



## 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

## Sisältö

<b>1</b>	<b>Johdanto.....</b>	<b>3</b>
<b>2</b>	<b>Teoria.....</b>	<b>3</b>
2.1	Antivirus.....	4
2.2	Vulnerability Protection.....	4
2.3	Anti-Spyware.....	4
2.4	File Blocking.....	4
2.5	WildFire Analysis.....	5
2.6	Flood Protection.....	5
2.7	EICAR-testitiedosto.....	5
<b>3</b>	<b>Työn kulku .....</b>	<b>5</b>
3.1	HTTPS-salauksen purku.....	12
3.2	Testaaminen.....	14
3.3	Liikennetulvasuojaus .....	17
<b>4</b>	<b>Pohdinta .....</b>	<b>18</b>
	<b>Lähteet .....</b>	<b>20</b>

## Kuviot

Kuvio 1.	Turvallisuussäännön asetukset .....	6
Kuvio 2.	Antivirusprofiilin säännöt.....	7
Kuvio 3.	Antivirussäännön asettaminen .....	8
Kuvio 4.	Web-browsing sovellus.....	8
Kuvio 5.	URL-suodattimen asetukset.....	9
Kuvio 6.	Kustomoidut URL-kategoriat.....	9
Kuvio 7.	Url-suodattimen muokkaus .....	10
Kuvio 8.	Suodattimen asettaminen turvallisuussääntöön .....	11
Kuvio 9.	Lisäosien asentaminen.....	11
Kuvio 10.	Sertifikaatin luonti .....	12
Kuvio 11.	Sertifikaatin asentaminen WS01-työaseman selaimelle .....	13
Kuvio 12.	Pura_salaus_sivulta purkusäännön asetukset .....	13

Kuvio 13. Yle.fi estetty.....	14
Kuvio 14. Pelisivustot .....	15
Kuvio 15 Palo Alton loki.....	16
Kuvio 16. Estetty lataus .....	16
Kuvio 17. Liikennetulvasuojauksen asetukset.....	17
Kuvio 18. Liikennetulvasuojauksen asettaminen .....	18
Kuvio 19. Palo Alto uhkaloki .....	18

## 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 palomuriin, 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 vakuuden 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 tiedostotyyppin 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. Palomuuuri seuraa, kuinka monta uutta yhteyttä muodostetaan sekunnissa (CPS, connections-per-second) jokaisesta flood-hyökkäystyypistä. Sitten se vertaa näitä määriä ennalta asetettuihin rajoihin, jotka määrittellään flood protection-profiiliin. Jos liikenne ylittää nämä rajat, palomuuuri 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.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The window is divided into several sections:

- Action Setting:**
  - Action: **Allow** (dropdown menu)
  - ☐ Send ICMP Unreachable
- Profile Setting:**
  - Profile Type: **Profiles** (dropdown menu)
  - Antivirus: **default** (dropdown menu)
  - Vulnerability Protection: **default** (dropdown menu)
  - Anti-Spyware: **default** (dropdown menu)
  - URL Filtering: **default** (dropdown menu)
  - File Blocking: **basic file blocking** (dropdown menu)
  - Data Filtering: **None** (dropdown menu)
  - WildFire Analysis: **default** (dropdown menu)
- Log Setting:**
  - ☒ Log at Session Start
  - ☒ Log at Session End
  - Log Forwarding: **None** (dropdown menu)
- Other Settings:**
  - Schedule: **None** (dropdown menu)
  - QoS Marking: **None** (dropdown menu)
  - ☐ Disable Server Response Inspection

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

Kuvio 1. Turvallisuussäännön asetukset

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

Antivirus Profile

Name

Alert Default

Description

Action

Signature Exceptions

WildFire Inline ML

☐ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
http	alert	alert	alert
http2	alert	alert	alert
smtp	default (alert)	default (alert)	default (alert)
map	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
ftp	alert	alert	alert
immb	alert	alert	alert

Application Exceptions

0 items

APPLICATION	ACTION

+

 Add
 

-

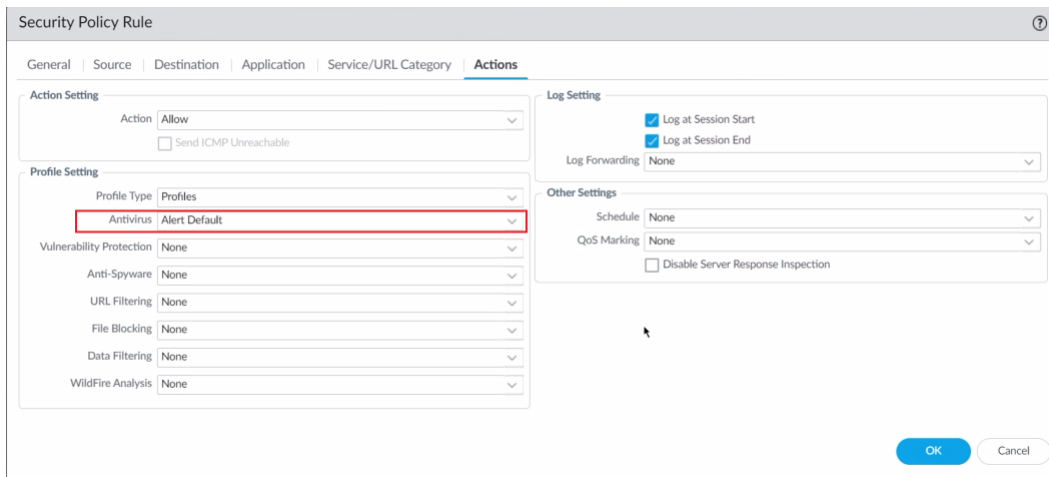
 Delete

OK

Cancel

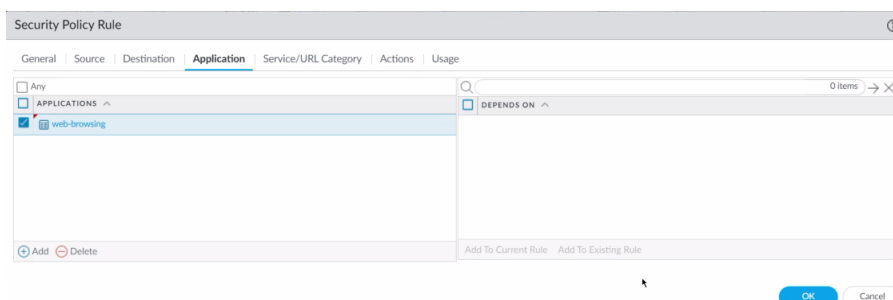
## Kuvio 2. Antivirusprofiilin säännöt

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

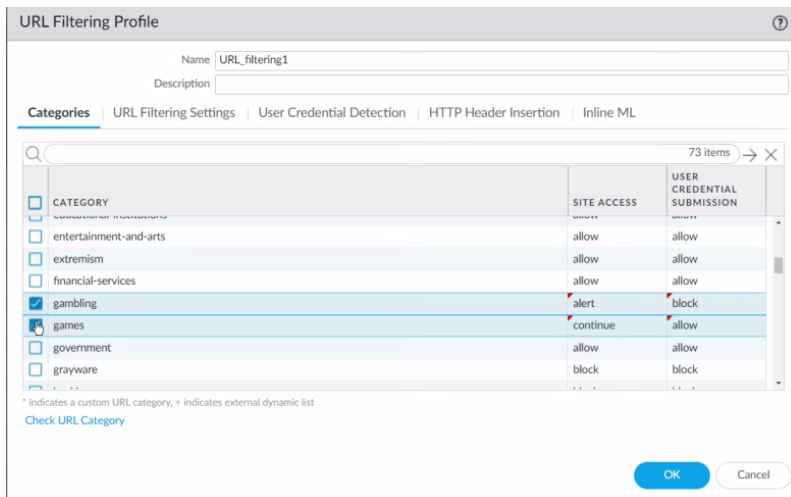
Loimme vielä yhden uuden säännön nimeltä WS-net\_to\_VLE\_netbrowsing. Siihen asetimme lähteeksi WS-NET:n ja määränpääksi VLE:n. Application-välilehdellä lisäsimme ainoastaan yhden sovelluksen, joka oli web-browsing. (Kuvio 4)



Kuvio 4. Web-browsing sovellus

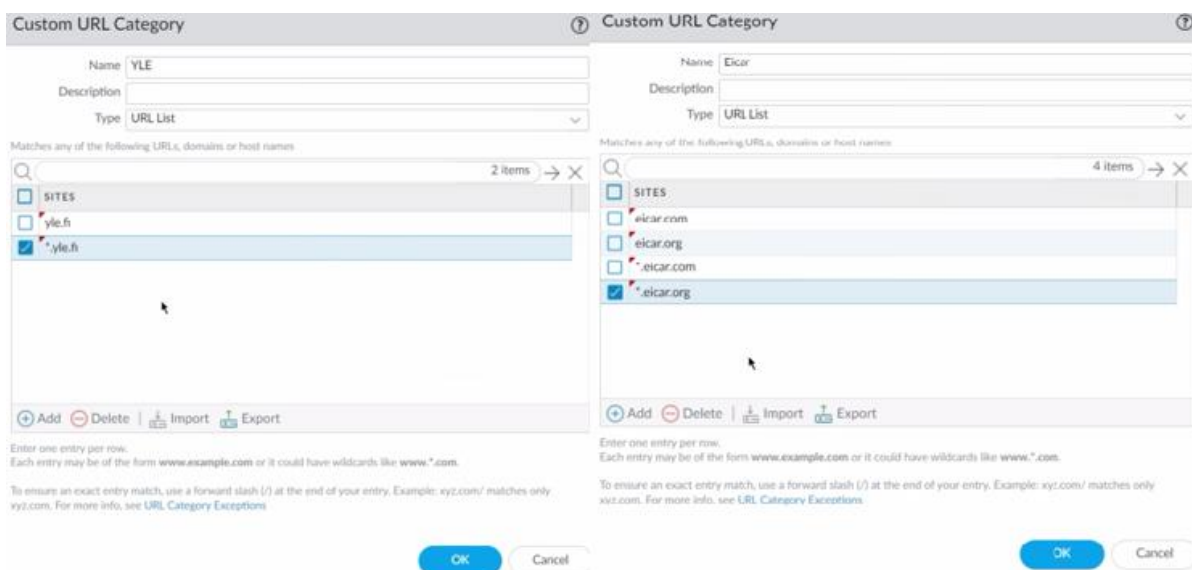
Siirryimme Objects-välilehdelle kohtaan URL filtering, joka löytyi Security Profiles -otsikon alta. Siellä loimme kopion default-säännöstä ja nimesimme sen nimellä URL\_filtering1. Teimme muokkauksia uhkapeli- ja pelisivustojen käsittelyyn: uhkapelisivustoille mennessä palomuriin tulee ilmoitus ja pelisivustoille 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

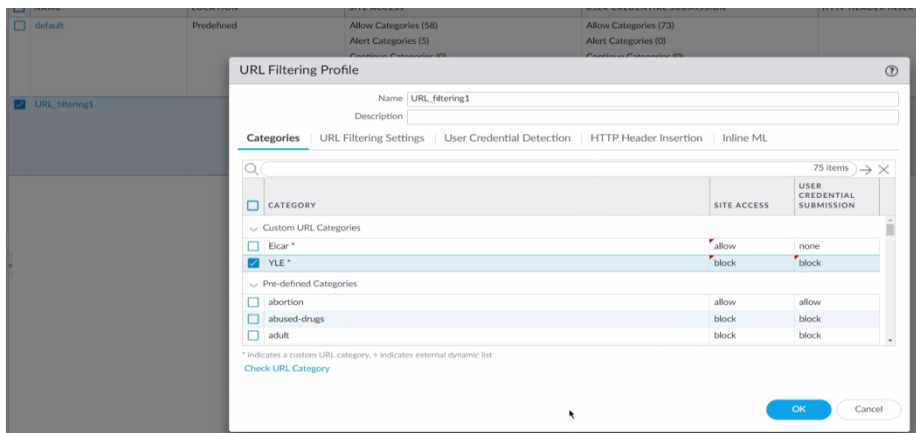
Teimme kaksi uutta kustomoitua URL-kategoriaa. Ensimmäinen ole yle.fi-sivustolle ja toinen eicar-sivustolle. Eicarille laitoimme päätteet .com ja .org, koska molemmilla päätteillä pääsee sivustolle. (Kuvio 6)



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)

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	INSTALLED	ACTION	DOCUMENTATION
Antivirus	Last checked: 2024/09/24 14:45:05 EEST	Schedule: None								
947-5465	panup-all-antivirus-4947-5465			99 MB	ME7a5E84...	2024/09/20 14:04:12 EEST			Download	Release Notes
948-5466	panup-all-antivirus-4948-5466								Download	Release Notes
949-5467	panup-all-antivirus-4949-5467								Download	Release Notes
950-5468	panup-all-antivirus-4950-5468								Download	Release Notes
951-5469	panup-all-antivirus-4951-5469								Download	Release Notes
Applications and Threats	Last checked: 2024/09/24 14:45:05 EEST	Schedule: None								
886-8935	panupv2-all-content-8886-8935								Download	Release Notes
887-8937	panupv2-all-content-8887-8937								Download	Release Notes
888-8941	panupv2-all-content-8888-8941								Download	Release Notes
889-8949	panupv2-all-content-8889-8949								Download	Release Notes
890-8951	panupv2-all-content-8890-8951								Download	Release Notes
891-8956	panupv2-all-content-8891-8956								Download	Release Notes
892-8959	panupv2-all-content-8892-8959								Download	Release Notes
893-8964	panupv2-all-content-8893-8964								Download	Release Notes
894-8969	panupv2-all-content-8894-8969								Download	Release Notes
895-8974	panupv2-all-content-8895-8974								Download	Release Notes
896-8979	panupv2-all-content-8896-8979								Download	Release Notes
GlobalProtect Clientless VPN	Last checked: 2024/09/24 14:45:05 EEST	Schedule: None								
8-260	panup-all-gp-98-260								Download	Release Notes
GlobalProtect Data File	Last checked: 2024/09/24 14:45:05 EEST	Schedule: None								
Device Dictionary	Last checked: 2024/09/24 14:44:39 EEST									
42-534	panup-all-deviceld-142-534	IoT	Full	227 KB	4e1ac3621af4...	2024/09/09 19:10:37 EEST				Release Notes
43-536	panup-all-deviceld-143-536	IoT	Full	227 KB	2d81e217f36...	2024/09/11 07:29:23 EEST				Release Notes
44-538	panup-all-deviceld-144-538	IoT	Full	228 KB	8aa3f6308a86...	2024/09/13 04:08:24 EEST				Release Notes

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)

The image shows two side-by-side windows from a certificate management application.

**Generate Certificate window:**

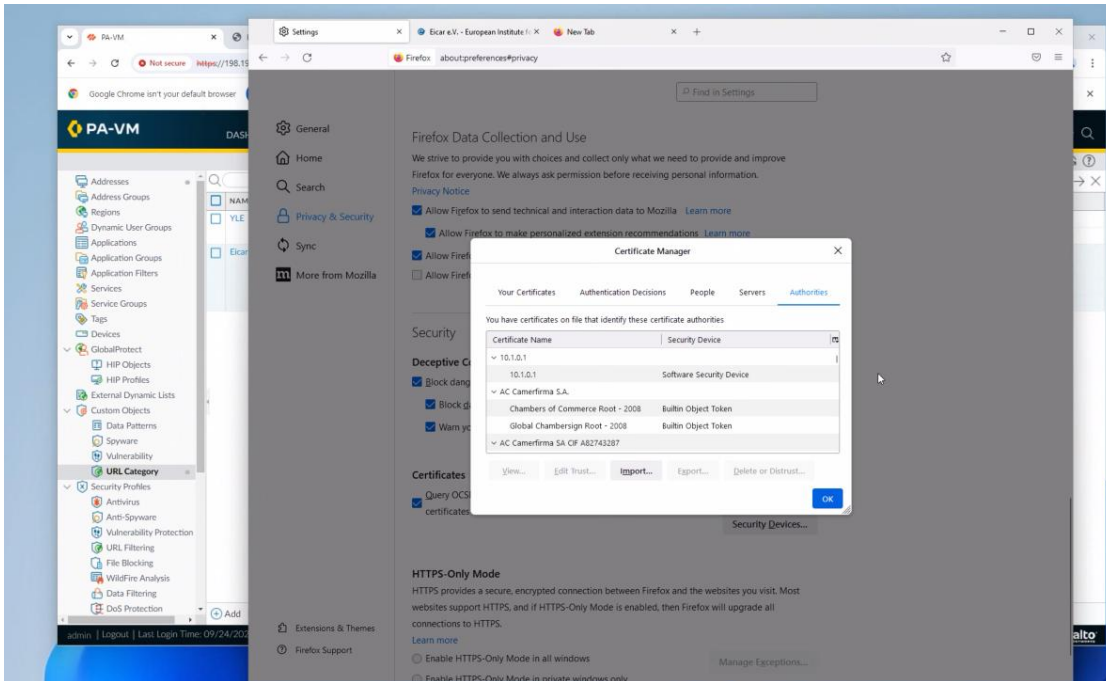
- Certificate Type:** Local (selected), SCEP
- Certificate Name:** PA\_purku\_luotettu
- Common Name:** 10.1.0.1 (with a note: "IP or FQDN to appear on the certificate")
- Signed By:** Certificate Authority (selected)
- Block Private Key Export:** unchecked
- OCSP Responder:** (empty)
- Cryptographic Settings:**
  - Algorithm: RSA
  - Number of Bits: 2048
  - Digest: sha256
  - Expiration (days): 365
- Certificate Attributes:** A table with columns TYPE and VALUE, currently empty.
- Buttons:** Generate, Cancel

**Certificate information window:**

- Name:** PA\_purku\_luotettu
- Subject:** /CN=10.1.0.1
- Issuer:** /CN=10.1.0.1
- Not Valid Before:** Sep 24 11:53:17 2024 GMT
- Not Valid After:** Sep 24 11:53:17 2025 GMT
- Algorithm:** RSA
- Options:**
  - ☒ Certificate Authority
  - ☒ Forward Trust Certificate
  - ☐ Forward Untrust Certificate
  - ☒ Trusted Root CA
- Buttons:** Revoke, OK, Cancel

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)

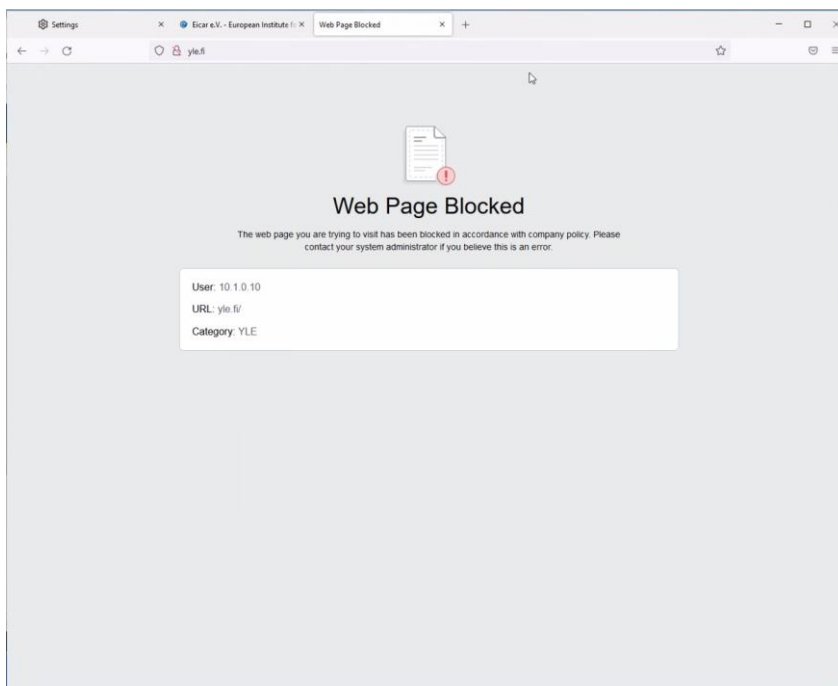
	NAME	TAGS	Source				Destination			URL CATEGORY	SEI
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
1	Pura_salaus_sivuilta	none	WS-NET	any	any	any	VLE	any	any	Eicar gambling games YLE	am

Kuvio 12. Pura\_salaus\_sivuilta purkusäännön asetukset

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

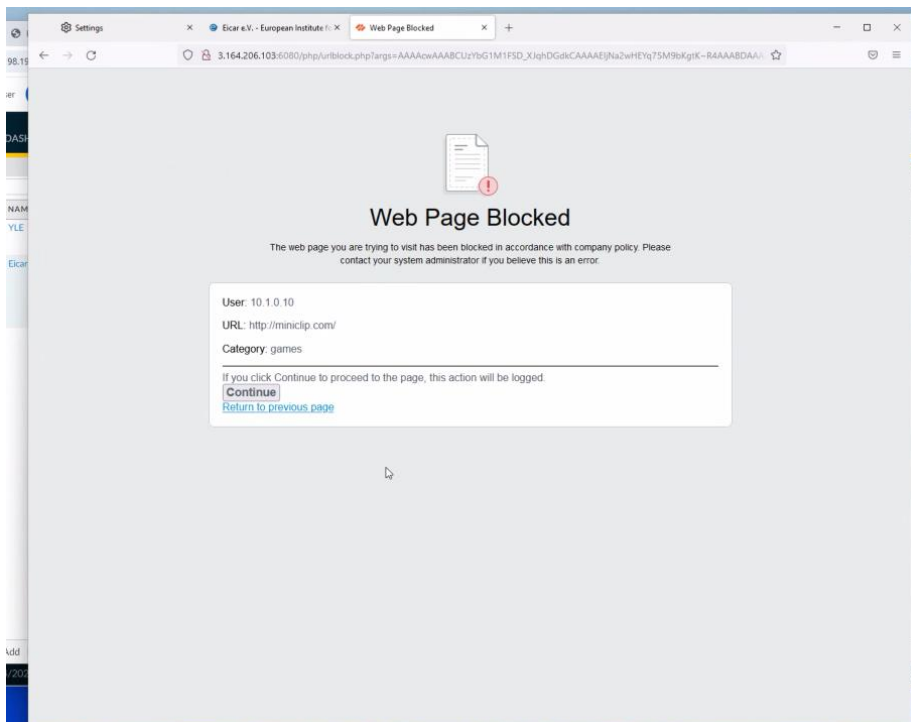
## 3.2 Testaaminen

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 palomuriin. (Kuvio 14)



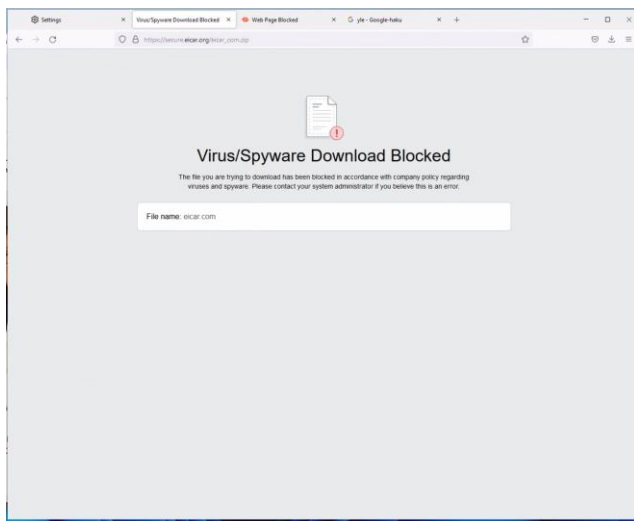
Kuvio 14. Pelisivustot

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

PA-VM																	
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE																	
Logs																	
Traffic																	
Threat																	
URL Filtering																	
WildFire Submissions																	
Data Filtering																	
HIP Match																	
GlobalProtect																	
Tag																	
User-ID																	
Decryption																	
Tunnel Inspection																	
Configuration																	
System																	
Adware																	
Authentication																	
Unleashed																	
Packet Capture																	
App Scope																	
Summary																	
Change Monitor																	
Threat Monitor																	
Threat Map																	
Network Monitor																	
Traffic Map																	
Session Browser																	
Adware																	
PDF Reports																	
Manage PDF Summary																	
User Activity Report																	
SaaS Application Usage																	
Report Groups																	
Email Scheduler																	
Manage Custom Reports																	
Reports																	
RECEIVE TIME	CATEGORY	URL CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED	HTTP/2 CONNECTION SESSION ID		
09/24 15:12:37	gambling	gambling,low-risk	www.lovegas.c...	WS-NET	VLE	10.1.0.10			107.154.248.168			web-browsing	alert		30501		
09/24 15:12:32	YLE	YLE,news,low-risk	yle.fi/login/css/L...	WS-NET	VLE	10.1.0.10			108.156.22.91			web-browsing	block-url		0		
09/24 15:12:32	YLE	YLE,news,low-risk	yle.fi/	WS-NET	VLE	10.1.0.10			108.156.22.40			web-browsing	block-url		0		
09/24 15:12:32	gambling	gambling,low-risk	www.lovegas.c...	WS-NET	VLE	10.1.0.10			107.154.248.168			web-browsing	alert		30501		
09/24 15:12:27	gambling	gambling,low-risk	lovegas.com/	WS-NET	VLE	10.1.0.10			107.154.248.168			web-browsing	alert		30501		
09/24 15:12:27	gambling	gambling,low-risk	www.lovegas.c...	WS-NET	VLE	10.1.0.10			107.154.248.168			web-browsing	alert		30501		
09/24 15:11:57	games	games,low-risk	miniclip.com/	WS-NET	VLE	10.1.0.10			107.154.248.168			web-browsing	alert		0		
09/24 15:09:02	YLE	YLE,news,low-risk	yle.fi/tvicon.co	WS-NET	VLE	10.1.0.10			108.156.22.91			web-browsing	block-url		0		
09/24 15:09:02	YLE	YLE,news,low-risk	yle.fi/login/css/L...	WS-NET	VLE	10.1.0.10			108.156.22.91			web-browsing	block-url		0		
09/24 15:09:02	YLE	YLE,news,low-risk	yle.fi/	WS-NET	VLE	10.1.0.10			108.156.22.91			web-browsing	block-url		0		
09/24 15:09:02	gambling	gambling,low-risk	images.velikkaus...	WS-NET	VLE	10.1.0.10			18.145.122.99			web-browsing	alert		30218		
09/24 15:09:02	gambling	gambling,low-risk	images.velikkaus...	WS-NET	VLE	10.1.0.10			18.145.122.99			web-browsing	alert		30218		
09/24 15:09:02	gambling	gambling,low-risk	images.velikkaus...	WS-NET	VLE	10.1.0.10			18.145.122.99			web-browsing	alert		30218		
09/24 15:08:52	gambling	gambling,low-risk	images.velikkaus...	WS-NET	VLE	10.1.0.10			18.145.122.99			web-browsing	alert		30218		
09/24 15:08:52	gambling	gambling,low-risk	www.velikkaus.fi/	WS-NET	VLE	10.1.0.10			18.145.122.33			web-browsing	alert		30169		
09/24 15:08:52	gambling	gambling,low-risk	velikkaus.fi/	WS-NET	VLE	10.1.0.10			99.83.242.243			web-browsing	alert		0		
09/24 15:05:52	gambling	gambling,low-risk	www.velikkaus.fi/	WS-NET	VLE	10.1.0.10			18.145.122.128			web-browsing	alert		29437		
09/24 15:05:42	gambling	gambling,low-risk	velikkaus.fi/	WS-NET	VLE	10.1.0.10			75.2.27.34			web-browsing	alert		0		

Kuvio 15 Palo Alton loki

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



Kuvio 16. Estetty lataus

Kaikki siis toimii, kuten pitääkin!



### 3.3 Liikennetulasuojaus

Ohjeissa oli vielä lisätehtävänä liikennetulasuojauksen (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.)

**Zone Protection Profile** ⓘ

Name: Lab3\_floodp\_testi

Description:

Flood Protection | **Reconnaissance Protection** | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protection

SCAN	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)
TCP Port Scan	<input checked="" type="checkbox"/>	block	2	10
UDP Port Scan	<input checked="" type="checkbox"/>	block	2	10
Host Sweep	<input type="checkbox"/>	alert	10	100

0 Items → ×

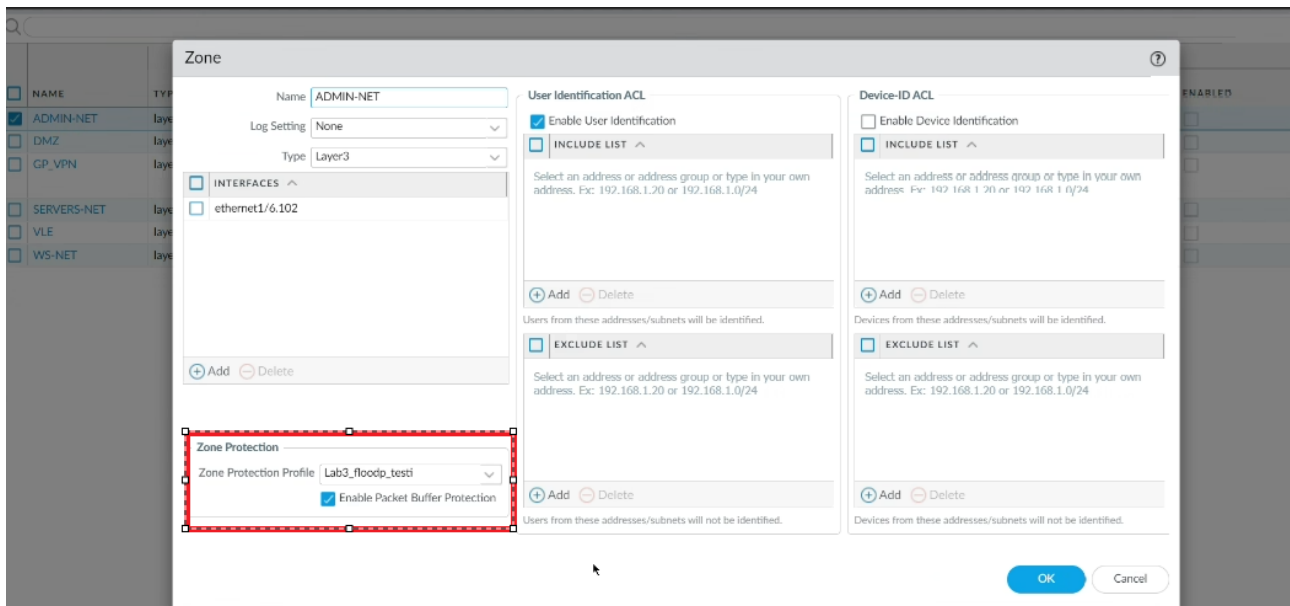
<input type="checkbox"/>	SOURCE ADDRESS EXCLUSION	ADDRESS TYPE	IP ADDRESS(ES)
--------------------------	--------------------------	--------------	----------------

+ Add - Delete

OK Cancel

Kuvio 17. Liikennetulasuojauksen 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. Liikennetulasuojauksen asettaminen

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

RECEIVE TIME	TYPE	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	FILENAME	URL	HTTP/2 CONNECTION SESSION ID
00/24 10:25:52	scan	SCAN.TCP Port Scan	ADMIN-NET	DMZ	10.2.0.13			10.4.0.11			1380	not applicable	drop	redact			0
00/24 10:25:47	scan	SCAN.TCP Port Scan	ADMIN-NET	DMZ	10.2.0.13			10.4.0.11			2909	not applicable	drop	redact			0
00/24 10:25:42	scan	SCAN.TCP Port Scan	ADMIN-NET	DMZ	10.2.0.13			10.4.0.11			1720	not applicable	drop	redact			0
00/24 10:25:32	scan	SCAN.TCP Port Scan	ADMIN-NET	DMZ	10.2.0.13			10.4.0.11			113	not applicable	drop	redact			0

Kuvio 19. Palo Alto uhkaloki

## 4 Pohdinta

Tietoturvakontrollien neljännessä laboratoriotyössä pääsimme taas mukavasti tutustumaan Palo Altton 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.

Liikennetulasuojaus 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>