



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
2	Teoria	3
2.1	DNS	4
2.2	NAT	4
3	Labran kysymykset	4
4	Työn kulku	7
4.1	Yhteys internetistä DMZ-alueelle	7
4.2	RDP-yhteys WS01 -> Servers-nety	10
4.3	Nat u-turn	13
5	Pohdinta	17
	Lähteet	18

Kuviot

Kuvio 1.	Application1	6
Kuvio 2.	Application2	6
Kuvio 3.	VLE_TO_DMZ	8
Kuvio 4.	Uusi osoite	8
Kuvio 5.	NAT-asetukset 1	9
Kuvio 6.	NAT-asetukset 2	9
Kuvio 7.	NAT-asetukset 3	10
Kuvio 8.	www-sivu	10
Kuvio 9.	Uusi turvallisuusalue WS-TO-SERVERS	11
Kuvio 10.	WS-TO-SERVERS asetukset	11
Kuvio 11.	WS-TO-SERVERS sovellukset	12
Kuvio 12.	Etäyhteys avattu	12
Kuvio 13.	WS_TO_DMZ turvallisuussäännön luonti	13
Kuvio 14.	WS-TO-DMZ asetukset	14
Kuvio 15.	NAT u-käännöksen luonti	14
Kuvio 16.	NAT u-käännöksen asetukset 1	15

Kuvio 17. NAT u-käännöksen asetukset 2	15
Kuvio 18. Hosts tiedosto	16
Kuvio 19. Hosts-tiedoston sisältö.....	16
Kuvio 20. WordPress-sivusto WS01-työasemalla	17

1 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.

2 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.

2.1 DNS

DNS (Domain Name System) on järjestelmä, joka kääntää verkkotunnukset, kuten 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. (Šimonélytė, Miglė. 2023).

2.2 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).

3 Labran kysymykset

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

Zonejen tai vyöhykkeiden säännöt Palo Alton palomuurissa organisoivat verkon liikennettä määrittellen 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**" paloalon turvallisuuspolitiikoissa?

Palo Altossa "**Application**" tarkoittaa sovelluksen tunnistamista perustuen sen toimintaan, joka johtaa tarkempaan toimintojen seurantaan, kuin vain porttien avulla. Palomuuuri 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).

The screenshot shows the Palo Alto Networks application catalog interface. A search bar at the top left contains the text 'youtube'. Below it, a list of categories is visible, including 'business-systems', 'collaboration', 'media', and 'saas'. The 'youtube-base' application is selected, and its details are displayed in a modal window. The details include a description, reference, depends on applications, characteristics, and SaaS characteristics. The characteristics section lists various attributes such as 'Evasive', 'Excessive Bandwidth', 'Prone to Misuse', 'Capable of File Transfer', 'Tunnels Other Applications', 'Used by Malware', 'Has Known Vulnerabilities', 'Widely Used', and 'SaaS'. The SaaS characteristics section lists 'Certifications', 'Data Breaches', 'IP Based Restrictions', 'Poor Financial Viability', and 'Poor Terms of Service'.

Kuvio 1. Application 1

youtube				
youtube-tv	media	photo-video	1	browser-based
youtube-livechat-posting	media	photo-video	2	browser-based
youtube-livechat-viewing	media	photo-video	2	browser-based
youtube-tv-streaming	media	photo-video	2	browser-based
youtube-streaming	media	photo-video	4	browser-based
youtube-uploading	media	photo-video	4	browser-based
youtube-base	media	photo-video	4	browser-based
youtube-safety-mode	media	photo-video	4	browser-based

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).

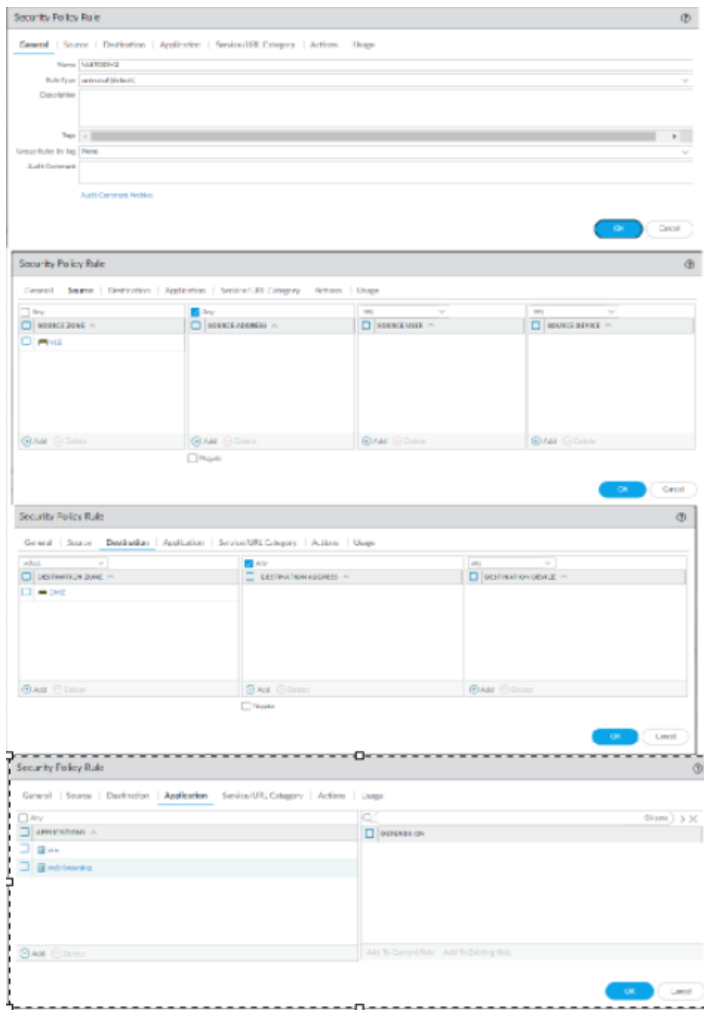
3. Mitä turvallisuuspolitiikoissa olevien profiilien (**Security Policy Rule -> Actions -> Profile**) avulla voidaan tehdä?

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)

4 Työn kulku

4.1 Yhteys internetistä DMZ-alueelle

Salliaksemme pääsyn www-sivulle, meidän täytyy sallia pääsy DMZ:lle VLE rajapinnasta. Teimme palomuriin 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.



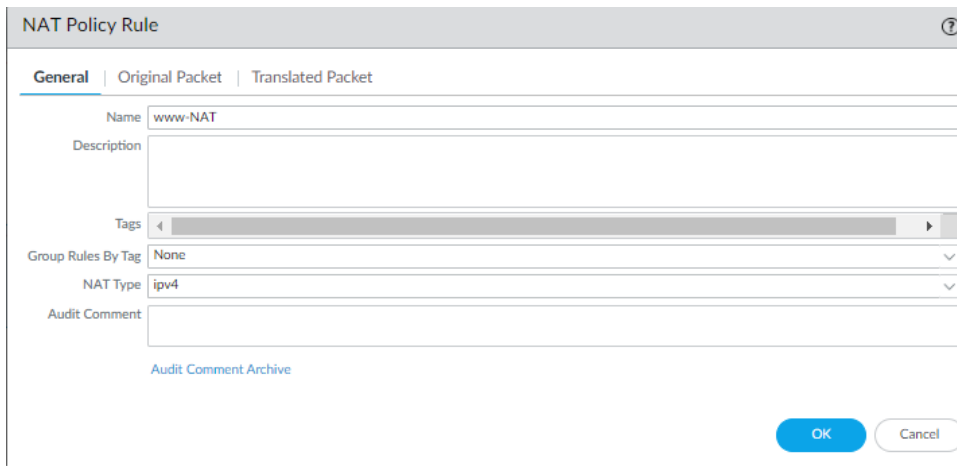
Kuvio 3. VLE_TO_DMZ

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



Kuvio 4. Uusi osoite

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



NAT Policy Rule ⓘ

General | Original Packet | Translated Packet

Name:

Description:

Tags:

Group Rules By Tag:

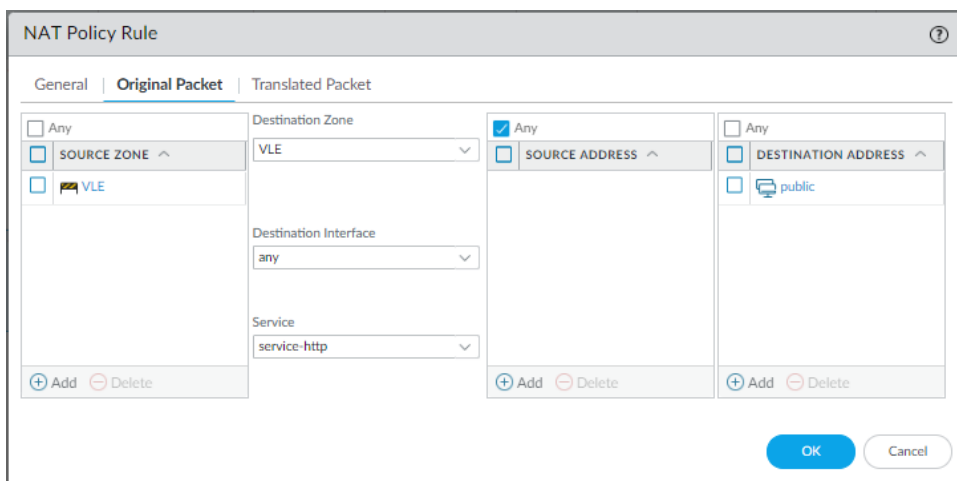
NAT Type:

Audit Comment:

[Audit Comment Archive](#)

Kuvio 5. NAT-asetukset 1

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



NAT Policy Rule ⓘ

General | **Original Packet** | Translated Packet

☐ Any

☒ SOURCE ZONE ^

☐ VLE

Destination Zone:

Destination Interface:

Service:

☒ Any

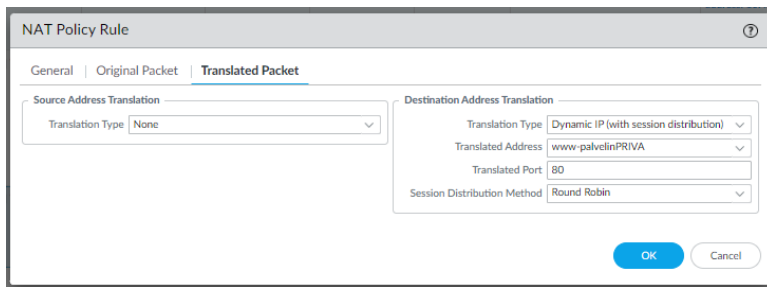
☒ SOURCE ADDRESS ^

☐ DESTINATION ADDRESS ^

☐ public

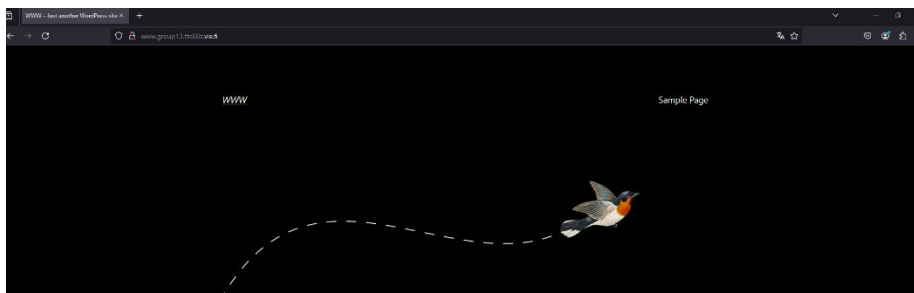
Kuvio 6. NAT-asetukset 2

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



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).



Kuvio 8. www-sivu

4.2 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).

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: WS-TO-SERVERS

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

Kuvio 9. Uusi turvallisuusalue WS-TO-SERVERS

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

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

☐ Any

☒ SOURCE ZONE ^

☐ WS-NET

☐ SOURCE ADDRESS ^

☐ SOURCE USER ^

☐ SOURCE DEVICE ^

☐ Add ☐ Delete

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

☐ DESTINATION ZONE ^

☐ SERVERS-NET

☒ Any

☐ DESTINATION ADDRESS ^

☐ DESTINATION DEVICE ^

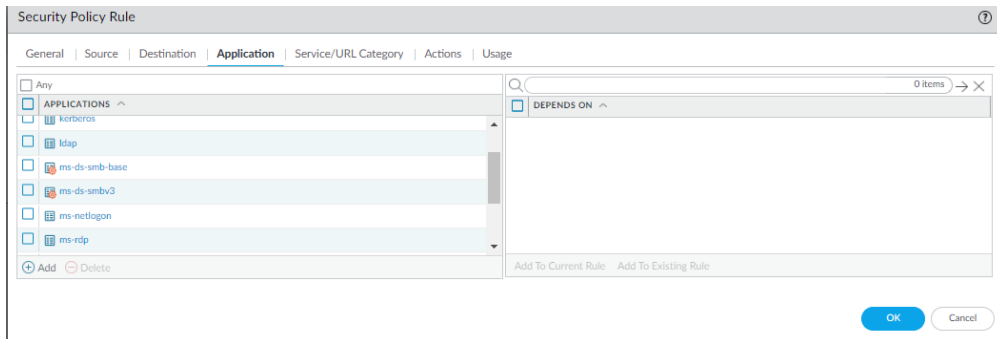
☐ Add ☐ Delete

☐ Negate

OK Cancel

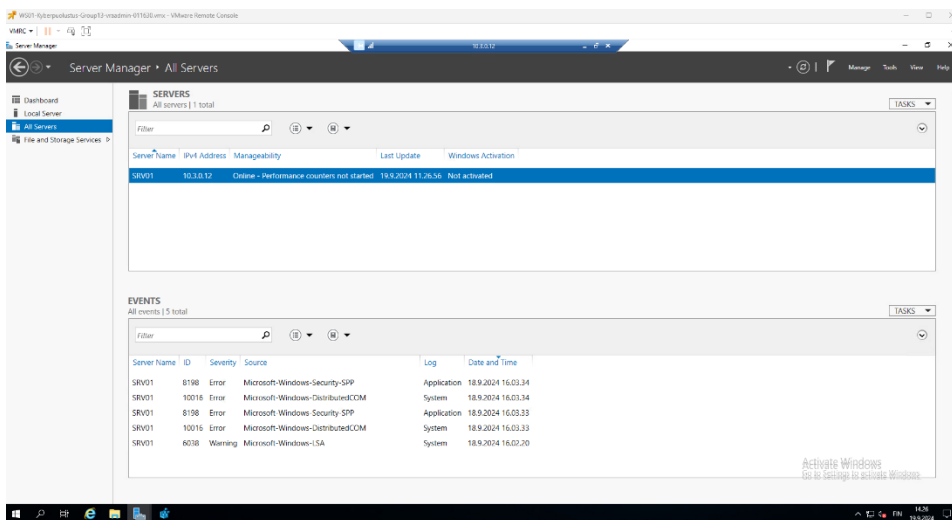
Kuvio 10. WS-TO-SERVERS asetukset

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).



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).

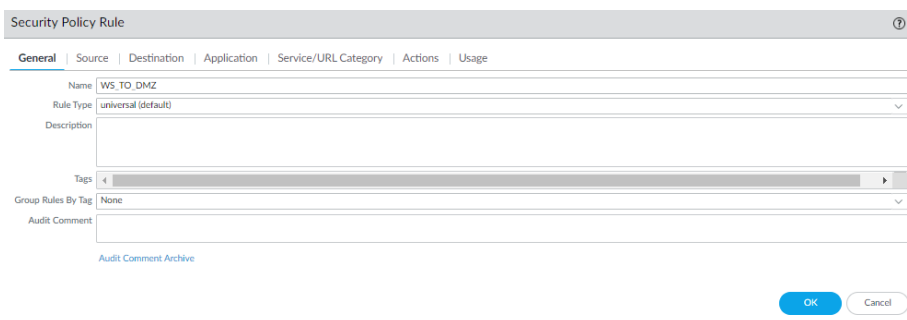


Kuvio 12. Etäyhteys avattu

4.3 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).



The screenshot shows a 'Security Policy Rule' configuration window. The 'General' tab is selected, showing fields for Name (WS_TO_DMZ), Rule Type (universal (default)), Description, Tags, Group Rules By Tag (None), and Audit Comment. There are 'OK' and 'Cancel' buttons at the bottom right.

Kuvio 13. WS_TO_DMZ turvallisuussäännön luonti

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

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any	any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input type="checkbox"/> WS-NET			

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select	<input checked="" type="checkbox"/> Any	any
<input type="checkbox"/> DESTINATION ZONE ^	<input type="checkbox"/> DESTINATION ADDRESS ^	<input type="checkbox"/> DESTINATION DEVICE ^
<input type="checkbox"/> DMZ		

+ Add - Delete

☐ Negate

OK Cancel

Kuvio 14. WS-TO-DMZ asetukset

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

NAT Policy Rule

General | Original Packet | Translated Packet

Name: Uturn_WWW

Description: Nat uturn

Tags: < >

Group Rules By Tag: None

NAT Type: ipv4

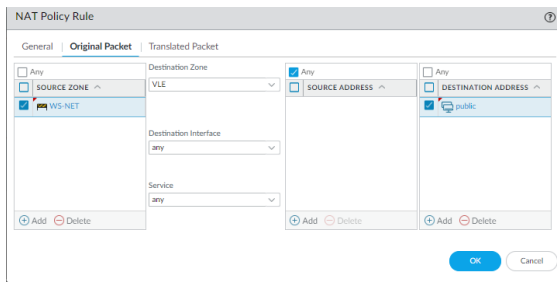
Audit Comment

Audit Comment Archive

OK Cancel

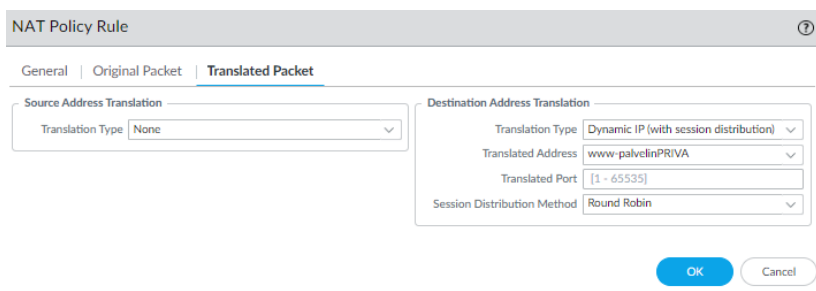
Kuvio 15. NAT u-käännöksen luonti

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



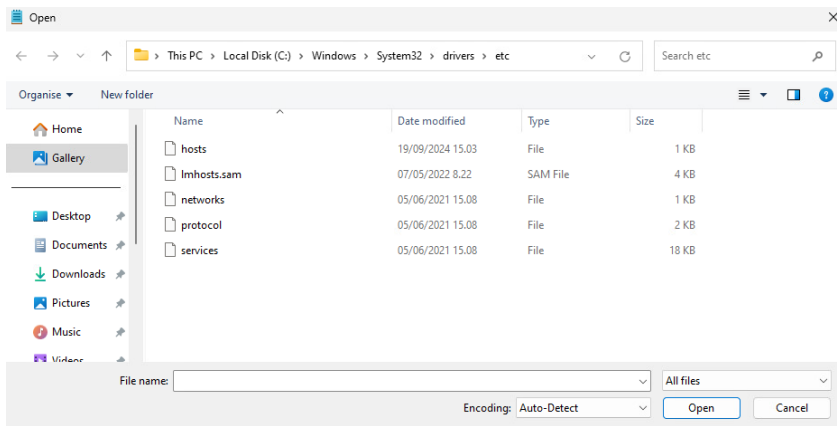
Kuvio 16. NAT u-käännöksen asetukset 1

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).



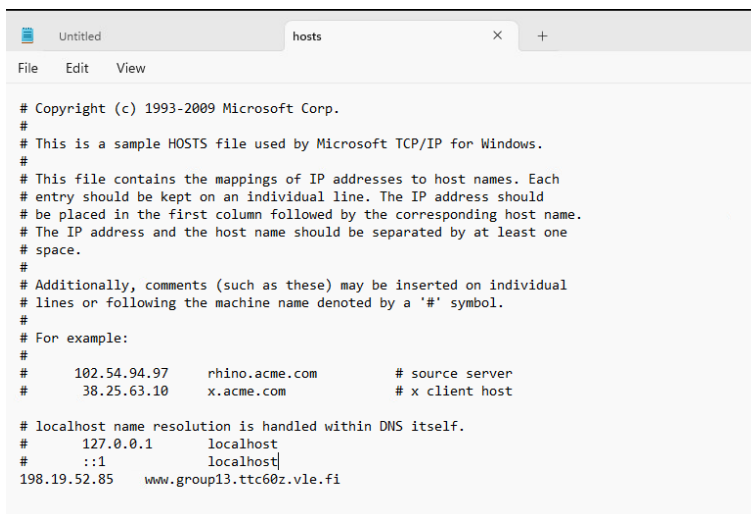
Kuvio 17. NAT u-käännöksen asetukset 2

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



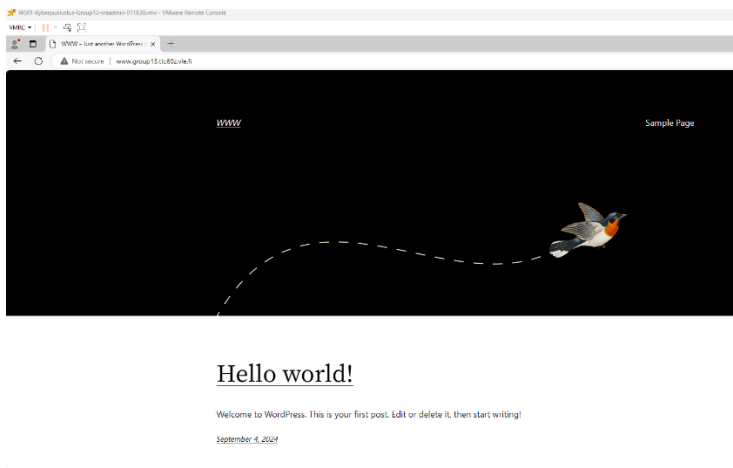
Kuvio 18. Hosts tiedosto

Hosts-tiedostoon lisäsimme alimmaksi riviksi IP-osoitteen ja osoitteen www.group13.ttc60z.vle.fi.
(Kuvio 19.)



Kuvio 19. Hosts-tiedoston sisältö

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



Kuvio 20. WordPress-sivusto WS01-työasemalla

5 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>

Šimonélytè, Miglè. 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/bap/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>