



Data Security Controls TTC6010-3005

Lab 2: Security Policies and NAT

Michael Herman

Toni Peltola

Karri Päivärinta

Project report

Instructor: Jarmo Viinikanoja

Return date: 12.9.2023

Group: TIC21S1

Contents

1	Introduction	4
2	Theoretical background	4
2.1	Firewall security policy	4
2.2	DNS and NAT	4
2.3	Interzone, intrazone and universal rules	5
2.3.1	Interzone rules	5
2.3.2	Intrazone rules	5
2.3.3	Universal rules	5
2.4	Application vs service policies	6
2.5	Security profiles	6
3	Internet access from the DMZ	7
3.1	DNS setup	7
3.2	WWW connection setup	9
3.3	WWW NAT settings	10
4	RDP from WS-net to Servers-net	12
5	Conclusions	17
6	Sources	18

Figures

Figure 1:	Firewall rule types and descriptions	6
Figure 2:	Beginning DNS setup	7
Figure 3:	DNS source	7
Figure 4:	DNS destination	8
Figure 5:	Public IP setup	8
Figure 6:	Application setup	9
Figure 7:	Application setup	9
Figure 8:	Service/URL setup	10
Figure 9:	NAT settings for original packet	10
Figure 10:	NAT settings for translated packet	11
Figure 11:	WWW access from the outside	11
Figure 12:	Remote Desktop Connection from remote workstation	12
Figure 13:	IP address input for "DC01"	13
Figure 14:	Input password for the given user	13

Figure 15: Certificate warning.....	14
Figure 16: Remote Desktop connection to "DC01"	15
Figure 17: Remote Desktop connection to "WSUS"	15
Figure 18: Remote Desktop connection to "SRV01"	16
Figure 19: Firewall policy rule change to accept only MS RDP connection between subnets...	16
Figure 20: RDP error when only ssh is specified for traffic between subnets	17

1 Introduction

This report discusses the effects of firewall security policies on the process of setting up DNS and NAT addresses in the Palo Alto VM firewall. The task was performed with reference to Palo Alto's official configuration guide (Palo Alto, 2018). The report begins by defining firewall security policy. It then examines DNS and NAT interactions within this context. This is followed by a discussion explaining the differences between security rules, policies and profiles. An example firewall is set up with the view towards providing a detailed breakdown of the logic behind its configuration. A conclusion summarizing the steps taken follows.

2 Theoretical background

2.1 Firewall security policy

A firewall is intended to serve as a means to establish security between trusted and untrusted networks (Tran, Al-Shaer & Boutaba, 2007). Firewall operations are determined by policies. Policies outline specific services and types of access allowed between trusted and untrusted domains (Hunt, 1998). Firewalls encompass network configurations, host systems, routers, encryption tunnels, authentication protocols and application systems. In this sense a firewall can be considered both a policy and its practical application. Different firewall architectures offer varying levels of protection. A clear delineation of the security perimeter is therefore required when defining firewall policies.

2.2 DNS and NAT

Domain Name System (DNS) is a distributed system which provides access to internet resources via human-readable domain names instead of numeric IP addresses. It achieves this by translating IP addresses to domain names and back. The primary security goals for DNS are data integrity and source authentication. These are required to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit (Chandramouli & Rose, 2013).

Network Address Translation (NAT) functions as a router between a range of private addresses and a sole public address. This is known as *many-to-one mapping* (Scarfone & Hoffman, 2009). NAT works by changing the source port for internal network connections. This helps identify hosts originating from internal connections while preventing external hosts from initiating contact. All

incoming HTTP requests directed at the NAT can be routed to a single host residing on the protected side of the firewall.

Firewalls influence significantly interactions between NAT and DNS. This is because NAT controls outbound and inbound DNS traffic, manages DNS server access and implements various security and filtering measures (Zarki, n.d.). Appropriately formulated firewall rules, policies and profiles are critical to ensuring DNS functions smoothly without sacrificing network integrity.

2.3 Interzone, intrazone and universal rules

Interzone, *intrazone* and *universal* rules are commonly used in firewalls to categorize and manage traffic based on source, destination and relevant security policy (Palo Alto, 2018).

2.3.1 Interzone rules

Intrazone rules apply to control and secure traffic originating and terminating within the same network security zone or trust level. They also control the policy defined for communication between devices in the same zone.

2.3.2 Intrazone rules

Interzone rules apply to traffic moving between different security zones. They are designed to control and secure traffic between different network segments with varying levels of trust (Palo Alto, 2023a). They help define how traffic should flow between these zones. This may include the DMZ (DeMilitarized Zone), internal network and the open internet.

2.3.3 Universal rules

Universal rules apply to all traffic passing through the firewall regardless of source or destination within the network. They are defined globally and enforced consistently across a given network. A universal rule can effectively be considered a combination of interzone and intrazone rules.

Figure 1: Firewall rule types and descriptions

Rule Type	Description
Universal	<p>By default, all the traffic destined between two zones, regardless of being from the same zone or different zone, this applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones.</p> <p>For example, if creating a universal rule with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A.</p>
Intrazone	<p>A security policy allowing traffic between the same zone, this applies the rule to all matching traffic within the specified source zones (cannot specify a destination zone for intrazone rules).</p> <p>For example, if setting the source zone to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.</p>
Interzone	<p>A security policy allowing traffic between two different zones. However, the traffic between the same zone will not be allowed when created with this type, this applies the rule to all matching traffic between the specified source and destination zones.</p> <p>For example, if setting the source zone to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not traffic within zones A, B, or C.</p>

Source: Palo Alto, 2023a

2.4 Application vs service policies

Firewall services can be defined as TCP or UDP ports within the Palo Alto ecosystem. This is not dissimilar to how traditional firewalls or access lists work. Firewall application policy is used to conduct Layer 7 inspections. This will determine if active applications within a data flow adheres to expected behavior. Deviations from expected behavior will in most cases be blocked automatically. If, for example, a session initially identified as DNS suddenly attempts an SQL query, it will be prevented from doing so (Palo Alto, 2020). Services and applications can be managed flexibly to create more dynamic security policies. The effectiveness of this type of security policy is attributed to its application identification capability.

2.5 Security profiles

Security profiles complement security policy rules by allowing for the scanning of permitted applications for threats like viruses, malware, spyware and DDoS attacks. They don't influence traffic flow decisions but are applied after an application or category has been allowed by the security policy rule. (Palo Alto, 2023b) Commonly used security profiles together into a *security profile group* to streamline this process. This simplifies their inclusion in security policy rules or makes them the default option for such rules. Profiles are available for a wide range of services. These include antivirus profiles, file blocking profiles, zone protection profiles and many more.

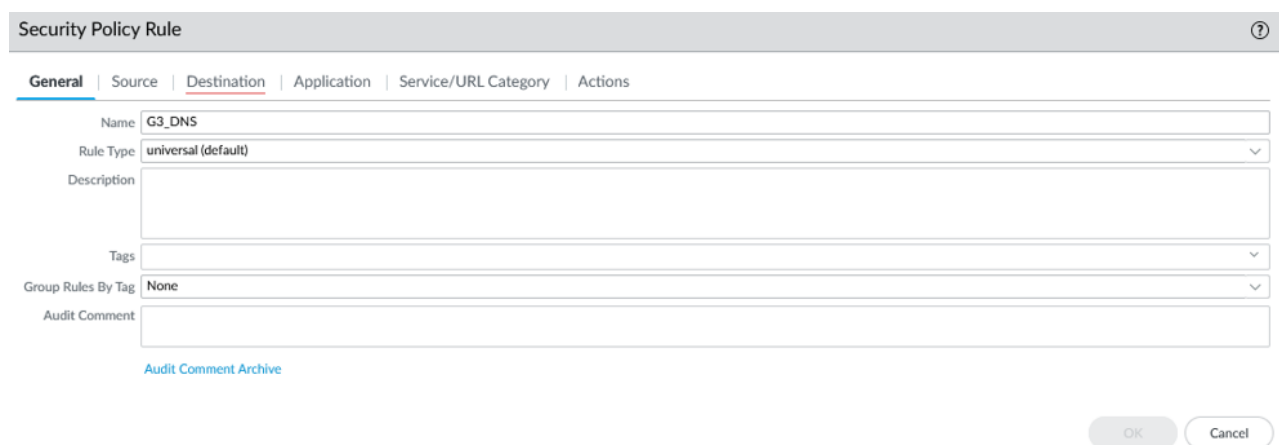
3 Internet access from the DMZ

The purpose of the lab was to establish connectivity between the public internet and two machines located in the VLE environment DMZ. DNS and NAT firewall settings for both machines had to be modified. Changes were made directly in the security tab of policy menu in the Palo Alto VM UI.

3.1 DNS setup

The initial setup of the VLE environment included a working DNS connection. Configuring a new DNS for the task was not necessary. The DNS setup process is outlined here only for the sake of completeness.

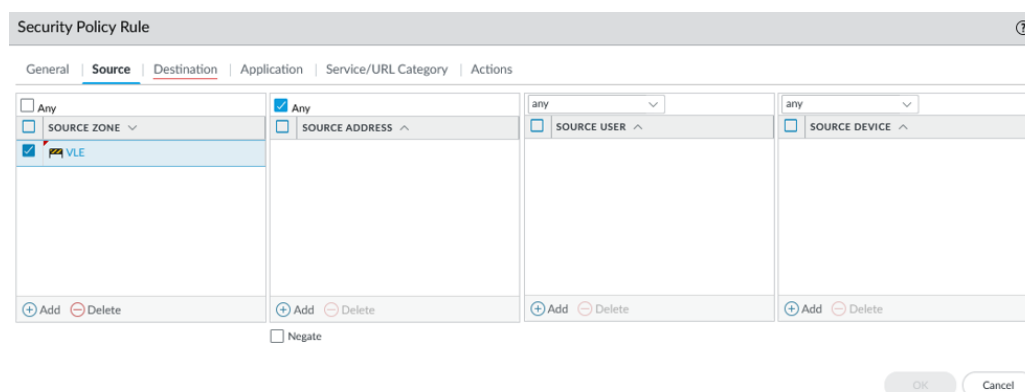
Figure 2: Beginning DNS setup



The screenshot shows the 'Security Policy Rule' configuration window in the Palo Alto VM UI. The 'General' tab is selected. The 'Name' field is 'G3_DNS'. The 'Rule Type' is 'universal (default)'. The 'Description' field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' is set to 'None'. The 'Audit Comment' field is empty. There is a link for 'Audit Comment Archive'. At the bottom right are 'OK' and 'Cancel' buttons.

The process began by specifying applicable source and destination settings. In this case the source was the public internet. This was the default VLE setting.

Figure 3: DNS source



The screenshot shows the 'Security Policy Rule' configuration window in the Palo Alto VM UI, with the 'Source' tab selected. The 'Source' section has four columns: 'Any', 'SOURCE ZONE', 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE'. The 'Any' checkbox is checked. The 'SOURCE ZONE' dropdown is set to 'VLE'. The 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE' sections are empty. At the bottom left is a 'Negate' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

The traffic destination was the DMZ environment.

Figure 4: DNS destination

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

Any	Any	any	any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input checked="" type="checkbox"/> VLE			
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete

☐ Negate

OK Cancel

The public IP of the Palo Alto firewall was used for the DNS destination address. This was 198.19.52.194.

Figure 5: Public IP setup

☐ Any

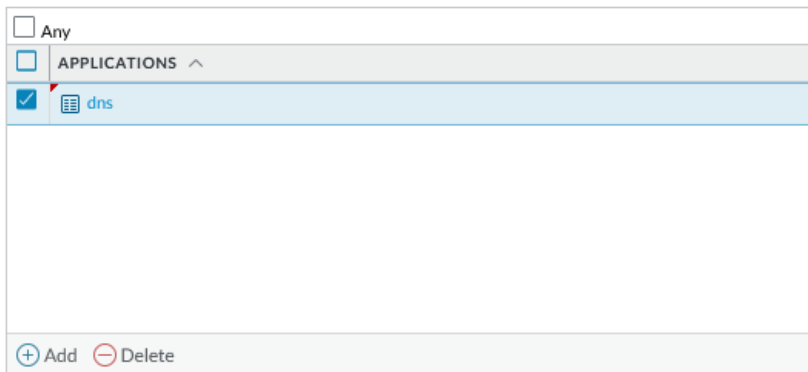
☐ DESTINATION ADDRESS ^

☒ public

☐ Add ☐ Delete

The application was set to *dns*.

Figure 6: Application setup

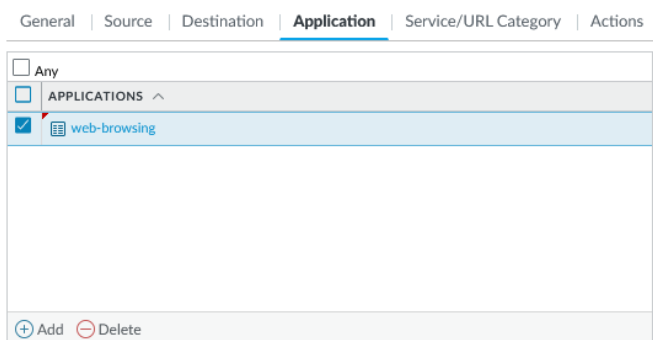


The setup process was quite straightforward but required understanding the flow of network traffic if packets were to arrive at their correct destinations. This also ensured against unauthorized access to restricted areas.

3.2 WWW connection setup

Setting the DNS for the WWW machine also required using the VLE as the source and the DMZ as the destination. The default address was again 198.19.52.194. The most significant divergence between standard DNS settings and settings for the WWW machine concerned the application and service/URL categories. In this case the *web-browsing* option was used.

Figure 7: Application setup



The service/URL category setting was set to *service-http*. This allowed the public IP to be accessible via browser.

Figure 8: Setvice/URL setup

The screenshot shows a configuration window with tabs: General, Source, Destination, Application, **Service/URL Category**, and Actions. The **Service/URL Category** tab is active. It features a search bar with the text 'select'. Below it, a list shows 'SERVICE ^' and 'service-http' (selected with a checkmark). At the bottom, there are '+ Add' and '- Delete' buttons.

3.3 WWW NAT settings

The final stage of the process required setting up NAT policies for the WWW machine. NAT settings were found from the same policies menu. They were found in a NAT-specific sub-menu in which new NAT policies could be created. The specified rules were enforced for both the original and translated packets. The source and destination were both set as VLE within the original packet sub-menu. The destination interface was set to *any* and the service set to *service-http*. The source address can be anything.

Figure 9: NAT settings for original packet

The screenshot shows the 'NAT Policy Rule' configuration window. It has tabs: General, **Original Packet**, and Translated Packet. The **Original Packet** tab is active. It contains several fields: 'Destination Zone' set to 'VLE', 'Destination Interface' set to 'any', and 'Service' set to 'service-http'. On the left, a list shows 'Any', 'SOURCE ZONE ^', and 'VLE' (selected with a checkmark). At the bottom, there are '+ Add' and '- Delete' buttons. To the right, there are two more lists: 'SOURCE ADDRESS ^' (with 'Any' selected) and 'DESTINATION ADDRESS ^' (with 'public' selected). At the bottom right, there are 'OK' and 'Cancel' buttons.

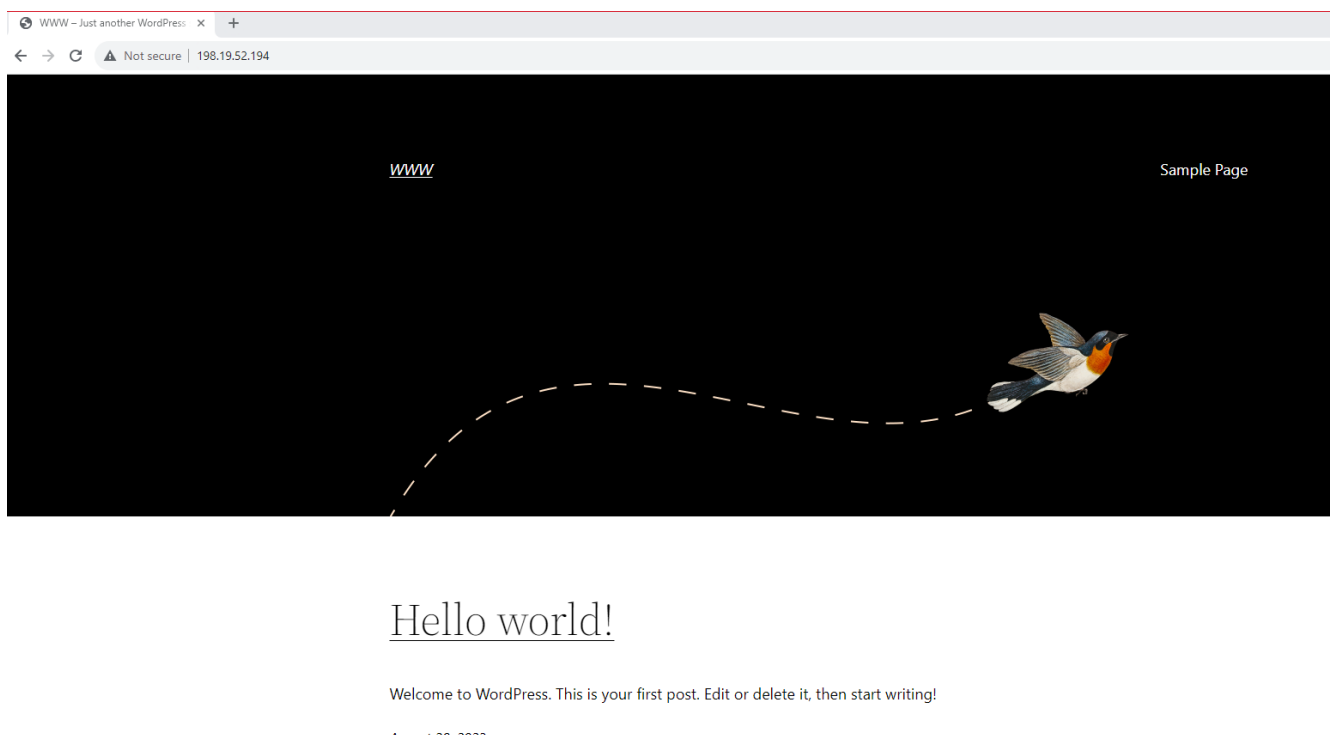
The destination address was again the Palo Alto public IP. Traffic for the translated packet should be directed via port 80 to the correct static IP address within the network.

Figure 10: NAT settings for translated packet

The image shows the 'NAT Policy Rule' configuration window. It has three tabs: 'General', 'Original Packet', and 'Translated Packet'. The 'Translated Packet' tab is selected. Under 'Source Address Translation', the 'Translation Type' is set to 'None'. Under 'Destination Address Translation', the 'Translation Type' is set to 'Static IP', the 'Translated Address' is '10.4.0.11', and the 'Translated Port' is '80'. There is an unchecked checkbox for 'Enable DNS Rewrite' and a 'Direction' dropdown set to 'reverse'. At the bottom right are 'OK' and 'Cancel' buttons.

Traffic was routed correctly with the settings above. The contents of the WWW machine could be viewed with a browser from outside of the VLE environment. They also ensured users using the internet from the WWW workstation would not have access to any other parts of the VLE environment.

Figure 11: WWW access from the outside



4 RDP from WS-net to Servers-net

The lab required a remote desktop connection be established from the WS01 workstation to the Servers-net subnet. Servers-net consisted of three virtual machines (DC01, WSUS and SRV01). Connectivity to each was tested manually. The process of connecting to WS01 from outside the environment was documented in the previous report.

The first step to testing connectivity inside the environment was establishing a remote desktop connection to the WS01 workstation. The next step was to open a remote desktop application on the remote workstation and provide credentials to connect to machines located in the Servers-net subnet.

Figure 12: Remote Desktop Connection from remote workstation

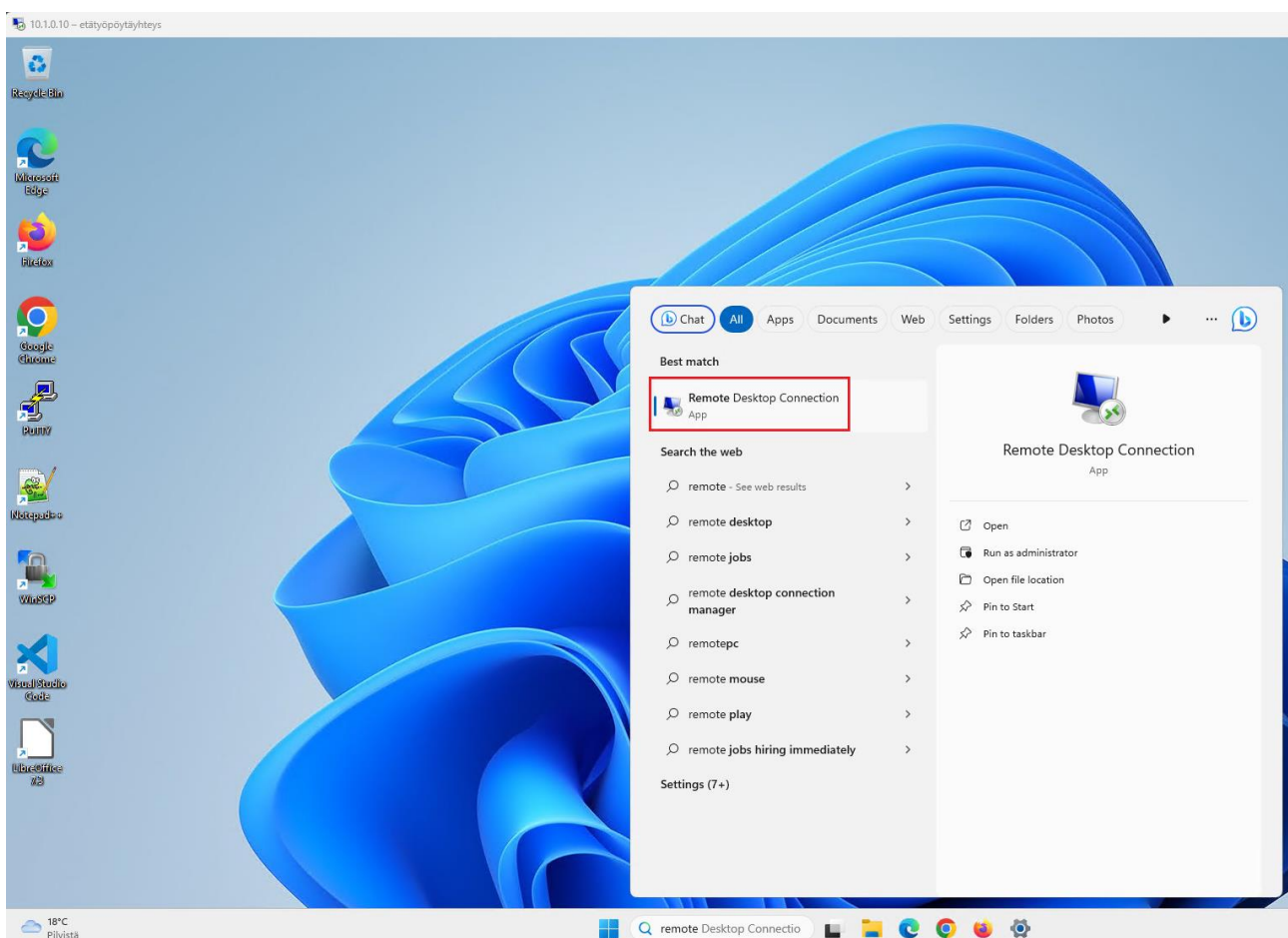


Figure 13: IP address input for DC01

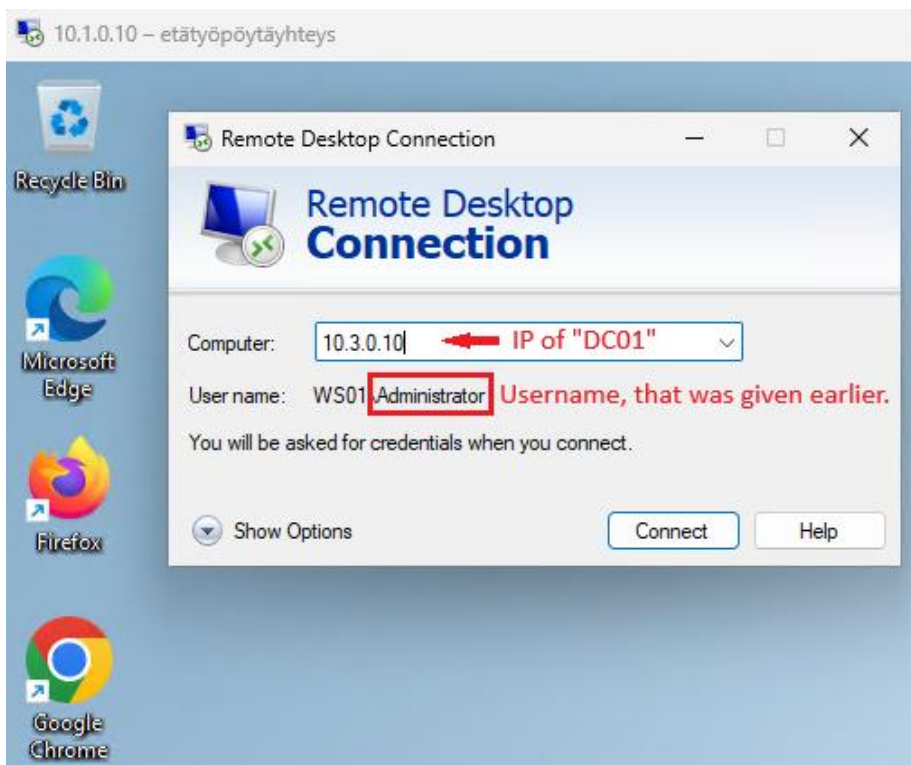
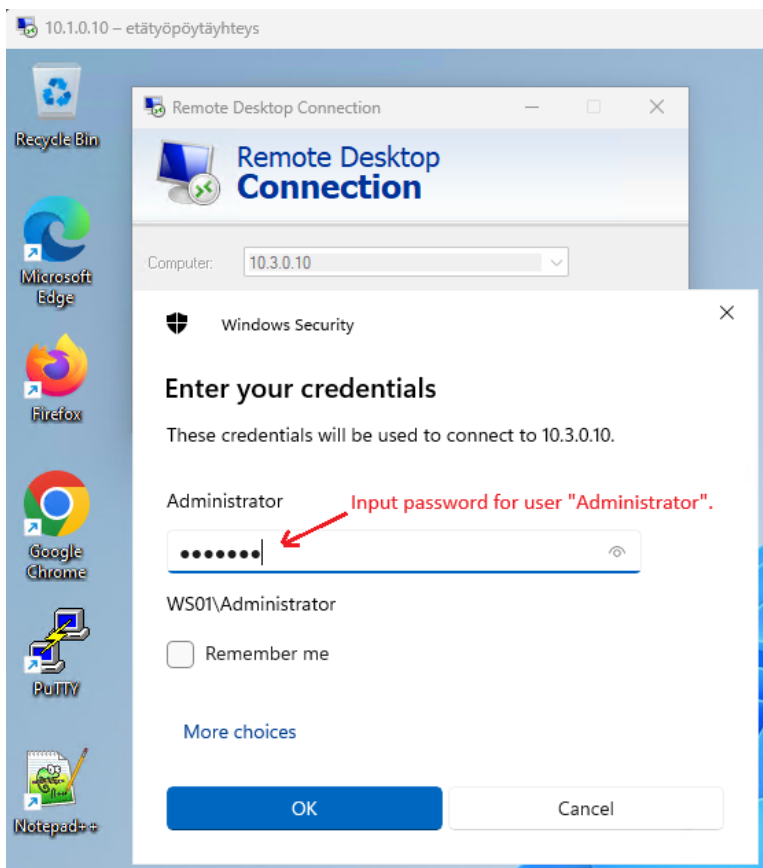
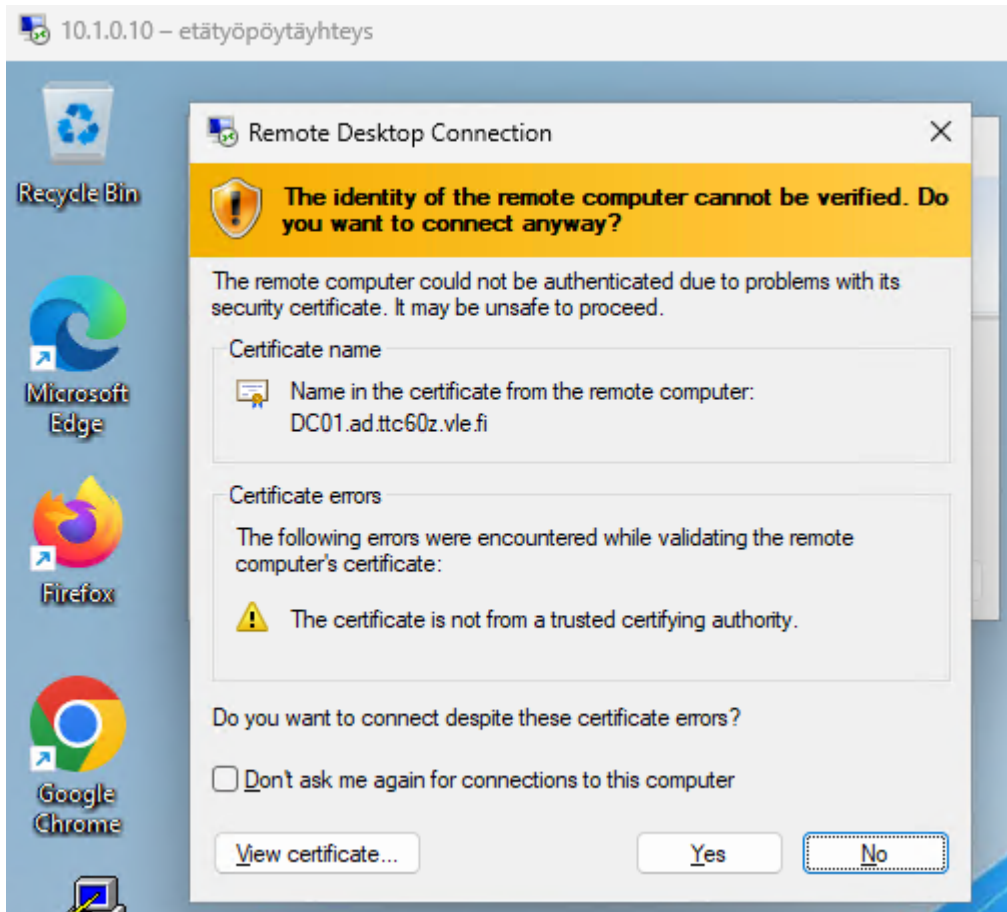


Figure 14: Input password for the given user



A warning popup concerning a certificate warning is raised after clicking OK. The same warning appeared in the previous lab when connecting remotely.

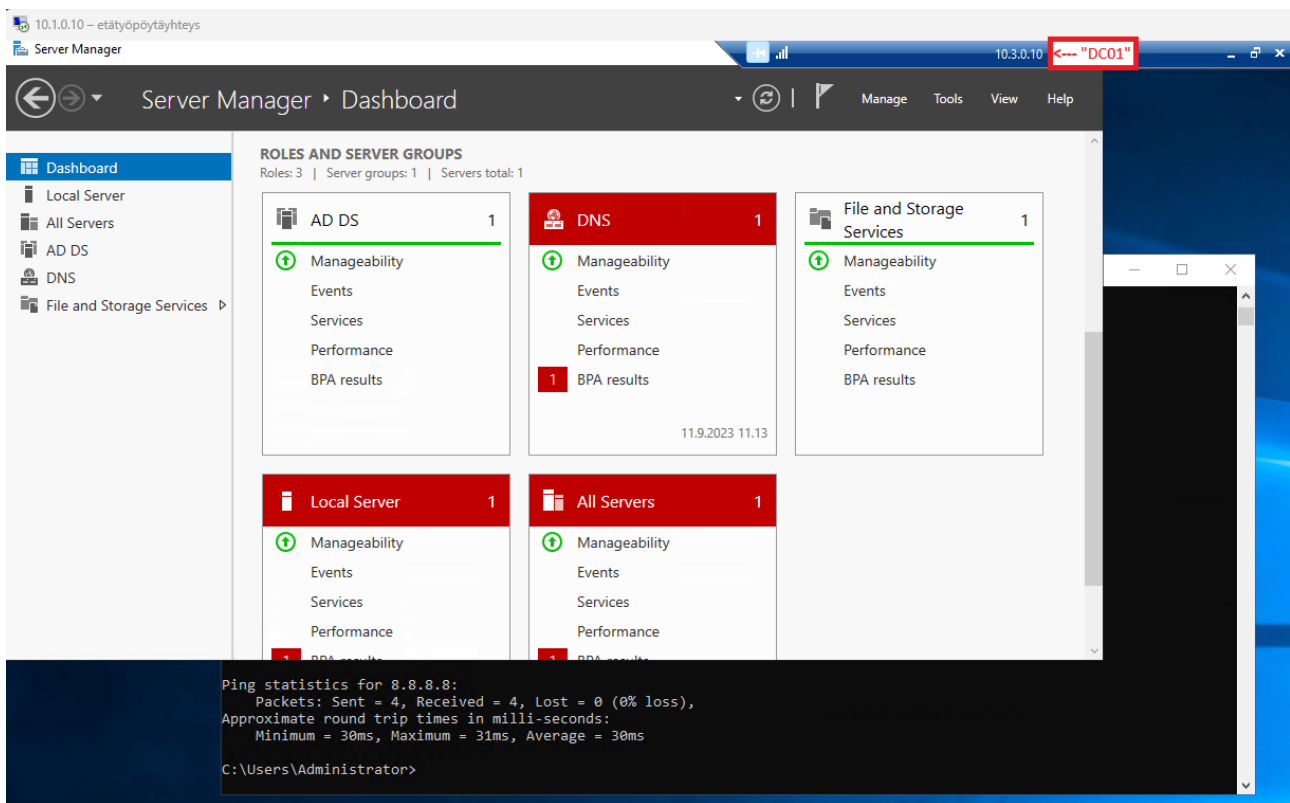
Figure 15: Certificate warning



Selecting Yes is acceptable in this case because the certificate is known to be trusted. This resulted in a remote connection to DC01.¹

¹ The certificate can be installed by clicking "View certificate" and then "Install Certificate". This was not a requirement for the present task, however.

Figure 16: Remote Desktop connection to DC01



The steps to connect to the two other machines were identical to those outlined above. They are illustrated in the images below.

Figure 17: Remote Desktop connection to WSUS

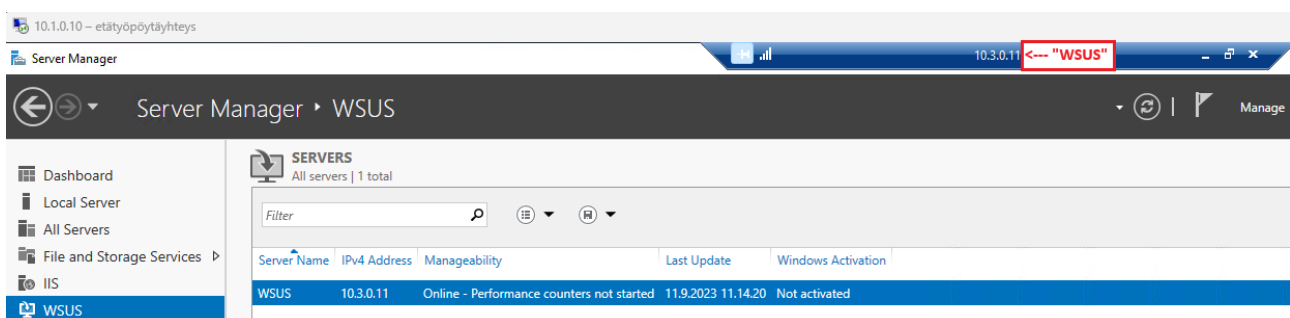
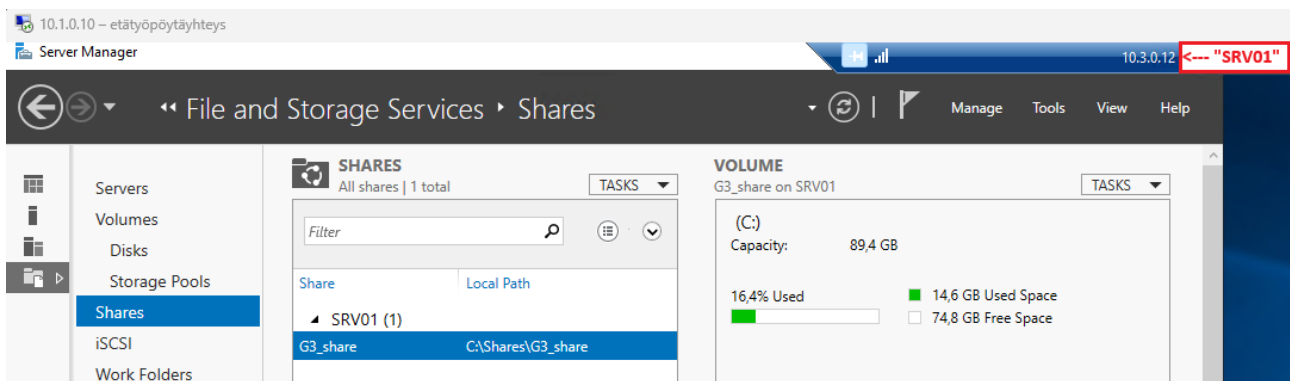
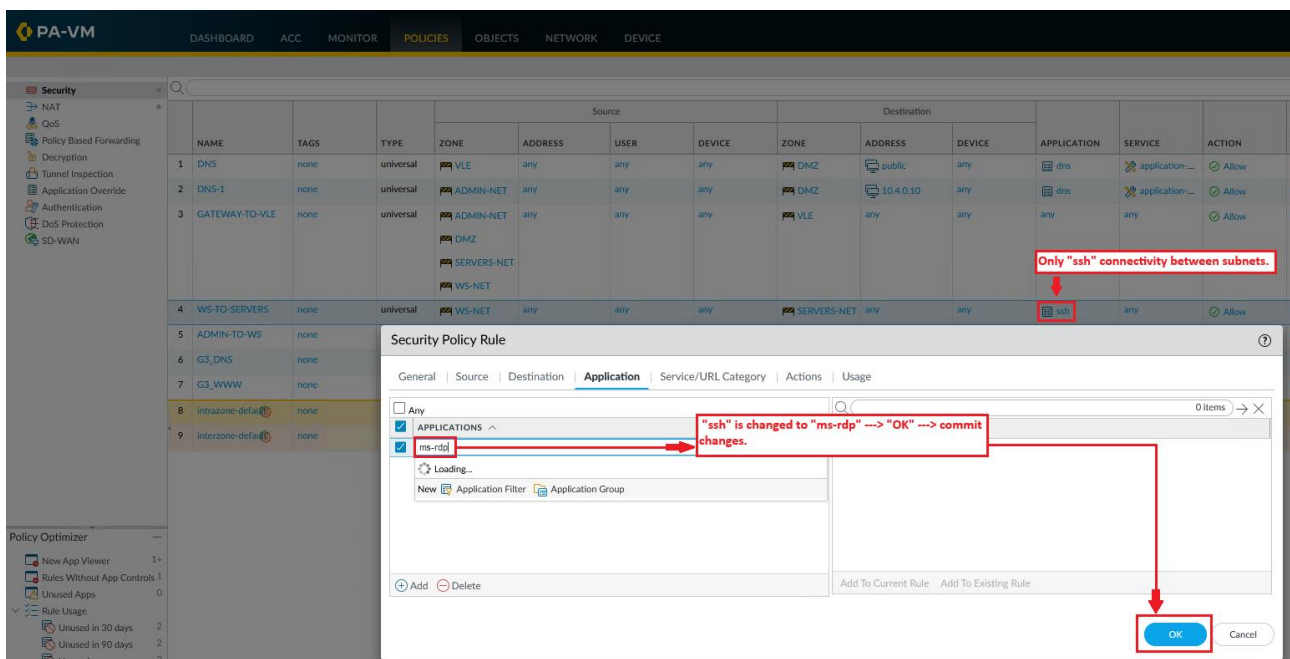


Figure 18: Remote Desktop connection to SRV01



No additional firewall configurations or configuration changes were required for the RDP to work. The firewall policy was modified to add more security in the environment in general, however. This change allowed only RDP connections from WS-net to Servers-net. A policy rule allowing only connection via SSH was added to *WS-TO-SERVERS* traffic. The connection is used only for demonstration purposes.

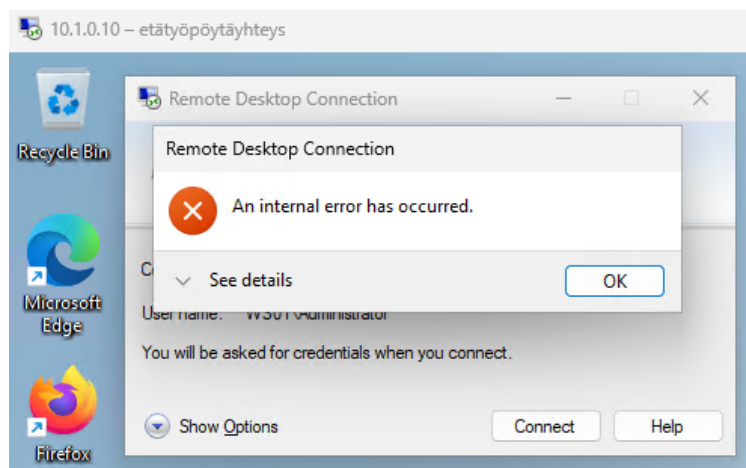
Figure 19: Firewall policy rule change to accept only MS RDP connection between subnets



The default setting for applications was set to *any*. This allowed any type of connection between subnets. Next a change to *ms-rdp* in the application section is made. The change is accepted by clicking *OK* and committing firewall changes. This set Microsoft Remote Desktop to be the only allowable connection between the WS-net and Servers-net subnets.

A warning popped up when only an SSH connection was specified for traffic between subnets. Connectivity returned after the change to *ms-rdp* was committed.

Figure 20: RDP error when only SSH is specified for traffic between subnets



5 Conclusions

The task built on the first lab. The report began with a theoretical discussion. The aim was to gain a foundational understanding of firewall rules, policies and profiles before proceeding to the practical aspects of the task. It was easier to make modifications to DNS and NAT rules once their roles in this context were understood. The result was an improved overall sense of how to implement appropriate changes to firewall configurations.

A DNS application and WWW application rule was added to the firewall to expose services to public internet with the abovementioned principles in mind. It also served as necessary revision of basic networking principles. It emerged during the task that a DNS application was configured by default. Setting it up again was therefore redundant. Going through the process was still beneficial because it further enhanced our understanding of the principles of firewall configuration.

Configuring remote desktop access from one subnet to another was straightforward. Firewall settings allow this type of connectivity by default. It was enough to begin by testing connectivity and not making any changes if it worked as expected. The configuration allowing only RDP connections between subnets was implemented and tested. It was a relief when modifications to the firewall did not result in a loss of network connectivity.

6 Sources

Chandramouli, R., & Rose, S. (2013). *Secure domain name system (DNS) deployment guide: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved September 11, 2023, from <https://doi.org/10.6028/nist.sp.800-81-2>

Hunt, R. (1998). *Internet/Intranet firewall security—policy, architecture and transaction services*. Computer Communications, 21(13), 1107-1123.

Scarfone, K., & Hoffman, P. (2009). *Special Publication 800-41 Revision 1 Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved September 11, 2023, from <https://www.govinfo.gov/content/pkg/GOVPUB-C13-f52fdee3827e2f5d903fa8b4b66d4855/pdf/GOVPUB-C13f52fdee3827e2f5d903fa8b4b66d4855.pdf>

Security Profiles. (2023b, August 1). Palo Alto TechDocs. Retrieved September 11, 2023, from <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles>

Tran, T., Al-Shaer, E. S., & Boutaba, R. (2007, November). *PolicyVis: Firewall Security Policy Visualization and Inspection*. In LISA (Vol. 7, pp. 1-16).

Zarki, M. (n.d.). *Ch 6: Networking Services: NAT, DHCP, DNS, Multicasting*. University of California: Irvine. Retrieved September 11, 2023, from <https://www.ics.uci.edu/~magda/cs620/ch6.pdf>

What are applications and services? (2022, November 21). Palo Alto Live. Retrieved September 11, 2023, from <https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508>

What are universal, intrazone and interzone rules? (2023a, May 8). Palo Alto Knowledgebase. Retrieved September 11, 2023, from <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>