Disseny i configuració d'una xarxa de comunicacions d'un CPD

Sergi Micola Garcia

Grau de Tecnologies de la Telecomunicació

José Manuel Castillo Pedrosa

15/01/2023

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FITXA DEL TREBALL FINAL

Títol del treball:	*Disseny i configuració d'una xarxa de comunicacions d'un CPD*
Nom de l'autor:	*Sergi Micola Garcia*
Nom del consultor:	*José Manuel Castillo Pedrosa*
Data de lliurament (mm/aaaa):	*01/2023*
Àrea del Treball Final:	*Administració de xarxes i sistemes operatius*
Titulació:	*Grau de Tecnologies de la Telecomunicació*

Resum del Treball (màxim 250 paraules):

El creixement corporatiu del client ha obligat a transformar la seva infraestructura de comunicacions per tal d'adaptar-se a les necessitats actuals del servei.

Aquest treball es basa en el cas real d'una gran empresa que dona servei a les aplicacions utilitzades per la gestió d'un port marítim. La infraestructura de comunicacions d'aquest client ha quedat obsoleta, no complint amb els requisits que actualment necessiten, sobretot en termes de disponibilitat, redundància, capacitat i seguretat.

L'objectiu del treball és dissenyar una xarxa de comunicacions que s'ajusti a les necessitats reals del servei i millorar la xarxa actual perquè es pugui adaptar a futurs canvis. S'analitzarà l'estat actual de la xarxa i es farà una proposta de transformació, reutilitzant els equips actuals que encaixin en la nova proposta, i detallant tots els elements d'aquesta nova infraestructura.

Per últim es farà un anàlisi del funcionament de tots els equips instal·lats fins el moment, indicant quina ha estat la configuració impactades i el motiu.

Abstract (in English, 250 words or less):

The client's corporate growth has forced it to transform his Communications infrastructure in order to adapt to the current needs of service.

This project is based on a real case of a large company that provides service to the applications used for a management of a maritime port. This client's communications infrastructure has been obsolete, doesn't meeting the requirements they currently need, especially in terms of availability, redundancy, capacity and security.

The goal of the work is to design a communication network that fits the real needs of the service and improve the current network so that it can adapt to a future changes. The current state of network will be analyzed and there will be a proposal of transformation, reusing the current equipment that fits into the new proposal, and detailing all elements of this new infrastructure.

Finally, we analyze will be made of the operation of all the equipment installed so far, indicating which configuration has been affected and the reason.

Paraules clau (entre 4 i 8):

infraestructura de comunicacions, switch, Firewall, WAF, CPD, VLAN

ÍNDEX

1 INTRODUCCIÓ

1.1 Descripció del treball

Es proposa com a treball final de grau "El disseny i configuració d'una xarxa" encarregada de gestionar tot el trànsit d'un port marítim. Es durà a terme en un entorn real. L'objectiu és dotar la infraestructura de xarxa de dos Centres de Dades (en endavant, CPDs). Es realitzarà complint amb les necessitats del servei i reaprofitant tots els elements que encaixin dins de la solució.

L'arquitectura de comunicacions proposada està estructurada en capes funcionals dotades de diferents nivells de redundància que permeten assegurar la disponibilitat de la solució enfront errors inter-CPD i intra-CPD. Les capes que integren la solució de comunicacions s'han dissenyat de manera que es mantinguin les funcionalitats avançades en el CPD principal i al CPD de redundància. Les directrius de disseny utilitzades han estat enfocades en optimitzar al màxim el retorn de la inversió de la infraestructura i al mateix temps garantir la renovació tecnològica i la disponibilitat de les tecnologies que permeten fer front a futurs reptes en l'àmbit dels serveis dels CPDs.

1.2 Objectius del treball

- Dissenyar una xarxa que s'ajusti a les necessitats i requeriments (redundància i disponibilitat) del servei i les millores proposades respecte l'entorn actual.
    - Ha de ser una xarxa escalable
    - Si hi ha un punt de fallada ha de continuar funcionant per altres línies (disponibilitat)
    - Ha de ser una xarxa segura
    - Ha de ser operable des de l'exterior
- Implementar el disseny proposat, mostrant l'estructura final i les configuracions dels equips
- Ajustar al màxim la seguretat de la xarxa, instal·lant algun dispositiu de seguretat en cas que es vegi necessari.

1.3 Requeriments

Per implementar la solució s'utilitzaran 4 equips Cisco Nexus 9318-EX amb connexions de Fibra Òptica a 10Gb i de coure a 1 Gb per donar servei a servidors i diferents elements.

S'utilitzaran 2 firewalls FORTINET FG-601E, 2 ubicats en un CPD i 2 firewalls FORTINET FG-500 a l'altre, treballant en actiu/passiu.

També s'instal·laran 3 WAF FORITWEB, 2 a cada CPD principal i 1 al CPD secundari.

Resum d'equips utilitzats:

EQUIPO		FABRICANTE	MODELO
CPD1	SWITCH	CISCO	NEXUS 9300-EX
	SWITCH	CISCO	NEXUS 9300-EX
	FIREWALL	FORTINET	FG-601E
	FIREWALL	FORTINET	FG-601E
	WAF	FORTIWEB	1000E
	WAF	FORTIWEB	1000E
CPD2	SWITCH	CISCO	NEXUS 9300-EX
	SWITCH	CISCO	NEXUS 9300-EX
	FIREWALL	FORTINET	FG-500
	FIREWALL	FORTINET	FG-500
	WAF	FORTIWEB	1000E

Taula 1 - Equipament

1.4 Planificació

La idea és dividir el treball en 4 parts. La primera és aquesta, la organització de com es farà i de que es farà el TFG.

La segona part és la part de disseny. Saber com és la situació actual i exposar teòricament quins canvis es faran, els motius i la idea final.

La tercera part és la implementació. Implementar tot el descrit a la part anterior, mostrar les configuracions que es faran i el perquè d'aquestes.

La última part és escriure les conclusions, i revisar. Per últim preparar l'exposició a fer.

Entrega	Tasca	Inici	Final	03-oct	10-oct	17-oct	24-oct	31-oct	07-nov	14-nov	21-nov	28-nov	05-dic	12-dic	19-dic	26-dic	02-ene	09-ene
PAC1	Pla de treball	03/10/2022	16/10/2022															
	Descripció	03/10/2022	09/10/2022															
	Objectius	03/10/2022	09/10/2022															
	Requeriments	03/10/2022	09/10/2022															
	Planificació	03/10/2022	12/10/2022															
	Esbós de sumari	10/10/2022	16/10/2022															
	Entrega	16/10/2022	16/10/2022															
PAC2	Disseny de la xarxa	17/10/2022	20/10/2022															
	Esquema situació actual	17/10/2022	23/10/2022															
	Descripció situació actual	21/10/2022	27/10/2022															
	Millores necessaries	27/10/2022	30/10/2022															
	Esquema nova xarxa	31/10/2022	08/11/2022															
	Descripció de la xarxa	07/11/2022	20/11/2022															
	Entrega	20/11/2022	20/11/2022															
PAC3	Implementació	21/11/2022	25/12/2022															
	Configuracions dels FW	21/11/2022	30/11/2022															
	Descripció de les configuracions	28/11/2022	15/12/2022															
	Configuracions equips switch	05/12/2022	16/12/2022															
	Descripció de les configuracions	12/12/2022	25/12/2022															
	Posada en marxa	12/12/2022	25/12/2022															
	Entrega	25/12/2022	25/12/2022															
Final	Memòria i presentació	26/12/2022	15/01/2023															
	Conclusió	26/12/2022	01/01/2023															
	Revisió	26/12/2022	08/01/2023															
	Entrega	15/01/2023	15/01/2023															
	Presentació	26/12/2022	15/01/2023															

Il·lustració 1 - Planificació

1.5 Esbós de sumari

En el cos de la memòria hi haurà 2 grans capítols, disseny i implementació:

1.0 Introducció: En aquest apartat s'introduirà tot el escrit en el pla de treball més modificacions que vagin sortint durant el projecte
- 1.1 Context i justificació del treball
- 1.2 Objectius del treball
- 1.3 Enfocament i mètode seguit
- 1.4 Planificació
- 1.5 Sumari de productes
- 1.6 Breu descripció de capítols

2.0 Disseny
- 2.1 Esquema situació actual: es vol representar de forma gràfica quina és la situació actual de la xarxa que volem tractar
- 2.2 Descripció de la situació actual: Es farà una descripció de la situació acutal
- 2.3 Millores: s'estudiaran les millores necessàries de la xarxa, i s'explicaran els motius de les necessitats d'aquest canvi d'infraestructura
- 2.4 Esquema nova xarxa: Es representarà de forma gràfica la solució que es vol aplicar
- 2.5 Descripció de la nova xarxa: Es farà una descripció de com quedarà la nova xarxa i les diferencies respecte a l'estat actual

3.0 Implementació
- 3.1 Configuració dels FW: Es mostraran les configuracions fetes en els FW, explicant que és cada configuració
- 3.2 Descripció de la configuració: S'explicaran perquè es fan aquestes configuracions i com es fan.
- 3.3 Configuració equips switch: Es mostraran les configuracions fetes en els switchs, explicant que és cada configuració
- 3.4 Descripció de la configuració switch: S'explicaran perquè es fan aquestes configuracions i com es fan.

4.0 Conclusió

5.0 Glossari

6.0 Bibliografia

1.6 Esbós de sumari

En la introducció es farà un breu descripció del treball, de les línies que seguirà aquest projecte. S'especificaran quins son els ojectius marcats abans de començar a elaborar el treball i s'especificaran quines necessitats d'equipament seran necessàries per a dur-lo a terme. Per últim es fara una planificació en setmanes i es definirà el glossari.

Seguidament es detallarà tot el que es pugui quin és l'estat de la xarxa abans de realitzar el projecte. Es definiran les diferents capes funcionals i s'identificaran els punts de millora i les necessitats d'aquestes.

A la següent fase, es dissenyarà una nova arquitectura de xarxa, tenint en compte tots els espectes rellevants i detallant cada capa funcional. Així com donant resposta a les millores exposades a l'anterior capítol.

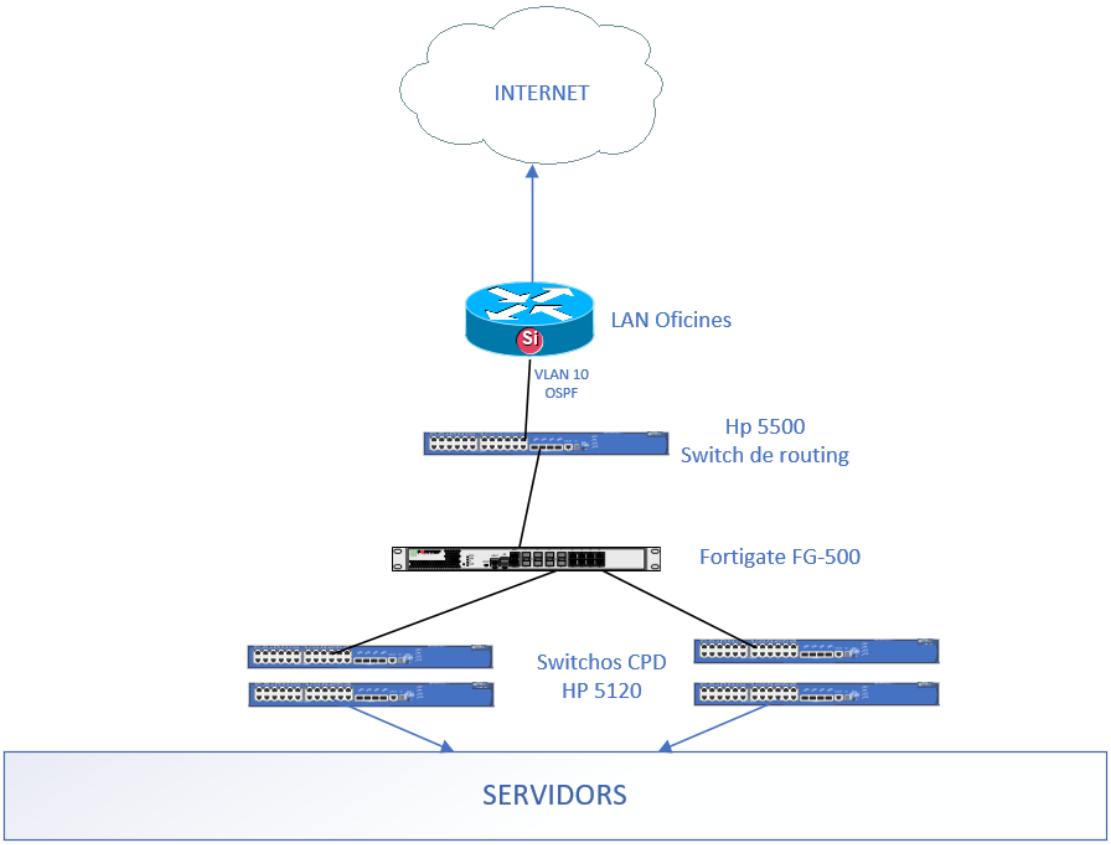
Una vegada acabat el disseny serà el moment de configurar els equips, es farà una descripció de totes les configuracions implantades en els equips, entrant en detall de perquè serveix cada una d'elles.

Per últim s'exposaran les conclusions extretes i es s'explicaran quines son les línies de futur que pot tenir aquest projecte.

2 DISSENY ÀNITC

2.1 Xarxa antiga

Actualment el CPD està integrat dins la mateixa xarxa de l'empresa. En concret és una subxarxa que connecta amb la xarxa mitjançant una ruta estàtica i te sortida cap a internet. Aquesta subxarxa està protegida per un Firewall FORTIGATE FG-500. Sota aquest Firewall, amb dues VLANS diferents (Managment i accés), hi ha 2 stacks de 2 switchos cada un, model HP 5120. En aquests switchos estan directament connectats els servidors corporatius.



Il·lustració 2 - Esquema de xarxa àntic

No podrem mostrar imatges de la configuració ja que no tenim permisos per accedir directament als equips.

2.1.1 Router CPD

Aquest equip és un HP 5500. Té 24 ports de Fibra Óptica i 8 ports RJ45. És l'encarregat d'enllaçar la xarxa empresarial amb la xarxa del CPD.

Aquest enllaç és fa mitjançant el protocol rutes estàtiques. En aquest router li arriba de la xarxa empresarial la VLAN 1, amb una IP 10.5.1.2, i mitjançant una ruta estàtica, sap que la xarxa del

CPD (10.10.10.0/24) està cap al fortigate. El tràfic ha de ser encaminat cap a la VLAN 10 (IP 10.10.10.1).

L'equip està configurat amb 2 VLANs:

- VLAN 1 (IP 10.5.1.2) – Aquesta VLAN és la que disposa d'una IP de la xarxa empresarial. És la branca del router connectada directament a la xarxa empresarial
- VLAN 10 (IP 10.10.10.1) – Aquesta VLAN pertany al rang del CPD. És la branca del router connectada a la xarxa del CPD i que fa d'enllaç amb el Firewall.

L'equip està configurat amb una ruta estàtica que enllaça la xarxa del CPD (VLAN 10) amb la xarxa general (VLAN 1).

2.1.2 Firewall

El Firewall és un equip FORTIGATE FG-500. Aquest equip disposa de 24 ports RJ45 + 2 ports RJ45 de WAN.

Només s'utilitzen 3 ports, un que connecta amb el router i els altres dos que connecten amb els switchos. Dins del Firewall hi ha 2 xarxes internes configurades:

- Accés: Té un direccionalment IP 10.10.10.0/24. En aquesta xarxa es troben tots els servidors de l'empresa.
- Managment: Té un direccionalment 10.1.1.0/24. En aquesta xarxa es troba la gestió dels equips de xarxa i gestió d'alguns servidors.

La xarxa de Gestió està encaminada mitjançant una ruta estàtica que pública el propi Firewall, d'aquesta manera la gestió dels equips és accessible des de la xarxa empresarial pels tècnics d'informàtica. La xarxa de Managment no té sortida cap a internet.

2.1.3 Switchos

Aquests switchos son model HP 5120, tenen 24 ports de RJ45 i 4 ports de Fibra Óptica. També tenen un mòdul de Stack per la part de darrere, que es connecta amb un cable propi d'HP i automàticament construeix un stack de 2 switchos en mode Actiu-Actiu.

En aquest enllaç es passen directament les VLANs d'Accés i gestió directament a nivell 2.

Els switchos tenen els servidors directament connectats. En alguns casos els servidors estan configurats amb bonding, per la qual cosa els switchos tenen configurats alguns Port-Channel. Cada port té la VLAN corresponent depenent del servei que té per sota.

2.1.4 Millores

Aquest model d'infraestructura ha quedat obsolet. Segons el client, la infraestructura ha anat creixent i actualment és necessària una renovació completa per millorar en tots els aspectes.

El primer que cal fer és dotar de redundància la infraestructura. Trobem un model sense cap mena de redundància en moltes línies.

S'identifiquen les següents millores bàsiques:

- La sortida a internet: El CPD disposa d'una única fibra òptica que connecta amb la xarxa empresarial. Si aquest enllaç falla, el CPD queda aïllat.
- Segmentació: La xarxa presenta diferents segments molt marcats, que actualment conviuen en una mateixa subxarxa, i son accessibles els uns als altres, sense tenir en compte la seguretat del sistema.
- Gestió: La gestió dels equips únicament és possible des de dins la pròpia empresa, accedint directament des dels PCs dels administradors.
- Els switchos nomes disposen d'una sola línia de sortida.
- Un únic Firewall centralitza totes les comunicacions del CPD. Totes les comunicacions han de passar per un únic equip, provocant un possible punt de fallada molt gran.

2.1.5 Requeriments del servei

S'han acordat amb el client els següents requeriments que ha de tenir el projecte final.

- Hi haurà redundància de tot el servei, tenint dos CPDs separats, un primari, i un secundari en una ubicació diferent.
- Es dotarà de dues fibres òptiques a cada CPD.
- Es segmentaran mitjançant els Firewalls els diferents segments de xarxa, i només tindran permisos els serveis estrictament necessaris.
- La gestió dels equips es farà mitjançant una VPNSSL, d'aquesta manera serà més segur, i els equips seran accessibles des de qualsevol lloc.
- Cada switch disposarà de una connexió cap als Firewalls per tal de no perdre servei en cas de fallada d'alguna línia.

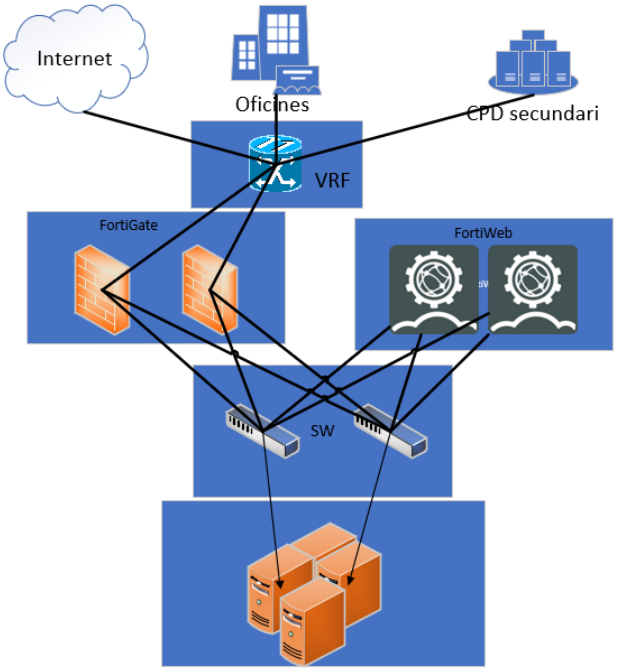
3 PROPOSTA

Degut al creixement, les necessitats del client han canviat. Actualment els sistemes han de ser accessibles 24x7. Una fallada dels sistemes pot provocar moltes pèrdues econòmiques, per tant s'ha de dotar al client d'una infraestructura capaç de superar qualsevol incident. Aquesta casuística provoca un canvi radical, i es procedirà a fer una migració integral dels sistemes cap a dues ubicacions externes.

Es migrarà el CPD a dues ubicacions (principal i secundari) diferents, a dos CPDs ubicats en recintes especialitzats dotats de les necessitats (ventilació, energia, accés...).

L'arquitectura de comunicacions plantejada està estructurada en capes funcionals dotades amb diferents nivells de redundància que permeten assegurar la disponibilitat de la solució enfront els punts de fallada inter-CPD i intra-CPD. Les capes que integren la solució de comunicacions s'han dissenyat de manera que es mantenen les funcionalitats avançades en el CPD principal i el secundari. Les directrius de disseny s'han enfocat en la renovació tecnològica i la disponibilitat de tecnologies que permeten a l'empresa fer front a futurs canvis en l'àmbit dels serveis dels CPDs.

A continuació, es descriuen les diferents capes funcionals que composen la solució en el CPD principal i secundari. A mode de referencia, s'adjunta un esquema amb els components que integren cada una de les capes.



Il·lustració 3 - Esquema de xarxa nou

El disseny proposat es realitza reaprofitant tots els elements de seguretat actuals que encaixen en la solució global i introduint elements nous de nova implantació específics. Per això, s'ha contemplat la renovació de manteniments i la subscripció de llicències de la solució actual del client per l'entorn del CPD secundari. La solució de seguretat està basada en equips del fabricant FORTINET, està concebuda per que existeixi una integració dels diferents elements de seguretat realitzant la seva gestió de manera centralitzada i permetent compartir informació entre ells sota aquests dos conceptes:

- Security Fabric: és el concepte o funcionalitat que fa d'engranatge entre totes les funcionalitats de les solucions proposades. La integració dintre els diferents elements de seguretat com FortiGate o FortiWeb. Es potencia per ser capaços de detectar anomalies de seguretat, aplicació de polítiques, etc... obtenint així una major sincronització en la capa de seguretat.
- FortiGuard: És la xarxa intel·ligent al cloud que nodreix a tots els dispositius d'informació, firmes, etc...

D'aquesta manera els diferents elements que asseguren l'entorn, estaran constantment actualitzant la seva informació.

3.1 Connectivitat WAN

El disseny treballat per la connectivitat WAN del servei està basat en les següents tecnologies:

- VPLS Ethernet Line, pels circuits Ethernet de interconnexió amb el client.
- Circuits DWDM per la interconnexió interna entre CPDs (primari i secundari).
- Internet Access, pels circuits d'accés a internet i publicació de serveis.

Ajustant-nos a les necessitats de servei de la infraestructura de xarxa, així com altres millores ofertes que asseguren l'evolució del servei d'acord amb les últimes tecnologies disponibles en el mercat i l'increment de capacitats que el client pugui requerir durant tota la vida del servei. Es planteja un escenari de connectivitat redundada que permeti mantenir els nivells de disponibilitats necessaris.

3.2 Connectivitat Ethernet

La plataforma es basa en una arquitectura de sistema moderna dissenyada per proporcionar un alt rendiment i satisfer les necessitats canviants dels centres de dades altament escalables i la demanda del creixement de les organitzacions.

Els commutadors de la sèrie Cisco Nexus 9300-EX ofereixen una veritat d'opcions de interfície per migrar de forma transparent els centres de dades existents, des de velocitats de 1Gbps i 10 Gbps a 25Gbps en l'accés, de 10 a 40Gbps en la capa d'agregació.

Pel CPD primari s'ha optat per una parella d'equips del model Cisco Nexus 93180YC-EX, dotats cada un de 48 interfícies 1/10/25Gb i 6 interfícies de 40Gb. Aquesta configuració permet tenir en una única parella diversitat d'opcions de connectivitat, tant a nivell òptic (SFP+/QSFP28) com elèctric (RJ45). Els dos equips formen un sol equip a nivell lògic, mitjançant la tecnologia VPC, permetent tolerància a fallades. Cada un dels equips està dotat a la vegada de fonts d'alimentació i ventiladors redundants. A nivell del CPD secundari l'arquitectura de l'entorn és una rèplica exacte a la del CPD primari.

El rendiment de cada equip suporta 3.6 Terabits per segon (Tbps) de capacitat de commutació i en rendiment, de 2.6 bilions de paquets per segon (bpps), amb una latència inferior a 1 microsegon.

3.3 Seguretat a la xarxa

El disseny de Firewalls proposat per donar servei pertanyen al fabricant FORTINET i compleixen amb tots els requeriments descrits anteriorment. Es proposa la utilització de dos Appliances dedicats Fortinet FG-601 llicenciats amb les característiques de seguretat necessàries per donar resposta a les funcionalitats requerides pel servei. Pel CPD secundari es contempla la reutilització dels equips actuals del client Fortinet FG-500, renovant els serveis i funcionalitats requerits per l'entorn.

La solució WAF proposada pertany al fabricant FORTINET. Compleix amb tots els requeriments necessaris. Es proposa la utilització de dos Appliances dedicats FORTINET FortiWeb-1000E llicenciats amb les característiques de seguretat necessàries per donar resposta a les funcionalitats requerides pel servei.

El disseny contempla alta disponibilitat tant pel CPD primari com pel secundari en una modalitat actiu/passiu.

3.4 Entorn de connectivitat física

3.4.1 Visió general de la connectivitat

En els següents apartats es completa una descripció del entorn de connectivitats físiques dels elements que componen el disseny de comunicacions. La major part d'aquestes característiques està proporcionat pel propietari del CPD.

- Connectivitat elèctrica dels equips de comunicacions

- Ventilació
- Layout de equipament en rack

3.4.1.1 Connectivitat elèctrica

Segons la normativa interna del CPD i complint amb els estàndards i recomanacions dels fabricants, els elements físics seran instal·lats en base als requeriments establerts en referència a la gestió eficient de la energia elèctrica que es fixa dins de les sales condicionades en cada un dels CPDs (primari i secundari). D'aquesta manera es pot garantir el correcte funcionament a nivell de capacitats de hardware i rendiment dels equips físics, així com la seva adequada alimentació elèctrica redundada i estable.

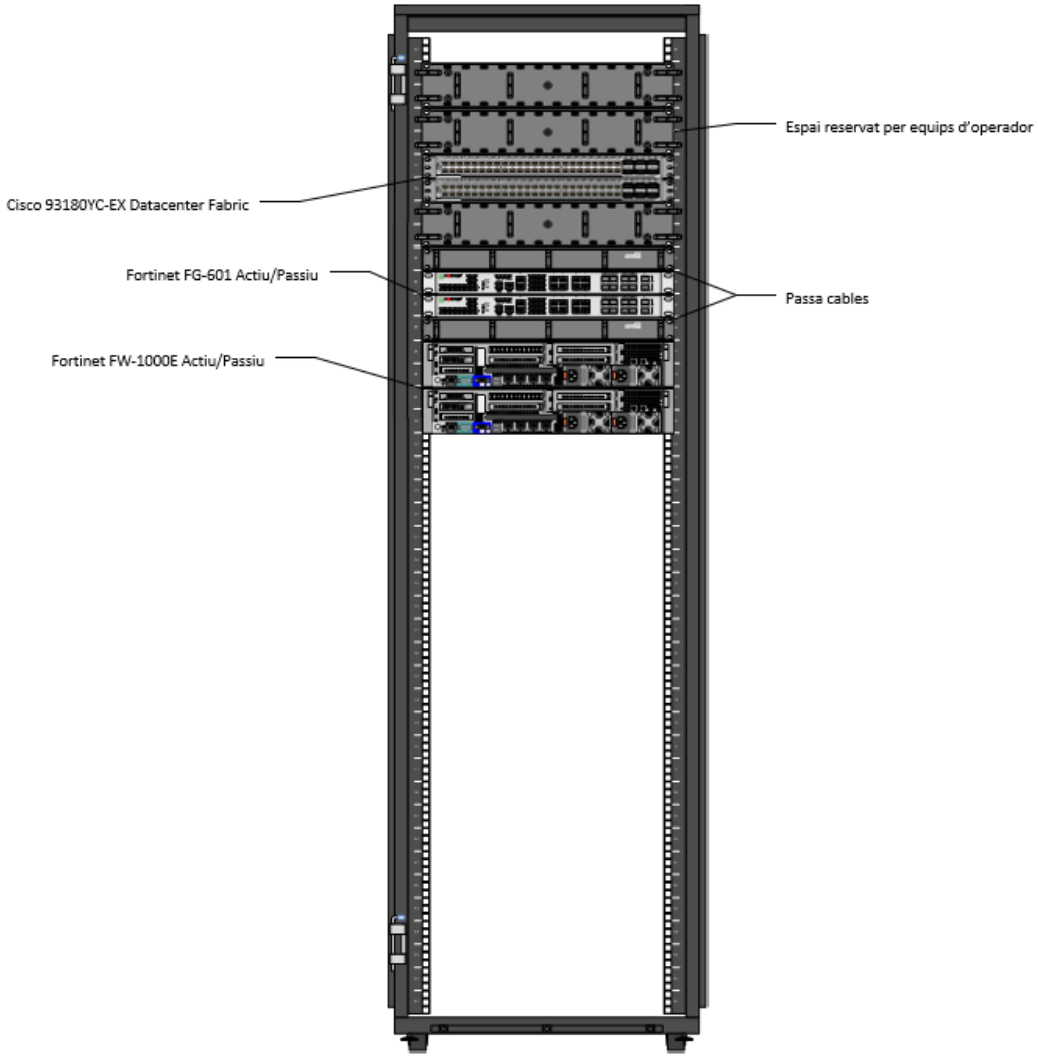
3.4.1.2 Ventilació

Segons la normativa interna del CPD i complint amb els estàndards i recomanacions dels fabricants, els elements físics seran instal·lats en base als requeriments establerts en referència a la gestió eficient dels fluxos d'aire que es fixen dins de les sales condicionades en cada un dels CPDs (primari i secundari). D'aquesta manera es pot garantir el correcte funcionament a nivell de capacitats de hardware i rendiment dels equips físics, així com la seva adequada ventilació.

3.4.1.3 Layout equipament físic

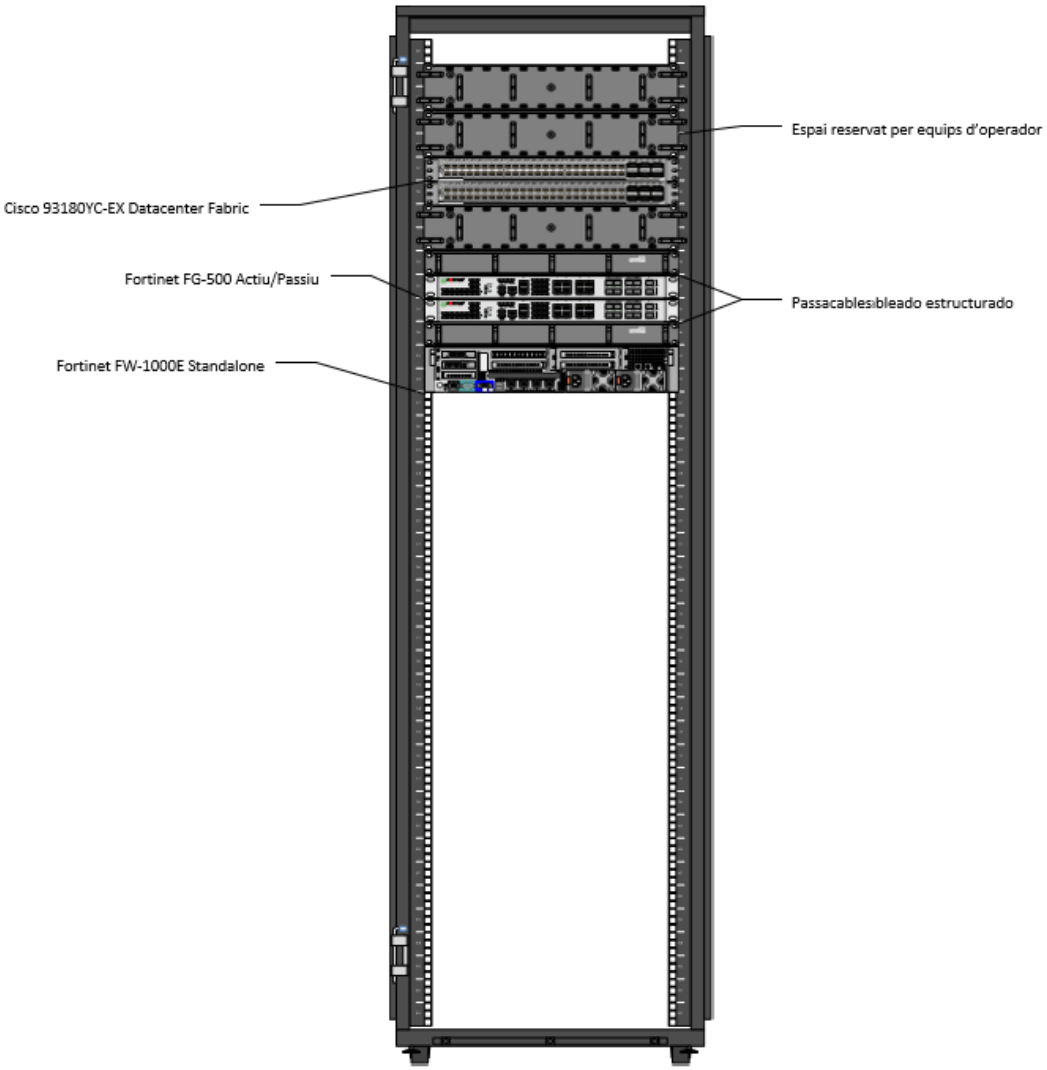
En referència a la implementació dels elements físics que composen el disseny i la seva distribució dins del rack de comunicacions, s'adjunten esquemes detallats de cada un dels elements i el seu posicionament dins dels racks de cada un dels CPDs.

Layout CPD primari:



Il·lustració 4 - Layout CPD primari

Layout del CPD secundari:



Il·lustració 5 - Layout del CPD secundari

3.5 Infraestructura ethernet

El disseny detallat de la infraestructura de connectivitat ethernet a nivell dels CPDs respon a les necessitats requerides pels sistemes que composen la solució i als requeriments específics a nivell de disponibilitat del servei. En els següents punts es descriu el disseny proposat i les seves capacitats

3.5.1 Descripció general

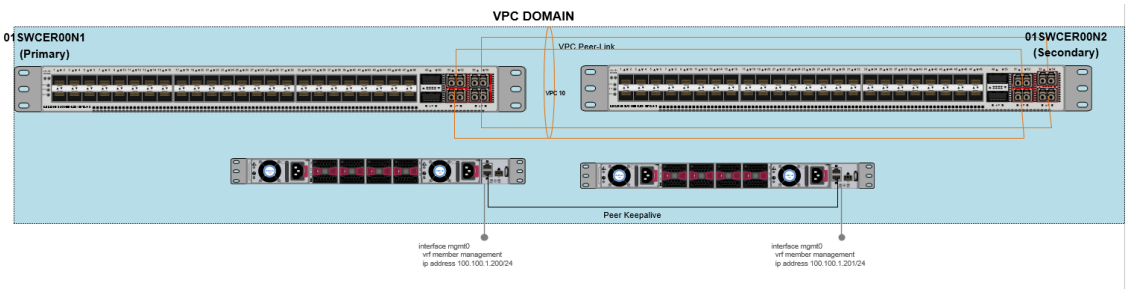
La solució de connectivitat ethernet que es descriu a continuació es replica de forma idèntica en els dos CPDs (primari i secundari).

El disseny està concebut per mantenir l'alta disponibilitat dels elements que es connecten als equips de switching que el composen, a més d'oferir els amples de banda requerits per garantir un servei estable, fiable i amb capacitat de creixement.

La infraestructura CORE la composen una parella de CISCO NEXUS 9318-EX configurats en un model Fabric Connect o VPC Domain d'alta disponibilitat. Els enllaços que estableixen aquest clúster son interfícies dedicades QSFP+ 40Gb en agregat conformant un backbone de interconnexió de 80Gbps entre els dos equips.

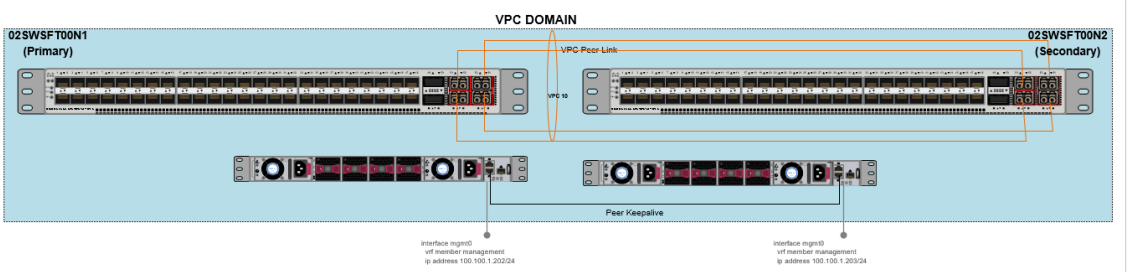
El disseny permet executar accions de manteniment de forma independent en els dos equips de forma individual i sense perdre la disponibilitat del servei que suporta. A nivell detallat, s'adjunten els esquemes de l'arquitectura contemplada per cada un dels CPD.

- Disseny LLD VPC Domain CPD principal



Il·lustració 6 - - Disseny LLD VPC Domain CPD principal

- Disseny LLD VPC Domain CPD secundari



Il·lustració 7 - - Disseny LLD VPC Domain CPD secundari

El detall dels components que composen la solució és:

Descripció	**Quantitat**
Nexus 9300-EX w/48 1/10/25G & 6p 40/100G	4
SNTC-8X5XNBD Nexus 9300 w/ 24p 10/25G 6p 40/100G	4

OPT OUT FOR “Default” DCN Subscription Selection	4
Power Cord, 250VAC 10A CEE 7/7 Plug, EU	8
40G BASE-CR4 Passive Copper Cable, 1m	8
Nexus Fan, 30CFM, port side exhaust airflow	16
NX-OS Essentials licenes for Nexus 9300 (10G+) Platforms	4
SWSS UPGRADES NX-OS Essentials licenes for Nexus 9300	4
Dummy PID for Airflow Selection Port-side Exhaust	4
Operating System Software (NX-OS 9.3(5))	4

Taula 2 – Components de connectivitat física

La base de la xarxa Ethernet en aquest disseny de CPD es basa en una parella de CISCO NEXUS 9318YC-EX per CPD. Aquests commutadors ofereixen la plataforma ideal per crear un CPD escalable i de alt rendiment compatible amb servidors connectats a 10Gb i 1Gb. El CPD està dissenyat per permetre una fàcil migració de servidors i serveis de de la seva sala de servidors original a un centre de dades que pot escalar el seu creixement de la organització.

Els switchos Cisco Nexus 9300 amb capacitats de port universal (UP) ofereixen suport Ethernet. Aquest disseny de centre de dades aprofita moltes funcionalitats avançades de la família de switchos Cisco Nexus sèrie 9300 per proporcionar una estructura de commutació central de capa 2 i capa 3 per l’entorn del centre de dades:

- La taula d’enrutament de capa 3 pot admetre fins 8000 rutes IPv4
- El motor de Capa 3 admet fins 8000 direccions MAC pel domini de capa 2

- La solució proporciona fins 1000 grups de multidifusió IP quan s'opera en l'entorn virtual recomanat

3.5.2 Resilència de l'entorn ethernet

El CPD ha de proporcionar una topologia en la que qualsevol VLAN del CPD pugui estendre a qualsevol servidor per acomodar noves instal·lacions sense interrupcions, i també la capacitat de moure una càrrega de servidor a qualsevol altre servidor físic del CPD. Els dissenys tradicionals de capa 2 amb commutadors LAN Spanning Tree (STP), que crea bucles quan una VLAN s'estén a diferents commutadors de capa d'accés.

El clúster de switchos de la sèrie Cisco Nexus 9300, proporcionen l'estructura de commutació ethernet central pels CPD i es configura mitjançant VPC. La funció VPC permet enllaços que estan connectats físicament a dos Cisco Nexus diferents aparèixer en un tercer dispositiu connectat a aquests, com a part d'un sol canal ethernet. El tercer dispositiu pot ser un servidor, commutador o qualsevol altre dispositiu o dispositiu compatible amb IEEE. Aquesta capacitat permet que els dos commutadors principals del CPD construeixin una capa resistent i sense bucles.

Cisco NX-OS Software VPC utilitzat en el disseny del CPD (VPC Domain) proporciona topologies sense bucles de STP, el que permet que els VLAN s'estenguin en tot el centre de dades mentre mantenim una arquitectura resilient. Un VPC consta de dos commutadores en alta disponibilitat de VPC connectats mitjançant un enllaç VPC Peer Link. Dels clúster VPC, un és el principal i l'altre és el secundari. El sistema format pels commutadors s'anomena VPC Domain.

Les VLANs que es contemplen en el disseny actual son les detallades a continuació:

Descripción VLAN	VLAN ID	Subnet	Mask	Gateway	CPD	Observaciones
Gestión LinuxONE CER	501	100.64.51.0	255.255.255.240	N/A	CER	Gestión interna LinuxONE (HMC/Support Elements) - No enrutada
Gestión LinuxONE SFT	505	100.64.51.0	255.255.255.240	N/A	SFT	Gestión interna LinuxONE (HMC/Support Elements) - No enrutada
Gestión	500	100.64.50.0	255.255.255.0	10.64.50.1	Extesa CER-SFT	Gestión infraestructura (Storage, HMC, KVM, etc.)

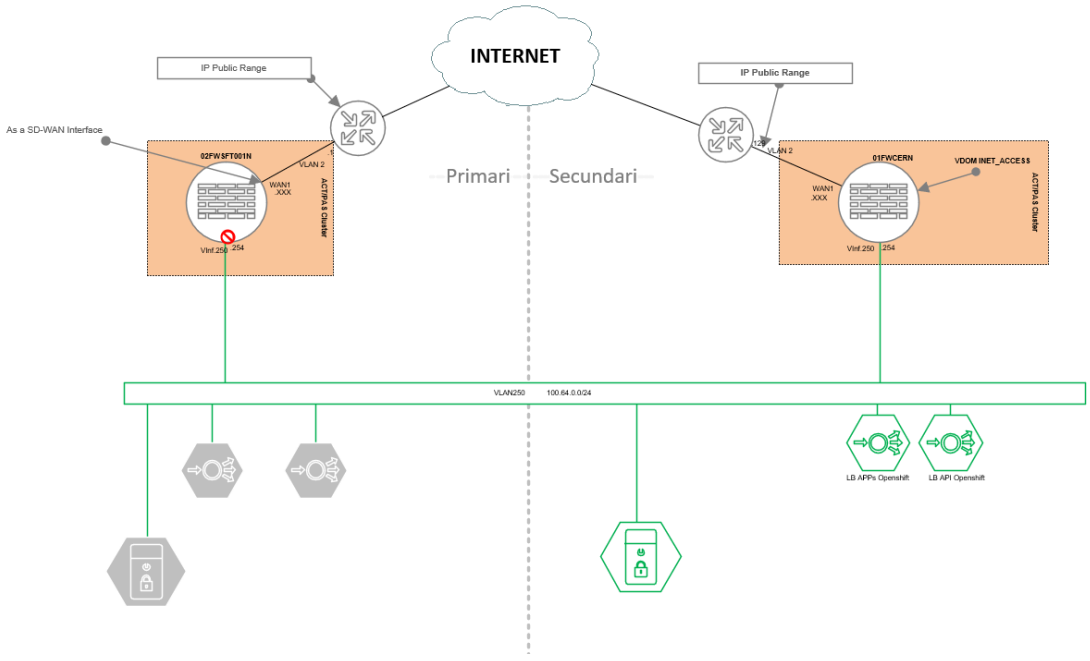
Producción	250	100.64.0.0	255.255.255.0	100.64.0.254	Extesa CER-SFT	Producción OCP, Oracle, MongoDB
Desarrollo	350	100.64.100.0	255.255.255.0	100.64.100.254	Extesa CER-SFT	Desarrollo OCP, Producción, Mongo DB
FC-IP	502	100.64.52.0	255.255.255.240	N/A	Extesa CER-SFT	FC-IP Replicación
RAC-Oracle	503	100.64.53.0	255.255.255.240	N/A	Extesa CER-SFT	RAC Oracle Replicación
Backup	1200	100.64.200.0	255.255.255.0	N/A	Extesa CER-SFT	Backup vlan
MGMT COMMs	600	100.100.1.0	255.255.255.0	100.100.1.1	Extesa CER-SFT	Vlan MGMT Comunicaciones

Taula 3 - Vlans

Passant a detallar la funcionalitat de cada una de les VLANs i els mecanismes d'alta disponibilitat que es contemplen per cada un dels elements que suporten:

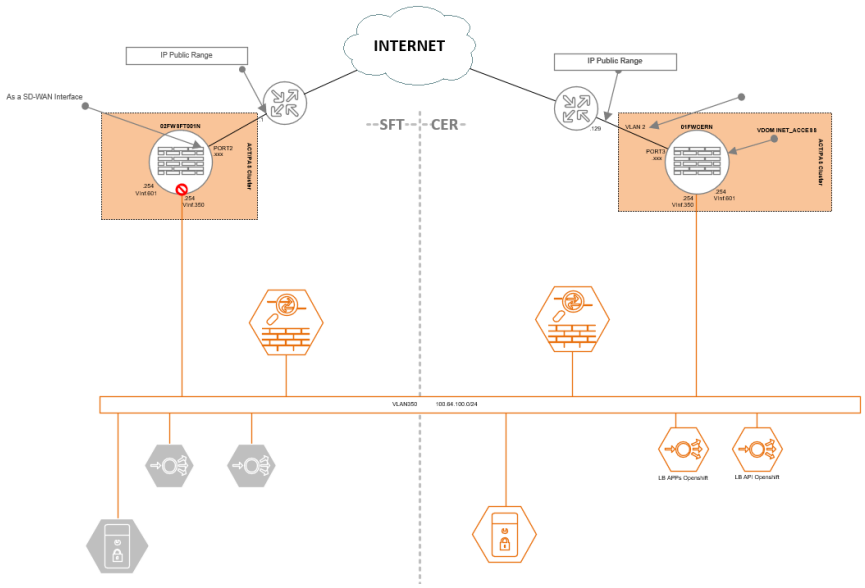
- Entorn de publicació Productiva: VLAN 250 DMZ "Producción". Es tracta de la VLAN des d'on es publiquen seran accessibles les aplicacions productives. Aquesta VLAN, serà estesa a nivell dos fins el CPD secundari, permeten poder aplicar mecanismes de Disaster Recovery àgils i que permetin simplificar al màxim el procés d'activació d'aquests.

  Detall de disseny LLD per DMZ Producció (VLAN 250):



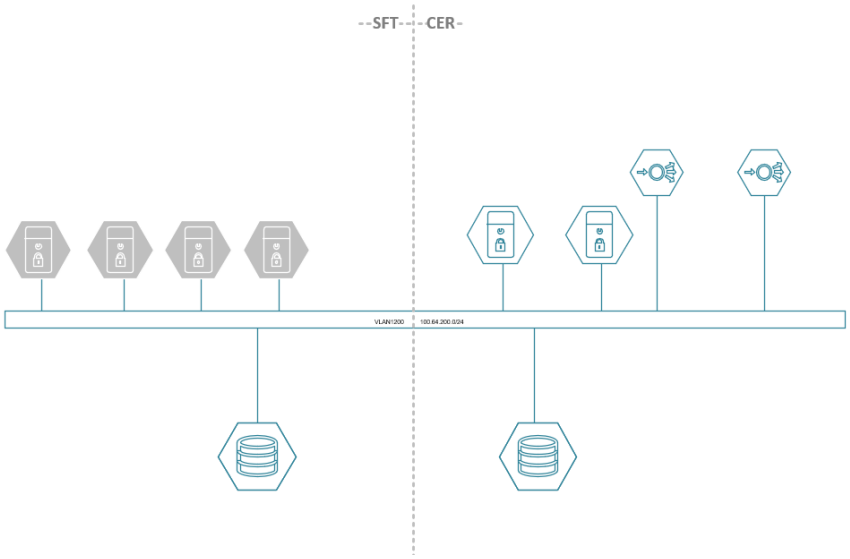
Il·lustració 8 - VLAN 250

- Entorn de publicació Desenvolupament: VLAN 350 DMZ “Desarrollo”. Es tracta de la VLAN des d’on es publicant i seran accessibles les aplicacions en fase de desenvolupament o producció. Aquesta vlan, serà estesa a nivell dos fins el CPD secundari, permeten poder aplicar mecanismes de Disaster Recovery àgils i que permetin simplificar al màxim el procés d’activació d’aquests.



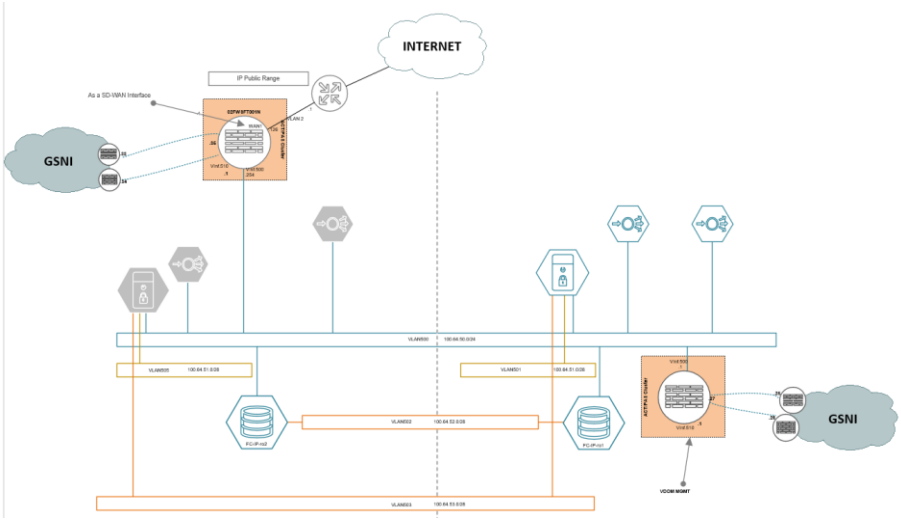
Il·lustració 9 - VLAN 350

- Entorn de Backup: VLAN 1200 Backup. Es tracta de la VLAN dedicada a tràfic exclusivament de Backup. Aquesta vlan, serà estesa a nivell dos fins el CPD secundari, permeten poder aplicar mecanismes de Disaster Recovery àgils i que permetin simplificar al màxim el procés d’activació d’aquests.



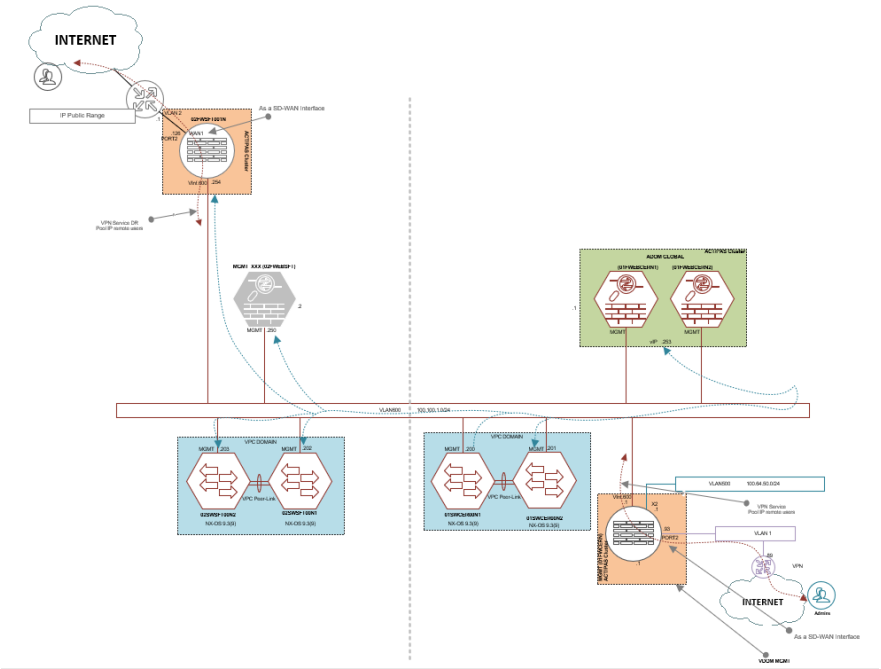
Il·lustració 10 - VLAN 1200

- Entorn de gestió de infraestructures: VLAN 500. Es tracta de la VLAN dedicada a tràfic exclusivament de gestió de infraestructura. Aquesta vlan, serà estesa a nivell dos fins el CPD secundari, permeten poder aplicar mecanismes de Disaster Recovery àgils i que permetin simplificar al màxim el procés d'activació d'aquests.



Il·lustració 11 - VLAN 500

- Entorn de gestió de comunicacions: VLAN 600. Es tracta de la VLAN dedicada a tràfic exclusivament de gestió de comunicacions. Aquesta vlan, serà estesa a nivell dos fins el CPD secundari, permeten poder aplicar mecanismes de Disaster Recovery àgils i que permetin simplificar al màxim el procés d'activació d'aquests.



Il·lustració 12 - VLAN 600

L'entorn de gestió de la infraestructura es realitzarà mitjançant la infraestructura de gestió pròpia de CPDs i mitjançant l'entorn VPN SSL dedicat. Tant des del CPD primari, com des del secundari.

3.6 Infraestructura de connectivitat WAN

El disseny detallat de la infraestructura de connectivitat WAN a nivell de CPD respon a les necessitats requerides pels sistemes i serveis que composen la solució i els requeriments identificats a nivell de disponibilitat del servei. En els següents punts es descriu el disseny proposat i les seves capacitats.

3.6.1 Descripció general

3.6.1.1 VPLS Ethernet Line

La tecnologia VPLS permet interconnectar la xarxa d'àrea local (LAN) Ethernet per que varies seus puguin treballar com una sola oficina. La solució permet als clients estendre Ethernet fins les xarxes metropolitanes i d'àrea àmplia (xarxes MAN i WAN) i en aquest cas des del client fins els CPDs (primari i secundari).

Els dos circuits VPLS Ethernet Lines proporciona les capacitats d'un servei de capa 2:

- Topologia punt a punt. Des de les localitzacions que es defineixin segons el pla de migració d'aplicacions
- Velocitats des de 1Gbps per enllaç VPLS

Per la connectivitat VPLS Ethernet no es requereix diversificació. Les característiques tècniques principals d'aquests circuits son:

- Les xarxes del client o seus, es trobaran connectades a la xarxa VPLS.
- Els CPDs (primari i secundari) ubicats en localitzacions diferents, estaran connectats a la xarxa VPLS
- Servei protegit dins del Backbone de l'operador.
- Equips Ethernet NTE del fabricant Accedian a cada seu i CPD
- Caudal de 1Gb 100% garantida.
- Entrega a interfície 1000BaseSR. Realitzant la connectivitat en els equips de core ethernet dels CPDs

3.6.1.2 Circuits DWDM per interconnexió interna entre CPDs (primari i secundari)

Es dissenya una solució de connectivitat inter-CPD (DCI) amb tecnologia DWDM, basada en plataforma òptica per dotar de diferents serveis de Wave Division Multiplexing (WDM), interconnectant mitjançant circuits metropolitans de fibra òptica els dos CPDs dins de l'abast del servei.

El DWDM és un mètode de multiplexació que s'utilitza en mitjans de transmissió electromagnètics. Varies senyals portadores es transmeten per una única fibra òptica utilitzant diferents longituds d'ona.

L'arquitectura DWDM ofereix una transmissió òptica de dades transparent de nivell 1 punt a punt d'alta capacitat entre dos ubicacions. Estan disponibles a nivell metropolità, nacional o internacional.

Pel disseny actual es contempla un ample de banda entre sites de 10Gbps, utilitzant interfícies i tipus de connectors estàndard.

Les tecnologies òptiques s'utilitzen en combinació amb equips OTN (xarxa de transport òptic), Mux/Demux o Muxponder. El Muxponder és l'element que envia i rep la senyal òptica en una fibra. Ofereixen unes prestacions fixes i son completament transparents per protocols de capes OSI 2, 3 i de nivell superior. La latència no està subjecta a variació i depèn principalment de la distancia de fibra entre els dos extrems. Les tasses de pèrdues de trames/bits erronis i de fluctuació de fase es troben en els nivells tècnics mínims possibles. Com correspon a una xarxa òptica multiplexada.

L'arquitectura DWDM d'interconnexió es recolza en un nucli de xarxa òptic DWDM (Multiplexació Densa per Divisió de Longitud d'Onada).

Per aquest servei s'han dissenyat servei protegit (ruta de fibra òptica) i diversificats entre si.

Cada circuit DWDM presenta les següents característiques:

- Topologia: Punt a Punt
- Tecnologia: WDM
- Circuit 1 per la primera ruta (color verd) de longitud 72Km
- Circuit 2 per la segona ruta (color vermell) de longitud 75Km
- Ample de banda 10Gbps 100% garantits
- Entrega en finestra multimode (850nm) i interfície 1000BaseSR, connectats al bloc de Core Ethernet dels sites i per on s'estendran els serveis entre localitzacions.

3.6.1.3 Accés a Internet

Per les publicacions de serveis a INTERNET s'aprovisionaran circuits d'accés a la xarxa pública a cada una de les seus, tant al CPD primari com al secundari, sent les seves característiques principals:

CPD Primari:

- Connexió permanent a internet mitjançant: accés dedicat de fibra òptica
- Connexió a node de xarxa d'operador, realitzant-se el peering d'accés a Internet mitjançant el seu Sistema Autònom.
- Ample de banda de 100Mbps simètrics i 100% garantits.
- Router virtual d'accés gestionat des de l'operador.
- Aprovisionament de direccions IP de tipus PA (Provider Aggregatable).

CPD secundari:

- Connexió permanent a internet mitjançant: accés dedicat de fibra òptica
- Connexió a node de xarxa d'operador, realitzant-se el peering d'accés a Internet mitjançant el seu Sistema autònom.
- Ample de banda de 100Mbps simètrics i 100% garantits.
- Router virtual d'accés gestionat des de l'operador.
- Aprovisionament de direccions IP de tipus PA (Provider Aggregatable).

3.7 Infraestructura de seguretat

El disseny de la infraestructura de seguretat a nivell de CPD respon a les necessitats requerides pels sistemes que composen la solució i als requeriments identificats a nivell de disponibilitat del servei. En els següents punts es descriu el disseny proposat i les seves capacitats.

3.7.1 Descripció general

3.7.1.1 Entorn de seguretat permietral (NGFW)

La solució de seguretat que es descriu a continuació es replica de forma idèntica en els dos CPDs (principal i secundari).

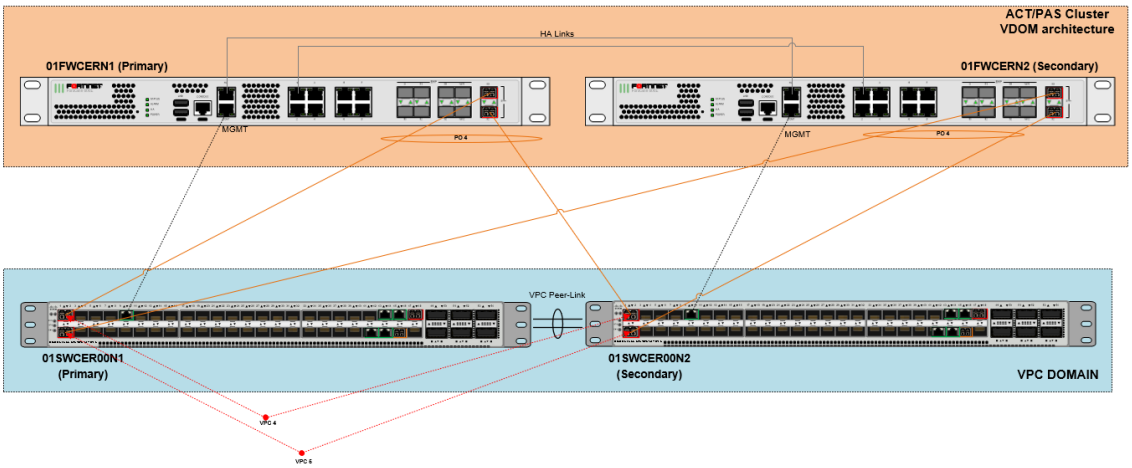
El disseny està concebut per mantenir l'alta disponibilitat dels elements que es protegeixen rere la infraestructura de seguretat que ho composen i protegeixen, a més d'oferir els amples de banda requerits per garantir un servei fiable i amb capacitat de creixement.

La infraestructura de seguretat la composen una parella de FORTINET Fortigate 601-E configurats en un model clúster Actiu/Passiu en alta disponibilitat i arquitectura de VDOMs (Firewalls Virtuals sobre la infraestructura física de Fortigate 601E). Els enllaços que estableixen aquest clúster son interfícies dedicades de 1Gbps en agregats conformant un Backbone d'alta disponibilitat de 2Gbps entre els dos equips.

Tots els enllaços d'interconnexió amb l'entorn de connectivitat ethernet s'estableixen mitjançant enllaços de 10Gbps en agregat.

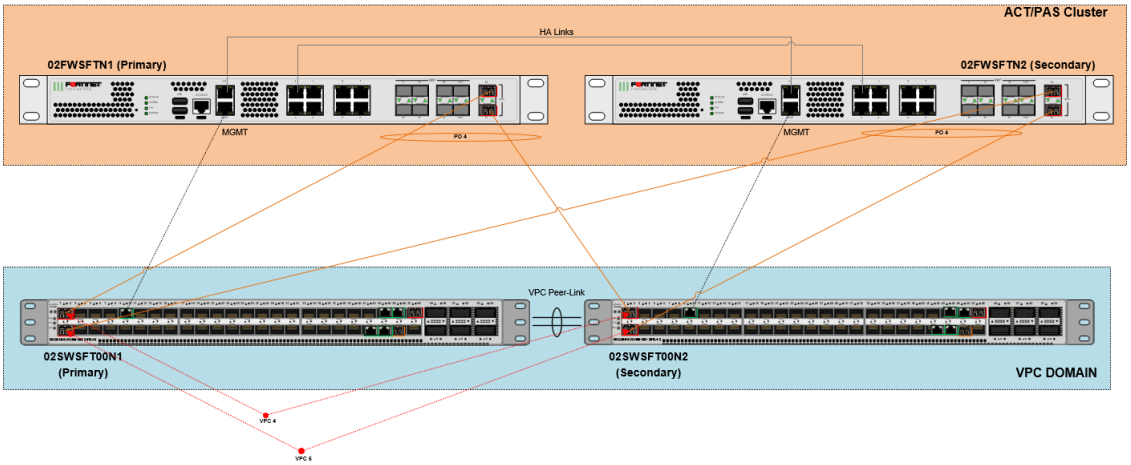
El disseny permet poder executar accions de manteniment de forma independent en els dos equips de forma individual i sense perdre la disponibilitat del servei que suporten. A nivell detallat, s'adjunten els esquemes de l'arquitectura contemplada per cada un dels CPDs.

- Disseny LLD infraestructura de seguretat CPD principal



Il·lustració 13 - Disseny LLD infraestructura de seguretat CPD principal

- Disseny LLD infraestructura de seguretat CPD secundari



Il·lustració 14 - Disseny LLD infraestructura de seguretat CPD secundari

Les capacitats tècniques de la plataforma Fortigate 601E que van a suportar el CPD primari son les següents:

Firewall	IPS	NGFW	Threat Protection	Interfaces
36 Gbps	10 Gbps	9.5 Gbps	7 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ Slots

Il·lustració 15 - Capacitats tècniques FG-601E

En base a tot l'entorn de seguretat descrit, les funcionalitats que es van desplegar en aquesta plataforma son:

Tallafocs (NGFW)

- Capacitat de filtrat avançat d'amenaces de seguretat a nivell d'aplicació.
- Enrutat avançat per navegació i alta disponibilitat
- Servei NAT avançat per publicacions de serveis
- Segmentació d'entorns productius i pre-productius
- Control d'accés avançat i anàlisis de tràfic IPS
- Servei de connectivitat VPN SSL
- Infraestructura VDOM per segmentació de serveis funcionals (producció, gestió i altres que es puguin requerir en un futur).

3.7.1.2 Entorn de seguretat WEB APPLICATION FIREWALL (WAF)

La solució de seguretat web que es descriu a continuació es replica de forma idèntica en els dos CPDs, principal i secundari.

El disseny està concebut per mantenir l'alta disponibilitat dels elements que es protegeixen rere la infraestructura de seguretat, a més d'oferir els amples de banda requerits per garantir un servei fiable i amb capacitat de creixement.

La infraestructura de seguretat web (WAF) la composen una parella de FORTINET Fortiweb 1000E configurats en un model clúster Actiu/Passiu en alta disponibilitat i arquitectura de ADOMs (Firewalls Virtuals sobre la infraestructura física de Fortiweb 1000E) en modalitat "Proxy Reverso", permetent el màxim de funcionalitats permeses per la plataforma, així com la capacitat de inspecció avançada de tot el tràfic HTTP/S de publicacions de aplicacions web.

Features:

Deployment options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

Web Security

- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP Reputation
- IP Geolocation
- HTTP RFC compliance

Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)

Security Services

- Web services signatures
- XML protocol conformance
- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie poisoning protection
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Protection

Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP and RADIUS support
- SSL client certificate support

Management and Reporting

- Web user interface
- Command line interface
- Central management for multiple devices
- REST API
- Centralized logging and reporting
- Real-time dashboards
- Bot dashboard
- Geo IP Analytics
- SNMP, Syslog and email Logging/Monitoring
- Administrative Domains with full RBAC

Other

- IPv6 Ready
- HSM Integration
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- Predefined security policies for Drupal and Wordpress applications

Il·lustració 16 - Features WAF

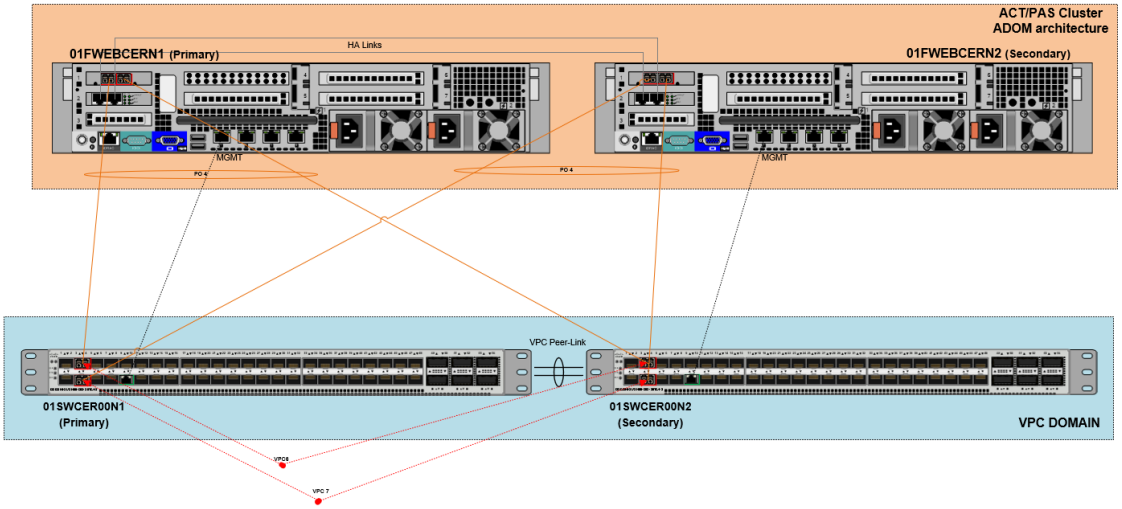
S'aplicaran tots els mecanismes de seguretat òptims, segons cada un dels serveis publicats i que aporten un nivell de seguretat suficient que asseguri el correcte funcionament de l'aplicació exposada i el control de les amenaces de la que puguin ser objecte. El perfilat de mecanismes de seguretat avançada, s'haurà d'analitzar en el moment de la seva migració i previ procés de testeig dins de la plataforma.

En referencia a l'arquitectura de connectivitat de l'entorn o bloc de seguretat WAF: Els enllaços que estableixen aquest clúster son interfícies dedicades de 1Gbps en agregat conformant un

backbone d'alta disponibilitat de 2Gbps entre els dos equips. Tots els enllaços d'interconnexió amb l'entorn de connectivitat s'estableixen mitjançant enllaços de 10Gbps en agregat.

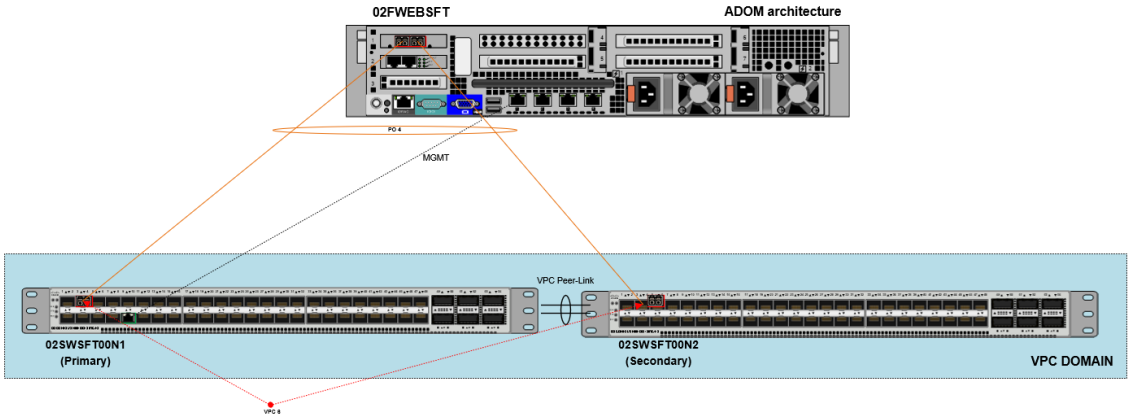
El disseny permet poder executar accions de manteniment de forma independent en els dos equips de forma individual i sense perdre la disponibilitat del servei que suporta. A nivell detallat, s'adjunten els esquemes detallats de l'arquitectura contemplada per cada un dels CPDs (primari i secundari).

- Disseny LLD infraestructura de seguretat del CPD Primari:



Il·lustració 17 - Disseny LLD infraestructura de seguretat del CPD Primari

- Disseny LLD infraestructura de seguretat del CPD secundari:



Il·lustració 18 - Disseny LLD infraestructura de seguretat del CPD Secundari

Cal destacar que l'entorn del CPD secundari contempla un únic element de seguretat WAF en format standalone amb rèplica asíncrona de la configuració de l'entorn productiu del site

primari. Aquesta sincronització es realitzarà cada 1 hora i permetrà evitar errors humans en la rèplica de configuracions entre els entorns de producció i el sistema WAF secundari.

3.7.1.3 Elements del bloc de seguretat

Descripció de elements del bloc de seguretat del servei:

Descripció	Uds
FortiGate-601E Hardware plus 24x7 Forticare and FortiGuard Unified Thread Protection (UTP)	2
FortiWeb-1000E Hardware plus 24x7 FortiCare and FortiWeb Standard Bundle	3
FortiGate-500E Hardware plus 24x7 Forticare and FortiGuard Unified Thread Protection (UTP)	2

Taula 4 - Equipament bloc de seguretat

3.7.2 Resiliència de l'entorn de seguretat

El disseny contemplat per l'entorn del bloc de seguretat contempla tots els mecanismes d'alta disponibilitat que la plataforma recomana i que es descriu en les següents característiques:

- Entorn d'alta disponibilitat en arquitectura Actiu/Passiu. Dotant de redundància a totes capacitats de seguretat avançada que aprovisionin des del bloc de seguretat perimetral i WAF en el CPD primari i secundari.
- Enllaços redundants cap a l'entorn de connectivitat ethernet (CORES Ethernet). Garantint la màxima disponibilitat en cas de caiguda des de qualsevol element extern de connectivitat interna del CPD
- Garantia de l'ús d'ample de banda a les interfícies d'interconnexió.
- Control dels mecanismes operatius d'aplicació de configuracions en el site primari cap al site secundari.
- Enrutament avançat per poder activar de forma àgil mecanismes de contingència davant eventualitats o incidències que poden comprometre el servei.
- Control avançat davant alertes de seguretat que requereixin d'un anàlisi profund i mitigació immediata.

La infraestructura del bloc de seguretat (NGFW i WAF), està dissenyada per poder encaminar els fluxos de tràfic entrants i sortints de forma eficient aplicant mecanismes d'encaminament avançat que permeten poder activar el pla de contingència del site primari de forma eficient i en base al pla del CPD secundari establint el servei.

4 CONFIGURACIONS

A continuació es farà una descripció de les configuracions més rellevants implantades en els equips de xarxa. Nomes es mostrarà les configuracions dels equips ubicats en el CPD principal.

4.1 Firewall

A continuació es mostrarà pas a pas la configuració feta en el Firewall. Primer de tot es mostrarà la configuració "global" de l'equip (configuració que s'aplica a totes les VDOMs) i seguidament la especifica de cada VDOM.

4.1.1 VDOMS

Una VDOM és una funcionalitat que ofereix Fortinet que ens permet crear instancies separades. Aquestes instancies actuen com Firewalls independents, i es poden configurar de manera independent.

INET_ACCESS		Profile-based	NAT	Enabled
MGMT		Profile-based	NAT	Enabled
root		Profile-based	NAT	Enabled

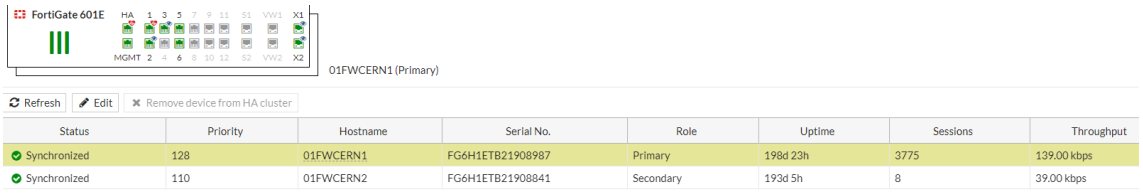
Il·lustració 19 - VDOMs Firewall

S'han creat 3 VDOMs diferents per separar el tràfic i els recursos de l'equip:

- INET_ACCESS: Aquesta VDOM és la que s'utilitza pel tràfic de servei. Aquí estan definides totes les VLANs per donar el servei i la sortida cap a internet.
- MGMT: Aquesta és una VDOM de gestió. Per aquesta VDOM passarà el tràfic de gestió de tot l'equipament de xarxa.
- Root: Aquesta és la VDOM per defecte del dispositiu. S'ha utilitzat per gestionar l'alta disponibilitat dels equips.

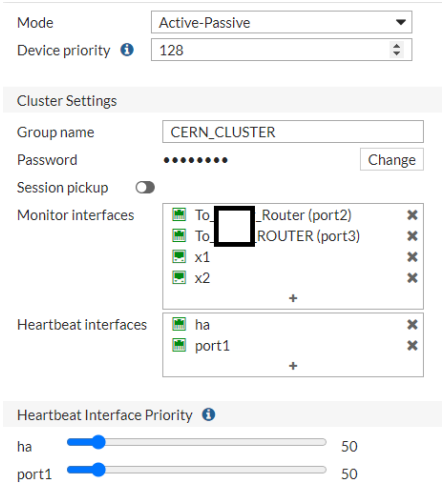
4.1.2 HA (Alta disponibilitat)

El HA (Alta disponibilitat) és la funció que ens permet interconnectar i sincronitzar diferents equips Fortigate entre si per tenir redundància davant possibles fallades i major capacitat de processament. L'equip primari sincronitza la configuració amb els altres.



Il·lustració 20 - HA Firewall

Es pot veure un resum de l'estat del HA dels equips. L'equip 01FWCERN1 és el que actualment està com a primari i actiu. Dels dos equips és el que més prioritat té i el que més temps porta com actiu (uptime).



Il·lustració 21 - Configuració HA Firewall

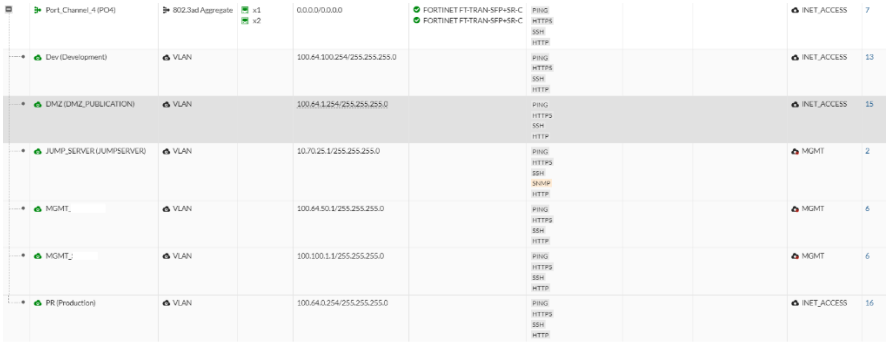
Dins de la configuració del HA podem veure les següents característiques:

- Mode: Indica que el HA està configurat en mode Actiu – Passiu.
- Group name: Indica el nom del grup de Firewalls que estan en HA.
- Password: És la contrasenya per entrar dins del grup de HA.
- Monitor interfaces: Són les interfícies que el HA monitoritza per veure la disponibilitat. En cas de caiguda d'alguna de les interfícies, el clúster es reorganitza, i balanceja la seva activitat cap al Firewall que te mes enllaços actius. En aquest cas s'ha decidit monitoritzar les interfícies de sortida a internet i les interfícies x1 i x2, que son les dues interfícies de 10Gb que connecten amb el switch i creen el port-channel per on passen totes les VLANs de servei.
- Heartbeat Interfaces: Son les interfícies per on el HA parla entre els dispositius. Aquestes interfícies estan connectades directament entre els dos equips.

- Heartbeat Interface Priority: És la prioritat que se li dona a cada port de HA. En aquest cas és la mateixa, per tant primàriament utilitzarà la interfícies de ha ja que està més amunt a la llista.

4.1.3 Interfícies

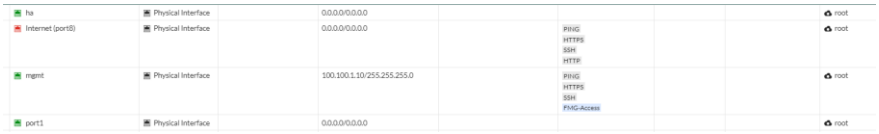
A continuació es mostren les interfícies creades en el FW i la VDOM a la que s'ha assignat cada interfície.



Il·lustració 22 - Interfícies Firewall

A les interfícies físiques X1 i X2 s'ha creat el port-channel PO4. Dins d'aquesta interfícies s'han creat les subinterfícies de servei i managment. Cada subinterficie té assignada una IP, que farà de gateway de la xarxa, i un tag de VLAN:

- Dev (Development): Se li ha assignat el tag de VLAN 350, i se li ha assignat la IP 100.64.1.254/24
- DMZ (DMZ_PUBLICATION): Se li ha assignat el tag 601, i se li ha assignat la IP 100.64.1.254/24
- JUMP_SERVER (JUMPSERVER): Se li ha assignat el tag 510, i se li ha assignat la IP 10.70.25.1/24. Aquesta és una interfície que actualment no està desenvolupada. En un futur està preparada per instal·lar-hi servidors de salt per si el client ho necessita.
- MGMT_X: Se li ha assignat el tag 500, i se li ha assignat la IP 100.64.50.1/24. Aquesta és una interfície perquè una 3a empresa es pugui connectar als servidors via VPN
- MGMT_Y: Se li ha assignat el tag 600, i se li ha assignat la IP 100.100.1.1/24. Aquesta és una interfície perquè una 3a empresa es pugui connectar a la gestió dels equips de xarxa via VPN.
- PR (Production): Se li ha assignat el tag 250, i se li ha assignat la IP 100.64.0.254/24



Il·lustració 23 - Interficies mgmt Firewall

També s'ha configurat el port de mgmt, que és el port al qual s'accedeix a l'administració del Firewall. En aquest port se li ha donat la IP 100.100.1.10/24

Els ports de ha i port1 son els dedicats a l'alta disponibilitat, hi no tenen cap configuració especial, ja que estan assignats a l'apartat de HA.

Per últim tenim els ports de sortida a internet. El port 3 és el que connecta amb el router de l'empresa proveïdora d'internet i per on s'encamina tot el tràfic de servei. Aquest port té una IP 213.229.151.254/25, que és una xarxa que gestiona el propi proveïdor.

Actualment també hi ha un port (port 2) de sortida internet dedicat amb l'empresa que està fent la instal·lació del projecte, per tal de tenir accés directe mitjançant una VPN.

4.1.4 VDOM INET_ACCESS

A continuació s'explica la configuració especifica de la VDOM INET_ACCESS, que és l'encarregada del tràfic de servei.

4.1.4.1 Static Routes

La ruta estàtica mostra el camí per defecte per encaminar el tràfic cap a qualsevol xarxa que no tingui especificada el propi Firewall.

0.0.0.0/0	213.229.151.129	To _ROUTER (port3)	Enabled

Il·lustració 24 - Rutes estàtiques Firewall

S'especifica que el següent salt és la IP 213.229.151.129 i que ha d'anar per la interfície on està connectat el router de sortida. Aquesta IP correspon a la del router del proveïdor extern.

4.1.4.2 Objects

Aquest apartat es troba dins del menú de "Policy & Objects" Addresses.

h-100.64.50.23	100.64.50.23/32
h-100.64.50.24	100.64.50.24/32
ibm1	129.33.206.139/32
ibm2	204.146.30.139/32
ibm3	170.225.126.11/32

Il·lustració 25 - Objects Firewall

Aquí es creen els objectes que després es podran utilitzar. Un objecte pot ser una IP, un nom DNS (FQDN), un rang d'IPs, una subxarxa o una localització. En l'exemple de la imatge son IPs concretes.

Tots els objectes s'han creat perquè puguin ser visibles des de totes les VDOMs.

4.1.4.3 Virtual IPs

S'utilitza per fer un NAT estàtic. Un NAT estàtic és quan una mateixa IP privada es tradueix sempre en una mateixa IP pública. Per tant quan al Firewall entri una petició cap a una IP pública com la 213.229.151.145, el Firewall automàticament farà la traducció a un IP privada com la 100.64.1.15, i el tràfic que gestiona cap dins serà amb la IP privada.

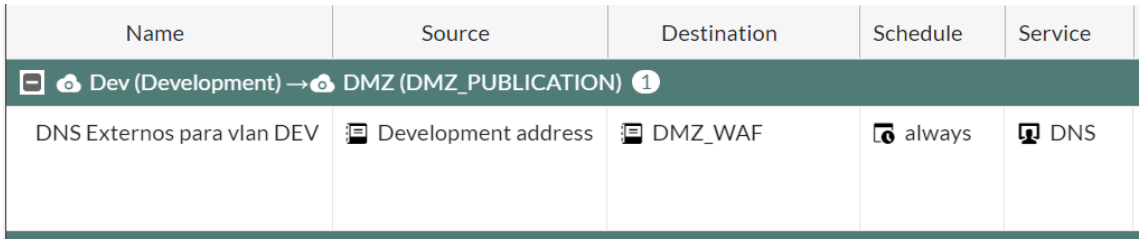
4.1.4.4 Security Profiles

Els perfils de seguretat son un grup d'opcions i filtres que es poden aplicar a les polítiques de seguretat del Firewall. Aquests permeten inspeccionar el tràfic que passa per la política en busca de accions que no es desitjant. De moment s'han configurat per defecte. Els perfils utilitzats son:
Antivirus: S'utilitza per la protecció contra la transmissió de codi maliciós.

- Web filtering: Observa les sol·licituds web i si la URL està en un llistat malicós actualitzada per fortinet, la connexió no es permetrà.
- Application control: Detecta les aplicacions que s'estan utilitzant a la xarxa i denega les especificades o les que considera poc segures.
- Intrusion Protection (IPS): Busca activitat o comportaments que estiguin relacionats amb atacs de seguretat o explotació de vulnerabilitats.

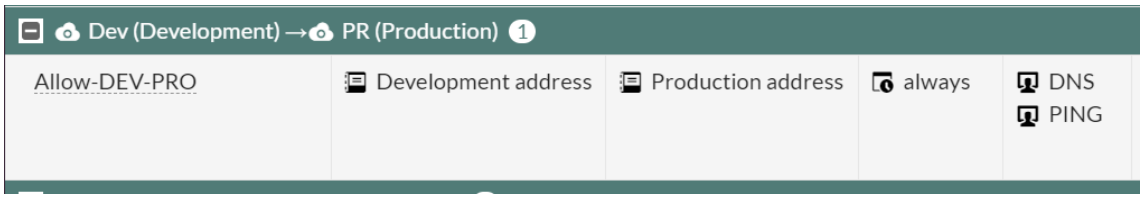
4.1.4.5 Firewall Policy

Aquí és on es defineixen les polítiques de tràfic que el Firewall permetrà o denegarà. En aquest cas s'han definit polítiques per permetre el tràfic, i tot el tràfic que no està explícitament permès serà denegat per un "DENY" implícit al final. Les polítiques estan organitzades per xarxa d'entrada i xarxa de sortida. Les polítiques implementades en un primer moment són:



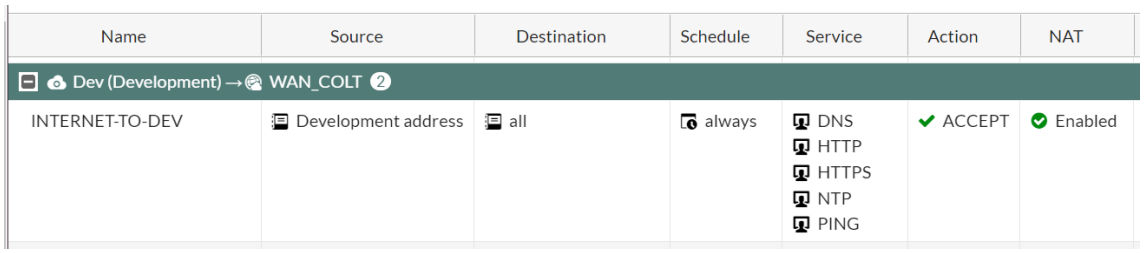
Il·lustració 26 - Política 1 Firewall

Es permet el tràfic DNS des de la xarxa de desenvolupament cap a la xarxa de publicació del WAF.



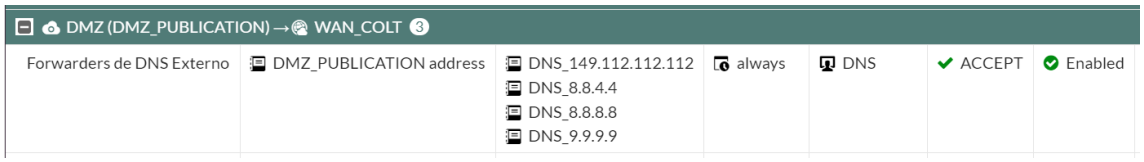
Il·lustració 27- Política 2 Firewall

Es permet el tràfic DNS i PING des de la xarxa de desenvolupament cap a la xarxa de producció.



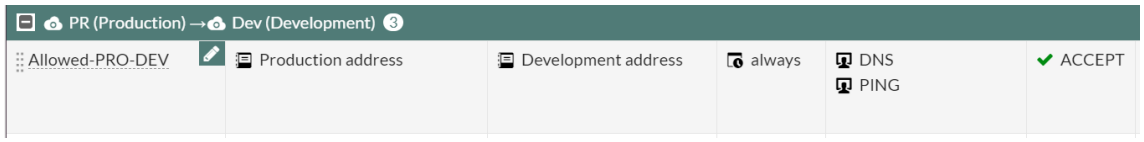
Il·lustració 28 - Política 3 Firewall

Es permet el tràfic DNS, HTTP, HTTPS, NTP i PING des de la xarxa de desenvolupament cap a internet.



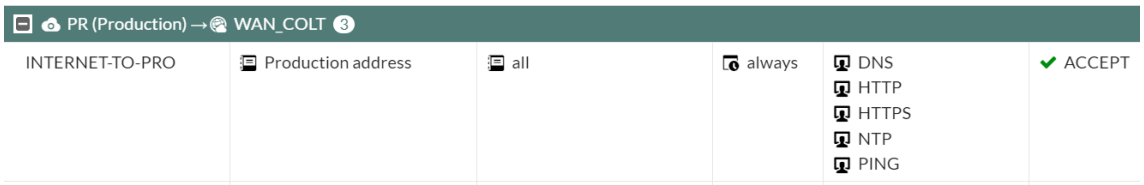
Il·lustració 29 - Política 4 Firewall

Es permet el tràfic DNS des de la xarxa de publicació cap a unes direccions de DNS públics de internet.



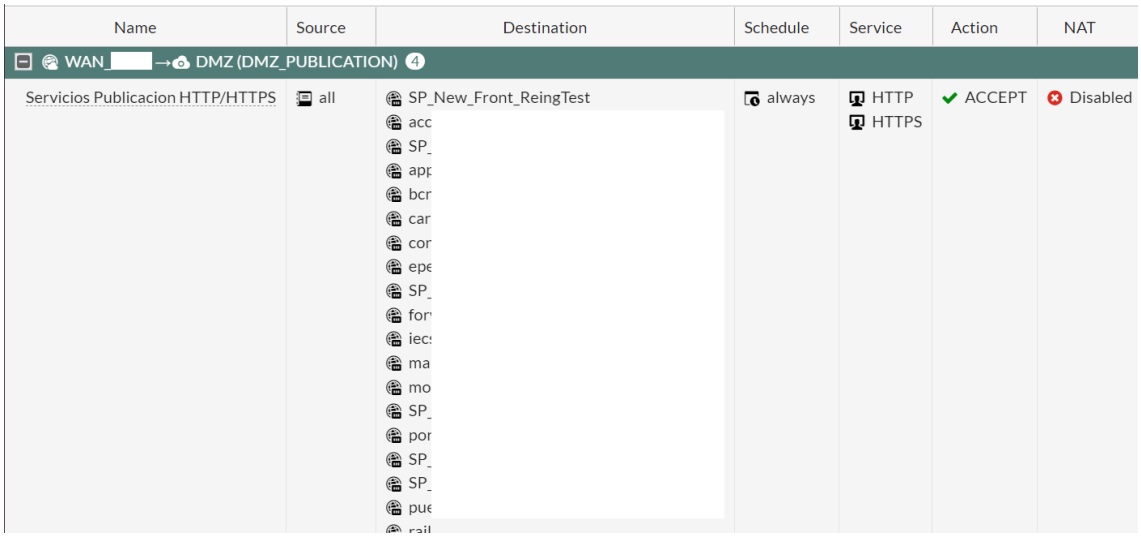
Il·lustració 30 - Política 5 Firewall

Es permet el tràfic DNS i PING des de la xarxa de producció cap a la xarxa de desenvolupament.



Il·lustració 31 - Política 6 Firewall

Es permet el tràfic DNS, HTTP, HTTPS, NTP i PING des de la xarxa de producció cap a internet.



Il·lustració 32 - Política 8 Firewall

Aquí és l'únic tràfic que es permet des d'internet. Es permet el tràfic d'internet que vingui per HTTP o HTTPS cap a unes direccions especificades de serveis que s'estan publicant.

Il·lustració 33 - Política 9 Firewall

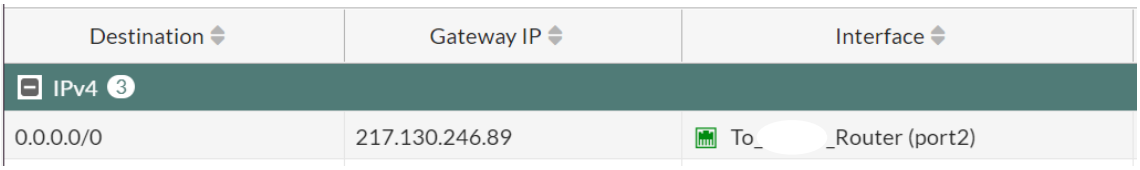
La resta del tràfic serà denegat pel DENY implícit.

També s'ha configurat el NAT per tot el tràfic entre xarxes i de sortida cap a internet. Aquest NAT es farà amb la IP de la interfície de sortida de la política.

4.1.5 VDOM MGMT

A continuació s'explica la configuració especifica de la VDOM MGMT, que és l'encarregada del tràfic de gestió de tot l'equipament de xarxa.

4.1.5.1 Static Routes



Il·lustració 34 - Ruta estàtica

S'especifica que el següent salt d'aquesta VDOM és la IP 217.130.246.89 i que ha d'anar per la interfície on està connectat el router de sortida que connecta directament amb la xarxa de l'empresa que realitza aquest servei.

4.1.5.2 Objects

Tots els objectes s'han creat perquè pugui ser visibles des de totes les VDOMs, per tant en aquest apartat es veuran els mateixos objectes que a la VDOM INET_ACCESS. En cas de crear un objecte nou també es veuria a les altres VDOMs.

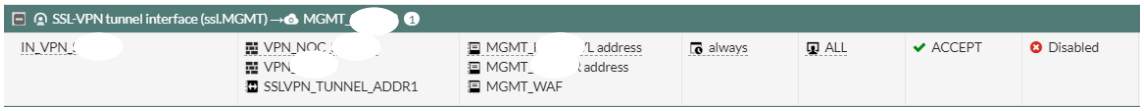
4.1.5.3 SSL-VPN

En aquesta VDOM s'ha configurat una SSL-VPN per l'empresa que gestiona l'equipament de xarxa. Una VPN-SSL és una xarxa privada virtual que utilitza el protocol SSL per crear una connexió segura i xifrar a través de la xarxa el tràfic que passa per internet.

Els usuaris remots que utilitzen la SSL-VPN accedeixen mitjançant la IP externa del router dedicat i utilitzant el FortiClient, un software de Fortinet per aquesta finalitat.

En aquest cas per un tema de seguretat no es mostrarà la configuració.

4.1.5.4 Firewall Policy



Il·lustració 35 - olítica de MGMT

En aquest cas només hi ha una política, que permet tot tipus de tràfic des del SSL-VPN túnel cap a les adreces de gestió de l'equipament de xarxa.

Tota la resta del tràfic està denegat.

4.1.6 VDOM root

La VDOM root s'ha utilitzat per assignar les interfícies de HA. Al només tenir aquestes interfícies, que la configuració es fa de forma global, no te cap configuració addicional.

4.2 Switch

A continuació es mostrarà pas a pas la configuració feta en els switchos Cisco Nexus.

4.2.1 Hostname i VDC

hostname 01SWCER00N1 *vdc 01SWCER00N1 id 1*	*hostname 01SWCER00N2* *vdc 01SWCER00N2 id 1*

En la primera línia s'especifica el hostname de l'equip. En aquest cas, els switchos es diran 01SWCER00N1 i 01SWCER00N2.

El VDC es refereix al "Virtual Device Context", que permet crear diferents switchos virtuals dins del mateix switch físic. En aquest cas només tindrem un únic switch virtual, i se li dona el id 1.

4.2.2 Limit-Resource

```
limit-resource vlan minimum 16 maximum 4094
limit-resource vrf minimum 2 maximum 4096
limit-resource port-channel minimum 0 maximum 511
limit-resource u4route-mem minimum 248 maximum 248
limit-resource u6route-mem minimum 96 maximum 96
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
```

En aquest cas es mostra una sola configuració ja que és idèntica en els dos switchos.
Les comandes de "límit-resource" poden establir límits de valors màxims i mínims pels recursos del dispositiu físic quan es crea un VDC.

- limit-resource vlan: S'estableix que el valor mínim d'una VLAN serà 16 i el màxim 4094. No podrà haver-hi VLANs amb un tag superior o inferior al descrit
- limit-resource vrf: S'estableix que el número de vrfs estarà entre 2 i 4096.
- limit-resource port-channel: S'estableix que el número de port-channel creats poden ser de mínim 0 i màxim 511.
- limit-resource u4route-mem: S'estableix en MegaBytes, els recursos de mémoria del mapa de rutes unicast IPv4 assignats al VDC. En aquest cas es fixe en 248Mb.
- limit-resource u6route-mem: S'estableix en MegaBytes, els recursos de mémoria del mapa de rutes unicast IPv6 assignats al VDC. En aquest cas es fixe en 96Mb.
- limit-resource m4route-mem: S'estableix en MegaBytes, els recursos de mémoria del mapa de rutes multicast IPv4 assignats al VDC. En aquest cas es fixe en 58Mb.
- limit-resource m6route-mem: S'estableix en MegaBytes, els recursos de mémoria del mapa de rutes multicast IPv6 assignats al VDC. En aquest cas es fixe en 8Mb.

4.2.3 RMON

```
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO
```

S’estableixen les diferents categories de events rmon que hi haurà.

4.2.4 SNMP

```
snmp-server user admin network-admin auth md5 XXX priv XXX localizedkey
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
snmp-server enable traps aaa server-state-change
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended
snmp-server enable traps config ccmCLIRunningConfigChanged
snmp-server enable traps snmp authentication
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps vtp notifs
snmp-server enable traps vtp vlancreate
snmp-server enable traps vtp vlandelete
snmp-server enable traps bridge newroot
snmp-server enable traps bridge topologychange
snmp-server enable traps stpx inconsistency
snmp-server enable traps stpx root-inconsistency
snmp-server enable traps stpx loop-inconsistency
snmp-server enable traps system Clock-change-notification
snmp-server enable traps feature-control ciscoFeatOpStatusChange
snmp-server enable traps mmode cseNormalModeChangeNotify
snmp-server enable traps mmode cseMaintModeChangeNotify
snmp-server enable traps syslog message-generated
snmp-server community portic group network-operator
```

En la primera línia s’estableix un usuari per SNMP.

Seguidament es configuren els traps SNMP. Els traps SNMP son notificacions d'alertes sobre els tipus activats. Per exemple en aquest cas s'activen els traps de:

- vtp vlandelete: En aquest cas es notificarà quan s'elimini una VLAN.
- aaa server-state-change: En aquest cas s'enviará el trap quan el servidor d'autenticació (RADIUS, TACACS) canviï d'estat.

4.2.5 IP Route

```
ip route 0.0.0.0/0 100.100.1.1
```

Amb aquesta comanda es defineix la ruta per defecte del swtich. Tot el tràfic que no tingui definit en cap altre ruta, l'enviarà cap a la direcció IP 100.100.1.1, que correspon a la xarxa interna del Firewall.

4.2.6 VLAN

```
vlan 1-2,250,350,500-503,510,600-602,801,1200
vlan 250
 name Produccion
vlan 350
 name Desarrollo
vlan 500
 name Gestion
vlan 501
 name Gestion_LinuxONE_CER
vlan 502
 name FC-IP
vlan 503
 name RAC-Oracle
vlan 600
 name MGMT_COMMs
vlan 601
 name DMZ_PUBLICATION
vlan 602
 name SYNC_CONF_PRE
vlan 801
 name GSNI_INTERCONNECt
vlan 1200
 name Backup
```

En aquest apartat es defineixen totes les VLANs del switch. En la primera VLAN es mostren totes les VLANs creades, i seguidament es mostra cada VLAN amb la seva descripció.

4.2.7 Spanning-Tree

```
spanning-tree port type edge bpduguard default
spanning-tree vlan 1-1300 priority 0
```

La primera comanda activa BPDU GUARD de forma predeterminada a tots els ports de capa 2.
En la segona comanda se li dona la màxima prioritat a totes les VLANs de la 1 a la 1300.

4.2.8 VRF

```
vrf context management
```

En la primera línia es defineix el VRF managment. Els VRF és una tecnologia que permet tenir més d'una taula d'encaminament en un sol enrutador.

4.2.9 VPC Domain

```
vpc domain 10
  role priority 16000
  peer-keepalive destination 100.100.1.201 source 100.100.1.200
  delay restore 360
  peer-gateway
ip arp synchronize
```

```
vpc domain 10
  role priority 16000
  peer-keepalive destination 100.100.1.200 source 100.100.1.201
  delay restore 360
  peer-gateway
ip arp synchronize
```

En aquest apartat es crea el domini VPC. El VPC (Virtual Port Channel) permet que els enllaços físics connectats a dos switchos CISCO diferents, apareixin com un sol canal de ports a un tercer dispositiu. Per tant els dos switchos poden funcionar com un sol, però es gestionen cada un per separat. En aquest cas s'identifica aquest VPC amb el domini 10.
El role priority li assigna un valor de prioritat per ser el VPC principal. En aquest cas els dos switchos tenen el mateix valor i qualsevol dels dos pot ser el VPC principal.
El peer-kkepalive destination monitoritza que l'altre VPC està actiu. En aquest cas se li especifica que es fa entre les dues IPs de gestió.
El delay restore s'utilitza per retardar el temps que s'envien paquets pel peer link, en aquest cas 360 segons. Això evita pèrdua de paquets.
El peer-gateway permet que el switch VPC actui com a porta d'enllaç pels paquets que es dirigeixen a la direcció MAC del peer de VPC.

L'IP arp synchronize permet una convergència més ràpida de les taules d'adreçament entre VPCs.

4.2.10 Interface VLAN

interface Vlan1 *no ip redirects* *no ipv6 redirects* *interface Vlan600* *description Gestion* *no shutdown* *no ip redirects* *ip address 100.100.1.200/24* *no ipv6 redirects*	*interface Vlan1* *no ip redirects* *no ipv6 redirects* *interface Vlan600* *description Gestion* *no shutdown* *no ip redirects* *ip address 100.100.1.201/24* *no ipv6 redirects*

A la interface vlan 1 no se li aplica cap configuració en cap dels dos dispositius.
La interface vlan600 és la vlan de gestió de l'equip en els dos dispositius. Es pot veure com el primer te la IP 100.100.1.200 i el segona la IP 100.100.1.201. Les dos interface tenen una descripció "Gestion". El no shutdown indica que la interface vlan està activa. Les comandes no ip redirects indiquen que el swtich no reencaminarà paquets ICMP tant de IPv4 com de IPv6, tot i que conegui un camí millor.

4.2.11 Port-Channel

Un port-channel és una agregació de ports que permet balancejar el tràfic entre diferents ports i permet augmentar l'ample de banda, augmentar la redundància i evitar problemes de bucles.
En aquest cas a cada port-channel se li assigna un vpc diferent ja que els port-channels estan fets entre dos switchos diferents. Perque això funcioni, els dos ports channel creats en els dos switchos han de tenir el mateix vpc id.

interface port-channel4 *description 01FWCERN1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 4* *interface port-channel5* *description 01FWCERN2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 5*	*interface port-channel4* *description 01FWCERN1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 4* *interface port-channel5* *description 01FWCERN2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 5*

Els port-channel 4 i 5 corresponen a les connexions amb els Firewalls. Veiem que son dos ports en mode trunk, això vol dir que deixaran passar diferentes vlan i les etiquetaran amb el tag corresponent. Cada port-channel te el seu vpc que correspon amb el de l'altre switch. Aquestes dues interfícies deixen passar les vlan 250, 350, 500 i de la 600 a la 601, que corresponen a les diferents zones del Firewall, on se'ls hi dona aquest tag.

interface port-channel6 *description 01FWEBCERMGMTN1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 6* *interface port-channel7* *description 01FWEBCERMGMTN2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 7*	*interface port-channel6* *description 01FWEBCERMGMTN1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 6* *interface port-channel7* *description 01FWEBCERMGMTN2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *vpc 7*

Els ports-channel 6 i 7 corresponen a les connexions amb els FortiWeb. Igual que en el cas anterior son ports trunk i deixen passar les vlan 250, 350, 500 i de la 600 a la 601.

interface port-channel10 *switchport* *switchport mode trunk* *spanning-tree port type network* *vpc peer-link* *interface port-channel20* *description 02SWSFT00N - Po20* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,502-503,600,1200* *vpc 20*	*interface port-channel10* *switchport* *switchport mode trunk* *spanning-tree port type network* *vpc peer-link* *interface port-channel20* *description 02SWSFT00N - Po20* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,502-503,600,1200* *vpc 20*

El port channel 10 correspon al vpc peer-link. Aquest port channel és la unió entre els dos switchos, i el port que fa que puguin funcionar com un de sol.

El port channel 20 és el corresponent a la unió entre els dos CPDs. Per aquest enllaç es passen totes les VLANs a nivell 2, per garantir la redundància en cas de fallada.

4.2.12 Ports

En aquest apartat es descriurà la configuració d'alguns ports físics.

interface Ethernet1/1 *description 01FWCERN1 - X1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *channel-group 4 mode active* *no shutdown*	*interface Ethernet1/1* *description 01FWCERN1 - X2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *channel-group 4 mode active* *no shutdown*
interface Ethernet1/2 *description 01FWCERN2 - X1* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *channel-group 5 mode active* *no shutdown*	*interface Ethernet1/2* *description 01FWCERN2 - X2* *switchport* *switchport mode trunk* *switchport trunk allowed vlan 250,350,500,600-601* *channel-group 5 mode active* *no shutdown*

Aquests dos ports corresponen amb les connexions amb els firewalls. Veiem que els dos estan en mode trunk i deixen passar les mateixes VLANs.

La comanda channel-group X mode active, indica que aquest port pertany al port-channel X creat anteriorment. En concret els ports Ethernet 1/1 son membres del port-channel 4, i els ports Ethernet 1/2 son membres del port-channel 5. Al indicar que el channel-group està en "mode active" significa que s'utilitzarà l'estàndard LACP, un mètode de negociació dels ports que permet que els dos enllaços treballin activament amb el tràfic.

Per últim veiem que tots els ports estan actius per la comanda "no shutdown".

Aquesta configuració és molt semblant a la que tenen altres ports, per exemple, els que fan d'enllaç amb el FortiWeb, que la única diferencia serà el channel-group del que son membres.

```
interface Ethernet1/9
  description 01FWCERN1 - MGMT
  switchport
  switchport access vlan 600
  no shutdown
```

Aquesta interfície és la que va connectada al port de managment del Firewall. En aquest cas el port està en mode "access", que significa que només hi pot passar una vlan i els paquets no van etiquetats. En aquest cas s'hi passa la VLAN de gestió d'equipament de xarxa.

Altres ports que van connectats a dispositius finals, com ara alguns servidors, tenen una configuració molt similar, la única diferència és la VLAN que hi passa.

```
interface Ethernet1/47
  description CON CPD SEC
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 250,350,500,502-503,600,1200
  channel-group 20 mode active
  no shutdown
```

```
interface Ethernet1/47
  description CON CPD SEC
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 250,350,500,502-503,600,1200
  channel-group 20 mode active
  no shutdown
```

Aquests ports corresponen a la connexió a nivell 2 amb el CPD secundari. En aquest cas son membres del channel-group 20 que hem descrit anteriorment.

```
interface Ethernet1/51
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/52
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/53
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/54
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown
```

```
interface Ethernet1/51
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/52
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/53
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown

interface Ethernet1/54
  description vpc peer link
  switchport
  switchport mode trunk
  channel-group 10 mode active
  no shutdown
```

Aquests ports son els membres del vpc peer link. Aquests ports estan connectats entre ells (els d'un switch amb l'altre) i serveixen per crear el vpc. Com veiem son 4 ports per switch, cada port és de 10Gb, per tant el vpc tindrà un ample de banda de 40Gb.

interface mgmt0 *vrf member management* *ip address 100.100.1.200/24*	*interface mgmt0* *vrf member management* *ip address 100.100.1.201/24*

Aquest és el port de "management". En aquests ports s'especifica la direcció IP que serveix per gestionar l'equip. Se li posa la comanda vrf member management per indicar que aquest port correspon al vrf de managment, i la seva taula d'enrutament estarà separada de la resta.

4.3 WAF

A continuació es mostrarà la configuració del FORTIWEB. Actualment només disposa d'una ADOM assignada a la VLAN de DMZ Publication.

El mètode amb el que està configurat, el Firewall envia el tràfic dirigit cap al Fortiweb, ja que és ell qui te tota la xarxa. El fortiweb fa de balancejador de carrega, rep el tràfic dirigit a les seves VIP (virtual IPs) i el balanceja cap el servidor d'aplicació ubicats a la VLAN de producció. Per tant el tràfic torna cap el Firewall mitjançant la ruta per defecte del Fortiweb i el firewall l'encamina cap a la vlan corresponent.

Actualment només es disposa d'un equip actuant com StandAlone. Està pendent la instal·lació d'un segon equip FortiWeb per tenir redundància i que actuïn com actiu-passiu

4.3.1 GLOBAL

A continuació es mostra la configuració de l'ADOM GLOBAL. És qui te la configuració global de l'equip.

4.3.2 Interficies

Name	Members	IPv4	IPv4 Access Options	Status	Link Status	Type	Ref.
Aggregate 3							
Port_Channel_4	port11, port12	0.0.0.0/0	HTTPS PING SSH HTTP	Bring Down		Aggregate	2
MGMT_		100.100.1.253/24	HTTPS PING SSH HTTP FortiWeb Manager	Bring Down		VLAN	1
DMZ_PUBLICATION		100.64.1.253/24	HTTPS PING SSH HTTP	Bring Down		VLAN	39
Physical 12							
mgmt1		10.10.1.1/24	HTTPS PING SSH SNMP HTTP FortiWeb Manager	Bring Down		Physical	0

Il·lustració 36 - Interficies WAF

Actualment l'equip té habilitades 3 interficies. 2 formen una agregació, el Port_Channel 4, i on tenim 2 VLAN, la de la xarxa de publicació (Vlan 601) i la de gestió de l'equip (600).

També te habilitada la interfície de mgmt amb una IP 10.10.1.1/24.

4.3.2.1 Virtual IP

En aquest apartat s'han de crear totes les "Virtual IP" (VIP) que tindrà l'equip configurades.

7	SP_WEB32-webservicesdemo.portic.net	100.64.1.10/32	::/0	DMZ_PUBLICATION
8	SP_WEB57-reingdesa	100.64.1.11/32	::/0	DMZ_PUBLICATION

Il·lustració 37 - VIP WAF

S'ha de indicar un nom descriptiu, la IP que tindrà la VIP i la interfície a la que estarà assignada. En aquest cas totes les VIPs creades estan assignades a la interfícies de DMZ_PUBLICATION.

4.3.2.2 Routes

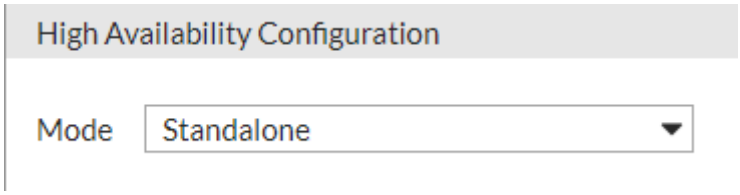
L'equip te definides dues rutes estàtiques.

#	IP/Mask(IPv4/IPv6)	Gateway(IPv4/IPv6)	Device
1	10.212.134.0/24	100.100.1.1	MGMT_S
2	0.0.0.0/0	100.64.1.254	DMZ_PUBLICATION

Il·lustració 38 - Rutes estàtiques WAF

La ruta estàtica 1 correspon a la ruta de gestió. La xarxa definida és la de la VPN de l'empresa que gestiona l'equipament de xarxa, i el gateway és la IP de la vlan de gestió (600).
La segona ruta estàtica és la ruta per defecte per tota la resta del tràfic. La IP del gateway correspon a la IP de la VLAN 601 del Firewall.

4.3.2.3 HA (Alta Disponibilitat)



Il·lustració 39 - HA WAF

Actualment l'equip està configurat com Standalone, que vol dir que només hi ha un equip, no hi ha redundància.

4.3.2.4 ADOMS

Les ADOMS (Administrative Domain) ens permeten crear instancies separades dins del mateix FortiWeb. En aquest cas només s'ha creat una instancia, la de "PRODUCTION".

Il·lustració 40 - ADOM Production WAF

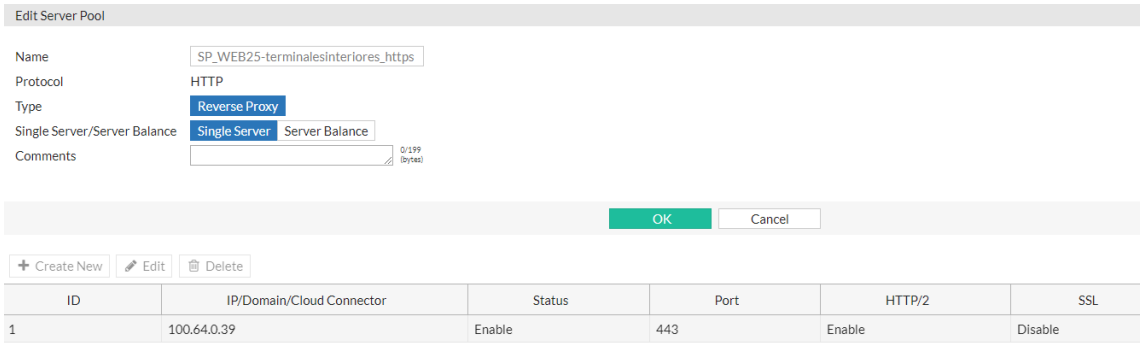
Dins d'aquesta instancia s'ha definit tota la configuració.

4.3.3 ADOM PRODUCTION

A continuació s'explica la configuració de l'ADOM PRODUCTION.

4.3.3.1 Server Pool

Dins dels server pool s'especifiquen els servidors que hi ha darrere de les virtual IP. Aquests grups contenen un o més membres que s'especifiquen utilitzant la IP o el nom DNS. Fortiweb protegeix aquests servidors web i son els destinataris del tràfic que FortiWeb reenvia o permet passar.



Il·lustració 41 - Server Pool WAF

Per cada VIP s'ha d'especificar un pool. A la imatge veiem un model de configuració. Primer s'ha de definir un nom, seguidament el protocol al que farà referencia. Seguidament s'ha de seleccionar si el pool serà:

- Single Server: El pool només tindrà un sol membre
- Server Balance: Hi haurà més d'un membre i la carrega es balancejarà entre els servidors.

Per últim hem de definir el servidor real al que enviarem el tràfic. S'ha de definir la IP del servidor, indicar a quin port se li reenviarà el tràfic, habilitar o deshabilitar les comunicacions HTTP/2 i indicar si la comunicació entre el FortiWeb i el servidor utilitzarà SSL/TLS.

4.3.3.2 Health Check

Els Health ckeck son els test que realitza el FortiWeb per saber si un servidor està operatiu o no. S'han definit els següents:

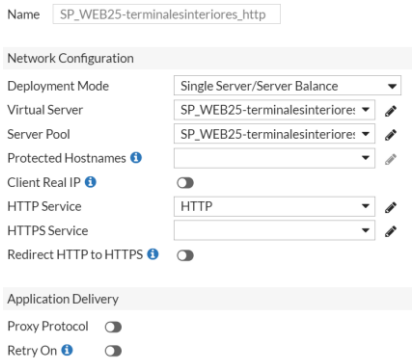
#	Name
Predefined 5	
1	HLTHCK_ICMP
2	HLTHCK_TCP
3	HLTHCK_TCP_HALF
4	HLTHCK_TCP_SSL
5	HLTHCK_HTTP

Il·lustració 42 - Health Check WAF

- HLTHCK_ICMP: Fa un ping al servidor. Si respon el dona com operatiu, en cas contrari el dona com caigut.
- HLTHCK_TCP: FortiWeb envia un TCP SYN al servidor i espera resposta. El servidor envia un TCP SYN ACK que indica resposta o fa timeout. Si s'envia el SYN ACK, el fotiweb envia un TCP ACK per completar el protocol d'enllaç a tres vies.
- HLTHCK_TCP_HALF: FortiWeb envia un TCP SYN al servidor i espera resposta. El servidor envia un TCP SYN ACK que indica resposta o fa timeout. Si s'envia el SYN ACK, el fotiweb envia un TCP RST per acabar la connexió. Aquesta verificació d'estat requereix menys recursos que la TCP.
- HLTHCK_TCP_SSL: Envia una sol·licitud HTTPS. El FortiWeb considera que el host respon si el protocol de enllaç SSL és exitós i tanca la connexió.
- HLTHCK_HTTP: Envia una sol·licitud HTTP i escolta una resposta que coincideixi amb els valors esperats. Si el contingut coincideix dona al servidor com actiu, si no coincideix el dona com caigut.

4.3.3.3 Server Policy

Aquí es fa la relació entre el Virtual Server i el Server Pool.



Il·lustració 43 - Server Policy WAF

S'ha de especificar el Virtual Server que es vulgui, i el Server Pool al que es vol reenviar el tràfic. S'ha d'indicar si la connexió amb el client és HTTP o HTTPS. En aquest cas és HTTP i no s'ha de especificar res més. Si la connexió fos HTTPS s'hauria d'especificar el certificat que se li serveix al client i el certificat entremig entre el FortiWeb i el servidor.

4.3.3.4 Security

A part de tot això el WAF aplica diferents perfils de seguretat a tot el tràfic que s'ha de reenviar cap als servidors reals. En aquest cas s'han deixat els perfils per defecte:

- Web Protection: Bloqueja les amenaces conegudes i de zero-day contra aplicacions sense bloquejar usuaris legítims i sense una sobrecarrega excessiva.
- API Protection: Protegeix les APIs compatibles amb les aplicacions mòbils i habilita les comunicacions B2B.
- Bot Mitigation: Bloqueja les activitats malicioses de bots sense bloquejar bots compatibles amb les necessitats legitimes de l'empresa, com motors de cerca o eines de monitoreig.
- DoS Protection: Identifica el tràfic potencialment perillós de ser un atac de denegació de servei mitjançant la cerca d'anomalies. Aquestes anomalies inclouen:
    - Inundacions de TCP SYN
    - Inundacions UDP
    - Inundacions ICMP
    - Escaneig de ports TCP
    - Atac de sessions TCP
    - Atac de sessions UDP
    - Atac de sessions ICMP
- IP Protection: Es poden bloquejar les sol·licituds dels clients en funció de la seva direcció IP d'origen, la seva reputació actual coneguda per FortiGuard, el país d'origen o la regió a la que està associada la direcció IP.

5 Conclusions

L'objectiu d'aquest treball era dissenyar una transformació d'una xarxa de comunicacions d'un CPD i implantar-la. Per arribar a aquest objectiu s'ha hagut d'estudiar quina xarxa tenien fins ara i s'han hagut d'identificar les necessitats que podia tenir el client.

Un cop analitzats tots aquests aspectes s'ha dissenyat una xarxa que intentes complir amb les necessitats del client i argumentant del perquè de cada decisió presa. S'han hagut d'estudiar diferents situacions i diferents solucions per tal d'arribar a la que més s'adequa en aquest cas. D'aquí hem pogut extreure que el món de les telecomunicacions, i més concretament el món de la telemàtica, està en constant canvi, i ara mateix, hi ha moltes possibilitats per arribar a obtenir el resultat objectiu. Actualment tenim a l'abast molts fabricants per a cada capa, que ofereixen diferents possibilitats i diferents recursos. En aquest cas ens hem quedat amb els que creiem que s'adequaven millor a la situació del client, i amb els que s'ha vist que els resultats estan contrastats.

Per últim, en aquest projecte es pretenia implantar completament el disseny proposat. Es volien instal·lar tots els equips i deixar tots els sistemes funcionant. Això no ha estat possible, tot i que el resultat final s'ha pogut veure, mostrant les configuracions dels equips, en la part real del projecte no s'han pogut instal·lar físicament els equips per deixar el CPD secundari funcionant. Això ha estat per causes alienes a aquest projecte. Llavors tot i que s'ha arribat a assolir l'objectiu de veure el projecte configurat i funcionant, no s'ha pogut veure el disseny completament muntat i operatiu.

Del global del projecte podem extreure que degut al constant canvi i millores de la tecnologia, tant empresarial com de punts finals, les telecomunicacions s'han d'adaptar constantment i estar preparades davant noves situacions que es puguin oferir. En aquest projecte s'ha intentat abastar això, deixant un disseny que compleix tots els requisits actuals i possibles nous requeriments futurs que pugui tenir el client.

Tot i això sempre hi ha punts de millora amb la tecnologia de les telecomunicacions. Aquest projecte encara pot avançar més. Les línies de treball d'un futur proper podrien anar encaminades en la millor del CPD secundari, posant el mateix tipus de Firewall que en el primari i afegint un segon FortiWeb per tenir més redundància. D'aquesta manera els dos CPDs seria exactament iguals, i l'empresa podria balancejar el tràfic d'un CPD a l'altre sense cap tipus d'afectació.

Una línia de treball més futura pot ser la de anar cap a un disseny al Cloud. El projecte seria el de pujar tots els servidors a una plataforma al núvol i gestionar totes les comunicacions des d'una plataforma virtual. Actualment ja s'estan adaptant d'aquesta manera, ja que amb l'oferta actual s'aconsegueixen una sèrie de beneficis importants, com per exemple la reducció de costos degut a que no s'ha de mantenir una infraestructura física. S'aconsegueix també una major escalabilitat i sobretot una major seguretat davant amenaces i una recuperació més ràpida davant a un desastre.

6 Bibliografia

Cisco. 2022. Documentació oficial de Cisco. URL: https://www.cisco.com/

Fortinet. 2022. Documentació oficial de Fortinet. URL: https://www.fortinet.com/

HP. 2022. Documentació oficial d'HP. URL: https://www.hp.com/

Fortinet. 2022. Ajuda de Fortinet. URL: https://help.fortinet.com/

Mediacloud. 2002. Documentació sobre VRF. URL: https://blog.mdcloud.es/vrf-que-es-y-las-ventajas-de-un-enrutamiento-virtual/

Netacad. 2022. Documentació sobre switching. URL: https://www.netacad.com/

Fortinet. 2002. Fortiweb Cloud: URL: https://www.fortiweb-cloud.com/index/login

Cisco. 2022. Diferentes consultes sobre configuracions/problemes dels switchos. URL: https://community.cisco.com/

Wikipedia. 2022. Documentació general. URL: https://es.wikipedia.org/

Adam. 2002. Informació sobre CPDs. URL: https://adam.es/data-center/racks/