jamk.fi

# FortiOS:n ajaminen OpenStack-ympäristössä

Markus Huutonen

Opinnäytetyö
Toukokuu 2018
Tekniikan ja liikenteen ala
Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

**Kuvailulehti**

| Tekijä(t) | Julkaisun laji | Päivämäärä |
|---|---|---|
| Huutonen, Markus | Opinnäytetyö, AMK | Toukokuu 2018 |
| | Sivumäärä<br>67 | Julkaisun kieli<br>Suomi |
| | | Verkkojulkaisulupa myönnetty: Kyllä |

Työn nimi

**FortiOS:n ajaminen OpenStack-ympäristössä**.

Tutkinto-ohjelma

Tieto- ja viestintätekniikka, Tietoverkkotekniikka

Työn ohjaaja(t)

Antti Häkkinen, Tero Kokkonen

Toimeksiantaja(t)

Nebula Oy


Tiivistelmä

Cloud computing on yksi nopeimmin kehittyviä ja leviäviä ilmiöitä tietotekniikan alalla ja yritykset ovat yhä enemmän kiinnostuneita sijoittamaan resurssinsa pilvialustoille. Sen sijaan, että palvelut sijaitsevat yhdellä raudalla, voidaan sijoittaa isoihin datakeskuksiin, joista yritykset voivat ostaa vain tarvittavan siivun itselleen. Tämä toteutus vaatii palveluntarjoajan asiantuntijoilta laajamittaista osaamista monilta eri osa-alueilta, koska esimerkiksi tietoverkot ja virtualisointi toimivat hyvin tiiviissä mallissa.

Normaalisti on totuttu, että palomuurit ovat fyysisiä laitteita, jotka sijoitetaan tiettyyn fyysiseen paikkaan tekemään oman osansa kohteessa. Virtualisointia voitaisiin hyödyntää myös palomuurien kohdalla, joten toimeksiannon tavoitteena oli tutkia FortiGate-mallisen virtuaalipalomuurin yhteensopivuutta toimeksiantajan kehittämällä ja hallinnoimalla Cloud 9-alustalla. Palomuurin virtualisointi voisi tuoda paljon etuja verrattuna perinteiseen malliin.

Toteutus suoritettiin tuottamalla kaksi identtistä virtuaalipalomuuria pilvialustalle, jossa niiden toimintaa ja yhteensopivuutta testattiin eri skenaarioissa. Palomuurien taakse sijoitettiin myös kaksi erillistä palvelinta, joiden käyttöä haluttiin simuloida samoin kuin oikeassa tilanteessa.

Virtuaalipalomuurin käyttöönotto oli pääsääntöisesti erittäin helppoa ja yksinkertaista. Yhteensopivuusongelmia esiintyi ainoastaan verkkoratkaisussa, jossa liikenne piti ohjata palomuurin läpi ulkoverkosta julkiverkon osoitteen omaavalle palvelimelle. Testitulokset palomuurin omien toimintojen osalta osoittautuivat onnistuneiksi.



Avainsanat (asiasanat)

Virtualisointi, Palomuurit, Cloud Computing, OpenStack, FortiGate, IaaS, Tietoverkko

Muut tiedot (salassa pidettävät liitteet)

jamk.fi

**Description**

| Author(s) | Type of publication | Date |
|---|---|---|
| Huutonen, Markus | Bachelor's thesis | May 2018 |
| | | Language of publication: Finnish |
| | Number of pages: 67 | Permission for web publication: Yes |

Title of publication

**Running FortiOS in OpenStack environment**

Degree programme

Information and Communications Technology, Data Network Engineering

Supervisor(s)

Antti Häkkinen, Tero Kokkonen

Assigned by

Nebula Oy


Abstract

Cloud computing is one of the fastest-growing and proliferating phenomena in the field of information technology, and companies are increasingly interested in investing their IT resources on cloud platforms. Instead of being on a single physical platform, resources can be placed in large data centers where companies can only buy the necessary share for themselves. A wide range of expertise is required from engineers, as for example, data networks and virtualization work in a very tight model.

Normally, it is customary that firewalls are physical devices that are placed in a certain physical location to make their own contribution to the site. Virtualization could also be exploited for firewalls; hence, the purpose of the assignment was to investigate the compatibility of the FortiGate virtual firewall with Cloud 9 platform developed and managed by the client. Virtualization of a firewall could bring a great deal of potential advantages over the traditional model.

The implementation was performed by producing two identical virtual firewalls on a cloud platform where their functionality and compatibility were tested in different scenarios. Behind the firewalls, two separate servers were also placed, the usage of which was simulated as in a real-life situation.

The introduction of a Virtual Firewall was mainly very easy and simple. Compatibility issues only occurred in a network solution where traffic had to be directed through the firewall from the external network to the server with a public IP address. The test results of the firewall functions proved to be successful.



Keywords/tags (subjects)

Virtualization, Firewalls, Cloud Computing, OpenStack, FortiGate, IaaS, Network


Miscellaneous (Confidential information)

# Sisältö

**Kuviot**

# Lyhenteet

| | |
|---|---|
| ACL | Access Control List |
| AZ | Availability Zone |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| FG | FortiGate |
| FW | Firewall |
| IaaS | Infrastructure as a Service |
| ICT | Information and Communications Technology |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security Architecture |
| LAN | Local Area Network |
| MPLS | Multiprotocol Label Switching |
| NGFW | Next-Generation Firewall |
| P2P | Peer-to-peer |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SSH | Secure Socket Shell |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VM | Virtual Machine |
| VPN | Virtual Private Network |
| VRF | Virtual routing and forwarding |
| WAN | Wide Area Network |

# 1 Johdanto

## 1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi suomalainen ICT-palveluyritys Nebula Oy. Nebula tuottaa suomalaisille yrityksille ICT-palveluja pääasiassa pääkaupunkiseudulla. Keskeisiin palveluihin kuuluvat muun muassa pilvialustat, verkkoinfrastruktuuri, konsultointi sekä muut palvelut kuten verkkotunnukset ja webhotellit. Nebula on osa Telia Company -konsernia.

## 1.2 Vaatimusmäärittely

Työn tavoitteena oli tehdä soveltuvuusselvitys virtuaalisen palomuurituotteen soveltuvuudesta toimeksiantajan pilviympäristöön. Työssä tuli ilmetä mahdolliset epäkohdat toteutukselle, sekä tuoda esiin mahdollisia kehitysehdotuksia. Virtuaalipalomuuriksi valittiin FortiNet:n oma FortiGate VM-järjestelmä, koska yrityksellä on nykyiseltään paljon ratkaisuja, jotka on toteutettu FortiNet:n laitteistoilla.

Toimeksiantajan pilviympäristö on Cloud 9 -nimellä toimiva alusta, joka on vapaaseen lähdekoodiin perustuva OpenStack-pohjainen alusta. Yritys tarjoaa asiakkailleen Cloud 9:n kautta IaaS-palveluita.

Virtuaalisen palomuuriympäristön käyttöönotto kiinnosti toimeksiantajaa erityisesti sen mahdollistamista helpotuksissa muun muassa käyttöönoton ja hallinnan suhteen. Virtualisointi voisi mahdollistaa esimerkiksi palomuuripalveluiden katastrofipalautuksen helpommin käyttämällä alustan snapshot-ominaisuutta. Tärkeää olisi saada myös käyttöön jonkinlainen etäyhteyden mahdollistava VPN-palvelu. Myös virtuaalipalomuurin Next-Generation Firewall (NGFW)-ominaisuuksista oltiin kiinnostuneita, koska nämä saattaisivat mahdollistaa asiakasliikenteen reitittämisen ja suodattamisen virtuaalipalomuurin kautta saaden samalla virtuaaliympäristön tuomat edut käyttöön.

Työ sisältää kaksi eri osiota, jossa ensimmäisessä keskitytään ympäristön yhteensopivuuteen Cloud9:ssä. Toisessa osiossa keskitytään testaamaan pystytetyn ympäristön toimivuutta erilaisissa tilanteissa.

# 2 Työkalut ja ympäristö

## 2.1 OpenStack

OpenStack on avoimeen lähdekoodiin perustuva pilvipalvelualusta. OpenStack koostuu erilaisista moduuleista, jotka muodostavat keskenään kokonaisuuden, joka mahdollistaa pilviympäristön rakentamisen ja hallinnan.

Se on Infrastructure as a Service (IaaS) -ratkaisu, joka tarjoaa palveluna asiakkaalle mahdollisuuden itsenäisen ympäristön pystytykseen ja palveluntarjoaja vastaa ainoastaan itse alustoista. (What is OpenStack? 2018).

Keskeisimmät moduulit OpenStack:ssa ovat:

**Horizon**

Horizon on OpenStack:in keskitetty graafinen hallintarajapinta, josta kaikkien OpenStack:in modulien hallinnointi tapahtuu. Rajapinnan kautta on mahdollista nähdä keskitetysti koko pilviprojektin tilannekuva.

**Nova**

Novan tehtävä OpenStack:ssa on toimia pilvialustan kontrollerina. Se hallitsee virtuaaliresurssien toimintaa käyttämällä erilaisia hypervisor-ratkaisuja.

**Neutron**

Neutron on OpenStack:n verkkokomponentti, joka hallitsee kaikkia sen verkkoresursseja. Neutron tukee itsessään monia eri verkkotekniikoita, kuten palomuuraukset, kuormantasauksen ja L2/3-verkkoliikenteen.

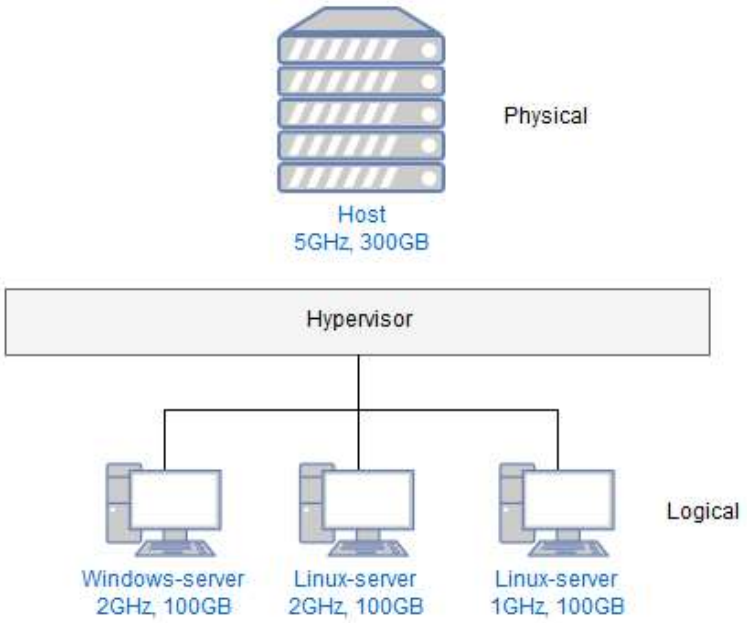
## 2.2 FortiOS

FortiOS on FortiNet:in kehittämä verkkoturvallisuuden käyttöjärjestelmä, jota käytetään FortiNet:in kehittämissä turvallisuusratkaisuissa. FortiOS tukee lukuisia erilaisia turvallisuussovelluksia aina Next-Generation Firewall:sta (NGFW) perinteiseen palomuuraukseen. Soveltuvuusselvityksen tekohetkellä uusin versio FortiOS:stä oli 6.0.0, joka oli julkaistu juuri.

# 3 Teknologiat

## 3.1 Virtualisointi

Virtualisoinnilla tarkoitetaan tekniikkaa, joka mahdollistaa useiden erilaisten ympäristöjen ajamisen yhdellä keskitetyllä fyysisellä järjestelmällä. Tämä järjestelmä (Host) sisältää Hypervisor-nimisen ohjelmiston, joka hallitsee sen sisällä ajettavia loogisia virtuaaliympäristöjä (Guests). (ks. Kuvio 1) Nämä virtuaaliympäristöt ovat toisistaan eriytettyjä instansseja, joita voidaan käyttää eri tarkoituksiin vapaasti. Host-koneelta voidaan määrittää eri määriä sen omaa suorituskykyä ja tallennuskapasiteettia virtuaaliympäristöille. (What is virtualization? 2018.)




Kuvio 1. Virtualisoinnin kerrokset

Virtualisointi vähentää fyysisiä laitehankintoja ja mahdollistaa helpomman hallittavuuden. Myös katastrofista palautumiseen on virtualisoinnissa etunsa. Jokaisesta virtuaalikoneesta on mahdollista ottaa snapshot, joka tallentaa virtuaalikoneen tilan. Tämä snapshot voidaan palauttaa esimerkiksi tilanteessa, jossa ajossa oleva virtuaalikone on vahingoittunut esimerkiksi konfigurointivirheen vuoksi. Tämä mahdollistaa katastrofipalautumisen lisäksi myös hyvän keinon testata helposti uusia käyttöönotettavia ominaisuuksia tai päivityksiä. Mikäli virtuaalikone saadaan hajotettua, voidaan palauttaa ennen muutosta luotu snapshot-versio ja tilanne palaa normaaliksi. (Virtual machines. 2018.)

## 3.2 Cloud computing

Pilvilaskennalla tarkoitetaan ympäristöä, jossa voidaan säilyttää erilaisia tietojenkäsittelyn resursseja, jotka ovat saatavilla internetin yli. Resursseja voivat olla muun muassa eri palveluita tuottavat palvelimet, tallennuskapasiteetti tai laskentateho. Teknologian ansiosta resurssit ovat helposti saatavilla mistä tahansa paikasta, riippumatta käyttäjän sijainnista. (How does cloud computing work? 2018.)

Pilvilaskennan tavoitteena vähentää kustannuksia ja helpottaa resurssien saatavuutta. Yrityksien ei tarvitse esimerkiksi omistaa omaa datakeskusta, jossa sen IT-resurssit säilytetään, vaan yritys pystyy ostamaan palvelun kolmannelta osapuolelta, joka ylläpitää datakeskusta. Tämä kolmas osapuoli pystyy hyödyntämään Cloud computing -teknologiaa myymällä yritykselle vain sen verran kapasiteettia ja resursseja, kun heillä on tarve. (How does cloud computing work? 2018.)

Pilvilaskennalla on myös erilaisia palvelumalleja, joita palveluntarjoajat tuottavat. Merkittävänä erona näiden välillä on tasot, mitä palveluja asiakkaalle tarjotaan ja mitä asiakas hallitsee itse. Näillä määritetään se vastuu, joka jakautuu asiakkaan ja palveluntarjoajan välille alustan resurssien osalta. (IaaS, PaaS, SaaS? 2016).

## 3.3 Cloud computing palvelumallit

### 3.3.1 Infrastructure as a Service

IaaS (Infrastructure as a Service) on palvelutaso, jossa palveluntarjoaja vastaa ainoastaan tuottamastaan alustasta. Käyttäjälle jätetään suuri vastuu ympäristön osalta, eikä palveluntarjoaja välttämättä vastaa alustalla ajettavista resursseista tai niiden tietoturvasta mitenkään. Käytännössä tämä tarkoittaa sitä, että käyttäjälle annetaan pelkkä tyhjä tila, jolle voidaan alkaa rakentamaan käyttäjän itse valitsemia palveluita. Käyttäjä saa määrittää vapaasti palveluille allokoitavan suorituskyvyn ja niillä ajettavat sovellukset. Tämä antaa käyttäjälle täyden hallittavuuden sen omiin resursseihin. (IaaS, PaaS, SaaS? 2016).

### 3.3.2 Platform as a Service

PaaS (Platform as a Service), on palvelutaso jossa palveluntarjoaja tarjoaa käyttäjälle sovellusalustan. Sovellusalusta voi tarkoittaa esimerkiksi tietyllä palvelimella sijaitsevaa http-palvelua (esim. Apache), johon käyttäjä pääsee tuottamaan haluamiaan verkkosivuja. Tässä mallissa käyttäjän ei tarvitse itse vastata esimerkiksi virtuaalikoneen hallinnasta ja ylläpidosta. (Mikä ihmeen PaaS? 2014.)

### 3.3.3 Software as a Service

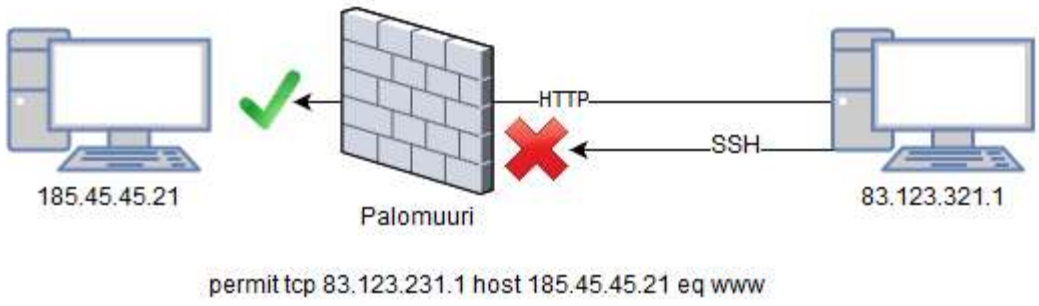
SaaS (Software as a Service), on palvelutaso, jossa palveluntarjoaja tarjoaa käyttäjälle kokonaisuudessaan pelkän sovelluksen. Kaikki alemmat alustat, joilla sovellusta pyöritetään, on palveluntarjoajan vastuulla. Esimerkkinä voi olla vaikka Microsoftin Office 365-palvelu, jota Microsoft vuokraa asiakkailleen ja vastaa käytännössä kaikesta ylläpidosta. Tämä mahdollistaa helpoimman mahdollisen käyttöönoton käyttäjälle ilman tarvetta omalle ylläpidolle tai pohjan rakentamiselle. (Software as a Service (SaaS). 2016).

## 3.4 Palomuuri

Palomuuri on järjestelmä verkossa, joka valvoo sen läpi kulkevaa liikennettä ja sen tarkoituksena on estää luvaton pääsy ja hyökkäykset käyttäjän verkkoon. Palomuuri käyttää hyväkseen toiminnassaan pääsylistoja (Access Control Lists, ACL), jotka sisältävät sääntöjä, joiden perusteella palomuuri tekee päätöksen; estetäänkö vai sallitaanko paketin liikkuminen eteenpäin? Pääsylistat sisältävät tyypillisesti lähteen ja kohteen IP-osoitteen ja sitä vastaavan kuljetuskerroksen TCP- tai UDP-protokollan. (Firewalls and Their Evolution. 2018).

Palomuuri voi olla toiminnaltaan joko tilallinen (stateful) tai tilaton (stateless). Nämä kaksi eri tilaa eroavat keskenään siinä, miten paketteja ja liikennettä tutkitaan.

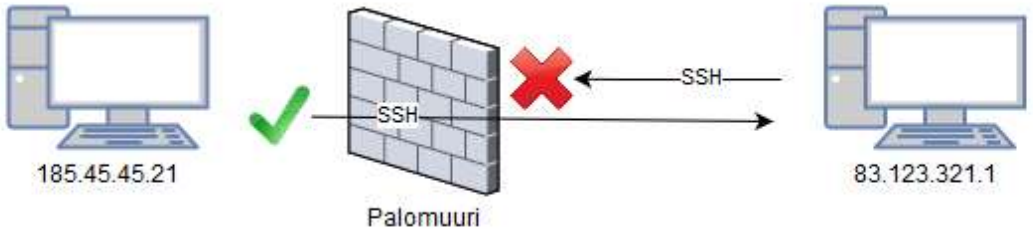
Stateless-tilassa toimivan palomuurin pääsylistat ovat täysin staattisesti konfiguroituja. Pääsylistoja noudatetaan juuri niin kuin ne on palomuurille konfiguroitu (ks. Kuvio 2). Tässä tilassa toimiva palomuuri suoriutuu raskaasta kuormasta paremmin yksinkertaisemman logiikan vuoksi. (Stateful vs. Stateless Firewalls. 2017)




Kuvio 2. Tilattoman palomuurin toiminta

Stateful-tilassa palomuuri kykenee tutkimaan liikennettä dynaamisesti. Perinteisen lähteen ja kohteen seurantaan voidaan lisätä tietoisuus muun muassa TCP-yhteyden tilasta. Jos TCP-paketti on osa jo muodostettua (established) istuntoa, sallii palomuuri sen perusteella paketin. Palomuuri voi myös esimerkiksi sallia SSH-paketit sisältä ulos mutta estää samalla ulkoa uusien yhteyksien muodostuksen (ks. Kuvio 3).

Stateful-tila parantaa palomuurauksen hallittavuutta erityisesti isoissa verkkoympäristöissä. (Stateful vs. Stateless Firewalls. 2017)

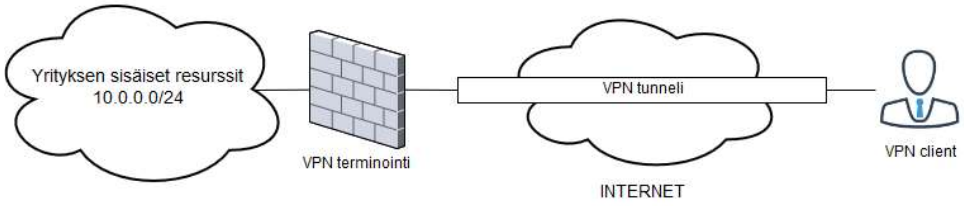



Kuvio 3. Tilallisen palomuurin toiminta

## 3.5 Virtual Private Network

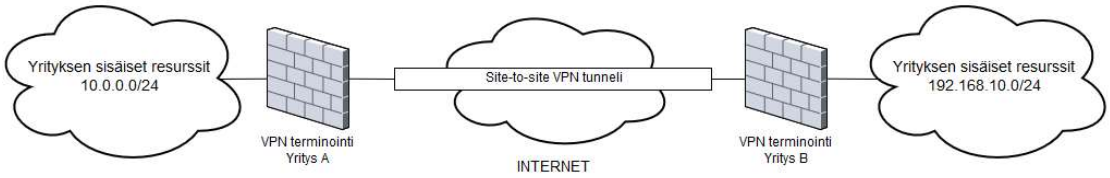
Virtual Private Network (VPN) tarkoittaa kahden verkon ja laitteen välille muodostettavaa suojattua yhteyttä. VPN:ää voidaan käyttää moniin eri käyttötarkoituksiin riippuen verkon ja käyttäjien vaatimuksista. Pääsääntöisesti VPN:ää käytetään kahteen eri käyttötarkoitukseen, jotka ovat etäyhteys (remote access) ja toimipisteiden välinen yhteys (site-to-site).

Etäyhteyden tavoitteena on antaa esimerkiksi yrityksen työntekijöille suojatun pääsyn yrityksen resursseihin myös toimiston ulkopuolelta. Käyttäjät muodostavat suojatun VPN-tunnelin julkiverkon yli esimerkiksi yrityksen palomuurille, jossa VPN-yhteyden terminointi tapahtuu. (ks. Kuvio 4) (What Is a VPN? - Virtual Private Network. 2018).




Kuvio 4. Etäyhteyden muodostaminen

Toimipisteiden välisen yhteyden tarkoitus on muodostaa suojattu yhteys esimerkiksi kahden eri yrityksen verkon välille. Yritys A voi esimerkiksi tarvita yhteyden kumppanin tai asiakkaan verkon resursseihin tietoturvallisesti, joten näiden kahden yrityksen toimipisteen verkon välille voidaan muodostaa VPN-tunneli. (ks. Kuvio 5) (What Is a VPN? - Virtual Private Network. 2018).




Kuvio 5. Toimipisteiden välinen yhteys VPN-tunnelin kautta

## 3.6 Intrusion Prevention System

Intrusion Prevention System (IPS) tarkoittaa käsitteenä systeemiä, joka kykenee reaktiivisesti estämään tunkeutumiset verkkoon. Uhat ja hyökkäykset toistuvat useimmiten tietyllä kaavalla ja tästä kaavasta voidaan muodostaa tunniste tietokantaan, jota IPS vertaa liikenteen valvonnan yhteydessä verkossa kulkevaan liikenteeseen. Tätä tapaa tunnistaa uhat kutsutaan nimellä Signature-based detection. (Intrusion Prevention and Detection System Basics, 2018)

Toinen tapa tunnistaa uhkia on ottaa satunnaisia näytteitä verkon liikenteestä ja verrata tätä näytettä niin sanotusti verkon lähtötilanteeseen (baseline), eli verkossa normaalisti tapahtuvaan liikennemäärään ja tapahtumiin. Tätä tapaa kutsutaan nimellä Statistical anomaly detection. (Intrusion Prevention and Detection System Basics, 2018)

# 4 Suunnitelma

## 4.1 Testausympäristö

Testausympäristöä varten perustettiin neljä eri virtuaali-instanssia, joista kaksi oli Windows Server 2012 R2 -palvelimia ja kaksi FortiGate VM -virtuaalipalomuuria. Nämä instanssit suunniteltiin määritettäväksi kahdelle eri saatavuusalueelle, jotta päästiin testaamaan palomuurien välistä kommunikointia eri saatavuusalueilla kahdennusta varten. Instanssien suorituskykyyn ei kiinnitetty erityistä huomiota, joten ne suunniteltiin asennettavaksi ajoon pienimmällä mahdollisella resurssipaketilla (1 vCPU, 786MB RAM ja 32GB SSD).

## 4.2 Verkkoympäristö

Tavoitteena verkkoliikenteelle oli, että kaksi eri saatavuusalueelle sijoitettua palvelinta saatiin kommunikoimaan aktiivisesti keskenään kahdennuksen toteutusta varten. Saatavuusalueet yhdistettiin keskenään Neutronin omilla reitittimillä ja niille annettiin staattiset reitit toistensa takana oleville LAN-verkoille palomuurien kautta (ks. Liite 1).

Saatavuusalueiden osoitteistukset määritettiin alla esitetyn mukaisesti.

**Availability Zone 1**

IP: 172.17.0.0 Mask: 255.255.0.0

**Availability Zone 2**

IP: 172.18.0.0 Mask: 255.255.0.0

**LAN 1**

IP: 10.0.0.0 Mask: 255.255.255.0

**LAN 2**

IP: 10.0.1.0 Mask: 255.255.255.0

Mikäli kommunikointi saatavuusalueiden välillä onnistuttiin tekemään suoraan hyödyntämällä Neutronin omia reitittimiä, hyödynnettiin tätä yhteyttä

muodostamaan aktiivinen kahdennus palvelinten välillä. Mikäli yhteyttä ei saatu muodostettua Neutronin omilla reitittimillä, rakennettiin saatavuusalueiden välille VPN-tunneli julkiverkon kautta.

## 4.3 Testausmenetelmät

**WAN -> LAN**

Intrusion Prevention System. Koska realistisessa skenaariossa haluttaisiin todennäköisesti estää tunkeutumiset ulkoverkosta palvelimelle, tämä tullaan toteuttamaan palomuurisääntöön, joka vastaa liikenteen sallimisesta ulkoverkosta. Testaaminen tullaan toteuttamaan nmap-porttiskannauksella ulkoverkosta palvelimen julkiosoitteeseen.

**LAN -> WAN**

AntiVirus. Toimintaa tullaan testaamaan käyttämällä EICAR-testivirusta, joka on vapaasti ladattavissa internetistä. EICAR-testivirus on tarkoitettu antivirus-ohjelmien toiminnan testaamiseen.

DNS-filter. Toimintaa testataan valikoimalla kaksi erilaista DNS-nimeä palomuurin tunnistelistalta ja näihin tullaan ajamaan nimenselvityspyynnöt.

Application Control. Toimintaa testataan valikoimalla palomuurin tunnistelistalta yksi sovellus, joka täsmää haitalliseen kategoriaan.

Web Filter. Toimintaa testataan vierailemalla verkkosivulla, joka on luokiteltu palomuurin tunnistelistalla haitalliseksi.

**Etäyhteys**

VPN-etäyhteys tullaan toteuttamaan SSL-VPN-ratkaisulla. Tavoitteena on saada yksi käyttäjä autentikoitumaan yhden palvelimen AD-käyttäjähakemistoa vasten palomuurille ja saada pääsy palvelinverkkoon LAN1.

**Palautuminen ja ylläpito**

Ensimmäisessä vaiheessa testataan palomuurin palauttamista disaster recovery -tilanteessa. Palomuurista otetaan täysi snapshot sen ollessa täysin toimintakykyinen.

Palomuuri-instanssi tehdään toimintakyvyttömäksi ja tämän jälkeen palautetaan aiemmin luotuun snapshot-tilaan. Tavoitteena on tarkastella, miten palautus onnistuu ja kuinka nopeasti.

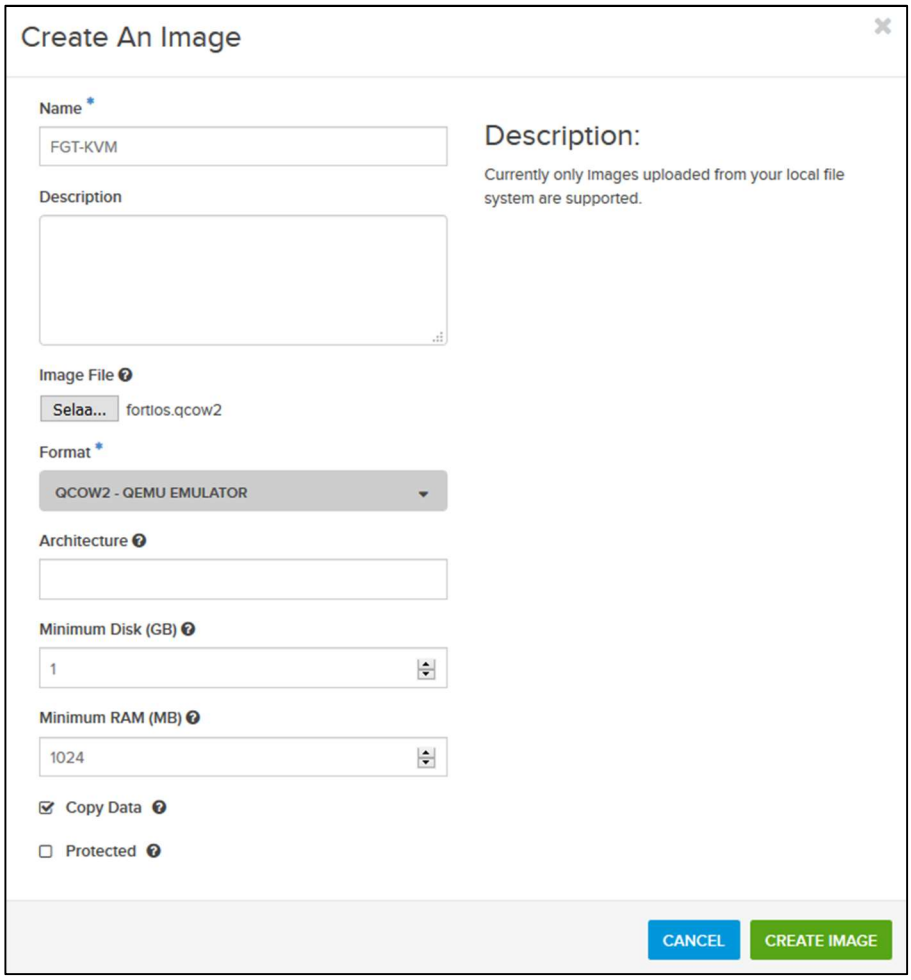
Toisessa vaiheessa palomuurin laiteohjelma (firmware) tullaan päivittämään uusimpaan versioon. Palomuuri asennetaan versiolla 5.6.3 ja päivitetään uusimpaan versioon 6.0.0. Päivityksen aikana seurataan palomuurin käyttäytymistä päivitysprosessin aikana.

Kolmannessa vaiheessa testataan palomuuri-instanssin resurssipaketin päivittämistä. Palomuuri asennetaan kevyimmällä resurssipaketilla käyttöön ja sen jälkeen sen paketti päivitetään yhdellä tasolla ylöspäin. Testissä seurataan palomuurin käyttäytymistä kesken päivityksen ja sen jälkeen.

# 5 Ympäristön pystytys

## 5.1 OpenStack

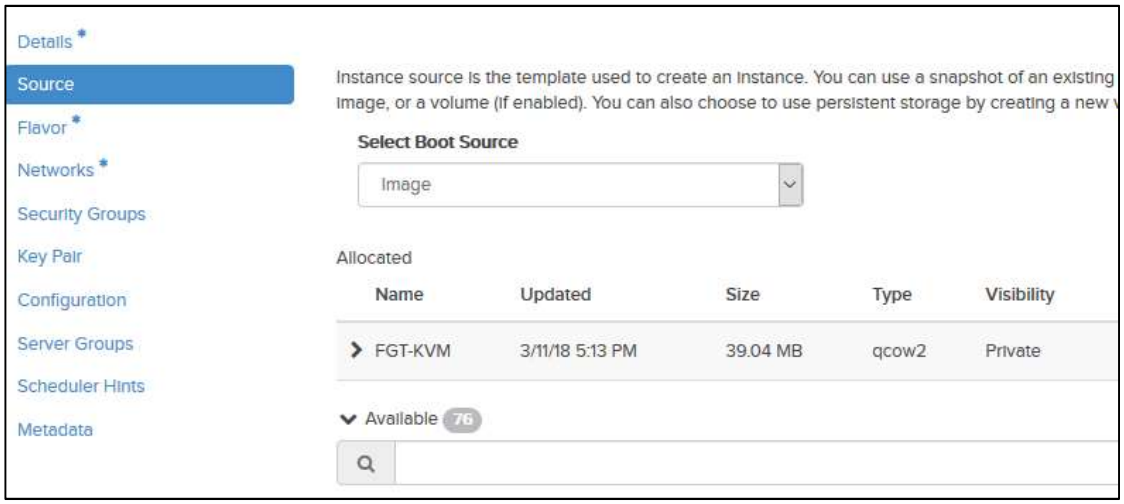
OpenStack-ympäristön pystytys aloitettiin luomalla käyttöjärjestelmille omat levykuvat (image) pilven hallintaan. Cloud9 pitää vakiona sisällään levykuvatiedostot yleisimmille käyttöjärjestelmille, kuten Linux ja Windows, joten näiden kohdalla ei tarvitse ladata tai luoda mitään erikseen. FortiGate:n osalta täytyy luoda uusi levykuva joka aloitettiin lataamalla FortiNet:in tukisivuilta uusin versio FortiGate KVM -palomuurista. Tämän jälkeen voidaan luoda suoraan OpenStack:in hallinnasta FortiGatelle uusi laitteiston käynnistyksen yhteydessä ajettava levykuva kuviossa 6 esitetyillä tiedoilla.



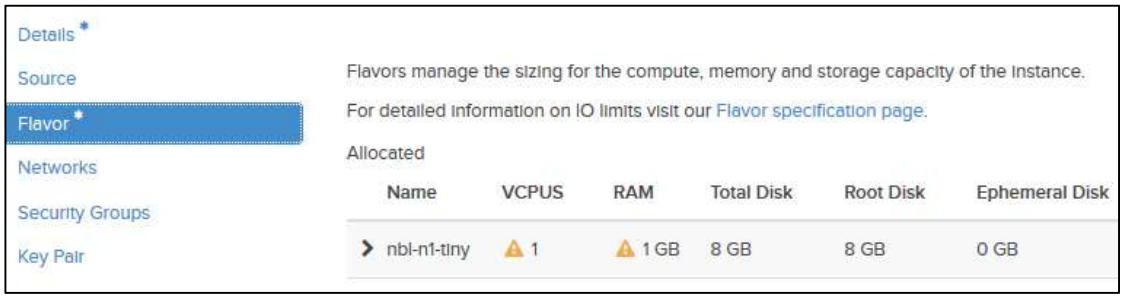

Kuvio 6. Levykuvan luonti

Levykuvan luonnissa on huomioitava tiedoston formaatti. Alusta tukee tällä hetkellä QCOW2- ja RAW-formaatissa olevia tiedostoja. Levykuvan luonnin jälkeen voidaan uusi instanssi luoda suoraan ajamalla levykuvan hallinnasta komento ”launch”.

Alussa valitaan uudelle instanssille sen nimi, sekä saatavuusalue jolle se sijoitetaan. Seuraavassa vaiheessa määritetään tarvittavat tiedot uuden instanssin luontia varten. Tässä tärkeimmät kohdat ovat määrittää uudelle instanssille, miltä levykuvalta se tullaan asentamaan (ks. Kuvio 7) ja kuinka paljon sille halutaan allokoida suorituskykyresursseja (ks. Kuvio 8).



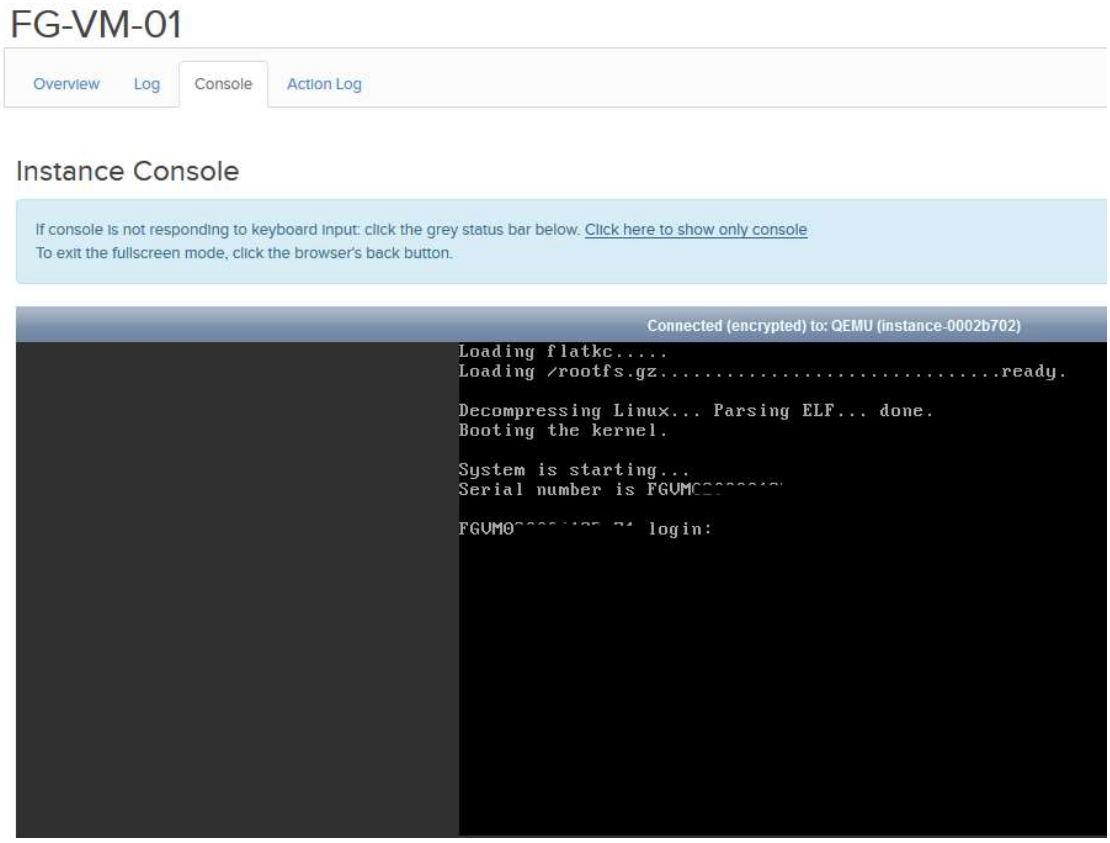

Kuvio 7. Levykuvan valinta




Kuvio 8. Suorituskyvyn allokointi

Näiden vaiheiden jälkeen alusta alkaa rakentamaan instanssia ja on hetken kuluttua käytettävissä. Loput määritykset instansseille tehdään myöhemmässä vaiheessa.

Tähän mennessä toteutus oli onnistunut ilman ongelmia. Instanssin onnistuneen luomisen jälkeen, onnistuu sen hallinta alustan konsoliyhteyden avulla (ks. Kuvio 9)

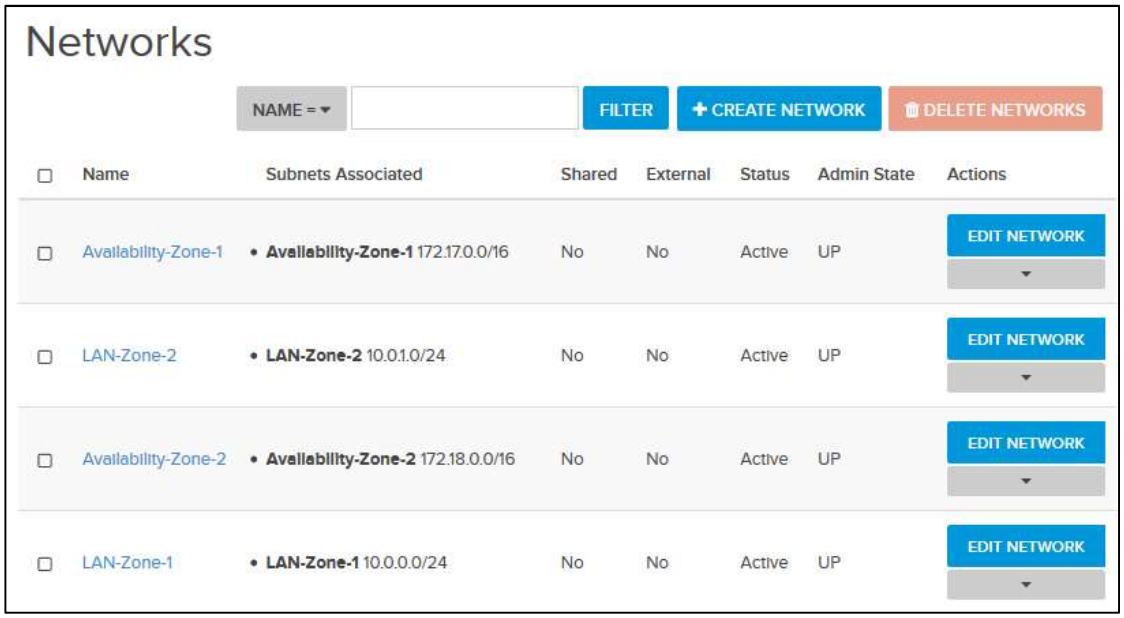



Kuvio 9. Konsoliyhteys

## 5.2 Verkko

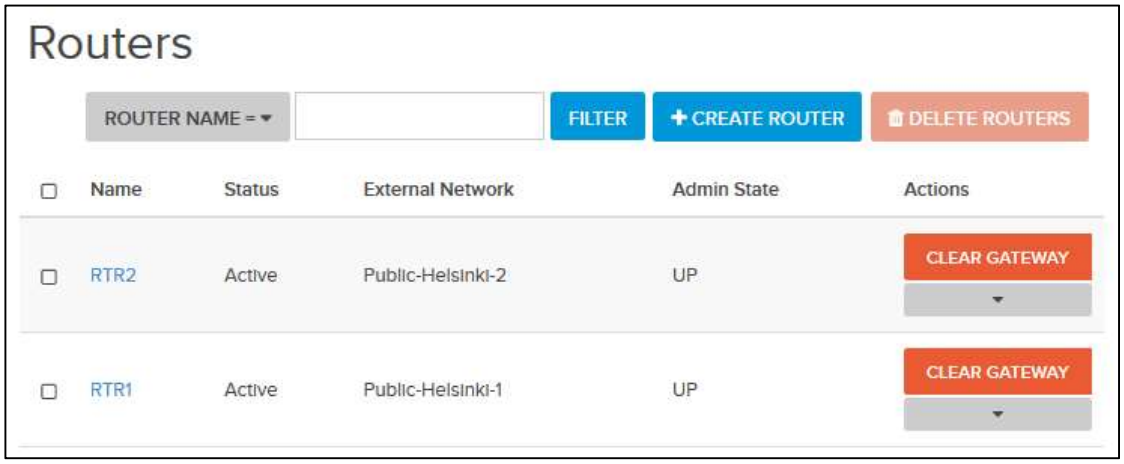
Alusta luo vakiona instansseille valmiit verkot molemmilta saatavuusalueilta, mutta työssä käydään läpi myös verkon luomiset itsenäisesti. Koska tavoitteena oli testata myös kahdennusta kahdella eri saatavuusalueella, tehdään kaksi eri verkkoa kohteisiin Helsinki-1 ja Helsinki-2. Verkoille annetaan nimeksi Availability-Zone-1 ja 2. Saatavuusalueille määritettiin seuraavat aliverkot: 172.17.0.0/16 (AZ 1) ja 172.18.0.0/16 (AZ 2).

Palvelimia varten luodaan vielä molempia saatavuusalueita varten omat LAN-verkot. Näille verkoille annetaan aliverkot 10.0.0.0/24 (LAN 1) ja 10.0.1.0/24 (LAN 2). Lopputulos verkkojen suhteen (ks. Kuvio 10).



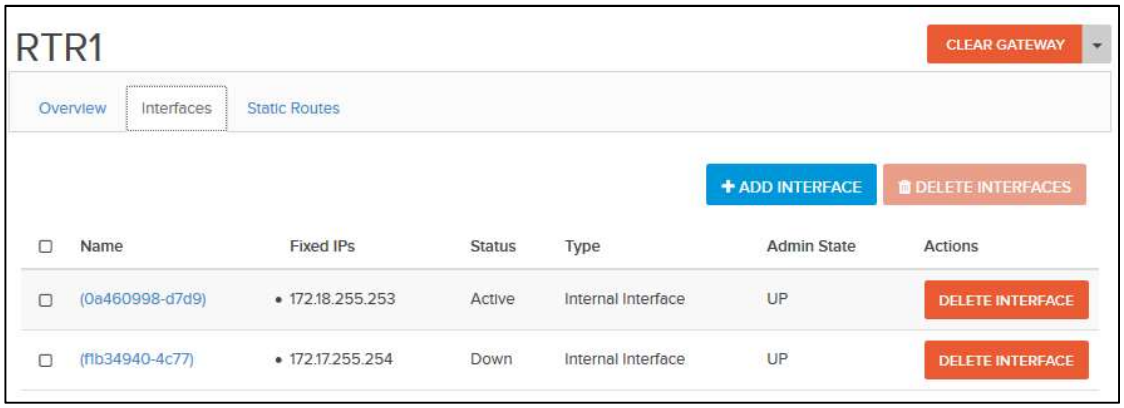

Kuvio 10. Aliverkot

Näiden verkkojen luonti itsessään ei vielä sijoita niitä eri saatavuusalueille vaan niille on luotava omat virtuaalireitittimet pilvialustan sisään, jotka sijaitsevat eri saatavuusalueilla. Lopputuloksena, molemmilla saatavuusalueilla on oma reititin RTR1 ja RTR2 (ks. Kuvio 11)




Kuvio 11. Reitittimet

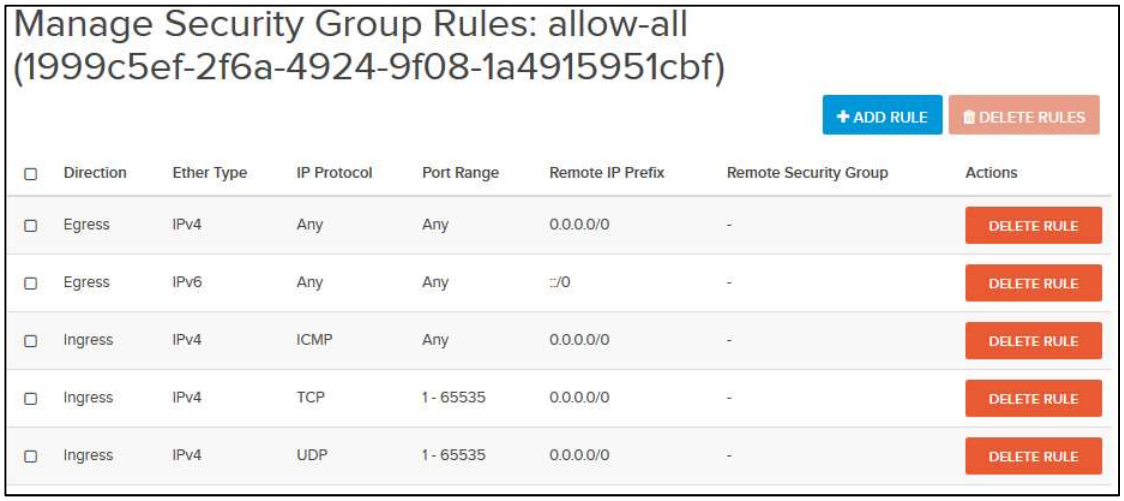
Jotta reitittimet saadaan liitettyä niille tarkoitettujen alueiden verkkoihin, on luotava uudet verkkorajapinnat, jotka toimivat aliverkkojen oletusyhdyskäytävinä. Näitä osoitteita tullaan hyödyntämään myöhemmässä vaiheessa palomuurien reittejä luodessa.




Kuvio 12. RTR1-reitittimen rajapinnat

Oletuksena OpenStack:ssa on käytössä Security Group -asetukset, jotka rajoittavat pääsyä alustan tasolla virtuaalikoneille. Vakiona listat sallivat kaiken liikenteen ulos (egress), mutta estävät ilman tarkennuksia kaiken liikenteen sisään (ingress).

Koska haluamme työssä luottaa palomuurin kykyyn torjua pääsy itseensä, sekä sen takana oleville palvelimille, avaamme Security Group -listat sallimaan kaiken liikenteen. Security Groupit sidotaan aina erikseen, joten sääntö on laitettava jokaiselle instanssille.

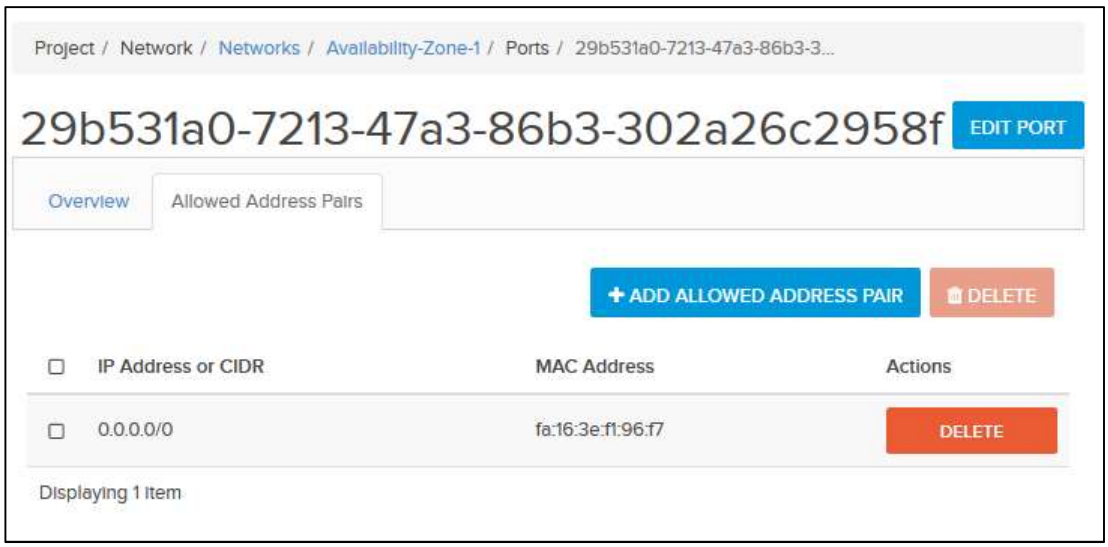



Kuvio 13. Security Group -säänöstö

Koska OpenStack luottaa vahvasti verkossa DHCP:n toimintaan, on sillä käytössä oletuksena DHCP-snooping-ominaisuus. Mikäli verkkojen portteihin kulkee liikennettä niin sanotuista. ”vääristä” osoitteista, ne tiputetaan. Tämä tulee ottaa

huomioon, kun palvelimille ja palomuurille annetaan staattisia IP-määrityksiä. Esimerkiksi verkon AZ1- rajapinta palomuurille FG-VM-01 on erikseen määritettävä, mistä IP-osoitteesta saa porttiin kulkea liikennettä (Allowed Address Pair). (ks. Kuvio 14)

Tässä tapauksessa rajapinnalle annetaan osoite 0.0.0.0/0, jolla poistetaan rajoitukset pois käytöstä. Tämä on tehtävä jokaisen verkon porteille erikseen.

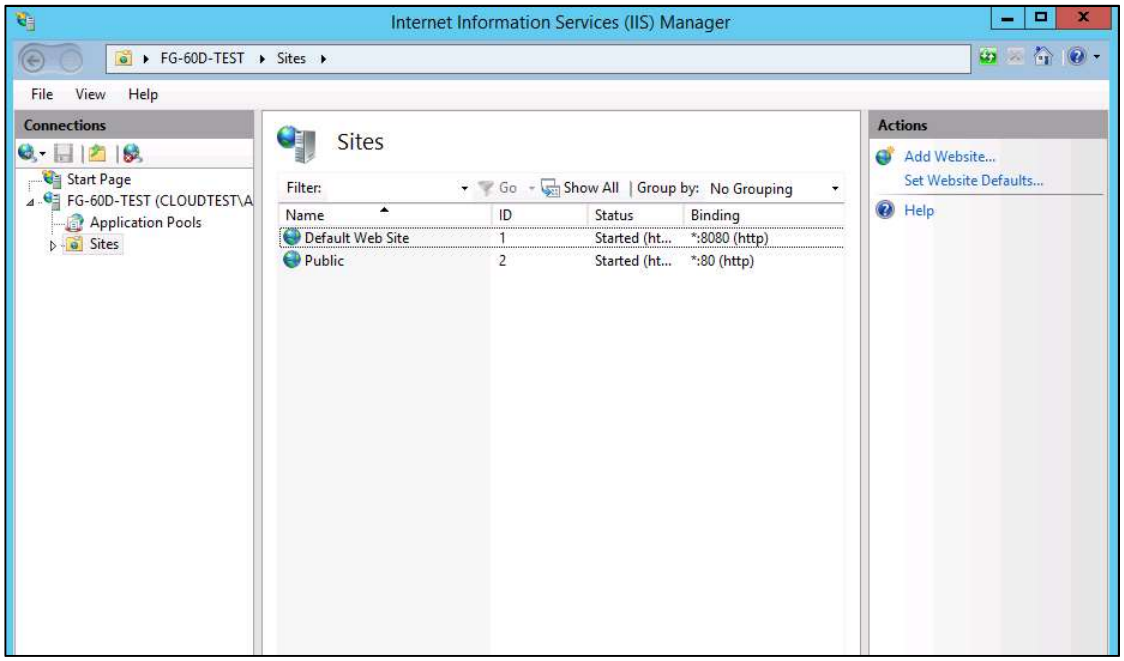



Kuvio 14. Allowed Address Pairs -näkymä

## 5.3 Palvelimet

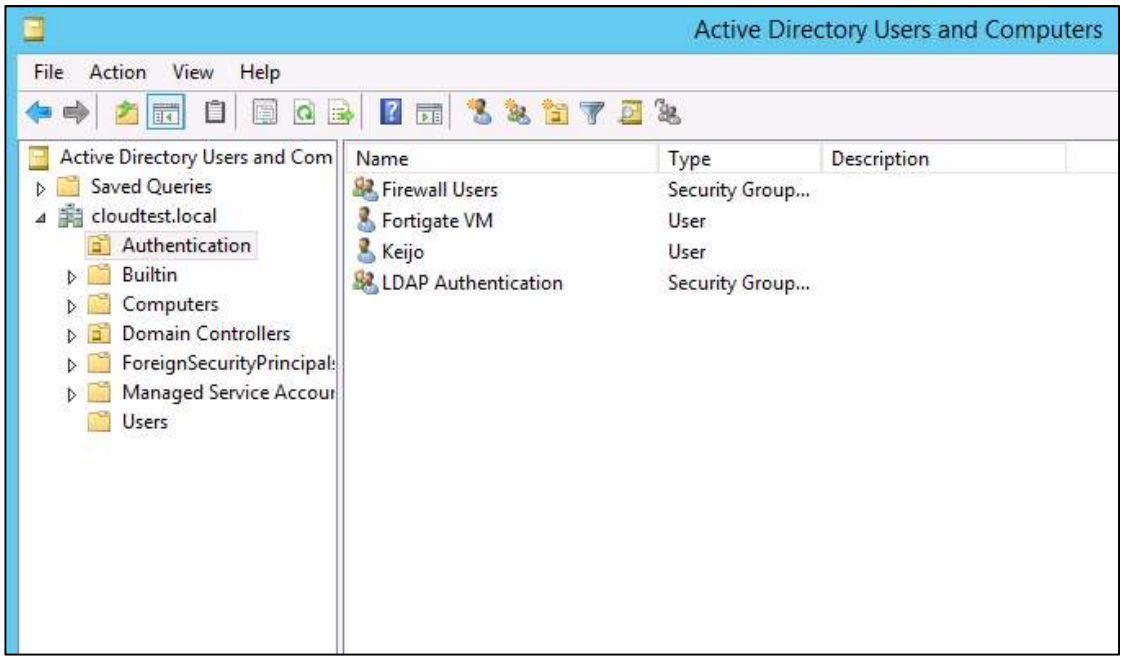
Palvelimet rakennetaan ajamalla alustalle kaksi levykuvaa Windows Server 2012 R2-versiosta. Molemmille allokoidaan testiä varten ainoastaan minimaalinen määrä suorituskykyä.

Palvelimille luodaan rajapinta ainoastaan LAN-verkosta, jolloin sen liikennöinti on riippuvainen palomuurista, koska LAN-verkon oletusyhdyskäytävä sijoitetaan palomuureille, eikä niille tehdä erillistä reittiä suoraan AZ-verkkojen reitittimille. Windowsin oma palomuuri otetaan myös pois käytöstä, koska sitä ei haluta ottaa kuvioon mukaan. VPN-yhteyden autentikoinnin testausta varten palvelimille tehdään AD (Active Directory) -rooli, sekä IIS (Internet Information Services) yleiseen testaamiseen ulkoverkon liikennöinnin näkökulmasta. IIS:lle luodaan kaksi eri verkkosivua, joita kuunnellaan eri TCP-porttien takaa (80 ja 8080). (ks. Kuvio 15)




Kuvio 15. IIS verkkosivut

AD:lle luodaan valmiiksi käyttäjäryhmät LDAP-autentikointia varten yhdellä käyttäjällä (ks. Kuvio 16). Samaan ryhmään luodaan myös yksi käyttäjä palomuurin LDAP-autentikoinnin lukuoikeuksia varten. Palomuuri vaatii yhden tunnuksen, joka pystyy lukemaan käyttäjien ryhmätietoja ja tämän perusteella määrittää niiden pääsy SSL-VPN-palveluun.




Kuvio 16. Authentication OU

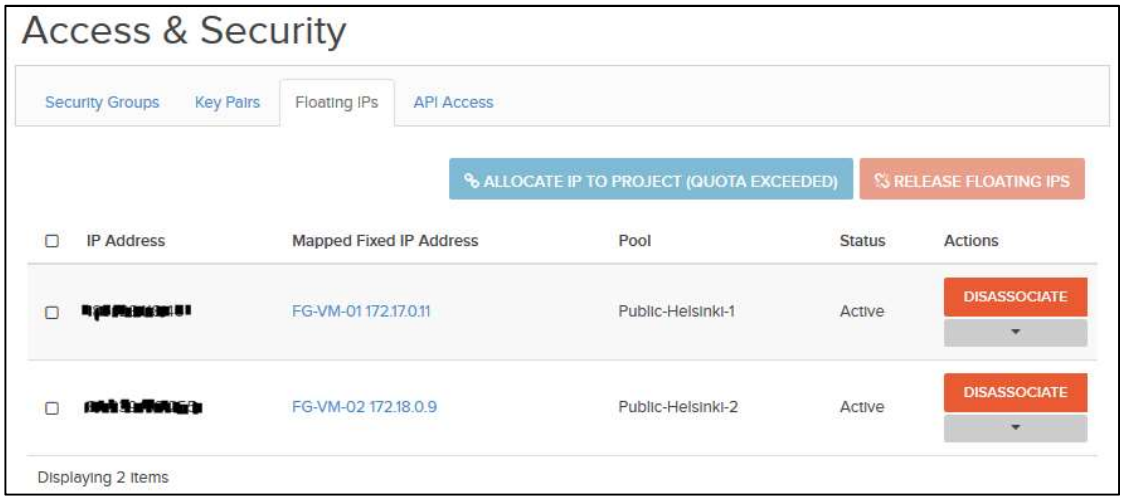
## 5.4 Palomuurit

### 5.4.1 Yleinen

Palomuureja luodaan vaatimusmäärittelyn mukaisesti kaksi kappaletta kahdennuksen vuoksi. Molemmat palomuurit liitetään niiden omien saatavuusalueiden mukaisiin AZ- ja LAN-verkkoihin (ks. Kuvio 17)


Kuvio 17. AZ-verkot

Alusta luo instansseille satunnaiset IP-osoitteet DHCP:llä niiden omalta verkkoalueelta. Verkkojen DHCP:t voidaan ottaa tarvittaessa pois päältä ja määrittää osoitteet käsin. Molemmille muureille annetaan floating IP-poolista oma julkinen IP-osoite, joka käytännössä tekee static NAT säännön alustalle julki- ja privaattiosoitteille. Static NAT ohjaa kaikki julkiverkon osoitteeseen tulevat paketit palvelimen privaattiosoitteeseen. Tässä tapauksessa floating IP annetaan palomuurin AZ-verkon rajapinnan osoitteelle, koska LAN-verkolla ei vielä tässä vaiheessa ole puuttuvien reitityksien johdosta yhteyttä internetiin. Osoitteiden hallinnointi onnistuu myös alustan hallinnasta Access & Security kohdan kautta (ks. Kuvio 18)




Kuvio 18. Floating IP -määritykset

Mikäli DHCP on automaattisesti päällä, on palomuuri saanut automaattisesti IP-osoitteen AZ-verkosta joka vastaa sille luotua floating IP:tä. Tässä tapauksessa palomuurille on suora pääsy ulkoverkosta. Mikäli palomuurilla ei ole DHCP aktiivisena, täytyy sille tehdä määritykset AZ-verkon rajapinnalle, sekä tehdä oletusreitti kohti AZ-verkon reitittimen rajapintaa.

AZ-verkon rajapinnan konfigurointi toteutettiin seuraavasti:

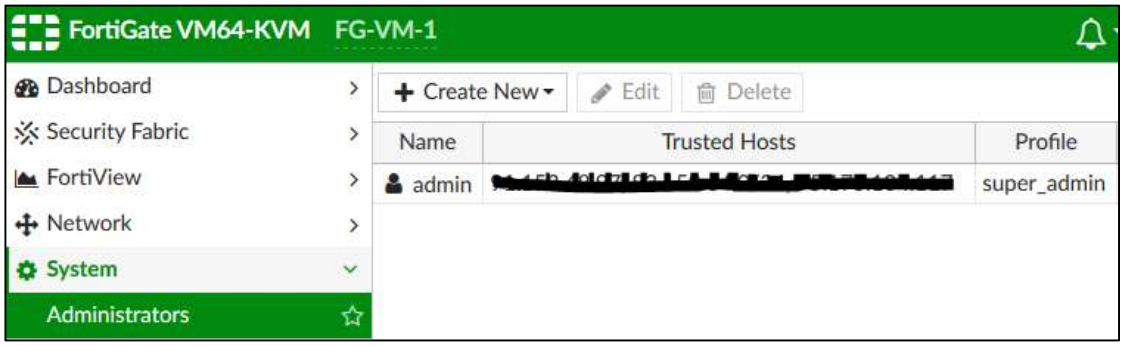
```
FG-VM-1 # show system interface
config system interface
   edit "port1"
      set vdom "root"
      set ip 172.17.0.11 255.255.0.0
      set allowaccess ping https ssh fgfm
      set type physical
      set alias "WAN"
      set role wan
      set snmp-index 1
```

Oletusreitti:

```
FG-VM-1 # show router static
config router static
   edit 1
      set gateway 172.17.255.254
      set device "port1"
```

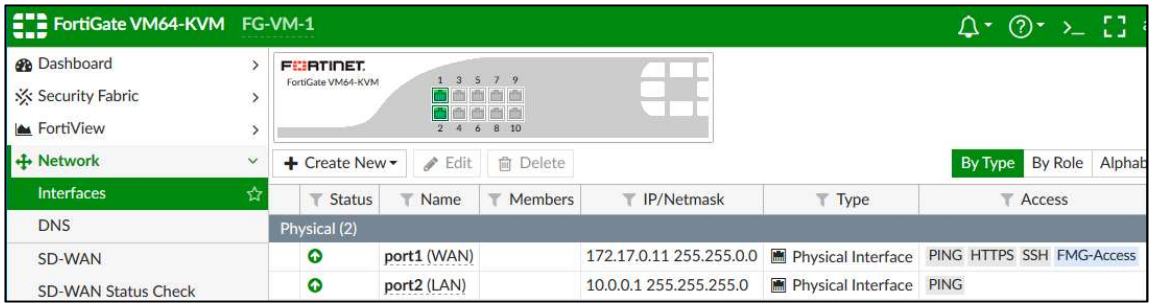
Tämän jälkeen palomuurille annettu floating IP mahdollistaa esimerkiksi sen WEB/SSH-hallinnan suoraan julkiverkosta

Koska palomuuri on nyt kytkettynä suoraan julkiverkkoon, on sen hallintaan pääsyä syytä rajoittaa määrittämällä ainoastaan tietyt luotetut IP-osoitteet sen admin-käyttäjälle (ks. Kuvio 19)



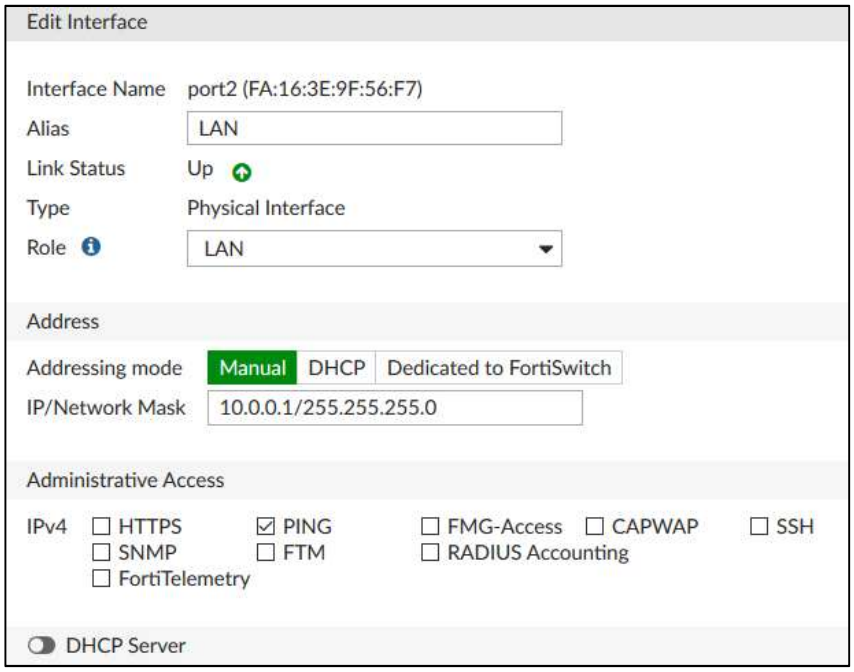

Kuvio 19. Näkymä pääkäyttäjien hallintaan

Tämän jälkeen itse palomuuri oli valmis liikennöintiä ja hallintaa varten. Seuraavaksi luotiin palvelimia varten rajapinta LAN-verkon suuntaan (ks. Kuvio 20). LAN-verkkoina käytettiin suunnitelmassa määritettyjä osoitealueita.



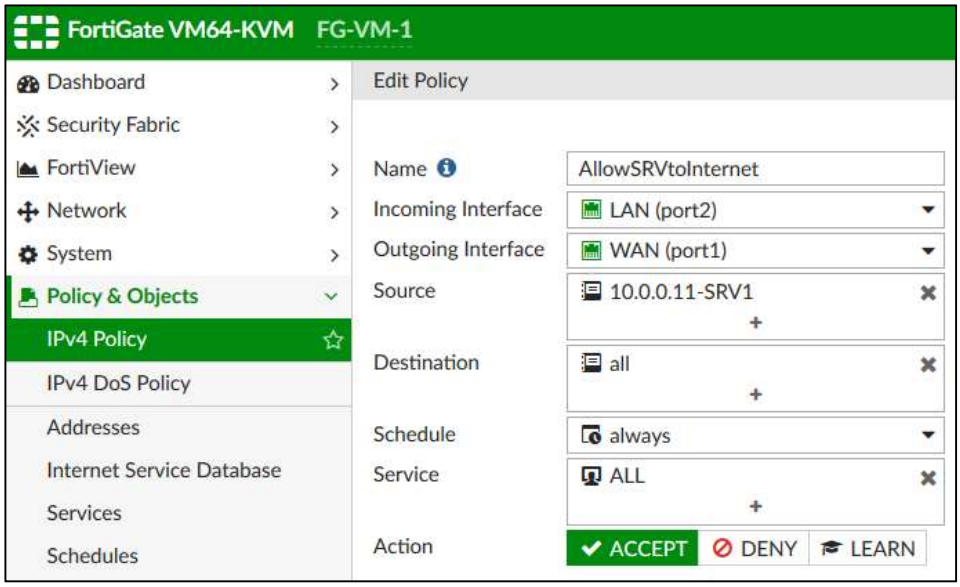

Kuvio 20. Rajapinnat

Rajapinnalle annetaan osoite LAN-verkosta, joka toimii palvelimille niiden oletusyhdyskäytävän osoitteena (ks. Kuvio 21)




Kuvio 21. LAN-rajapinnan asetukset

Rajapinnan määrityksien jälkeen LAN-verkolle on tehtävä erillinen palomuurisääntö, joka sallii LAN-verkosta liikenteen WAN-suuntaan (AZ). Säännössä voidaan rajoittaa eri protokollia, mutta tässä tapauksessa ei haluta rajoittaa mitään liikennettä LAN -> WAN suuntaan.




Kuvio 22. Palvelimen liikenteen salliminen

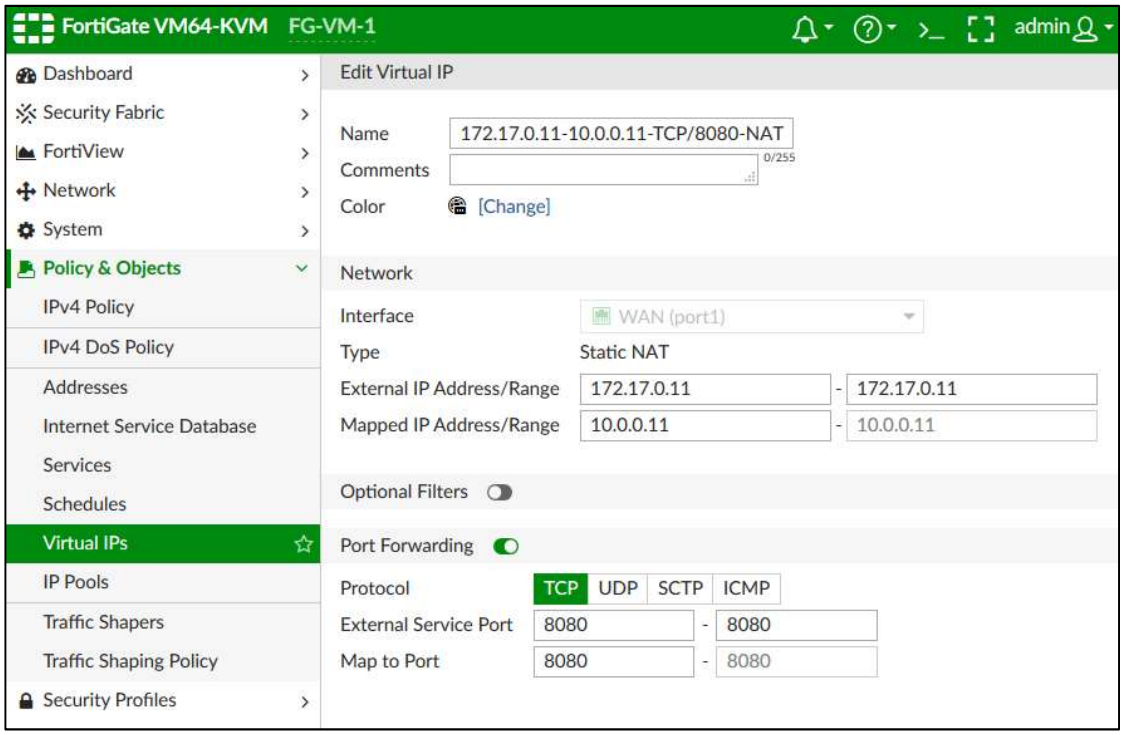
Jotta liikenne lähtee palomuurilta oikein, täytyy sääntöön kertoa vielä, että liikenteen lähdeosoite muutetaan NAT-säännöllä ulosmenevän rajapinnan osoitteeksi (ks. Kuvio 23)


Kuvio 23. NAT-toiminnon aktivointi

Toteutuksen ensimmäinen ongelma ilmeni WAN -> LAN suunnan liikennöinnin suhteen. Koska OpenStack on rakennettu toimimaan julkisten osoitteiden suhteen ainoastaan static NAT muunnosta tekevillä floating IP-osoitteilla, ei palomuurille pystytä antamaan suoraan julkiverkon osoitetta. Static NAT (1:1 NAT) kiinnittää suoraan yhden kiinteän julkiverkon osoitteen lähiverkon osoitteelle.

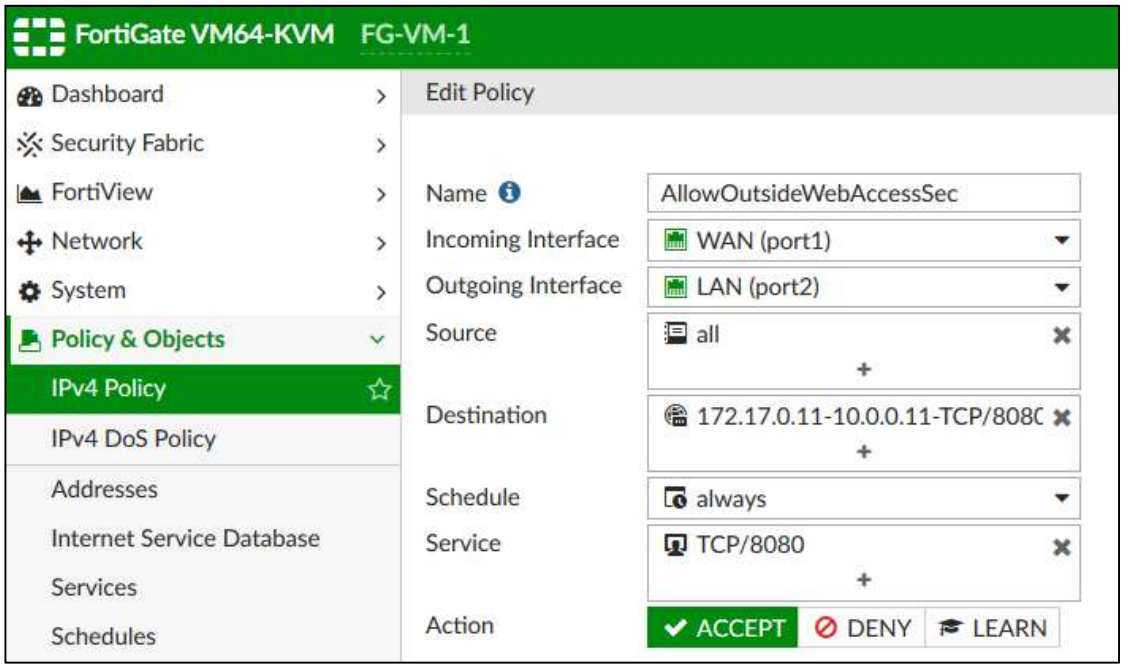
Tästä syystä kaikki floating IP-osoitteeseen kohdistettu liikenne päätyy aina palomuurille itselleen. Palvelimille ei voida itselleen antaa omaa floating IP:tä koska pilvialustan rakenteen takia liikenne kulkee suoraan palvelimelle ohittaen palomuurin.

Jotta tämä kyseinen ilmiö saadaan kierrettyä, täytyy muurille asettaa Virtual IP-sääntö, joka ohjaa sille tiettyyn porttiin tulevat paketit suoraan palvelimelle. Koska SRV-01-palvelimelle asennettiin aiemmin IIS-palvelulle verkkosivu, jonka se on sitonut TCP-porttiin 8080, tehdään seuraavanlainen sääntö palomuurille (ks. Kuvio 24)



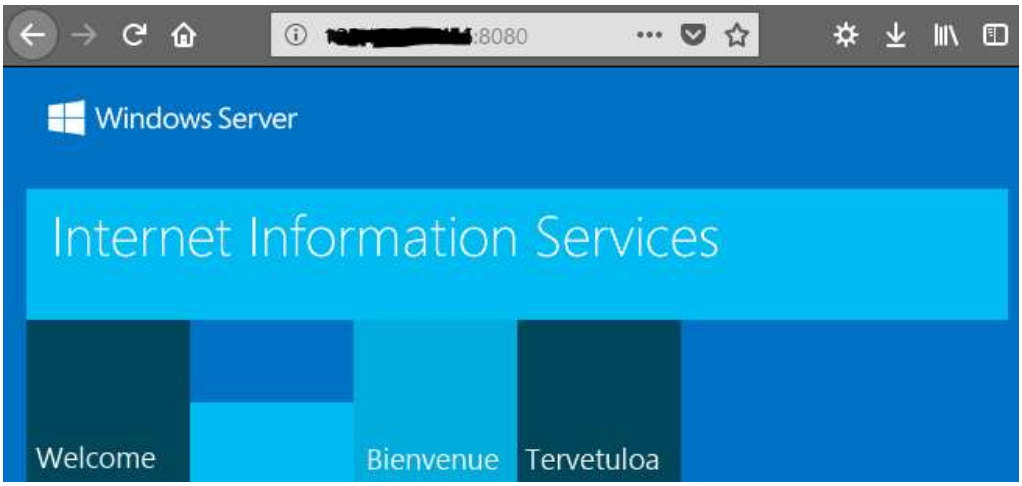

Kuvio 24. NAT-sääntö

Koska pilvialustan 1:1 kääntää floating IP-osoitteeseen tulevat osoitteet 1:1 NAT-säännöllä palomuurin AZ-verkon rajapinnan osoitteeksi, täytyi muurille tehdä määritys, joka kääntää nämä paketit palvelimen osoitteeseen 10.0.0.11. Kun esimerkiksi selaimella otetaan yhteys floating IP-osoitteeseen, esimerkiksi portilla 8080, ohjataan nämä suoraan palvelimen IIS-palvelun verkkosivulle. Tätä voidaan hyödyntää kaikkien porttien kanssa, mutta täytyy ottaa huomioon, että esimerkiksi portit 80 ja 443 ovat oletuksena FortiGate:n Web-hallinnan kuunteluportteja, joten ne täytyy vaihtaa muuksi, jotta näitä portteja pystytään hyödyntämään palomuurin takana olevilla palvelimilla. Kyseinen Virtual IP pitää vielä erikseen sallia palomuurisäännöllä WAN -> LAN suunnasta ja koska halutaan, että kuka tahansa voi päästä SRV-01:llä sijaitsevaan verkkosivuun, annetaan säännölle lähdeosoitteeksi all. Kohdeosoitteeksi annetaan aiemmin luotu Virtual IP-objekti ja sallitaan portti 8080. (ks. Kuvio 25).




Kuvio 25. Outbound-sääntö ulospäin menvälle liikenteelle

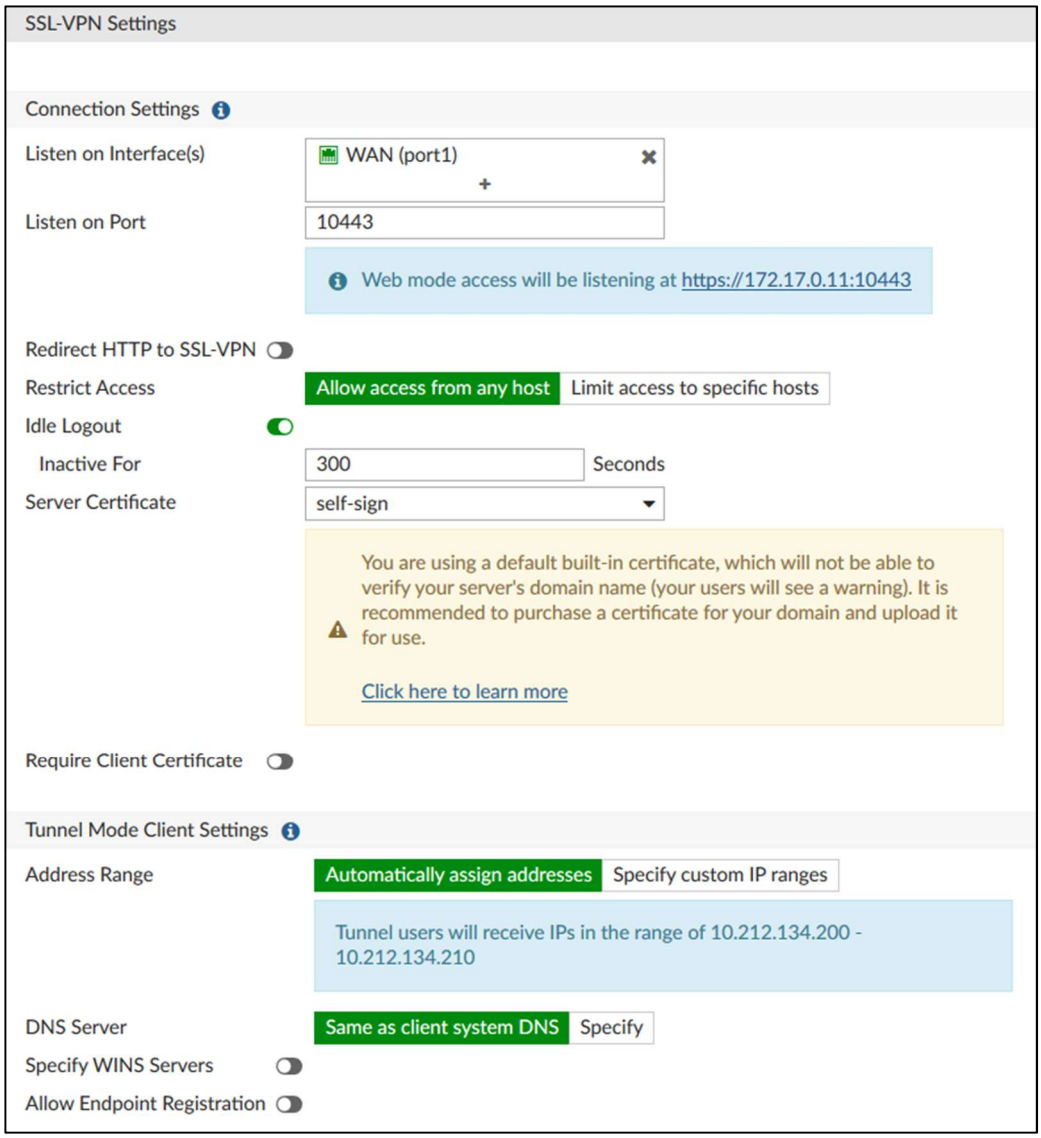
Säännön luomisen jälkeen toimintaa voidaan testata ottamalla yhteys selaimella floating IP-osoitteeseen portilla 8080 (ks. Kuvio 26). Tästä voitiin myös päätellä että palvelimille kohdistuva liikenne internetin suunnasta on mahdollista ajaa palomuurin läpi.




Kuvio 26. IIS-testisivu

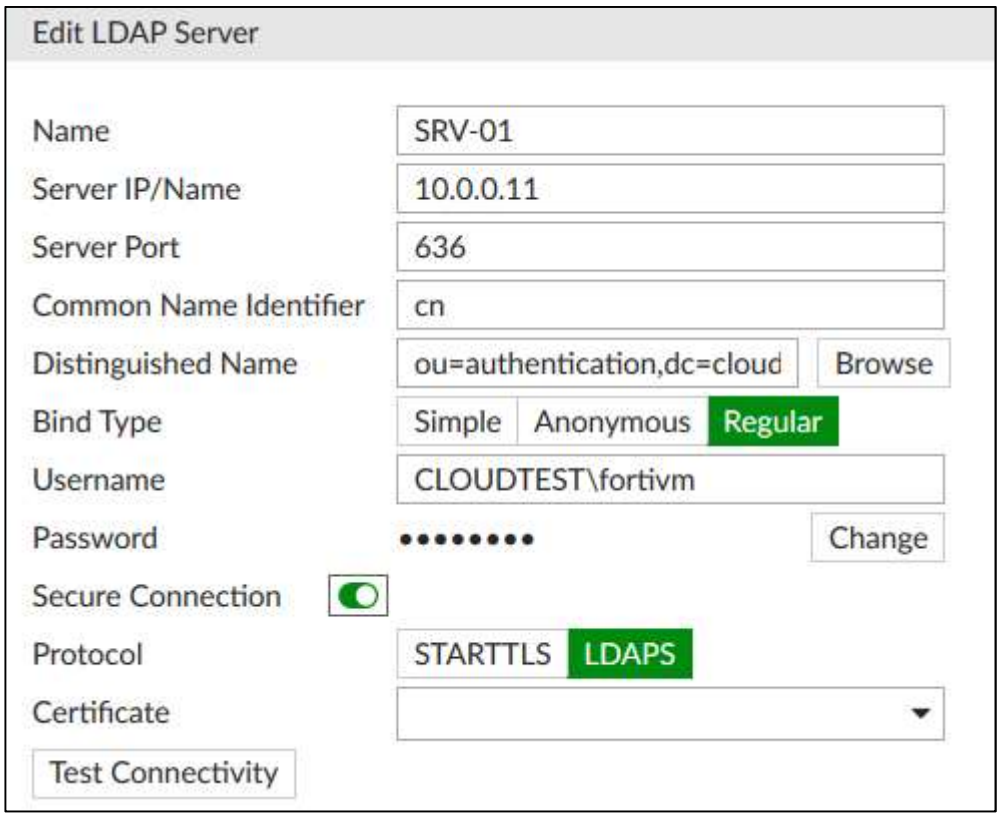
### 5.4.2 VPN

SSL-VPN:n käyttöönotto aloitettiin määrittämällä yhteydelle perusasetukset. Yhteydelle määritetään kuunneltava TCP-portti ja rajapinta jotka ovat tässä tapauksessa WAN TCP/10443. Vakiona FortiGate:n SSL-VPN kuuntelee portissa 443, mutta tämä joudutaan vaihtamaan muuksi, jotta portti ei mene päällekkäin port forwarding-määritysten kanssa palvelimille. Tarpeellista on myös määrittää mihin portaaliin kukin palomuurin paikallinen käyttäjäryhmä ohjataan (ks. Kuvio 27).



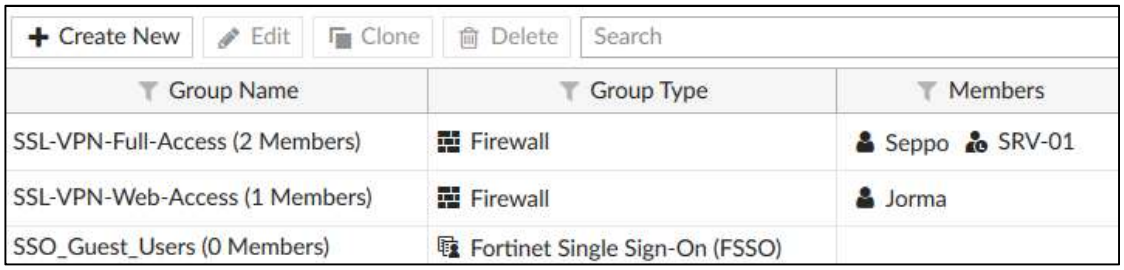

Kuvio 27. SSL-VPN-asetukset

Käyttäjien tunnistuksessa hyödynnettiin palomuurin LDAP-autentikointiominaisuutta ja aiemmin luotua AD-palvelinta. Autentikointi palomuurin päässä vaatii yhden käyttäjän AD:lle, jolla on oikeudet lukea käyttäjien ryhmätietoja AD:lta. (ks. Kuvio 28)



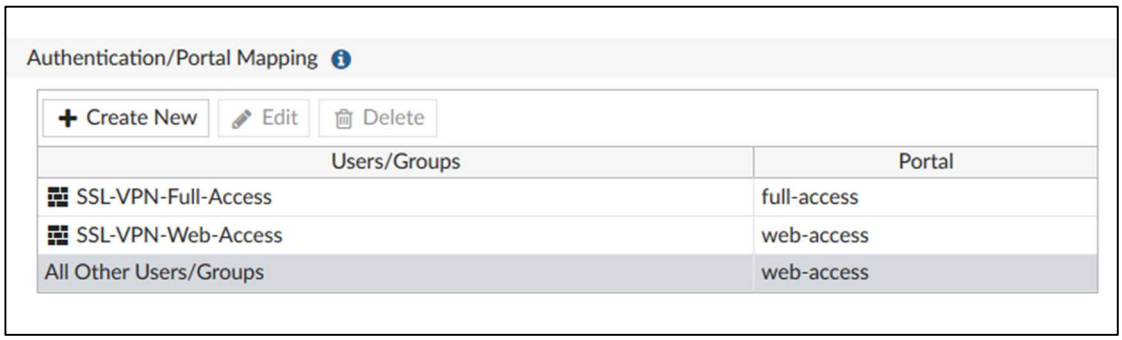

Kuvio 28. LDAP-palvelimen yhteysmääritykset

Jotta eri käyttäjien pääsyä voidaan rajoittaa eri palveluihin SSL-VPN:n sisällä, luodaan palomuurille omat paikalliset käyttäjäryhmät. Tunnel- ja Web-access-tiloja varten luotiin kaksi eri käyttäjäryhmää, joissa toisella ryhmällä oli pääsy molempiin ja toisella vain Web-tilaan. (ks. Kuvio 29)




Kuvio 29. Käyttäjäryhmät

Käyttäjäryhmät tuli myös määrittää SSL-VPN:n asetuksiin. Ryhmät osataan tämän perusteella ohjata oikeisiin portaaleihin, joissa pääsyoikeudet määritetään (ks. Kuvio 30).

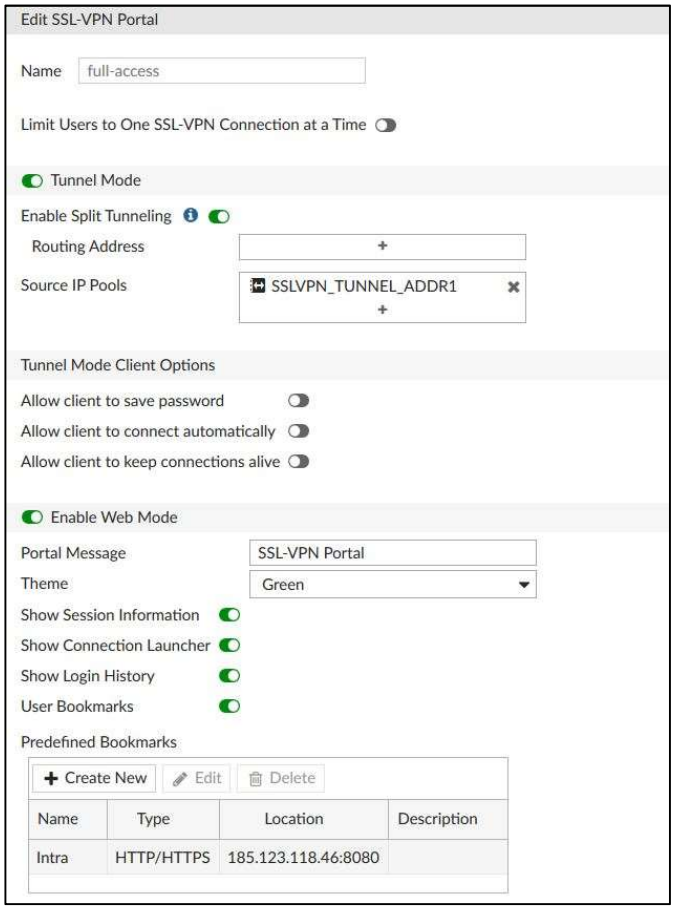



Kuvio 30. Käyttäjien ohjaus

Portaalissa määritetään tunnelointitilalle (tunnel mode) IP-alue, joka jaetaan käyttäjille jotka ohjautuvat kyseiseen portaaliin. IP-alue voidaan luoda uutena objektina (ks. Kuvio 31) tai vaihtoehtoisesti käyttää vakiona olevaa osoitealuetta.

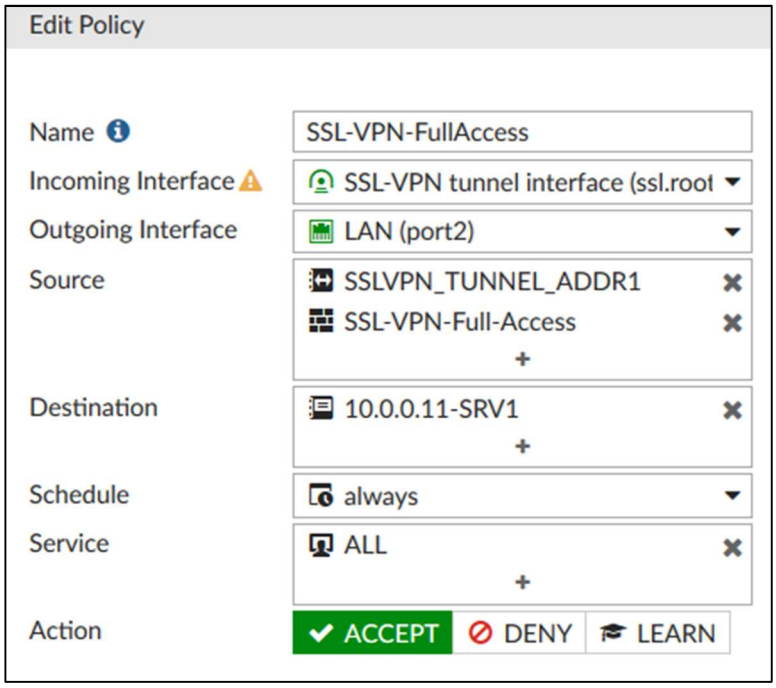

Kuvio 31. Address pool

Samaan portaaliin voidaan aktivoida sekä tunnel- että web-tila käyttöön. Web-tilan määrityksiin voidaan antaa käyttäjille pääsyjä tietyille sisäverkon web-sivuille. Testinä portaalille annetaan aiemmin luodun palvelimen osoite ja portti, jossa IIS-palvelu kuuntelee (ks. Kuvio 32)




Kuvio 32. SSL-VPN-portaalin määritys

Viimeisessä vaiheessa SSL-VPN:lle määritetään palomuurisäännöt, joissa voidaan sallia esimerkiksi vain tiettyjä pääsyjä tietyille käyttäjäryhmille. Testiä varten SSL-VPN:lle tehtiin palomuurisääntö, joka sallii SSL-VPN-Full-Access-ryhmän pääsyn SRV1:n resursseihin vapaasti. (ks. Kuvio 33)



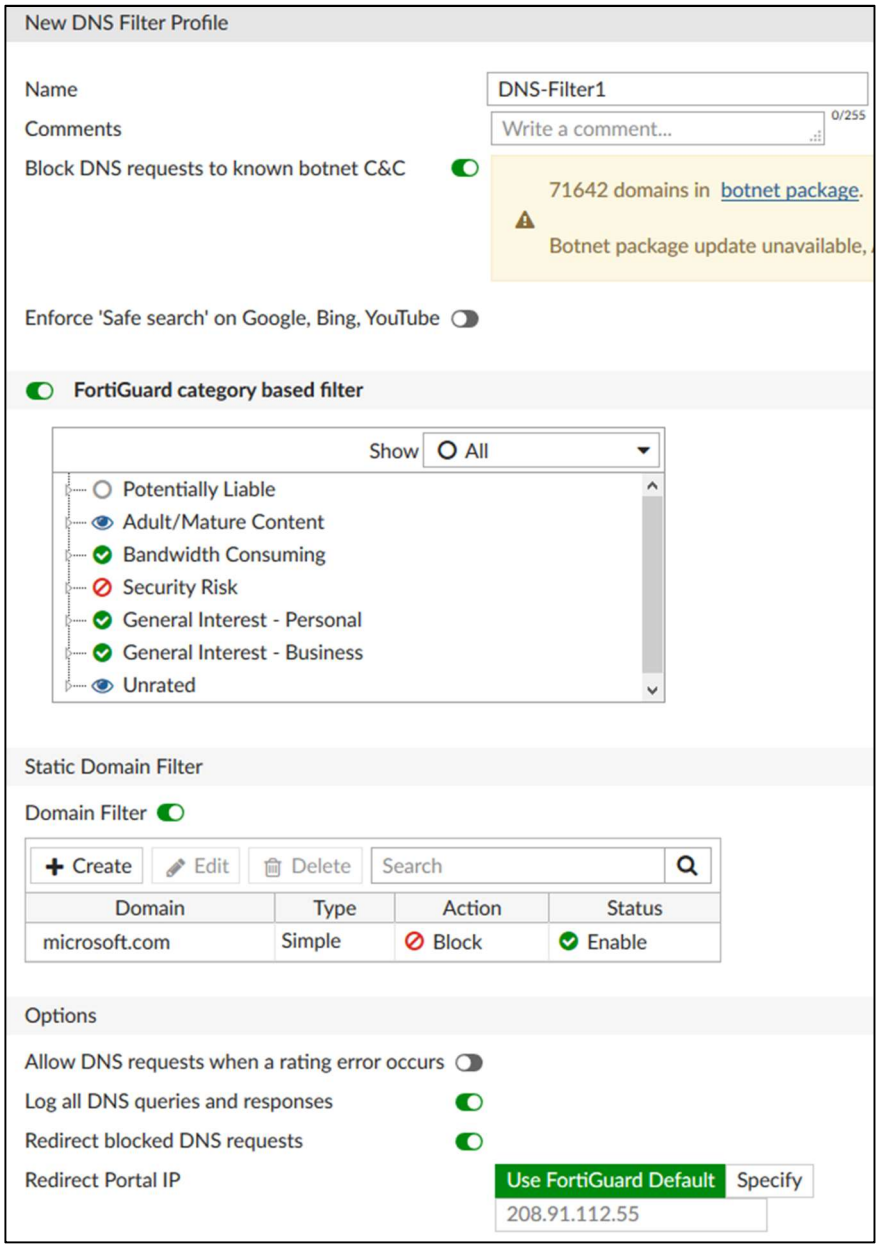

Kuvio 33. SSL-VPN-liikenteen salliminen

### 5.4.3 Liikenteen valvonta ja rajoitus

Palomuurin ominaisuuksiin liikenteen valvonnan ja rajoituksen suhteen kuuluvat Anti-Virus, Web Filter, DNS Filter, Application Control sekä Intrusion Prevention (IPS). Nämä asennettiin palomuurille valvomaan yhden palvelimen liikennettä.

Käyttöönotto aloitettiin tutkimalla uhkien painoarvoa liikenteen valvonnan asetuksista. Painoarvot määrittävät muun muassa Palomuurin kynnystä reagoida tai jättää reagoimatta tiettyihin uhkiin. Painoarvot jätettiin testausta varten vakioasetuksille.

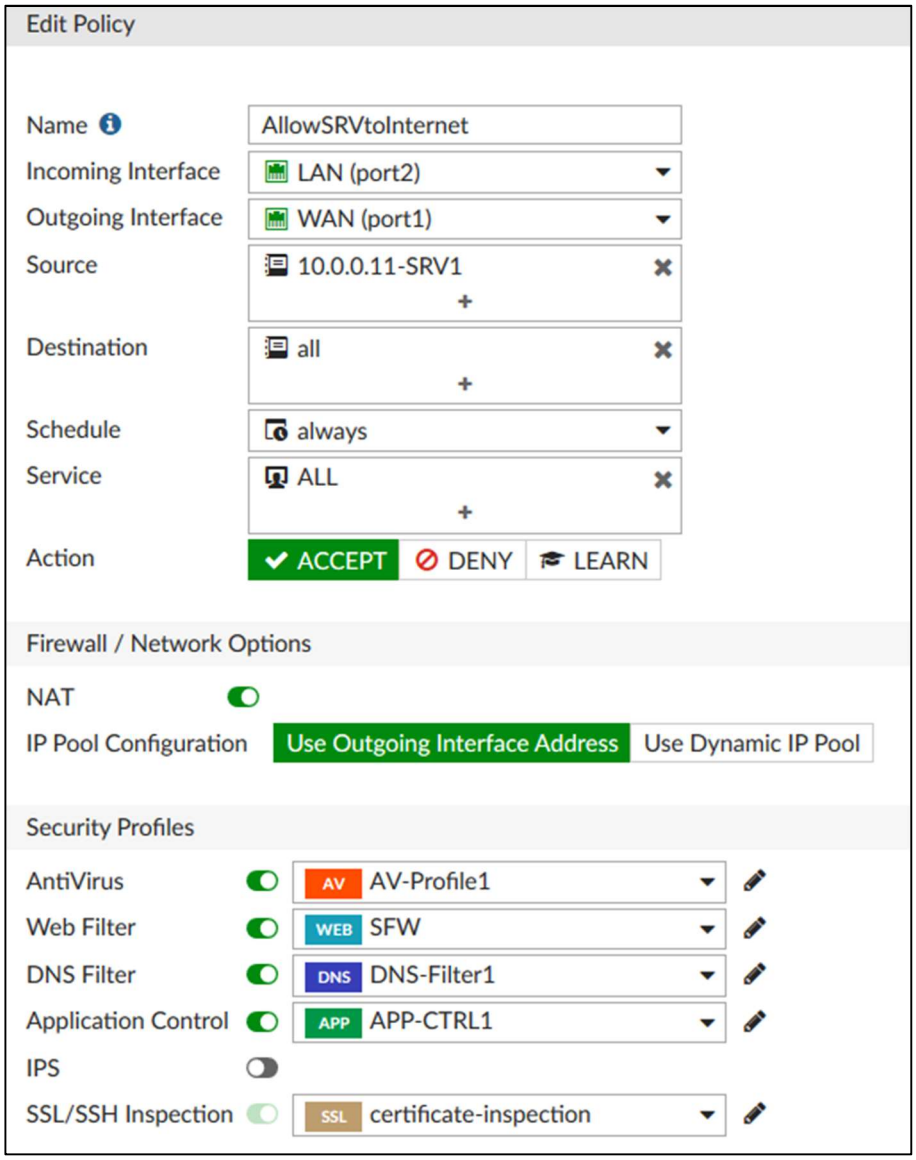
Liikenteen valvonnassa ja rajoituksessa on mahdollista luoda eri profiileja esimerkiksi DNS-suodatukselle (ks. Kuvio 34). Profiilimääritykset esimerkiksi Web-liikenteen suodatuksen kanssa toimivat hyvin samalla periaatteella.




Kuvio 34. DNS-suodatuksen asetukset

DNS-suodattimen asetuksiin on mahdollista muokata estettäviä kategorioita (Category based filter), kiinteän toimialueen esto ja DNS-ohjaus joka tehdään kriteerien täyttyessä. Kuvassa oleva microsoft.com-toimialueen suodatin ohjaa kaikki DNS-kyselyt FortiGuard portaaliin.

Liikenteen valvonta ja rajoitus saatiin käyttöön määrittämällä profiili aktiiviseksi palomuurisääntöön, joka sallii liikenteen palvelimelta ulkoverkkoon (ks. Kuvio 35).




Kuvio 35. Suodatusprofiilien aktivointi

Koska kyseessä on palomuurisääntö palvelimelta ulospäin, aktivoitiin valvontaan Anti-Virus, Web Filter, DNS Filter sekä Application Control ja ulkoverkosta palvelimen suuntaan testattiin erikseen IPS:n toimintaa.

### 5.4.4 Kahdennus

Palvelimille annettiin kaksi rajapintaa molempiin LAN-verkkoihin ja saatavuusalueet yhdistettiin keskenään pilven omilla reitittimillä. Reitittimille annettiin seuraavat staattiset reitit, jotta ne osaisivat reitittää paketteja palvelimien välillä.

Router1: Destination: 10.0.1.0/24, Next hop: 172.18.0.9 (FG-VM-02)

Router2: Destination: 10.0.0.0/24, Next hop: 172.17.0.11 (FG-VM-01)

Valmiiksi rakennettua ympäristöä voidaan tarkastella Horizonin ominaisuudella, joka piirtää kokonaisen verkkokuvan lopputuloksesta. (ks. Liite 2). Molemmat palvelimet sijoitettiin vikasietoisuuden vuoksi erillisille saatavuusalueille.

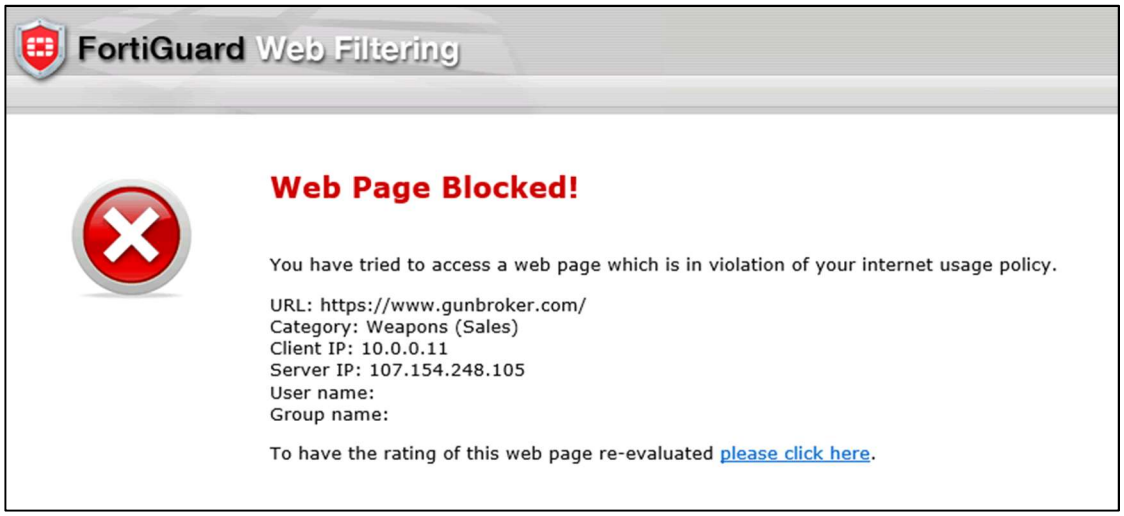
# 6 Testaustulokset

## 6.1 Liikenteen valvonta ja rajoitus

Ensimmäisessä vaiheessa testattiin palomuurin ominaisuuksia liittyen liikenteen valvontaan ja rajoitukseen. Ominaisuuksien toimintaa testattiin oikeiden käytännön esimerkkien mukaisesti.

**Web Filtering**

Yhteys muodostettiin SRV-01-palvelimelta verkkosivuille, jotka osuvat palomuurin rajoitettavien sivujen kategoriaan. Esimerkissä otettiin satunnainen verkkosivu google-haulla, joka osuu palomuurin kategoriaan ”Weapons”, eli kun selain yhdistää tälle sivulle, estää palomuuri yhteyden kyseiselle palvelimelle (ks. Kuvio 36). Tämä testi osoittaa, että Web Filtering -ominaisuus on täysin toimiva.




Kuvio 36. Ilmoitus ei-sallitun verkkosivun estämisestä

**DNS-filter**

Toimintaa testattiin DNS-filterin kohdalla tekemällä DNS-haku osoitteisiin, jotka täsmäävät palomuurin suodatuslistaan. Listalta valittiin kaksi osoitetta, joille ajettiin Windowsin komentoriviltä nslookup-komento.

```
C:\Users\Administrator>nslookup hawacyso.info
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    hawacyso.info
Address:  208.91.112.55


C:\Users\Administrator>nslookup dbgoku.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    dbgoku.com
Address:  208.91.112.55


C:\Users\Administrator>
```

Kuvio 37. Nslookup-haun tuloste

Tuloksesta voidaan todeta, että kaikki palomuurin listalta löytyvien domain-nimien DNS-kyselyt ohjataan turvallisesti oikein FortiGuard DNS-filter portaaliin 208.91.112.55. Ongelmiin testien aikana ei törmätty.

**Application Control**

Todennus toimivuudesta sovellusten kontrollointiin liittyen tehtiin testaamalla kategoriaa liittyen P2P-sovelluksiin. Käytännössä testaaminen tapahtui lataamalla BitTorrent-niminen sovellus palvelimelle. Koska BitTorrent on palomuurin P2P-sovellusten listalla, estää se sen lataamisen ja tämä voidaan todeta tarkistelemalla palomuurin lokia liittyen Application Control-suojaan (ks. ).

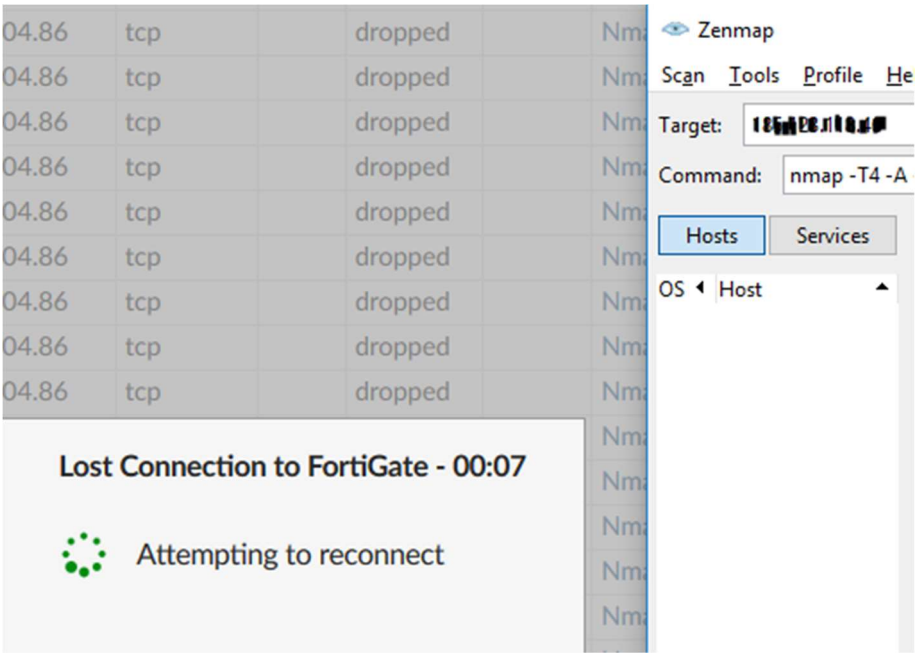
| # | | Date/Time | Source | Destination | Application Name | Action |
|---|---|---|---|---|---|---|
| 1 | | 19:27:38 | 10.0.0.11 | 178.79.242.147 (www.bittorrent.com) | BitTorrent | block |
| 2 | | 19:27:36 | 10.0.0.11 | 178.79.242.147 (www.bittorrent.com) | BitTorrent | block |
| 3 | | 19:27:02 | 10.0.0.11 | 178.79.242.147 (www.bittorrent.com) | BitTorrent | block |
| 4 | | 19:25:00 | 10.0.0.11 | 178.79.242.147 (www.bittorrent.com) | BitTorrent | block |

Kuvio 38. Sovelluksen estämisen määritykset

Testistä voitin todeta, että palomuurin Application Control-ominaisuus toimii halutulla tavalla. Testin aikana ei myöskään törmätty ongelmiin

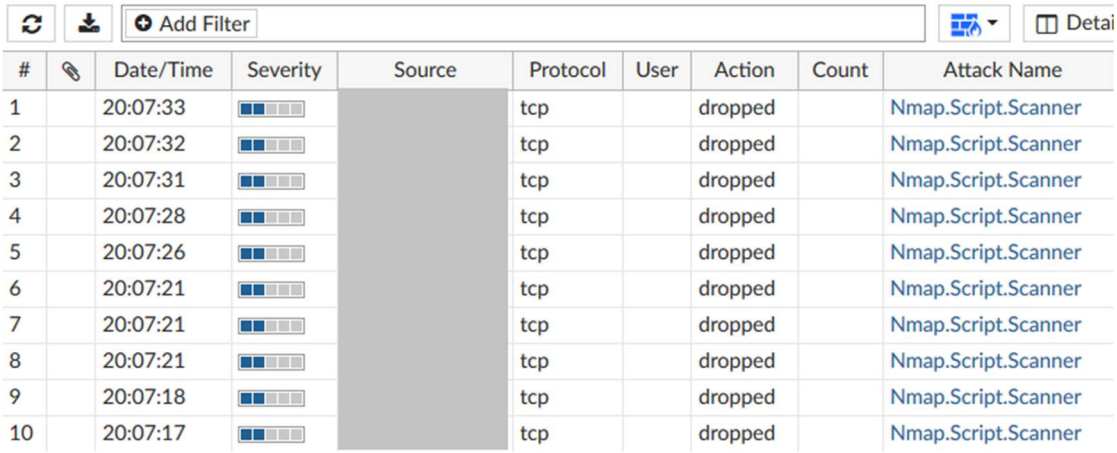
**Intrusion Prevention System**

IPS-moduulia testattiin ulkoverkosta päin kohdistamalla porttiskannauksia palomuurin floating IP-osoitteeseen nmap-ohjelmalla. IPS-moduuli sisältää tunnisteet nmap:lla tapahtuviin skannausyrityksiin ja tätä käytettiin esimerkkinä toiminnan toteamista varten. Skannaus aloitettiin kohdeosoitteeseen ja samalla hetkellä yhteys lähdekoneeseen estettiin, koska yhteys palomuurille katkesi (ks. Kuvio 39).




Kuvio 39. Nmap-skannaus

Tämän jälkeen tutkittiin palomuurin lokeja IPS:n osalta, josta nähtiin, että merkintöjä estetyistä Nmap.Script.Scanner-hyökkäyksistä oli tullut testauksessa käytetyltä koneelta (ks. Kuvio 40). Skannaus ei myöskään onnistunut palvelimen suuntaan koska yhteys estettiin, kun hyökkäys havaittiin. Nämä tulokset osoittavat, että IPS-ominaisuus toimii oikein ja estää hyökkäykset tunnisteiden mukaisesti.




| # | Date/Time | Severity | Source | Protocol | User | Action | Count | Attack Name |
|---|---|---|---|---|---|---|---|---|
| 1 | 20:07:33 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 2 | 20:07:32 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 3 | 20:07:31 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 4 | 20:07:28 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 5 | 20:07:26 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 6 | 20:07:21 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 7 | 20:07:21 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 8 | 20:07:21 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 9 | 20:07:18 | | | tcp | | dropped | | Nmap.Script.Scanner |
| 10 | 20:07:17 | | | tcp | | dropped | | Nmap.Script.Scanner |

Kuvio 40. IPS-toiminnon tapahtumaloki

**AntiVirus**

Moduulin toimintaa testattiin lataamalla internetistä EICAR-testivirus, joka on tarkoitettu virustorjuntaohjelmien testaamista varten. Testivirus on käytännössä yksi .COM-tiedosto, joka voidaan pakata useita kertoja eri formaateilla vaikeuttaakseen tiedoston havaitsemista (What's an EICAR test file? 2018).

Testaamiseen käytettiin FortiNet:n omaa Malware Detection Capability testaussivustoa http://metal.fortiguard.com/ , joka hyödyntää EICAR-testinäytettä. Testi ajoi 18 eri versiota EICAR-tiedostosta, jotka pakattiin eri muotoihin kuten .zip, .rar ja 7z. Testin jälkeen tarkistettiin palomuurin AntiVirus-lokit, joista voitiin todeta, että kaikki 18 tiedostoa tunnistettiin ja niiden eteneminen estettiin (ks. Kuvio 41).

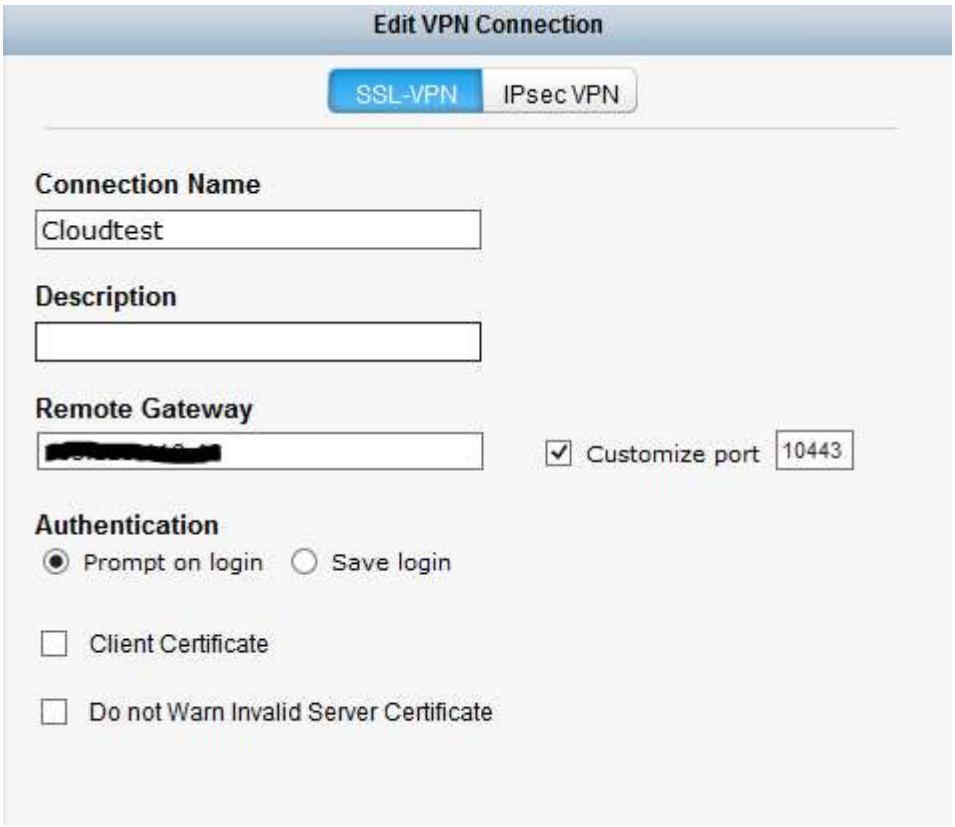
| # | Date/Time | Service | Source | File Name | Virus/Botnet | User | Details | Action |
|---|---|---|---|---|---|---|---|---|
| 1 | 20:19:35 | HTTP | 10.0.0.11 | 20180419-171504.samples.arj | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 2 | 20:19:30 | HTTP | 10.0.0.11 | 20180419-171504.samples.cab | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 3 | 20:19:25 | HTTP | 10.0.0.11 | 20180419-171504.samples.password.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 4 | 20:19:19 | HTTP | 10.0.0.11 | 20180419-171504.samples.7z | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 5 | 20:19:15 | HTTP | 10.0.0.11 | 20180419-171504.samples.rar | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 6 | 20:19:10 | HTTP | 10.0.0.11 | 20180419-171504.samples.tar.gz | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 7 | 20:19:05 | HTTP | 10.0.0.11 | 20180419-171504.samples.tar | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 8 | 20:19:00 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 9 | 20:18:55 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 10 | 20:18:50 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 11 | 20:18:45 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 12 | 20:18:40 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 13 | 20:18:35 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 14 | 20:18:31 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 15 | 20:18:26 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 16 | 20:18:21 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 17 | 20:18:17 | HTTP | 10.0.0.11 | 20180419-171504.samples.zip | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |
| 18 | 20:18:12 | HTTP | 10.0.0.11 | eicar.com | EICAR_TEST_FILE | | host: 104.236.145.4 | blocked |

Kuvio 41. EICAR-testitiedosto

Palomuurin lokeista voitiin nähdä, missä muodossa testisivu tarjosi tiedostot, ja lähteen mistä tiedostoja haettiin, joka oli tässä tapauksessa IP-osoite 10.0.0.11 palvelimella SRV-01. Testin tuloksista voitiin näin ollen todeta, että AntiVirus-moduuli toimii palomuurilla oikein.

## 6.2 Etäyhteys

SSL-VPN-yhteyden muodostusta voitiin testata FortiClient-ohjelmalla, joka mahdollistaa SSL- ja Ipsec VPN-yhteyksien muodostuksen FortiGate-tuotteisiin. Osoitteena käytetään FG-VM-01:n käyttämää julkista floating IP-osoitetta, joka on sidottu palomuurin omalle osoitteelle 172.17.0.11. VPN-palvelu konfiguroitiin kuuntelemaan portissa 10443, joten tämä täytyy muuttaa vakioportista 443.




Kuvio 42. Forticlient-asiakasohjelman yhteysmääritykset

Tunnistautumiseen hyödynnettiin LDAP-palvelinautentikointia, joka luotiin pystytyksen yhteydessä. Palvelimelle luotiin testitunnus ”Keijo”, jolle annettiin palomuurilla SSL-VPN-Full-Access-oikeudet verkkoon. Yhteyden muodostuksen jälkeen toimivuus voitiin todeta katsomalla palomuurin autentikointisessioiden aktiiviset kirjautumiset (ks. Kuvio 43).


Kuvio 43. Aktiivisen SSL-VPN-istunnon tiedot

Yhteyden muodostuksen jälkeen käyttäjällä keijo sai Forticlientin kautta oman työaseman reittitauluun reitin palvelimelle W2012-SRV-01 (10.0.0.11). SSL-VPN ja LDAP-autentikointi voitiin todeta tällä testillä toimivaksi.

## 6.3 Kahdennus

Kahdennuksen testaamisessa rakennetuilla topologioilla ei saatu muodostettua yhteyttä eri saatavuusalueiden palvelinten välille hyödyntämällä OpenStack:in Neutronin reitittimiä. Paketit testin aikana jäivät siirtoverkkoon näiden alueiden välillä eivätkä koskaan päässeet palomuurille asti. Tämä todennettiin vastapuolen palomuurilla aktivoimalla liikenteen vianmääritys seuraavilla komennoilla:

*diagnose debug reset*
*diagnose debug flow filter addr 10.0.1.11*
*diagnose debug enable*
*diagnose debug flow trace start 100*

Palomuurit eivät myöskään pystyneet kommunikoimaan keskenään WAN-osoitteiden kautta 172.x.x.x-verkoista. Neutronin reitittimiltä liikennettä ei ollut mahdollista seurata millään tasolla, joten syyn selvittäminen jäi mahdottomaksi.

Kahdennusta varten testattiin myös IPSec site-to-site VPN-tunnelin rakentamista palomuurien välille julkiverkon yli (ks. Liite 4). Palomuureille tehtiin policy-määritys, jolla kryptataan palvelinten 10.0.0.11 ja 10.0.1.11 liikenne (ks. Kuvio 44).

```
FG-VM-01 # get vpn ipsec tunnel details

gateway
  name: 'AZ-S2S'
  type: route-based
  local-gateway: 172.17.0.11:4500 (static)
  remote-gateway: 84.239.153.255:4500 (static)
  mode: ike-v1
  interface: 'port1' (3)
  rx  packets: 0  bytes: 0  errors: 0
  tx  packets: 0  bytes: 0  errors: 0
  dpd: on-demand/negotiated  idle: 20000ms  retry: 3  count: 0
  nat traversal mode: keep-alive   RFC 3947   interval: 10
  selectors
    name: 'AZ-S2S'
    auto-negotiate: disable
    mode: tunnel
    src: 0:10.0.0.11/255.255.255.255:0
    dst: 0:10.0.1.11/255.255.255.255:0
```

Kuvio 44. IPsec-tunnelin tiedot

Molemmille palomuureille oli tarpeellista myös luoda staattiset reitit toistensa luo seuraavilla komennoilla:

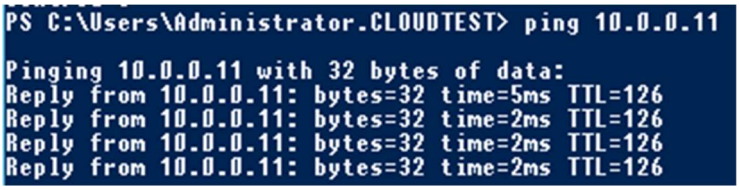
**FG-VM-02**

*configure router static*
*edit 1*
*set dst 10.0.0.0 255.255.255.0*
*set device AZ-S2S*

**FG-VM-01**

*configure router static*
*edit 1*
*set dst 10.0.1.0 255.255.255.0*
*set device AZ-S2S*

Toimintaa voitiin testata ping-komennolla suoraan palvelimelta palvelimelle (ks. Kuvio 45). Tuloksesta voitiin todeta, että yhteys saatavuusalueiden välille voitiin muodostaa VPN-tunnelin avulla.



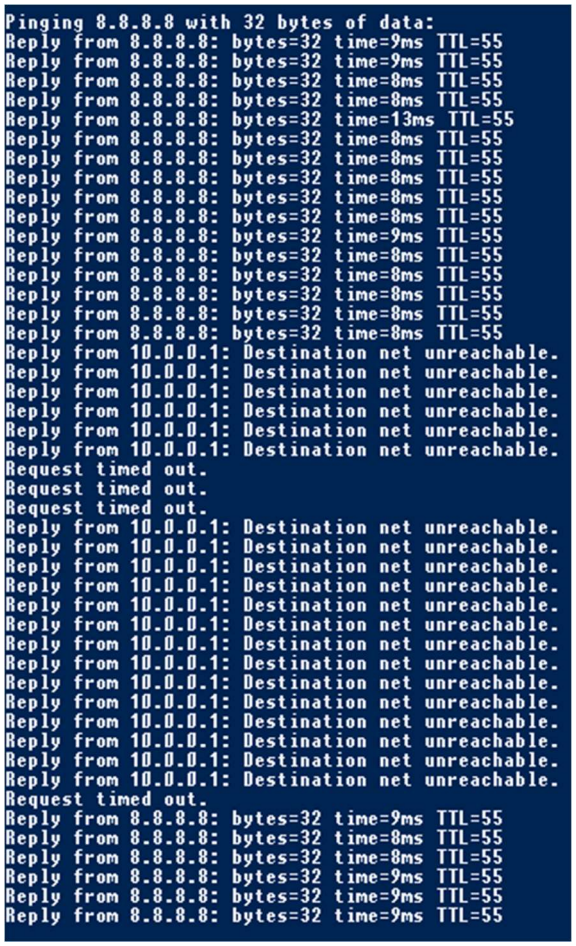

Kuvio 45. Yhteyden testaus

Kun yhteys saatavuusalueiden välille oli muodostettu, voitiin palvelimet replikoida tunnelin yli kulkevaa yhteyttä hyödyntäen. Replikointi testattiin palvelinten SRV1 ja SRV2 välillä ja tämä saatiin onnistuneesti suoritettua. Lopputilanne oli se, että molemmilla palvelimilla oli oma floating IP, johon voitiin ottaa julkiverkosta yhteys ja palvelimien replikointi tapahtui IPsec-tunnelin kautta.

## 6.4 Palautuminen ja ylläpito

**Snapshot**

Ensimmäisessä vaiheessa haluttiin testata palomuuri-instanssin palautusta snapshot-ominaisuudella. Kohteeksi otettiin FG-VM-02-instanssi, josta otettiin snapshot valmiista tilasta ja tehtiin toimintakelvottomaksi poistamalla sen rajapinnat LAN- ja WAN-suuntaan. Testin ajaksi laitettiin ping-komento palvelimelta W2012-SRV-02 toistamaan kohti julkiverkkoa (ks. Kuvio 46) ja aikaa snapshotin palautukseen otettiin sekuntikellolla.



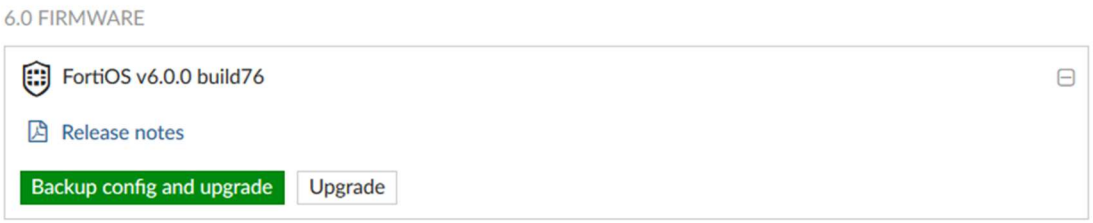

Kuvio 46. Ping-testi

Aikaa toimintakyvyn palautumiseen snapshotin palautuksella kesti sekuntikellon mukaan 1 minuutti ja 21 sekuntia. Snapshotin palautuksen jälkeen liikenne palvelimelta toimi normaalisti.

**Laiteohjelmiston päivitys**

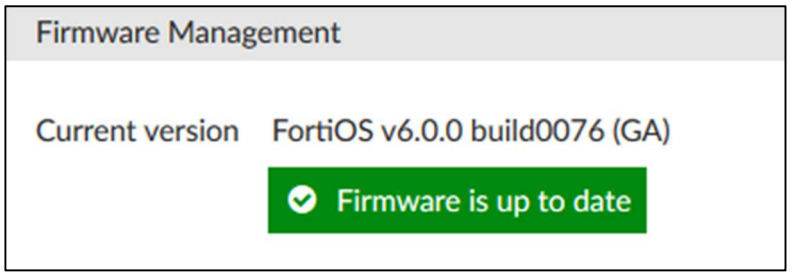
Seuraavassa vaiheessa testattiin palomuuri-instanssin laiteohjelmiston päivitysprosessia. Testaushetkellä palomuurilla oli ajossa FortiOS 5.6.3 ja uusin päivitys oli saatavilla versioon FortiOS 6.0.0. Tässä osiossa haluttiin testata

palomuurin päivitystä suoraan graafisen käyttöliittymän kautta sen oman päivitysohjelman avulla (ks. Kuvio 47)




Kuvio 47. FortiOS 6.0 päivitys

Palomuurilta otettiin talteen nykyiset konfiguraatiot ja aloitettiin päivittäminen. Uudelleenkäynnistyksen jälkeen palomuuri oli päivittynyt uusimpaan versioon ja tämä tapahtui erittäin nopeasti (ks. Kuvio 48)

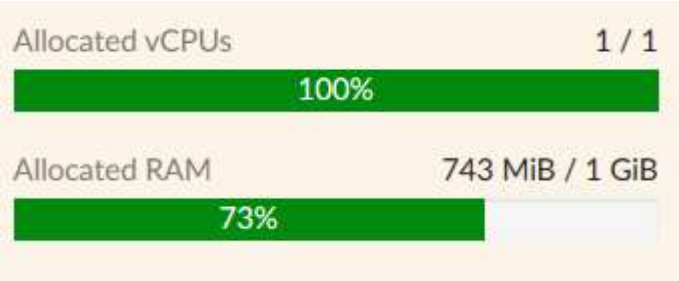



Kuvio 48. FortiOS 6.0 päivitys valmis

**Resurssien lisäys**

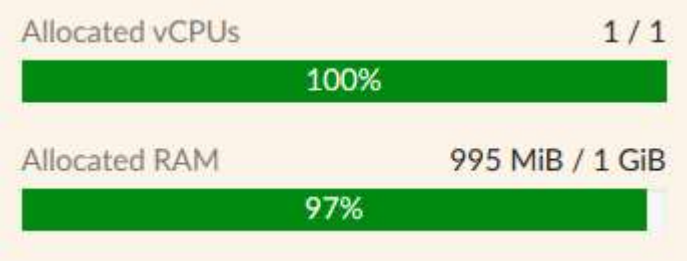
Viimeisessä vaiheessa testattiin palomuuri-instanssin resurssien lisäämistä lennosta. Instanssi asennettiin pienimmällä mahdollisella resurssimäärällä ja päivitettiin tehokkaampaan. Resurssien päivittäminen tapahtuu Horizonin hallinnan kautta, jossa instanssille voidaan allokoida uusi resurssipaketti.

Alkutilanne: 1 vCPU, 768MB RAM ja 32GB leytilaa. (ks. Kuvio 49)




Kuvio 49. Resurssipaketti 1

Päivityksen jälkeen: 1 vCPU, 1GB RAM ja 32GB levytilaa. (ks. Kuvio 50)




Kuvio 50. Resurssipaketti 2

Resurssipaketin vaihto onnistui helposti ja nopeasti käyttämällä OpenStack:in Horizon-hallintaa. Päivittäminen vaati ainoastaan palomuuri-instanssin käynnistämisen uudelleen, jonka jälkeen uusi resurssipaketti oli käytettävissä. Mitään ongelmia päivityksen jälkeen ei ilmennyt.

# 7 Testitulosten ja sopivuuden analysointi

## 7.1 Havainnot

Yhteensopivuus OpenStack-alustan kanssa voitiin todeta erinomaiseksi. Käyttöönoton kanssa ei ilmennyt juuri mitään ongelmia ja käyttöönotto vastasi mitä tahansa muuta virtualisointialustaa helppoudellaan. Neutronin verkko-ominaisuudet olivat helppoja määrittää ja uusien aliverkkojen luontiin ei tarvinnut nähdä vaivaa. Ainoa huomioonotettava asia yhteensopivuudessa ilmeni julkisten IP-osoitteiden kanssa. Testivaiheessa käytettiin esimerkkinä web-palvelinta, johon haluttiin saada yhteys julkiverkosta siten, että liikenne kulkisi myös palomuurin kautta. Koska palvelimille ei pystytä reitittämään suoraan julkista IP-osoitetta, joudutaan tyytymään Neutronin static NAT -määritykseen joka allokoi yhden julkisen IP-osoitteen sen lohkosta vastaamaan palvelimen sisäverkon osoitetta. Tämä jouduttiin kiertämään määrittämällä julkinen osoite palomuurille ja luomaan uusi NAT-sääntö palomuurille, joka muuttaa sille tulleet paketit siten, että ne vastaavat palvelimen sisäverkon osoitetta. Eli käytännössä paketille tehdään osoitemuunnos kahteen kertaan. Tämä johtaa luonnollisesti joissakin tilanteissa ongelmiin koska palvelimelle kohdistuva julkiverkon liikenne on ainoastaan porttiohjausta tekevän port forwarding -toiminteen varassa. Tämä ei myöskään ole välttämättä kovin hyvä asia käyttöönoton helppouden kannalta.

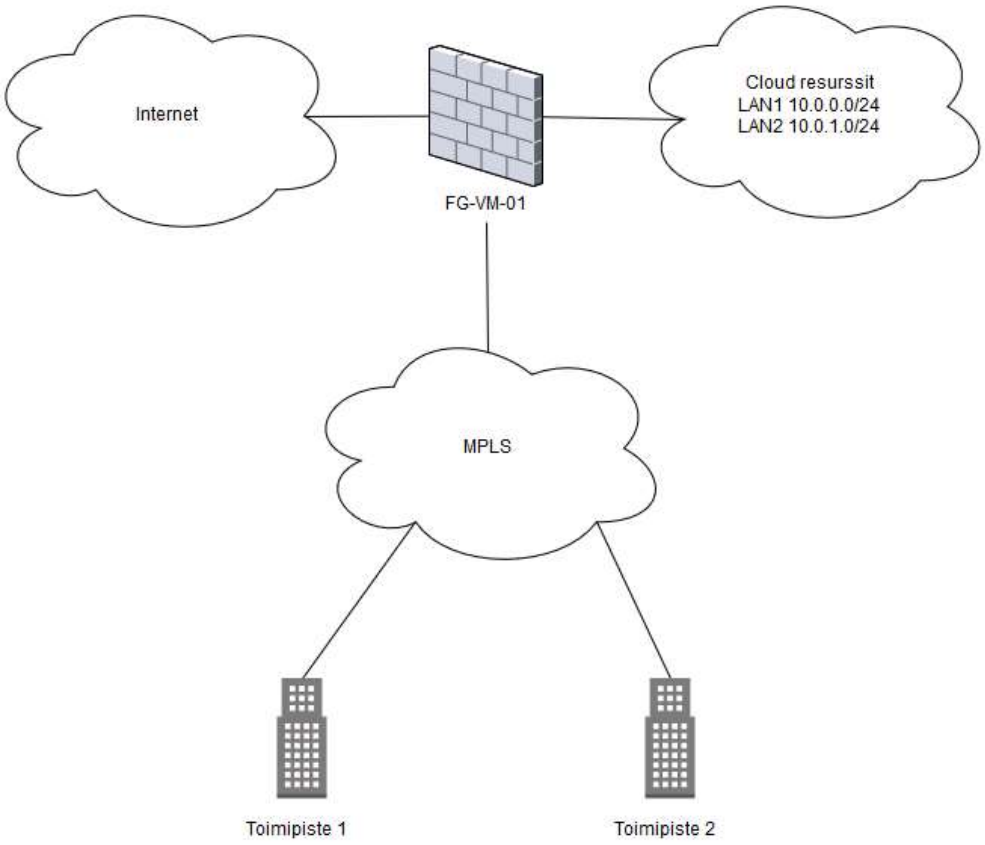
Kesken työn törmättiin kerran ongelmaan, joka johti lähestulkoon työn aloittamiseen alusta palomuuri-instanssien kanssa. Molemmat palomuurit olivat lakanneet vastaamasta mihinkään hallintapyyntöihin lukuisista uudelleenkäynnistyksistä huolimatta. Tässä vaiheessa törmättiin myös toiseen ongelmaan, joka koski OpenStack:in konsoliyhteyttä. Palomuureille oli asetettu erittäin monimutkaiset salasanat, jotka sisälsivät paljon erilaisia erikoismerkkejä ja kun palomuureille yritettiin päästä konsoliyhteydellä kiinni, havaittiin että OpenStack:in konsoliyhteys ei pysty kirjoittamaan tiettyjä erikoismerkkejä joita salasanoissa oli. Instanssit jouduttiin siis rakentamaan uusiksi osittaisen konfiguraatiovarmuuskopion pohjalta.

Palomuurien yhteyksien katkeamisen juurisyy jäi tuntemattomaksi, koska konsoliyhteyttä ei päästy muodostamaan virtuaalikoneille.

Yleisellä tasolla voitiin sanoa, että testaukset olivat kaikin puolin onnistuneita. Kaikki testaukseen liittyvät ominaisuudet saatiin toimimaan ilman juuri minkäänlaisia ongelmia. Ainoa ongelma testauksessa ilmeni saatavuusalueiden välisessä liikennöinnissä. Ongelma hyvin epätodennäköisesti jäi OpenStack:in Neutronin reitittimien reititysongelmaksi koska reitittimien reititysominaisuudet toimivat muuten normaalisti. Saatavuusalueiden välistä liikennöintiä Neutronin reitittimillä ei lähdetty tässä työssä tutkimaan syvemmin toimeksiantajan siirtoverkossa, koska selvitys menee toimeksiannon ulkopuolelle. Saatavuusalueiden välille saatiin kuitenkin muodostettua VPN-tunneli, joka ajaa tässä tapauksessa lähes saman asian, joten sen osalta testi oli onnistunut.

Palautumisen ja ylläpidon kannalta ei esiintynyt minkäänlaisia ongelmia. Snapshotin nopea palautuminen yllätti myös tekijän positiivisesti. Ohjelmistopäivitys ja resurssipakettien lisäyksessä selvittiin ainoastaan palomuurin uudelleenkäynnistyksellä. NGFW-ominaisuuksista toimi testien osalta kaikki. Ominaisuudet oli helppo aktivoida käyttöön ja mitään ongelmia testien aikana ei ilmennyt. Etäyhteyden käyttöönotto SSL-VPN:llä oli vaivatonta ja käyttöönotto vastasi samaa mitä fyysisellä palomuurilla. LDAP-autentikointi palvelimen kanssa toimi myös vaivattomasti.

Koska Cloud 9 tukee pilviprojektin liittämistä MPLS-verkkoon, palomuuria voitaisiin hyödyntää myös porttina esimerkiksi asiakkaiden toimipisteiden liikenteen reitittämiselle ja suodatukselle. Mahdollisuus olisi rakentaa MPLS-verkko, joka reitittää yhden VRF:n sisällä liikenteen oletusreitin mukaan virtuaalipalomuurin rajapinnalle ja siitä eteenpäin internetiin (ks. Kuvio 51). Ratkaisu mahdollistaisi myös toimipisteiden liikennöinnin VRF:n sisällä pilviresursseihin käytännössä yhdessä ja samassa lähiverkossa. Tämä vaatisi kuitenkin keskittymistä syvemmin toimeksiantajan siirtoverkkoon, joka taas ei ollut tämän toimeksiannon pääpaino.




Kuvio 51. MPLS-ratkaisu

## 7.2 Kehitysideat

Mitä tulee kehitysideoihin OpenStack:in osalta, olisi syytä kiinnittää huomioon Neutronin toimintaan. Neutron tukee tällä hetkellä julkisten IP-osotteiden osalta ainoastaan floating IP-ominaisuutta, joka perustuu yksinkertaiseen static NAT-muunnokseen. Yksi mahdollisuus tälle olisi kehittää ominaisuus Neutronin reitittimille, joka mahdollistaa jukisten IP-osotteiden reitittämisen suoraan palvelimien käyttöön.

Ongelmat konsoliyhteyden kanssa myös nostivat esille tarpeen muutokselle. Monimutkaiset salasanat palomuureille oli generoitu KeePass-salasananhallintaohjelmalla ja salasanan tyyppi oli sitä luokkaa, minkä pitäisi sopia jokaiseen paikkaan. Erikoismerkkien käytön rajoitus alentaa tietoturvaa.

Muita kehitysideoita ei tekijälle juuri ilmennyt. OpenStack oli työn toimeksiannon tekohetkellä erittäin yhteensopiva monien eri järjestelmien kanssa ja tämä näkyi käyttöönoton helppoudessa ja vaivattomuudessa.

# 8 Pohdinta

Toimeksianto oli osittain haastava sen vuoksi, että vaatimusmäärittelyt olivat melko suppeat alkuun ja aiheita jouduttiin keksimään lisää sitä mukaa kun työ edistyi. Siitä huolimatta virtuaalipalomuurin ominaisuudet saatiin lähes kokonaan testattua ja todettua toimiviksi onnistuneesti.

Aihealueena ja käytännössä FortiGate ja OpenStack olivat tekijälle erittäin tuttuja johtuen niiden päivittäisestä käytöstä työtehtävissä. Kokemusta fyystisten FortiGate -laitteiden konfiguroimisesta oli myös paljon, joka näkyi myöskin käyttöönoton helppoudessa. Virtuaalipalomuurin käyttöönotto vastasi lähes identtisesti fyysisen palomuurin käyttöönottoa, pois lukien pilviosio. Toimeksianto opetti tekijälle kuitenkin paljon uutta muun muassa FortiGate:n edistyneimpien ominaisuuksien kanssa. Koska toimeksiantoa varten tekijä sai täysversion FortiGate VM:n lisenssistä, päästiin testaamaan myös muun muassa Palomuurin NGFW-ominaisuuksia joihin lukeutuvat esimerkiksi IPS- ja suodatusominaisuudet. Näistä tiedoista on tekijälle varmasti hyötyä tulevaisuudessa.

Eniten aikaa vaativa selvitys oli, että miten palvelimille kohdistuva liikenne saadaan ohjattua palomuurin läpi, ilman että se ohitetaan suoralla osoitteenmuutoksella. Selvitykseen auttoivat pakettien tutkimiset palvelimilla hyödyntäen Wireshark-paketinkaappausohjelmaa. Myös virtuaalipalomuurit sisälsivät hyvät työkalut pakettien flow-seurantaan.

Työ oli mielestäni onnistunut siinä määrin, että testaustuloksista voidaan todeta toteutettujen virtuaalipalomuurien olevan täysin varteenotettava vaihtoehto tuotantoa varten. Toteutus vaatii kuitenkin paljon osaamista eri osa-alueilta, joten mikäli tuotetta myytäisiin IaaS-ratkaisuna, vaatisi käyttöönotto paljon osaamista myös käyttäjän osalta.

# Lähteet

Firewalls and Their Evolution. 2018. Palo alto Cyberpedia. Viitattu 6.5.2018. https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

How does cloud computing work? 2018. Zdnet-artikkeli. Viitattu 17.5.2018. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

IaaS, PaaS, SaaS? 2016. Planeetta-blog. Viitattu 17.5.2018. https://blog.planeetta.net/iaas-paas-saas

Intrusion Prevention and Detection System Basics. 2018. Paloalto Cyberpedia. Viitattu 6.5.2018 https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Mikä ihmeen PaaS? 2014. Cybercom Group-blog. https://www.cybercom.com/fi/Suomi/Yritys/Blogit/Blogit/Mika-ihmeen-PaaS/

Software as a Service (SaaS). 2016. Techtarget-sivusto. https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

Stateful vs. Stateless Firewalls. 2017. TcPSolution. Vittattu 8.5.2018. https://tcpsolution.com/stateful-vs-stateless-firewalls/

Virtual machines. 2018. VirtualBox-wiki. Viitattu 17.5.2018. https://www.virtualbox.org/wiki/Virtualization

What Is a VPN? - Virtual Private Network. 2018. Cisco.com Viitattu 8.5.2018 https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

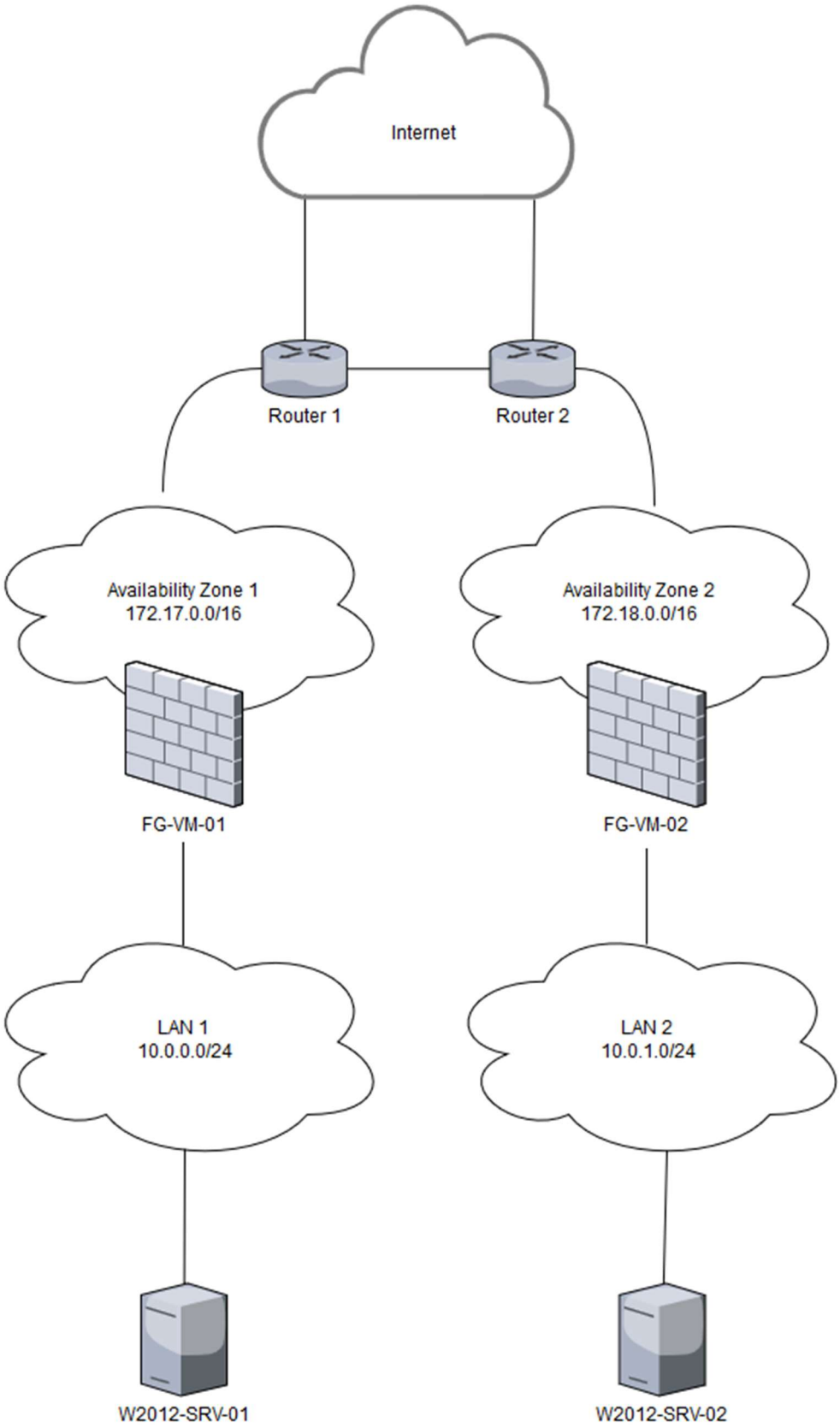
What’s an EICAR test file? 2018. FortiNet-sivusto. Viitattu 16.5.2018. http://metal.fortiguard.com/

What is OpenStack? 2018. Opensource.com-sivusto. Viitattu 19.2.2018. https://azure.microsoft.com/en-us/overview/what-is-iaas/

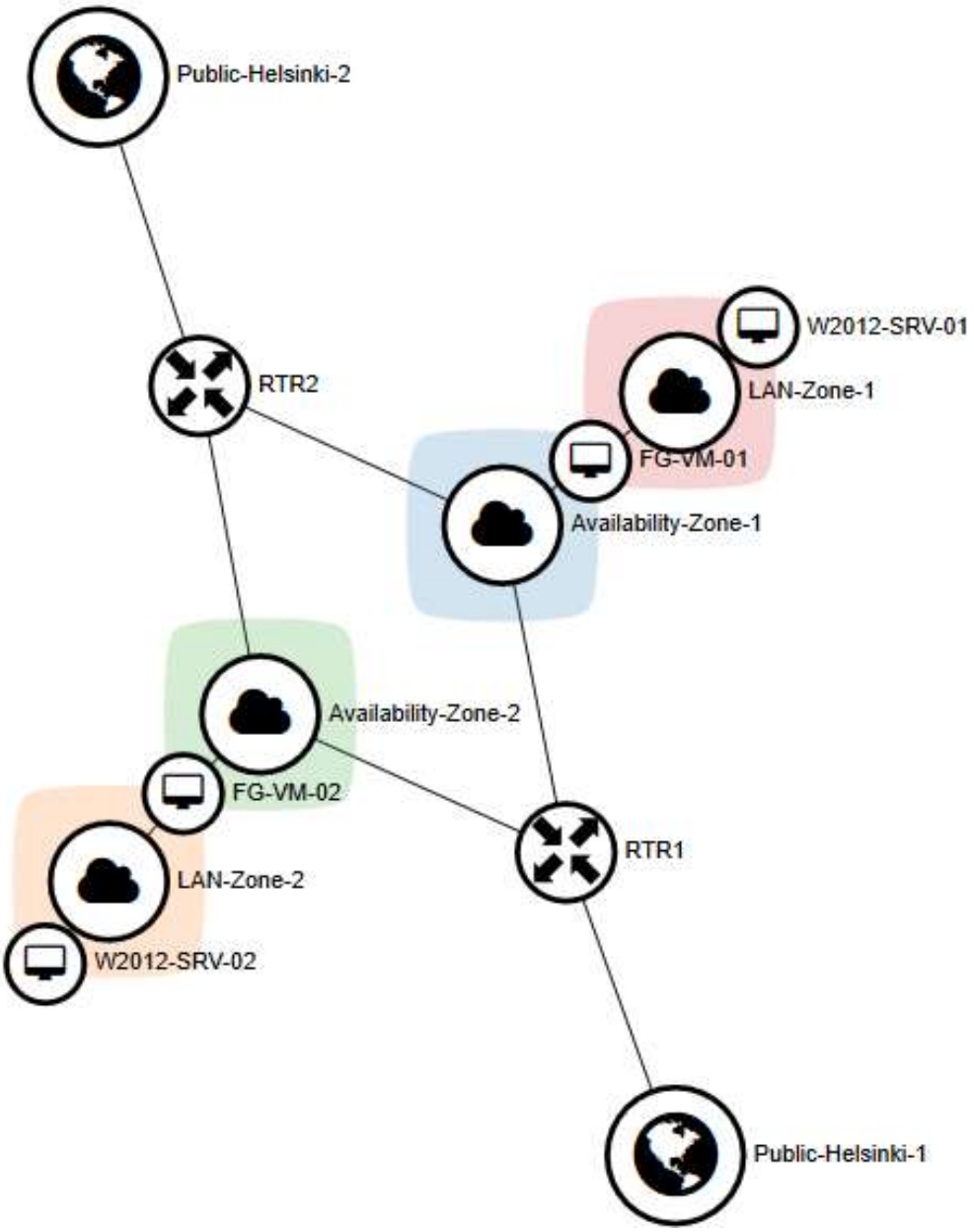
What is virtualization? 2018. Redhat topics. Viitattu 14.5.2018. https://www.redhat.com/en/topics/virtualization

# Liitteet

Liite 1. Verkkotopologian suunnitelma



Liite 2. Toteutettu verkkotopologia



Liite 3. Palomuurisäännöt

```
FG-VM-01 # show firewall policy
config firewall policy
    edit 6
        set name "SRVtoSRV"
        set uuid 4d675dae-2f6c-51e8-e071-d762d879ca07
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "10.0.0.11-SRV1"
        set dstaddr "10.0.1.11-SRV2"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 1
        set name "AllowSRVtoInternet"
        set uuid 16b02606-13dd-51e8-3c45-335fe2eccf9c
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "10.0.0.11-SRV1"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set av-profile "AV-Profile1"
        set webfilter-profile "SFW"
        set dnsfilter-profile "DNS-Filter1"
        set application-list "APP-CTRL1"
        set profile-protocol-options "default"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
    next
    edit 2
        set name "AllowOutsideWebAccessSec"
        set uuid 73edeeb6-13e2-51e8-f940-daca698c1d1e
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "172.17.0.11-10.0.0.11-TCP/8080-NAT"
        set action accept
        set schedule "always"
        set service "TCP/8080"
        set utm-status enable
        set ips-sensor "high_security"
        set ssl-ssh-profile "certificate-inspection"
    next
```

```
edit 3
    set name "SSL-VPN-FullAccess"
    set uuid 29b501c4-189a-51e8-caf8-aa0eba80578d
    set srcintf "ssl.root"
    set dstintf "port2"
    set srcaddr "SSLVPN_TUNNEL_ADDR1"
    set dstaddr "10.0.0.11-SRV1"
    set action accept
    set schedule "always"
    set service "ALL"
    set groups "SSL-VPN-Full-Access"
next
edit 4
    set name "SSL-VPN-WebAccess"
    set uuid d0333672-1a27-51e8-28f5-bc06511b8558
    set srcintf "ssl.root"
    set dstintf "port2"
    set srcaddr "SSLVPN_TUNNEL_ADDR1"
    set dstaddr "10.0.0.11-SRV1"
    set action accept
    set schedule "always"
    set service "TCP/8080"
    set groups "SSL-VPN-Web-Access"
next
edit 5
    set name "AllowOutsideWebAccessPri"
    set uuid 135f1eee-1a31-51e8-03de-da026976b3a0
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "172.17.0.11-10.0.0.11-TCP/80-NAT"
    set action accept
    set schedule "always"
    set service "HTTP"
    set utm-status enable
    set ips-sensor "protect_http_server"
    set ssl-ssh-profile "certificate-inspection"
next
edit 7
    set name "SRVtoSRV-in"
    set uuid ddd869b4-2f6c-51e8-8c44-2839794f1d47
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "10.0.0.11-SRV1"
    set action accept
    set schedule "always"
    set service "ALL"
next
```

```
    edit 8
        set name "AllowAZ-S2S-OUT"
        set uuid fb6d7568-3968-51e8-8d72-86a691866fa7
        set srcintf "port2"
        set dstintf "AZ-S2S"
        set srcaddr "10.0.0.11-SRV1"
        set dstaddr "10.0.1.11-SRV2"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 9
        set name "AllowAZ-S2S-IN"
        set uuid 967bca76-396b-51e8-1165-8cb98f4308c3
        set srcintf "AZ-S2S"
        set dstintf "port2"
        set srcaddr "10.0.1.11-SRV2"
        set dstaddr "10.0.0.11-SRV1"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end


FG-VM-02 # show firewall policy
config firewall policy
    edit 2
        set name "SRVtoSRV"
        set uuid 8dad5daa-2f6c-51e8-513f-e896e9fe4fc0
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "10.0.1.0/24-SRV2"
        set dstaddr "10.0.0.0/24-SRV1"
        set action accept
        set status disable
        set schedule "always"
        set service "ALL"
    next
    edit 1
        set name "AllowSRVtoInternet"
        set uuid 0a32e4ea-2f6c-51e8-03fd-c33b08dae383
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "10.0.1.0/24-SRV2"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
```

```
        set nat enable
    next
    edit 3
        set name "SRVtoSRV-in"
        set uuid c9e333bc-2f6c-51e8-4b07-12f38721f295
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "10.0.1.0/24-SRV2"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 4
        set name "AllowAZ-S2S"
        set uuid a81dee82-3969-51e8-6164-f51931cce04c
        set srcintf "port2"
        set dstintf "AZ-S2S"
        set srcaddr "10.0.1.0/24-SRV2"
        set dstaddr "10.0.0.0/24-SRV1"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 5
        set name "AllowAZ-S2S-src"
        set uuid 7ac8d4fe-396b-51e8-fc15-87b9a4fe913c
        set srcintf "AZ-S2S"
        set dstintf "port2"
        set srcaddr "10.0.0.0/24-SRV1"
        set dstaddr "10.0.1.0/24-SRV2"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Liite 4. IPsec VPN konfiguraatiot

```
FG-VM-01 # show full-configuration vpn ipsec phase1-interface
config vpn ipsec phase1-interface
   edit "AZ-S2S"
      set type static
      set interface "port1"
      set ip-version 4
      set ike-version 1
      set local-gw 0.0.0.0
      set keylife 86400
      set authmethod psk
      set mode main
      set peertype any
      set passive-mode disable
      set exchange-interface-ip disable
      set mode-cfg disable
      set proposal aes256-sha256
      set localid ''
      set localid-type auto
      set auto-negotiate enable
      set negotiate-timeout 30
      set fragmentation enable
      set dpd on-demand
      set forticlient-enforcement disable
      set comments ''
      set npu-offload enable
      set dhgrp 5
      set suite-b disable
      set wizard-type custom
      set xauthtype disable
      set mesh-selector-type disable
      set idle-timeout disable
      set ha-sync-esp-seqno enable
      set auto-discovery-sender disable
      set auto-discovery-receiver disable
      set auto-discovery-forwarder disable
      set encapsulation none
      set nattraversal enable
      set rekey enable
      set remote-gw 84.239.153.255
      set monitor ''
      set add-gw-route disable
      set psksecret ENC
IJ0e22mPYc02gzN5ZZuOVaWFkj5gOw8pVY0z9xoc3ImBOQlEQq582plDfGt0cRqhkP7w
M22gf/rryKFz7TCCJFcGPIAc-
GHzuxJnQUL/rFJg5jWE/vSmVigXa/W8W9ft83WEGnM5aRDs5Q0cEe-
gDUW38HxpeVbsKXgXNTanCeVua9TuGMw/PCckjgNaniA1f4u3972w==
```

```
        set keepalive 10
        set dpd-retrycount 3
        set dpd-retryinterval 20
    next
end


FG-VM-01 # show full-configuration vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "AZ-S2S"
        set phase1name "AZ-S2S"
        set proposal aes256-sha256
        set pfs enable
        set dhgrp 5
        set replay enable
        set keepalive disable
        set auto-negotiate disable
        set auto-discovery-sender phase1
        set auto-discovery-forwarder phase1
        set keylife-type seconds
        set encapsulation tunnel-mode
        set comments ''
        set protocol 0
        set src-addr-type subnet
        set src-port 0
        set dst-addr-type subnet
        set dst-port 0
        set keylifeseconds 43200
        set src-subnet 10.0.0.11 255.255.255.255
        set dst-subnet 10.0.1.11 255.255.255.255
    next
end

FG-VM-02 # show full-configuration vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "AZ-S2S"
        set type static
        set interface "port1"
        set ip-version 4
        set ike-version 1
        set local-gw 0.0.0.0
        set keylife 86400
        set authmethod psk
        set mode main
        set peertype any
        set passive-mode disable
        set exchange-interface-ip disable
        set mode-cfg disable
        set proposal aes256-sha256
```

```
        set localid ''
        set localid-type auto
        set auto-negotiate enable
        set negotiate-timeout 30
        set fragmentation enable
        set dpd on-demand
        set forticlient-enforcement disable
        set comments ''
        set npu-offload enable
        set dhgrp 5
        set suite-b disable
        set wizard-type custom
        set xauthtype disable
        set mesh-selector-type disable
        set idle-timeout disable
        set ha-sync-esp-seqno enable
        set auto-discovery-sender disable
        set auto-discovery-receiver disable
        set auto-discovery-forwarder disable
        set encapsulation none
        set nattraversal enable
        set rekey enable
        set remote-gw 185.123.118.46
        set monitor ''
        set add-gw-route disable
        set psksecret ENC
8gXTubURdH/HiD3IVJZf9KZBW+2i94ZZh3QYX+px+wr24uyPTV+I9T4MWDQHuviXTUm
fVU-
ZovPwa9VhN6xQd2ARRQDmjG3A2YWz3pS/C8rS9+bqDpk+/DbwgbtwwXwlh0nfvmLj
D9oKkS/XbNSd5FKt14+DzcdoeAAR/EY5kh5M/QRyROdyPtyqQfH2BJM/Bqp7aJQ==
        set keepalive 10
        set dpd-retrycount 3
        set dpd-retryinterval 20
    next
end


FG-VM-02 # show full-configuration vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "AZ-S2S"
        set phase1name "AZ-S2S"
        set proposal aes256-sha256
        set pfs enable
        set dhgrp 5
        set replay enable
        set keepalive disable
        set auto-negotiate disable
        set auto-discovery-sender phase1
        set auto-discovery-forwarder phase1
```

```
        set keylife-type seconds
        set encapsulation tunnel-mode
        set comments ''
        set protocol 0
        set src-addr-type subnet
        set src-port 0
        set dst-addr-type subnet
        set dst-port 0
        set keylifeseconds 43200
        set src-subnet 10.0.1.11 255.255.255.255
        set dst-subnet 10.0.0.11 255.255.255.255
    next
end
```