Labra 1

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit

9/2024

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 4](#_Toc177388167)

[2 Teoria / ympäristö tms tms 5](#_Toc177388168)

[2.1 Palo Alto 5](#_Toc177388169)

[2.2 VPN 5](#_Toc177388170)

[2.2.1 GlobalProtect 6](#_Toc177388171)

[3 Etäkäyttö 6](#_Toc177388172)

[3.1 SSH 7](#_Toc177388173)

[4 Mitä tehtiin 7](#_Toc177388174)

[4.1 Sertifikaattien luonti 8](#_Toc177388175)

[4.2 SSL/TLS palveluprofiili 11](#_Toc177388176)

[4.3 Portaalin konfigurointi 11](#_Toc177388177)

[4.4 Yhdyskäytävän konfigurointi 15](#_Toc177388178)

[4.5 GlobalProtectin käyttöönotto 19](#_Toc177388179)

[4.6 Etäkäyttö Windowsiin 23](#_Toc177388180)

[4.7 Etäkäyttö SSH:lla 26](#_Toc177388181)

[5 Pohdinta 28](#_Toc177388182)

[Lähteet 30](#_Toc177388183)

[Liitteet 31](#_Toc177388184)

[Liite 1. Lab1-VPN Configuration guide(syksy 2024) 31](#_Toc177388185)

[Liite 2. Arizona State University mmc ohje 31](#_Toc177388186)

Kuviot

[Kuvio 1. Laboratorioympäristö 5](#_Toc177377905)

[Kuvio 2 Ip-osoitteen asettaminen. 9](#_Toc177377906)

[Kuvio 3. Juuri-sertifikaatin luonti. 10](#_Toc177377907)

[Kuvio 4. Kaksi muuta sertifikaattia. 11](#_Toc177377908)

[Kuvio 5. Sertifikaatit 11](#_Toc177377909)

[Kuvio 6. SSL/TLS profiili. 12](#_Toc177377910)

[Kuvio 7. Portaalin luonti. 13](#_Toc177377911)

[Kuvio 8. Autentikointiprofiili 13](#_Toc177377912)

[Kuvio 9. Client Authetication 14](#_Toc177377913)

[Kuvio 10. Autentikointi profiili 14](#_Toc177377914)

[Kuvio 11. Asiakasohjelman luonti 15](#_Toc177377915)

[Kuvio 12 15](#_Toc177377916)

[Kuvio 13. Yhdyskäytävän luonti 16](#_Toc177377917)

[Kuvio 14. Yhdyskäytävän SSL/TLS-profiili 16](#_Toc177377918)

[Kuvio 15. Client Authetication 17](#_Toc177377919)

[Kuvio 16. Yhdyskäytävän autentikointiprofiili 17](#_Toc177377920)

[Kuvio 17. Tunnelirajapinnan valinta 18](#_Toc177377921)

[Kuvio 18. Tunnelirajapinnan luonti 19](#_Toc177377922)

[Kuvio 19. Turvallisuusalueen luonti 19](#_Toc177377923)

[Kuvio 20. Yhdyskäytävän asetukset 20](#_Toc177377924)

[Kuvio 21. Network Services -asetukset 20](#_Toc177377925)

[Kuvio 22. GlobalProtectin version valinta 21](#_Toc177377926)

[Kuvio 23. Testikäyttäjän luonti 21](#_Toc177377927)

[Kuvio 24. GlobalProtect portaali 22](#_Toc177377928)

[Kuvio 25. Sertifikaatin lataaminen 22](#_Toc177377929)

[Kuvio 26.GlobalProtectin käyttöönotto 23](#_Toc177377930)

[Kuvio 27. GlobalProtect yhdistettynä 23](#_Toc177377931)

[Kuvio 28. Turvallisuussäännön luonti 24](#_Toc177377932)

[Kuvio 29. Turvallisuus säännön asetukset 25](#_Toc177377933)

[Kuvio 30. Windows etäyhteyden avaaminen 25](#_Toc177377934)

[Kuvio 31. Etäyhteys on saavutettu! 26](#_Toc177377935)

[Kuvio 32. Turvallisuussäännön luonti SSH:ta varten 27](#_Toc177377936)

[Kuvio 33. Turvallisuus säännöt admin-net 28](#_Toc177377937)

[Kuvio 34. SSH-yhteyden luominen 29](#_Toc177377938)

# Johdanto

Kyberturvallisuus-moduulin kurssilla Tietoturvakontrollit ensimmäisessä tehtävässä (Lab1) oli tarkoituksena saada **PaloAlto** palomuurin avulla **GlobalProtect VPN**- yhteys ryhmälle luotuun laboratorio ympäristöön. Labrassa tuli saada turvallinen yhteys ympäristön sisäverkkoon ja sen laitteisiin käyttäen **SSH**- ja **RDP**-protokollia.

Ohjeistuksena työhön annettiin kuva ympäristöstä (Kuvio 1.), jossa näkyi verkon segmentointi (Työasemaverkko (WS-Net), Hallintoverkko (Admin-Net), Palvelinverkko (Servers-Net) ja DMZ (Demilitarized Zone)) ja laitteiden IP osoitteet. Labraa varten annettiin myös PaloAlto palomuurin konfigurointiohjeet GlobalProtectin asennusta varten. (Liite 1.)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, diagrammi, muotoilu

Kuvaus luotu automaattisesti

Kuvio 1. Laboratorioympäristö

# Teoria / ympäristö tms tms

Tässä labrassa keskityimme virtuaalikone Palo Alto-palomuurin konfiguraation tekemiseen ja sen kautta Global Protect VPN- yhteyden saamiseen. Sen jälkeen SSH ja RDP yhteyksiä käyttäen voimme ottaa yhteyden ympäristön koneisiin. Ympäristönä toimi ryhmälle annettu VLE- ympäristön palomuuri ja muut koneet sekä GlobalProtect portaali. Palo Alto- palomuuri sisältää edistyneitä tietoturvaominaisuuksia sekä se on monipuolinen palomuuri suojata verkkoympäristöjä. Palo Alto hallinnoi ja valvoo liikennettä meidän ympäristön sisäverkkojen välillä. Yläpuolella kuvassa näkyy konkreettisesti meidän käyttämämme ympäristö.

## Palo Alto

Palo Alto on yhdysvaltalainen kyberturvallisuus yritys, joka tarjoaa asiakkailleen edistyksellisiä palomuureja ja niihin liittyviä pilvipalveluita. Tässä harjoituksessa käytimme Palo Alton palomuuria, joka toimii virtuaalikoneena. Palomuurin toiminta perustuu sääntöjen, profiilien ja muiden tietoturvaominaisuuksien hallintaan. (About us. 2024.)

## VPN

Virtuaalinen erillisverkko eli Virtual Private Network (**VPN**) on teknologia, joka luo suojatun ja salatun yhteyden laitteen ja VPN-palvelimen välille. VPN:llä voidaan luoda salattu yhteys VPN-palvelimeen, jolloin kaikki liikenne kulkee sen kautta. VPN:a käyttäessä myös käyttäjän IP-osoite korvataan palvelimen IP-osoitteella ja kaikki tieto kulkee VPN-tunnelin kautta. Näin yhteys on yksityisempi ja mahdollinen tietojen urkinta voidaan estää. Tässä labrassa VPN-yhteyden muodostaminen tehtiin **GlobalProtectilla**, jolla otettiin yhteys **Palo Alto** palomuurin kautta laboratorio ympäristön sisäverkkoon. (What is a VPN? 2024.)

### GlobalProtect

GlobalProtect on Palo Alto Networksin sovellus, jonka avulla saadaan etätyöyhteys halutun ympäristön sisäverkkoon riippumatta käyttäjän omasta fyysisestä sijainnista. GlobalProtect on Palo Alton kehittämä VPN-ratkaisu, joka on suunniteltu tarjoamaan turvallinen pääsy organisaation säiseen verkkoon, kuten tietokoneet ja verkkolevyt, etäkäyttäjille. GlobalProtectin avulla yritykset voivat käyttää tarkkoja pääsynhallintapolitiikkoja, eli esimerkiksi eri käyttäjille voidaan määritellä erilaiset käyttö- ja pääsyoikeudet. (GlobalProtect overview. 2024)

GlobalProtect koostuu käyttäjän laitteelle asennettavasta GlobalProtect-sovelluksesta ja yhdyskäytävästä (gateway), joka on osa palomuuria. GlobalProtect muodostaa suojatun yhteyden yhdyskäytävään. Käyttääkseen GlobalProtectia käyttäjän täytyy tunnistautua käyttämällä tunnusta ja salasanaa, erillistä varmennetta tai monivaiheista tunnistautumista. Tunnistautumisen vahvuus voidaan määritellä GlobalProtectia käyttöön ottaessa. Onnistuneen tunnistautumisen jälkeen yhteys salataan SSL/TLS-protokollan avulla. Kaikki käyttäjän verkkoliikenne reititetään yhdyskäytävän kautta, joka soveltaa palomuurissa asetettuja politiikkoja ja GlobalProtect tarkistaa liikenteen mahdollisten uhkien varalta. (GlobalProtect. 2024.)

# Etäkäyttö

Windowsin etätyöpöytä (Remote Desktop Connection, RDC) työkalulla mahdollistamme tietokoneen etäkäytön. Voimme käyttää toisen tietokoneen työpöytää, aplikaatioita ja tiedostoja ikään kuin olisimme fyysisesti tietokoneen ääressä. Tässä labrassa sallimme etäkäytön turvallisuus säännöllä Palo Alto- palomuurista, ja yhdistämme Windowsin etätyöpöytäyhteys -sovelluksella yhteyden virtuaalikoneeseen.

RDP:n käytössä on tärkeätä rajata pääsyä yhteyteen luvattomilta tekijöiltä. Esimerkiksi luomalla RDP-pääsyoikeuskäytäntöjä käyttäen palomuureja pääsyn hallintaan tietyistä IP-osoitteista tai verkostoista. Turvallisuutta voitaisiin parantaa myös vahvoilla salasanoilla tai kahden tekijän todennuksella (2FA).

## SSH

SSH (Secure Shell) on protokolla, joka mahdollistaa turvallisen yhteyden muodostamisen kahden tietokoneen välillä salaamalla tiedonsiirron. Näin saadaan yhteys saadaan ulkopuolisilta ja estettyä tietojen kalastelu. Protokollaa käytetään usein komentorivin kautta ja sen avulla voidaan esimerkiksi siirtää tiedostoja, suorittaa komentoja etäjärjestelmässä ja hallita verkon laitteita.

Yksi SSH:n hyödyllisimmistä ominaisuuksista on porttien edelleenlähetys (port forwarding), jonka avulla voidaan esimerkiksi turvallisesti käyttää sisäisiä resursseja ulkoisen yhteyden kautta. SSH salaa yhteyden, joten se tarjoaa myös suojan tiedonsiirrolle julkisissa verkoissa. SSH-protokolla on keskeinen työkalu turvallisen verkonhallinan ja ehtäyhteyksien toteuttamisessa. (Mikä on SSH? 2024; What is SSH? | Secure Shell (SSH) protocol. 2024.)

Tässä labrassa otettiin SSH-etähallintayhteys sisäverkon päätelaitteisiin, kun VPN-yhteys oli aktivoitu.

# Mitä tehtiin

Kirjauduimme Palo Alton palomuurin hallintasivustolle (<https://198.19.50.30>), jossa suoritimme palomuurin ja GlobalProtectin konfiguroinnin. Näiden tekemiseen käytimme apuna Palo Alton omia ohjeita (Knowledgebase. 2024.) ja tehtävän annon yhteydessä ollutta ohjetta (Liite 1). Ensimmäisenä kuitenkin aktivoimme koulun meille tarjoaman Palo Alton virtuaaliympäristön lisenssin ja vaihdoimme palomuurin yleisen IP-osoitteen oikeaksi. (Kuvio 2.) Oikea IP-osoite löytyi Networks-välilehteä tutkimalla.Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

Kuvio 2 Ip-osoitteen asettaminen.

## Sertifikaattien luonti

Seuraavaksi loimme kolme sertifikaattia, jotka tarvitsemme myöhemmin yhdyskäytävää ja GlobalProtectin sovellusta varten. Sertifikaattien luonti tapahtui palomuurin device -välilehdeltä Certificates-otsikon alta. Ensimmäisenä loimme juuri-sertifikaatin RootCA (kuvio 3), joka toimii muiden luotavien sertifikaattien vahvistajana.

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

Kuvaus luotu automaattisesti

Kuvio 3. Juuri-sertifikaatin luonti.

Tämän jälkeen loimme jäljelle jäävät kaksi muuta sertifikaattia (kuvio 4). Tässä vaiheessa oli tärkeää, että allekirjoittajaksi (signed by) tuli aiemmin luoto juurisertifikaatti RootCA.

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

Kuvaus luotu automaattisesti

Kuvio 4. Kaksi muuta sertifikaattia.

Lopputuloksena syntyi kolmesertifikaattia, joista ylimpänä oli RootCA (kuvio 5.)

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

Kuvaus luotu automaattisesti

Kuvio 5. Sertifikaatit

Sertifikaattien tarkoituksena on varmistaa sekä käyttäjän että portaalin/gatewayn luotettavuus ja estää luvattomien käyttäjien pääsy verkkoon. Emme vielä luo sertifiointi profiileja yksinkertaistaaksemme ongelmien etsimistä ja ratkomista.

## SSL/TLS palveluprofiili

Seuraavaksi loimme SSL-TLS palveluprofiilin. Luonti tapahtui Device-välilehdellä Certificate Management otsikon alta kohdasta SSL/TLS Service Profile. Käytimme vain yhtä profiilia, koska sama rajapinta toimii sekä portaalina että yhdyskäytävänä. Sertifikaattina käytimme aiemmin luotua Portal1\_True-sertifikaattia (kuvio 6.).

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

Kuvaus luotu automaattisesti

Kuvio 6. SSL/TLS profiili.

GlobalProtectin yhteydessä tätä profiilia käytetään määrittämään GlobalProtect-portaalin/gatewayn "palvelinvarmenne" ja SSL/TLS "protokollaversioiden valikoima (<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFoCAK>)

## Portaalin konfigurointi

Portaalin konfiguraation aloitimme luomalla portaalin palomuurin Network-välilehdeltä GlobalProtect otsikon alta Portal kohdasta klikkaamalla Add-painiketta. Nimesimme portaalin mielikuvituksellisesti nimellä Portal1(kuvio 7) ja asetimme rajapinnaksi ethernet 1/5 ohjeiden (liite 1) mukaan.

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

Kuvaus luotu automaattisesti

Kuvio 7. Portaalin luonti.

Seuraavaksi siirryimme Authentication -välilehdelle ja valitsimme käyttöön aiemmin luomamme SSL/TLS profiilin. (Kuvio 8).

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

Kuvaus luotu automaattisesti

Kuvio 8. Autentikointiprofiili

Tämän jälkeen painoimme Add-painiketta Client authentication otsikon alta (kuvio 8). Vaihdoimme Allow Authentication with User Credentials OR Client Certificate kohtaan valinnaksi Yes (User Credentials OR Client Certificate Required) (kuvio 9).

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

Kuvaus luotu automaattisesti

Kuvio 9. Client Authetication

Kuvio 9:n Authentication Profile kohtaan loimme uuden profiilin nimeltä Portal\_client. Tyypiksi vaihdoimme paikallinen tietokanta (Local Database) (kuvio 10.)

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

Kuvaus luotu automaattisesti

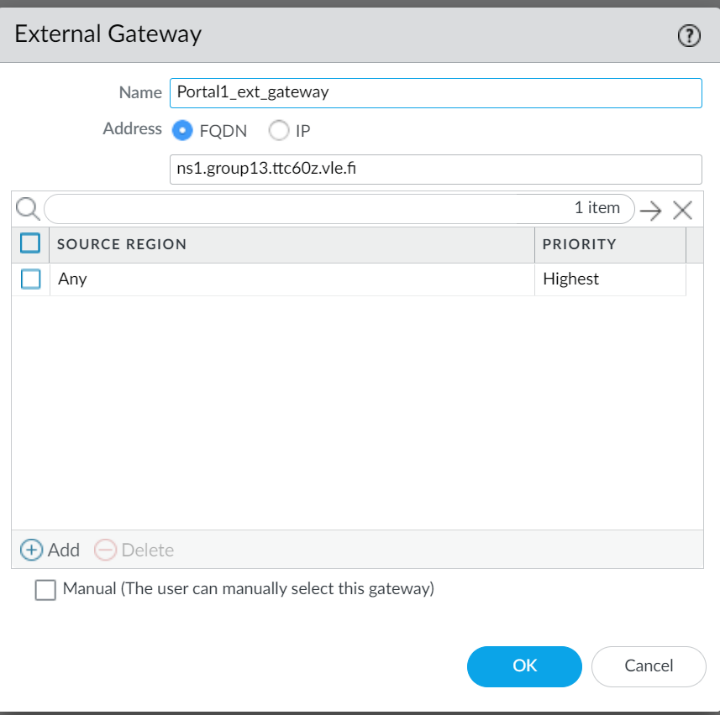
Kuvio 10. Autentikointi profiili

Siirryimme seuraavaksi Agent-välilehdelle ja loimme uuden kuvion 11 mukaisesti. Sertifikaattina käytimme aiemmin luotua GP\_ClientCert:iä.  
Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 11. Asiakasohjelman luonti

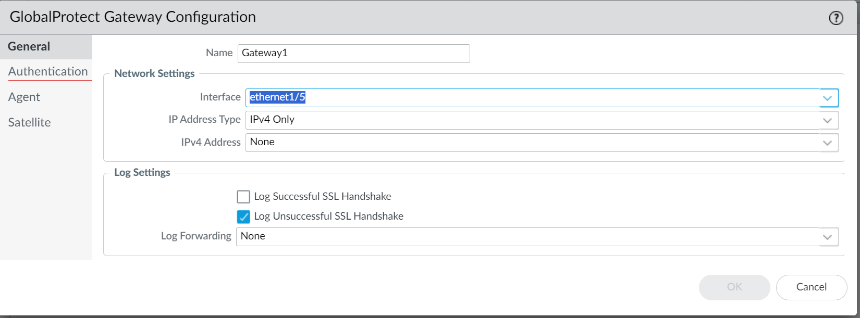
Siirryimme External-välilehdelle (kuvio 12) ja nimesimme yhdyskäytävän Portal1\_ext\_gateway:ksi. Osoitteeksi asetimme meidän palvelimemme nimen eli ns1.group13.ttc60z.vle.fi. Tästä osoitteesta pystymme jatkossa lataamaan GlobalProtectin omille tietokoneillemme. Tähän olisi voinut vaihtaa myös palvelimemme IP-osoitteen 198.19.50.85, jos valinnan olisi vaihtanut FDQN:stä IP:ksi. Lähdealueeksi laitoimme ohjeen (liite 1) mukaisesti Any eli mikä tahansa. Tämän aiomme myöhemmin muuttaa paremmin meidän tarkoituksiimme sopivaksi, koska ainakaan tällä hetkellä kaikkialta maailmasta ei ole tarvetta saada yhteyttä meidän GlobalProtect portaaliimme.



Kuvio 12

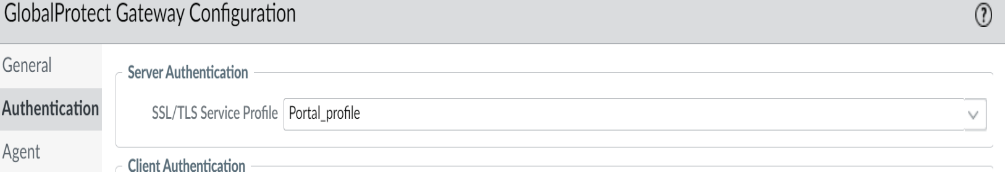
## Yhdyskäytävän konfigurointi

Kun olimme saaneet portaalin valmiiksi, siirryimme GlobalProtectin yhdyskäytävän (gateway) luontiin. Tämän löysimme palomuurin Network-välilehdeltä GlobalProtect otsikon alta kohdasta Gateways. Painoimme Add-painiketta luodaksemme uuden yhdyskäytävän. Nimesimme yhdyskäytävän nimellä Gateway1 ja asetimme rajapinnaksi ethernet1/5, joka toimii etäpisteiden sisääntulorajapintana. (Kuvio 13).



Kuvio 13. Yhdyskäytävän luonti

Authentication välilehdelle vaihdoimme SSL/TLS-profiiliksi portaalin luonnin yhteydessä tehdyn Portal\_profilen. (Kuvio 14)



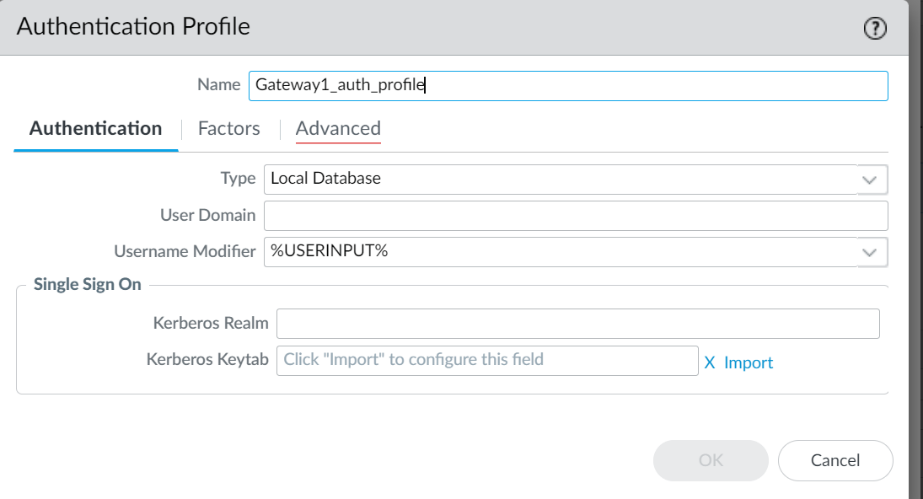
Kuvio 14. Yhdyskäytävän SSL/TLS-profiili

Jatkoimme Client Authentication -kohtaan ja lisäsimme uuden Add-painikkeesta ja nimesimme sen nimellä Gateway1\_client. Vaihdoimme alimmaiseen kenttään taas Yes, kuten portaalia luodessa samassa kohdassa. (kuvio 15).

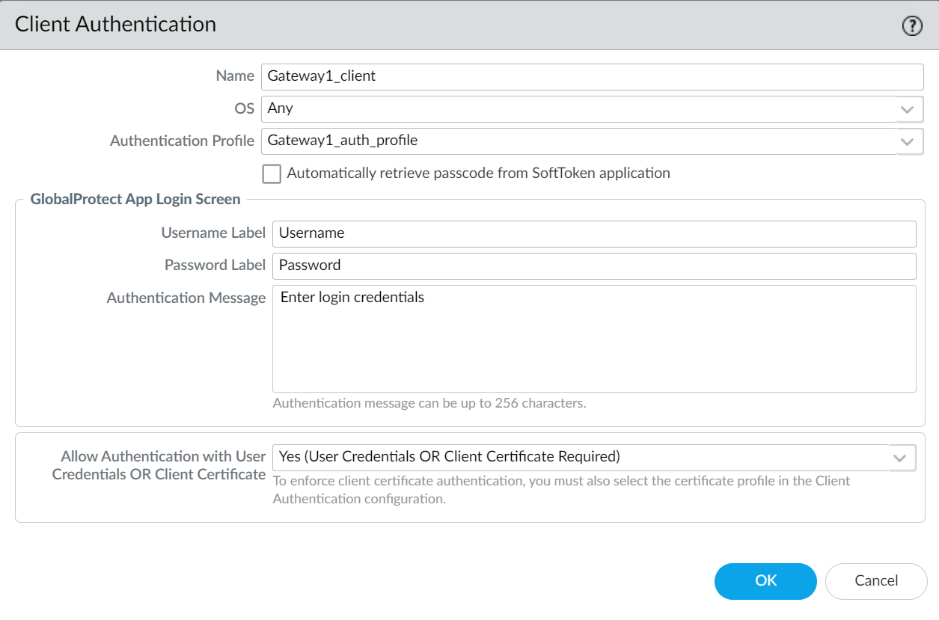
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

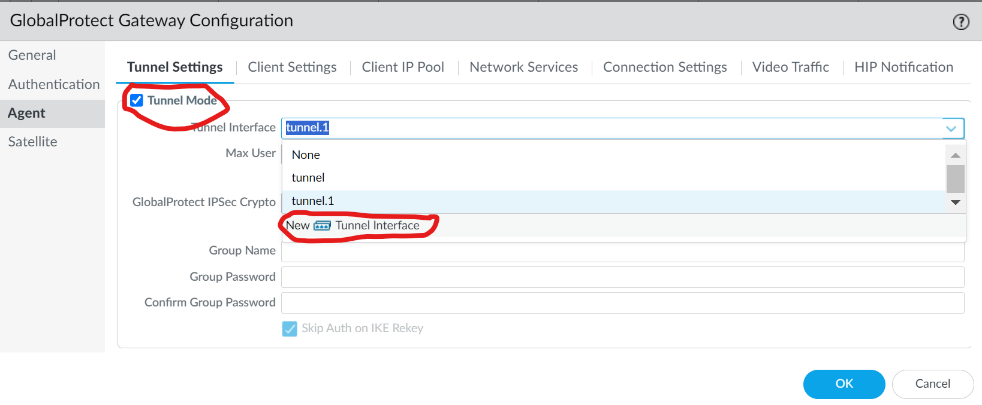
Kuvio 15. Client Authetication

Autentikointiprofiili -kohtaan loimme uuden profiilin nimellä Gateway1\_auth\_profile ja vaihdoimme tyypiksi paikallinen tietokanta (Local Database). (Kuvio 16)  


Kuvio 16. Yhdyskäytävän autentikointiprofiili

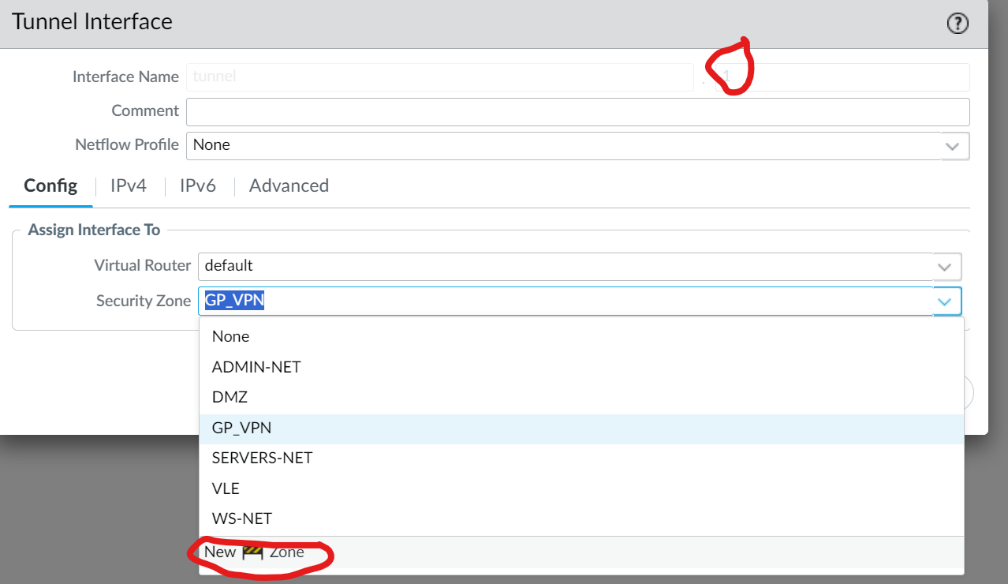


Siirryimme Agent-välilehdelle ja valitsimme kohdan “Tunnel Mode” ja loimme uuden tunnelirajapinnan. (Kuvio 17).



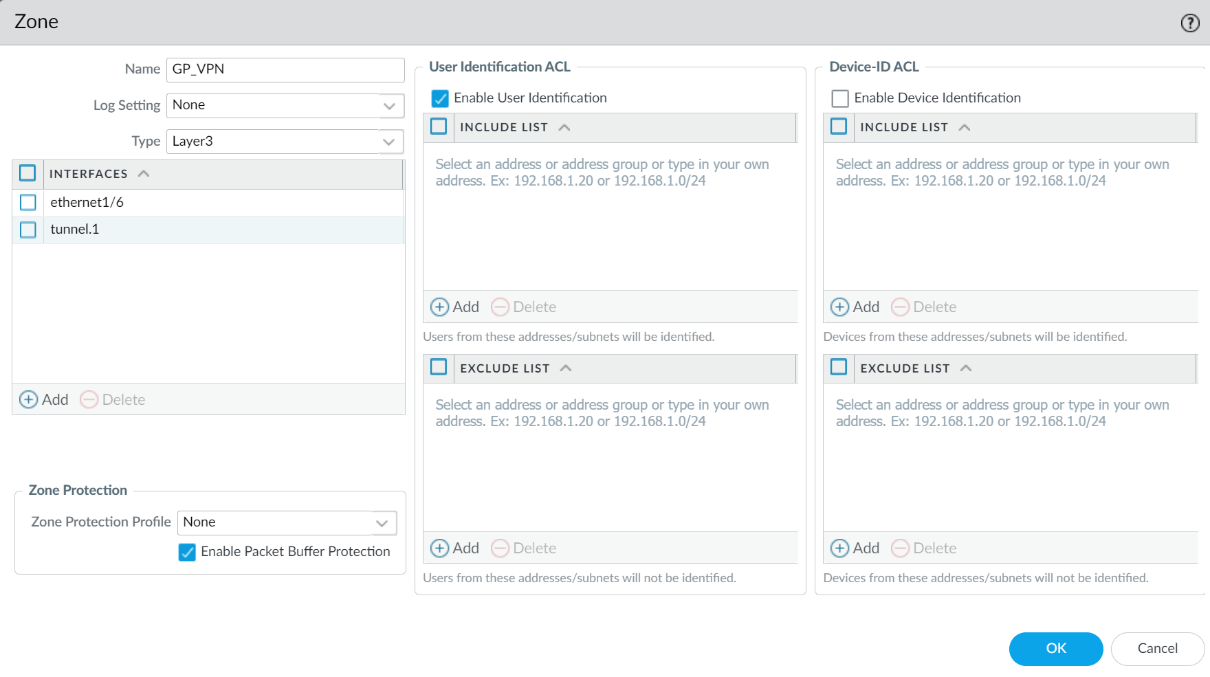
Kuvio 17. Tunnelirajapinnan valinta

Annoimme tunnelirajapinnalle numeron 1, vaihdoimme virtuaaliseksi reitittimeksi valinnan default ja loimme uuden turvallisuusalueen (Security Zone) nimeltä GP\_VPN. (Kuvio 18).



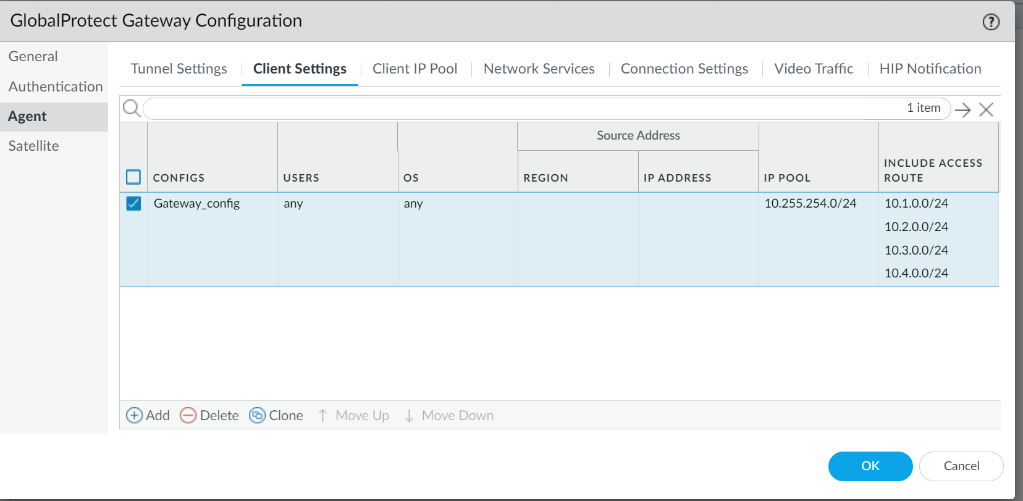
Kuvio 18. Tunnelirajapinnan luonti

Uuden turvallisuusalueen luomiseksi valitsemme rajapinnaksi ethernet1/6. Tunnel.1 -tunneli on jo valmiiksi rajapintojen alla, koska valitsimme luoda sille uuden turvallisuusalueen. Laitoimme myös käyttäjän tunnistuksen käyttöön (Enable User Identification). Tämän jälkeen turvallisuusalue ja tunneli olivat valmiita. (Kuvio 19).



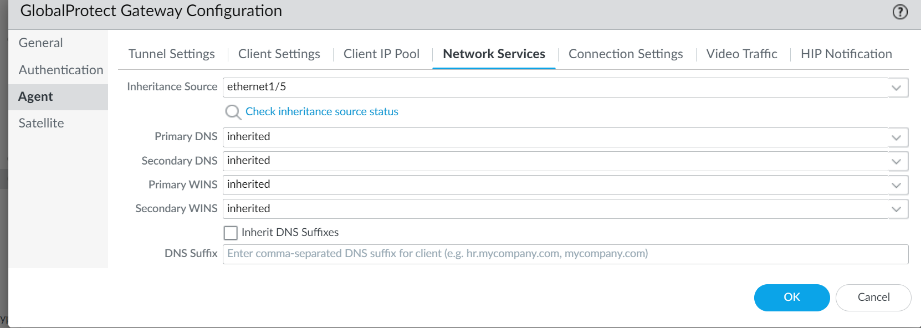
Kuvio 19. Turvallisuusalueen luonti

Siirryimme Client Settings -välilehdelle ja loimme uuden asetuksen nimeltä Gateway\_config. Asetimme IP-osoiteavaruudeksi ohjeen mukaan 10.255.254.0/24. Tällä määrittelimme IP-avaruuden, joka jaetaan GlobalProtect VPN:n käyttäjille. Split Tunnel osiossa lisäsimme kuvion 20 mukaiset IP-osoitteet, jotka ovat oman verkkomme osoitteita. Ne näkyvät otsikon Include Access Route alla.



Kuvio 20. Yhdyskäytävän asetukset

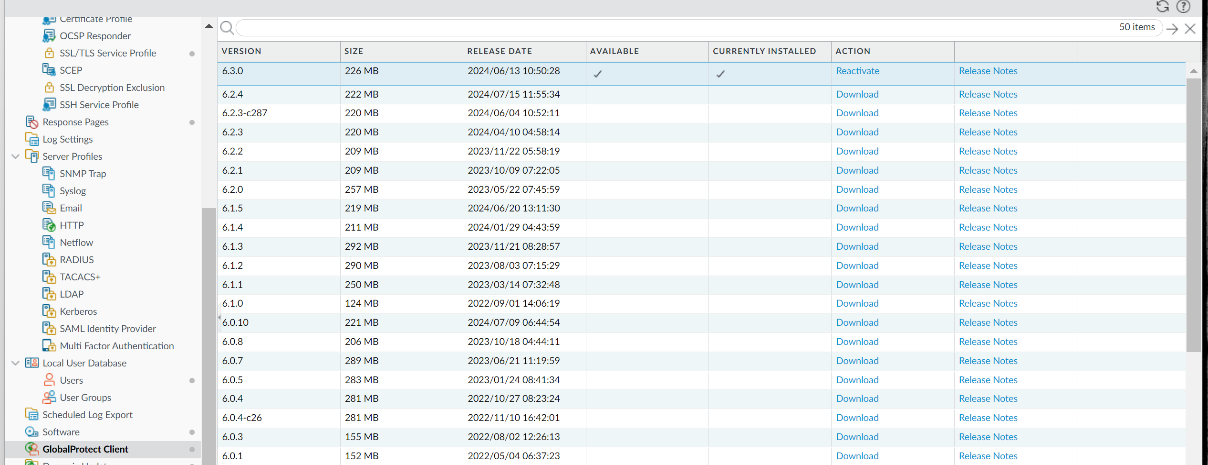
Network services -välilehdelle syötimme kuvion 21 mukaiset asetukset. Rajapinnan lähteeksi valitsimme ethernet1/5 ja kaikkiin muihin kohtiin inherit eli ominaisuudet periytyvät valitulta lähteeltä.



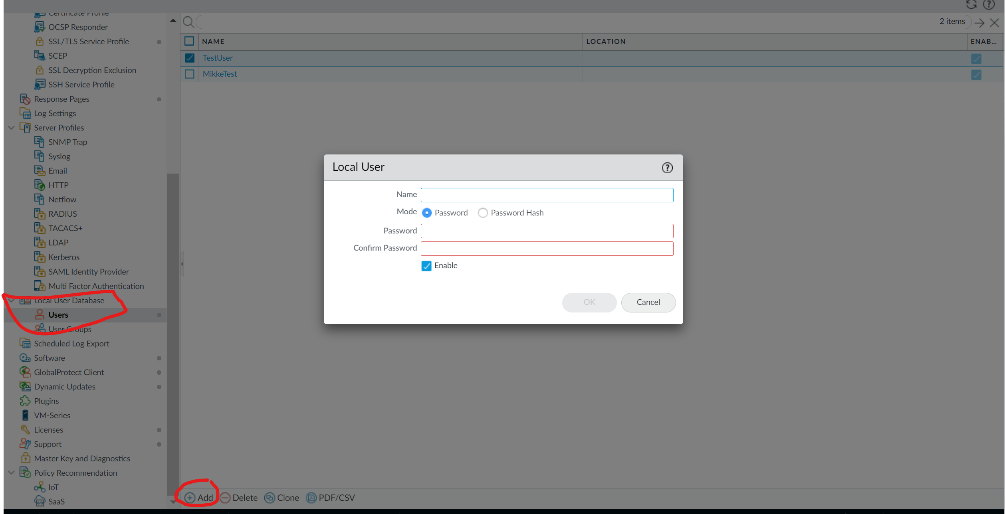
Kuvio 21. Network Services -asetukset

## GlobalProtectin käyttöönotto

Ennen GlobalProtectin asentamista omalle koneelle menimme palomuurin käyttöliittymässä Device-välilehdelle ja GlobalProtect Client-otsikon alta valitsimme käyttöön Global Protectin uusimman version eli version 6.3.0. (Kuvio 22).



Kuvio 22. GlobalProtectin version valinta

Lisäsimme vielä itsellemme testikäyttäjän Device-välilehdeltä Local User Database -> Users -> Add. Nimesimme käyttäjän nimellä TestUser ja asetimme sille salasanan. (Kuvio 23).   


Kuvio 23. Testikäyttäjän luonti

Avasimme selaimelle uuden välilehden ja menimme aiemmin asettamaamme osoitteeseen ns1.group13.ttc60z.vle.fi, josta pääsimme kirjautumaan portaaliin testikäyttäjällä ja lataamaan GlobalProtectin omalle tietokoneellemme. (Kuvio 24).

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

Kuvaus luotu automaattisesti

Kuvio 24. GlobalProtect portaali

Ennen GlobalProtectin käyttöönottoa asensimme luomamme sertifikaatin RootCA omille tietokoneillemme. Ensimmäisenä latasimme sertifikaatin Palo Altosta (Kuvio 25.)Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, tietokone

Kuvaus luotu automaattisesti

Kuvio 25. Sertifikaatin lataaminen

Seuraavaksi avasimme mmc:n Microsoft Management Consolen ja asensimme sertifikaatin tietokoneellemme Arizone State Universityn ohjeen mukaisesti. (Liite 2).

Asensimme ladatun GlobalProtectin ja aloitimme sen käyttöönoton. Ensimmäiseen kenttään kirjoitimme portaalin osoitteen ja sen jälkeen annamme käyttäjätunnuksen ja salasanan jonka loimme aiemmin. (Kuvio 26)

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

Kuvaus luotu automaattisesti

Kuvio 26.GlobalProtectin käyttöönotto

Kirjautumisen jälkeen GlobalProtect oli toiminnassa (Kuvio 27.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, logo, graafinen suunnittelu

Kuvaus luotu automaattisesti

Kuvio 27. GlobalProtect yhdistettynä

## Etäkäyttö Windowsiin

Etäkäytön RDP:n avulla mahdollistamiseksi teimme uuden turvallisuussäännön palomuuriin Policies-välilehdeltä Security-otsikon alta Add-painiketta painamalla (kuvio 28). Nimesimme säännön nimellä VPN-to-WS-net, koska WS-net on se turvallisuusalue, jonka alla verkkomme virtuaalinen Windows-työasema on. Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, tietokone

Kuvaus luotu automaattisesti

Kuvio 28. Turvallisuussäännön luonti

Asetimme lähteeksi turvallisuusalueen GP\_VPN ja kohteeksi WS-Net:in. Application välilehdellä valitsimme aplikaatioksi ms-rdp ja actions-välilehdeltä allow. (Kuvio 29).

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

Kuvaus luotu automaattisesti

Kuvio 29. Turvallisuus säännön asetukset

Kun turvallisuussääntö oli valmis varmistimme, että GlobalProtect omalla koneellamme oli päällä, jonka jälkeen avasimme Etätyöpöytäyhteys -sovelluksen, syötimme Windows-työaseman IP-osoitteen 10.1.0.10. (Kuvio 30.) Tunnusta ja salasanaa kysyttäessä annoimme ohjeissa annetun User -käyttäjätunnuksen ja salasanan.

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

Kuvaus luotu automaattisesti

Kuvio 30. Windows etäyhteyden avaaminen

Pienen latailun jälkeen yhteys avautui ja pääsimme käyttämään virtuaalikonetta GlobalProtect VPN:n avulla. (Kuvio 31).

Kuva, joka sisältää kohteen vesi, kuvakaappaus, ohjelmisto, järvi

Kuvaus luotu automaattisesti

Kuvio 31. Etäyhteys on saavutettu!

## Etäkäyttö SSH:lla

Ottaaksemme yhteyden SSH:n avulla adminverkon laitteeseen Kali-WS, loimme vielä toisen turvallisuussäännön palomuuriin noudattaen samaa periaatetta kuin aiemmin RDP-yhteyden sallimisen yhteydessä (kuvio 32). Sääntö nimettiin VPN\_to\_admin\_net, saman periaatteen mukaisesti kuin aiemmin.

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

Kuvaus luotu automaattisesti

Kuvio 32. Turvallisuussäännön luonti SSH:ta varten

Asetimme lähteeksi turvallisuusalueen GP\_VPN ja kohteeksi ADMIN-NET. Application-välilehdellä valitsimme aplikaatioksi SSH sekä ping testaamisen vuoksi ja Actions-välilehdeltä allow. (Kuvio 33).

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

Kuvaus luotu automaattisesti

Kuvio 33. Turvallisuus säännöt admin-net

Tämän jälkeen pystyimme omalla tietokoneella ottamaan yhteyden SSH:lla Kali virtuaalikoneeseen GlobalProtectin päällä ollessa syöttämällä Windowsin komentokehotteella komennon ”ssh [kali@10.2.0.13](mailto:kali@10.2.0.13)”. Kali on käyttäjä, jolla kirjaudumme ja 10.2.0.13 on Kali-WS:n IP- osoite. Komennon jälkeen syötetään salasana ja yhteys on muodostettu. (Kuvio 34).

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

Kuvaus luotu automaattisesti

Kuvio 34. SSH-yhteyden luominen

# Pohdinta

Labran aikana pääsimme tutustumaan Palo Alton palomuurin toimintaan ja luomaan GlobalProtectille sertifikaatin, portaalin ja yhdyskäytävän. Teimme myös turvallisuussääntöjä, jotka mahdollistivat etäyhteyden oman fyysisen tietokoneen ja labraympäristössä olevien virtuaalikoneiden välille.

Labra oli kaiken kaikkiaan mielenkiintoinen, vaikka GlobalProtectin käyttöönotto aiheuttikin alkuun vähän harmaita hiuksia. Palomuurin käyttö vaikutti aluksi monimutkaiselta, koska sen käyttöliittymä on niin laaja ja siellä oli paljon välilehtiä ja toimintoja, joita emme vielä päässeet käyttämään. Löysimme kuitenkin meille tehtävänannon yhteydessä annetun ohjeen lisäksi muita ohjeita, ja saimme vaikeuksista huolimatta niiden avulla GlobalProtectin käyttöön ja toimimaan. Suuri apu oli myös muiden ryhmien kanssa keskustelu ja vinkkien jako.

Labraa tehdessä käytännön lisäksi pääsimme syventymään teoriaan siitä, mikä on RDP ja SSH. Molemmat näistä ovat protokollia, joita tulemme varmasti hyödyntämään tulevaisuudessakin niin koulutehtävissä kuin työelämässäkin.

Lähteet

About Us. Palo Alto verkkosivut. 2024. Viitattu 15.9.2024. <https://www.paloaltonetworks.com/about-us>

GlobalProtect. Paloguard.com -verkkosivusto. 2024. Viitattu 15.9.2024. <https://www.paloguard.com/GlobalProtect.asp>

GlobalProtect overview. Palo Alto TechDocs. 2024. Viitattu 14.9.2024. <https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-overview>

Certificate config for GlobalProtect. Paloalto Knowledgebase. 25.9.2018. Viimeksi muokattu 25.8.2022. Viitattu 10.9.2024. <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFoCAK>

Mikä on SSH? One.com. 2024. Viitattu 16.9.2024. <https://www.one.com/fi/webhotelli/mika-on-secure-shell>

What is SSH? | Secure Shell (SSH) protocol. Cloudflare.com. 2024. Viitattu 16.9.2024. <https://www.cloudflare.com/learning/access-management/what-is-ssh/>

What is a VPN? F-secure.com verkkosivusto. 2024. Viitattu 15.9.2024. <https://www.f-secure.com/en/articles/what-is-a-vpn>

What is SSH? Secure Shell (SSH) protocol. Cloudflare.com -verkkosivusto. 2024. Viitattu 14.9.2024. <https://www.cloudflare.com/learning/access-management/what-is-ssh/>

Liitteet

Liite 1. Lab1-VPN Configuration guide(syksy 2024)

https://moodle.jamk.fi/pluginfile.php/1460933/mod\_label/intro/Lab1-VPN%20configuration%20guide%28syksy2024%29.pdf

Liite 2. Arizona State University mmc ohje

https://asu.my.salesforce-sites.com/kb/articles/FAQ/How-Do-I-Add-Certificates-to-the-Trusted-Root-Certification-Authorities-Store-for-a-Local-Computer