



## 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

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Johdanto.....</b>                                    | <b>4</b>  |
| <b>2</b> | <b>Teoria / ympäristö tms tms .....</b>                 | <b>5</b>  |
| 2.1      | Palo Alto.....  | 5         |
| 2.2      | VPN .....   | 5         |
| 2.2.1    | GlobalProtect .....                                     | 6         |
| <b>3</b> | <b>Etäkäyttö .....</b>                                  | <b>6</b>  |
| 3.1      | SSH .....   | 7         |
| <b>4</b> | <b>Mitä tehtiin.....</b>                                | <b>7</b>  |
| 4.1      | Sertifikaattien luonti.....                             | 8         |
| 4.2      | SSL/TLS palveluprofiili.....                            | 11        |
| 4.3      | Portaalin konfigurointi.....                            | 11        |
| 4.4      | Yhdyskäytävän konfigurointi.....                        | 15        |
| 4.5      | GlobalProtectin käyttöönotto .....                      | 19        |
| 4.6      | Etäkäyttö Windowsiin.....                               | 23        |
| 4.7      | Etäkäyttö SSH:lla.....                                  | 26        |
| <b>5</b> | <b>Pohdinta .....</b>                                   | <b>28</b> |
|          | <b>Lähteet .....</b>                                    | <b>30</b> |
|          | <b>Liitteet .....</b>                                   | <b>31</b> |
|          | Liite 1. Lab1-VPN Configuration guide(syksy 2024) ..... | 31        |
|          | Liite 2. Arizona State University mmc ohje.....         | 31        |

## Kuviot

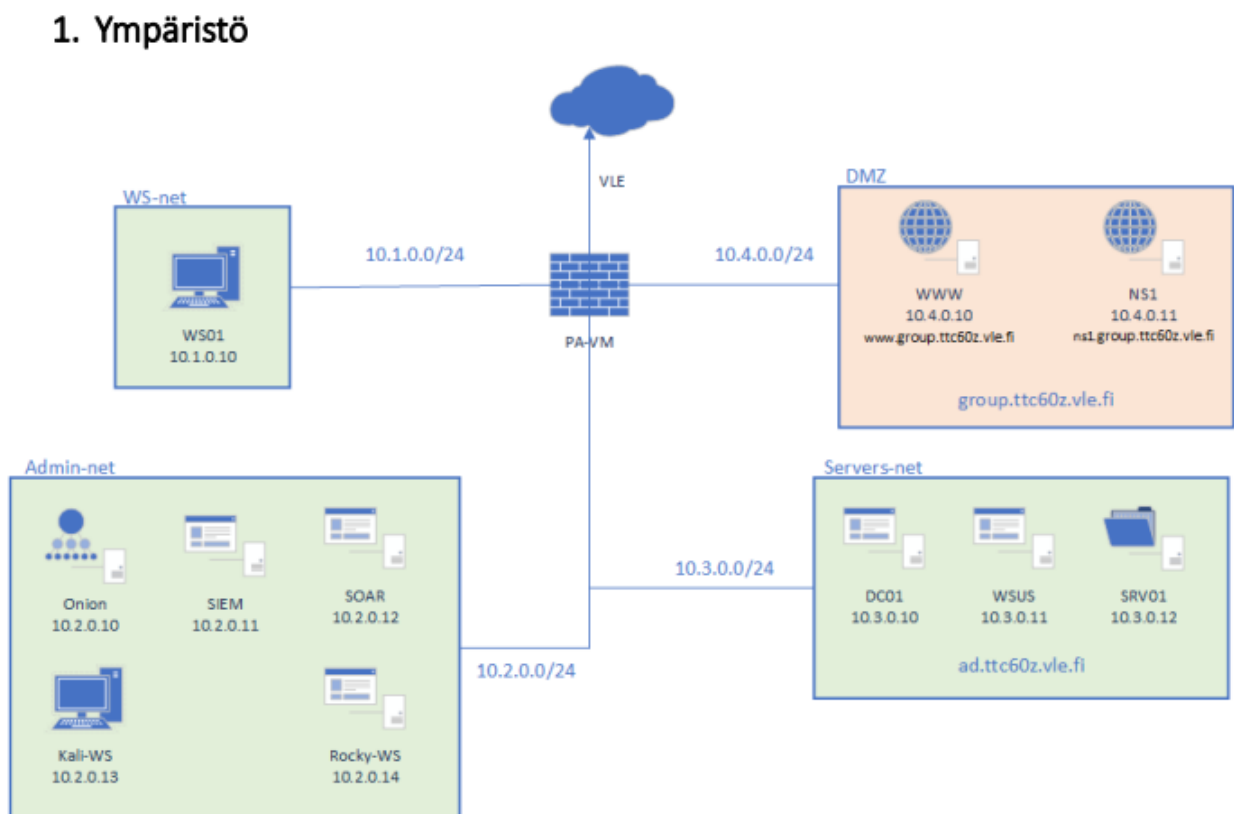
|          |                                  |    |
|----------|----------------------------------|----|
| Kuvio 1. | Laboratorioympäristö .....       | 4  |
| Kuvio 2  | Ip-osoitteen asettaminen.....    | 8  |
| Kuvio 3. | Juuri-sertifikaatin luonti.....  | 9  |
| Kuvio 4. | Kaksi muuta sertifikaattia. .... | 10 |
| Kuvio 5. | Sertifikaatit.....               | 10 |
| Kuvio 6. | SSL/TLS profiili. ....           | 11 |
| Kuvio 7. | Portaalin luonti.....            | 12 |

|  |    |
|--|----|
| Kuvio 8. Autentikointiprofiili .....                     | 12 |
| Kuvio 9. Client Authentication.....                      | 13 |
| Kuvio 10. Autentikointi profiili.....                    | 13 |
| Kuvio 11. Asiakasohjelman luonti.....                    | 14 |
| Kuvio 12.....  | 14 |
| Kuvio 13. Yhdyskäytävän luonti.....                      | 15 |
| Kuvio 14. Yhdyskäytävän SSL/TLS-profiili.....            | 15 |
| Kuvio 15. Client Authentication.....                     | 16 |
| Kuvio 16. Yhdyskäytävän autentikointiprofiili.....       | 16 |
| Kuvio 17. Tunnelirajapinnan valinta .....                | 17 |
| Kuvio 18. Tunnelirajapinnan luonti.....                  | 18 |
| Kuvio 19. Turvallisuusalueen luonti .....                | 18 |
| Kuvio 20. Yhdyskäytävän asetukset .....                  | 19 |
| Kuvio 21. Network Services -asetukset.....               | 19 |
| Kuvio 22. GlobalProtectin version valinta .....          | 20 |
| Kuvio 23. Testikäyttäjän luonti .....                    | 20 |
| Kuvio 24. GlobalProtect portaali.....                    | 21 |
| Kuvio 25. Sertifikaatin lataaminen.....                  | 21 |
| Kuvio 26. GlobalProtectin käyttöönotto .....             | 22 |
| Kuvio 27. GlobalProtect yhdistettynä .....               | 22 |
| Kuvio 28. Turvallisuussäännön luonti .....               | 23 |
| Kuvio 29. Turvallisuus säännön asetukset.....            | 24 |
| Kuvio 30. Windows etäyhteyden avaaminen.....             | 24 |
| Kuvio 31. Etäyhteys on saavutettu! .....                 | 25 |
| Kuvio 32. Turvallisuussäännön luonti SSH:ta varten ..... | 26 |
| Kuvio 33. Turvallisuus säännöt admin-net .....           | 27 |
| Kuvio 34. SSH-yhteyden luominen.....                     | 28 |

# 1 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.)



Kuvio 1. Laboratorioympäristö

## 2 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 palomuuuri ja muut koneet sekä GlobalProtect portaali. Palo Alto- palomuuuri sisältää edistyneitä tietoturvaominaisuuksia sekä se on monipuolinen palomuuuri suojata verkkoympäristöjä. Palo Alto hallinnoi ja valvoo liikennettä meidän ympäristön sisäverkkojen välillä. Yläpuolella kuvassa näkyy konkreettisesti meidän käyttämämme ympäristö.

### 2.1 Palo Alto

Palo Alto on yhdysvaltalainen kyberturvallisuus yritys, joka tarjoaa asiakkailleen edistyksellisiä palomuuureja 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.)

### 2.2 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.)

### 2.2.1 GlobalProtect

GlobalProtect on Palo Alto Networksin sovellus, jonka avulla saadaan etätyöyhteys halutun ympäristön sisäverkkoon riippumatta käyttäjän omasta fyysisestä sijainnista. GlobalProtect on Palo Altoon 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.)

## 3 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 tärkeitä rajata pääsyä yhteyteen luvattomilta tekijöiltä. Esimerkiksi luomalla RDP-pääsyoikeuskäytäntöjä käyttäen palomuuereja pääsyn hallintaan tietyistä IP-osoitteista tai verkostoista. Turvallisuutta voitaisiin parantaa myös vahvoilla salasanoilla tai kahden tekijän todennuksella (2FA).

### 3.1 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 verkonhallinnan 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.

## 4 Mitä tehtiin

Kirjautuimme 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 tehtävänannon 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.

Address

Name

publid

Description

198.19.52.85

Type

IP Netmask

198.19.52.85/32

Resolve

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

OK

Cancel

Kuvio 2 Ip-osoitteen asettaminen.

## 4.1 Sertifikaattien luonti

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



Generate Certificate

Certificate Type
Local
SCEP

Certificate Name
RootCA

Common Name

Signed By

Signed By
Certificate Authority
Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm
RSA

Number of Bits
2048

Digest
sha256

Expiration (days)
365

Certificate Attributes

| TYPE | VALUE |
|------|-------|
|------|-------|

Add
Delete

Generate

Cancel

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.

Generate Certificate

Certificate Type ☒ Local ☐ SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By

☐ Certificate Authority

☐ Block Private Key Export

OCSP Responder

^ Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

Certificate Attributes

| TYPE           | VALUE |
|----------------|-------|
| + Add - Delete |       |

Generate Cancel

Kuvio 4. Kaksi muuta sertifiikaattia.

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

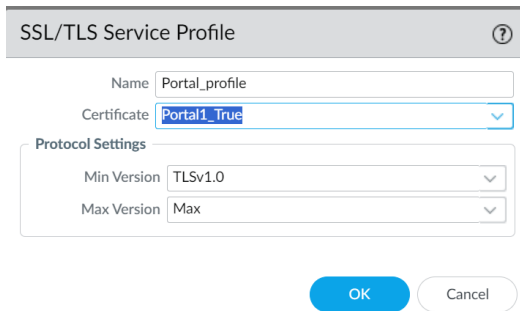
|                          |               |                |              |                                     |                                     |               |       |     |  |
|--------------------------|---------------|----------------|--------------|-------------------------------------|-------------------------------------|---------------|-------|-----|--|
| <input type="checkbox"/> | RootCA        | CN = GPRo...   | CN = GPRo... | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Sep 11 09:... | valid | RSA |  |
| <input type="checkbox"/> | Portal1_True  | CN = ns1.gr... | CN = GPRo... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Sep 11 09:... | valid | RSA |  |
| <input type="checkbox"/> | GP_ClientCert | CN = GP_C...   | CN = GPRo... | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Sep 11 09:... | valid | RSA |  |

Kuvio 5. Sertifiikaatit

Sertifiikaattien tarkoituksena on varmistaa sekä käyttäjän että portaalin/gatewayn luotettavuus ja estää luvottomien käyttäjien pääsy verkkoon. Emme vielä luo sertifiointi profiileja yksinkertais- taaksemme ongelmien etsimistä ja ratkomista.

## 4.2 SSL/TLS palveluprofiili

Seuraavaksi loimme SSL-TLS palveluprofiiliin. 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.).



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=kA10g000000CIf0CAK>)

## 4.3 Portaalin konfigurointi

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

GlobalProtect Portal Configuration

**General**

Name: Portal1

**Network Settings**

Interface: ethernet1/5

IP Address Type: IPv4 Only

IPv4 Address: None

**Appearance**

Portal Login Page: factory-default

Portal Landing Page: factory-default

App Help Page: None

**Log Settings**

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding: None

OK Cancel

Kuvio 7. Portaalin luonti.

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

GlobalProtect Portal Configuration

**Authentication**

SSL/TLS Service Profile: Portal\_profile

**Client Authentication**

|                          | NAME         | OS  | AUTHENTIC...<br>PROFILE | AUTO<br>RETRIEVE<br>PASSCODE | USERNAME<br>LABEL | PASSWORD<br>LABEL | AUTHENTI...<br>MESSAGE     | ALLOW<br>AUTHENTI...<br>WITH USER<br>CREDENTI...<br>OR CLIENT<br>CERTIFICA... |
|--------------------------|--------------|-----|-------------------------|------------------------------|-------------------|-------------------|----------------------------|---|
| <input type="checkbox"/> | portal1_auth | Any | Portal_client           | <input type="checkbox"/>     | Username          | Password          | Enter login<br>credentials | Yes   |

+ Add - Delete Clone ↑ Move Up ↓ Move Down

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).

Kuvio 9. Client Authentication

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

Kuvio 10. Autentikointi profiili

Siirryimme seuraavaksi Agent-välilehdelle ja loimme uuden kuvion 11 mukaisesti. Sertifikaattina käytimme aiemmin luotua GP\_ClientCert:iä.

**Configs**

**Authentication** | Config Selection Criteria | Internal | External | App | HIP Data Collection

Name: Portal1\_agent

Client Certificate: Local | GP\_ClientCert

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: Yes

**Authentication Override**

☒ Generate cookie for authentication override

☒ Accept cookie for authentication override

Cookie Lifetime: Hours | 24

Certificate to Encrypt/Decrypt Cookie: GP\_ClientCert

**Components that Require Dynamic Passwords (Two-Factor Authentication)**

☐ Portal

☐ Internal gateways-all

☐ External gateways-manual only

☐ External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

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.

**External Gateway**

Name: Portal1\_ext\_gateway

Address: ☒ FQDN ☐ IP

ns1.group13.ttc60z.vle.fi

| SOURCE REGION                | PRIORITY |
|------------------------------|----------|
| <input type="checkbox"/> Any | Highest  |

+ Add - Delete

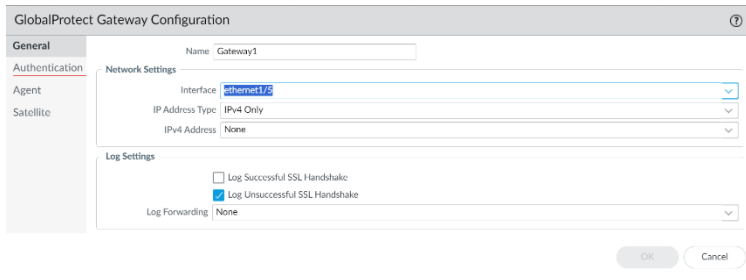
☐ Manual (The user can manually select this gateway)

OK Cancel

Kuvio 12

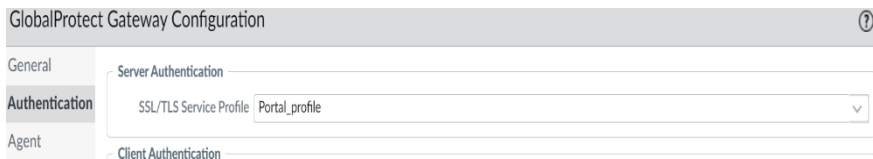
## 4.4 Yhdyskäytävän konfigurointi

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).

The screenshot shows the 'Client Authentication' configuration window. It includes fields for Name (Gateway1\_client), OS (Any), and Authentication Profile (Gateway1\_auth\_profile). There is a checkbox for 'Automatically retrieve passcode from SoftToken application'. Below this is a 'GlobalProtect App Login Screen' section with fields for Username Label (Username), Password Label (Password), and Authentication Message (Enter login credentials). At the bottom, there is a dropdown for 'Allow Authentication with User Credentials OR Client Certificate' set to 'Yes (User Credentials OR Client Certificate Required)'. The window has 'OK' and 'Cancel' buttons at the bottom right.

Kuvio 15. Client Authentication

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

The screenshot shows the 'Authentication Profile' configuration window. It has tabs for 'Authentication', 'Factors', and 'Advanced'. The 'Name' field is set to 'Gateway1\_auth\_profile'. Under the 'Authentication' tab, the 'Type' is set to 'Local Database'. There are fields for 'User Domain' and 'Username Modifier' (set to '%USERINPUT%'). Below this is a 'Single Sign On' section with fields for 'Kerberos Realm' and 'Kerberos Keytab' (with a button to 'Click "Import" to configure this field'). The window has 'OK' and 'Cancel' buttons at the bottom right.

Kuvio 16. Yhdyskäytävän autentikointiprofiili



**Client Authentication** ⓘ

Name:

OS:

Authentication Profile:

☐ Automatically retrieve passcode from SoftToken application

**GlobalProtect App Login Screen**

Username Label:

Password Label:

Authentication Message:

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate:

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

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

**GlobalProtect Gateway Configuration** ⓘ

General | **Tunnel Settings** | Client Settings | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

Authentication

**Agent**

Satellite

☒ **Tunnel Mode**

Tunnel Interface:

Max User:

GlobalProtect IPSec Crypto:

Tunnel Interface

Group Name:

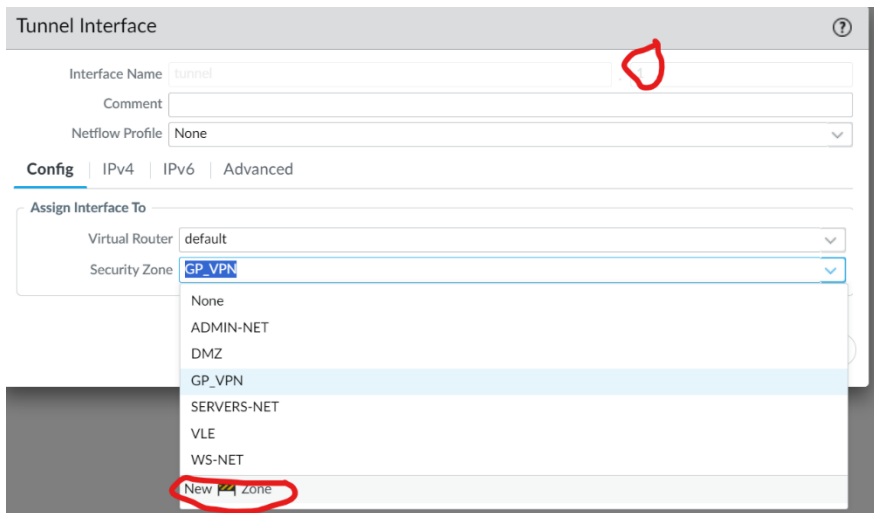
Group Password:

Confirm Group Password:

☒ Skip Auth on IKE Rekey

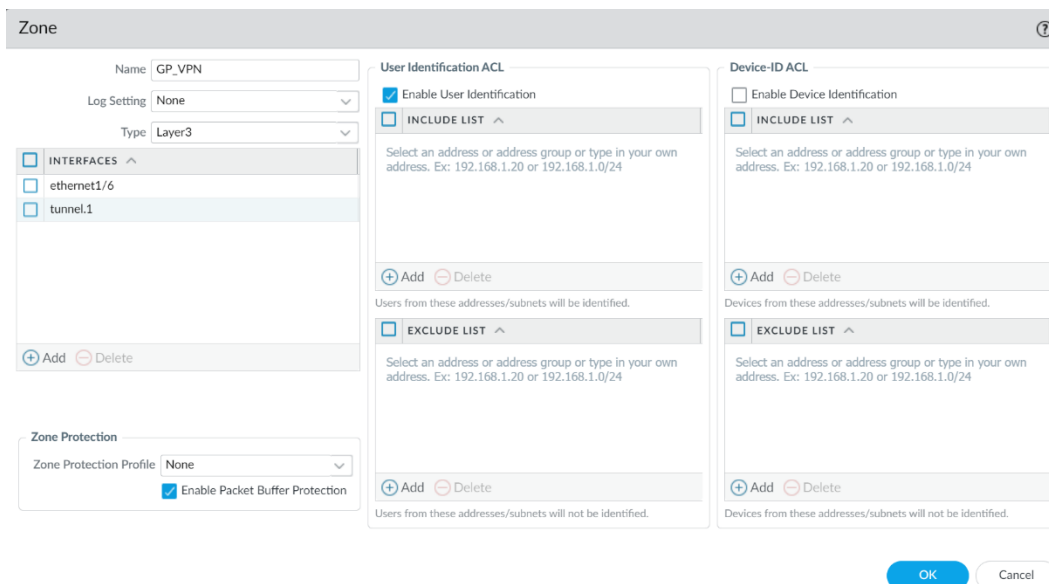
Kuvio 17. Tunnelirajapinnan valinta

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



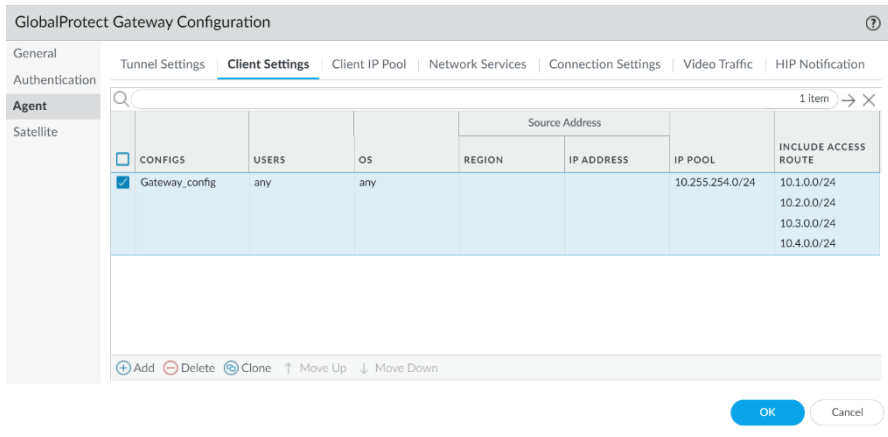
Kuvio 18. Tunnelirajapinnan luonti

Uuden turvallisuusalueen luomiseksi valitsimme 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).



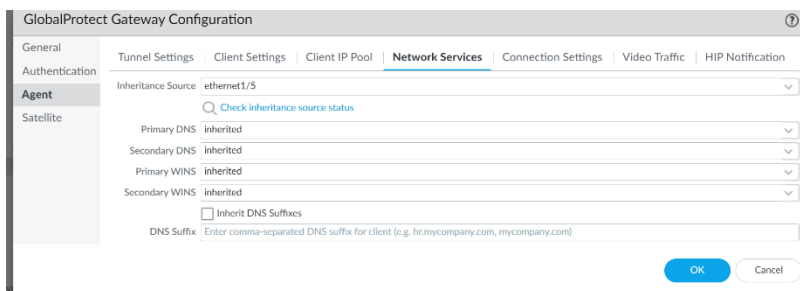
Kuvio 19. Turvallisuusalueen luonti

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

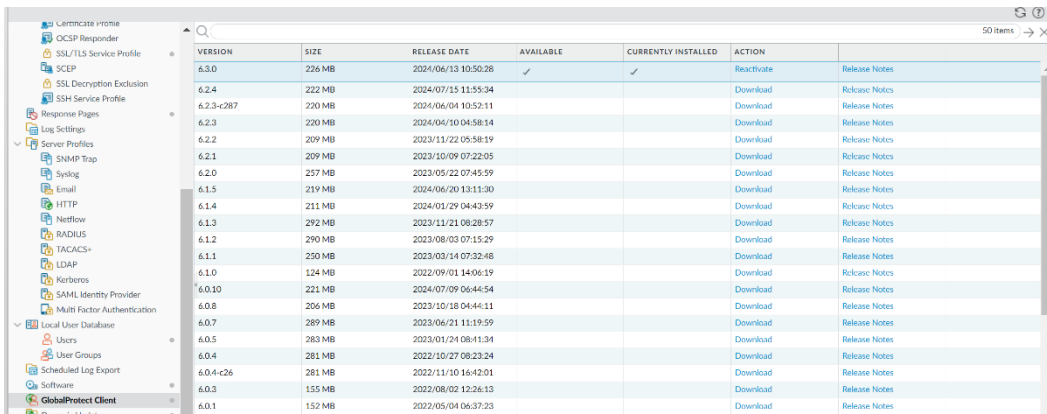
Network services -välilehdelle syötimme kuvion 21 mukaiset asetukset. Rajapinnan lähteeksi valitsimme ethernet1/5 ja kaikkiin muihin kohtiin inherit eli ominaisuudet periytyvät valitulta lähteeltä.



Kuvio 21. Network Services -asetukset

## 4.5 GlobalProtectin käyttöönotto

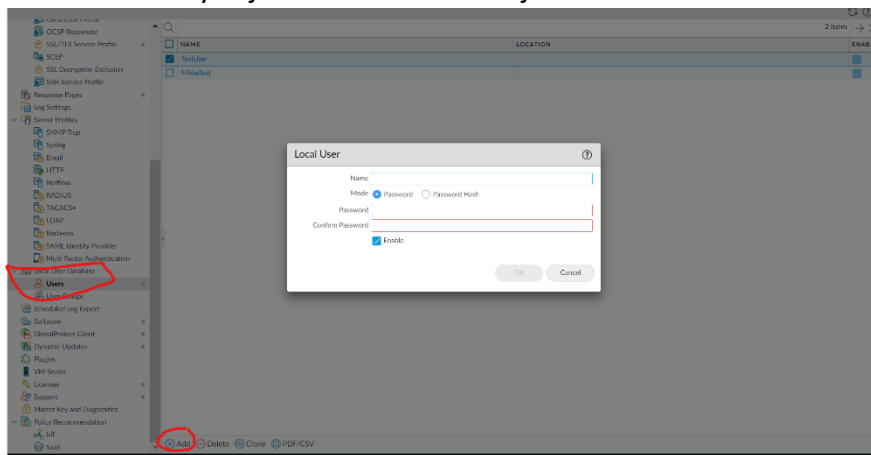
Ennen GlobalProtectin asentamista omalle koneelle menimme palomuurin käyttöliittymässä Device-välilehdelle ja GlobalProtect Client-otsikon alta valitsimme käyttöön Global Protectin uusimman version eli version 6.3.0. (Kuvio 22).



| VERSION    | SIZE   | RELEASE DATE        | AVAILABLE | CURRENTLY INSTALLED | ACTION      |               |
|------------|--------|---------------------|-----------|---------------------|-------------|---------------|
| 6.3.0      | 226 MB | 2024/06/13 10:50:28 | ✓         | ✓                   | Resubscribe | Release Notes |
| 6.2.4      | 222 MB | 2024/07/15 11:55:34 |           |                     | Download    | Release Notes |
| 6.2.3-r287 | 220 MB | 2024/06/04 10:52:11 |           |                     | Download    | Release Notes |
| 6.2.3      | 220 MB | 2024/06/10 04:58:14 |           |                     | Download    | Release Notes |
| 6.2.2      | 209 MB | 2023/11/22 05:58:19 |           |                     | Download    | Release Notes |
| 6.2.1      | 209 MB | 2023/10/09 07:22:05 |           |                     | Download    | Release Notes |
| 6.2.0      | 257 MB | 2023/05/22 07:45:59 |           |                     | Download    | Release Notes |
| 6.1.5      | 219 MB | 2024/06/20 13:11:30 |           |                     | Download    | Release Notes |
| 6.1.4      | 211 MB | 2024/03/29 04:43:59 |           |                     | Download    | Release Notes |
| 6.1.3      | 292 MB | 2023/11/21 08:28:57 |           |                     | Download    | Release Notes |
| 6.1.2      | 290 MB | 2023/08/03 07:15:29 |           |                     | Download    | Release Notes |
| 6.1.1      | 230 MB | 2023/03/14 07:32:48 |           |                     | Download    | Release Notes |
| 6.1.0      | 124 MB | 2022/09/01 14:06:19 |           |                     | Download    | Release Notes |
| 6.0.10     | 221 MB | 2024/07/09 06:44:54 |           |                     | Download    | Release Notes |
| 6.0.8      | 206 MB | 2023/10/18 04:44:11 |           |                     | Download    | Release Notes |
| 6.0.7      | 289 MB | 2023/06/21 11:19:59 |           |                     | Download    | Release Notes |
| 6.0.5      | 283 MB | 2023/01/24 08:41:34 |           |                     | Download    | Release Notes |
| 6.0.4      | 281 MB | 2022/10/27 08:23:24 |           |                     | Download    | Release Notes |
| 6.0.4-r26  | 281 MB | 2022/11/10 16:42:01 |           |                     | Download    | Release Notes |
| 6.0.3      | 155 MB | 2022/08/02 12:26:13 |           |                     | Download    | Release Notes |
| 6.0.1      | 152 MB | 2022/05/04 06:37:23 |           |                     | Download    | Release Notes |

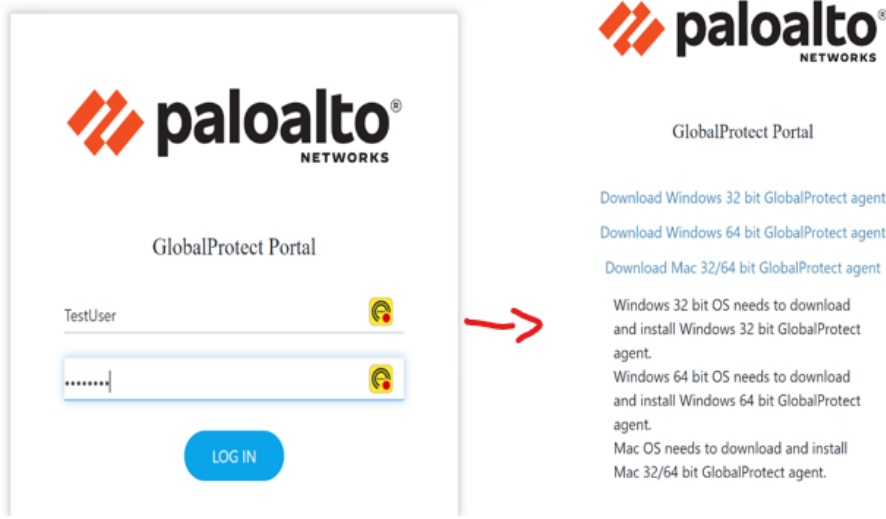
Kuvio 22. GlobalProtectin version valinta

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



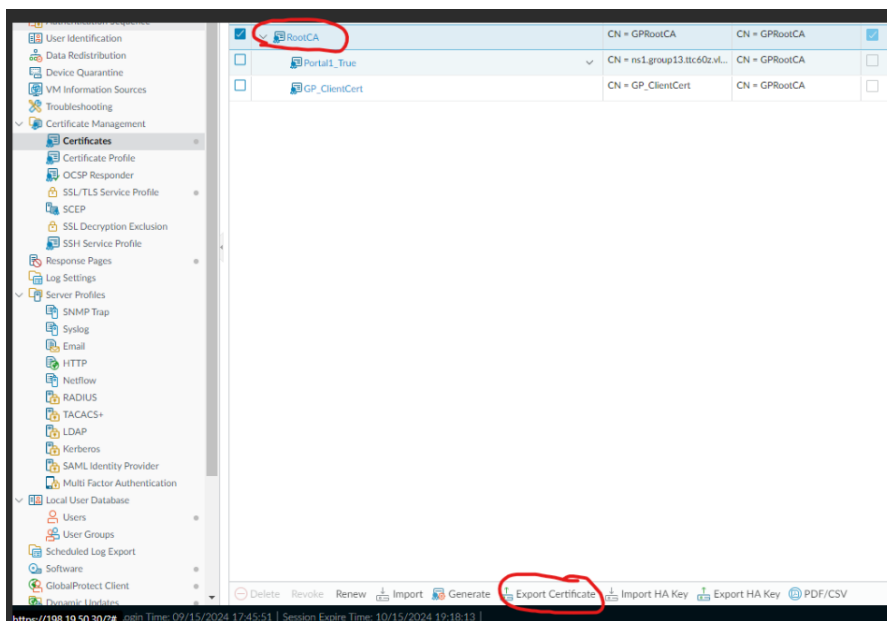
Kuvio 23. Testikäyttäjän luonti

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).



Kuvio 24. GlobalProtect portaali

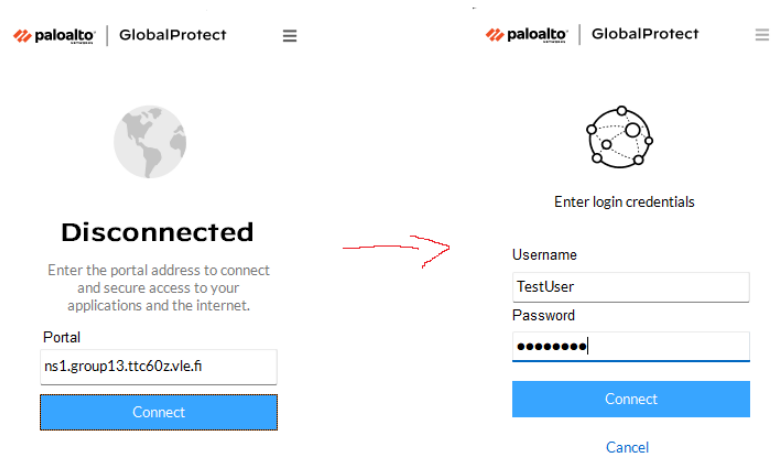
Ennen GlobalProtectin käyttöönottoa asensimme luomamme sertifikaatin RootCA omille tietokoneillemme. Ensimmäisenä lataimme sertifikaatin Palo Altosta (Kuvio 25.)



Kuvio 25. Sertifikaatin lataaminen

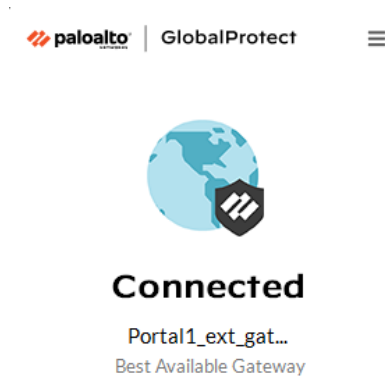
Seuraavaksi avasimme mmc:n Microsoft Management Consolen ja asensimme sertifikaatin tietokoneellemme Arizone State Universityn ohjeen mukaisesti. (Liite 2).

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



Kuvio 26. GlobalProtectin käyttöönotto

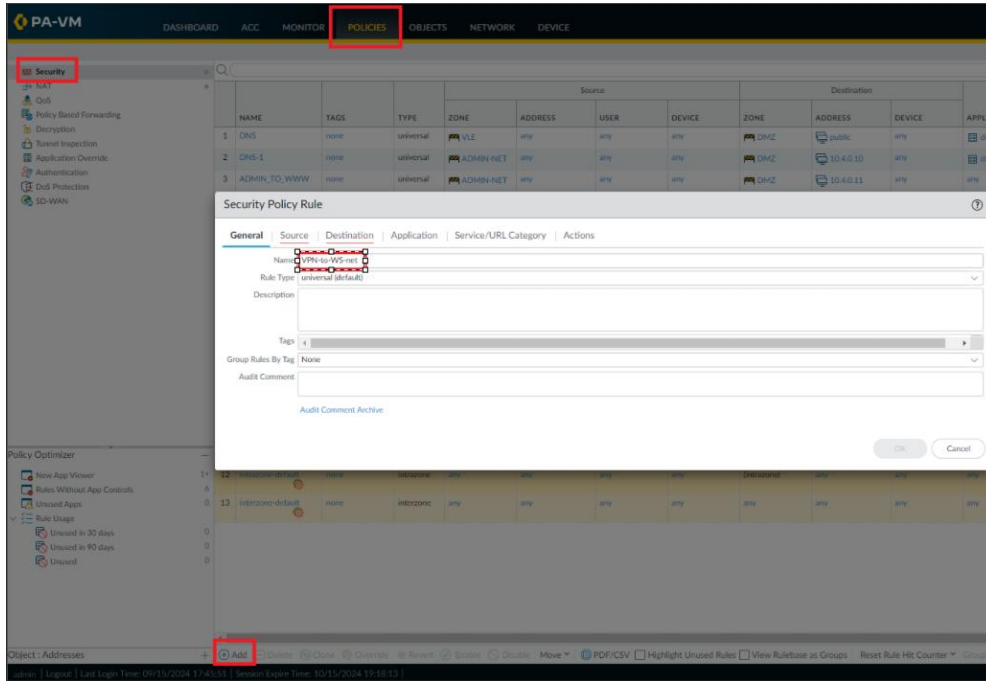
Kirjautumisen jälkeen GlobalProtect oli toiminnassa (Kuvio 27).



Kuvio 27. GlobalProtect yhdistettynä

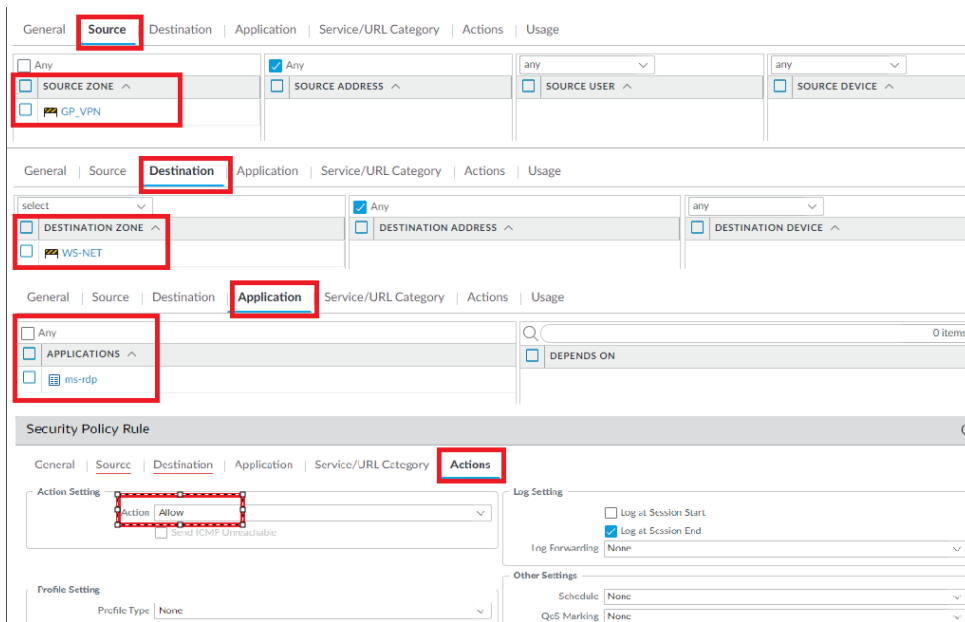
## 4.6 Etäkäyttö Windowsiin

Etäkäytön RDP:n avulla mahdollistamiseksi teimme uuden turvallisuussäännön palomuriin 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.



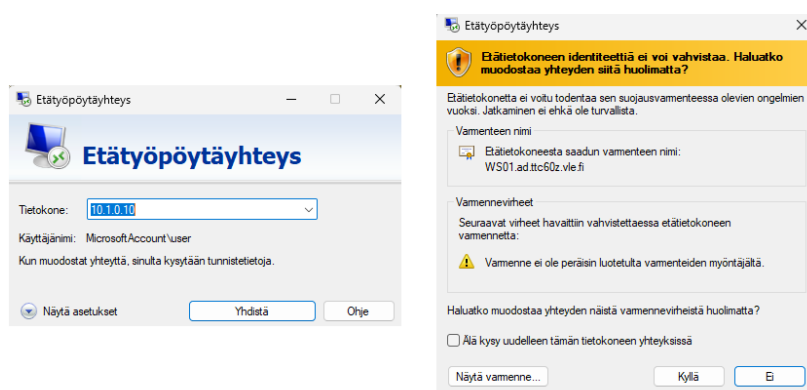
Kuvio 28. Turvallisuussäännön luonti

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



Kuvio 29. Turvallisuus säännön asetukset

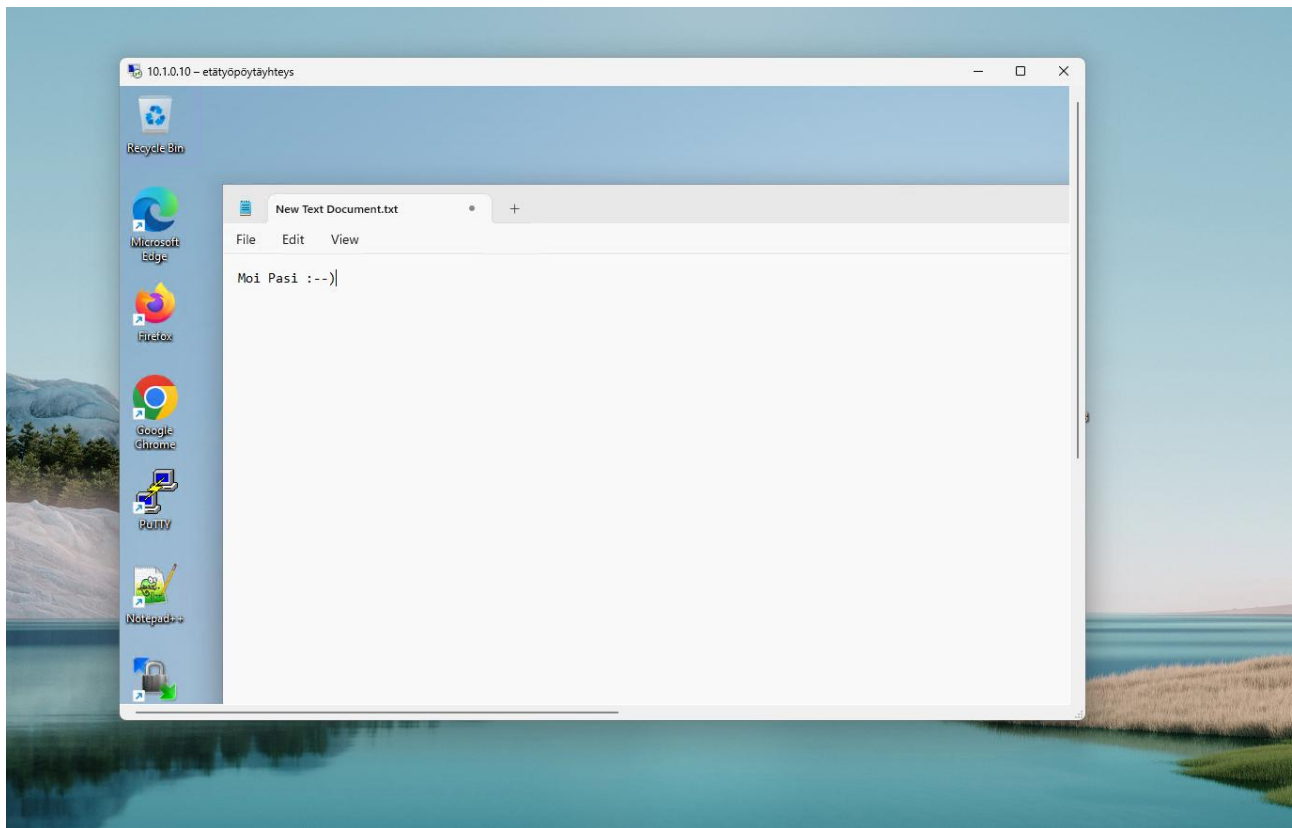
Kun turvallisuussääntö oli valmis varmistimme, että GlobalProtect omalla koneellamme oli päällä, jonka jälkeen avasimme Etätyöpöytäyhteys -sovelluksen, syötimme Windows-työaseman IP-osoitteen 10.1.0.10. (Kuvio 30.) Tunnusta ja salasanaa kysyttäessä annoimme ohjeissa annetun User -käyttäjätunnuksen ja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



Kuvio 30. Windows etäyhteyden avaaminen



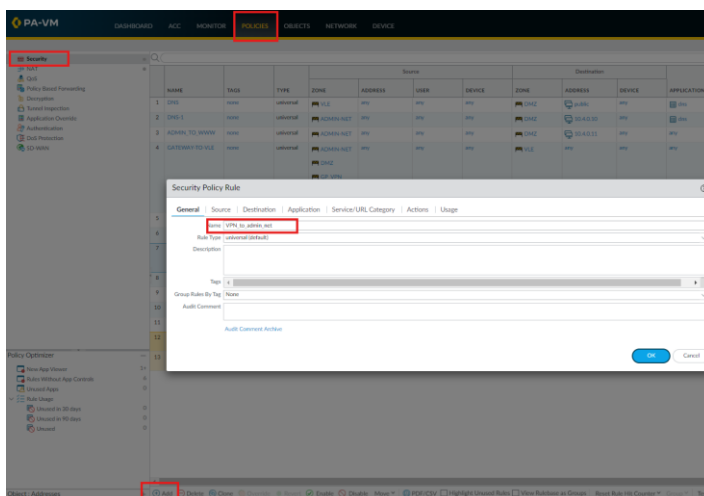
Pienen latailun jälkeen yhteys avautui ja pääsimme käyttämään virtuaalikonetta GlobalProtect VPN:n avulla. (Kuvio 31).



Kuvio 31. Etäyhteys on saavutettu!

## 4.7 Etäkäyttö SSH:lla

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



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).

The figure consists of four screenshots of the 'Security Policy Rule' configuration window, showing the following settings:

- Source Tab:** The 'SOURCE ZONE' is set to 'GP\_VPN'.
- Destination Tab:** The 'DESTINATION ZONE' is set to 'ADMIN-NET'.
- Application Tab:** The 'APPLICATIONS' list includes 'SSH' and 'ping'.
- Action Tab:** The 'Action' is set to 'Allow'. The 'Log Setting' section has 'Log at Session Start' and 'Log at Session End' checked. The 'Other Settings' section has 'Schedule' set to 'None', 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked.

Kuvio 33. Turvallisuus säännöt admin-net

Tämän jälkeen pystyimme omalla tietokoneella ottamaan yhteyden SSH:lla Kali virtuaalikoneeseen GlobalProtectin päällä ollessa syöttämällä Windowsin komentokehoteella 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).

```

kali@kali-ws: ~
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. Kaikki oikeudet pidätetään.

C:\Users\Leevi>ssh kali@10.2.0.13
kali@10.2.0.13's password:
Linux kali-ws 6.0.0-kali6-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.12-1kali1 (2022-12-19) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 13 13:24:40 2024 from 10.255.254.5
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
= https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
kali@kali-ws:~$

```

Kuvio 34. SSH-yhteyden luominen

## 5 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=kA10g000000CIf0CAK>

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](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>