IKT aktiboen eta IT zerbitzuen auditoria eta laguntzaren web-ingurune seguru baterako migrazioa

Mikel Iturbe
Ibai Osa
Unai Pagalday

2011.eko maiatzaren 19a

Laburpena

Lan monografiko honetan, ITILeko praktika onei jarraiki inzidentziak (enpresako IT zerbitzuetan jazotako edozein anomalia) jakinarazteko zerbitzu seguruaren inplantazioa jorratzen da. Horretarako, prozesu osoaren deskribapena egiten da: ITIL prozesuak lokalizatzea, garapena, segurtasun azpiegituraren (firewall, VPN) eraikitzea... Atal kronologiko desberdinetan jarrita: arazoaren hasieratik hasita, bukaerako ondorioetara arte. Era berean, diseinu eta garapen ahalik eta eraginkorrena izateko, ondo aztertuko dira software ingeniaritzak eskaintzen dituen metodologia desberdinak.

Aurkibidea

Irudien Zerrenda

Sarrera

Lan honetan, enpresa fiktizio batean zerbitzu seguru bat jartzen da, inzidentzia desberdinak era eraginkor eta seguru batean jasotzeko.

Enpresa fiktizio hori, hezkuntzarekin loturikoa izango da, proiektua hasi baino lehen eginiko lanetan egindako ikerketak berrerabili ahal izateko eta gainera, ez duelako horrenbesteko eraginik proiektuaren funtsan.

Eraginkortasuna aipatzen da, industrian hainbatetan erreferente moduan ikusi den ITIL prozesuei jarraiki egin baita, enpresa-arkitekturarekin lerratuz IT teknologiak, nahiz eta inzidentzien bakarrik loturiko lagin txikia izanik.

Segurtasuna, aldiz, aplikazioaren eta bere datuen konfidentzialtasuna, eskuragarritasuna eta integritatea bermatzeko erabiliko da, sarea firewall baten bitartez babestuz eta kanpoko konexioen konfidentzialtasuna bermatuz, kontrako oso faktore gutxirekin, sare pribatu birtualen bitartez.

Azkenik, esparru horietan lan egiteko metodologiak ere garrantzi handia izango du, garaturiko produktuaren kalitate teknikoa (ez funtzionalitate aldetik) baino gehiago. Beraz, lan egiteko erak izango du protagonismo handiena, softwareari dagokionez.

Hurrengo orrietan, proiektu eta produktuaren deskribapen osoa egingo da, bai garaturiko proiektuarena, baita garapen horren prozesuan emandako pausu guztiak ere.

Egileek, Arrasaten, 2011.eko maiatzaren 19an.

1 Arazoaren Analisia

1.1 Inzidentzia-aplikazioa

Sistema honen muina osatzen duen web bidezko aplikazioan, inzidentziak jasoko dira, ITILeko (*Information Technology Infrastructure Library, Informazio Teknologien Azpiegituraren Liburutegia*) Zerbitzua emateko liburuan aholkatzen diren praktikei jarraiki:

Erabiltzaileen logeoa

Gure sistemak bi erabiltzaile mota izango ditu: informatika departamentuko langileak eta gainontzeko langileak. Edonork web orrian zerbait egin nahi izango badu lehendabizi logeatu egin beharko da. Ondoren langile motaren arabera gauza batzuk egiteko aukera izango dute baina beste batzuk ezingo dituzte egin. Langile guztiek izango dute enpresako aktiboak ikusteko aukera eta inzidentziak zabaltzeko aukera. Bestalde, informatika departamentuko langileek soilik izango dute inzidentziak itxi, inzidentziak ikusi edo inzidentzien taula historikoa ikusteko aukera.

Aktiboak ikusi

Esan bezala enpresako langile guztiek izango dute enpresako aktibo ezberdinak ikusteko aukera. Aktibo hauek taldeka ikusiko dira motaren arabera sailkatuta. Beraz aktiboak ikusi nahi badira zein aktibo mota ikusi nahi den zehaztu beharko da eta hau egin ostean aktiboen taula azalduko da. Era honetan langileak zein aktibotan eragiten duen inzidentziak adierazi ahalko du eta informatikako departamentuko langileak aktibo hori zein beste aktiborekin dagoen erlazionatuta begiratu.

Inzidentziak sartu

Langile guztiek daukate inzidentziak berriak irekitzeko aukera. Inzidentzia bat sortzerakoan zein aktibori eragiten dion adierazi beharko da.Gainera, inzidentzia horren deskribapen bat sartzeko aukera egongo da eta inzidentzia hori zein motatako den ere adierazi beharko da. Horretaz gain, sistemak automatikoki inzidentzia zein langilek eta noiz ireki duen gordeko du.

Inzidentziak ikusi

Informatikako departamentuko langileek izango duten aukeren artean inzidentziak ikusteko aukera izango dute. Honela irekita baina oraindik konpondu gabe dauden inzidentzien informazioa begiratu ahalko da.

Inzidentziak itxi

Informatikako departamentuko langileek inzidentzia bat itxi nahi badute lehendabizi, hau aukeratu beharko dute eta ondoren zein soluzio aplikatu dioten deskribatzeko aukera izango dute horretaz gain, sistemak zein langilek itxi duen inzidentzia ere erregistratuko du eta inzidentzia hau inzidentzien taulatik ezabatu eta taula historikora pasako du.

Inzidentzia historikoak ikusi

Informatika departamentuko langileek iada konponduta dauden inzidentzien informazio ikusteko aukera ere izango dute, hau oso erabilgarri izan daiteke etorkizuneko akatsak zuzentzen lagun diezagukelako.

Funtzionalitate guzti hauek definiturik, erabiltzaileek era egokian eman ahalko dituzte inzidentziak, eta IT departamentuko langileek arreta gune zentralizatua izango dute euren egitekoak ikusteko. Aplikazio hau, baina, ezin dute sare lokalean dauden langileek bakarrik erabili, kanpoan dauden langileek ere (bidaian dauden komertzialak e.a.) erabili beharko dute, daukaten arazoen berri emateko. Horrek eramaten gaitu hurrengo atalera.

1.2 Aplikazioaren segurtasuna

Esan bezala, aplikazioa ez da egon behar eskuragarri bakarrik enpresako sare lokalean dauden langileentzat, kanpoan egon daitezkeen langileek eta batez ere, zerbitzu teknikoko langileek gure inzidentziak jakinarazteko zerbitzua erabili behar dute. Noski, ziurtatu behar dugu kanpokoen artean, langileek bakarrik erabil dezaketela zerbitzu hau eta gainera, hirugarren pertsona batek ezin izango duela langilearen eta gure zerbitzuaren arteko komunikazioa atzeman.

Hori zirutatzeko bi tresna ezberdin erabiliko dira *firewall* edo su-hesia eta VPN-a (*Virtual Private Network, Sare pribatu birtuala*). Firewall-aren bitartez lortzen dena da trafikoa filtratu, izan ditzakeen jatorri eta helburuaren arabera. Era honetan, kanpotik gure inzidentzia zerbitzura egindako eskaera guztiak galarazi ditzakegu, VPN-a erabiltzen duten erabiltzaileak kenduta. VPN-a nahiz eta kanpoan egon, sare lokalean egongo litzatekeen modura jokatzea ahalbidetzen duen softwarea da, beste sare batzuetan barrena trafikoa eramanez. Gainera, trafiko hori zifratu egiten duenaren abantaila du, hirugarren pertsonengandik trafikoaren edukia ezkutatuz.

1.3 Metodologia

Ez da nahikoa aurretik aipaturiko bi garapenak beste gabe egitea, lanerako metodologia propio eta egokia garatzea beharrezkoa da, proiektua bere osotasunean ahalik eta akats gutxien eta errekurtsu erabilera egokiena eginez garatu dela ahal den heinean ziurtatzeko. Baliabide hauek daude definitu ditugu, besteak beste:

Bertsio-kontrolerako sistema Hainbat pertsona aplikazio bera garatzen egon ahal izateko.

Kodifikazio manuala Kodearen egitura uniformea eta ulerterrazagoa izateko.

Berrikuspen sistema Kodean egon litezkeen akatsak ekiditeko.

Frogak Kodeak funtzionalitateak ahalik eta akats gutxienekin betetzen duela ikusteko

Baliabide hauetaz gain, baliabideen balorazioa ere txertatuko da dokumentuan, berauen eragina aztertuz eta egin ahalko liratekeen hobekuntza posibleak azalduz. Aparteko dokumentu bat ere garatuko da, aplikazioaren funtzionalitateak eta diseinua zehaztuko dituena, Analisia eta Diseinua izenekoa. [1].

[1]Dokumentu horren edukiera lan honetan dago bere osotasunean eta ez da eranskinen batean idatzi edukia ez errepikatzeko. Balizko dokumentu horren zati izango liratekeen atalak, hauek dira: 1.1, 1.2, 2.1 eta 2.3

2 Diseinua

2.1 Informazio sistemak

2.1.1 ITIL prozesuak

Inzidentziak nola jasoko diren definitu aurretik, beharrezkoa da definitzea enpresak berak nola jokatuko duen inzidentzia bat jasotzerakoan, hortik gero plano praktikora jaitsi eta aplikazioa nola garatuko den pentsatuz. Baina, hori egin baino lehen, nahitaezkoa da IT departamentuaren egitura definitzea, hau da, departamentua nortzuk osatuko duten. Osaketa hori egiteko, 14 pertsona eskuragarri izango ditugula uste da.

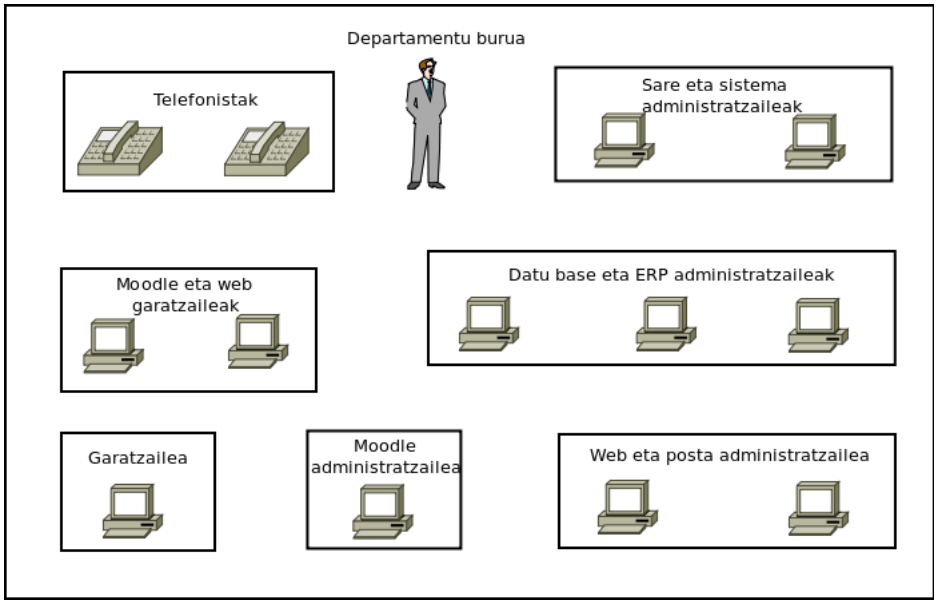
Jarraian zerrendaturiko dira IT departamentuak kudeatu beharko lituzkeen zerbitzuak, heziketa arloko enpresa bat dela suposatuz:

- Moodle
- Webgunea
- Web zerbitzuak (idazkaritza birtuala, intranet)
- E-posta zerbitzuak
- Erabiltzaileen kudeaketa
- Baliabideen kontrola (nominak, ERP-a)
- Datu-base desberdinen kudeaketa
- Sarearen kudeaketa (barne-sarea, interneterako sarbidea)
- Ordenagailu pertsonalen kudeaketa (instalazioak e.a.)
- Datuen segurtasuna kudeatu

Ikusita zerbitzuak zeintzuk diren, ikusi beharko da, gure bezeroei (enpresako gainerako zatia) eskaintzen diegun zerbitzu hauen arabera, nola egongo den banatuta gure departamentua, zerbitzu hauen garrantziaren eta eskatutako lanaren arabera. Era berean, departamentuaren muina da erabiltzaileen eskariak aztertu eta konpontzea, baita funtzionalitate berriak ahal den heinean txertatzea, enpresaren eguneroko jarduna ahalik eta gutxien oztopatu eta kontrara, berau bultzatzeko.

1 irudian agertzen den moduan banatu dugu gure balizko departamentua:

Departamentu-burua (pertsona bat). Izenak dioen moduan, gure IT departamentua eta beraz, Service Desk-aren burua izango litzatekeen pertsona da, formazio tekniko zein kudeaketarakoa duen pertsona litzateke berau, erabaki estrategikoak hartu eta azken hitza esateko ahalmena izateko. Era berean, gure departamentua eta gainerakoen arteko zubia litzateke, enpresako erabakietan informazio teknologien esparruan aholkatuz, edota soluzio berriak eskainiz. Ez luke parte hartuko zerbitzuen kudeaketa zuzenean, baina zerbitzuen araberako baliabideak lortzeko gaitasuna luke eta departamentuaren martxa on edo txarraren arduradun edo erantzule izango litzateke.



Irudia (1): *IT departamentuaren egitura*

Hartzaileak Bi pertsona. Arduraduna maila administratibo batean enpresarekin dugun lotura den bezala, hartzaileak, egunerokotasunean gertatzen diren gora-beheretzako kontaktuak lirateke. Zubia lirateke, beraz, gora-behera duten pertsonen eta gora-behera hori konpontzeko gai diren pertsonen artean. Arazoa konpontzeko erraza baldin bada edota askotan errepikatutakoa, eurak izango lirateke zuzenean erabiltzaileari eskaera konponduko lioketenak. Beraiek ikusiko lukete ea inzidentzia berriak dauden edo ez.

Moodle eta Web garatzaileak bi lirateke eta euren lana, Moodle-i funtzionalitate berriak gehitu edota web aplikazioak garatzea/eguneratzea litzateke, esate baterako, enpresako intranet sarean jartzeko.

Garatzaile bat Honek ere, aurrekoek bezala, aplikazioak garatuko lituzke, baina ez web ingurune baterako, baizik eta datu-base bateko interfazea, kalkuluak egiteko zenbait aplikazio... garatuko lituzke.

Moodle administratzailea Moodle zerbitzua behar bezala dabilela ziurtatuko duen pertsona da, erabiltzaileak alta eta baja emateaz gain. Bera litzateke arduraduna zerbitzua, gero ezarriko diren baldintzen pean mantentzeko.

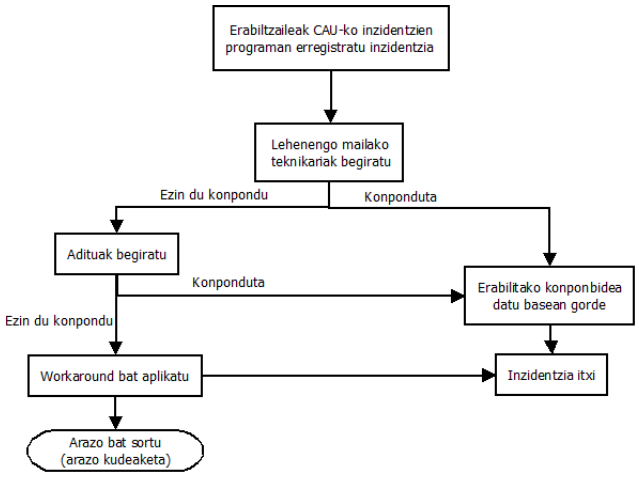
Bi Web eta posta administratzaile Hauek, webguneak, garaturiko web aplikazioak eta posta zerbitzua mantenduko luketen pertsonak dira, erabiltzaileentzat ahalik eta eskuragarrien jarriaz.

Bi Sistema eta sare administratzaile Sistema (zerbitzariak, erabiltzaileen ekipoak...) eta sarea kudeatuko luketen pertsonak dira.

Hiru datu-base eta ERP administratzaile Horietatik bi arduratuko lirateke ERPa kudeatzeaz eta bestea datu-baseko administratzaile modura. ERPko administra-

tzaileetariko bat, datu-baseko administratzaile ere izan daiteke, besteari lagundu eta zerbitzu hobe bat eman ahal izateko.

Behin departamentua osaturik, bi hartzaile eta hainbat adituk osatuko luketela ikusirik, inzidentzia baten aurrean nola jokatuko litzatekeen definitu behar da, ITIL liburuetan azaltzen den modura. Gurean, 2. irudian ikus daiteke nola jokatuko den inzidentzia baten aurrean. Bertan,*Arazoen kudeaketa* izeneko hitzak agertzen dira, baina hori askoz ere hedadura handiagoa duen gaia da eta lan honetako zioa baino askoz harago doa. Lan honetan suposatuko da, inzidentzia guztiak atoan konpondu edo bestela workaround (momentuko konponketa), zerbitzuaren aldaketa sakonak beste era batera landu beharreko gaia litzateke.



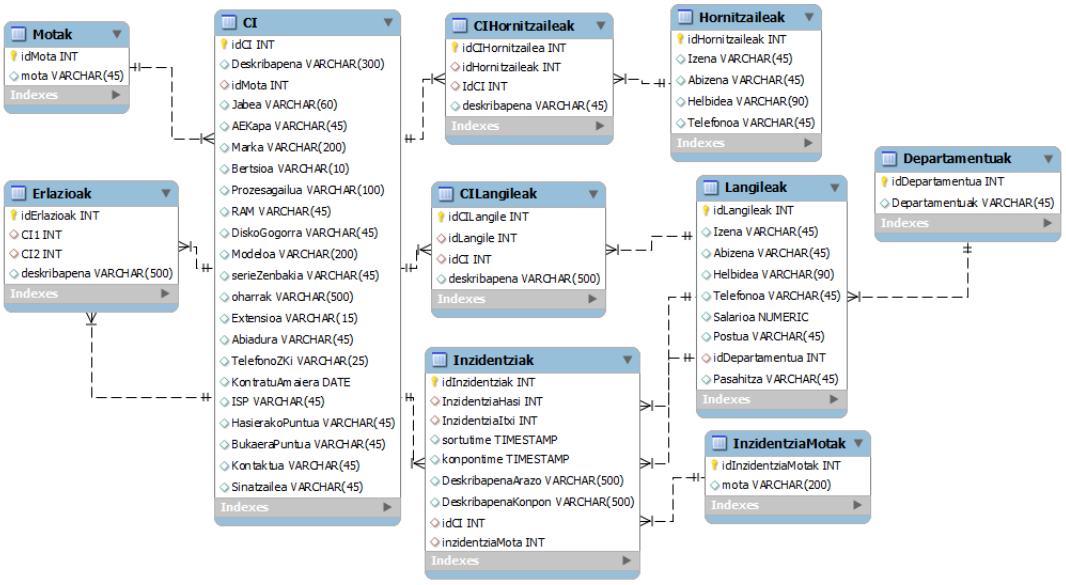
Irudia (2): *Inzidentzien kudeaketa*

2.1.2 CMDB

Behin enpresan nola jokatuko den definiturik dagoela, behar-beharrezkoa da dokumentaturik izatea zeintzuk diren inzidentziekin loturik egongo diren elementuak, hau da, enpresako IT aktiboak. Beharrezkoa da ondo gordeta izatea aktibo bakoitza zer den, zein atributu dituen eta zein den aktibo horren jabe edo arduradua. Horretarako tresna, CMDB-a da.

CMDB (*Configuration management database, Konfigurazioaren kudeaketarako datubasea*) delakoa da inzidentziak gordetzeko web aplikazioaren muina. Bertan daude gordeta, IT teknologiekin loturiko enpresako aktibo guztiak (CI edo konfigurazio item-ak deritzena). 3. irudian ikus daiteke zein den CMDB-aren egitura. Aktibo gehienak taula berean daude jarrita, kodeak esleitzerako orduan erraztasuna izateko. Era berean, asmo horrekin garaturiko funtzioen bitartez sartuko dira datuak datu-basean, erabiltzailearentzat taulako NULL balio guztiak guztiz gardenak izango direlarik.

3. irudian ikus daitekeenez, inzidentziak gordetzerako orduan, inzidentzia kodea, inzidentzia zabaldu duen langilearen kodea, inzidentzia itxi duen langilearen kodea, inzidentzia hasi zen momentua, bukatutako momentua, inzidentziaren deskribapen laburra, konponketaren inzidentzia laburra, inplikaturiko konfigurazio itemaren kodea eta, azkenik, zein inzidentzia mota litzatekeen, motak, beste taula batean egongo lirateke, katego-



Irudia (3): *CMDB-aren eredu erlazionala*

rizatuta. Era honetan, inzidentziaren inguruko datu guztiak gorde ahal izango lirateke, bertan.

2.1.3 Inzidentzien web aplikazioa

Erabiltzaileak web orrira sartzean izena eta pasahitza sartu beharko dute (datubasean hash baten bitartez egongo direlarik gordeta), gure enpresan lana egiten dutela ziurtatzeko. Behin sisteman logeatuta, inzidentziak sortzeko aukera, edo enpresako CI(configuration item) ezberdinak ikusteko aukera izango dute. Inzidentzia bat zabaltzerako orduan, langileek beraien kodea eta intzidentzia infektatzen dion itemaren kodea sartu beharko du, deskribapen batekin eta intzidentzia mota bat aukeratuz.

IT departamentuko langileak badira ordea, honetaz gain jendeak zabalduriko intzidentziak ikusteko edota ixteko gaitasuna ere izango dute. Inzidentzia bat ixtean intzidentzia hori konpontzeko bete behar izan diren pausuak idatzi beharko ditu langileak, dokumentazio eta erreferentzia modura gordeta izateko.

2.2 Metodologia

2.2.1 Kodifikazio manuala

2.1.3 atalean azaldu den aplikazioa garatzen hasi baino lehen, beharrezkoa da jakitea aplikazioa *nola* garatuko den. Ez funtzionalitate aldetik, horiek jada definiturik baitaude, baizik eta kode aldetik nola egongo den eginda. Era honetan lortzen dena da, kodearen estiloan uniformetasun bat bermatzea, egingo diren berrikuspenak erraztu (programatzaile bakoitzaren programazio-estiloak inpaktu txikiagoa izango baitu eta komentatuta egongo baita), bertsio berriak egitea errazteko (kodifikazio manualak, kodea berriztagarria izateko irizpideak lantzen baditu, bederen). Finean, kode eraginkorragoa eta ikuspegi

profesionalagoa emango diona egitea dugu helburu. Irakurleak nahi izanez gero A eranskinean du ikusgai manuala osorik.

2.2.2 Bertsio-kontrola

Behin kodea nola idatziko dugun definitu dugula, beharrezkoa da era eraginkorrean kode hori garatzeko bitartekoak izatea. Hainbat pertsonen artean kodea garatuko delarik (era eraginkorrean espero da, horretarako sortu baita kodifikazio manuala), beharrezkoa da bakoitzak izango duen bertsioa azkena izatea, integraziorako aldaketak ez egoteko eta garatzaile guztiek funtzionalitate aldetik bertsiorik osoena izateko.

Gainera, funtzionalitate oso interesgarriak eskaintzen dituzte.

- Kudeatu beharreko kodearen biltegiratzea.
- Kodeari aldaketak egitea ahalbidetzea.
- Eginiko aldaketa guztiak erregistratzea.

Beraz, ez da izango beharrezkoa garatzaile guztiek kode osoa izatea euren laneko makinetan, errepositoriotik deskargatu, bertan landu (aldaketa partzialak, fitxategiak gehitu, kendu...) besterik ez baitu egin beharko. Gainera, ikusi ahal izango da nork egin duen zein aldaketa.

Gure kasuan Git softwarea aukeratu dugu, web zerbitzu bati lotura egonik, beti eskuragarri dago (guk zerbitzari moduan erabiliko geunkeen ordenagailu jakin batean gorde behar izan gabe kodea, baliabideak aurreztuz). Gainera, funtzionalitate gehigarri gisa, bezeroa ere sartu ahalko litzateke web interfaze horretara bere lanaren nondik norakoak nola doazen ikusi ahal izateko (hala nahi izanez gero, noski). Ezingo luke edukirik igo web interfazetik, baina ikusi ahal izango luke berau. 3.2.1 atalean azalduko da tresna hau nola erabiltzeari buruzko argibide praktikoak.

Direktorioen estrukturari dagokionez, hiru direktorio nagusi leudeke: bat garapen nagusirako eta beste bi albo lanetarako (datu-baseko datuak eta proiektuaren dokumentazioa). Kasu honetan, direktorio laguntzaileen kasuan, ez luke lagunduko bertsio-kontrola eginez, baizik eta sarean dagoen errepositorioa izanez, fitxategiak gordetzeko.

2.2.3 Berrikuspenak eta Frogak

Berrikuspen eta frogen helburua, kodea behin sorturik dagoela ahalik eta arazo gutxien dituela bermatzea da, bai *bug*ak bilatuz zein funtzionalitateak betetzen dituela ikusiz. Berrikuspenen helburua garatzaile batek idatzitako kodea beste garatzaile edo kodea irakurtzeko gai den beste norbaitek, ea bug-ik sortu daitekeen edo egin beharreko funtzionalitateak betetzen dituen garatzaileak sortutako kodea. Gure kasuan, lan-talde txikia izanik, jende desberdinak egindako kodea guk ikus dezakegu, sistematikoki. Aurretik aipaturiko errepositorioan kodea izanda, erraztu egiten du kodea begiratzearen lana.

Frogei dagokionez, bi eratako frogak daude, kutxa beltzekoak eta kutxa zurikoak. Kutxa beltzekoetan ez da kodea begiratzen eta aplikazioak ea espero den moduan jokatzen duen aztertzen da, hau da erabiltzaile normal batek, kode itxiko aplikaziobatean erreportatuko lukeena, gauza jakin bat ezin daitekeela egin aplikazioarekin. Kutxa beltzeko

frogen helburua, erabiltzaileak egin ditzakeen pausuak errepikatzea da (funtzionalitateak eskura izanik), erroreak geronek ikusteko, erabiltzailearengana heldu baino lehen.

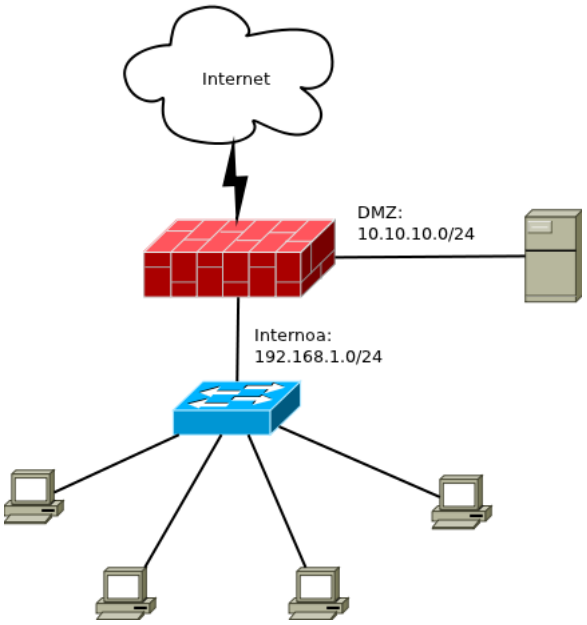
Kutxa zuriko frogak, jada kodea ikusgai daukagularik egiten dira (hortik izena, gardentasuna-edo erakutsiz) eta kodean dauden balioen arabera egiten dira frogak (String bateko balioak zeintzuk diren ikusirik, balio hori baino handiagoak jarriaz, adibidez edo funtzio bati beste aldagai mota bat pasaz).

Definituriko frogak Kutxa beltzeko frogak

- Erabiltzaile izen edo pasahitz oker bat sartu
- Langile arrunt baten erabiltzaile izen eta pasahitz zuzenak sartu eta aktiboak ikusteko aukeratu
- Informatikari bat logeatu eta inzidentzia historikoak ikusi
- Informatikari bat logeatu eta inzidentziak ikusi
- Informatikari batek inzidentzia berri bat sortu ondoren inzidentziak ikusteko sakatu
- Informatikari batek inzidentzia bat itxi eta inzidentziak ikusteko sakatu
- Informatikari batek inzidentzia bat itxi eta inzidentzia historikoak ikusteko sakatu

Kutxa zuriko frogak

- Inzidentzia bat sortu eta begiratu inzidentzia berriarentzat kode berri bat sortzen den automatikoki
- Inzidentzia bat sortu eta begiratu inzidentzia hori sortu den data benetan sortu den dataren berdina den.
- Inzidentzia bat sortu erabiltzaile batekin eta begiratu ea inzidentzia sortu duen erabiltzailearen kodea benetan inzidentzia sortu duenarena den.
- Inzidentzia mota berri bat sartu datu basean eta begiratu ea inzidentzia mota berri hori comboboxean agertzen den
- Aktibo berri bat sartu eta ondoren begiratu aktibo hori agertzen dela.
- Inzidentzia bat itxi eta begiratu konponduta parametroaren egoera aldatzen den.
- Inzidentzia bat itxi eta begiratu inzidentzia itxi duen langilearen kodea ongi gordetzen den.
- Inzidentzia bat itxi eta begiratu inzidentzia itxi den data ongi gordetzen den.



Irudia (4): *Sarearen eskema*

2.3 Segurtasuna

Aipatu bezala, beraz, web aplikazioa sare lokaletik kanpo joango da, baina era berean kanpoko saretik babestuta joango den inguru batean. Inguru horri, DMZ (*DeMilitarized Zone, zona desmilitarizatua*) deritzo, bi *fronte* ezberdinen arteko mugan baitago, aparteko ingurune batean. Era honetan, bertara sarbidea kontrolatuko duen firewall-aren bitartez, sare lokaletik eta kanpotik, VPN bat erabilita sartu ahal izango da.

Firewall-ak, horretarako, konexioak baimendu behar ditu, bai sare lokal eta DMZ artean, baita kanpotik datorren VPN bitartezko trafikoa (kanpoko langileak eta batez ere zerbitzu teknikoko enpresa) ere. Beste konexio guztiak deseginez, DMZ horren segurtasuna bermatzen dugu, guk espreski baimentzen ez diogunari sarbidea ukatuz.

Laburbilduz, hauek lirateke Firewall-eko oinarrizko arauak (portuak ez dira esplizituki adierazi, zerbitzu bakarra dagoelako, suposatuko da, zerbitzaria helburu duten paketeak 80. portura joango direla eta erantzunak $>$ 1024 portuetara).

Jatorrizko helbidea	Helburu helbidea	Protokoloa	Flag-ak	Ekintza
192.168.1.0/24	10.10.10.0/24	http		Baimendu
10.10.10/24	192.168.1.0/24	http	STB	Baimendu
192.168.1.0/24	ANY	http		Baimendu
ANY	192.168.1.0/24	http	STB	Baimendu
220.100.65.98	10.10.10/24	vpn		Baimendu
10.10.10/24	220.100.65.98	vpn	STB	Baimendu
ANY	ANY	ANY		Ez baimendu

Era honetan, zerbitzu teknikoko enpresakoek (zeina 220.100.65.98 helbidea erabiliko luketen), gure enpresakoekin batera kontsultak egin ahal izango lukete sarearen bitartezko VPN trafiko zifratua erabiliz. VPN zerbitzaria, Firewall-eko 10.10.10/24 sareko gateway-ean egongo litzateke eta beste enpresakoak, bertako IP helbidea jakinda, euren VPN

bezeroa erabiliz konektatu ahalko lirateke, baina, esan bezala, bakarrik euren enpresako helbidetik.

3 Inplementazioa

3.1 Informazio sistemak

Web aplikazioa, JSP (*JavaServer Pages*) erabilita sortu da, azpitik Java erabiliz. Honen arrazoi nagusia, webgune dinamikoak sortzeko duen erraztasuna, datu-basearekin konektatzeko eginiko funtzioak eta duen integrazio maila altua da.

Txosten honen helburua berau ez denez, labur-labur azalduko da webgunearen egitura:

Web orrira index.jsp orritik sartzen da, behin logeatuta beste orrietara sartzeko baimena izango duelarik erabiltzaileak: inzidentziak.jsp inzidentziak ikusteko, inzidentziaSortu.jsp inzidentziak sortzeko eta aktiboakIkusi.jsp aktiboak ikusi ahal izateko. Web orriak akzio bat egitean kontrol.jsp-ra doa, honek egin beharreko kalkuluak egin ostean behar den orrira berbideratzen du, aktiboakIkusi.jsp orrian izan ezik, horri honetan comboBox bat egongo da aktibo mota aukeratu ahal izateko, comboBox honen submit-a fitxategia beraren aurka egingo da. Beste bi fitxategi ere badaude aktiboakTaula.jsp eta inzidentziaTaula.jsp bi orri hauek iframe-en bidez sartuko dira beste web-orrietan, taulak bistaratzeko bakarrik dira.

3.2 Metodologia

3.2.1 Bertsio kontrola

Aurreko diseinu atalean aztertuz gero zein erraminta erabiliko den eta zergatik, oraingoan Git (Github errepositorio zentral modura) nola konfiguratu eta erabili. IDE batekin sinkronizatu beharrean, zuzeneko metodoa erabili da, komando-lerroa erabiliz. Git instalatu ondoren, gure proiekturako konfiguratu behar da, erabiltzailearen izena eta e-posta helbidea jarriaz:

```
git config --global user.name "popbl6"
git config --global user.email popbl6@gmail.com
```

Behin konfiguraturik, has gaitezke lanean:

```
mkdir POPBL6                                    (proiektuaren direktorioa
                                                sortu)

cd POPBL6                                       (direktoriora joan)

git init                                        (git errepositorio
                                                hutsa sortu)

touch README                                    (README sortu)

git add README                                  (fitxategia indizera
                                                gehitu)

git commit -m 'lehen commita'                   (aldaketa egin
```

```
                                                    errepositoriora,
                                                    lehen commita mezuarekin)

git remote add origin git@github.com:popbl6/POPBL6.git  (Github-en dagoen
                                                    errepositorioa gehitu
                                                    origin izenarekin)

git push -u origin master                           (gure errepositorio
                                                    lokaleko adar nagusia
                                                    Github-era pasa)
```

Github-eko azken kodea hartzeko, aldiz, nahikoa da gure errepositoriora joan eta hau idaztea:

```
git pull origin
```

Automatikoki hartuko du bertako adar nagusia (*master* defektuz). Agindu honek bi ekintza egiten ditu: lehenik eta behin norberaren errepositorioan ez dauden commit-ak (ekarpen kodean) jaitsi (`fetch` ekintza) eta gero, jaitsitakoa eta errepositorio lokala batu (`merge` deritzona). Era honetan, sinkronizaturik geratuko dira guk lan egiteko erabiltzen dugun errepositorio lokala eta github-eko zentrala.

3.3 Segurtasuna

Atal honetan, azalduko dena da nola konfiguratu den erabili den Fortigate firewall-a Diseinu atalean planteaturiko soluzioa lortzeko. Dena dela, irakurleak interesa izanez gero, *backup*eko konfigurazio fitxategi osoa aurkitu dezake B eranskinean. Era berean, hainbat gauza gehigarri jarri dira (web filtroa e.a.), baina ez denez txosten honetako muina, ez dira jorratuko hemen.

Lehenik eta behin, Firewall-aren interfazeak konfiguratu behar dira (gogoan izan behar da diseinuko atalean azaltzen den 4 irudia):

```
System > Network > Interface > dmz

Addressing mode              Manual
IP/Netmask                   10.10.10.1/255.255.255.0
Administrative access        PING
```

Adibide moduan jarritako DMZko interfazeaz gain, beste biak (barne-sareari eta `wan1`, internetera konektatuko lukeen interfazeak) antzera konfiguratu behar dira. Behin hiru interfazeak konfiguraturik daudela, beharrezkoa da firewall-eko erregelak kargatzea:

```
Firewall > Policy

Source Interface / Zone          internal
Source Address                   FinEng
Destination Interface / Zone     wan1
```

```
Destination Address                All
Schedule                           Always
Service                            ANY
Action                             ACCEPT
NAT                                Enable
Protection Profile                 standard_profile
```

Erregela honekin, FinEng taldeari dagozkion helbideetatik (taldearen sorrera ez da jorratzen hemen, baina era berean, sare interno osoari dagokion helbidea jar daiteke bertan), edonora doazen konexioak baimentzen dira, `standard_profile` profila aplikatzen zaielarik (guk sortua) eta NAT ere aktibatuz.

Era berean aplikatu daiteke DMZn egongo den zerbitzarira konektatzeko:

```
Firewall > Policy

Source Interface / Zone            internal
Source Address                     FinEng
Destination Interface / Zone       dmz
Destination Address                10.10.10.5
Schedule                           Always
Service                            ANY
Action                             ACCEPT
NAT                                Enable
Protection Profile                 standard_profile
```

Suposatuz, noski, zerbitzariaren IP helbidea hor agertzen den 10.10.10.5-a delarik. Behin erregela horiek definituta, beharrezkoa da VPNa aktibatzea eta ostean erregela batzuk gehiago definitzea, kanpoko enpresako kideak konektatu ahal izateko gure zerbitzarira. Lehenengo, helbideei izenak emango dizkiegu.

```
Firewall > Address > New

Address name           DMZ sarea
Type                   Subnet / IP Range
Subnet / IP Range      10.10.10.0
Interface              Any

Firewall > Address > New

Address name           Enpresa teknikoa
Type                   Subnet / IP Range
Subnet / IP Range      64.230.254.50
Interface              Any
```

Esan behar da, bigarren IP helbidea, simulatzeko asmoarekin esleitu zaiola, `wan1`-en sare berean egon beharko duelako, baina, benetan beste sare batean egongo litzateke eta beste IP helbide guztiz desberdina litzateke.

Helbideak definiturik izanda, hurrengo pausua, Fortigate-ko aldeko VPNa konfiguratu behar da.

Lehen fasea konfiguratzeko:

```
VPN > IPSEC > Auto Key (IKE)

Create phase 1

Name                    Enpresa teknikoa
Remote Gateway          Static IP Address
IP address              64.230.254.50
Local interface         wan1
Mode                    main
Authentication Method   Preshared Key
Pre-shared key          pasahitza
Peer options            edozein
```

Bigarren fasea konfiguratzeko:

```
VPN > IPSEC > Auto Key (IKE)

Create phase 2

Name                  enpresa_tunel_1
Phase 1               Enpresa teknikoa

> Advanced

Jatorrizko helbidea:  64.230.254.50
Helbide helburua:     10.10.10.0
```

Era honetan, lehen fasearen ostean, sortuko den tunela konfiguratzen da, jatorria beste enpresak duen bezeroan egongo litzatekeelarik eta gure DMZko interfazeko VPN zerbitzaria izango delarik konexioaren helburua. Tunelak eginda, beharrezkoa da, tunel horien arteko trafikoa ahalbidetuko duen firewall erregela berriak.

```
Firewall > Policy

Source Interface / Zone          dmz
Source Address                   DMZ sarea
Destination Interface / Zone     wan1
Destination Address              Enpresa teknikoa
Schedule                         Always
Service                          ANY
Action                           IPSEC
VPN Tunnel                       enpresa_tunel_1
Allow Inbound                    yes
```

```
Allow outbound                  yes
Inbound NAT                     yes
Outbound NAT                    no
Protection Profile              standard_profile
```

Era honetan, firewall-ak baimenduko du, enpresa teknikoko eta gure DMZn dagoen sarearen arteko VPN trafiko zifratua. Firewall eta VPN zerbitzaria konfiguraturik daudela, beharrezkoa da VPN bezeroa (FortiClient, zerbitzu teknikoko enpresak izango lukeena) konfiguratzea.

```
VPN > Connections

Connection Name             konexioIzena
Configuration               Manual
Remote Gateway              64.230.120.8 (FortiGate-aren wan1 interfazea)
Remote Network              10.10.10.0  / 255.255.255.0
Authentication method       Preshared key
Preshared key               1. fasean jarritako pasahitza
```

Behin jada konektaturik dagoela eta martxan jarrita, inolako arazo gabe ikusi ahal izango dugu inzidentzia zerbitzariaren edukia.

4 Ondorioak

4.1 Informazio teknologiak

Informazio teknologiei dagokionez, zailtasun handiena ITILeko praktika onak gure proiektu honetara era zehatz batean inplementatzea izan da, baina behin aplikaturik dagoela, konturatu gara asko errazten duela IT teknologien eraginkortasuna enpresan. Gure kasuan, inzidentzia guztiak leku zentralizatu batean jarriaz, IT departamentuari lana asko erraztuz eta erabiltzaileei begira seriotasun irudia emanez. Horrelako webgune bat izateak, telefonoak eta antzeko baliabideek ez bezala, asko handitzen du eskalagarritasuna eta hainbat eta hainbat erabiltzaile egon daitezke inzidentziak sartzen webguneak. Gero kontuan izan behar da, noski, gero IT departamentuak ere izan behar dituela baliabideak inzidentziei aurre egiteko, notifikazio zerbitzua, aurpegia besterik ez baita.

4.2 Metodologia

Hainbat dokumentu sortu dira, garapenari laguntzeko. Horietako bat izan da kodifikazio manuala, nola kodifikatu behar den adieraziz. Erabilgarria izan arren, badaude hobetu ahalko litzatekeen gauza nagusi bat, esplizitua izatea. Bertan datozen gauza asko, lengoai askotan erabili daitezkeenak dira, baina beharrezkoa da Javan eta bereziki JSPko gauza propioetan direnak (beste lengoaiek ez dituzten propietate edo sintaxia) gehiago sakontzea, gure produktua hobetzeko.

Bertsio kontrolari dagokionez, asko erraztu du hainbat pertsonen artean aplikazioa garatzea, eta autokritikarako ere tresna egokia izan da (noiz egin diren aurrerapen handienak, noiz gutxien). Oro har, esan daiteke behar-beharrezko tresna bihurtu dela taldean lan egiteko.

Berrikuspen eta frogekin, esan behar da berrikuspenak era informalean egin direla baina ez dela egon aparteko txostenik, egin den gauza bakarra izan da, hurbiltasuna profitatuz, garatzaileari galdetu ea zertarako zen gauza bat edo bestea, kasu batzuetan zuzenketak eginez. Frogak aplikatu egin dira eta ez da egon inolako arazorik, behintzat txosten hau bukatu den egunera arte.

4.3 Segurtasuna

Firewall eta VPNen erabilgarritasuna konprobatu da, erregela desberdinek trafikoari nola eragiten dion ikusita. VPNaren kasuan, zifraketaren balioa ere kontuan hartu da, birtualki, oso urrun egon daitekeen pertsona bati gure sarean bertan egotearen abantaila guztiak emateak dituenak, hain zuzen, zifraturiko konexioak hori ahalbidetzen duelako. VPNak eskaintzen duen alternatiba merkea ere baloratu da, puntutik punturako konexioekin alderatuz gero.

5 Hobekuntzak

Hobekuntza posibleen artean nabarmendu daitezke eginiko aplikazioaren alorrean, CMDB-aren diseinu hobea (horrenbeste eremu nulo izango ez lituzkeena) edota inzidentzietaz harago doan kudeaketa eredu osoaren inplementazioa, ITILek eskaintzen duen bibliografia eta lan-tresna mardulak profitatuz.

Era berean, segurtasunari dagokionez, Firewall-aren diseinu errealistagoa egin daiteke, DMZtan beste zerbitzari batzuk jarriaz eta bertara kanpoko sarbidea baimenduz (web eta posta zerbitzariak, akaso). Era berean, barne saretik kanporako trafiko osoa baimenduta dagoen aldetik (web filtroekin, egia da), agian hori findu beharko litzateke eta konexio mota batzuk ez baimendu, segurtasun neurriak zorrozteko. Datu-basean, *hash* algoritmo indartsuago bat erabiltzea ere ondo legoke, pasahitzen krakeoa zailtzeko.

Azkenik, erabilitako metodologiarekin, alderik nabarmenena, Github erabiltzerakoan erabiltzaile bakarra ez erabiltzea da, baizik eta garatzaile bakoitzak bere izena edo izenordaina erabiltzea, jakiteko zehatz-mehatz nork egin duen zer. Oraingo metodoarekin, talde guztiak dauka erantzukizuna, eta ez da maila pertsonalera heltzen.

Eranskinak

A Kodifikazio manuala

A.1 Sarrera

Kodea idazteko momentuan, kontuan izan behar dugu kodea ahal den ulergarriena egin behar dela. Kontura gaitezen, kodea irakurterreza bada lenguai horretan jakintza daukan edonor ulertu eta aldatu dezakela kodea edo programa hobetzeko asmoz. Lenguai bakoitzak arau ezberdinak izango ditu bere beharretara moldatuz. Gure kasuan, Java lenguaiko kodifikazio manual bat daukagu honek behar dituen atal ezberdinekin.

A.2 Fitxategien estruktura

.java bakoitzak public class edo interface bat eduki behar du gutxienez. Fitxategi bakoitzeko elementu ezberdinak hurrengoko ordena izan beharko du:

- Hasierako komentario bat
  - Modifikazio data,bertsioa, lizentzia, klase izena...
- Definitu erabili beharreko paketeak
- Erabiliko diren import-en deklarazioa
- Klase komentarioa javadoc-a sortzeko komentarioa
- Klasea
  - Aldagaiak: Sarrera modifikatzailea erabilita ordenatuta, public, protected, modifikatzaile gabe eta private.
  - Konstruktoreak
  - Metodoak: Funtzionalitatearen arabera batuta.

A.3 Koska(tabulazioak)

Proeiktua tabulatzeko orduan norma batzuk erabili behar dira kodea irakurterreza izan dadin.

- Tabulazio batek 4 espazio izan behar ditu
- Lerro bakoitzak gehienez 80 karaktere.
- Lerroak mozteko momentuan
  - Beti koma bat, operadore bat eta antzeko elementuen ostean egin daiteke
  - Lerro berria aurreko lerroarekin alineatu behar da
  - Nibel altuan moztu

A.4 Komentarioak

Komentarioak egiteko momentuan bi komentario mota ezberdin erabi ditzakegu:

- Inplementazio komentarioak
  - /*...*/ edo //
  - Funtzio baten barruan badago ingurunearekin alineatu behar da ulergarria izan dadin.
  - Komnetaio batek linea bat baino gehiago badu bloke komentarioa izan behar du.
  - Kode erdian komentario bat jartzerako orduan, aurretik lerro huts bat eduki behar du.
- Dokumentazio komentarioak
  - /**...*/ erabiliz sortzen dira komentario hauek
  - Javadoc-en estiloa jarraituz

A.5 Deklarazioak

- Aldagaiak
  - Linea bakoitzeko aldagai deklarazio bakar bat egotea gomendagarria da.
  - Ez jarri lerro batean mota desberdinako bi aldagai.
  - Aldagai lokalak deklaratzen diren lekuan hasieratu.
  - Deklarazioak bloke hasieretan egin behar dira, ezepzio batekin, bukleak.
  - Nibel altuko aldagaiak ez berrizendatu.
- Metodo eta klaseak
  - Metodo baten izena eta bere parametroa listaren hasierako parentesiaren artean ez da espaziorik egongo
  - Giltza zabaltzerakoan, deklarazioaren lerro berdinean egingo da.
  - Giltza ixtean zabaltzen den lerroaren tabulazio berdina izango du.
  - Giltza ixtea lerro berri batean egingo da, lerro bateko metodotan izan ezik.
  - Metodoen artean lerro huts bat egongo da.

A.6 Instrukzioak

- Lerro bakoitzak instrukzio bakarra izango du.
- Bloke berri bat zabaltzean, aurreko instrukzioa baino tabulazio bat gehiago izango du.
- Giltzak beti sartzen dira, lerro bateko if-else-tan ere bai.

- Return batek, ez du parentesirik edukiko beharrezkoak ez badira.
- Ezin dira hiru for, while... baino gehiago egongo bata bestearen barruan.
- Ezin dira bost if baino gehiago egon bata bestearen barruan.
- Metodo batek ez du pantaila bat baino gehiago okupatuko

A.7 Errore tratamendua

- Ahal den heinean errorea berriro bota mezu esanguratsu batekin.
- Ezepzio berriak sortzea ekidin behar da.
- Errore tratamendua ahal den nibelik altuenean egin(main-a)

A.8 Izendapen konbetzioak

- Paketeak
  - Nibel altuko domeinu bat punto batez, empresako izenarekin banatu behar da adb: domeinu.empresa.
- Klaseak eta interfazeak
  - Maiuskulaz hasten dira eta hitz bat baino gehiagoz osatuta badago hitz guztien lehen letra maiuskulaz egongo da.
  - Izen simple eta esanguratsua izan behar dute.
  - Beti hitza osorik idatzi behar da, ez laburbildu oso ezaguna ez bada.
- Metodoak
  - Metoroaren izena minuskulaz hasi beharko da eta hitz bat baino gehiagoz osatuta badago, beste hitzen izenak maiuskulaz hasi beharko dira.
- Aldagaiak
  - Izen motzak eta esanguratsuak izan behar dute minuskulaz hasi beharko da eta hitz bat baino gehiagoz osatuta badago, beste hitzen izenak maiuskulaz hasi beharko dira.
  - Letra bateko aldagaiak ekidin, aldagai tenporalak ez badira.
- Konstanteak
  - Izen esanguratsua eta dena maiuskulaz, hitzak _ batekin banatuz.

A.9 Praktika Onak

- Klase edo aldagai bat ez deklaratu public moduan arrazoi on bat izan gabe.
- Ez erabili objetu bat funtzio estatikoak erabiltzeko.
- Ez erabili zenbakiak kodean zehar, konstanteak erabili.
- Adierazpen konplikatuetan parentesiak erabili.

B Fortigate Firewall-aren konfigurazioa

Jarraian dago idatzirik, Fortigate firewall eta VPN-aren konfigurazio osoa.

```
#config-version=FGT60B-3.00-FW-build670-080729:opmode=0:vdom=0:user=admin
#conf_file_ver=16784395341234991495
#buildno=0670
config system global
    set access-banner disable
    set admin-https-pki-required disable
    set admin-lockout-duration 60
    set admin-lockout-threshold 3
    set admin-maintainer enable
    set admin-port 80
    set admin-scp disable
    set admin-server-cert "Fortinet_Factory"
    set admin-sport 443
    set admin-ssh-port 22
    set admin-ssh-v1 disable
    set admin-telnet-port 23
    set admintimeout 5
    set allow-interface-subnet-overlap disable
    set auth-cert "self-sign"
    set auth-http-port 1000
    set auth-https-port 1003
    set auth-keepalive disable
    set batch-cmdb enable
    set cfg-save automatic
    set check-reset-range disable
    set clt-cert-req disable
    set conn-tracking enable
    set daily-restart disable
    set detection-summary enable
    set dst disable
    set failtime 5
    set fds-statistics enable
    set fsae-burst-size 300
```

```
34      set fsae-rate-limit 100
35      set gui-ipv6 disable
36      set gui-lines-per-page 50
37      set hostname "FGT60B3909602556"
38      set http-obfuscate modified
39      set ie6workaround disable
40      set internal-switch-mode switch
41      set interval 5
42      set ip-src-port-range 1024-25000
43      set language english
44      set ldapconntimeout 500
45      set loglocaldeny disable
46      set management-vdom "root"
47      set ntpserver "pool.ntp.org"
48      set ntpsync disable
49      set phase1-rekey enable
50      set radius-port 1812
51      set refresh 0
52      set remoteauthtimeout 5
53      set reset-sessionless-tcp disable
54      set sslvpn-sport 10443
55      set strong-crypto disable
56      set syncinterval 60
57      set tcp-halfclose-timer 120
58      set tcp-halfopen-timer 60
59      set tcp-option enable
60      set tcp-timewait-timer 120
61      set timezone 04
62      set tos-based-priority high
63      set udp-idle-timer 180
64      set user-server-cert "Fortinet_Factory"
65      set vdom-admin disable
66      set vip-arp-range restricted
67      set fds-statistics-period 60
68  end
69  config system accprofile
70      edit "prof_admin"
71          set admingrp read-write
72          set authgrp read-write
73          set avgrp read-write
74          set fwgrp read-write
75          set imp2pgrp read-write
76          set ipsgrp read-write
77          set loggrp read-write
78          set mntgrp read-write
79          set netgrp read-write
```

```
80            set routegrp read-write
81            set spamgrp read-write
82            set sysgrp read-write
83            set updategrp read-write
84            set vpngrp read-write
85            set webgrp read-write
86        next
87    end
88    config system interface
89        edit "wan1"
90            set vdom "root"
91            set ip 220.100.65.1 255.255.255.0
92            set allowaccess ping https
93            set type physical
94        next
95        edit "modem"
96        next
97        edit "ssl.root"
98            set vdom "root"
99            set type tunnel
100       next
101       edit "wan2"
102           set vdom "root"
103           set allowaccess ping
104           set type physical
105       next
106       edit "dmz"
107           set vdom "root"
108           set ip 10.10.10.1 255.255.255.0
109           set allowaccess ping
110           set type physical
111       next
112       edit "internal"
113           set vdom "root"
114           set ip 192.168.1.99 255.255.255.0
115           set allowaccess ping https ssh
116           set type physical
117       next
118   end
119   config system admin
120       edit "admin"
121           set accprofile "super_admin"
122           set vdom "root"
123               config dashboard
124                   edit "sysinfo"
125                       set column 1
```

```
126                     next
127                     edit "licinfo"
128                         set column 1
129                     next
130                     edit "jsconsole"
131                         set column 1
132                     next
133                     edit "sysres"
134                         set column 1
135                         set show-fds-chart enable
136                         set show-fortianalyzer-chart enable
137                     next
138                     edit "sysop"
139                         set column 2
140                     next
141                     edit "alert"
142                         set column 2
143                         set show-conserve-mode enable
144                         set show-firmware-change enable
145                         set show-system-restart enable
146                     next
147                     edit "statistics"
148                         set column 2
149                     next
150                 end
151     next
152 end
153 config system ha
154     set group-id 0
155     set group-name "FGT-HA"
156     set mode standalone
157     set password ENC 81
          raSMH3WeKuQrYVEHy1HkkkzqLuqt7xLzoZOZo55CV1iyND0XbJagt9UrrEu54clagfnnr
          +zs7PSCCPDBqgzZrwri8hjPaFv
158     set hbdev "dmz" 50 "wan1" 50
159     set route-ttl 10
160     set route-wait 0
161     set route-hold 10
162     set sync-config enable
163     set encryption disable
164     set authentication disable
165     set hb-interval 2
166     set hb-lost-threshold 6
167     set helo-holddown 20
168     set arps 5
169     set arps-interval 8
```

```
170     set session-pickup disable
171     set link-failed-signal disable
172     set uninterruptable-upgrade enable
173     set vcluster2 disable
174     set override disable
175     set priority 128
176     set pingserver-failover-threshold 0
177     set pingserver-flip-timeout 60
178 end
179 config system dns
180     set primary 65.39.139.53
181     set secondary 65.39.139.63
182     set domain ''
183     set autosvr enable
184     set fwdintf "internal"
185     set dns-cache-limit 5000
186     set cache-notfound-responses disable
187 end
188 config system replacemsg mail "email-block"
189     set buffer "Potentially Dangerous Attachment Removed. The
        file \"%%FILE%%\" has been blocked. File quarantined as:
        \"%%QUARFILENAME%%\"."
190     set format text
191     set header 8bit
192 end
193 config system replacemsg mail "email-virus"
194     set buffer "Dangerous Attachment has been Removed. The file
        \"%%FILE%%\" has been removed because of a virus. It
        was infected with the \"%%VIRUS%%\" virus. File
        quarantined as: \"%%QUARFILENAME%%\"."
195     set format text
196     set header 8bit
197 end
198 config system replacemsg mail "email-filesize"
199     set buffer "This email has been blocked. The email message
        is larger than the configured file size limit."
200     set format text
201     set header 8bit
202 end
203 config system replacemsg mail "partial"
204     set buffer "Fragmented emails are blocked."
205     set format text
206     set header 8bit
207 end
208 config system replacemsg mail "smtp-block"
209     set buffer "The file %%FILE%% has been blocked. File
```

```
        quarantined as: %%QUARFILENAME%%"
    set format text
    set header none
end
config system replacemsg mail "smtp-virus"
    set buffer "The file %%FILE%% has been infected with the
        virus %%VIRUS%% File quarantined as %%QUARFILENAME%%"
    set format text
    set header none
end
config system replacemsg mail "smtp-filesize"
    set buffer "This message is larger than the configured limit
        and has been blocked."
    set format text
    set header none
end
config system replacemsg http "bannedword"
    set buffer "<HTML><BODY>The page you requested has been
        blocked because it contains a banned word. URL = http
        ://%%URL%%</BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "url-block"
    set buffer "<HTML><BODY>The URL you requested has been
        blocked. URL = %%URL%%</BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "infcache-block"
    set buffer "<HTML><BODY><H2>High security alert!!!</h2><p>
        The URL you requested was previously found to be infected
        .</p><p>URL = http://%%URL%%</p></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "http-block"
    set buffer "<HTML> <BODY> <h2>High security alert!!!</h2> <p
        >You are not permitted to download the file \"%%FILE
        %%\".</p> <p>URL = http://%%URL%%</p> </BODY> </HTML>"
    set format html
    set header http
end
config system replacemsg http "http-virus"
    set buffer "<HTML><BODY><h2>High security alert!!!</h2><p>
        You are not permitted to download the file \"%%FILE%%\"
```

```
        because it is infected with the virus \"%%VIRUS%%\". </p
        ><p>URL = http://%%URL%%</p><p>File quarantined as: %%
        QUARFILENAME%%.</p></BODY></HTML>"
245     set format html
246     set header http
247 end
248 config system replacemsg http "http-filesize"
249     set buffer "<HTML><BODY>  <h2>Attention!!!</h2><p>The file
        \"%%FILE%%\" has been blocked.  The file is larger than
        the configured file size limit.</p> <p>URL = http://%%URL
        %%</p> </BODY></HTML>"
250     set format html
251     set header http
252 end
253 config system replacemsg http "http-client-block"
254     set buffer "<HTML> <BODY> <h2>High security alert!!!</h2> <p
        >You are not permitted to upload the file \"%%FILE%%\".</
        p> <p>URL = http://%%URL%%</p> </BODY> </HTML>"
255     set format html
256     set header http
257 end
258 config system replacemsg http "http-client-virus"
259     set buffer "<HTML><BODY><h2>High security alert!!!</h2><p>
        You are not permitted to upload the file \"%%FILE%%\"
        because it is infected with the virus \"%%VIRUS%%\". </p
        ><p>URL = http://%%URL%%</p><p>File quarantined as: %%
        QUARFILENAME%%.</p></BODY></HTML>"
260     set format html
261     set header http
262 end
263 config system replacemsg http "http-client-filesize"
264     set buffer "<HTML><BODY>  <h2>Attention!!!</h2><p>Your
        request has been blocked.  The request is larger than the
        configured file size limit.</p> <p>URL = http://%%URL
        %%</p> </BODY></HTML>"
265     set format html
266     set header http
267 end
268 config system replacemsg http "http-client-bannedword"
269     set buffer "<HTML><BODY>The page you uploaded has been
        blocked because it contains a banned word. URL = http
        ://%%URL%%</BODY></HTML>"
270     set format html
271     set header http
272 end
273 config system replacemsg ftp "ftp-dl-infected"
```

```
274     set buffer "Transfer failed.  The file %%FILE%% is infected
            with the virus %%VIRUS%%. File quarantined as %%
            QUARFILENAME%%."
275     set format text
276     set header none
277 end
278 config system replacemsg ftp "ftp-dl-blocked"
279     set buffer "Transfer failed.  You are not permitted to
            transfer the file \"%%FILE%%\"."
280     set format text
281     set header none
282 end
283 config system replacemsg ftp "ftp-dl-filesize"
284     set buffer "File size limit exceeded."
285     set format text
286     set header none
287 end
288 config system replacemsg nntp "nntp-dl-infected"
289     set buffer "Dangerous Attachment has been Removed.  The file
            \"%%FILE%%\" has been removed because of a virus.  It
            was infected with the \"%%VIRUS%%\" virus.  File
            quarantined as: \"%%QUARFILENAME%%\"."
290     set format text
291     set header none
292 end
293 config system replacemsg nntp "nntp-dl-blocked"
294     set buffer "The file %%FILE%% has been blocked. File
            quarantined as: %%QUARFILENAME%%"
295     set format text
296     set header none
297 end
298 config system replacemsg nntp "nntp-dl-filesize"
299     set buffer "This article has been blocked.  The article is
            larger than the configured file size limit."
300     set format text
301     set header none
302 end
303 config system replacemsg alertmail "alertmail-virus"
304     set buffer "Virus/Worm detected: %%VIRUS%% Protocol: %%
            PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %%
            DEST_IP%% Email Address From: %%EMAIL_FROM%% Email
            Address To: %%EMAIL_TO%% "
305     set format text
306     set header none
307 end
308 config system replacemsg alertmail "alertmail-block"
```

```
309     set buffer "File Block Detected: %%FILE%% Protocol: %%
            PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %%
            DEST_IP%% Email Address From: %%EMAIL_FROM%% Email
            Address To: %%EMAIL_TO%%"
310     set format text
311     set header none
312 end
313 config system replacemsg alertmail "alertmail-nids-event"
314     set buffer "The following intrusion was observed: %%
            NIDS_EVENT%%."
315     set format text
316     set header none
317 end
318 config system replacemsg alertmail "alertmail-crit-event"
319     set buffer "The following critical firewall event was
            detected: %%CRITICAL_EVENT%%."
320     set format text
321     set header none
322 end
323 config system replacemsg alertmail "alertmail-disk-full"
324     set buffer "The log disk is Full."
325     set format text
326     set header none
327 end
328 config system replacemsg fortiguard-wf "ftgd-block"
329     set buffer "<html><head><title>Web Filter Violation</title
            ></head><body><font size=2><table width=\"100%\"><tr><td
            >%%FORTIGUARD_WF%%</td><td align=\"right\">%%FORTINET%%</
            td></tr><tr><td bgcolor=#ff6600 align=\"center\" colspan
            =2><font color=#ffffff><b>Web Page Blocked</b></font></td
            ></tr></table><br><br>You have tried to access a web page
            which is in violation of your internet usage policy.<br
            ><br>URL: %%URL%%<br>Category: %%CATEGORY%%<br
            ><br>To have the rating of this web page re-evaluated <u
            ><a href=\"%%FTGD_RE_EVAL%%\">please click here</a></u>.<
            br>%%OVERRIDE%%<br><hr><br>Powered by %%SERVICE%%.</font
            ></body></html>"
330     set format html
331     set header http
332 end
333 config system replacemsg fortiguard-wf "http-err"
334     set buffer "<html><head><title>%%HTTP_ERR_CODE%% %%
            HTTP_ERR_DESC%%</title></head><body><font size=2><table
            width=\"100%\"><tr><td>%%FORTIGUARD_WF%%</td><td align=\"
            right\">%%FORTINET%%</td></tr><tr><td bgcolor=#3300cc
            align=\"center\" colspan=2><font color=#ffffff><b>%%
```

```
        HTTP_ERR_CODE%% %%HTTP_ERR_DESC%%</b></font></td></tr></
        table><br><br>The webserver for %%URL%% reported that an
        error occurred while trying to access the website.   
        Please click <u><a onclick=\"history.back()\">here</a></u
        > to return to the previous page.<br><br><hr><br>Powered
        by %%SERVICE%%.</font></body></html>"
335     set format html
336     set header http
337 end
338 config system replacemsg fortiguard-wf "ftgd-ovrd"
339     set buffer "<html><head><title>Web Filter Block Override</
        title></head><body><font size=2><table width=\"100%\"><tr
        ><td>%%FORTIGUARD_WF%%</td><td align=\"right\">%%FORTINET
        %%</td></tr><tr><td bgcolor=#3300cc align=\"center\"
        colspan=2><font color=#ffffff><b>Web Filter Block
        Override</b></font></td></tr><tr><td colspan=2><br><br>If
        you have been granted override creation privileges by
        your administrator, you can enter your username and
        password here to gain immediate access to the blocked web
        -page.   If you do not have these privileges, please
        contact your administrator to gain access to the web-page
        .<br><br></td></tr><tr><td align=\"center\" colspan=2>%%
        OVRD_FORM%%</td></tr></table><br><br><hr><br>Powered by
        %%SERVICE%%.</font></body></html>"
340     set format html
341     set header http
342 end
343 config system replacemsg spam "ipblocklist"
344     set buffer "Mail from this IP address is not allowed and has
        been blocked."
345     set format text
346     set header none
347 end
348 config system replacemsg spam "smtp-spam-dnsbl"
349     set buffer "This message has been blocked because it is from
        a DNSBL/ORDBL IP address."
350     set format text
351     set header none
352 end
353 config system replacemsg spam "smtp-spam-feip"
354     set buffer "This message has been blocked because it is from
        a FortiGuard - AntiSpam black IP address."
355     set format text
356     set header none
357 end
358 config system replacemsg spam "smtp-spam-helo"
```

```
359     set buffer "This message has been blocked because the HELO/
            EHLO domain is invalid."
360     set format text
361     set header none
362 end
363 config system replacemsg spam "smtp-spam-emailblack"
364     set buffer "Mail from this email address is not allowed and
            has been blocked."
365     set format text
366     set header none
367 end
368 config system replacemsg spam "smtp-spam-mimeheader"
369     set buffer "This message has been blocked because it
            contains an invalid header."
370     set format text
371     set header none
372 end
373 config system replacemsg spam "reversedns"
374     set buffer "This message has been blocked because the return
            email domain is invalid."
375     set format text
376     set header none
377 end
378 config system replacemsg spam "smtp-spam-bannedword"
379     set buffer "This message has been blocked because it
            contains a banned word."
380     set format text
381     set header none
382 end
383 config system replacemsg spam "smtp-spam-fsurl"
384     set buffer "This message has been blocked because it
            contains FortiGuard - AntiSpam blocking URL(s)."
385     set format text
386     set header none
387 end
388 config system replacemsg spam "smtp-spam-fschksum"
389     set buffer "This message has been blocked because its
            checksum is in FortiGuard - AntiSpam checksum blacklist."
390     set format text
391     set header none
392 end
393 config system replacemsg spam "submit"
394     set buffer "If this email is not spam, click here to submit
            the signatures to FortiGuard - AntiSpam Service."
395     set format text
396     set header none
```

```
end
config system replacemsg admin "admin-disclaimer-text"
    set buffer "WARNINGWARNINGWARNINGWARNING
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. All use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
WARNINGWARNINGWARNINGWARNING
"
    set format text
    set header none
end
config system replacemsg auth "auth-disclaimer-page-1"
    set buffer "<HTML><HEAD><TITLE>Firewall Disclaimer</TITLE></
        HEAD><BODY><FORM ACTION=\"/\" method=\"POST\"><INPUT TYPE
        =\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><
        INPUT TYPE=\"hidden\" NAME=\"%%ANSWERID%%\" VALUE=\"%%
        DECLINEVAL%%\"><INPUT TYPE=\"hidden\" NAME=\"%%REDIRID
        %%\" VALUE=\"%%PROTURI%%\"><TABLE ALIGN=\"CENTER\" width
        =400 height=250 cellpadding=2 cellspacing=0 border=0
        bgcolor=\"#008080\"><TR><TD><TABLE border=0 width
        =\"100%\" height=\"100%\" cellpadding=0 cellspacing=0
        bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD
        ><b><font size=2 face=\"Verdana\" color=\"#ffffff\">
        Disclaimer Agreement</font></b></TD><TR><TR height
        =\"100%\"><TD><TABLE border=0 cellpadding=5 cellspacing=0
        width=\"320\" align=center><TR><TD colspan=2><font size
        =2 face=\"Times New Roman\">You are about to access
        Internet content that is not under the control of the
        network access provider. The network access provider is
        therefore not responsible for any of these sites, their
        content or their privacy policies. The network access
        provider and its staff do not endorse nor make any
        representations about these sites, or any information,
        software or other products or materials found there, or
        any results that may be obtained from using them. If you
        decide to access any Internet content, you do this
```

```
        entirely␣at␣your␣own␣risk␣and␣you␣are␣responsible␣for␣
        ensuring␣that␣any␣accessed␣material␣does␣not␣infringe␣the
        ␣laws␣governing,␣but␣not␣exhaustively␣covering,␣copyright
        ,␣trademarks,␣pornography,␣or␣any␣other␣material␣which␣is
        ␣slanderous,␣defamatory␣or␣might␣cause␣offence␣in␣any␣
        other␣way.</font></TD></TR><TR><TD>Do␣you␣agree␣to␣the␣
        above␣terms?</TD></TR><TR><TD><INPUT␣CLASS=\"button\"␣
        TYPE=\"button\"␣VALUE=\"Yes,␣I␣agree\"␣ONCLICK=\"agree()
        \"><INPUT␣CLASS=\"button\"␣TYPE=\"button\"␣VALUE=\"No,␣I␣
        decline\"␣ONCLICK=\"decline()\"></TD></TR></TABLE></TD></
        TR></TABLE></TD></TR></TABLE></FORM><SCRIPT␣LANGUAGE=\"
        JavaScript\">function␣agree(){document.forms[0].%%
        ANSWERID%%.value=\"%%AGREEVAL%%\";document.forms[0].
        submit();}function␣decline(){document.forms[0].submit()
        ;}</SCRIPT></BODY></HTML>"
419     set format html
420     set header http
421 end
422 config system replacemsg auth "auth-disclaimer-page-2"
423     set buffer ''
424     set format html
425     set header http
426 end
427 config system replacemsg auth "auth-disclaimer-page-3"
428     set buffer ''
429     set format html
430     set header http
431 end
432 config system replacemsg auth "auth-reject-page"
433     set buffer "<HTML><HEAD><TITLE>Firewall␣Disclaimer␣Declined
        </TITLE></HEAD><BODY><FORM␣ACTION=\"/\"␣method=\"POST\"><
        INPUT␣TYPE=\"hidden\"␣NAME=\"%%MAGICID%%\"␣VALUE=\"%%
        MAGICVAL%%\"><INPUT␣TYPE=\"hidden\"␣NAME=\"%%REDIRID%%\"␣
        VALUE=\"%%PROTURI%%\"><TABLE␣ALIGN=\"CENTER\"␣width=400␣
        height=250␣cellpadding=2␣cellspacing=0␣border=0␣bgcolor
        =\"#008080\"><TR><TD><TABLE␣border=0␣width=\"100%\"␣
        height=\"100%\"␣cellpadding=0␣cellspacing=0␣bgcolor=\"#9
        dc8c6\"><TR␣height=30␣bgcolor=\"#008080\"><TD><b><font␣
        size=2␣face=\"Verdana\"␣color=\"#ffffff\">Disclaimer␣
        Declined</font></b></TD><TR><TR␣height=\"100%\"><TD><
        TABLE␣border=0␣cellpadding=5␣cellspacing=0␣width=\"320\"␣
        align=center><TR><TD␣colspan=2><font␣size=2␣face=\"Times␣
        New␣Roman\">Sorry,␣network␣access␣cannot␣be␣granted␣
        unless␣you␣agree␣to␣the␣disclaimer.</font></TD><TR><TR><
        TD></TD><TD><INPUT␣TYPE=\"submit\"␣VALUE=\"Return␣to␣
        Disclaimer\"></TD></TR></TABLE></TD></TR></TABLE></TD></
```

```
        TR></TABLE></FORM></BODY></HTML>"
434     set format html
435     set header http
436 end
437 config system replacemsg auth "auth-login-page"
438     set buffer "<HTML><HEAD><TITLE>Firewall Authentication</
        TITLE></HEAD><BODY><FORM ACTION=\"/\" method=\"POST\"><
        INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%
        MAGICVAL%%\"><TABLE ALIGN=\"CENTER\" width=400 height=250
        cellpadding=2 cellspacing=0 border=0 bgcolor
        =\"#008080\"><TR><TD><TABLE border=0 cellpadding=0
        cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor
        =\"#008080\"><TD><b><font size=2 face=\"Verdana\" color
        =\"#ffffff\">Authentication Required</font></b></TD></TR
        ><TR><TD><TABLE border=0 cellpadding=5 cellspacing=0
        width=\"320\" align=center><TR><TD colspan=2><font size=2
        face=\"Times New Roman\">%%QUESTION%%</font></TD></TR><
        TR><TD><font size=2 face=\"Times New Roman\">Username:</
        font></TD><TD><INPUT TYPE=\"text\" NAME=\"%%USERNAMEID
        %%\" size=25></TD></TR><TR><TD><font size=2 face=\"Times
        New Roman\">Password:</font></TD><TD><INPUT TYPE=\"
        password\" NAME=\"%%PASSWORDID%%\" size=25></TD></TR><TR
        ><TD><INPUT TYPE=\"hidden\" NAME=\"%%REDIRID%%\" VALUE
        =\"%%PROTURI%%\"><INPUT TYPE=\"submit\" VALUE=\"Continue
        \"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE
        ></FORM></BODY></HTML>"
439     set format html
440     set header http
441 end
442 config system replacemsg auth "auth-login-failed-page"
443     set buffer "<HTML><HEAD><TITLE>Firewall Authentication</
        TITLE></HEAD><BODY><FORM ACTION=\"/\" method=\"POST\"><
        INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%
        MAGICVAL%%\"><TABLE ALIGN=\"CENTER\" width=400 height=250
        cellpadding=2 cellspacing=0 border=0 bgcolor
        =\"#008080\"><TR><TD><TABLE border=0 cellpadding=0
        cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor
        =\"#008080\"><TD><b><font size=2 face=\"Verdana\" color
        =\"#ffffff\">Authentication Failed</font></b></TD></TR><
        TR><TD><TABLE border=0 cellpadding=5 cellspacing=0 width
        =\"320\" align=center><TR><TD colspan=2><font size=2 face
        =\"Times New Roman\">%%FAILED_MESSAGE%%</font></TD></TR><
        TR><TD><font size=2 face=\"Times New Roman\">Username:</
        font></TD><TD><INPUT TYPE=\"text\" NAME=\"%%USERNAMEID
        %%\" size=25></TD></TR><TR><TD><font size=2 face=\"Times
        New Roman\">Password:</font></TD><TD><INPUT TYPE=\"
```

```
        password\" NAME=\"%%PASSWORDID%%\" size=25></TD></TR><TR
        ><TD><INPUT TYPE=\"hidden\" NAME=\"%%REDIRID%%\" VALUE
        =\"%%PROTURI%%\"><INPUT TYPE=\"submit\" VALUE=\"Continue
        \"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE
        ></FORM></BODY></HTML>"
444     set format html
445     set header http
446 end
447 config system replacemsg auth "auth-challenge-page"
448     set buffer "<HTML><HEAD><TITLE>Firewall Authentication</
        TITLE></HEAD><BODY><FORM ACTION=\"/\" method=\"POST\"><
        INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%
        MAGICVAL%%\"><TABLE ALIGN=\"CENTER\" width=400 height=250
        cellpadding=2 cellspacing=0 border=0 bgcolor
        =\"#008080\"><TR><TD><TABLE border=0 cellpadding=0
        cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor
        =\"#008080\"><TD><b><font size=2 face=\"Verdana\" color
        =\"#ffffff\">Authentication Required</font></b></TD></TR
        ><TR><TD><TABLE border=0 cellpadding=5 cellspacing=0
        width=\"320\" align=center><TR><TD colspan=2><font size=2
        face=\"Times New Roman\">%%QUESTION%%</font></TD></TR><
        TR><TD><font size=2 face=\"Times New Roman\">Answer:</
        font></TD><TD><INPUT TYPE=\"password\" NAME=\"%%
        PASSWORDID%%\" size=25></TD></TR><TR><TD><INPUT TYPE=\"
        hidden\" NAME=\"%%USERNAMEID%%\" VALUE=\"%%USERNAMEVAL
        %%\"><INPUT TYPE=\"hidden\" NAME=\"%%REQUESTID%%\" VALUE
        =\"%%REQUESTVAL%%\"><INPUT TYPE=\"hidden\" NAME=\"%%
        REDIRID%%\" VALUE=\"%%PROTURI%%\"><INPUT TYPE=\"hidden\"
        NAME=\"%%USERGROUPID%%\" VALUE=\"%%USERGROUPVAL%%\"><
        INPUT TYPE=\"submit\" VALUE=\"Continue\"></TD></TR></
        TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM></BODY
        ></HTML>"
449     set format html
450     set header http
451 end
452 config system replacemsg auth "auth-keepalive-page"
453     set buffer "<HTML>
454 <HEAD>
455 <TITLE>Firewall Authentication Keepalive Window</TITLE>
456 </HEAD>
457 <BODY>
458 <SCRIPT LANGUAGE=\"JavaScript\">
459 var countDownTime=%%TIMEOUT%% + 1;
460 function countDown(){
461 countDownTime--;
462 if (countDownTime <= 0){
```

```
463 ␣␣␣␣location.href=\"%%KEEPALIVEURL%%\";
464 ␣␣␣␣return;
465 }
466 document.getElementById(\'countdown\').innerHTML␣=␣countDownTime
    ;
467 counter=setTimeout(\"countDown()\",␣1000);
468 }
469 function␣startit(){
470 ␣␣␣␣countDown();
471 }
472 window.onload=startit
473 </SCRIPT>
474 <table␣width=\"100%\"␣height=\"100%\"><tr><td␣align=\"center\">
475 <H3>This␣browser␣window␣is␣used␣to␣keep␣your␣authentication␣
    session␣active.</H3>
476 <H3>Please␣leave␣it␣open␣in␣the␣background␣and␣open␣a␣<a␣href
    =\"%%AUTH_REDIR_URL%%\"␣target=\"_blank\">new␣window</a>␣to␣
    continue.</H3>
477 <p>Authentication␣Refresh␣in␣<b␣id=countdown>%%TIMEOUT%%</b>␣
    seconds</p>
478 <p><a␣href=\"%%AUTH_LOGOUT%%\">logout</a></p>
479 </td></tr></table>
480 </BODY>
481 </HTML>
482 "
483     set format html
484     set header http
485 end
486 config system replacemsg im "im-file-xfer-block"
487     set buffer "Transfer␣failed.␣␣You␣are␣not␣permitted␣to␣
        transfer␣the␣file␣\"%%FILE%%\"."
488     set format text
489     set header none
490 end
491 config system replacemsg im "im-file-xfer-name"
492     set buffer "Transfer␣%%ACTION%%.␣␣The␣file␣name␣\"%%FILE%%\"
        ␣matches␣the␣configured␣file␣name␣block␣list."
493     set format text
494     set header none
495 end
496 config system replacemsg im "im-file-xfer-infected"
497     set buffer "Transfer␣%%ACTION%%.␣␣The␣file␣\"%%FILE%%\"␣is␣
        infected␣with␣the␣virus␣%%VIRUS%%.␣␣File␣quarantined␣as␣
        %%QUARFILENAME%%."
498     set format text
499     set header none
```

```
end
config system replacemsg im "im-file-xfer-size"
    set buffer "Transfer %%ACTION%%.  The file \"%%FILE%%\" is
        larger than the configured limit."
    set format text
    set header none
end
config system replacemsg im "im-voice-chat-block"
    set buffer "Connection failed.  You are not permitted to use
        voice chat."
    set format text
    set header none
end
config system replacemsg im "im-photo-share-block"
    set buffer "Photo sharing failed.  You are not permitted to
        share photo."
    set format text
    set header none
end
config system replacemsg im "im-long-chat-block"
    set buffer "Message blocked.  The message is longer than the
        configured limit."
    set format text
    set header none
end
config system replacemsg sslvpn "sslvpn-login"
    set buffer "<html><head><title>login</title><meta http-equiv
        =\"Pragma\" content=\"no-cache\"><meta http-equiv=\"cache
        -control\" content=\"no-cache\"><meta http-equiv=\"cache-
        control\" content=\"must-revalidate\"><link href=\"/
        ssl_style.css\" rel=\"stylesheet\" type=\"text/css\"><
        script language=\"JavaScript\"><!--if (top && top.
        location != window.location) top.location = top.location;
        if (window.opener && window.opener.top) { window.opener.
        top.location = window.opener.top.location; self.close(); }
        }//--></script></head><body class=\"main\"><center><table
        width=\"100%\" height=\"100%\" align=\"center\" class=\"
        container\" valign=\"middle\" cellpadding=\"0\"
        cellspacing=\"0\"><tr valign=middle><td><form action=\"%%
        SSL_ACT%%\" method=\"%%SSL_METHOD%%\" name=\"f\"><table
        class=\"list\" cellpadding=10 cellspacing=0 align=center
        width=400 height=180>%%SSL_LOGIN%%</table>%%SSL_HIDDEN
        %%</td></tr></table></form></center></body><script>
        document.forms[0].username.focus();</script></html>"
    set format html
    set header http
```

```
end
config vpn certificate ca
end
config vpn certificate local
end
config gui console
    unset preferences
end
config system session-helper
    edit 1
        set name pptp
        set port 1723
        set protocol 6
    next
    edit 2
        set name h323
        set port 1720
        set protocol 6
    next
    edit 3
        set name ras
        set port 1719
        set protocol 17
    next
    edit 4
        set name tns
        set port 1521
        set protocol 6
    next
    edit 5
        set name tftp
        set port 69
        set protocol 17
    next
    edit 6
        set name rtsp
        set port 554
        set protocol 6
    next
    edit 7
        set name rtsp
        set port 7070
        set protocol 6
    next
    edit 8
        set name ftp
```

```
571             set port 21
572             set protocol 6
573         next
574         edit 9
575             set name mms
576             set port 1863
577             set protocol 6
578         next
579         edit 10
580             set name pmap
581             set port 111
582             set protocol 6
583         next
584         edit 11
585             set name pmap
586             set port 111
587             set protocol 17
588         next
589         edit 12
590             set name sip
591             set port 5060
592             set protocol 17
593         next
594         edit 13
595             set name dns-udp
596             set port 53
597             set protocol 17
598         next
599         edit 14
600             set name rsh
601             set port 514
602             set protocol 6
603         next
604         edit 15
605             set name rsh
606             set port 512
607             set protocol 6
608         next
609         edit 16
610             set name dcerpc
611             set port 135
612             set protocol 6
613         next
614         edit 17
615             set name dcerpc
616             set port 135
```

```
617             set protocol 17
618         next
619         edit 18
620             set name mgcp
621             set port 2427
622             set protocol 17
623         next
624         edit 19
625             set name mgcp
626             set port 2727
627             set protocol 17
628         next
629 end
630 config system auto-install
631         set auto-install-config enable
632         set auto-install-image enable
633         set default-config-file "fgt_system.conf"
634         set default-image-file "image.out"
635 end
636 config system console
637         set mode line
638         set output more
639 end
640 config antivirus service "http"
641         set port 80
642         set scan-bzip2 disable
643         set uncompnestlimit 12
644         set uncompsizelimit 10
645 end
646 config antivirus service "https"
647         set port 443
648         set scan-bzip2 disable
649         set uncompnestlimit 0
650         set uncompsizelimit 0
651 end
652 config antivirus service "ftp"
653         set port 21
654         set scan-bzip2 disable
655         set uncompnestlimit 12
656         set uncompsizelimit 10
657 end
658 config antivirus service "pop3"
659         set port 110
660         set scan-bzip2 disable
661         set uncompnestlimit 12
662         set uncompsizelimit 10
```

```
end
config antivirus service "imap"
    set port 143
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "smtp"
    set port 25
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "nntp"
    set port 119
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "im"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus grayware "Adware"
end
config antivirus grayware "Dial"
end
config antivirus grayware "Game"
end
config antivirus grayware "Joke"
end
config antivirus grayware "P2P"
end
config antivirus grayware "Spy"
end
config antivirus grayware "Keylog"
end
config antivirus grayware "Hijacker"
end
config antivirus grayware "Plugin"
end
config antivirus grayware "NMT"
end
config antivirus grayware "RAT"
end
```

```
config antivirus grayware "Misc"
end
config antivirus grayware "BHO"
end
config antivirus grayware "Toolbar"
end
config antivirus grayware "Download"
end
config antivirus grayware "HackerTool"
end
config system dhcp server
    edit "internal_dhcp_server"
        set default-gateway 192.168.1.99
        set dns-server1 192.168.1.99
        set end-ip 192.168.1.210
        set interface "internal"
        set netmask 255.255.255.0
        set start-ip 192.168.1.110
    next
end
config firewall address
    edit "all"
    next
    edit "Finance"
        set type iprange
        set end-ip 192.168.1.20
        set start-ip 192.168.1.10
    next
    edit "Eng"
        set type iprange
        set end-ip 192.168.1.90
        set start-ip 192.168.1.51
    next
    edit "Help_Desk"
        set type iprange
        set end-ip 192.168.1.49
        set start-ip 192.168.1.21
    next
    edit "DMZ_network"
        set associated-interface "dmz"
        set subnet 10.10.10.0 255.255.255.0
    next
    edit "Tech_support_1"
        set subnet 220.100.65.98 255.255.255.255
    next
end
```

```
config firewall addrgrp
    edit "FinEng"
            set member "Eng" "Finance"
    next
end
config ips sensor
    edit "all_default"
        set comment "all predefined signatures with default setting"
            config filter
                edit "1"
                next
            end
    next
    edit "all_default_pass"
        set comment "all predefined signatures with PASS action"
            config filter
                edit "1"
                    set action pass
                next
            end
    next
    edit "protect_http_server"
        set comment "protect against HTTP server-side vulnerabilities"
            config filter
                edit "1"
                    set location server
                    set protocol HTTP
                next
            end
    next
    edit "protect_email_server"
        set comment "protect against EMail server-side vulnerabilities"
            config filter
                edit "1"
                    set location server
                    set protocol SMTP POP3 IMAP
                next
            end
    next
    edit "protect_client"
        set comment "protect against client-side vulnerabilities"
            config filter
```

```
797                 edit "1"
798                     set location client
799                 next
800             end
801     next
802 end
803 config firewall profile
804     edit "strict"
805         set log-web-ftgd-err enable
806         set ftp block oversize scan splice scanextended
807         set http block oversize scan activexfilter bannedword
               cookiefilter javafilter rangeblock urlfilter
               scanextended
808         unset https
809         set imap block oversize scan bannedword spamemailbwl
               spamfsip spamfschksum spamfssubmit spamfsurl
               spamhdrcheck spamraddrdns scanextended
810         set pop3 block oversize scan bannedword spamemailbwl
               spamfsip spamfschksum spamfssubmit spamfsurl
               spamhdrcheck spamraddrdns scanextended
811         set smtp block oversize scan bannedword spamemailbwl
               spamfsip spamfschksum spamfssubmit spamfsurl
               spamhdrcheck spamhelodns spamipbwl spamraddrdns
               spamrbl splice scanextended
812         set nntp block oversize scan scanextended
813         set im block oversize scan scanextended
814         set ftgd-wf-options strict-blocking
815         set ftgd-wf-https-options strict-blocking
816     next
817     edit "scan"
818         set log-web-ftgd-err enable
819         set ftp scan splice
820         set http scan rangeblock
821         unset https
822         set imap scan
823         set pop3 scan
824         set smtp scan splice
825         set nntp scan
826         set im scan
827         set ftgd-wf-options strict-blocking
828         set ftgd-wf-https-options strict-blocking
829     next
830     edit "web"
831         set log-web-ftgd-err enable
832         set ftp splice
833         set http scan bannedword rangeblock urlfilter
```

```
834             unset https
835             set imap fragmail
836             set pop3 fragmail
837             set smtp fragmail splice
838             unset nntp
839             unset im
840             set ftgd-wf-options strict-blocking
841             set ftgd-wf-https-options strict-blocking
842         next
843         edit "unfiltered"
844             set log-web-ftgd-err enable
845             set ftp splice
846             set http rangeblock
847             unset https
848             set imap fragmail
849             set pop3 fragmail
850             set smtp fragmail splice
851             unset nntp
852             unset im
853             set ftgd-wf-options strict-blocking
854             set ftgd-wf-https-options strict-blocking
855         next
856         edit "Standard_profile"
857             set log-web-ftgd-err enable
858             set ftp splice
859             set http fortiguard-wf
860             unset https
861             set imap fragmail spamfssubmit
862             set pop3 fragmail spamfssubmit
863             set smtp fragmail spamfssubmit splice
864             set pop3-spamtagtype subject
865             set imap-spamtagtype subject
866             set nntp no-content-summary
867             set ips-sensor-status enable
868             set ips-sensor "all_default"
869             unset im
870             set ftgd-wf-options strict-blocking
871             set ftgd-wf-https-options strict-blocking
872             set ftgd-wf-allow 7 9 11 13 15 16 63 64 65 66 67 17 18
                    19 23 68 69 70 71 28 29 30 31 32 33 35 36 38 39 40 41
                     43 44 46 47 48 77 78 79 80 g07 g08 g21 g22 c01 c02
                    c03 c04 c05 c06
873             set ftgd-wf-deny g01 8 12 14 20 g04 g05 34 37 42
874         next
875         edit "Help_Desk_work"
876             set log-web-ftgd-err enable
```

```
877         set ftp splice
878         set http bannedword exemptword urlfilter
879         set https urlfilter
880         set imap fragmail spamfssubmit
881         set pop3 fragmail spamfssubmit
882         set smtp fragmail spamfssubmit splice
883         set pop3-spamtagtype subject
884         set imap-spamtagtype subject
885         set weburlfiltertable 2
886         set nntp no-content-summary
887         set ips-sensor-status enable
888         set ips-sensor "all_default"
889         unset im
890         set aim enable-inspect block-im
891         set icq enable-inspect block-im
892         set msn enable-inspect block-im
893         set yahoo enable-inspect block-im
894             config simple
895                 set status enable
896                 set block-message enable
897             end
898         set p2p enable
899         set bittorrent block
900         set edonkey block
901         set gnutella block
902         set kazaa block
903         set winny block
904         set skype block
905         set ftgd-wf-options strict-blocking
906         set ftgd-wf-https-options strict-blocking
907     next
908     edit "Help_Desk_lunch"
909         set log-web-ftgd-err enable
910         set ftp splice
911         unset http
912         unset https
913         set imap fragmail spamfssubmit
914         set pop3 fragmail spamfssubmit
915         set smtp fragmail spamfssubmit splice
916         set pop3-spamtagtype subject
917         set imap-spamtagtype subject
918         set nntp no-content-summary
919         set ips-sensor-status enable
920         set ips-sensor "all_default"
921         unset im
922         set aim enable-inspect block-im
```

```
923             set icq enable-inspect block-im
924             set msn enable-inspect block-im
925             set yahoo enable-inspect block-im
926                 config simple
927                     set status enable
928                     set block-message enable
929                 end
930             set p2p enable
931             set bittorrent block
932             set edonkey block
933             set gnutella block
934             set kazaa block
935             set winny block
936             set skype block
937             set ftgd-wf-options strict-blocking
938             set ftgd-wf-https-options strict-blocking
939             set ftgd-wf-allow 17 18 19 23 68 69 70 71 28 29 30 31 32
                    33 35 36 38 39 40 41 43 44 46 47 77 78 79 80 g07 g08
                    g21 g22 c01 c02 c03 c04 c05 c06
940             set ftgd-wf-deny g01 g02 20 g04 g05 34 37 42 48
941         next
942     end
943     config webfilter bword
944     end
945     config webfilter exmword
946     end
947     config webfilter urlfilter
948         edit 1
949                 config entries
950                     edit ".*"
951                         set action block
952                         set type regex
953                     next
954                 end
955             set name "CompanyA_Blocked_URLs"
956         next
957         edit 2
958                 config entries
959                     edit "www.mondragon.edu"
960                     next
961                     edit ".*"
962                         set action block
963                         set type regex
964                     next
965                 end
966             set name "CompanyA_Support"
```

```
967         next
968     end
969     config webfilter ftgd-ovrd
970     end
971     config webfilter ftgd-ovrd-user
972     end
973     config webfilter ftgd-local-rating
974     end
975     config vpn ipsec phase1
976         edit "Tech_support_1"
977             set interface "wan1"
978             set nattraversal enable
979             set proposal 3des-sha1 3des-md5
980             set remote-gw 220.100.65.98
981             set psksecret ENC QWwcc3jkHGEovDNLwa+
                    kKCCPG3BaAUSI99K4siX5lG3W3ar4EO2x033cC3BaG+NmYfK5+
                    hNWoq+AyvPTgtE8hu6Y4w5yhxJcMoOlDXFrikux86VO
982         next
983         edit "Tech_support_2"
984             set type ddns
985             set interface "wan1"
986             set nattraversal enable
987             set proposal 3des-sha1 3des-md5
988             set remotegw-ddns "techsupport.com"
989             set psksecret ENC
                    P4mEEWxidwfNqB6GpwzyE8BBseMAvbuODV2OejIqCOqvxmFex7Ra9KD0i066BvOA
                    /kHzhx23zGFNa3rZC
990         next
991     end
992     config vpn ipsec phase2
993         edit "Tech_1_tunnel"
994             set dst-addr-type ip
995             set pfs enable
996             set phase1name "Tech_support_1"
997             set proposal 3des-sha1 3des-md5
998             set replay enable
999             set dst-start-ip 220.100.65.98
1000            set src-subnet 10.10.10.0 255.255.255.0
1001        next
1002        edit "Tech_2_tunnel"
1003            set pfs enable
1004            set phase1name "Tech_support_2"
1005            set proposal 3des-sha1 3des-md5
1006            set replay enable
1007            set src-subnet 10.10.10.0 255.255.255.0
1008        next
```

```
1009 end
1010 config firewall schedule recurring
1011     edit "always"
1012         set day sunday monday tuesday wednesday thursday friday
                saturday
1013     next
1014     edit "Lunch"
1015         set day monday tuesday wednesday thursday friday
1016         set end 14:00
1017         set start 11:45
1018     next
1019 end
1020 config firewall vip
1021 end
1022 config firewall policy
1023     edit 1
1024         set srcintf "internal"
1025         set dstintf "wan1"
1026             set srcaddr "FinEng"
1027             set dstaddr "all"
1028         set action accept
1029         set schedule "always"
1030             set service "ANY"
1031         set profile-status enable
1032         set profile "Standard_profile"
1033         set nat enable
1034     next
1035     edit 3
1036         set srcintf "internal"
1037         set dstintf "wan1"
1038             set srcaddr "Help_Desk"
1039             set dstaddr "all"
1040         set action accept
1041         set schedule "Lunch"
1042             set service "ANY"
1043         set profile-status enable
1044         set profile "Help_Desk_lunch"
1045         set nat enable
1046     next
1047     edit 2
1048         set srcintf "internal"
1049         set dstintf "wan1"
1050             set srcaddr "Help_Desk"
1051             set dstaddr "all"
1052         set action accept
1053         set schedule "always"
```

```
1054                set service "ANY"
1055            set profile-status enable
1056            set profile "Help_Desk_work"
1057            set nat enable
1058        next
1059        edit 4
1060            set srcintf "dmz"
1061            set dstintf "wan1"
1062                set srcaddr "all"
1063                set dstaddr "Tech_support_1"
1064            set action ipsec
1065            set schedule "always"
1066                set service "ANY"
1067            set profile-status enable
1068            set profile "Standard_profile"
1069            set inbound enable
1070            set outbound enable
1071            set natinbound enable
1072            set vpntunnel "Tech_support_1"
1073        next
1074        edit 5
1075            set srcintf "dmz"
1076            set dstintf "wan1"
1077                set srcaddr "all"
1078                set dstaddr "all"
1079            set action ipsec
1080            set schedule "always"
1081                set service "ANY"
1082            set inbound enable
1083            set outbound enable
1084            set natinbound enable
1085            set vpntunnel "Tech_support_2"
1086        next
1087        edit 6
1088            set srcintf "internal"
1089            set dstintf "dmz"
1090                set srcaddr "all"
1091                set dstaddr "all"
1092            set action accept
1093            set schedule "always"
1094                set service "ANY"
1095            set nat enable
1096        next
1097    end
1098    config firewall policy6
1099    end
```

```
config spamfilter bword
end
config spamfilter ipbwl
end
config spamfilter dnsbl
end
config spamfilter emailbwl
end
config spamfilter mheader
end
config spamfilter iptrust
end
config ips DoS
    edit 1
            config address
                edit 1
                next
            end
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set threshold 2000
                next
                edit "tcp_port_scan"
                    set status enable
                    set threshold 1000
                next
                edit "tcp_src_session"
                    set status enable
                    set threshold 5000
                next
                edit "tcp_dst_session"
                    set status enable
                    set threshold 5000
                next
                edit "udp_flood"
                    set status enable
                    set threshold 2000
                next
                edit "udp_scan"
                    set status enable
                    set threshold 2000
                next
                edit "udp_src_session"
                    set status enable
                    set threshold 5000
```

```
                next
                edit "udp_dst_session"
                    set status enable
                    set threshold 5000
                next
                edit "icmp_flood"
                    set status enable
                    set threshold 50
                next
                edit "icmp_sweep"
                    set status enable
                    set threshold 100
                next
                edit "icmp_src_session"
                    set status enable
                    set threshold 300
                next
                edit "icmp_dst_session"
                    set status enable
                    set threshold 1000
                next
            end
        set name "all_default"
    next
    edit 2
            config address
                edit 1
                next
            end
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set action block
                    set threshold 2000
                next
                edit "tcp_port_scan"
                    set threshold 1000
                next
                edit "tcp_src_session"
                    set threshold 5000
                next
                edit "tcp_dst_session"
                    set threshold 5000
                next
                edit "udp_flood"
                    set status enable
```

```
1192                    set action block
1193                    set threshold 2000
1194                next
1195                edit "udp_scan"
1196                    set threshold 2000
1197                next
1198                edit "udp_src_session"
1199                    set threshold 5000
1200                next
1201                edit "udp_dst_session"
1202                    set threshold 5000
1203                next
1204                edit "icmp_flood"
1205                    set status enable
1206                    set action block
1207                    set threshold 50
1208                next
1209                edit "icmp_sweep"
1210                    set threshold 100
1211                next
1212                edit "icmp_src_session"
1213                    set threshold 300
1214                next
1215                edit "icmp_dst_session"
1216                    set threshold 1000
1217                next
1218            end
1219        set name "block_flood"
1220    next
1221 end
1222 config router rip
1223        config redistribute "connected"
1224        end
1225        config redistribute "static"
1226        end
1227        config redistribute "ospf"
1228        end
1229        config redistribute "bgp"
1230        end
1231 end
1232 config router static
1233    edit 1
1234        set device "wan1"
1235        set gateway 192.168.100.1
1236    next
1237    edit 2
```

```
1238         set device "wan1"
1239         set gateway 64.230.254.39
1240     next
1241 end
1242 config router ospf
1243         config redistribute "connected"
1244         end
1245         config redistribute "static"
1246         end
1247         config redistribute "rip"
1248         end
1249         config redistribute "bgp"
1250         end
1251 end
1252 config router bgp
1253         config redistribute "connected"
1254         end
1255         config redistribute "rip"
1256         end
1257         config redistribute "ospf"
1258         end
1259         config redistribute "static"
1260         end
1261 end
1262 config router multicast
1263 end
1264 config antivirus filepattern
1265     edit 1
1266             config entries
1267                 edit "*.bat"
1268                 next
1269                 edit "*.com"
1270                 next
1271                 edit "*.dll"
1272                 next
1273                 edit "*.doc"
1274                 next
1275                 edit "*.exe"
1276                 next
1277                 edit "*.gz"
1278                 next
1279                 edit "*.hta"
1280                 next
1281                 edit "*.ppt"
1282                 next
1283                 edit "*.rar"
```

```
1284                    next
1285                    edit "*.scr"
1286                    next
1287                    edit "*.tar"
1288                    next
1289                    edit "*.tgz"
1290                    next
1291                    edit "*.vb?"
1292                    next
1293                    edit "*.wps"
1294                    next
1295                    edit "*.xl?"
1296                    next
1297                    edit "*.zip"
1298                    next
1299                    edit "*.pif"
1300                    next
1301                    edit "*.cpl"
1302                    next
1303                end
1304            set name "builtin-patterns"
1305        next
1306    end
```

C Bibliografia

FORTINET. *FortiGate SOHO and SMB Version 3.0 MR6* [linean]. Fortinet, 2011. http://docs.fortinet.com/fgt/archives/3.0/techdocs/FortiGate_Example_SOHO_01-30006-0062-20080310.pdf [Azken kontsulta: 2011-5-19]

GITHUB. *GitHub:Help* [linean]. GitHub, 2011. http://help.github.com/ [Azken kontsulta: 2011-5-19]

ITIL. *The Official Introduction to the ITIL Service Lifestyle*. Londres: TSO, 2007. http://help.github.com/ [Azken kontsulta: 2011-5-19]