Lauri Partinen ktkt23sp

# Statefull firewall & VPN

2025

Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

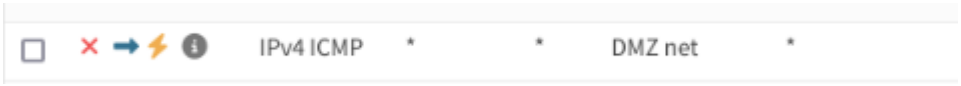
# 1 STATEFULL

**Policy 1: Allow ICMP Traffic from Inside to Outside and Block from Outside to DMZ direction**

- **Mikä on tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Juustomarket inside olevien käyttäjien ja järjestelmien täytyy pystyä tekemään verkon vianmääritystä ulospäin käyttäen ICMP-protokollaa. Samalla halutaan estää outside tulevat ICMP-pyynnöt DMZ-alueelle.
  - **Tekeminen:** Määritetään Juustomarketkaksi palomuurisääntöä: yksi, joka sallii ICMP-liikenteen INSIDE -> OUTSIDE, ja toinen, joka estää ICMP-liikenteen OUTSIDE -> DMZ.
  - Testataan icmp toiminta pingaamalla.

```
lab@VLABKALI2023:~$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=63 time=1.99 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=63 time=4.10 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=63 time=1.78 ms
^C
── 10.0.0.5 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.777/2.621/4.096/1.046 ms
```

  - Estetty liikenne: Blokataan liikenne outside->Dmz suntaan.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** ICMP ulospäin on hyödyllinen työkalu yhteyksien toimivuuden testaamiseen esim. ping. Sen estäminen vaikeuttaisi vianetsintää. ICMP estäminen sisäänpäin julkisiin palvelimiin vähentää hyökkäyspinta-alaa järjestelmästä. Hyökkääjät käyttävät usein ICMP echo requestia selvittääkseen aktiivisia kohteita verkossa.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**

        - Turvallisuuden parantuminen juustomarketissa. Aiemmin ICMP saattoi olla sallittu molempiin suuntiin tai kokonaan estetty. Nyt liikennettä pystytään kontrolloimaan.
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - Mahdollistaa sisäverkon käyttäjien perusvianetsinnän ulkoverkon suuntaan.
        - *Neutraalisti/Huomioitavaa:* Ei suoraan vaikuta muihin palveluihin (HTTP, SMTP jne.), mutta jos jokin sovellus tai protokolla *luottaisi* ICMP-vastauksiin DMZ-palvelimilta ulospäin, se voisi lakata toimimasta (epätodennäköistä yleisissä tapauksissa). Estää ulkopuolisia (myös legitimitejä ylläpitäjiä ilman VPN:ää tms.) pingaamasta DMZ-palvelimia.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?** Kyllä. Ulospäin suuntautuvan ICMP salliminen on käytännöllistä vianetsinnän kannalta, ja sisäänpäin suuntautuvan ICMP estäminen DMZ on perustason tietoturvatoimenpide.
    - **Voiko niitä kiertää? Miten?** Hyökkääjä voi käyttää muita protokollia tiedusteluun esimerkiksi UDP portti skannaaminen.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?** Sallia vain tietyt ICMP-tyypit ulospäin ja estää kaikki muut. Voidaan rajoittaa, ketkä sisäverkossa saavat lähettää ICMP ulospäin.

**Policy 2 :Allow External Access to WebStore at http://10.10.10.5 from OUTSIDE**

- **Mikä on tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Juustomarketilla on WebStore-palvelin 10.10.10.5 inside verkossa, jonka tulee olla saavutettavissa asiakkaita varten. Pääsyn tulee toimia sekä http ja https protokollilla.
    - **Tekeminen:** Määritetään palomuuriin säännöt. Liikenne porteissa 80 ja 443 ohjataan sisäiselle WebStore-palvelimelle 10.10.10.5.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

- Tehtiin palomuurisäännöt http ja https->10.10.10.5


- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Säännön avulla juustomarket toimii internetissä turvallisesti. Porttien rajaaminen vain http ja https on tärkeää, jotta tarpeettomista porteista sisäänpääsy pystytään estämään.
  - **Havainnollistus:**
  - Nmapin avulla pystytään todentamaan porttien 80 ja 433 toiminnallisuus.
  - 

```
lab@VLABKALI2023:~$ nmap 10.10.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 22:53 EEST
Nmap scan report for 10.10.10.5
Host is up (0.0027s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   filtered http
443/tcp  filtered https
```

- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Turvallisuus parani verrattuna alkuperäiseen tilanteeseen, jossa *kaikki* portit olisivat auki tai jos palomuuri olisi kokonaan pois päältä. Sääntö mahdollistaa kontrolloidun pääsyn vain tarvittaviin palveluihin.
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
    - Mahdollistaa webstoren liiketoiminnallisen toiminnan internettiin.
    - Negatiivisia puolia: Lisää verkon kuormitusta ja palomuurin prosessointitaakkaa.
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?** Kyllä, tarpeellisia webstoren toiminnan kannalta.
  - **Voiko niitä kiertää? Miten?**
  - hyökätä itse WebStore-sovelluksen haavoittuvuuksia vastaan esimerkiksi SQL-injektio porteissa 80 tai 443. Palvelunestohyökkäykset kohdistuvat myös sallittuihin portteihin.

- Onko olemassa muita parempia vaihtoehtoja? Mitä?
  - **Web Application Firewall:** Sijoitetaan palomuurin eteen tarkastamaan http ja https-liikennettä sovellustason hyökkäysten varalta.
  - **Intrusion Prevention System:** Voi tunnistaa ja estää yleisimpiä hyökkäystaktiikoita liikenteestä.

**Policy 3: Allow Web Browsing from Juustomarket HQ Inside**

- Mikä on tilanne ja mitä ollaan tekemässä?
  - **Tilanne:** Juustomarket inside verkon täytyy pystyä selaamaan internetiä.
  - **Tekeminen:** Määritetään palomuuriin sääntö, joka sallii lähtevän liikenteen inside verkosta ulkoverkkoon käyttäen http tcp portti 80 ja https tcp portti 443 protokollia.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  - Opnsenseen luotiin palomuurisääntö: INSIDE 10.10.10.0/24, kohdeverkko any, protokolla tcp ja kohdeportit 80 ja 443
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Verkkoselaus on perustarve yrityksen toiminnan kannalta. Säännön rajaaminen vain http ja https-portteihin rajaa riskiä verrattuna aiempaan tilanteeseen.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Verkkoselauksen salliminen avaa mahdollisuuden haittaohjelmille, tietojenkalastelulle ja muille verkkouhkille.
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
    - Mahdollistaa käyttäjien normaalin työskentelyn ja tiedonhaun internetistä.
    - Lisää verkon kuormitusta. Altistaa sisäverkon koneet web-pohjaisille uhille.
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?** Kyllä, perusvaatimus yrityksen toiminnan kannalta.

- **Voiko niitä kiertää? Miten?** Sääntöä itsessään ei kierretä, mutta sitä voidaan väärinkäyttää:
  - Haittaohjelmat voivat kommunikoida komentopalvelimien kanssa käyttäen http ja https-portteja.
- **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
  - **DNS-suodatus:** Estetään pääsy tunnetuille haitallisille tai ei-toivotuille verkkotunnuksille jo dns-kyselyvaiheessa.
  - **SSL/TLS Inspection :** Edistyneemmissä palomuureissa tai välityspalvelimissa voidaan purkaa https-liikenne tarkastusta varten.

**Policy 4: Salli Web-selailu Juustomarket OY Varastolta (INSIDE -> OUTSIDE)**

- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Juustomarket OY:n varastoverkon käyttäjillä ei ole pääsyä ulkoisille verkkosivustoille internetissä
  - **Tekemässä:** Luodaan palomuurisääntö opnsenseen, joka sallii https ja https -liikenteen varaston sisäverkosta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  - Luotiin uusi "Pass" (Salli) -sääntö seuraavilla määrityksillä:
  - Workerpc luotiin sallittavat säännöt.


    - **Description :** "Salli web-selailu varastolta"
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Tämä sääntö sallii eksplisiittisesti vain TCP-liikenteen varaston verkosta mihin tahansa IP-osoitteeseen kohdeportteihin 80 ja 443. Web-selailu käyttää pääasiassa näitä portteja, sääntö mahdollistaa halutun toiminnallisuuden.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Turvallisuus heikkeni verrattuna tilanteeseen, jossa kaikki liikenne ulos oli estetty. Sallimalla lähtevä liikenne avataan mahdollinen reitti haittaohjelmille ladata sisältöä.
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**

        - Pääasiassa ei vaikuta negatiivisesti muuhun toimintaan. Mahdollistaa varaston käyttäjien web-selailun, mikä on juustomarketin liiketoiminnan kannalta tarpeellista.

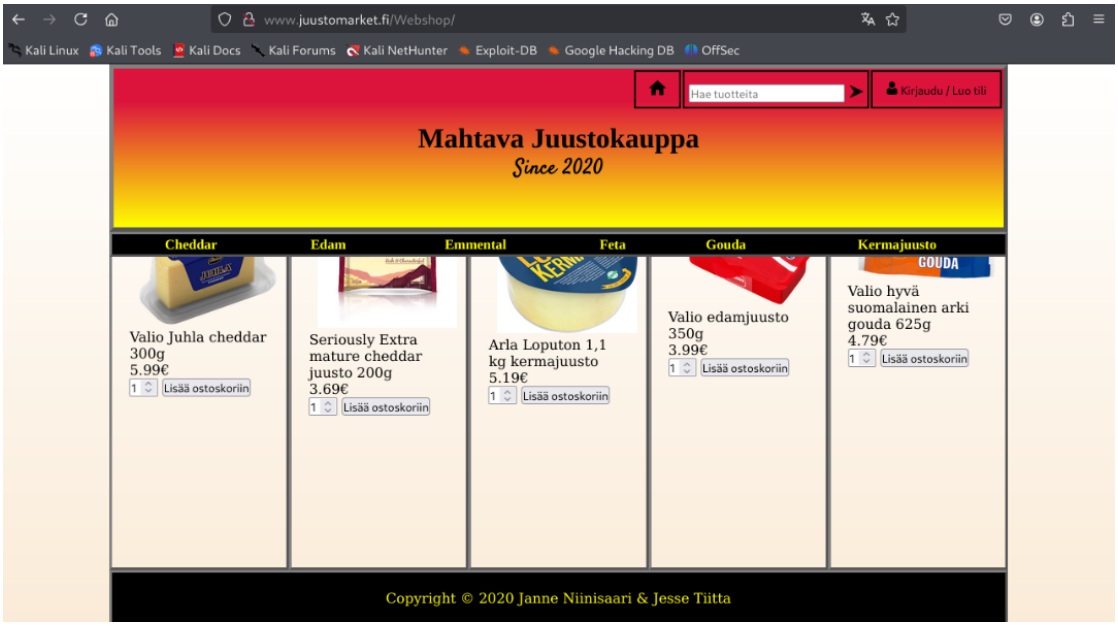
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Ratkaisu on tarpeellinen, koska warehouse segmentistä tulee päästä internettiin, jotta juustomarketin liiketoiminta on sujuvaa.
    - **Voiko niitä kiertää? Miten?**
        - Käyttäjä voi yrittää tunneloida muuta liikennettä sallittujen http tai https-porttien kautta.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **Web Proxy:** Kaikki web-liikenne ohjataan välityspalvelimen kautta, joka voi tehdä tarkempaa sisällönsuodatusta ja kulunvalvontaa.

**Policy 5: Salli Pääsy WebStoreen osoitteessa http(s)://www.juustomarket.fi Varastolta**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Varaston käyttäjien täytyy päästä käyttämään yrityksen omaa webstore-sovellusta, joka sijaitsee DMZ-verkossa palvelimella 10.10.10.5.
    - **Tekemässä:** Luodaan palomuurisääntö, joka sallii http ja https -liikenteen varaston verkosta webstore-palvelimelle.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin**

Worker_Pc luotiin säännöt liikenteen sallimiseksi.


Testataan juustomarket.fi toiminta.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Tämä sääntö avaa tarkan ja rajoitetun pääsyn varastoverkosta dmz:ssa sijaitsevaan webstore-palvelimeen vain tarvittavien web-porttien kautta.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Turvallisuus heikkeni verrattuna tilanteeseen, jossa varasto -> dmz -liikenne oli täysin estetty. Liikenteen avaaminen verkkojen välille lisää riskiä, jos varaston kone saastuu, hyökkääjä voi yrittää hyökätä webstoreen. Riski on kuitenkin rajattu, koska pääsy on rajoitettu vain tiettyyn palvelimeen ja portteihin.
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
    - Mahdollistaa tarvittavan liiketoimintaprosessin webstoren käytön varastolta.

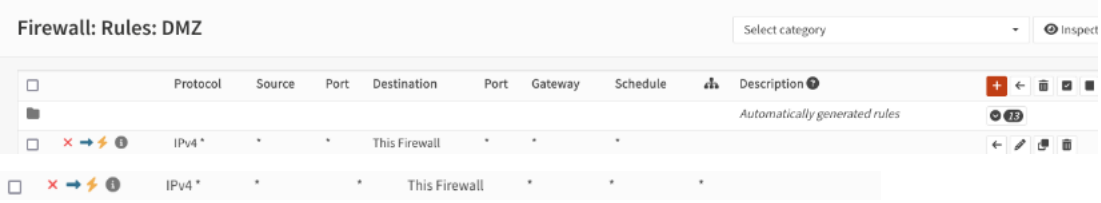
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Kyllä, webstoren käyttö varastolta on välttämätöntä liiketoiminnalle esimerkiksi tilausten käsittely huomioiden.
  - **Voiko niitä kiertää? Miten?**

        - Jos varaston kone saastuu, hyökkääjä saa sen kautta pääsyn webstoreen ja voi yrittää hyökkäystä sieltä käsin.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **Web Application Firewall:** Sijoittamalla waf webstoren eteen voidaan tarkastaa http ja https-liikennettä sovellustason hyökkäysten varalta.
        - **Tarkempi segmentointi:** Tilanne, jossa vain tietyt varaston koneet tarvitsevat pääsyn webstoreen, voidaan luoda niille oma VLAN ja erillinen sääntö.

**Policy 6: Vierasverkosta (GUEST) ja DMZ-palvelimilta ei saa olla pääsyä palomuurin hallintaan**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** dmz ja guest pääsee hallinnoimaan palomuuria. Tavoite on estää dmz ja guestin pääsy palomuurin hallintaan.
    - **Tekemässä:** Luodaan palomuurisäännöt, jotka estävät *kaiken* liikenteen guest ja dmz-verkoista opnsense-palomuurin hallintaan.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

Luotiin säännöt, jotta dmz ja guest ei ole pääsyä palomuurin hallintaan.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Nämä säännöt kieltävät kaiken liikenteen guest ja dmz verkoista palomuurin hallintaan. Käyttämällä this firewall asetusta varmistetaan, että pääsy estetään riippumatta siitä, mitä palomuurin IP-osoitetta käyttäjä yrittää käyttää.
- **Analyysi:**
    - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
        - Turvallisuus parani. Ilman sääntöjä oli mahdollista, että oletussäännöt tai virheellinen konfiguraatio olisi sallinut pääsyn palomuurin hallintaan guest ja dmz -verkoista.

Rajaaminen poistaa potentiaalisen hyökkäys mahdollisuuden palomuurin konfiguraatiota vastaan.

- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Palomuurin hallinnan suojaaminen on tärkeää liiketoiminnan ja turvallisuuden näkökulmasta.
    - **Voiko niitä kiertää? Miten?**
        - **Vaikeaa suoraan, mutta epäsuorasti mahdollista:**
            - **Hyökkäys sallitusta verkosta:** Jos hyökkääjä saa jalansijan luotetussa sisäverkossa, josta hallinta on sallittu, hän voi päästä hallintaan sieltä.
            - **Fyysinen pääsy:** Pääsy palomuurilaitteen konsoliporttiin ohittaa verkkosäännöt.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **IP-osoitteiden rajoitus:** Sallitaan pääsy hallintaan vain tietyistä, staattisista IP-osoitteista luotetussa verkossa.

**Policy 7: Salli Vierasverkon (GUEST) pääsy internetiin**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Guest ei pääse internettiin. Tavoite on sallia guest verkolle internet pääsy.
    - **Tekemässä:** Luodaan palomuurisääntö, joka sallii vierasverkosta lähtevän liikenteen internetiin.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

Guest palomuuri säännöistä luodaan salliva sääntö internettiin.


**Perustele ratkaisu ja tarvittaessa havainnollista.**

- **Perustelu:** Mahdollistaa vierasverkon käyttäjille internet yhteyden.

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

        - Turvallisuuden kannalta tämä on kontrolloitu riski, koska guest verkosta vierailu on sallittava liiketoiminnan kannalta.
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Guest pääsy internet on tarpeellista liiketoiminnan kannalta.

**Policy 8: Vierasverkon (GUEST) käyttäjillä pääsy VAIN osoitteeseen http(s)://www.juustomarket.fi eikä muualle siinä palvelimessa**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Haluamme antaa vierasverkon käyttäjille pääsyn juustomarket.fi, mutta ei mihinkään muualle.
    - **Tekemässä:** Luodaan vierasverkolle säännöt, jotka sallivat liikenteen gues-verkosta vain IP-osoitteeseen 10.10.10.5. Kaikki muu liikenne estetään.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**


    - Luotiin säännöt, jotka estävä mysql ja ftp liikenteen aiempien palomuurisääntöjen lisäksi.
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Aiemmin luotu sääntö päästää guestin webstoreen sisälle, Estot ftp ja mysql rajaavat kattavasti guestin pääsyä eri toimintoihin. Säännöt minimoivat hyökkäyspinta-alaa vierasverkosta DMZ-palvelimeen päin.
- **Analyysi:**
    - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
        - Turvallisuus parani aiemmasta, jossa vierasverkolla olisi ollut laajempi pääsy. Rajoittamalla pääsy vain välttämättömiin palveluihin vähennetään riskiä merkittävästi.

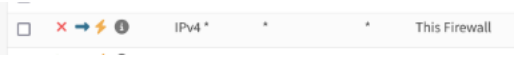
- **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
  - Mahdollistaa vieraille pääsyn webstoreen samalla kun ylläpidetään tiukkaa segmentointia ftp ja mysql kiellon avulla.

- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Vieraille halutaan antaa pääsy vain webstoreen. Rajoitettujen oikeuksien periaatteen noudattaminen on kriittistä juustomarketin turvallisuuden kannalta.
  - **Voiko niitä kiertää? Miten?**
    - **Web-sovelluksen kautta:** Merkittävin riski on itse webstoren haavoittuvuudet.
  - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
    - **Web Application Firewall:** WAF tarjoaa laadukkaamman tason suojauksen web-liikenteelle.

**Policy 9: Vierasverkolla (GUEST) ei saa olla pääsyä sisäverkkoihin (INSIDE)**

- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Vierasverkko on määritelmällisesti epäluotettu verkko. Sen käyttäjillä tai laitteilla ei saa olla pääsyä yrityksen inside verkkoon.
  - **Tekemässä:** Luodaan palomuurisäännöt, jotka estävät liikenteen guest verkosta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

Luotiin guest palomuurisääntö, joka estää guest pääsy inside verkkoon.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Sääntö toteuttaa turvallisuusvaatimuksen: guest verkon täydellisen eristämisen inside verkosta.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**

        - Turvallisuus parani huomattavasti. Ilman palomuurisääntöä mahdollinen hyökkääjä olisi guest verkosta olisi pääsy sisäverkkoon aiheuttaen vahinkoja.
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - Varmistaa, että vierasverkko toimii suunnitellusti.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Ilman vierasverkon palomuurisääntöjä, sisäverkko voi altistua suoraan vierasverkon uhille.
    - **Voiko niitä kiertää? Miten?**
        - **Erittäin vaikeaa verkkotasolla, jos säännöt ovat oikein:**
            - **Palomuurin murtaminen :** Jos hyökkääjä onnistuu murtamaan palomuurin, hän voi muuttaa sääntöjä.
            - **Fyysinen pääsy:** Houkutella sisäverkon käyttäjä avaamaan yhteys vierasverkosta tai hankkia fyysinen sisäänpääsy inside verkon koneeseen.

**Policy 10: Työntekijöillä (INSIDE) ei saa olla pääsyä vierasverkkoon (GUEST)**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Inside työntekijöillä on sisäänpääsy guest verkkoon. Tavoite on tehdä sääntö, joka estää inside työntekijöiden pääsyoikeuden
    - **Tekemässä:** Luodaan palomuurisäännöt, jotka estävät kaiken liikenteen Office- ja Warehouse-verkoista GUEST-verkkoon.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  Luotiin sääntö, jotta inside ei ole asia guest verkkoon.


- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Nämä säännöt täydentävät vierasverkon eristämistä tekemällä siitä kaksisuuntaisen. Estämällä liikenne vähentää riskiä inside verkon koneet saastuisivat tai altistuisivat hyökkäyksille vierasverkon kautta.
- **Analyysi:**

- **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
  - Turvallisuus parani entisestään. Säännön lisääminen parantaa turvallisuutta estämällä potentiaalisia riskejä ja väärinkäyttömahdollisuuksia toiseen suuntaan. Se vahvistaa segmentointia.

- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
  - Suositeltava. Kaksisuuntainen esto kovettaa turvallisuutta, mutta ei ole välttämätön.

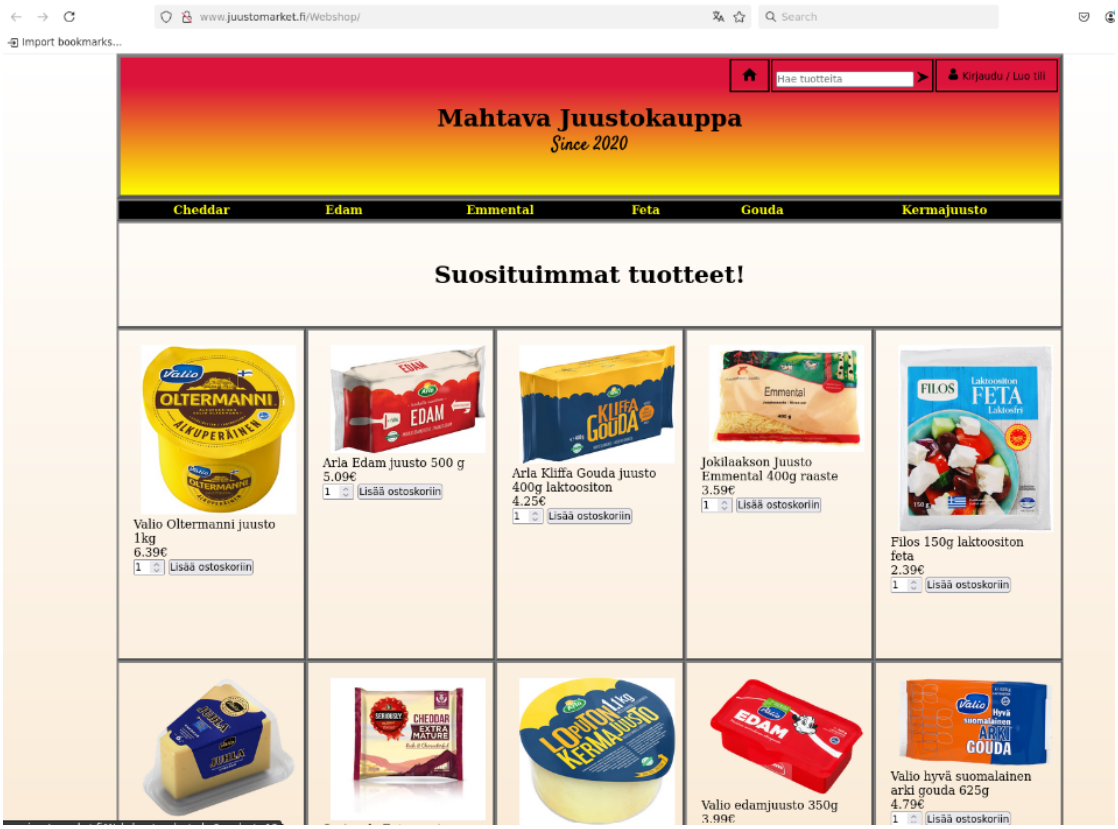
**Policy 11: Työntekijöillä (INSIDE) on oltava pääsy osoitteeseen http(s)://www.juustomarket.fi**

- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Yrityksen työntekijöiden on ei pääse juustomarket.fi nettisivulle. Tavoite on päästää työntekijät sivustolle.
  - **Tekemässä:** Luodaan palomuurisäännöt, jotka sallivat liikenteen warehousesta ja officesta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

Blokataan mysql inside.


Sallitaan ftp inside


Tehdään worker_pc sallivat säännöt http ja https




Testattiin toiminta.

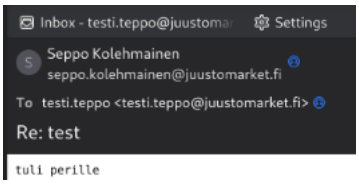
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Nämä säännöt mahdollistavat tarvittavan yhteyden työntekijöiden työasemilta juustomarket.fi
- **Analyysi:**
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - Mahdollistaa tarvittavan juustomarket.fi sivustolle pääsyn.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Kyllä, koska työntekijöiden työtehtävät vaativat juustomarketin käyttöä.
    - **Voiko niitä kiertää? Miten?**
        - **Kaapattu sisäverkon kone:** Jos sisäverkon kone tulee kaapatuksi, hyökkääjä saa sen kautta pääsyn juustomarkettiin.
    - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
        - **Sovellustason kontrollit:** Vahva autentikointi ja tarkka käyttöoikeuksien hallinta juustomarket.fi.
        - **Zero Trust -arkkitehtuuri:** Periaatteessa jokainen yhteyspyyntö todennetaan ja auktorisoidaan erikseen.

**Policy 12: Sähköpostin tulee toimia Juustomarket HQ:n sisällä (INSIDE)**

- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Juustomarket officen käyttäjien täytyy voida lähettää ja vastaanottaa sähköpostia.
  - **Tekemässä:** Määritellään opnsenseen tarvittavat palomuurisäännöt ja porttiohjaukset sähköpostiliikenteelle.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

Tehdään inside Sähköpostin sallimiseen tarvittavat säännöt.


Testataan, että sähköpostia voi lähettää.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - Sääntöjen luominen mahdollistaa sähköpostiliikenteen kulun kaikkiin tarvittaviin suuntiin. Palvelin voi lähettää postia ulospäin ja vastaanottaa postia.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Turvallisuus heikkeni verrattuna tilanteeseen, jossa sähköpostipalvelua ei olisi tai se olisi kokonaan ulkoistettu. Smtp-portin avaaminen internetistä dmz-palvelimelle luo uuden hyökkäyskohteen. Sähköpostipalvelimet ovat jatkuvasti hyökkäysten kohteena. Sähköpostipalvelimen tietoturvan jatkuva ylläpito ja päivittäminen ovat kriittisiä.
  - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
    - Mahdollistaa sähköpostin lähettämisen.
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
  - Kyllä. Sähköposti on juustomarketin henkilökunnalle välttämätön työväline.

- Voiko niitä kiertää? Miten?
  - **Protokollien heikkoudet:** Vanhentuneiden tai turvattomien protokollien esim. smtp käyttö.
  - **Roskaposti ja kalastelu:** Hyökkääjät käyttävät sallittua sähköpostiliikennettä levittääkseen haittaohjelmia ja kalastellakseen tietoja käyttäjiltä.
- Onko olemassa muita parempia vaihtoehtoja? Mitä?
  - **Pilvipalvelut:** Siirtää palvelimen ylläpidon ja osan turvallisuusvastuusta palveluntarjoajalle.
  - **Secure Email Gateway:** Sijoitetaan sähköpostipalvelimen eteen suodattamaan roskapostia, haittaohjelmia ja muita uhkia ennen niiden saapumista palvelimelle tai käyttäjille.

**Policy 14: Estä kaikki muu paitsi HTTP ja HTTPS osoitteeseen 10.10.10.5 ulkoa (OUTSIDE)**

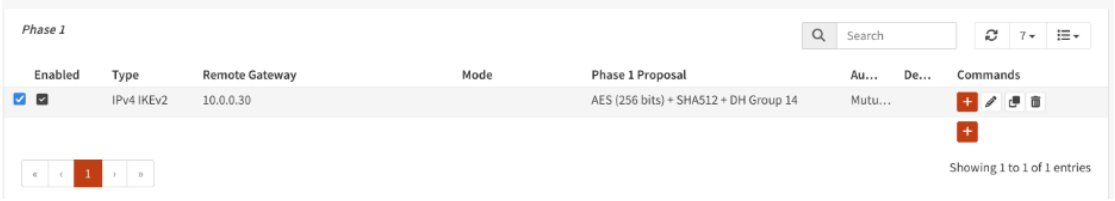
- Tilanne ja mitä ollaan tekemässä?
  - **Tilanne:** Haluamme varmistaa, että internetistä juustomarket-palvelimelle pääsee käsiksi vain http ja https protokollilla.
  - **Tekemässä:** Varmistetaan, että opnsensen WAN-interfacen säännöt sallivat TCP-portit 80 ja 443 kohteeseen 10.10.10.5 ja e kaikki muu liikenne kohteeseen estetään.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
  - Tämä toteutetaan yleensä hyödyntämällä palomuurin oletusestoa ja sallimis- sääntöjä.
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
  - **Perustelu:** Noudattaa vähimpien oikeuksien periaatetta internetistä saapuvalle liikenteelle. Sallimalla vain tarpeellinen liikenne juustomarket palvelimelle, parantaa juustomarketin turvallisuuttaa mahdollisilta hyökkääjiltä.
- **Analyysi:**
  - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
    - Turvallisuus parani. Lukitaan juustomarkettiin pääsy ulkoa ja sallitaan http ja https liikenne. Tehdään hyökkääjän työstä vaikeampaa.

- **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
- Estää vain ei-toivotun ja tarpeettoman liikenteen, mikä on tärkeää turvallisuuden kannalta.

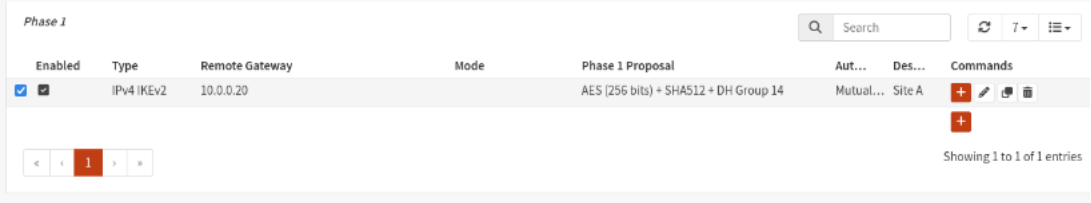
- **Arviointi:**
  - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Kyllä. Laiminlyönti jättää palvelimen alttiiksi laajalle kirjolle erilaisia hyökkäyksiä.
  - **Voiko niitä kiertää? Miten?**
    - **Sovellustason hyökkäykset:** Hyökkääjä voi edelleen yrittää hyödyntää haavoittuvuuksia sallitun http ja https-liikenteen joukosta.
  - **Onko olemassa muita parempia vaihtoehtoja? Mitä?**
    - **Web Application Firewall:** Analysoi http ja https -liikennettä ja estää tunnettuja sovellustason hyökkäyksiä.

## 2 VPN

- **Policy 1: Varaston työasemat voivat kommunikoida Toimiston INSIDE-segmentin työasemien kanssa ja päinvastoin.**
- **Tilanne ja mitä ollaan tekemässä?**
  - **Tilanne:** Yrityksen toimiston ja varaston sisäverkoissa olevien työasemien täytyy pystyä kommunikoimaan keskenään).
  - **Tekemässä:** Luodaan palomuurisäännöt OPNsenseen, jotka sallivat tarvittavan liikenteen officest warehouse inside.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
- Luotiin tunnelia varten officesta warehouselle päin phase 1.



Guard_pc warehouse office suuntaan.




- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Vpn tunneli avaa kommunikaation warehousen ja officen välillä.

    - **Analyysi:**
    - **Vaikuttaako tehty ratkaisu kokonaisuuden muuhun toimintaan? Miten, miksi?**
        - Mahdollistaa sisäisen kommunikaation warehousen ja Officen välillä.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
        - Kyllä. Yrityksen toiminta vaatii yhteistyötä ja resurssien jakoa toimiston ja varaston välillä.
    - **Voiko niitä kiertää? Miten?**
        - Itse sääntöä ei voi "kiertää", mutta sen sallimaa liikennettä voi käyttää väärin:
            - **Sivuttaisliike:** Jos hyökkääjä saa jalansijan toisessa verkossa, hän voi käyttää sallittua yhteyttä hyökätäkseen toisen verkon koneisiin.

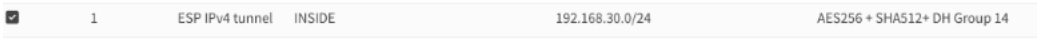
- **Policy 2: Varaston työasemat EIVÄT saa kommunikoida Toimiston GUEST-segmentin työasemien kanssa ja päinvastoin.**

- **Tilanne ja mitä ollaan tekemässä?**
    - **Tilanne:** Sisäverkkojen työasemilla ei saa olla mitään yhteyttä vierasverkkoon, eikä vierasverkon laitteilla saa olla yhteyttä varaston verkkoon.
    - **Tekemässä:**
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**

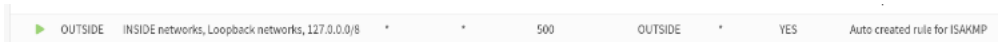
Guard_pc tehdään tunneli sääntö kohti officea osoite 192.168.10.0




Worker_pc tehdään tunneli toiseen suuntaan kohti warhousea 192.168.30.0



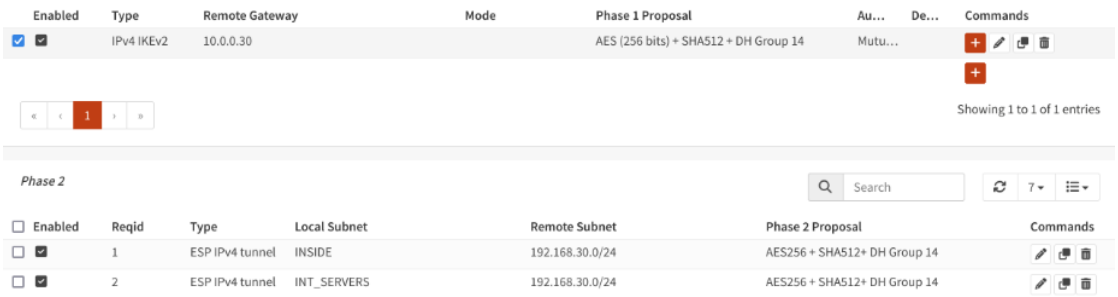

- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** varmistavat, ettei varaston sisäverkon ja epäluotetun vierasverkon välillä voi kulkea liikennettä kumpaankaan suuntaan. Tämä on kriittistä vierasverkon ja sisäverkon eristämiseksi toisistaan ja turvallisuuden ylläpitämiseksi.
- **Arviointi:**
    - **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
    - Kyllä mahdollistaa icmp liikenteen officesta warehouseen ja toisinpäin

- **Policy 7: Secure IPsec ISAKMP Port**
    - **Tekemässä:** Halutaan rajoittaa liikenne ISAKMP-porttiin tuleva liikenne sallituksi tunnetusta ja luotetusta lähteestä, eli varaston julkisesta IP-osoitteesta.
- **Miten ongelma saatiin ratkaistua tai miten jokin asia toteutettiin?**
- **Guard_pc luotiin nat sääntö, joka sallii ISAKMP portin**
- 

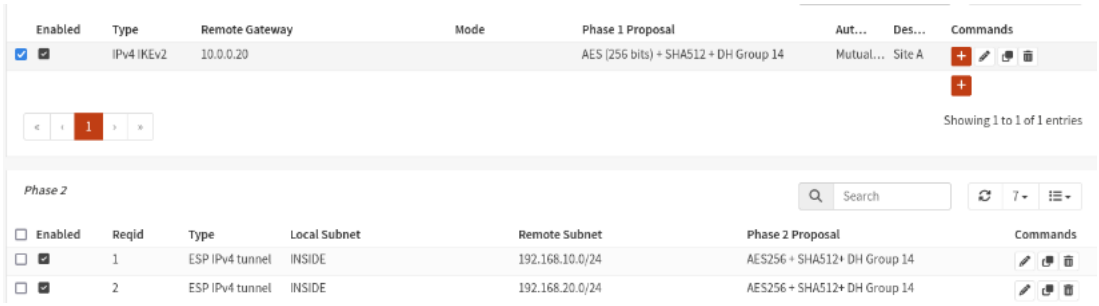
- **Perustele ratkaisu ja tarvittaessa havainnollista.**
    - **Perustelu:** Vaikka IPsec-protokolla itsessään sisältää vahvan tunnistuksen ja salauksen, sen kuuntelemien porttien jättäminen avoimeksi koko internetille altistaa palvelun tarpeettomasti:
        - Resurssien kulutus: Jokainen yhteysyritys kuluttaa palomuurin resursseja.
        - Haavoittuvuuksien hyödyntäminen: Mahdollistaa IPsec-toteutuksen mahdollisten haavoittuvuuksien etsimisen ja hyödyntämisen kenelle tahansa.
- **Analyysi:**
    - **Miten järjestelmän turvallisuus muuttui vs aiempi tilanne? Miksi?**
        - Turvallisuus parani. VPN-päätepisteen ISAKMP hyökkäyspinta-ala internetistä pienennettiin minimiin.
- **Arviointi:**

- **Onko tehdyt ratkaisut tarpeellisia? Miksi?**
- Normaali ja suositeltava tapa koventaa internetiin avoinna olevia VPN.
- **Voiko niitä kiertää? Miten?**
  - **IP Spoofing :** Hyökkääjä voisi yrittää väärentää IP-osoitteekseen Varaston IP-osoitteen.

Worker_pc vpn tunnelit.




Guard_Pc tunnelit




## 3 REFLEKTOINTI:

### OPNsense Tilallinen Palomuuri ( Stateful Firewall ) ja VPN-Politiikat

- Tämä harjoitus keskittyi opnsense palomuurin tilallisten sääntöjen ja IPsec VPN -yhteyksien konfigurointiin.
- **Mitä saavutin?**
- **Tilallisten palomuurisääntöjen toteutus:** Onnistuin toteuttamaan ja testaamaan palomuurisääntöjä, jotka hallitsevat liikennettä eri suuntiin. Esimerkiksi Vpn tunnelin ja ipsec tunnelin kautta
- **Mitä jäi saavuttamatta?**

- Vpn osio meni pieleen, koska en vain osannut tehdä sitä. Olisi pitänyt pyytää apua.
- **Miten opin asian?**
- Opin statefullin osalta hyvin, kun ymmärsin testaamalla ja kokeilemalla, mitä mikäkin sääntö tekee. Vpn osiossa yritin, mutta en löytänyt ratkaisua suurinpaan osaan tehtävistä.

**Kuinka taitoni kehittyivät?**

- Taidot käyttää opnsensea palomuurisääntöjen ja NATin konfigurointiin kehittyivät
- **Verkkosegmentointi:** Ymmärrykseni verkkojen segmentoinnin tärkeydestä ja sen käytännön toteutuksesta palomuurisäännöillä syveni.
- Sain pintaraapaisun, miten vpn tunnelointia tehdään.
- **Miten lähestyisin asiaa seuraavalla kerralla?**
- **Dokumentaatio:** Jos ongelmia ilmenee, kysyisin apua matalammalla kynnyksellä ja dokumentoisin tarkemmin tehdyt säännöt ja testitulokset. Jotta ymmärtäisin, mitä olin tehnyt aikaisemmin paremmin.

**Miten pystyn käyttämään tätä taitoa/osaamista tulevaisuudessa?**

- 
- **Verkon suunnittelu ja ylläpito:** Osaan jonkin verran konfiguroida ja ylläpitää palomuureja
- **Tietoturvan parantaminen:** Osaan toteuttaa verkon segmentointia ja palomuurisäännöillä koventaa verkkoa ja palomuureja.