Labra 3

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007
2.10.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tietoturvakontrollit-opintojakson kolmannessa laboratorioharjoituksessa oli tarkoituksena jatkaa Palo Alton turvallisuusominaisuuksiin tutustumista ja parantaa ympäristömme turvallisuutta yhä entisestään. Harjoituksessa hyödynnetään Palo Alton ominaisuuksia kuten Threat-ID ja URL-filteröinti. Tutustuimme myös Antivirus, Vulnerability Protection, Anti-Spyware, File Blocking sekä Wildfire Analysis ominaisuuksiin.

Edellä mainittujen työkalujen avulla meille annettiin tehtäväksi estää pääsy yle.fi-sivustolle, tehdä asetus, joka lähettää ilmoituksen palomuuriin, kun selaimella mennään uhkapelisivustoille ja pelisivustoille, kuten miniclip.com, mennessä selain antaa käyttäjälle ilmoituksen, että organisaatio ei suosittele sivulle siirtymistä, mutta käyttäjä pystyy jatkaa sivulle klikkaamalla continue-painiketta. Tehtävänä oli myös asettaa sääntö, että käyttäjä pääsee eicar.com -sivustolle, mutta ei pysty ladata siellä olevaa testitiedostoa.

2 Teoria

Teoria-osuudessa käymme lyhyesti läpi harjoituksessa käytettyjä Palo Alto -palomuurin ominaisuuksia ja tekniikoita sekä niiden eroja.

2.1 Antivirus

Palo Alton Antivirus suojaa tunnetuilta viruksilta, madoilta ja muilta haittaohjelmilta. Antivirus kohdistuu tiedostopohjaisiin haittaohjelmiin ja tunnistaa ne virustietokannan perusteella. AV-profiileja voidaan konfiguroida määrittelemään, mitä toimia toteutetaan havaittujen uhkien vakavuuden mukaan, mikä mahdollistaa räätälöidyt vastaukset kohdatuille haittaohjelmille. (Network Security, Antivirus. 2024).

2.2 Vulnerability Protection

Haavoittuvuussuojaus estää hyökkäyksiä, jotka hyödyntävät tunnettuja haavoittuvuuksia ja kohdistuvat verkkoon ja ohjelmistoihin. Suojaus kohdistuu erityisesti haavoittuvuuksiin. (Network Security, Vulnerability Protection. 2024).

2.3 Anti-Spyware

Anti-Spyware tunnistaa ja estää vakoiluohjelmia ja muita haitallisia ohjelmia, jotka yrittävät varastaa tietoja tai seurata käyttäjien toimintaa. Se analysoi liikennettä. Anti-Spyware keskittyy erityisesti vakoiluohjelmien ja tietojen keräämisen estämiseen. (Network Security, Anti-Spyware. 2024).

2.4 File Blocking

Palo-altossa voidaan luoda file blocking profiileja, joiden avulla voidaan määrittää tiedostotyyppejä, joiden lataamista ja käsittelyä halutaan estää tai rajoittaa. On mahdollista myös tehostaa monitorointia asettamalla hälytyksiä tiedostomuodon ilmaantuessa. (Network Security, File Blocking. 2024).

Estää tiettyjen tiedostotyyppien lataamisen, kuten .exe ja .bat, lataamisen, lähettämisen ja avaamisen. Ei havaitse haittaohjelmia vaan estää tiedostotyypin perusteella tiedostojen siirron.

2.5 WildFire Analysis

Pilvipohjainen analyysipalvelu, joka tutkii epäilyttäviä tiedostoja, kuten uusia haittaohjelmia, joita ei vielä ole muissa tietokannoissa. Se pyrkii havaitsemaan nollapäiväuhat. Keskittyy erityisesti uusien ja tuntemattomien haittaohjelmien tunnistamiseen ja estämiseen. Muut suojaukset käyttävät ennalta määrättyjä tunnisteita. (Network Security, WildFire Analysis. 2024).

2.6 Flood Protection

Flood protection eli liikennetulva suoja puolustaa valittua turvallisuus aluetta SYN, ICMP, ICMPv6, UDP, ja muilta IP tulva hyökkäyksiltä. Palomuuri seuraa, kuinka monta uutta yhteyttä muodostetaan sekunnissa (CPS, connections-per-second) jokaisesta flood-hyökkäystyypistä. Sitten se vertaa näitä määriä ennalta asetettuihin rajoihin, jotka määritellään flood protection-profiiliin. Jos liikenne ylittää nämä rajat, palomuuri voi ryhtyä toimenpiteisiin, kuten estää ylimääräiset yhteydet. (Flood Protection. 2024).

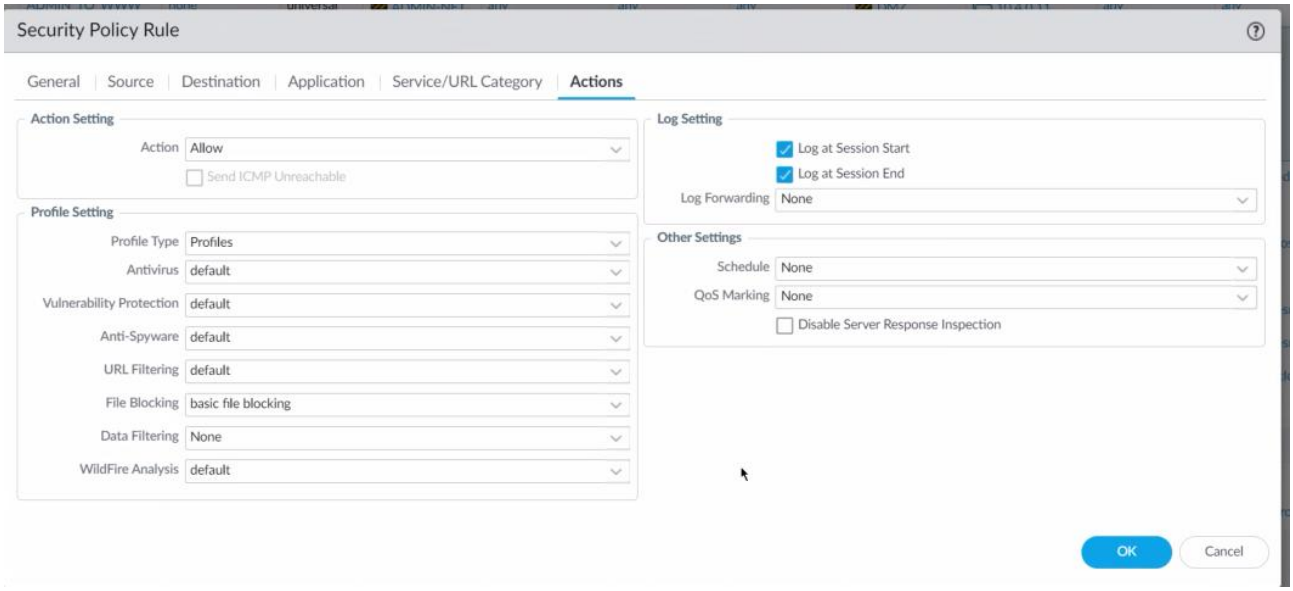
2.7 EICAR-testitiedosto

EICAR-testitiedosto on European Institute for Computer Antivirus Research (EICAR) ja Computer Antivirus Research Organization (CARO) -instituuttien kehittämä testi, joka on tarkoitettu testaamaan virustorjuntaohjelmien toimintaa. Tiedosto ei ole oikea virus tai haittaohjelma, vaan tiedoston ladattaessa se on suunniteltu niin, että virustorjunnan pitäisi havaita se samanlailla kuin se havaitsisi oikean viruksen sisältävän tiedoston. EICAR-testitiedosto on täysin haitaton ja turvallinen sekä sen testaaminen on täysin ilmaista. Eli käytännössä EICAR:lla testataan, että virustorjuntaohjelma toimii oikein. (Anti Malware Testfile).

3 Työn kulku

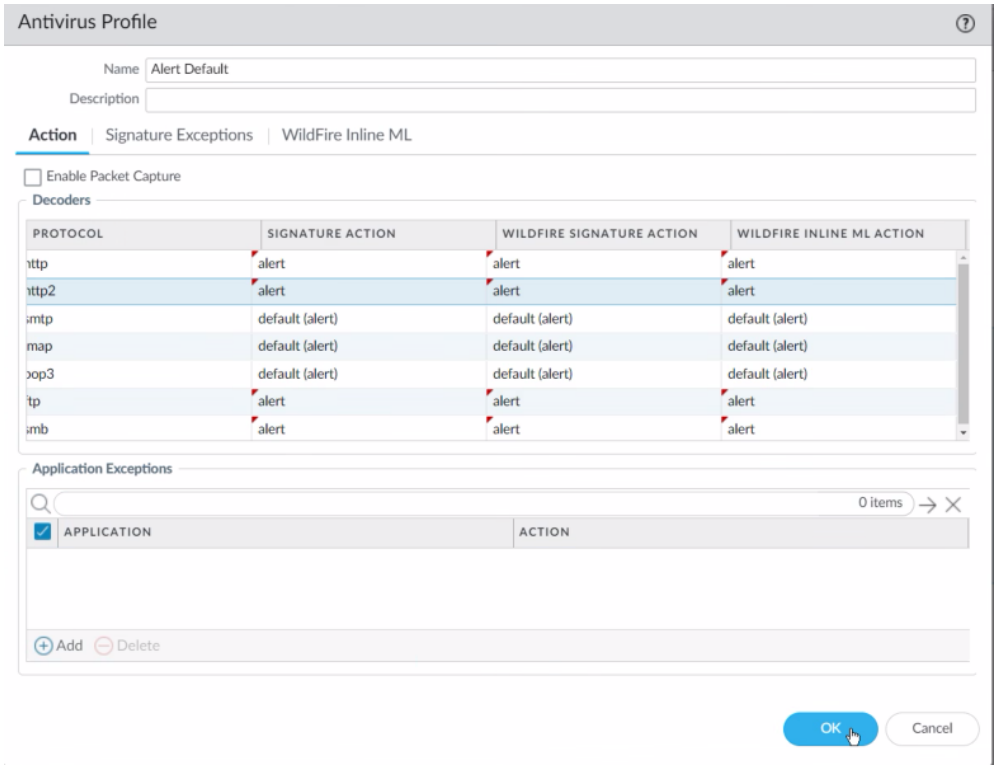
Aloitimme luomalla uuden turvallisuussäännön nimeltä DMZ_to_VLE. Säännössä lähdevyöhykkeenä oli DMZ ja määränpäänä VLE, eli internet. Sääntöä luodessa menimme Actions-välilehdelle ja laitoimme Profile Settings -otsikon alle ohjeiden mukaan (Kuvio 1.) mukaisesti default-säännön

päälle. Tässä vaiheessa ohjeen mukaisesti poistimme myös DMZ turvallisuusvyöhykkeen olemassa olevasta, valmiiksi meille luodusta GATEWAY-TO-VLE-säännöstä.



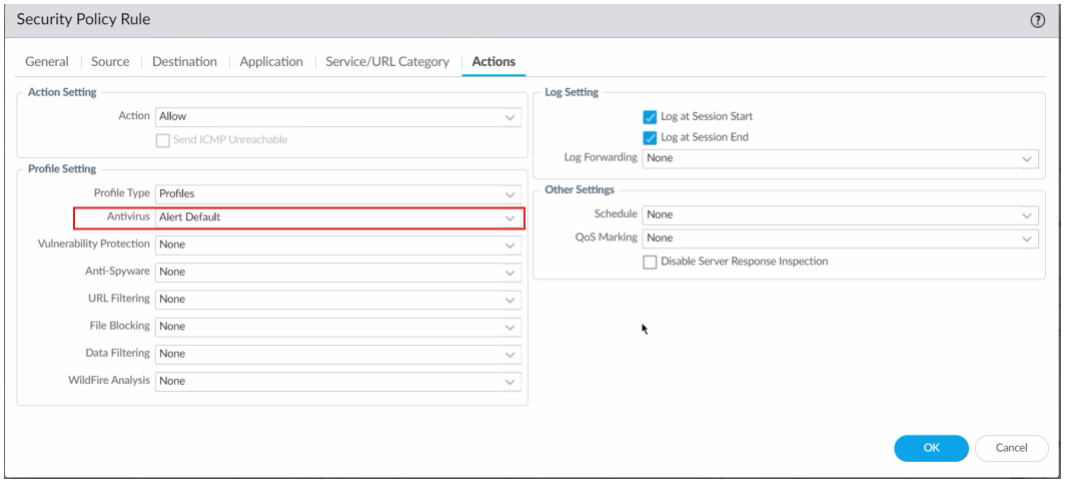
Kuvio 1. Turvallisuussäännön asetukset

Siirryimme Objects-välilehdelle Security Policies -otsikon alle Antiviruksen asetuksiin ja kopiomme säännön ”Default”. Asetimme kopiolle nimeksi Alert Default ja muokkasimme sen asetuksia siten, että kaikesta toiminnasta tulee hälytys. (Kuvio 2)



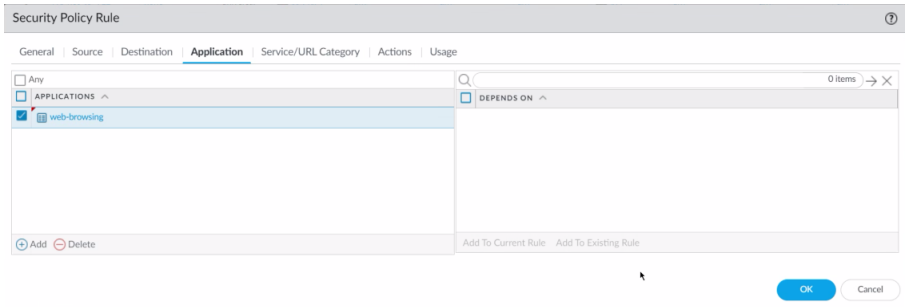
Kuvio 2. Antivirusprofiilin säännöt

Siirryimme takaisin muokkaamaan turvallisuussääntöjä. Olimme jo aiempien töiden ohessa luoneet säännön, jossa lähde on WS-NET ja määränpää VLE. Säännön Actions-välilehdeltä Profile Settings -otsikon alta vaihdoimme Antivirukselle aiemmin luomamme säännön Alert Default. (Kuvio 3). Poistimme myös tässä vaiheessa WS-NET-turvallisuusvyöhykkeen GATEWAY-TO-VLE-turvallisuussäännöstä.



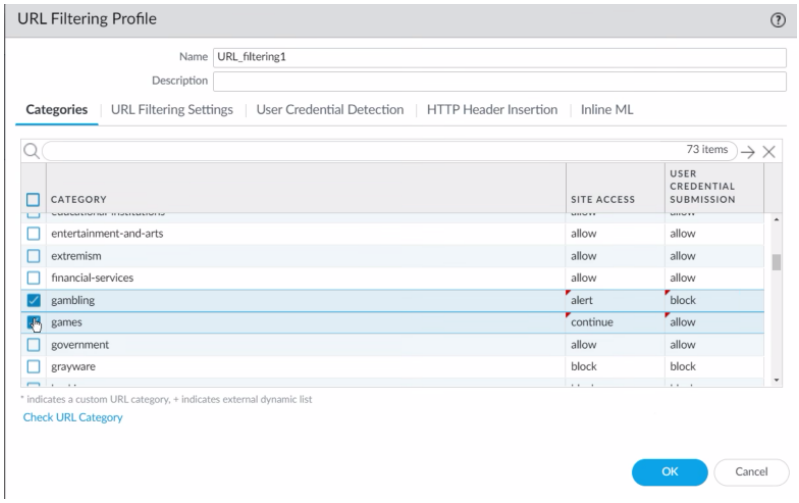
Kuvio 3. Antivirussäännön asettaminen

Loimme vielä yhden uuden säännön nimeltä WS-net_to_VLE_netbrowsing. Siihen asetimme lähteeksi WS-NET:n ja määränpääksi VLE:n. Application-välilehdellä lisäsimme ainoastaan yhden sovelluksen, joka oli web-browsing. (Kuvio 4)



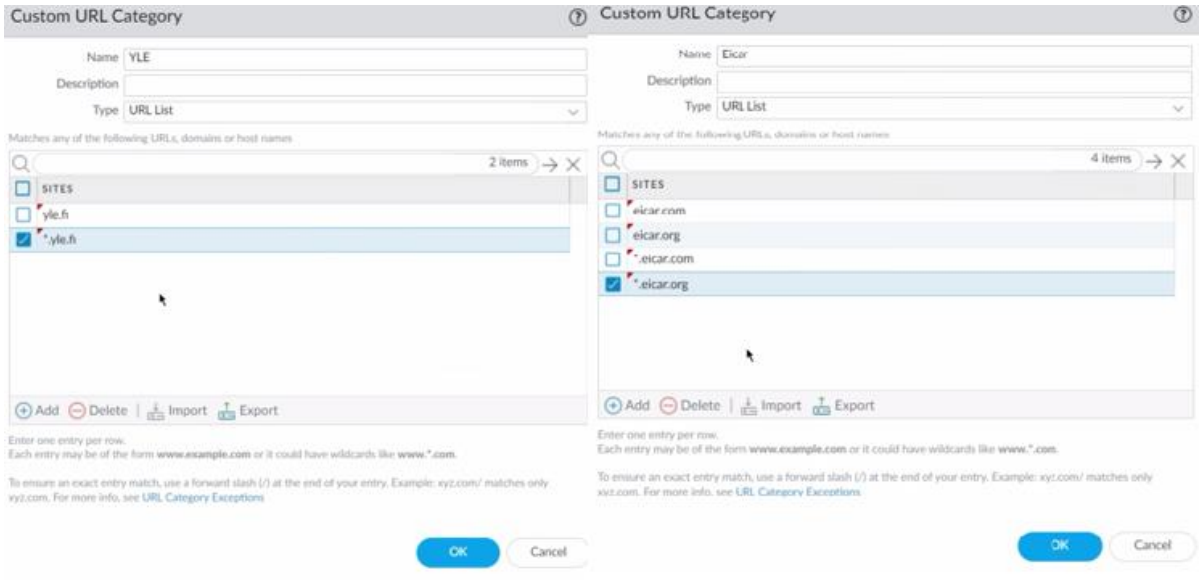
Kuvio 4. Web-browsing sovellus

Siirryimme Objects-välilehdelle kohtaan URL filtering, joka löytyi Security Profiles -otsikon alta. Siellä loimme kopion default-säännöstä ja nimesimme sen nimellä URL_filtering1. Teimme muokkauksia uhkapeli- ja pelisivustojen käsittelyyn: uhkapelisivustoille mennessä palomuuriin tulee ilmoitus ja pelisivustoille mennessä käyttäjälle tulee ilmoitus (alert), että organisaatio ei suosittele sivulle siirtymistä, mutta käyttäjä voi siirtyä sivulle kuitenkin (continue). (Kuvio 5)



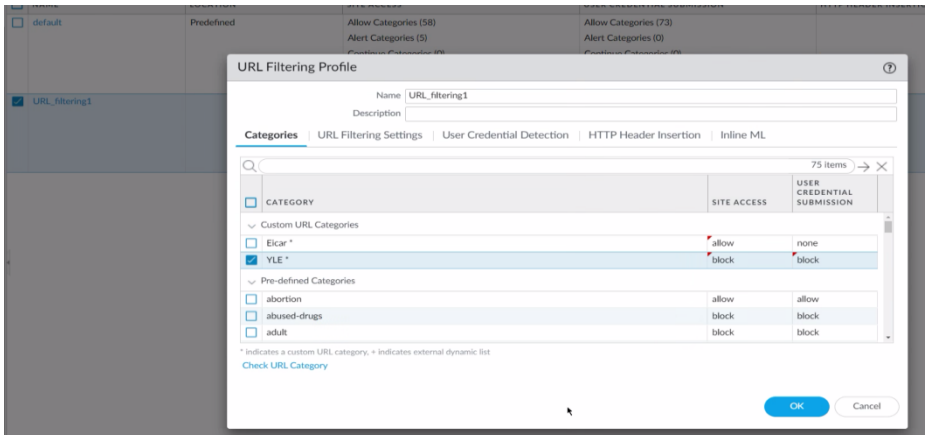
Kuvio 5. URL-suodattimen asetukset

Teimme kaksi uutta kustomoitua URL-kategoriaa. Ensimmäinen ole yle.fi-sivustolle ja toinen eicar-sivustolle. Eicarille laitoimme päätteet .com ja .org, koska molemmilla päätteillä pääsee sivustolle. (Kuvio 6)



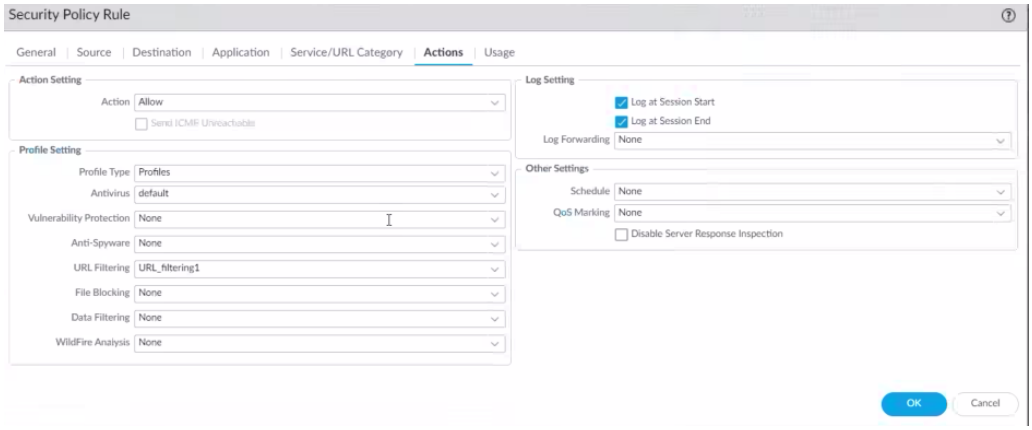
Kuvio 6. Kustomoidut URL-kategoriat

Siirryimme takaisin muokkaamaan aiemmin luotua URL-suodatinprofiilia. Kustomoitujen kategorioiden alta muokkasimme luomiemme kategorioiden pääsyä. Eicar-sivustolle on pääsy, koska haluamme päästä sinne ja haluamme vain estää sieltä testitiedoston lataamisen. Ylen sivuille haluamme estää pääsyn kokonaan, eli valitsemme molempiin valintakenttiin toimenpiteeksi block. (Kuvio 7)



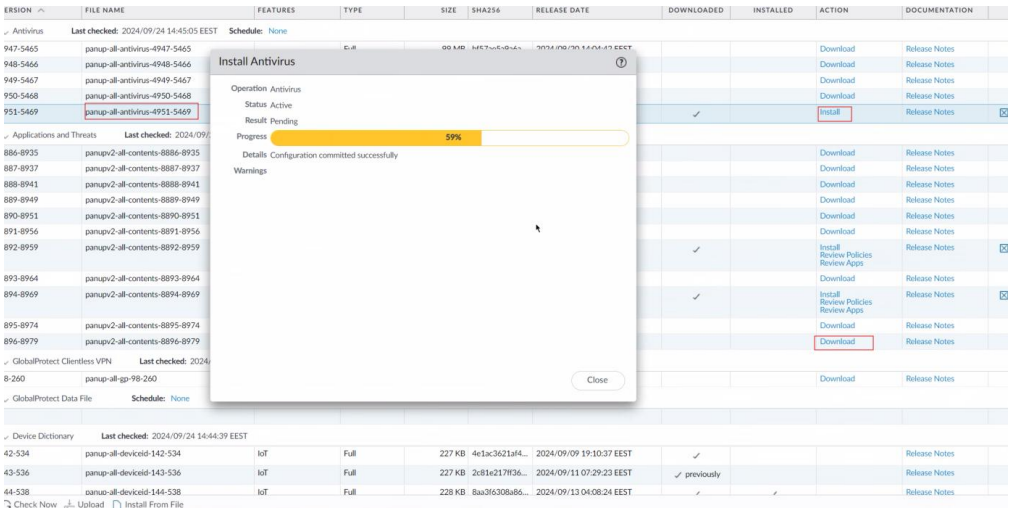
Kuvio 7.Url-suodattimen muokkaus

Seuraavaksi menimme takaisin Policies-välilehdelle muokkaamaan aiemmin luotua WS-net_to_VLE_netbrowsing turvallisuussääntöä. Actions-välilehdellä Profile Settings -otsikon alta Url Filtering kohtaan vaihdoimme luomamme URL_filtering1 -suodattimen. (Kuvio 8)



Kuvio 8. Suodattimen asettaminen turvallisuussääntöön

Tässä vaiheessa tajusimme, että kaiken jo tehdyn toimimiseksi, että Antivirus ja muut sovellukset täytyy käydä asentamassa, joten asensimme ne. Valitsimme molemmista uusimmat saatavilla olevat versiot. (Kuvio 9)

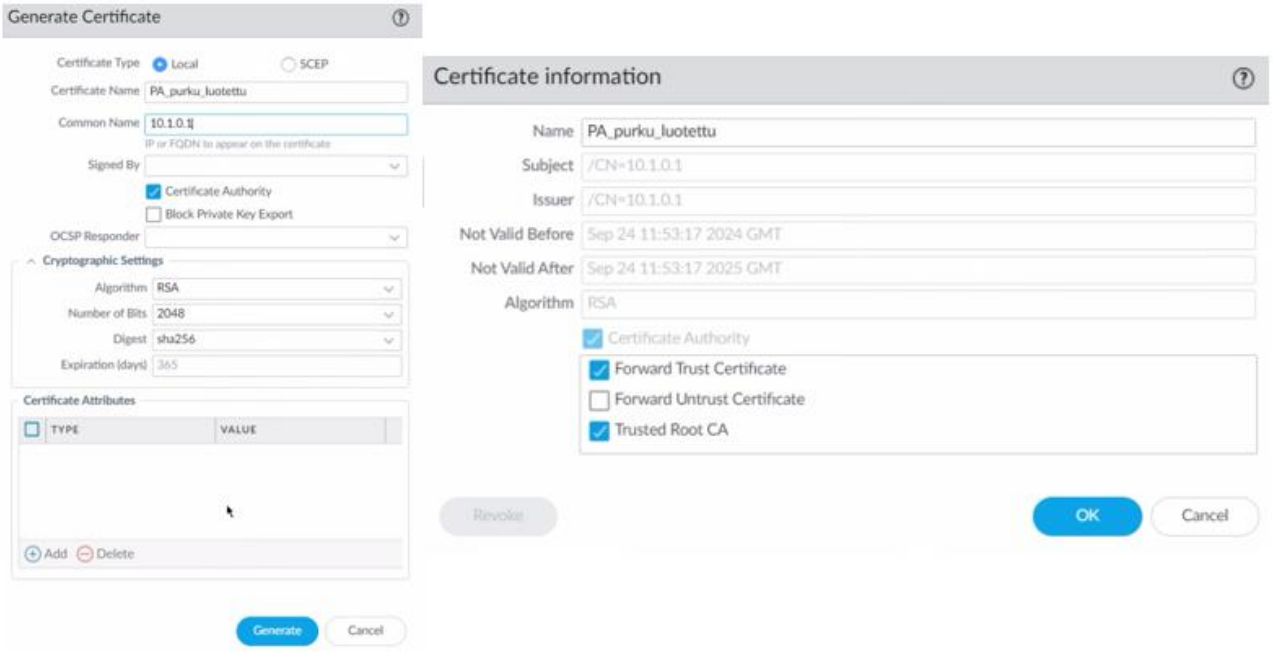


Kuvio 9. Lisäosien asentaminen

3.1 HTTPS-salauksen purku

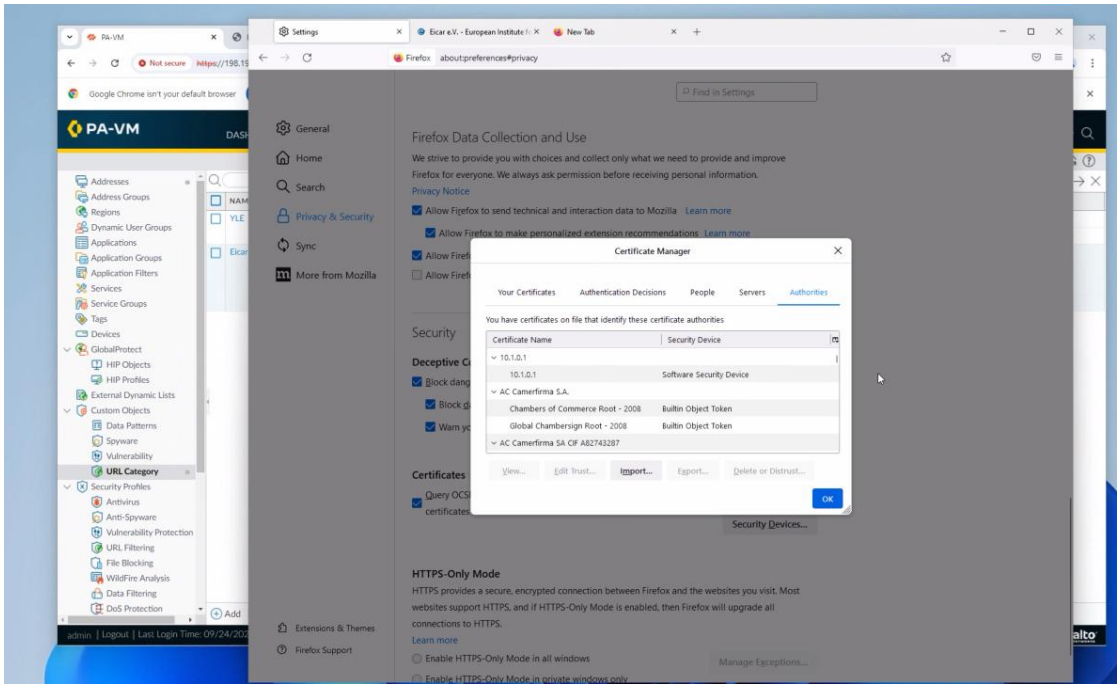
Tähän mennessä tehdyt turvallisuussäännöt, antiviruksen asetukset ja url-suodattimet toimivat ainoastaan, jos verkkosivut eivät ole https-salattuja. Meidän täytyi siis purkaa Palo Altolla nämä https-salaukset.

Aloitimme luomalla uuden sertifikaatin. Nimesimme sen nimellä PA_purku_luotettu ja asetimme Common Name kohtaan WS01-työaseman IP-osoitteen, eli 10.1.0.10, koska tämä sertifikaatti tulisi käyttöön kyseiselle työasemalle. Valitsimme myös kohdan Certificate Authority. Muokkasimme myös sertifikaattia sen verran, että valitsimme Forward Trust Certificate- ja Trusted Root CA-kohdat. (Kuvio 10)



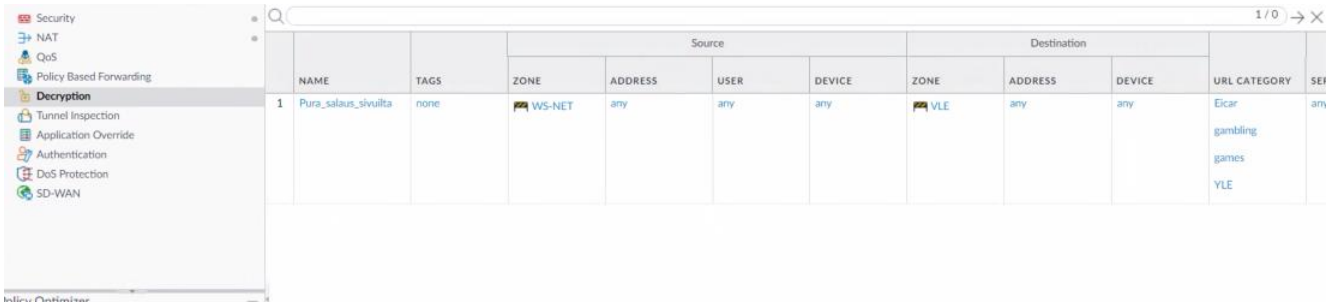
Kuvio 10. Sertifikaatin luonti

Seuraavana avasimme WS01-työaseman ja avasimme Palo Alton sen selaimella. Latasimme juuri luodun sertifikaatin koneelle ja asensimme sen selaimeen. (Kuvio 11)



Kuvio 11. Sertifikaatin asentaminen WS01-työaseman selaimelle

Palasimme takaisin Palo Altoon ja siirryimme Policies-välilehdelle kohtaan Decryption. Täällä loimme uuden säännön salauksen purkua varten. Nimesimme sen nimellä Pura_salaus_sivuilta, asetimme lähteeksi WS_NET:n ja määränpääksi VLE:n. Purettaviksi kategorioiksi asetimme Eicarin, uhkapeli- ja pelisivustot sekä YLE:n verkkosivut, eli samat mihin aiemmin loimme url-suodattimen. (Kuvio 12)

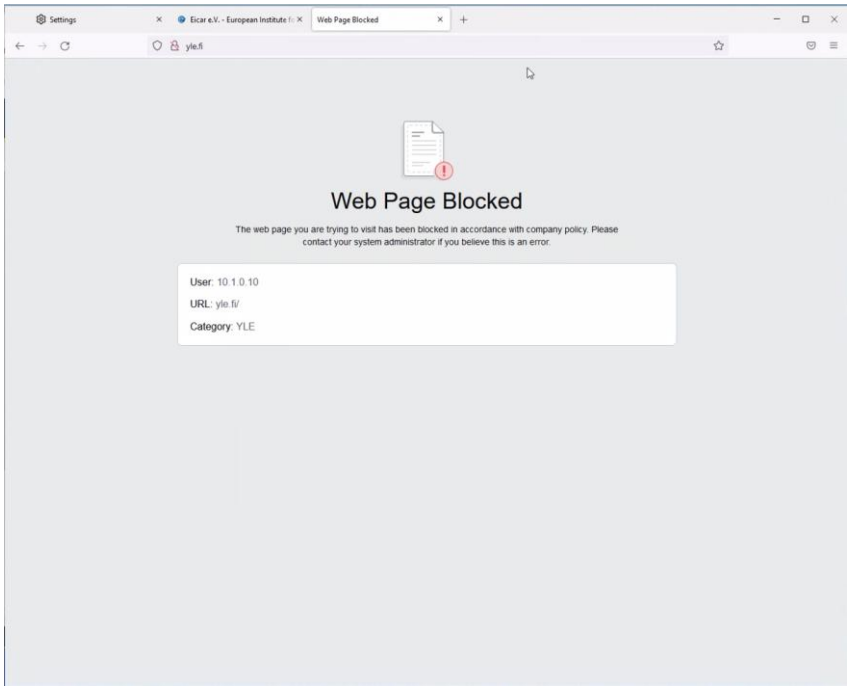


Kuvio 12. Pura_salaus_sivulta purkusäännön asetukset

Lopuksi vielä valitsimme Palo Altosta commit, jolloin tekemämme asetukset astuivat voimaan.

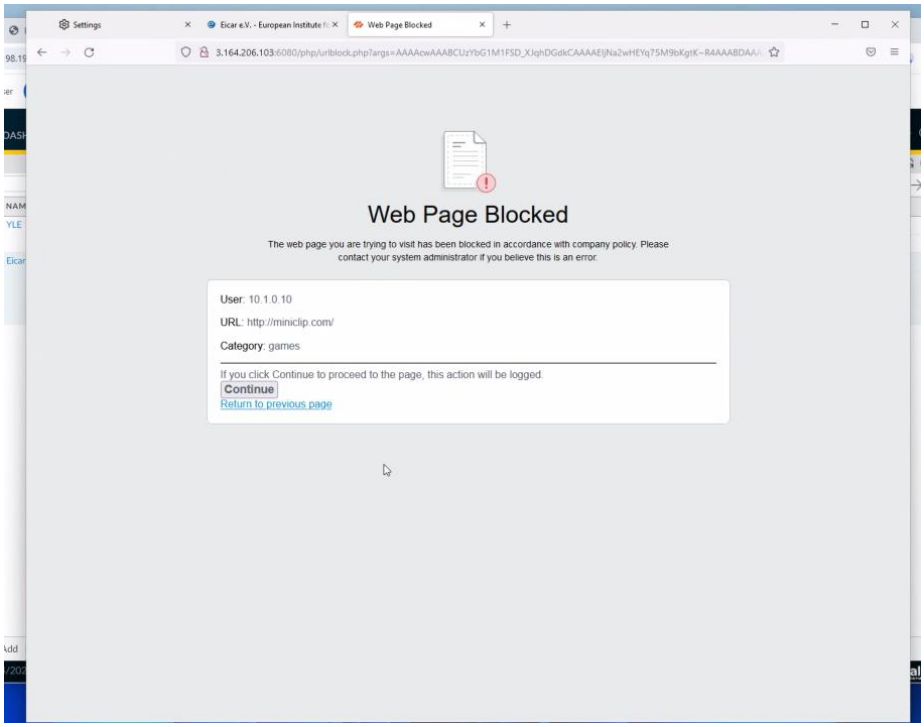
3.2 Testaaminen

Kun kaikki oli valmista, siirryimme WS01:lle ja testasimme, toimiiko tekemämme muutokset. Ensimmäisenä yritimme mennä yle.fi sivustolle lukemaan uutisia. Saimme kuitenkin ilmoituksen, että verkkosivusto on estetty, emmekä päässeet etenemään. Näin sen kuuluikin toimia! (Kuvio 13)



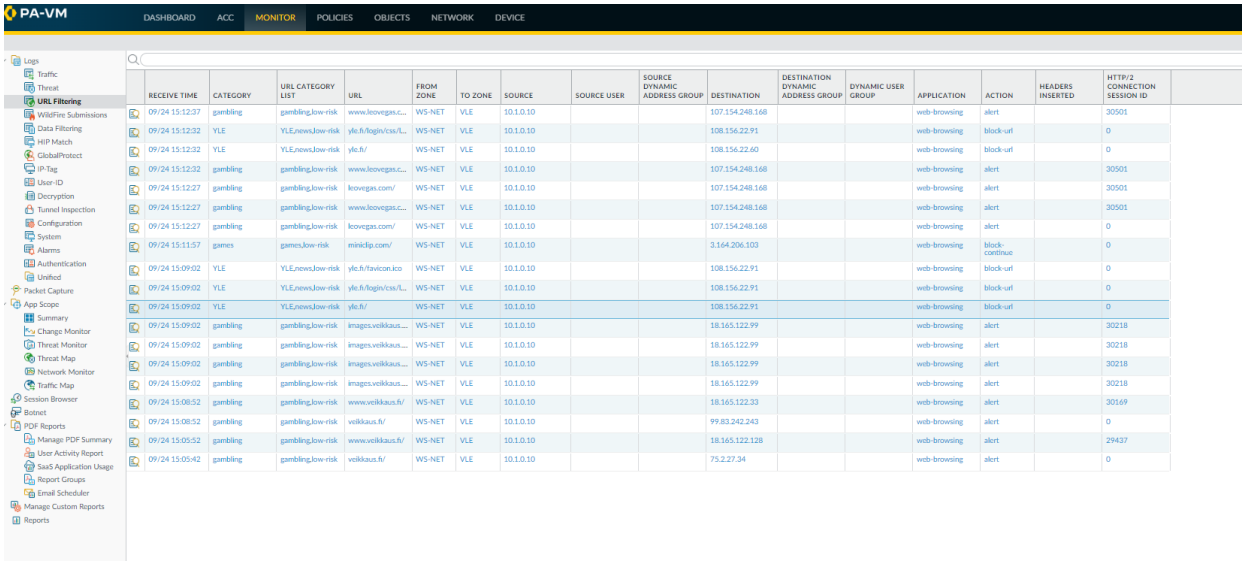
Kuvio 13. Yle.fi estetty

Seuraavaksi testasimme, pääsemmekö miniclip.com -sivustolle pelaamaan hauskoja selainpelejä. Saimme ilmoituksen, että sivu on estetty, mutta voimme jatkaa sivulle klikkaamalla Continue-painiketta. Tästä jäisi kuitenkin jälki palomuuriin. (Kuvio 14)



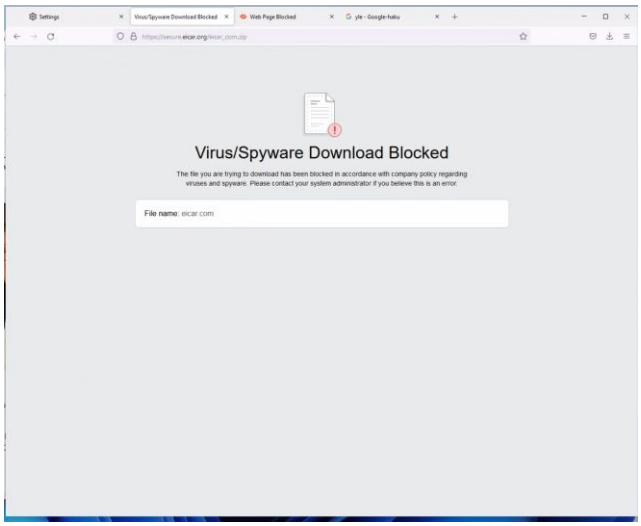
Kuvio 14. Pelisivustot

Siirryimme myös veikkauksen sivuille testataksemme, tuleeko siitä Palo Altoon ilmoitus. Palo Altossa Monitor-välilehdellä URL-filteringin alta löysimme ilmoituksia, että yritimme mennä uhkapelisivuille. Näistä lokeista näemme myös estetyt yritykset mennä YLE:n sivuille. (Kuvio 15)



Kuvio 15 Palo Alton loki

Viimeisenä testinä oli mennä eicar.com -sivustolle ja yrittää ladata sieltä eicar.com-zip -testitiedosto. Kuten pitikin, antivirus tunnisti tiedoston haittaohjelmaksi ja esti lataamisen. (Kuvio 16)



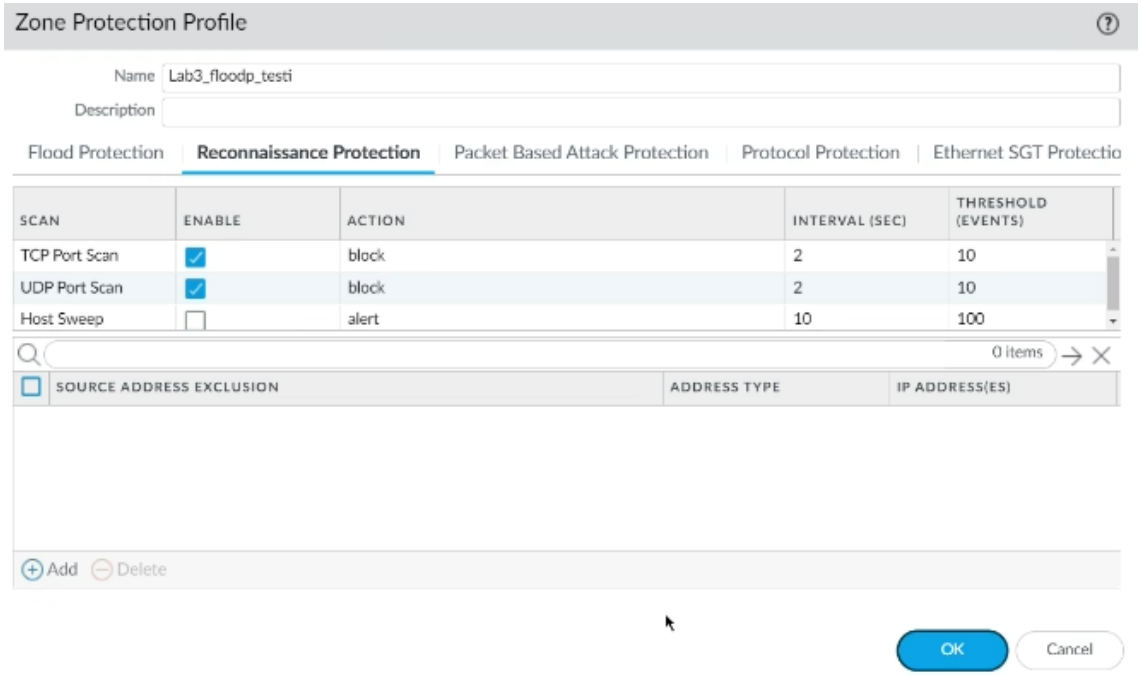
Kuvio 16. Estetty lataus

Kaikki siis toimii, kuten pitääkin!

3.3 Liikennetulvasuojaus

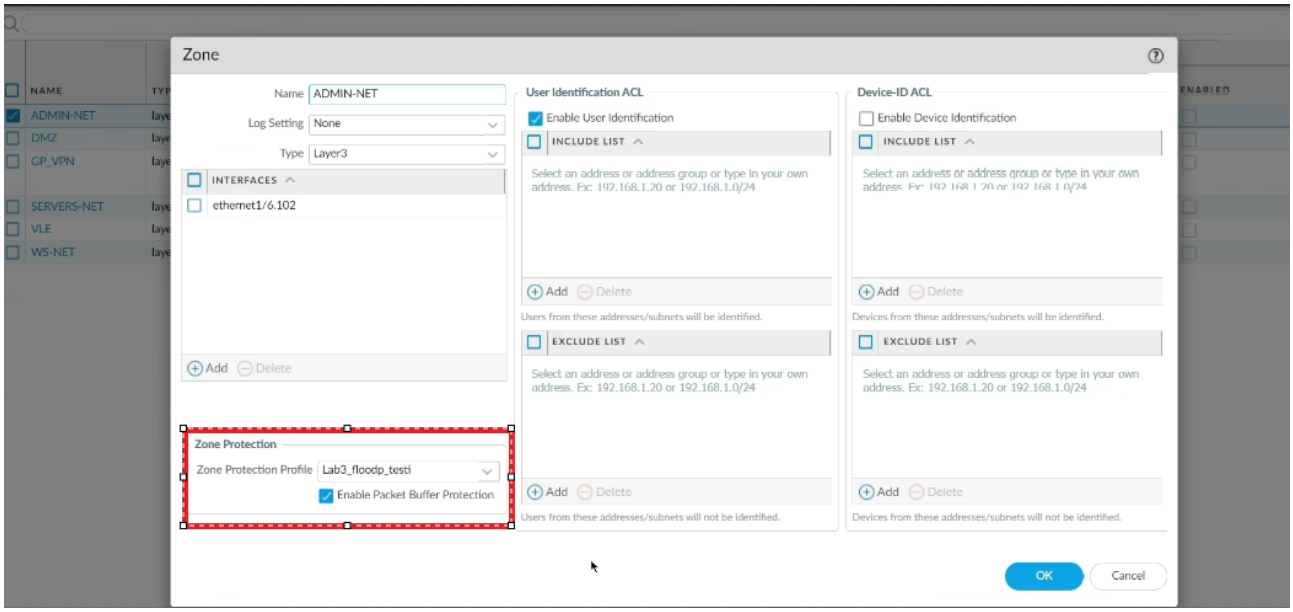
Ohjeissa oli vielä lisätehtävänä liikennetulvasuojauksen (flood protection) asettaminen. Halusimme tietenkin vielä yrittää tätä. Aloitimme navigoimalla Palo Altossa Network-välilehdellä Zone Protection kohtaan, joka löytyi Network Profiles-otsikon alta. Loimme sinne uuden säännön nimeltä Lab3_floodp_testi ja teimme asetuksia kuvion 17 mukaisesti. Estimme siis porttien skannailut. (Kuvio 17)

Laitoimme alue suojauksen päälle (Kuvio 17.)



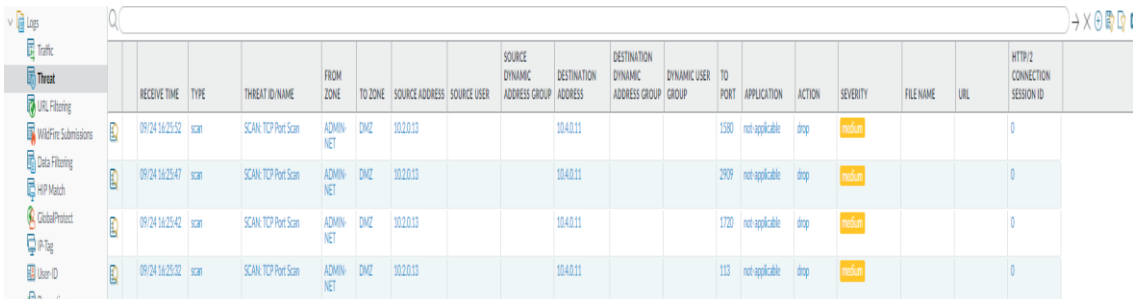
Kuvio 17. Liikennetulvasuojauksen asetukset

Nyt kun sääntö oli asetettu, lisäsimme sen ADMIN-NET turvallisuusvyöhykkeeseen. Tämä sääntö asetetaan lähtöpäähän ja tarkoituksenamme oli testata toimintaa Kalilla, joka on ADMIN-NET:n alla. (Kuvio 18)



Kuvio 18. Liikennetulvasuojauksen asettaminen

Seuraavaksi testasimme toimintaa komennolla nmap 10.4.0.11. Katsoimme Palo-Altosta lokeja ja näimme, että kali tiputtaa näitä skannauksia, joten liikennetulvasuojaus toimii. (Kuvio 19)



Kuvio 19. Palo Alto uhkaloki

4 Pohdinta

Tietoturvakontrollien neljännessä laboratoriotyössä pääsimme taas mukavasti tutustumaan Palo Alton laajoihin ominaisuuksiin pieni pala kerrallaan. Navigointi Palo Altossa oli mielestämme jo

erittäin selkeää ja löysimme oikeat välilehdet ja kohdat nopeasti. Jopa sellaiset kohdat, mitä emme aiemmin olleet käyttäneet löytyi helposti. Labrassa oli paljon jo entuudestaan tuttua. Esimerkiksi turvallisuussääntöjen tekeminen ja muokkaaminen kävi nopeasti.

Opimme paljon uutta työtä tehdessä. Teoreettisella puolella opimme mitä Palo Alton antivirus, vulnerability protection, anti-spyware, file blocking ja wildfire protection tekevät ja mitä eroja niillä on. Käytännössä näimme lähinnä antiviruksen ja file blockingin toimintaa. Url-suodattimet vaikuttavat todella kätevältä työkalulta, etenkin, kun sieltä löytyy valmiita tunnisteita kuten tässä työssä käytetyt gambling ja gaming.

Liikennetulvasuojaus on myös tärkeä työkalu, mihin oli kiva päästä tutustumaan tässä vaiheessa. Se ilmeisesti tulee myöhemmissä harjoituksissa vielä vastaan, joten oli hyvä nähdä jo vähän sen toimintaa. Ihan kaikkia asetuksia emme vielä siellä ymmärtäneet, mutta eiköhän nekin selkeydy opintojaksojen edetessä.

Labran loppuvaiheilla oli kiva, kun pääsi käytännössä näkemään ja kokeilemaan mitä kaikki tehdyt asetukset tekevät. Ryhmällämme oli pieniä vaikeuksia saada yle.fi -sivuston esto toimimaan Google Chrome -selaimella, vaikka se toimi moitteetta Edgellä ja Firefoxilla. Hetken pähkäilimme ja yritimme ajaa sertifikaatin uudestaan Chromelle ja tutkimme Palo Alton asetuksia. Tajusimme sitten jossain vaiheessa, että kannattaa taas, kuten aiemmissakin labratöissä, tyhjentää välimuisti. Ennen kuin olimme painaneet commit Palo Altossa menneet chromella jo testaamaan yleä, joten etusivu oli jäänyt välimuistiin. Välimuistin tyhjentäminen auttoi tilanteeseen ja lopuksi myös yle.fi oli onnistuneesti estetty myös Chromella.

Lähteet

Anti Malware Testfile. Eicar.org -verkkosivusto. Viitattu 1.10.2024. https://www.eicar.org/download-anti-malware-testfile/

Flood Proteciton. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection

Network Security, Antivirus. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-antivirus

Network Security, Anti-Spyware. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware

Network Security, File Blocking. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-file-blocking

Network Security, Vulnerability Protection. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-vulnerability-protection

Network Security, WildFire Analysis. Paloalto Techdocs. 10.9.2024. Viitattu 30.9.2024 https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire