White Paper: Which Firewall Option to Choose

Q and A with Tim Campbell

Q: With all of today's security threats and rapid technological change, how does a business owner determine what type of firewall he or she needs?
Tim: The short answer is the owner probably needs a much more sophisticated firewall than he or she currently has. Here are a few sobering statistics:

- 43 percent of cyber attacks target small business.*
- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.*
- 60 percent of small companies go out of business within six months of a cyber attack.*
- 43 percent of small business data security breaches are caused by Email Phishing / Social Engineering.*

Q: But where to start?
How about with some basic terminology. "Legacy" firewalls or stateful firewalls are what most businesses have today. They are more easily bypassed by hackers, leaving the network and clients vulnerable. "Next-gen firewalls" have the ability to greatly increase network security, but of course they are more expensive and require a lot more effort to set up.

Q: When is a standard firewall adequate?
Tim: When you can answer "no" to all of the following questions:

- ☐ Do you have on-premise applications or systems that are accessed via the Internet by customers, vendors or mobile employees? These applications may include, but are not limited to, your company website, file sharing applications, on-site cameras, POS system, building management systems, etc.
- ☐ Are you concerned about employee productivity and the effect that unauthorized or excessive usage of such sites as Facebook or YouTube might have?
- ☐ Do you allow employees, customers, vendors or visitors to bring their own devices (laptops, tablets and smartphones) and connect them to your company local area network (LAN) or WiFi network?
- ☐ Do your employees receive email attachments at part of their normal daily business?

Q: Okay, that seems like a loaded quiz. Isn't just about every business going to answer "yes" to one or more of these?
Tim: Yup. Keep in mind I'm here to scare you. If you're not, go back and read the answer to the first question.

Q: Well, certainly these businesses differ greatly in their "next-gen" firewall needs. Can you help clarify a still muddy situation?
Tim: Let's categorize the threats:

1. Theft of proprietary information contained in your systems (e.g. patient records, credit card numbers, etc.)
2. Viruses and malware that can degrade computer performance and steal information (like ACH routing numbers).
3. Ransomware that prevents victims from accessing their data or threatens to publish their data unless a ransom is paid (some versions of this have already destroyed the data and the ransom is a decoy while data is being destroyed).

4. Phishing attacks that trick people into giving out information like passwords.
5. Productivity killing unauthorized or excessive use of Internet sites by employees.
6. Hijacking of Internet bandwidth by unauthorized WiFi bandwidth.

Obviously the threat of someone stealing credit card information from your billing system is far worse than Kari in your accounting department spending too much time on Facebook. Most companies will want to address the category #1 threats first. And most will have taken some action outside the firewall to prevent viruses and malware (category #2).

Some of these threats are going to be very difficult to deal with, and a next-gen firewall isn't the total solution. For instance, phishing relies on tricking unsuspecting employees, and requires ongoing training and individual vigilance to prevent. Operating systems (e.g., WIndow) updates need to occur in a timely fashion--but what about an employee that has been on vacation and their laptop has been powered off for two weeks?

And finally, go ahead and try to limit Internet access by employees to see just how big a can of worms can be.

Q: You succeeded. I'm worried. And I want to do something about it right now. What do I do?
Tim: Schedule a meeting with key people in your company (finance, owner(s), IT, etc.) and start digging into this. Here's a suggested agenda:

1. What are we most worried about?
2. What kind of firewall do we have now?
3. How secure are our systems?
4. How secure are our computers?
5. Are our company information security policies adequate?

This will be a long and painful meeting, and you should have your IT providers and your network provider there. Your goal should be to emerge with some idea of the top threats and whether they are best addressed by:

- A next-gen firewall
- Improved systems and computer security
- Revamped employee policies and training

It's unlikely this will be your most entertaining meeting of the week. Just your most important. But I also want to stress that developing and maintaining a sound information security posture is an ongoing process, it's NOT a one time event. It requires continuous care and feeding.

Tim Campbell is Director of Technology Services for Avid Communications and has extensive experience in and a longstanding passion for network security.

***Source: Small Business Trends, CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know January 3, 2017**

https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

https://pixabay.com/en/locked-gate-padlock-security-2143493/

https://pixabay.com/en/cyber-security-computer-security-1784985/

For more information about Firewall options, please call us at 816.994.7070.