



# Managed Firewall Prospecting Guide

# What you can find here

- Customer profiles
- Common buzzwords
- Key benefits
- Positioning
- Overcoming common objections
- Sample cost analysis and value props
- Available resources



A person is seen from behind, sitting at a desk in a server room. They are looking at several computer monitors. The monitors display various network-related information, including maps, diagrams, and data tables. The room is dimly lit with blue light, and server racks are visible in the background. The text "Managed Firewall" is overlaid in the center of the image.

# Managed Firewall

# Managed Firewall: Customer Profile

Any customer is a potential managed firewall customer

- Small businesses with no IT
- Small and mid-sized business with limited IT who are stretched thin and who are looking to offload this responsibility
- Multi-site businesses looking to centralize security policies
- Businesses with aging infrastructure
- Businesses with no firewall
- Businesses with compliance requirements (PCI, HIPAA)

# Managed Firewall: Buzzwords & Definitions

**Next Generation Firewall** Firewall technology that is implemented in hardware or software and is capable of detecting and blocking sophisticated attacks by enforcing security policies at the application, port and protocol levels.

**UTM** Unified Threat Management consolidates multiple security and networking functions all on one appliance to protect small and medium businesses

**Deep Packet Inspection** A type of data processing that inspects in detail the data being sent over a network and takes action by blocking, re-routing, or logging it accordingly

# Managed Firewall: Buzzwords & Definitions

**Web Content** Filtering piece of software designed to restrict what websites a user can visit on his or her computer.

**Security Operations Center (SOC)** Facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis.

**SSL VPN** A virtual private network that allow users to connect to a private network and use its systems even when not directly connected to that network.

# Managed Firewall: Buzzwords & Definitions

**SIEM** Security Information and Event Management tech that supports threat detection and security incident response via real-time collection and historical analysis of security events from a variety of event/contextual sources

**Malware** Malware is any software that tries to infect a digital device to extract personal information, steal money, or lock you out of your device.

**Virus** Type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

# Managed Firewall: Key Benefits

Fully customized Next Gen firewall provisioned/deployed to provide enterprise-level security at prices SMBs can afford

- Security specific SOC analysts and engineers
- Full suite of Unified Threat Management (UTM) features
  - Web content filtering, application control, intrusion prevention (IPS), Anti-virus, SSL deep packet inspection
- Compliance reporting
- 24/7 monitoring
- SIEM and other management tools

# Managed Firewall: Key Benefits

Greater visibility into network

- Network troubleshooting
- View network resource usage
- Shape traffic on your network
- Control bandwidth usage to save costs
- Help enforce company policies
- Reduce potential liabilities
- Boost productivity

# Managed Firewall: Qualifying Questions

Do you have a firewall? Who manages it? How old is it?

Unless the answer is “I have a dedicated security engineer on call 24/7 that manages my new next gen firewall” there is an opportunity

Do you take credit cards, have compliance requirements or just want more visibility into your network?

Get the customer thinking about the added value of a firewall solution, more than just a security offering.

# Managed Firewall: Qualifying Questions

Have you ever had a virus or malware on your network that cost you time and money to resolve?

Look to find if a customer has had any pain in the past related to security that could have been addressed.



# Managed Firewall: Overcoming Objections

*I am a small business. I'm not really a target of attacks.*

- More than half (55%) of smaller businesses reported at least one data breach in the previous year
- Almost two-thirds of all cyberattacks are now directed at small business
- 60% of small businesses go out of business within six months of an attack

# Managed Firewall: Overcoming Objections

*I can't afford it.*

- Prevention is cheaper than remediation
- According to PwC Health Research Institute analysis, the likely cost of a serious cyber security breach in the healthcare industry is \$200 for every patient record. This includes the overall cost of the breach, including the business downtime, reputational damages, litigations, and business loss. On the other hand, the cost to thwart a cyber attack is only \$8 for every patient record.

# Managed Firewall: Overcoming Objections



*I can do it myself.*

- It's unlikely a customer can provide 24/7 monitoring for the same price and same expertise
- The various systems for management, monitoring and logins are very expensive for a single organization. This cost is shared with a managed service.

# Managed Firewall: Overcoming Objections

*I like to have control of firewall and concerned about response times to make small changes.*

- Integrating with active directory addresses this by keeping the ability to change user policies in the hands of IT and implemented via changes in active directory
- Portal lets customer make web content filtering changes
- Direct access to SOC engineers allows them to implement changes or do troubleshooting
  - 800 number, email, DASH ticket

# Managed Firewall: Value Props

- Equipped with the latest technology to help monitor and manage your firewall. *Too expensive for most businesses.*
- Staffed 24/7 to ensure no gaps in coverage. *Again, too expensive to deploy for most businesses.*
- SOC and engineering members are highly specialized. All they do is security and firewalls. *This specialization is difficult and expensive to maintain in house.*

IT technicians salaries have been growing at an 8% rate nationally every year, so customers can save money while gaining a stable, knowledgeable experience and cost structure

# Managed Firewall: Value Props

- Incredibly flexible cost options for customers, based on their service level needs and service commitment lengths
- Few providers in the U.S. can offer a product portfolio scope of a nationwide managed services carrier like we do
- Single provider provides one throat to choke for all customer's problems

# Managed Firewall: Key Resources

- Dedicated Channel Sales Team
- Dedicated Channel Sales Engineers & Evangelist
- Dedicated Channel Provisioning & Project Management Team
- Security blogs such as <https://thehackernews.com>
- Customer Facing Brochures
- Case Studies
- Videos