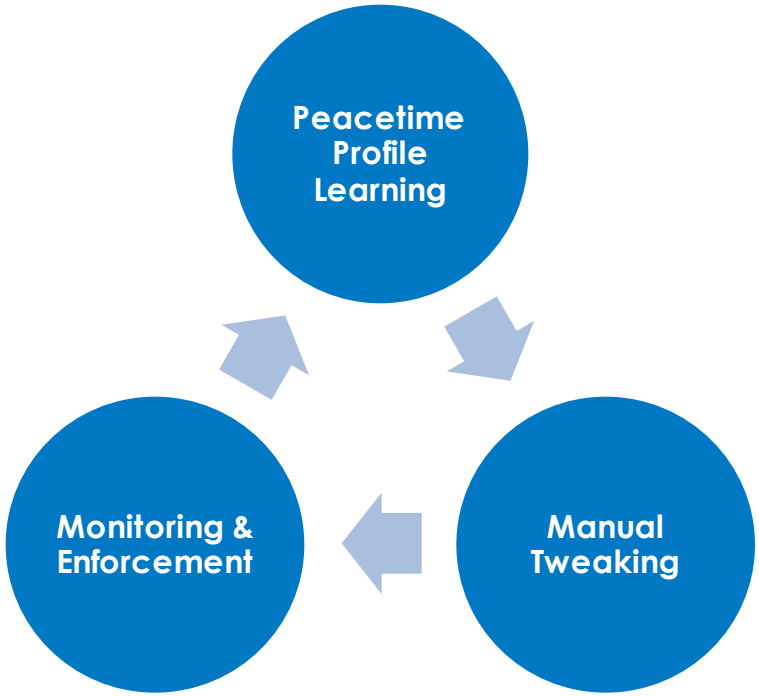
TCP	
Packet Rate	Empty ACK Rate
Packet Drop Rate	Small Payload Rate
SYN Rate	Session Miss Rate
FIN Rate	Bytes-to / Bytes-from
RST Rate	SYN Rate / FIN Rate
Small Window ACK Rate	Packet Drop / Packet Received
Concurrent Sessions	

UDP
Packet Rate
Packet Drop Rate
Bytes-to / Bytes-from
Packet Drop / Packet Received
Concurrent Sessions

ICMP	
Packet Rate	Bytes-to / Bytes-from
Packet Drop Rate	Packet Drop / Packet Received

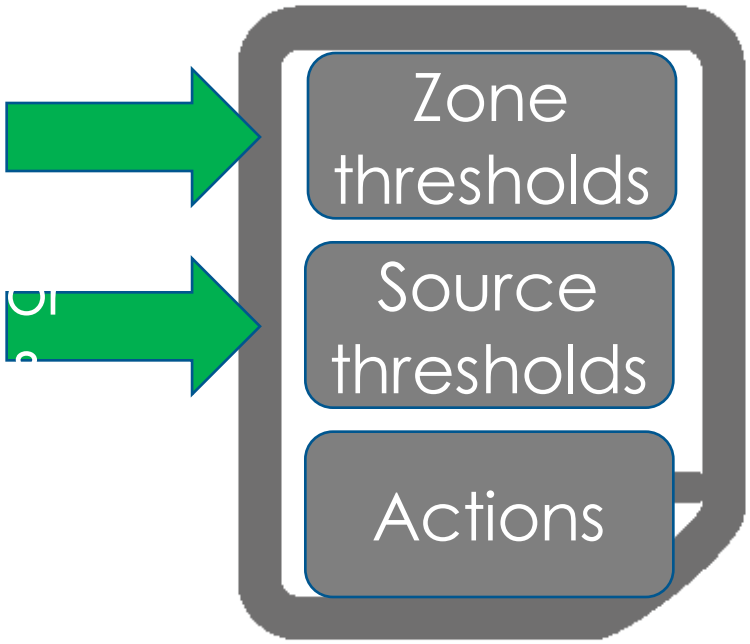
IP/Other	
Packet Rate	Bytes-to / Bytes-from
Packet Drop Rate	Packet Drop / Packet Received
Fragment Rate	

Operational States

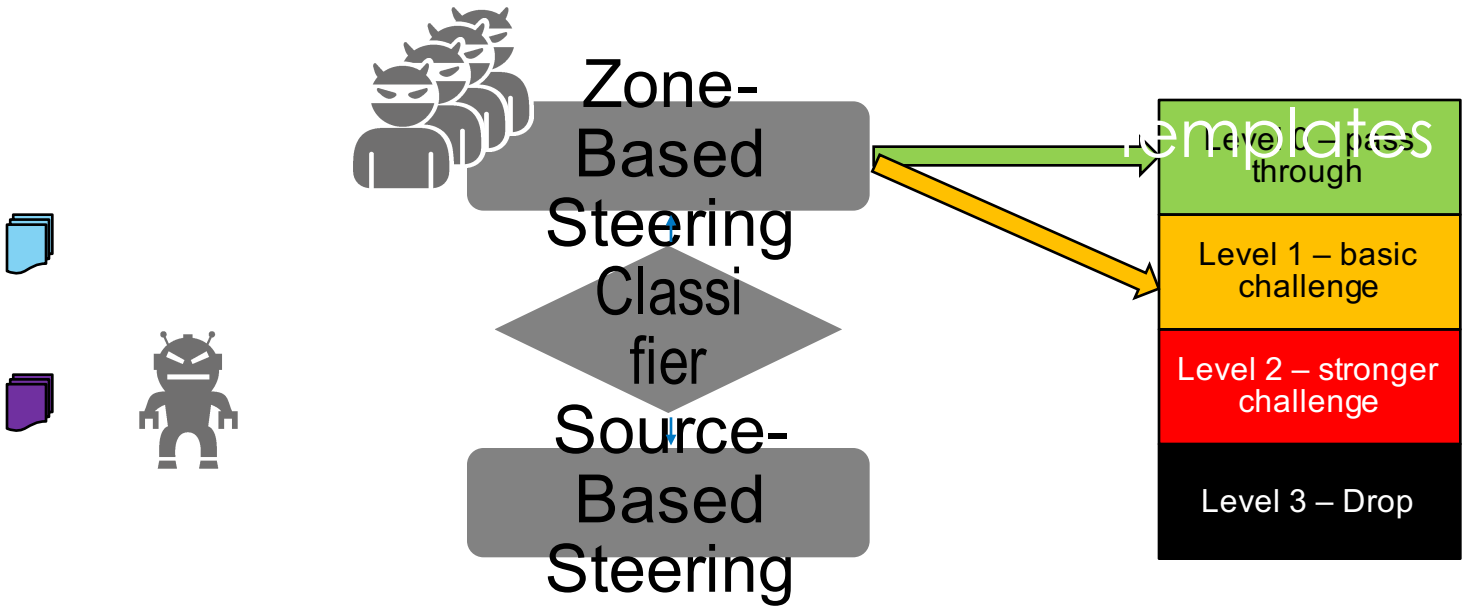


Protection lifecycle - Learning

- Monitor per protected object indicator levels
- Monitor typical source indicator levels
- Build peacetime profile and thresholds



Mitigation – escalating templates



Thank you