jamk

Tietoturvakontrollit – Labra 2

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Helmikuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuvat

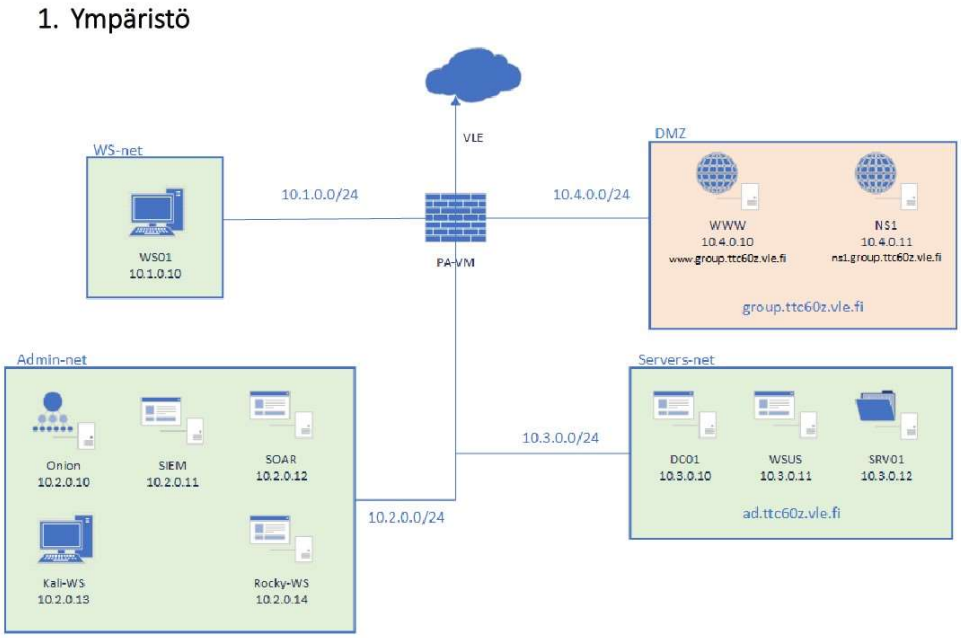
1 JOHDANTO

Dokumentaatio on osana Tietoturvakontrollit kurssin laboratorioharjoituksia. Lab2 laboratoriohar-joituksen tarkoituksena on tutustua PaloAlto:n turvallisuus sääntöihin ja NAT:iin tarkemmin. Har-joituksessa ryhmän tulee sallia DMZ:lla oleviin koneisiin pääsy internetistä (VLE rajapinta). Lisäksi WS-netistä pitää saada RDP (Remote Desktop Protocol) otettua Servers-netissä oleviin laitteisiin.

Lab2 aikana dokumentoidaan kuvankaappauksilla VLE ympäristössä toteutetut toimenpiteet, nii-den kuvaus, sekä mahdolliset ongelmatilanteet sekä niiden ratkaiseminen. Harjoituksen teoria-osuudessa käydään läpi teoria laboratorion virtuaalikoneen Palo Alto palomuurista, URL-filtering, NAT & Security Policies.

Lisäksi harjoituksessa ryhmän tulee selvittää/selittää:

1. Mikä ero on INTERZONE, INTRAZONE ja UNIVERSAL säännöillä
2. Mikä ero on ”Applicationilla” ja ”Servicellä” paloalton turvallisuus poliitikoissa?
3. Mitä turvallisuus poliitikoissa olevien profiilien (Security Policy Rule -> Actions -> Profile) avulla voidaan tehdä? Näiden kysymyksien vastaukset esitetään teoria osuudessa.



Kuva 1 VLE ympäristö

2 TEORIA

2.1 Palo Alto palomuuri

Palomuuri on tärkeä osa tietoverkon suojaamista. Kun sisäverkosta ollaan yhteydessä ulkoverkkoon, tarvitaan väliin palomuuri. Karkeasti jaettuna palomuurit voidaan jakaa joko laite- tai sovelluspalomuureihin tai sitten toimintaperiaatteen mukaisesti tilattomiin, tilallisiin ja seuraavan sukupolven eli palomuureihin (kolmannen sukupolven). Kolmannen sukupolven palomuurissa on uusia ominaisuuksia aikaisempien sukupolven palomuurien lisäksi, tehostamaan verkon uhkien tunnistamista sekä valvontaa. (Parkki 2019, 8.)

Järjestyksessään kolmannen teknologiasukupolven (NGFW) palomuurin periaate on yhdistelmä aikaisempien palomuurien tekniikoita, kuten osoitteenmuunnoksen (NAT), pakettisuodatuksen ja porttiosoitteen (PAT). Uusia ominaisuuksia ovat pakettien syvätarkastus ja tunkeutumisestojärjestelmä. (Parkki 2019, 10.)

OSI-mallissa kolmannen sukupolven palomuurit toimivat kerroksilla 4–7 (kuljetus-, istunto-, esitystapa ja sovelluskerroksella). Uudistus on tarpeen, koska vanhemmille palomuurisukupolville on tullut ongelmaksi web-pohjaiset haittaohjelmat sekä kohdennetut hyökkäykset sovelluskerrokseen. Haittaohjelmat kykenevät piilottamaan itsensä, esimerkiksi SSL-salauksen tai porttihyppelyn tai epästandardin portin käytön avulla. (Parkki 2019, 10.)

Kolmannen sukupolven palomuurilla voidaan tarkoittaa laitepalomuuria(fyysinen) tai sovelluspalomuuria. Harjoitustyössä käytämme yhdysvaltalaisen tietoturvayhtiön Palo Alto Networksin virtuaalista palomuuria. Yritys valmistaa pääasiassa palomuureja ja pilvipohjaisia tietoturvapalveluita. Palo Alton kolmannen sukupolven (Next-gen) palomuurit käyttävät PAN-OS ohjelmistoa. Palo Alton Nex-gen palomuurin ominaisuuksia ovat esimerkiksi sovellussuodatus/analyysi, käyttäjätunnistus, tunkeilijan havaitsemis- ja estojärjestelmät, TAP-liikenteenkaappauspiste, URL-suodatus (URL-Filtering) ja SSL-salauksen purku. (Parkki 2019, 14.)

2.2 URL Filtering

URL-suodatuksen (URL-Filtering) avulla voidaan hallita paitsi verkkokäyttöä myös sitä, miten käyttäjät ovat vuorovaikutuksessa verkkosisällön kanssa (URL Filtering Best Practices 2023).

Palo Alto Networksin URL-suodatus on tilauspohjainen ominaisuus, joka suojaa verkkopohjaisilta uhilta ja antaa yksinkertaisen tavan seurata ja hallita verkkotoimintaa. Käyttäjä voi luoda sallimissäännöt sovelluksille, joihin luottaa. Sekä tehdä URL-kategoriat, jotka luokittelevat haitallisen ja hyväksikäyttävän sisällön ja estävät ne. URL-suodatus opastaa ja auttaa vähentämään altistumista verkkopohjaisille uhille rajoittamatta käyttäjien pääsyä tarvitsemaansa verkkosisältöön. (URL Filtering Best Practices 2023.)

URL suodatusta luodessa ensin tunnistetaan sovellukset, jotka halutaan sallia ja sitten luodaan sovelluksen sallimissäännöt osana internet-yhdyskäytävän suojauskäytännön rakentamista (Internet Gateway security policy). Kun sallitut sovellukset on tunnistettu, voidaan käyttää URL-suodatusta hallitsemaan ja suojaamaan kaikkea verkkotoimintaa, joka ei ole sallittujen joukossa. URL-suodatuksen avulla voi sallia, estää, varoittaa, vaatia salasanaa tai hälyttää. (URL Filtering Best Practices 2023.)

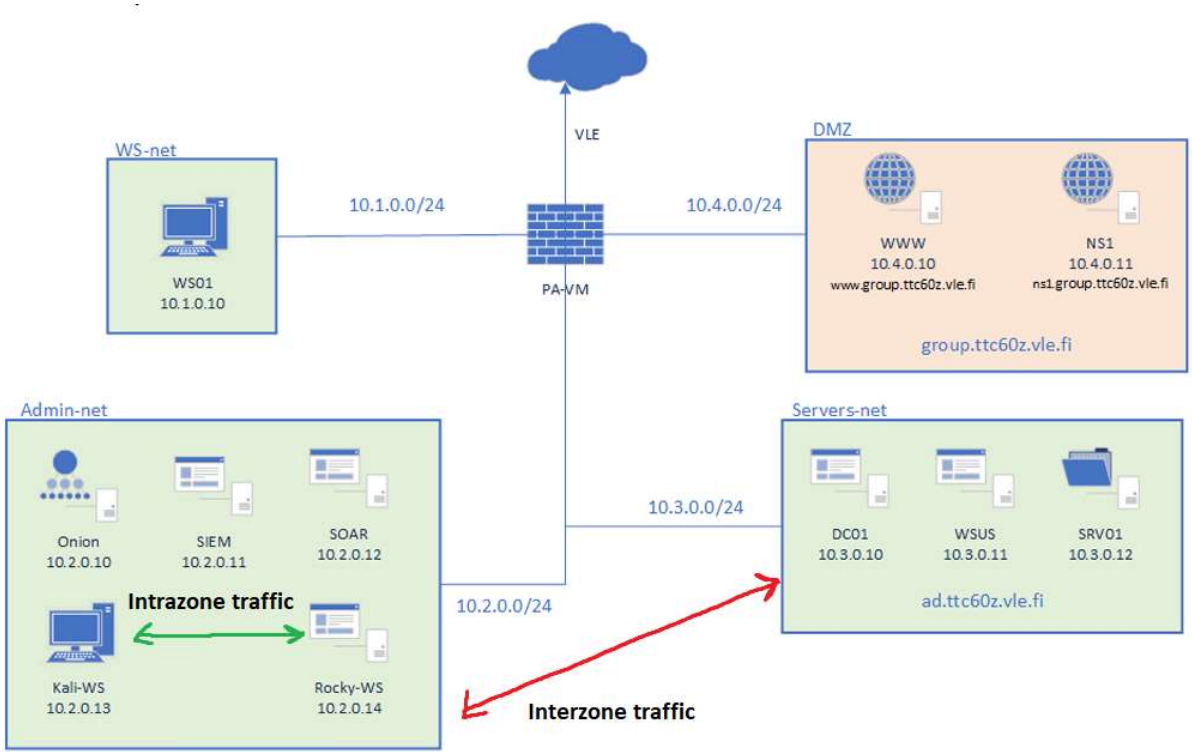
2.3 NAT

NAT (Network Address Translation) on tekniikka, joka mahdollistaa yhden julkisen IP-osoitteen käytön useilla verkkolaitteilla. Reititin vastaa NAT:ista ja ohjaa verkon välisen liikenteen oikeaan osoitteeseen. Useimmat NAT-toteutukset ovat Port Address Translation (PAT) -malleja, joissa NAT-laite muuntaa datapaketin käyttämän portin ja IP-osoitteen. NAT lisää tietoturvaa internetissä, sillä se estää suoran yhteyden NAT:in takana oleviin laitteisiin. Tämä kuitenkin aiheuttaa ongelman palvelinten pitämisessä, sillä ulkopuoliset tahot eivät pääse suoraan NAT:in takana oleviin laitteisiin. Tämän ongelman voi kuitenkin kiertää käyttämällä porttiohjausta. NAT:ia käytetään myös sen takia, että nykyinen IPv4-protokolla tarjoaa rajallisesti IP-osoitteita, joten NAT mahdollistaa verkkoon liittämisen useilla laitteilla ilman ylimääräisiä IP-osoitteita. (Blanchet 2007, 6-7)

2.4 Security Policies

Security Policy eli turvallisuuspolitiikka määrittelee säännökset ja toimintatavat, joita organisaation välineitä ja resursseja käyttävän yksilön on noudatettava. Dokumentissa määritellään mitä pitää ja mitä ei pidä tehdä, sekä mitä kenelläkin on oikeus käyttää ja seuraukset määräysten noudattamatta jättämisestä. Säännösten tavoitteena on tietoturvariskien vähentäminen sekä kertoa toimintatavat mahdollisen tapahtuman jälkeen. Selkeästi dokumentoitu tietoturvapolitiikka on vaatimuksena organisaatioille, joiden täytyy täyttää tietyt määräykset tai standardit, esimerkiksi GDPR ja ISO. (Arkvik 2021)

2.5 Mikä ero on INTERZONE, INTRAZONE ja UNIVERSAL säännöillä



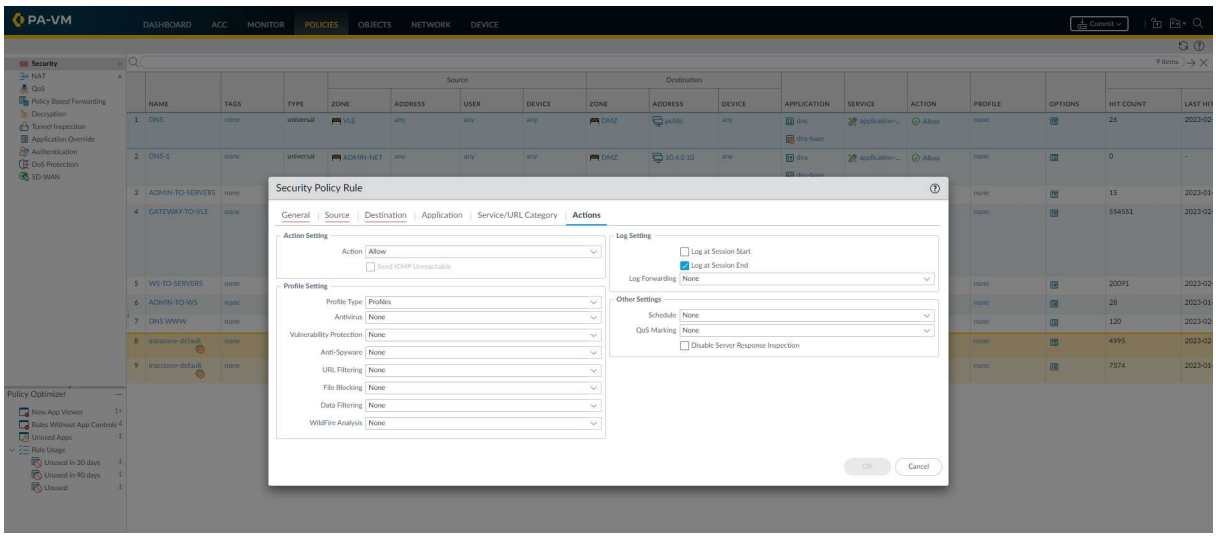
Kuva 2 Intrazone & Interzone traffic

Paloaltossa on olemassa security zoneja joidenka avulla pystytään hallitsemaan ja turvaamaan verkkoja. Esimerkiksi järjestelmät, jotka vaativat samankaltaisia suojauksia voidaan laittaa samaan security zoneen. Intrazone, Interzone ja Universal ovat valmiita sääntöjä security zoneille paloaltossa. Intrazone sallii liikenteen vain zonen sisällä olevien järjestelmien kesken. Interzone taas sallii security zonejen välisten järjestelmien liikenteen, mutta ei security zonejen sisällä niin kuin Intrazone. Universal pitää sisällään molemmat Intrazone ja Interzone säännöt. (What are Universal, Intrazone and Interzone Rules? 2019.)

2.6 Mikä ero on ”Applicationilla” ja ”Servicellä” paloalton turvallisuus poliitikoissa?

Paloalton turvallisuus politiikoissa ”Service” kohtaan voidaan määritellä portit, jotka halutaan auki, jotta saataisiin jokin sovellus kuten vaikka RDP toimimaan. Applicationit ovat paloalton määrittelemiä ja niihin sisältyy tiedetyt portit ja protokollat, jota sovellus käyttää. Jos esimerkiksi valitaan application kohtaan RDP ja jätetään services kohta defaultiksi kulkee RDP liikenne ainoastaan sen default portista TCP/3389. Jos taas valitaan services: any ja applicationiin RDP sallitaan RDP:n liikkenne kaikista porteista. (What Are Applications and Services? 2020.)

2.7 Mitä turvallisuus poliitikoissa olevien profiilien (Security Policy Rule -> Actions -> Profile) avulla voidaan tehdä?



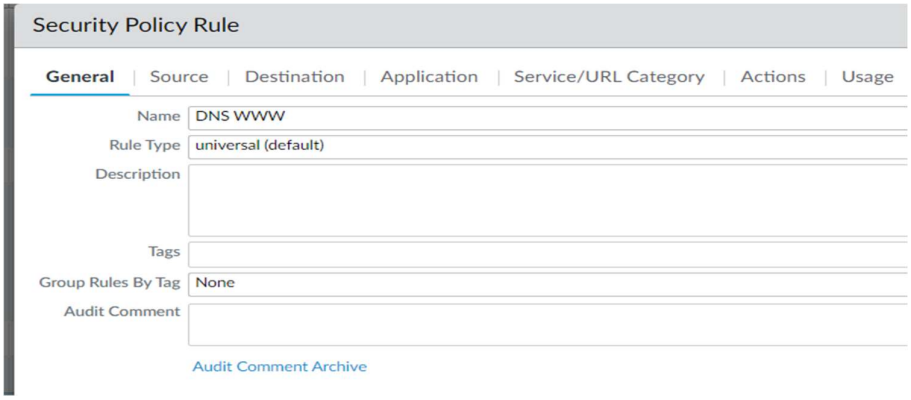
Kuva 3 Security Policy Rule - Action - Profile

Turvallisuus politiikoissa olevat profiilit auttavat, kun halutaan esimerkiksi sallia jonkun sovelluksen liikenne, mutta halutaan tarkemmin scannata sovelluksen sallittua liikennettä uhkilta. Paloaltossa on valmiiksi oletuksena profiileita, joita pystytään käyttämään. Esitetty kuvassa 3. Esimerkiksi asetus Data Filtering Profiles estää sensitiivisen tiedon kuten henkilötunnuksen ja luottokortin tietojen lähdön verkosta. (Security Profiles 2023.)

3 DOKUMENTOINTI

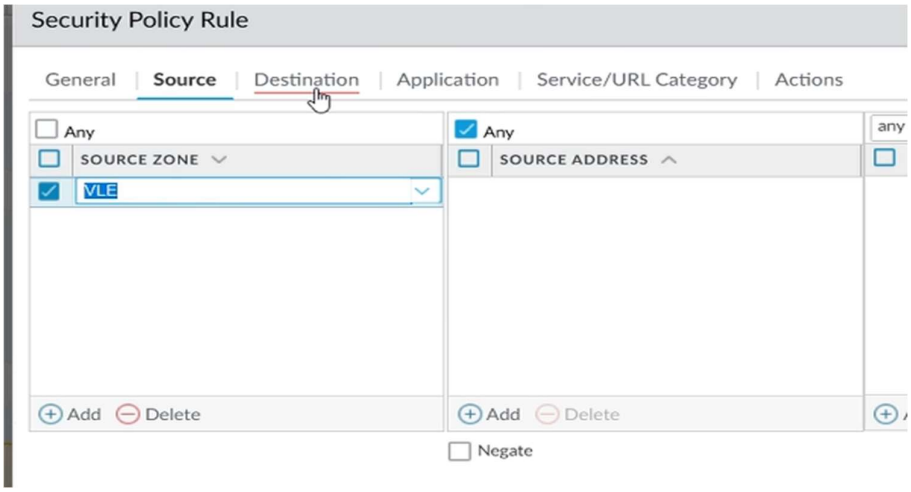
3.1 Lab2 - Paloalto Firewall Rules for Public Services

Lab 2 oli todella suoraviivaiset ohjeet, jota noudattamalla meille ei tullut ongelmia. Aloitimme palomuurin turvallisuus politiikan muokkauksen menemällä Policies -> Security -> Add. Annoimme General kohtaan nimeksi DNS WWW. Esitetty kuvassa 4.



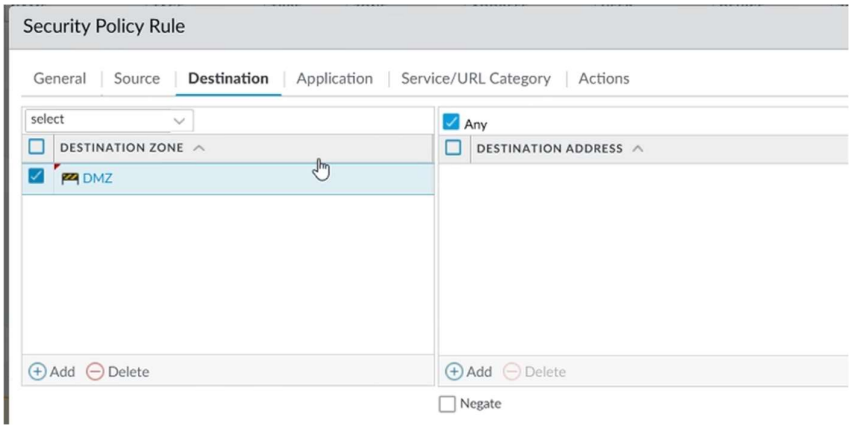
Kuva 4 General

Source välilehdellä valittiin VLE (internet). Esitetty kuvassa 5.



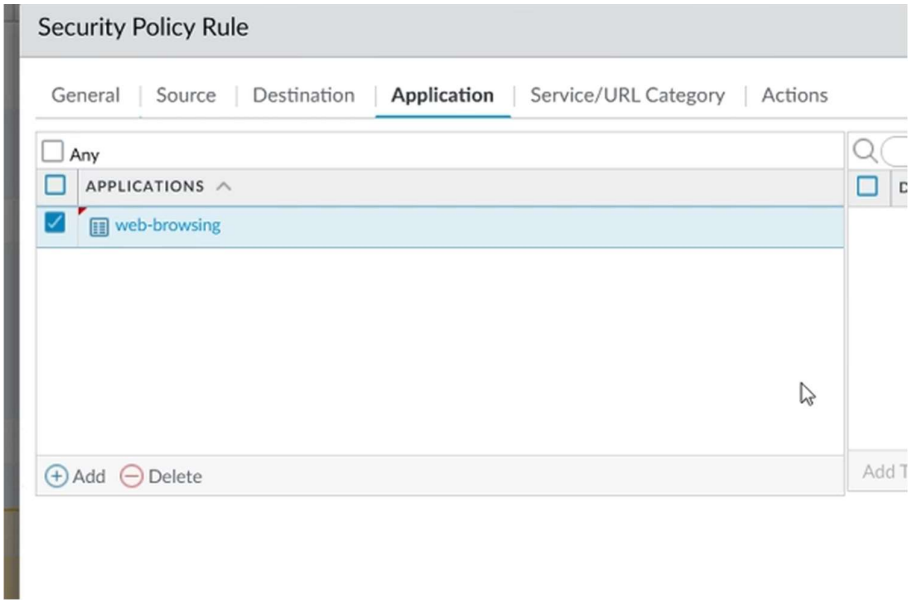
Kuva 5 Source

Destination välilehdellä valittiin DMZ. Esitetty kuvassa 6.



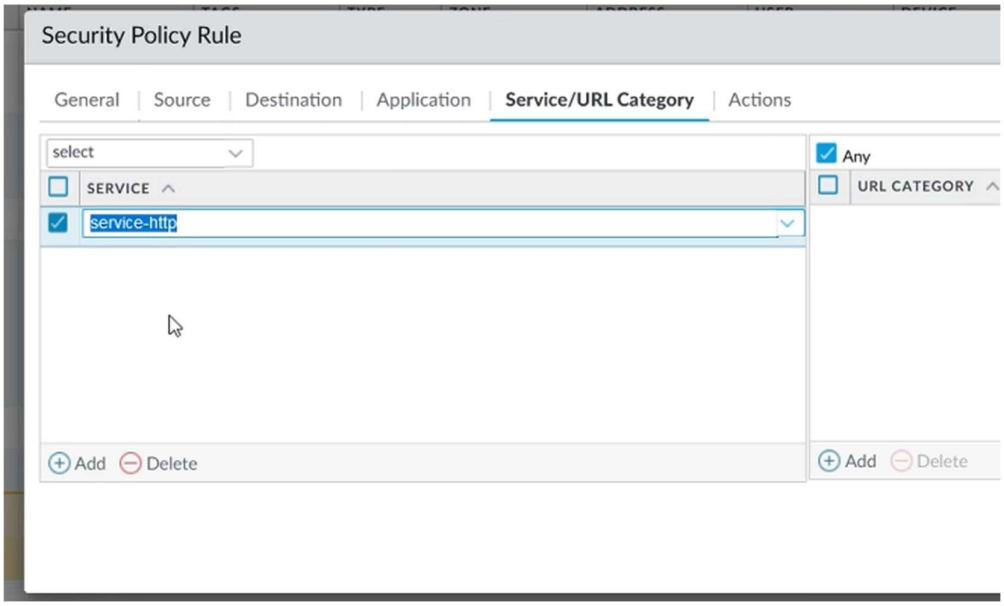
Kuva 6 Destination

Application välilehden kohtaan web-browsing. Esitetty kuvassa 7.



Kuva 7 Application

Service/URL Category välilehdelle service-http painetaan ok ja commitetaan muutokset. Esitetty kuvassa 8.



Kuva 8 Service

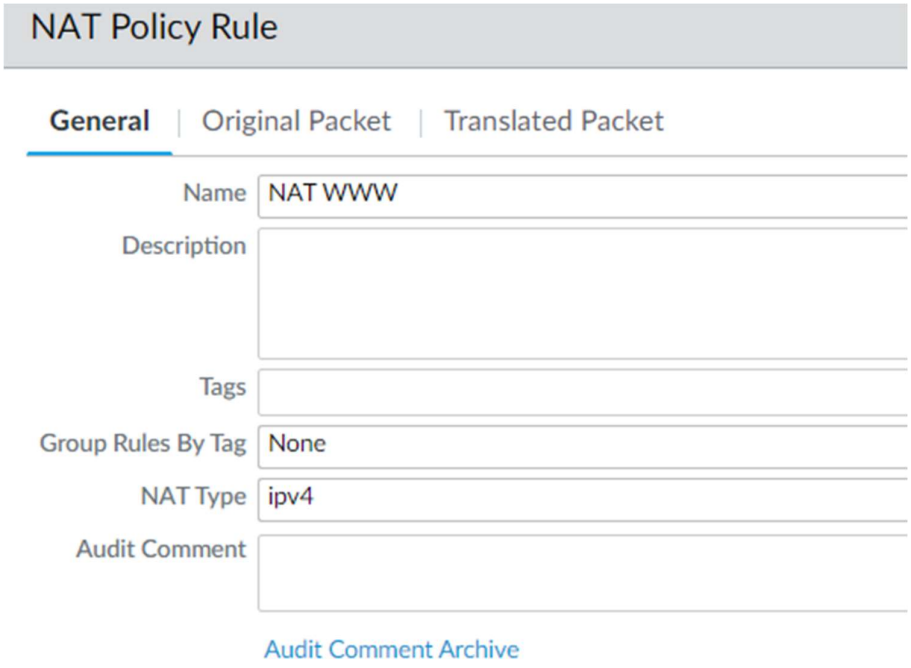
Tarkistettiin, menikö commit läpi ja tuliko DNS WWW Policies ->security listaan. Esitetty kuvassa 9.

1	DNS	none	universal	VLE	any	any	any	DMZ	public	any	dns dns-base	application-...	Allow
2	DNS-1	none	universal	ADMIN-NET	any	any	any	DMZ	10.4.0.10	any	dns dns-base	application-...	Allow
3	ADMIN-TO-SERVERS	none	universal	ADMIN-NET	any	any	any	SERVERS-NET	any	any	any	application-...	Allow
4	GATEWAY-TO-VLE	none	universal	ADMIN-NET DMZ SERVERS-NET WS-NET	any	any	any	VLE	any	any	any	any	Allow
5	WS-TO-SERVERS	none	universal	WS-NET	any	any	any	SERVERS-NET	any	any	any	any	Allow
6	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	any	any	Allow
7	DNS WWW	none	universal	VLE	any	any	any	DMZ	any	any	web-browsing	service-http	Allow
8	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Kuva 9 policies

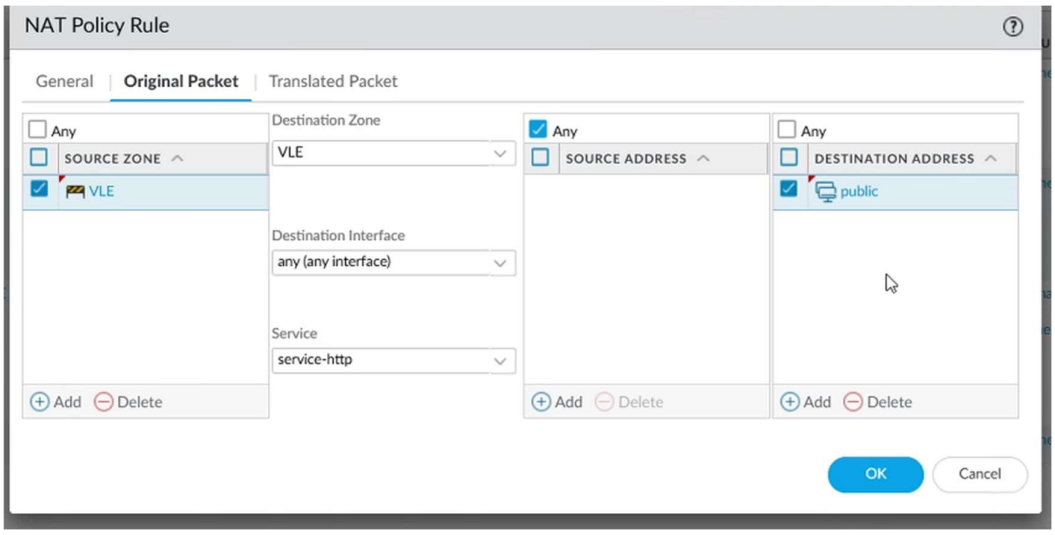
3.2 Nat säännöt sekä testaus

Mennään kohtaan Policies -> NAT ->add. Annetaan nimeksi NAT WWW, esitetty kuvassa 10.



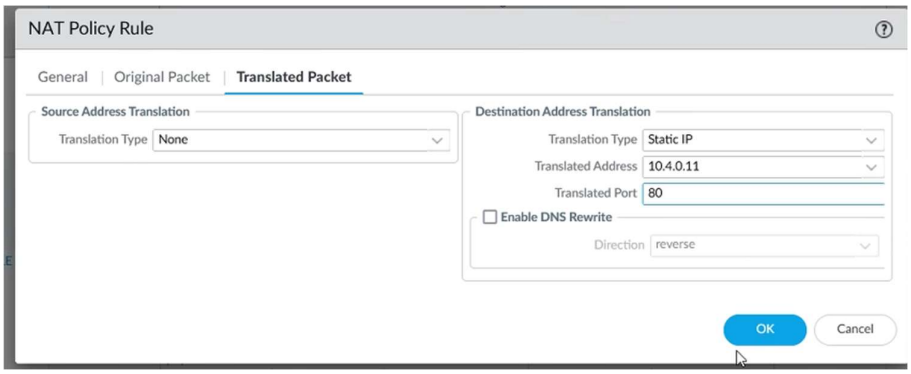
Kuva 10 NAT policy

Orginal Packet välilehdeltä: Source zone VLE, Destination zone VLE, Source Address any laatikkoon rasti ja Destination address public laatikkoon rasti. Esitetty kuvassa 11.



Kuva 11 Original_packet

Translated Packet välilehdeltä: Source Address Translation kohtaan: Translation type None, Destination Address Translation kohtaan Translation type static IP addres 10.4.0.11 (meidän WWW koneen IP) ja portti 80 (yleinen http portti mutta siihen voi pistää minkävain) ja painetaan ok, sekä commitetaan muutokset. Esitetty kuvassa 12.



Kuva 12 Translated

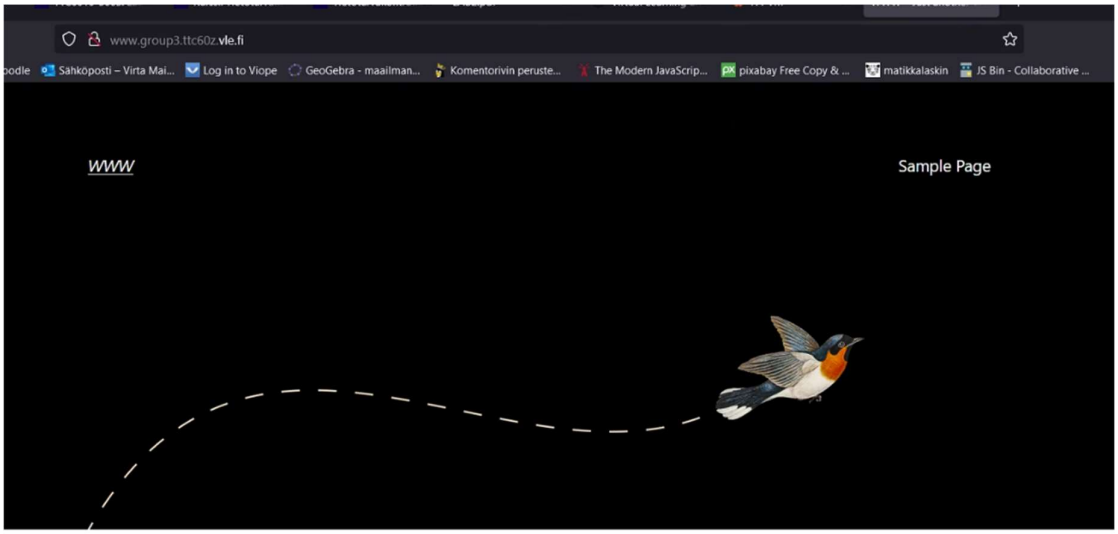
Katsottiin, että commitukset meni läpi, sekä Policies -> NAT sivulta oli tullut NAT WWW sääntö voimaan. Esitetty kuvassa 13.

Kuva 13 NAT_sääntö

Varmistettiin, että wordpress kontti on päällä avaamalla VLE-ympäristöstä www kone ja ajamalla komento: docker ps –a. Näytti olevan. Esitetty kuvassa 14.

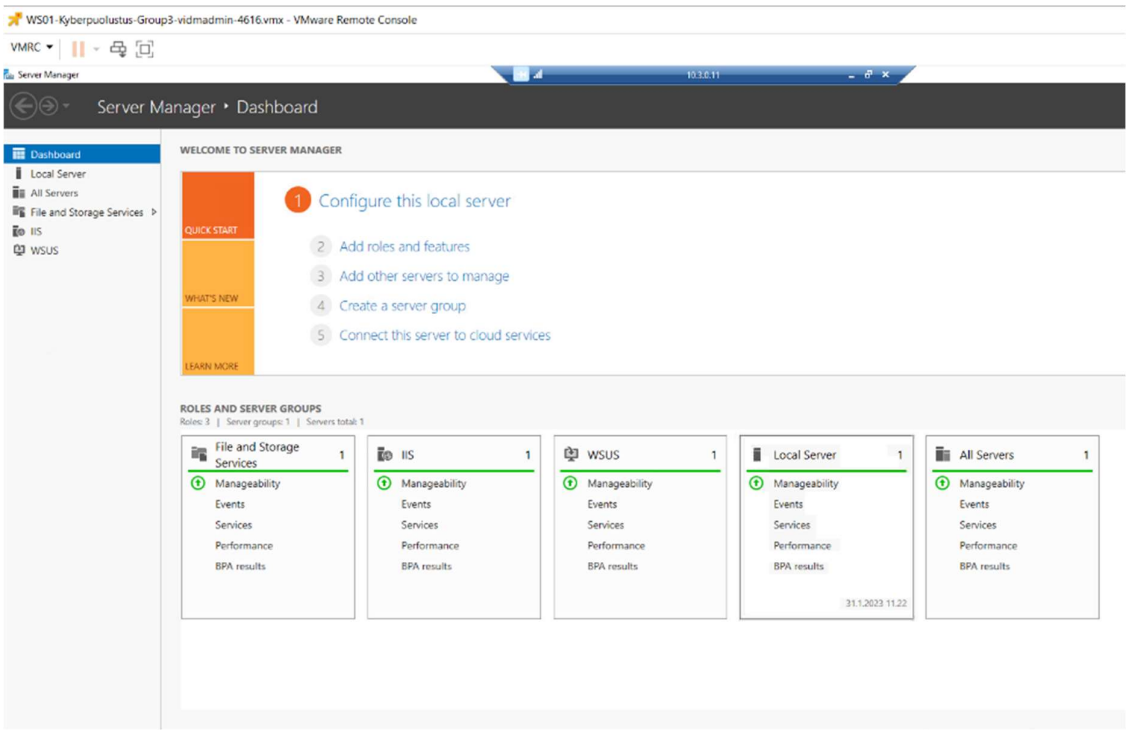
Kuva 14 kontti_ylhäällä

Kokeiltiin seuraavaksi toimivuutta menemällä osoitteeseen http://www.group3.ttc60z.vle.fi/ Esitetty kuvassa 15.



Kuva 15 sivusto

Vielä kokeiltiin etäyhteyden ottamista WS-netistä -> Servers netin koneeseen ja onnistui hyvin. Esitetty kuvassa 16.



Kuva 16 RDP

4 POHDINTA

Harjoitustyön tavoitteena oli tutustua ryhmätyönä VLE-ympäristöön toteutetun Palo Alto palomuurin turvallisuus sääntöihin sekä NAT:iin. Ryhmä salli harjoituksessa DMZ:lla oleviin koneisiin pääsyn internetistä. Lisäksi harjoituksen tavoitteena oli saada WS-netistä RDP (Remote Desktop Protocol) otettua servers-netissä oleviin laitteisiin.

Harjoitustyössä käytiin läpi teoria laboratorion virtuaalikoneen Palo Alto palomuurista, URL-filtering:stä, NAT:ista & turvallisuus säännöistä (Security Policies). Lisäksi vastattiin kysymyksiin: Mikä ero on INTERZONE, INTRAZONE ja UNIVERSAL säännöillä, mikä ero on ”Applicationilla” ja ”Servicellä” paloalton turvallisuus poliitikoissa, ja mitä turvallisuus poliitikoissa olevien profiilien (Security Policy Rule -> Actions -> Profile) avulla.

Ensimmäisen harjoitustyön tekemiseen verrattuna, Palo Alton käyttöliittymä tuntui toisessa harjoituksessa ryhmän jäsenien mielestä paljon selkeämmältä. Harjoitustyön aloittaminen oli ohjeistettu hyvin ja se oli suhteellisen helppo toteuttaa ongelmitta, eikä sen tekemiseen mennyt ajallisesti kauan aikaa. Ryhmä jopa hieman yllättyi harjoituksen yksinkertaisuudesta verraten ensimmäiseen harjoitukseen, joka tuntui ongelmatilanteiden ratkaisun takia työläämmältä.

Kokonaisuutena harjoitustyö syvensi ymmärrystä Palo Alton graafisen käyttöliittymän toimintaan ja loogisuuteen, sekä opetti turvallisuus sääntöjen konfiguroinnin perusteita. Teoriaosuudet olivat mielenkiintoisia ja ne avasivat ymmärrystä erityisesti esitettyjen lisäkysymyksien teorian osalta.

LÄHTEET

Arkvik, I. 2021. What is an IT Security Policy? Visma verkkosivut. Viitattu 4.2.2023. https://www.visma.com/blog/what-is-an-it-security-policy-2/

Blanchet, M. 2007. Migrating to IPv6. John Wiley & Sons Ltd.

Parkki, J. 2019. Palo Alto PA5060 palomuurin ominaisuudet ja käyttöönotto. Opinnäytetyö, AMK. Tampereen Ammattikorkeakoulu, Tieto- ja viestintätekniikan tutkinto-ohjelma. Viitattu 4.2.2023. https://www.theseus.fi/bitstream/handle/10024/167797/Parkki_Jouni.pdf?sequence=2

Security Profiles. 2023. Palo Alto verkkosivut. Viitattu 4.2.2023. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-profiles

URL Filtering Best Practices. 2023. Palo Alto verkkosivut. Viitattu 4.2.2023. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/url-filtering/url-filtering-best-practices

What Are Applications and Services? 2020. Palo Alto verkkosivut. Viitattu 4.2.2023. https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508

What are Universal, Intrazone and Interzone Rules? 2019. Palo Alto verkkosivut. Viitattu 4.2.2023. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC