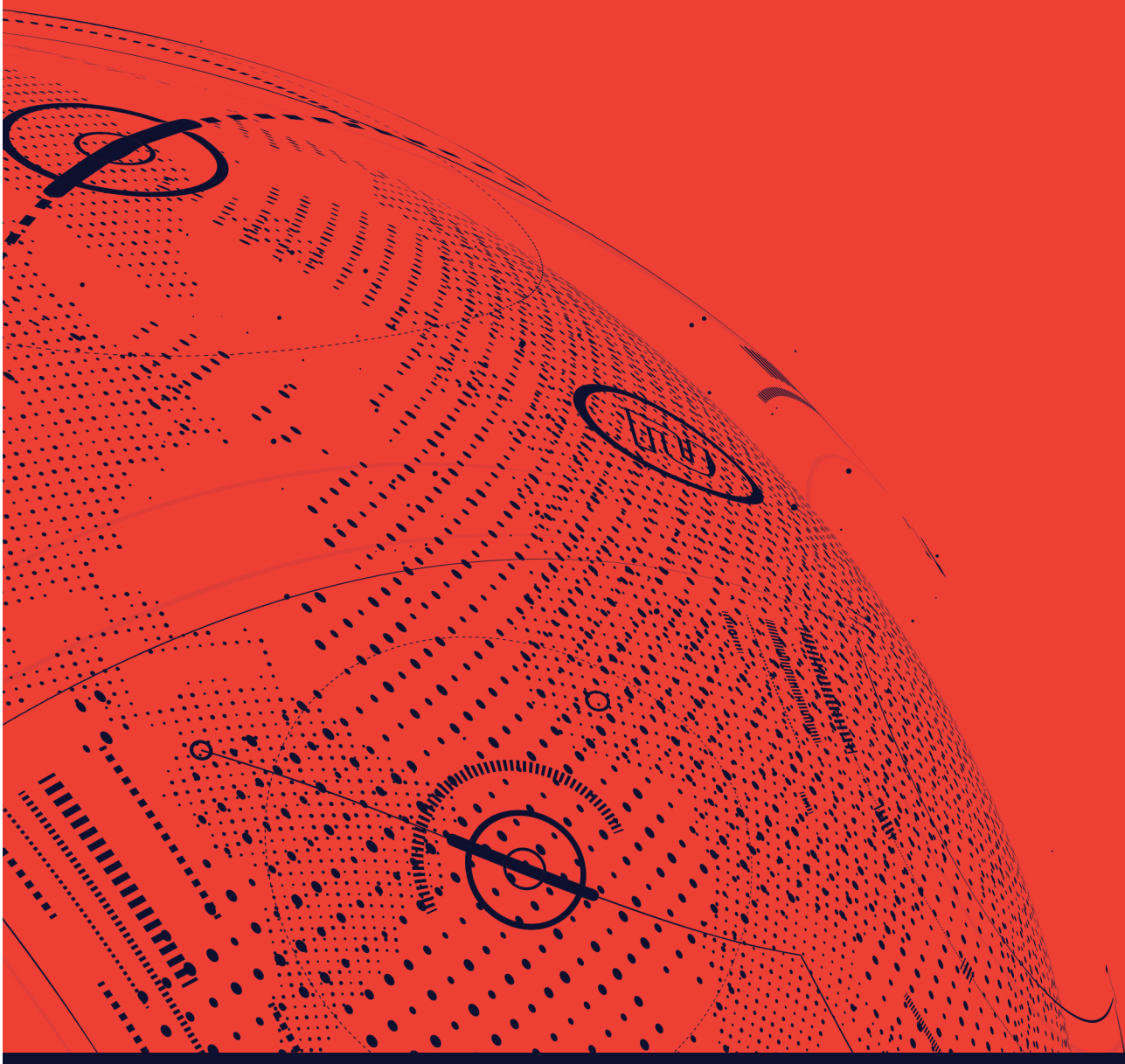
BUILD VS BUY:

MANAGED FIREWALL

A MERIT NETWORK, INC. WHITEPAPER

NOVEMBER 2017



Contact us:
sales@merit.edu | 734-527-5785

merit

From network servers or the cloud to the tiniest thumb drive or solid state disk – every organization that stores data needs cybersecurity.

Without exception.

FROM THE 2017 DATA BREACHES at Equifax, or Target's $19 million settlement this year over a 2013 cyberattack, most Americans are convinced that the need for additional security equipment and software is real. It's easy to believe from the headlines that hackers only seek high-value, personally identifying information that can be stolen en masse and then deployed quickly in fraudulent transactions. In fact, cyberattackers can be very patient and ambitious. Your organization may not have any Social Security number – however information within your databases could be used to target your customers phishing emails. Your organization's construction contracts may contain no addresses or account numbers, but could have vendor information that lets a hacker present themselves to another company's network as a trusted user. No one is immune to the risk of cyberattack, but firewalls help ensure everyone is prepared.

Sounds simple, doesn't it? In practice, firewalls are a complex solution that must factor in all the available software and technology, the manpower an organization will need to maintain them, the full landscape of potential threats and the value of institutional data being protected, plus employment and contracting needs – all balanced against the costs of implementation and upgrades.

WHAT IS A FIREWALL?

In short, a firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic using predefined security rules.[1] Think of it as your barrier between controlled and trusted internal networks and outside hostile environments, like the internet.

You can configure your system with one firewall or several, though with two firewalls the likelihood of unwanted entry significantly decreases. If one defense measure fails, a second firewall can still contend with an untrusted user while allowing other traffic to flow normally. Firewalls sit in front of the network infrastructure they protect, whether in a perimeter location or internal server networks.

A perimeter firewall is an essential component for detecting and protecting the network from unwanted traffic, by screening potentially dangerous content for intrusion attempts and flagging these threats to the network administrator. Perimeter firewalls block incoming traffic from reaching internal network and bar outgoing traffic from accessing undesirable external hosts. Host-based firewalls, in contrast, run on individual computers as needed to block unwanted traffic within a trusted network, and protect against unauthorized access.

BASIC FIREWALL DESIGN

Firewalls can be configured by any capable IT professional, but it is always preferable to engage an expert who can tailor that configuration to suit your needs. This helps ensures that all configuration, setup, monitoring and support is taken care of in a timely manner.[2] Building your own firewall may be cheaper in the short term, but the benefits of a cloud-based or external firewall service can outweigh building your own over the life cycle of a network.

Obviously your security policy will govern the rest of this process. It defines who can access your resources, what uses for those resources are acceptable, how the resources should be protected and the proper responses when security issues arise. Be sure that this policy addresses which resources will require internal and external user access, the vulnerabilities associated with each of these resources, measures that can be taken to protect these resources and a cost-benefit analysis comparing the different measures and solutions.

Design should adhere to security policy. The simpler your design is, the easier it will be to implement, maintain, test, troubleshoot, and adapt to new changes. Network devices such as routers and switches have functional and basic purposes, but should be used correctly. Using the wrong product to solve a security problem can itself create security threats.

Experts will generally agree, a layered defense is ideal for your network because if one layer gets compromised then others behind it can go on protecting your data and your functionality. Also, not all threats come from outsiders and any sound security configuration should account for the possibility of internal security lapses and threats.

THE FIVE BASIC FIREWALL DESIGN PRINCIPLES:[3]

- Develop a security policy
- Create a simple design solution
- Use devices as they were intended
- Implement a layered defense to provide extra protection
- Consider solutions to internals threats that should be included in your design

KEY COMPONENTS

The main component of a firewall includes either a physical, virtual or cloud-based appliance. This appliance allows or denies traffic, provides Virtual Private Network (VPN) access used to protect users connecting to the internet in public places and routes traffic as needed. Additional features of a firewall include Intrusion Detection Sensor (IDS)/Intrusion Prevention Sensor (IPS) or a Unified Threat Management (UTM), content filtering and malware protection.

Like many software systems, firewalls themselves have been migrating to the as-a-service business model, which can incorporate implementation and upgrades to adapt to the threat landscape as part of a nominal ongoing cost.

FEATURES TO LOOK FOR IN A FIREWALL PROVIDER:

- Internet connection support
- Wireless support
- Antivirus
- Intrusion prevention service (IPS)
- Web filtering
- Reporting
- Virtual private network (VPN)
- Technical support

USE STUDY:

DETROIT PUBLIC LIBRARY

An invaluable public institution of the state, the Detroit Public Library (DPL) bridges the digital divide in the community with over 700,000 visitors signing into their computers yearly. Open accessibility to the public creates the need for a strong and versatile firewall service.

Merit's Managed Firewall can be used as a bundled service with internet, which provides fully reliable uptime with dependable stability. The 3 x 5 Rule for Funding allows for Category 2 fund savings for the Detroit Public Library. Further costs for firewall service are reduced by 25% when using a Fortigate 37000 HA by Fortinet.

Confident in its ability to meet their legal and regulatory requirements, the Detroit Public Library can enjoy a more robust capability for protecting its 334,000 DPL Card Holders from an ever-increasing range of online attacks and inappropriate content, using Merit Managed Firewall as a security solution.

Adding in quote by Victor from DPL

Onsequod icidel eosaped ut et est repudae dolupicabo. Enderum aspero mo quias nones esti conecusamus cum adi ulpa quis peria quunt

WHY MERIT?

When buying a firewall system you must consider the equipment, manpower and the continuous support that is needed. The price for a managed firewall will vary depending on device type and organization size.

For organizations of any size and budget, Merit has a managed firewall service that will fit your needs. From the high value, low-cost solution to the powerful next generation firewall, you can be assured that unauthorized access to your network is blocked and your vital data is kept safe behind this first line of defense.

Some self-managed solutions have been found by other organizations to be cost-prohibitive, and can still require equipment on site for users to manage, that Managed Firewall doesn't. Not every organization has the same on-site expertise or faces the same landscape of security threats. Things to consider when comparing self- managed vs. a managed service are: equipment, employment and contracting needs, as well as the ongoing maintenance and upgrade costs.

As a fully managed service, we take care of the installation, configuration and maintenance. Merit Managed Firewall offers flexible billing options and is backed by our 24x7 hyper-local support. Managed Firewall can be custom tailored to your organization – offering everything you need and nothing that you don't, to provide the best protection at a cost-conscious price. **Merit managed firewall is e-rate eligible for schools and libraries.**

REFERENCES

1. https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work

2. https://www.mtg.im/the-best-firewall-router-for-a-small-business/)

3. http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Design/