Firewall Setup Tips for SMEs

A firewall helps defend against cyber attacks and data breaches through shielding computer or network from malicious or unnecessary network traffic

www.cybersecurity.hk

www.cyberdefender.hk

GovCERT.HK
Government Computer Emergency Response Team Hong Kong

HKCERT
Hong Kong Computer Emergency Response Team Coordination Centre

Hong Kong Police Force

What are the differences between a hardware and a software firewall?

- A hardware firewall is a physical device, while a software firewall is installed on an individual computer or server and operates via an application.
- A hardware firewall, usually installed at the network perimeter, is the first line of defense against cyber attack by controlling incoming traffic before data enter an enterprise network, while a software firewall controls the data entering or leaving the computer or server and blocks any suspicious traffic.

Is the firewall in the operating system good enough?

- It functions as a software firewall, which may be sufficient to protect individual devices during daily Internet browsing.
- Yet, it may not offer comprehensive coverage and protection to the enterprise network, e.g. blocking specific traffic, virus or malware infections.

Is the built-in firewall in routers good enough?

- A router can function as a hardware firewall by using network address translation (NAT) to direct incoming requests to designated devices.
- Various security settings can also be made, e.g. enabling access control via whitelisting, putting a computer in a demilitarised zone (DMZ).
- Nevertheless, it may not offer comprehensive coverage and protection as a hardware firewall does.

Which firewall fits SMEs?

It depends on the business needs and the network size. For best protection, installation of both hardware and software firewalls is recommended. In reality, there are different considerations regarding cost and maintenance. Some pros and cons are listed below for reference:

- A hardware firewall provides centralised protection for devices in the entire network, whereas a software firewall only protects individual computers, and each needs to be configured and updated individually.
- A hardware firewall takes up physical space and the installation cost is higher. If a computer is used outside a protected office network, a hardware firewall cannot offer protection. Software firewall configuration is more flexible, but it may slow down computer performance.
- A hardware firewall can be easily integrated with other security features, e.g. intrusion prevention system (IPS), sandboxing and threat intelligence gathering.

General tips for firewall setup

Basic firewall security

- Update the firewall firmware to the latest version
- Set up administrative accounts with limited privileges based on their responsibilities
- Change all default passwords
- Do not use shared user accounts

Design network zones

- Collectively group devices with similar functions and similar sensitivity requirements into network zones
- Servers that provide web-based services (e.g. email, VPN) should be placed inside the DMZ to limit inbound traffic. Other servers (e.g. file, database) should be placed in internal server zones

Configure access control lists

- Create inbound and outbound access control lists (ACL) to allow designated traffic flow into and out of each zone
- The list should be made specific to allow or deny the IP addresses/ ranges and port numbers

Test firewall configuration

- Conduct vulnerability scanning and penetration testing to verify if a firewall is functioning properly
- Keep a backup of the configuration

Firewall management

- Conduct regular reviews and audits, and also properly maintain and review log records to ensure a firewall functions properly