ACLs and Firewalls

NATHAN R. MIXON, DYLAN A. KELLY, & STEPHEN G. NJUGUNA

CSCI 352

03/18/2023

ACLs

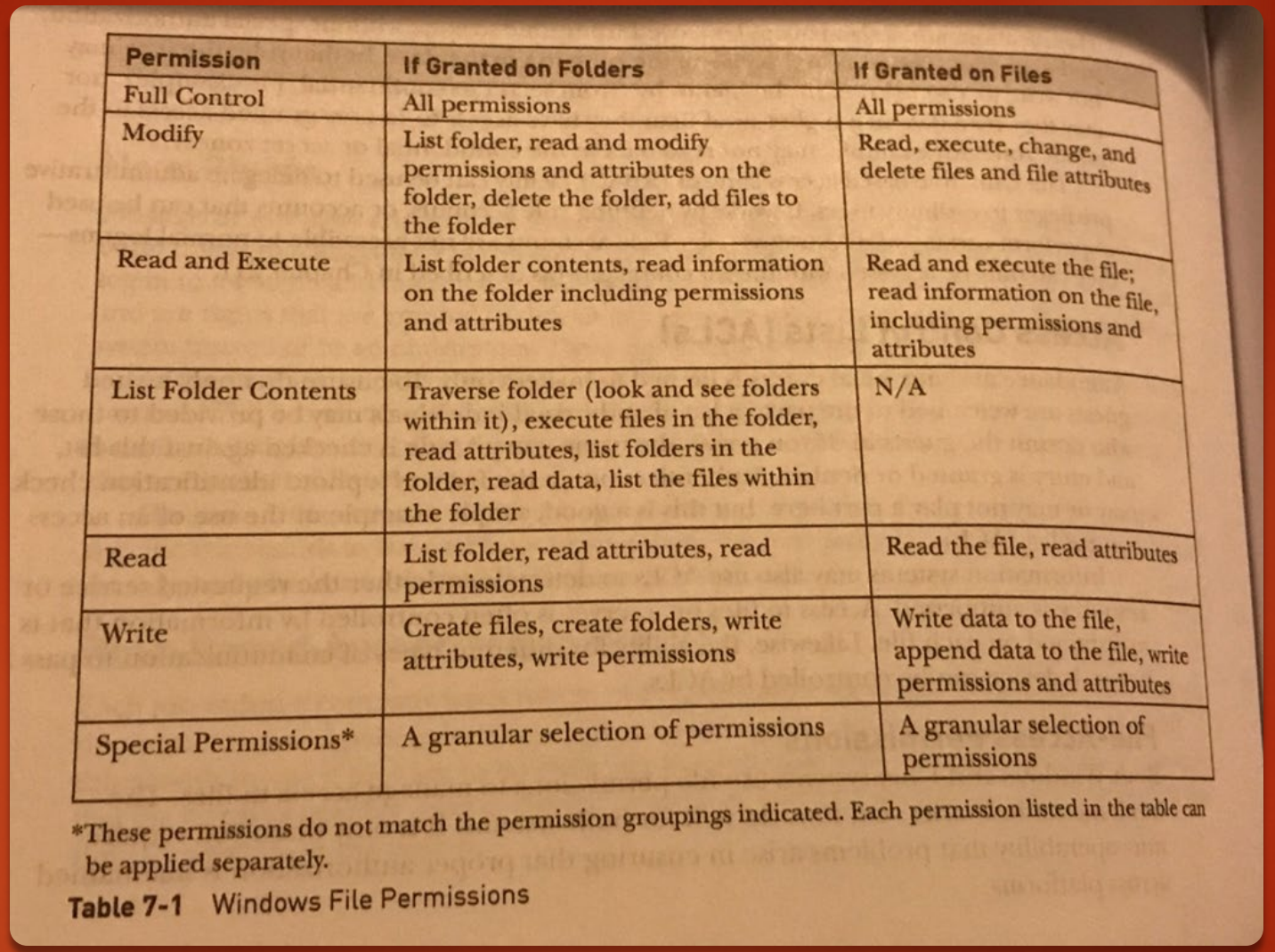
- What is an ACL?
- How do ACLs work?
- What are the advantages of using an ACL?
- What are the disadvantages of using an ACL?

What is an ACL?

- An ACL is best defined as “[a]n electronic list that specifies who can do what with an object” (Rhodes-Ousley, 2013).
- For example, an ACL on a file determines who can manipulate the file, as well as the extent to which a person can manipulate the file.
- Depending on the level of access granted by the ACL, the user can read, write, execute, delete, and further alter the file.

How do They Work? (Windows)

- For Windows systems, the ACL is made up of multiple access control entries (ACEs), and each access control entry contains a security identifier (SID) and the permissions associated with that security identifier.
- For each user, a list is made that contains the user's SID, the SIDs of the groups that the user has access to, and the privileges that the user has.
- It is important to note that in the event of a conflict between permissions (i.e. one permission allows a user to do x, while another prohibits them from doing x), the permission that is the *most restrictive* takes precedence over the other permission(s).
- In the given example, the permission that prevents a user from doing x would take precedence, meaning that the user would be unable to do x.



Permission	If Granted on Folders	If Granted on Files
Full Control	All permissions	All permissions
Modify	List folder, read and modify permissions and attributes on the folder, delete the folder, add files to the folder	Read, execute, change, and delete files and file attributes
Read and Execute	List folder contents, read information on the folder including permissions and attributes	Read and execute the file; read information on the file, including permissions and attributes
List Folder Contents	Traverse folder (look and see folders within it), execute files in the folder, read attributes, list folders in the folder, read data, list the files within the folder	N/A
Read	List folder, read attributes, read permissions	Read the file, read attributes
Write	Create files, create folders, write attributes, write permissions	Write data to the file, append data to the file, write permissions and attributes
Special Permissions*	A granular selection of permissions	A granular selection of permissions

*These permissions do not match the permission groupings indicated. Each permission listed in the table can be applied separately.

Table 7-1 Windows File Permissions

Figure 1: Table 7-1 Windows File Permissions (Rhodes-Ousley, 2013)

How do They Work? (Unix)

- Traditional Unix file systems typically protect files by limiting access by user account and group instead of using ACLs (Rhodes-Ousley 2013).
- This means that, for example, an individual cannot be given read permission in addition to the owner.
- Another example of the limitations of traditional Unix permissions is that one group cannot be given read access, while another is given write access. ACLs help remedy these limitations (Rhodes-Ousley 2013).

How do They Work? (Unix cont.)

- ACLs are used in addition to the traditional Unix file protection system.
- ACEs can be “defined on a file and set through commands”. These commands “include information on the type of entry [(user or ACL mask)], the user ID (UID), group ID (GID), and the *perms* (permissions)” (Rhodes-Ousley 2013).
- The mask permission dictates the maximum permissions allowed for users and groups, excluding the owner.
- For example: An ACL mask is set to read. An explicit permission has also been granted for write or execute permission. Despite this, the only permission granted will be read, because the ACL mask takes precedence.

Permission	File users may...	Directory user may...
Read	Open and read contents of the file	List files in the directory
Write	Write to the file and modify, delete, or add to its contents	Add or remove files or links in the directory
Execute	Execute the program	Open or execute files in the directory; make the directory and the directories beneath it current
Denied	Do nothing	Do nothing

Table 7-2 Traditional Unix File Permissions

Figure 2: Table 7 – 2 Traditional Unix File Permissions (Rhodes-Ousley, 2013)

ACL Advantages

- One advantage of using an ACL is that it is relatively simple. “An ACL clearly lays out the levels of access and permissions that each user, group, or device has on a particular system” (Hoffman, 2020).
- This means that the ACLs can be made readable and easy for a human to interpret, allowing an administrator the ability to quickly and easily determine the permissions and access controls on any given system. This also means that an administrator can easily change the ACL or remove permissions if the need arises (Hoffman, 2020).

ACL Disadvantages

- ACLs are somewhat inefficient due to the fact that “they only support explicitly declared access controls” (Hoffman, 2020).
- Additionally, the fact that ACLs must have explicitly declared access controls means that it can be challenging to upscale. An increase in users and groups means that the ACL will get longer and that the length of time needed “to determine the level of access granted to a particular user” will also increase (Hoffman, 2020).
- Another disadvantage of ACLs is that it can be difficult to track down all of the permissions and levels of access granted to a user or group. Since permissions and levels of access can be scattered across multiple lists, it can be challenging to find or change permissions (Hoffman, 2020).

Firewalls

- What is a Firewall?
- What are the core functions of a Firewall?
- What are the advantages of using a Firewall?
- What are the disadvantages of using a Firewall?

What is a Firewall?

- A Firewall is essentially a filter that "screen[s] network traffic for the purposes of preventing unauthorized access between computer networks." (Rhodes-Ousley, 2013).
- For example, a firewall may allow a user to send email but not an email with an attachment. Also, firewalls can prevent incoming and outgoing data from certain ports.
- Firewall capabilities are dependent upon the rules applied by network administrators. More complex businesses are going to have more rules. (Rhodes-Ousley, 2013).

What are the core functions of a Firewall?

- Network Address Translation(NAT) is a functionality firewalls employ to allow multiple devices on a local network to map to a public IP address before being sent onto the internet.
- Firewalls employ static NAT to rewrite IP address for outgoing and incoming packets. One example of this is internal servers that must be reached across the internet reliably on an IP address that doesn't change.
- Dynamic NAT allows a group of local addresses to map to a global address. By mapping to a global address, you can connect many hosts to the internet using the least amount of registered addresses. (Rhodes-Ousley, 2013).

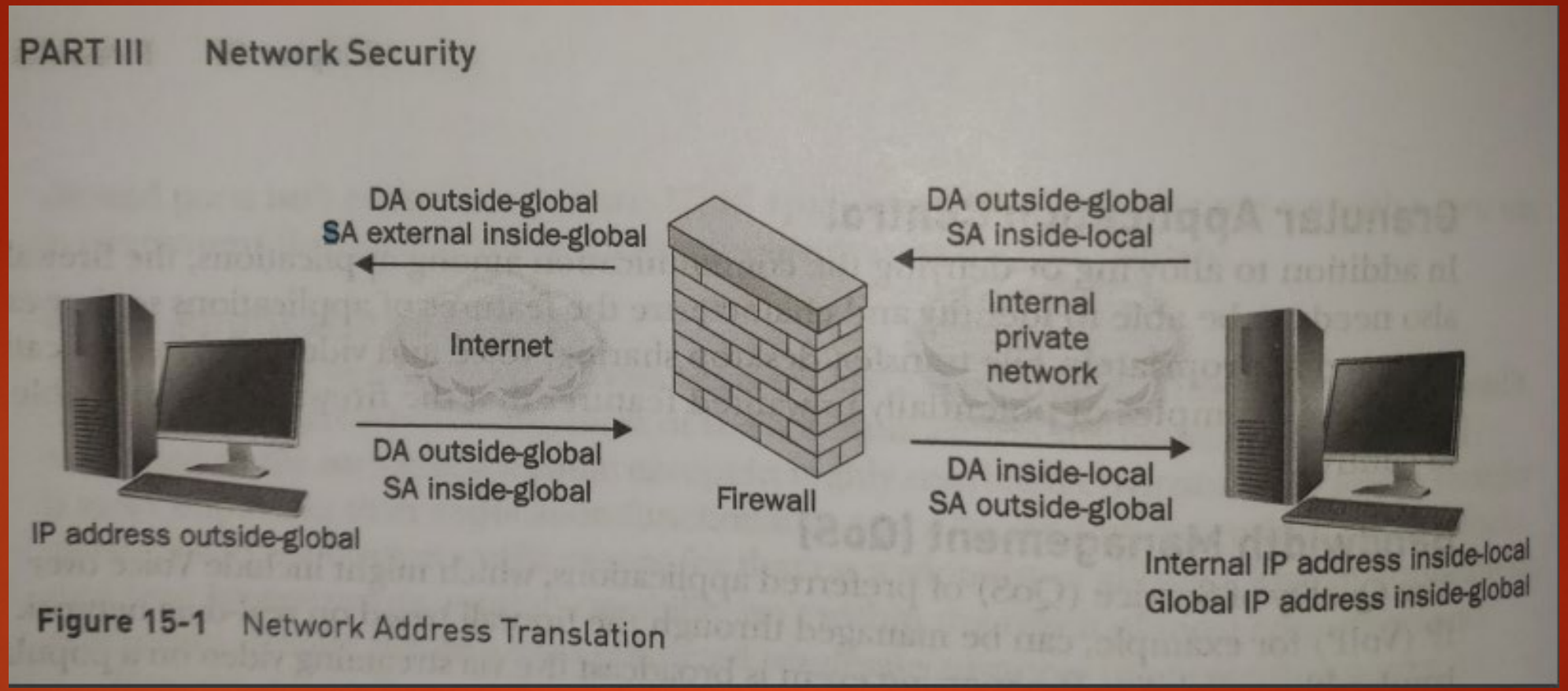


Figure 3: Figure 15-1 Network Address Translation (Rhodes-Ousley, 2013)

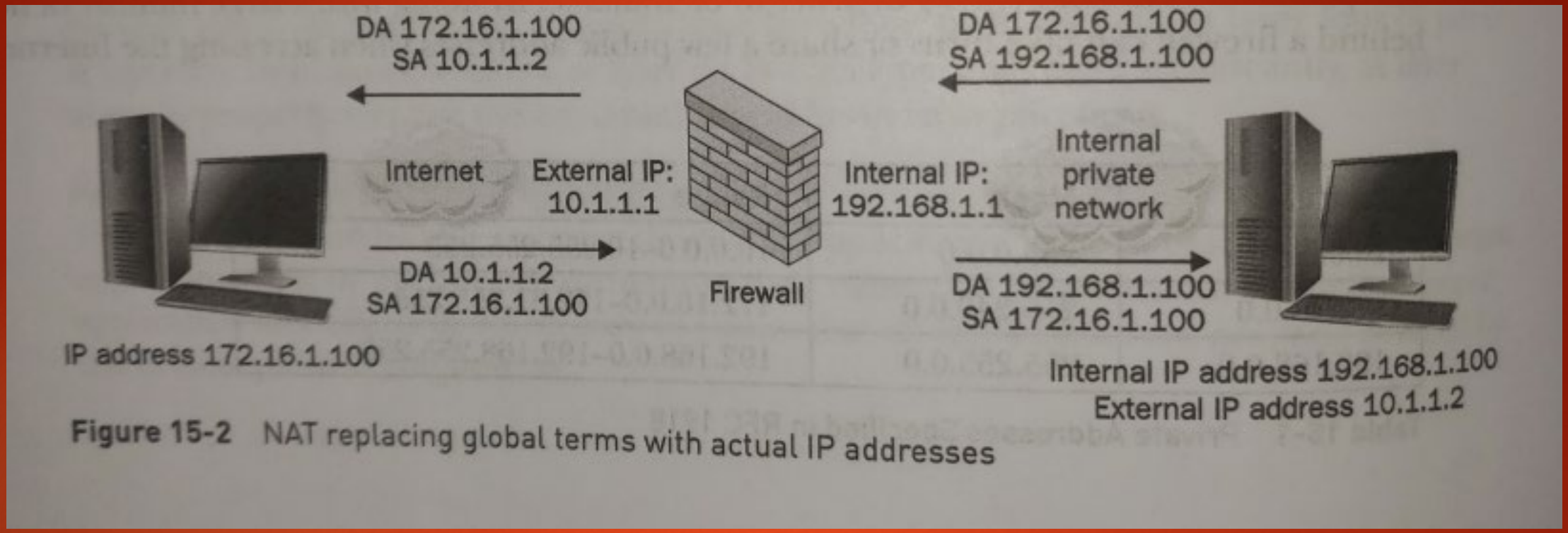


Figure 15-2 NAT replacing global terms with actual IP addresses

Figure 4: Figure 15-2 NAT replacing global terms with actual IP addresses (Rhodes-Ousley, 2013)

What are the core functions of a Firewall (cont.)?

- Port Address Translation(PAT) maps the entire local address space to one global address. To do this, the firewall modifies the communication port, source IP, and destination IP addresses. By doing so, the firewall uses a single IP address to track which ports are affiliated with which sessions.
- Firewalls are phenomenal auditors and loggers. They can record all traffic that goes through them, so it is important to monitor systems regularly. They can help administrators spot suspicious activity before a breach. (Rhodes-Ousley, 2013).

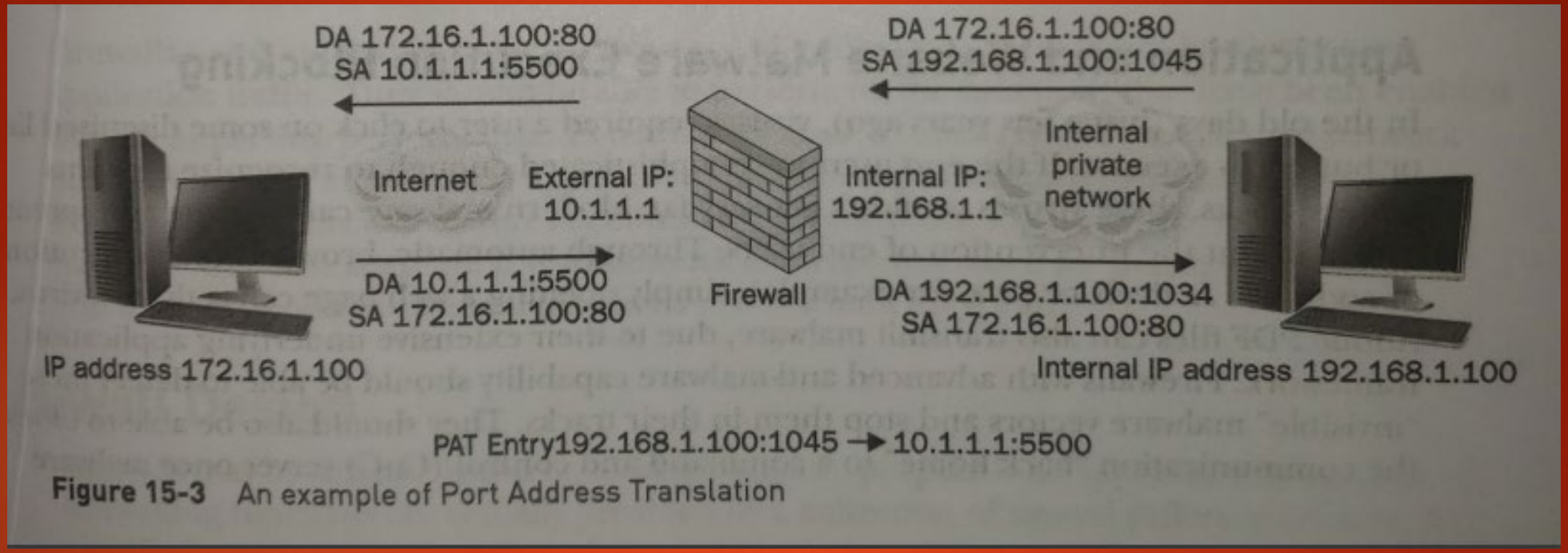


Figure 5: Figure 15-3 An example of Port Address Translation (Rhodes-Ousley, 2013)

Firewall Advantages

- Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.
- Firewalls are used to restrict access to specific services.
- Firewalls are transparent on the network—no software is needed on end-user workstations.
- Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities, they can log interesting traffic that passes through them.
- Firewalls can alert appropriate people of specified events. (Rhodes-Ousley, 2013).

Firewall Disadvantages

- Firewalls are only as effective as the rules they are configured to enforce. An overly permissive rule set will diminish the effectiveness of the firewall.
- Firewalls cannot stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.
- Firewalls cannot enforce security policies that are absent or undefined.
- Firewalls cannot stop attacks if the traffic does not pass through them. (Rhodes-Ousley, 2013).

References

Hoffman, A. (2020, April 23). Understanding the Pros and Cons of Access Control Lists. Retrieved March 15, 2023, from https://dandelife.com/understanding-the-pros-and-cons-of-access-control-lists/

Rhodes-Ousley, M. (2013). *Information Security: The Complete Reference*. Emeryville, CA: McGraw-Hill/Osborne.