Labra 1

Ryhmä 14

Helminen Mikko

Hyyrynen Eetu

Kallio Niko

Leppänen Juuso

Martin Mikko

30.1.2025  
Opiskelutehtävä  
TTC6010-3008, Jarmo Viinikanoja  
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

[1 Johdanto 2](#_Toc189505159)

[2 Teoria 2](#_Toc189505160)

[2.1 VPN 2](#_Toc189505161)

[2.2 Palo Alto 2](#_Toc189505162)

[3 Labra 3](#_Toc189505163)

[3.1 Portalin konfigurointi 5](#_Toc189505164)

[3.2 External Gateway 9](#_Toc189505165)

[3.3 GlobalProtect lataus ja yhdistäminen 13](#_Toc189505166)

[3.4 (Policy) säännöt, ssh ja rdp yhteys 14](#_Toc189505167)

[4 Pohdinta 18](#_Toc189505168)

[Lähteet 19](#_Toc189505169)

Kuviot

[Kuvio 1. Snapshot 3](#_Toc189505170)

[Kuvio 2. Public IP 4](#_Toc189505171)

[Kuvio 3. Ensimmäinen commit 4](#_Toc189505172)

[Kuvio 4. Käyttäjän luominen 5](#_Toc189505173)

[Kuvio 5. GlobalProtect portalin kongifurointi 6](#_Toc189505174)

[Kuvio 6. Clientin authentikointiprofiili 6](#_Toc189505175)

[Kuvio 7. Sertifikaatin generointi 7](#_Toc189505176)

[Kuvio 8. Authentikointiprofiilin määritykset 8](#_Toc189505177)

[Kuvio 9. Clientin authentikaation määrityksiä 9](#_Toc189505178)

[Kuvio 10. Ulkoisen yhdyskäytävän IP-osoite 10](#_Toc189505179)

[Kuvio 11. Tunneli rajapinnan määrittäminen 11](#_Toc189505180)

[Kuvio 12. Yhdyskäytävän konfiguraation asetukset 11](#_Toc189505181)

[Kuvio 13. GlobalProtect-clientin lataaminen 12](#_Toc189505182)

[Kuvio 14. GlobalProtect portaliin pääsee onnistuneesti 13](#_Toc189505183)

[Kuvio 15. Yhdistäminen omaan GlobalProtect-portaaliin 14](#_Toc189505184)

[Kuvio 16. VPN Zone 14](#_Toc189505185)

[Kuvio 17. VPN Zonen lisäys NAT 15](#_Toc189505186)

[Kuvio 18. Sääntö SSH-yhteydelle 15](#_Toc189505187)

[Kuvio 19. Sääntö SSH-yhteydelle 2.0 15](#_Toc189505188)

[Kuvio 20. SSH-yhteyden muodostaminen 16](#_Toc189505189)

[Kuvio 21. Sääntö RDP-yhteydelle 16](#_Toc189505190)

[Kuvio 22. Koneen IP-osoite 17](#_Toc189505191)

[Kuvio 23. Yhteyden muodostaminen PowerShellillä 17](#_Toc189505192)

[Kuvio 24. Etätyöpöytäyhteyden muodostaminen 18](#_Toc189505193)

# Johdanto

Tässä harjoituksessa konfiguroitiin Palo Alto –palomuuriin GlobalProtect-portaali, gatewayt ja VPN-tunneli. Lisäksi määritettiin säännöt RDP Windows-koneelle. Yhdistettiin omalta tietokoneelta portaaliin, asennettin GlobalProtect-client omalle koneelle, sekä lisättiin sertifikaatit. Käytimme tässä hyödyksi Moodlesta löytynyttä VPN configuration guidea. (Lab1- VPN configuration guide, n.d.)

# Teoria

## VPN

VPN eli Virtual Private Network on virtuaalinen erillisverkko, joka luo salatun yhteyden internetin kautta. VPN:n avulla voidaan turvallisesti siirtää arkaluonteista dataa ja estää ulkopuolisia salakuuntelemasta verkkoliikennettä. Näin tiedonsiirto pysyy yksityisenä. Esimerkiksi työntekijä voi työskennellä toimiston ulkopuolella ja silti muodostaa turvallisen yhteyden yrityksen verkkoon. (What Is a Virtual Private Network (VPN)?, n.d.)

Tiedämme myös, että VPN:n avulla voi päästä käsiksi sisältöön ja verkkosivustoihin, jotka voivat olla estettyjä omassa maassa. Vaihtamalla IP-osoitteen toiseen maahan voi esimerkiksi katsella eri maiden suoratoistopalveluita. Kaiken kaikkiaan 22,9 prosenttia internetin käyttäjistä maailmanlaajuisesti käyttää virtuaalista erillisverkkoa. (Petrosyan, 2024.)

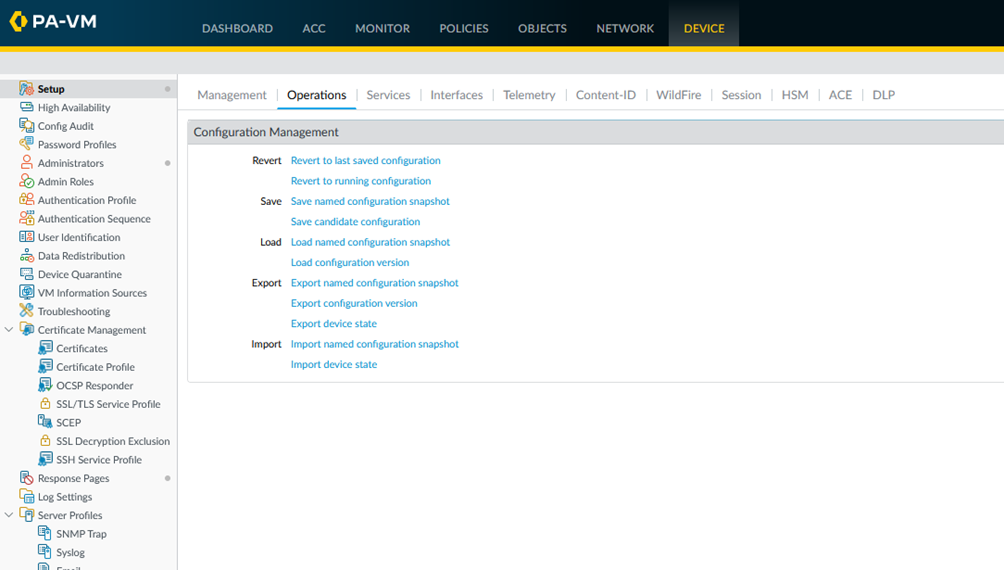
## Palo Alto

Palo Alto on yhdysvaltalainen monikansallinen kyberturvallisuusyritys, jonka ydintuotteita ovat muun muassa palomuurit. Yhtiö on kyberturvallisuuden uuden aikakauden edelläkävijä, tarjoten turvallisia sovellusten käyttöönottoja ja estäen kyberhyökkäyksiä kymmenille tuhansille organisaatioille. (Palo Alto Networks, n.d.)

Palo Alton palomuurit erottuvat tehokkaalla yhden läpikulun arkkitehtuurillaan, joka käsittelee tietoliikenteen paketteja vain kerran, vaikka useita suojaustoimintoja olisi käytössä. Tämä takaa korkean suorituskyvyn ja skaalautuvuuden. Palomuurit tarjoavat kattavaa suojaa muun muassa uhkien torjunnan, URL-suodatuksen ja hiekkalaatikkoanalyysin avulla. Ne tukevat monipuolisesti fyysisiä, virtuaalisia ja pilviympäristöjä, jolloin ne pystyvät sopeutumaan erilaisten organisaatioiden tarpeisiin. (Bevis, 2022.)

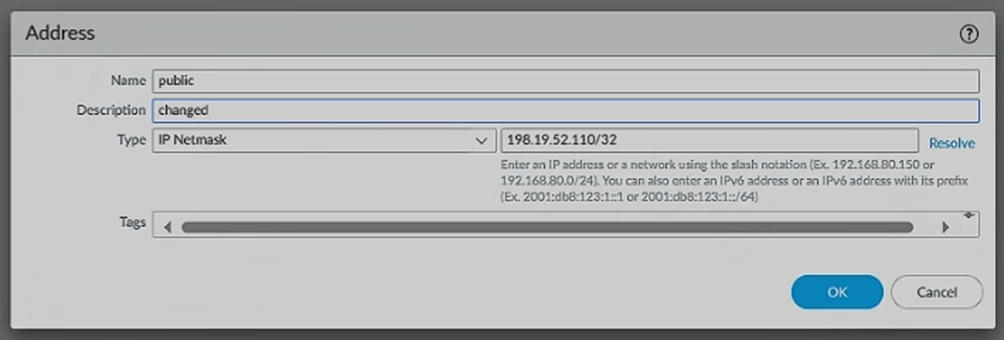
# Labra

Aloitettu Palo Alton käyttäminen ottamalla snapshot alkutilanteesta (ks. kuvio 1).

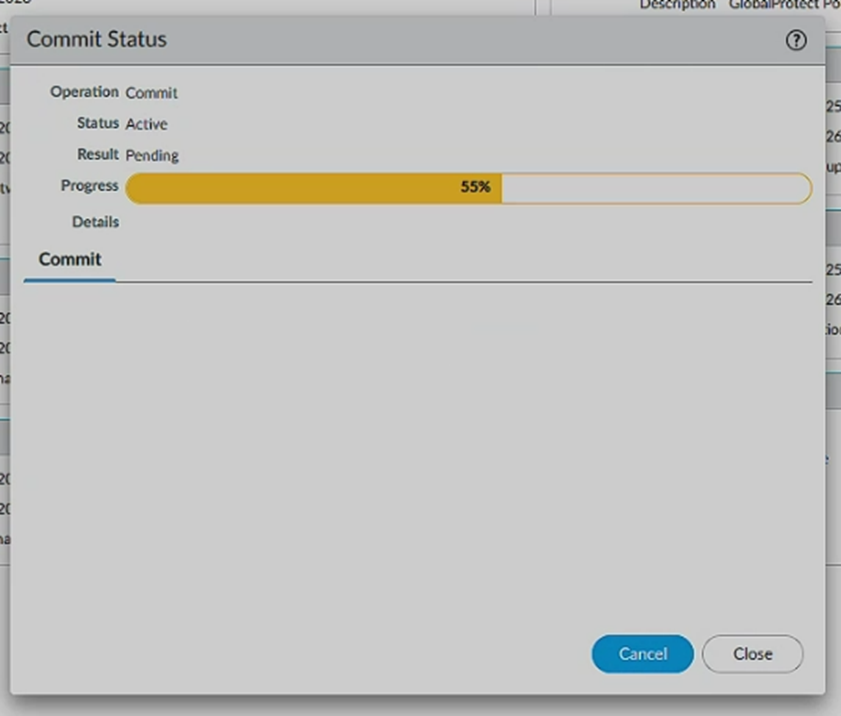


Kuvio 1. Snapshot

Vaihdettu description ja julkinen IP-osoite (ks. kuvio 2). Tämän jälkeen ensimmäinen commit onnistuneesti (ks. kuvio 3).

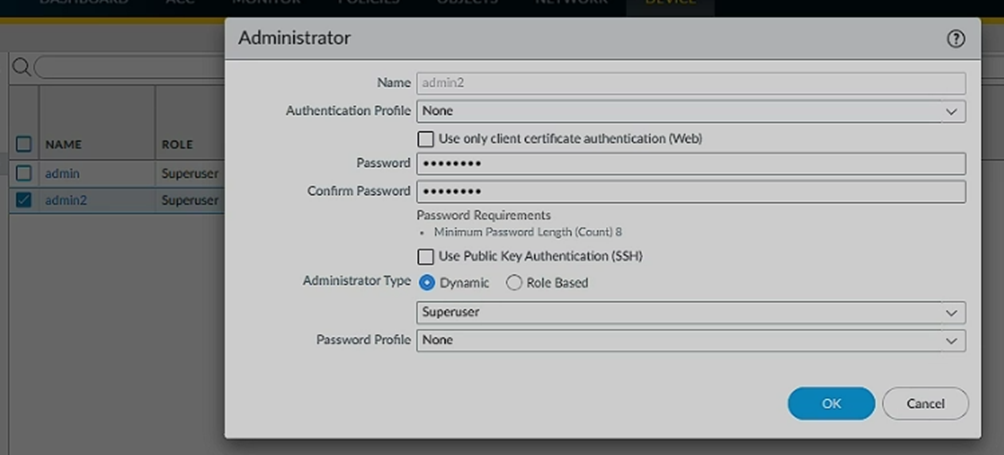


Kuvio 2. Public IP



Kuvio 3. Ensimmäinen commit

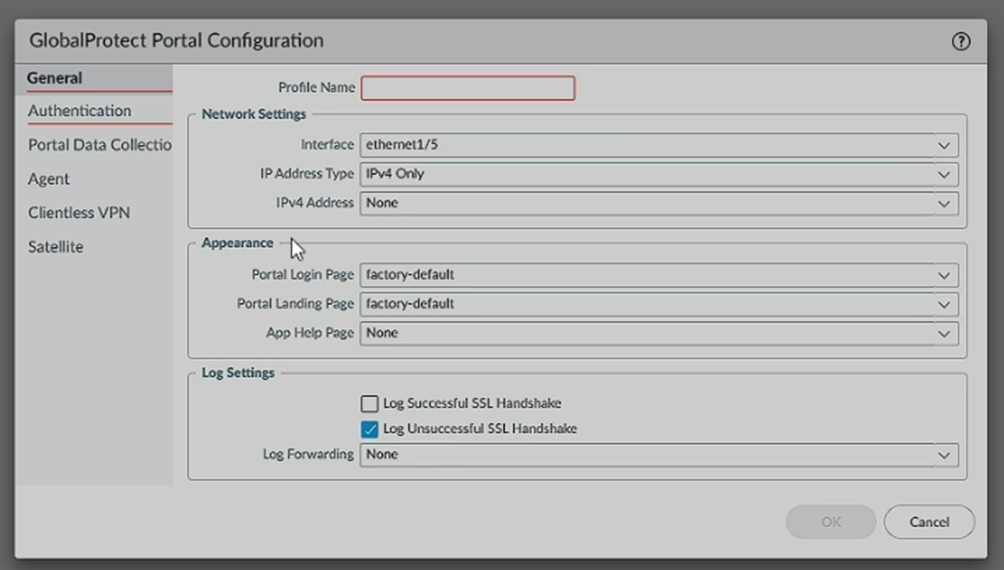
Tehtiin toinen käyttäjä paloaltolle (ks. kuvio 4).



Kuvio 4. Käyttäjän luominen

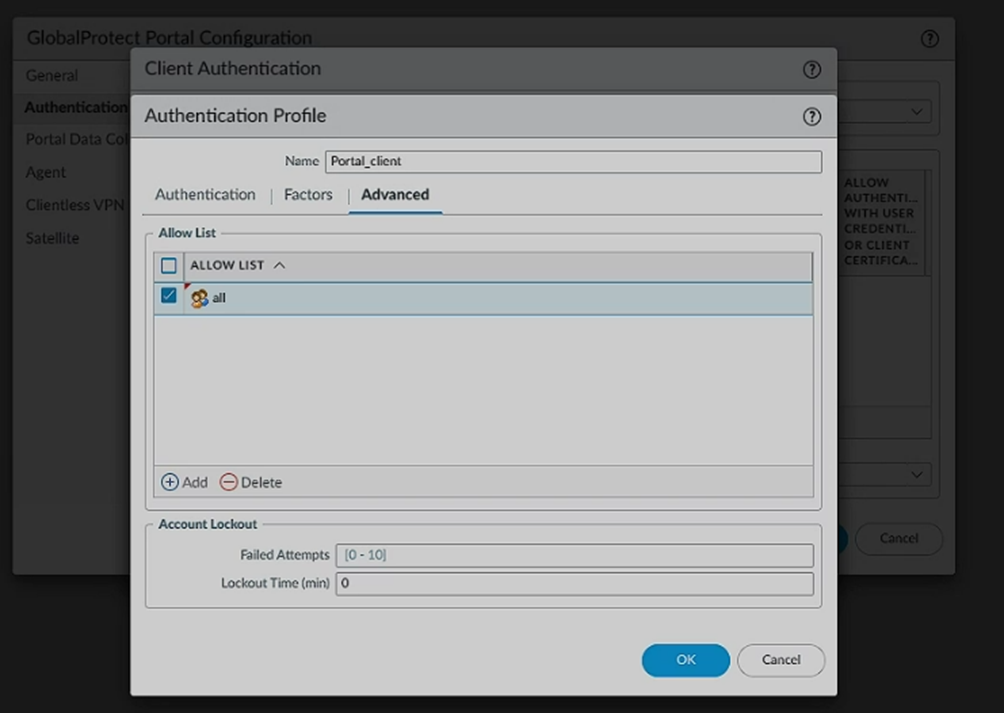
## Portalin konfigurointi

Seuraavaksi konfiguroimme GlobalProtect portaalin (ks. kuvio 5).

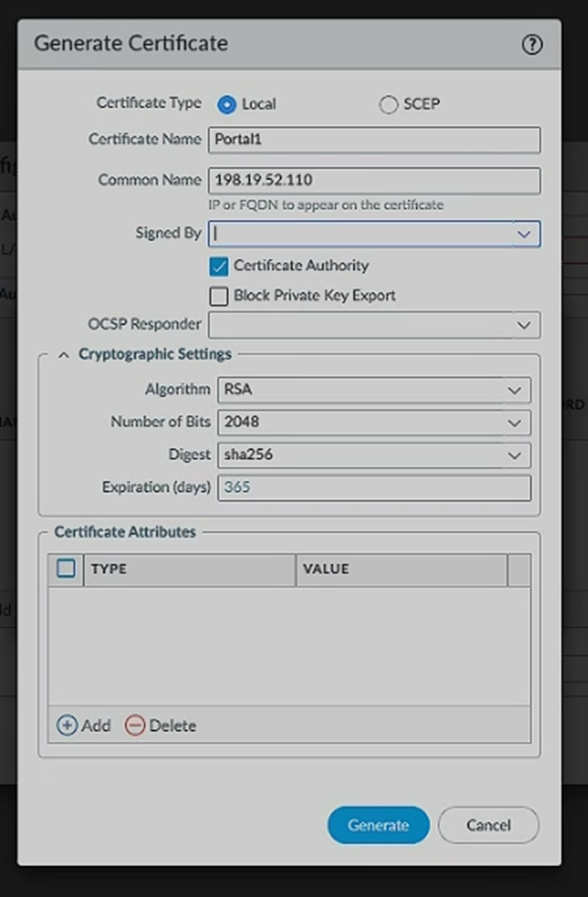


Kuvio 5. GlobalProtect portalin kongifurointi

Tämän jälkeen aloimme määrittelemään autentikaatioprofiilia (ks. kuvio 6). Generoimme myös sertifikaatin, jota tarvitaan myöhemmin (ks. kuvio 7). Käytimme tässä vaiheessa apuna myös Palo Alton dokumentaatiota. (Set Up Access to the GlobalProtect Portal, n.d.)

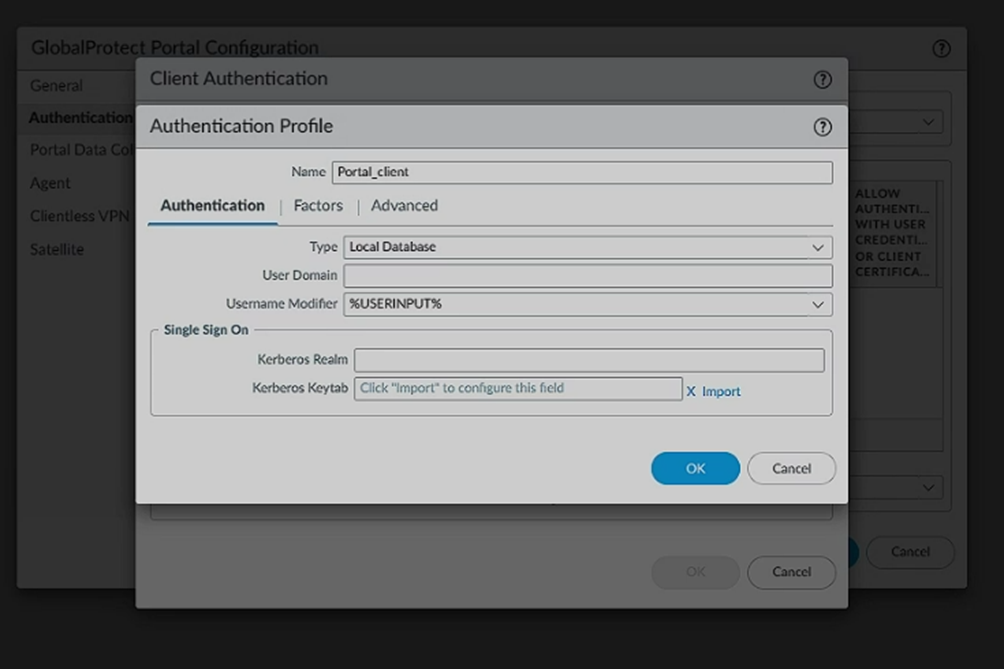


Kuvio 6. Clientin authentikointiprofiili

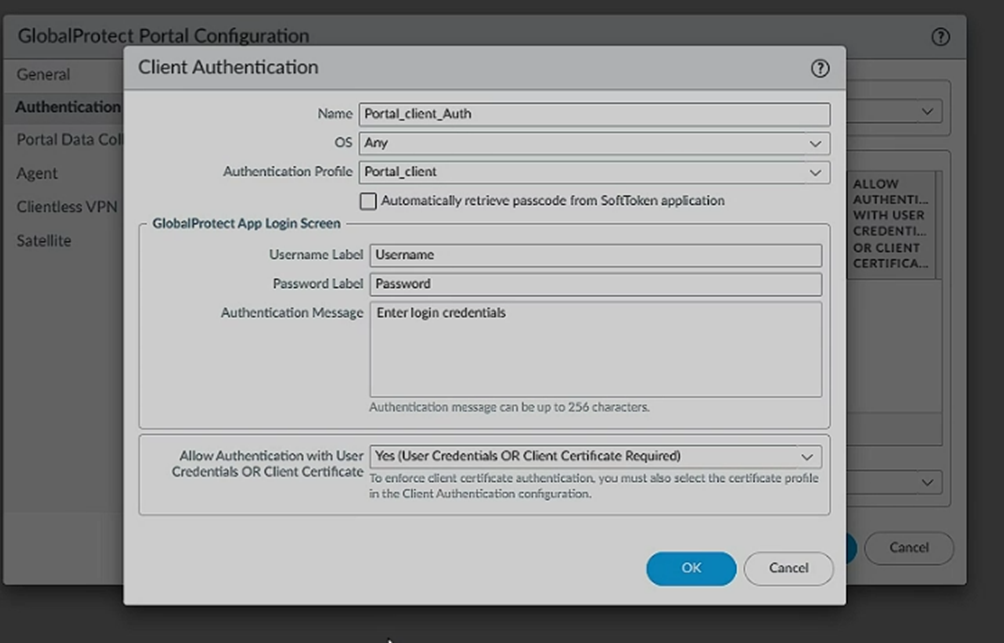


Kuvio 7. Sertifikaatin generointi

Määrittelimme nimen autentikaatioprofiilille (ks. kuvio 8). Lisäksi (ks. kuvio 9).



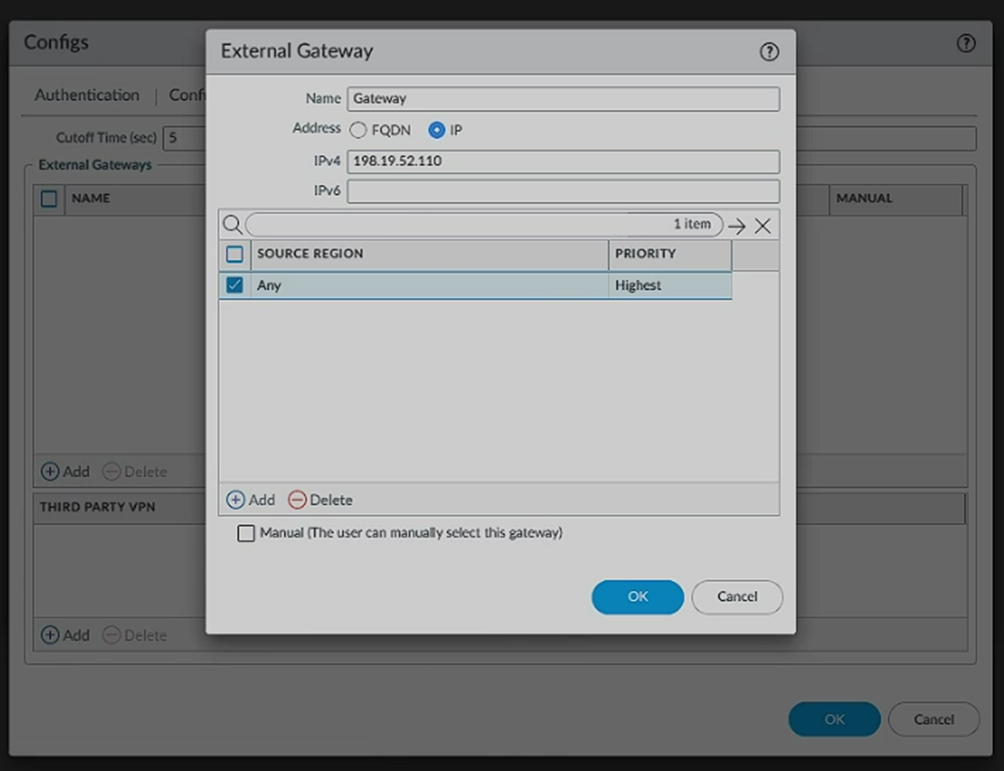
Kuvio 8. Authentikointiprofiilin määritykset



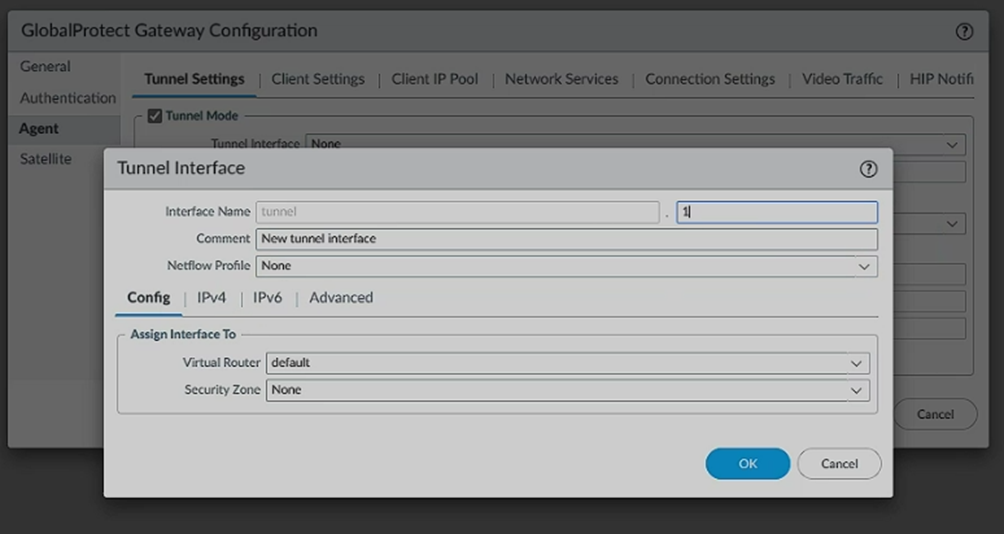
Kuvio 9. Clientin authentikaation määrityksiä

## External Gateway

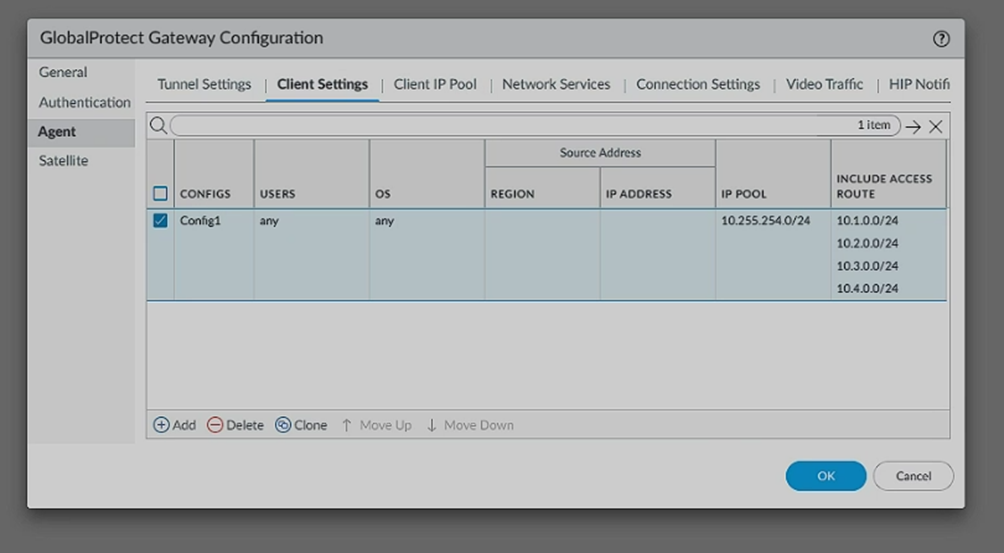
Seuraavana vuorossa oli ulkoisen yhdyskäytävän konfigurointi. Käytimme sille IP-osoitetta 198.19.52.110 (ks. kuvio 10). Myös tunnelin rajapinta piti määritellä (ks. kuvio 11). Viimeisenä laitoimme IP-poolin (ks. kuvio 12). Käytimme IP-poolia, mikä näkyi ohjeissa 10.255.254.0/24, subnet IP-osoitteet ovat aika itsestään selviä, koska ne ovat suoria osoitteita eri nettiympäristöihin esimerkiksi 10.3.0.0/24 --> Servers-net. Nämäkin näkyivät ohjeissa.



Kuvio 10. Ulkoisen yhdyskäytävän IP-osoite

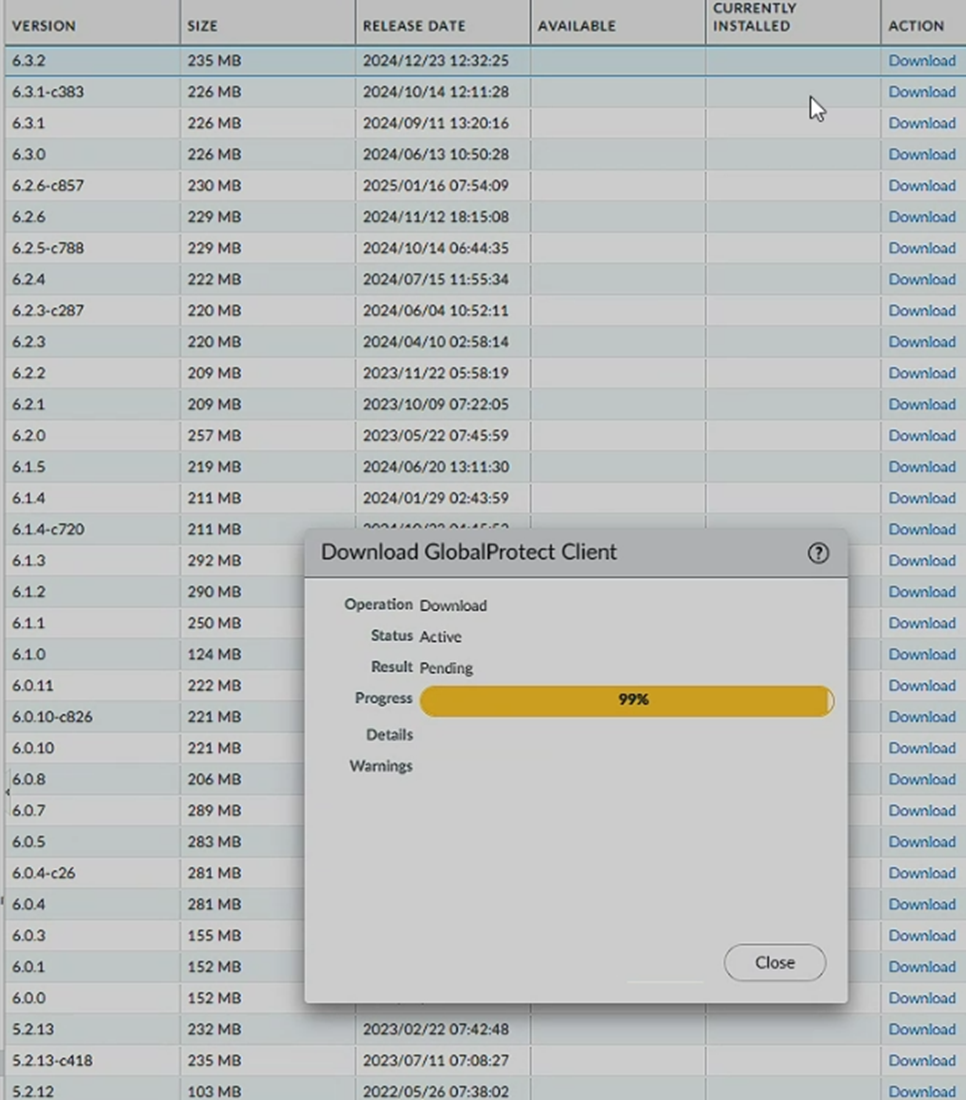


Kuvio 11. Tunneli rajapinnan määrittäminen



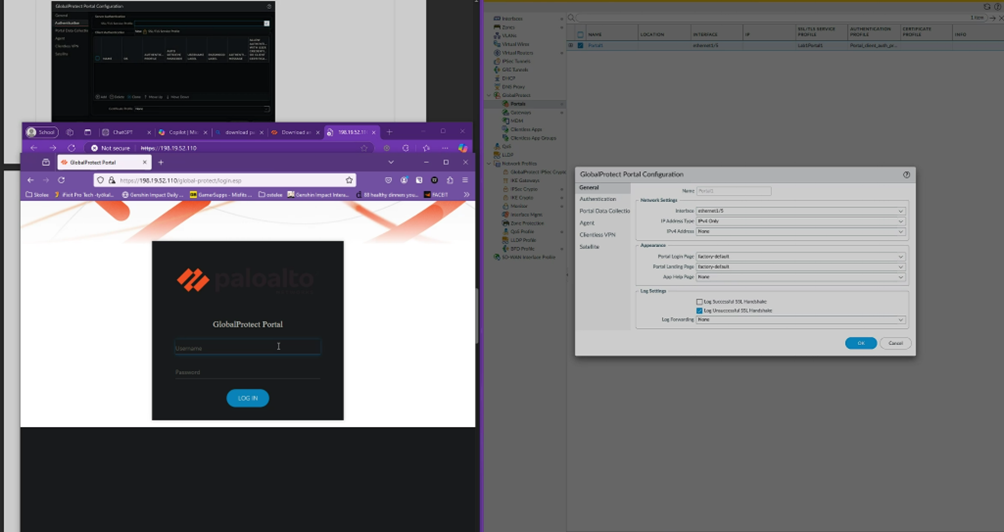
Kuvio 12. Yhdyskäytävän konfiguraation asetukset

GlobalProtect Client piti ladata (ks. kuvio 13).



Kuvio 13. GlobalProtect-clientin lataaminen

Kun ulkoinen yhdyskäytävä oli konfiguroitu oikein, GlobalProtect portaliin pääsi selaimen kautta (ks. kuvio 14).



Kuvio 14. GlobalProtect portaliin pääsee onnistuneesti

## GlobalProtect lataus ja yhdistäminen

Saimme sertifikaatin kiinnitettyä omiin koneisiimme ja sen jälkeen yhdistettyä oman GlobalProtect-portaalin (ks. kuvio 15). Sertifikaatti piti erikseen asentaa MMC:n kauttaa Trusted Root Certification Authorities kansioon. (Trusted Root Certification Authorities Certificate Store, n.d.)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 15. Yhdistäminen omaan GlobalProtect-portaaliin

## (Policy) säännöt, ssh ja rdp yhteys

Ensimmäisenä loimme uuden "security zonen" ja lisäsimme sen omaan tunneliimme sekä NAT-konfiguraatioon, jotta yhteys VLE:hen onnistuu. (ks. kuvio 16&17).

Kuva, joka sisältää kohteen teksti, viiva, kuvakaappaus, numero

Kuvaus luotu automaattisesti

Kuvio 16. VPN Zone

Kuva, joka sisältää kohteen teksti, viiva, kuvakaappaus, numero

Kuvaus luotu automaattisesti

Kuvio 17. VPN Zonen lisäys NAT

Teimme tämän jälkeen säännöt, jolla pystyimme sallimaan ssh ja rdp yhteyden toisiin ympäristön koneisiin. Alla olevassa kuvassa (ks. kuvio 18) teimme säännön, jolla saimme ssh yhteyden Admin-net ympäristön Kali-WS koneeseen.

Kuva, joka sisältää kohteen kuvakaappaus, viiva, teksti, Tontti

Kuvaus luotu automaattisesti

Kuvio 18. Sääntö SSH-yhteydelle

Kuva, joka sisältää kohteen teksti, viiva, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 19. Sääntö SSH-yhteydelle 2.0

Tässä saimme yhteyden ssh:lla Kali-WS koneeseen (ks. kuvio 20).

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 20. SSH-yhteyden muodostaminen

Teimme vielä säännön rdp yhteyden muodostamiseksi (ks. kuvio 21). Tämä yhteys on sallittu suoraan WS-net ympäristön WS01 laitteelle. Kuvassa näkyy lisäksi VPN:lle määritetty sääntö (ks. kuvo 21&22).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, viiva, Tontti

Kuvaus luotu automaattisesti

Kuvio 21. Sääntö RDP-yhteydelle

Alla olevassa kuvassa näkyy mikä on koneen IP-osoite (ks. kuvio 22).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, viiva, Fontti

Kuvaus luotu automaattisesti

Kuvio 22. Koneen IP-osoite

Yritimme yhteyden muodostamista PowerShellin kautta ja se meni läpi (ks. kuvio 23).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 23. Yhteyden muodostaminen PowerShellillä

Alla olevassa kuvassa (ks. kuvio 24) etäyhteys työpöytään.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, pussieläin, nisäkäs

Kuvaus luotu automaattisesti

Kuvio 24. Etätyöpöytäyhteyden muodostaminen

# Pohdinta

Palo Alto päivitettiin alussa, jotta commitit menevät läpi. Lisäksi osalla ryhmässä piti siirtää Palo Alto certifikaatti manuaalisesti Personal Certificates kansiosta Trusted Root Certification Authoritiesin Certificates kansioon. Labra oli itsessään mielenkiintoinen ja jokainen ryhmänjäsen sai tuntuman Palo Alton terminaaliin.

Lähteet

Bevis, R. 2022. Why Use Palo Alto? Viitattu 3.2.2025. <https://www.cbtnuggets.com/blog/certifications/security/why-use-palo-alto>.

Lab1-VPN configuration guide. N.d. JAMK Moodle. Viitattu 30.01.2025. <https://moodle.jamk.fi/pluginfile.php/1714994/course/section/158984/Lab1-VPN%20configuration%20guide.pdf?time=1737353259142.>

Set Up Access to the GlobalProtect Portal. N.d. Palo Alto dokumentaatio. Viitattu 30.01.2025. <https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/set-up-access-to-the-globalprotect-portal.>

Trusted Root Certification Authorities Certificate Store. 2024. Windows Learn. Viitattu 28.01.2025. <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-root-certification-authorities-certificate-store.>

Palo Alto Networks. N.d. World Economic Forum. Viitattu 3.2.2025. <https://www.weforum.org/organizations/palo-alto-networks/>.

Petrosyan, A. 2024. Usage of virtual private networks (VPN) worldwide as of 2nd quarter 2024, by country. Viitattu 3.2.2025. <https://www.statista.com/statistics/1382869/use-of-virtual-private-networks-vpn-by-country/?utm_source=chatgpt.com>.

What Is a Virtual Private Network (VPN)?. N.d. Cisco. Viitattu 2.3.2025. <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~related-topics>.