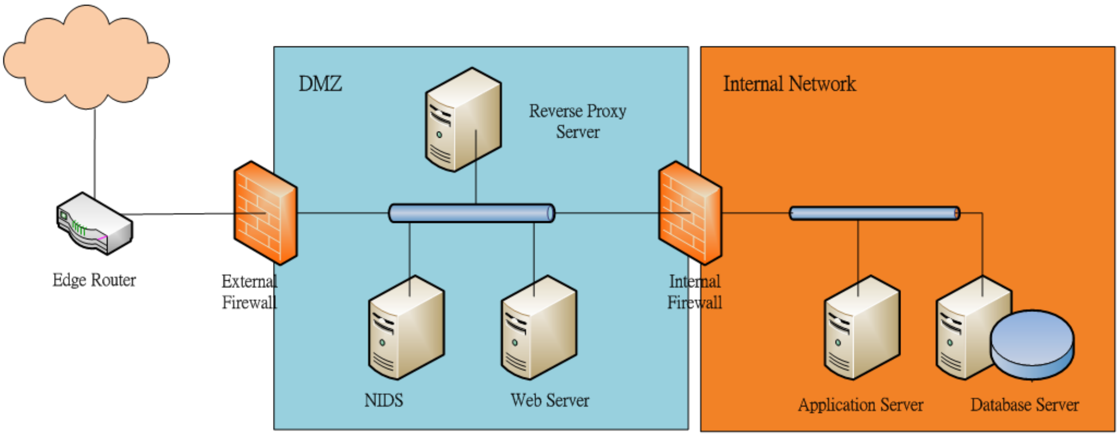
CHAPTER 8
WEBSITE AND WEB APPLICATION SECURITY

8.1 Website and Web Application Security Architecture

8.1.1 A typical website and web application architecture contains three tiers, which separate an external facing web server, application server, and database server as shown in the diagram below. With such a tier-based architecture, even if an attacker compromises the external facing web server from outside, the attacker still has to find ways to attack the internal network.



(a) The external facing web server should be confined within a demilitarized zone (DMZ), which is a special network segment containing servers with access to Internet services. Servers with sensitive information are located in the internal network with additional protection. The internal and external firewalls should be from different vendors or types so that the firewalls will not have the same vulnerability.

(b) Network intrusion detection system (NIDS) / intrusion prevention system (NIPS) should be installed to detect / prevent attacks or suspicious traffic in the DMZ and to identify attacks at the earliest possible moment. In addition, NIDS / NIPS should always be updated with the latest attack signatures provided by the vendor. Web Application Firewall (WAF) and anti distributed denial of service (anti-DDoS) attack are application specific security devices to protect a website and web application against common threats such as injection and application-based distributed denial of service (DDoS) attacks. Therefore, they should be considered to be deployed for the monitoring and blocking of web traffic in the DMZ.

8.2 Web Server Security

8.2.1 Schools are recommended to perform security risk assessment in order to determine the most appropriate security protection measures.

8.2.2 Schools are recommended to perform system hardening for associated servers such as web, application, database and file.

8.2.3 Schools are advised to check their web servers to see if they are configured and running properly. The following suggestions can be observed in enhancing the security of the web servers:

(a) Follow security requirements based on the information classification.

(b) Configure web server securely according to the vendor's security guidelines.

(c) Run web server processes with appropriate privilege account. Avoid running the web server processes using privileged accounts, e.g. 'root', 'SYSTEM', 'Administrator'.

(d) Apply the latest approved security patches to the web server software and avoid using the end of supported components.

(e) Configure access rights strictly according to system hardening guideline and application requirements such as read-only access for information to public.

(f) Disable all unused accounts, including user and default accounts. If possible, the unused accounts should be removed if there is no impact for running websites and web applications.

(g) Avoid storing users' passwords in database or file without proper protection such as hashing and / or encryption.

(h) Install host-based intrusion detection system (HIDS) / intrusion prevention system (HIPS) in web servers especially the website(s) storing or processing confidential information in order to monitor suspicious activities or unauthorised creation / deletion / modification / access of files.

(i) Review alerts and reports from the security devices such as HIDS / HIPS to identify security attacks at the earliest possible moment. In addition, HIDS / HIPS should always be updated with the latest signatures approved by change management, if appropriate.

(j) Do not disclose configuration information such as server software version, internal IP address and directory structure.

(k) Disable unnecessary modules and remove them if possible.

(l) Ensure that unused or less commonly used services, protocols, ports and functions are disabled to reduce the chance of being attacked.

(m) Remove default or sample files from the web server software.

(n) Restrict web crawling for the contents that are not supposed to be searched or reached by public search engines.

(o) Identify important files on the web server for running the web application and protect them with proper controls such as access right control.

(p) When using secure sockets layer (SSL) / transportation layer security (TLS), backup the private key for server certification and protect it from unauthorised access.

(q) Backup data of the school's website including data files, database and settings of the whole website.

8.3 Web Server Monitoring and Incident Handling

8.3.1 For security monitoring, schools are recommended to actively review alerts and reports from NIDS / NIPS to identify attacks at the earliest possible moment.

8.3.2 For security incidents such as web defacement and DoS / DDoS attack, IT staff should follow the security incident handling procedure to handle the security incident until it is mitigated. Schools should also report the case to Hong Kong Police Force (HKPF) and Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT).

8.4 Web Application Security

8.4.1 The following are recommended administrative controls that may help schools in strengthening the security of web applications and protecting data handled by such applications.

(a) Put in place key guidelines to provide direction on the development and maintenance of websites and / or online applications.

(b) Put in place key guidelines on coding and development practices for web applications. Software developers should follow a set of secure web application coding practices designed to combat common web application security vulnerabilities.

(c) Collect and manage sensitive information and user data in compliance with policies and regulations.

(d) Prepare a security and quality assurance plan, and adopt quality assurance methods such as code review, penetration testing, user acceptance tests.

(e) Perform a complete IT security audit before the final production launch of a web application, and after any major changes or upgrades to the system.

8.5 Keep Your School's Website Safe:

8.5.1 The following practices are recommended to keep the school's website safe:

(a) Software update: update operating system, applications and framework libraries regularly.

(b) Data encryption: encrypt sensitive information in web page.

(c) Remote administration: adopt secure remote access solution for website administration.

(d) Authentication password: adopt strong authentication and password.

(e) Alert notification: enable and review event logs and alerts.

(f) Search indexing: prevent data leakage through public search engine.

(g) Security scan: conduct security vulnerability scanning or penetration test.

(h) Outsourcing: select web hosting service that can meet the school's security requirements.

8.6 Secure Website with HTTPS Protocol

8.6.1 Points to note about HTTPS and Website Security:

(a) Use server certificate issued by a recognised certificate authority and keep the certificate in "trusted" condition.

(b) Employ secure protocols only, e.g. TLS 1.2.

(c) Automatically redirect web traffic to HTTPS site, e.g. enable HTTP Strict Transport Security (HSTS) Support.

(d) Use strong cipher suites, e.g. SHA-256, AES 256-bit and disable those functions with security risks, e.g. TLS compression.

(e) Update operating systems, applications, framework libraries and cipher suites periodically.

(f) Store sensitive data in the backend server with proper protection.

(g) Do not include sensitive information in the URL.

8.6.2 To enable HTTPS on websites for content delivery, schools need to acquire digital certificates for servers. Reference could be made at the following webpage of OGCIO on the recognised certification authorities in Hong Kong:
https://www.ogcio.gov.hk/en/our_work/regulation/eto/ordinance/ca_in_hk/

8.7 Anti-DDoS Protection

8.7.1 DDoS attack is initiated from Internet. As such, an effective way to address both the volumetric and application layer DDoS attack is to adopt the anti-DDoS clean pipe solution, which provides real-time protection to analyse the network traffic to block malicious traffic and permit the legitimate traffic.

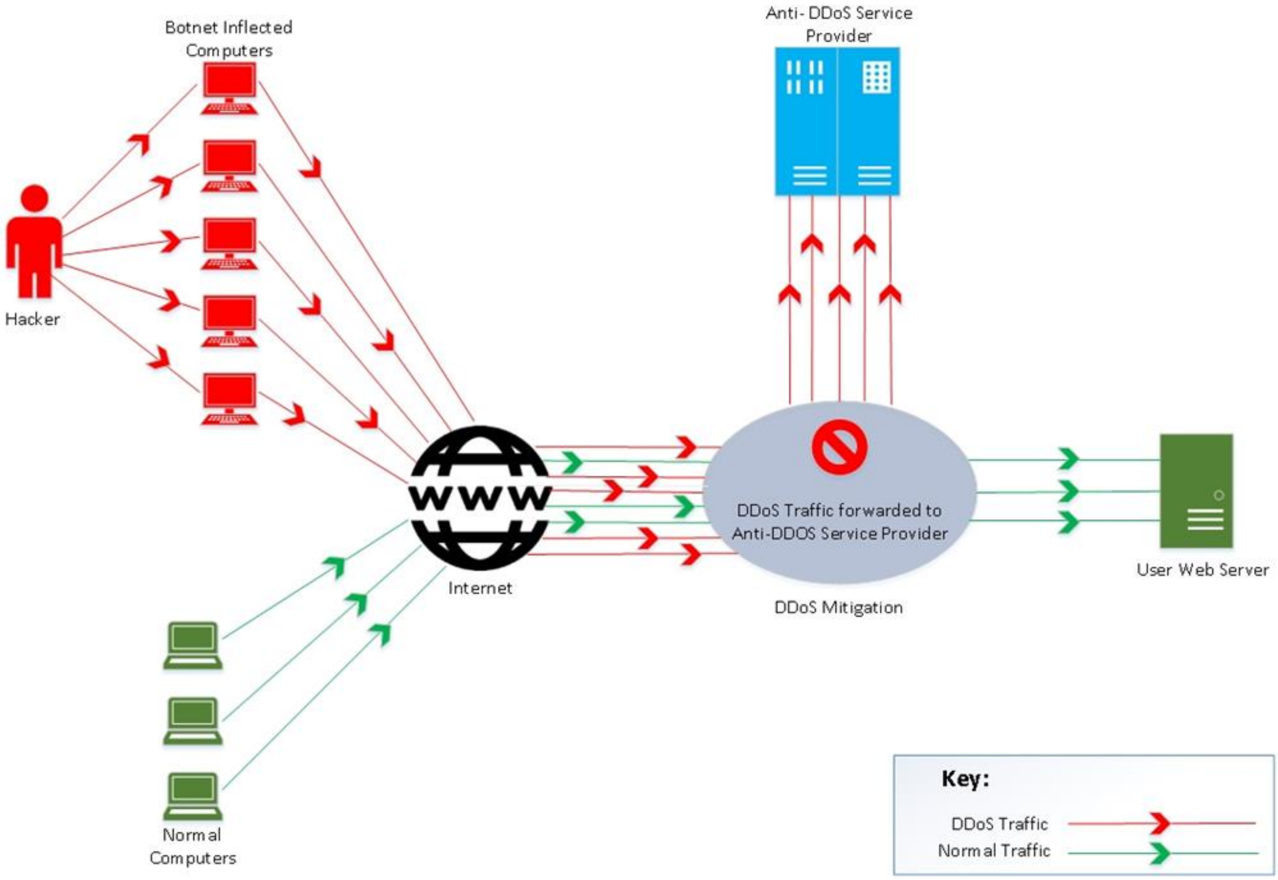
8.7.2 Anti-DDoS clean pipe solution also offers benefits on real-time and proactive mitigation on DDoS attack, better bandwidth utilisation with network-based defence as well as the immediate notification on the attack event.

8.7.3 School should define the service requirements such as the service level agreement (SLA), the subscribed clean pipe bandwidth and the needs for the anti-DDoS attack protection in order to engage anti-DDoS outsourcing or external service providers.

8.7.4 Anti-DDoS solution should be transparent to user and user’s involvement in operation is minimal. User may receive alert notification and routine reports about the DDoS attack and service level summary. User should raise enquiry or report to the school’s IT staff when there is potential access issue, such as inaccessible for website or missing email.

8.7.5 IT staff is responsible for administration of the anti-DDoS solution provided by outsourcing or external service providers, and is required to observe and follow up timely for any DDoS attack alerts to ensure the Internet network service and related e-services are sustained.

8.7.6 IT staff should review the service report and follow up issues with anti-DDoS outsourcing or external service providers such as missing SLA and unresolved technical problems, and recommend the subscription of additional bandwidth where appropriate.


Botnet Inflected Computers
Anti- DDoS Service Provider
Hacker
Internet
DDoS Traffic forwarded to Anti-DDOS Service Provider
DDoS Mitigation
User Web Server
Normal Computers
Key:
DDoS Traffic
Normal Traffic