



RED DE DATOS EMPRESARIAL

Daniel Serrano Gallur
I.T. Informática de gestión

Consultor: José Manuel Castillo Pedrosa

Junio de 2016

Copyright © 2016 Daniel Serrano Gallur.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free

FICHA DEL TRABAJO FINAL

Título del trabajo:	Red de datos empresarial
Nombre del autor:	Daniel Serrano Gallur
Nombre del consultor:	José Manuel Castillo Pedrosa
Fecha de entrega:	06/2016
Área del Trabajo Final:	Administración de redes y sistemas operativos.
Titulación:	I.T. Informática de gestión.
Resumen del trabajo (máximo 250 palabras):	
<p>Se desarrolla la conexión a nivel de red de una empresa que tiene tres sedes: un centro administrativo, un centro productivo y un centro logístico.</p> <p>Las tres sedes tendrán conexión a Internet mediante una línea principal y otra de respaldo. Además, el centro logístico dispondrá de una VPN permanente con el centro administrativo y con el centro productivo. El desarrollo será sobre un entorno supuesto.</p> <p>Respecto a la ubicación física de las tres sedes es la siguiente: el centro administrativo y el centro productivos están situados en el mismo polígono industrial a escasos 200 metros de distancia, el centro logístico está en un polígono industrial distinto a 30 kilómetros de distancia.</p>	

Índice

1. Introducción	1
1.1 Contexto i justificación del Trabajo	1
1.2 Objetivos del Trabajo	1
1.3 Enfoque y método seguido	1
1.4 Planificación del Trabajo	2
1.5 Resumen de productos obtenidos	2
2. Resto de capítulos	3
2.1. Diseño lógico de la red	3
2.2. Diseño físico de la red	5
2.3. Contratación de líneas de acceso a Internet.	9
2.4. Configuración de dispositivos de red	18
2.5. Plan de contingencias.	59
2.6. Costes del proyecto.	62
3. Conclusiones	63
4. Glosario	64
5. Bibliografía	67
6. Anexos	68
Anexo A: Protección de los switches.	68
Anexo B: Configuración de VLANs e IP de administración en los switches.	71
Anexo C: configuración de enlacen agregados y redundantes	73
Anexo D: Protección de los routers.	76
Anexo E: Configuración del entrutamiento en los routers	78
Anexo F: Configuración de la VPN entre las sedes	81
Anexo G: Instalación y configuración del servicio DHCP en Windows Server 2012	83
Anexo H: Instalación y configuración del servicio DNS en Windows Server 2012	103
Anexo I: Instalación y configuración de PfSense	119
Anexo J: Ficheros de configuración de switches y routers Cisco	134
Anexo K: Fichero “switch.cfg” de Nagios	198

Lista de figuras

Ilustración 1 – Diagrama de Gantt del Proyecto	2
Ilustración 2 - Diseño lógico	3
Ilustración 3 - Diseño físico centro administrativo y productivo	8
Ilustración 4 - Diseño físico centro logístico	8
Ilustración 5 - Solución propuesta Telefónica	10
Ilustración 6 - Imagen de nuestros enlaces	22
Ilustración 7 - Esquema físico de la distribución de los puntos de acceso	24
Ilustración 8 - Configuración de un punto de acceso	25
Ilustración 9 - Enlaces entre los routers y switches	28
Ilustración 10 - Diseño lógico y físico de la configuración IP de los routers	29
Ilustración 11 - Esquema lógico de configuración de VPN	31
Ilustración 12 - Ejemplo de ubicación de un cortafuegos	36
Ilustración 13 - Interface web ClearOS	38
Ilustración 14- Interface Web IPCOP	39
Ilustración 15 - Interface Web ZENTYAL	40
Ilustración 16 - Interface Web MONOWALL	42
Ilustración 17 - Interface Web PFSENSE	43
Ilustración 18 - Interface Web SMOOTHWALL	44
Ilustración 19 - Nagios: mapa con vista circular	56
Ilustración 20 - Nagios: vista en forma de lista	57
Ilustración 21 - Nagios: vista en forma de árbol	58
Ilustración 22 - Nagios en vista de árbol con dispositivo en fallo.	58
Ilustración 23 - Instalación DHCP (paso 1)	83
Ilustración 24 - Instalación DHCP (paso 2)	83
Ilustración 25 - Instalación DHCP (paso 3)	84
Ilustración 26 - Instalación DHCP (paso 4)	84
Ilustración 27 - Instalación DHCP (paso 5)	85
Ilustración 28 - Instalación DHCP (paso 6)	85
Ilustración 29 - Instalación DHCP (paso 7)	86
Ilustración 30 - Instalación DHCP (paso 8)	86

Ilustración 31 - Instalación DHCP (paso 9)	87
Ilustración 32 - Instalación DHCP (paso 10)	87
Ilustración 33 - Configuración DHCP (paso 1)	88
Ilustración 34 - Configuración DHCP (paso 2)	88
Ilustración 35 - Configuración DHCP (paso 2)	89
Ilustración 36 - Configuración DHCP (paso 3). Industrial.	89
Ilustración 37 - Configuración DHCP (paso 3). Usuarios.	90
Ilustración 38 - Configuración DHCP (paso 4). Industrial.	90
Ilustración 39 - Configuración DHCP (paso 4). Usuarios.	91
Ilustración 40 - Configuración DHCP (paso 5). Industrial.	91
Ilustración 41 - Configuración DHCP (paso 5). Usuarios.	92
Ilustración 42 - Configuración DHCP (paso 6).	92
Ilustración 43 - Configuración DHCP (paso 7).	93
Ilustración 44 - Configuración DHCP (paso 8). Industrial.	94
Ilustración 45 - Configuración DHCP (paso 8). Usuarios.	94
Ilustración 46 - Configuración DHCP (paso 9).	95
Ilustración 47 - Configuración DHCP (paso 10).	96
Ilustración 48 - Configuración DHCP (paso 11).	96
Ilustración 49 - Configuración DHCP (paso 12).	97
Ilustración 50 - Realizar reserva en DHCP (paso 1).	98
Ilustración 51 - Realizar reserva en DHCP (paso 2).	99
Ilustración 52 - DHCP: Copia de seguridad y restauración	99
Ilustración 53 - DHCP: Conmutación por error (paso 1)	100
Ilustración 54 - DHCP: Conmutación por error (paso 2)	101
Ilustración 55 - DHCP: Conmutación por error (paso 3)	101
Ilustración 56 - DHCP: Conmutación por error (paso 4)	102
Ilustración 57 - Instalación servicio DNS (paso 1)	103
Ilustración 58 - Instalación servicio DNS (paso 2)	103
Ilustración 59 - Instalación servicio DNS (paso 3)	104
Ilustración 60 - Instalación servicio DNS (paso 4)	104
Ilustración 61 - Instalación servicio DNS (paso 5)	105
Ilustración 62 - Instalación servicio DNS (paso 6)	105
Ilustración 63 - Instalación servicio DNS (paso 7)	106
Ilustración 64 - Instalación servicio DNS (paso 8)	106

Ilustración 65 - Configuración del servicio DNS (paso 1).	107
Ilustración 66 - Configuración del servicio DNS (paso 2).	107
Ilustración 67 - Configuración del servicio DNS (paso 3).	108
Ilustración 68 - Configuración del servicio DNS (paso 4).	108
Ilustración 69 - Configuración del servicio DNS (paso 5).	109
Ilustración 70 - Configuración del servicio DNS (paso 6).	109
Ilustración 71 - Configuración del servicio DNS (paso 7).	110
Ilustración 72 - Configuración del servicio DNS (paso 8).	110
Ilustración 73 - Configuración del servicio DNS (paso 9).	111
Ilustración 74 - Configuración del servicio DNS (paso 10).	111
Ilustración 75 - Configuración del servicio DNS (paso 11).	112
Ilustración 76 - Configuración del servicio DNS (paso 12).	112
Ilustración 77 - Configuración del servicio DNS (paso 13).	113
Ilustración 78 - Configuración del servicio DNS (paso 14).	113
Ilustración 79 - Configuración del servicio DNS (paso 15).	114
Ilustración 80 - Configuración del servicio DNS (paso 16).	114
Ilustración 81 - Configuración de reenviadores en servicio DNS (paso 1).	115
Ilustración 82 - Configuración de reenviadores en servicio DNS (paso 2).	116
Ilustración 83 - Configuración de reenviadores en servicio DNS (paso 3).	117
Ilustración 84 - Configuración de reenviadores en servicio DNS (paso 4).	117
Ilustración 85- Configuración de reenviadores en servicio DNS (paso 5).	118
Ilustración 86 - Descarga de PfSense	119
Ilustración 87 - Instalación PfSense (Paso 1)	119
Ilustración 88 - Instalación PfSense (Paso 2)	120
Ilustración 89 - Instalación PfSense (Paso 3)	120
Ilustración 90 - Instalación PfSense (Paso 4)	121
Ilustración 91 - Instalación PfSense (Paso 5)	121
Ilustración 92 - Instalación PfSense (Paso 6)	122
Ilustración 93 - Ubicación del cortafuegos	122
Ilustración 94 - Configuración PfSense (Paso 1)	123
Ilustración 95 - Configuración PfSense (Paso 2)	123
Ilustración 96 - Configuración PfSense (Paso 3)	124
Ilustración 97 - Configuración PfSense (Paso 4)	124
Ilustración 98 - Configuración PfSense (Paso 5)	125

Ilustración 99 - Configuración PfSense (Paso 6)	125
Ilustración 100 - Configuración PfSense (Paso 7)	126
Ilustración 101 - Configuración PfSense (Paso 8)	126
Ilustración 102 - Configuración PfSense (Paso 9)	127
Ilustración 103 - Configuración PfSense (Paso 10)	128
Ilustración 104 - Configuración PfSense (Paso 11)	128
Ilustración 105 - Configuración PfSense (Paso 12)	128
Ilustración 106 - Configuración PfSense (Paso 13)	129
Ilustración 107 - Configuración PfSense (Paso 14)	129
Ilustración 108 - Configuración PfSense (Paso 15)	130
Ilustración 109 - Configuración PfSense (Paso 16)	130
Ilustración 110 - Configuración PfSense (Paso 17)	130
Ilustración 111 - Configuración PfSense (Paso 18)	131
Ilustración 112 - Configuración PfSense (Paso 19)	131
Ilustración 113 - Configuración PfSense (Paso 20)	132
Ilustración 114 - Configuración PfSense (Paso 21)	132
Ilustración 115 - Configuración PfSense (Paso 22)	133

Lista de tablas

Tabla 1 - Direccionamiento IP	4
Tabla 2 - Solución propuesta Telefónica	9
Tabla 3 - Valoración económica Telefónica	10
Tabla 4 - Contenido de la oferta de Vodafone	13
Tabla 5 - Gestión del servicio de Vodafone	15
Tabla 6 - Características del servicio de Telefónica	16
Tabla 7 - Características del servicio de Vodafone	16
Tabla 8 - Valoración económica Telefónica	16
Tabla 9 - Direcciones IP de los switches	18
Tabla 10- Subredes de la organización	19
Tabla 11 - Enlaces entre dispositivos	20
Tabla 12 - Gateways predeterminados	23
Tabla 13 - Relación de puntos de acceso con switches	26
Tabla 14 - Enlaces entre switches y routers	28
Tabla 15 - Costes del proyecto.	62

1. Introducción

1.1 Contexto i justificación del Trabajo

Se parte de una empresa en plena expansión la cual abandona su antigua pequeña sede para trasladarse a una de nueva creación. La nueva sede se dividirá en tres partes: centro administrativo, centro productivo y centro logístico.

Con el actual proyecto se realizará la interconexión a nivel de infraestructura de red de los tres centros, tanto entre ellos como con el exterior (Internet).

Para la resolución del problema se realizará un diseño de la red (lógico y físico) y se implementará la instalación y configuración de los dispositivos de red necesarios.

1.2 Objetivos del Trabajo

El objetivo es cubrir las necesidades de conexión de red de datos de una empresa. Se cubrirá tanto la conexión interna entre diferentes tipos de dispositivos, como la conexión con el exterior (Internet).

Los objetivos parciales son los siguientes:

- Diseño lógico de la red.
- Diseño físico de la red.
- Contratación de líneas de acceso a Internet.
- Configuración de dispositivos de red.
- Monitorización de la red.
- Planes de contingencias.
- Costes del proyecto.

1.3 Enfoque y método seguido

Como metodología de trabajo en un primer lugar se analizan las necesidades del cliente y sus requerimientos.

En un segundo lugar se realiza un análisis de toda la información recogida para obtener un diseño lógico de la red.

Después, en tercer lugar, ya se puede realizar en base al diseño lógico un diseño físico de la red, incluyendo las configuraciones en los dispositivos de red, para cubrir el objetivo final de interconexión de sedes.

Por último, se establece un plan de contingencias antes fallos de la red y se implementa un sistema de monitorización de la misma.

1.4 Planificación del Trabajo

En el siguiente diagrama de Gantt queda reflejado el desglose temporal del desarrollo del Trabajo:

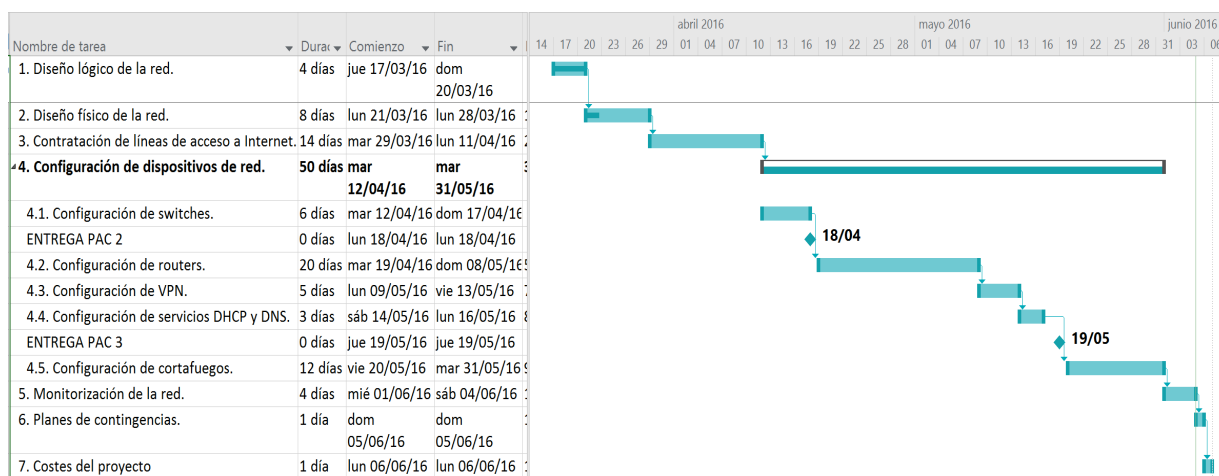


Ilustración 1 – Diagrama de Gantt del Proyecto

Recursos necesarios para la elaboración del Trabajo:

- Software: Cisco Packet Tracer, Microsoft Visio, Microsoft Project, Microsoft Office, Nagios, pfSense (firewall), Windows Server 2012, Ubuntu Server, Vmware Fusion.
- Hardware: ordenador capaz de ejecutar hasta cuatro máquinas virtuales a la vez para las pruebas del firewall. Procesador de cuatro núcleos con soporte de virtualización y ocho gigas de RAM.

1.5 Resumen de productos obtenidos

El producto final obtenido de este Trabajo será una red de datos de una empresa u organización totalmente funcional, que permitirá la interconexión entre sus sedes y conexión a Internet. Además, será una red totalmente escalable y ampliable en un futuro, según las necesidades de la organización.

English Version:

The final product of this work will be a data network of a company or organization fully functional, enabling the interconnection between their headquarters and Internet. It will also be a fully scalable and expandable network in the future, depending on the needs of the organization.

2. Resto de capítulos

2.1. Diseño lógico de la red

Descripción del diseño lógico de la red

El diseño lógico de la red a implementar consta de tres partes:

1. Centro logístico
2. Centro administrativo y el centro productivo.
3. Interconexión de ambos centros.

El centro logístico constará de una única red, un firewall y un router de acceso a Internet, además este dará conexión por VPN al centro administrativo y productivo.

El centro administrativo y el centro productivo constará de una red general subdividida en cinco redes para diferentes propósitos que se describirán en puntos posteriores. Además, dispondrá de un router de acceso a Internet y conexión VPN permanente con el centro logístico. Por último, también dispondrá de un firewall.

La interconexión entre ambas sedes será permanente por medio de una VPN.

Descripción del diseño lógico de la red

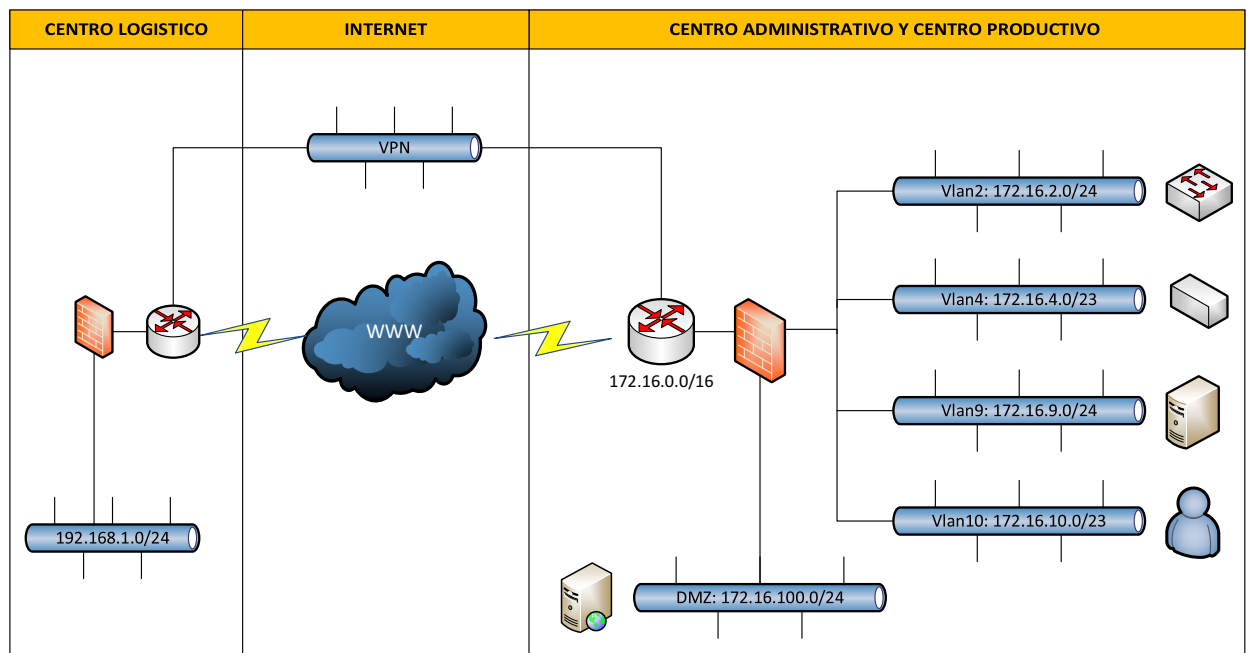


Ilustración 2 - Diseño lógico

Direccionamiento IP de la red

El direccionamiento IP de las redes en las sedes será el siguiente:

- Centro logístico -> 192.168.1.0/24

Este direccionamiento IP nos permitirá conectar 254 hosts. Dicha sede dispondrá de aproximadamente cuatro PCs, cuatro dispositivos inalámbricos y unos cuatro puntos de acceso distribuidos por la nave. Quedando así un amplio margen de ampliación de dispositivos.

- Centro Administrativo y centro productivo -> 172.16.0.0/16

Este direccionamiento nos permitirá realizar la posterior subdivisión de redes de una manera estructurada, además también permitirá un posterior crecimiento en número de hosts. En el siguiente apartado se define con más detalle dicha subdivisión.

Subredes: su direccionamiento y su funcionalidad

Dentro del centro administrativo y productivo se han generado las siguientes subredes:

IDENTIFICADOR	DIRECCIONAMIENTO	Nº HOSTS	FUNCIONALIDAD
VLAN 2	172.16.2.0/24	254	Administración de dispositivos de red.
VLAN 4	172.16.4.0/23	510	Dispositivos industriales: PLCs, RPI, Visión artificial, Dispositivos de pesaje, etc.
VLAN 9	172.16.9.0/24	254	Servidores
VLAN 10	172.16.10.0/23	510	PCs, portátiles, impresoras, dispositivos móviles.
VLAN 100	172.16.100.0/24	254	DMZ

Tabla 1 - Direccionamiento IP

Cabe destacar que se deja suficientes rangos de IPs entre la VLAN 4 y la VLAN 9 para la ampliación o subdivisión de la VLAN 4 en un futuro, ya que puede haber un crecimiento de la empresa. Igualmente existe esta posibilidad en a VLAN 10.

2.2. Diseño físico de la red

Descripción del diseño físico de la red

El diseño físico de la red se divide de la siguiente forma:

- Centro Administrativo.
- Centro Productivo.
- Enlace de respaldo.
- Centro Logístico.

A continuación se define con más detalles los elementos que componen los puntos anteriores y su propósito dentro de la infraestructura de red definida.

Centro Administrativo.

El centro administrativo es un edificio que se divide en tres plantas:

Planta Baja: consta de un *switch* para dar acceso a la red corporativa a los ordenadores e impresoras de los usuarios de dicha planta. Además, también consta de un *punto de acceso* inalámbrico para dar conexión a los dispositivos inalámbricos de dicha planta.

Primera planta: en dicha planta está situado el Centro de Proceso de Datos principal de la organización, en adelante CPD. Dicho CPD consta del *router* principal, que conecta a la organización con el exterior, a través de una conexión de acceso a Internet de fibra óptica. Seguidamente detrás del router se encuentra el *cortafuegos* y este a su vez conectado al CORE principal de red. El CORE principal de la red será un *switch* de capa 3 (permitiendo así enrutamiento) donde se conectarán los servidores de propósito general de la organización, así como los *switches* de acceso del edificio. Además, ha dicho CORE también se conectará el CORE secundario y el enlace de respaldo (cuya función la definiremos más adelante). Por último, en esta primera planta también dispondremos de un *switch* de acceso donde conectar ordenadores e impresoras (también situado en el CPD) y un punto de acceso para dar cobertura inalámbrica en esta planta.

Segunda planta: consta de un *switch* para dar acceso a la red corporativa a los ordenadores e impresoras de los usuarios de dicha planta. Además, también consta de un *punto de acceso* inalámbrico para dar conexión a los dispositivos inalámbricos de dicha planta.

Centro Productivo.

El centro productivo es una nave industrial que se divide en tres zonas:

Zona 1 (fabricación producto): consta de un *switch* para dar acceso a la red corporativa a los diferentes dispositivos industriales de dicha zona. Además, también consta de un *punto de acceso* inalámbrico para dar conexión a los dispositivos inalámbricos de dicha zona.

Zona oficinas fábrica: en dicha zona está situado el CPD secundario de la organización. Dicho CPD consta del *router* de backup que conecta a la organización con el exterior en caso de caída del router principal o de caída de la línea de datos de acceso a Internet principal. Dicha conexión de acceso a Internet se realiza mediante un radio enlace, teniendo así redundancia de conexión al exterior. El router secundario se encuentra conectado al CORE secundario de red. El CORE secundario de la red será un *switch* de capa 3 donde se conectarán los servidores de fabricación de la empresa, así como los *switches* de acceso de la nave. Además, ha dicho CORE secundario también se conectará el CORE principal y el enlace de respaldo (cuya función también la definiremos más adelante). Por último, en esta zona de oficinas también dispondremos de un *switch* de acceso donde conectar ordenadores e impresoras (también situado en el CPD secundario).

Zona 2 (producto final): consta de un *switch* para dar acceso a la red corporativa a los diferentes dispositivos industriales de dicha zona. Además, también consta de un *punto de acceso* inalámbrico para dar conexión a los dispositivos inalámbricos de dicha zona.

Enlace de respaldo.

El enlace de respaldo tiene el propósito de cubrir la comunicación entre el centro administrativo y el centro productivo en caso de caída de la línea de fibra óptica que une el CORE principal y el CORE secundario. Dicho enlace estaría en modo pasivo, siendo activo solo en caso de caída del enlace principal

Este enlace de respaldo consta de un *switch* colocado estratégicamente en una zona de unión de ambos centros mediante cables de cobre (4 cables por extremo, permitiendo así una ancho de banda más que aceptable).

Centro Logístico.

El centro logístico (nave industrial) tiene una infraestructura más sencilla que la descrita en los puntos anteriores ya que no dispone de servidores y los clientes se conectan por escritorio remoto a la sede central. Además consta de una serie de dispositivos inalámbricos para realizar las entradas y salidas de mercancía.

A continuación se describen los elementos de los que consta en el pequeño CPD que tiene:

- Línea principal de acceso a Internet: esta línea es de fibra óptica.
- Router principal: da conexión con el exterior y con la sede central a través de una VPN.
- Línea de respaldo de acceso a Internet: esta línea es mediante un radio enlace para en caso de caída de la línea principal de acceso a Internet.
- Router de respaldo: este está en modo pasivo, y se activa en caso de caída de la línea principal de acceso a Internet o en caso de caída del router principal.
- Switch de acceso: donde se conecta el cortafuegos (línea principal) y el router de respaldo (línea secundaria). Además, a él también se conectan tres puntos de acceso inalámbricos distribuidos por la nave industrial para dar cobertura a los dispositivos inalámbricos. Por último, también se le conectan los ordenadores e impresoras que hay en dicha sede.

Esquema del diseño físico de la red

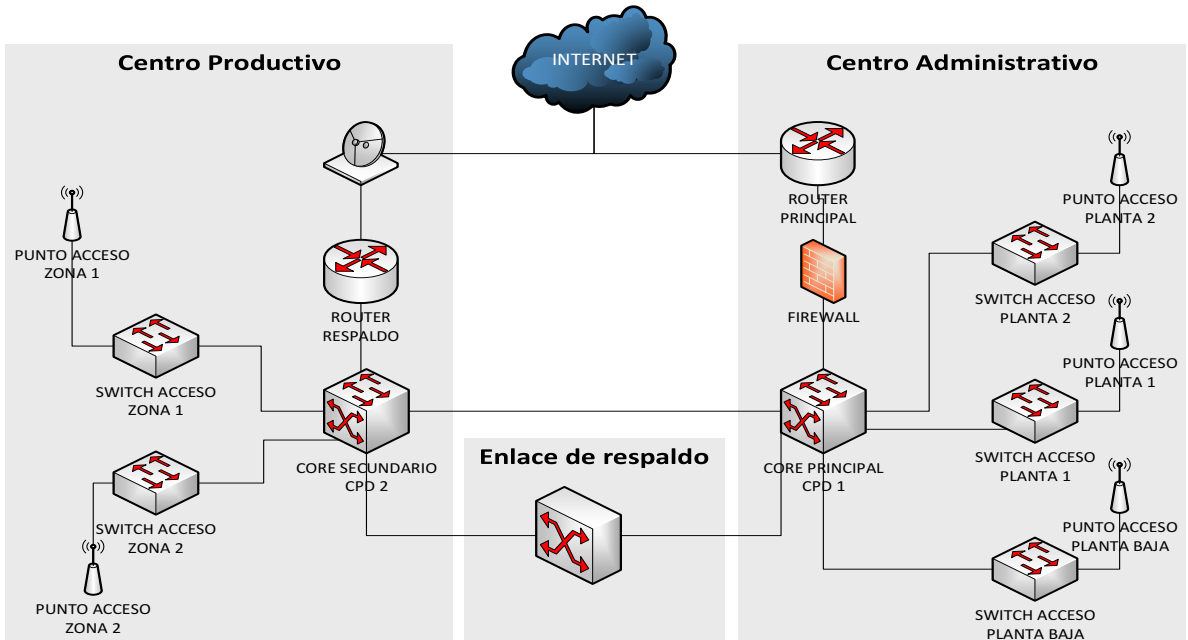


Ilustración 3 - Diseño físico centro administrativo y productivo

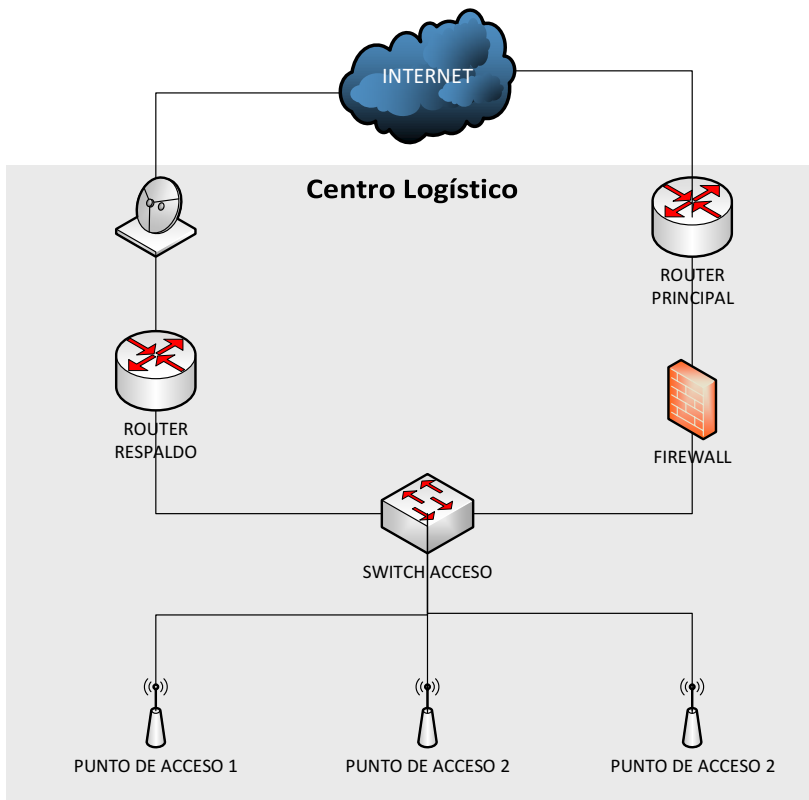


Ilustración 4 - Diseño físico centro logístico

2.3. Contratación de líneas de acceso a Internet.

Búsqueda de proveedores en el mercado.

Se realiza la consulta para la contratación de servicios de Internet a través de fibra óptica a dos de las grandes operadoras de comunicaciones en España: Vodafone (ONO) y Telefónica.

Telefónica.

Telefónica se presenta como una empresa líder mundial, capaz de proporcionar una solución integral y global para las Tecnologías de la Información y Comunicaciones de nuestra organización. Además dispone de un departamento de I+D que proporciona constantemente nuevas soluciones para sus clientes, basadas siempre en las tecnologías más punteras del mercado, con la calidad y garantía de Telefónica.

Solución propuesta y descripción de la oferta.

Telefónica presenta una oferta para la constitución de una red mediante la integración en una VPN de nuestras distintas sedes, con el siguiente escenario de red:

	TIPO DE ACCESO	CAUDAL VPN	CAUDAL INTERNET	TIPO DE BACKUP
CENTRO ADMINISTRATIVO Y PRODUCTIVO	Fibra Óptica	100 Mbps	40 Mbps	Radio Enlace 100 Mbps
CENTRO LOGISTICO	Fibra Óptica	10 Mbps	Mismos 10 Mbps que VPN	ADSL 20 Mbps

Tabla 2 - Solución propuesta Telefónica

Descripción de la Oferta

Solución propuesta

- ESQUEMA DE RED:

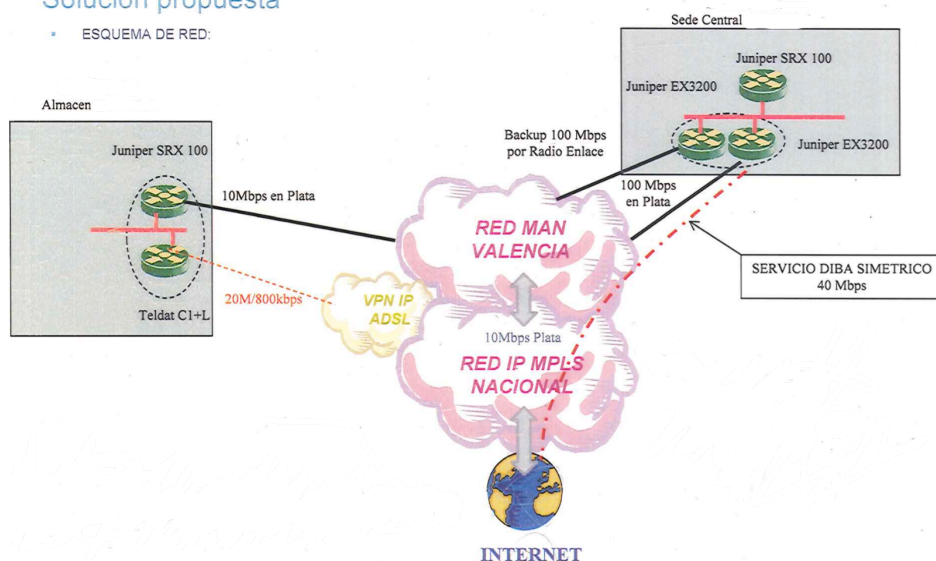


Ilustración 5 - Solución propuesta Telefónica

Valoración económica.

Seguidamente se muestra el detalle económico de la propuesta. A la aceptación de la oferta se formalizará un contrato con una duración mínima de 3 años. Los precios indicados no incluyen IVA.

SEDE		COSTE MENSUAL	
CENTRO PRODUCTIVO	ADMINISTRATIVO	Y	1.739 €
CENTRO LOGISTICO			1.416 €
TOTAL COSTE MENSUAL			3.155 €

Tabla 3 - Valoración económica Telefónica

Condiciones del servicio.

El plazo para la aceptación por parte del cliente de la presente oferta es de treinta días a partir de la fecha indicada.

Los precios indicados en este documento no incluyen los impuestos vigentes.

Ante cualquier variación de los datos de partida, servicios, trabajos o equipamientos contemplados en el presente documento, Telefónica se reserva el derecho a realizar un nuevos estudio y una nueva valoración económica, sin que sean de aplicación a los nuevos servicios, trabajos o equipamientos de

forma automática lo dispuesto en la presente oferta, salvo manifestación en contrario.

La presente oferta se considerará vinculante desde el momento de su aceptación por parte del cliente, o desde el inicio de la prestación de los servicios objeto e la presente oferta por parte de Telefónica a solicitud del cliente si éste fuera anterior a la aceptación.

Telefónica responderá de los daños y perjuicios ocasionados directamente al cliente, por causa exclusivamente imputable a Telefónica en relación con el presente contrato y la prestación de los servicios objeto del mismo. El resarcimiento de daños y perjuicios alcanzará hasta una suma máxima equivalente al precio a pagar por el cliente por el servicio o servicios afectados por el plazo de un mes en relación con los servicios objeto de reclamación, y/o no excederá del 5% del valor de los productos objeto del contrato si los hubiese. Para ello se calculará la media mensual correspondiente a la anualidad anterior o, en caso de no haber transcurrido un año desde el inicio en la prestación del servicio, a los meses transcurridos.

La vigencia inicial de los servicios detallados en la presente oferta será de tres años salvo que se acuerde otro plazo.

Finalizada la duración inicial del contrato de prestación del servicio, éste se prorroga por periodos de un año, a no ser que cualquiera de las partes manifieste lo contrario con una antelación mínima de quince días a la fecha de terminación del periodo inicial o de cualquiera de sus prórrogas. Telefónica se reserva el derecho a aplicar a los precios comprometidos las posibles variaciones del IPC del año vencido, según los datos oficiales publicados por el INE.

Vodafone

El grupo Vodafone es un líder mundial en el suministro de servicios de comunicaciones, incluyendo voz, acceso a Internet, mensajería y otros servicios de datos con presencia en los cinco continentes.

Vodafone España se presenta como un operador que asume compromisos, los cumple y apuesta fuertemente por el futuro. Su apuesta por la globalidad se fundamenta en:

- Redes e infraestructuras propias de última generación basados en protocolos IP y nodos de red inteligente sobre redes de conmutación y transporte IP, que permiten el soporte de esa gama de servicios avanzados.
- Servicios muy competitivos, que se adaptan de forma sencilla a las necesidades de los distintos tipos de clientes así como en la implantación de soluciones integradas.

Solución propuesta y descripción de la oferta.

El servicio de Oficina Vodafone emplea MPLS para interconectar las distintas sedes de la compañía de forma segura a través de la Red Privada IP de Vodafone:

- Calidad: servicio basado en la red de última generación de Vodafone. Infraestructura de red de fibra óptica propia con las más altas calidades: 24 horas al día, 7 días a la semana, 365 días al año.
- Escalabilidad: topología mallada entre todas las sedes de la organización lo que permite añadir nuevas conexiones a la VPN de forma transparente para las ya existentes.
- Innovación: MPLS ofrece niveles de rendimiento diferenciados por clase de servicio y priorización de aquellos tráficos considerados más críticos por la organización.
- Robustez: solución de alta disponibilidad, backup de línea de acceso o backup dual.
- Flexibilidad: el acceso desde las dependencias de la organización hasta la red de Vodafone se realizará mediante el despliegue de la infraestructura necesaria (DSL, PaP, 3G) y con la solución tecnológica más apropiada (bucle de abonado, radioenlace, cable, fibra óptica...)

Tecnologías de acceso:

- Acceso ADSL indirecto:
 - Tecnología basada en el par de cobre.
 - Acceso local a través de Telefónica en calidad de mayorista.
 - Velocidades de transmisión del servicio: 3M y 10M asimétricos. 1M simétrico.
- Bucle local desagregado:
 - Totalmente regulado.
 - Vodafone gestiona totalmente el par y está capacitado para ofrecer cualquier perfil y garantizar calidades de servicio.
 - Velocidades del servicio para accesos asimétricos: 6M y 12M.
 - Velocidades del servicio para accesos simétricos: 1M, 2M y 4M. Garantía del 100%.
- Circuitos dedicados:
 - Circuitos dedicados y con una garantía del 100%.
 - Ancho de banda simétrico de 2Mbps a 10Mbps.
 - Mediante cobre, radioenlace propio o fibra óptica.
- GPRS/3G/HSPA:
 - Tecnología GPRS/UMTS/HSPA.
 - Velocidad de hasta 7,2Mbps de bajada y 2Mbps de subida de datos. El ancho de banda depende de la cobertura y la concurrencia que haya en cada momento.

- Necesario asociar el acceso a una Tarjeta SIM con plan de precios de datos 3G.

Vodafone presenta una oferta para la constitución de una red mediante la integración en una VPN de nuestras distintas sedes, con el siguiente escenario de red:

	TIPO DE ACCESO	CAUDAL VPN	CAUDAL INTERNET	TIPO DE BACKUP
CENTRO ADMINISTRATIVO Y PRODUCTIVO	Fibra Óptica	100 Mbps	100 Mbps	Radio Enlace 100 Mbps
CENTRO LOGISTICO	Fibra Óptica	10 Mbps	Mismos 10 Mbps que VPN	ADSL 20 Mbps

Tabla 4 - Contenido de la oferta de Vodafone

Otras características personalizadas del servicio:

- Conexión para permitir la navegación de los usuarios de la delegación.
- Conexión para permitir la navegación de los usuarios a toda la empresa (tanto los usuarios de la sede central como la sede del centro logístico que se conectan a través de la VPN).
- Conexión a Internet para los servidores públicos del cliente (servidor web, correo, etc.)
- Conexión a la red local de los usuarios remotos que se conectan a través de Internet.
- Posibilidad de asignación de un rango de direcciones IP públicas propiedad de Vodafone.

Ventajas de la solución propuesta:

- Oficina Vodafone Company Net:
- Eficiencia:
 - Gestión más eficaz del ancho de banda.
 - Implementación de políticas de Calidad de servicio para poder priorizar el tráfico de la empresa en función de su criticidad, siempre condicionado a la tipología de acceso de cada sede en particular.
 - Routing optimizado en la red: comunicación directa entre los diferentes CPEs.
 - Mayor velocidad de enrutamiento.
- Escalabilidad:

- La posibilidad de interconectarse “todos con todos” permite la inclusión de nuevas sedes a la VPN de forma ágil y sencilla, sin modificar la configuración del resto de sedes en funcionamiento, lo que le añade una gran transparencia a la solución.
- Seguridad:
 - Direccionamiento IP totalmente privado para la VPN del cliente.
 - Prevención de intrusiones derivadas de la utilización de direccionamiento IP público accesible desde Internet.
- Flexibilidad:
 - El acceso desde las sedes de la organización a la red de Vodafone se realiza sobre cualquier tipo de acceso buscando en cada caso la solución que mejor se adapte a sus necesidades.
- Garantía:
 - Vodafone se responsabiliza de la entrega, instalación y puesta en marcha de los distintos elementos que forman el proyecto de comunicación de datos.
 - Vodafone se hará cargo de la gestión y mantenimiento de los equipos y líneas de acceso para así poder garantizar el máximo nivel de calidad.
- Internet:
 - Flexibilidad:
 - El acceso desde las sedes de la organización a la red de Vodafone se realiza sobre cualquier tipo de acceso buscando en cada caso la solución que mejor se adapte a sus necesidades.
 - Garantía:
 - Vodafone se responsabiliza de la entrega, instalación y puesta en marcha de los distintos elementos que forman el proyecto de comunicación de datos.
 - Vodafone se hará cargo de la gestión y mantenimiento de los equipos y líneas de acceso para así poder garantizar el máximo nivel de calidad.

Implantación: el plazo estimado de entrega de la solución ofrecida a la organización es de 15 semanas.

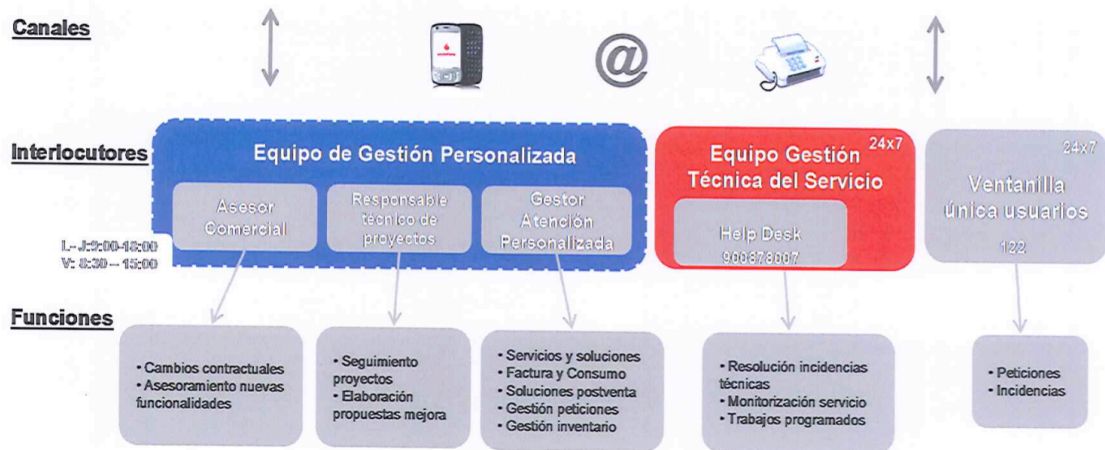


Tabla 5 - Gestión del servicio de Vodafone

Valoración económica.

- Facturación:
 - Alta: 0 €
 - Cuota mensual: 3.053,05 €
- Características proyecto:
 - Duración contrato: 5 años.
 - Descuenta de alta por duración de contrato: 100%

Comparativa de ofertas

Características del servicio

Telefónica:

	TIPO DE ACCESO	CAUDAL VPN	CAUDAL INTERNET	TIPO DE BACKUP
CENTRO ADMINISTRATIVO Y PRODUCTIVO	Fibra Óptica	100 Mbps	40 Mbps	Radio Enlace 100 Mbps
CENTRO LOGISTICO	Fibra Óptica	10 Mbps	Mismos 10 Mbps que VPN	ADSL 20 Mbps

Tabla 6 - Características del servicio de Telefónica

Vodafone:

	TIPO DE ACCESO	CAUDAL VPN	CAUDAL INTERNET	TIPO DE BACKUP
CENTRO ADMINISTRATIVO Y PRODUCTIVO	Fibra Óptica	100 Mbps	100 Mbps	Radio Enlace 100 Mbps
CENTRO LOGISTICO	Fibra Óptica	10 Mbps	Mismos 10 Mbps que VPN	ADSL 20 Mbps

Tabla 7 - Características del servicio de Vodafone

Valoración económica.

Telefónica.

SEDE	COSTE MENSUAL
CENTRO ADMINISTRATIVO Y PRODUCTIVO	1.739 €
CENTRO LOGISTICO	1.416 €
TOTAL COSTE MENSUAL	3.155 €

Tabla 8 - Valoración económica Telefónica

Vodafone.

- Alta: 0 €
- Cuota mensual: 3.053,05 €

Otras características.

- Telefónica.
 - Duración contrato: 3 años.
 - Plazo de entrega de implementación del servicio: no definido.
- Vodafone.
 - Duración contrato: 5 años.
 - Plazo de entrega de implementación del servicio: 15 semanas.

Elección del proveedor de servicios de Internet

Siendo las dos operadoras de Internet analizadas grandes y fiables en sus servicios ofrecidos nos decantamos en la elección por la compañía **VODAFONE** por los siguientes motivos:

1. Mejor precio.
2. Mejor ancho de banda en el caudal de Internet.
3. Oferta mejor elaborada, trabajada y con mejor nivel de detalle de lo solicitado.

2.4. Configuración de dispositivos de red

El [Anexo J: Ficheros de configuración de switches y routers Cisco](#) contiene todo el contenido del “running-config” de los dispositivos Cisco (switches y routers) usados para este Trabajo mediante el software Cisco Packet Tracer. Además en la documentación entregada junto a esta memoria también se entrega el fichero con extensión “PKT” que contiene el diseño e implementación de los switches y routers empleados para la realización de este Trabajo, para realizar las pruebas oportunas.

Configuración de switches

Protección de dispositivos.

Lo primero que pasos que debemos realizar en los switches es establecer las medidas de seguridad adecuadas para proteger los dispositivos de acceso no autorizados.

Dichos pasos de configuración son descritos en el [Anexo A: Protección de los switches](#) del presente documento.

Configuración de Vlans e IP de administración.

En este apartado se explica los pasos a seguir para dotar a los switches de una IP de administración, que nos aportara la ventaja de poder conectarnos vía SSH (configurado en el punto anterior) para su administración y gestión.

Para ello tal y como se especificó en el diseño lógico de la red se hará uso de la Vlan 2, con la asignación de las siguientes IPs:

DISPOSITIVO	IP	MASCARA
CA-CORE	172.16.2.1	255.255.255.0
CP-CORE	172.16.2.2	255.255.255.0
ER-ER	172.16.2.3	255.255.255.0
CA-P0	172.16.2.4	255.255.255.0
CA-P1	172.16.2.5	255.255.255.0
CA-P2	172.16.2.6	255.255.255.0
CP-Z1	172.16.2.7	255.255.255.0
CP-Z2	172.16.2.8	255.255.255.0
CL-Z1	192.168.1.1	255.255.255.0

Tabla 9 - Direcciones IP de los switches

En este proceso también se aprovechara la creación de la Vlan 2 para crear el resto de Vlans definidas en el diseño lógico:

VLAN	DIRECCIONAMIENTO	FUNCION
VLAN 2	172.16.2.0/24	RED DE ADMINISTRACION
VLAN 4	172.16.4.0/23	RED INDUSTRIAL
VLAN 9	172.16.9.0/24	RED SERVIDORES
VLAN 10	172.16.10.0/23	RED USUARIOS
VLAN 100	172.16.100.0/24	RED DMZ

Tabla 10- Subredes de la organización

Dichos pasos de configuración son descritos en el [Anexo B: Configuración de VLANs e IP de administración en los switches](#), del presente documento.

Configuración de enlaces entre dispositivos.

Para la interconexión entre dispositivos se utiliza el criterio definido en la siguiente tabla:

DISPOSITIVO	INTEFACE	PROPOSITO
CORES	GI1-2	CORE
CORES	FA1-2	CORE RESPALDO
CORES	FA22-24	SWITCHES ACCESO
CORES	FA3-21	SERVIDORES
SWITCH ACCESO	FA1	AP
SWITCH ACCESO	FA24	CORE
SWITCH ACCESO	FA2-23	ACCESO
ENLACE RESPALDO	FA1-2	CORE PRINCIAL
ENLACE RESPALDO	FA3-4	CORE SECUNDARIO

Tabla 11 - Enlaces entre dispositivos

Para el funcionamiento de estos enlaces es necesaria la configuración de las conexiones en modo TRUNK para que admita todo tipo de tráfico procedente de distintas VLANs. Para ello procedemos con los siguientes comandos en las distintas interfaces tal y como se definió en la tabla anterior.

Ejemplo de enlace entre el core principal y el core secundario:

```
>configure terminal
>interface range g0/1-2
>switchport mode trunk
>switchport trunk encapsulation dot1q
```

Configuración enrutamiento entre VLANs.

Para conseguir el enrutamiento entre las distintas VLANs debemos activar el ruteo en capa 3 en los 3 dispositivos multicapa, permitiendo así el acceso desde una IP de una VLAN a otra distinta. Para ello introducimos los siguientes comandos (ejemplo del CORE principal):

```
>configure terminal
>ip routing
>interface vlan 4
>ip address 172.16.4.1 255.255.254.0
>exit
>interface vlan 9
>ip address 172.16.9.1 255.255.255.0
>exit
>interface vlan 10
>ip address 172.16.10.1 255.255.254.0
>exit
>interface vlan 100
>ip address 172.16.100.1 255.255.255.0
>exit
```

Después de esta configuración ya podríamos utilizar estas IPs como puerta de enlace en la configuración de red de los dispositivos de acceso. Por ejemplo, una configuración de un PC de usuario podría ser la siguiente:

Dirección IP: 172.16.10.10

Mascara: 255.255.254.0

Puerta de enlace: 172.16.10.1

Además de estas configuración al switch de acceso que conectáramos dicho PC tendríamos que darle acceso a dicha VLAN con los siguiente comandos introducidos en el dicho switch:

```
>configure terminal
>interface f0/2
>switchport mode access
>switchport access vlan 10
>exit
```

Configuración de enlaces agregados y redundantes.

En este punto definiremos unos enlaces agregados entre nuestros dispositivos CORE y además haremos que nuestros enlaces sean redundantes.

La agregación de enlaces permite la creación de enlaces lógicos que se componen de dos o más enlaces físicos. Esto proporciona un mayor rendimiento más allá del uso de un único enlace físico. Si uno de los enlaces falla, la agregación de enlaces también proporciona redundancia.

Configuraremos EtherChannel, que es una forma de agregación de enlaces que se utiliza en las redes conmutadas. Lo haremos mediante el protocolo de agregación de puertos (PAgP) y el protocolo de control de agregación de enlaces (LACP).

PAgP es un protocolo exclusivo de Cisco que solo se puede ejecutar en switches Cisco. LACP es un protocolo de agregación de enlaces definido en IEEE 802.3ad y no se asocia a ningún proveedor específico. En LACP cuando falla alguno de los puertos activos, se activa un puerto en espera. El modo de espera funciona solo para LACP, no para PAgP.

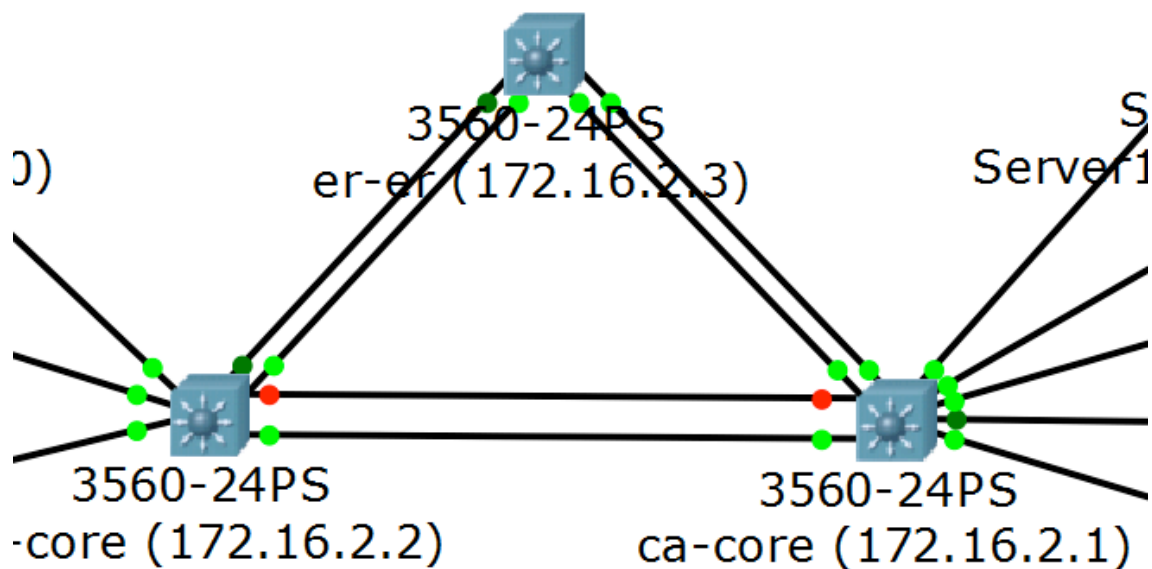


Ilustración 6 - Imagen de nuestros enlaces

En el [Anexo C: configuración de enlaces agregados y redundantes](#) se muestra cómo proceder para la configuración.

Configuración de protocolo de redundancia de primer salto (HSRP).

En este apartado vamos a proporcionar a nuestra red de gateways predeterminados redundantes para los dispositivos de los usuarios finales, para en el caso de que falle uno de los dos COREs que unen el centro administrativo y el centro productivo. Para ello utilizaremos el protocolo de redundancia de primer salto (HSRP) que proporcionan gateways predeterminados redundantes para los terminales sin necesidad de una modificación tras una caída en el usuario final.

Para realizar dicha configuración seguiremos el siguiente esquema:

VLAN	DEFAULT GATEWAY
VLAN 2	172.16.2.250
VLAN 4	172.16.5.250
VLAN 9	172.16.9.250
VLAN 10	172.16.11.250
VLAN 100	172.16.100.250

Tabla 12 - Gateways predeterminados

Se introducen en los dispositivos CA-CORE y CP-CORE los siguientes cambios, tras entrar en el modo de configuración:

```
>config t
>interface vlan 2
>standby 1 ip 172.16.2.250
>standby 1 priority 90 (valor 90 en CA-CORE y valor 80 en CP-CORE)
>standby 1 preempt
>exit
```

Dicha configuración se introduce en el resto de VLANs tal y como se muestra en la tabla anterior.

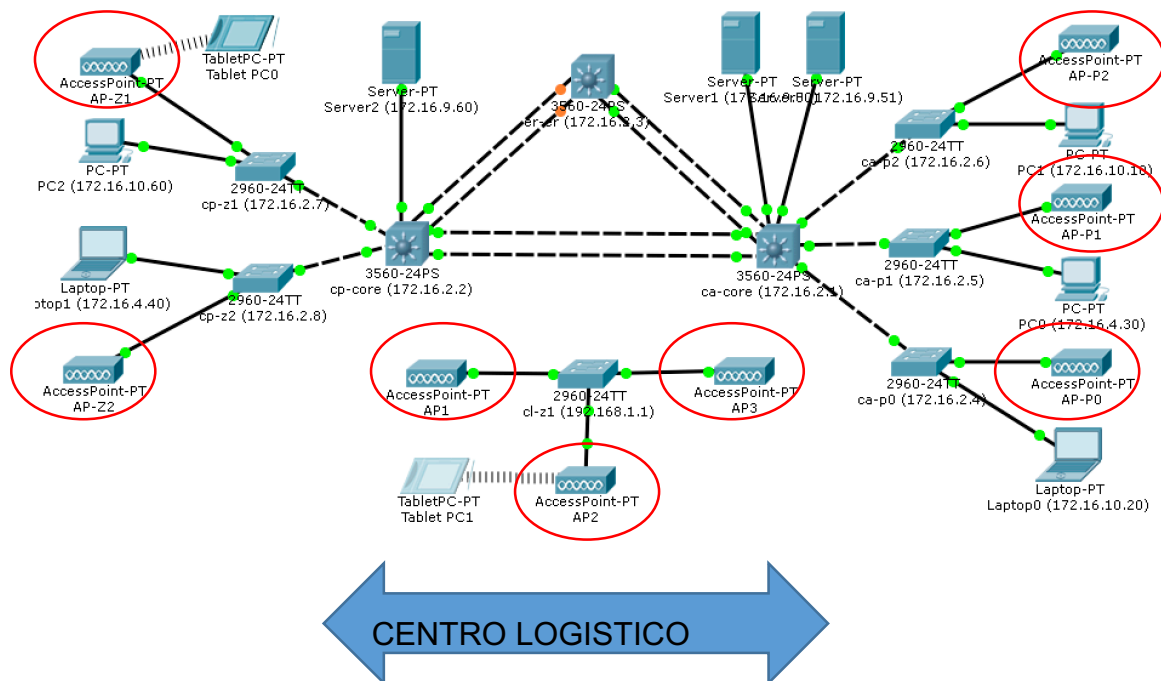
Distribución y configuración de dispositivos puntos de acceso inalámbricos.

Es este apartado se describe la distribución, conexionado y configuración de los dispositivos de acceso inalámbrico en la organización.

La distribución de los puntos de acceso en la siguiente:

- ❖ Centro Administrativo:
 - Planta 2 (1): AP-P2.
 - Planta 1 (1): AP-P1.
 - Planta baja (1): AP-P0.
- ❖ Centro Productivo:
 - Zona 1 (1): AP-Z1.
 - Zona 2 (1): AP-Z2.
- ❖ Centro Logístico:
 - Zona 1 (1): AP1.
 - Zona 2 (1): AP2.
 - Zona 3 (1): AP3.

Ilustración 7 - Esquema físico de la distribución de los puntos de acceso



La configuración de esta sección se divide en dos partes: configuración del punto de acceso y configuración del switch de acceso.

1. Configuración del punto de acceso:

Configurar una SSID tal y como muestra en la imagen:

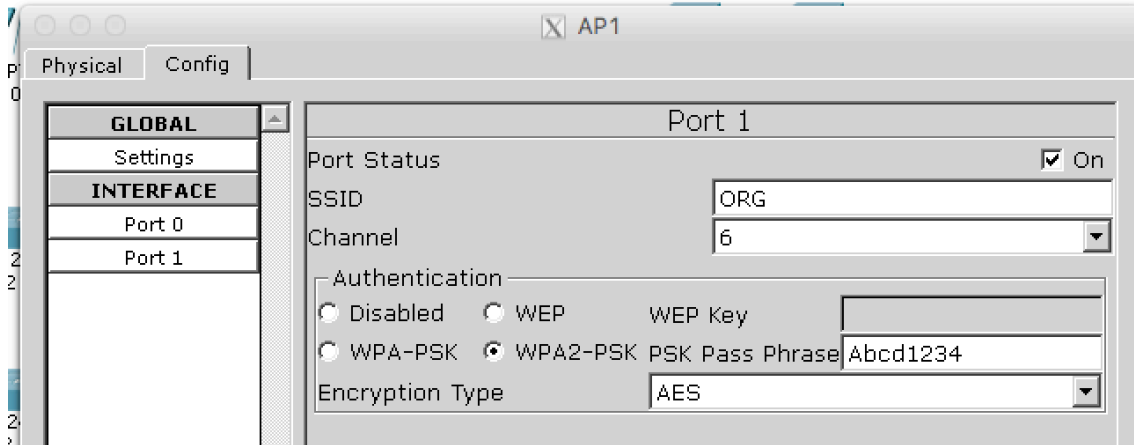


Ilustración 8 - Configuración de un punto de acceso

- SSID: ORG (Utilizaremos como SSID a publicar y conectarse el nombre de ORG)
- Authentication: WPA2-PSK: Abcd1234 (Utilizaremos como autenticación WPA2-PSK por ser de las más seguras que existen, con la contraseña "Abcd1234")

2. Configuración de los switches de acceso.

En puntos posteriores se procederá a configurar un servidor DHCP que nos permita asignar de forma automática IPs a los clientes de la subred de USUARIOS (VLAN 10). Por este motivo, y por su funcionalidad debemos poner la toma del switch a la que conectamos los puntos de acceso en modo de acceso a la VLAN 10 (VLAN 2 en centro logístico) para ello procedemos de la siguiente forma tras conectar a los switches:

```
>config t
>interface f0/1
>switchport mode access
>switchport access vlan 10
>exit
```

Repetir estos pasos en todos los dispositivos siguiendo la distribución de la siguiente tabla:

PUNTO ACCESO	DE SWITCH ACCESO	DE INTERFAZ	VLAN
AP-P2	CA-P2	F0/1	VLAN 10
AP-P1	CA-P1	F0/1	VLAN 10
AP-P0	CA-P0	F0/1	VLAN 10
AP-Z1	CP-Z1	F0/1	VLAN 10
AP-Z2	CP-Z2	F0/1	VLAN 10
AP1	CL-Z1	F0/1	VLAN 2
AP2	CL-Z1	F0/2	VLAN 2
AP3	CL-Z1	F0/3	VLAN 2

Tabla 13 - Relación de puntos de acceso con switches

Configuración de routers

Protección de dispositivos.

A continuación se definen los pasos necesarios para proteger los routers de Cisco de la organización.

Se protegerán los dispositivos mediante una contraseña cifrada para las conexiones de consola y conexiones de red seguras mediante el protocolo SSH.

Se van a introducir las medidas de seguridad en los siguientes dispositivos:

1. Centro administrativo:
 - 1.1. Router principal (R-CA).
2. Centro Productivo:
 - 2.1. Router de respaldo (R-CP).
3. Centro Logístico:
 - 3.1. Router principal (RP).
 - 3.2. Router de respaldo (RB).

En el [Anexo D: Protección de los routers](#) se muestra cómo proteger los routers detallados en la lista anterior.

Configuración de enlaces entre dispositivos.

Para la interconexión entre los switches y los routers para tener conexión con el exterior y entre las sedes administrativa/productiva y la sede logística se sigue el siguiente esquema:

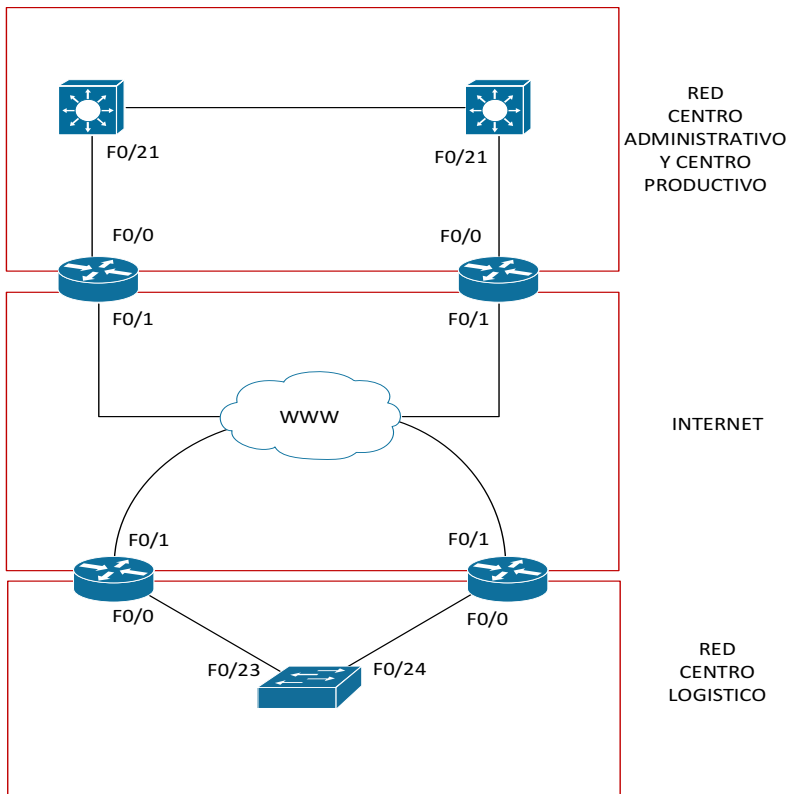


Ilustración 9 - Enlaces entre los routers y switches

Tabla de enlaces entre dispositivos, incluyendo interfaces de conexión:

UBICACION	DISPOSITIVO 1	INTEFACE 1	DISPOSITIVO 2	INTEFACE 2
SEDE ADMINISTRATIVA	CA-CORE	F0/21	R-CA	F0/0
SEDE PRODUCCION	CP-CORE	F0/21	R-CP	F0/0
SEDE ADMINISTRATIVA	R-CA	F0/1	ISP	
SEDE PRODUCCION	R-CP	F0/1	ISP	
SEDE LOGISTICA	RP	F0/1	ISP	
SEDE LOGISTICA	RB	F0/1	ISP	
SEDE LOGISTICA	CL-Z1	F0/23	RB	F0/0
SEDE LOGISTICA	CL-Z1	F0/24	RA	F0/0

Tabla 14 - Enlaces entre switches y routers

Configuración del enrutamiento.

Para el enrutamiento vamos a utilizar OSPF que es un protocolo de encaminamiento jerárquico o de IGP (Protocolo de Gateway interior), el cual utiliza el algoritmo Dijkstra para calcular la ruta más corta posible. OSPF se basa en el estado del enlace el cual es un tipo de protocolo que se basa en un conocimiento exacto de la topología de la red sobre la que se trabaja. Así se crean tablas de encaminamiento basadas en la información de la topología de la red, a partir de paquetes denominados de estados de enlace que se intercambian los routers entre sí para conocer el estado del enlace.

Al ser un protocolo que se diseñó para reemplazar al protocolo RIP, en OSPF se destaca su mayor variedad de métrica de distancia en donde se contempla la distancia física, retardos, y otros. Además, es un protocolo que posee un algoritmo dinámico, el cual se adapta automática y rápidamente a los cambios de la topología. Otra importancia de OSPF son los tipos desconexiones y redes que soporta como las líneas punto a punto entre dos enrutadores, las redes multiacceso con difusión como las LAN y las redes multiacceso sin difusión como las WAN de paquetes conmutados. Frente al protocolo RIP, en OSPF las rutas que se calculan nunca presentan bucles, puede escalar a interconexiones de redes mayores. Las principales desventajas que presenta OSPF es que requiere mayor capacidad de memoria y potencia de procesamiento, además de que requiere un diseño jerárquico estricto.

En el [Anexo E: Configuración del enrutamiento en los routers](#) se detalla los pasos a seguir para la configuración de dicho enrutamiento en los routers.

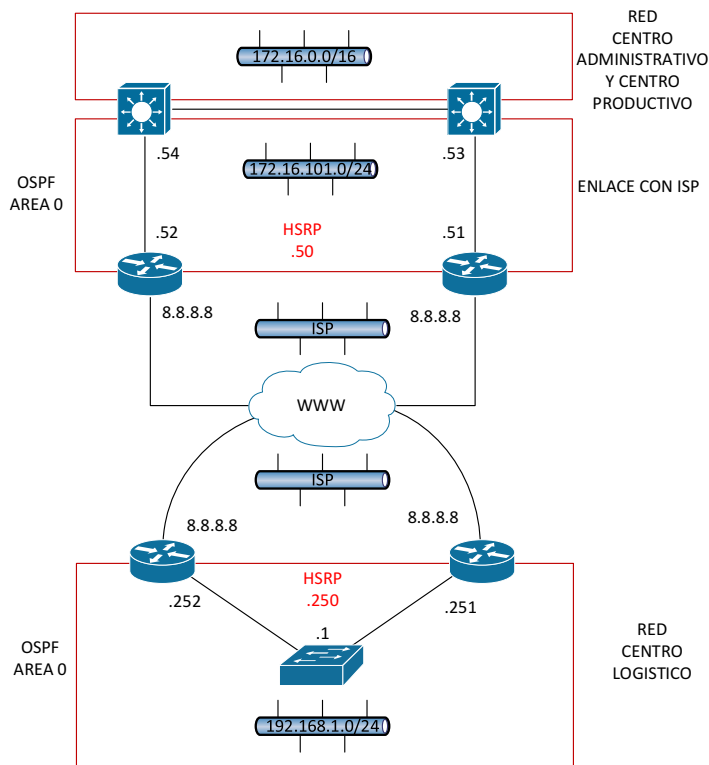


Ilustración 10 - Diseño lógico y físico de la configuración IP de los routers

Configuración de VPN.

Para la conexión de red permanente del centro logístico con el centro administrativo y el centro productivo vamos a configurar una VPN, para ello haremos la configuración de un túnel GRE mediante los routers de Cisco.

Generic Routing Encapsulation (GRE) es un protocolo del nivel de transporte que puede encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre dos máquinas que estén comunicándose por este protocolo. Su uso principal es crear túneles VPN.

En esta configuración vamos a incluir dos routers que simularán los routers del proveedor de servicios de Internet, ISP1 y ISP2. Además, para realizar las pruebas de balanceo se debe cortar totalmente los dos extremos de un ISP.

En el [Anexo F: Configuración de la VPN entre las sedes](#) se detalla los pasos a seguir para la configuración de la VPN entre las sedes Centro Administrativo-Productivo <-> Centro Logístico.

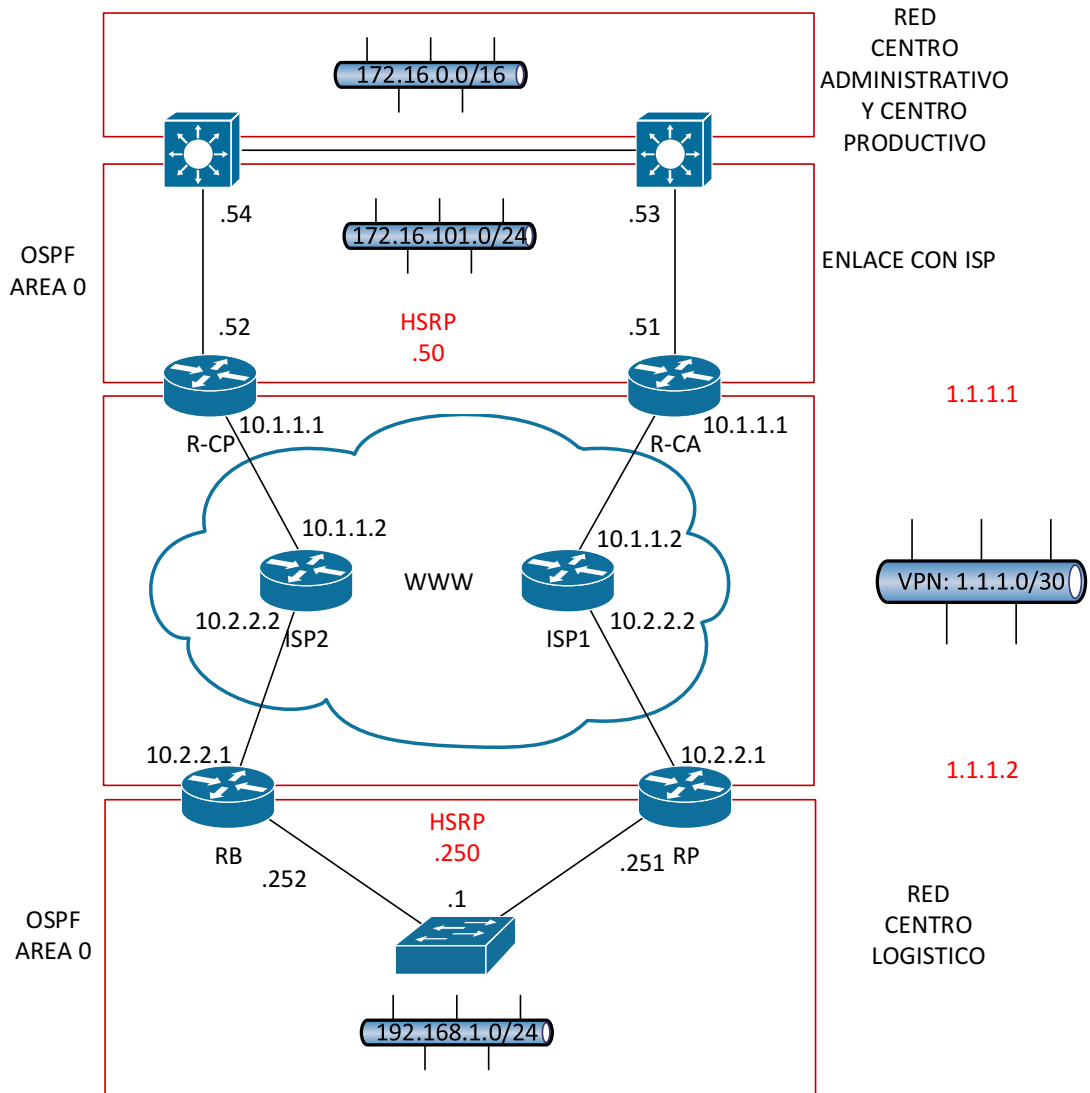


Ilustración 11 - Esquema lógico de configuración de VPN

Servicio DHCP

Partiendo de nuestro escenario actual vamos a instalar y configurar un servidor DHCP para el centro administrativo y productivo. El centro logístico por su pequeño tamaño no va a utilizar DHCP y tendrá IPs fijas en los dispositivos finales.

DHCP (Protocolo de configuración de host dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración de red en forma dinámica.

Los objetivos principales de la implementación del DHCP es simplificar la administración de la red, evitar errores respecto a la configuración IP e incluso disminuir el desperdicio de direcciones IP en la red.

El servicio DHCP funciona de la siguiente manera:

- El servidor DHCP es el que distribuye las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP estática.
- Cuando un equipo cliente se inicia no tiene información sobre su configuración de red y desea obtenerla. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo enviará un paquete de broadcast (255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local. Cuando el servidor DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión que contiene toda la información solicitada por el cliente.

En nuestro proyecto nos hemos decantado por la instalación y configuración de un servidor DHCP sobre un servidor con Windows Server 2012 por los siguientes motivos:

- Fácil manejo en el día a día.
- Flexibilidad de uso.
- Permite realizar reservar de IP para direcciones MAC específicas.

Por otro lado, de todas las subredes definidas inicialmente sólo la Vlan 4 y la Vlan 10 dispondrán del servicio DHCP, debido a su tamaño y a su ámbito de uso diario:

- Vlan 4 (Red Industrial): será una red que toda ella estará excluida de la asignación de IPs, pero utilizaremos el servidor DHCP para poder gestionar las reservas de IPs según la MAC del dispositivo final.
- Vlan 10 (Red Usuarios): esta red se le asignaran IPs desde el servidor DHCP, excepto a las 50 primeras IPs del rango, que quedaran para reservas para periféricos de distintas índole, como impresoras y otros, que puedan requerir una reserva específica.

En el [Anexo G: Instalación y configuración del servicio DHCP en Windows Server 2012](#) se encuentran todos los pasos necesarios para la implementación y activación del servicio en nuestra red.

Servicio DNS

Es este punto vamos a dotar a nuestra red de un servidor DNS interno, que nos ofrecerá la ventaja de no tener que realizar la resolución de nombres a través de servidores externos a nuestra red, con la ventaja de la rapidez que ello implica.

Lo óptimo sería dotar a nuestra red de dos servidores DNS, uno en el centro administrativo y otro en el centro productivo, para tener el servicio replicado ante caída de alguno de ellos. Además, de dotar a nuestro servidor de DHCP de dichas IPs para que sea configurado de manera automática en los dispositivos finales de la red. Como en el caso anterior del DHCP queda fuera de esta configuración el centro logístico por su tamaño reducido. En este apartado solo realizaremos la instalación de un servidor DNS.

Un servidor DNS (Domain Name System - Sistema de nombres de dominio) es un servidor que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

Trabajar con direcciones IP es incómodo para las personas, ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. En su lugar utilizamos nombres de dominio que son más fáciles de recordar y utilizar como por ejemplo www.google.es, www.educacion.gob.es, etc...

Cada equipo y cada servidor conectado a Internet, dispone de una dirección IP y de un nombre perteneciente a un dominio. Internamente, la comunicación entre los PCs se realiza utilizando direcciones IP por eso es necesario algún sistema que permita, a partir de los nombres de los PCs, averiguar las direcciones IPs de los mismos.

Un servidor DNS es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio.

No existe una base de datos única donde se almacenan todas las IPs existentes en el mundo, sino que cada servidor almacena las IPs correspondientes a su dominio. Los servidores DNS están dispuestos jerárquicamente de forma que cuando nuestro servidor más inmediato no puede atender nuestra petición, éste la traslada al DNS superior.

En el [Anexo H: Instalación y configuración del servicio DNS en Windows Server 2012](#) se encuentran todos los pasos necesarios para la implementación y activación del servicio en nuestra red.

Firewall

En este apartado vamos a dotar a nuestra red de un firewall que controle el tráfico entrante y saliente de nuestra organización. Para ello haremos uso de un firewall OpenSource que hay disponibles en la red. Para el desarrollo de esta sección solo implementaremos un firewall común para el Centro Administrativo y Productivo, quedando fuera el Centro Logístico.

El firewall que se pretende implementar dispondrá de dos interfaces de red:

1. WAN (Acceso al exterior)
2. LAN:
 - 2.1. DMZ (Acceso a servidores con servicios publicados al exterior)
 - 2.2. LAN (Acceso a la red interna).

Que es y para qué sirve un firewall.

Un cortafuegos o firewall, es un dispositivo, en forma de hardware o software, situado dentro de un sistema o red, que tiene la función de bloquear el acceso no autorizado y al mismo tiempo permitir las comunicaciones autorizadas, a través de unas determinadas reglas.

Si el tráfico entrante o saliente cumple con una serie de reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

Por lo tanto a partir de la definición podemos asegurar que con un firewall bien configurado podemos evitar intrusiones no deseadas en nuestra red y ordenador así como también bloquear cierto tipo de tráfico saliente de nuestro ordenador o nuestra red.

Básicamente la función de un firewall es proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que nos pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en nuestra red.

Así por lo tanto queda claro que es altamente recomendable que todo el mundo utilice un firewall por los siguientes motivos:

1. Preservar nuestra seguridad y privacidad.
2. Para proteger nuestra red doméstica o empresarial.
3. Para tener a salvo la información almacenada en nuestra red, servidores u ordenadores.
4. Para evitar intrusiones de usuarios no deseados en nuestra red y ordenador. Los usuarios no deseados tanto pueden ser hackers como usuarios pertenecientes a nuestra misma red.
5. Para evitar posibles ataques de denegación de servicio.

El firewall normalmente se encuentra en el punto de unión entre 2 redes. En el caso que podéis ver en la captura de pantalla se halla en el punto de unión de una red pública (internet) y una red privada.

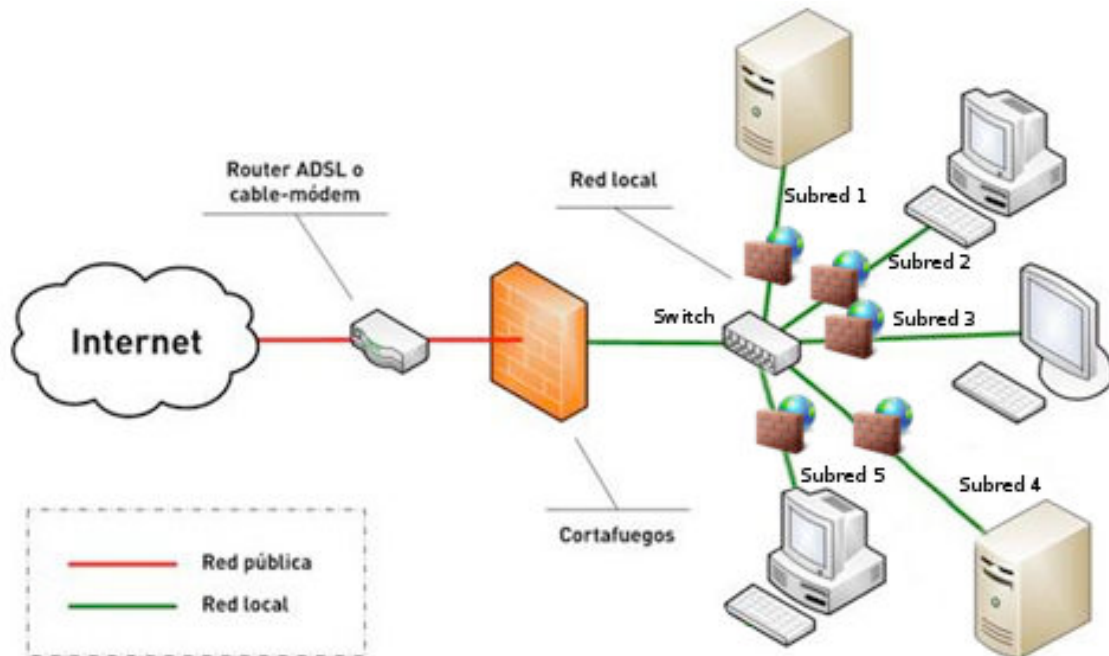


Ilustración 12 - Ejemplo de ubicación de un cortafuegos

Así mismo también vemos que cada una de las subredes dentro de nuestra red puede tener otro firewall, y cada uno de los equipos a la vez puede tener su propio firewall por software. De esta forma, en caso de ataques podemos limitar las consecuencias ya que podremos evitar que los daños de una subred se propaguen a la otra.

Lo primero que tenemos que saber para conocer el funcionamiento de un firewall es que la totalidad de información y tráfico que pasa por nuestro router y que se transmite entre redes es analizado por cada uno de los firewall presentes en nuestra red.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

1. Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.
2. Registrar todos los intentos de entrada y salida de una red. Los intentos de entrada y salida se almacenan en logs.
3. Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.
4. Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, Telnet, TCP, UDP, SSH, FTP, etc.
5. Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
6. Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto podemos restringir el acceso a ciertas aplicaciones.
7. Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

Lógicamente un Firewall dispone de una serie de limitaciones. Las limitaciones principales de un firewall son las siguientes:

1. Un firewall en principio es probable que no nos pueda proteger contra ciertas vulnerabilidades internas. Por ejemplo cualquier usuario puede borrar el contenido de un ordenador sin que el firewall lo evite, introducir un USB en el ordenador y robar información, etc.
2. Los firewall solo nos protegen frente a los ataques que atraviesen el firewall. Por lo tanto no puede repeler la totalidad de ataques que puede recibir nuestra red o servidor.
3. Un firewall da una sensación de seguridad falsa. Siempre es bueno tener sistemas de seguridad redundantes por si el firewall falla. Además no sirve de nada realizar una gran inversión en un firewall descuidando otros aspectos de nuestra red ya que el atacante siempre intentará buscar el eslabón de seguridad más débil para poder acceder a nuestra red. De nada sirve poner una puerta blindada en nuestra casa si cuando nos marchamos dejamos la ventana abierta.

Comparativa de firewalls OpenSource.

Se analizan los siguientes cortafuegos OpenSource:

ClearOS

ClearOS es, con mucho, la distribución firewall más elegante en su interfaz web. A la vez que tiene una sencilla configuración.

La mayoría de las distribuciones firewall traen detrás una configuración tediosa y siempre enfocada a administradores con altos conocimientos. En cambio ClearOS está más enfocada a informáticos que no tienen interés en realizar pruebas con el software y lo único que necesitan es un buen firewall que funcione y no presente muchos dolores de cabeza.

La instalación de ClearOS no llevará más de 15 minutos en un proceso sencillo.

Presenta una gran cantidad de paquetes para instalar otras funcionalidades de red adicionales al firewall. Funciona con iptables.

En general, ClearOS es una distribución de gran alcance, respaldada por un gran soporte, que le da las herramientas que necesita para hacer funcionar su red y la opción de ampliar aún más las características a la medida de sus necesidades específicas.



Ilustración 13 - Interface web ClearOS

Hardware mínimo: CPU 500MHz RAM 512mb

Sitio web: [www.clearfoundation.com / Software / overview.html](http://www.clearfoundation.com/Software/overview.html)

Valoración: 8/10 - Distro que combina facilidad de uso con funcionalidad.

IPCop

Esta distribución ha sido considerada por muchos como ‘The Killer Smoothwall’. Es una distribución derivada de Smoothwall Express.

Al igual que Smoothwall, IPCop utiliza colores para representar diferentes conexiones. El verde es para LAN, red de internet, naranja para DMZ, y el azul para separar los clientes inalámbricos.

De hecho, IPCop es un fork de Smoothwall, por lo que probablemente encontrará una gran cantidad de similitudes entre los dos. IPCop se separa de Smoothwall en 2002, y ha crecido con fuerza desde entonces.

La instalación es simple y fácil de seguir, aunque con algunas preguntas trampa que pueden desconcertar al usuario novato. Aceptar las opciones predeterminadas no causará ningún problema.

La interfaz web de IPCop es simple y un poco austera. Sin embargo, aparte de los gráficos de “tiempo real” que Smoothwall proporciona, IPCop da mucha más información sobre la configuración de Wi-Fi, y sobre el funcionamiento del propio firewall, incluyendo una lista de las conexiones que estén abiertas.

También proporciona un “proxy caché” por lo que se puede almacenar en caché las páginas de acceso frecuente a nivel local. Proporcionando un acceso a internet mas ágil.

IPCop hace un buen trabajo como un servidor de seguridad, dando un montón de información sobre el tráfico en la red, y si bien podría no ser la distro más bonita del mundo, hace lo que está diseñado para hacer.

Distribución en decadencia. Sin actualizaciones actuales.

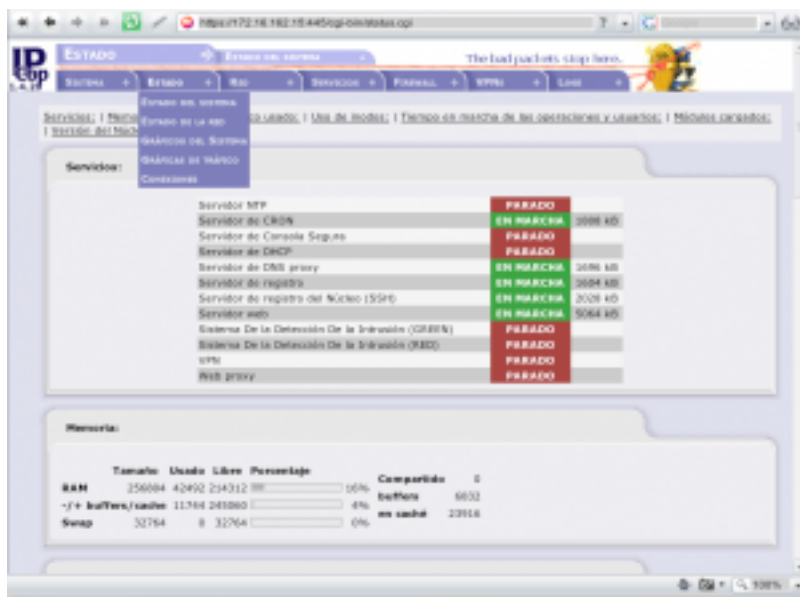


Ilustración 14- Interface Web IPCOP

Hardware minimo: CPU 160MHz RAM 32mb

Sitio web: www.ipcop.org

Valoración: 7/10 - Una distro basada en códigos de colores versátil y veloz.

Zentyal

Zentyal (anteriormente eBox-platform) no se declara como una distribución de servidor de seguridad por parte de sus creadores, sino como un “Linux Small Business Server ‘ y ciertamente hace honor a su descripción.

Como está basado en Ubuntu Server, la instalación en su sistema es muy similar a una instalación de Ubuntu normal. También puede instalar los diversos componentes de zentyal a una versión genérica Ubuntu LTS con sólo añadir un repositorio APT y la instalación de ciertos paquetes.

Esto es útil si ya se tiene un pc por ahí con Ubuntu instalado en él, o si sólo necesita ciertas partes de la plataforma eBox (ebox la red y ebox-firewall, por ejemplo). Esto se debe a que zentyal se ha construido entorno al núcleo de Ubuntu Server, y utiliza sus componentes internos. Para obtener más información acerca de las diferentes maneras en que se pueden instalar zentyal, echar un vistazo a [esta página](#).

Una vez instalado, inicie sesión en zentyal con su navegador, utilizando la contraseña que proporcionó durante la instalación. En este punto, puede parecer demasiado complejo por el gran número de opciones que zentyal ofrece. Pero una vez encuentre la pantalla firewall, la configuración es simple.

Zentyal es una de las mayores distribuciones de firewall que probamos en términos de la magnitud de la descarga, debido a los paquetes de un montón de características, incluyendo bases de datos y servidores SIP.

Posee una interfaz demasiado compleja y con demasiadas opciones si lo que estamos buscando es solamente un firewall de seguridad y nada más.

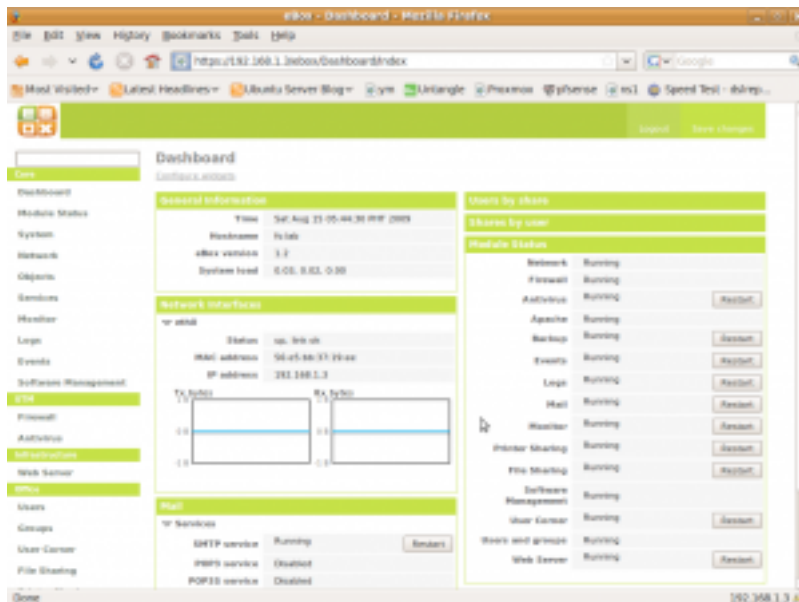


Ilustración 15 - Interface Web ZENTYAL

Hardware mínimo: CPU 1,5Ghz RAM 1GB

Sitio web: www.zentyal.org

Valoración: 9/10 - Éste es algo más que una distro cortafuegos.

Monowall

Monowall es un firewall basado en BSD diseñado para ejecutarse en una tarjeta de memoria de 16 MB, y tiene el tamaño más pequeño de los firewalls que probamos. Debido a esto, Monowall sólo proporciona las características básicas para un servidor de seguridad. Sin embargo, dado que es tan pequeño, es una distribución bastante interesante.

Monowall arranca directamente en el menú de configuración. En primer lugar, tenemos que configurar las interfaces de red con la función Monowall de “Auto Detect”, que le permite asignar una interfaz LAN / WAN mediante la detección de si el cable está conectado o no.

Monowall tiene la ventaja de ser uno de los pocos servidores de seguridad que proporciona calidad de servicio (QoS) de enrutamiento por defecto, lo que le permite dar prioridad a algunos tipos de paquetes. Esto es útil si se quiere utilizar VoIP.

Una vez que haya asignado a sus interfaces de red, puede establecer una contraseña para el sistema WebGUI, que le permite configurar el resto del servidor de seguridad a través de la interfaz basada en web.

Al ser un sistema basado en BSD, algunos de los términos pueden parecer confusos al principio, pero después de algunas búsquedas en la web se convierte en un proceso simple.

Aunque Monowall es una distribución de servidor de seguridad pequeña, la seguridad no se ve comprometida.



Ilustración 16 - Interface Web MONOWALL

Sitio web: <http://m0n0.ch>

Calificación: 6/10 - Una de las distribuciones firewall más ligeras.

PfSense

PfSense es un fork de Monowall, y por tanto está basado en BSD. BSD utiliza un programa llamado pf (filtro de paquetes) como filtro de paquetes con estado, que es muy parecido a Iptables, aunque quizás más potente. Esto se debe a que pf y Iptables funcionan de maneras diferentes.

Pf funciona mejor con reglas con estado (donde se necesita o usa la información acerca de los paquetes anteriores en un histórico), y Iptables es mejor con reglas sin estado (donde no se necesita información acerca de los paquetes anteriores). En este sentido, pf es un poco más seguro que un cortafuegos con iptables, pues mediante el seguimiento de los números de secuencia TCP, tiene una conexión más difícil de falsificar.

PfSense, como Monowall, tiene un sencillo proceso de instalación que se reduce a una línea de comandos, pero a diferencia de Monowall, se le pedirá configurar las interfaces durante la instalación, y no una vez que se inicie.

Al ser un fork de Monowall, era de esperar las características sean similares o incluso idénticas, pero pfSense añade características adicionales, tales como multi-WAN, conmutación por error de hardware, y los diferentes métodos de autenticación. Tiene una interfaz más limpia y simple de usar. Una vez más, siendo BSD, algunos de los términos utilizados son confusos, pero es simple habituarse. PfSense es posiblemente la distribución con más características firewall, Si lo único que se necesita es un firewall sin ninguna otra característica de red, esta es sin duda la mejor distribución.

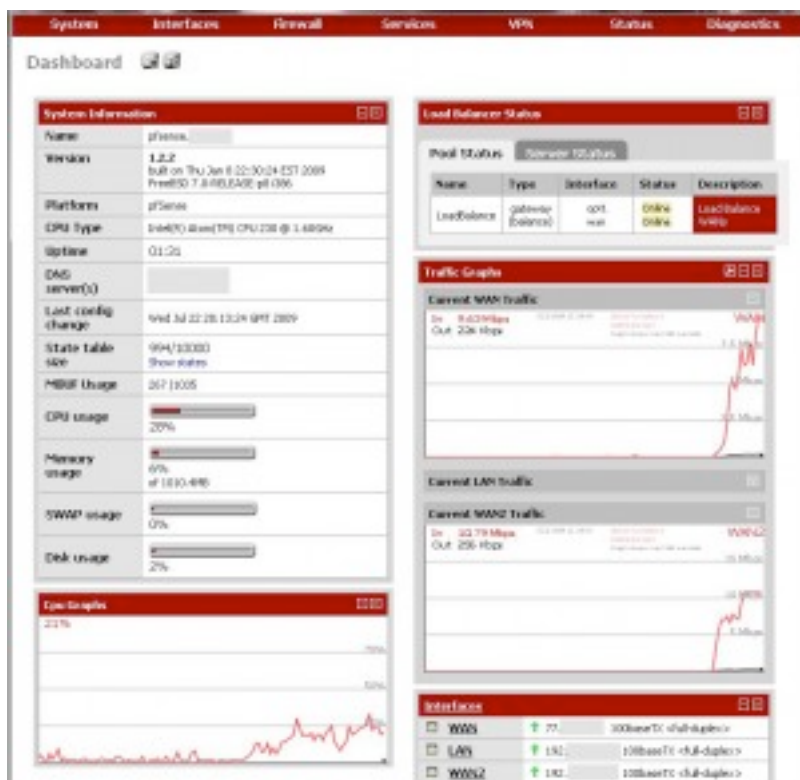


Ilustración 17 - Interface Web PFSense

Sitio web: www.pfsense.org

Valoración: 9/10 - Si quieres un firewall integral y nada más, pfsense quizás sea el más interesante.

Smoothwall Express

Smoothwall es probablemente la distro firewall por excelencia.

La instalación de Smoothwall Express es bastante rápida, aunque un poco confusa. Vale la pena utilizar la guía de instalación que os guiará a través del proceso de instalación. La mayoría de las opciones predeterminadas deberían ser válidas, a menos que tenga una configuración de red inusual.

Una vez que haya terminado la configuración inicial de Smoothwall Express, ya estaría en condiciones para funcionar, ya que no requiere de muchos más ajustes.

Aunque es una distribución muy buena, no debemos olvidar que es la versión gratuita y viene limitada. Esto puede llegar a ser un problema si por nuestros requerimientos de red necesitamos algo en concreto.

Podemos consultar las características de cada versión en:

<http://www.smoothwall.org/about/feature-comparison-chart/>

En definitiva: Un buen firewall, fácil de usar, pero queda un poco corto en cuanto a funciones más avanzadas. Que si tendríamos en la versión de pago de Smoothwall.

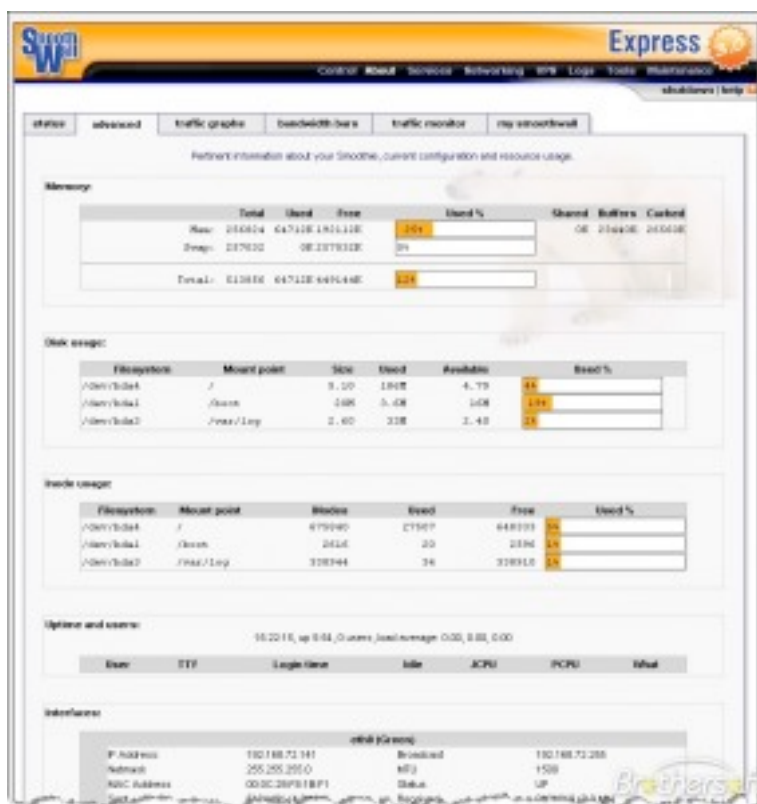


Ilustración 18 - Interface Web SMOOTHWALL

Sitio web: www.smoothwall.org

Valoración: 7/10 - Probablemente la distribución de firewall con la mayor reputación.

Elección del firewall.

Tras los cortafuegos analizados en el punto anterior nos decantamos por **PfSense** que cuenta con casi todas las funcionalidades de los costosos cortafuegos comerciales y en muchos casos incluye en más.

Firewall

- Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destinación para TCP y UDP tráfico.
- Habilitación de límites para conexiones simultaneas con reglas de base.
- pfSense® utiliza p0f, una avanzada herramienta de red para huellas dactilares digitales que habilita la filtración a través el sistema operativo al inicio de la conexión.
- Políticas de enrutamiento con alta flexibilidad para la selección del gateway sobre las reglas de base para el equilibrio de banda, failover, WAN múltiple, backup sobre mas ADSL, etc...
- Posibilidad de creación de Alias de grupos de IP y nombres de IP, networks y puertas de enlace. Estas características ayudan a mantener la configuración limpia y fácil de entender, especialmente con configuraciones con varias IP públicas y numerosos Servers.
- Filtración transparente de capa 2. Posibilidad de puentear interfaces y filtrar el tráfico entre estas.
- Posibilidad de inhabilitar la filtración (firewalling) para utilizar pfSense® como solo router.

State Table (tabla de estado)

La tabla de estado del firewall mantiene informaciones de las conexiones abiertas. pfSense es un stateful firewall, por defecto todas las reglas son stateful. Muchos firewall no tienen la capacidad de controlar la tabla de estados. PfSense tiene muchas funciones en grado de hacer un control granular de la tabla de estado.

- Regulación del tamaño de la tabla de estado – existen muchas instalaciones de pfSense que usan diferentes cientos de estados. De norma la tabla de estado varía según la RAM instalada en el sistema, pero puede ser aumentada en tiempo real a la dimensión deseada. Cada estado ocupa aproximadamente 1 KB de RAM, este parámetro viene mantenido en la mente cuando se debe dimensionar la memoria.
- Reglas de base:
 - Límites de conexiones simultáneas de clientes.
 - Límites de estado para host.
 - Límites de nuevas conexiones al segundo.
 - Definir el estado de timeout.
 - Definir el tipo de estado.

- Tipos de estado – pfSense ofrece numerosas opciones para la gestión del estado:
 - Keep state – Trabaja con todos los protocolos. De norma con todas las reglas.
 - Modulate state – Trabaja solo con TCP. pfSense® generará ISNs (Initial Sequence Numbers) por cuenta del host.
 - Synproxy state – Los Proxy inician las conexiones TCP para ayudar los server de spoofed TCP SYN floods.
 - None – No se mantiene ninguna información sobre el estado.
- Opciones de optimización de la tabla de estado – pfSense ofrece cuatro estados para la optimización de la tabla de estado:
 - Normale – de norma.
 - Hight latency – usada para links de alta latencia, como enlaces por satélite.
 - Aggressive – fecha límite del estado de idle más veloz. Más eficiente usando más recursos hardware, pero puede eliminar conexiones correctas.
 - Conservative – Trata de evitar la cancelación de conexiones correctas a costa de mayor utilización de CPU y RAM.

NAT: Network Address Tranlation

- El Port forwards incluye unos rangos y uso de IP públicas múltiples.
- NAT 1:1 para IP individuales o subredes enteras.
- Outband NAT:
 - Todo el tráfico en salida al IP de la WAN. En configuraciones con WAN múltiples, vendrá usado el tráfico en salida a la IP de la interfaz WAN.
 - Advanced Outbound NAT.
- NAT Reflection – en alguna configuración, NAT Reflection es utilizado para servicios que pueden acceder con IP públicos desde redes internas.

NAT Limitation

PPTP / GRE Limitation – El monitoreo del estado de colas en pfSense para el protocolo GRE puede monitorizar una sola sesión por IP publica para un servidor externo. Esto significa que si usan conexiones PPTP VPN, solo una máquina interna podrá conectarse simultáneamente al PPTP server en internet. Miles de máquinas pueden conectarse simultáneamente con miles de server PPTP, pero solo una simultáneamente podrá conectarse a un server PPTP. El único modo para evitar el problema es utilizar IP públicas diferentes en el firewall, uno para el cliente, o usar IP públicas múltiples para los PPTP

servidores. Este problema no existe para conexiones VPN con diferentes protocolos. La solución a este problema es actualmente en desarrollo.

Redundancia

El protocolo CARP de OpenBSD gestiona el hardware failover. Dos o más grupos de firewall hardware pueden ser configurados como un grupo de failover. Si una interfaz falla en el dispositivo primario o el dispositivo primario pasa a offline, el segundo dispositivo se activa. PfSense incluye también capacidad de sincronización automática entre el dispositivo primario y el secundario. Pfsync asegura que la tabla de estado del firewall será reproducida en todos los firewall incluidos en el failover. Esto significa que las conexiones existentes serán mantenidas en caso de fallo.

Limitaciones

Funciona solo con IP públicas estáticas, no funciona el failover usando DHCP, PPPoE o PPTP en la red WAN.

Balance de carga

Balance de carga en salida: (Outbound)

El balance de carga en salida se usa en redes WAN para brindar balanceo y failover. El tráfico es directo a un Gateway designado o a un pool de balanceo de carga definido en las reglas de base del firewall.

Inbound Load Balancing

El balanceo de carga en entrada se usa para distribuir la carga entre los servidores. Es comúnmente usado para servidores web, servidores de correo electrónico y otros. Los servidores que no responden al ping o conexiones TCP en la puerta de enlace definida serán excluidos por el pool.

VPN

pfSense ofrece tres opciones para la conectividad VPN: IPsec, OpenVPN, e PPTP.

IPsec

IPsec consiente en conectividad con todos los dispositivos que soportan el standard IPsec. Esto es de uso común en las configuraciones site-to-site con otros dispositivos pfSense. Otros firewall open source como m0n0wall y muchos otros firewall comerciales como Cisco, Juniper, etc... la implementan. Es usada a menudo en las conexiones móviles de clientes.

OpenVPN

OpenVPN es una flexible y potente solución SSL VPN que soporta una amplia gama de sistemas operativos cliente.

PPTP Server

PPTP es un sistema VPN muy popular porque está instalado en casi todos los sistemas operativos cliente incluidos todos los sistemas operativos Windows a partir de Windows 95. El server pfSense PPTP puede usar una base de datos

local o un RADIUS server para la autenticación. La compatibilidad RADIUS está también soportada.

PPPoE Server

pfSense ofrece un server PPPoE. La base de datos de usuarios locales pueden ser usados para la autenticación y la autenticación RADIUS con opciones de accounting también es soportada.

Reportes y Monitoreo

Gráficos RRD. Los gráficos RRD en pfSense ofrecen las siguientes informaciones:

- Utilizo de la CPU.
- Tráfico total.
- Estado del firewall.
- Tráfico individual de las interfaces.
- Packets por second-rates para todas las interfaces.
- Tiempo de respuesta al ping del gateway de la interfaz WAN.
- Cola de tráfico shaper sobre el sistema si el tráfico shaper está habilitado.

Información en tiempo real

Las informaciones sobre la historia del sistema son importantes, pero a veces son más importantes las informaciones en tiempo real. Los gráficos SVG muestran el tráfico en tiempo real para todas las interfaces. La página inicial incluye gráficos AJAX que muestran en tiempo real el cargo de la CPU, memoria, swap y espacio disco usado y la tabla de estado.

DNS Dinámica

El cliente de DNS Dinámica activa el registro mediante uno de los siguientes servicios:

- DynDNS
- DHS
- DNSexit
- DyNS
- EasyDNS
- FreeDNS
- HE.net
- Loopia
- Namecheap

- No-IP
- ODS.org
- OpenDNS
- ZoneEdit

Captive Portal

El captive portal permite de forzar la autenticación o redirigir el tráfico de red a una página de autenticación de red. Esto es comúnmente usado en las conexiones de red hot spot, ampliamente usada también para niveles de seguridad adicionales en el acceso de redes internet a través sistemas Wireless. La que sigue es una lista de funciones y características del Captive Portal.

- Conexiones máximas competidoras - Límite al número de conexiones competidoras para cada IP cliente. Esta funcionalidad impide ataques DOS.
- Idle timeout – Desconecta los clientes que no efectúan conexiones por más de un cierto número de minutos.
- Hard timeout – Fuerza la desconexión de cliente conectados por más de un numero definido de minutos.
- Pop up de logon – Opción de pop up de la ventana de desconexión
- URL Redirection – después de la autenticación los usuarios pueden ser direccionados a una página definida.
- MAC Filtering – de norma pfSense usa el filtración direcciones MAC.
- Opciones de autenticación – existen tres métodos de autenticación:
 - Ninguna autenticación: habilita la navegación sin la inserción de ningún dato.
 - Usuarios locales – la base de datos de los usuarios locales puede ser configurada y usada para la autenticación.
 - Autenticación RADIUS – Este es el método preferido por las empresas, entes y ISP. Puede ser usado con la autenticación de Microsoft Active Directory y otros tipos de servidores RADIUS.
- Capacidad de RADIUS
 - Forzar la re-autenticación.
 - Activación de la actualización de cuentas de usuarios.
 - Autenticación MAC RADIUS, habilita el Captive Portal en la autenticación de cliente usando el MAC address, username y password.
 - Acepta configuraciones redundante de RADIUS Server.

- http e HTTPS – La página del portal puede ser configurada sea en http que en https.
- Pass-through MAC and IP addresses – Direcciones MAC y IP pueden ser inseridas en una lista blanca sin pasar por el portal.
- File manager – Esto permite de cargar imágenes que pueden ser utilizadas en la página inicial del captive portal.

DHCP Server and Relay

pfSense incluye DHCP Server y funcionalidad Relay.

Instalación y configuración de PfSense

En el [Anexo I: Instalación y configuración de PfSense](#) se explica todo lo relacionado con la instalación y configuración del cortafuegos PfSense aptado a nuestra red corporativa.

Monitorización de la red con Nagios

Introducción

En este apartado vamos a dotar a nuestra red de un sistema de monitorización que nos permitirá tener en todo momento control visual y de envío de alertas por correo electrónico del estado de nuestros dispositivos de red (ON/OFF). Aunque Nagios es una potente herramienta de monitorización que permite el control de muchos estados de los elementos monitorizados, en nuestro caso de ejemplo sólo vamos a controlar que tengamos respuesta al ping de nuestros elementos de la red, es decir, si están activos o han caído por algún motivo.

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Características:

- Monitorización de servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP).
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins NRPE_NT o NSClient++.
- Monitorización remota, a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).

- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros....

FUENTE: Wikipedia.

Monitorización de nuestra red

Para la instalación y configuración de Nagios partimos de un servidor Ubuntu versión 14.04 instalado en una máquina virtual de nuestra organización. Para dicha instalación se necesitan los siguientes prerequisites en nuestra distribución Linux:

- Apache 2
- PHP
- GCC: librerías de desarrollo y compilación
- GD: librerías de desarrollo

De las diferentes web donde se explica la instalación se ha seguido la del siguiente enlace, que es en la que menos problemas hemos encontrado:

➤ [Instalación Nagios](#)

Tras la instalación pasamos a configurar el fichero `switch.cfg` ubicado en la ruta: `/usr/local/nagios/etc/object` tal y como se adjunta en el [Anexo K: Fichero "switch.cfg" de Nagios](#).

Quedan monitorizados los siguientes dispositivos de la red y servicios:

1. CENTRO ADMINISTRATIVO

- 1.1. CA-CORE
- 1.2. CA-P0
- 1.3. CA-P1
- 1.4. CA-P2
- 1.5. AP-P0
- 1.6. AP-P1
- 1.7. AP-P2
- 1.8. FIREWALL
- 1.9. R-CA
- 1.10. SALIDA INTERNET

2. CENTRO PRODUCTIVO

- 2.1. CP-CORE
- 2.2. CP-Z1
- 2.3. CP-Z2
- 2.4. AP-Z1
- 2.5. AP-Z2
- 2.6. R-CP
- 2.7. SALIDA INTERNET

3. ENLACE ENTRE SEDE ADMINISTRATIVA Y LOGISTICA

- 3.1. ER-ER

4. CENTRO LOGISTICO

- 4.1. CL-Z1
- 4.2. AP1
- 4.3. AP2
- 4.4. AP3
- 4.5. RP
- 4.6. RB
- 4.7. SALIDA INTERNET PRINCIPAL
- 4.8. SALIDA INTERNET RESPALDO

Una vez introducidos todos nuestros dispositivos de red en el fichero switch.cfg con sus respectivas dependencias ya podemos reiniciar el servicio de Nagios y mostrar nuestra red monitorizada (se muestran varios ejemplos de vistas monitorizadas de la red):

- Mapa con vista circular:

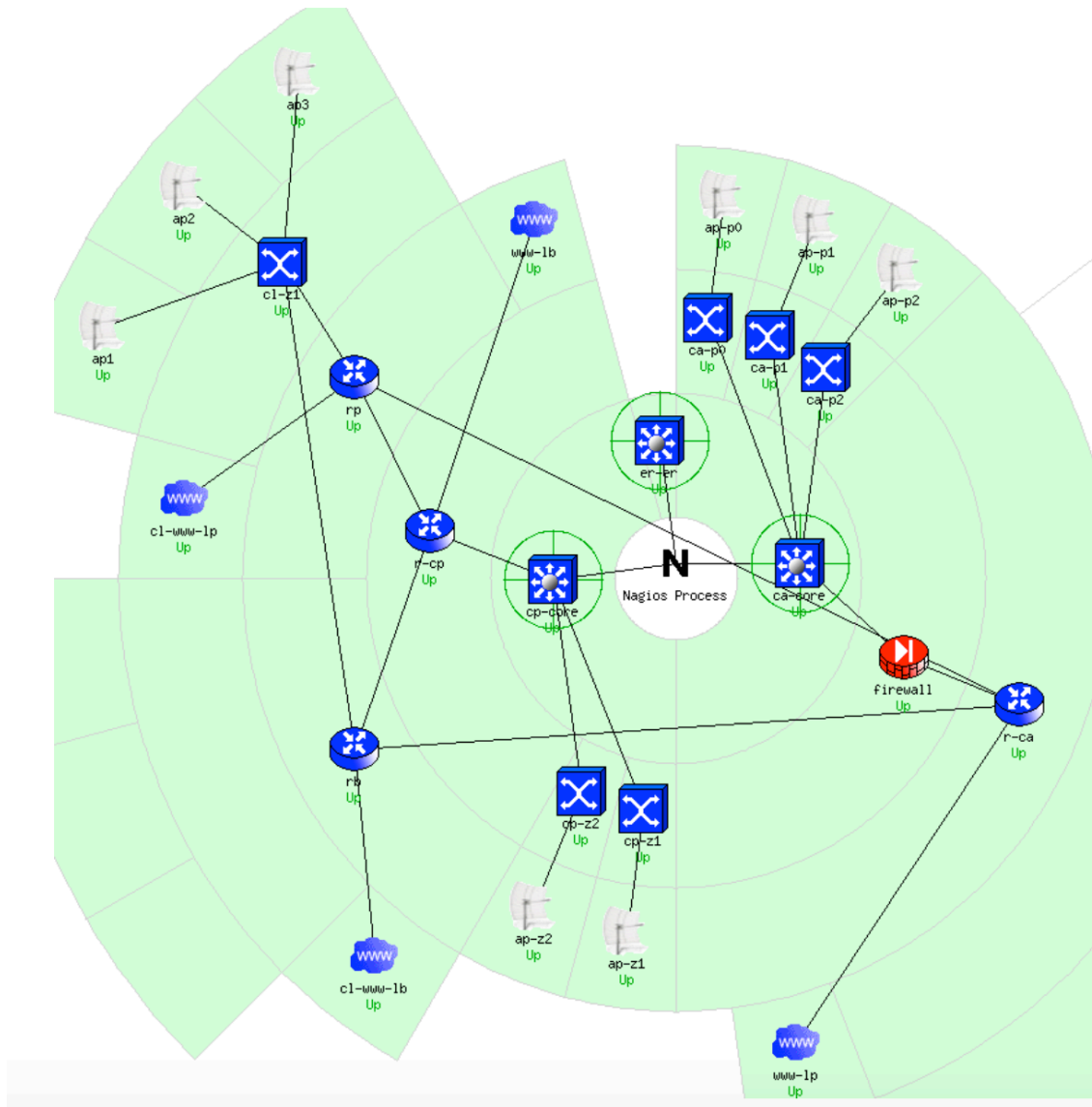


Ilustración 19 - Nagios: mapa con vista circular

- Vista de los dispositivos en forma de lista:

Current Network Status
 Last Updated: Sat Jun 4 16:49:19 CEST 2016
 Updated every 30 seconds
 Nagios® Core™ 4.0.4 - www.nagios.org
 Logged in as nagiosadmin

View Service Status Detail For All Host Groups
 View Status Overview For All Host Groups
 View Status Summary For All Host Groups
 View Status Grid For All Host Groups

Host Status Totals				Service Status Totals				
Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
26	0	0	0	26	0	0	0	0
All Problems All Types				All Problems All Types				
0		26		0		26		

Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
ap-p0	UP	06-04-2016 16:46:43	0d 0h 48m 41s	ECO OK - Paquetes perdidos = 0%, RTA = 43.82 ms
ap-p1	UP	06-04-2016 16:48:06	0d 0h 48m 41s	ECO OK - Paquetes perdidos = 0%, RTA = 45.60 ms
ap-p2	UP	06-04-2016 16:44:51	0d 0h 48m 49s	ECO OK - Paquetes perdidos = 16%, RTA = 91.90 ms
ap-z1	UP	06-04-2016 16:44:35	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 42.39 ms
ap-z2	UP	06-04-2016 16:47:26	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 36.81 ms
ap1	UP	06-04-2016 16:45:46	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 44.79 ms
ap2	UP	06-04-2016 16:46:07	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 25.80 ms
ap3	UP	06-04-2016 16:46:07	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 43.49 ms
ca-core	UP	06-04-2016 16:44:17	0d 0h 48m 49s	ECO OK - Paquetes perdidos = 0%, RTA = 50.48 ms
ca-p0	UP	06-04-2016 16:48:36	0d 0h 48m 45s	ECO OK - Paquetes perdidos = 0%, RTA = 36.66 ms
ca-p1	UP	06-04-2016 16:44:04	0d 0h 48m 45s	ECO OK - Paquetes perdidos = 0%, RTA = 52.87 ms
ca-p2	UP	06-04-2016 16:47:56	0d 0h 48m 53s	ECO OK - Paquetes perdidos = 0%, RTA = 32.96 ms
cl-www-lb	UP	06-04-2016 16:44:47	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 159.09 ms
cl-www-lp	UP	06-04-2016 16:46:03	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 37.93 ms
cl-z1	UP	06-04-2016 16:46:00	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 29.16 ms
cp-core	UP	06-04-2016 16:47:26	0d 0h 48m 52s	ECO OK - Paquetes perdidos = 0%, RTA = 37.61 ms
cp-z1	UP	06-04-2016 16:47:32	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 33.92 ms
cp-z2	UP	06-04-2016 16:46:03	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 30.58 ms
er-er	UP	06-04-2016 16:46:15	0d 2h 14m 53s	ECO OK - Paquetes perdidos = 0%, RTA = 52.13 ms
firewall	UP	06-04-2016 16:48:49	0d 0h 48m 44s	ECO OK - Paquetes perdidos = 0%, RTA = 33.01 ms
r-ca	UP	06-04-2016 16:45:40	0d 0h 48m 48s	ECO OK - Paquetes perdidos = 0%, RTA = 36.97 ms
r-cp	UP	06-04-2016 16:47:57	0d 0h 48m 56s	ECO OK - Paquetes perdidos = 0%, RTA = 39.57 ms
rb	UP	06-04-2016 16:47:26	0d 0h 48m 52s	ECO OK - Paquetes perdidos = 0%, RTA = 34.77 ms
rp	UP	06-04-2016 16:48:49	0d 0h 48m 52s	ECO OK - Paquetes perdidos = 0%, RTA = 45.78 ms
www-lb	UP	06-04-2016 16:45:19	0d 0h 48m 52s	ECO OK - Paquetes perdidos = 16%, RTA = 33.52 ms
www-lp	UP	06-04-2016 16:48:58	0d 0h 48m 40s	ECO OK - Paquetes perdidos = 0%, RTA = 41.73 ms

Ilustración 20 - Nagios: vista en forma de lista

- Vista en forma de árbol:

suppress pc

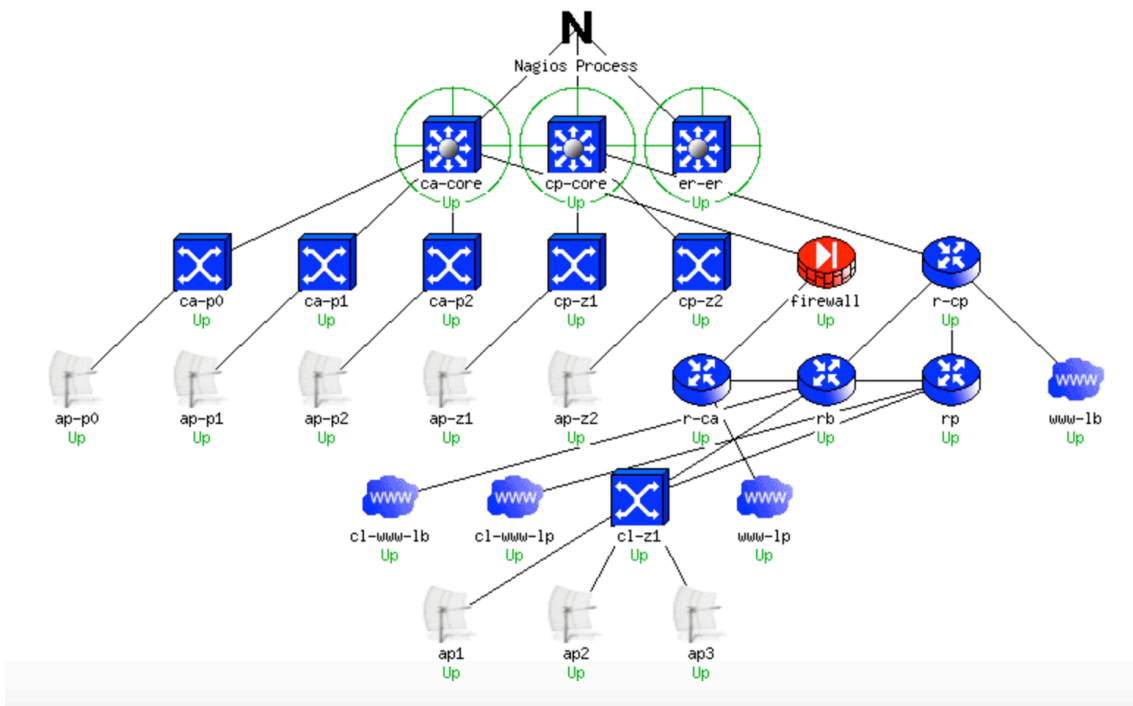


Ilustración 21 - Nagios: vista en forma de árbol

- Vista en árbol con switch de la planta 2 del centro administrativo caído:

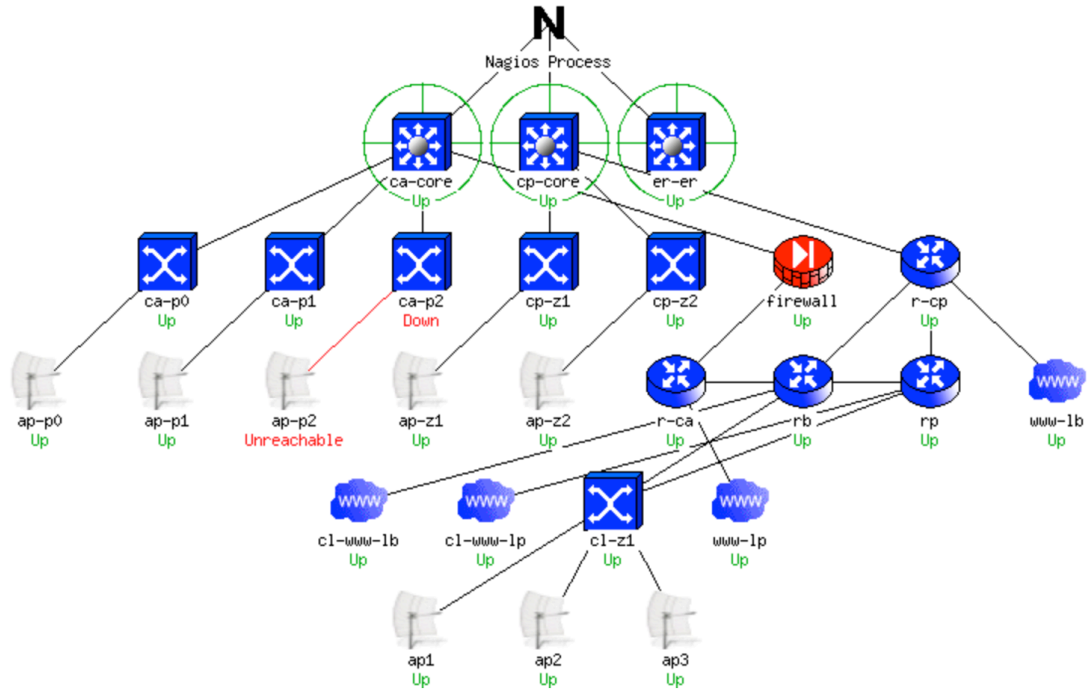


Ilustración 22 - Nagios en vista de árbol con dispositivo en fallo.

2.5. Plan de contingencias.

Nuestro plan de contingencias va a consistir en una serie de supuestos fallos que se produzcan en los elementos de nuestra red y como restablecer el servicio en el menor tiempo posible.

Supuesto 1 – Caída de uno de los switches de acceso.

Dispondremos de un switch de acceso de backup guardado para reponer rápidamente la caída de alguno de los switches de acceso distribuidos por los tres centros en el menor tiempo posible.

Para ello también dispondremos de copias de seguridad de los ficheros “running-config” de nuestros switches de acceso, volcaremos el backup del dispositivo caído en el dispositivo de respaldo, para su posterior sustitución.

Esto nos permitirá una pronta respuesta ante la caída del elemento mencionado.

- Tiempo de respuesta centro administrativo y centro productivo: 15 minutos.
- Tiempo de respuesta centro logístico: 15 minutos + 30 minutos de desplazamiento. 45 minutos.

Posteriormente se procedería a la sustitución del dispositivo caído por uno en buen estado, quedando en backup.

Supuesto 2 – Caída de uno de los punto de acceso.

Dispondremos de un punto de acceso de backup guardado para reponer rápidamente la caída de alguno de los puntos de acceso distribuido por los tres centros en el menos tiempo posible.

Para ello dicho punto de acceso estará pre-configurado con la SSID de la organización.

Esto nos permitirá una pronta respuesta ante la caída del elemento mencionado.

- Tiempo de respuesta centro administrativo y centro productivo: 5 minutos.
- Tiempo de respuesta centro logístico: 5 minutos + 30 minutos de desplazamiento. 45 minutos.

Posteriormente se procedería a la sustitución del dispositivo caído por uno en buen estado, quedando en backup.

Supuesto 3 – Caída de uno de los switches multicapa.

En este supuesto utilizaríamos el switch multicapa ER-ER que hace de enlace de respaldo entre el centro administrativo y el centro logístico.

Para ello también dispondremos de copias de seguridad de los ficheros “running-config” de nuestros switches multicapa, volcaremos el backup del dispositivo caído en el dispositivo de respaldo, para su posterior sustitución.

Esto nos permitirá una pronta respuesta ante la caída del elemento mencionado.

- Tiempo de respuesta centro administrativo y centro productivo: 15 minutos.

Posteriormente se procedería a la sustitución del dispositivo caído por uno en buen estado, volcado del backup ER-ER y vuelta a su función original.

Supuesto 4 – Caída del switch multicapa del enlace de respaldo.

En este supuesto nuestro servicio no se ve afectado, sólo perdemos redundancia en los enlaces.

En este caso se procedería a la gestión del cambio del dispositivo, posterior volcado de backup y su instalación en origen.

Supuesto 5 – Caída del firewall.

En este supuesto se realizarían los siguientes pasos:

1. Cambiar la conexión física del router, que dejaría de estar conectado con el firewall y lo conectaríamos directamente al switch multicapa del centro administrativo.
2. Cambiar la tabla de ruteo del switch multicapa del centro administrativo para que se envíen el tráfico hacia el exterior directamente al router.

Con esto ya tendríamos de nuevo servicio con el exterior. Esto nos permitirá una pronta respuesta ante la caída del elemento mencionado.

- Tiempo de respuesta centro administrativo y centro productivo: 15 minutos.

Los pasos para restablecer el servicio a su estado original:

1. Restaurar la copia de la máquina virtual del firewall.
2. Volver a cambiar la tabla de ruteo del switch multicapa del centro administrativo para que se envíe el tráfico hacia el exterior a través del firewall
3. Volver a cambiar el cable de conexión del router y conectarlo a la conexión WAN del firewall.

Supuesto 6 – caída de routers.

En el caso de que caiga alguno de los cuatro routers de los tres centros no tendremos que hacer nada, ya que el sistema está preparado previamente por HSRP para balancear la salida hacia el exterior.

Simplemente gestionaremos con nuestro proveedor de servicios de Internet la reparación o sustitución del router.

Supuesto 7 – Fallo en el servicio de Internet

En esta caso, como el anterior, en el caso de fallo en el servicio de Internet de los tres centros no tendremos que hacer nada, ya que el sistema está preparado previamente por HSRP para balancear la salida hacia el exterior.

Simplemente gestionaremos con nuestro proveedor de servicios de Internet la reparación de la avería.

Supuesto 8 – Fallo en el cableado de red.

En el caso de corte de alguno de los cables de red o fibra de la instalación de red, procederemos a su sustitución.

Para ello dispondremos de una caja con rollo de cable de red y otra con cable de fibra para su sustitución por parte del departamento de mantenimiento de la organización o una empresa externa.

El tiempo de respuesta para la resolución de este fallo dependerá de la zona y metros a sustituir, pero puede oscilar desde una hora hasta varias horas.

2.6. Costes del proyecto.

En este último punto se pretende dar una orientación sobre los costes del proyecto a nivel de hardware, a los cuales se tendría que añadir los 3.053€ mensuales de los servicios de Internet.

Queda fuera los costes de consultoría o desarrollo del proyecto realizado en este Trabajo y la mano de obra de instalación de todo el cableado, realizado por los operarios de mantenimiento de la organización.

DISPOSITIVO	CANTIDAD	COSTE UNIDAD	TOTAL
2960-24TT	6+1	700 €	4.900 €
3560-24PS	3	3.500 €	10.500 €
AP AIRONET 1600	8+1	600 €	5.400 €
TOTAL			20.800 €

Tabla 15 - Costes del proyecto.

3. Conclusiones

Durante el desarrollo del presente trabajo se ha aprendido detalles desconocidos en la configuración de dispositivo de Cisco como configurar *HSRP* o configurar tablas de ruteo. Otro aspecto importante abordado ha sido la puesta en marcha del firewall *PfSense* y conocer todas sus extensas posibilidades.

En un aspecto menos técnico se ha reforzado a nivel personal los puntos de la planificación, del análisis técnico y detallado de las problemáticas a resolver.

El presente trabajo tenía cierta envergadura y se han cumplido todos los objetivos iniciales, aunque cierto es que con más tiempo se podrían haber abordado algunos puntos extras relacionados con el tema como ampliar funcionalidades de *PfSense* y *Nagios* o el uso de las herramientas de Cisco como *Cisco Configuration Professional* (CCP) que es una herramienta de administración de dispositivos basada en GUI para el acceso a los dispositivos de Cisco o *Cisco Network Assistant* (CNA) es una aplicación del tipo software que permite administrar equipos individuales y en conjunto.

El principal problema de la planificación fue que inicialmente se propuso realizar la configuración de dispositivos desde de la vista de agrupación por centro de trabajo, pero conforme se comenzó el desarrollo se decidió que la mejor forma de enfocar el problema a resolver era viéndolo todo como un conjunto y desarrollar de dentro hacia fuera.

Respecto al plan de contingencias se ha elaborado en base a la red diseñada y un bajo coste. Evidentemente, los tiempos de respuesta en los planes de contingencias son mejorables normalmente mediante mayor inversión económica, por ejemplo podríamos haber diseñado una red en estrella con más conexiones entre los dispositivos de red e incluso incorporando más dispositivos de red.

En los costes del proyecto se ha optado por precios de dispositivos nuevos, pero se podrían haber rebajado usando dispositivos *Refurbished* (probados, certificados y configurados por Cisco, que tienen una completa garantía a través de Cisco TAC) o incluso de segunda mano. Por otro lado, este tipo de proyectos es difícil evaluar los costes de consultoría o de mano de obra ya que se parte desde cero y surgen muchas modificaciones sobre el desarrollo del mismo. Siguiendo con los costes, incluso se podrá haber añadido una auditoría de la red por una tercera empresa independiente que certificase principalmente el rendimiento y la seguridad de la misma.

4. Glosario

Switch: es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Router: también conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.

Ruteo: el encaminamiento, enrutamiento o ruteo, es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla.

VLAN: Una VLAN, acrónimo de *virtual LAN* (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

VPN: Una red privada virtual (RPV), en inglés: *Virtual Private Network* (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.¹ Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

IP: Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, *smartphone*) que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red.

Host: El término *host* ("anfitrión", en español) es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar *anfitriones* para tener acceso a la red. En general, los *anfitriones* son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc. Los usuarios que hacen uso de los *anfitriones* pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red. De forma general un *anfitrión* es todo equipo informático que posee una dirección IP y que se encuentra interconectado con uno o más equipos. Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Comúnmente descrito como el lugar donde reside un sitio web. Un anfitrión de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de anfitrión.

CPD: Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

MPLS (siglas de *Multiprotocol Label Switching*): es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

HTTP o Hypertext Transfer Protocol (en español *protocolo de transferencia de hipertexto*): es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

HTTPS o Hypertext Transfer Protocol Secure (en español: *Protocolo seguro de transferencia de hipertexto*), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales y/o contraseñas.

Telnet: es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet,

la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

TCP: *Transmission Control Protocol* (TCP) o Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear “conexiones” entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

UDP (User Datagram Protocol) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

SSH (Secure SHell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows). Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

FTP (*File Transfer Protocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

5. Bibliografía

Libro 1: PRINCIPIOS DE ROUTING SWITCHING (CCNA 2),

ISBN 9788490354742 , PEARSON, 2014

Libro 2: REDES ESCALARES (CCNA 3)

ISBN 9788490354759, PEARSON, 2015

Libro 3: CONEXIÓN DE REDES (CCNA 4)

ISBN 9788490354766, PEARSON, 2015

Web 1: <http://blog.capacityacademy.com> (abril - mayo 2016)

Web 2: <https://www.nagios.org> (mayo 2016)

Web 3: <https://www.pfsense.org> (mayo 2016)

Web 4: <https://es.wikipedia.org> (abril – mayo 2016)

Web 5: <http://www.ubuntu.com> (mayo 2016)

Web 6: <http://blog.soporteti.net> (mayo 2016)

Web 7: <https://www.digitalocean.com/community/tutorials/how-to-install-nagios-4-and-monitor-your-servers-on-ubuntu-14-04> (mayo 2016)

Web 8: <http://www.cisco.com> (abril – mayo 2016)

6. Anexos

Anexo A: Protección de los switches.

A continuación se definen los pasos necesarios para proteger los switches de Cisco de la organización.

Se protegerán los dispositivos mediante una contraseña cifrada para las conexiones de consola y conexiones de red seguras mediante el protocolo SSH.

Se van a introducir las medidas de seguridad en los siguientes dispositivos:

- Centro administrativo:
 - Core principal.
 - Switch acceso planta baja
 - Switch acceso planta 1.
 - Switch acceso planta 2.
- Centro Productivo:
 - Core secundario.
 - Switch acceso zona 1.
 - Switch acceso zona 2.
- Enlace de respaldo:
 - Switch enlace respaldo.
- Centro Logístico:
 - Switch acceso.

Los siguientes pasos serán aplicables a los dispositivos detallado anteriormente.

1. Acceder al dispositivo mediante el puerto de consola, para ello se utiliza un cable RJ45-RS232 suministrado con el dispositivo.
 - 1.1. Conectar dicho cable en el puerto de consola del dispositivo mediante el conector RJ45 y con un PC mediante el puerto RS232.
 - 1.2. Abrir un programa para conexiones Telnet, SSH y consola como Putty.
 - 1.3. Escoger la conexión de consola.
2. Una vez conectados al dispositivo de red:
 - 2.1. Ingresamos en modo EXEC (modo que permite modificar) mediante el comando:
enable
 - 2.2. Ingresamos en modo de configuración mediante el comando:

configure terminal

2.3. Le damos un nombre al dispositivo de red mediante el comando:

```
hostname ca-p0
```

Para los distintos dispositivo le asignamos los siguientes nombres:

- Centro administrativo:
 - ca-p0: switch acceso planta baja
 - ca-p1: switch acceso primera planta
 - ca-p2: switch acceso segunda planta
 - ca-core: core principal del centro administrativo
- Centro Productivo:
 - cp-core: Core secundario.
 - cp-z1: Switch acceso zona 1.
 - cp-z2: Switch acceso zona 2.
- Enlace de respaldo:
 - er-er: Switch enlace respaldo.
- Centro Logístico:
 - cl-z1: Switch acceso.

2.4. Deshabilitamos la búsqueda DNS para evitar que el dispositivo intente traducir los comandos incorrectos como si fueran nombres de host:

```
no ip domain lookup
```

2.5. Configuramos el nombre de usuario de una base de datos local con máximos privilegios mediante el comando:

```
username admin privilege 15 secret uoc
```

Utilizaremos la contraseña uoc en todos los dispositivos.

2.6. Habilitamos el acceso por consola con el usuario de la base de datos local mediante los siguientes comandos:

```
>line con 0
```

```
>login local
```

```
>end
```

2.7. Habilitamos el acceso seguro por ssh con el usuario de la base de datos local mediante los siguientes comandos:

```
>ip domain-name org.com
```

```
>crypto key generate rsa 1024
```

```
>line vty 0 15
```

```
>transport input ssh
```

>login local

>end

2.8. Creamos un mensaje de aviso que advierta de acceso no autorizados mediante el siguiente comando:

>banner motd "Acceso solo usuarios permitidos. "

2.9. Salimos del modo de configuración con el siguiente comando:

>exit

2.10. Guardamos la configuración introducida mediante el siguiente comando:

>copy r s

Anexo B: Configuración de VLANs e IP de administración en los switches.

1. Acceder al dispositivo mediante el puerto de consola, para ello se utiliza un cable RJ45-RS232 suministrado con el dispositivo.
 - 1.1. Conectar dicho cable en el puerto de consola del dispositivo mediante el conector RJ45 y con un PC mediante el puerto RS232.
 - 1.2. Abrir un programa para conexiones Telnet, SSH y consola como Putty.
 - 1.3. Escoger la conexión de consola.
2. Una vez conectados al dispositivo de red:

- 2.1. Nos pedirá Username y Password (ya definidos en el punto anterior):

Username: admin

Password: uoc

- 2.2. Pasamos a modo de configuración del dispositivo mediante el siguiente comando:

```
>configure terminal
```

- 2.3. Preparamos el “ca-core” como servidor del protocolo VTP (nos permitirá crear vlans en este dispositivo y que se propaguen al resto de switches):

- 2.4. Servidor VTP (solo “ca-core”):

```
>vtp domain ORG
```

```
>vtp mode server
```

```
>vtp password uoc
```

```
>exit
```

- 2.5. Cliente VTP (resto de switches):

```
>vtp domain ORG
```

```
>vtp mode client
```

```
>vtp password uoc
```

```
>exit
```

- 2.6. Después creamos las distintas vlans mediante los siguientes comandos(en el switch CA-CORE, se propagara al resto cuando completemos el punto 2.c.ii):

```
>vlan 2
```

```
>name RED
```

```
>exit
```

```
>vlan 3
```

```
>name INDUSTRIAL
```



```
>exit
>vlan 9
>name SERVIDORES
>exit
>vlan 10
>name USUARIOS
>exit
>vlan 100
>name DMZ
>exit
```

2.7. A continuación configurar la IP de administración en todos los switches mediante los siguientes comandos:

```
>interface vlan 2
>ip address 172.16.2.1 255.255.255.0
>no shutdown
>exit
```

2.8. En los diferentes switches sustituir la IP y la máscara del segundo comando por sus datos correspondientes, definidos en la tabla anterior.

Anexo C: configuración de enlaces agregados y redundantes

Para proceder con la configuración lo haremos de la siguiente forma:

1. Configurar PAgP entre CA-CORE y CP-CORE:

1.1. CA-CORE:

```
>configure terminal
>interface range g0/1-2
>channel-group 1 mode desirable
>no shutdown
>exit
>interface port-channel 1
>switchport mode trunk
>switchport trunk encapsulation dot1q
>exit
```

1.2. CP-CORE:

```
>configure terminal
>interface range g0/1-2
>channel-group 1 mode auto
>no shutdown
>interface port-channel 1
>switchport mode trunk
>switchport trunk encapsulation dot1q
>exit
```

Con estos pasos ya tenemos un enlace lógico entre el centro administrativo y el centro productivo, compuesto por 2 cables de red conectados a dos tomas Gigabit, lo cual nos ofrece un ancho de banda entre las dos sedes de 2000 megabits por segundo. Además, esto también nos permite que ante el corte de alguno de los dos cables no perdemos conectividad, solo ancho de banda, este pasaría a la mitad.

El siguiente objetivo de este punto será realizar un enlace redundante utilizando el switch ER-ER, el cual estará en espera de una posible caída del enlace principal entre en centro administrativo y el centro logístico. Para configurarlo utilizaremos el protocolo LACP de agregación de enlaces, con esto además de tener un enlace redundado también tenemos mayor ancho de banda.

2. Configurar LACP entre CA-CORE y ER-ER:

2.1. CA-CORE:

```
>configure terminal
>interface range f0/1-2
>switchport mode trunk
>switchport trunk encapsulation dot1q
>channel-group 2 mode active
>no shutdown
>exit
```

2.2. ER-ER:

```
>configure terminal
>interface range f0/1-2
>switchport mode trunk
>switchport trunk encapsulation dot1q
>channel-group 2 mode passive
>no shutdown
>exit
```

3. Configurar LACP entre ER-ER y CP-CORE:

3.1. ER-ER:

```
>configure terminal
>interface range f0/3-4
>switchport mode trunk
>switchport trunk encapsulation dot1q
>channel-group 3 mode active
>no shutdown
>exit
```

3.2. CP-CORE:

```
>configure terminal
>interface range f0/1-2
>switchport mode trunk
>switchport trunk encapsulation dot1q
>channel-group 3 mode passive
>no shutdown
>exit
```

Después de esto ya podemos hacer las pruebas necesarias para probar la redundancia de los enlaces haciendo “shutdown” en las distintas conexiones que forman el anillo de conexiones.

Anexo D: Protección de los routers.

1. Acceder al dispositivo mediante el puerto de consola, para ello se utiliza un cable RJ45-RS232 suministrado con el dispositivo.
 - 1.1. Conectar dicho cable en el puerto de consola del dispositivo mediante el conector RJ45 y con un PC mediante el puerto RS232.
 - 1.2. Abrir un programa para conexiones Telnet, SSH y consola como Putty.
 - 1.3. Escoger la conexión de consola.
2. Una vez conectados al dispositivo de red:
 - 2.1. Ingresamos en modo EXEC (modo que permite modificar) mediante el comando:

```
>enable
```

- 2.2. Ingresamos en modo de configuración mediante el comando:

```
>configure terminal
```

- 2.3. Le damos un nombre al dispositivo de red mediante el comando:

```
>hostname R-CA
```

Para los distintos dispositivo le asignamos los siguientes nombres:

- Centro Administrativo:
 - R-CA: router principal.
- Centro Productivo:
 - R-CP: router de respaldo.
- Centro Logístico:
 - RP: router principal.
 - RB: router de respaldo.

- 2.4. Deshabilitamos la búsqueda DNS para evitar que el dispositivo intente traducir los comandos incorrectos como si fueran nombres de host:

```
>no ip domain lookup
```

- 2.5. Configuramos el nombre de usuario de una base de datos local con máximos privilegios mediante el comando:

```
>username admin privilege 15 secret uoc
```

Utilizaremos la contraseña uoc en todos los dispositivos.

- 2.6. Habilitamos el acceso por consola con el usuario de la base de datos local mediante los siguientes comandos:

```
>line con 0
```

```
>login local
```

```
>end
```

2.7. Habilitamos el acceso seguro por ssh con el usuario de la base de datos local mediante los siguientes comandos:

```
>ip domain-name org.com  
>crypto key generate rsa 1024  
>line vty 0 4  
>transport input ssh  
>login local  
>end
```

2.8. Creamos un mensaje de aviso que advierta de acceso no autorizados mediante el siguiente comando:

```
>banner motd "Acceso solo usuarios permitidos. "
```

2.9. Salimos del modo de configuración con el siguiente comando:

```
>exit
```

2.10. Guardamos la configuración introducida mediante el siguiente comando:

```
>copy r s
```

Anexo E: Configuración del enrutamiento en los routers

Centro administrativo y centro productivo.

Lo primero que tenemos que hacer es que los switches multicapa del centro administrativo y el centro productivo enruten en capa 3 en la interfaz que conectemos los routers. Para ello procedemos de la siguiente manera en CA-CORE y CP-CORE:

```
>configure terminal
>interface f0/21
>no switchport
>ip address 172.16.101.53 255.255.255.0
>exit
```

NOTA: utilizar la IP 172.16.101.54 en CP-CORE

Después implementamos el enrutamiento OSPF en los dos switches multicapa de la siguiente forma:

```
>configure terminal
>router ospf 1

>network 172.16.2.0 0.0.0.255 area 0

>network 172.16.4.0 0.0.1.255 area 0
>network 172.16.9.0 0.0.0.255 area 0
>network 172.16.10.0 0.0.1.255 area 0
>network 172.16.100.0 0.0.0.255 area 0
>network 172.16.101.0 0.0.0.255 area 0
>exit
```

Por último configuramos los dos routers siguiendo también el enrutamiento OSPF, además también en ambos routers vamos a implementar el protocolo HSRP para que el router principal sea R-CA (centro administrativo) y se esté falla gracias a dicho protocolo se active la salida del router R-CP.

Para ello procedemos con los siguientes comandos en R-CA:

```
>configure terminal
>interface f0/0
>ip address 172.16.101.51 255.255.255.0
>standby 1 ip 172.16.101.50
>standby 1 priority 150
>standby 1 preempt
>exit
```

```
>router ospf 1
>network 172.16.101.0 0.0.0.255 area 0
>exit
```

Después, configuramos los siguientes comandos en R-CP:

```
>configure terminal
>interface f0/0
>ip address 172.16.101.52 255.255.255.0
>standby 1 ip 172.16.101.50
>exit
>router ospf 1
>network 172.16.101.0 0.0.0.255 area 0
>exit
```

Centro logístico.

Para el centro logístico vamos a seguir las mismas pautas citadas anteriormente. Primero, vamos a preparar el switch del centro logístico CL-Z1 para ello. Introducimos los siguientes comandos para preparar los enlaces donde conectar los routers:

```
>configure terminal
>interface range fastethernet0/23-24
>switchport access vlan 2
>switchport mode access
>exit
>ip default-gateway 192.168.1.250
```

NOTA: con el ultimo comando le decimos el Gateway de salida al switch.

Ahora configuramos el router principal del centro logístico (RP) con los siguientes comandos:

```
>configure terminal
>interface FastEthernet0/0
>ip address 192.168.1.251 255.255.255.0
>standby 1 ip 192.168.1.250
>standby 1 priority 150
>standby 1 preempt
>exit
>router ospf 1
>network 192.168.1.0 0.0.0.255 area 0
```



```
>exit
```

Por último, configuramos el router de la línea de respaldo (RB):

```
>configure terminal
>interface FastEthernet0/0
>ip address 192.168.1.252 255.255.255.0
>standby 1 ip 192.168.1.250
>exit
>router ospf 1
>network 192.168.1.0 0.0.0.255 area 0
>exit
```

Interfaz Loopback.

Para realizar las pruebas a través de la aplicación Cisco Packet Tracer se ha configurado una interfaz de Loopback en los cuatro routers (8.8.8.8). Esto nos permite definir una IP fija para simular los balaceos ante caídas de líneas. Para ello se han introducido los siguientes comandos en los cuatro routers:

```
>configure terminal
>interface Loopback1
>ip address 8.8.8.8 255.255.255.0
>exit
```

Anexo F: Configuración de la VPN entre las sedes

Centro administrativo y centro productivo.

Para configurar los routers del centro administrativo (R-CA) y del centro productivo (R-CP) procedemos con los siguientes comandos en ambos:

1. Configuración del túnel VPN:

```
>configure terminal
>interface tunnel 0
>ip address 1.1.1.1 255.255.255.252
>tunnel source s0/0/0
>tunnel destination 10.2.2.1
>exit
```

2. Configuración de conexión con el ISP:

```
>interface s0/0/0
>ip address 10.1.1.1 255.255.255.252
>clock rate 128000
>exit
```

3. Configuración de rutas estáticas para la conexión entre tres puntos (Centro Administrativo-Productivo, Centro Logístico, salida Internet:

```
>ip route 0.0.0.0 0.0.0.0 10.1.1.2
>ip route 192.168.1.0 255.255.255.0 1.1.1.2
>ip route 172.16.2.0 255.255.255.0 172.16.101.53
>ip route 172.16.10.0 255.255.254.0 172.16.101.53
>ip route 172.16.4.0 255.255.254.0 172.16.101.53
>ip route 172.16.9.0 255.255.255.0 172.16.101.53
>ip route 172.16.100.0 255.255.255.0 172.16.101.53
>exit
```

Centro logístico.

Para configurar los routers del centro logístico (RP y RB) procedemos con los siguientes comandos en ambos:

1. Configuración del túnel VPN:

```
>configure terminal
>interface tunnel 0
>ip address 1.1.1.2 255.255.255.252
>tunnel source s0/0/0
```

```
>tunnel destination 10.1.1.1
```

```
>exit
```

2. Configuración de conexión con el ISP:

```
>interface s0/0/0
```

```
>ip address 10.2.2.1 255.255.255.252
```

```
>exit
```

3. Configuración de rutas estáticas para la conexión entre tres puntos (Centro Administrativo-Productivo, Centro Logístico, salida Internet):

```
>ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

```
>ip route 172.16.101.0 255.255.255.0 1.1.1.1
```

```
>ip route 172.16.2.0 255.255.255.0 1.1.1.1
```

```
>ip route 172.16.10.0 255.255.254.0 1.1.1.1
```

```
>ip route 172.16.4.0 255.255.254.0 1.1.1.1
```

```
>ip route 172.16.100.0 255.255.255.0 1.1.1.1
```

```
>ip route 172.16.9.0 255.255.255.0 1.1.1.1
```

```
>exit
```

ISPs.

En este apartado configuraremos dos routers que simularán los de los proveedores de servicios de Internet y las IPs públicas de la organización.

Para configurar los routers del ISP (ISP1 y ISP2) procedemos con los siguientes comandos en ambos:

Configuración de IPs de ambos extremos del router:

```
>configure terminal
```

```
>interface Serial0/0/0
```

```
>ip address 10.1.1.2 255.255.255.252
```

```
>exit
```

```
>interface Serial0/0/1
```

```
>ip address 10.2.2.2 255.255.255.252
```

```
>clock rate 128000
```

```
>exit
```

Anexo G: Instalación y configuración del servicio DHCP en Windows Server 2012

Instalación.

Partimos de que ya tenemos un Windows Server 2012 Standard instalado y configurado con los siguientes requisitos previos:

- IP fija.
- Ser miembro de un dominio.

Procedemos a la instalación del rol de Servidor DHCP del siguiente modo:

1. Agregar rol: desde el administrador del servidor nos vamos a Administrar y pulsamos en “Agregar roles y características”.

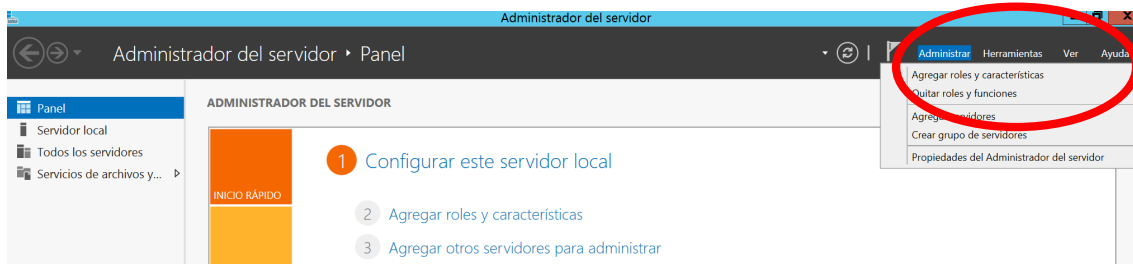


Ilustración 23 - Instalación DHCP (paso 1)

2. Se abre un asistente en el que marcamos las siguientes opciones:

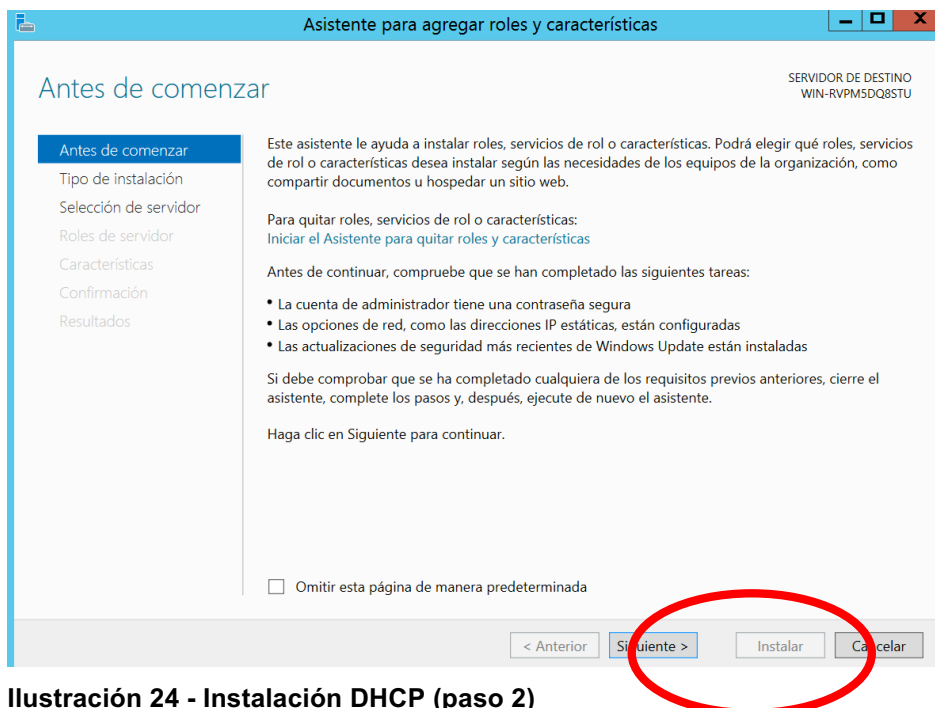


Ilustración 24 - Instalación DHCP (paso 2)

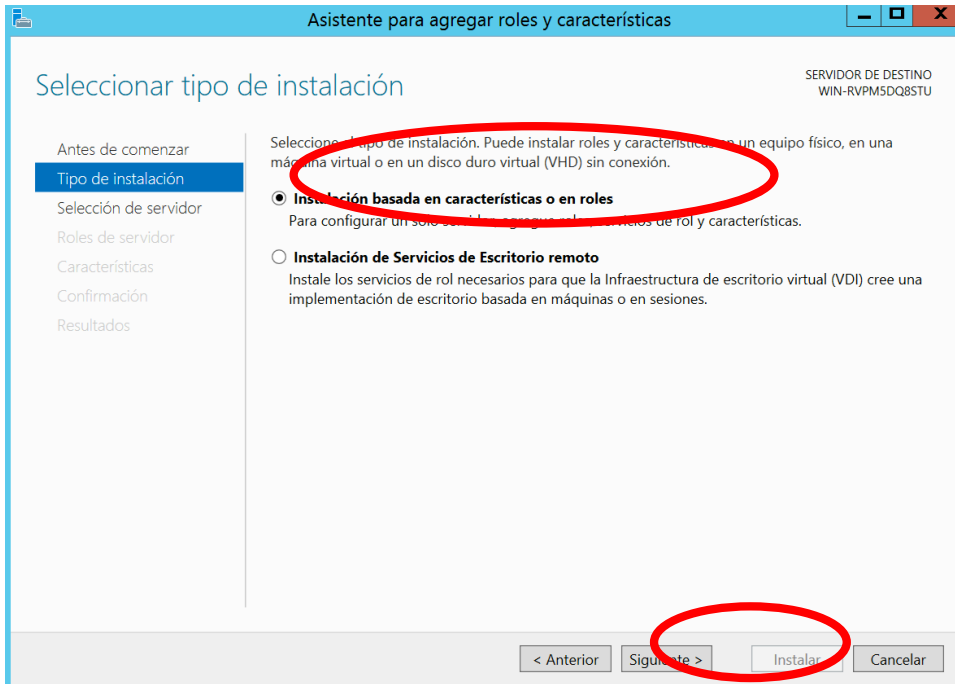


Ilustración 25 - Instalación DCP (paso 3)

3. Marcar “Servidor DHCP” y se nos abre una ventana donde se pulsa “Agregar característica”:

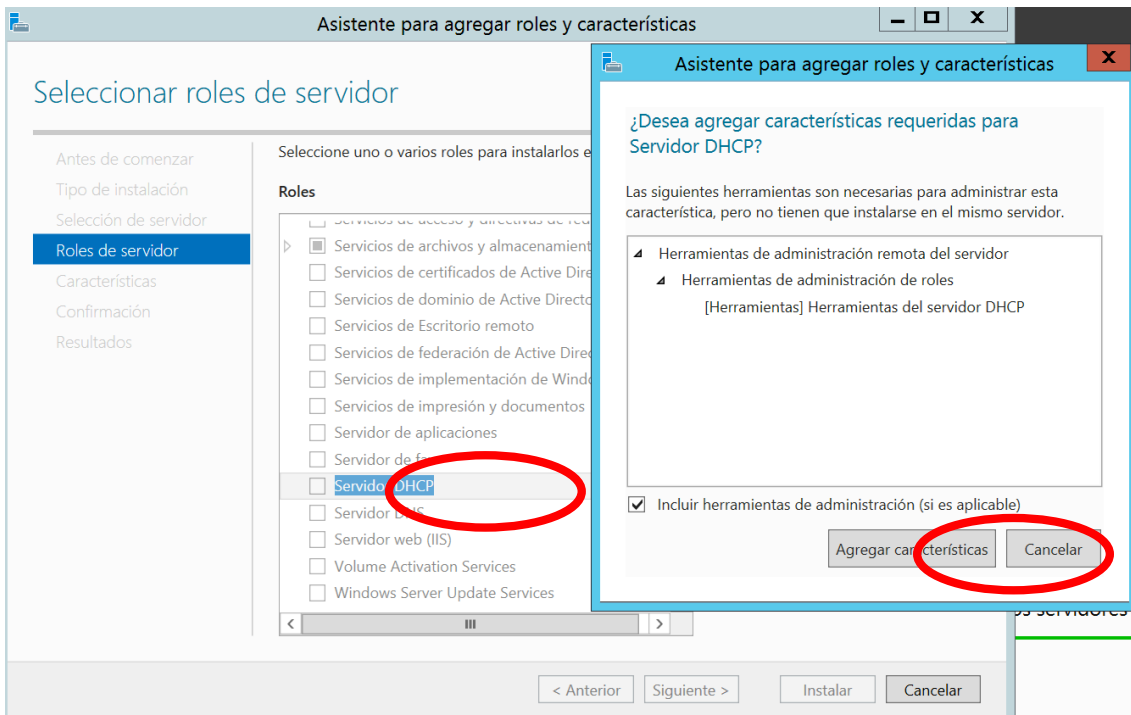


Ilustración 26 - Instalación DHCP (paso 4)

4. Seguir como se indica en las siguientes imágenes para finalizar el asistente:

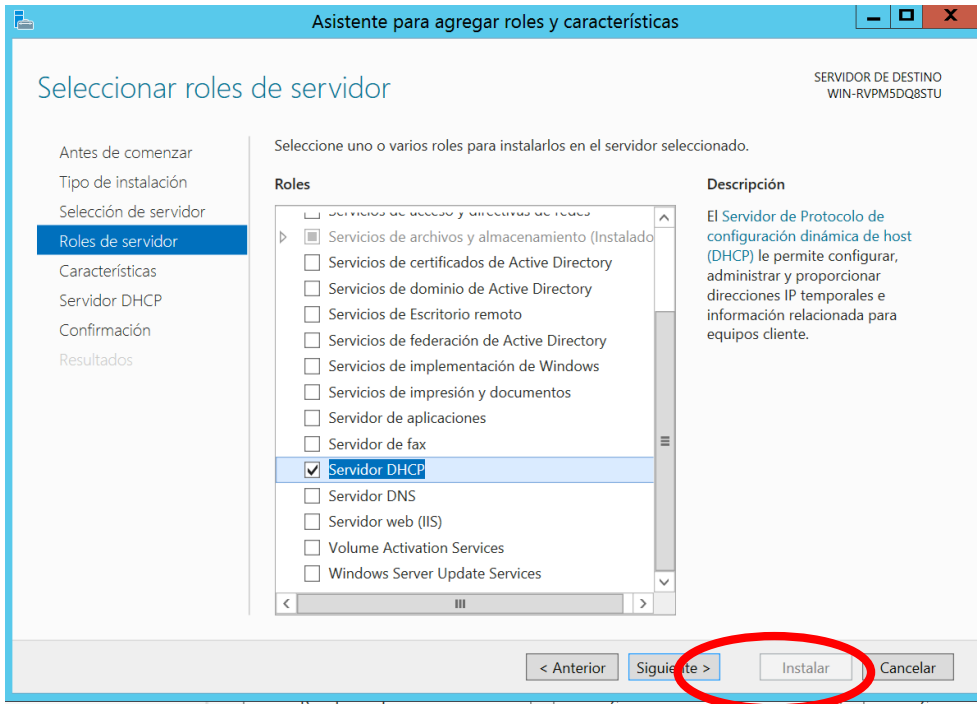


Ilustración 27 - Instalación DHCP (paso 5)

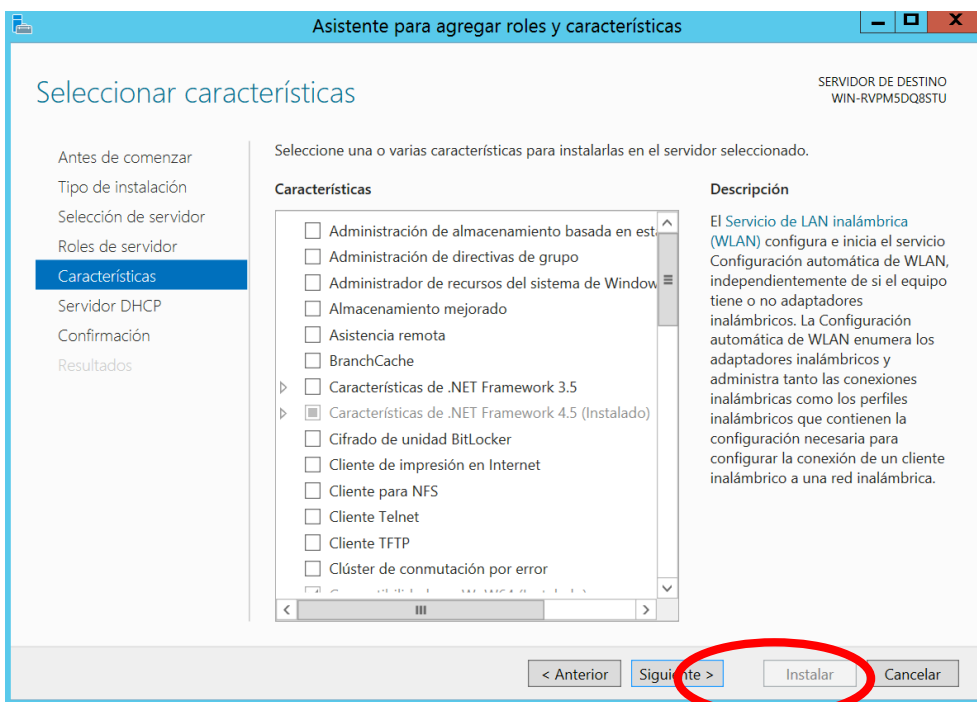


Ilustración 28 - Instalación DHCP (paso 6)

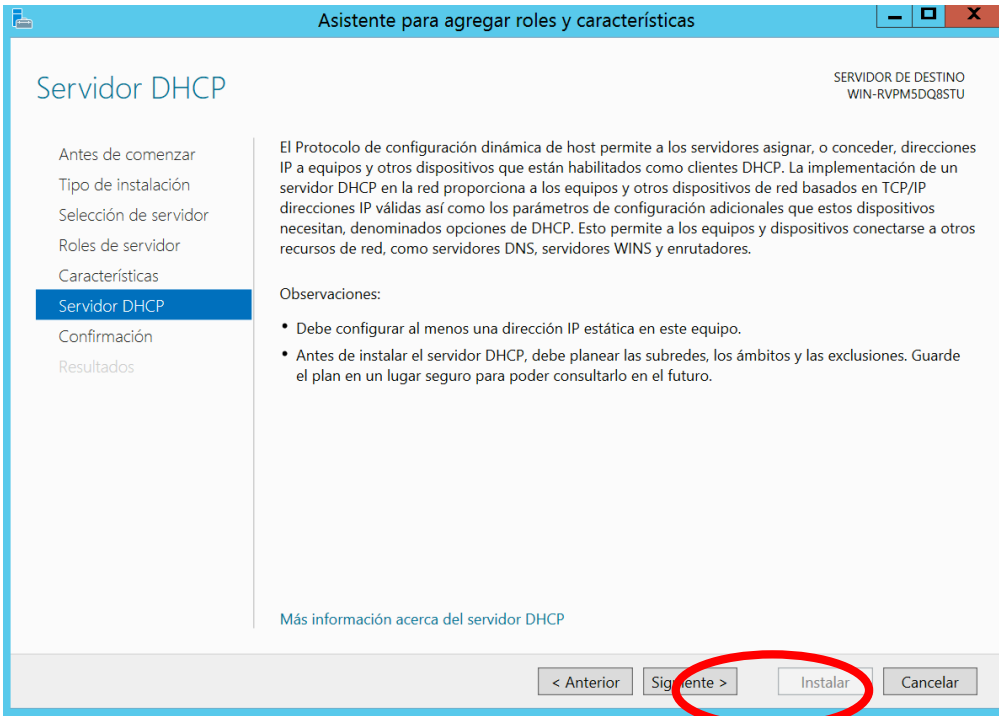


Ilustración 29 - Instalación DHCP (paso 7)

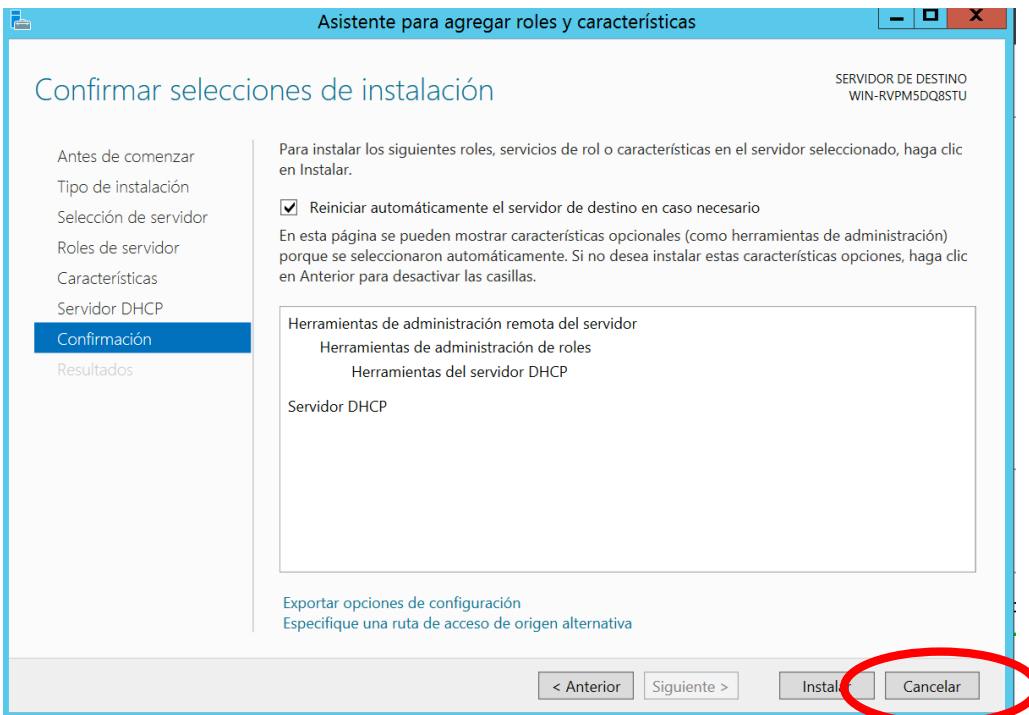


Ilustración 30 - Instalación DHCP (paso 8)

5. Comenzará el proceso de instalación del rol de DHCP:

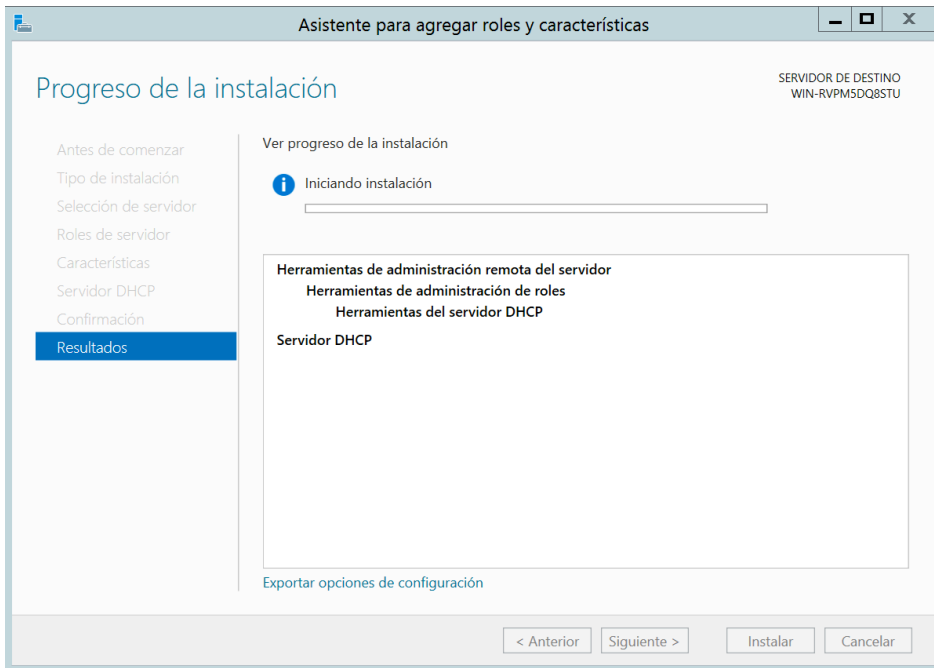


Ilustración 31 - Instalación DHCP (paso 9)

6. Una vez finalizada la instalación pulsar en el botón de “Cerrar”:

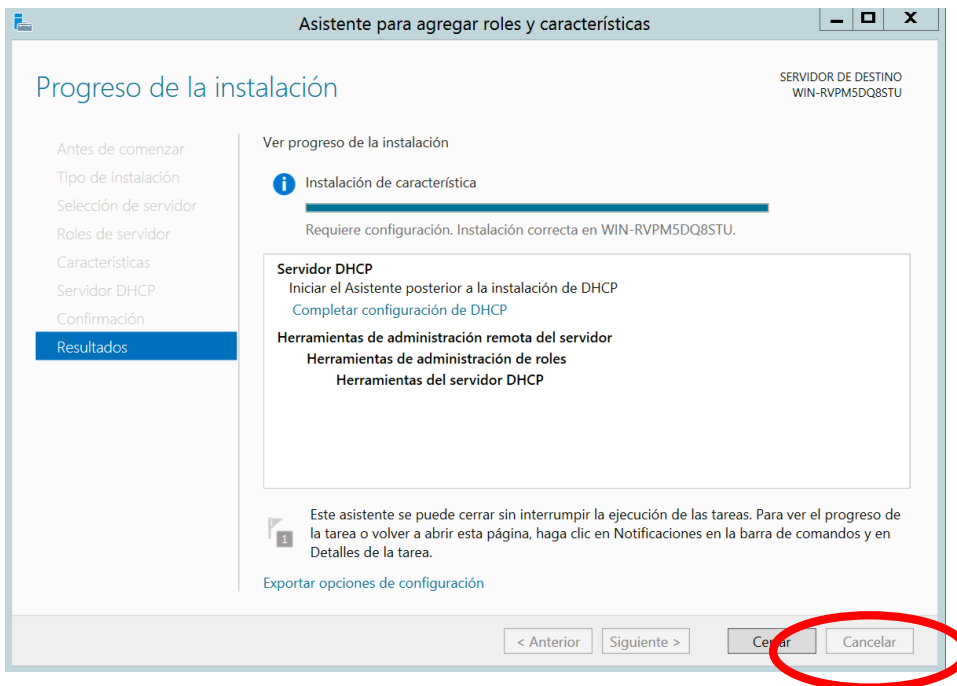


Ilustración 32 - Instalación DHCP (paso 10)

Configuración.

En el siguiente apartado se muestra como configurar dos ámbitos distintos, uno para la red industrial y otro para la red de usuarios.

1. Desde el panel “Administrador del servidor” pulsamos en Herramientas - > DHCP, para abrir el gestor del servicio DHCP:

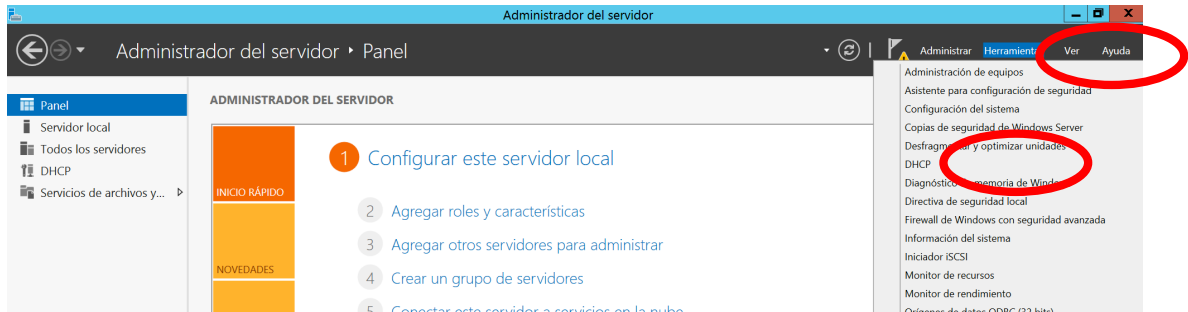


Ilustración 33 - Configuración DHCP (paso 1)

2. Desde IPv4 pulsar el botón derecho del ratón y escoger “Ámbito nuevo...”:

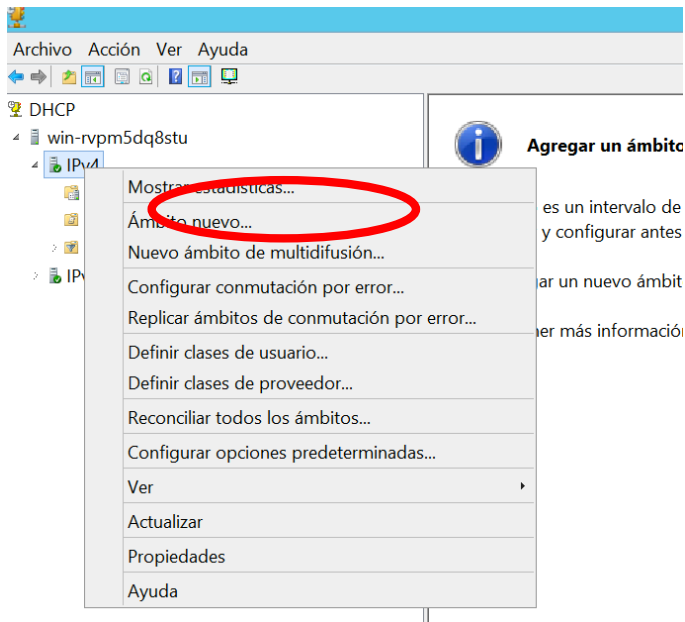


Ilustración 34 - Configuración DHCP (paso 2)

3. Se ejecuta un asistente para la creación de un ámbito nuevo. Pulsamos en "Siguiente":

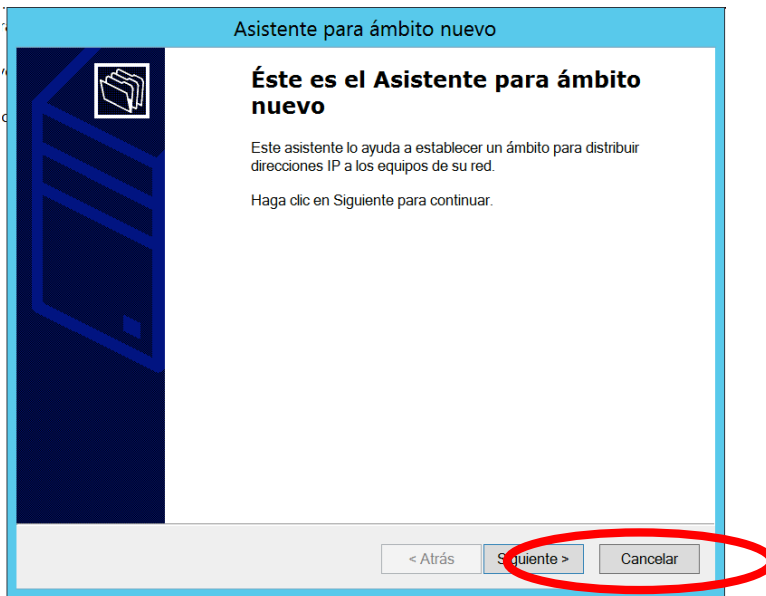


Ilustración 35 - Configuración DHCP (paso 2)

4. Le damos al ámbito un nombre y una descripción, y pulsamos siguiente:

- Ejemplo red industrial:

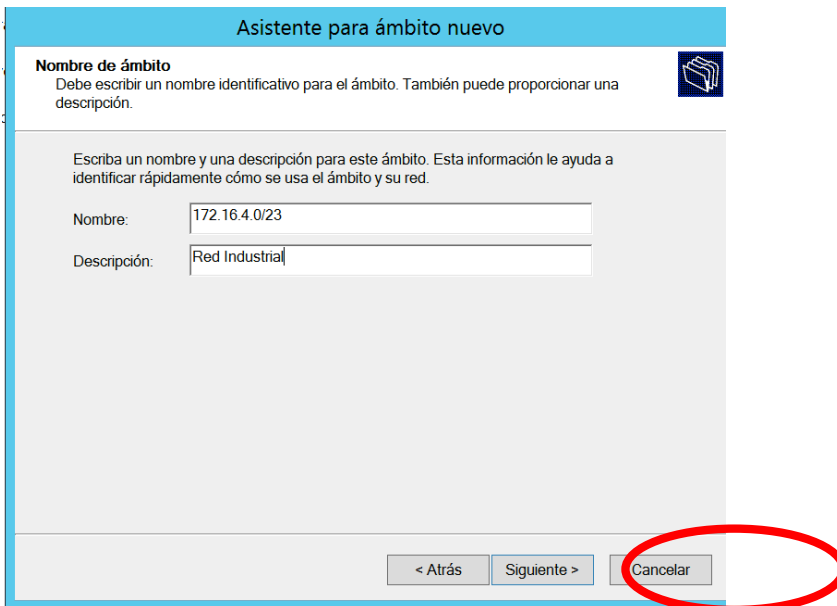


Ilustración 36 - Configuración DHCP (paso 3). Industrial.

- Ejemplo red usuarios.

Asistente para ámbito nuevo

Nombre de ámbito
Debe escribir un nombre identificativo para el ámbito. También puede proporcionar una descripción.

Escriba un nombre y una descripción para este ámbito. Esta información le ayuda a identificar rápidamente cómo se usa el ámbito y su red.

Nombre: 172.16.10.0/23

Descripción: Red usuarios

< Atrás Siguiete > Cancelar

Ilustración 37 - Configuración DHCP (paso 3). Usuarios.

5. Le asignamos un rango de direcciones al ámbito y pulsamos “Siguiete” para continuar:

- Ejemplo red industrial.

Asistente para ámbito nuevo

Intervalo de direcciones IP
Para definir el intervalo de direcciones del ámbito debe identificar un conjunto de direcciones IP consecutivas.

Escriba el intervalo de direcciones que distribuye el ámbito.

Dirección IP inicial: 172 . 16 . 4 . 1

Dirección IP final: 172 . 16 . 5 . 254

Opciones de configuración que se propagan al cliente DHCP

Longitud: 23

Máscara de subred: 255 . 255 . 254 . 0

< Atrás Siguiete > Cancelar

Ilustración 38 - Configuración DHCP (paso 4). Industrial.

- Ejemplo red industrial.

Ilustración 39 - Configuración DHCP (paso 4). Usuarios.

6. Definimos un rango de IPs a excluir en la asignación automática de DHCP y pulsamos siguiente:

- Red industrial: excluimos todo el rango.

Ilustración 40 - Configuración DHCP (paso 5). Industrial.

- Red usuarios: excluimos el rango entre 172.16.10.1-172.16.10.50.

Asistente para ámbito nuevo

Agregar exclusiones y retraso
Exclusiones son direcciones o intervalos de direcciones que no son distribuidas por el servidor.
Retraso es el tiempo que retrasará el servidor la transmisión de un mensaje DHCP OFFER.

Escriba el intervalo de direcciones IP que desee excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.

Dirección IP inicial: Dirección IP final:

Intervalo de direcciones excluido:

- 172.16.10.1 a 172.16.10.50

Retraso de subred en milisegundos:

< Atrás **Cancelar**

Ilustración 41 - Configuración DHCP (paso 5). Usuarios.

7. Indicamos la duración de la concesión. Dejamos la opción por defecto (8 días) y pulsamos en siguiente:

Asistente para ámbito nuevo

Duración de la concesión
La duración de la concesión especifica durante cuánto tiempo puede utilizar un cliente una dirección IP de este ámbito.

La duración de las concesiones debería ser típicamente igual al promedio de tiempo en que el equipo está conectado a la misma red física. Para redes móviles que consisten principalmente de equipos portátiles o clientes de acceso telefónico, las concesiones de duración más corta pueden ser útiles.

De igual modo, para una red estable que consiste principalmente de equipos de escritorio en ubicaciones fijas, las concesiones de duración más larga son más apropiadas.

Establecer la duración para las concesiones de ámbitos cuando sean distribuidas por este servidor.

Limitada a:

Días: Horas: Minutos:

< Atrás

Ilustración 42 - Configuración DHCP (paso 6).

8. Pulsamos en “Configurar estas opciones ahora” y pulsamos en siguiente para continuar:

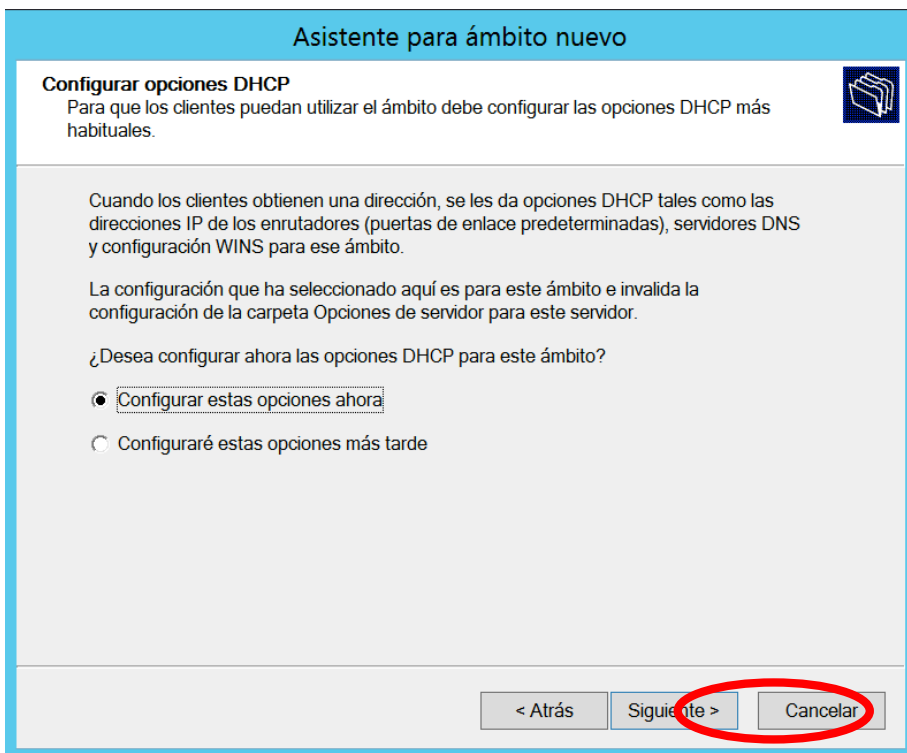


Ilustración 43 - Configuración DHCP (paso 7).

9. En este apartado se configura que IP asiganara al dispositivo final como puerta de enlace predeterminada.
- Red industrial: 172.16.5.250

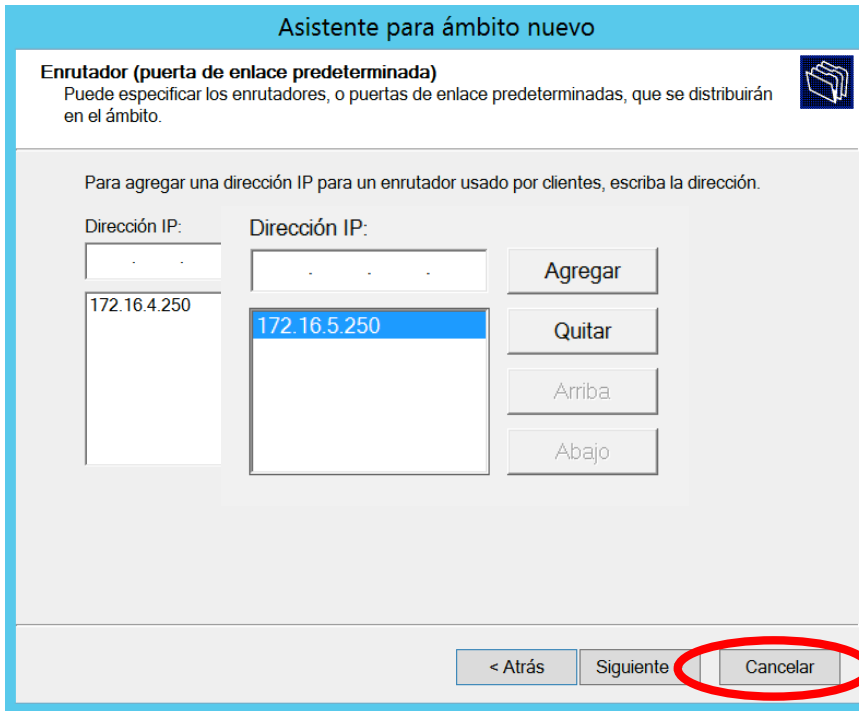


Ilustración 44 - Configuración DHCP (paso 8). Industrial.

- Red usuarios: 172.16.11.250

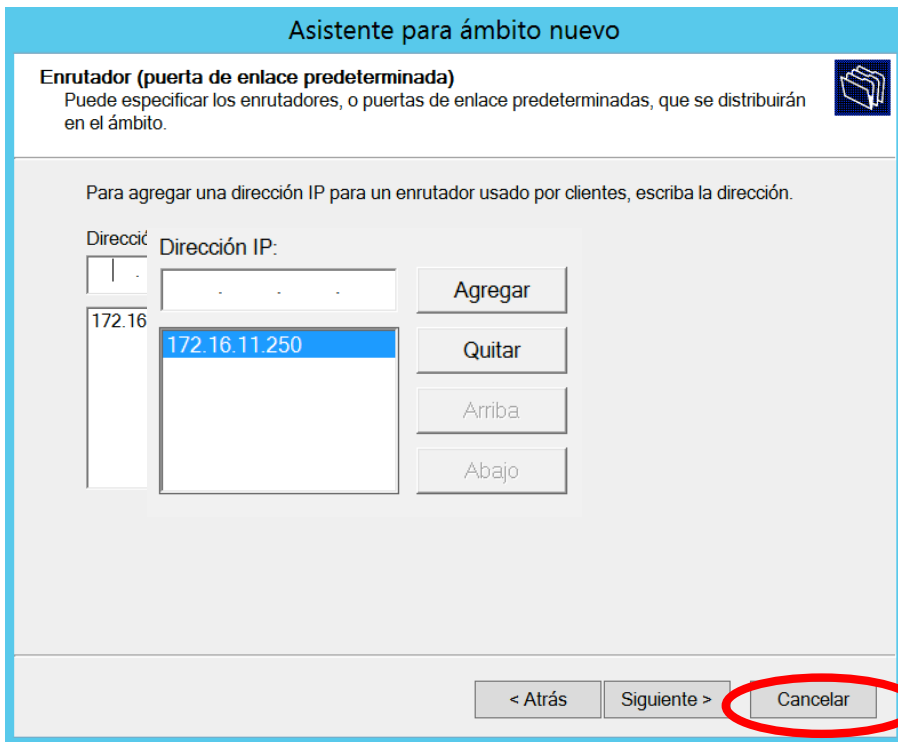


Ilustración 45 - Configuración DHCP (paso 8). Usuarios.

10. Introducimos el nombre del servidor DNS y su IP, pulsamos Siguiete:

Asistente para ámbito nuevo

Nombre de dominio y servidores DNS
El Sistema de nombres de dominio (DNS) asigna y traduce los nombres de dominio que utilizan los clientes de la red.

Puede especificar el dominio primario que desee que los equipos clientes de su red usen para la resolución de nombres DNS.

Dominio primario:

Para configurar clientes de ámbito para usar servidores DNS en su red, escriba las direcciones IP para esos servidores.

Nombre de servidor:	Dirección IP:	
<input type="text"/>	<input type="text"/>	<input type="button" value="Agregar"/>
<input type="button" value="Resolver"/>	172.16.76.2	<input type="button" value="Quitar"/>
		<input type="button" value="Arriba"/>
		<input type="button" value="Abajo"/>

Ilustración 46 - Configuración DHCP (paso 9).

11. En este apartado no introducimos ningún dato y pulsamos en Siguiente:

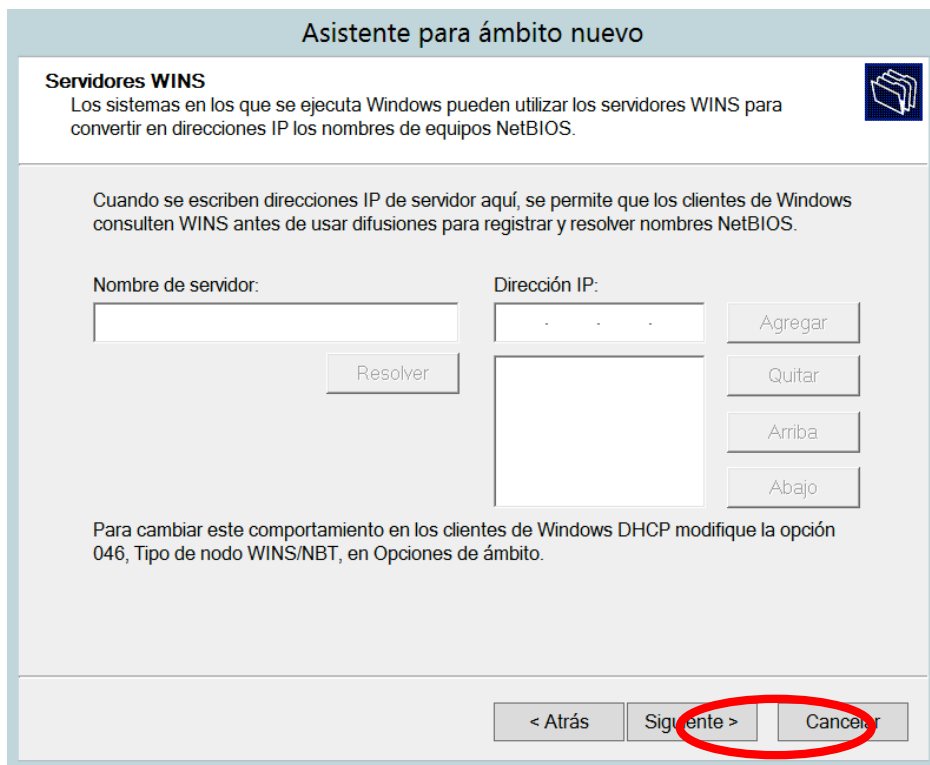


Ilustración 47 - Configuración DHCP (paso 10).

12. Activamos el ámbito y pulsamos Siguiente:

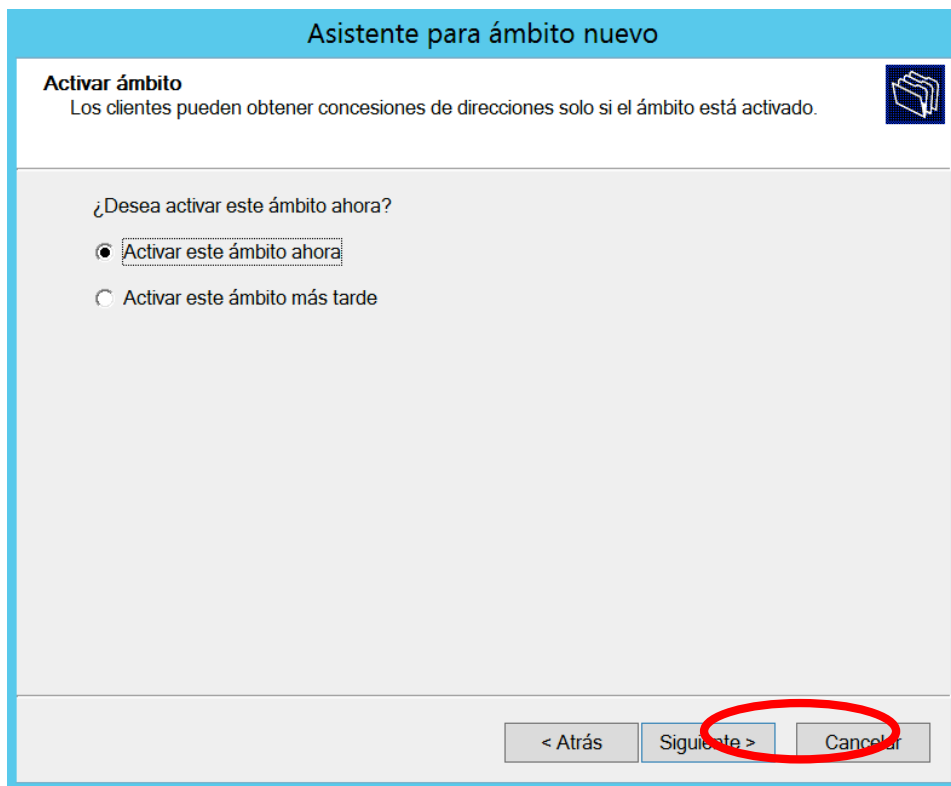


Ilustración 48 - Configuración DHCP (paso 11).

13. Finalizamos el asistente:

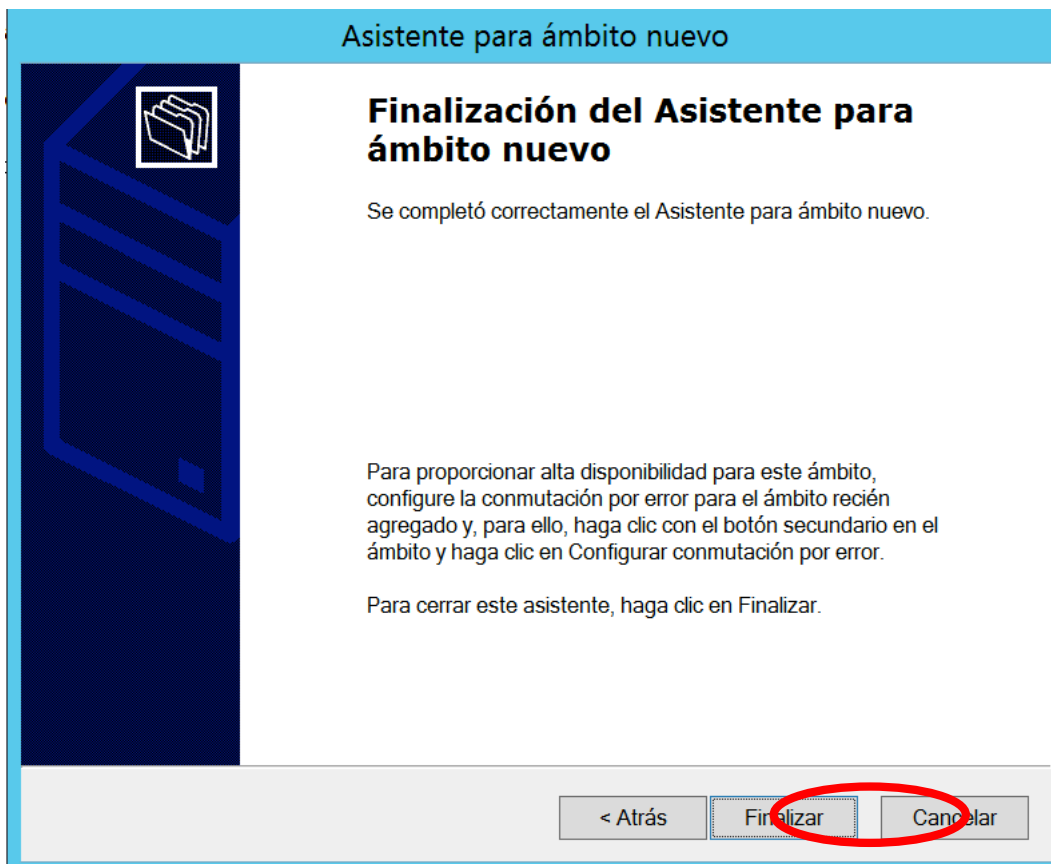


Ilustración 49 - Configuración DHCP (paso 12).

Uso del servicio.

1. Realizar una reserva.

Una de las ventajas que disponemos con la implementación de este servicio es poder realizar reservas de IP basadas en la dirección MAC del dispositivo final. Esto nos puede servir para configurar por ejemplo dispositivos finales industriales de difícil acceso para su configuración.

Para realizar una reserva procedemos de la siguiente forma:

- 1.1. Elegimos un ámbito, apartado reservas y pulsamos con el botón derecho. En el desplegable elegimos “Reserva nueva...”:

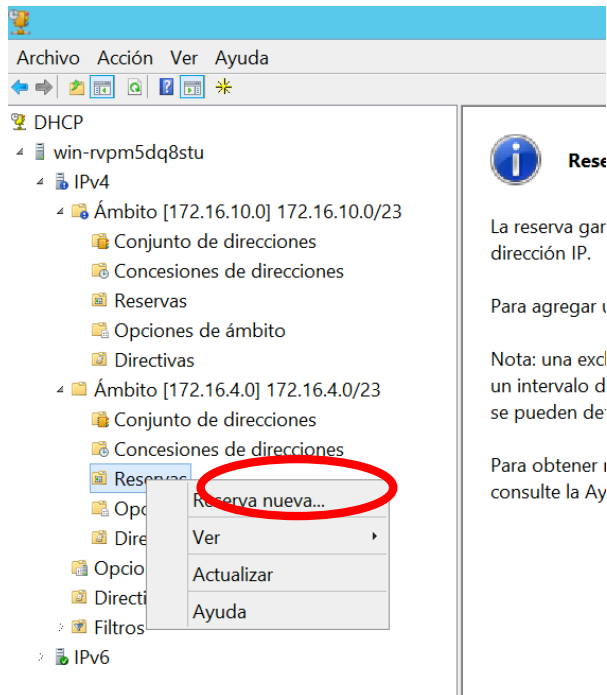


Ilustración 50 - Realizar reserva en DHCP (paso 1).

- 1.2. En la ventana que se abre introducimos un nombre, la dirección IP, la dirección MAC del dispositivo final y una descripción. Pulsamos “Agregar” para confirmar la reserva:

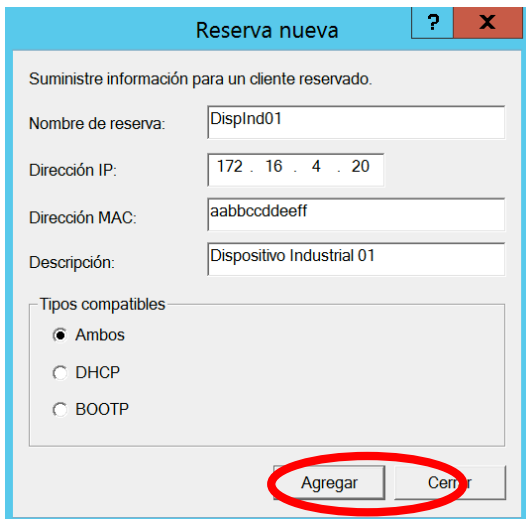


Ilustración 51 - Realizar reserva en DHCP (paso 2).

2. Copia de seguridad y restauración.

El rol de DHCP dispone de la opción de realizar copias de seguridad y restaurarlas.

Para ello tenemos las opciones pulsando botón derecho sobre el nombre del servidor DHCP en las opciones:

- Copia de seguridad...
- Restaurar...

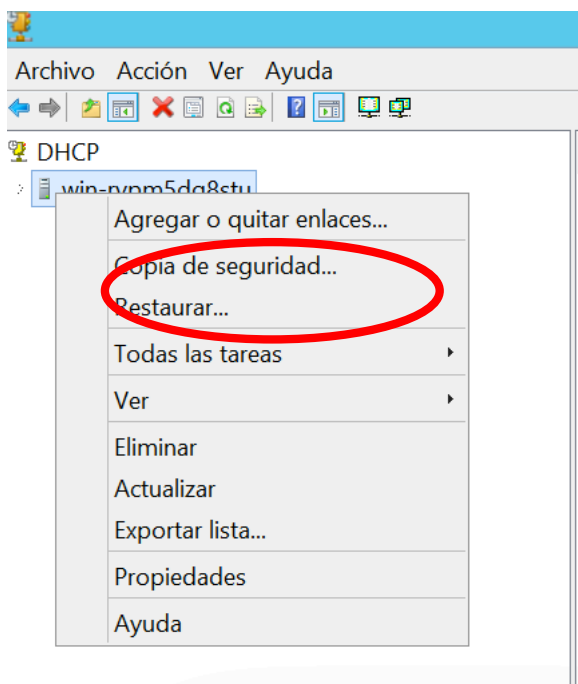


Ilustración 52 - DHCP: Copia de seguridad y restauración

3. Conmutación por error.

Desde la versión de Windows Server 2012 el rol de DHCP nos ofrece la opción de configurar un servidor DHCP en modo de “espera” que se activaría cuando cayera el servicio en el servidor principal.

Para realizar la configuración realizaremos los siguientes pasos:

- 3.1. Crearemos un segundo servidor en el que añadiremos el rol de DHCP sin configurar ningún ámbito.
- 3.2. En el servidor principal (ya tiene configurado los ámbitos) pulsamos sobre IPv4 con el botón derecho y pulsamos en “Configurar conmutación por error...”:

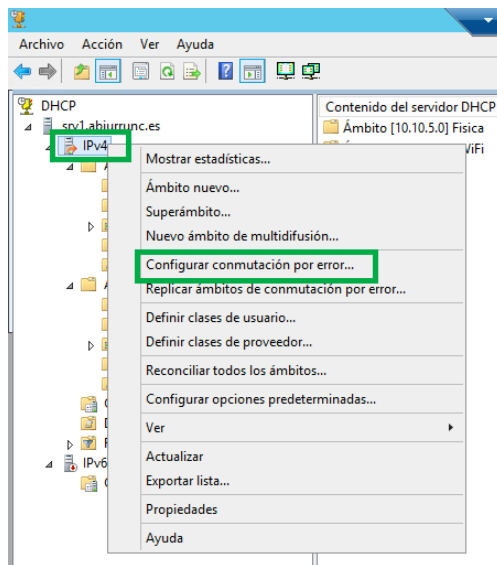


Ilustración 53 - DHCP: Conmutación por error (paso 1)

- 3.3. Se nos abre un asistente para la configuración en el que seleccionamos todos los ámbitos y pulsamos siguiente:

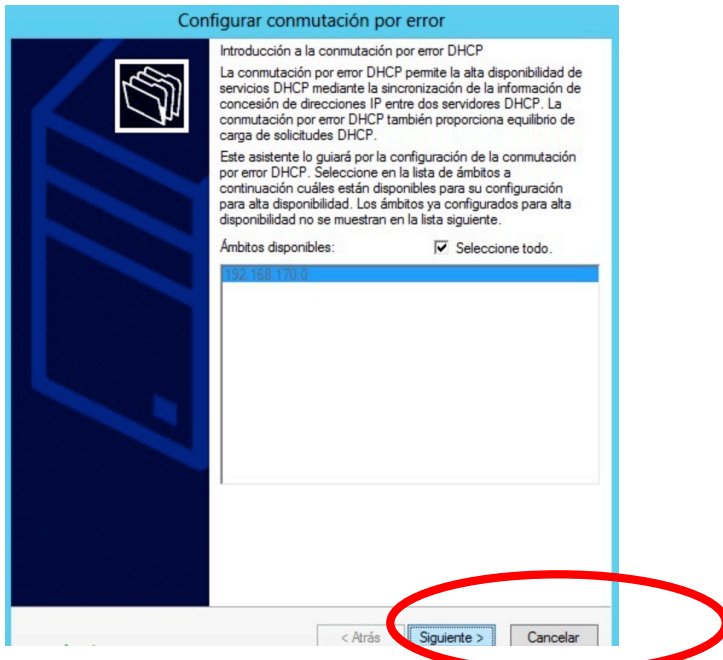


Ilustración 54 - DHCP: Conmutación por error (paso 2)

3.4. Introducimos la IP o el nombre del servidor DHCP que estará en espera:

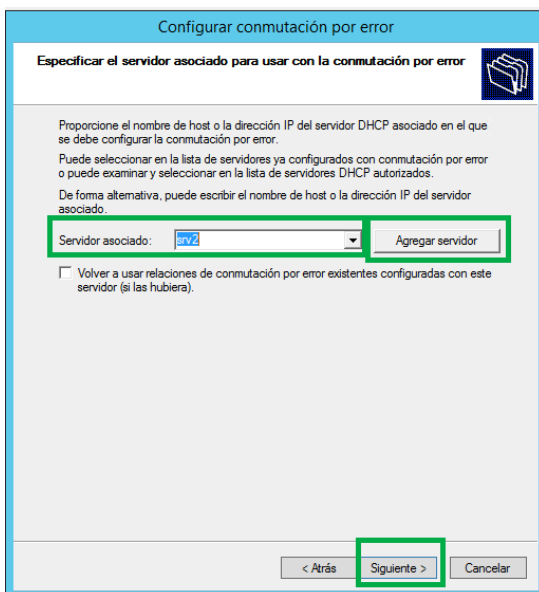


Ilustración 55 - DHCP: Conmutación por error (paso 3)

3.5. La siguiente ventana introducimos la configuración de “Espera activa” tal y como se muestra en la imagen, para que solo sea el principal el que trabaje y el secundario este en espera de una caída del servidor principal. Después pulsamos en siguiente:

Configurar conmutación por error

Crear una nueva relación de conmutación por error

Crear una nueva relación de conmutación por error con el asociado srv2

Nombre de la relación: DHCP Clúster SRV1 - SRV2 EA

Plazo máximo para clientes: 1 horas 0 minutos

Modo: Espera activa

Configuración de espera activa

Rol de servidor asociado: Espera

Direcciones reservadas para el servidor en 30 %

Intervalo de cambio de estado: 60 minutos

Habilitar autenticación de mensajes

Secreto compartido: *****

< Atrás Siguiente > Cancelar

Ilustración 56 - DHCP: Conmutación por error (Paso 4)

3.6. En la siguiente ventana del asistente pulsamos en “Finalizar” para terminar la configuración.

Después de terminar ya podemos ir al segundo servidor y verificar el que el servicio NO está activo y se ha replicado la configuración de los ámbitos seleccionados.

Anexo H: Instalación y configuración del servicio DNS en Windows Server 2012

Instalación.

Para la instalación vamos a aprovechar el servidor DHCP configurado anteriormente para agregarle el rol de DNS.

Para ello procedemos a la instalación del rol de la siguiente manera:

1. Agregar rol: desde el administrador del servidor nos vamos a Administrar y pulsamos en “Agregar roles y características”.



Ilustración 57 - Instalación servicio DNS (paso 1)

2. Se abre un asistente en el que marcamos las siguientes opciones:

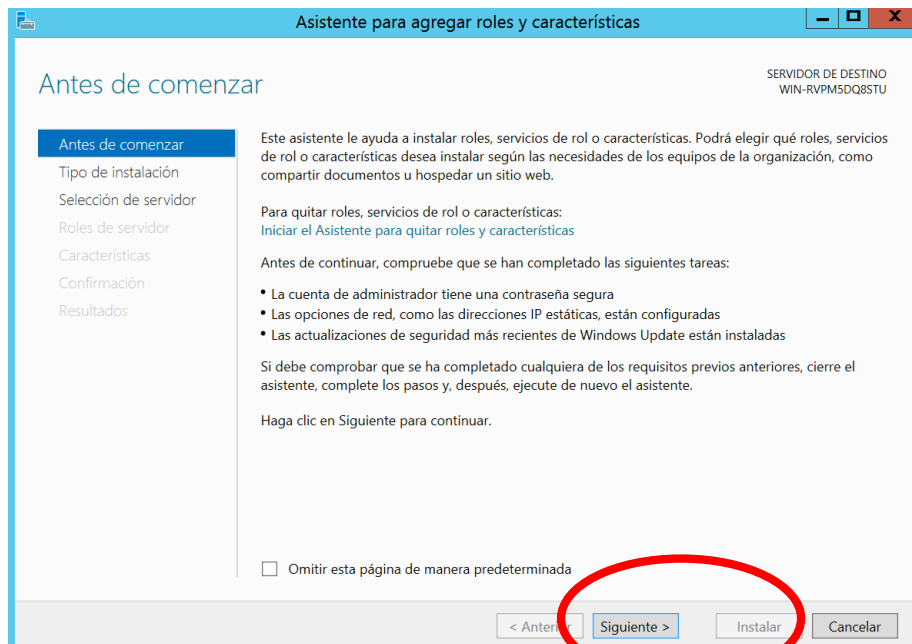


Ilustración 58 - Instalación servicio DNS (paso 2)

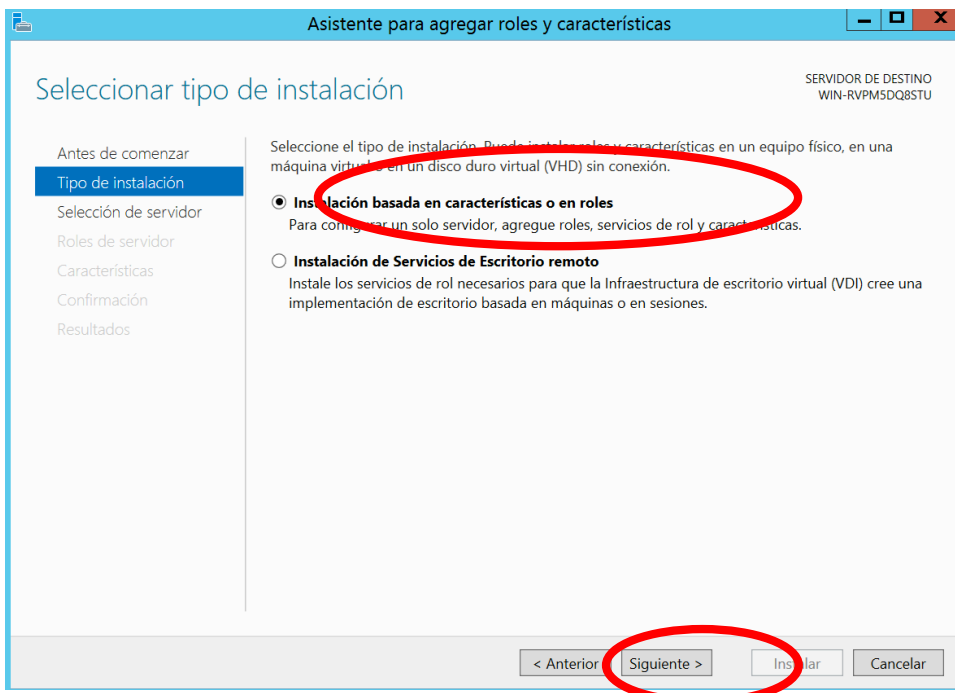


Ilustración 59 - Instalación servicio DNS (paso 3)

3. Marcar “Servidor DNS” y se nos abre una ventana donde se pulsa “Agregar característica”:

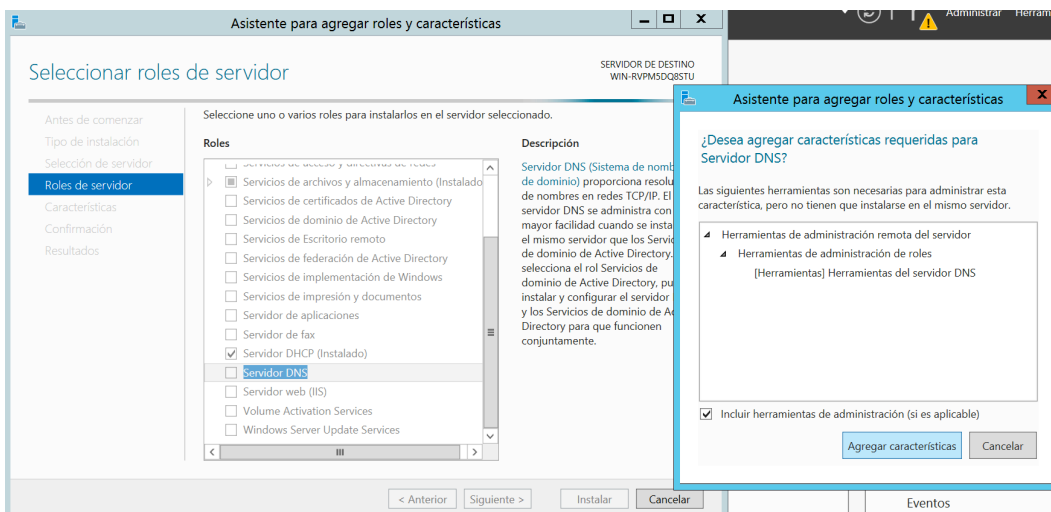


Ilustración 60 - Instalación servicio DNS (paso 4)

4. Seguir como se indica en las siguientes imágenes para finalizar el asistente:

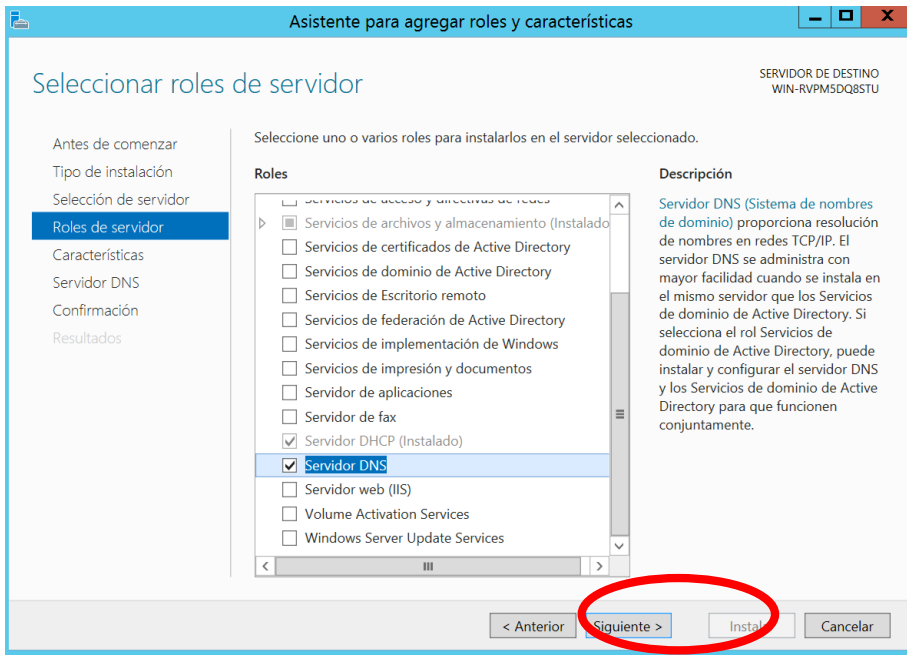


Ilustración 61 - Instalación servicio DNS (paso 5)

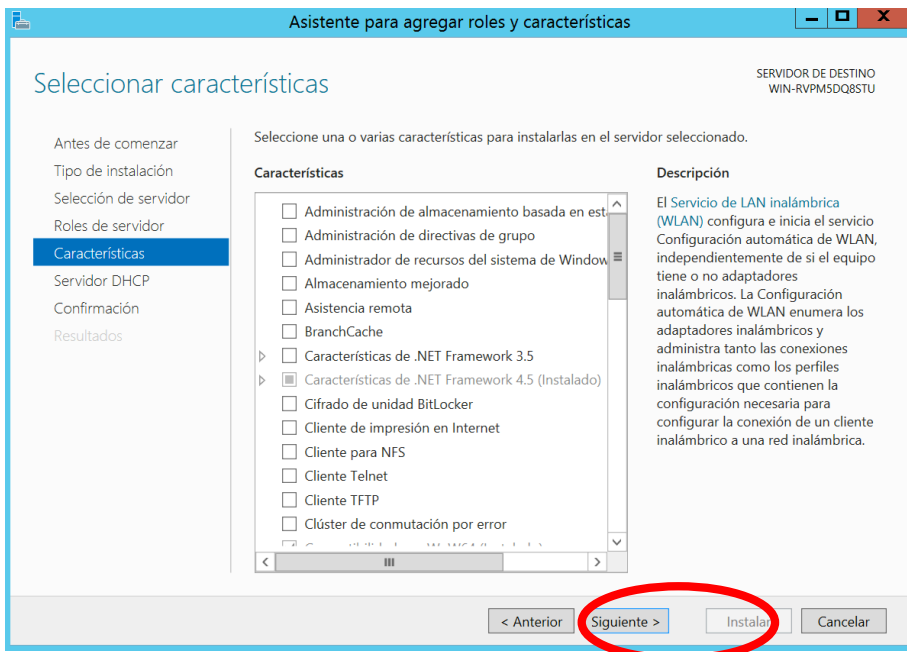


Ilustración 62 - Instalación servicio DNS (paso 6)

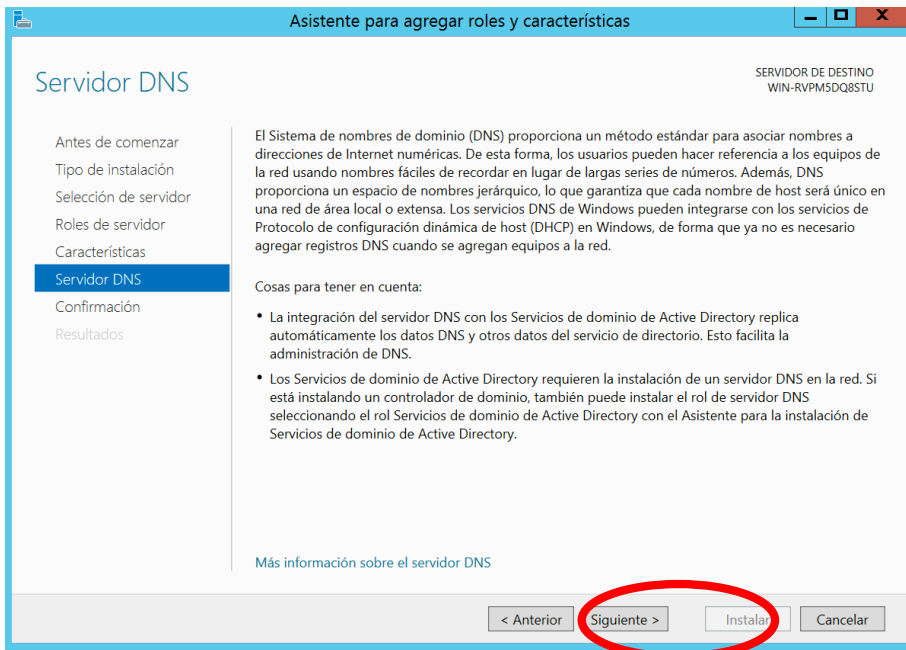


Ilustración 63 - Instalación servicio DNS (paso 7)

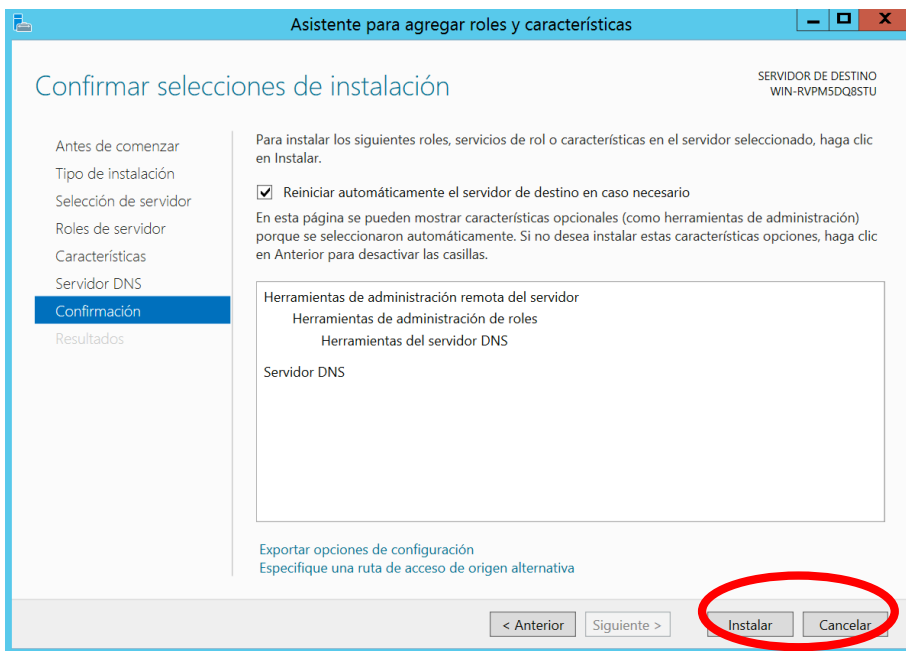


Ilustración 64 - Instalación servicio DNS (paso 8)

5. Una vez finalizada la instalación pulsar en el botón de “Cerrar”.

Configuración.

En el siguiente apartado se muestra como configurar las opciones del rol de DNS. Para que el rol de DNS sea funcional y realice la resolución de nombres hay que configurar una ZONA tanto para búsqueda directa como para búsqueda indirecta.

1. Zona de búsqueda directa.

1.1. Desde el panel “Administrador del servidor” pulsamos en Herramientas - > DNS, para abrir el gestor del servicio DNS:

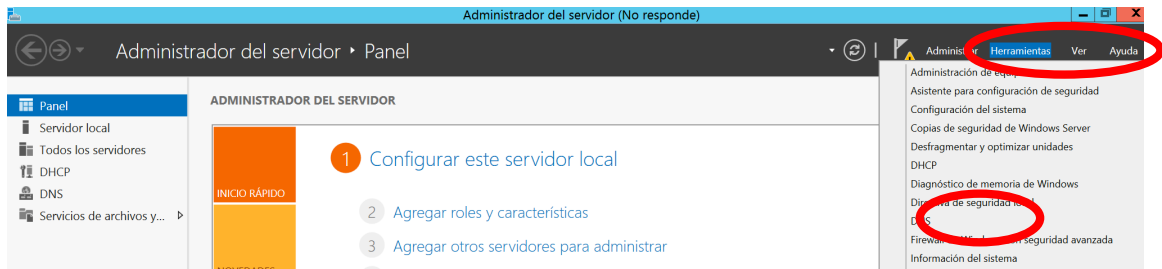


Ilustración 65 - Configuración del servicio DNS (paso 1).

1.2. Vamos a zona de búsqueda directa y pulsamos con el botón derecho. Se mostrara un desplegable donde pulsaremos en “Zona nueva...”:

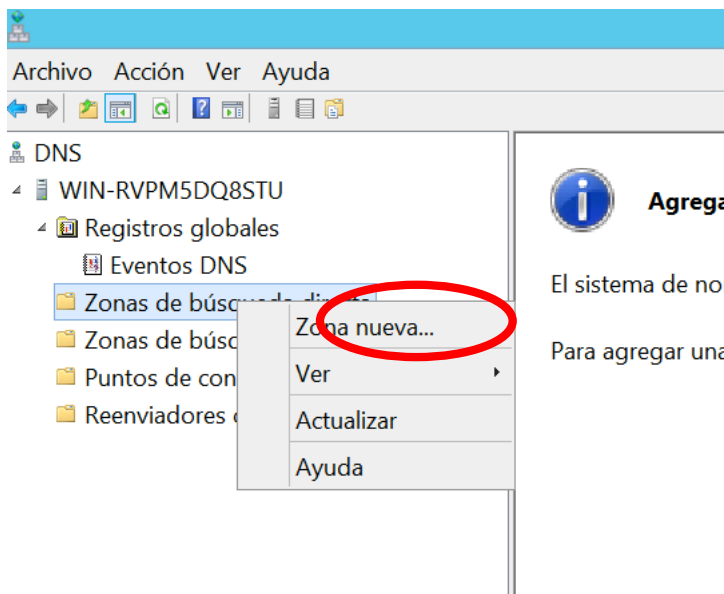


Ilustración 66 - Configuración del servicio DNS (paso 2).

1.3. Se nos abre un asistente y pulsamos en Siguiente:

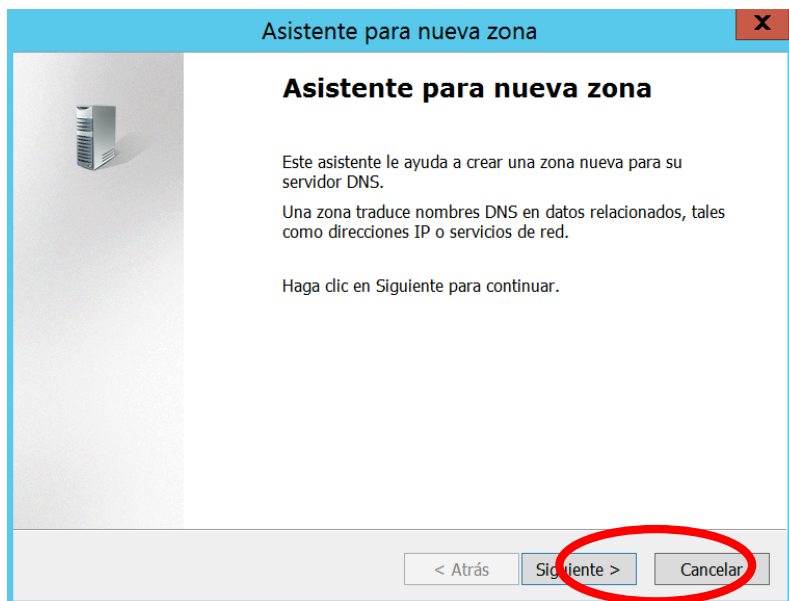


Ilustración 67 - Configuración del servicio DNS (paso 3).

1.4. Elegimos “Zona principal” y pulsamos siguiente:

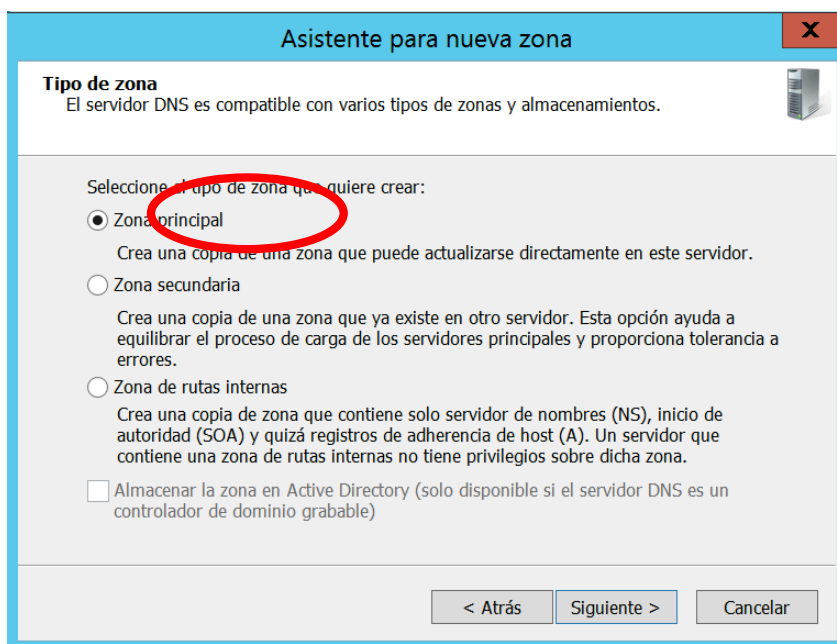


Ilustración 68 - Configuración del servicio DNS (paso 4).

1.5. Asignamos un nombre a la zona y pulsamos en siguiente:

Nombre de zona
¿Qué nombre tiene la zona nueva?

El nombre de zona especifica la parte del espacio de nombres DNS para el que actúa el servidor de autorización. Puede ser el nombre de dominio de la organización (por ejemplo, microsoft.com) o una parte del nombre de dominio (por ejemplo, nuevazona.microsoft.com). El nombre de zona no es el nombre del servidor DNS.

Nombre de zona:
organizacion.com

< Atrás Siguiente > Cancelar

Ilustración 69 - Configuración del servicio DNS (paso 5).

1.6. Dejamos marcado la opción “Crear un archivo nuevo con este nombre de archivo” y pulsamos en siguiente:

Archivo de zona
Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

Crear un archivo nuevo con este nombre de archivo:
organizacion.com.dns

Usar este archivo:
[Empty text box]

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

< Atrás Siguiente > Cancelar

Ilustración 70 - Configuración del servicio DNS (paso 6).

1.7. Dejar la opción por defecto “No admitir actualizaciones dinámicas” y pulsar siguiente:

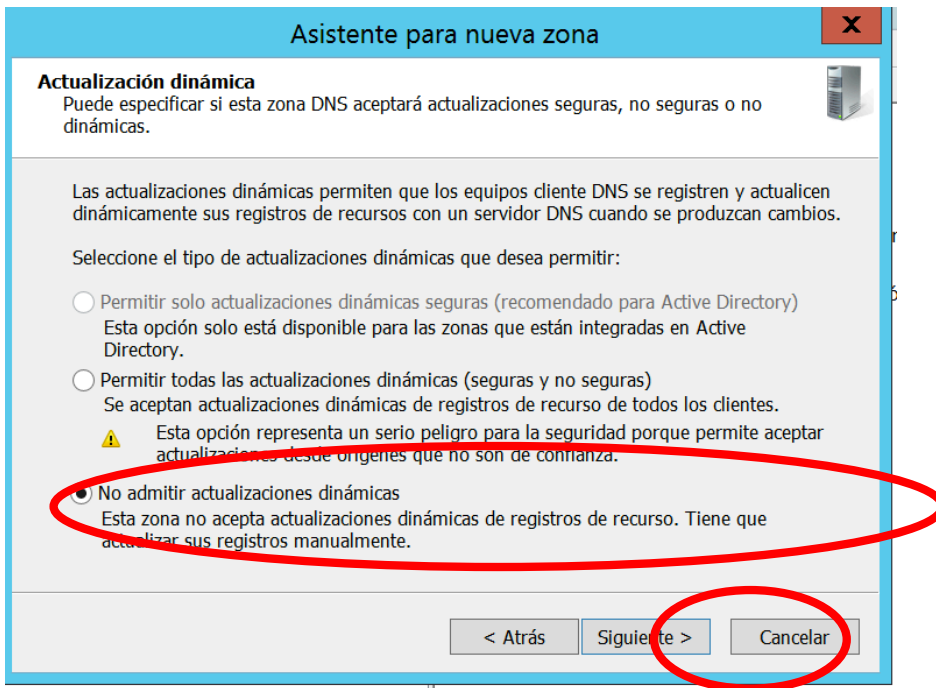


Ilustración 71 - Configuración del servicio DNS (paso 7).

1.8. Pulsar en finalizar.

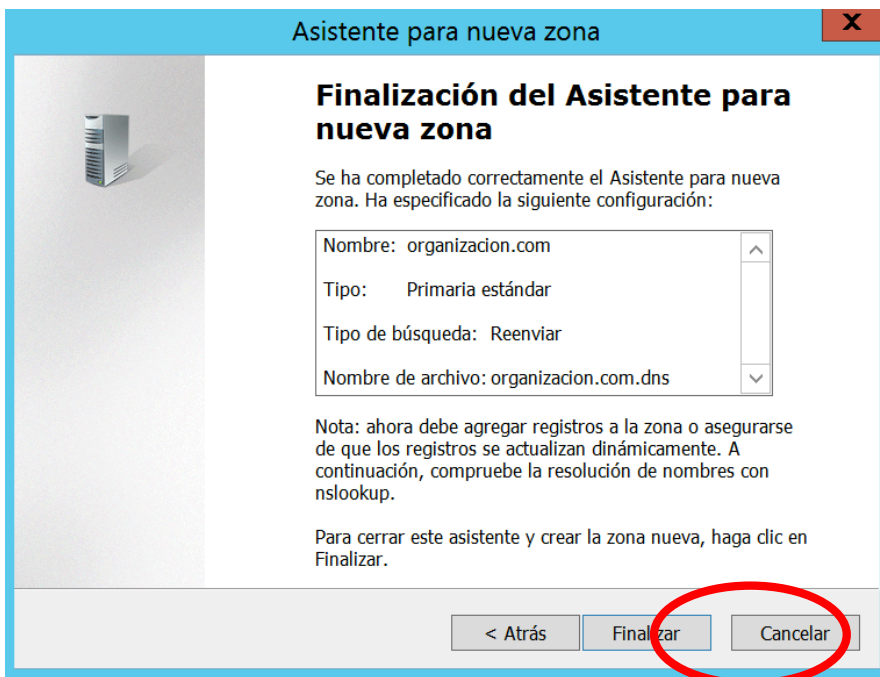


Ilustración 72 - Configuración del servicio DNS (paso 8).

2. Zona de búsqueda indirecta.

2.1. Pulsamos con el botón derecho sobre “Zona de búsqueda indirecta” y en el desplegable pulsamos “Zona nueva...”:

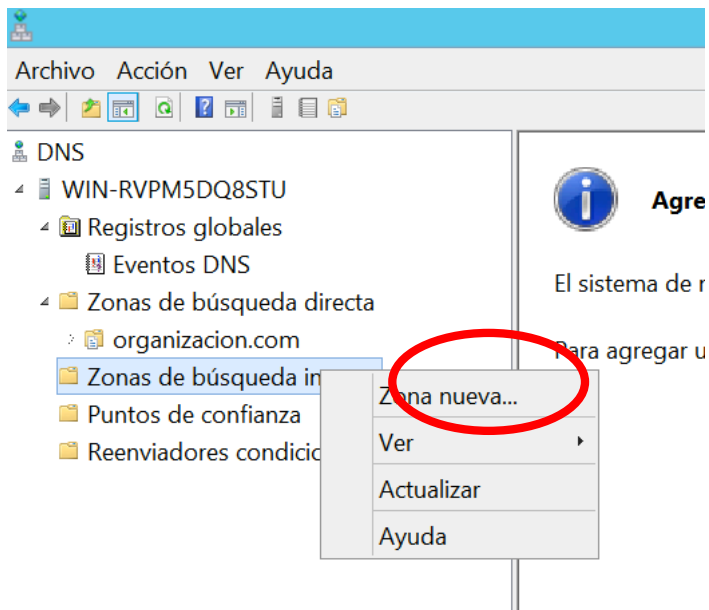


Ilustración 73 - Configuración del servicio DNS (paso 9).

2.2. Se abre un asistente de configuración donde pulsamos en siguiente:

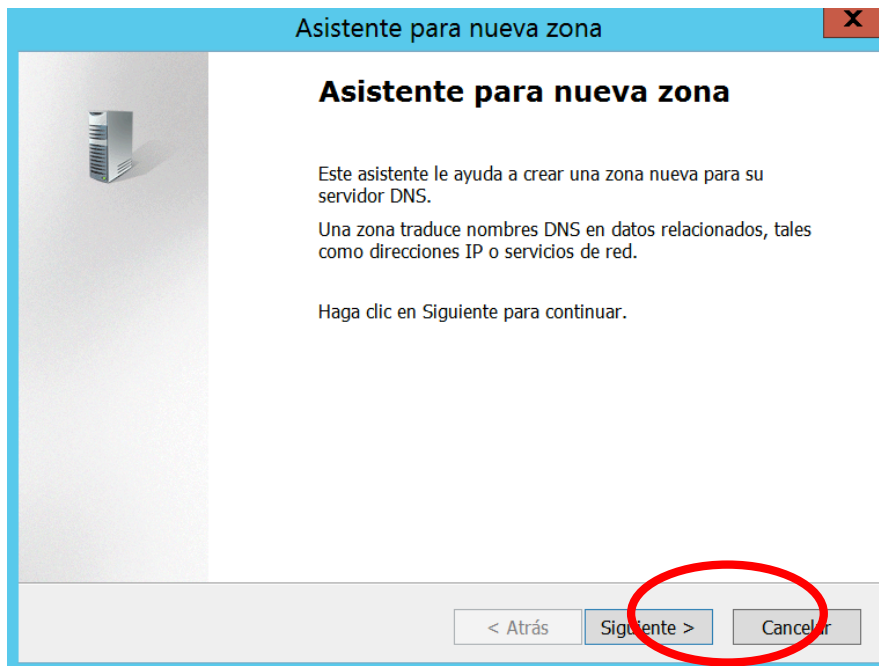


Ilustración 74 - Configuración del servicio DNS (paso 10).

2.3. Elegimos zona principal y pulsamos siguiente:

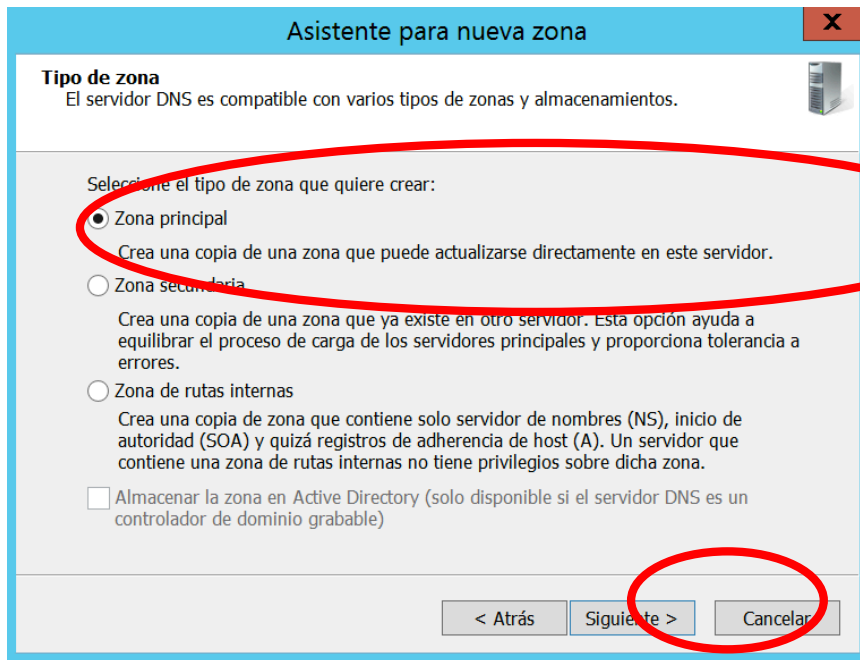


Ilustración 75 - Configuración del servicio DNS (paso 11).

2.4. Elegimos "Zona de búsqueda inversa para IPv4" y pulsamos siguiente:

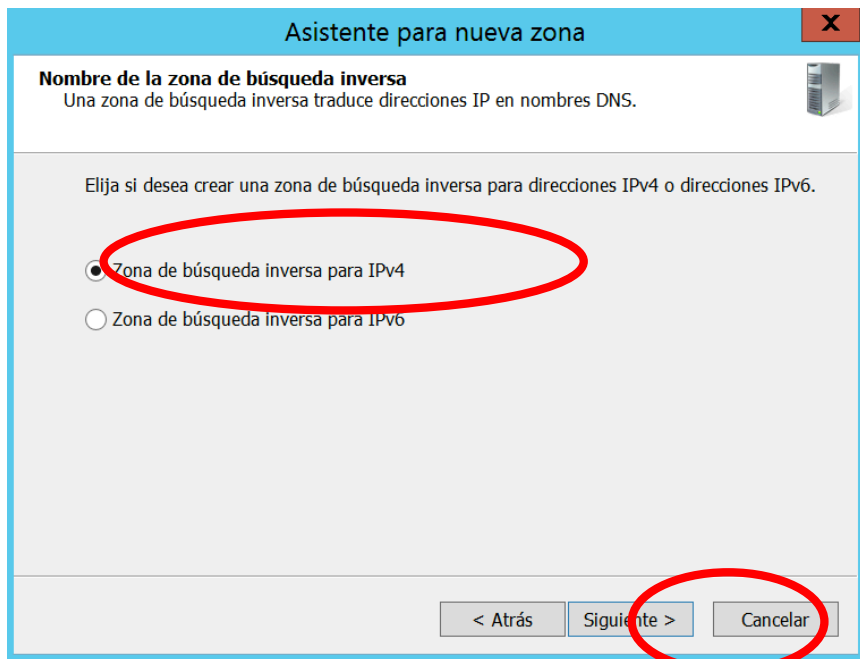


Ilustración 76 - Configuración del servicio DNS (paso 12).

2.5. Introducimos el rango de la Vlan 10: 172.16.10.0 y pulsamos siguiente:

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

Id. de red:
172.16.10

El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.

Nombre de la zona de búsqueda inversa:
10.16.172.in-addr.arpa

< Atrás Siguiente > Cancelar

Ilustración 77 - Configuración del servicio DNS (paso 13).

2.6. Dejamos la opción por defecto y pulsamos siguiente:

Archivo de zona
Puede crear un archivo de zona nuevo o usar un archivo copiado de otro servidor DNS.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro servidor DNS?

Crear un archivo nuevo con este nombre de archivo:
10.16.172.in-addr.arpa.dns

Usar este archivo:

Para usar este archivo existente, asegúrese primero de que se ha copiado en la carpeta %SystemRoot%\system32\dns en este servidor y haga luego clic en Siguiente.

< Atrás Siguiente > Cancelar

Ilustración 78 - Configuración del servicio DNS (paso 14).

2.7. Dejamos marcada la opción “No admitir actualizaciones dinámicas” y pulsamos siguiente:

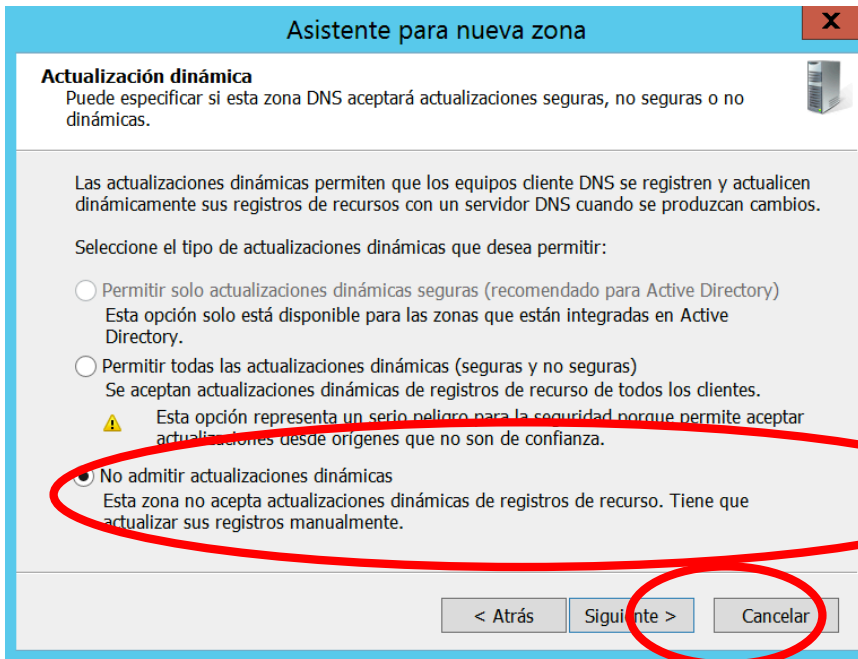


Ilustración 79 - Configuración del servicio DNS (paso 15).

2.8. Finalizamos el asistente:

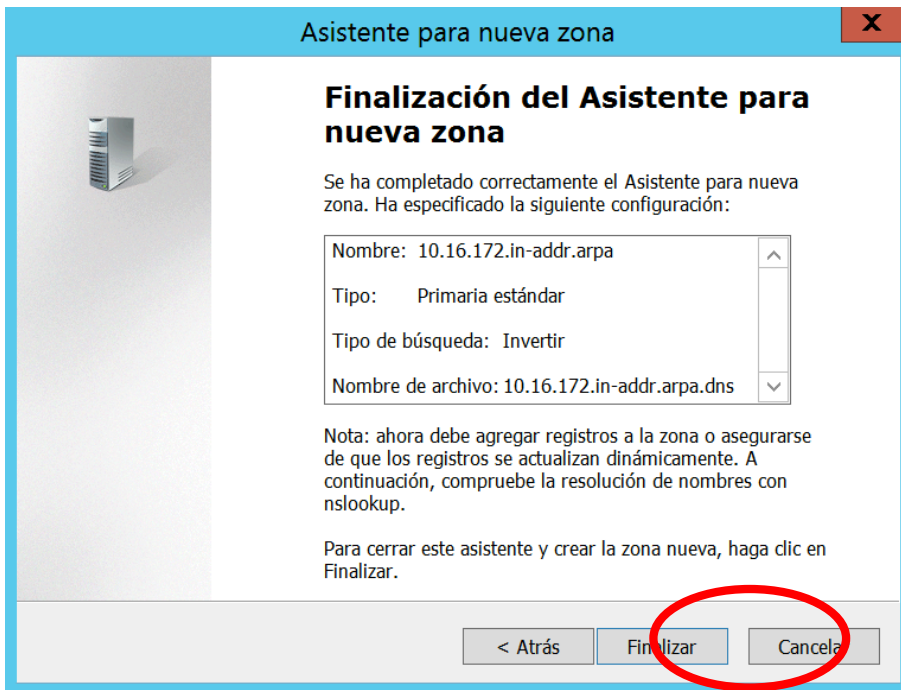


Ilustración 80 - Configuración del servicio DNS (paso 16).

NOTA: repetir estos pasos para configurar la búsqueda inversa en la Vlan 4 y Vlan 9.

Reenviadores.

En este punto vamos a configurar los reenviadores, que hacen la función de resolver los nombre que nuestros servidores DNS no tienen en su base de datos. Se pueden usar servidores DNS de nuestro proveedor de servicios de Internet u otros conocidos como los de Google (4.4.4.4 y 8.8.8.8).

1. Pulsamos con el botón derecho sobre el nombre del servidor DNS y en el desplegable pulsamos en propiedades:

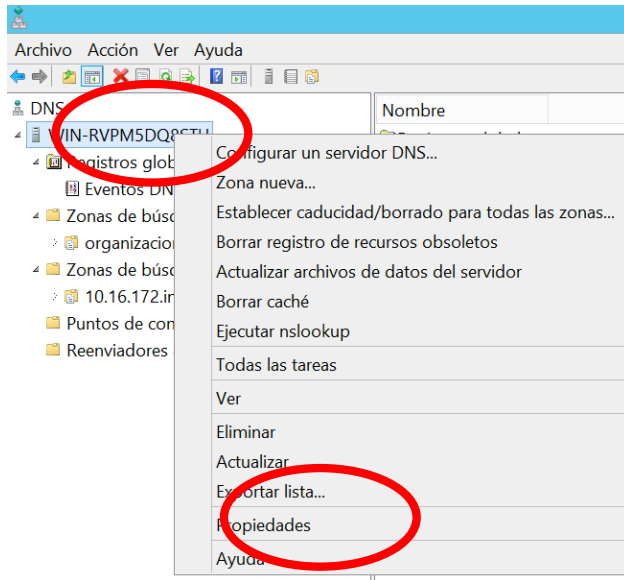


Ilustración 81 - Configuración de reenviadores en servicio DNS (paso 1).

2. Pulsamos sobre la pestaña de Reenviadores:

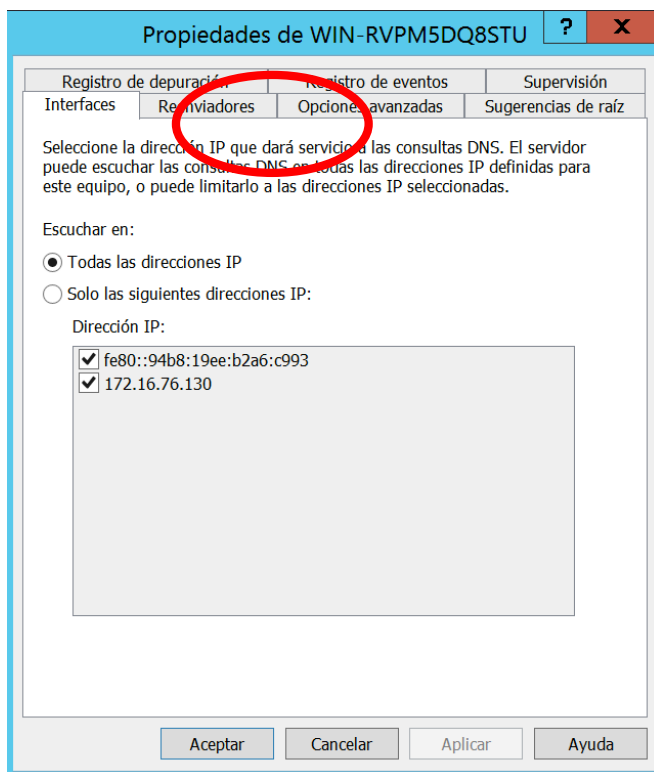


Ilustración 82 - Configuración de reenviadores en servicio DNS (paso 2).

3. Pulsamos sobre editar:

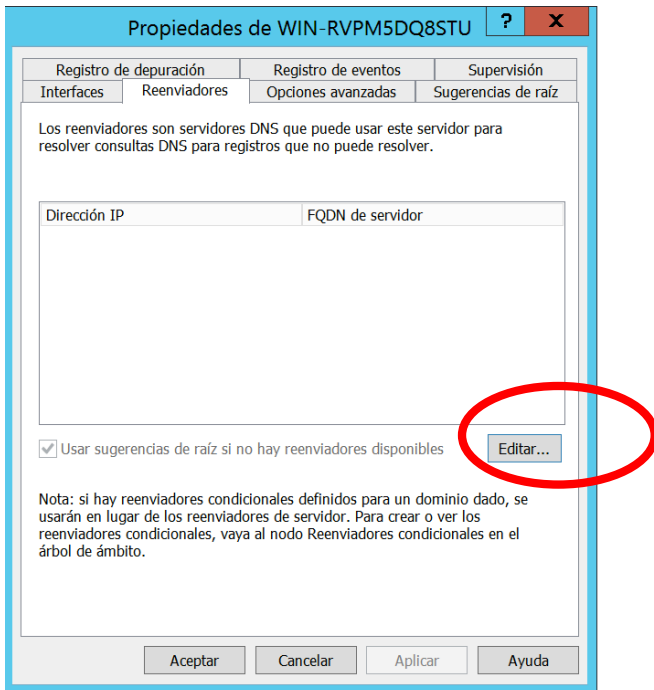


Ilustración 83 - Configuración de reenviadores en servicio DNS (paso 3).

4. Introducimos como DNS las IPs 8.8.8.8 y 4.4.4.4 y pulsamos en aceptar:

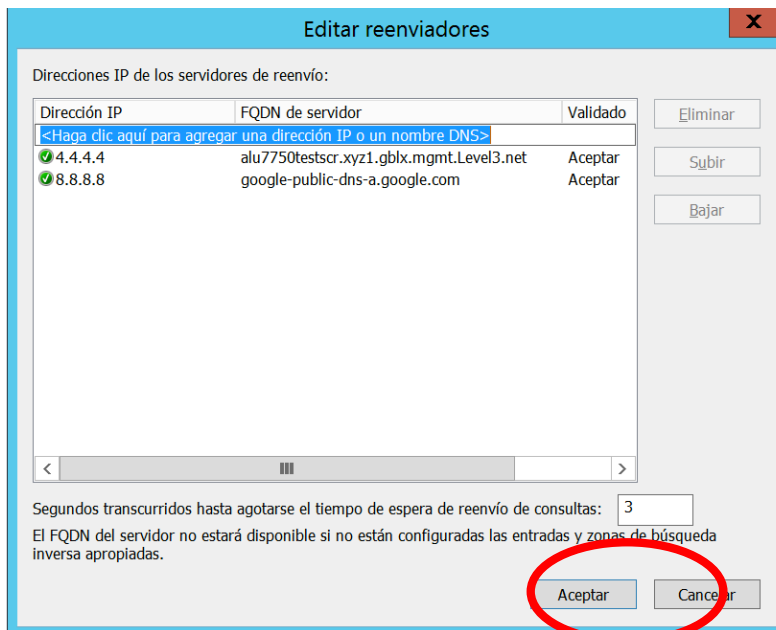


Ilustración 84 - Configuración de reenviadores en servicio DNS (paso 4).

5. Aplicamos los cambios.

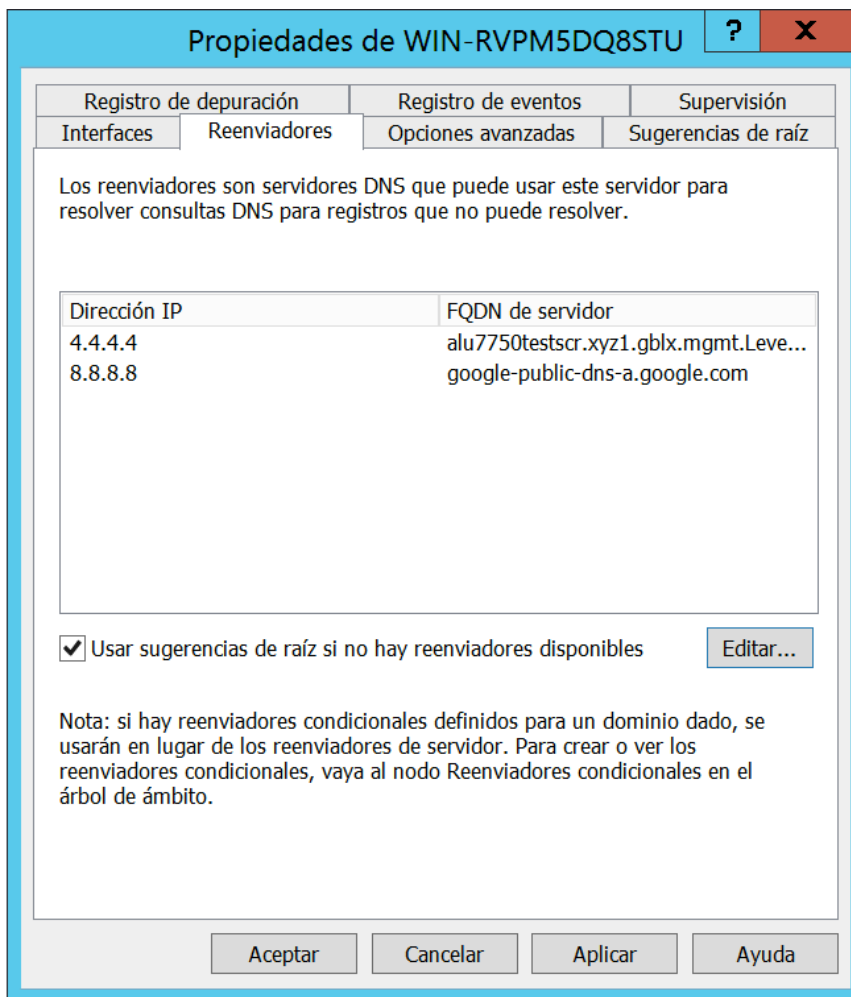


Ilustración 85- Configuración de reenviadores en servicio DNS (paso 5).

Anexo I: Instalación y configuración de PfSense

Instalación

1. Descargamos la imagen ISO del portal web de PfSense:

<https://www.pfsense.org/download/>

2. Elegimos la arquitectura del computador y elegimos “CD image (ISO) with Installer”:

Download Full Install

Need to [update an existing installation](#) instead?

Which Image Do I Need?

Computer Architecture:

NOTE: If your system has a 64 bit capable Intel or AMD CPU, use the 64 bit version. *32 bit should only be used with 32 bit CPUs.*

Platform:

Or [just show me the mirrors](#) so I can choose which file to download on my own.

Click on a mirror location (second column) to **download the appropriate image** for the installation information you've selected above.

Ilustración 86 - Descarga de PfSense

NOTA: En nuestro caso vamos a instalar pfSense sobre una maquina virtual con dos interfaces de red, una para la WAN y otra para la LAN.

3. Montamos la imagen ISO en la máquina virtual para que arranque desde este y comenzar la instalación.
4. Elegimos la opción 1 para iniciar la instalación:



Ilustración 87 - Instalación PfSense (Paso 1)

5. Comenzará el asistente de instalación. En la primera opción elegimos “Accept these Settings”:

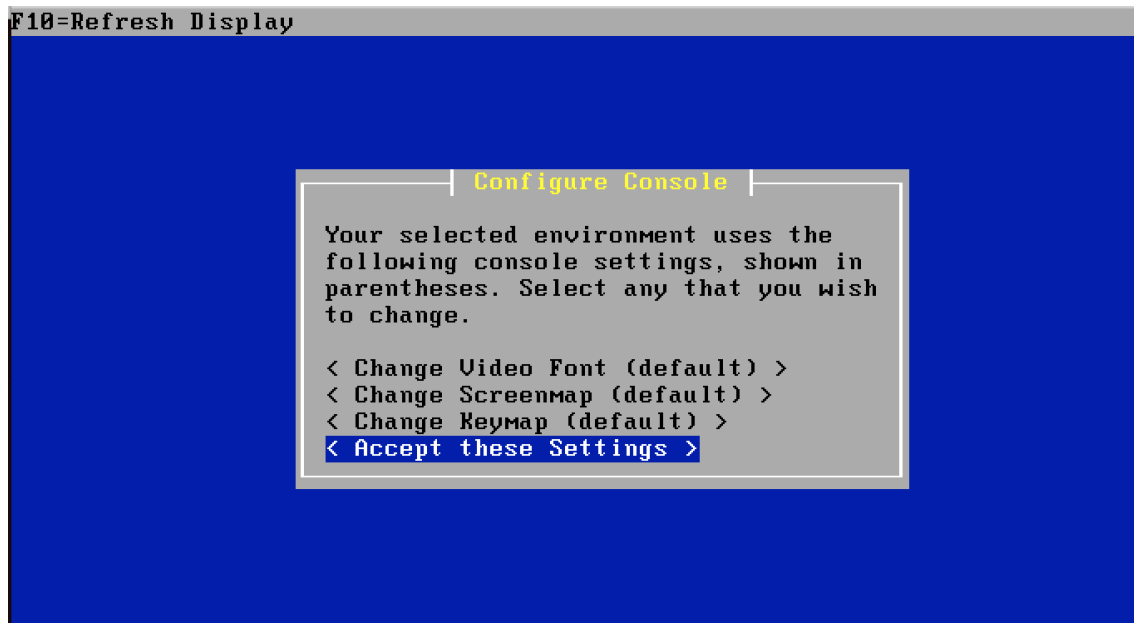


Ilustración 88 - Instalación PfSense (Paso 2)

6. Después elegimos “Quick/Easy Install”:

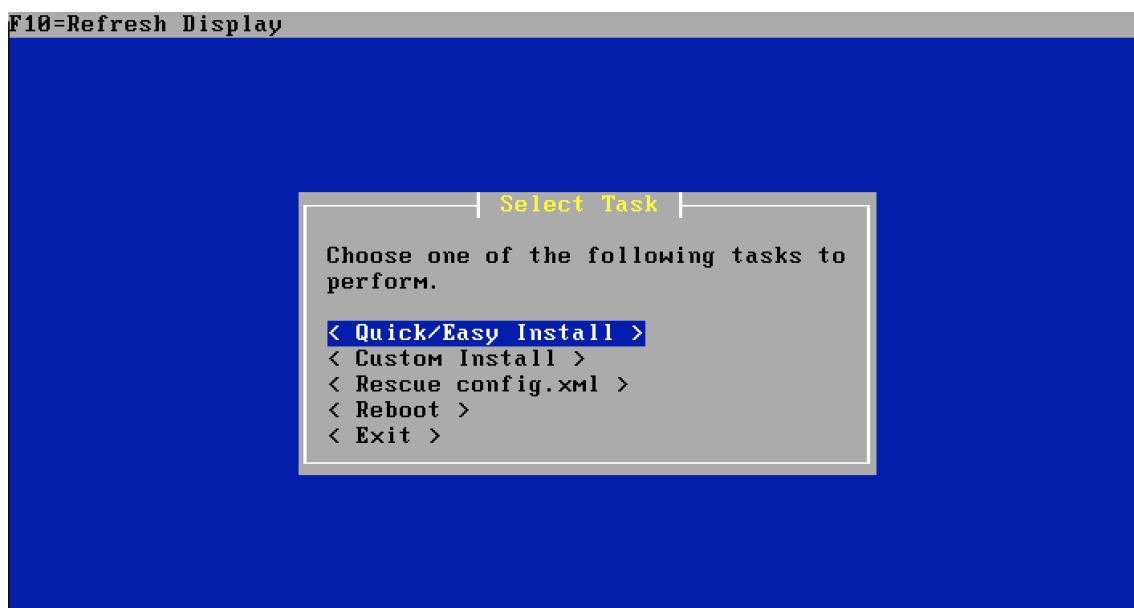


Ilustración 89 - Instalación PfSense (Paso 3)

7. A continuación pulsamos OK para confirmar las opciones elegidas:

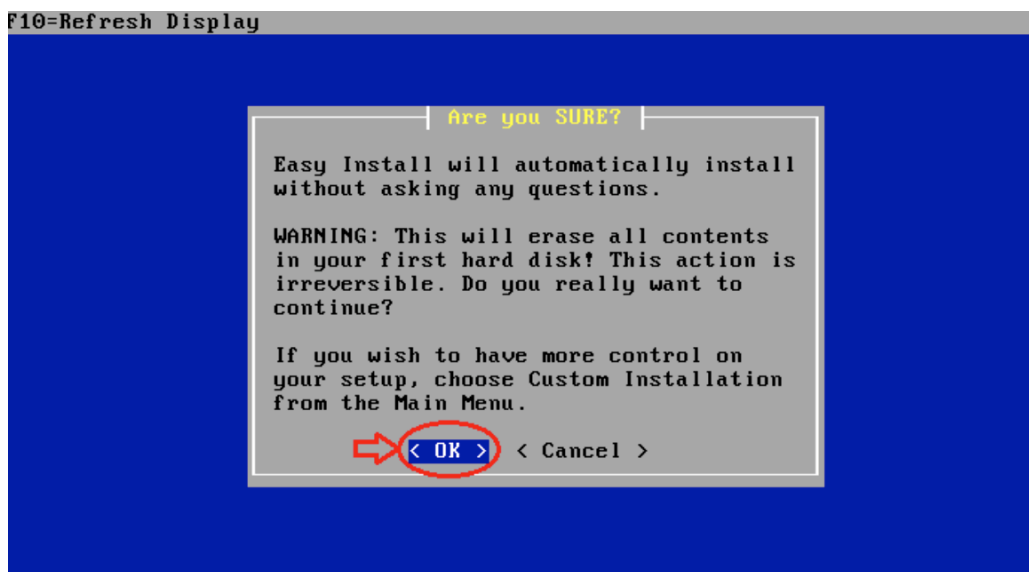


Ilustración 90 - Instalación PfSense (Paso 4)

8. Después, elegimos "Standard Kernel" para comenzar la instalación:

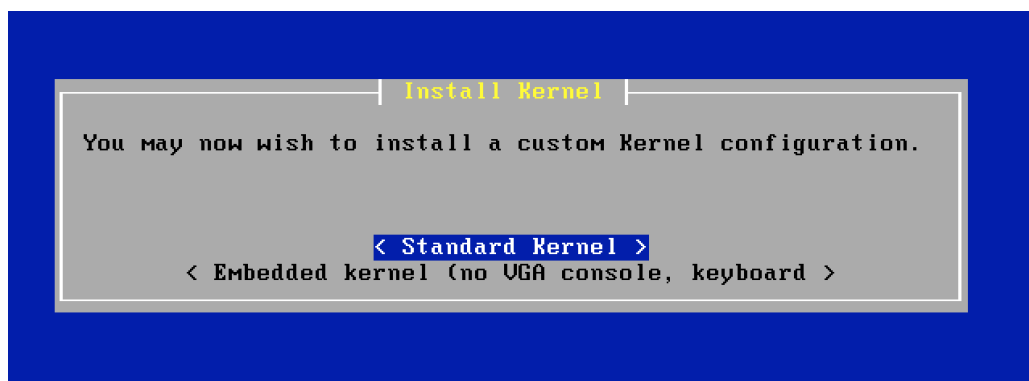


Ilustración 91 - Instalación PfSense (Paso 5)

9. Por último, cuando termine la instalación reiniciar marcando "Reboot". Antes desconectar la imagen ISO para que tras el reinicio inicie ya PfSense instalado:

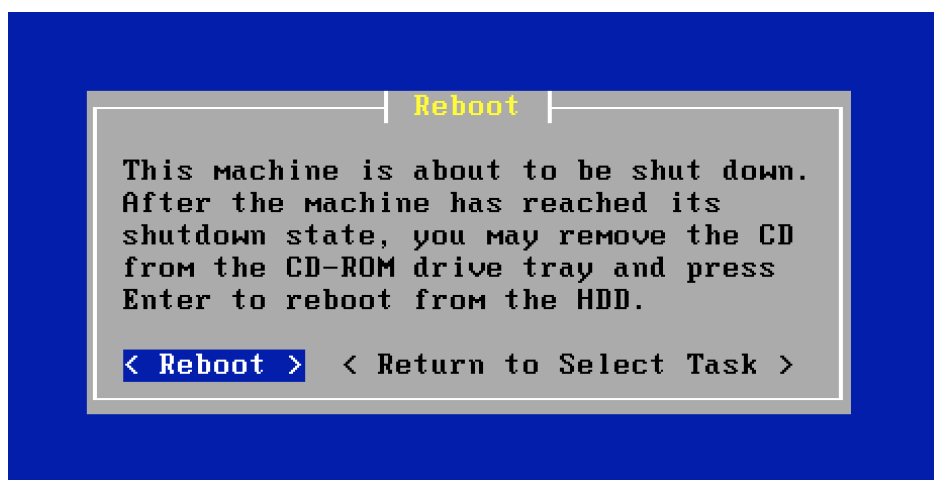


Ilustración 92 - Instalación PfSense (Paso 6)

Configuración

Para poder realizar las pruebas necesarias se monta sobre un escenario con máquinas virtuales como el siguiente:

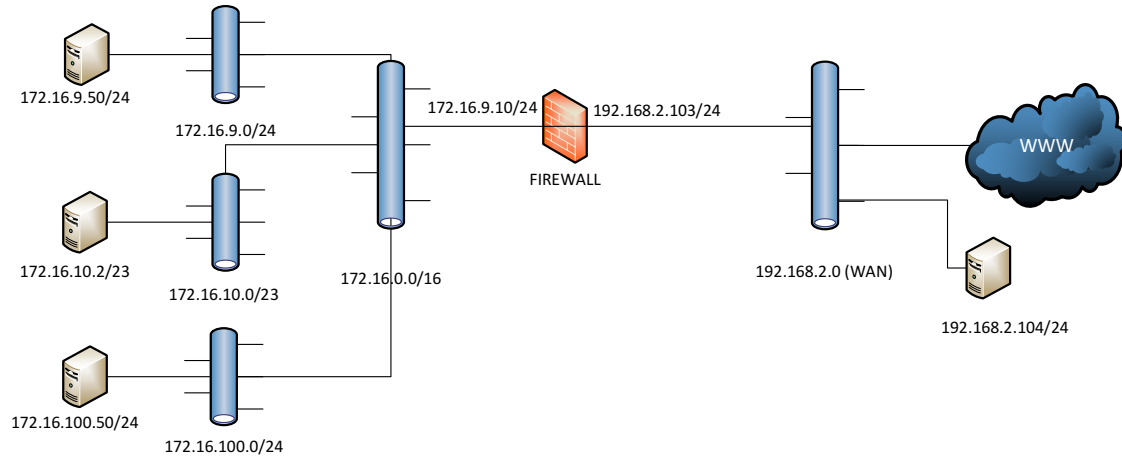


Ilustración 93 - Ubicación del cortafuegos

- PfSense (firewall):
 - WAN: 192.168.2.103
 - LAN: 172.16.9.10
- PC en la WAN: 192.168.2.104
- Servidor en VLAN 9 (servidores): 172.16.9.50
- PC en VLAN 10 (usuarios): 172.16.10.2
- Servidor en DMZ: 172.16.100.50

Llegados a este punto, post instalación, vamos a configurar las IPs de las interfaces de red de PfSense (WAN y LAN).

1. Tras arrancar PfSense tras la instalación, aparecen las siguientes opciones de la imagen. Pulsamos 1 para asignar las interfaces:

```
generating ARD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3-RELEASE amd64 Mon Apr 11 18:10:34 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.104/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Ilustración 94 - Configuración PfSense (Paso 1)

2. Asignamos “em0” a la WAN y “em1” a la LAN:

```
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Warning: Configuration references interfaces that do not exist: em3

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

em0   00:0c:29:b9:f3:11   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em1   00:0c:29:b9:f3:1b   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em2   00:0c:29:b9:f3:25   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]? n

If you do not know the names of the interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0^[IJ█
```

Ilustración 95 - Configuración PfSense (Paso 2)

```

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

em0    00:0c:29:b9:f3:11    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em1    00:0c:29:b9:f3:1b    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em2    00:0c:29:b9:f3:25    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]? n

If you do not know the names of the interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1^[[J

```

Ilustración 96 - Configuración PfSense (Paso 3)

```

em0    00:0c:29:b9:f3:11    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em1    00:0c:29:b9:f3:1b    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em2    00:0c:29:b9:f3:25    (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]? n

If you do not know the names of the interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2^[[J^[[J

```

Ilustración 97 - Configuración PfSense (Paso 4)

3. Confirmamos los cambios:

5. Después de asignar las interfaces, la WAN ya tiene asignada una IP por el DHCP y nos queda asignar un IP para la LAN. Para ello elegimos la opción 2:

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.104/24
LAN (lan)     -> em1      ->
OPT1 (opt1)   -> em2      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2^[[J

```

Ilustración 100 - Configuración PfSense (Paso 7)

6. Asignamos la IP 172.16.9.10. Elegimos NO activar el servicio DHCP:

```

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.9.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n^[[J

```

Ilustración 101 - Configuración PfSense (Paso 8)

7. Llegados a este punto ya está activado el servicio web para acceder a configurar las reglas y otros aspectos del firewall PfSense:

```
The IPv4 LAN address has been set to 172.16.9.10/16
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://172.16.9.10/

Press <ENTER> to continue.
*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.104/24
LAN (lan)      -> em1      -> v4: 172.16.9.10/16
OPT1 (opt1)    -> em2      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: ^[[J^[[J
```

Ilustración 102 - Configuración PfSense (Paso 9)

8. Accedemos via web a través del PC que tenemos conectado a la Vlan 10, al cual le hemos configurado la siguiente IPs:
- Dirección IP: 172.16.10.2
 - Mascara: 255.255.254.0
 - Puerta de enlace: 172.16.9.10
 - DNS: 8.8.8.8
9. Tecleamos la IP de la LAN del firewall en el navegador Web: <http://172.16.9.10>. Usuario y contraseña por defecto:
- Usuario: admin
 - Contraseña: pfsense

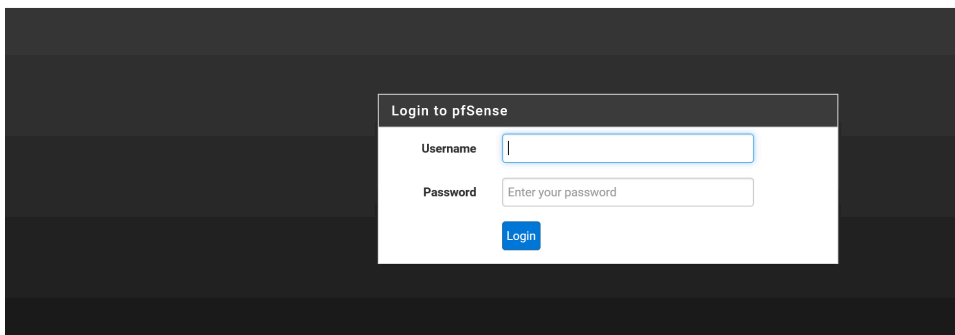


Ilustración 103 - Configuración PfSense (Paso 10)

10. Se abre un asistente de configuración previa. Pulsamos NEXT:

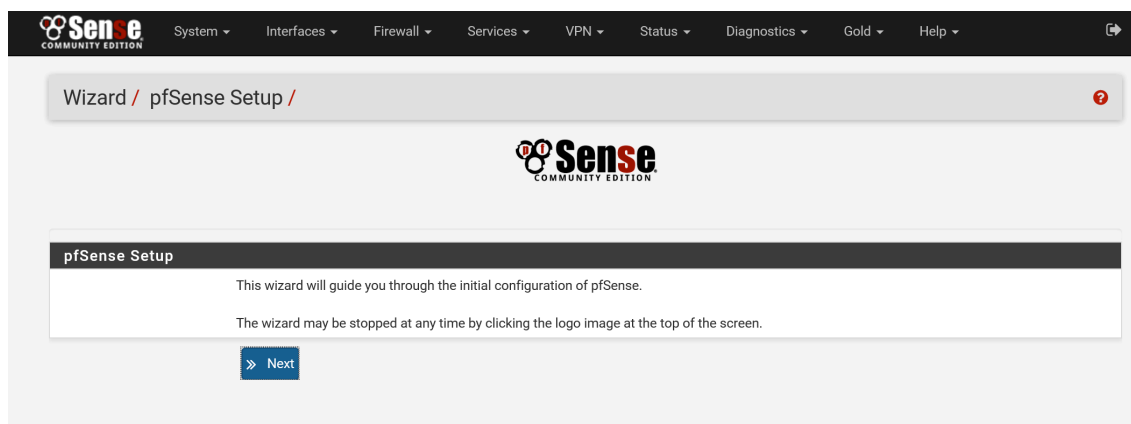


Ilustración 104 - Configuración PfSense (Paso 11)

11. Volvemos a pulsar NEXT:

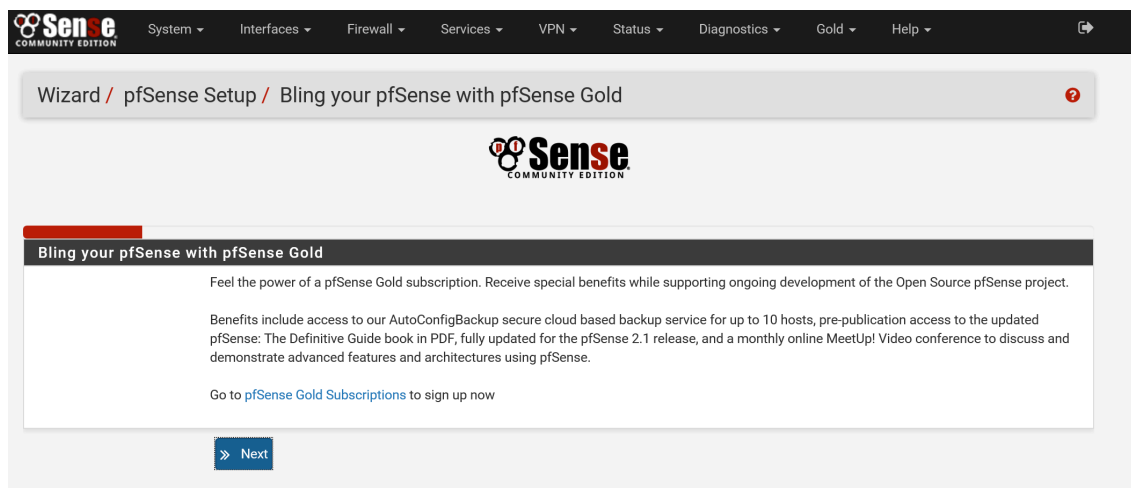
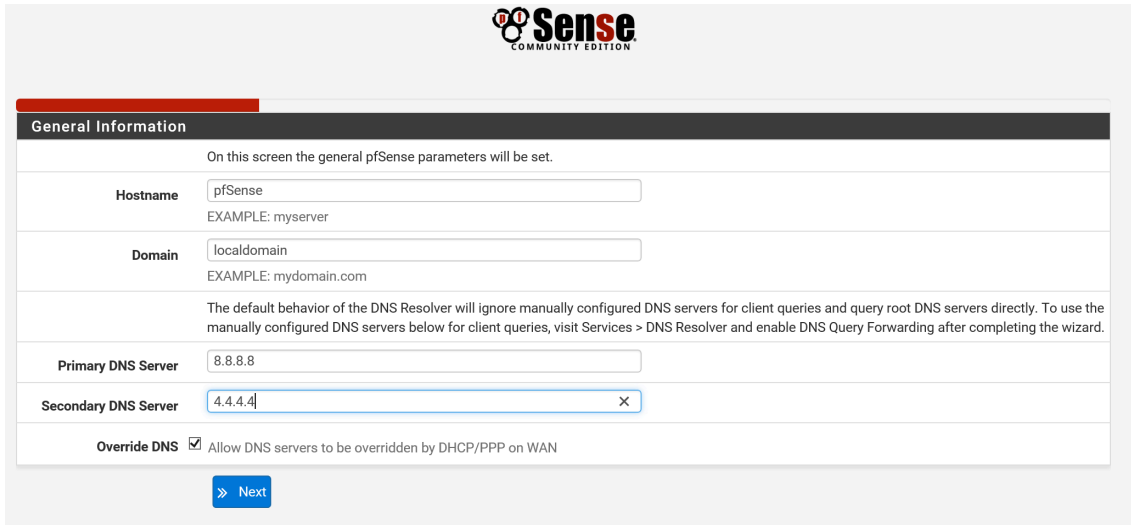


Ilustración 105 - Configuración PfSense (Paso 12)

12. Le asignamos un nombre host y unos DNS. En nuestro caso, para las pruebas, utilizamos unos públicos. Después pulsamos NEXT:



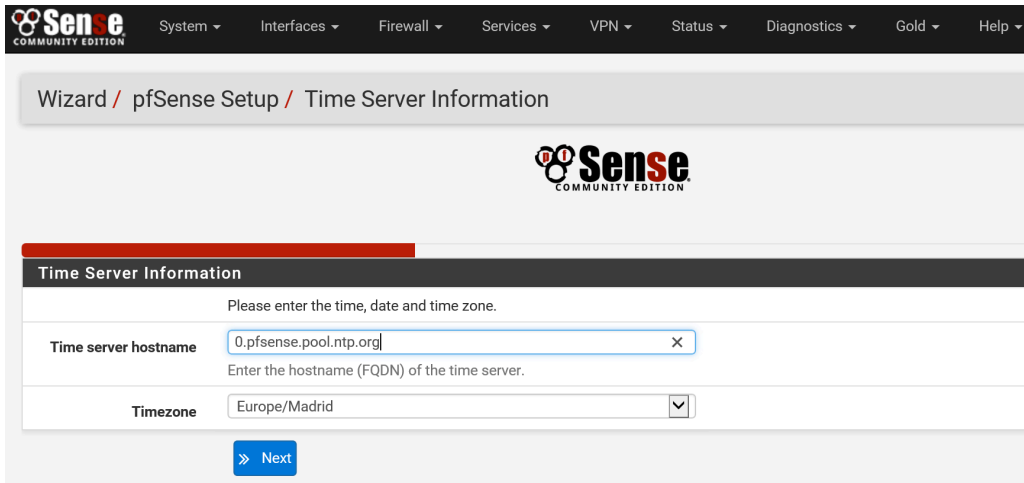
The screenshot shows the 'General Information' configuration page in pfSense. At the top, there is a red progress bar and the pfSense logo. Below the title, a message states: 'On this screen the general pfSense parameters will be set.' The form contains the following fields:

- Hostname:** A text input field containing 'pfSense'. Below it, the text 'EXAMPLE: myserver' is displayed.
- Domain:** A text input field containing 'localdomain'. Below it, the text 'EXAMPLE: mydomain.com' is displayed.
- Primary DNS Server:** A text input field containing '8.8.8.8'.
- Secondary DNS Server:** A text input field containing '4.4.4.4' with a clear button (X) on the right.
- Override DNS:** A checkbox that is checked, with the label 'Allow DNS servers to be overridden by DHCP/PPP on WAN'.

At the bottom of the form, there is a blue button with a right-pointing arrow and the text 'Next'.

Ilustración 106 - Configuración PfSense (Paso 13)

13. Elegimos el Timezone y pulsamos NEXT:



The screenshot shows the 'Time Server Information' configuration page in pfSense. At the top, there is a dark navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. Below the navigation bar, a breadcrumb trail reads 'Wizard / pfSense Setup / Time Server Information'. The main content area features the pfSense logo and a red progress bar. Below the title, a message states: 'Please enter the time, date and time zone.' The form contains the following fields:

- Time server hostname:** A text input field containing '0.pfsense.pool.ntp.org' with a clear button (X) on the right. Below it, the text 'Enter the hostname (FQDN) of the time server.' is displayed.
- Timezone:** A dropdown menu with 'Europe/Madrid' selected.

At the bottom of the form, there is a blue button with a right-pointing arrow and the text 'Next'.

Ilustración 107 - Configuración PfSense (Paso 14)

14. Dejamos la opción DHCP para la WAN y pulsamos NEXT:

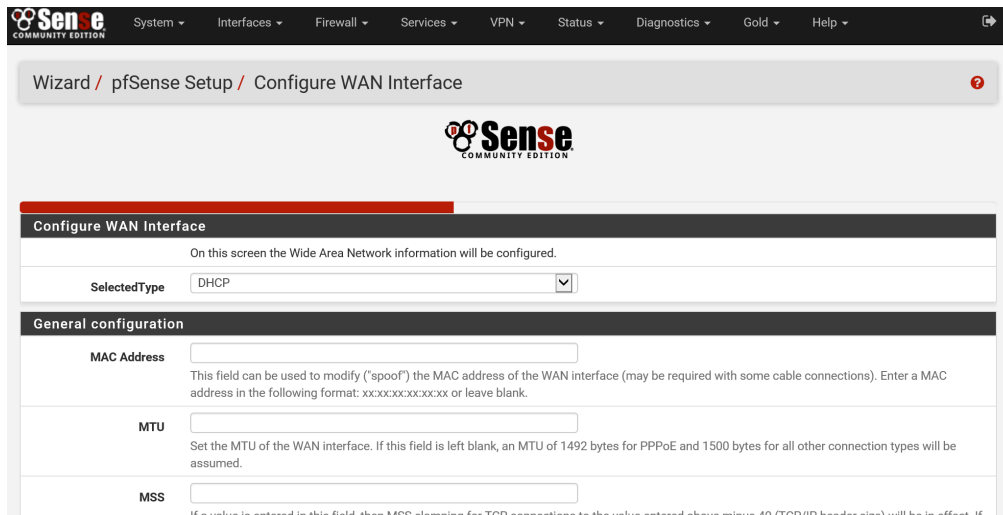


Ilustración 108 - Configuración PfSense (Paso 15)

15. Para la LAN dejamos la configuración que ya hemos realizado anteriormente y pulsamos NEXT:

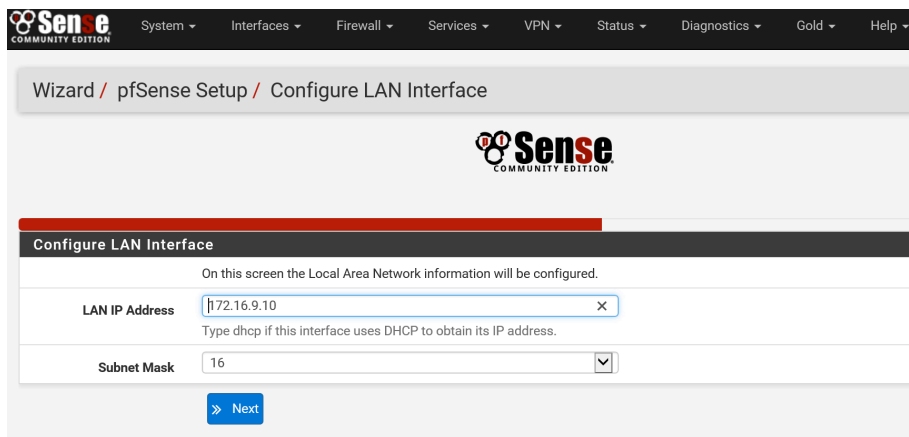


Ilustración 109 - Configuración PfSense (Paso 16)

16. Introducimos un contraseña nueva y pulsamos NEXT:

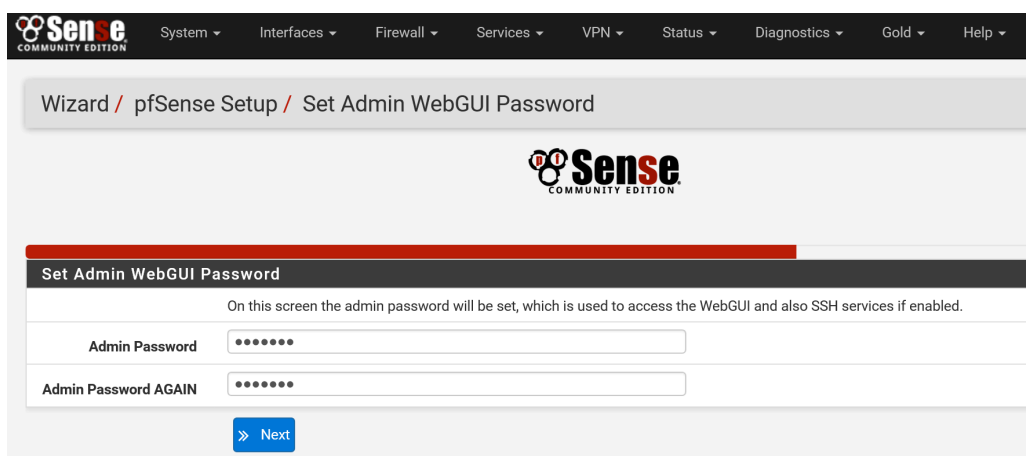


Ilustración 110 - Configuración PfSense (Paso 17)

17. Finalizamos el asistente con RELOAD:

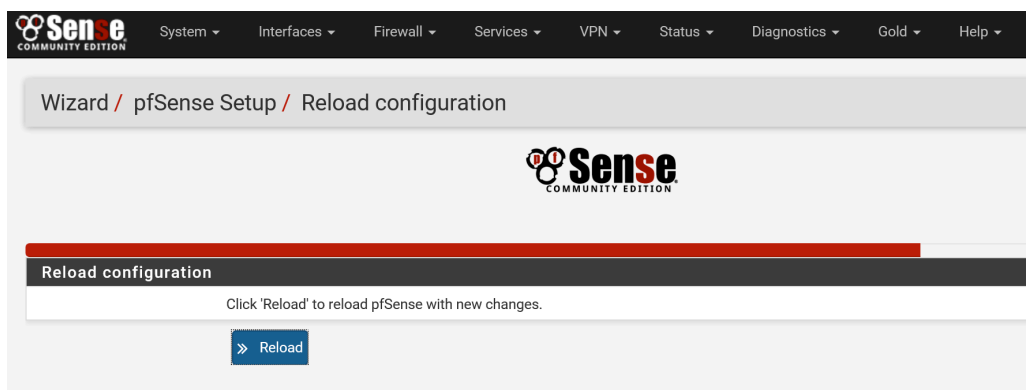


Ilustración 111 - Configuración PfSense (Paso 18)

18. PfSense dispone de la opción de crear ALIAS que nos resulten más familiares a la hora de crear reglas. En nuestro caso hemos creado uno por cada VLAN de nuestra red empresarial, tal y como se muestra en la imagen. Para acceder vamos a Firewall->Alias->IP:

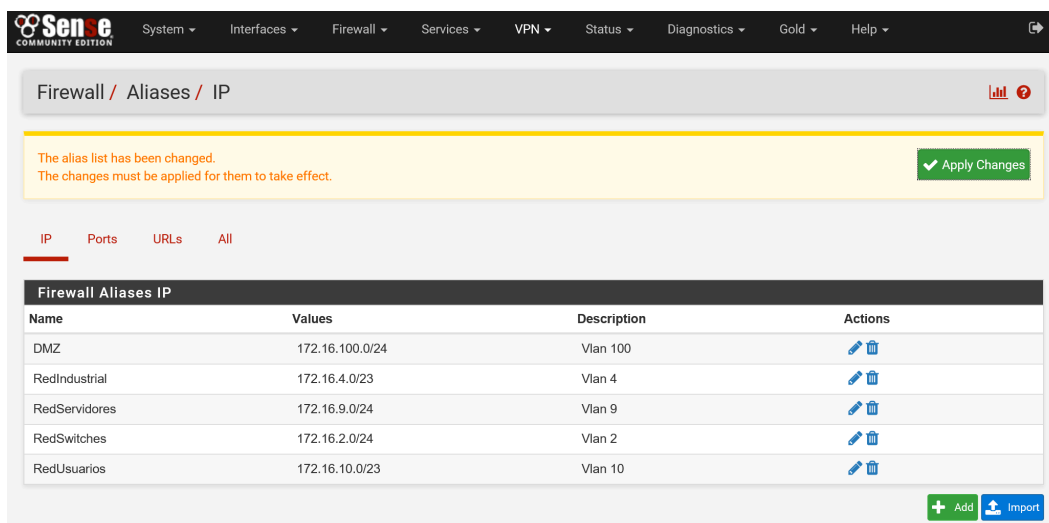


Ilustración 112 - Configuración PfSense (Paso 19)

19. Hacemos lo mismo para puertos, en nuestro caso hemos creado unos para el acceso Web, que engloba los puertos 80 y 443. Para ello vamos a Firewall->Alias->Ports:

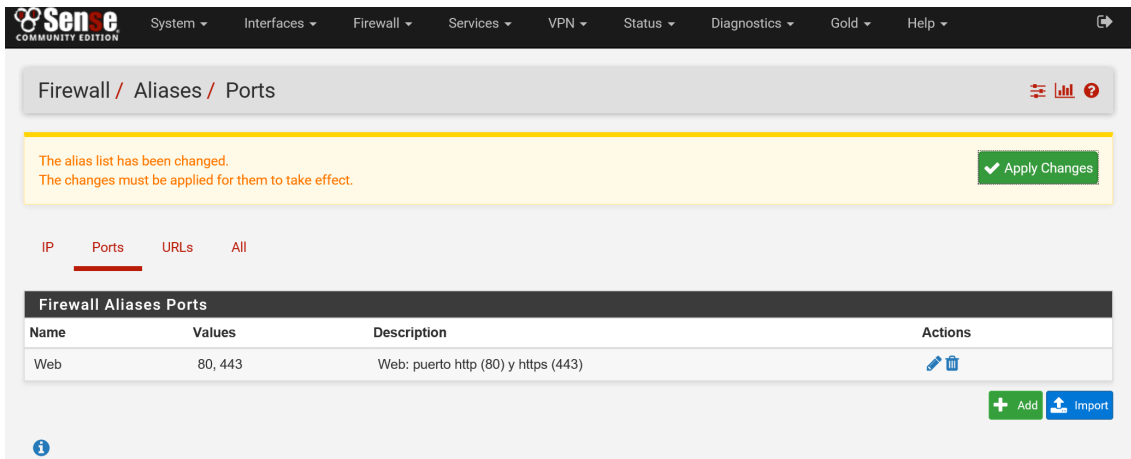


Ilustración 113 - Configuración PfSense (Paso 20)

Cabe destacar que en este apartado también se pueden configurar URLs para posteriormente permitir o denegar el acceso a dichas direcciones web.

20. Ahora vamos a configurar las reglas de acceso a nuestra red desde el exterior. Por defecto, PfSense viene con el acceso cortado desde el exterior. Aplicamos una regla para permitir el acceso a nuestra red DMZ desde el exterior a los puertos WEB (80 y 443) de nuestro servidor web 172.16.100.50.

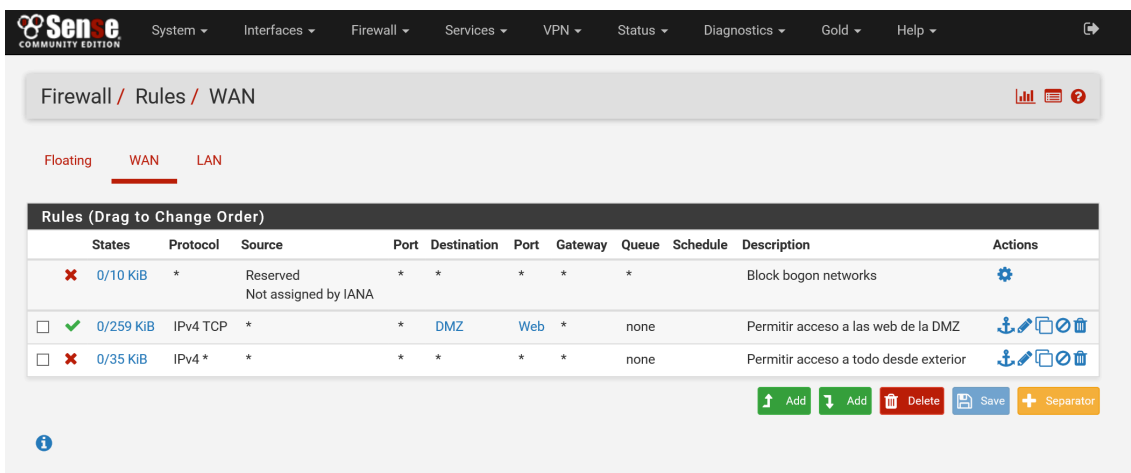


Ilustración 114 - Configuración PfSense (Paso 21)

Evidentemente, en este punto se pueden aplicar multitud de reglas de acceso a nuestra LAN para diferentes servicios como Escritorio Remoto, SSH, etc.

21. Por último, vamos a configurar la salida de los equipos de nuestra LAN hacia el exterior, que van a ser las siguientes:

- Permitir conexiones WEB a los servidores de la DMZ.
- Permitir conexiones desde servidores de la DMZ al servidor de base de datos de la red de servidores con IP 172.16.9.50.
- Denegar el resto de conexiones desde la DMZ hacia el resto de equipos de la LAN.

- Denegar el resto de conexiones desde la LAN a la DMZ.
- Denegar el resto de conexiones desde la DMZ hacia el exterior (WAN/Internet).
- Denegar las conexiones hacia el exterior (WAN/Internet) de la red de switches.
- Denegar las conexiones hacia el exterior (WAN/Internet) de la red industrial.
- Denegar las conexiones hacia el exterior (WAN/Internet) de la red de servidores.
- Permitir el resto de conexiones al exterior. En nuestro caso, solo se permite acceso al exterior (WAN/Internet) a la red de usuarios.

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/6.98 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	⚙️
<input type="checkbox"/> ✓ 0/254 KIB	IPv4 TCP	*	*	DMZ	Web	*	none	*	Permitir conexiones Web a la DMZ	📌🔗🗑️
<input type="checkbox"/> ✓ 0/960 B	IPv4 *	DMZ	*	172.16.9.50	*	*	none	*	Permitir conexiones de la DMZ a servidor BBDD	📌🔗🗑️
<input type="checkbox"/> ✗ 0/40 KIB	IPv4 *	DMZ	*	LAN net	*	*	none	*	Aislar DMZ hacia LAN	📌🔗🗑️
<input type="checkbox"/> ✗ 0/626 B	IPv4 *	LAN net	*	DMZ	*	*	none	*	Aislar DMZ desde LAN	📌🔗🗑️
<input type="checkbox"/> ✗ 0/105 KIB	IPv4 *	DMZ	*	! LAN net	*	*	none	*	Aislar DMZ del exterior	📌🔗🗑️
<input type="checkbox"/> ✗ 0/0 B	IPv4 *	RedSwitches	*	! LAN net	*	*	none	*	Aislar Vlan 2 del exterior	📌🔗🗑️
<input type="checkbox"/> ✗ 0/0 B	IPv4 *	RedIndustrial	*	! LAN net	*	*	none	*	Aislar Vlan 4 del exterior	📌🔗🗑️
<input type="checkbox"/> ✗ 0/106 KIB	IPv4 *	RedServidores	*	! LAN net	*	*	none	*	Aislar Vlan 9 del exterior	📌🔗🗑️
<input type="checkbox"/> ✓ 9/104.13 MiB	IPv4 *	LAN net	*	*	*	*	none	*	Default allow LAN to any rule	📌🔗🗑️
<input type="checkbox"/> ✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none	*	Default allow LAN IPv6 to any rule	📌🔗🗑️

⬆️ Add ⬇️ Add 🗑️ Delete 💾 Save ➕ Separator

Ilustración 115 - Configuración PfSense (Paso 22)

Como se comentó anteriormente PfSense dispone de multitud de opciones interesantes que se quedan fuera de este proyecto, pero que son interesantes como configurar un proxy transparente Squid en el propio firewall, utilizarlo de router o servidor DHCP.

Anexo J: Ficheros de configuración de switches y routers Cisco

```
ca-core (172.16.2.1)_running-config
```

```
!
```

```
version 12.2
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname ca-core
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
ip routing
```

```
!
```

```
!
```

```
!
```

```
!
```

```
username admin privilege 15 secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
no ip domain-lookup
```

```
ip domain-name org.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel 1
description Enlace con CP-CORE
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 2
description Enlace con ER-ER
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 9
switchport mode access
!
```



```
interface FastEthernet0/4
  switchport access vlan 9
  switchport mode access
!
interface FastEthernet0/5
  shutdown
!
interface FastEthernet0/6
  shutdown
!
interface FastEthernet0/7
  shutdown
!
interface FastEthernet0/8
  shutdown
!
interface FastEthernet0/9
  shutdown
!
interface FastEthernet0/10
  shutdown
!
interface FastEthernet0/11
  shutdown
!
interface FastEthernet0/12
  shutdown
!
interface FastEthernet0/13
  shutdown
!
interface FastEthernet0/14
  shutdown
!
```

```
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 description ROUTER PRINCIPAL
 no switchport
 ip address 172.16.101.53 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/1
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
ip address 172.16.2.1 255.255.255.0
standby version 2
standby 1 ip 172.16.2.250
standby 1 priority 90
standby 1 preempt
!
interface Vlan4
ip address 172.16.4.1 255.255.254.0
standby version 2
standby 1 ip 172.16.5.250
standby 1 priority 90
standby 1 preempt
!
interface Vlan9
ip address 172.16.9.1 255.255.255.0
standby version 2
```

```
standby 1 ip 172.16.9.250
standby 1 priority 90
standby 1 preempt
!
interface Vlan10
ip address 172.16.10.1 255.255.254.0
standby version 2
standby 1 ip 172.16.11.250
standby 1 priority 90
standby 1 preempt
!
interface Vlan100
ip address 172.16.100.1 255.255.255.0
standby version 2
standby 1 ip 172.16.100.250
standby 1 priority 90
standby 1 preempt
!
router ospf 1
log-adjacency-changes
network 172.16.2.0 0.0.0.255 area 0
network 172.16.4.0 0.0.1.255 area 0
network 172.16.9.0 0.0.0.255 area 0
network 172.16.10.0 0.0.1.255 area 0
network 172.16.100.0 0.0.0.255 area 0
network 172.16.101.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 192.168.1.0 255.255.255.0 172.16.101.50
ip route 0.0.0.0 0.0.0.0 172.16.101.50
!
ip flow-export version 9
```

```
!  
!  
!  
banner motd _____Acceso solo usuarios  
permitidos._____  
!  
!  
!  
!  
line con 0  
 login local  
!  
line aux 0  
!  
line vty 0 4  
 login local  
 transport input ssh  
line vty 5 15  
 login local  
 transport input ssh  
!  
!  
!  
end
```

```
ca-p0 (172.16.2.4)_running-config
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ca-p0
!
!
!
no ip domain-lookup
ip domain-name org.com
!
username admin privilege 15 password 0 uoc
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/3
  shutdown
!
interface FastEthernet0/4
  shutdown
!
```

```
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
```

```
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
```



```

interface Vlan2
 ip address 172.16.2.4 255.255.255.0
 !
 ip default-gateway 172.16.2.1
 !
 banner motd _____Acceso solo usuarios
 permitidos._____
 !
 !
 !
 line con 0
 login local
 !
 line vty 0 4
 login local
 transport input ssh
 line vty 5 15
 login local
 transport input ssh
 !
 !
 end

```

```

ca-p1 (172.16.2.5)_running-config
 !
 version 12.2
 no service timestamps log datetime msec
 no service timestamps debug datetime msec
 no service password-encryption
 !
 hostname ca-p1
 !
 !

```

```
!  
no ip domain-lookup  
ip domain-name org.com  
!  
username admin secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1  
!  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
  switchport access vlan 10  
!  
interface FastEthernet0/2  
  switchport access vlan 4  
  switchport mode access  
!  
interface FastEthernet0/3  
  shutdown  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!
```

```
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
```

```

shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
ip address 172.16.2.5 255.255.255.0
!
ip default-gateway 172.16.2.1
!
banner motd _____Acceso solo usuarios
permitidos._____
!
!
!
line con 0
login local

```

```
!  
line vty 0 4  
  login local  
  transport input ssh  
line vty 5 15  
  login local  
  transport input ssh  
!  
!  
end
```

```
ca-p2 (172.16.2.6)_running-config  
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname ca-p2  
!  
!  
!  
no ip domain-lookup  
ip domain-name org.com  
!  
username admin secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1  
!  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
  switchport access vlan 10
```

```
!  
interface FastEthernet0/2  
  switchport access vlan 10  
  switchport mode access  
!  
interface FastEthernet0/3  
  shutdown  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  shutdown  
!  
interface FastEthernet0/11  
  shutdown  
!  
interface FastEthernet0/12  
  shutdown
```

```
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown  
!  
interface FastEthernet0/16  
shutdown  
!  
interface FastEthernet0/17  
shutdown  
!  
interface FastEthernet0/18  
shutdown  
!  
interface FastEthernet0/19  
shutdown  
!  
interface FastEthernet0/20  
shutdown  
!  
interface FastEthernet0/21  
shutdown  
!  
interface FastEthernet0/22  
shutdown  
!  
interface FastEthernet0/23  
shutdown  
!
```

```

interface FastEthernet0/24
  switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan2
  ip address 172.16.2.6 255.255.255.0
!
ip default-gateway 172.16.2.1
!
banner motd _____Acceso solo usuarios
permitidos._____
!
!
!
line con 0
  login local
!
line vty 0 4
  login local
  transport input ssh
line vty 5 15
  login local
  transport input ssh
!
!
end

```



```
cp-core (172.16.2.2)_running-config
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname cp-core
!
!
!
!
!
!
!
!
ip routing
!
!
!
!
username admin privilege 15 secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name org.com
```

```
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Port-channel 1  
  description enlace ca-core  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface Port-channel 3  
  description enlace er-er  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/1  
  channel-group 3 mode desirable  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  channel-group 3 mode desirable  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  switchport access vlan 9  
  switchport mode access  
!  
interface FastEthernet0/4
```

```
shutdown
!  
interface FastEthernet0/5  
shutdown  
!  
interface FastEthernet0/6  
shutdown  
!  
interface FastEthernet0/7  
shutdown  
!  
interface FastEthernet0/8  
shutdown  
!  
interface FastEthernet0/9  
shutdown  
!  
interface FastEthernet0/10  
shutdown  
!  
interface FastEthernet0/11  
shutdown  
!  
interface FastEthernet0/12  
shutdown  
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown
```

```
!  
interface FastEthernet0/16  
shutdown  
!  
interface FastEthernet0/17  
shutdown  
!  
interface FastEthernet0/18  
shutdown  
!  
interface FastEthernet0/19  
shutdown  
!  
interface FastEthernet0/20  
shutdown  
!  
interface FastEthernet0/21  
description ROUTER BAKCUP  
no switchport  
ip address 172.16.101.54 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/22  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface FastEthernet0/23  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface FastEthernet0/24  
switchport trunk encapsulation dot1q  
switchport mode trunk
```

```
!  
interface GigabitEthernet0/1  
  channel-group 1 mode auto  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet0/2  
  channel-group 1 mode auto  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
interface Vlan2  
  ip address 172.16.2.2 255.255.255.0  
  standby version 2  
  standby 1 ip 172.16.2.250  
  standby 1 priority 80  
  standby 1 preempt  
!  
interface Vlan4  
  ip address 172.16.4.2 255.255.254.0  
  standby version 2  
  standby 1 ip 172.16.5.250  
  standby 1 priority 80  
  standby 1 preempt  
!  
interface Vlan9  
  ip address 172.16.9.2 255.255.255.0  
  standby version 2  
  standby 1 ip 172.16.9.250  
  standby 1 priority 80
```

```
standby 1 preempt
!
interface Vlan10
ip address 172.16.10.2 255.255.254.0
standby version 2
standby 1 ip 172.16.11.250
standby 1 priority 80
standby 1 preempt
!
interface Vlan100
ip address 172.16.100.2 255.255.255.0
standby version 2
standby 1 ip 172.16.100.250
standby 1 priority 80
standby 1 preempt
!
router ospf 1
log-adjacency-changes
network 172.16.2.0 0.0.0.255 area 0
network 172.16.4.0 0.0.1.255 area 0
network 172.16.9.0 0.0.0.255 area 0
network 172.16.10.0 0.0.1.255 area 0
network 172.16.100.0 0.0.0.255 area 0
network 172.16.101.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 192.168.1.0 255.255.255.0 172.16.101.50
ip route 0.0.0.0 0.0.0.0 172.16.101.50
!
ip flow-export version 9
!
!
```

```
!  
banner motd _____Acceso solo usuarios  
permitidos._____  
!  
!  
!  
!  
line con 0  
 login local  
!  
line aux 0  
!  
line vty 0 4  
 login local  
 transport input ssh  
line vty 5 15  
 login local  
 transport input ssh  
!  
!  
!  
end
```

```
cp-z1 (172.16.2.7)_running-config
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname cp-z1
!
!
!
no ip domain-lookup
ip domain-name org.com
!
username admin secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
  switchport access vlan 10
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/3
  shutdown
!
interface FastEthernet0/4
  shutdown
!
interface FastEthernet0/5
```



```
shutdown
!  
interface FastEthernet0/6  
shutdown  
!  
interface FastEthernet0/7  
shutdown  
!  
interface FastEthernet0/8  
shutdown  
!  
interface FastEthernet0/9  
shutdown  
!  
interface FastEthernet0/10  
shutdown  
!  
interface FastEthernet0/11  
shutdown  
!  
interface FastEthernet0/12  
shutdown  
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown  
!  
interface FastEthernet0/16  
shutdown
```

```
!  
interface FastEthernet0/17  
shutdown  
!  
interface FastEthernet0/18  
shutdown  
!  
interface FastEthernet0/19  
shutdown  
!  
interface FastEthernet0/20  
shutdown  
!  
interface FastEthernet0/21  
shutdown  
!  
interface FastEthernet0/22  
shutdown  
!  
interface FastEthernet0/23  
shutdown  
!  
interface FastEthernet0/24  
switchport mode trunk  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
no ip address  
shutdown  
!  
interface Vlan2
```

```
ip address 172.16.2.7 255.255.255.0
!
ip default-gateway 172.16.2.1
!
banner motd _____Acceso solo usuarios
permitidos._____
!
!
!
line con 0
login local
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
end
```

```
cp-z2 (172.16.2.8)_running-config
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname cp-z2
!
!
```

```
!  
no ip domain-lookup  
ip domain-name org.com  
!  
username admin secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1  
!  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
  switchport access vlan 10  
!  
interface FastEthernet0/2  
  switchport access vlan 4  
  switchport mode access  
!  
interface FastEthernet0/3  
  shutdown  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!
```

```
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
```

```
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
ip address 172.16.2.8 255.255.255.0
!
ip default-gateway 172.16.2.1
!
banner motd _____Acceso solo usuarios
permitidos._____
!
!
!
line con 0
login local
```

```
!  
line vty 0 4  
  login local  
  transport input ssh  
line vty 5 15  
  login local  
  transport input ssh  
!  
!  
end
```

```
er-er (172.16.2.3)_running-config
```

```
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname er-er  
!  
!  
!  
!  
!  
!  
!  
!  
ip routing  
!  
!  
!  
!  
username admin privilege 15 secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
no ip domain-lookup  
ip domain-name org.com  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Port-channel 2  
description Enlace con CA-CORE  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface Port-channel 3  
description Enlace con CP-CORE  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface FastEthernet0/1  
channel-group 2 mode desirable  
switchport trunk encapsulation dot1q  
switchport mode trunk
```



```
!  
interface FastEthernet0/2  
  channel-group 2 mode desirable  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  channel-group 3 mode auto  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/4  
  channel-group 3 mode auto  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  shutdown  
!
```

```
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
```

```
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
ip address 172.16.2.3 255.255.255.0
!
interface Vlan4
ip address 172.16.4.3 255.255.254.0
!
interface Vlan9
ip address 172.16.9.3 255.255.255.0
!
interface Vlan10
ip address 172.16.10.3 255.255.254.0
!
interface Vlan100
ip address 172.16.100.3 255.255.255.0
!
ip classless
```

```
!  
ip flow-export version 9  
!  
!  
!  
banner motd _____Acceso solo usuarios  
permitidos._____  
!  
!  
!  
!  
line con 0  
login local  
!  
line aux 0  
!  
line vty 0 4  
login local  
transport input ssh  
line vty 5 15  
login local  
transport input ssh  
!  
!  
!  
end
```

```
cl-z1 (192.168.1.1)_running-config  
!  
version 12.2  
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
no service password-encryption
!
hostname cl-z1
!
!
!
no ip domain-lookup
ip domain-name org.com
!
username admin secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/5
 shutdown
!
```

```
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
```

```
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
```

```
ip address 192.168.1.1 255.255.255.0
!
ip default-gateway 192.168.1.250
!
banner motd _____Acceso solo usuarios
permitidos._____
!
!
!
line con 0
login local
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
end
```


R-CA_running-config

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R-CA

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

username admin privilege 15 secret 5 \$1\$mERr\$xySXv9jc77/yYJu9Jj2VT1

!

!

!

!

!

!

!

!

no ip domain-lookup

ip domain-name org.com

!

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Loopback1  
  ip address 8.8.8.8 255.255.255.0  
!  
interface Tunnel0  
  ip address 1.1.1.1 255.255.255.252  
  mtu 1476  
  tunnel source Serial0/0/0  
  tunnel destination 10.2.2.1  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.101.51 255.255.255.0  
  duplex auto  
  speed auto  
  standby version 2  
  standby 1 ip 172.16.101.50  
  standby 1 priority 150  
  standby 1 preempt  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  ip address 10.1.1.1 255.255.255.252
```

```

clock rate 128000
!
interface Serial0/0/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 172.16.101.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip route 192.168.1.0 255.255.255.0 1.1.1.2
ip route 172.16.2.0 255.255.255.0 172.16.101.53
ip route 172.16.10.0 255.255.254.0 172.16.101.53
ip route 172.16.4.0 255.255.254.0 172.16.101.53
ip route 172.16.9.0 255.255.255.0 172.16.101.53
ip route 172.16.100.0 255.255.255.0 172.16.101.53
!
ip flow-export version 9
!
!
!
banner motd _____Acceso solo usuarios
permitted_____
!
!
!

```

```
!  
line con 0  
  login local  
!  
line aux 0  
!  
line vty 0 4  
  login local  
  transport input ssh  
!  
!  
!  
end
```

R-CP_running-config

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R-CP

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

username admin privilege 15 secret 5 \$1\$mERr\$xySXv9jc77/yYJu9Jj2VT1

!

!

!

!

!

!

!

!

no ip domain-lookup

ip domain-name org.com

!

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Loopback1  
  ip address 8.8.8.8 255.255.255.0  
!  
interface Tunnel0  
  ip address 1.1.1.1 255.255.255.252  
  mtu 1476  
  tunnel source Serial0/0/0  
  tunnel destination 10.2.2.1  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.101.52 255.255.255.0  
  duplex auto  
  speed auto  
  standby version 2  
  standby 1 ip 172.16.101.50  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface Serial0/0/0  
  ip address 10.1.1.1 255.255.255.252  
  clock rate 128000
```

```

!
interface Serial0/0/1
  no ip address
  clock rate 2000000
!
interface Vlan1
  no ip address
  shutdown
!
router ospf 1
  log-adjacency-changes
  network 172.16.101.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip route 192.168.1.0 255.255.255.0 1.1.1.2
ip route 172.16.10.0 255.255.254.0 172.16.101.54
ip route 172.16.4.0 255.255.254.0 172.16.101.54
ip route 172.16.9.0 255.255.255.0 172.16.101.54
ip route 172.16.100.0 255.255.255.0 172.16.101.54
ip route 172.16.2.0 255.255.255.0 172.16.101.54
!
ip flow-export version 9
!
!
!
banner motd _____Acceso solo usuarios
permitted_____
!
!
!
!

```

```
line con 0
  login local
!
line aux 0
!
line vty 0 4
  login local
  transport input ssh
!
!
!
end
```



```
RP_running-config
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RP
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$xySXv9jc77/yYJu9Jj2VT1
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name org.com
!
```

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Loopback1  
  ip address 8.8.8.8 255.255.255.0  
!  
interface Tunnel0  
  ip address 1.1.1.2 255.255.255.252  
  mtu 1476  
  tunnel source Serial0/0/0  
  tunnel destination 10.1.1.1  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.1.251 255.255.255.0  
  duplex auto  
  speed auto  
  standby version 2  
  standby 1 ip 192.168.1.250  
  standby 1 priority 150  
  standby 1 preempt  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface Serial0/0/0
```

```

ip address 10.2.2.1 255.255.255.252
!
interface Serial0/0/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.2.2
ip route 172.16.101.0 255.255.255.0 1.1.1.1
ip route 172.16.2.0 255.255.255.0 1.1.1.1
ip route 172.16.10.0 255.255.254.0 1.1.1.1
ip route 172.16.4.0 255.255.254.0 1.1.1.1
ip route 172.16.100.0 255.255.255.0 1.1.1.1
ip route 172.16.9.0 255.255.255.0 1.1.1.1
!
ip flow-export version 9
!
!
!
banner motd _____Acceso solo usuarios
permitted_____
!
!
!

```

```
!  
line con 0  
  login local  
!  
line aux 0  
!  
line vty 0 4  
  login local  
  transport input ssh  
line vty 5 15  
  login local  
  transport input ssh  
!  
!  
!  
end
```

RB_running-config

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname RP

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

username admin privilege 15 secret 5 \$1\$mERr\$xySXv9jc77/yYJu9Jj2VT1

!

!

!

!

!

!

!

!

no ip domain-lookup

ip domain-name org.com

!

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface Loopback1  
  ip address 8.8.8.8 255.255.255.0  
!  
interface Tunnel0  
  ip address 1.1.1.2 255.255.255.252  
  mtu 1476  
  tunnel source Serial0/0/0  
  tunnel destination 10.1.1.1  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.1.252 255.255.255.0  
  duplex auto  
  speed auto  
  standby version 2  
  standby 1 ip 192.168.1.250  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface Serial0/0/0  
  ip address 10.2.2.1 255.255.255.252  
!
```

```

interface Serial0/0/1
  no ip address
  clock rate 2000000
!
interface Vlan1
  no ip address
  shutdown
!
router ospf 1
  log-adjacency-changes
  network 192.168.1.0 0.0.0.255 area 0
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.2.2
ip route 172.16.101.0 255.255.255.0 1.1.1.1
ip route 172.16.2.0 255.255.255.0 1.1.1.1
ip route 172.16.10.0 255.255.254.0 1.1.1.1
ip route 172.16.4.0 255.255.254.0 1.1.1.1
ip route 172.16.100.0 255.255.255.0 1.1.1.1
ip route 172.16.9.0 255.255.255.0 1.1.1.1
!
ip flow-export version 9
!
!
!
banner motd _____Acceso solo usuarios
permitted_____
!
!
!
!
line con 0

```

```
login local
!  
line aux 0  
!  
line vty 0 4  
login local  
transport input ssh  
line vty 5 15  
login local  
transport input ssh  
!  
!  
!  
end
```



```
ISP1_running-config
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP1
!
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX15247I0S
!
!
!
!
!
!
!
!
!
!
```

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/0/0  
ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/0/1  
ip address 10.2.2.2 255.255.255.252  
clock rate 128000  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9
```

```
!  
!  
!  
no cdp run  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
!  
!  
!  
end
```

```
ISP2_running-config
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP2
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524152M
!
!
!
!
!
!
!
!
!
```

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface GigabitEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/0/0  
ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/0/1  
ip address 10.2.2.2 255.255.255.252  
clock rate 128000  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9
```

```
!  
!  
!  
no cdp run  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
!  
!  
!  
end
```

Anexo K: Fichero “switch.cfg” de Nagios

```
#####  
#####  
# SWITCH.CFG - SAMPLE CONFIG FILE FOR MONITORING A SWITCH  
#  
#  
# NOTES: This config file assumes that you are using the sample configuration  
#       files that get installed with the Nagios quickstart guide.  
#  
#####  
#####  
#####  
#####  
#####  
#####  
#  
# HOST DEFINITIONS  
#  
#####  
#####  
#####  
#####  
# Define the switch that we'll be monitoring  
  
define host{  
    use          generic-switch          ; Inherit default values from a  
template  
    host_name    ca-core                ; The name we're giving to this switch  
    alias        ca-core (172.16.2.1)   ; A longer name associated with  
the switch  
    address      172.16.2.1             ; IP address of the switch  
    hostgroups   switches                ; Host groups this switch is associated  
with  
    icon_image   multilayer_switch.gif  
    statusmap_image multilayer_switch.gd2  
}
```

```
define host{
    use          generic-switch
    host_name    cp-core
    alias        cp-core (172.16.2.2)
    address      172.16.2.2
    hostgroups   switches
    icon_image   multilayer_switch.gif
    statusmap_image multilayer_switch.gd2
}
```

```
define host{
    use          generic-switch
    host_name    er-er
    alias        er-er (172.16.2.3)
    address      172.16.2.3
    hostgroups   switches
    icon_image   multilayer_switch.gif
    statusmap_image multilayer_switch.gd2
    #parents     ca-core,cp-core
}
```

```
define host{
    use          generic-switch
    host_name    ca-p0
    alias        ca-p0 (172.16.2.4)
    address      172.16.2.4
    hostgroups   switches
    icon_image   network_switch.gif
    statusmap_image network_switch.gd2
    parents      ca-core
}
```

```
define host{
```



```
use          generic-switch
host_name    ca-p1
alias        ca-p1 (172.16.2.5)
address      172.16.2.5
hostgroups   switches
icon_image   network_switch.gif
statusmap_image network_switch.gd2
parents      ca-core
}
```

```
define host{
    use          generic-switch
    host_name    ca-p2
    alias        ca-p2 (172.16.2.6)
    address      172.16.2.6
    hostgroups   switches
    icon_image   network_switch.gif
    statusmap_image network_switch.gd2
    parents      ca-core
}
```

```
define host{
    use          generic-switch
    host_name    ap-p0
    alias        ap-p0
    address      172.16.10.5
    hostgroups   switches
    icon_image   antenna.gif
    statusmap_image antenna.gd2
    parents      ca-p0
}
```

```
define host{
    use          generic-switch
```

```
host_name ap-p1
alias ap-p1
address 172.16.10.6
hostgroups switches
icon_image antenna.gif
statusmap_image antenna.gd2
parents ca-p1
}
```

```
define host{
    use generic-switch
    host_name ap-p2
    alias ap-p2
    address 172.16.10.7
    hostgroups switches
    icon_image antenna.gif
    statusmap_image antenna.gd2
    parents ca-p2
}
```

```
define host{
    use generic-switch
    host_name cp-z1
    alias cp-z1 (172.16.2.7)
    address 172.16.2.7
    hostgroups switches
    icon_image network_switch.gif
    statusmap_image network_switch.gd2
    parents cp-core
}
```

```
define host{
    use generic-switch
    host_name cp-z2
```

```
alias      cp-z2 (172.16.2.8)
address    172.16.2.8
hostgroups switches
icon_image network_switch.gif
statusmap_image network_switch.gd2
parents    cp-core
}
```

```
define host{
    use      generic-switch
    host_name ap-z1
    alias    ap-z1
    address  172.16.10.8
    hostgroups switches
    icon_image antenna.gif
    statusmap_image antenna.gd2
    parents  cp-z1
}
```

```
define host{
    use      generic-switch
    host_name ap-z2
    alias    ap-z2
    address  172.16.10.9
    hostgroups switches
    icon_image antenna.gif
    statusmap_image antenna.gd2
    parents  cp-z2
}
```

```
define host{
    use      generic-switch
    host_name r-ca
    alias    r-ca (172.16.101.51)
```

```
address          172.16.101.51
hostgroups       switches
icon_image       router.gif
statusmap_image router.gd2
parents          ca-core
}
```

```
define host{
    use          generic-switch
    host_name    r-cp
    alias        r-cp (172.16.101.52)
    address      172.16.101.52
    hostgroups   switches
    icon_image   router.gif
    statusmap_image router.gd2
    parents      cp-core
}
```

```
define host{
    use          generic-switch
    host_name    rp
    alias        rp (192.168.1.251)
    address      192.168.1.251
    hostgroups   switches
    icon_image   router.gif
    statusmap_image router.gd2
    parents      r-ca, r-cp
}
```

```
define host{
    use          generic-switch
    host_name    rb
    alias        rb (192.168.1.252)
    address      192.168.1.252
}
```

```
hostgroups switches
icon_image router.gif
statusmap_image router.gd2
parents      r-cp, r-ca
}
```

```
define host{
    use          generic-switch
    host_name    cl-z1
    alias        cl-z1 (192.168.1.1)
    address      192.168.1.1
    hostgroups  switches
    icon_image   network_switch.gif
    statusmap_image network_switch.gd2
    parents      rp, rb
}
```

```
define host{
    use          generic-switch
    host_name    ap1
    alias        ap1
    address      192.168.1.5
    hostgroups  switches
    icon_image   antenna.gif
    statusmap_image antenna.gd2
    parents      cl-z1
}
```

```
define host{
    use          generic-switch
    host_name    ap2
    alias        ap2
    address      192.168.1.6
    hostgroups  switches
```

```
icon_image antenna.gif
statusmap_image antenna.gd2
parents cl-z1
}
```

```
define host{
    use generic-switch
    host_name ap3
    alias ap3
    address 192.168.1.7
    hostgroups switches
    icon_image antenna.gif
    statusmap_image antenna.gd2
    parents cl-z1
}
```

```
define host{
    use generic-switch
    host_name firewall
    alias Firewall PfSense
    address 192.168.9.10
    hostgroups switches
    icon_image firewall.gif
    statusmap_image firewall.gd2
    parents r-ca
}
```

```
define host{
    use generic-switch
    host_name www-lp
    alias Salida Internet Linea Principal
    address 8.8.8.8
    hostgroups switches
    icon_image www_cloud.gif
}
```

```
statusmap_image www_cloud.gd2
parents      firewall
}
```

```
define host{
    use          generic-switch
    host_name    www-lb
    alias        Salida Internet Linea Backup
    address      8.8.8.8
    hostgroups   switches
    icon_image   www_cloud.gif
    statusmap_image www_cloud.gd2
    parents      r-cp
}
```

```
define host{
    use          generic-switch
    host_name    cl-www-lp
    alias        Centro logistico: Salida Internet Linea Principal
    address      8.8.8.8
    hostgroups   switches
    icon_image   www_cloud.gif
    statusmap_image www_cloud.gd2
    parents      rp
}
```

```
define host{
    use          generic-switch
    host_name    cl-www-lb
    alias        Centro logistico: Salida Internet Linea Backup
    address      8.8.8.8
    hostgroups   switches
    icon_image   www_cloud.gif
    statusmap_image www_cloud.gd2
}
```

```
parents    rb
}
```

```
#####
#####
```

```
#####
#####
```

```
#
```

```
# HOST GROUP DEFINITIONS
```

```
#
```

```
#####
#####
```

```
#####
#####
```

```
# Create a new hostgroup for switches
```

```
define hostgroup{
    hostgroup_name    switches           ; The name of the hostgroup
    alias              Network Switches  ; Long name of the group
}
```

```
#####
#####
```

```
#####
#####
```

```
#
```

```
# SERVICE DEFINITIONS
```

```
#
```

```
#####
#####
```

```
#####
#####
```

```
# Create a service to PING to switch
```

```
define service{
```



```

    use                generic-service    ; Inherit values from a template
    host_name          ca-core,r-ca,cp-core,r-cp,er-er,ca-p0,ca-p1,ca-p2,ap-
p0,ap-p1,ap-p2,cp-z1,cp-z2,ap-z1,ap-z2,rp,rb,cl-z1,ap1,ap2,ap3,firewall,www-
lp,www-lb,cl-www-lp,cl-www-lb ; The name of the host the service is associated
with
    service_description PING              ; The service description
    check_command       check_ping!200.0,20%!600.0,60%    ; The
command used to monitor the service
    normal_check_interval 5                ; Check the service every 5
minutes under normal conditions
    retry_check_interval 1                 ; Re-check the service every
minute until its final/hard state is determined
}

```