



## Tietoturvakontrollit - Labra 4

### Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Jukka Virtanen

Harjoitustyö

Helmikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

## Sisältö

<b>1</b>	<b>Johdanto .....</b>	<b>4</b>
<b>2</b>	<b>Teoria.....</b>	<b>4</b>
2.1	User-ID.....	4
2.2	LDAP (Lightweight Directory Access Protocol).....	5
2.2.1	LDAP Active Directoryssa .....	6
2.2.2	LDAP Palo Altossa .....	6
2.3	Paikallinen ja ulkoinen tunnistautuminen .....	6
<b>3</b>	<b>Toteutus.....</b>	<b>7</b>
3.1	Local ympäristö .....	7
3.2	Active Directory Integraatio .....	11
3.3	Testaaminen ja uudet säännöt sekä extra tehtävä.....	22
<b>4</b>	<b>Pohdinta.....</b>	<b>28</b>
	<b>Lähteet .....</b>	<b>30</b>

## Kuviot

Kuvio 1. Autentikaatio profiili .....	7
Kuvio 2. Profiilin vaihtaminen .....	8
Kuvio 3. Tunnistautumisen määrittely.....	8
Kuvio 4. Tunnistautumisen sääntö.....	9
Kuvio 5. Säännön asetukset .....	9
Kuvio 6. Tietojen lisäys Kali-työasemalle .....	10
Kuvio 7. Näkymä tunnistautumisen sivusta.....	10
Kuvio 8. Käyttäjistä jää jälki lokiin .....	11
Kuvio 9. Uusi käyttäjä.....	12
Kuvio 10. Ryhmät joihin uusi käyttäjä kuuluu.....	13
Kuvio 11. Sallitut portit .....	14
Kuvio 12. Thumbprint .....	15
Kuvio 13. Kolme käskyä.....	16
Kuvio 14. Sertifikaatti ulos .....	16

Kuvio 15. Sertifikaatti viety Palo Altoon .....	17
Kuvio 16. LDAP Server Profile .....	17
Kuvio 17. User-ID Agent .....	18
Kuvio 18. Server Monitoring .....	19
Kuvio 19. Certificate Profile .....	20
Kuvio 20. Uusi käyttäjä lisätty Cert Publishers ryhmään .....	21
Kuvio 21. Group Mapping ryhmien lisäys .....	22
Kuvio 22. Policy säännöt .....	23
Kuvio 23. Uusi käyttäjä, joka linkitetty testiryhmään .....	23
Kuvio 24. Domadmin -käyttäjä.....	24
Kuvio 25. Veikkaus -sivu varoituksella .....	24
Kuvio 26. Testiryhma -monitorlehdellä .....	25
Kuvio 27. Veikkaus ilman varoitusta .....	25
Kuvio 28. Luodaan uusi profiili .....	26
Kuvio 29. Otetaan uusi profiili käyttöön .....	26
Kuvio 30. Luodaan uusi captive portal .....	27
Kuvio 31. Päivitetään autentikaatio sääntö .....	27
Kuvio 32. Oletus sivuille päästään .....	28
Kuvio 33. Näkymä palomuurin loki:sta .....	28

# 1 Johdanto

Tietoturvakontrollien neljännessä labrassa tutustuttiin käyttäjäidentiteetin mukaan ottamiseen pääsykontrolleihin. Aluksi käytettiin Palo Altoon paikallisesti luotua käyttäjää ja toteutettiin siihen sidottu konfiguraatio, jossa webbisivullemme sallittiin pääsy vain kyseiselle käyttäjälle. Konfiguroitiin Captive Portal jonne tunnistautumaton käyttäjä aluksi ohjataan tunnistautumaan ja mikäli OK, sallitaan pääsy eteenpäin.

Seuraavaksi siirryttiin konfiguroimaan AD-integraatio Palo Altoon, jotta saatiin sille näkyvyys AD-käyttäjiin ja -ryhmiin. Integraation käyttämä AD-käyttäjä luotiin, domain controllerin paikallisella palomuurilla sallittiin tarvittavat yhteydet, sertikaatti ja muu tarvittava konfiguraatio säädettiin ohjeiden mukaisesti ja testattiin, minkä jälkeen päästiin tutustumaan AD-käyttäjiin sidottuun pääsykontrolliin. Testattiin sekä AD-käyttäjään että AD-ryhmään perustuvaa kontrollia.

## 2 Teoria

### 2.1 User-ID

User-ID:n ideana on liittää IP-osoitteesta tulevan verkkoliikenne tunnistettuun käyttäjään siten että liikenteestä ja lähdelaitteesta riippumatta voidaan saavuttaa:

- Näkyvyys siihen mitkä käyttäjät ovat minkäkin verkkoaktiviteetin takana, millaista käyttö on ja liittykö siihen mahdollisesti uhkia
- Kontrolli siihen mitä oikeuksia käyttäjittäin tai käyttäjäryhmittäin on sallittu liikenteen suhteen
- Lokitus, raportit ja forensikka josta saadaan käyttäjäkohtaisesti selville mitä on tehty ja milloin.

Käyttäjäidentiteetin liittämiseen verkkoliikenteeseen eli User Mappingin toteuttamiseen on erilaisia mahdollisuuksia, joita Palo Alto tukee: Server Monitoring, Port Mapping, Syslog, XFF Headers, Username Header Insertion, Authentication Policy and Captive Portal, GlobalProtect, XML API ja Client Probing

Palo Altolla tulee olla lisäksi käytössään tiedot käyttäjistä ja ryhmistä. Tyypillinen tapa tämän toteuttamiseen on käyttää integraatiota LDAP-hakemistopalveluun, josta nämä tiedot löytyvät. (User-ID Overview 2023.)

## 2.2 LDAP (Lightweight Directory Access Protocol)

LDAP on ohjelmistoprotokolla, joka mahdollistaa datan löytämisen organisaatio ja yksilötasolla sekä mm. tiedostojen sijainnin tai verkossa olevat laitteet. Sitä voidaan käyttää julkisen verkon yli tai yrityksen intranetissä. LDAP on kevennetty versio Directory Access Protocol:sta (DAP), joka on osa X.500 standardia, hakemistopalvelut tietoverkossa. LDAP:a pidetään kevyenä, koska se käyttää muita protokollia vähemmän koodia. (Gillis 2022)

Hakemistot kertovat käyttäjälle, minne jokin verkossa on sijoittunut. TCP/IP verkoissa DNS on hakemistojärjestelmä, jolla verkkotunnusta verrataan tarkkaan verkko-osoitteeseen. Käyttäjä ei välttämättä tiedä tarkkaa verkkotunnusta. LDAP mahdollistaa yksilöidyn tiedon etsimisen silloinkin, kun tarkka sijainti ei ole tiedossa. LDAP:n yleisin käyttöaihe on tarjota keskitetty ympäristö tunnistautumiselle, siellä siis voidaan säilyttää käyttäjätunnuksia ja salasanoja. Silloin sitä on mahdollista käyttää eri sovelluksissa sekä palveluissa käyttäjien tunnistamiseen ja käyttöoikeuksien vahvistamiseen, liitännäisten (plugin) avulla. (Gillis 2022.)

Yleisesti LDAP- tunnistautuminen saavutetaan client/server mallin mukaisella bind-operaatiolla. Tyypilliseseti client on LDAP-valmis järjestelmä tai sovellus, jota käyttäjä käyttää. LDAP hakemistotietokanta toimii serverinä. Käyttäjä lähettää omilla pääsytiedoillaan (credential) kyselyn LDAP-serverille, joka vertaa niitä LDAP tietokantaan tallennettuihin tietoihin. Jos käyttäjä tunnistetaan ja pääsy tavoiteltuun resurssiin sallitaan, tapahtuu se clientin kautta. Jos pääsytiedot eivät vastaa, pääsy evätään. (Blanton 2023.)

### 2.2.1 LDAP Active Directoryssa

AD on hakemistopalvelu, jolla voidaan hallita domaineita, käyttäjiä sekä hajautettuja resursseja (distributed resources), kuten Windows käyttöjärjestelmiä. Palvelulla voidaan hallita domaineita ja objekteja, samalla määrittäen jokaisen käyttäjän tai ryhmän oikeudet tiettyyn resurssiin. Se sisältää tiedon jokaisesta verkon käyttäjätalista ja kohtelee niitä objekteina. Jokaisella käyttäjällä on monta ominaisuutta, kuten käyttäjänimi, salasana, sähköposti yms. LDAP:n tehtävänä on saattaa tämä tieto käytettävään muotoon. Se käyttää merkkijonopohjaista (string-based) kyselyä tiedon hakemiseksi AD:sta. LDAP kykenee tallentamaan ja poimimaan objekteja AD:sta ja jakamaan objektidataa verkon läpi. (Gillis 2022.)

### 2.2.2 LDAP Palo Altossa

Palo Alton palomuurilla LDAP:aa voidaan käyttää tunnistamaan sovelluksia tai verkkoa käyttäviä käyttäjiä tunnistautumisportaalin (authentication portal) kautta. Se mahdollistaa sääntöjen (policy) luomisen käyttäjille sekä ryhmillä, ei pelkästään IP-osoitteille. (LDAP 2024). Tähän käytetään Group Mappingia. (Map Users to Groups 2024). Kun User-ID on sallittu (enable) palomuurilla, mahdollistuu käyttäjien ja ryhmien Security-sääntöjen hyödyntäminen. (Enable User- and Group-Based Policy 2024.)

## 2.3 Paikallinen ja ulkoinen tunnistautuminen

Paikallinen tunnistautuminen tapahtuu palomuurille luoduilla käyttäjillä. Näitä voidaan käyttää esimerkiksi erityisille tileille, joita ei haluta hallinnoida tavalliselle käyttäjille varattujen hallintapalvelinten (directory server) kautta. Esimerkiksi paikallisesti palomuurille määritetty superuser-tili mahdollistaa palomuuriin yhteyden saamisen silloinkin, kun hallintapalvelin on kaatunut. Palo Alton palomuuereille voidaan määrittää tietokantoja, jotka sisältävät käyttäjiä ja ryhmiä. Joille voidaan antaa erilaisia autentikaatio- ja kirjautumisprofiileja. Tarvittaessa voidaan esimerkiksi palomuurille luoda adimin- tili ilman paikallista tietokantaa. Tällä metodilla on mahdollista luoda käyttäjätilejä, joiden salasanojen vanhentumisasetukset poikkeavat globaaleista säännöistä. (Local

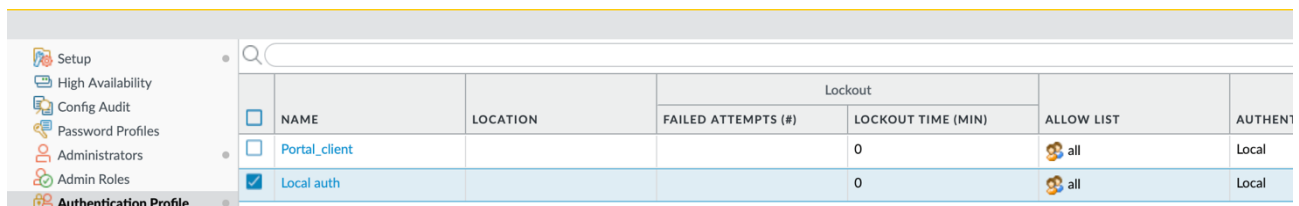
Authentication 2024.) Paikalliselle käyttäjälle voidaan Authentication policyn avulla määrittää, milloin hän ohjautuu Authentication Portaliin. Tällä voidaan varmistaa, kenellä on pääsy kaikkein arkaluontoisimpiin sovelluksiin ja dataan. (Map IP Addresses to Usernames Using Authentication Portal 2024.)

Ulkoinen tunnistautuminen vaatii palvelinprofiilin, joka määrittää miten palomuuuri yhdistyy palveluun. Palvelinprofiili liitetään tunnistautumisprofiiliin, jolla määritetään sovellusten ja käyttäjien asetukset. PaloAlton palomuuuri voidaan integroida Multi-Factor Authentication (MFA), SAML, Kerberos, TACACS+, RADIUS sekä LDAP- servereiden kanssa. (External Authentication Services 2024.)

### 3 Toteutus

#### 3.1 Local ympäristö

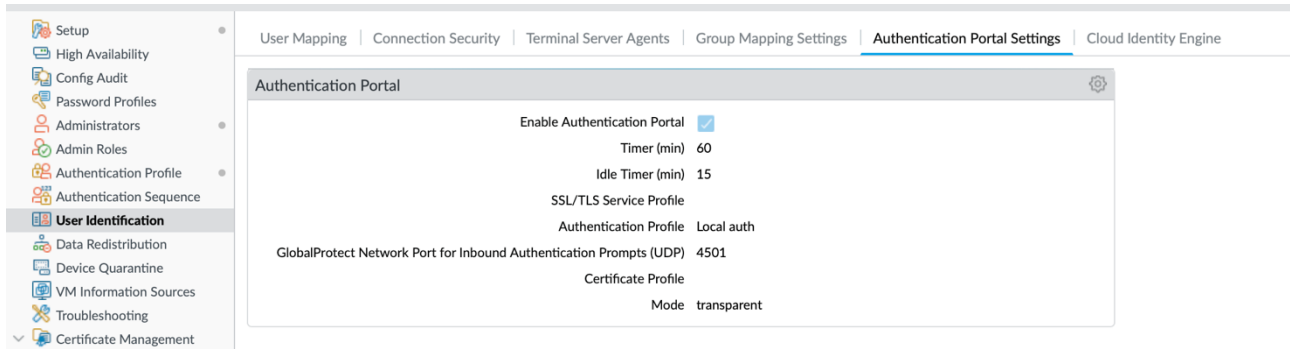
Ensimmäiseksi tehtävässä piti luoda uusi käyttäjä tai käyttää labra 1:ssä tehtyä käyttäjää. Valitsimme jälkimmäisen tavan. Meidän käyttäjämme oli nimeltään ”test”. Tämän jälkeen piti tehdä autentikaatio profiili (ks. Kuvio 1). Polku: Device – Authentication Profile.



NAME	LOCATION	Lockout		ALLOW LIST	AUTHENTICATION
		FAILED ATTEMPTS (#)	LOCKOUT TIME (MIN)		
<input type="checkbox"/> Portal_client			0	all	Local
<input checked="" type="checkbox"/> Local auth			0	all	Local

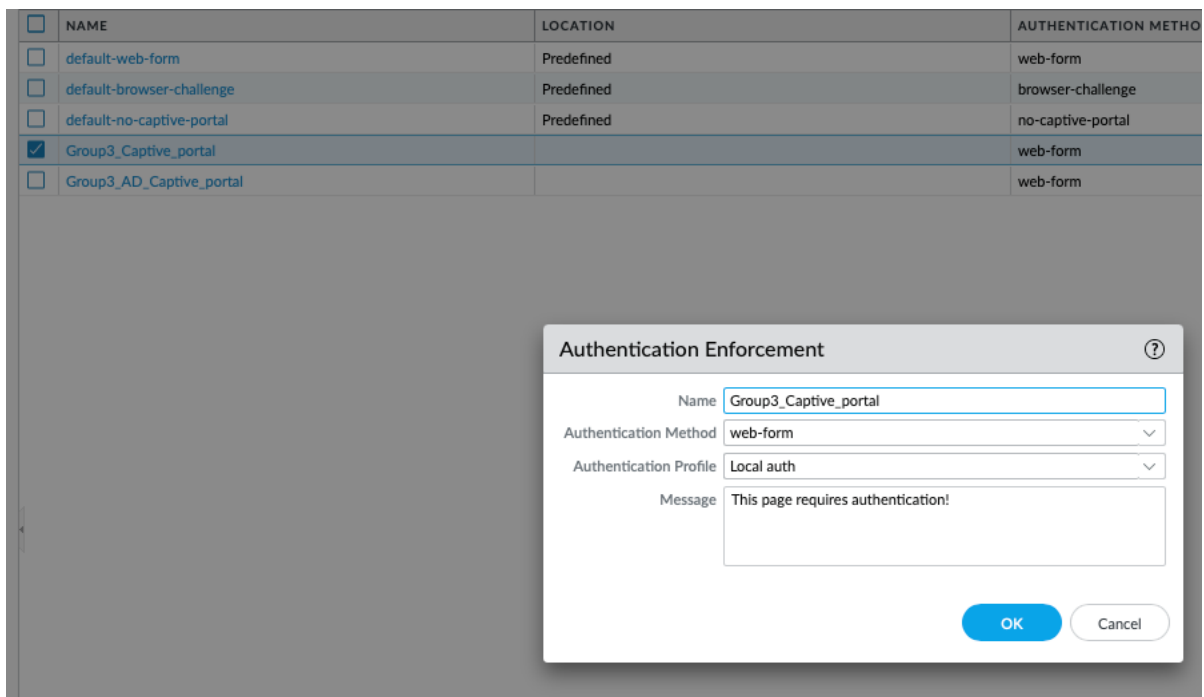
Kuvio 1. Autentikaatio profiili

Tämän jälkeen piti käydä vaihtamassa käyttäjä autentikaation asetuksissa oikea profiili eli ”local auth” (ks. Kuvio 2). Polku: Device – User Identification – Authentication Portal Settings.



Kuvio 2. Profiilin vaihtaminen

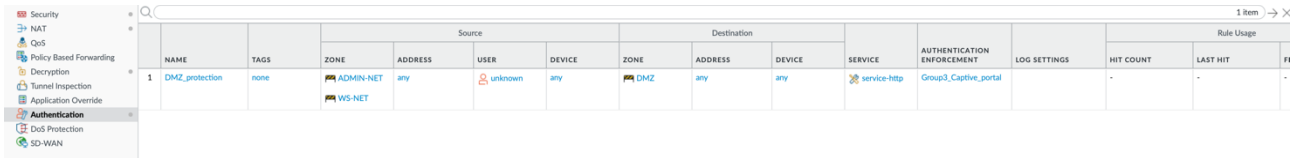
Seuraavaksi luodaan uusi tunnistautumistapa, joka tulee käyttäjälle eteen, kun hän menee selaimella haluttuun osoitteeseen eli tässä harjoituksessa WWW-palvelimen osoitteeseen (ks. Kuvio 3). Asetuksissa määritellään tavaksi web-form.



Kuvio 3. Tunnistautumisen määrittely



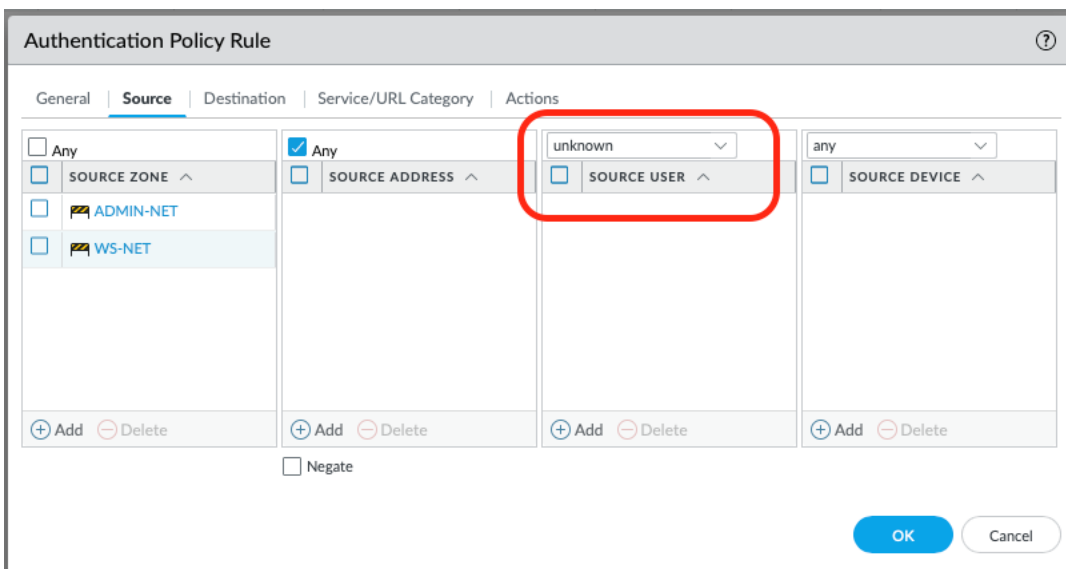
Luodaan sääntö, joka ohjaa käyttäjän tunnistautumaan (ks. Kuvio 4). Tässä säännössä myös määritellään, että ohjataan käyttäjä group3 captive portal sivulle, mikä äskettäin luotiin.



NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS	HIT COUNT	LAST HIT	FI
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE						
1 DMZ_protection	none	ADMIN-NET	any	unknown	any	DMZ	any	any	service-http	Group3_Captive_portal		-	-	-

Kuvio 4. Tunnistautumisen sääntö

Asetuksissa tuli valita kohtaan source user: unknown (ks. Kuvio 5).



Authentication Policy Rule

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

☐ Any

☒ Any

☐ SOURCE ZONE ^

☐ SOURCE ADDRESS ^

☐ SOURCE USER ^

☐ SOURCE DEVICE ^

☐ ADMIN-NET

☐ WS-NET

☐ unknown

☐ any

+ Add - Delete

+ Add - Delete

+ Add - Delete

+ Add - Delete

☐ Negate

OK Cancel

Kuvio 5. Säännön asetukset

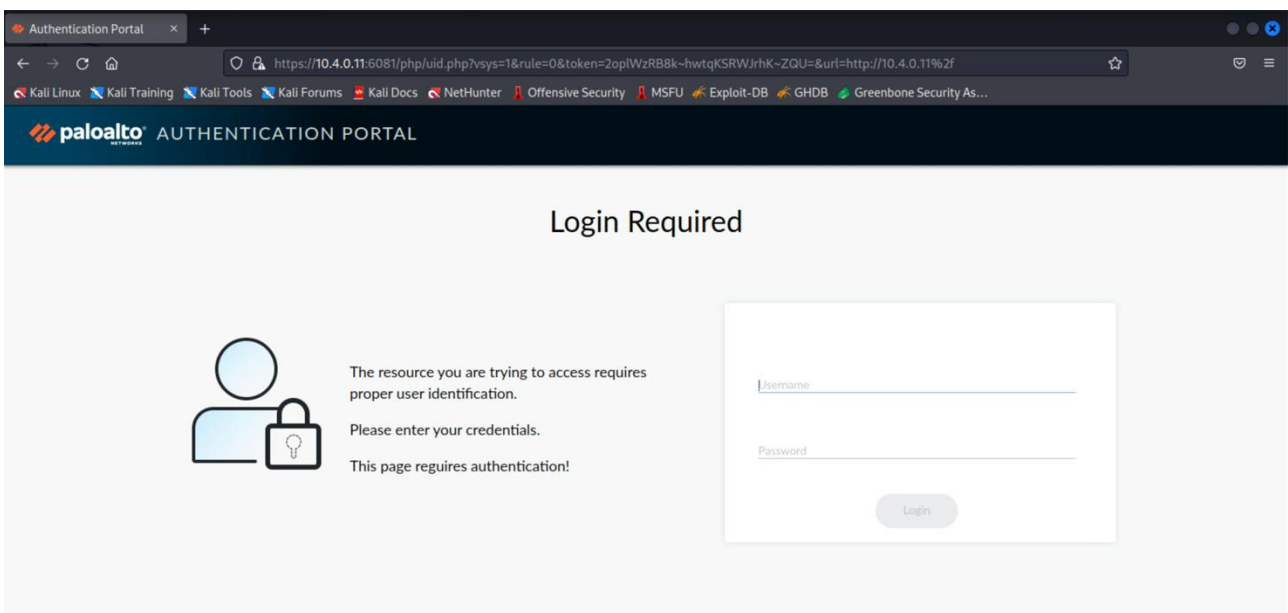
Tässä harjoituksessa on siis tarkoitus pakottaa käyttäjä tunnistautumaan, kun hän menee Kali-Linux työasemalla WWW-palvelimen osoitteeseen. Seuraavaksi lisätään WWW-palvelimen IP-osoite sekä domain nimi työaseman asetuksiin, polussa /etc/hosts (ks. Kuvio 6).

```
(kali@kali-ws)-[~]
$ cat nano /etc/hosts
cat: nano: No such file or directory
10.4.0.11      www.group3.ttc60z.vle.fi
127.0.0.1      localhost
127.0.1.1      kali-vle

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Kuvio 6. Tietojen lisäys Kali-työasemalle

Asetukset olivat oikein ja captive portal näkymä avautuu selaimessa (ks. Kuvio 7).



Kuvio 7. Näkymä tunnistautumisen sivusta

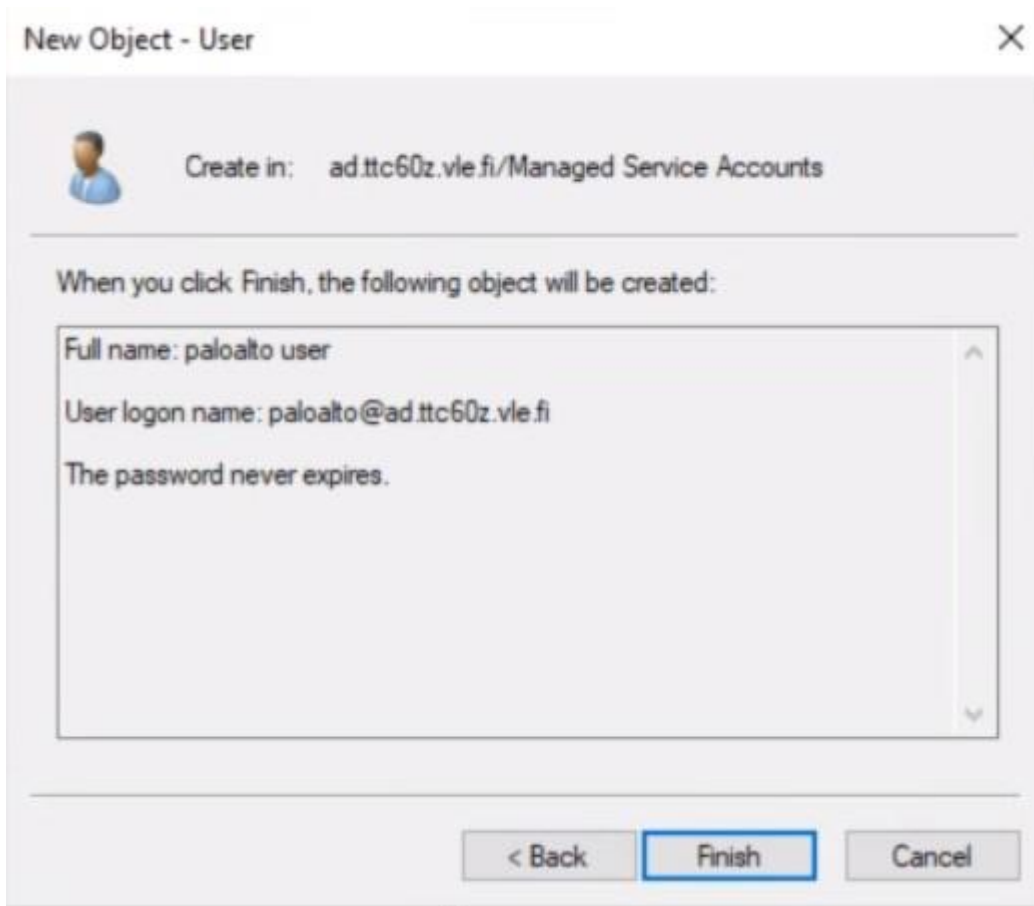
Ja kun kirjautuu test -käyttäjänä, jää myös monitor – user lokissa tiedot talteen (ks. Kuvio 8).

PA-VM												
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE												
<ul style="list-style-type: none"> <li>Logs</li> <li>Traffic</li> <li>Threat</li> <li>URL Filtering</li> <li>WildFire Submissions</li> <li>Data Filtering</li> <li>HIP Match</li> <li>GlobalProtect</li> <li>IP-Tag</li> <li>User-ID</li> </ul>	RECEIVE TIME	IP	USER	TIMEOUT	TAG	DATA SOURCE	SOURCE NAME	SOURCE TYPE	FACTOR TYPE	FACTOR COMPLETION TIME	FACTOR NUMBER	USER PROVIDED BY SOURCE
	02/15 18:55:06	10.2.0.13	test	3600		captive-portal		authenticate		2024/02/15 18:55:07	1	test
	02/15 09:49:08	10.255.254.3	test	0		vpn-client		globalprotect		2024/02/15 09:49:09	1	test
	02/15 09:45:04	10.255.254.3	test	10800		vpn-client		globalprotect		2024/02/15 09:45:05	1	test
	02/15 09:45:01	10.255.254.3	test	2591999		vpn-client		globalprotect		2024/02/15 09:45:02	1	test

Kuvio 8. Käyttäjistä jää jälki lokiin

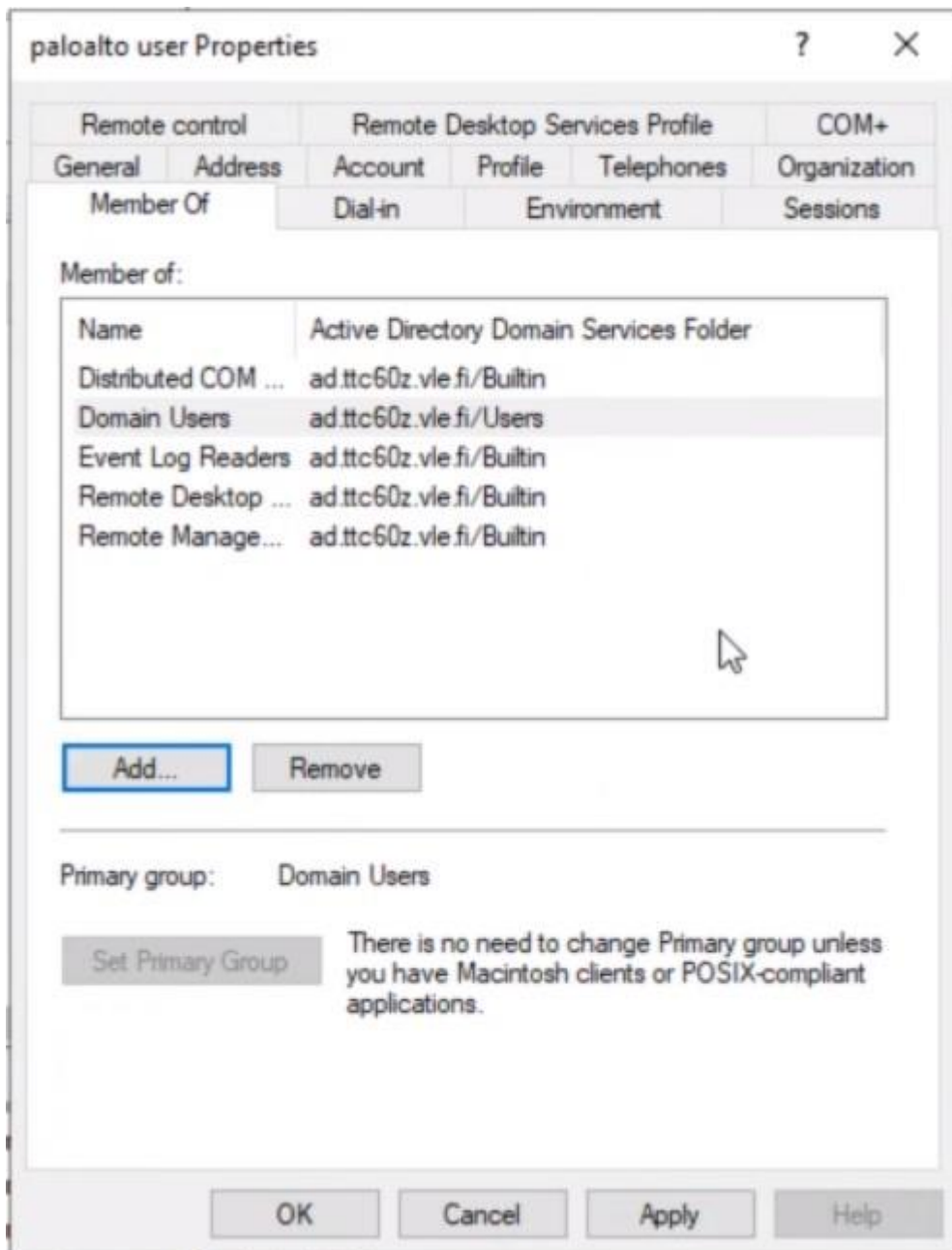
### 3.2 Active Directory Integraatio

Seuraavaksi aloimme integroimaan Palo Altoa AD:hen jolloin AD:sta saisi haettua ryhmät ja tunnukset. Vaihdoimme Service Routeen, LDAP:iin ja UID Agenttiin ethernet1/6.103, jolloin Palo Alto tietää mihin rajapintaan lähettää kyselyitä. Teimme uuden käyttäjä Managed Service Accountin alle (ks. Kuvio 9).



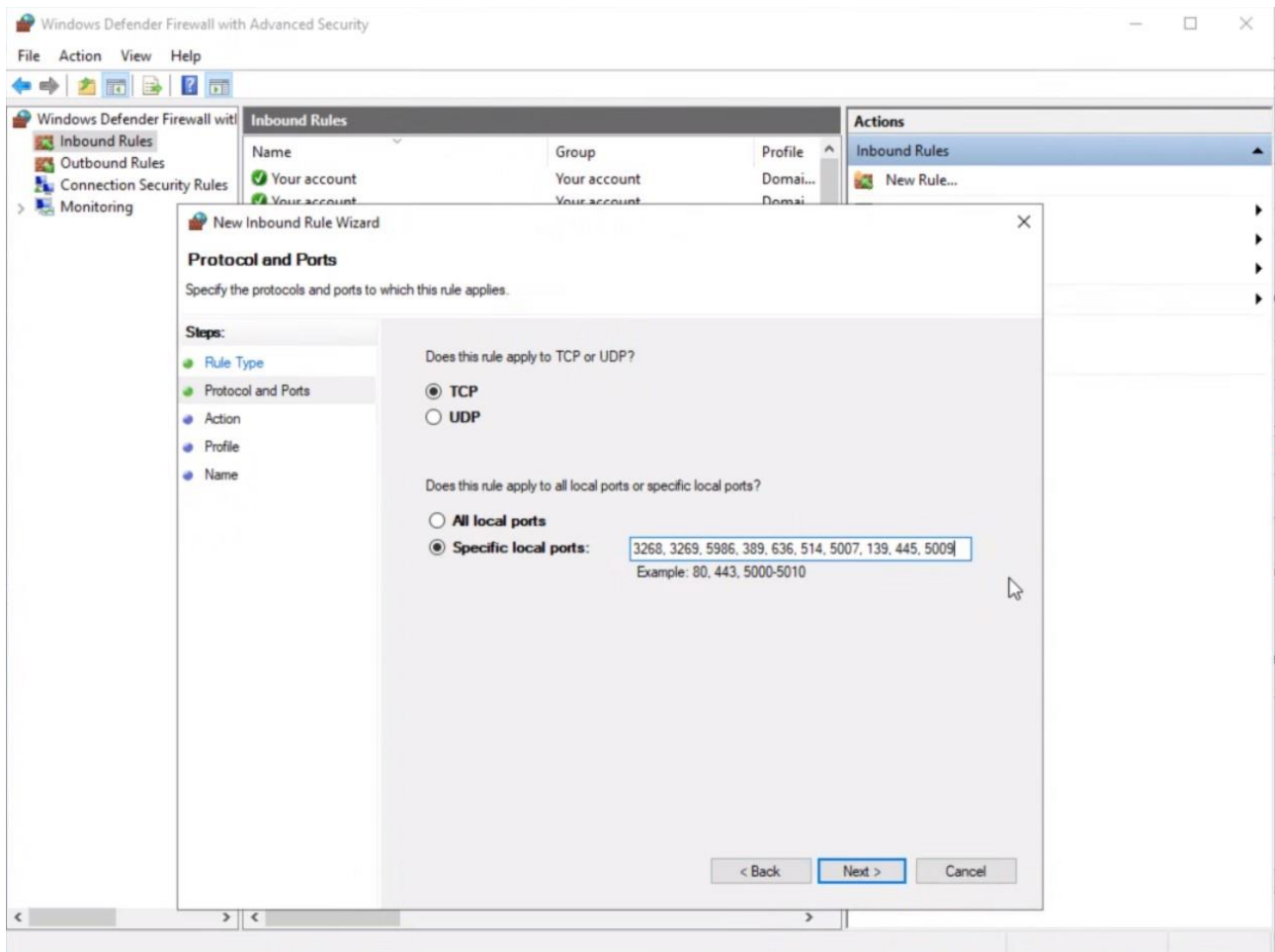
Kuvio 9. Uusi käyttäjä

Kävimme tässä vaiheessa lisäämässä uuden käyttäjän Event Log Readers, Distributed COM Users ja kolmeen muuhun ryhmään mitkä ohjeessa neuvottiin (ks. Kuvio 10).



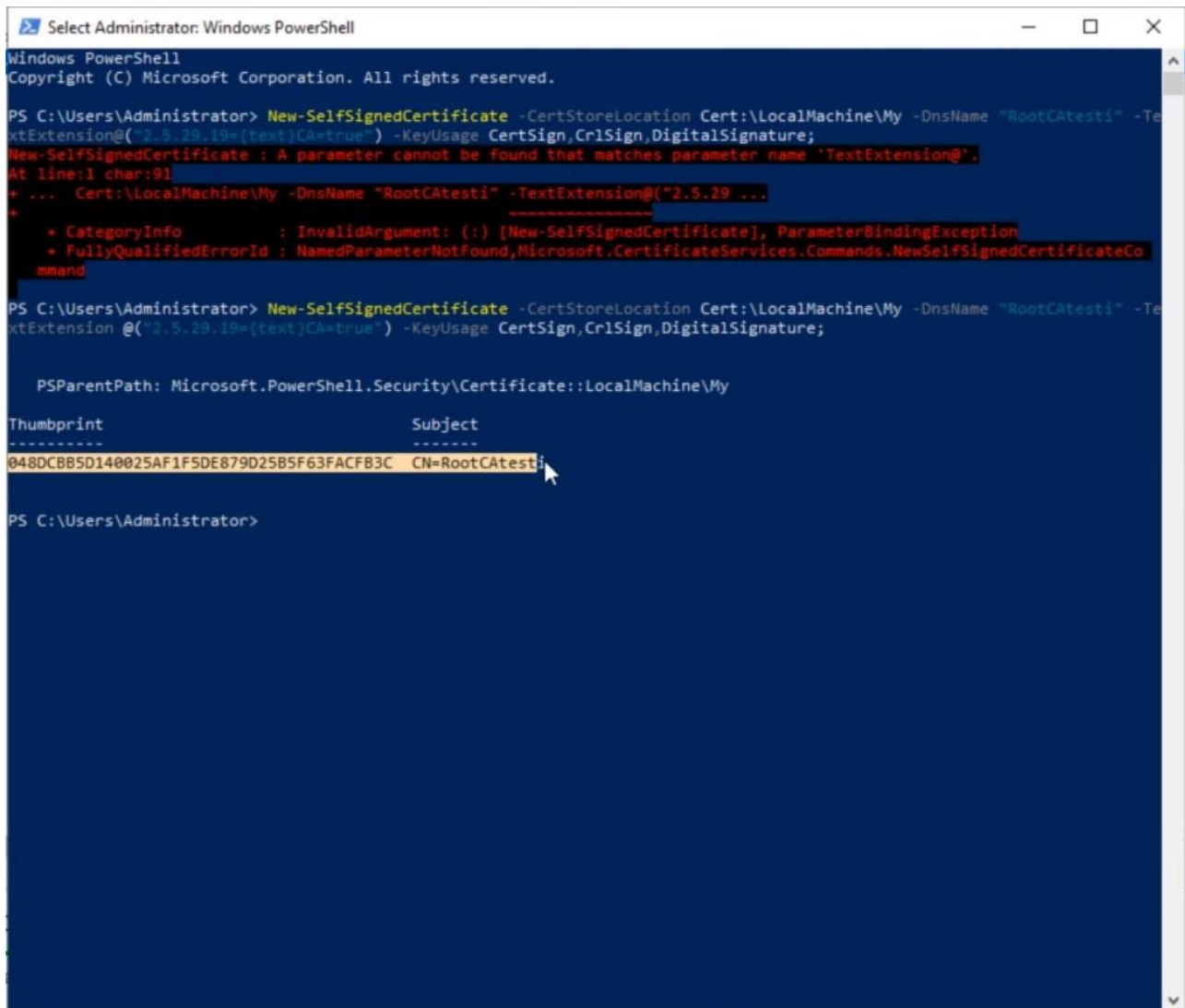
Kuvio 10. Ryhmät joihin uusi käyttäjä kuuluu

Siirryimme Windows Defender Firewalliin ja teimme uuden säännön nimeltä WINRM. Sallimme säännöstä portit, jotka mielestämme kuului sallia (ks. Kuvio 11). Emme lähteneet tutkimaan sallim- meko liikaa portteja koska toimi näillä.



Kuvio 11. Sallitut portit

WINRM-HTTPS:ää varten loimme itseallekirjoitetun sertifikaatin. Loimme sen ohjeessa annetulla käskyllä ja saimme thumbprintin (ks. Kuvio 12).



```

Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "RootCAtesti" -TextExtension@("2.5.29.19={text}CA=true") -KeyUsage CertSign,Cr1Sign,DigitalSignature;
New-SelfSignedCertificate : A parameter cannot be found that matches parameter name 'TextExtension@'.
At line:1 char:91
+ ... Cert:\LocalMachine\My -DnsName "RootCAtesti" -TextExtension@("2.5.29 ...
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [New-SelfSignedCertificate], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.CertificateServices.Commands.NewSelfSignedCertificateCommand

PS C:\Users\Administrator> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "RootCAtesti" -TextExtension @("2.5.29.19={text}CA=true") -KeyUsage CertSign,Cr1Sign,DigitalSignature;

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
048DCBB5D140025AF1F5DE879D25B5F63FACF83C CN=RootCAtesti

PS C:\Users\Administrator>

```

Kuvio 12. Thumbprint

Ajoimme seuraavat kolme käskyä ohjeen mukaan ja kaikki meni hyvin (ks. Kuvio 13). Jos ymmärsimme oikein, ensimmäinen käsky tekee WinRM-Listenerin HTTPS-protokollaa varten, joka käyttää aiemmin määriteltäviä sertifiikaattia. Toinen ja kolmas käsky sallii basic authenticationin clientille ja servicelle.

```

Administrator: Command Prompt
Thumbprint="048DCBB5D140025AF1F5DE879D25B5F63FACFB3C"}
ResourceCreated
  Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
  ReferenceParameters
    ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
  SelectorSet
    Selector: Address = *, Transport = HTTPS

C:\Users\Administrator>winrm set winrm/config/client/auth @{Basic="true"}
Auth
  Basic = true
  Digest = true
  Kerberos = true
  Negotiate = true
  Certificate = true
  CredSSP = false

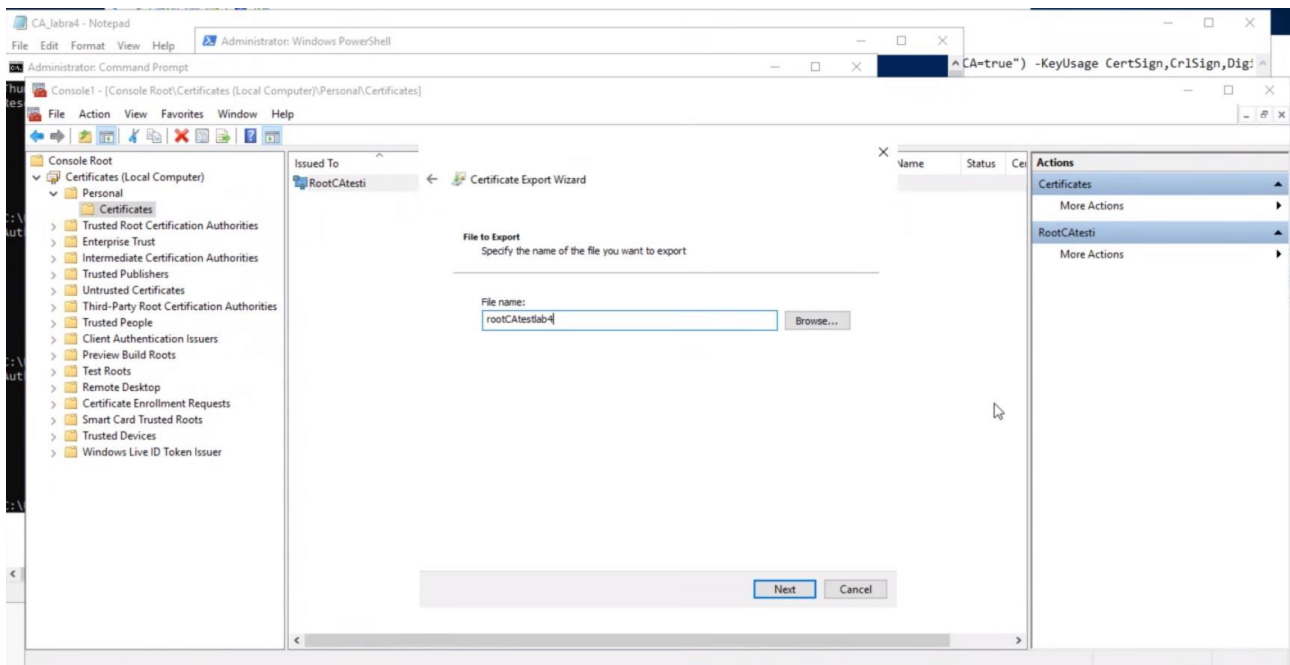
C:\Users\Administrator>winrm set winrm/config/service/auth @{Basic="true"}
Auth
  Basic = true
  Kerberos = true
  Negotiate = true
  Certificate = false
  CredSSP = false
  CbtHardeningLevel = Relaxed

C:\Users\Administrator>

```

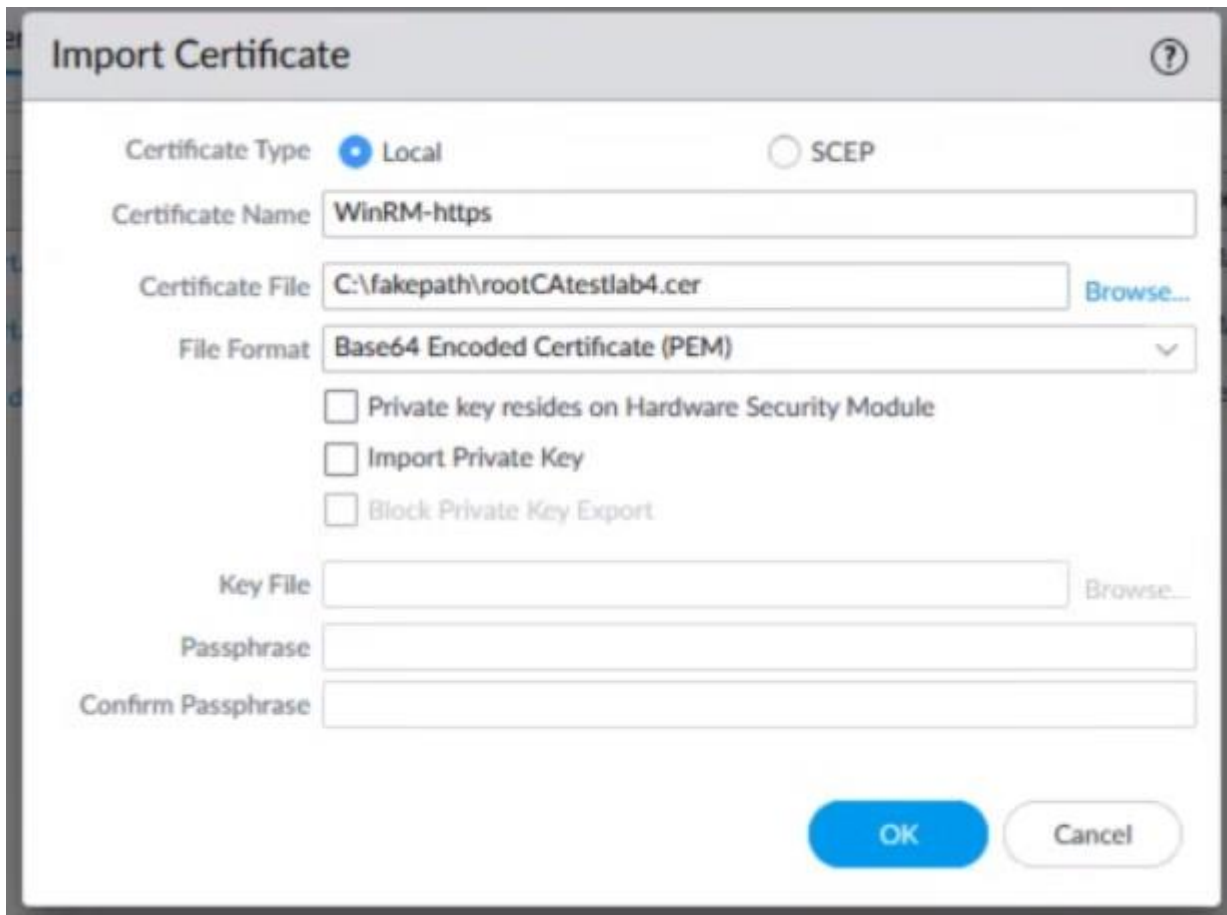
Kuvio 13. Kolme käskyä

Otimme sertifiikaatin ulos ja lisäsimme sen Palo Altoon (ks. Kuvio 14 ja Kuvio 15).



Kuvio 14. Sertifikaatti ulos





**Import Certificate**

Certificate Type: ☒ Local ☐ SCEP

Certificate Name: WinRM-https

Certificate File: C:\fakepath\rootCAtestlab4.cer [Browse...](#)

File Format: Base64 Encoded Certificate (PEM) [v](#)

☐ Private key resides on Hardware Security Module

☐ Import Private Key

☐ Block Private Key Export

Key File: [Browse...](#)

Passphrase:

Confirm Passphrase:

[OK](#) [Cancel](#)

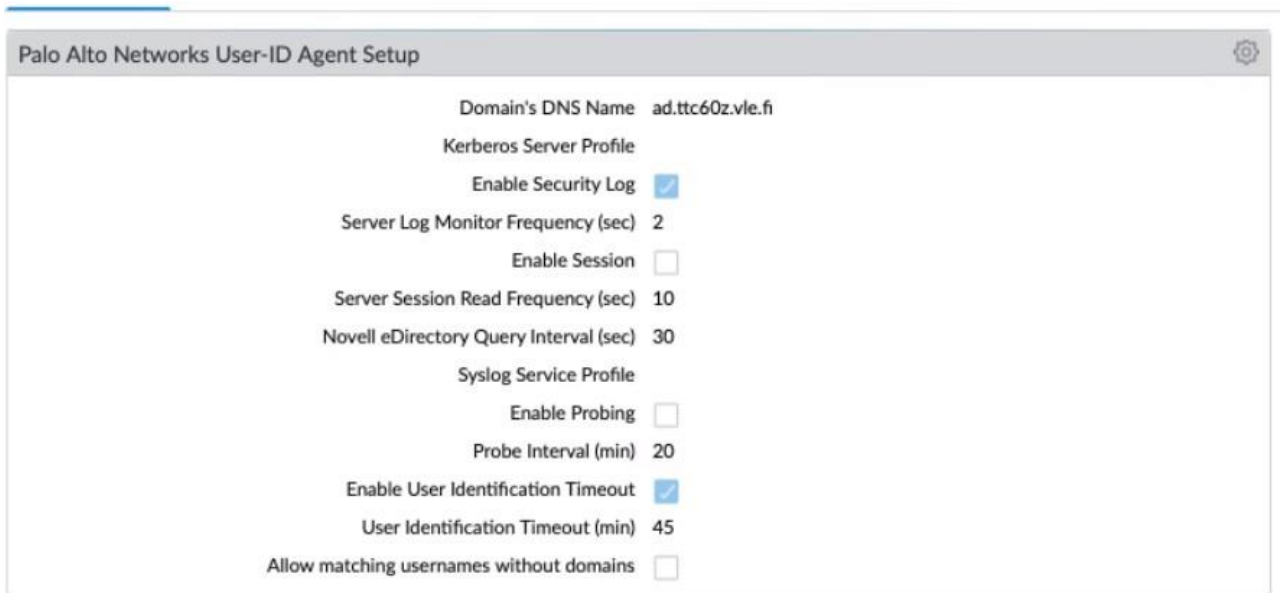
Kuvio 15. Sertifikaatti viety Palo Altoon

Teimme seuraavaksi LDAP Server Profilen. Annoimme nimen ja IP:n. Tyypiksi laitoimme active-directory ja otimme ruksin pois Require SSL/TLS secured connection kohdasta. Pudotus valikosta löysimme oikean Base DN:n (ks. Kuvio 16).

NAME	LOCATION	SERVICES	OTHERS
<input checked="" type="checkbox"/> dc01		Name: dc01 LDAP Server: 10.3.0.10 Port: 389	Type: active-directory Base: DC=ad,DC=ttc60z,DC=vle,DC=fi Bind DN: paloalto@ad.ttc60z.vle.fi

Kuvio 16. LDAP Server Profile

Siirryimme User Identification sivulle ja painoimme ruksia. Laitoimme käyttäjänimen oikeassa formatissa, Domain's DNS Nimen ja tunnuksen salasanat (ks. Kuvio 17).

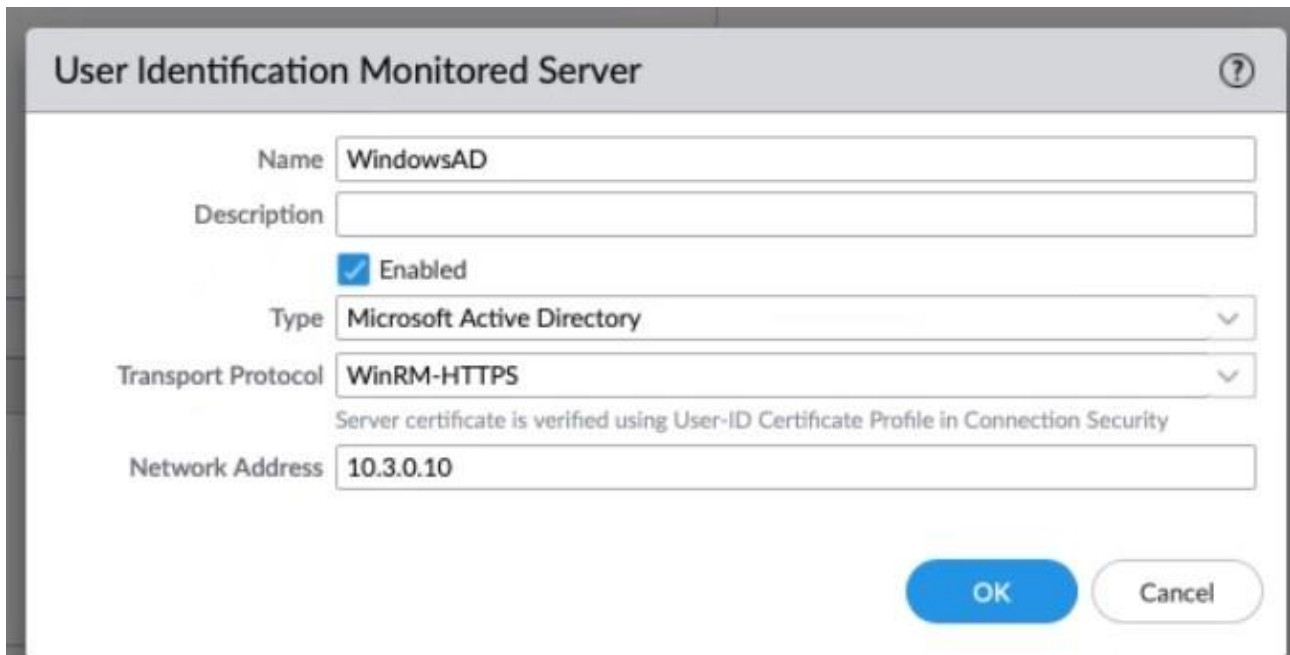


The screenshot shows the 'Palo Alto Networks User-ID Agent Setup' window. It contains the following configuration options:

- Domain's DNS Name: ad.ttc60z.vle.fi
- Kerberos Server Profile
  - Enable Security Log: ☒
  - Server Log Monitor Frequency (sec): 2
  - Enable Session: ☐
  - Server Session Read Frequency (sec): 10
  - Novell eDirectory Query Interval (sec): 30
- Syslog Service Profile
  - Enable Probing: ☐
  - Probe Interval (min): 20
- Enable User Identification Timeout: ☒
- User Identification Timeout (min): 45
- Allow matching usernames without domains: ☐

Kuvio 17. User-ID Agent

Server Monitoring kohdasta painoimme Add ja annoimme oikeat tiedot (ks. Kuvio 18).



User Identification Monitored Server

Name: WindowsAD

Description:

☒ Enabled

Type: Microsoft Active Directory

Transport Protocol: WinRM-HTTPS

Server certificate is verified using User-ID Certificate Profile in Connection Security

Network Address: 10.3.0.10

OK Cancel

Kuvio 18. Server Monitoring

Teimme vielä Certificate Profiiliin, jossa käytimme tuomaamme sertifikaattia ja asetimme profiilin käytettäväksi Connection Security välilehdellä (ks. Kuvio 19).

**Certificate Profile** ?

Name

Username Field

User Domain

CA Certificates

<input type="checkbox"/>	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
<input type="checkbox"/>	WinRM-https			

Default OCSP URL (must start with http:// or https://)

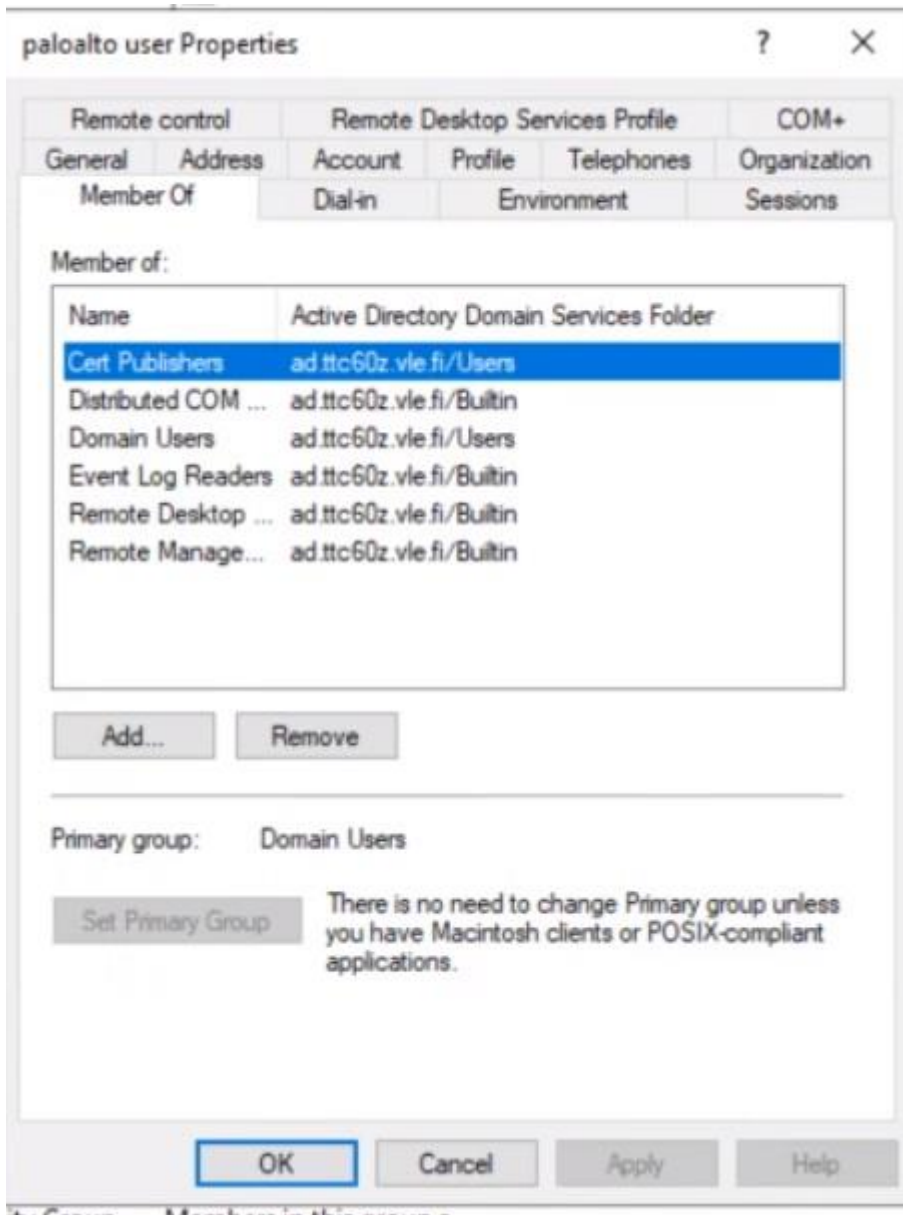
☐ Use CRL  
☐ Use OCSP  
OCSP takes precedence over CRL

CRL Receive Timeout (sec)   
OCSP Receive Timeout (sec)   
Certificate Status Timeout (sec)

☐ Block session if certificate status is unknown  
☐ Block session if certificate status cannot be retrieved within timeout  
☐ Block session if the certificate was not issued to the authenticating device  
☐ Block sessions with expired certificates

Kuvio 19. Certificate Profile

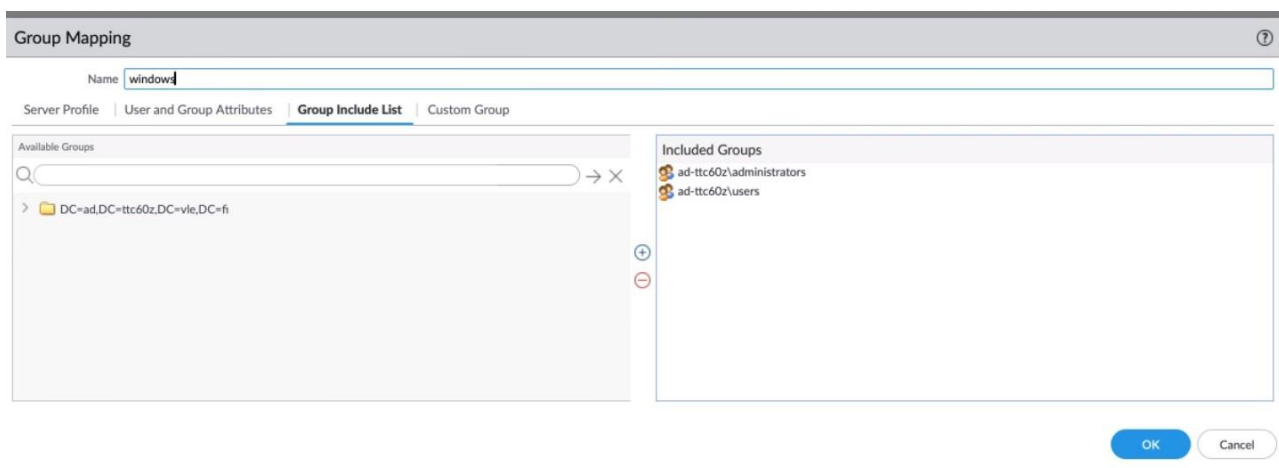
Ihmettä ei tapahtunut ja status oli Connection refused (0). Lähdimme tutkimaan asiaa ja ensin lisäsimme uuden käyttäjän Cert Publishers ryhmään (ks. Kuvio 20).



Kuvio 20. Uusi käyttäjä lisätty Cert Publishers ryhmään

Status pysyi Connection refused (0) tilassa ja tämän jälkeen lisäsimme uuden käyttäjän Cimv2:een oikeuksilla remote enabled ja enable account. Tämänkin jälkeen status pysyi Connection refused (0) tilassa ja ryhmä päätti jatkaa toisena päivänä labran tekoa. Yksi ryhmän jäsen kuitenkin kävi noin puolen tunnin päästä lopettamisesta palomuurilla ja huomasi että status oli muuttunut Connected tilaan, joten jompikumpi näistä asetuksista auttoi. Emme lähteneet sitä enempää tutkimaan, että kumpi.

Kun status oli Connected tilassa, jatkoimme labran tekoa. Menimme User Identification – Group Mapping Settings ja loimme uuden Group Mappingin. Server Profileen laitoimme dc01:n ja User Domain kohtaan piti lisätä ad-ttc60z viivalla eikä pisteellä niin kuin ohjeessa oli, jotta säännöt toimivat oikein. Nyt pystyimme lisäämään ryhmiä, joita halusimme käyttää (ks. Kuvio 21).



Kuvio 21. Group Mapping ryhmien lisäys

### 3.3 Testaaminen ja uudet säännöt sekä extra tehtävä

Testaamisessa käytimme seuraavia sääntöjä, jotka näkyvät alhaalla kuvassa (Ks. Kuvio 22). Kyseiset säännöt eivät olleet voimassa yhtäaikaisesti, kun testasimme että pääsemme domadminilla tai testiryhmässä olevalla käyttäjällä haluttuun lopputulokseen. Säännöissä sallimme tietyn käyttäjän tai ryhmän WS-NETistä VLE:hin, eli halusimme käyttää viime labrassa olleita sääntöjä hyväksi. Aluksi loimme säännön, jossa WS-NET:stä pääsee VLE:hen, ja valitsimme vain lähtökäyttäjäksi ad-ttc60z\domadmin, jonka olimme luoneet aikaisemmin. Kyseiseen sääntöön laitoimme edellisessä labrassa olleen Antivirus -säännön päälle, eli mentäessä esim. uhkapeli -sivustolle antaisi internet-selain varoituksen käyttäjälle kyseiselle sivustolle siirtymisestä. Toinen sääntö oli hyvin samanlainen, mutta tällä kertaa laitoimme lähtökäyttäjäksi ad-ttc60z\testiryhma, jolla pyrimme antamaan vaan kyseisessä ryhmässä oleville käyttäjille oikeudet sellaiseksi, ettei ole mitään url-filtteröintiä, antivirusa tai muutakaan lisäsuojauksia päällä. Yksi käyttäjä luotiin tähän kyseiseen ryhmään, joka

näkyä alhaalla (Ks. Kuvio 23).

Security

NAT

QoS

Policy Based Forwarding

Policy Based Forwarding Description

Tunneled Inspection

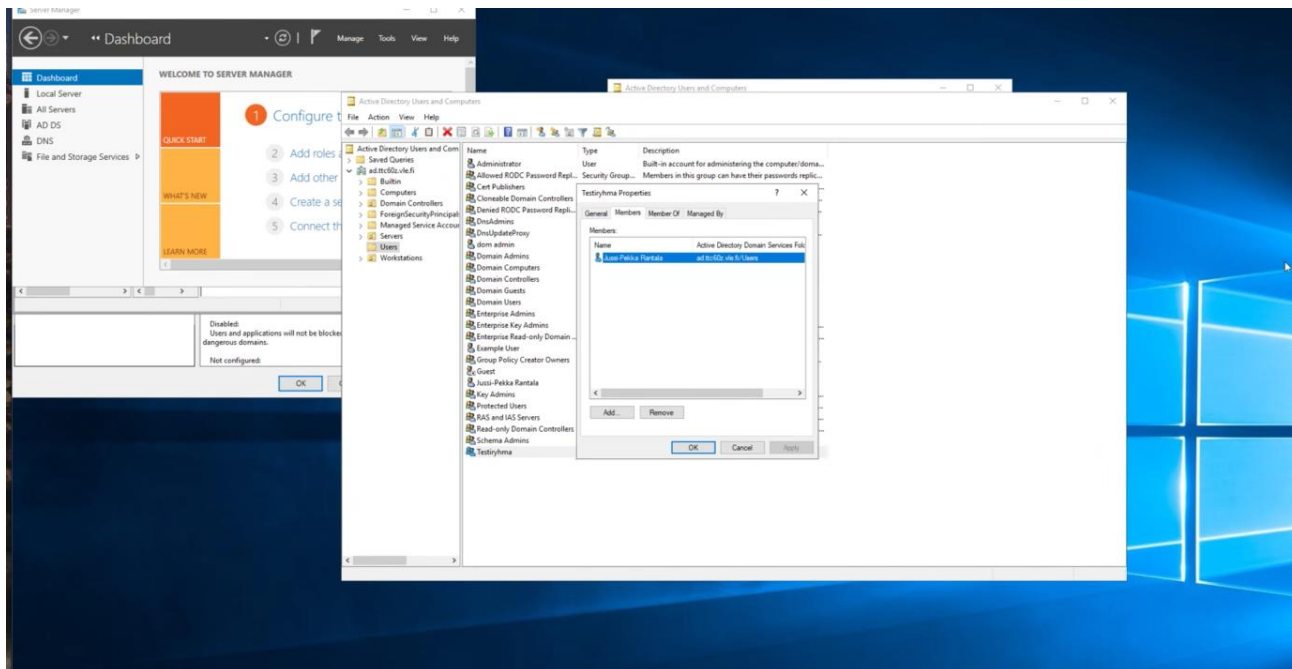
Application Overrule

Authentication

QoS Protection

SD-WAN

Kuvio 22. Policy säännöt

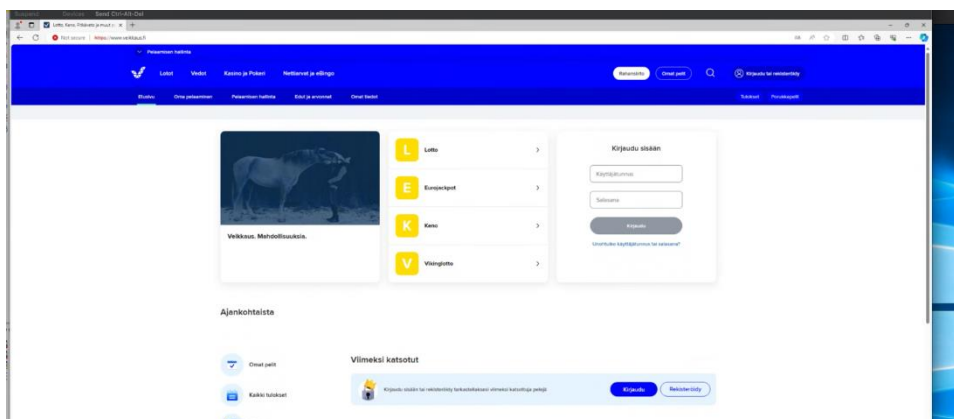


Kuvio 23. Uusi käyttäjä, joka linkitetty testiryhmään

Alla olevassa kuvassa (Ks. Kuvio 24) näkyy domadmin -käyttäjän pääsy WS01-koneelta nettiin, ja näkyy, että olemme päässeet uhkapelisivustolle (Ks. Kuvio 25), ja kuten url-osoitteen kohdassa huomataan, niin se on varoittanut meitä siirtymästä kyseiselle sivustolle. Varoitus -kohdasta unohdimme ottaa kuvan.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP CONN SESS
	02/18 18:46:31	end	SERVERS-NET	VLE	10.3.0.10			205.251.196.173			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	471	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		10.10.0.103			7680	incomplete	allow	WS-NET-TO-VLE-ANY	aged-out	70	0
	02/18 18:46:26	end	ADMIN-NET	VLE	10.2.0.13			34.117.237.239			443	ssl	allow	GATEWAY-TO-VLE	tcp-fin	4.6k	0
	02/18 18:46:26	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	224	0
	02/18 18:46:26	end	ADMIN-NET	VLE	10.2.0.10			198.18.100.4			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	218	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		142.250.74.65			443	google-base	allow	WS-NET-TO-VLE-ANY	tcp-fin	12.6k	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		104.18.28.86			443	ssl	allow	WS-NET-TO-VLE-ANY	tcp-fin	8.3k	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		104.18.28.86			443	ssl	allow	WS-NET-TO-VLE-ANY	tcp-fin	8.3k	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		104.18.28.86			443	ssl	allow	WS-NET-TO-VLE-ANY	tcp-fin	8.4k	0
	02/18 18:46:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		104.18.28.86			443	ssl	allow	WS-NET-TO-VLE-ANY	tcp-fin	8.3k	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			205.251.193.111			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	267	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			205.251.193.111			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	342	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			205.251.198.237			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	471	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			192.52.178.30			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	812	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			192.52.178.30			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	812	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			161.232.12.6			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	831	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			192.203.230.10			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	903	0
	02/18 18:46:26	end	SERVERS-NET	VLE	10.3.0.10			96.7.49.66			53	dns-base	allow	GATEWAY-TO-VLE	aged-out	210	0
	02/18 18:46:21	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		142.250.74.98			443	google-base	allow	WS-NET-TO-VLE-ANY	tcp-fin	41.9k	0
	02/18 18:46:21	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\domadmin		142.250.74.110			443	youtube-base	allow	WS-NET-TO-VLE-ANY	tcp-fin	13.2k	0

Kuvio 24. Domadmin -käyttäjä



Kuvio 25. Veikkaus -sivu varoituksella

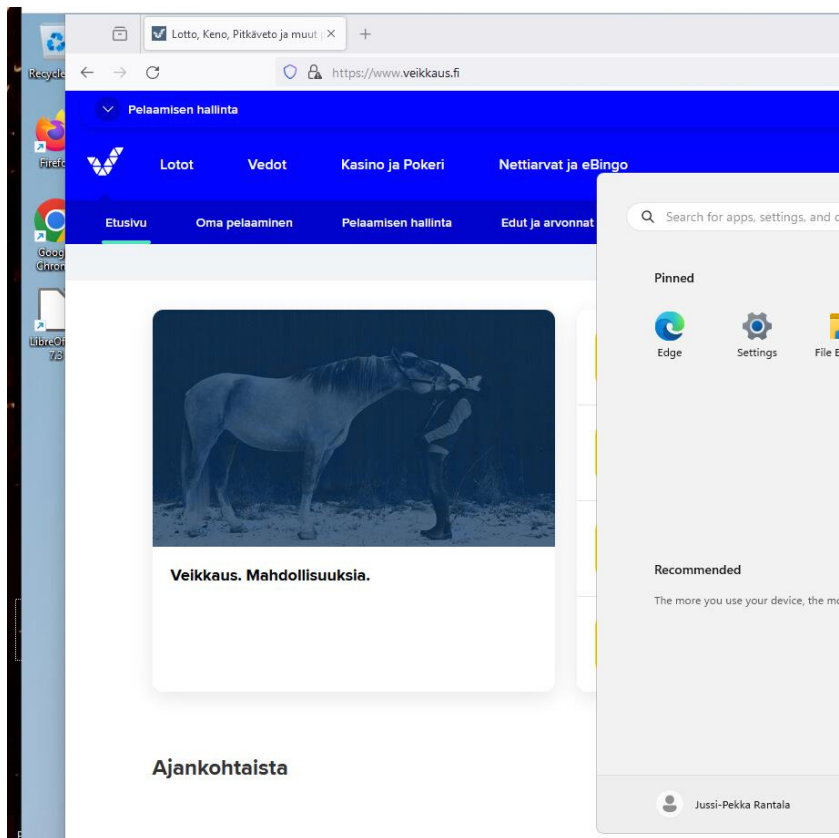
Testiryhmässä olevan käyttäjän eli Jussi-Pekka.Rantala testauksessa policy antoi mennä suoraan kaikille mahdollisille sivuille, joista alhaalla kuvat (Ks. Kuvio 26 ja Kuvio 27). Kyseisen säännön kanssa oli aluksi haasteita, joita pohdinnassakin käydään läpi ja tämä liittyi luomaamme Group Mappin Settingissä olevaan User Domain –kohtaan, jossa aluksi oli ad.ttc60z, jolla emme saaneet



sääntöä toimimaan, mutta opettajan ohjauksella, kun vaihdoimme sen ad-ttc60z niin sääntö rupesi toimimaan kuten pitikin.

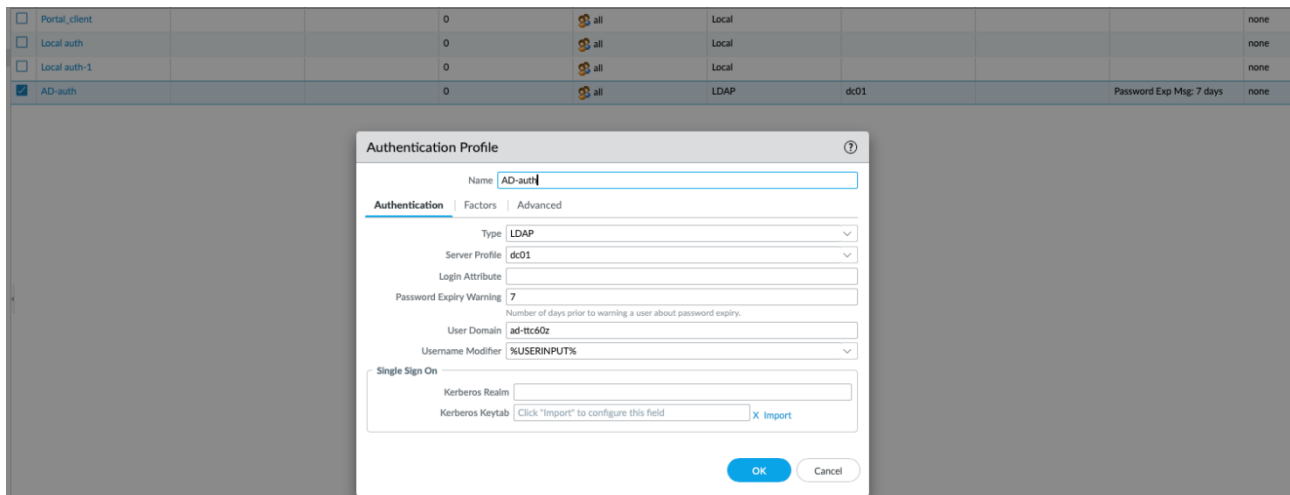
02/26 18:33:44	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\jussi-pekka.rantala	52.85.49.11	443	web-browsing	allow	WS-NET-TO-VLE-WEB-spe_group_testiryhma
02/26 18:33:44	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\jussi-pekka.rantala	52.85.49.11	443	web-browsing	allow	WS-NET-TO-VLE-WEB-spe_group_testiryhma
02/26 18:33:44	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\jussi-pekka.rantala	52.85.49.11	443	web-browsing	allow	WS-NET-TO-VLE-WEB-spe_group_testiryhma

Kuvio 26. Testiryhma -monitorlehdellä



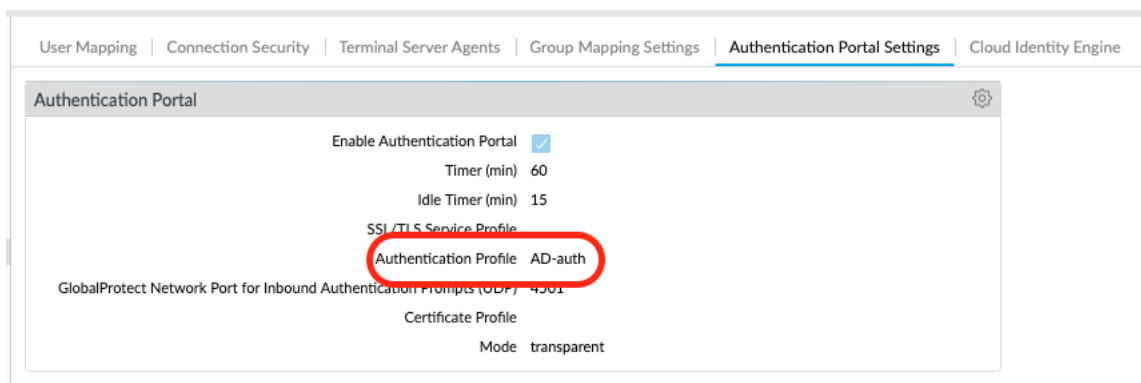
Kuvio 27. Veikkaus ilman varoitusta

Extra tehtävässä pitää tunnistautumista muuttaa siten, että AD-käyttäjä pystyy tunnistautumaan omalla käyttäjänimellä ja salasanalla. Luodaan uusi authentication profile nimeltään AD-auth. Asetuksiin valitaan LDAP tyyppi ja dc01 palvelimen profiiliksi (ks. Kuvio 28).



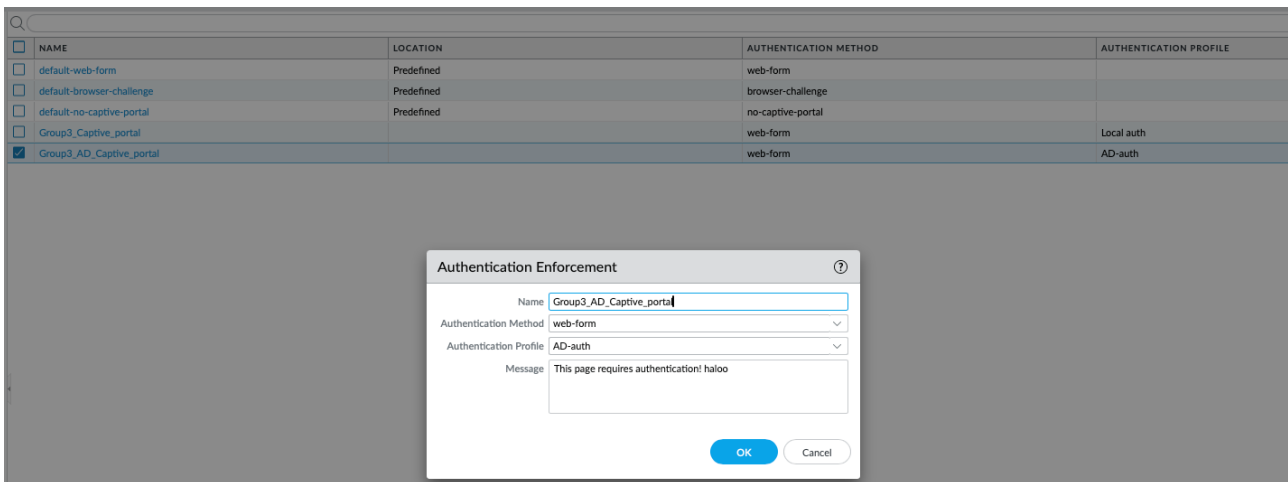
Kuvio 28. Luodaan uusi profiili

Vaihdetaan asetuksissa uusi profiili käyttöön (ks. Kuvio 29).



Kuvio 29. Otetaan uusi profiili käyttöön

Seuraavaksi luodaan uusi captive portal autentikaatio ja valitaan tähän äsken luotu uusi AD-auth profiili (ks. Kuvio 30).



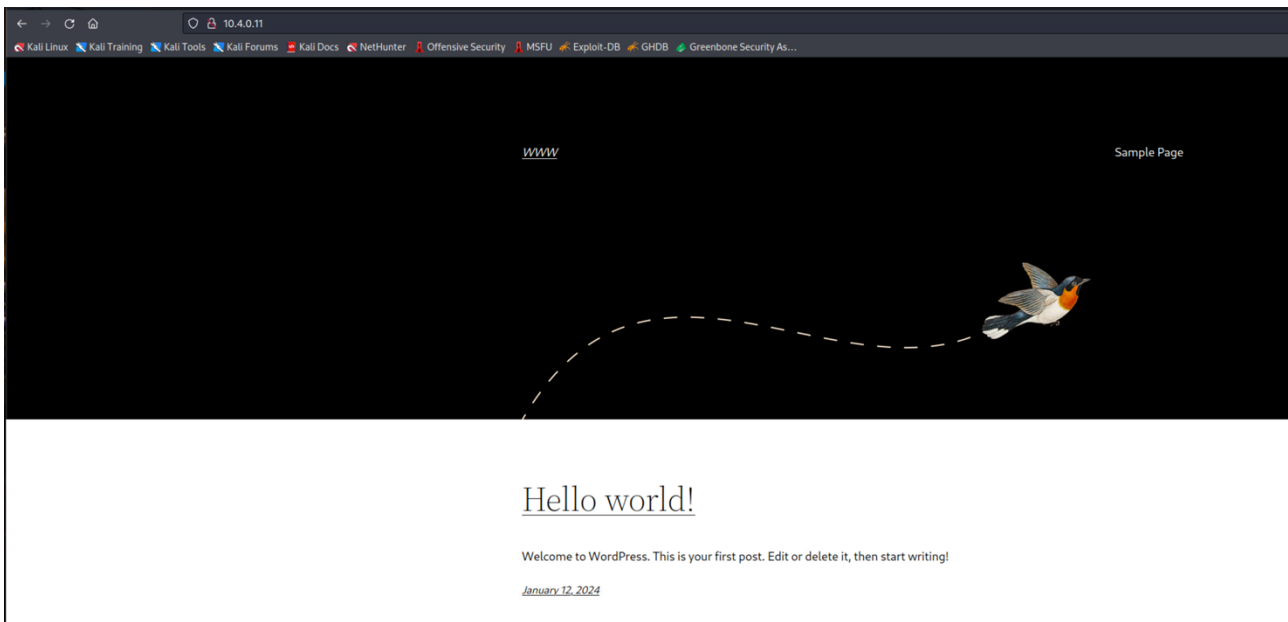
Kuvio 30. Luodaan uusi captive portal

Vaihdetaan authentication välilehdellä olevaan sääntöön uusi captive portal (ks. Kuvio 31)

	NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	DMZ_protection	none	ADMIN-NET WS-NET	any	unknown	any	DMZ	any	any	service-http	Group3_AD_Captive_p...	
2	DMZ_protection-AD	none	ADMIN-NET WS-NET	any	any	any	DMZ	any	any	service-http service-https	Group3_AD_Captive_portal	

Kuvio 31. Päivitetään autentikaatio sääntö

Todennus. Kirjaututaan dom admin käyttäjänä ja todetaan että autentikaatio toimii oikein, koska palomuurin loki:lta nähdään, että dom admin käyttäjätunnukset autentikoidaan DC01-palvelimella ja selaimelle avautuu oletusnäkö (ks. Kuvio 32 ja Kuvio 33).



Kuvio 32. Oletus sivuille päästään

RECEIVE TIME	IP ADDRESS	USER	NORMALIZED USER	GENERATE TIME	VENDOR	OBJECT	SERVER PROFILE	TYPE	SUBTYPE	RULE	EVENT	DESCRIPTION	AUTHENTICATI... PROTOCOL
02/19 16:32:48	10.2.0.13	domadmin	ad-ttc60z\domadmin	02/19 16:32:48		AD-auth	dc01	Authentication Portal	LDAP	DMZ_protection	Authentication Success	server address '10.3.0.10'	

Kuvio 33. Näkymä palomuurin loki:sta

## 4 Pohdinta

Labra eteni hyvää vauhtia aina Server Monitoring kohtaan, jolloin tuli ensimmäinen este. Status oli Connection refused (0) tilassa ja se ratkesi lisäämällä uusi käyttäjä Cert Publishers ryhmään ja/tai Cimv2:een. Emme tutkineet kumpi ratkaisi asian vai pitikö molemmat tehdä. Mietimme myös aiemmin sallittuja portteja, että mitkä kaikki niistä pitää olla sallitussa tilassa ja mitkä eivät.

Lopussa tuli vielä pari ongelmaan. Teimme säännön, joka sallii nyt tietyn AD-ryhmän käyttäjien pääsyn Ylen sivuille mutta monitoring välilehdeltä näimme, että säännön yli hypättiin. Pohdimme tätä opettajan kanssa ja löysimme ratkaisun Group Mapping Settingeistä. Olimme laittaneet User Domain kohtaan ad.ttc60z ja vaihdoimme sen ad-ttc60z:aan jolloin sääntö alkoi toimimaan eikä

sen yli enää hypätty. Viimeinen ”ongelma” tuli säätäessä AD-tunnuksia toimimaan tunnistautumisessa. Yritimme kirjautua käyttäjällä, jonka olimme laittaneet tätä varten tehtyyn sääntöön ja vastaan tuli Unable to connect sivu. Tämä ratkesi tyhjentämällä sivuhistorian ja käynnistämällä selaimen uudestaan, jolloin monitoring sivulla näkyi onnistunut kirjautuminen.

Labra oli mielestämme mielenkiintoinen ja opetti paljon. Varsinkin AD-integraation tekeminen oli mieluisaa ja Palo Alton käyttöjärjestelmä alkaa tulla tutummaksi mitä pidemmälle etenemme kursilla.

## Lähteet

Blanton S. 2023. What Is LDAP Authentication?. Artikkel- sivustolla jumpcloud. Viitattu 24.2.2024. <https://jumpcloud.com/blog/what-is-ldap-authentication>

Enable User- and Group-Based Policy. 2024, Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/enable-user-and-group-based-policy#id8d92ab06-b513-4120-a463-2c5b5cf3b6de>

External Authentication Services. 2024. Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/authentication-types/external-authentication-services#id49b22330-2e18-4007-9cdd-643fd1e13743>

Gillis A.S. 2022. LDAP (Lightweight Directory Access Protocol). Artikkel- TechTarget. Viitattu 24.2.2024. <https://www.techtarget.com/searchmobilecomputing/definition/LDAP>

LDAP. 2024. Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024 <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/authentication-types/ldap#id9b2c506d-7319-4b39-894d-773ec210d587>

Local Authentication. 2024. Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/authentication-types/local-authentication>

Map IP Addresses to Usernames Using Authentication Portal. 2024. Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal>

Map Users to Groups. 2024. Artikkel- Paloalto TECHDOCS. Viitattu 24.2.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/map-users-to-groups#id44a39121-660d-4197-abe7-26c897b64e7e>

User-ID Overview. 2023. Viitattu 21.2.2024. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-overview>