



Tietoturvakontrollit – Labra 3

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Helmikuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

1	Johdanto	3
2	TEORIA	3
2.1	EICAR	3
2.2	NMAP	4
2.3	Lyhyet selitykset mitä tekevät Dokumentoinnin kohdassa 3.1.1 määriteltävät asetukset, "Profile Settings"	4
2.3.1	Antivirus	4
2.3.2	Vulnerability protection.....	4
2.3.3	Anti-Spyware.....	4
2.3.4	File Blocking	4
2.3.5	Wildfire Analysis	5
2.4	Mitre ATT&CK	5
2.5	Uhkatieto (Threat Intelligence)	5
3	DOKUMENTOINTI	6
3.1	Lab 3 – Paloalto Security Fe	6
3.1.1	Ympäristön turvallisuuden lisääminen	6
3.1.2	Antivirus hälytykset ja URL suodatus liikenteeseen WS-netistä VLE:hen	9
3.1.3	Sertifikaatin luonti	13
3.1.4	Decryption	18
3.1.5	Testaus	20
3.1.6	Flood Protection	23
4	POHDINTA	26
	Lähteet	28

Kuvat

Kuva 1. Snapshot alkutilanteesta	7
Kuva 2. Delete DMZ.....	7
Kuva 3. DMZ poistunut "GATEWAY-TO-VLE" - säännöstä.	8
Kuva 4. Profile Settings.	8
Kuva 5. Uusi Antivirus - sääntö.	9
Kuva 6. URL-filteröinti profiilin kopiointi.	9
Kuva 7. Gambling ja games asetukset.....	10

Kuva 8. YleFiltteri.	11
Kuva 9. EicarFiltteri.	11
Kuva 10. Luodut kategoriat.	12
Kuva 11. YleFiltteri ja EicarFiltteri lisätty.	12
Kuva 12. WS-TO-VLE asetukset.	13
Kuva 13. Sertifikaatin luominen.	14
Kuva 14. "Forward Trust Certificate" sekä "Trusted Root CA" aktiiviseksi.	14
Kuva 15. Ladataan sertifikaatti WS01 koneelle.	15
Kuva 16. Avataan ladattu tiedosto Notepad++ ohjelmalla.	15
Kuva 17. Tiedosto avattuna.	16
Kuva 18. Tallennetaan sertifikaatti-muodossa.	16
Kuva 19. "Trust this CA to identify websites" aktiiviseksi.	17
Kuva 20. Lisätty sertifikaatti näkyy listalla.	17
Kuva 21. Nimi decryption säännölle.	18
Kuva 22. Source Zone.	18
Kuva 23. Destination Zone.	19
Kuva 24. URL Category.	19
Kuva 25. Log Settings.	20
Kuva 26. Pelisivun onnistunut testaus.	20
Kuva 27. Yle.fi onnistunut testaus.	21
Kuva 28. Eicar onnistunut testaus.	21
Kuva 29. Tiedostojen latausyritykset näkyvät threat - sivulla.	22
Kuva 30. Gambling sivujen hälytykset (alert).	22
Kuva 31. Flood protection nimi.	23
Kuva 32. Flood protection asetukset.	23
Kuva 33. Flood Profile liitetty ADMIN-NETiin.	24
Kuva 34. Sallittu liikenne ADMIN-NETistä DMZ:lle.	24
Kuva 35. Ensimmäinen skannausyritys meni läpi.	25
Kuva 36. Ympyröidyn osion sisällä olevista asetuksista mitään ei ollut aktivoitu.	25
Kuva 37. Nmap skannaus estetty onnistuneesti.	26

1 Johdanto

Kolmannen laboratorioharjoituksen Labra 3:n tarkoituksena on tutustua Palo Alton turvallisuus ominaisuuksiin paremmin. Harjoituksessa hyödynnetään Thread-Id:tä ja URL filteröintiä.

Harjoituksen tavoitteena on saada opiskelijoille ymmärrys, miten ympäristöön voidaan asettaa turvallisuus sääntöjä esimerkiksi verkkoselailuun. Harjoituksessa Palo Altoon tehdään uusi sääntö, joka koskee vain web-browsing liikennettä WS-netistä VLE:hen johon luodaan URL filteröinti. Filteröinti estää pääsyn Yle.fi verkkosivulle, aiheuttaa hälytyksen uhkapelisivustoilla sekä antaa peli (games)sivustoilla continue vaihtoehdon eikä suoraan mene sivulle.

Harjoitustyön lopussa asetetaan lisätehtävänä flood protection joka estää porttien skannaamiseen. Zone Protection profiilin toimivuus tullaan testaamaan nmapilla Kali-WS koneelta kokeilemalla skannausta www-palvelimelle (10.4.0.11).

Labra 3. aikana dokumentoidaan kuvankaappauksilla VLE ympäristössä toteutetut toimenpiteet, niiden kuvaus, sekä mahdolliset ongelmatilanteet sekä niiden ratkaiseminen. Lisäksi käydään läpi teoria osuudessa laboratorioympäristön virtuaalikoneen Palo Alto palomuurin Profile Settings, EICAR, NMAP, Mitre ATT&CK sekä mitä on uhkatieto.

2 TEORIA

2.1 EICAR

EICAR eli European Institute of Computer Anti-virus Research on vuonna 1991 perustettu kyberturvallisuus organisaatio, joka on erikoistunut virustorjunnan tehostamiseen sekä virustorjuntaohjelmistojen kehittämiseen.

EICAR on tehnyt haittaohjelmien torjunnan testaamiseksi niin sanotun ”dummy” testitiedoston. Testitiedoston ladatessa tulisi haittaohjelmien torjunnan havaita tiedosto haitalliseksi. Käytimme harjoitustyössä hyväksemme EICAR testitiedostoa testaamaan palomuurimme haittaohjelmien eston toimimista. (EICAR N.d.)

2.2 NMAP

Nmap on laajalti käytetty työkalu verkon tutkimiseen, hallintaan ja tietoturvatarkastukseen. Sen avulla käyttäjät voivat skannata verkkoja ja tunnistaa aktiiviset isännät, niissä toimivat käyttöjärjestelmät ja palvelut sekä avoimet verkkoportit. Nmapin avulla voidaan tunnistaa mahdolliset tietoturva-aukot, havaita luvaton käyttö ja seurata verkon muutoksia ajan mittaan. Työkalu on hyödyllinen myös verkko-ongelmien vianmäärityksessä ja verkon suorituskyvyn optimoinnissa. Nmap on ilmainen ja avoimen lähdekoodin työkalu, jota voidaan käyttää useissa käyttöjärjestelmissä, mukaan lukien Windows, macOS ja Linux. Tehokkaiden ominaisuuksiensa ja helppokäyttöisyytensä ansiosta Nmap on tärkeä työkalu verkonvalvojille ja tietoturva-ammattilaisille. (Nmap Reference Guide N.d.)

2.3 Lyhyet selitykset mitä tekevät Dokumentoinnin kohdassa 3.1.1 määriteltävät asetukset, "Profile Settings"

2.3.1 Antivirus

Suojaa viruksia, matoja ja troijalaisia vastaan. Antaa suojaa myös vakoiluohjelmien latausta vastaan. (Security Profiles, 2023)

2.3.2 Vulnerability protection

Estää luvattomat pääsyt järjestelmään ja yritykset käyttää järjestelmän vikoja hyväkseen. (Security Profiles, 2023)

2.3.3 Anti-Spyware

Auttaa huomaamaan ja estämään haitallisen liikenteen lähtemisen spywarelle altistuneesta isännästä verkon sisällä. (Security Profiles, 2023)

2.3.4 File Blocking

Näillä profiileilla annetaan hälytys tai blokataan määritellyt tiedostotyyppit, määritellyille sovelluksille. Blokkauksen voi määrittää lähettämiseen, lataamiseen tai molempiin. Voit myös tehdä oman

sivun, joka ilmestyy blokkauksen / hälytyksen yhteydessä antaen käyttäjälle mahdollisuuden miettiä uusiksi haluaako todella ladata tiedoston tms. (Security Profiles, 2023)

2.3.5 Wildfire Analysis

WildFire antaa turvaa nollapäivähaittaohjelmia (zero-day malware) vastaan. (WildFire Overview, 2022)

Paloalto välittää tuntemattomia tiedostoja tai sähköpostilinkkejä analysoitavaksi WildFirelle. Voit määrittää tiedostot mitkä välitetään WildFirelle analysoitavaksi tiedostotyyppin, liikenteen suunnan (lataus / lähetys) tai sovelluksen perusteella. (Security Profiles, 2023)

2.4 Mitre ATT&CK

MITRE Corporation on 1958 perustettu yhdysvaltalainen liittovaltion rahoittama, voittoa tavoittelematon tutkimus- ja kehitysorganisaatio. Se toimii yleisen edun hyväksi ja ratkaisee ongelmia turvallisemman maailman puolesta. Mitrellä on rooleja tieto- ja kyberturvan lisäksi muun muassa puolustus-, ilmailu- ja tiedustelun osa-alueilla. (Toivonen 2022, 8.)

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) on tietokanta/viitekehys, jossa listataan erilaisia tekniikoita ja taktiikoita, joita hyökkääjät voivat käyttää hyökkäyksen eri vaiheissa. Ne perustuvat tosielämän havaintoihin. ATT&CK-tietokantaa käytetään maailmanlaajuisesti perustana erityisten uhkamallien ja -menetelmien kehittämiseksi yksityisellä sektorilla kuin myös hallinnossa sekä kyberturvallisuuden tuote- ja palveluyhteisössä. (MITRE ATT&CK 2023.)

2.5 Uhkatieto (Threat Intelligence)

Uhkatiedoksi voidaan luokitella mikä tahansa tietoturvaauhkilta suojautumiseen auttava tieto. Uhkatietoja esimerkiksi ovat taktiikat, tekniikat ja menetelmät, joita uhkatoimija käyttää tietoverkko-hyökkäyksessä sekä uhkatietoraportit eli tiettyyn kontekstiin rakennettu, analysoitu tai aggregoitu uhkatieto ja tunnistetiedot, kuten IP-osoite, haittaohjelman tiiviste tai URL-osoite. (Toivonen 2022, 5)

Uhkatiedon avulla saadaan tietoa, miten esimerkiksi tunnistaa mahdolliset uhat, kuka organisaa-tiota vastaan hyökkää, mikä on hyökkääjän motiivi, ja millaiset toimet tai käyttäytyminen heillä on (Toivonen 2022, 7).

Nykyaikaisena tietoturva- tai kyberuhkilta suojautumisena voidaan pitää menetelmää, jossa uhka-tieto ohjaa suojautumista ja tapoja, joiden avulla voidaan ennakoida, estää ja havaita tietoverkko-hyökkäyksiä sekä reagoida niihin. Vastakeinona voidaan määrittää minkä tahansa prosessin tai tek-nologian, joka on kehitetty estämään tai kompensoimaan tietoverkkohyökkäyksiä. (Toivonen 2022, 7.)

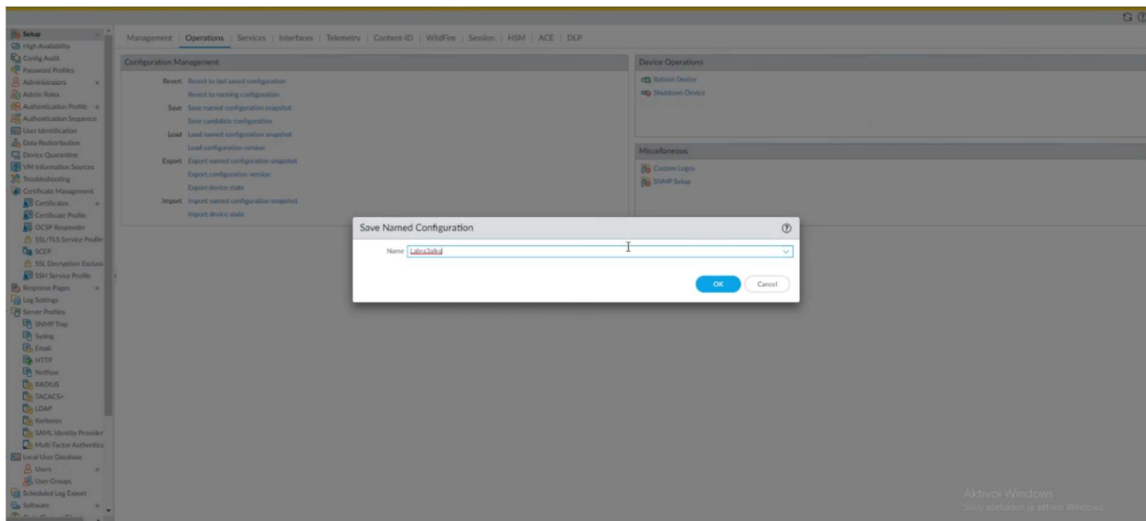
Esimerkiksi Mitren ATT&CK-viitekehys on tietokanta, joka pohjautuu objektimalliin ja objektien vä-lisiin suhteisiin. Kokonaisuutena ATT&CK kuvaa uhkatoimijoiden tietoverkkohyökkäyksissä käyttä-miä offensiivisia ATT&CK taktiikoita(tavoitteita) hyökkäyksessä ja offensiivisia ATT&CK-tekniikoita, joilla asetettu tavoite pyritään saavuttamaan. ATT&CK kuvaa lisäksi tekniikoiden toteuttamiseen mahdollisesti tarvittavia työkaluja ja ohjelmistoja, joita uhkatoimija voi käyttää hyökkäyksessä. Sekä ehkäisy- ja havainnointikeinoja, joilla pyritään kompensoimaan tai estämään offensiivisten tekniikoiden käyttöä. (Toivonen 2022, 8.)

3 DOKUMENTOINTI

3.1 Lab 3 – Paloalto Security Fe

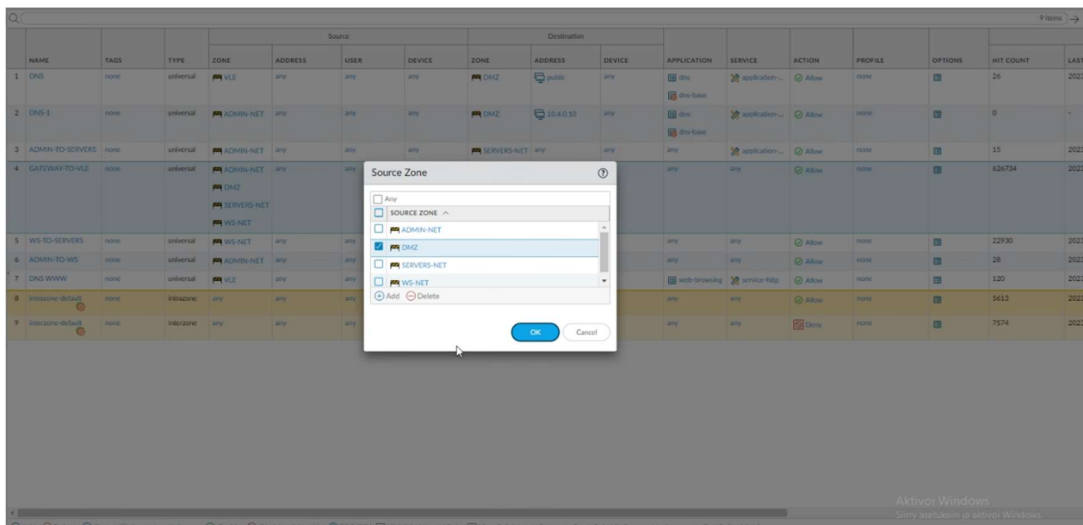
3.1.1 Ympäristön turvallisuuden lisääminen

Lab 3:n toteutus sujui nopeasti ja ilman suurempia ongelmia, lukuun ottamatta pientä pulmaa lab-ran loppuvaiheessa, johon palataan myöhemmin. Toteutus aloitettiin ottamalla snapshot alkutilan-teesta. Esitetty kuvassa 1.



Kuva 1. Snapshot alkutilanteesta.

Seuraavaksi tuli tehdä DMZ:stä VLE:hen kulkevaan liikenteeseen uusi sääntö, jossa Antivirus, vulnerability protection, anti-spyware, file blocking, sekä Wildfire analysis ovat päällä "Default" tai "basic" asetuksilla. Näistä asetuksista tarkemmat selitykset Teoria - kappaleessa. Sääntö tehdään "Policies -> Security" alle. Ennen tämän säännön luontia tuli kuitenkin jo olemassa olevasta "GATEWAY-TO-VLE" säännöstä ja sen alta "Source Zone" osiosta poistaa "DMZ zone", jotta uudessa säännössä olevat asetukset tulevat voimaan. "DMZ zone" poisto esitetty kuvissa 2-3.



Kuva 2. Delete DMZ.

	NAME	TAGS	TYPE	Source	Destination	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
1	DNS	none	universal	VLE	any	any	any	DMZ	public	any	26	2023-02
2	DNS-1	none	universal	ADMIN-NET	any	any	any	DMZ	10.4.0.10	any	0	-
3	ADMIN-TO-SERVERS	none	universal	ADMIN-NET	any	any	any	SERVERS-NET	any	any	15	2023-01
4	GATEWAY-TO-VLE	none	universal	ADMIN-NET	any	any	any	VLE	any	any	426755	2023-02
5	WS-TO-SERVERS	none	universal	WS-NET	any	any	any	SERVERS-NET	any	any	22930	2023-02
6	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	28	2023-01
7	DNS WWW	none	universal	VLE	any	any	any	DMZ	any	any	120	2023-02
8	Intranet-default	none	intranet	any	any	any	any	Intrazone	any	any	5613	2023-02
9	Interzone-default	none	interzone	any	any	any	any	any	any	any	7574	2023-01

Kuva 3. DMZ poistunut "GATEWAY-TO-VLE" - säännöstä.

DMZ zonen poiston jälkeen loimme edellä mainitun uuden säännön "DMZ-TO-VLE" nimellä. Tarvit-
tavat asetukset laitettiin voimaan säännön luonnissa "Actions" – välilehden alla olevassa "Profile
Settings" osiossa. Esitetty kuvassa 4.

Security Policy Rule

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

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: **None**

Other Settings

Schedule: **None**

QoS Marking: **None**

☐ Disable Server Response Inspection

Profile Setting

Profile Type: **Profiles**

Antivirus: **default**

Vulnerability Protection: **default**

Anti-Spyware: **default**

URL Filtering: **None**

File Blocking: **basic file blocking**

Data Filtering: **None**

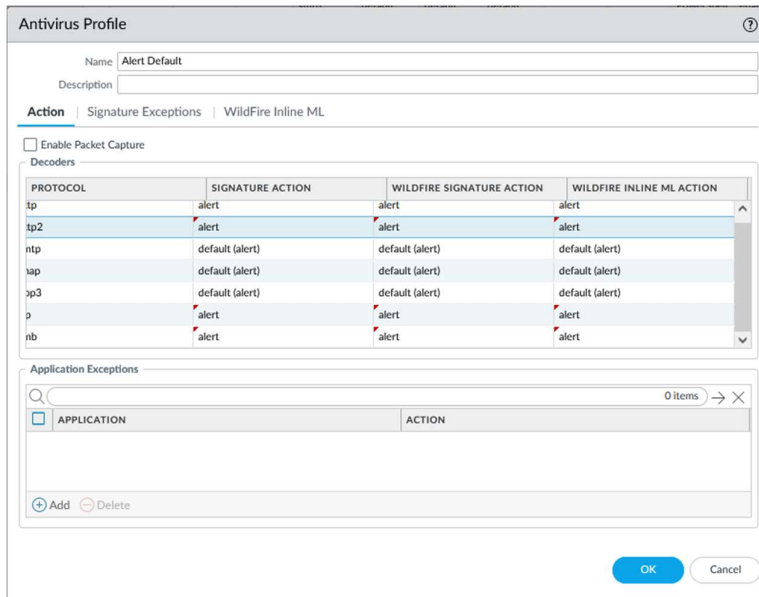
WildFire Analysis: **default**

OK **Cancel**

Kuva 4. Profile Settings.

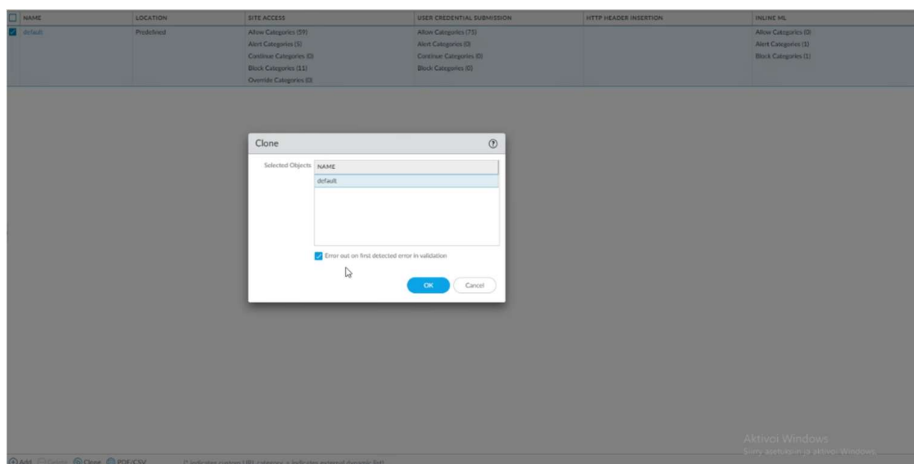
3.1.2 Antivirus hälytykset ja URL suodatus liikenteeseen WS-netistä VLE:hen

Jotta antivirus aiheuttaa vain hälytyksen, tuli luoda uusi sääntö "Objects -> Security Policies -> Antivirus" alle. Kopioimme olemassa olevan default – säännön "Alert Default" – nimellä, ja muokkasimme asetukset niin, että se aiheuttaa pelkkiä hälytyksiä. Esitetty kuvassa 5.



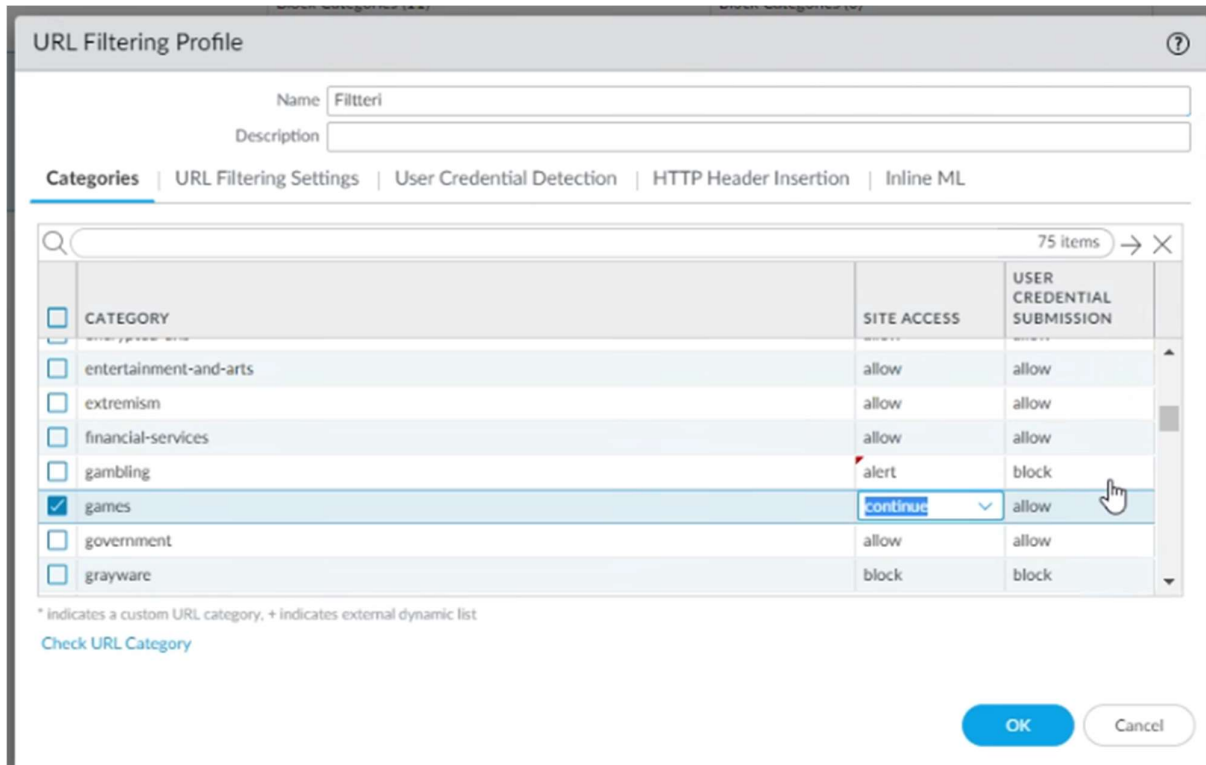
Kuva 5. Uusi Antivirus - sääntö.

Seuraavaksi teimme uuden URL-filteröinti profiilin kopioimalla olemassa olleen "default" profiilin nimellä "Filtteri". Esitetty kuvassa 6.



Kuva 6. URL-filteröinti profiilin kopiointi.

Tähän uuteen profiiliin tuli laittaa asetuksiksi yle.fi blokattu, tiedoston lataus osoitteesta eicar.com aiheuttaa antivirus hälytyksen, uhkapelisivut (gambling) aiheuttavat hälytyksen, sekä pelisivut (games) asetukseen "continue". Uhkapeli- ja pelisivujen asetukset esitetty kuvassa 7.



Kuva 7. Gambling ja games asetukset.

Jotta pystyimme lisäämään yle.fi ja eicar.com sivut filttiin, teimme "Objects -> Custom Object -> URL Category" alle molemmille oman kategorian nimillä "YleFiltteri" ja "EicarFiltteri". Eicarille filtoimme sekä eicar.com että eicar.org päätteet. Kategorioiden luonti esitetty kuvissa 8-10.

Custom URL Category ⓘ

Name: YleFilteri

Description:

Type: URL List

Matches any of the following URLs, domains or host names

2 items → ×

<input type="checkbox"/>	SITES
<input type="checkbox"/>	yle.fi
<input checked="" type="checkbox"/>	*yle.fi

+ Add - Delete | Import Export

Enter one entry per row.
Each entry may be of the form [www.example.com](#) or it could have wildcards like [www.*.com](#).

To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: [xyz.com/](#) matches only [xyz.com](#). For more info, see [URL Category Exceptions](#)

OK Cancel

Kuva 8. YleFilteri.

Custom URL Category ⓘ

Name: EicarFilteri

Description:

Type: URL List

Matches any of the following URLs, domains or host names

4 items → ×

<input type="checkbox"/>	SITES
<input type="checkbox"/>	eicar.com
<input type="checkbox"/>	eicar.org
<input type="checkbox"/>	*eicar.com
<input checked="" type="checkbox"/>	*eicar.org

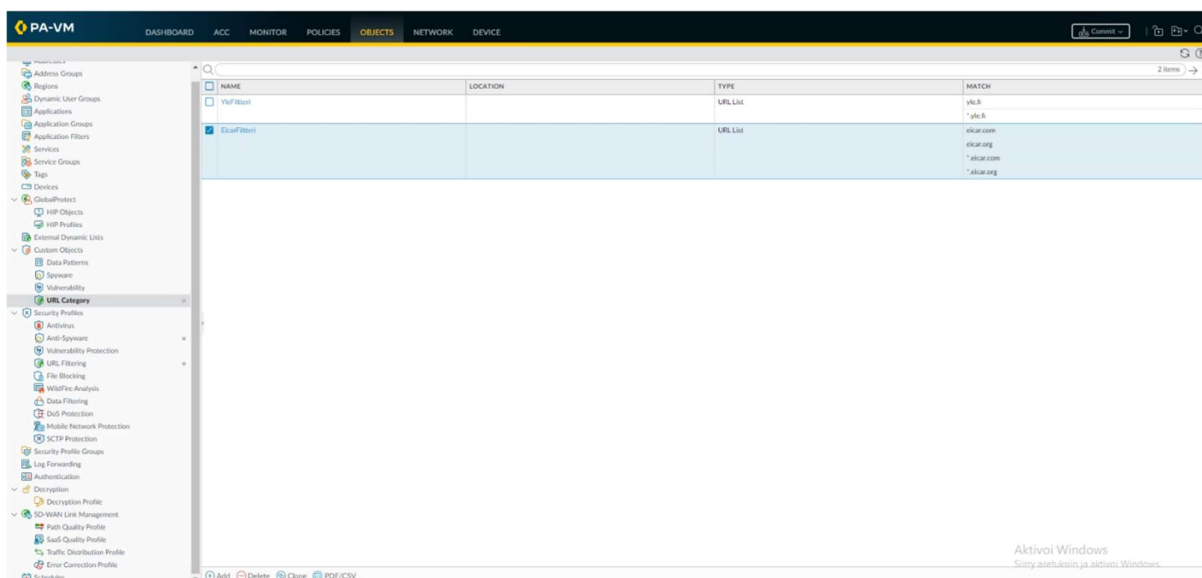
+ Add - Delete | Import Export

Enter one entry per row.
Each entry may be of the form [www.example.com](#) or it could have wildcards like [www.*.com](#).

To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: [xyz.com/](#) matches only [xyz.com](#). For more info, see [URL Category Exceptions](#)

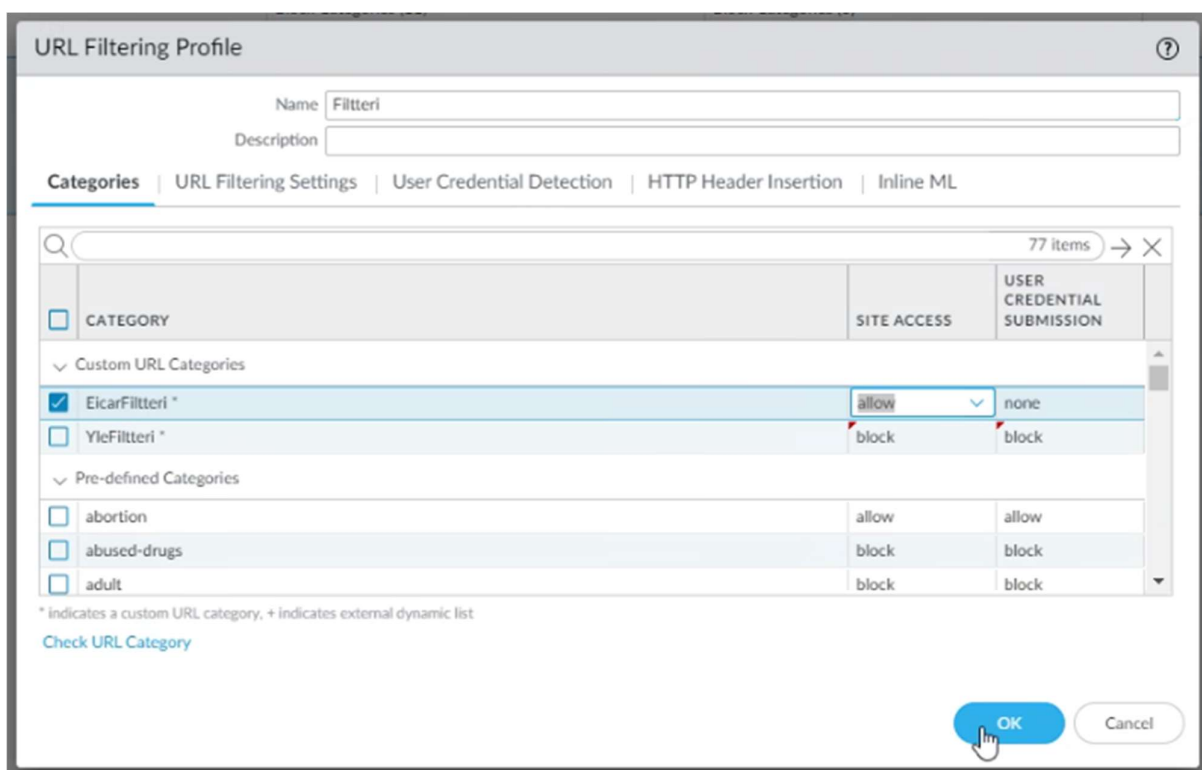
OK Cancel

Kuva 9. EicarFilteri.



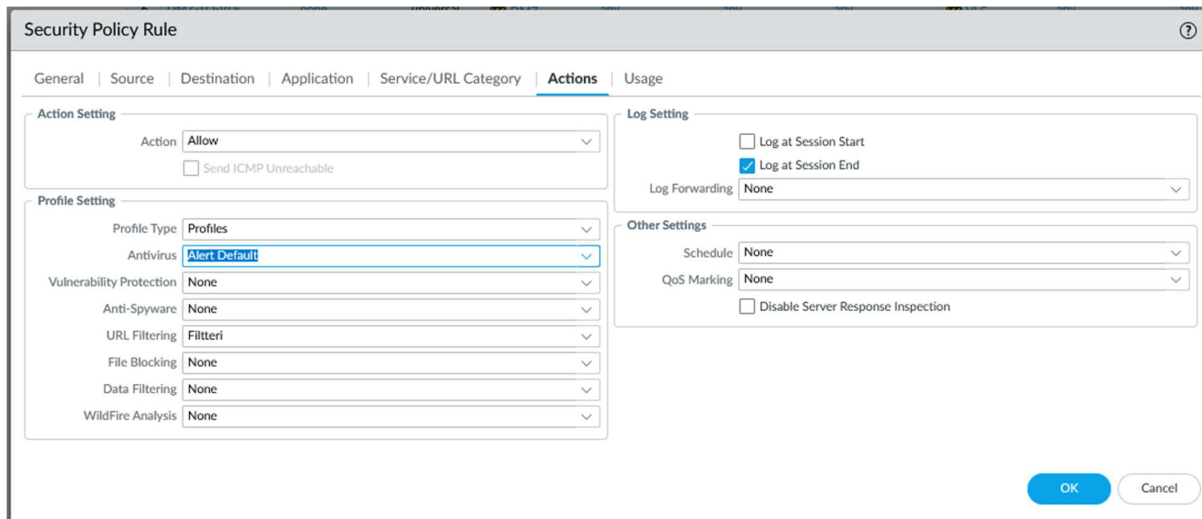
Kuva 10. Luodut kategoriat.

Kategorioiden luonnin jälkeen lisäsimme ne URL-filteriimme. Esitetty kuvassa 11.



Kuva 11. YleFilteri ja EicarFilteri lisätty.

Saadaksemme Antivirus säännön sekä URL-filteröinnin käyttöön, loimme jälleen uuden policyn "Policies -> Security" alle nimellä "WS-TO-VLE", jonka asetuksissa "Profile Settings" osiossa kohtaan "Antivirus" valitaan juuri luomamme "Alert Default" sääntö ja kohtaan "URL Filtering" teke-
mämme "Filterteri" profiili. Esitetty kuvassa 12.



Kuva 12. WS-TO-VLE asetukset.

3.1.3 Sertifikaatin luonti

Luodaan uusi sertifikaatti "Device -> Certificate Management -> Certificates" nimellä "PA Decryption Trusted". Kirjoitetaan "Common Name" kohtaan WS01 koneen default gateway, eli 10.1.0.10 ja laitetaan "Certificate Authority" asetus aktiiviseksi. Esitetty kuvassa 13.

Generate Certificate ?

Certificate Type: ☒ Local ☐ SCEP

Certificate Name: PA Decryption Trusted

Common Name: 10.1.0.10
IP or FQDN to appear on the certificate

Signed By: ▼

☒ Certificate Authority
☐ Block Private Key Export

OCSP Responder: ▼

Cryptographic Settings

Algorithm: RSA ▼
Number of Bits: 2048 ▼
Digest: sha256 ▼
Expiration (days): 365

Certificate Attributes

TYPE	VALUE
------	-------

+ Add - Delete

Generate Cancel

Kuva 13. Sertifikaatin luominen.

Sertifikaatin luomisen jälkeen avataan se uudelleen ja laitetaan ruksit "Forward Trust Certificate" sekä "Trusted Root CA" kohtiin. Esitetty kuvassa 14.

Certificate information ?

Name: PA Decryption Trusted

Subject: /CN=10.1.0.10

Issuer: /CN=10.1.0.10

Not Valid Before: Feb 7 08:55:38 2023 GMT

Not Valid After: Feb 7 08:55:38 2024 GMT

Algorithm: RSA

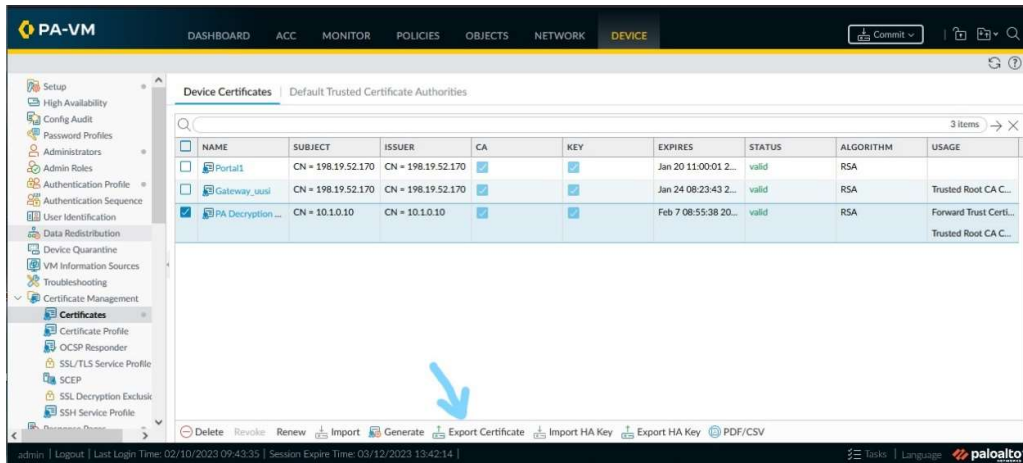
☒ Certificate Authority

☒ Forward Trust Certificate
☐ Forward Untrust Certificate
☒ Trusted Root CA

Revoke: OK Cancel

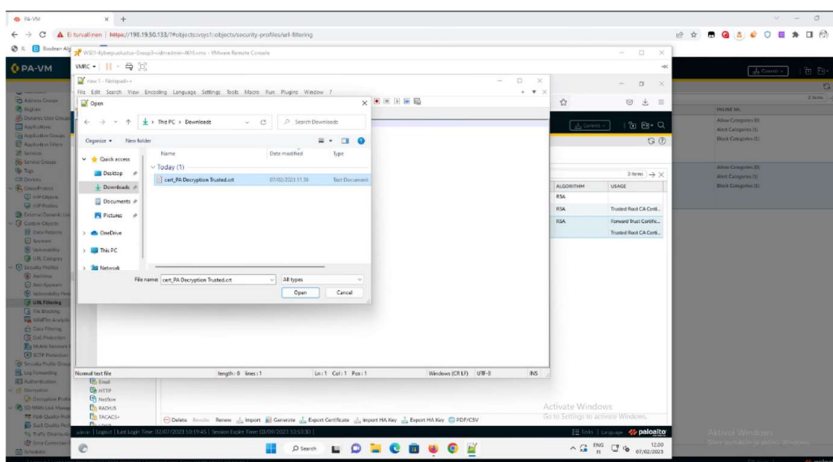
Kuva 14. "Forward Trust Certificate" sekä "Trusted Root CA" aktiiviseksi.

Kirjautuimme WS01 koneella PaloAltoon ja lataimme luodun sertifikaatin koneelle. Onnistuu klikkaamalla sertifikaatti aktiiviseksi ja sivun alalaidasta valitsemalla ”Export Certificate”. Esitetty kuvassa 15.

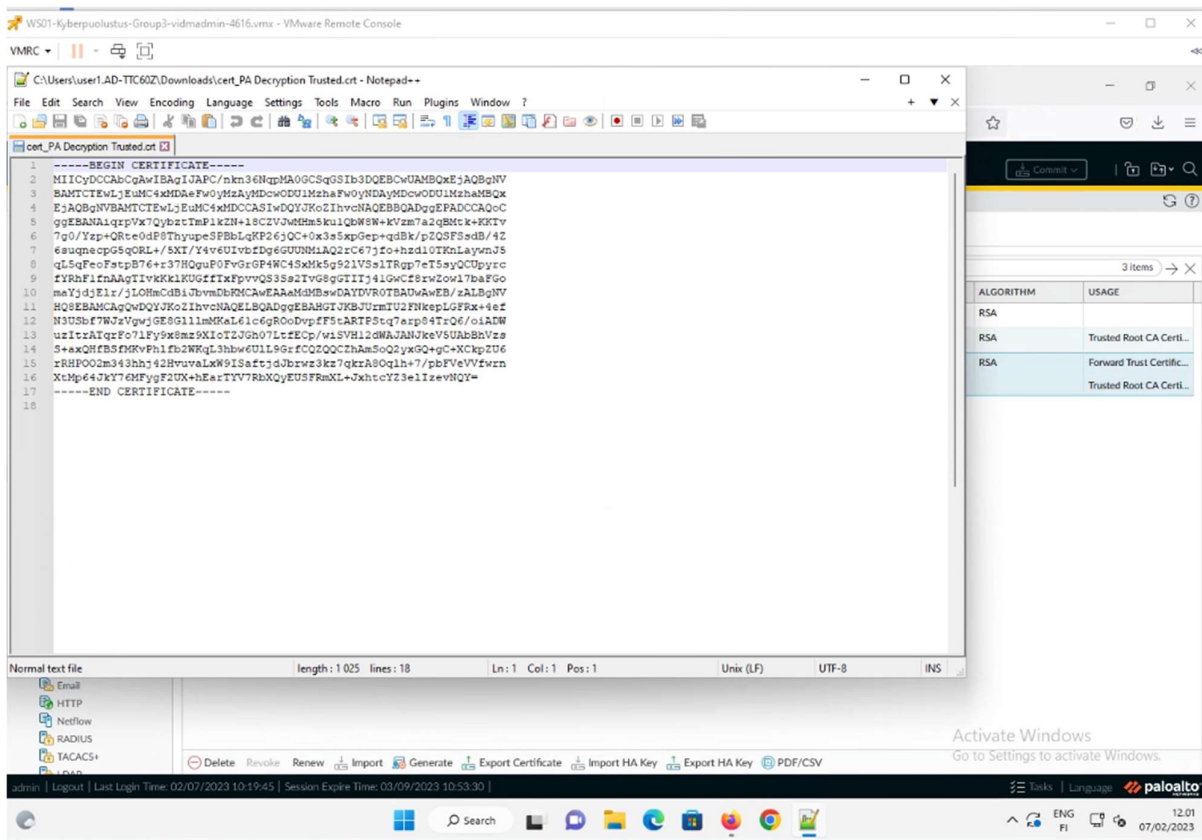


Kuva 15. Ladataan sertifikaatti WS01 koneelle.

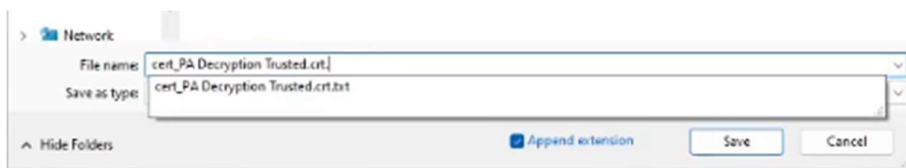
Koska ladattu tiedosto tallentuu oletuksena tekstitiedosto-muodossa, avasimme sen Notepad++ ohjelmalla ja tallensimme sen sertifikaatti – muotoon lisäämällä tallennusvaiheessa tiedoston nimen perään pisteen, valitsemalla tiedostotyyppiä ”All types” sekä laittamalla ”Append Extension” aktiiviseksi. Eli tiedosto ”cert_PA Decryption Trusted.crt” tallennetaan nimellä ”cert_PA Decryption Trusted.crt”. Esitetty kuvissa 16-18.



Kuva 16. Avataan ladattu tiedosto Notepad++ ohjelmalla.

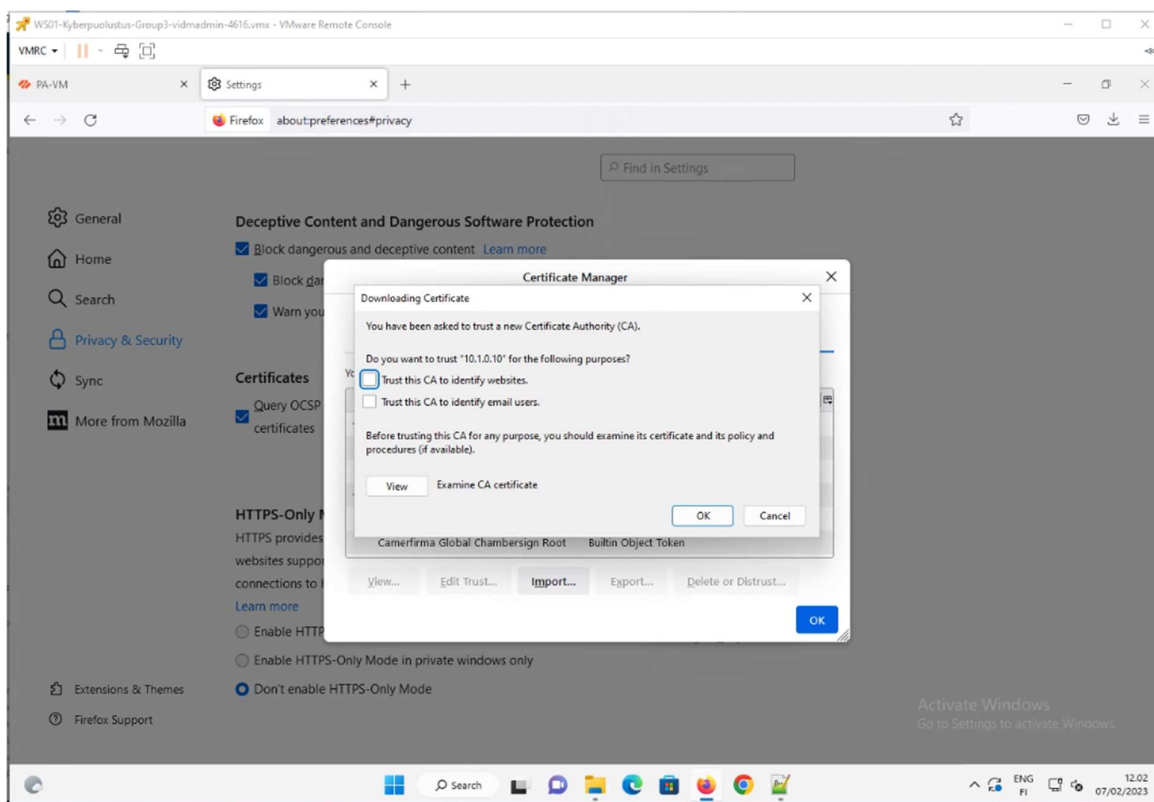


Kuva 17. Tiedosto avattuna.

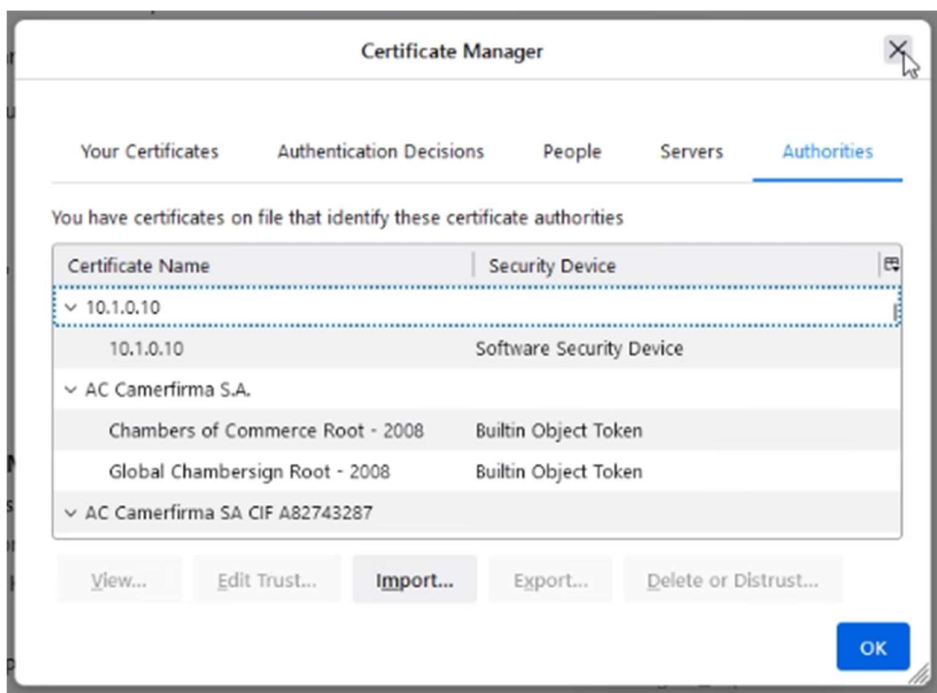


Kuva 18. Tallennetaan sertifikaatti-muodossa.

Sertifikaatin tallennuksen jälkeen laitoimme sen käyttöön Firefoxissa menemällä ”Settings -> Privacy & Security -> Certificates -> View Certificates”, josta ”Import” nappia painamalla voimme valita tiedoston koneelta. Kun tiedosto valitaan, laitetaan avautuvassa ikkunassa ”Trust this CA to identify websites.” aktiiviseksi. Esitetty kuvissa 19-20.



Kuva 19. "Trust this CA to identify websites" aktiiviseksi.



Kuva 20. Lisätty sertifikaatti näkyy listalla.

3.1.4 Decryption

Loimme uuden decryption - säännön "Policies → Decryption" alta painamalla "Add" sivun alalaidassa. Nimeksi annoimme "Purettu liikenne WS-NET-TO-VLE". Esitetty kuvassa 21.

The screenshot shows the 'Decryption Policy Rule' configuration window with the 'General' tab selected. The 'Name' field is filled with 'Purettu liikenne WS-NET-TO-VLE'. The 'Description' field is empty. The 'Tags' dropdown is set to 'None'. The 'Group Rules By Tag' dropdown is also set to 'None'. The 'Audit Comment' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons. A link for 'Audit Comment Archive' is visible below the audit comment field.

Kuva 21. Nimi decryption säännölle.

Source - > Source Zone: "WS-NET". Esitetty kuvassa 22.

The screenshot shows the 'Decryption Policy Rule' configuration window with the 'Source' tab selected. The 'General' tab is also visible. The 'Source' section has four columns: 'Any', 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE'. The 'Any' column is checked. The 'SOURCE ADDRESS' column is also checked. The 'SOURCE USER' and 'SOURCE DEVICE' columns are not checked. The 'Any' column has a dropdown menu set to 'any'. The 'SOURCE ADDRESS' column has a dropdown menu set to 'any'. The 'SOURCE USER' and 'SOURCE DEVICE' columns have dropdown menus set to 'any'. At the bottom, there are 'Add' and 'Delete' buttons for each column, and a 'Negate' checkbox. At the bottom right, there are 'OK' and 'Cancel' buttons.

Kuva 22. Source Zone.

Destination -> Destination Zone: "VLE". Esitetty kuvassa 23.

Decryption Policy Rule ⓘ

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

<input type="checkbox"/> Any <input checked="" type="checkbox"/> DESTINATION ZONE ^ <input type="checkbox"/> VLE <input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input checked="" type="checkbox"/> Any <input type="checkbox"/> DESTINATION ADDRESS ^ <input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input checked="" type="checkbox"/> Any <input type="checkbox"/> DESTINATION DEVICE ^ <input type="button" value="+ Add"/> <input type="button" value="- Delete"/>
--	---	--

☐ Negate

Kuva 23. Destination Zone.

URL Categoryyn lisäsimme aiemmin mainitut estot (Yle, Eicar, gambling, games). Esitetty kuvassa 24.

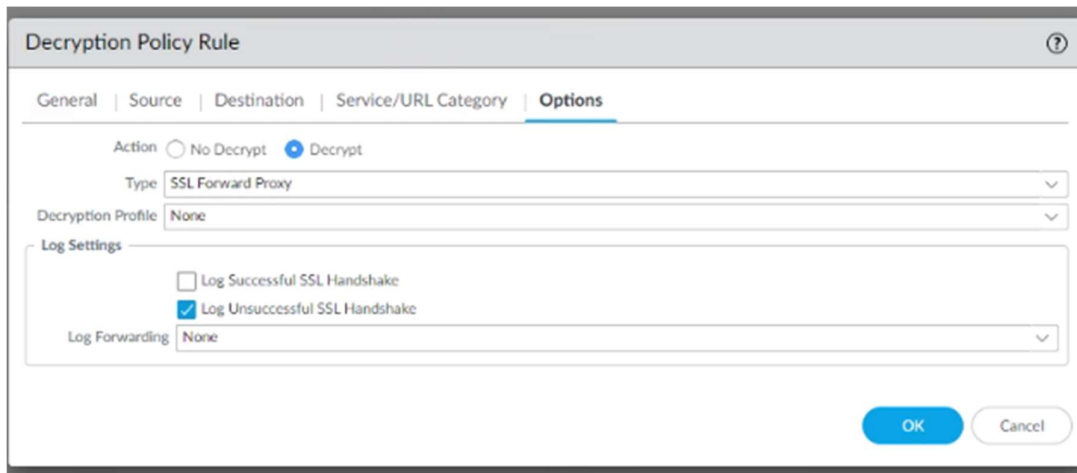
Decryption Policy Rule ⓘ

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

<input type="text" value="any"/> <input checked="" type="checkbox"/> SERVICE ^ <input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="checkbox"/> Any <input type="checkbox"/> URL CATEGORY ^ <input checked="" type="checkbox"/> EicarFilteri <input checked="" type="checkbox"/> YleFilteri <input type="checkbox"/> gambling <input checked="" type="checkbox"/> games <input type="button" value="+ Add"/> <input type="button" value="- Delete"/>
---	---

Kuva 24. URL Category.

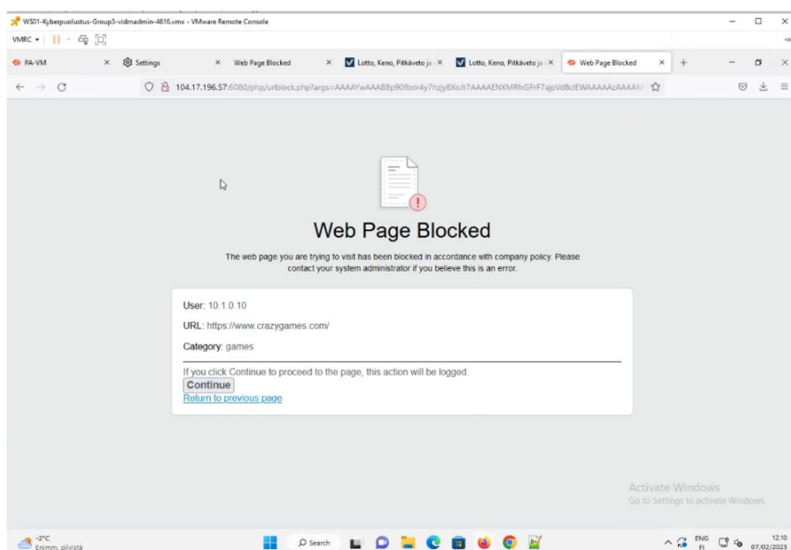
Options -> Log Settings: "Log Unsuccessful SSL Handshake" aktiiviseksi. Esitetty kuvassa 25.



Kuva 25. Log Settings.

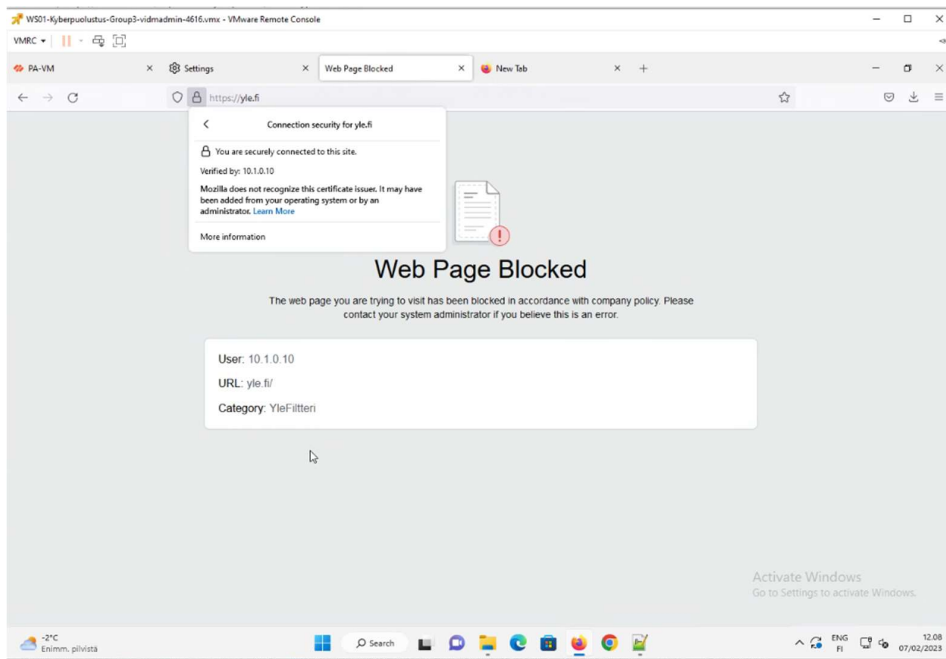
3.1.5 Testaus

Testasimme luotuja asetuksia Firefoxilla WS01 koneella. Ensimmäiseksi gaming. Kuvassa 26 näkyy, että pelisivusto on blokattu, mutta on mahdollista jatkaa sivulle "Continue" napilla.



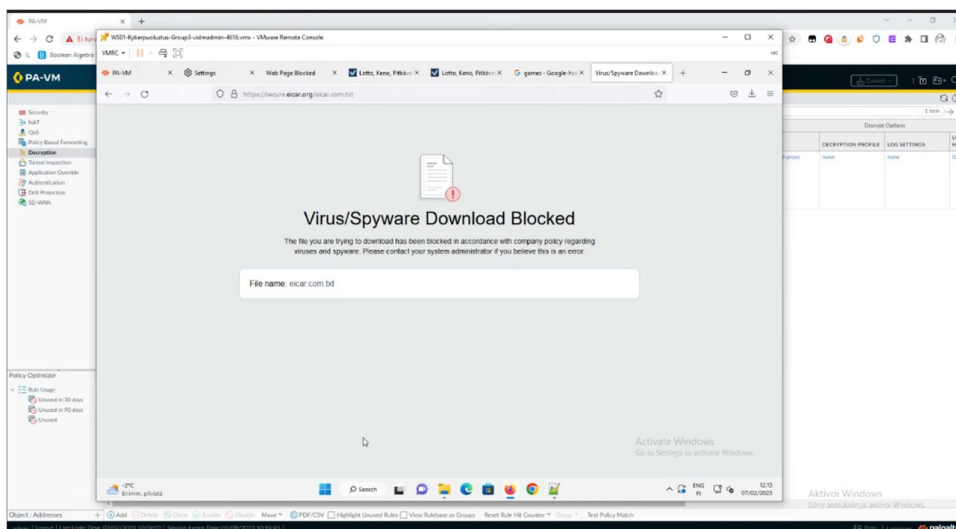
Kuva 26. Pelisivun onnistunut testaus.

Seuraavaksi yle.fi. Huomataan, että sivu blokattu onnistuneesti. Esitetty kuvassa 27.



Kuva 27. Yle.fi onnistunut testaus.

Kolmanneksi testasimme ladata tiedostoa eicarin sivuilta. Jälleen onnistunut testaus. Esitetty kuvassa 28.



Kuva 28. Eicar onnistunut testaus.

Tiedostojen latausyritykset eicar.comista näkyvät myös "Monitor -> Threat" alta. Esitetty kuvassa 29.

RECEIVE TIME	THREAT	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME	URL	HTT CON
02/07 11:16:12	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com		0
02/07 11:16:02	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com		0
02/07 11:15:52	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com		0
02/07 11:13:56	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com		0
02/07 11:13:46	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com		0
02/07 11:13:06	vlna	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	reset-sender	Critical	elcar.com.dat		0

Kuva 29. Tiedostojen latausyritykset näkyvät threat - sivulla.

Gambling sivut asetettiin aiheuttamaan vain hälytyksen (alert) ja ne näkyvät paikassa "Monitor -> URL Filtering". Esitetty kuvassa 30.

PA-VM

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

Manual

<

Kuva 30. Gambling sivujen hälytykset (alert).

3.1.6 Flood Protection

Teimme vielä extratehtävänä Flood Protectionin asettamisen. Ensiksi luodaan uusi Zone Protection profiili menemällä ”Network -> Zone Protection” ja painamalla ”Add” sivun alalaidassa. Nimeksi annoimme ”Flood Protection. Esitetty kuvassa 31.

The screenshot shows the 'Zone Protection Profile' configuration window. The 'Name' field is set to 'Flood Protection'. The 'Description' field is empty. The 'Flood Protection' tab is selected, showing settings for SYN, ICMP, and UDP attacks. Each attack type has a checkbox to enable it, an 'Action' dropdown (set to 'Random Early Drop' for SYN), and three input fields for 'Alarm Rate (connections/sec)', 'Activate (connections/sec)', and 'Maximum (connections/sec)'. The values are all set to 10000 for Alarm Rate and 40000 for Activate and Maximum. The 'ICMPv6' tab is also visible with similar settings. The 'OK' and 'Cancel' buttons are at the bottom right.

Kuva 31. Flood protection nimi.

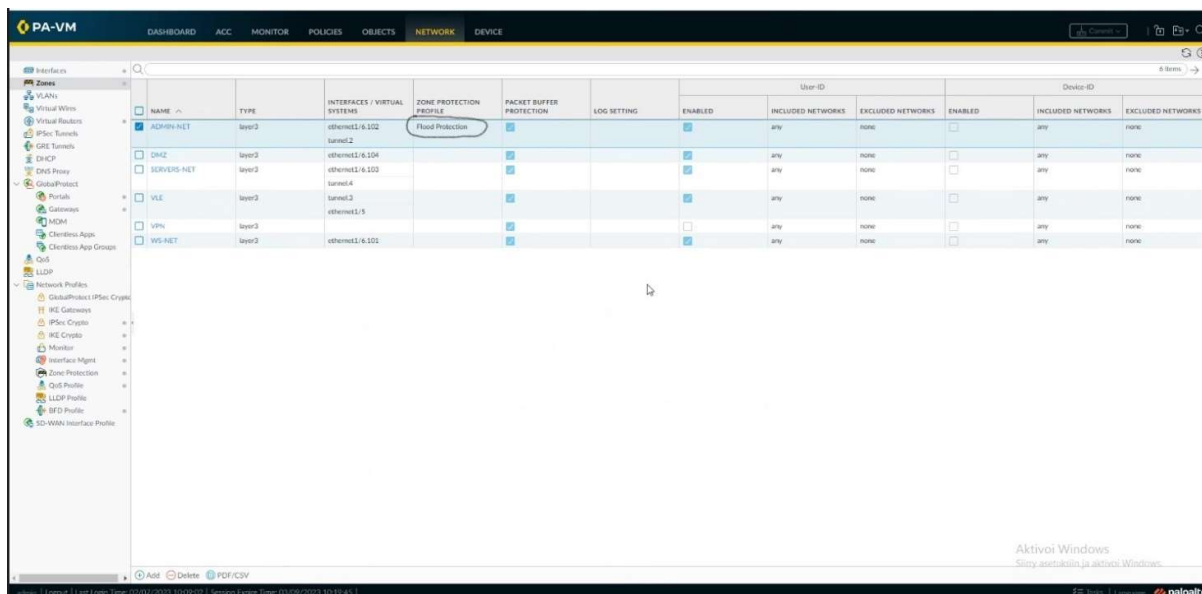
Reconnaissance Protectionin alta vaihdettiin ”Threshold (Events)” arvot kymmeneen ja ”Action” kaikkiin ”block”. Esitetty kuvassa 32.

The screenshot shows the 'Zone Protection Profile' configuration window with the 'Reconnaissance Protection' tab selected. It displays a table of reconnaissance attacks with columns for SCAN, ENABLE, ACTION, INTERVAL (SEC), and THRESHOLD (EVENTS). The actions are all set to 'block' and the thresholds are all set to 10. Below the table is a search bar and a section for 'SOURCE ADDRESS EXCLUSION' with a dropdown for 'ADDRESS TYPE' and a field for 'IP ADDRESS(ES)'. The 'Add' and 'Delete' buttons are at the bottom left, and the 'OK' and 'Cancel' buttons are at the bottom right.

SCAN	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)
UDP Port Scan	<input type="checkbox"/>	block	2	10
TCP Port Scan	<input type="checkbox"/>	block	2	10
Host Sweep	<input type="checkbox"/>	block	10	10

Kuva 32. Flood protection asetukset.

Liitettiin luotu profiili ADMIN-NETiin, näkyy kuvassa 33.



Kuva 33. Flood Profile liitetty ADMIN-NETiin.

Sallittiin liikenne ADMIN-NETistä DMZ:lle. Esitetty kuvassa 34.

7	WS-TO-SERVERS	none	universal	WS-NET	any	any	any	SERVERS-NET	any	any	any	any	Allow	none
8	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	any	any	Allow	none
9	ADMIN-TO-VLE	none	universal	VLE	any	any	any	DMZ	any	any	any	any	Allow	none
10	ADMIN-NET-TO-DMZ	none	universal	ADMIN-NET	any	any	any	DMZ	any	any	any	any	Allow	none
11	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Allow	none
12	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

Kuva 34. Sallittu liikenne ADMIN-NETistä DMZ:lle.

Testattiin nmapilla Kali-WS koneelta skannausta www-palvelimelle (10.4.0.11). Ensimmäinen skannaus meni läpi ja aiheutti hieman ihmetystä. Esitetty kuvassa 35.

```

kali@kali-ws: ~
File Actions Edit View Help
(kali@kali-ws)-[~]
$ nmap 10.4.0.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 11:35 EET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
done: 1 IP address (0 hosts up) scanned in 0.04 seconds

(kali@kali-ws)-[~]
$ nmap 10.4.0.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 11:35 EET
Nmap scan report for 10.4.0.11
Host is up (0.65s latency).
Not shown: 922 filtered tcp ports (no-response), 73 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
8080/tcp  open  http-proxy

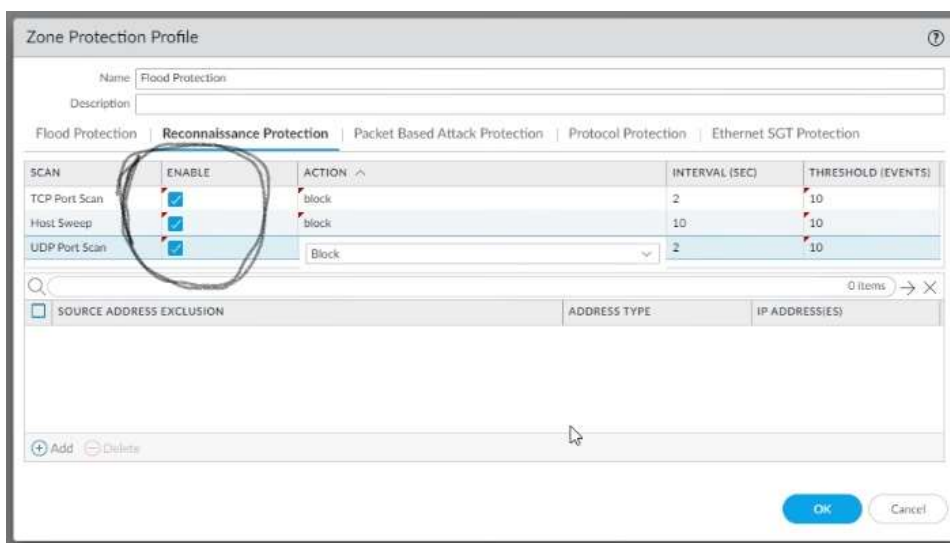
Nmap done: 1 IP address (1 host up) scanned in 69.28 seconds

$ ping 10.4.0.10

```

Kuva 35. Ensimmäinen skannausyritys meni läpi.

Hetken aikaa ihmeteltyämme tutkimme uudestaan aikaisemmin tekemäämme Zone Protection profiilia ja huomasimme, että oli jäänyt aktivoimatta luodut blokkaussäännöt. Esitetty kuvassa 36.



Kuva 36. Ympyröidyn osion sisällä olevista asetuksista mitään ei ollut aktivoitu.

Toinen harjoitustehtävä selkeästi valmisti URL-filtteröinnin teorialla tämän kolmannen harjoitustyön tekemiseen. Aihealue oli jo tuttu teoriassa ja päästiin toteuttamaan URL-filtteröinti käytännössä. Harjoitustyön tekeminen oli kokonaisuudessaan ohjeistettu hyvin ja se ryhmän mielestä helppo toteuttaa. Flood protectioniin ei ollut suoraa ohjeistusta, mutta ymmärrys Palo Alton toimintaan on jo selkeästi ryhmällä syventynyt, jonka takia se saatiin myös toimimaan lähes ongelmitta. Hetken jouduimme miettimään miksi nmapilla tehty skannaus Kali-WS koneelta www-palvelimelle (10.4.0.11) meni läpi, mutta Zone Protection profiilia tarkastellessa huomasimme nopeasti, että luodut blokkauksäännöt oli vain jäänyt aktivoimatta ja ongelma ratkesi muutamassa minuutissa.

Harjoitustyö onnistuttiin tekemään viikko-ohjaustuntien aikana ja se oli mieluisa harjoitus kokonaisuudessaan. Palo Alton graafisen käyttöliittymän käyttö alkaa selkeästi nopeutumaan ryhmän jäsenillä sekä ongelmanratkaisu on tehokkaampaa, kun ymmärrämme tekemämme eri vaiheet sääntöjen luomisessa.

Lähteet

EICAR N.d. F-secure verkkosivut. Viitattu 10.2.2023. <https://www.f-secure.com/v-descs/eicar.shtml>

Nmap Reference Guide N.d. Viitattu 9.2.2023 <https://nmap.org/book/man.html>

MITRE ATT&CK® 2023. Mitre verkkosivut. Viitattu 11.2.2023. <https://attack.mitre.org/>

Security Profiles. 2023. Palo Alto verkkosivut. Viitattu 10.2.2023. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-profiles>

Toivonen, S. 2022. Tietoverkkohyökkäys. Opinnäytetyö, AMK.Hämeen Ammattikorkeakoulu, Tieto- ja viestintätekniikka, insinööri. Viitattu 11.2.2023. https://www.theseus.fi/bitstream/handle/10024/749470/Toivonen_Simo.pdf?sequence=2

WildFire Overview. 2022. Palo Alto verkkosivut. Viitattu 10.2.2023. <https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview>

