SMARTFILE

Protecting the Perimeter:
A Guide to Using Next Generation Firewalls to Safeguard Your IP

By: Nick Espinosa | November 2016

Let the Right One In: Protecting the Perimeter

Perimeter defense is one of the most important aspects of securing a network. In the most classic sense, the perimeter is the defender of the internal network against the rest of the Internet.

This definition, as we shall see, is changing. Traditionally, the perimeter is protected by a firewall that filters all external traffic before it is allowed into the private network. More recently there have several advancements to firewall technology and how we view the perimeter of a network.

Today's modern firewalls, known as a Next Generation Firewalls (NGFW), offer significantly more protection and are designed to keep pace with the ever-changing landscape of threats that can harm networks. When talking about perimeter defense, this is an excellent place to start.

The NGFW and Keeping Ahead of the Threats

At its core, an NGFW has several technologies built into its firmware and hardware that help to proactively identify and handle potential threats and attacks. Some of the major "must-haves" for an NGFW include:

Detection Antivirus

The best way to defend computers and servers on a network from infection is to stop the infection before it can even touch the systems. NGFWs will do this by attempting to detect and stop incoming viruses before they can enter the network, as well as scan outbound traffic to stop any infected computers from trying to phone home to the origin of the infection. Antivirus in an NGFW is incredibly more effective than a traditional antivirus scanner installed into a computer, providing the NGFW has all of the points listed here.

Zero Day Updating

This is essential to maintaining an up-to-date and secure perimeter defense. Zero Day basically means that the maker of the NGFW will detect a new infection in the Internet somewhere in the world, and within 24 hours will have written an inoculation for it. The inoculation will be pushed to the NGFW to keep it up-to-date on the latest and newest threats. The top-tier NGFWs have an average turnaround time of a few hours at most, well exceeding the Zero Day standard, and the best of the best is currently averaging around 11 minutes from detection to inoculation worldwide.

Unified Threat Management (UTM)

This is a blanket term for a firewall that gives the IT staff a quick overview of all threats and issues that the firewall detects and encompasses managing the technologies listed below.

Intrusion Prevention System (IPS)

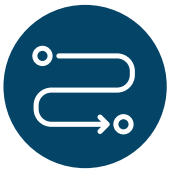
An IPS examines network traffic for patterns and flow to detect and prevent vulnerability exploits. Not all incoming threats are viral in nature. Some are looking to exploit weaknesses in the NGFW or a system. A good IPS will detect these unique threats and shut them down.

Application Whitelisting

An NGFW with Application Whitelisting integration goes a very long way to preventing rogue or malicious applications from being used. The easiest way to explain Application Whitelisting is by example.

Assume that the only three applications allowed to be used in a network are Microsoft Word, Adobe Acrobat and Microsoft Excel. An NGFW will see that traffic from these three applications are allowed and will let the traffic through while still scanning it for potential threats.

If someone on the network tries to use PowerPoint, the NGFW will see that this is not an application that is allowed and simply block the traffic. In this manner, if a person becomes infected, then that virus is seen as an application and because its traffic signature is not one of the three approved applications, the NGFW will simply shut down the traffic, thus not allowing the virus to phone home.



Sandboxing

As part of the analysis for Zero Day Updating, virus and IPS inoculations for new threats, the sandbox is very critical. It is the actual technology that allows the NGFW maker to detect new threats rapidly. Sandboxing can be done both on-premises and virtually. All NGFW, with a few notable exceptions, offer a cloud version that links directly to the firewall.

How it works: a new, unknown threat is detected by the NGFW. Instead of the letting this unknown traffic into the network, the NGFW will stop the traffic and redirect it to the sandbox.

The sandbox will then let the unknown traffic run as it normally would so it can analyze the behavior. If it's not a threat, then the traffic can be rerouted back to the computer or server that made the original request. If it is determined to be a threat, the inoculation process begins and new antiviral definitions are created and pushed to the NGFW so it can more effectively block this kind of traffic in the future.

An Independent Management Plane

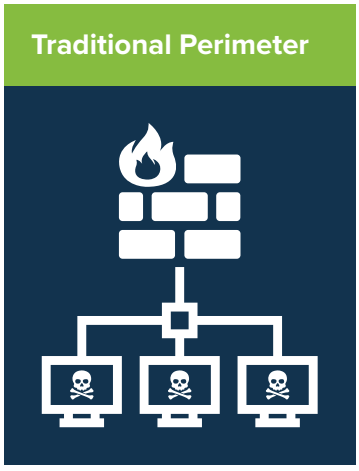
This is one many do not think about, but it's very critical. Basic firewalls use the data plane to both manage the hardware and also route the live traffic. This works fine except when the firewall is under attack and the entire firewall's processing power is consumed in fending off the attack.

A good NGFW will have an independent management plane that is separate from the data plane. This way, if the NGFW comes under very heavy attack, the IT personnel can still log into the firewall without interruption to manage the attack live without losing connection. Not all NGFWs have this and it's very important to know if the NGFW under consideration for purchase does indeed have this feature.

All of the above is the most effective way to protect a traditional perimeter from Internet-based external threats. The proper equipment will proactively stop the latest kinds of attacks and threats and will vastly mitigate the surface area for attack of the network as a whole.

Redefining the Perimeter: The Zero Trust Network

Lately, the cybersecurity world has been taking a new approach to what we call the "perimeter" of a network. In the most classic sense, an example of a traditional perimeter would be 10 computers connected together on a local area network and protected from the Internet by a firewall.

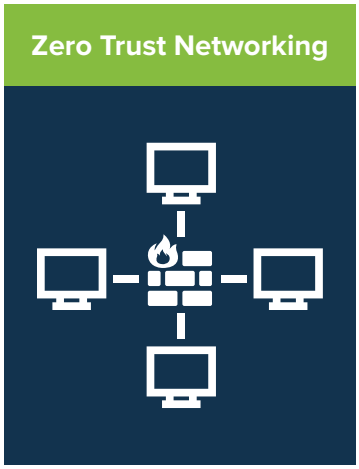


Everything on this local area network that is behind the firewall is automatically authenticated to talk to one another. Newer infections will not only infect the initial computer but also other computers within the authenticated perimeter. Therefore, a traditional perimeter does nothing to prevent internal outbreak of infection like ransomware or other malicious activity that threaten your IP.

Historically, we've installed antivirus software or enabled user policies to help mitigate spreading infections within the perimeter, but as I've written about before, these traditional methods are very inadequate and leave many holes open in the defensive posture.

Redefining the Perimeter: The Zero Trust Network

To combat this growing issue, cyber security experts such as myself, are turning to the Zero Trust networking model developed by Forrester. In a fully implemented Zero Trust environment, each computer, server, printer, device and anything else that is on the local area network becomes its own perimeter at the infrastructure level.



In other words, each computer's traffic flows through an NGFW before it can do anything, including talk to other computers on the local area network. Because the NGFW is the best defense and antivirus money can buy, an infected computer on a local network has virtually little-to-no chance of spreading the infection to the other computers within the network.

In this way, we have removed the defense of the computer on the network from inadequate antivirus software installed locally to its own high-end infrastructure defense. No computer trusts another computer and must validate itself before being able to communicate.

This helps prevent hackers or other intruders from acquiring your IP, whether they're trying to steal someone's password to comeback later or use malicious code to upload data to a remote server.

Companies that have implemented a perimeter-based on the Zero Trust model do not have to worry about intrusion or infection because the chances of infection, let alone outbreaks on the network, are so incredibly low. Anecdotally, every network I've seen with the Zero Trust model properly implemented has never had an infection. Not even a pop-up.