



A Comprehensive Guide to Firewalls

FROM THE MANAGED SERVICES EXPERTS AT TPX



Executive Summary

As the volume of digital assets grows and cyber threats intensify, companies of all types are working with security experts to deploy firewalls as a frontline defense to protect their business data. However, the relentless world of cyber threats requires more than a static firewall security system. Businesses need an agile and adaptive approach. Managed firewalls, offered by qualified MSPs, provide continuous 24/7/365 protection, and dynamically adapt to the ever-evolving threat landscape.

This guide introduces firewalls and how they can help businesses protect their network and assets from cyberattacks.

Key Takeaways

- Firewalls are an organization's first line of defense against cyberattacks.
- The costs to manage an in-house firewall 24/7 can reach upwards of \$695,000 per year or more.
- Firewall management is complex and requires technical security expertise for deployment, configuration, patch management and ongoing monitoring.
- Outsourcing firewall management can give businesses instant access to expertise and quicker time to value without adding overhead.

Table of Contents

Part 1: What is a Firewall?

- What is a Firewall?
- What is a Managed Firewall?
- How Do Firewalls Work?

Part 2: What Are Network Firewall Solutions?

- What Are the Types of Network Firewall Solutions?
- Next-gen Firewall (NGFW)
- Unified Threat Management (UTM) Firewall
- Firewall vs Antivirus

Part 3: Why Should Businesses Invest in a Firewall Solution?

- What Challenges Do Firewall Solutions Solve?
- What Are Real-World Stats on Needing a Firewall Solution?
- What Challenges Do Firewall Solutions Not Solve?
- Why Do Small to Medium Businesses (SMBs) Need to Invest in Firewalls?

Part 4: How Can Businesses Choose the Right Firewall Solution?

- What Are Key Considerations in Firewall Selection?
- What Are Common Mistakes Made When Selecting Firewalls?

Part 5: Should Businesses In-source or Outsource Firewall Management?

- In-house vs. Outsourced
- What Are the Benefits of a Managed Firewall?
- How Do Managed Firewall & Managed Detection & Response (MDR) Work Together?
- Firewall as Part of a Cybersecurity Protection Plan

Part 6: What Should Businesses Look for in a Managed Service Provider (MSP) Delivering a Managed Firewall Solution?

- What Capabilities Should Your MSP Deliver?
- What Are Common Firewall Management Issues MSPs Need to Address?
- How to Make the Most Out of Your MSP Relationship

Part 7: Why Should Businesses Choose TPx?

- What is TPx's Managed Firewall Solution?
- Why Use TPx for Managed Firewall?

PART 1

What is a Firewall?

A firewall is a network security device that prevents unauthorized access to a network. Firewalls inspect both inbound and outbound traffic on an organization's network using pre-determined security rules to identify and block potential cyberthreats seeking access to the organization's network.

Firewalls can take multiple forms, including:

- Physical Hardware
- Digital Software
- Software-as-a-Service (SaaS)
- Virtual Private Cloud

Firewalls are used for businesses and consumers, with many devices including built-in firewalls. The firewall can be considered the first line of defense in protecting your business and your people from Internet-based threats. It's analogous to a security guard standing at the front door checking the ID of everything looking to enter or exit the building.



What is a Managed Firewall?

Once a firewall is deployed and configured, it must be monitored and managed to ensure that it continues to operate effectively and that evolving cyberthreats are detected and addressed.

Since this process can be time-consuming, complicated and is an ongoing daily need, many businesses opt for a managed firewall service. With a managed firewall service, a managed firewall service provider takes care of everything, from deployment to proper configuration to ongoing management around the clock.

Managed Firewalls are more than security and provide:

Secured Access

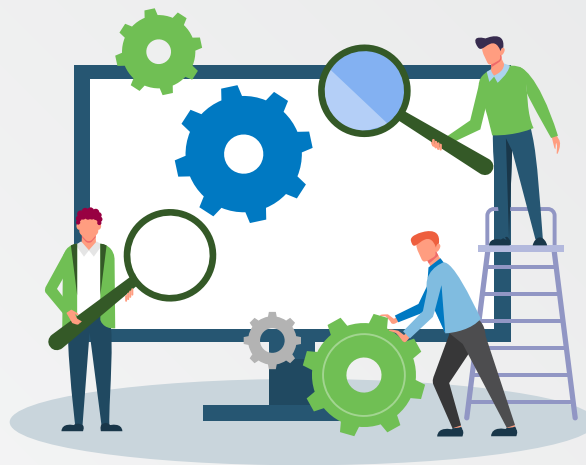
Managed firewall providers deploy software-defined wide area networking (SD-WAN) and a virtual private network (VPN) to enable organizations to leverage multiple business internet services to connect in-person, hybrid and remote users securely to the network.

Visibility

With detailed reporting from providers like TPx, you know what is happening on your network — from the top applications running and the websites being visited to which users are on the VPN.

Control

Once you know what is happening on your network, you can take action to control your network so your productivity is maximized. Want to stop bandwidth and time-draining applications like video streaming? The choice and control are in your hands.



How Do Firewalls Work?

A firewall establishes a border between an external network and the network it guards. It's inserted inline across a network connection and inspects all packets entering and leaving the guarded network. As it inspects, it uses a set of preconfigured rules to distinguish between benign and malicious traffic or packets.

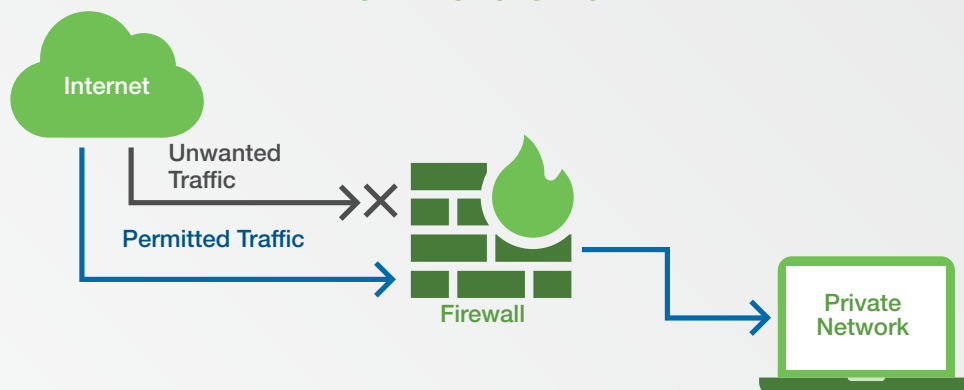
The term “packet” refers to data formatted for internet transfer. Packets contain the data itself and information about the data, such as where it came from. Firewalls can use this packet information to determine whether a given packet abides by the rule set. The packet is barred from entering the guarded network if it doesn't follow the rule set.

Rule sets can be based on several things packet data indicates, including source, destination and content.

These characteristics can be represented differently at different levels of the network. As a packet travels through the network, it's reformatted several times to tell the protocol where to send it. Different types of firewalls exist to read packets at different network levels.

Each firewall has to be configured appropriately to accept and reject certain types of traffic. Configuring the firewall means setting up rules and policies to control access to the network and configuring settings such as logging and reporting.

How Firewalls Work



PART 2

What Are Network Firewall Solutions?

Now that you understand network firewalls, let's look at the types of network firewall solutions you can deploy to protect your organization.

What Are the Types of Network Firewall Solutions?

The major types of network firewall solutions include software firewalls, hardware firewalls, stateless firewalls, stateful firewalls, next-generation firewalls and unified threat management firewalls:



Software Firewall

A software-based or host firewall runs on a server or other device. Host firewall software needs to be installed on each device requiring protection. As such, software-based firewalls consume some of the host device's CPU and RAM resources.

Hardware Firewall

A hardware-based firewall is an appliance that acts as a secure gateway between devices inside the network perimeter and those outside it. Because they are self-contained appliances, hardware-based firewalls don't consume the host devices' processing power or other resources.

Stateless Firewall

Stateless firewalls determine the threat level of data packets by examining parameters like source and destination, predefined through rules set by administrators or manufacturers. If a packet violates the predetermined criteria, the stateless firewall protocol identifies it as a threat and restricts or blocks the associated data. Unlike stateful firewalls, stateless ones evaluate each packet in isolation, without considering the connection's context or state.

Stateful Firewall

A stateful firewall, on the other hand, monitors the state of active connections and makes decisions based on the context of the traffic. It keeps track of the state of the connections and uses this information to determine whether to allow or block traffic. The state-aware firewall devices examine each packet and keep track of whether that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a more significant toll on network performance.

Next-Generation Firewall (NGFW)

Next-generation firewalls are more sophisticated than traditional firewalls, giving businesses a range of essential features for modern cybersecurity. Next-generation firewalls use advanced technology such as deep packet inspection, intrusion prevention and application awareness to provide greater visibility and control over network traffic. As a result, next-generation firewalls can identify and block potential threats more effectively than traditional firewalls, reducing the risk of cyberattacks and data breaches.





Unified Threat Management (UTM) Firewall

A unified threat management (UTM) firewall is a comprehensive software solution that combines multiple security features into a single unified system with out-of-the-box policies, simplifying management and reducing the complexity of deploying various security solutions. Most UTM firewalls have functionalities such as:

Antivirus

Antivirus helps prevent employees from downloading malicious payloads that could infect computers

IDS & IPS

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) detect and block known offensive attacks and active hacking attempts

Web Filtering

Control web access by employees and keep them from reaching sites that may contain malicious code

Application Control

Block users from running bandwidth-hogging apps like Netflix or BitTorrent file-sharing

VPN



Provides a secure connection between remote users and internal network resources

SSL DPI

Deep Packet Inspection makes sure encrypted traffic is inspected for malicious payloads

Firewall vs Antivirus

Firewalls and antivirus software are often used alongside each other and combined with other cybersecurity defense technologies. For businesses unfamiliar with the differences, below is a chart comparing the key factors:

	 Firewall	 Antivirus
Operation Scope	A firewall is a network security device and acts as a “traffic cop” for an organization’s network	Antivirus is solely a software application deployed on individual endpoints (computers, laptops, tablets or smartphones)
Implementation Format	Implemented by both software and hardware	Implemented by software only
Cyberthreat Target	Typically handles only external threats	Addresses both internal and external dangers
Operation Process	Operates by filtering and monitoring	Works by scanning and isolating infected files and viruses in software
Cyberattack Efficacy	Hackers can attempt to bypass firewalls via routing attacks or spoofing	There are no counterattacks possible once the malware is removed from the environment
Protection Scope	Protects the system from many kinds of threats	Protects the system only from malware and viruses
Purpose	Monitors incoming packets for threats and prevents unauthorized access	It searches, monitors, identifies, stops and deletes any malware or virus that is a danger to the computer system
Programming Complexity	Programming is more complex than antivirus	Programming is comparatively more straightforward than firewalls

PART 3

Why Should Businesses Invest in a Firewall Solution?

The consequences of successful cyberattacks vary in severity, ranging from substantial financial losses to a compromised brand reputation, as the affected company is seen as a security concern.

Most cyberattacks are directed at small businesses. According to the Federal Emergency Management Agency (FEMA), 90 percent of smaller companies fail within a year following an incident unless they can resume operations within five days. Hackers love small businesses even more than large ones, primarily due to these three reasons:



Lower Budget & Expertise

SMBs typically lack in-house IT staff with the know-how to protect their organization effectively and don't usually set budgets high enough to evaluate and update network firewalls (and other cybersecurity solutions) as well as manage them day to day.



Higher Volume of Vulnerabilities

SMBs are uniquely vulnerable because cybercriminals view them as easy targets with low or no defenses in place. And they're often right. At TPx, many of our cybersecurity clients are SMBs. Sadly, most don't turn to us for help until they've been attacked. One of these victims-turned-clients lost \$200,000 to ransomware just weeks after they asserted their company was "too small to be at risk."



Act as Gateways to Larger Targets

Small businesses do business with or source equipment and services from more prominent companies. While small companies don't have resources at the scale of enterprise organizations, they have valuable customer information and can provide access to large companies via unprotected connections. For example, the 2013 Target breach was perpetrated by [hacking a small HVAC company first](#)).

What Challenges Do Firewall Solutions Solve?

Firewall solutions protect against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can block data from specific locations (i.e., computer network addresses), applications or ports while allowing relevant and necessary data.

What Are Real-World Stats on Needing a Firewall Solution?

- According to FEMA, following a disaster, 90% of smaller companies fail within a year unless they can resume operations within five days.
- Small businesses are 3x more likely to be targeted by cybercriminals than larger companies. (Barracuda's 2021 Report)
- More than 30% of U.S. small businesses have weak points that bad actors can exploit. (CyberCatch study)
- Small organizations (those with fewer than 500 employees) spend an average of \$7.68 million per incident. (2020 Ponemon Study)

What Challenges Do Firewall Solutions Not Solve?

If a cyberattack gets past network firewall solutions and is inside the network, additional solutions such as endpoint detection and response (EDR), managed detection and response (MDR) and antivirus software become essential to remove the threat. While the firewall effectively identifies and prevents unauthorized access, it lacks the capability to independently eliminate malicious actors if they gain access to the network.

Why Do Small to Medium Businesses (SMBs) Need to Invest in Firewalls?

Many businesses, especially small businesses, think “it won't happen to me” due to the size of their organization and how they aren't the “whale” target that hackers would like to pursue. Think again:

- 43% of cybersecurity attacks happen to SMBs ([Microsoft](#))
- 50% of SMBs experienced a data breach ([Ponemon Institute](#))
- 33% of business downtime is caused by IT equipment failures ([Singlehop](#))
- An Institute for Critical Infrastructure Technology study found that ransomware attacks cost small businesses an average of \$133,000 in lost revenue and recovery costs.

PART 4

How Can Businesses Choose the Right Firewall Solution?

Just like all security guards aren't created equal, not all firewalls are created equal; you need the right one to stop intruders from getting in.

What Are Key Considerations in Firewall Selection?

There are several key considerations to keep in mind when selecting a network firewall and the service provider offering it:

Level of Protection

The firewall needs to provide adequate levels of protection against both known and emerging threats. An MSP actively defending their clients' business against cyberthreats daily will know the proper firewalls to deploy and the newest threats to watch out for.

Breadth of Portfolio

An all-in-one provider with a fully managed suite of firewall offerings will give your business a cohesive solution and even pass on cost savings through comprehensive service bundles.



Ease of Use

The firewall configuration settings and reporting dashboards should be accessible for your company to access if needed. The MSP providing the firewall should have fully-managed, co-managed or self-managed options available to your business for ongoing monitoring and maintenance of the firewall.

Pricing Models

Generally speaking, larger MSPs can give you the ability to pay off capital expenses like firewalls and network builds over time, which can help you get the best solution for the job while making your IT and finance teams happy.

Service Levels

The MSP providing the firewall should offer 24/7/365 fully managed services and provide you the flexibility to co-manage the solution or operate on an on-demand basis. As your business scales, your MSP should adapt to meet your requirements.

Certifications

Certifications present an instant test for the credibility of the firewall provider. An MSP certified by dozens of technology vendors and compliance auditors will keep your solutions up-to-date and in line with industry standards.

Geographic Availability

An MSP with nationwide coverage can grow with your business as you expand into new regional markets and meet the IT needs of multiple locations.





Technical Expertise

Your MSP should have specialists on staff who can handle installation, ongoing management and troubleshooting for every solution set you're using. Select a provider that can deliver genuine expertise for all your services.

Technical Infrastructure

Your MSP should have the infrastructure necessary to manage the solutions they're providing. These include capital investments like Network Operations Centers (NOCs) for managed network providers, Security Operations Centers (SOCs) for managed security vendors, remote desktop access for instantaneous support and testing labs for testing firmware and software updates in staging environments before applying them to your live setup.

Size for Scale & Influence

Small MSPs lack the resources to deliver a fully managed IT solution that spans a broad spectrum of services. Further, the relationship power of large MSPs pays off in ways that smaller MSPs can't match, such as getting the head of engineering on the phone at an underlying firewall provider. Smaller and regional MSPs don't have that same clout.

Compliance

Compliance with industry regulations, especially PCI DSS for retail environments and HIPAA for healthcare institutions, is critical for every network firewall.

What Are Common Mistakes Made When Selecting Firewalls?

When selecting a network firewall solution, businesses tend to make these mistakes:

MISTAKE 1

Incorrectly sizing your firewall.

Organizations need to consider the volume of traffic on their network and the needs for the performance of staff using the network. Working with a managed service provider can help as they can work to map the correct firewall to current traffic composition and throughput.

MISTAKE 2

Selecting a firewall with only one department's needs in mind.

The IT department at a larger organization may be the primary stakeholder purchasing a firewall solution; however, they need to consider the entire organization's needs, not just the IT department, and get other decision-makers in other departments to sign off on the selection.

MISTAKE 3**Purchasing a firewall only for future product roadmap milestones.**

There may be critical features you need for your organization that a given firewall provider may have on their roadmap and not have at the time of purchase. Product roadmaps can change and if you're purchasing a firewall in Q1 because in Q2, a key feature is promised to be added, you're setting your organization up not to have your needs met if the firewall provider doesn't meet roadmap milestone timelines.

MISTAKE 4**Not evaluating scalability and integration capabilities of the firewall.**

Suppose you're working in a high-growth organization. In that case, you may expand to multiple locations or new regional markets and incorporate various new applications in your tech stack while your new firewall is deployed. It's imperative this firewall can scale with you and integrate with your new cloud applications as needed.

MISTAKE 5**Not actively managing your firewall.**

Merely deploying a great firewall solution does not ensure your business is protected over time. Data, systems and applications change. An effective firewall solution requires focused attention from skilled resources for configuration, monitoring, ongoing management and maintenance of the technology. This challenges all businesses, especially SMBs, who typically have limited IT resources. To solve these challenges, many SMBs are looking to work with a managed service provider like TPx to deploy, configure and manage their firewall.

Avoid these common mistakes and seek the advice of an experienced provider to help you get there.

PART 5

Should Businesses In-source or Outsource Firewall Management?

Ultimately, companies have two options to address their network firewall management needs. They can take it on themselves or outsource it to a qualified managed services provider (MSP).

Why Should Your Business Outsource Firewall Management?

Organizations like yours outsource network firewall management instead of handling it in-house for these key reasons:



Lack of Expertise

The breadth and depth of knowledge demanded by IT teams today is vast and spans not only cybersecurity expertise but data storage, data integrity insight, software development, information technology infrastructure library (ITIL) knowledge, database design and management, network services, cloud computing, data analysis, troubleshooting and more. Security is a unique and complex discipline.



Lack of Time

Due to the interconnected nature of applications, devices and other technologies, IT departments are stretched thin, putting out fires. Many teams don't have the time to handle complex cybersecurity measures, like backup and disaster recovery, effectively.



Lack of Talent

The IT skills gap is a well-known challenge for businesses, especially SMBs, that cannot typically pay for hard-to-source expertise. This skills gap is prominent in the hyper-specialized realm of cybersecurity and backup and disaster recovery.

Costs to Do In-House

The average costs to manage network firewalls in-house include:

NEED	COST
Security information and event management (SIEM) firewall license	\$40,000 per year
Security Analyst	\$87,000 per year
Senior Security Analyst	\$110,000 per year

To guarantee 24/7/365 network coverage, organizations need:

- Five analysts
- One manager
- One correlation rules engineer

On top of this, the costs of benefits and training for each individual have to be accounted for, which varies between organizations.

Technology Can Only Go So Far

Human factor means businesses are always vulnerable

Six in seven companies (85%) experienced phishing and social engineering cyberattacks last year.

In-house systems and staff do not usually detect threats

The majority of breached organizations are notified by someone other than their own staff; an external source discovers 53 percent of breaches.

Technology costs

Access to and keeping up with the most advanced tools and threat feeds is fundamental but beyond the reach of most businesses.

Cybersecurity professionals are expensive, hard to find and retain

In 2021, there were 3.5 million unfilled cybersecurity jobs, according to a Cybersecurity Ventures report.

Increasing threat landscape

A cyberattack occurs every 39 seconds.

The longer a breach goes undetected, the more expensive it is

280 days is the average time to detect a breach.



Having a Firewall Isn't Enough

Cybersecurity technology is meaningless unless adequately configured, monitored and maintained. Managing firewalls involves costly technology and people that many small to mid-size businesses can't afford.

What Are the Benefits of a Managed Firewall?

A managed firewall environment helps organizations through:

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.

How Do Managed Firewall & Managed Detection & Response (MDR) Work Together?

Managed Firewalls with Managed Detection and Response do more than block suspicious IP addresses and preconfigured static signatures; they augment existing firewall controls with dedicated security analysts who combine context, deep security understanding and expertise with today's advanced technology to make data actionable.

It isn't enough to just detect threats. When a breach happens or an attack transpires, response time is critical, as is knowing how to respond. A qualified MSP orchestrates a rapid, coordinated and effective response to threats, ensuring your business thrives and your people are better protected.

An MSP like TPx deploys a managed firewall solution with a Managed Detection and Response (MDR) to provide:

- 24/7 monitoring of messages generated by security appliances and applications (firewall)
- Security analysts apply technology, advanced analytics and human expertise to detect indications of compromise or active attacks
- When threats are found, action is immediately taken to eliminate, investigate or contain the threat
- Information learned from the incident is used to implement better security controls

The steps involved in quarantining a threat using a managed firewall with MDR include:

1. Stop the attack
2. Identify what assets may have been affected
3. Collect all relevant evidence for civil, criminal or regulatory proceedings
4. Remove and quarantine the source of the breach
5. Recommend or implement operational improvements to prevent similar breaches in the future
6. Generate an incident response report

Firewall as Part of a Cybersecurity Protection Plan

A firewall is a component of the overall cybersecurity strategy. An MSP can develop the entire security strategy for a business.



PART 6

What Should Businesses Look for in a Managed Service Provider (MSP) Delivering a Managed Firewall Solution?



Deploying a firewall from a managed services provider (MSP) with security expertise is the most cost-effective choice for most businesses.

When seeking the right MSP to partner with, you must find one you can rely on to help you through your company's growth phases. That means top-tier expertise, financial stability, the size and reach to scale with your company as it grows, flexibility, reliability and 24/7/365 support.

What Capabilities Should Your MSP Deliver?

Key attributes to look for when selecting an MSP to manage your network firewall include:

24/7 Monitoring

True cybersecurity requires 24/7/365 management from a security operations center (SOC) staffed by security professionals. An 8/5/260 watch from a small provider won't cut it with today's threats.

Solid Technology

Your MSP should have the infrastructure to manage their solutions. These include capital investments like security operations centers for managed security vendors, remote desktop access for instantaneous support and testing labs for testing firmware and software updates in staging environments before applying them to your live setup.

Clear Trouble Ticketing System

The MSP needs to provide a straightforward way to access support from their technical team and quickly resolve any issues.

Regular IT Strategy Planning Meetings

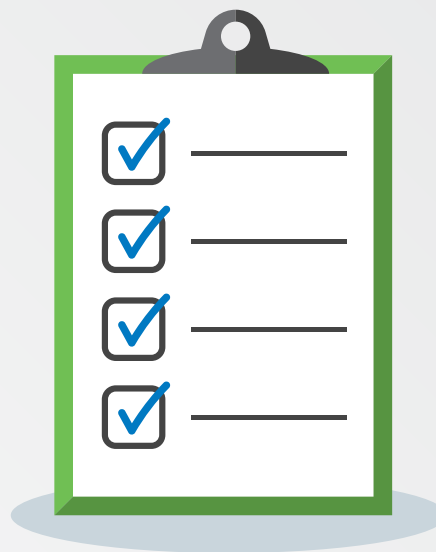
Your organization is expanding and changing – and so will your IT strategy, including your network firewall solution. Your MSP should regularly schedule quarterly meetings with your IT team to ensure solutions are still a fit and address any new requirements.

Easily Understandable Per Workstation Per-Month Billing Structure

A high-quality MSP offers standardized monthly pricing that is easy to scale and add or remove workstations as needed.

Clear Service Level Agreement (SLA)

What escalation paths does the MSP have available?
Does the MSP offer your business a dashboard for your staff to view and see if SLAs are being met?



What Are Common Firewall Management Issues MSPs Need to Address?

When managing a network firewall solution, MSPs need to address these common issues:

MANAGEMENT ISSUE 1

Selecting the proper firewall for client needs.

MSPs need to help their clients select the right firewall solution from the beginning of the engagement and typically include a few different firewall options, such as:

- Packet-Filtering Firewalls
- Circuit-Level Gateways
- Stateful Inspection Gateways
- Application-Level Gateways
- Next-Generation Firewalls

MANAGEMENT ISSUE 2

Creating a clearly defined network segmentation.

Network segmentation helps organizations slow down attackers, improve overall data security, simplify implementing a policy of least privilege, and reduce the damage caused by a breach. Configuring firewalls correctly will help segment various parts of the network from each other, making it harder for hackers to get further inside the network, even if they have access to one component.

Note that a possible strategy to add further layers of protection is to deploy multiple types of firewalls on various parts of the network, making it more difficult for bad actors when they encounter each new firewall.

MANAGEMENT ISSUE 3**Blocking all malicious traffic and allowing all valid traffic in.**

The process of blocking traffic from cyber criminals must not impact valid traffic from employees or consumers of the organization, creating a bad user experience. The MSP needs to make customized configuration settings on each firewall to let through specific types of traffic and block others. This is often why an MSP is critical, as internal IT teams will not have the know-how to configure the firewalls appropriately.

MANAGEMENT ISSUE 4**Updating the firewall correctly.**

Lots of firewall solutions are software-based and require updates that need to be made to them by the underlying technology provider. MSPs can quickly take care of these updates for organizations when their internal IT teams get overloaded and overlook them.

How to Make the Most Out of Your MSP Relationship

The managed services model is based on a partnership between your business and the MSP. You're a critical factor in the success of the partnership. Here are some tips to improve your chances for a positive outcome:

Communicate Your Goals

Are you adequately articulating what you need from your MSP? Many solutions can benefit your business, but not all meet your company's requirements. Your MSP needs to know what you aim to accomplish to advise and assist you effectively.

For example, if you're trying to address your network security concerns but approach an MSP requesting to "manage my network," true cybersecurity may not be part of their solution. On the one hand, they may not offer robust security. On the other hand, they may not scope that component into your tech stack even if they do. Clear communications can help you identify which MSPs can help you and ensure that an MSP delivers what you need.

Know What You're Actually Buying

Whether it's a network, security or communications service, the depth of your solution is primarily determined by your budget from both a technology standpoint and a service-level perspective.

For instance, when looking at a network redundancy solution, if you're purchasing a managed SD-WAN service along with your managed firewall service from TPx, your edge router options vary considerably in quality and price.

- A low-end router that's \$50 per month per location delivers a typical SD-WAN solution but does not have subsecond failover to keep voice and video up even through an outage. Sessions start up after you reinitiate the call, but they aren't persistent.
- If your business requires subsecond failover no matter what, the router that can deliver that service is \$500 a month per location.

Establish Designated Points of Contact

The MSP needs to reach out to you for the partnership to work. This is especially true in co-managed environments wherein the MSP and your IT team work together to solve problems requiring clear, documented and reliable communication channels between both organizations.

Prioritize Solutions & Locations Realistically

Unless you're a vast enterprise with high-maintenance facilities, not all your locations will require 100 percent of an MSP's given solution set. If you're working with limited funds, you'll need to determine which needs are vital and which can be tabled until next year's budgeting cycle. In other words, you may not be able to secure every location and have a great network connection this year. You'll need to work with your MSP to determine how comprehensive your solutions can be at a budget that works for you.

Understand That Each Solution Category Has Layers

Case in point: if you're looking at security, no single widget solves all your network's issues. If you purchase managed endpoint detection and response (EDR) from an MSP, they patch and protect your machines and servers but aren't touching the rest of your network unless you scope for those services. In this scenario, having EDR is a significant step, but it's not a silver bullet and your security solution as a whole will have gaps if this is the only service you deploy.

Be Honest About What You Don't Know

You must be upfront with the MSP about gaps in your knowledge and experience. Remember that the MSP is there to support your existing IT department, not to replace it. Don't feign understanding of complicated solutions to save face. You don't want a critical component of your tech stack to be overlooked because your MSP mistakenly believes you have it covered.



PART 7

Why Should Businesses Choose TPx?

You have a lot of challenges for your business including data breaches and the potentially catastrophic impact on customer relations, business operations, workflow and your bottom line.

At TPx, we have the solutions, experience and certifications to solve these challenges and keep your network safe and running smoothly.



What is TPx's Managed Firewall Solution?

TPx's Managed Firewalls service goes beyond the traditional constructs of a firewall – we deliver secure access, visibility and control so that your business can benefit from greater cybersecurity and productivity.

Network Intrusion Detection & Prevention

TPx's Managed Firewall solution features both Intrusion Detection (IDS) and Intrusion Prevention (IPS) systems, which work in tandem to detect and block known threats. By sending suspicious activity alerts, IDS proactively protects you from cyber threats, such as malware, viruses and zero-day attacks. If malicious activity is detected, then IPS blocks those packets.

Gateway Antivirus

Hackers often attach malicious code to high-traffic websites, so when an unsuspecting visitor clicks on this site, a virus, worm or other malicious code downloads to the machine. TPx's Managed Firewall leverages gateway anti-virus to thwart these attacks. The anti-virus checks all HTTP, HTTPS, SMTP and FTP traffic for malicious code embedded within the traffic and blocks access to infected sites.

Web Content Filtering

TPx's firewall management services help you know what is happening on your network, from the top applications running and the websites being visited to which users are on the VPN. Our web content filtering helps you go one step further to implement company policies to prevent unauthorized browsing on your corporate network.

Managed Detection & Response (MDR)

Threats are inevitable, so quick response times matter. Managed Detection and Response (MDR) augments existing firewall controls with dedicated security analysts who combine context, deep security understanding and expertise with advanced technology to detect the threats others miss and orchestrate a rapid, coordinated and effective response to threats.

Additional solution features include:

- Web application firewall
- Data leak prevention
- Traffic shaping
- Policy scheduling
- Site-to-site IPsec
- Active directory integration
- VPNs with 2-factor authentication
- 4G failover Third-party access vendor support
- Wireless access point, switch integration and management
- Threat intelligence
- Sandboxing
- Vulnerability cans
- SD-WAN
- Anti-virus
- SSL deep packet inspection

Why Use TPx for Managed Firewall?

**Continuously Trained
& Seasoned
Security Professionals**

**24/7 Health Monitoring
& Troubleshooting**

**Customized
Device Configuration
& Tuning**

**Updates
& Patch Management**

**Log Retention
& Reporting**

Licensing

**Hardware
Assurance**

**Configuration
Backup
& Storage**

**Frees Internal
IT Staff**

**No Managing
or Monitoring from
Internal Teams**

**Protects
Company Reputation,
Clients, Profitability
& Productivity**

**Comply with
Industry Standards
& Regulations, Including
HIPAA & PCI DSS**

Why Choose TPx?



Our mission is being the easiest MSP to do business with



We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella



We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more



We offer HIPAA, PCI DSS and SOC 2 Compliant solutions



We provide enterprise-class, 24/7 support



We offer different service levels and highly customizable solutions



We have a national footprint, with multi-site, multi-carrier, partner coverage



With thousands of clients nationwide, we're big enough to get the job done and small enough to be agile



We have various dedicated teams to ensure service excellence



We continuously invest in automation, self-service innovation and back-office transformation



We are committed to providing the most densely monitored service delivery platform in the industry



We understand and embrace the criticality of our customers' performance analytics

TPx is a Single Source for Managed Security Services

Security Advisory Services

TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services include a Virtual Compliance Officer (VCO) with a cybersecurity gap assessment, network vulnerability and penetration scanning, network security assessments, wireless site survey and ransomware readiness assessment.

Security Awareness Training

Users are your first line of defense. The more they know, the less prone they are to becoming victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.

Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your business from internet-based threats. Next-generation firewalls block today's advanced threats while providing secure access, visibility and control to help your business be more productive.

Endpoint Management and Security

TPx helps keep your servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an "always-on," best-in-class, 24/7/365 service.

Managed Detection and Response (MDR)

Discover, prevent and recover from cyber threats faster. TPx's MDR helps you identify more threats, reduce attack dwell time and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Email Security

Protecting your email communications is an important part of any security strategy. Whether it's protecting against email-based cyberattacks like phishing or ensuring that sensitive information doesn't fall into the wrong hands, we can help you navigate the email security challenge. Our Managed Inbox Detection and Response (IDR) user security solution provides professional evaluation and handling of suspicious emails reported by users — right from the inbox.

DNS Protection

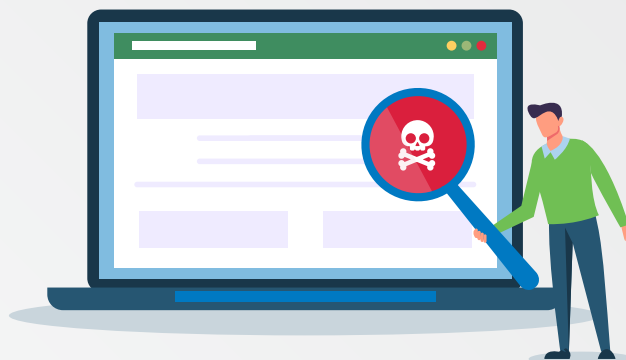
We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless and non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Backup and Disaster Recovery

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives.

Ransomware Detection

All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems as if it never happened.



PART 8

Glossary of Terms

Below are definitions of cybersecurity terms featured in this guide:

Firewall: A firewall is a software or firmware that prevents unauthorized access to a network. It inspects incoming and outgoing traffic using a set of rules to identify and block threats.

Next-gen Firewall (NGFW): A next-generation firewall (NGFW) is part of the third generation of firewall technology that can be implemented in hardware or software. It can detect and block sophisticated attacks by enforcing security policies at the application, port and protocol levels.

Unified Threat Management (UTM): Unified threat management (UTM) describes an information security (infosec) system that provides a single point of protection against threats, including viruses, worms, spyware, malware and network attacks. It combines security, performance, management and compliance capabilities into a single installation, making it easier for administrators to manage networks.

Managed Detection & Response (MDR): Managed detection and response (MDR) services are a collection of network-, host- and endpoint-based cybersecurity technologies that a third-party provider manages for a client organization. The provider typically installs technology on premises at the client organization and provides additional external and automated services through software.

Software Firewall: A software-based or host firewall runs on a server or other device. Host firewall software needs to be installed on each device requiring protection. As such, software-based firewalls consume some of the host device’s CPU and RAM resources.

Hardware Firewall: A hardware-based firewall is an appliance that acts as a secure gateway between devices inside the network perimeter and those outside it. Because they are self-contained appliances, hardware-based firewalls don’t consume the host devices’ processing power or other resources.

Stateless Firewall: Stateless firewalls use a data packet’s source, destination, and other parameters to determine whether the data presents a threat. These parameters have to be entered by either an administrator or the manufacturer via rules they set beforehand. If a data packet goes outside what is considered acceptable, the stateless firewall protocol will identify the threat and restrict or block the data housing it.

Stateful Firewall: Stateful firewalls make it so that state-aware devices examine each packet and keep track of whether it is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a more significant toll on network performance.

Antivirus: Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems.



Ready to Secure
Your Network?

[CONTACT US TODAY](#)