jamk

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)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuvat

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 käyttävät 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 tiedostotyypit, 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 tiedostotyypin, 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 kehittämiselle yksityisellä sektorilla kuin myös hallinnossa sekä kyberturvallisuuden tuote- ja palveluyhteisössä. (MITRE ATT&CK 2023.)

2.5 Uhkatieto (Threat Intelligence)

Uhkatiedoksi voidaan luokitella mikä tahansa tietoturvauhkilta suojautumiseen auttava tieto. Uhkatietoja esimerkiksi ovat taktiikat, tekniikat ja menetelmät, joita uhkatoimija käyttää tietoverkkohyökkäyksessä 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 organisaatiota 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 uhkatieto ohjaa suojautumista ja tapoja, joiden avulla voidaan ennakoida, estää ja havaita tietoverkkohyökkäyksiä sekä reagoida niihin. Vastakeinona voidaan määrittää minkä tahansa prosessin tai teknologian, joka on kehitetty estämään tai kompensoimaan tietoverkkohyökkäyksiä. (Toivonen 2022, 7.)

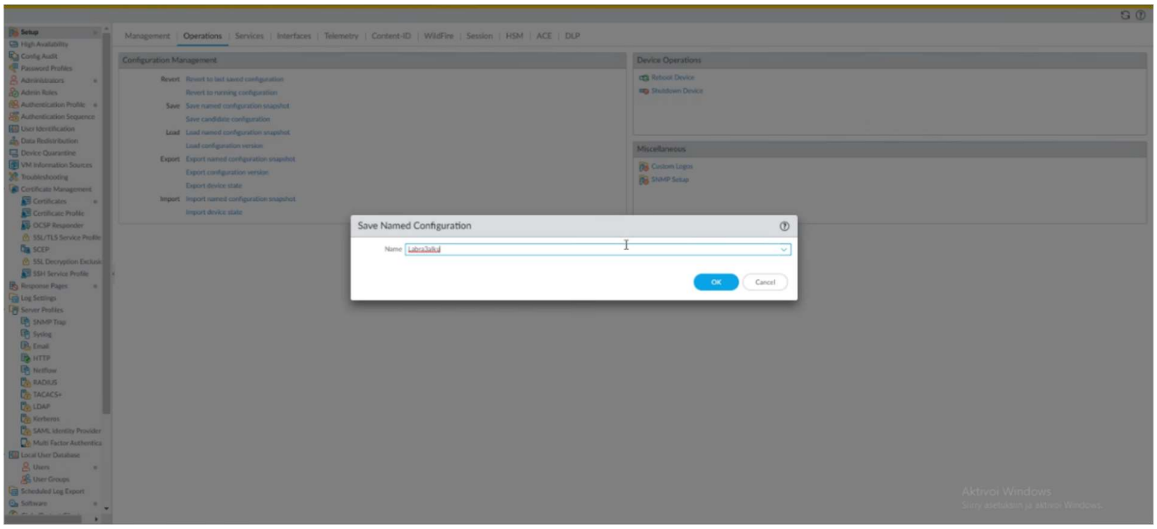
Esimerkiksi Mitren ATT&CK-viitekehys on tietokanta, joka pohjautuu objektimalliin ja objektien välisiin suhteisiin. Kokonaisuutena ATT&CK kuvaa uhkatoimijoiden tietoverkkohyökkäyksissä käyttämiä offensiivisia ATT&CK taktiikoita(tavoitteita) hyökkäyksessä ja offensiivisia ATT&CK-tekniikoita, joilla asetettu 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

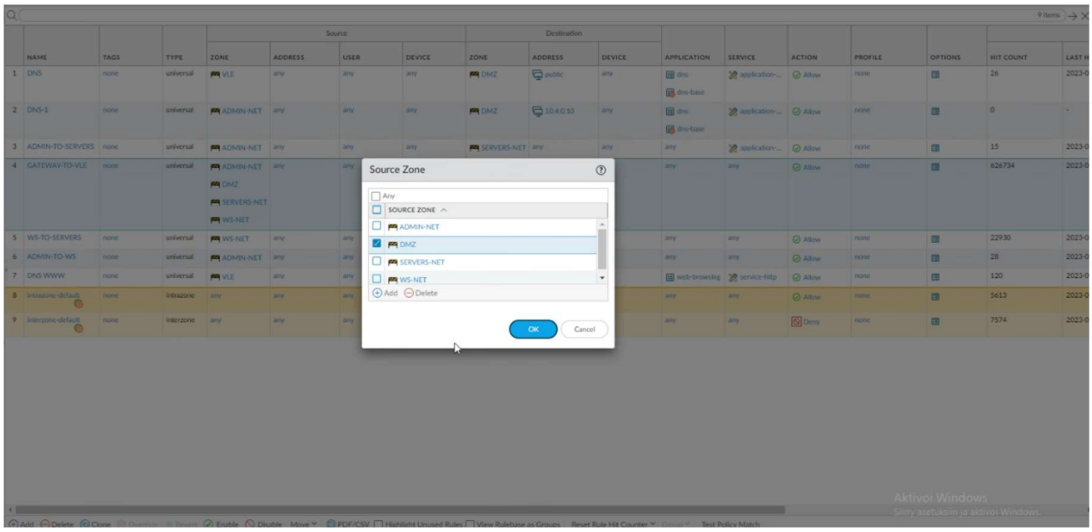
3.1.1 Ympäristön turvallisuuden lisääminen

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

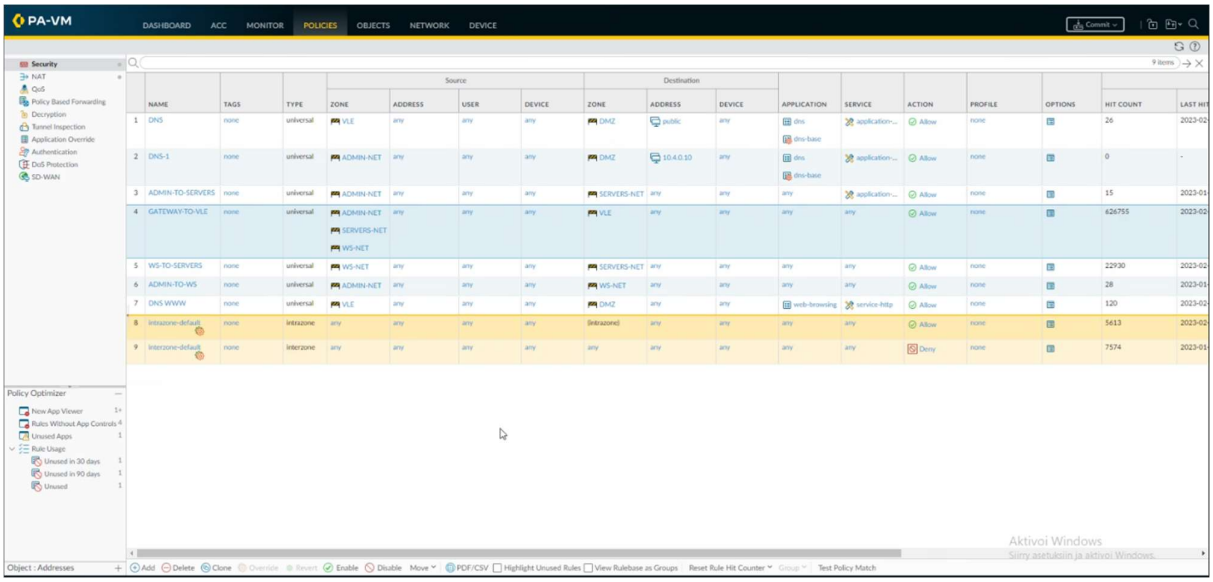


Kuva 1. Snapshot alkutilanteesta.

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.

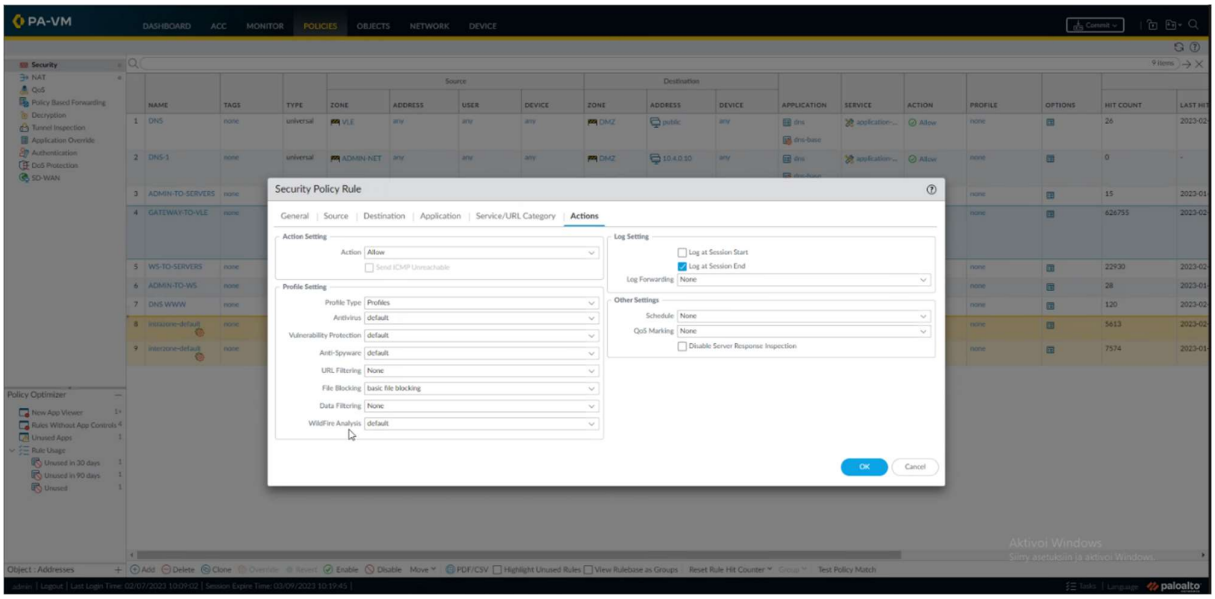


Kuva 2. Delete DMZ.



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

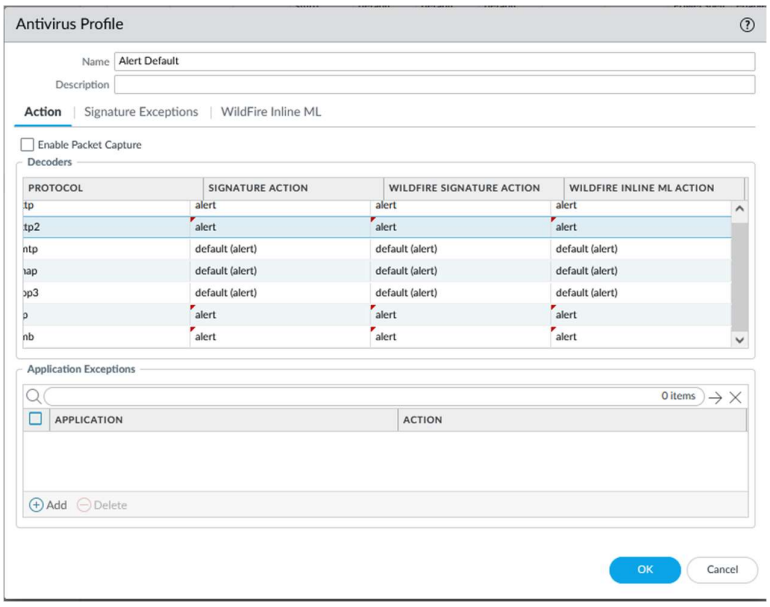
DMZ zonen poiston jälkeen loimme edellä mainitun uuden säännön ”DMZ-TO-VLE” nimellä. Tarvittavat asetukset laitettiin voimaan säännön luonnissa ”Actions” – välilehden alla olevassa ”Profile Settings” osiossa. Esitetty kuvassa 4.



Kuva 4. Profile Settings.

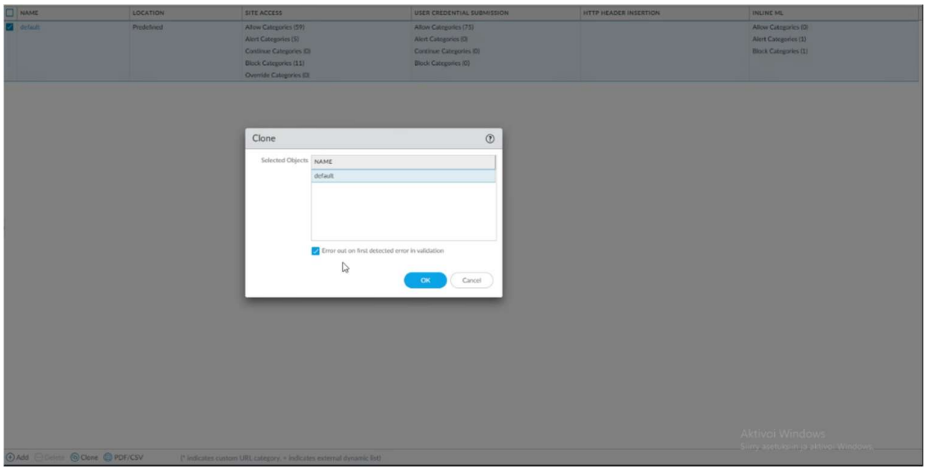
3.1.2 Antivirus hälytykset ja URL suodatus liikenteeseen WS-netistä VLE:hen

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.



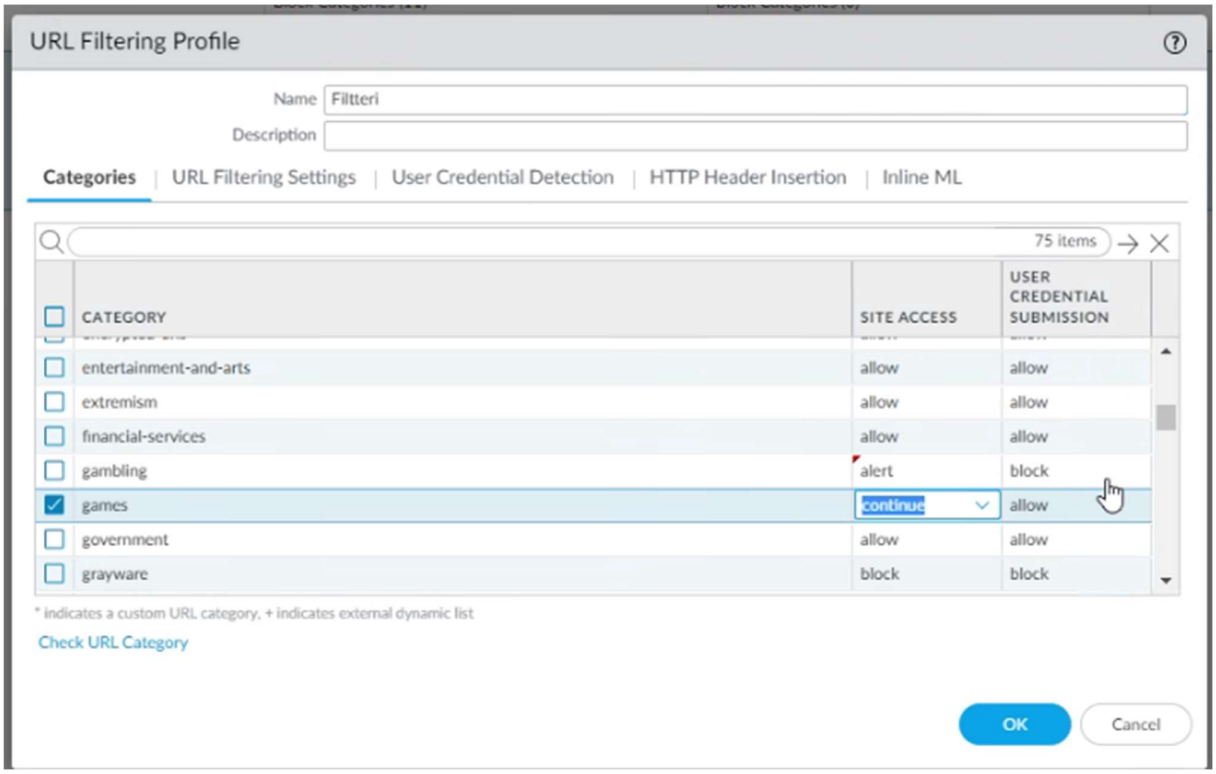
Kuva 5. Uusi Antivirus - sääntö.

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



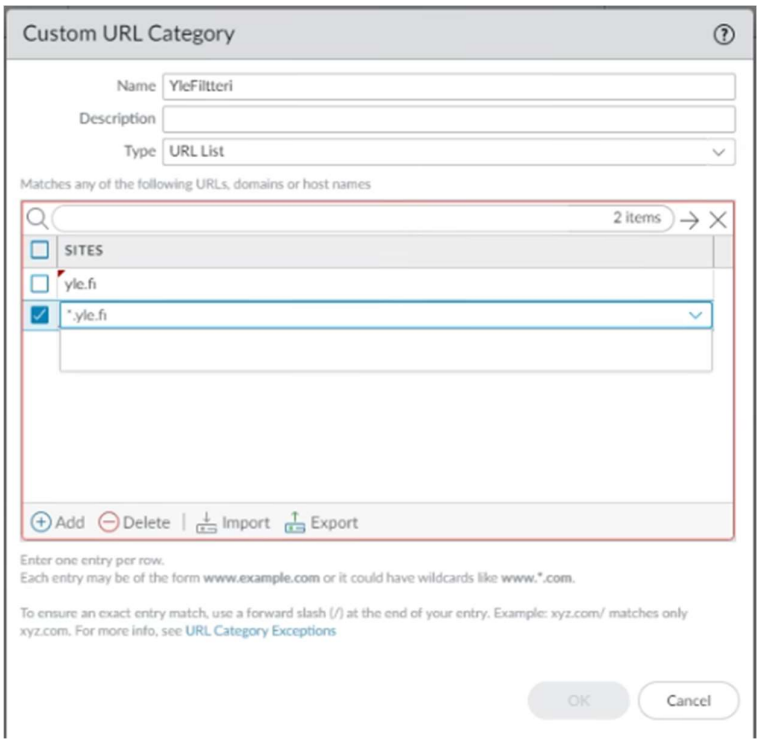
Kuva 6. URL-filteröinti profiilin kopiointi.

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.

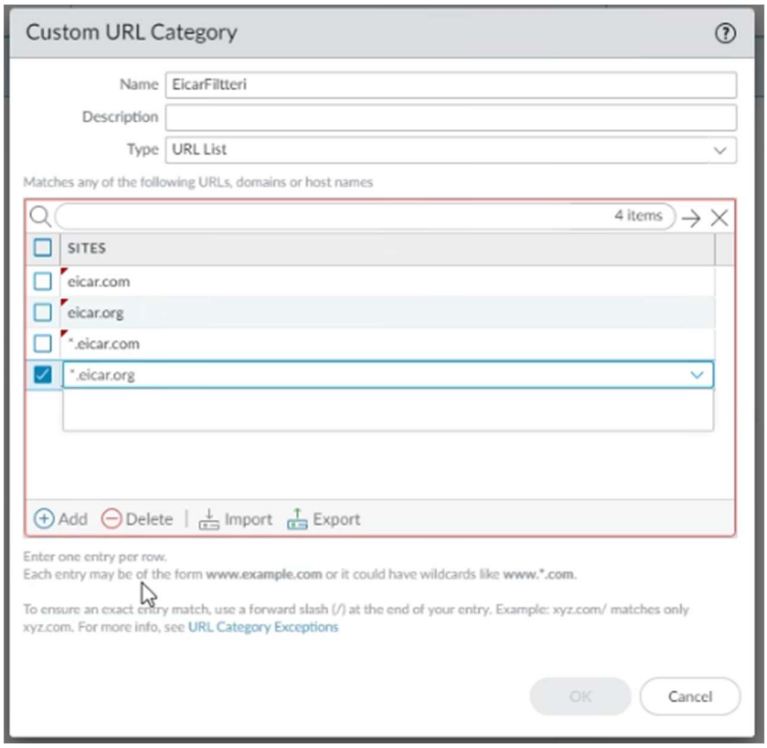


Kuva 7. Gambling ja games asetukset.

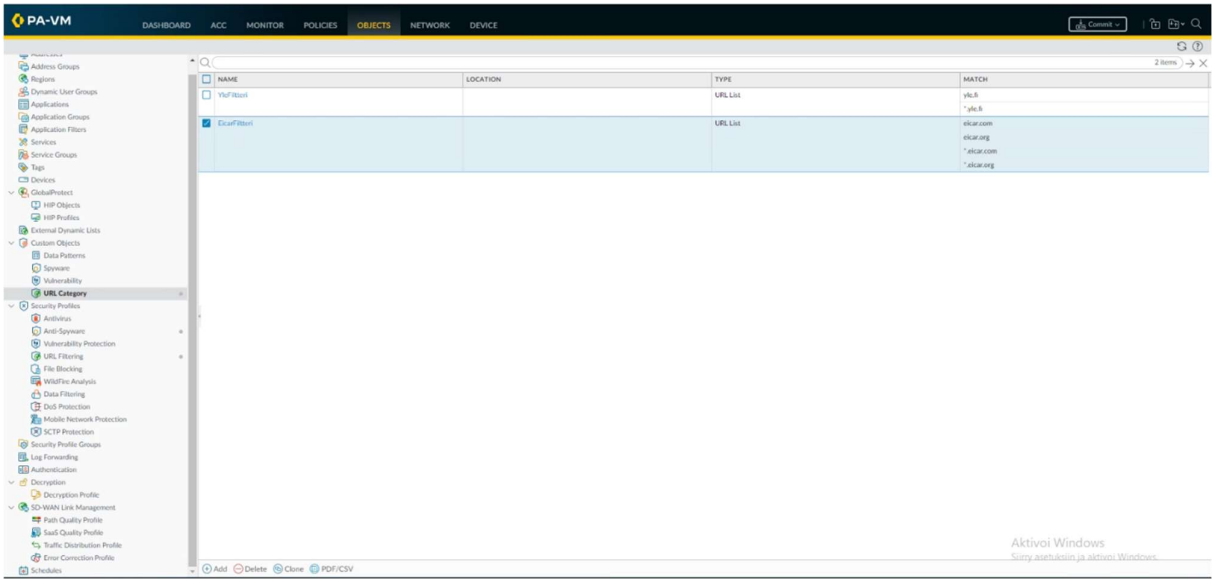
Jotta pystyimme lisäämään yle.fi ja eicar.com sivut filtteriin, teimme ”Objects - > Custom Object -> URL Category” alle molemmille oman kategorian nimillä ”YleFiltteri” ja ”EicarFiltteri”. Eicarille filteröimme sekä eicar.com että eicar.org päätteet. Kategorioiden luonti esitetty kuvissa 8-10.



Kuva 8. YleFiltteri.

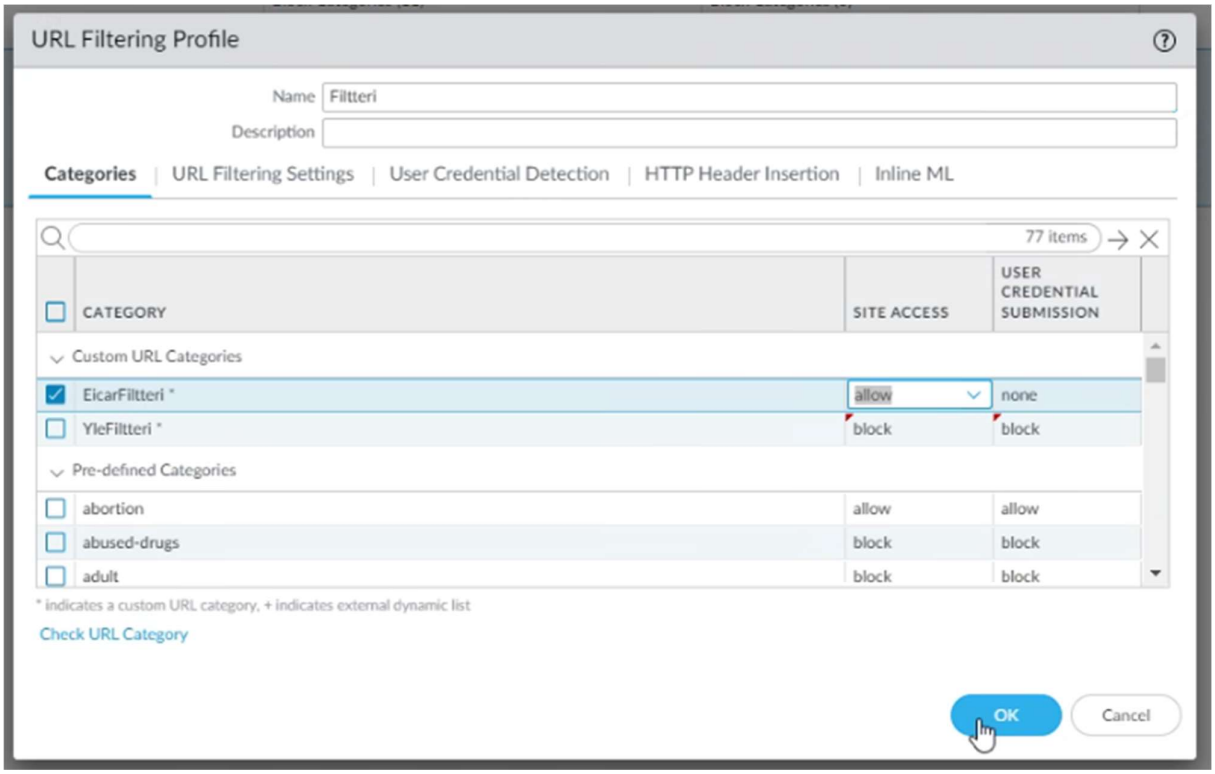


Kuva 9. EicarFiltteri.



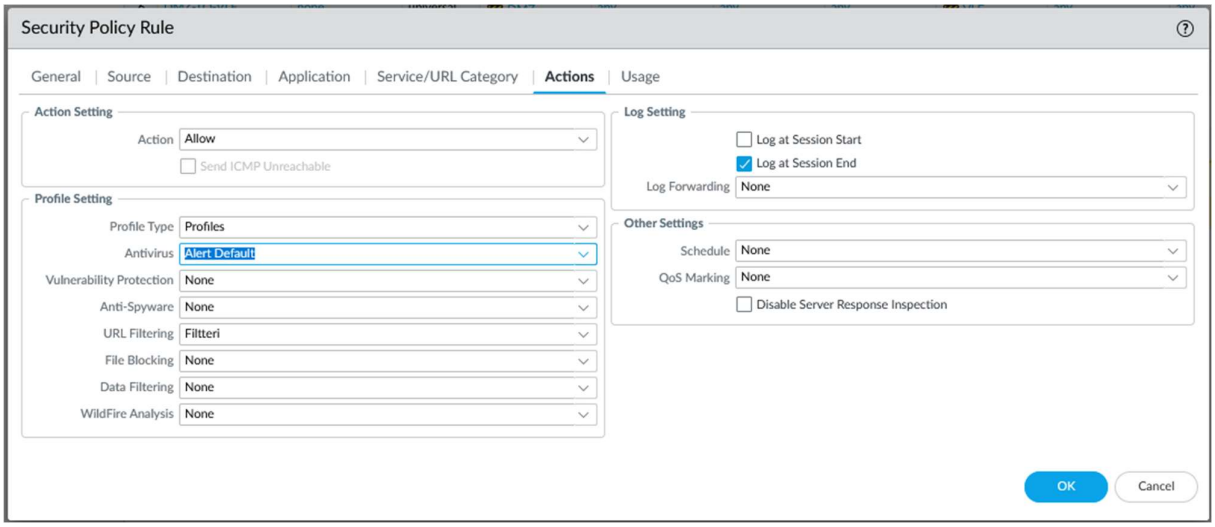
Kuva 10. Luodut kategoriat.

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



Kuva 11. YleFiltteri ja EicarFiltteri lisätty.

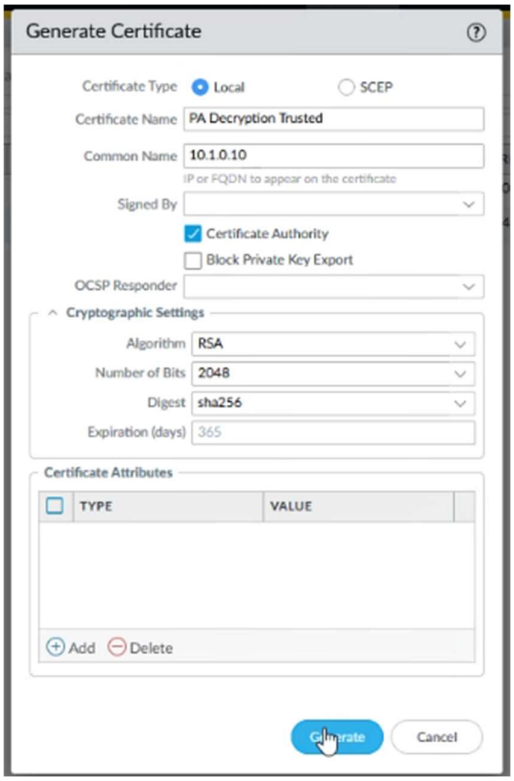
Saadaksemme Antivirus säännön sekä URL-filteröinnin käyttöön, loimme jälleen uuden policyn ”Policies -> Security” alle nimellä ”WS-TO-VLE”, jonka asetuksissa ”Profile Settings” osiossa kohtaan ”Antivirus” valitaan juuri luomamme ”Alert Default” sääntö ja kohtaan ”URL Filtering” tekemämme ”Filtteri” profiili.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



Kuva 12. WS-TO-VLE asetukset.

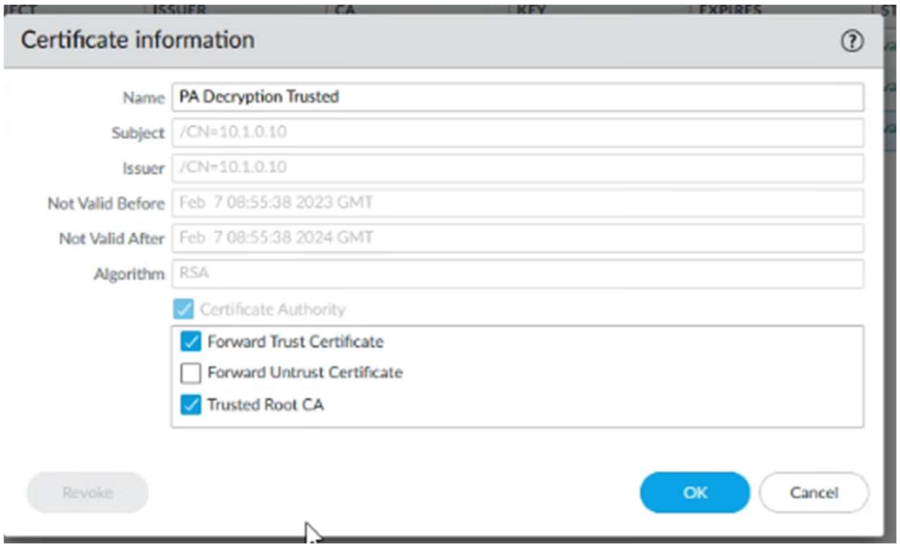
3.1.3 Sertifikaatin luonti

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 Auhtority” asetus aktiiviseksi. Esitetty kuvassa 13.



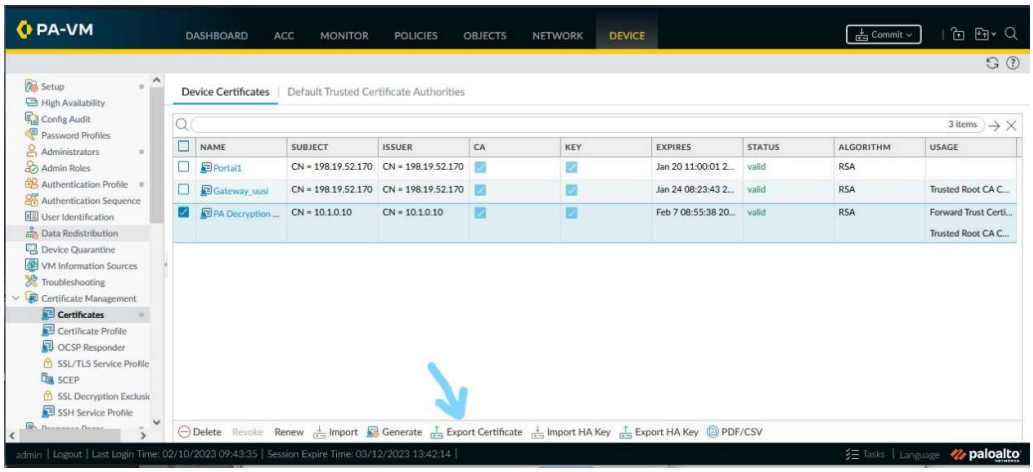
Kuva 13. Sertifikaatin luominen.

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



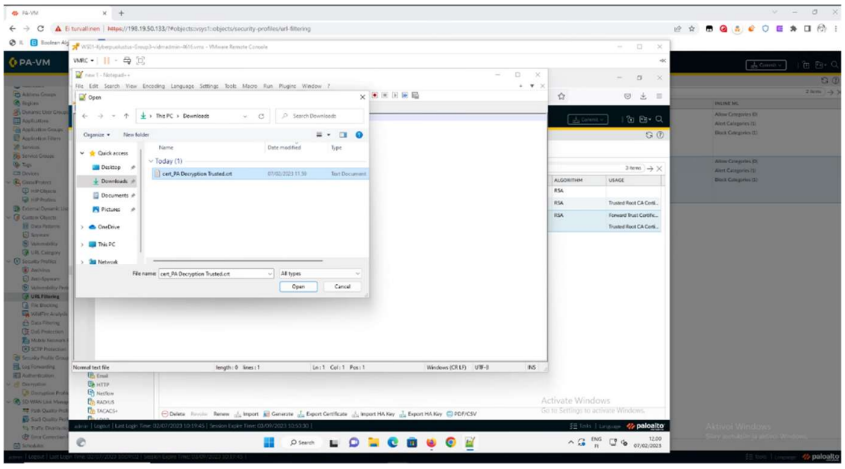
Kuva 14. "Forward Trust Certificate" sekä "Trusted Root CA" aktiiviseksi.

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

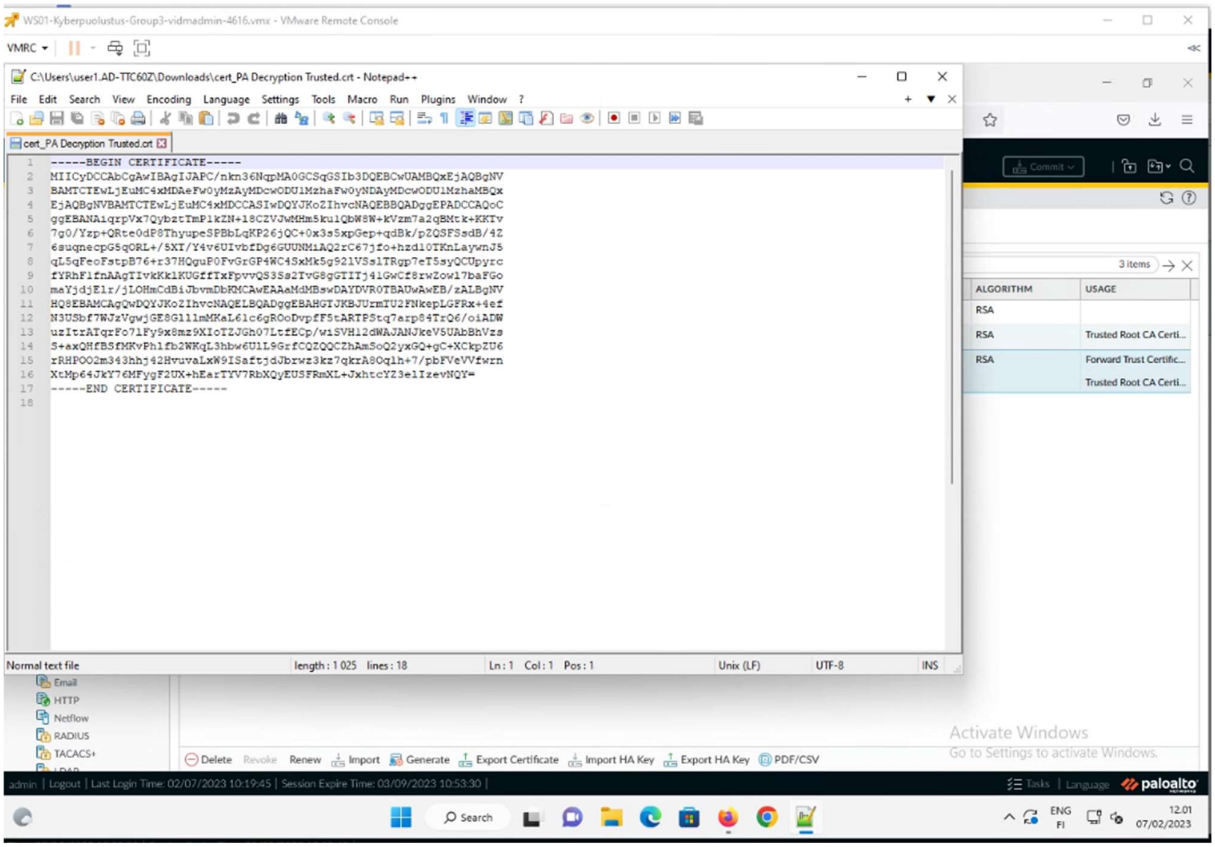


Kuva 15. Ladataan sertifikaatti WS01 koneelle.

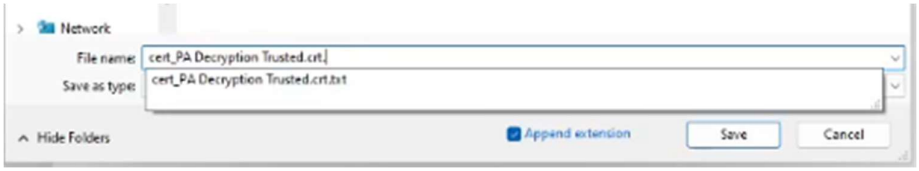
Koska ladattu tiedosto tallentuu oletuksena tekstitiedosto-muodossa, avasimme sen Notepad++ ohjelmalla ja tallensimme sen serftifikaatti – muotoon lisäämällä tallennusvaiheessa tiedoston nimen perään pisteen, valitsemalla tiedostotyypiksi ”All types” sekä laittamalla ”Append Extension” aktiiviseksi. 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.

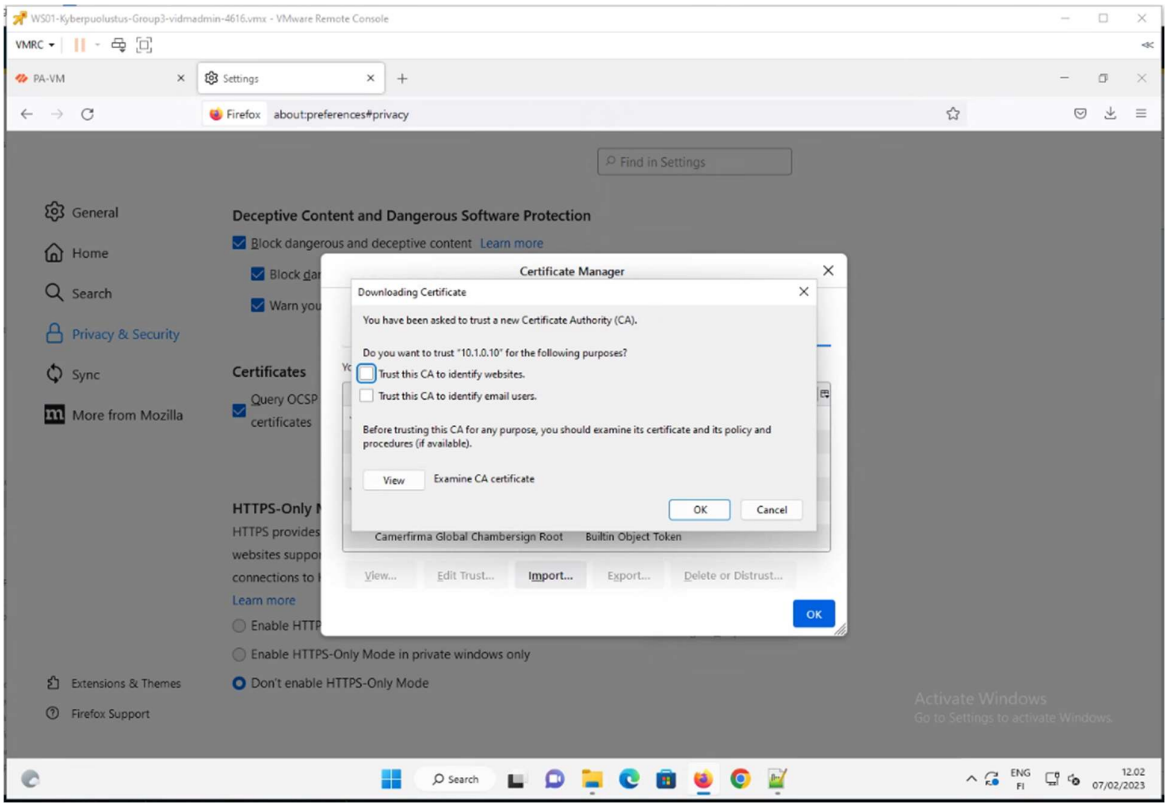


Kuva 17. Tiedosto avattuna.

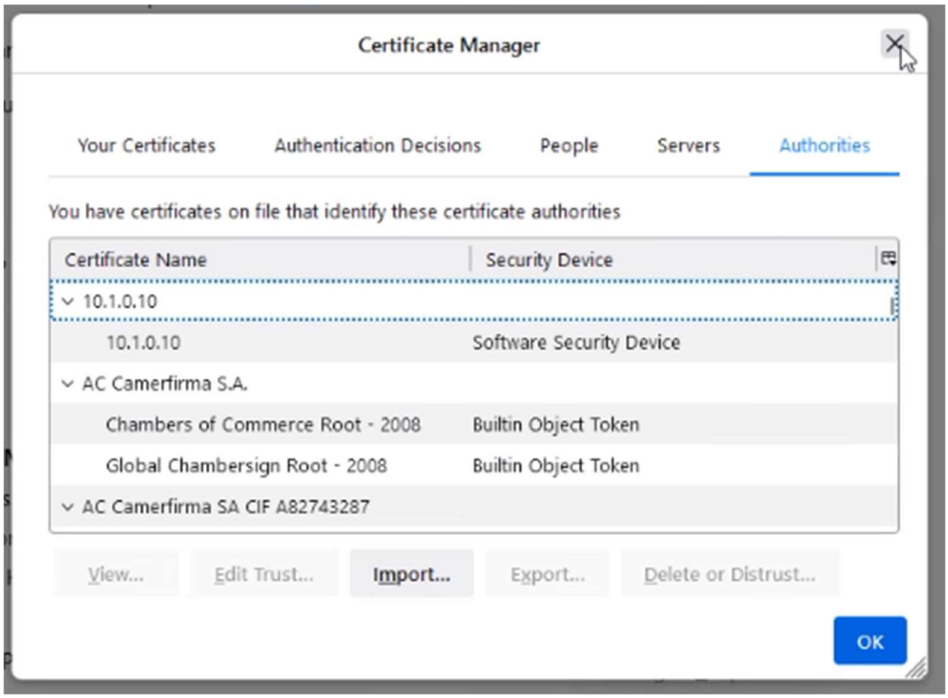


Kuva 18. Tallennetaan sertifikaatti-muodossa.

Sertifikaatin tallennuksen jälkeen laitoimme sen käyttöön Firefoxissa menemällä ”Settings - > Privacy & Sercurity -> 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.



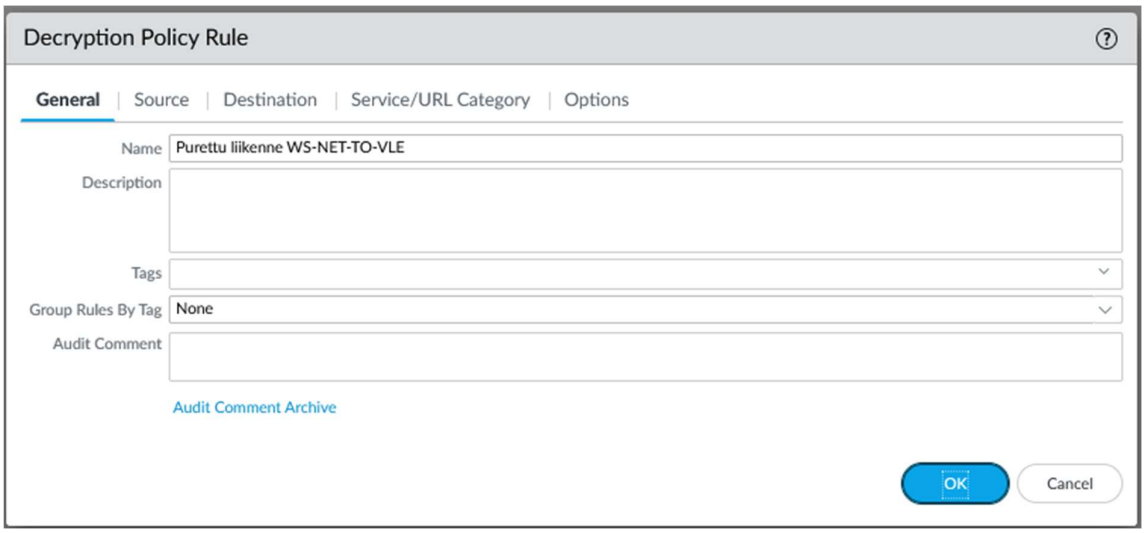
Kuva 19. "Trust this CA to identify websites" aktiiviseksi.



Kuva 20. Lisätty sertifikaatti näkyy listalla.

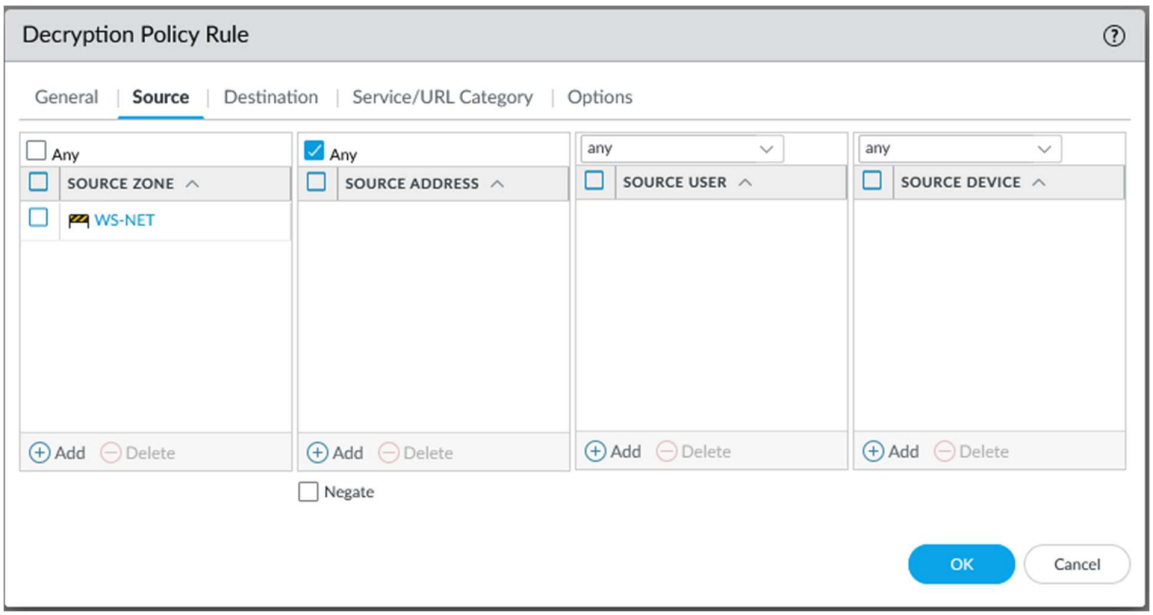
3.1.4 Decryption

Loimme uuden decryption - säännön ”Policies –> Decryption” alta painamalla ”Add” sivun ala-laidassa. Nimeksi annoimme ”Purettu liikenne WS-NET-TO-VLE”. Esitetty kuvassa 21.



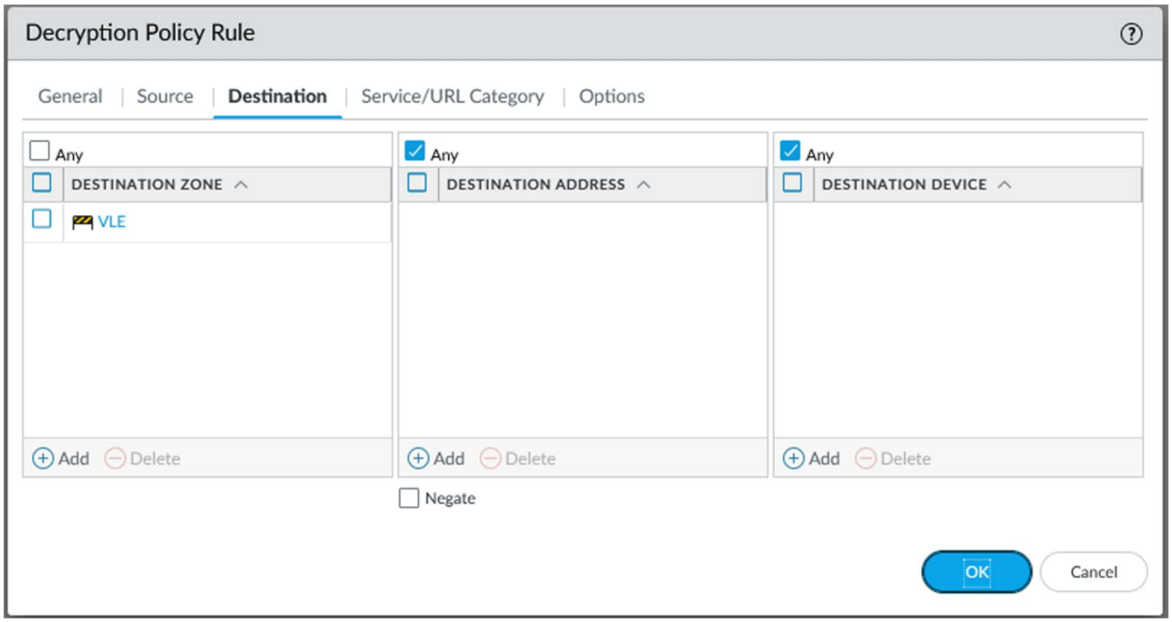
Kuva 21. Nimi decryption säännölle.

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



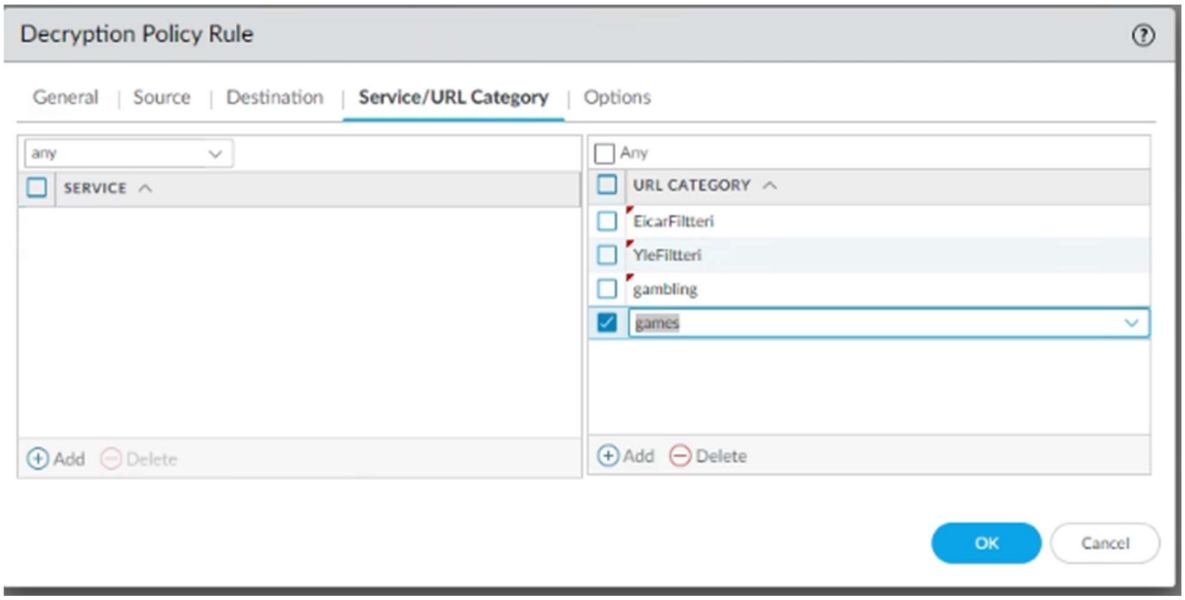
Kuva 22. Source Zone.

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



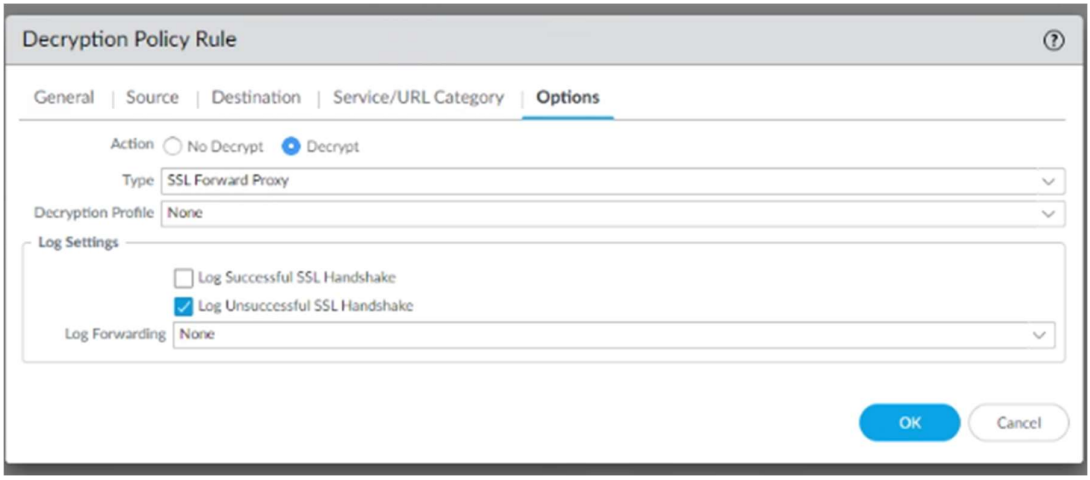
Kuva 23. Destination Zone.

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



Kuva 24. URL Category.

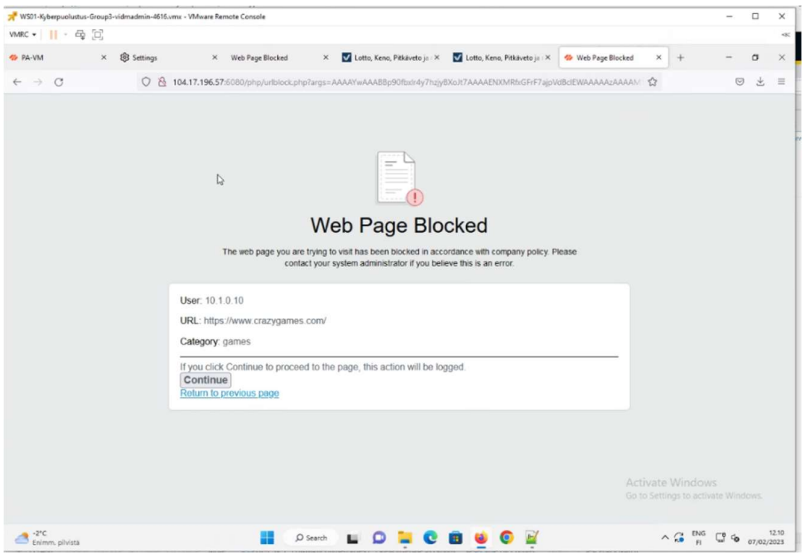
Options -> Log Settings: “Log Unsuccessful SSL Handshake” aktiiviseksi. Esitetty kuvassa 25.



Kuva 25. Log Settings.

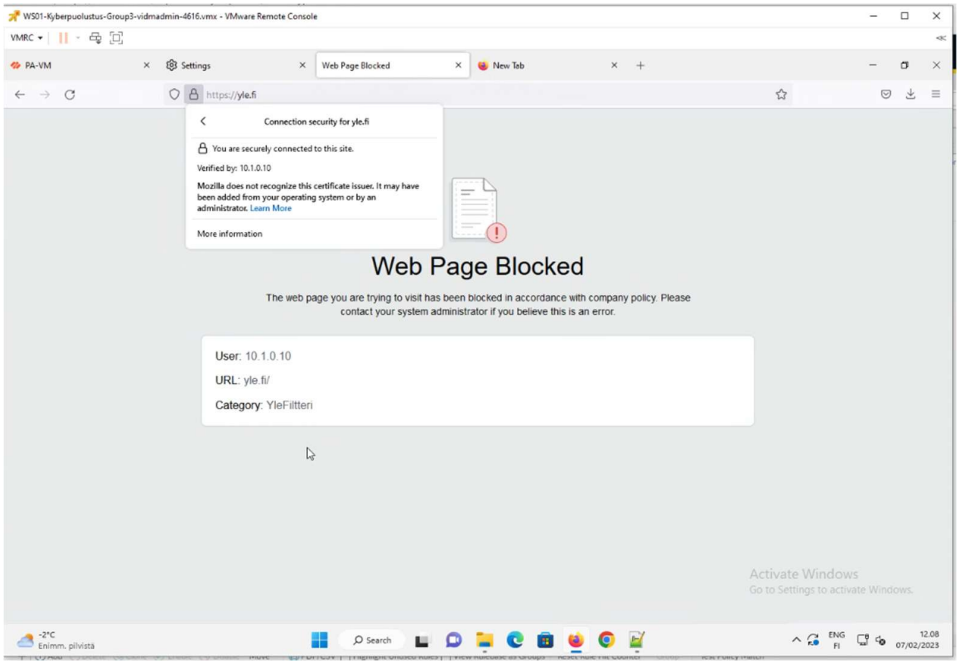
3.1.5 Testaus

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



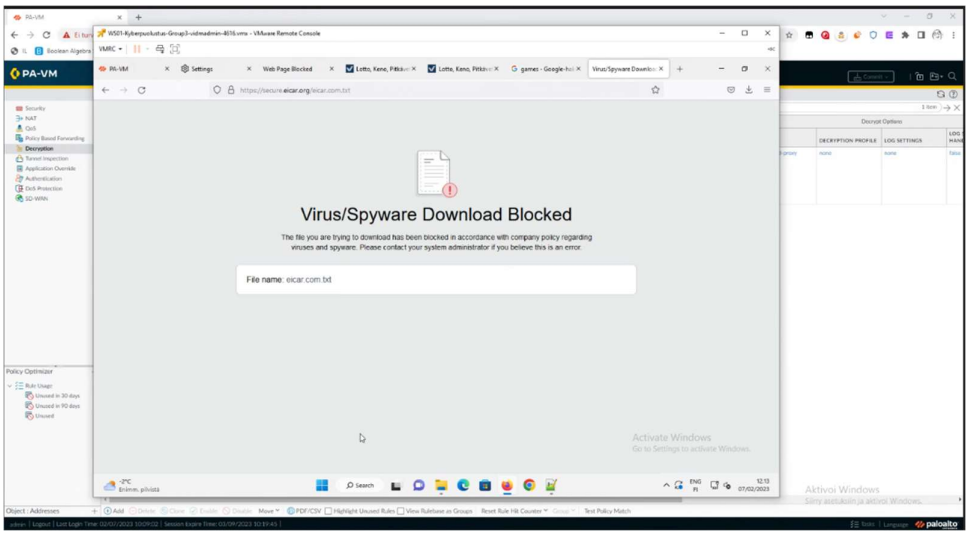
Kuva 26. Pelisivun onnistunut testaus.

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



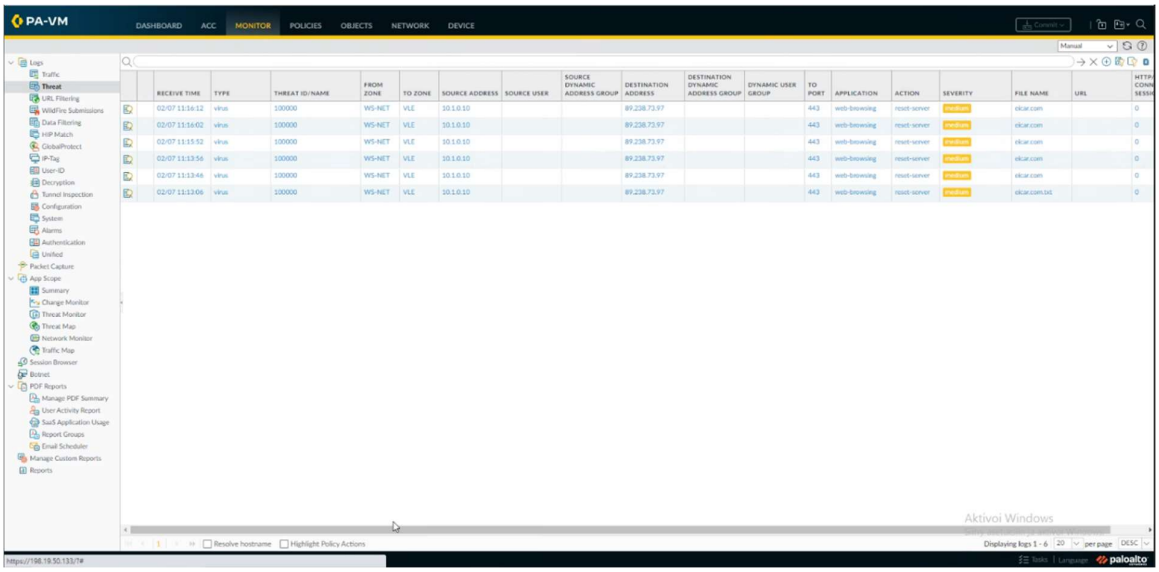
Kuva 27. Yle.fi onnistunut testaus.

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



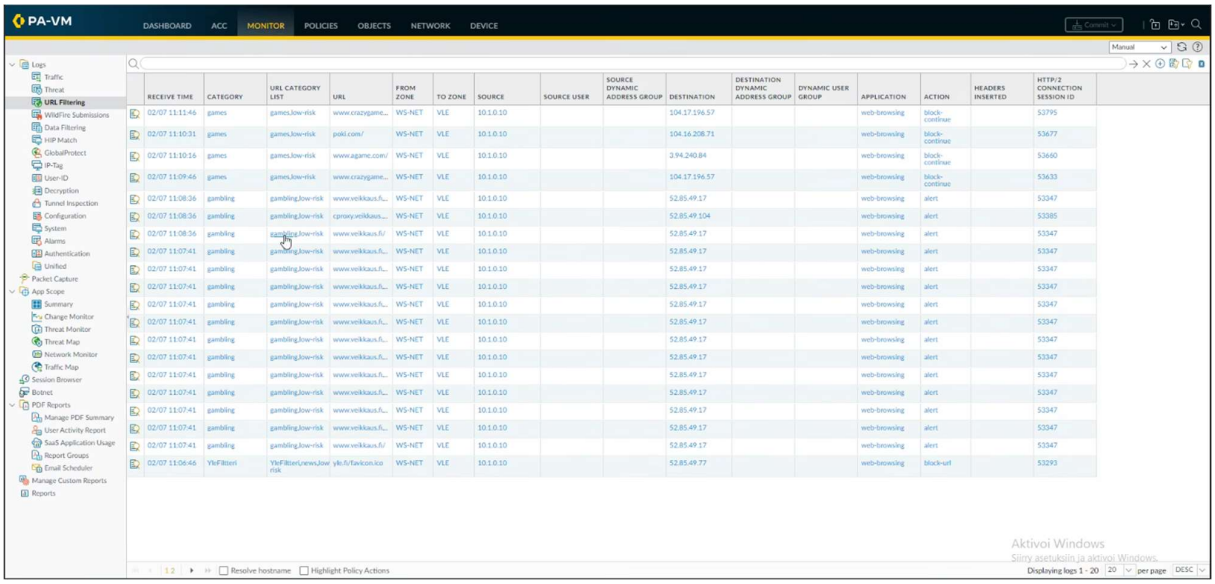
Kuva 28. Eicar onnistunut testaus.

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



Kuva 29. Tiedostojen latausyritykset näkyvät threat - sivulla.

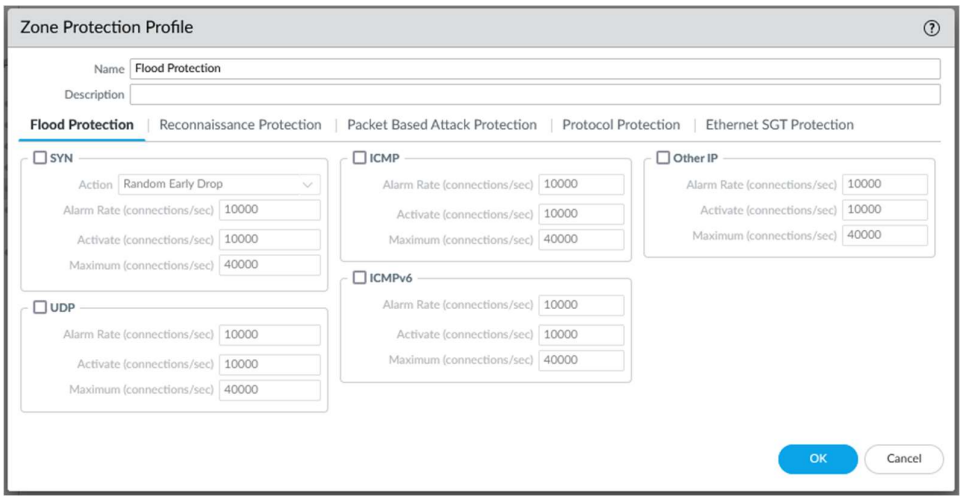
Gambling sivut asetettiin aiheuttamaan vain hälytyksen (alert) ja ne näkyvät paikassa ”Monitor -> URL Filtering”. Esitetty kuvassa 30.



Kuva 30. Gambling sivujen hälytykset (alert).

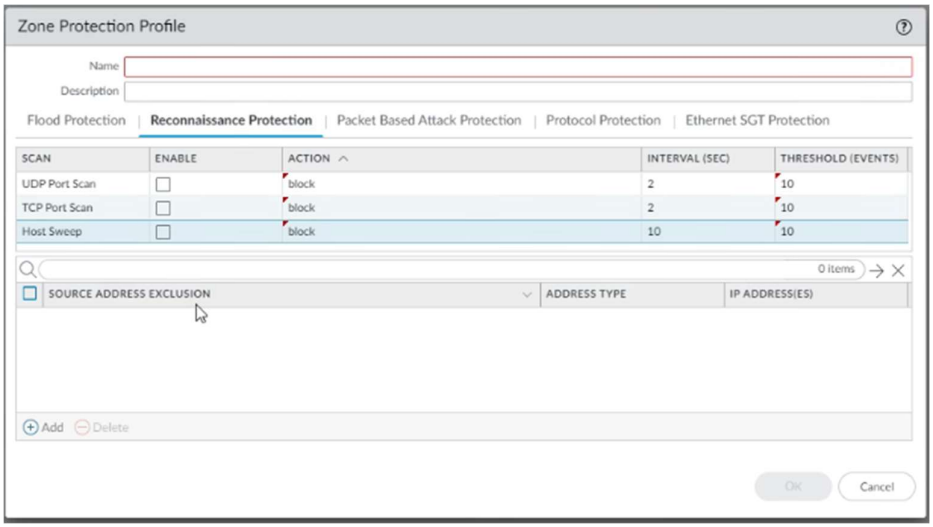
3.1.6 Flood Protection

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.



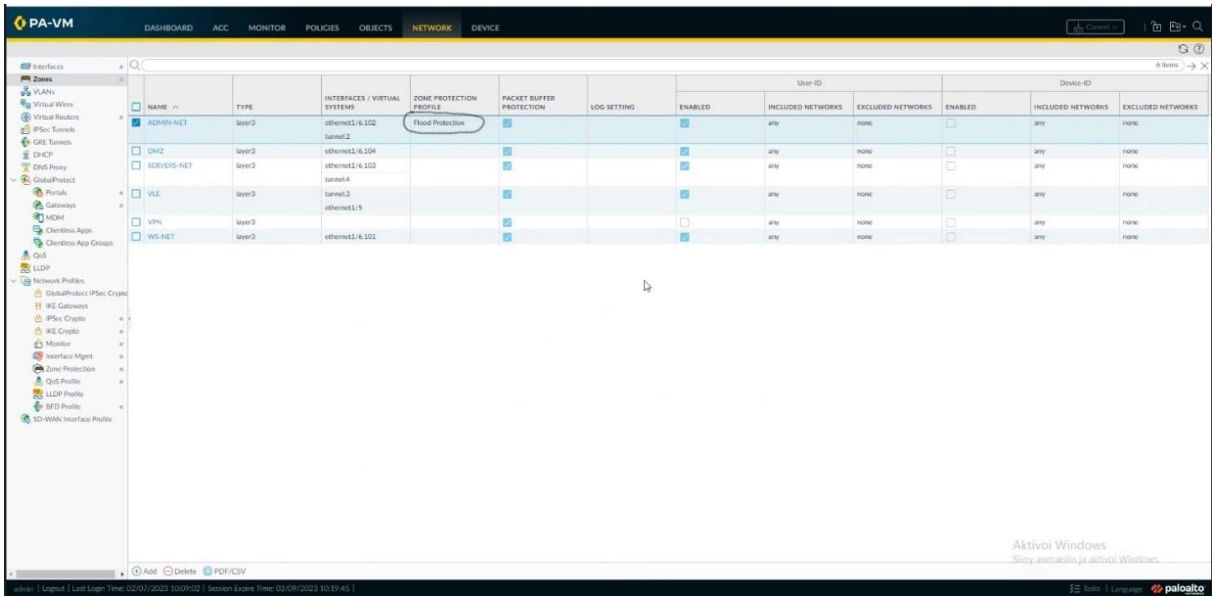
Kuva 31. Flood protection nimi.

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



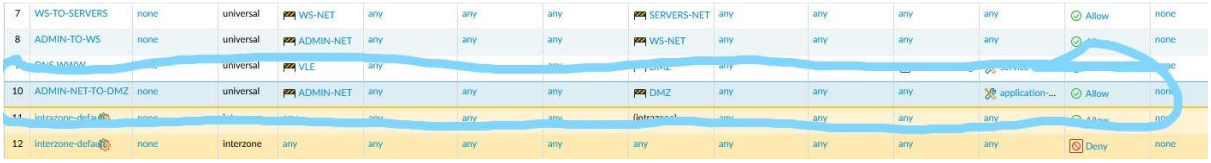
Kuva 32. Flood protection asetukset.

Liitettiin luotu profiili ADMIN-NETiin, näkyy kuvassa 33.



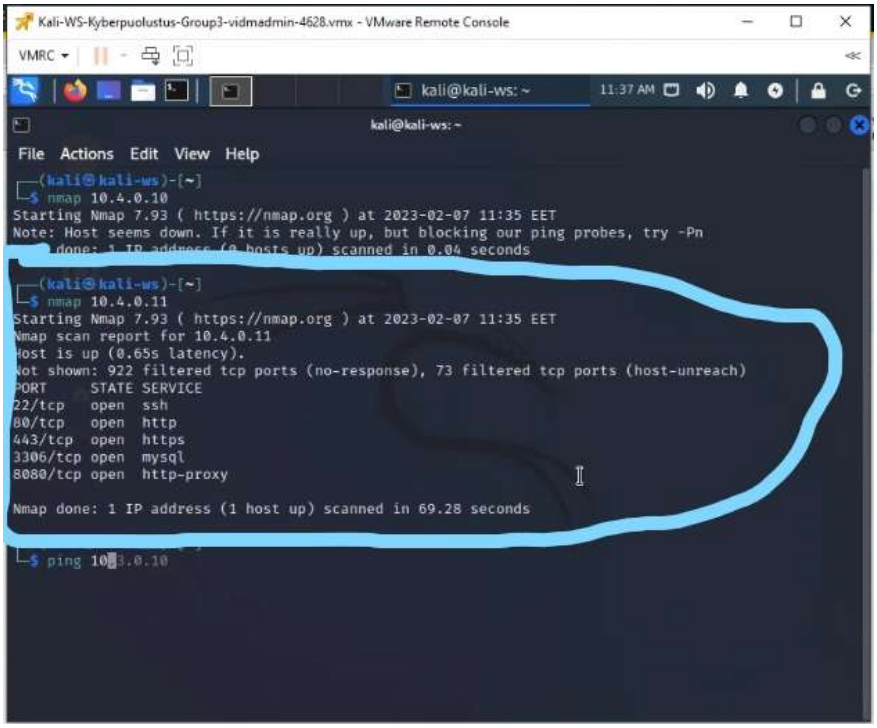
Kuva 33. Flood Profile liitetty ADMIN-NETiin.

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



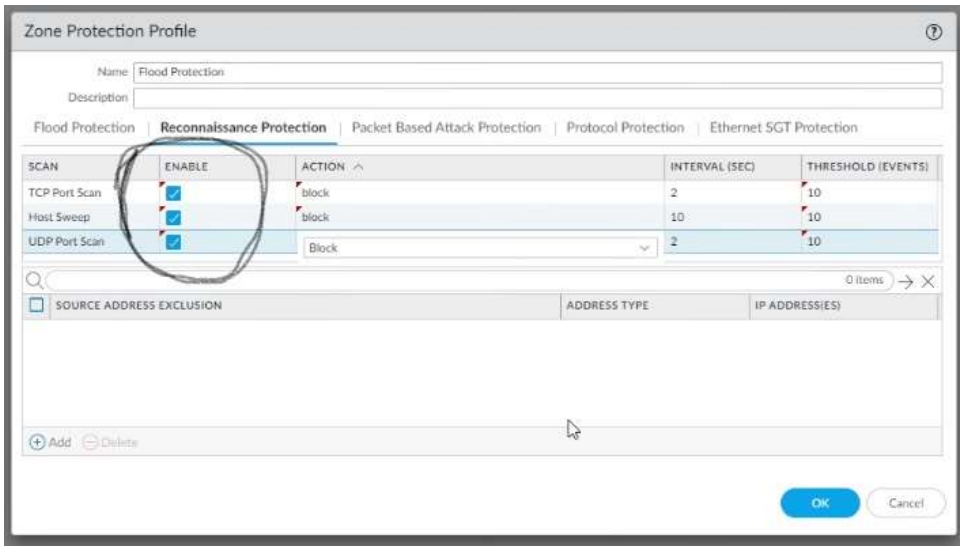
Kuva 34. Sallittu liikenne ADMIN-NETistä DMZ:lle.

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



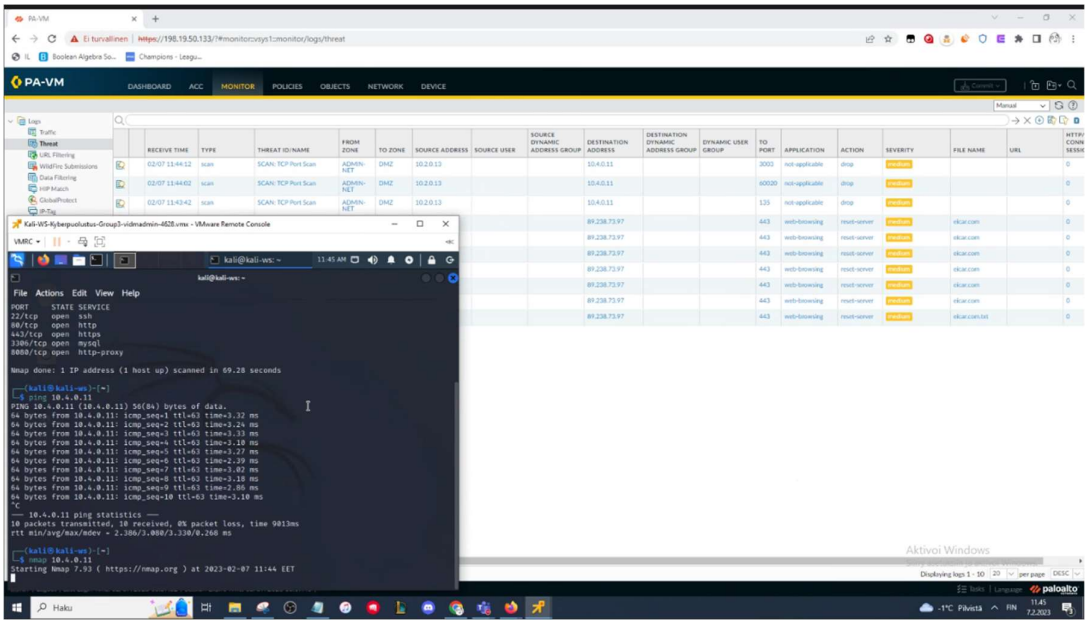
Kuva 35. Ensimmäinen skannausyritys meni läpi.

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



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

Muutoksen jälkeen teimme nmap skannauksen uudelleen ja tällä kertaa skannaus estettiin. Kali-WS konsoli ei antanut scan reportia ja paloalto näytti ”Monitor -> Threat” alla estetyt yritykset. Esitetty kuvassa 37.



Kuva 37. Nmap skannaus estetty onnistuneesti.

4 POHDINTA

Harjoitustyön tavoitteena oli tutustua ryhmätyönä VLE-ympäristöön toteutetun Palo Alton turvallisuus ominaisuuksiin paremmin, erityisesti keskittymällä URL-filtteröintiin. Harjoituksessa Palo Altoon tehtiin uusi turvallisuus sääntö, joka koski vain web-browsing liikennettä WS-netistä VLE:hen johon luotiin URL-filteröinti. Filteröinti esti onnistuneesti pääsyn Yle.fi verkkosivulle, aiheutti hälytyksen uhkapelisivustoilla sekä antoi peli (games) sivustoilla continue vaihtoehdon eikä mennyt suoraan verkkosivulle. Harjoitustyön lopussa asetettiin lisäksi onnistuneesti flood protection joka esti porttien skannaamiseen.

Harjoitustyössä käytiin lisäksi läpi teoria laboratorion virtuaalikoneen teoria osuudessa laboratorioympäristön virtuaalikoneen Palo Alto palomuurin Profile Settings, EICAR, NMAP, Mitre ATT&CK ja mitä on uhkatieto.

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 blokkaussäännöt 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