Firewalls are networking tools that prevent unauthorized access and protect critical assets from malicious traffic. Firewalls guard networks at their most vulnerable point, adding an essential layer of security to the network perimeter.

This role makes firewalls indispensable. But **choosing the wrong firewall configuration can actually damage network security**. That's why it's important to be aware of the available options before making a decision.

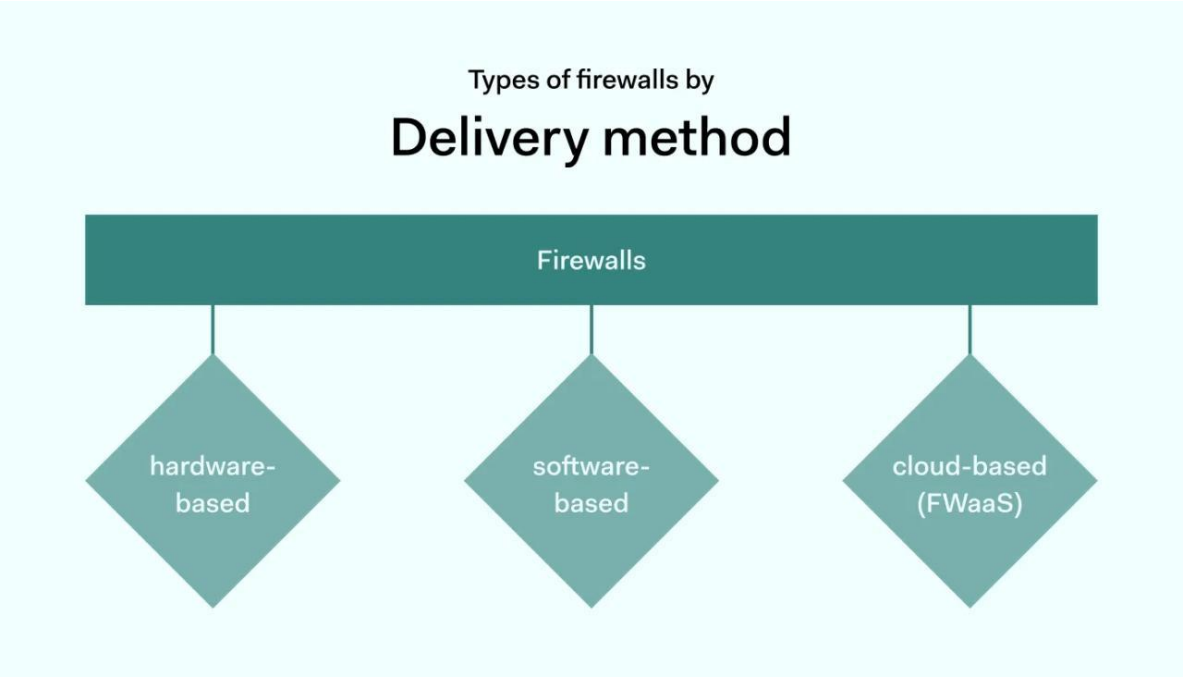
This article will help you understand the different types of firewalls. We will look at how to classify firewalls and learn about the main forms of firewall architecture. The result will be a solid foundation in guarding the network perimeter.

Types of firewalls

Firewalls come in various forms, and companies must find a solution that meets their unique networking needs. Broadly speaking, there are two ways of understanding the types of firewalls.

- **Delivery**. This refers to **where firewalls operate in the network context**. Delivery options can include hardware, software, or cloud-based systems.
- **Technology**. This refers to **how firewalls actually work**. Firewall technology includes packet inspection, proxy or app-based firewalls, stateful firewalls, and next-generation systems.
  These aren't concrete categories. You'll find hardware firewalls with deep packet inspection, and simpler versions that only block IP addresses. But thinking about delivery and technology helps us locate the right firewall for each situation.

Firewalls based on delivery method



The first way of defining the types of firewalls is the method of delivery. There are 3 main delivery types: hardware-based, software-based, and cloud-based firewalls (also known as Firewall-as-a-Service or FWaaS).

1. Hardware-based firewalls

Hardware firewalls are installed on specialist devices within your network rack. These devices contain firmware that creates a barrier between the external internet and on-premises systems. Inbound traffic must traverse this barrier, which provides a secure boundary to block malicious attacks.

Hardware-based firewalls inspect traffic entering and leaving the network, using IP address data to block blacklisted addresses and block unauthorized traffic.
Solutions can also be more complex. For instance, hardware-based firewalls may block unused ports and prevent traffic using them. This counteracts a common route for data exfiltration. Hardware varies in size, from desktop units to designs for server rooms. Stateful models also add extra functionality, enabling deep dives into the content of data packets.

Advantages of hardware firewalls:

- Users can configure hardware to meet specific network conditions.
- Firewalls provide protection without using resources on workstations or servers.
- Updates apply to single devices, making management easier.
- Hardware is less vulnerable to OS exploits, so may be more secure.
- Security teams can centralize data monitoring via a single firewall device.

Disadvantages of hardware-based firewalls:

- Sourcing hardware is expensive compared with software-based alternatives.
- Devices can be bulky, adding clutter to office environments. Additional hardware is always required.
- Upgrades can be challenging. Security teams may need to patch firmware and/or replace equipment.
- Scaling up hardware systems is cumbersome. Companies may be reluctant to update firewalls after investments in expanding their hardware. This may lock in security vulnerabilities over time.
  Hardware-based firewalls are becoming less popular. However, they may still be useful in situations where companies need total control over specific security situations. Otherwise, lightweight software or cloud solutions make more sense.

2. Software-based firewalls

Software firewalls provide the same services as hardware-based firewalls but require no separate equipment. **Instead, software firewalls run on network devices**. For example, Microsoft Windows and macOS come with a native firewall to protect internet traffic.
Users can install software-based firewalls on individual workstations. But they can also install them on servers to provide network-wide protection.

Advantages of software-based firewalls:

- Users can apply granular security protection for each device. Capable of filtering content arriving at individual devices, not just at the network edge.
- Firewalls are easy to install. There is no need for specialist technical networking knowledge.
- They often come bundled with operating systems and servers.
- Affordable to set up and run. Extend easily across on-premises environments.
-

Disadvantages of software firewalls:

- Software may be incompatible with network devices, creating security gaps or requiring costly adaptations.
- While installation is simple, software must be updated on all network devices. This is complex and prone to human error.
- Software consumes resources on individual devices. This can impair network performance.

3. Cloud-based firewalls (FWaaS)

Software and hardware-based firewalls operate in traditional on-premises environments. They protect groups of devices against external threats. Cloud-based firewalls are different. **Firewall-as-a-Service exists in the cloud and requires no extra hardware or software installation**.

Cloud firewalls primarily protect cloud assets. This includes Software-as-a-Service (SaaS) apps as well as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) implementations.

At the same time, cloud firewalls extend protection to on-premises servers and remote work devices. Instead of using software or hardware, they employ cloud-based applications to monitor traffic and block attacks.

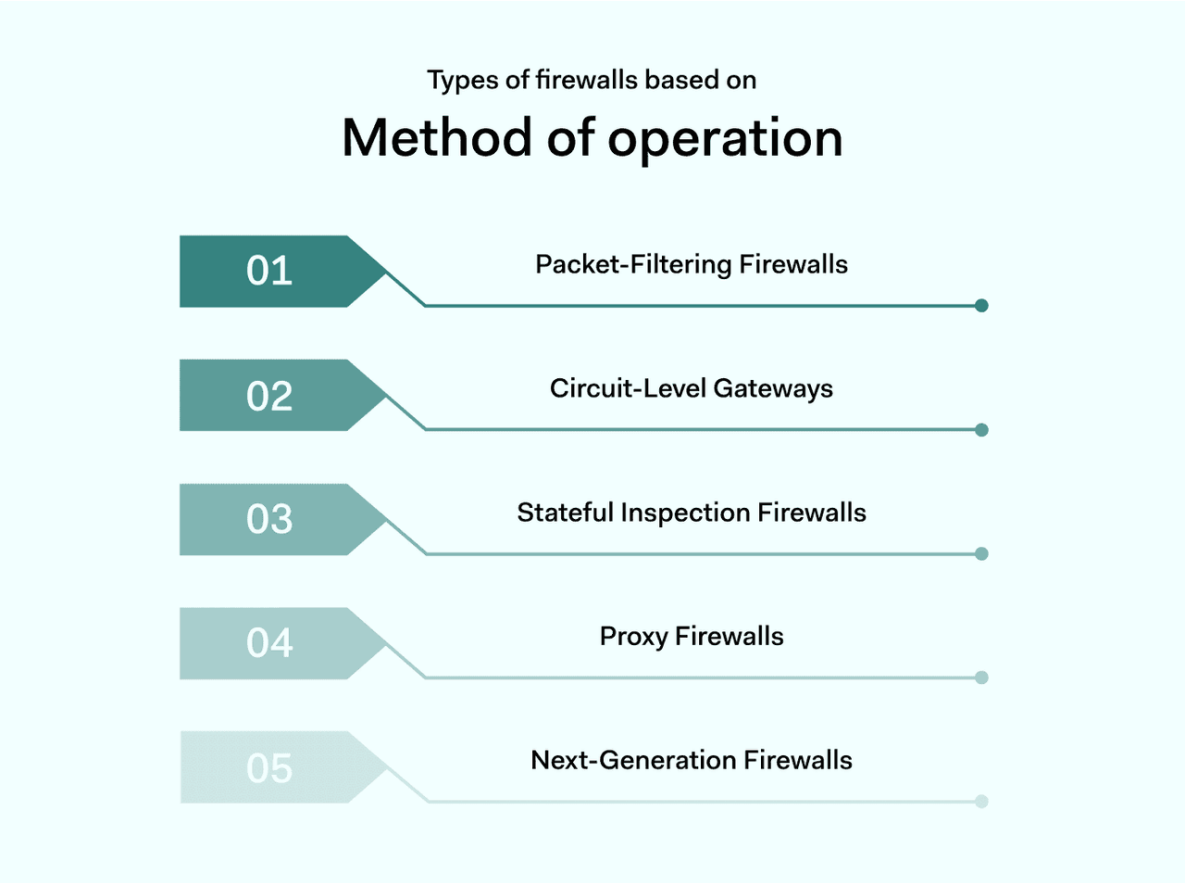
Advantages of cloud-based firewalls:

- Optimized protection for SaaS applications and cloud infrastructure. Virtual firewalls are located close to cloud resources. This reduces the need to backhaul data and boosts efficiency.
- Centralized management. Administrators can configure firewalls from a single device and apply controls to all cloud users.
- Integration with IAM and SSO portals. Users can combine firewall protection and cloud authentication systems.
- Lightweight, off-the-shelf protection from third-party experts. No installation or hardware is required. This makes cloud firewalls a good option for companies with small tech teams.
- Smooth expansion. Cloud firewalls scale easily as SaaS applications come online.
  These advantages make cloud-based firewalls attractive for companies reliant on hybrid cloud environments and remote working. But cloud firewalls also have some potential drawbacks.

Disadvantages of cloud-based firewalls:

- Users must rely on third party providers. Reliance on third-parties generally reduces customization options. Providers may fail to deliver promised security functions. Clients may suffer if virtual firewalls experience availability issues.
- Subscription payments may result in high costs.

Firewall types based on method of operation



The other way of defining types of firewalls is how they work. In technical terms, there are 5 main types of firewalls users need to know about.

1. Packet-filtering firewalls

Packet-filtering firewalls assess data packets passing across network boundaries. Each packet must be compared to a set of pre-defined rules. If the packets meet these rules, the firewall allows traffic to pass. If not, packets are blocked and alerts may be issued.

Information assessed by packet-filtering firewalls can include the destination port in use, the type of packet, and the destination IP address. This data **provides a snapshot of where incoming packets come from, who is sending them, and whether they are safe**.

Packet filtering firewalls are **generally installed at junctions within network environments**. They may operate alongside switches and routers, processing traffic at high-volume locations. This enables packet-filtering firewalls to handle traffic for an entire network.

Advantages of packet-filtering firewalls:

- Low data requirements make them relatively fast and efficient.
- Can cover the whole network with ease.
- Affordable to install and maintain.
- Low data overheads, minimal impact on network performance.

Disadvantages of packet filtering firewalls:

- PFIs do not catch all security threats and only analyzes limited amounts of information. Payload spoofing can compromise firewall protection.
- Managing access control ledgers can be problematic.

2. Circuit-level gateways

Circuit level gateways operate at the session level. They **assess traffic when local and remote hosts establish a connection**. If this connection is deemed insecure, circuit level gateways will close and prevent communication between the two devices. Circuit level gateways use session information such as TCP handshaking and protocol messaging. By leveraging this information, the circuit level gateway can establish whether sessions are legitimate. There is no data packet inspection. Everything relates to the way connections are created.

Advantages of circuit level gateways:

- They are affordable to implement and have little impact on network performance.
- Simple to manage and calibrate.
- Provide strong protection against unauthenticated access requests. Limits access to legitimate devices.

Disadvantages of circuit level gateways:

- Minimal protection against data leakage. The firewall acts at the session layer, not the application layer. It only inspects information about identity, not the content of packets.
- Must be regularly patched to keep pace with changing identification rules.

These negatives mean that **circuit level gateways usually function alongside application-level filters**.

3. Stateful inspection firewalls

Stateful inspection firewalls add another level of sophistication to firewall protection. Standard firewalls are stateless. They make decisions based on inputs, with no further requests for information.

Stateful firewalls take inputs and interrogate them. They leverage data from all network layers to establish context. Information about past connections is stored and mobilized to analyze future access requests.

Contextual and historical information enables stateful firewalls to make informed decisions. In general, this results in **more comprehensive threat protection in complex network environments**.

Advantages of using stateful inspection firewalls:

- Combine contextual data with packet inspection and IP checking. This delivers robust security compared with other firewall variants.
- Users can collect data logs to use in threat analysis.
- Users enjoy extended control over network traffic with more options to customize their firewall settings.

Disadvantages of stateful inspection firewalls:

- High data requirements. Stateful inspection firewalls can compromise network speeds due to resource overheads.
- Expensive to implement and complex to maintain.

4. Proxy firewalls

Also known as web application or application layer firewalls, **proxy firewalls route data packets through separate proxy servers**.

Proxy servers act as a network gateway between remote devices and web applications. Proxy firewalls screen incoming and outgoing traffic, blocking direct access to web servers without proper authentication.

Proxy firewalls operate at the application layer. They filter by destination port, but also assess data packets using application data. For instance, the firewall may check HTTP request strings to determine whether connections are legitimate.

Operating at the application layer allows security teams to apply controls over web usage. Admins can block access to content according to HTTP addresses. Granular controls also allow access to certain web resources while blocking insecure websites.

Advantages of proxy firewalls:

- Proxy firewalls provide robust security by applying application-level filtering. Security teams can leverage port information, TCP headers and also packet contents.
- Application layer firewalls can act as web filters. Security teams can place risky web resources off limits to users.

Disadvantages of proxy firewalls:

- Proxies tend to have high data overheads. This may result in impaired network performance.
- Security teams may face higher workloads to maintain appropriate filters.
- Compatibility issues may arise with web apps and protocols.
  Application layer or proxy firewalls are **well-suited to protecting services that are vulnerable to web threats**. For example, they provide extra protection against phishing attacks via malicious links.

5. Next-generation firewalls

Next-generation firewalls (NGFWs) build on other firewall types and add extra functionality. **Generally, an NGFW will blend packet inspection with the contextual controls offered by stateful firewalls**.

NGFW services offer deep security controls to protect sensitive data. **Deep Packet Inspection (DPI)** analyzes the content of data packets, not just header information. This extra knowledge allows the firewall to verify the authenticity of HTTP transfers. The result is improved web security.

Anti-malware and antivirus scanning extend protection further. NGFWs also commonly include intrusion prevention and detection systems (IDS/IPS). Intrusion prevention services detect possible threats and deliver alerts before attacks become critical.

Advantages of next generation firewalls:

- In-depth threat protection against malware and viruses. Traffic passes multiple filters before reaching network devices.
- Delivery of deep security insights to inform threat mitigation strategies.
- Contextual analysis adapts to emerging threats. Next generation firewalls often detect threats that other firewalls cannot.

Disadvantages of next generation firewalls:

- NGFW systems have higher setup and maintenance costs than alternative firewall varieties.
- Users may need to integrate NGFW systems with SIEM technology and access controls to maximize their effectiveness.

Generally, **next generation firewalls provide the highest and most flexible level of network security**. They meet strict regulatory rules in sensitive business sectors where protecting sensitive data is absolutely critical. And these types of firewalls integrate with cloud environments to secure complex threat surfaces.

Firewall architecture

The types of firewalls listed above must fit into network architecture if they are to deliver maximum benefit. There are several ways to visualize this task. Here are the main firewall architecture models to consider.

Dual-homed host architecture

Dual-homed architecture is **constructed around host devices with two or more network connections**. These devices route traffic between different networks. These **networks cannot communicate directly**. The firewall intervenes, accepting IP packets from one network before transmitting them to the other.
Dual-homed hosts screen traffic and virtually exclude external traffic if required. They can apply packet filtering or deeper inspection systems to assess data security.
However, users must connect to dual-homed hosts before accessing external resources. This can give rise to security issues based around user access. Dual-homed systems also employ proxies, which may not suit all network architecture.

Screened host architecture

Screened host technology resembles dual-homed architecture. But in this case, **firewall services are provided by screening routers**. These devices connect with "bastion hosts" on the internal network, which in turn connect to local devices.
The screening router employs packet filtering to assess network traffic. Traffic admitted to the network passes through the bastion. This device must be equipped with sufficient security controls to screen emails and file transfers and exclude malicious traffic.
Packet filtering allows the host to open internet connections on network devices. It can also divert risky connections through proxy hosts. This adds extra flexibility compared with dual-homed architecture.
Defending the screening router is easier than guarding dual-home hosts. The reliance on packet filtering also makes screened hosts faster in most situations. However, **the bastion host is vulnerable to external attacks** – a significant security weakness.

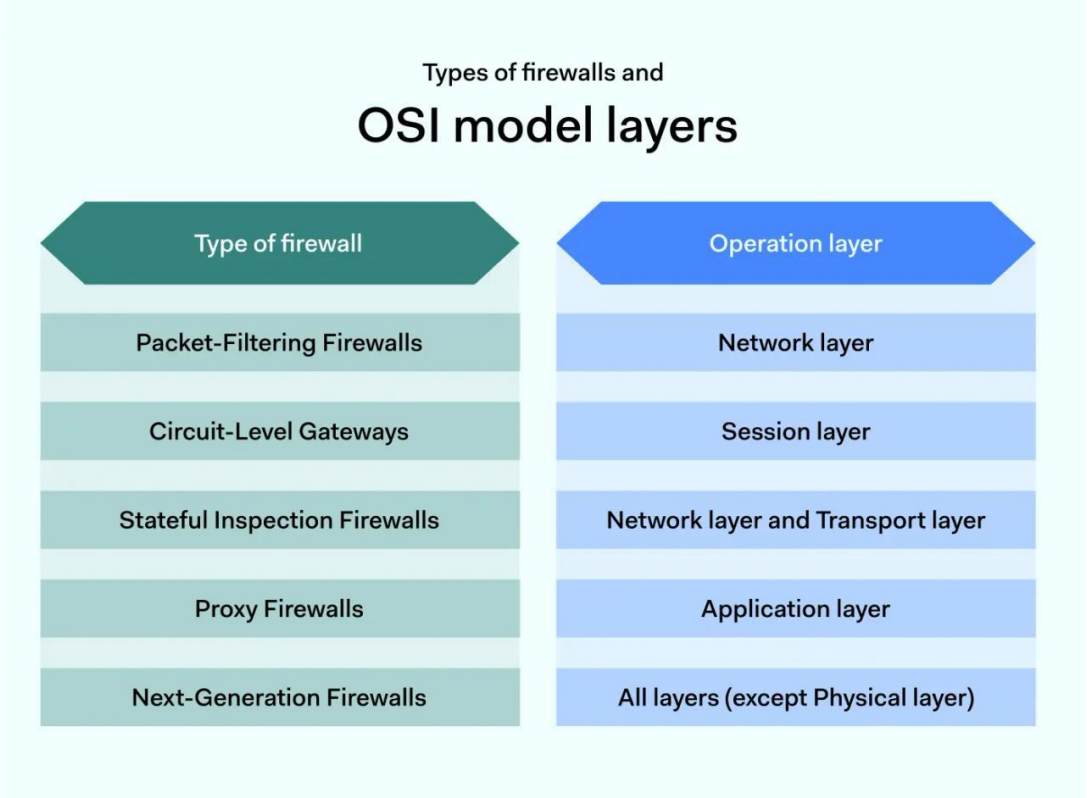
Screened subnet architecture

Screened subnet systems provide a solution to these security problems. This form of firewall architecture **creates an additional perimeter layer around the bastion host**. This makes movement within the network more difficult for cyber attackers.
The general idea behind screened subnets is simple. While screened host models have a single point of failure, **screened subnets have multiple protections**. This creates an "insurance policy", reducing the risk of security breaches.

Screened subnets generally use a router pair to provide host protection. One screening router lies between the internet and the bastion host. The other stands between the bastion and internal network devices.
Subnets can be more complex. For example, network managers can create perimeter nets around critical assets and apply loser protections to less important network nodes. **Subnets apply a form of network segmentation**, blocking east-west movement within the network.

Find the right firewall type for your network

Firewall architecture is a core security challenge for all modern businesses. Every company must secure their network perimeter and lock down confidential data. But **there are many options to think about when choosing between the various types of firewalls**.



Cloud-based firewalls suit companies reliant on SaaS apps and off-premises infrastructure. Hardware and software firewalls are a good fit for organizations with extensive on-premises assets. And hybrid products provide a mix of cloud and local perimeter protection.

Companies handling health or financial data can maximize data security with next generation firewall technology. Lightweight packet filtering or circuit level alternatives will suit those in less demanding regulatory environments.
Assess your needs and find the right firewall setup. And build firewalls into networks with dual-homed, screened host or subnet architecture. The result will be robust edge protection and reliable network security.