台灣大哥大
企業服務

台哥大DDoS防禦服務

2022/01

Agenda

何謂DDoS攻擊?

DDoS攻擊型態

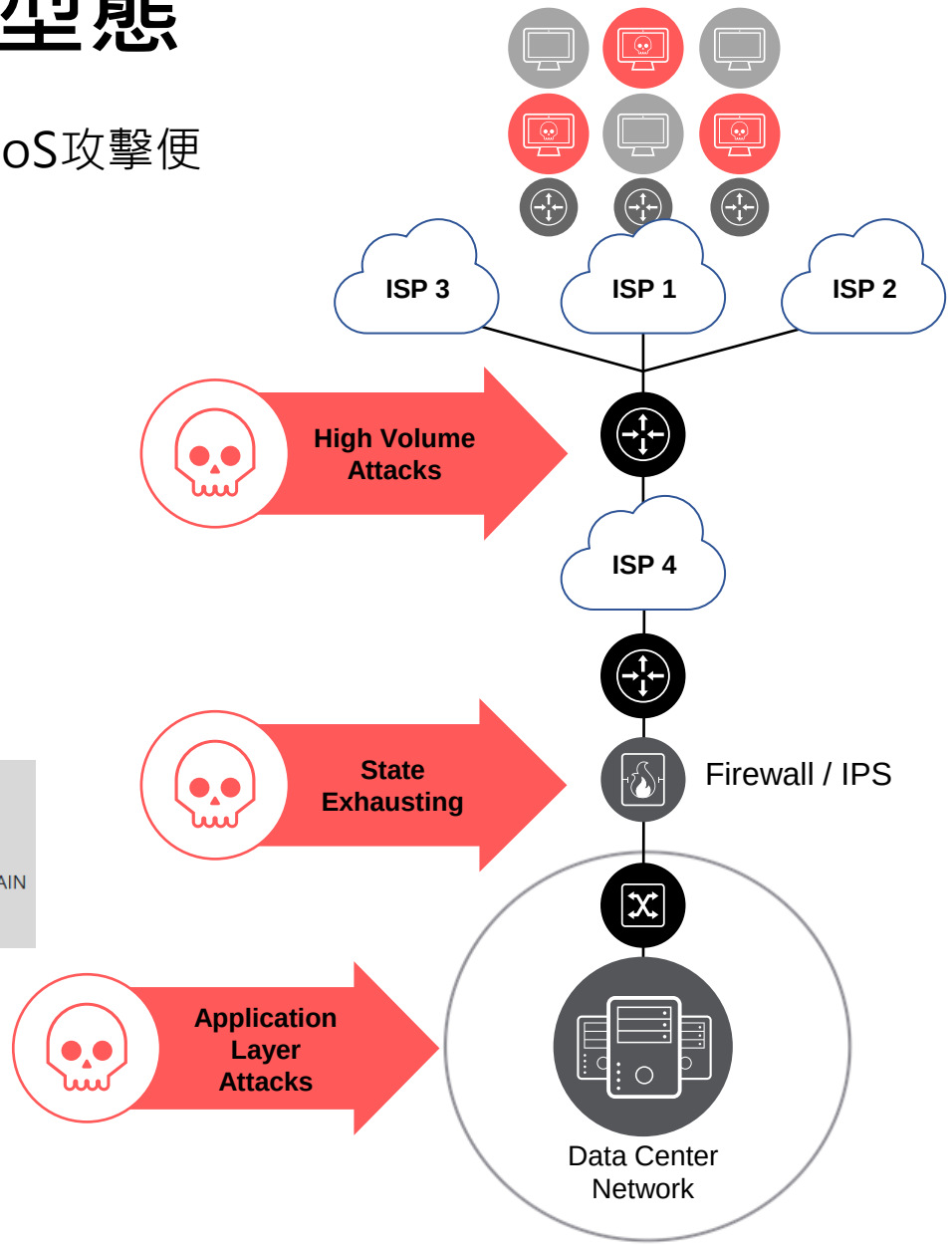
基於不同的目的， 如因政治事件、偷竊機敏資料...等，DDoS攻擊便有不同的型態及不同的排列組合方式進行。

- **流量攻擊**
  - 塞爆頻寬的暴力洪水攻擊
- **狀態耗盡攻擊**
  - 針對資安設備耗盡其連線數(Session)
- **應用層攻擊**
  - 癱瘓特定應用服務

- **ICMP Flood**
- IP/ICMP Fragmentation
- UDP Flood
- IPSec Flood (IKE/ISAKMP association attempts)

- **SYN Flood**
- SSL Exhaustion
- DNS query/NXDOMAIN floods

- **BGP Hijacking**
- Slowloris
- Slow Post
- Slow Read
- HTTP/S Flood
- Low and Slow Attack
- Large Payload POST requests
- Mimicked User Browsing

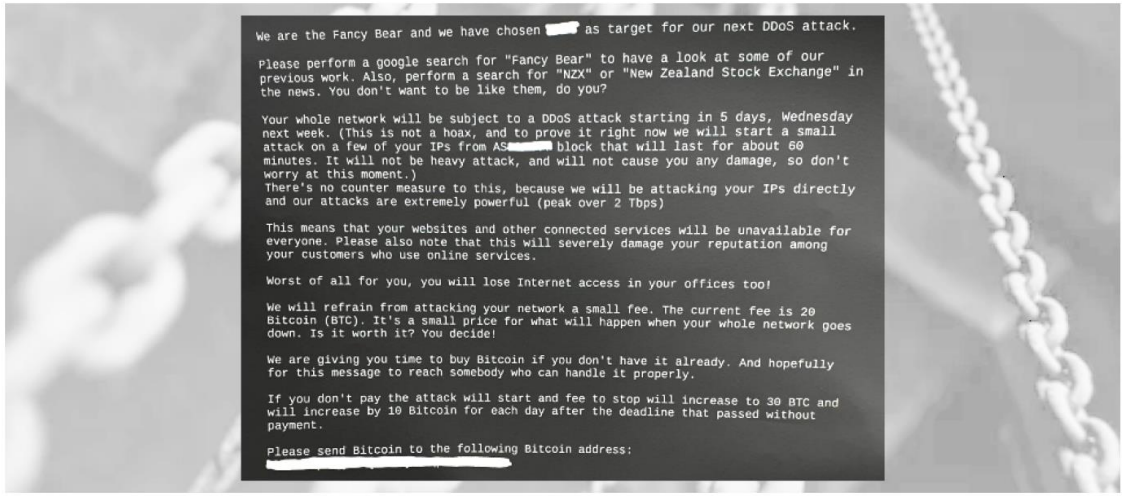


DDoS阻斷服務攻擊仍為常態

【2021資安大預測】趨勢10：製造業資安｜駭客鎖定製造業發動目標式勒索和DDoS攻擊，成為新常態

駭客利用網站漏洞入侵企業後，加密系統與檔案後進行勒索；或是受到DDoS攻擊，曾有臺灣業者面臨持續8小時、100Gbps的流量

文/ 黃彥棻 | 2021-01-13 發表

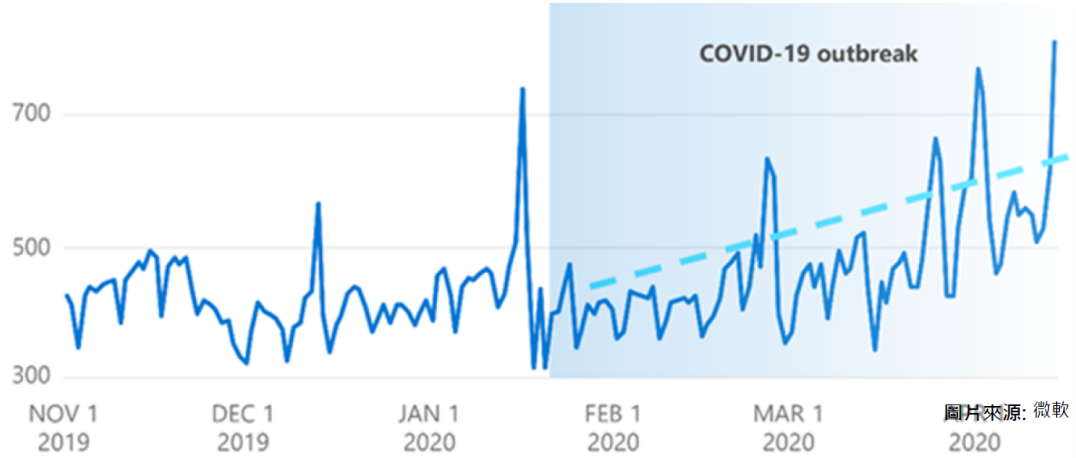


根據不具名消息來源指出，有自稱是Fancy Bear的駭客組織寄信給臺灣的高科技業者宣稱，企業如果不支付10個或是20個比特幣，將對企業發動高達2Tbps攻擊流量的DDoS攻擊。

Cloud周報第97期：疫情導致DDoS攻擊次數增加，Azure去年每日平均遭500次攻擊

疫情使得數十億人必須在家遠距工作、學習，讓網路流量暴增。微軟表示，這樣的轉變使攻擊者不需產生這麼大的流量，就能阻斷服務，且攻擊者挾巨大流量發動DDoS攻擊，使得企業更難區分惡意流量。疫情導致DDoS攻擊次數增加，去年Azure總共防禦了20萬次針對全球基礎設施的DDoS攻擊

文/ 黃郁芸 | 2021-02-25 發表



圖片來源: 微軟

DDoS已是金融企業必要防禦措施

各國金管單位均已將DDoS列為網銀必要防禦措施

台灣金管會

依據金融監督管理委員會105年7月6日金管銀國字第10500102770號函說明二辦理

說明：為避免金融機構網際網路應用系統遭受DDoS攻擊，導致無法提供電子銀行金融服務， 請貴機構對DDoS攻擊建立監控與事故應變機制，並於每年進行程序演練.....

中國銀監會

电子银行业务的风险管理原则

原则13：银行应该拥有有效的能力、业务连续性和应急计划程序，以确保电子银行系统和服务的连续可用性。确保体系的正常运转也取决于应急支持系统缓释***拒绝服务的攻击***（或其他可能造成业务中断的事件）的能力。

香港金融管理局
HKMA

Independent Assessment of Security Aspects of Transactional E-banking Services

2.2.14 ....plans and procedures for dealing with interruptions caused by attacks such as ***Denial of Services (DoS) and Distributed Denial of Services (DDoS)***;

新加坡金融管理局 MAS

INTERNET BANKING AND TECHNOLOGY RISK MANAGEMENT GUIDELINES

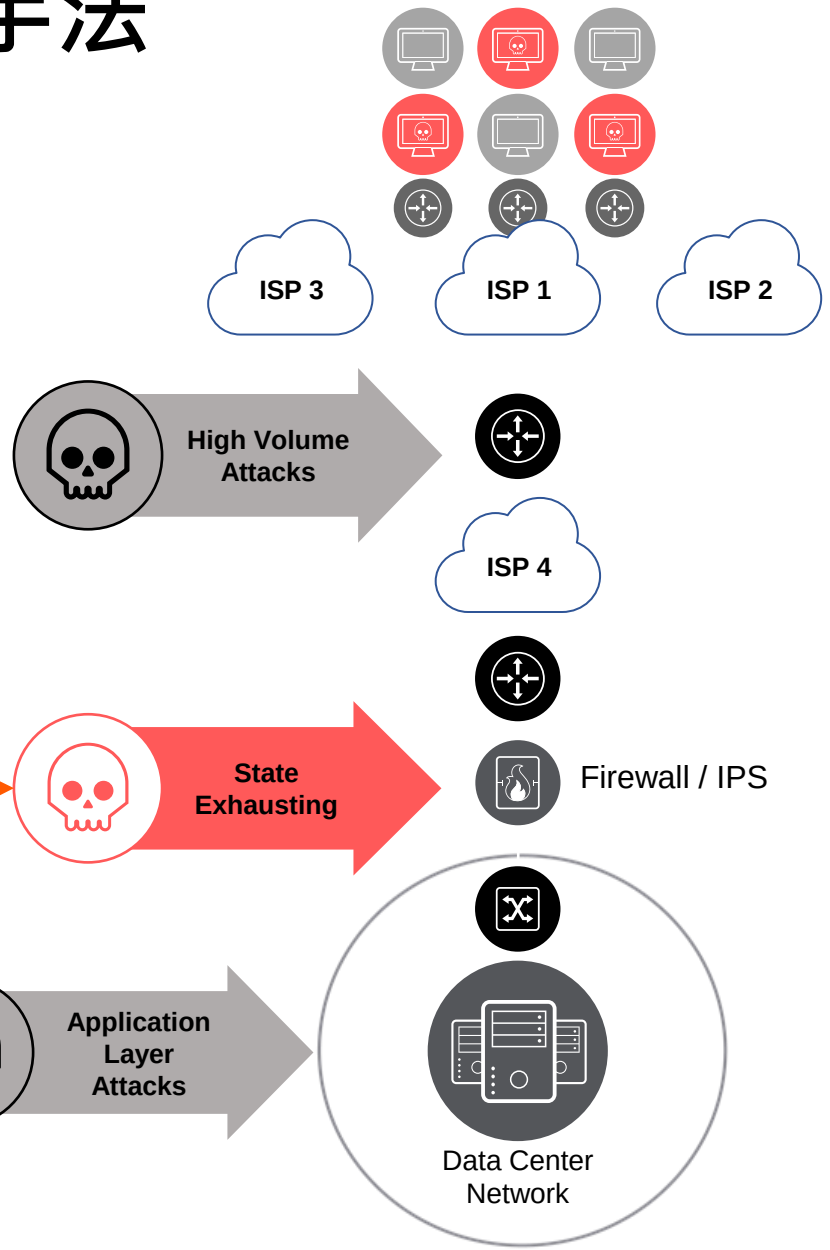
9.0 **DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS) 專章**

Agenda

市場概況

常見DDoS防禦手法

1. **建置IPS / Firewall / DDoS防禦設備**
2. CDN
3. 加大使用上網頻寬
4. 加強主機的效能



Firewalls and IPS

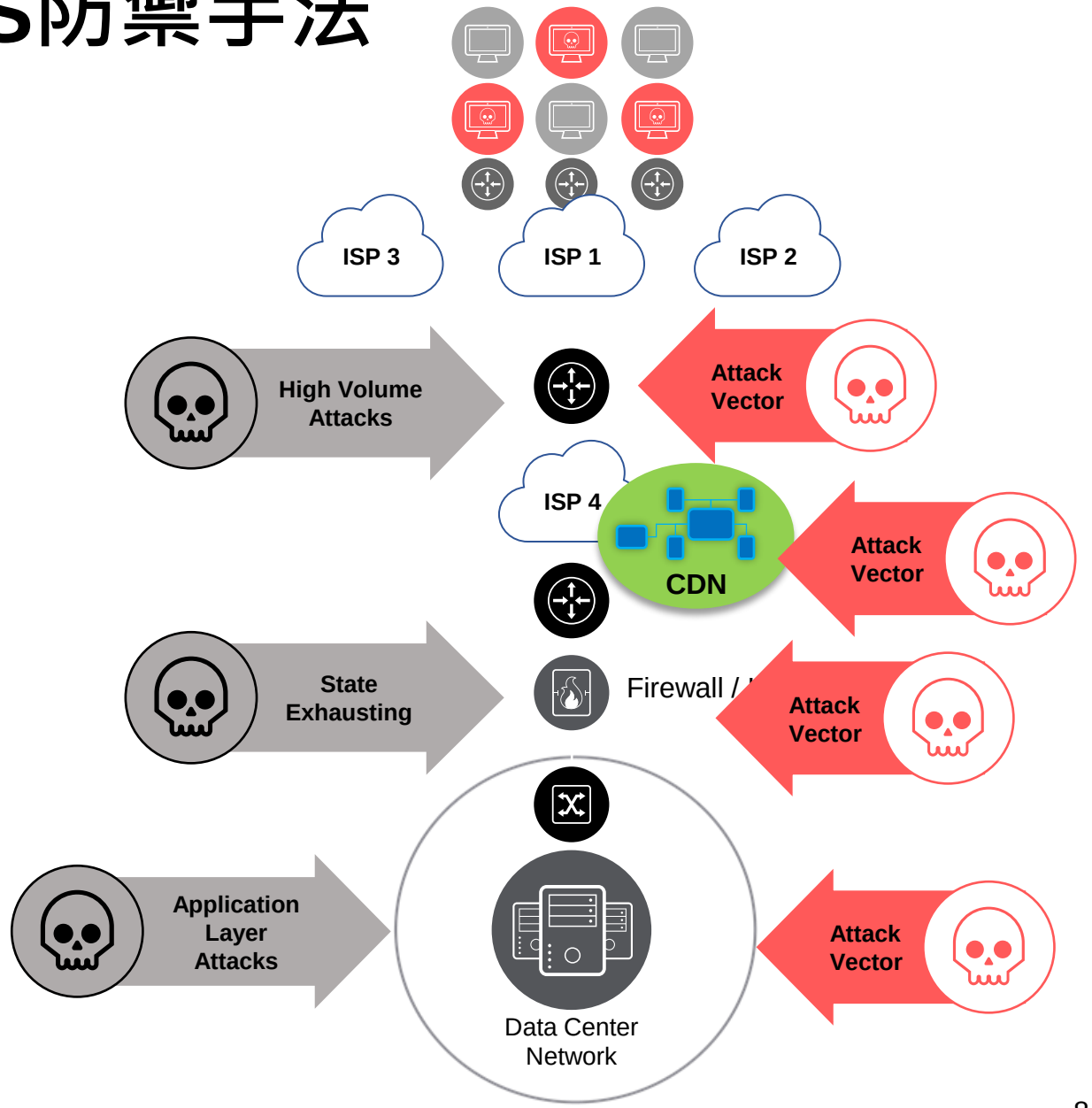
- 這些有狀態表(Stateful)設備, 容易被駭客利用狀態耗盡攻擊, 自身難保 !!!
- 非專業DDoS保護設備, 容易造成誤擋

常見DDoS防禦手法

1. 建置IPS / Firewall / DDoS防禦設備
2. **CDN**
3. 加大使用上網頻寬
4. 加強主機的效能

CDN

- 不能阻擋非網頁型態的攻擊行為(only for 80/443 port)
- 駭客針對實體IP進行攻擊無法攔截
- 無法阻擋狀態耗盡攻擊, 特別是動態網頁型態的客戶
- 受限金融法規規範, 對金融交易所需加解密無法支援



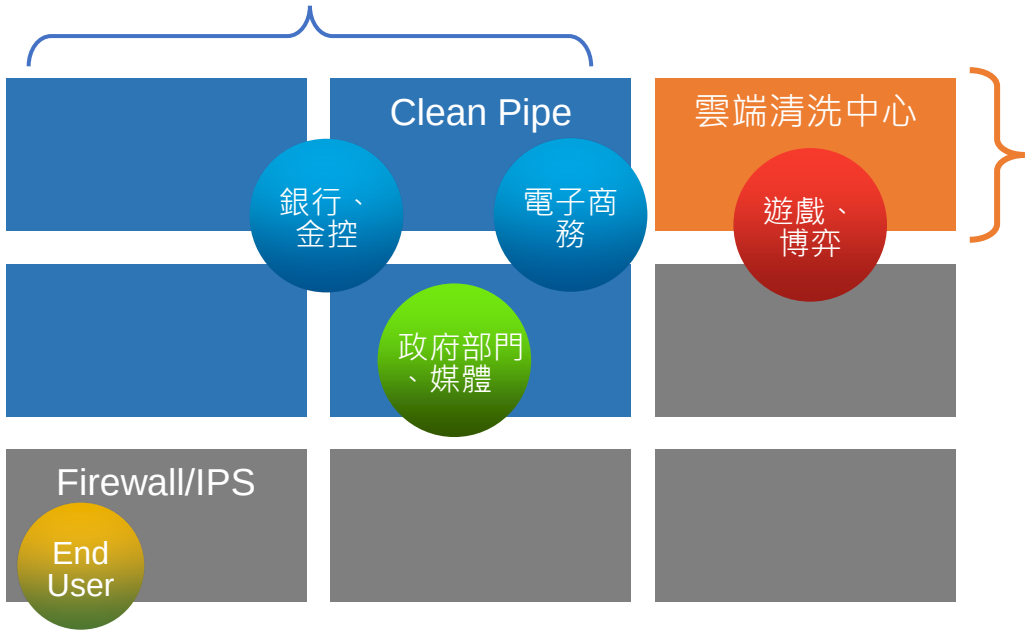
常見DDoS防禦手法

Clean Pipe DDoS Solutions

中華電信 | 果核數位 Digicentre | Level(3) COMMUNICATIONS | PCCW | KDDI | StarHub | TELSTRA | AT&T | TATA

- ✓ ISP/IDC/Hosting業者
- ✓ 建構於骨幹之清洗服務，清洗量1~30G

註1：遠傳以代銷INCAPSULA 為主。



Cloud-based DDoS Solutions

ARBOR NETWORKS | NEXUSGUARD | IMPERVA INCAPSULA | f5 | radware | Akamai

- ✓ Global業者、設備業者、CDN業者
- ✓ 網路規模及清洗能力>1T

Agenda

服務介紹

如何有效防禦DDoS攻擊

多層次DDoS防禦架構，全面協助客戶抵禦各種型態攻擊!

乾淨流量

第二層有如淨水器
L7
針對L7資源耗盡及應用層攻擊進行清洗防禦
確保正常流量抵達應用服務伺服器

第一層有如淨水廠
L3 ~ L4
針對L3~L4大流量阻斷攻擊進行清洗防禦
避免頻寬塞爆中斷營運

包含了L3~L7各式流量、資源耗盡及應用層攻擊

自動監控/客製化告警報表系統

台灣大哥大 DDoS 防禦服務大管家

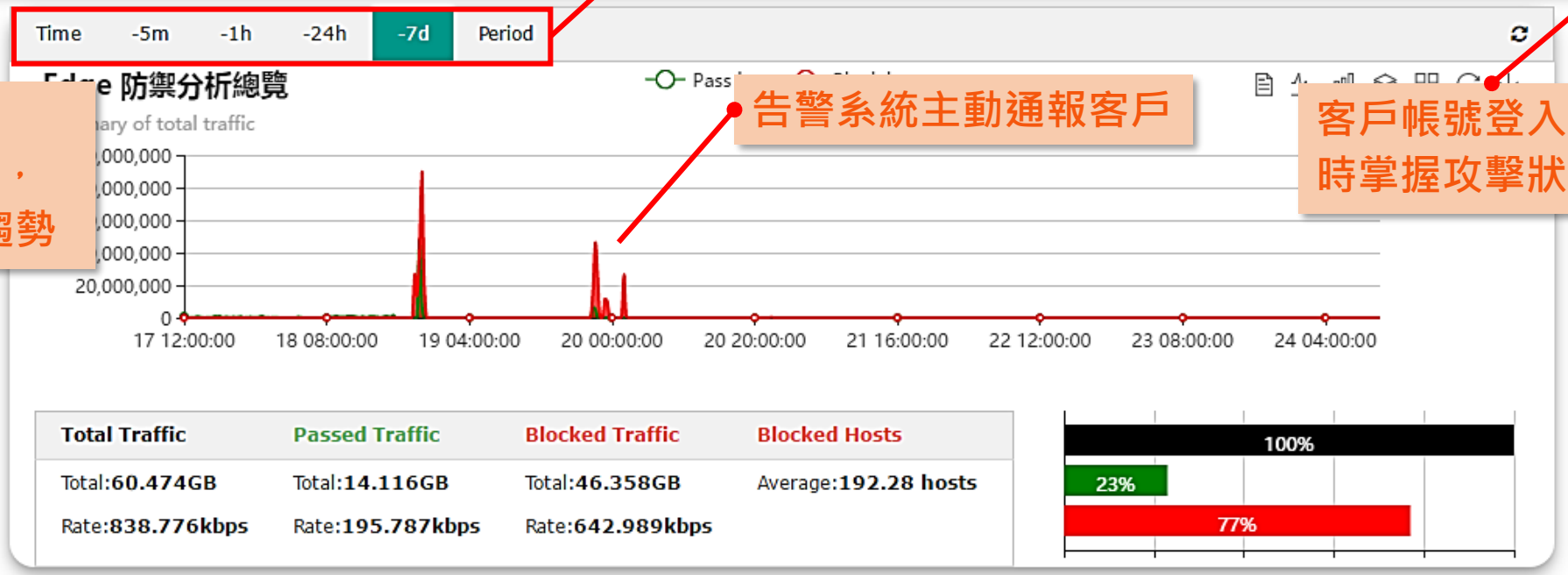
24小時自動即時監控

服務總覽 | 流量分析 | 事件分析 | 報表總管 | 管理設定

客戶自訂報表
email至客戶端，
即時掌握攻擊趨勢

告警系統主動通報客戶

客戶帳號登入，隨
時掌握攻擊狀態



防禦網站
1.服務總覽
2.報表查詢:
  防禦分析總覽
  保護PG內容
  攻擊型態分析
  IP來源分析
  國別分析
3.事件分析
4.報表總管
  報表設定,發送
5.管理設定

All Protection Groups

Protection Group Name	Passed Traffic (Max)	Blocked Traffic (Max)	Prefixes	Server Type
Default Protection Group	194.33mbps (1.444mbps) 20.771kpps (155.0pps)	21.0bps (1.0bps) 0.0pps (0.0pps)	[0.0.0.0/0]	Generic Server
Web	126.689kbps (1.413kbps) 165.0pps (2.0pps)	119.0bps (9.0bps) 0.0pps (0.0pps)	[192.168.1.9/32]	Web

多層次防禦服務優勢

- **兩段式清洗架構**
  骨幹端及用戶接取端各有專責的清洗設備.可將不同型態的攻擊封包清洗乾淨.
  可針對L3 ~ L7 的攻擊,完全阻隔
  7 x 24 always on 清洗服務(採In Line Mode)

- **電信骨幹佈建及管理**
  清洗設備廣佈於台灣大哥大骨幹網路上.可針對不同客戶需求提供立即服務
  7x24 網管中心監測網路封包.隨時啟動應變機制.

- **提供Portal網站**
  客戶可以隨時進入多層次DDoS防禦服務入口網站,得知所有的攻擊行為,攻擊來源IP,攻擊來源國家,攻擊量等完整報表

Agenda

總結

台灣大哥大服務特色與優勢

電信級多層次DDoS防禦服務全面抵禦**L3~L7**攻擊

安全

7x24 Always On+自動即時監控、通報、客製化告警報表系統，**即時掌握攻擊狀況**

效率

電信骨幹佈建及管理，客戶端不需投資設備及改變既有網路架構，**快速無痛導入**

彈性

攜手國際領導大廠Arbor Network，打造**電信等級最嚴密**DDoS防禦服務

信任

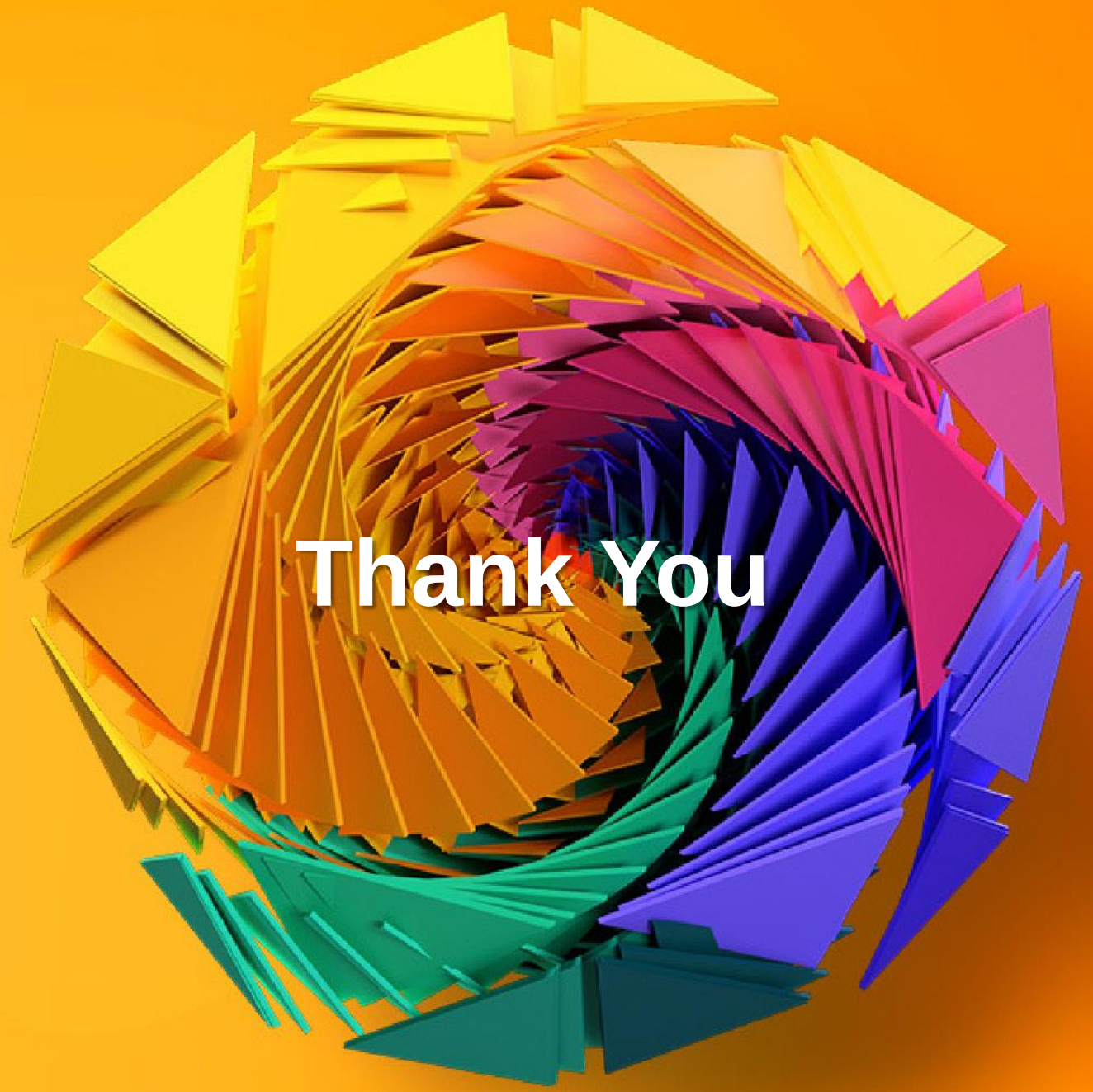
免責條款

基於網路安全防禦無法保證100%之防禦率：

- 甲方以既有之規劃及現有技術提供，不擔保所提供之服務將符合乙方的所有需求，且不擔保本服務可發現所有網路入侵、攻擊、病毒、網頁程式及網站之弱點、隱藏於網頁中之惡意程式或木馬程式，也並不擔保百分百有效阻絕並清除之。

- 甲方無法就乙方擷取資訊之正確性、完整性、安全性、可靠性、合適性、不會斷線及出錯負責，亦不保證乙方與甲方間資料傳輸速率，倘乙方因傳輸速率、擷取使用網路資料、安裝或使用本服務導致直接或間接之損害或損失時，甲方不負任何損害賠償責任。

台灣大哥大
企業服務



Thank You