



Tietoturvakontrollit Labra 2

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Jukka Virtanen

Harjoitustyö

Tammikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

Sisältö

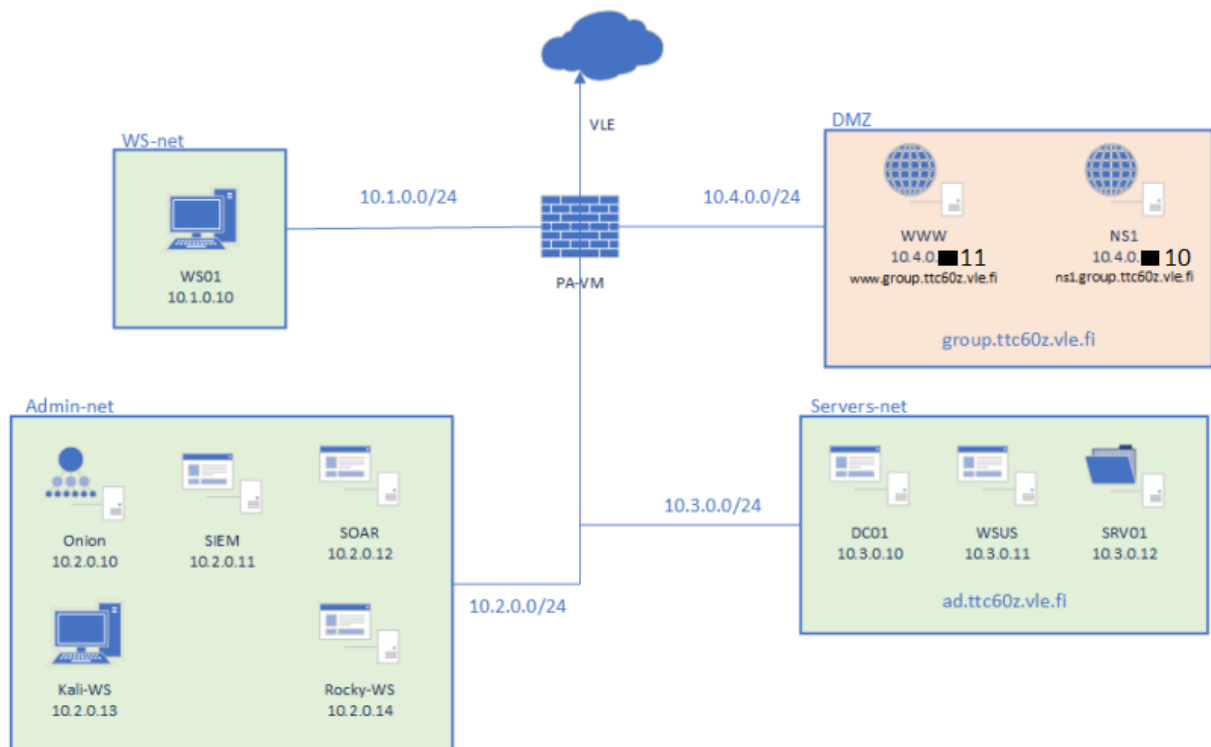
1	Johdanto	3
2	Teoria.....	4
2.1	Palomuuuri	4
2.2	NAT	5
2.2.1	U-turn NAT	5
3	Toteutus	5
3.1	Yhteys VLE:stä DMZ alueelle	5
3.2	RDP WS-netistä Servers-netiin	7
3.3	U-TURN-NAT.....	9
3.4	Objektit.....	12
4	Selvitykset	12
4.1	Eroavaisuudet sääntötyypeissä.....	12
4.2	Eroavaisuudet Applicationilla ja Servicellä PaloAltossa	13
4.3	Turvallisuuspoliitikoissa olevat profiilit.....	13
5	Pohdinta.....	14
	Lähteet	16

Kuviot

Kuvio 1.	VLE-ympäristö	3
Kuvio 2.	VLE-TO-DMZ	6
Kuvio 3.	WWW-NAT sääntö	7
Kuvio 4.	Toimiva ryhmän 3 sivu	7
Kuvio 5.	RDP-WSNET-TO-SERVERS.....	8
Kuvio 6.	Toimiva RDP-yhteys Workstationilta SRV01:een	9
Kuvio 7.	U-TURN security policy.....	10
Kuvio 8.	UTURN NAT policy, INTERNAL-ACCESS	10
Kuvio 9.	Toimiva U-turn varmennettuna WS01 koneelta	11
Kuvio 10.	Objektit.....	12
Kuvio 11.	Security Profile Group -näkyvä	14

1 Johdanto

Tietoturvakontrollien toisessa labrassa on tavoitteena tutustua Palo Alton NATtiin sekä turvallisuussääntöihin tarkemmin. Toivotussa tilanteessa DMZ:ssa oleviin koneisiin pääsee internetin kautta. Servers-netissä oleviin laitteisiin pitäisi myös saada RDP-yhteys WS-netissä olevalta koneelta. Palo Altoon konfiguroidaan U-Turn NAT harjoitusmielessä. Labra suoritetaan VLE-ympäristössä (ks. Kuvio 1) pääasiassa Palo Alton palomuurilla mutta myös WS01 koneella otetaan RDP-yhteys Servers-netin laitteeseen sekä kokeillaan U-Turn NATin toimivuus. Tämä raportti sisältää teorian, toteutuksen, selvitykset ja pohdinnan ryhmän kolme osalta.



Kuvio 1. VLE-ympäristö

2 Teoria

2.1 Palomuuuri

Tietokoneverkon palomuuuri tarjoaa suojaa verkon rajalla valvomalla verkkoliikenteessä saapuvia ja lähteviä datapaketteja haittaohjelmien ja poikkeavuuksien varalta. Palomuuuri suodattaa liikennettä, kun se yrittää tulla verkkoon ja poistua verkosta, toisin kuin virustorjuntaohjelmisto, joka skannaa verkon laitteita ja tallennusjärjestelmiä suojauksen läpi tunkeutuneiden uhkien varalta. (Definition: What Is a Firewall?)

Palomuuuri on suunniteltu noudattamaan ennalta määritettyjä turvallisuussääntöjä, joiden avulla määritetään, mitä verkkoon sallitaan ja mitä estetään. (Definition: What Is a Firewall?)

Palomuuuri voidaan toimittaa laitteistolaitteena, ohjelmistona tai SaaS-palveluna (Software as a Service) riippuen siitä, missä se otetaan käyttöön ja mihin tarkoitukseen se on tarkoitettu.

Palomuuureja on viisi päätyyppiä niiden toimintatavan mukaan:

- Tilaton eli pakettisuodatusta käyttävä palomuuuri (stateless or packet filtering firewall)
- Tilatarkkailupalomuuuri (stateful inspection firewall)
- Piiritason yhdyskäytävä (circuit-level gateway)
- Sovellustason yhdyskäytävä (application-level gateway)
- Seuraavan sukupolven palomuuuri (NGFW) (next-generation firewall (NGFW))

(Definition: What Is a Firewall?)

Periaatteessa palomuuureissa on kahdenlaisia toimitusmenetelmiä: ohjelmistoja ja laitteistoja.

Yleensä ohjelmistopalomuuuri suojaa isäntäkoneen, kuten tietokoneen tai laitteen, ja laitteistopalomuuuri suojaa verkkoa. (What Is A Software Firewall vs A Hardware Firewall?)

Lisäerona voidaan todeta, että tietokoneverkon laitteistopalomuuuri käyttää ohjelmistoa, joka on asennettu laitteistolaitteeseen, kun taas tietokoneverkon ohjelmistopalomuuuri käyttää tietokonetta laitteistolaitteena, jossa se toimii. Tästä syystä ohjelmistopalomuuureista käytetään

usein nimitystä "isäntäpalomuri" ja laitteistopalomureista nimitystä "verkkopalomuri". (What Is A Software Firewall vs A Hardware Firewall?)

2.2 NAT

NAT (Network Address Translation) mahdollistaa yksityisten IP-osoitteiden, jotka eivät ole reititettävällä kerroksella, kääntämisen yhdeksi tai useammaksi julkiseksi IPv4-osoitteeksi. Tämä menetelmä ei ainoastaan salaa todelliset IP-osoitteet julkisesta verkosta, vaan myös säästää reititettäviä osoitteita. Kun käytetään yksityisiä IP-osoitteita sisäverkossa, NAT on välttämätöntä niiden kääntämiseksi julkisiksi osoitteiksi, jotta paketit voidaan reitittää julkisissa verkoissa. PAN-OS palomuurissa luodaan NAT-sääntöjä (policy), jotka kertovat palomuurille mitkä pakettien osoitteet ja portit tarvitsevat käännöstä, ja mitkä käännetyt osoitteet ja portit ovat. (Paloalto NAT 2024.)

2.2.1 U-turn NAT

U-turnia hyödynnetään, kun sisäverkon käyttäjä haluaa käyttää sisäverkon palveluita, kuten esimerkiksi palvelinta, käyttäen palvelimen julkista osoitetta. Esimerkkinä käyttötilanteesta voisi olla WWW-palvelimen sijainti DMZ-alueella. Kun U-turn NAT otetaan käyttöön, on välttämätöntä konfiguroida sekä NAT- sääntö että turvallisuus (security) sääntö palomuurissa. (Paloalto U-turn NAT 2023.)

3 Toteutus

3.1 Yhteys VLE:stä DMZ alueelle

Aloitimme labran tekemisen lisäämällä VLE-TO-DMZ säännön (ks. kuvio 2). *Security policy* määrittää millä säännöillä liikenne läpäisee palomuurin. Tähän löytyi suoraviivainen ohje labran ohjeista, jota seurailimme. Sourceksi tehtävänannon mukaisesti VLE ja destination alueeksi DMZ. Kohdeosoitteeksi tuli palomuurin julkinen IP-osoite. Lupa annettiin Application tasolla *web-browsingille* ja palvelutasolla *service-http:lle*. Tässä vaiheessa yhteyttä ei saatu vielä toimimaan.

Security policy

Name: VLE-TO-DMZ

Type: universal

Source zone: VLE

Destination zone: DMZ

Destination address: public (palomuurin julkinen ip)

Application: web-browsing

service: service-http

5	ADMIN-TO-WS	none	universal	ADMIN-NET	any	any	any	WS-NET	any	any	any	any	Allow	none		0	-
6	VLE-TO-DMZ	none	universal	VLE	any	any	any	DMZ	public	any	web-browsing	service-http	Allow	none		0	-

Kuvio 2. VLE-TO-DMZ

Seuraavaksi laadimme NAT:lle WWW- säännön (ks. kuvio 3). Sekä Source- että Destination-zoneksi NAT:iin tuli VLE. Kohdeosoitteeksi palomuurin julkinen osoite. Sallittu service on *service-http*. Translated packet kohdassa liikenne ohjattiin WWW serverille porttiin 80. WWW-PRIVA objektin takaa löytyy IP 10.4.0.11.

Nat Policy

Name: WWW

Original packet

Source zone: VLE

Destination zone: VLE

Destination interface: any

Destination address: public (palomuurin julkinen ip)

Service: service-http

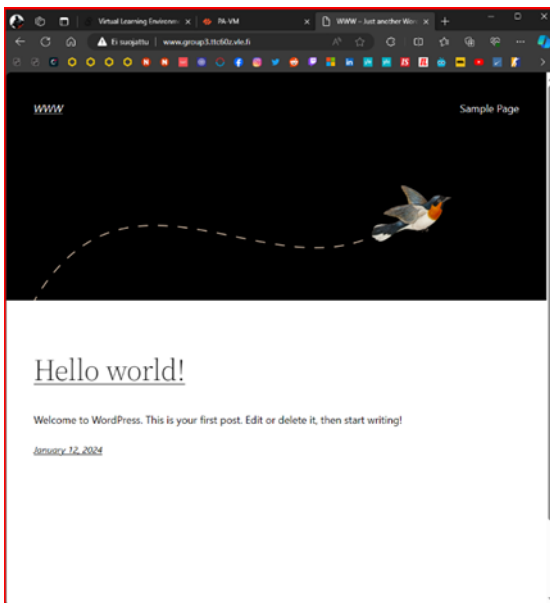
Translated packet

destination translation: destination-translation, address WWW-PRIVA (www-serverin ip)

5	WWW	none	VLE	VLE	any	any	public	service-http	none	destination-translation address: WWW-PRIVA port: 80	45	2024-01-2
---	-----	------	-----	-----	-----	-----	--------	--------------	------	---	----	-----------

Kuvio 3. WWW-NAT sääntö

Kuviossa 4. todennetaan yhteyden toimiminen käyttäjän omalta koneelta eli VLE:n läpi ryhmän nettisivulle.



Kuvio 4. Toimiva ryhmän 3 sivu

3.2 RDP WS-netistä Servers-nettiin

Tehtävänantona oli luoda WS-netistä rdp-yhteys servers-nettiin. Labrassa 1. RDP-sääntö oltiin luotu VPN:lle. Lähdimme rakentamaan tätä sääntöä samalta pohjalta. (ks. kuvio 5)

Security policy

Name: RDP-WSNET-TO-SERVERS


















Source zone: WS-Net

Type: interzone (liikenne sallittu vain valittujen alueiden välille)

Destination zone: Servers-net

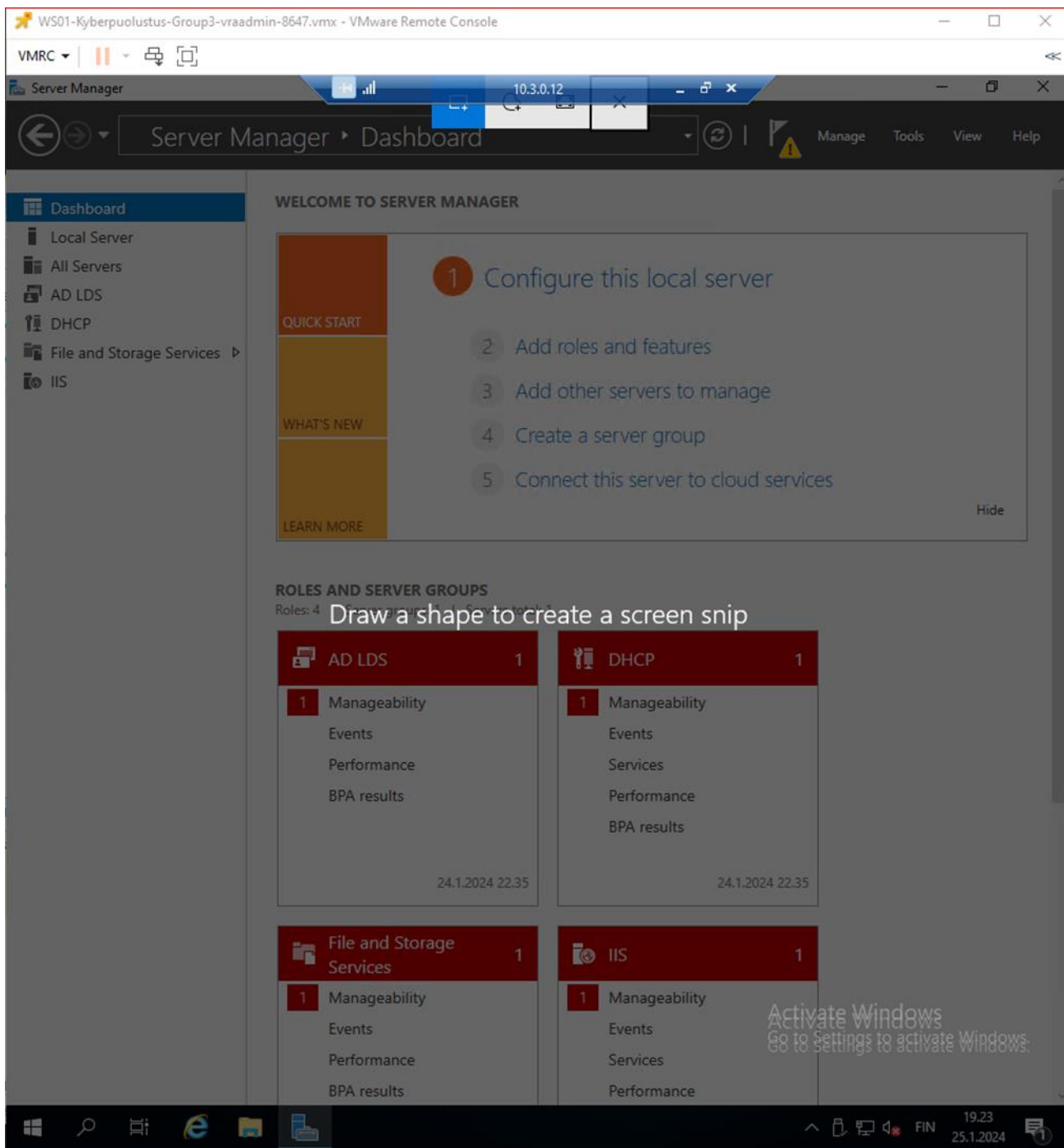
Application: ms-rdp

Service: application-default

4	WS-TO-SERVERS	none	universal	 WS-NET	any	any	any	 SERVERS-NET	any	any	any	any		Allow	none		21929	2024-0		
5	ADMIN-TO-WS	none	universal	 ADMIN-NET	any	any	any	 WS-NET	any	any	any	any		Allow	none		0	-		
6	VLE-TO-DMZ	none	universal	 VLE	any	any	any	 DMZ	 public	any		web-browsing		service-http		Allow	none		85	2024-0
7	VPN-SSH	none	universal	 VPN-ZONE	any	any	any	any	any	any		ssh		application...		Allow	none		31	2024-0
8	VPN-RDP	none	universal	 VPN-ZONE	any	any	any	any	any	any		ms-rdp		application...		Allow	none		55	2024-0
9	VPN-INTERNET	none	universal	 VPN-ZONE	any	any	any	 VLE	any	any		dns		application...		Allow	none		530	2024-0
												dns-base								
												ms-teams								
												web-browsing								
10	RDP-WSNET-TO-SER...	none	interzone	 WS-NET	any	any	any	 SERVERS-NET	any	any		ms-rdp		application...		Allow	none		20	2024-0

Kuvio 5. RDP-WSNET-TO-SERVERS

Rdp-sääntöä kokeilimme sekä WS-TO-SERVERS säännön ollessa päällä ja pois. Alkuun type oli any, mutta tehtävänannon mukaisesti rajasimme liikenteen lopulta interzone-typellä vain Ws-netin ja Servers-Netin välille. Lopuksi todensimme yhteyden SRV01:een WS01:ltä (ks kuvio 6.).



Kuvio 6. Toimiva RDP-yhteys Workstationilta SRV01:een

3.3 U-TURN-NAT

U-Turn security policy

Name: UTURN-WEB-ACCESS

Type: universal

Source zone: WS-net

Destination zone: DMZ

Application: web-browsing

Service: service-http, service-https

11	UTURN-WEB-ACCE...	none	universal	WS-NET	any	any	any	DMZ	any	any	web-browsing	service-http service-https	Allow	none		110
----	-------------------	------	-----------	--------	-----	-----	-----	-----	-----	-----	--------------	-------------------------------	-------	------	--	-----

Kuvio 7. U-TURN security policy

U-Turn NAT policy

Name: INTERNAL-ACCESS (ks. kuvio 8)

Original packet:

Source zone: WS-NET

Destination zone: VLE

Destination address: public (palomuurin julkinen osoite)

Translated packet:

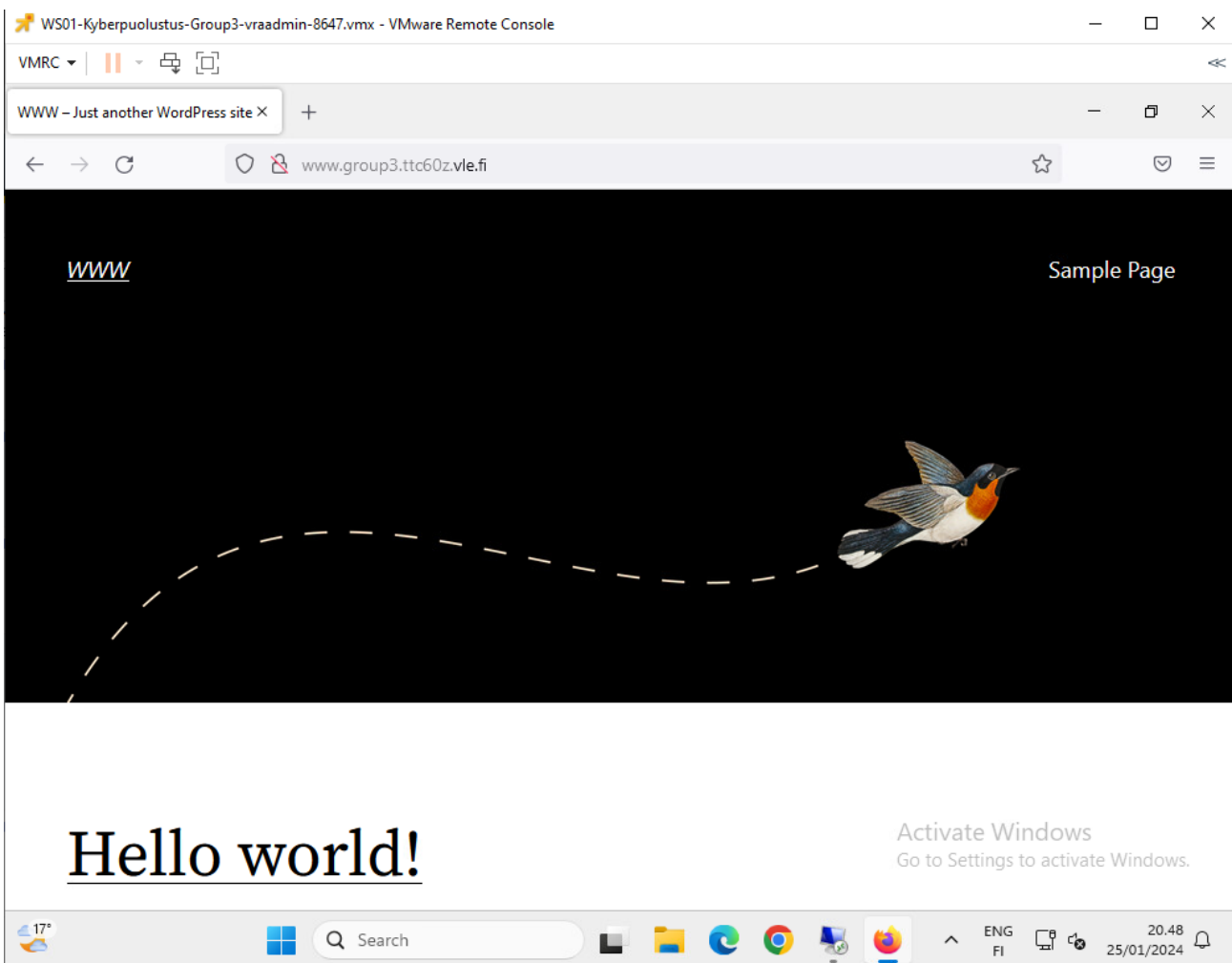
Destination translation: destination-translation WWW-PRIVA (www-palvelimen osoite)

	NAME	TAGS	Original Packet					Translated Packet			Rule Usage			
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT	LAST HIT	FIRST HIT	MODIFIED
1	INTERNAL-ACCESS	none	WS-NET	VLE	any	any	public	any	none	destination-translation address: WWW-PRIVA	160	2024-01-25 19:55:36	2024-01-25 18:58:28	2024-01-25
2	DNS	none	VLE	VLE	any	any	public	DNS	none	destination-translation address: 10.4.0.10/32 port: 53	0	-	-	2022-08
3	DNS-1	none	VLE	VLE	any	any	public	DNSUDP	none	destination-translation address: 10.4.0.10/32 port: 53	33	2024-01-25 19:53:55	2024-01-16 19:09:51	2022-08
4	ACCESS-TO-VLE	none	ADMIN-NET DMZ SERVERS-NET VPN-ZONE WS-NET	VLE	ethernet1/5	any	any	any	dynamic-ip-and-port ethernet1/5	none	414131	2024-01-25 19:55:42	2024-01-12 10:32:39	2024-01-25
5	WWW	none	VLE	VLE	any	any	public	service-http	none	destination-translation address: WWW-PRIVA port: 80	45	2024-01-25 19:46:49	2024-01-25 17:57:06	2024-01-25

Kuvio 8. UTURN NAT policy, INTERNAL-ACCESS

U-turn NAT:n kanssa jouduimme pohtimaan jonkun aikaa. Labran dokumentaatioissa www- ja name serverin ip:t ovat pyörähtäneet ympäri ja annoimme aluksi destination translation sääntöön ns:n ip:n. Tässä vaiheessa emme olleet vielä luoneet objekteja. Huomasimme, että WWW-säännöllä on dokumentaation mukaan name serverin ip-osoite. Vaihdoimme siihenkin dokumentaation mukaisen www-serverin osoitteen ja liikenne lakkasi toimimasta. Tässä vaiheessa kävimme tarkistamassa servereiden ip:t VLE-ympäristöstä ja totesimme labra- dokumentaation olevan väärässä. Laitoimme sääntöihin oikeat ip:t. ja todensimme yhteyden toimivuuden (ks. kuvio 9).

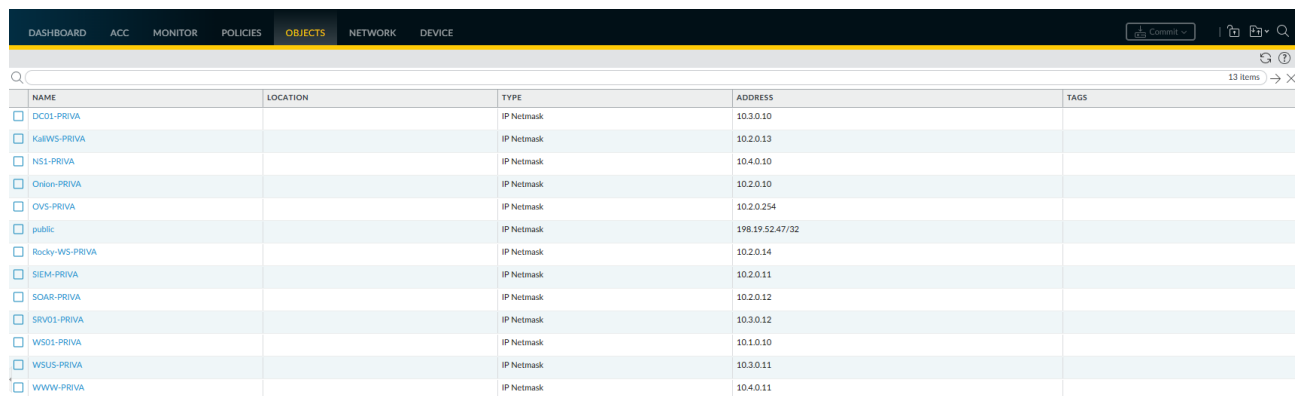
Tämä NAT-sääntö oli nostettava listan kärkeen, koska palomuuuri lukee säännöt järjestyksessä. Mikäli U-TURN sääntö ei olisi listan kärjessä, ympäristön sisäiset laitteet voivat yrittää yhteyttä ulkoiseen ip-osoitteeseen eikä palomuuuri ymmärtäisi, että destination ip on oikeasti sisäverkon puolella.



Kuvio 9. Toimiva U-turn varmennettuna WS01 koneelta

3.4 Objektit

Labraa tehdessämme teimme mm. NAT- säännöt ensi suorilla IP-osoitteilla ja varmistimme niiden toimivuuden. Lopussa, kun näimme yhteyksien toimivan halutulla tavalla, teimme jokaisesta ympäristön laitteesta objektin palomuurille (ks. kuvio 10). Vaihdoimme konfiguraatiossa IP:t vastamaan oikeita objekteja. Tämä mahdollistaa IP-osoitteiden muutokset jatkossa pelkkään objektiin, vähentäen kirjoitusvirheiden riskiä sekä helpottaen tarvittavien muutosten tekemistä ympäristötasolla.



NAME	LOCATION	TYPE	ADDRESS	TAGS
<input type="checkbox"/> DC01-PRIVA		IP Netmask	10.3.0.10	
<input type="checkbox"/> KallWS-PRIVA		IP Netmask	10.2.0.13	
<input type="checkbox"/> NS1-PRIVA		IP Netmask	10.4.0.10	
<input type="checkbox"/> Onkon-PRIVA		IP Netmask	10.2.0.10	
<input type="checkbox"/> OVS-PRIVA		IP Netmask	10.2.0.254	
<input type="checkbox"/> public		IP Netmask	198.19.52.47/32	
<input type="checkbox"/> Rocky-WS-PRIVA		IP Netmask	10.2.0.14	
<input type="checkbox"/> SIEM-PRIVA		IP Netmask	10.2.0.11	
<input type="checkbox"/> SOAR-PRIVA		IP Netmask	10.2.0.12	
<input type="checkbox"/> SRV01-PRIVA		IP Netmask	10.3.0.12	
<input type="checkbox"/> WS01-PRIVA		IP Netmask	10.1.0.10	
<input type="checkbox"/> WSUS-PRIVA		IP Netmask	10.3.0.11	
<input type="checkbox"/> WWW-PRIVA		IP Netmask	10.4.0.11	

Kuvio 10. Objektit

4 Selvitykset

4.1 Eroavaisuudet sääntötyypeissä

Universal -sääntötyyppi: Kyseisessä turvallisuuskäytäntö säännössä määritellään lähtövyöhyke sekä kohdevyöhykkeet. Kyseisessä säännössä liikenne tapahtuu kaikkien valittujen vyöhykkeiden välillä sekä vyöhykkeen sisäisesti. Esimerkkinä jos valitaan lähtövyöhykkeeksi A ja B, sekä kohdevyöhykkeeksi A ja B. Tällöin liikenne tapahtuu sekä A:n ja B:n välillä, B:n ja A:n välillä sekä A:n sisäisesti kuten myös B:n sisäisesti. (What are Universal, Intrazone and Interzone Rules?. 2023)

Intrazone -sääntötyyppi: Kyseessä on turvallisuuskäytäntö, joka sallii saman vyöhykkeen välisen liikenteen. Kyseinen sääntö koskee kaikkea liikennettä määritetyillä lähdevyöhykkeillä, ja

kyseiseen sääntöön ei voi määrittää kohdevyöhykettä. Esimerkkinä, jos valitaan lähtövyöhykkeeksi A ja B, niin liikenne on sallittu vain A:n sisäisesti ja B:n sisäisesti. Ei A:n ja B:n välillä kumpaankaan suuntaan. (What are Universal, Intrazone and Interzone Rules?. 2023)

Interzone -sääntötyyppi: Tämä turvallisuuskäytäntö sallii liikenteen kahden eri vyöhykkeen välillä, mutta ei salli saman vyöhykkeen välistä liikennettä. Kyseisessä säännössä valitaan sekä lähtö- että kohdevyöhykkeet. Esimerkiksi, jos valitaan lähtövyöhykkeeksi A, B ja C ja kohdevyöhykkeeksi A ja B, niin sääntö koskee liikennettä A:n ja B:n välillä, B:n ja A:n välillä, C:n ja A:n välillä sekä C:n ja B:n välillä. Sääntö ei koske liikennettä vyöhykkeiden A, B tai C:n sisällä. (What are Universal, Intrazone and Interzone Rules?. 2023)

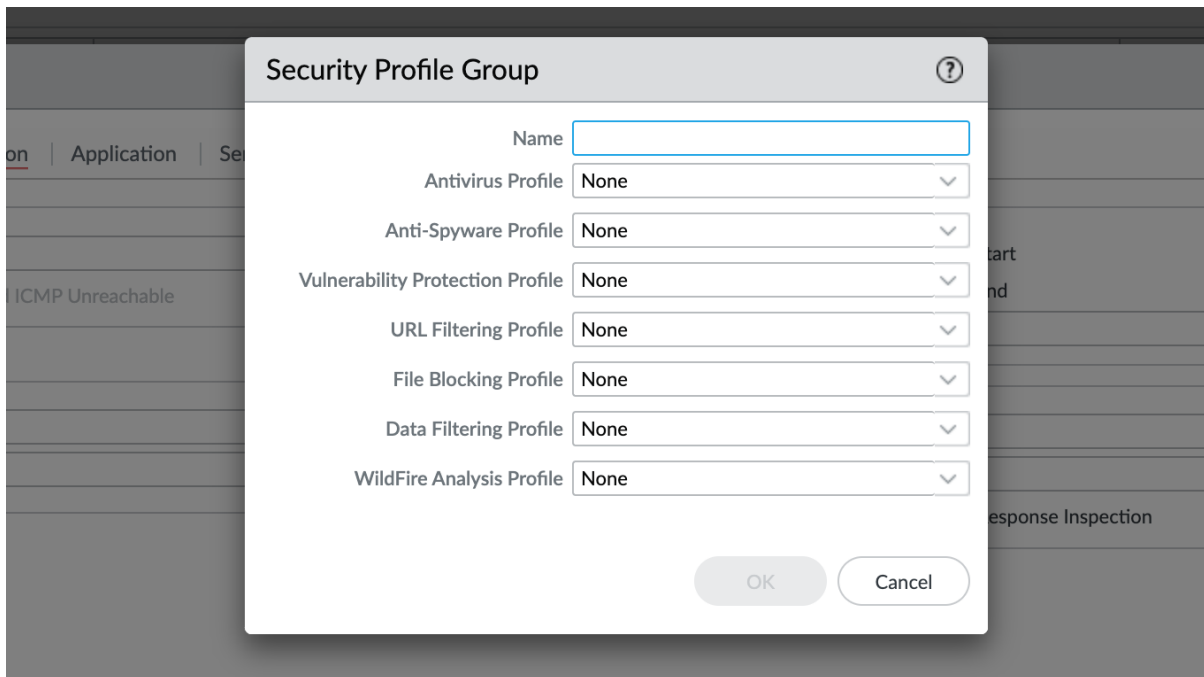
4.2 Eroavaisuudet Applicationilla ja Servicellä PaloAltossa

Application käyttää ohjelmalle tunnettuja portteja, ja hyväksyy vain kyseisen ohjelman läpipääsyn kyseisessä tietoturvapoliitikassa. Oletetaan, vaikka että torrent ja DNS käyttävät porttia 80, mikäli olemme avanneet vain kyseisessä politiikassa portin 80, niin molemmat paketit pääsevät sisään. Nyt kun lisäämme vielä kyseiseen turvallisuuspolitiikan application –kohtaan DNS, niin nyt kyseinen politiikka estää torrentin, koska ei ole listalla. Service –kohdassa voit määritellä, että käyttääkö ohjelma default –porttiaan vai käytetäänkö jotain muuta / ohjataanko toiseen porttiin. Servicessä käytetään siis porttia hyväksi, kun taas Application tunnistaa ohjelman. (What Are Applications and Services.)

4.3 Turvallisuuspoliitikoissa olevat profiilit

Tietoturvakäytäntöjen sääntöjen avulla voit sallia tai estää verkkoliikenteen, mutta tietoturva-profiilien (Profiles) avulla voit määrittää sallia mutta skannata -säännön, eli kun tietoliikenne vastaa turvallisuuskäytännössä (Policies) määriteltäviä sallimissääntöä, niin tietoturva-profiilissa (Profiles) sovelletaan sisällön tarkastussääntöä, kuten virustentorjuntaa, tietojen suodatusta yms. Näitä tietoturva-profiileita käytetään vasta sen jälkeen, kun sovellus tai luokka on sallittu turvallisuuskäytäntösäännössä (Security Policies, 2023).

Profiilien avulla voidaan luoda joko yksittäinen profiili tai ryhmäprofiili, johon voidaan määritellä suoraan halutut turvatoimet seuraavista vaihtoehdoista: Virustorjunta (Antivirus), Anti-Spyware, Haavoittuvuus (Vulnerability Protection), URL –suodatus (URL Filtering), Tiedostojen esto (File Blocking), Tietojen suodatus (Data Filtering) ja WildFire –analyysi (WildFire Analysis). Palo Altossa, jos tallennat ryhmäprofiilin nimellä default, tulee siitä automaattinen profiili, joka lisätään jokaiseen turvallisuus politiikan sääntöön. (ks. **Error! Reference source not found.**)



Kuvio 11. Security Profile Group -näkymä

5 Pohdinta

Labra 2 tehtävänanto koettiin pienitöisemmäksi kuin labra 1, varmastikin osaltaan sen takia että labra 1 myötä oltiin päästy jo alustavasti sinuiksi ympäristön kanssa. Tehtävänannon mukaiset uudet pääsyt saatiin aikaiseksi varsin nopeasti ja menestyksekkäästi testattua. Hieman pohdintaa herätti se miten on viisainta toimia kun on mahdollisuus tehdä joko kokonaan uusia policyjä tai

laajentaa jo olemassaolevia. Tässä lieneekin selvä kohde organisaation hyvät käytännöt-tyyppiselle ohjeistukselle.

Tehtävänannon lisäksi päätettiin toteuttaa luennolla läpikäyty NAT U-turn ja se osoittautui kaikkein suuritöisimmäksi osuudeksi. Suurimpana syynä tähän oli se että ns1 ja www -palvelinten IP-osoitteet olivat ohjeistuksessa ristissä ja tämän havaitsemiseen meni paljon aikaa. Saimme tilaisuuden ryhmässä tehdä varsin perinpohjaista aivotyötä ja debuggausta ennekuin ongelma selvisi. Ehdimme käydä läpi konfiguraatiot useaan kertaan, kuten myös erinäiset ohjeet ja videot ja niiden pohjalta kokeilla yhtä sun toista. Tämä herätti myös huomaamaan Palo Alton snapshot-toiminnallisuuden hyödyllisyyden, testailun tiimellyksessä kun muutokset helposti kumuloituvat ja edellisen stabiilin tilan palauttaminen sujuu niiden avulla helposti.

Lähteet

Definition: What Is a Firewall?. Artikkel Fortinet –sivustolla. Viitattu 28.1.2024.

<https://www.fortinet.com/resources/cyberglossary/firewall>

Paloalto NAT. 2024. PaloAlto tech docs. Viitattu 27.1.2024.

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/nat>

Paloalto U-turn NAT. 2023. Paloalto networks. Viitattu 27.1.2024.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEiCAK>

Security Profiles, 2023. Artikkel PaloAlto Networks -sivustolla. Viitattu 28.1.2024.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles>

What Is A Software Firewall vs A Hardware Firewall?. Artikkel Fortinet –sivustolla. Viitattu

28.1.2024. <https://www.fortinet.com/resources/cyberglossary/firewall>

What Are Applications and Services. Viitattu 28.1.2024.

<https://live.paloaltonetworks.com/t5/community-blogs/what-are-applications-and-services/ba-p/566471>

What are Universal, Intrazone and Interzone Rules? 2023. Viitattu 24.1.2024

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomC>