Universitat Oberta de Catalunya

uoc.edu

Seguridad de red Universitaria

Ricard Albert Cabrera
Seguridad de las TIC
Seguridad de redes

Jorge Chinea López
Victor Garcia Font

6 de mayo del 2018

Índice

1. Introducción

1.1 Justificación del Trabajo

Hoy en día, todos sabemos de la importancia de la seguridad y más después de los acontecimientos con Criptolocker y otros malware que han dado un aviso sobre la fragilidad de la seguridad en muchas empresas.

También tenemos el hecho de que cualquier persona habitualmente hace uso de un gran número de dispositivos personales que quiere conectar a una red, sin tener en cuenta el estado de seguridad de los dispositivos o las aplicaciones instaladas en ellos, así como la mala utilización de las redes institucionales para usos propios (descargas ilegales).

1.2 Objetivo

El objetivo del TFM es poder mejorar la seguridad de una red Universitaria para evitar infecciones, pérdida de datos y otros prejuicios que puedan ocasionar diferentes ataques.

Así como una vez conseguidos los objetivos anteriores, que son los principales, también, limitar el ancho de banda y los protocolos permitidos según la red usada para evitar mal uso de los recursos proporcionados por la institución.

Para poder llevar a cabo este propósito hay que:

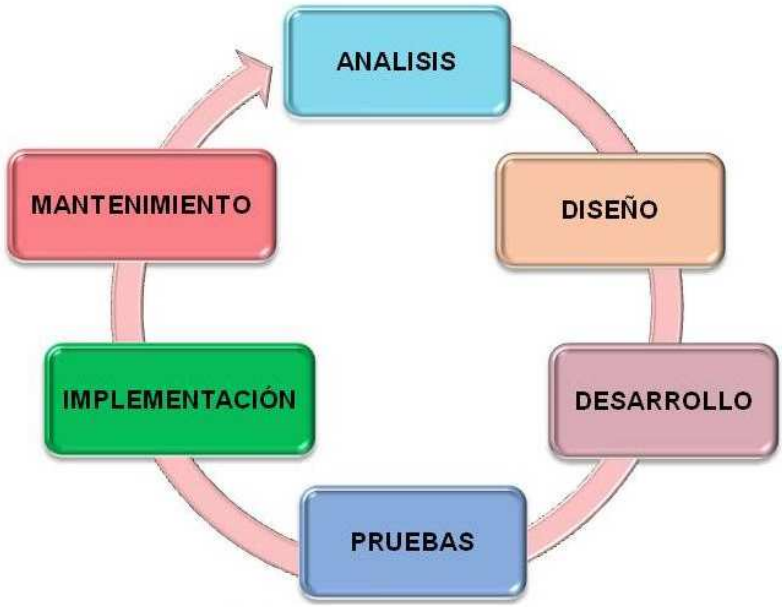
- Valorar el estado actual de la red.
- Valorar los riegos durante la migración.
- Hacer un estudio de las máquinas conectadas a la red.
- Revisar puertos útiles de servidores.
- Dividir la red en vlan.

Después de la fase de estudio y análisis, tendríamos que empezar con la implementación:

- Instalación de Firewall(Untangle).
- Primeros pasos de Configuración de firewall.
- Configuración de los switches con las vlan.
- Configuración del DHCP.
- Definición de las reglas .
- Configuración de reglas del Firewall.

1.3 Enfoque y método seguido

Pera éste proyecto, se ha decidido usar una metodología clásica o en cascada, que tendrá un análisis de las necesidades, diseño de la arquitectura, configuración de los servicios y pruebas.



1.4 Planificación

El proyecto tiene como fecha de cierre el día 7 de mayo de 2018. El proyecto cuenta con tres fases, repartidas en el tiempo del siguiente modo:

Fase 1	12/03/18	29/03/18
Valoracion del estado actual de la red	12/03/18	12/03/18
Valoración riegos implementación	13/03/18	13/03/18
•Hacer un estudio de las maquinas conectada...	14/03/18	16/03/18
•Revisar puertos útiles de servidores	19/03/18	21/03/18
Estudio Aplicaciones usadas	21/03/18	27/03/18
Dividir la red en vlan deseadas	28/03/18	29/03/18
Fase 2	30/03/18	23/04/18
Creacion entorno virtual	30/03/18	2/04/18
Configuracion de Firewall	3/04/18	5/04/18
Configuracion de electronica	6/04/18	9/04/18
Configuracion de reglas	10/04/18	17/04/18
Configuracion DHCP	18/04/18	23/04/18
Fase 3	24/04/18	2/05/18
Juego de pruebas	24/04/18	2/05/18

Los tiempos expuestos pueden variar dependiendo de las incidencias encontradas durante la evolución del proyecto

1.5 Productos Obtenidos

Una vez finalizado el proyecto se obtendrá:

- Una documentación sobre cómo se segmentara la red.
- Documento sobre el tipo y la frecuencia de las copias de seguridad.
- Dos máquinas con el Firewall escogido (Untangle) configurado con las reglas necesarias activas para ser usadas en el entorno descrito.

2. Análisis actual de la red

2.1 Riesgos Preliminares

- Dificultad en el cumplimiento de los plazos. Al tener un equipo humano limitado y otros proyectos en marcha, así como no poder hacer paradas de la red por el uso académico.
- Falta de conocimiento de todas las aplicaciones usadas en la institución.
- Falta de una infraestructura adecuada para la verificación de la herramienta. Será necesario crear un entorno de pruebas.
- Falta de conocimiento de los puertos usados por diferentes aplicaciones o máquinas específicas. Será necesario invertir gran cantidad de tiempo para poder calificar los puertos por aplicación.

En las siguientes tablas, se tomaran los siguientes valores para cuantificar los riesgos y las medidas para poder paliarlos:

- Muy Alto: 5
- Alto: 4
- Medio: 3
- Bajo: 2
- Muy Bajo: 1

- Tabla. Tabla de riesgos

Identificador	Riesgo	Probabilidad	Impacto	TOTAL
Tiempo limitado	Dada la carga de trabajo de otros proyectos, plantea la posibilidad de no lograr todos los objetivos.	media/alta (4)	Medio/alto (5)	20
Falta de todas las aplicaciones usadas	Fallos en programas el uso de programas no detectados.	Medio(3)	Alto(4)	12
Falta de infraestructuras para pruebas	Puede dificultar las pruebas y comprobaciones a realizar.	Alto (4)	Alto (4)	16
Falta de conocimiento del funcionamiento a bajo nivel de la aplicación	Dificultará la detección de fallos.	Medio (4)	Media-Alta (5)	20

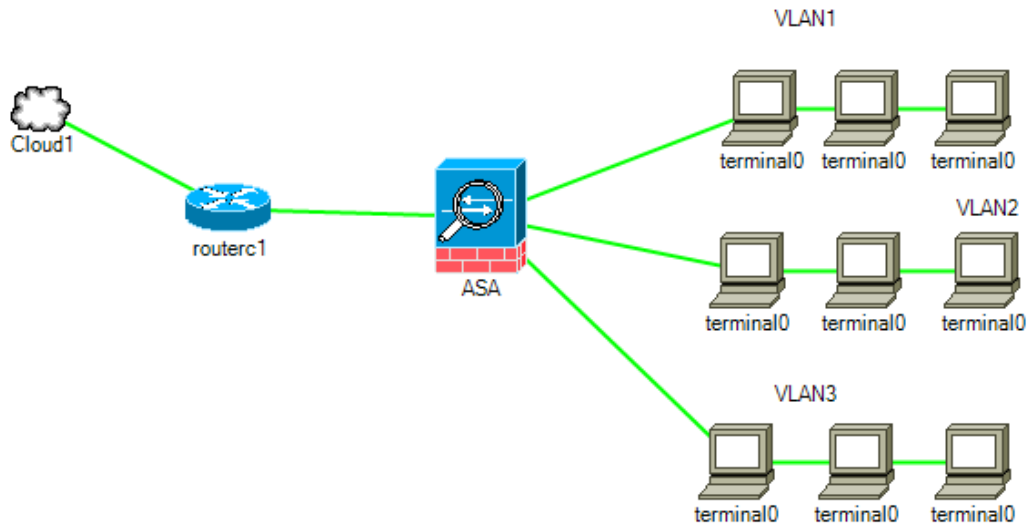
Sobre estos riesgos detectados, se van a tomar una serie de medidas para su mitigación:

Tabla. Tabla de acciones para la mitigación de riesgos

Identificador	Acciones de mitigación	Probabilidad	Impacto	TOTAL (residual)
Tiempo limitado	Trabajo rápido. Ser concisos.	Media-Alta (4)	Medio-Alto (5)	20
Falta de aplicaciones usadas	Pedir listado al equipo(HelpDesk)	Alta(4)	Alta(4)	16
Falta de infraestructuras para pruebas	Investigación por Internet. Creación entorno virtual	Alta (5)	Alto (5)	25
Falta de conocimiento del funcionamiento a bajo nivel de la aplicación	Obtención de información por internet. Revisión de log	Media (4)	Medio-Bajo (4)	16

2.2 Valoración actual de la red

En la actualidad, la institución tiene la red dividida en tres subredes distintas que son las siguientes:



Vlan 1

Red de servidores, esta subred, contiene los servidores tanto de acceso externo, como puede ser el servidor web, como los de interno, por ejemplo el LDAP o el servidor KMS.

En esta subred, también están configuradas las ip's de toda la electrónica de la red, es decir, Router, switches, antenas Wifi, controladora Wifi, así como también las ILO's de los servidores físicos.

Vlan 2

En esta subred están las estaciones de trabajo, es decir, las máquinas con las que los usuarios trabajan, ya pueden ser las del personal de ayuda a la docencia, que son los que las usan 8 horas al día.

Las de los profesores, son estaciones compartidas con un número inferior de aplicaciones.

Las de los alumnos, que las utilizan para dar clase o hacer trabajos y contienen software específico.

También están las impresoras en este rango, ya que cualquier usuario puede imprimir en ellas.

Vlan 3

En la subred Wifi, cualquier dispositivo se puede conectar con el password correspondiente, también podemos encontrar puntos de red activos para conectar por cable dispositivos personales.

La estructura descrita es la que en estos momentos tiene la institución, es una configuración muy sencilla, al solo ser 3 subredes, las reglas son muy básicas.

Por ejemplo, al estar en la misma subred, las impresoras y las máquinas se pueden comunicar directamente.

La vlan 3 sólo tiene configurado el acceso a DHCP, DNS y salida a internet, mientras que la vlan 2 tiene para todas las máquinas diferentes accesos a los servidores y la vlan 1 tiene accesos tanto desde Internet como desde las diferentes subredes internas.

Toda está simplicidad provoca que la seguridad no sea buena, al dar acceso a los servidores a máquinas que no lo necesitan o que los servidores tengan acceso desde internet.

O algo más grave, como podría ser una infección por un ransomware, en la vlan 2, que infectaría todas las máquinas de la subred y los servidores a los que tuviera acceso. Justamente este tipo de incidencia sucedió el pasado año, con la consiguiente pérdida de información y la necesidad de aislar los equipos infectados y recuperar la información dañada.

2.3 Valoración de las máquinas

En este apartado hablaremos de la tipología de las máquinas conectadas en la red, empezaremos con los servidores.

Los servidores conectados son todos Windows Server 2008 R2, Linux, distribuciones SLES y Centos, los servidores son los siguientes:

- Svcontab01: servidor con software específico para contabilidad.
- Svgrpext02: servidor con un radius y ldap para uso de aplicaciones de fuera de la institución.
- Svproxadm01: servidor con el Proxy.
- Svgrpext03: servidor que contiene el webmail.
- Svoes03: Imanager y carpetas compartidas.
- Svweb01: web institucional.
- Svmanteniment01: contiene software específico para mantenimiento.
- Charlie: AD azure.
- Svmail01: Mail scanner, postfix.
- Svinformatica03: web para uso interno del profesorado.
- Omega: Servidor con un AD, DNS y DHCP.
- Svoes01: Imanager y carpetas compartidas .
- Svmoodle01: web Moodle.
- Svoes02: Imanager y carpetas compartidas.
- Alpha: AD.
- Svrrhh01: software específico para RRHH, control marcajes.
- Svgrp01: servidor de correo con groupwise.
- Svweb03: Vacío.
- Svinformatica02: scripts para obtener datos de otras plataformas y procesarlos.
- Svintranet: Intranet institucional.
- Svgrpdatasync01: Contiene el software de conexión de correo con los móviles, mobility.
- Svinformatica01: servidor kms, antivirus y gestor de otras licencias.

Toda la electrónica es del proveedor CISCO. Hay diferentes switches:

- Un switch core dónde están conectadas las fibras.
- Una controladora wifi para configurar automáticamente los AP.
- Un router.

Sobre las máquinas conectadas a la red, todas usan Windows 7 o Windows 10, están dentro del mismo dominio, la diferencia radica en las aplicaciones que usan, dependiendo de donde están ubicadas tienen software específico que necesita validación por licencia.

Por lo que hace referencia a las impresoras, son RICOH que necesitan una salida para una gestión desde fuera de la institución y también hay Hp.

Finalmente, tenemos la red de invitados en la que se puede conectar cualquier dispositivo que la gente pueda traer así como algunas máquinas de la institución, como pueden ser las pantallas o sondas de control de temperaturas.

2.4 Puertos utilizados en servidores

Para los servidores que se han explicado en el anterior apartado, analizaremos los puertos que necesitan para comunicarse tanto con las redes internas como con las externas.

Nombre servidor	Puertos internos	puertos externos
svcontab01	80,8080,443	8530,8531,80,443
svgrpext02	-	389
svproxadm01	80,8080,443	80,8080,443
svgrpext03	80,8080,443	80,8080,443
svoes03	389,137,138,139,9100	-
svweb01	80,8080,443	80,8080,443
svmanteniment01	-	-
Charlie	-	80,443
svinformatica03	80,8080,443	8530,8531
svoes01	389,137,138,139,9100	-
svmoodle01	80,443	80,443

svoes02	389,137,138,139,9100	8530,8531
alpha	389,53,66,67	8530,8531
svrrhh1	80,8080,443	-
svgrp01	1677	-
svweb03	-	-
svinformatica02	21,22	80,8080,443
svintranet	80,8080,443	-
svgrpdatasync01	-	80,443,8120,4500
svinformatica01	13000,14000,15000,1688	8530,8531

2.5 Aplicaciones usadas en máquinas

Las máquinas conectadas a la red en estos momentos son Windows y tienen acceso a todos los puertos de los servidores, entraremos a analizar los puertos y accesos que necesitan.

Servicio	Puerto	Servidor	Todas las máquinas
1688	KMS	Svinformatica01	Si
13000	Antivirus	Svinformatica01	Si
14000	Antivirus	Svinformatica01	Si
15000	Antivirus	Svinformatica01	Si
389	LDAP	Svoes01,svoes02,svoes03	Si
137,138,139,445	Samba	Svoes01,svoes02,svoes03	Si
67,68	DHCP	Omega, aplha	Si
53	DNS	Omega, Alpha	Si
13331	PXE	Zcm	Si
1761	Zenworks	Zcm	Si
9100	Printer	Svoes01,svoes02,svoes03	Si
80,443	HTTP/S	exterior	Si
1677	Groupwise	svgrp	No
9100	VNC		No

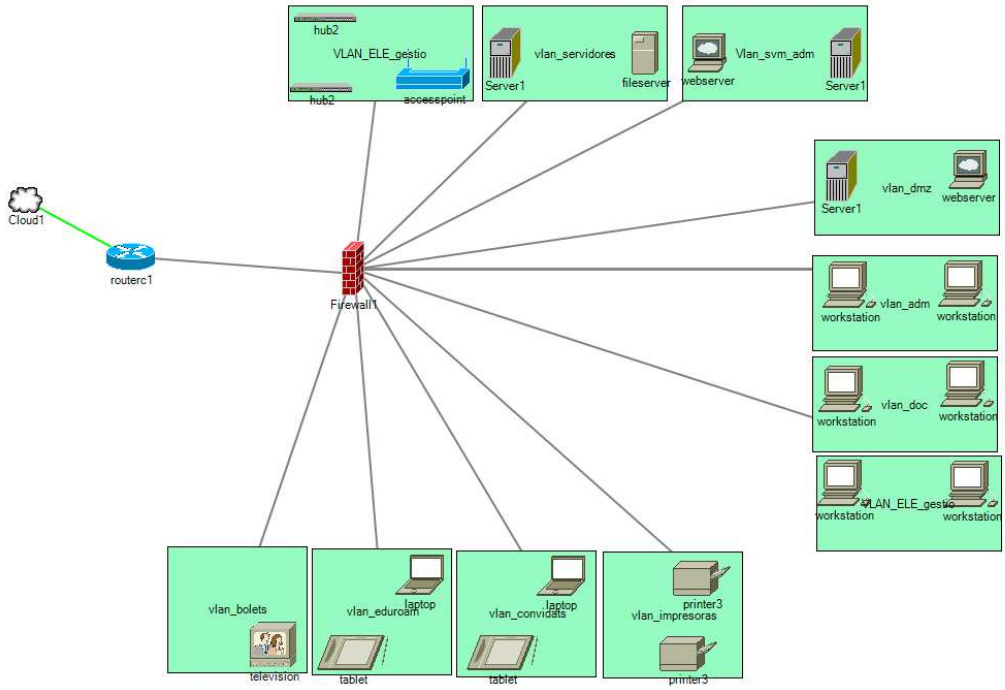
Analizados los puertos básicos de la red actual, podemos empezar a estructurar las diferentes vlan que queremos utilizar.

Pueden aparecer puertos que no hayan sido detectados, en éste caso se explicará cómo solucionar el problema al ser detectados en los siguientes apartados.

3. Diseño de la nueva red

3.1 Vlan's Deseadas

Una vez analizados los puertos y aplicaciones que están en uso en las diferentes estaciones de trabajo, comenzamos a segmentar la red para poder hacer grupos de estaciones y mejorar la seguridad y también la gestión sobre ellas.
Entonces las subredes quedarían del siguiente modo:



- Vlan_tic: subred que tendrá acceso tanto a las demás subredes en los puertos habituales descritos anteriormente como a ssh, ping, rdp, etc... Para gestionar todo el sistema.
- Vlan_gestió: subred para los pc's que tengan el cliente de Groupwise instalado que son los mismos que tienen el office, también son los pc's que más se usan normalmente en despachos.
- Vlan_docencia: aquí están los pc's que se usan en la biblioteca o las aulas, simplemente tienen acceso para imprimir y navegar, así como a algunas carpetas compartidas, pero sin validación de software especial.
- Vlan_convidats: creada para eventos, simplemente acceso a internet.

- Vlan_eduroam: para los trabajadores y alumnos de las universidades que se les da acceso mediante usuario y password, tendrán algunos puertos más que los de convidats.
- Vlan_impresoras: aquí estarán todas las impresoras, solo se tendrá acceso a web para ver las colas y para mandar a imprimir, al tener máquinas de renting, también hay un acceso de los proveedores para poder ver el estado de las mismas.
- Vlan_electronica: para todos los equipos de infraestructura, es decir, switches, router, AP, ILO.
- Vlan_dmz: servidores a los que se necesita acceso al exterior, como ldap, radius, web, correo.
- Vlan_svm_adm: servidores de uso solamente interno, como robots o con software específico.
- Vlan_servidores: servidores a los que se tiene acceso tanto dentro como fuera de la institución.

Con esta configuración conseguimos dividir el acceso de cada máquina a los recursos que pueda necesitar. De esta manera, aunque la configuración inicial será más compleja, tendríamos una mayor seguridad al no dejar conexiones directas entre todas las máquinas, también sería mucho más sencillo en un futuro aplicar nuevas reglas para nuevos servicios que se pudiesen añadir en la institución.

Por ejemplo, en el mismo caso del ransomware que se comentaba en el apartado de la vieja configuración, el virus quedaría restringido a la vlan dónde se produjera la infección, esto evitaría que todas las máquinas de la red fueran infectadas.
Dependiendo de en la vlan que sucediera, evitaríamos servidores infectados, quizá algunas carpetas compartidas. De este modo la recuperación de la red infectada sería más rápida y con menos problemas para el resto de usuarios.

3.2 Selección del Firewall

Para seleccionar el Firewall más idóneo para nuestra empresa, se han analizado diferentes productos que hay en el mercado con los diferentes criterios necesitados.

- Actualmente hay un total de 1200 usuarios en el sistema, no todos están conectados simultáneamente, pero según estudios internos, pueden estar hasta 500 usuarios llegando a ser 700 en momentos puntuales (Eventos).

- Se quiere poder hacer una VPN desde el mismo Firewall para poder trabajar desde redes externas.

- Poder añadir fácilmente nuevas reglas a las redes.

- Que tenga un bajo coste o gratuito.

- Poder reutilizar material antiguo.

Con estos criterios, se ha seleccionado finalmente Untangle en su versión gratuita, este es un Firewall por software que permite a la empresa no tener que desembolsar nada más que las horas del técnico para su puesta en marcha.

Untangle nos permite su instalación basada en Linux, en dos servidores antiguos Hp con 8 tarjetas de red que la institución tiene sin uso.
De esta manera podemos tener una réplica y en caso de que uno de ellos fallara, automáticamente el otro se pondría como principal para no perder conectividad.
Este software se basa en una interficie web “friendly”, que permite hacer la configuración de una manera sencilla, así como un paquete de aplicaciones gratuitas, entre ellas la de Firewall y VPN, muy intuitivas. También contiene, si se desea algunas aplicaciones no gratuitas para mejorar la seguridad.

La interface inicial ofrece una serie de diagramas con las conexiones actuales y el uso de la red, es muy útil para poder ver si hay algún problema.

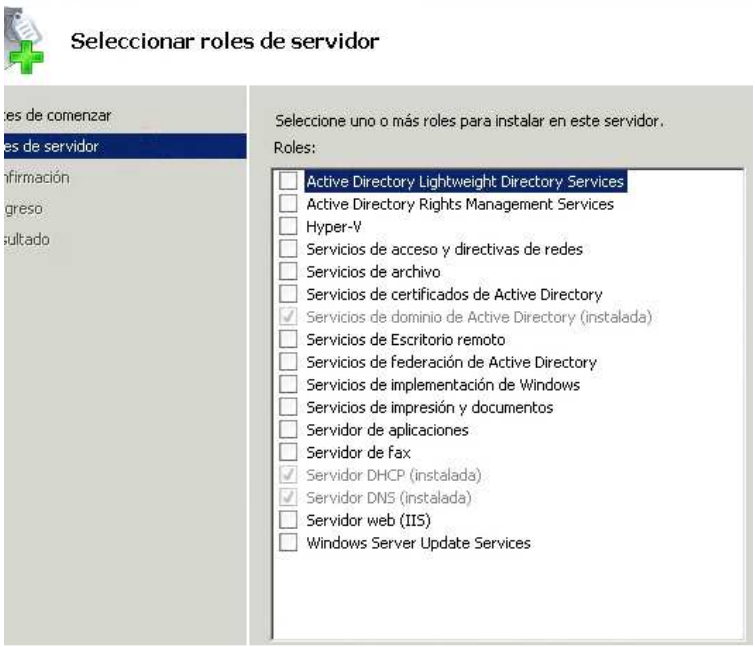
Finalmente, ofrece un backup sencillo con la descarga a través de un simple botón de la configuración total o parcial de éste.

4. Instalación y configuración

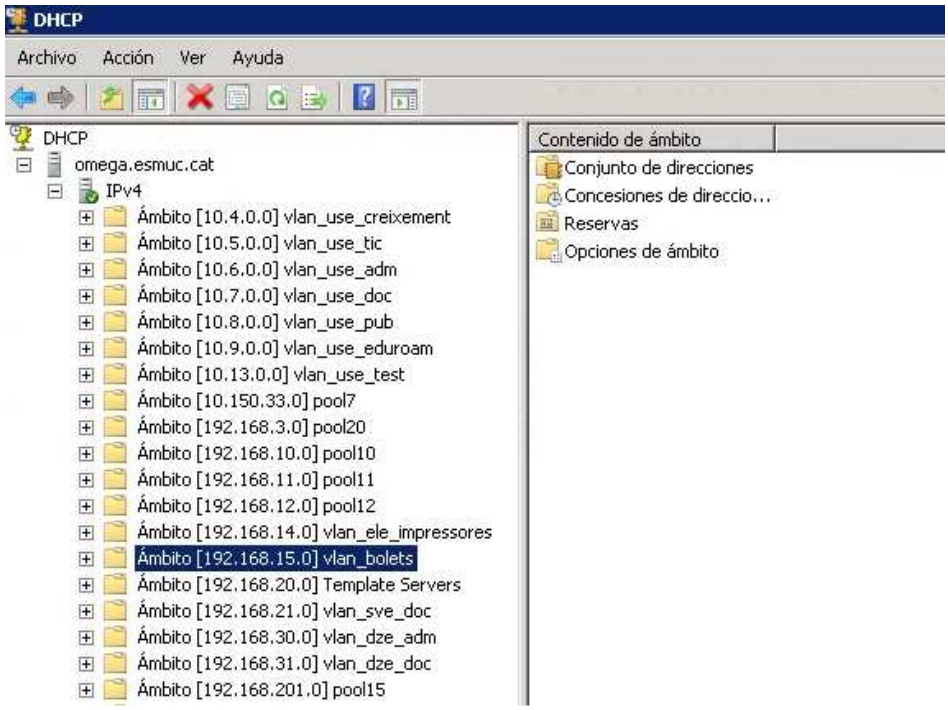
4.1 Creación de un nuevo DHCP

Para evitar problemas, se decide crear un nuevo servidor DHCP, esto solucionará en la futura migración hacia las nuevas subredes, que las máquinas se queden sin dirección IP.

Para ello, se ha seleccionado un servidor ya instalado, como es Omega, que lleva un Windows 2008 Server R2 y se le ha instalado el servicio de DHCP.



Una vez instalado el programa se han configurado las subredes comentadas anteriormente.



Con esta funcionalidad añadida en nuestro servidor evitaremos los problemas anteriormente mencionados y se podrán hacer mejoras de seguridad de la red que quedan fuera de este proyecto.

4.2 Configuración de los Switches

Toda la red que tenemos tiene una infraestructura con Cisco, en estos momentos no están creadas las vlan, para poder solucionar este problema y adelantar trabajo, decidimos crearlas mediante los comandos pertinentes.

Este proceso se tiene que hacer por cada uno de los switch que la institución tiene repartidos por las diferentes plantas

- Nos conectamos al swicth mediante telnet.
- Introducimos las credenciales.
- En modo Enable.
- Config terminal.
- Vlan “vlan-id” (Por cada una de las nuevas vlan).
- Vlan “vlan-id”(entramos en modo configuración de la vlan).
- Name “nombre vlan”.

```
swing31-0#show vlan

VLAN Name                                Status
---- ----------------------------------- --------
1    default                             active
2    Vlan_W_Eduroam_test                 active
3    Electronica                         active
4    vlan_creixement                     active
5    vlan_use_tic                        active
6    vlan_use_adm                        active
7    vlan_use_doc                        active


8    vlan_use_pub                        active
9    vlan_use_eduroam                    active
10   Vlan_SvE_Gestio                     active
11   AnellaDocent                        active
12   Vlan_ILO_Esmuc                      active
13   Vlan_Testing                        active
14   vlan_ele_impressores                active
15   vlan_ele_bolets                     active
20   Vlan_SvE_Adm                        active
21   Vlan_SvE_Docent                     active
22   Vlan_SvE_Cluster                    active
30   vlan_dze_adm                        active
31   vlan_dze_doc                        active
33   Vlan_W_Publica                      active
99   LAN-2-FW                            active
100  Servidors_ADM                       active
111  VLAN0111                            active
```

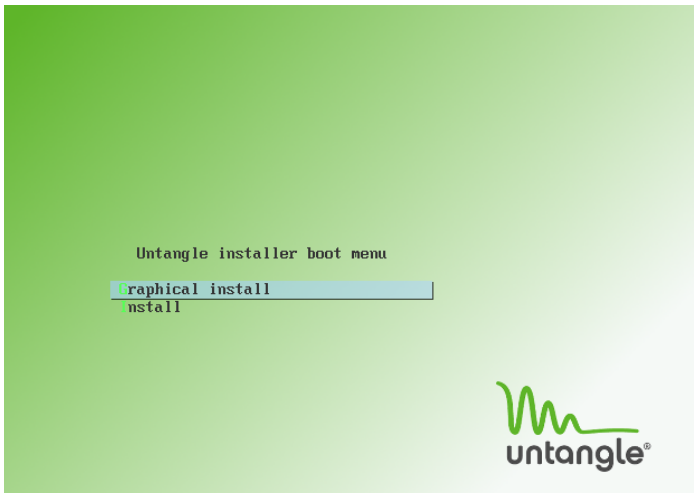
Con este proceso previo, se podrán modificar las redes de los Pc's y el usuario solo notará un micro corte de la red.

4.3 Firewall

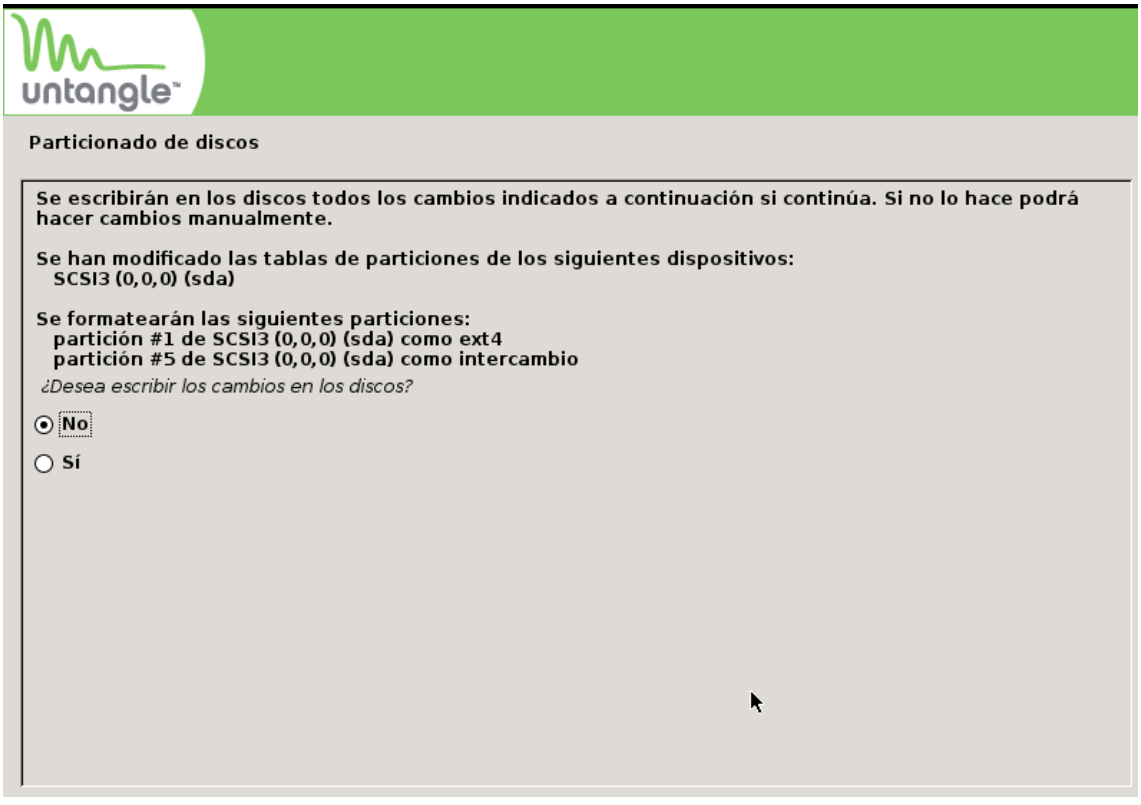
4.3.1 Instalación del Firewall

Primeramente descargamos de la web (https://www.untangle.com/get-untangle/) la imagen, una vez grabada en un disco, procedemos a realizar la instalación en el primer servidor.

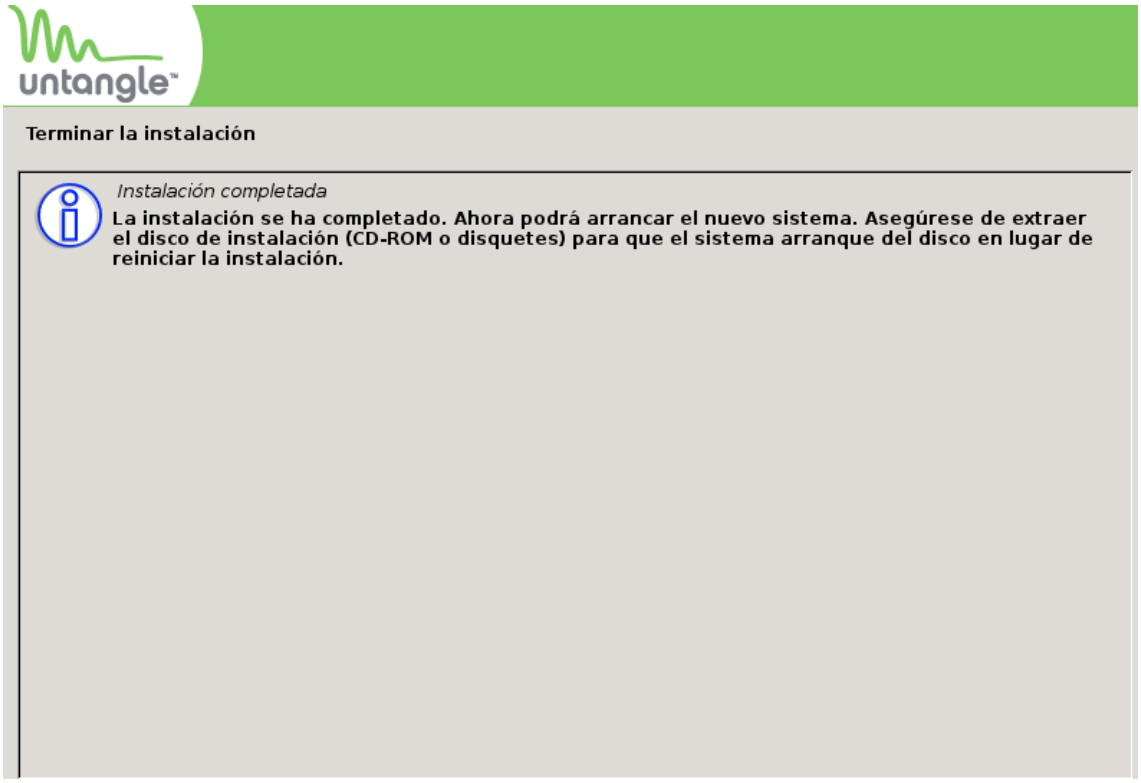
Para empezar, seleccionamos las preferencias de región y teclado.



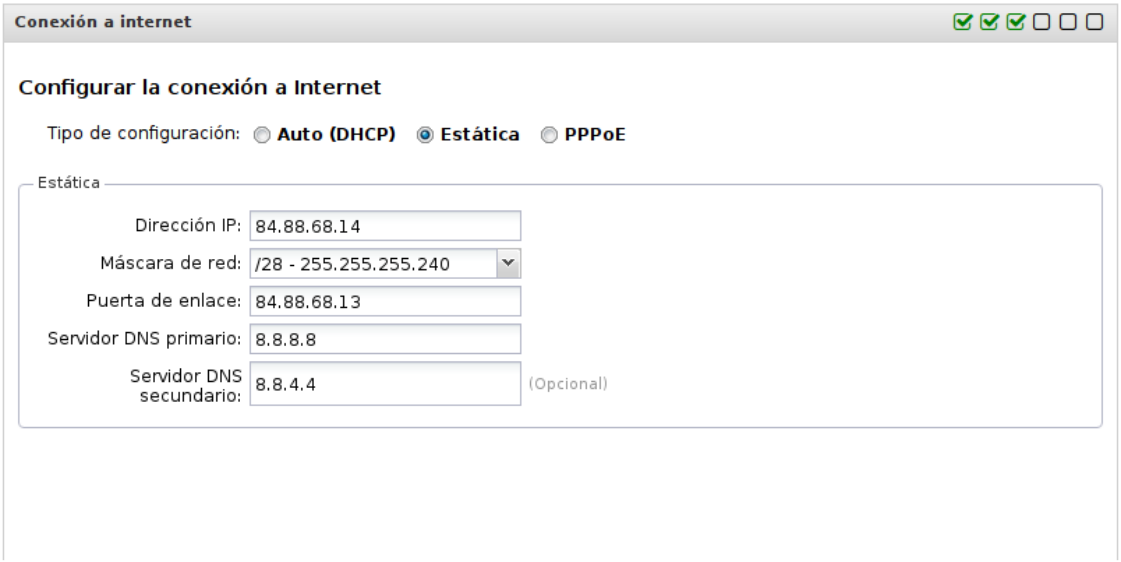
Seguimos con las particiones.



Dejamos que instale los paquetes y finalice, se reiniciará.



Empezamos con la configuración inicial, introducimos el password de admin y la configuración de la red.



4.3.2 Configuración de las redes y reglas

Finalizada la configuración inicial, podemos acceder al firewall, lo primero será configurar las diferentes redes, para ello, se accede a config>network.

Los servidores reutilizados tienen ocho tarjetas de red. Como el número de redes a crear es superior a estas tarjetas, se decide agrupar por cada tarjeta diferentes subredes, valorando el volumen de tráfico que hay por cada una.

1	External	Connected	eth0	1 Gbit	Full-duplex	Addressed	84.88.68.14/28	true		
2	Internal	Connected	eth1	1 Gbit	Full-duplex	Addressed	192.168.99.178/24	false		
3	Interface ISCSI	Connected	eth2	1 Gbit	Full-duplex	Addressed	192.168.111.178...	false		
4	Interface WIFI	Connected	eth3	1 Gbit	Full-duplex	Addressed	10.9.0.178/16	false		
5	Interface Personal Int...	Connected	eth4	1 Gbit	Full-duplex	Addressed	10.5.0.178/16	false		
6	Interface Servidors	Connected	eth5	1 Gbit	Full-duplex	Addressed	192.168.200.178...	false		
7	Interface Eta	Connected	eth6	1 Gbit	Full-duplex	Disabled				
8	Interface Theta	Connected	eth7	1 Gbit	Full-duplex	Disabled				
100	vlan_use_pub	Connected	eth3.8	1 Gbit	Full-duplex	Addressed	10.8.0.178/16	false		
101	vlan_ele_bolets	Connected	eth3.15	1 Gbit	Full-duplex	Addressed	192.168.15.178/24	false		
102	vlan_sve_adm	Connected	eth5.20	1 Gbit	Full-duplex	Addressed	192.168.20.178/24	false		
103	dmzesmuc	Connected	eth5.220	1 Gbit	Full-duplex	Addressed	10.220.0.178/24	false		
104	vlan_use_doc	Connected	eth4.7	1 Gbit	Full-duplex	Addressed	10.7.0.178/16	false		
105	vlan_use_adm	Connected	eth4.6	1 Gbit	Full-duplex	Addressed	10.6.0.178/16	false		

Configuramos los enrutamientos de puertos y las reglas de NAT

Interfaces | Hostname | Services | **Port Forward Rules** | NAT Rules | Bypass Rules | Filter Rules | Routes | DNS Server

Port Forward rules forward sessions matching the configured criteria from a public IP to an IP on an internal (NAT'd) network. The rules ar

Add

Rule Id	Enable	Description	Conditions	New Destination	New Port
1	☑	esmuc.cat svweb01 puerto 80	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.139	80
2	☑	esmuc.cat svweb01 puerto 3000	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.139	3000
3	☑	esmuc.cat puerto 2122	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.139	2122
4	☑	svinformatica03 puerto 80	Destined Local ⇒ True • Protocol ⇒ T...	192.168.200.143	80
5	☑	10.220.0.132 puerto 3102	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.132	3102
6	☑	groupwise datasync puerto 443	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.140	443
7	☑	moddle website	Destined Local ⇒ True • Protocol ⇒ T...	192.168.200.145	80
8	☑	svweb03 puerto 80	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.142	80
9	☑	svweb03 puerto 2122	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.142	2122
10	☑	svweb03 puerto 3000	Destined Local ⇒ True • Protocol ⇒ T...	10.220.0.142	3000

Interfaces | Hostname | Services | Port Forward Rules | **NAT Rules** | Bypass Rules | Filter Rules | Routes | DNS Server

NAT Rules control the rewriting of the IP source address of traffic (Network Address Translation). The rules are evaluated in order.

Add

Rule Id	Enable	Description	Conditions	NAT Type	New Source
1	☑	svmail01	Source Address ⇒ 10.220.0.137 • Destination Port ⇒ 25	Custom	84.88.68.2
2	☑	Radius	Source Address ⇒ 10.220.0.136	Custom	84.88.68.2
3	☑	Autoprestec	Source Address ⇒ 10.6.33.33	Custom	84.88.68.12
4	☐	autoprestec	Source Address ⇒ 84.88.68.12	Custom	10.6.33.33

4.3.3 Migración del Firewall

Con la configuración mínima del Firewall podemos empezar a hacer la migración, para ello seguiremos unos pasos muy concretos para que el impacto en el usuario sea el mínimo posible. También se podría haber decidido hacer en época de cierre, pero se ha planificado un impacto mínimo siempre que no se produzcan errores.

Los pasos a seguir son los siguientes:

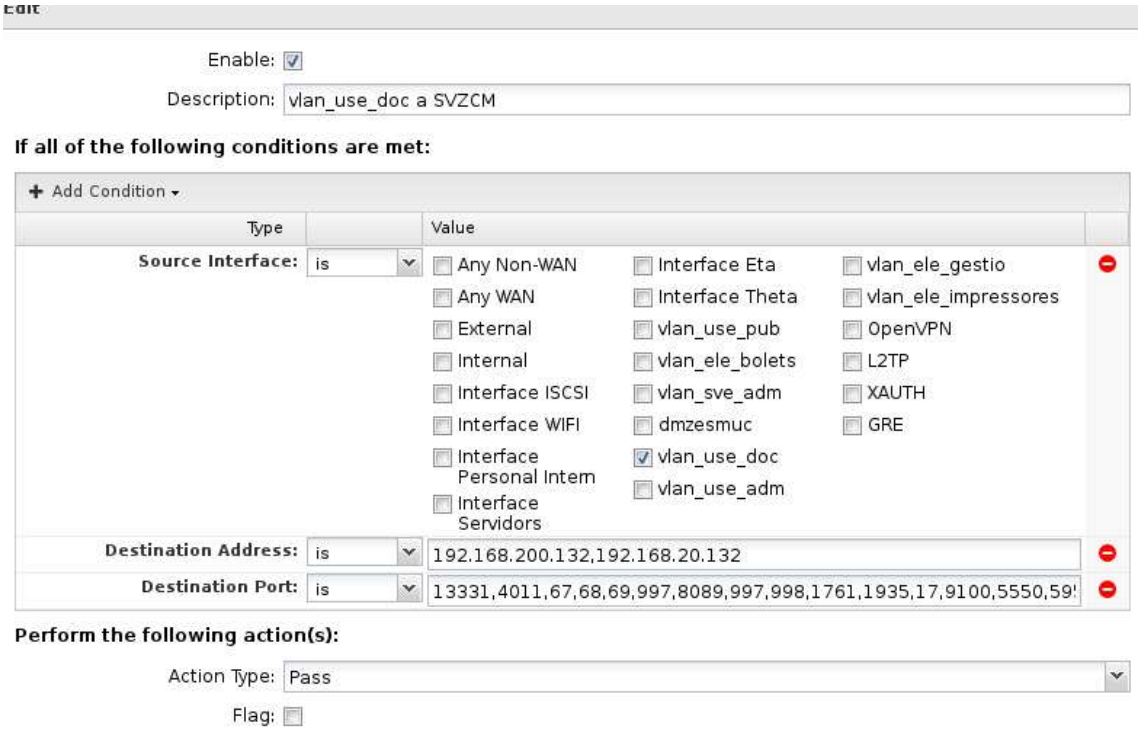
- Crear una red 192.168.99.* para conectar el router y los firewalls.
- Comprobar las nuevas vlan en los switches cisco.
- Migrar las redes del viejo firewall al nuevo.
- Modificar las bocas de los switches para que estén en la vlan correspondiente.
- Comprobar las vlan nuevas.
- Apagar el Firewall viejo.

Siguiendo estos pasos, conseguimos una migración con un impacto mínimo sobre el usuario. Aún no hay reglas en el nuevo Firewall para evitar aumentar las probabilidades de errores o problemas durante la migración.

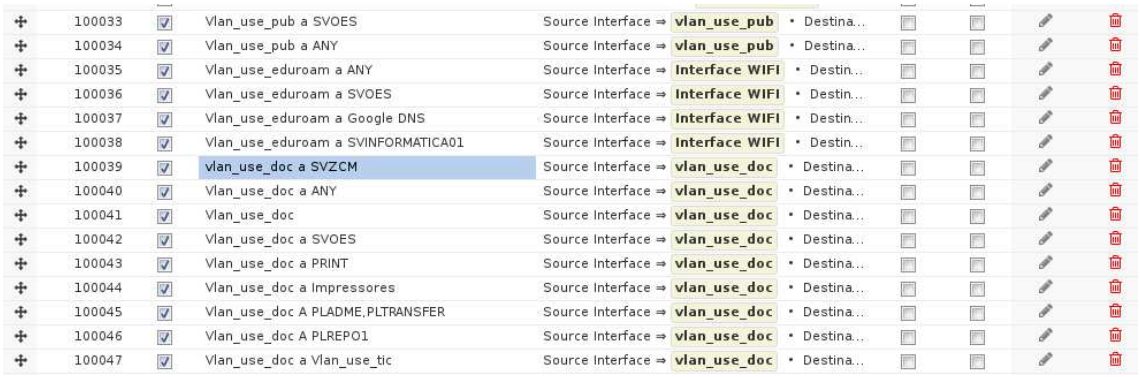
4.3.4 Configuración de las reglas del Firewall

Con el nuevo Firewall en funcionamiento, las redes creadas y en uso, procedemos a crear las reglas que tenemos analizadas en apartados anteriores.

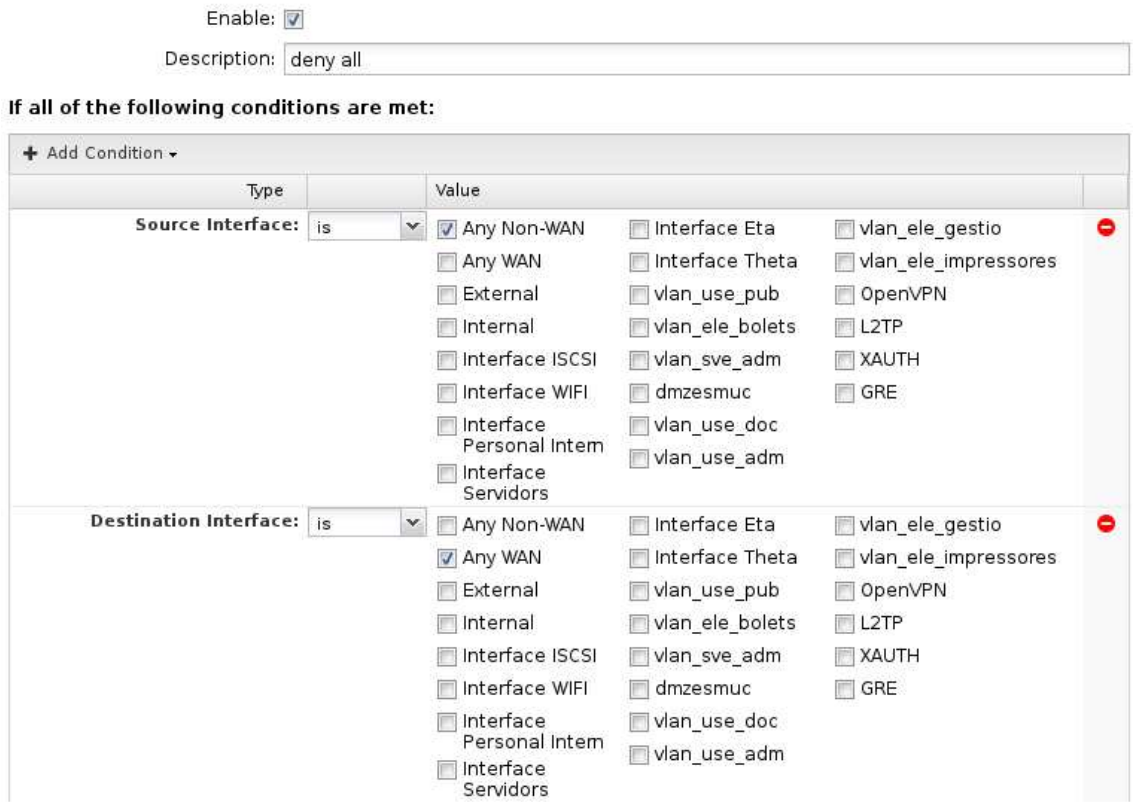
Para ello vamos a Apps>Firewall>Rules, y empezamos a añadir las reglas de la siguiente manera:



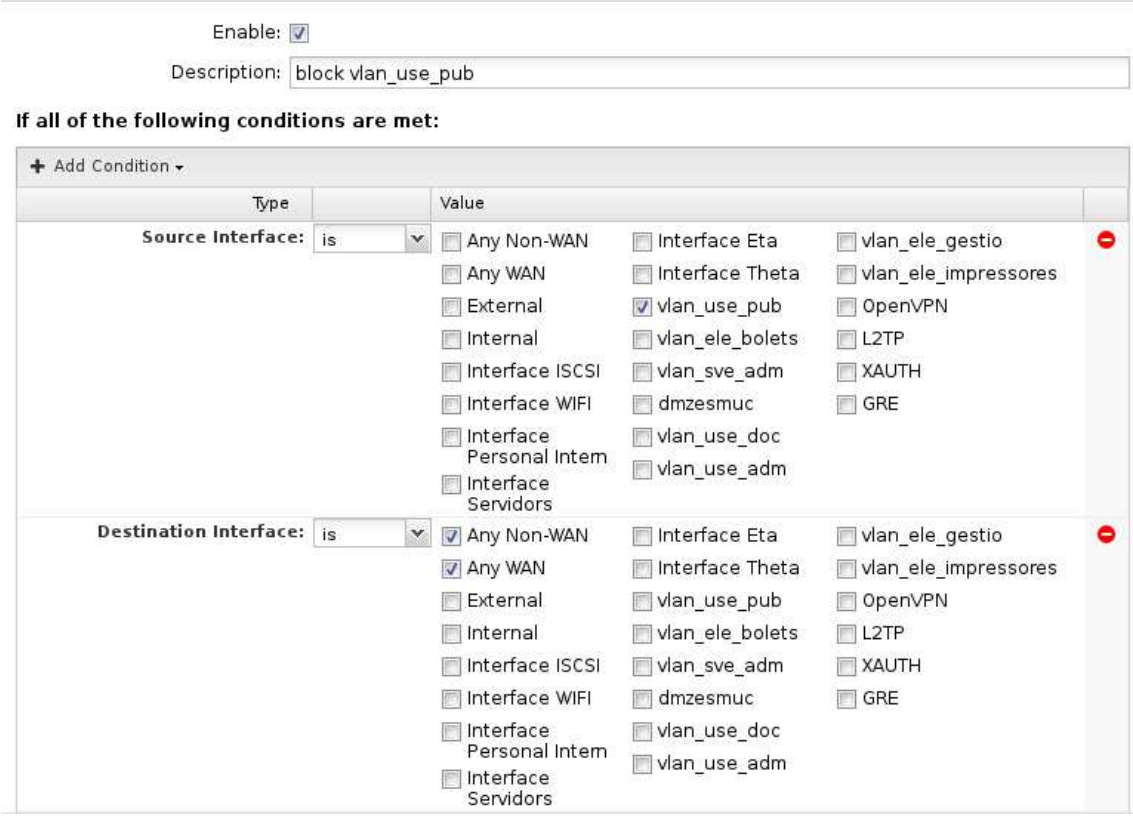
Vamos añadiendo las reglas por cada vlan para no afectar a las demás y comprobamos si son correctas, ya que muchas serán similares en otras vlan's. Una vez configuradas todas quedarían del siguiente modo:



Para finalizar, se añadirá una regla para bloquear el acceso desde fuera no permitido.



Para conseguir una red totalmente segura hay que añadir las reglas de bloqueo en las diferentes redes internas, para ello se añaden reglas de bloqueo para cada una de las redes internas.



Una vez añadidas las reglas, obtendremos la red segura deseada. Para comprobar su funcionamiento, podemos ver el tráfico y las reglas de bloqueo que están actuando.

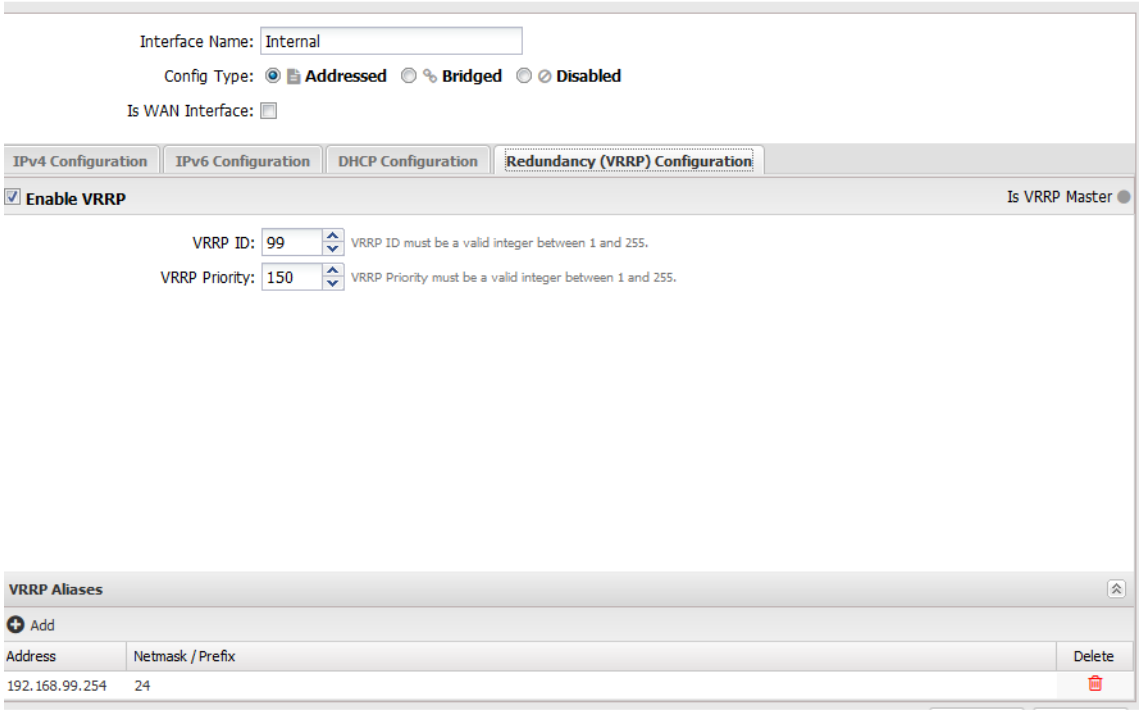
Finalizada la configuración del primer servidor, procederemos a hacer la instalación del segundo, siguiendo los mismos pasos que se han indicado para instalar el anterior.

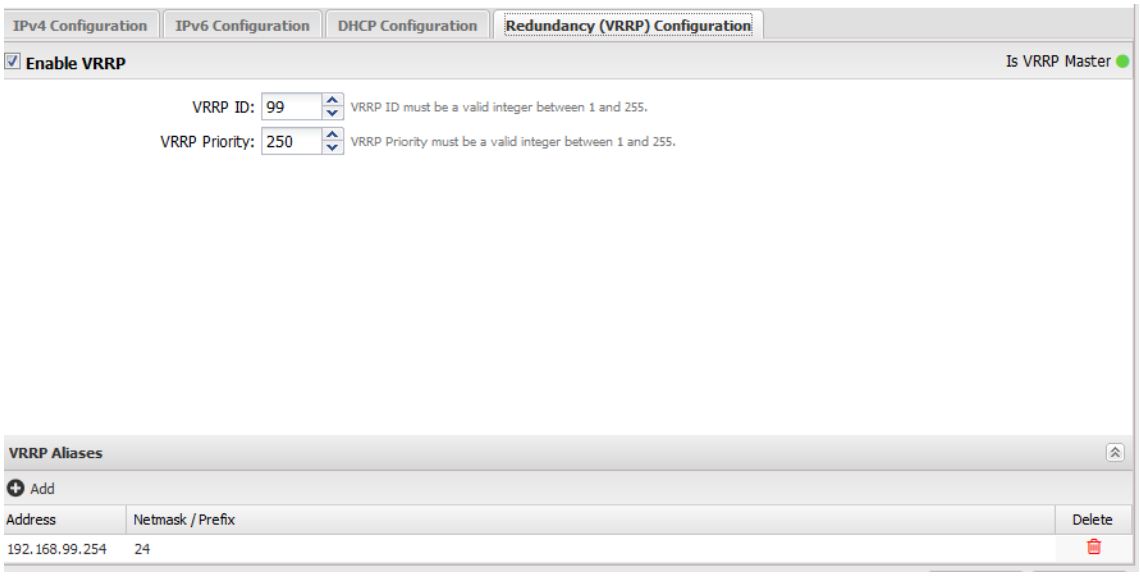
Completada la instalación procederemos a crear las redes, ya que éstas no se pueden importar. Hay que crear las redes en el mismo orden para una mayor facilidad posterior.

	Name	Connected	Device	Speed	Duplex	Config	Current Address	is WAN
1	External	Connected	eth0	1 Gbit	Full-duplex	Addressed	84.88.68.11/28	true
2	Internal	Connected	eth1	1 Gbit	Full-duplex	Addressed	192.168.99.179/24	false
3	Interface ISCSI	Connected	eth2	1 Gbit	Full-duplex	Addressed	192.168.111.179/24	false
4	Interface WIFI	Connected	eth3	1 Gbit	Full-duplex	Addressed	10.9.0.179/16	false
5	Interface Personal Intern	Connected	eth4	1 Gbit	Full-duplex	Addressed	10.5.0.179/16	false
6	Interface Servidors	Connected	eth5	1 Gbit	Full-duplex	Addressed	192.168.200.179/24	false
7	Interface Eta	Disconnected	eth6	0Mbit	Unknown	Disabled		
8	Interface Theta	Disconnected	eth7	0Mbit	Unknown	Disabled		
00	vlan_use_pub	Connected	eth3.8	1 Gbit	Full-duplex	Addressed	10.8.0.179/16	false
01	vlan_ele_bolets	Connected	eth3.15	1 Gbit	Full-duplex	Addressed	192.168.15.179/24	false

Hay que recordar que las direcciones Ip tienen que ser distintas para que puedan funcionar y no tengan conflicto.

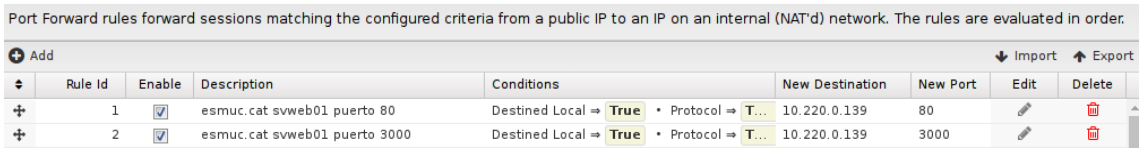
Configuraremos el VRRP de los dos firewalls con diferentes prioridades.





Comprobando que una se queda con el master activado.

Llegados a este punto, vamos a exportar las reglas del Firewall 1 e importarlas al Firewall 2 para mayor rapidez.



Finalizado el proceso de las importaciones, tenemos redundancia de Firewall por si uno fallase. Hay que recordar que siempre que se haga una modificación en uno hay que reproducirla en el otro.

5. Juego de Pruebas

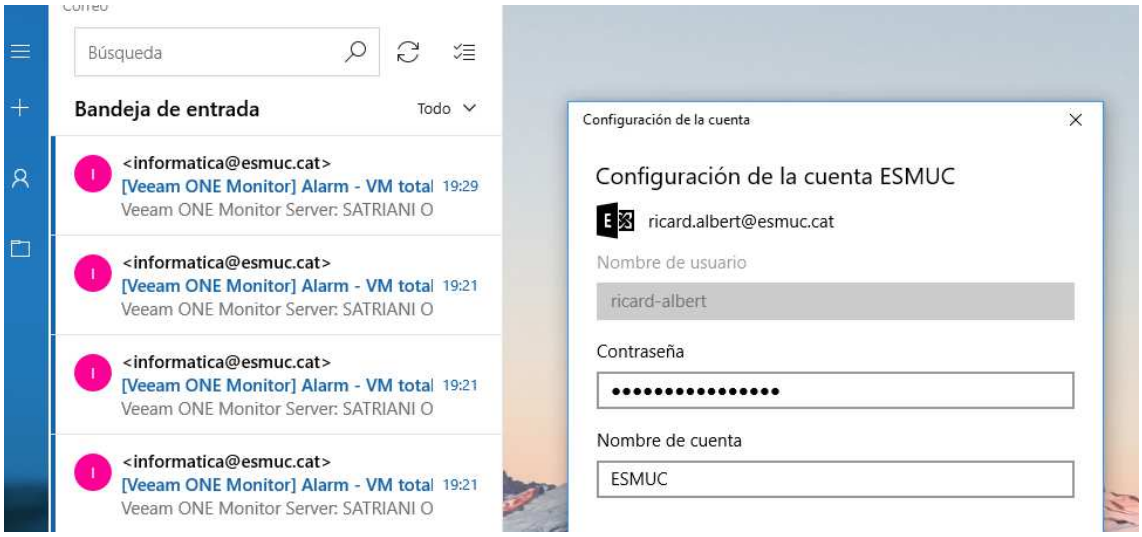
5.1 Pruebas externas

Para poder realizar estas pruebas desde un dispositivo fuera de la red, se procede a comprobar el acceso a la web:

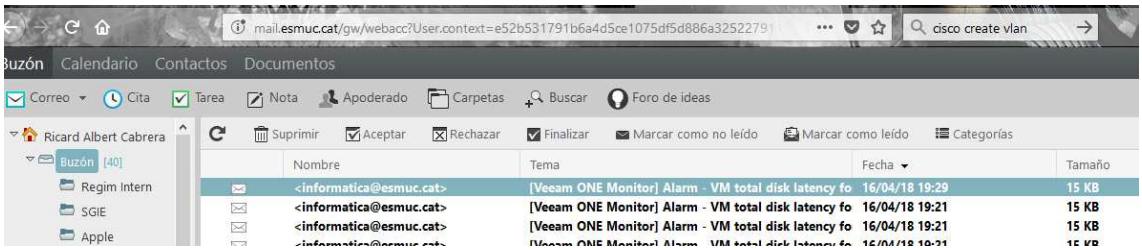
La validación en ella:

Con esta verificación, podremos ver que tenemos acceso desde las aplicaciones web que validan contra nuestro LDAP.

Se configura el correo desde un cliente externo.

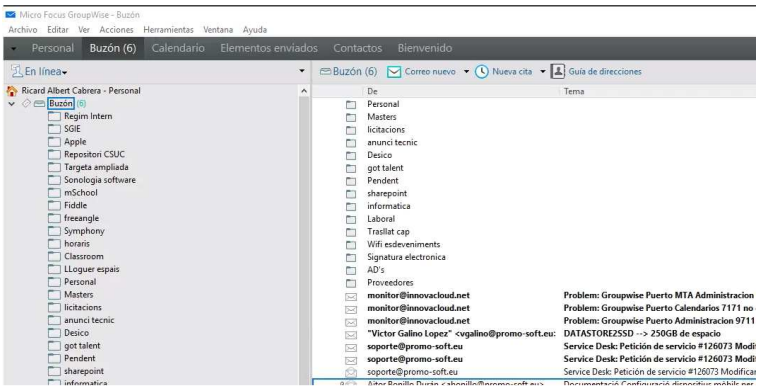


También comprobaremos el funcionamiento vía web:

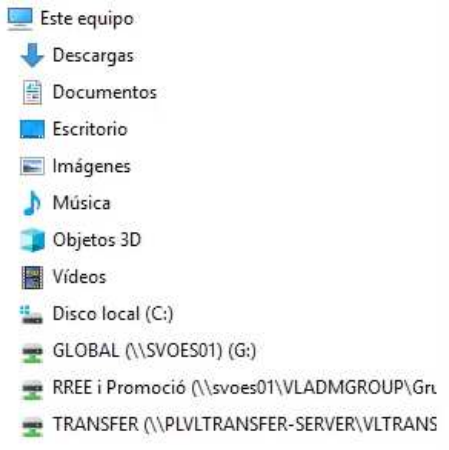


5.2 Pruebas internas

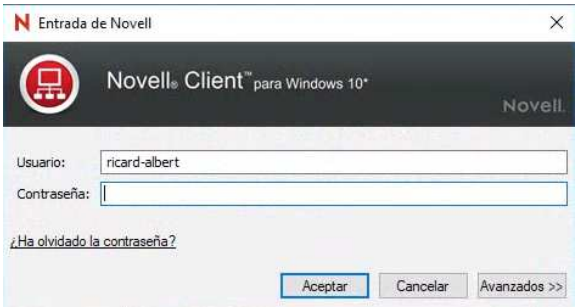
Desde las diferentes subredes se comprueba que se tiene acceso a las aplicaciones básicas, como es el gestor del correo:



Unidades de red:



Así como la validación en el dominio:

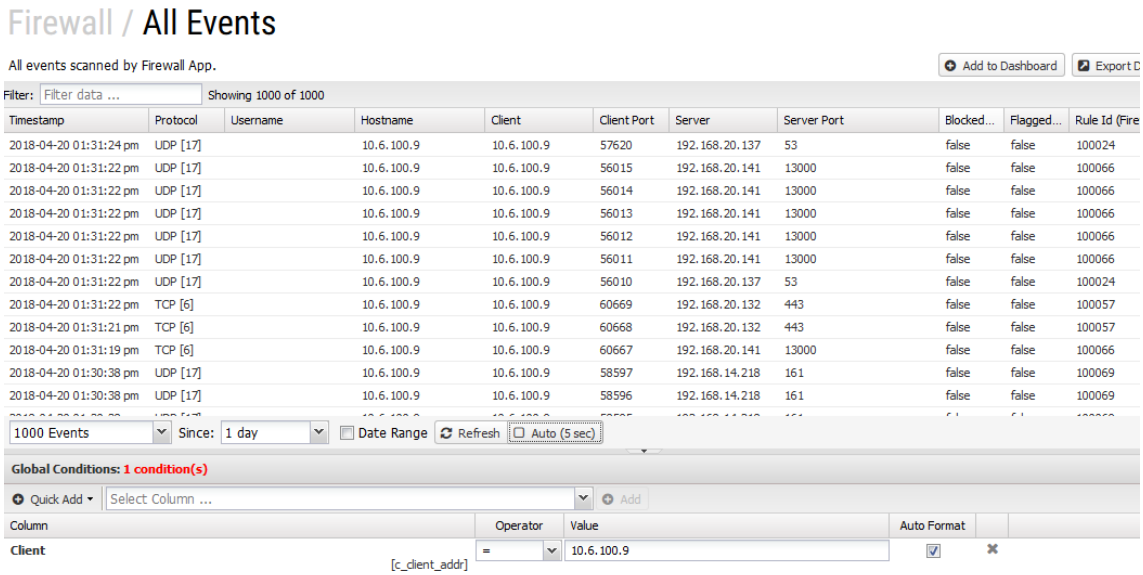


Realizadas estas tareas, y algunas más desde cada una de las subredes, todas ellas satisfactorias, podremos concluir que la migración del Firewall y la aplicación de sus reglas han sido correctas.

5.3 Solución de problemas

Después de la aplicación de las reglas, se contempla que pueden existir puertos restringidos que deberían estar abiertos, para ello, se informa a los usuarios que si detectan cualquier problema en alguna aplicación que anteriormente funcionaba, deben informar al equipo de IT.

Para solucionar los problemas, se recomienda, sabiendo la Ip del usuario que tiene la incidencia y conociendo el servidor al que tiene que acceder, dentro del mismo firewall hacer una búsqueda de esos campos.



Aquí encontraríamos el problema en la columna “blocked”. Simplemente añadiendo una nueva regla con el puerto necesario, siempre que haya sido contrastado que se ha de utilizar, se solucionaría la incidencia.

6. Conclusiones

Durante la realización del proyecto, se han podido analizar diferentes sistemas de seguridad. Todos ellos muy óptimos pero a precios muy elevados, cosa que las pequeñas empresas no se pueden permitir. También se han identificado sistemas que permiten la reutilización de material antiguo.

Nos ha permitido hacer un análisis riguroso de la multitud de puertos usados en un ordenador de un dominio, así como ver para que se utiliza cada uno.

Por otro lado, hemos aplicado los conocimientos de redes adquiridos en otros estudios para poder configurar correctamente las redirecciones de Ip's.

Con todo lo comentado anteriormente, se ha podido conseguir el objetivo del TFM que era hacer más segura la red de la universidad evitando el mal uso o la propagación de software dañino por toda la red.

Al seguir la metodología descrita en los primeros apartados, se ha podido evitar un impacto en la red de la universidad. Planificando los pasos correctamente, el usuario no ha percibido, exceptuando los problemas detectados después de la implementación, grandes cortes o problemas en la red.

Finalmente, para poder afirmar que seríamos totalmente seguros, mediante el DHCP configurado, tendríamos que fijar Ip's a cada ordenador dentro de la red, de esta manera, podríamos habilitar a máquinas específicas los puertos que necesitan sin abrir a toda la subred estos puertos, como sería el caso de las máquinas de contabilidad. Puesto que en nuestro ámbito siempre hay que mejorar, sería un proyecto para el futuro.

7. Bibliografía

https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-800-series

https://www.fortinet.com/products/next-generation-firewall/mid-range.html

https://www.sonicwall.com/es-mx/products/firewalls/mid-range

https://www.untangle.com/

https://www.vmware.com/es.html

https://forums.untangle.com/

https://www.speedguide.net/

https://es.stackoverflow.com/

8. Anexo

- Manual de Usuario.