jamk

Tietoturvakontrollit - Labra 3

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Jukka Virtanen

Harjoitustyö

Helmikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tietoturvakontrollien kolmannessa labrassa määritellään aiempiin Palo Alto –konfiguraatioihin lisää turvallisuusominaisuuksia. Näitä ovat Antivirus, Vulnerability protection, Anti-spyware, File blocking, sekä Wildfire analysis. Tutustutaan hälytysten konfiguroimiseen havaituista viruksista sekä määritellyn selainliikenteen blokkaamiseen tai lokittamiseen. Jotta myös salattuun liikenteeseen saadaan em. ominaisuuksilla näkymä, konfiguroidaan Palo Altolle https-liikenteen purku. Myös extra-tehtävänä annettu Flood Protection toteutettiin ja testattiin.

2 Teoria

2.1 Antivirus

Antivirus-profiileilla voidaan suojautua viruksia, troijalaisia, matoja sekä spywarea vastaan. Palo Alto tutkii liikennettä lennossa ja pyrkii havaitsemaan haittaohjelmat ilman merkittävää vaikutusta suorituskykyyn. Profiilin asetuksilla määritellään mitä toimia havainnot aiheuttavat, esimerkiksi lokitus tai esto. Suodatusta voidaan tehdä SMTP, IMAP, POP3, FTP, HTTP ja SMB-liikenteelle. Kun palomuurilla on konfiguroitu liikenteen dekryptaus, voidaan haittaohjelmia havaita myös salatusta liikenteestä. (Security Profiles 2023.)

2.2 Vulnerability

Vulnerability protection -profiili estää yritykset hyödyntää järjestelmän haavoittuvuuksia tai saada luvaton pääsy järjestelmään. Profiili suojaa verkkoon tulevilta uhilta eli uhilta, jotka yrittävät tunkeutua verkkoa kohti. Esimerkiksi profiili auttaa suojaamaan puskurin ylivuodolta (buffer overflows), laittoman koodin suorittamiselta (illegal code execution) tai muilta yrityksiltä hyödyntää haavoittuvuuksia (exploit system vulnerabilities). Oletusarvoisesti profiili suojaa isäntiä (hosts) ja palvelimia kaikilta tunnetuilta kriittisiltä, korkeilta ja keskitason luokkien uhilta. Asetuksissa voi myös luoda poikkeuksia, joilla voidaan muuttaa suoja tiettyyn tunnisteeseen (signature). (Security profile: Vulnerability Protection 2024.)

2.3 URL filtering

URL suodatusteknologia suojaa käyttäjiä verkkopohjaisilta uhilta. Sen avulla voidaan hallita käyttäjien pääsyä ja vuorovaikutusta Internetissä. URL suodatuspolitiikalla voidaan rajoittaa pääsyä tietyille sivustoille URL kategorioiden, ryhmien ja käyttäjien perusteella. Tämän avulla organisaatiot voivat estää pääsyn sivustoille, joilla tiedetään olevan haittaohjelmia tai jotka ovat määritelty riskialttiiksi. URL suodatusprofiililla voidaan määrittää käyttöoikeudet ennalta määritetyille ja mukautetuille URL luokille ja URL suodatusprofiili voidaan liittää turvallisuuspolitiikan sääntöihin. URL suodatus auttaa hallitsemaan ja valvomaan paremmin käyttäjien verkkokäyttäytymistä sekä suojaa heitä mahdollisilta verkkohyökkäyksiltä. (URL Filtering Basics 2023.)

2.4 Anti-Spyware

Anti-Spyware-profiilit estävät vakoiluohjelmien lähettämän haitallisen liikenteen, kuten yhteydenottoyritykset ulkoisiin komento- ja ohjauspalvelimiin (C2). Profiileilla voidaan asettaa eri suojaustasoja eri vyöhykkeille, esimerkiksi tiukempi tarkastus epäluotettavasta vyöhykkeestä tulevalle liikenteelle. Voit luoda mukautettuja Anti-Spyware-profiileja tai käyttää valmiiksi määriteltyjä profiileja, kuten "Oletus" ja "Tiukka". "Oletus" käyttää Palo Alto Networksin määrittelemää oletustoimintoa ja "Tiukka" profiili estää kaikki kriittiset ja korkean vakavuuden uhkat. (Security Profiles 2023.)

Kun uhka havaitaan, Anti-Spyware-profiilissa voidaan määrittää toimet kuten "Allow" (sallii liikenteen ilman lokitusta), "Alert” (generoi hälytyksen uhkalokiin), "Drop" (pudottaa liikenteen), "Reset client" (katkaisee asiakaspuolen yhteyden), "Reset Server" (katkaisee palvelinpuolen yhteyden), "Reset both" (katkaisee molemmat yhteydet) ja "Block IP" (estää liikenteen määräajaksi). (Security Profiles 2023.)

2.5 Fileblocking

Tiedostojen estoprofiilit (File Blocking) mahdollistavat tiettyjen tiedostotyyppien estämisen tai valvonnan. Voit estää uhkia sisältäviä tai tarpeettomia tiedostoja useimmissa liikennetyypeissä, mukaan lukien sisäverkon liikenne. Esimerkkejä estettävistä tiedostoista ovat eräajotiedostot (batch files), DLL-tiedostot, Java-luokkatiedostot, ohjetiedostot, Windowsin pikakuvakkeet ja BitTorrent-tiedostot. Voit myös vaatia käyttäjiä kuittaamaan latauksensa, mikä lisää tietoisuutta selaimen taustoiminnasta. Tiukempi tiedostojen estoprofiili on suositeltavaa liittää yleiseen verkkoselaamiseen liittyviin tietoturvakäytäntöihin, koska haitallisten tiedostojen lataamisen riski on suurempi. (Palo Alto – Set up file blocking 2023.)

Voit luoda omia mukautettuja tiedostojen estoprofiileja tai käyttää valmiiksi määriteltyjä profiileja, kuten perustiedoston esto ja tiukka tiedostojen esto, jotka ovat saatavilla sisältöversiosta 653 alkaen. Perustiedoston esto estää yleisiä haittaohjelmiin liittyviä tiedostotyyppejä ja tiukka tiedostojen esto lisää estolistalle useita muita tiedostotyyppejä. Voit muokata näitä profiileja tarpeen mukaan ja soveltaa niitä turvallisuuskäytäntösääntöihin. On tärkeää käyttää muita turvatoimia, kuten WildFire-analyysiä ja URL-suodatusta, varmistaaksesi, että lataukset eivät aiheuta uhkaa organisaatiollesi. (Palo Alto – Set up file blocking 2023.)

2.6 WildFire

WildFire on PaloAlton pilvipohjainen palvelu, se käyttää jatkuvaa reaaliaikaista koneoppimista, joten uusia uhkia löytäessään, jos tuntematon tiedosto vastaa olemassa olevaan sormenjälkeen tai on luokiteltuna PaloAlton ML-Powered NGFW (virtuaalikone) järjestelmässä. Se suorittaa tiedostoanalyysin, poimii tarvittavan tiedon ja datan turva-analyysiin, päivittää koneoppimisen harjoitusmallit ja jakaa tiedon muiden käyttäjien kanssa. WildFire tunnistaa mahdollisia haitallisia malleja ja vastaa niihin uhkatieto analyysin ja korrelaation pohjalta. WildFire pystyy tunnistamaan uhkia sadoissa sovelluksissa, esimerkiksi sähköposti ja tiedostonjako protokollissa salauksesta huolimatta. Seuraa epäilyttävän tiedoston kaikkea verkkoliikennettä, mm. takaportin luomista, seuravan vai-

heen haittaohjelmien lataamista ja tietoverkko tiedustelua. Fileless attack/script detection havaitsee mahdollisia pahansuopia skriptejä kuten JScriptejä sekä PowerShell-skriptejä niiden kulkiessa verkon läpi ja ohjaamaa ne WildFireen analysoitavaksi ja toteutettavaksi. (WildFire 2023.)

2.7 Flood Protection

Flood protection on osa Zone Protection -profiilia. Se puolustaa koko sisääntulovyöhykettä SYN, ICMP, ICMPv6, UDP ja muiden IP-tulva-iskujen varalta. Palomuuri mittaa kunkin tulvatyypin kokonaisuutta vyöhykkeeseen tulevissa uusissa yhteyksissä sekunnissa (CPS) ja vertaa kokonaismääriä niihin kynnysarvoihin, jotka on määrittänyt Zone Protection -profiilissa. Flood protectionissa:

Alarm Rate säännöllä, ympäristöön voidaan asettaa CPS- kynnysarvo, jos arvo ylittyy palomuuri hälyttää. Arvon ollessa oikein asetettu turhia hälytyksiä ei synny liikennemäärien vaihdellessa normaalisti.

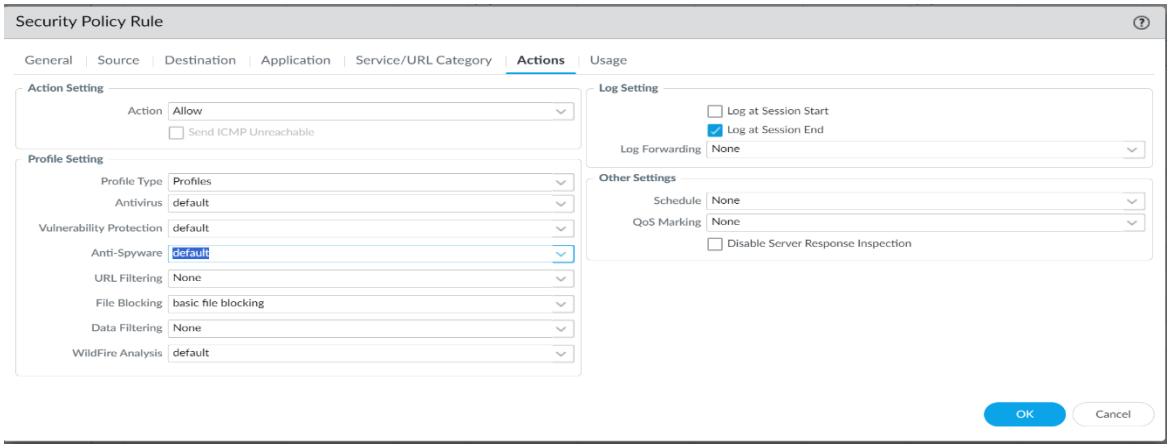
Activate säännöllä flood protection mekanismi voidaan käynnistää ja uusia yhteyksiä voidaan tarvittaessa alkaa droppaamaan. Arvo voidaan asettaa esimerkiksi juuri CPS:n oletetun huippuarvon yläpuolelle, jolloin mahdollisia tulvia voidaan lieventää.

Maximum – säännöllä yhteyksiä voidaan pudottaa, kun palomuurille tulee liikaa liikennettä. Maximum sääntöä asetettaessa on otettava huomioon myös muut palomuurin resursseja syövät toiminnot. (Flood Protection 2023.)

3 Toteutus

3.1 Ympäristön turvallisuuden lisääminen

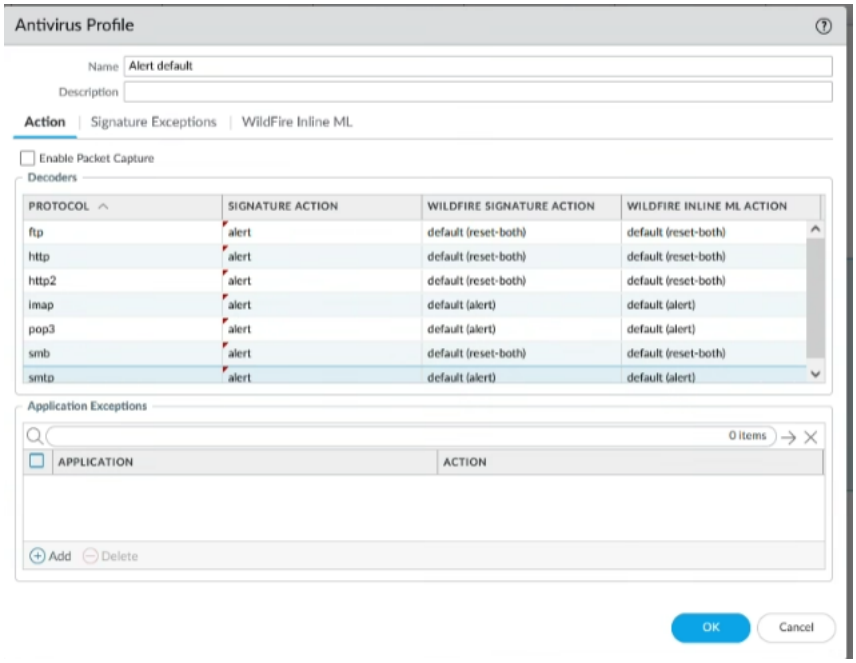
Loimme uuden säännön DMZ-TO-VLE-ANT-VUL-SPY-FIL-WILD, asetimme sille lähteeksi DMZ ja kohteeksi VLE. Seuraavaksi konfiguroimme tehtävänannon mukaiset Antivirus, Vulnerability protection, Anti-spyware, File blocking, sekä Wildfire analysis –profiilit päälle default-asetuksillaan (ks. Kuvio 1).



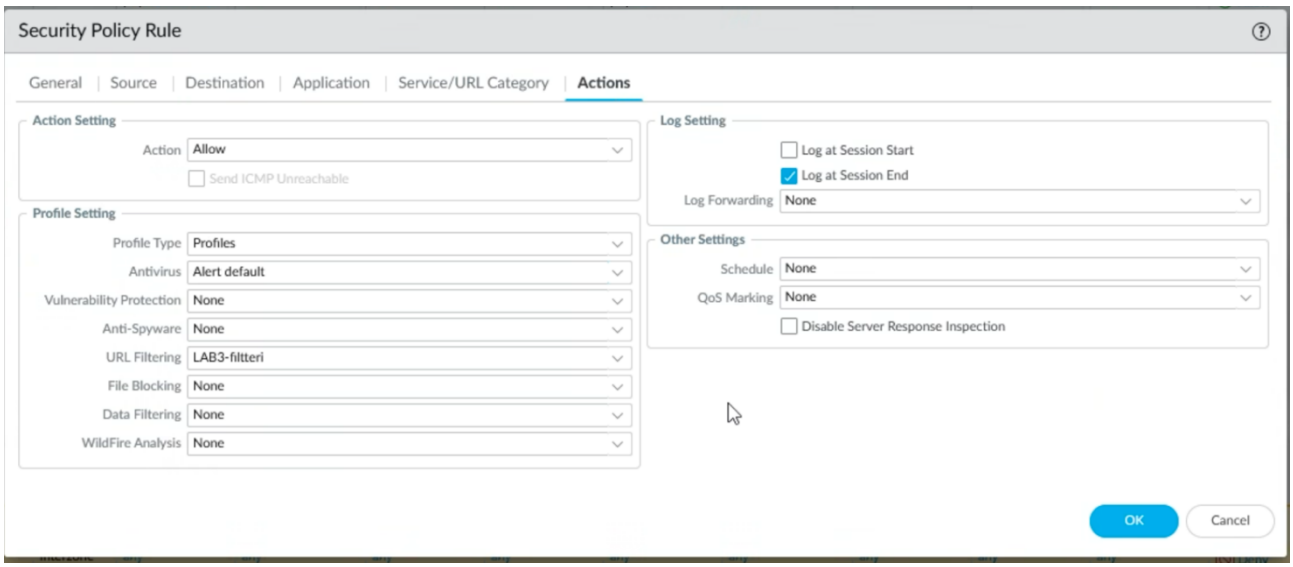
Kuvio 1. Turvallisuusprofiilit

3.2 Antivirus hälytykset

Seuraavaksi piti ottaa käyttöön antivirus -profiili, joka suojaa WS-netistä VLE:en menevää liikennettä ja pakettien tarkistamista vastaanottamisen jälkeen. Suojaus asetetaan päälle Objects – Security Policies – Antivirus. Kopioidaan oletussääntö ja nimetään kopio Alert defaultiksi. Asetuksissa asetetaan siten, että profiili antaa hälytyksiä (ks. Kuvio 2). Tämän jälkeen tehdään uusi sääntö, joka nimetään WS-NET-TO-VLE-WEB. Sääntöön lisätään Actions välilehden asetuksissa Alert default antivirus -profiili (ks. Kuvio 3).



Kuvio 2. Luodaan Antivirus -profiili



Kuvio 3. WS-net to VLE sääntö, johon asetetaan antivirus -profiili

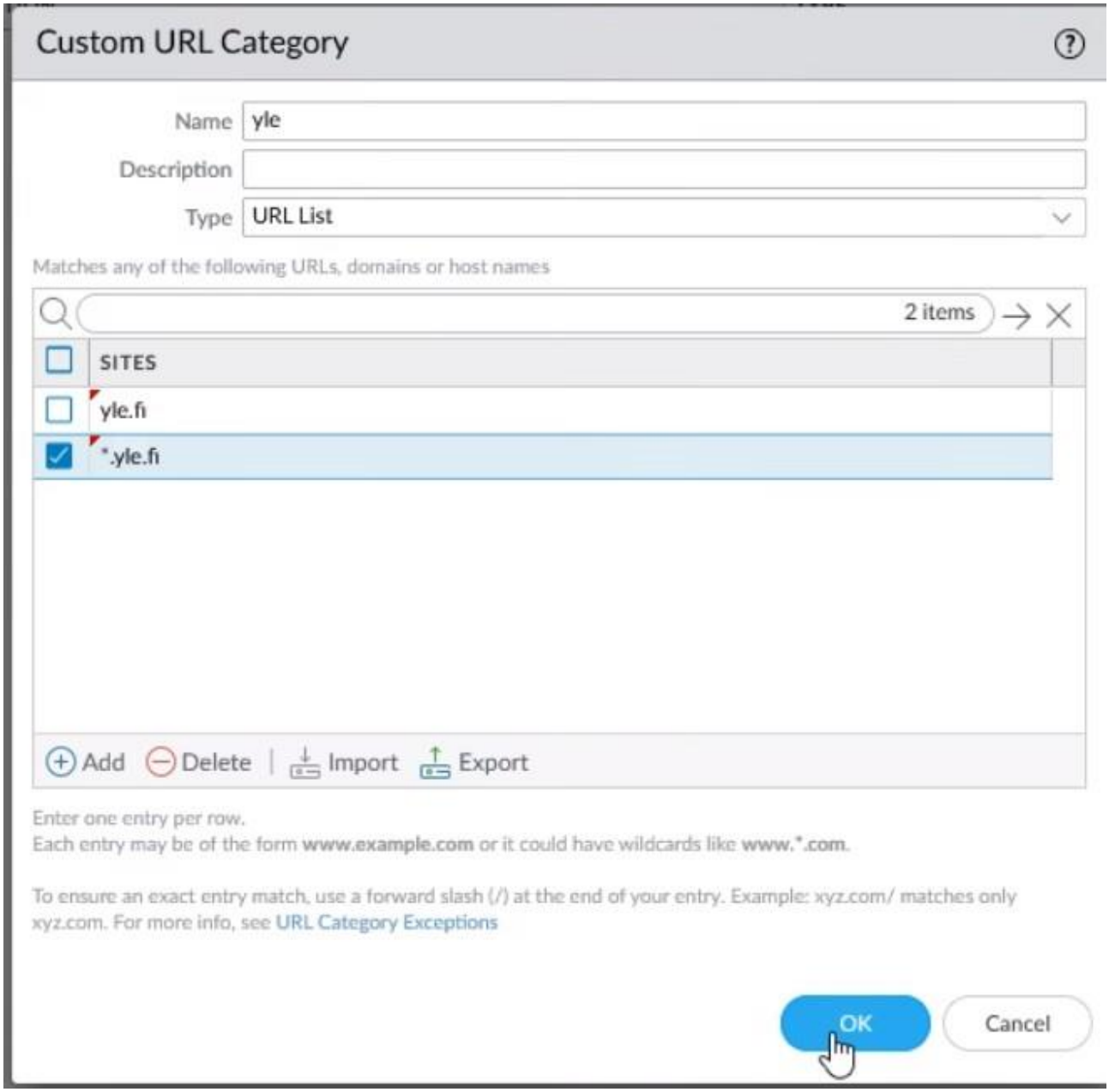
3.3 URL filtteröinti

Teimme uuden säännön ja asetimme sen ylimmäksi. Tähän sääntöön laitoimme application kohtaan web-browsing ja profile kohtaan tekemämme antivirus profiilin sekä URL filtering profiilin (ks. Kuvio 4).

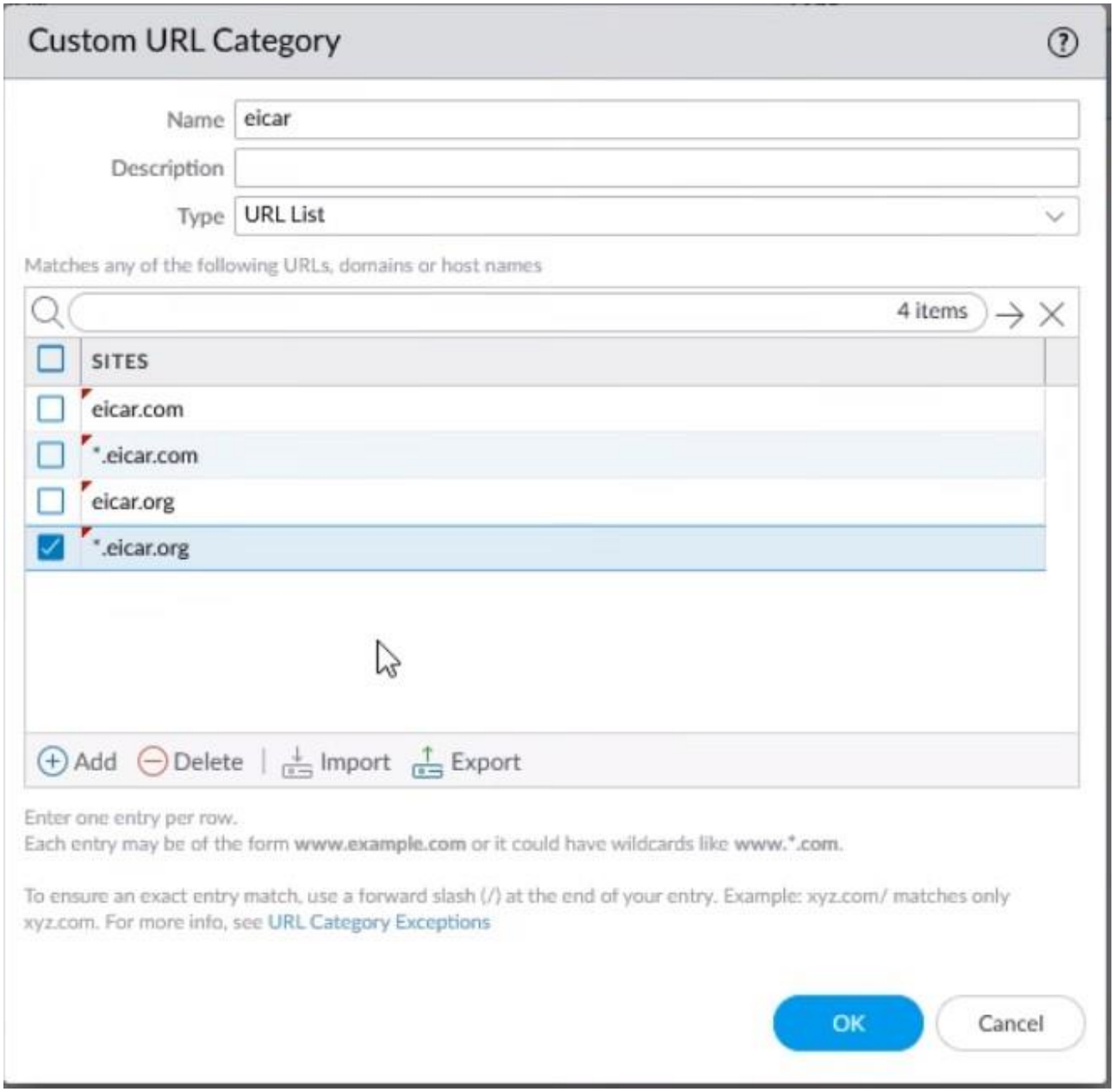
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	Rule Usage HIT COUNT	Rule Usage LAST HIT	Rule Usage FIRST HI
1	WS-NET-TO-VLE-URL	none	universal	WS-NET	any	any	any	VLE	any	any	web-browsing	application-...	Allow			12426	2024-02-07 15:03:46	2024-02
2	WS-NET-TO-VLE-A...	none	universal	WS-NET	any	any	any	VLE	any	any	any	application-...	Allow			231	2024-02-07 15:03:46	2024-02
3	DMZ-TO-VLE-ANT-...	none	universal	DMZ	any	any	any	VLE	any	any	any	application-...	Allow			692	2024-02-07 14:58:37	2024-02

Kuvio 4. Sääntö web-browsingia varten

Menimme URL Category välilehdelle ja teimme ylelle sekä eicarille omat kategoriat, johon kuului molempien sivustojen kaikki sivut (ks. Kuvio 5 ja Kuvio 6).

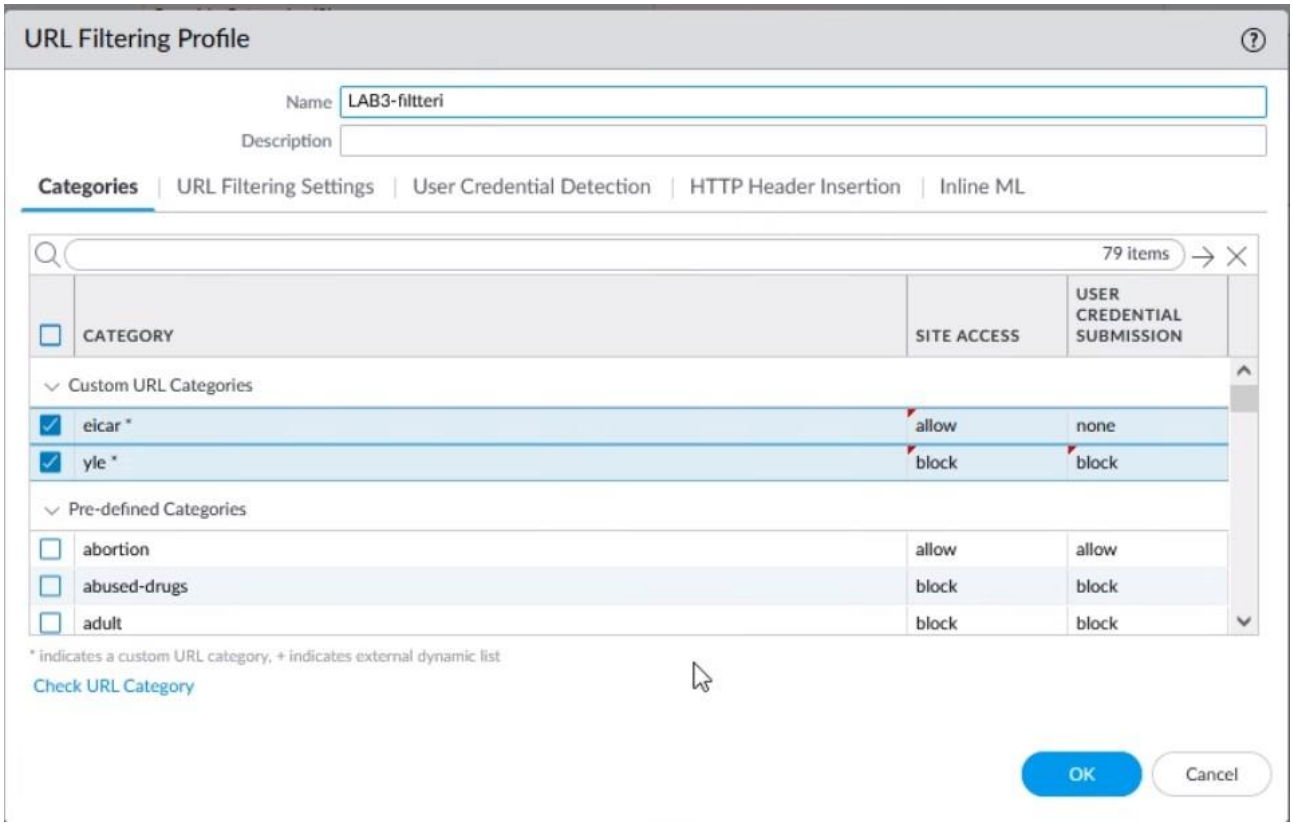


Kuvio 5. Ylen kategoria

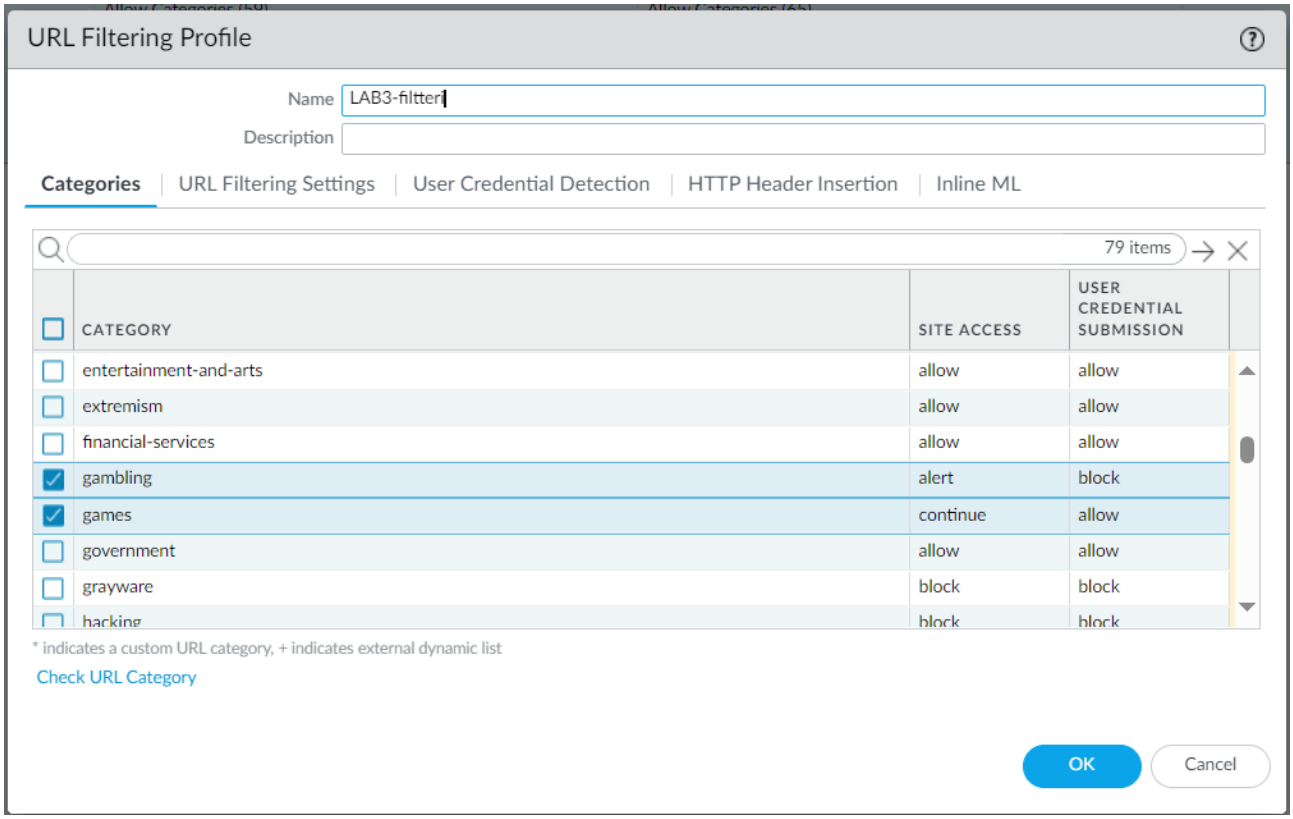


Kuvio 6. Eicarin kategoria

URL Categoryn jälkeen menimme URL Filtering välilehdelle ja kopioimme valmiina olleen profiilin. Annoimme kopiolle nimen ja laitoimme Ylen estoon ja Eicarin allow tilaan. Games sivustot laitoimme continue tilaan ja uhkapelisivustot aiheuttavat hälytyksen (ks. Kuvio 7 ja Kuvio 8).

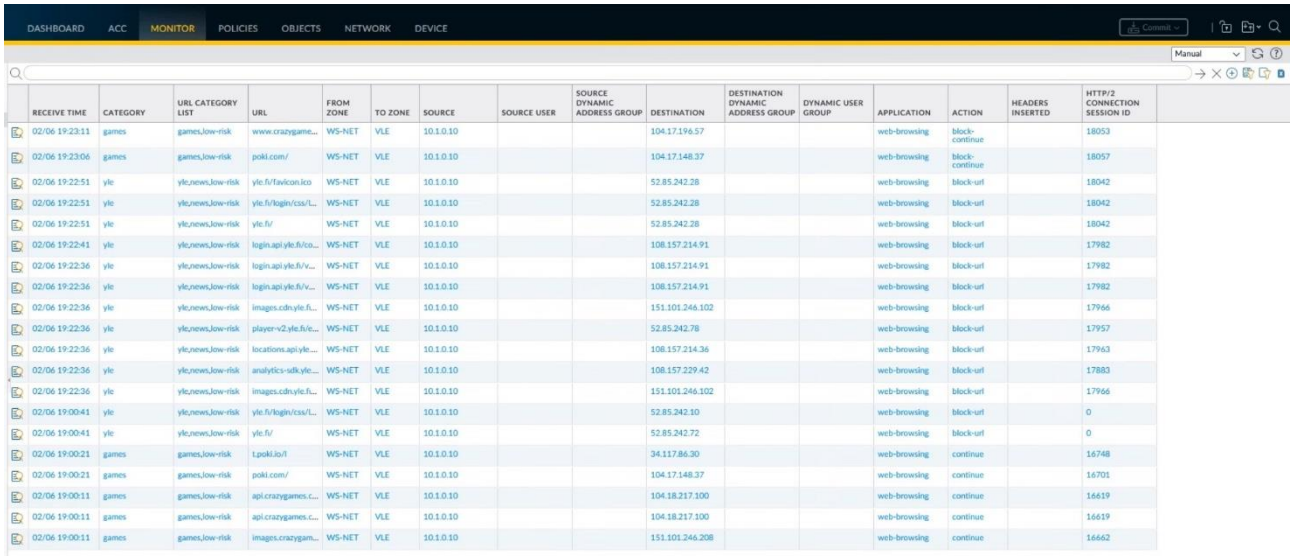


Kuvio 7. Ylen ja Eicarin asetukset

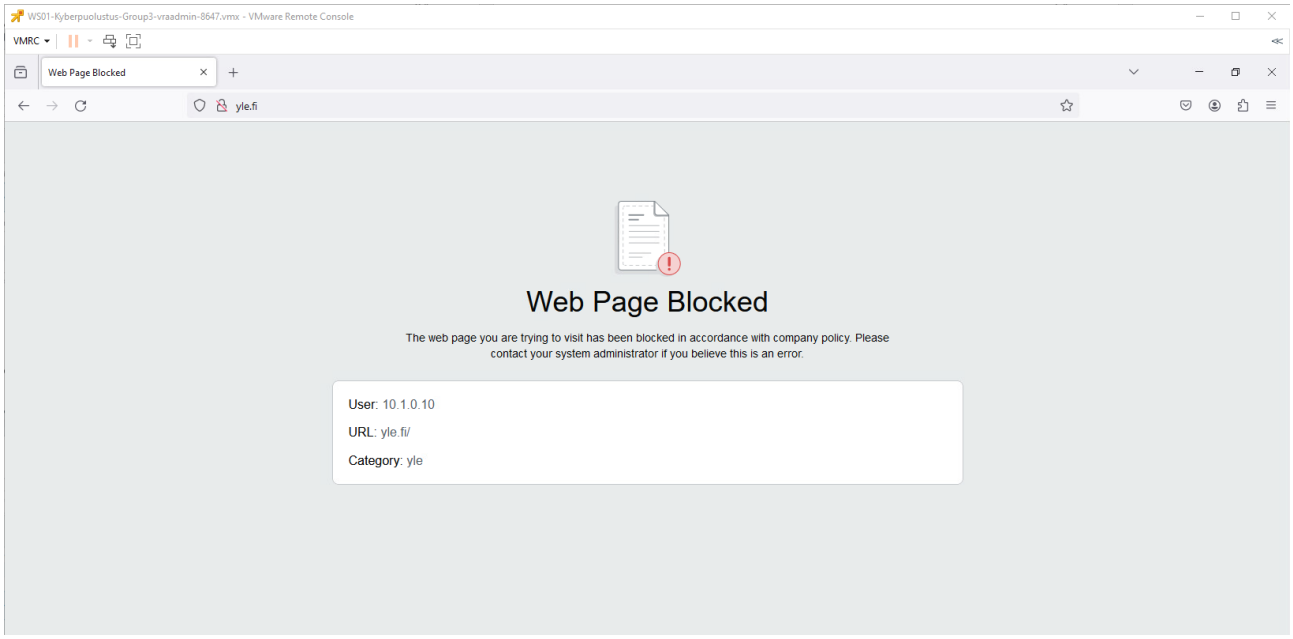


Kuvio 8. Gamblingin ja gamesin asetukset

Lopuksi seurasimme monitoria, josta näimme URL filttereiden toimivan, kun yritimme käydä Ylen sivulla tai pelisivustolla (ks. Kuvio 9 ja Kuvio 10).



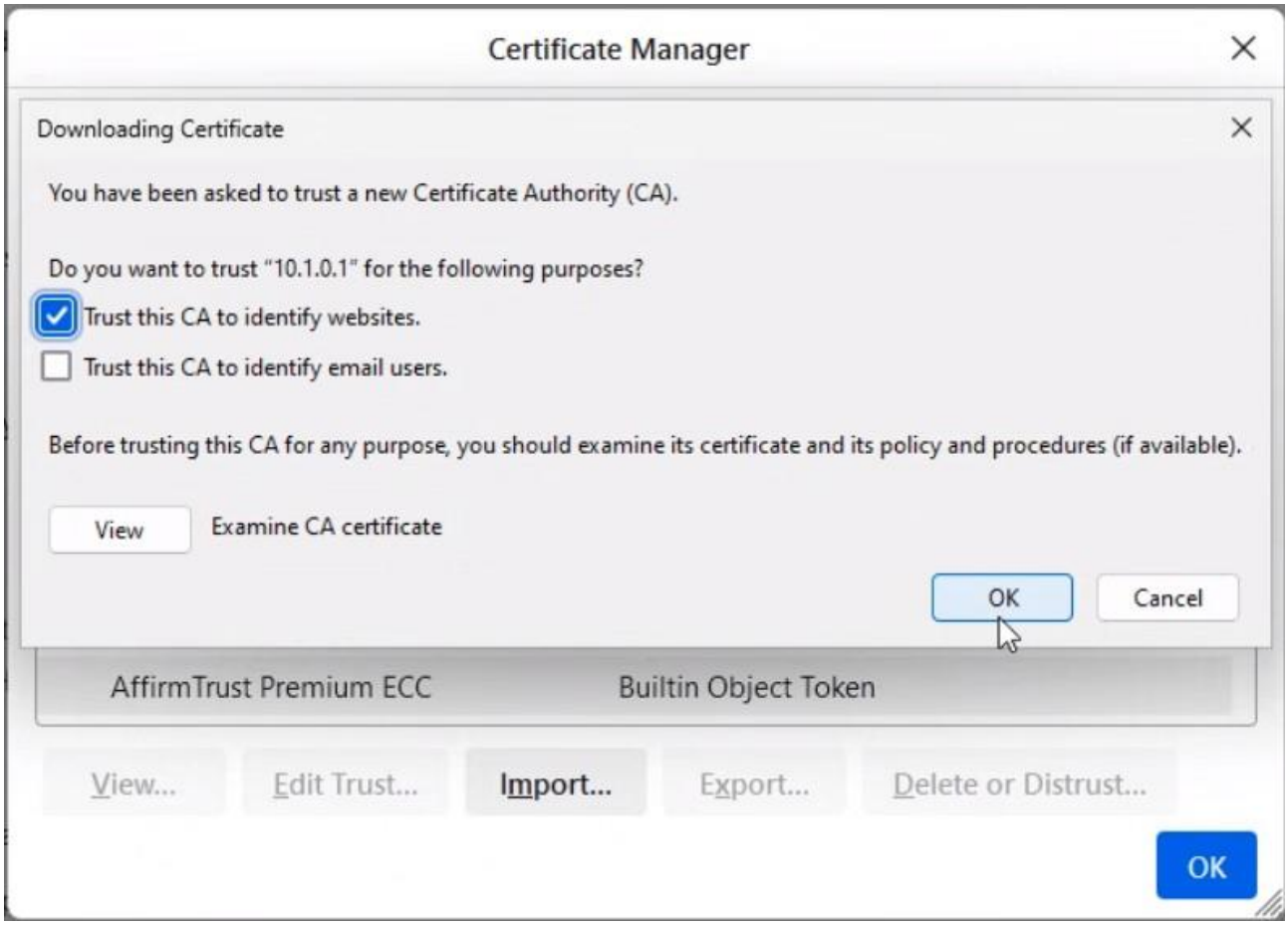
Kuvio 9. Monitor välilehti



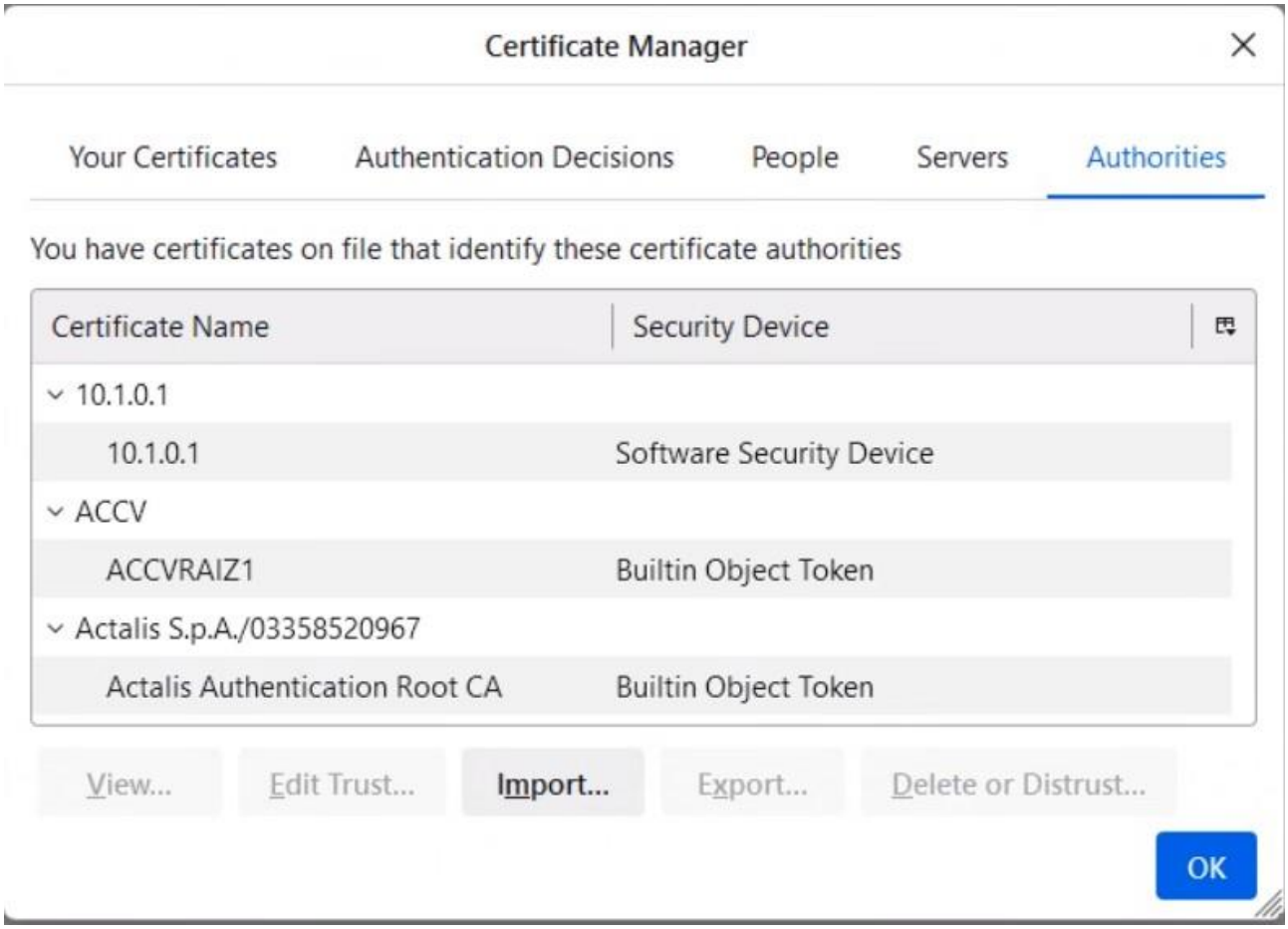
Kuvio 10. Yle estetty

3.4 Sertifikaatti

Labran viides vaihe aloitettiin luomalla sertifikaatti (device-> certificates). Annoimme omalle sertifikaatillemme nimeksi ”PA decrypt trusted” ja common nameen ws01 koneen gateway, 10.1.0.1. ohjeistuksen mukaisesti. Tälle sertifikaatille annettiin lupa tunnistaa verkkosivustoja (ks. Kuvio 11). Seuraavaksi kirjauduimme palomuurille ws01 koneella, latasimme sertifikaatin koneelle paloalton export-toiminnolla ja lisäsimme sen Firefoxin privacy and security- featureissa sertifikaatteihin (ks. Kuvio 12).

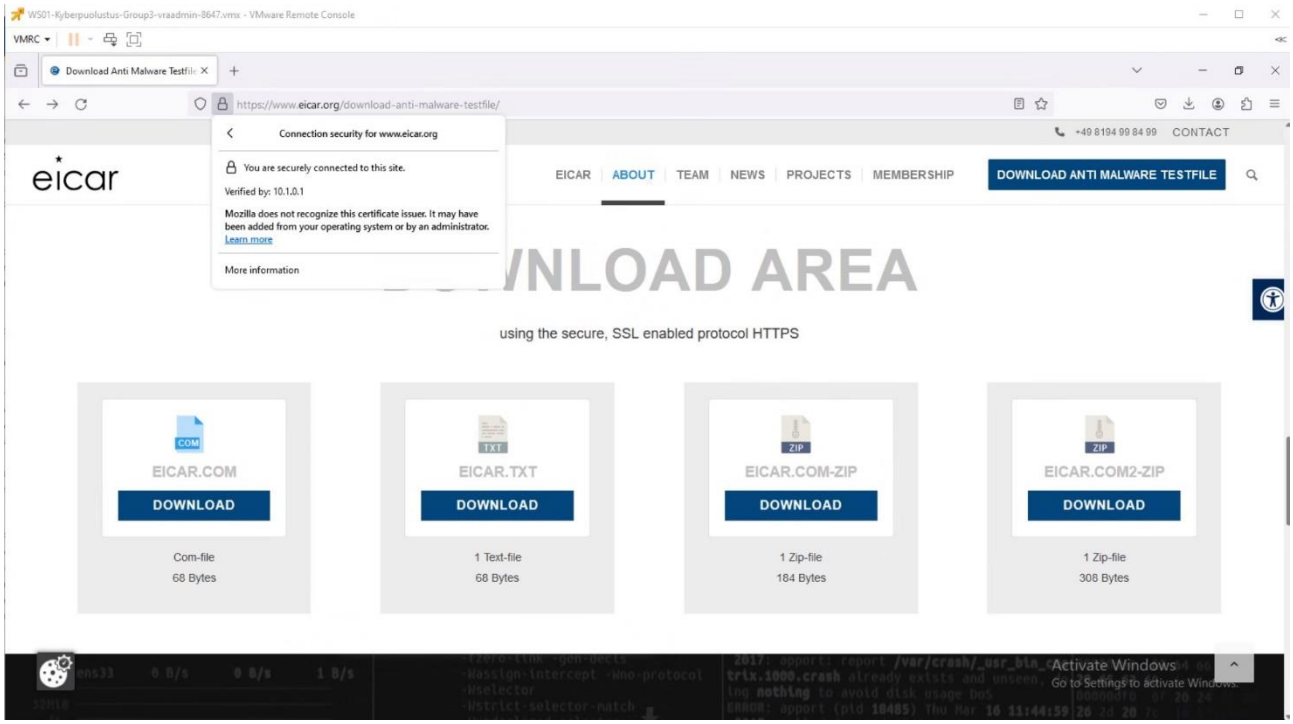


Kuvio 11. Sertifikaatti identifioi verkkosivut

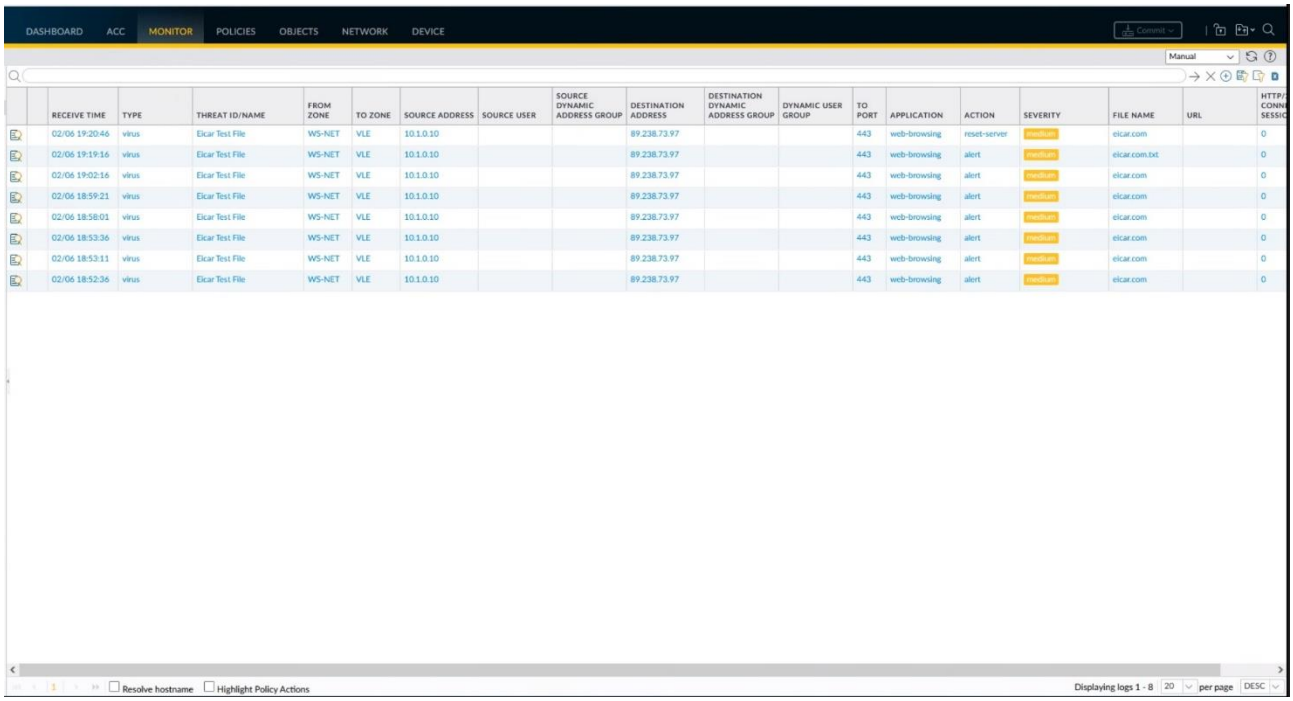


Kuvio 12. Sertifikaatti lisätty Firefox-selaimeen

Varmistimme selaimella, että laatimamme sertifikaatti oli käytössä eicarin sivustolla (ks. Kuvio 13). PaloAlton monitoroinnista (ks. Kuvio 14.), näkyy Alert-säännön mukainen ilmoitus palomuurilla.



Kuvio 13. Sertifikaatti eicarin sivuilla



Kuvio 14. Palomuuri havaitsee tiedoston lataamisen

Kun sertifikaatti oli ladattu selaimeen, loimme palomuurille uuden Decryption säännön ”Pura salaus sivuilta-LAB3”. Säännön mukaan eicar, yle, gambling ja games sivustoilta tullut liikenne puretiin tarkastusta varten. SSL Forward Proxy- tilassa, palomuuri toimii välityspalvelimena, lopettaen SSL/TLS-istunnon clientin ja serverin puolesta. Tämän takia palomuuri voi tarkastaa puretun sisällön. (ks. Kuvio 15).

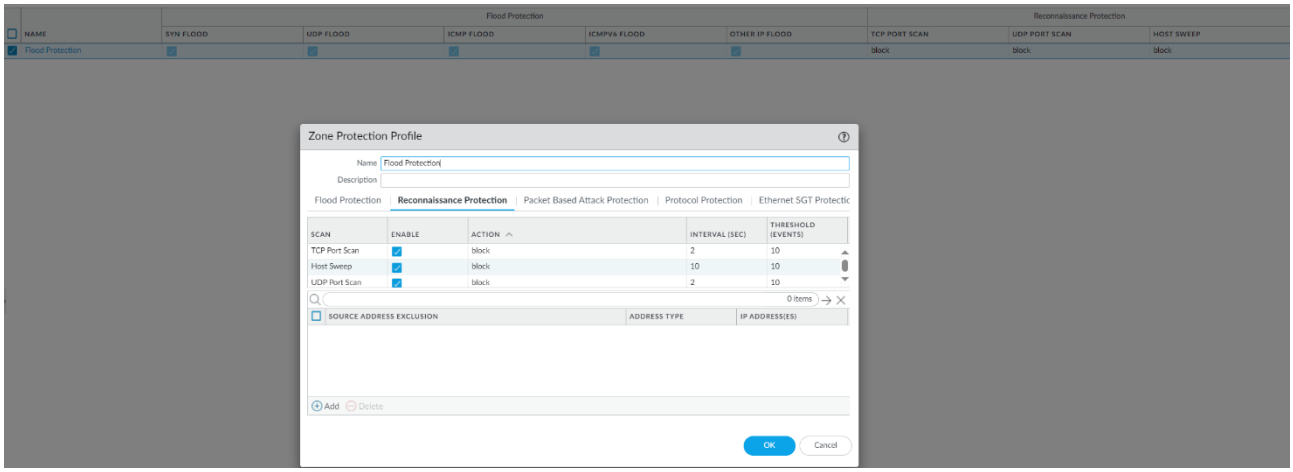
Kuvio 15. Decryption sääntö

3.5 Flood Protection

Aloitimme sallimalla liikenteen Kalilta WWW-palvelimelle (ks. Kuvio 16).

Kuvio 16. Liikenne Kalilta WWW-palvelimelle sääntö

Zone Protection löytyi Network välilehdeltä. Annoimme profiilille nimen ja laitoimme skannien eston päälle sekä rajan 10:een. Tämä Zone Protection profiili myös liitettiin ADMIN-NET Zoneen (ks. Kuvio 17 ja Kuvio 18).

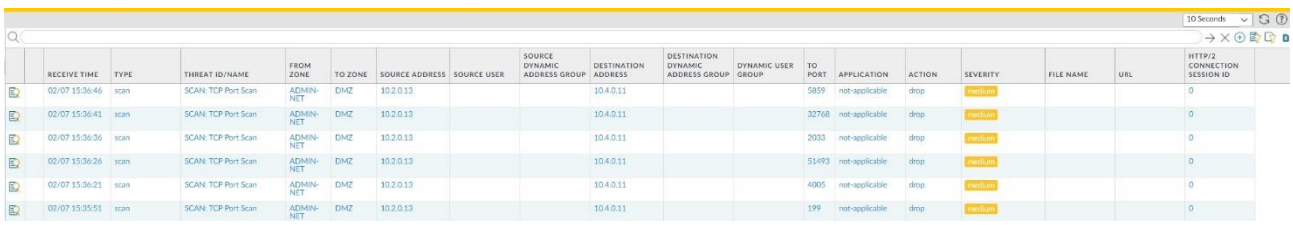


Kuvio 17. Skannien esto

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION
ADMIN-NET	layer3	ethernet1/6.102	Flood Protection	✓
DMZ	layer3	ethernet1/6.104		✓
SERVERS-NET	layer3	ethernet1/6.103		✓
VLE	layer3	ethernet1/5		✓
VPN-ZONE	layer3	tunnel.1		✓
WS-NET	layer3	ethernet1/6.101		✓

Kuvio 18. Flood Protection ADMIN-NET Zonessa

Tarkistimme WWW-palvelimen IP-osoitteen, joka oli 10.4.0.11. Avasimme Kalin terminaalin ja syötimme komennon nmap 10.4.0.11 joka skannaa portteja. Monitor välilehdellä avasimme Threat osion ja näimme että ADMIN-NETistä yritetään skannata DMZ zoneen (ks. Kuvio 19).



Kuvio 19. Monitorin Threat osio

4 Pohdinta

Tämä harjoitus oli erittäin mielenkiintoinen ja erinomainen oppimiskokemus. Oli todella hyödyllistä saada syvempää ymmärrystä erilaisista turvallisuusprofiileista, joita PaloAlto:n palomuuri tarjoaa. Erityisen mielenkiintoista oli päästä käytännössä toteuttamaan URL-suodatus sekä purkamaan HTTPS-salaus. Lisäksi huomasimme, että PaloAlton dokumentaation lukeminen sujui entistä paremmin, ja valmistautuminen tehtävään oli vaivatonta, koska turvallisuusprofiilit oli esitetty selkeästi ja asetuksiin navigointi oli helppoa. Tämä nopeutti itse labra -harjoituksen tekoa, ja tehtävien suorittaminen oli yllättävän sujuvaa.

Tällä kertaa koimme eniten pohdintaa siitä, miksi emme päässeet heti tehtävien suorittamisen jälkeen WS01 -työasemalla internettiin VLE:n kautta. Haaste näyttäytyi niin, että nettiliikenne ei osunut tehtävässä 3. asetettuun web-browsing sääntöön, vaikka näin oletimme tapahtuvan. Nettiliikenne pysähtyi vasta sääntöjen viimeiseen riviin, mikä esti kaiken liikenteen. Asiaa pohdittiin ja kokeiltiin erilaisia lähestymistapoja, ja lisäksi konsultoimme Jarmoa. Pienen harkinnan jälkeen huomasimme, että olimme ymmärtäneet tehtävänannon eri tavalla. Meidän piti luoda neljä turvallisuussääntöä sen sijaan, että olimme luoneet alussa vain kolme. Meiltä puuttui alla olevassa listauksessa esitetty sääntö 2.

1. Sääntö: WS-NET-TO-VLE-WEB, johon on asetettu application sääntöön web-browsing sekä filtteröinti. Tähän sääntöön menee esimerkiksi YLE.fi blokki ja Eicar filu HTTPS-salauksen purun jälkeen.
2. Sääntö: WS-NET-TO-VLE-ANY, johon asetettu application sääntöön any ja antivirus alert default. Tämä sääntö päästää VLE:n nettiin, mikäli liikenne ei ole blokki listalla.
3. Sääntö: Tämä ei aiheuttanut sen enempää mietintää. DMZ-TO-VLE-VUL-SPY-FIL-WILD. Tähän laitettiin tehtävänannon mukaisesti turvallisuusprofiilit
4. Sääntö: Tämä oli selkeä eli KALI-TO-WWW, jolla varmistetaan porttiskannaus haluttuun WWW-palvelimeen.

Tämän kokonaisuuden, kun ymmärsimme ja opimme, toimi liikenne halutulla tavalla. Eniten aiheutti pohdintaa, miksei web-browsing sallinut VLE:en nettiliikennettä. Ilmeisesti liikenne ei osu tähän sääntöön, vaan se tapahtuu vasta säännössä 2.

Lähteet

Flood Protection. 23.12.2023. Viitattu 11.2.2024. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection

URL Filtering Basics. 15.12.2023. Viitattu 7.2.2024. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics

Security Profiles. 23.12.2023. Viitattu 8.2.2024. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles

Security Profile: Vulnerability Protection. 2024. Viitattu 10.2.2024. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-vulnerability-protection

Palo Alto – Set up file blocking. 3.12.2023. Viitattu 9.2.2024. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/set-up-file-blocking#idab30127f-3fb2-4a84-99e6-30d7009860fc

WildFire. 2023. Viitattu 8.2. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/wildfire