Labra 2

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

20.9.2024

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 3](#_Toc178177006)

[2 Teoria 3](#_Toc178177007)

[2.1 DNS 4](#_Toc178177008)

[2.2 NAT 4](#_Toc178177009)

[3 Labran kysymykset 4](#_Toc178177010)

[4 Työn kulku 7](#_Toc178177011)

[4.1 Yhteys internetistä DMZ-alueelle 7](#_Toc178177012)

[4.2 RDP-yhteys WS01 -> Servers-nety 10](#_Toc178177013)

[4.3 Nat u-turn 13](#_Toc178177014)

[5 Pohdinta 17](#_Toc178177015)

[Lähteet 18](#_Toc178177016)

Kuviot

[Kuvio 1. Application1 6](#_Toc178168176)

[Kuvio 2. Application2 6](#_Toc178168177)

[Kuvio 3. VLE\_TO\_DMZ 8](#_Toc178168178)

[Kuvio 4. Uusi osoite 8](#_Toc178168179)

[Kuvio 5. NAT-asetukset 1 9](#_Toc178168180)

[Kuvio 6. NAT-asetukset 2 9](#_Toc178168181)

[Kuvio 7. NAT-asetukset 3 10](#_Toc178168182)

[Kuvio 8. www-sivu 10](#_Toc178168183)

[Kuvio 9. Uusi turvallisuusalue WS-TO-SERVERS 11](#_Toc178168184)

[Kuvio 10. WS-TO-SERVERS asetukset 11](#_Toc178168185)

[Kuvio 11. WS-TO-SERVERS sovellukset 12](#_Toc178168186)

[Kuvio 12. Etäyhteys avattu 12](#_Toc178168187)

[Kuvio 13. WS\_TO\_DMZ turvallisuussäännön luonti 13](#_Toc178168188)

[Kuvio 14. WS-TO-DMZ asetukset 14](#_Toc178168189)

[Kuvio 15. NAT u-käännöksen luonti 14](#_Toc178168190)

[Kuvio 16. NAT u-käännöksen asetukset 1 15](#_Toc178168191)

[Kuvio 17. NAT u-käännöksen asetukset 2 15](#_Toc178168192)

[Kuvio 18. Hosts tiedosto 16](#_Toc178168193)

[Kuvio 19. Hosts-tiedoston sisältö 16](#_Toc178168194)

[Kuvio 20. WordPress-sivusto WS01-työasemalla 17](#_Toc178168195)

# Johdanto

Tietoturvakontrollit kurssin toisessa labrassa (Lab 2 – Paloalto Firewall Rules for Public Services) perehdytään PaloAlto -palomuurin turvallisuussääntöihin ja NAT (Network Address Translation) -tekniikkaan. Harjoituksessa keskeisinä tavoitteina ovat sisäverkon suojaus palomuurin sääntöjen avulla ja ulkoverkosta tulevan liikenteen hallinta turvallisesti. Labrassa on myös muutama kysymys liittyen PaloAlton turvallisuus asetuksiin -ja vyöhykkeisiin, näitä varten tulee perehtyä vähän syvemmin PaloAlto:n konfigurointiin.

Labran tavoitteena on saada julkisesta VLE verkosta internet yhteys DMZ palvelimille, eli nettisivulle pitäisi päästä sivuston nimen avulla, ilman että vierailijat joutuvat syöttämään IP-osoitetta. Tulee siis sallia palomuurissa VLE -ja DMZ alueiden välinen yhteys www- ja DNS-palveluilla. Labrassa tulee myös saada RDP-yhteys WS-netistä Servers-netin laitteille. NAT-tekniikan avulla palvelin voidaan avata julkiseen verkkoon ilman, että sisäverkko näkyy ulkopuolisille.

# Teoria

Tämä labra liittyy Palo Alto -palomuurin turvallisuussääntöihin sekä NAT-sääntöjen ymmärtämiseen. Tarkoituksena on tutustua www- ja DNS-palveluihin sekä ymmärtää NAT-periaatteen toiminta. Tehtävänä on päästä julkisesta VLE-verkosta muodostamaan yhteys DMZ:lla oleviin koneisiin. Eli konkreettisesti meidän täytyy päästä julkisesta VLE-verkosta internetyhteydellä omille www -sivuille. Tämän täytyy toimia julkisella osoitteella eli ilman ip-osoitetta.

## DNS

DNS (Domain Name System) on järjestelmä, joka kääntää verkkotunnukset, kuten [www.group13.ttc60z.vle.fi](http://www.group13.ttc60z.vle.fi), IP-osoitteiksi. Kun selaimeen kirjoitetaan verkkosivuston osoite, DNS-palvelin hakee siihen liittyvän IP-osoitteen, jotta selain voi muodostaa yhteyden oikeaan palvelimeen. Prosessin vaiheet ovat seuraavat:

1. DNS-kysely: Selain lähettää kyselyn DNS-palvelimelle
2. Välimuisti: Jos osoite löytyy selaimen välimuistista, se palautetaan heti
3. Juuripalvelimet: Jos välimuistista ei löydy tietoa, DNS kysyy juuripalvelimilta, joka ohjaa kyselyn seuraaville palvelimille.
4. Valtuutetut nimipalvelimet: Lopulta kysely ohjataan nimipalvelimelle, joka palauttaa oikean IP-osoitteen.
5. Osoitteen palautus: IP-osoite lähetetään selaimelle, joka lataa verkkosivun.

(Šimonėlytė, Miglė. 2023).

## NAT

NAT (Network Address Translation) on verkkotekniikka, joka muuntaa yksityisiä IP-osoitteita julkisiksi IP-osoitteiksi ja päinvastoin. Tämä mahdollistaa useiden laitteiden pääsyn internetiin yhdellä julkisella IP-osoitteella. Tällä keinoin säästetään IP-osoitteita ja parannetaan verkon tietoturvaa. NAT toimii seuraavasti:

1. Yksityiset IP-osoitteet: Laitteilla on yksityiset IP-osoitteet paikallisessa verkossa
2. Muunnos: Kun laite lähettää datan internetiin, NAT-laite, kuten reititin, muuntaa yksityisen IP-osoitteen julkiseksi IP-osoitteeksi.
3. Osoitteen kartoitus: NAT-laite pitää kirjaa siitä, mikä laite lähetti pyynnön, jotta vastaukset voidaan ohjata oikeaan laitteeseen.
4. Vastaus internetistä: Kun vastaus saapuu, NAT muuntaa julkisen IP-osoitteen takaisin alkuperäiseksi yksityiseksi osoitteeksi ja lähettää datan oikealle laitteelle.

(NAT).

# Labran kysymykset

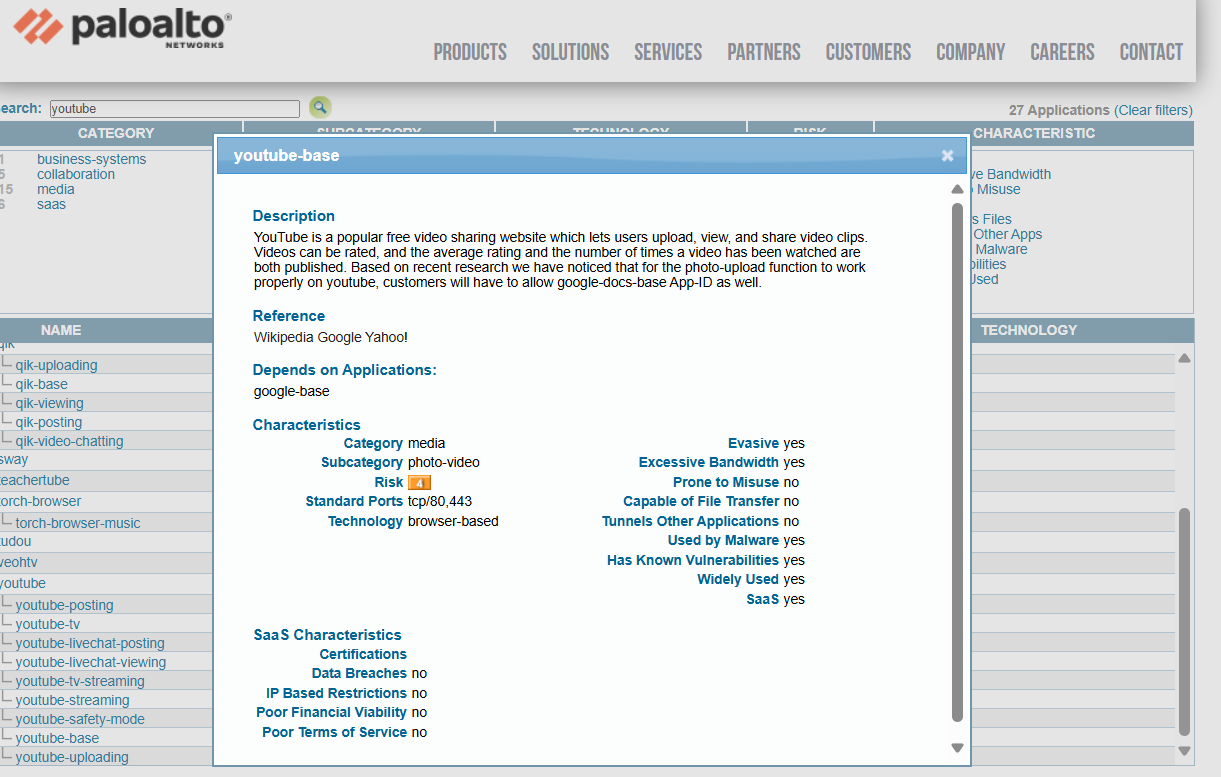
1. Mikä ero on **INTERZONE**, **INTRAZONE** ja **UNIVERSAL** säännöillä?

Zonejen tai vyöhykkeiden säännöt Palo Alton palomuurissa organisoivat verkon liikennettä määritellen mistä liikenne tulee, mihin se saa mennä. **Intrazone** säännöllä voidaan sallia liikenne samassa verkon segmentissä (vyöhykkeessä) esim. Admin-netissä kaikki vyöhykkeen sisäinen liikenne laitteiden välillä.

**Interzone** sääntö sallii liikenteen vyöhykkeiden välillä, samalla estää vyöhykkeen sisällä liikenteen laitteiden välillä. Esimerkiksi Kali saa yhteyden DC01-palvelimeen Servers-netissä, mutta Interzone estää Kalin yhteyden toisesta Admin-netin laitteesta, koska ne ovat samassa vyöhykkeessä.

**Universal** sääntö sallii liikenteen sekä vyöhykkeiden sisällä, että välillä. Esimerkiksi Kali voi ottaa yhteyden muihin Admin-netin laitteisiin ja myös vaikkapa Servers-netin DC01-palvelimeen. Universal ei siis tee estoja liikenteelle vyöhykkeiden välillä. (What are Universal, Intrazone and Interzone Rules? 2018).

2. Mikä ero on ”**Applicationilla**” ja ”**Servicellä**” paloalton turvallisuuspoliitikoissa?

Palo Altossa "**Application**" tarkoittaa sovelluksen tunnistamista perustuen sen toimintaan, joka johtaa tarkempaan toimintojen seurantaan, kuin vain porttien avulla. Palomuuri voi tunnistaa vaikkapa Youtube-sovelluksen ja vielä tarkemmin sovelluksen eri toimintoja, kuten striimaus ja videoihin kommentointi. (Kuvio 1). Palo Alto palomuurin avulla voidaan sallia Youtube, mutta ei sallita videoiden lisäys toimintoa, koska se tuo enemmän riskitekijöitä sovelluksen käyttöön. (Kuvio 2).

Kuvio 1. Application 1



Kuvio 2. Application 2

Palvelut tai "**Servicet**" ovat verkkoliikenteeseen perinteisemmin määritellyt portit (esim. HTTP portti 80, HTTPS portti 443). Ne käsittelevät reititystietoja ja porteissa tapahtuvaa liikennettä, kun "Applications" perustuu toiminnan tunnistamiseen. (What Are Applications and Services? 2023).

3. Mitä turvallisuuspoliitikoissa olevien profiilien **(Security Policy Rule -> Actions -> Profile)** avulla voidaan tehdä?

Palo Alto **turvallisuusprofiilit** (Security Policy Rule -> Actions -> Profile) mahdollistavat liikenteen tarkemman suojauksen käyttämällä erilaisia tietoturva toimintoja. Profiileilla saadaan aikaan vaikkapa virussuojaus (Antivirus), tunkeutumisen estojärjestelmiä (Intrusion Prevention System, IPS), tiedostojen tarkistuksen (File Blocking) sekä URL-suodatuksen (URL Filtering). Niiden avulla voidaan suodattaa haitallista verkkoliikennettä ja löytää uhkia. Profiileilla voidaan myös esim. estää käyttäjien pääsy kyseenalaisille nettisivuille (URL Filtering). (Security Policy Rule Best Practices. 2024)

# Työn kulku

## Yhteys internetistä DMZ-alueelle

Salliaksemme pääsyn www-sivulle, meidän täytyy sallia pääsy DMZ:lle VLE rajapinnasta. Teimme palomuuriin ensin säännön VLE\_TO\_DMZ kuvion 3 mukaisilla säännöillä. Asetimme lähdevyöhykkeeksi VLE:n ja kohdevyöhykkeeksi DMZ:n. Application välilehdellä asetimme sovelluksiksi DNS ja web-browsing.

Kuva, joka sisältää kohteen kuvakaappaus, teksti, Samansuuntainen, numero

Kuvaus luotu automaattisesti

Kuvio 3. VLE\_TO\_DMZ

Loimme uuden osoitteen objects-välilehden address-osiossa. (Kuvio 4).



Kuvio 4. Uusi osoite

Seuraavaksi loimme uuden Nat politiikan nimellä www-NAT. (Kuvio 5).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, Fontti

Kuvaus luotu automaattisesti

Kuvio 5. NAT-asetukset 1

Original Packet välilehdellä asetimme lähteeksi VLE vyöhykkeen ja määränpääksi public-osoitteen. (Kuvio 6).

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, numero

Kuvaus luotu automaattisesti

Kuvio 6. NAT-asetukset 2

Translated Packet välilehdellä käytimme aiemmin luomaamme uutta osoitetta www-palvelin-PRIVA. (Kuvio 7).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 7. NAT-asetukset 3

Tallennettuamme muutokset, kokeilimme päästä WordPress-sivuillemme omalla tietokoneellamme. Kirjoitimme selaimen osoitekenttään <http://www.group13.ttc60z.vle.fi> ja pääsimme sivuille. (Kuvio 8).

Kuva, joka sisältää kohteen kuvakaappaus, teksti, Multimediaohjelmisto, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 8. www-sivu

## RDP-yhteys WS01 -> Servers-net

Seuraavana tavoitteena oli sallia Servers-net laitteiden etäkäyttö RDP:n välityksellä työasemalta WS-netissä. Tämän toteuttamiseksi loimme uuden turvallisuussäännön WS-TO-SERVERS. (Kuvio 9).

Kuva, joka sisältää kohteen teksti, viiva, numero, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 9. Uusi turvallisuusalue WS-TO-SERVERS

Asetimme lähdevyöhykkeeksi WS-netin ja määränpääksi SERVERS-netin. (Kuvio 10).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 10. WS-TO-SERVERS asetukset

Application-välilehdelle lisäsimme kaikki tarpeelliseksi havaitut toiminnot Servers-netin ja WS-netin väliseen toimintaan, RDP-yhteyden luomiseksi täytyy olla valittuna ms-rdp. Muut valinnat lisäsimme sitä mukaa, kun saimme virheilmoituksia ja lisäsimme ehdotetut sovellukset. (Kuvio 11).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 11. WS-TO-SERVERS sovellukset

Kirjauduimme WS01-koneelle, avasimme etäyhteys-sovelluksen (RDP) ja asetimme osoitteeksi 10.3.0.12 ja saimme yhteyden tiedostopalvelimelle SRV01. (Kuvio 12).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

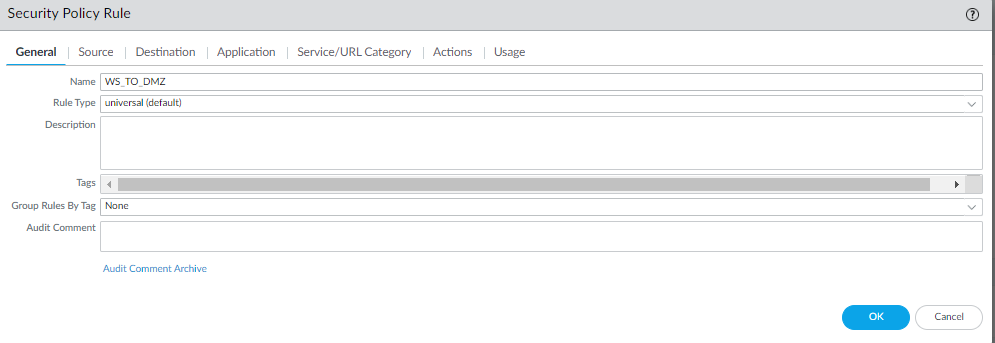
Kuvaus luotu automaattisesti

Kuvio 12. Etäyhteys avattu

## Nat u-turn

Halusimme myös saada WordPress www-sivumme näkyviin WS-netin laitteille. Tämän saavuttamiseksi meidän täytyi tehdä uusi turvallisuus sääntö, joka sallii liikenteen WS-netistä DMZ vyöhykkeelle. Tämän lisäksi loimme NAT-sääntöihin niin sanotun NAT u-käännöksen, jotta löysimme sivun julkisella osoitteella.

Aloitimme luomalla uuden turvallisuus säännön WS\_TO\_DMZ. (Kuvio 13).



Kuvio 13. WS\_TO\_DMZ turvallisuussäännön luonti

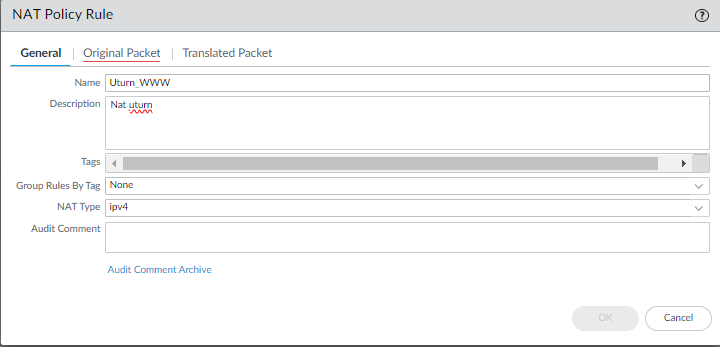
Asetimme lähdevyöhykkeeksi WS-netin ja määränpääksi DMZ:n. (Kuvio 14).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 14. WS-TO-DMZ asetukset

Seuraavaksi loimme NAT u-käännöksen, jotta pääsimme sivuillemme niiden julkisella osoitteella. (Kuvio 15).



Kuvio 15. NAT u-käännöksen luonti

Original Packet -välilehdellä asetimme lähdealueeksi WS-netin ja määränpääksi public-osoitteen. (Kuvio 16).

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 16. NAT u-käännöksen asetukset 1

Translated Packet -välilehdellä Translated Address kohtaan valitsimme www-palvelinPRIVA:n, johon asetimme aiemmin WordPress-sivustoa ylläpitävän palvelimen IP-osoitteen eli 10.4.0.11, portin jätimme tyhjäksi. (Kuvio 17).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 17. NAT u-käännöksen asetukset 2

Löytääksemme sisäisessä verkossamme olevan sivuston, määritimme WS01-työasemalla hosts-tiedostoon IP-osoitteen ja palvelimen nimen. (Kuvio 18).

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 18. Hosts tiedosto

Hosts-tiedostoon lisäsimme alimmaksi riviksi IP-osoitteen ja osoitteen [www.group13.ttc60z.vle.fi](http://www.group13.ttc60z.vle.fi). (Kuvio 19.)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 19. Hosts-tiedoston sisältö

Näiden muokkausten tuloksena saimme WS01-työasemalta avattua WordPress-sivustomme. (Kuvio 20).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 20. WordPress-sivusto WS01-työasemalla

# Pohdinta

Tehtävän aikana pääsimme syventymään lisää Palo Alton palomuurin konfigurointiin ja ympäristömme toimintaan. Monet labrassa asetetut säännöt olivat ensimmäisestä labrasta tuttuja, joten navigointi oli nopeaa ja ryhmälle helppoa. Lisäksi opintojakson Moodle-työtilasta löytyi hyvät ja kattavat ohjeet labratyön tekoon, mikä nopeutti tekemistä huomattavasti.

NAT-tekniikka oli ryhmällemme uutta, joten sen kanssa kikkailu toi labraan mukavasti uutuuden tunnetta. U-käännöksen tekeminen ja sen toimintaperiaatteet olivat myös uutta ja jäivät hiukan avoimeksi ryhmälle, että miten se oikeasti toimii. Uutena asiana labrassa ryhmälle oli myös hosts-tiedoston muokkaus.

Lähteet

NAT. Afterdawn-verkkosivuston tietopankki. Viitattu 23.9.2024. <https://dawn.fi/sanasto/nat>

Security Policy Rule Best Practices. 2024. Palo Alto dokumentti. Viitattu 20.9.2024. <https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices>

Šimonėlytė, Miglė. DNS: aloittelijan opas internetin nimipalvelujärjestelmään. Blogikirjoitus Nordvpn.com -sivustolla. 4.4.2023. Viitattu 23.9.2024. <https://nordvpn.com/fi/blog/mika-on-dns/?srsltid=AfmBOorkWYZk6jkML_ioV40j0qtMhOf-kROggsEdw2D_asBMBy0ZLgmy>

What Are Applications and Services? 2023. Palo Alto blog postaus. Viitattu 20.9.2024. <https://live.paloaltonetworks.com/t5/community-blogs/what-are-applications-and-services/ba-p/566471>

What are Universal, Intrazone and Interzone Rules? 2018. Päivitetty 6.8.2023. Palo Alto knowledgebase artikkeli. Viitattu 20.9.2024. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC