COMMERCIAL SECURITY

# Managed firewall services: Are they right for you?

*By Rich Aycock, Manager of Cyber Operations for ADT*

As cybercrime continues to plague companies of all sizes, across all industries both public and private, we wanted to take this opportunity to explore options that can help protect your data and your business. We are often asked whether a Security-as-a-Service (SaaS) is the right option for many organizations. In this case, we are tackling the topic of managed firewalls versus a self-administered solution. But before we get there, let's take a brief look at the history of network firewalls and how to determine which type may be best for you.

## History of network firewalls

Simply put, a network firewall is a system or group of systems used to control access between two networks—a trusted network and an untrusted network—using pre-configured rules or filters. Firewalls can be comprised of a single router, multiple routers, a single host system or multiple hosts running firewall software, hardware appliances specifically designed to provide firewall services, or any combination of the above. They vary greatly in design, functionality, architecture, and cost. They are also sometimes known as a Border Protection Device (BPD) where the firewall separates networks by creating perimeter networks in a demilitarized zone (DMZ).

Network firewalls have been around almost as long as the internet itself, first emerging in the late 1980 in response to a number of internet security breaches.

Over the years they have gone through many iterations, starting with packet-level filter firewalls developed in 1988 by Digital Equipment Corporation, later evolving to circuit-level firewalls. The current generation, often referred to as next-generation firewalls (NGFW), combines the attributes of the previous versions but has been expanded to include other network device filtering functionalities, such as application-level firewalls incorporating deep packet inspection (DPI), intrusion prevention systems (IPS), stateful inspection, identity awareness and the ability to use external intelligence sources to identify and help stop potential breaches. In some instances, they may also have anti-virus capabilities.

## Who should use firewalls?

The short answer is every company and organization in business today should be using some type of firewall, including small and even home-based businesses. The hackers of days gone by may have been savvy teenagers showing off their digital prowess or the lone wolf trying to break into networks by attacking passwords. Today, many of these breaches are the result of concentrated efforts of organized criminals that deploy automated attacks. Worms and viruses initiate the vast majority of attacks, using worms and advanced malware to probe for weaknesses and infiltrate ill-secured networks. These types of attacks generally find their targets randomly. As a result, even organizations that may feel they have little or no confidential information may end up as victims of cybercrime without taking adequate preventative measures.

## So everyone needs a firewall, but what kind?

In order to decide what type of firewall will work best for your organization, here are a few questions to identify the right solution:

- What security measures will the firewall need to perform?
- What additional services would you like to be part of the offering?
- What networking functions will it need to perform, i.e., routing?
- How will it interact with existing services and users?
- What does the firewall need to control or protect?
  - » Access into the network
  - » Access out of the network
  - » Access between internal networks, departments, or buildings
  - » Access for specific groups, users or addresses
  - » Access to specific resources or services
- What regulations is my business subject to that would require a firewall or specify how it is configured and/or managed? (ex. HIPAA, PCI)
- What would it need to protect?
  - » Specific machines or networks
  - » Specific services
  - » Information—private or public
  - » Users

*Continued on the next page >*

CONTINUED

# Managed firewall services: Are they right for you?

*By Rich Aycock, Manager of Cyber Operations for ADT*

- What impact will a firewall have on your organization, network and users?
  - » Is hardware available that meets the requirements to support a firewall solution?
  - » Will existing services be able to function through a firewall?
  - » What will the financial impact be on the organization? Financial impact should include initial implementation costs, ongoing maintenance and upgrades, hardware and software costs, and technical support costs.

## Self-administered firewalls or managed firewall services? Which is a better choice for you?

While we have established that firewalls are an important component for every business in operation today, there are also a variety of firewalls to choose from. Now it is time to determine if a self-administered approach works best for you or if a third-party managed firewall service is a better choice.

**Key questions to consider in the decision-making process may include:**

- Who will administer the solution?
- Are experienced technical personnel available for the job or will someone need to be hired from outside your organization?

With the cyberthreat landscape ever-evolving, your cybersecurity policies and procedures along with your cyber defenses, including firewalls and anti-virus software, need to be evolving as well. This means that a "set-it and forget-it" methodology just will not work. Organizations that lack the expertise to properly maintain their cybersecurity programs may struggle to keep their data safe. To further complicate matters, a *2017 Cybersecurity Jobs Report* by Cyber Security Ventures predicts that there may be as many as 3.5 million cybersecurity job openings by the year 2021 and not enough people to fill them. The lack of resources will make it hard for many organizations, particularly small to medium-sized ones, attract and retain cybersecurity experts. Add that to the cost of those individuals and the potential for high turn-over rates for individuals in demand, maintaining a safe and secure environment can become even more daunting.

**A third-party managed firewall service** administered by certified Managed Security Service Providers (MSSP) may be the solution for many, if not most, organizations. Key benefits to this approach may include:

- Device provisioning and deployment
- Performance, availability and policy management, upgrades and patch management
- Real-time security and health monitoring and expert response to threats and health issues
- 24/7 real-time security event and device health monitoring
- Support from certified network security experts
- Potential for improved total cost of ownership and reduced costs
- Simplified management
- Better internal threat protection
- Reduced internal IT security training

**One final consideration** when determining which approach will work better for your organization is the number of firewalls that may need to be managed and maintained.

Historically organizations generally only had one firewall, between them and the world. Now, not only are the devices themselves more complicated, but there are more of them in an organization. Segmentation and even micro-segmentation means that organizations are employing more firewalls to put controls and safeguards between areas inside their network, as well as help protect them from the outside. This adds to the complexity of your cybersecurity defenses.

*Continued on the next page >*

# Managed firewall services: Are they right for you?

*By Rich Aycock, Manager of Cyber Operations for ADT*

## Conclusion

Using a managed firewall service can deliver a team of IT security experts to proactively detect new threats and help to reduce threat issues without the expense of hiring, training and managing an internal staff. With cybersecurity threats on the rise, constantly evolving, and presenting a risk to organizations of all sizes across every industry, keeping your data secure is paramount no matter what path you choose to pursue.

## About ADT Commercial

At ADT Commercial, we take a holistic approach to security through traditional solutions such as intrusion alarms, fire/life safety solutions, access control and video, but by also helping design, install, monitor and manage security-only networks, deliver cybersecurity services and help manage and monitor firewalls and anti-virus software. We operate two Network Operation Centers and an Advanced Security Operations Center to deliver 24/7/365 management and monitoring of client's networks. Our engineers hold a number of certifications for various Cisco Meraki applications and is one of the only security providers to hold Cisco Cloud and Managed Services Express Partner certification. ADT Commercial is also a certified Managed Security Services Provider (MSSP) for Palo Alto, Fortinet, Sonicwall and Cisco solutions.





04/19