Network Perimeter Defense

"The Perimeter Is Dead" Should Be Laid To Rest

August 2014

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

Introduction

Over the next year, EnergySec will be releasing a series of white papers, technical documents, and how-to articles focusing on the topic of perimeter security. The series will examine the types of information that should be collected from firewalls and other perimeter security devices, how to make sense of the information that is collected, and common mistakes in the implementation of perimeter defense devices. The purpose of the series is to share tips and best practices about how to setup and manage a network perimeter. As you read the series, we hope that you can take away both an overview of what a network perimeter is and how to improve your organization's perimeter defenses, as well as specific ideas for how you can best manage your perimeter defense.

A recent survey by TripWire found that 'too much data' was a key limiting factor in companies' ability to detect breaches. As their Chief Technical Officer said about the report, however, "…the bigger issue is that most organizations are ignoring the foundational security controls needed to run a secure infrastructure. Organizations must shift their focus from hoping they will notice breaches 'in the moment' to reducing their attack surface through configuration hardening and proactive vulnerability management."[1] Proper perimeters are not yet a ubiquitous art.

Although the concept of perimeter security is not new, it must evolve to meet the changing threat landscape. For example, the concept of the "perimeter" is no longer just a prevention boundary, but also a detection boundary. This underscores the point that firewalls alone are no longer enough. Devices to monitor and protect the perimeter of a network now include Virtual Private Network (VPN) concentrators, Intrusion Detection and Intrusion Prevention System (IDS/IPS) solutions, advanced threat detection, mail and web filters, and proxy servers. Also, perimeters are not just for the internet boundary anymore. Networks used for operations, supervisory control and data acquisition (SCADA), and control systems need to be protected from less trusted business networks, and partner networks.

Perimeter security is a rich topic with many subplots. We look forward to an extended period of exploration and explanation as we support industry's forward progress on this important issue. We begin with a rebuttal of the assertion of the perimeter's demise. A reported death which is no doubt, as Mark Twain might say, "greatly exaggerated."

Executive Summary

Every month, it seems there are reports that the perimeter model of cybersecurity is no longer an adequate way to defend a network. At the Gartner Security and Risk Management Summit 2014, Gartner analyst Joseph Feiman said, “Stop investing endlessly in perimeter security--teach applications to protect themselves.”[2] That isn’t the first time that has been said. Jason Hiner of Tech Republic wrote an article in 2007 about how security experts were trying to “disabuse [him] of the notion that network security is even relevant any more.”[3] Even employees of Juniper Networks, a major vendor for firewall security, have written that traditional perimeter security is dead.[4]

Most of the people saying that perimeter defense is dead are overhyping the point they are trying to make, or trying to sell you something.

The fact of the matter is, most of the people saying this are overhyping the point they are trying to make. The Technical Trainer from Juniper, Stefan Fouant, even said in a comment after his article that he isn’t advocating getting rid of firewalls, but rather making the point that a firewall isn’t good enough, on its own, to provide effective security. Or, if they’re not legitimately trying to make a point, but using excessive language, they are trying to sell you a product. Thevi Sundaralingam was quoted in an article at darkreading.com as saying, “Perimeter security is no longer relevant to enterprises. With the mobilization of the workforce, it's very hard to define the perimeter of any organization because mobile-enabled employees are connecting to the network from all over the world on devices of their choosing. Next-gen security needs to focus keeping content safe, not on defining a network perimeter." The article says that Sundaralingam works for Accellion, but what the article doesn’t tell you is that Accellion is in the business of selling a “secure Dropbox alternative.”[5] In other words, he’s in the business of trying to sell a product which touts security while ignoring the idea of network perimeters.

When used appropriately, perimeter defense provides many benefits to an organization.

The notion that the idea of a network perimeter is dead, itself needs to be laid to rest. There will always be a router or a firewall in place on your network. Even home networks use routers with access control list capabilities. Does the idea of “the perimeter is dead” mean we’re not going to implement any firewall rules? The device is there, it might as well be used. And, when used appropriately, it can provide many benefits to your organization. There is a great point to be made that we can think of a network as being many smaller networks, with security at each place the networks intersect. But, just as the Transportation Security Administration (TSA) does their primary screening at a central location in an airport instead of at each individual gate, computer networks have central points where it makes sense to perform security checks. This is a good idea which never gets old.

Overview of Cybersecurity Frameworks

NIST Cybersecurity Framework

A basic fact that confirms perimeter defense as an integral part of network security is that various regulatory and management frameworks demand it. Many utilities have to comply with cybersecurity requirements of some kind, and these typically include perimeter protections. The most common frameworks all make reference to perimeter defense. The National Institute of Standards and Technology (NIST) Cybersecurity Framework makes perimeter defense an integral part of both the Protect and Detect Functions.[6] For example, PR-AC.5 says, "Network integrity is protected, incorporating network segregation where appropriate," and PR.PT-1 says, "Audit/log records are determined, documented, implemented, and reviewed in accordance with policy." Both of those, and other subcategories from the Protect Function, touch on or deal directly with defining and defending a network perimeter. In the same way, DE.CM-7 says, "Monitoring for unauthorized personnel, connections, devices, and software is performed," and DE.AE-3 says, "Event data are aggregated and correlated from multiple sources and sensors."

NIST SP 800-53 R4

In the same way, the NIST Special Publication 800-53 R4 incorporates the ideas of perimeter defense into its framework.[7] The two largest security control families are System and Communication Protection and Access Control, which both deal specifically with perimeter defense. While these controls are generally mandated only for federal government entities, they are often used as guidance, and the amount of space given over to perimeter defense serves as a reminder of its importance.

NERC CIP Standards

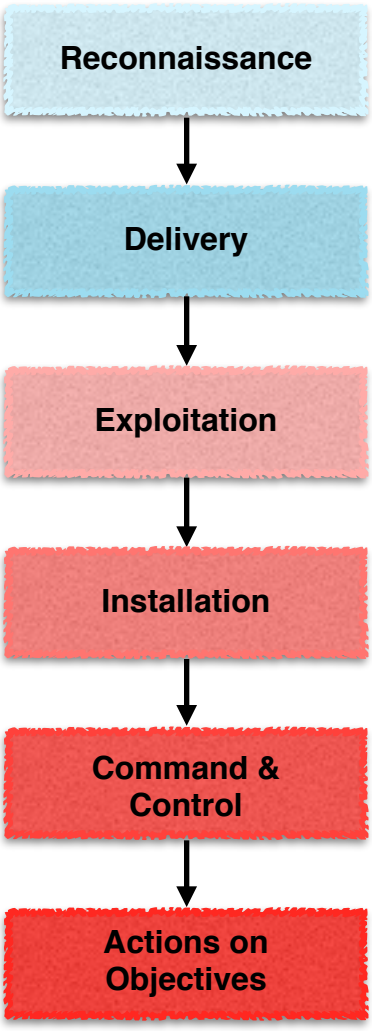
Specifically for the electric industry, though, the NERC CIP standards also address perimeter defense.[8] CIP-005-3a "requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter." Version 5 of those standards adds in a requirement to detect malicious communications, both inbound and outbound. This implies a need to know a baseline of what is normal traffic and what is not, and requires the creation and maintenance of a network perimeter.

SANS Critical Security Controls

There is always a concern that compliance with regulations is not the same thing as implementing the best security possible. That is not the case here, however. In the SANS Critical Security Controls, which are a collection of best practices rather than a set of regulations, a full 30% of the Controls deal with network perimeter defense.[9] CSC 13 specifically talks about perimeter defense, and CSCs 1, 5, 10, 14, and 17 also deal with perimeter defense in some way.

Perimeter Defense and the Kill Chain Model

The Kill Chain Model the various phases of an attack progressing from reconnaissance all the way through the actions and objectives of the attacker. The tools and techniques of perimeter defense can disrupt the Kill Chain at every level.[10] Also, the earlier in the kill chain at which the attack can be disrupted, the less likely it is that the attack will lead to a successful data breach or disruption of service.



Reconnaissance

In the reconnaissance stage, Network Intrusion Detection Systems (NIDS) and router logs can detect intrusion attempts. At the same time, Firewall Access Control Lists (ACLs) can deny entry to your network.

Delivery

At the delivery phase, NDIS can again detect attempts by recognizing malicious payloads as they are entering the network. Mail and web filters can deny or disrupt attempts to deliver the malicious payloads.

Exploitation

During the exploitation phase, NIDS can again detect attempts at exploiting systems on your networks. Also, Network Intrusion Prevention Systems (NIPS) and antivirus systems are able to deny and disrupt exploitation attempts.

Installation

Antivirus can also be effective during the installation phase, as it can detect and disrupt attempts to install malware. Even more effective, application whitelisting can deny attempts to install the malicious applications.

Command & Control

During the C&C phase, NIDS and antivirus solutions are able to detect attempts to connect to a C&C server. Egress filtering and firewall ACLs are able to deny those attempts. Firewall session and connection tracking is extremely helpful in monitoring traffic that is allowed in or out, which can help to detect when an infected host is attempting to connect to a C&C server.

Actions on Objectives

An example, in the energy sector, of an objective is to sabotage ICS systems. NIDS and antivirus can detect attempts to achieve a malicious actor's objectives. Firewall ACLs and network segmentation can make it possible to deny those attempts. Network segmentation

can also disrupt or degrade the attempts at objectives, even if they do not deny them completely. In the case of a data breach, egress filtering can also prevent the data from leaving the network.

Top Six Reasons to Focus on Perimeter Defense

1. It's Common Sense

If you lived in a dangerous neighborhood, you wouldn't want to leave your doors and windows unlocked, or, even worse, open. That would make it likely that somebody would walk in and take your TV, your kids, or other possessions. Likewise, the Internet is not a safe place to leave your network open and exposed. Another analogy would be that of a military base. They have a security perimeter, where visitors and intruders are stopped, questioned, or detained. They also have protocols for how to raise an alarm if a malicious intruder does attempt to infiltrate the base. Those security precautions are what allows a soldier to sleep at night without having to worry about having to be alert and with a weapon ready at all times.

2. Harden Yourself, and Attackers May Target Somebody Else

Attackers often want to find the easiest targets. Some attackers may not even care who they are attacking, just as long as they can attack somebody. In those cases, the more you harden your defenses, the more likely they are to go after somebody else. For example, ICS-CERT recently disclosed a cyber intrusion on a public utility.[11] The attack was the result of brute-force guessing of a password on an Internet-connected control system device. That level of attack could be neutralized if appropriate perimeter defenses were in place.

3. Use Network Segmentation to Protect Sensitive Data

The idea of a perimeter can be extended to encompass many "little perimeters" around sensitive data, user groups, or control systems. This allows security controls to be put into place which can protect those resources. For example, the Target breach happened as a result of a vendor having access to part of their network, and the attackers using that access to pivot into more sensitive areas of the Target network.

4. Egress Visibility Allows You to See if a Breach is Occurring

Egress visibility, or using the perimeter to inspect data which is leaving your network, is an important part of detecting when an attack has occurred. For example, session tracking could be monitored and it could be seen if a port has had an open connection for an extended period of time to a random IP address. This visibility would allow you to investigate that further, and possibly stop a data breach as it is happening.

5. Protect Your Company From Liability

By not following recommended cybersecurity measures, you face criticism and fines after a data breach. For example, Wyndham Hotels suffered three data breaches in two years, and a federal judge recently ruled that the Federal Trade Commission can pursue fines against them for acting “unfairly” by failing “to provide ‘reasonable’ measures to secure customer data.”[12]

6. Security at the Perimeter can be More Persistent

In this era of BYOD and shadow IT, it is unrealistic to expect every device which is connected to your network to have its defenses correctly and adequately configured, including with a firewall. Many end-users have the capability to turn off security controls at their devices, and for many reasons, both good and bad, they do turn off or bypass security features. Turning off security controls at perimeter devices, however, usually (should) require a change management process, which makes it more difficult to bypass security controls on the perimeter devices.

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

[1] “How fast can security pros detect a breach?,” Help Net Security, 12-Aug-2014. [Online]. Available: http://www.net-security.org/secworld.php?id=17244

[2] E. Messmer, “Will perimeter firewalls give way to ‘RASP’?,” Network World, 23-Jun-2014. [Online]. Available: http://www.networkworld.com/article/2365739/security0/will-perimeter-firewalls-give-way-to-rasp.html

[3] J. Hiner, “Is perimeter security dead and is protecting the data all that matters?,” TechRepublic, 24-Aug-2007. [Online]. Available: http://www.techrepublic.com/blog/tech-sanity-check/is-perimeter-security-dead-and-is-protecting-the-data-all-that-matters/

[4] S. Fouant, “Reality Check: Traditional Perimeter Security is Dead,” 08-Aug-2011. [Online]. Available: http://forums.juniper.net/t5/Security-Mobility-Now/Reality-Check-Traditional-Perimeter-Security-is-Dead/ba-p/102952

[5] http://www.accellion.com/

[6] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[7] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[8] http://www.nerc.com/files/cip-005-3.pdf

[9] http://www.sans.org/critical-security-controls

[10] C. Sanders, “Making the Mandiant APT1 Report Actionable,” Applied Network Security Monitoring, 19-Feb-2013. [Online]. Available: http://www.appliednsm.com/making-mandiant-apt1-report-actionable/

[11] “ICS-CERT Monitor,” ICS-CERT, Apr-2014. [Online]. Available: http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf.

[12] J. Furtsch and S. Nayak, “FTC v. Wyndham – What Does it Mean for Your Data Governance Programs?” TRUSTe Blog, 19-Apr-2014. Available: http://www.truste.com/blog/2014/04/18/ftc-v-wyndham-%E2%80%93-what-does-it-mean-for-your-data-governance-programs/