HKMA Guidance on Anti-DDoS Protection

KPMG China

February 2023

Background

On 25 November 2022, The Hong Kong Monetary Authority (HKMA) issued an additional guidance to authorised institutions (AIs) on protection against distributed denial-of-service (DDoS) attacks ***"Guidance on anti-DDoS protection"***. In consideration of the growing incidence and sophistication of DDoS attacks, the HKMA provides more detailed guidance to complement the relevant requirements stated in "TM-E-1 Risk Management of E-banking" and "TM-G-1 General Principles for Technology Risk Management" Supervisory Policy Manual (SPM).

The HKMA developed the additional guidance based on the findings from the thematic reviews completed to assess the effectiveness of the anti-DDoS protective measures maintained by AIs. The additional guidance is grouped and summarised into four key principles as discussed below.

Summary of Guidance on Anti-DDoS Protection

Key Guidance Principles covered in the HKMA guidance

Regular Risk Assessment and Vulnerability Management

- Establish a robust mechanism to regularly identify, assess and mitigate vulnerabilities in networks and systems which may be at risk to emerging DDoS attacks.
- Critically assess whether AIs' anti-DDoS defense mechanism remains adequate, including in terms of mitigation capacity, and activation and mitigation time.

Anti-DDoS Controls Architecture

- Properly configure and regularly review the architecture of AIs' anti-DDoS controls.
- Ensure Anti-DDoS controls cover both customer-facing channels (e.g. E-banking) and key components supporting AI's operations (e.g. VPN, email service).
- Deploy multi-layered defense in AI's network architecture to achieve optimal anti-DDoS protection (e.g. combine cloud-based protection, ISP protection and on-premises defence).

Service Providers Governance

- Regularly evaluate the cyber defense capability of AIs' key third parties which are critical to the availability of internet-facing services and are potential DDoS attacks targets.
- Develop contingency arrangements for potential disruption to the services of the key third parties, and implement controls to minimise the risk of single point of failure.
- Perform due diligence and formulate written key performance indicators with anti-DDoS service providers.

Incident Response and Regular Drills

- Establish end-to-end incident response procedures including actions required from anti-DDoS service providers.
- Incorporate lessons learned from significant DDoS incidents occurred locally and internationally into AIs' incident response and escalation procedures.
- Perform technical drills (with appropriate involvement of anti-DDoS service providers) to validate the effectiveness of the anti-DDoS protective measures.

According to our understanding of HKMA's expectations and based on our experience obtained from DDoS assessments performed for our clients, enterprises should ask the below questions to assess their readiness:

- *Does your risk assessment cover **adequacy** and **effectiveness** of anti-DDoS protection measures?*
- *Can anti-DDoS controls mitigate DDoS attacks on **remote access** and **email** service?*
- *Do you set clear key performance indicators and regularly evaluate the **anti-DDoS capability** of ISPs, SaaS/Cloud and DNS service providers?*
- *Do your regular DDoS drill exercises include **table-top** or **technical** drills that involve simulation of DDoS traffic?*

Areas AIs Should Consider with regards to Anti-DDoS Protection

Anti-DDoS Protection Measures

In our view, the HKMA expects that AIs should be able to:

- Assess the adequacy and effectiveness of existing anti-DDoS control measures
- Be able to enhance DDoS mitigation measures based on threat intelligence of emerging DDoS attacks
- Design anti-DDoS control architecture properly to ensure sufficient DDoS protection coverage
- Conduct technical DDoS simulation drills to validate the effectiveness of anti-DDoS protective measures

Key expectations from HKMA on enhancing anti-DDoS measures

Governance and Compliance Controls

Regular Review of Anti-DDoS Solution Configuration

- Enforce anti-DDoS measures effectively
- Fulfil service level agreement
- Meet the Bank's DDoS mitigation requirement

DDoS Incident Response Procedure

- DDoS attack severity classification
- Impact assessment
- Incident escalation channel
- Remediation timeframe requirement
- Internal and external coordination and notification procedure (with Call Tree)

DDoS Threat Intelligence Lifecycle

- Subscribe threat intelligence sources on emerging DDoS attacks
- Collect DDoS attacks information from industry peers, government and external parties
- Analyse threat intelligence and enhance DDoS mitigation measures

Validation of Anti-DDoS Controls Architecture, Coverage and Effectiveness

Capability to Mitigate Different DDoS Attack Types (Examples)

- TCP Connection Flood
- DNS Query Flood
- HTTP/HTTPS GET Flood
- SYN Flood
- Slow Loris
- Out of State TCP attacks
- DNS/NTP Reflection
- Browser Automation Based Attacks
- Targeting Application Layer Attack (Layer 7)
- CDN Bypass Attack
- Teardrop Attack

Multi-layered Defense Architecture

- Cloud-based DDoS protection service subscription
- ISP level DDoS protection
- On-premises protection (e.g. Firewalls, IPS, WAF)

DDoS Protection Coverage

- Internet facing channels (e.g. internet banking)
- Corporate website
- Remote access service
- Corporate email
- Disaster recovery environment
- DNS servers

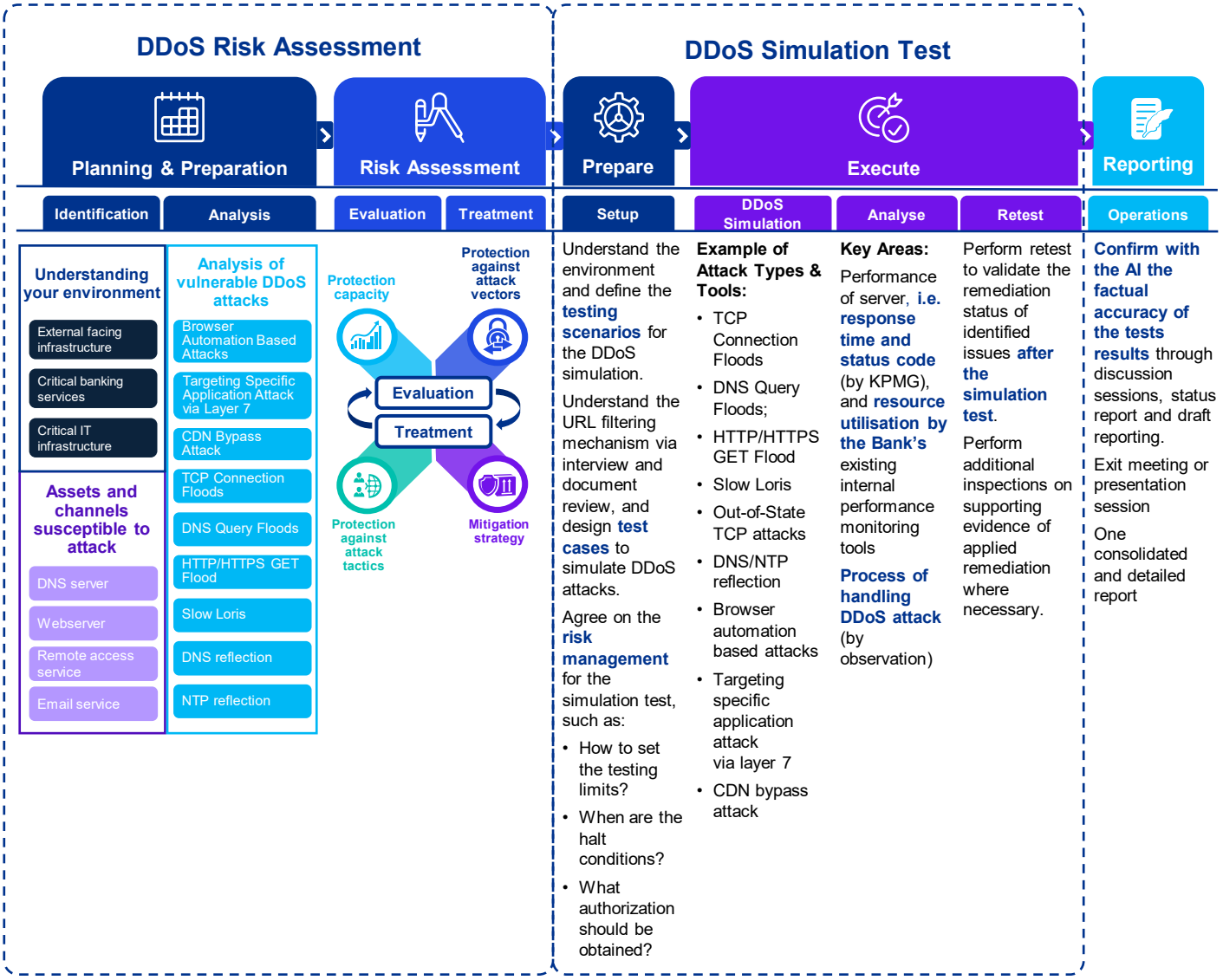
Technical DDoS Simulation Drill

- Simulate intensive magnitude of DDoS traffics
- Trigger automatic DDoS mitigation
- Include mitigation of different DDoS attack scenarios (e.g. Volumetric, Protocol and Application layer attacks)
- Test out communication strategy
  - Internal communication
  - Escalation to management
  - Communication with customer
  - Line to take (e.g. press release)
- Verify activation and effectiveness of DDoS defense

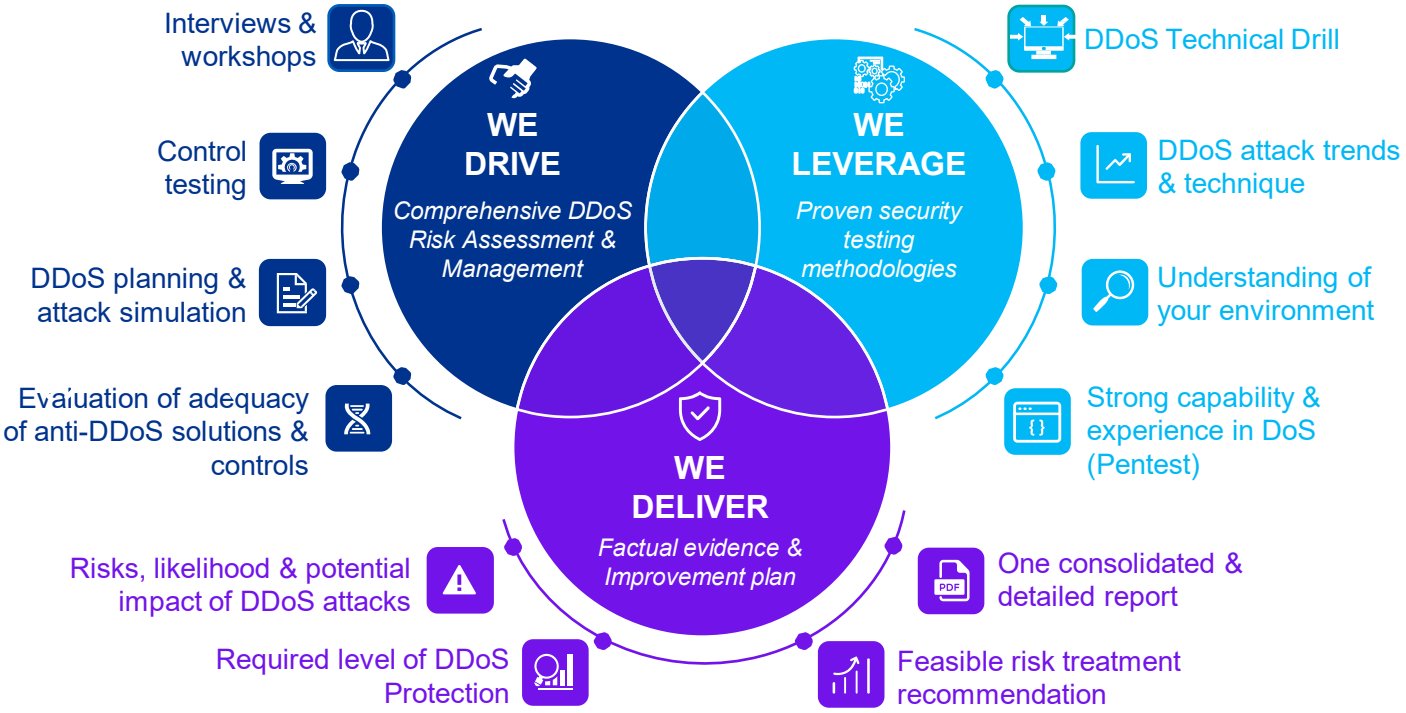
Our Approaches To Fulfill Anti-DDoS Protection Guidance

To fulfill HKMA guidance requirements, a combination of DDoS Risk Assessment and DDoS Simulation Testing should be conducted to meet HKMA expectations and identify potential issues on the Bank's anti-DDoS control measures. We recommend AIs to first conduct a DDoS Risk Assessment to identify critical control gaps, followed by further DDoS Simulation Testing to validate the effectiveness of the anti-DDoS protective measures.

Our 5-Phase Approach on DDoS Security Assessment



Our Holistic DDoS Security Assessment Framework



Contact us

Henry Shek
Partner, Management Consulting
T: +852 2143-8799
E: henry.shek@kpmg.com

Brian Cheung
Partner, Management Consulting
T: +852 2847-5026
E: brian.cheung@kpmg.com

Lanis Lam
Partner, Management Consulting
T: +852 2143-8803
E: lanis.lam@kpmg.com

Tony Yu
Associate Director, Management Consulting
T: +852 3927-5929
E: ty.yu@kpmg.com

Kenson Cheung
Manager, Management Consulting
T: +852 2847-5068
E: kenson.cheung@kpmg.com

Gordon Chen
Manager, Management Consulting
T: +852 2847-5091
E: gordon.j.chen@kpmg.com

kpmg.com/cn/socialmedia