

CryptoPanel

27 MAJA 10:00

Bezpieczeństwo danych to nie tylko poufność, ale też ich dostępność.

Dyskusje poprowadzą: Piotr Wróbel i Bartosz Chmielewski



THALES
Building a future we can all trust

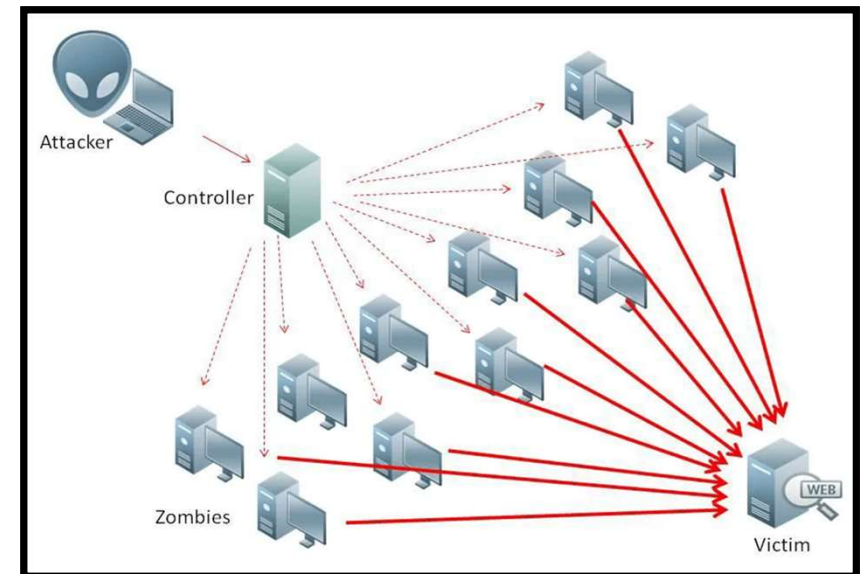
imperva
a Thales company

CLICO



The nature of DDoS attacks and why they are so dangerous?

- ✓ Different kinds of attacks: L3/L4 versus L7 attacks.
- ✓ Different examples: syn Flood, NTP amplification, burst attacks, JavaScript Attacks, etc.
- ✓ For volumetric attacks there is no much you can do locally.
- ✓ Biggest attacks: around 5,5Tbps. Imperva capacity is over 12 Tbps.
- ✓ Attacks can be carried out without technical knowledge.
- ✓ Drivers behind attacks: hacktivism, ransomware, just for fun...





Four DDoS Protection Offerings

An overview of our DDoS protection services

	DDoS for Networks	DDoS for IPs	DDoS for Web	Protected DNS*
Asset	Class-C+ network	Individual IPs	Websites	DNS servers
Customer	Enterprises with DCs	Customers w/o DCs	With sites/apps	With DNS Infra
Operation	AO + On-Demand	Always On	Always On	Always On
Method	BGP advertising	DNS Update	DNS Update (A)	DNS Update (NS)
In/Out	Ingress Only	Ingress+Egress	Ingress+Egress	Ingress+Egress
Protocols	L3/L4	L3/L4	HTTP	TCP, UDP
Connectivity	GRE, EF, Direct-Connect	TCP Proxy, GRE, IPnP, IPinIP	TCP Proxy	TCP Proxy



Imperva Global Network

- Global Mesh
- CDN
- Anycast Network
- Fully Automated Load Balancing and Policy Adjustment
- 63+ PoPs
- 13+ TBps capacity
- Tier 1 ISPs, IXs and T1 Data Centers
- Single Stack

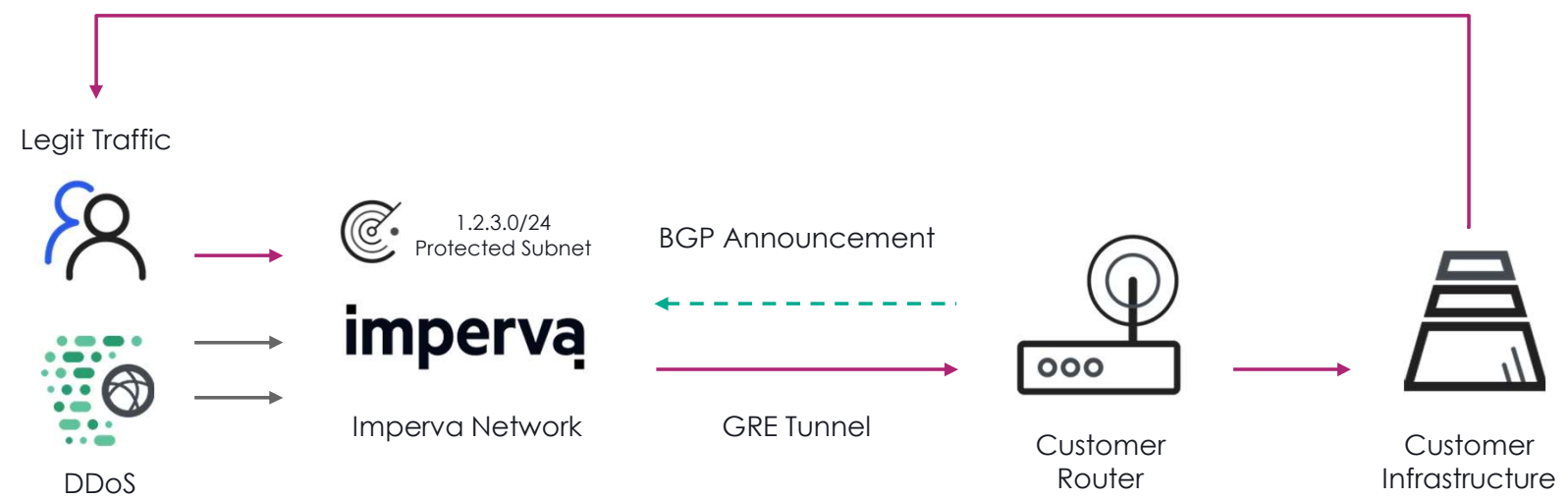


DDoS Protection for Networks

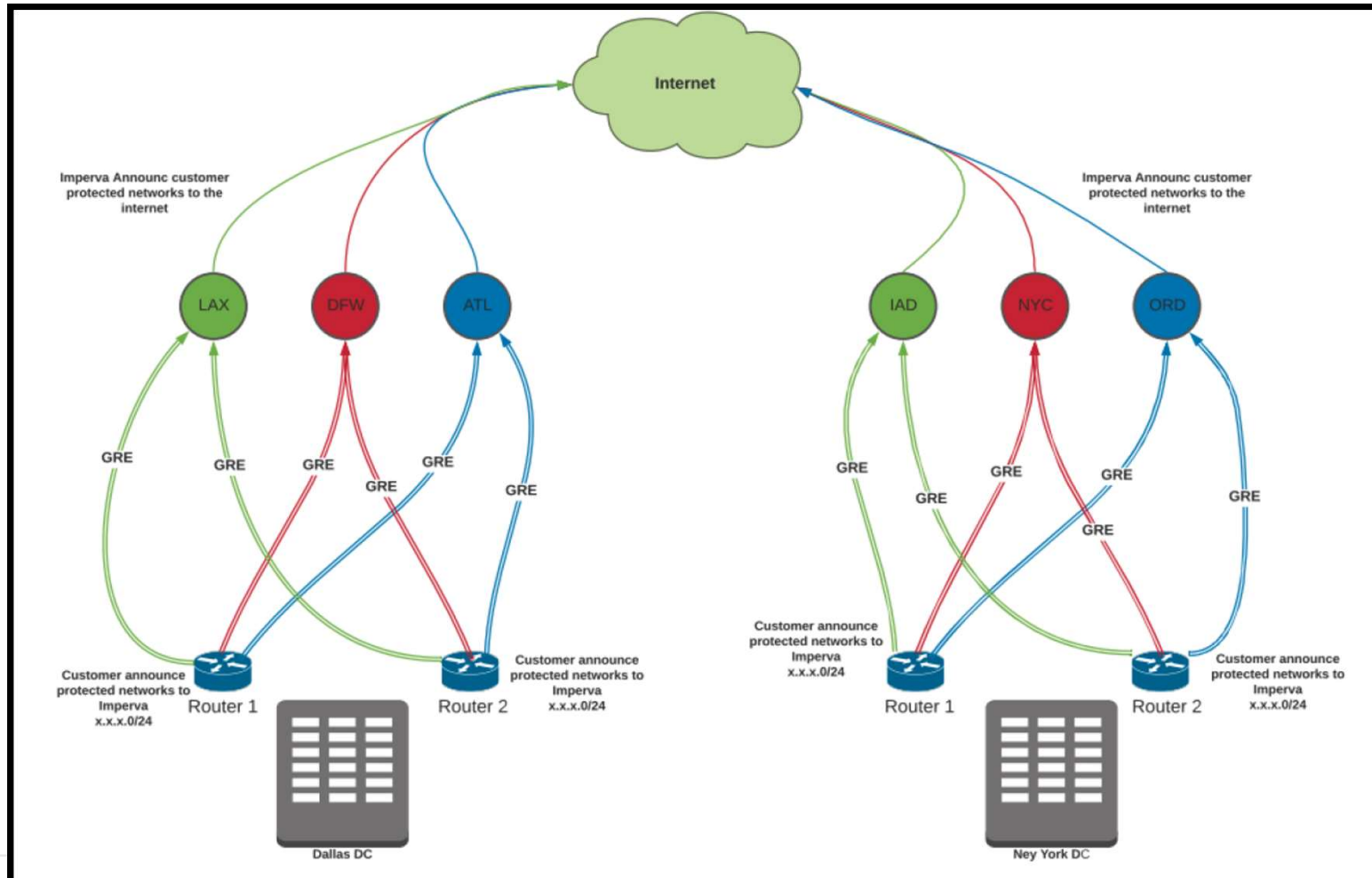
www.thalesgroup.com



DDoS Protection for Networks

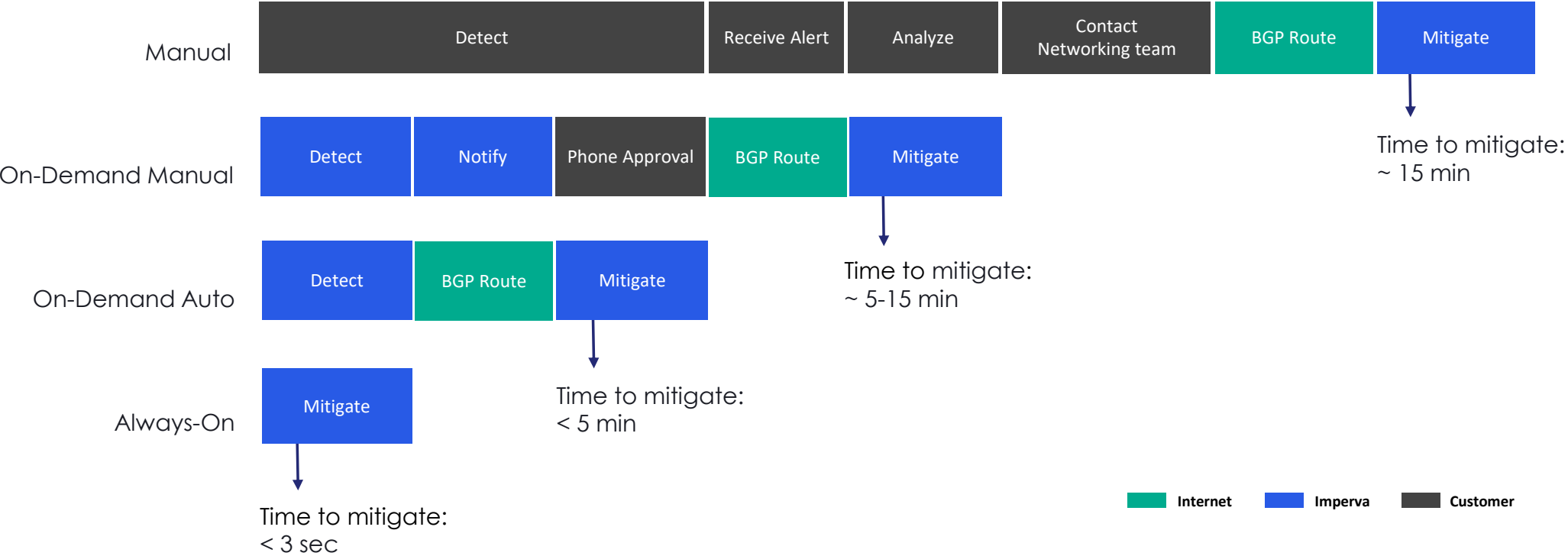


Example setup – (2 sites, 2 routers/site)



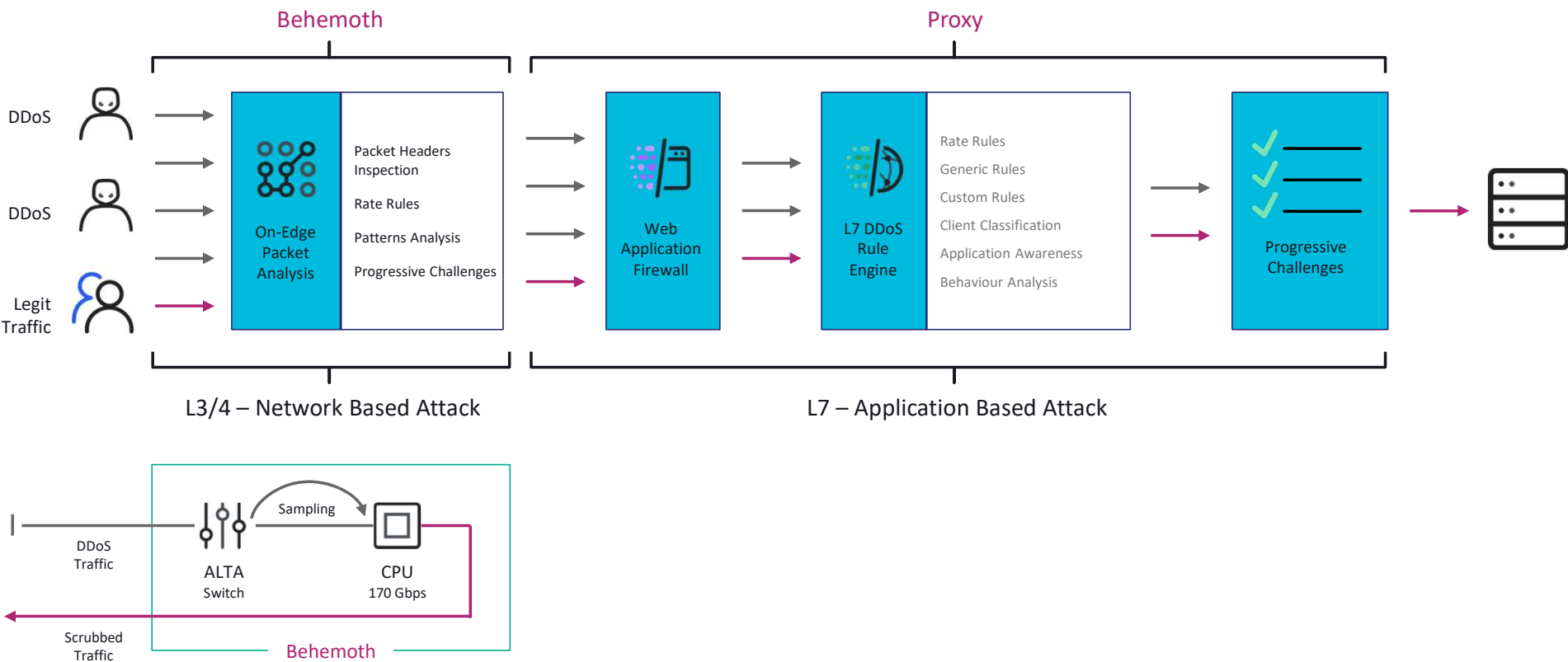


Your Mitigation Deployment Options





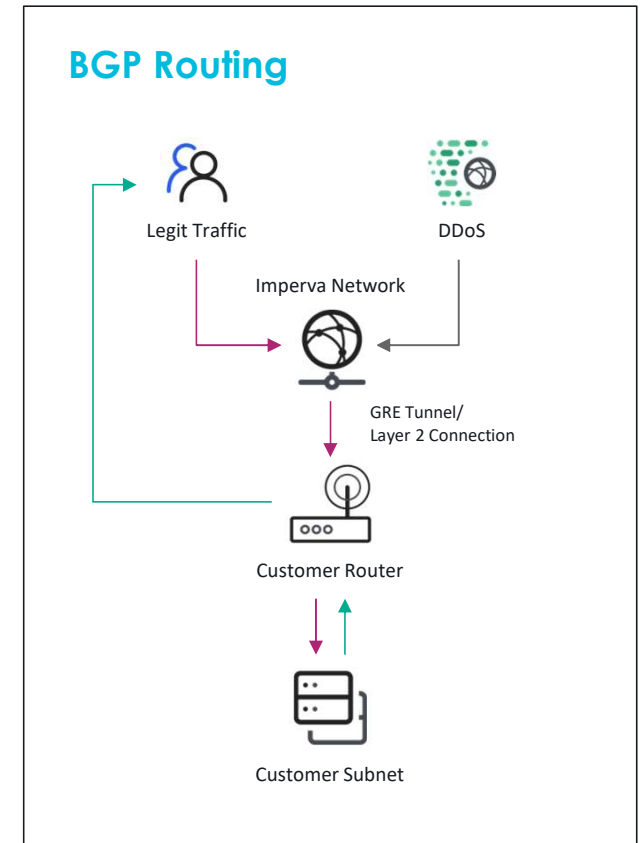
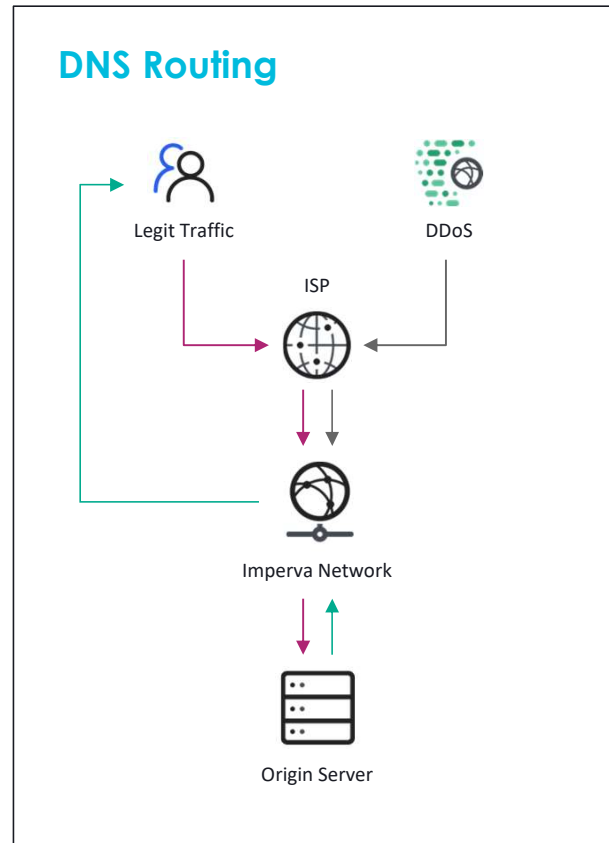
Imperva DDoS Protection



Quick Onboarding

- ✓ Nothing on-prem
- ✓ Simple configuration
- ✓ Self-service
- ✓ Operational Flexibility
 - Always On
 - On-Demand
- ✓ Deployment Flexibility
 - DNS Routing
 - BGP Routing

Fastest time to implementation





Test your defences!

Dedicated DDoS Simulation Platform

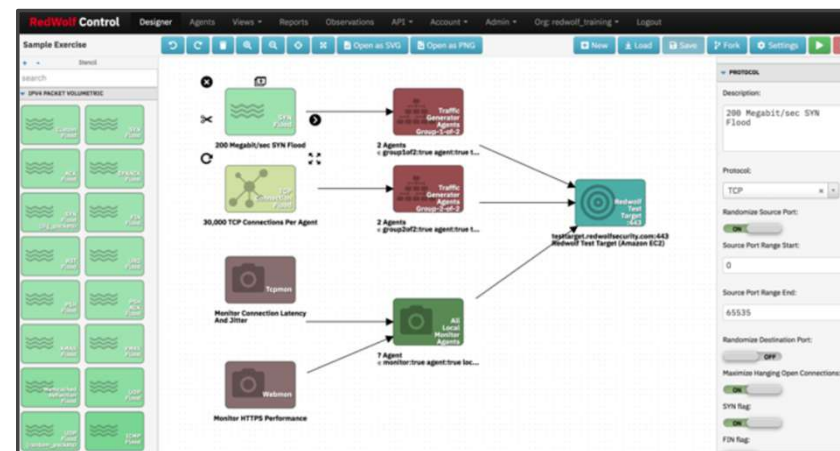
Using distributed, dynamically generated single use hosts to generate traffic (Good or Bad). In parallel using monitoring to measure the impact of the attack.

Fine Control of Testing Scenarios

Full control on the types, volume of traffic and GEO origin of traffic attacks.

Multi-Vector and Morphing Attacks

Most attacks these days are short and massive. Involving multiple vectors of direct communication, reflection attacks and changing attacks.





Examples of attacks we protect against...

UDP floods (volumetric)

NTP amplification (volumetric)

DNS amplification (volumetric)

SYN floods (protocol)

DNS Query floods (layer-7)

HTTP(S) GET request floods (layer-7)

TCP ACK floods (volumetric & proto)

Tsunami SYN flood (volumetric)

CHARGEN amplification (volumetric)

Memcache amplification (volumetric)

SSDP amplification (volumetric)

SNMP amplification (volumetric)

HTTP(S) POST request floods (layer-7)

TCP RST floods (protocol)

SSL negotiation floods (protocol)

SlowLoris attack (protocol)

TCP connect() floods (protocol)

SMTP request flood (layer-7)

GRE-IP UDP floods (volumetric)

Fragmented attacks (protocol)

CLDAP attacks (volumetric)

CoAP (volumetric & protocol)

WS-DD (volumetric & protocol)

ARMS (volumetric)

Jenkins (volumetric)

DNS Water Torture (volumetric)

And many, many more...



Self-Service onboarding

Add range

General

The ASN

ASN Number

Select

Enter Prefix

1.2.3.4

Protected

Always-on

diverted a

☐ Always-on

☐ On-demand

Protected Networks

IP ranges (/24 or larger) or specific IPs that are protected by Imperva. [More](#)

Filter by Keyword or ID

Prefix	Description	Security Policy	Monitoring Policy	Protection Type	Onboarding Status
1.2.1.0/24	1.1.1.0/24 production range	Sub. TCP with UDP and IPSec (tunnel) - 1000Mb_(1.2.1.0/24)	None	Always-on	☒ Fully configured 4/4
12.23.34.0/24	On Demand Network	Sub. General purpose UDP - 100Mb_(12.23.34.0/24)	Alert Only Default UDP 1000Mb_(12.23.34.0/24)	On-demand Requires Confirmation	☒ Fully configured 4/4

Showing 1 to 2 of 2 entries Show 25 rows

Traffic Profile

The traffic profile is used for setting initial security and detection policies. These policies will be regularly adjusted based on your actual monitored traffic. If you would like to avoid automatic adjustments, please [contact support](#) for further assistance.

Network/Range bandwidth

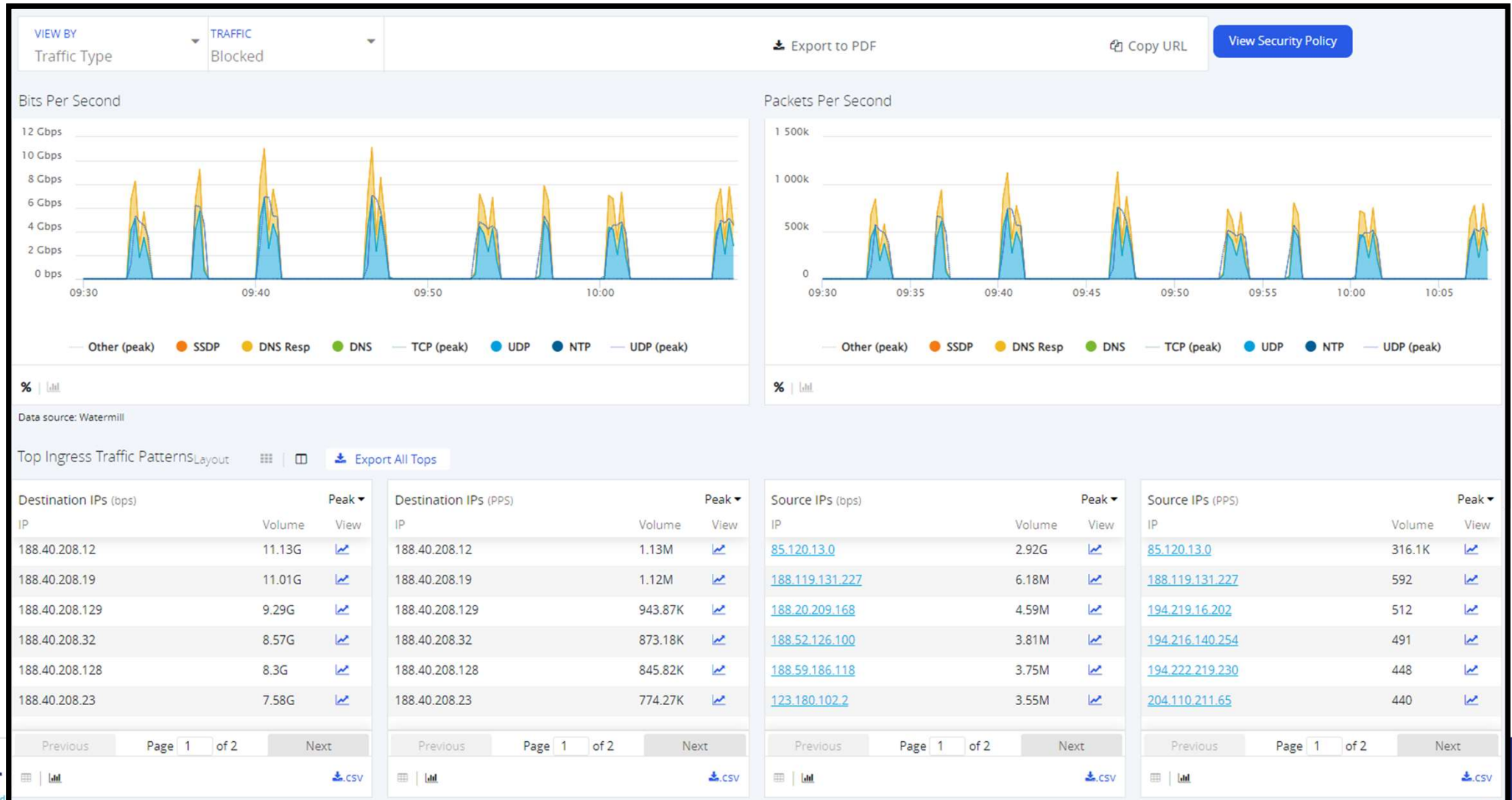
Up to 500 Mbps

Traffic mix

50% UDP | 50% TCP | 0% Other



Comprehensive reporting...





Licensing

- ✓ Base plan. Base plans are available for:
 - Always On: 20Mbps, 50Mbps and 100Mbps.
 - On-Demand: 100Mbps.

Each base plan also includes entitlement for:

- 8 network prefixes
- 8 router connections
- External Flow Based Monitoring (only for On-Demand)
- *For Always-On plans only:* 4 Individual IPs (Imperva Edge IPs)

- ✓ Bandwidth add-ons (in 1 Mbps increments)
- ✓ Network Prefixes add-ons (for IPv4 - /24 subnet)
- ✓ Router Connection add-ons (GRE, ECX/EF, Cross Connect)
- ✓ Individual IP add-on
- ✓ Onboarding Services to assist in initial onboarding (optional but recommended)



Prerequisites

The following prerequisites are required for DDoS Infrastructure protection:

- ✓ The prospect must own at least one Class C (/24) network segment
- ✓ The network prefix must be registered with IRR as route object (such as RIPE)
- ✓ The prospect must be able to adjust the TCP-MSS value on the physical interface of the router (not the GRE tunnel)
- ✓ Imperva must be set to be the best BGP path for traffic to flow through us when required
- ✓ The appropriate traffic monitoring servers should be provided for On-Demand (e.g. NetFlow)
- ✓ The prospect should consult with its ISPs, and network MSS, and advise us if its has known security protections such as Firewall, Access Lists or URPf (filtering on asymmetric routing)



PoV Scope

The following covers the scope of the PoV

- ✓ A single router in a datacenter will be configured
- ✓ The PoV will only cover GRE
- ✓ A single /24 prefix network will be protected
- ✓ If a Volumetric DDoS Test is needed, it is focused on L3/L4 traffic only.
- ✓ Any DDoS/Performance stress testing must be agreed in advance
 - Imperva can provide L3/L4 DDoS testing using RedWolf if required
 - Limited to 5Gbps / 30 minutes – just to prove the concept
 - Imperva SOC/NOC must be notified of the details of the test – form to be provided (lead time 2 weeks!)



Sample Success Criteria

- ✓ Onboarding Process
 - Onboarding was performed quickly and according to Imperva's SLA
- ✓ Latency and Routing
 - Latency is within the expected ranges
- ✓ GRE Tunnel failover
 - Test out primary/secondary GRE Tunnels based on customer preference and failover
- ✓ Attack Simulation Mitigation
 - These could be multiple tests conducted by 3rd party partner like RedWolf, Nimbus or others
- ✓ Attack Real Time Visibility
 - Using infrastructure dashboard to get real time visibility into attack velocity, methods, blocked/passed traffic etc
- ✓ Attack Post Mortem Analysis.
 - Historical analysis of targeted hosts, active attackers, vectors, protocols used etc...



Contact

Bartosz Chmielewski

Sr System Engineer



+48 601277206



bartosz.chmielewski@external.thalesgroup.com