Four Tips for Designing a Secure Network Perimeter

www.securityweek.com/four-tips-designing-secure-network-perimeter

By Nimmy Reichenberg on September 26, 2013

As the first layer of defense in your network, it is important to take a step back and review the design of your perimeter security. To ensure a sound architecture, you want to start with what ultimately must be protected and then design your perimeter security so it can scale as your needs grow/change. Since the threats you know about and face today may not be the ones you face tomorrow, you want to be sure your design is flexible enough to meet future needs.

Think of your network perimeter like a castle during medieval times, which has multiple layers of defense – a moat, high walls, big gate, guards, etc. Even in medieval times, people understood the importance of having layers of security and the concept is no different today in information security. Here are four tips:

1. Build layers of security around your castle

No defense is 100% effective. That's why defense-in-depth is so important when it comes to building out your security. The traditional first line of defense against attacks is typically the firewall, which is configured to allow/deny traffic by source/destination IP, port or protocol. It's very binary - either traffic is allowed or it's blocked by these variables. The evolution of these network security devices has brought the Next-Generation firewall, which can include application control, identity awareness and other capabilities such as IPS, web filtering, advanced malware detection, and more baked into one appliance.

Whether or not it's part of your firewall or a separate device, IPS is another important perimeter defense mechanism. Having your IPS properly optimized and monitored is a good way to catch attackers that have slipped past the first castle defense (firewall/router).

The popularity of moving more into the cloud has brought cloud-based malware detection and DDoS services. Unlike appliance-based solutions these are cloud-based services that sit outside your architecture and analyze traffic before it hits your network.

2. Harden your device configurations, software updates and security policies

Here is where we start building those walls to prevent attackers from getting inside the castle. The first line of defense typically involves network security devices such as routers, firewalls, load balancers, etc. which each act like the guards, gate, moats, etc. of long ago.

For each layer of security, you want to ensure they are running the most up-to-date software and operating systems, and that devices are configured properly. A common misstep occurs when organizations assume they are secure because of their many layers of defense, but a misconfigured device is like giving an attacker a key to the castle. Another important practice is to tighten security policies (of course without impacting the business), so for example you don't have a router allowing ANY to Telnet to it from outside your network.

3. Enable secure network access

While firewalls, routers and other security layers are in place to prevent unauthorized access, they also enable access that is approved. So how do we let authorized personnel into the castle? The drawbridge of course! Next-generation firewalls can help here by scanning inbound and outbound user traffic, all while looking for patterns of suspicious behavior.

Another way to have secure access from the outside through the perimeter is to install a VPN that is configured to allow encrypted communication to your network from the outside. Utilizing two-factor authentication with a VPN contributes towards ensuring the integrity of the users making the request. This is external-facing to your network and allows users to tunnel into your LAN from the outside once the appropriate measures are taken to secure access.

4. Create and segment the DMZ

If firewalls, routers, web filters, etc. are the guards, moat, gate, walls of a castle, then the DMZ is like the courtyard once inside the castle – another area before you can get to the private quarters.

When creating a DMZ, there should be at least a front-end firewall for the external traffic and a back-end firewall for the internal traffic. Firewall rules should be optimized and tightened on all publicly available systems to allow traffic to only the necessary ports and services living within the DMZ. From an internal perspective you also want to limit who can access systems within the DMZ. One approach is creating firewall rules to only allow the source IP addresses and port to the specific server and then adding proxies in the network from which administrators are allowed access to the systems. You can also place authentication on the LAN before access to the DMZ is even attempted. This prevents allowing complete control over these systems at any given time.

Segmenting systems within the DMZ is also something to strongly consider so that if a system is breached in the DMZ, it can't spread as easily. For example, you don't want a web server passing data to an application or database server in a "public DMZ". Configuring systems within different VLANs (with a layer 3 switch) will help you isolate and respond to incidents if a server in a DMZ is compromised.

A sound network security perimeter architecture requires multiple layers of defense, up-to-date and hardened policies and controls and segmentation. All of these things make it harder for an attacker to gain access to your crown jewels and easier for you to isolate and respond to breaches when they occur. Good luck!

Nimmy Reichenberg is the VP of Marketing and Strategy for AlgoSec, a solution provider for Network Security Policy Management. Nimmy began his career as a security software engineer and has spent the last 10 years working with organizations across the world to address their security needs, focusing mainly on mobile device management and network security. He holds a B.Sc. in Computer Science and an MBA from Tel Aviv University.