



Labra 1

Ryhmä 3

Antti Tammelin

Tero Räsänen

Elmeri Söderholm

Eliel Taskinen

Raportti

Syyskuu 2022

Tieto- ja viestintätekniikan tutkinto-ohjelma

Tietoturvakontrollit TTC6010-3002

Sisältö

1	Johdanto	2
1.1	Tehtävänanto	2
1.2	Labrassa käytetyn ympäristön kuvaus	2
2	Palomuurin konfigurointi	3
2.1	Portaalin ja Gatewayn konfigurointi	3
2.2	GlobalProtect Sertifikaatit	5
3	RDP ja SSH yhteyden muodostaminen	7
4	Pohdinta	11
	Lähteet	13
	Liitteet	14
	Liite 1. Labraympäristö	14

Kuviot

Kuvio 1.	VLE ympäristön uusi public IP	3
Kuvio 2.	Sertifikaatin generointi	4
Kuvio 3.	Väärin tehty portalin EXT gateway	4
Kuvio 4.	Oikein tehty portalin EXT gateway	5
Kuvio 5.	Portaali GlobalProtectin lataukseen.	5
Kuvio 6.	GlobalProtect Cert is not signed.	6
Kuvio 7.	GlobalProtect connection worked.	7
Kuvio 8.	Palomuurin policyt.	7
Kuvio 9.	RDP salliminen WS01 sisällä	8
Kuvio 10.	Kuvankaappaus RDP yhteydestä	9
Kuvio 11.	Palomuurin loki onnistuneesta RDP yhteydestä	9
Kuvio 12.	SSH salliminen WS01 Osa 1.	10
Kuvio 13.	SSH salliminen WS01 Osa 2.	10
Kuvio 14.	Palomuurin lokit onnistuneista SSH yhteyksistä	10
Kuvio 15.	dir komento User1.	11
Kuvio 17.	Ryhmän uudet käyttäjät	12
Kuvio 18.	Loki esimerkki omista käyttäjistä	12

1 Johdanto

Tämä labra on osa kurssia Tietoturvakontrollit TTC6010-3002. Kurssilla ryhmien käyttöön luotiin virtuaalinen oppimisympäristö VLE (Virtual Learning Environment), jota käytetään kaikkiin kurssilla suoritettavien labrojen tekemiseen. VLE mahdollistaa sen, että ryhmät pystyvät suorittamaan labroja etänä, eikä ryhmäläisten tarvitse kokoontua koululla.

1.1 Tehtävänanto

Ensimmäisen labran tehtävänantona oli tutusta kurssin ympäristöön VLE:n sisällä (Virtual Learning Environment) ja konfiguroida ympäristössä oleva muuri, jotta jokainen ryhmän jäsen pystyy saamaan SSH ja RDP yhteyden VLE:n sisällä oleviin laitteisiin. (ks. liite 1). Tehtävänannossa myös tarkennettiin, että se on tarpeeksi, jos pystymme tekemään RDP yhteyden tiettyyn koneeseen, WS01.

Labran eri vaiheet koostuivat palomuurin käyttöönottamisesta ja sen IP-asetusten muokkaamisesta, Palo Alton tarjoaman VPN:n portaalin ja gatewayn konfiguroinnista, VPN-yhteyden muodostamisesta VLE:n sisälle, ja yhteyden kokeilemisestä.

1.2 Labrassa käytetyn ympäristön kuvaus

Tämän labran aikana piti käyttää osia VLE:stä, ja välillä ajaa tiettyjä asioita omalla koneella. VLE osat mitä käytettiin, olivat Palo Alton palomuuuri, sekä testikoneena toiminut WS01. Muita virtuaalisia koneita ei tässä harjoituksessa käytetty. Sen lisäksi omalle koneelle piti ladata Palo Alton tuote GlobalProtect.

Palomuurin avulla määriteltiin, mitä yhteyksiä voidaan käyttää lähiverkon sekä internetin välillä. Palo Alto-palomuurin asetuksiin päästiin muokkaamaan käyttöliittymällä, jonka tunnukset saimme toimeksiannon aikana.

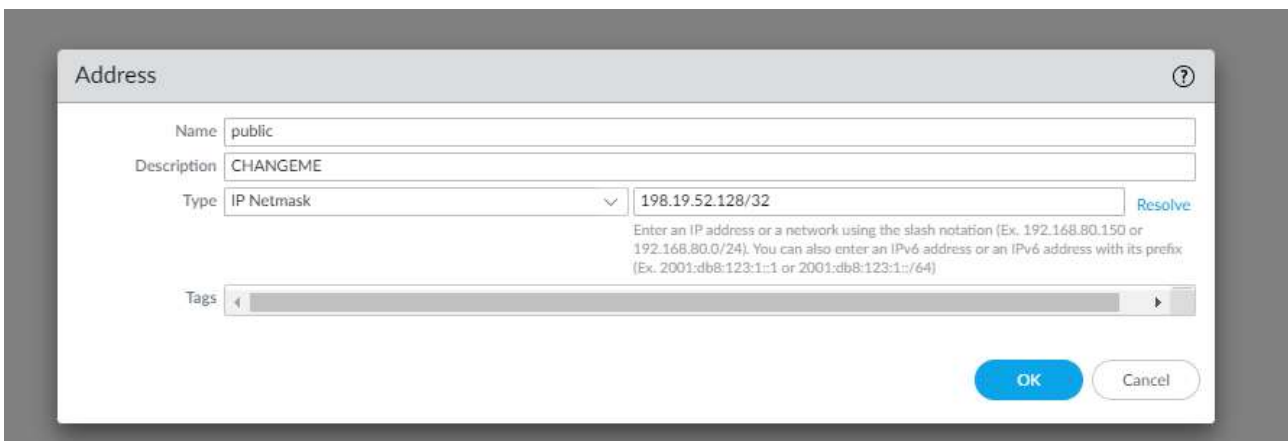
GlobalProtect on Palo Alto palomuurin VPN-sovellus. VPN on lyhenne sanoista Virtual Private Network. VPN:n avulla voidaan yhdistää tietokone julkisen verkon yli esimerkiksi koulun tai yrityksen omaan verkkoon. Jokainen ryhmän jäsen latasi GlobalProtectin omalle koneelleen. VPN-sovellusta voi käyttää myös oman koneen suojaamiseen internetin selaamisessa. VPN:n avulla tietokoneen

IP-osoitteen voi muuttaa, joten koneen sijainnin selvittäminen ei onnistu. GlobalProtectin avulla saimme yhdistettyä SSH (Secure Shell) ja RDP (Remote Desktop Protocol) testikoneeseen WS01.

Etätyöpöytäyhteys (Remote Desktop Protocol) on ohjelma, jolla voidaan muodostaa yhteys toiseen Windows-koneeseen. Etätyöpöytäyhteyttä voi käyttää myös Android- ja iOS-laitteilla. Yhteys muodostetaan IP-osoitteen, käyttäjänimen ja salasanan avulla.

2 Palomuurin konfigurointi

Ensimmäiseksi vaihdoimme Palo Alton palomuurin julkisen IP-osoitteen sen omasta IP:stä DNS serverin tarjoamaan IP:seen. Tämä on tarpeellinen vaihe koko labraan, koska muuten emme pystyisi yhdistämään muihin ympäristön sisäisiin laitteisiin. Otimme kuvan miltä uusi IP näytti, ja miltä tämän IP:n konfigurointivalikko näytti. (ks. kuvio 1).



Kuvio 1. VLE ympäristön uusi public IP

2.1 Portaalin ja Gatewayn konfigurointi

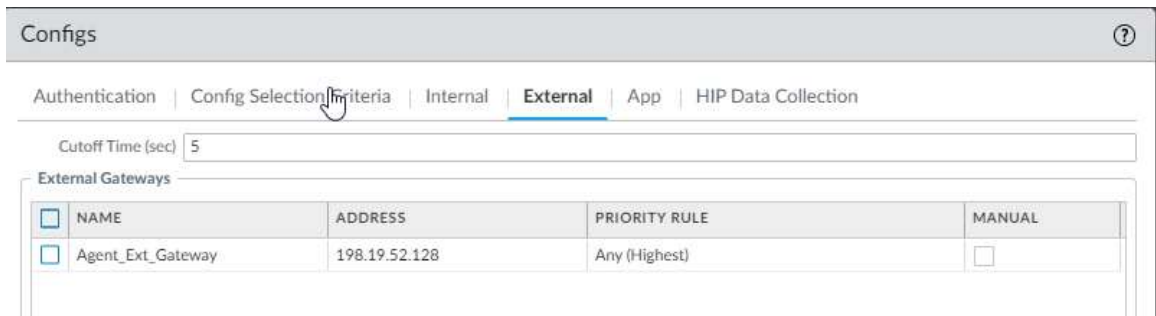
Julkisen IP:n vaihtamisen jälkeen aloimme konfiguroimaan GlobalProtectin portaalia ja gatewaytä. Portaalin konfiguroinnissa piti aluksi luoda uusi portaali, johon käytimme VLE-rajapintaa (ethernet1/5). Portaalille piti myös generoida uusi sertifikaatti, joka nimettiin uudella julkisella IP:llä. (ks. kuvio 2.)

Kuvio 2. Sertifikaatin generointi

Yleisesti Portalin ja Gatewayn konfigurointi oli suhteellisen helppoa, kun seurasimme ohjeita, mitkä oli annettu labran alussa. Tästä huolimatta meille tuli muutamia ongelmia, koska tiettyjä asioita ei selitetty ohjeissa, ja tässä moduulin alkuvaiheessa oli hankala ymmärtää mitä teimme väärin. Olimme laittaneet Global Protect Portalin External Gatewayn osoitteen väärin (ks. kuvio 3), jonka takia emme saaneet yhteyttä VPN:ään. Saimme korjattua virheen muuttamalla osoite samaan, mikä oli konfiguroitu palomuurin julkiseksi IP:ksi. (ks. kuvio 4).

NAME	ADDRESS	PRIORITY RULE	MANUAL
Agent_Ext_Gateway	ryhma3.portal.fi	Any (Highest)	<input type="checkbox"/>

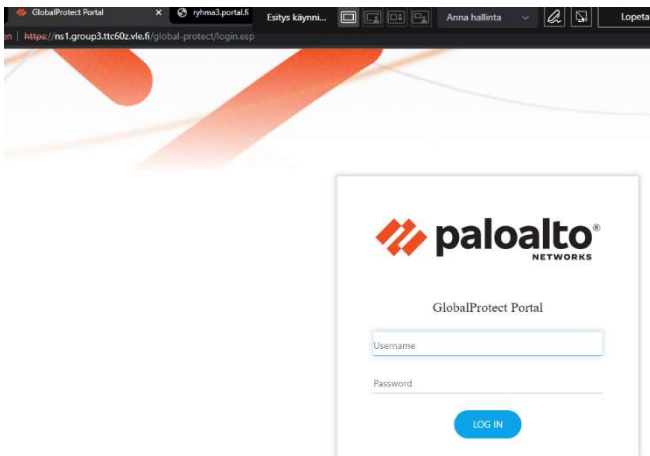
Kuvio 3. Väärin tehty portalin EXT gateway.



Kuvio 4. Oikein tehty portalin EXT gateway.

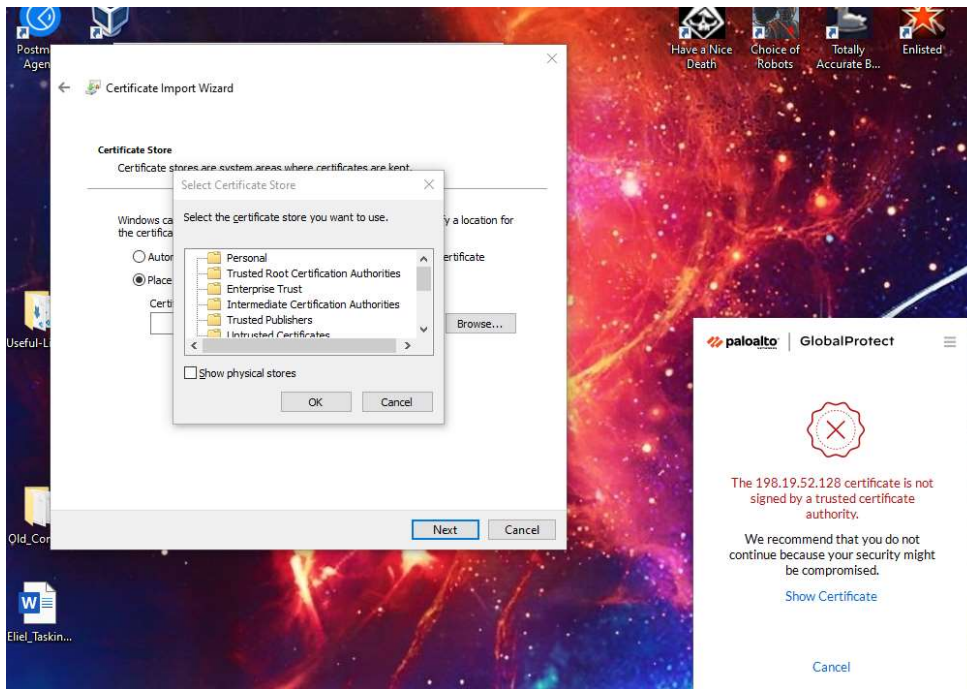
2.2 GlobalProtect Sertifikaatit

GlobalProtectin kanssa meillä oli paljon ongelmia. Me saimme sen ladattua tämän GlobalProtectin julkisen IP:n kautta, mikä meillä oli **198.19.52.128**. (ks. kuvio 5).



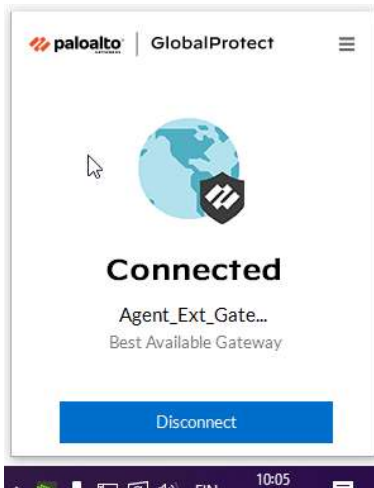
Kuvio 5. Portaali GlobalProtectin lataukseen.

Sen jälkeen, kun olimme saaneet GlobalProtectin ladattua, kohtasimme ensimmäisen ongelman mistä mainitsin jo aiemmin. Me olimme konfiguroineet väärin GlobalProtect Portalin External Gatewayn osoitteen (ks. kuvio 3 ja 4). Kun saimme tämän korjattua, seuraavaksi ongelmaksi tuli GlobalProtectin sertifikaatit. Alla olevasta kuvasta näkyy yleisin ongelma. (ks. kuvio 6).



Kuvio 6. GlobalProtect Cert is not signed.

Tämä selvisi melkein kaikilla ryhmän jäsenillä sillä, että painoi show certificate, ja vastasi kyllä kysymyksiin, kunnes kysyttiin mihin sertifikaatti haluttiin tallentaa. Silloin meidän piti manuaalisesti valita "Trusted Root Certification Authorities". Tämä ei kuitenkaan onnistunut yhdelle ryhmänjäsenelle, jonka listasta ei löytynyt tätä "Trusted Root Certification Authorities" vaihtoehtoa. Hänen piti asentaa sertifikaatti koko tietokoneelle, eikä vain yhdelle käyttäjälle, jotta GlobalProtect saatiin toimimaan. Alla olevassa kuvassa näkyy miltä GlobalProtect näyttää, kun se toimii. (ks. kuvio 7).



Kuvio 7. GlobalProtect connection worked.

Tämän kaiken lisäksi me konfiguroimme meidän GlobalProtect Gateway:n väärin, missä se tunnel-
litti meidän yhteytemme väärään Zoneen, josta tuli vähän ongelmia palomuurin, ja sen policyjen
kanssa. Tämä pieni ongelma löydettiin nopeasti, ja teimme VPN yhteyksille oman Zonen, ja
teimme sille omat policyt selkeyden ja yksinkertaisuuden takia nimellä VPN-To-WS-Net. (ks. kuvio
8.)

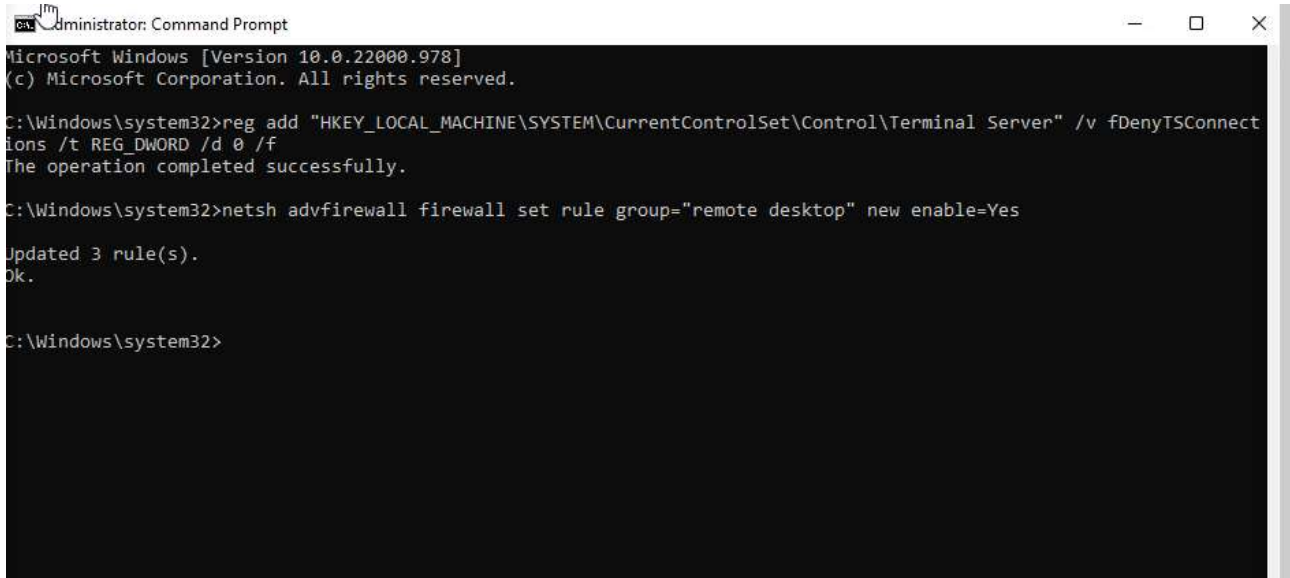
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
1	DNS	none	universal	VLE	any	any	any	DMZ	public	any	dns	application-...	Allow
2	VPN-To-WS-Net	none	universal	VPN	any	any	any	WS-NET	any	any	ms-rdp ssh ssh-tunnel	application-...	Allow
3	DNS-1	none	universal	ADMIN-NET	any	any	any	DMZ	10.4.0.10	any	dns	application-...	Allow
4	GATEWAY-TO-VLE	none	universal	ADMIN-NET DMZ SERVERS-NET WS-NET	any	any	any	VLE	any	any	any	any	Allow
5	WS-TO-SERVERS	none	universal	WS-NET	any	any	any	SERVERS-NET	any	any	any	any	Allow
6	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	any	any	Allow
7	Intrazone-default	none	Intrazone	any	any	any	any	(Intrazone)	any	any	any	any	Allow
8	Interzone-default	none	Interzone	any	any	any	any	any	any	any	any	any	Deny

Kuvio 8. Palomuurin policyt.

3 RDP ja SSH yhteyden muodostaminen

VPN yhteyden jälkeen tehtävänä oli konfiguroida palomuuuri niin, että jokainen ryhmäläinen pystyy
ottamaan VPN-yhteyden kautta yhteyden ympäristön koneisiin. RDP (Remote Desktop Protocol) ja

SSH (Secure Shell) yhteyden saavuttamiseksi pitää konfiguroida työaseman (WS01) ja palomuurin asetuksia. Aloitimme konfiguroimalla WS01 palomuuriasetuksia sallimalla RDP:n. (ks. kuvio 9.) (Huc, 2022).

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following commands and output:

```
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
The operation completed successfully.

C:\Windows\system32>netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
Updated 3 rule(s).
Ok.

C:\Windows\system32>
```

Kuvio 9. RDP salliminen WS01 sisällä.

Windows 10 laitteilla on sisäänrakennettu RDP-sovellus, mitä käytimme labran aikana. Testikoneen, WS01, IP-osoite oli `10.0.1.10`, jonka käyttäjänä toimi local user `.\User` eikä domain user `User1`. Otimme kuvan RDP yhteydestä WS01 koneen sisältä. (ks. Kuvio 10).



Kuvio 10. Kuvankaappaus RDP yhteydestä.

Otimme myös kuvan palomuurin lokeista, missä näkyy onnistuneita RDP yhteyksiä. (ks. Kuvio 11).

09/14 12:49:24	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			3389	ms-rdp	allow	VPN-To-WS-Net
09/14 12:48:49	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			3389	ms-rdp	allow	VPN-To-WS-Net
09/14 12:31:14	end	VPN	WS-NET	10.255.254.1	testuser		10.1.0.10			3389	ms-rdp	allow	VPN-To-WS-Net
09/14 12:31:09	end	VPN	WS-NET	10.255.254.1	testuser		10.1.0.10			3389	ms-rdp	allow	VPN-To-WS-Net

Kuvio 11. Palomuurin loki onnistuneesta RDP yhteydestä.

Sen jälkeen siirryimme SSH:n puolelle. WS01 koneen puolella SSH palvelu piti käynnistää, jotta kone hyväksyisi SSH yhteyden. Kuvassa näkyy miten kummatkin tarvittavat palvelut eivät ole toiminnassa, ja muutamat komennot mitä ajoimme WS01 sisällä. (ks. kuvio 12) (Kardashevsky 2021).

```

PS C:\Windows\system32> Get-Service -Name *ssh*

Status      Name            DisplayName
-----
Stopped     ssh-agent       OpenSSH Authentication Agent
Stopped     sshd            OpenSSH SSH Server

PS C:\Windows\system32> Start-Service sshd
PS C:\Windows\system32> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Windows\system32> Start-Service ssh-agent

```

Kuvio 12. SSH salliminen WS01 Osa 1.

Kaikki komennot eivät toimineet niin helposti, joten teimme ne kahdessa osassa. Kuitenkin lopulta saimme kummankin, ssh-agentin ja sshd-servicen toimimaan. (ks. kuvio 13). (Kardashevsky 2021).

```

PS C:\Windows\system32> Start-Service ssh-agent
PS C:\Windows\system32> Get-Service -Name *ssh*

Status      Name            DisplayName
-----
Running     ssh-agent       OpenSSH Authentication Agent
Running     sshd            OpenSSH SSH Server

```

Kuvio 13. SSH salliminen WS01 Osa 2.

WS01 konfiguraation jälkeen RDP ja SSH yhteydet piti sallia palomuurissa. Käytimme hyväksi VPN:lle tehtyä omaa Zonea nimeltä VPN, ja sallimme applikaatiot ms-rdp, ssh ja ssh-tunnel VPN Zonesta WS-Net Zoneen. Tämän jälkeen saimme kummankin, RDP ja SSH, toimimaan. Otimme kuvakaappauksen myös onnistuneista SSH lokitiedoista. (ks kuvio 14).

09/14 13:16:29	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net
09/14 13:16:14	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net
09/14 13:16:04	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net
09/14 13:15:54	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net
09/14 13:15:14	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net
09/14 13:12:14	end	VPN	WS-NET	10.255.254.3	teror		10.1.0.10			22	ssh	allow	VPN-To-WS-Net

Kuvio 14. Palomuurin lokit onnistuneista SSH yhteyksistä.

Saimme käyttäjällä `User1` SSH yhteyden WS01:seen, mutta valitettavasti emme saaneet käyttäjällä `.\User` SSH yhteyttä. (ks. kuvio 15).

```
ad-ttc60z\user1@WS01 C:\Users\user1.AD-TTC60Z>dir
Volume in drive C has no label.
Volume Serial Number is A283-0E61

Directory of C:\Users\user1.AD-TTC60Z

04/08/2022  12.58    <DIR>          .
04/08/2022  12.58    <DIR>          ..
04/08/2022  12.57    <DIR>          Contacts
23/08/2022  13.50    <DIR>          Desktop
04/08/2022  12.57    <DIR>          Documents
04/08/2022  12.57    <DIR>          Downloads
04/08/2022  12.57    <DIR>          Favorites
04/08/2022  12.57    <DIR>          Links
04/08/2022  12.57    <DIR>          Music
04/08/2022  12.58    <DIR>          OneDrive
04/08/2022  12.57    <DIR>          Pictures
04/08/2022  12.57    <DIR>          Saved Games
04/08/2022  12.57    <DIR>          Searches
08/08/2022  12.53    <DIR>          Videos
               0 File(s)                0 bytes
               14 Dir(s)  66 618 916 864 bytes free

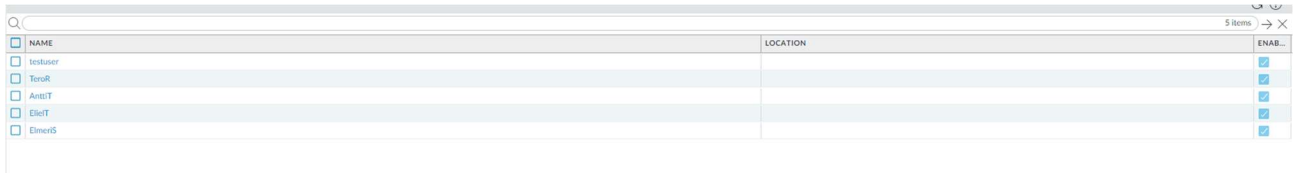
ad-ttc60z\user1@WS01 C:\Users\user1.AD-TTC60Z>
```

Kuvio 15. dir komento User1.

4 Pohdinta

Labran aloitus oli meidän ryhmällemme melko hidas ja hämmentävä. Uusia asioita tuli paljon ja päätimme vain lähteä seuraamaan VPN:n konfiguraatio-ohjetta. Konfigurointia pystyi tekemään vain yksi ihminen kerrallaan, joka vaikeutti myös hieman labran ymmärtämistä ja seuraamista. Ohjeissa oli myös hieman epäselvyyksiä ja joitain vaiheita oli jätetty pois kokonaan, joka hidasti työskentelyä ja vaati opettajalta kysymistä. Tästä huolimatta, ympäristöön tutustumisen ja muutaman asian selventämisen jälkeen, ymmärsimme mielestämme labran idean ja saimme tehtyä labran loppuun asti hyvin tuloksin.

Labraan tarvittavien askelten lisäksi loimme myös kaikille käyttäjätilit GlobalProtectia varten. Teke-
misiä on helpompi seurata, kun jokainen käyttää omaa käyttäjätiliä. (ks. kuvio 17).



NAME	LOCATION	ENAB...
<input type="checkbox"/> testuser		<input type="checkbox"/>
<input type="checkbox"/> Terror		<input checked="" type="checkbox"/>
<input type="checkbox"/> AntiT		<input checked="" type="checkbox"/>
<input type="checkbox"/> Ellet		<input checked="" type="checkbox"/>
<input type="checkbox"/> ElmerS		<input checked="" type="checkbox"/>

Kuvio 16. Ryhmän uudet käyttäjät.

Lokitiedostoissa näkyy, miten eri käyttäjät näkyvät palomuurin sisällä. Sen lisäksi tämä tekee ryh-
mäjaosta, ja kuka tekee mitäkin, selkeämpää. (ks. Kuvio 18).



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID
	09/14 12:54:49	drop	VPN	VLE	10.255.254.3	terror		198.18.100.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
	09/14 12:54:49	drop	VPN	VLE	10.255.254.3	terror		198.18.100.4			53	not-applicable	deny	interzone-default	policy-deny	0	0
	09/14 12:54:49	drop	VPN	VLE	10.255.254.3	terror		198.18.100.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
	09/14 12:54:49	drop	VPN	VLE	10.255.254.3	terror		198.18.100.4			53	not-applicable	deny	interzone-default	policy-deny	0	0

Kuvio 17. Loki esimerkki omista käyttäjistä.

Lähteet

Huc, M. 2022 How to enable Remote Desktop using Command Prompt on Windows 10. Pureinfotech 19.4.2022, Viitattu 19.9.2022 <https://pureinfotech.com/enable-remote-desktop-command-prompt-windows-10/>

Kardashevsky, C. 2021 How to SSH into Windows 10 or 11? TheItBros 15.9.2021, Viitattu 19.9.2022 <https://theitbros.com/ssh-into-windows/>

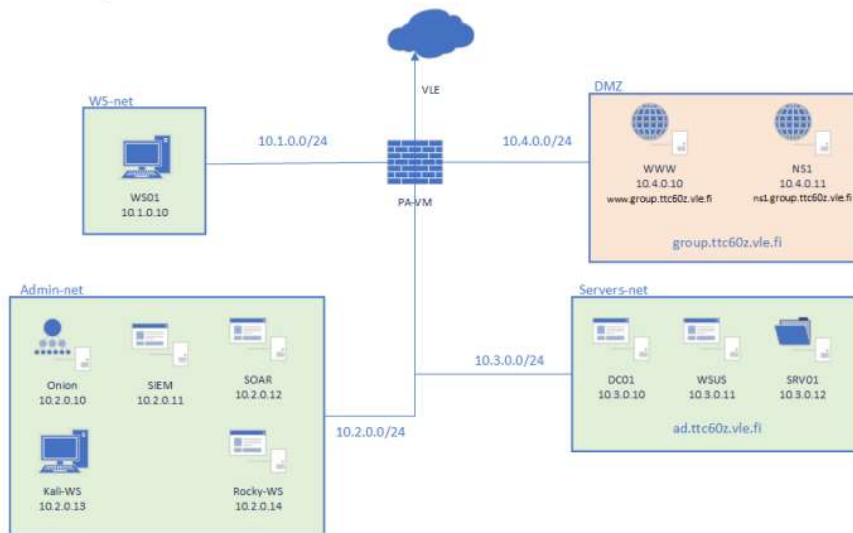
Stanton, L. 2022 How To Check Which Ports Are Open On A Windows 10 PC. Alphr 14.7.2022, Viitattu 19.9.2022 <https://www.alphr.com/how-to-check-which-ports-open-windows-10-pc/>

TTC6010. n.d. Configuring the Paloalto FW vpn to external interface <https://moodle.jamk.fi/pluginfile.php/790760/course/section/81507/Lab1-VPN%20configuration%20guide.pdf>

Liitteet

Liite 1. Labraympäristö

1. Ympäristö



Kuvio 1 Laboratorio ympäristö