Firewall Security Update

Technology with Integrity

By Tim Torian, Torian Group, Inc.

Summary:
A network firewall protects your computers and network from everyone on the internet. Investing in a good firewall helps protect your data. We recommend a Fortigate firewall for optimum security.
Network monitoring software can use network traffic logs to alert you of any unusual activity and provide the tools to catch problems before they spread. We recommend Auvik monitoring software.
Segmenting your network by separating less secure devices from your business network reduces the risk of network compromise.

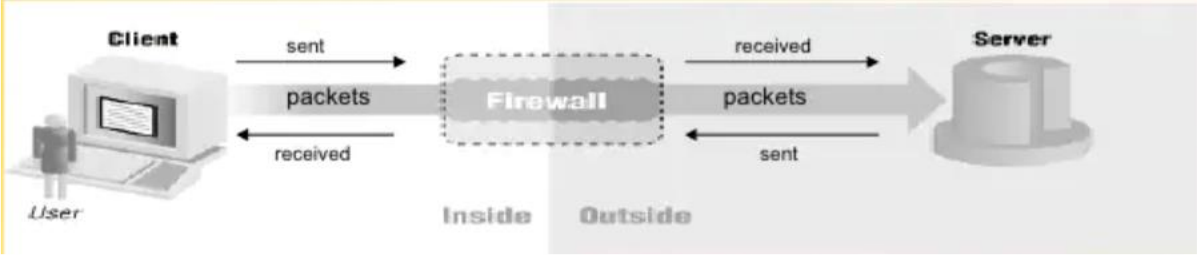
The Risk

Criminals, hackers, and now governments use automated network scanning tools which constantly search the internet for computers or networks with open connections that they can exploit. You can watch these attacks in real-time on the FireEye Cyber Threat Map, the Fortinet Threat Map, and others.
Once a network with any open connection is found, automated tools (often using AI) will try various ways to gain control of the device or computer that is listening for a connection. These tools can easily be downloaded, rented, purchased, or you can hire someone. Governments and criminal organizations have employees that develop their own tools and "exploits".
In addition, malware delivered via email or web browsing can provide a point of entry into your network by establishing an outbound network connection.
If access is gained, various tools can be used to gain further access into the network server(s). If possible, this activity will be hidden, allowing long-term control of your assets.
This access can then be sold off or used as a base for other attacks. Or the attacker may target you directly: gather financial logins, collect identity or credit card data, install ransomware, or trick you into giving away assets or transferring money. If you hold financial data for clients, you are a prime target.

The Benefits of a Good Firewall

Cyber-insurance agencies require that insured companies follow basic security practices to prevent ransomware and security breaches. These include protecting your network. Security best practices include a "next-generation" network firewall, "intrusion detection," and having a log of network activity. Many companies are required to follow specific security "best practices" by law. This includes PCI-DSS requirements for those that process credit cards, IRS requirements and GLBA requirements for CPAs and financial firms, and HIPAA requirements for health practitioners.

How a firewall works



Computers send “packets” of information between each other to transfer information. It is like a very fast postal system. The packets travel one way – to or from a device.
The firewall inspects the “from” and “to” address, and then decides if it is allowed to pass. When you connect to a web page, the firewall remembers that you sent packets out to that address and allows the packets back in if they are a response to your request.
More advanced firewalls open each packet and inspect the contents, then decide what to do with it.

Select the right network firewall for your needs

We recommend a “Unified Threat Management” (sometimes called next-generation) firewall if you have sensitive data or if you connect remotely to your customers or clients. These provide protection that more basic firewalls don’t.
This includes the following:

- Blocking traffic to known malicious sites or addresses using a constantly updated list (botnet filter).
- Inspecting website traffic and downloads for malware.
- Inspection of HTTPS:// (encrypted) web traffic. Malware is often hidden this way.
- Web content filtering – Blocking sites based on a rating or category.
- DNS filtering – another way of blocking known bad destinations.
- Intrusion detection and prevention – alerts for unusual activity.
- Data loss prevention – inspect for outgoing traffic with sensitive information such as credit card numbers.
- Secure VPN connections, with traffic inspection and logging
- The ability to log all traffic.
- Logging, intrusion detection, and data loss prevention can help meet compliance requirements for some companies.

There are many good UTM firewall brands. We recommend Fortigate. They perform better for the price and have received top ratings in reviews.

These firewalls have a price for the hardware and an additional annual subscription fee for the updates to the malware filtering engines, firmware, etc. Different models are designed to handle different size networks (and the amount of network traffic). Because this industry changes so quickly, you will want to budget for replacing them every 4-5 years. Prices start at about $600.

If you don't need high security, it is still a good idea to rely on your own firewall rather than the firewall built into the equipment provided by your internet provider. The Cisco RV340 is a good choice for a small network. Turn your Internet provider's firewall off and use your firewall to protect your network. This has the added benefit of isolating your business from any built-in Wi-Fi provided by your Internet company.

Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (November 2020)

1. Monitor network traffic

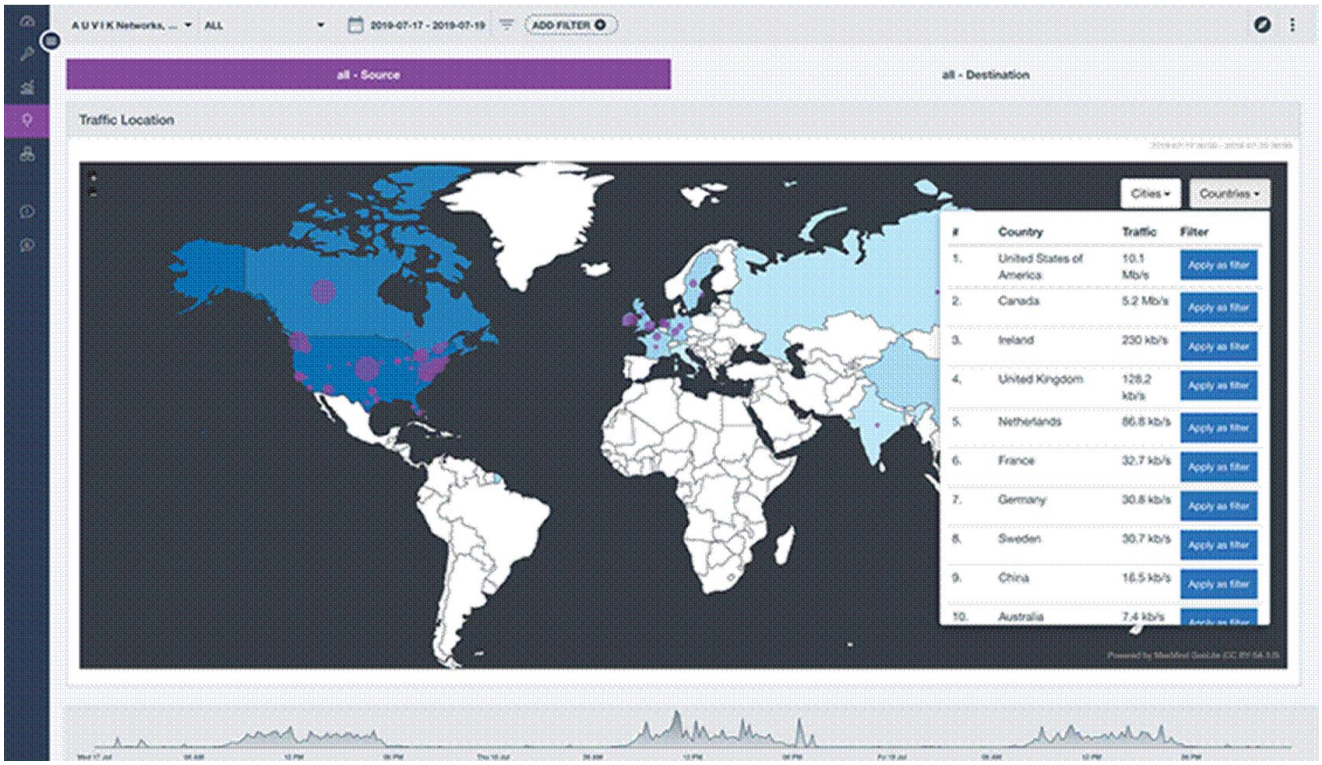
The next level of firewall protection is to send the firewall logs to monitoring software. Log monitoring can be part of an intrusion detection system (IDS). These have traditionally been quite expensive - starting at about $5,000. The goal is to filter huge amounts of logs and other data to see patterns of activity that represent a potential threat and then present the threat data in a way that can be acted upon. The IDS can be set to take action based on specific patterns, such as sending an alert.

This is why I wrote this article. We are now able to offer a reasonably priced network monitoring solution called Auvik. For clients who have an advanced firewall such as the Fortigate or Sonicwall, I strongly recommend adding this monitoring to your network. We also recommend that you purchase a next-generation firewall in order to take advantage of this service if security is a concern for your business. We are not planning to charge any extra for the additional time it takes to manage and monitor the network devices using Auvik. The additional visibility into the network makes our job easier in some ways.

The cost of the agent is $20/Month per managed router. Any managed switches on the network would also be monitored with an agent license at $20/Month per managed switch. This provides the ability to monitor the traffic down to the individual PC.

Here are some of the things we can do with Auvik network monitoring:

- Get full details on every device on the network. Provide a full network map in real-time.
- Get detailed real-time information about why your internet connection may be slow.
- Continuously monitor for network traffic to locations you should not be connecting to, such as Russia or China. This could indicate active malware.



- Identify specific computers or users that are the source of unusual or suspicious network traffic.
- Identify devices on the network that are causing problems due to hardware failure or misconfiguration.
- See patterns of network activity that are abnormal and generate an alert.
- Look back in time to troubleshoot a connectivity issue.
- Link information generated by the anti-virus software to the related network traffic to ensure malware did not spread before it was caught.
- Automate backups of router and switch configurations.

2. Segment your network

Make sure that any wireless devices that don't need access to your company data are on a separate wireless network. Keep devices that allow remote access in a separate "DMZ" network. Most routers can easily be configured for this. If you are working from home, separate your work computer from your home entertainment and smart home devices. If you have IP phones, they can be put on a VLAN network segment to improve call quality and keep them secure. Managed switches may be required to implement a VLAN. A managed switch is about double the price of an unmanaged switch, but prices have come down. For example, a 24 port managed switch is about $170.

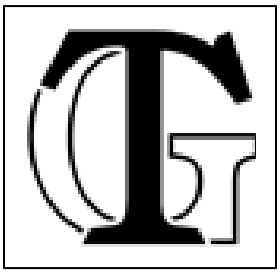
3. Enable the firewall on your computer

This is critical for laptops or tablets you travel with, important if you work remotely, and adds extra safety measures on work networks. It needs to be configured so it doesn't interfere with your work yet blocks any unwanted network connections. We can activate the firewall remotely using the managed service tools.

4. Secure your remote users

Remote work is a big topic – ask for our article with recommendations. It impacts your firewall selection because a good VPN solution works with the network firewall. The Fortigate firewall can be configured to use the same user credentials you use for Office 365. This can enhance your VPN login security with Two-Factor Authentication. You can also limit where VPN logins can come from by IP address or geographic location. A VPN can be limited to allow only remote desktop connections, further securing remote access.

Security measures work together to protect your data. Have a good firewall properly configured, keep your software up to date, provide malware protection (anti-virus), filter your email, and monitor your network to prevent or detect problems.



Tim Torian has his degree in Computer Science and has been consulting on technology for business for the past 30+ Years. He has multiple industry certifications including Microsoft and Cisco. He has taught computer networking at the College of Sequoias and Cal Poly Extension. He was awarded "Entrepreneur of the year" by the Tulare County EDC in 2008. Torian Group was awarded "Technology Business of the Year" by the SBDC in 2011. He is president of Torian Group, Inc. which provides a full range of Technology Consulting services to local business, including computer services and network design. www.toriangroup.com