TWE SOLUTIONS

FIVE COMMON FIREWALL MANAGEMENT MISTAKES

Don't Let the Very Thing That Should Protect Your Business Become A Vulnerability

Congratulations! You've just taken the critical step of implementing a industry leading Next Generation Firewall to protect your business. However, securing a network isn't just about purchasing the best tools—it's about using them effectively. Hackers often count on companies mismanaging firewalls, leaving them vulnerable to attacks. In fact, studies indicate that misconfigured firewalls and outdated software account for a significant percentage of breaches. By addressing common gaps in firewall management, you can prevent costly exposure and safeguard your organization's data and reputation.

68% of organizations experienced targeted endpoint attacks that compromised their data or IT infrastructure, even with firewalls in place.[1]

1 Most Common Mistake
Delaying or Ignoring Software Updates

Why it matters: Outdated firewalls are a prime target for hackers who exploit known vulnerabilities.

How to fix it: Set up an automated update schedule or ensure manual updates are part of your regular IT process.

2 Most Common Mistake
Overly Permissive or Incorrect Rules

Why it matters: Poorly configured rules create openings for unauthorized access, exposing sensitive systems.

How to fix it: Conduct regular rule audits to ensure only necessary access is permitted and review configurations for accuracy.

3 Most Common Mistake
Leaving Unused Ports and Services Open

Why it matters: Open but inactive ports act as gateways for attackers.

How to fix it: Periodically review and disable unnecessary ports and services to close off these potential vulnerabilities.

Cybersecurity Fact

The three factors most likely to increase the cost of a data breach are:[2]
- Security skills shortage
- Security system complexity
- Noncompliance with regulations

Firewall Management Mistakes

2 Overly permissive or incorrect rules

3 Leaving unused ports and services open.

1 Delaying or ignoring software updates

4 Weak access controls

5 Lack of active monitoring.

4 Most Common Mistake
Weak Access Controls

Why it matters: Weak passwords or single-factor authentication makes it easy for attackers to gain control of your firewall.

How to fix it: Require strong, unique passwords and enforce multi-factor authentication for all firewall administrators.

5 Most Common Mistake
Lack of Active Monitoring

Why it matters: Without constant oversight, suspicious activity can go unnoticed until it's too late.

How to fix it: Use real-time monitoring tools that leverage machine learning to quickly detect and respond to unusual behavior on your network.

Cybersecurity Fact

The three factors[2] most likely to decrease the cost of a data breach are:

- DevSecOps approach
- IR planning and testing
- Employee training

TWE is the Leader in Management for Palo Alto Networks Firewalls

TWE Solutions specializes in keeping businesses secure with expertly managed firewall services. Our certified engineers combine industry-leading expertise with a co-managed approach, working seamlessly with your in-house team to fortify your defenses.

Free Best Practices Assessment

Schedule a Best Practices Assessment with TWE today, and let us identify ways to strengthen your firewall management while minimizing your exposure to cyber threats.

By addressing these key challenges with the right expertise, your business can turn its firewall into an effective barrier against even the most sophisticated attack.

TWE BPA Assessment

The TWE Best Practices Assessment (BPA) is a comprehensive assessment of your firewall's security, performance, and configuration. The BPA includes:
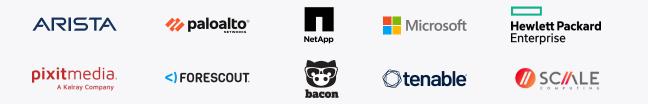
- Configuration review and gap analysis
- Security policy alignment with industry standards
- Threat and vulnerability analysis
- Performance optimization recommendations
- Rule and subscription evaluation
- Compliance readiness check
- Actionable steps to enhance protection and efficiency

[1]Security Boulevard, 2023
[2]Cost of a Data Breach, IBM, 2024

Contact us now to learn more or schedule your best practices assessment.

twe-solutions.com/contact-us
+1.888.535.9370

OUR PARTNERS

ARISTA   paloalto NETWORKS   NetApp   Microsoft   Hewlett Packard Enterprise

pixitmedia A Kalray Company   FORESCOUT   bacon   tenable   SCALE COMPUTING

About TWE Solutions   **twe-solutions.com**

TWE Solutions is the only IT partner that combines a security-first approach with co-managed technology services, seamlessly integrating with your staff to manage infrastructure, firewalls, cloud systems, and endpoints. With highly certified, U.S.-based engineers, TWE brings unmatched expertise to secure your technology and streamline operations, keeping your business efficient, scalable, and compliant.