Lauri Partinen(ktkt23sp)

Ngfw ja tls inspection

Tietoturvalaitteet

2025

Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1 CONTENT FILTERING

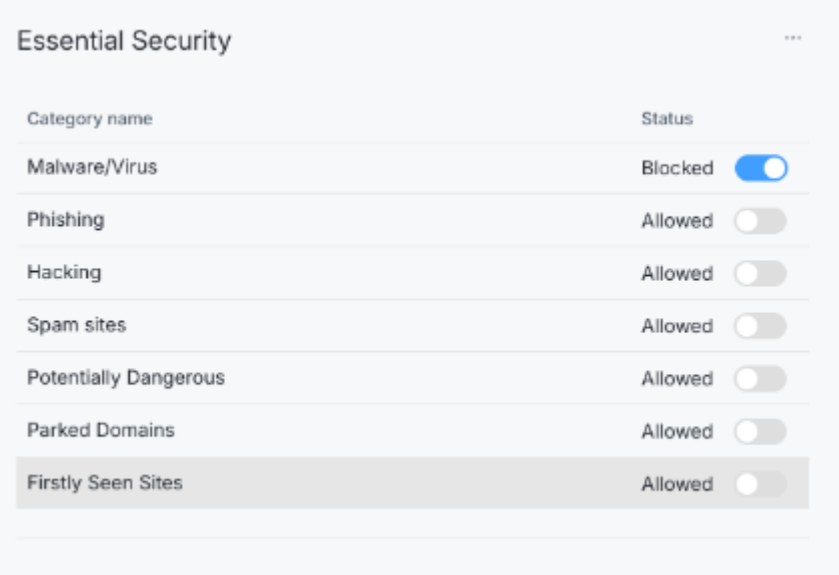
Politiikka 1: Security - Haitake-/Virusliikenteen Esto (Block Traffic Related into Malware/Virus)

Mikä on tilanne ja mitä ollaan tekemässä?

Verkko oli altis haittaohjelmien ja virusten aiheuttamille uhille. Tarkoitus on lisätä turvallisuuttaa ottamalla käyttöön zenarmorista Malware/Virus.

Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?

Toteutus: Blokataan zenarmorista Malware/Virus kohta.



Testaus:

Perustele ratkaisu ja tarvittaessa havainnollista.

Haittaohjelmien esto verkon reunalla on perustavanlaatuinen suojausmekanismi. Se estää monia uhkia saavuttamasta juustomarketin työasemia tai palvelimia.

Analyysi:

Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?

Turvallisuus parani merkittävästi. Aktiivinen haittaohjelmien torjunta verkkotasolla vähentää riskiä mahdolliselle virustartunnalle tai haittaohjelmalle.

Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?

Vähäinen vaikutus juustomarketin toimintaan.

Arviointi:

Onko tehdyt ratkaisut tarpeellisia? Miksi?

Kyllä Haittaohjelmat ovat jatkuva ja vakava uhka juustomarketin toiminnan jatkumisen kannalta.

Voiko niitä kiertää? Miten?

Kyllä. Nollapäivähaavoittuvuudet, haittaohjelmat esimerkiksi usb-tikusta tai sähköpostiviestin linkistä

Onko olemassa muita parempia vaihtoehtoja? Mitä?

Päätepisteiden suojaus tai DNS-suodatus.

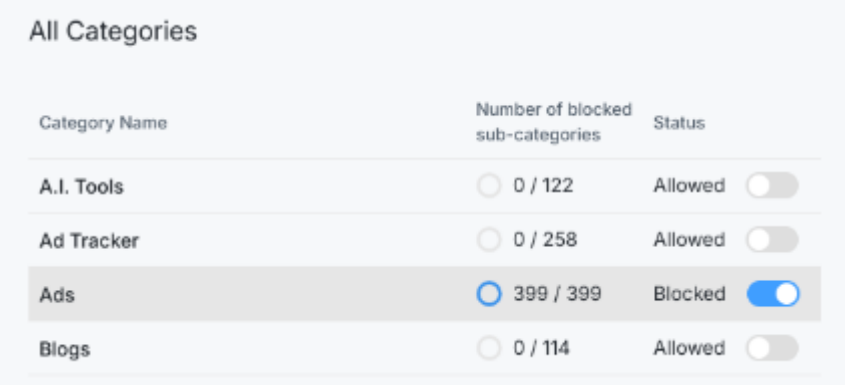
Politiikka 2: App Controls - Mainosten Esto (Block Advertises from various Web-sites)

Mikä on tilanne ja mitä ollaan tekemässä?

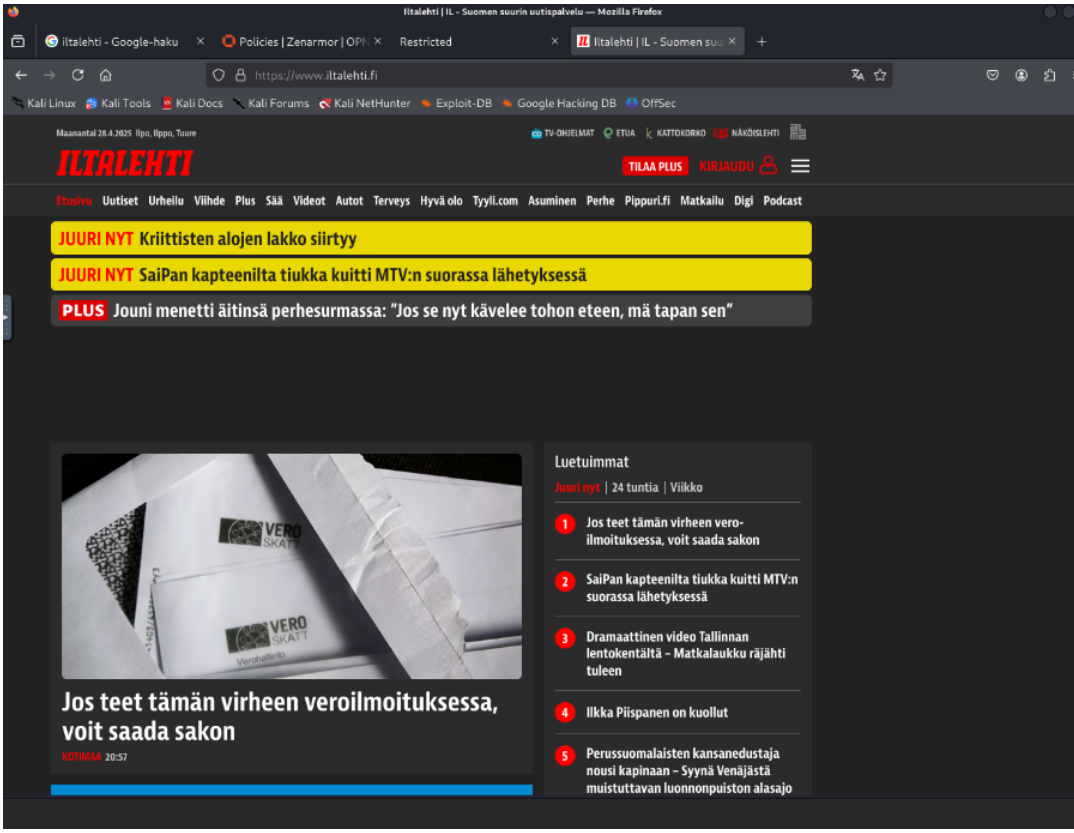
Verkkosivujen mainokset kuluttavat kaistanleveyttä, voivat häiritä työntekijöitä. Otettiin käyttöön mainosten estävä sääntö zenarmorista, joka estää mainosten näkymisen selaisemessa.

Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?

Zenarmoriin toteutus



Toimivuus testattiin selaamalla verkkosivuja, ja mainosten todettiin estyvän onnistuneesti esim. Iltalehti.



Perustele ratkaisu ja tarvittaessa havainnollista.

Mainosten esto parantaa käyttökokemusta juustomarketissa nopeuttamalla sivujen latautumista ja poistamalla mainokset sivuilta.

Analyysi:

Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?

Turvallisuus parani jonkin verran, koska yksi mahdollinen haittaohjelmien levityskanava mainostenkautta tulevat haittaohjelmien riski pieneni.

Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?

Mainoksien poistaminen sivustolta mukavoittaa juustomarketin netin selaamista.

Arviointi:

Onko tehdyt ratkaisut tarpeellisia? Miksi?

Hyödyllinen, mutta ei välttämättömyys

Onko olemassa muita parempia vaihtoehtoja? Mitä?

Selainlaajennukset esim. AdBlock Plus. Ne voivat olla tehokkaampia tietyissä tapauksissa selaimessa.

Politiikka 3: App Controls - Sosiaalisen Median Estäminen (Block access to Social Media)

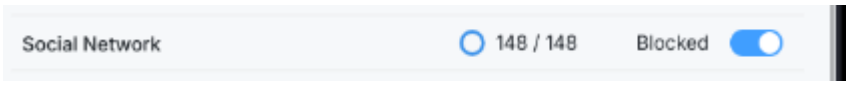
Mikä on tilanne ja mitä ollaan tekemässä?

Tilanne: Juustomarketin työntekijät käyttivät merkittävästi työaikaa sosiaalisen median palveluissa, mikä heikensi tuottavuutta.

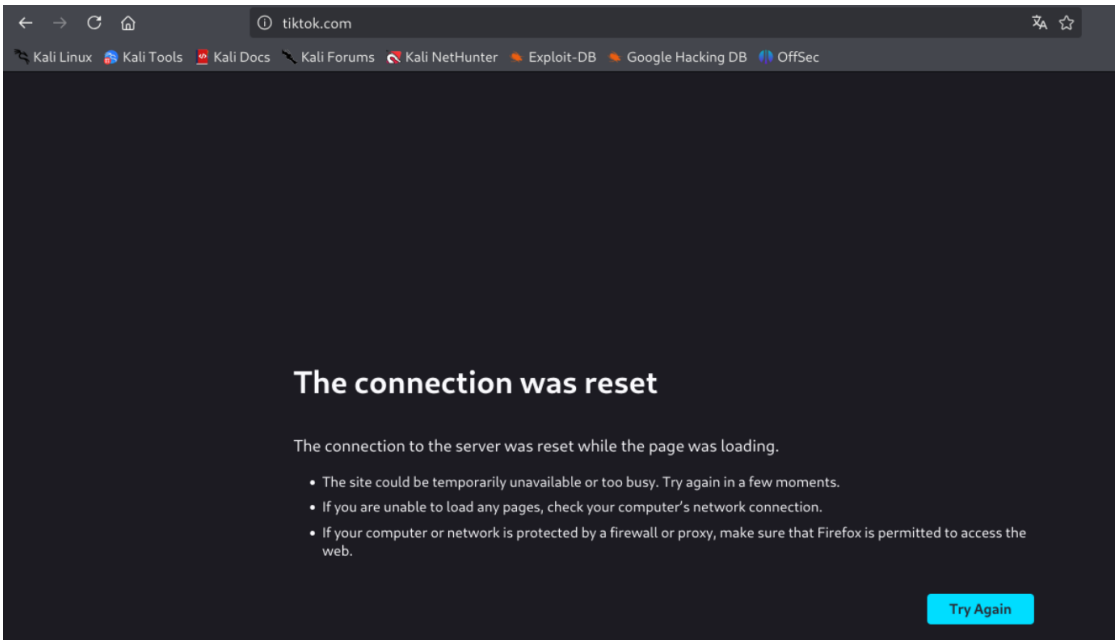
Tekeminen: Otettiin käyttöön sovelluskontrollipolitiikka estämään pääsy yleisimpiin sosiaalisen median palveluihin työaikana.

Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?

Toteutus: Zenarmoriin pistettiin sosiaalisen median esto päälle



Testaus: Toimivuus varmistettiin yrittämällä käyttää Tiktok.



Perustele ratkaisu ja tarvittaessa havainnollista.

Ratkaisu perustuu havaintoon tuottavuuden laskusta sosiaalisen median käytön vuoksi. Estämällä pääsy näihin palveluihin pyritään varmistamaan, että työaika käytetään tehokkaammin työtehtäviä varten.

Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?

Suora vaikutus on pääsyn estyminen määriteltyihin palveluihin kaikilta käyttäjiltä, joiden liikenne kulkee politiikan valvoman laitteen kautta.

Arviointi:

Onko tehdyt ratkaisut tarpeellisia? Miksi?

Tarpeellinen, jos tuottavuusongelmia työntekijöiden keskuudessa esiintyy.

Voiko niitä kiertää? Miten?

Käyttämällä henkilökohtaisia mobiililaitteita ja niiden nettiä tai käyttämällä VPN-palveluita.

Onko olemassa muita parempia vaihtoehtoja? Mitä?

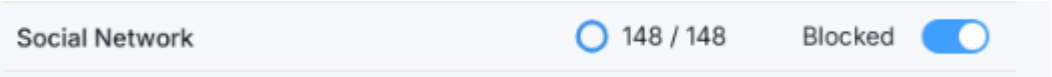
Vaihtoehtoja ovat:

Käyttöehdot (AUP): Selkeät säännöt ja ohjeistus some-käytöstä työajalla ja seuraukset rikkomuksista.

DNS-suodatus: Estää pääsyn verkkotunnustasolla.

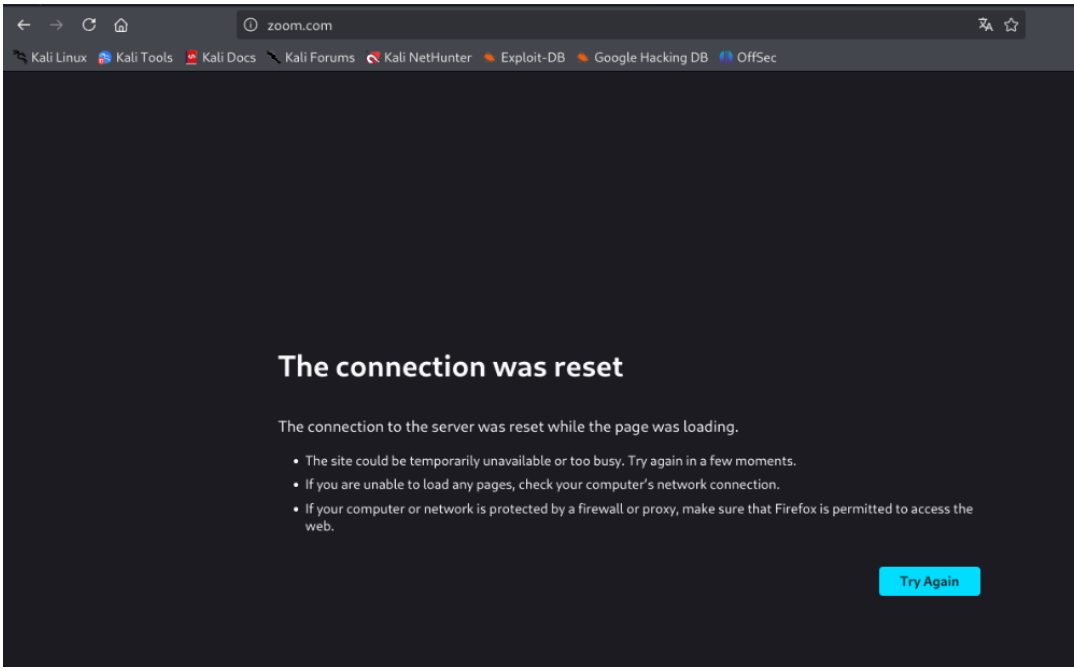
Politiikka 4: App Controls - Tarpeettomien Neuvottelupalveluiden Estäminen (Block access unnecessary conference services)

- **Mikä on tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Juustomarket käyttää virallisena neuvottelu- ja yhteistyöalustanaan Microsoft Teamsia. Muiden, mahdollisesti ei-hyväksyttyjen tai vähemmän turvallisten, neuvottelupalveluiden (kuten Zoom) käyttö voi aiheuttaa tietoturvariskejä, yhteensopivuusongelmia ja hallinnan vaikeutta.
  - **Tekeminen:** Tavoitteena oli Microsoft Teamsin käyttö sallitaan ja kaikki muut vastaavat palvelut esim. Zoom estetään.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  - **Toteutusyritys:** Zenarmorista laitettiin Zoom blockki päälle



  - **Testaus:**

Zoom.com blokkaus onnistui, mutta Teams:in salliminen ei onnistunut.

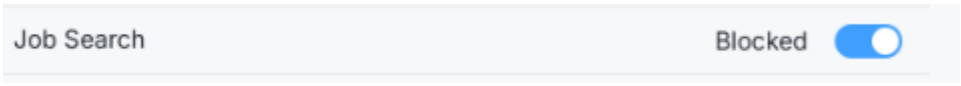


- **Perustele ratkaisu (tavoiteltu ratkaisu) ja tarvittaessa havainnollista.**
    - **Perustelu (tavoitteelle):** Standardoimalla käytettävät työkalut (Teams) voidaan parantaa yhteistyön sujuvuutta, yksinkertaistaa käyttäjätukea ja hallita tietoturvariskejä paremmin.
- **Analyysi:**
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - **Merkittävä negatiivinen vaikutus.** Estää Juustomarketin virallisen ja välttämättömän kommunikaatio- ja yhteistyöalustan käytön, mikä haittaa vakavasti työntekoa ja sisäistä/ulkopuolista viestintää.
- **Arviointi tavoitellusta politiikasta:**
    - **Onko tavoiteltu ratkaisu tarpeellinen? Miksi?**
        - Kyllä, jos tavoitteena on standardointi ja hallinnan keskittäminen. Virallisen työkalun määritteleminen ja muiden estäminen on yleinen ja perusteltu käytäntö juustomarketin toiminnan kannalta.

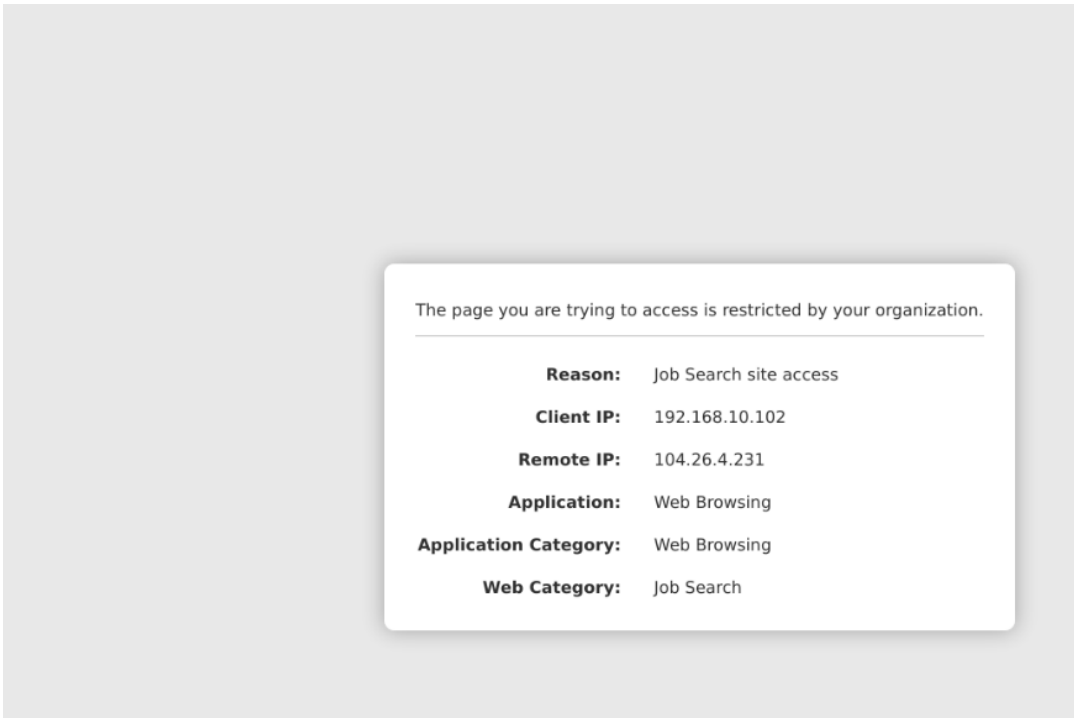
Politiikka 5: Web Controls - Työnhaku (Job Search)

- **Mikä on tilanne ja mitä ollaan tekemässä?**
- **Tilanne:** Juustomarketin työntekijöiden on havaittu etsivän uusia työpaikkoja työaikana, jonka toimitusjohtaja haluaa estää.

- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
    - **Toteutus:** Zenarmorista job search block päälle.



    - **Testaus:** jobly.fi block toimii.

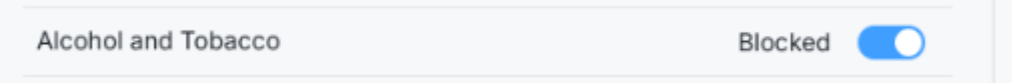


- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Ratkaisu perustuu suoraan johdon pyyntöön puuttua havaittuun tuottavuutta heikentävään toimintaan.
- **Analyysi:**
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - Ei vaikuta merkittävästi liiketoimintaan, ellei työntekijä rekrytoinnissa tai esimiehillä ole tarvetta käyttää näitä sivustoja työssään.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Tarpeellisuus on liikkeenjohdon päätös, joka perustuu havaittuun tuottavuusongelmaan.
    - **Voiko niitä kiertää? Miten?**
        - Kyllä. Käyttämällä mobiililaitteiden omaa datayhteyttä tai VPN.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**

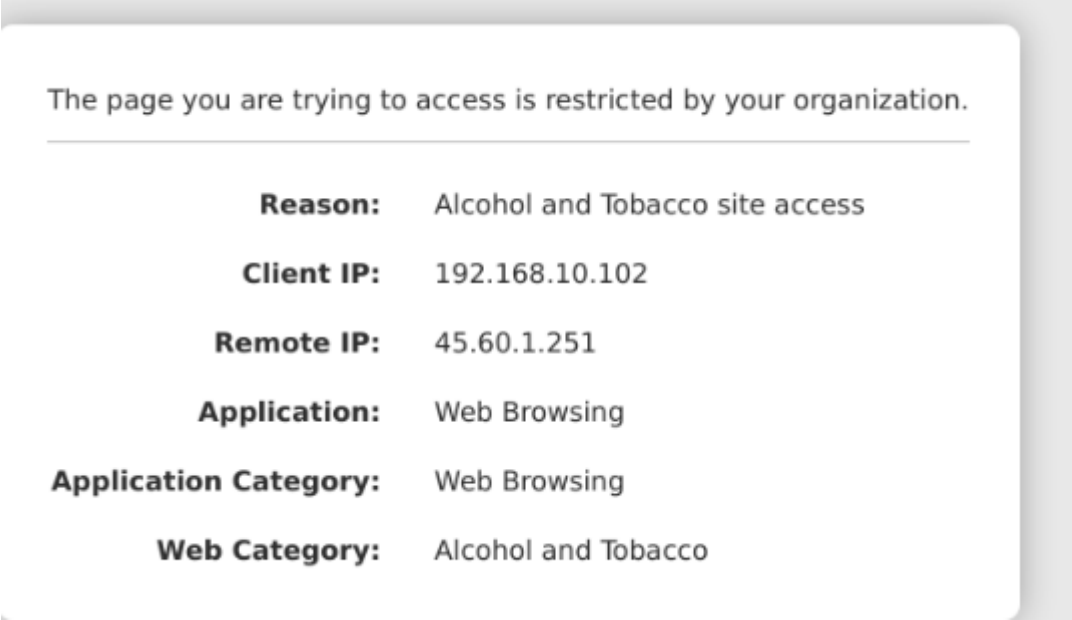
- Käyttöehtopolitiikka AUP, jossa määritellään selkeästi mitä saa käyttää.

Politiikka 6: Web Controls - Alkoholi ja Tupakka (Alcohol and Tobacco)

- **Mikä on tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** On havaittu, että työntekijät selaavat alkoholiin liittyviä verkkosivustoja työaikana.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  - **Toteutus:** Zenarmorista laitettiin block päälle



  - **Testaus:** Block toimii.



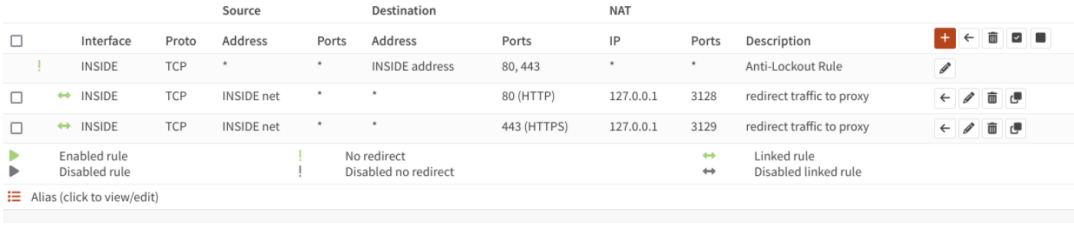
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Ratkaisu toteuttaa johdon pyynnön rajoittaa tupakkaan ja alkoholiin liittyvää selailua työpaikalla.
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Tarpeellisuus perustuu toimitusjohtajan linjaukseen estää sivustot. Teknisestä näkökulmasta ei välttämättömiä.
  - **Voiko niitä kiertää? Miten?**
  - Mobiilidatan käyttö tai Vpn.
  - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
    - Käyttöehtopolitiikka AUP

2 TLS INSPECTION

1. **TLS Inspection:** Otettiin käyttöön järjestelmän asetus, joka purkaa ja tarkastaa salatun TLS/SSL-liikenteen. Edellytys monien muiden sääntöjen tehokkaalle toiminnalle.

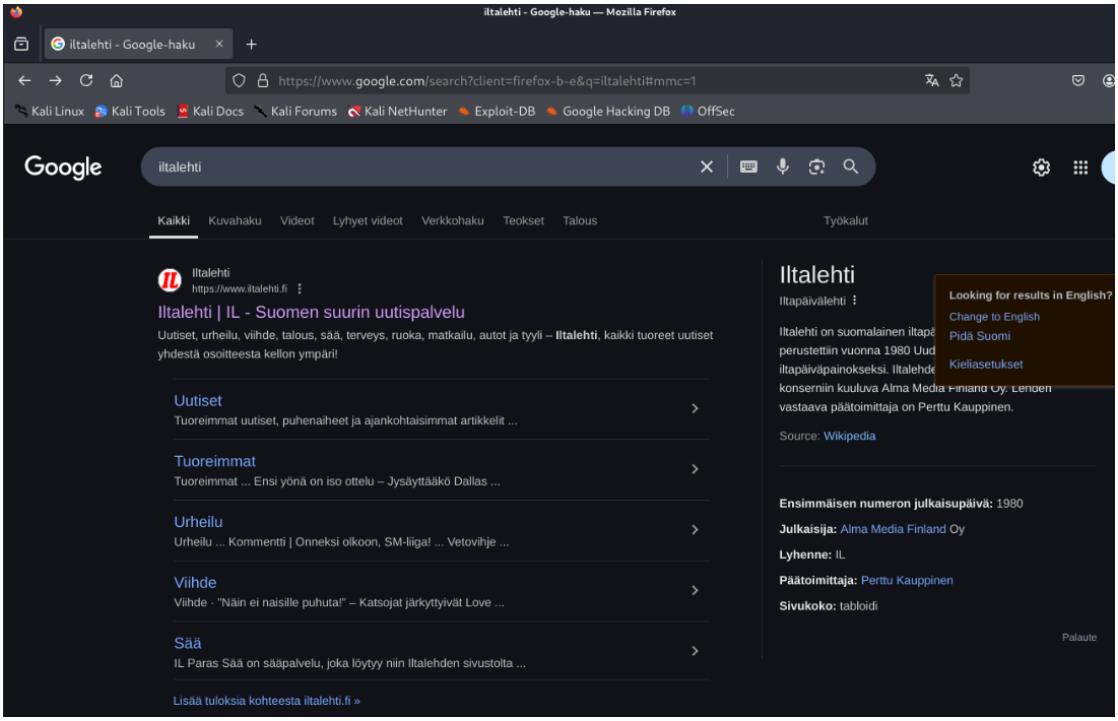
Totetusvaiheet:

- Generoitiin Ca-varmenne, jota käytetään liikenteen salaamiseen.
- Määritellään politiikat



- Aktivoidaan TLS inspection.

Varmennus: Testataan verkkosivun lataus ilman selainvaroituksia.



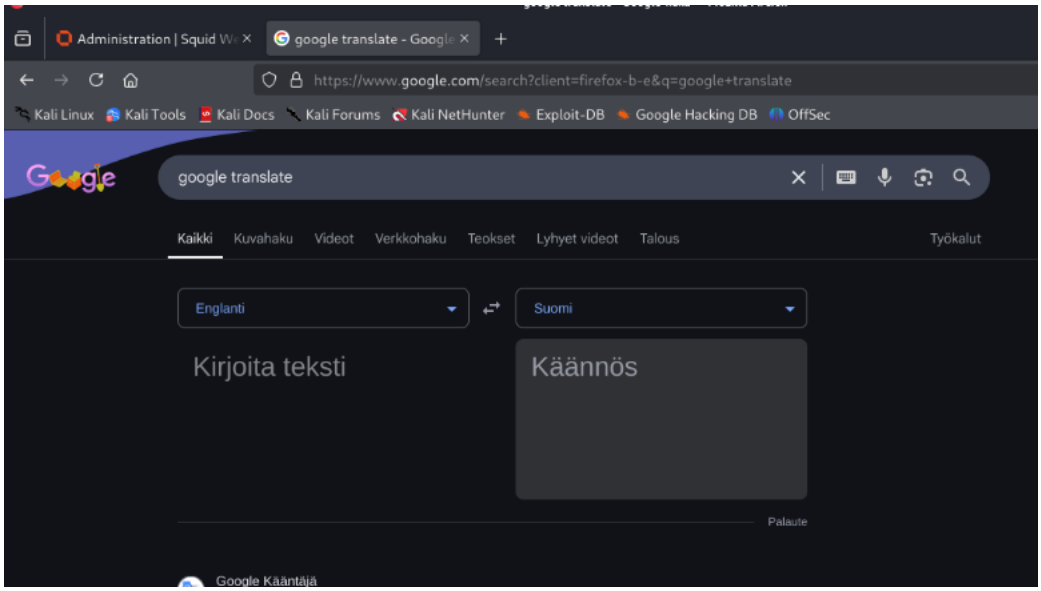
- **Policy 1: Google Translate tulee olla saavutettavissa.**

- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Juustomarketin työntekijät tarvitsevat Google kääntäjää työtehtäviinsä. Ongelmana on, että työntekijät ovat myös

keksineet käyttää Google kääntäjää eräänlaisena web-välityspalvelimena ohittaakseen muita verkkosisällön suodattimia (Policy 2).

- **Tekemässä:** Varmistetaan, että pääsy Google kääntäjään on sallittu palomuurin säännöissä, vaikka sen väärinkäyttöä Proxynä pyritään estämään.

- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?** Google translateen pääse käsiksi sallimalla http ja https liikenne. Testataan google translate tominta.

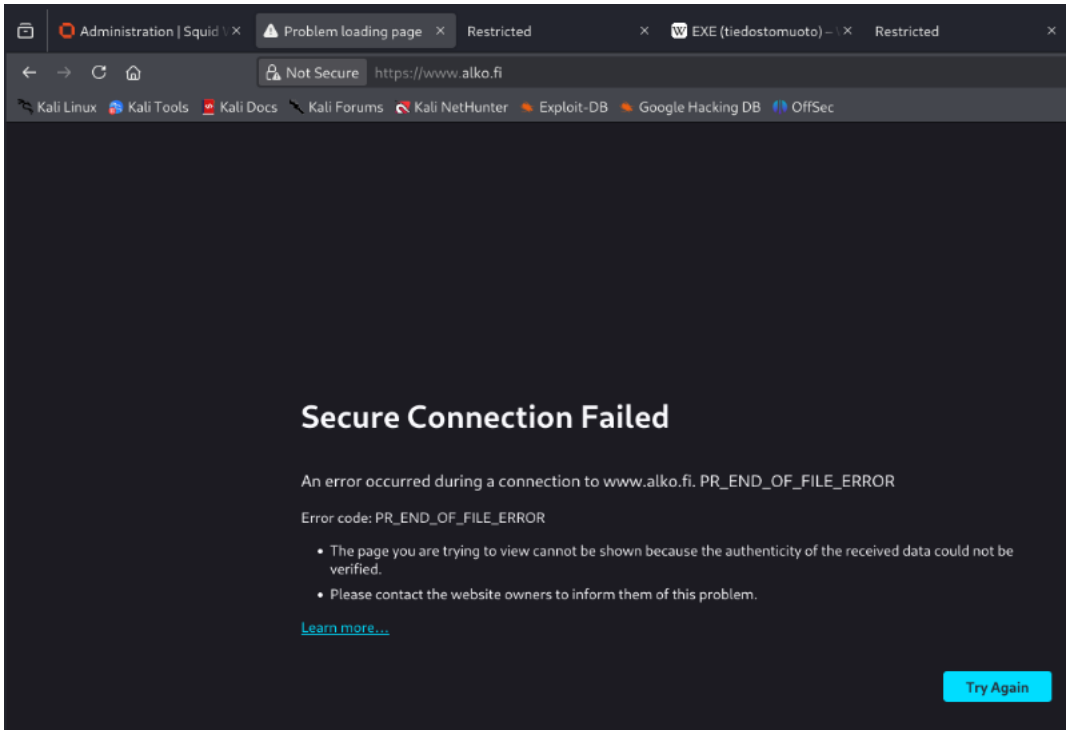


- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Google Translate on tarpeellinen työkalu työntekijöille, täydellinen estäminen haittaisi työntekijöiden tuottavuutta.
- **Analyysi:**
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
    - Mahdollistaa Google Translaten käytön, mikä vaikuttaa positiivisesti niihin työtehtäviin, joissa sitä tarvitaan.
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Kyllä. Google Translate on tarpeellinen työkalu työntekijöille.

Policy 2: Estä käyttäjiä pääsemästä alko.fi-sivustolle käyttämällä Google Translatea tai muuta WebProxya.

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Yrityksen käytännöt kieltävät pääsyn tietyille verkkosivustoille. Käyttäjät ovat kuitenkin keksineet kiertää tämän eston käyttämällä Google Translatea, jotka hakevat kohdesivun sisällön.
    - **Tekemässä:** Konfiguroidaan squid web proxy tunnistamaan ja estämään tällaiset kiertoyritykset. Tavoitteena on, että alko.fi-sivustolle ei pääse, vaikka sinne yrittäisi mennä Google Translaten kaltaisen palvelun kautta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
- Blacklistataan alko.fi, jotta alkon sivutolle ei pääse.

Yritetään mennä google translaten kautta alko.fi sivulle



- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Estämällä pääsyn kiellettyihin kohteisiin myös välityspalveluiden kautta varmistetaan työntekijöiden

Analyysi:

- **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**

        - Turvallisuus parani. Alkon Black listaus sulkee yleisesti hyödynnettävän tavan kiertää sisältösuodatusta. Vähentää riskiä, että käyttäjät pääsevät käsiksi haitalliseen tai yrityksen käytäntöjen vastaiseen sisältöön.

- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Tarpeellisia, jos yritys haluaa aidosti valvoa verkon käyttöä ja estää pääsyn tiettyihin sisältöihin.
    - **Voiko niitä kiertää? Miten?**
        - **Muut proxy-tyypit:** Käyttäjät voivat etsiä muita, tuntemattomampia tai salaavia proxy-palveluita tai VPN-yhteyksiä, joita suodatin ei vielä tunnista.
        - **Henkilökohtaiset laitteet ja verkot:** Käyttäjä voi käyttää omaa puhelintaan tai kotiverkkoaan päästäkseen sivuille.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **Asiakasohjelmistot:** Jotkin työasemiin asennettavat tietoturvaohjelmistot voivat valvoa ja rajoittaa verkkoliikennettä tarkemmin suoraan koneella.
        - **DNS-suodatus:** Voi auttaa estämään pääsyn tunnettuihin proxy-sivustoihin, mutta ei estä itse proxy-toiminnallisuutta.

- **Policy 3: Estä Juustomarketin työntekijöitä lataamasta .exe-tiedostoja internetistä.**
- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Suoritettavat .exe tiedostot ovat yksi yleisimmistä tavoista levittää haittaohjelmia. Tavoitteena on estää .exe tiedostojen lataaminen internetistä.
    - **Tekemässä:** Konfiguroidaan OPNsensen Web Proxy estämään kaikkien .exe-tiedostojen lataaminen internetistä selaimen kautta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?** Blacklistattiin .exe, jotta lataaminen ei onnistu.

- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Estämällä .exe-tiedostojen lataukset vähennetään merkittävästi riskiä mahdollisten haittaohjelmien varalta.
- **Analyysi:**
    - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
        - Turvallisuus parani. Sulkee yhden yleisimmistä ja vaarallisimmista tavoista saada haittaohjelmatartunta.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Tarpeellinen turvatoimi lähes kaikissa yritysverkoissa. Työntekijät voivat vahingossa aiheuttaa tuhoa yrityksen toimintaan lataamalla haittaohjelman sisältävän .exe tiedoston.
    - **Voiko niitä kiertää? Miten?**
        - **Pakkaaminen/Arkistointi:** .exe-tiedosto voidaan piilottaa esim. .zip tai .rar muotoon.
        - **Uudelleennimeäminen:** Tiedoston pääte voidaan vaihtaa esim. .exe tiedostosta .txt muotoon.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **Gateway Antivirus:** Skannaa ladatut tiedostot tunnettujen haittaohjelmien varalta.
        - **Sandboxaus:** Epäilyttävät tiedostot voidaan automaattisesti suorittaa eristetyssä ympäristössä ennen niiden toimittamista käyttäjälle.
        - **Application Whitelisting:** Sallitaan työasemilla vain ennalta hyväksyttyjen sovellusten suorittaminen.

- **Reflektointi: Sisällönsuodatus ja TLS-Tarkastus**
- Tämä harjoitus keskittyi verkkoliikenteen sisällön suodattamiseen ja salatun liikenteen tarkastamiseen OPNsense-palomuurin työkaluilla Zenarmorilla ja Squidilla.

Mitä saavutin?

- **Zenarmor-pohjainen suodatus:** Onnistuin toteuttamaan ja testaamaan useita Zenarmor-pohjaisia suodatuspolitiikkoja:
- **TLS-tarkastuksen käyttöönotto:** Sain onnistuneesti käyttöön TLS-tarkastuksen luomalla tarvittavan CA-varmenteen, asentamalla sen testikoneelle ja aktivoimalla tarkastuksen politiikassa.
- **Web Proxy (Squid) -pohjainen suodatus:** Onnistuin Web Proxyn avulla:
    - Estämään pääsyn tietylle sivustolle esim. alko.fi
    - Estämään .exe tiedostojen lataamisen.

Mitä jäi saavuttamatta?

- **Policy 4 (Neuvottelupalvelut):** En onnistunut toteuttamaan vaatimusta, jossa Zoom estetään, mutta Microsoft Teams sallitaan.

Miten opin asian?

- Käyttöliittymän ohjeiden ja kokeilemalla ja testaamalla. jos olin jumissa kysyin apua.

Miten lähestyisin asiaa seuraavalla kerralla?

- **Dokumentointi:** Otan kuvat ja dokumentoinnin samalla kun teen.

Miten pystyn käyttämään tätä taitoa/osaamista tulevaisuudessa?

- **Yritysverkkojen suojaaminen:** Voin hyödyntää osaamistani yritysverkkojen suojaamisessa konfiguroimalla palomuurisääntöjä.
- **Tietoturva-arkkitehtuurin suunnittelu:** Ymmärrys sisällönsuodatuksesta ja TLS-tarkastuksesta auttaa suunnittelemaan tietoturvallisempia verkkoratkaisuja.