# Firewall security considerations

CANADIAN CENTRE FOR CYBER SECURITY

September 2023 | ITSAP.00.059

A firewall is a security mechanism that monitors and controls the incoming and outgoing traffic based on the organization's rules established in policies. Firewalls are an essential security control that help to segment your network to prevent the unauthorized flow of data from one area of the network to another. Traffic passing through firewalls often contains your organization's data. If firewalls aren't properly configured or maintained they can be exploited by threat actors, putting your data at risk of being compromised. Whether you're a small, medium, or large organization, this publication provides guidance on actions you can take to secure your firewalls.

## What are the general deployment use-cases for firewalls?

Firewalls can be placed at various points in your network to create zones of allowable traffic flow based on your use-case. The following provides a listing of deployment scenarios for firewalls:

**Network-based**: These are hardware or software-based firewalls that are typically installed between network boundaries or at the network perimeter. Their purpose is to defend against network threats such as blocking malicious Internet traffic from penetrating your corporate network. In a virtualized environment, these firewalls can also be used to create segmented areas of trust zones within the network. They are typically used in software defined networking (SDN) and SDN wide area network (WAN) solutions to improve network security and management.

**Host based**: These are software or agent-based firewalls that are installed on endpoints or servers such as computers and devices. Their purpose is to restrict incoming and outgoing network traffic to protect the device on which the firewall is configured. A common example is the firewall built into most major operating systems.

**Application-based**: These are firewalls that are deployed to manage traffic to and from a system application (app) or service whether on-premise or in the cloud. They are available as hardware or in virtual options, and their primary focus is to protect against application-layer attacks. These are typically deployed to protect web apps, mobile apps, application programming interfaces (APIs) and services. Web app firewalls (WAF) are used to detect and block malicious hypertext transfer protocol (HTTP) traffic. Reverse proxy solutions also incorporate these capabilities to make it harder for threat actors to launch a distributed denial of service (DDoS) attack.

**Cloud-based**: These are virtual firewalls that are primarily deployed within a cloud environment to control the flow of traffic into and from the cloud tenancy (e.g. between untrusted zones like the Internet and trusted zones like your organization's on-premise segments). Cloud firewalls enforce policies and permissions to protect data and resources in the cloud.

## What are the risks associated with firewalls?

When implementing firewalls, one of the most serious mistakes is to leave the vendor default configurations. Firewalls aren't shipped with settings established so that they can be used right out of the box; they must be configured for each network's purposes. Failing to change default configurations can make your organization more susceptible to compromises. Similarly, improperly configured firewalls can also make your network vulnerable to threat actors. The following are potential threats associated with deploying and managing firewalls:

- May contain zero-day vulnerabilities in its firmware or software which threat actors could exploit to access your network and system resources.
- May contain exploitable components or malware if manufactured by vendors without proper or robust security practices.
- May contain outdated software or firmware patches.
- May cause your organization to be noncompliant with regulatory standards if misconfigured firewall systems result in data breaches or data loss.

## What is a next-generation firewall (NGFW)?

Traditional types of firewalls control network traffic based on states, ports, and protocols which are filters based on predefined rules. A NGFW provides all of the functionality of a traditional firewall but has enhanced capabilities including the detection of malware. NGFWs not only inspect a packet's header but also its content and source. Additional features that NGFWs can provide include:

- intrusion prevention system (IPS)
- Intrusion detection system (IDS)
- standard policy-based protection
- application filtering
- geo-location blocking
- anti-virus (AV) protection
- uniform resource locator (URL) filtering
- virtual private networking (VPN) support
- secure socket layer/transport layer security (SSL/TLS) traffic inspection
- DDoS protection
- data loss prevention (DLP)
- email protection

Communications Security Establishment | Centre de la sécurité des télécommunications



Canada

# Firewall security considerations

CANADIAN CENTRE FOR CYBER SECURITY

September 2023 | ITSAP.00.059

## How to secure your firewall

Firewalls alone, even if properly configured, are not enough to protect your network from malicious traffic. Like most security controls and as a best practice, firewalls should be used as part of a layered defence-in-depth approach to strengthen your organization's resistance to cyber attacks. For more information on other measures you can implement to protect your networks and devices, see Preventative security tools (ITSAP.00.058). Depending on your organization's needs and the assets at risk, the following are important actions that can help secure your firewalls:

- ☐ Procure products from trusted vendors that have robust security protection practices. Validate its integrity by performing hash verification to ensure values match the vendor's database.
- ☐ Flash network devices with trusted firmware before using them for the first time. Perform hash or checksum verification to verify the integrity of the downloaded firmware file. This can help reduce cyber supply chain risks such as introduction of malicious firmware.
- ☐ Install software updates and patches regularly and as soon as they are made available.
- ☐ Monitor and audit firewall logs for any unusual or suspicious activities. Regularly review logs to identify potential security incidents, such as unauthorized access attempts or unusual traffic patterns. For more information, see Network security logging and monitoring (ITSAP.80.085).
- ☐ Set up a secure administrative workstation for managing firewall configuration that is isolated from the network with no access to the Internet. If there's a clear business need for Internet access, then protect the workstation with additional controls such as multi-factor authentication (MFA) or an IP allow list that limits access to trusted IP addresses. For more information, see Top 10 IT security actions: No. 3 managing and controlling administrative privileges - ITSM.10.094.
- ☐ Change all default administrative passwords and limit the number of system administrators that can make changes to your firewall devices. Ensure each has their own account with passphrases or strong passwords and MFA, where possible.
- ☐ Use anti-virus and anti-malware software (or activate it if it's a built-in feature of your firewalls) to protect against malicious programs. For more information, see Protect your organization from malware (ITSAP.00.057).
- ☐ Manage firewall policies by regularly reviewing and updating the rules to ensure they're in the correct order and reflect the current architecture. Check if rules create open holes (e.g. vulnerable services, ports or protocols). Clean up and remove rules that should be temporary or no longer used.
- ☐ Define strict change management processes to ensure that all changes are tracked and are in accordance with your organization's security policies.
- ☐ Deactivate unused ports (both physical and virtual) and services on firewalls. This can reduce the risk of threat actors connecting to your network if they can gain physical access to these devices.
- ☐ Remove from the network firewalls that are no longer supported by the vendor. Upgrade or replace these devices as soon as possible.
- ☐ Use multiple firewalls to segment and secure critical networks that hold sensitive data. Isolate the critical networks from the Internet and other areas of the corporate network. For more information, see Top 10 IT security actions: No. 5 segment and separate information – ITSM.10.092.
- ☐ Consider using firewalls from different vendors to protect sensitive areas of network. This way, if one manufacturer reports a flaw or security vulnerability, the other might not have the same vulnerabilities.
- ☐ Use a domain name system (DNS) firewall solution for content filtering to protect your employees from inadvertently visiting potentially malicious domains on the Internet. This could protect your organization from phishing attacks as the DNS firewall will block their access to the malicious site. For more information, see Protective Domain Name System (ITSAP.40.019). The Canadian Internet Registration Authority (CIRA) offers a public protective DNS called the Canadian Shield.
- ☐ Consider activating transparent mode if the feature is available on your firewalls. Transparent firewalls lack IP addresses within the network, making them harder for threat actors to detect and less vulnerable to cyber attacks, such as denial of service (DoS).
- ☐ Keep backups of firewalls to ensure that you can quickly restore settings in case of a failure or security incident. Store the backups securely and test the restoration process periodically. At a minimum, backup the firewall configurations and if possible have a physical backup of the equipment with or without the configurations.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada