Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

TELEKOMUNIKAZIO TEKNOLOGIEN INGENIARITZA GRADUA

GRADU AMAIERAKO LANA

SARE KORPORATIBO BATENTZAKO SEGURTASUN EBAZPEN ZENTRALIZATU ETA AUTOMATIZATUA

Ikaslea: Abrisqueta Sanchez, Unai

Zuzendaria : Astorga Burgo, Jasone

Ikasturtea: 2018-2019

Data: Bilbon, 2019ko ekainaren 26a

Laburpena

Proiektu honen helburua sare korporatibo batean segurtasun mekanismo sendoak inplementatzea eta sarea automatizatzea da. Proiektu Honen arrazoia automatizazioa eta sare korporatiboen segurtasuna gero eta garrantzi handiago dutela gaur egungo gizartean da, erabiltzaileen kopuruaren igoera dela eta. Ondorioz, zerbitzu telematiko gehiago daude eta zerbitzu hauek automatizatu eta babestu behar dira. Helburuak lortzeko ebazpen posible ezberdinak aztertuko dira, ebazpen hoberena aukeratzeko. Behin ebazpena aukeratuta, proiektuaren espezifikazioetan oinarrituta egongo den ebazpena diseinatuko da. Horretarako, segurtasun mekanismo berriak diseinatuko dira, segurtasun ekipamendu berriak instalatuko dira eta diseinatutako mekanismoak inplementatuko dira. Gainera, programa bat garatuko da sarearen segurtasun arauen sorrera automatizatzeko.

Hitz gakoak: Segurtasuna, automatizazioa, suebakia, segurtasun arauak, segurtasun mekanismoak, sarea.

Resumen

El objetivo de este proyecto es la implementación de mecanismos de seguridad y la automatización de la red corporativa. La razón de esto es principalmente la importancia que ha tomado la securización de las redes corporativas y la automatización de las mismas. Esto se debe al creciente número de usuarios en la red que implica que haya más servicios telemáticos y que haya que proteger y automatizarlos. Para lograr los objetivos, se analizarán las diferentes soluciones con el fin de elegir la mejor. Una vez se haya elegido la solución, se diseñará está acorde a las especificaciones del proyecto. Para ello, se diseñarán mecanismos de seguridad y se instalará equipamiento nuevo de seguridad y se implementaran nuevos mecanismos de seguridad. Además, se desarrollará un programa que automatizará la creación de reglas de seguridad.

Palabras claves: Seguridad, automatización, cortafuegos, reglas de seguridad, mecanismos de seguridad, red.

Abstract

The aim of this project consists on the implementation of security mechanisms and the automation of the corporative network. The reason for that is the importance that the corporative network securization has taken in the society. This belong to the increasing number of network users which implies that the network telematics services are increasing and these have to be secured and protected. To get the objectives different solutions will be analyzed in order to find the best solution. Once the solution is chosen, it will be designed a solution based on the project specifications. For that new security equipment will be installed and security mechanisms will be designed. Moreover, a script will be developed which will automatize the creation of security rules.

Key words: Security, automation, firewall, security rules, security mechanisms, network.

Aurkibidea

Irudien aurkibidea

Taulen aurkibidea

Akronimoak

VPN	**Virtual Private Network**
IPS/IDS	**Intrusion prevention/detection system**
IKT	**Informatika eta komunikazio teknologiak**
BPG	**Barne proruktu gordina**
DoS	**Denial of Service**
SW	**Software**
SQL	**Structured Query Language**
API	**Application Programming Interface**
HTTP	**HyperText Transfer protocol**
HTTPS	**HyperText Transfer protocol Secure**
ACL	**Access Control List**
GUI	**Graphic User Interface**
VLAN	**Virtual Local Area Network**
XML	**eXtensible Markup Lenguage**
JSON	**JavaScript Object Notation**
MPLS	**Multiprotocol Label Switching**
VSS	**Virtual Switching System**
VDOM	**Virtual Domain**
ADOM	**Administrative Domain**
CPD	**Centro de procesamiento de datos**
UTM	**Unified Threat Management**
HA	**High Availability**
IP	**Internet Protocol**
URL	**Uniform Resource Localizator**
SSL	**Secure Sockets Layer**
CSV	**comma-separated values**
DHCP	**Dynamic Host Configuration Protocol**
DNS	**Domain Name System**

1.Sarrera

Telekomunikazio ingeniaritza urrutiko komunikazioa ahalbidetzen dituzten teknologiak, mekanismoak eta protokoloak batzen ditu. Baliabide hauek erabiliz komunikazio azkarra, kalitatezkoa eta segurua lortzen da.

Urrutiko komunikazio hauek babestu behar dira, erasoak edo informazioaren xurgapena ez jasateko. Beraz, hor jaiotzen da zibersegurtasun terminoa. Termino honek ordenagailu azpiegitura baten babesa definitzen du, era zehatzago batean, azpiegitura honek gordetzen edo garraiatzen duen informazioaren babesaren berma da. Segurtasun informatiko hau bermatzeko protokolo, irizpide eta tresneria ezberdinak erabiltzen dira.

Protokoloen bidez, komunikazio arautua lortzen da. Arau multzo horiei protokoloa deritze. Protokolo bakoitzak funtzio ezberdinak ditu eta hauen multzo bat segurtasuna bermatzeko erabili edo sortu dira.

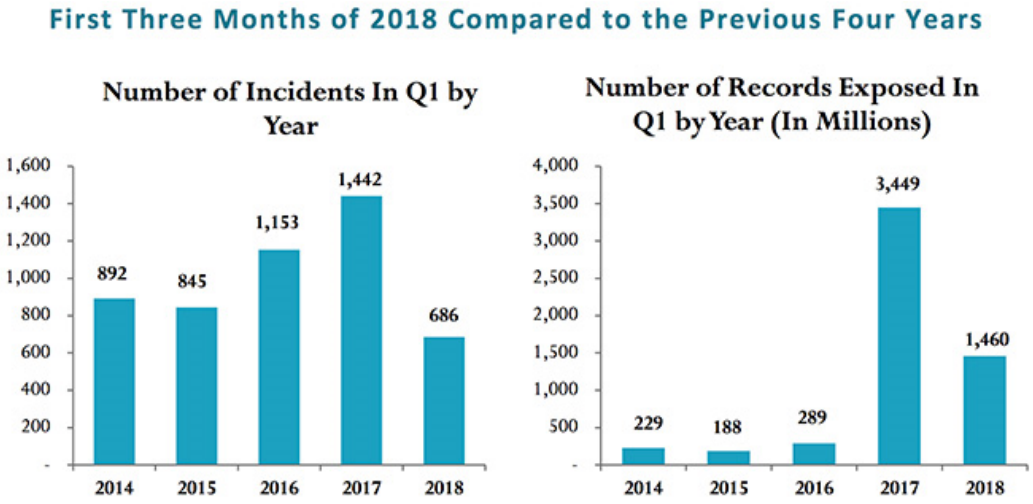
Halaber, kontuan eduki behar da segurtasuna inplementatzeko irizpidea, ingurumen ezberdinen arabera segurtasuna era batean edo bestean bermatu nahi dugu. Hau lortzeko zerbitzu ezberdinak ahalbidetuz, aplikazio jakin batzuk ahalbidetuz edo webgune jakin batzuk blokeatuz.

Protokolo hauek eta irizpide ezberdinen pertsonalizazioa ahalbidetzeko tresneria erabiltzen da. Tresneria hau birtuala edo fisikoa izan daiteke; hau da, Software soilik izatea edo Hardware ere izatea. Tresneria birtuala zerbitzarietan integratzen da; aldiz, tresneria fisikoa makineria izaten da.

Software soilik dituzten makinak, makina birtualak dira eta makina birtual hauetan makina fisiko baten funtzionaltasunak inplementatzen dira; normalean, zerbitzari batean integratuta. Fisikoak; aldiz, Rack batean instalatzen diren ekipoak dira.

Enpresa guztiek (edozein motakoak edo tamainakoak) gero eta aktibo digital gehiago dituzte eta euren negozioa gero eta gehiago komunikazioetan oinarritzen da. Enpresa mailan IKTko (Informatika eta komunikazio teknologiak) [1] inbertsioa 2018an 41.500 milioi eurokoa izan da eta aurreikusten da etorkizunean munduko BPGaren (Barne Produktu Gordina) erdia izango dela. Begi-bistakoa denez, enpresa ezberdinak beharrizan ezberdinak dituzte eta hauen arabera segurtasun politika ezberdin bat aukeratzen da.

Internetek industrian eragiten dituen arriskuak aztertuz, esan beharra dago industrian gertatzen diren arrisku gehienak eraso informatikoak sortzen dituztela. 2018ko [2] lehen zatian 668 milioi datu jario egon dira. Horregatik, enpresa gehienak inbertsio handia egiten dute eraso hauen prebentzioan, saihespenean eta ebazpenean. 1. Irudiaren grafikoan aztertu ahal den moduan:



1. Irudia: 2014tik 2018ra egon diren datu jarioen grafikoa

Iturria: *https://www.helpnetsecurity.com/2018/05/09/data-breach-quickview-report/*

Enpresa guztiak babestu nahi dute bere informazioa ez soilik enpresa informatikoak, Enpresa baten barne sarearen babesa segurtasun perimetrala da.

Segurtasun perimetrala bermatzeko elementu ezberdinak erabili ohi dira; adibidez, firewallak, detekzio eta prebentzio segurtasun sistemak, VPN (Virtual Point Network), IPS/IDS (Intrusion Prevention/Detection System), antibirusak, anti-spam eta honeypot-ak.

Zibersegurtasuna inplementatzeko firewallak [3] erabiltzen dira normalean beste ekipo batzuekin osatuz. Ordenagailuen zientzian, firewall bat firmware edo Software bat da zein arau multzo bat ezartzen du eta hauen bidez erabakitzen du zeinak datu pakete sartuko diren sarera eta zeintzuk ez. Aldiz, gaur egungo firewallak, lehenago aipatu diren segurtasun elementu askoren funtzionalitateak esleitzen ditu. Adibidez, IPS, Web filtering, Antivirus...

Segurtasun eta sare kudeaketa industrialean kontuan eduki behar den beste aspektu bat automatizazioa da. Automatizazioan inbertitzea etorkizunean aurrezpena ekarriko du, giza baliabideak gutxiagotzeko

aukera emanez. Automatizazio hau zeharo lotuta dago programazioarekin.

Programazioa erabiliz script batean batzen dira egin nahi diren zereginak eta horrela lan hau berriro egin behar denean script hau exekutatu baino ez da egin beharko.

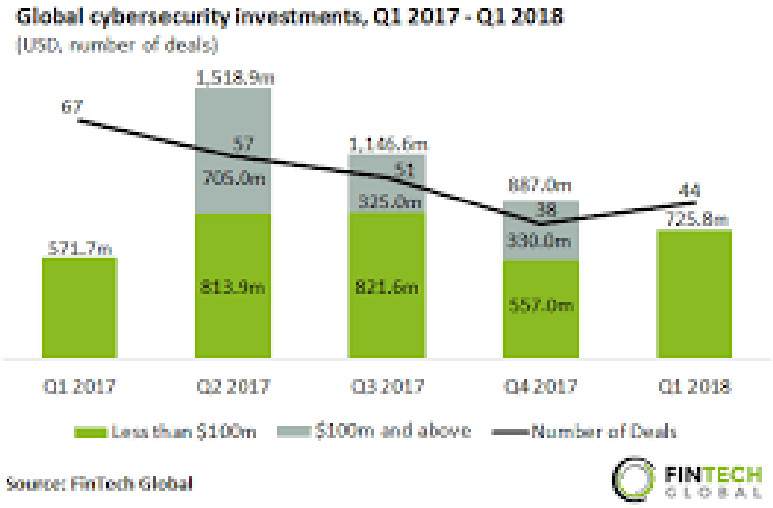
Era zehatzago batean aztertuz, lan honetan automatizazioa eta zibersegurtasun industrialeko diseinu bat inplementatuko da, enpresa jakin batean segurtasun mekanismoak ezarriz.

Enpresa honetan hiru egoitza daude eta egoitza hauek bi departamentutan banatuko dira, honen ondorioz departamentu berrirako segurtasun babesa ezartzeko segurtasun diseinu bat inplementatu beharko da.

Halaber, sare objektuen sorrera automatizatuko da, hau lortzeko APIen interakzioa eta programa bat programatuz egingo da.

2.Testuingurua

Gradu Amaierako Lan honen sarreran aipatu dugun bezala, zibersegurtasuna oso alderdi garrantzitsua da gaur egun edozein enpresarentzat eta horregatik, enpresek inbertsio (ekonomiko eta pertsonenak) handiak egiten dituzte euren sareak babesteko zibersegurtasun arloan, 2018. [4] Urteko lehenengo laurdenean 725,8 milioi dolar inbertitu dira munduan zibersegurtasunean. 2. irudiaren grafikoan ikusi ahal den moduan:



2. Irudia: Gastua zibersegurtasunean 2017tik 2018ko lehen laurdenera

Iturria: *https://fintech.global/cybersecurity-investments-declined-in-q1-2018-as-later-stage-deals-dried-up/*

Gaur egungo industrian era ezberdinetan inplementatzen da segurtasun informatikoa; beraz, atal honetan segurtasun mekanismo ezberdinak aztertuko dira. Mekanismo hauen helburua enpresa edo erakunde baten aktiboak eta datuak babestea da eta kontuan eduki beharreko ezaugarriak dira sare bati segurtasuna esleitzeko momentuan.

2.1 Sare mailako segurtasun mekanismoak

Lehen aipatu den bezala, sare perimetraleko segurtasun mekanismoak sare horri segurtasuna esleitzeko irizpideak batzen dituzten kontzeptuak dira [5]. Kontzeptu hauek ez dira zergatik izan behar sare logikoa babesten dituzten mekanismoak, fisikoak ere izan daitezke, aurrerago ikusiko den bezala.

2.1.1 Segurtasun mekanismo fisikoak

Segurtasun mekanismoen artean fisikoak oso garrantzitsuak dira. Askotan mekanismo hauek ez dira kontuan hartzen segurtasun informatikoari buruz hitz egiten denean. Gure sareko elementuak edonorentzat fisikoki eskuragarri ez edukitzea oso garrantzitsua da. Hauen artean segurtasun fisikoa eta autentifikazioa daude.

Segurtasun fisikoa segurtasun informatikoa edo ekipo informatikoak dituen gela zein eraikinak modu egokian babestean datza. Hau da, zerbitzariak dituzten gelak babestu beharko lirateke, adibidez, alarma edo segurtasun pertsonalarekin. Gainera, sarbide mugatua izan behar da eta pertsonal espezializatua soilik sartu ahalko zen makineriari erabilera desegokia eman ez dezan.

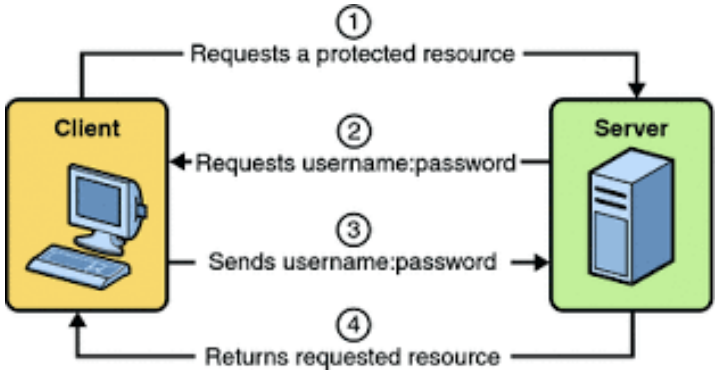
Segurtasun fisikoa oso garrantzitsua da, gure ekipo informatikoak ez baditugu behar bezala babesten, sarea babesteko beste mekanismoek ez dute arrakasta izango nahiz eta diseinu perfektua egin.

2.1.2 Segurtasun mekanismo logikoak

Segurtasun mekanismoen beste mota segurtasun mekanismo logikoak dira. Segurtasun mekanismo hauei esker sareko elementuak beste sareen erabiltzaileagandik babestea ahalbidetzen du. Hauen artean sarbide kontrola, accounting, datagramen zifratzea eta trafiko iragazia daude.

Autentifikazioa

Segurtasun mekanismo honek sare erabiltzaile baten nortasuna konprobatzen du, kredentzialetan oinarrituz. Hau da, baliabide korporatibo batera sartzeko erabiltzaile eta pasahitza ez duenak ezin izango du zerbitzu hori erabili.



3. Irudia: Autentifikazioaren eredua

Iturria: *https://docs.oracle.com/cd/E19879-01/819-3669/bncbo/index.html*

Normalean autentifikazioa hiru printzipiotan oinarritzen da

- **Erabiltzaileak dakien zeozer: Erabiltzaileak daukan gako sekretu eta bakarra izango zen. Adibidez, erabiltzaile baten pasahitza.**
- **Erabiltzaileak daukan zeozer: Honek normalean eragiten du erabiltzaileak objektu bakarra izatea. Adibidez, segurtasun txartelak geletara sartzeko.**
- **Erabiltzailea den zeozer: Honek eragiten du erabiltzailearen ezaugarri fisiko baten bat erabiltzea. Adibidez, atzamar marka edo begi ninia.**

Askotan, aurrean ikusi diren bi printzipio erabiltzen dira segurtasun handiago bat bermatzeko. Adibidez, atzamar eta pasahitz bat eskatzea sarbidea emateko gela batera, hau izendatzeko hedatuta dagoen ingelesezko terminoa *double factor authentication* da.

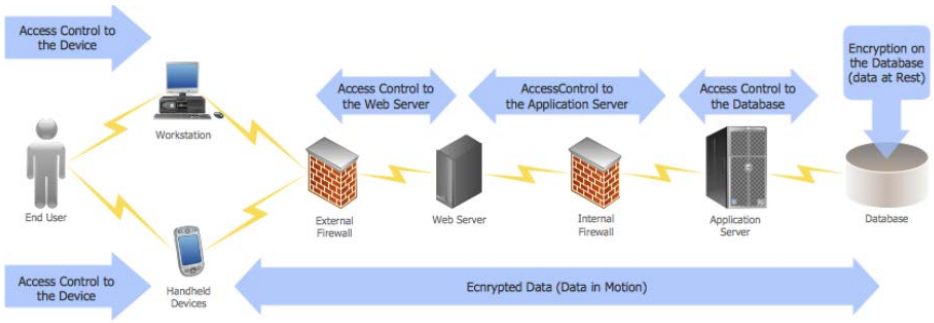
Sarbide kontrola

Segurtasun mekanismo honek erabakiko luke erabiltzaile bati sare sarbidea esleitzea. Hau da, sarean dauden zerbitzuei sarbide mugatua ematen zaie, lehendik autentifikazio prozesua arrakastarekin betetzea ez du esan nahi zerbitzu guztietara sarbidea izango denik.

Honek ahalbidetzen du erabiltzaile ezberdinak izatea sarean eta eskubide ezberdinak ematea langile ezberdinei. Adibidez, batzuei interneterako sarbidea eman baina sarbide mugatu bat Youtube bezalako webgunetara sarbidea mugatuz.

Segurtasunean adituek gomendatzen dute ahalik eta pribilegio gutxien ematea sare batean. Hau da, ahalik eta baliabide gutxienetara sarbide ematea erabiltzaileei bere beharren arabera.

Honekin oso lotuta dagoen kontzeptua segurtasun politika da, hau eratuz sareko zerbitzu telematikoei emango den sarbidea erabakitzen da. Era berean, saretik kanpoko zerbitzuei sarbidea arautzen da.



4. Irudia: Sarbide kontrolaren eredua

Iturria: *https://www.conceptdraw.com/examples/access-control-and-encryption*

Ikuskaritza

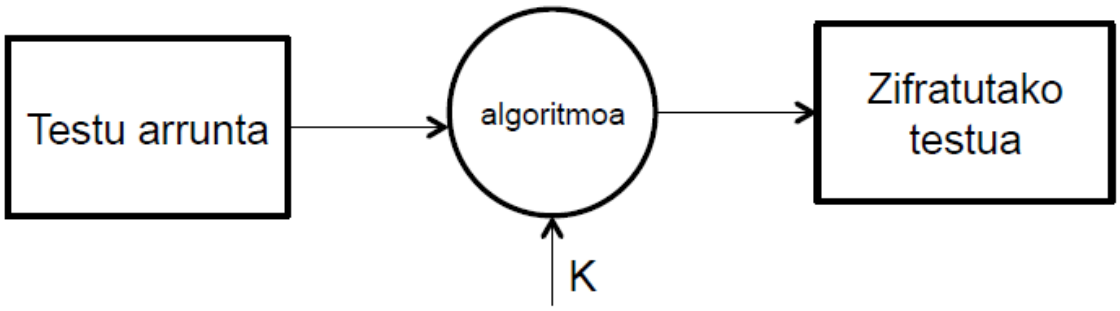
Sare baten segurtasuna aztertzeko era eraginkorrean eta segurtasun intzidentziei era egokian erantzuteko, sarea frogatzeko prozedurak ezarri behar dira, honen portaera segurtasun arriskuen aurrean aztertzea posiblea izan dadin. Prozedura hauek egitea ikuskatzea da.

Segurtasun gogorra duten sareak ikuskatzerakoan autentifikazioa eta baimentzea lortzeko edozein saiakera egiten da. Horrela frogatzen da zein eraso informatikoen aurrean sentikorragoa den sarea.

Ikuskatzen denean ez da kriptanalisi erasorik egiten, honek datuen jarioa sor dezakeelako. Ikuskaritza baino pausu bat aurrerago doana segurtasun ebaluazioa da, honek sarearen ahultasun guztiak kontuan edukitzen duten profesional batzuek egiten dute.

Datuen zifratzea

Zifratzea datuen esanahia ezkutatzen duen prozesu bat da hauen edukia eskuraezina bihurtuz, hartzailea ez den beste edonorentzat. Nahiz eta hau den bere helburua, ez da asmatu zifratzea perfektua, hau da, deskodetzeko ezinezkoa den zifratzea. Enkriptatu gabeko datuak *plain text edo clear text* izendatzen dira.



5. Irudia: Datu zifratzearen azalpena

Zifratze teknikak oso erabilgarriak dira datuen konfidentzialtasuna bermatzeko, datuak bi muturretako kideak soilik irakurri ahalko dute eta.

Zifratzea bi parte ditu: algoritmoa eta gakoa. Algoritmoa instrukzioa sorta bat dira datuak kodetzeko eta deskodetzeko. Gakoa informazio sekretua da eta algoritmo publikoa parametrizatzeko erabiltzen da. Horrela mugatzen da informazioa eskuragarri izateko aukerak, informazioa berreskuratzeko gakoa ezagutu beharko baita.

Askotan, datuak saretik zifratuak bidaiatzen dute, VPN tunelen erabileraren ondorioz. VPN tunelak sare pribatu baten sarea sare publikoa era seguruan atzitzea edo erabiltzea ahalbidetzen du. Gainera, sare korporatibo edo pribatu horren segurtasun mekanismoak gehituko zaio bere konexioari. Hau da, tunel birtual bat sortzen da sare korporatiboraino eta hortik, irtengo dira VPNra konektatuta dagoen ekipoaren datagramak. Ondorioz, ekipo honen paketeak sare korporatiboen firewall, antibirus etab. babestuko dituzte.

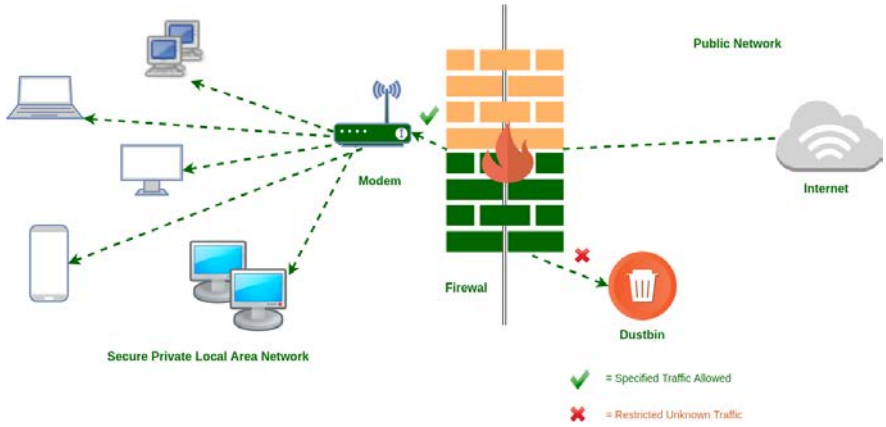
Datagrama iragaziak

Mekanismo hauekin sarera sartzen diren datagramak onartzea edo ukatzea ahalbidetzen da arau sorta baten arabera. Ahalbidetzen dute sarea babestea baimenik gabeko erabilpenetik, lapurretatik, suntsiketatik eta DoS (Denial of Service) erasoetatik. DoS erasoa zerbitzuak ukatzea lortzen saiatzen diren erasoak dira.

Bi iragazketa irizpide daude datagrama guztiak blokeatzea eta soilik sarera sartu behar direnak ahalbidetu edo dena ahalbidetu eta sarera sartu behar ez diren datagramak blokeatu.

Trafikoa ahalbidetzen duten arauak sortze errazago da, sareen beharren edo zerbitzuen arabera definitu daitezkeelako. Ukatzea traketsagoa da, segurtasun erasoei buruzko jakintza izan behar da etorkizunean eraso posible dat eragin ahal duten datagramak identifikatzeko kapaza izateko.

Datagramen iragazien sistema ezagunenak firewallak dira. Sarreran azaldu da hauen funtzioa eta nola gero eta gehiago mekanismo gehiago dituzte eta ez dira soilik trafiko iragazi sinpleak. Gaurko firewallak, funtzioa asko betetzen dituzte, routing, trafiko iragazia, VPN, Web Filter, Application Control... Beraz, makina konplexuak izaten ohi dira.



6. Irudia: Datu iragazkiaren eredua

Iturria: *https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/*

2.2 Host mailako segurtasun mekanismoak

Host bat makina komun bat da; beraz, atal honetan host hori segurua bihurtzeko mekanismoak ikusiko dira, hosta sarearen parte bezala aztertu gabe.

Askotan segurtasun bretxarik handiena hostean dago, host hauek erabiltzen duten erabiltzaileek ez baitute eduki behar inolako jakituria teknikorik. Ondorioz, gaur egun hosten babesa ardura asko ekartzen du, sare bat infektatzeko erarik sinpleena baita.

Hosta babesteko segurtasun mekanismo nagusienak Antimalware programak, host mailako firewallak eta lista beltza dira.

2.2.1 Antimalware

Antimalwarea programa maltzurrak eteteko segurtasun mekanismoa da. Antimalware motako mekanismo nagusiak Antibirus, Anti-spam, Anti-spyware eta pop-up blocker-ak dira.

Antibirusak birusak sistematik kanpo edukitzea laguntzen du, horrela hosta ez infektatzea ahalbidetzen du.

Anti-spama mezu elektroniko maltzurrak blokeatzeko tresnari deritzo.

Anti-spywarea hosta izan ahal dituen espioien aurkako sistemak dira, programa maltzurren bidez hostaren nabigazio edo beste motako informazioa lortzen dute, keylogger spyware mota adibidez, teklatuaren zein teklen zein frekuentzia erabiltzen duen erabiltzaile infektatua aztertzen du, maiztasun hau aztertuz, makinaren edo makinak erabiltzen dituen zerbitzuen pasahitza lortu daiteke.

Pop-up Blockerrak nabigatzailean publizitate leihoak ez agertzea ahalbidetzen du, ahal den heinean behintzat.

2.2.2 Host mailako firewallak

Firewall hauek host mailan konfiguratzen dira eta sistema eragilean inplementatzen ohi dira. Sistema eragile horren ataka batzuk blokeatzen dira; adibidez, Telnet erabiltzen duen ataka.

Host mailako firewallak sistema eragilearen arabera doaz; adibidez, Ubuntuk ufw firewalla du eta Windows Windows defenderreko firewalla.

2.2.3 Zerrenda Beltzak

Zerrenda beltzen bidez erabiltzailearentzako arriskutsuak diren aplikazio batzuk blokeatzen edo ukatzen dira, erabiltzaileak aplikazio hauekin arazorik ez izateko. Nabigatzaileak askotan abisatzen du programa bat arriskutsua dela eta erabiltzailearen esku dago hau sisteman gordetzea eta ondoren instalatzea.

Honekin lotuta dagoen beste kontzeptu bat zerrenda zuria da, zerrenda beltzen kontrako kontzeptua dena. Askotan programa guztiak blokeatzen dira zerrenda zurian daudenak izan ezik. Era honetan sistema mugatuagoa da.

2.3 Segurtasun erasoak

Sareen ahultasunak aprobetxatuz hainbat segurtasun eraso mota daude, hauek beti saiatzen dira sarearen puntu ahulenak identifikatzen eta handik sarea suntsitzen edo informazioa lortzen . Eraso ezagunenak hauek dira: Malware, phising, SQL (Structured Query Language) injection erasoa, Cross-Site Scripting, Denial of Service eta man in the middle.

2.2.1 Malware

Malware hitzak erreferentzia egiten die sistemarentzako kaltegarriak diren edozein Softwareei, gehienetan ramsonware edo birusak. Behin malwarea zure ekipoan sartzen dela, zure ekipoaren kontrola har dezake, zeure ekintzak monitorizatu ahal ditu edo informazio konfidentziala bidali beste ekipo batera. Gainera, ekipoaren funtzionamendu egokia eragotzi dezake, sistemaren gaitasunak gutxituz.

Askotan malwarea ekipoan sartzeko erabiltzaileak instalatu beharko du, lotura maltzur bat klikatuz edo izaera maltzurreko dokumentu bat deskargatuz.

Antibirusen eta lista beltzen bidez saihestu daiteke, malware bat erabiltzaile komun baten ekipoan instalatzeko saiakera egiten duenean hau etenduz.

2.2.2 Phising

Phising erasoetan erasotzaileak mezu elektroniko maltzurrak bidaltzen dituzte sareko erabiltzaileei. Mezu elektroniko hauen bidez erasoa jaso duena irekitzen badu edo mezu elektronikoa eskatzen duena erantzuten badu, bere datuak erasotzailearen menpe jarriko dira.

Askotan mezu elektroniko hauek mezu normalen formatua dute, erasoa jaso duena engainatzeko. Mezu hauek sarritan dokumentu erantsiak edo loturak dituzte eta hauek instalatu edo klikatzen badira erabiltzaileen ekipoetan malwarea instalatuko da.

Mezu elektroniko iragazkiak daude, iturri maltzurra identifikatzen dutenak eta mezu hauek ez dute pasatzen uzten; adibidez, lehen ikusitako Anti-spam mekanismoak.

2.2.3 SQL injection attack

Eraso hauek datu baseen aurkako erasoak dira, hauek dituzten ahultasunak aprobetxatuz. Datu base hauek datu pribatuak izan ahal ditzakete, kreditu txartelak, izenak, erabiltzaile izenak eta pasahitzak...

Datu baseak dituzten datu horiek eraso hauen bitartez zabaltzen dira, datu jarioen eraso bat eraginez. Eraso hau SQL zerbitzarietan kode maltzurra sartuz gauzatzen da.

Eraso mota hau ikuskaritza teknikarekin saihestu daiteke ahultasun posibleak indartuz. Ikuskaritzaren bitartez, sistemak edo webguneak aztertuko dira eta etorkizunean egon daitezkeen erasoak identifikatu eta aurre-ebatziko dira.

2.2.4 Cross-Site Scripting

Aurreko erasoa bezala, eraso hau kode maltzurra txertatuz lortzen da. Hala ere, eraso hau ez doa zerbitzariaren aurka, hauen webgunearen erabiltzaileen aurka doa.

Eraso hauek gauzatzeko erarik ohikoena, webgune batean iruzkin baten barruan lotura maltzur edo JavaScript kode bat txertatuz egiten dira. Eraso honen bitartez webgunearen izena zikinduz, webgune honen erabiltzaileak datuen konfidentzialtasuna galtzearen ondorioz.

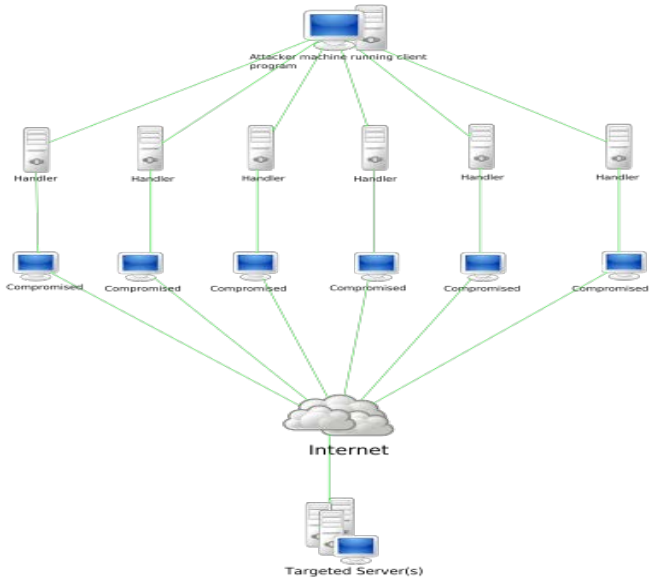
Eraso hauek saihestu ahal daitezke sarearen kudeaketa zuzen batekin, scriptak dituzten iruzkinak ezabatuz.

2.2.5 Denial of Service

Eraso honen bidez, sarearen trafikoa asko handitzen da sarea kolapsatuz. Sareak trafiko kantitate baterako prestatuak daude eta trafiko hau asko handitzen bada, routerren, switchen, amaierako zerbitzariaren eta firewallen prozesatze ahalmena gaindituz, sarearen zerbitzuak zapuztu ahal dira.

Eraso honek sarearen zerbitzuak eteten ditu, begi-bistakoa denez eraso hau oso kritikoa da. Pentsatu Google-ren zerbitzuak eteten direla, mundu mailako krisi garaia sortu ahalko luke.

Eraso hau saihesteko sarbide kontrola eta accounting erabiltzen da, trafikoa iragazteko eta arrisku posibleak aztertzeko.



7. Irudia: DoS attack eredua

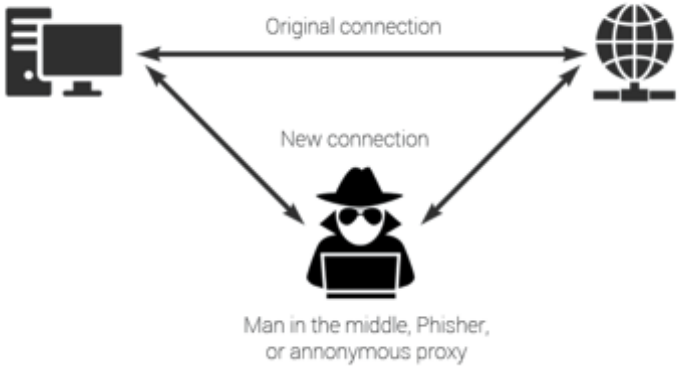
Iturria: *https://en.wikipedia.org/wiki/Denial-of-service_attack*

2.2.6 Man in the middle

Eraso honetan, erasotzaile maltzurra trafikoa aztertzen du komunikazio fluxu baten erdian, bidaltzen diren mezuak aztertuz eta hauetatik datuak lortuz.

Gainera, mezu hauek aldatu ahal ditu datu berriak txertatuz. Era horretan datu konfidentzialak jaso ahalko luke.

Eraso mota hau saihesteko autentifikazioa eta datuen zifratzea erabiltzen dira, era honetan datuak ez dira ulergarriak. Autentifikazioari esker, 3. Parte bat ezin izango da komunikazio erdian sartu.



8. Irudia: Man in the middle eredua

Iturria: ***https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/***

2.4 Automatizazioa segurtasun elementuetan

Gaur egungo industrian, automatizazioak garrantzi handia hartu du, etekin ekonomikoa dela eta. Etekin ekonomikoa baliabideen aurrezpenaren ondorioz ematen da, programatzaile batekin hainbat langileen lana egin baitaiteke, lan errepikakorrak programen bidez eginez, denbora eta diru asko aurreztuz.

Automatizazio garai honetan API (Application Programming Interface)-en erabilera asko handitu da, automatizazioa kudeatzeko ezarri den tresna baita. APIak komando eta funtzionalitate multzo bat dira aplikazioak haien artean komunikatzeko ahalmena izateko. APIak programazioaren bidez kudeatzen edo lantzen dira.

APIak programazio lengoaia batekin konbinatuz, web interfazean denbora askoan konfiguratzen duzuna, klik soil batez egin daiteke, denbora handia aurreztuz. Normalean, HTTP (HyperText Transfer protocol) POST eskaeren bidez egiten da eta makinak eskatutako datuak bidaltzen ditu edo agindutako objektuak sortzen ditu, metodo ezberdinak erabiliz.

Segurtasunaren industrian, garrantzi handia irabazi dituzte APIak askotan oso errepikakorra diren lanak egin behar baitira. Adibidez, askotan segurtasun arau berrien sorrera egingo da; aldiz, APIak erabiliz, programa bat garatuz lan mota berdinen konfigurazioak ez dira errepikatu behar.

APIen erabileraren ikasketa errazteko, fabrikatzaileek dokumentazioa esleitzen dute haien webgunetan eta gainera, bakoitzak

bere foroak ditu (batzuetan ordaindu beharrekoak) non garatzaileen galderei erantzuten dute.

APIak lantzen dituzten garatzaileak normalean python lengoaiarekin lan egiten dute; beraz, dokumentazio gehiena python programei buruzkoa da.

3. Lanaren helburuak eta irismena

Proiektu honen irismena, 3 lurralde ezberdinetan dauden egoitzei beharrezko segurtasuna esleitzea da, hauen kudeaketa era zentralizatuan antolatuz. Gainera, politika taldearen eraketan automatizazioa inplementatzea bilatzen da ere.

Irismen hau zehazten da helburu nagusi batekin eta aldi berean, bigarren mailako helburu gehiagorekin.

GRAL honen helburu nagusia, 3 kokapen fisikotan banatutako erakunde batentzat segurtasun ebazpen baten diseinua eta inplementazioa egitea da. Sare enpresarial honetan diseinu zaharkitu bat inplementatua dago; beraz, proiektuaren ibilbidea honegatik guztiz mugatua egongo da.

Halaber, segurtasun politikaren eraketan automatizazioa inplementatzea bilatzen da ere. Diseinua aurreikusi ahal diren arriskuak saihesteko erabiliko da. Diseinatutako eta inplementatuko politika hauek eskalagarriak eta moldakorrak izan behar dira, etorkizunean sareak beste zerbitzuen beharrizan baditu, segurtasun politikak moldatzeko aukera izateko. Segurtasun politika hauek sarearen jabeak ezarritako espezifikazioen araberakoak izango dira. Hala ere, arrisku analisi bat diseinatuko da segurtasun politika zaharra hobetzeko.

Hori dela eta, segurtasun politika bat ezarriko da zeinak sarrera kontrola, trafiko miatzea eta erabilgarritasuna antolatzen edo arautzen duen.

Helburu hau lortzeko, bigarren mailako beste helburu batzuk definitzen dira, zeinek batera, helburu nagusi bat lortzea ahalbidetzen dute. Helburu hauek besteengan menpetasuna dute, hauen lorpena beste helburu baten lorpenaren menpekotasuna baitute. Jarraian, definituko dira bigarren mailako helburuak:

- **Eskakizunen definizioa: lehenengo helburua, eskakizunen identifikazioa eta definizioan datza. Hau da, segurtasun politikaren inplementazioaren bitartez lortu nahi diren segurtasun eskakizunen deskripzioa eta beharrezko eskakizunak automatizazio prozesurako era zehatzean definitzea.**
- **Segurtasun politikaren diseinua: Behin eskakizunak identifikatuta, eskakizun hauek asebeteko dituen segurtasun politika definituko da.**

- **Segurtasun politikaren inplementazioa: Helburu honetan,definitutako segurtasun politika produkzio ingurumen batean inplementatuko da. Segurtasun politika froga ingurumen batean testatuko da bere baliagarritasuna frogatu dadin.**
- **Segurtasun politiken eraketen automatizazioa: Automatizazioaren bitartez saihesten da lan errepikakorrak egitea segurtasun politiken eraketan.**
- **Ebazpenaren azterketa: Behin helburu denak beteta, aztertuko beharko da ezarritako ebazpenaren ahultasunak eta hauek hobetu beharko lirateke proiektuaren eginkizuna borobiltzeko.**

4. Onurak

Proiektu guztiak era batean edo bestean onuragarriak dira ekonomikoki, sozialki, teknikoki... Onura hauek proiektua egingarria izatea lortzeko arrazoia baitira. Azken finean proiektu bat egiteko interesa onuren kantitatean datza; hau da, abantailak desabantailak baino gehiago izatean proiektua egiteko interesa sortzen du.

Proiektu honek gehien bat ekarriko dituen onurak hiru motakoak dira: onura teknikoak, onura sozialak eta onura ekonomikoak.

4.1 Onura teknikoak

Proiektuaren alderdi teknikoa aztertuz, argi eta garbi dago proiektua onuragarria izango dela, aztertuko dugun azpiegitura nabarmenki hobetuko da, segurtasuneko mekanismo ahaltsuagoak inplementatuko dira sarearen babesa bermatzeko.

Gainera, segurtasun politiken diseinu berriarekin segurtasun politika hauek sendotuko eta finduko dira; era honetan, azpiegiturari hobeto moldatzen diren politikak inplementatuz eta sareak jaso behar duen trafikoa soilik ahalbidetuz. Legezko trafikoa soilik ahalbidetzen denez, sarearen eraginkortasuna hobetzen da eta sarearen zerbitzuen erantzuna hobea izango da, hau da, errendimendua hobea izango da.

Aldi berean, automatizazio ebazpenaren ondorioz, sarearen kudeaketa optimizatuko da, asko azkartuz kudeaketa hau. Gainera, modernizazio konbergentziara goaz, automatizazioa erabiliko da etorkizunean sare segurtasuna kudeatuko duen pertsonak jakituria tekniko zehatzak izan behar ez ditzan.

4.2 Onura ekonomikoak

Proiektuaren alderdi ekonomikoak aztertuz, proiektua ekonomikoki onuragarria izango da bi entitateentzat: azpiegituraren jabedunentzat eta proiektua bideratuko duen entitatearentzat.

Jabeentzat, proiektua onuragarria izango da haien datuak, transakzioak eta proiektuak babestuagoak egongo direlako, segurtasun mekanismo sendoengatik. Gainera, bere sarearen segurtasuna kudeatzeko inplementatuko den automatizazioak denbora aurreztea ekarriko du, diru aurreztea eraginez.

Halaber, diru galera erraldoiak eragin ahalko luketen eraso informatikoak ekidin ahalko lirateke. Era honetan, inbertsoreen eta

bezeroen konfiantza maila handituko zen, hauek negozio segurua dela aitortuz; beraz, sarearen jabearen negozioa bultzatuz.

Proiektua bideratuko duen entitateak, proiektu hau egiteagatik diru sarrera jasoko du eta gainera, proiektu egokia garatzen bada azpiegituraren jabea den entitatearekin erlazioak hobetuko lirateke eta etorkizuneko proiektu ezberdinak eragin ahalko lukete.

4.3 Onura sozialak

Proiektu hau sozialki onuragarria da, hobetuko den sarearen erabiltzaileak onurak nabarituko dituzte bai erabileraren azkartasunean, sarea hobetu baita, eta segurtasunean, datu jarioak ahal den heinean saihestuz.

Gaur egungo gizartean nahiko garrantzitsua da gure datuak babestea, horren ondorioz Europak nazioarteko datuen babes araudia ezarri du [6], pertsonen datuak zelan eta zer helbururekin prozesatu daitezkeen zehazteko. Honek eragiten duena gure datu pertsonalak erabiltezinak bihurtzea gure baimenik gabe; hala ere, gure datu estatistikoak bai erabili daitekeela.

Proiektu honi esker sare korporatibo baten erabiltzaileen datu fugak ekidingo dira, erabiliko diren segurtasun mekanismoei esker, erabiltzaileen mesfidantza eta ardura Interneten erabilerari buruz saihestuz.

Gainera, segurtasun mekanismo hobeak, zerbitzu telematiko seguruagoak ematea ahalbidetzen du, gizartearen aurrerapena ekarriz. Aspaldi segurtasun ezagatik arriskutsuak ziren zerbitzu telematikoak seguruak bihurtuz.

5.Espezifikazioak

Sare enpresarialaren jabeak eskakizun edo espezifikazio batzuk ezarri ditu proiektua egiteko eta hauek atal honetan laburki azaltzen dira. Espezifikazio edo eskakizun orokorrak hauek dira:

- Segurtasun perimetralaren inplementazioa B eta C egoitzetan eta kudeaketa zentralerako tresnen integrazioa A egoitzan.
- Komunikazioen kudeaketarako azpiegituraren berritzea egoitza guztietan.
- A egoitzako segurtasun elementuen berritzea.
- Automatizazio ebazpen bat diseinatzea segurtasun politiken sorrerako.
- Funtzionamenduaren frogak eta produkziora pasatzeko prozesua jarraitzea.
- Dokumentazio zehatza entregatzea.

Hala ere, hain orokorrak ez diren beste espezifikazio batzuk daude, egoitza bakoitzaren arabera aztertzea interesgarriagoa izango dena.

5.1 A egoitzaren espezifikazioak

A egoitzak espezifikazio zehatz batzuk eskatzen ditu. Hauek hurrengok dira:

- Azterlana, diseinu eta ikasketa kudeaketa zentralerako tresnaren inplementazioari buruz.
- Firewall fisikoen egoera aztertzea eta Softwaren bertsioa eguneratzea beharrezkoa bada.
- kudeaketa zentralerako makina birtualaren hedapena fabrikatzaileak gomendatzen duen azkenengo bertsioan. Kontuan eduki firewallen bertsioaren bera izan beharra.
- Sare kudeaketarako tresnara migratu A egoitzako antzinako FortiGatetan zegoen konfigurazioa.
- Sare kudeaketa zentralerako tresna integratzea B eta C egoitzen firewallak.
- Interneterako irteeran Web Filter eta Application Control politikak ezartzea.

5.3 B egoitzaren espezifikazioak

B egoitzak eskakizun zehatz batzuk ditu eta ondoren azaltzen dira:

- **Migratu behar diren ebazpenen azterlana, ikasketa eta diseinua egitea:**
  - **Firewallen maila altuko eta maila baxuko diseinua egitea.**
  - **Migrazioaren konfigurazioaren dokumentazioa entregatzea.**
  - **Frogen dokumentazioa egitea.**
- **Firewall fisikoen egoera aztertzea eta Softwarearen bertsioa eguneratzea beharrezkoa bada.**
- **Firewall berrien instalazio fisikoa eta sare kudeaketa zentraleko poolean integratzea.**
- **Juniper SG-550 firewallaren segurtasun politiken migrazioa firewall berrietara eta hobespena.**
- **Interneterako irteeran Web Filter eta Application Control politikak ezartzea.**

5.2 C egoitzaren espezifikazioak

C egoitzak eskakizun zehatz batzuk ditu eta ondoren azaltzen dira:

- **Migratu behar diren ebazpenen azterlana, ikasketa eta diseinua egitea:**
  - **Firewallen maila altuko eta maila baxuko diseinua egitea.**
  - **Migrazioaren konfigurazioaren dokumentazioa entregatzea.**
  - **Frogen dokumentazioa egitea.**
- **Firewall fisikoen egoera aztertzea eta softwarra bertsioz igo beharrezkoa bada.**
- **Firewall berrien instalazio fisikoa eta sare kudeaketa zentraleko tresnaren poolean integratzea.**
- **Oinarrizko iragazketarako segurtasun politiken inplementazioa ingurumen ezberdinak banatzeko.**
- **Internetarako irteeran Web Filter eta Application Control politikak ezartzea.**

6. Diseinu alternatiben analisia

Behin espezifikazioen definizioa eginda hauek betetzeko aukera ezberdinak aztertu behar dira. Horretarako teknologia ezberdinen azterketa sakona egingo da hainbat beharrizan asebetetzeko.

Alternatibak aukeratu dira irizpide zehatz batzuen definizioaren ondorioz, irizpide hauek ponderatuko dira izan behar duten garrantzia esleituz.

Hartu den erabaki bakoitzarekin, erabaki honen arrazoia eta honek ze inpaktu izango duen proiektuan azalduko da, argi utziz ze abantaila espero diren ebazpen horretatik. Ondoren, alternatiba guztiak laburki azalduko dira eta geroago, erabilitako irizpideak erakutsiko dira, bere garrantzia kontuan hartuz ponderatuak. Azkenik, bakoitzak lortu duen puntuazioaren ondorioz, erabakia hartuko da.

Proiektu honetan, sare korporatibo baten segurtasun ebazpen berria planteatuko da, gainera, automatizazio ebazpen bat planteatuko da. Honek hainbat alternatiben azterlana planteatzen du:

- **Firewall fabrikatzaile ezberdinen arteko aukeraketa.**
- **Automatizazio programa garatzeko teknologia ezberdinen arteko aukeraketa.**
- **Cluster topologia ezberdinen arteko aukeraketa.**

Jarraian alternatiba ezberdin hauek aztertuko dira erabaki hoberena zein den aztertzeko.

6.1 Firewall fabrikatzaileak

Proiektu hau firewalletan oinarritzen denez, guztiz beharrezkoa da, aztertzea zein fabrikatzaile izango zen hoberena. Erabaki hau hartzeko lau irizpide nagusi definitu dira: Segurtasun mekanismoen sendotasuna, prezioa, kudeaketa zentralerako gaitasuna, VPNak eratzeko gaitasuna eta konfiguratzeko erraztasuna.

Hiru fabrikatzaile nagusi aztertuko dira: Checkpont Security Appliance, Fortinet FortiGate eta Juniper SRX.

Proiektu honetan inplementatu behar den segurtasun ekipamenduaren arabera, fabrikatzaile horiek soilik aztertuko dira; adibidez, PaloAlto oso garestia da eta aurrekontua asko handituko luke.

6.1.1 Alternatibak

Juniper SRX

Juniper SRX Juniper fabrikatzaileak egiten dituen firewallak dira. Firewall hauek era zuzenago baten oinarrituak daude sare mailara, Juniper ekipamenduak sare ekipamenduak izaten ohi baitira. Hau da, ez dute soilik segurtasun funtzioak.

Ekipamendu hauek ACLetan (Access Control List) oinarritzen da; hau da, trafikoa kontrolatzen da sareen arabera eta sare ezberdin hauek taldekatzen dira pribilegio ezberdinak esleituz bakoitzari. Honen ondorioz L7 mailan; hau da, aplikazio mailan ez du egiten inolako azterlanik, funtzionalitate hau ez izanik.

Gainera, ez dute kudeaketa zentralerako ekipamendurik ez SW-ik.

Normalean, erabiltzen dira router eta firewall gisa sare txiki eta ertainetan, sare ekipamendu asko ez daudenean.

Ezaugarri bereizgarri gisa, konfigurazio oso traketsa da eta honek denbora asko galtzea eragiten du.

Azkenik, azpimarratu behar da ez duela VPN ebazpenik firewallen funtzionaltasunaren barnean; beraz, beste tresna bat instalatu beharko zen sarean horrelako zerbitzua eman nahiko bazen.

Checkpoint Security Appliance

Checkpoint fabrikatzailearen firewallak dira, funtzionalitate asko dituzte eta oso osoak dira firewall moduan. Juniper SRXekin alderatuz guztiz zuzenduak daude firewall lanetara eta ez daude bideratuak sare mailako operazioetara.

Beraz, segurtasun mekanismo sendoagoak dituzte. Hala ere, ez dute HTTPS (HyperText Transfer protocol Secure) inspection, beraz Application Control funtzionaltasuna ez da oso sendoa, HTTPS trafikoa ezin baita aplikazio batekin identifikatu zifratzearen ondorioz.

Hala ere, URL Filtering eta trafiko iragazketa ahaltsua du. Halaber, politiken arauekin bat etortzen den trafikoa miatzeko tresna oso ahaltsua du.

Gainera, kudeaketa zentralerako ekipamendua du, eta horrela, arau guztiak SmartConsole deritzon tresna batekin kudeatu daitezke. Tresna honetan definitzen dira arauak era zentralean eta trafikoaren Log guztiak ikusten dira, instalatutako firewallak, pakete politika ezberdinak...

Horren ondorioz, kudeatzeko oso erraza bihurtzen du, dena tresna global batean konfiguratzeko ahalmena izanik.

Azkenik, VPN ebazpen bat ez du firewallen barnean hau esleitzeko beste tresna bat esleitzen du Checkpointek, prezioa nabarmenki igoz.

Fortinet FortiGate

Azken aukera, Fortinet FortiGate firewalla da. Fabrikatzaile honek, Checkpointen antzera, firewall lanetara zuzenduta dago eta ez sare mailako ekipamendura. Beraz, segurtasun mekanismo sendoagoak ditu.

Checkpointekin komunean duen ezaugarria, kudeaketa zentralerako tresna da, kasu honetan FortiManager deitzen dena. Honekin, konfigurazio guztiak egin daiteke eta gero firewalletan instalatu.

Checkpoiten aurka duen desabantaila, trafiko miatzailea da, ez duelako trafiko miatzailea ahaltsua.

Checkpointen aurka duen abantaila handia, HTTPS inspection-a da, honetaz baliatuz Application Control ahaltsua ezartzen du. Beraz, segurtasun mekanismoa sendoagoa da.

VPN ebazpena esleitzen dute Fortinet ekipamenduak, beraz, diru atalean abantaila handia da.

Azkenik, azpimarratu behar da FortiGate Web GUIa (Graphic User Interface) kudeatzeko oso erraza da, konfigurazio egiteko momentuak gauzak asko erraztuz.

6.1.2 Irizpideak

Aukeratzeko aukera ezberdinen arteko bat, irizpide batzuk definitu dira lana errazago egiteko.

- Konfiguratzeko erraztasuna: Diseinatuko den ebazpenaren inplementazioaren erraztasuna baloratuko da. Hau oso garrantzitsua izango da proiektuaren aurrekontua oso garestia izan ez dadin, ingeniaritza orduak askotan oso garestiak irteten baitira. Gainera, konfiguratzeko edo inplementatzeko errazak badira, etorkizunean kudeatzeko errazagoak izango baitira.
- Kudeaketa zentralerako tresna: Tresna bat edukitzea firewallak kudeatzeko asko errazten du firewallen konfigurazioa eta firewall askotarako segurtasun politikak era zentralean instalatu daiteke. Gainera, clusterren egoera aztertu daiteke konektibitatea badu etab.
- Prezioa: Firewall bakoitzaren prezioa oso garrantzitsua da, oso altua baita proiektuaren aurrekontua asko handituko luke. Beraz,

oso garrantzitsua da proiektuetan eraginkortasun kostu erlazioa ondo aztertzea, proiektuak egitea lortzeko ezinbestekoa baita prezio on bat proposatzea.

- **Segurtasun mekanismoen sendotasuna: Firewallen ezaugarririk garrantzitsuena segurtasun mekanismoen sendotasuna da, segurtasun mekanismoak sendoak badira firewalla gure sarea seguruagoa egingo du. Azken finean, firewall baten eginkizuna sarea babestea da.**
- **VPNak eratzeko gaitasuna: Firewall mota guztiek ez dute VPNak eratzeko gaitasuna eta funtzionalitate hau oso erabilia da industrian. Horrela, sare korporatibora beste sare batzuetatik komunikatu ahal da.**

6.1.3 Ebazpenaren aukera

Aurrean ikusitako irizpideak kontuan hartuz eta ponderatuz bakoitzaren garrantzia kontuan edukiz, taula bat eratu da grafikoki ebazpena aukeratzeko irizpidea hobeto ulertu dadin:

Irizpideak	Juniper SRX	FortiGate	Checkpoint Appliance
Konfigurazio erraztasuna (%10)	4	9	8
Kudeaketa zentralerako tresna (%15)	0	7	8
Prezioa (%25)	7	8	6
Segurtasun mekanismoen sendotasuna (%45)	4	8	7
VPNak eratzeko gaitasuna (%5)	0	10	0
Guztira	39,5	81,5	66,5

1. Taula: Fabrikatzaileen analisiaren taula

Konklusioa: proiektu honetarako firewall hoberena Fortinet firewall fabrikatzailearen FortiGatea izan da. Konfigurazio erraztasun handiena ematen du, proiektuan diru asko aurreztuz ingeniaritza orduetan. Gainera, firewallen preziorik baxuena du, honek aurrekontu merke bat proposatzeko erraztasunak esleituz. Gainera, segurtasun mekanismo sendoenak ditu eta kudeaketa zentralerako tresna ona du, nahiz eta, Checkpoint firewallak tresna hobeagoa izan.

6.2 Automatizazio programa

Proiektuaren espezifikazioetan definitu den moduan, proiektu honetan firewallen politikak sortzeko automatizazio programa bat diseinatu behar da.

Programa hauen bidez lan errepikakorrak saihets daitezke, ingeniaritza ordu asko aurreztuz. Programa hauek lan horiek klik batean bihurtzen ditu.

Kasu honetan VLAN (Virtual Local area Network) berri bat sortu ondoren VLAN hori sartu behar da arau sorta batean; hau da, VLAN horretako ekipoak sarbide minimoak izan daitezen programa bat egin beharko da.

Honetarako firewallak konfiguratzeko APIak erabiltzen dira, API hauek ekipoen funtzio sorta bat dira, kanpo Software batetik erabili daitezen. Baina hauek erabili ahal dira era edo teknologia ezberdinetan. HTTP eskaeren bidez konfiguratu daiteke firewall bakoitzaren konfigurazio atazak.

Gainera, HTTP eskaera hauen barruan formatu ezberdineko datu blokeak gehituko dira; hala nola, XML (eXtensible Markup Lenguage) eta JSON (JavaScript Object Notation). Datu bloke hauetan konfigurazio datuak sartuko dira eta APIen bidez ekipoen datu baseetan konfiguratzen dira.

HTTP eskaerak egiteko teknologia edo programazio lengoaia ezberdinak erabiltzen dira, ezagunenak Postman aplikazioen artean eta Perl eta Python programazio lengoaien artean dira.

Teknologia edo programazio lengoaien artean bat aukeratzeko irizpide ezberdinak definituko dira:

- **Inplementazio erraztasuna.**
- **Interneten dagoen dokumentazio lengoaia edo teknologia hauei buruz.**
- **Programaren portaera exekutatzerakoan.**

Irizpide hauek kontuan eduki eta ponderatuko dira aukera onena aukeratzea posiblea izan dadin. Halaber, lehen aipatutako aukera posibleak aztertuko dira, aukera bakoitza hobeto ulertu dadin.

6.2.1 Alternatibak

Postman

Postman ordenagailu aplikazio bat da, aplikazio honen bidez HTTP eskaeren bitartez APIekin lan egiten da. Aplikazio hau, APIekin mezuak nola izan behar diren frogatzeko erabili ohi da. HTTP mezuen barnean JSON datu blokeak sartzen dira, konfigurazio hori helburuan konfiguratu dadin.

Era berean, programa bat garatzeko erabili daiteke, Python eta Perl informatika lengoaien funtzionaltasun berberak eskaintzen baititu. Era errelean lan egiten du ekipoen datu baseen aurka, konfiguratutako terminoak zuzenean indarrean jarriz ekipoetan.

Desabantaila nagusi bat du, aplikazio hau ez duen erabiltzaile arrunt batek ezin du programak erabili. Gainera, dokumentazio gutxiago dago honi buruz.

Tresna hau frogak egiteko diseinatuta dago eta berez ez da erabiltzen ebazpen gisa.

Python

Python programazio lengoaia multifuntzional bat da; hau da, hainbat funtziotarako erabiltzen da. Hau lortzeko liburutegi ezberdinak erabiltzen ditu, lortu nahi den gauza bakoitzerako liburutegi sorta bat erabiliz. Python objektuei bideratutako programazio lengoaia da eta honek ahalbidetzen du fabrikatzaile ezberdinak definitutako objektuak erabiltzea, APIen sarbidea errazago izan dadin.

Kasu honetan APIekin lan egiteko erabiliko da; beraz, hau lortzeko beharrezko liburutegiak erabiliko lirateke programa azkar bat lortuz. Gainera, Python lengoaiak duen alderdi positibo bat Interneten dagoen dokumentazio kopurua da, programa diseinatzerakoan arazorik egongo balitz, dokumentazio honek era errazean arazoa ebaztea ahalbidetuko du.

Halaber, Python eta bere liburutegiak oso erraz instalatzen da makinetan eta exekutatzeko oso errazak dira programak ez da zergatik izan behar jakituria berezirik.

Azkenik, Pythonen programak CSV motako fitxategiak irakurri ahal dituzte, konfigurazio parametroak eskuz sartzea saihestuz.

Perl

Perl programazio lengoaia C programazio lengoaiaren antzekoa da, baina era zuzenago batean bideratua testu fitxategien kudeaketara. Horregatik, testuak prozesatzeko askotan erabiltzen da, era berean, moldagarria eta muga gutxi dituenez, UNIX sistemak administratzeko erabiltzen da.

Perl lengoaia interpretatu bat da; hau da, konpilatzaile baten beharra behar du. Perl-ek scripten garapen azkarra eta erraza esleitzen du, beraz, proiektuaren kasuan hainbat erraztasun emango lituzke.

Nahiz eta hasiera batean UNIX sistemak kudeatzeko diseinatuta dago, paketeen bidez funtzionaltasun nabari gehitu ahalko lioke, horien arteko bat API REST zerbitzuen erabilera da. REST::Client eta JSON paketeak erabiliz APIekin lan egin daiteke script sinple baten bidez.

6.2.2 Irizpideak

Aukera ezberdinen artean proiektura hobeto moldatzen dena aukeratzea posiblea izan dadin irizpide ezberdinak kontuan hartu dira:

- **Inplementazioa: Diseinatutako ebazpena etorkizunean inplementatzeko erraza izatea baloratuko da, scriptaren erabiltzailea ez da zergatik izan beharko aditua programazioan edo APIetan, beraz honen exekuzio erraztasuna garrantzia handia izango du.**
- **Dokumentazioa: Interneten Scripta egiteko erraztasunak aurkitzea positiboki baloratuko da. Hau da, Interneten programa diseinatzeko dokumentazioa aurkitzeak ingeniaritza orduak aurreztuko lituzke.**
- **Programaren portaera: Diseinatutako programaren errendimendua oso garrantzitsua izango da, programa geldo eta akastun bat ez zen izango programa egoki bat. Beraz, teknologia bakoitzaren zailtasun zein errendimendua oso garrantzitsua izango da, teknologia zail bat akatsak handitzea eragin ahalko luke.**

Irizpide hauek guztiak kontuan edukiz, ebazpenaren aukeraketara igaro behar da.

6.2.3 Ebazpenaren aukeraketa

Aurrean aztertutako irizpide zein aukera ezberdinak kontuan edukita, taula baten bidez ebazpen hoberena zein den erabakiko da:

Irizpideak	Postman	Python	Perl
Inplementazio erraztasuna(%30)	7	9	8
Dokumentazioa (%40)	4	9	6
Programaren portaera (%30)	7	7	8
Guztira	58	84	72

2. Taula: Programazio metodoaren analisiaren taula

Konklusioa: Python izan da aukera hoberen gisa erabaki dena, bere abantaila handiena dokumentazioa izanik. Halaber, inplementatzeko momentuan errazena da eta errendimendu nahiko ona du; nahiz eta, Perl lengoaiarena hobea izan.

6.3 Cluster topologia

Cluster topologiak firewallen portaera aldatzen du, hauek karga kantitate handiagoa jasan dezakete edo master unitatea amatatzen bada beste unitatea bere rola clusterrean har dezake. Orokorrean, bi topologia mota daude Active-Active edo Active-Standby.

Horregatik sareak dituen beharrizanak aztertu behar dira, ebazpen onena aukeratzeko. Trafiko fluxua edo sarearen egonkortasuna aztertu behar da eta honen arabera garrantzia gehien duena ponderaketa handiagoa izango du.

Beraz, bi irizpide nagusi egongo dira, lehen aipatutako biak:

- **Trafiko fluxua aztertzeko gaitasuna.**
- **Sarea egonkor mantentzeko gaitasuna.**
- **Akatsak detektatzeko eta kudeatzeko erraztasuna.**

6.3.1 Alternatibak

Active-Standby

Topologia modu honetan firewall unitate bat era aktiboan lan egingo du eta beste bat era pasiboan. Era aktiboan lan egiten duena trafiko guztia aztertzen du eta era pasiboan lan egiten duena, itxaroten egongo da beste unitatea jauzi arte. Momentu horretan, rol aktiboa hartuko du clusterrean.

Active-Active

Topologia modu honetan firewall unitate biak modu aktiboan lan egiten du eta bakoitzak sarera sartzen den trafikoaren erdia aztertzen du horrela gaitasunak bikoiztuz.

Aldiz, unitate bat jausten denean clusterra jauzten da momentu horretan. Gero, beste unitateak konexioak abiatuko ditu baina zerbitzu mozketa hanidago izango da.

6.3.2 Irizpideak

Cluster topologia bat aukeratzeko momentuan bi irizpide nagusi daude, load balancing gaitasuna; hau da, karga bi unitateen artean banatu edo backup gaitasuna; hau da, zerbitzu mozketa bat saihesteko bigarren unitate bat egongo da rol pasiboan rol aktiboa hartzeko.

Halaber, kontuan edukitzen den beste irizpide bat akatsen aurrean izango duen portaera da. Honen ondorioz, akatsak kudeatzea errazagoa izango da. Cluster topologiaren arabera akatsa non dagoen identifikatzea zailagoa egiten da.

6.3.3 Ebazpenaren aukeraketa

Irizpideak behin definituta, ebazpen egokia bilatu behar da alternatiba ezberdinen artean. Hurrengo taulan irizpide bakoitza ponderatuko da eta alternatibekin erlazionatuz erabaki bat hartuko da:

Irizpideak	Active-Standby	Active-Active
Trafikoa fluxua aztertzeko gaitasuna(%30)	6	9
Sarea egonkor mantentzeko gaitasuna(%60)	9	5
Akatsen identifikatzeko eta kudeatzeko erraztasuna(%10)	9	6
Guztira	81	63

3. Taula: Cluster topologiaren analisiaren taula

Konklusioa: Active-Standby topologia aukeratuko da, sarea egonkorra mantentzea garrantzia handia baitu. Trafiko fluxua aztertzeko gaitasun nahikoa izango baitute sareko firewallak era independentean.

7.Ebazpenaren diseinua

Atal honetan, sarean eskatutako segurtasun neurriak inplementatzeko hautatu dugun ebazpenaren diseinua azalduko da. Gainera, sarearen segurtasun politiken sortzearen automatizazioaren ebazpena ere azalduko da.

Gradu Amaierako Lan honetan, dagoeneko hedatuta dagoen sare enpresarial baten segurtasunaren hobekuntzan arituko gara. Horregatik, hasiera batean, laburki aurkeztuko dugu orain dagoen sarea, diseinatu beharreko segurtasun ebazpenaren abiapuntua baita. Sare honetatik sare berriaren topologiara iragango da.

Ondoren, segurtasun politikaren eraketarako egin beharreko automatizazio programen diseinua azalduko dira.

Azken finean, nahiko logikoa da ebazpen horiei garrantzia ematea, hauek baitira helburua betetzea erraztuko dutenak.

7.1 Babestu beharreko sarearen hasierako egoera

Aztertuko dugun kasua hobeto ulertzeko, bere sare azpiegitura aztertuko da. Aztertuko den sarea hiru egoitza ditu momentu honetan; hau da, A, B eta C egoitzak. Egoitza hauen azpiegitura guztiz aldatuko da, enpresa, gaur sail bakar batean antolatuta dagoena, sail ezberdin bitan banatuko baita. Egoitza hauek azpiegitura ezberdinak dituzte, segurtasun maila ezberdineko elementuak izanik.

Egoitza bakoitzaren azpiegitura logikoa aztertuko da, proiektuaren sare testuingurua hobeto ulertzeko eta jakiteko zer migratuko den eta zer aldatuko edo modu berri batean inplementatuko den kasu bakoitzean.

Azpiegitura hauen segurtasun elementu nagusienak firewallak dira. Firewall bat sare baten trafikoa iragazi egiten du, trafiko jakin bat, arau sorta baten bidez, ahalbidetuz edo blokeatuz. Arau sorta hauen taldeak rulebase edo politika pakete bat eratzen du eta babesten duen sarera sartzen den trafikoa erabakitzen du.

Firewallak hiru egitura nagusietan lan egiten dute:

- **Standalone: Egitura honetan, Firewall bakoitza bere politikak, atakak etab. edukiko ditu eta bera bakarrik lan egiten du; hau da, bere baliabideak erabiliz eta erredundantzia gabe lan eginez.**
- **Active-Active: Egitura honetan, bi firewallak lan egiten dute aldi berean, interfazeak eta beraz, baliabideak bikoiztuz. Hala**

ere, firewall bakar baten moduan aztertzen da, hauek 4 interfaze badute bakoitzak 8 interfazeko firewall baten moduan ikusiko da.

- Active-Passive (Active-Standby) : Egitura honetan, firewall bat era aktiboan lan egingo du eta beste firewall bat standby egoeran egongo da, hots, kide aktiboa jausten denean bere lekua okupatuko du, sareari erredundantzia gehituz.

Firewallak blade formatukoak dira eta blade hauek txartela modukoak dira txasis batean instalatzen direnak, era zentralizatu batean kudeatu ahal izateko. Blade formatuarekin, txartelen bat txarto funtzionatzen badu, ez dugu txasis osoa aldatu behar soilik txartel hori. Halaber, instalatzeko momentuan ere errazten da rackean txasisa sartzen da eta han txertatzen dira txartelak; beraz, etorkizunean txartel gehiago sartzeko gaitasuna ere izango da.

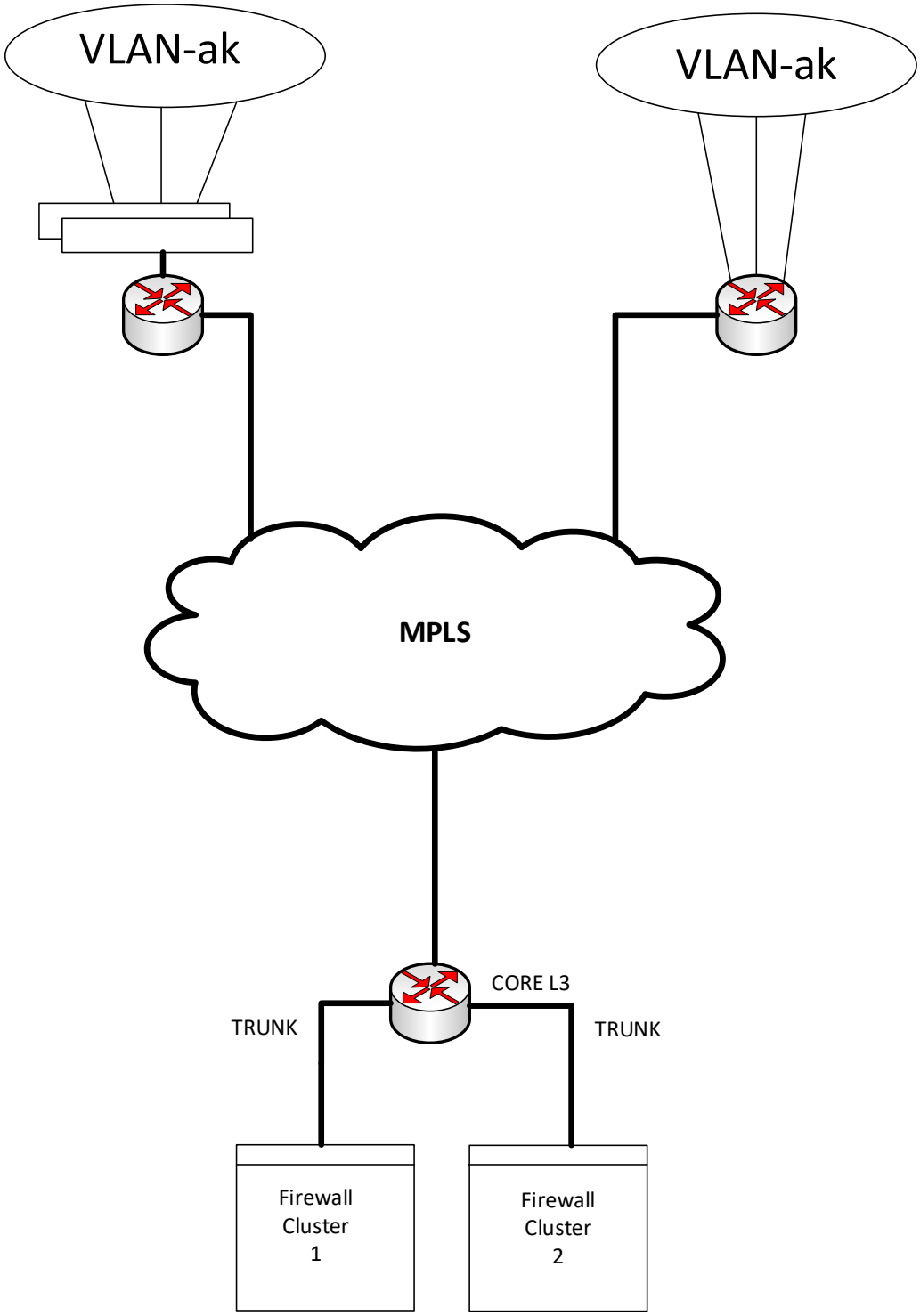
Azpiegituraren arabera, diseinu maila ezberdina garatuko da. Beste faktore eragingarri bat erabilitako fabrikatzailea izango da, honen arabera migrazioa ezberdina izango da. Bi fabrikatzaile berdinen artean beti askoz errazagoa da objektuak eta politikak migratzea, komandoak berdinak izango baitira, aldiz, fabrikatzaile ezberdinen artean ezin da hain erraz erreplikatu, komandoak aldatzen direlako.

Egoitza artean MPLS (Multiprotocol Label Switching) [6] sare bat erabiliz eratuko da komunikazioa, era honetan 2. mailan komunikatuta egongo dira; hau da, lotura mailan, era azkarragoan kudeatuz sarea.

MPLS teknologian pakete bat jasotzen duen lehen bideragailua, LERa (Label Edge Router), ezartzen du pakete honek sarean egingo duen ibilbidea pakete honi bi etiketa jarriz. Bata jarraituko duen bidea ezartzeko eta bestea VPN etiketa bat zein testuinguru enpresariala identifikatzen du, overlay sare bikoitza bat ezarriz. Overlay sare bat beste sare azpiegitura baten gainetik diseinatzen den sare birtuala da.

Gainera, egoitza bakoitzeko firewallak bere bideragailuarekin trunk lotura baten bidez komunikatzen dira. Hau lotura hauek konfiguratzeko era da, access edo trunk izan ahal dira. Access motatakoak soilik VLAN bakarra uzten dute pasatzen loturatik. Aldiz, trunk motatakoak hainbat VLAN pasatzen uzten dute, normalean trunk motako interfazeak uplink eta downlink loturetan ezartzen dira.

Hasierako sarearen interkonexioa definitzen duen eskema aztertzea interesgarria da, ikusteko nola egoitzen arteko interkonexioa ematen den eta egoitza bakoitzaren ikuspegi orokor bat edukitzeko; beraz, 9. Irudian erakusten da hasierako sare osoa:

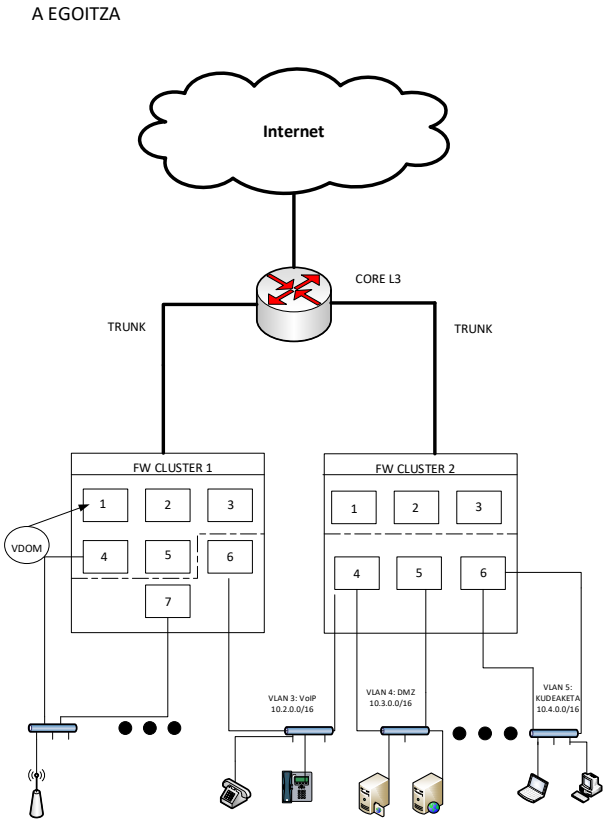


9. Irudia: Hasierako sarearen eskema

7.1.1 A egoitzaren azpiegitura

Lehenengo egoitza 2 firewall cluster ditu, cluster bakoitzak 2 firewall active-active moduan konfiguratuta ditu, baliabideak bikoiztuz. Cluster bien artean VSS-ren (Virtual Switching System) [7] bitartez Active-Standby cluster topologia eratuta dago, bien bat jausten bada orduan bestea honen funtzioa egingo du sarean. Firewall clusterrak Fortinet fabrikatzailearen bladeak dira.

Firewall cluster bakoitza VDOMekin (Virtual Domain) osatuta dago, VDOM hauek firewall birtualen instantziak dira, instantzia hauek firewallak zerbitzu ezberdinetarako instantzia birtual ezberdinak eduki ahal izatea ahalbidetzen du; adibidez, VDOM bat eduki korporatiboentzako, beste bat gonbidatuentzako... Lehenengo clusterrak 7 VDOM ditu eta besteak 6 VDOM. Azpiegituraren eskema logikoa 10. Irudian ikusten dena da:



10. Irudia: A Egoitzaren eskema

Cluster bakoitza CPD ezberdin batean egongo da eta lehen aztertu den moduan, VSSren bitartez komunikatzen dira. Fisikoki bi router ezberdin

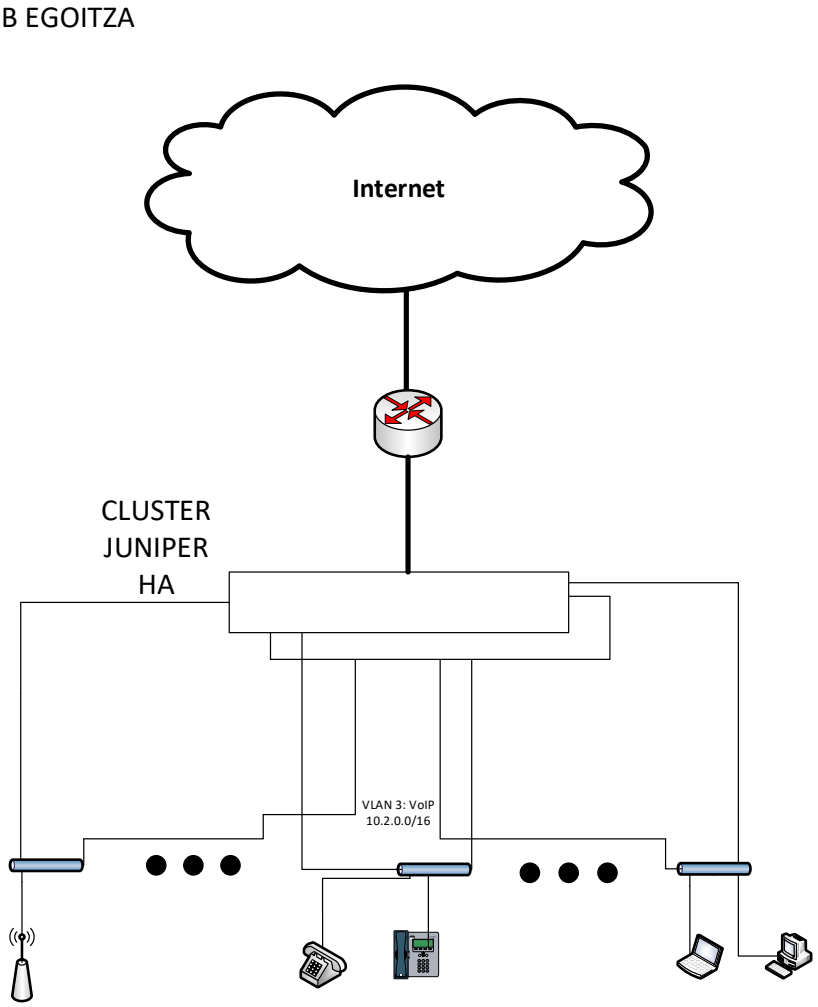
dira eskeman adierazitako CORE L3a, eta hauek dira VSSren bitartez komunikatzen direnak, logikoki router bakar baten gisa lan eginez eta beraz firewallei erredundantzia emanez era berean.

7.1.2 B Egoitzaren azpiegitura

B azpiegitura; aldiz, ezberdina da, erredundantzia inplementatzen du, active-standby cluster bat da, bere baliabideak erredundatuz; hau da, bat jausten denean bestea bere rola hartuko du zerbitzu ukatzea saihestuz, lehen azaldu den moduan.

Cluster hau, Juniper firewall pare bat eratzen dute; beraz, aurreko clusterrekiko fabrikatzailea aldatu da.

B egoitzaren azpiegituraren eskema 11. Irudian aztertzen da:



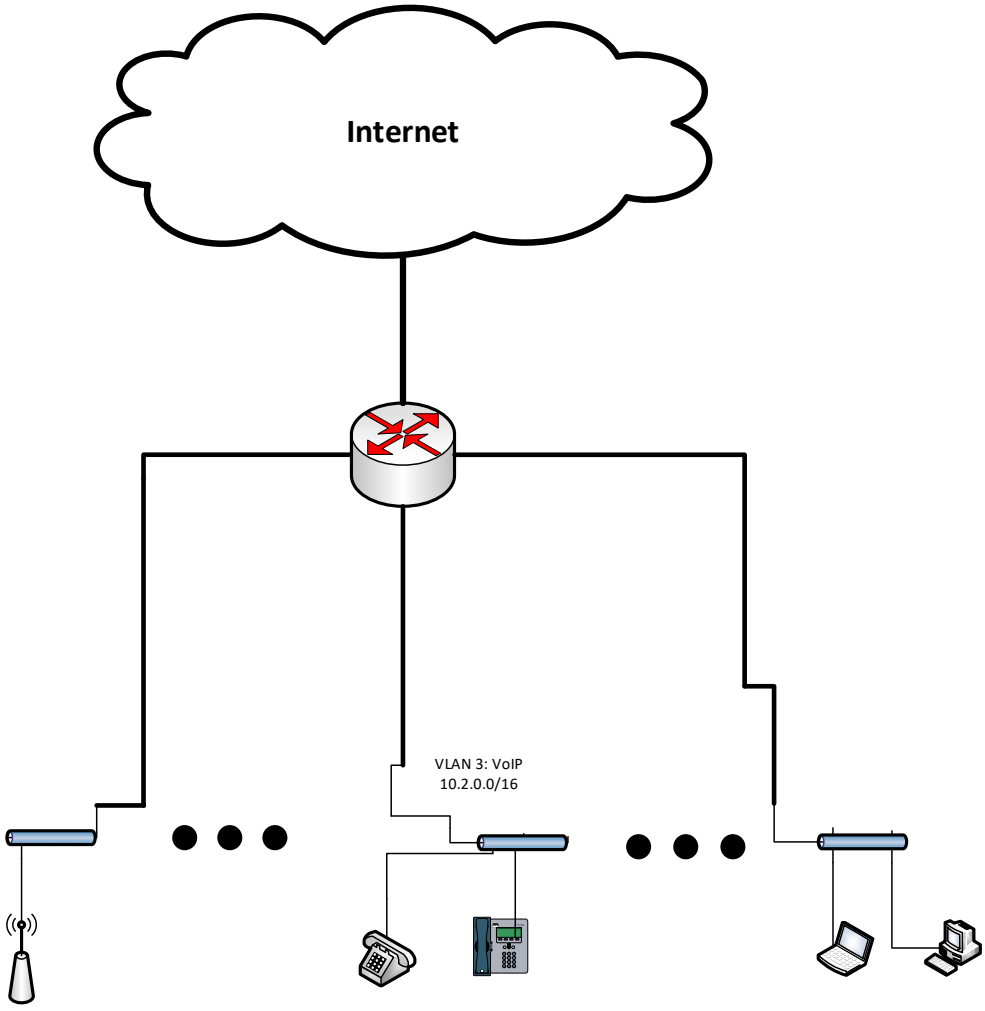
11. Irudia: B egoitzaren azpiegitura

7.1.3 C Egoitzaren azpiegitura

C Egoitzak segurtasun elementu gutxien dituen egoitza da. Beraz, diseinu gehien beharko duen egoitza da, segurtasun ebazpena guztiz berria izango da.

Egoitzaren azpiegitura router eta VLAN taldeez osatuta dago soilik; beraz, segurtasun diseinu minimoa du. Azpiegituraren eskema 12. Irudian ikusten dena da:

C EGOITZA



12. Irudia: C egoitzaren azpiegitura

7.2 Sare berriaren diseinua

Sare berrian, segurtasun tresna berriak inplementatuko dira sarea modernizatuz eta honen segurtasuna handituz. Diseinu alternatiben analisitik ateratako Fortinet fabrikatzailearen firewallak ezarriko dira. Modelo zehatza fabrikatzailearekin adostuko da, hardwarearen arabera erabakiko baita, geroago ikusiko den moduan, egoitza guztietan ez da modelo bera inplementatuko.

Diseinatutako segurtasun politika UTM (Unified Threat Management) politika izango da, hau da, Antibirus, Threat Prevention, Rulebase, Application Control eta Web Filter politikak barnean hartzen dituen kontzeptua.

Fortineteko firewallak aukeratzearen ondorioz, A egoitzan fabrikatzaile berdinen arteko migrazioa egingo da, asko erraztuz lana, konfigurazio objektuen eraketen sintaxia berdina izango baita.

Aldiz, B eta C egoitzetan ez da hau gertatuko. B egoitzan, Juniper eta Fortinet arteko migrazioa egin beharko da, lana zailduz. C egoitzan firewallik ez dagoenez, diseinu guztiz berria egin beharko da, lehen aipatutako UTM politika eratuz.

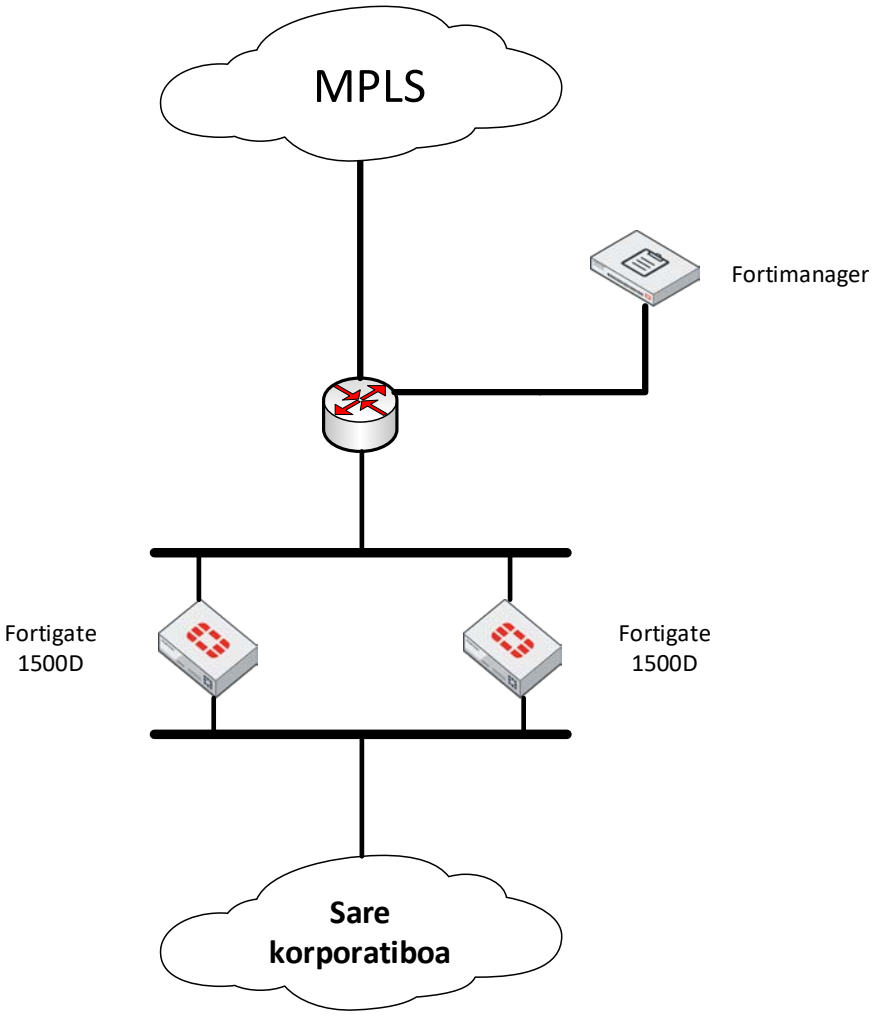
Ebazpenaren zehaztasunak egoitza bakoitzean ezberdinak izango direnez, atal ezberdinetan azalduko dira.

7.2.1 A egoitzaren diseinu berria

A egoitzan FortiGate 1500D bi arteko clusterra inplementatuko da. Firewall hauetan lehengo topologiako lehenengo clusterretik 5 VDOM eta bigarren clusterretik 3 VDOM migratuko dira, sail berriarenak baitira.

Firewall fisiko hauen konfiguraziorako FortiManager birtual bat inplementatuko da. FortiManager hainbat FortiGate era zentralean kudeatzeko plataforma da.

Ondoren, A egoitzaren topologia berrirako ebazpena erakutsiko da, bi firewall active-standby moduan instalatuko dira. Haien artean clusterra eratzeko VSSren bidez komunikatuko dira, CPD ezberdinetan egongo baitira. Era berean, birtualki instalatuko da FortiManager bat clusterra atzitzeko. 13. irudian ikus daiteke eskemaren errepresentazioa:



13. Irudia: A egoitzaren topologia berria

Eratuko ditugun segurtasun mekanismoak FortiManagerrean konfiguratuko dira eta honek firewall fisikoetan instalatuko ditu pool baten bitartez; hau da, FortiManagerrak segurtasun mekanismoak pool batera igoko ditu eta pool horretatik FortiGateak instalatu behar dutena deskargatuko dute. Alderantzizko bidea ere egin daiteke baina ez du "Best practise" doktrinak jarraitzen, kudeaketa zentrala konfigurazioak ezartzen dituen makina izan behar baita.

Gainera, inplementatuko dira ezarritako UTM iragazketa bat; hau da, trafikoa kontrolatzen dituzten politikak, sare korporatiboaren arabera.

UTM iragazketaren barruan hainbat segurtasun mekanismo daude: AntiMalware, IPS, URL Filtering eta Application Control.

Gainera, kontuan eduki behar den puntu bat firewallen bertsioak dira. Migratzeko garaian konfigurazio komandoak aldatzen dira bertsio batetik bestera eta akatsak sortu ahal dituzte.

Lehen aipatu denez, cluster bat sortuko da; horretarako, garrantzi handia du HAren (High Availability) konfigurazioa.

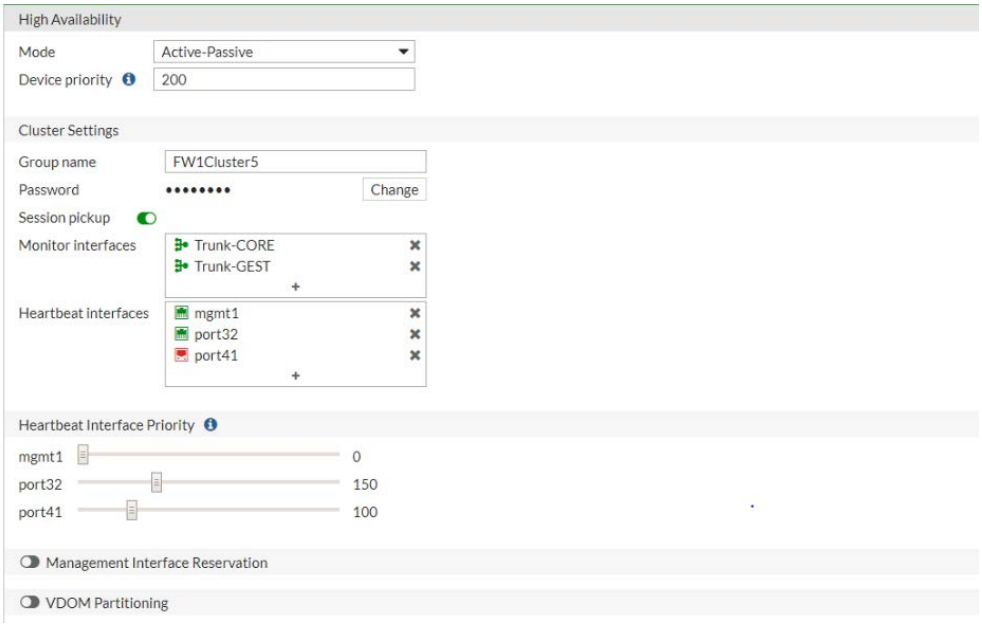
7.2.1.1 HA Konfigurazioa

Migrazio pausuetatik kanpo beste konfigurazio batzuk daude, HA konfigurazioa adibidez. Konfigurazio honen bitartez clusterra sortzeko trafikoa ezarri egingo da eta era honetan proiektuan lehen aipatu den Active-Standby modua ezarriko da.

HA konfiguratu behar da firewall bakoitzean independenteki, cluster izen eta pasahitz bera konfiguratuz. Konfigurazioa kargatuta duena Master kidea izan behar denez, lehentasun parametroa Slave kidearena baino altuagoa izan behar da.

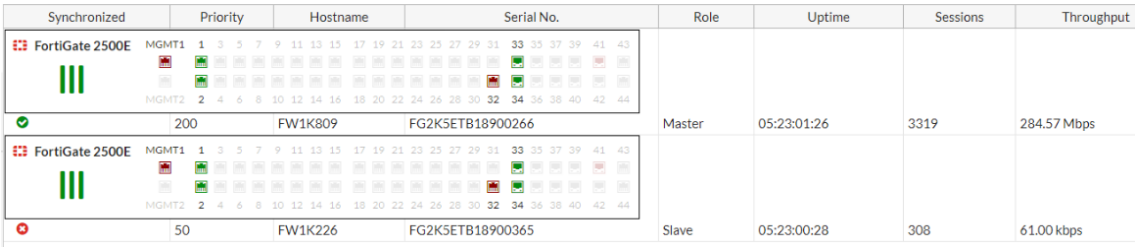
Hala ere, standby kidearen lehentasuna defektuzkoa baino altuagoa izan behar da. Etorkizunean, Masterra aldatu nahi bada ekipamendu berria clusterrean sartzerakoan lehen standby zena Master bihurtu beharko baita konfigurazioa gal ez dezan.

Diseinatu den HA konfigurazioa 14. Irudian ikusten dena da:



14. Irudia: FortiGaten HA konfigurazioa

Konfigurazio hau bi ekipoetan eginez, lehentasuna baxuagoa izanez standby egoeran edo era pasiboan egongo den ekipoan lehen aipatu den bezala, firewall biak komunikatzeko gai izango dira eta HA trafikoaren ondorioz, Clusterra osatuko da, 15. irudia erakutsiz:



15. Irudia: Cluster osatua

Konfigurazio honek ahalbidetzen du clusterreko kide bakoitzak CPD ezberdinetan egotea; hau da, eraikin ezberdinetan egotea. Masterra dagoen eraikinean istripu bat gertatzen bada; adibidez, argi mozketa bat, trafikoa Standby unitatea kudeatzen hasiko da.

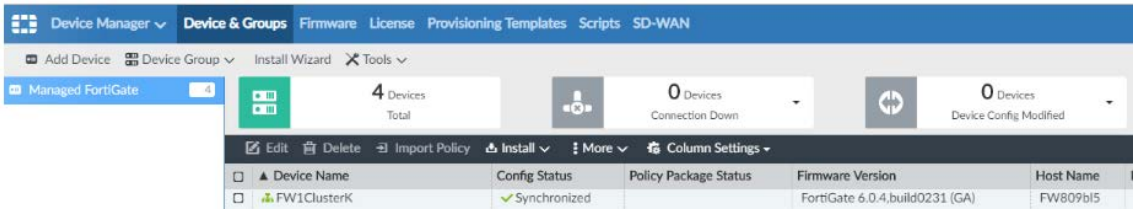
Clusterraren funtzionamendua aztertzeko HA proba batzuk egingo dira, portaera posible guztiak aztertuz, proba hauek metodologia atalean aztertuko dira.

7.2.1.2 FortiManager Integrazioa

Gainera, FortiGate clusterra FortiManagerrean integratu behar da, kudeaketa zentraleko segurtasun ebazpena lor dezan. Etorkizuneko segurtasun politiken eraketak zuzenean FortiManagerrean egingo baitira.

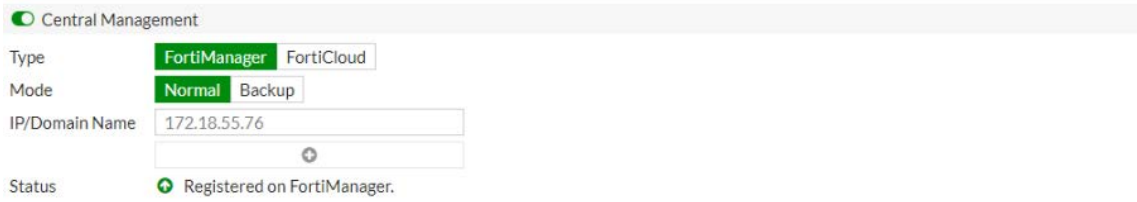
Hau egiteko, FortiManagerraren device manager atalean, *add device* egin beharko da. IP (Internet Protocol) helbidea, erabiltzailea eta bere pasahitza jarri beharko da. Honek clusterra detektatuko du eta bere konfigurazioa bereganatuko du.

Lortuko zen emaitza FortiManagerrean holako itxura izango luke:



16. Irudia: FortiManager gailuen kudeaketa atala

Era berean, FortiGatean kudeatzen duen FortiManagerraren IPa ikusi beharko da dashboardean. 17. irudian ikusten den bezala:



17. Irudia: Kudeaketa konfigurazioa FortiGatean

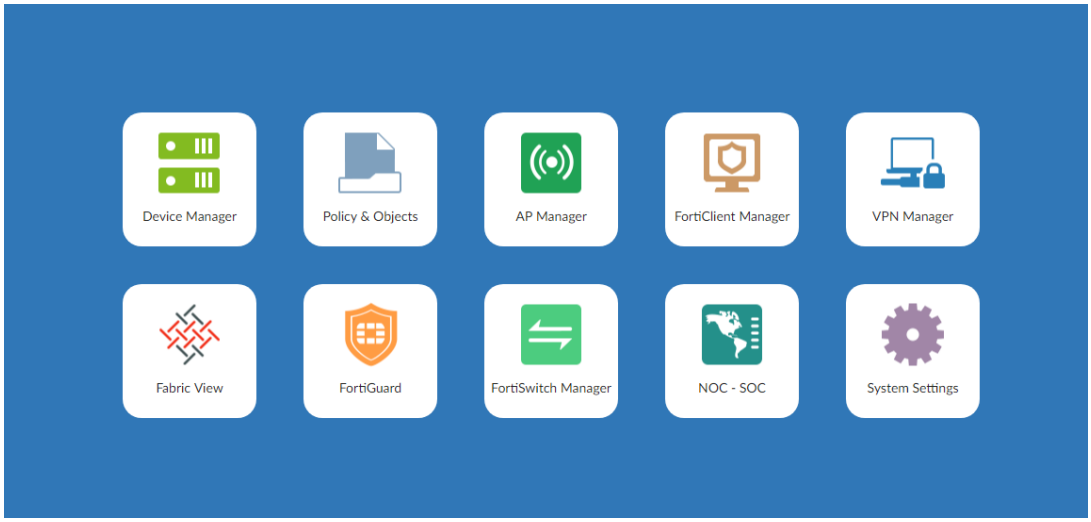
FortiManagerrak firewall honek dituen VDOM-en konfigurazioa egiteko gaitasuna izango du, honek ematen dituen aukera guztiak ustiatuz; hau da, segurtasun politiken konfigurazioa, VPN konfigurazioak...

Hasierako menuan zein ADOMera (Administrative Domain) konektatu nahi den galdetuko du. ADOMa [8] gailu ezberdinak batzen ditu domeinu batean horrela administrari ezberdinak soilik haien domeinura sartu behar dira; beraz, banatzen dira gailuak administrari ezberdinen arabera. Menu hau 18. Irudian erakusten dena da:

18. Irudia: ADOM ezberdinak aukeratzeko menua

Gainera, esan beharra dago, ADOMak bere barnean hartzen dituen gailuen artean, bertsio ezberdinak kudeatzeko gai izan behar da. Honek ahalbidetzen du FortiManager batean bertsio ezberdinetako FortiGateak izatea konfigurazio bateraezintasunik gabe.

Ondoren, ADOM bat aukeratzerakoan FortiManagerrak esleitzen dituen funtzionalitate ezberdinak agertzen dira, konfiguratu nahi dena aukeratu dadin. Hurrengo funtzionalitateak eskaintzen ditu:



19. Irudia: FortiManagerraren funtzionalitateak

VDOM bakoitzean aldaketa bat egiten denean, aldaketa hauek firewalletan kargatu daitezen, instalazio bat hasieratu beharko da, hau ere aurrerago ikusiko den automatizazio programaren barnean garatuko da.

7.2.2 B Egoitzaren diseinu berria

Egoitza honetan, lehen aipatu diren Juniper SRX 550etatik Fortinet 501E firewalletara aldatuko da. Beraz, ekipamendu berriarekin hainbat funtzionalitate ezberdin lortuko dira. Hala nola, VPN ebazpena edo DDoS erasoen aurkako babespen efektiboa.

Juniper SRX teknologia, diseinu alternatiben analisietan aipatu den moduan, bideratze lanetara bideratuegia dago eta askotan segurtasun ebazpen ahulak eskaintzen ditu.

Kasu honetan 501E firewall bi instalatuko dira Active-Standby egitura bat osatuz, horrela Fortinet defendatzen duen HA (High Availability) lortuz. Hau da, edozein motako mozketa edo arazo egonda ekipo batean bestea trafikoa hartzailearen rola hartuko luke.

A egoitzan azaldu den bezala arazo elektrikoak saihesteko CPD (Centro de Procesamiento de Datos) ezberdinetan egongo dira firewall bakoitza, horrela area geografiko batean arazo bat badago, beste area batean dagoen ekipamenduak era aktiboan jo egingo du.

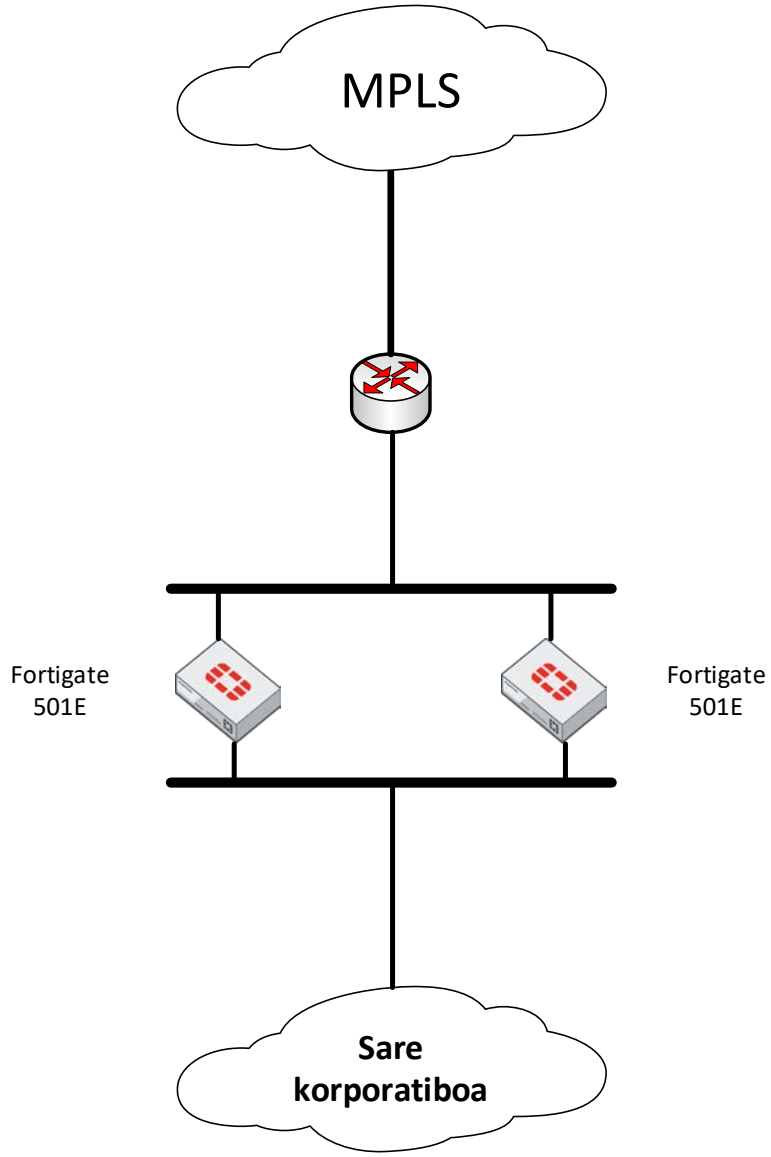
Beraz, era logikoan komunikatuko dira soilik, era fisikoan lotuta egon gabe egongo baitira; hau da, lotura mailan egongo dira lotuta.

Diseinu berri hau ez da egongo integratuta FortiManager kudeaketa ekipamenduarekin kudeaketa maila hori ez baita beharrezkoa kontsideratu, trafiko maila ta konfigurazio kantitateak baxuagoak baitira.

Era berean, automatizazio inplementazioa ez da egoitza honetan aplikatuko. Automatizazio hau FortiManagerrarako soilik pentsatuta baitago aurrerago aztertuko den moduan.

Sare eskema berrian trafiko irteera MPLS sare batetik egingo da, aurrean zegoen topologia moduan, bideragailu baten bitartez.

Sare eskema berria 20. irudikoa izango da:



20.Irudia: B egoitzaren sare eskema berria

Sare berri honetan UTM politika inplementatuko da, segurtasun mekanismo gehiago inplementatuz; adibidez, URL (Uniform Resource Localizator) filtering, Application Control...

HA konfigurazioa A egoitzako konfigurazio berbera izango da, beraz honen azalpena ez da egingo erredundantzia saihestuz

7.2.3 C Egoitzaren diseinu berria

Egoitza honetan segurtasun inplementazioa guztiz berria izango da; beraz, ez dira migrazio lanak antolatu behar. Gainera, ez da FortiManagerrean inplementatuko eta beraz, ez dira egongo inolako automatizazio scripten erabilerarik. B egoitzan azaldu den moduan, bi egoitz hauek trafiko maila eta konfigurazio kantitate txikiagoak jasango dituztelako.

FortiGate 501E bi instalatuko dira Active-Standby topologian, A eta B egoitzetan bezala, HA funtzionalitatea erabiliz.

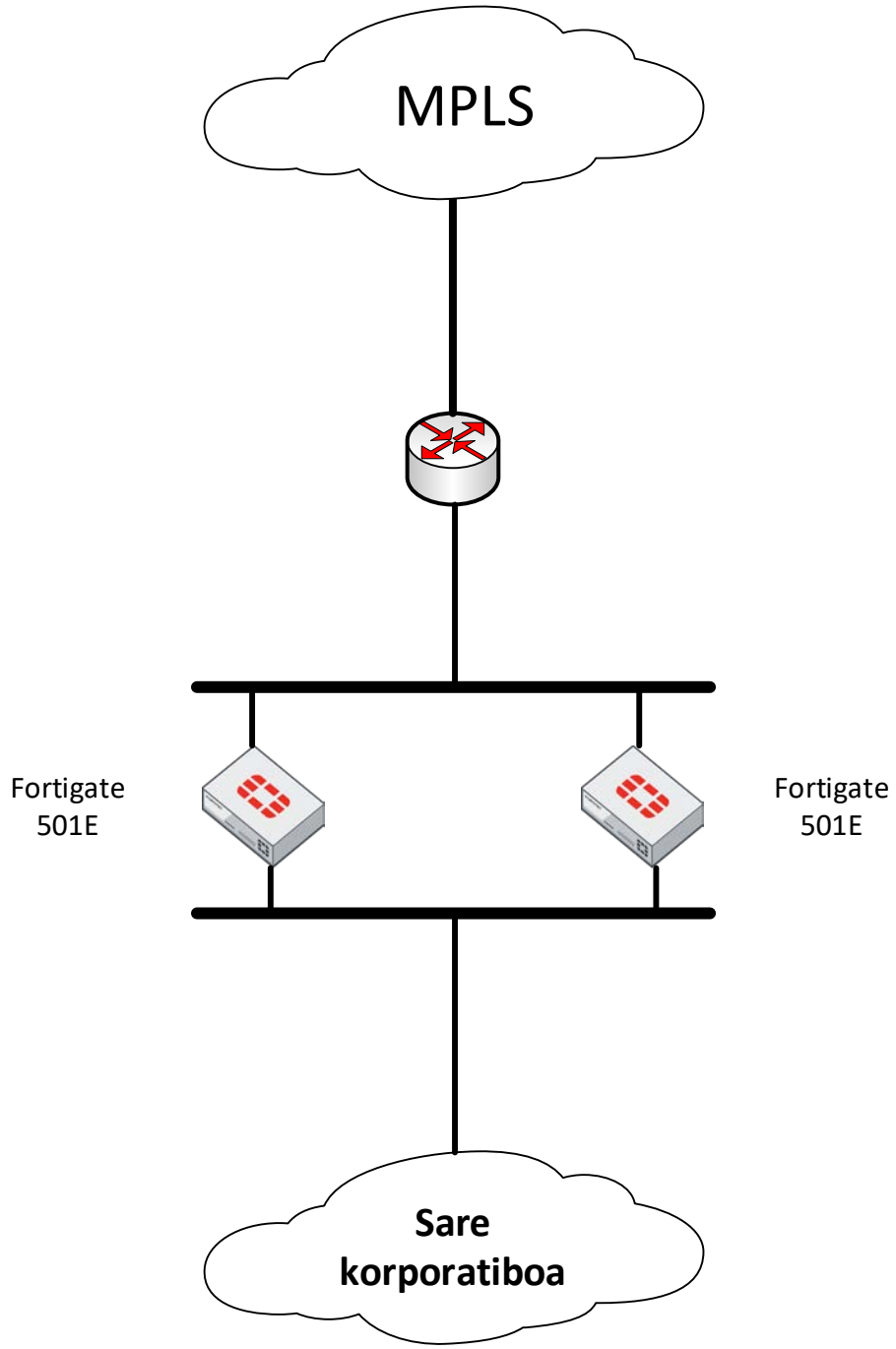
Lehen aipatu den moduan beste egoitzetan, makina bakoitza CPD ezberdinean egongo da, mozketa bat egongo balitz, kontingentzia mekanismo bat eduki dezan azpiegiturak.

Kasu hau ezberdina da, inolako segurtasun politiken jakituriarik ez baita edukiko. Ondorioz, ebazpen berri bat bilatu beharko da sarearen beharrizanen arabera. Hau VLAN ezberdinak aztertuz eta hauetan dauden zerbitzuak edo makineria ezberdinak aztertuko dira, horrela jakin dadin segurtasun arauak nola sortu.

Gainera, azkenengo araua ALLOW ekintzarekin utziko da, firewalletik ihesi egiten duen trafiko desiragarria identifikatzeko. Era honetan, segurtasun politika oso bat lortu ahalko da.

Segurtasun mekanismoen atalean era nabarmenago batean ikusiko da hauetara zuzenki lotuta dagoen atalean. Hor UTM politika era luzeago aztertuko da, honen mekanismo bakoitza aztertuz.

Sare eskeman, lehen bezala, firewallak sare korporatiboa izango dute eskegita eta Interneterako sarbidea MPLS sare batetik izango dute. Eskema B egoitzaren oso antzekoa izango da, 21. irudian ikusi ahal den moduan:



21. Irudia: C egoitzaren sare eskema berria

7.3 Sare berrien segurtasun mekanismoak

Sare berrietan mekanismo segurtasun mekanismo berriak inplementatuko dira segurtasun neurriak hobetzeko. Segurtasun mekanismo hauek Application Control, Web Filter eta SSL-inspection (Secure Sockets Layer) izango dira. Mekanismo hauek konbinatuko dira segurtasun arauekin segurtasun politika sendo bat ezartzea posiblea izateko.

Gainera, VPN-SSL profilak konfiguratuko dira VPN atariak inplementatzeko. Egoitza bakoitzean, segurtasun mekanismoak ezberdinak izango direnez, bananduko dira azaltzeko momentuan.

Orduan, segurtasun mekanismoak A, B eta C egoitzetan bananduko dira eta egoitza bakoitzaren barnean segurtasun mekanismo ezberdinak azalduko dira.

7.3.1 A egoitzaren segurtasun mekanismoak

Egoitza hau trafiko karga handiena izango du; beraz, segurtasun mekanismo sendoenak izango ditu, egoitza nagusia baita. Beraz, hasiera batean segurtasun arauen eredu bat azalduko da eta ondoren, segurtasun arau hauek segurtasun profilekin erlazionatuko dira.

Segurtasun arauak

Segurtasun arauen politika diseinatzeko sarearen ezaguera handia izan beharko da. Sarean dauden sare ezberdinak aztertuko beharko dira bere beharrizanen arabera zerbitzu ezberdinak sare horietarako ahalbidetu beharko dira eta.

Beraz, trafiko fluxu ezberdinak identifikatu beharko dira; hau da, zein da jatorria, helburua eta trafikoaren protokoloa identifikatu beharko da, hau behin eginda, datu horiekin arau bat sortu beharko zen trafiko hori ahalbidetua izan dadin. Arau hauek atal ezberdinetan banatzen dira, atal hauek zerbitzu berdintsuen edo sare baten arabera egiten ohi dira. Beraz, atal hauen arauak gauzak komunean daukate.

Behin azalduta arauen egitura nola den, arau atal baten eredua erakutsiko da 22. irudian:

ID	From	To	Source	Destination	Schedule	Service	Action	Security Pr...	Bytes
Reglas_APM 29									
103278	any	any	VDI_INDRA_172.18.148.1	172.18.78.249 172.18.78.250	always	ALL	ACCEPT		196.61 MB
103271	any	any	VPN_APM_Axians	172.18.78.249 172.18.78.250	always	domain-tcp LDAP_UDP	ACCEPT		8.52 kB
103272	any	any	VPN_APM_Axians	ges1impre_datos_172.18.78.83	always	LDAP_UDP domain-tcp microsoft-ds t49152-65535 t135	ACCEPT		0 B
103273	any	any	VPN_APM_Axians	cor1servpro_172.18.78.223	always	microsoft-ds	ACCEPT		0 B
103274	any	any	VPN_APM_Axians	NLB_Intranet	always	HTTPS	ACCEPT		369.03 MB
103275	any	any	VPN_APM_Axians	wgroup2frontpro_172.18.78.27 172.18.78.13	always	HTTP	ACCEPT		0 B
103276	any	any	VPN_APM_Axians 172.18.181.101	Router 4500	always	TELNET	ACCEPT		197.89 MB
103361	any	any	VPN_APM_Axians	172.16.1.39 172.16.1.66	always	GestorBDlq_udp2635 GestorBDlqiq_2639	ACCEPT		0 B

22. Irudia: Araua atal baten adibidea

Irudian ikusi ahal den moduan, iturri eta helburu bat ezartzen dira arau bakoitzean, bai sare mailan bai maila fisikoan; gainera, zerbitzuak definitu beharko dira. Era berean, irudian ikusten den moduan, ekintza ere definitu beharko da, hau da, araua onartzeko edo ezeztatzeko izaera izango duen definitu behar da.

Aurrekoarekin lotuta dagoen kontzeptua arauen ordena da. Arauak orden sekuentzialean ezartzen dira; hau da, trafiko mota bat lehenengo arauarekin ahalbidetzen bada, ez da konparatuko hurrengo arauekin.

Hori dela eta, kontuan eduki beharko da eta sare bat zerbitzu batzuk ahalbidetuak izango baititu eta beste batzuk ezeztatuak, kontuan eduki beharko da zerbitzuen parametroa ondo definitu beharko da, kontu handia eduki behar da any jartzearekin. Bestela ondoren edozein arau beste zerbitzu zehatz batekin definitzen bada, erroreak emango lituzke.

Hala ere, kasu hau kasu sinplea da, beste kasu batzuetan arauak segurtasun profilak erantsita dituzte. Segurtasun profil hauek beste segurtasun mekanismoen barnean definiturik daude.

Horregatik, arauen beste eredu bat erakutsiko da segurtasun mekanismo ezberdinekin.Arau sorta honetatik segurtasun mekanismo ezberdinen azalpenera joan ahal izateko. 23. irudian ikusiko da arau sorta hau:

ID	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Bytes
VLAN Invitados 4									
103375	any	any	VLAN982_Invitados	Pooles_Priv_10 Pooles_Priv_172.16 Pooles_Priv_192.168	always	ALL	ACCEPT	WEB PERFIL_CORP_Navegacion_Euskaltel APP APP_Control_CORP_Euskaltel SSL certificate-inspection	0 B
102475	any	any	VLAN982_Invitados	all	always	Web Access POP3 POP3S IMAP +3	ACCEPT	WEB PERFIL_CORP_Navegacion_Euskaltel APP APP_Control_CORP_Euskaltel SSL certificate-inspection	0 B
102476	any	any	VLAN982_Invitados	coradpro_srv_virtual_DHCP	always	DHCP	ACCEPT		0 B
102474	any	any	VLAN982_Invitados	all	always	ALL	DENY		0 B

23. Irudia: Segurtasun profilak arauen barnean

Irudian ikusten den bezala segurtasun politika honetan 3 segurtasun profil erabiltzen dira, lehen aipatutako Web Filter, Application Control et SSL-inspection. Honek eragiten du arau bete behar dela eta gainera, segurtasun profilen eskakizun minimoak bete behar dira.

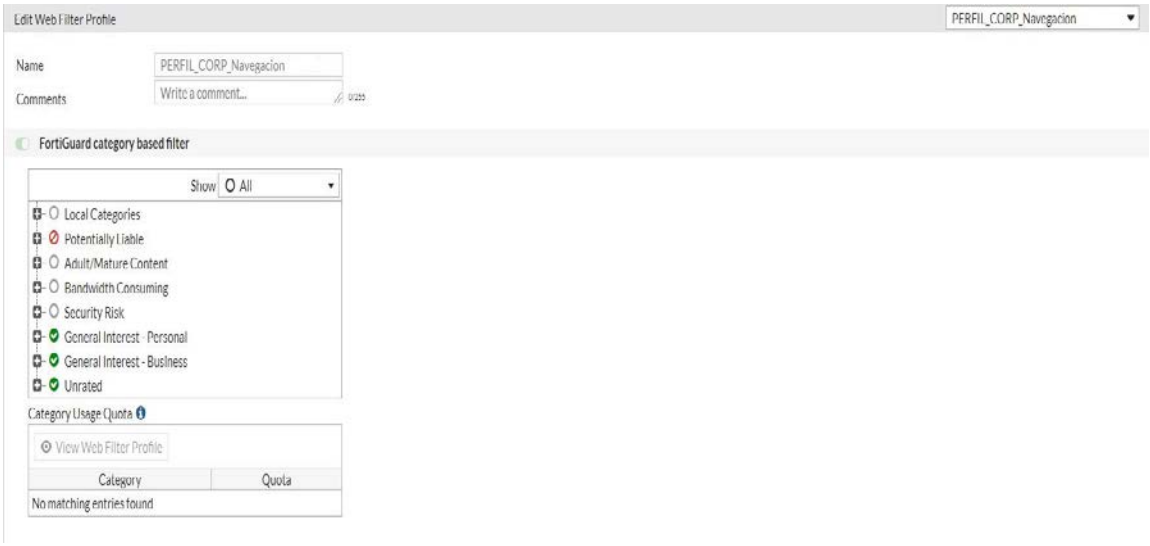
Ondorioz, segurtasun profil hauek banaka aztertu beharko dira ikusteko ze inplikazio izango dute sarean.

Web Filter

Segurtasun profil honetan webguneen edukiaren arabera iragaziko da trafikoa; adibidez, nagusientzako edukia duten webguneak blokeatu daiteke, horrela lanean webgune desegokiak blokeatuta egon ahal dira.

Era honetan, hainbat webgune maltzur edo eduki desegokiarekin blokeatzeko gai da sarearen kudeaketa egiten duen sailak. Gainera, gonbidatuen WiFIra konektatzen diren gonbidatuen konexioak mugatu daitezke, horrela sarearen gaitasunak mantenduz.

Sare honetan inplementatuko den Web Filter profila, 24. irudian ikusten dena da:



24. Irudia: A egoitzaren Web Filter profila

Profil honetan ikusten moduan, hainbat eduki mota ahalbidetuko dira beste batzuk azpimoten arabera ahalbidetu edo blokeatuko dira eta beste batzuk blokeatuko dira.

Gainera, ahalbidetutako edukien artean batzuk monitorizatuko dira, horrela ikusteko eduki horretara nork nabigatu duen.

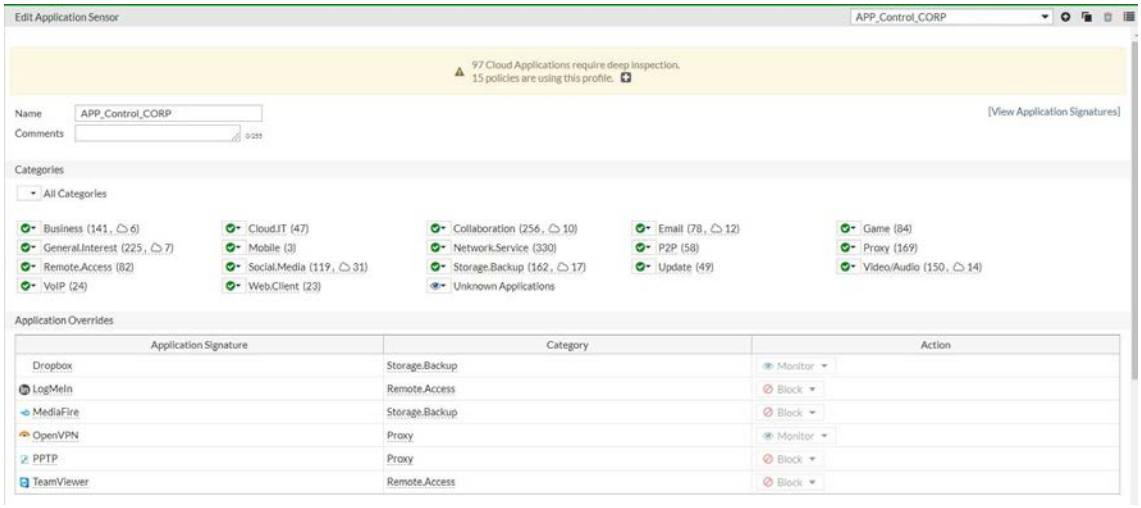
Application Control

Segurtasun profil honetan, aurreko profilaren antzera trafikoa iragazten da, baina kasu honetan aplikazioaren arabera iragaziko da trafikoa; adibidez, TeamViewer aplikazioaren trafikoa ahalbidetu edo blokeatu daiteke.

Horrela, sare enpresarial batean korporatiboak ez diren aplikazioak blokeatu ahal dira eta era honetan lanean beharrezkoak ez diren aplikazioak blokeatuko lirateke.

Esan daiteke, aurreko profilean trafikoaren eduki motaren arabera kudeatzen da trafikoa; aldiz, kasu honetan trafikoaren edukiaren arabera iragazten da trafikoa.

A egoitzaren kasuan 25. irudian ikusten den profila inplementatuko da:



25. Irudia: A egoitzako Application Control profila

Kasu honetan, Fortinet identifikatuta dituen aplikazioak ahalbidetuko dira; aldiz, aplikazio ezezagunak monitorizatuko dira trafiko hori identifikatu dezan firewalla.

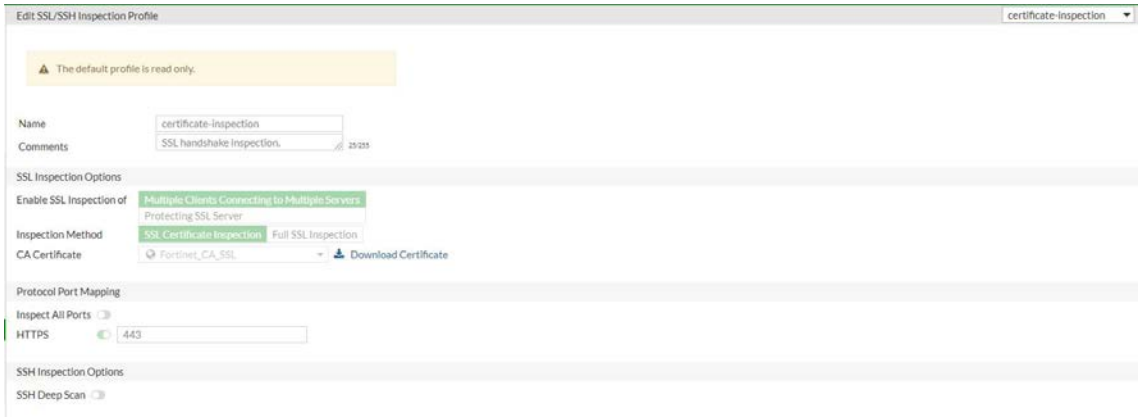
Hala ere, Application Overrides eremuan ikusten diren aplikazioak salbuespen gisa kudeatuko dira, aplikazio hauek identifikatuen artean ezberdin tratatuko dira, batzuetan blokeatuko dira eta beste batzuetan monitorizatuko dira.

Aurreko profila eta profil hau ez dira balizkoak izango SSL-inspection profila gabe, HTTPS trafiko zifratua miatzeko gai izan gaitezen ezinbestekoa baita.

SSL-inspection

Profil honi esker HTTPS trafikoa miatzeko gai izango da firewalla eta horrela Web Filter eta Application Control profilak bere lana egin ahalko dute, trafikoa zifratua egongo balego, firewalla ez litzateke izango kapaza trafiko mota edo trafikoaren aplikazioa aztertzeko gai.

Beraz, firewall honetan defektuzko SSL-inspection profila erabiliko da, 26. irudian ikusi ahal den bezala:



26. Irudia: A egoitzaren SSL-inspection profila

Gainera, bisitatuko diren webguneen SSL zigiluak egokiak diren edo konfiantzazko CA batek esleitzen badu aztertuko da, hau da, zigilu horrek ematen duen entitatea konfiantzazkoa ikusiko da.

7.3.2 B egoitzaren segurtasun mekanismoak

Egoitza honetan trafiko zama ez denez hain handia izango, identifikatzeko errazagoa izango da. Beraz, arauak egingo dira era errazago batean ez baitira hainbeste sare firewalletatik eskegita egongo.

Kasu honetan lehen A egoitzan aztertu den moduan, segurtasun arauak dira lehenago aztertuko diren segurtasun mekanismoak.

Segurtasun arauak

Kasu honetan lehen ikusi den moduan, segurtasun politika pakete bat eratuko da. Lehen aipatu den moduan, iturri eta helburu posible guztiak aztertuko dira eta kontu handiarekin segurtasun arauak sortuko dira. Arau hauek trafiko egokia ahalbidetuko dute eta desegokia blokeatuko dute.

Egoitza honetako segurtasun arauen adibidea 27. irudian aztertu daiteke:

ID	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Bytes
Acceso TOTAL 120									
49	any	any	all	GRUPO_DESTINOS	always	ALL	ACCEPT		367.83 GB
252	any	any	cor003s217_172.21.60.101	172.18.255.6 172.18.255.4	always	tl8081	ACCEPT		
253	any	any	172.18.255.6 172.18.255.4	cor003s217_172.21.60.101	always	tl92	ACCEPT		
2	any	any	srv_CDRs_Bidali_172.21.40.231 srv_172.21.41.122 srv_10.0.128.28 cor0001s218.rJan_172.21.40.215 +10	1ftp	always	SSH	ACCEPT		102.61 GB
254	any	any	cor002s217_172.21.50.156 cor002s218_172.21.50.162 cor0001s217.rJan_172.21.40.212 cor0001s218.rJan_172.21.40.215	Red_172.18.130.0	always	X11 echo-reply echo-request TRACEROUTE	ACCEPT		1.74 GB
135	any	any	cor0001s218.rJan_172.21.40.215	NLB_Intranet	always	http-https	ACCEPT		
106	any	any	srv_10.1.148.2 srv_10.1.148.3 srv_10.1.147.0_24 Srv_172.21.40.132 +2	areaclienteprivada_172.18.50.87	always	tl8080	ACCEPT		13.73 MB
215	any	any	PCs_Total	Pega_BBDD	always	sqlnet1_sqlnet2-1521	ACCEPT		0 B

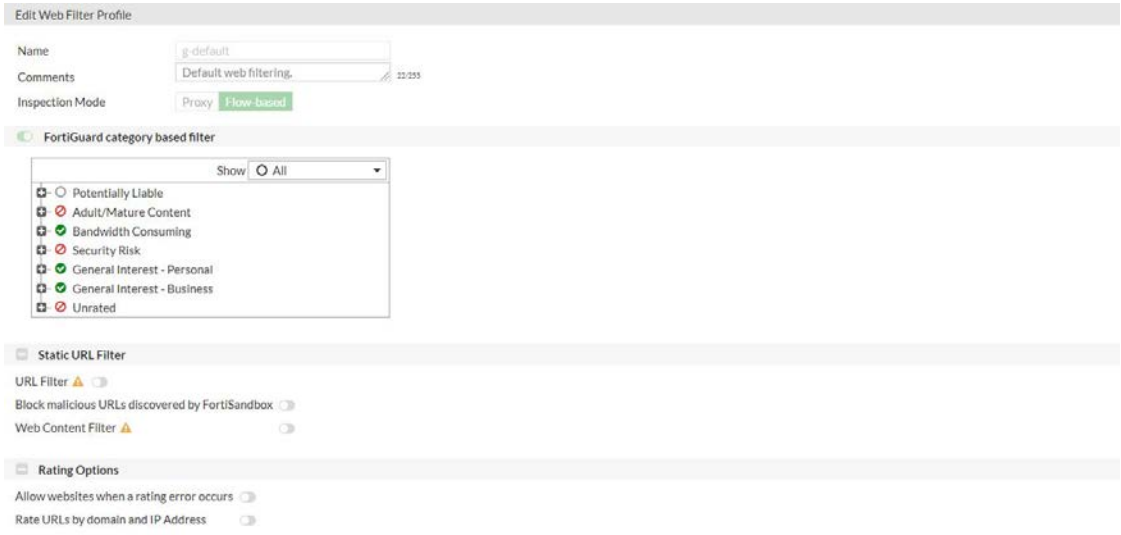
27. Irudia: B egoitzaren segurtasun arauen eredua

Ikus daitekeen bezala, A egoitzaren antzeko forma du B egoitzaren segurtasun arauak, kasu honetan kudeaketarako trafikoa ahalbidetzen da gehien bat zerbitzu gehiegi ez baitaude.

Kasu honetan ez daude segurtasun profil berririk egiteko beharra; beraz, defektuzkoak erabiliko dira. Beraz, bakoitza laburki azalduko da.

Web Filter

Aurreko atalean azaldu denez defektuzko profilak erabiliko dira; beraz, profiletan azterlan sakona ez da egingo. B egoitzan indarrean egongo den defektuzko profila, 28. irudian ikusten dena izango da:



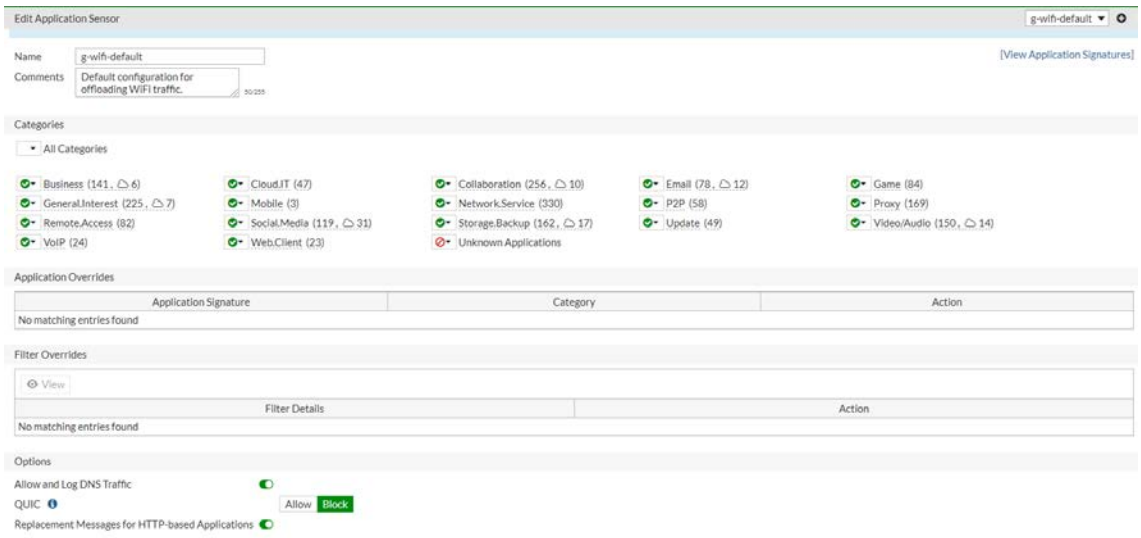
28. Irudia: B egoitzaren Web Filter profila

Ikusi ahal den moduan, zuzenean eduki mota gehienak edo blokeatuta edo ahalbidetuta daude; beraz, trafikoa ez da monitorizatuko eta soilik blokeatuko da.

Application Control

Aurreko profilean bezala defektuzko profila ezarriko da segurtasun arauetan. Kasu honetan, Fortinet lan handia egiten du konfiantzazko aplikazioak identifikatzen, beraz, segurtasun mekanismo nahiko sendoa izango da.

Aplikatuko den Application Control profila 29. irudian ikusten dena izango da:



29. Irudia: B egoitzaren Application Control profila

Ikusten den moduan trafiko guztia ahalbidetuko da aplikazio ezezagunak izan ezik. Gainera, ez da Application overrides funtzioa erabiliko.

Kasu honetan A egoitzaren SSL-inspection profil bera erabiliko da, beraz, ez da berriro azalduko.

7.3.3 C egoitzaren segurtasun mekanismoak

C egoitzan B egoitzan bezala trafiko identifikatzea errazagoa da, zama kantitatea dela eta. Kasu honetan soilik segurtasun arauak azalduko dira, profilak B egoitzako berdinak erabiliko baitira.

Segurtasun Arauak

C egoitzan beste egoitzen antzerako politika paketea eratuko da, behin C egoitzako firewalletik eskegita dauden sareen trafikoa identifikatuta edukita, segurtasun arauak sortu dira, hauen eredua 30. irudian erakusten da:

ID	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Bytes
Nuevos Accesos 195									
293	any	any	Red_10.0.35.0_24	NLB	always	ALL	ACCEPT		1.86 MB
291	any	any	Grupo_VPN PCs_Total	srv_R_SGCA_SHOCKS_VUX	always	HTTP HTTPS	ACCEPT		3.16 GB
281	any	any	dw1rsbdprep	dw1Rrsbddes_172.21.60.117	always	t10000-10010 t20501	ACCEPT		657.77 kB
280	any	any	Red_R_172.21.60.0_24	dw1rsbdprep	always	ALL	ACCEPT		6.35 MB
278	any	any	Red_R_172.21.70.0_24	Net_172.19.4.0	always	ALL	ACCEPT		0 B
273	any	any	Red_R_172.21.50.0_24 Red_R_172.21.60.0_24 Red_R_172.21.40.0_23	TC_DCN_SSAA_10.121.20.0_24	always	ALL	ACCEPT		0 B
289	any	any	Red_VDI_GFI_172.18.147.0	Grp_Cluster_Apache	always	ALL_ICMP HTTP HTTPS	ACCEPT		90.83 kB
270	any	any	PCs_Total	FQDN_rds rds1pro_VS_ADC_172.18.69.147	always	HTTPS	ACCEPT		0 B
269	any	any	PCs_Total	FQDN_Imap.corporativo mail2corpro_212.142.145.32 mail1corpro_212.142.145.31	always	IMAP	ACCEPT		0 B
268	any	any	PCs_Total	FQDN_smtpout.corporativo	always	SMTP	ACCEPT		0 B

30. Irudia: C egoitzaren segurtasun arauen eredua

Kasu honetan, B egoitzan bezala, kudeaketarako protokoloak ahalbidetuko dira C egoitzako sare korporatiboetan, zerbitzu gehienak mail zerbitzariak edo Web zerbitzariak baitira.

7.4 Automatizazio programaren diseinua

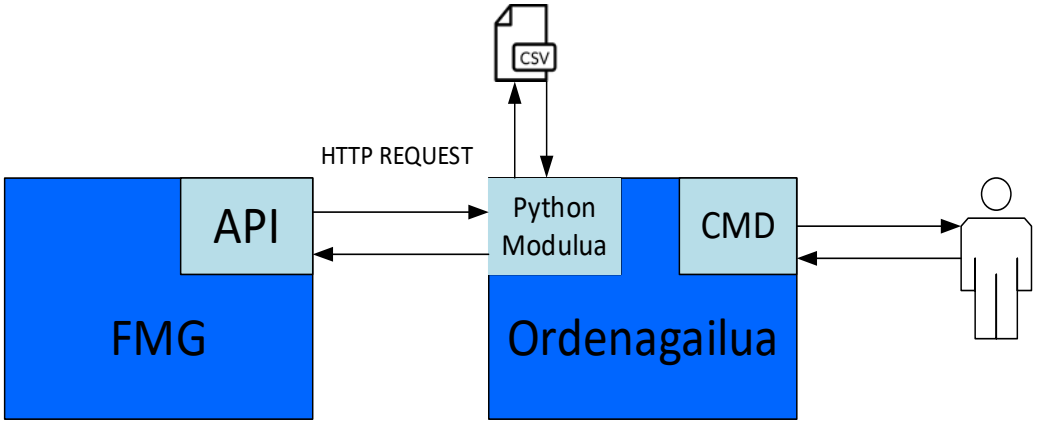
Proiektu honen zehar luzaro aipatu da automatizazio ebazpena, proiektu honen atalik erakargarriena baita. Automatizazio programa bat diseinatuko da, programa honen bidez, VLAN bat sortzerakoan, VLAN hori beharrezko sarbideak izan ditzan, segurtasun arau sorta bat sortuko da.

Hau lortzeko FortiManager makinak dituen APIak erabiliko dira, konfigurazioak era automatikoan egin daitezen.

Gainera, APIekin komunikatzeko Python programazio lengoaia erabiliko da alternatiben analisietan erabaki delako.

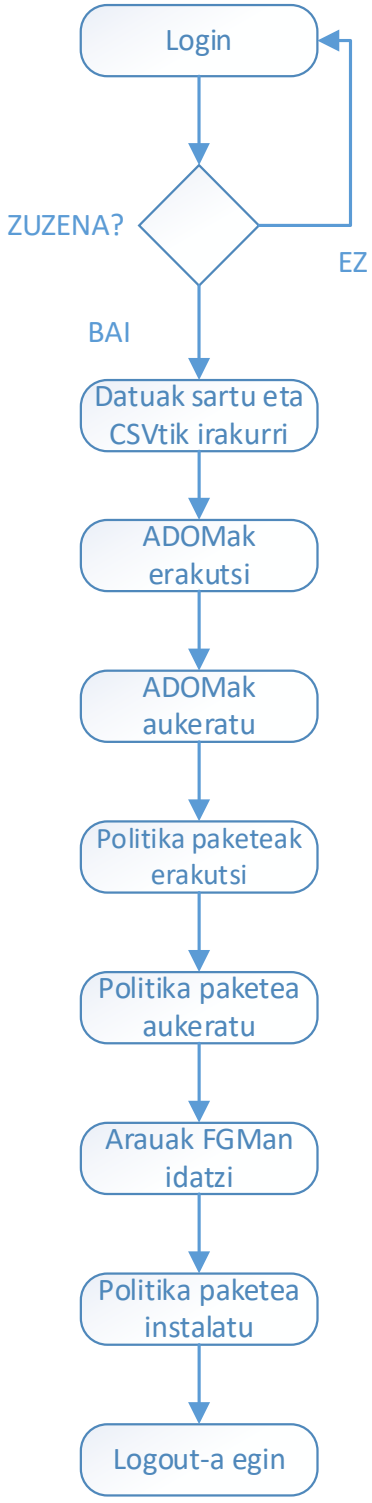
Lengoai hau lehenago azaldu denez, liburutegietan oinarritu da eta APIekin komunikatzeko request eta JSON liburutegiak erabiliko dira. JSON liburutegia datu blokeak kudeatzeko eta request liburutegia HTTP eskaerak egiteko.

Gainera, CSV (Comma-separated Values) fitxategiak kudeatzeko csv liburutegia erabiliko da. CSV honetatik arau sorten datuak irakurriko dira, eskuz sartu behar ez izateko. Komunikazioa hobeto ulertzeko goi mailako diseinua erakusten duen irudi bat egin da; hain zuzen ere, 31. Irudia:



31. Irudia: Programaren goi mailako diseinua

Modu berean, Programazio script honetan hainbat atal egongo dira, politika arau sorta sortzeko. Programaren atalak nola izango diren azaltzeko 32. Irudiko UML diagrama diseinatu da:



32. Irudia: Automatizazio programaren UML diagrama

UML diagramaren atalak laburki azalduko dira jarraian:

- **1. pausua: Login, pausu honetan FortiManagerrarekin loggeatuko da scripta, erabiltzaile eta pasahitza zuzena erabiliz. Login honetan, hurrengo konexioak autentifikatuak egon daitezen, token bat lortuko da.**
- **2. pausua: Datuak lortu, pausu honetan hainbat datu lortuko dira; adibidez, arauen parametroak CSV fitxategi batetik irakurriko dira, ondoren JSON formatuan FortiManagerrari bidali daitezen eta honek bere konfigurazioan erantsi dezan.**
- **3. pausua: ADOMak erakutsi, pausu honetan FortiManagerrak dituen ADOMak erakutsiko du, honetako bat aukeratzeko gaitasuna izan dadin.**
- **4. pausua: ADOMa aukeratu,konfiguratu nahi dugun ADOMa aukeratu beharko da lehen erakutsitako zerrendatik.**
- **5. pausua: Politika paketeak erakutsi, pausu honetan lehen aukeratutako ADOMaren barnean dauden politika paketeak erakutsiko dira.**
- **6. pausua: Politika paketea aukeratu, erakutsitako politika paketeen barneko bat aukeratuko da.**
- **7. pausua: Arauak FMGan idatzi, pausu honetan CSV fitxategitik irakurritako datu blokea firewallera bidaliko da POST HTTP mezuaren bidez, arau sorta hau FortiManagerrean konfiguratu dadin.**
- **8. pausua: Politika paketea instalatu, lehen aukeratutako politika paketea instalatuko da dagokion firewallean**
- **9. pausua: Logout-a egin, pausu honetan FMGtik irtengo gara sesio bukatu dadin.**

FortiManager APIari buruzko informazioa https://fndn.Fortinet.net webgunetik aterako da. Webgune horretan, HTTP eskaerak ze URLtara zuzendu beharko dira azalduko da. Gainera, mezuetan gehituko diren parametroak zeintzuk diren azalduko da.

Webgune hau ordaindu beharrezko webgunea da eta foro bat du zein zalantza posible guztietara momentuan erantzuten dute.

Halaber, hainbat dohainezko programazio foro erabiliko dira, zalantza posibleak ebazteko; adibidez, StackOverFlow foroa.

Scriptaren frogak egiteko FortiGate eta FortiManager makina birtualak erabiliko dira, lehen aipatutako VMWare zerbitzarian.

8. Metodologia

Behin ebazpenaren diseinua eta beharrezko konfigurazioak eginda, ebazpena produkzioan sartzeko metodologia azalduko da. Hori dela eta, migrazio plana azalduko da eta scriptaren funtzionamenduaren demoa.

8.1 Migrazio plana

Antzina egoitza honetan instalatuta zeuden firewallen bertsioa FGT-5.2.13 zen; ondorioz, firewall berrien bertsioarekin desfasatuak daude, hau da, FGT-6.0.4arekin. Kasu hauetan bi ebazpen ematen ditu Fortinetek:

- **Forticonverteren erabilera: Tresna hau dohainik erabili daiteke, konfigurazioa 5.2.x bertsiotik 5.4.4 FortiOS bertsiora aldatzeko balio du.**
- **Makina birtual lizentziatua instalatu 5.2.13 bertsioan, konfigurazioa bertsio horretan sartuz eta gero, beharrezko eguneraketak egin 6.0.4 bertsioan jartzeko, gero aztertuko den upgrade patha aztertuz.**

Forticonverter tresna aztertu ondoren, zifratze tekniken bateraezintasunaren ondorioz deuseztatu da. Hainbat konfigurazio ataletan erabiltzen baitira zifratze algoritmoak. Azken finean, pasahitza behar duen edozein konfigurazio zifratuta joango da, ulertezina bihur dadin konfigurazio gordina aztertzerakoan.

Horregatik, erabaki da bigarren aukera erabiltzea era honetan zifratze bateraezintasunak saihestuz. Metodo hau erabiliz, kontu handiarekin ibili beharko da, ezin da edozein bertsiotik beste batera salto egin, upgrade path bat errespetatuz egin behar da. Upgrade path hau Fortineten webgunean aztertu behar da, Fortineten kideentzako erabilgarri dago soilik, gure kasuan upgrade patha 5.2.13tik 6.0.4ra doa eta webgunea kontsultatuz 33. Irudiaren edukia lortzen dugu:

Recommended Upgrade Path

Following is the recommended FortiOS migration path for your product.

Version	Build Number
5.2.13	0762
5.4.9	1202
5.6.8	1672
6.0.4	0231

33. irudia: A egoitzako upgrade path-a

Beraz, prozesu laburtuta hurrengoa izango zen:

- **1. Pausua: Makina birtual bat instalatu VMWare zerbitzarian, makina hau FortiGate 5.2.12 bertsiokoa izango da.**
- **2. Pausua: Makina birtual hau lizentziatu behar da, horrela VDOM gehiago edukitzeko gaitasuna ematen du, bestela defektuz soilik VDOM bat eduki daiteke eta 8 gutxienez beharko ziren. Lizentzia ale komertzialak Fortineteri eskatzen dio eta Fortinetek 60 egunetarako lizentzia ematen du.**
- **3. Pausua: Makina birtual lizentziatu honetan produkzioan dauden bi firewallen konfigurazioa ezartzen da.**
- **4. Pausua: Makina birtual hau bertsioz bertsio igo behar da, akats posibleak aztertuz eta bere garrantzia kontuan edukiz.**
- **5. Pausua: Makina birtuala 6.0.4 bertsioan dagoenean, bere konfigurazioa FortiGate berrian itsats daiteke arazorik gabe horrela migrazioa bukatuz.**
- **6. Pausua: Azkenik, firewall berriak produkziora pasatu behar dira, lotura mailan blokeatuta zeudelako routing ekipamenduan, VDOM-ka ahalbidetuko dira egun ezberdinetan.**

Prozesua gainetik azalduta pausuak era zehatzago eta luzeago baten azalduko dira.

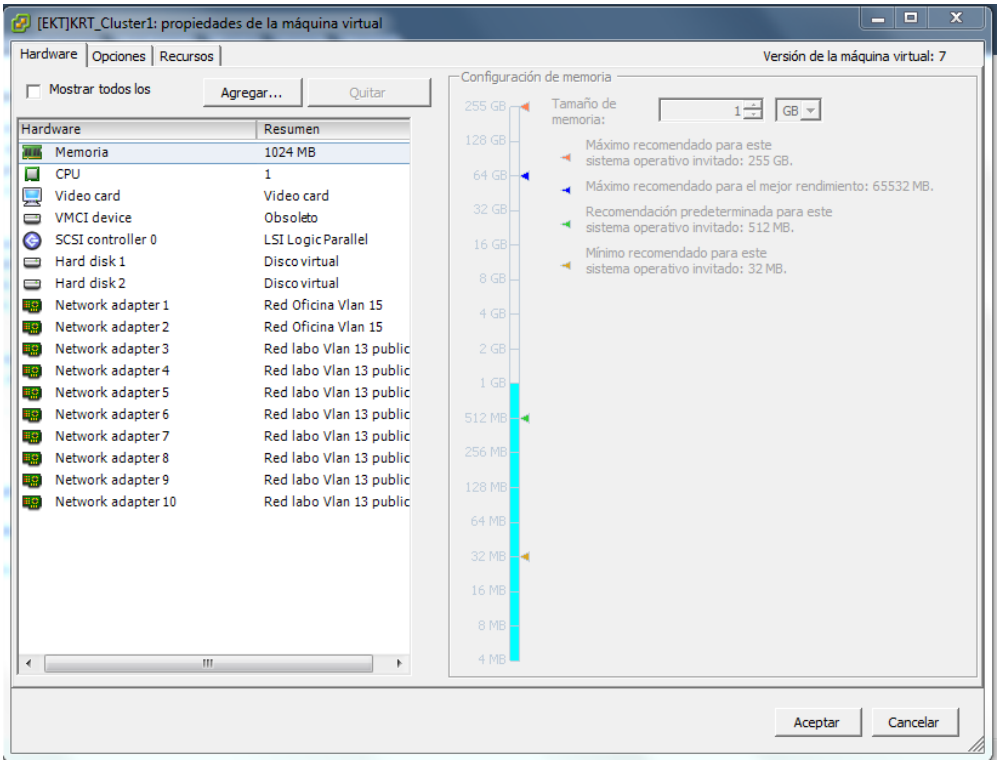
1. Pausua: Makinaren instalazioa

Proiektu honen kasuan, VMWare zerbitzari bat erabiliko da, laborategi ingurumenean dagoena delako. Horren ondorioz, Fortinet support webgunetik deskargatuko da beharrezko Softwarea, kasu honetan irudia FGT_VM64-v5-build0762-FORTINET.out.ovf.zip da.

Ondoren Software hau VMWare zerbitzarian inplementatuko da. 34. irudian ikusi ahal den bezala:

34. Irudia: Makina birtualaren irudiren inplementazioa

VMWare zerbitzari birtualean inplementatu ondoren, makina birtualari IP helbide bat esleitu beharko zaio, enpresaren saretik eskuragarria izateko, gainera HTTPS trafikoa erabiliko den interfazean ahalbidetu beharko da. Horrela, firewalla webgunetik atzitu ahalko da, bere konfigurazioa erraztuz. IP helbide hori baliozkoa izan dadin, makina birtualaren sare konfigurazioa garrantzitsua da; hau da, VMWare mailan sare konfigurazioa, sare interfaze birtualak VLAN egokiarekin lotu behar dira, kanpoko sareei sarbidea izan dezan. 35. irudian bezala:



35. Irudia: Makina birtualaren espezifikazioak

Hau egiteko erarik onena interfaze hori IP helbidea era automatikoan lortzeko konfiguratzea da; hau da, IP helbidea DHCP (Dynamic Host Configuration Protocol) zerbitzari bati eskatuz. Era

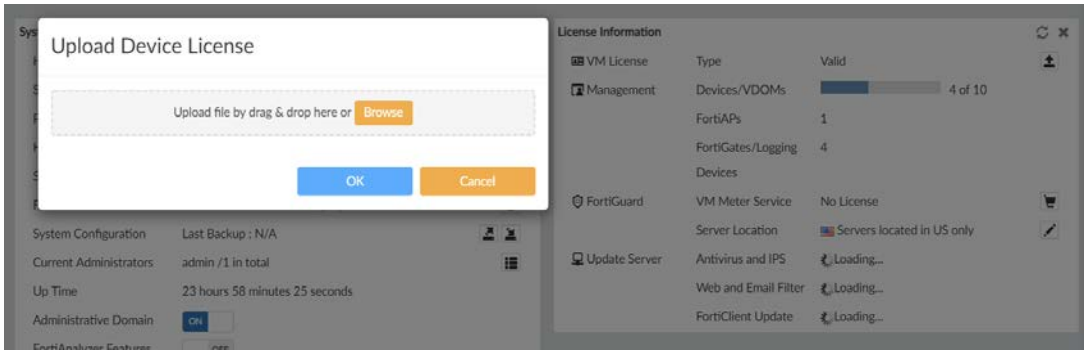
honetan, pausu bi aurrezten dira, bestela DNS (Domain Name System) zerbitzaria eskuz konfiguratu beharko zen. Horrela lizentziaren balizkotasuna frogatu daiteke 2. Pausuan adierazten den bezala.

Halaber, bideratze taulan sarrera bat gehitzea aurrezten da, DHCPrekin era automatikoan hartzen du defektuzko bidea. Defektuzko bide hau gabe Internetera sarbidea izatea ezinezkoa da, honek internetera joateko lehenengo bideragailura joateko bidea adierazten baitu.

2. Pausua: Makina lizentziatzea

Behin makina birtualaren hasierako prestaketa eginda, proiektuaren espezifikazioetara hurbiltzeko lizentziatu beharko da. Fortineteko teknikariei lizentzia eskatu beharko da, hauek gako bat ematen dute "Activation Key" deritzena.

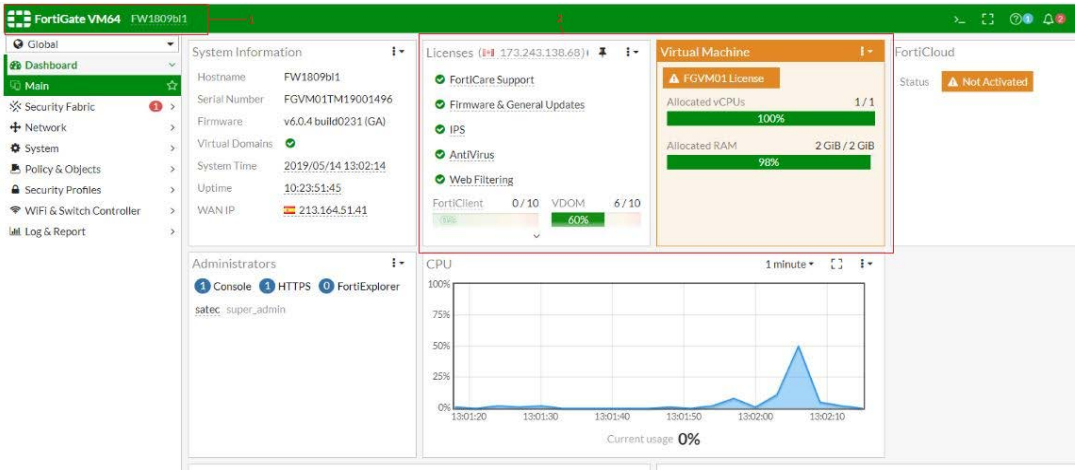
Behin gakoa lortuta, makina birtuala lizentziatu ahal da, lizentzia hemen sartu beharko da:



36. Irudia: Lizentzia sartzeko tokia

Makinaren lizentzia gakoa sartzen denean, makina berpiztuko da eta FortiGuard zerbitzariekin komunikatzen saiatuko da, honen balizkotasuna frogatzeko. FortiGuard zerbitzariak Fortinet firewallen lizentzien arduraduna den zerbitzaria da.

FortiGuardekin komunikatzen bada eta gakoa balizkoa bada, orduan prest egongo da makina birtuala proiektuan erabiltzeko. 37. Irudiko edukia izango zen FortiGate makina birtual lizentziatuaren dashboard-a:



37. irudia: Makina birtual lizentziaduna

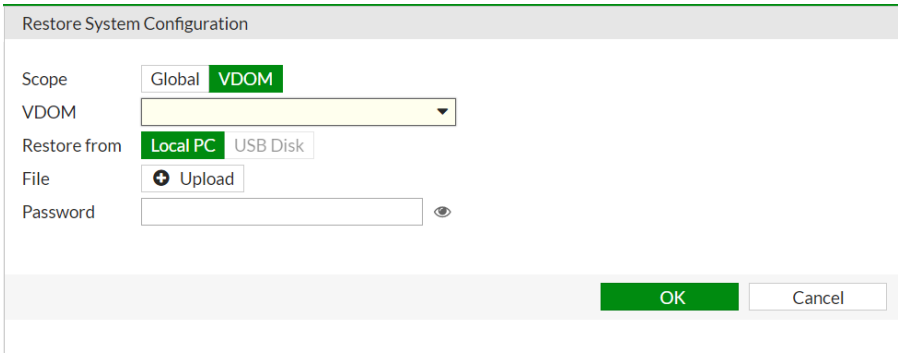
Irudian ikusten den 1. laukian, makina birtual bat dela ikusten da izena FortiGate VM64 baita. 2. laukian, lizentziaren datuak ikusten dira; hau da, Fortiguard zerbitzariaren IP helbidea, aktibatuta dituen segurtasun mekanismoak, VDOM kantitate maximoa...

Lizentziaren egoera zuzena dela ikusita hurrengo pausu hau bukatutzat emango da.

3. Pausua: Produkziozko konfigurazioa makina birtualera

Pausu honetan, produkzioan dauden bi firewallen VDOM-ak hartuko dira eta makina birtualean kargatuko dira. Beti hartu behar da bi firewalletako bat erreferentzia gisa, konfigurazio globalaren interfazeen konfigurazioa direla eta. Kasu honetan, lehenengo firewall clusterra erreferentzia gisa hartuko da; beraz, etorkizuneko firewalla honen konfigurazio globala izango du.

Bigarren Clusterretik VDOM-ak banaka kargatuko dira, konfigurazio globala ez delako aldatu behar. 46. irudian ikusten den aukera zehaztu behar da:



38. Irudia: VDOM baten konfigurazioaren karga

Kontuan eduki behar da konfigurazioa kargatzerakoan erroreak eman daitezkeela. Hau konprobatuko da *diagnose debug config-log-error read* komandoarekin, komando honek irteerarik ateratzen badu, ateratako irteera aztertuko beharko litzateke akatsak ebazteko asmoarekin. Behin arazo guztiak ebatsita, pausua hau bukatutzat emango da.

4. Pausua: Bertsioen eguneratzea

Aurreko pausuan makina birtualaren bertsioa 5.2.13an utzi da eta lortu nahi den bertsioa 6.0.4 bertsioa da; ondorioz, eguneratze bat behar da. Lehen aipatu den upgrade path-a errespetatuz, eguneratze prozesua hurrengo segida jarraituko du: 5.2.12->5.4.9->5.6.8->6.0.4. Behin eta berriz, makina birtualaren Software irudi berria igoz, behin igota, hau eguneratuko da.

Eguneraketa prozesu honetan akatsik balego, diagnose debug config-error-log irteerarik emango balu, aurreko bertsioko backup fitxategian ikusi beharko zen akastuna izan dena eta bertsio bakoitzaren oharrak (Release notes) aztertuz honen garrantzia ikusiko da, ebazpen on bat bilatuz.

5. Pausua: Aurreko firewallen konfigurazioa firewall berrietan kargatu

Makina birtualean dugun konfigurazioa firewall berrietan kargatzeko prest dagoenez, honen backup-a egin beharko da eta hau lortu ondoren, konfigurazio fitxategian aldaketa txiki bat eginez firewall berrietan kargatzeko moduan egongo da.

Aldaketa hau konfigurazio fitxategiaren lehenengo lerroan egin behar da. FGVM aldatu behar da FG2K5Egaitik, firewall fisikoa eta 2500E modeloa dela adierazten duen lerroa baita.

```
1  #config-version=FG2K5E-6.0.4-FW-build0231-190107:opmode=0:vdom=1:user=satec
2  #conf_file_ver=357122235778248
3  #buildno=0231
4  #global_vdom=1
5
```

39. irudia: Konfigurazio fitxategiaren aldaketa

Aldaketa labur hau behin eginda, konfigurazio fitxategia migratzeko prest dago. Desiratutako konfigurazioa firewall berrietan edukita, berriro aurreko ataletan bezala *diagnose debug config-log-error* komandoa erabili beharko da. Hainbat akats egongo dira makina birtuala eta firewall fisikoaren arteko ezberdintasunen ondorioz; hala ere, ez dira akats garrantzitsuak izango, baina banan-banan aztertuko dira eduki ahal duten inpaktua aztertuz.

6. Pausua: Firewall berriak produkziora pasatzea

Behin konfigurazioa kargatuta edukita firewall berriak sare korporatiboan instalatzeko prest daude. Migrazio honek produkzioan ordu erdiko etenaldia suposatuko du; ondorioz, instalazio hau bezeroekin adostu beharko da. Haien agendaren arabera eta produkzioan mozketa txikiena eduki dezaten.

Lehen aipatu den bezala; nahiz eta, firewalla instalatuta utzi, VDOMak ez dira ahalbidetuak egongo lotura mailan beste ertzean blokeatuta egongo baitira, kudeaketa interfazea soilik ahalbidetuta egonda, konfiguratzeko gaitasuna izanik.

VDOMak produkziora pasatuko dira banaka, hasieran sarean inpaktu gutxien dutenak migratuz eta ondoren, inpaktu gehien dutenak. Arazorik egotekotan hasieran, inpaktu gutxien duten VDOMetan izango lirateke eta inpaktu handiena duten VDOMentzako akats hauek aurreikusiko lirateke.

8.2 Balidazio funtzionala

Proiektuaren atal batzuen zuzentasuna frogatzeko bi froga nagusi egingo dira: HA probak eta scriptaren portaeraren demo bat.

8.2.1 HA probak

Proiektuaren espezifikazioetara hurbilduz, bi HA interfaze egongo dira sinkronizazio komunikazioa egiteko. Gainera, firewall clusterraren trunk interfazea heartbeat interfazea izango da. Hau da, interfaze monitorizatua izango da, hau jauzten bada clusterraren hierarkian inpaktu zuzena izango du aurrerago azalduko denez.

HAren funtzionamendu egokia konprobatzeko hainbat proba planteatu dira, kasuistika guztiak kontuan edukiz:

- **Failover Primary: Master kidea jauzten da.**
- **Comeup Primary: Masterra errekuperatzen da minutu bat baino lehenago.**
- **Comeup Primary lately: Masterra errekuperatzen bada minutu bat pasatu ondoren.**
- **Failover Secondary: Standby kidea jauzten bada.**
- **Comeup Secondary: Standby kidea errekuperatzen bada..**

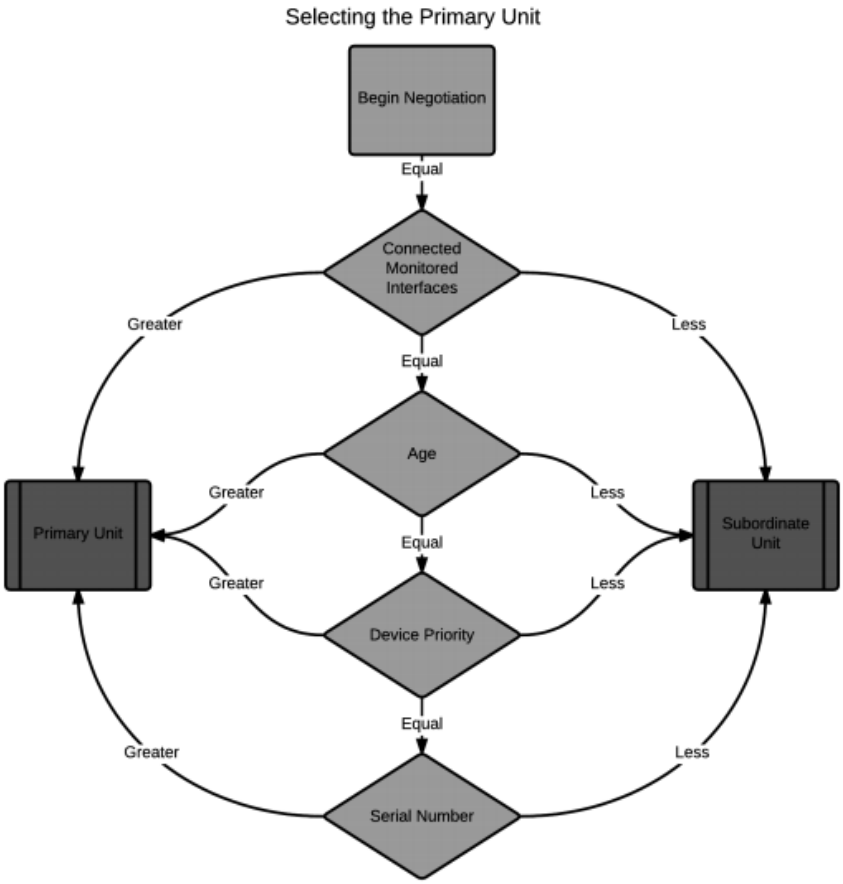
Kasuistika hauek guztiak taula batean irudikatzea egokia dela identifikatu da, kasu bakoitzean sarean edo konektibitatean duen inpaktua adieraziz. 4. Taulan adierazten da aztertu den portaera:

Egoera posibleak	HA interfaze biak jauzi dira	Interfaze monitorizatua jauzita	Interfaze ez monitorizatua jauzita
Failover Primary	Primary kidea master bezala geratzen da	Secondary kidea master bezala jartzen da zerbitzu mozketarik gabe.	Primary unitatea master bezala jarraitzen du eta zerbitzu mozketa jasotzen da.
Comeup Primary Tw< *ha-uptime-diff-margin*)	Ez dago aldaketarik	Primary unitatea master gisa birjartzen da, pakete batzuen galerarekin.	Zerbitzura bueltatzen da galdutako interfazea
Comeup Primary Tw> *ha-uptime-diff-margin*)	Ez dago aldaketarik	Unitate bigarrena master bezala jarraitzen du, primary unitatea berriro master gisa jartzeko eskuz egin beharko da.	Zerbitzura bueltatzen da galdutako interfazea.
Failover Secondary	Primary kidea master bezala geratzen da	Primary kidea masterra bihurtzen da	Secondary kidea master bezala geratzen da. Zerbitzuan mozketa edukiz.
Comeup Secondary	Primary kidea master bezala geratzen da	Primary kidea master bezala geratzen da.	Zerbitzura bueltatzen da galdutako interfazea

4. Taula: HA proben taula

HA cluster master unitatearen interfaze biak jausten badira, standby unitateak ahalbidetuak edukita, Masterra Master gisa mantentzen da. Standby unitatearenak jauzten badira, Standby kidea clusterretik aterako da eta HA komunikazioa etengo da.

Kasu bakoitzean gertatzen dena, master kidearen aukeraketa prozesuaren errepikapena da. Prozesu hau hurrengo irudian agertzen diren irizpideak kontuan edukiz egiten da. Aukeraketa irizpideen artean, interfaze monitorizatu aktiboen kantitatea elementu nagusiena da. Bigarrena, kideen denbora clusterraren barruan sistemak definitua duen parametro baten arabera, parametro hori definitzen du zein denboratik aurrera biak denbora berdina daramate clusterrean. Hirugarrena, kideen lehentasuna cluster barruan da. Azkenik, bi firewallen serie zenbakien konparaketa da, elementu hau ezin daitekeelako berdintsua izan.



40. Irudia: Nola erabaki zein izango den Clusterraren masterra [10]

Orden hau moldatu daiteke HA override parametroa ahalbidetuz, honek lehentasunari garrantzi handiago ematen dio clusterrean daramaten denborari baino. Hala ere, override parametroa ezgaituta uztea gomendatua dago.

Age parametroa komentatzea merezi du. Parametro hau garrantzi handia izango du lehentasun handiagoa duen kidea "comeup" egiten badu. Bi kasu daude lehentasun handiena duen kidea comeup bat egin behar izateko:

- **Cluster unitatea amatatzen bada eta berriro pizten bada bere Age parametroa 0ra hasieratuko da.**
- **Cluster unitateari interfaze bat jauzten bazaio, Age parametroa 0ra hasieratzen da.**

Age parametroa nola funtzionatzen duen aztertzeko sistemaren ha-uptime-diff-margin garrantzi handia du. Parametro honek definitzen du

zenbat denbora izango duen master unitatea clusterrera bueltatzeko eta master bezala berriro jartzeko.

Denbora hau garaitzen bada, secondary kidea master bezala ezarriko da, nahiz eta, lehentasun baxuagoa izan. Berriro primary kidea master gisa jarri nahi badugu, eskuz egin beharko dugu secondary kidearen failoverra eginez.

Sistemaren parametroa aldatzeko hurrengo komandoak erabili beharko lirateke:

Config system ha

Set ha-uptime-diff-margin [time]

End

Primary unitatea konektibitatea galtzen badu interfaze monitorizatu batean, bere denbora kontagailua berrerasiko da. Comeup-a egiterakoan, master kidea nor izango den negoziatuko da, clusterrean daramaten denboraren arabera. Horren ondorioz, interesgarria da bi egoera definitzea:

- **Kide bakoitza denbora bera darama clusterraren barruan; hau da, secondary kidea ez darama ha-uptime-diff-margin baino denbora gehiago.**
  Kasu horretan, hurrengo maila hierarkikoa kontuan edukiko da; hau da lehentasuna, ondorioz, primary kidea masterra bihurtuko da.
- **Secondary unitatea primary-a baino denbora gehiago darama; hau da, ha-uptime-diff-margin baino denbora gehiago darama secondary unitatea. Secondary kidea master bezala jarraitzen du, berreskurapen denbora garaitu delako.**

Sarearen beharrizanak aurreikusiz, 60 segundoko balioa ezarri zaio ha-uptime-diff-margin parametroari.

8.2.2 Scriptaren funtzionamenduaren demoa

Atal honetan scriptaren funtzionamendua erakusten duen demo bat aurkeztuko da. Demo honetan scripta nola exekutatuko den eta lortuko duen emaitza ikusiko da.

Hasiera batean, segurtasun arauen datuak batzen dituen CSV fitxategi bat eduki beharko da, horrela, scriptak datuak eskuratu ahalko ditu. CSV fitxategia 41. irudian agertzen duena izan beharko du:

name	dstintf	srcintf	srcaddr	logtraffic	logtraffic-start	service	schedule	dstaddr	Package
ANTIVIRUS1	WAN	$vlan_interface	all	2	0	ALL	ALWAYS	Grupo GEO KASPERSKY,Grupo KASPERSKY	VDOM1-FW1_root
ANTIVIRUS2	WAN	$vlan_interface	all	2	0	HTTP,HTTPS	ALWAYS	Panda Nube,Webs Panda	VDOM1-FW1_root
ANTIVIRUS3	OFIMATICA	$vlan_interface	all	2	0	ALL	ALWAYS	Servidor Nextelv_Kaspersky	VDOM1-FW1_root
Administradores	$vlan_interface	OFIMATICA	Administradores Red	2	0	ALL	ALWAYS	all	VDOM1-FW1_root
Monitorizacion	$vlan_interface	OFIMATICA	Servidores de monitorizacion	2	0	ALL_ICMP,SNMP	ALWAYS	all	VDOM1-FW1_root
Actualizaciones1	OFIMATICA	$vlan_interface	all	2	0	ALL	ALWAYS	Servidor WSUS2016V	VDOM1-FW1_root
Actualizaciones2	WAN	$vlan_interface	all	2	0	Servicios WSUS2012v	ALWAYS	Servidor VA WSUS2016VAV,Servidor WSUS2016GALV	VDOM1-FW1_root
Actualizaciones3	OFIMATICA	WAN	all	2	0	Servicios WSUS2012v	ALWAYS	Servidor WSUS2016GALV	VDOM2-FW1_root
Actualizaciones4	OFIMATICA	WAN	all	2	0	Servicios WSUS2012v	ALWAYS	Servidor VA WSUS2016VAV	VDOM2-FW1_root
IMPRESORAS1	IMPRESORAS	$vlan_interface	all	2	0	ALL	ALWAYS	Sercidor Impresion	VDOM3-FW1_root
IMPRESORAS2	WAN	$vlan_interface	all	2	0	UDP 137,ALL_ICMP	ALWAYS	Servidor Impresion ,Servidor impresion	VDOM3-FW1_root
IMPRESORAS3	IMPRESORAS	WAN	all	2	0	UDP 137,ALL_ICMP	ALWAYS	Servidor Impresion	VDOM4-FW1_root
IMPRESORAS4	IMPRESORAS	WAN	all	2	0	UDP 137,ALL_ICMP	ALWAYS	Servidor Impresion	VDOM5-FW1_root

41. Irudia: CSV fitxategiaren formatua

Fitxategia hainbat eremu izango ditu, eremu edo zutabe hauek arauak sortzeko beharrezko parametroak izango dira. Arau guztiak izena, iturriko eta helburuko interfazeak, iturriko eta helburuko sareak, log-en konfigurazioak, zerbitzuak, instalatuko den paketean eta *schedule* izan beharko dituzte.

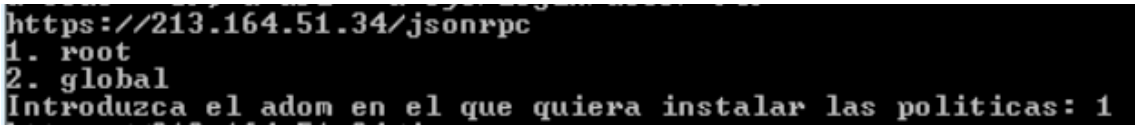
Fitxategi hau eginda edukita, programa exekutatzera abiarazi daiteke. Exekutatzeko laguntza behar bada 42. irudian agertzen den bezala egin daiteke:

```
C:\Users\unai.abrisqueta\Desktop\Satec\Farmacias>python -tt [CABB]Fortimanager_F
inal.py -h
********************************************************************************
********************
Uso: Fortimanager.py -i <hostname ip[:port]> -v <vdom> -u <username> -p <passwor
d> -f <archivo.csv>

  Los datos hacen referencia al  FortiManager

  En caso de no especificar hostname, username y/o password se solicitaran

  -i: hostname o IP del FortiManager, puerto por defecto: 443.

  -a: adom a utilizar, por defecto adom=root

  -p: dejando la opcion en blanco se solicitara el password sin mostrarse en pan
talla

  -f: dejando la opcion en blanco se solicitara el nombre de fichero
      El formato de fichero tiene que ser: User,Pass,Resource,DstInt
      Las columnas han de tener encabezado con los nombres mencionados
********************************************************************************
********************
Ejemplos:
  python Fortimanager.py
  python Fortimanager.py -i 192.168.1.99 -a myAdom -u admin -f politics.csv
  python Fortimanager.py -i 192.168.1.99 -u admin -p password
  python Fortimanager.py -i 192.168.1.99:8443 -u admin -a myAdom
********************************************************************************
********************

C:\Users\unai.abrisqueta\Desktop\Satec\Farmacias>
```

42. Irudia: Scripta nola erabili jakiteko laguntza

Hasieran, erabiltzaile eta pasahitza sartu beharko da; honi esker, FortiManagerraren APIarekin trukatuko diren mezuak autentifikatuak izango dira. FortiManagerrak token bat esleituko du lehen erantzunean eta hurrengo mezuetan token hori gehitu beharko da komunikazioa posiblea izan dadin.

Ondoren, ADOM ezberdinak aurkeztuko dira eta haietako bat aukeratu beharko da, 43. Irudian erakusten den moduan:



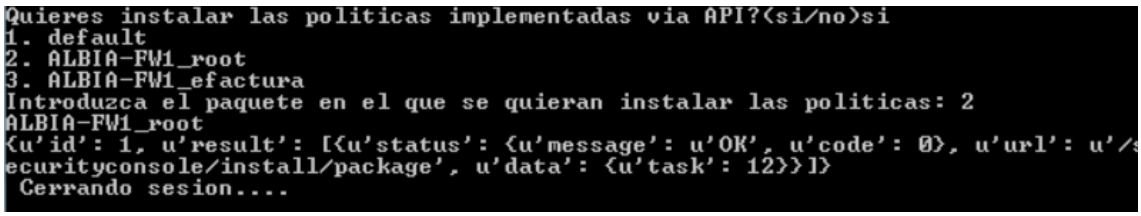
43. Irudia: ADOMak erakusten dituen scriptaren zatia

Behin ADOM egokia aukeratuta, segurtasun arauak zein politika paketean instalatu nahi diren jakin beharko da, scriptak datu hau CSVtik irakurriko du, arau bakoitza politika pakete ezberdinetan txertatu beharko denez, fitxategi batetik irakurtzea eraginkorragoa da.

Ondoren, CSVn zeunden segurtasun arauak politika pakete horretan instalatuko dira momentuan, 44. Irudian ikusi ahal den moduan:

44. Irudia: APIak erabiliz nstalatutako segurtasun arauak

Azkenik, segurtasun arauak FortiGatetan instalatu beharko dira, indarrean jar daitezen. Honekin, segurtasun arauak indarrean jarriko dira. Hau egiteko gaitasuna ere izango da scriptarekin, 45. Irudian ikusi ahal den bezala:



45. Irudia: Politika paketea Fortigatean instalatu

Azken pausu horrekin exekutazioa bukatutzat eman daiteke.

9. Planifikazioa

Proiektu honetan zehar hainbat ataza bete dira, ataza hauek lan paketeetan taldekatzen dira, atazaren kokapena proiektuaren faseetan eta atazen funtzionaltasunak kontuan edukiz. Beraz, atal honetan lan taldea, lan paketeen deskribapena eta mugarriak aztertuko dira; hala nola, proiektuaren hasiera eta bukaera data definituko dira.

9.1 Lan taldea

Proiektu hau martxan jartzeko hainbat langile beharko dira, 3 langile zehatz-mehatz beharko dira. Langile bakoitzak bere eginkizunak izango dute, funtzio ezberdinak izanik eta ataza ezberdinetan parte hartuz.

Jarraian lan taldea definituko da:

- **Junior ingeniaria: Langile honek, konfigurazioen ardura hartuko du; hau da, diseinuan erabaki diren ebazpenen konfigurazioa egingo du.**
- **Senior ingeniaria: Langile honek, diseinuaren zama handiena hartuko du; gainera, junior ingeniariari lagunduko dio zalantzetan.**
- **Proiektu burua: Langile honek, kudeaketa lanetara zuzenduta egongo da, hala ere, diseinuan parte hartuko du hein txiki batean.**

9.2 Lan paketeak

Proiektua taldekatuko da atazetan eta hauek era berean lan paketeetan erlazionatuko dira. Beraz, atal honetan lan paketeak azalduko dira.

LP1: Proiektuaren ezaguera eta formakuntza fasea

A1.1 Automatizazioan eta APIen inguruko formakuntza

- **Iraupena: 10 egun**
- **Deskripzioa: Junior ingeniaria automatizazio eta APIen inguruko ikasketak egingo ditu; halaber, hauek Fortinet fabrikatzailearekin nola lan egiten dute ulertu beharko du.**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta bulego materiala.**

A1.2 Fortinet fabrikatzailea ezagutu

- **Iraupena: 10 egun**
- **Deskripzioa: Ataza honetan, junior ingeniaria Fortinet fabrikatzailearen berezitasunak eta konfigurazio komandoak ikasi beharko ditu. Horretarako fabrikatzaileak hainbat ikastaro labur ditu.**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta bulegoko materiala.**

LP2: Proiektua egiteko aukeren analisia

A2.1 Fabrikatzaileen azterlana

- **Iraupena:5 egun**
- **Deskripzioa: Fabrikatzaile ezberdinen azterlana egingo da proiektura era onenean moldatzen den firewalla aurkitzea posiblea izan dadin.**
- **Giza baliabideak: Senior ingeniaria eta junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A2.2 Automatizazioari buruzko aukerak aurkitu

- **Iraupena: 5 egun**
- **Deskripzioa: Teknologia ezberdinak aztertu ondoren, aukera ezberdinak baloratuko dira, aukera onena erabiltzea posiblea izan dadin.**
- **Giza baliabideak. Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A2.3 Topologia ezberdinen aukerak aztertu

- **Iraupena:egun 1**
- **Deskripzioa. Topologia ezberdinak aztertu onena aukeratzeko gai izateko, topologia guztiak aztertuz eta bakoitzaren portaera aztertuz eta konparatuz.**
- **Giza baliabideak: Senior ingeniaria eta junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta 2 Fortinet 2500E.**

LP3: Ebazpenaren diseinua: arkitektura, segurtasun politika eta automatizazioa

A3.1 Sare arkitekturaren definizioa

- **Iraupena: 5 egun**
- **Deskripzioa: Firewallak eratuko duten arkitektura diseinatuko da.**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta Visio programa**

A3.2 Segurtasun mekanismoen diseinua

- **Iraupena: 20 egun**
- **Deskripzioa: Sareak beharko dituen segurtasun mekanismoen diseinua egingo da.**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A3.3 Automatizazio programaren diseinua

- **Iraupena: 5 egun**
- **Deskripzioa: automatizazio programaren goi mailako diseinua egingo da.**
- **Giza baliabideak: junior ingeniariak**
- **Baliabide teknikoak: Ordenagailua, VMWare zerbitzaria birtuala eta FortiGate makina birtuala.**

LP4. Inplementazioa eta kodifikazioa

A4.1 A egoitzaren Segurtasun ekipamenduen konfigurazioak

- **Iraupena: 20 egun**
- **Deskripzioa: A egoitzaren segurtasun ekipamenduak diseinua atalean ezarri den moduan konfiguratuko dira.**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua, 2 FortiGate 2500E, FortiManager birtuala eta ekipamenduaren lizentzia.**

A4.2 B egoitzaren segurtasun ekipamenduen konfigurazioa

- **Iraupena. 15 egun**
- **Deskripzioa: B egoitzaren segurtasun ekipamenduak diseinua atalean ezarri den moduan konfiguratuko dira.**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua, 2 FortiGate 1500D eta lizentziak**

A4.3 C egoitzaren segurtasun ekipamenduaren konfigurazioa

- **Iraupena. 15 egun**
- **Deskripzioa: C egoitzaren segurtasun ekipamenduak diseinua atalean ezarri den moduan konfiguratuko dira.**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua, 2 FortiGate 1500D eta lizentziak**

A4.4 Automatizazio programaren kodifikazioa

- **Iraupena:10 egun**
- **Deskripzioa: Automatizazio programaren garapena eta beharrezko probak ingurumen errealean funtzionatu dezan.**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A4.5 A egoitzaren ekipamenduaren instalazioa

- **Iraupena: egun 1**
- **Deskripzioa: Konfiguratutako ekipamenduaren instalazioa**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta instalazio tresnak**

A4.6 B egoitzaren ekipamenduaren instalazioa

- **Iraupena: egun 1**
- **Deskripzioa: Konfiguratutako ekipamenduaren instalazioa**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta instalazio tresnak**

A4.7 C egoitzaren ekipamenduaren instalazioa

- **Iraupena: egun 1**
- **Deskripzioa: Konfiguratutako ekipamenduaren instalazioa**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua eta instalazio tresnak**

LP5: Frogak eta ekipamendua produkzioan jarri

A5.1 Segurtasun ekipamenduen konektibitatea konprobatu

- **Iraupena: egun 1**
- **Deskripzioa: Egoitza ezberdinetan instalatutako ekipamenduen konektibitatea konprobatu.**
- **Giza baliabideak: Junior ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A5.2 A egoitzaren ekipamendua produkziora igaro

- **Iraupena: egun 1**
- **Deskripzioa: A egoitzaren ekipamendua produkziora igaro**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A5.3 B egoitzaren ekipamendua produkziora igaro

- **Iraupena: egun 1**
- **Deskripzioa: B egoitzaren ekipamendua produkziora igaro**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A5.4 C egoitzaren ekipamendua produkziora igaro

- **Iraupena: egun 1**
- **Deskripzioa: C egoitzaren ekipamendua produkziora igaro**
- **Giza baliabideak: Junior Ingeniaria**
- **Baliabide teknikoak: Ordenagailua**

A5.5 Automatizazio programa produkzio ekipamenduan frogatu

- **Iraupena: egun 1**
- **Deskripzioa: Kodifikatutako programaren erabilpena produkzioan dauden ekipamenduen aurka.**
- **Giza baliabideak:Junior ingeniaria**
- **Baliabide teknikoak: ordenagailua**

LP6: Proiektuaren kudeaketa

A6.1 Proiektuaren jarraipena

- **Iraupena: Proiektuaren iraupena**
- **Deskripzioa: Proiektuaren zehar, astelehen guztietan ordu bateko batzarra egingo da.**
- **Giza baliabideak: Proiektu burua, junior ingeniaria eta senior ingeniaria.**
- **Baliabide teknikoak: Trello eta 3 ordenagailu**

A6.2 Proiektuaren memoria idaztea

- **Iraupena: 20 egun**
- **Deskripzioa: Proiektua bukatzerakoan proiektuaren metodologia, diseinua, konfigurazioak eta ondorioak batzen dituen dokumentua entregatuko da.**
- **Giza baliabideak: Junior ingeniaria, Senior ingeniaria eta proiektu burua**

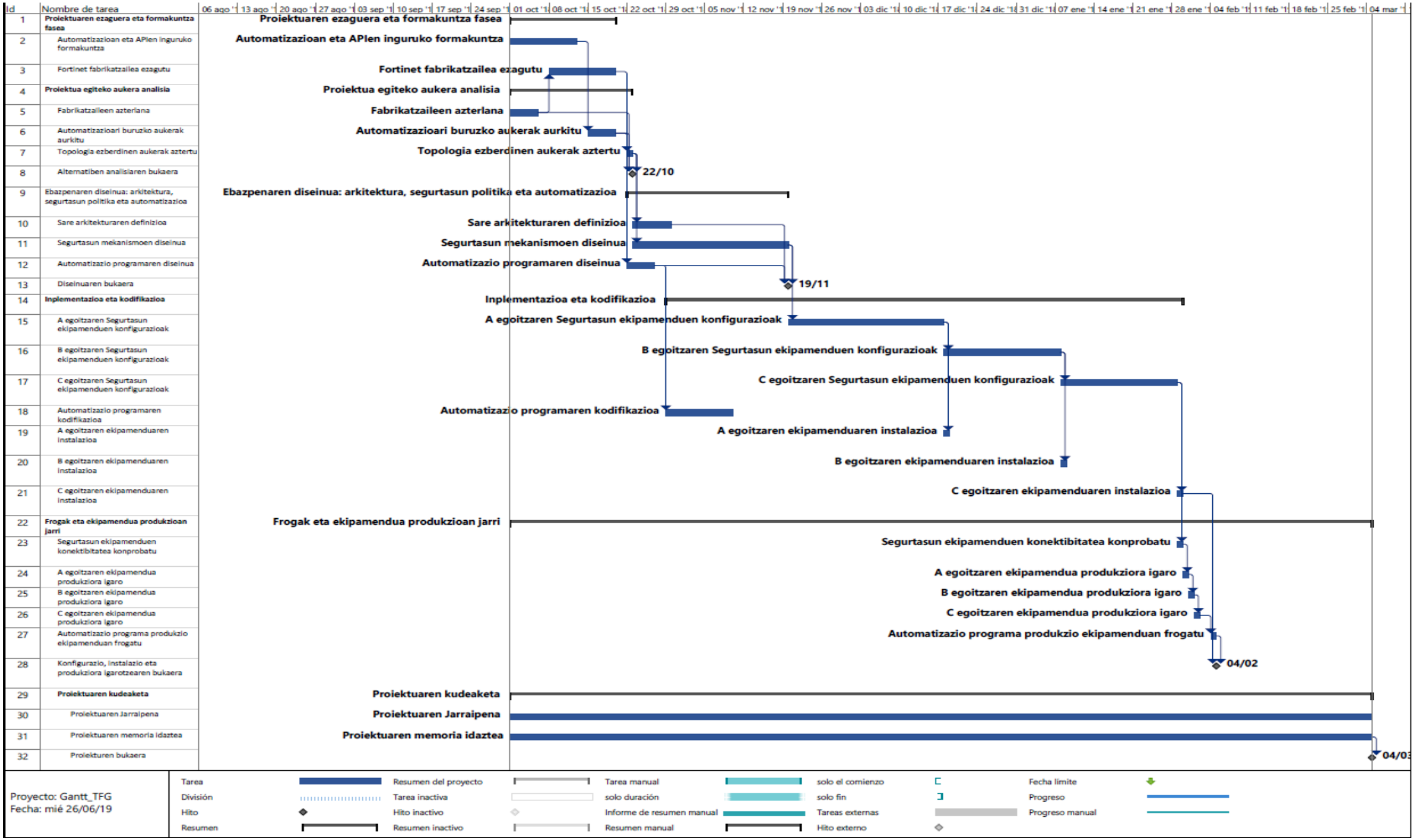
9.3 Proiektuaren mugarriak eta entregagarriak

Proiektuaren kontrol zehatza eramateko, hainbat entregagarri definituko dira eta hauek entregatzeko data mugak. Horrela, proiektuaren kudeaketa jarraitua eramango da eta ez da azken helburua ahaztuko. Proiektua 2018ko urriaren 1n hasiko da eta 2019ko martxoaren 4a baino lehenago bukatu beharko da, gainera beste mugarri batzuk egongo dira proiektuaren zehar. 5. taulan ikus daiteke mugarri eta entregagarrien arteko lotura:

Mugarria	Entregagarria	Data
Alternatiben analisien bukaera	Alternatiben analisia	22/10/2018
Diseinuaren bukaera	Diseinu dokumentuaren entrega	19/11/2018
Konfigurazio, instalazio eta produkziora igarotzearen bukaera	Migrazioaren txostena	04/02/2019
Proiektuaren bukaera	Proiektuaren memoria	04/03/2019

5. Taula: Proiektuaren mugarrien taula

9.4 Gantt diagrama



46. irudia: Gantt diagrama

10. Aurrekontua

Proiektuaren atal honetan alderdi ekonomikoa azalduko da, kontuan edukiko dira barne orduak, amortizazio eta gastuen kostuak. Hurrengo tauletan aurrekontua deskribatuko da:

Barne Orduak			
Langilea	Kostua(€/h)	Orduak(h)	Kostua(€)
Junior Ingeniaria	20 €/h	272 h	5.440,00 €
Senior Ingeniaria	35 €/h	80 h	2.800,00 €
Proiektu burua	45 €/h	63 h	2.835,00 €
Guztira			11.075,00 €

6. Taula: Barne orduen kostuak

Amortizazioak					
Materiala	Kantitatea	Kostu totala(unitateko)	Bizitza osoa(h)	erabilitako orduak(h)	Kostua(€)
Ordenagailuak	3	1.000,00 €	43800 h	2664 h	182,47 €
VMWare zerbitzaria	1	5.000,00 €	43800 h	60 h	6,85 €
Visio lizentzia	2	300,00 €	43800 h	60 h	0,82 €
Guztira					190,14 €

7. Taula: Amortizazioen kostuak

Gastuak			
Tresna	Kantitatea	Kostua(unitateko)	Kostu totala(€)
Bulegoko materiala	1	50,00 €	50,00 €
Fortigate 2500E	2	33.209,00 €	66.418,00 €
Fortigate 1500D	4	25.000,00 €	100.000,00 €
FortiManager VM	1	10.000,00 €	10.000,00 €
Guztira			176.468,00 €

8. Taula: Gastuen kostuak

Aurrekontua	
Kontzeptua	Kostua(€)
Barne Orduak	8.975,00 €
Amortizazioa	190,14 €
Gastuak	176.468,00 €
Guztira	185.633,14 €

9. Taula: Aurrekontu totala

11. Ondorioak

Proiektu honetan, sare korporatibo bat segurua bihurtu da, bere baliabideak babestuak mantendu dadin. Horretarako, segurtasun politika sendo bat diseinatu da, segurtasun mekanismo ezberdinak erabiliz. Segurtasun mekanismo hauek segurtasun ekipamenduan inplementatuko dira eta ekipamendu hauek, sarearen segurtasunaren rola hartuko dute.

Internetera konektatuta dauden gailuen igoeraren ondorioz, sare korporatiboen administrariei erakutsi beharko zaie sarearen segurtasunaren garrantzia. Proiektu honetan ikusten denez. Sarbide kontrola inplementatzea oso garrantzitsua da, dagokion segurtasun arauekin eta profilekin.

Proiektuaren beste atal garrantzitsu bat automatizazioa izan da, azpimarratu beharra dago honek industrian hartzen ari duen garrantzia. Gaur egun, fabrikatzaile gehienak bere ekipamenduen APIak garatu dute, automatizazioa haien ekipamenduekin posiblea izan dadin. Proiektu honen kasuan, Python programazio lengoaia erabiliz, Fortinet ingurunean segurtasun arauen sorrera automatizatu da.

Azkenik, proiektu hau erreferentzia gisa har daiteke segurtasun korporatiboen proiektuetarako. Era berean, automatizazioaren bultzadarako erabilgarria izan daiteke, eranskinetan erabilitako kodea publikatu baita.

12. Eranskinak

12.1 Programazio script-a

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import sys
import getpass
import requests
import getopt
import argparse
import JSON
import urllib3
import csv
import datetime
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarnin
g)

# FortiManager klasearen sorrera
class FMG(object) :
    # aldagaien lokalen deinizioak
   def __init__(self,ip,adom,package) :
         self._hostname=None
         self._url= self.__url='https://' + ip + '/JSONrpc'
         self._user= None
         self._pass=None
         self._adom=adom
         self._package=package
         self._token=1
   # Adomaren setterra
   def _adoms(self,adom):
         self._adom=adom
         return
   # Paketearen setterra
   def _packs(self,pack):
         self._package=pack
         return
   #loggeatuko gara token bat lortu dezagun
   def _login(self,ip,user,password) :

         self._user=user
         self._pass=password
         params = [{
               'url' : 'sys/login/user/',
               'data': [{
                   'user' : user,
                    'password': password
            }]

         }]
```

```
            #JSON mezu motak bidaltzen ditu
            response=self._request('exec',params)
            #print response
            self._token=response['session']
            #print self._token
            return response
      # Sesioa desloggeatzeko funtzioa
      def _logout(self) :
            params= [{
                'url' : 'sys/logout'

            }]
            response=self._request('exec',params)
            return response
      # Adom guztiak erakusteko funtzioak
      def _showAdoms(self):
            adoms=""
            params= [{
                'url' : '/dvmdb/adom',
                 'filter' : [
                       'restricted_prds',
                       '==',
                       'fos'
            ]
            }]
            adoms=self._request('get',params)
            k=0
            adoms=JSON.dumps(adoms)
            adoms=JSON.loads(adoms)
            while k < len(adoms['result'][0]['data']):
                  if     adoms['result'][0]['data'][k]['name']     ==
'rootp':

      adoms['result'][0]['data'][k]['name']='global'
                  print                                    ''+str(k+1)+'.
'+adoms['result'][0]['data'][k]['name']+''
                  k=k+1
            return adoms

      # Instalazio paketeak erakusteko funtzioa
      def _showPackages(self):
            packages=""
            params= [{
                'url' : '/pm/pkg/adom/'+self._adom
            }]
            packages=self._request('get',params)
            k=0
            packages=JSON.dumps(packages)
            packages=JSON.loads(packages)
            while k < len(packages['result'][0]['data']):
```

```
                print                                                 ''+str(k+1)+'.
'+packages['result'][0]['data'][k]['name']+''
                k=k+1

          return packages
      # Politikak sortzeko funtzioa
      def _addpolicy(self,line,variable) :
            name_api="API_NEW_"
            name_api=name_api+line["name"]
            print name_api
            if "$" in line["srcintf"] :
                  line["srcintf"]=variable
            else:
                  line["dstintf"]=variable
            if "," in line["service"] :
                  service=line["service"].split(",")
                  #print service
            else:
                  service=line["service"]
            if "," in line["srcaddr"] :
                  srcaddr=line["srcaddr"].split(",")
                  #print srcaddr
            else:
                  srcaddr=line["srcaddr"]
            if "," in line["dstaddr"] :
                  dstaddr=line["dstaddr"].split(",")
                  print dstaddr
            else:
                  dstaddr=line["dstaddr"]

            params=[{
                  'url':
'/pm/config/adom/'+self._adom+'/pkg/'+line["Package"]+'/firewall/
policy',
                  'data' : {
                        'name' : name_api,#'prueba_rule',
                        'dstintf': [
                              line["dstintf"]#'sslvpn_tun_intf'
                        ],
                        'srcintf': [
                              line["srcintf"]#'virtual-wan-link'
                        ],
                        'srcaddr': srcaddr#'all'
                        ,
                        'logtraffic': 'utm',
                        'action': 'accept',
                        'logtraffic-start': 0,
                        'service': service#'ALL'
                        ,
                        'schedule': [
                              'always'
                        ],
```

```
                        # meter campo de descripcion
                        'dstaddr' : dstaddr#'all'
                  }

            }]
            #print params
            response=self._request('add',params)
            return response
      # Bidalketa funtzioa da
      def     _request(self,     method,     params,     option=None,
request_id=1,verbose=False) :
            #try:
            post_data = JSON.dumps({
                  'method': method,
                  'params': params,
                  'id': request_id,
                  'verbose': verbose,
                  'JSONrpc': '2.0',
                  'session': self._token if self._token else 1
                  # 'skip': skip
            })
            #print post_data
            #print self._url
            #logger.debug('POST DATA: {}'.format(post_data))
            # Set verify to True to verify SSL certificates
            r = requests.post(self._url, post_data, verify=False)
            """if not r.ok:
                  logger.error('Erroneous response')
                  r.raise_for_status()
            logger.debug(r.text)
            res =  r.JSON()
            assert res['id'] == request_id, 'Request ID changed.'
            return res
      except requests.exceptions.SSLError as e:
            logger.error(
                  'SSL Handshake failed: {}\n'
                  'You may want to disable SSL cert verification '
                  '[!!!INSECURE!!!]'.format(e)
            )
            raise e"""
            return r.JSON()
      #def gettoken(self):
            #print self._token
      # Paketeen instalazioa egiteko funtzioa
      def _install_pack(self,adom):
            #hacer algo pa coger el tiempo y meterlo en el nombre de
la revision
            rev_name=""
            rev_name="rev_"+str(datetime.datetime.now())
            print self._package
            params=[{
                  'url':'/securityconsole/install/package',
```

```
                'data':{
                'pkg':self._package,
                'flags' : {
                      'generate_rev':'true'
                },
                'adom_rev_name':rev_name,
                'adom':adom
                }
        }]
        response=self._request('exec',params)
        return response
# Leemos opciones
#print '**argv: ', sys.argv[1:]
opts, args = getopt.getopt(sys.argv[1:],"hi:a:u:p:f:",["help"])
#print "**options: ", opts

# Fijamos valores por defecto
hostname = ""
adom = ""
username = ""
password = ""
filename = ""
package = ""

# Argumentu ezberdinak erabiliko dira.
for opt, arg in opts:
    #print "*arg* " + opt + " : " + arg
   if opt in ('-h', '--help'):
        print
"*********************************************************************
***********************************"
        print "Uso: FortiManager.py -i <hostname ip[:port]> -v
<vdom> -u <username> -p <password> -f <archivo.csv>"
        print ""
        print "  Los datos hacen referencia al  FortiManager "
        print ""
        print "  En caso de no especificar hostname, username y/o
password se solicitaran "
        print ""
        print "   -i: hostname o IP del FortiManager, puerto por
defecto: 443. "
        print ""
        print "  -a: adom a utilizar, por defecto adom=root "
        print ""
        print "  -p: dejando la opcion en blanco se solicitara el
password sin mostrarse en pantalla"
        print ""
        print "  -f: dejando la opcion en blanco se solicitara el
nombre de fichero"
        print "          El formato de fichero tiene que ser:
User,Pass,Resource,DstInt"
```

```
            print "      Las columnas han de tener encabezado con los
nombres mencionados"
            print
"*****************************************************************
**********************************"
            print "Ejemplos:"
            print "  python FortiManager.py    "
            print "  python FortiManager.py -i 192.168.1.99 -a myAdom
-u admin -f politics.csv"
            print "  python FortiManager.py -i 192.168.1.99 -u admin
-p password"
            print "   python FortiManager.py -i 192.168.1.99:8443 -u
admin -a myAdom"
            print
"*****************************************************************
**********************************"
            sys.exit(2)
      elif opt == '-i':
            hostname = arg
      elif opt == '-a':
            adom = arg
      elif opt == '-u':
            username = arg
      elif opt == '-p':
            password = arg
      elif opt == '-f':
            filename = arg
      elif opt == 'p':
            package=arg

host = "213.164.51.30"
username = "admin"
password = ""
# Baliorik ez daukaten aldagaiei balioa esleitzeko kodea
if host == "":
   host = raw_input('Introduzca IP: ')
if username == "":
   username = raw_input('Introduzca usuario: ')
if password == "":
   password = getpass.getpass('Introduzca password: ')
fm=FMG(host,adom,package)
# loggeatzen gara
print fm._login(host,username,password)
# Adomak erakusten dira bat aukeratzeko
#adoms=fm._showAdoms()
adom="Sedes_principales"
# Adoma aukeratzen da
if adom == "":
   adom = raw_input('Introduzca el adom en el que quiera instalar
las politicas: ')
"""adom=adoms['result'][0]['data'][int(adom)-1]['name']
#print adom
```

```
#adom=str(adom)"""
# Adom aldagai lokalaren balioa esleitzen zaio
fm._adoms(adom)
# Paketeak erakusten dira
packages=fm._showPackages()


"""if package == "" :
   package = raw_input('Introduzca el paquete al que se quiera
añadir las politicas: ')
packages=packages['result'][0]['data'][int(package)-1]['name']
"""

#csv fitxategia irakurtzen da, politiken edukia definitzeko
with open("CreaReglas_Galindo.csv") as f:
   reader = csv.DictReader(f,delimiter=',')
   dataread = [r for r in reader]
respuesta=""
bucle=1
variable=""
# VLAN berriaren izena sartzen da
variable=raw_input('Introduce el nombre de la nueva vlan:')
#print 'El session token es:'
#fm.gettoken()
# csv fitxategiaren lerro bakoitza politika gisa gehitzen da
for line in dataread:
   #print line

   print fm._addpolicy(line,variable)

   #revisar y poner la version mas estetica
   #for x in line:
   #     print (x+':'+line[x])

# Paketeak erakusten dira, beharrezko paketean instalatu dezazun
packages=fm._showPackages()
if package == "" :
   package = raw_input('Introduzca el paquete al que se quiera
añadir las politicas: ')
packages=packages['result'][0]['data'][int(package)-1]['name']
# pakete aldagaia eguneratzen da
fm._packs(packages)
# Aldaketak instalatzen dira
print fm._install_pack(adom)

print ' Cerrando sesion....'
response=fm._logout()
```

13. Erreferentziak

[1] Esdiario. (2017). La inversión en TIC superará los 41.500 millones de euros en 2018. Esdiario. Hemendik hartua:

https://www.esdiario.com/744652707/La-inversion-en-TIC-superara-los-1.500-millones-de-euros-en-201.html

[2] Statista Research Department. (2019). Cyber crime: number of breaches and records exposed 2005-2018. Statista. Hemendik hartua.

https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[3] Margaret Rouse. (2019). Firewall. SearchSecurity. Hemendik hartua:

https://searchsecurity.techtarget.com/definition/firewall

[4] FintechGlobal. (2018). Cybersecurity investments in Q1 2018 increased by more than 25% YoY. FINTECHGLOBAL. Hemendik hartua:

https://fintech.global/cybersecurity-investments-declined-in-q1-2018-as-later-stage-deals-dried-up/

[5] Priscilia Oppenheimer. (2010). Developing Network Security Strategies. Ciscopress. Hemendik hartua:

http://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2

[6] DOUE. (2016). Reglamento 2016/679. BOE. Hemendik hartua:

https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[7] Margaret Rouse. (2019). Multiprotocol Label Switching. SearchNetworking. Hemendik hartua:

https://searchnetworking.techtarget.com/definition/Multiprotocol-Label-Switching-MPLS

[8] Ashrikar. (2019). Virtual switching system (VSS) Configuration For Cisco 4500 series switches. Cisco. Hemendik hartua:

https://community.cisco.com/t5/networking-documents/virtual-switching-system-vss-configuration-for-cisco-4500-series/ta-p/3147865

[9] Fortinet. (2018). Administrative domain.Fortinet. Hemendik hartua:

https://help.Fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Central%20Management/Administrative%20domains.htm

[10] Fortinet. (2019). HA override. Fortinet. Hemendik hartua:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_override.htm