SIX THINGS YOU NEED TO KNOW ABOUT FIREWALLS

To combat hackers aiming to steal data, businesses of all sizes and types work with security experts to deploy firewalls to secure their networks. Managed firewalls provided by qualified managed service providers (MSPs) give companies the ongoing management and coverage they need for 24/7/365 protection of their company.

1 Firewalls Are the First Line of Defense for Your Network

A firewall is a network security device that prevents unauthorized access by inspecting traffic on a network using security rules to block cyberthreats seeking access to the organization. The firewall is the first layer of protection from Internet-based threats. It's analogous to a guard who protects your house (data) so no one steals from (hacks) you.

2 Different Types of Network Firewall Solutions

Your business has an array of network firewall solutions to choose from, including:

Software Firewalls

A software-based firewall runs on a server or other device and must be installed on each device requiring protection.

Hardware Firewalls

A hardware-based firewall is an appliance that acts as a secure gateway between devices inside the network perimeter and those outside.

Stateless Firewalls

Stateless firewalls use a data packet's source, destination and other parameters to determine if the data presents a threat and blocks it.

Stateful Firewalls

Stateful firewalls make state-aware devices examine packets and keep track of whether they're part of an established protocol or session, or whether they're a threat.

Next-Generation Firewalls

Next-generation firewalls use tech such as deep packet inspection, intrusion prevention and app awareness to block threats more effectively than traditional firewalls.

Unified Threat Management Firewalls

A unified threat management firewall is a comprehensive software solution that combines security features into a single unified system simplifying management of security solutions.

3 The Benefits of Hiring an MSP to Manage Your Firewalls

Proper configuration and updating is critical as even advanced firewalls can be ineffective if not configured, updated or patched correctly. Once deployed, they must be monitored and managed to ensure effective operation and detect cyberthreats. Managed Firewalls are more than security and provide:

24/7/365 Security

Adopting a managed firewall service ensures the traffic in and out of your network is monitored nonstop by the MSP, so your business is protected even when your own staff is out.

IT Cost Savings

A managed solution means that all firewall maintenance, patch management and updates are taken care of by the MSP, so your in-house IT resources can be assigned to revenue-generating tasks, instead of putting out fires.

Comprehensive Coverage

A high-quality MSP will deliver comprehensive coverage in the firewall offering, including virus and malware prevention, IDS, IPS, vulnerability scanning and web filtering with configuration and optimization from knowledgeable experts.

4 Managing Firewalls In-House Costs $695,000 or More Annually

The average costs to manage network firewalls 24/7/365 in-house include:

NEED	COST
Security information and event management (SIEM) firewall license	$40,000 per year
Five Security Analysts	$435,000 per year
One Senior Security Analyst Manager	$110,000 per year
One Correlations Rule Engineer	$110,000 per year

5 Businesses Should Partner with an MSP

Consider partnering with an MSP if:

- You need specialized expertise in cybersecurity
- Your IT team is stretched too thin
- You want your IT team to focus on other tasks
- You need a cost-effective way to manage your network firewalls

6 Consider TPx for Managed Firewalls

Businesses like to choose TPx to manage their firewalls because:

Regulatory Compliance

TPx complies with industry standards and regulations, including HIPAA and PCI DSS

Health Monitoring

TPx provides 24/7 health monitoring and troubleshooting from seasoned security professionals

Customized Configuration

TPx offers customized device configuration and tuning

Patch Management

TPx takes care of firewall updates and patch management

Log Reporting

TPx is responsible for firewall log retention and reporting

Licensing, Backup & Storage

TPx handles firewall licensing, hardware assurance, configuration backup and storage

Your business has enough challenges. Partner with an MSP like TPx that offers firewall solutions to give your business the data security and management you need so your IT team can focus on revenue-producing business goals.

Learn More About Firewalls in TPx's Guide.

DOWNLOAD NOW

TPX
www.tpx.com