



Labra 4

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

Palautuspvm

Tieto- ja viestintätekniikka

Sisältö

1	Johdanto.....	4
2	Teoria.....	4
3	Toteutus	6
3.1	Active Directory Integrointi.....	13
3.2	Testaaminen.....	27
4	Pohdinta	33
	Lähteet	35

Kuviot

Kuvio 1.	Snapshot alkutilanteesta.....	6
Kuvio 2.	Users	7
Kuvio 3.	Authentication profile.....	7
Kuvio 4.	Authentication profile advanced	8
Kuvio 5.	Authentication portal	8
Kuvio 6.	Authentication Enforcement.....	9
Kuvio 7.	Authentication policy.....	10
Kuvio 8.	Turvallisuussääntö WS-NET + ADMIN-NET -> DMZ	10
Kuvio 9.	Kalin hosts-tiedosto	10
Kuvio 10.	Captive Portal kirjautuminen	11
Kuvio 11.	Hello world	11
Kuvio 12.	Monitor	12
Kuvio 13.	Rajapinnan asettaminen	13
Kuvio 14.	Rajapinnan asettaminen 2	14
Kuvio 15.	Uuden käyttäjän luonti	14
Kuvio 16.	Uuden käyttäjän luonti 2	15
Kuvio 17.	Ryhmien lisäys3	16
Kuvio 18.	UDP-porttien salliminen.....	17
Kuvio 19.	Porttien salliminen tcp	17
Kuvio 20.	Allekirjoitettu sertifikaatti	18

Kuvio 21. WinRM 1.....	18
Kuvio 22. WinRM 2.....	19
Kuvio 23. Sertifikaatin vienti.....	19
Kuvio 24. Sertifikaatin vienti onnistui	20
Kuvio 25. Sertifikaatin tuonti	21
Kuvio 26. LDAP-profiili.....	22
Kuvio 27. User-ID agentin asetukset.....	22
Kuvio 28. Monitored server	23
Kuvio 29. CIMV2-asetukset	24
Kuvio 30. Advanced-välilehti	24
Kuvio 31. Yhteys avattu	25
Kuvio 32. User Mapping	25
Kuvio 33. Virheviesti.....	26
Kuvio 34. Käytön estänyt GPO	26
Kuvio 35. group mapping	27
Kuvio 36. Boross YouTubessa	27
Kuvio 37. Autentikointiprofiili ad_auth.....	28
Kuvio 38. Autentikointiprofiilin vaihto	28
Kuvio 39. Captive Portalin profiilin vaihto.....	29
Kuvio 40. Monitor MaMyyjä.....	29
Kuvio 41. Hyväksytyjen käyttäjien lisääminen turvallisuuspolitiikkaan	29
Kuvio 42. Matti Myyjä verkossa.....	30
Kuvio 43. Käyttäjryhmän lisääminen turvallisuuspolitiikkaan.....	31
Kuvio 44. Hanna HR verkossa.	31
Kuvio 45. Captive portal Kalilla lopussa	32
Kuvio 46. Bob Ross verkossa	32
Kuvio 47. Boross-käyttäjä monitorissa.....	33

1 Johdanto

Tietoturvakontrollit labrassa 4 (Paloalto User-ID) parannetaan palomuurin läpi kulkevan liikenteen tunnistamista ja seurantaan. User-ID sääntöjen avulla voidaan tehdä tarkempia, käyttäjäkohtaisia turvallisuussääntöjä, joiden avulla esimerkiksi lokitiedoista nähdään IP osoitteen lisäksi kirjautunut käyttäjätunnus. Seurannan tarkentaminen auttaa ymmärtämään paremmin hallintaympäristöä ja tapahtuneiden ongelmien jäljittämistä. Labra 4:n tavoitteena on siis varmistaa vain tiettyjen käyttäjien pääsyn meidän [www-sivuillemme](http://www.sivuillemme).

Tavoitteena on myös saada PaloAlton ja Windows Active Directoryn välille yhteys, jotta Windows käyttäjä- ja ryhmätiedot saadaan suoraan palomuurin asetuksiin. AD:n ja PaloAlton integrointi on suhteellisen haastava homma, mutta sen seurauksena nykyiset käyttäjätiedot, ja tietojen muutokset saadaan jatkossa päivittymään palomuuriin. Tätä ennen tehdään sääntö PaloAltoon Captive Portalin avulla tunnistautuville käyttäjille, jotta heidän toimintaansa saadaan seurattua, näin voidaan testata käyttäjäkohtaisten politiikoiden toimintaa käytännössä.

2 Teoria

Palomuurin liikenteen seurannassa on olennaista saada mahdollisimman paljon tietoa siitä, mitä on tehty, miltä laitteelta ja kuka on tehnyt. Varsinkin, kun tiedetään tekijä, on paljon helpompaa lähteä selvittämään asetuksia tai toimintoja, jotka ovat johtaneet vaikkapa haittaohjelmien tai viruksien pääsyn omaan sisäverkkoon. Näin on helpompaa selvittää, onko hakkerit päässeet käyttäjätietoihin käsiksi. Tarvittaessa voidaan kysyä käyttäjätunnuksen haltijalta, oliko hän kirjautuneena lokitietojen näyttämään aikaan ja esimerkiksi onko hänen omat konfigurointinsa menneet metseen. Edellisessä labrassa tehdyillä estosäännöillä ja varoituksilla, esimerkiksi tarpeettomat nettisivut voitaisiin estää/sallia käyttäjäkohtaisesti tai ryhmäkohtaisesti, jotka muille käyttäjille olisivat vapaasti käytettävissä.

Ennen Active Directoryn integrointia tulee testata käyttäjäkohtaisten sääntöjen toimintaa Palo Alto Local Database Authentication toiminnon avulla. Palomuurin omaan tietokantaan voidaan siis

lisätä käyttäjiä tai ryhmiä, joilta vaaditaan tunnistautuminen nettisivuille. Näin käyttäjien toimintaa sivuilla voidaan monitoroida tarkemmin palomuurilla. Paikallisten käyttäjien tunnistamisen saadaan aikaiseksi autentikointi profiilin avulla, joka liitetään Captive Portal kirjautumiseen. Käyttäjä "TestUser" sallitaan myös turvallisuus säännöissä, jotta pääsee sivuille (Admin-net, WS-net -> DMZ) ja kirjautumaan.

Active Directoryn liittäminen Palo Altoon tapahtuu DC:n avulla. Palo Alto tarvitsee yhteyden Active Directoryyn, jotta se voi käyttää käyttäjätietoja ja päivittää niitä. **LDAP (Lightweight Directory Access Protocol)** avulla saadaan verkon yli pääsy AD:n tietoihin palomuurilta. Sen avulla Palo Alto pääsee hakemaan käyttäjä- ja ryhmätietoja Active Directorystä, näin käyttäjä- tai ryhmäkohtaisia sääntöjä voidaan asettaa palomuuriin, esimerkiksi rajaten muiden käyttäjien kuin haluttujen pääsyn johonkin sovellukseen tai nettisivuun. Labrassa palomuuri liitetään LDAP palvelimeen (dc01), josta AD tiedot saadaan palomuurille. Windows päässä tulee myös sallia Windows Firewall asetuksista portit, joita esim. LDAP ja WinRM vaativat yhteyden muodostamiseen.

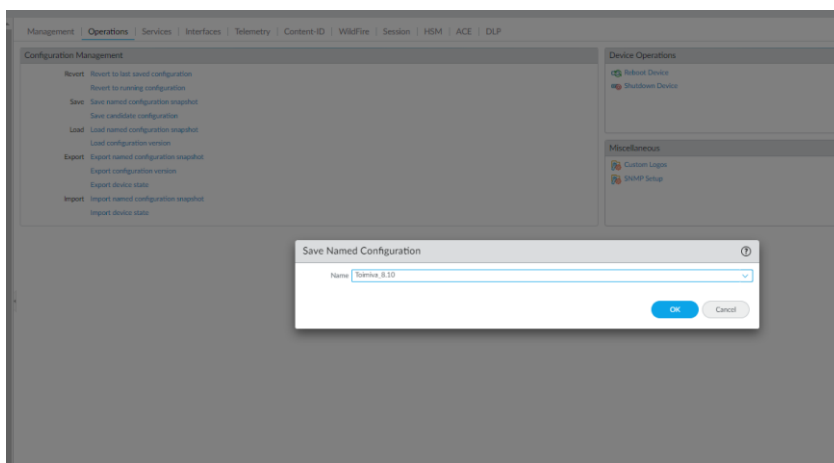
WinRM (Windows Remote Management) on Microsoft protokolla, jolla voidaan hallita ja valvoa Windows- järjestelmää. Sen avulla saadaan etäyhteys AD:n ja muiden palveluiden etähallintaan, se ei kuitenkaan liity suoraan hakemistopalveluun (AD), vaan nimenomaan turvallisen yhteyden muodostamiseen. **WinRM** tarvitsee sertifikaatit, Windows – Palo Alto välisen yhteyden salaamiseksi. Tässä labrassa **WinRM** käyttää HTTPS:ää, jonka avulla palomuuri ja palvelin saadaan yhdistettyä salatun tunnelin sisällä (SSL). Palomuuri siirtää AD:n tunnistetiedot (käyttäjänimi ja salasana) SSL-tunnelissa. (Configure Server Monitoring Using WinRM. 2024)

User-ID on Palo Alto palomuurin ominaisuus, jonka avulla voidaan tunnistaa käyttäjät verkkoympäristössä eri menetelmien avulla. Tämän avulla käyttäjien toimia voidaan seurata verkon eri sijainneissa ja monilla eri käyttöjärjestelmillä. Active Directoryn integroinnissa User-ID kerää ja käyttää AD:n käyttäjätietoja, kuten käyttäjänimiä ja ryhmiä. (User-ID Overview. 2024)

User-ID mahdollistaa käyttäjäkohtaiset politiikat palomuurissa, joilla voidaan rajata tiettyjen käyttäjien pääsyä sovelluksiin tai palveluihin. Se auttaa myös lokituksessa ja forensiikassa, jos on tapahtunut kyberhyökkäys organisaatiota kohtaan tai haittaohjelmia on päätyntä verkon laitteille, saadaan helpommin selville mitä on tapahtunut etsimällä epäilyttäviä toimintoja lokitiedoista. (User-ID Overview. 2024). User-ID vaatii myös erikseen luodun Service-profiilin, jonka avulla voidaan kerätä ja käsitellä käyttäjätietoja, jotka perustuvat tietoturvalokeihin. (Create a dedicated Service Account for the User-ID Agent. 2024)

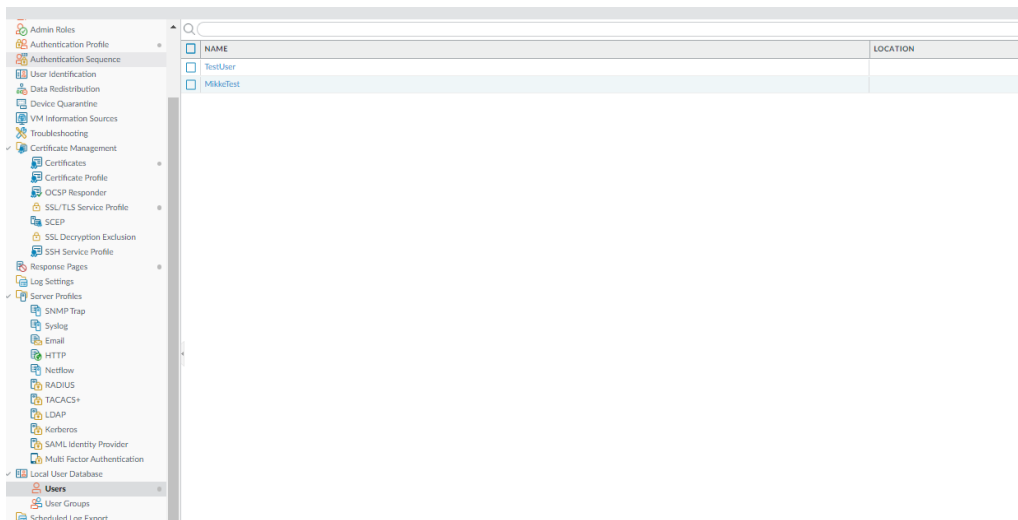
3 Toteutus

Otimme aluksi snapshotin alkutilanteesta, jotta voimme palata toimivaan asetelmaan, mikäli jokin menee vikaan. (Kuvio 1)



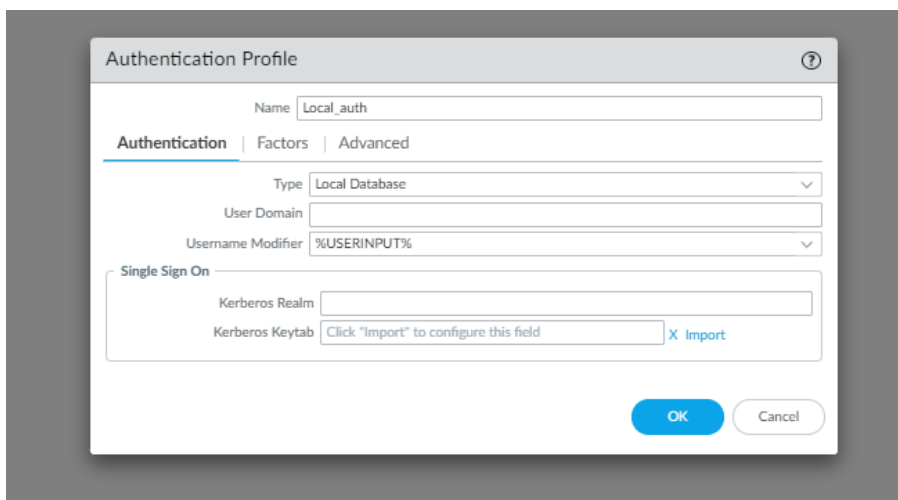
Kuvio 1. Snapshot alkutilanteesta

Emme luoneet aluksi uusia käyttäjiä vaan käytimme testaukseen aiemmassa harjoituksessa luotua TestUser tiliä. (Kuvio 2)



Kuvio 2. Users

Loimme uuden autentikointiprofiilin palomuurin oman käyttäjätietokannan (Local Database) käyttäjien todentamista varten, kuten aiemmin luotu TestUser.



Kuvio 3. Authentication profile

Advanced välilehdellä lisäsimme hyväksytyihin käyttäjiin all, eli kaikki paikallisen tietokannan käyttäjät sallitaan. (Kuvio 4)

Authentication Profile

Name: Local_auth

Authentication | Factors | **Advanced**

Allow List

☐ ALLOW LIST ^

☒ all

+ Add - Delete

Account Lockout

Failed Attempts: [0 - 10]

Lockout Time (min): 0

OK Cancel

Kuvio 4. Authentication profile advanced

Muokkasimme User Identification -välilehdeä autentikointi portaalin asetuksia, jotta paikalliset käyttäjät voivat tunnistautua. (Kuvio 5)

User Mapping | Connection Security | Terminal Server Agents | Group Mapping Settings | **Authentication Portal Settings** | Cloud Identity Engine

Authentication Portal

Enable Authentication Portal ☒

Timer (min): 60

Idle Timer (min): 15

SSL/TLS Service Profile: None

GlobalProtect Network Port for Inbound Authentication Prompts (UDP): 4501

Authentication Profile: **Local_auth**

Mode: ☒ Transparent ☐ Redirect

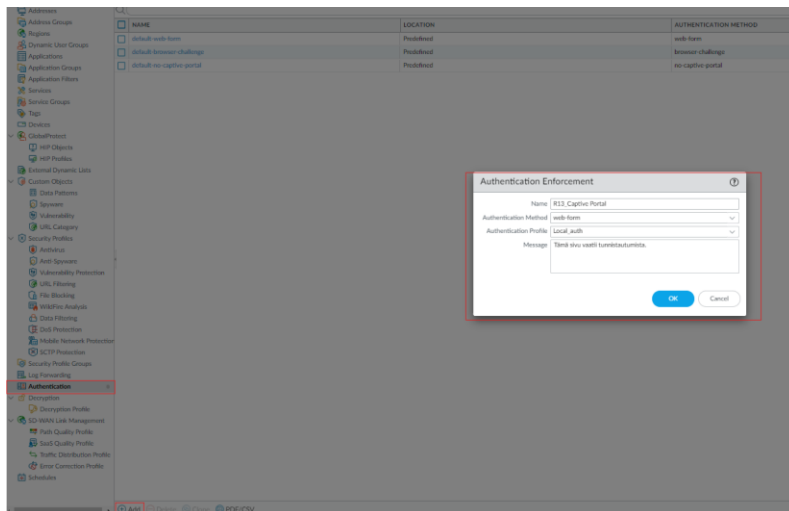
Certificate Authentication

Certificate Profile: None

OK Cancel

Kuvio 5. Authentication portal

Objects-välilehden authentication osiossa loimme uuden tunnistautumistavan. Tähän valitsimme Authentication profile -kohtaan aiemmin tehdyn Local_auth -profiilin. Authentication method kohta määrittelee itse tunnistautumistavan, tähän valitsimme web-form eli kirjautumislomake. (Kuvio 6).



Kuvio 6. Authentication Enforcement

Siirryimme Policies-välilehdelle Authentication-osioon. Loimme sinne uuden politiikan nimeltä DMZ suojaus. Kuvion 7 mukaisesti määrittelimme, että tunnistautumista pyydetään tuntemattomilta käyttäjiltä ja heidät ohjataan tunnistautumaan erillisellä lomakkeella (Captive Portal).

The screenshot shows the PA-VM interface with the 'POLICIES' tab selected. A search bar is at the top. On the left, a sidebar lists various security features, with 'Authentication' highlighted. The main table displays a single policy:

	NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS	HIT COUNT	LAST P
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1	DMZ Suojaus	none	ADMIN-NET	any	unknown	any	DMZ	any	any	service-http	R13_Captive Portal		-	-

Kuvio 7. Authentication policy

Loimme Policies-välilehdellä Security-osiossa uuden turvallisuussäännön. WS-NETistä ja ADMIN-NETistä DMZ:lle tuleva liikenne sallitaan TestUser käyttäjältä. (Kuvio 8).

The screenshot shows a new policy entry in the table:

18	WS-netAdmin-net-L...	none	universal	ADMIN-NET	any	TestUser	any	DMZ	any	any	web-browsing	application...	Allow	none		-
----	----------------------	------	-----------	-----------	-----	----------	-----	-----	-----	-----	--------------	----------------	-------	------	--	---

Kuvio 8. Turvallisuussääntö WS-NET + ADMIN-NET -> DMZ

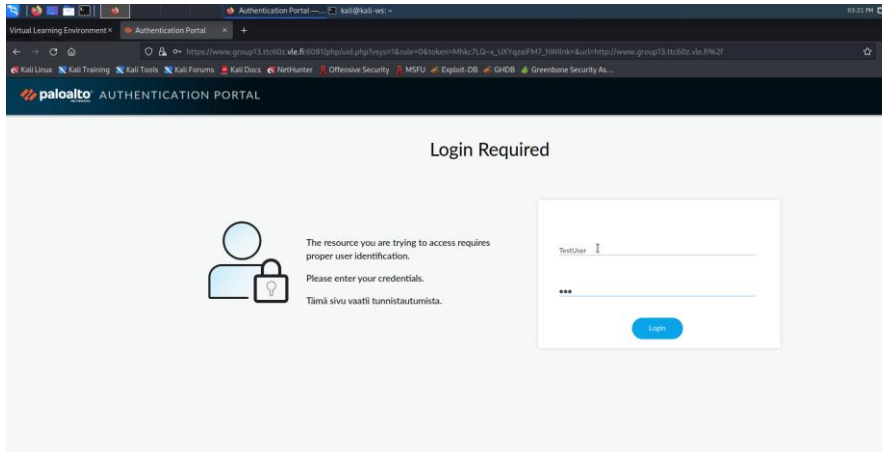
Siirryimme Kali-WS virtuaalikoneelle, joka sijaitsee ADMIN-NET turvallisuusalueella. Ajoimme komennon `sudo nano /etc/hosts` ja lisäsimme sinne rivin, jossa on www-palvelimen sisäverkon IP:n ja sivun osoitteen (Kuvio 9).

```
File Actions Edit View Help
GNU nano 7.1
10.4.0.11 www.group13.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
```

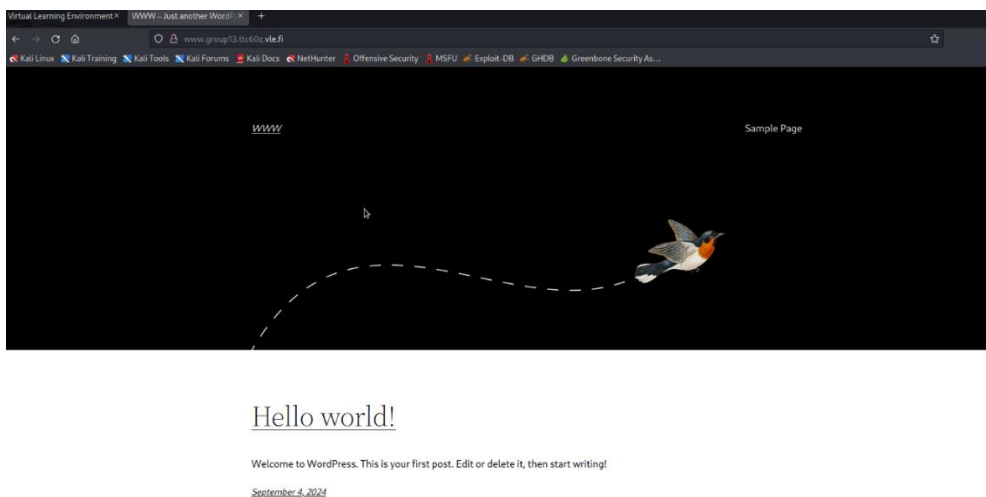
Kuvio 9. Kalin hosts-tiedosto

Kun navigoimme selaimella osoitteeseen www.group13.ttc60z.vle.fi, niin sivusto pyytää tunnistautumista (Kuvio 10). Tähän syötimme aiemmin määritellyn käyttäjän ja salasanan, jolla sivulle pitäisi päästä, eli TestUser:n.



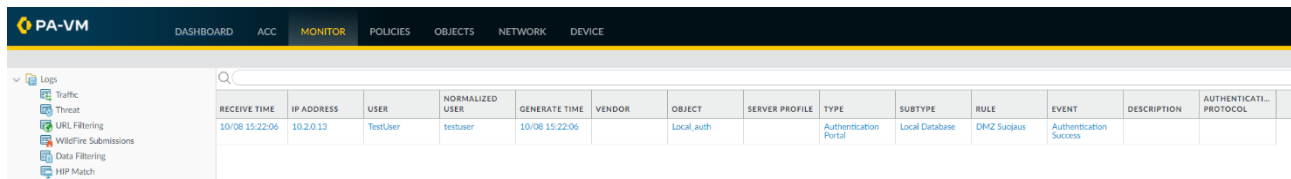
Kuvio 10. Captive Portal kirjautuminen

Tunnistautumisen jälkeen pääsimme sivustolle. (Kuvio 11).



Kuvio 11. Hello world

Palo Alton monitorissa näkyi kirjautuminen (Kuvio 12). Monitori näyttää käyttäjän, miten on tunnistauduttu ja mikä autentikointiprofiili on kyseessä (Local_auth).



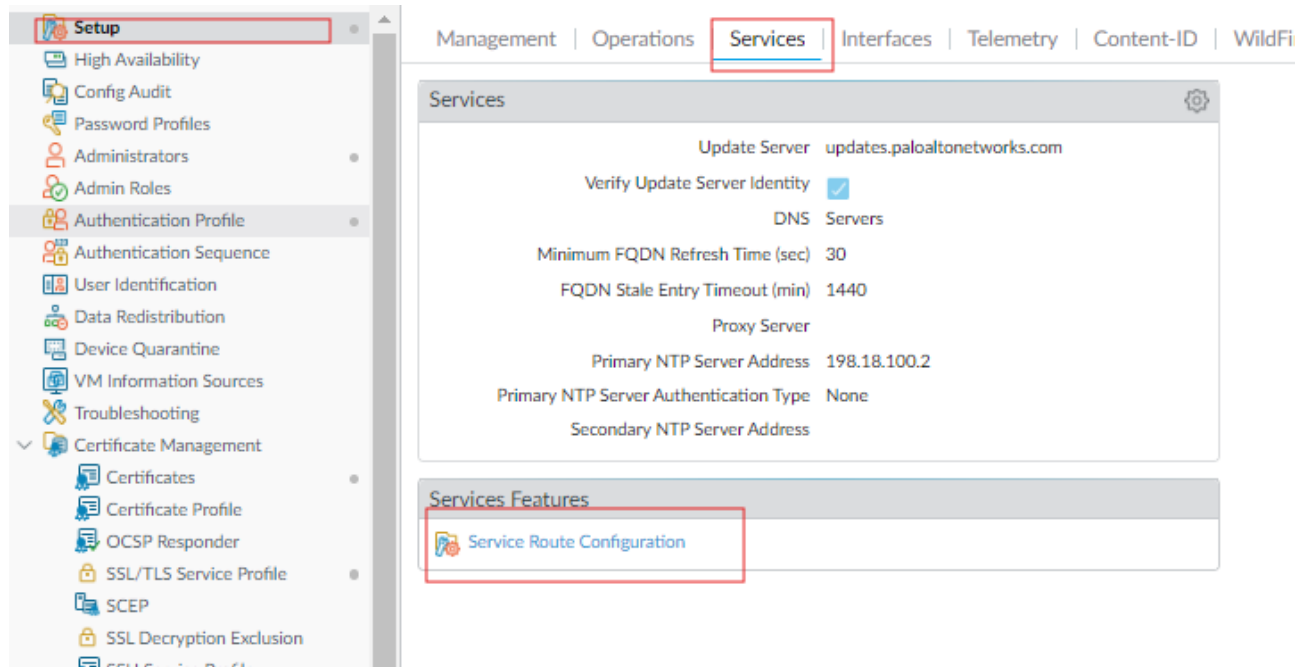
The screenshot shows the Palo Alto VM Monitor interface. The top navigation bar includes 'PA-VM', 'DASHBOARD', 'ACC', 'MONITOR' (selected), 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. On the left, a sidebar lists various log categories: Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, and HIP Match. The main area displays a table of log entries. The first entry is for a successful authentication event.

RECEIVE TIME	IP ADDRESS	USER	NORMALIZED USER	GENERATE TIME	VENDOR	OBJECT	SERVER PROFILE	TYPE	SUBTYPE	RULE	EVENT	DESCRIPTION	AUTHENTICATI... PROTOCOL
10/08 15:22:06	10.2.0.13	TestUser	testuser	10/08 15:22:06		Local_auth		Authentication Portal	Local Database	DMZ Suojus	Authentication Success		

Kuvio 12. Monitor

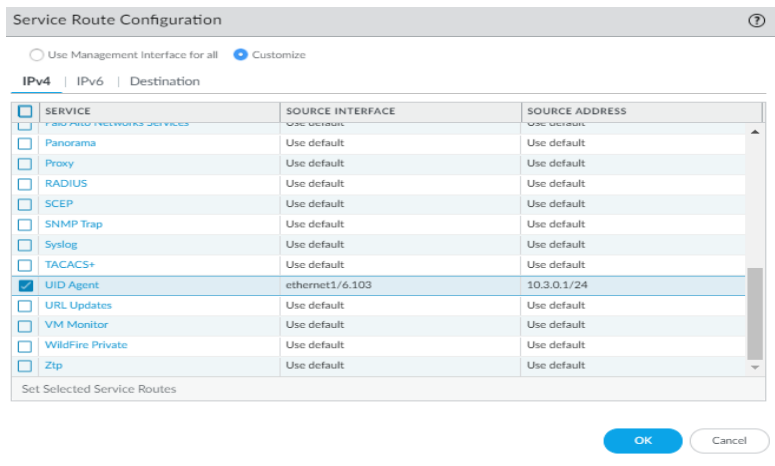
3.1 Active Directory Integrointi

AD:n integroimiseksi täytyy Palo Alto -palomuurin päässä asettaa rajapinta, josta se saa haettua käyttäjä- ja ryhmätiedot. (Kuvio 13).



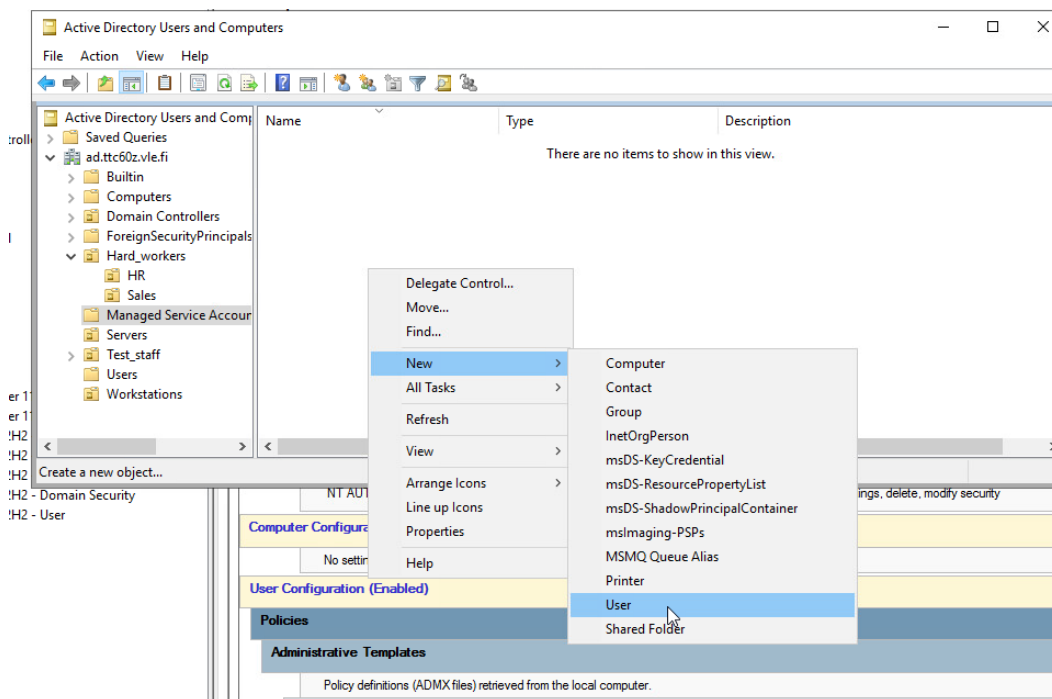
Kuvio 13. Rajapinnan asettaminen

User-ID (UID) agentille asetimme lähdeosoitteeksi dc01, jotta Palo Alto osaa kysellä tietoja sieltä. Tämä tehtiin myös LDAP agentille samoilla arvoilla. (Kuvio 14).



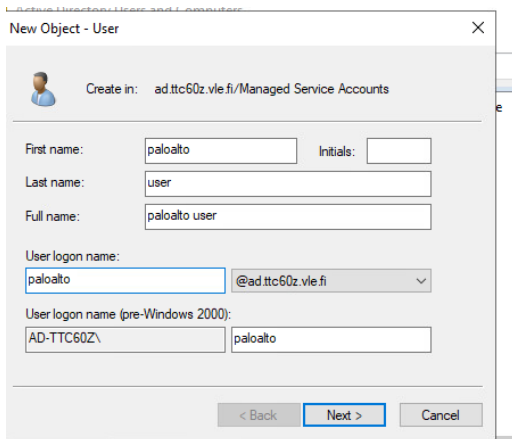
Kuvio 14. Rajapinnan asettaminen 2

Seuraavaksi avasimme DC01 -virtuaalikoneen ja loimme uuden palveluprofiili-käyttäjän, jonka avulla saamme kerättyä lokitietoja DC:ltä ja välitettyä ne sitten Palo Altoille. (Kuvio 15).



Kuvio 15. Uuden käyttäjän luonti

Annoimme käyttäjälle nimeksi paloalto, jotta tiedämme käyttäjän tarkoituksen. (Kuvio 16)



New Object - User

Create in: ad.ttc60z.vle.fi/Managed Service Accounts

First name: paloalto Initials:

Last name: user

Full name: paloalto user

User login name: paloalto @ad.ttc60z.vle.fi

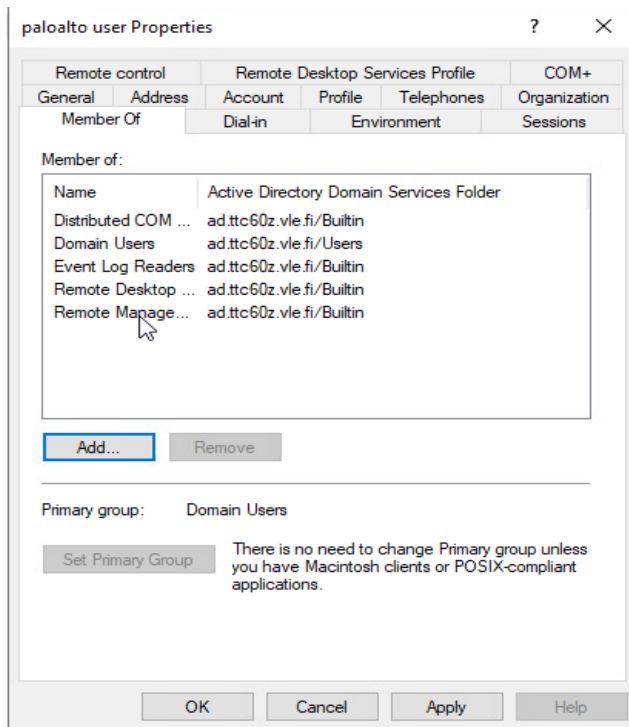
User login name (pre-Windows 2000): AD-TTC60Z\ paloalto

< Back Next > Cancel

Kuvio 16. Uuden käyttäjän luonti 2

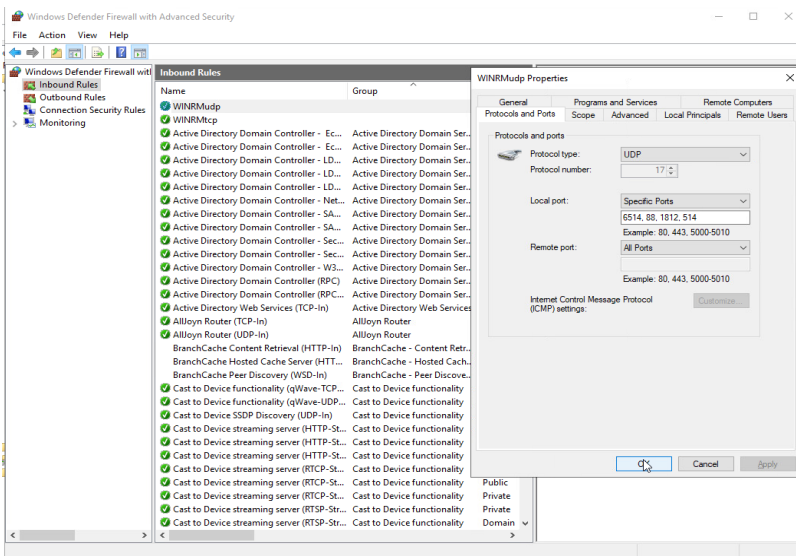
Tällä “paloalto” käyttäjällä tulee olla tarvittavat valtuudet lukea lokitietoja ja saada etäyhteys palvelimeen. Valtuudet tarvitaan, koska tämä käyttäjä tulee olemaan Palo Alto palomuurin “server monitoring” tili, tai User-ID tili, eli käyttäjätili, jonka avulla palomuri voi hakea tietoa AD:sta. Event Log Readers ja Remote Management Users ovat ryhmät, joihin käyttäjä tulee ainakin liittää, näillä valtuuksilla saadaan näkymään lokitiedot ja ne saadaan haettua etäyhteydellä AD:sta Palo Altoon. Agentin avulla AD:n toimintaa pystytään seuraamaan myös käyttäjän tunnuksen perusteella, ei pelkästään IP-osoitteen avulla.

Lisäsimme käyttäjän kuvion 17 mukaisiin ryhmiin.



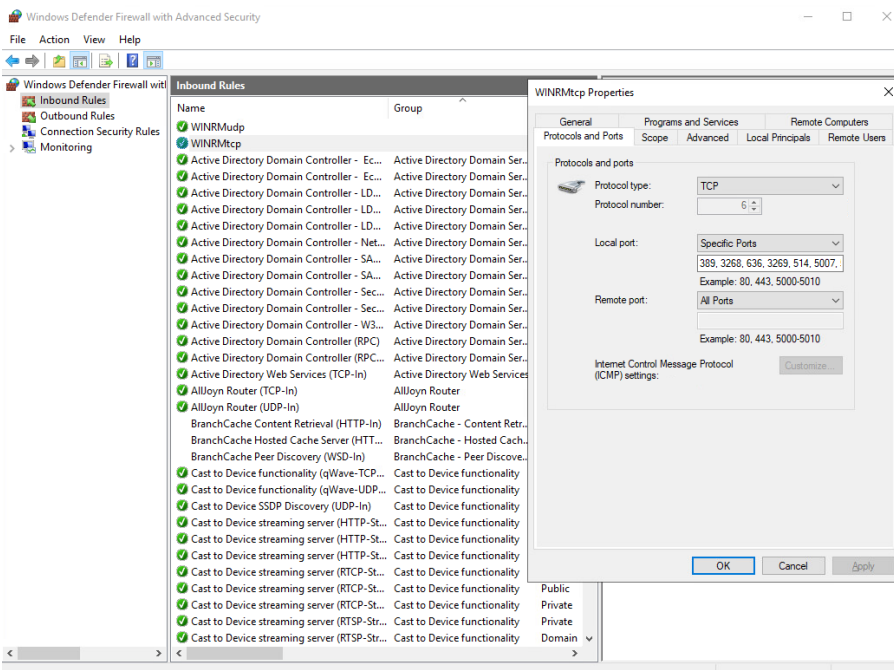
Kuvio 17. Ryhmien lisäys3

WinRM (Remote Management) yhteyden saamiseksi tuli meidän täytyä avata useita portteja palomuurin kautta. Tarpeellisten porttien lista löytyi Palo Alton dokumentaatioista. Teimme säännön UDP-porteille. (Kuvio 18).



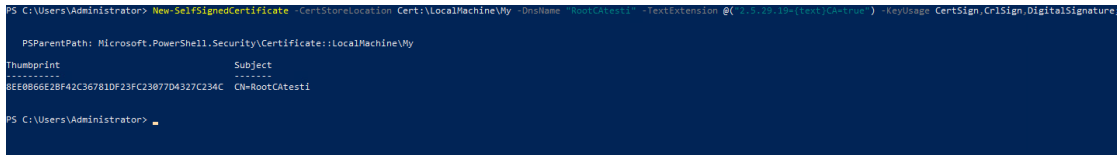
Kuvio 18. UDP-porttien salliminen

Teimme toisen samanlaisen säännön erikseen TCP-porteille. (Kuvio 19)



Kuvio 19. Porttien salliminen tcp

Seuraavaksi loimme sertifikaatin, jotta yhteys saadaan salattua AD:n ja palomuurin välillä. Ajoimme kuvion 20 mukaisen komennon PowerShellillä ja kopioimme saadun Thumbprintin.



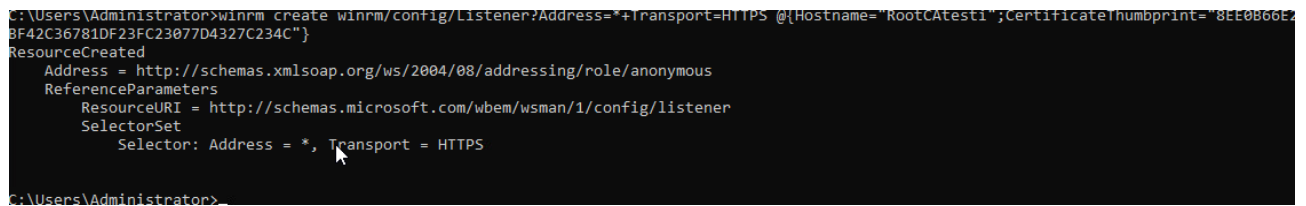
```
PS C:\Users\Administrator> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -FriendlyName RootCAtest1 -TextExtension @( "2.5.2.25={text;C=Fin}" ) -KeyUsage CertSign,CriSign,DigitalSignature;

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint      Subject
-----
8Et0866E2BF42C36781DF23FC23077D4327C234C CN=RootCAtest1

PS C:\Users\Administrator>
```

Kuvio 20. Allekirjoitettu sertifikaatti

Loimme uuden Windows Remote Management (WinRM) kuuntelija, joka käyttää HTTPS-protokollaa tiedonsiirtoon. Käytimme aiemmin luotua sertifikaattia asettamalla CertificateThumbprint kohtaan tallentamamme Thumbprintin. (Kuvio 21).



```
C:\Users\Administrator>winrm create winrm/config/Listener?Address=*&Transport=HTTPS @{Hostname="RootCAtest1";CertificateThumbprint="8Et0866E2BF42C36781DF23FC23077D4327C234C"}
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>
```

Kuvio 21. WinRM 1

Muokkasimme vielä WinRM konfiguraatioita niin että hyödynnämme Basic Authenticationia kuvion 22 mukaisesti.

```

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

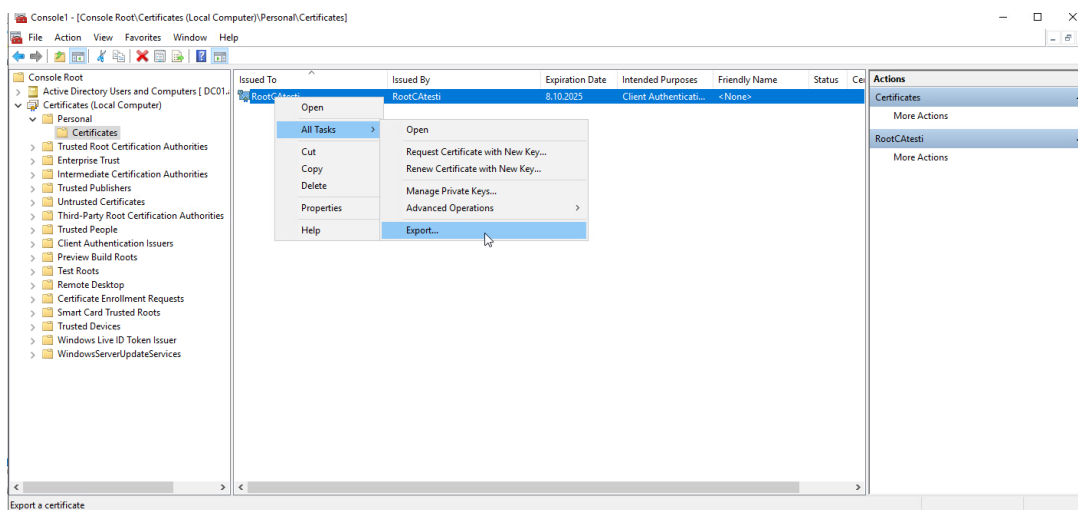
C:\Users\Administrator>winrm set winrm/config/service/auth @{Basic="true"}
Auth
  Basic = true
  Kerberos = true
  Negotiate = true
  Certificate = false
  CredSSP = false
  CbtHardeningLevel = Relaxed

C:\Users\Administrator>

```

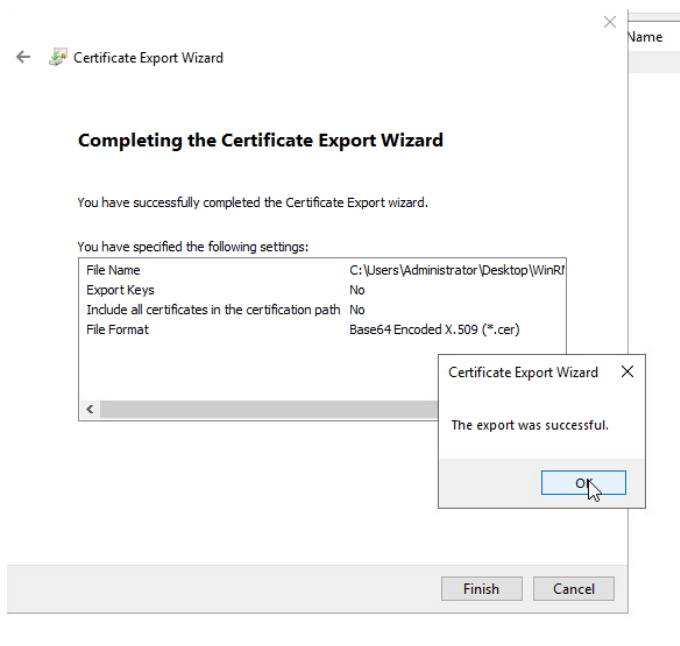
Kuvio 22. WinRM 2

Otimme luodun sertifiikaatin ulos MMC:n kautta ja viemme sen Palo Altoon. (Kuvio 23).



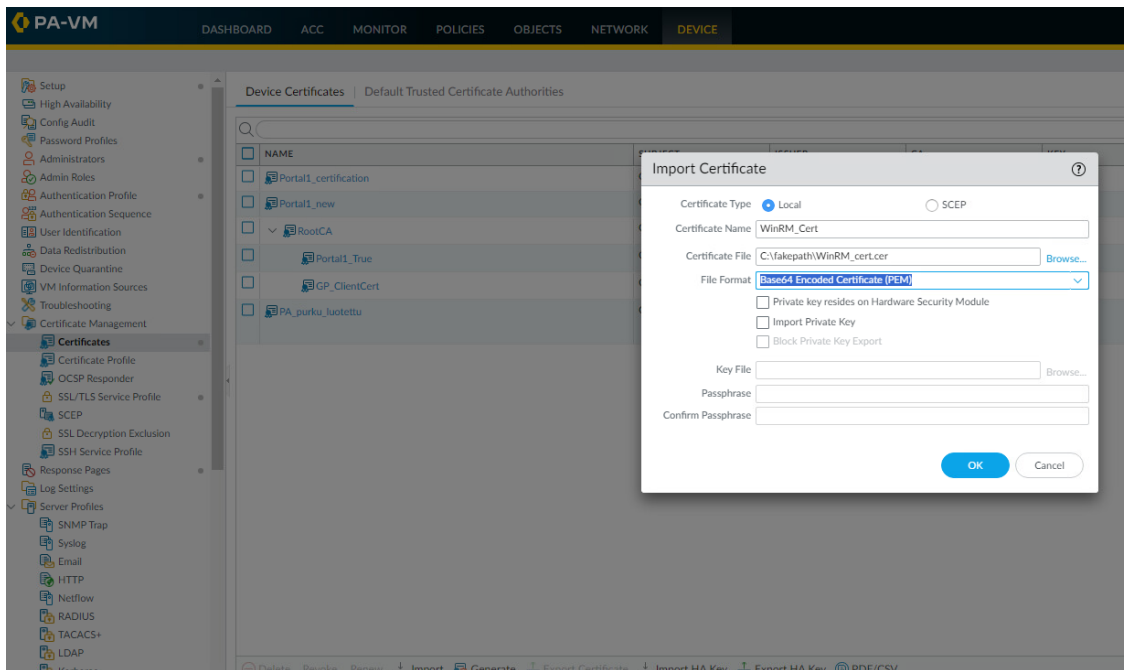
Kuvio 23. Sertifiikaatin vienti

File Format kohtaan vaihdoimme kuvion 26 mukaisesti Base64 Encoded X.509 (*.cer), eli tiedosto-
muodoksi tulee .cer. (Kuvio 24).



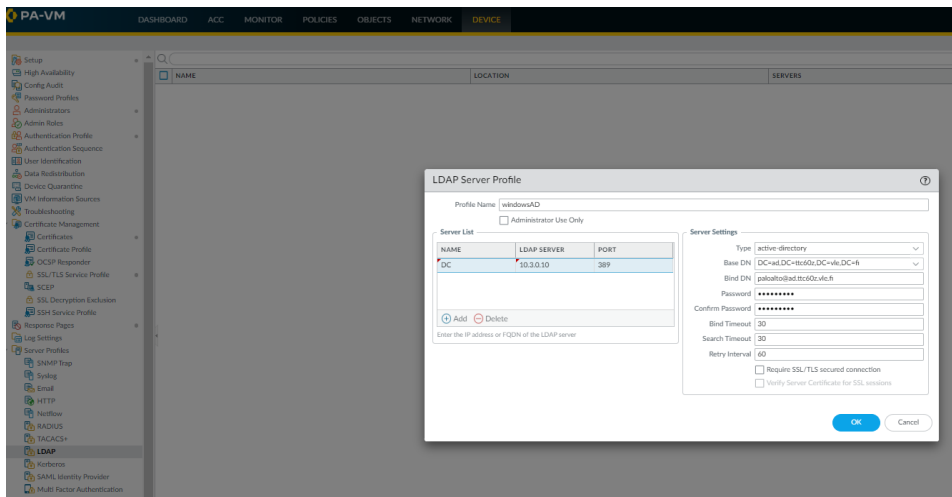
Kuvio 24. Sertifikaatin vienti onnistui

Seuraavaksi lisäsimme sertifiikaatin Palo Altoon Device-välilehden Certificate Management -osiosta. (Kuvio 25).



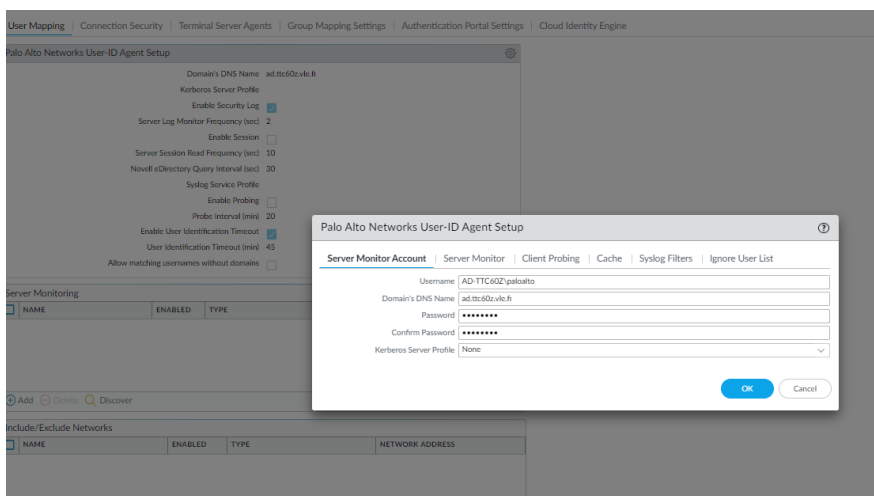
Kuvio 25. Sertifiikaatin tuonti

Loimme LDAP palvelinprofiili ja asetimme sen käyttämään AD:lla luotua palveluprofiilia paloalto. LDAP- protokolla hakee tämän käyttäjän avulla tiedot Active Directorysta. Profiili vaati myös LDAP palvelimen IP- osoitteen ja portin, jonka kautta kommunikoida sen kanssa. (Kuvio 26)



Kuvio 26. LDAP-profiili

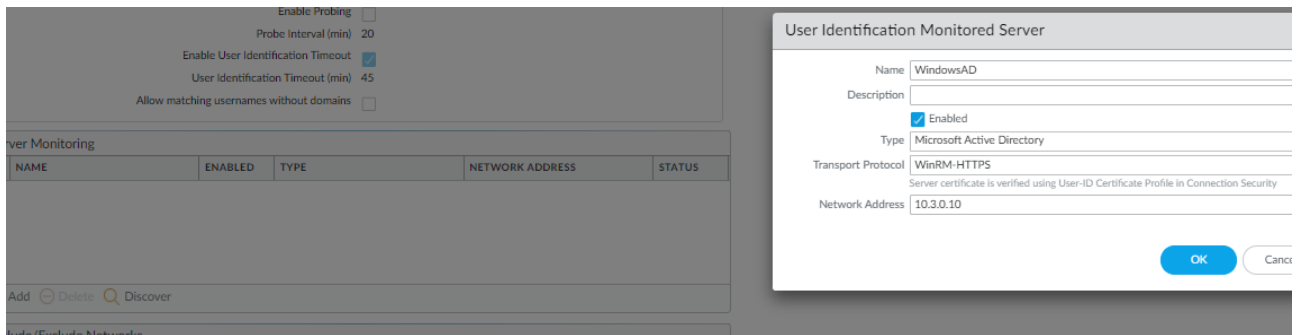
Seuraavaksi siirryimme Device-välilehde User Identification osioon, jossa painoimme mutteria Palo Alto Networks User-ID Agent Setup laatikon yläkulmasta. Asetimme tähän aiemmin luomamme paloalto-palveluprofiilin tunnisteet. (Kuvio 27).



Kuvio 27. User-ID agentin asetukset

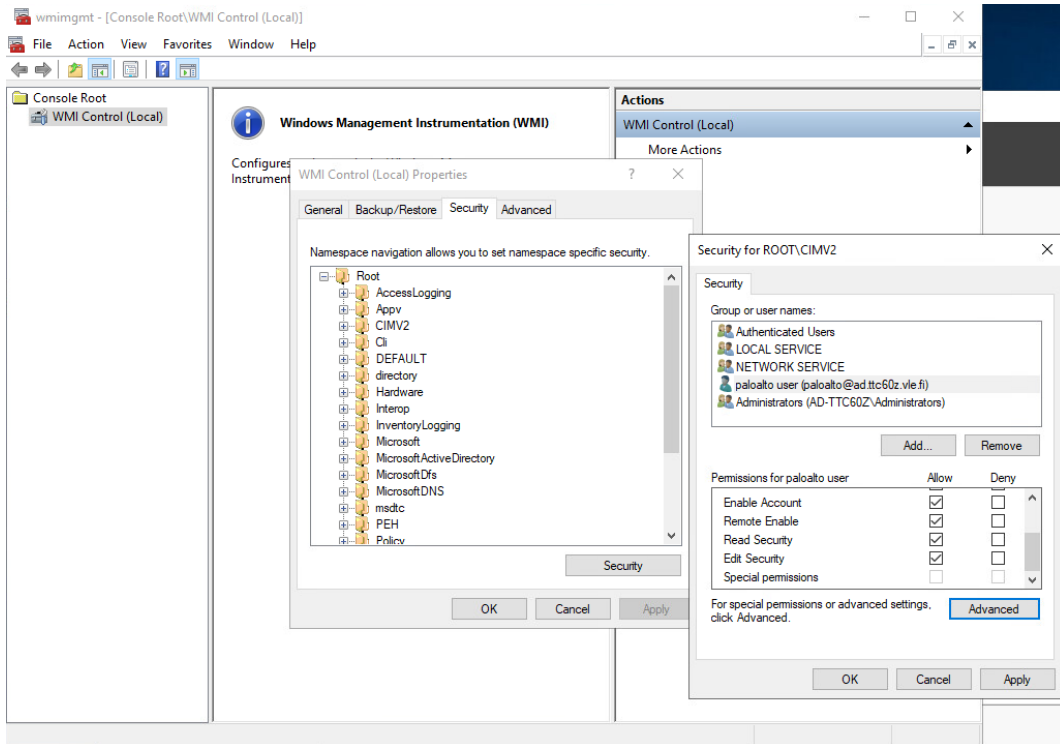
User Identification Monitored Server asetuksilla saadaan Palo Alto yhdistettyä AD palvelimeen WinRM-HTTPS kuljetusprotokollan avulla. Palvelimen tyyppi saadaan valittua Palo Alto palomuurin

hyväksytyistä tiedostopalveluista. Valitsimme valikosta Microsoft Active Directoryn, koska käytämme sitä. (Kuvio 28).



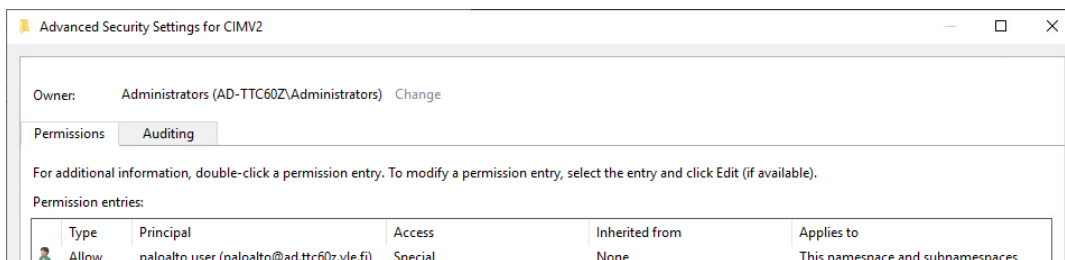
Kuvio 28. Monitored server

Törmäsimme ongelmaan, jossa user agent ei suostunut yhdistämään, jos DC01:n palomuuuri oli päällä tai paloalto käyttäjällä. Vaihdoimme käyttäjän administraattoriin ja palomuurin pois päältä ja tällöin Palo Alto sai yhteyden DC01:n. Ongelma johtui WMI kontrollien oikeuksista, käyttäjä paloaltolle piti lisätä ROOT\CIMV2 oikeuksia. (Kuvio 29).



Kuvio 29. CIMV2-asetukset

Varmistimme vielä Advanced-välilehdeltä, että Applies to- kohdassa on valittuna this namespace and subnamespaces. (Kuvio 30).



Kuvio 30. Advanced-välilehti

Nyt saimme yhteyden käyttäen paloalto käyttäjää ja ilman palomuuria. (Kuvio 33).

Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	WindowsAD	<input checked="" type="checkbox"/>	Microsoft Active Directory	10.3.0.10	Connected

Kuvio 31. Yhteys avattu

Kun asetimme palomuurin päälle niin yhteys katkesi. Lisäsimme HTTPS-portin 5986 sallittaviin TCP-yhteyksiin. Tämä ratkaisi ongelman ja yhteys pysyi päällä, vaikka laitoimme DC01:n palomuurin takaisin päälle.

Seuraavaksi loimme säännön User-Id:lle Device-välilehdellä User Identification -osiossa Group Mapping Settings kohdassa. (Kuvio 32).

Group Mapping

Name: windows

Server Profile: windowsAD | Update Interval: [60 - 86400]

Domain Setting: User Domain: ad-ttc60z

Group Objects: Search Filter: | Object Class: group

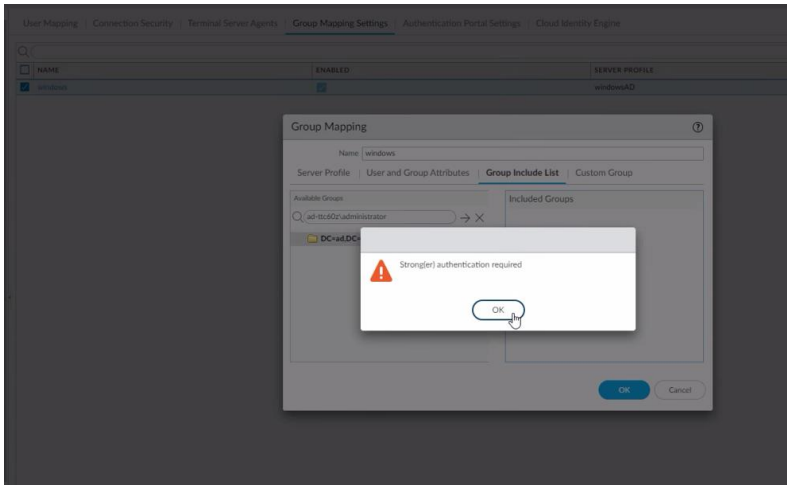
User Objects: Search Filter: | Object Class: person

☒ Enabled
☐ Fetch list of managed devices

OK Cancel

Kuvio 32. User Mapping

Kun yritimme lisätä käyttäjäryhmiä huomiotaviin käyttäjäryhmiin, saimme virheviestin tarvittavasta vahvemmassa tunnistautumisesta. (Kuvio 33).



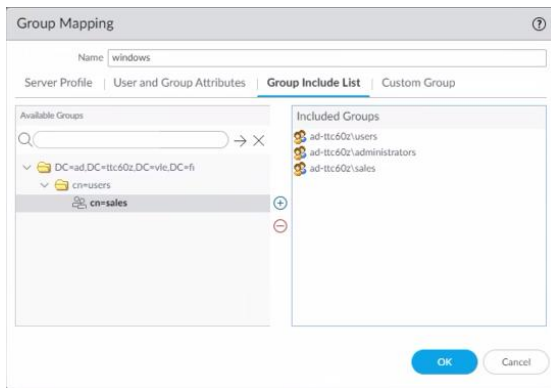
Kuvio 33. Virheviesti

Käyttäjärhymiä ei jostain syystä pystynyt lisäämään. Huomasimme, että ongelma johtui GPO-säännöstä "LDAP server signing requirements". Vaihdoimme tähän none. (Kuvio 34).

Domain Controller	
Policy	Setting
Domain controller: LDAP server signing requirements	None

Kuvio 34. Käytön estänyt GPO

Nyt pystyimme lisäämään käyttäjärhymiä ja lisäsimme aluksi users, administrators ja sales -ryhmät. (Kuvio 35).



Kuvio 35. group mapping

3.2 Testaaminen

Kirjauduimme WS01-virtuaalikoneelle boross-käyttäjällä, joka kuuluu sales-ryhmään, ja avasimme selaimella YouTuben. Palo Alton monitorissa näkyi boross-käyttäjän käynti YouTubessa. (Kuvio 36)

10/09 14:27:59	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	172.217.21.174	443	youtube-base	allow	WS-net_to_VLE	n/a	2.1k	0
10/09 14:27:30	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.110	443	youtube-base	allow	WS-net_to_VLE	tcp-rst-from-client	11.8k	0
10/09 14:27:26	end	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	216.58.207.246	443	youtube-base	allow	WS-net_to_VLE	tcp-rst-from-client	11.7k	0
10/09 14:27:25	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	216.58.207.206	443	youtube-base	allow	WS-net_to_VLE	n/a	1.7k	0
10/09 14:27:20	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	173.194.24.200	443	youtube-base	allow	WS-net_to_VLE	n/a	4.2k	0
10/09 14:27:20	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	173.194.24.200	443	youtube-base	allow	WS-net_to_VLE	n/a	5.0k	0
10/09 14:27:15	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.54	443	youtube-base	allow	WS-net_to_VLE	n/a	2.1k	0
10/09 14:27:11	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.110	443	youtube-base	allow	WS-net_to_VLE	n/a	1.7k	0
10/09 14:27:11	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.110	443	youtube-base	allow	WS-net_to_VLE	n/a	2.1k	0
10/09 14:27:11	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.22	443	youtube-base	allow	WS-net_to_VLE	n/a	1.7k	0
10/09 14:27:11	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.78	443	youtube-base	allow	WS-net_to_VLE	n/a	2.1k	0
10/09 14:27:11	start	WS-NET	VLE	10.1.0.10	ad-ttc60z\boross	142.250.74.46	443	youtube-base	allow	WS-net_to_VLE	n/a	1.7k	0

Kuvio 36. Boross YouTubessa

Jotta saamme autentikointiportaaliin tunnistautumisen onnistumaan ad tunnuksilla, loimme uuden authentication profiiliin. (Kuvio 37)

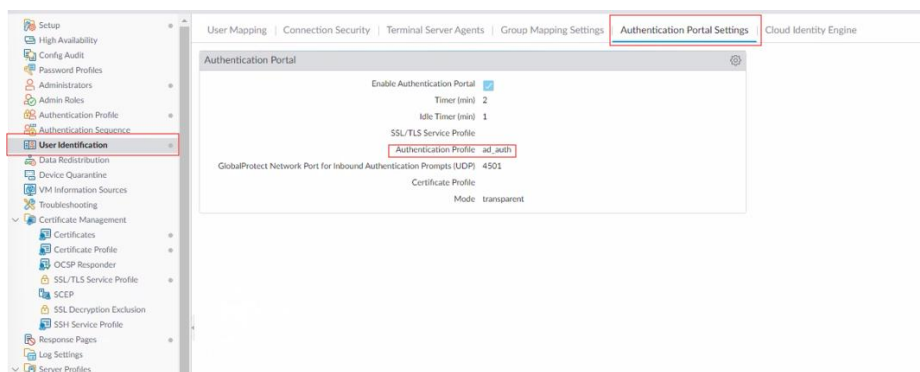
The screenshot shows the 'Authentication Profile' configuration window for a profile named 'ad_auth'. The window has three tabs: 'Authentication', 'Factors', and 'Advanced'. The 'Authentication' tab is active. It contains the following fields and settings:

- Name:** ad_auth
- Type:** LDAP
- Server Profile:** windowsAD
- Login Attribute:** (empty)
- Password Expiry Warning:** 7 (with a note: 'Number of days prior to warning a user about password expiry.')
- User Domain:** (empty)
- Username Modifier:** %USERINPUT%
- Single Sign On:**
 - Kerberos Realm:** (empty)
 - Kerberos Keytab:** Click "Import" to configure this field. There is an 'X Import' button next to it.

At the bottom right, there are 'OK' and 'Cancel' buttons.

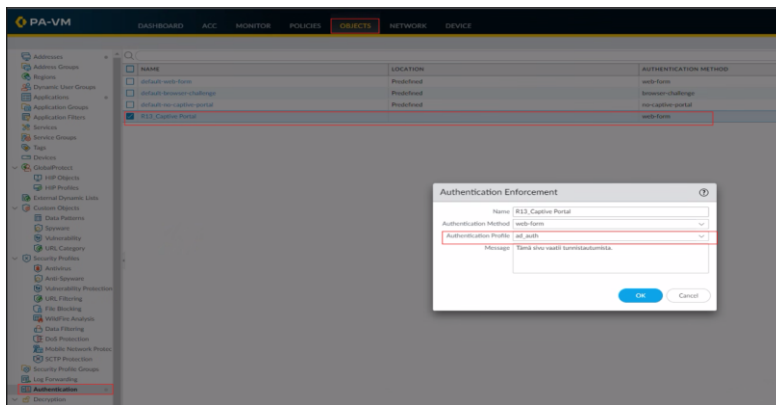
Kuvio 37. Autentikointiprofiili ad_auth

Seuraavaksi vaihdoimme Devices-välilehdeltä User Identification -osiosta Authentication Portal settings -kohdasta käytettäväksi profiiliksi luomamme ad_auth. (Kuvio 38)



Kuvio 38. Autentikointiprofiilin vaihto

Vaihdoimme myös aiemmin tekemäämme R13_Captive_portal:iin autentikointiprofiiliksi ad_auth:n. (Kuvio 39)



Kuvio 39. Captive Portalin profiilin vaihto

Seuraavaksi kokeilimme mennä sales-ryhmään kuuluvalla MaMyyjä-käyttäjällä

www.group13.ttc60z.vle.fi -sivullemme. Monitorissa näkyi action kohdassa deny, eli pääsy estettiin. (Kuvio 40).

	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/2 CONNECTION SESSION ID	SOWA NAME
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	start	WS-NET	VLE	10.1.0.10	ad-ttc60z/mammyja		142.250.74.131			443	qalc-base	allow	WS-net_to_VLE	n/a	1.3k	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	
	10/09 16:45:51	drop	WS-NET	DMZ	10.1.0.10	ad-ttc60z/mammyja		198.19.52.85			80	not-applicable	deny	interzone-default	policy-deny	0	0	

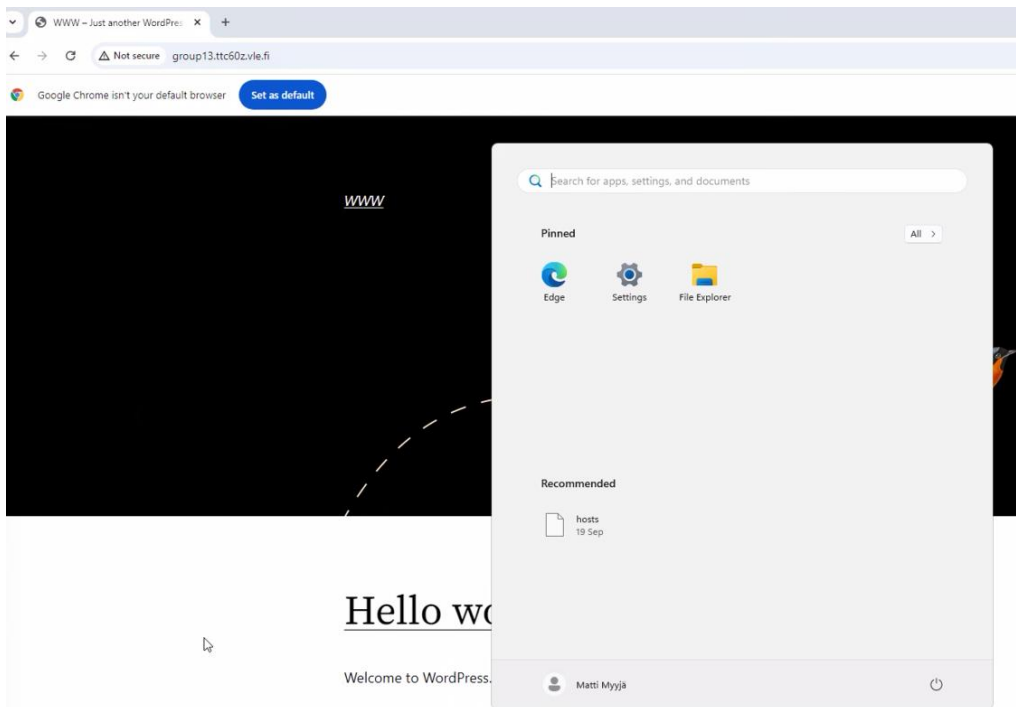
Kuvio 40. Monitor MaMyyjä

Lisäsimme käyttäjän MaMyyjä turvallisuuspolitiikkaan, jonka loimme harjoituksen alussa. (Kuvio 41).

18	WS-netAdmin-net-L...	none	universal	ADMIN-NET	any	ad-ttc60z/boorss	any	DMZ	any	any	web-browsing	application...	Allow	none
----	----------------------	------	-----------	-----------	-----	------------------	-----	-----	-----	-----	--------------	----------------	-------	------

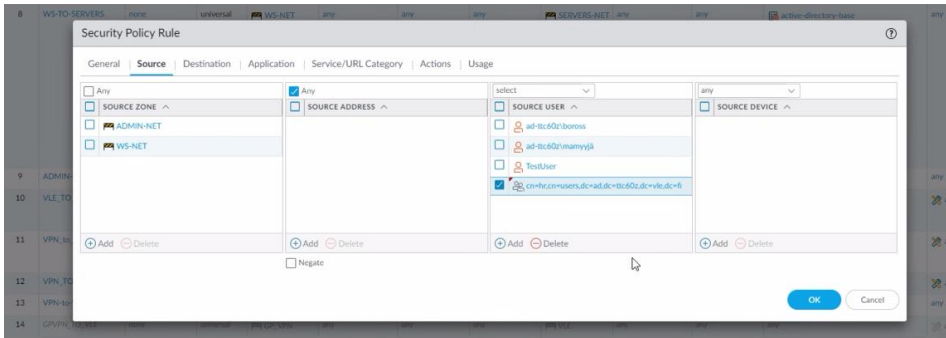
Kuvio 41. Hyväksyttyjen käyttäjien lisääminen turvallisuuspolitiikkaan

Tämän jälkeen MaMyyjäkin pääsi sivullemme. (Kuvio 42).



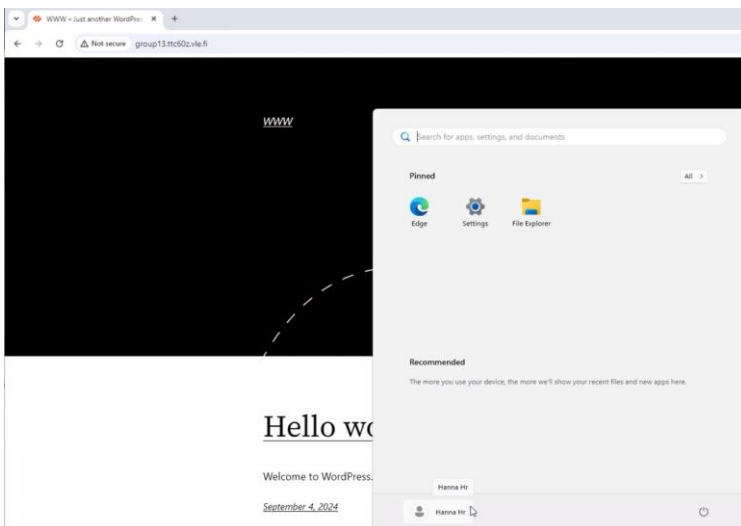
Kuvio 42. Matti Myyjä verkossa

Testasimme vielä AD-ryhmän perusteella. Kokeilimme Hanna Hr -käyttäjää, joka kuuluu HR-ryhmään. Lisäsimme tämän ryhmän turvallisuuspolitiikkaan. (Kuvio 43).



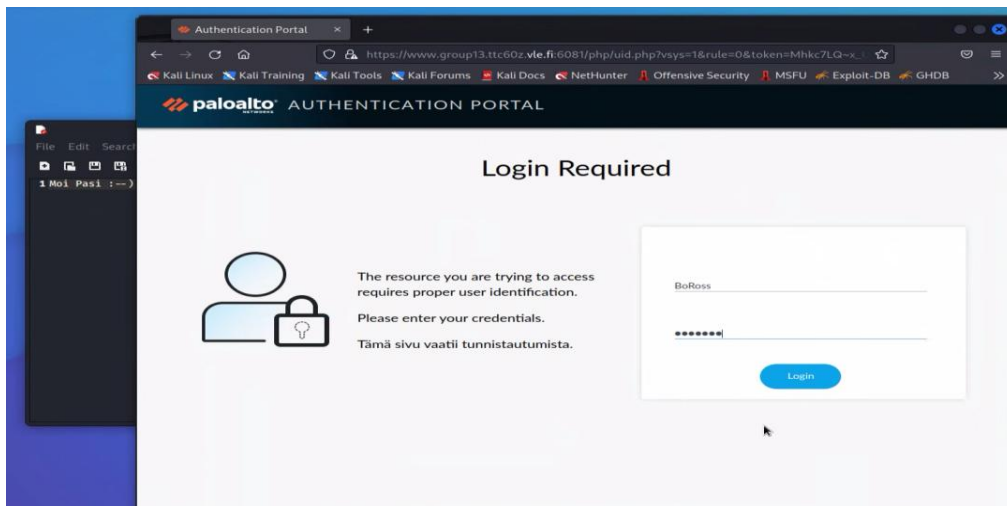
Kuvio 43. Käyttäjäryhmän lisääminen turvallisuuspolitiikkaan

Nyt pääsi myös Hanna Hr sivuille. (Kuvio 44)



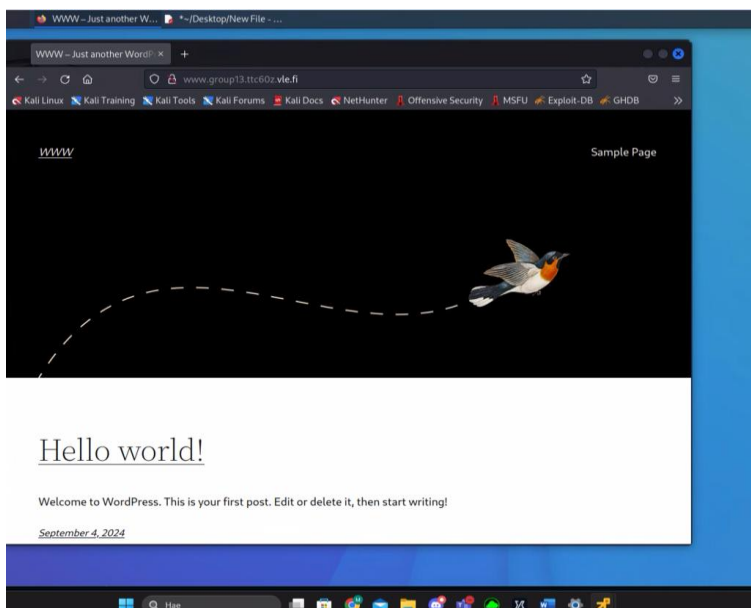
Kuvio 44. Hanna HR verkossa.

Testasimme vielä Captive Portalin toiminnan boross -käyttäjällä Kalilla. (Kuvio 45).



Kuvio 45. Captive portal Kalilla lopussa

Ja tunnistus onnistui hyvin. (Kuvio 46)



Kuvio 46. Bob Ross verkossa

Varmistimme asian vielä monitorista. Lähteenä näkyy 10.2.0.13 eli Kali ja käyttäjänä boross. (Kuvio 47)

10/09 17:05:36	end	ADMIN-NET	DMZ	10.2.0.13	boross	10.4.0.11	80	web-browsing	allow	ADMIN_TO_WL...	tcp-fin	467.5k	0	0
10/09 17:05:36	end	ADMIN-NET	DMZ	10.2.0.13	boross	10.4.0.11	80	incomplete	allow	ADMIN_TO_WL...	tcp-fin	436	0	0
10/09 17:05:36	end	ADMIN-NET	DMZ	10.2.0.13	boross	10.4.0.11	80	web-browsing	allow	ADMIN_TO_WL...	tcp-fin	131.6k	0	0
10/09 17:05:36	end	ADMIN-NET	DMZ	10.2.0.13	boross	10.4.0.11	80	web-browsing	allow	ADMIN_TO_WL...	tcp-fin	3.5k	0	0

Kuvio 47. Boross-käyttäjä monitorissa

4 Pohdinta

Harjoitustyössä pääsimme tutustumaan vielä syvällisemmin paloalton asetuksiin ja mahdollisuuksiin. Loimme tunnistautumisportaalin ja konfiguroimme Active Directory -integraation, jonka avulla pystymme rajoittamaan käyttäjien ja käyttäjäryhmien pääsyä ja tunnistautumista haluamiimme kohteisiin.

Ongelmilta ei välttytty tässäkään ja jouduimme syventymään ad:n ja paloalton toimintaan vielä enemmän ongelmien ratkomiseksi. Ensimmäinen ongelma tuli vastaan, kun koitimme yhdistää domain controllerille käyttäen paloalto käyttäjää, yhteys onnistui kuitenkin administraattorina, ja kun palomuurit olivat pois päältä eli ongelmaa löytyi sekä käyttäjästä, että palomuurin asetuksista. Ongelma johtui käyttäjän WMI (Windows Management Instrumentation) oikeuksien puutteesta. Lisäsimme siis oikeuksia nimialueeseen Root\CIMV2, joiden avulla käyttäjä voi suorittaa tarvittavia WMI-kyselyjä. Palomuurin kanssa olevan ongelman saimme ratkaistua lisäämällä palomuurin asetuksista TCP-portteihin HTTPS-portin 5986.

Harjoitusta tehdessä myös muut ryhmät olivat törmänneet samankaltaisiin ongelmiin. Ryhmämme oli kerennyt jo ratkaista ongelmat, joten pääsimme auttamaan muita ryhmiä. Tämä oli ryhmällemme hyvää kertausta labran aiheista. Pääsimme myös tutustumaan ongelmiin, mitä meillä itsellämme ei ollut.

Kaiken kaikkiaan harjoitus oli opettavainen ja mielenkiintoinen. Harjoituksen sai suurimmaksi osaksi tehtyä ohjeiden avulla, mutta käytimme työssä myös laajasti paloalton omia ohjeistuksia ja dokumentaatioita, varsinkin ongelman ratkaisussa.

Lähteet

Configure Server Monitoring Using WinRM. Palo Alto ohje. 2024. Viitattu 10.10.2024. <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-server-monitoring-using-winrm>

User-ID Overview. Palo Alto dokumentti. 2024. Viitattu 8.10.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-overview>

Create a dedicated Service Account for the User-ID Agent. Palo Alto dokumentti. 2024. Viitattu 10.10.2024. <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/map-ip-addresses-to-users/create-a-dedicated-service-account-for-the-user-id-agent>