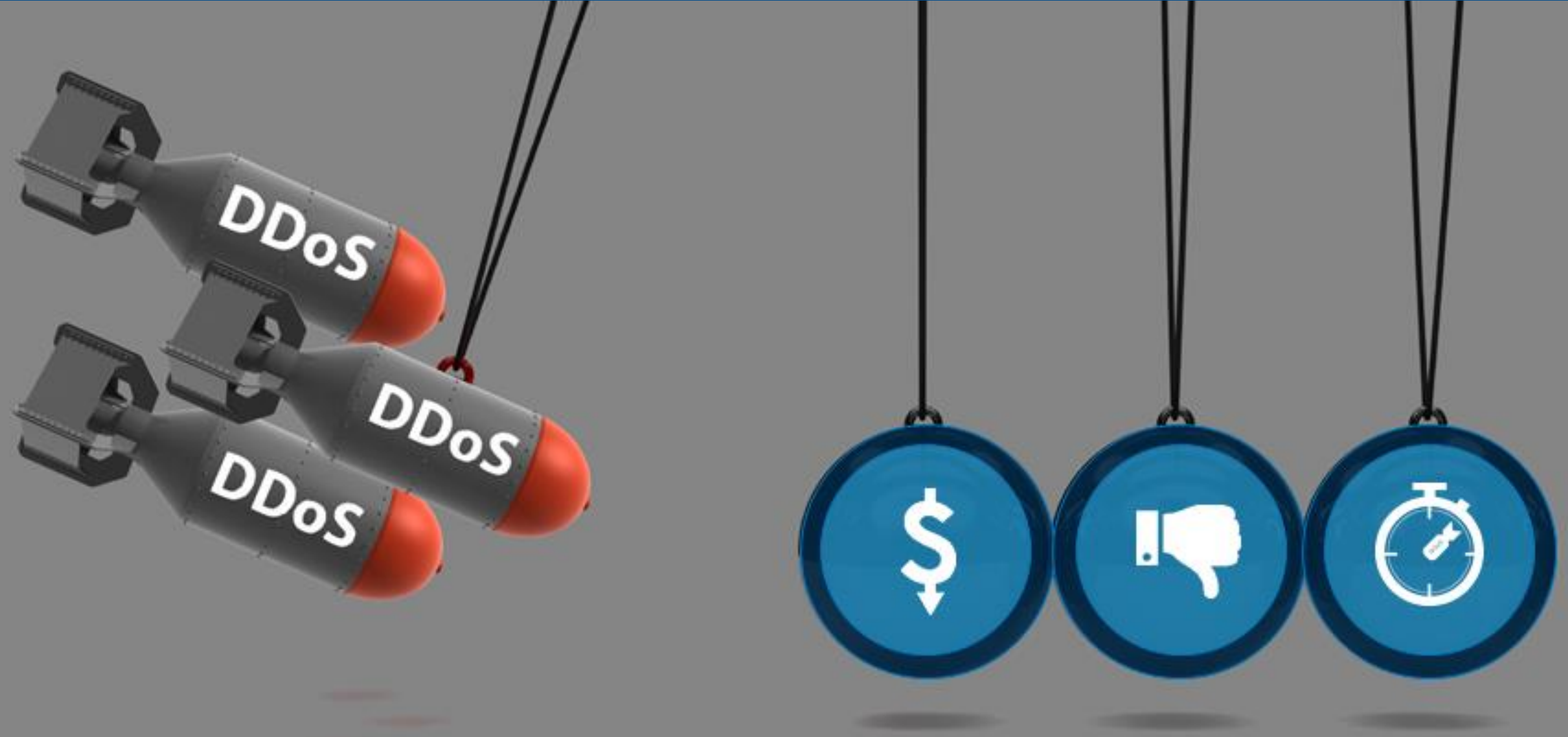
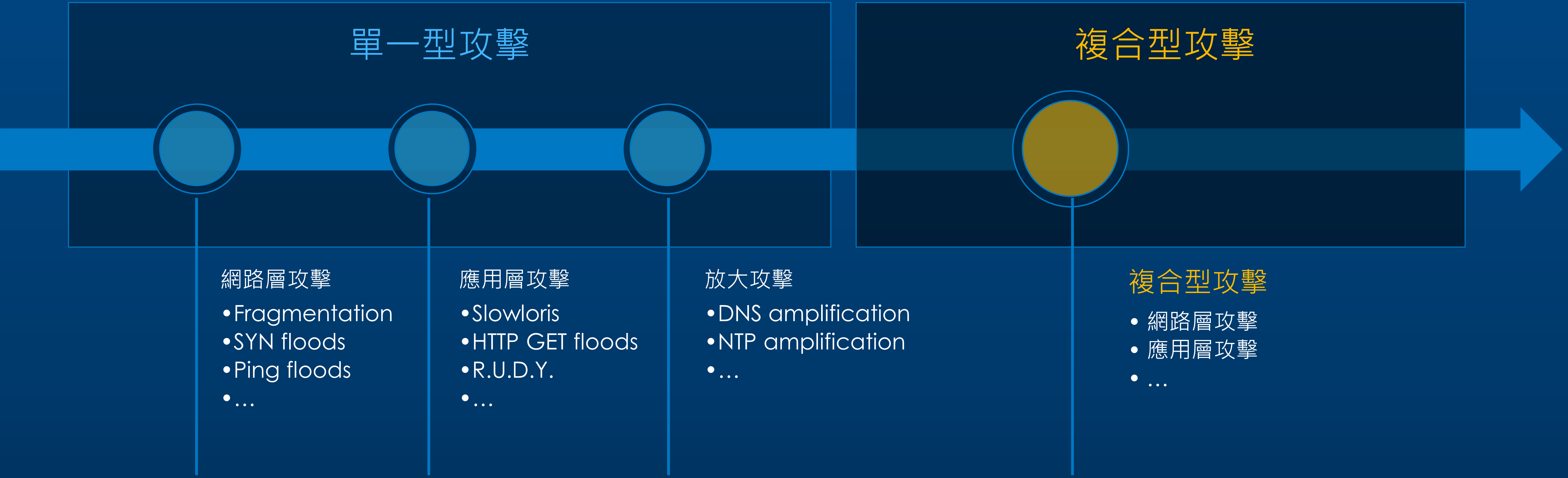


雲端及巨量資料的安全威脅與進階防護

A10 台灣區技術經理 陳志緯

DDoS 攻擊持續演進



單一型攻擊

網路層攻擊

- Fragmentation
- SYN floods
- Ping floods
- …

應用層攻擊

- Slowloris
- HTTP GET floods
- R.U.D.Y.
- …

放大攻擊

- DNS amplification
- NTP amplification
- …

複合型攻擊

複合型攻擊

- 網路層攻擊
- 應用層攻擊
- …

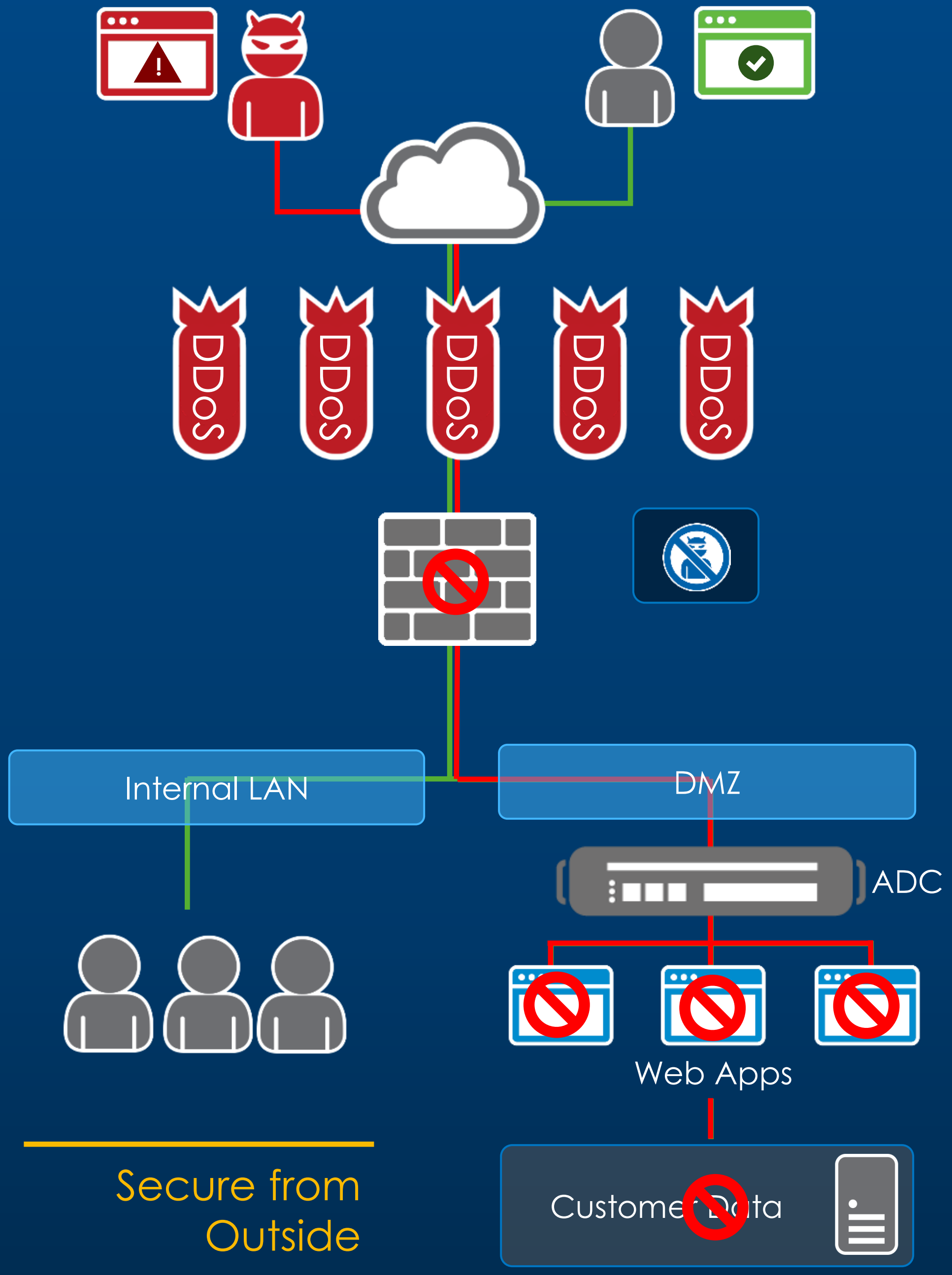
電信商遭受 DDoS 攻擊事件

1. DDoS 攻擊流量

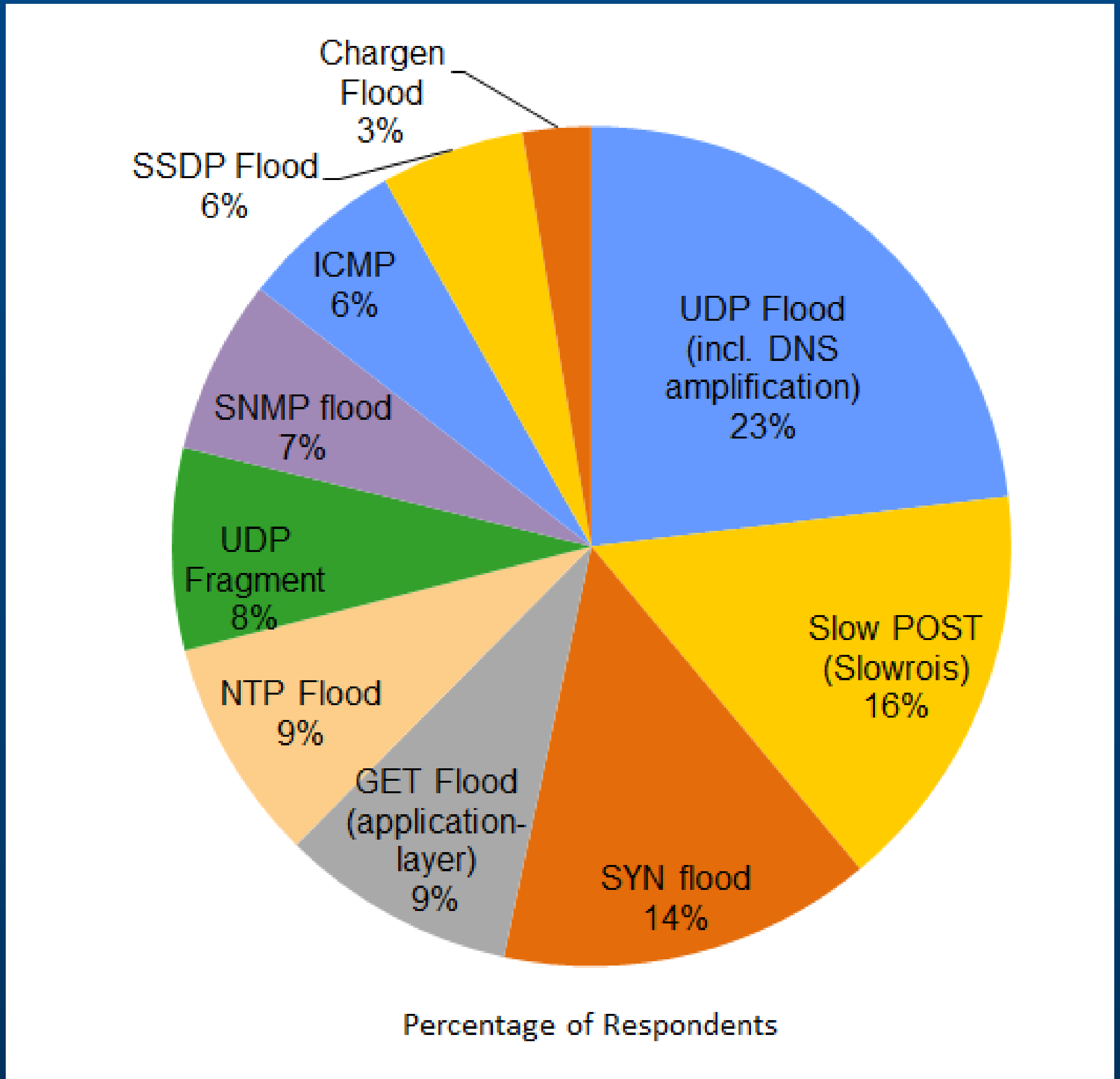
   600Mbps / 200K CPS / 2M Concurrent Sessions

2. 多層次 DDoS 攻擊 (複合型 DDoS Attacks)
   a. Network Attack (網路層攻擊)(ICMP)
   b. Amplification Attack (放大攻擊)(DNS-UDP)
   c. Resource Attack (資源耗損攻擊) (TCP)
   d. Application Attack (應用層攻擊) (HTTP Slowloris)

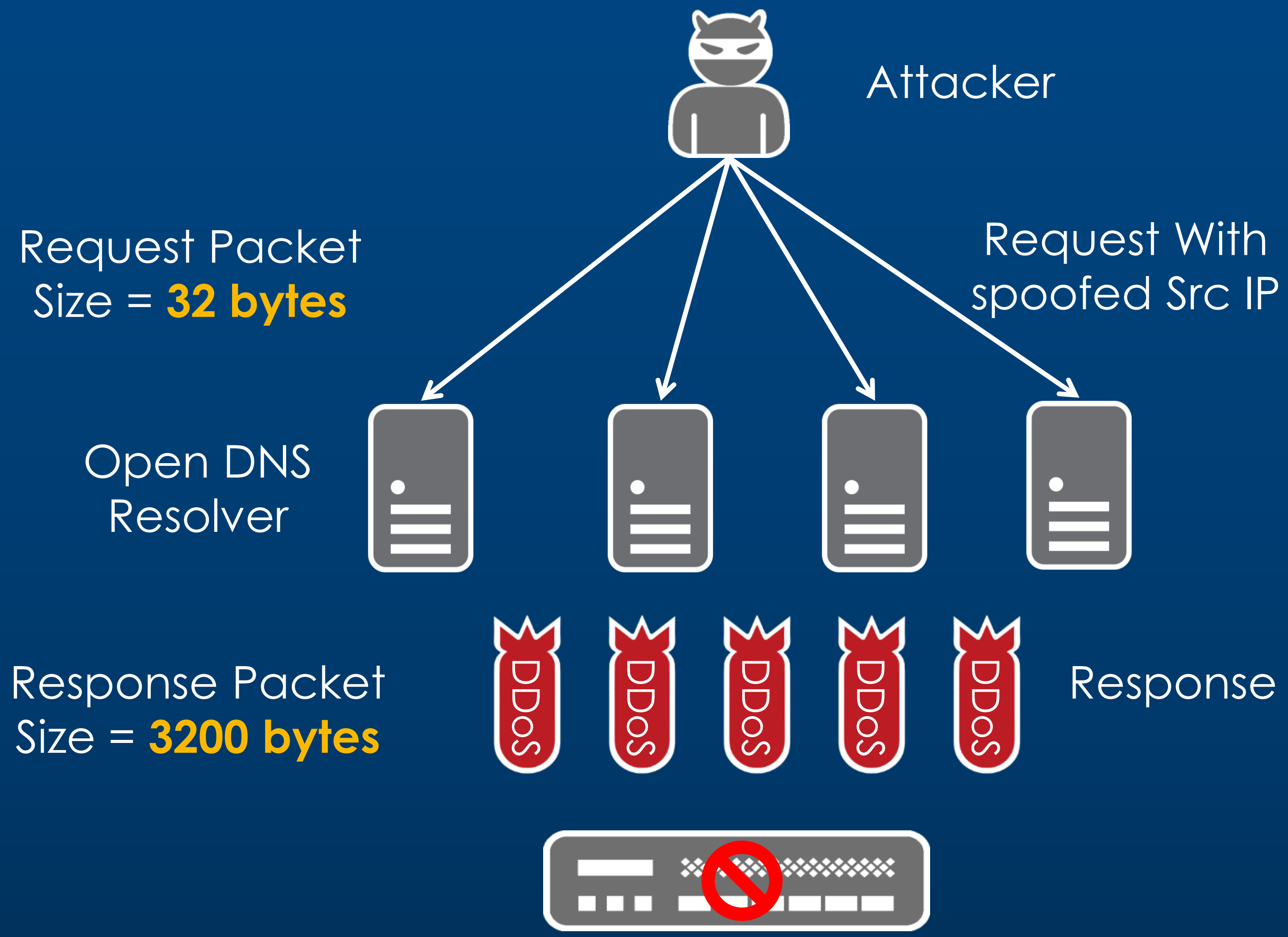
3. 應用層攻擊 特性說明：
   a. Attacker 透過殭屍網路(Botnet)(90% from TW)發起大量TCP連線及HTTP Request封包 (~1K conns per bot)
   b. 對於防火牆而言屬於正常連線存取
   c. 防火牆效能下降及 Server 資源耗盡。



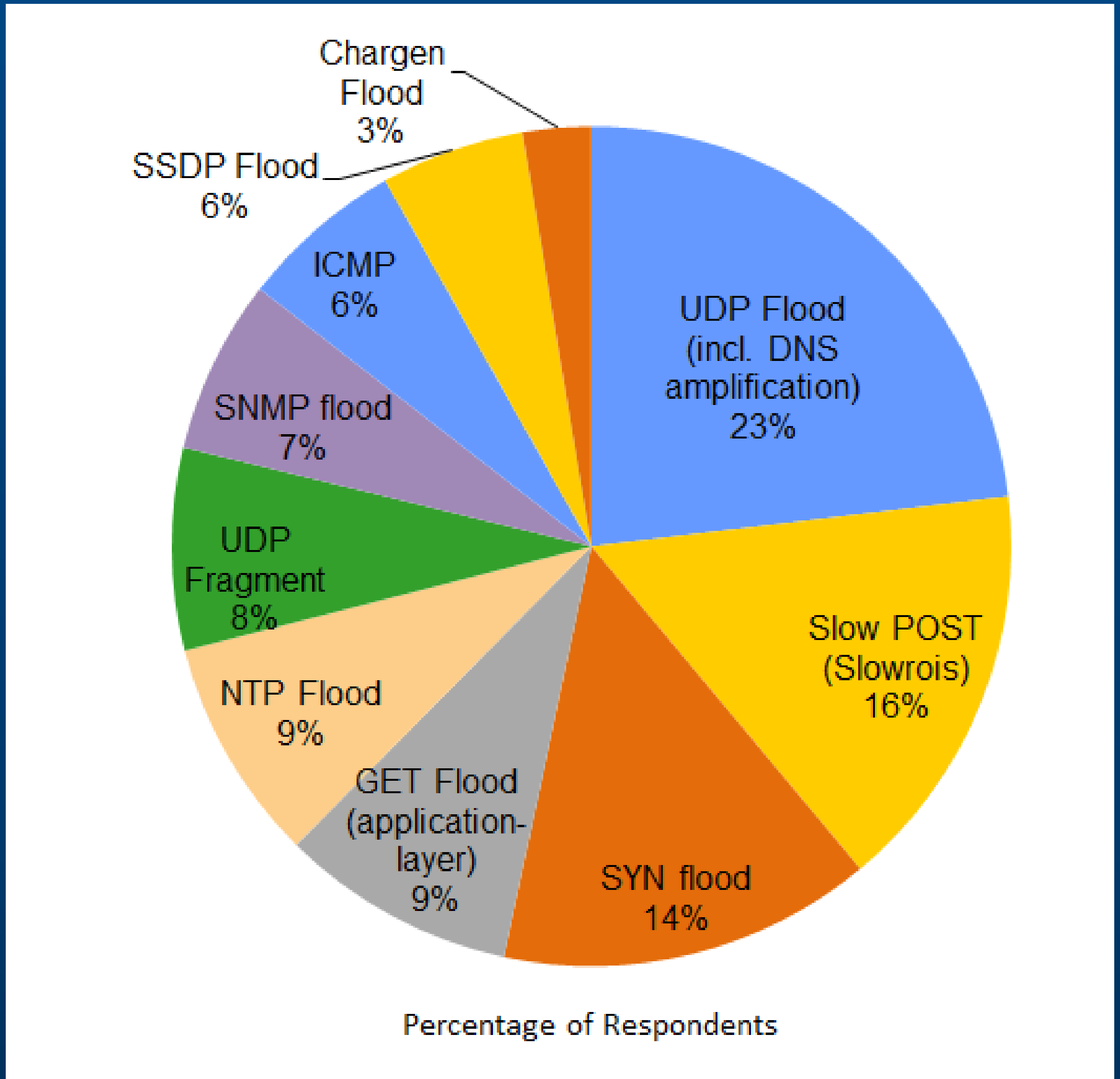
DNS 放大攻擊 (Amplification)



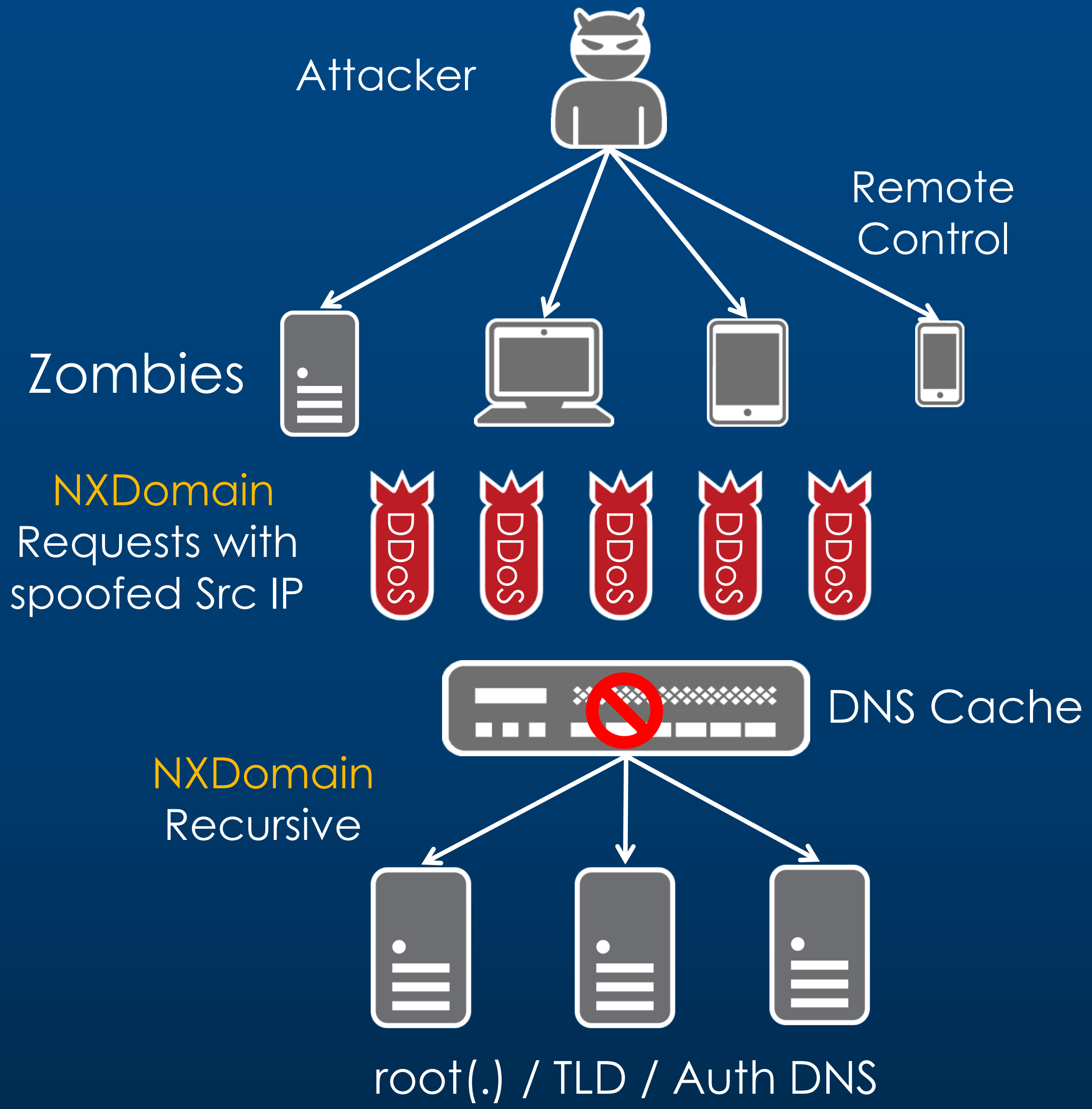
Source: IDG, 2016


Attacker
Request Packet Size = 32 bytes
Request With spoofed Src IP
Open DNS Resolver
DDoS
DDoS
DDoS
DDoS
DDoS
Response Packet Size = 3200 bytes
Response

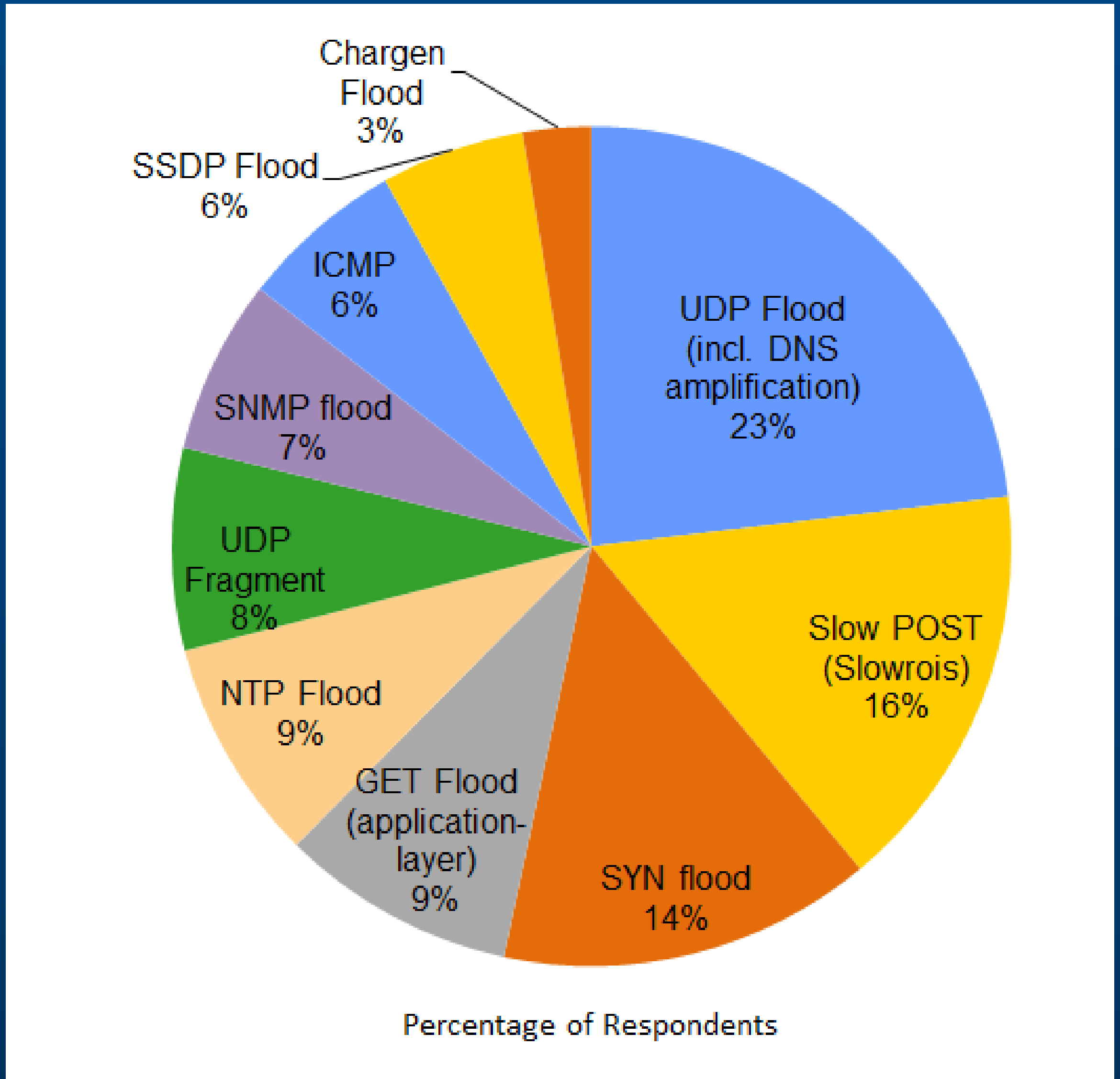
DNS NXDomain 攻擊



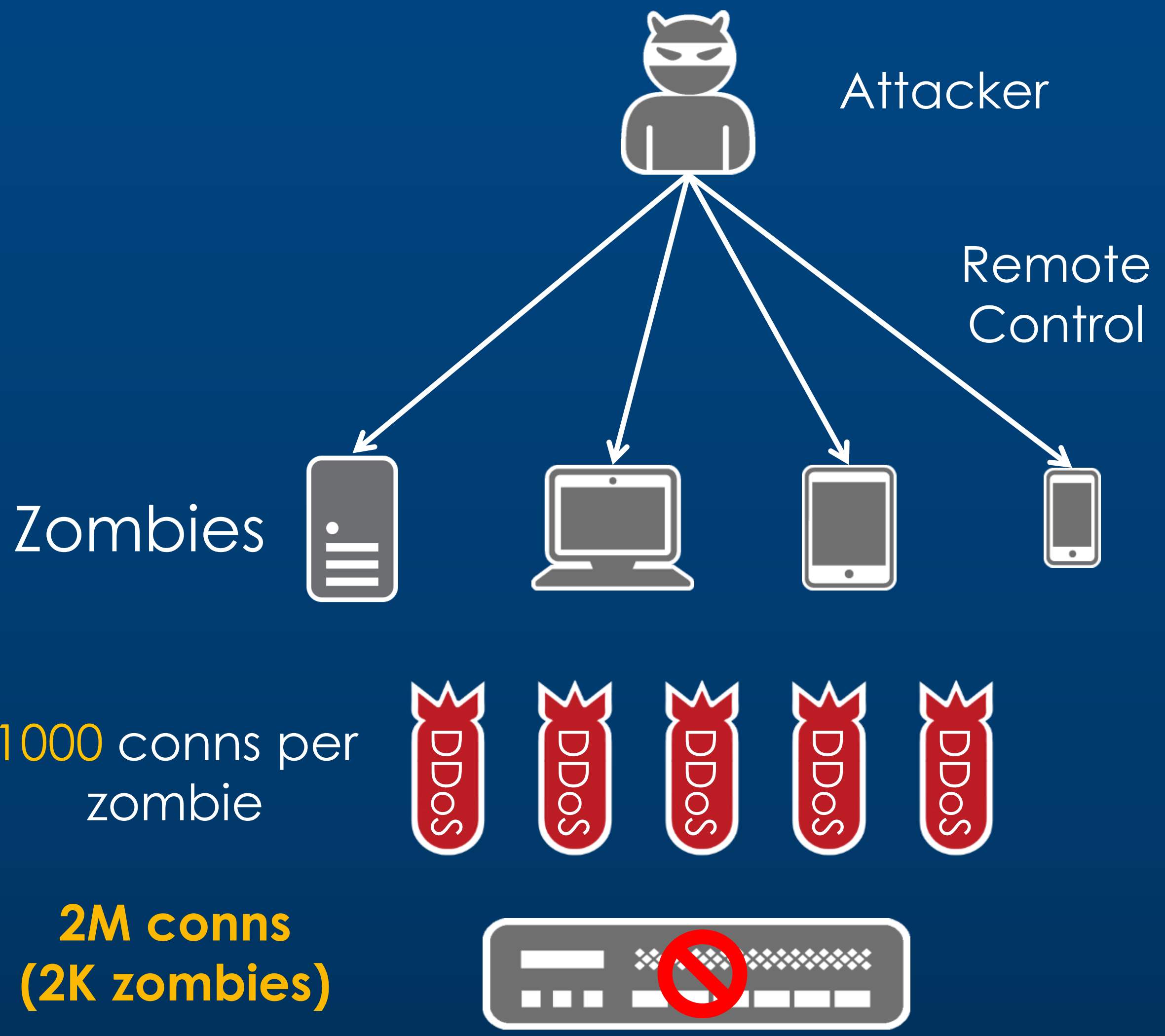
Source: IDG, 2016



HTTP GET Flood / TCP Flood 攻擊



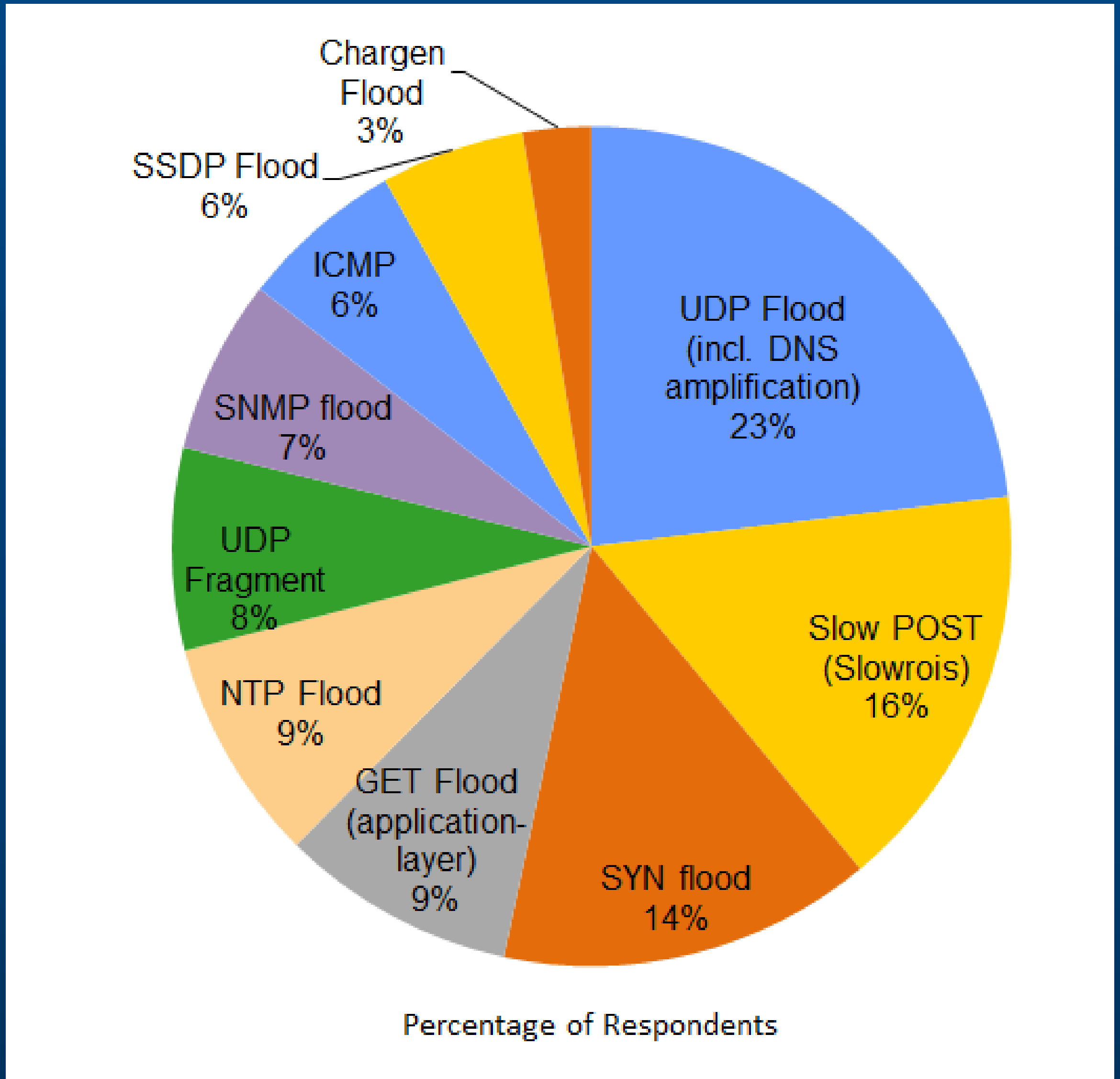
Source: IDG, 2016



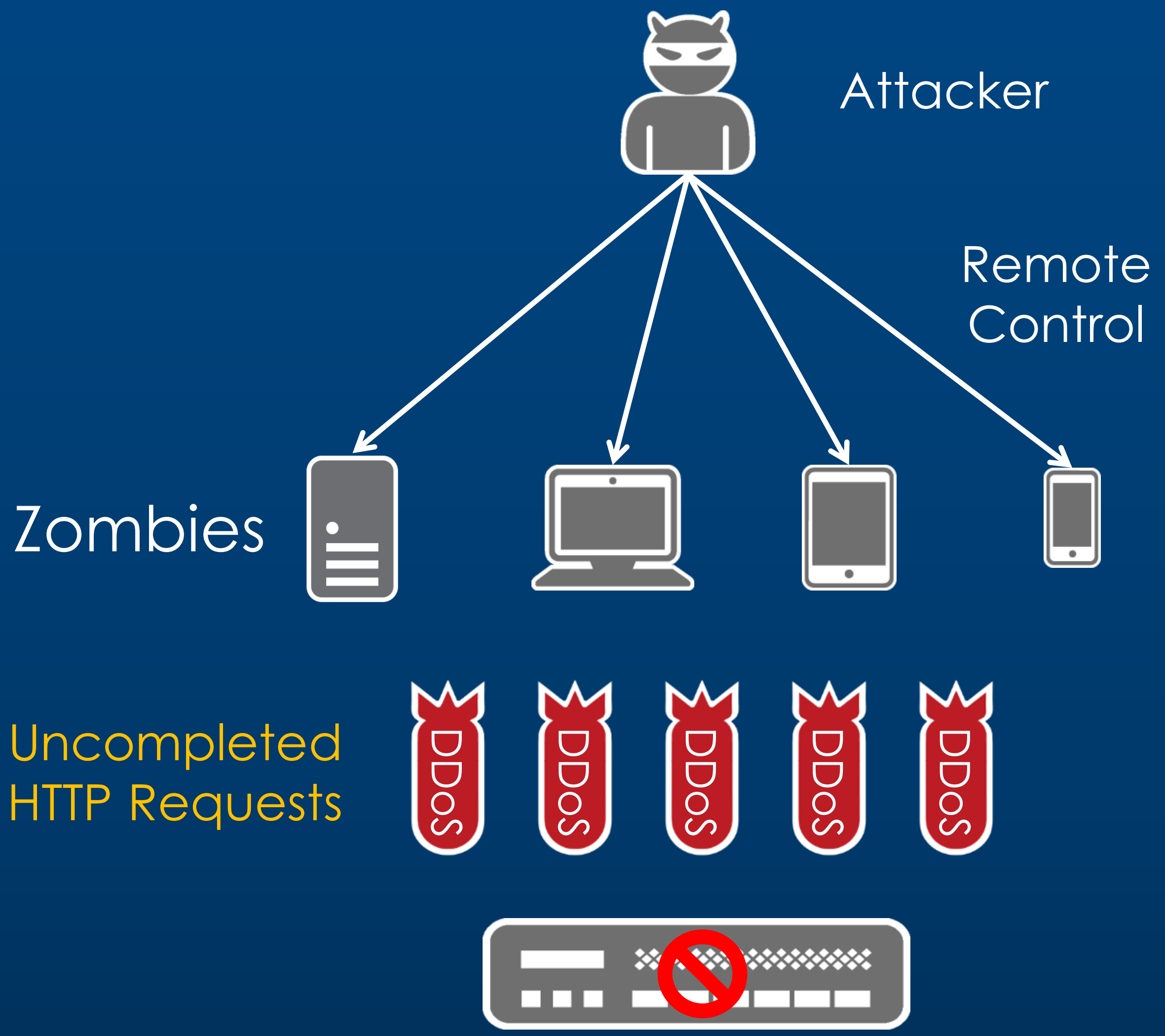
1000 conns per zombie

2M conns (2K zombies)

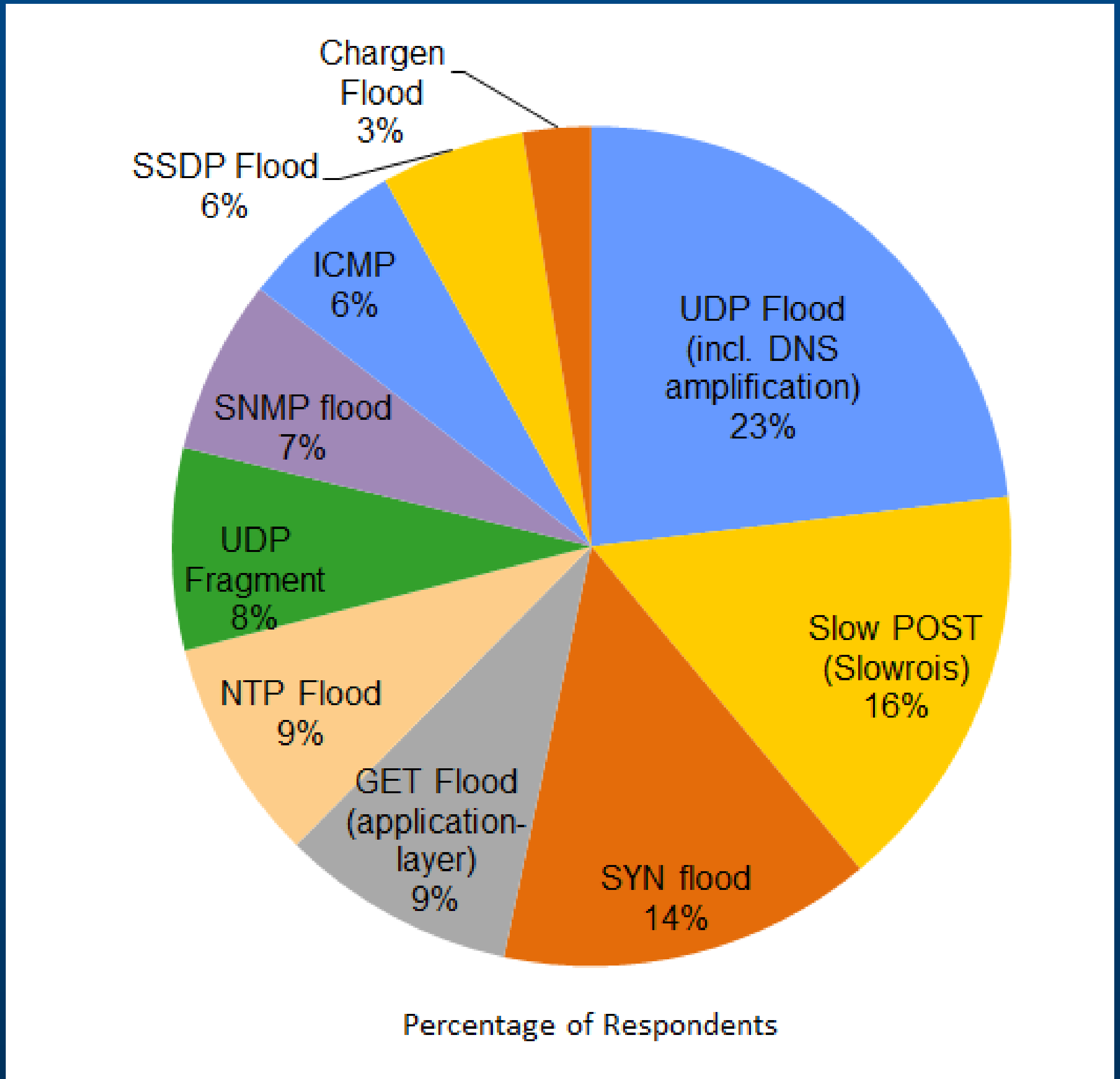
HTTP Slowloris 攻擊



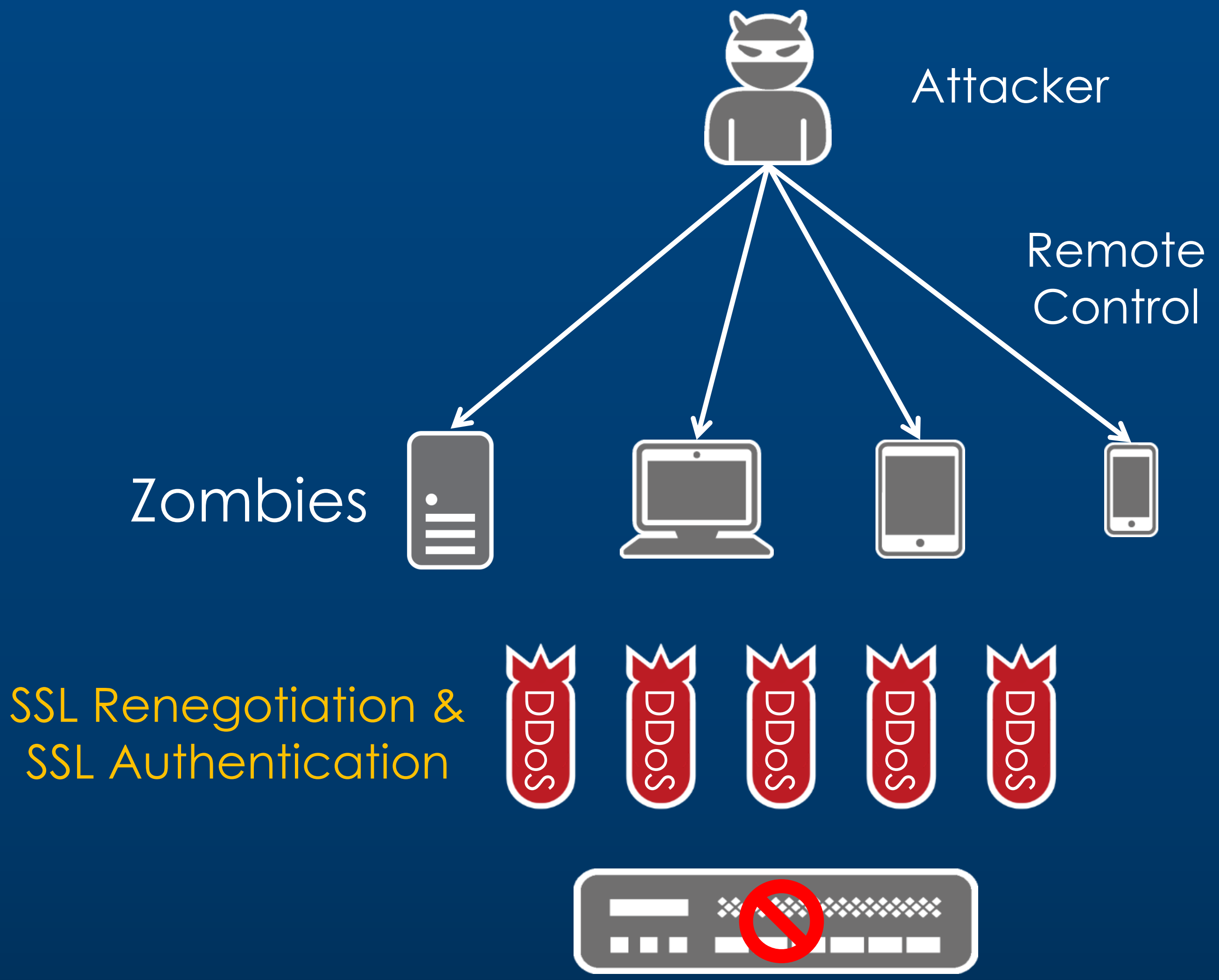
Source: IDG, 2016



SSL Renegotiation / SSL Conn Flood 攻擊

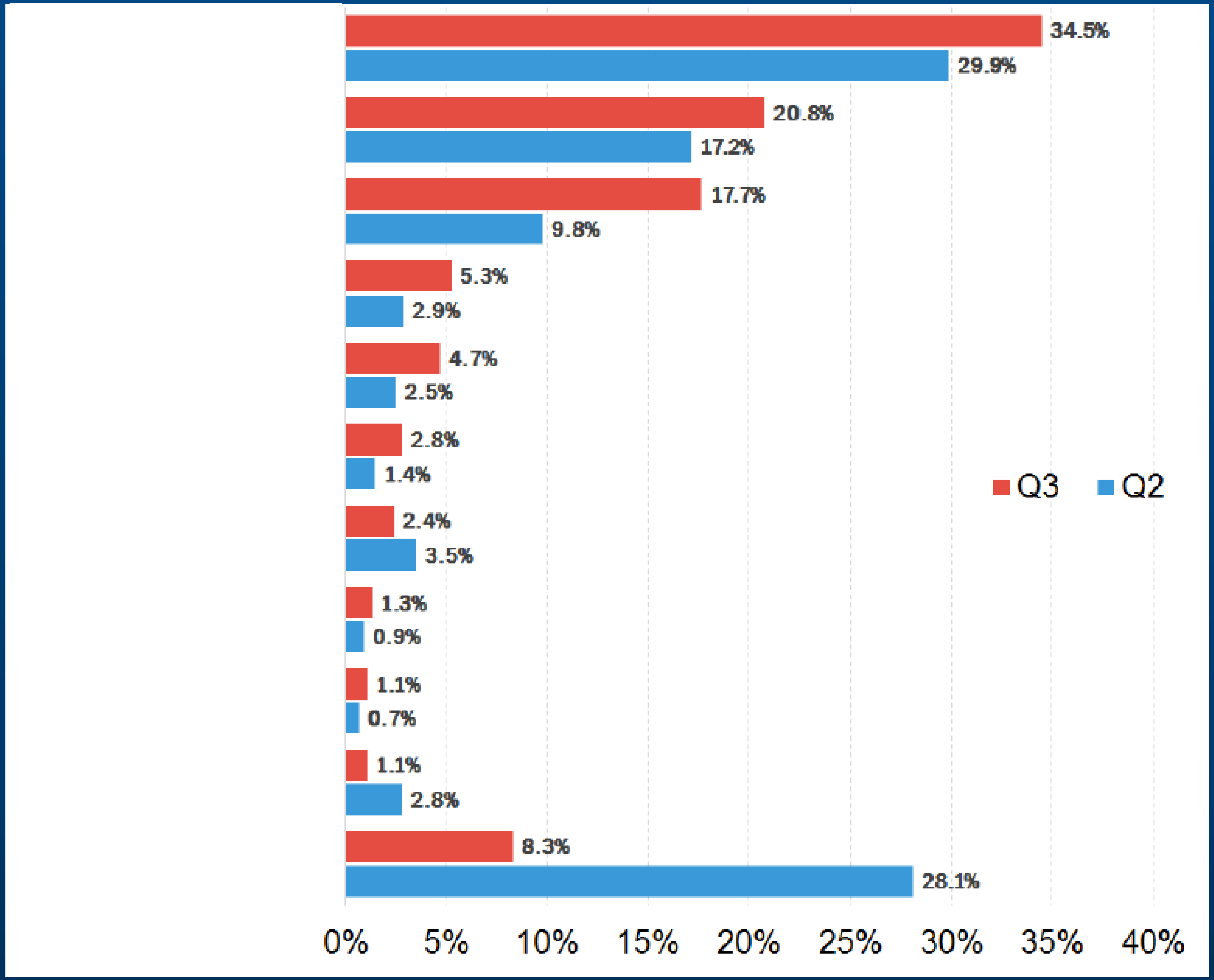


Source: IDG, 2016



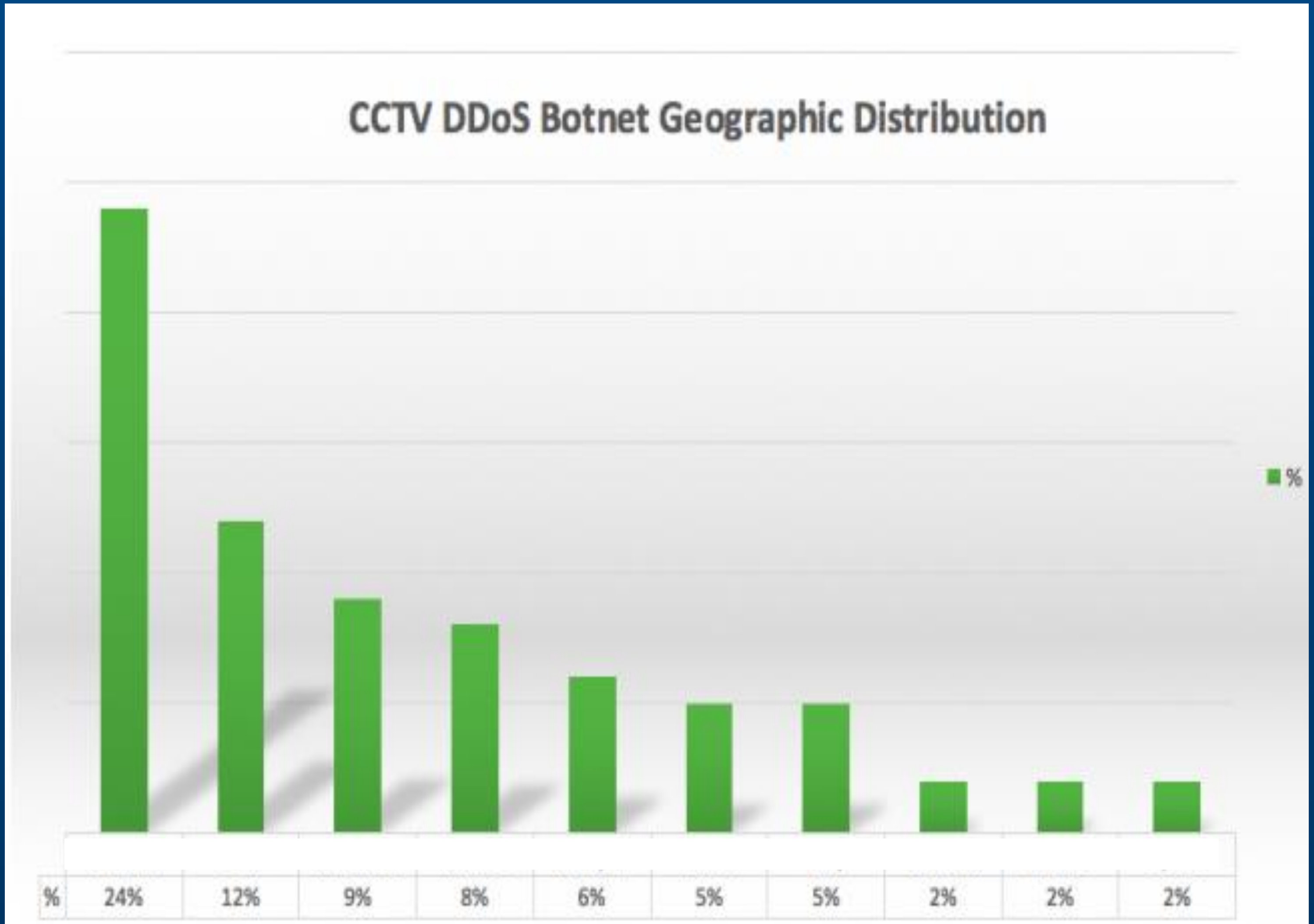
SSL Renegotiation &
SSL Authentication

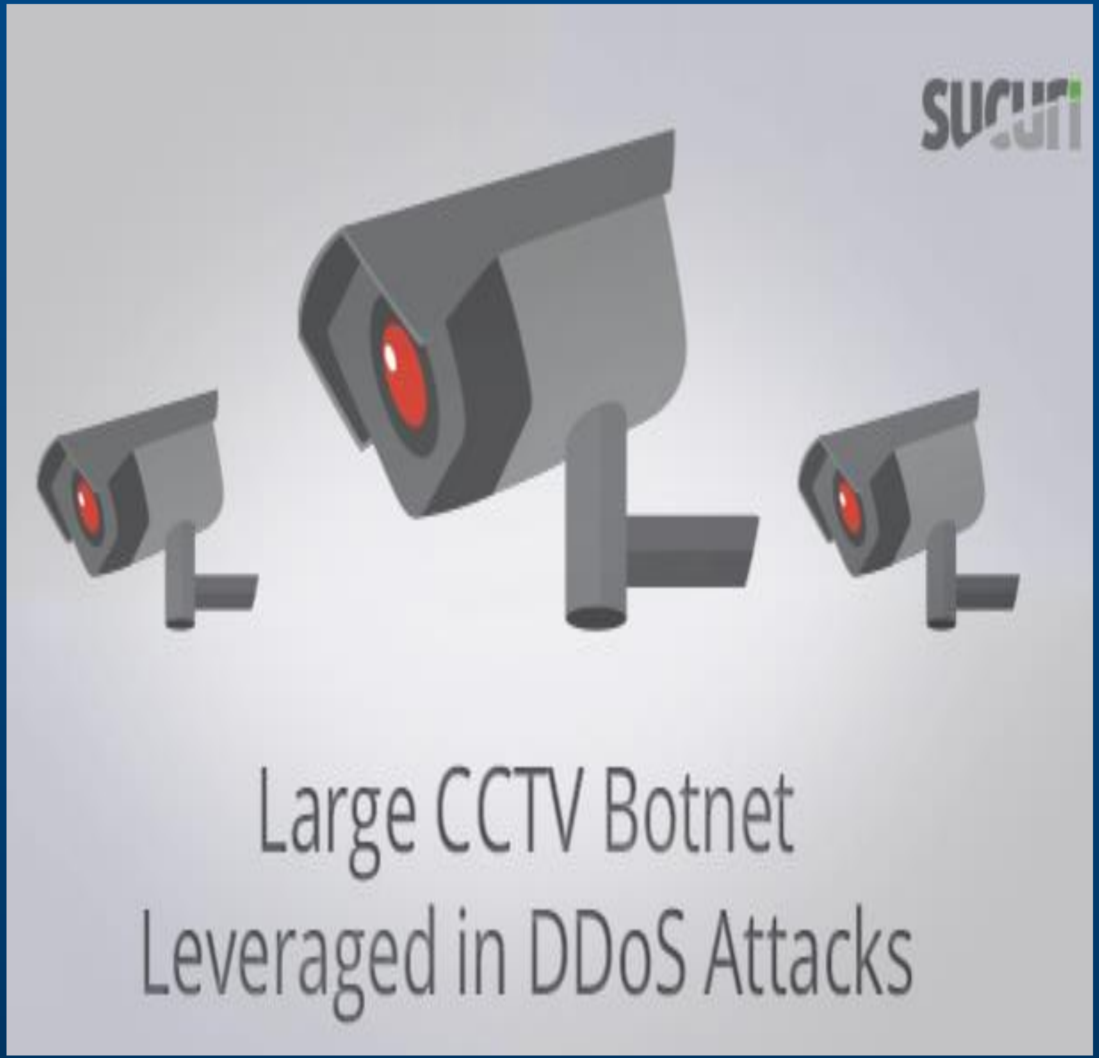
DDoS 攻擊來源



Source: Kaspersky , Q3 2015

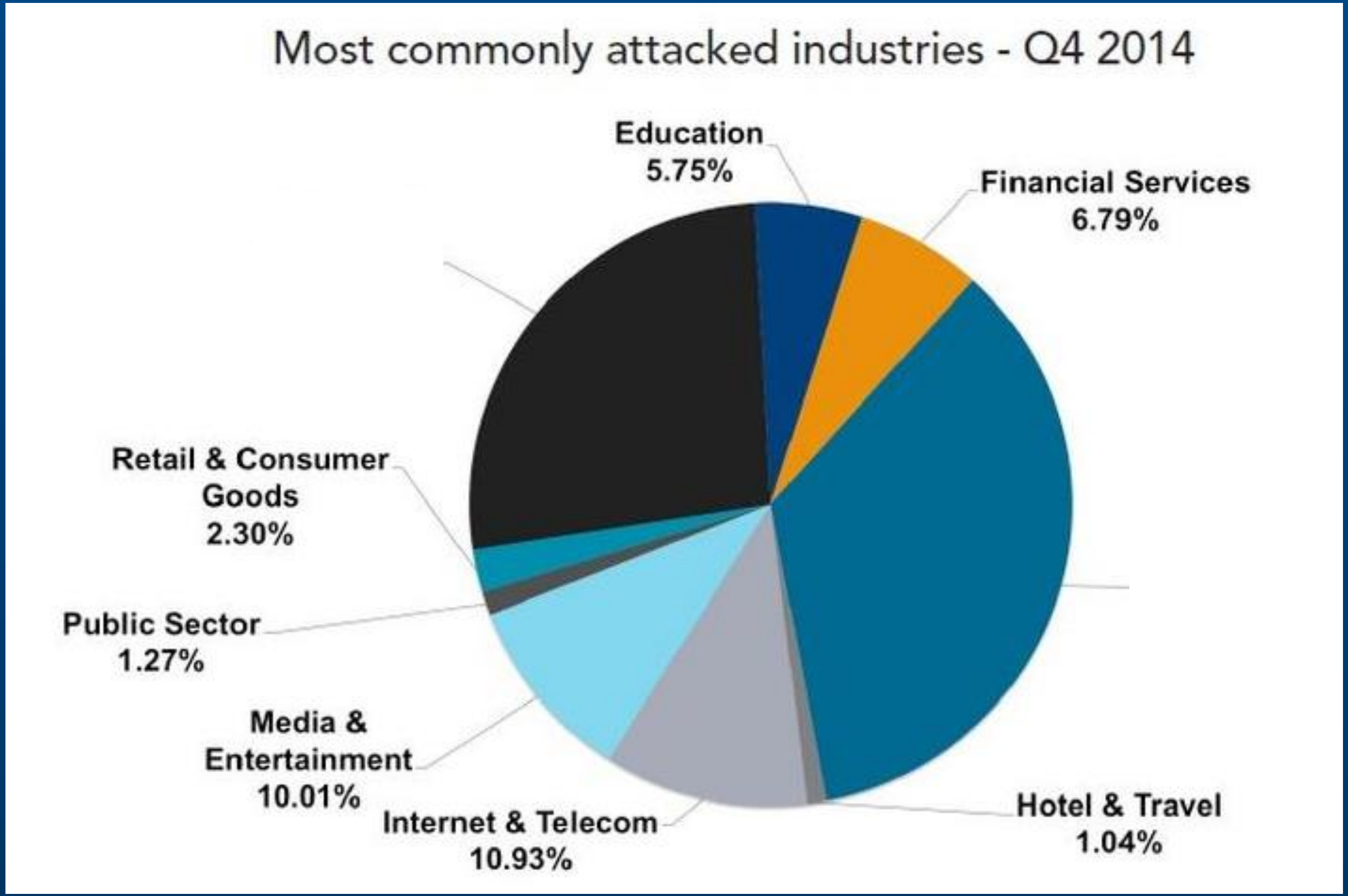
DDoS 攻擊來源 – CCTV 影像監視系統





Source: SUCURI BLOG , Q2 2016

DDoS 攻擊目標



Source: Akamai Q4 2014

頻寬型 DDoS 攻擊

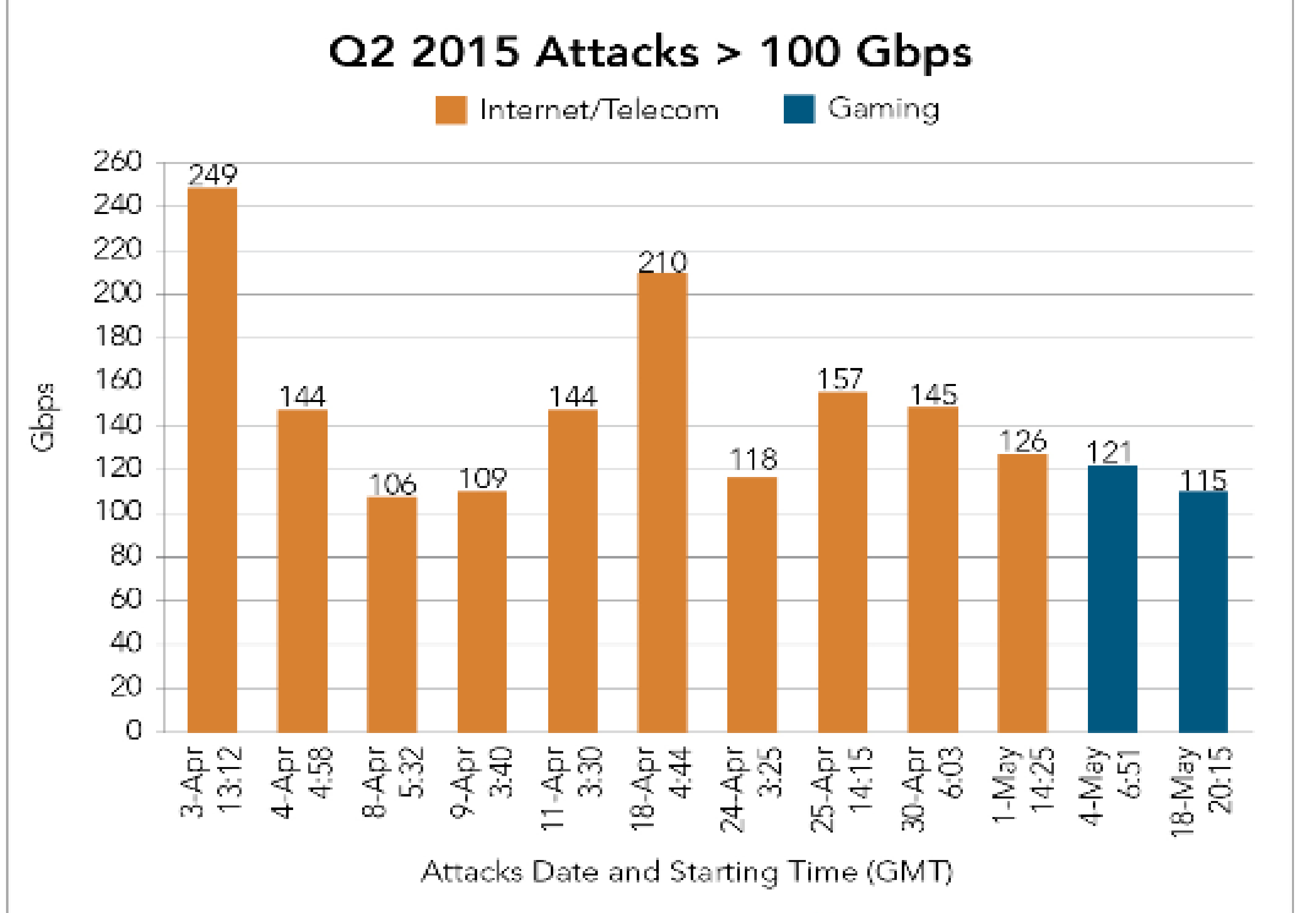


Figure 1-1: Ten of the mega attacks targeted the Internet and telecom industry

Akamai FASTER FORWARD www.stateoftheinternet.com

Source: Akamai

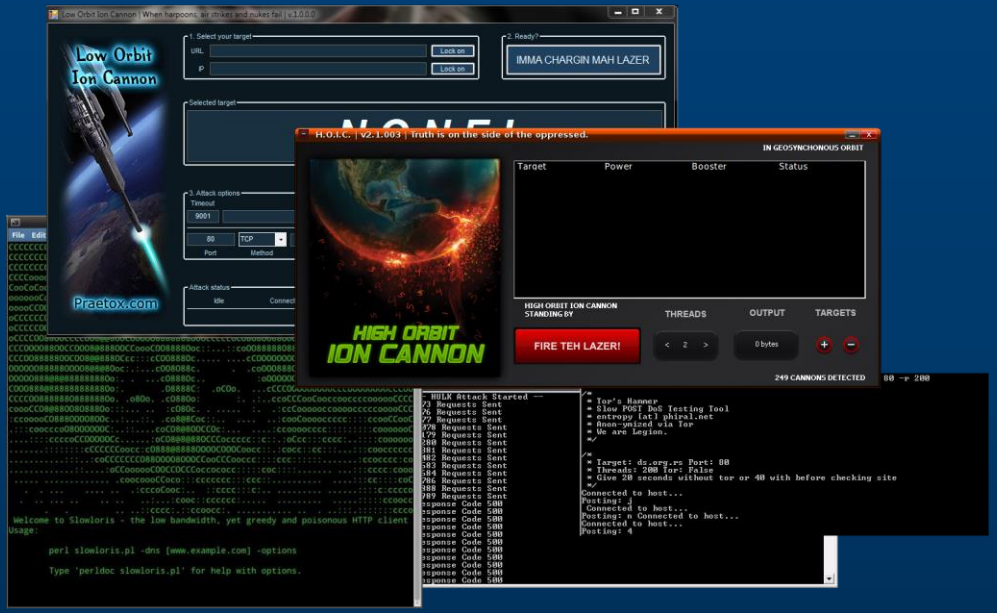
1 Gbps DDoS Traffic :

SYN Flood (0.5Kb) : 2M PPS

ICMP Flood(2Kb) : 500K PPS

DNS Flood (10Kb) : 100K QPS

UDP Flood (2Kb) : 500K PPS

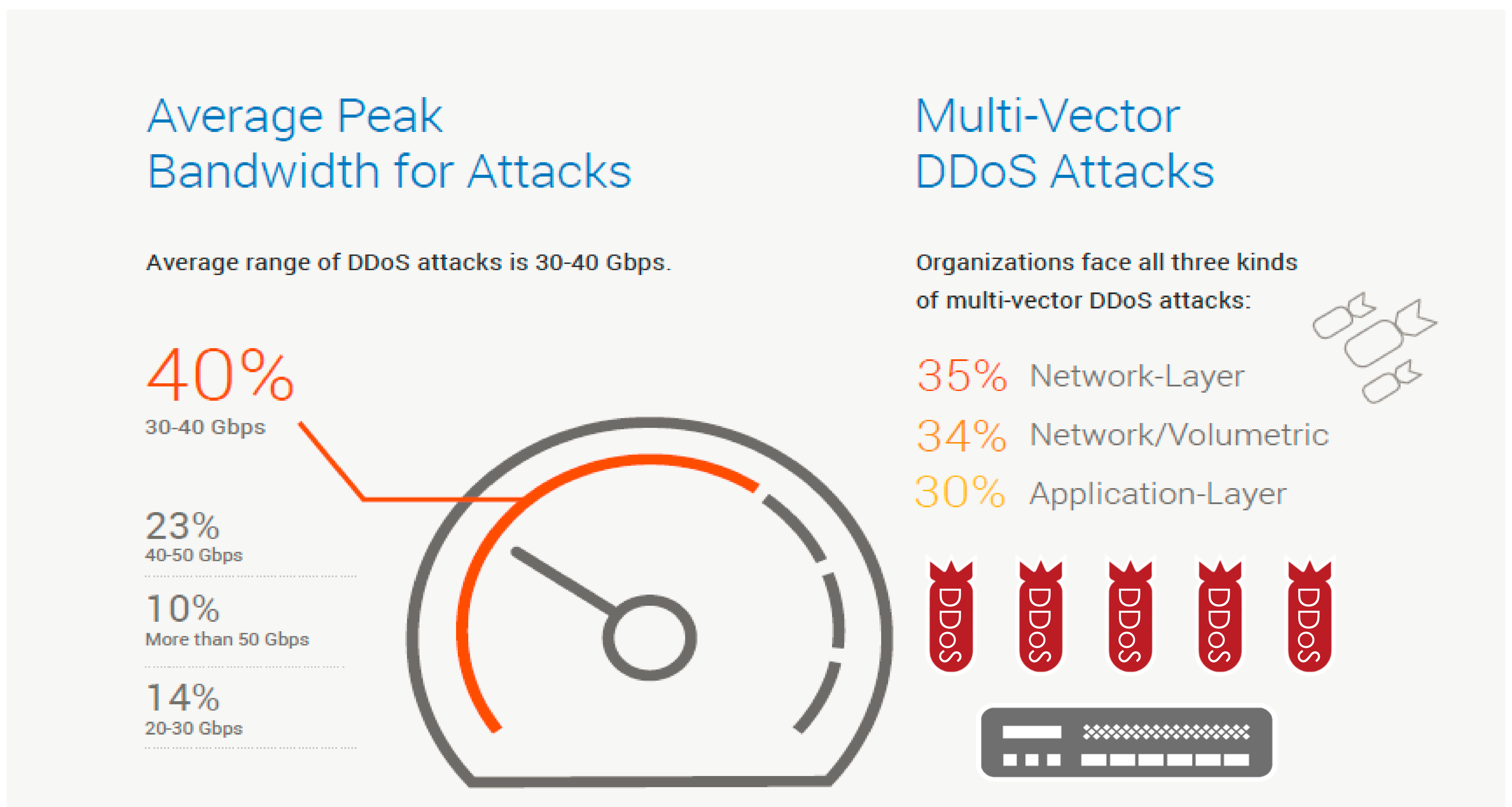


```
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl slowloris.pl -dns [www.example.com] -options

        Type 'perldoc slowloris.pl' for help with options.
```

```
-- HULK Attack Started --
73 Requests Sent
76 Requests Sent
77 Requests Sent
978 Requests Sent
179 Requests Sent
280 Requests Sent
381 Requests Sent
482 Requests Sent
583 Requests Sent
584 Requests Sent
786 Requests Sent
888 Requests Sent
789 Requests Sent
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
esponse Code 500
```

```
80 -r 200
/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
 * Anon-ymized via Tor
 * We are Legion.
 */
/*
 * Target: ds.org.rs Port: 80
 * Threads: 200 Tor: False
 * Give 20 seconds without tor or 40 with before checking site
 */
Connected to host...
Posting: j
 Connected to host...
Posting: n Connected to host...
Connected to host...
Posting: 4
```

DDoS 攻擊類型比例



Average Peak Bandwidth for Attacks

Average range of DDoS attacks is 30-40 Gbps.

40%
30-40 Gbps

23%
40-50 Gbps

10%
More than 50 Gbps

14%
20-30 Gbps

Multi-Vector DDoS Attacks

Organizations face all three kinds of multi-vector DDoS attacks:

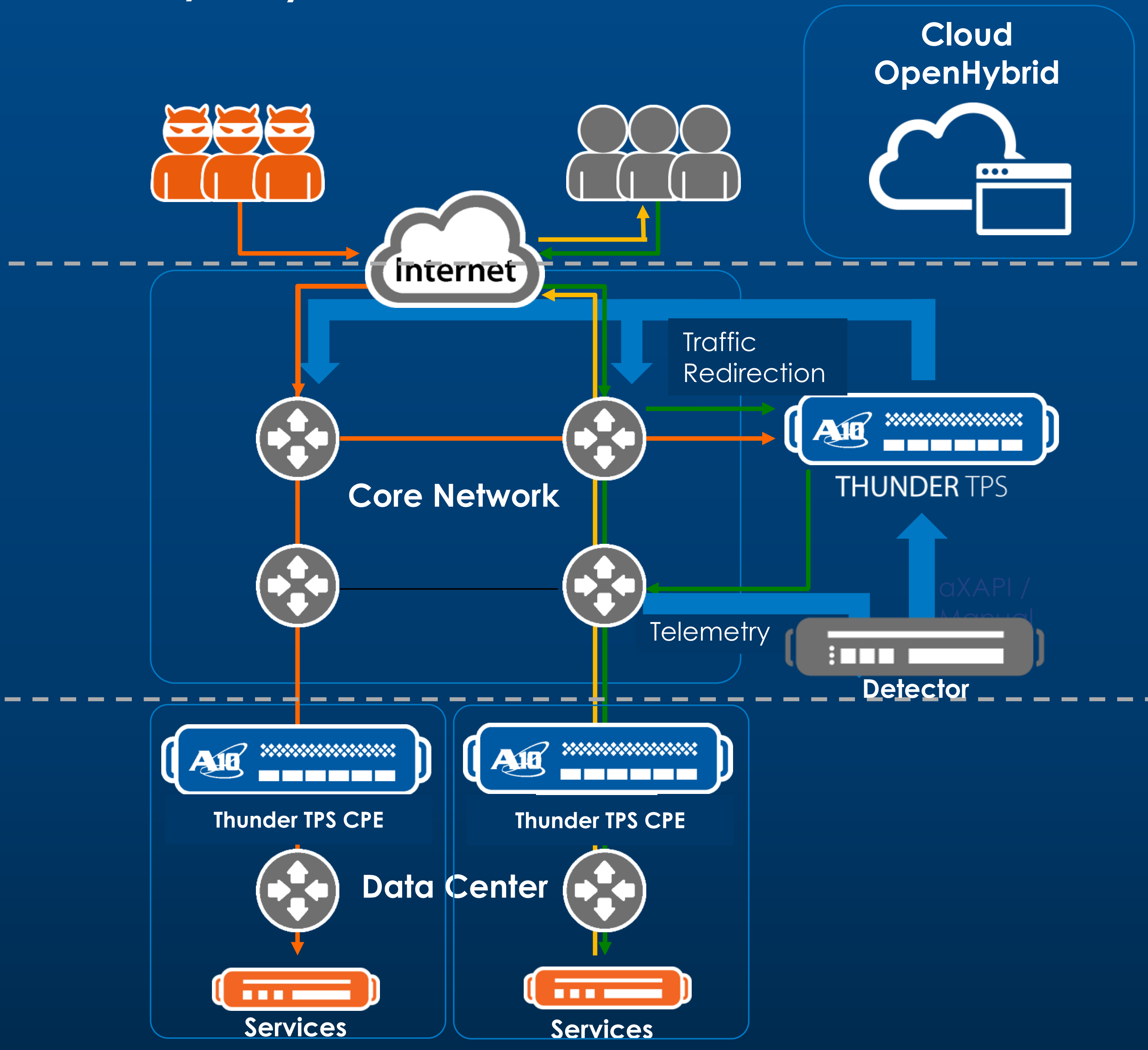
35% Network-Layer

34% Network/Volumetric

30% Application-Layer

Source: IDG, 2016

多層次(Multi-Layer) DDoS 防禦網路

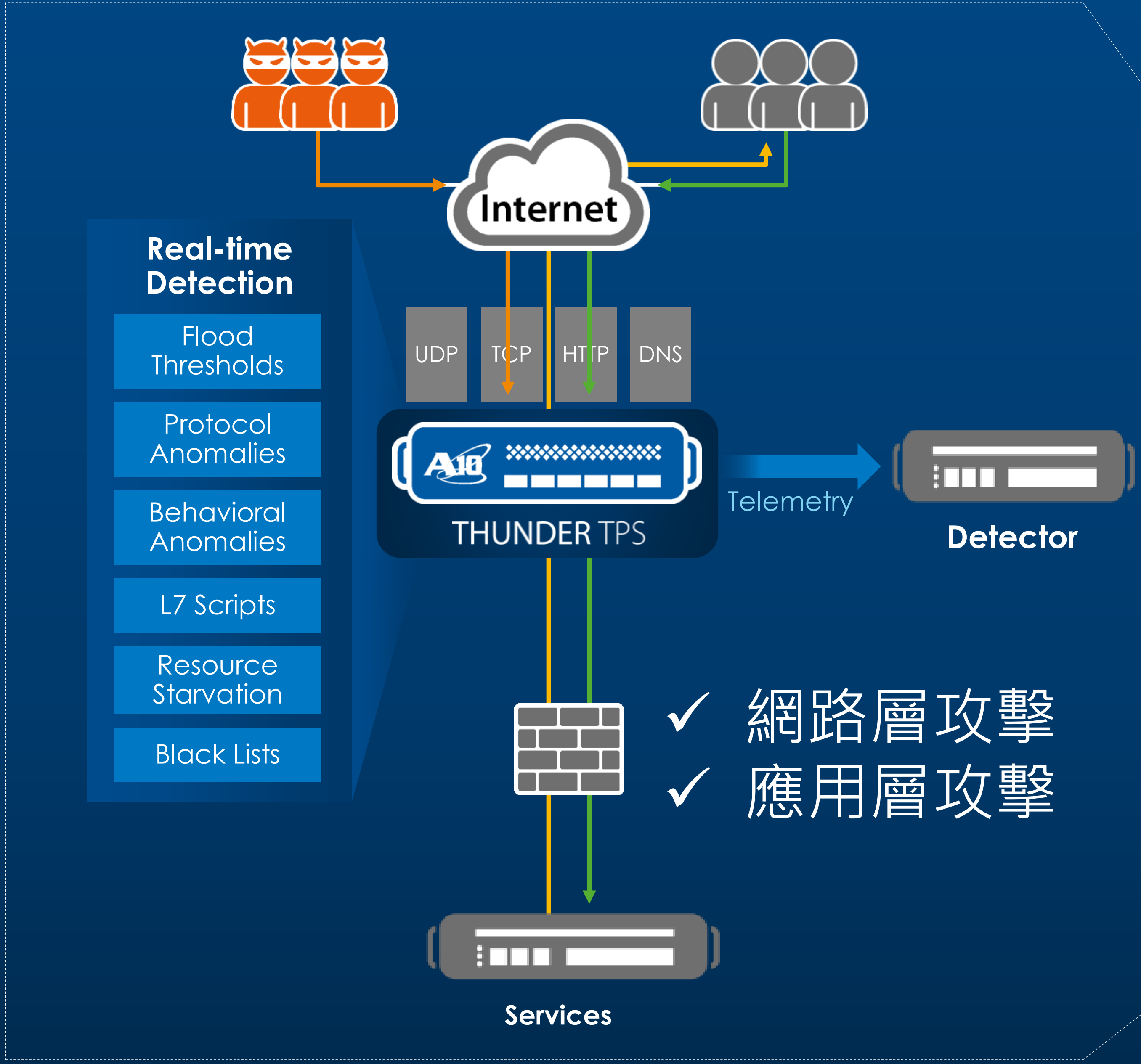


✓ 頻寬型攻擊

✓ 頻寬型攻擊
✓ 網路層攻擊

✓ 網路層攻擊
✓ 應用層攻擊

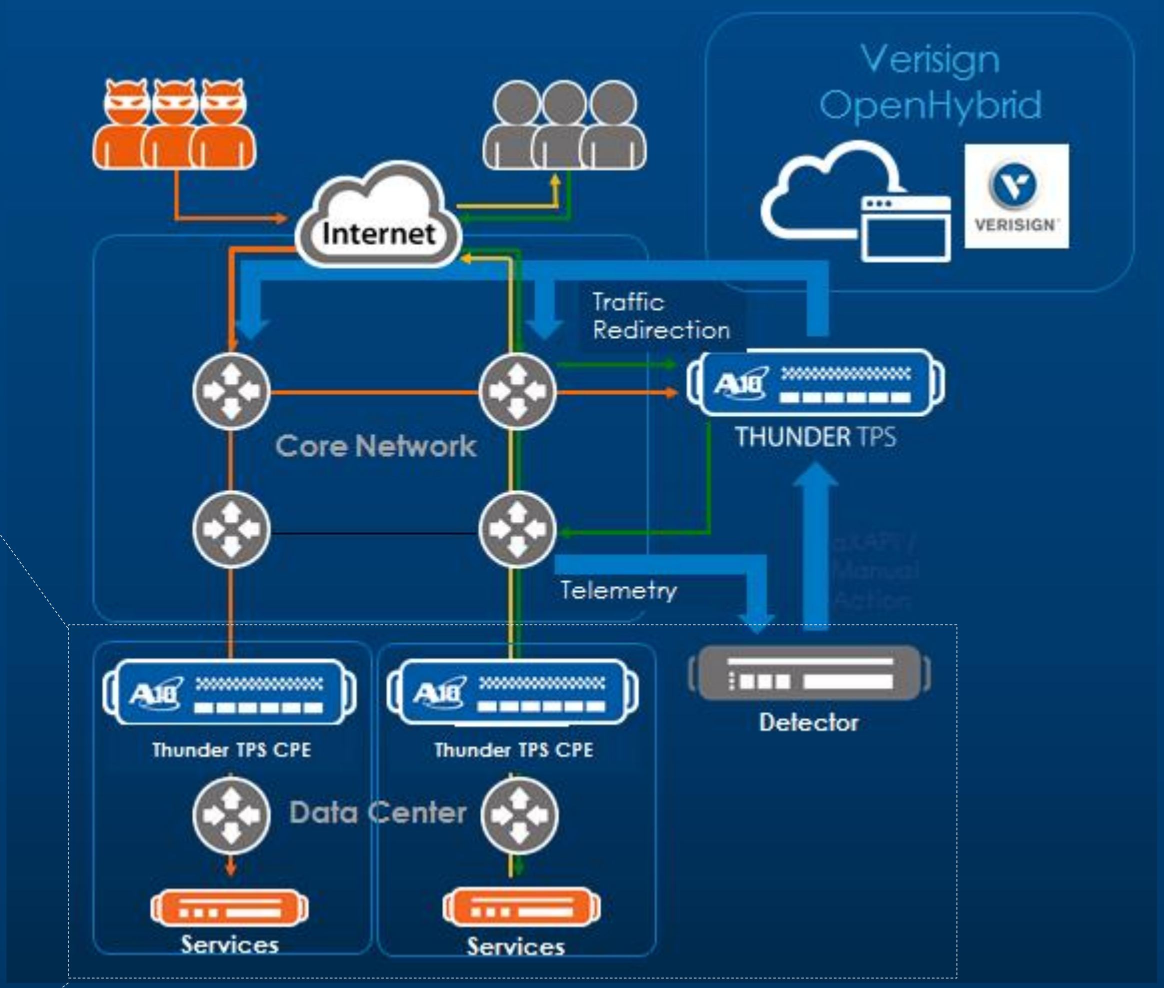
用戶端防禦架構 (CPE)



Real-time Detection

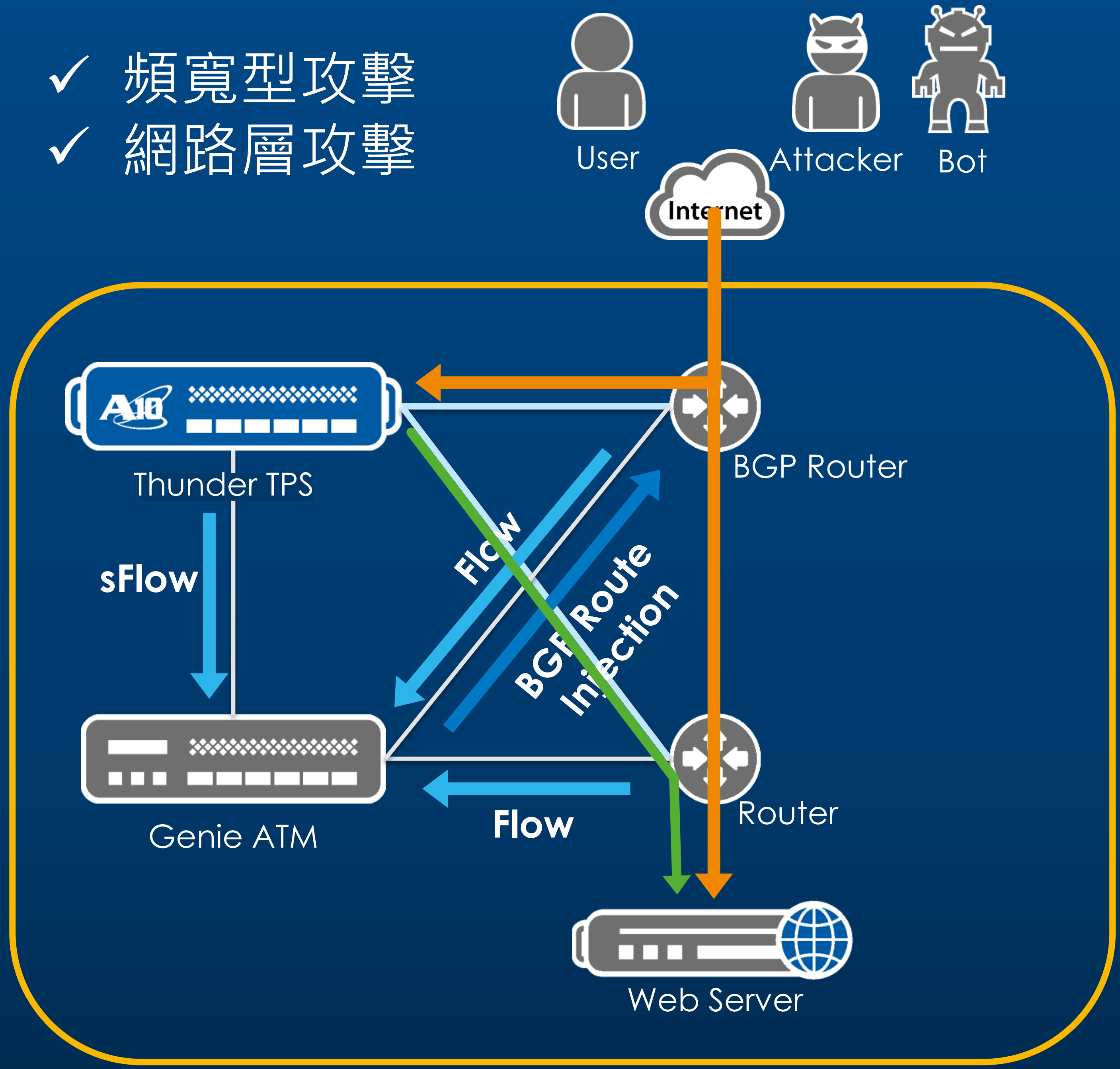
- Flood Thresholds
- Protocol Anomalies
- Behavioral Anomalies
- L7 Scripts
- Resource Starvation
- Black Lists

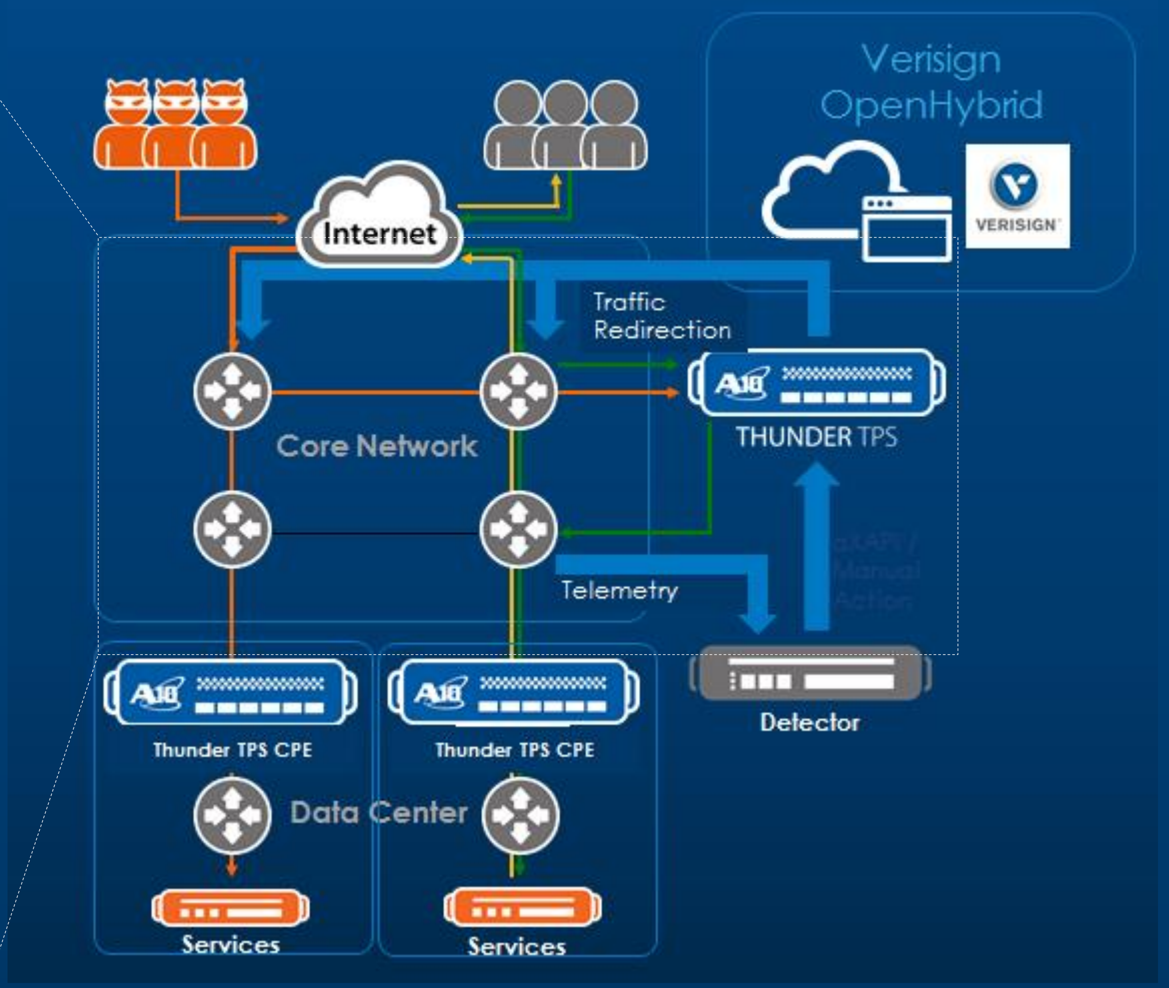
✓ 網路層攻擊
✓ 應用層攻擊



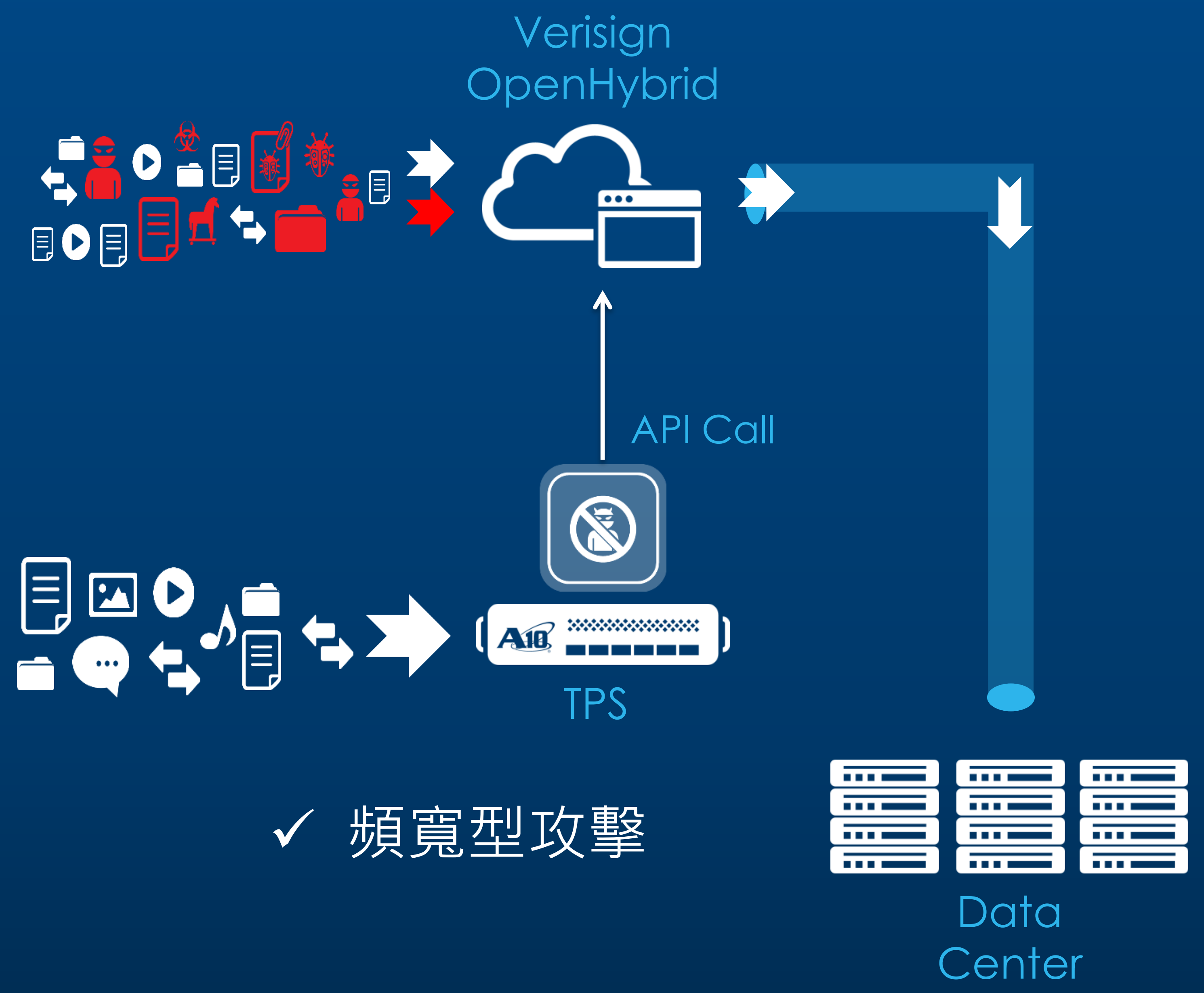
ISP 端流量清洗中心(Clean Pipe)

- ✓ 頻寬型攻擊
- ✓ 網路層攻擊

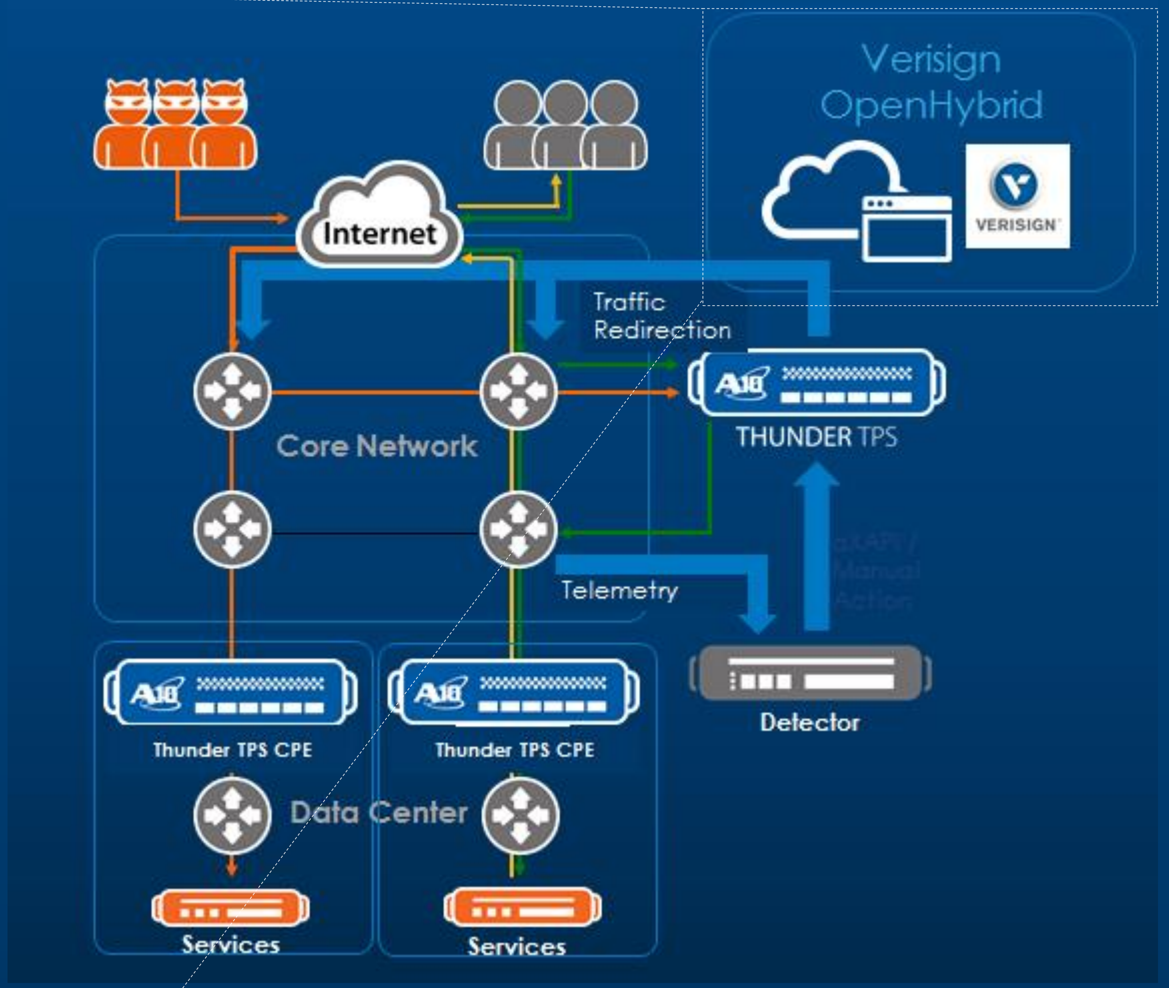




雲端流量清洗中心(Cloud Clean Pipe)

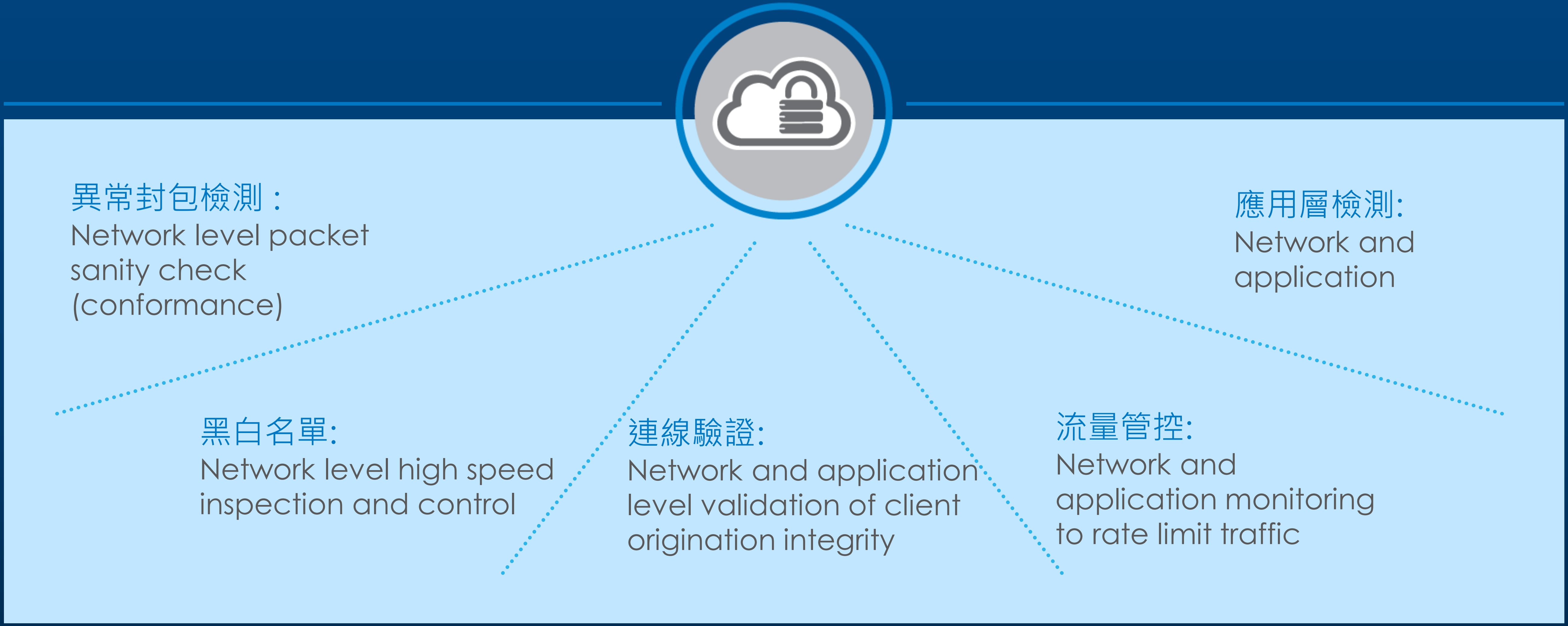


✓ 頻寬型攻擊



DDoS 攻擊偵測與防禦

透過五道防護，有效阻絕複合型 DDoS 攻擊



異常封包檢測：
Network level packet sanity check (conformance)

應用層檢測:
Network and application

黑白名單:
Network level high speed inspection and control

連線驗證:
Network and application level validation of client origination integrity

流量管控:
Network and application monitoring to rate limit traffic

異常封包檢測

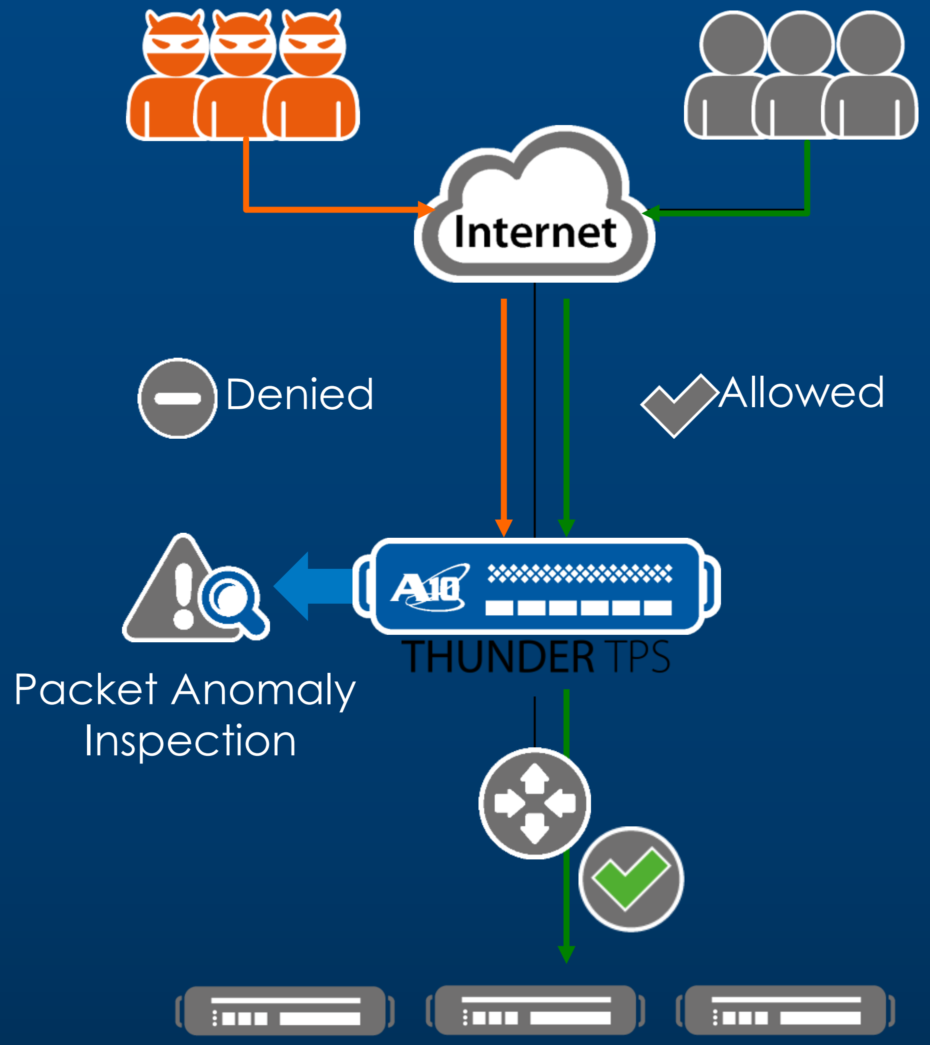
Packet sanity check in hardware and software

- Prevents volumetric attacks and protocol attacks
- Network checks (L3-4) for standard behavior

Examples

- TCP SYN & FIN,
- TCP XMAS (URG + FIN + PSH flags),
- LAND Attack (source IP = destination IP),
- TCP Bad Checksum,
- UDP Bad Checksum,
- more…

```
hping3 10.10.10.10 –s 80 –p 80 –S –a 10.10.10.10 –-flood
```



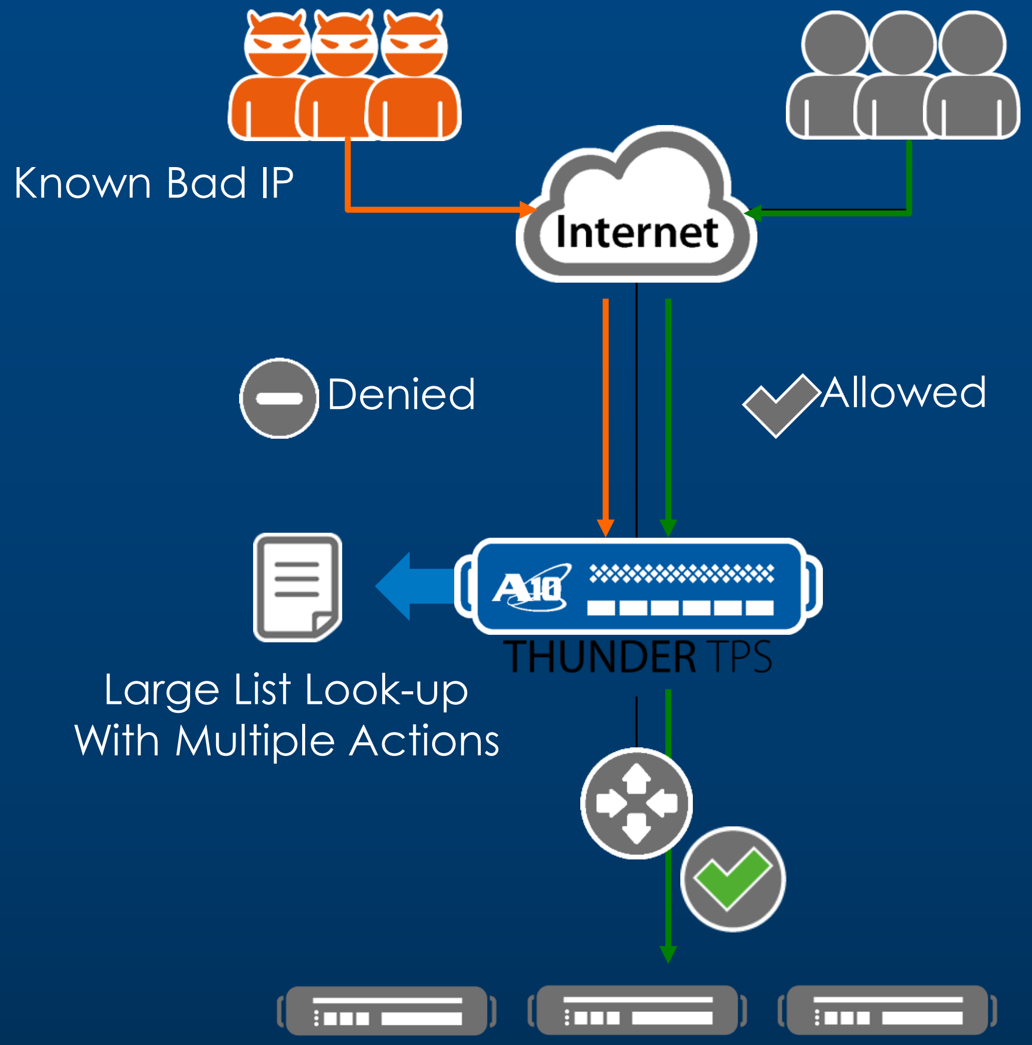
黑白名單

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

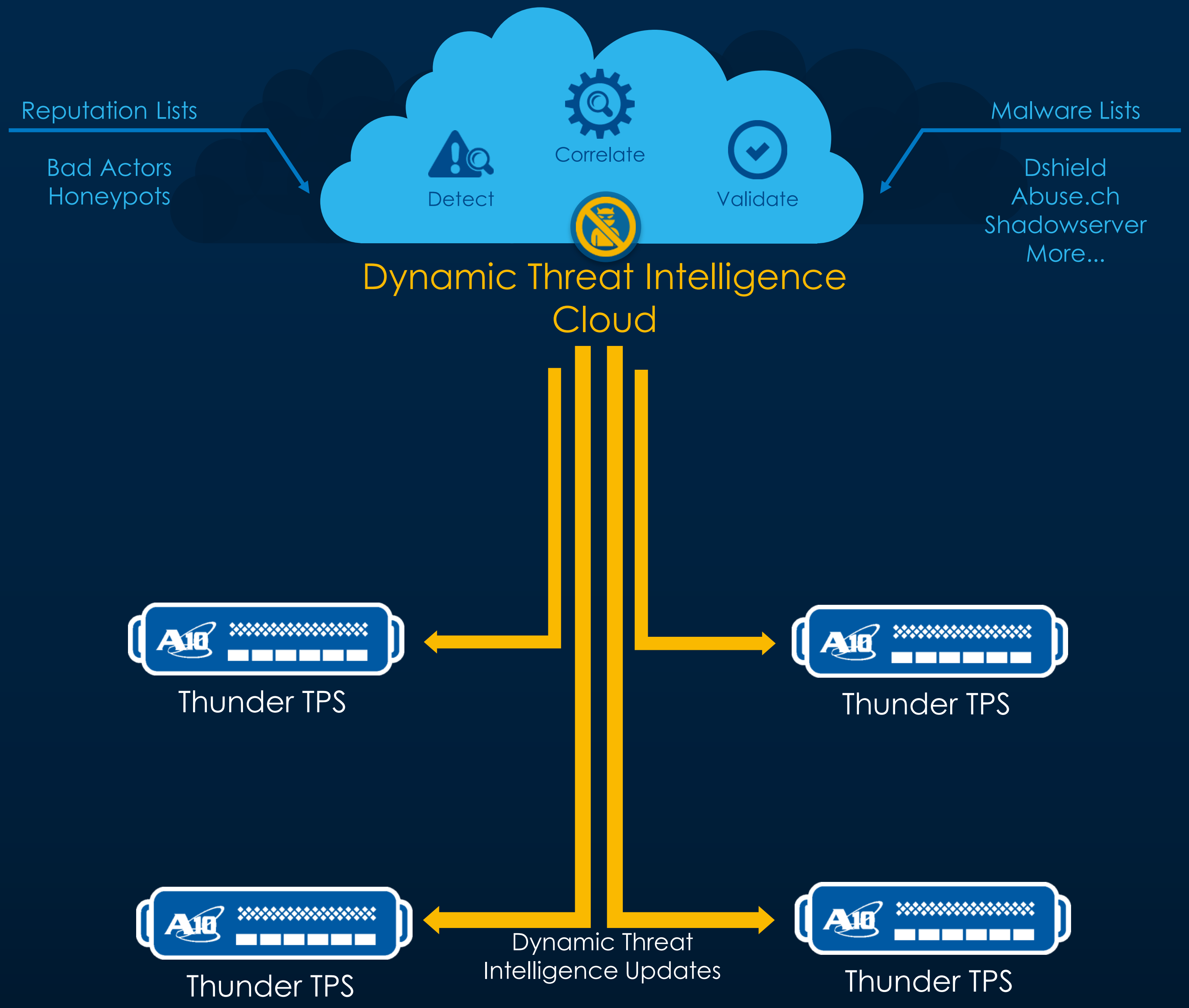
- Import 3rd Black/White Lists,
- Dynamic White List creates from SYN Cookie, SYN authentication & Action-on-ACK, DNS authentication
- Dynamic Black List with scanning detection, TCP abnormal packets threshold, HTTP header filter, more…



透過 ThreatSTOP 提供
A10 威脅情報服務

- 保護網路以避免未來的威脅
- 封鎖非 DDoS 相關威脅，例如垃圾郵件與網路釣魚
- 提高 Thunder TPS 效率

Powered by ThreatSTOP



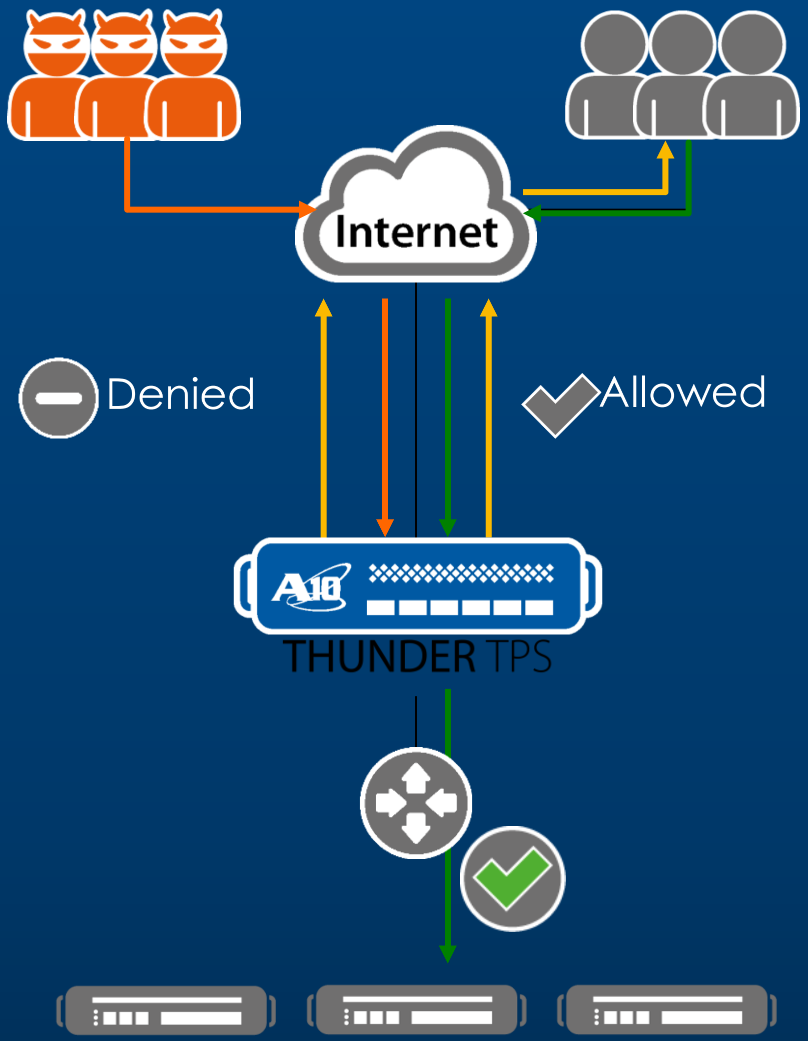
連線驗證

Validates client origination integrity

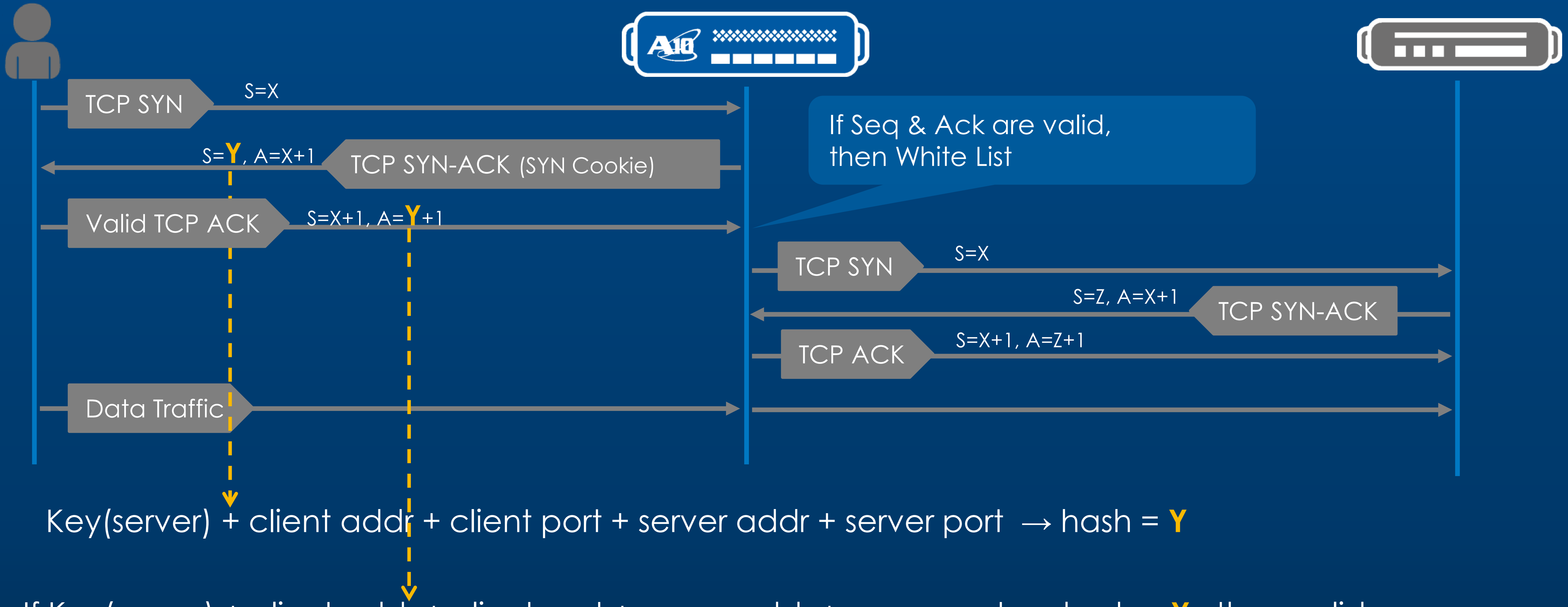
- Bot detection
- Prevents volumetric and protocol attacks
- Network and application checks (L3-7)

Examples

- TCP SYN authentication,
- TCP SYN cookie,
- UDP authentication,
- DNS authentication,
- HTTP Challenge,
- TCP error packet limit, more…



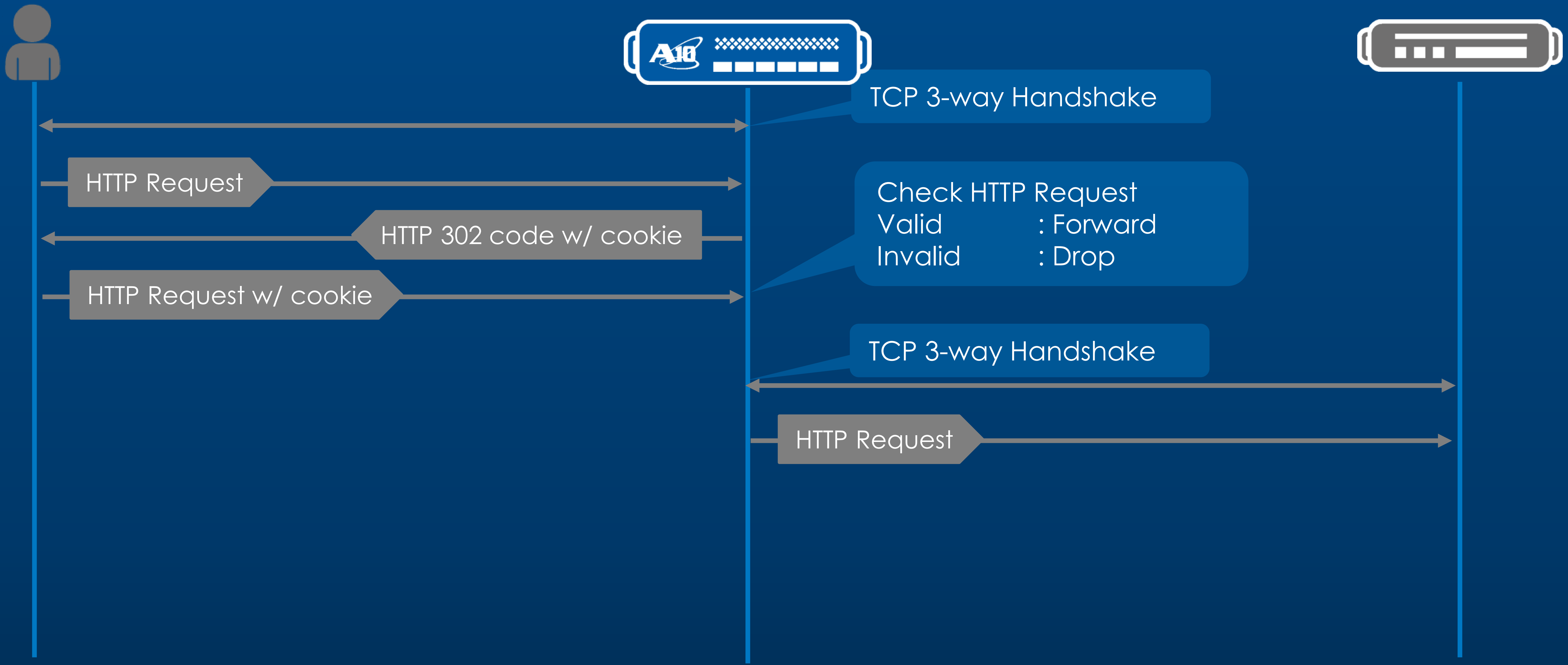
TCP SYN Cookie



Key(server) + client addr + client port + server addr + server port → hash = **Y**

If Key(server) + client addr + client port + server addr + server port → hash = **Y** , then valid

HTTP Authentication



TCP 3-way Handshake

HTTP Request

HTTP 302 code w/ cookie

HTTP Request w/ cookie

Check HTTP Request
Valid : Forward
Invalid : Drop

TCP 3-way Handshake

HTTP Request

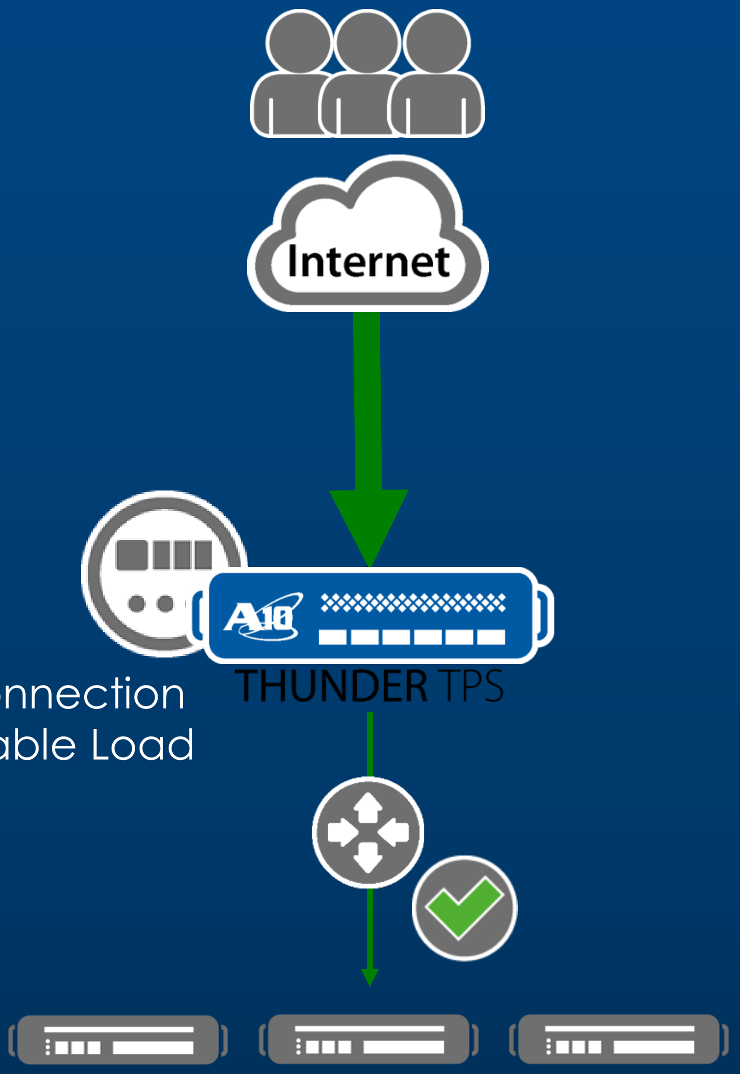
流量管控

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

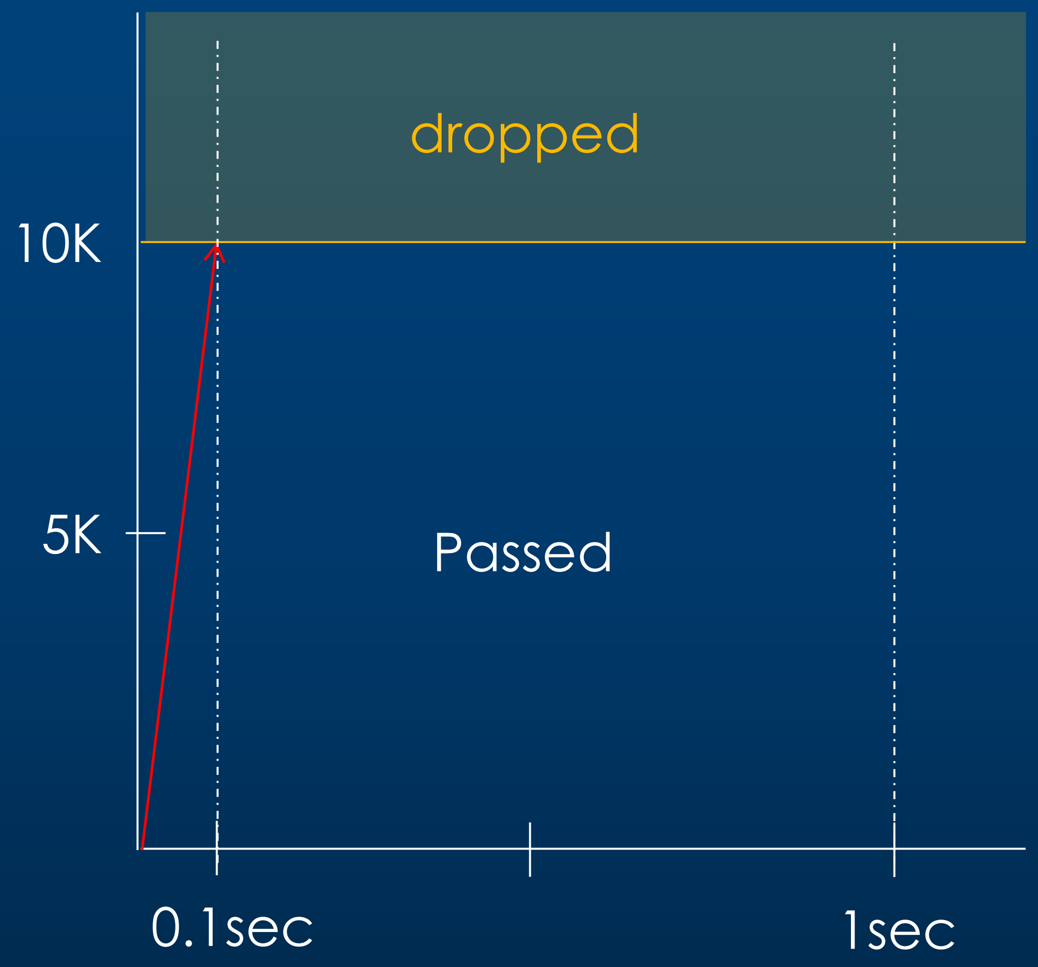
- Connection limit,
- Connection rate limit,
- Fragment rate limit,
- Packet rate limit,
- Bandwidth limit,
- HTTP Request rate limit,
- DNS request limit per DNS Record Type,
- SSL request rate limit, more…



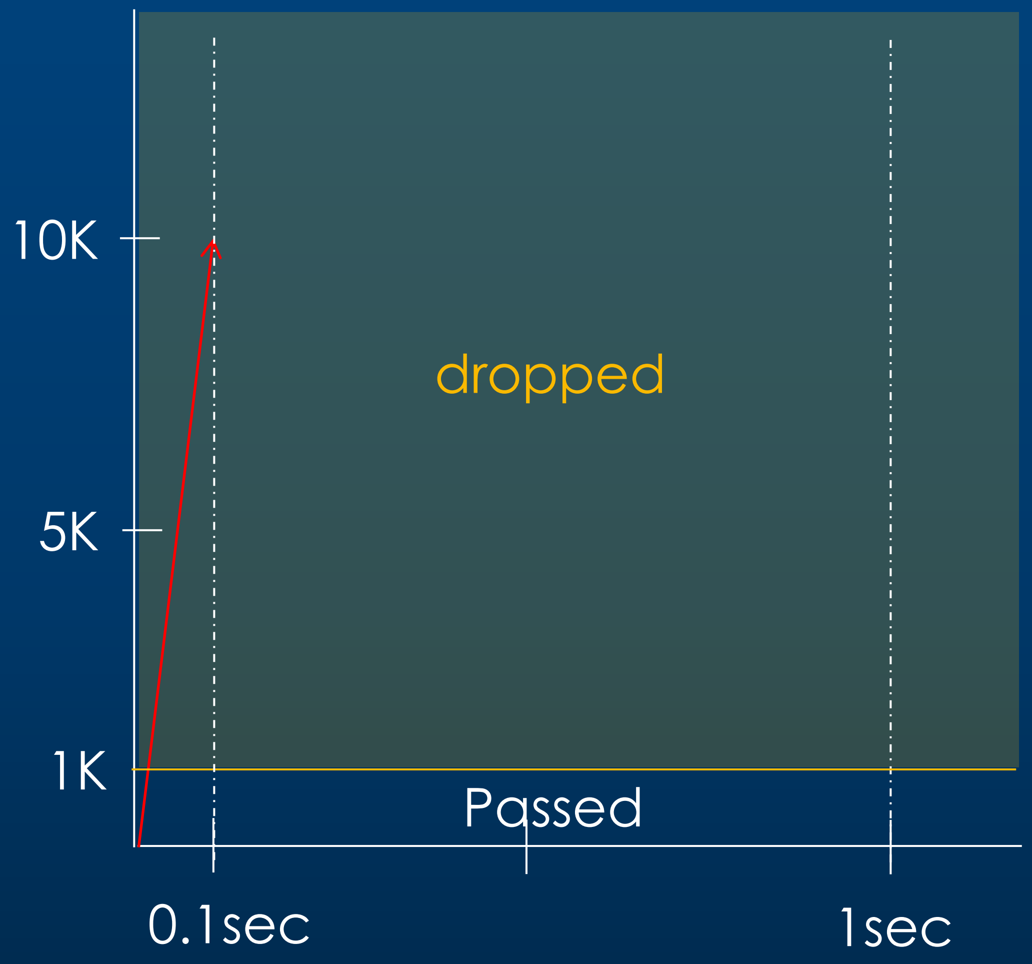
Rate and/or Connection Limits for Predictable Load

偵測頻率(0.1sec vs 1sec)

Rate interval = 1 sec
Rate limit = 10K / 1 sec = 1K / 0.1sec
Attack (Burst) : 10K / 0.1sec
Passed :10K , Dropped : 0K



Rate interval = 0.1 sec
Rate limit = 1K / 0.1sec = 10K / 1sec
Attack (Burst) : 10K / 0.1sec
Passed :1K , Dropped : 9K



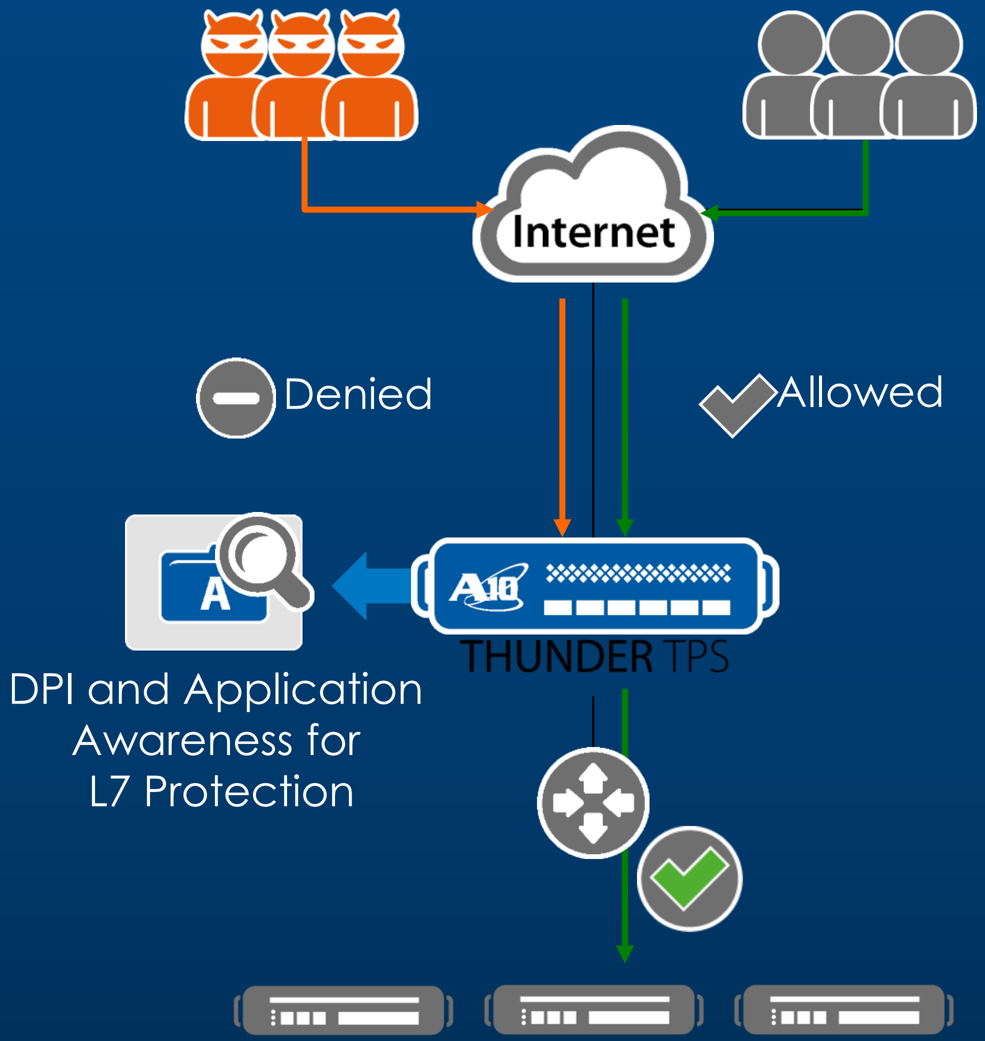
應用層行為檢測

Monitor and check traffic behavior

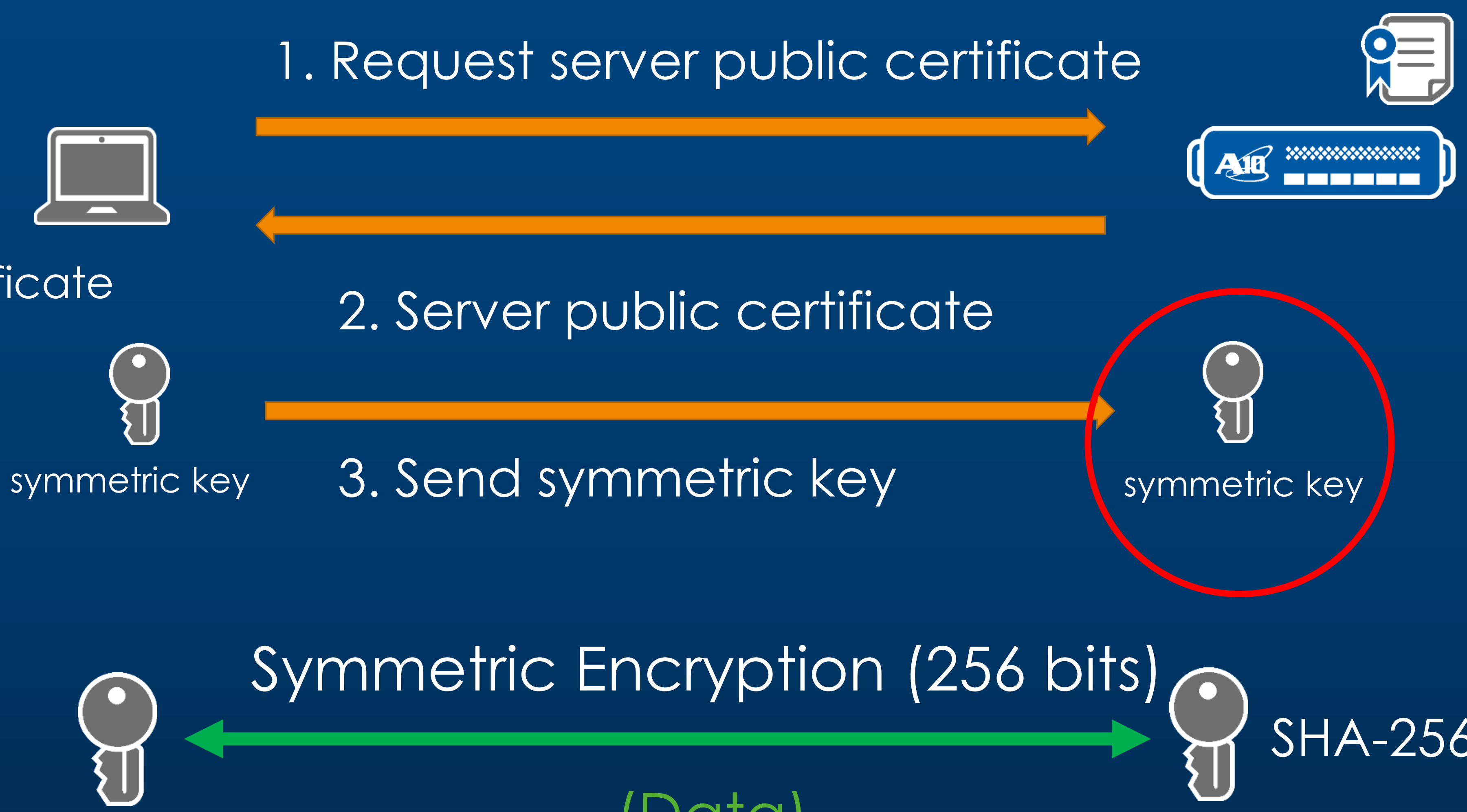
- 400+ global, destination-specific and behavioral counters
- All counters available through GUI, CLI, sFlow export
- Enforce specific values
- Network and application checks (L3-7)

Examples

- TCP template, HTTP template, DNS template, UDP template, SSL-L4 template, Scan detection, aFleX scripting, more…
- HTTP Slowloris
- SSL authentication as bot detection
- SSL Renegotiation



SSL Handshaking



Asymmetric Encryption (2048 bits)

Server public certificate (key)
Private Key (Signed by CA)

1. Request server public certificate

Server certificate
Validation

2. Server public certificate

symmetric key

3. Send symmetric key

symmetric key

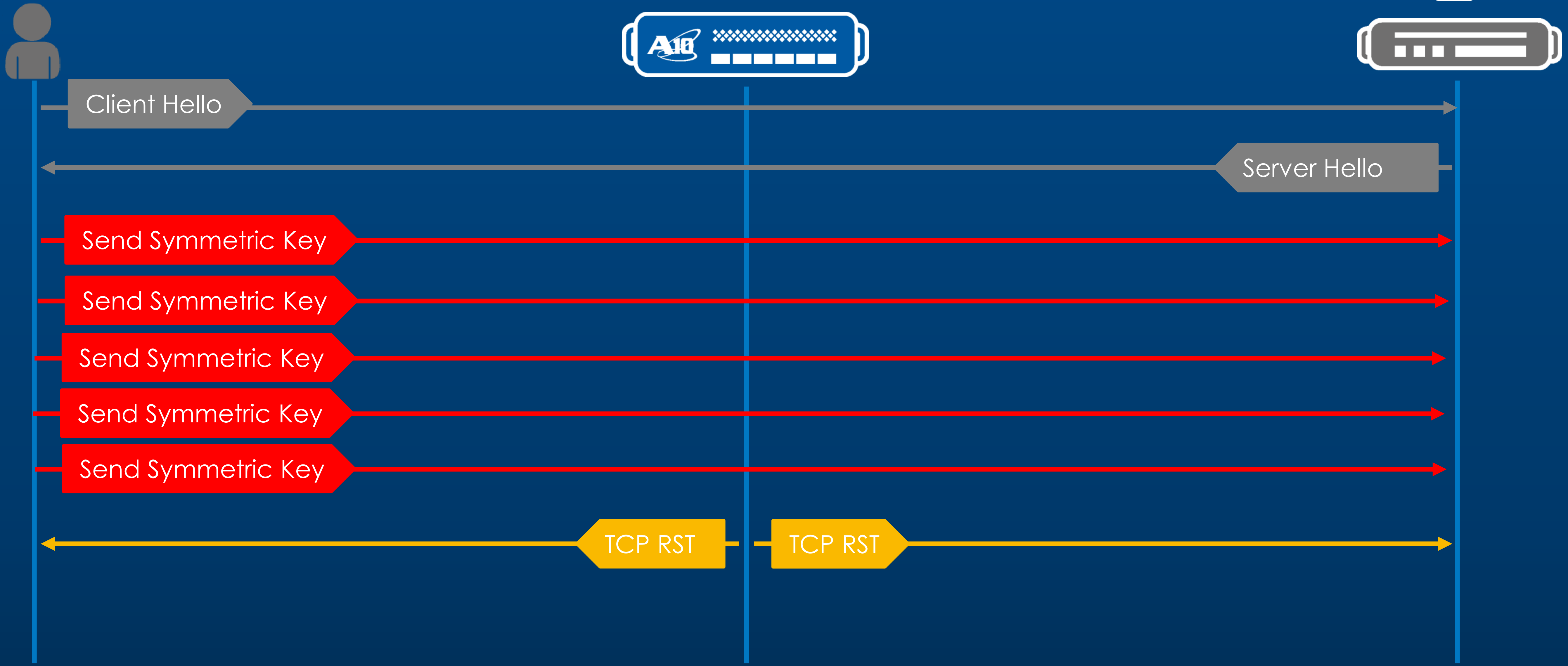
Symmetric Encryption (256 bits)

SHA-256(SHA-2)

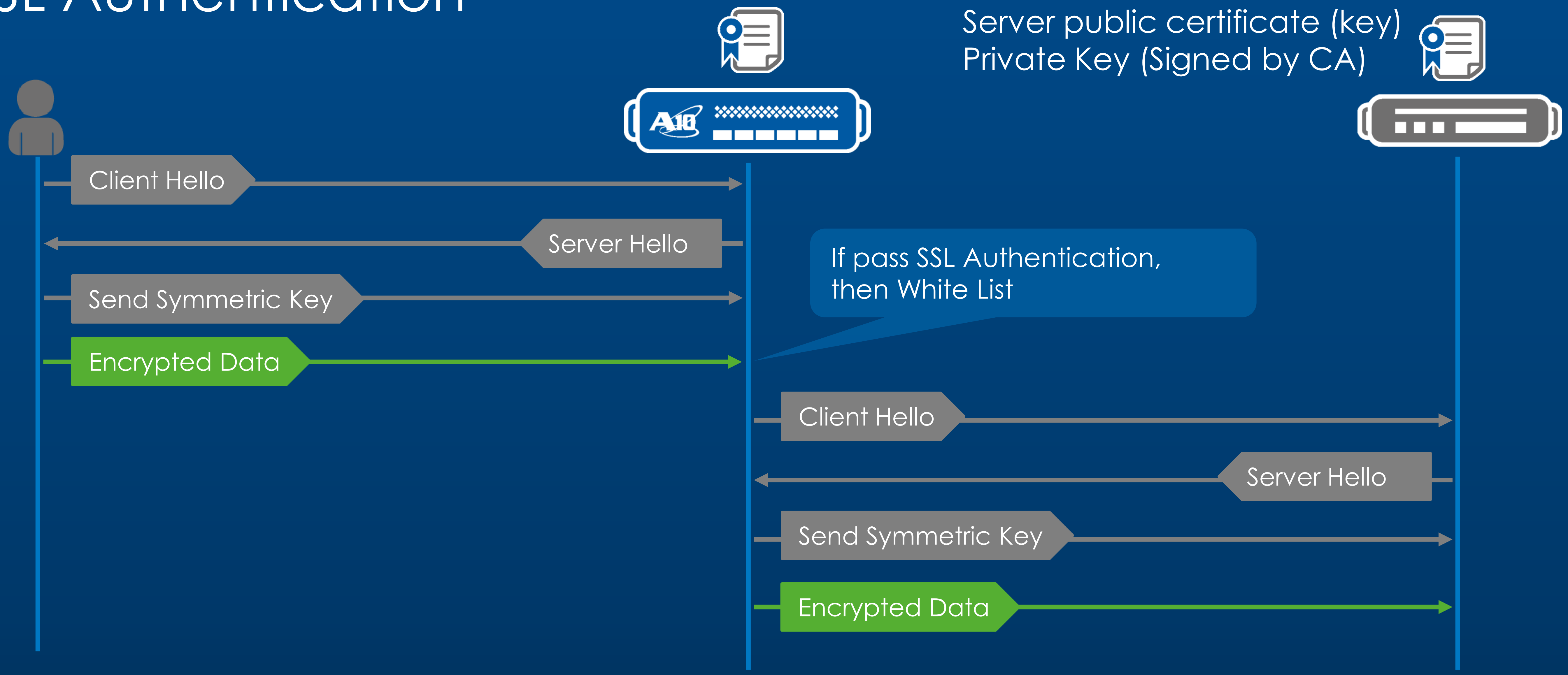
(Data)

SSL Renegotiation

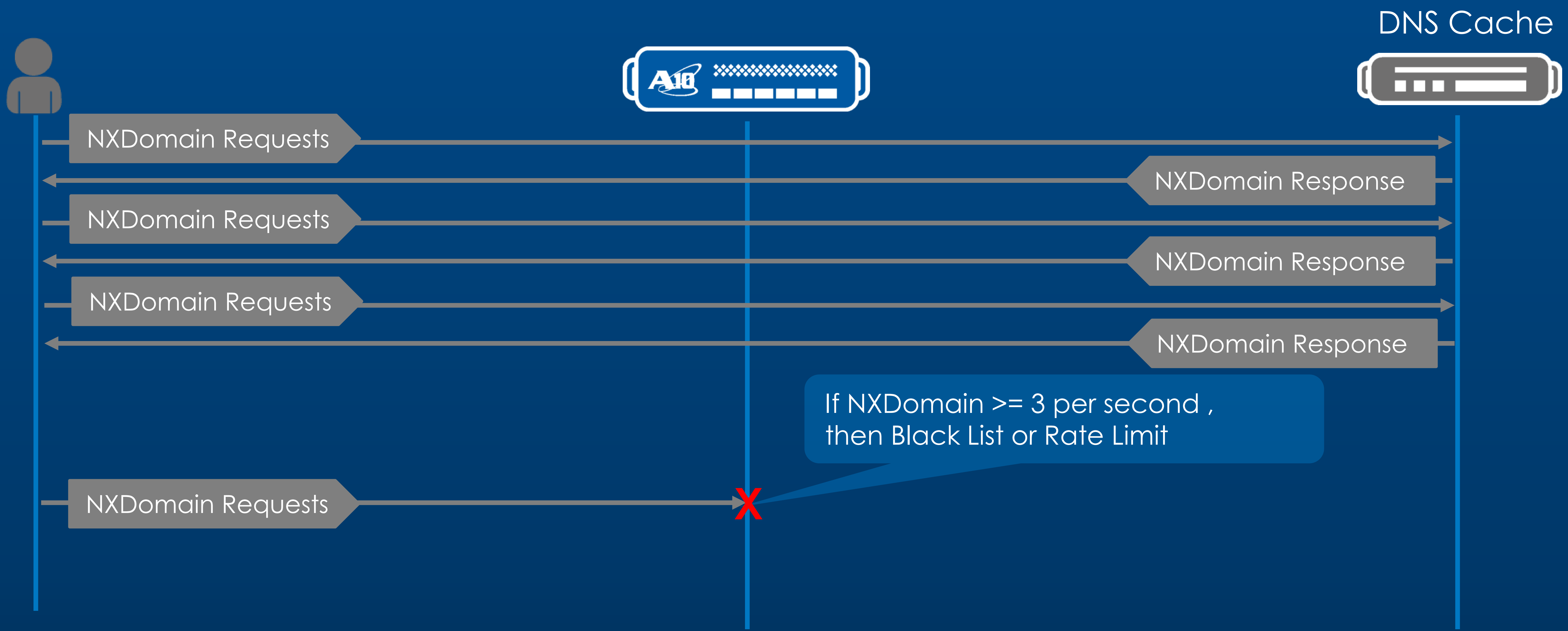
Server public certificate (key)
Private Key (Signed by CA)



SSL Authentication

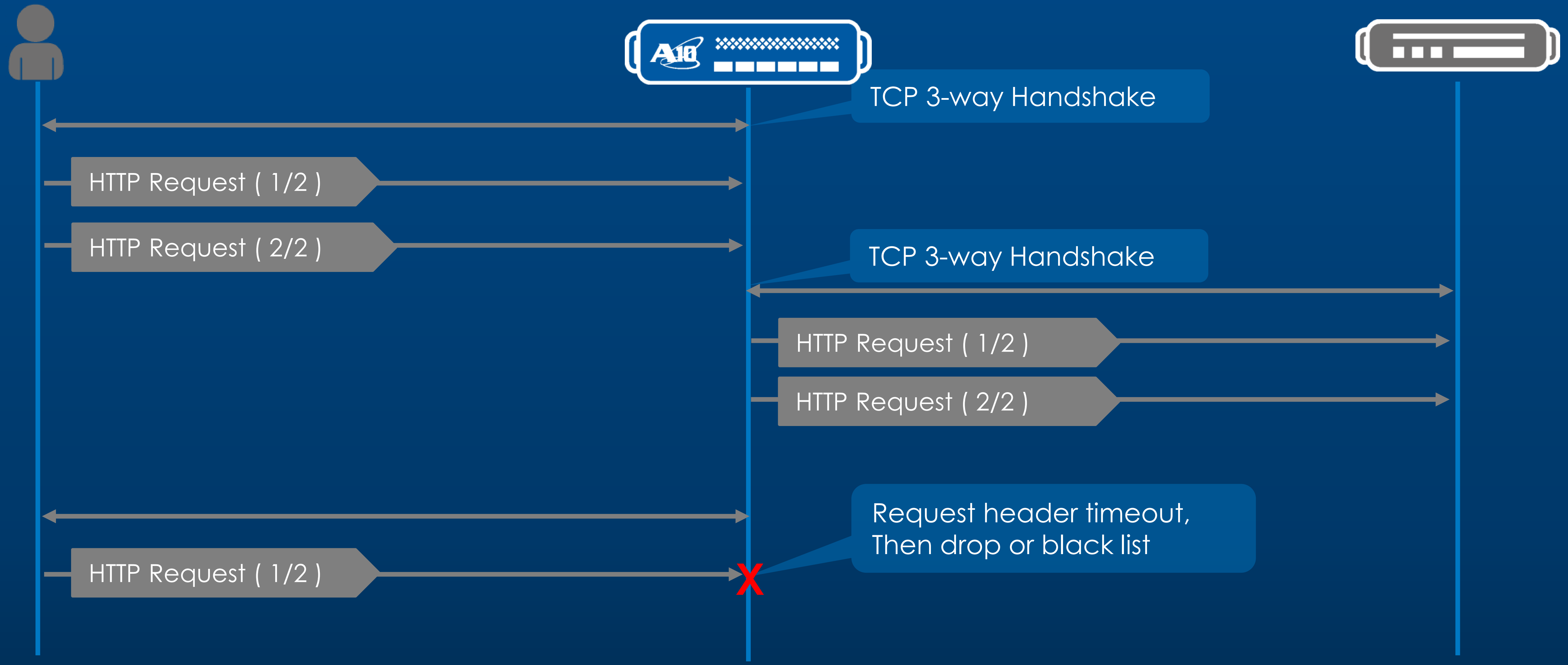


DNS NXDomain Mitigation



If NXDomain >= 3 per second ,
then Black List or Rate Limit

HTTP Slowloris



TCP 3-way Handshake

TCP 3-way Handshake

Request header timeout,
Then drop or black list

智慧型威脅偵測與防護

Smarter Detection

Automated baselining

Dynamic Mitigation

Progressive countermeasures

Extended Policy Actions

Including Verisign escalation

Protected Zones

Superset of “ddos dst”

智慧型威脅偵測：Automated Baselining

Sales Benefit

- Sell to organizations with limited security staff

Main Features

- Leverage multi-protocol counters providing deep visibility
- Apply this baseline intelligently to trigger security policies

Baselining: Indicators and Threshold

Baselining /behavioral learning for detection

- Building traffic pattern profiles (peacetime learning) for
  - **Dst zone threshold**
  - **Per source threshold**

Threshold for automatic escalation

- Traffic pattern profile = zone-profile consists of multiple indicators with the threshold

Zone profile and individual threshold can be manually configured

TCP (incl. HTTP port)

Packet Rate
SYN Rate
FIN Rate
RST Rate
Small Window ACK Rate
Empty ACK Rate
Small Payload Rate
Bytes-to / Bytes-from
SYN Rate / FIN Rate
Session Miss Rate
Packet Drop Rate
Pkt Drop / Pkt Rcv'd
Concurrent Sessions

UDP (incl. DNS port)

Packet Rate
Packet Drop Rate
Bytes-to / Bytes-from
Pkt Drop / Pkt Rcv'd
Concurrent Sessions

ICMP

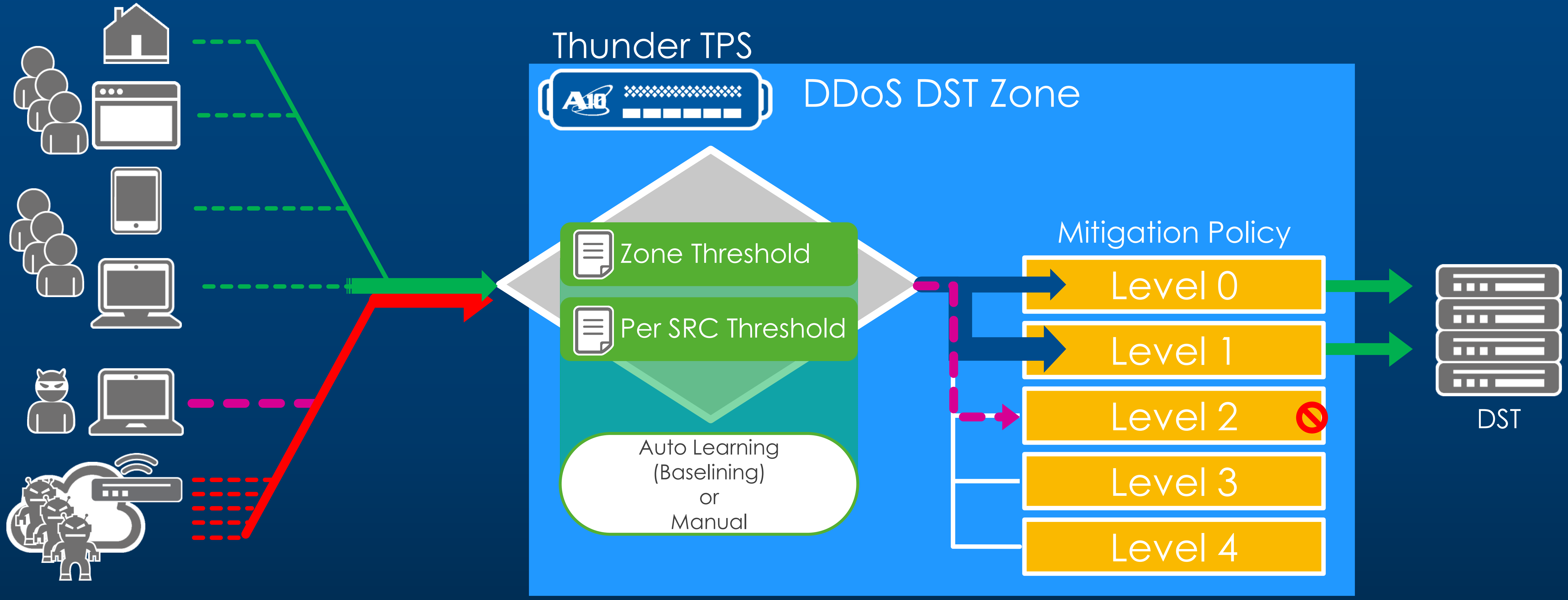
Packet Rate
Packet Drop Rate
Bytes-to / Bytes-from
Pkt Drop / Pkt Rcv'd

IP/Other

Packet Rate
Packet Drop Rate
Bytes-to / Bytes-from
Pkt Drop / Pkt Rcv'd
Fragment Rate

動態防禦政策: Progressive countermeasures

- 可透過漸趨嚴格的對策來提高可疑流量的等級，以期盡可能減少誤判的發生



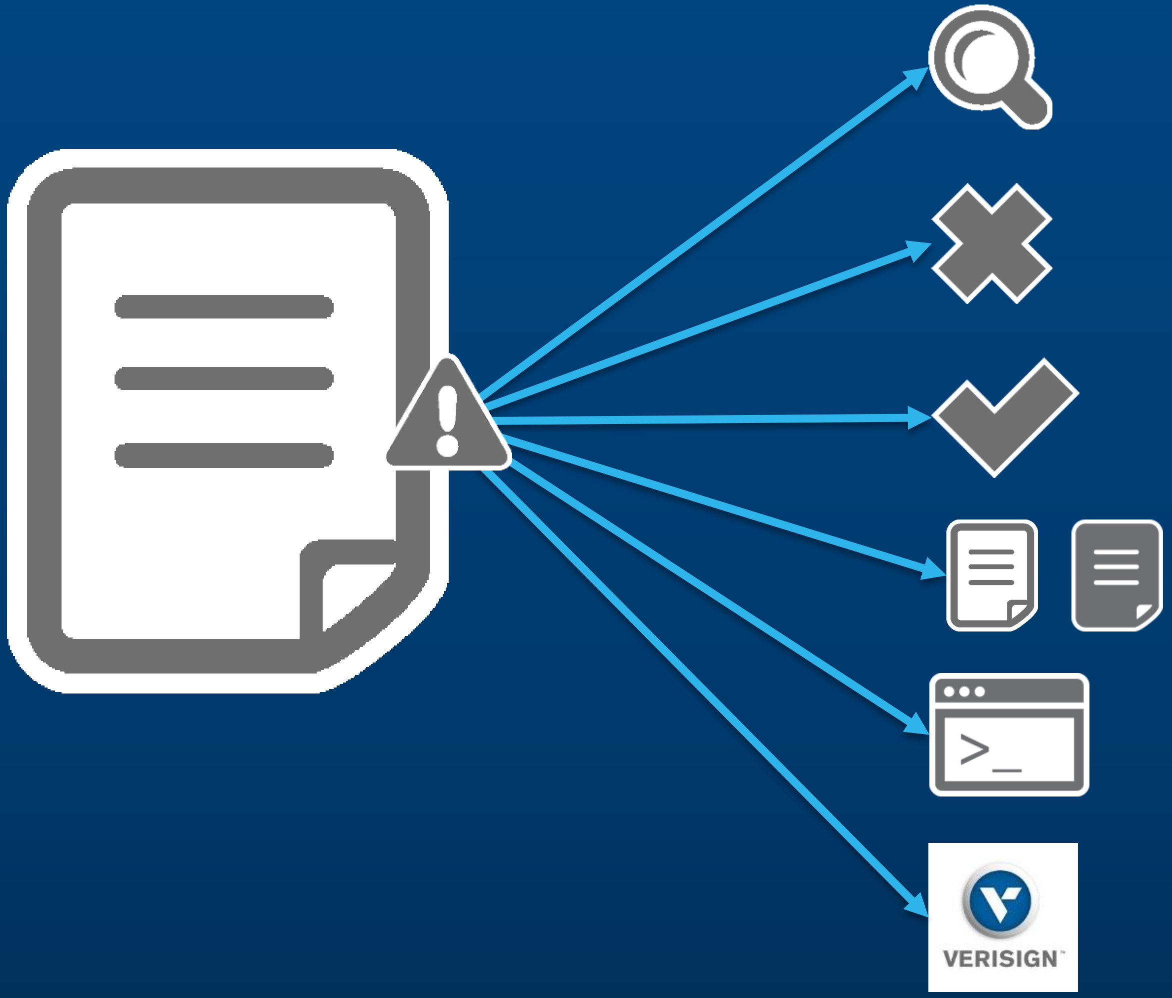
Extended Policy Actions

Sales Benefit

- More flexibility for DevOps, or easy automation for limited staff

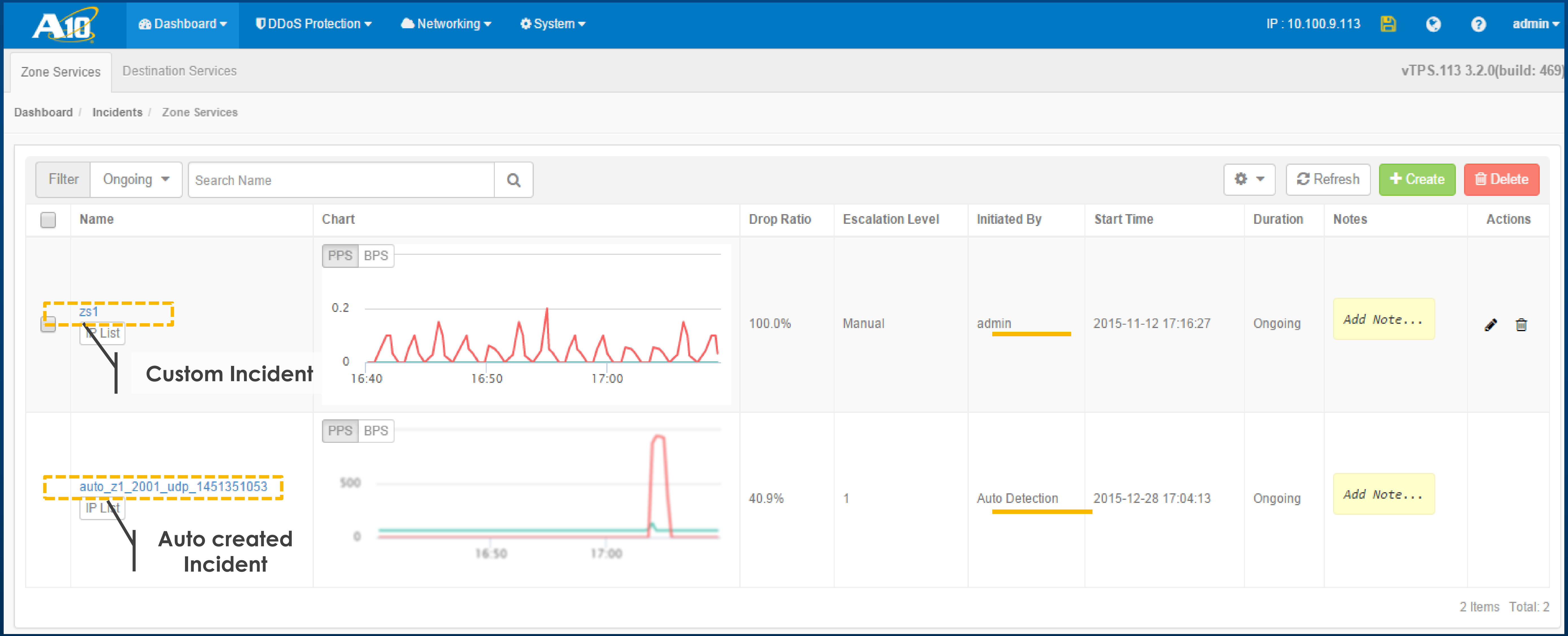
Main Features

- More elaborate action-lists
  - Logging
  - Capture packets
  - Drop the packet
  - Ignore – continue processing the packet
  - Reset the connection
  - Whitelist or blacklist the source
  - Custom script execution using bash



DDoS Dashboard - Incidents

List of incidents report for traffic visibility

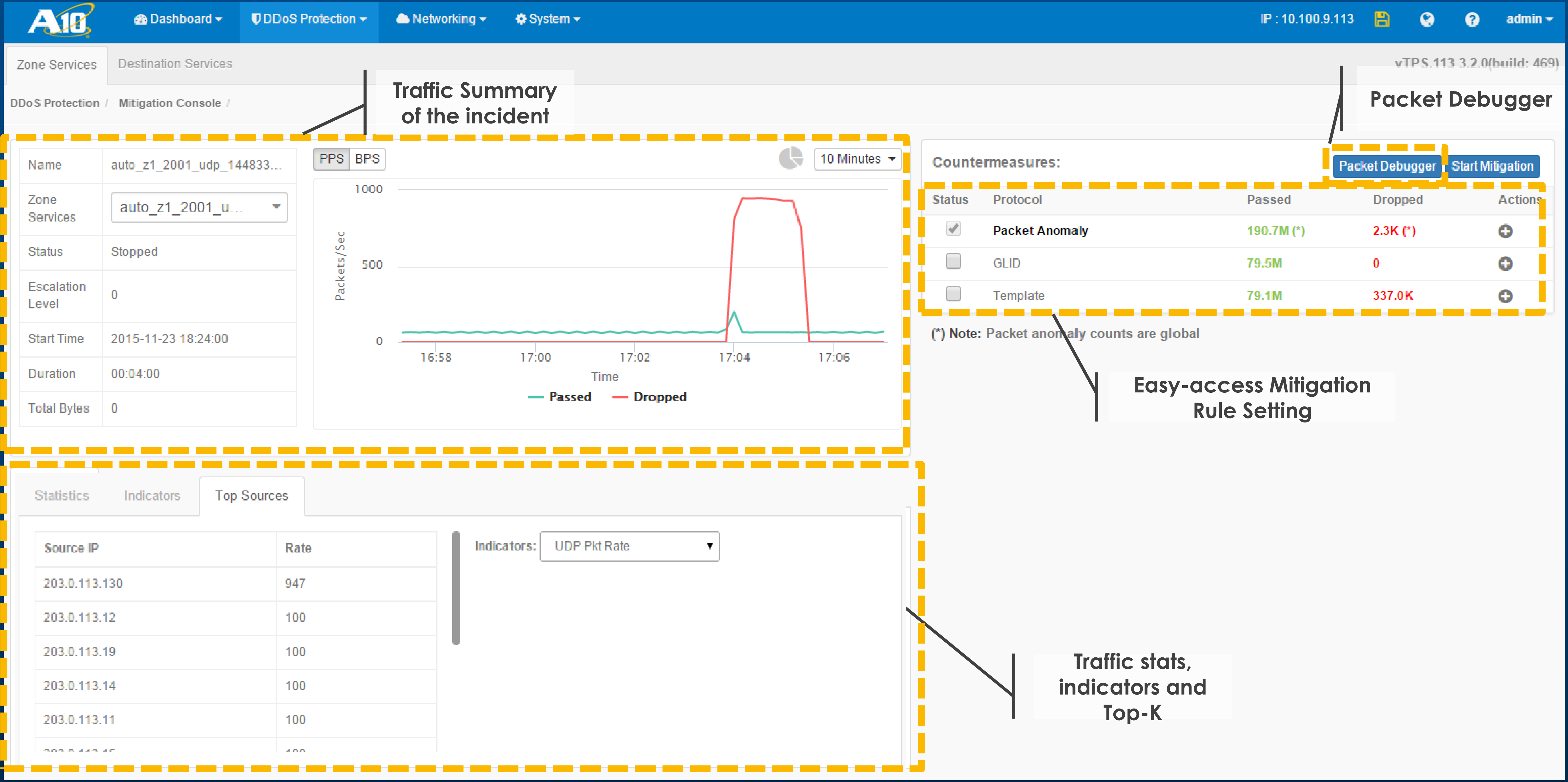


□	Name	Chart	Drop Ratio	Escalation Level	Initiated By	Start Time	Duration	Notes	Actions
□	zs1 IP List		100.0%	Manual	admin	2015-11-12 17:16:27	Ongoing	Add Note...	
	auto_z1_2001_udp_1451351053 IP List		40.9%	1	Auto Detection	2015-12-28 17:04:13	Ongoing	Add Note...	

Custom Incident

Auto created Incident

DDoS Protection – Mitigation Console



DDoS Protection / Mitigation Console /

Name	auto_z1_2001_udp_144833...
Zone Services	auto_z1_2001_u...
Status	Stopped
Escalation Level	0
Start Time	2015-11-23 18:24:00
Duration	00:04:00
Total Bytes	0

Countermeasures:

Status	Protocol	Passed	Dropped	Actions
☑	Packet Anomaly	190.7M (*)	2.3K (*)	⊕
☐	GLID	79.5M	0	⊕
☐	Template	79.1M	337.0K	⊕

(*) Note: Packet anomaly counts are global

Source IP	Rate
203.0.113.130	947
203.0.113.12	100
203.0.113.19	100
203.0.113.14	100
203.0.113.11	100

Indicators: UDP Pkt Rate

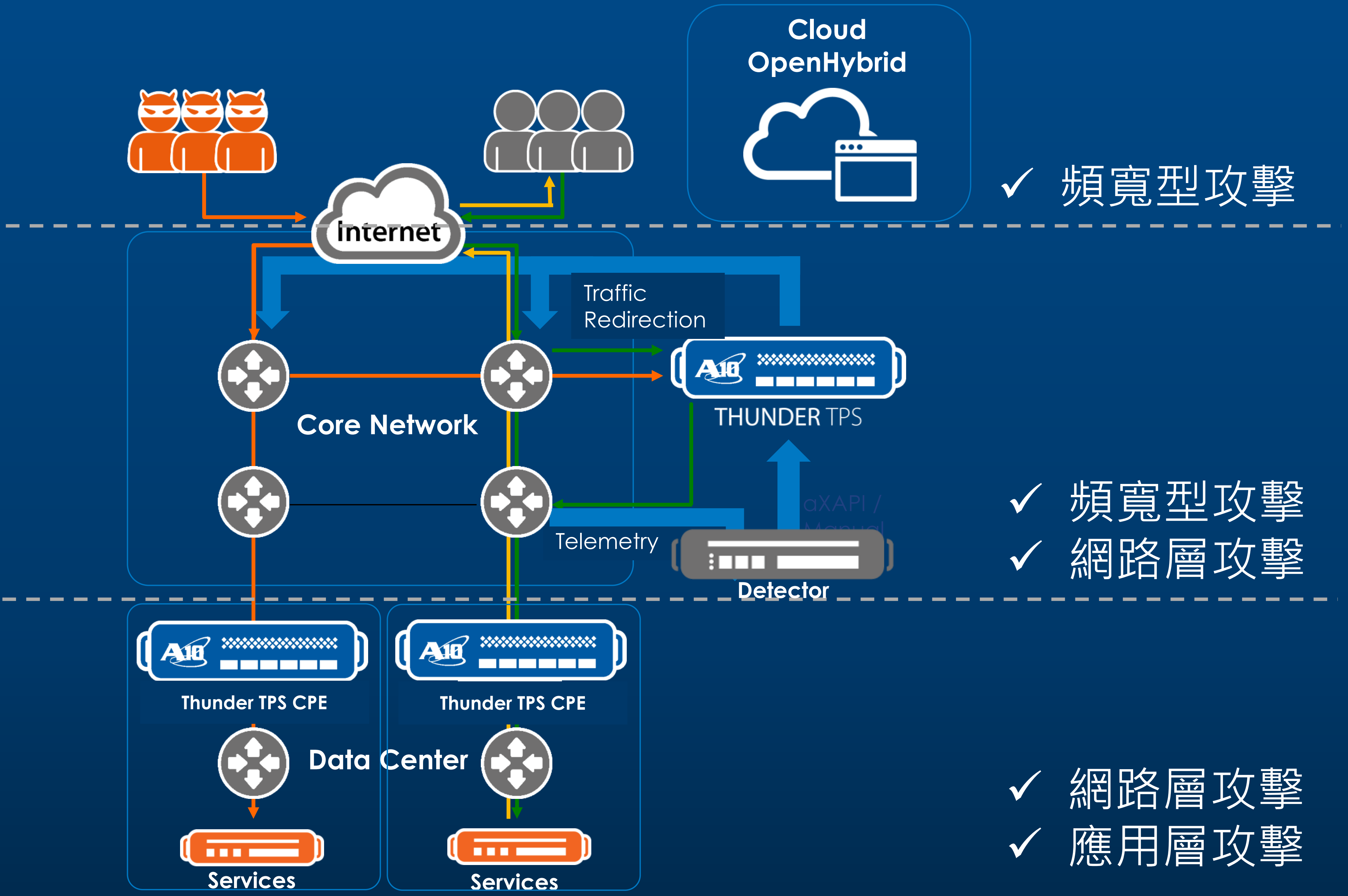
Traffic Summary of the incident

Packet Debugger

Easy-access Mitigation Rule Setting

Traffic stats, indicators and Top-K

A10 Thunder TPS Solution



✓ 頻寬型攻擊

✓ 頻寬型攻擊
✓ 網路層攻擊

✓ 網路層攻擊
✓ 應用層攻擊

Thank you