Adam Gray

CSCI 4957-203

11/16/17

The Need for Internal Firewalls: Why a Perimeter Firewall Just Isn't Enough

Often, there is a misconception among professionals and students alike in the field of Information Technology that firewalls are simply a "gate" of sorts that should be placed at the perimeter of the network to keep unwanted things out, private things in, and nothing else. This, however, could not be further from the truth. Albeit, in certain scenarios with a very simple network setup, little to no users, and no important resources to protect, a simple perimeter firewall very well may do the trick and provide adequate security. For most organizations, however, this is simply not the case. While a perimeter firewall is assuredly necessary, an internal firewall structure is equally important due to differing security requirements between subnetworks, the need to protect the local network from outside-access machines, and the necessity to contain breaches locally.

There are some easily-thought of purposes for internal firewalls. Among these, however, is not the idea of protecting internal subnetworks from other internal subnetworks. This may seem like an odd concept, initially, but it very quickly begins to come into focus as we dive deeper into the subject. Many software or IT-related organizations incorporate test networks into their network structure. These are generally used as sandboxes to test the effects of developmental software, viruses, or potential network changes. These tests are carried out on the test network to avoid damaging or disrupting any components on the main network. This is not a very effective means of protection, however, if the main network is not guarded from the test network. Luckily, the firewall setup for such an issue is generally very simple. "In most cases, you'll want a packet filtering router that allows any connection inbound to the test network but only known safe connections from it," according to Zwicky, Cooper, & Chapman

(2000). This is one of the simpler setups most IT professionals will encounter regarding firewalls. Of course, there are other scenarios where the setups may be slightly more complex, such as if the test environment's purpose is for testing network bandwidth or a new router, but regardless, the need for a firewall here is very tangible. Aside from test networks, an additional need to protect internal subnetworks from each other arises from having subnetworks that require extra security. Assets such as databases housing secure information, critical servers, and more all require additional protection from the rest of the local network as well as the outside world. Specifically, an internal firewall guarding the sensitive resources could prevent access from insider threats, as well as non-employee users who may be on the network for the use of a locally-hosted public server. An added bonus of having a firewall protecting critical servers is how much easier it makes monitoring traffic to them. "Any malicious activity would be much easier to detect, since the firewall has a limited amount of traffic passing through it," Bridge (2001) states. By narrowing the breadth of traffic that is reaching the firewall, it is much easier to quickly identify any unusual activity in the case of an issue occurring. Not only does this need for separation apply to particularly sensitive resources, however, it also applies to departmental resources that simply do not need to be accessed by employees in other departments (Zwicky, Cooper, & Chapman, 2000). The best way to protect any data is by following the principle of least privilege, and it certainly applies here as well. Even aside from departmental data, different areas within an organization may also require different services and levels of security. All of these departmental issues, at the very least, suggest the use of internal firewalls to easily separate resources.

Another important issue to consider when determining where internal firewalls need to be located is outside access to the network. There are a few scenarios where an organization may allow outside entities to access its network while off-premises. One very common one, though, is in the case of simple remote-access for employees. This can be an easily overlooked security hole in the network. If a perimeter firewall is essential to keep unwanted things from getting in your network, then a firewall

between the remote-users' area of the network and the rest of the network is surely essential as well. As far as security is concerned, any remote user's machine is simply a portal to the external internet. If a remote user's computer and/or local network is any less secure than the organization's main network, an incident is more likely to occur. Any infection or breach of a remote user's computer can easily spread to the main network if safeguards aren't in place. By separating the remote resources from the main network with a firewall, you continue implementing a principle of least privilege—only allowing these users access to the necessary resources—as well as helping to prevent intrusions and the spread of worms throughout the main network. All of these ideas apply to remote offices that connect via WAN or VPN traffic as well. Although often overlooked since they are part of the same organization, smaller office locations are often much less secure, allowing them to become easy targets to gain access to the entire organization's network with. With the discussed firewalls in place, this can be greatly avoided while still allowing them access to the resources they need (Noonan & Dubrawsky, 2006). A slightly less glaring issue, but an important one nonetheless, is that of joint ventures between organizations utilizing shared resources. If the collaborating organizations are competitors, then naturally they will want to protect their resources from each other, but even aside from that, each party simply doesn't know how good the other's security is. A breach into one's network could easily cross over into the other's via the shared resources if not careful. Having the networks completely open to each other also opens up lots of room for simple errors, such as routing mistakes where data could be unknowingly sent to the other organization, where it very well may go unnoticed if they aren't closely monitoring their traffic. To protect each other from these things happening, various internal firewall configurations can be of aid, depending on needs. According to Zwicky, Cooper, & Chapman (2000), "An internal firewall limits exposure in such a situation. It provides a mechanism for sharing some resources, while protecting most of them." More specifically, a shared perimeter network may be ideal, allowing the organizations to set up the shared space as desired. Also depending on requirements and trust, bastion hosts may or may not be necessary.

The third and final need for internal firewalls I will discuss arises from security breaches. Plain and simple, if the network is breached from any given access point, internal firewalls can protect the rest of the network from being breached as well. By using firewalls to divide subnetworks by relation and necessity, we get closer and closer to the idea of distributed firewalls. While a dedicated firewall for each device is not necessary, separating groups of machines can easily localize breaches, making them pre-contained without the security team having to scramble to stop it from spreading. As everyone knows, the smaller the breach, the easier it is to clean up. More importantly, though, attackers are forced to penetrate multiple layers to reach valued assets (Bridge, 2001). Logically, mission critical servers should be guarded by firewalls to keep threats out due to their importance, but on the converse side of this, the groups of workstations, offices, etc. should all be guarded by firewalls as well to keep threats *in*. At the bottom line, internal firewalls should be used to keep threats from getting to resources. By dividing the network into somewhat closed-off blocks, this assuredly moves us in the right direction, toward the ideal network.

Although perimeter firewalls are important and necessary to create a secure network, internal firewalls very well may be more important, yet are sometimes overlooked. By adding more internal firewalls, layers of protection are created that separate critical resources from attackers. Each layer provides less chance of success for the attacker and a greater chance of containing and eliminating the issue for the security team. Due to this fact, an internal firewall structure is crucial to proper network security. Differing security requirements between subnetworks, the need to protect the local network from outside-access machines, and the need to contain breaches locally all support this necessity for an internal firewall structure as well.

Bibliography

Bridge, S. (2001, August 15). *Achieving Defense-in-Depth with Internal Firewalls*. Retrieved October 4, 2017, from https://www.sans.org/reading-room/whitepapers/firewalls/achieving-defense-in-depth-internal-firewalls-797

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2000). 6.7. Internal Firewalls. In *Building Internet Firewalls* (2nd ed.). Beijing: OReilly. Retrieved October 04, 2017, from http://www.safaribooksonline.com/

Noonan, W. J., & Dubrawsky, I. (2006). Using Firewalls to Segment Internal Resources. In *Firewall Fundamentals* (pp. 172-174). Indianapolis, IN: Cisco Press. Retrieved October 04, 2017, from http://www.safaribooksonline.com/