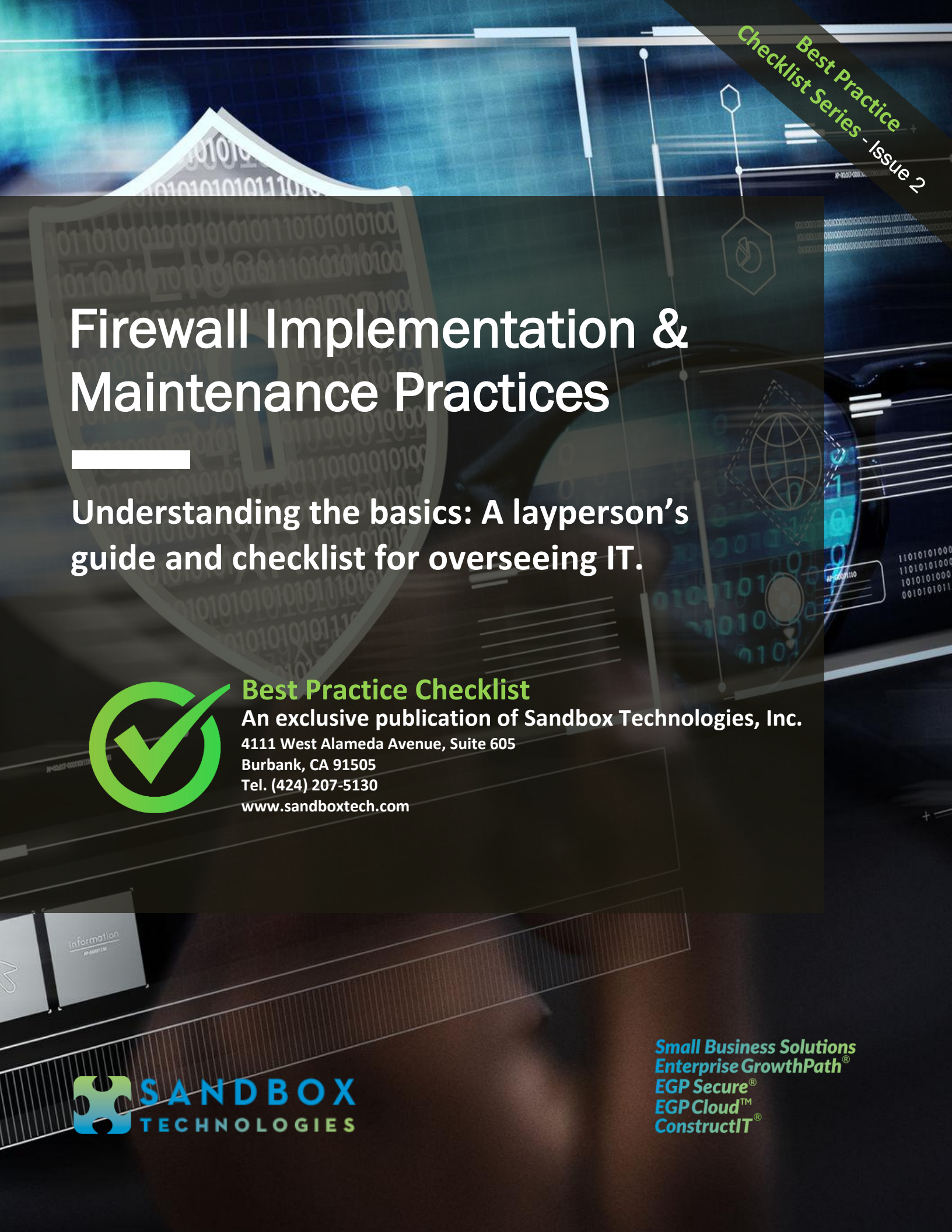

Best Practice Checklist Series - Issue 2

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®

Firewall Implementation and Maintenance Practices

It is widely understood that firewalls are essential to an organization's security. Unfortunately, the level of involvement by management often stops there, trusting that their IT provider has implemented a configuration consistent with the firm's priorities and risk tolerance.

While it's important to trust your IT provider, the simple fact is that no two environments are identical, and some measures require trade-offs in functionality, such that only the business owner is truly equipped to make a viable and accurate determination of what risks are and are not acceptable.

The purpose of this guide is to empower non-technical personnel by providing a brief overview of key firewall configurations, basic maintenance practices and what they mean. Consider it a brief primer for the terminology you'll need to understand common firewall functions and configuration settings, and why they may or may not be important to your particular environment.

At a time when threats to information security are at an all time high, the importance of asking the right questions and ensuring you're receiving optimal protection has never been more important.

As always, should you wish to discuss your current firewall settings and protections, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

Table of Contents

Recommended Implementation Practices - Basic

Storage and Cooling

At the most basic level, it is important that firewalls be deployed in a secure location with proper ventilation/cooling. Firewalls represent a key network failure point, so theft or alteration by a disgruntled employee, or an otherwise avoidable equipment failure due to the inadequate flow of cool air should be avoided.

Status ☐ ✔ ☐ – ☐ ?   NOTES ______________________________

Deploy Business Class Hardware

Many "off the shelf" routers advertise firewall features. As the first lines of defense for a network environment, it is important to have a suitable, business class firewall. Generally speaking, business class firewalls provide faster throughput for local and VPN users, better security, and the ability to perform more security functions at higher speeds.

Status ☐ ✔ ☐ – ☐ ?   NOTES ______________________________

Manufacturer's Warranty & Support

Like any other technical device, firewalls sometimes experience failures or technical difficulties. It is recommended that businesses maintain actively supported equipment that is covered by a 24/7 warranty to ensure critical updates and support are available when needed.

Status ☐ ✔ ☐ – ☐ ?   NOTES ______________________________

Set Password Complexity & Minimum Length Requirements

This simple practice should go without saying, yet it is commonly overlooked or ignored for convenience. Password complexity is the practice of requiring that different types of characters be used in the creation of passwords, such as the include the mandatory use of upper and lowercase letters, numeric digits, and special characters. A minimum password length of 14 characters is recommended.

Status ☐ ✔ ☐ – ☐ ?   NOTES ______________________________

Require Use of Discrete Passwords and Update Passwords Periodically

Many any organizations engage in the dangerous practice of utilizing the same administrative password for multiple network devices or cloud services to simplify administration. When the same password is used for multiple devices, a malicious actor who compromises a device's password can potentially gain access to other devices using that same password, resulting in deeper and deeper penetration into the network. Firewalls should have their own unique passwords and be changed periodically.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Avoid Sharing Administrative Passwords

Sharing of administrative credentials between trusted users may be convenient, however it can severely impair forensic efforts in the event of a breach or make it difficult to identify responsible parties when unwanted or improper configuration changes are made. Business owners should always have administrative passwords in their possession, so it is recommended that organizations maintain a policy of keeping separate administrative passwords for their IT professional or provider, and for themselves. Optimally, this should be done in conjunction with the implementation of simple audit utilities for ease of reference to historical activity should the need arise.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Require Multifactor Authentication for All Access

Before access is granted, multifactor authentication requires entry of a code generated by a device such as a token or a mobile device application in addition to a password. Multifactor authentication should be required for administrative access to the firewall, as well as for users to access the network via various types of VPN (Virtual Private Networking) services.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Disable Public Administrative Interfaces

Most firewalls provide the ability for administrative personnel to connect to them via a publicly accessible interface. While convenient, and typically quite secure, it is recommended that this feature be disabled, and administrators required to connect to the network via VPN before access to the firewall login interface will be granted.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Close Non-Essential Firewall Ports and Disable Unneeded Protocols and Services

The key role of a firewall is to limit inbound communication to only those ports that are necessary. While often overlooked, an administrator should inspect and document those ports, protocols and services that are required and disable all others. Similarly, unnecessary outbound traffic should be limited to help prevent malicious software from making connections to remote attackers.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Activate Antivirus Protection

Firewall-based antivirus (also sometimes known as "Gateway Antivirus") typically represents the first line of defense by scanning for viruses and malware at the perimeter of a network. Without firewall-level virus scanning, the mitigation of infections relies largely on client workstation protections being active and up to date with the latest virus definitions. Firewall-based virus inspection is highly recommended for optimal protection against threats.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Activate Stateful Packet Inspection

Also referred to as IPS (Intrusion Prevention Service) by some device manufacturers, stateful packet inspection scans for the attempted use of exploits, backdoors, trojans, worms and spyware. It works by inspecting traffic for activity that matches signatures of known attacks and terminating connections in the event of a match. Stateful Packet Inspection is an essential protection, and is particularly helpful in preventing permitted traffic from being used to exploit devices that do not employ antivirus, such as printers, network switches, VoIP telephones, etc.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Activate Web Content Filtering

Access to pornography, shopping, file sharing, and social media websites carries a substantial risk of exposure to ad-based malware, online phishing attacks and drive-by infections. Web content filtering permits an organization to selectively disallow access to such sites to the extent the organization's firewall is capable of identifying them. To the extent that access to certain website categories is not required for business purposes, restriction of those categories is recommended.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

SANDBOX TECHNOLOGIES

Restrict Direct Access by Geographic Regions

As many malicious actors originate their attacks from foreign nations that business executives neither travel to, nor engage in commerce with, Geographic Region-based IP filtering is a simple and useful way to prevent direct communications from those locations, helping to mitigate the threat from direct hacking attempts. This protective measure is typically easy to implement and does not affect email communications.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Enable Available DOS or DDOS Protections and Limit Inbound Connections

"DOS" and "DDOS" refer to "Denial of Service" and "Distributed Denial of Service", types of attacks through which malicious actors seek to disrupt communications. To help protect against these types of attacks, firewalls should be configured to limit the number of concurrent inbound connections allowed, and when available, DOS and/or DDOS protection should be enabled.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Activate SSL Traffic Inspection

To secure communications between users and websites, many sites employ the use of what is known as SSL encryption. An unfortunate drawback to this otherwise beneficial technology, is that without SSL Traffic Inspection enabled, an organization's firewall is unable to inspect encrypted communications for malware and other threats. Knowing this, malicious actors seek to bypass firewall protections by exploiting encrypted connections. (It should be noted that SSL inspection comes with caveats that require significant planning and preparation to implement smoothly.) For more information, visit www.sandboxtech.com/ssl-inspection .

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Employ Perimeter Firewall Protection to Segment Wi-Fi Access and Corporate Network

Wi-Fi networks are susceptible to numerous attack vectors, making them less secure than hardwired connections. For this reason, wireless networks should provide Internet access only, permitting access to LAN resources only when used in conjunction with a suitable VPN client on authorized mobile devices, laptops, and the like.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

SANDBOX TECHNOLOGIES

Employ Multiple WAN Connections

Multiple WAN connections is a technical way of saying that an organization subscribes to more than one Internet connection. When properly configured, multiple WAN connections can enable a firewall to spread traffic over multiple connections for better performance and fail over to secondary or tertiary WAN connections in the event of an Internet Service Provider failure, mitigating downtime and lost productivity. When multiple WAN connections are employed, they should be tested to confirm proper function when one or more Internet connections are offline.

Status ☐ ☐ ☐

NOTES _____

_____

_____

Recommended Implementation Practices - Optional & Purpose-Specific

High Availability Configurations

High availability is a hardware configuration in which two firewalls are installed and work as a failover pair. The firewalls communicate with each other, and in the event that the primary firewall fails, the secondary firewall automatically assumes the role of the primary. Such a configuration promotes greater Internet uptime in the event of a firewall equipment failure. Many organizations choose to forego high availability configurations due to cost, however for companies with minimal tolerance for downtime, may find one a worthwhile investment.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Secondary DMZ

Businesses requiring an extra high level of security protection often deploy multiple firewalls, effectively embedded one behind another. This is a common practice engaged in by organizations that are engaged in the editing or development of creative content for the entertainment industry. Subject to highly restrictive guidelines imposed by third parties, such as the MPAA (Motion Picture Association of America), such companies follow rigorous standards to protect digital assets from falling into the wrong hands. For entities subject to these and similar audit requirements, Sandbox Technologies offers configuration services to assist organizations in meeting compliance requirements.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Recommended Maintenance Practices

For optimal security and performance, it is essential that firewalls be maintained regularly.

When many people think of maintenance, the first thing that comes to mind is the deployment of updates. The optimal maintenance routine encompasses much more, such as exporting or backing up settings, and conducting periodic reviews of logs and configurations to identify potential attacks and minimize unnecessary threat vectors.

The following are basic firewall maintenance items that are recommended:

Update Firmware

Firmware updates entail checking the most recent firmware release for the firewall against the current firmware installed, briefly reviewing the new release for any known caveats that may adversely impact the environment, exporting existing firewall configuration settings should the need to roll-back arise, downloading the new firmware version (or versions if the device has fallen behind on several), installing the new releases, re-booting the appliance, testing connectivity, confirming services have re-started, and spot-checking hardware VPN connections (if applicable) to confirm successful re-connection.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Export or Create Backup of Configuration Settings

The method of approach for this task can vary widely from one type of firewall to another. Some firewalls may be cloud-based or configurable to automatically maintain a copy of configuration settings. Others require settings to be exported manually. Whatever the case may be, creating a copy of configuration settings before and after performing upgrades or making major changes can save hours of lost time in the event of a problem.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

Review Log Data

A periodic review of firewall logs can help to identify possible attacks, and sometimes even reveal their place of origin. The heightened awareness that results enables security to be further tightened in various areas if deemed appropriate. In some cases, logging is not active by default and must be enabled. Log data collected can vary significantly from one firewall to another. For optimal logging, third-party log data collectors can be employed.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____

SANDBOX TECHNOLOGIES

Review/Audit User Accounts and Services

Inspect, or minimally, spot-check user VPN accounts, port mappings and firewall rules to identify settings that may no longer be necessary. Legacy accounts relating to former users, unused services, and inactive vendors are often overlooked, and can pose a security risk. Ex-employees and former vendors may be in possession of access credentials, and unused credentials may predate stricter security measures, leaving them with weak or non-expiring passwords that could be breached by malicious parties. Any such findings should be discussed with management and disabled and/or removed.

Status ☐ ✓ ☐ – ☐ ?

NOTES _____

_____

_____