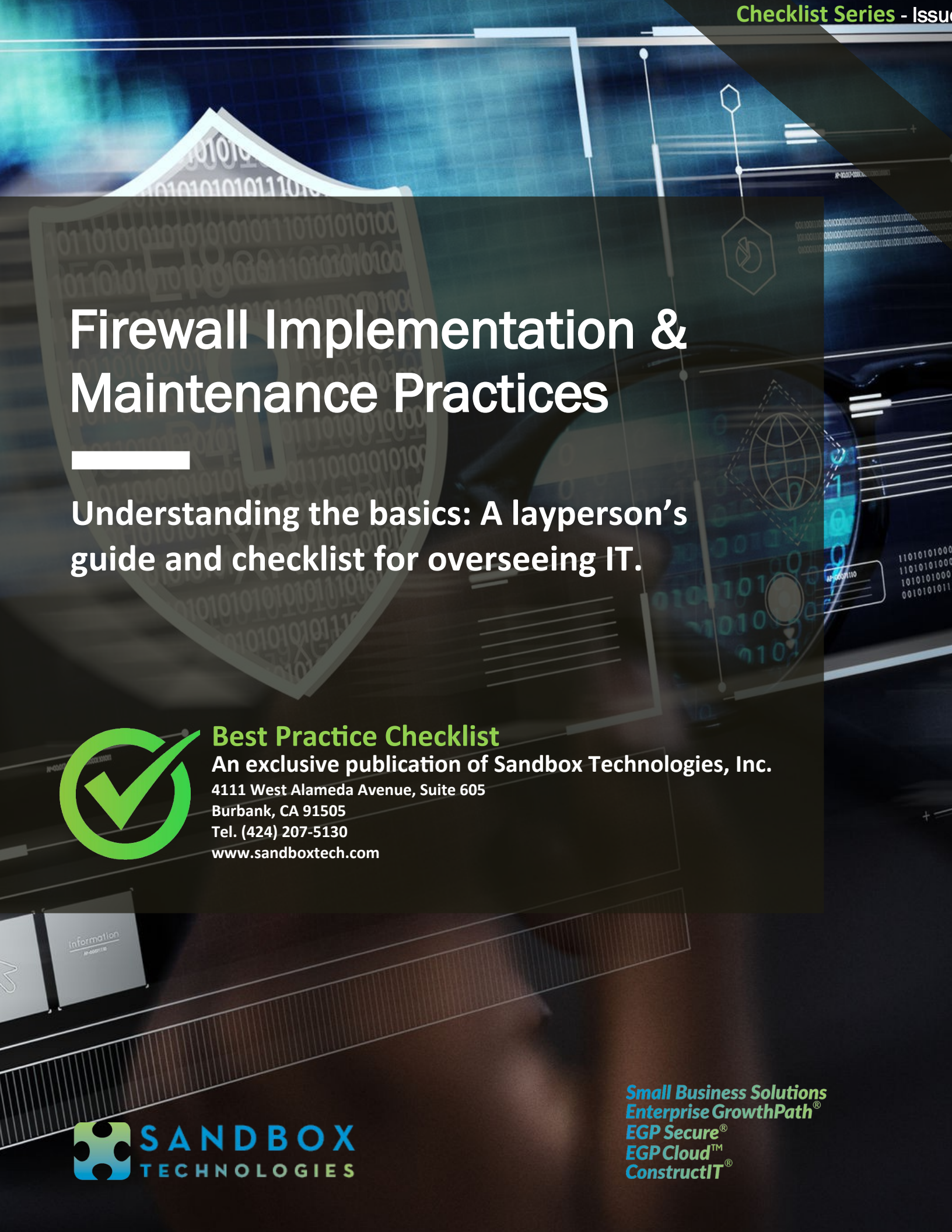


Firewall Implementation & Maintenance Practices

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist
An exclusive publication of Sandbox Technologies, Inc.
4111 West Alameda Avenue, Suite 605
Burbank, CA 91505
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Table of Contents

Firewall and Perimeter Security 3
Where it quietly fails 4
- The Router That Called Itself a Firewall 4
- The VPN Account Nobody Closed 4
- The Traffic No One Could See 4
- Firmware Years Behind 4
- One Flat Network 4
- The common thread 4

What to Ask Your IT Manager or Provider 6
- Business-Class Firewall 6
- Physical Security, Power and Cooling 6
- Active Warranty and Support 6
- Strong, Unique Administrative Credentials 7
- Separate Admin Accounts and an Audit Trail 7
- Multifactor Authentication on All Access 7
- No Public Administrative Interface 7

Perimeter Protections and Inspection 8
- Close Unneeded Ports, Protocols and Services 8
- Gateway Antivirus 8
- Intrusion Prevention (IPS) 8
- Web Content Filtering 9
- TLS/SSL Traffic Inspection 9
- Geographic (Geo-IP) Restrictions 9
- DoS/DDoS Protection and Connection Limits 9
- Network Segmentation (Wi-Fi and Corporate) 10

Resilience and Purpose-Specific Measures 10
- Multiple WAN Connections 10
- High Availability (Failover Pair) 10
- Layered Firewalls and Compliance Segmentation 11

Recommended Maintenance Practices 11
- Firmware and Security Updates 11
- Backed-Up Configuration 11
- Log Review 12
- Account, Rule and Service Audits 12

Terminology 12
- Next-Generation Firewall (NGFW) 12
- Stateful Inspection vs. Intrusion Prevention (IPS) 12
- Gateway Antivirus 12
- TLS/SSL Inspection 13
- VPN (Virtual Private Network) 13
- DMZ and Layered Firewalls 13
- High Availability and Multiple WAN 13
- A note on passwords 13

© 2026 Sandbox Technologies, Inc.

Firewall and Perimeter Security

A firewall you install and forget is a firewall that quietly stops protecting you

Almost every organization has a firewall. Far fewer can say what it is actually configured to do. The protection does not live in the box, it lives in dozens of settings and in the upkeep behind them, and only the business owner is truly positioned to decide which trade-offs are acceptable. The situations below show what tends to go wrong when those decisions are left to a default.

© 2026 Sandbox Technologies, Inc.

Where it quietly fails

No firewall configuration removes every risk, and that is normal. Every environment trades some functionality for security, and for many organizations a measure of exposure is an acceptable business decision. The point is not to alarm. It is to make sure each trade was chosen on purpose rather than left unset.

The Router That Called Itself a Firewall

A small office runs an off-the-shelf router that advertises firewall features. Gateway antivirus, intrusion prevention, and content filtering are either absent or switched off. A routine drive-by infection reaches a workstation through traffic the device never inspected.

The VPN Account Nobody Closed

A vendor was granted VPN access for a project two years ago. The account was never disabled, its password predates the move to multifactor authentication, and it never expired. An attacker reaches it through reused credentials and arrives inside the local network.

The Traffic No One Could See

Most web traffic is now encrypted. With encrypted-traffic inspection turned off, the firewall passes it through without reading it. Malware arrives over an encrypted connection, past antivirus and intrusion prevention alike, because none of them could see inside it.

Firmware Years Behind

No one was assigned to firewall updates. A vulnerability in the firewall's own remote-access service is disclosed and patched by the manufacturer. Months later it is exploited on an appliance still running the old firmware.

One Flat Network

Guest Wi-Fi, staff laptops, and the servers all share a single flat network. A visitor's compromised laptop joins with the guest password and finds an unobstructed path to the file server holding accounting and client records.

The common thread

None of these required a sophisticated adversary or a larger budget. In each case the firewall was purchased and then left alone: default settings never hardened, protective services never enabled, updates never applied, old access never reviewed. The exposure was in the upkeep, not the hardware.

A firewall is not a product you install once. It is a configuration you maintain. Nearly every failure above was a decision that was never made, or a task that belonged to no one. That is what the checklist below is designed to surface.

© 2026 Sandbox Technologies, Inc.

© 2026 Sandbox Technologies, Inc.

What to Ask Your IT Manager or Provider

and how to know if the answers are good ones

You do not need to administer a firewall to oversee one. You need to know what to ask. A short primer on the terminology is provided at the end, for those who want it. First, the part that matters: run the checklist below with your IT professional. If any item is not marked green, it may warrant a closer look. Some items are foundational; others are optional and depend on your environment and risk tolerance.

Business-Class Firewall

Is the perimeter protected by a business-class firewall, not a consumer router that merely advertises firewall features? Business-class firewalls, often called next-generation firewalls (NGFWs), provide higher throughput for local and VPN users and can run modern security services such as antivirus, intrusion prevention, and content filtering at usable speeds. A consumer router generally cannot.

Compliant	NOTES:
Needs Attention	
N/A	

Physical Security, Power and Cooling

Is the firewall kept in a secure location with adequate ventilation and clean power? A firewall is a single point of network failure, so physical tampering, theft, or an avoidable heat-related failure can take the whole network offline. Restricting physical access also guards against alteration by a disgruntled insider.

Compliant	NOTES:
Needs Attention	
N/A	

Active Warranty and Support

Is the firewall covered by an active manufacturer warranty and support agreement, ideally with 24/7 coverage? Firewalls fail and require security updates. Lapsed coverage can leave an organization without replacement hardware or critical patches at the moment it needs them most.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Strong, Unique Administrative Credentials

Does the firewall use a long, unique administrative password that is not reused on any other device or service? Current guidance favors length over forced complexity, so a longer passphrase is preferred to a short string of mixed symbols. A password reused across devices lets a single compromise spread from one to the next.

Compliant	NOTES:
Needs Attention	
N/A	

Separate Admin Accounts and an Audit Trail

Does each administrator have their own login rather than a shared account, and does the organization retain its own administrative credentials independent of its IT provider? Shared logins make it difficult to attribute a configuration change or a breach to anyone. It is recommended that the business owner always hold administrative access, ideally alongside simple audit logging for later reference.

Compliant	NOTES:
Needs Attention	
N/A	

Multifactor Authentication on All Access

Is multifactor authentication (MFA) required for administrative access to the firewall and for every VPN user? MFA requires a second factor, such as a token or an authenticator application, in addition to a password, so a stolen password alone is not enough. Where supported, phishing-resistant methods are preferable to codes sent by text message or email.

Compliant	NOTES:
Needs Attention	
N/A	

No Public Administrative Interface

Is the firewall's administrative login closed to the public internet, reachable only after connecting through the VPN? Management interfaces exposed directly to the internet are a routine target for automated attacks. Requiring a VPN connection first removes that exposure while remaining convenient for administrators.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Perimeter Protections and Inspection

These are the services that decide what a firewall actually inspects and blocks. Availability varies by device and licensing, so it is worth confirming which are present, which are enabled, and which were deliberately left off.

Close Unneeded Ports, Protocols and Services

Have the required inbound ports, protocols, and services been documented, with everything else disabled, and is unnecessary outbound traffic restricted as well? A firewall's core job is to permit only what is needed. Limiting outbound traffic also helps stop malware already inside from reaching an outside attacker.

Compliant	NOTES:
Needs Attention	
N/A	

Gateway Antivirus

Is gateway (firewall-based) antivirus enabled to scan traffic at the network perimeter? It provides a first line of defense before threats reach a workstation. Without it, the organization depends entirely on each endpoint's own protection being present and current.

Compliant	NOTES:
Needs Attention	
N/A	

Intrusion Prevention (IPS)

Is an intrusion prevention service enabled? IPS inspects traffic for patterns matching known exploits, backdoors, trojans, worms, and spyware, and drops connections that match. It is especially valuable for protecting devices that cannot run their own antivirus, such as printers, network switches, and VoIP telephones. Intrusion prevention is a distinct, deeper layer than the basic stateful inspection every firewall performs; both are covered in the primer.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Web Content Filtering

Is web content filtering enabled for categories the business does not need? Categories such as adult content, file sharing, and some social media carry a higher risk of ad-based malware, phishing, and drive-by infection. Filtering reduces that exposure to the extent the firewall can identify the sites, and the categories restricted are a business decision.

Compliant	NOTES:
Needs Attention	
N/A	

TLS/SSL Traffic Inspection

Is encrypted-traffic inspection enabled, or has the decision to leave it off been made deliberately? Most web traffic is now encrypted with TLS (still widely called SSL), and a firewall cannot scan what it cannot decrypt, so attackers increasingly hide inside encrypted connections. Inspection does carry real planning and compatibility caveats, so it warrants a considered decision rather than a default. A fuller discussion is available at http://www.sandboxtech.com/ssl-inspection .

Compliant	NOTES:
Needs Attention	
N/A	

Geographic (Geo-IP) Restrictions

Does the firewall block direct connections from regions the organization neither travels to nor does business with? A large share of attack traffic originates abroad. Geo-IP filtering is usually simple to apply, blocks direct hacking attempts from those regions, and does not affect email communications.

Compliant	NOTES:
Needs Attention	
N/A	

DoS/DDoS Protection and Connection Limits

Are denial-of-service protections enabled and inbound connections capped? Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks try to overwhelm a network and disrupt communications. Limiting concurrent inbound connections and enabling the firewall's DoS and DDoS features where available helps blunt them.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Network Segmentation (Wi-Fi and Corporate)

Is wireless access segmented from the corporate network at the firewall? Wi-Fi is exposed to more attack vectors than a wired connection, which makes it less trustworthy. A common approach is to give wireless internet access only, granting access to internal resources solely through a VPN client on authorized laptops, phones, and similar devices.

Compliant	NOTES:
Needs Attention	
N/A	

Resilience and Purpose-Specific Measures

The following are optional and depend on how much downtime an organization can tolerate and what obligations it carries. Many organizations reasonably forgo them; others treat them as essential.

Multiple WAN Connections

Does the firewall use more than one internet connection, and has failover been tested? Multiple WAN links let a firewall spread traffic for better performance and fail over automatically if one provider goes down, reducing downtime. They should be tested with a connection offline to confirm failover actually works.

Compliant	NOTES:
Needs Attention	
N/A	

High Availability (Failover Pair)

For operations with little tolerance for downtime, is a second firewall configured as an automatic failover? In a high-availability pair, a standby firewall assumes the primary role if the primary fails, promoting greater uptime. Many organizations reasonably decline this on cost, but where downtime is expensive it can be a worthwhile investment.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Layered Firewalls and Compliance Segmentation

If the organization handles material subject to strict third-party or contractual controls, is a layered or segmented firewall design in place? Some environments, such as those producing content for the entertainment industry, must meet rigorous standards, today typically assessed through the Motion Picture Association's content-security program and the Trusted Partner Network, that can call for firewalls embedded one behind another. Sandbox Technologies offers configuration services to help organizations meet such requirements.

Compliant	NOTES:
Needs Attention	
N/A	

Recommended Maintenance Practices

For sustained security and performance, a firewall must be maintained, and maintenance is more than applying updates. It also includes backing up settings and periodically reviewing logs, rules, and accounts to catch attacks early and remove unnecessary exposure.

Firmware and Security Updates

Is someone responsible for reviewing and applying firmware updates on a regular schedule? Done properly, this means checking the installed version against the latest release, reviewing release notes for caveats, exporting the configuration first in case a rollback is needed, applying the update, and then confirming connectivity, services, and any VPN tunnels have recovered. Known vulnerabilities are frequently exploited long after a fix is available.

Compliant	NOTES:
Needs Attention	
N/A	

Backed-Up Configuration

Is the firewall configuration backed up, and captured again before and after any major change? Some firewalls save configurations automatically or in the cloud; others must be exported by hand. Either way, a saved configuration can turn hours of rebuilding into minutes after a failure or a bad change.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Log Review

Are firewall logs enabled and reviewed periodically? Logs can reveal attacks in progress and sometimes their point of origin, allowing protections to be tightened where appropriate. Logging is not always on by default, and for fuller retention and analysis the logs can be forwarded to a dedicated collector or SIEM.

Compliant	NOTES:
Needs Attention	
N/A	

Account, Rule and Service Audits

Are VPN accounts, port mappings, and firewall rules reviewed periodically, with stale ones removed? Legacy accounts for former staff and vendors, unused services, and outdated rules are easily overlooked. They may carry weak or non-expiring passwords that predate current security standards, and anything found should be reviewed with management and disabled or removed.

Compliant	NOTES:
Needs Attention	
N/A	

Terminology

Next-Generation Firewall (NGFW)

The current term for a business-class firewall that bundles deeper security services, such as antivirus, intrusion prevention, content filtering, and encrypted-traffic inspection, alongside basic traffic control. A consumer router that advertises a “firewall” generally offers only the basics.

Stateful Inspection vs. Intrusion Prevention (IPS)

Stateful inspection is a baseline function of essentially every modern firewall: it tracks the state of each connection and allows return traffic only for sessions the network started. Intrusion prevention (IPS) is a separate, deeper layer that examines the contents of traffic against signatures of known attacks and blocks matches. The two are often confused, but stateful inspection alone does not scan for exploits, backdoors, or malware; that is the work of IPS.

Gateway Antivirus

Virus and malware scanning performed at the firewall, at the edge of the network, before traffic reaches a workstation. It complements, rather than replaces, the antivirus running on each device.

© 2026 Sandbox Technologies, Inc.

TLS/SSL Inspection

Most web traffic is encrypted with TLS, a protocol still commonly called SSL after its predecessor. Because encrypted traffic is unreadable in transit, a firewall must decrypt and re-encrypt it to scan for threats. This is powerful but intrusive, and it requires planning to avoid breaking applications, so it is a deliberate decision rather than a simple switch.

VPN (Virtual Private Network)

An encrypted tunnel that lets an authorized remote user or device reach the internal network as if on site. Requiring a VPN, protected by multifactor authentication, is a common way to grant remote access without exposing internal systems directly to the internet.

DMZ and Layered Firewalls

A DMZ (demilitarized zone) is a segment positioned between the internet and the internal network, often between two firewalls, used to isolate systems that must be reachable from outside or to meet strict compliance controls. It limits how far an intruder can move if an exposed system is compromised.

High Availability and Multiple WAN

High availability pairs two firewalls so a standby takes over if the primary fails. Multiple WAN refers to more than one internet connection, allowing traffic to be balanced across links and to fail over if a provider goes down. The first protects against firewall failure; the second protects against internet failure.

A note on passwords

Current guidance now favors length over forced complexity: a longer passphrase is stronger and easier to use than a short string of mixed character types, and routine scheduled password changes are discouraged in favor of changing a password when there is reason to believe it has been exposed. Length, uniqueness per device, and multifactor authentication carry more weight than composition rules.

© 2026 Sandbox Technologies, Inc.

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2026 Sandbox Technologies, Inc.