

Tietoturvakontrollit – Labra 1

Juha-Matti Hietala

Topi Liljeqvist

Markus Pollari

Maija Virta

Oppimistehtävä

Tammikuu 2023

Tekniikan ala

Insinööri (AMK), tieto- ja viestintätekniikka

Sisältö

| | | |
|----------|--|-----------|
| 1 | Johdanto | 3 |
| 2 | TEORIA | 3 |
| 2.1 | Palomuri | 3 |
| 2.2 | Tilalliset ja tilattomat palomuurit | 4 |
| 2.3 | SSH, RDP & VPN | 4 |
| 3 | DOKUMENTOINTI | 5 |
| 3.1 | PaloAlto Palomuurin VPN:n konfigurointi ulkoiseen käyttöliittymään. | 5 |
| 3.2 | Ongelmatilanteiden ratkaisu & harjoitustyön viimeistely | 15 |
| 4 | POHDINTA | 19 |
| | Lähteet | 20 |

Kuvat

| | | |
|---------|--|----|
| Kuva 1 | Laboratorio ympäristö | 5 |
| Kuva 2 | Dynamic DHCP Client | 6 |
| Kuva 3 | Palomuurin public IP | 6 |
| Kuva 4 | Rajapinta | 7 |
| Kuva 5 | Generate Certificate | 7 |
| Kuva 6 | SSL/TLS | 8 |
| Kuva 7 | Authentication Profile | 8 |
| Kuva 8 | Client Authentication - Local database | 9 |
| Kuva 9 | External Gateway | 9 |
| Kuva 10 | Gateway Configuration | 10 |
| Kuva 11 | Gateway - Generate Certificate | 10 |
| Kuva 12 | Tunnel1 luontia | 10 |
| Kuva 13 | Security Zone - Tunnel Interface | 11 |
| Kuva 14 | IP Pool | 11 |
| Kuva 15 | IP Pool ja aliverkon koko /24 | 11 |

| | |
|---|----|
| Kuva 16 Inherited - External Gateway..... | 12 |
| Kuva 17 Testikäyttäjän luonti (user1 – root6666)..... | 12 |
| Kuva 18 GlobalProtect Client lataus..... | 13 |
| Kuva 19 Palo Alto -GlobalProtect Client - Asennus 1 | 13 |
| Kuva 20 Valmis asennus | 14 |
| Kuva 21 GlobalProtect Client - Kirjautuminen | 14 |
| Kuva 22 Kirjautumisen ongelma – Error 1..... | 14 |
| Kuva 23 Gateway11 luontia | 15 |
| Kuva 24 Gateway1 poisto..... | 15 |
| Kuva 25 Sertifikaatti ongelma - Error 2 | 16 |
| Kuva 26 Error - Certificate | 16 |
| Kuva 27 GlobalProtect Client – Connected | 17 |
| Kuva 28 Incoming – RDP (Etätyöpöytäyhteys) luonti..... | 17 |
| Kuva 29 Security - Zone asetukset | 17 |
| Kuva 30 Onnistunut etätyöpöytäyhteys (WS01) | 18 |
| Kuva 31 Onnistunut muodostettu SSH-yhteys (Kali-WS) | 18 |

1 Johdanto

Dokumentaatio on osana Tietoturvakontrollit kurssin laboratorioharjoituksia. Ensimmäisen LAB1 harjoituksen tavoitteena on tutustua palomuurin teoriaan sekä harjoitella kurssin VLE-ympäristössä muuriin konfiguraatioita niin, että ryhmän jäsenet saavat muodostettua VPN-yhteyden muurin kautta ympäristön koneisiin. Teorialla ja käytännön harjoituksilla ryhmän jäsenet saavat tarvittavat tiedot sekä taidot toteuttamaan konfiguraatioita palomuriin.

Labra 1. aikana dokumentoidaan kuvankaappauksilla VLE ympäristössä toteutetut toimenpiteet, niiden kuvaus, sekä mahdolliset ongelmatilanteet ja niiden ratkaiseminen. Lisäksi käydään läpi teoria palomuurin, RDP, SSH ja VPN:n toiminnasta. Laboratorion virtuaalikoneen palomuuuri on Palo Alto.

2 TEORIA

2.1 Palomuuuri

Palomuuuri suodattaa verkkoliikennettä esimääriteltujen turvallisuuskäytäntöjen mukaisesti ja suojaa verkkoa ulkopuolisilta hyökkäyksiltä. Oletus-sääntöjen mukaisesti palomuurit estävät kaiken verkkoliikenteen, joten niihin täytyy erikseen luoda säännöt, joiden avulla haluttu liikenne sallitaan ja ei-haluttu liikenne estetään. (Hyppänen 2021, 9.)

Verkkoliikenteen suodatus tapahtuu vertailemalla saapuneiden IP-pakettien sisältöä ennalta määriteltuihin sääntöihin. IP-paketti saa jatkaa matkaansa, jos sen sisältö on sallittu säännöissä. Jos paketin sisältö täsmää kieltolistojen sisältöön, ei paketti pääse liikkumaan määränpäähensä. (Hyppänen 2021, 9.)

Palomuurit sijaitsevat verkon reunalla toimien yhteyskäytävien sisä- ja ulkoverkkojen välillä. Silloin kun palomuuuri on asianmukaisesti konfiguroitu, se kykenee pitämään hakkerit, virukset ja muut ei-toivotut käyttäjät ulkopuolella ja vastavuoroisesti päästämään sallitut käyttäjät läpi. Verkon käytön rajoittamisen lisäksi palomuuuri pitää lo-

kia kaikesta verkkoon tulevasta ja sieltä lähtevästä liikenteestä sekä hallinnoi etäyhteyksiä todennussertifikaattien ja turvallisten kirjautumisien kautta. (Hyppänen 2021, 9.)

2.2 Tilalliset ja tilattomat palomuurit

Yksinkertaisin palomuuuri on pakettisuodatin. Pakettivirrasta seulotaan paketit lähde- ja kohdeosoitteen sekä porttien perusteella. Näitä on kahdentyyppisiä, tilattomia ja tilallisia.

Tilaton palomuuuri määrittelee yhdestä tai useammasta säännöstä koostuvan sarjan eli pääsylistan. Pääsylista määrittää, mitä paketille tehdään, kun ehdot täsmäävät paketin sisällön kanssa eli toisin sanoen pääsylistaan kirjataan säännöt, joita palomuurin halutaan noudattavan. Tilaton pääsylista tyypillisesti asetetaan verkkolaitteen liitännänsä mihin on konfiguroitu jonkin protokollan ominaisuuksia. Palomuuuri vertaa tulevan tai lähtevän paketin otsikkoa pääsylistan sääntöihin rivi riviltä, minkä jälkeen paketti joko päästetään läpi tai hylätään. (Hyppänen 2021, 11.)

Tilallinen palomuuuri taas seuraa verkkoyhteyksien ominaisuuksia ja toimintatilaa. Sen toiminta perustuu ominaisuuteen, jossa palomuuuri tietää yhteyden tilan ja tekee päätöksen paketin hyväksymisestä tai hylkäämisestä. Vain aktiiviset, tunnetut yhteydet voivat läpäistä palomuurin. Toimintaa kutsutaan tilalliseksi paketin tarkastukseksi (SPI) tai dynaamiseksi pakettisuodatuksiksi. Tilallinen palomuuuri sisältää periaatteessa tilattoman palomuurin ominaisuudet, jolloin paketin lähtiessä tai saapuessa sen on ensin läpäistävä pääsylistan säännöt. Jos paketti pääsee tilattoman tarkastuksen läpi, tarvitaan tilallista paketin tarkastusta. Yksinkertaisin tapa havainnoida tilallista paketin tarkastusta on käyttää TCP-yhteyttä. (Hyppänen 2021, 11.)

2.3 SSH, RDP & VPN

SSH (Secure Shell) on verkkoprotokolla, joka mahdollistaa turvallisen etäkäytön tietokoneeseen. Sitä käytetään usein palvelimien etäkäyttöön ja hallintaan, tiedostojen siirtämiseen ja komentojen suorittamiseen useilla laitteilla kerralla. (Encryption Techniques and Systems TTC6540-3001 n.d.)

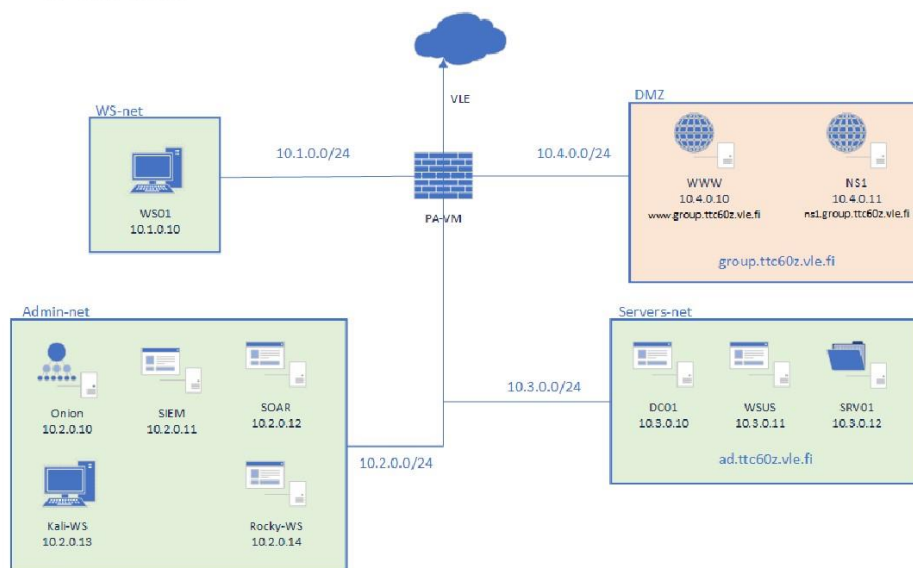
RDP (Remote Desktop Protocol) on Microsoftin kehittämä tietoliikenneprotokolla, joka mahdollistaa etäyhteyden, jonka avulla voidaan hallita etäkonetta ja sen syöttö- ja tulostuslaitteita sekä jakaa tiedostoja ja/tai muita resursseja (Mustonen 2014, 14.).

VPN (Virtual Private Network) tarkoittaa virtuaalista erillisverkkoa, joka luo suojatun yhteyden käyttäjän ja internetin välille. VPN mahdollistaa laitteiden yhdistämisen internetiin VPN-palveluntarjoajan ylläpitämän serverin kautta. VPN:n avulla internetin käyttäjä parantaa yksityisyyttään, koska se salaa internet-yhteydessä olevan laitteen (esim. tietokoneen tai kännykän) verkkoyhteyden. (Mustonen 2014, 6.)

3 DOKUMENTOINTI

3.1 PaloAlto Palomuurin VPN:n konfigurointi ulkoiseen käyttöliittymään.

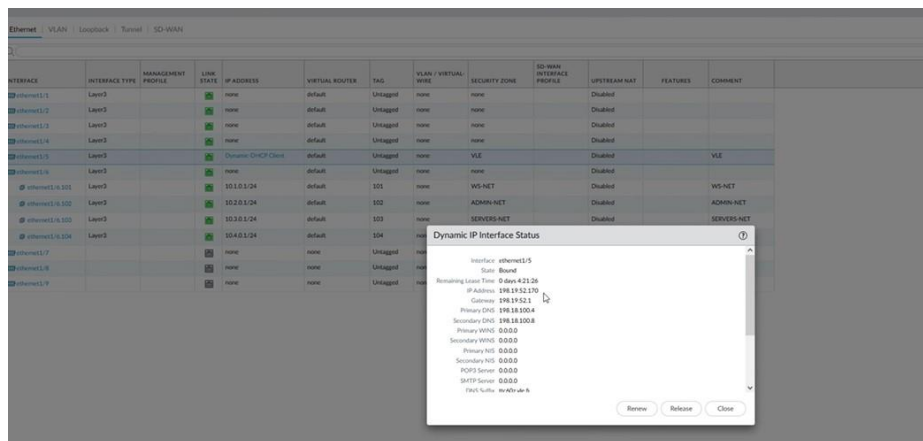
1. Ympäristö



Kuva 1 Laboratorio ympäristö

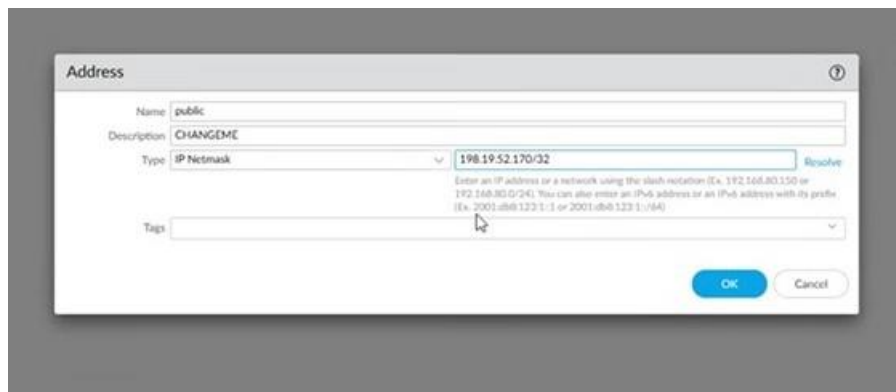
Harjoitustyö LAB 1 aloitettiin aktivoimalla Palo Alto palomuri syöttämällä valtuutus-koodi. Ilman aktivointia jotkin tarvittavat ominaisuudet eivät toimi.

2. vaiheessa määritettiin oikea IP osoite sääntöjen tekemiseen (Network - Ethernet - ethernet1/5 - Dynamic-DHCP Client). Kuvassa 2 esiteltynä.



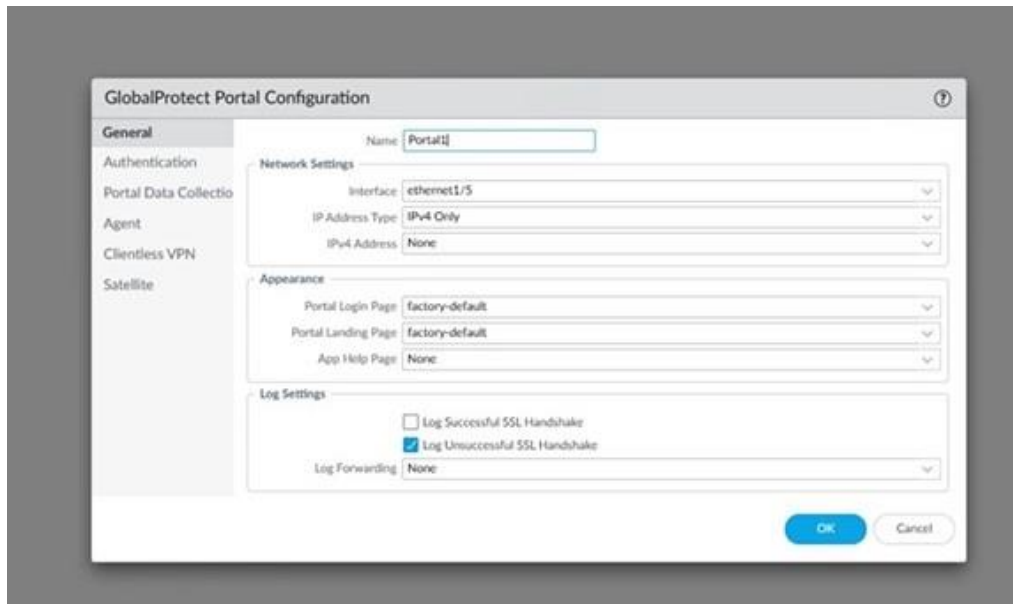
Kuva 2 Dynamic DHCP Client

Seuraavaksi vaihdettiin julkinen IP osoite **198.19.50.170/32** (Objects -> Addresses -> public ja asetettiin oikea IP osoite sekä verkon maski /32). Esitetty kuvassa 3.



Kuva 3 Palomuurin public IP

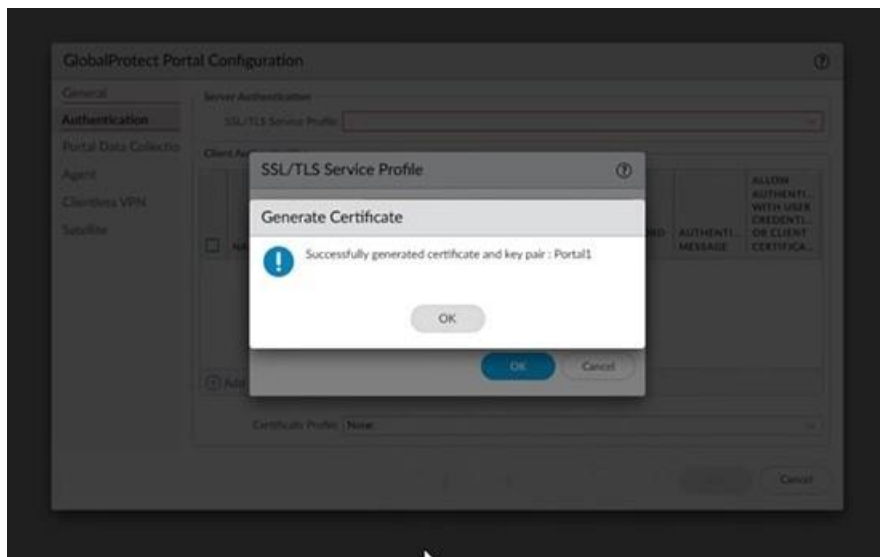
Konfiguraatiot (Network -> GlobalProtect -> Portals -> Add). Nimettiin portaalin rajapinta sekä määriteltiin Interface. Esitetty kuvassa 4.



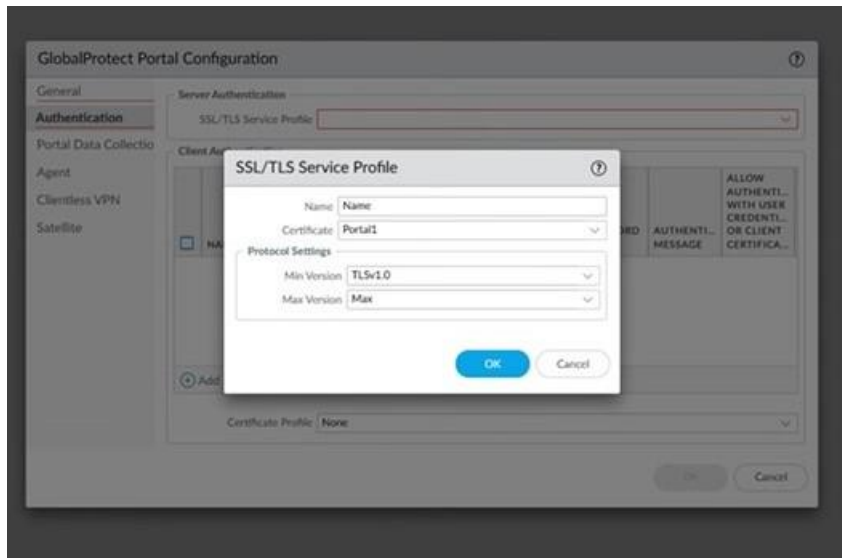
Kuva 4 Rajapinta

Varmennetta/sertifikaattia varten oli annettava portaalin Fully Qualified Domain Name (FQDN) tai IP osoite. Annoimme IP osoitteen sekä valitsimme aktiiviseksi Certificate Authority kohdan.

Valittiin Authentication-välilehden valikosta Uusi SSL/TLS, nimettiin se ja luotiin uusi varmenne/sertifikaatti. Esitettyinä kuvissa 5 & 6.

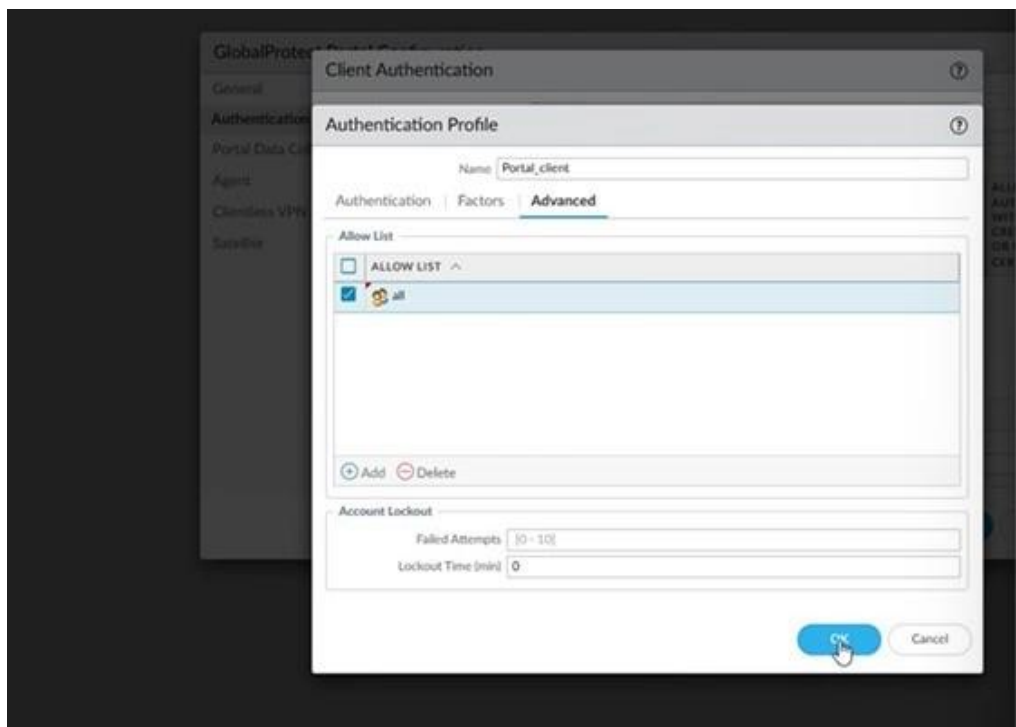


Kuva 5 Generate Certificate

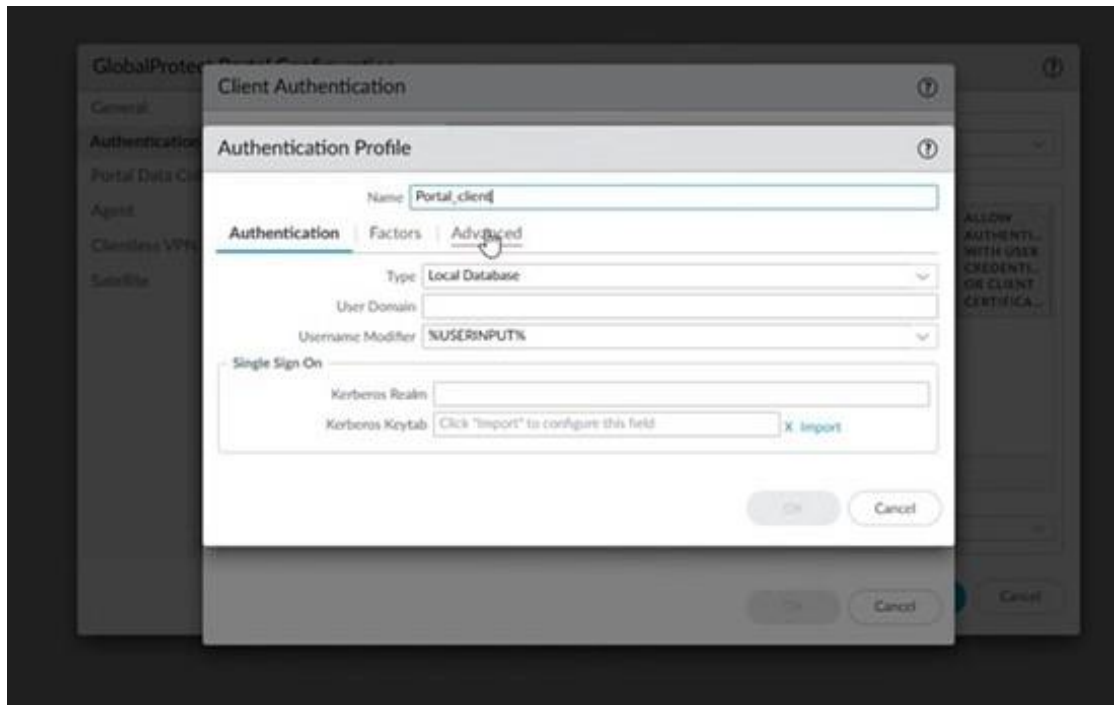


Kuva 6 SSL/TLS

Client Authenticationista valittiin lisää uusi, nimettiin se, jätettiin käyttöjärjestelmän valinta mille tahansa ja valittiin ohjeen mukaan " New Authentication Profile". Asetettiin tyyppi "Local Database". Sitten siirryttiin Lisäasetukset-välilehteen ja lisättiin kaikki sallittujen luetteloon. Esitetty kuvissa 7 ja 8.

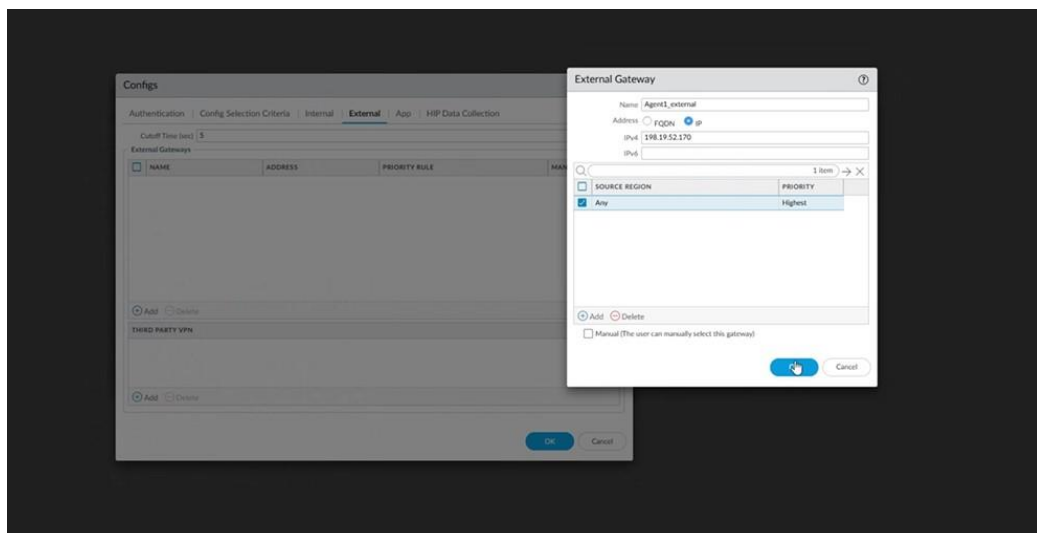


Kuva 7 Authentication Profile



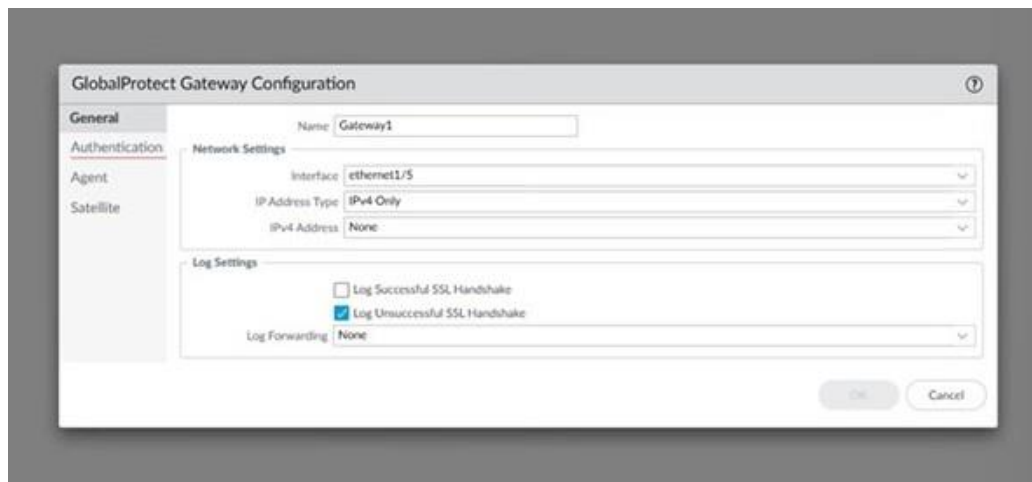
Kuva 8 Client Authentication - Local database

External -välilehdeeltä lisättiin uusi ja nimettiin kohta sekä lisättiin IP osoite. Esitelly kuvassa 9.

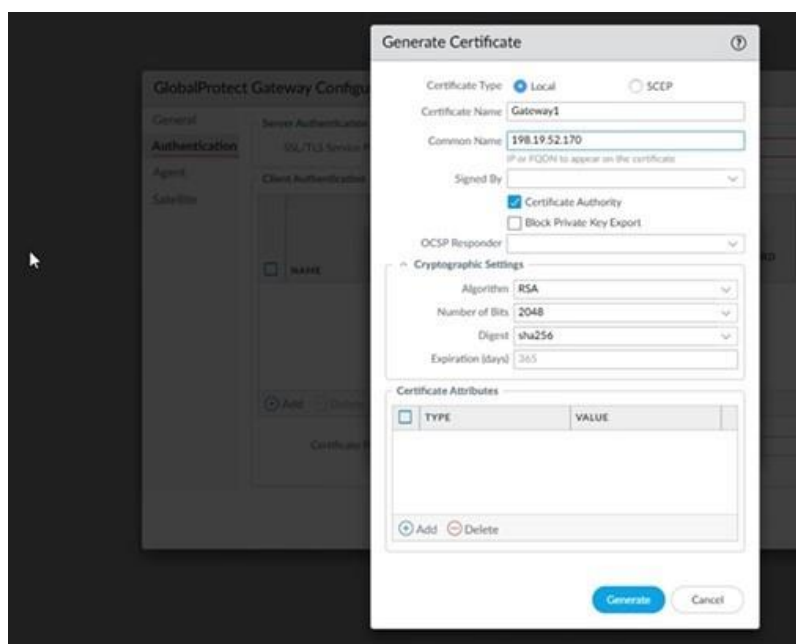


Kuva 9 External Gateway

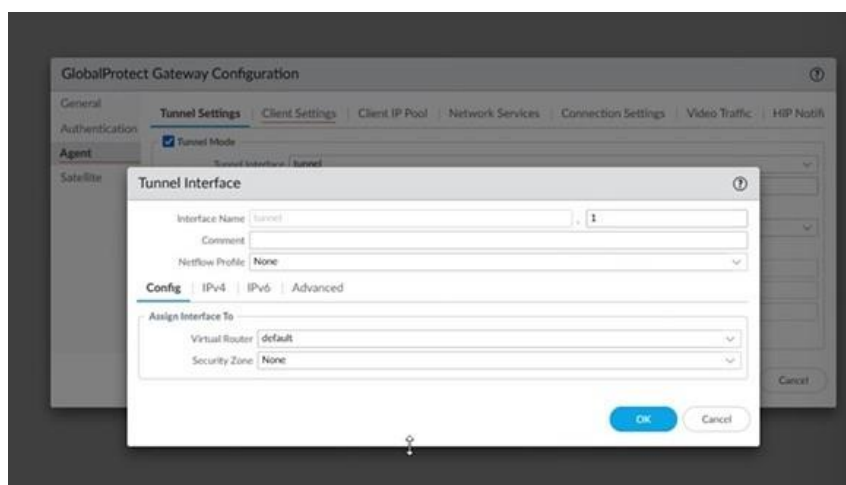
3. Vaihe: Gateway1 konfiguraatio (Network -> GlobalProtect -> Gateways -> Add). Esitetty kuvassa 10.



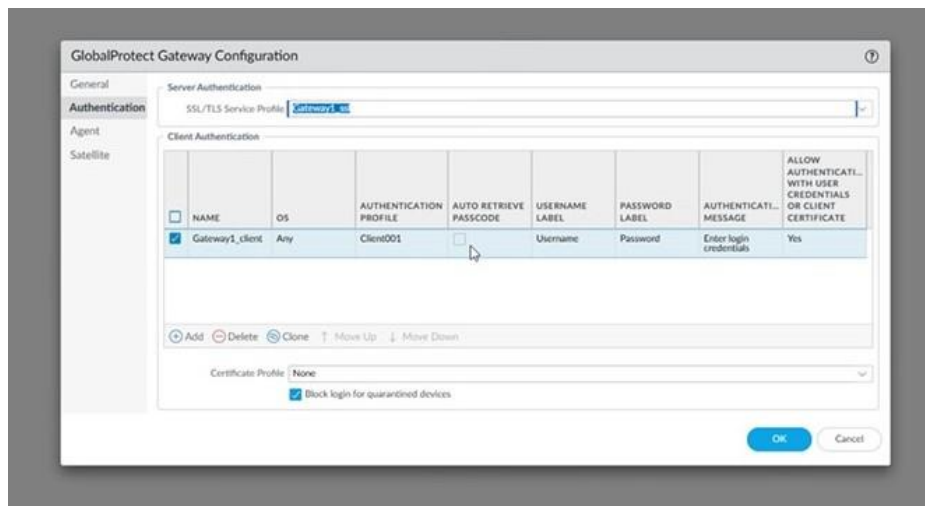
Kuva 10 Gateway Configuration



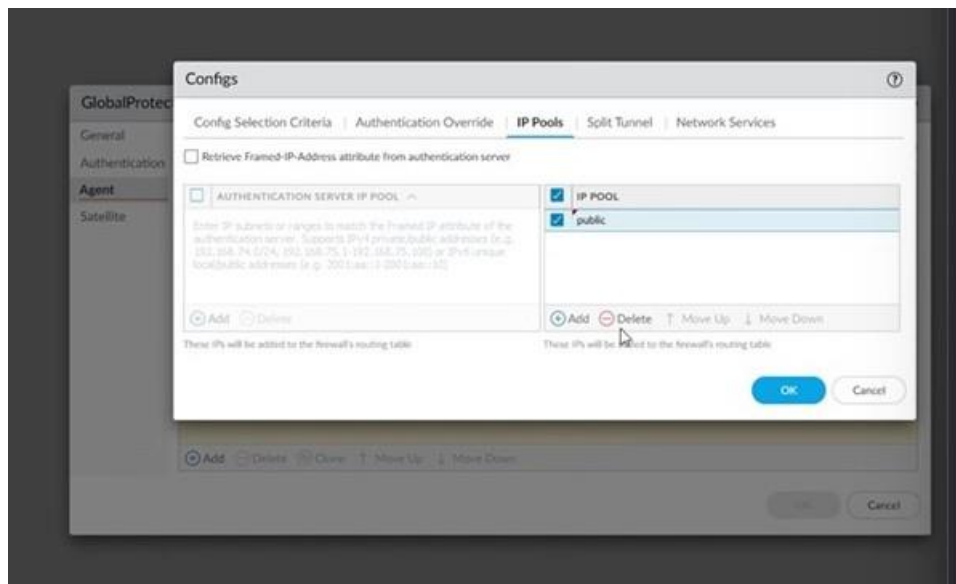
Kuva 11 Gateway - Generate Certificate



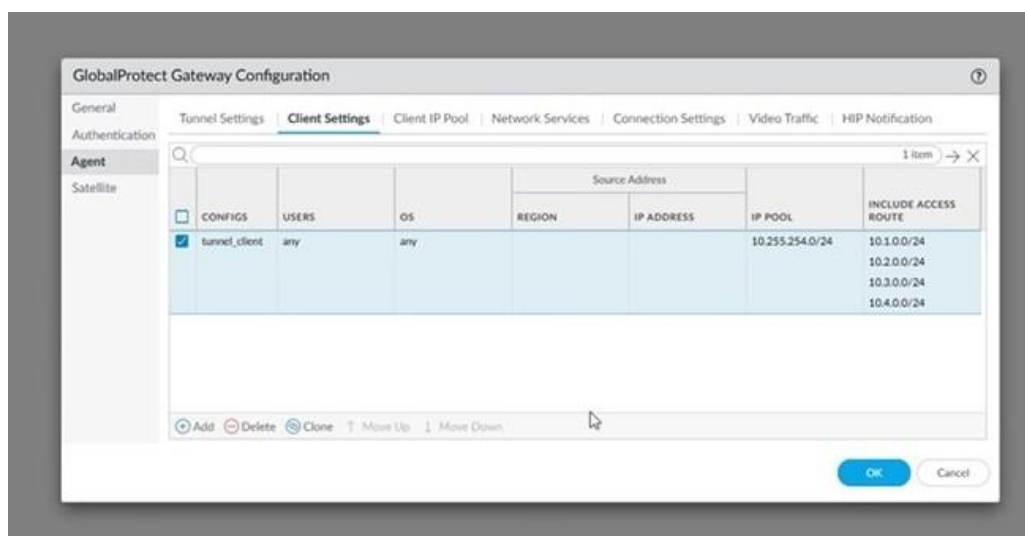
Kuva 12 Tunnel1 luontia



Kuva 13 Security Zone - Tunnel Interface

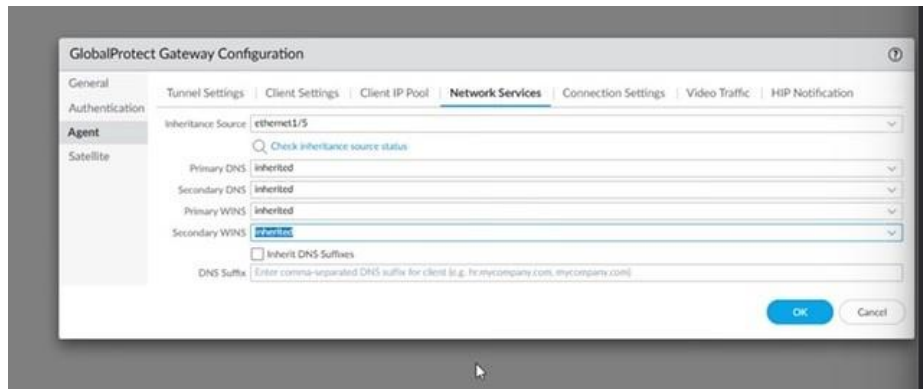


Kuva 14 IP Pool



Kuva 15 IP Pool ja aliverkon koko /24

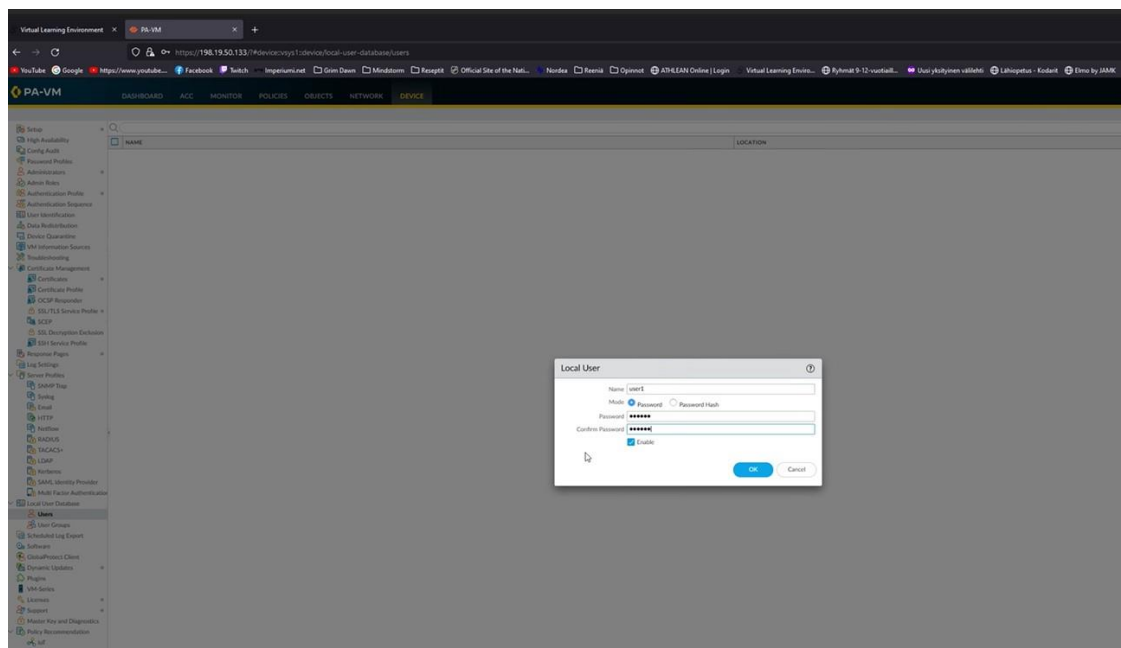
Lopuksi Network välilehdeeltä asetettiin kaikki "Inherited" ulkoisesta yhdyskäytävästä. Esitetty kuvassa 16.



Kuva 16 Inherited - External Gateway

Vaihe 4: Testikäyttäjän luonti

Aloitettiin testikäyttäjän lisäämisellä VPN:lle (Device -> Local User Database -> Users -> Add). Esitetty kuvassa 17.



Kuva 17 Testikäyttäjän luonti (user1 – root6666)

Vaihe 5. GlobalProtect Clientin aktivointi ja lataus

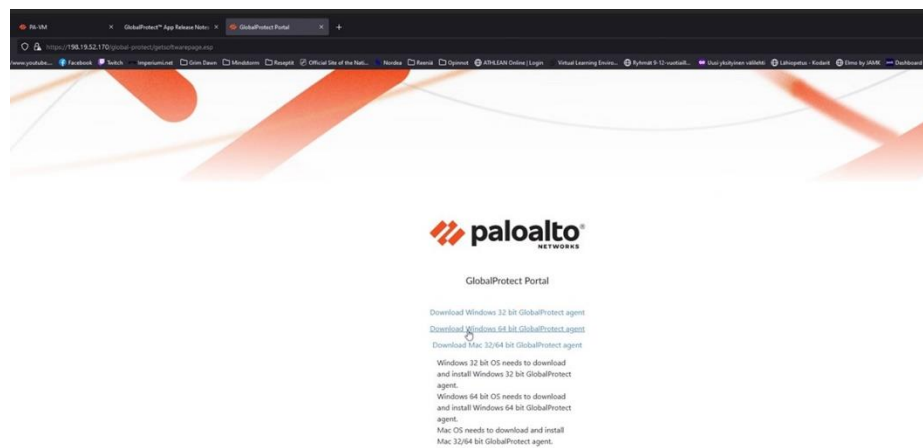
Device - GlobalProtect Client - Check now (sivun alaosasta) - ladattiin sopiva versio-aktivoitiin ladattu versio.

| VERSION | SIZE | RELEASE DATE | AVAILABLE | CURRENTLY INSTALLED |
|-----------|--------|---------------------|-----------|---------------------|
| 6.1.0 | 124 MB | 2022/09/01 14:06:19 | ✓ | |
| 6.0.4-c26 | 281 MB | 2022/11/10 16:42:01 | | |
| 6.0.4 | 281 MB | 2022/10/27 08:23:24 | | |
| 6.0.3 | 155 MB | 2022/08/02 12:26:13 | | |
| 6.0.1 | 152 MB | 2022/05/04 06:37:23 | | |
| 6.0.0 | 152 MB | 2022/02/22 12:11:06 | | |
| 5.2.12 | 103 MB | 2022/05/26 07:38:02 | | |
| 5.2.11 | 99 MB | 2022/03/09 11:49:56 | | |
| 5.2.10 | 99 MB | 2021/12/16 14:20:18 | | |
| 5.2.9 | 99 MB | 2021/11/20 09:57:03 | | |
| 5.2.8 | 96 MB | 2021/08/04 13:10:27 | | |
| 5.2.7 | 94 MB | 2021/06/10 14:41:40 | | |
| 5.2.6 | 89 MB | 2021/04/08 03:44:12 | | |
| 5.2.5-c84 | 70 MB | 2021/03/24 13:53:52 | | |
| 5.2.5 | 66 MB | 2021/01/13 09:07:01 | | |
| 5.2.4 | 65 MB | 2020/11/18 14:46:46 | | |
| 5.2.3 | 65 MB | 2020/10/08 12:24:26 | | |
| 5.2.2 | 64 MB | 2020/08/31 12:36:14 | | |
| 5.2.1 | 64 MB | 2020/08/13 13:08:08 | | |
| 5.2.0 | 64 MB | 2020/07/30 10:05:36 | | |
| 5.1.11 | 61 MB | 2022/05/12 09:23:14 | | |
| 5.1.10 | 61 MB | 2022/02/08 15:45:41 | | |
| 5.1.9 | 61 MB | 2021/11/04 16:33:39 | | |
| 5.1.8 | 61 MB | 2020/12/28 11:08:39 | | |
| 5.1.7 | 61 MB | 2020/10/22 11:37:59 | | |
| 5.1.6 | 60 MB | 2020/08/27 13:09:36 | | |
| 5.1.5 | 59 MB | 2020/07/02 11:26:27 | | |
| 5.1.4 | 59 MB | 2020/06/04 13:41:17 | | |
| 5.1.3 | 58 MB | 2020/04/22 13:17:06 | | |
| 5.1.1 | 57 MB | 2020/02/24 15:02:59 | | |
| 5.1.0 | 57 MB | 2019/12/12 12:55:31 | | |

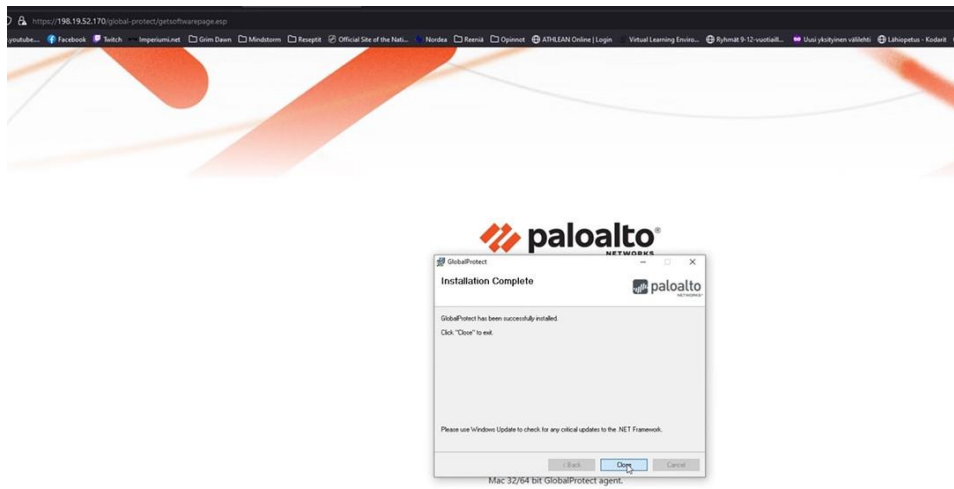
Activate GlobalProtect Client version 6.1.0

Operation: Software Install
 Status: Completed
 Result: Successful
 Details: client package activation successfully completed.
 Warnings:

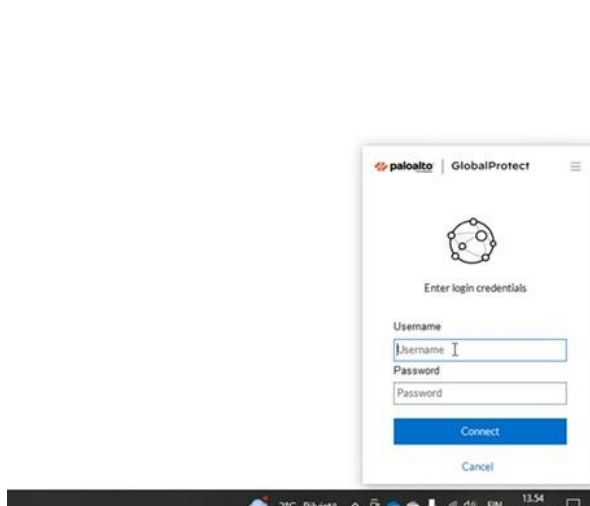
Kuva 18 GlobalProtect Client lataus



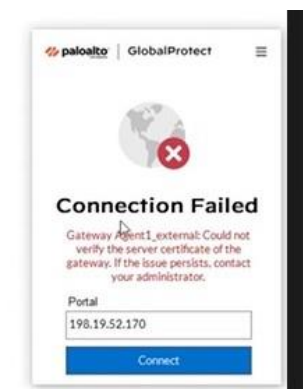
Kuva 19 Palo Alto -GlobalProtect Client - Asennus 1



Kuva 20 Valmis asennus



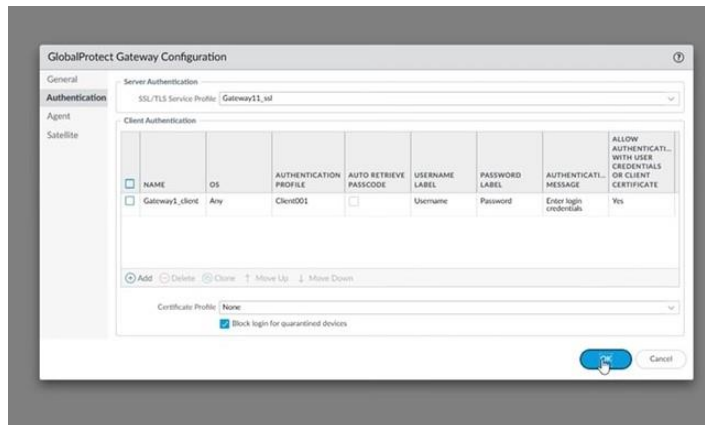
Kuva 21 GlobalProtect Client - Kirjautuminen



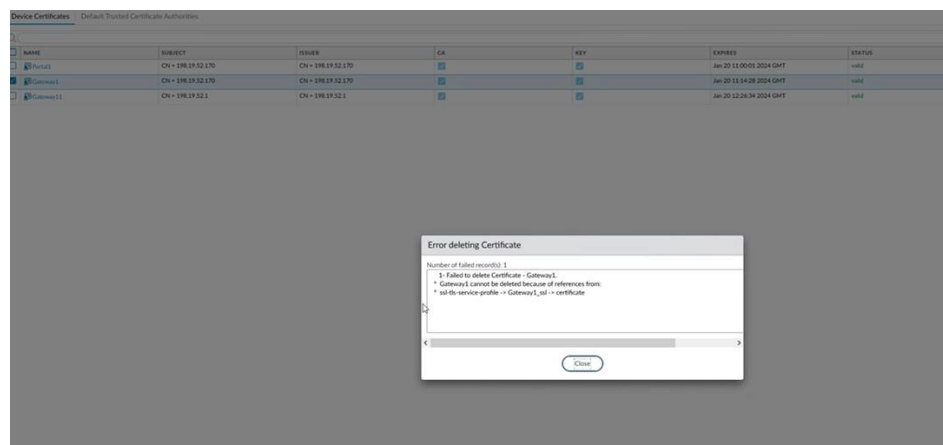
Kuva 22 Kirjautumisen ongelma – Error 1

3.2 Ongelmatilanteiden ratkaisu & harjoitustyön viimeistely

Lähdettiin miettimään missä vaiheessa mahdollisia virheitä tullut. Päätettiin luoda uudestaan Gateway asetukset → Gateway11 muuten samoilla asetuksilla, paitsi osoitteella IP **198.19.50.1** (Gateway1 luotu IP 198.19.50.170). Tämä liike osoittautui vääräksi ja myöhemmin vaihdettiin IP osoite takaisin 198.19.50.170.



Kuva 23 Gateway11 luontia



Kuva 24 Gateway1 poisto



Kuva 25 Sertifikaatti ongelma - Error 2

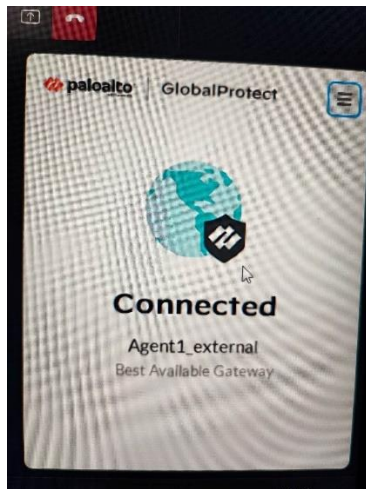
Virhekoodi muuttui ja asennettiin kohdasta "show Certificate" kohdasta sertifikaatti, mutta sama virhekoodi.



Kuva 26 Error - Certificate

Ongelma selvisi seuraavalla luennolla opettajan avustuksella. Sertifikaatin IP osoite oli virheellinen 198.19.52.1 aikaisemmin luodun Gateway11 perusteella.

Tilanne ratkaistu uuden, oikealla IP osoitteen (198.19.52.170) sertifikaatin lataamisella. Onnistunut yhteyden luonti esitetty kuvassa 27.



Kuva 27 GlobalProtect Client – Connected

Seuraavaksi muurille muokattiin/tehtiin uusia sääntöjä, jotka sallivat RDP:n & SSH yhteydet. Lopuksi esitetty miten omalta koneelta saatiin yhteys sisäverkon koneisiin luodun VPN:n avulla. Esitetty kuvissa 28-31.

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

+

Q

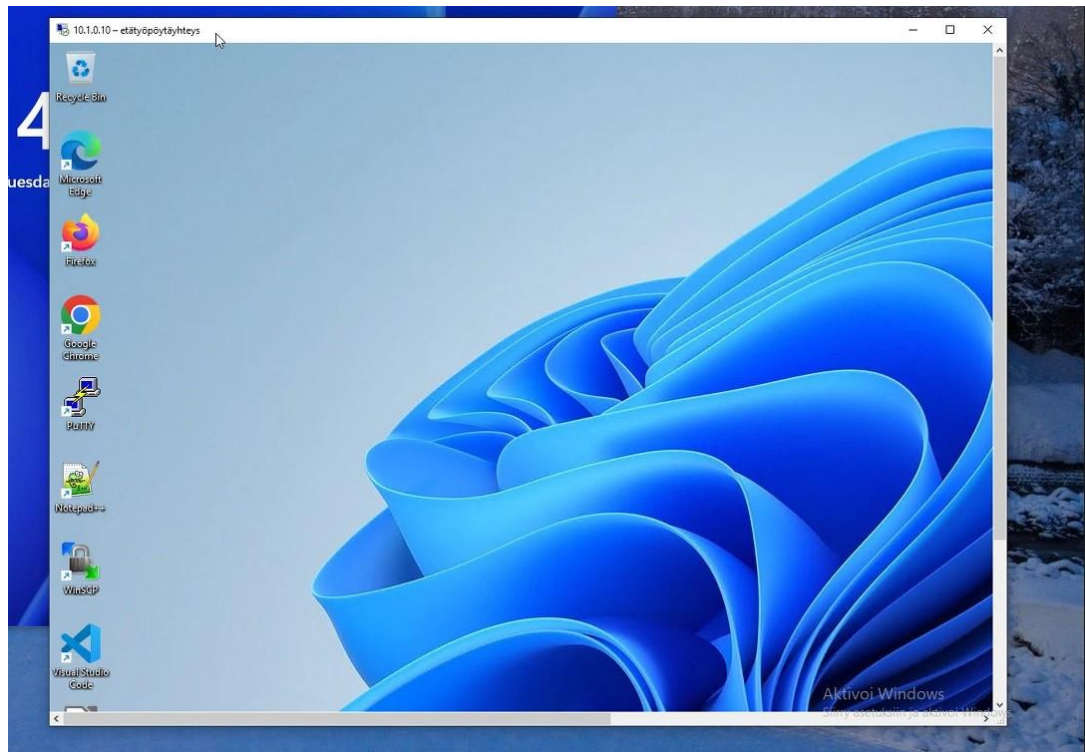
0ms

| | NAME | TAGS | Original Packet | | | | | Translated Packet | | Rule Usage | | | MODIFIED | CREATED | |
|---|---------------|------|-----------------|------------------|-----------------------|----------------|---------------------|-------------------|------------------------------------|--|-----------|---------------------|---------------------|---------------------|---------------------|
| | | | SOURCE_ZONE | DESTINATION_ZONE | DESTINATION_INTERFACE | SOURCE_ADDRESS | DESTINATION_ADDRESS | SERVICE | SOURCE_TRANSLATION | DESTINATION_TRANSLATION | HIT_COUNT | LAST_HIT | | | FIRST_HIT |
| | | | | | | | | | | | | | | | |
| 1 | DNS | none | VLE | VLE | any | any | public | DNS | none | destination-translation address: 10.4.0.10/32 port: 53 | 0 | - | - | 2022-08-10 01:08:34 | 2022-08-10 00:59:56 |
| 2 | DNS-1 | none | VLE | VLE | any | any | public | DNSUDP | none | destination-translation address: 10.4.0.10/32 port: 53 | 4 | 2023-01-20 12:41:54 | 2023-01-20 12:41:54 | 2022-08-10 01:08:34 | 2022-08-10 00:59:56 |
| 3 | ACCESS-TO-VLE | none | ADMIN-NET | VLE | ethernet1/5 | any | any | any | dynamic ip-and-port ethernet1/5 | none | 195880 | 2023-01-24 12:36:32 | 2023-01-17 15:03:46 | 2022-08-10 01:08:34 | 2022-08-10 00:59:56 |
| 4 | Incoming-RDP | none | VPN | VPN | ethernet1/6.101 | any | any | RDP | none | none | 0 | - | - | 2023-01-24 12:36:34 | 2023-01-24 12:36:34 |

Kuva 28 Incoming – RDP (Etätyöpöytäyhteys) luonti

| NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION | PROFILE | OPTIONS | HIT COUNT |
|---------------------|------|-----------|-----------|---------|------|--------|--------------|-----------|--------|-------------|----------------|--------|---------|---------|-----------|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | | | |
| 1 DNS | none | universal | VLE | any | any | any | DMZ | public | any | dns | application... | Allow | none | | 8 |
| 2 DNS-1 | none | universal | ADMIN-NET | any | any | any | DMZ | 10.4.0.10 | any | dns | application... | Allow | none | | 0 |
| 3 ADMIN-TO-SERVERS | none | universal | ADMIN-NET | any | any | any | SERVICES-NET | any | any | any | application... | Allow | none | | - |
| 4 GATEWAY-TO-VLE | none | universal | ADMIN-NET | any | any | any | VLE | any | any | any | any | Allow | none | | 197463 |
| 5 WS-TO-SERVERS | none | universal | WS-NET | any | any | any | SERVICES-NET | any | any | any | any | Allow | none | | 9674 |
| 6 ADMIN-TO-WS | none | universal | ADMIN-NET | any | any | any | WS-NET | any | any | any | any | Allow | none | | 24 |
| 7 Intrazone-default | none | Intrazone | any | any | any | any | Intrazone | any | any | any | any | Allow | none | | 3156 |
| 8 Interzone-default | none | Interzone | any | any | any | any | any | any | any | any | any | Deny | none | | 7070 |

Kuva 29 Security - Zone asetukset



Kuva 30 Onnistunut etätyöpöytäyhteys (WS01)

```
C:\Users\maker>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: Tue Jan 24 13:45:57 2023 from 10.255.254.3
-(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)-[~]
$ pwd
/home/kali
```

Kuva 31 Onnistunut muodostettu SSH-yhteys (Kali-WS)

4 POHDINTA

Harjoitustyön tavoitteena oli harjoitella ryhmätyönä VLE-ympäristöön toteutetun Palo Alto palomuurin hallintaan liittyvät toimenpiteet graafisen käyttöliittymän avulla sekä samalla luoda kokonaisvaltainen ymmärrys palomuurin toiminnasta ja tärkeydestä. Lisäksi harjoitustyössä käytiin läpi teoria VPN, SSH ja RDP yhteyksistä ja niiden luomisesta.

Palo Alto palomuuuri tuntui harjoitustyötä aloittaessa ryhmän opiskelijoiden mielestä moniulotteisuutensa takia monimutkaiselta. Palo Altossa on selkeä käyttöliittymä mutta se tarjoaa niin suuren määrän ominaisuuksia ja toiminnallisuuksia ettei ensikertalaisen silmin voi heti sisäistää kaikkea.

Harjoitustyön aloittaminen oli ohjeistettu hyvin, mutta ryhmätyö aloitettiin erillisenä päivänä kuin oli ollut mahdollisuus ohjaukseen. Ohjaus olisi ollut tarpeellinen ja sen takia harjoituksessa tuli tehtyä ylimääräistä työtä. Teimme Gateway1 konfiguraation kahteen kertaan, vaikka loppuen lopuksi asetuksissa ei ollut vikaa vaan sertifikaatissa. Onneksi päätimme jättää virhetilanteen ratkaisemisen kesken ja odottaa seuraavaan ohjaukseen. Virhetilanteen selvittäminen olin todella yksinkertaista opettajan opastuksella ja sertifikaatin korjaaminen oli nopeaa, kun saimme ymmärryksen ongelmasta. Itsenäisesti olisimme tehneet todennäköisesti saman asian paljon monimutkaisemmalla tavalla.

Kokonaisuutena ensimmäinen harjoitustyö oli opettavainen ajankäytön suhteen tulevaisuuden harjoituksiin sekä se korosti opettajan opastuksen tärkeyttä. Harjoitustyö opetti ryhmän jäsenille palomuurin toimivuudesta ja erityisesti graafisen käyttöliittymän monipuolisuudesta, toiminnasta ja hallinnoinnista.

Lähteet

Encryption Techniques and Systems TTC6540-3001 n.d. Oppimateriaali. Viitattu 26.1.2022. <https://moodle.jamk.fi/course/view.php?id=5311§ion=5#tabs-tree-start>

Hyppänen, V. 2021. Palomuuripalvelu. Opinnäytetyö, AMK. Kaakkois-Suomen Ammattikorkeakoulu, tieto- ja viestintätekniikan tutkinto-ohjelma. Viitattu 21.1.2023. https://www.theseus.fi/bitstream/handle/10024/501442/v%C3%A4in%C3%B6_hypp%C3%A4nen.pdf?sequence=2&isAllowed=y

Mustonen, M. 2014. VPN VIRTUAALIKONEIDEN ETÄKÄYTÖSSÄ. Opinnäytetyö AMK. Oulun Ammattikorkeakoulu Tietojenkäsittely. Viitattu 26.01.2023. https://www.theseus.fi/bitstream/handle/10024/85740/Mustonen_Marko.pdf?sequence=1