Firewall DNS

Como herramienta para la protección de los menores de edad en el ámbito escolar y familiar.

Carlos Villa Ferrer

Estudio e implementación de un Firewall DNS

Seguridad Empresarial

Nombre Tutor/a de TF
Borja Guaita Pérez

Profesor/a responsable de la asignatura
Víctor García Font

Fecha Entrega
13/06/2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Firewall DNS como herramienta para la protección de los menores de edad en el ámbito escolar y familiar.*
Nombre del autor:	*Carlos Villa Ferrer*
Nombre del consultor/a:	*Borja Guaita Pérez*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	*06/2023*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*DNS, Firewall, menores*

Resumen del Trabajo

En este trabajo se analiza si los firewalls DNS pueden ser una herramienta útil que permita proteger a los menores en el hogar o en las escuelas haciendo posible controlar el acceso a sitios web o servicios en la nube que puedan ser inapropiados o peligrosos para ellos.

La utilización de esta tecnología puede ayudar a proteger la seguridad y privacidad de los menores al bloquear la conexión a servicios de internet inapropiados para la edad del usuario, a sitios web maliciosos, que contengan malware o páginas de phishing para capturar sus credenciales.

Algunos firewalls DNS disponen de funcionalidades adicionales como actualización automática de dominios restringidos a partir de listas publicas u otras características como la capacidad de bloquear el acceso a servidores de juegos, plataformas de streaming o a redes sociales durante periodos horarios configurables, permitiendo que durante el horario escolar no puedan acceder a determinados contenidos.

Para analizar la utilidad de esta tecnología se determinan los requerimientos del ámbito escolar y familiar.

Seguidamente se analizan las distintas soluciones open source o que se ponen a disposición de forma gratuita, comparando y valorando el nivel de cumplimiento con los requerimientos, sus características, sus funcionalidades, los requerimientos de hardware exigidos, así como las arquitecturas y nivel de flexibilidad que se pueden adoptar para su configuración.

Las soluciones y arquitecturas valoradas como las más adecuadas son probadas y evaluadas durante un periodo en una red local de ámbito familiar, obteniendo las conclusiones y proponiendo una solución implantable.

Abstract

This paper analyses DNS firewalls in other to check if they can be a useful tool to protect children at home or at school, making it possible to control access to websites or cloud services that may be inappropriate or dangerous for them.

Using this technology helps to protect the safety and privacy of minors by blocking the connection to Internet services that are inappropriate for the user's age, blocking malicious websites that contain malware or blocking phishing pages that try to capture their credentials.

There are DNS firewalls that have additional features such as automatic updating of restricted domains from public lists or other features such as the ability to block access to game servers, streaming platforms, or social networks during configurable time periods, allowing that at school times children cannot access certain content.

To analyse the usefulness of this technology, the requirements of the school and family environment are determined.

Different open-source solutions, or the solutions that are free of change, are checked to obtain the level of compliance with the requirements as well as their characteristics, functionalities, hardware requirements, but also its architecture flexibility that can be adopted for its configuration.

The solutions and architectures evaluated as the most appropriate are test in this paper during a period in a local family network, obtaining the final conclusions and proposing an implementable solution.

Índice

1. Introducción 1
1.1. Contexto y justificación del Trabajo 1
1.2. Objetivos del Trabajo 2
1.3. Impacto en sostenibilidad, ético-social y de diversidad 2
1.3.1. Sostenibilidad 2
1.3.2. Comportamiento ético y responsabilidad social 3
1.3.3. Diversidad y derechos humanos 3
1.4. Enfoque y método seguido 3
1.5. Planificación del Trabajo 5
1.5.1. Recursos necesarios 5
1.5.1.1. Hardware 5
1.5.1.2. Software 5
1.5.1.3. Tiempo 6
1.5.1.4. Presupuesto económico 6
1.5.1.5. Planificación 6
1.6. Breve sumario de productos obtenidos 8
1.7. Breve descripción de los otros capítulos de la memoria 8
1.8. Riesgos durante la realización del trabajo 9
2. Materiales y métodos 9
2.1. Estado del arte 9
2.1.1. Que es y para qué sirve un Firewall DNS 9
2.1.2. Tendencias en Firewall DNS 10
2.1.3. RPZs, categorización de sitios e información para firewalls DNS 11
2.2. Perfiles de usuario 14
2.3. Dispositivos, Servicios y amenazas 15
2.4. Arquitecturas y topologías de red 15
2.5. Requerimientos 18
2.5.1. Requerimientos en los centros educativos 19
2.6. Herramientas Firewall DNS 19
2.6.1. Akamai ETP 19
2.6.2. Cisco Umbrella 19
2.6.3. Palo Alto DNS Security 20
2.6.4. Check Point Secure Web Gateway 21
2.6.5. DNSFilter 22
2.6.6. Comodo DNS Firewall 22
2.6.7. OpenDNS 23
2.6.8. Neustar UltraDNS 24
2.6.9. Quad9 24
2.6.10. BIND 24
2.6.11. Dnsmasq 25
2.6.12. Knot-resolver 25
2.6.13. Pi-hole 25
2.6.14. AdGuard Home 26
2.6.15. pfBlockerNG 27
2.7. Análisis comparativo 28
2.7.1. Conclusiones del análisis comparativo 30
3. Implantación 31

3.1. Arquitectura del entorno en Laboratorio 31
3.2. Implementación practica de los Firewall DNS 33
3.2.1. Sitios de prueba 33
3.2.2. Servidores DNS para utilizar durante la evaluación 34
3.2.3. Proceso de instalación 34
4. Análisis de resultados y valoración de riesgos 35
4.1. Problemas encontrados y soluciones 35
4.2. Análisis de diferencias entre los aspectos de las soluciones 42
4.3. Solución final 43
4.4. Análisis de los resultados obtenidos 45
4.5. Estudio de los requerimientos legales y de protección de datos 47
4.6. Valoración de los riesgos de la implantación del Firewall DNS 48
5. Conclusiones 51
5.1. Conclusiones del trabajo realizado 51
5.2. Reflexión crítica sobre la consecución de los objetivos 52
5.3. Cumplimiento de la planificación 53
6. Líneas de trabajo futuras 53
7. Glosario 54
8. Bibliografía y fuentes consultadas 56
i. Anexos 59
i. Anexo I: Instalación y configuración de Pfsense 59
ii. Anexo II: Instalación y configuración de OpenDNS 64
iii. Anexo III: Instalación y configuración de AdGuard Home 72
iv. Anexo IV: Instalación y configuración de Pi-Hole 89
v. Anexo V: Instalación y configuración de pfBlockerNG 107
vi. Anexo VI: Instalación y configuración de DNSCloak en iPhone 119
vii. Anexo VII: Instalación y configuración de Quad9 en Android 121
viii. Anexo VIII: Análisis de un caso real de Phishing 121
ix. Anexo IX: Configuración de personalDNSfilter en Android 128
x. Anexo X: Certificados para SSL y DNS dinámico para conexión FTTH 130
xi. Anexo XI: Configuración de VPN OpenVPN en router pfSense 134
xii. Anexo XII: Configuración del portal cautivo 141

Lista de figuras y tablas

Figura 1: Desglose de los costes de materiales necesarios para el trabajo. 6
Figura 2: Gantt con la planificación del trabajo. 7
Figura 3: Listas públicas de URLs e IPs para su uso con Firewalls DNS. 13
Figura 4: Diagrama de ítems que intervienen en el proyecto. 17
Figura 5: Cuadro resumen de funcionalidades de Cisco Umbrella. [95] 20
Figura 6: Cuadro resumen de funcionalidades de Palo Alto DNS Sec. [97] 21
Figura 7: Appliances de CheckPoint Secure Web Gateway [99] 22
Figura 8: Categorias de filtrado de DNSFilter [101] 22
Figura 9: Prestaciones de Cómodo DNS Firewall [102] 23
Figura 10: Modalidades de uso de OpenDNS [103] 23
Figura 11: Opciones de servicio de UltraDNS [102] 24
Figura 12: Interfaz de usuario de Pi-Hole 25
Figura 13: Interfaz de usuario de AdGuard Home 26
Figura 14: Interfaz de usuario de pfBlockerNG 27
Figura 15: Análisis comparativo de los principales Firewalls DNS. 29
Figura 16: Arquitectura previa a las modificaciones para la red de laboratorio. 31
Figura 17: Bloqueo del ISP de la configuración de los DNS en el router. 31
Figura 18: Diseño de la arquitectura del entorno de pruebas. 32
Figura 19: Resultado de la prueba con DNS Benchmark a servidores DNS. ... 34
Figuras 20 y 21: Monitorización con arpwatch y configuración con Adguard. .. 35
Figura 22: Escáneres de Censys y otros en los logs al abrir el puerto DNS. ... 36
Figura 23: Configuración y bloqueo de escáneres de China y USA 36
Figura 24: Filtrado de conexiones por geolocalización. 37
Figura 25: Filtrado de conexiones por geolocalización en pfBlockerNG 38
Figura 26: Identificación de los clientes móviles por VPN en Adguard. 38
Figura 27: Solución a los falsos positivos que afectan a Alexa 39
Figura 28: Añadir manualmente filtros de URL. 40
Figura 29: Añadir manualmente filtros de URL en Adguard Home. 41
Figura 30: Uso de fuentes OSINT para analizar la amenaza. 41
Figura 31: Análisis comparativo de las diferencias entre soluciones. 42
Figura 32: Diagrama de la solución final propuesta. 44
Figura 33: Diagrama de la solución final propuesta con el mínimo hardware. . 44
Figura 34: Medición del ancho de banda disponible. 45
Figura 35: Medición de la latencia. 45
Figura 36: Cumplimiento de los requerimientos por parte de las soluciones. .. 46
Figura 37: Estadísticas y cálculos del ahorro y sostenibilidad. 48
Figura 38: Descarga de la imagen de pfSense para su instalación. 59
Figura 39: IPs de las interfaces de red. 59
Figura 40: Vista frontal de dispositivos LiveBox+, pfSense y AP DDWRT. 60
Figura 41: Vista cenital y de cableado de LiveBox+, pfSense y AP DDWRT. .. 60
Figura 42: Configuración básica de red del DDWRT. 60
Figura 43: Configuración del Livebox+. 60
Figura 44: Configuración de red de los AP OpenWRT. 61
Figura 45: Configuración las reglas del firewall pfSense. 61
Figura 46: Configuración del DHCP server – Rango de IPs (1). 62
Figura 47: Configuración del DHCP server - Servidores DNS (2). 62
Figura 48: Verificación de asignaciones IP y servidores DNS por DHCP. 62

Figura 49: Verificación de conectividad a Internet por ICMP. 63
Figura 50: Configuración del tipo de cuenta en OpenDNS (1). 64
Figura 51: Configuración del tipo de cuenta en OpenDNS (2). 64
Figura 52: Crear nueva red en OpenDNS (1). 65
Figura 53: Crear nueva red en OpenDNS (2). 65
Figura 54: Actualización del DNS dinámico de OpenDNS desde pfSense. 66
Figura 55: Activar estadísticas y logs de OpenDNS. 66
Figura 56: Activar filtrado de contenidos de OpenDNS. 67
Figura 57: Activar protección contra Malware, Phishing y DNS rebinding. 68
Figura 58: Personalización de la pantalla de bloqueo en OpenDNS. 68
Figura 59: Personalización de los mensajes de las pantallas de bloqueo. 69
Figura 60: Pantalla de bloqueo en OpenDNS. 70
Figura 61: Estadísticas de uso en OpenDNS. 71
Figura 62: Selección de la instalación del plugin Adguard Home. 72
Figura 63: Progreso de la instalación de Adguard Home. 72
Figura 64: Fin del proceso de instalación de Adguard Home. 72
Figura 65: Post Install Notes de Adguard Home. 73
Figura 66: Menú de acciones sobre un Plugin de TrueNas. 73
Figura 67: Login al portal de Adguard Home. 73
Figura 68: Panel de control de Adguard Home. 74
Figura 69: Uso de filtros y actualizaciones horarias en Adguard Home. 74
Figura 70: Bloqueo de phishing y malware en Adguard Home. 75
Figura 71: Activación del filtrado de control parental en Adguard Home. 75
Figura 72: Aviso de filtrado de control parental en Adguard Home. 75
Figura 73: Forzado de uso de búsquedas seguras. 75
Figura 74: Anonimización de la IP del cliente en Adguard Home. 76
Figura 75: Registro de consultas DNS y estadísticas en Adguard Home. 76
Figura 76: Fuentes DNS en Adguard Home. 77
Figura 77: Fuentes DNS de arranque para TLS y HTTPS. 77
Figura 78: Configuración de DNS inverso en Adguard Home. 77
Figura 79: Página de aviso de filtrado personalizada en Adguard. 78
Figura 80: Configuración parámetros de servidor DNS en Adguard. 78
Figura 81: Prueba de configuración en Adguard Home. 79
Figura 82: Resultado satisfactorio de la prueba de configuración. 79
Figura 83: Parámetros de cache y rendimiento. 79
Figura 84: Personalización de configuración por dispositivo. 80
Figura 85: Edición de la configuración personalizada. 81
Figura 86: Bloqueo de servicios en el dispositivo Xbox. 82
Figura 87: Verificación del bloqueo de servicios en el dispositivo Xbox. 82
Figura 88: Configuración de listas de bloqueo. 83
Figura 89: Configuración de listas de bloqueo personalizadas en Adguard. 84
Figura 90: Listas blancas en Adguard Home. 84
Figura 91: Reescrituras DNS en Adguard Home. 84
Figura 92: Servicios bloqueados por defecto. 85
Figura 93: Excepciones para servicios de Amazon. 86
Figura 94: Dashboard con estadísticas de uso del DNS. 86
Figura 95: Extracto del registro de consultas DNS. 87
Figura 96: Cambio de contraseña en Adguard Home. 88
Figura 97: Máquina virtual Ubuntu en TrueNAS para Pi-hole. 89
Figura 98: Instalación de Pi-hole (1). 89

Figura 99: Instalación de Pi-hole (2)..... 90
Figura 100: Instalación de Pi-hole (3)..... 91
Figura 101: Modificación de la página de bloqueo en Pi-hole. 92
Figura 102: Acceso a la web de gestión de Pi-hole..... 93
Figura 103: Menú 'settings' del software Pi-hole. 93
Figura 104: Configuración de los servidores resolutores DNS en Pi-hole. 94
Figura 105: Configuración de búsquedas DNS inversas. 94
Figura 106: Verificación de la resolución DNS y DNS inversas..... 95
Figura 107: Configuración de los logs de registro de actividad. 95
Figura 108: Configuración de las búsquedas seguras en Pi-hole. 96
Figura 109: Configuración de los grupos de filtrado en Pi-hole. 96
Figura 110: Configuración de los clientes en Pi-Hole. 97
Figura 111: Asignación de dominios a grupos en Pi-Hole. 97
Figura 112: Asignación de listas de filtrado a grupos en Pi-Hole. 98
Figura 113: Actualización de la configuración de filtrado en Pi-Hole. 99
Figura 114: Programación de las actualizaciones de los filtros en Pi-hole. 103
Figura 115: Prueba de filtrado en Pi-hole (1)..... 103
Figura 116: Prueba de filtrado en Pi-hole (2)..... 104
Figura 117: Prueba de filtrado en Pi-hole (3)..... 104
Figura 118: Prueba de filtrado en Pi-hole (4)..... 104
Figura 119: Prueba de filtrado en Pi-hole (5)..... 104
Figura 120: Dashboard y estadísticas en Pi-hole. 105
Figura 121: Registro de actividad en Pi-hole. 106
Figura 122: Configuración de DNS Resolver en pfSense. 107
Figura 123: Asistente de configuración de pfBlockerNG (1)..... 108
Figura 124: Asistente de configuración de pfBlockerNG (2)..... 108
Figura 125: Asistente de configuración de pfBlockerNG (3)..... 108
Figura 126: Asistente de configuración de pfBlockerNG (4)..... 109
Figura 127: Asistente de configuración de pfBlockerNG (5)..... 109
Figura 128: Asistente de configuración de pfBlockerNG (6)..... 109
Figura 129: Configuración de DNSBL en pfBlockerNG (1)..... 110
Figura 130: Configuración de DNSBL en pfBlockerNG (2)..... 110
Figura 131: Configuración de DNSBL en pfBlockerNG (3)..... 110
Figura 132: Configuración de DNSBL en pfBlockerNG (4)..... 111
Figura 133: Configuración de Safe Search en pfBlockerNG 111
Figura 134: Bloqueo de DNS HTTPS/TLS/QUIC en pfBlockerNG 111
Figura 135: Filtrado por categorias en pfBlockerNG 112
Figura 136: Alta en maxmind.com para key GeoIP 113
Figura 137: Configuración de GeoIP en pfBlockerNG 113
Figura 138: Reglas de firewall de las interfaces de red 114
Figura 139: Estado de los servicios en pfSense..... 116
Figura 140: Configuración de los Feeds (1) 116
Figura 141: Configuración de los Feeds (2) 117
Figura 142: Verificación de bloqueos DNSBL en pfBlockerNG 117
Figura 143: Verificación de las búsquedas seguras en youtube. 118
Figura 144: Logs de pfSense. 118
Figura 145: Detección de malware en una app de iPhone. 119
Figura 146: Configuración de DNS Cloak en iPhone. 120
Figura 147: Configuración de Quad9 en Android. 121
Figura 148: Correo del phishing original..... 122

Figura 149: Portal de captura de contraseñas..... 122
Figura 150: Texto de ciberdelincuentes advirtiendo del robo. 123
Figura 151: Contacto de los ciberdelincuentes vía WhatsApp. 124
Figura 152: nslookup. 126
Figura 153: WAS con Subgraph Vega. 127
Figura 154: Aplicación en la Playstore. 128
Figura 155: Configuración de los servidores DNS. 128
Figura 156: Configuración de los filtros y de VPN always-on. 129
Figura 157: Configuración del NAT en router pfSense 130
Figura 158: Configuración del NAT en router Jazztel 130
Figura 159: Configuración de los DNS dinámicos en router pfSense 131
Figura 160: Proceso de importar certificados en router pfSense 132
Figura 161: Certificados almacenados en router pfSense 132
Figura 162: Configuración del cifrado SSL en Adguard Home 133
Figura 163: Configuración de OpenVPN en pfSense (I) 134
Figura 164: Configuración de OpenVPN en pfSense (II) 134
Figura 165: Configuración de OpenVPN en pfSense (III) 134
Figura 166: Configuración de OpenVPN en pfSense (IV) 135
Figura 167: Configuración de OpenVPN en pfSense (IV) 135
Figura 168: Configuración de OpenVPN en pfSense (IV) 136
Figura 169: Configuración de OpenVPN en pfSense (IV) 136
Figura 170: Configuración de OpenVPN en pfSense (IV) 136
Figura 171: Servidor OpenVPN en pfSense configurado 137
Figura 172: Creación de usuario para acceso por OpenVPN 137
Figura 173: Regla de firewall para OpenVPN (última línea) 138
Figura 174: Nueva regla de NAT para OpenVPN 138
Figura 175: Exportando la configuración de cliente de OpenVPN (I) 138
Figura 176: Exportando la configuración de cliente de OpenVPN (II) 139
Figura 177: Conexión del cliente OpenVPN 139
Figura 178: Conexión del cliente OpenVPN en logs de Adguard Home 140
Figura 179: Verificación de visibilidad entre red local y VPN. 140
Figura 180: Acceso a la configuración del portal cautivo en pfSense. 141
Figura 181: Parámetros de configuración del portal cautivo implantado (I) 141
Figura 182: Parámetros de configuración del portal cautivo implantado (II) ... 142
Figura 183: Aspecto del portal cautivo implantado. 142

1. Introducción

1.1. Contexto y justificación del Trabajo

Este trabajo nace de la necesidad de proteger a los menores de edad, en los ámbitos escolares y familiares, de su exposición a la información potencialmente inadecuada accesible en Internet y así como de los riesgos a los que se enfrentan al navegar por la red.

Hoy en día, los menores de edad tienen un acceso muy temprano y frecuente a Internet, lo que conlleva riesgos para su seguridad y bienestar emocional. Por ello, no solo es recomendable, sino necesario el que los padres, profesores y responsables de la educación de los menores tomen medidas con el objetivo de protegerlos de los contenidos inapropiados, del malware, del ciberacoso, del phishing, del grooming y de muchos otros peligros en línea.

Las grandes firmas de software y hardware, como Microsoft, Apple, Google o Nintendo proporcionan herramientas de supervisión y control familiar para sus productos, que permiten que los padres y tutores gestionen los accesos a los contenidos, así como los horarios en que les permiten el uso de los dispositivos, de los servicios y de las aplicaciones. Inicialmente, estas herramientas se ofrecían de forma gratuita, pero en la actualidad empiezan a comercializarse ciertas funcionalidades solo bajo subscripciones de pago periódicas. Adicionalmente, cada fabricante provee sus propias herramientas y teniendo en cuenta que un menor puede utilizar tecnología de multitud de fabricantes (PCs, ordenadores portátiles, consolas de videojuegos, SmartTVs, tablets, móviles, smartwatches…), el uso de este tipo de herramientas se vuelve complejo por la necesidad de tener que instalar, configurar y acceder a multitud de aplicaciones e interfaces de control parental.

En el ámbito escolar, los equipos informáticos son utilizados y compartidos por múltiples usuarios y no suelen implantarse más medidas de seguridad que el control y supervisión del tutor durante su uso, caso en que un tutor o profesor tiene que supervisar (a la vez que imparte su clase) a grupos de 25 o más alumnos de forma simultánea, lo que es complejo y poco eficiente.

La propuesta de este trabajo, un Firewall DNS, se presenta como una solución técnica centralizada, viable, de bajo coste y efectiva. Mediante esta herramienta se permite, entre otras funciones: filtrar el acceso a contenidos inapropiados, limitar el rastreo, bloquear sitios web maliciosos, proteger contra malware o el phishing, así como establecer restricciones de tiempo al uso y delimitar los servicios de la red a los que se permite acceder a los menores de edad.

La justificación de este trabajo radica en la importancia de proteger a los menores de edad en su acceso a Internet. La protección de los derechos de los menores, su seguridad y bienestar emocional son responsabilidades compartidas por los padres, tutores, educadores y la sociedad en general. El Firewall DNS se presenta como una medida preventiva y de control de los riesgos en línea, contribuyendo así a la formación de ciudadanos digitales responsables y seguros, considerando los principios de la Competencia de Compromiso Ético y Global (CCEG) y los Objetivos de Desarrollo Sostenible (ODS) de la Universitat Oberta de Catalunya (UOC).

1.2. Objetivos del Trabajo

Los objetivos de este trabajo son:

- Recopilar y describir las diferentes técnicas y métodos utilizados por los ciberdelincuentes para atacar a menores de edad en el ámbito escolar y familiar.
- Identificar los principales riesgos a los que se enfrentan los menores de edad en el ámbito escolar y familiar al utilizar internet.
- Recopilar y describir los diferentes tipos de Firewalls DNS y comparar sus características, así como sus ventajas y desventajas.
- Identificar y analizar los distintos protocolos y tecnologías involucrados en el uso de Firewalls DNS.
- Determinar y establecer diferentes perfiles de usuario que se beneficien de la implementación de un Firewall DNS.
- Probar y analizar el impacto de la implementación del Firewall DNS en la experiencia del usuario.
- Analizar las implicaciones éticas y sociales de la implementación de un Firewall DNS para la protección de menores de edad en el ámbito escolar y familiar.
- Analizar el impacto que puede tener la implementación de un Firewall DNS en el cumplimiento de los objetivos de desarrollo sostenible.
- Analizar la viabilidad económica de la implementación de un Firewall DNS, teniendo en cuenta no solo los costes de adquisición e implementación, sino también los costes de mantenimiento.
- Establecer los requisitos mínimos de hardware y software necesarios para la implementación de un Firewall DNS.
- Determinar el procedimiento de integración de un Firewall DNS en una infraestructura de red ya existente.
- Probar y analizar el impacto de la implementación del Firewall DNS en el rendimiento de la red.
- Identificar los diferentes tipos de amenazas y vulnerabilidades que pueden afectar la seguridad del Firewall DNS.
- Identificar los principales indicadores de rendimiento (KPIs) para la evaluación de la efectividad del Firewall DNS.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Un "Firewall DNS como herramienta para la protección de los menores de edad en el ámbito escolar y familiar" tiene impactos positivos en las tres dimensiones de la competencia transversal UOC "Compromiso ético y global". Asimismo, también puede tener impactos negativos. Estos impactos se enumeran y describen a continuación.

1.3.1. Sostenibilidad

- Impactos positivos: Si se implementa adecuadamente, un firewall DNS contribuye a la sostenibilidad al ayudar a proteger los recursos y activos digitales de la organización escolar o familiar. Además, el filtro de contenidos web puede reducir el consumo de ancho de banda y aumentar la eficiencia energética de los equipos.

- Impactos negativos: Dependiendo de la implementación de un firewall DNS se pueden generar mayores costes de infraestructura y consumo de energía, así como una mayor complejidad en la gestión y administración del sistema, lo que podría implicar un impacto negativo en la sostenibilidad.

1.3.2. Comportamiento ético y responsabilidad social

- Impactos positivos: Un firewall DNS contribuye a mejorar el comportamiento ético y la responsabilidad social dado que protege a los menores de edad de contenidos inapropiados y potencialmente dañinos. Esto incluye protección contra los contenidos violentos o pornografía y sin olvidar contenidos relacionados con el odio, de ideologías radicales o ilegales.

- Impactos negativos: Un firewall DNS también puede generar desconfianza y falta de privacidad dado que es posible utilizarlo para monitorizar el uso de Internet de los menores en las escuelas o en los hogares sin su conocimiento o consentimiento. Por otra parte, los filtros de contenidos o de categorías en internet pueden generar restricciones innecesarias a la libertad de expresión y a la información por una excesiva sobreprotección.

1.3.3. Diversidad y derechos humanos

- Impactos positivos: La implementación de un firewall DNS ayuda a proteger los derechos humanos en los menores de edad, al evitar la exposición a contenido dañino. Además, con una configuración adecuada, garantiza la equidad en el acceso a la información y contribuye a reducir los riesgos de discriminación de género y otros tipos de discriminación.

- Impactos negativos: Las restricciones a los servicios y contenidos de internet no suelen ser perfectas y generan falsos positivos en la detección de contenidos inapropiados. Esto puede traducirse en la censura involuntaria de ciertos contenidos en función de su origen cultural, étnico o lingüístico. Por otra parte, un firewall DNS puede limitar la libertad de expresión y limitar el acceso a información relevante o importante, especialmente si se restringe excesivamente los contenidos admitidos, si la supervisión y configuración no es la adecuada.

1.4. Enfoque y método seguido

Se plantea una estrategia que aborda de manera sistemática los aspectos relevantes a considerar para cumplir con el objetivo de implementar un firewall DNS para la protección del menor, basándose en un análisis pormenorizado y detallado, así como estudiando y definiendo los requerimientos mínimos a cubrir y con los que se realiza un cribado que permite la selección de la mejor implementación.

La estrategia y enfoque de la metodología para realizar de este trabajo consiste en:

1. Estudio del estado del arte. Consiste en realizar una revisión de los artículos, textos e investigaciones en el área de los firewalls DNS para comprender el estado actual de la tecnología, así como sus usos, aplicaciones y limitaciones.

2. Amenazas de seguridad para los menores. Se identifican las principales amenazas a la seguridad a las que están expuestos los menores en Internet.

3. Recolección de herramientas disponibles. Se recopilan e investigan las distintas soluciones de firewall DNS disponibles en los mercados privados, opensource y los de uso libre o gratuito. Se identifican las características y funcionalidades de cada herramienta para su evaluación posterior.

4. Definir los distintos perfiles de usuario posibles. Se definen los diferentes perfiles o roles de usuario que existen en el uso de un Firewall DNS, así como las necesidades de seguridad. El objetivo es identificar qué funciones, características y requerimientos son necesarias para cada perfil.

5. Determinar los dispositivos que se requiere proteger. Se identifican los dispositivos que se busca proteger, incluyendo tanto ordenadores como dispositivos móviles, así como dispositivos electrónicos o IoT.

6. Analizar las posibles arquitecturas de red. Se estudian las arquitecturas de red donde se puede requerir implementar un firewall DNS para identificar los requisitos de infraestructura necesarios para su implementación.

7. Definir la lista de requerimientos a cubrir. Se define la lista de requerimientos que un firewall DNS debe cubrir para proteger los dispositivos identificados, satisfacer las necesidades de los diferentes perfiles de usuario y encajar en las arquitecturas de red determinadas.

8. Evaluación teórica de las herramientas disponibles y cribado en base a las funcionalidades y características declaradas por el fabricante o autor. En esta fase se evalúan y puntúan de forma teórica las herramientas disponibles en base a cumplimiento de los requerimientos, Las herramientas que no cumplen con los requerimientos definidos son cribadas y no serán evaluadas en un entorno practico de laboratorio.

9. Preparación de los entornos y laboratorios de pruebas. Se preparan los entornos de pruebas en base a las necesidades identificadas anteriormente.

10. Evaluación practica de las herramientas que han superado el cribado, desplegándolas, configurándolas e implementándolas. Se definen PKIs para la evaluación de las herramientas y se realiza un análisis y evaluación práctica de las herramientas seleccionadas que han pasado la criba, verificando su efectividad y capacidad real para cumplir con los requisitos definidos, así como las amenazas y vulnerabilidades que pueden afectarles.

11. Análisis de resultados y conclusiones: Se analizan todos los resultados obtenidos anteriormente y se llega a la conclusión sobre qué herramienta es la mejor opción para implementar un firewall DNS en cada escenario y arquitectura considerada, considerado su impacto económico, las implicaciones éticas y morales de su uso, así como la afectación a la experiencia del usuario.

1.5. Planificación del Trabajo

1.5.1. Recursos necesarios

1.5.1.1. Hardware

Se requieren equipos informáticos, ordenadores y servidores virtualizados, así como dispositivos de distintas tipologías para realizar pruebas en laboratorio.

El hardware necesario, teniendo en cuenta que se han marcado con * los equipos/dispositivos que pueden ser susceptibles de ser adquiridos, objeto de instalación de software o reconfiguración derivado de la implementación de un firewall DNS consta de:

- Hardware de red:
  - 1 x Router del operador de telefonía (Jazztel) para el acceso a Internet.
  - 1 x MiniPC/Firewall* fanless con pfSense.
  - 2 x Routers con AP Wifi OpenWRT*
  - 1 x Router con AP Wifi DD-WRT*
  - 1 x Switch
- Raspberry Pi*, con distintos usos:
  - Plataforma de entretenimiento (Kodi, OSMC…)
  - Plataforma de emulación de juegos.
  - Capacidad de correr un Firewall DNS.
- Servidor* con TrueNAS core y virtualización de máquinas y SO's.
- Dispositivos móviles
  - Teléfonos móviles con Sistema Operativo Android y IOS
  - Tabletas con Sistema Operativo Android
- PCs de escritorio y portátiles
  - PCs Linux*, FreeBSD* y Windows*
- SmartTVs LG con WebOS y con S.O de Samsung.
- Videoconsolas y dispositivos de juego:
    - Nintendo Switch
    - Xbox 360 y Xbox One
    - Playstation 3
    - PC con Batocera
- Dispositivos IoT variados, tales como:
    - Enchufes e interruptores Wifi
    - Termostato Wifi
    - Concentrador de emisión de intrarrojos y radiofrecuencia.
    - Amazon Echo
    - Amazon FireTV Stick
    - Alarma de hogar Wifi

1.5.1.2. Software

Además de las propias herramientas de Firewall DNS, se requieren herramientas y programas informáticos especializados para el análisis y evaluación de parámetros como el tráfico de red, o su seguridad, concretamente:

- pfSense Firewall con plugins para registro y monitorización del tráfico red.
- Routers OpenWrt y DD-Wrt con capacidad de monitorización de red.

- Wireshark, Nmap y otros útiles de análisis de redes.
- Software TrueNas con *jails* e *hipervisor byhve*.

1.5.1.3. Tiempo

Se cuenta con 3 meses y medio para llevar a cabo el estudio, realizar las pruebas y las evaluaciones, así como para la elaboración de informes y presentaciones.

1.5.1.4. Presupuesto económico

La práctica totalidad de los equipos a utilizar durante las pruebas ya fueron adquiridos para otros fines, a excepción del hardware de PC que implementa un firewall pfSense.

Se valora también el coste de una Raspberry Pi 3.

No se considera el coste del resto de hardware de red, así como el de instalación e implantación en una instalación real, que se considera de bajo coste y limitado a las horas de trabajo del personal que realizaría la instalación y configuración.

Grupo	Ítem	Precio	Observaciones
Raspberry Pi 3	Cubierta Caja Protectora con Disipador de Calor de Refrigeración de Aluminio para Raspberry Pi 3	8,99 €	
Raspberry Pi 3	Raspberry Pi 3 Model B	139,90 €	
Raspberry Pi 3	Fuente alimentación Raspberry Pi 3	10,22 €	
Switch DD-WRT	D-Link DIR-825 rev. B1	49,95 €	Stock existente
Switch OpenWRT	D-Link DIR-825 rev. B1	49,95 €	Stock existente
Switch OpenWRT	TP-Link TL-WR1041N/ND v2	29,00 €	Stock existente
Firewall PfSense	Intel Celeron N5100 4 nucleos, TDP 8GB RAM, 128GB SSD, 4xGigabit Ethernet i226-V, 10W	179,78 €	
TrueNAS	Equipo Intel i5-4570 CPU @ 3.20GHz, 24GB RAM, 7 TiB	No relevante	Piezas recicladas
Cables de red	Cables de red	No relevante	Stock sobrante
Router ISP	Arcadyan PRV3397B_E_LT - LiveBox+ Jazztel	No relevante	Ya Existente

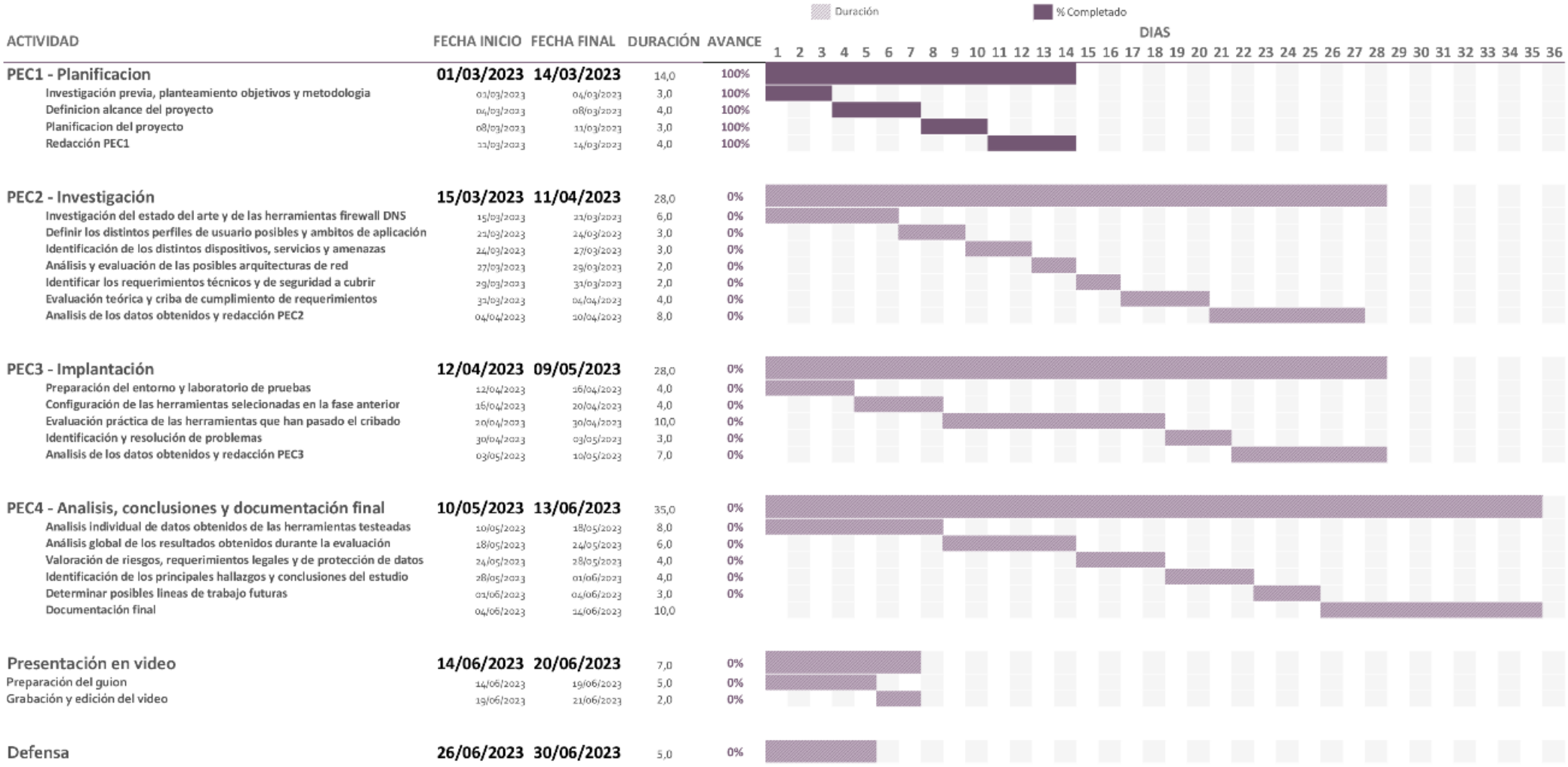
Figura 1: Desglose de los costes de materiales necesarios para el trabajo.

NOTA: Se valoran los costes de mantenimiento en las conclusiones de este trabajo.

1.5.1.5. Planificación

Se considera una planificación por hitos, con 3 entregas parciales programadas y una entrega final. Tras la entrega final se elaborará un video de presentación y se preparará una defensa pública del trabajo final.

En la página siguiente se muestra un diagrama Gantt con la planificación del trabajo.



ACTIVIDAD	FECHA INICIO	FECHA FINAL	DURACIÓN	AVANCE
PEC1 - Planificacion	**01/03/2023**	**14/03/2023**	14,0	100%
Investigación previa, planteamiento objetivos y metodologia	01/03/2023	04/03/2023	3,0	100%
Definicion alcance del proyecto	04/03/2023	08/03/2023	4,0	100%
Planificacion del proyecto	08/03/2023	11/03/2023	3,0	100%
Redacción PEC1	11/03/2023	14/03/2023	4,0	100%
PEC2 - Investigación	**15/03/2023**	**11/04/2023**	28,0	0%
Investigación del estado del arte y de las herramientas firewall DNS	15/03/2023	21/03/2023	6,0	0%
Definir los distintos perfiles de usuario posibles y ambitos de aplicación	21/03/2023	24/03/2023	3,0	0%
Identificación de los distintos dispositivos, servicios y amenazas	24/03/2023	27/03/2023	3,0	0%
Análisis y evaluación de las posibles arquitecturas de red	27/03/2023	29/03/2023	2,0	0%
Identificar los requerimientos técnicos y de seguridad a cubrir	29/03/2023	31/03/2023	2,0	0%
Evaluación teórica y criba de cumplimiento de requerimientos	31/03/2023	04/04/2023	4,0	0%
Analisis de los datos obtenidos y redacción PEC2	04/04/2023	10/04/2023	8,0	0%
PEC3 - Implantación	**12/04/2023**	**09/05/2023**	28,0	0%
Preparación del entorno y laboratorio de pruebas	12/04/2023	16/04/2023	4,0	0%
Configuración de las herramientas selecionadas en la fase anterior	16/04/2023	20/04/2023	4,0	0%
Evaluación práctica de las herramientas que han pasado el cribado	20/04/2023	30/04/2023	10,0	0%
Identificación y resolución de problemas	30/04/2023	03/05/2023	3,0	0%
Analisis de los datos obtenidos y redacción PEC3	03/05/2023	10/05/2023	7,0	0%
PEC4 - Analisis, conclusiones y documentación final	**10/05/2023**	**13/06/2023**	35,0	0%
Analisis individual de datos obtenidos de las herramientas testeadas	10/05/2023	18/05/2023	8,0	0%
Análisis global de los resultados obtenidos durante la evaluación	18/05/2023	24/05/2023	6,0	0%
Valoración de riesgos, requerimientos legales y de protección de datos	24/05/2023	28/05/2023	4,0	0%
Identificación de los principales hallazgos y conclusiones del estudio	28/05/2023	01/06/2023	4,0	0%
Determinar posibles lineas de trabajo futuras	01/06/2023	04/06/2023	3,0	0%
Documentación final	04/06/2023	14/06/2023	10,0	
Presentación en video	**14/06/2023**	**20/06/2023**	7,0	0%
Preparación del guion	14/06/2023	19/06/2023	5,0	0%
Grabación y edición del video	19/06/2023	21/06/2023	2,0	0%
Defensa	**26/06/2023**	**30/06/2023**	5,0	0%

Figura 2: Gantt con la planificación del trabajo.

1.6. Breve sumario de productos obtenidos

De este trabajo se obtienen los siguientes productos:

- Un informe del estado del arte que incluye las herramientas disponibles para la protección de los menores de edad en el ámbito escolar y familiar, con una evaluación teórica y práctica de su eficacia.
- Un informe de los principales riesgos a los que están expuestos los menores en Internet.
- Un análisis de las posibles arquitecturas de red donde se puede implantar un firewall DNS para la protección de los menores de edad en el ámbito escolar y familiar.
- Una lista de requerimientos a cubrir en la implementación de un firewall DNS para la protección de los menores de edad en el ámbito escolar y familiar.
- Un informe detallado de la evaluación teórica y práctica de las herramientas que han pasado el cribado, con valoraciones individualizadas, resultados y conclusiones.
- Un análisis del coste y del beneficio del uso de un firewall DNS en el ámbito escolar y familiar para proteger a los menores.
- Un análisis de las vulnerabilidades y de las salvaguardas, mitigaciones y contramedidas del firewall DNS.
- Ejemplos y recomendaciones para implementar de distintas herramientas firewall DNS.

1.7. Breve descripción de los otros capítulos de la memoria

Los capítulos de esta memoria se estructuran secuencialmente, siguiendo la metodología y planificación ordenada descrita en este capítulo. Para ello los siguientes capítulos se estructuran de la siguiente manera:

2. Investigación
    - Estado del Arte
    - Perfiles de usuario
    - Dispositivos, servicios y amenazas
    - Arquitecturas y topologías de red
    - Requerimientos del Firewall DNS para la protección del menor.
    - Evaluación de distintos Firewall DNS.
    - Análisis comparativo
3. Implantación
    - Arquitectura del entorno en laboratorio
    - Implementación practica de los Firewall DNS
4. Análisis de resultados y valoración de riesgos
    - Análisis de los resultados obtenidos
    - Valoración de los riesgos del Firewall DNS
    - Estudio de los requerimientos legales y de protección de datos
5. Conclusiones
6. Líneas de trabajo futuras.

1.8. Riesgos durante la realización del trabajo

Se identifican los siguientes riesgos que pueden materializarse durante el desarrollo de la investigación:

- Exposición de datos personales y/o sensibles de los usuarios con los que se comparte la conexión a internet durante las pruebas de laboratorio.
  Mitigaciones: Se notifica a los usuarios de los periodos en que se van a realizar las pruebas y se les informa de los datos que se van a recopilar durante esos periodos, se anonimizan o eliminan los datos no anónimos para su estudio y procesado.

- Riesgo de bloquear contenido legítimo y relevante y riesgo de interrupción en el servicio de internet.
  Mitigaciones: Se notifica a los usuarios de los periodos en que se van a realizar las pruebas y se les resolverán las incidencias en el menor plazo de tiempo posible.

- Insuficientes conocimientos técnicos o experiencia para implementar, configurar y administrar algunas herramientas firewall DNS.
  Mitigación: Se llevan a cabo investigaciones exhaustivas previa verificación de disponibilidad de documentación suficiente de las herramientas en cuanto a su puesta en servicio para ser candidatas a su selección, descartando aquellas herramientas no suficientemente documentadas.

- Costes de uso o licenciamiento de herramientas no previstos.
  Mitigación: Se seleccionarán únicamente herramientas opensource o opensource. Se busca una solución sea con coste gratuito o con el mínimo coste y que sea sencilla de implementar en hogares y escuelas.

Además de los riesgos mencionados anteriormente, existen otros factores que pueden afectar al desarrollo del trabajo concretamente el hecho de compaginar el trabajo con los estudios. Mitigaciones: Es posible que los plazos deban ser ajustados o que el trabajo tenga que ser simplificado debido a las limitaciones de tiempo.

2. Materiales y métodos

2.1. Estado del arte

2.1.1. Que es y para qué sirve un Firewall DNS

DNS o sistema de nombres de dominio es, según la RFC1035, el mecanismo que permite a un usuario o equipo obtener la dirección IP asociada a un nombre de un equipo en particular en la red. Un resolutor DNS o servidor DNS es aquel servicio que, en base al nombre de un equipo (también denominado host), devuelve sus direcciones IP asociadas y que son necesarias para establecer conexión de red con dicho host.

Un firewall DNS es un tipo de firewall que basa su sistema de protección en el sistema de nombres de dominio (DNS) haciendo posible filtrar el tráfico de la red, facilitando o denegando la resolución DNS correcta para sitios de internet específicos.

Los firewalls DNS basan su funcionamiento en actuar como el resolutor de DNS de los equipos de la red o subred que protegen, resolviendo las consultas en base a reglas de configuración definidas y haciendo de intermediarios de las resoluciones basándose bien en una lista que mantienen localmente, haciendo de intermediarios a otro resolutor DNS o una combinación de ambas.

Su principal objetivo es proteger a los equipos y usuarios de:
- Ataques de phishing y sitios difusores de malware
- El rastreo de la navegación de los usuarios y el bloqueo de anuncios.
- El acceso a categorías de sitios web no deseados por su posible contenido.

El uso de firewalls DNS es, en general, fácil de implementar, no requiere una inversión excesiva y es una medida bastante eficaz que puede combinarse con otras medidas para aumentar la seguridad de los equipos y usuarios de la red. Además, muchas de las herramientas firewall DNS disponibles permiten integrarse fácilmente en infraestructuras de red existentes sin requerir de hardware adicional.

Sus principales ventajas son:
- Mejoran la seguridad al bloquear el acceso a sitios maliciosos.
- Previenen y dificultan el rastreo en línea.
- Aumentan el ancho de banda disponible, al disminuir el tráfico innecesario, generado por anuncios, rastreadores o transmisiones de telemetría y estadísticas de uso innecesarias de ciertos softwares o sistemas operativos.
- Mejoran la experiencia del usuario al navegar, pues cuando disponen de una caché de consultas DNS aumentan la velocidad de respuesta, reducen la latencia en el proceso al reducir las consultas a los servidores DNS externos.
- Sencillez de uso y configuración.
- Facilitan estudios de actividad y conectividad de la red local.

Por el contrario, sus principales inconvenientes:
- Posibilidad de falsos positivos y negativos.
- Dependencia de terceros por las listas de sitios bloqueados o categorías.
- Problemas de privacidad, el administrador del servicio puede acceder a los datos de navegación y uso de internet de los usuarios.

2.1.2. Tendencias en Firewall DNS

Hay multitud de proveedores comerciales que ofrecen soluciones de firewall DNS, desde empresas de seguridad de prestigio como Cisco, Palo Alto Networks, Check Point Software Technologies o Fortinet. También lo ofrecen proveedores de servicios en la nube como Amazon Web Services (AWS) o Microsoft Azure. De la misma manera, existen muchas soluciones de la comunidad de código abierto y que son accesibles de forma universal y sin coste en licenciamiento como son Pi-Hole, Adguard Home o pfBlockerNG.

Algunas de las tendencias más importantes actualmente en el estado del arte de los firewalls DNS son:

- Integración con otros sistemas de seguridad para mejorar la protección y proporcionar una capacidad de respuesta integral ante las amenazas. Para ello se busca la interoperabilidad con otros sistemas de seguridad, como soluciones de protección del tipo Endpoint, cortafuegos tradicionales, SIEMs o soluciones de análisis de seguridad.

- Filtrado por ubicación: consiste en determinar la ubicación de los hosts a los que se desea acceder, aplicando filtros en función de su geolocalización.

- Filtrado por algoritmos: consiste en dar pesos determinados a indicadores de amenazas, como consultas muy recurrentes, en localizaciones sospechosas, con nombres de dominio no habituales, etc. Cuando la combinación de estas variables supera cierto umbral el firewall DNS bloquea el acceso.

- Segmentación de redes: consiste en permitir bloquear cierto tráfico en segmentos específicos de la red, mientras permiten que otros segmentos tengan acceso a recursos específicos distintos. Una aplicación en el contexto de este trabajo es disponer de un segmento de red para los alumnos con una configuración de políticas y otro segmento para profesores o padres con otra configuración.

- Acceso a datos de inteligencia de amenazas de fuentes externas. Estos datos pueden incluir información sobre sitios web o direcciones IP maliciosas y otros indicadores de compromiso como la geolocalización, así como el uso de listas negras para bloquear el acceso a sitios web ya conocidos por alojar malware, phishing y otros tipos de amenazas.

- Gestión centralizada: se persigue disponer de plataformas de gestión centralizada que permitan controlar múltiples dispositivos desde una sola interfaz y simplificar su gestión y mantenimiento.

- Personalización de políticas de seguridad para adaptarse a las necesidades específicas del entorno a proteger, incluyendo la capacidad de permitir o bloquear el acceso a sitios web específicos o establecer políticas de filtrado de contenido en función del equipo o usuario, a los que el Firewall DNS tiene identificados.

- Tecnología predictiva basada en inteligencia artificial, como la de bfore.ai. [93]

2.1.3. RPZs, categorización de sitios e información para firewalls DNS

Existen diversos sistemas de categorización de sitios web que se utilizan para clasificar y etiquetar el contenido de manera uniforme y coherente. Estos estándares permiten a los motores de búsqueda, navegadores web, Firewalls DNS y otros sistemas de seguridad a clasificar los usos y contenidos de las URLs.

Uno de los primeros estándares fue el discontinuado Internet Content Rating Association (ICRA), creado en 1996 por la Asociación Internacional de Proveedores de Servicios de Internet (ISPA). Se basa en etiquetas en los sitios web. ICRA utiliza un conjunto de categorías temáticas que se pueden aplicar a cualquier tipo de contenido web, como violencia, desnudez, lenguaje ofensivo, etc.

PICS (Platform for Internet Content Selection) es un sistema del W3C para etiquetado de contenido web que permite clasificar los sitios web en función de su contenido. PICS es compatible con varios sistemas de categorización de contenido web, incluyendo ICRA. PICS ha sido sucedido por el estándar POWDER (Protocol for Web Description Resources), también del W3C.

Lamentablemente, como se puede comprobar, cada fabricante adopta su propio sistema de categorización:

- OpenDNS (https://domain.opendns.com)
  - Propietario: Cisco.
- Palo Alto Networks - PAN-DB (https://urlfiltering.paloaltonetworks.com/query)
  - Propietario: Palo Alto Networks
- URL Filtering (URL Categorization | Check Point Software Technologies)
  - Propietario: Checkpoint
- URLFilterDB (https://urlfilterdb.com/products/urlfilterdb.html)
  - Propietario: URLFilterDB
- SiteAdvisor y McAfee Web Gateway (https://sitelookup.mcafee.com)
  - Propietario: McAfee (parte de Intel Security)
- Blue Coat y Symantec Web Security (https://sitereview.bluecoat.com)
  - Propietario: Symantec (ahora Broadcom)
- Fortinet Web Filter (https://www.fortiguard.com/webfilter/categories)
  - Propietario: Fortinet
- Websense Web Filter (https://www.forcepoint.com/product/url-filtering)
  - Propietario: Forcepoint
- BrightCloud (https://www.brightcloud.com/tools/url-ip-lookup.php)
  - Propietario: Webroot (ahora Carbonite de OpenText)

Otros sistemas de categorización orientados al contenido de sitios web son:

- Lista de categorías de IAB, creada por la Interactive Advertising Bureau, se utilizan en la publicidad en línea, para ayudar a los anunciantes a enfocar sus campañas de publicidad a audiencias determinadas. (List of IAB Categories – AerServ)

- Protocolo de Autorregulación de la Alianza de Publicidad Digital (DAA). Es otro sistema de categorización específico para anuncios en línea. [47]

- RSACi (Recreational Software Advisory Council on the Internet): Sistema de clasificación de contenido web basado en el lenguaje empleado y es compatible con varios sistemas de etiquetado de contenido web, incluyendo PICS.[45] [73]

- Safesurf [50], diseñado por una organización de madres y padres, que consta de categorias y subcategorías. [73]

Cuanto a las Response Policy Zones (RPZs), fueron desarrolladas como un mecanismo de filtrado para hacer frente al uso indebido del DNS, que extiende el uso de datos de reputación al sistema de nombres de dominio y fue publicado como un estándar abierto. RPZ nace como un componente del Servidor DNS BIND.

Mediante el uso de RPZ se puede filtrar el acceso a ciertos dominios de internet o redirigir las respuestas DNS a otros equipos. Un ejemplo claro del uso de la reputación en el filtrado es con los dominios de reciente creación que no han podido ser verificados, pero existen listas por categorias como piratería, ramsonware, drogas...

Existen listas públicas de sitios web, URLs e IPs para aplicar a aquellos Firewall DNS que admiten datos de configuración de fuentes externas, por ejemplo:

Nombre	Descripción	URL
AdAway Hosts File	Mantenida por el proyecto AdAway. Licencia GPLv3.	https://adaway.org/hosts.txt
AdGuard DNS filter	Mantenida por AdGuard. Licencia GPLv3.	https://github.com/AdguardTeam/AdGuardSDNSFilter/tree/master/Filters
Blocklist Project	Mantenida por The Blocklist Project. Licencia unlicense.	https://github.com/blocklistproject/Lists
Blocklist.de	Ofrecen listas de bloqueo de dominios e IPs que se han reportado con actividades sospechosas o malware.	https://www.blocklist.de/en/export.html
DShield Block List	La lista es mantenida por el proyecto DShield. Licencia CC BY-NC-SA 4.0	https://www.dshield.org/block.txt
EasyList	Mantenida por la comunidad de usuarios de AdBlock. Licencia GNUGPL.	https://easylist.to/easylist/easylist.txt
Fanboy's List	Mantenida por un usuario de la comunidad de AdBlock. Licencia GNUGPL.	https://fanboy.co.nz/
Firebog	Varias listas mantenidas por Wally3K. Utilizada por Pi-Hole. Licencia MIT.	https://firebog.net/
FireHOL IP Lists	Mantenidas por proyecto FireHOL. Licencia GNUGPL.	https://github.com/firehol/blocklist-ipsets
iblocklist.com	Mantenida por la empresa IBlocklist LLC. Algunas listas son gratuitas y otras de suscripción.	https://www.iblocklist.com/lists.php
Ioc2rpz.net	Ioc2rpz community. Licencia Apache2.	https://github.com/Homas/ioc2rpz
Notracking	Mantenidas por el proyecto Notracking. Licencia GPLv3.	https://github.com/notracking/hosts-blocklists
SANS Internet Storm Center	Mantenida por SANS Internet Storm Center. Licencia Creative Commons.	https://isc.sans.edu/
Someonewhocares.org	Mantenida por Dan Pollock. Es gratuita.	https://someonewhocares.org/hosts/
Spamhaus	Mantenida por Spamhaus Project Ltd. Licencia Creative Commons.	https://www.spamhaus.org/
StevenBlack	Mantenida por StevenBlack. Lic. MIT.	https://github.com/StevenBlack/hosts
URLhaus	Mantenida por abuse.ch. Licencia Creative Commons.	https://urlhaus.abuse.ch/browse/
Yoyo	Mantenida por Wael Nasreddine. Licencia Creative Commons.	https://pgl.yoyo.org/as/serverlist.php?hostformat=hosts&showintro=0&mimetype=plaintext

Figura 3: Listas públicas de URLs e IPs para su uso con Firewalls DNS.

2.2. Perfiles de usuario

A continuación, se determinan los distintos perfiles y roles de usuarios desde el punto de vista del uso de un firewall DNS.

En un hogar familiar con menores, se identifican perfiles de usuarios con diferentes niveles de conocimiento, responsabilidades y de exposición a los riesgos de la red:

- Los padres o tutores: responsables de educar y supervisar el uso de Internet por parte de sus hijos. Deben adoptar y fomentar prácticas seguras de uso de Internet, establecer normas y límites en el uso de dispositivos electrónicos por parte de los menores y hacerles conscientes de los peligros y beneficios del acceso a Internet. Un Firewall DNS les proporciona filtrado por categorias, protección contra malware, phishing y privacidad contra el rastreo y la publicidad.

- Los menores:
    - Los niños: los más vulnerables a sufrir ciberacoso, grooming, sexting o robo de identidad a través de Internet. Necesitan orientación para navegar por Internet de forma segura y responsable. Tienen que aprender a proteger su información personal, no hablar con los desconocidos, no compartir imágenes, respetar a los demás en el ciberespacio y denunciar situaciones sospechosas o incómodas.

    - Los adolescentes: más activos en las redes sociales y en el uso de las aplicaciones móviles. Tienen mayor autonomía e interés por explorar contenidos. Pueden caer en conductas imprudentes o ilegales como el ciberbullying, el phishing o la piratería informática.

En lo que respecta a colegios o institutos, se identifican:

- Los profesores: los responsables de impartir conocimientos y competencias digitales a sus alumnos. Deben mantenerse al día sobre las amenazas del entorno digital e incorporar la ciberseguridad como parte del currículo educativo. Tienen que promover el uso seguro y ético de Internet, así como detectar posibles casos de ciberacoso o relacionados.

- Los alumnos: usuarios de Internet dentro del ámbito escolar. Deben seguir las normas y restricciones establecidas por el centro educativo para acceder a los Sistemas de Información así como al utilizar los ordenadores. También deben respetar la propiedad intelectual, la privacidad ajena y las leyes vigentes.

- El personal administrativo: Utilizan Internet durante su jornada laboral y como herramienta de trabajo. Un Firewall DNS les aporta protección contra el malware, el phishing y protección contra el rastreo.

- El responsable de informática: es el encargado del mantenimiento y gestión del sistema informático. Debe garantizar la disponibilidad, integridad y confidencialidad de los sistemas de información utilizados por profesores y alumnos, implantar medidas preventivas y mantener el firewall.

2.3. Dispositivos, Servicios y amenazas

Los dispositivos que deben protegerse son:

- Los **ordenadores, móviles o smartphones, tabletas** y otros dispositivos móviles que los menores puedan usar para acceder a Internet.
- Los **asistentes virtuales**, como Apple Siri, Amazon Alexa o Google Home, para evitar que los niños puedan acceder a contenido inapropiado o peligroso.
- **Routers de la red local**, para poder proteger la red interna en su conjunto y evitar que los menores puedan acceder a contenido inapropiado o peligroso.
- Las **cámaras de seguridad del hogar o de la escuela** [68], pues muchas cámaras en el mercado se conectan a plataformas en internet y se tiene en los objetivos evitar que los menores puedan ser vistos o vigilados por extraños.

En cuanto a los servicios, se identifican:

- **Páginas web,** incluyendo sitios de noticias, blogs, foros y otros sitios en línea que puedan contener contenido inapropiado o peligroso para los menores.
- **Redes sociales,** como Facebook, TikTok, Instagram o Twitter. Se busca evitar que los niños puedan ser víctimas de acoso, intimidación o explotación en línea.
- **Plataformas de streaming**, como Netflix, YouTube, HBO o Disney. Se pretende restringir que los niños puedan acceder a contenido inapropiado o peligroso.
- **Plataformas de gaming**, como Xbox Live, Nintendo Online o PlayStation Network, limitando así que los niños puedan acceder a contenido inapropiado o peligroso y evitar que se comuniquen con extraños en línea.
- **Aplicaciones de mensajería**, como WhatsApp, Telegram o Snapchat, para evitar que los niños puedan ser víctimas de acoso, intimidación o explotación en línea.

Con respecto a las amenazas objeto de este estudio se consideran:

- Acoso, como el grooming o el ciberbullying [66]
- Intimidación
- Explotación en línea, como con el sexting o la sextorsión [65].
- Contenido inapropiado, como contenido de carácter sexual o pornográfico.[66]
- Contenido peligroso, como juegos de azar y apuestas en línea.
- Robo de datos personales [67]
- Acceso no autorizado a la red wifi
- Acceso no autorizado a los dispositivos
- Robo de datos bancarios [67]
- Malware
- Phishing

2.4. Arquitecturas y topologías de red

Las topologías de red que pueden encontrarse en el ámbito de aplicación del Firewall DNS son:

PAN: del inglés “Personal Area Network”, es una red que se constituye en torno a una persona y conecta los dispositivos electrónicos dentro de su área de alcance. Ejemplos de dispositivos que pueden encontrarse en esta red son teléfonos móviles, smartwatches, tabletas, ordenadores portátiles, sensores de actividad corporal...

El dispositivo que enlaza con internet es el punto donde debe actuar el Firewall DNS para asegurar que se cubre al resto de dispositivos de la PAN.

Para proteger los dispositivos de una red PAN utilizando Firewall DNS, se pueden seguir las siguientes estrategias:

- Instalar el Firewall DNS en el dispositivo que se conecta a Internet y la proporciona al resto de dispositivos.
- Configurar la IP del firewall DNS como resolutor de nombres en el dispositivo que se conecta a internet. Esto puede ser:
    - Apuntando a una maquina directamente en internet.
    - Configurando el Firewall DNS en un servidor en el cloud.
    - Implementando una política de VPN "always on" que garantice que todas las comunicaciones se realicen a través del Firewall DNS de la red del hogar o la escuela donde siempre se estaría conectado por VPN.

LAN (Local Area Network), es una red que conecta los dispositivos electrónicos en un área local, como una oficina, una escuela o un hogar. Se considera que la WLAN (o Wireless LAN) y los dispositivos conectados a ella están incluida en la topología LAN. Algunos ejemplos de dispositivos que se pueden encontrar en esta red son ordenadores de sobremesa o portátiles, móviles (teléfonos y tabletas), Impresoras, consolas de videojuegos, SmartTVs, dispositivos IoT…

Para proteger los dispositivos de una red LAN utilizando Firewall DNS, se pueden seguir una o varias de las siguientes estrategias:

- Propagar la dirección del Firewall DNS automáticamente por DHCP o configurar manualmente en cada equipo.
  Para este trabajo se valoran ambas opciones
- Instalar el Firewall DNS el router de salida a internet: algunos routers tienen la capacidad de actuar como Firewall DNS, aunque con funcionalidades generalmente más limitadas. Esta opción suele implicar cambiar el router de la compañía proveedora del acceso a internet, lo que suele se complejo y costoso.
  Para este trabajo se valora si se puede instalar en un router con firmware opensource OpenWRT o DDwrt.
- Instalar el Firewall DNS en un servidor. Puede utilizarse un pequeño equipo dedicado como una Raspberry Pi o una máquina virtual en un servidor.
  Para este trabajo se prueba en una Raspberry Pi o en una máquina virtual dentro de la red local o en la nube.
- Implantarlo en un dispositivo intermedio o firewall: se puede utilizar un dispositivo independiente como Firewall DNS, que se conecta entre el router y la red local. Esta arquitectura ofrece una protección más avanzada y personalizable, dado que combina distintas medidas de seguridad al permitir, por ejemplo, bloquear la consulta a servidores DNS no autorizados.
  Para este trabajo se prueba y evalúa en un Intel Celeron con pfSense.

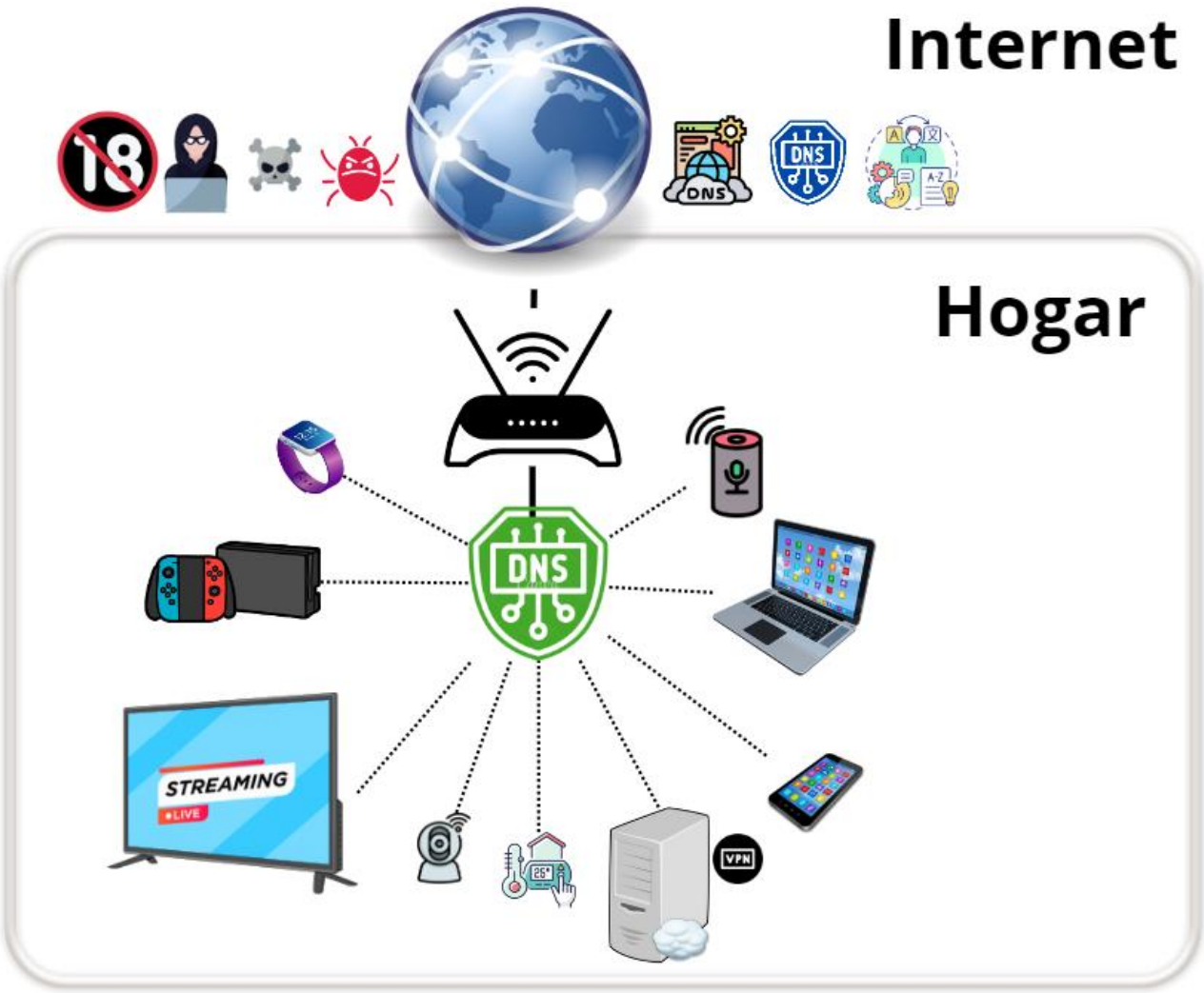


Figura 4: Diagrama de ítems que intervienen en el proyecto.

2.5. Requerimientos

En este capítulo se identifican los requerimientos deseables en un firewall DNS para la protección de los menores. Estos son los siguientes:

- **Bloqueo de sitios web:**
  - Permitir el bloqueo de sitios web inapropiados o peligrosos. [46]
- **Bloqueo de descarga:**
  - Bloquear la descarga de archivos peligrosos o no autorizados.
- **Registro de actividad y reportes:**
  - Registrar la actividad de navegación del menor.
  - Soporte de informes y análisis detallados de uso de DNS.
- **Bloqueo de redes sociales:**
  - Limitar el acceso a redes sociales y mensajería instantánea.
- **Bloqueo de contenidos:**
  - Bloqueo de contenidos violentos, sexuales, discriminatorios o ilegales.
  - Soporte de políticas de filtrado basadas en categorías de sitios web.
  - Reglas de acceso basadas en la ubicación geográfica del destino.
- **Bloqueo de enlaces:**
  - Bloquear los enlaces presentes en correos tipo phishing o spam.
- **Control por tiempo:**
  - Personalizar el filtrado por franjas horarias o por días de la semana.
- **Protección contra malware:**
  - Proteger contra ataques de phishing y malware. [46]
- **Perfiles de usuario**:
  - Configuración personalizable según perfiles de usuario.
  - Soporte de autenticación de usuarios y dispositivos.
- **Compatibilidad**:
  - Soporte para múltiples dispositivos, plataformas y sistemas operativos.
- **Bloqueo de aplicaciones:**
  - Capacidad de bloquear aplicaciones concretas en dispositivos móviles.
- **Monitorización:**
  - Monitorización de la actividad en tiempo real
- **Envío de Alertas:**
  - Capacidad de generar alertas en tiempo real por posibles amenazas.
- **Actualización automática:**
  - Actualización automática de la lista de sitios peligrosos e inapropiados.
- **Bloqueo parental:**
  - Permitir establecer un bloqueo de seguridad parental por contraseña.
- **Listas blancas y listas negras:**
  - Soporte de listas negras y blancas de direcciones IP y de dominios.
- **Integración:**
  - Capacidad de integración con antivirus, syslog, SIEM, etc.
- **Caché de consultas:**
  - Soporte de la resolución de nombres de dominio en caché.
- **Bloqueo de DNS externos:**
  - Capacidad de bloqueo de consultas DNS a servidores no autorizados o en direcciones IP específicas.
- **Página de bloqueo customizable:**
  - Capacidad de mostrar una página a medida para informar del bloqueo.
- **Incorporar servidor DHCP:**
  - Incorporar un servidor DHCP integrado para facilitar el despliegue.

2.5.1. Requerimientos en los centros educativos

Se identifica el siguiente requerimiento adicional a los del capítulo anterior:

- **Protección de datos personales**: Los colegios deben garantizar la protección de los datos personales de los estudiantes mientras utilizan sus sistemas de información. Esto incluye, en el caso que estén permitidas, el uso responsable de las redes sociales y otras herramientas en línea, así como la prevención del rastreo y garantizar su derecho a la privacidad, lo que incluye el tratamiento de los registros de actividad DNS.

Adicionalmente, se considera conveniente mencionar en este capítulo el hecho de que los colegios pueden y deben proporcionar formación en ciberseguridad a los estudiantes y al personal docente. Esto incluye enseñar a los estudiantes sobre los riesgos en línea y cómo protegerse de ellos. La Ley Orgánica de Protección de Datos, en su artículo 83, establece el derecho a la educación digital estableciendo “en el desarrollo del currículo la competencia digital” y “los elementos relacionados con las situaciones de riesgos derivadas de la inadecuada utilización de las TIC”. [69] El INCIBE dispone de un programa de formación en centros educativos para mejorar las competencias digitales del profesorado y del alumnado en ciberseguridad. [70]

2.6. Herramientas Firewall DNS

En esta sección se hace una descripción y un análisis de las principales características de los Firewall DNS más conocidos, tanto comerciales, como gratuitos, como opensource y que se han considerado relevantes al obtenerlos durante la búsqueda e investigación para el análisis del estado del arte.

2.6.1. Akamai ETP

URL: https://www.akamai.com/products/secure-internet-access-enterprise

Akamai Enterprise Threat Protection y su producto Secure Internet Access Enterprise incluye funcionalidades de Firewall DNS, combinadas con otras tecnologías como DLP o análisis de payloads.

Es una infraestructura DNS externa basada en el cloud que busca mejorar las defensas contra las amenazas dirigidas. Está diseñado para ayudar a identificar los datos que se filtran mediante DNS, y para identificar y mitigar phishing, ataques de malware, ransomware y malware. También puede identificar la categoría de contenido del dominio solicitado y bloquear el acceso a contenido o dominios inapropiados. [98]

Admite filtrado de contenidos seleccionables por el usuario.

Es una solución de pago y orientada a empresas.

2.6.2. Cisco Umbrella

URL: https://umbrella.cisco.com/products/cloud-security-service

Cisco Umbrella es una solución de seguridad en el cloud. Está orientada a proteger a las empresas de las amenazas de internet y permite el filtrado de contenidos y de aplicaciones así como protección contra el malware y el phishing. Dispone de una red

de servidores distribuida por todo el mundo y se integra con los demás productos de seguridad de Cisco, añadiendo capas adicionales de protección de ciberseguridad.

Al ser basada en la nube es una solución relativamente sencilla de implementar y no requiere hardware adicional si no se va a combinar con otros productos de Cisco.

Es una solución de pago y orientada a empresas.

Security & Controls			DNS Security Advantage	SIG Advantage NEW
DNS-Layer Security	Block domains for malware, phishing, botnet, and other high risk		✓	✓
	Block domains from Cisco SecureX, direct integrations (Splunk, Anomali, & others), and custom lists using enforcement API		✓	✓
	Block direct-to-IP traffic for C2 callbacks that bypass DNS*1		✓	✓
Secure Web Gateway (SWG)	Proxy web traffic for inspection [Decrypt and inspect SSL (HTTPS) traffic]		Risky domains only	✓
	Enable web filtering	Of domains	✓	✓
		Of URLs		✓
	Create custom block/allow lists	Of domains	✓	✓
		Of URLs		✓
	Block URLs based on Cisco Talos and other feeds; block files based on AV Engine and malware defense		Risky domains only	✓
	Use Secure Malware Analytics (sandbox) on suspicious files			Unlimited samples
	Use retrospective security to identify previously-benign files that became malicious			✓
Cloud Access Security Broker	Discover and block shadow IT with App Discovery report	Of domains	✓	✓
		Of URLs		✓
	Create policies with more granular controls (block uploads, attachments, and posts) for select apps			✓
	Scan and remove malware from cloud-based file storage apps NEW			All supported applications
Cloud-Delivered Firewall (CDFW)	Create layer 3/layer 4 policies to block specific IPs, ports, and protocols			✓
	Deepen protection for outbound traffic using application layer 7 policies with intrusion prevention system (IPS) NEW			✓
	Use IPsec tunnel termination			✓
Data Loss Prevention (DLP)	Enable inline inspection of web and cloud app traffic for sensitive data NEW			✓
Remote Browser Isolation (RBI)	Provide safe access to risky sites, web apps and all web destinations NEW			Add-on
XDR and Threat Intelligence	Integrate with SecureX to aggregate activity across Cisco products	Reporting & enforcement APIs	✓	✓
		All APIs	✓	✓
	Access Umbrella's deep domain, IP, and ASN data for rapid investigations		✓	✓

*1 Endpoint footprint (Umbrella Roaming Client, Umbrella Chromebook Client, or Umbrella Roaming Security Module for AnyConnect) is required.

Figura 5: Cuadro resumen de funcionalidades de Cisco Umbrella. [95]

2.6.3. Palo Alto DNS Security

URL: https://www.paloaltonetworks.com/resources/datasheets/dns-security-service

Palo Alto Networks ofrece una solución de seguridad de DNS llamada "DNS Security" que se enfoca en proteger a las empresas de las amenazas a nivel DNS.

A pesar de que su solución está en el cloud, se requiere de sus Firewalls hardware para su uso.

Admite filtrado de contenidos seleccionables por el usuario e incorpora analítica predictiva con "*machine learning*".[96]

Es una solución muy completa, pero es de pago y muy orientada a empresas.

Feature	Description
ML-Based Inline Protection	Uses ML-based analysis to identify advanced DNS-based threats (listed under DNS security detectors).
Cloud Database	Contains tens of millions of known malicious domains, enabling you to block phishing, malware, and other high-risk categories.
DNS Security Analytics	Provides threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time.
DNS Sinkholing	Enables you to forge a response to a DNS query for a known malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client. Client attempts to access the sinkhole address can be logged and trigger automated actions (e.g., quarantine). This technique can be used to identify infected hosts on the network.
DNS Security Categories	Allows you to define separate policy actions as well as a log severity level for a specific signature type. You can create specific security policies based on the nature of a threat (e.g., C2, dynamic DNS, malware, newly registered domain, phishing, grayware, parked domain, proxy avoidance, and anonymizers) according to your network security protocols.
DNS Security Detectors	
Domain Generation Algorithm (DGA)	Identifies the use of DGAs, which generate random domains on the fly for malware to use as a way to call back to a C2 server.
Dictionary DGA	Identifies DGA domains based on dictionary words.
DNS Tunneling	Prevents the use of this technique, which exploits the DNS protocol to tunnel malware and other data through a client-server model.
Ultra-Slow DNS Tunneling	Disrupts ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network.
Strategically Aged Domains	Predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors.
Fast Flux Domains	Prevents fast flux, a technique cybercriminals use to cycle through bots and DNS records. Fast flux networks are used for phishing, malware distribution, scams, and botnet operations.
Compromised Domain Zones	Protection from domains surreptitiously added to hacked DNS zones of reputable domains.
DNS Rebinding Attacks	Prevents DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet.
Dangling DNS Attacks	Prevents dangling DNS attacks, which take advantage of stale DNS zone data to take over domains and cause reputational harm or launch phishing attacks.
Wildcard DNS	Prevents attackers from directing users to malicious domains with the use of a wildcard DNS record.
DNS infiltration	Prevents technique that exploit DNS protocol to tunnel malicious payloads into your network.
NXNS Denial-of-Service Domains	Protects users from connecting to domains that can be used to launch DDoS attacks.
Malicious Newly Registered Domains (NRD)	Uses predictive analysis to identify domains registered by malicious actors at the time of registration.

Figura 6: Cuadro resumen de funcionalidades de Palo Alto DNS Sec. [97]

2.6.4. Check Point Secure Web Gateway

URL: https://www.checkpoint.com/harmony/connect-sase

Check Point ofrece una solución en línea para empresas que cubre el filtrado de contenido y la protección contra malware.

Harmony de Check Point es una solución muy completa que se integra con el resto de los productos de seguridad de Check Point e incorpora una completa generación de informes del tráfico de peticiones DNS y uso de la conexión a internet, así como funcionalidades de investigación forense.

Admite filtrado de contenidos que permite establecer políticas distintas para cada usuario o grupos de usuarios.

Está basada en Appliances que se montan en la infraestructura de cada empresa.

	SWG-4400	SWG-4600	SWG-4800	SWG-12400	SWG-12600
					
Sizing					
Users (recommended)[1]	up to 250	up to 500	up to 1,000 users	up to 5,000 users	up to 10,000 users
Concurrent Connections	20,000	32,000	50,000	66,000	160,000
Connections per Second	650	1,000	1,800	2,500	5,700
HTTP Transactions per Second	2,700	4,200	7,000	10,000	22,000
System Resources					
Cores	2	2	4	6	12
Memory	4 GB	4 GB	8 GB	8 GB (up to 12 GB)	12 GB
Storage	250 GB	250 GB	250 GB	500 GB (up to 2x500 GB)	2x500 GB
Network Interfaces	8 x 10/100/1000Base-T RJ45 ports	8 x 10/100/1000Base-T RJ45 ports	8 x 10/100/1000Base-T RJ45 ports	2 on board 1GbE copper 8 x 1GbE copper interface card	2 on board 1GbE copper 4 x 1GbE copper interface card 8 x 1GbE copper interface card

Figura 7: Appliances de CheckPoint Secure Web Gateway [99]

Es una solución de pago y muy orientada a empresas.

2.6.5. DNSFilter

URL: https://www.dnsfilter.com/features/content-filtering

DNSFilter ofrece una solución comercial en línea para el filtrado de contenido y protección contra malware.

Es una solución de pago, pero está orientada tanto a hogares como a empresas y escuelas, con distintos niveles de servicio y precios.

Es de destacar su cumplimiento con la regulación CIPA (Children's Internet Protection Act), que busca la seguridad de los menores que se conectan a Internet en lugares públicos, con casos de éxito en distritos escolares de California. [100]

Figura 8: Categorias de filtrado de DNSFilter [101]

2.6.6. Comodo DNS Firewall

URL: https://www.comodo.com/secure-dns/

"Comodo" ofrece una solución en la nube para el filtrado de contenido y protección contra malware. Es una solución de pago, pero ofrece una versión gratuita limitada funcional y volumétricamente a 300000 consultas DNS al mes, lo que la hace extremadamente limitada.

La solución está más orientada a empresas, con distintos niveles de servicio y precios.

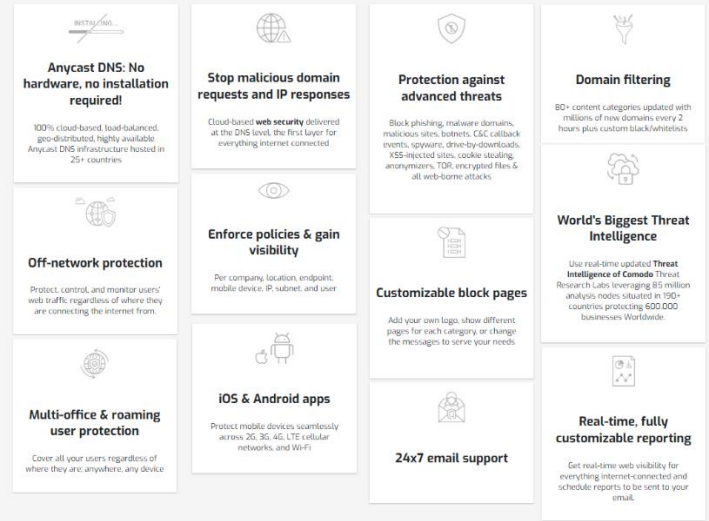


Figura 9: Prestaciones de Cómodo DNS Firewall [102]

2.6.7. OpenDNS

URL: https://www.opendns.com/home-internet-security/

OpenDNS, que fue adquirida por Cisco, además de soluciones de suscripción, ofrece varias soluciones gratuitas:

- OpenDNS Home: es un servicio para el hogar que proporciona protección contra malware, phishing y otros tipos de amenazas de seguridad en línea.

- OpenDNS Family Shield: es una solución diseñada específicamente para proteger a los niños de contenido inapropiado en línea.

Admiten filtrado de contenidos seleccionables por el usuario.

Las versiones empresariales se comercializan bajo la marca Cisco Umbrella, que lo adquirió en 2015, ver capítulo 2.6.2 Cisco Umbrella.

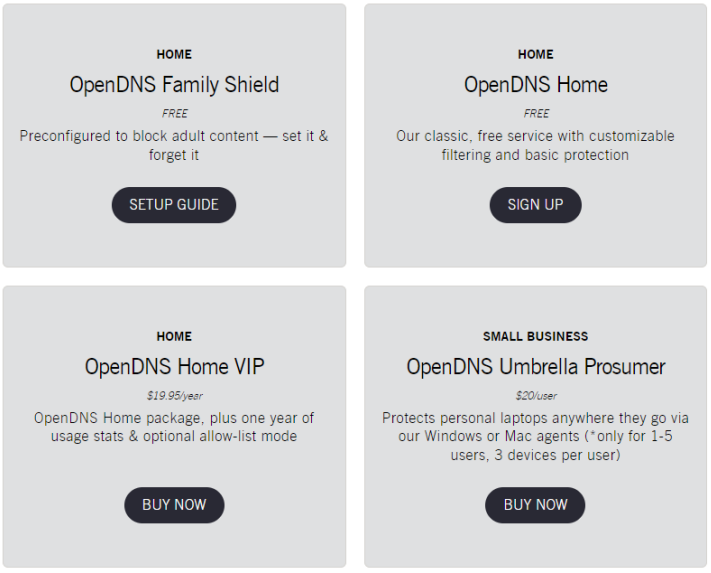


Figura 10: Modalidades de uso de OpenDNS [103]

2.6.8. Neustar UltraDNS

URL: https://www.publicdns.neustar/

Neustar ofrece varias soluciones basadas en la nube:

- Threat Protection: es un servicio gratuito contra dominios maliciosos.
- Family Secure: combina la protección anterior con protección para que los menores no accedan a contenidos para adultos.

No admite filtrado de contenidos seleccionables por el usuario, siendo categorias fijas determinadas por el propio proveedor.

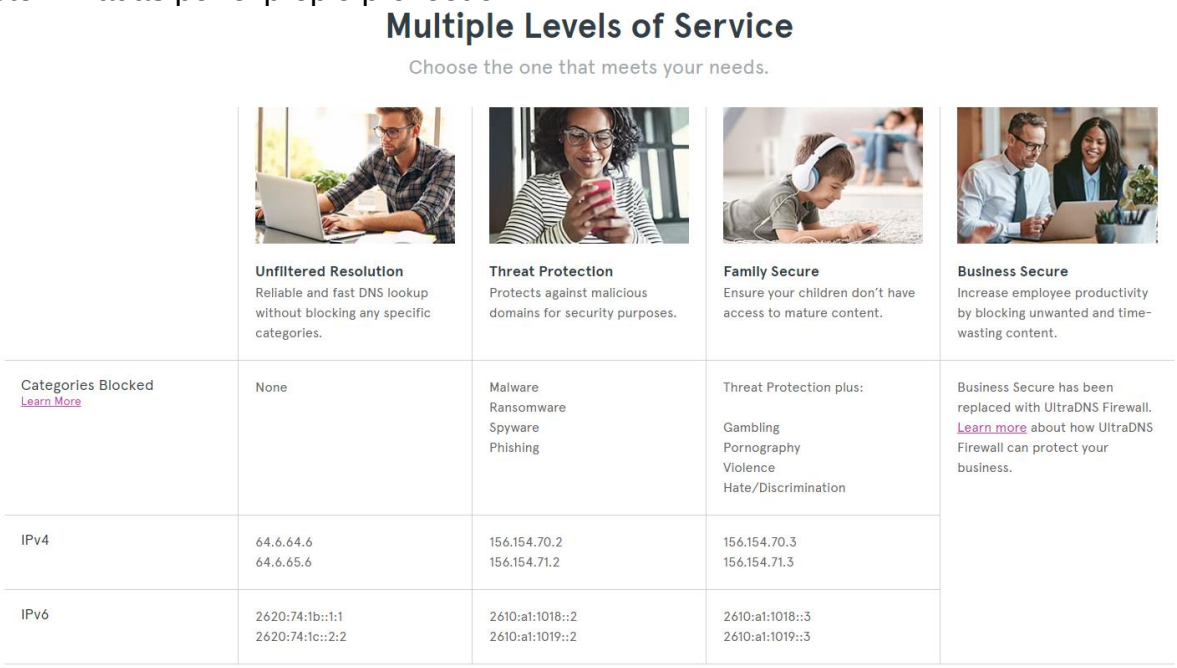


Figura 11: Opciones de servicio de UltraDNS [102]

2.6.9. Quad9

URL: https://www.quad9.net/

Quad9 DNS es un servicio gratuito de resolución de DNS basado en la nube.
Es una iniciativa sin fines de lucro creada por la Global Cyber Alliance e IBM, entre otras. Sus DNS bloquean los sitios web conocidos por alojar malware, spyware y phishing. No admite filtrado de contenidos seleccionables por el usuario.

Sus responsables aseguran no recopilar información de identificación personal de los usuarios y que no vende datos de usuarios a terceros.

2.6.10. BIND

URL: https://www.isc.org/bind/

BIND es un servidor DNS open source con licencia MPL 2.0 que se puede utilizar como un firewall DNS y proporciona trazabilidad de uso. BIND puede utilizar RPZ para establecer políticas de filtrado contra phishing, malware o filtrado de contenidos.

Requiere de un servidor físico o en el cloud donde instalarlo y configurarlo.

2.6.11. Dnsmasq

URL: https://www.isc.org/bind/

Dnsmasq es un servidor DNS y DHCP open source, con funcionalidades de caché para mejorar el rendimiento.

Dnsmasq soporta RPZs.

2.6.12. Knot-resolver

URL: https://www.knot-resolver.cz/

Knot-resolver es un servidor DNS similar a BIND, que admite RPZs para filtrar contenidos.

2.6.13. Pi-hole

URL: https://pi-hole.net/

Pi-hole es una herramienta de código abierto que se ejecuta generalmente en un servidor de la red local, actuando como resolutor DNS y puede bloquear anuncios, rastreadores, así como contenidos o malware y phishing a través de listas blancas y negras. Incorpora servidor DHCP.

Es fácil de integrar con herramientas de análisis de datos tratar los datos de tráfico.

No requiere suscripción ni licenciamiento y puede ser instalado en sistemas operativos basados en Linux.

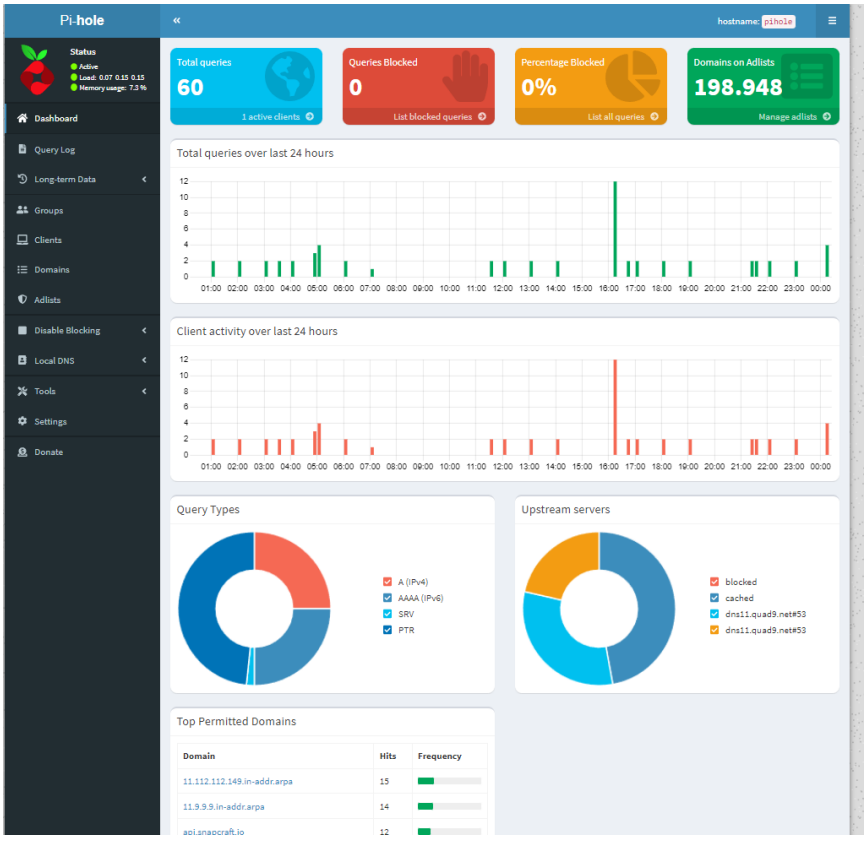


Figura 12: Interfaz de usuario de Pi-Hole

2.6.14. AdGuard Home

URL: https://github.com/AdguardTeam/AdGuardHome

AdGuard Home es una solución de código abierto de firewall DNS bloqueador de anuncios, malware, rastreadores y filtrado de contenidos.

Incorpora un servidor DNS y DHCP, así como una completa interfaz de configuración.

Utiliza filtros basados en dominios para bloquear el acceso a sitios web no deseados.

Es fácil de instalar y configurar, lo que lo hace muy práctico para el hogar.

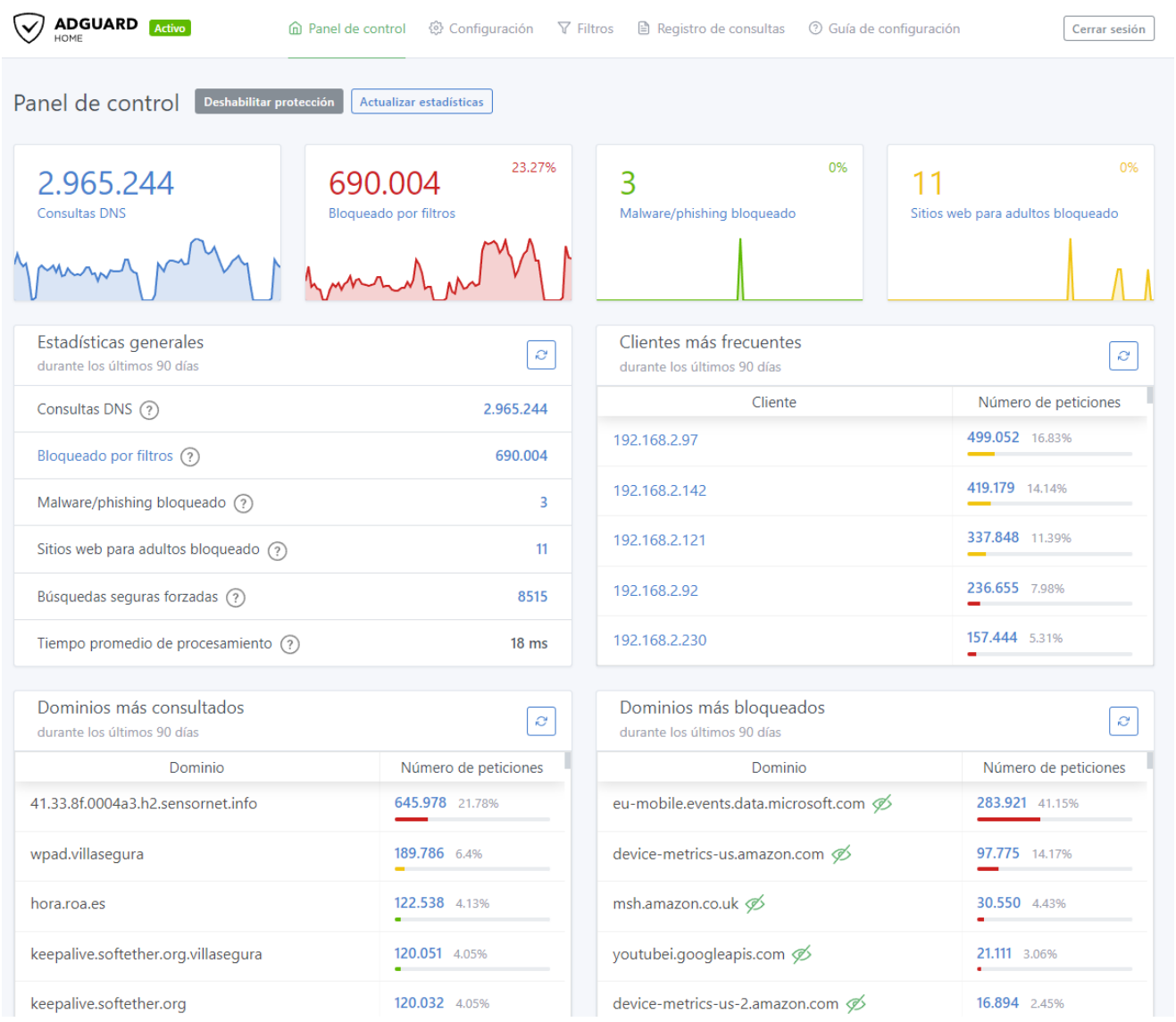


Figura 13: Interfaz de usuario de AdGuard Home

2.6.15. pfBlockerNG

URL: https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html

pfBlockerNG es un software gratuito basado en sistemas operativos FreeBSD y de código abierto que se añade como un plugin al firewall pfSense. Utiliza listas blancas y negras para bloquear y filtrar contenidos en internet en la capa DNS. Es una buena opción combinada con un firewall de bajo coste para el hogar o un colegio.

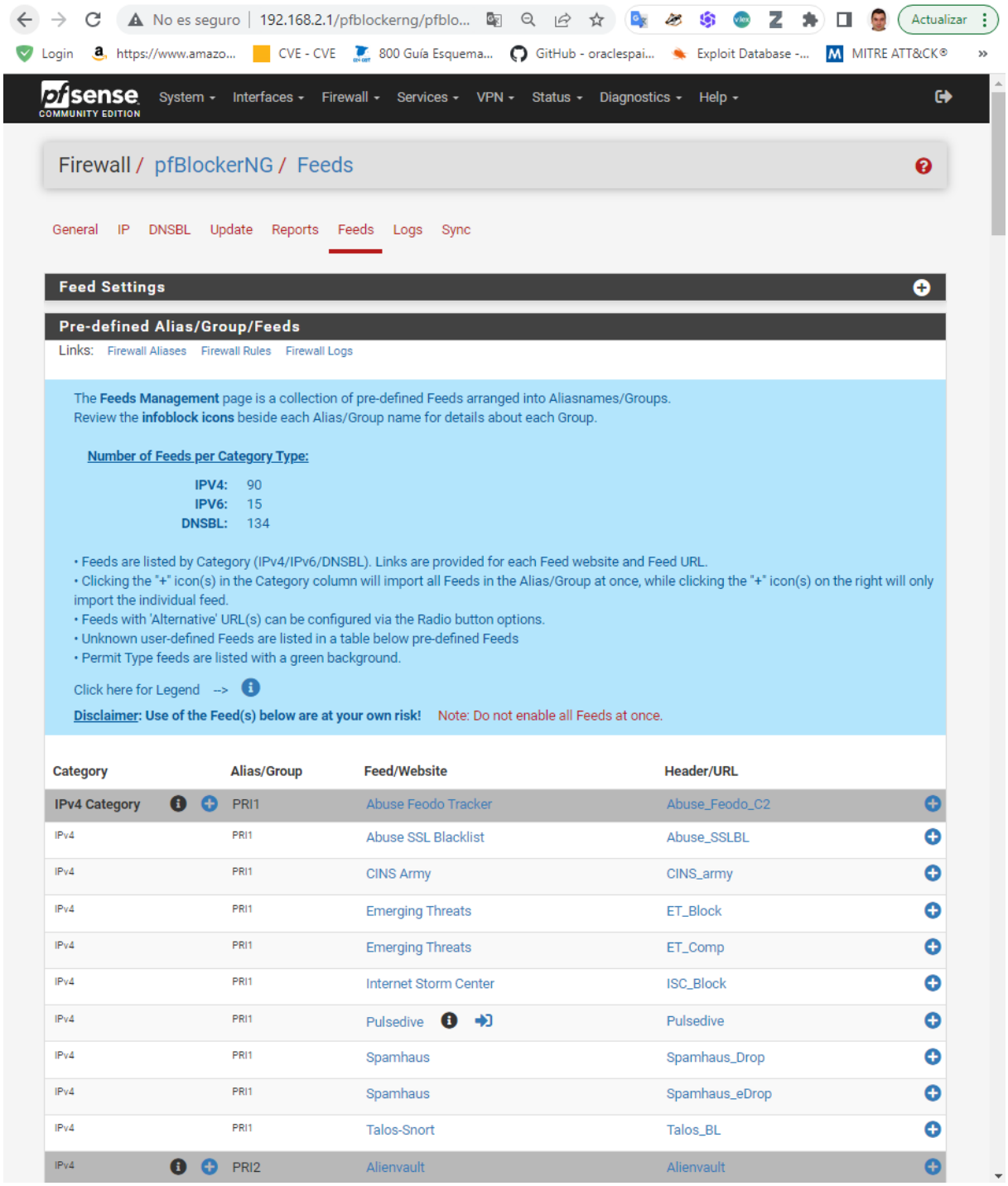


Figura 14: Interfaz de usuario de pfBlockerNG

2.7. Análisis comparativo

A continuación, se muestra una tabla con el análisis realizado en base a la información localizada y disponible en forma de datasheets, páginas web y/o manuales en línea para cada herramienta de las enumeradas en el capítulo anterior valorando su cumplimiento con cada uno de los requerimientos establecidos en el capítulo 2.5 Requerimientos.

La valoración del cumplimiento con cada requerimiento se ha considerado en una escala del 0 al 5 con el siguiente significado, que se adapta a cada fila valorada:

- 0: No cumple con el requerimiento.
- 1: Cumple con el requerimiento con muchas limitaciones.
  Cumplimiento muy limitado o indirecto o que puede requerir un esfuerzo muy elevado de integración con otras herramientas, un gran esfuerzo de desarrollo a medida o un esfuerzo económico significativo.
- 2: Cumple con el requerimiento de manera básica.
  Cumplimiento muy básico o a través de una integración previa con otras herramientas o ciertos desarrollos.
- 3: Cumple con el requerimiento de manera adecuada.
  Cumple, pero otras herramientas proporcionan más funcionalidades.
- 4: Cumple con el requerimiento de manera notable.
  Además de cumplir, proporciona mejoras sobre los mínimos exigibles.
- 5: Cumple con el requerimiento de manera excelente.
  No solo cumple el requerimiento de forma total, sino que adicionalmente destaca por su facilidad de uso, rendimiento, coste o innova en su forma de cumplirlo.

Las herramientas se agrupan en columnas según las siguientes cuatro tipologías:

- Herramientas de pago o con coste de suscripción que proporcionan servicios de Firewall DNS. Entran en esta categoría:
  - Cisco Umbrella
  - Palo Alto Networks
  - Akamai ETP
  - CheckPoint Firewall DNS
  - DNSFilter
- Herramientas o iniciativas gratuitas que proveen de un servidor DNS en la nube con funciones de Firewall DNS. En esta categoría se encuentran:
  - Cómodo DNS Firewall.
  - OpenDNS
  - Neustar UltraDNS
  - Quad9 DNS Firewall
- Servidores DNS de código abierto que se pueden configurar para realizar las funciones de Firewall DNS. En esta categoría se consideran:
  - BIND
  - Dnsmasq
  - Knot Resolver
- Herramientas especializadas de código abierto y gratuitas para su uso como Firewall DNS. En esta categoría se consideran:
  - Pi-Hole
  - AdGuard Home
  - pfBlockerNG

Peso	Requisito	Cisco Umbrella	Palo Alto Networks	Akamai ETP	CheckPoint Firewall DNS	DNS Filter	Comodo DNS Firewall*	OpenDNS**	Neustar UltraDNS	Quad9 DNS Firewall	BIND	dnsmasq	Knot Resolver	Pi-hole	AdGuard Home	pfBlockerNG
10	Bloqueo de sitios web	5	5	5	5	5	0	5	4	0	2	2	2	4	5	5
10	Bloqueo de descarga	4	5	4	5	4	3	3	3	3	1	1	1	4	4	4
10	Registro de actividad y reportes	5	5	5	5	5	4	5	0	3	4	3	4	4	5	5
10	Bloqueo de redes sociales	5	5	5	4	4	0	5	0	0	2	2	2	4	5	4
10	Bloqueo de contenidos	5	5	5	5	5	0	5	3	0	2	2	2	4	5	5
10	Bloqueo de enlaces	4	4	4	4	4	4	4	2	4	1	1	1	3	4	3
10	Control por tiempo	4	5	4	5	0	0	0	0	0	1	1	1	1	1	2
10	Protección contra malware	5	5	5	5	5	5	5	5	5	2	2	2	5	5	5
10	Perfiles de usuario	1	5	1	5	1	0	1	3	0	0	0	0	3	4	4
10	Compatibilidad	4	4	4	4	5	5	5	4	4	4	4	3	5	5	2
10	Bloqueo de aplicaciones	5	5	5	5	5	1	4	0	1	2	2	2	3	5	4
10	Monitorización en tiempo real	5	5	5	5	5	3	4	0	3	3	2	4	5	4	5
10	Alertas en tiempo real	4	5	3	5	2	3	1	0	3	2	2	2	1	4	4
10	Actualización automática	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5
10	Bloqueo parental	2	2	2	2	2	0	3	0	0	2	2	2	2	5	5
10	Listas negras/blancas	5	5	5	5	5	3	3	0	3	3	3	3	4	5	4
10	Integración	4	4	4	4	4	2	2	1	1	3	2	2	4	4	5
8	Caché de consultas	2	5	2	5	0	0	0	0	0	5	5	5	5	4	5
10	Bloqueo de DNS externos	3	5	3	5	0	3	0	0	3	2	2	2	3	3	4
30	Gratuito	0	0	0	0	0	1	5	5	5	5	5	5	5	5	5
20	Valoración uso en hogar	0	0	0	0	1	1	3	2	3	3	3	3	5	5	5
20	Valoración uso en escuela	1	1	1	1	1	1	3	2	3	3	3	3	5	5	5
8	Pagina de bloqueo customizable	5	5	5	5	5	5	5	0	0	1	1	1	5	5	5
20	No requiere hardware adicional	4	1	3	3	5	5	5	5	5	1	2	1	3	3	0
15	Utilizable desde el cloud	5	5	5	5	5	5	5	5	5	3	3	3	5	5	5
10	Protección iOS	4	4	4	4	3	2	3	2	2	2	2	2	4	4	4
10	Protección Android	4	4	4	5	3	3	3	2	3	2	2	2	4	4	4
15	Incorpora servidor DHCP	0	0	0	3	0	0	0	0	0	5	5	5	5	5	5
	TOTAL (promedio)	**3,57**	**3,89**	**3,50**	**4,07**	**3,18**	**2,29**	**3,29**	**1,89**	**2,29**	**2,50**	**2,43**	**2,46**	**3,93**	**4,39**	**4,21**
	TOTAL (aplicando pesos)	**3,16**	**3,32**	**3,07**	**3,57**	**2,90**	**2,22**	**3,41**	**2,22**	**2,60**	**2,67**	**2,64**	**2,64**	**4,05**	**4,44**	**4,20**
	Seleccionado para su evaluación	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓

0: No cumple con el requerimiento.
1: Cumple con el requerimiento pero con muchas limitaciones.
2: Cumple con el requerimiento de manera básica.
3: Cumple con el requerimiento de manera adecuada.
4: Cumple con el requerimiento de manera notable.
5: Cumple con el requerimiento de manera excelente.

* Comodo tiene una modalidad gratuita limitada a 300.000 consultas mes
** OpenDNS es gratuito para el hogar y ambito educativo

Gratuito
De pago

Figura 15: Análisis comparativo de los principales Firewalls DNS.

2.7.1. Conclusiones del análisis comparativo

Se han identificado multitud de herramientas que pueden aplicarse al objetivo de este trabajo y se han seleccionado cuatro de ellas que tienen enfoques y/o arquitecturas distintas que permitirían a un hogar o escuela proteger a los menores contra los contenidos inadecuados y contra las amenazas que pueden encontrar en internet.

Las herramientas seleccionadas tras el análisis son:

- Adguard Home, un servidor DNS con licencia GPL3 con muchas opciones de configuración, pero que requiere un hardware donde instalarlo. Se prueba en:
  - Máquina virtual en un NAS
  - Raspberry Pi
  - Máquina virtual en el cloud
- pfBlockerNG, una herramienta de filtrado que se integra en el firewall pfSense, con licencia Apache 2.0, puede implantarse en una máquina de bajo coste a la vez que provee capas adicionales de protección.
  Requiere el hardware del firewall pfSense.
- Pi-Hole, un Servidor DNS con licencia EUPL, que admite listas de dominios a partir de fuentes RPZ. Se prueba en:
  - Máquina virtual en un NAS
  - Raspberry Pi
  - Máquina virtual en el cloud
- OpenDNS, una solución gratuita que no requiere de infraestructura adicional. Ser prueba:
  - Como fuente DNS de las tres herramientas anteriores
  - Como solución independiente.

Las herramientas escogidas son probadas en laboratorio, y utilizadas por todos los dispositivos conectados a la red definidos en 2.3 Dispositivos, Servicios y amenazas.

Para cada una de las herramientas que se configuran y prueban, se analizan:

- Los registros de consultas efectuadas
- Las latencias y velocidad de respuesta
- La experiencia de usuario
- La facilidad de uso y de configuración para aplicar los requerimientos definidos
- Su seguridad y las posibles vulnerabilidades de cada solución, así como las mitigaciones aplicables.

3. Implantación

En este capítulo se describe el proceso seguido para la implantación del entorno de laboratorio, desde las modificaciones realizadas en la arquitectura de red existente hasta el proceso de instalación y configuración de los firewalls DNS analizados.

3.1. Arquitectura del entorno en Laboratorio

El entorno de partida es la red de un hogar, con la siguiente topología:

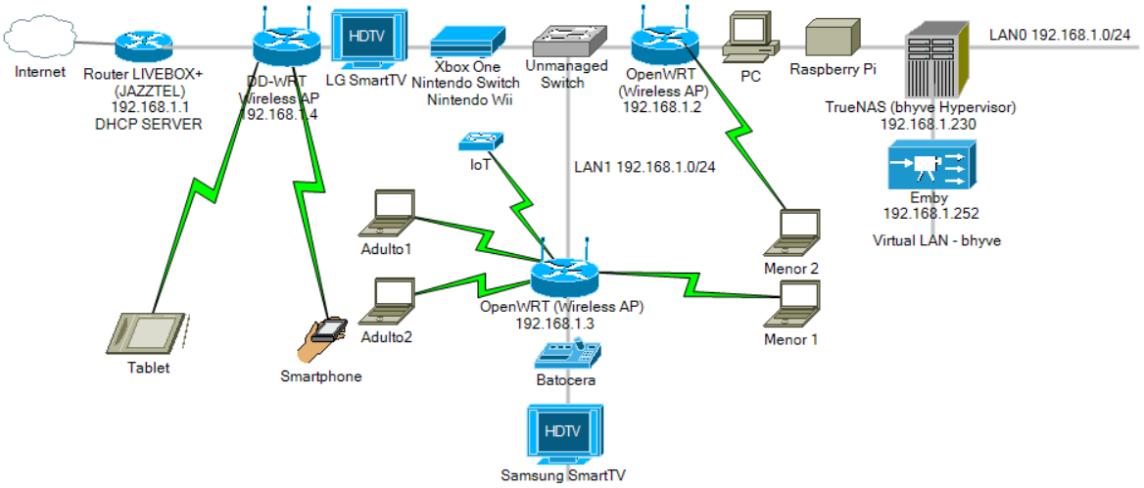


Figura 16: Arquitectura previa a las modificaciones para la red de laboratorio.

El primer inconveniente detectado al inicio es que el router LiveBox+ de Jazztel tiene bloqueada por parte de la operadora de telefonía la opción de cambio de los servidores DNS. Tras consultar con el soporte técnico se confirma que no pueden facilitar una forma desactivar dicha restricción y solo sugieren la opción de cambiar los DNS manualmente en cada uno de los dispositivos. Esta no se considera una opción poco viable, dado el gran volumen de dispositivos en el hogar (5 móviles, 4 consolas, 2 TVs, 5 portátiles, 2 tabletas, dispositivos IoT, alarma, cámaras CCTV, etc…)

Figura 17: Bloqueo del ISP de la configuración de los DNS en el router.

Dado que se ha adquirido un equipo arquitectura Intel x64 con 4 puertos ethernet para el entorno de laboratorio se opta por desactivar el servidor DHCP del router LiveBox+

y montar el equipo adquirido para el proyecto como un router con firewall con el software pfSense y habilitar se le habilita un servidor DHCP. Puesto que el router pfSense actuará como firewall tradicional se divide la red en dos segmentos, el de antes del firewall, con red 192.168.1.0/24 y el de detrás del firewall con red 192.168.2.0/24. Se dejan otras dos redes con las bocas de red sobrantes por si son requeridas para otras configuraciones con los rangos 192.168.3.0/2 y 192.168.4.0/24. Adicionalmente se monta una antena Wifi para habilitar una WLAN con rango 192.168.5.0/24.

Dado que se disponer del equipo justo antes de la salida al router del operador para salir a internet se permite monitorizar el comportamiento y todo el tráfico de red de los equipos y las herramientas Firewall DNS a evaluar. Para ello se plantea instalar y habilitar diversos paquetes adicionales en dicho firewall:

- pfBlockerNG, una de las herramientas a evaluar
- arpwatch, para poder monitorizar las direcciones de red asignadas por el servidor DHCP.
- Darkstat, para recopilar estadísticas del uso de la red

Puede consultarse una descripción detallada del proceso de configuración del firewall pfSense en los Anexos, concretamente en la “Sección 7 Anexo I: Instalación y configuración de Pfsense”.
Adicionalmente se reconfiguran las direcciones IPs estáticas, que corresponden a:

- Los routers AP Wi-Fi (192.168.2.2, 192.168.2.3,192.168.2.4)
- El servidor NAS (192.168.2.230) y los servicios en Jails y máquinas virtuales.

El resto de IPs las asigna el servidor DHCP que se habilita en el router pfSense. De este modo, se pueden configurar y cambiar fácilmente el servidor DNS que se facilita a los equipos que se conectan a la red. Esto permite tener todos los firewalls DNS instalados y configurados simultáneamente, y basta con cambiar la IP del DNS en el servidor DHCP por la del firewall DNS que se quiere utilizar y el servidor DHCP la proporciona a los equipos que conecten a la red del hogar como la predeterminada.

De esta forma, la arquitectura para laboratorio se plantea según el diagrama siguiente:

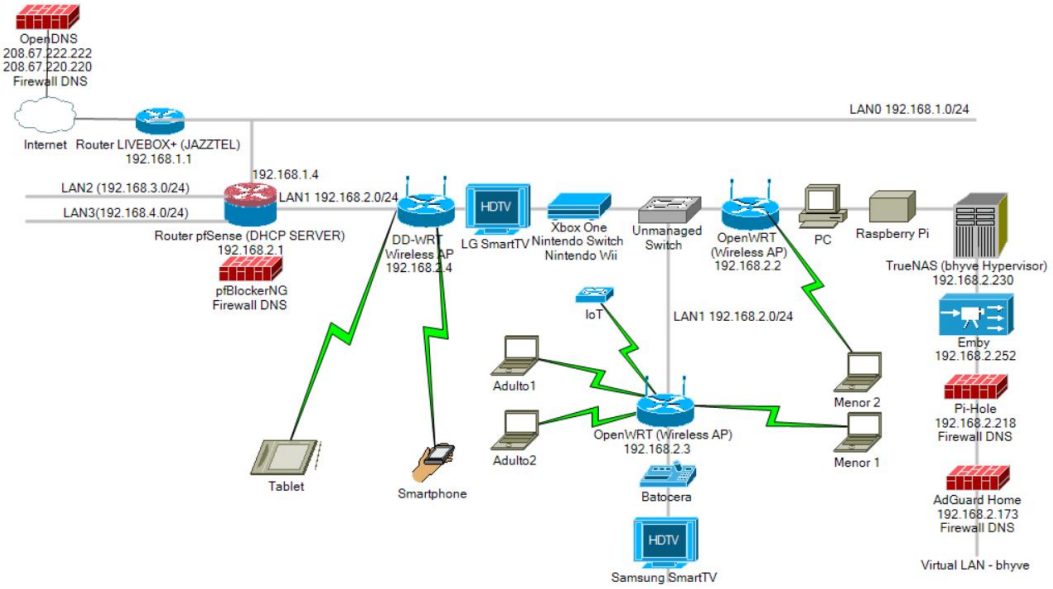


Figura 18: Diseño de la arquitectura del entorno de pruebas.

3.2. Implementación practica de los Firewall DNS

Antes de proceder con la instalación del firewall DNS, es necesario llevar a cabo un estudio exhaustivo para determinar la mejor configuración y evaluación de las soluciones. El objetivo es lograr la estandarización de la configuración en la medida de lo posible para garantizar que sea lo más completa y óptima posible en todos los firewalls DNS. En los siguientes subcapítulos se determinan algunas fuentes con sitios de pruebas para los Firewall DNS así como el proceso seguido para determinar los resolutores DNS que los van a alimentar.

Además, como resultado de un ciberataque sufrido por una organización sin ánimo de lucro con la que colaboro, se ha considerado revisar el escenario de protección, dado que tanto adultos como menores pueden acceder a Internet a través de dispositivos móviles fuera del hogar, lo que los expone a ciberdelincuentes, especialmente al Phishing, que es aún más peligroso en situaciones de movilidad. Los atacantes tienen más posibilidades de que su víctima no identifique el ataque debido a las circunstancias que rodean al usuario, como el ruido ambiente, estar distraído con otras tareas, etc. En el Anexo VIII se describen y analizan las técnicas utilizadas por los ciberdelincuentes para ejecutar el ataque de Phishing sufrido por la organización sin ánimo de lucro Red Infértiles [134] previas a la solicitud que se realizó para su incorporación a listas RPZ por el bien del resto de internautas.

En una instalación en producción, es necesario disponer de una protección que no se vea limitada por el ancho de banda o la capacidad de procesamiento. Dado que una Raspberry Pi tiene recursos de proceso y conectividad limitados, se ha decidido descartar su instalación en este tipo de plataformas limitadas a favor de un hardware más potente, como el Intel Celeron de 4 nucleos con 4 puertos gigabit ethernet, o en máquinas virtuales.

Además, se aprovecha la irrupción de este ataque de phishing para ampliar el alcance del presente trabajo y utilizar firewall DNS en dispositivos móviles, ya sea:

- Con productos en la nube analizados previamente, como OpenDNS o Quad9,
- Mediante una VPN always-on en local, como con personalDNSfilter, con objeto de aumentar la protección a adultos y menores en movilidad.
- Mediante una VPN always-on con la conexión FTTH del hogar o escuela.

En el caso de los menores se añaden herramientas de control parental en movilidad, que serán Google FamilyLink y Microsoft Family Safety, para maximizar la protección de los menores.

Gracias a esta combinación de herramientas se aumenta la seguridad en Internet tanto de menores como de adultos.

3.2.1. Sitios de prueba

Se han localizado sitios con listas para verificar la configuración de los Firewall DNS:

- Phishing: https://phishtank.org/ [114]
- Adultos:https://raw.githubusercontent.com/chadmayfield/my-pihole-blocklists/master/lists/pi_blocklist_porn_top1m.list
- Anuncios:https://pgl.yoyo.org/adservers/serverlist.php?hostformat=hosts&showintro=0&mimetype=plaintext
- Rastreadores: https://hostfiles.frogeye.fr/firstparty-trackers-hosts.txt

3.2.2. Servidores DNS para utilizar durante la evaluación

Dado que uno de los puntos a evaluar es el rendimiento de los firewall DNS, deben escogerse cuidadosamente los servidores DNS a utilizar durante las pruebas y establecer una configuración y/o lista de servidores resolutores DNS fuente que sea lo más similar posible entre los firewall DNS evaluados utilizando los resolutores DNS óptimos para las pruebas: no es lo mismo la latencia de un servidor próximo a la ubicación que el de uno en el otro extremo del planeta. Para ello se opta por utilizar la herramienta DNS Benchmark (freeware, de Steve Gibson). La herramienta permite probar el rendimiento y la fiabilidad de los servidores DNS permitiendo localizar y determinar los servidores DNS más rápidos y eficientes para la ubicación desde donde se ejecuta en base a una lista de más de 3800 tras unos procesos de pruebas automáticas que dura poco más de 35 minutos y en la que se proponen al usuario los servidores más rápidos.

Haciendo una prueba de rendimiento, este software construye una lista de resolutores DNS de referencia óptimos para la ubicación geográfica desde donde se hacen las pruebas. Como observación, el servidor DNS del ISP, que no se permite desactivar resultó ser el décimo de la lista (UNI2, que se corresponde con el del router Jazztel), siendo más lento que Quad9, OpenDNS o Telefónica:

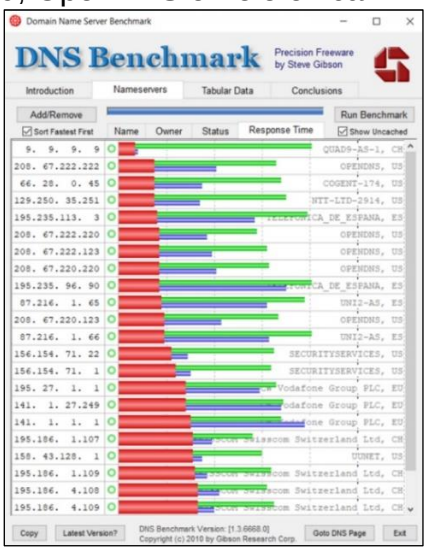


Figura 19: Resultado de la prueba con DNS Benchmark a servidores DNS.

3.2.3. Proceso de instalación

El proceso de instalación seguido para cada una de las herramientas se describe en los anexos a este trabajo:

- Instalación del software y configuración del router pfSense ➔ Anexo I
- Configuración de OpenDNS ➔ Anexo II
- Instalación y configuración de AdGuard Home ➔ Anexo III
- Instalación y configuración de Pi-Hole ➔ Anexo IV
- Instalación y configuración de pfBlockeNG ➔ Anexo V
- Instalación y configuración de DNSCloak en iPhone ➔ Anexo VI
- Instalación y configuración de Quad9 en Android ➔ Anexo VII
- Instalación y configuración de personalDNSfilter ➔ Anexo IX
- Creación de certificados para cifrado y DNS dinámico ➔ Anexo X
- Configuración de VPN OpenVPN en router pfSense ➔ Anexo X

4. Análisis de resultados y valoración de riesgos

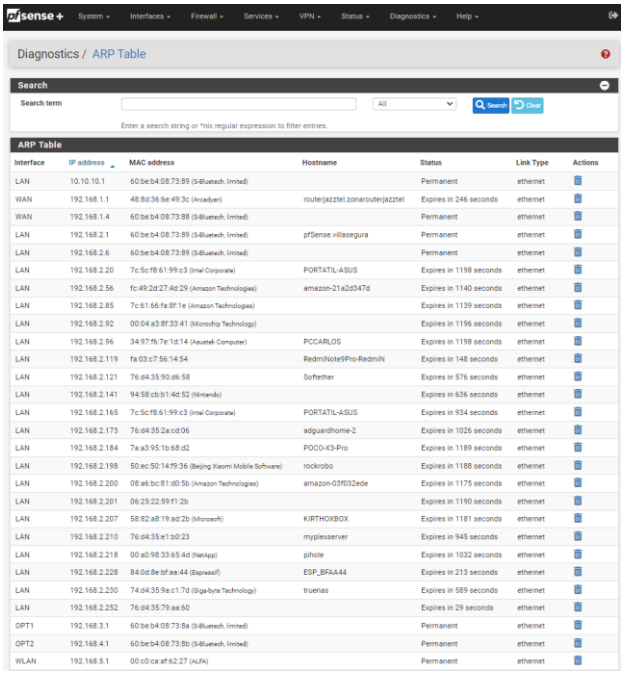
4.1. Problemas encontrados y soluciones

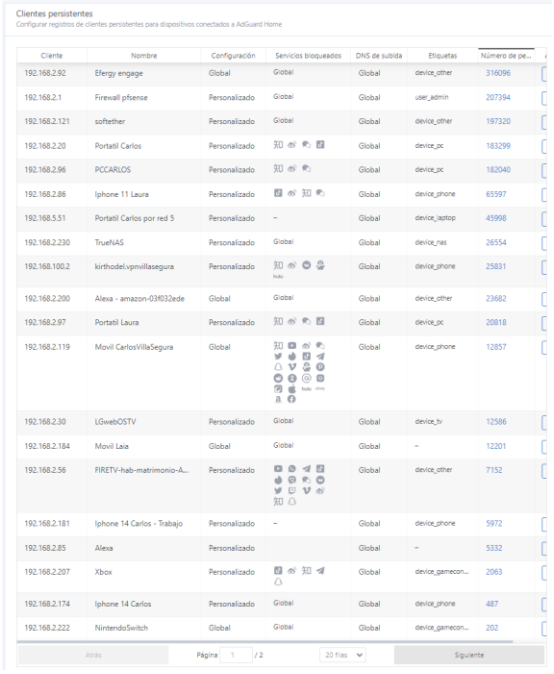
Durante el análisis del Firewall DNS se detectaron los siguientes problemas:

4.1.1. Identificación de dispositivos

Identificar todos los dispositivos de la red y mantener su inventario suele ser complejo, pero también es clave para poder gestionar correctamente los permisos y filtros de protección de los usuarios de la conexión a internet.

La identificación se soluciona realizando un barrido con herramientas como nmap para detectar todos los dispositivos de la red, configurándolos con DHCP para que obtengan la IP y configuración DNS desde el servidor DHCP del pfSense y monitorizando los dispositivos con 'arpwatch' de pfSense.
Con los dispositivos inventariados se procede a realizar la configuración personalizada para cada dispositivo en los Firewalls DNS:





Figuras 20 y 21: Monitorización con arpwatch y configuración con Adguard.

:.

4.1.2. DNS Prefetch

El DNS Prefetch se utiliza para acelerar la carga de enlaces y el navegador puede mantener una caché. Esto puede causar problemas y tiene el riesgo de que un filtro no se aplique. Incluso algunos navegadores como Chrome, podría utilizan DNS de Google en lugar del firewall DNS para precargarlos. Para prevenir que una dirección bloqueada sea accedida durante su vida en caché se soluciona desactivando el DNS Prefetch de los navegadores, especialmente en dispositivos móviles. Sobre el papel tiene el inconveniente de perder la aceleración de carga, pero dado que el servidor DNS del firewall DNS dispone de su propia cache y además se ubica en la red local (y por tanto tiene muy baja latencia) no se aprecia diferencia.

4.1.3. Protección de los teléfonos móviles cuando utilizan conexión 3G/4G/5G.

Los móviles pueden conectarse por Wifi o por la conexión de datos del teléfono. Para prevenirlo se puede cambiar sus DNS con software como Quad9 o PersonalDNSfilter, que es un Firewall DNS para móviles Android. El nuevo problema que surge al instalar este tipo de software es tener que mantener distintas configuraciones y se pierde la trazabilidad centralizada.

Una mala solución que se puede aplicar y se ha probado es abrir el firewall DNS del hogar/escuela por el puerto 53 TCP a internet previa configuración de un DNS dinámico asociada a la dirección IP de salida del hogar/escuela. A los pocos minutos de hacerlo se detecta como empiezan a aparecen conexiones desde escáneres de red automáticos en los logs:

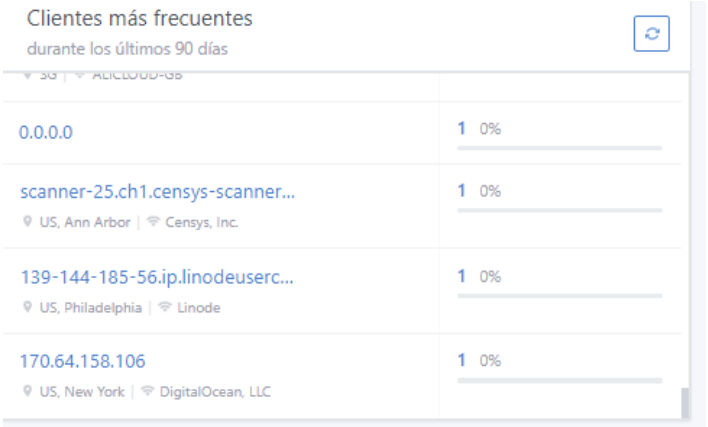


Figura 22: Escáneres de Censys y otros en los logs al abrir el puerto DNS.

Como mitigación inicial podría plantearse bloquear los escáneres desde el propio Adguard Home, pero en la práctica es algo inviable, pues son miles:

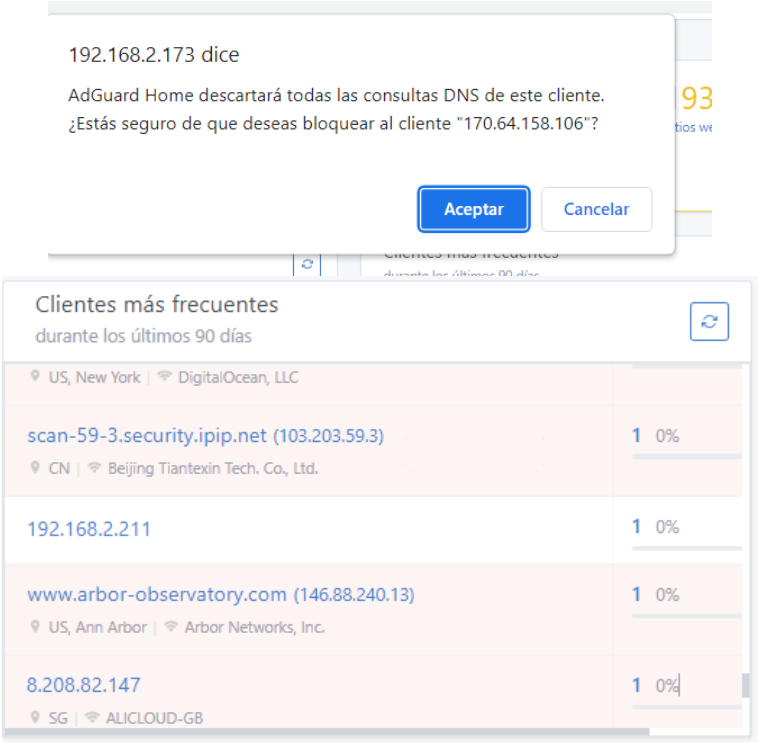


Figura 23: Configuración y bloqueo de escáneres de China y USA

Otra mitigación adicional que se ha aplicado es utilizar el bloqueo GeoIP de pfSense para conexiones entrantes con lo que se consiguen bloquear a clientes DNS del Firewall DNS en función la geolocalización de su IP.
Se ha implantado configurando el bloqueo entrante a toda conexión que no pertenezca a una IP de un país europeo, desapareciendo prácticamente los accesos de visitantes indeseados puesto que se ha verificado que la gran mayoría proceden de Asia y América, pero tampoco se considera suficiente mitigación para el riesgo de exposición de un puerto sin protección en Internet.

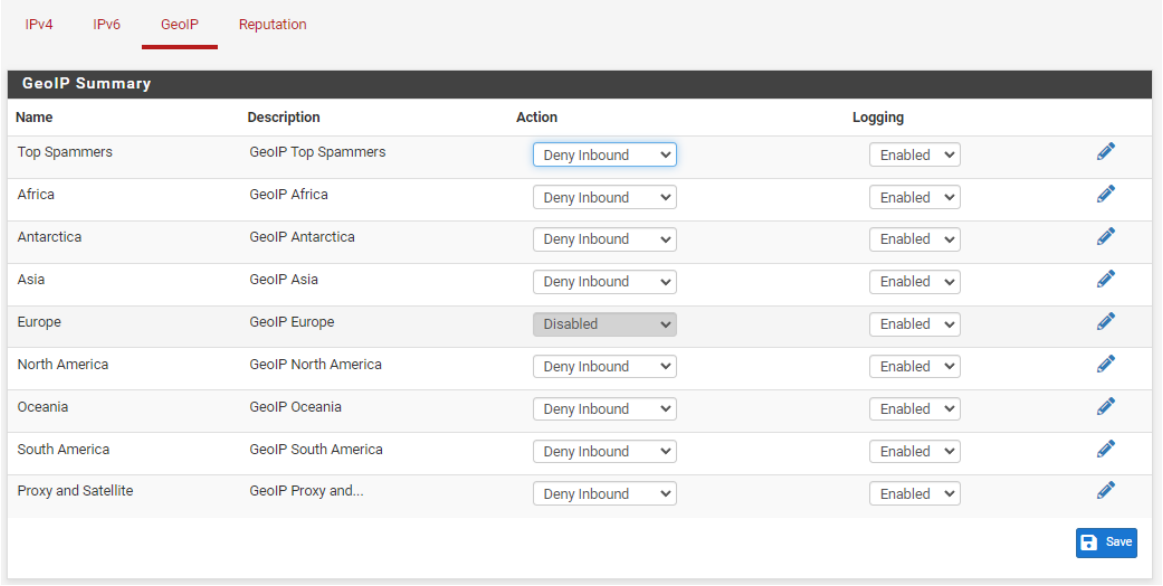


Figura 24: Filtrado de conexiones por geolocalización.

El escenario ideal es una VPN al hogar/escuela, pero como plan alternativo, si no se puede disponer de dicha VPN, la opción menos mala que se ha probado teniendo en cuenta que se expone un puerto a internet sin protección de acceso, es la combinación del bloqueo por geolocalización, la monitorización periódica con un IDS y la configuración de la resolución de DNS por HTTPS (conocida como TLS o DoH).

En los Anexos se dan los detalles para:

- Configurar un puerto no estándar, con cifrado TLS para que no lo detecten fácilmente los escáneres, como seria el 44443
- Configurar en el teléfono móvil una aplicación (personalDNSfilter en Android o DNSCloak en iPhone) que actúa de Firewall DNS local en el dispositivo con la forma de una VPN siempre activa y resuelve las peticiones DNS contra el Firewall DNS del hogar/escuela.

Adicionalmente se ha configurado como IDS/IPS la herramienta Snort en el Firewall DNS como medida de protección contra barridos o futuros exploits sobre el Firewall DNS. La conexión se ha mantenido activa y en pruebas durante más de 1 mes con esta configuración y no se han apreciado conexiones.

Esta configuración de la arquitectura con un puerto expuesto sin control de acceso comporta un problema adicional: no se permite identificar

correctamente al dispositivo puesto que un teléfono móvil continuamente cambia su dirección IP según la celda de telefonía a la que se conecta y su ubicación y obliga a utilizar una configuración común muy restrictiva para los adultos en sus móviles.
Adicionalmente y en cuanto al rendimiento, el uso de HTTPS para resolución de DNS (DoH) en lugar del DNS sin cifrar habitual tiene una latencia sensiblemente superior puesto que obliga a cifrar y descifrar para cada petición.

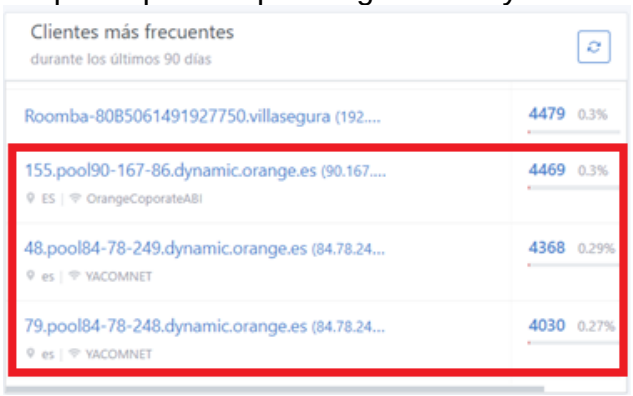


Figura 25: Filtrado de conexiones por geolocalización en pfBlockerNG

La solución más recomendable que se ha encontrado e implementado es el uso de una VPN siempre activa con OpenVPN y utilizar la resolución DNS por el puerto 53, sin cifrar puesto que ya existe un túnel cifrado entre el móvil y la red del hogar/escuela.

Este túnel VPN debe estar protegido por certificados X509 y manteniendo el filtrado por geolocalización con el software pfBlockerNG de pfSense. Esta configuración permite una menor latencia, trazabilidad centralizada y a diferencia de las anteriores, una configuración personalizada para cada dispositivo que se conecta, pues es posible identificarlo inequívocamente asociando el nombre de usuario de acceso a la VPN al dispositivo y permitiendo que siempre tengan la misma dirección IP.

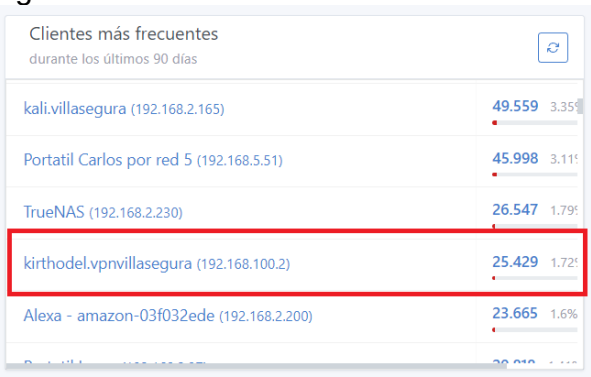


Figura 26: Identificación de los clientes móviles por VPN en Adguard.

4.1.4. Falsos positivos

Un falso positivo es la detección como amenaza y por tanto bloqueo de un dominio que no lo es.

Es posible que aparezcan falsos positivos, que refieren a bloqueos de conexiones que no deberían ser bloqueadas. Durante las pruebas se experimentaron problemas con Amazon Alexa y Amazon FireTV, puesto que en algunas de las listas RPZ implantadas se restringían dominios que no eran de rastreo.

Para solucionar estos casos, basta con acceder al registro de consultas, localizar los bloqueos de los servicios que tienen problemas, ver las URLs afectadas y añadirlas como excepciones.

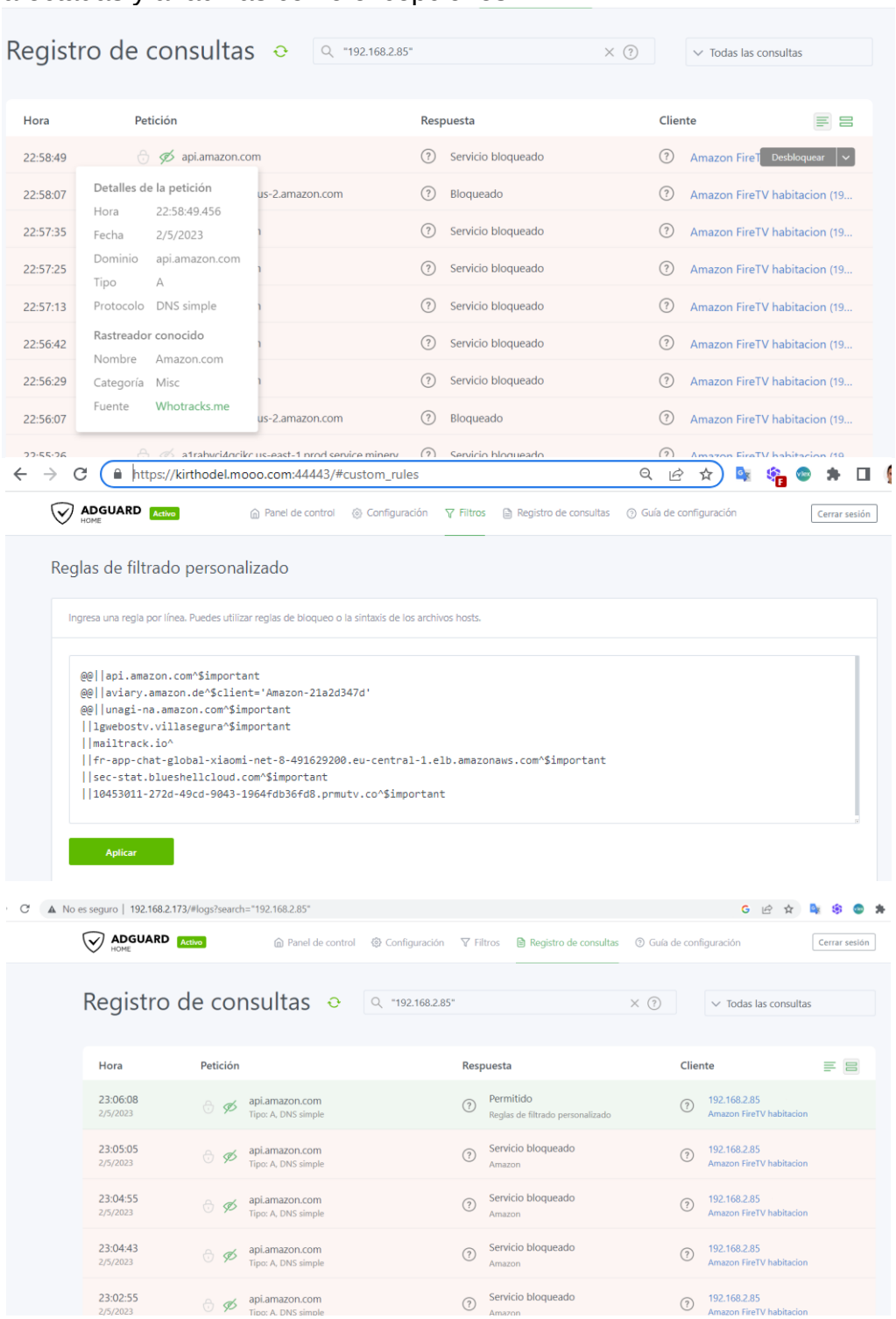


Figura 27: Solución a los falsos positivos que afectan a Alexa

4.1.5. Desconexiones de la VPN

Se ha observado que cuando falla la cobertura en móviles es posible que la conectividad VPN se pierda y al volver a conectar a la red de datos se utilice internet sin protección.
La solución en este caso es configurar en la “VPN siempre activa” tanto en Android como en iPhone desde el menú de configuración de la VPN.

4.1.6. Filtrado personalizado para fuentes y aplicaciones no listadas en RPZs

Disponer de listas realiza gran parte del trabajo de configuración, pero los logs que proporcionan los Firewall DNS son sin duda una fuente de información importante, tanto para detectar software no deseado como para perfeccionar las listas de bloqueos en un entorno determinado, permitiendo identificar resoluciones DNS no deseadas previas al establecimiento de las transmisiones de información.

Es útil realizar ocasionalmente estadísticas sobre las conexiones que realizan los dispositivos de la red controlada, para determinar si existen conexiones sospechosas o innecesarias que se pueden filtrar para mejorar la seguridad. Dichas conexiones pueden filtrase desde el firewall DNS, el firewall pfSense y/o la configuración de la propia aplicación, incluso se puede determinar que una aplicación tiene demasiado riesgo para permitir que este instalada y/o en ejecución.

Un proceso sencillo es descargar el registro de consultas DNS y procesarlo con herramientas ofimáticas como Excel, buscando las consultas que más veces se repiten y que son permitidas, eliminando las de la red local y revisando por cada dispositivo.

Las direcciones que sean sospechosas pueden buscarse en fuentes OSINT o en foros de comunidades donde se comparten listas RPZs para determinar su finalidad y utilidad.

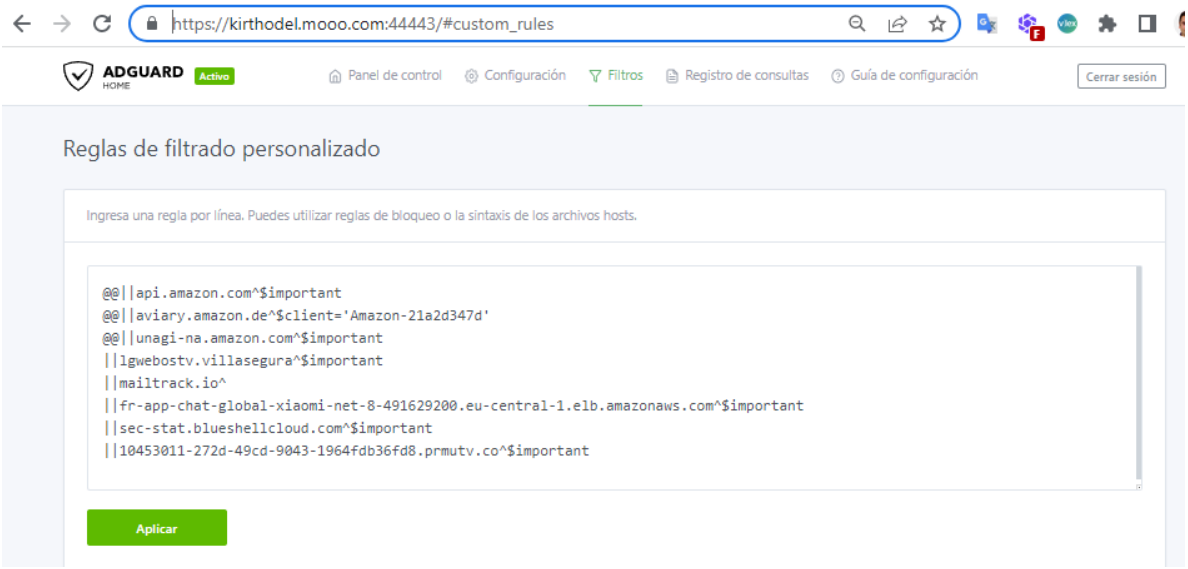


Figura 28: Añadir manualmente filtros de URL.

4.1.7. Detección de malware

Problema: Mediante la monitorización periódica de los logs del firewall pueden aparecer bloqueos de amenazas. Estos bloqueos deben investigarse, puesto que ningún equipo de la red controlada debe intentar acceder a un servidor sospechoso, por tanto puede tratase, por ejemplo, de una vulneración de las normas de uso o un malware.

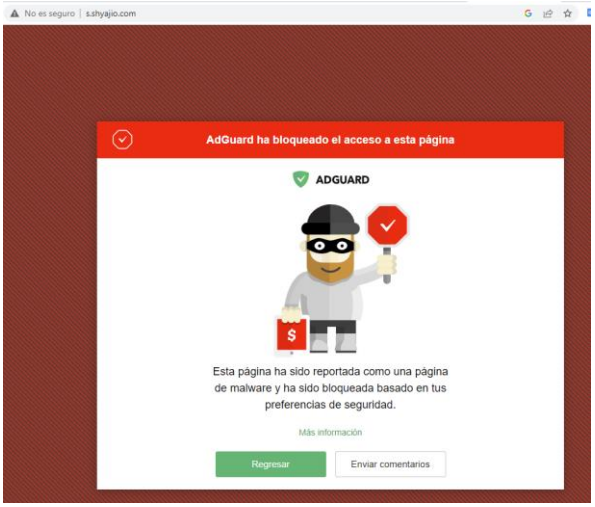


Figura 29: Añadir manualmente filtros de URL en Adguard Home.

Para determinar si son amenazas reales o falsos positivos, pueden realizarse investigaciones con fuentes abiertas de inteligencia como:

- https://www.joesandbox.com/
- https://otx.alienvault.com/
- https://socradar.io/labs/ipreputation/
- https://threatyeti.com/search
- https://talosintelligence.com/

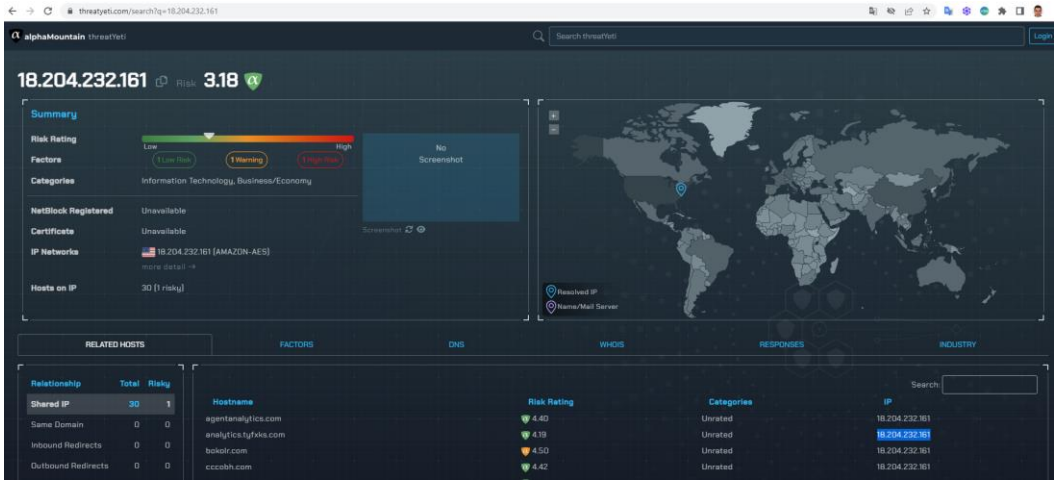


Figura 30: Uso de fuentes OSINT para analizar la amenaza.

Solución: Con la información obtenida de la investigación de fuentes se determina cual es la aplicación que ha hecho saltar la alerta y se procede a su desinstalación y se avisa al usuario. En el Anexo VI se explica tal como el ejemplo del juego de solitario localizado en un dispositivo móvil durante el análisis de las soluciones y que se explica en el Anexo VI.

4.2. Análisis de diferencias entre los aspectos de las soluciones

Durante el análisis de las soluciones se ha profundizado en los aspectos diferenciales de las soluciones, que se resumen en la tabla siguiente:

Aspecto	OpenDNS	PiHole	Adguard Home	pfBlockerNG
Facilidad de uso (1-10)	8	6	9	3
Configuración basada en GUI	Sí	Sí	Sí	Sí
Informes y estadísticas	Sí	Sí	Sí	Sí
Respaldo de logs y auditoría	Sí	Sí	Sí	Sí
Modos de privacidad en logs	Anónimo (todos los registros con la misma IP)	Normal, IP origen Anónima, Anónimo completo	Normal, IP origen Anónima	Varios
Actualizaciones automáticas de las listas de filtrado	Sí	Sí	Sí	Sí
Personalización de página de bloqueo	Sí	Sí	Sí	Sí
Arquitectura	**SaaS (Software as a Service)**	On-Premise	On-Premise	On-Premise
Plataformas soportadas	No aplica, es un SaaS	Linux, Docker, VM, Raspberry Pi	Linux, FreeBSD, Docker, VM, Raspberry Pi	FreeBSD + pfSense
Caché de consultas	No aplica por arquitectura	Sí	Sí	Sí
Requisitos de hardware minimos	**No se requiere hardware adicional**	ARM tipo Raspberry Pi 2 o x86/x64 de baja gama	ARM tipo Raspberry Pi 3 o x86/x64 de baja gama	Intel Celeron 2 nucleos con 2 interfaces Ethernet y 4 GB RAM
Bloqueo de aplicaciones/servicios específicos (Tiktok, telegram, discord, youtube, netflix...)	No	No	**Sí, nativo**	No
Analisis de trafico de red IDS/IPS (por ejemplo Snort)	No	No	No	**Sí**
Bloqueo de conexiones salientes no deseadas	No	No	No	**Sí**
Bloqueo de descargas de DNS/IPs en listas	No	No	No	**Sí**
Bloqueo de DNS externos	No	No	No	**Sí**
Capacidad de bloqueo por categoría	**Sí**	No nativamente, requiere listas	No nativamente, requiere listas	**Sí**
Bloqueos con programación horaria	**Sí**	No	No	**Sí**
Listas preconfiguradas	Sí	Insuficientes	Sí	Sí
Búsqueda segura	No	Manualmente, usando CNAME	Si, nativo	Si, nativo
Personalización de puertos escucha DNS	No	No soportado desde la GUI	Sí	Sí
Capacidad de redirección DNS	No	Sí	Sí	Sí
Configuración por dispositivo/cliente	No, limitado por IP de salida a Internet	Sí, pero solo con grupos a los clientes	**Sí, total, incluyendo bloqueo de aplicaciones y servicios especificos**	Si, pero excesivamente compleja de configurar y mantener
Control de acceso basado en IP	Sí, pero la de internet de salida	Sí	Sí	Sí
Estadísticas detalladas	No distingue IP de origen	Sí	Sí	Sí
Incorpora DHCP	No	Sí	Sí	Sí
Soporta personalización de listas RPZ	No	Sí	Sí	Sí
Protocolos para servidores upstream	No aplica	DNS TCP & UDP	DNS TCP & UDP, DNS over HTTPS (DoH)	DNS TCP & UDP, DNS over HTTPS (DoH)
Protocolos para servir resoluciones DNS	DNS TCP & UDP, DoH, TLS	DNS	DNS, DNS over HTTPS (DoH), TLS, QUIC, DNS Crypt	DNS, DNS over HTTPS (DoH)

Leyenda:

Rojo - Negativo, No soportado o excesiva limitacion/complejidad
Amarillo - Aspecto neutral o que está soportado, pero tiene limitaciones
Verde - Aspecto positivo o soportado
Negrita - Aspecto diferencial

Figura 31: Análisis comparativo de las diferencias entre soluciones.

4.3. Solución final

Teniendo en cuenta estas diferencias, se determina como la solución óptima la combinación estas herramientas de forma que se optimizan las mejores prestaciones de cada una, minimizando el coste al no ser todas gratuitas y no tener que adquirir suscripciones y maximizando la seguridad:

I. Se utiliza **OpenDNS** para el bloqueo por categoría de sitios web y utilizándolo como DNS resolutor de Adguard Home.
II. **pfSense**, instalado entre el router del proveedor de internet y la red local, actúa como:
    a. Servidor DHCP
    b. Resolutor de nombres inverso para la red local.
    c. Servidor VPN con OpenVPN para fuera del hogar/escuela.
    d. IDS / IPS con la herramienta Snort, para proteger accesos a los puertos abiertos (OpenVPN y DoH).
    e. Servidor de portal cautivo, desde donde se informa de las normas y condiciones de uso que el usuario debe aceptar para utilizar la conexión a internet.
    f. Mantenedor de la asignación de la IP de salida a internet con un subdominio con DNS dinámico.
    g. Repositorio de certificados de CA, cifrado y de identificación.
III. **pfBlockerNG** actúa como:
    a. Bloqueador de conexiones salientes no permitidas (por ejemplo, otros servidores DNS o DNS relacionados con Malware o Phishing.
    b. Bloqueador de conexiones entrantes por geolocalización.
IV. **Adguard Home** es la herramienta Firewall DNS para los dispositivos de la red local, los que se conectan por VPN y opcionalmente servidor DNS TLS publicado en internet, utilizando:
    a. Una configuración global por defecto, donde se aplica el mínimo privilegio y que corresponde a la configuración más restrictiva. Esto incluye:
        i. Búsqueda segura (Safesearch).
        ii. Restricción de acceso a los contenidos para adultos.
        iii. Protección contra amenazas emergentes y malware.
        iv. Protección contra Phishing
        v. Protección contra rastreadores
        vi. Protección contra anuncios
    b. Configuraciones personalizadas para dispositivos y grupos de usuarios en función de la necesidad.
    c. Cifrado SSL para consultas TLS o DoH así como para la interfaz web de configuración.
    d. Registro centralizado de consultas DNS y acciones realizadas.
V. Uso en dispositivos móviles y tabletas de **VPN always on** contra el servidor contra el servidor **OpenVPN** que publica el pfSense en un subdominio dinámico o, alternativamente, uso de **DNSCloak** (en iOS) o **PersonalDNSfilter** (en Android) como herramientas que fuerzan el uso a utilizar el Firewall DNS del hogar a través de DoH. (ver Anexos)
VI. Uso de herramientas **Google Family Link, Microsoft Family Safety, Microsoft Xbox Family, Nintendo Switch (Control Parental).**

Esta solución es la que se ha implantado en laboratorio con la siguiente arquitectura tecnológica:

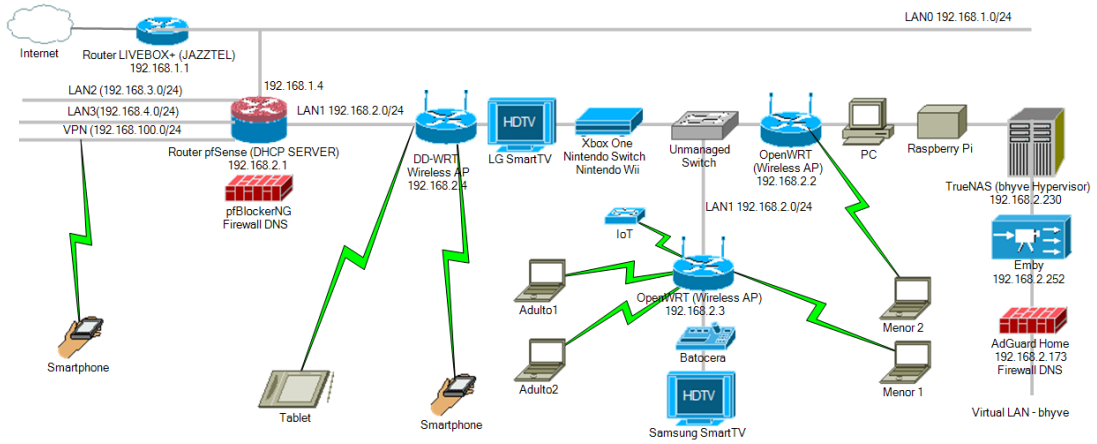


Figura 32: Diagrama de la solución final propuesta.

4.3.1. Implantación utilizando el mínimo hardware

Una implantación mínima y completamente funcional de la solución propuesta pasa por instalar todos los componentes en el dispositivo que ejecuta el software pfSense, sobre sistema operativo FreeBSD, excepto el OpenDNS, en modalidad SaaS:

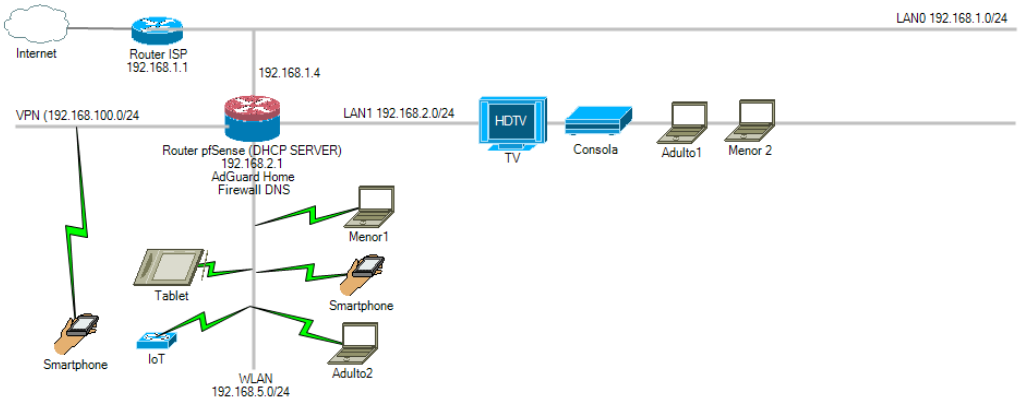


Figura 33: Diagrama de la solución final propuesta con el mínimo hardware.

4.3.2. Implantación básica en el hogar reduciendo capas de seguridad

La implantación más básica de la solución y con el mínimo coste en hardware, todo y que pierde algunas de las características de protección sobre la solución final, consiste en la instalación de Adguard Home en un hardware limitado y de bajo coste como es una Raspberry PI 3 o superior, que actúa como:

- Servidor DHCP,
- Servidor OpenVPN
- Resolutor de DNS inverso.

Si se compara esta solución con respecto a la solución final propuesta, al no disponer de pfSense:

- No se dispone de bloqueo de fuentes DNS no permitidas, por lo que debe revisarse regularmente si hay usuarios que se saltan la protección.
- No se dispone de bloqueo a las direcciones IP salientes ni a entrantes (solo filtrará por nombre DNS las salientes).

- No se dispone de protección IDS / IPS, por lo que no se recomienda publicar en internet el resolutor por DoH.
- No se dispone de portal cautivo, por lo que no se puede advertir al usuario de las condiciones de uso de la red.
- La latencia en respuestas DNS aumentará si existen muchos dispositivos en la red realizando consultas de forma simultánea, dado que se ejecuta la solución en un equipo con pocos recursos y limitada velocidad de red.

Aún que esta solución básica mejora la seguridad notablemente en un hogar tipo con dos adultos y uno o dos menores con respecto a utilizar la salida a internet genérica que proporciona el proveedor de telecomunicaciones/ISP, esta solución básica no es apta ni por rendimiento ni por requerimientos de seguridad para una escuela.

4.4. Análisis de los resultados obtenidos

4.4.1. Experiencia de usuario

La experiencia de usuario es buena y no se percibe diferencia excepto cuando se accede a hosts filtrados por el Firewall DNS.

4.4.2. Impacto en el rendimiento

El ancho de banda no se ve afectado en absoluto, puesto que el equipo que ejecuta el pfSense dispone de capacidad real de Gigabit Ethernet.

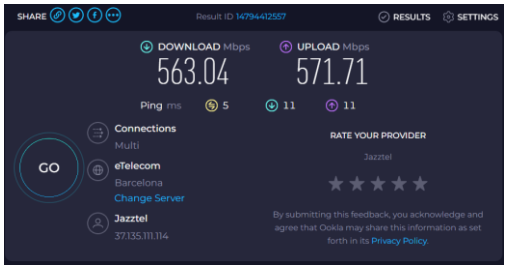
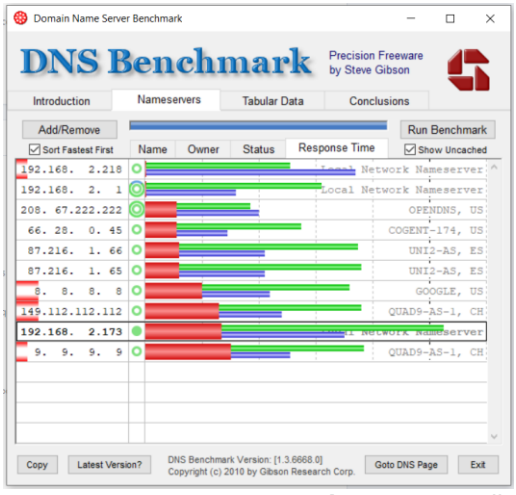


Figura 34: Medición del ancho de banda disponible.

La latencia ha empeorado con respecto a la instalación inicial, dado que se han incorporado muchas listas de filtrado. Se aprecia mucha variabilidad en los tiempos de respuesta máxima, tal como revela el cálculo de la desviación estándar. Aún y así los tiempos de respuesta medios son similares a los de Quad9:




```
  8.  8.  8.  8 |  Min  |  Avg  |  Max  |Std.Dev|Reliab%|
----------------+-------+-------+-------+-------+-------+
- Cached Name   | 0,014 | 0,020 | 0,043 | 0,005 | 100,0 |
- Uncached Name | 0,018 | 0,072 | 0,279 | 0,071 |  95,9 |
- DotCom Lookup | 0,024 | 0,044 | 0,052 | 0,006 | 100,0 |
---<--------->---+-------+-------+-------+-------+-------+
                    dns.google
                    GOOGLE, US

149.112.112.112 |  Min  |  Avg  |  Max  |Std.Dev|Reliab%|
----------------+-------+-------+-------+-------+-------+
- Cached Name   | 0,025 | 0,026 | 0,029 | 0,001 |  98,0 |
- Uncached Name | 0,026 | 0,076 | 0,246 | 0,061 | 100,0 |
- DotCom Lookup | 0,043 | 0,048 | 0,054 | 0,002 |  97,9 |
---<--------->---+-------+-------+-------+-------+-------+
                   dns.quad9.net
                   QUAD9-AS-1, CH

192.168.  2.173 |  Min  |  Avg  |  Max  |Std.Dev|Reliab%|
----------------+-------+-------+-------+-------+-------+
+ Cached Name   | 0,013 | 0,027 | 0,192 | 0,027 | 100,0 |
+ Uncached Name | 0,044 | 0,105 | 0,300 | 0,076 | 100,0 |
+ DotCom Lookup | 0,059 | 0,070 | 0,079 | 0,005 | 100,0 |
---<--------->---+-------+-------+-------+-------+-------+
                   adguardhome-2.villasegura
                   Local Network Nameserver
```

Figura 35: Medición de la latencia.

4.4.3. Cumplimiento de requerimientos

El cumplimiento de requerimientos es total para la Solución Final y la Mínima.

Requerimiento	Detalle	Solución Final	Solución Mínima	Solución Básica
Bloqueo de sitios web	Permitir el bloqueo de sitios web inapropiados o peligrosos.	Si	Si	Si
Bloqueo de descarga	Bloquear la descarga de archivos peligrosos o no autorizados.	Si	Si	Si
Registro de actividad y reportes	Registrar la actividad de navegación del menor.	Si	Si	Si
	Soporte de informes y análisis detallados de uso de DNS.	Si	Si	Si
Bloqueo de redes sociales	Limitar el acceso a redes sociales y mensajería instantánea.	Si	Si	Si
Bloqueo de contenidos	Bloqueo de contenidos violentos, sexuales, discriminatorios o ilegales.	Si	Si	Si
	Soporte de políticas de filtrado basadas en categorías de sitios web.	Si	Si	Si
	Reglas de acceso basadas en la ubicación geográfica del destino.	Si	Si	No
Bloqueo de enlaces	Bloquear los enlaces presentes en correos tipo phishing o spam.	Si	Si	Si
Control por tiempo	Personalizar el filtrado por franjas horarias o por días de la semana.	Si	Si	No
Protección contra malware	Proteger contra ataques de phishing y malware. [46]	Si	Si	Si
Perfiles de usuario	Configuración personalizable según perfiles de usuario.	Si	Si	Si
	Soporte de autenticación de usuarios y dispositivos.	Si	Si	Si
Compatibilidad	Soporte para múltiples dispositivos, plataformas y sistemas operativos.	Si	Si	Si
Bloqueo de aplicaciones	Capacidad de bloquear aplicaciones concretas en dispositivos móviles.	Si	Si	Si
Monitorización	Monitorización de la actividad en tiempo real	Si	Si	Si
Envío de Alertas	Capacidad de generar alertas en tiempo real por posibles amenazas.	Si	Si	Si
Actualización automática	Actualización automática de la lista de sitios peligrosos e inapropiados.	Si	Si	Si
Bloqueo parental	Permitir establecer un bloqueo de seguridad parental por contraseña.	Si	Si	No
Listas blancas y listas negras	Soporte de listas negras y blancas de direcciones IP y de dominios.	Si	Si	Si
Integración	Capacidad de integración con antivirus, syslog, SIEM, etc.	Si	Si	Si
Caché de consultas	Soporte de la resolución de nombres de dominio en caché.	Si	Si	Si
Bloqueo de DNS externos	Capacidad de bloqueo de consultas a otros servidores DNS	Si	Si	No
Página de bloqueo customizable	Capacidad de mostrar una página a medida para informar del bloqueo.	Si	Si	Si
Incorporar servidor DHCP	Incorporar un servidor DHCP integrado para facilitar el despliegue.	Si	Si	Si

Figura 36: Cumplimiento de los requerimientos por parte de las soluciones.

En cuanto a los requerimientos para la escuela, la solución final permite establecer un portal cautivo para la aceptación y notificación de las normas de uso, así como de la naturaleza del tratamiento de la información, aun y así es necesario recoger el consentimiento de los padres en el caso de menores de 14 años tal como se trata en el capítulo 4.5.

4.5. Estudio de los requerimientos legales y de protección de datos

Aun y que pueda parecer que no se registran datos personales al solo contenerse información al respecto de dominios visitados por dispositivo, los dispositivos en muchas ocasiones pueden asociarse a individuos concretos, por ello la implantación de este tipo de soluciones requiere cumplir con las siguientes leyes y marcos legislativos:

4.5.1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

El **artículo 7** establece requisitos para el **consentimiento del tratamiento de datos personales** de menores de edad, que debe obtenerse cuando sean mayores de catorce años, pero para menores de catorce años el consentimiento debe ser otorgado por los titulares de la patria potestad o tutela. Por tanto, en las escuelas los padres de menores de 14 años deben dar el consentimiento para que los menores utilicen la conexión a Internet que les proporción la escuela, aceptando el tratamiento de los datos y las condiciones de uso. Los mayores de 14 deberán aceptar. En el hogar los padres deben explicar claramente a los menores las condiciones de uso. Los profesores y cualquier otro usuario adulto también deben aceptar el tratamiento. El uso de un portal cautivo que recuerde las condiciones de uso del servicio de internet es una medida informativa en este sentido.

El **artículo 5** establece los requisitos de **confidencialidad** para que los datos recopilados y se mantengan en secreto por parte de quien hace el tratamiento. Además, no se guardan datos identificativos directos de personas en los registros, pero aún y así deben tomarse precauciones al configurar los permisos de clientes o los nombres de los equipos o dispositivos para que no identifiquen directamente a los usuarios.

El **artículo 84** establece la **responsabilidad de los padres, madres, tutores o representantes legales** para procurar un uso equilibrado y responsable de los dispositivos digitales por parte de los menores. Esta implantación proporciona a los padres y escuelas información y herramientas para que puedan configurar y ajustar los filtros y restricciones según las necesidades y edades de los menores, permitiendo supervisar y controlar el acceso a contenidos en línea.

El **artículo 12** establece disposiciones sobre el **ejercicio de los derechos del interesado**, incluido el derecho a recibir información clara y transparente sobre el tratamiento de sus datos personales. Mediante un portal cautivo se facilita eta información al utilizar los servicios de internet a través del firewall DNS.

4.5.2. Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual

El **artículo 10** (Alfabetización mediática) indica que se procuraran "***medidas para promover que los padres, madres, tutores o representantes legales procuren que los menores hagan un uso beneficioso, seguro, equilibrado y responsable de los dispositivos digitales****, de los servicios de comunicación audiovisual y de los servicios de intercambio de vídeos a través de plataforma*", el filtro de contenidos, el

control horario y las herramientas de control parental del Firewall DNS facilitan esta función.

El **articulo 44** deja claros los "***límites a la libertad de recepción de servicios prestados desde la Unión Europea***" como aquel que "*b)* ***Pueda perjudicar el desarrollo físico, mental o moral de los menores***". De igual manera, el articulo 89 indica que se tomaran medidas de protección para: "*e) Establecer y operar sistemas de verificación de edad para los usuarios con respecto a los contenidos que puedan* ***perjudicar el desarrollo físico, mental o moral de los menores*** *que, en todo caso, impidan el acceso de estos a los contenidos audiovisuales más nocivos, como la violencia gratuita o la pornografía*" y "*f)* ***Facilitar sistemas de control parental*** *controlados por el usuario final con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores*". Estos limites justifican el establecimiento de medidas como el Firewall DNS para proteger a los menores.

4.6. Valoración de los riesgos de la implantación del Firewall DNS

4.6.1. Impacto en sostenibilidad

Analizando y extrapolando un periodo de tráfico de datos de 17 horas juntamente con estadísticas de un periodo de filtrado de 30 días se obtienen los datos siguientes:

Dato	Valor	Unidades	Valor	Unidades
Consumo equipo pfSense	6	W	4,32	kWh
Plazo temporal	17	horas		
Tráfico total (filtrado)	72.593.101.796	bytes	67,61	GiB
Paquetes en total	59.505.508	paquetes		
Bytes por paquete promedio	1.220	bytes		
Número de consultas DNS	1.969.126	consultas		
Consultas bloqueadas por filtros	330.718	consultas	16,795	%
Malware/phishing bloqueado	62	consultas	0,003	%
Sitios para adultos bloqueados	193	consultas	0,010	%
Trafico por consulta promedio	36.866	bytes		
Hipotético tráfico total sin Firewall	**84.788.742.898**	**bytes**	**78,97**	**GiB**
Cálculo del tráfico ahorrado	**12.195.641.102**	**bytes**	**11,36**	**GiB**

Figura 37: Estadísticas y cálculos del ahorro y sostenibilidad.

El equipo que hace de firewall, que tiene un consumo máximo de 6W se calcula que proporciona aproximadamente un ahorro de casi un 17% en transmisión de datos. Esa reducción repercute en ahorro energético en:

- Los equipos receptores de la información (PCs, portátiles, móviles, tabletas…)
- Los equipos intermedios en la comunicación. Para acceder a un periódico online, como www.elperiodico.es, se requieren 12 saltos por distintos routers, sin tener en cuenta los switches, conversores de medios u otros equipos intermedios. Por cada anuncio o rastreador multiplica el número de equipos necesarios que deben mover esa información.

Filtrar contenido indeseado puede ser una contribución al ahorro energético y de recursos, por lo que se considera logrado mitigar los riesgos asociados a un mayor consumo de recursos al implementar un Firewall DNS adecuadamente.

De hecho, el filtrado de URLs contribuye a reducir el consumo de ancho de banda y, en consecuencia, aumentar la eficiencia energética de todos los equipos en la cadena de conexión punto a punto desde el usuario final hasta el CPD donde este albergado un servidor, pasando por todos los switches, routers, conversores de medios, etc...

Por otro lado, un firewall DNS requiere de un mantenimiento, actualizaciones, supervisión, pero su carga de trabajo se estima muy baja y se compensa por la protección y prevención que se proporciona al menor y adulto. Adicionalmente, las jornadas de dedicación y las pérdidas económicas que potencialmente se evitan para resolver un ciberataque que podría producir cualquiera de las consultar filtradas compensa sobradamente la baja carga de trabajo de mantenimiento que comporta.

Se considera muy positivo en global y mitigados los aspectos negativos.

4.6.2. Comportamiento ético y responsabilidad social

El Firewall DNS evita la exposición a contenidos violentos, pornografía y otros contenidos perjudiciales para los menores.

También los protege de las amenazas de la red del tipo malware, phishing o ramsonware, al igual que a los adultos.

Se considera conseguido el objetivo de proteger a los menores de edad de contenidos inapropiados y potencialmente dañinos, mejorando así su comportamiento ético y promoviendo la responsabilidad social.

Por otra parte, se podría considerar negativo o poco ético el limitar la información que se recibe (anuncios) y se da (telemetría del uso de las aplicaciones y servicios), dado que podría generar pérdidas económicas a empresas que sus ingresos dependen en mayor o menor medida de estos datos que se recopilan por parte de los usuarios. La realidad es que, como usuario, se reciben continuas peticiones de tratamiento de datos, complejas de rechazar, pero muy fáciles de recibir. Un ejemplo reciente es que en los televisores LG han empezado a aparecer avisos de tratamiento de cookies y de rastreo o publicidad que son bastante complejos de rechazar pero excesivamente fáciles de aceptar. Utilizar un firewall DNS facilita el derecho de la privacidad, bloqueando a esos rastreadores, especialmente de los menores, que no entienden de revisar condiciones de uso o complejos mecanismos para rechazar algo que con un simple botón aceptar les permite ver los contenidos que desean sin saber ni ser conscientes de las autorizaciones que conlleva apretar el botón aceptar sin leer.

Se considera muy positivo en global y mitigados los aspectos negativos.

4.6.3. Diversidad y derechos humanos

La implementación del Firewall DNS ha contribuido a proteger los derechos de los menores, evitando su exposición a contenido dañino y reduciendo los riesgos de

discriminación. Además, se ha garantizado un acceso equitativo a la información, disminuyendo la discriminación de género y otros tipos de discriminación.

Solo se han encontrado casos de falsos positivos con Amazon Alexa y FireTV, y se ha podido mitigar corrigiéndolo fácilmente con la modificación de la configuración añadiendo una excepción.

Para reforzar la mitigación de este inconveniente es importante establecer un canal de comunicación para reportar los falsos positivos, para así evitar la censura y la libertad de expresión, evitando limitar el acceso a información relevante.

Se considera que es positivo en global, dado que refuerza y protege los derechos de la infancia y de los menores.

4.6.4. Impactos no previstos

Concienciación (Positivo):
Durante las pruebas en laboratorio los menores manifestaron curiosidad y se alarmaron al ver la cantidad de ataques que se sufren al utilizar Internet. Se considera que la experiencia del laboratorio de un Firewall DNS ha mejorado su conciencia y su educación digital y que esto permitirá que hagan un uso más responsable y seguro de Internet.

Detección de malware (Positivo):
El firewall DNS ha servido para detectar malware en uno de los dispositivos familiares, se trataba de un juego del solitario. Este uso no previsto del firewall DNS refuerza los aspectos positivos de su uso.

Intranquilidad (Negativo):
Monitorizar y ser consciente de la cantidad de ataques a la privacidad y a integridad de los datos y comunicaciones hace perder la sensación de inocuidad de navegar por Internet, aumentando la sensación de estar vigilado y acechado constantemente, lo que lleva a los usuarios a autocensurarse y dejar de realizar acciones que de otro modo realizarían y hubieran sido inocuas.

Confidencialidad (Negativo):
Registrar las consultas del hogar (o de la escuela) puede limitar la confidencialidad del uso de internet. Como mitigación se pueden buscar fórmulas como una contraseña compuesta donde solo conoce una parte de ella cada uno de los progenitores y asegurar que el acceso a los registros es siempre de forma consensuada.

5. Conclusiones

5.1. Conclusiones del trabajo realizado

La implementación de un sistema de seguridad y control parental en el entorno doméstico y educativo es fundamental para garantizar la protección y derechos de los usuarios, especialmente de los niños y jóvenes que acceden a internet. La solución final propuesta, que combina diversas herramientas y tecnologías, ha demostrado ser efectiva en la mitigación de los riesgos a los que se exponen los usuarios y proporciona un entorno más seguro en Internet.

El uso de pfSense como firewall, servidor DHCP, VPN e IDS/IPS ha permitido una gestión eficiente de las conexiones de red, garantizando la protección contra amenazas y la configuración de políticas de acceso personalizadas. Además, la incorporación del Firewall DNS pfBlockerNG ha fortalecido aún más la seguridad, bloqueando a nivel de firewall conexiones no autorizadas y disponer de filtros basados en geolocalización.

La configuración de Adguard Home como Firewall DNS proporciona una capa de seguridad que bloquea contenido inapropiado, protege contra amenazas emergentes, contra el rastreo en línea y además, filtra los anuncios no deseados. El facilitar hacer configuraciones personalizadas para cada uno de los distintos dispositivos de la red y activar y desactivar servicios desde una interfaz gráfica de usuario permite una gran flexibilidad en el control de acceso y la protección individualizada adaptándola a las necesidades y requerimientos de cada usuario, ya sea menor o sea adulto.

El uso de OpenDNS desde Adguard Home como resolutor DNS ha resultado ser eficaz en el bloqueo por categorías de sitios web y en la protección contra phishing y malware, al demostrar que se pueden utilizar y combinar distintas fuentes de ciber inteligencia.

Todo y no ser la intención inicial del trabajo, donde se pretendía seleccionar el mejor firewall DNS para la protección de los menores en el ámbito del hogar y familiar, el combinar y añadir distintos productos, como la VPN para la protección fuera del entorno del hogar o la escuela y las herramientas de control parental que proporcionan fabricantes como Microsoft, Google o Nintendo ha permitido un mayor control y un filtrado del uso de internet mucho más completo, sumando funcionalidades y esquivando las carencias de cada producto, consiguiendo mejorar significativamente la seguridad tanto en la navegación web como de aplicaciones, juegos (en línea y fuera de línea) o servicios.

En cuanto a los resultados obtenidos en general se ha cumplido perfectamente con las expectativas dado que la solución propuesta cumple satisfactoriamente todos los requerimientos y el objetivo planteado en términos de seguridad y control parental.

Sin embargo, algunos resultados han sido sorprendentes en cuanto al impacto en el rendimiento y la latencia de la red. Aunque la disponibilidad del ancho de banda no se ha visto afectado colocando un elemento entre la red y el router del ISP, se ha observado un aumento en los tiempos de respuesta promedio debido a la

incorporación de las diferentes reglas de filtrado ya que a pesar de que tras la instalación inicial, sin aplicar la configuración el rendimiento era mucho más rápido y con menos latencia que utilizar un servidor DNS de internet directamente, tras la configuración el rendimiento promedio es similar al de los DNS de Google.

También ha sorprendido otros usos que se pueden dar a un Firewall DNS, como es el análisis y control de los servidores en internet donde acceden las aplicaciones, pudiéndose utilizar como un apoyo para investigaciones de ingeniería inversa o forense de software, facilitando la detección de comportamientos sospechosos.
Este hallazgo hace poner el foco en la importancia de considerar el equilibrio entre seguridad y rendimiento al implementar soluciones de firewall DNS.

5.2. Reflexión crítica sobre la consecución de los objetivos

La solución final propuesta, a pesar de que se cumple con los requerimientos planteados y los requerimientos adicionales que se han considerado durante la realización del trabajo tanto por referencias consultadas como por eventos sucedidos en el entorno del autor (como la protección fuera del hogar o escuela), la solución final propuesta e implantada en laboratorio no es óptima en cuanto a uso de recursos, complejidad y coste por ello se ha propuesto una solución teórica que utiliza el mínimo hardware posible teniendo en cuenta los recursos disponibles en el router pfSense que no se utilizan en la solución de laboratorio.

Esta solución mínima propuesta no puede ser a coste 0 puesto que requiere de una inversión económica en adquirir un hardware que corra la solución, el coste de este hardware ha sido de 179,78 €, esta inversión, que no debería suponer un problema para una escuela, pero si lo puede ser para un hogar.

Para ofrecer una solución más básica, con una menor inversión económica se ha propuesto una solución básica que, al involucrar una implementación mínima en términos de hardware y funciones, no cumple con todos los requerimientos y tampoco lo hace de manera óptima. La solución básica proporciona una mejora significativa en la seguridad en comparación con una conexión a internet genérica, pero carece del rendimiento y de algunas características de protección presentes en la solución final propuesta y obligan a tomar medidas de mitigación compensatorias, como el uso de aplicaciones firewall DNS en teléfonos móviles, para las que se ha estudiado por separado los casos en iPhone y en Android.

Esta investigación ha demostrado que la implementación de una solución integral de seguridad y control parental en el entorno doméstico y educativo es esencial para garantizar la protección en línea.

5.3. Cumplimiento de la planificación

La planificación inicial ha sido seguida y cumplida en plazo, a pesar de ello, se ha sido algo optimista en los plazos de algunas de las subtareas intermedias planteados dado que se han materializado eventos (como el robo de la cuenta de la asociación sin ánimo de lucro con la que colaboro) de que han obligado a dedicar noches adicionales o tiempo extra no previsto en fines de semana para recuperar el hilo del planning. Aún y así estas interrupciones se consideran positivas, puesto que han hecho patentes riesgos que pueden mitigarse con este tipo de soluciones y han permitido añadir funcionalidades a la solución propuesta que el autor considera no solo útiles sino también necesarias.

La metodología ha sido buena, pero ha sido ligeramente modificada en su etapa final, al detectar las carencias y virtudes de cada Firewall DNS, para introducir cambios y definir una solución que sea lo más completa posible utilizando distintas herramientas Firewall DNS en lugar de uno solo, que era el planteamiento inicial.

6. Líneas de trabajo futuras

Las líneas de trabajo futuro que no han podido explorarse en este trabajo y han quedado pendientes son las siguientes:

- Investigar si es posible la implantación de la solución en OpnSense, similar a pfSense pero desarrollado por otra compañía y que no dispone de pfBlockerNG.
- Investigar la implantación con OpenWRT. En la fase de análisis del estado del arte se planteó la posibilidad de buscar una solución de coste mínimo utilizando un router ya existente cambiándole el firmware por uno abierto como es OpenWRT. Esta línea de trabajo se descartó al ver los requerimientos de memoria y de procesado de las listas de filtrado. Sin embargo, existe la posibilidad de instalar OpenWRT en un hardware con características similares al elegido para el pfSense. Esta configuración, basada en Linux en lugar de en FreeBSD podría aumentar las posibilidades de customización del firewall y el uso de otras herramientas integradas en el mismo hardware, como una VPN utilizando SoftEther u otras herramientas disponibles para Linux, que tiene una mayor comunidad de usuarios.
- Redactar plantillas de políticas y normas de uso del servicio de internet, para mostrarlas en el portal cautivo.
- Explorar las posibilidades que ofrece la implantación de un portal cautivo en la solución, como por ejemplo:
    - Limitar horarios de conexión
    - Uso de cupones de tiempo de conexión para que los menores los canjeen o para la conexión de invitados al hogar o escuela.
- Integrar los logs de resolución de DNS y los eventos de pfSense en un SIEM.

7. Glosario

Definición de los términos y acrónimos más relevantes utilizados en la Memoria.

bhyve: "*hipervisor para FreeBSD" [79]*

Ciberacoso: "*uso de medios digitales para molestar o acosar a una persona o grupo de personas mediante ataques personales, divulgación de información personal o falsa entre otros medios."* [30]

Ciberbullying: ver Ciberacoso.

Cortafuegos: ver firewall.

DDWRT: *"firmware OpenSource alternativo basado en Linux adecuado para una gran variedad de enrutadores WLAN y sistemas integrados. El énfasis principal radica en proporcionar el manejo más fácil posible y, al mismo tiempo, admitir una gran cantidad de funcionalidades dentro del marco de la plataforma de hardware respectiva utilizada."* [36]

DHCP: del inglés Dynamic Host Configuration Protocol (RFC 2131), "*es un protocolo de red que permite a un servidor DHCP/servidor de red asignar dinámicamente la dirección IP, la máscara de subred, los gateways predeterminados y otros parámetros de configuración de red a los dispositivos que lo soliciten*."[150]

DNS: Sistema de Nombres de Dominios. Servicio que relaciona nombres de dominio con direcciones IP (más información en [4].

Firewall: (FW) *"la parte de un sistema informático o de una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas."* [33]

FTTH: (Fiber To The Home): Fibra hasta la casa, conexión a internet por fibra óptica.

Gateway: enlace que interconecta dos o más redes

Grooming: "*una serie de conductas y acciones emprendidas por adultos, en muchos casos a través de Internet, con el objetivo deliberado de ganarse la amistad de menores de edad, creando una conexión emocional con los mismos, con el fin de ganarse su confianza y poder abusar sexualmente de ellos*" [29]

Hipervisor: *"es un software que crea y ejecuta máquinas virtuales (VM) y que, además, aísla su sistema operativo y recursos de las máquinas virtuales y permite crearlas y gestionarlas."* [35]

IDS: del inglés Intrusion Detection System, Sistema de detección de intrusos.

IoT: del inglés "Internet of Things", *"Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana"* [71]

IPS: del inglés Intrusión Prevention System, Sistema de Prevención de Intrusos.

Jail: *"implementación de virtualización a nivel de sistema operativo que tiene disponible el sistema operativo FreeBSD"* [34]

KPI: Del inglés "Key Performance Indicator", indicador de rendimiento para medir el funcionamiento de un sistema o proceso.

Malware: *"cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario"* [31]

OpenWRT: *"es un sistema operativo Linux dirigido a dispositivos integrados. En lugar de intentar crear un único firmware estático, OpenWrt proporciona un sistema de archivos totalmente grabable con administración de paquetes. Esto lo libera de la selección y configuración de aplicaciones proporcionadas por el proveedor y le permite personalizar el dispositivo mediante el uso de paquetes para adaptarse a cualquier aplicación."* [37]

pfSense: "*es una distribución de cortafuegos de red gratuita, basada en el sistema operativo FreeBSD con un kernel personalizado e incluye paquetes de software gratuitos de terceros para funciones adicionales. El software pfSense, con la ayuda del sistema de paquetes, puede proporcionar la misma funcionalidad o más que los firewalls comerciales comunes, sin ninguna de las limitaciones artificiales."* [38]

Phishing: "*conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer clic en un enlace).*" [32]

Programa malicioso: ver Malware.

RPZ: (Response Policy Zone) mecanismo utilizado en los servidores DNS para bloquear o redirigir consultas a dominios específicos en función de una política personalizada. [80]

SaaS: "Software como un Servicio o SaaS (del inglés: Software as a Service) es un modelo de distribución de software donde el soporte lógico y los respectivos datos que maneja se alojan en los servidores de un proveedor, cuyo acceso es a través de Internet. El proveedor no solo proporciona el hardware, sino también el software correspondiente" [148]

Sexting: envío de imágenes y videos íntimos a través de Internet.

VPN: del inglés Virtual Private Network, "*tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet*".[149]

8. Bibliografía y fuentes consultadas

[1] José Antonio Salom, UOC, 2019, “Ventajas e implementación de un sistema IDS/SIEM en el ámbito familiar”
[2] Marc Hernández Sánchez, “DNS Firewall in local network”, UOC 2022
[3] Adrián Navas Ajenjo, “Estudio e implementación de un Firewall DNS”, UOC, 2022
[4] https://www.rfc-es.org/rfc/rfc1034-es.txt, 03/03/2023
[5] https://www.rfc-editor.org/rfc/rfc1035 03/03/2023
[6] https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/umbrella-dns-monitoring-package#page=1 03/03/2023
[7] https://login.opendns.com/?return_to=https://dashboard.opendns.com/ 03/03/2023
[8] https://www.ietf.org/rfc/rfc1918.txt 03/03/2023
[9] https://nextdns.io/ 03/03/2023
[10] https://news.ycombinator.com/item?id=22717650 03/03/2023
[11] https://pi-hole.net/ y https://docs.pi-hole.net/ 03/03/2023
[12] https://cleanbrowsing.org/ 06/03/2023
[13] https://www.cloudflare.com/es-es/products/zero-trust/gateway/ 06/03/2023
[14] https://www.quad9.net/ 06/03/2023
[15] https://adnauseam.io/ 07/03/2023
[16] https://adguard.com/es/welcome.html 07/03/2023
[17] https://adguard-dns.io/es/public-dns.html 07/03/2023
[18] https://adguard.com/en/adguard-home/overview.html 07/03/2023
[19] https://www.dnsfilter.com/pricing 08/03/2023
[20] https://cleanbrowsing.org/articles/response-policy-zones-rpz/ 08/03/2023
[21] https://www.admuncher.com/download 08/03/2023
[22]https://github.com/julian-klode/dns66 08/03/2023
[23]https://ublockorigin.com/ 09/03/2023
[24]https://diversion.ch/diversion/diversion.html 09/03/2023
[25]https://www.rediris.es/gt/gt2019/programa/gt/ponencias/?id=gt2019-gt--a11b2c1.pdf 09/03/2023
[26] https://en.wikipedia.org/wiki/Response_policy_zone 09/03/2023
[27] https://en.wikipedia.org/wiki/BIND 10/03/2023
[28] https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html 11/03/2023
[29] https://es.wikipedia.org/wiki/Enga%C3%B1o_pederasta 11/03/2023
[30] https://es.wikipedia.org/wiki/Ciberacoso 11/03/2023
[31] https://es.wikipedia.org/wiki/Malware 12/03/2023
[32] https://es.wikipedia.org/wiki/Phishing 12/03/2023
[33] https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica) 12/03/2023
[34] https://es.wikipedia.org/wiki/FreeBSD_jail 12/03/2023
[35] https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor 12/03/2023
[36] https://dd-wrt.com/ 12/03/2023
[37]https://openwrt.org/ 12/03/2023
[38]https://www.pfsense.org/ 12/03/2023
[39]https://grafana.com/grafana/dashboards/6603-pi-hole/ 13/03/2023
[40]https://bobcares.com/blog/add-pi-hole-to-pfsense/ 13/03/2023
[41]https://discourse.pi-hole.net/t/how-block-netflix-and-co/50777/6 13/03/2023
[42]https://blog.viktorpetersson.com/2018/01/27/jails-on-pfsense.html 15/03/2023
[43]https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC 15/03/2023
[44]https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/url-categories 15/03/2023
[45]RSACi - Registration - Definitions (mit.edu) 17/03/2023
[46]Recreational Software Advisory Council Launches Objective, Content-Labeling Advisory System for the Internet (w3.org) 17/03/2023
[47]https://youradchoices.com/control 17/03/2023
[48]https://www.surfieapp.com/ 17/03/2023
[49]Websense_Web_Security_Suite_DB_URL 17/03/2023
[50]SafeSurf ® - Keeping families safe on the Web 17/03/2023
[51]List of IAB Categories – AerServ 17/03/2023
[52]https://www.safesurf.com/index.html 17/03/2023
[53]https://www.safesurf.com/ssplan.htm 17/03/2023
[54]https://www.w3.org/PICS/ 18/03/2023
[55]https://github.com/AdguardTeam/AdguardHome#comparison-pi-hole18/03/2023
[56]https://github.com/kongfl888/luci-app-adguardhome 18/03/2023
[57]Ciberseguridad para familias | Internet Segura for Kids (is4k.es) 19/03/2023
[58]Menores en la red: ciberseguridad para niños - Cyber War Mag19/03/2023
[59]Ciberseguridad en los colegios | Hard2bit CyberSecurity 19/03/2023
[60]La ciberseguridad gana presencia en colegios e institutos (entreestudiantes.com) 22/03/2023
[61]¿Ciberseguridad en los colegios? - CyberSecurity News 22/03/2023

[62]https://www.osi.es/es/cibercooperantes24/03/2023
[63]Guía para profesionales de servicios de protección a la infancia | Internet Segura for Kids (is4k.es) 25/03/2023
[64]https://www.kaspersky.com/web-filter 25/03/2023
[65]https://www.fbi.gov/how-we-can-help-you/parents-and-caregivers-protecting-your-kids25/03/2023
[66]https://www.is4k.es/sites/default/files/contenidos/guia_para_profesionales_de_servicios_de_proteccion_a_la_infancia.pdf 25/03/2023
[67]https://www.bbva.com/es/innovacion/para-que-quieren-tus-datos-los-ciberdelincuentes/ 26/03/2023
[68]https://www.eleconomista.com.mx/tecnologia/Cuando-los-objetos-ciberatacan-hay-que-delegar-responsabilidades--20170116-0060.html 26/03/2023
[69]https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 31/03/2023
[70]https://www.is4k.es/programas/programa-de-jornadas-escolares 31/03/2023
[71]https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html 1/04/2023
[72]https://universoabb.com/que-tipo-de-red-se-utiliza-en-la-escuela/ 1/04/2023
[73](REC-PICS-services-961031 (w3.org) 1/04/2023
[74]https://www.malwarepatrol.net/rpz-dns-firewall-configuration-guide/ 1/04/2023
[75]https://www.malwarepatrol.net/dns-firewall/ 2/04/2023
[76]https://www.semanticscholar.org/paper/Key-factors-in-building-a-Secure-Web-Gateway-Yeh/2116888f96a57a8c84ca9ed775fab5df5f6809b82/04/2023
[77]https://researchcommons.waikato.ac.nz/bitstream/handle/10289/11548/thesis.pdf?sequence=3&isAllowed=y2/04/2023
[78]https://techdocs.akamai.com/etp/docs/welcome-etp2/04/2023
[79]https://bhyve.org/2/04/2023
[80]https://en.wikipedia.org/wiki/Response_policy_zone6/04/2023
[81]https://www.isc.org/rpz/ 6/04/2023
[82]http://repositorio.ipvc.pt/bitstream/20.500.11960/2677/1/Claudio_Marques.pdf 6/04/2023
[83]https://www.is4k.es/blog/oh-no-me-toca-ser-el-coordinador-tic-por-donde-empiezo-i?origen=d2 6/04/2023
[84]https://www.is4k.es/blog/oh-no-me-toca-ser-el-coordinador-tic-por-donde-empiezo-ii-la-red-local 6/04/2023
[85]https://www.is4k.es/blog/oh-no-me-toca-ser-el-coordinador-tic-por-donde-empiezo-iii-la-red-wifi 6/04/2023
[86]https://www.is4k.es/blog/filtrado-de-contenidos-en-el-aula 6/04/2023
[87]https://www.sipbench.eu/transfer/FullStudyonparentalcontroltoolsfortheonlineprotectionofchildren.pdf 6/04/2023
[88]https://www.sipbench.eu/index.cfm/secid.7/secid2.4 7/04/2023
[89]Francisco José Bordes Romaguera – "Seguridad en DNS": https://openaccess.uoc.edu/bitstream/10609/107128/6/fbordesTFM1219memoria.pdf, 2019, UOC
[90] https://hmong.es/wiki/Response_policy_zone 7/04/2023
[91] https://www.isc.org/rpz/ 8/04/2023
[92] https://dnsrpz.info/ 8/04/2023
[93] https://ioc2rpz.net/ 8/04/2023
[94] https://servidordebian.org/es/jessie/config/network/diagram 10/04/2023
[95]https://www.cisco.com/c/dam/global/en_sg/solutions/small-business/pdfs/cisco-umbrella-brochure.pdf 10/04/2023
[96] https://www.paloguard.com/datasheets/dns-security-service.pdf 10/04/2023
[97]https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/dns-security-service 10/04/2023
[98]https://www.akamai.com/site/es/documents/akamai/akamai-services-descriptions.pdf 10/04/2023
[99]https://sc1.checkpoint.com/uc/pdf/datasheets/SWG-appliance-datasheet.pdf 10/04/2023
[100]https://go.dnsfilter.com/rs/997-HCT-261/images/DNSF-FresnoUnifiedSchoolDistrict-CS.pdf?_gl=1*1g9b1k1*_ga*MTE5NzEzOTU2MC4xNjgwMDQwMTI2*_ga_MMR27NNV7M*MTY4MTE2NDAxMS41LjEuMTY4MTE2NDEwOC4wLjAuMA. 10/04/2023
[101]https://www.dnsfilter.com/features/content-filtering 11/04/2023
[102] https://www.publicdns.neustar/ 11/04/2023
[103] https://www.comodo.com/secure-dns/ 11/04/2023
[104] https://www.opendns.com/home-internet-security/ 11/04/2023
[105] https://www.dnsperf.com/dns-speed-benchmark 22/04/2023
[106] https://github.com/jedisct1/dnsblast 22/04/2023
[107] https://www.grc.com/dns/benchmark.htm 22/04/2023
[108] https://www.paessler.com/download/prtg-download?download=1 22/04/2023
[109] https://comunidad.jazztel.com/t5/ADSL-Fibra/SOLUCIONADO-Cambiar-DNS-router-livebox/td-p/41771 22/04/2023
[110] https://www.malwarepatrol.net/pfblockerng-configuration-guide/ 23/04/2023
[111] https://help.dnsfilter.com/hc/en-us/articles/1500008110782-Test-Domains 25/04/2023
[112] https://welcome.opendns.com/ 25/04/2023
[113]https://support.umbrella.com/hc/en-us/articles/230903728-How-To-Successfully-test-to-ensure-you-re-running-Umbrella-correctly2604/2023
[114] https://firebog.net/ 26/04/2023
[115] https://forum.archive.openwrt.org/viewtopic.php?id=59803&p=4 27/04/2023
[116] https://www.ismoothblog.com/2021/06/configure-pi-hole-on-openwrt-router.html 28/04/2023

[117] https://forum.openwrt.org/t/running-pihole-on-openwrt-x86-rpi-using-docker-tutorial-experiences/108144 28/04/2023
[118] https://www.balena.io/etcher/ 30/04/2023
[119] https://www.pfsense.org 2/05/2023
[120]https://support.opendns.com/hc/en-us/articles/227987727-Linux-IP-Updater-for-Dynamic-Networks 3/05/2023
[121] https://sourceforge.net/projects/ddclient/ 3/05/2023
[122] https://www.elasticourse.com/how-to-force-google-safe-search-using-dns-or-pi-hole/ 4/05/2023
[123] https://github.com/d43m0nhLInt3r/socialblocklists 4/05/2023
[124] https://discourse.pi-hole.net/t/force-safe-search-using-pi-hole/54813/2 4/05/2023
[125] https://cloudtechtips.com/linux/ubuntu/force-safesearch-using-pi-hole/396/ 4/05/2023
[126] https://mangolassi.it/topic/16905/add-porn-blocking-to-your-pi-hole 4/05/2023
[127] https://coygeek.com/docs/pihole-tiktok/ 4/05/2023
[128]https://www.reddit.com/r/pihole/comments/a9v7jj/how_to_install_a_custom_block_page_for_websites/ 4/05/2023
[129] http://desmotivaciones.es/394694/No-puedes-pasar 4/05/2023
[130]https://support.opendns.com/hc/en-us/community/posts/115001134428-Create-an-Android-and-Apple-family-shield-app 5/05/2023
[131] https://play.google.com/store/apps/details?id=com.aykutcevik.dnschanger 6/05/2023
[132] https://discourse.pi-hole.net/t/possible-to-exclude-device-from-pihole/56527 6/05/2023
[133] https://tech.lobobrothers.com/rematando-con-pfblockerng-en-pfsense/ 6/05/2023
[134] https://redinfertiles.com/red-infertiles-3/quienes-somos/ 8/05/2023
[135] https://github.com/IngoZenz/personaldnsfilter 8/05/2023
[136] https://broadbandforum.co/threads/installing-adguard-home-on-pfsense.205884/ 8/05/2023
[137] https://freedns.afraid.org/ 12/05/2023
[138] https://bobcares.com/blog/setup-openvpn-on-pfsense/ 13/05/2023
[139] https://github.com/AdguardTeam/AdGuardHome/wiki/Configuration#password-reset 13/05/2023
[140] https://docs.netgate.com/pfsense/en/latest/firewall/time-based-rules.html 15/05/2023
[141] https://bandaancha.eu/articulos/proteccion-datos-absuelve-usuario-tener-6347 15/05/2023
[142]https://www.linkedin.com/pulse/wifi-hotspot-para-hoteles-lo-que-la-ley-obliga-d%C3%ADa-de-paco-menendez/?originalSubdomain=es 16/05/2023
[143]https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101095329/program/43251567/details 18/05/2023
[144]https://www.genbeta.com/actualidad/dns4eu-dns-publicos-gratuitos-que-prepara-union-europea-para-bloquear-sitios-web-ilegales 18/05/2023
[145]https://www.ucm.es/data/cont/docs/39-2015-03-22-Gu%C3%ADa%20para%20padres%20y%20educadores%20sobre%20el%20uso%20seguro%20de%20Internet,%20videojuegos%20y%20m%C3%B3viles.pdf 22/05/2023
[146] https://www.privacyaffairs.com/ip-filtering-pfsense/ 22/05/2023
[147] https://youtu.be/sppZXLTWVdY 22/05/2023
[148] https://es.wikipedia.org/wiki/Software_como_servicio 22/05/2023
[149]https://www.welivesecurity.com/la-es/2022/07/08/vpn-funcionamiento-privacidad-informacion/ 08/06/2023
[150] https://www.manageengine.com/latam/oputils/servidor-dhcp.html 08/06/2023
[151] https://datatracker.ietf.org/doc/html/rfc2131 08/06/2023

i. Anexos

i. Anexo I: Instalación y configuración de Pfsense

Para instalar pfSense en el mini PC se ha descargado una imagen desde la página web oficial de pfSense (https://www.pfsense.org/download/), seleccionando la imagen para instalación desde USB, con consola VGA y 64 bits:

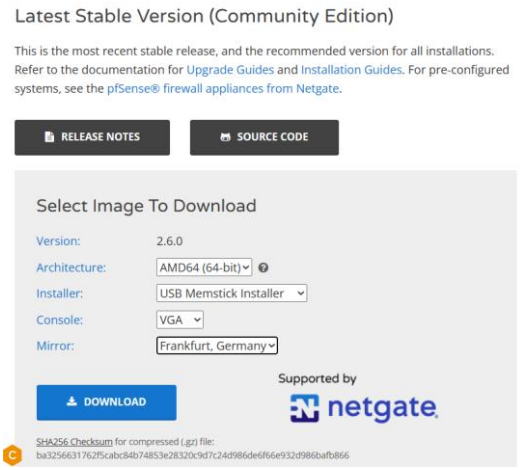


Figura 38: Descarga de la imagen de pfSense para su instalación.

Se crea un dispositivo de arranque USB con Etcher [118] y se procede a su instalación en el disco SSD, utilizando el disco completo.
Tras el primer reinicio aparece en la consola las opciones de configuración de las redes, donde se establece:

- Boca de red 1 → Interfaz WAN: 192.168.1.4/24
- Boca de red 2 → Interfaz LAN: 192.168.2.1/24
- Boca de red 3 → Interfaz OPT1: 192.168.3.1/24
- Boca de red 4 → Interfaz OPT2: 192.168.4.1/24
- Dispositivo Wifi USB → Interfaz WLAN: 192.168.5.1/24

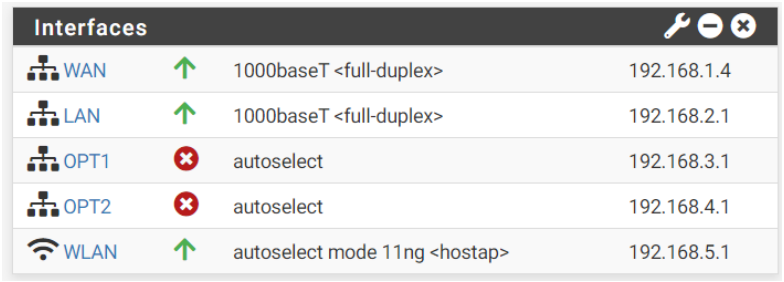


Figura 39: IPs de las interfaces de red.

Se procede a cablear el dispositivo, conectando la boca de red 1 al router LiveBox+ y la boca de red 2 al AP Wifi 192.168.2.4 con DDWRT, del que ya existe de la arquitectura de red original un cable ethernet que lo conecta al switch no gestionado que reparte el cableado ethernet por el resto del hogar (ver diagrama en sección 3.1 Arquitectura del entorno en Laboratorio). El router LiveBox+ tiene su boca WAN conectada a la ONT.

Figura 40: Vista frontal de dispositivos LiveBox+, pfSense y AP DDWRT.

Figura 41: Vista cenital y de cableado de LiveBox+, pfSense y AP DDWRT.

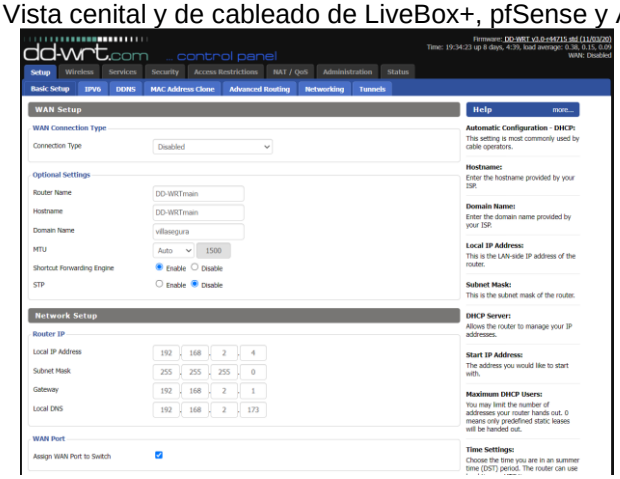


Figura 42: Configuración básica de red del DDWRT.

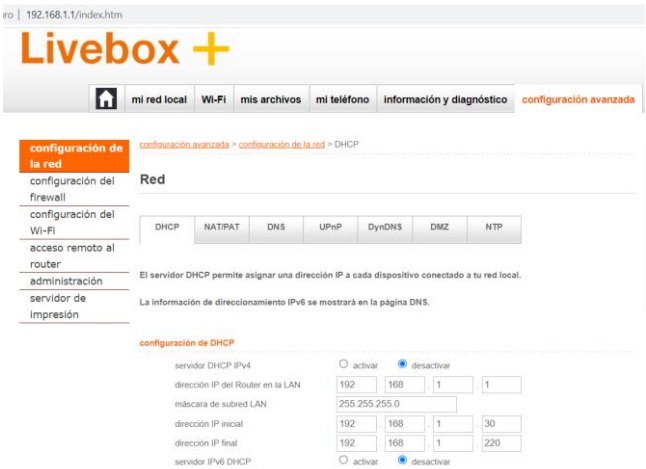


Figura 43: Configuración del Livebox+.

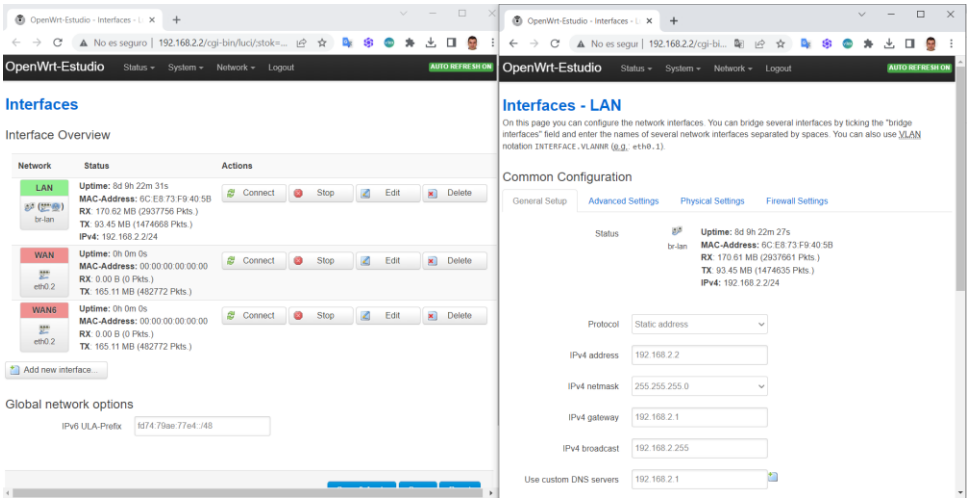


Figura 44: Configuración de red de los AP OpenWRT.

Se configuran las reglas de firewall para permitir tráfico entre la LAN y la WAN:

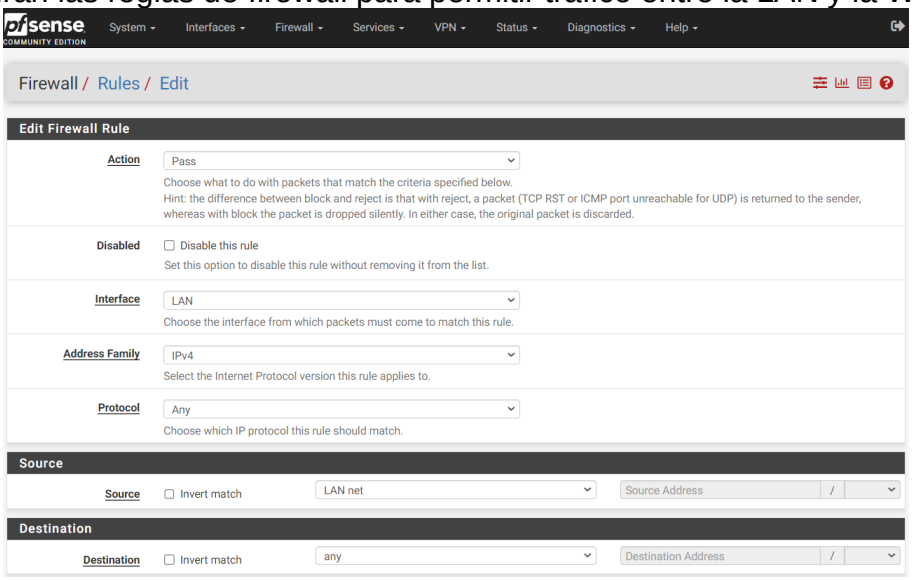


Figura 45: Configuración las reglas del firewall pfSense.

En el router pfSense, se activa el servidor DHCP en la LAN1:

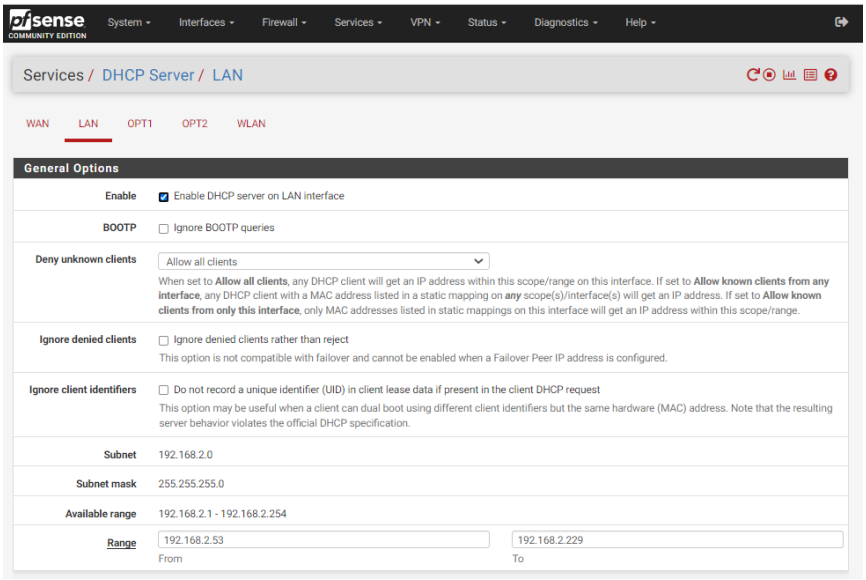


Figura 46: Configuración del DHCP server – Rango de IPs (1).

Y se establece el servidor DNS que propagará el servidor DHCP:

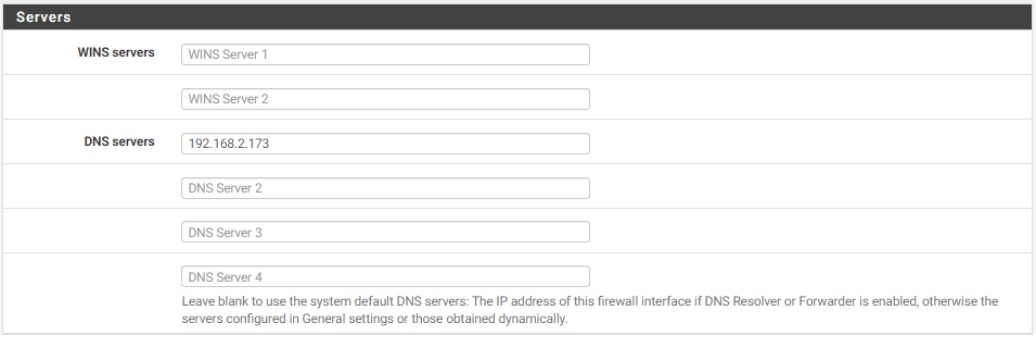


Figura 47: Configuración del DHCP server - Servidores DNS (2).

Este servidor DNS variará durante la evaluación según el Firewall DNS que se quiera probar en cada momento.

Una vez configurados los parámetros se verifica que un equipo que se conecte a la red LAN tiene asignada una IP del rango y el servidor DNS configurado, para ello se ejecuta en el equipo que se conecta:

```
ipconfig /all
```

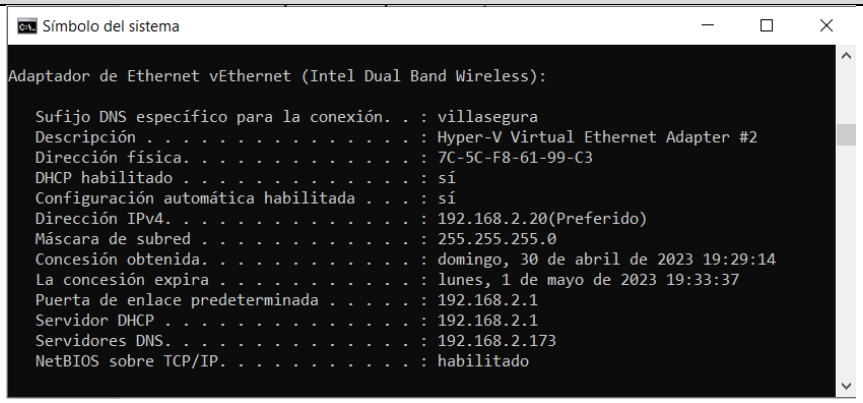


Figura 48: Verificación de asignaciones IP y servidores DNS por DHCP.

También se verifica si hay conectividad con internet haciendo un ping:

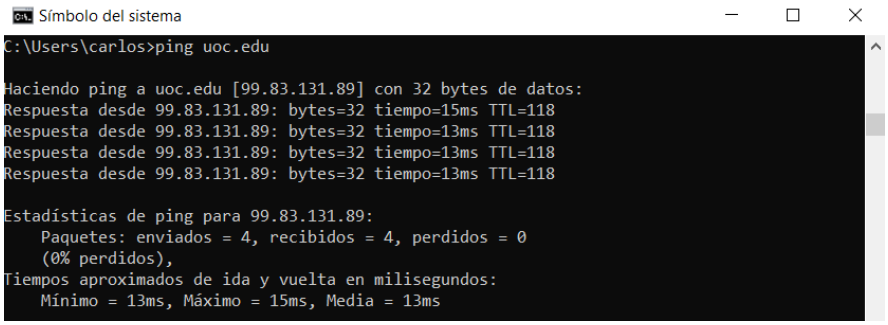
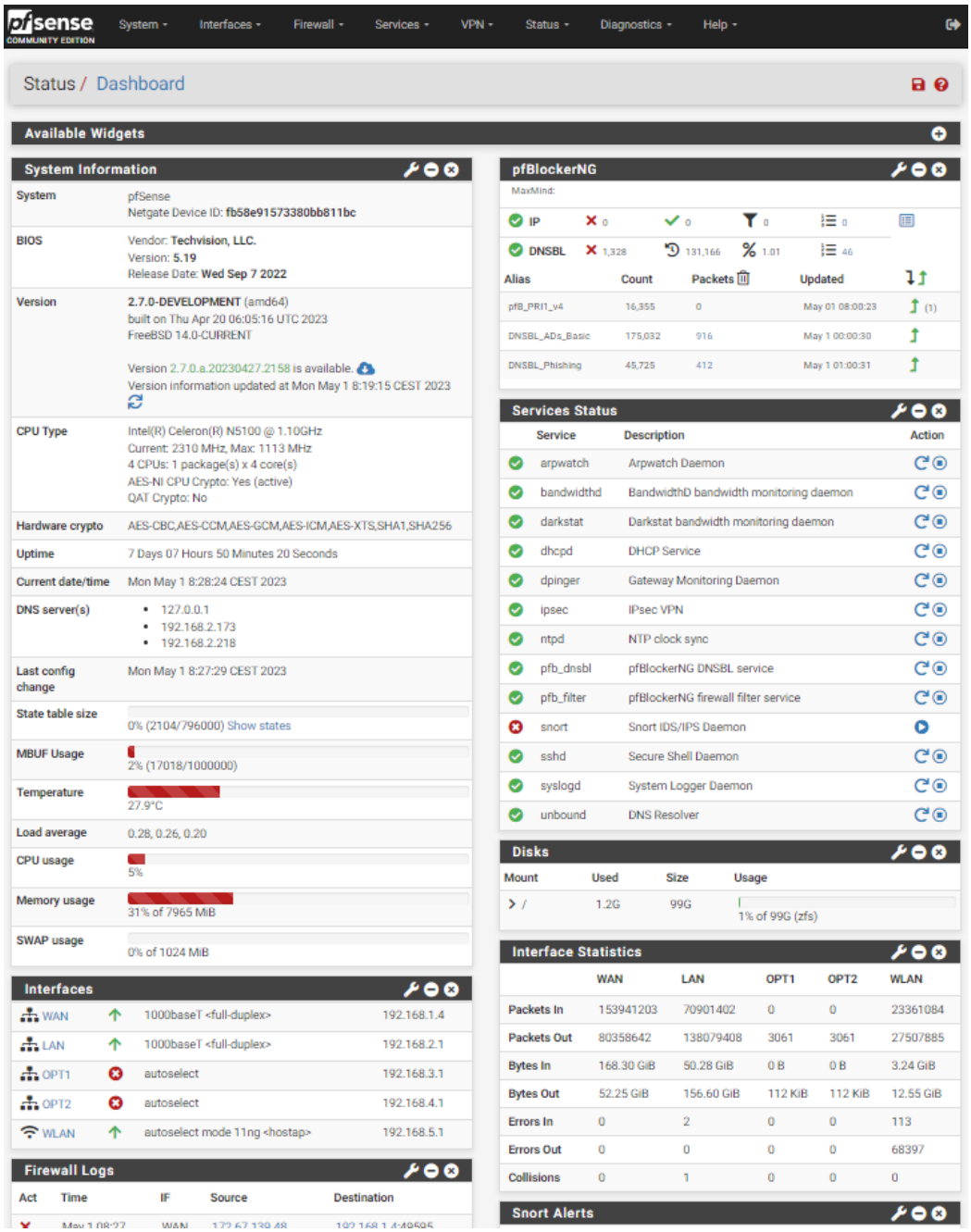


Figura 49: Verificación de conectividad a Internet por ICMP.

Finalmente se configura un layout con los widgets para la pantalla de información del firewall:



ii. Anexo II: Instalación y configuración de OpenDNS

Para instalar OpenDNS en el laboratorio se crea una cuenta de usuario en https://signup.opendns.com/homefree/.

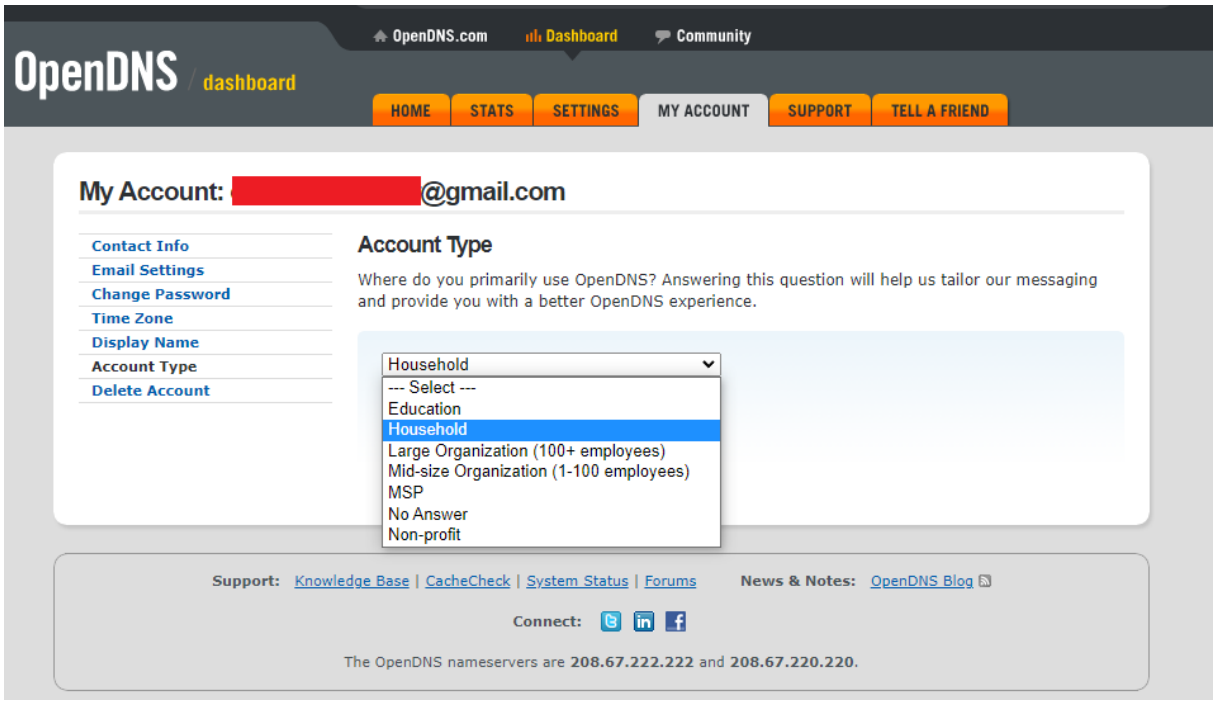


Figura 50: Configuración del tipo de cuenta en OpenDNS (1).

Una vez creada y confirmado el email ya se tiene acceso al panel de control, donde se debe acceder a settings para configurar una red:

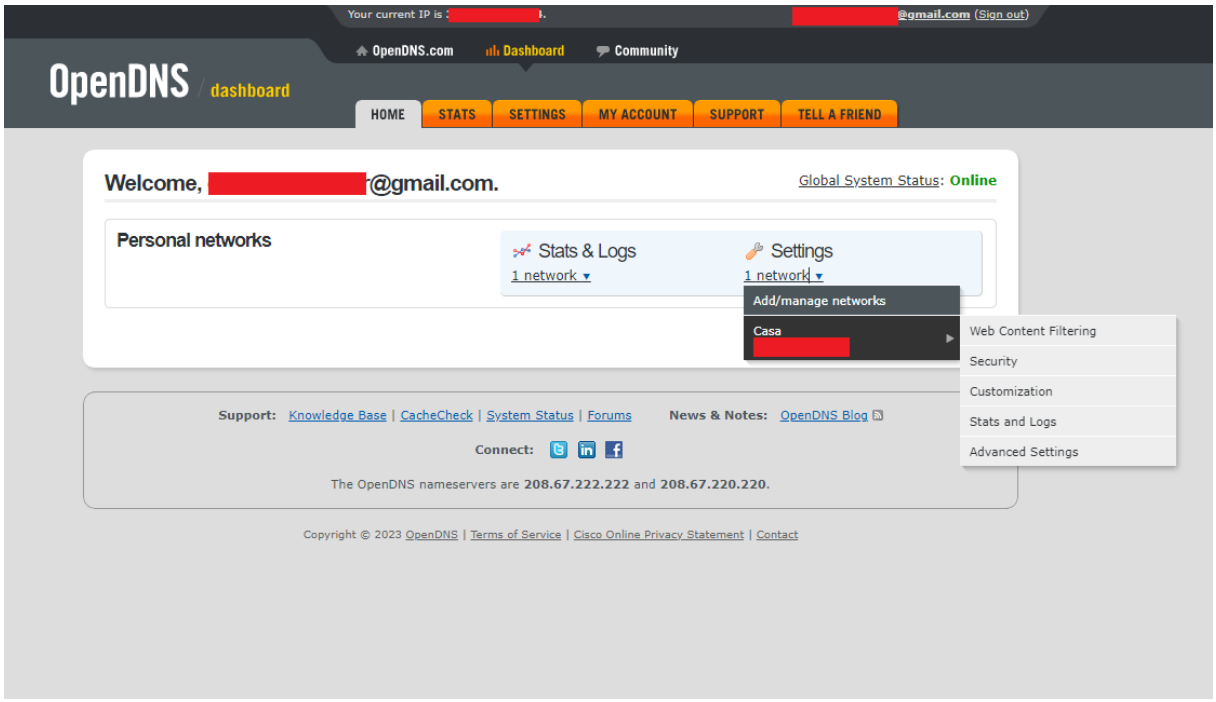


Figura 51: Configuración del tipo de cuenta en OpenDNS (2).

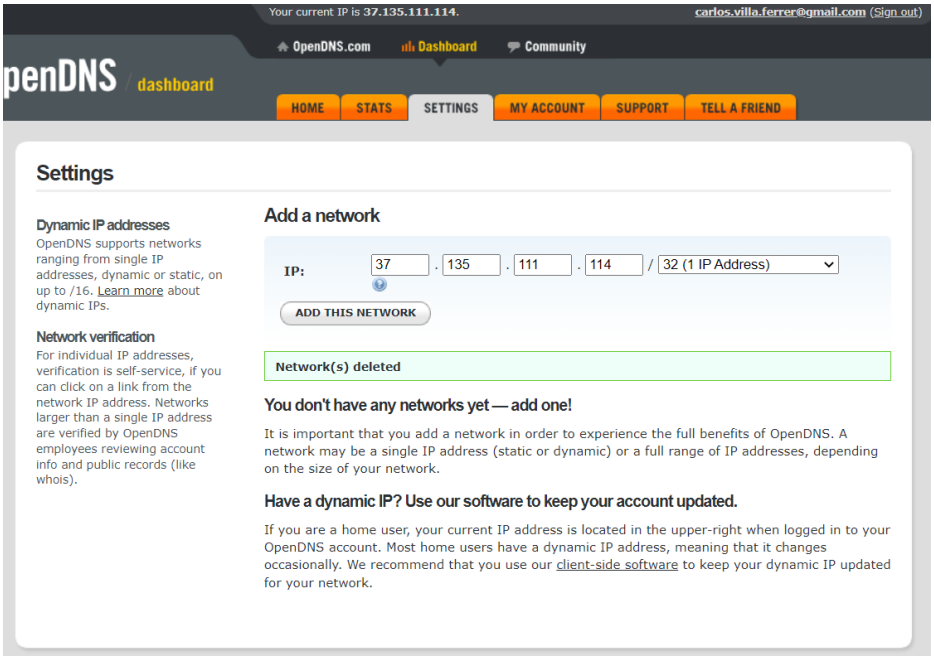


Figura 52: Crear nueva red en OpenDNS (1).

Por defecto aparece la IP de internet de nuestro router, pero, a no ser que tengamos IP fija, debe utilizarse y configurarse el software que actualiza la cuenta con la IP actualizada de la red.
Se añade la red, a la que se le llama 'casa' y se indica que es una IP dinámica:

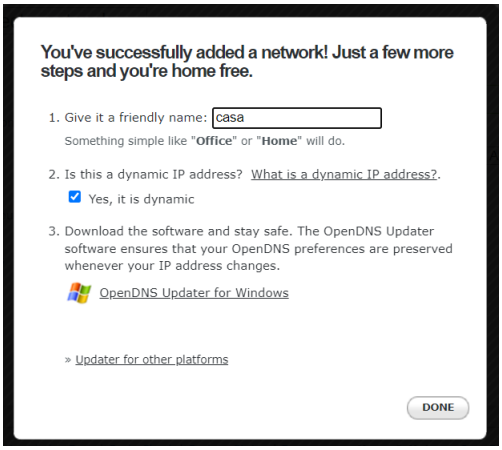


Figura 53: Crear nueva red en OpenDNS (2).

Dado que se ha configurado un router pfSense, se utilizará su cliente de Dynamic DNS para actualizar la IP, para ello se selecciona "Services→Dynamic DNS→Dynamic DNS Clients" y se pulsa el botón "Add" donde se selecciona:

- Service Taype= OpenDNS
- Hostname= casa (el nombre de la red que se ha creado en el paso anterior).
- Username y Password/Confirm= los datos de acceso a la cuenta OpenDNS.
- Description= "OpenDNS - Actualiza cuenta" (para localizar la entrada fácilmente)

Si todo es correcto se activa automáticamente y se marca con un Check bajo la columna status, indicando la IP publica bajo la columna Cached IP:

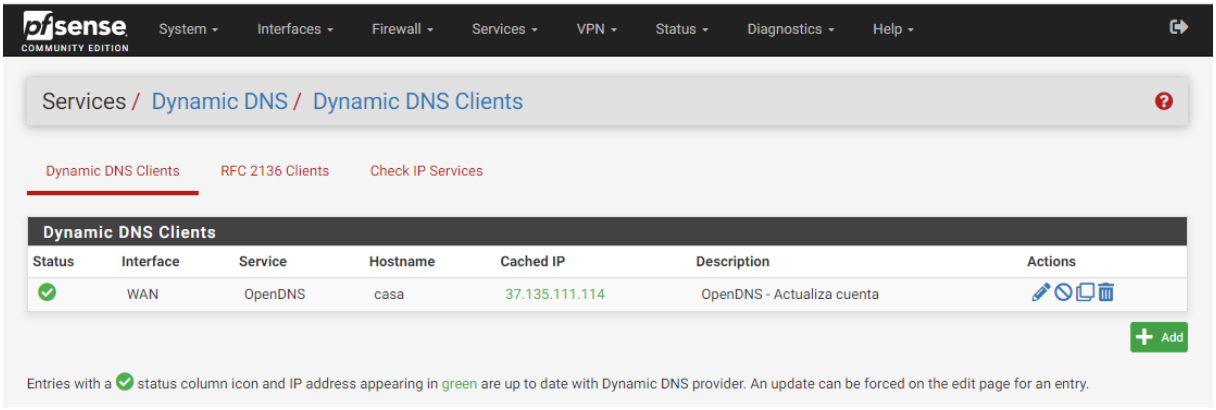


Figura 54: Actualización del DNS dinámico de OpenDNS desde pfSense.

A continuación se continúa configurando OpenDNS, estableciendo cada pantalla de configuración de la siguiente manera:
Activar las estadísticas y logs, marcando la casilla correspondiente y pulsando “Apply”:

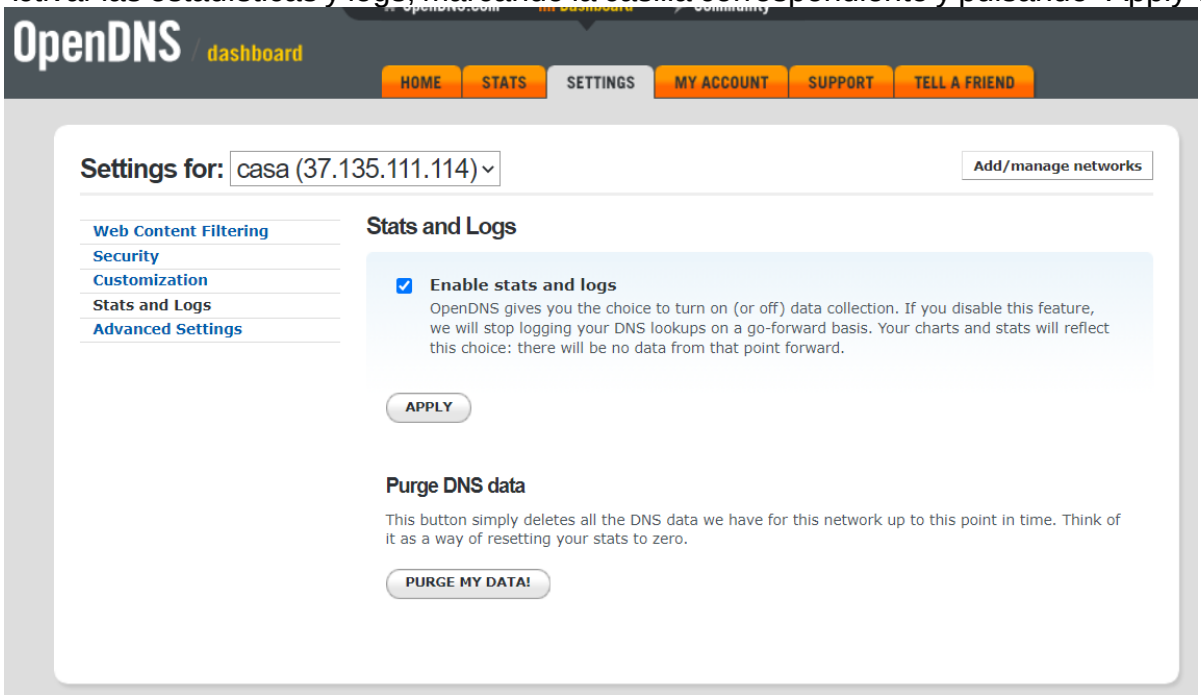


Figura 55: Activar estadísticas y logs de OpenDNS.

En “Web content Filtering”, se selecciona “High” y después “customize”, seleccionando adicionalmente: “Academic Fraud” y “German Youth Protection”:

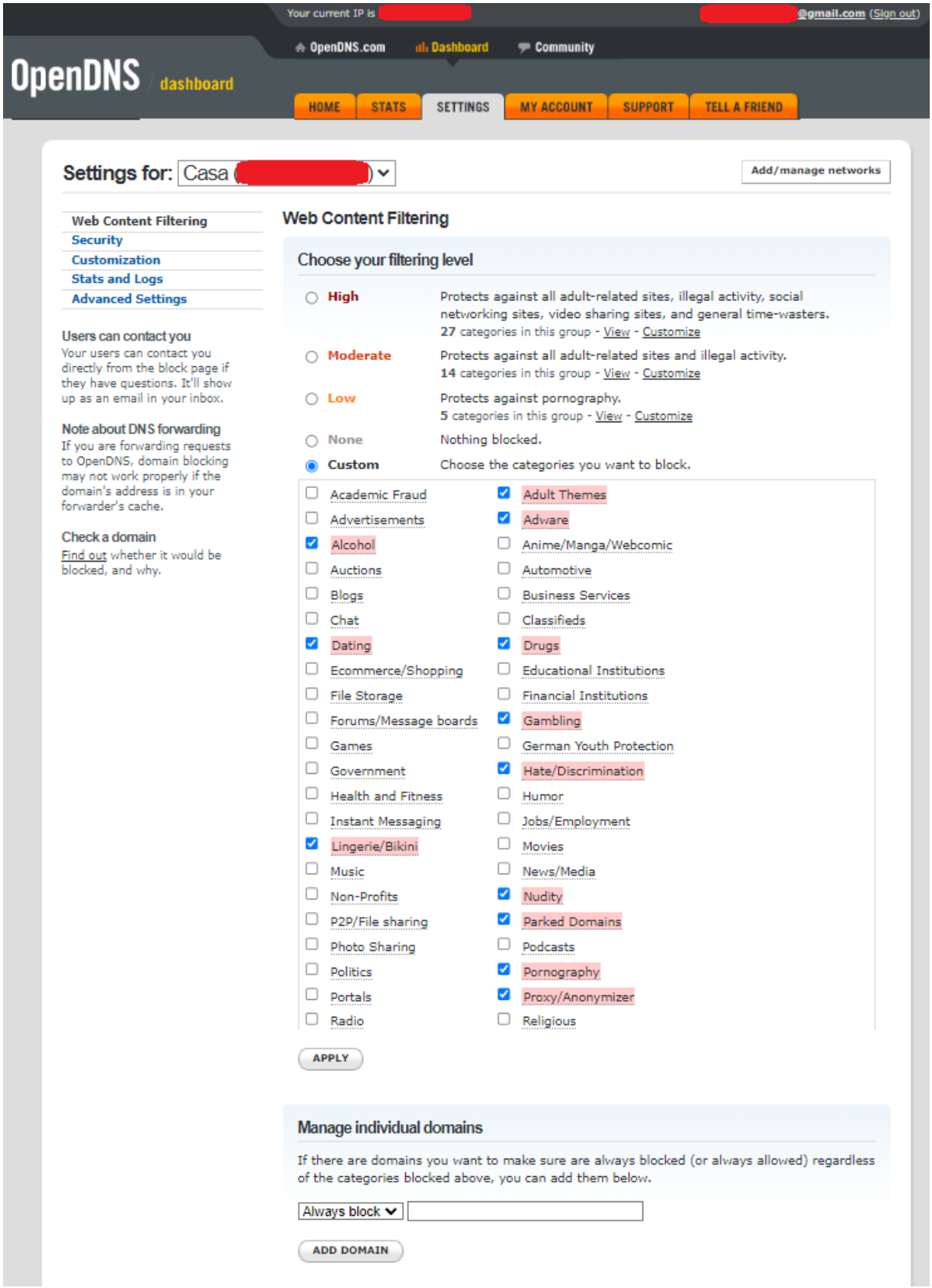


Figura 56: Activar filtrado de contenidos de OpenDNS.

La sección Settings->Security se configura de la siguiente manera:

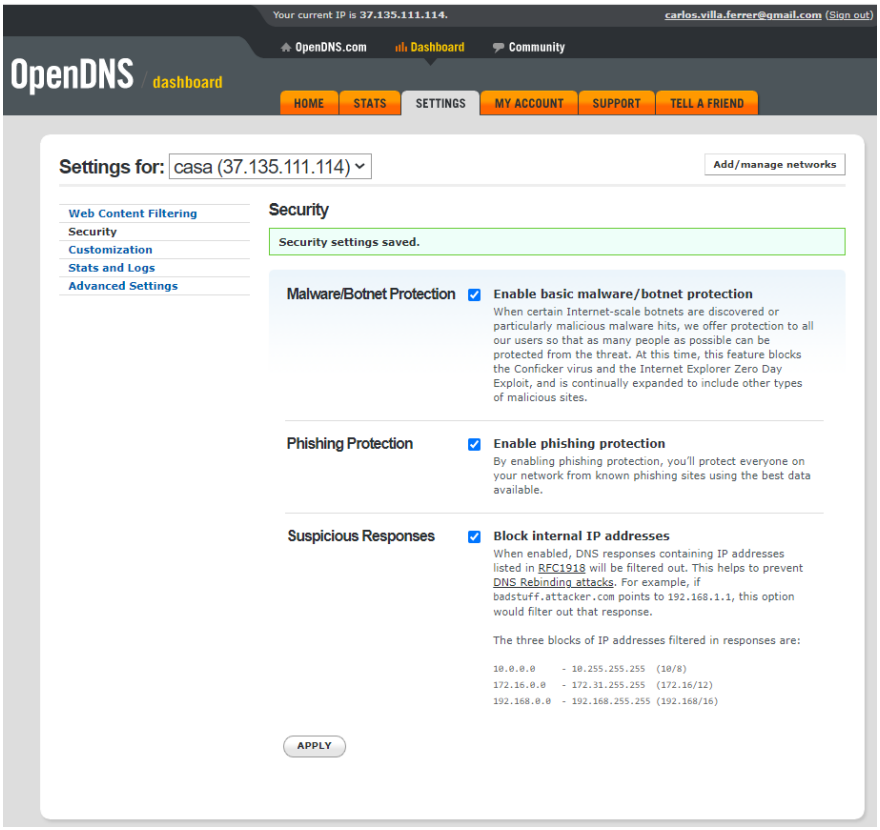


Figura 57: Activar protección contra Malware, Phishing y DNS rebinding.

En el apartado “customization” añadimos una imagen que aparecerá cada vez que OpenDNS bloquee el acceso a un sitio:

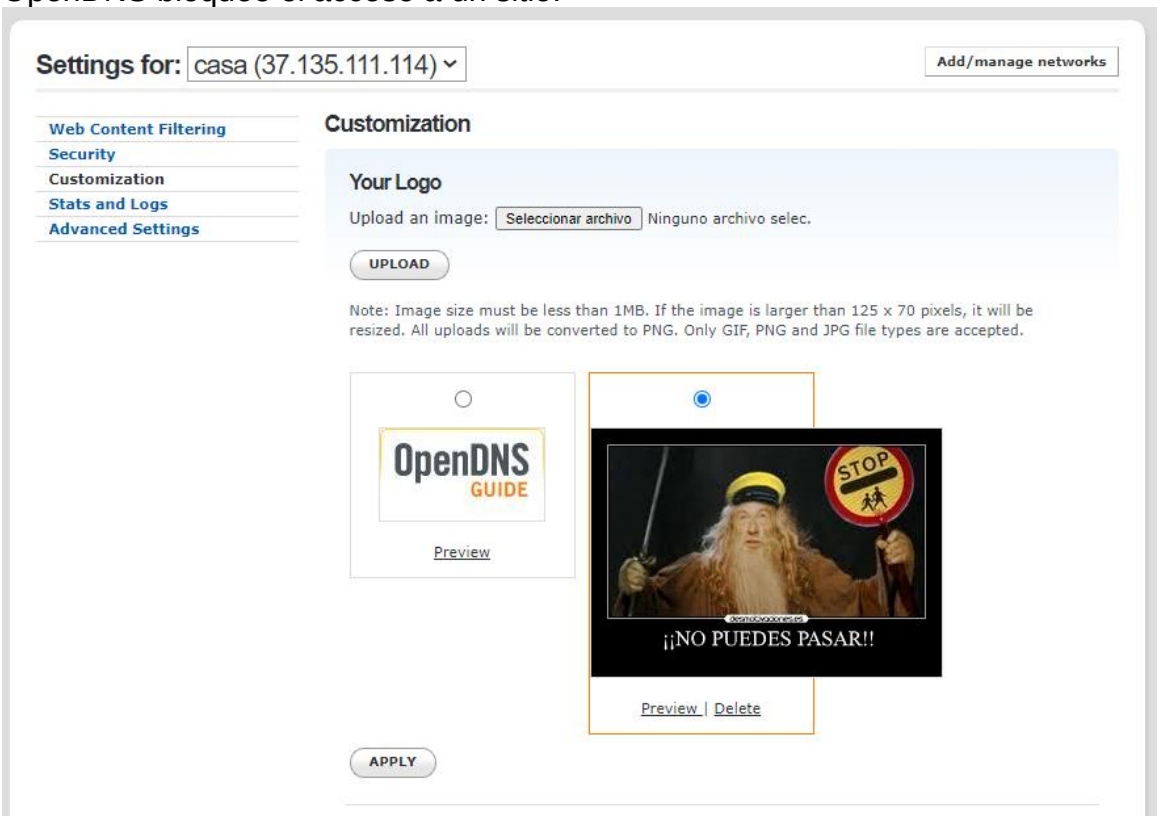


Figura 58: Personalización de la pantalla de bloqueo en OpenDNS.

A continuación se personalizan los mensajes de advertencia al usuario:

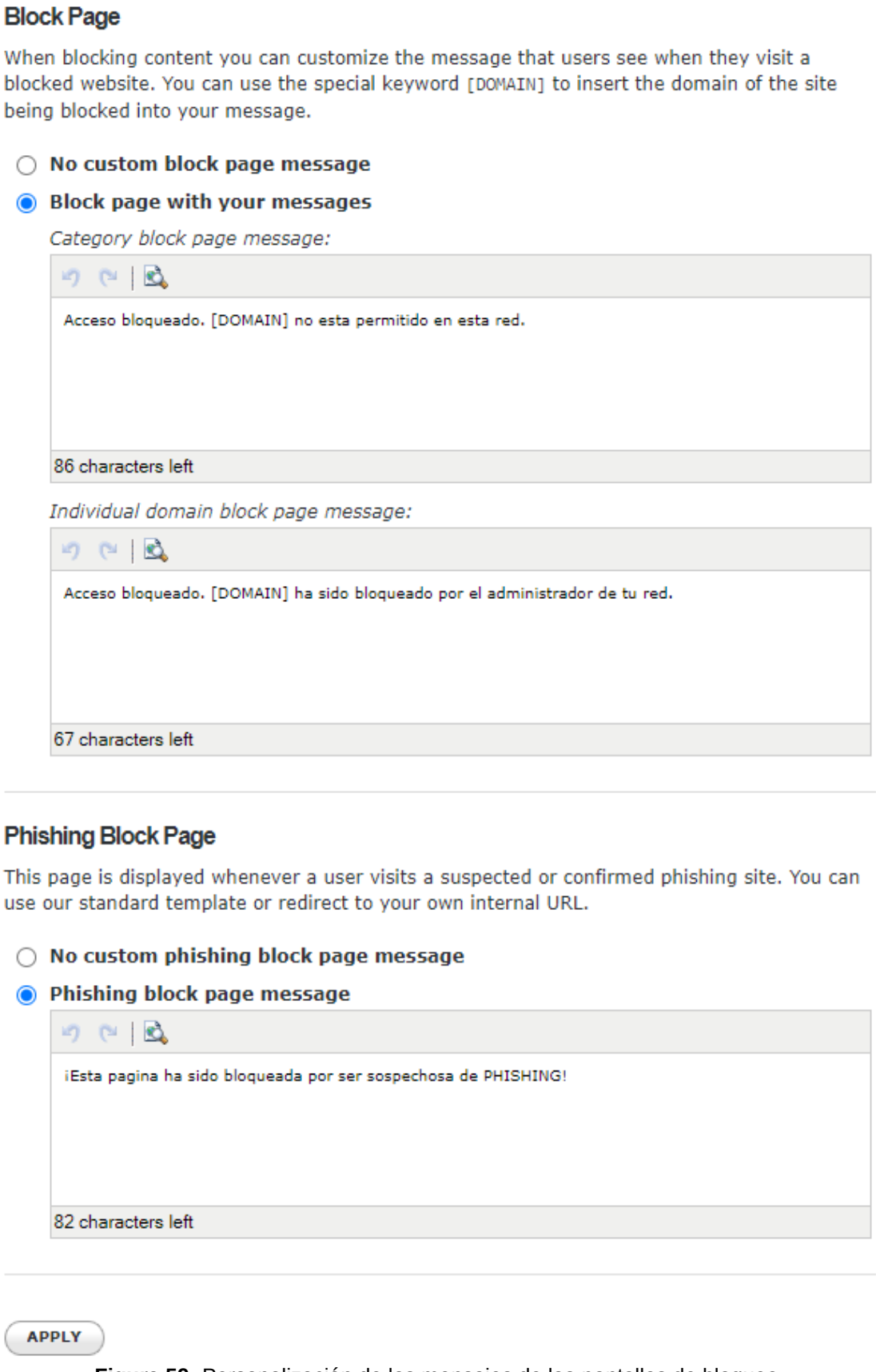


Figura 59: Personalización de los mensajes de las pantallas de bloqueo.

Para verificar el correcto funcionamiento, se configuran las DNS de OpenDNS en el servidor DHCP y se vuelve a conectar a la red, se abre un navegador y se intenta acceder a una página que se ha bloqueado temporalmente en la configuración de filtrado:

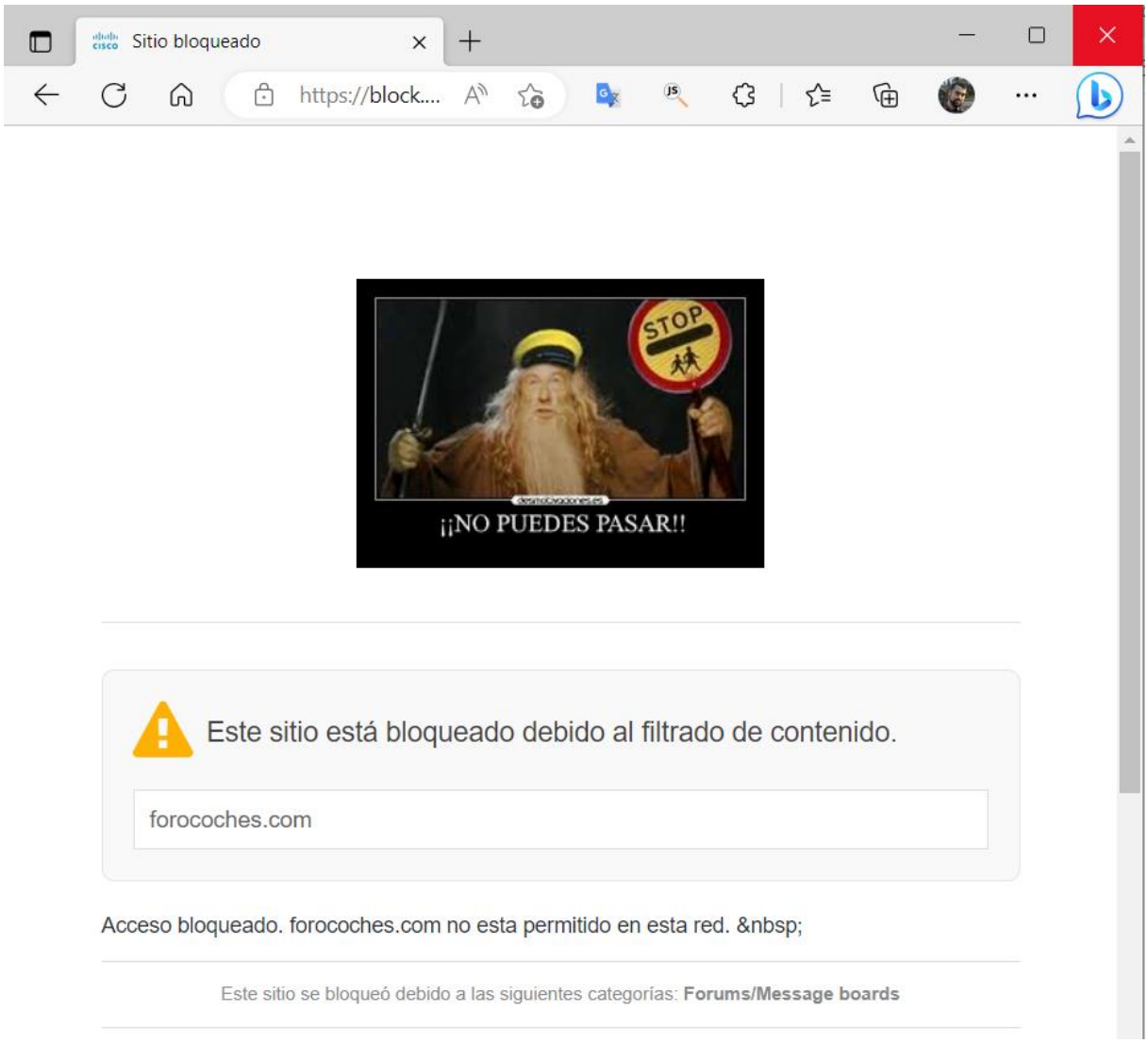


Figura 60: Pantalla de bloqueo en OpenDNS.

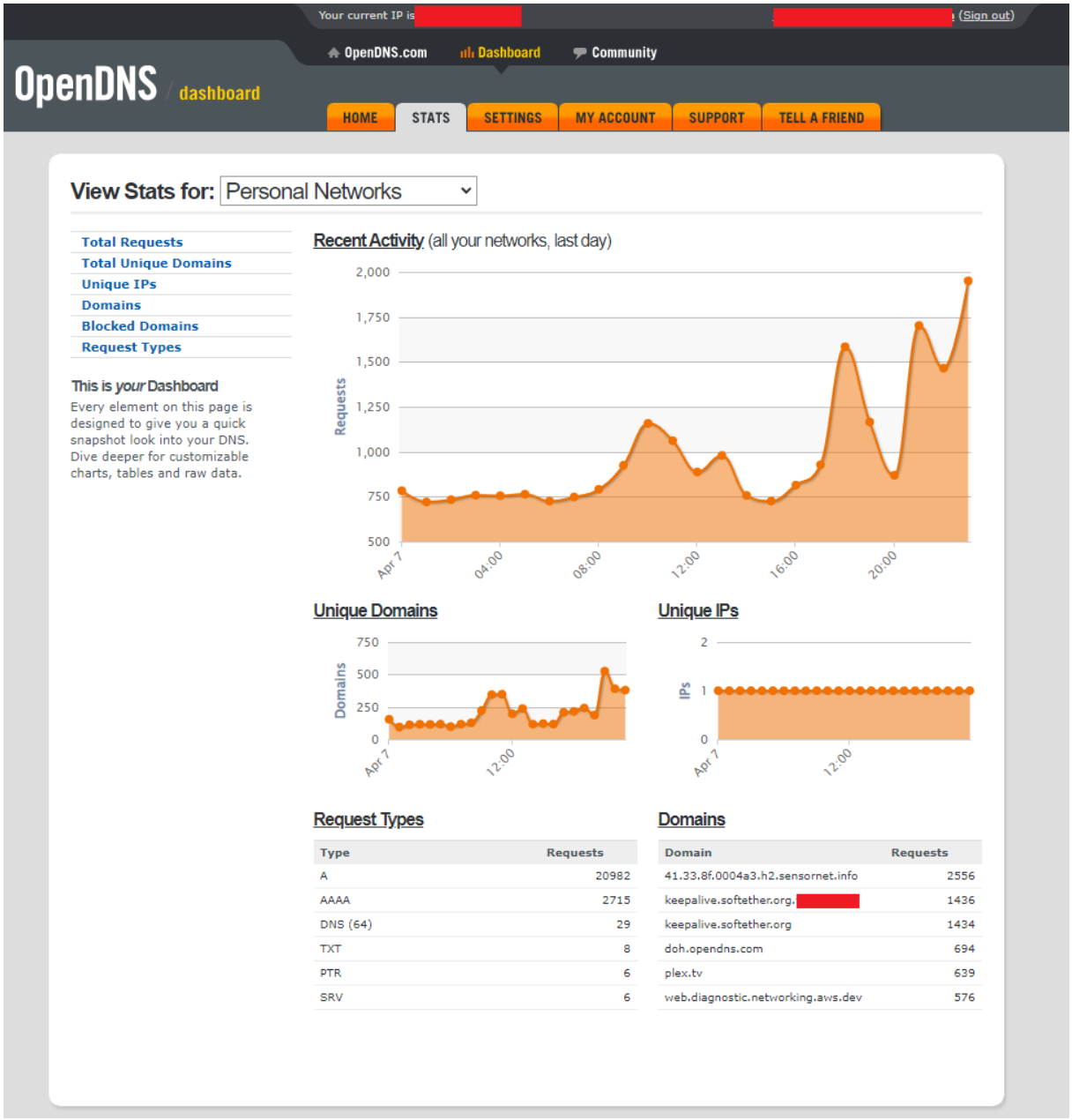


Figura 61: Estadísticas de uso en OpenDNS.

iii. Anexo III: Instalación y configuración de AdGuard Home

Se instala el plugin Adguard Home en el servidor TrueNas, bajo una Jail, que es el equivalente a un Docker de Linux en FreeBSD.
Puesto que existe una imagen de la Jail disponible como plugin, basta con acceder al menú Plugins del servidor TrueNas, seleccionar el Plugin y pulsar instalar:

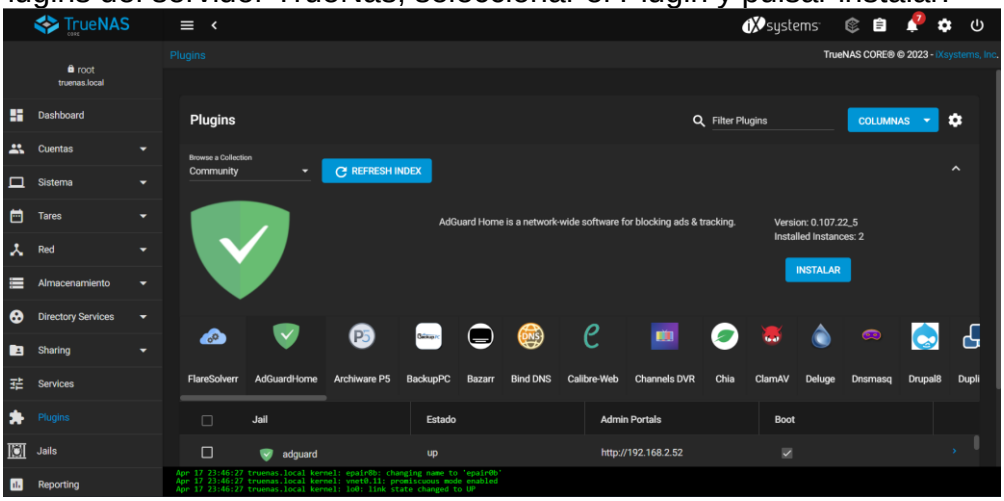


Figura 62: Selección de la instalación del plugin Adguard Home.

Se introducen los parámetros de creación de la Jail, en este caso se da un nombre a la Jail y al Plugin y se selecciona una asignación de IP por DHCP. Una vez se pulsa guardar se inicia el proceso de instalación:

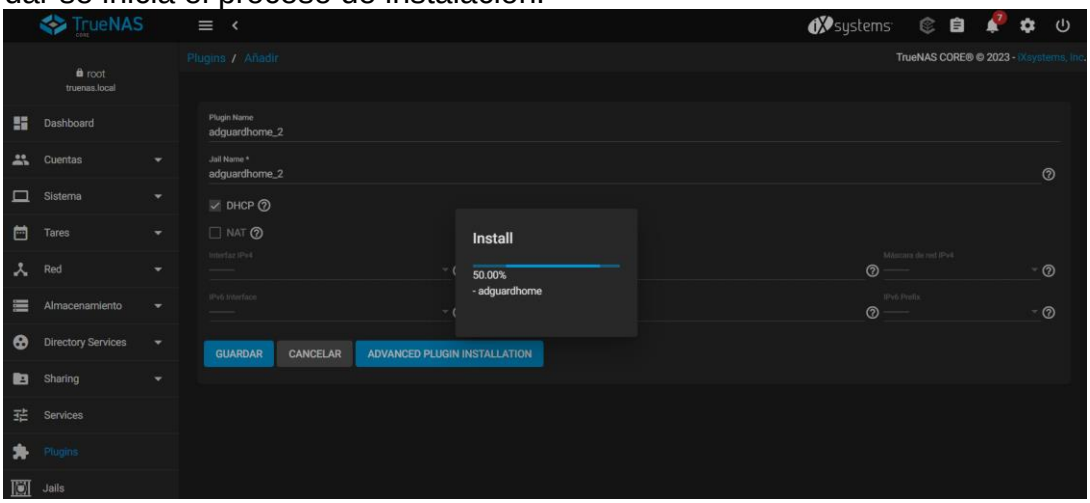


Figura 63: Progreso de la instalación de Adguard Home.

Una vez concluido el proceso se mostrará un mensaje similar al siguiente, con la IP y el portal de administración:

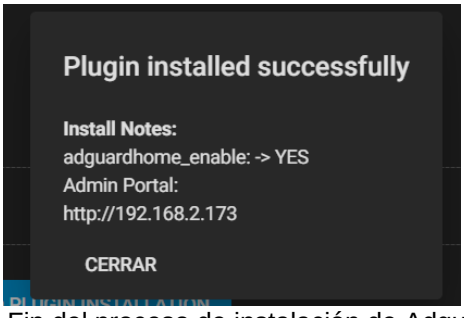


Figura 64: Fin del proceso de instalación de Adguard Home.

Una vez instalado, en las 'Post Install Notes', se indica el usuario por defecto para acceder a la herramienta, que se cambia tras el primer inicio de sesión:

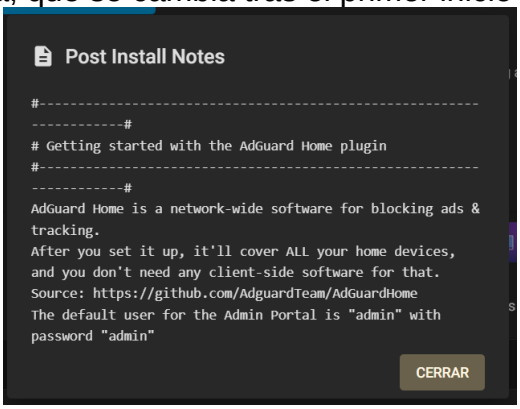


Figura 65: Post Install Notes de Adguard Home.

A través del botón "manage" se accede al portal web de gestión de la herramienta:

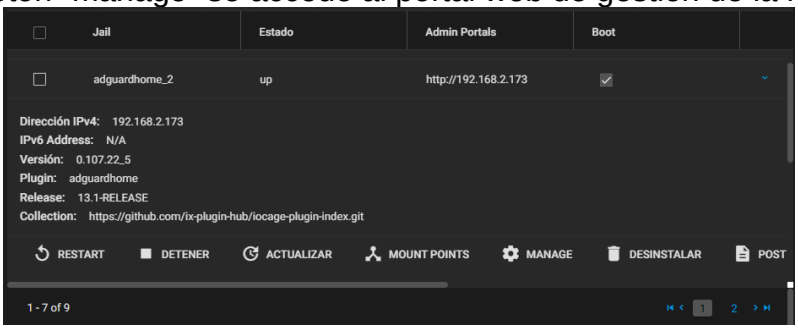


Figura 66: Menú de acciones sobre un Plugin de TrueNas.

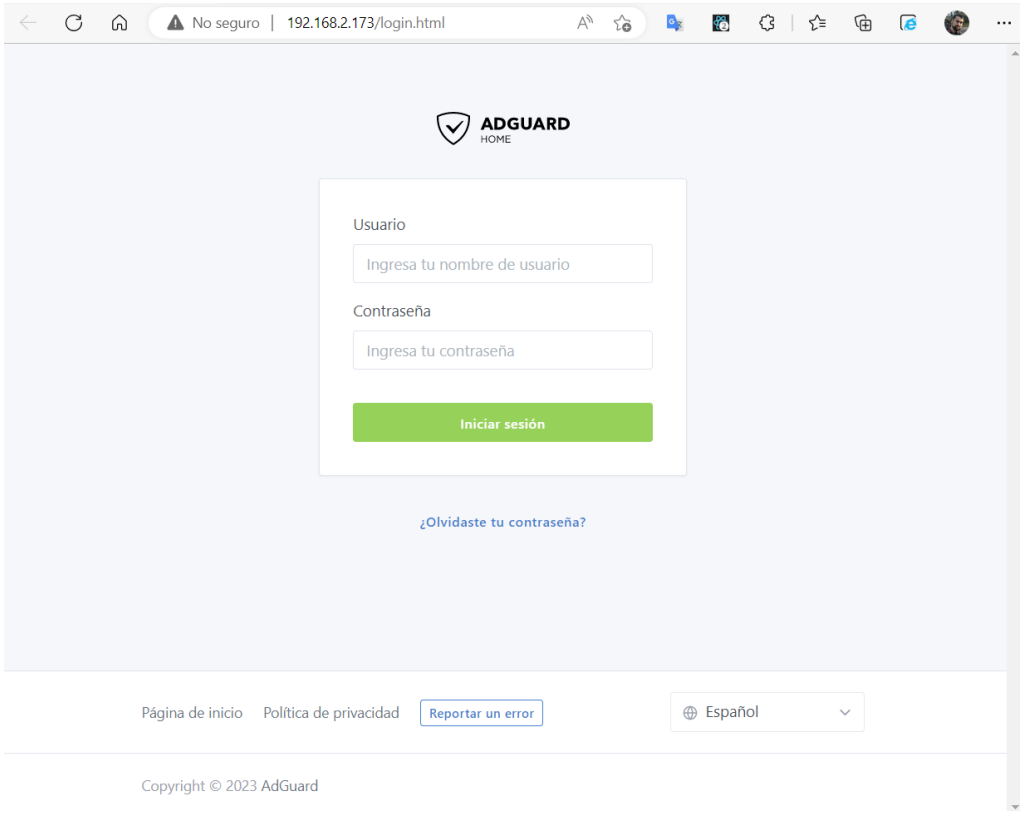


Figura 67: Login al portal de Adguard Home.

La primera vez se accede con admin/admin (contraseña por defecto, que se debe cambiar desde la web de administración tras el primer login) y se muestra el panel de control:

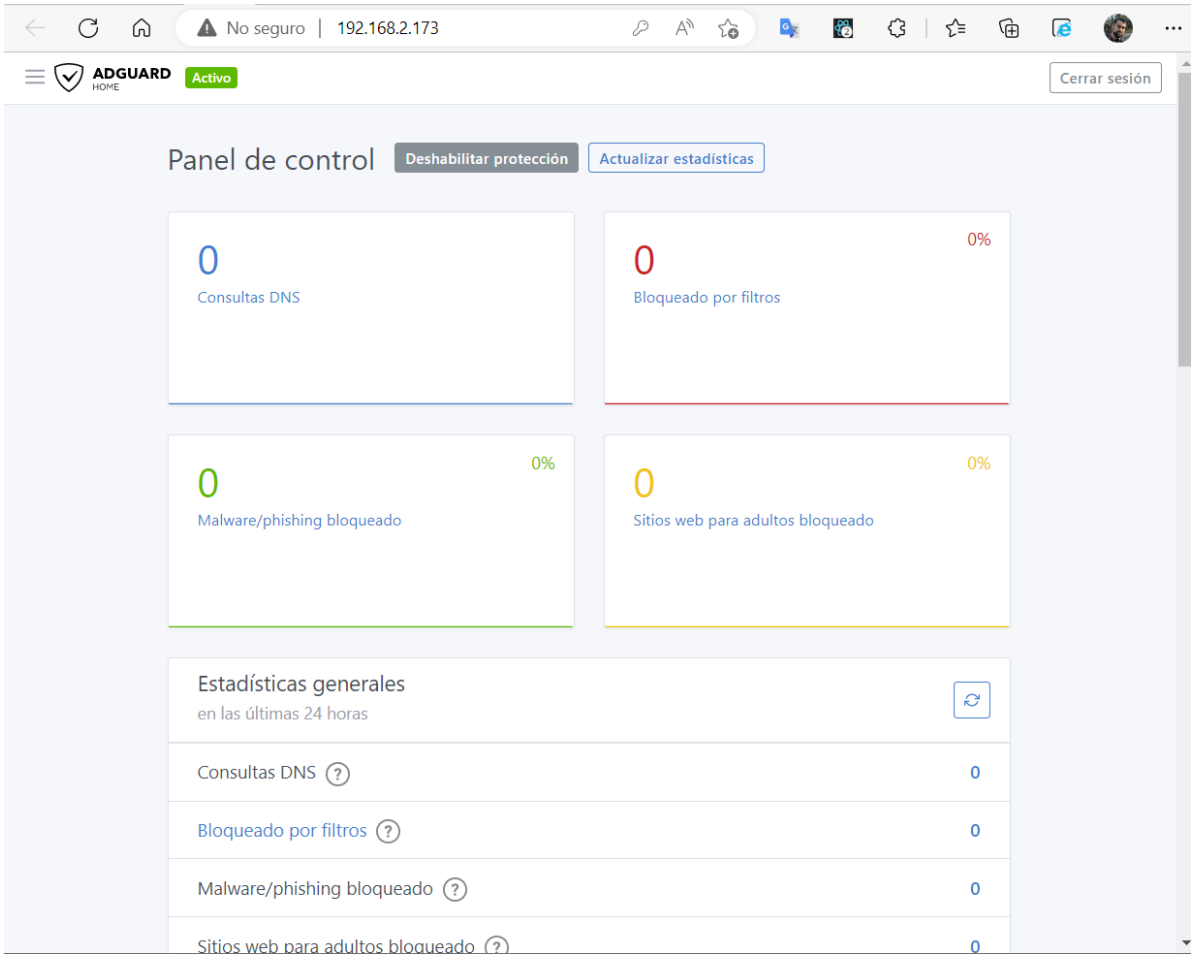


Figura 68: Panel de control de Adguard Home.

Se accede al menú Configuración->Configuración General y se establecen los parámetros como configuración por defecto, incluyendo el bloqueo con filtros, actualización horaria de las listas de bloqueo, bloqueo de phishing y malware, control parental y búsquedas seguras para menores, todo el proceso es muy sencillo y solo hay que seguir el orden de los parámetros que aparecen en la página web, estableciéndolos tal como se muestra en las siguientes imágenes:

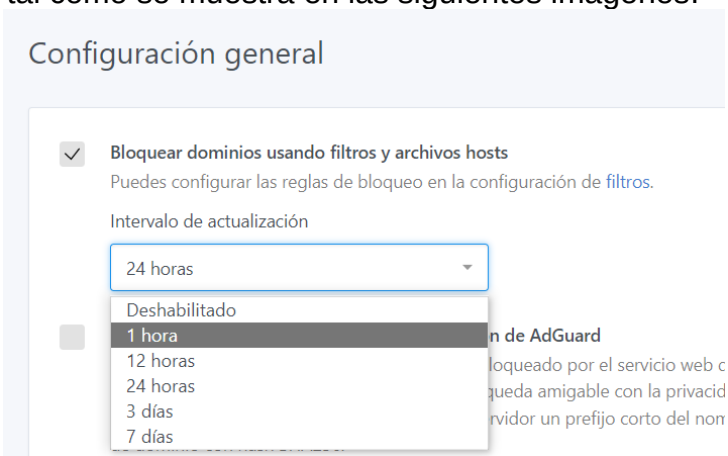


Figura 69: Uso de filtros y actualizaciones horarias en Adguard Home.

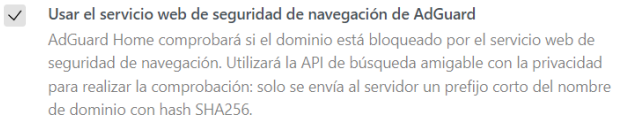


Figura 70: Bloqueo de phishing y malware en Adguard Home.

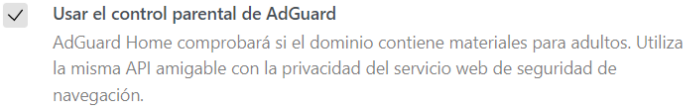


Figura 71: Activación del filtrado de control parental en Adguard Home.

Cuando se accede a una página protegida por el control parental se muestra la página siguiente:

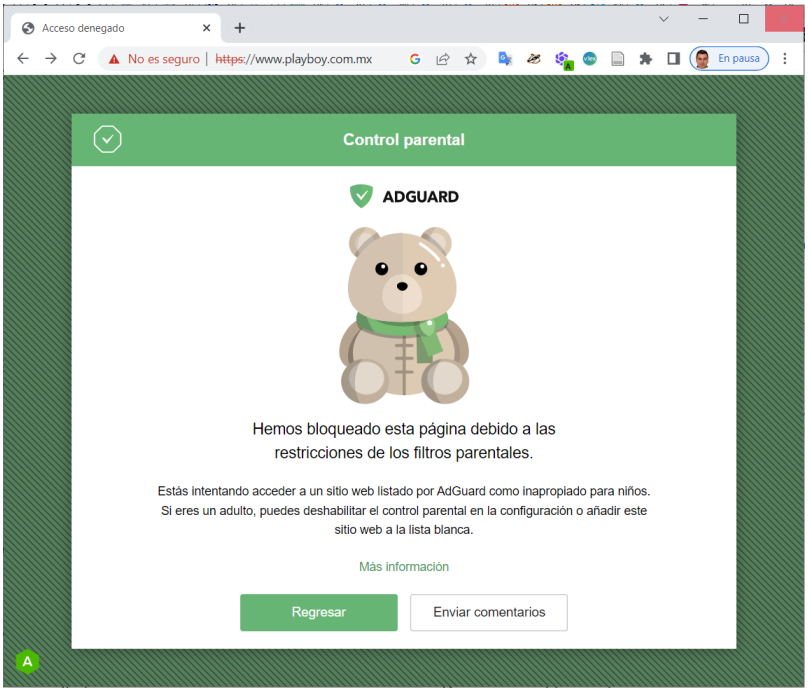


Figura 72: Aviso de filtrado de control parental en Adguard Home.

A continuación, se habilita la búsqueda segura para evitar contenidos no aptos para menores en búsquedas:

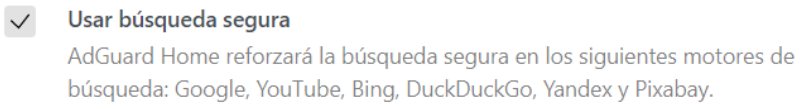


Figura 73: Forzado de uso de búsquedas seguras.

Adicionalmente se activa la casilla de habilitar el registro de actividad, pero **no se anonimiza la IP de los clientes** para poder analizar el comportamiento y uso de la herramienta:

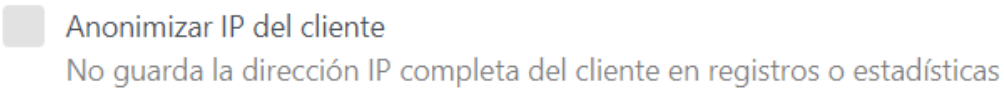


Figura 74: Anonimización de la IP del cliente en Adguard Home.

Para el análisis de la herramienta y monitorización del uso durante las pruebas, no se activa la anonimización, pero en una configuración final, activarlo respeta que no se almacenen las IPs de los clientes por lo que conlleva mantener el anonimato de los usuarios.

Se activa el registro de consultas por un periodo de 90 días y las estadísticas (también por 90 días) y se pulsa guardar.

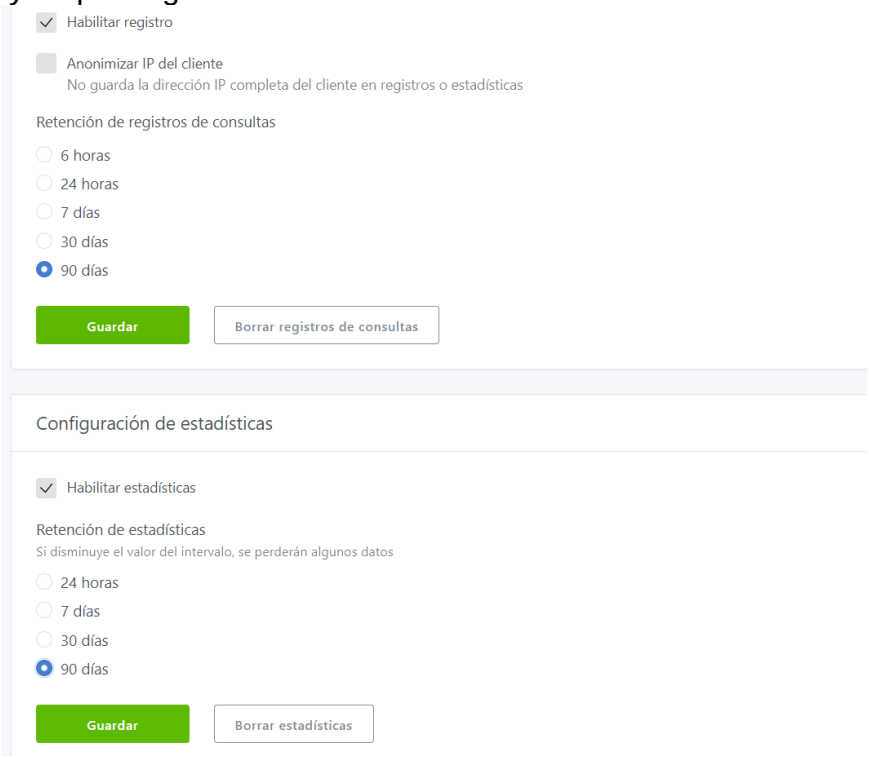


Figura 75: Registro de consultas DNS y estadísticas en Adguard Home.

A continuación, se configuran los DNS que se utilizarán de fuentes para resolver las consultas, donde se aplicarán los resultados de las pruebas realizadas en el capítulo 3.3. Se establecen como en la imagen siguiente y con consultas paralelas, para buscar la máxima velocidad de respuesta posible:

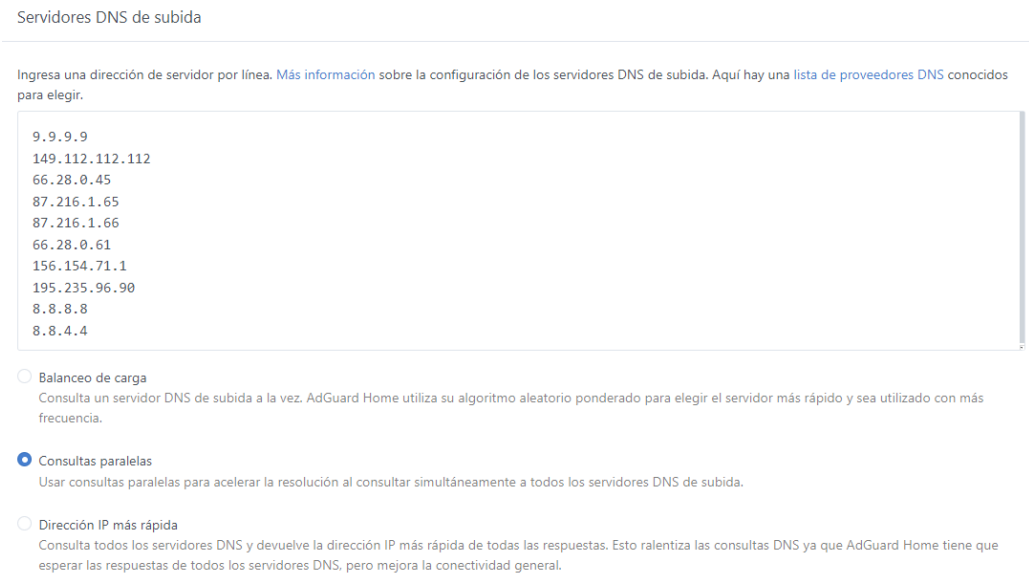


Figura 76: Fuentes DNS en Adguard Home.

Para el análisis inicial no se va a utilizar consultas DNS por HTTPS, TLS ni DNSCrypt, aunque en un sistema en producción es recomendable su uso para maximizar la privacidad, aun y así se dejan configurados DNS de arranque para, en un futuro, poderlos resolver:

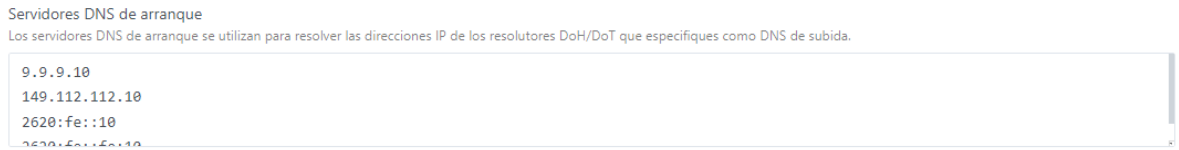


Figura 77: Fuentes DNS de arranque para TLS y HTTPS.

Adicionalmente se configuran los DNS inversos para resolver las consultas de la red local, en este caso se utilizará el router pfSense para resolverlos, puesto que tiene el servidor DHCP de la red, para ello se configuran los siguientes parámetros:

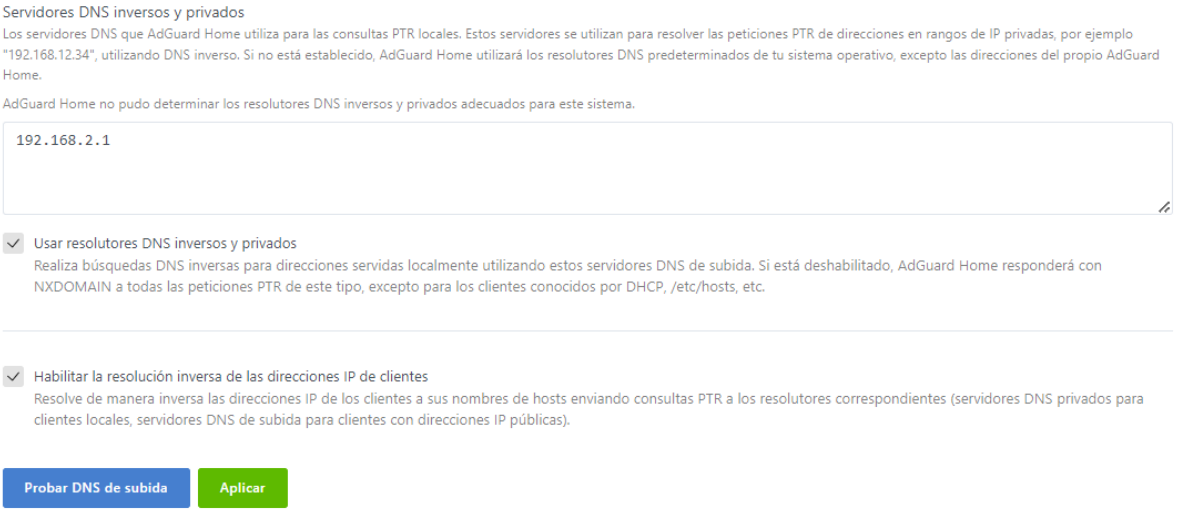


Figura 78: Configuración de DNS inverso en Adguard Home.

A continuación se configuran los parámetros del servidor DNS de Adguard Home, estableciendo el máximo de consultas por segundo y host, se desactivan las consultas

IPv6 (no se utilizan en la red de laboratorio) y se establece una dirección IP para las direcciones bloqueadas. En este caso, dado que se tendrá activo simultáneamente durante la evaluación, se aprovecha el servidor lighthttpd en el que se configura la página de bloqueo de Pi-Hole, 192.168.2.218 (ver Anexo 7.4):

Figura 79: Página de aviso de filtrado personalizada en Adguard.

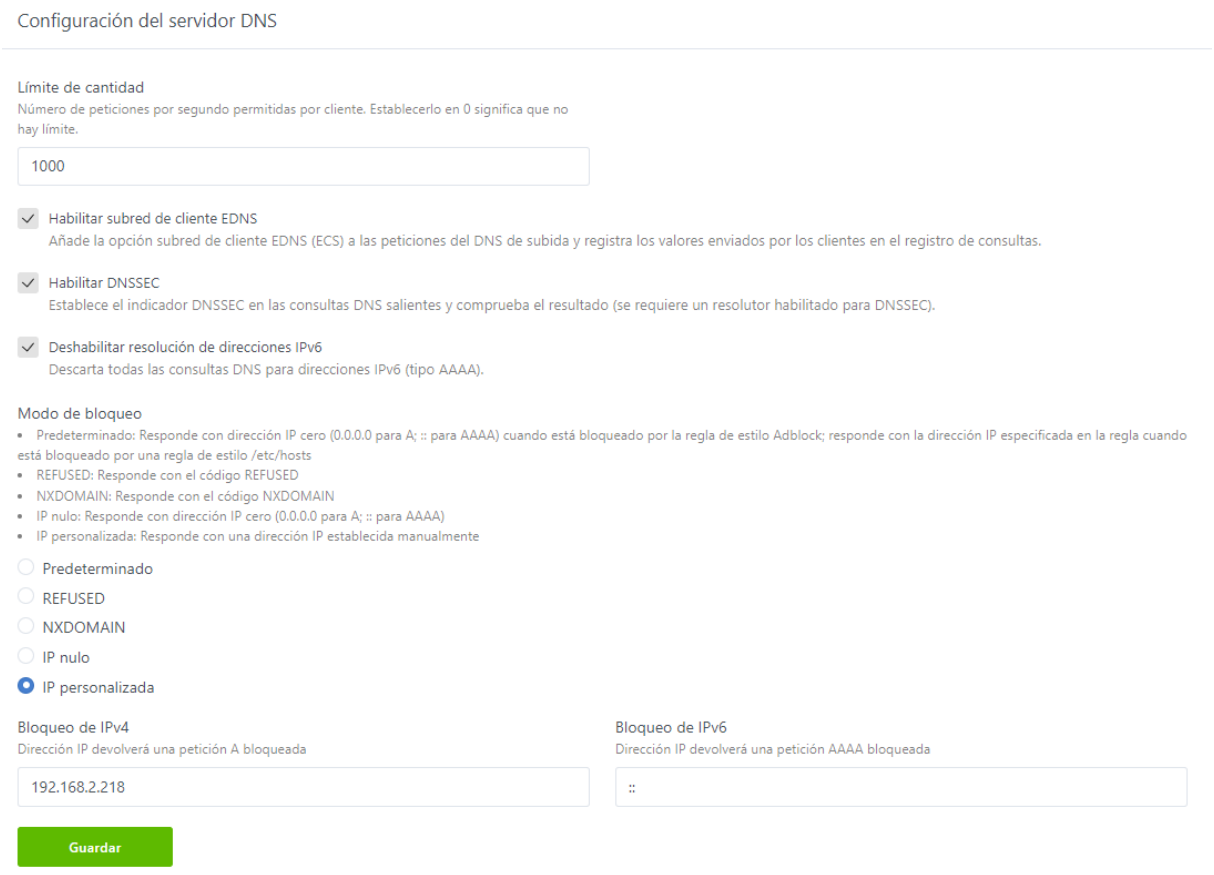


Figura 80: Configuración parámetros de servidor DNS en Adguard.

A continuación se prueban los resolutores DNS:

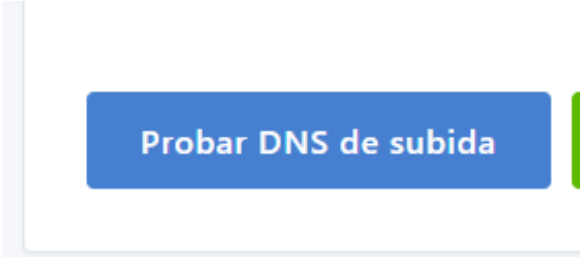


Figura 81: Prueba de configuración en Adguard Home.

Si todo ha ido bien se mostrará el siguiente mensaje:

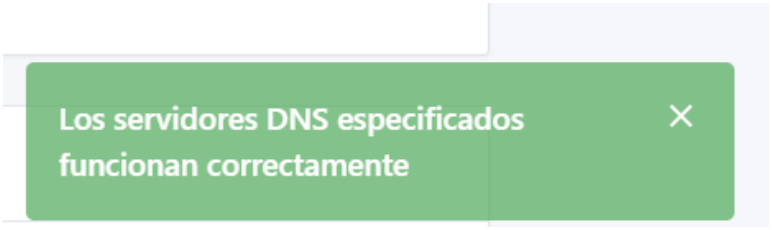


Figura 82: Resultado satisfactorio de la prueba de configuración.

Para terminar con la configuración de DNS se establecen los parámetros de caché para maximizar la velocidad de respuesta, estableciendo un día de tiempo de vida y 16 Mb de caché:

Figura 83: Parámetros de cache y rendimiento.

La configuración de cifrado se deja por defecto y la configuración de DHCP se dejan desactivadas, puesto que se utilizará el router pfSense como servidor DHCP y no se van a realizar pruebas con cifrado activado.

A continuación, se configuran los clientes de la red, desde la pantalla “Configuración de clientes”:

Cliente	Nombre	Configuración	Servicios bloqueados	DNS de subida	Etiquetas	Número de
192.168.2.1	Firewall pfsense	Personalizado	Global	Global	user_admin	186188
192.168.2.121	softether	Personalizado	Global	Global	device_other	104081
192.168.2.20	Portatil Carlos	Personalizado		Global	device_pc	81548
192.168.2.92	Efergy engage	Global	Global	Global	device_other	78857
192.168.2.96	PCCARLOS	Personalizado		Global	device_pc	72938
192.168.2.86	Iphone 11 Laura	Personalizado		Global	device_phone	48685
192.168.2.97	Portatil Laura	Personalizado		Global	device_pc	19176
192.168.2.200	Alexa - amazon-03f032ede	Global	Global	Global	device_other	17227
192.168.5.51	Portatil Carlos por red 5	Personalizado	–	Global	device_laptop	16103
192.168.2.230	TrueNAS	Personalizado	Global	Global	device_nas	12331
192.168.2.119	Movil CarlosVillaSegura	Global		Global	device_phone	5769
192.168.2.181	Iphone 14 Carlos - Trabajo	Personalizado	–	Global	device_phone	5425
192.168.2.30	LGwebOSTV	Personalizado	Global	Global	device_tv	5303
192.168.2.85	Amazon FireTV habitacion	Global		Global	device_tv	2933
192.168.2.56	Amazon-21a2d347d	Personalizado	Global	Global	device_other	1985
192.168.2.207	Xbox	Personalizado		Global	device_gameconsole	1104
192.168.2.184	Movil Laia	Global	Global	Global	–	977
192.168.2.174	Iphone 14 Carlos	Personalizado	Global	Global	device_phone	470
192.168.2.222	NintendoSwitch	Global	Global	Global	device_gameconsole	163
192.168.2.202	Termostato	Personalizado	Global	Global	device_other	126
192.168.2.189	Broadlink IR blaster RF IoT	Global	Global	Global	os_other	53
192.168.2.206	Batocera	Personalizado		Global	device_gameconsole	27

Figura 84: Personalización de configuración por dispositivo.

Para añadir una configuración personalizada para cada dispositivo cliente se pulsa “Añadir Cliente” y se debe rellenar la pantalla siguiente:

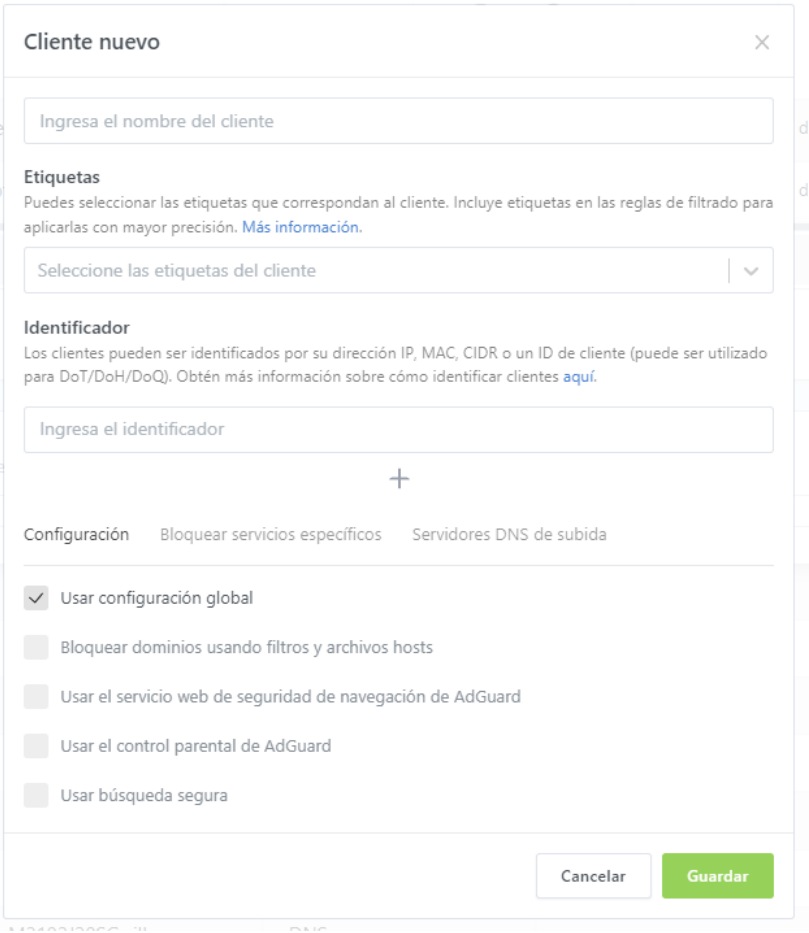


Figura 85: Edición de la configuración personalizada.

Se asigna un nombre para el dispositivo (texto libre), una etiqueta del tipo de dispositivo (PC, consola, SmartTV, Phone...) y la IP o MAC del dispositivo. Dado que se ha configurado el router pfSense con IPs persistentes durante mucho tiempo, se configuran con la IP.

En la sección inferior se puede escoger utilizar la configuración global por defecto que se ha establecido al inicio o una configuración personalizada, estableciendo la configuración específica del dispositivo. Adicionalmente se pueden filtrar servicios o aplicaciones concretas distintas a las configuradas globalmente desde la pestaña “Bloquear servicios específicos”, por ejemplo, en la Xbox, en los portátiles y en teléfonos móviles de los menores se configuran de la siguiente manera:

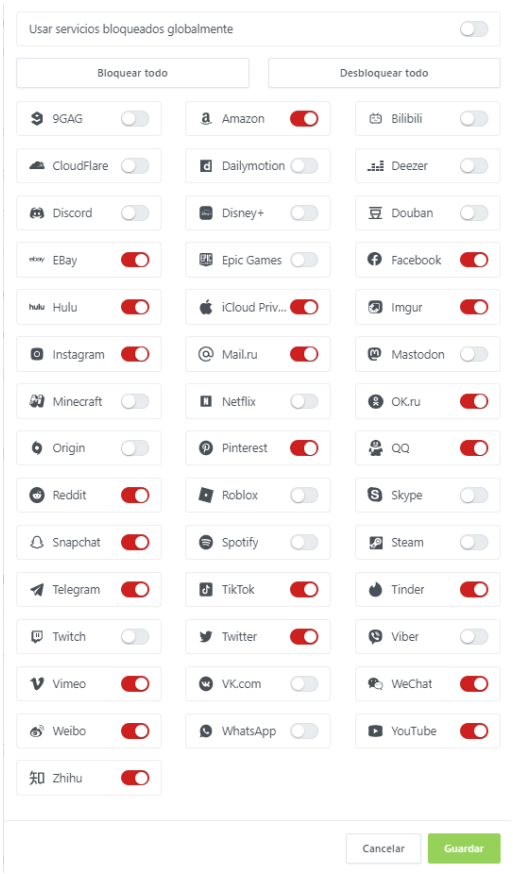


Figura 86: Bloqueo de servicios en el dispositivo Xbox.

Se verifica el correcto funcionamiento del filtrado, tomando como ejemplo Youtube en la Xbox, tanto desde la app como desde el navegador:

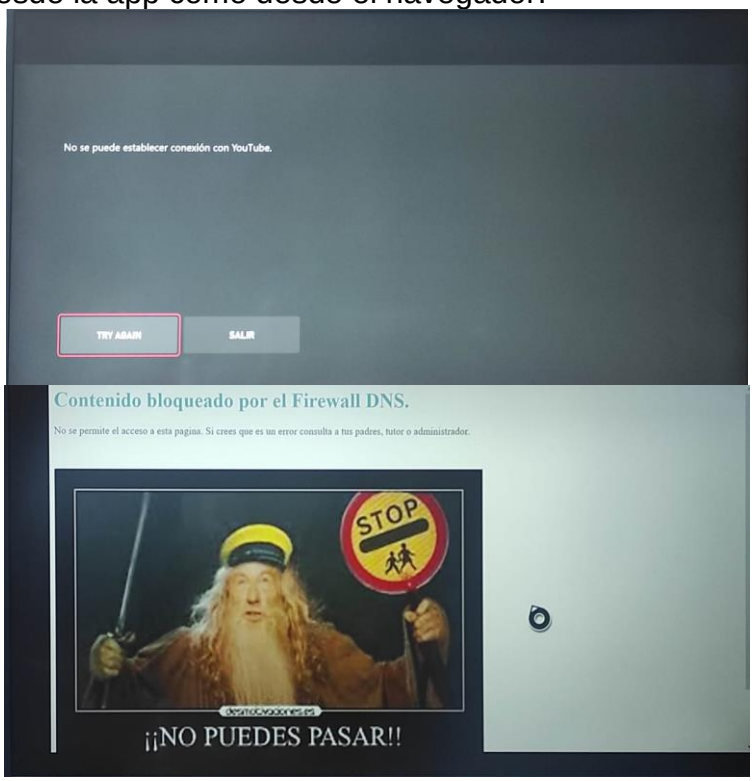


Figura 87: Verificación del bloqueo de servicios en el dispositivo Xbox.

A continuación, se configuran los filtros de contenidos que procederán de listas RPZ, desde la opción del menú Filtros->Listas de Bloqueo DNS. Se configuran las siguientes listas que se ofrecen desde el propios menú 'Añadir lista de bloqueo' de Adguard Home:

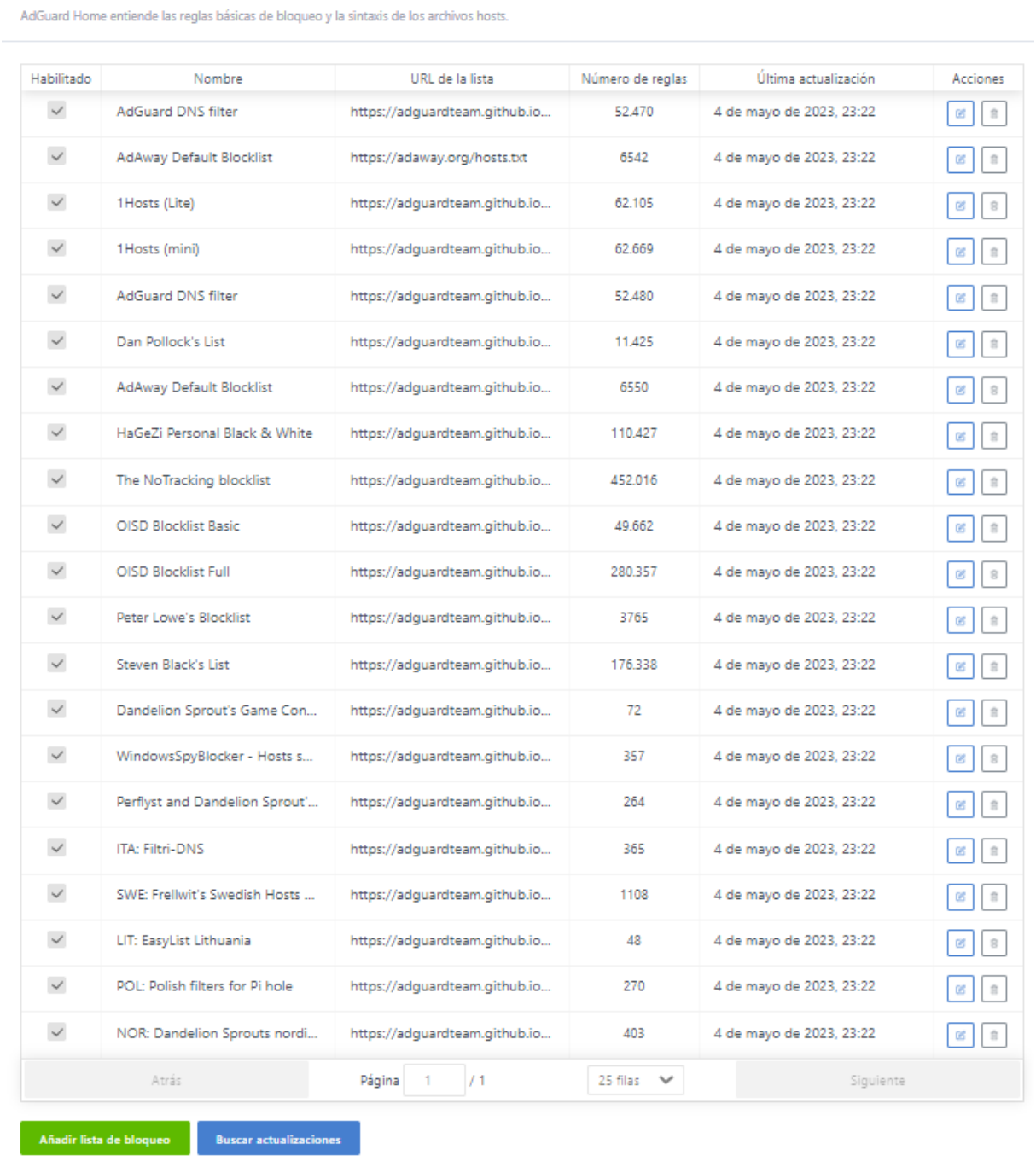


Figura 88: Configuración de listas de bloqueo.

Es posible añadir listas de bloqueo personalizadas o de otras fuentes, para hacerlo se debe escoger Añadir lista personalizada tras pulsar en 'Añadir lista de bloqueo':

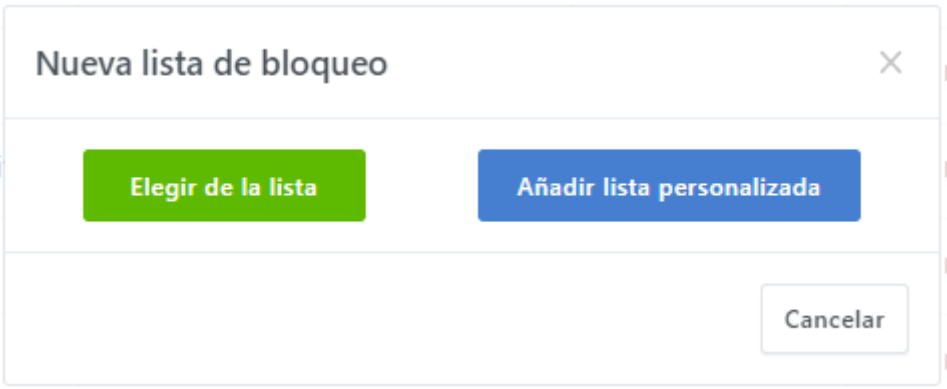


Figura 89: Configuración de listas de bloqueo personalizadas en Adguard.

Al hacerlo se mostrará una ventana que solicitará darle un nombre a la lista y una URL donde se encuentra la lista de bloqueo.

Las listas blancas (Listas de permitido DNS) no se requieren configuran por el momento, pero si durante las pruebas aparece alguna página que debe ser desbloqueada se añadiría en esta sección:

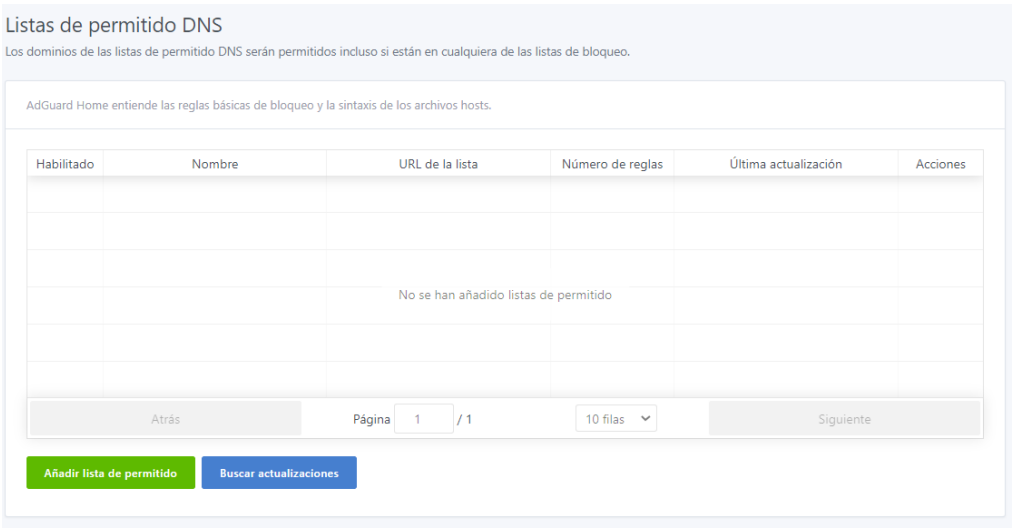


Figura 90: Listas blancas en Adguard Home.

Desde reescrituras DNS se podrían proteger URL que dispongan de ‘modo seguro’ para menores y que no estén soportadas en la configuración activada anteriormente:

Figura 91: Reescrituras DNS en Adguard Home.

En servicios bloqueados se definen los servicios que se bloquean por defecto en cualquier dispositivo que no esté dado de alta o se configure en el modo por defecto que implica el 'usar configuración global'.

Por defecto se configura bloquear los siguientes servicios:

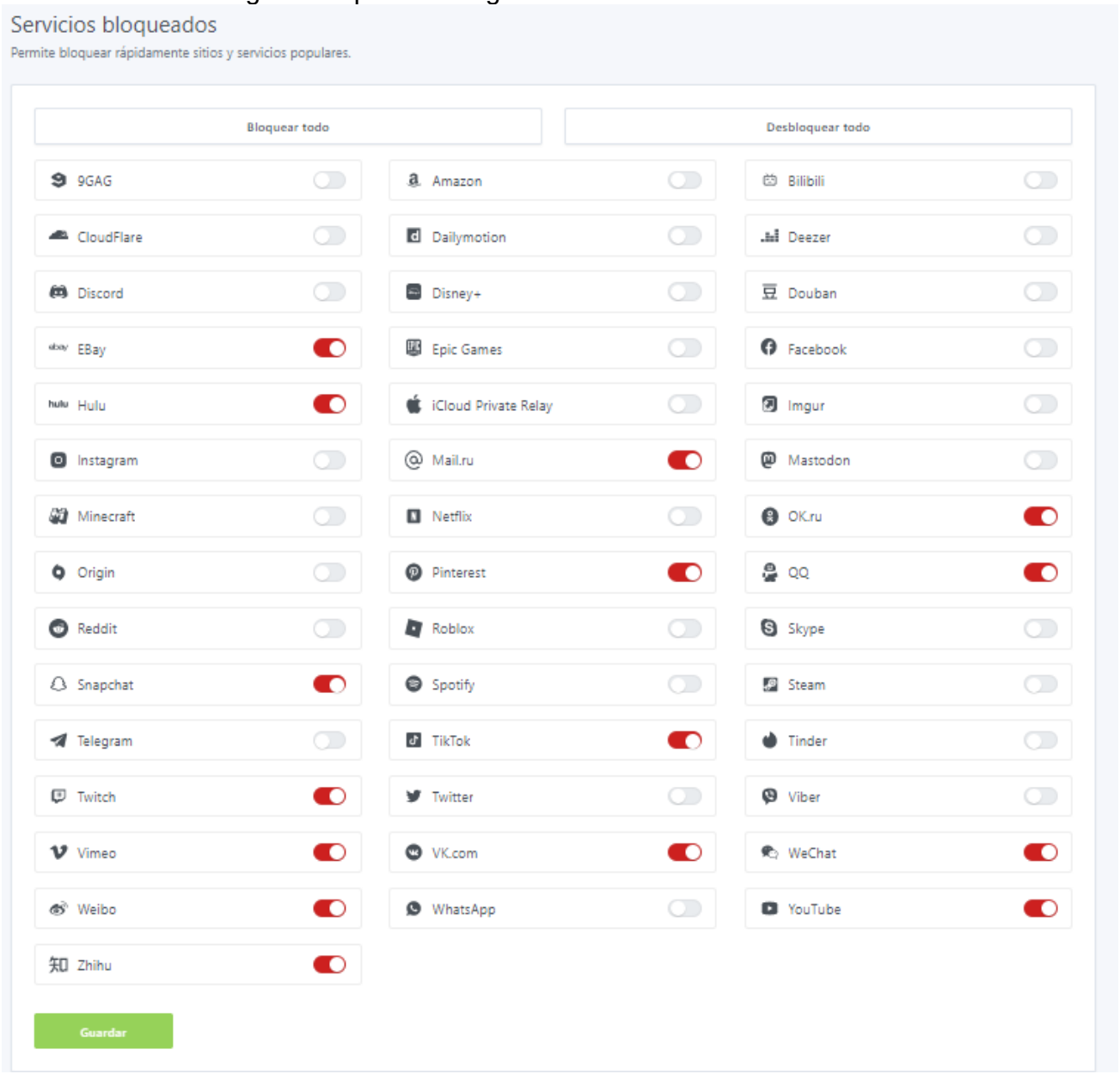


Figura 92: Servicios bloqueados por defecto.

Finalmente, en "reglas de filtrado personalizado" se añaden reglas personalizadas, con excepciones para que, con las listas seleccionadas no se bloqueen los servicios requeridos por los dispositivos Alexa Echo Dot ni el canal Amazon Prime Video o los Amazon FireTV Stick, pues se han detectado problemas de funcionamiento por los filtrados:

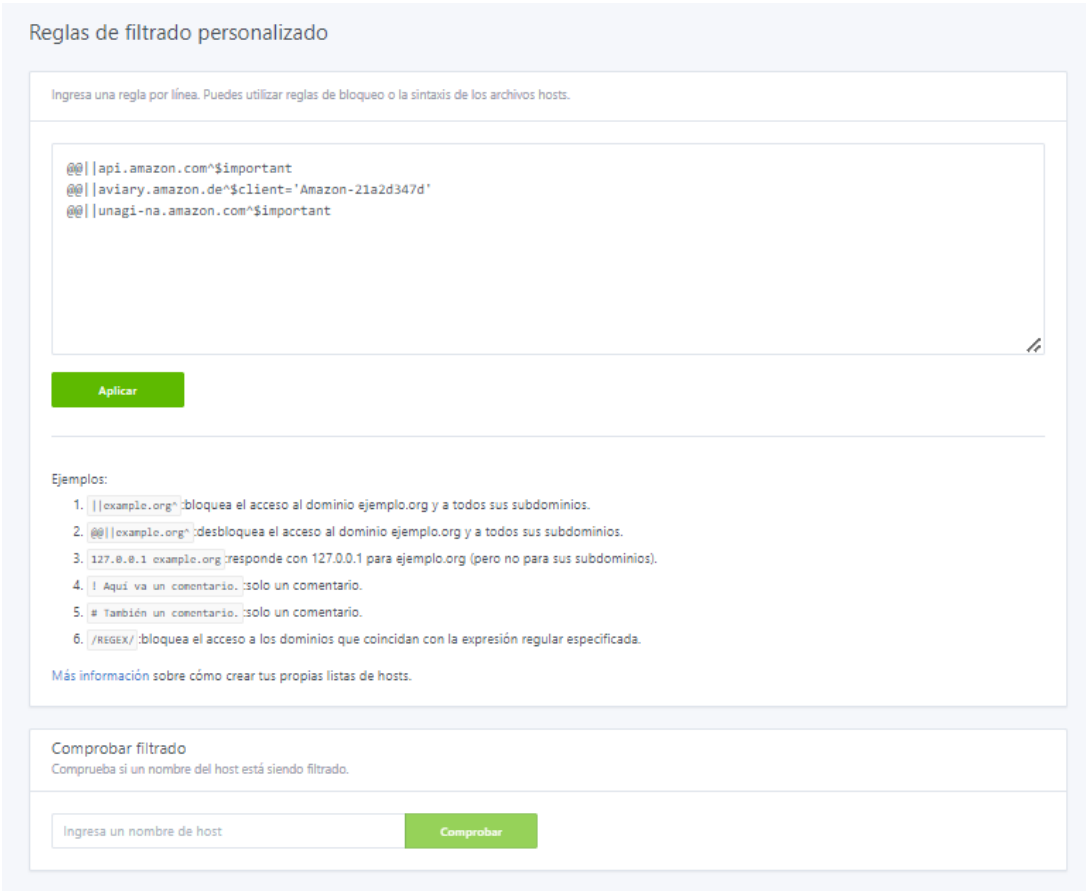


Figura 93: Excepciones para servicios de Amazon.

Una vez configurado y tras unos días de prueba ya se pueden consultar las estadísticas y el registro de actividad DNS del hogar:

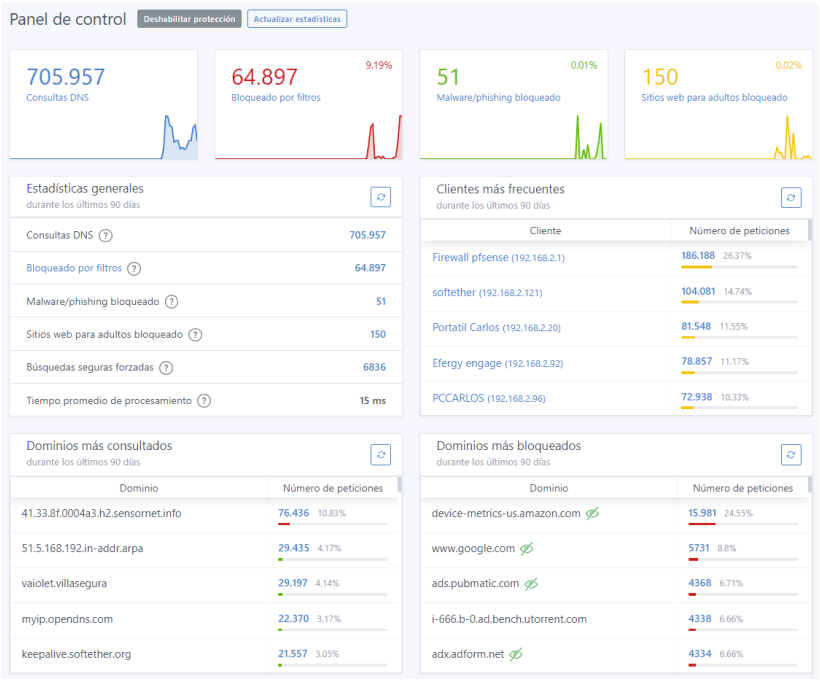


Figura 94: Dashboard con estadísticas de uso del DNS.

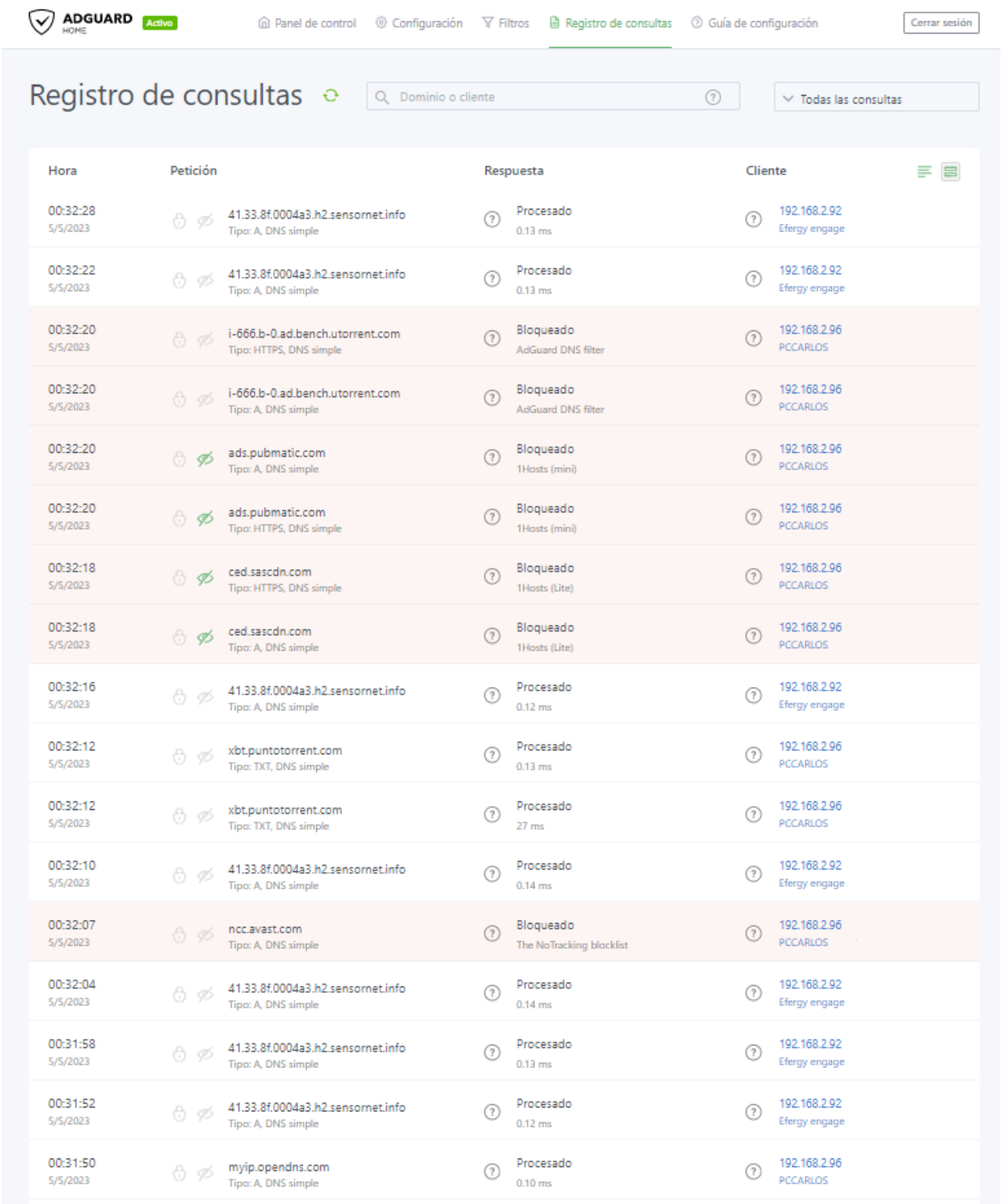


Figura 95: Extracto del registro de consultas DNS.

Finalmente se procede a cambiar la contraseña de la consola de administración de Adguard Home, para lo que se debe editar el archivo /usr/local/etc/AdGuardHome.yaml, donde se definen los usuarios y contraseñas, que pueden generarse con htpasswd:

```
carlos@adguardhome-2:~ $ cd /
carlos@adguardhome-2:/ $ cd usr
carlos@adguardhome-2:/usr $ cd local
carlos@adguardhome-2:/usr/local $ cd etc
carlos@adguardhome-2:/usr/local/etc $ nano AdGuardHome.yaml
```

```
pihole@pihole:~$ htpasswd -B -n -b root loquesea
root:$2y$05$004ITAOe10a.MKmpeKL.uOo9BTCX6ANnjvWtSU6Vot0aWhIfzYGVW
```

```
  GNU nano 7.2                                                    AdGuardHome.
bind_host: 0.0.0.0
bind_port: 80
beta_bind_port: 3001
users:
  - name: root
    password: $2y$05$I.6zVJRQq/NYVzVA/8wk5.h/cWJmi4PuOvG5x.TdXUHxE9sTtnORK
auth_attempts: 5
block_auth_min: 15
http_proxy: ""
language: ""
theme: auto
debug_pprof: false
web_session_ttl: 720
dns:
  bind_hosts:
    - 0.0.0.0
  port: 53
  statistics_interval: 90
  querylog_enabled: true
  querylog_file_enabled: true
  querylog_interval: 2160h
  querylog_size_memory: 1000
  anonymize_client_ip: false
  protection_enabled: true
  blocking_mode: custom_ip
```

Figura 96: Cambio de contraseña en Adguard Home.

iv. Anexo IV: Instalación y configuración de Pi-Hole

El servidor de Pi-Hole se instala en una máquina virtual bhyve en un servidor TrueNAS.
Para ello se crea una máquina virtual con la siguiente configuración:

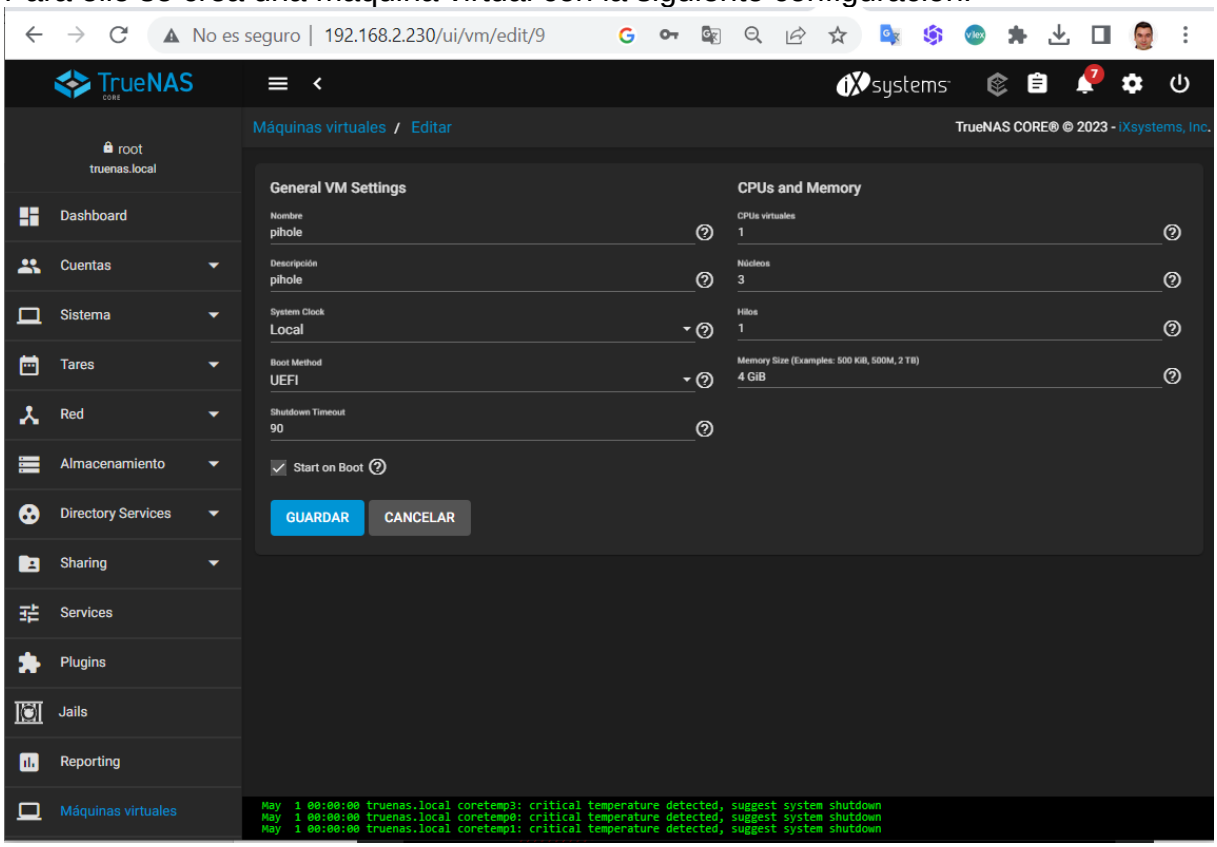


Figura 97: Máquina virtual Ubuntu en TrueNAS para Pi-hole.

Sobre la máquina virtual se instala un Ubuntu 22.04 mínimo y sin GUI y una vez instalado el sistema operativo se descarga y ejecuta la instalación de Pi-Hole, para lo que se ejecuta desde la consola:

```
wget -o basic-install.sh https://install.pi-hole.net
sudo bash basic-install.sh
```

Lo que da las siguientes salidas por pantalla:

```
pihole@pihole:~$ wget -O basic-install.sh https://install.pi-hole.net
--2023-04-07 22:13:34--  https://install.pi-hole.net/
Resolving install.pi-hole.net (install.pi-hole.net)... 164.90.255.4
Connecting to install.pi-hole.net (install.pi-hole.net)|164.90.255.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/pi-hole/pi-hole/master/automated%20install/basic-install
.sh [following]
--2023-04-07 22:13:34--  https://raw.githubusercontent.com/pi-hole/pi-hole/master/automated%20instal
l/basic-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133,
 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connecte
d.
HTTP request sent, awaiting response... 200 OK
Length: 121397 (119K) [text/plain]
Saving to: 'basic-install.sh'

basic-install.sh         100%[=================================>] 118,55K  --.-KB/s    in 0,02s

2023-04-07 22:13:34 (5,21 MB/s) - 'basic-install.sh' saved [121397/121397]

pihole@pihole:~$ sudo_bash basic-install.sh
```

Figura 98: Instalación de Pi-hole (1).

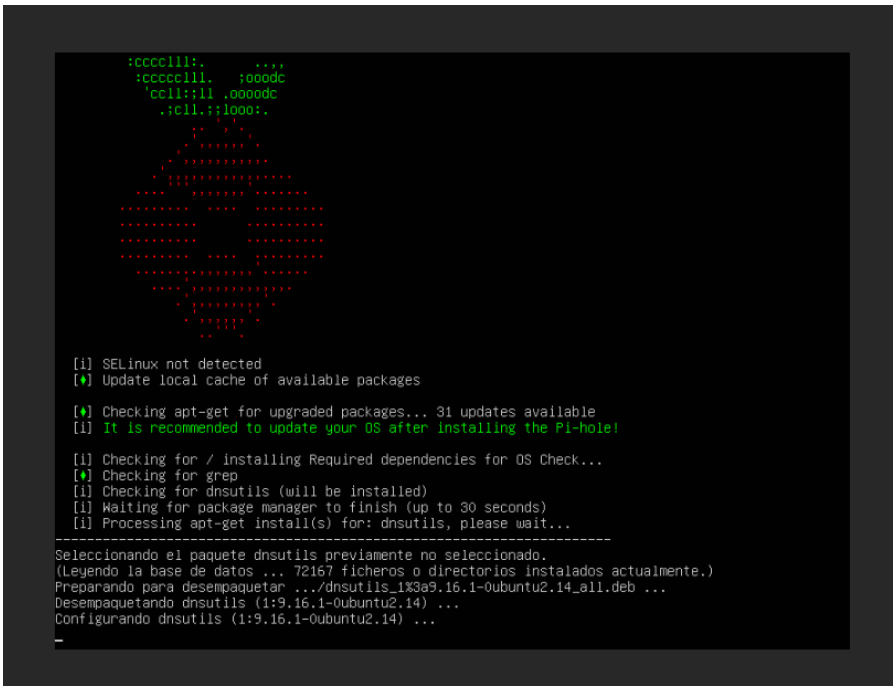
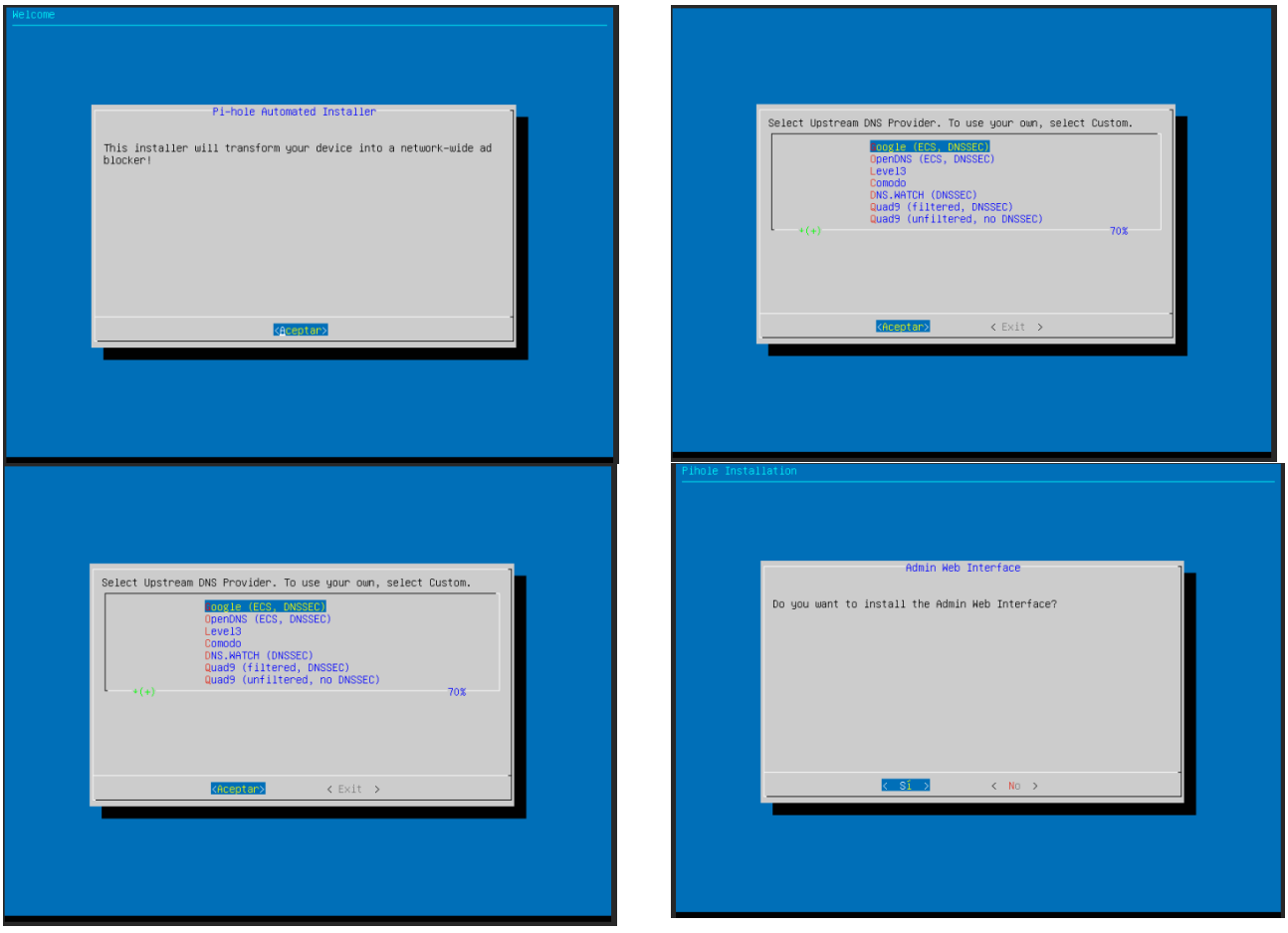


Figura 99: Instalación de Pi-hole (2).

A continuación, aparece un asistente para la configuración inicial, en el que se avanza seleccionando las opciones indicadas en las siguientes pantallas:



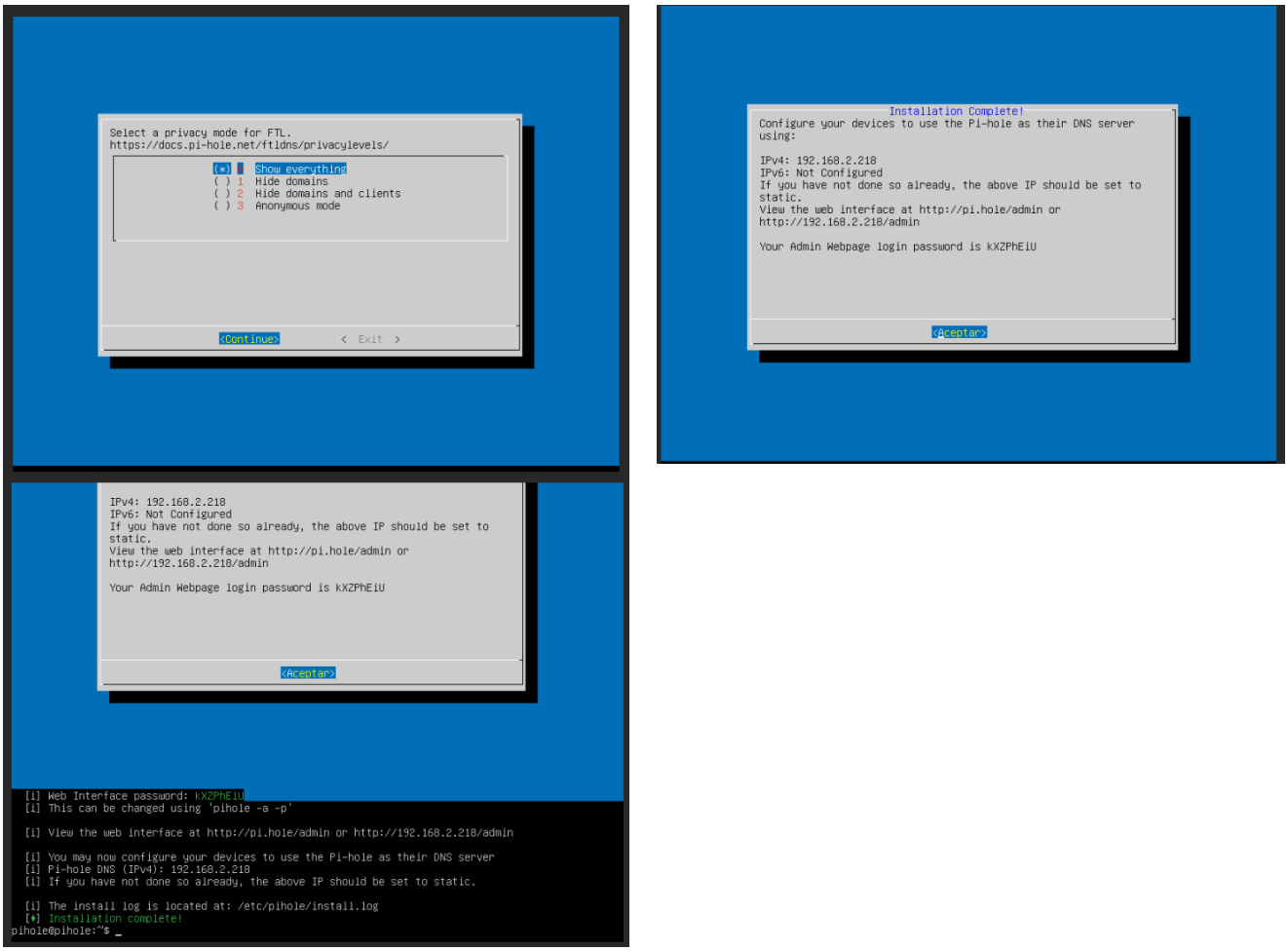
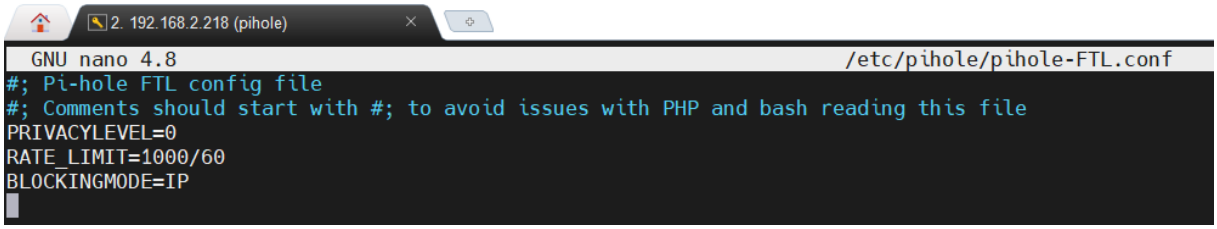


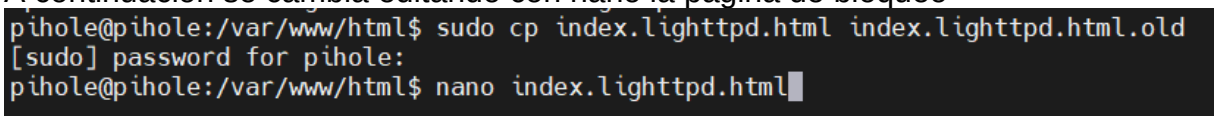
Figura 100: Instalación de Pi-hole (3).

El servidor DHCP del pfSense asigna a este equipo que ejecuta Pi-Hole la IP 192.168.2.218.

Una vez instalado se activa el parámetro BLOCKINGMODE=IP para cambiar la página de aviso de bloqueo:



A continuación se cambia editando con nano la página de bloqueo



```
3. 192.168.2.218 (pihole)
 GNU nano 4.8                    index.lighttpd.html                    Modified
<html>
<h1 style="color: #5e9ca0;">Contenido bloqueado por el Firewall DNS.</h1>
<p>No se permite el acceso a esta pagina. Si crees que es un error consulta a tus padres, tutor o administrador.</p>
<p> </p>
<p><img src="gandalf.png" alt="No puedes pasar" width=700/></p>
<p><strong> </strong></p>
</html>

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo
```

Y se copia una imagen en /var/www/html:

```
pihole@pihole:/var/www/html$ sudo cp /home/pihole/gandalf.png .
pihole@pihole:/var/www/html$ ls -lisa
total 76
917758  4 drwxrwxr-x 3 www-data www-data  4096 may  4 20:11 .
917716  4 drwxr-xr-x 3 root     root      4096 abr  7 22:18 ..
920977  4 drwxr-xr-x 7 root     root      4096 abr  7 22:18 admin
921184 56 -rw-r--r-- 1 root     root     55501 may  4 20:11 gandalf.png
921185  4 -rw-r--r-- 1 root     root       316 may  4 20:11 index.lighttpd.html
920600  4 -rw-r--r-- 1 root     root      3371 may  4 20:08 index.lighttpd.html.old
```

Tras estos pasos se reinicia el servidor web lighthttpd:

```
pihole@pihole:/var/www/html$ sudo nano /etc/lighttpd/lighttpd.conf
pihole@pihole:/var/www/html$ sudo service pihole-FTL restart
```

Y se verifica que en 192.168.2.218 carga la página correctamente:

Figura 101: Modificación de la página de bloqueo en Pi-hole.

Una vez modificada la página se inicia el proceso de configuración de Pi-Hole. Este proceso es más lento que Adguard, dado que hay que introducir muchas listas de forma manual, crear grupos e ir asignado grupos y listas tal como se explicará paso a paso en este anexo.

Se inicia el proceso accediendo a la URL http://192.168.2.218/admin, donde se solicitan credenciales de paso:

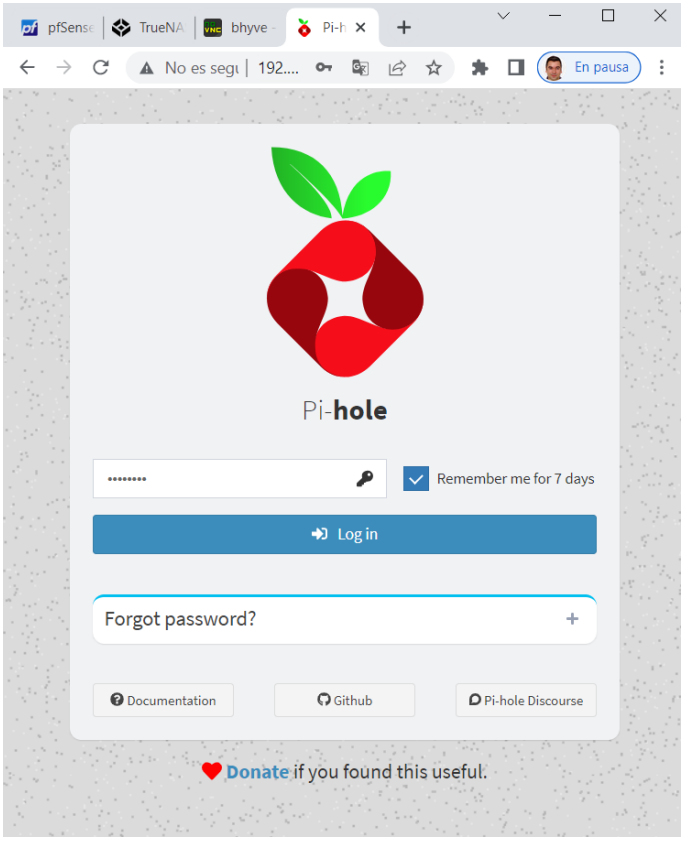


Figura 102: Acceso a la web de gestión de Pi-hole.

El primer paso es revisar el menú settings:

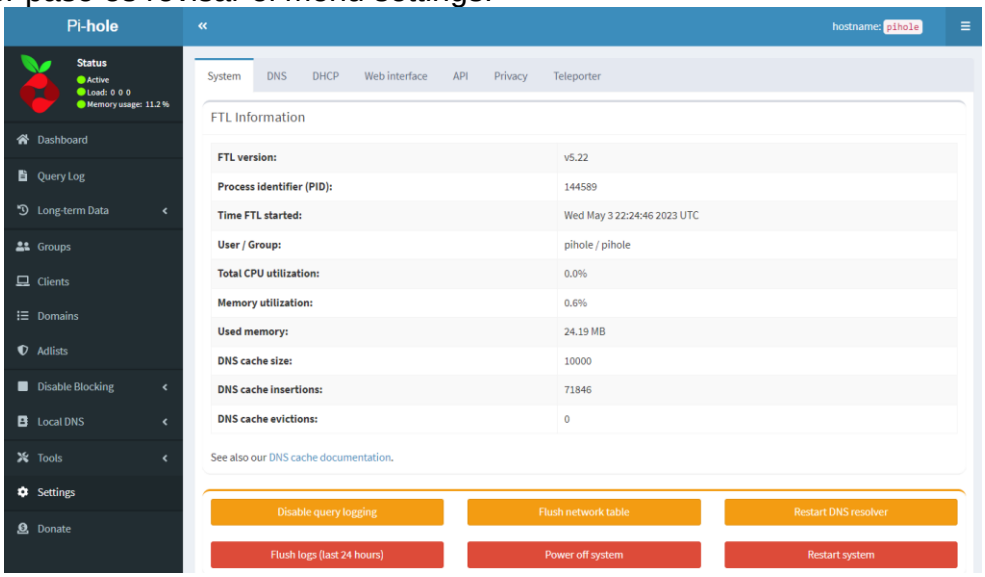


Figura 103: Menú 'settings' del software Pi-hole.

En la sección DNS se configura utilizando los DNS de forma lo más equivalente posible a Adguard Home, esto es cumplimentando las IPs de la siguiente manera:

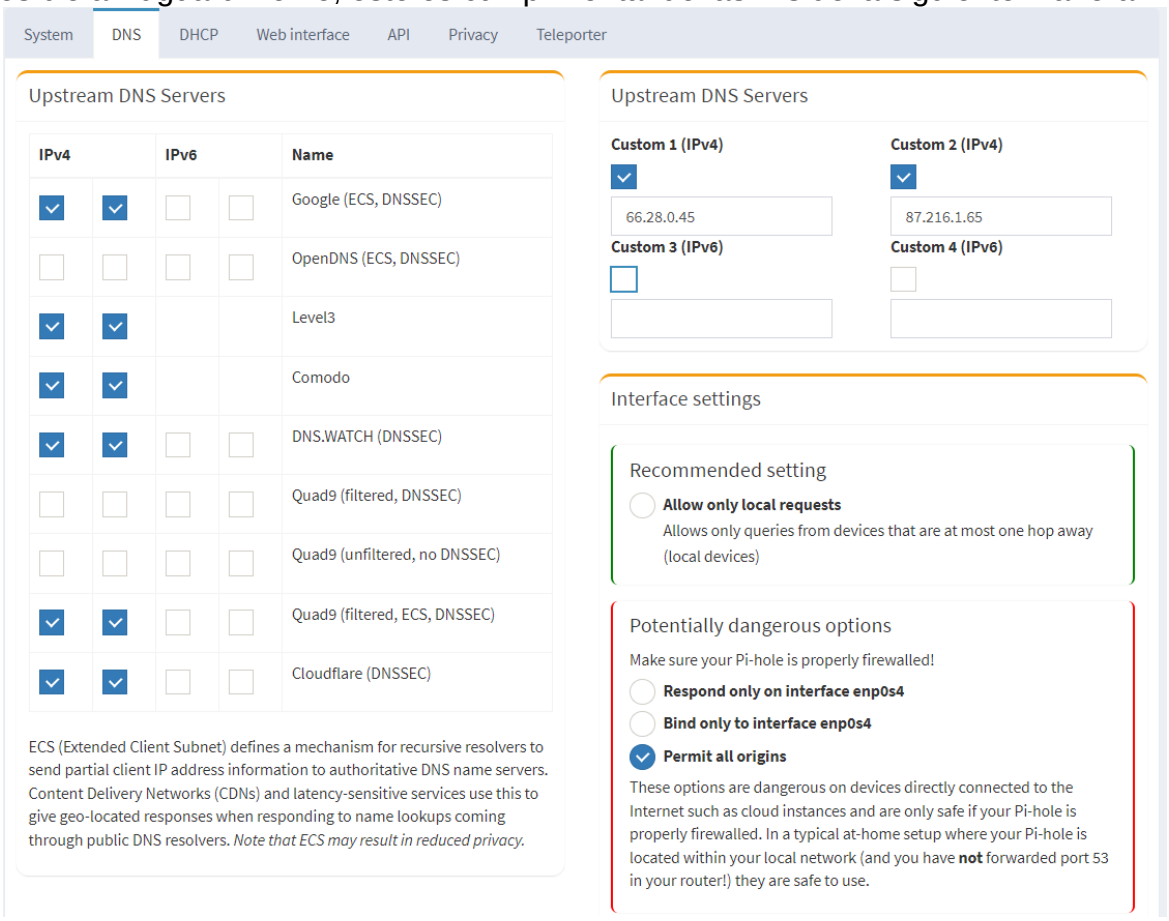


Figura 104: Configuración de los servidores resolutores DNS en Pi-hole.

A continuación, se configura la resolución de nombres de la red local para que utilice la IP de pfSense, que es el equipo que hace de servidor DHCP:

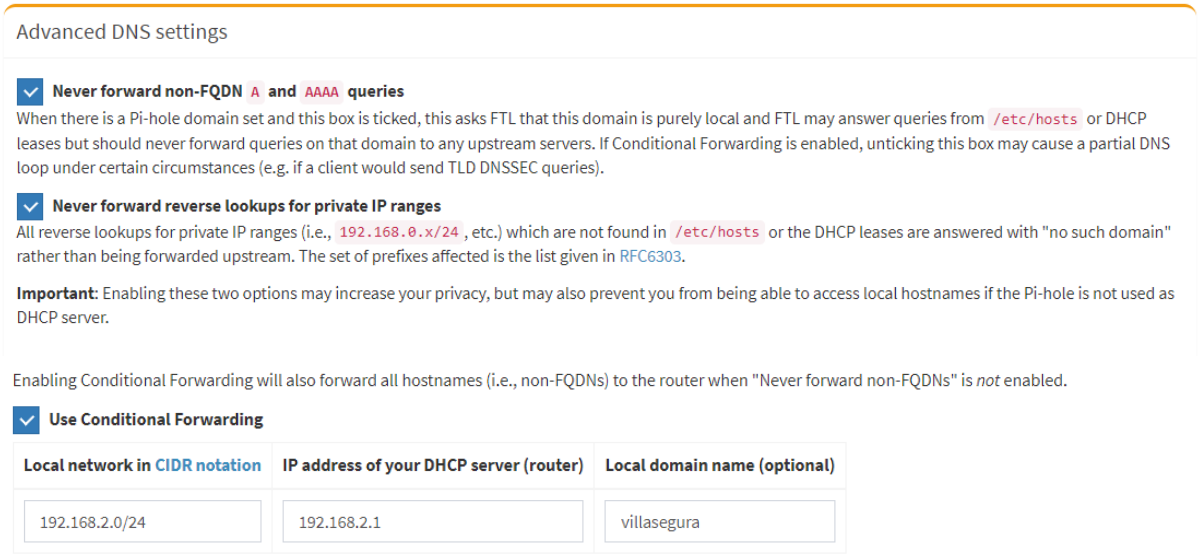


Figura 105: Configuración de búsquedas DNS inversas.

Se pulsa “Save” y se aplica la configuración y se verifica la resolución de nombres locales y la se verifica la resolución de nombres de internet:

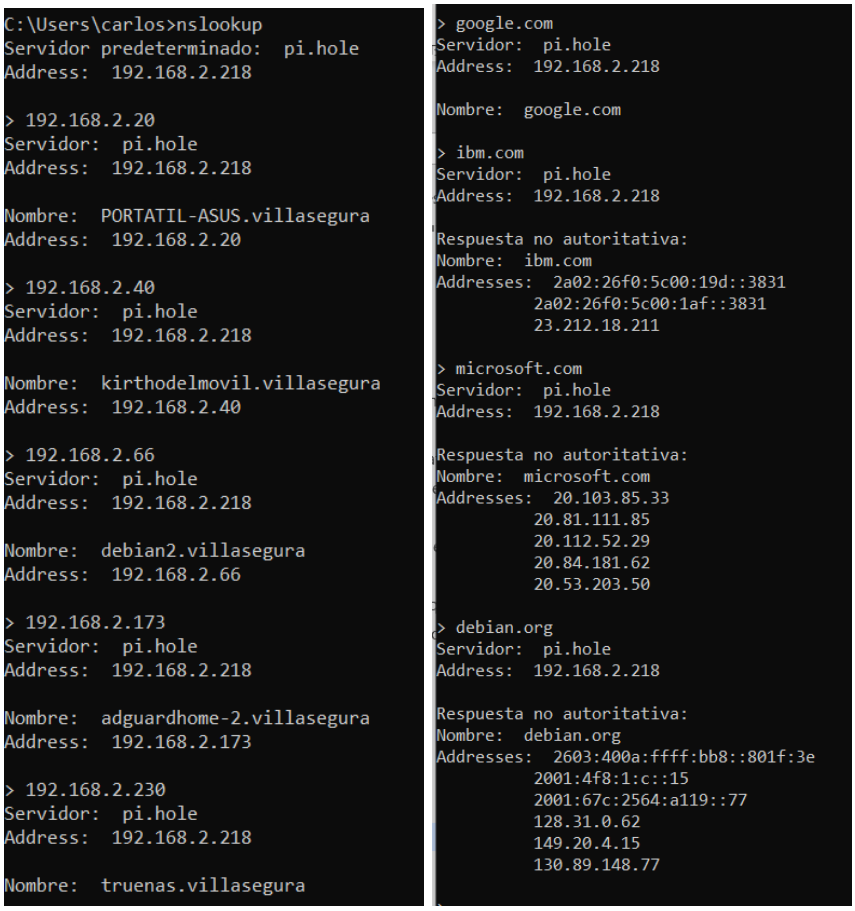


Figura 106: Verificación de la resolución DNS y DNS inversas.

En las opciones de DHCP no se requiere configurar nada ya que no se utiliza el servidor DHCP que incorpora Pi-Hole, se utiliza el router pfSense como servidor DHCP. Las opciones de “Web Interface” se dejan con los valores por defecto dado que solamente es un aspecto estético. En la sección “privacy” se activa el registro de toda la actividad y sin anonimizar, pues durante las pruebas se requiere revisar los logs, una vez terminadas las pruebas se puede establecer:

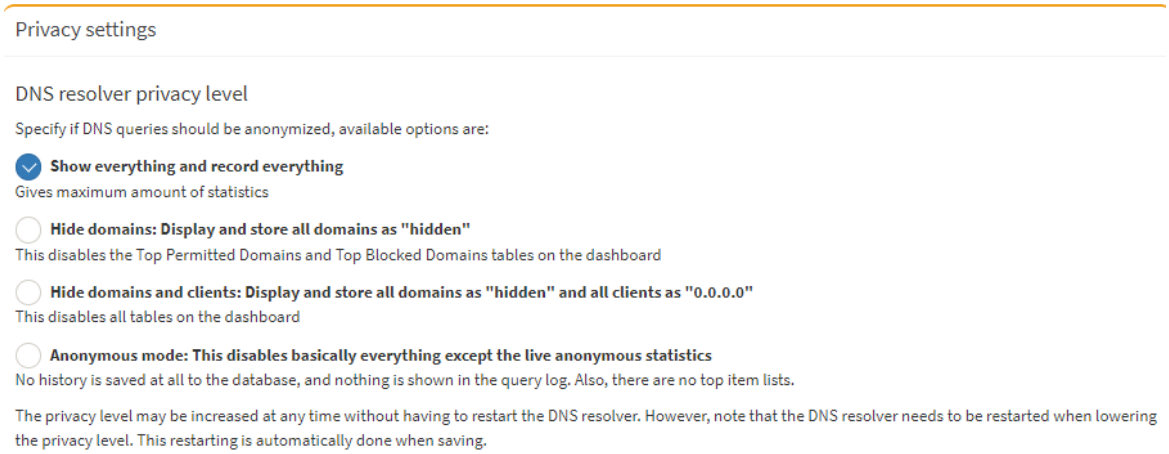


Figura 107: Configuración de los logs de registro de actividad.

A continuación se activan las búsquedas seguras para menores en los buscadores, para ello se añaden a la lista de CNAME locales las siguientes entradas:

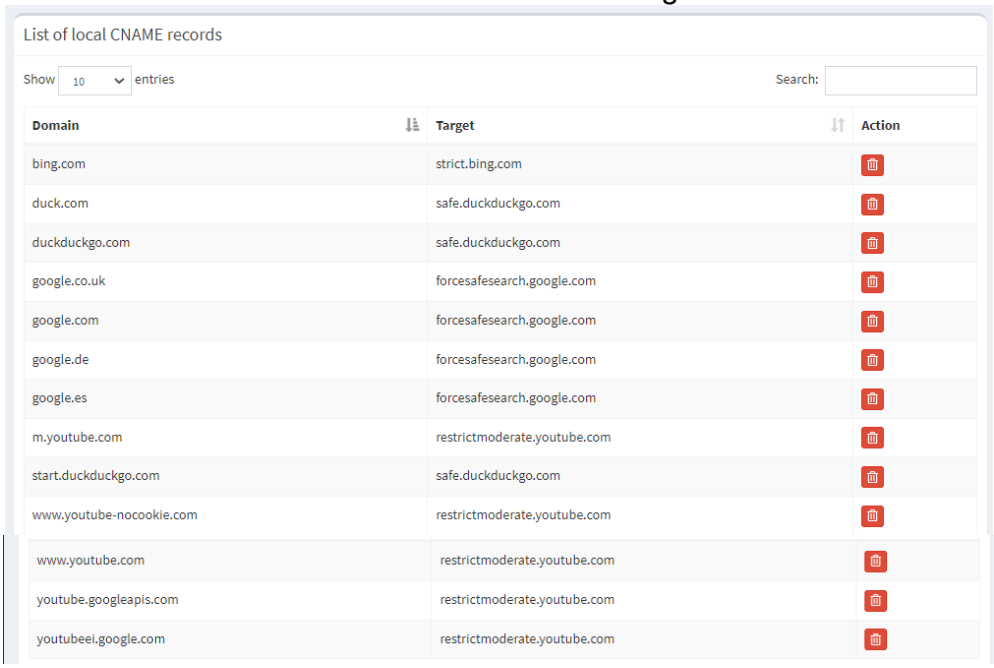


Figura 108: Configuración de las búsquedas seguras en Pi-hole.

El siguiente paso es de crear los grupos de filtrado, desde la opcion “Groups“ del menú se accede a la pantalla. En estos grupos se asignan conjuntos de listas de bloqueos. Se deciden crear los siguientes utilizando la opcion “Add” de dicha pantalla:

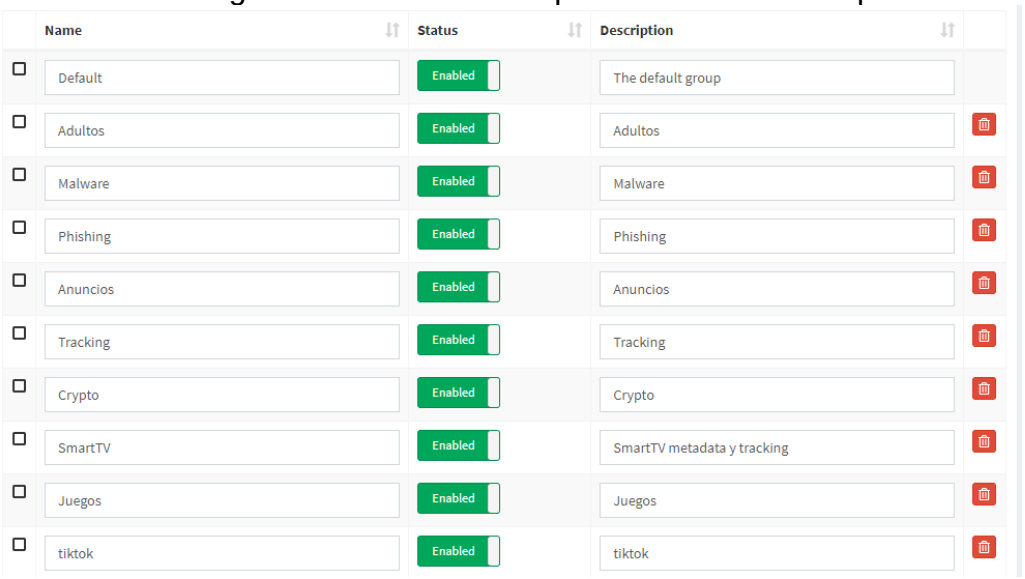


Figura 109: Configuración de los grupos de filtrado en Pi-hole.

A continuación se crean los clientes desde la opción “Clients” del menú. Al igual que en Adguard Home se debe introducir un identificador descriptivo y una IP o una MAC o el nombre del host.
Para cada cliente se configuran los grupos de filtros que se le desean aplicar y a los clientes no dados de alta se les aplica el grupo ‘default’. Si se desea que no se apliquen reglas a algun cliente, se le debe asignar el grupo ‘unassigned’:

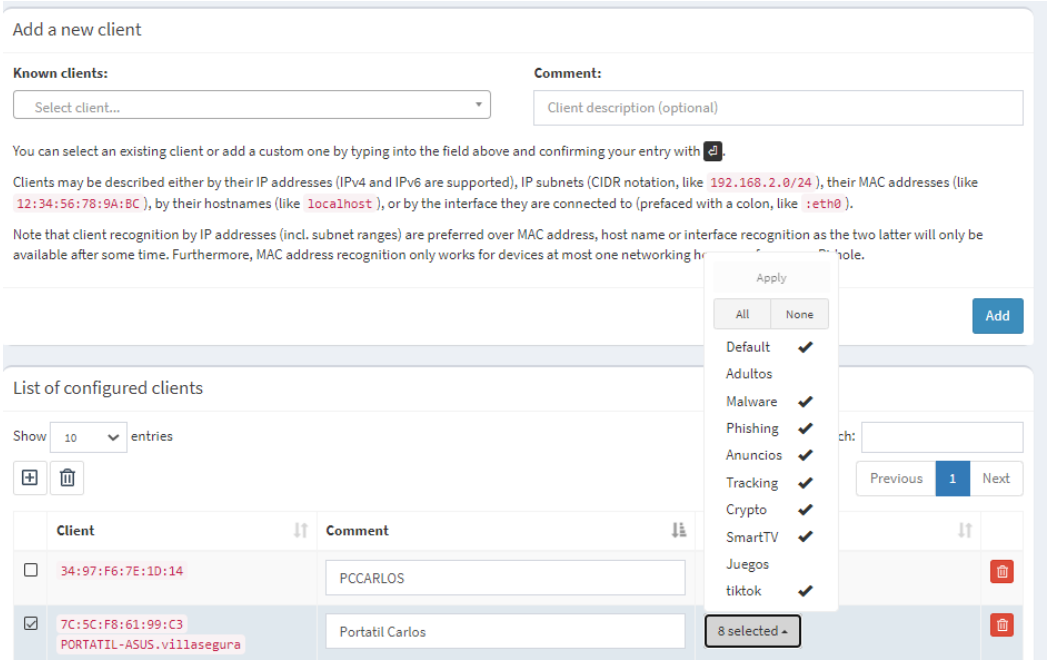


Figura 110: Configuración de los clientes en Pi-Hole.

A continuación, se configuran los dominios y en cada caso se asigna el tipo de regla (lista blanca, lista negra, regex…). Por ejemplo, se restringe TikTok asignando las reglas al grupo llamado TikTok y al grupo 'Default' y las whitelist se aplican a todos los grupos:

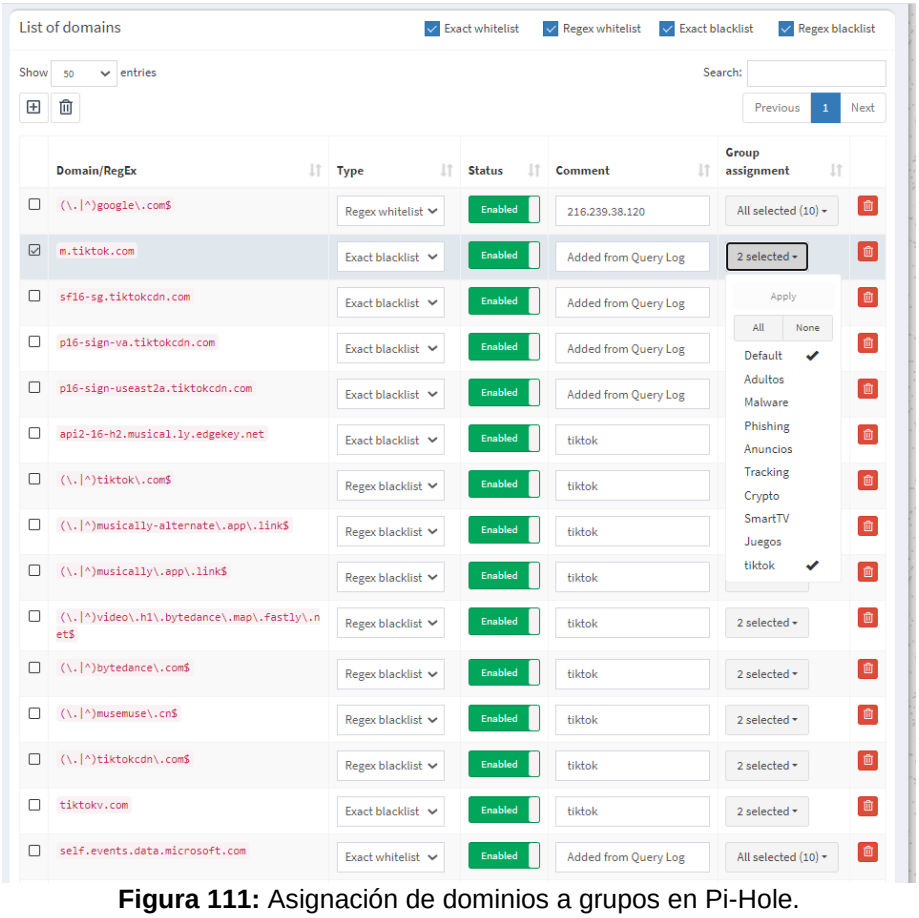


Figura 111: Asignación de dominios a grupos en Pi-Hole.

Para terminar con la configuración debe accederse a la opción del menú “Adlists”, donde se configuran las listas de filtrados:

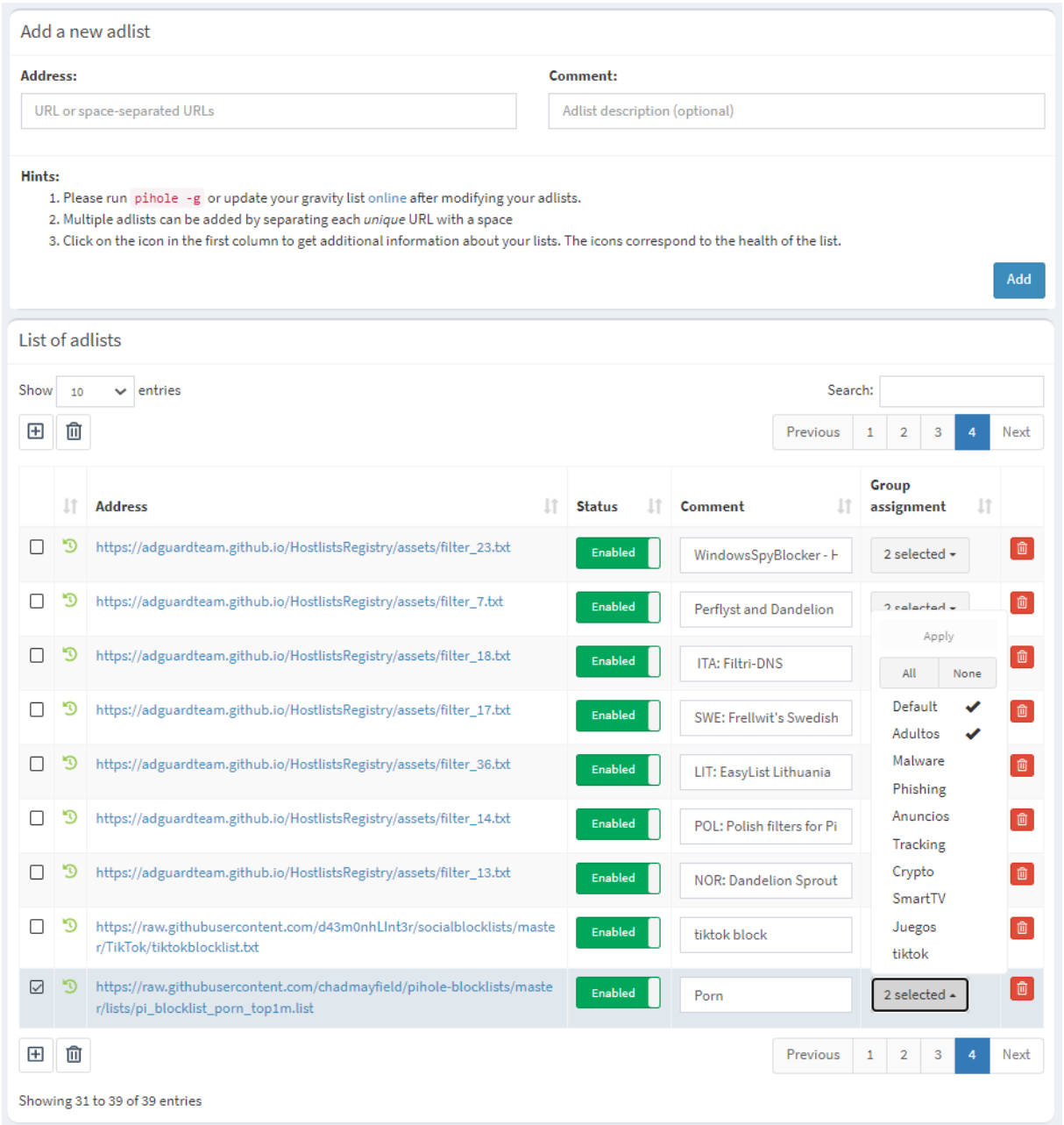


Figura 112: Asignación de listas de filtrado a grupos en Pi-Hole.

El funcionamiento consiste en añadir una URL para cada lista y una descripción. A continuación, se pulsa Add para añadirla. Desde el listado inferior se pueden asignar las listas a grupos concretos. Con la configuración planteada, una lista de tracking se asigna al grupo Tracking y al grupo default, con esta estrategia, un cliente no dado de alta tendrá aplicados todos los filtros y los clientes que se den de alta podrán personalizarse a nivel de los grupos creados anteriormente.

Dado que Adguard Home contiene ya referencias a listas que se mantienen actualizadas periódicamente, se opta por añadir una por una todas las listas

seleccionadas en la configuración de Adguard Home (ver Anexo III), introduciendo las IPs que utiliza Adguard para poder evaluar ambos productos en condiciones similares (Adguard Home y Pi-Hole).

Una vez terminadas de introducir todas las listas se debe ejecutar “update” del sistema desde el menú “tools”, opción "Update Gravity (list of blocked domains)”.

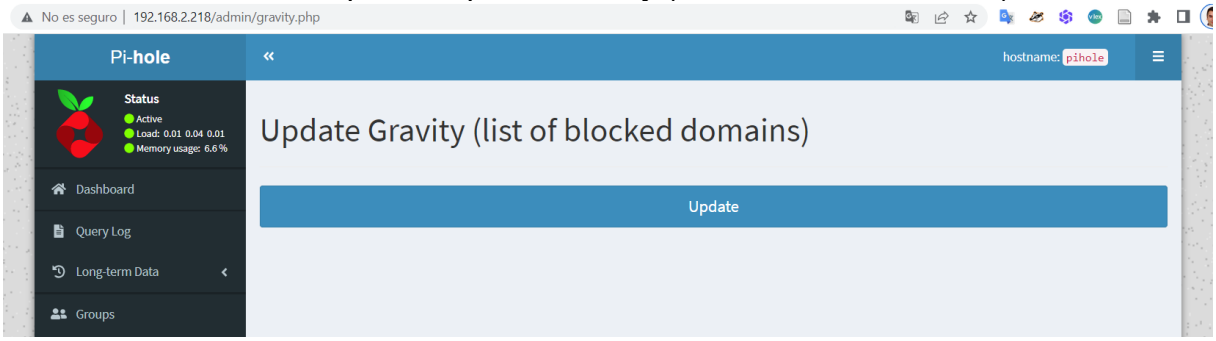


Figura 113: Actualización de la configuración de filtrado en Pi-Hole.

A medida que se va ejecutando se van mostrando logs de progreso por pantalla:

```
[i] Neutrino emissions detected...
  [✓] Pulling blocklist source list into range

  [✓] Preparing new gravity database
  [i] Using libz compression

  [i] Target: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
  [✓] Status: Retrieval successful
  [i] Imported 177554 domains, ignoring 2 non-domain entries
      Sample of non-domain entries:
        - 0.0.0.0
        - www
  [i] List stayed unchanged

  [i] Target: https://adaway.org/hosts.txt
  [✓] Status: No changes detected
  [i] Imported 6540 domains

  [i] Target: https://v.firebog.net/hosts/AdguardDNS.txt
  [✓] Status: No changes detected
  [i] Imported 50794 domains, ignoring 3 non-domain entries
      Sample of non-domain entries:
        - 10.10.34.
        - 4adtf.com.
        - ejghgjhhgadcdchjaada.ru.

  [i] Target: https://v.firebog.net/hosts/Admiral.txt
  [✓] Status: No changes detected
  [i] Imported 1013 domains

  [i] Target: https://raw.githubusercontent.com/anudeepND/blacklist/master/adservers.txt
  [✓] Status: Retrieval successful
  [i] Imported 42536 domains
  [i] List stayed unchanged

  [i] Target: https://v.firebog.net/hosts/Easyprivacy.txt
  [✓] Status: No changes detected
  [i] Imported 18677 domains, ignoring 2 non-domain entries
      Sample of non-domain entries:
        - _.net.asambeauty.com
        - _tcp.academyofconsciousleadership.net

  [i] Target: https://v.firebog.net/hosts/Prigent-Ads.txt
  [✓] Status: No changes detected
  [i] Imported 3674 domains

  [i] Target: https://www.github.developerdan.com/hosts/lists/ads-and-tracking-extended.txt
  [✓] Status: Retrieval successful
  [i] Imported 432108 domains, ignoring 8 non-domain entries
      Sample of non-domain entries:
        - _ldap._tcp.pdc._msdcs.adserver.com
        - _dmarc.js.alexametrics.com
        - outping--.callrail.com
```

```
        - aes-.corp.com
        - 7cjyxsb-.micpn.com
  [i] List has been updated

  [i] Target: https://gitlab.com/quidsup/notrack-blocklists/raw/master/notrack-blocklist.txt
  [✓] Status: Retrieval successful
  [i] Imported 16598 domains
  [i] List stayed unchanged

  [i] Target: https://raw.githubusercontent.com/DandelionSprout/adfilt/master/Alternate%20versions%20Anti-Malware%20L
ist/AntiMalwareHosts.txt
  [✓] Status: Retrieval successful
  [i] Imported 13178 domains, ignoring 13 non-domain entries
      Sample of non-domain entries:
        - 5.8.47.3
        - 190.238.183.5
        - 85.239.33.9
        - 113.116.89.1
        - 182.116.104.6
  [i] List stayed unchanged

  [i] Target: https://osint.digitalside.it/Threat-Intel/lists/latestdomains.txt
  [✓] Status: Retrieval successful
  [i] Imported 45 domains
  [i] List has been updated

  [i] Target: https://v.firebog.net/hosts/Prigent-Crypto.txt
  [✓] Status: No changes detected
  [i] Imported 15886 domains

  [i] Target: https://v.firebog.net/hosts/RPiList-Malware.txt
  [✓] Status: No changes detected
  [i] Imported 113834 domains

  [i] Target: https://v.firebog.net/hosts/RPiList-Phishing.txt
  [✓] Status: No changes detected
  [i] Imported 509420 domains

  [i] Target: https://malware-filter.gitlab.io/malware-filter/phishing-filter-hosts.txt
  [✓] Status: Retrieval successful
  [i] Imported 46136 domains, ignoring 16 non-domain entries
      Sample of non-domain entries:
        - _._domainkey.hmhmkk.cyou
        - _._domainkey.service.hmhmkk.cyou
        - _.service.hmhmkk.cyou
        - emptyfullsequel-bhd-.bhg406.repl.co
        - exu0wgk0298bi9oj8c3f@2muchlove.one
  [i] List has been updated

  [i] Target: https://zerodot1.gitlab.io/CoinBlockerLists/hosts_browser
  [✓] Status: No changes detected
  [i] Imported 3496 domains

  [i] Target: https://raw.githubusercontent.com/chadmayfield/my-pihole-blocklists/master/lists/pi_blocklist_porn_top1
m.list
  [✓] Status: Retrieval successful
  [i] Imported 11868 domains
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/AdGuardSDNSFilter/Filters/filter.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 51165 patterns, ignoring 558 non-domain entries
      Sample of non-domain entries:
        - ||ads.livetv*.me^
        - ||counter*.stat.ovh^
        - ||fxhpaoxqyajvmdg.
        - ||rgfftupf.
        - ||clk.rtpdn*.com^
  [i] List has been updated

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_24.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 61716 domains
  [i] List has been updated

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_38.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 62733 domains
  [i] List has been updated
```

```
[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_1.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 51163 patterns, ignoring 558 non-domain entries
    Sample of non-domain entries:
      - ||ads.livetv*.me^
      - ||counter*.stat.ovh^
      - ||fxhpaoxqyajvmdg.
      - ||rgfftupf.
      - ||clk.rtpdn*.com^
[i] List has been updated

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_4.txt
[✓] Status: Retrieval successful
[i] Imported 11410 domains
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_2.txt
[✓] Status: Retrieval successful
[i] Imported 6540 domains
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_34.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 111925 patterns, ignoring 288 non-domain entries
    Sample of non-domain entries:
      - @@||7eer.net^
      - @@||adfoc.us^
      - @@||adj.st^
      - @@||affiliatefuture.com^
      - @@||anrdoezrs.net^
[i] List has been updated

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_32.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 438355 patterns, ignoring 5 non-domain entries
    Sample of non-domain entries:
      - ||9904.a^
      - ||cloudacademies.p^
      - ||ionix.co.d^
      - ||mightbesupposed.t^
      - ||reken-bhf.d^
[i] List has been updated

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_5.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 49711 domains
[i] List has been updated

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_27.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 281071 domains
[i] List has been updated

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_3.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 3739 domains
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_33.txt
[✓] Status: Retrieval successful
[i] Imported 177553 domains
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_6.txt
[✓] Status: Retrieval successful
[i] List contained AdBlock Plus style domains
[i] Imported 9 patterns, ignoring 1 non-domain entries
    Sample of non-domain entries:
      - ||arc.msn.com^$ctag=~device_pc|~os_windows
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_23.txt
[✓] Status: Retrieval successful
[i] Imported 347 domains
[i] List stayed unchanged

[i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_7.txt
```

```
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 129 patterns, ignoring 21 non-domain entries
      Sample of non-domain entries:
        - @@||mhc-ajax-eu.myhomescreen.tv^
        - @@||mhc-ajax-eu-s2.myhomescreen.tv^
        - @@||mhc-xpana-eu.myhomescreen.tv^
        - @@||mhc-xpana-eu-s2.myhomescreen.tv^
        - |lgtvsdp.com^
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_18.txt
  [✓] Status: Retrieval successful
  [i] Imported 355 domains
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_17.txt
  [✓] Status: Retrieval successful
  [i] Imported 1100 domains
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_36.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 31 domains
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_14.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 260 domains
  [i] List stayed unchanged

  [i] Target: https://adguardteam.github.io/HostlistsRegistry/assets/filter_13.txt
  [✓] Status: Retrieval successful
  [i] List contained AdBlock Plus style domains
  [i] Imported 317 patterns, ignoring 75 non-domain entries
      Sample of non-domain entries:
        - ||prod-adops-proxy.dnitv.net^$ctag=os_android|os_ios|device_tv
        - ||82.221.81.9^
        - ||norwegian.com.
        - ||flysas-no.
        - ||tusenfryd-com.
  [i] List stayed unchanged

  [i] Target: https://raw.githubusercontent.com/d43m0nhLInt3r/socialblocklists/master/TikTok/tiktokblocklist.txt
  [✓] Status: Retrieval successful
  [i] Imported 24 patterns, ignoring 5 non-domain entries
      Sample of non-domain entries:
        - (^|\.)muscdn\.com$
        - (^|\.)musical\.ly$
        - (^|\.)tiktok\.com$
        - (^|\.)tiktok\.org$
        - (^|\.)tiktokcdn\.com$
  [i] List stayed unchanged

  [i] Target: https://raw.githubusercontent.com/chadmayfield/pihole-blocklists/master/lists/pi_blocklist_porn_top1m.l
ist
  [✓] Status: Retrieval successful
  [i] Imported 11868 domains
  [i] List stayed unchanged

  [✓] Creating new gravity databases
  [✓] Storing downloaded domains in new gravity database
  [✓] Building tree
  [✓] Swapping databases
  [✓] The old database remains available.
  [i] Number of gravity domains: 6495819 (1929374 unique domains)
  [i] Number of exact blacklisted domains: 12
  [i] Number of regex blacklist filters: 14
  [i] Number of exact whitelisted domains: 10
  [i] Number of regex whitelist filters: 50
  [✓] Cleaning up stray matter

  [✓] FTL is listening on port 53
     [✓] UDP (IPv4)
     [✓] TCP (IPv4)
     [✓] UDP (IPv6)
     [✓] TCP (IPv6)

  [✓] Pi-hole blocking is enabled
```

Esta actualización se realiza por defecto cada semana los domingos por lo que se cambia hay que actualizar el cron.d para que se actualice de forma horaria:

```
Last login: Thu May  4 20:15:20 2023 from 192.168.2.20
pihole@pihole:~$ cd /etc/cron.d
pihole@pihole:/etc/cron.d$ ls
e2scrub_all  php  pihole  popularity-contest
pihole@pihole:/etc/cron.d$ sudo nano pihole
```

Se debe comentar la línea existente y añadir la nueva programación:

```
 GNU nano 4.8                                    pihole                                    Modifi
# Pi-hole: A black hole for Internet advertisements
# (c) 2017 Pi-hole, LLC (https://pi-hole.net)
# Network-wide ad blocking via your own hardware.
#
# Updates ad sources every week
#
# This file is copyright under the latest version of the EUPL.
# Please see LICENSE file for your rights under this license.
#
#
#
# This file is under source-control of the Pi-hole installation and update
# scripts, any changes made to this file will be overwritten when the software
# is updated or re-installed. Please make any changes to the appropriate crontab
# or other cron file snippets.

# Pi-hole: Update the ad sources once a week on Sunday at a random time in the
#          early morning. Download any updates from the adlists
#          Squash output to log, then splat the log to stdout on error to allow for
#          standard crontab job error handling.
#00 4   * * 7   root    PATH="$PATH:/usr/sbin:/usr/local/bin/" pihole updateGravity >/var/log/pihole/pihole_updateGravity.log || cat /var/log/pihole/pihole_updateGravity.log
0 * * * * root PATH="$PATH:/usr/sbin:/usr/local/bin/" pihole updateGravity >/var/log/pihole/pihole_updateGravity.log || cat /var/log/pihole/pihole_updateGravity.log
# Pi-hole: Flush the log daily at 00:00
#          The flush script will use logrotate if available
#          parameter "once": logrotate only once (default is twice)
#          parameter "quiet": don't print messages
00 00   * * *   root    PATH="$PATH:/usr/sbin:/usr/local/bin/" pihole flush once quiet

@reboot root /usr/sbin/logrotate --state /var/lib/logrotate/pihole /etc/pihole/logrotate

# Pi-hole: Grab remote and local version every 24 hours
10 14  * * *   root    PATH="$PATH:/usr/sbin:/usr/local/bin/" pihole updatechecker
@reboot root    PATH="$PATH:/usr/sbin:/usr/local/bin/" pihole updatechecker reboot
```

Figura 114: Programación de las actualizaciones de los filtros en Pi-hole.

Una vez realizado los cambios se reinicia la máquina virtual y una vez vuelve a ejecutarse Pi-Hole se hace una prueba de la configuración, para lo que por ejemplo se busca un articulo para el que aparecan anuncios:

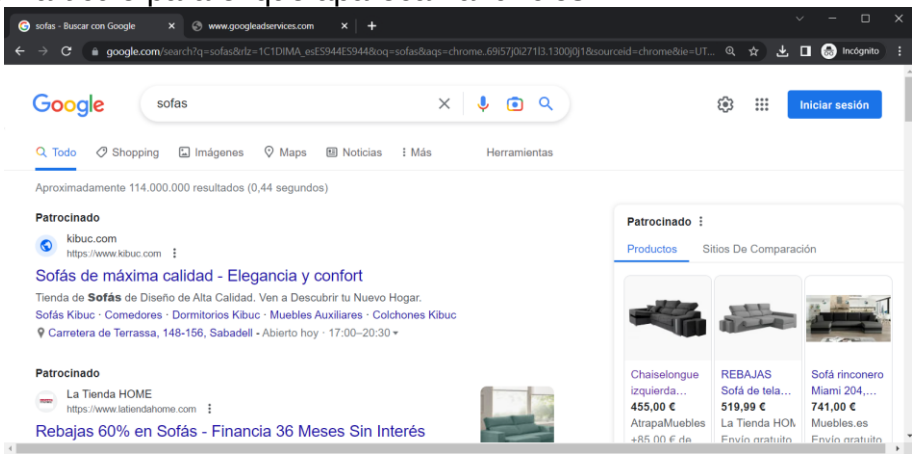


Figura 115: Prueba de filtrado en Pi-hole (1).

Al hacer clic sobre un producto se verifica el filtrado:

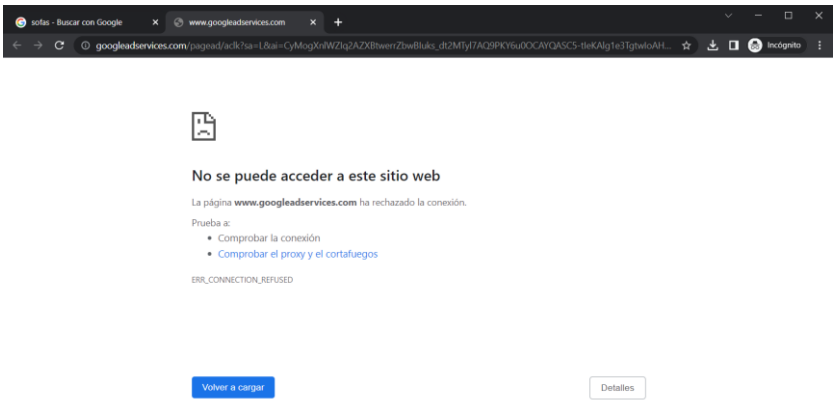


Figura 116: Prueba de filtrado en Pi-hole (2).

Pero si se desactiva el grupo de filtros para el cliente:

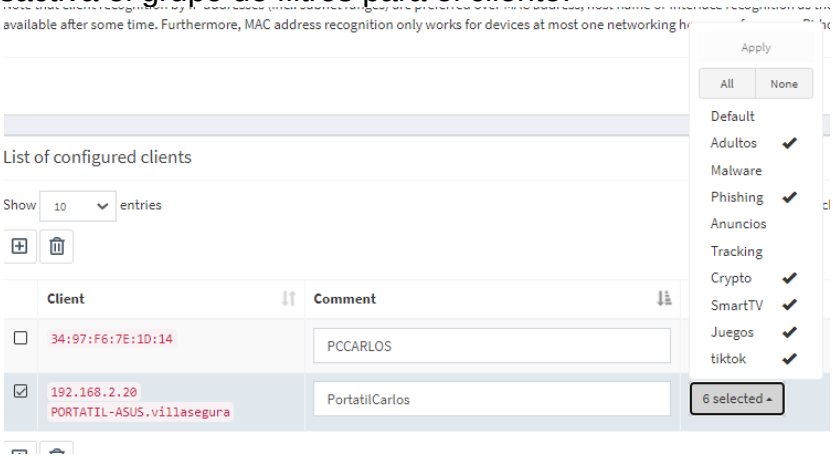


Figura 117: Prueba de filtrado en Pi-hole (3).

Aseguramos que se borra la cache de DNS:

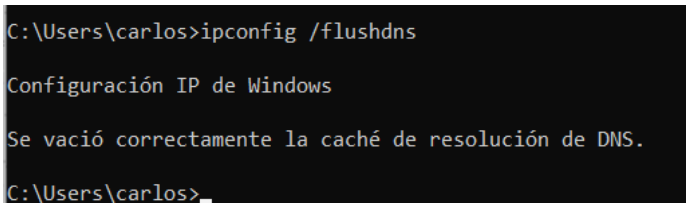


Figura 118: Prueba de filtrado en Pi-hole (4).

Y volvemos a hacer clic sobre un anuncio de producto se resuelven los "googleadservices":

Figura 119: Prueba de filtrado en Pi-hole (5).

Tras un tiempo funcionando se verifica que las estadísticas se van actualizando correctamente y los logs registran la actividad:

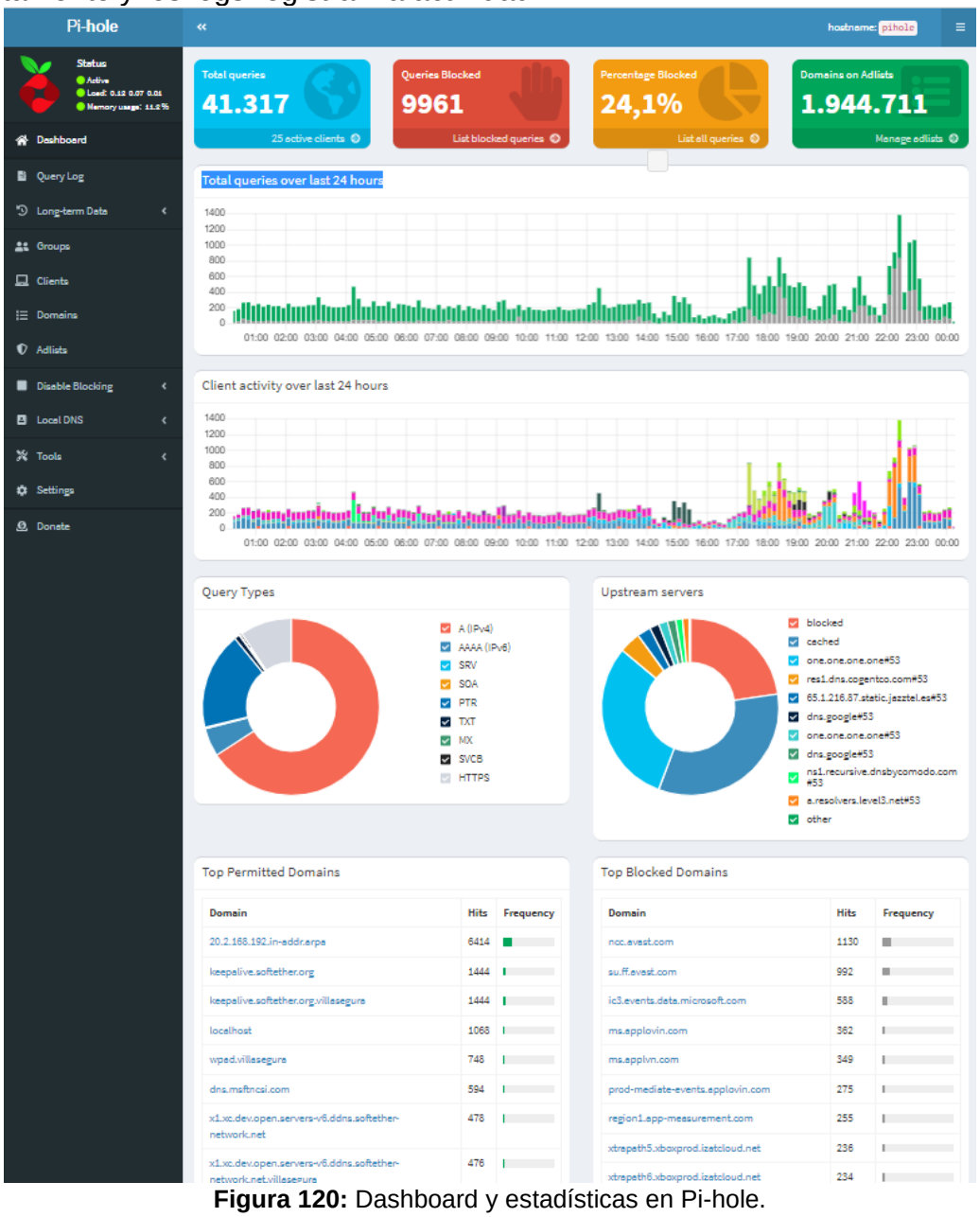


Figura 120: Dashboard y estadísticas en Pi-hole.

Network overview

Search:

Show 10 entries

Previous 1 2 3 4 Next

IP address	Hardware address	Interface	Hostname	First seen	Last Query	Number of queries	Uses Pi-hole	Action
192.168.2.20 192.168.2.183	7c:5c:f8:61:99:c3 Intel Corporate	enp0s4	PORTATIL-ASUS.villasegura debian11.villasegura	2023-04-18 23:00:00	2023-05-06 00:38:57	24.305	✔	
192.168.2.121	76:d4:35:90:d6:58	enp0s4	Softether.villasegura	2023-05-04 10:59:00	2023-05-06 00:38:30	15.123	✔	
192.168.2.181	d2:99:ec:fa:97:72	enp0s4		2023-05-04 01:11:00	2023-05-06 00:37:55	4084	✔	
192.168.2.56	fc:49:2d:27:4d:29 Amazon Technologies Inc.	enp0s4	amazon-21a2d347d.villasegura	2023-05-04 21:41:00	2023-05-06 00:37:47	1627	✔	
192.168.2.184	7a:a3:95:1b:68:d2	enp0s4	POCO-X3-Pro.villasegura	2023-05-04 21:53:00	2023-05-06 00:37:40	1429	✔	
192.168.2.200	08:a6:bc:81:d0:5b Amazon Technologies Inc.	enp0s4	amazon-03f032ede.villasegura	2023-04-08 20:12:00	2023-05-06 00:35:53	2910	✔	
192.168.2.207	58:82:a8:19:ad:2b Microsoft	enp0s4	KIRTHOXBOX.villasegura	2023-05-04 11:32:00	2023-05-06 00:33:11	1293	✔	
127.0.0.1 ::1	00:00:00:00:00:00 virtual interface	lo	localhost	2023-04-08 00:20:00	2023-05-06 00:31:40	8303	✔	
192.168.2.119	fa:03:c7:56:14:54	enp0s4	RedmiNote9Pro-RedmiN.villasegura	2023-05-04 08:20:00	2023-05-06 00:17:03	4513	✔	
192.168.2.210	76:d4:35:e1:b0:23	enp0s4	myplexserver.villasegura	2023-05-04 11:13:00	2023-05-06 00:15:59	337	✔	

Figura 121: Registro de actividad en Pi-hole.

v. Anexo V: Instalación y configuración de pfBlockerNG

El paso previo es la configuración del DNS Resolver de pfSense, que se configura desde Services->DNS Resolver con los siguientes parámetros:

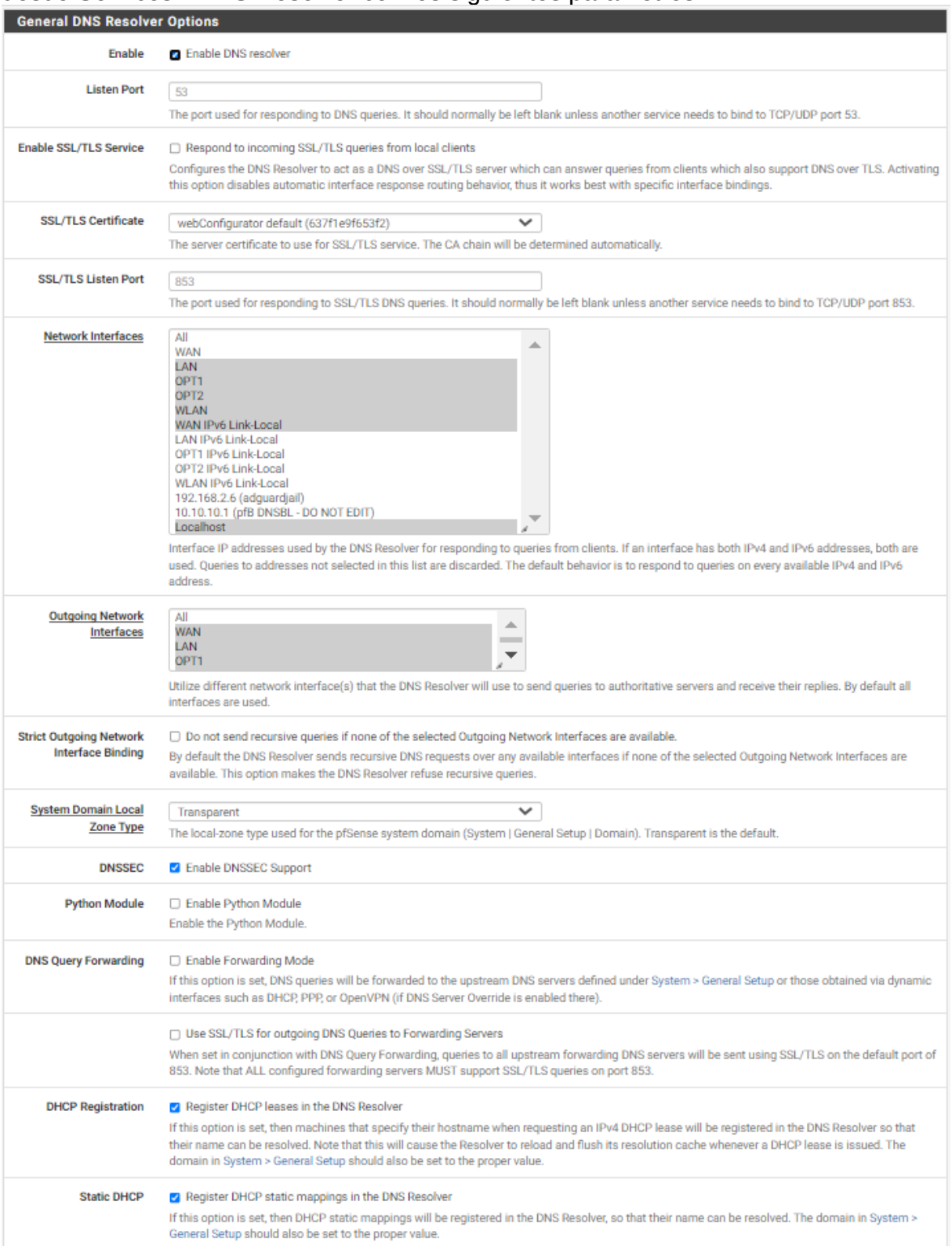


Figura 122: Configuración de DNS Resolver en pfSense.

Una vez guardada la configuración se inicia el proceso de instalación de pfBlockerNG seleccionándolo desde System->Package Manager->Available Packages.
Una vez instalado se accede e inicia un asistente de primera configuración desde Firewall->pfBlockerNG que instala dos componentes:

- Reglas de firewall 'tradicional'
- Reglas de filtrado de firewall DNS

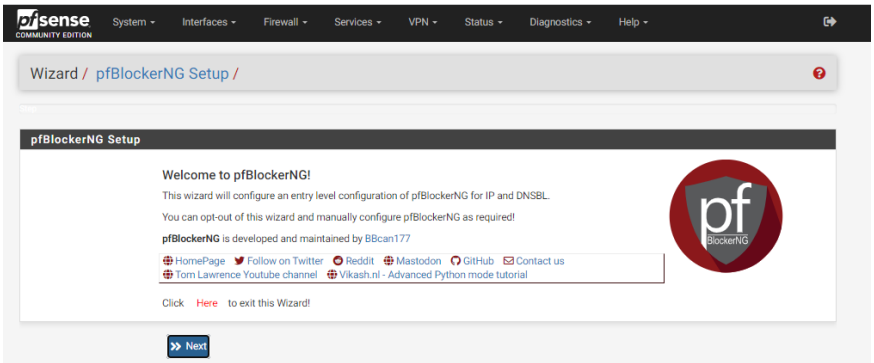


Figura 123: Asistente de configuración de pfBlockerNG (1)

Son 4 pasos, el primero es informativo:

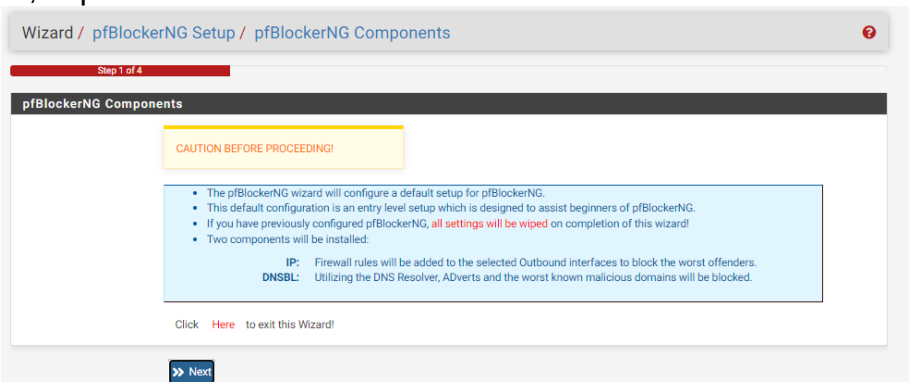


Figura 124: Asistente de configuración de pfBlockerNG (2)

En el segundo paso se selecciona la interfaz de red entrante y la saliente:

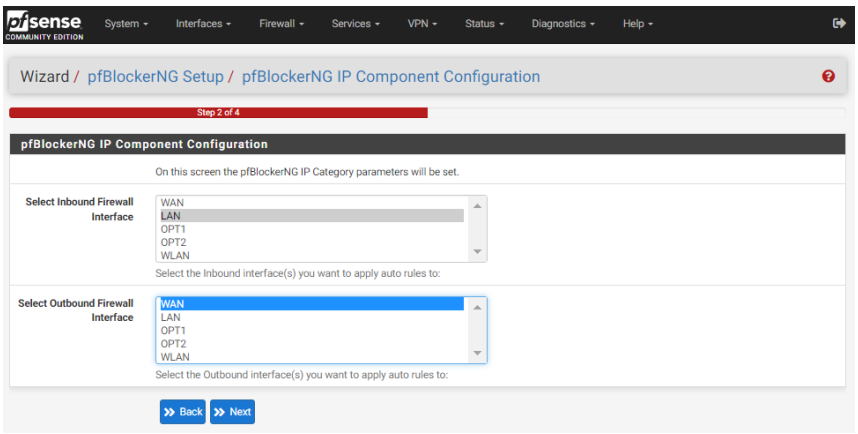


Figura 125: Asistente de configuración de pfBlockerNG (3)

En el tercer paso se dejan los parámetros por defecto:

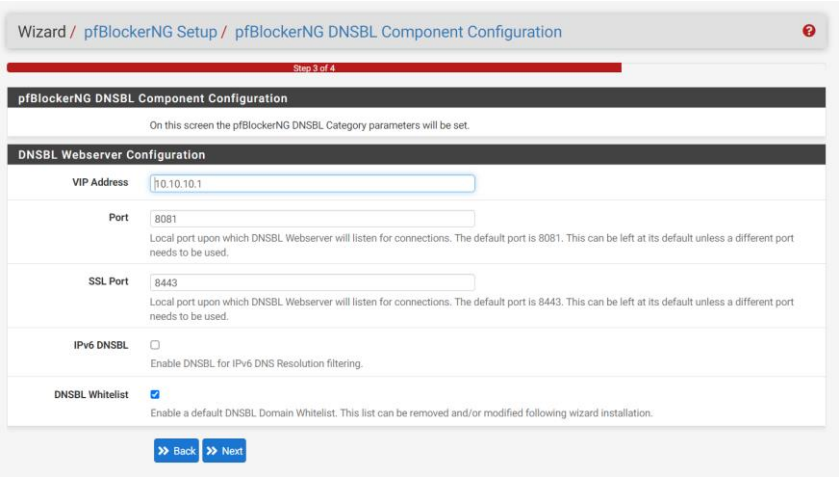


Figura 126: Asistente de configuración de pfBlockerNG (4)

Y en la siguiente pantalla se pulsa 'Finish':

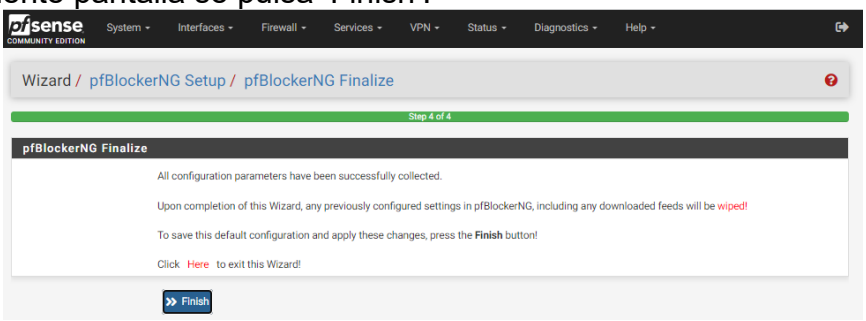


Figura 127: Asistente de configuración de pfBlockerNG (5)

Acto seguido se inicia el proceso de configuración, cuyo progreso se muestra en una ventana de logs:

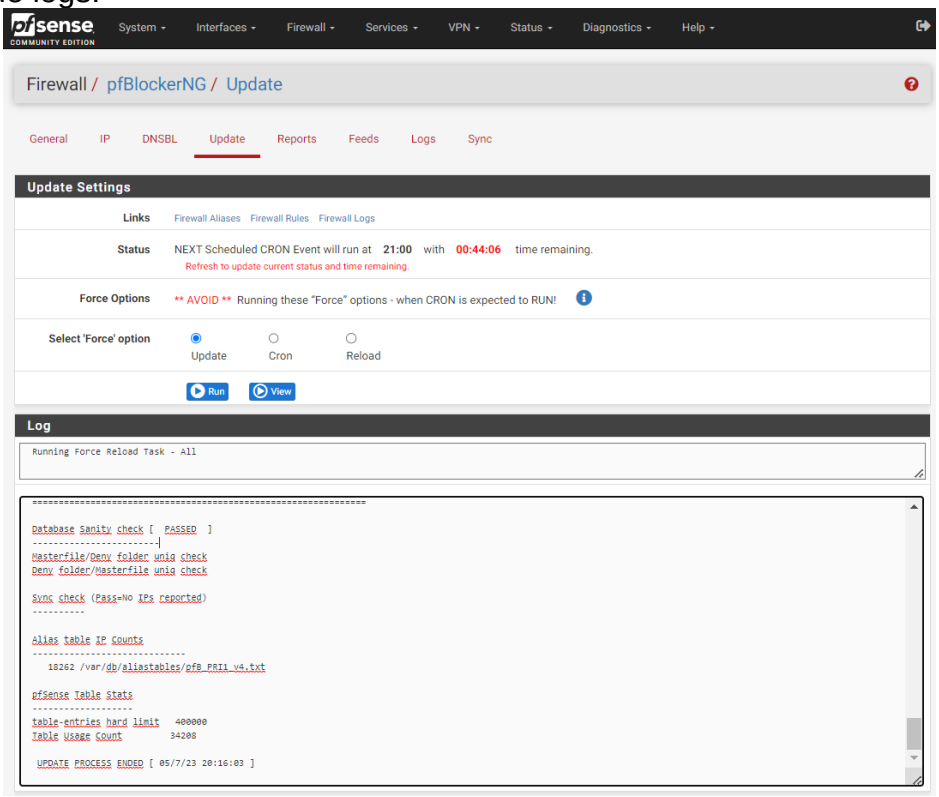


Figura 128: Asistente de configuración de pfBlockerNG (6)

A continuación se accede a la pestaña DNSBL y se configura de la siguiente forma:

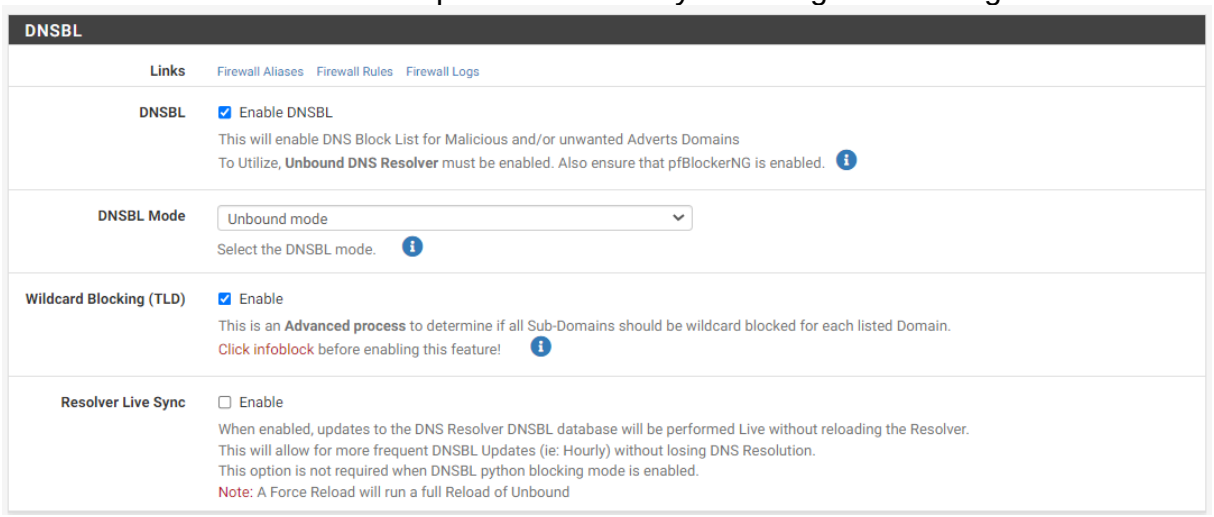


Figura 129: Configuración de DNSBL en pfBlockerNG (1)

A continuación se activa la interfaz web en la interfaz LAN (por defecto viene en localhost):

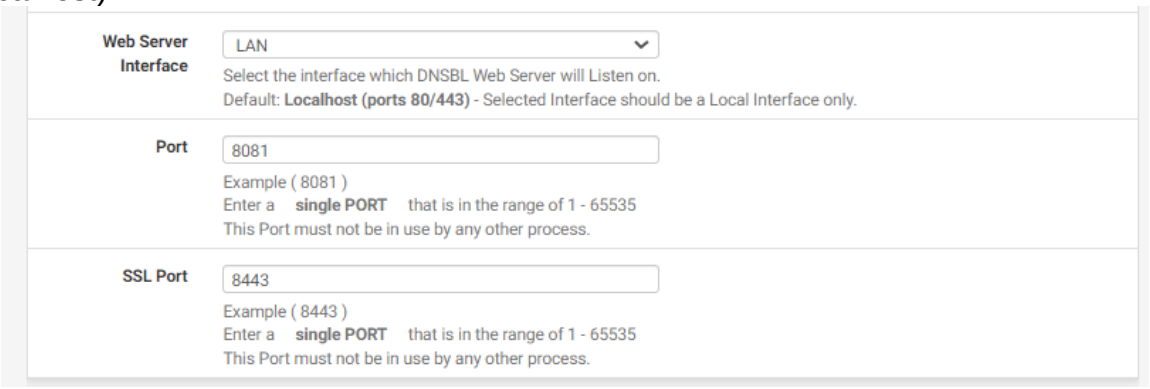


Figura 130: Configuración de DNSBL en pfBlockerNG (2)

Se establece el registro de los dominios bloqueados:

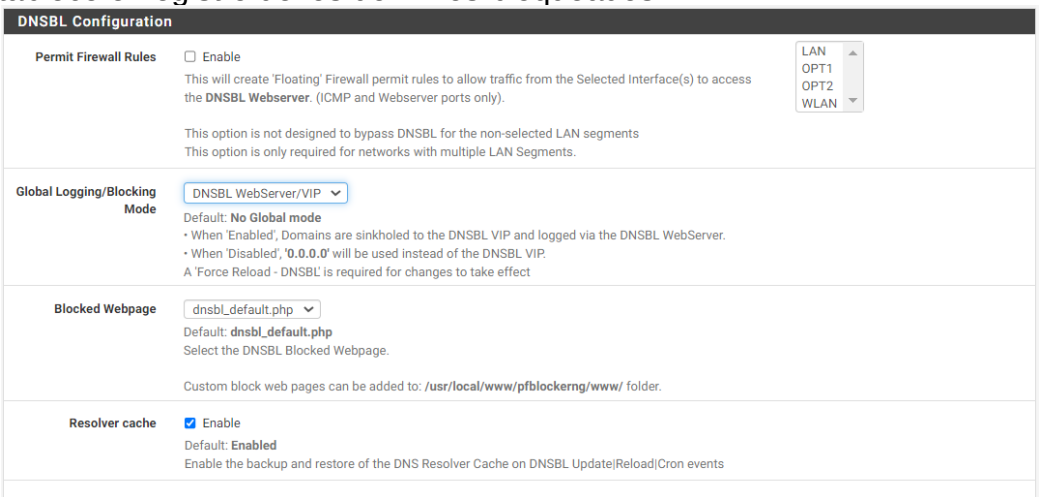


Figura 131: Configuración de DNSBL en pfBlockerNG (3)

Finalmente, dentro de la misma pantalla se activa el DNSBL IP para bloquear en el firewall las IPs de los Feeds:

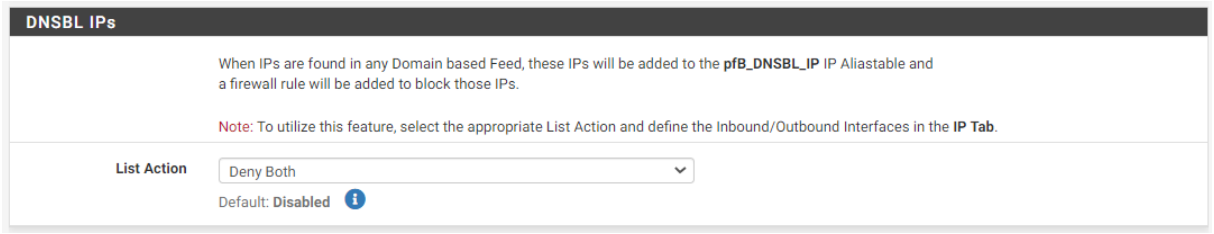


Figura 132: Configuración de DNSBL en pfBlockerNG (4)

El siguiente paso es configurar DNSBL Safesearch, que fuerza el uso de búsquedas seguras para menores en los principales buscadores y que se establece con la siguiente configuración:

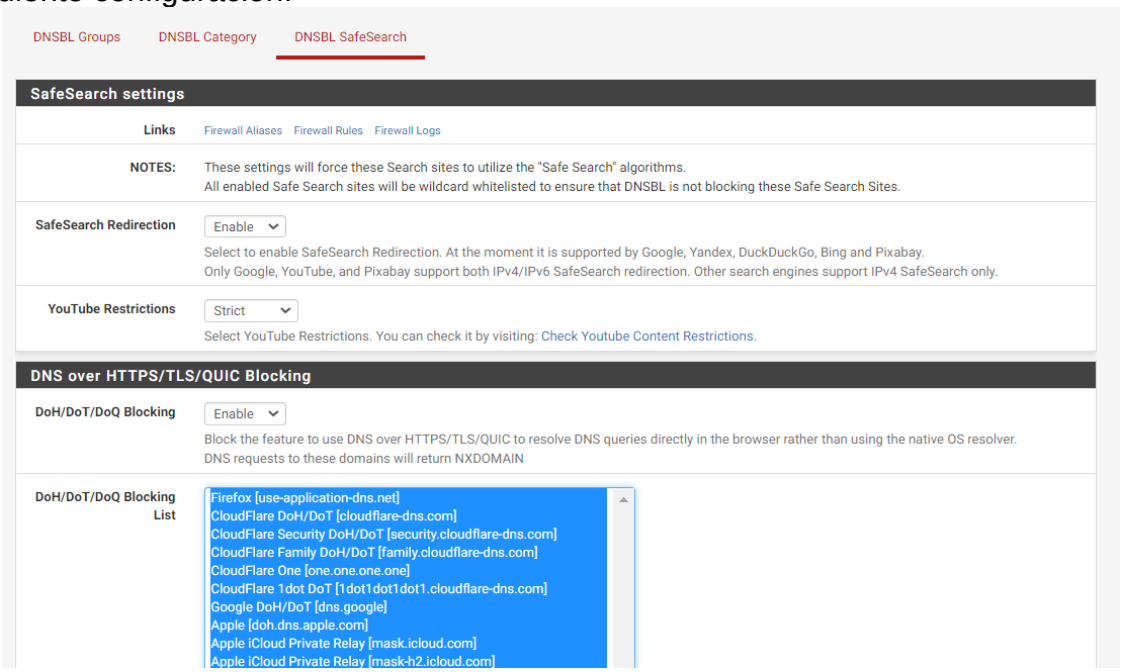


Figura 133: Configuración de Safe Search en pfBlockerNG

A continuación, desde la misma pantalla se bloquea el uso de DNS bajo HTTPS/TLS/QUIC para evitar que se puedan saltar las restricciones DNS, seleccionando todos los elementos de la lista:

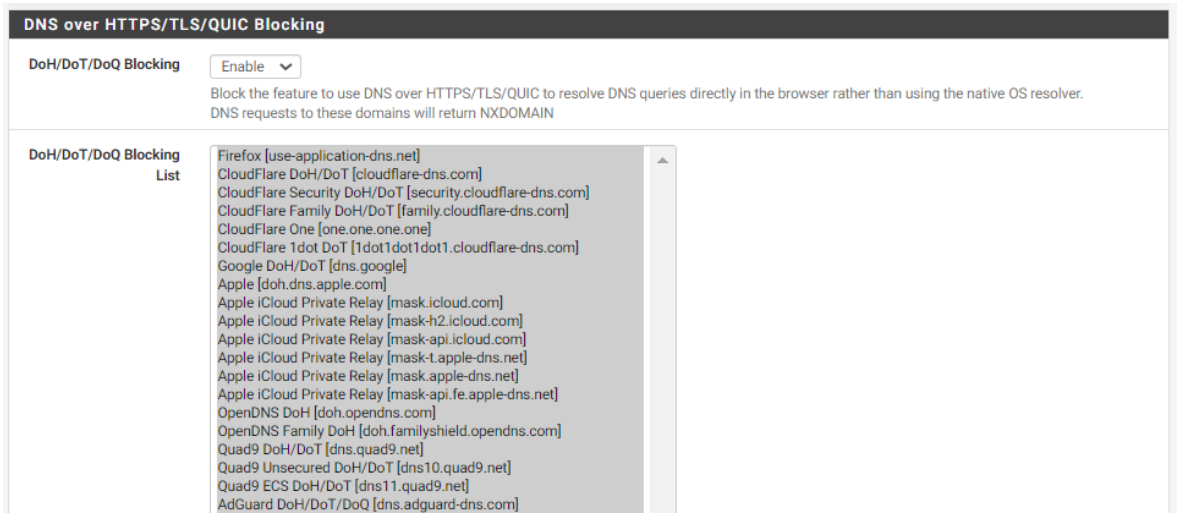


Figura 134: Bloqueo de DNS HTTPS/TLS/QUIC en pfBlockerNG

El siguiente paso es configurar el bloqueo de categorias no adecuadas para menores, desde DNSBL Category, estableciéndolo como en la captura de pantalla siguiente:

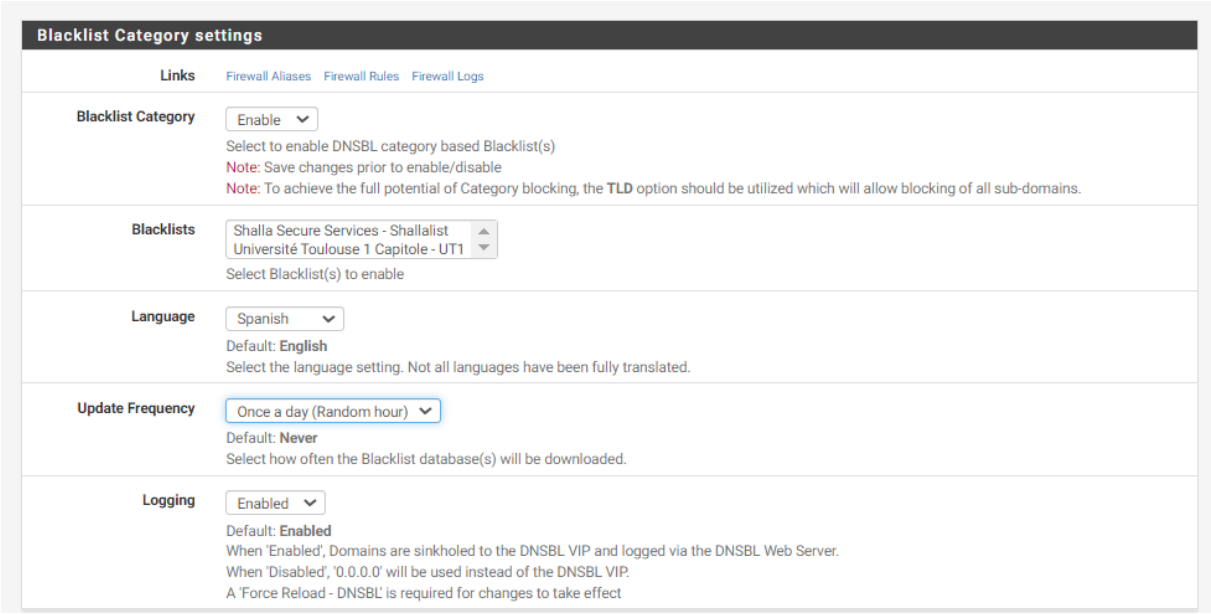


Figura 135: Filtrado por categorias en pfBlockerNG

La Shallalist se configura marcando las siguientes categorias:

- Anuncios
- Cost Traps
- Dating
- Drugs
- Gambling
- Porn
- Remote Control
- Spyware
- Tracker
- Violence

La UT1 se configura marcando:

- Porno (xxx)
- Materiales peligrosos
- Citas
- Drogas
- Apuestas/Casino
- Malware
- Control Remoto
- Phishing
- Publicidad
- Sectas

Una vez marcados, se pulsa save.

Para utilizar bloqueos por geolocalización se debe crear cuenta en https://dev.maxmind.com/geoip/geolite2-free-geolocation-data, generar una licencia:

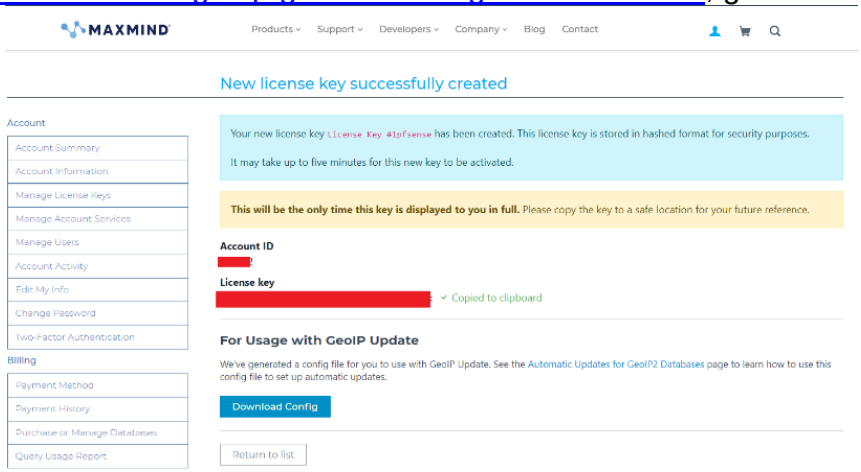


Figura 136: Alta en maxmind.com para key GeoIP

La licencia se debe establecer en Firewall->pfBlockerNG->IP:

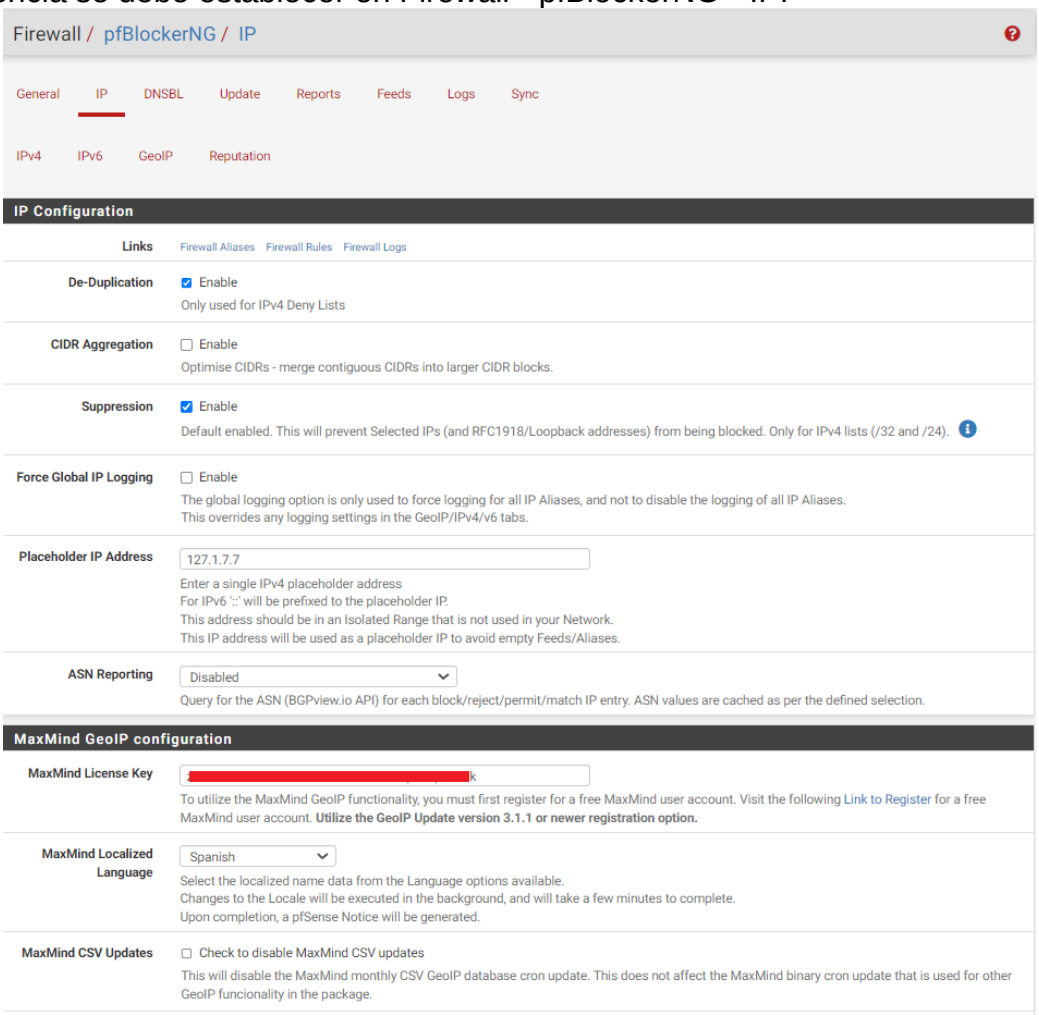


Figura 137: Configuración de GeoIP en pfBlockerNG

Acto seguido se configuran las opciones de configuración de reglas de la siguiente manera:

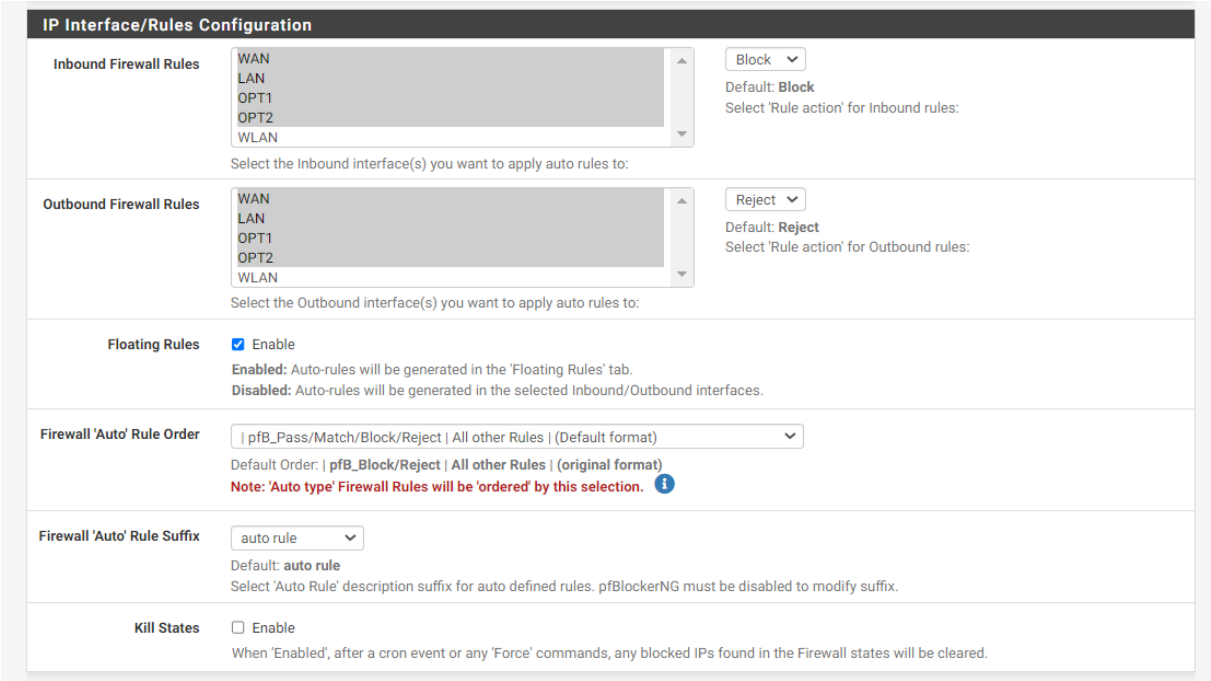


Figura 138: Reglas de firewall de las interfaces de red

Tras esto se selecciona “Run” desde el menú “update” para que se actualice la configuración del firewall DNS con los parámetros que se han establecido, obteniendo el siguiente log:

```
UPDATE PROCESS START [ v3.2.0_4 ] [ 05/7/23 20:47:58 ]

===[  DNSBL Process  ]=============================================

 Missing DNSBL stats and/or Unbound DNSBL files - Rebuilding

 Loading DNSBL SafeSearch... enabled
 Loading DNSBL Whitelist... completed
 Loading TOP1M Whitelist...
 TOP1M Database downloading ( approx 21MB ) ... Please wait ...
 Building TOP1M Whitelist [.] [ Parsed 13317 lines | Found 10000 of 10000 ]...
 DNSBL - TOP1M changes found - Rebuilding!
 completed

[ StevenBlack_ADs ]               Downloading update [ 05/7/23 20:48:03 ] .. 200 OK.
  Whitelist:
ads.bing.com|ads.google.com|ads.youtube.com|adsdk.yandex.ru|adserver.bing.com|adservice.google.be|adservice
.google.ca|adservice.google.co.in|adservice.google.co.jp|adservice.google.co.za|adservice.google.com|adserv
ice.google.com.au|adservice.google.com.mt|adservice.google.com.vn|adservice.google.cz|adservice.google.nl|a
dvertising.yandex.ru|an.yandex.ru|analytics.google.com|bat.bing.com|bs-
meta.yandex.ru|bs.yandex.ru|c.bing.com|fundingchoicesmessages.google.com|indetiske.ya.ru|informer.yandex.ru
|kiks.yandex.ru|localhost.localdomain|mail-
ads.google.com|marketingplatform.google.com|mc.yandex.ru|ms.yandex.ru|pagead-
googlehosted.l.google.com|pagead.l.google.com|partnerad.l.google.com|s.youtube.com|s0-2mdn-
net.l.google.com|smartlock.google.com|ssl-google-analytics.l.google.com|ttnet.yandex.com.tr|video-
stats.video.google.com|www-google-analytics.l.google.com|www.ttnet.yandex.com.tr|
  ------------------------------------------------------------------------
  Orig.    Unique     # Dups     # White    # TOP1M    Final
  ------------------------------------------------------------------------
  177554   177554     0          43         0          177511
  ------------------------------------------------------------------------

------------------------------------------------------------------------
Assembling DNSBL database..... completed [ 05/7/23 20:48:19 ]
TLD:
TLD analysis.. completed [ 05/7/23 20:48:30 ]
TLD finalize..
 ---------------------------------------
 Original    Matches    Removed    Final
 ---------------------------------------
 177511      46306      51823      125688
 ---------------------------------------
TLD finalize... completed [ 05/7/23 20:48:39 ]

Saving DNSBL statistics... completed [ 05/7/23 20:48:42 ]
Stopping Unbound Resolver.
Unbound stopped in 2 sec.
Starting Unbound Resolver... completed [ 05/7/23 20:48:45 ]
DNSBL update [ 125688 | PASSED  ]... completed [ 05/7/23 20:48:47 ]
------------------------------------------------------------------------
```

```
===[  GeoIP Process  ]=============================================


===[  IPv4 Process  ]==============================================

[ Abuse_Feodo_C2_v4 ]              exists.
[ Abuse_SSLBL_v4 ]                 exists.
[ CINS_army_v4 ]           exists.
[ ET_Block_v4 ]                    exists.
[ ET_Comp_v4 ]                     exists.
[ ISC_Block_v4 ]           exists.
[ Spamhaus_Drop_v4 ]               exists.
[ Spamhaus_eDrop_v4 ]              exists.
[ Talos_BL_v4 ]                    exists.
[ DNSBLIP_v4 ]                     Downloading update .. completed ..
[ pfB_DNSBLIP_v4 DNSBLIP_v4 ] No IPs found! Ensure only IP based Feeds are used! ]

===[  Aliastables / Rules  ]=================================

Firewall rule changes found, applying Filter Reload


** Restarting firewall filter daemon **

===[ FINAL Processing ]=====================================

   [ Original IP count   ]  [ 19445 ]

   [ Final IP Count  ]  [ 18261 ]


===[ Deny List IP Counts ]==========================

   18262 total
   15000 /var/db/pfblockerng/deny/CINS_army_v4.txt
    1442 /var/db/pfblockerng/deny/ET_Block_v4.txt
     778 /var/db/pfblockerng/deny/Talos_BL_v4.txt
     634 /var/db/pfblockerng/deny/ET_Comp_v4.txt
     238 /var/db/pfblockerng/deny/Spamhaus_eDrop_v4.txt
     134 /var/db/pfblockerng/deny/Abuse_Feodo_C2_v4.txt
      31 /var/db/pfblockerng/deny/Abuse_SSLBL_v4.txt
       4 /var/db/pfblockerng/deny/ISC_Block_v4.txt
       1 /var/db/pfblockerng/deny/Spamhaus_Drop_v4.txt

====================[ Empty Lists w/127.1.7.7 ]==================

Spamhaus_Drop_v4.txt

===[ DNSBL Domain/IP Counts ] ================================

  125688 /var/db/pfblockerng/dnsbl/StevenBlack_ADs.txt

====================[ IPv4/6 Last Updated List Summary ]==============

May 5    06:30    ET_Block_v4
May 5    12:39    Spamhaus_Drop_v4
May 5    22:37    ET_Comp_v4
May 6    22:51    Spamhaus_eDrop_v4
May 7    18:50    ISC_Block_v4
May 7    19:18    CINS_army_v4
May 7    20:04    Talos_BL_v4
May 7    20:10    Abuse_SSLBL_v4
May 7    20:15    Abuse_Feodo_C2_v4
May 7    20:48    DNSBLIP_v4

====================[ DNSBL Last Updated List Summary ]==============

May 7    20:48    StevenBlack_ADs
================================================================

Database Sanity check [  PASSED  ]
------------------------
Masterfile/Deny folder uniq check
Deny folder/Masterfile uniq check

Sync check (Pass=No IPs reported)
----------

Alias table IP Counts
-----------------------------
   18262 /var/db/aliastables/pfB_PRI1_v4.txt

pfSense Table Stats
-------------------
table-entries hard limit   400000
Table Usage Count         955

 UPDATE PROCESS ENDED
```

Se verifica en este punto que los servicios de pfBlockerNG (pfb_dnsbk y pdb_filter) estén en ejecución (Check verde) y que la RAM y CPU del router estén dentro de los parámetros normales:

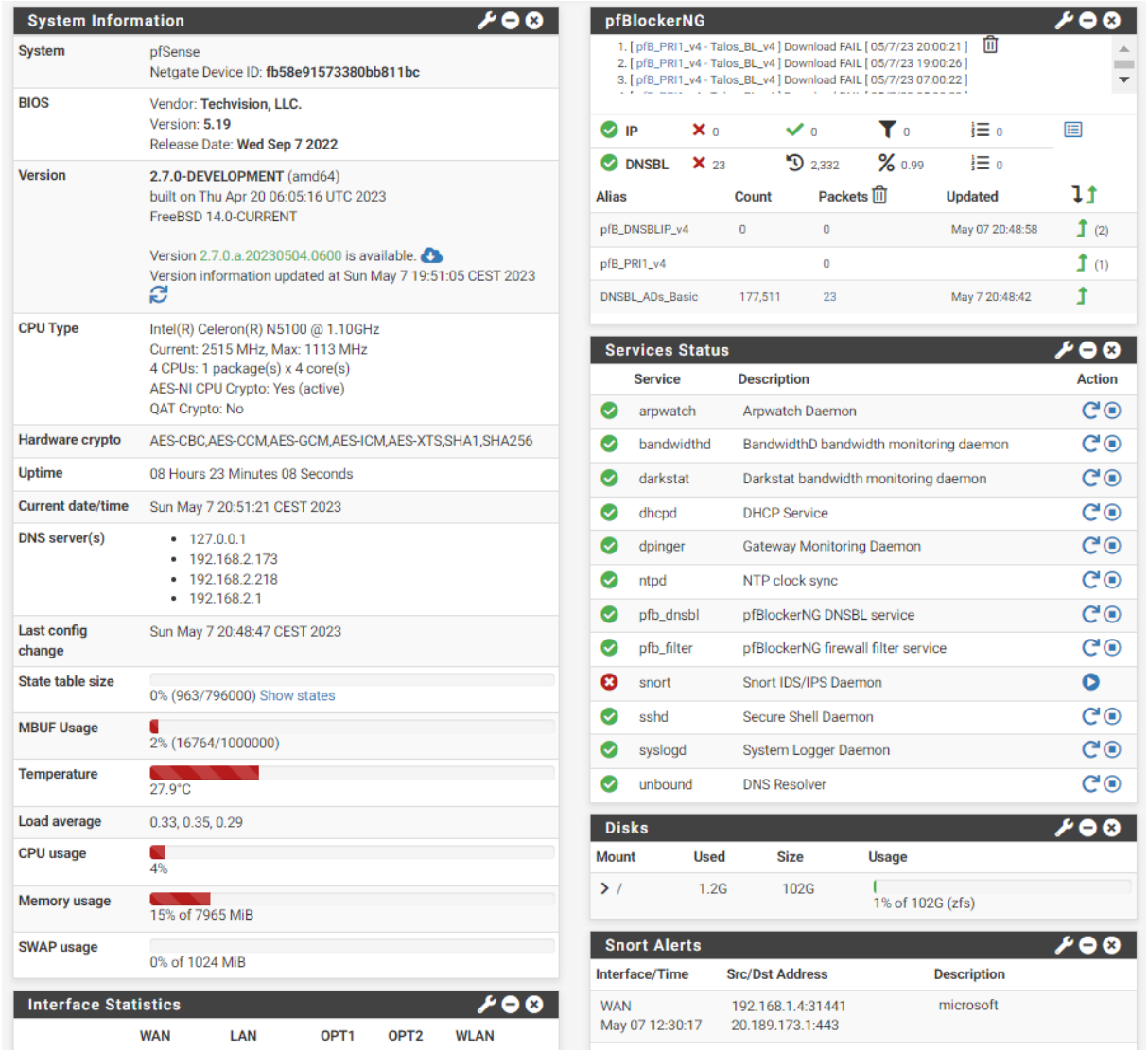


Figura 139: Estado de los servicios en pfSense

A continuación, se seleccionan los Feeds desde los que se alimentarán las reglas que se han configurado, pues la configuración de filtrado, hasta el momento, está prácticamente limitada a anuncios.
Se da un ejemplo con Alienvault, desde Feeds se marca el '+':

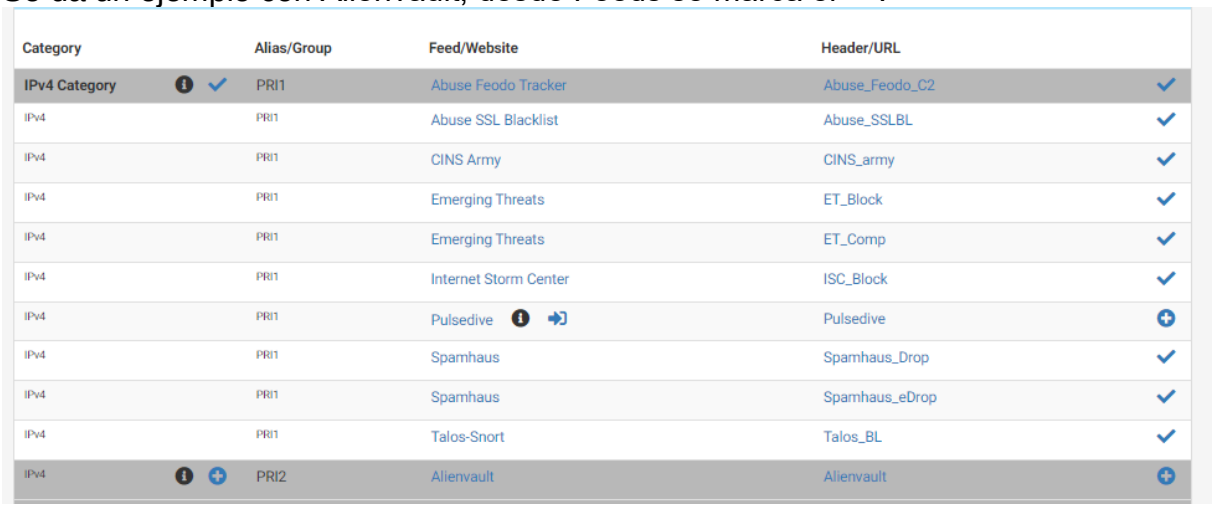


Figura 140: Configuración de los Feeds (1)

Se selecciona ON y en action deny both, se selecciona actualización cada 24 horas y se pulsa Save IP settings:
Se repite la operación con "**DNSBL Category**", seleccionando las listas EasyList Spanish, EasyListPrivacy, ADaway, Abuse URLhaus .
En este caso se seleccionan las listas indicadas, Action=Unbound, actualización diaria:

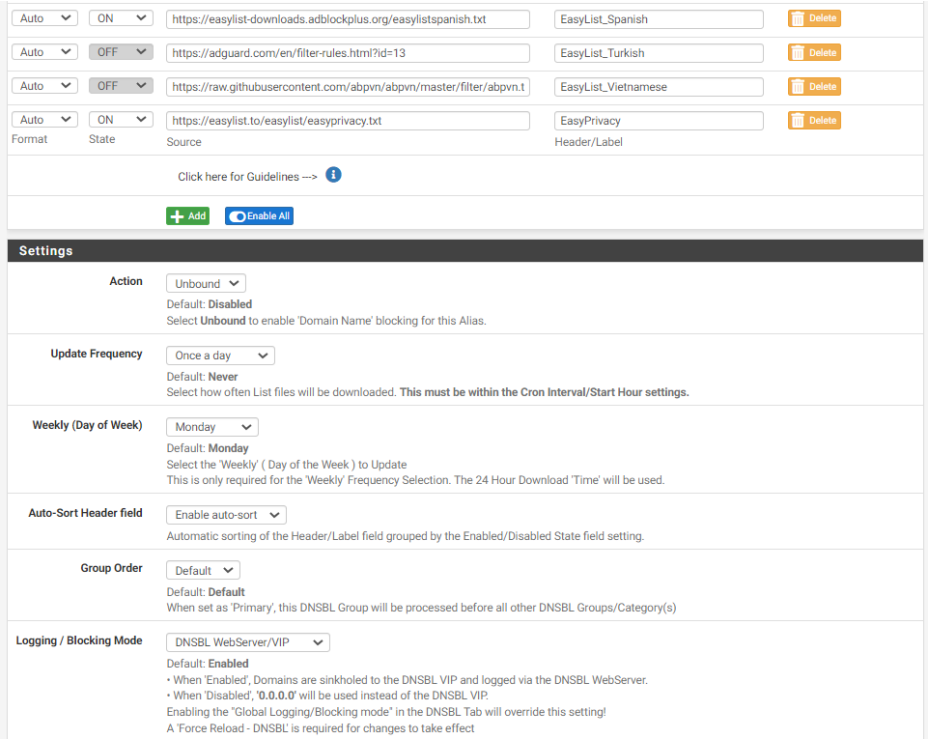


Figura 141: Configuración de los Feeds (2)

A continuación, se realiza un Update->Run para forzar la actualización de la configuración y se revisa que el servidor DHCP asigna el DNS 192.168.2.1 a los equipos que se conectan a la red.

Una vez completado el proceso se verifica el correcto funcionamiento con algunos ejemplos:

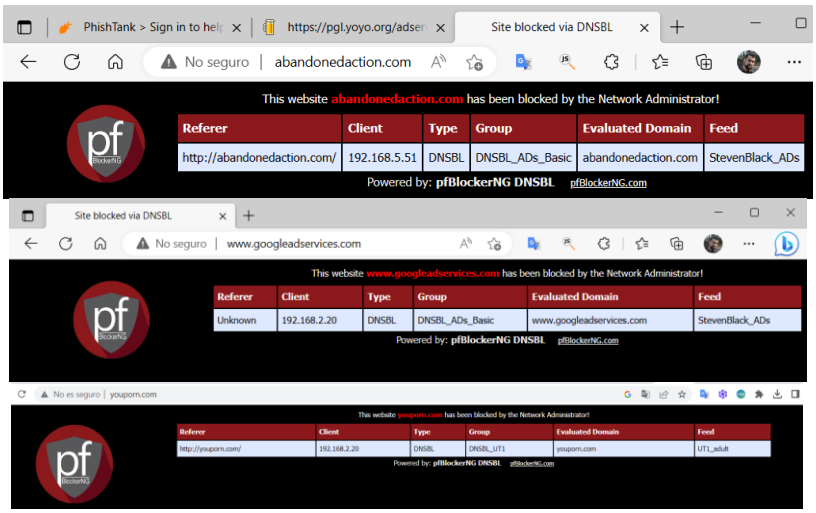


Figura 142: Verificación de bloqueos DNSBL en pfBlockerNG

Se verifica el funcionamiento de las búsquedas estrictas en YouTube:

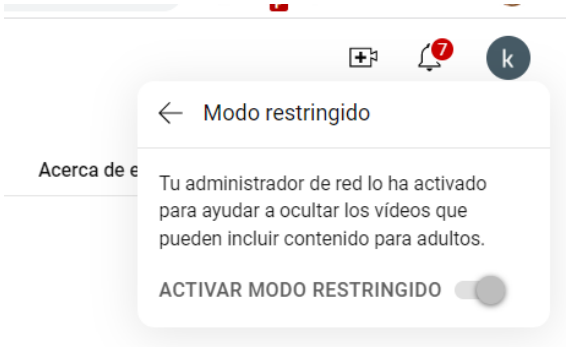


Figura 143: Verificación de las búsquedas seguras en youtube.

Finalmente se verifica que se están registrando los logs de los bloqueos:

DNSBL Block - Last 25 Alert Entries

Date	IF	Source	Domain/Referer|URI|Agent	Feed/Group
May 7 23:01:14 [2]	LAN	192.168.2.86	app-measurement.com [TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 23:00:47 [7]	WLAN	192.168.5.51 PORTATIL-ASUS	analytics.ff.avast.com [~~Unknown~~ | Unknown] DNSBL-Full | -|PRI|HTTP/2.0|-	Unknown Unknown
May 7 22:29:58	LAN	192.168.2.20 portatil-asus	s.click.aliexpress.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:56 [1]	LAN	192.168.2.20 portatil-asus	track.sunmedia.tv [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	EasyPrivacy DNSBL_EasyList
May 7 22:29:56	LAN	192.168.2.20 portatil-asus	onetag-sys.com [TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:54	LAN	192.168.2.20 portatil-asus	sync.richaudience.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	UT1_publicite DNSBL_UT1
May 7 22:29:54	LAN	192.168.2.20 portatil-asus	id5-sync.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:54 [3]	LAN	192.168.2.20 portatil-asus	c2shb.pubgw.yahoo.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:54	LAN	192.168.2.20 portatil-asus	id5-sync.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:54	LAN	192.168.2.20 portatil-asus	c2shb.pubgw.yahoo.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:51	LAN	192.168.2.20 portatil-asus	s.click.aliexpress.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:49 [4]	LAN	192.168.2.20 portatil-asus	c2shb.pubgw.yahoo.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:47	LAN	192.168.2.20 portatil-asus	id5-sync.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:46 [1]	LAN	192.168.2.20 portatil-asus	etahub.com [TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:45 [1]	LAN	192.168.2.20 portatil-asus	prod.us-east-1.cxm-bcn.publisher-services.amazon.dev [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:44	LAN	192.168.2.20 portatil-asus	onetag-sys.com [TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:36	LAN	192.168.2.20 portatil-asus	ncc.avast.com [DNSBL] DNSBL-1x1 | -|GET /ncc.txt HTTP/1.1|...	StevenBlack_ADs DNSBL_ADs_Basic
May 7 22:29:18	LAN	192.168.2.20 portatil-asus	storage.googleapis.com [DNSBL] DNSBL-Full | -|PRI|HTTP/2.0|-	PhishTank DNSBL_Phishing
May 7 22:29:15 [3]	LAN	192.168.2.20 portatil-asus	etahub.com [TLD] DNSBL-Full | -|PRI|HTTP/2.0|-	StevenBlack_ADs DNSBL_ADs_Basic

Figura 144: Logs de pfSense.

vi. Anexo VI: Instalación y configuración de DNSCloak en iPhone

Durante el proceso de instalación se descubrió un posible malware en uno de los móviles (IPhone 11) de los adultos:

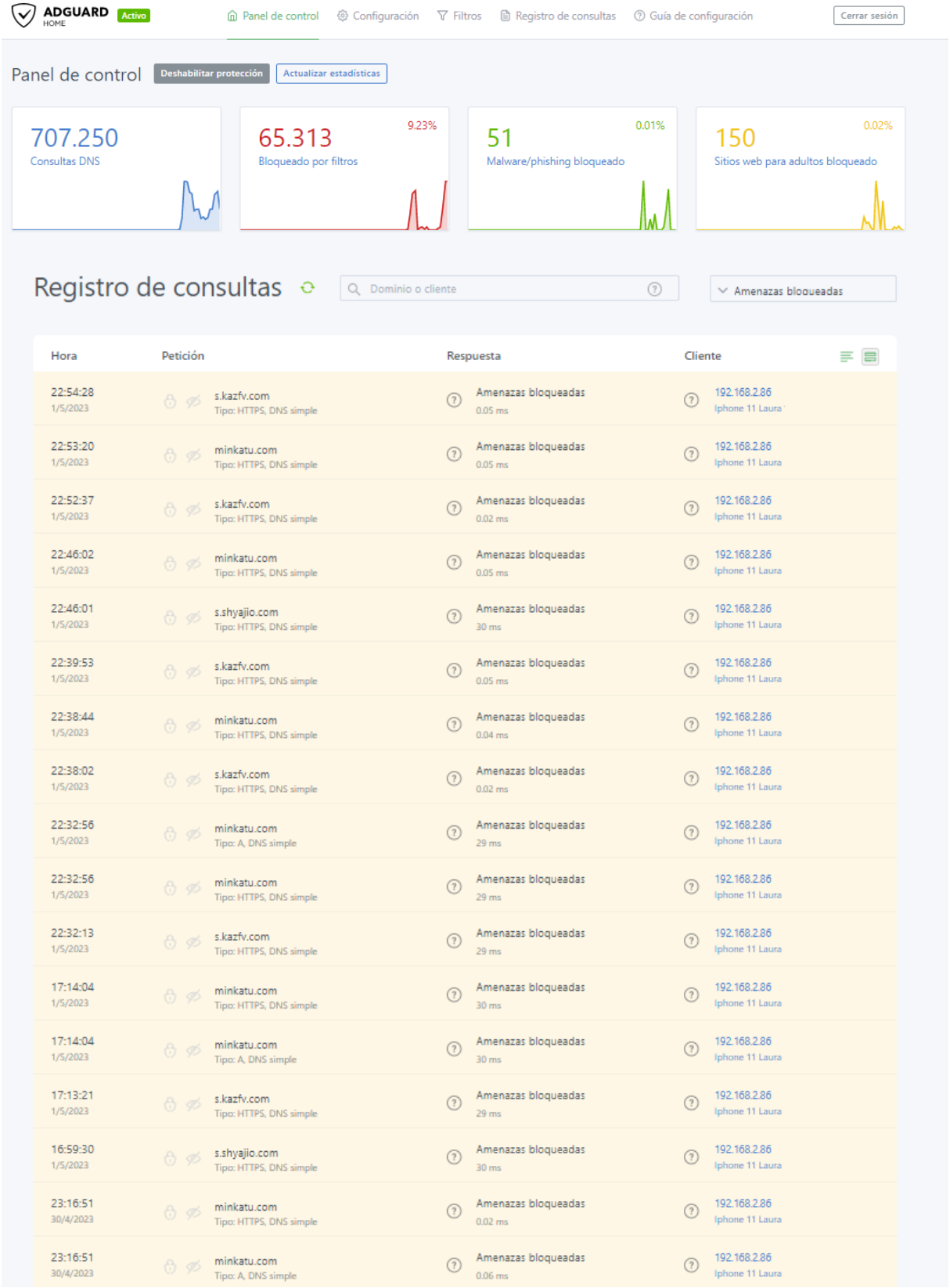


Figura 145: Detección de malware en una app de iPhone.

Tras estudiar el comportamiento del móvil y realizar búsquedas en webs de reputación de IPs y dominios, se termina concluyendo que se trata de una app-juego del tipo “solitario”, que procedió a desinstalar. Dado que se trata de un móvil con tarjeta SIM, quedaba claro que dejaba de estar protegido al salir del hogar mientras utiliza datos móviles y el resolutor DNS que el proveedor de telefonía tenga preconfigurado.
A este hallazgo se suman los crecientes ataques de phishing que se suceden en la actualidad por lo que, aun y no estar definido en el alcance inicial de este trabajo se procedió a buscar e instalar un firewall DNS para iPhone: DNSCloak.
DNSCloak permite escoger el servidor DNS seguro de una lista o introducir uno manualmente, por lo que se deja configurado con el servidor DNS de quad9 que incorpora filtros antimalware y antiphising.
El proceso es tan simple como instalar la aplicación desde la Apple Store y seleccionar quad9-dnscrypt-ip4-filter-ecs-pri (o el OpenDNS) que se ha configurado:

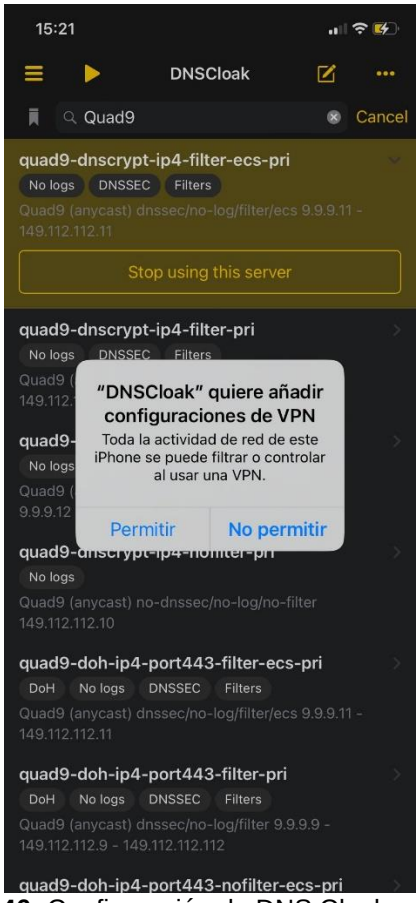


Figura 146: Configuración de DNS Cloak en iPhone.

A continuación, se aceptan los cambios que va proponiendo la aplicación para que termine instalando en el dispositivo una VPN local “always On” con el fin de centralizar la resolución de DNS para todas las aplicaciones, protegiendo así el dispositivo y permitiendo utilizar un DNS en internet público o, si se configura adecuadamente, uno de los 3 servidores DNS que se han instalado en la red de laboratorio (Adguard Home, Pi-Hole, pfBlockerNG).
La configuración que se propone para utilizar el Firewall DNS de la red local implica:

- Configurar NAT hacia el servidor DNS de la red local
- Configurar el firewall DNS para TLS o HTTPS
- Limitar el acceso mediante ACL.

vii. Anexo VII: Instalación y configuración de Quad9 en Android

Tras la protección del IPhone fuera del hogar se decide aplicar el mismo criterio en los móviles Android. Para Android Quad9 provee su propia aplicación, que se instalar y configura con los siguientes parámetros:

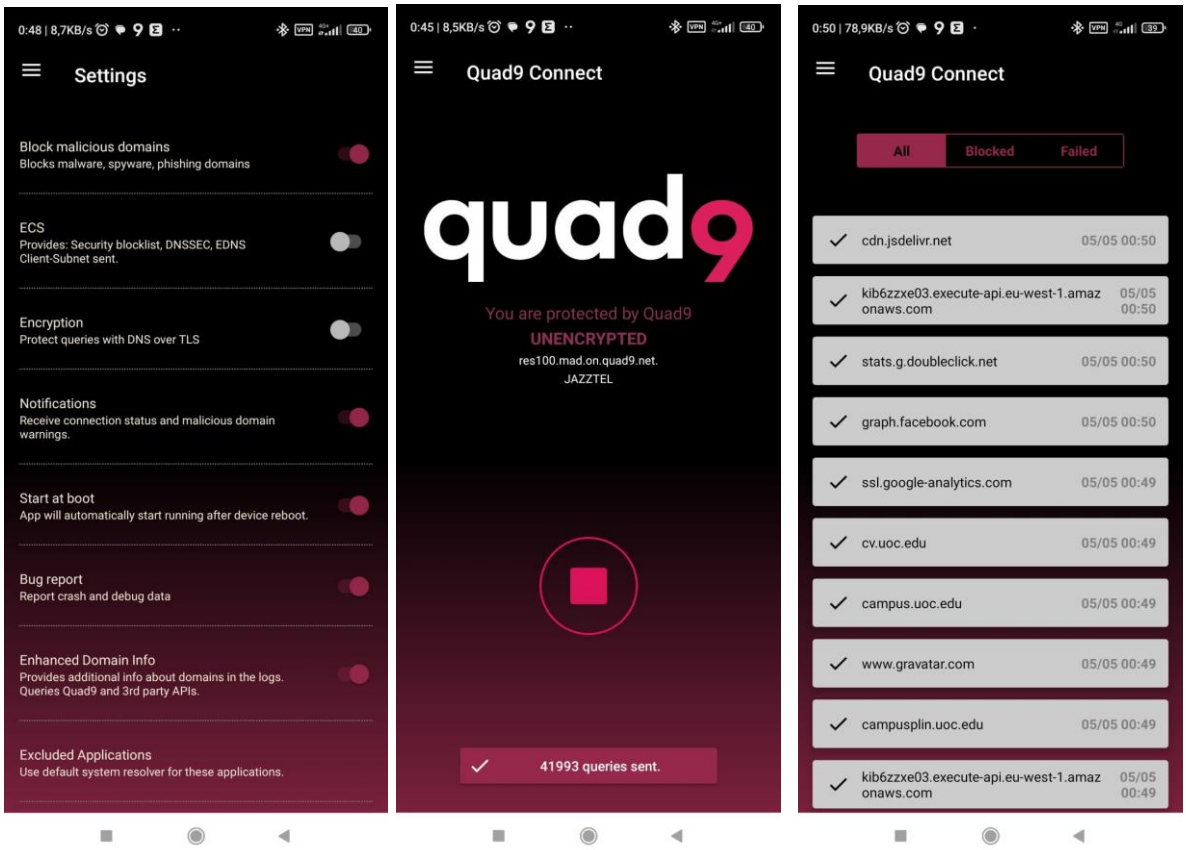


Figura 147: Configuración de Quad9 en Android.

viii. Anexo VIII: Análisis de un caso real de Phishing

El día 27 de abril de 2023, la Asociación Red Nacional de Infértiles, una organización sin ánimo de lucro sufrió un robo de su cuenta de Instagram @redinfertiles, lo que pudiera haber llevado a una brecha de seguridad en cuanto a la protección de datos personales, puesto que pacientes se comunican con ellos por esta vía dando en ocasiones datos de salud.

El proceso consistió en que la presidenta de la asociación recibió un correo electrónico de phishing en el que se le informaba falsamente de que una de sus publicaciones había sido denunciada por lo que se le solicitaba justificarla a través de un enlace. Al hacer clic en el enlace e introducir sus credenciales, se les robó la cuenta y los ciberdelincuentes les exigieron un rescate (económico) a cambio de no eliminar su cuenta y devolvérsela.

En el momento en que se dieron cuenta del robo, el mismo 27 de abril de 2023, notificaron a Instagram a través del correo phish@instagram.com, con la apertura de un ticket de ayuda en Meta Business y con una comunicación al Delegado de Protección de Datos de Instagram. Además, presentaron una denuncia ante la Policía Nacional y notificaron al Instituto Nacional de Ciberseguridad Español (INCIBE) y a la Agencia Española de Protección de Datos sobre la brecha de seguridad. Asimismo,

solicitaron al DPD de Instagram la adopción de medidas en relación con el robo y la posible brecha de seguridad sufrida.
Se ha realizado un estudio sobre este caso real, con el objetivo de documentarlo y difundir la forma de proceder de estos delincuentes.

a. Cuerpo del correo y funcionamiento del web cebo del Phishing

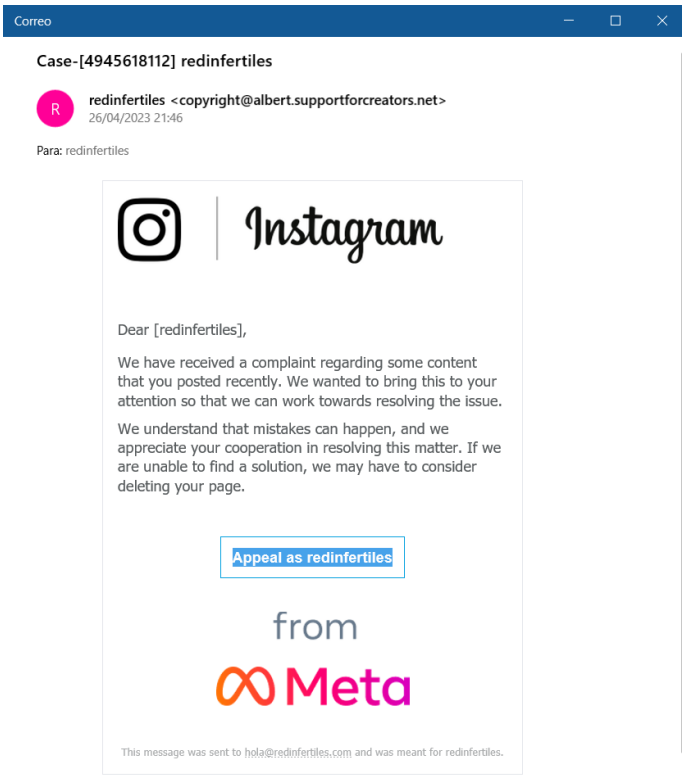


Figura 148: Correo del phishing original

El texto “Appeal as redinfertiles” enlaza a https://www.google.com/amp/a/bit.ly/3naNZMP que a su vez redirige a https://fb-creators.com/589792164/3022951002.

Esta web tenía un aspecto similar a esta otra alojada en el mismo servidor (NOTA: no se pudo disponer ni analizar la página original, dado que cuando ha realizado su función se sustituye por un mensaje avisando del secuestro de cuenta):

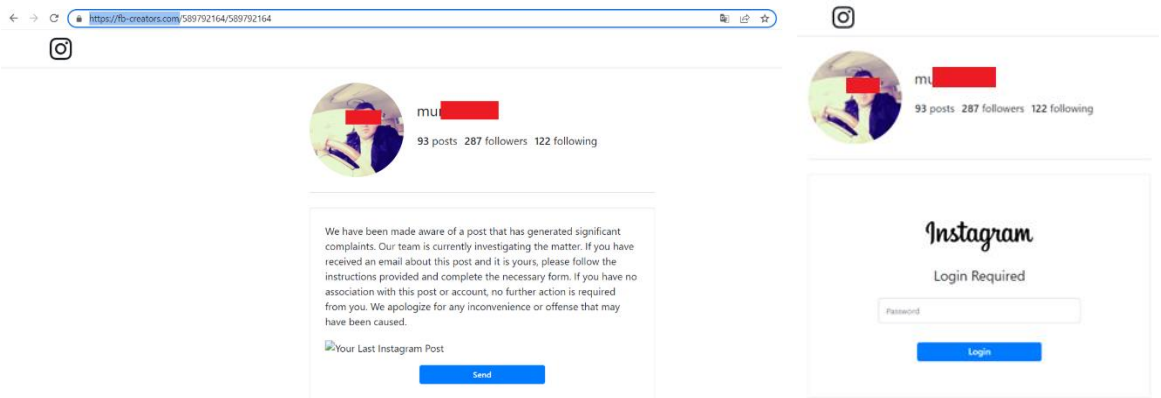


Figura 149: Portal de captura de contraseñas

Cuando se hace clic en “send” aparece una solicitud de contraseña.

Una vez rellenada la contraseña, la web llama a verify.php y se realiza un inicio de sesión en Instagram para validar la contraseña. La web dispone de código que verifica la contraseña, dado que, si se introduce de forma errónea, aparece un mensaje indicando 'wrong password'. Se ha descargado el código javascript y se ha podido comprobar (una vez desofuscado) que contiene funcionalidades para saltarse el captcha e incluso hacer de puente para solicitar **un doble factor de autenticación**:

```
        $.ajax({
            url: "api/ajax-login.php",
            type: "POST",
            data: formValues,
            dataType: 'json',
            success: function (jsondata) {
                saveData("murad_662",JSON.stringify(jsondata));
                if (jsondata.status == 'fail') {
                    if (jsondata.error_type == "old_login") {
                        $("#error").html("You already have an objection made before.");
                    }
                    if (jsondata.error_type == "bad_password") {
                        $("#error").html("Wrong password. Please check your password and try again.");
                        $("#iYLrFMgT").prop("value", "");
                    }
                    if (jsondata.error_type == "invalid_user") {
                        $("#error").html("Username not found please check and try again.");
                    }
                    if (jsondata.error_type == "ip_block" || jsondata.error_type == "bad_request") {
                        $("#error").html("There was a problem please try again.");
                    }
                    if (jsondata.error_type == "two_factor_required") {

                        if (jsondata.two_factor_info.whatsapp_two_factor_on == true) {
                            code_text = "Enter the 6-digit confirmation code we sent to your WhatsApp account.";
                        }else if (jsondata.two_factor_info.totp_two_factor_on == true) {
                            code_text = "Enter a 6-digit login code generated by an authentication app.";
                        }else if (jsondata.two_factor_info.sms_two_factor_on == true) {
                            code_text = "Enter the code we sent to your number ending in " +
jsondata.two_factor_info.obfuscated_phone_number + ".";
                        }
                        window.location = "Code.php?data=" + btoa(code_text);
                    }
                    if (jsondata.error_type == "checkpoint_challenge_required") {
                        window.location.href  = "Verify.php";
                    }
                }
                if (jsondata.status == 'ok') {
                    window.location = "Form.php";
                }
            }
        });
```

Si el receptor del phishing termina confiando e introduciendo su contraseña, la página web cambia a mostrar el siguiente mensaje:

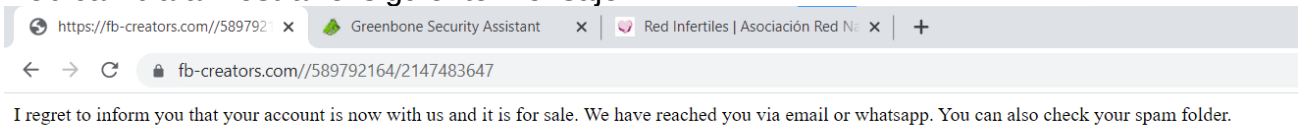


Figura 150: Texto de ciberdelincuentes advirtiendo del robo.

Esto confirma que es un ataque automatizado, dado que la propia web, una vez autentica al usuario, posteriormente realiza operaciones para cambiar la cuenta desde el propio código javascript, que una vez desofuscado se verifica que contiene llamadas a librerías que tienen por objeto saltarse 'captchas'.

Al poco rato de haber recibido el mensaje, el usuario engañado por el phishing recibe por WhatsApp un mensaje del ciberdelincuente (que además se marca por WhatsApp como ‘cuenta de empresa’):

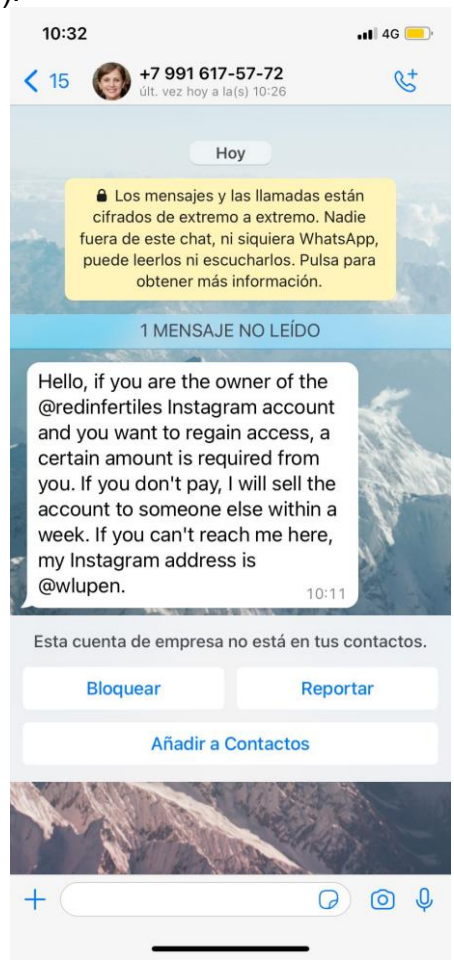


Figura 151: Contacto de los ciberdelincuentes vía WhatsApp.

b. Análisis de las cabeceras del correo recibido

Email Subject

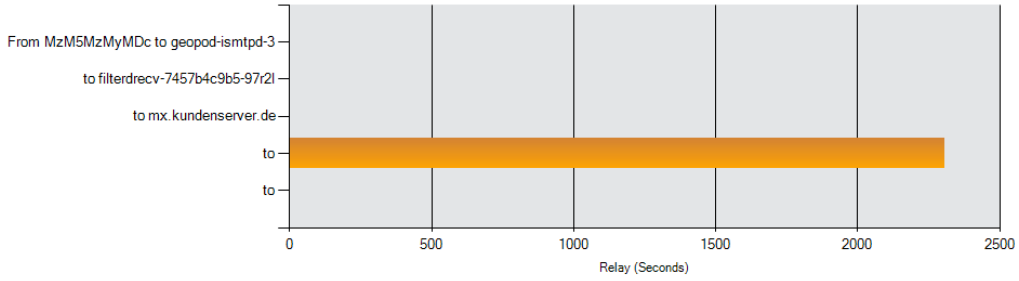
Case-[4945618112] redinfertiles

Delivery Information

- DMARC Compliant (No DMARC Record Found)
- Alignment
- SPF Authenticated
- DKIM Alignment
- DKIM Authenticated

Relay Information

Received Delay: 2309 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	MzM5MzMyMDc	geopod-ismtpd-3	HTTP	[]	
2	*		filterdrecv-7457b4c9b5-97r2l	SMTP	[]	
3	*	wrqvtkxs.outbound-mail.sendgrid.net 149.72.113.166	mx.kundenserver.de 217.72.192.67	ESMTPS (Nemesis)	4/26/2023 7:46:31 PM	
4	38 minutes		2002:a05:600c:3d15:b0:3f1:7b9b:ac4a	POP3	4/26/2023 8:24:57 PM	
5	3 seconds		2002:a05:7412:37cd:b0:c9:8bfa:7826	SMTP	4/26/2023 8:25:00 PM	

SPF and DKIM Information

dmarc:albert.supportforcreators.net

DMARC Record for albert.supportforcreators.net

No DMARC Record found for sub-domain.
Organization Domain of this sub-domain is: supportforcreators.net Inbox Receivers will apply supportforcreators.net DMARC record to mail sent from albert.supportforcreators.net

DMARC Record for supportforcreators.net (organizational domain)

No DMARC Record found for supportforcreators.net

	Test	Result
	DMARC Record Published	No DMARC Record found

Reported by **ns-cloud-a2.googledomains.com** on 4/27/2023 at **8:08:48 PM (UTC 0)**

spf:sendgrid.net:149.72.113.166

v=spf1 ip4:167.89.0.0/17 ip4:208.117.48.0/20 ip4:50.31.32.0/19 ip4:198.37.144.0/20 ip4:198.21.0.0/21 ip4:192.254.112.0/20 ip4:168.245.0.0/17 ip4:149.72.0.0/16 ip4:159.183.0.0/16 include:ab.sendgrid.net ~all

dkim:sendgrid.net:smtpapi

Dkim Public Record:

k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPtW5iwpXVPiH5FzJ7Nrl8USzuY9zqqzjE0D1r04xDN6qwziDnmgcFNNfMewVKN2D1O+2J9N14hRprzByFwfQW76yojh54Xu3uSbQ3JP0A7k8o8GutRF8zbFUA8n0ZH2y0cIEjMliXY4W4LwPA7m4q0ObmvSjhd63O9d8z1XkUBwIDAQAB

Dkim Signature:

v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.net; h=content-transfer-encoding:content-type:from:mime-version:subject:to: cc:content-type:from:subject:to; s=smtpapi; bh=RUJvuOgGRJGqcqDqHFWGBWSuseQcu9imo9KJJY1TA5Q=; b=m7bt2JGp0c7Vo5nsOazo/dda5daoJsTi6Oza4S4jwKSG9aMB5ZaIiAYJ1Nceqbs2xtlr lPzKDMN2nek0zeabkREmxdajYh1gFqjMHTx90LkGI6sxmBBHtz7zANH8KOArv0/wkxszNm uo/xmWwD1CgHAcYHV9P+uYuvzbl2JynvU=

Dkim Signature Error:

There must be at least one aligned DKIM-Signature for the message to be considered aligned. -

Header Name	Header Value
Delivered-To	redinfertiles@gmail.com
X-Google-Smtp-Source	AKy350aPEAX2khCxUxJNl+WulaFXswT7230O3qoj3nkss69UBEBRe0Gvx8oAcsxRye1l4pePIj+y4v1PpY4=
X-Received	by 2002:a5d:6781:0:b0:2ff:f37:9d08 with SMTP id v1-20020a5d6781000000b002ff0f379d08mr2715131wru.14.1682540697612; Wed, 26 Apr 2023 13:24:57 -0700 (PDT)

Authentication-Results	mx.google.com; spf=pass (google.com: domain of bounces+33933207-8ee8-hola=redinfertiles.com@sendgrid.net designates 149.72.113.166 as permitted sender) smtp.mailfrom="bounces+33933207-8ee8-hola=redinfertiles.com@sendgrid.net"; dkim=pass header.i=@sendgrid.net header.s=smtpapi header.b=m7bt2JGp
Received-SPF	pass (google.com: domain of bounces+33933207-8ee8-hola=redinfertiles.com@sendgrid.net designates 149.72.113.166 as permitted sender) client-ip=149.72.113.166;
X-Gmail-Fetch-Info	hola@refinfertiles.com 4 imap.ionos.es 110 hola@redinfertiles.com
Return-Path	<bounces+33933207-8ee8-hola=redinfertiles.com@sendgrid.net>
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.net; h=content-transfer-encoding:content-type:from:mime-version:subject:to: cc:content-type:from:subject:to; s=smtpapi; bh=RUJvuOgGRJGqcqDqHFWGBWSuseQcu9imo9KJJY1TA5Q=; b=m7bt2JGp0c7Vo5nsOazo/dda5daoJsTi6Oza4S4jwKSG9aMB5ZaIiAYJ1Nceqbs2xtlr lPzKDMN2nek0zeabkREmxdajYh1gFqjMHTx90LkGI6sxmBBHtz7zANH8KOArv0/wkxszNm uo/xmWwD1CgHAcYHV9P+uYuvzbl2JynvU=
Content-Transfer-Encoding	quoted-printable
Content-Type	text/html; charset=us-ascii
Date	Wed, 26 Apr 2023 19:46:29 +0000 (UTC)
From	redinfertiles <copyright@albert.supportforcreators.net>
Mime-Version	1.0
Message-ID	<B7qK9u5fQZKhK1IfFpXRWA@geopod-ismtpd-3>
Subject	Case-[4945618112] redinfertiles
X-SG-EID	=?us-ascii?Q?3VSAhyMx0B30NazNA5VM0VG0HlYW9W5tL4ykgosCqT+FVciMMdj0Uee0wBVSeL?= =?us-ascii?Q?mIcegQpx9tnn16TqPDiLzLa9=2FL7xMpe=2Fjop=2FgCS?= =?us-ascii?Q?GYSZdBbaJLQtWM=2FwKSc=2F48evgUc75htfDyHhqKn?= =?us-ascii?Q?0DaIl4rPrxlEVNAICc=2FHXQQqBHecil7UHa+tlvh?= =?us-ascii?Q?2XWz7LcUFdp0UKkScg5Ev197lbK52n+DT8=2F5rwK?= =?us-ascii?Q?VjWD4KVt3Bau9+8jMSMJL1Vwf57b0nEw8z3uqaF?= =?us-ascii?Q?TZQ5MFkBMzNHdMu=2Fm7ePw=3D=3D?=
To	redinfertiles <hola@redinfertiles.com>
X-Entity-ID	7MeuMClzjSQiNDizy7XQiw==
Envelope-To	<hola@redinfertiles.com>
X-Spam-Flag	NO

c. Auditoria del portal de captura de credenciales con Subgraph Vega y GreenBone OpenVAS

Se revisa el registro DNS, que apunta a dos IPs:

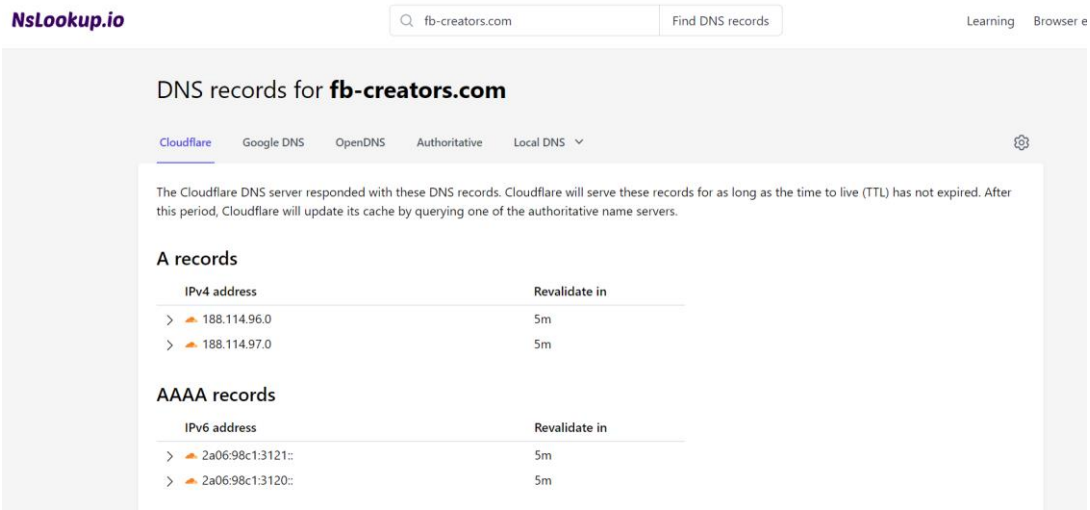


Figura 152: nslookup.

Además de utilizar el debugger del navegador Chrome, se realiza un análisis WAS de la web para recopilar información sobre los archivos y Servicios que contiene, descubriendo algunos cebos Preparados adicionales y la ubicación de código ofuscada.

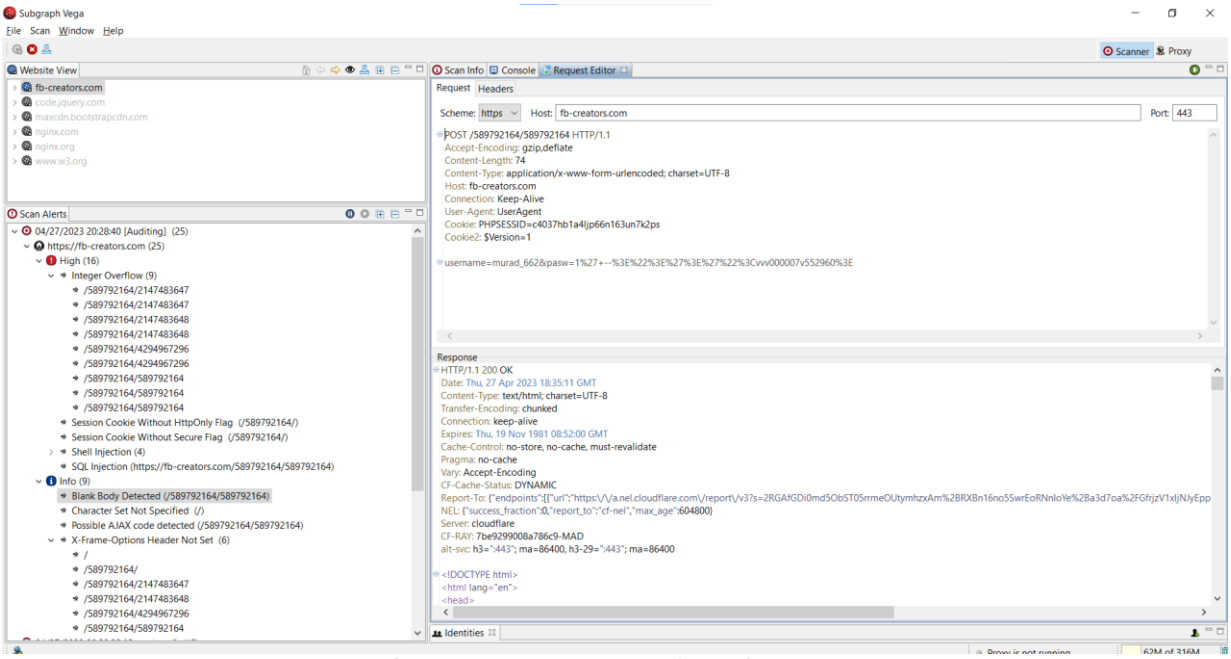


Figura 153: WAS con Subgraph Vega.

Tras escaneo de vulnerabilidades con Greenbone/OpenVAS se detecta el servidor web en 15 puertos distintos de la maquina: 80;443,8080;8443;8081; etc…

Tras este análisis la web y el emisor del correo fue denunciada al INCIBE, Cloudfare y reportada a listas de filtrado RPZ de Phishing para utilizarla en Firewalls DNS.

La web no fue desmantelada hasta 10 días más tarde

ix. Anexo IX: Configuración de personalDNSfilter en Android

Desde la PlayStore se busca el software personalDNSfilter y se pulsa instalar:

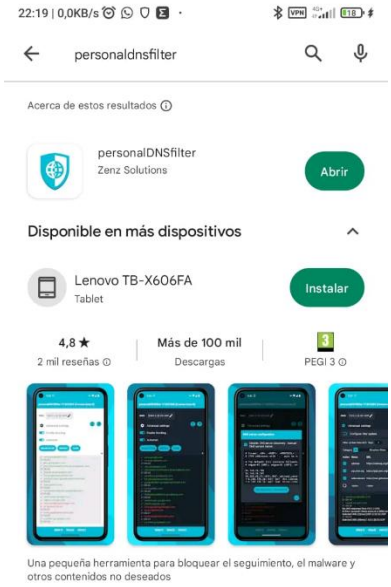


Figura 154: Aplicación en la Playstore.

Una vez instalado se configuran los servidores DNS:

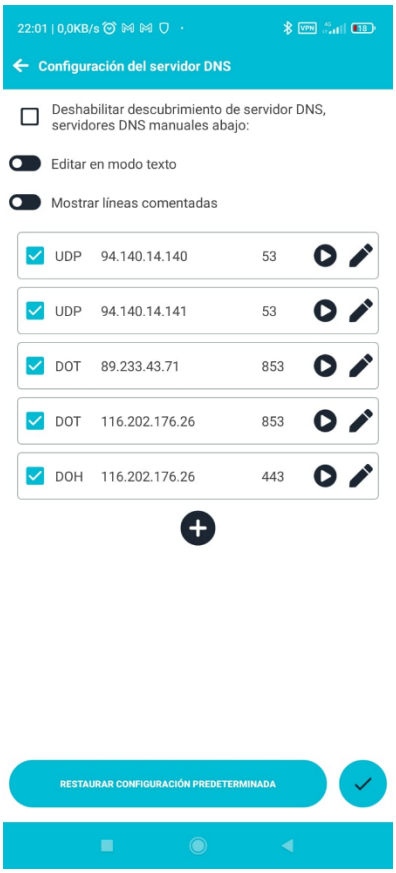


Figura 155: Configuración de los servidores DNS.

Y a continuación se seleccionan las listas RPZ, donde hay listas de filtros por categorias:

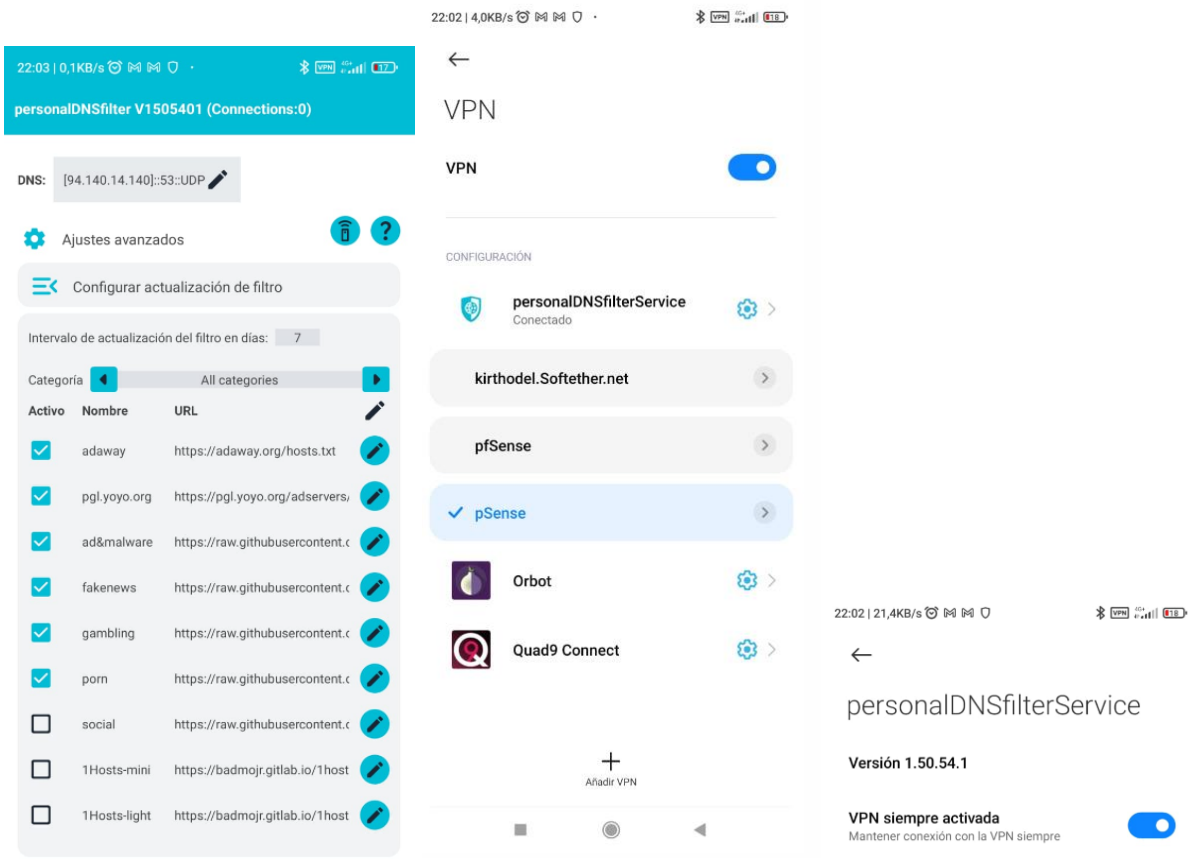


Figura 156: Configuración de los filtros y de VPN always-on.

Una vez configuradas las categorias y las listas se accede a la configuración de VPN de Android, donde se ha configurado una nueva VPN de personalDNSfilter, cuya función es forzar a todas las aplicaciones a resolver las DNS pasando por la aplicación. Tras hacer clic sobre el engranaje se configura la VPN-Always-On.

x. Anexo X: Certificados para SSL y DNS dinámico para conexión FTTH

Con Lets Encrypt! es sencillo y gratuito el proceso de crear un certificado que sea avalado por una CA de confianza reconocida en Internet.

Para crearlo es suficiente con disponer de Python e instalar “certbot”, con el siguiente comando:

```
Pip3 install certbot
```

A continuación, hay que asegurarse de no tener corriendo ningún servicio como Internet Information Server en los puertos 80 y 443 el equipo en el que se va a ejecutar, en Windows puede verificarse con el siguiente comando:

```
C:\WINDOWS\system32>netstat -ano | findstr :80 | findstr LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING       5956
  TCP    127.0.0.1:8085         0.0.0.0:0              LISTENING       5956
  TCP    192.168.56.1:8080      0.0.0.0:0              LISTENING       5956
  TCP    192.168.170.1:8080     0.0.0.0:0              LISTENING       5956
  TCP    [::]:80                [::]:0                 LISTENING       4
```

Si aparece el Puerto en estado LISTENING se puede detener el servicio con el siguiente comando:

```
C:\WINDOWS\system32>net stop http
Los siguientes servicios son dependientes del servicio de Servicio HTTP.
Detener el servicio de Servicio HTTP también detendrá estos servicios:

   Servicio de uso compartido de red del Reproductor de Windows Media
   Servicio de publicación World Wide Web
   Dispositivo host de UPnP
   Detección SSDP
   Cola de impresión
   Publicación de recurso de detección de función

¿Desea continuar esta operación? (S/N) [N]: S

El servicio de Servicio de publicación World Wide Web está deteniéndose.
El servicio de Servicio de publicación World Wide Web se detuvo correctamente.

El servicio de Dispositivo host de UPnP está deteniéndose.
El servicio de Dispositivo host de UPnP se detuvo correctamente.

El servicio de Publicación de recurso de detección de función está deteniéndose.
El servicio de Publicación de recurso de detección de función se detuvo correctamente.
```

A continuación, hay que establecer NAT desde el puerto 80 y el puerto 443 del router hacia el equipo que va a solicitar el certificado:

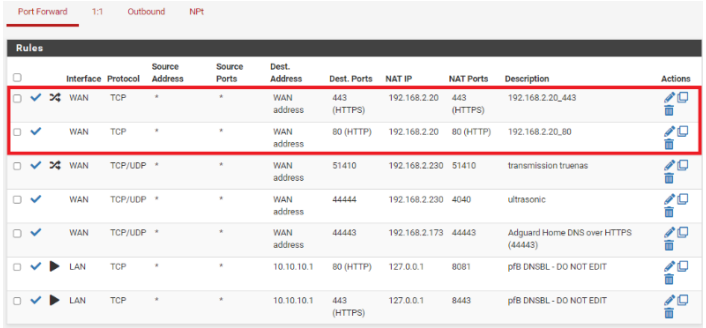


Figura 157: Configuración del NAT en router pfSense

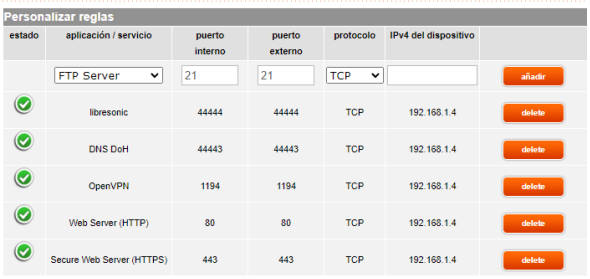


Figura 158: Configuración del NAT en router Jazztel

A continuación, si no se dispone de un subdominio, se puede registrar uno de forma gratuita en webs como freedns[137]. Para el laboratorio se han utilizado dos subdominios, uno de freedns y otro de softether.net: kirthodel.softether.net y kirthodel.mooo.com.

En el router pfsense se configuran los subdominios para su actualización automática:

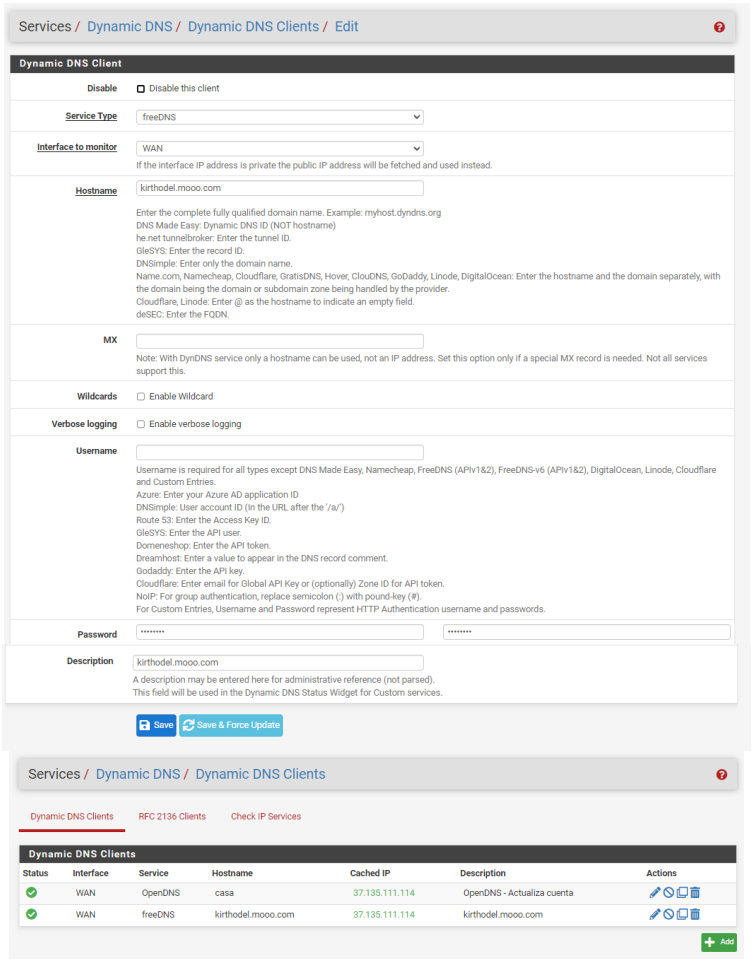


Figura 159: Configuración de los DNS dinámicos en router pfSense

Con todo preparado, ya se puede ejecutar la solicitud de certificado, para ello se debe seguir la siguiente secuencia (en negrita):

```
C:\WINDOWS\system32>certbot certonly -manual
Saving debug log to C:\Certbot\log\letsencrypt.log

How would you like to authenticate with the ACME CA?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Runs an HTTP server locally which serves the necessary validation files under
the /.well-known/acme-challenge/ request path. Suitable if there is no HTTP
server already running. HTTP challenge only (wildcards not supported).
(standalone)
2: Saves the necessary validation files to a .well-known/acme-challenge/
directory within the nominated webroot path. A seperate HTTP server must be
running and serving files from the webroot path. HTTP challenge only (wildcards
not supported). (webroot)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): kirthodel.softether.net
Requesting a certificate for kirthodel.softether.net

Successfully received certificate.
Certificate is saved at: C:\Certbot\live\kirthodel.softether.net\fullchain.pem
Key is saved at:         C:\Certbot\live\kirthodel.softether.net\privkey.pem
This certificate expires on 2023-08-11.
These files will be updated when the certificate renews.
```

Y se repite la operación con el otro subdominio:

```
C:\WINDOWS\system32>certbot certonly -manual
Saving debug log to C:\Certbot\log\letsencrypt.log

How would you like to authenticate with the ACME CA?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Runs an HTTP server locally which serves the necessary validation files under
the /.well-known/acme-challenge/ request path. Suitable if there is no HTTP
server already running. HTTP challenge only (wildcards not supported).
(standalone)
2: Saves the necessary validation files to a .well-known/acme-challenge/
directory within the nominated webroot path. A seperate HTTP server must be
running and serving files from the webroot path. HTTP challenge only (wildcards
not supported). (webroot)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): kirthodel.mooo.com
Requesting a certificate for kirthodel.mooo.com

Successfully received certificate.
Certificate is saved at: C:\Certbot\live\kirthodel.mooo.com\fullchain.pem
Key is saved at:         C:\Certbot\live\kirthodel.mooo.com\privkey.pem
This certificate expires on 2023-08-12.
These files will be updated when the certificate renews.
```

Estos certificados se almacenan importándolos al gestor de certificados de pfSense:

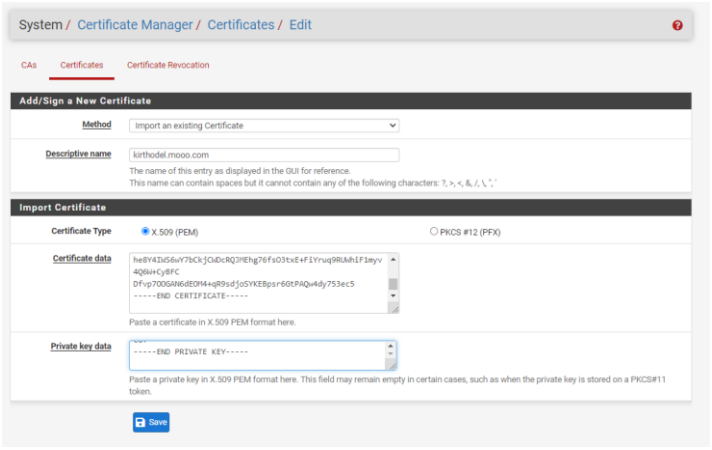


Figura 160: Proceso de importar certificados en router pfSense

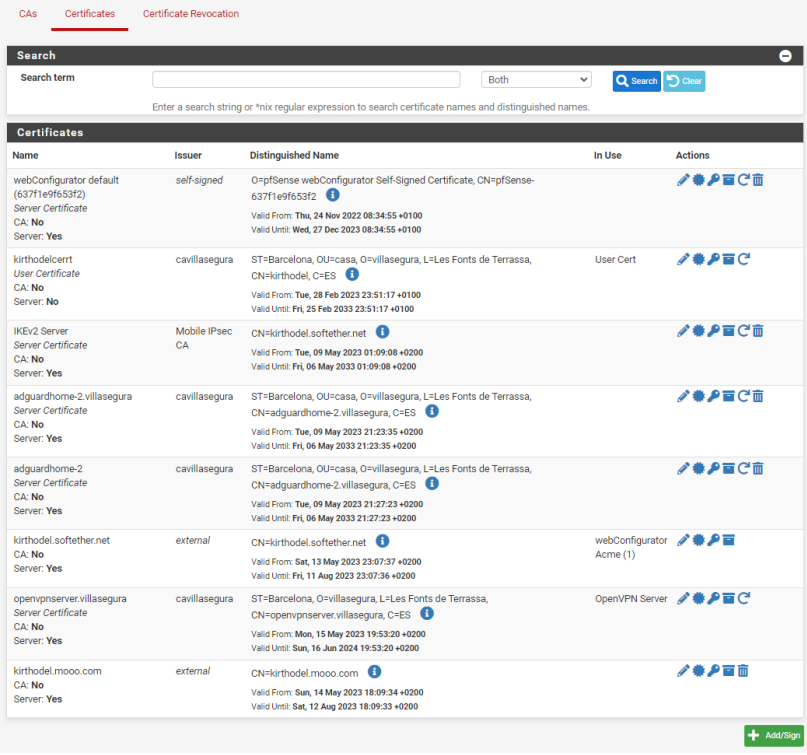


Figura 161: Certificados almacenados en router pfSense

Una vez se dispone de certificado se configura en el servidor Adguard Home, habilitando el cifrado:

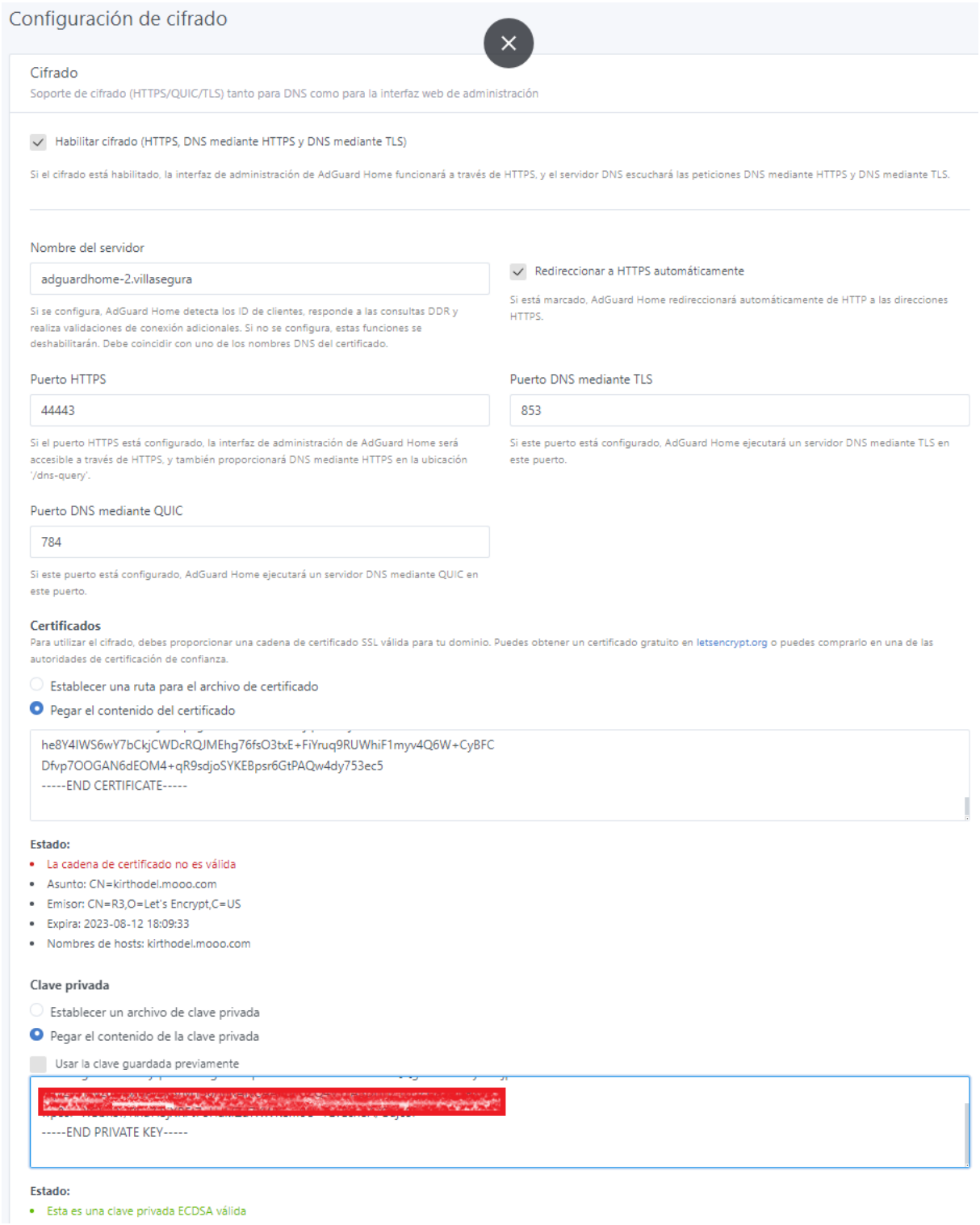


Figura 162: Configuración del cifrado SSL en Adguard Home

xi. Anexo XI: Configuración de VPN OpenVPN en router pfSense

Para poder extender la protección fuera del ámbito del hogar o escuela en los dispositivos móviles, se configura una VPN con OpenVPN desde pfSense.
Para ello se utiliza el asistente en VPN->OpenVPN->Wizard y se siguen los siguientes pasos:

Selección de autenticación de usuario local:

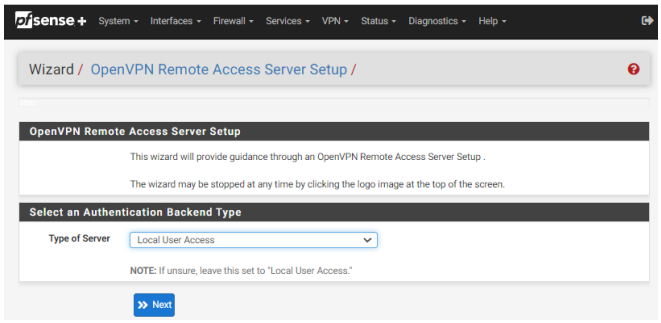


Figura 163: Configuración de OpenVPN en pfSense (I)

Selección de la CA (si no se dispone de una se puede crear desde el propio asistente):

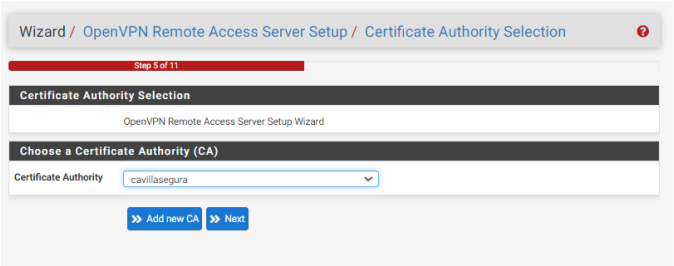


Figura 164: Configuración de OpenVPN en pfSense (II)

Configuración del servidor, en el puerto 1194, con TLS y solo para TCP con IPv4.

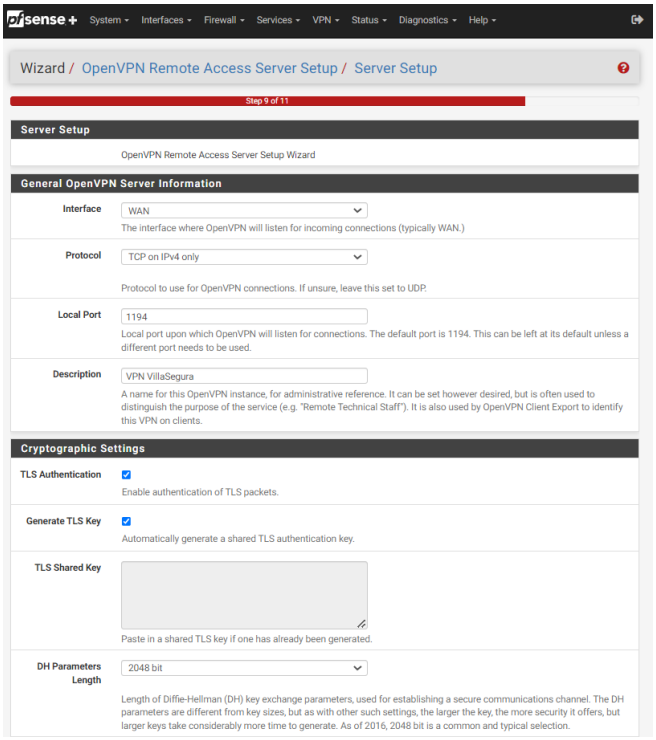


Figura 165: Configuración de OpenVPN en pfSense (III)

Se establecen las suites de cifrado, la aceleración por hardware del equipo y se establece la red 192.168.100.0/24 para la VPN. Se establecen 10 conexiones concurrentes y el DNS el Adguard Home (192.168.2.173):

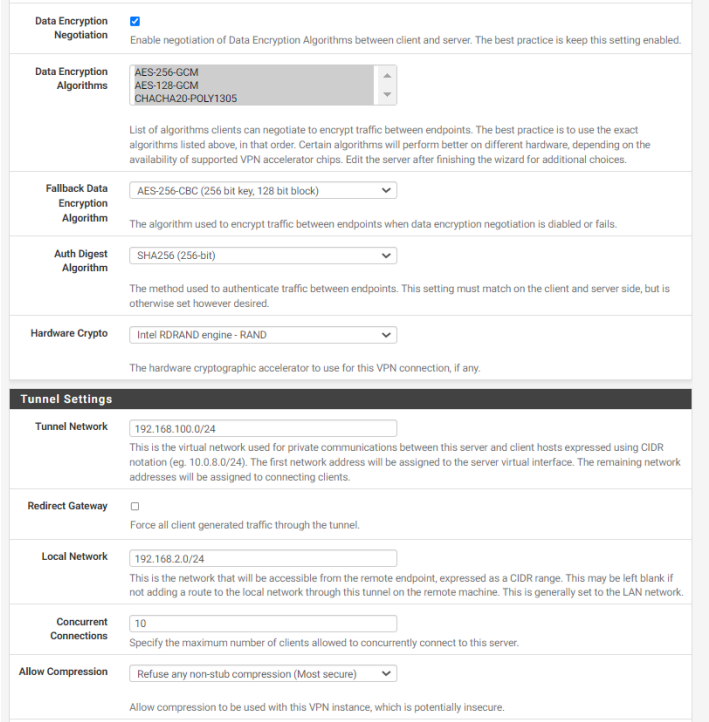


Figura 166: Configuración de OpenVPN en pfSense (IV)

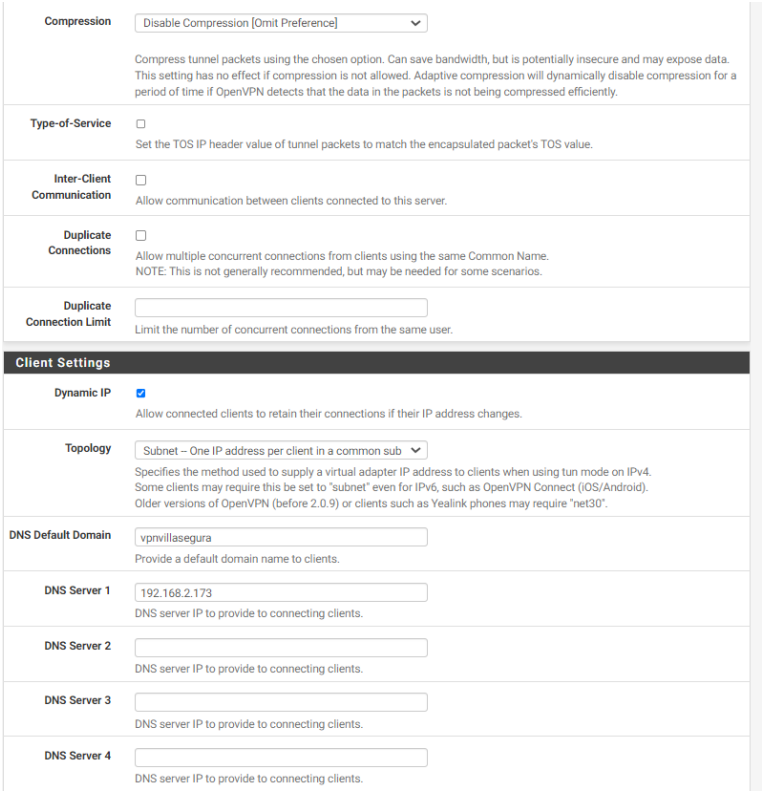


Figura 167: Configuración de OpenVPN en pfSense (IV)

Finalmente se configura como servidor de tiempos al propio router pfSense, que a su vez toma la fecha de hora.roa.es:

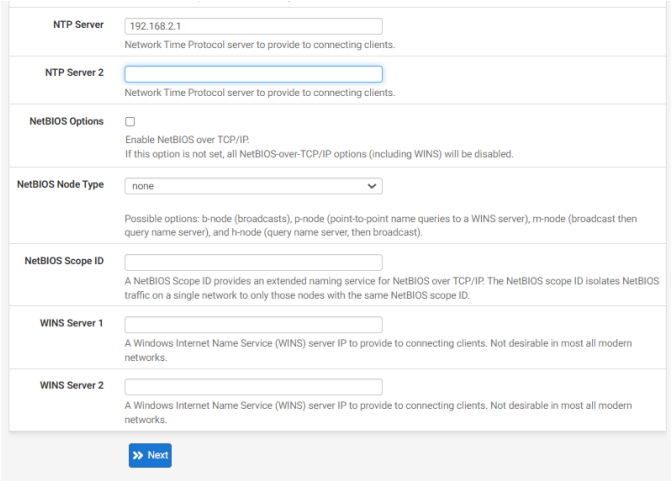


Figura 168: Configuración de OpenVPN en pfSense (IV)

Se configura para que el wizard cree las reglas del firewall y el acceso de la red de OpenVPN a comunicarse con las otras redes del hogar / escuela:

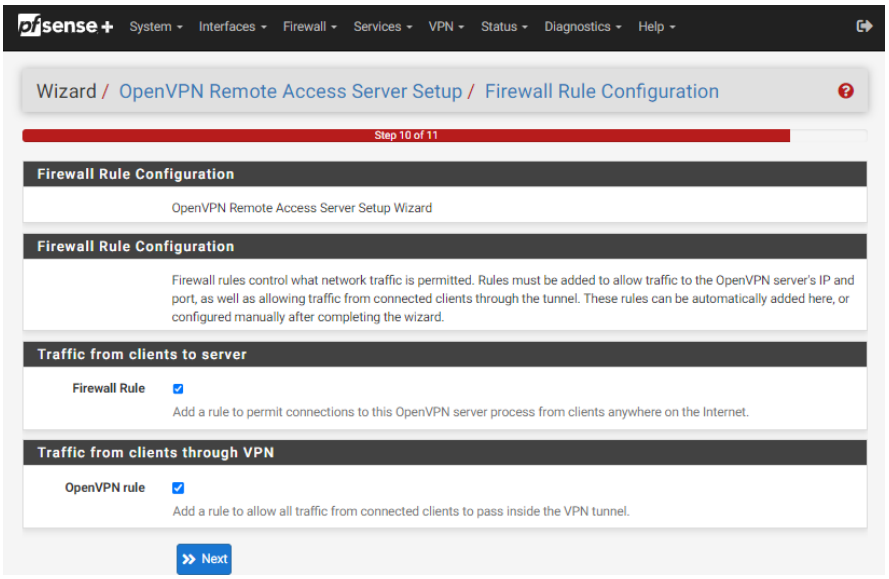


Figura 169: Configuración de OpenVPN en pfSense (IV)

Finalmente se pulsa “Finish” para aplicar la configuración:

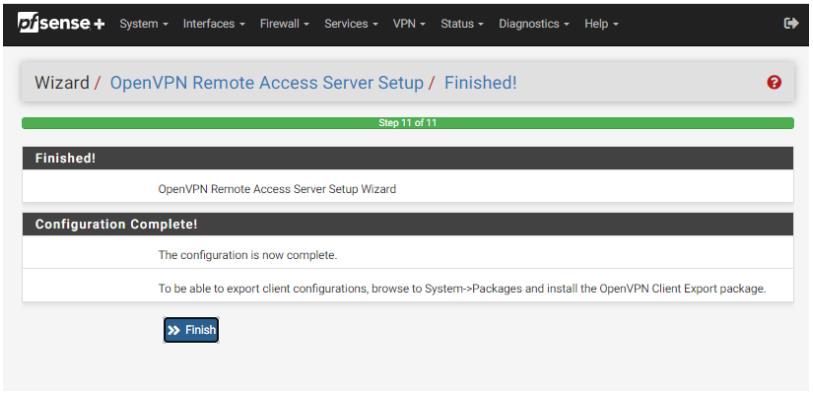


Figura 170: Configuración de OpenVPN en pfSense (IV)

Una vez completado el asistente ya aparece configurado el servidor de VPN:

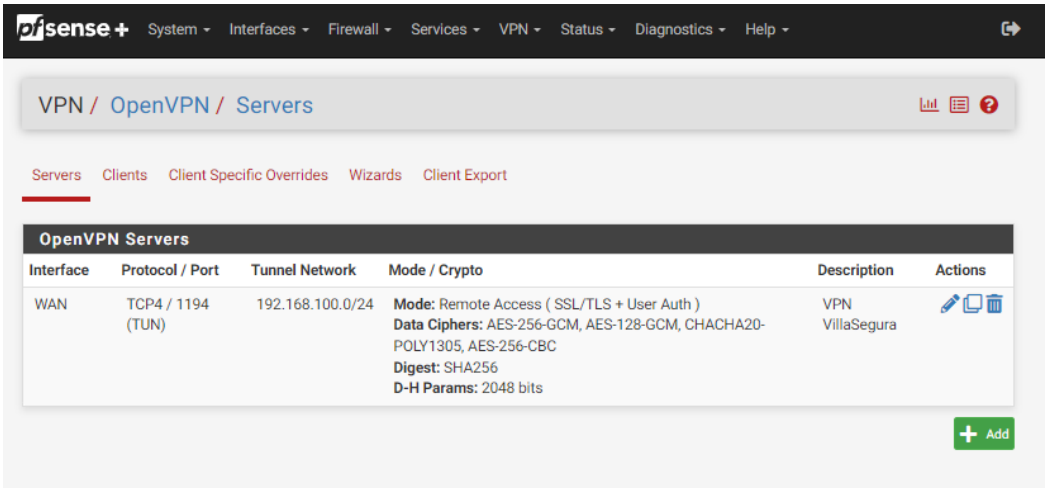


Figura 171: Servidor OpenVPN en pfSense configurado

Para poder conectar con ella se requiere crear un usuario desde System->User Manager->Users->Add, al que se le añade un certificado de usuario:

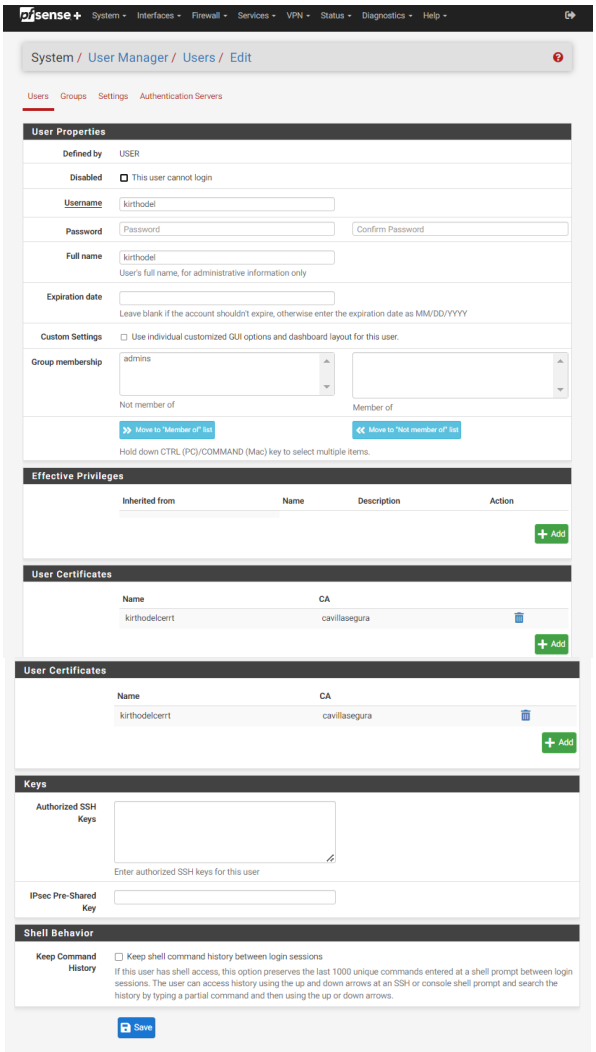


Figura 172: Creación de usuario para acceso por OpenVPN

El siguiente paso es verificar las reglas del firewall para acceso al puerto 1194 desde la WAN y la configuración del NAT en el Router del ISP del puerto 1194 TCP hacia el pfSense:

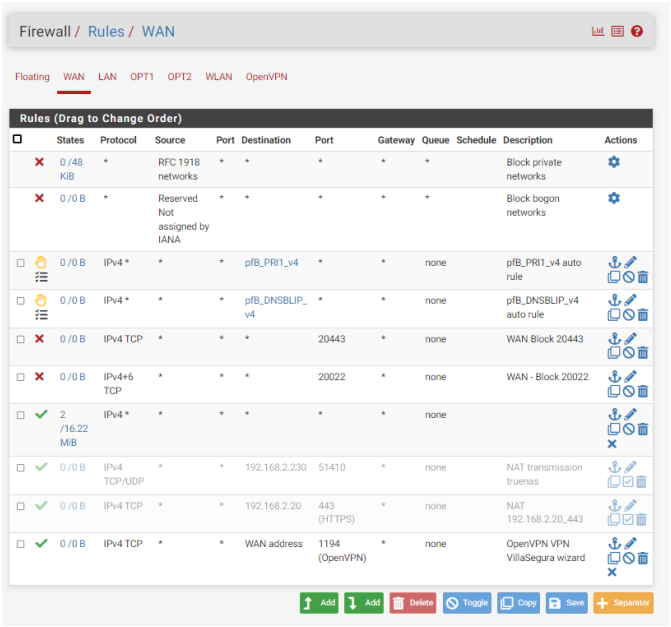


Figura 173: Regla de firewall para OpenVPN (última línea)

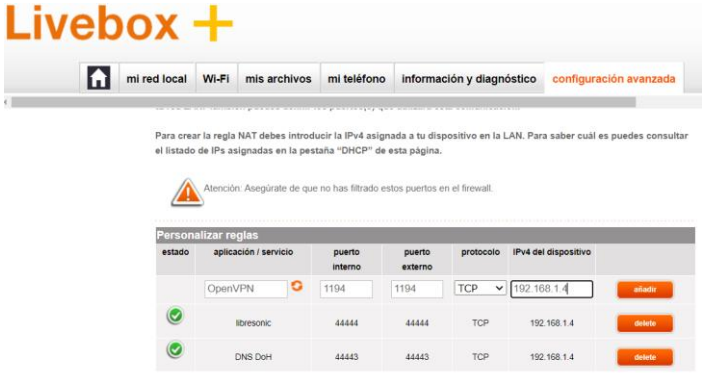


Figura 174: Nueva regla de NAT para OpenVPN

A continuación utilizamos el exportador de configuración de pfSense para generar el archivo de configuración de la VPN:

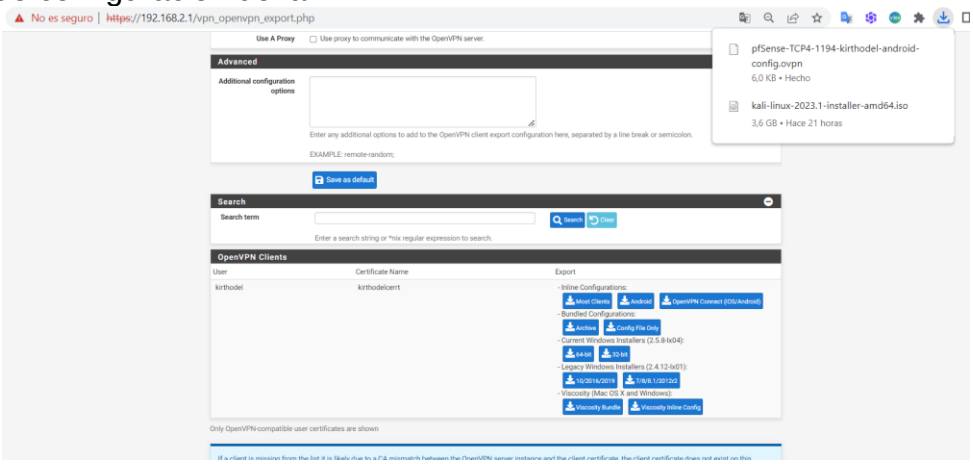


Figura 175: Exportando la configuración de cliente de OpenVPN (I)

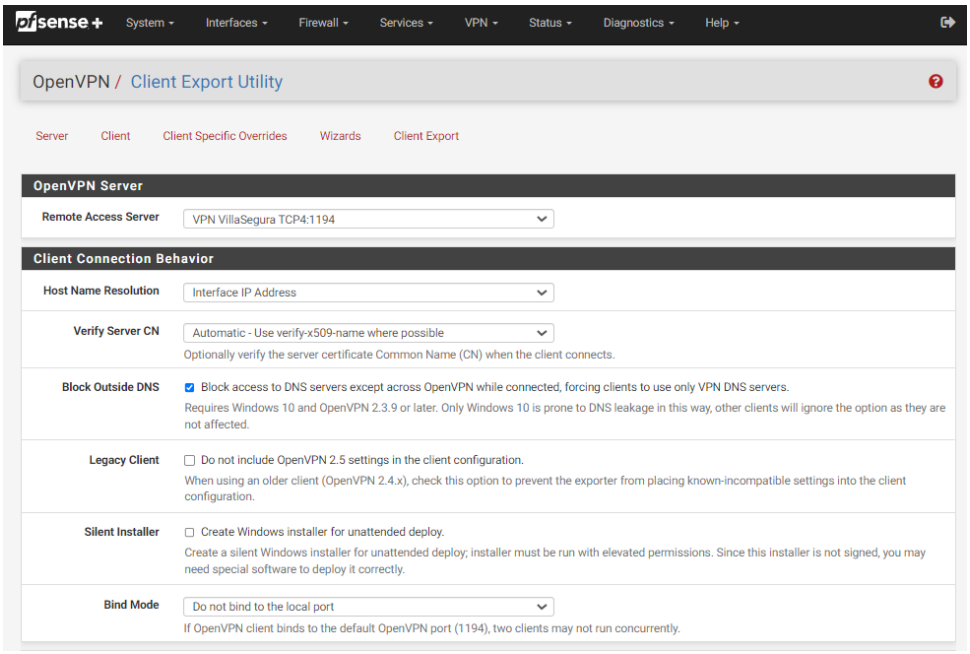


Figura 176: Exportando la configuración de cliente de OpenVPN (II)

Acto seguido, en el teléfono móvil se instala la aplicación OpenVPN y se importa y configura la conexión:

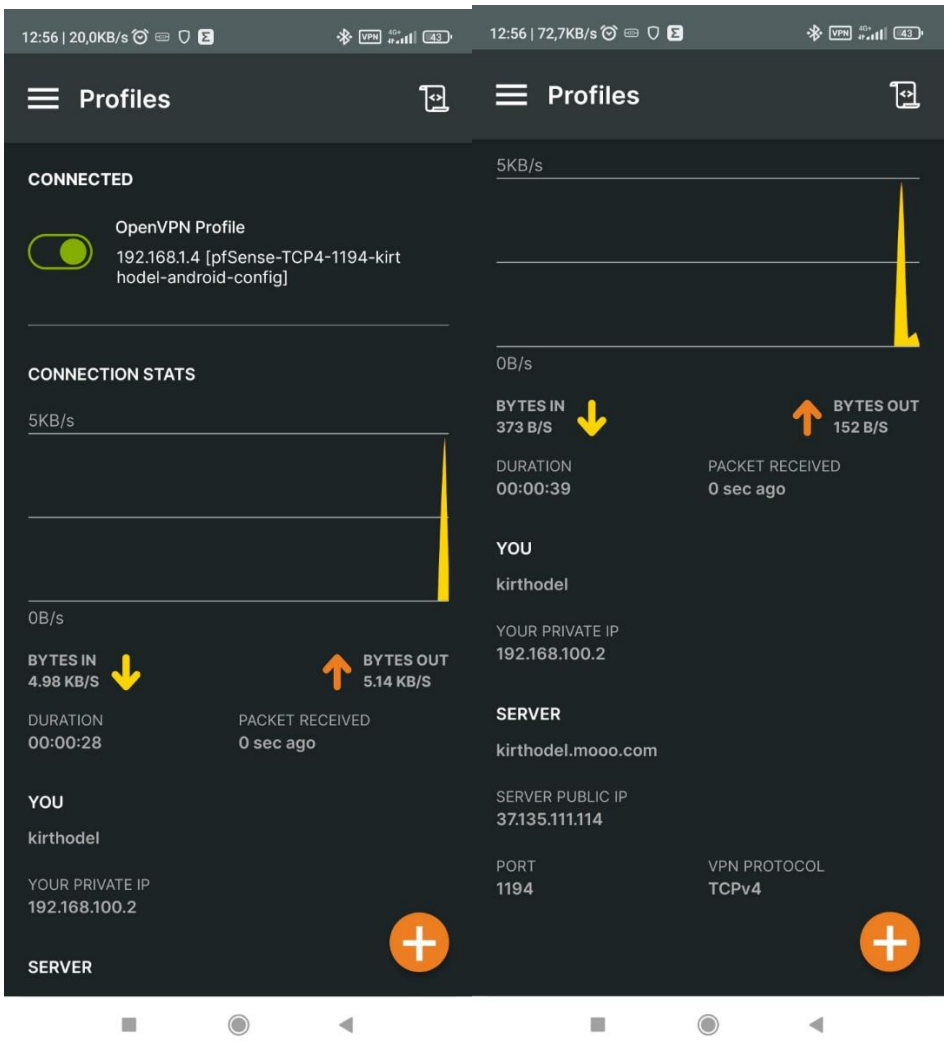


Figura 177: Conexión del cliente OpenVPN

A continuación, se verifica que el dispositivo está utilizando Adguard Home, en este caso el dispositivo se llama kirthodel.vpnvillasegura y tiene la IP 192.168.100.2. Adicionalmente se verifica que el firewall DNS está filtrando y bloqueando peticiones:

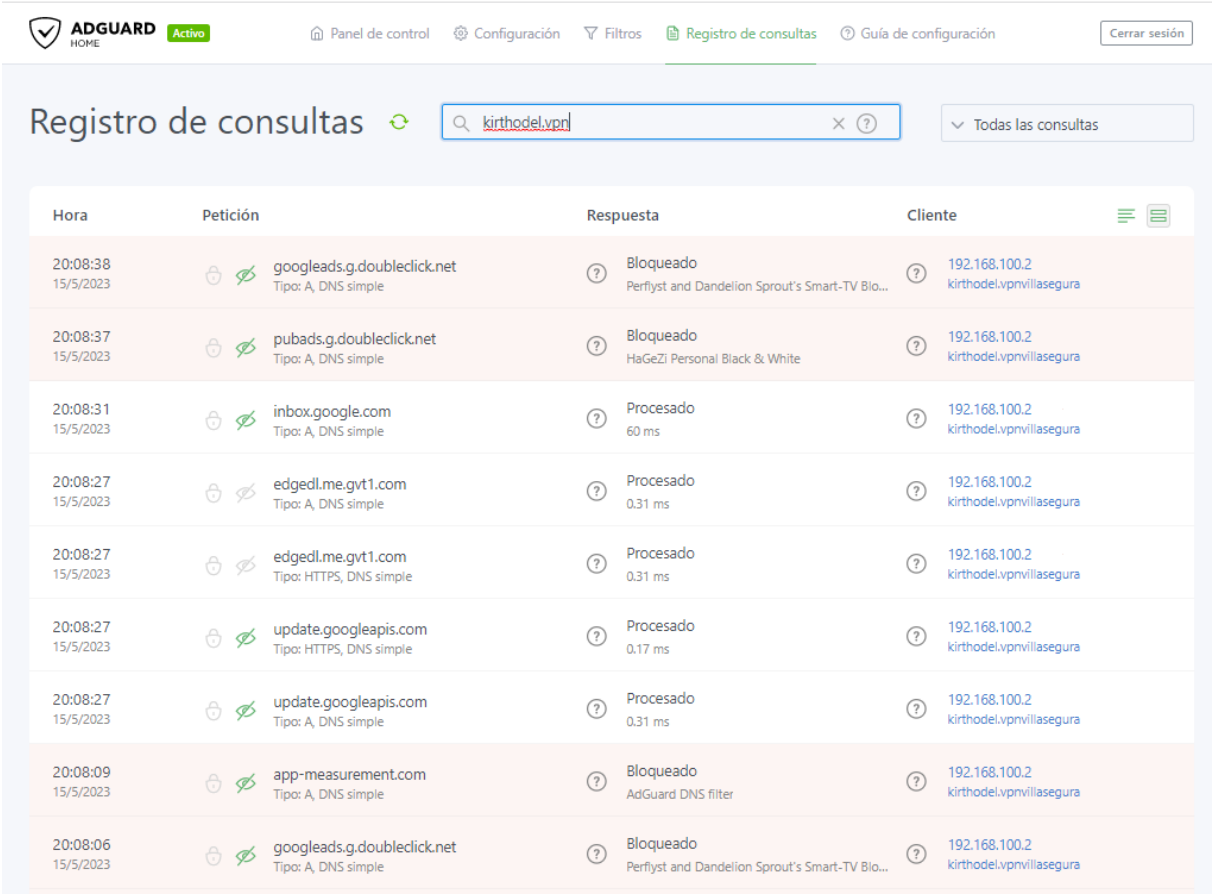


Figura 178: Conexión del cliente OpenVPN en logs de Adguard Home

Para terminar se verifica que hay visibilidad bidireccional con los dispositivos que se conectan con la red VPN:

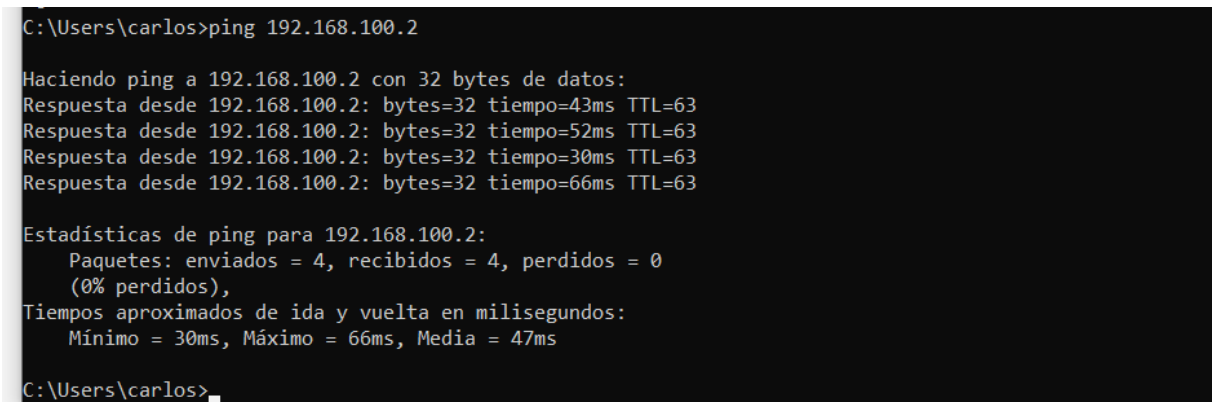


Figura 179: Verificación de visibilidad entre red local y VPN.

xii. Anexo XII: Configuración del portal cautivo

Para configurar un portal cautivo en pfSense basta con acceder a Services->Captive Portal en la GUI de pfSense y pulsar Add.

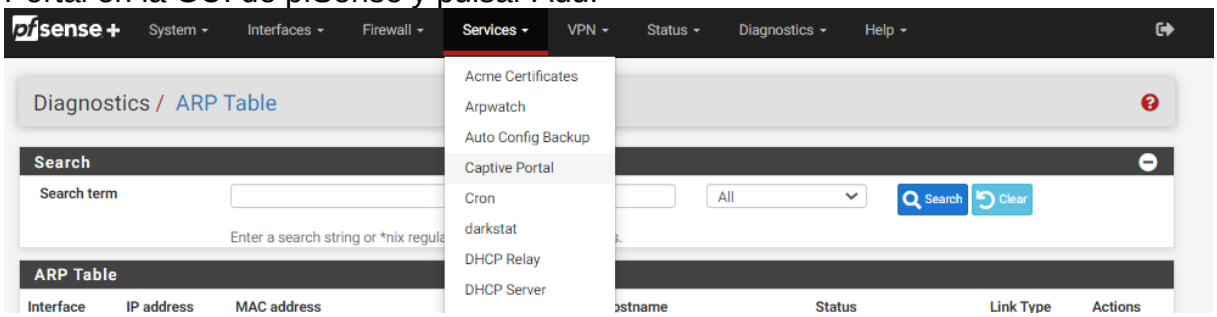


Figura 180: Acceso a la configuración del portal cautivo en pfSense.

A continuación se configuran las redes que requerirán al portal cautivo y los parámetros de configuración como en la imagen que muestra a continuación.

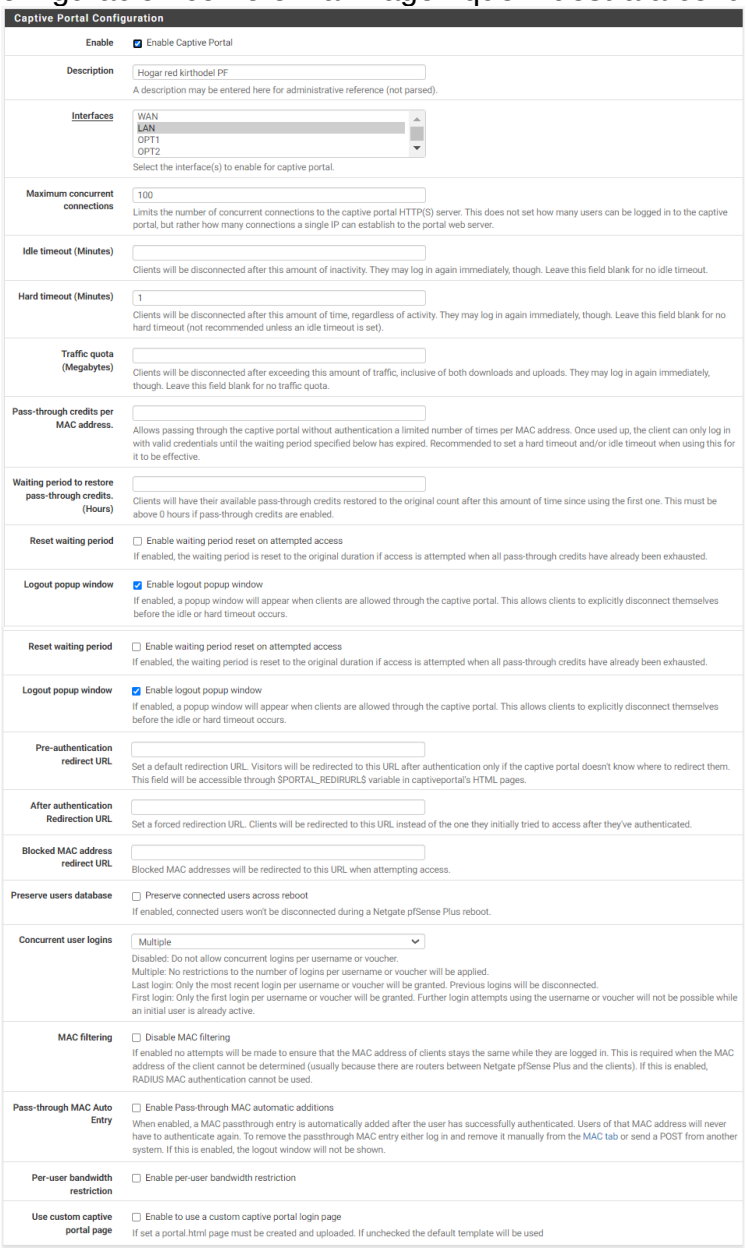


Figura 181: Parámetros de configuración del portal cautivo implantado (I)

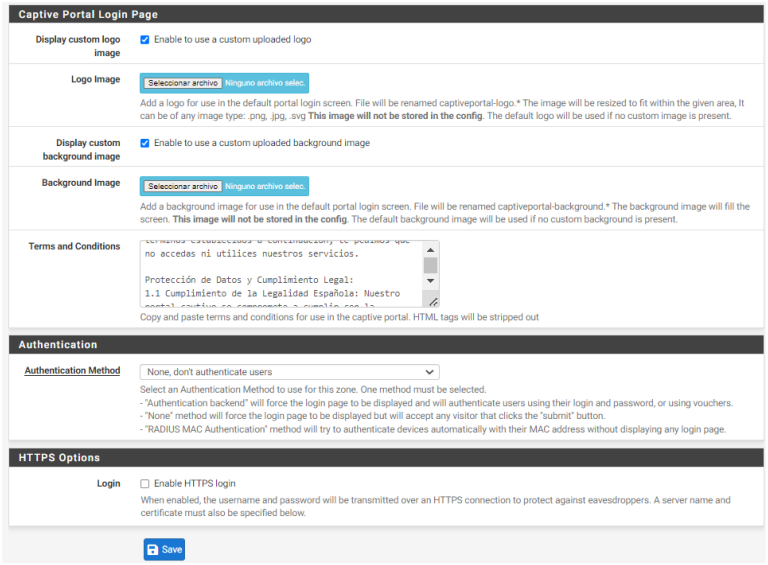


Figura 182: Parámetros de configuración del portal cautivo implantado (II)

Tras configurarlo se pulsa ‘save’ y se verifica el correcto funcionamiento.

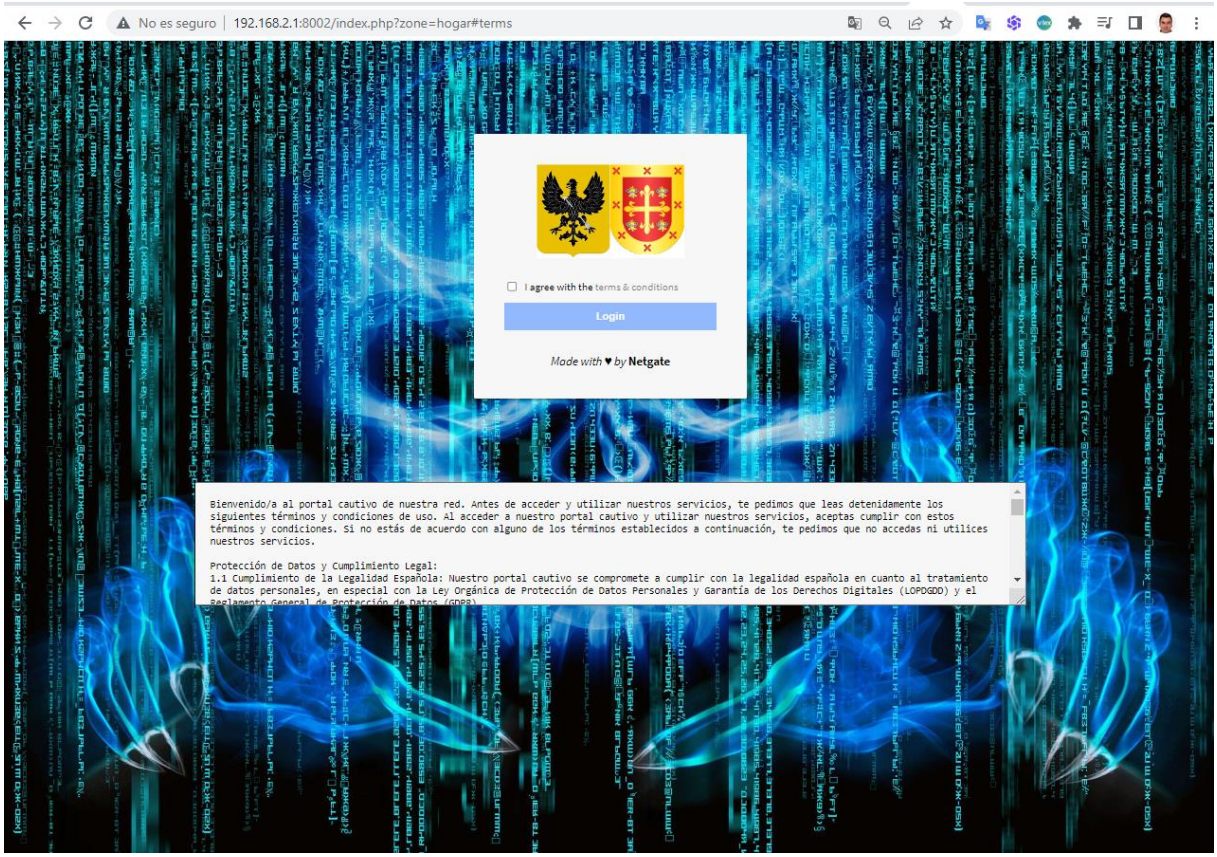


Figura 183: Aspecto del portal cautivo implantado.