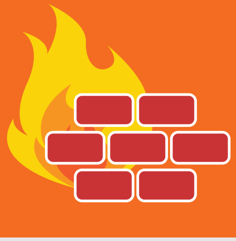
Managed Firewall



TBI Battlecard

What to Look for in the Field

- Customers looking to do a firewall refresh
- Customers who have been/recently attacked
- Customers who can not remember the last time they updated/patched their firewall
- Customers with compliance needs
- Customers with little understanding of security
- SMB customers (usually huge targets, typically think they are too small to be breached)

Overview

With so many cyber security threats, it makes sense to invest in a managed firewall solution.

Traditional firewalls include:

- Packet Filtering
- Network Address Translation
- URL Blocking
- Virtual Private Networks (VPN)

A managed firewall solution takes on management, maintenance and reporting. It includes:

The Device

A centralized virtual or physical appliance, now part of a monthly contract moving it from CapEx to OpEx. As needs grow and a larger device is required, scale the solution without having to purchase a new device.

Firewall Maintenance

Updates, patch management, change management and other maintenance is handled 24x7x365 by the vendor. This service will occur within an agreed upon SLA to ensure needs are met in an acceptable time frame.

Portal

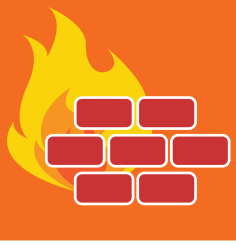
Continuous visibility into perimeter security for monitoring, logging and reporting all done through a cloud-based portal. View data and analytics, assess trends, utilize logs for audits and compliance requirements.

Discovery Questions

Use these discovery questions to talk to your customers about their security policy, upcoming needs and how they plan to evolve their security posture in our ever changing, high threat environment.

- Do you have a security policy? An acceptable use policy? What does it include?
- Do security policies include: data protection, destruction, passwords and reporting procedures?
- What regulatory and compliance standards do you have to adhere to?
- Do you employ any security staff or IT employees with security duties?
- Where would you say your biggest vulnerabilities lie? What challenges do you face as it relates to security?
- Do you run audits on your security, who do you use, when was your last audit?
- When was the last time you completed a security assessment?
- When was the last time you updated your firewall?
- How old is your firewall? Can you provide make and model "I have resources (TBI) who can verify if the device is still supported"
- Do you have application visibility and control?
- How do you handle security attacks, before, during and after?

Managed Firewall



TBI Battlecard

Add-ons to Managed Firewall

- SD-WAN
- DDoS mitigation
- Secure web gateways
- Endpoint security solutions
- Wireless backup/routers
- Enhanced email security
- Management and analytics software
- Web application firewalls and delivery controls
- Cloud instant security (public and private cloud security solutions)

The Next-gen Firewall

With a next-gen firewall, additional features are layered on with QoS and no additional devices are needed. Additions can include:

Intrusion Detection System (IDS)

IDS identifies malicious traffic targeting the network and provides alerts. Activity is logged to provide an audit trail available for review in a portal.

Intrusion Prevention System (IPS)

IPS works in conjunction with IDS to block malicious traffic and quarantine suspicious traffic. Parameters can be set through the cloud-based portal.

Antivirus

Antivirus software/applications protects inbound and outbound traffic against viruses, worms, trojans and other malware. Protection is at the edge of the network and in real time. Threats are logged in the same SIEM portal.

Content Filtering/URL Filtering

Often the last piece of the security puzzle, content filtering protects your internal network. This web filtering blocks access to web sites outside of a company's Internet "Acceptable Use Policy", ranging from social media sites and YouTube to gambling and drugs.

Deep Packet Inspection (DPI)

DPI grabs pieces of each packet to thoroughly inspect and identify anomalies or violations of normal protocol/communications.

Application Awareness

Log and track application use throughout the network to create a baseline and use these parameters to set policy around which users can access what.

Active Directory/LDAP Integration

This integration allows a higher level of content/URL filtering based on the user's roles within Active Directory.

Debunking Myths

I have a firewall that's all I need.
Response: While definitely a critical part of your security posture, a firewall does not protect against all threats.

I bought a firewall years ago and its running fine.
Response: When was the last time it was updated/patched?

Firewalls protect against all threats.
Response: No, although it is crucial, it is only one part of a complete security posture to fully protect a company against threats. Look to Endpoint protection, DDoS Mitigation, Cloud/mobile security, etc..

Firewall logs are just false alerts.
Response: While many alerts are false positive, it can be very difficult to catch the ones that ID true threats. This opens the conversation to SIEM.

Top Providers

AT&T | Airespring | CenturyLink | Forsythe | Hypercore | Masergy | MegaPath
MetTel | Tata | Telstra | TPX | Windstream | Verizon