



## **Tietoturvakontrollit Labra 1**

### **Ryhmä 3**

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Jukka Virtanen

Harjoitustyö

Tammikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

## Sisältö

<b>1</b>	<b>Johdanto .....</b>	<b>3</b>
<b>2</b>	<b>Teoria.....</b>	<b>3</b>
2.1	Virtual Private Network.....	3
2.2	RDP .....	3
2.3	SSH-protokolla.....	4
2.4	Palomuuuri .....	5
2.5	GlobalProtect .....	6
<b>3</b>	<b>Toteutus .....</b>	<b>6</b>
3.1	VPN-palvelun asennus ja clientin käyttöönotto.....	6
3.2	Palomuurin säännöt .....	17
3.3	Todennukset.....	21
<b>4</b>	<b>Pohdinta.....</b>	<b>25</b>
	<b>Lähteet .....</b>	<b>26</b>

## Kuviot

Kuvio 1.	SSH -protokolla.....	5
Kuvio 2.	Julkinen IP-osoite .....	7
Kuvio 3.	Palomuurin julkisen IP-osoitteen asentaminen .....	7
Kuvio 4.	NSlookup kysely .....	8
Kuvio 5.	Lisenssin asentaminen .....	9
Kuvio 6.	Portaalin asennus - yleinen sivu.....	10
Kuvio 7.	Portaalin asennus - SSL autentikaatio .....	10
Kuvio 8.	Portaalin asennus – gateway .....	11
Kuvio 9.	Portaalin asennus - gateway osoite .....	11
Kuvio 10.	Portaalin asennus valmis.....	12
Kuvio 11.	Gateways asennus - yleinen asetussivu .....	12
Kuvio 12.	Gateways asennus – autentikaatio .....	13
Kuvio 13.	Gateways asennus -tunnelointi.....	13
Kuvio 14.	Gateways asennus - IP-pooli 10.255.254.0/24 .....	14
Kuvio 15.	Gateways asennus – valmis .....	14
Kuvio 16.	Lisätään käyttäjätili .....	15
Kuvio 17.	Client-ohjelma versio 6.2.2 on valmis ladattavaksi.....	15
Kuvio 18.	Näkymä portaalin sivusta .....	16

Kuvio 19. Sertifikaatti piti asettaa luotetuksi ja siirtää se oikeaan paikkaan.....	17
Kuvio 20. Zone-alueen määrittäminen .....	18
Kuvio 21. Tunneloinnin yhdistäminen ZONE:en .....	19
Kuvio 22. SSH valittuna applications välilehdellä.....	19
Kuvio 23. MS-RDP valittuna applications välilehdellä .....	20
Kuvio 24. NAT-säännöt.....	20
Kuvio 25. Policies välilehti.....	21
Kuvio 26. VPN-client yhteys palomuurille todennus .....	21
Kuvio 27. SSH-yhteyden todennus.....	22
Kuvio 28. Etätyöpöytäyhteys 10.1.0.10 osoitteeseen .....	22
Kuvio 29. RDP-yhteys WS01-koneelle.....	23
Kuvio 30. RDP-yhteys DC01-palvelimelle.....	24
Kuvio 31. Kuva verkonvalvonta sivulta .....	25

# 1 Johdanto

Tietoturvakontrollien 1. labran tarkoituksena on tutustuttaa ryhmä ympäristön PaloAlto- palomuu- riin ja sen jälkeen konfiguroida se niin, että jokainen ryhmäläinen saa otettua SSH tai RDP- yhteyden kotikoneeltaan ympäristön koneeseen. Tämä raportti sisältää lyhyen teoriaosuuden tärkeimmistä termeistä sekä kuvauksen toteutuksesta ryhmän kolme osalta.

## 2 Teoria

### 2.1 Virtual Private Network

Virtual Private Network (VPN) eli virtuaalinen erillisverkko. VPN:n avulla käyttäjällä on mahdollisuus luoda suojattu verkkoyhteys julkista verkkoa käytettäessä. VPNn salaa käyttäjän tietoliikenteen ja kykenee häivyttämään hänen online identiteettinsä. (What is VPN? How It Works, Types of VPN 2024)

VPN salaa käyttäjän IP-osoitteen kierrättämällä liikenteen VPN hostin tarjoaman etäpalvelimen kautta. Yhteytesi kulkiessa etäpalvelimen kautta verkkopalvelut näkevät liikenteesi tulevan VPN-palvelimen IP-osoitteesta, ei omasta IP-osoitteesta. Tämän takia kolmannet osapuolet sekä internet palveluntarjoajat (ISP) eivät esimerkiksi näe mitä tietoa lähetät tai vastaanotat verkon yli tai millä nettisivuilla vieraillet. VPN-yhteyden käyttöaiheita ovat mm. oman yksityisyytesi piilottaminen verkossa, verkkoliikenteesi suojaaminen julkisissa Wi-Fi verkoissa tai internetin maarajoitusten ohittaminen virtuaalista sijaintia vaihtamalla. (Mikä on VPN? 2024)

### 2.2 RDP

RDP (Remote Desktop Protocol) perustuu T-120-protokollastandardin laajennukseen ja mahdollistaa useiden virtuaalisten kanavien käytön tiedonsiirtoon. RDP on T.Share-ydinprotokollan laajennus ja tarjoaa luotettavan point-to-point tiedonsiirron. Se tukee myös monipistetiedonsiirtoa, joka mahdollistaa sovelluksen tiedonsiirron useille osapuolille reaaliajassa. (Understanding the Remote Desktop Protocol (RDP), 2023)

Microsoft otti RDP:n käyttöön Windows NT Terminal Serverin yhteystarkoituksiin, koska se tarjoaa laajennettavan perustan muiden ominaisuuksien rakentamiselle. RDP tukee erilaisia verkkotopologioita ja lähiverkkoprotokollia, kuten ISDN, POTS, IPX, NetBIOS ja TCP/IP. Protokollapinon käsittely RDP:n avulla on abstrahoitu, mikä helpottaa puhtaiden ja hyvin suunniteltujen sovellusten kehittämistä. (Understanding the Remote Desktop Protocol (RDP), 2023)

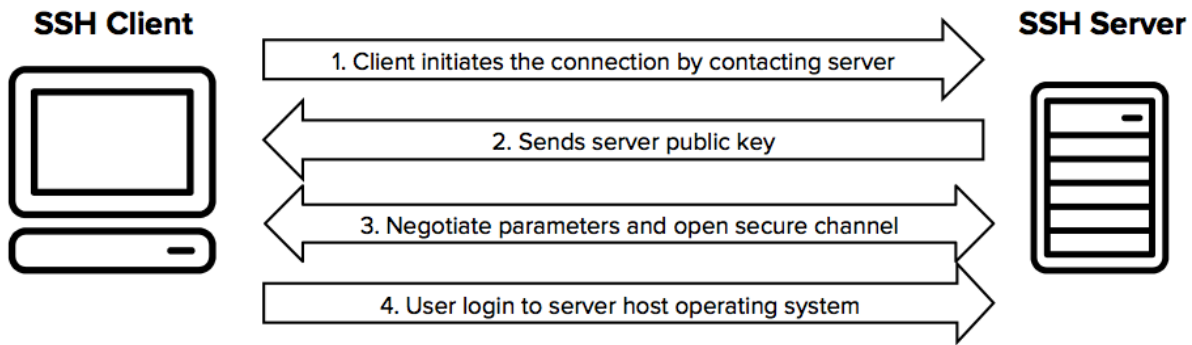
RDP-pinon neljä keskeistä komponenttia ovat Multipoint Communication Service (MCSMUX), Generic Conference Control (GCC), Wdtshare.sys ja Tdtcp.sys. MCSMUX toteuttaa monipistepalvelut ja tiedonsiirtoprotokollan. GCC vastaa useiden kanavien hallinnasta ja mahdollistaa istuntoyhteyksien luomisen ja poistamisen. Wdtshare.sys on RDP-ajuri käyttöliittymän siirtoa, pakkausta, salausta ja kehystämistä varten. Tdtcp.sys on kuljetusajuri, joka pakatoi protokollan verkkoprotokollaan (TCP/IP). (Understanding the Remote Desktop Protocol (RDP), 2023)

RDP on suunniteltu riippumattomaksi taustalla olevasta siirtopinosta, kuten TCP/IP:stä. Tämä mahdollistaa muiden kuljetusajureiden lisäämisen tarpeen mukaan ilman suuria muutoksia protokollan perusosiin. RDP:n suorituskyky ja laajennettavuus verkossa riippuvat näistä keskeisistä tekijöistä. (Understanding the Remote Desktop Protocol (RDP), 2023)

Yhteenvetona voidaan todeta, että RDP on T-120-protokollan laajennus, joka mahdollistaa luotettavan tiedonsiirron useiden virtuaalisten kanavien avulla. Se tukee monipistetiedonsiirtoa ja on suunniteltu riippumattomaksi taustalla olevasta siirtopinosta. RDP-pinolla on neljä komponenttia, jotka vastaavat kanavien hallinnasta, kuljetuksesta ja protokollapinon käsittelystä. RDP:n joustavuus ja laajennettavuus tekevät siitä tehokkaan työkalun verkkotiedonsiirtoon. (Understanding the Remote Desktop Protocol (RDP), 2023)

## **2.3 SSH-protokolla**

SSH-protokolla käyttää salausta asiakkaan ja palvelimen välisen yhteyden suojaamiseen (ks. kuvio 1). Kaikki käyttäjän todennus, komennot, tulosteet ja tiedostojen siirrot salataan verkossa tapahtuvien hyökkäysten estämiseksi. (Tatu Ylönen. What is SSH (Secure Shell)?)



Kuvio 1. SSH -protokolla

Erilaisia SSH –ohjelmistoja ovat mm. Putty (Windows), WinSCP (Windows), FileZilla (Windows), CyberDuck (Mac), Open SSH (Linux). (SSH software downloads)

## 2.4 Palomuuuri

Tietokoneverkon palomuuuri tarjoaa suojaa verkon rajalla valvomalla verkkoliikenteessä saapuvia ja lähteviä datapaketteja haittaohjelmien ja poikkeavuuksien varalta. Palomuuuri suodattaa liikennettä, kun se yrittää tulla verkkoon ja poistua verkosta, toisin kuin virustorjuntaohjelmisto, joka skannaa verkon laitteita ja tallennusjärjestelmiä suojauksen läpi tunkeutuneiden uhkien varalta. (Definition: What Is a Firewall?)

Palomuuuri on suunniteltu noudattamaan ennalta määritettyjä turvallisuussääntöjä, joiden avulla määritetään, mitä verkkoon sallitaan ja mitä estetään. (Definition: What Is a Firewall?)

Palomuuuri voidaan toimittaa laitteistolaitteena, ohjelmistona tai SaaS-palveluna (Software as a Service) riippuen siitä, missä se otetaan käyttöön ja mihin tarkoitukseen se on tarkoitettu. Palomuuureja on viisi päätyyppiä niiden toimintatavan mukaan:

- Tilaton eli pakettisuodatusta käyttävä palomuuuri (stateless or packet filtering firewall)
- Tilatarkkailupalomuuuri (stateful inspection firewall)
- Piiritason yhdyskäytävä (circuit-level gateway)
- Sovellustason yhdyskäytävä (application-level gateway)
- Seuraavan sukupolven palomuuuri (NGFW) (next-generation firewall (NGFW))

(Definition: What Is a Firewall?)

Periaatteessa palomuuureissa on kahdenlaisia toimitusmenetelmiä: ohjelmistoja ja laitteistoja. Yleensä ohjelmistopalomuuuri suojaa isäntäkoneen, kuten tietokoneen tai laitteen, ja laitteistopalomuuuri suojaa verkkoa. (What Is A Software Firewall vs A Hardware Firewall?)

Lisäeron voidaan todeta, että tietokoneverkon laitteistopalomuuuri käyttää ohjelmistoa, joka on asennettu laitteistolaitteeseen, kun taas tietokoneverkon ohjelmistopalomuuuri käyttää tietokonetta laitteistolaitteena, jossa se toimii. Tästä syystä ohjelmistopalomuuureista käytetään usein nimitystä "isäntäpalomuuuri" ja laitteistopalomuuureista nimitystä "verkkopalomuuuri". (What Is A Software Firewall vs A Hardware Firewall?)

## 2.5 GlobalProtect

Global Protect -konseptilla pyritään tarjoamaan tietoturvallinen tapa päästä organisaation verkkoihin ulkoa käsin. Global Protect koostuu komponenteista, joita ovat Portal, Gateway ja App. Portalin kautta jaetaan sovellukset ja konfiguraatiot, Gateway määrittelee muodostettavan yhteyden kohteen ja sen rajaukset ja App on client-sovellus, jonka avulla yhteys muodostetaan. Portaaleja ja Gatewayta voidaan luoda tarvittava määrä eri tarpeisiin ja käyttäjäprofiileihin. (GlobalProtect Overview 2023)

## 3 Toteutus

### 3.1 VPN-palvelun asennus ja clientin käyttöönotto

Labran ensimmäisessä osiossa asensimme palomuurille VPN-palvelun. Palvelun käyttöönotossa piti asentaa palomuurille julkinen IP-osoite, lisenssi, portaalin SSL-yhteyden sertifikaatti sekä VPN-verkon oletusyhdykskäytävän sertifikaatti sekä siihen liittyvät muut asetukset. Lisäksi piti luoda käyttäjä sekä aktivoida VPN-ohjelman asennusversio. Lopuksi piti asentaa omalle työasemalle VPN-client ja määritellä siihen liittyvät asetukset.

Ensimmäiseksi asensimme julkisen IP-osoitteen. IP-osoite piti hakea DHCP-asetuksista (ks. kuvio 2), joka oli 198.19.52.47.

Dynamic IP Interface Status

Interface ethernet1/5

State Bound

Remaining Lease Time 0 days 7:31:07

IP Address 198.19.52.47

Gateway 198.19.52.1

Primary DNS 198.18.100.4

Secondary DNS 198.18.100.8

Primary WINS 0.0.0.0

Secondary WINS 0.0.0.0

Primary NIS 0.0.0.0

Secondary NIS 0.0.0.0

POP3 Server 0.0.0.0

SMTP Server 0.0.0.0

DNS Suffix ttc60z.vle.fi

Renew

Release

Close

Kuvio 2. Julkinen IP-osoite

Tämän jälkeen IP-osoite määriteltiin palomuurin julkiseksi osoitteeksi, koska palomuuuri käyttää NAT-muunnosta (ks. kuvio 3).

Address

Name public

Description CHANGEME

Type IP Netmask

198.19.52.47/32

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 3. Palomuurin julkisen IP-osoitteen asentaminen

Julkisen osoitteen asennuksen jälkeen DNS-palvelin vastasi nslookup kyselyyn DNS Rocky Linux palvelimelta oikealla osoitteella (ks. kuvio 4).



```
Rocky Linux release 8.6 (Green Obsidian)
For JAMK/IT use only

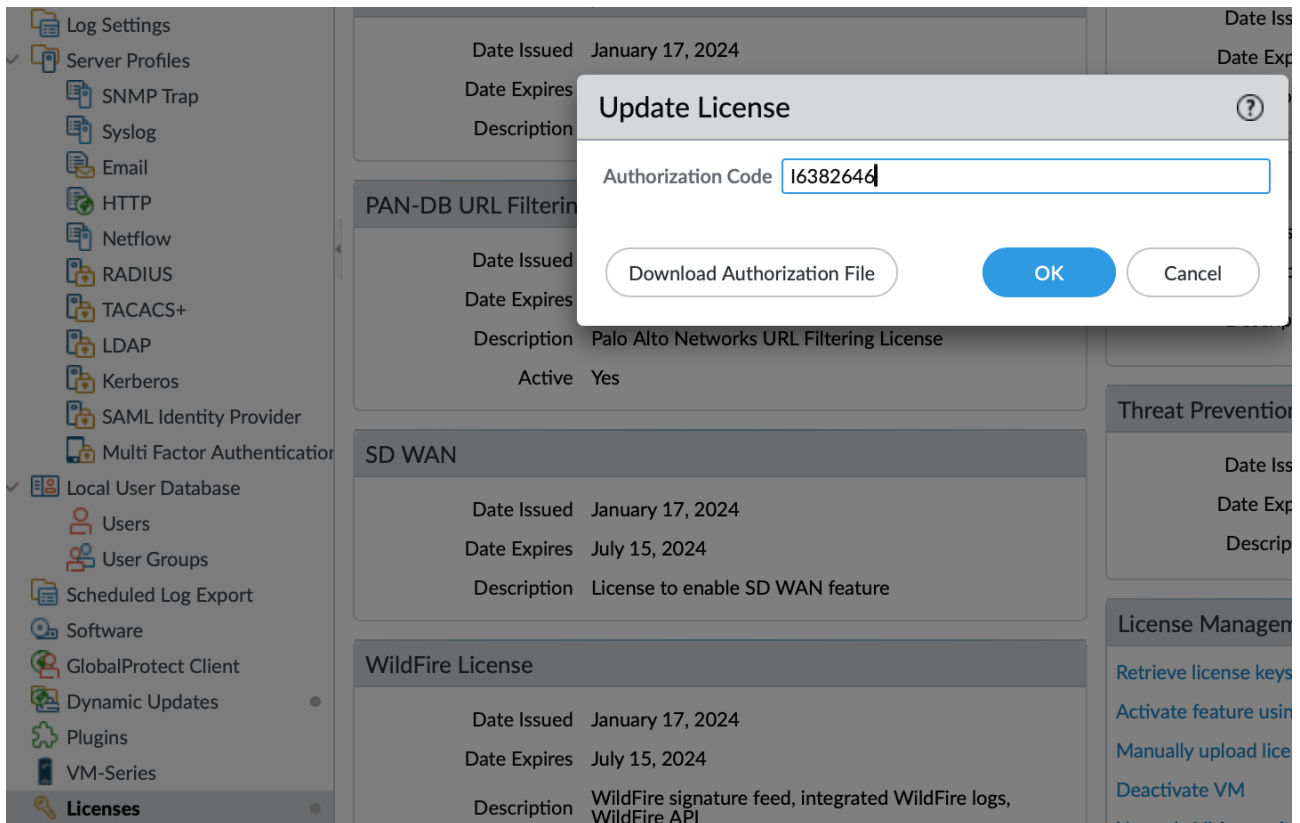
IP address (probably): 10.4.0.10

ns1 login: root
Password:
Last login: Thu Sep  1 15:19:04 on tty1
[root@ns1 ~]# nslookup ns1.group3.ttc60z.vle.fi
Server:          198.18.100.4
Address:         198.18.100.4#53

Non-authoritative answer:
Name:   ns1.group3.ttc60z.vle.fi
Address: 198.19.52.47
```

Kuvio 4. NSlookup kysely

Seuraavaksi asensimme lisenssin aktivointikoodin. Tiettyjen ominaisuuksien käyttöönotto vaatii ilmaisen lisenssin aktivoimista (ks. kuvio 5).



#### Kuvio 5. Lisenssin asentaminen

Seuraavaksi piti asentaa GlobalProtect portaalin SSL-yhteyttä varten sertifikaatti. Koska asennus tapahtui opettajan antaman asennusohjeen mukaisesti, joka piti sisällään kuvat. Emme ota kaikista vaiheista todennuskuvia, ainoastaan tärkeimmistä. Asennus tehtiin kohdasta: Network – GlobalProtect - Portals (Ks. kuviot 6–10).

**GlobalProtect Portal Configuration** ⓘ

**General**

Name: GP\_group\_3

**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 6. Portaalin asennus - yleinen sivu

**GlobalProtect Portal Configuration** ⓘ

**General**

**Authentication**

Portal Data Collection

Agent

Clientless VPN

Satellite

**Server Authentication**

SSL/TLS Service Profile: GP\_group\_3\_SSL

**Client Authentication**

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

+ Add - Delete Clone ↑ Move Up ↓ Move Down

Certificate Profile: None

OK Cancel

## Kuvio 7. Portaalin asennus - SSL autentikaatio

**GlobalProtect Portal Configuration** ?

General  
Authentication  
Portal Data Collection  
**Agent**  
Clientless VPN  
Satellite

**Agent**

<input type="checkbox"/>	CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
<input type="checkbox"/>	GP_group_3_conf	any	any	GP_group_3_ext_gw	local

+ Add - Delete Clone ↑ Move Up ↓ Move Down

<input type="checkbox"/>	TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE
<input type="checkbox"/>		

+ Add - Delete

Agent User Override Key   
Confirm Agent User Override Key

OK Cancel

Kuvio 8. Portaalin asennus – gateway

**Configs** ?

Authentication | Config

Cutoff Time (sec) 5

**External Gateways**

<input type="checkbox"/>	NAME
<input checked="" type="checkbox"/>	GP_group_3_ext_gw

+ Add - Delete

**THIRD PARTY VPN**

**External Gateway** ?

Name

Address ☐ FQDN ☒ IP

IPv4

IPv6

1 item → ×

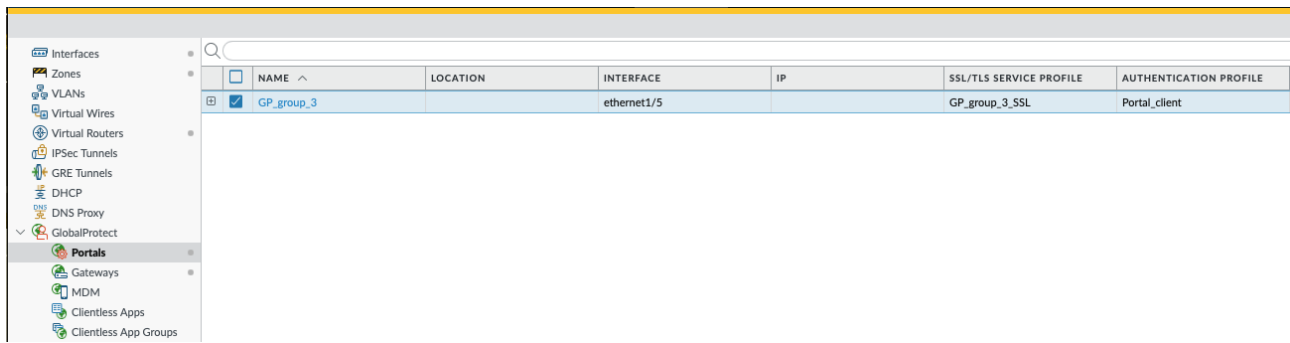
<input type="checkbox"/>	SOURCE REGION	PRIORITY
<input type="checkbox"/>	Any	Highest

+ Add - Delete

☐ Manual (The user can manually select this gateway)

OK Cancel

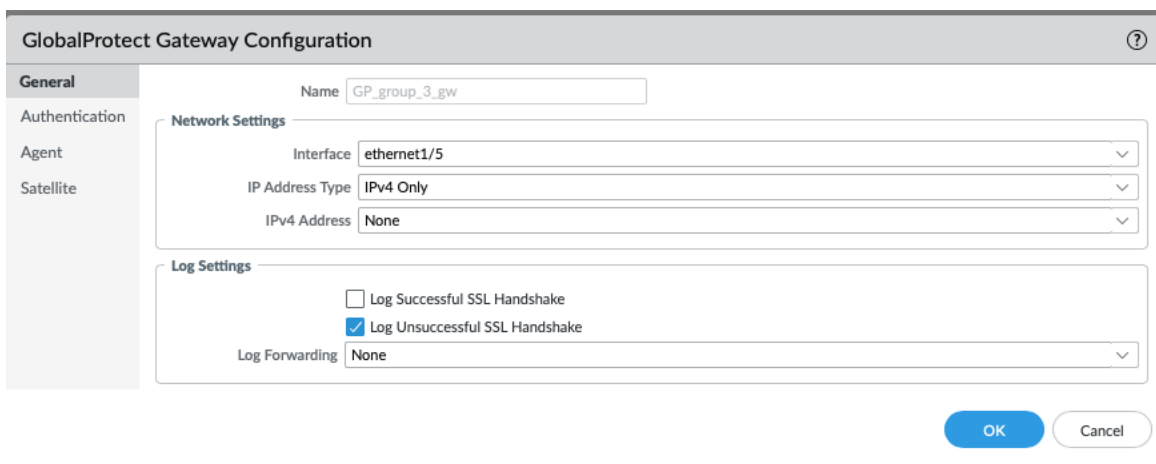
Kuvio 9. Portaalin asennus - gateway osoite



NAME ^	LOCATION	INTERFACE	IP	SSL/TLS SERVICE PROFILE	AUTHENTICATION PROFILE
<input checked="" type="checkbox"/> GP_group_3		ethernet1/5		GP_group_3_SSL	Portal_client

Kuvio 10. Portaalin asennus valmis

Seuraava vaihe oli asentaa GlobalProtectiin gateway. Asennus tehtiin kohdasta: Network – Global-Protect - Gateways (Ks. kuviot 11–15).



**GlobalProtect Gateway Configuration**

**General**

Name: GP\_group\_3\_gw

**Authentication**

**Agent**

**Satellite**

**Network Settings**

Interface: ethernet1/5

IP Address Type: IPv4 Only

IPv4 Address: None

**Log Settings**

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding: None

OK Cancel

Kuvio 11. Gateways asennus - yleinen asetussivu

**GlobalProtect Gateway Configuration** ⓘ

General

**Authentication**

Agent

Satellite

**Server Authentication**

SSL/TLS Service Profile

**Client Authentication**

<input type="checkbox"/>	NAME	OS	AUTHENTICAT... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
<input type="checkbox"/>	GP_group_3_...	Any	Portal_client	<input type="checkbox"/>	Username	Password	Enter login credentials	Yes

+ Add - Delete ↺ Clone ↑ Move Up ↓ Move Down

Certificate Profile

☒ Block login for quarantined devices

OK Cancel

Kuvio 12. Gateways asennus – autentikaatio

**GlobalProtect Gateway Configuration** ⓘ

General

Authentication

**Agent**

Satellite

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

☒ Tunnel Mode

Tunnel Interface

Max User

☒ Enable IPSec

GlobalProtect IPSec Crypto

☐ Enable X-Auth Support

Group Name

Group Password

Confirm Group Password

☒ Skip Auth on IKE Rekey

OK Cancel

Kuvio 13. Gateways asennus -tunnelointi

**GlobalProtect Gateway Configuration**

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

**Agent**

Satellite

1 item → ×

	CONFIGS	USERS	OS	Source Address		IP POOL	INCLUDE ACCESS ROUTE
				REGION	IP ADDRESS		
<input type="checkbox"/>	GP_group_...	any	any			10.255.254.0/24	10.1.0.0/24 10.2.0.0/24 10.3.0.0/24 10.4.0.0/24

+ Add - Delete Clone ↑ Move Up ↓ Move Down

OK Cancel

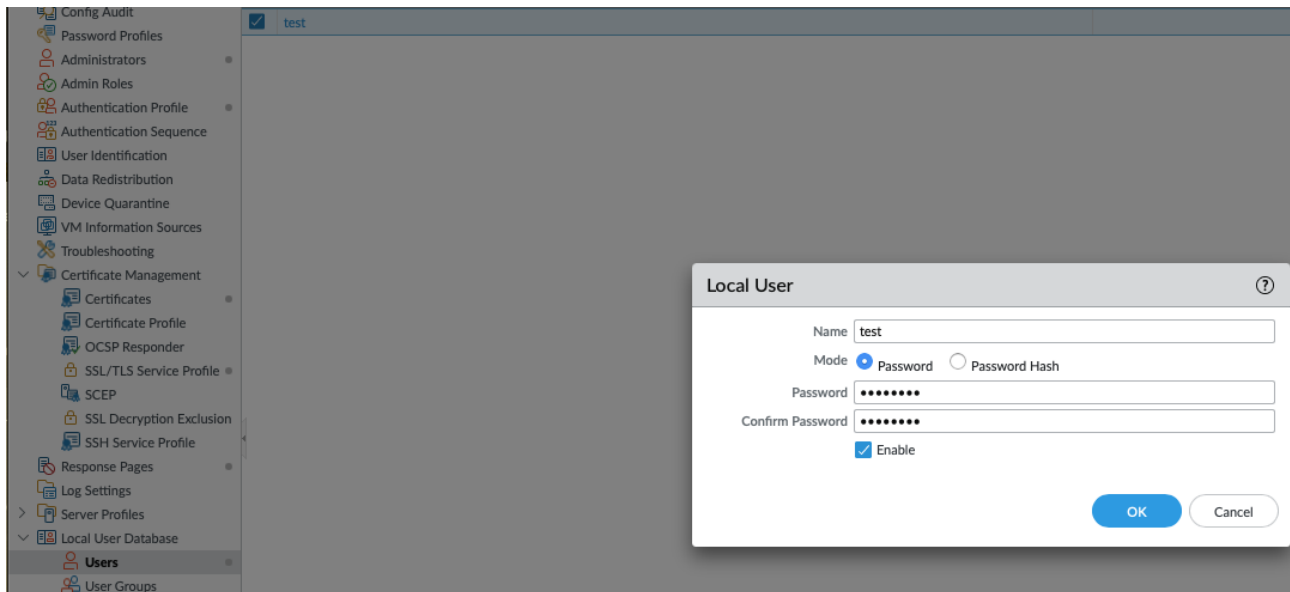
Kuvio 14. Gateways asennus - IP-pooli 10.255.254.0/24

Interfaces	
Zones	
VLANs	
Virtual Wires	
Virtual Routers	
IPSec Tunnels	
GRE Tunnels	
DHCP	
DNS Proxy	
GlobalProtect	
Portals	
<b>Gateways</b>	
MDM	
Clientless Apps	
Clientless App Groups	

	NAME	LOCATION	LOCAL INTERFACE	LOCAL IP	TUNNEL
<input checked="" type="checkbox"/>	GP_group_3_gw		ethernet1/5		tunnel.1

Kuvio 15. Gateways asennus – valmis

Seuraavaksi teimme ohjeen mukaisesti käyttäjätilin millä kirjaututaan VPN-client sovelluksella tai ladataan portaalista client-ohjelma työasemalle (ks. kuvio 16). Asennus tapahtuu Device – local user database – users sivulta.



Kuvio 16. Lisätään käyttäjätili

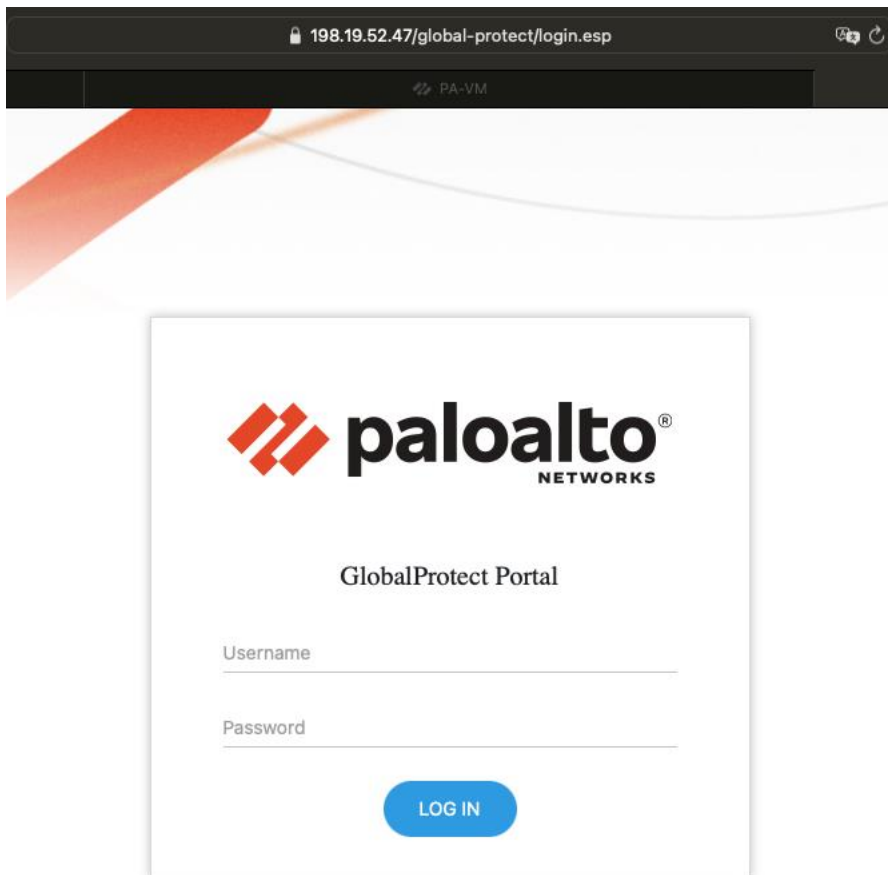
Seuraavaksi piti aktivoida GlobalProtect client, jotta client-ohjelman voi ladata omalle työasemalle. Asennus tapahtui Device – GlobalProtect Client (ks. kuvio 17).

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	
6.2.2	209 MB	2023/11/22 07:58:19	✓	✓	<a href="#">Reactivate</a>	<a href="#">Release Notes</a>

Kuvio 17. Client-ohjelma versio 6.2.2 on valmis ladattavaksi

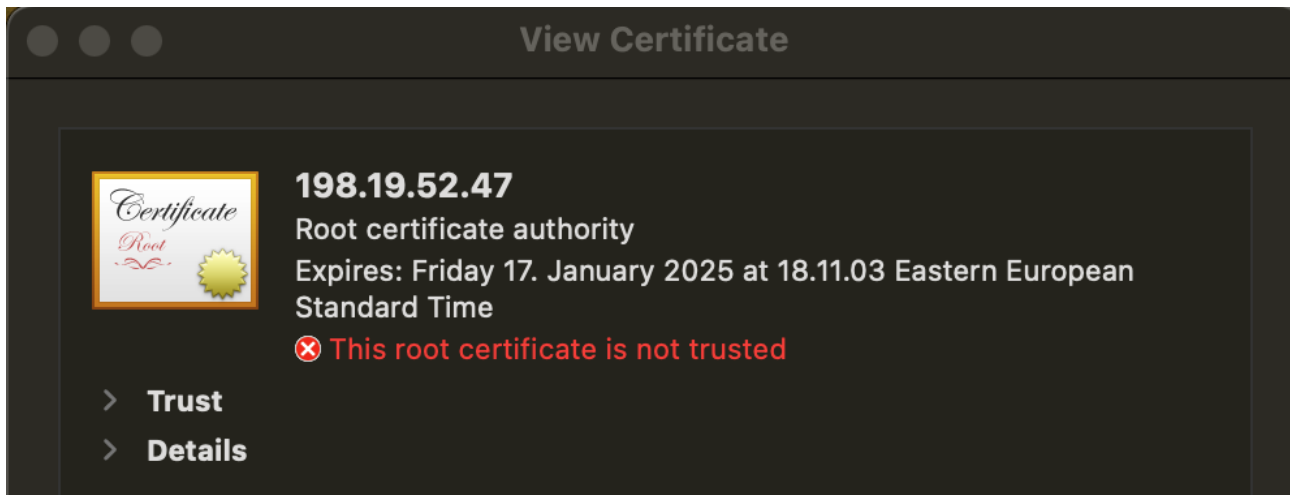
Client-ohjelman lataamista varten piti navikoida portaalin WEB-sivulle (ks. kuvio 18).





Kuvio 18. Näkymä portaalin sivusta

Ohjelman asennuksen jälkeen jokaisen käyttäjän piti kirjatua VPN-client liittymään. Asettaa Gateway sertifikaatti luotetuksi ja mahdollisesti siirtää sertifikaatti oikeaan kansioon riippuen käyttääkö WIN- tai MacOS-käyttöjärjestelmää (ks. kuvio 19). Kun nämä olivat tehty, VPN-yhteys alkoi toimimaan. Yhteyden todennuskuva kohdassa 3.3.



Kuvio 19. Sertifikaatti piti asettaa luotetuksi ja siirtää se oikeaan paikkaan

### 3.2 Palomuurin säännöt

Toisessa vaiheessa tutkimme, miten voisimme saada SSH- ja RDP-yhteydet toimimaan lisäämällä palomuurille uusia sääntöjä sekä luomme uuden alueen VPN:lle vai käytämmekö WS-nettiä.

Tunnelia tehdessä mietimme, luomme uuden alueen VPN:lle vai käytämmekö WS-nettiä. Aluksi päädyimme käyttämään WS-nettiä, jolloin RDP-yhteydellä sai heti yhteyden WS01-koneelle. Teimme myös uudet säännöt SSH:lle ja RDP:lle, jolloin pystyimme ottamaan yhteyden Linux- ja Windows-koneisiin. Säännöistä lisää myöhemmin.

Tässä kohtaa mietimme kuitenkin uuden alueen tekoa VPN:lle. Uuden alueen avulla voimme tehdä sääntöjä, minne käyttäjät saa mennä ja minne ei. Muita hyviä puolia uudessa alueessa on eristäminen ja se on turvallisempi. VPN-liikenne voidaan eristää muusta verkkoliikenteestä ja se mahdollistaa erillisen turvallisuuspolitiikan VPN-liikenteelle. WS-nettiä käytettäessä hyvät puolet olisivat olleet sen yksinkertaisuudessa ja yhdenmukaisessa hallinnassa.

Menimme tunnel.1 asetuksiin ja security zone kohdassa valitsimme New Security Zone. Zonen asetuksissa nimesimme sen VPN-ZONEksi ja laitoimme User Identificationin päälle. Asetuksissa oli myös include ja exclude list joilla voidaan tunnistaa tai ei tunnistaa tietyistä osoitteista tulevia käyttäjiä mutta näihin emme laittaneet mitään (ks. kuvio 20).

Zone

NameVPN-ZONE

Log SettingNone

TypeLayer3

INTERFACES

+ Add - Delete

Zone Protection

Zone Protection ProfileNone

☒ Enable Packet Buffer Protection

User Identification ACL

☒ Enable User Identification

☐ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

☐ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will not be identified.

Device-ID ACL

☐ Enable Device Identification

☐ INCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Devices from these addresses/subnets will be identified.

☐ EXCLUDE LIST

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Devices from these addresses/subnets will not be identified.

OK

Cancel

Kuvio 20. Zone-alueen määrittäminen

Tunnelin security zone kohtaan laitoimme nyt VPN-ZONE (ks. kuvio 21).

**Tunnel Interface** ⓘ

Interface Name  .

Comment

Netflow Profile  ▼

**Config** | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router  ▼

Security Zone  ▼

OK Cancel

Kuvio 21. Tunneloinnin yhdistäminen ZONE:en

Menimme policies välilehdelle ja teimme uuden säännön VPN-SSH. Rule type kenttään laitoimme universal eli tätä yleissääntöä käytetään kaikkeen liikenteeseen kahden alueen välillä riippumatta siitä, onko se samalta vai eri alueelta. Lähteeksi laitoimme VPN-ZONE ja kohteeksi any. Olisimme voineet laittaa kohteeksi esimerkiksi pelkän Kali Linuxin, jolloin se olisi ollut ainoa kohde mihin olisi voinut ottaa SSH-yhteyden. Lähde tarkoittaa tässä mistä liikenne lähtee ja kohde, mihin liikenne menee. Application (sovellus) kohtaan laitoimme ssh eli minkälaista liikennettä sääntö koskee (ks. kuvio 22).

**Security Policy Rule** ⓘ

General | Source | Destination | **Application** | Service/URL Category | Actions | Usage

☐ Any

☒ APPLICATIONS ^

☒ ssh

☐ DEPENDS ON

0 items → ×

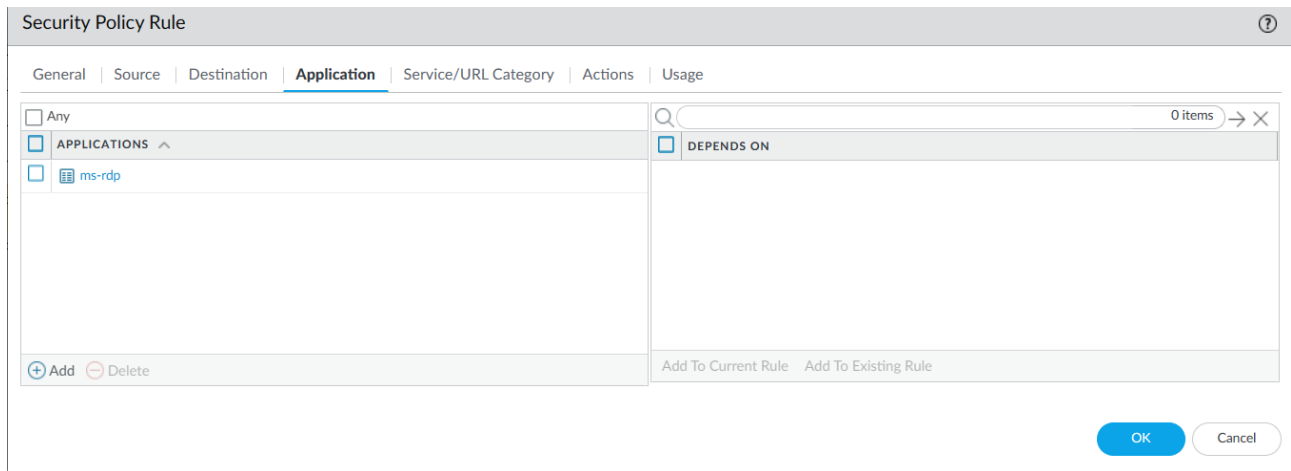
+ Add - Delete

Add To Current Rule Add To Existing Rule

OK Cancel

Kuvio 22. SSH valittuna applications välilehdellä

Windows-koneita varten teimme uuden VPN-RDP säännön. Sääntö oli muuten samanlainen kuin SSH:ta varten tehty sääntö mutta applications kohtaan laitoimme ms-rdp (ks. kuvio 23).



Kuvio 23. MS-RDP valittuna applications välilehdellä

Näiden sääntöjen asettamisen jälkeen pystyimme ottamaan SSH- ja RDP-yhteyksiä Linux-koneisiin sekä Windows-koneisiin. Huomasimme myös, kun laitoimme VPN-yhteyden päälle, yhteys internetiin katkesi. Tämä saatiin ratkaistua luomalla uusi sääntö VPN-INTERNET, joka sallii internetin selaamisen. Tämän lisäksi NAT välilehdellä piti lisätä tekemämme VPN-ZONE ACCES-TO-VLE sääntöön (ks. kuvio 24).

Security

HAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

DoS Protection

SD-WAN

3 items

→

×

	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	
2	DNS-1	none	VLE	VLE	any	any	public	DNS/UDP	none	destination-translation address: 10.4.0.10/32 port: 53	19	2024-01-22 13:01:03	2024-01-16 19:09:51	2022-08-10 01:08:34	2022-08-10	
3	ACCESS-TO-VLE	none	ADMIN-NET DMZ SERVERS-NET VPN-ZONE WS-NET	VLE	ethernet1/5	any	any	any	dynamic-ip-and-port ethernet1/5	none	30983	2024-01-22 13:40:38	2024-01-12 10:32:39	2024-01-22 13:22:11	2022-08-10	

Kuvio 24. NAT-säännöt

Lopuksi vielä kuva policies välilehdeltä (ks. kuvio 25).

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	Rule Usage		
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE						HIT COUNT	LAST HIT	FIRST HIT
1 LNS	none	unilateral	VLE	any	any	any	DMZ	any	any	dns	application...	Allow	none	☑	30	2024-05-22 12:02:02	2024-05-
2 DNS-1	none	unilateral	ADMIN-NET	any	any	any	DMZ	172.16.0.10	any	dns	application...	Allow	none	☑	0	-	-
3 GATEWAY-TO-VLE	none	unilateral	ADMIN-NET	any	any	any	VLE	any	any	any	any	Allow	none	☑	320566	2024-05-22 13:37:01	2024-05-
			DMZ														
			SUBVLE-NET														
			WS-NET														
4 WS-TO-SERVERS	none	unilateral	WS-NET	any	any	any	SERVICES-NET	any	any	any	any	Allow	none	☑	17135	2024-05-22 15:36:40	2022-04-
5 ADMIN-TO-WS	none	unilateral	ADMIN-NET	any	any	any	WS-NET	any	any	any	any	Allow	none	☑	0	-	-
6 VPN-SSH	none	unilateral	VPN-ZONE	any	any	any	any	any	any	ssh	application...	Allow	none	☑	21	2024-05-20 20:33:21	2024-05-
7 VPN-RDP	none	unilateral	VPN-ZONE	any	any	any	any	any	any	rdp	application...	Allow	none	☑	55	2024-05-20 21:41:53	2024-05-
8 VPN-INTERNET	none	unilateral	VPN-ZONE	any	any	any	VLE	any	any	any	any	Allow	none	☑	126	2024-05-22 13:28:39	2024-05-
										any	any						
										any	any						
										any	any						
9 Internet-Default	none	intrazone	any	any	any	any	Internet	any	any	any	any	Allow	none	☑	4041	2024-05-22 12:30:17	2022-04-
10 Internet-Default	none	intrazone	any	any	any	any	any	any	any	any	any	Deny	none	☑	213141	2024-05-22 13:05:43	2022-04-

Kuvio 25. Policies välilehti

3.3 Todennukset

VPN-clientin toimivuus työasemalla (ks. kuvio 26).



Kuvio 26. VPN-client yhteys palomuurille todennus

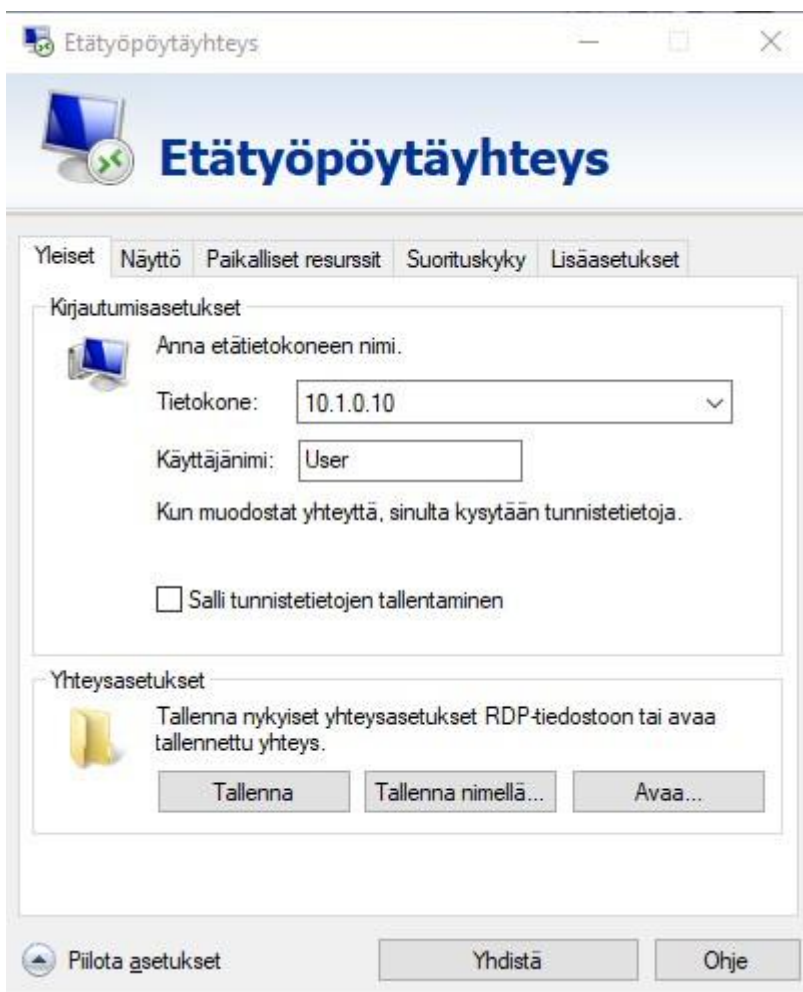
SSH-yhteyden todennus DNS-palvelimelle (ks. kuvio 27).

```
Restored session: 08 / Jan 2024 10:40:21 EDT
(base) markkusutinen@MarkkuSutinen-3 ~ % ssh root@10.4.0.11
The authenticity of host '10.4.0.11 (10.4.0.11)' can't be established.
ED25519 key fingerprint is SHA256:aNdPKJCG00IaVIG9ej75g9hpyaWw102ED4CBBcJA54.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.4.0.11' (ED25519) to the list of known hosts.
root@10.4.0.11's password:
Activate the web console with: systemctl enable --now cockpit.socket

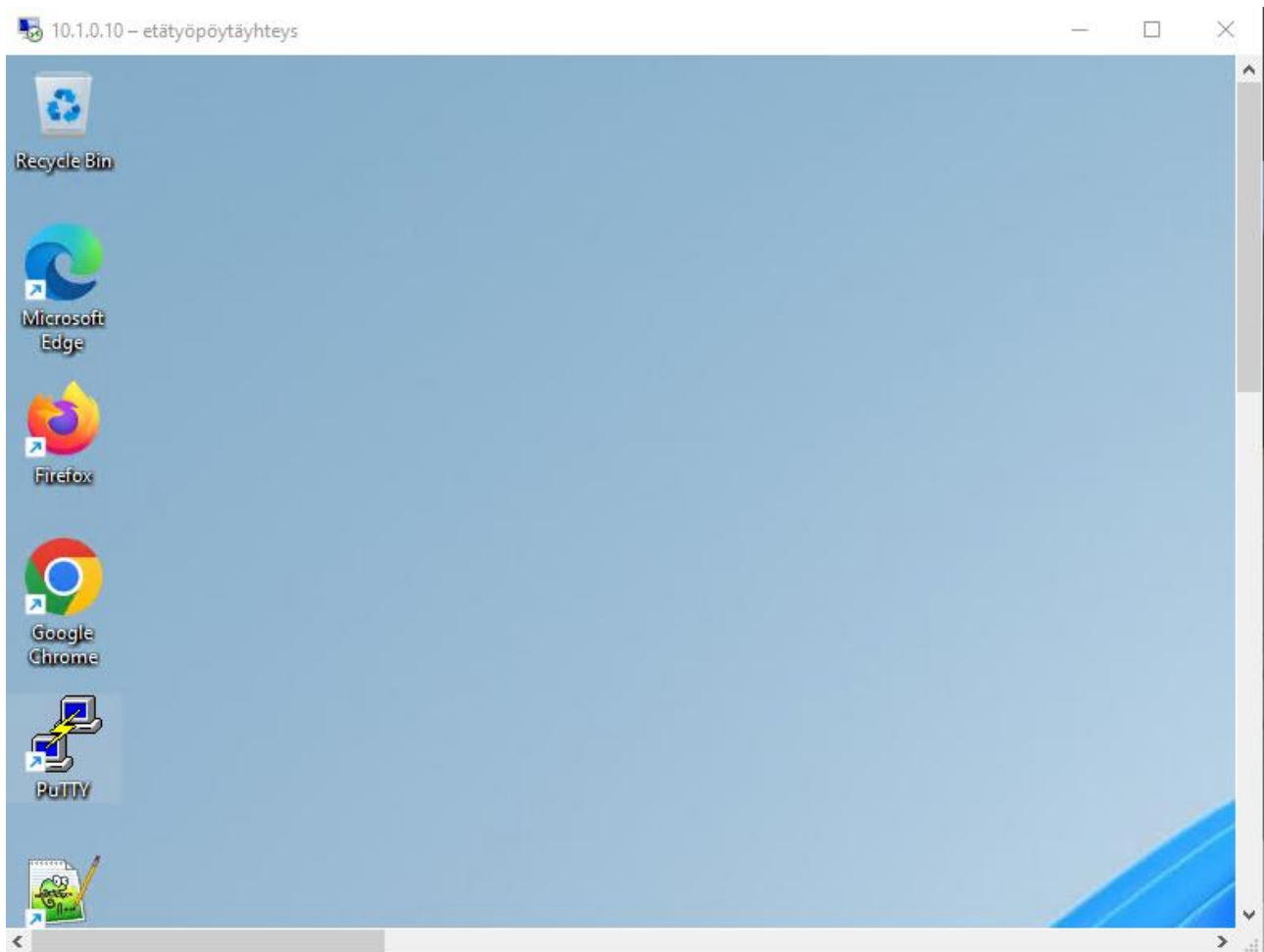
Rocky Linux 8 for IT/JYVSECTEC Production use only
Last login: Thu Jan 18 20:27:42 2024
[[root@www ~]# pwd
/root
[root@www ~]#
```

Kuvio 27. SSH-yhteyden todennus

RDP-yhteyden todennus WS01-koneelle (ks. kuvio 28 ja 29).



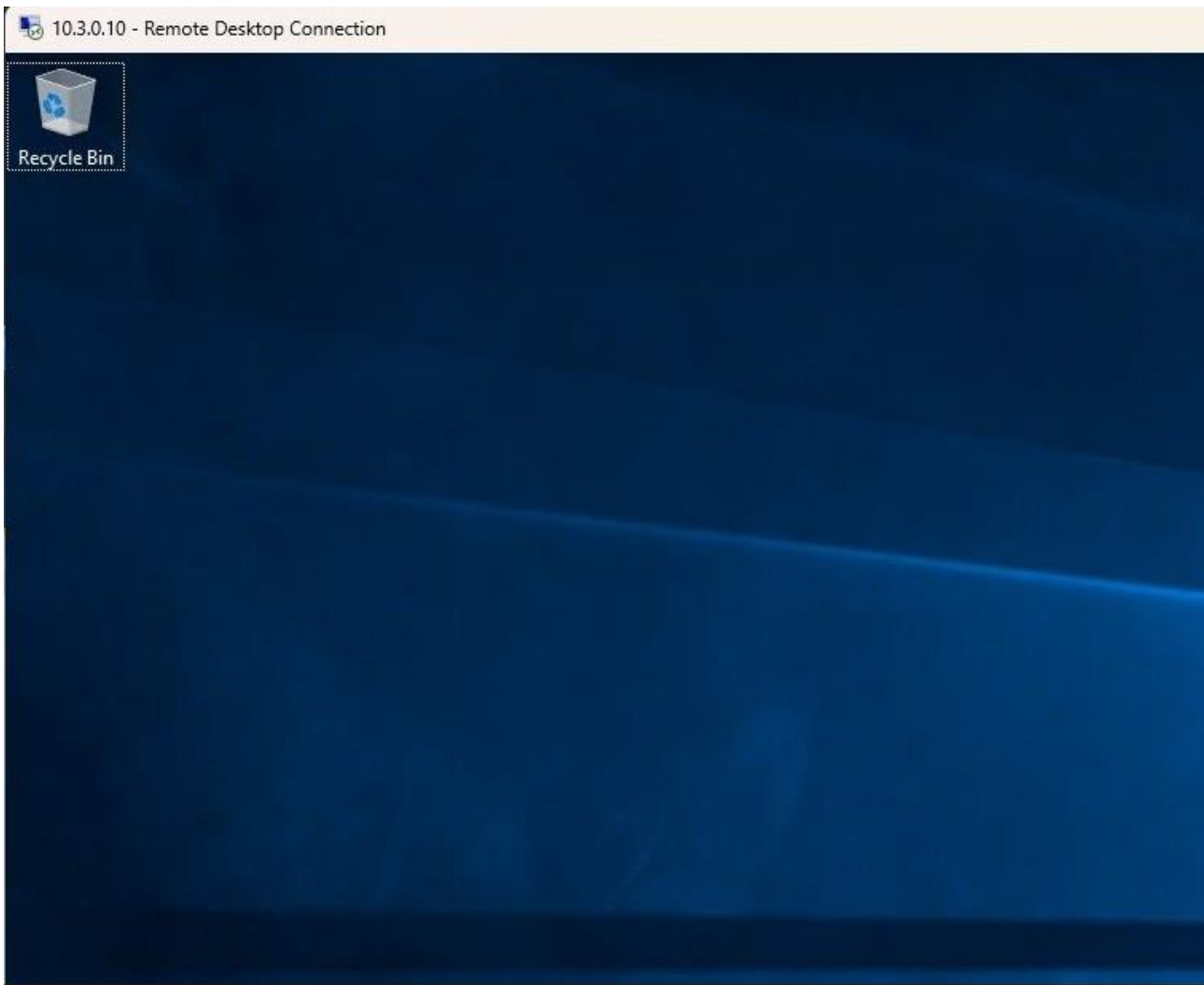
Kuvio 28. Etätyöpöytäyhteys 10.1.0.10 osoitteeseen



Kuvio 29. RDP-yhteys WS01-koneelle





















Kokeilimme myös RDP-yhteyttä DC01-palvelimelle (ks. kuvio 30).





Kuvio 30. RDP-yhteys DC01-palvelimelle

Onnistuneen yhteydenoton jälkeen palomuurin liikenteenvalvonta sivulle ilmestyi test-käyttäjä, joka oli saanut ip-poolista 10.255.254.0/24 osoitteen. Aivan niin kuin pitikin (Ks. kuvio 31)!

	01/18 20:20:12	end	WS-NET	VLE	10.255.254.1	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	620	0
	01/18 20:20:12	end	WS-NET	VLE	10.255.254.1	test		198.18.100.8			53	dns	allow	GATEWAY-TO-VLE	aged-out	634	0
	01/18 20:20:12	end	WS-NET	VLE	10.255.254.1	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	634	0
	01/18 20:20:07	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	218	0
	01/18 20:20:07	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	224	0
	01/18 20:20:07	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	224	0
	01/18 20:20:07	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	218	0
	01/18 20:20:07	end	SERVERS-NET	VLE	10.3.0.10			2.23.146.45			80	soap	allow	GATEWAY-TO-VLE	tcp-rst-from-server	2.7k	0
	01/18 20:20:07	end	WS-NET	VLE	10.255.254.1	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	640	0
	01/18 20:20:07	end	WS-NET	VLE	10.255.254.1	test		198.18.100.8			53	dns	allow	GATEWAY-TO-VLE	aged-out	640	0
	01/18 20:20:02	end	SERVERS-NET	VLE	10.3.0.10			138.91.171.81			80	incomplete	allow	GATEWAY-TO-VLE	aged-out	70	0
	01/18 20:19:57	end	SERVERS-NET	VLE	10.3.0.10			138.91.171.81			80	incomplete	allow	GATEWAY-TO-VLE	aged-out	140	0
	01/18 20:19:57	end	WS-NET	VLE	10.1.0.10			198.18.102.132			7680	insufficient-data	allow	GATEWAY-TO-VLE	tcp-fin	908	0
	01/18 20:19:57	end	WS-NET	VLE	10.255.254.2	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	2.3k	0
	01/18 20:19:57	end	WS-NET	VLE	10.255.254.2	test		198.18.100.8			53	dns	allow	GATEWAY-TO-VLE	aged-out	645	0
	01/18 20:19:57	end	WS-NET	VLE	10.255.254.1	test		198.18.100.8			53	dns	allow	GATEWAY-TO-VLE	aged-out	645	0
	01/18 20:19:57	end	WS-NET	VLE	10.255.254.1	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	642	0
	01/18 20:19:52	end	WS-NET	VLE	10.255.254.2	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	2.6k	0
	01/18 20:19:52	end	WS-NET	VLE	10.255.254.2	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	3.2k	0
	01/18 20:19:47	end	WS-NET	VLE	10.255.254.1	test		198.18.100.4			53	dns	allow	GATEWAY-TO-VLE	aged-out	308	0

Kuvio 31. Kuva verkonvalvonta sivulta

## 4 Pohdinta

Ensimmäinen ryhmätehtävä lähti hienosti liikkeelle, eikä suurempia ongelmia ollut. VPN-clienttiä käyttöön otettaessa jouduimme hieman enemmän käyttämään aikaa sertifikaatin hyväksymisen kanssa ja selvittämään miksi internetin selaaminen ei toimi. Nämä kaikki saatiin ratkaistua. Lisäksi pohdimme, voisiko tämän tehtävän tehdä yhdellä sertifikaatilla, eikä nyt tehdyllä ratkaisulla, jossa käytimme kahta. Asiaa pohdittiin ja opittiin, että vaihtoehto on myös käyttää yhtä. Lisäksi pohdimme External Gateway asetuskohdassa, että käytämmekö FQDN- vai IP-asetusta. FQDN ymmärryksemme mukaan olisi suositeltava käytäntö ja helpompi ylläpitää, mikäli IP-osoite vaihtuu. Tässä raporttiversiossa on nyt raportoitu siten, että käytämme IP-asetusta. Kumpikin tapa PaloAlton manuaalin mukaan on kuitenkin mahdollista käyttää. Kumpaa tapaa sitten käytetään, riippuu useammasta eri asiasta, jotka suunnitteluvaiheessa tulee ottaa huomioon.

## Lähteet

Definition: What Is a Firewall?. Artikkel Fortinet –sivustolla. Viitattu 20.1.2024. <https://www.fortinet.com/resources/cyberglossary/firewall>

GlobalProtect Overview. 2023. Palo Alto Networks dokumentaatio. Viitattu 21.2.2023. <https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-overview>

Mikä on VPN?. 2024. F-Secure. Viitattu 21.1.2024. <https://www.f-secure.com/fi/articles/what-is-a-vpn>

SSH software downloads. Viitattu 20.1.2024. <https://www.ssh.com/download/>

Tatu Ylönen. What is SSH (Secure Shell)?. Viitattu: 19.1.2024. <https://www.ssh.com/academy/ssh#the-ssh-protocol>

Understanding the Remote Desktop Protocol (RDP). 2023. Artikkel Microsoft –learn ympäristössä 23.2.2023. Viitattu 19.1.2024. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol>

What Is A Software Firewall vs A Hardware Firewall?. Artikkel Fortinet –sivustolla. Viitattu 20.1.2024. <https://www.fortinet.com/resources/cyberglossary/firewall>

What is VPN? How It Works, Types of VPN. 2024. Kaspersky. Viitattu 21.1.2024. <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

