Distributed Denial-of-Service (DDoS) Mitigation Advisory

Version 1.0

Released Aug 8, 2024

Table of Contents

Distributed Denial-of-Service (DDoS) Mitigation Advisory

Background

The Cyber Security Agency of Singapore (CSA) is releasing this set of best practices to provide guidance to organisations on how to identify, contain and mitigate Distributed Denial-of-Service (DDoS) attacks whilst minimising impact to business operations.

This advisory is built with reference to the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework (CSF) 2.0, structured around the GIPDRR (Govern, Identify, Protect, Detect, Respond and Recover) functions. It applies an in-depth approach with a detailed set of best practices for mitigating a DDoS attack at each function. The advisory also includes a People, Process and Technology (PPT) framing of each best practice which can be viewed at Appendix B. As different organisations may have different deployment models (on-premises/cloud/hybrid) that require tailored countermeasures, organisations should further contextualise and adapt the practices to their operating environments to ensure that their business needs are balanced with their security requirements.

Audience

The audience, effectively the key stakeholders of organisation's IT assets, for this publication includes but is not limited to:

1. System owners who are responsible for the design and maintenance of systems, who can leverage this advisory to incorporate system resiliency against DDoS attacks into their systems.
2. Policy owners who are responsible for developing and enforcing policies related to system resiliency, who can leverage this advisory to integrate system resiliency into their policies and processes.
3. Incident Response (IR) teams in charge of responding to and recovering from incidents such as DDoS attacks, who can leverage this advisory to improve response coordination and recovery time.
4. Operational team involved in the everyday operations and maintenance of systems (e.g., network engineers, system administrators) and are responsible for the development, implementation, and management of software-based, hardware-based, or service-based, security controls, who can leverage this advisory to ensure that such controls promote a resilient- and secure-by-design system.
5. Third-party service providers that offer protection services against DDoS attacks, who can reference this advisory to understand the scope of their responsibilities to the organisation during normal operations as well as when under DDoS attack.

Disclaimer

This advisory provides guidelines and best practices on how to mitigate and respond to possible DDoS incidents. The best practices provided are not exhaustive and do not constitute to endorsement by CSA or imply compliance to policies and regulations published by CSA. Organisations shall be solely responsible for the selection, use, and suitability of the information and assume any liability resulting from such use. Always consult a trained cybersecurity professional for advice before making any business-critical decisions within your organisation. Risk assessment may be one of the bases for the selection of mitigations within your organisation.

Acknowledgements

The development of this document has benefited significantly from the inputs and support provided by the following agencies and organisations, as well as the resources listed under References.

Defence Science and Technology Agency (DSTA)

Government Technology Agency (GovTech)

Singtel

Cloudflare

What is Denial-of-Service (DoS)?

A Denial-of-Service (DoS) attack refers to a malicious attempt by cybercriminals to render computer services or resources unavailable to the intended user(s). A successful DoS attack significantly exhausts available network or system resources to a point that it introduces latency or disruption, either by overwhelming the target or its surrounding infrastructure with fraudulent traffic that may appear legitimate, or by exploiting a vulnerability in the systems, protocols, or application architecture.

DoS attacks commonly fall under one of the following 3 categories:

1. **Exhaustion** of network resources targets the available **network bandwidth** of the victim. This can be done by congesting the network capacity with illegitimate requests such that legitimate traffic cannot be transmitted. This may happen through a direct flood of traffic or a reflection / amplification attack, which exploits an intermediary (e.g., open DNS resolvers) to deliver network traffic to the victim. A response, often larger than the request, is reflected to the victim from the attacker's request through spoofed Internet Protocol (IP) addresses.
2. Resource exhaustion by **exploiting specific weaknesses in network communication protocols** to disrupt and overwhelm the intermediary devices and system components handling incoming requests. This is regularly seen in common stateful protocols such as TCP.
3. **Resource exhaustion** of application targets the victim's **application services**, in particular, exploiting specific **weaknesses in the application functions**, affecting the available compute or storage resources of the application.

When multiple computer systems (or botnets - made up of networks of compromised devices) are used to mount a DoS attack, this is referred to as a **Distributed Denial-of-Service (DDoS)** attack. DDoS attacks are particularly destructive as a well-timed attack during peak hours or an attack against time-sensitive services could have substantial impact on business operations, including but not limited to degradation of critical services, severe remediation costs, operational toil on application and network administrators combatting the attacks, and significant reputational damage.

Evolution of DDoS Attacks

DDoS attacks emerged in the late 1990s with the growth of the internet and online services. Threat actors initially relied on simple methods such as Internet Control Message Protocol (ICMP) floods to conduct DDoS attacks, involving sending a large number of 'ping' requests to overwhelm a target's network. Since then, however, DDoS attacks have since evolved in sophistication and complexity, and no longer rely solely on floods of requests or data to disrupt networks. Modern attacks often involving a combination of different techniques, blending volumetric, application layer, and reflective methods. Refer to Appendix A for the common types of DDoS attacks.

The evolution of DDoS attacks can be broadly summarised as follow:

- Early days (1990s)
  - DDoS attacks emerged in the late 1990s with the growth of the internet.
  - Threat actors initially relied on simple methods such as ICMP flood attacks, where a large number of ping requests were sent to overwhelm a target's network.
- Volumetric attacks (2000s)
  - In the 2000s, threat actors began to use botnets, comprising networks of compromised computers, to amplify the scale of their DDoS attacks.

    - Threat actors employed User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) flood attacks, overwhelming network bandwidth and server resources.
- Application layer attacks (mid-2000s)
    - As defensive measures against volumetric attacks improved, threat actors shifted their focus to the application layer.
    - Application layer attacks, such as Hypertext Transfer Protocol (HTTP) floods, target specific applications or services, overwhelming them with seemingly legitimate requests.
- Reflection and Amplification Attacks (2010s)
    - Threat actors started utilising reflection and amplification techniques, exploiting vulnerabilities in internet protocols to amplify their attack traffic.
    - Domain Name System (DNS) and Network Time Protocol (NTP) amplification attacks became prevalent, allowing threat actors to generate large-scale traffic with relatively small resources.
- IoT-based Attacks (late 2010s)
    - The rise of the Internet of Things (IoT) introduced a new vector for DDoS attacks. Insecure IoT devices were harnessed into botnets for large-scale attacks.
    - In 2016, the Mirai botnet gained significant attention for exploiting weak security in IoT devices to launch large-scale DDoS attacks.
- Sophistication and Complexity (present)
    - Modern DDoS attacks often involve a combination of different techniques, blending volumetric, application layer, and reflective methods.
    - Threat actors increasingly use encrypted traffic to make detection and mitigation more challenging.
    - Increasing use of random prefix / “DNS water torture” attacks which overwhelm DNS servers by sending numerous domain queries (often to non-existent sub-domains), causing service degradation and resource exhaustion. Such attacks often do not require high bandwidth, unlike traditional volumetric DDoS attacks.
    - UDP floods continue to dominate, constituting 62% of DDoS attacks.[1]
    - DDoS-for-hire services have made it easier for even non-technical threat actors to launch attacks, contributing to the overall growth in the frequency of DDoS incidents.

Contemporary DDoS Attack Volumes

Cybersecurity vendors have highlighted significant year-on-year increases in DDoS peak attack volume, at times doubling, with attacks varying in duration vastly from three minutes to nine hours:

- *Volumetric (bits per second)*: Tech firm Gcore stated in its latest ‘Gcore Radar Report’ that DDoS peak attack volume had spiked from 300 Gbps in 2021, to 650 Gbps in 2022, and exponentially to 1,600 Gbps in 2023. Internet service provider and tech firm Verizon also stated in its ‘2023 Data Breach Investigations Report’ that majority of DDoS attacks saw their volumes grow about 25%, from 99 Gbps to 124 Gbps.

- *Protocol based (typically network and application layers) attacks* (measured in packets per second (pps), requests per second, among others): Cloudflare stated in its ‘DDoS Attack Trends for 2023 Q4’ that it observed a 117% year-on-year increase in network-layer DDoS attacks, as compared to 79% in 2022 Q4. In 2023 Q4, two out of every 100 network-layer DDoS attacks exceeded 1 Gbps,

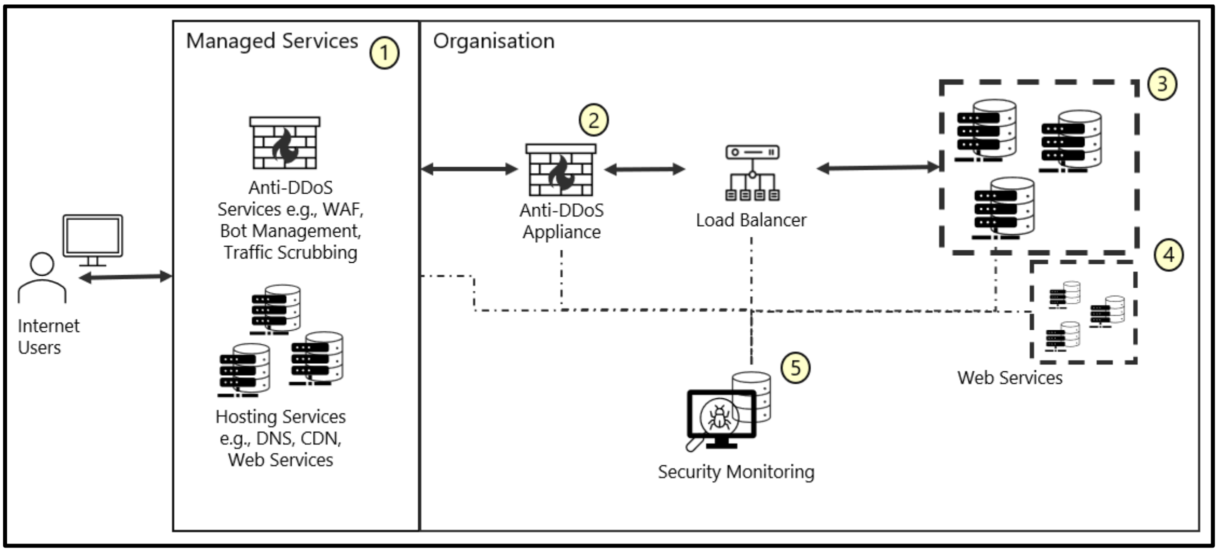
[1] https://smebusinessnews.co.uk/2024/01/24/gcore-radar-report-reveals-ddos-peak-attack-volumes-doubled-in-h2-of-2023/

whereas one out of every 100 attacks exceeded 1 million pps, and the amount of network-layer DDoS attacks exceeding 100 million pps increased by 15% (as compared to Q3).

- Protocol-based attacks often aim to exhaust the resources of targeted applications and systems, rendering them incapable of handling legitimate requests. These attacks need not be volumetric and are insidious as they require fewer resources from the attacker. A small number of machines or even a single machine itself can initiate such attacks, making them a favoured tactic among attackers. For example, Cloudflare reported in its 2022 Q2 report that most network-layer DDoS attacks remained below 50,000 pps, which was enough to disrupt poorly secured networks.

Given the varying visibility over DDoS peak attack volume across cybersecurity vendors, there is hence no universal threshold for what is considered a high-volume attack, especially for protocol-based DDoS attacks. Volumetric attacks can vary depending on the industry, the specific online services offered by the target, and the overall capacity and resilience of the target's network infrastructure. As such, organisations need to employ strategies and services to detect and mitigate DDoS attacks, regardless of their volume to ensure the availability and reliability of their systems and services.

DDoS Mitigation Conceptual Diagram



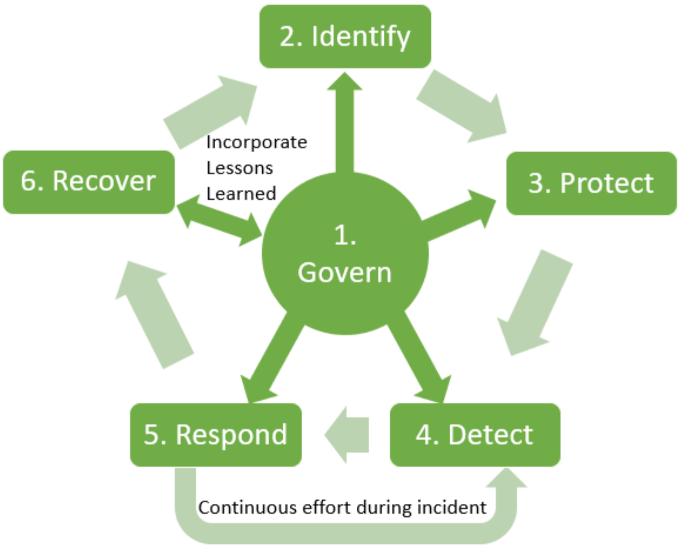
The conceptual diagram above illustrates how an organisation may defend against DDoS attacks through a **layered defence strategy** that involves **filtering malicious DDoS traffic** and **absorbing DDoS attempts** at multiple points across service providers' as well as within the organisation's infrastructure.

As an illustrative example, this strategy is applicable across on-premises, Cloud, and hybrid environments. The following key recommendations are reflected within the diagram:

1. Mitigate and absorb DDoS attacks by subscribing to **managed DDoS protection services and hosting services**.
2. For traffic entering an organisation's network, mitigate DDoS attempts targeting network and application vulnerabilities with **security appliances deployed on-premises**. This offers an additional layer of protection should DDoS attacks happen to evade subscribed DDoS protection services.
3. Absorb DDoS traffic by catering for **application resources to scale** on top of **load balancing** to distribute requests.
4. For DoS attacks that bypass earlier defence layers, limit the impact of DDoS attacks by **segmenting application resources** to contain failure within the targeted services.
5. Respond in a timely manner by **monitoring for signs of DDoS attacks** on organisation's assets, as well as through **alerts from subscribed services**. Relying on multiple alert sources increases the chances for organisations to pre-emptively counter DDoS attacks with appropriate mitigating measures.

These recommendations should be complemented by the organisation's processes for identifying and responding to DDoS attacks, such as through regular reviews of their appliance and service configurations, as well as having a robust DDoS incident response plan to support remediation and recovery activities.

How to use the Advisory


2. Identify
3. Protect
4. Detect
5. Respond
6. Recover
1. Govern
Incorporate Lessons Learned
Continuous effort during incident

The subsequent sections will share best practices that organisations may wish to consider when building their CONOPS and strategies for DDoS Mitigation. These best practices are grouped under the functions of NIST's CSF 2.0, as follows:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

The best practices with GIPDRR framing are intended as a *cyclical* and *iterative* process. Each function builds upon the foundations laid by the previous functions – and organisations are encouraged not only to progress through the functions, but also to consistently revisit prior functions. This will enable controls and practices to be adjusted to address current and emerging threats as well as adapt to changes in the operating environment.

Organisations should note that GOVERN function is the primary function that sets the foundation for all other functions (IPDRR), and directly contributes to the success and efficacy of actions taken under those functions.

Additionally, as part of incident response efforts, organisations should cycle between the DETECT and RESPOND stages – vigilant monitoring will enable detection of threats (e.g. intrusion attempts, escalation of DDoS traffic) and trigger the appropriate response to the threats such as rerouting incoming traffic. Subsequently, actions taken for response should reinforce further detection efforts if the actions have successfully deterred the attack or require further response actions.

By taking this approach, organisations can build a robust DDoS mitigation strategy where controls evolve to effectively address changing DDoS threats and operational requirements.

Best Practices for Mitigating DDoS

1 Govern

Governance refers to the establishment, communication and enforcement of policies, procedures, and controls to effectively manage and mitigate cybersecurity risks in line with the organisation's risk appetite, priorities, and constraints. An organisation's cybersecurity strategy manifests in its organisational policies, which delineate the various risk management activities that key stakeholders are responsible for. Governance also extends to visibility and oversight of various risk response activities, enabling management to govern the incident response plan as it unfolds during cybersecurity incidents.

This section recommends the organisational policies and DDoS incident response plan content that should be in place fulfil the objectives of the Govern function.

1.1 Establish Organisational Policies

The foundation of an organisation's security is built from **organisational policies**, which set the scope of security for the organisation by outlining the security goals and practices as well as defining roles and responsibilities of various stakeholders for smooth execution of their risk management activities during times of need. The following is a non-exhaustive list of policies which are essential for managing information technology (IT) setup in an organisation.

1.1.1 Develop, communicate, and enforce an **IT asset management policy**, covering the roles and responsibilities of key stakeholders and processes for identifying, categorising, maintaining, modifying, and disposing of assets throughout the asset lifecycle. This should account for both on-premises, off-site and cloud assets.

1.1.2 Develop, communicate, and enforce a **change management policy**, covering the roles and responsibilities of key stakeholders and processes for identifying, approving, acquiring, testing, and deploying system, service or environment changes relating to information security.

1.1.3 Develop, communicate, and enforce a **configuration management policy**, covering the roles and responsibilities of key stakeholders and processes for documenting configuration of systems and software, establishing baselines as well as detecting, addressing and documenting deviations from the baseline.

1.1.4 Develop, communicate, and enforce a **patch management policy**, covering the roles and responsibilities of key stakeholders and processes for identifying, approving, acquiring, testing, and deploying updates to systems and services.

1.1.5 Develop, communicate, and enforce a **vulnerability management policy**, covering the roles and responsibilities of key stakeholders and processes for identifying, documenting, evaluating and mitigating risks associated with vulnerabilities in systems and services.

1.1.6 Develop, communicate, and enforce a **network security policy**, covering the roles and responsibilities of key stakeholders and processes for identifying, testing, and deploying network security controls.

1.1.7 Develop, communicate, and enforce an **access control policy**, covering the roles and responsibilities of key stakeholders and processes for managing, granting, reviewing, and revoking user access, defining access levels, and adhering to the elements of identification, authentication, authorisation, and accountability (IAAA).

1.1.8 Develop, communicate, and enforce an **audit logging and monitoring policy**, covering the roles and responsibilities of key stakeholders and processes for collection, analysis, and storage of activity data. This should account for both on-premises, off-site and cloud assets.

1.1.9 Develop, communicate, and enforce a **business continuity plan**, covering the roles and responsibilities of key stakeholders and processes for ensuring that the organisation's operations can continue during and after disruption from an incident. This should include strategies for risk assessment, identifying critical functions and assets, backup & recovery procedures, and communication plans during and post-incident. For business continuity aspects specific to DDoS attacks, please refer to section 1.2, *Establish a DDoS Incident Response Plan* for more details.

1.1.10 Develop, communicate, and enforce a **security awareness and training policy**, covering the roles and responsibilities of key stakeholders and processes for educating employees on security best practices and promoting a security-aware organisational culture.

1.2 Establish a DDoS Incident Response plan

Having established procedures that the organisation and involved parties are familiar with will help facilitate smooth execution for a more effective response.

1.2.1 **Develop a robust organisation DDoS incident response plan** for identifying, mitigating, and rapidly recovering from DDoS attacks. This may include classifying incidents by severity with corresponding response measures (e.g., geo-blocking, request rate limiting) to balance between maintaining business operations and denying DDoS attack traffic. The incident's severity should also inform the level of notification required, i.e., who needs to be informed and how frequently.

1.2.2 Ensure that **all stakeholders** including leaders, operational and application teams, extended IR teams (legal counsel, HR, public relations etc.) and service providers **understand their roles and responsibilities** at every stage in response to a DDoS attack.

1.2.3 Clearly document **incident reporting and escalation procedures**, inclusive of defining triggers for escalation, defining escalation paths for who needs to be informed at each stage of the incident, and clarifying the decision-making authority at each level of escalation.

1.2.4 For internal communications, establish **communication protocols** for the appropriate level of **notification** as required by the incident's severity, inclusive of upward reporting from frontline staff to senior leadership for visibility and downward reporting of directives or strategic information.

1.2.5 For external communications, ensure established **communication protocols** and Point-of-Contacts with Managed Service Providers are documented and reviewed periodically to ensure timely activation of DDoS services when required.

1.2.6 For any communications, plan for **alternate communication protocols** in case of a situation where the established communication mechanism is ineffective or unavailable.

1.2.7 Ensure that any **backup mechanisms** used for system and service recovery are regularly maintained and tested for reliability and integrity.

2 Identify

2.1 Identify Critical Assets and Services

Having a clear and updated overview of the organisation's attack surface from Internet-exposed assets and services sets a strong foundation for subsequent measures to address DDoS attempts.

2.1.1 Identify **critical assets and services** of the organisation that are exposed to public internet, such as through scanning with analysis tools, and generate a **Bill of Materials (BOM).**

2.1.2 **Prioritise** assets and services based on their criticality.

2.1.3 Identify the **network access path** to each critical assets and services from public internet.

2.1.4 Identify potential **network/application chokepoints** to each critical assets and services both within and external to the organisation's network (i.e., from public internet).

2.1.5 Establish a **baseline of typical and peak network activity and traffic patterns** of the organisation's critical assets and services from public access on normal days and days coinciding with activities that might increase the traffic e.g., promotion events such as the redemption of vouchers.

2.1.6 Determine the **appropriate thresholds to activate DDoS mitigation services and measures.** These should be set with an appropriate buffer below the maximum operating specifications of the organisation's network appliances while accounting for the estimated network activity established in 2.1.5.

2.1.7 Ensure that the organisation's **network design** is capable of handling network traffic spikes to mitigate resource exhaustion. This includes **adequate sizing of network appliances** with sufficient throughput, considering **network redundancy** for inbound and outbound network traffic, **load balancing** and **traffic shaping** for critical assets.

i) As a starting point, organisations may want to consider accounting for 1.5x – 3x of the peak traffic baseline established in 2.1.5 when designing for their maximum traffic capacity, and scale accordingly (in line with their resources).

3 Protect

3.1 Design for Resiliency

A resilient infrastructure aims to withstand and contain the impact of DDoS attacks through **DDoS security appliances** and catering for **redundancy** at the network and application layers to ensure that critical services receive minimal disruptions. This can be through assets and services deployed in multiple separate environments.

3.1.1 **Enforce network traffic inspection** with appliances such as a Next-Generation Firewall (NGFW) that includes deep packet inspection (DPI), intrusion detection / prevention, and application control capabilities. With these appliances, organisations may wish to adopt a mixture of positive and negative security models where applicable e.g., allowlisting and blocklisting. Additionally, for Cloud implementation, a Cloud Network Firewall may offer auto-scaling capability.

3.1.2 **Implement a Web Application Firewall (WAF)** for inspection and validation of application payload against application security risks referencing industry resources such as OWASP Top 10 or CWE Top 25. Additional capabilities may include rate limiting API requests and blocking traffic from known malicious bots. Firewall thresholds for raising alerts or activating mitigation measures (e.g., rate limiting) should also be established in line with the baselines established in 2.1.5. Organisations should consider the following best practices for firewall thresholds:

i) Alerts should be raised if network traffic increases by 10% - 20% compared to baseline traffic.

ii) Activation of mitigation measures should be triggered if network traffic increases by 15% - 20% of the alert threshold, or an increase of around 30% - 50% compared to baseline traffic.

3.1.3 Deploy **dedicated pathways for serving different organisation functions** or functions of differing criticality. This reduces the attack surface for critical services and ensures they receive minimal disruptions when non-critical services are targeted.

3.1.4 Deploy **load balancers** to distribute requests for workload processing for each set of critical assets and services.

3.1.5 Deploy and configure **application nodes at each load balancer** such that application resources can scale according to workload processing demands.

3.1.6 For applicable use cases, enable **mutual Transport Layer Security (mTLS)** to mutually authenticate users and services such that only genuine requests are served.

3.2 Maintain Good Cyber Hygiene

Establishing a secure baseline for assets and services through patching and hardening reduces the likelihood of succumbing to non-targeted as well as targeted but non-sophisticated attacks.

3.2.1 Keep track of **new Common Vulnerabilities and Exposures (CVE) records** based on the BOM list.

3.2.2 **Regularly scan** assets and services for vulnerabilities.

3.2.3 **Deploy patches** to critical assets and services in a timely manner.

3.2.4 **Deploy workarounds and detection rules for zero-day CVE** if the assets and services cannot be brought offline.

3.2.5 Reference industry's benchmarks for **secure configurations and contextualise to the deployed environment** to minimise exploits from the public internet.

3.2.6 Ensure that critical assets and services remain aligned to hardening baselines through **periodic follow-up assessments and necessary remediations**.

3.3 Engage DDoS Protection Service Providers

Managed DDoS protection services by Internet Service Providers (ISPs), Cloud Service Providers (CSPs), etc., with dedicated infrastructure on a global scale may be better suited to handle DDoS attacks of increasing volume and complexity at both network and application levels. Note that engaging a DDoS protection service does not grant immunity to DDoS attacks, and organisations are still responsible for putting in place appropriate measures such as incident response plans and business continuity plans to prepare for, respond to and recover from DDoS attacks.

3.3.1 Enable **network traffic inspection** to detect and block illegitimate protocols and volumetric network attacks for network traffic routed through service providers before arriving at organisation's application resources.

3.3.2 Enable **web application traffic inspection** or a WAF appliance with rules configured against application security risks referencing industry resources such as OWASP Top 10 or CWE Top 25, rate limit API requests and block traffic from malicious bots.

3.3.3 Subscribe to highly available and resilient **Domain Name System (DNS) hosting service** with a global network of servers located in multiple geographic regions to deliver DNS responses efficiently. The service should filter out malicious DNS traffic and enable **Domain Name System Security Extensions (DNSSEC)** to mitigate DNS-related attacks such as DNS spoofing, man-in-the-middle, unauthorised DNS changes.

3.3.4 Utilise **Content Delivery Network (CDN)** with a global network of servers located in multiple geographic regions to offload and cache content from origin servers. Utilising a CDN also hides the IP address of the origin server, obscuring the actual hosting infrastructure and protecting it from attacks. CDNs can also employ captcha challenges, which reduces the risks of application layer attacks.

3.3.5 Enable **bot management solutions** that can detect and prevent activities of malicious bots/ botnets often utilised in DDoS attacks. Solutions may leverage detection capabilities such as behavioural analysis and client request or device fingerprinting.

3.4 Understand the Responsibilities between Subscriber and Service Provider

When deciding on the use of managed DDoS protection services, **understand, assess, and review** the service provider's (ISP/CSP) defences, and **service level agreements** to ensure both parties are aligned on minimally the points mentioned below. A common understanding helps ensure **effective protection services** as well as **timely response** of the parties involved.

3.4.1 The **scope of protections** offered by DDoS mitigation services:

i) Service Provider should clearly define the scope of DDoS protection services, specifying the assets covered, types of DDoS attacks mitigated, the extent of protection (e.g., network, application layer attacks) and support for incident response. Regular communication of updates to the scope based on emerging threats or changes in infrastructure should be carried out.

ii) Subscriber should ensure that organisational assets, critical infrastructure, and specific security requirements for DDoS protection are communicated effectively to the Service Provider. If there are changes or updates to the scope of protection, inform Service Provider promptly.

3.4.2 The **risks** posed by gaps/limitations in coverage.

i) Subscriber, in consultation with Service Provider, should conduct risk assessments to identify potential DDoS attack vectors and vulnerabilities in the organisation's infrastructure.

ii) Identified risks should be clearly communicated between both parties, and it would be best for subsequent mitigation strategies to be a collaborative effort. Additionally, Subscriber should inform Service Provider if there are any perceived gaps or limitations in the security coverage that may impact organisational assets or compliance.

3.4.3 **Thresholds** for raising alerts for volume traffic and subsequent performance of DDoS mitigation which should be set below the maximum capacity of the agency's network appliances' bandwidth.

i) Service Provider should **establish clear alert thresholds for different types and magnitudes of DDoS attacks**, considering factors such as traffic volume, patterns, and duration. These thresholds should be communicated with the Subscriber to ensure that it suits the Subscriber's needs and should be below the maximum capacity of the Subscriber's network appliance throughput. Response times and escalation procedures should be discussed so that DDoS incidents are addressed promptly and effectively.

ii) Subscriber should in turn **understand the established alert thresholds and criteria for severity**. Clearly communicate with Service Provider about their infrastructure's maximum thresholds and discuss their needs with the service provider. Regular reviews should be conducted to ensure that appropriate adjustments are made for dynamic environments.

3.4.4 **Communications channel** for effective and transparent incident and problem management, covering the following:

i) Primary communication channel e.g., mobile call, mobile message, email. Ideally, primary communication channel should allow the other party to verify that the message has been received (e.g., a phone call is answered, read receipts for messages).

ii) Secondary communication channel if the primary channel fails. Parties may want to consider using multiple means of communication simultaneously, and not just as a backup option, for greater efficiency of response.

iii) Relevant organisation personnel to be notified.

iv) Frequency of updates to organisation in the event of an attack.

3.4.5 **Definitions** of terminology used.

i) Service Provider should try to provide a comprehensive glossary of DDoS-related terminologies used in the cybersecurity domain. A common understanding between Service Provider and Subscriber should be established.

ii) Subscriber should ensure that users are familiar with key DDoS-related terms and concepts through training programs. Clarifications should be made on unfamiliar terms. Common vocabulary should be used to facilitate effective communication before, during and after any possible cybersecurity incident.

3.5 Conduct DDoS Sustainability Tests

Simulation and load tests help to ensure configurations and thresholds are appropriately configured for effective DDoS mitigation. Such tests may also highlight single points of failure that were missed during design and implementation.

3.5.1 Conduct DDoS simulation and load tests to determine the **maximum workload transactional capacity** for critical assets and services as well as validate the configured thresholds of DDoS mitigation services and measures.

3.5.2 Engage the assistance of professional service providers, if necessary, and ensure that tests are conducted in compliance with the user agreement of hosting environment providers.

3.5.3 Take note of the **metrics and indicators** relevant to the organisation's operating environment such as service transactions, network health, application servers' performance (e.g., CPU utilisation, memory usage, network bandwidth).

3.5.4 **Adjust the thresholds and configuration parameters** of the environment based on the results and metrics captured from the tests above. These tests should be performed when significant changes are made to the environment, as well as periodically to ensure that the growth of the organisation does not outpace the configured thresholds and parameters.

3.6 Be familiar with the Incident Response Plan

Periodic drills and refresher training for all stakeholders to be familiar with their roles is critical in ensuring that the established processes are effectively carried out with the support of implemented technology solutions. Drills and simulation exercises may also help to highlight potential improvements that may be incorporated into the plans.

3.6.1 **Conduct DDoS tabletop exercises** and drill tests of the DDoS response plan on a regular basis with all internal and external stakeholders, including support from managed security service providers if applicable. This is to familiarise all stakeholders with the processes involved, as well as to identify gaps and issues before a real attack.

3.6.2 Conduct an **after-action review (AAR)** after each tabletop exercise/test and update the DDoS response plan based on lessons learned regarding communication, mitigation, and recovery.

4 Detect

4.1 Monitor for Early Warnings of DDoS Attacks

Security monitoring for early signs of DDoS attacks can allow organisations to respond promptly with mitigating measures and minimise the disruption to operations.

4.1.1 Monitor for **abnormal slowness or abnormal surges in network traffic** (e.g., network latency) to critical assets and services from the public internet.

i) Keep track of **optimal response time and latency time** of critical assets and services during business-as-usual period.

ii) Set up and fine-tune **alarm thresholds** to detect abnormal response time and latency time to critical assets and services.

iii) **Automate notification to operation team and disaster recovery team** for immediate diagnostic and investigation upon detection.

iv) Upon detection, **enable network packet capture** to support further investigation and analysis of attack traffic if resources permit.

4.1.2 Monitor for **unusual traffic (reconnaissance traffic)** coming from a single or a group of IP addresses.

4.1.3 Other indicators of DDoS include but are not limited to:

i) Slow application performance

ii) High processor and memory utilisation

iii) Websites being unavailable

iv) Unexpected surge in ingress traffic

4.2 Determine the Nature and Scope of the DDoS Attack

After verifying that suspicious traffic is a DDoS attack, identify the relevant details and communicate those details to the right teams for efficient mobilisation of mitigation measures.

4.2.1 Verify that the suspicious traffic is a DDoS attack:

i) Perform **internal checks** to assess if service disruptions stem from internal faults or events e.g., organisation's server failure or configuration errors on network devices.

ii) **Contact managed service providers** through previously established communication channels, if applicable, to verify if observed service disruptions for the organisation's services arose from service provider outages.

4.2.2 Identify the **details** of the DDoS attack:

i) **Identify the critical assets and services** that are being affected, including IP addresses of the systems, through available tools and documentation such as network monitoring services or network infrastructure diagrams.

ii) Work with **managed security service providers**, if applicable, to **identify malicious packets** e.g., destination port number, communication protocol, and **determine the DDoS attack vectors**.

iii) Review **logs/critical equipment health status** e.g., DNS logs, Router/Firewall CPU and Memory, etc.

iv) Ensure that logs are **shared among various teams** e.g., Apps, Server, Network, Cybersecurity, in a timely manner for a more holistic view of incident.

v) Inform managed service providers, if applicable, on the possibility of DDoS attacks such that **packet inspection** may be enabled for specific network traffic to facilitate subsequent investigations.

5 Respond

5.1 Execute DDoS Incident Response Plan and Other Mitigation Measures

Execute the DDoS Incident Response Plan and mitigation measures to minimise the impact of the DDoS attack and reduce disruption to delivery of services, with the end goal of resuming normal operations.

5.1.1 In the event of a DDoS attack, **follow the established DDoS response plan, adapt, and respond to the situation**, inclusive of incident escalation procedures and communication plans to internal and external stakeholders.

5.1.2 The following mitigation strategies to minimise the impact of the attack and restore normal operations may be adopted:

i) **Identifying and blocking malicious traffic:** Once the attack path has been identified, custom rules can be added into network firewall or WAF to block malicious traffic (such as through IP address or geolocation restrictions), reducing the load on the target server or network.

ii) **Absorbing attack traffic:** Managed DDoS protection services and workload scaling can help absorb attack traffic while permitting legitimate user traffic to still be processed. This involves activating redundant systems and resources to increase the network and application load that may be served.

iii) **Rerouting traffic:** Network traffic can be rerouted to other services or networks to avoid overwhelming a single target server or network.

iv) **Implementing rate limiting:** Rate limiting can be used to control the amount of traffic that can be sent to a server or network, preventing it from being overwhelmed.

v) **Shutting down affected vulnerable service(s)/resource(s) for remediation**: For attacks targeting known vulnerabilities of services/resources, organisation may isolate and remediate the vulnerable resources against observed attacks before bringing them back online. Note that, depending on the scale of affected services/resources, this might disrupt the entire system.

vi) **Preserve essential service(s)/resource(s)**: During persistent attacks on non-critical services/ resources that impact business-critical services/ resources, organisation may choose to deny attack paths of the threat actor by shutting down targeted services/resources and preserve the availability of essential organisation services/resources. This separation should ideally be accounted for during design and implementation of services.

5.1.3 Where feasible, **automation of the above processes** might enable faster response and activation of the response plan, alongside a streamlined incident response process, reducing the impact of the attack. However, **human oversight of the automated processes** is key to addressing the risk of false positives/negatives, as well as to make critical judgement decisions.

5.1.4 Take note of the following considerations when leveraging automated DDoS mitigation/ incident response measures:

i) Not all incidents are suitable for automation and may require human intervention/decision-making. As such, **conduct a risk assessment to evaluate the impact of automated response**, such as the risk of false positives and negatives, and ensure that there are **fallback**

mechanisms i.e., human intervention to address unintended consequences of the automated solution.

ii) Automated solutions should have **granular controls** for thresholds, triggers, and escalation paths, ensuring that the configuration aligns with the changing needs of the organisation; these should be fine-tuned in accordance with insights derived from DDoS sustainability tests and post-incident reviews.

5.1.5 **Continue to monitor** other network assets for any additional anomalous or suspicious activity that could indicate **intrusion attempts or other malicious activity targeting** the organisation while the current DDoS attack has **diverted the organisation's attention and resources**.

5.1.6 Organisations suspected to be a victim of DDoS attacks are strongly advised to report the case to SingCERT via the Incident Reporting Form as the information could help alert and assist other individuals and organisations. If monetary loss(es) or criminal activity is involved, organisations may lodge a police report at any neighbourhood police post or online here.

5.1.7 Organisations that encounter Ransom DDoS (RDDoS), where a malicious actor threatens to conduct DDoS attacks on an organisation unless a ransom is paid, are strongly encouraged **not** to pay the ransom – doing so does not guarantee that the attack will not happen and will further fund criminal activity. Instead, report the case to SingCERT via the Incident Reporting Form and mobilise your response teams against a potential DDoS attack, taking actions as outlined in your DDoS Incident Response Plan.

6 Recover

6.1 Resume Normal Operations

Perform restoration activities to ensure that system and services affected by DDoS incident resume normal operating status.

6.1.1 **Initiate recovery phase** of incident response plan, such as restoring data from backups and other restoration assets and restoring network channels and connections.

6.1.2 **Verify that services have been restored** to the level required for business operations, such as in terms of bandwidth, latency, and application performance.

6.1.3 **Notify internal and external stakeholders** on the activities performed for recovery as well as the progress for restoration of operational capabilities.

6.2 Review and Incorporate Lessons Learned

Review the incident and improve upon the DDoS response plan based on lessons learned.

6.2.1 When the attack has subsided and normal operations have resumed, **review and document the incident** with managed security service providers, covering at least the following:

i) **Attack Analysis**: assets targeted, attack characteristics (sustained flood, level of sophistication), peak amount of network traffic, length of attack.

ii) **Impact Analysis**: services impacted (extent of impact + length of downtime), indirect damages (e.g., loss of IP, reputational damage), user impact (from both attack and from defensive measures).

6.2.2 **Update the DDoS response plan** to include improvements drawn from lessons learned regarding communication, mitigation, architecture improvements and recovery. **Continue to conduct DDoS tabletop exercises** and drill test the DDoS response plan.

6.2.3 **Participate in collaborative threat intelligence sharing partnerships** with other organisations to exchange information about cyber threats including DDoS attacks. Collective knowledge can enhance situational awareness to detect recent types of DDoS attacks and mitigate them effectively.

References

1. Cybersecurity and Infrastructure Security Agency (CISA) Understanding and Responding to Distributed Denial-of-Service Attacks.
   https://www.cisa.gov/sites/default/files/pulications/understanding-and-responding-to-ddos-attacks_508c.pdf.
   Accessed on Nov 2023.
2. CISA Capacity Enhancement Guide: Volumetric DDoS Technical Guidance for FCEB Agencies.
   https://www.cisa.gov/sites/default/files/2023-09/TLP%20CLEAR%20-DDOS%20Mitigations%20Guidance_508c.pdf.
   Accessed on Nov 2023.
3. CISA DDoS Quick Guide.
   https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf.
   Accessed on Nov 2023.
4. CSA DDoS Playbook.
   https://www.csa.gov.sg/Tips-Resources/singcert/incident-response-playbooks.
   Accessed on Dec 2023.
5. NIST Cybersecurity Framework 2.0.
   https://www.nist.gov/cyberframework.
   Accessed on Mar 2024.
6. Gcore Radar: DDoS Attack Trends.
   https://hello.gcore.com/hubfs/wp-security-gcore-radar-q3-4-2023.pdf.
   Accessed on Feb 2024.
7. Verizon 2023 Data Breach Investigations Report:
   https://www.verizon.com/business/resources/T108/reports/2023-data-breach-investigations-report-dbir.pdf.
   Accessed on Feb 2024.
8. Cloudflare Radar: DDoS attack trends for 2023 Q4.
   https://radar.cloudflare.com/reports/ddos-2023-q4.
   Accessed on Feb 2024.
9. NetScout blog: Beware of Application-Layer Attacks.
   https://www.netscout.com/blog/beware-application-layer-attacks.
   Accessed on Feb 2024.
10. Palo Alto Networks Tech Docs: DoS and Zone Protection Best Practices.
    https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices.
    Accessed on Jul 2024.