UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
CAMPUS D'ALCOI

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Politécnica Superior de Alcoy

Next Generation Firewalls

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Ochoa Donate, Santiago

Tutor/a: Llinares Llopis, Raúl

Cotutor/a externo: VAELLO REIG, DAVID

CURSO ACADÉMICO: 2022/2023

Resumen castellano

En este proyecto se detallan los servicios ofrecidos por dispositivos NGFW (Next Generation Firewalls), un elemento de red capaz de monitorizar, analizar y mitigar ciberataques. Comercialmente, estos dispositivos son conocidos como UTM (Unified Threat Management) denotando que son sistemas de tratamiento de amenazas de forma unificada. Se estudiarán los servicios proporcionados por estos dispositivos, realizando especial hincapié en: AntiVirus, URL Filtering e IPS (Intrusion Protection System).

El TFG se basará en dos dispositivos NGFW de dos fabricantes diferentes: FortiGate y Hillstone. Mediante una serie de programas, principalmente herramientas de ataques, se diseñarán y ejecutarán una serie de pruebas sobre estos dispositivos, estudiando el proceso de detección por parte de los NGFW y la mitigación de los ataques / problemas planteados. Se analizarán los tiempos de respuesta y las acciones llevadas a cabo por parte de cada uno de ambos NGFW.

Palabras claves: Firewall, FortiGate, Hillstone, ciber-ataques, NGFW

Summary English

This project details the services offered by NGFW (Next Generation Firewalls) devices, a network element capable of monitoring, analyzing and mitigating cyberattacks. Commercially, these devices are known as UTM (Unified Threat Management) denoting that they are unified threat treatment systems. The services provided by these devices will be studied, placing special emphasis on: AntiVirus, URL Filtering and IPS (Intrusion Protection System).

The TFG will be based on two NGFW devices from two different manufacturers: FortiGate and Hillstone. Through a series of programs, mainly attack tools, a series of tests will be designed and executed on these devices, studying the detection process by the NGFW and the mitigation of the attacks / problems raised. The response times and the actions carried out by each of the two NGFWs will be analyzed.

Key words: Firewall, FortiGate, Hillstone, cyber- attack, NGFW

Contenido

Índice Figuras

1. Introducción

1.1 Entorno del proyecto

El proyecto se desarrollará durante **periodo de prácticas en una empresa de telecomunicaciones** dedicada a diseño gestión de ISP. Esta empresa es distribuidora de diferentes tipos de firewalls además de su posterior mantenimiento. Mediante **hardware real de la empresa se pretende poner a prueba las herramientas de defensa de dos diferentes firewalls**

1.2 Objetivo Principal

El principal objetivo de este proyecto **es realizar una comparativa entre 2 firewalls NGFW reales de diferentes fabricantes para comprobar las capacidades de estos y adecuarlas a las necesidades de un cliente**, para ello se necesita **recopilar información acerca de la resolución/mitigación de estos ataques,** mediante las diferentes pruebas realizadas que caerán sobre cada módulo de defensa que disponen los diferentes firewalls de sus respectivos fabricantes. Sobre estas herramientas se pretenden explotar sus capacidades de configuración y entender las opciones que ofrecen, además de diferentes pruebas para ver sus respectivas acciones a tomar

1.3 Justificación del proyecto

Este proyecto tiene la **necesidad** de llevar a cabo un **proceso de análisis** con el fin de ampliar el **conocimiento en ciberseguridad** para una mejor adaptación/satisfacción del dispositivo a **elegir** para determinado **cliente** ante la **exposición/demanda de lo que necesita**. Esto se logra llevando a cabo una **variedad de ataques para la "puesta a punto"** de los módulos de seguridad de los firewalls, evaluando tanto lo que han sido capaces de detectar y tomar acción y de lo que no han sido capaces.

1.4 Estructura del proyecto

Este proyecto consta de 5 puntos;

- El **primer punto**, la introducción se tiene una breve explicación de lo que tratara el proyecto hablando sobre el objetivo de este y su puesta en escena
- El **segundo punto**, los fundamentos teóricos, explicándose en detalle los casos de ataques a comprobar en la parte práctica para el entendimiento sobre que atacan y cuál es la parte encargada de analizarlo
- El **tercer punto**, la implementación practica podrá verse la puesta a punto de los equipos con sus respectivas pruebas y resultados, teniendo una explicación de lo utilizado para cada punto
- En el **cuarto punto**, la conclusión donde se tendrá una opinión respecto a lo comprobado y visualizado. Futuras líneas de trabajo
- En el **punto cinco**, la bibliografía de donde se ha sacado la información

2 Fundamentos teóricos

2.1 Firewall

El concepto básico de firewall es el del equipo o uno de los equipos principalmente encargados del **control del tráfico y de la seguridad** de la red a través de políticas de acceso y comprobaciones sobre esta [14,13]

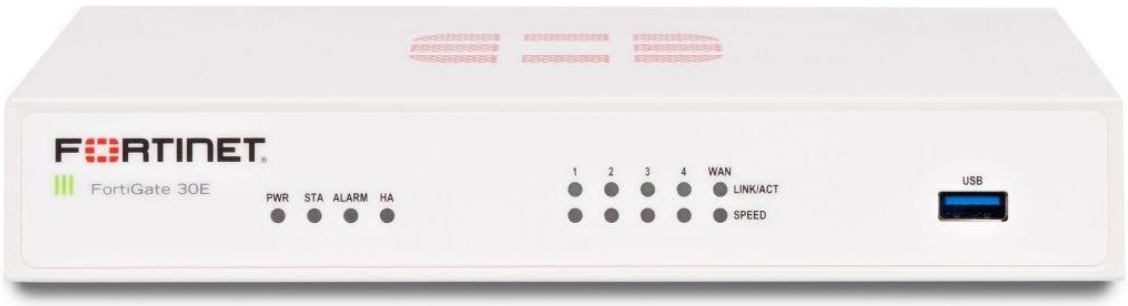


FIGURA 1. FIREWALL FORTIGATE

FIGURA 2. FIREWALL HILSLTONE

Los **firewalls** controlan el **flujo de la red**, es decir, se encargan de decidir que tráfico se **admite y que tráfico se considera peligroso** y se procede a su toma de acciones, el objetivo de estos firewalls no deja de ser otro que la de de **proteger a los equipos de red**. Para ello, implementan un **conjunto de reglas y políticas configurables**, que actúan como filtros y mecanismos de inspección para determinar la legitimidad y la seguridad del tráfico y los más “novedosos” o ”especializados” son aquellos que no solo tienen las herramientas mencionadas si no que son **capaz de configurarlas a mayor nivel de las necesidades requerida y realizan una inspección más a fondo a través de técnicas más avanzadas** [14,13]

Una vez entendido el concepto general de firewall cabe distinguir en firewall UTM y firewall Next Generations Firewall (NGFW)

2.1.1 Firewalls UTM y NGFW

2.1.1.1 UTM

UTM significa **gestión unificada de amenazas** como su propio nombre parece indicar habla de un sistema el cual de forma unificada se encarga de manejar la protección de la red, la **mitigación de las amenazas y la administración de estas mismas a través de unas "herramientas"** que se encargan de esas amenazas [18]

- Antivirus
- sistema de detección de intrusos
- Sistema de prevención de intrusiones
- Filtrados de URL
- VPN

2.1.1.2 NGFW

El entendimiento de los firewalls NGFW podría verse en su especificación a la hora de tratar **amenazas más concretas** viéndose como un "UTM" pero con "herramientas" **más personalizables y obtener una solución que se adapte a las necesidades requeridas**, los firewalls NGFW básicamente tratan de ser más precisos y abarcar más las amenazas a través de inspecciones profundas de paquetes como algoritmos de aprendizaje automático [18]

2.2 Módulo Antivirus (AV)

Un **antivirus** se trata de un **Software especializado en asegurar y prevenir los dispositivos** ante distintos tipos de amenazas a través del **análisis y el bloqueo/eliminación** de estas amenazas llamadas **Malware** tras ser catalogados como **potencialmente peligrosos**

A través de una variedad de formas de resolver esto como pueden ser: mediante comprobación de firmas, análisis de comportamiento o autoaprendizaje

Cabe destacar que existen muchos y diferentes tipos de malware con diferentes propósitos y métodos de acción. Además de malware más especializado nombrado como APT que son malware de amenaza persistentes, los cuales intentan evitar los sistemas de seguridad, para ello se emplean mecanismos como EDR (EndPoint Detection and Response)

2.2.1 Malware

Un malware es la palabra que hace referencia a software que en su ejecución tiene intenciones maliciosas [20]

El objetivo que estos suelen tener está relacionado con el **deterioro** y **manipulación** del equipo ya sea para obtener datos u apropiarse del dispositivo, extorsión, dañar la reputación o interrupción del equipo y espionaje, etc…

Este puede presentarse en diversas formas como:

- Virus
- Gusanos
- Troyanos
- Ransomware
- Spyware
- Adware
- Rootkits

El cómo estos malware se propagan puede variar desde distribución a través de archivos adjuntos hasta la explotación de vulnerabilidades en software o el propio sistema

2.2.2 FortiGate (AV)

FortiGate emplea un conjunto de **tecnologías integradas** con el propósito de ofrecer protección contra amenazas **conocidas y desconocidas**, incluyendo amenazas persistentes como los **APT** (Advanced Persistent Threats). [5]

El sistema de Antivirus (AV) utiliza una **base de datos de firmas** para llevar a cabo la **detección** de virus durante la **inspección del tráfico** de red que está sujeto al perfil de seguridad correspondiente.

Se debe activar la característica de Antivirus

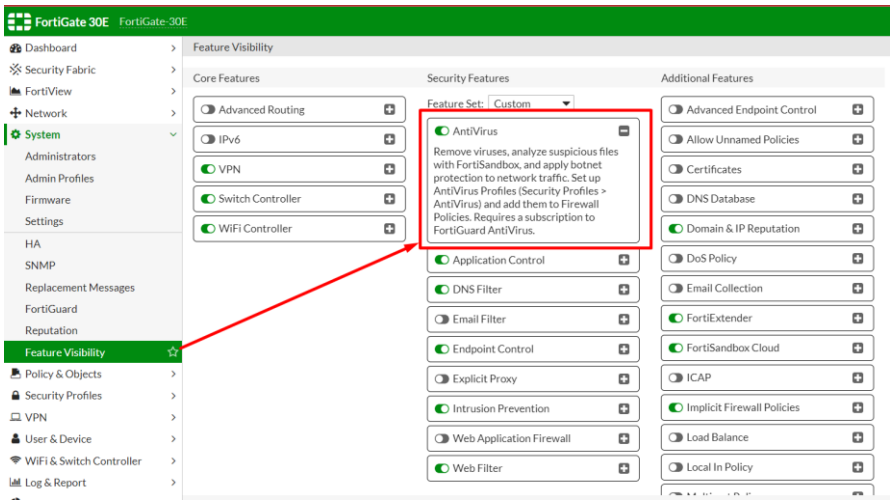


FIGURA 3. VENTANA ACTIVAR FUNCIÓN AV

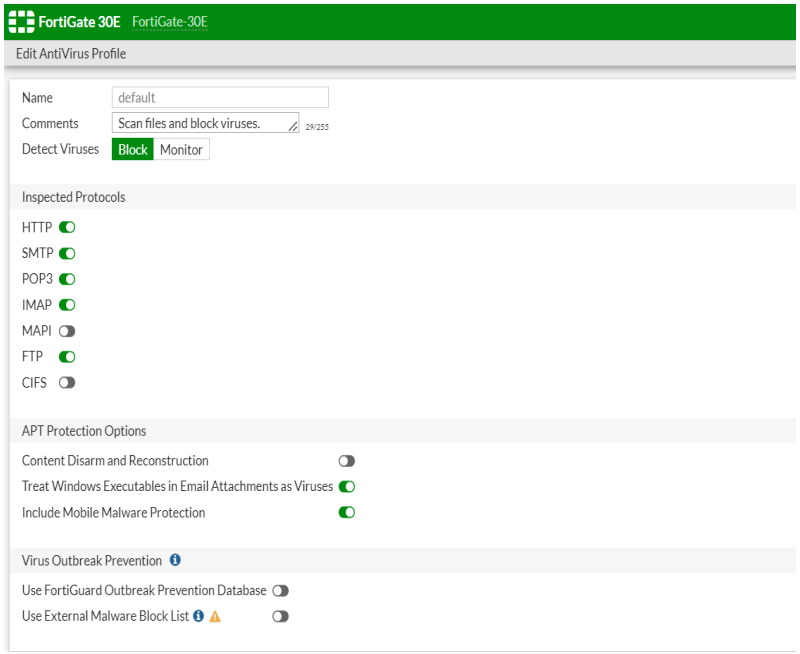


FIGURA 4. VENTANA CONFIGURACIÓN AV FORTIGATE

2.2.3 Hillstone (AV)

Hillstone proporciona una **Protección y detección avanzada** donde dispone de mecanismos para proporcionar detección **y protección en tiempo real durante todo el espectro de ataques de red y malware**

Las funcionalidades de las que se dispone en el módulo de antivirus son: [15]

- Actualizaciones manuales, automáticas, mediante empuje o extracción.
- Agregar o eliminar manualmente firmas MD5 de la base de datos del antivirus.
- Soporte de firma MD5 para cargar en el sandbox en la nube y agregar o eliminar manualmente en la base de datos local.
- Antivirus basado en flujo: los protocolos incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB.
- **Escaneo de virus en archivos comprimidos**

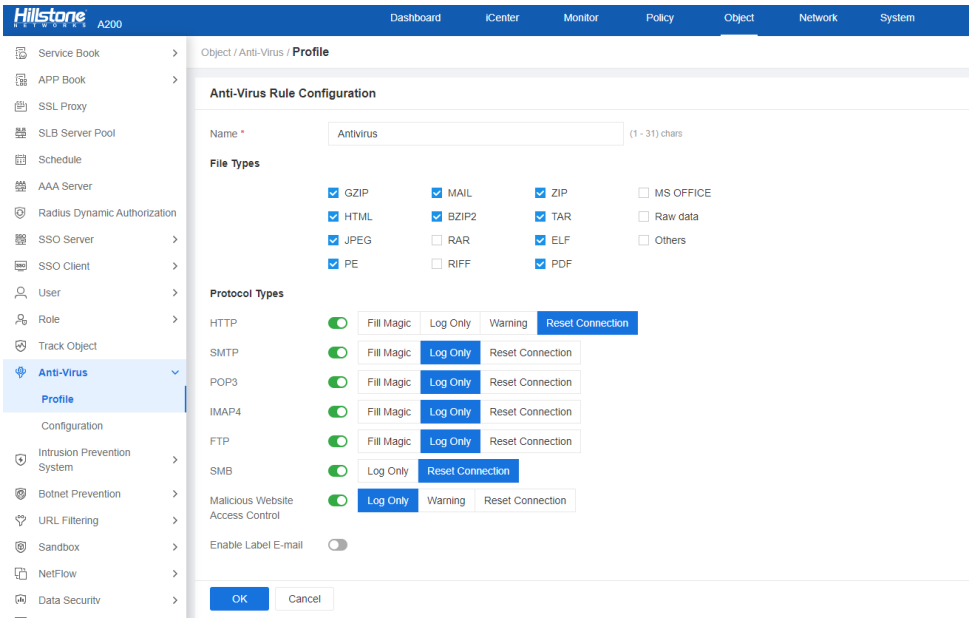


FIGURA 5. VENTANA CONFIGURACIÓN AV HILLSTONE

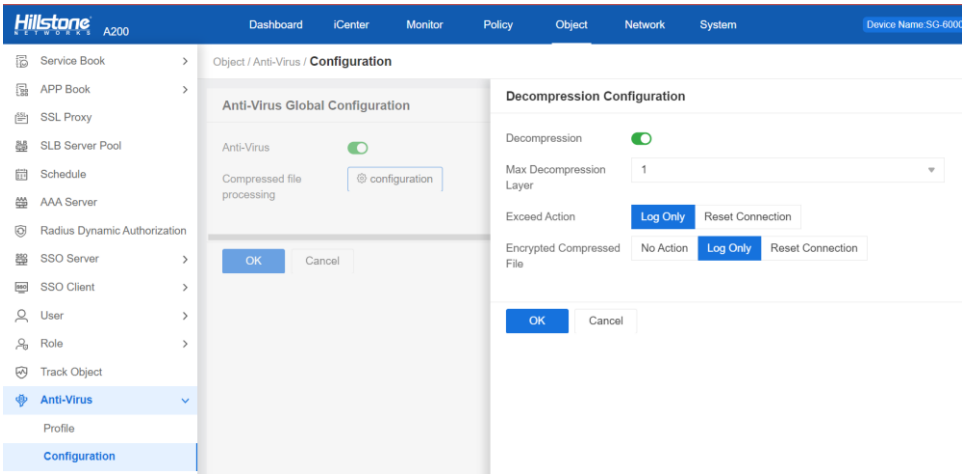


FIGURA 6. CONFIGURACIÓN ANÁLISIS COMPRIMIDOS HILLSTONE

2.3 Módulo IDS/IPS

2.3.1 IDS

Un **Sistema de detección de Intrusos** (IDS) es una aplicación diseñada para **detectar y alertar** sobre **accesos no autorizados** a dispositivos o redes. Su función principal es **monitorear el tráfico entrante y compararlo con una base de datos de firmas**, notificando al administrador en caso de encontrar discrepancias. [1]

Es importante destacar que los sistemas de detección de intrusos no llevan a cabo **ninguna acción o mitigación directa sobre el tráfico identificado como "dudoso"**. Su propósito se limita a la notificación de posibles intrusiones. En caso de requerir una acción o mitigación efectiva, será necesario considerar la complementación de otro sistema o enfoque apropiado.

2.3.2 IPS

Un **Sistema de Prevención de Intrusiones** (IPS) se utiliza con el propósito de **salvaguardar los sistemas contra ataques e intrusiones**. Su enfoque principal es llevar a cabo un control en **tiempo real** para **analizar** las **conexiones** y los **protocolos** utilizados. Además, el IPS identifica ataques mediante la **detección de patrones** específicos o anomalías en el tráfico. [1]

2.3.3 IPS/IDS

Estos sistemas, debido a su complementariedad y capacidad de sinergia, suelen ser implementados y utilizados de manera conjunta para realizar un análisis exhaustivo y una actuación eficaz sobre la red. Al trabajar en conjunto, se **potencian mutuamente y permiten una mayor protección y respuesta frente a amenazas y ataques**

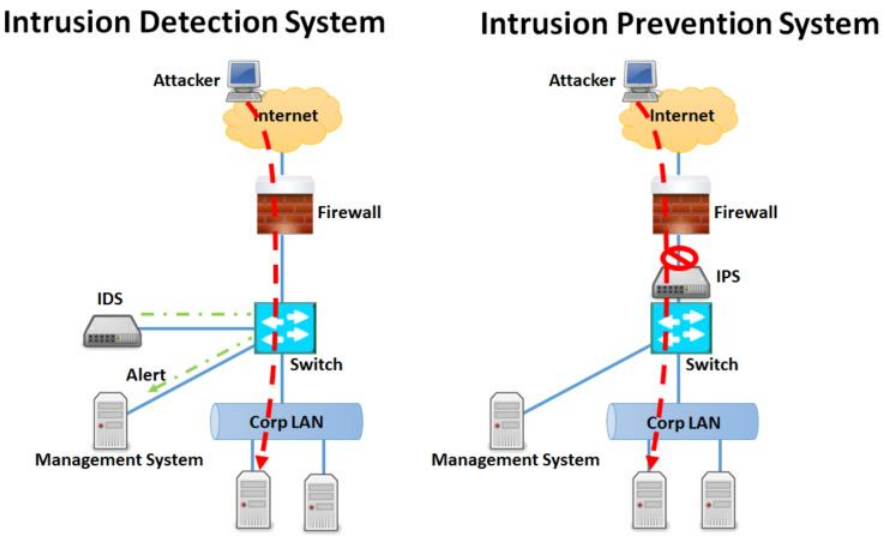


FIGURA 7. DIFERENCIAS ACTUACIÓN IDS/IPS

2.3.4 FortiGate (IDS/IPS)

El uso de un Sistema de Prevención de Intrusiones (IPS) **impulsado por Inteligencia Artificial/Aprendizaje Automático** (IA/ML) brinda una protección en **tiempo real** al proporcionar miles de reglas para prevenir **intrusiones** y llevar a cabo **bloqueos** tanto de **amenazas conocidas como de día cero**. [11]

FortiGate, a través de perfiles de seguridad de IPS, garantiza la seguridad mediante la detección y prevención de intrusiones, utilizando dos técnicas principales:

1. **Detección basada en firmas**: Esta técnica implica buscar firmas específicas en el tráfico utilizando **decodificadores de protocolo**. De esta manera, los ataques dirigidos a un protocolo en particular se pueden **identificar buscando la firma del ataque en el tráfico correspondiente**. Las firmas de detección se pueden clasificar en tres formas:
    a. **Basada en patrones**: Se seleccionan atributos relacionados con el ataque para identificarlo.
    b. **Basada en puntuación**: En la base de datos de firmas, algunas tienen una opción asociada de "Monitor". Solo se consideran una amenaza si se detectan en grupo.
    c. **Personalizadas**: Estas firmas se escriben manualmente para adaptarse a amenazas específicas.

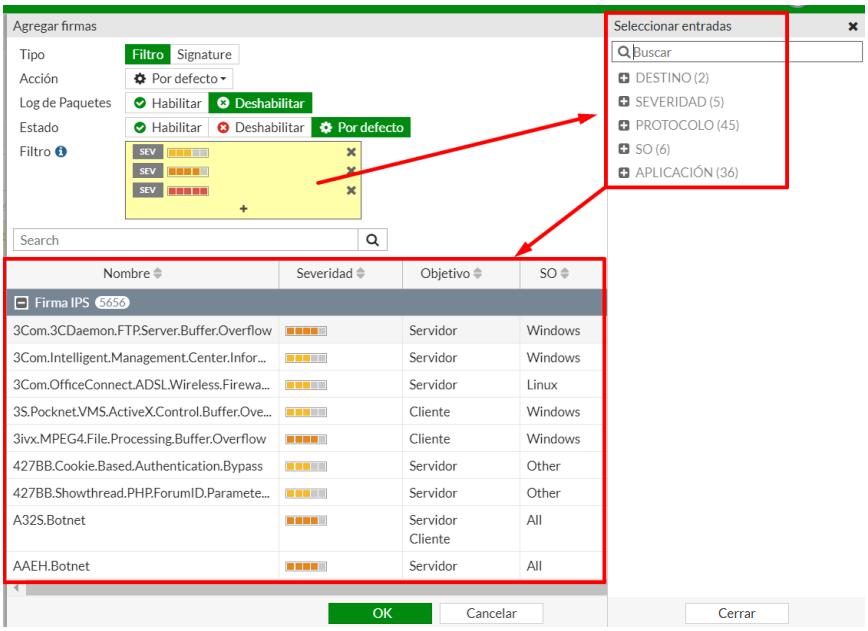


FIGURA 8. VENTANA FIRMAS DE TIPOS DE ATAQUES CONOCIDOS

2. **Detección basada en anomalías**: Esta técnica implica **monitorear y analizar el tráfico** en busca de **comportamientos inusuales o anómalos** que podrían

indicar una intrusión. Mediante el **aprendizaje automático**, el sistema puede **identificar patrones de tráfico anómalos y generar alertas** en tiempo real.

Las opciones que te brinda la posibilidad de ejercer sobre el tráfico analizado son las siguientes:

- **Pass**: Al seleccionar esta opción, el tráfico será permitido sin ningún tipo de intervención o limitación.
- **Monitor**: permitir el tráfico, se registra detalladamente todo lo que ocurre en relación con el mismo. Esto implica que se realiza un seguimiento exhaustivo de todas las actividades y eventos asociados con el tráfico analizado.
- **Block**: Impide que cualquier comunicación proveniente de la fuente del tráfico seleccionado pueda acceder a los recursos o sistemas destino.
- **Reset**: cerrar la sesión activa y se restauran los valores y configuraciones predeterminados. Esta opción resulta útil cuando se requiere finalizar y reiniciar todo el proceso de análisis y gestión del tráfico.
- **Quarantine**: rechazar y bloquear el tráfico proveniente de una determinada dirección IP de origen durante un período de tiempo específico. La duración de este tiempo puede ser configurada de acuerdo a las necesidades y políticas establecidas. Al aplicar la opción "Quarantine", se restringe el acceso del tráfico de esa IP en particular, evitando así posibles amenazas o actividades no deseadas durante el período establecido.

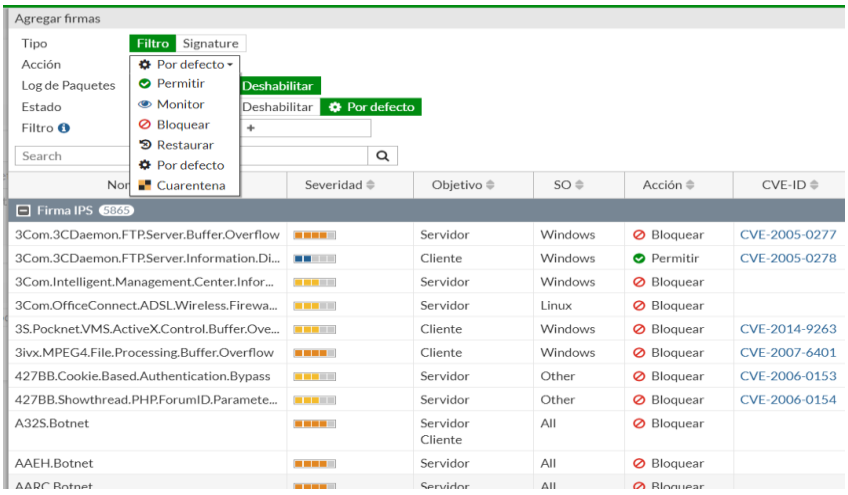


FIGURA 9. OPCIONES DE FILTRADO

2.3.5 Hillstone (IDS/IPS)

Incluye una tecnología para la detección y prevención de intrusiones **basada en comportamiento** (BIPS), que utiliza algoritmos de aprendizaje automático para detectar patrones de comportamiento malicioso.

Puede configurarse la política de seguridad, esta política de seguridad es esencial para la detección y bloqueo de los ataques, esta política de seguridad puede incluir la configuración del "comportamiento" a nivel de reglas de detección, las acciones de respuesta y excepciones

Estas son características de Hillstone para la **Prevención de intrusiones**: [15]

- Mas de 8.000 firmas
- Acciones IPS: Monitoreo, bloqueo, reinicio con tiempo de caducidad
- Selección de filtros: gravedad, destino, SO, aplicación o protocolo
- Excepciones de IP de formas de IPS
- Protección DoS ante inundaciones TCP Syn, escaneo puertos, paquetes fragmentados, barrido ICMP
- Modo husmeo IDS
- Bypass activo con interfaces

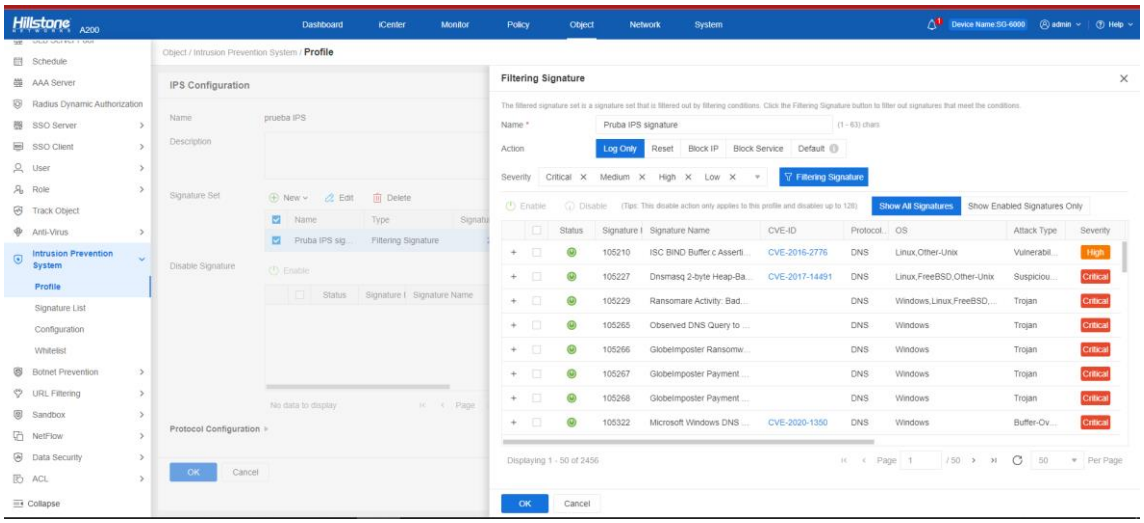


FIGURA 10. VENTANA CONFIGURACIÓN IPS Y FIRMAS HILLSTONE

2.4 Módulo IPR

IPR sin las siglas de **IP Reputation**

evaluación y clasificación de la confiabilidad y la calidad de una dirección **IP** específica en relación con su historial de **comportamiento en línea**. Se utiliza para determinar la **probabilidad** de que una dirección **IP** esté involucrada en **actividades maliciosas,** como el envío de spam, ataques cibernéticos o distribución de malware [4]

La reputación IP **tiene importancias significativas** en la gestión del correo electrónico, el filtrado de spam y la seguridad en línea. Una reputación IP de calidad es fundamental para **garantizar la entrega confiable de mensajes legítimos y prevenir la participación involuntaria en actividades maliciosas**

FIGURA 11. CONCEPTO REPUTACIÓN DE IP

2.4.1 Fortigate (IPR)

FortiGate usa **5 niveles de reputación**, aparte de poder definir niveles de reputación personalizados, puede configurarse políticas de firewalls para filtrar el tráfico según el nivel de reputación que se desea [7]

Los cinco niveles por defecto son:

1. Sitios maliciosos conocidos como sitios de phishing o sitios relacionados con servidores botnet
2. Sitios de servicios de alto riesgo, como TOR, proxy y P2P
3. Sitios no verificados
4. Sitios de redes sociales de buena reputación
5. Sitios seguros conocidos y verificados

Por **defecto** el **nivel** de reputación **configurado** en una **política** es **cero**, lo que dice que no está habilitada

Para una **IP** que **no está** en la base de datos de servicios de Internet el servicio **por defecto es 3**

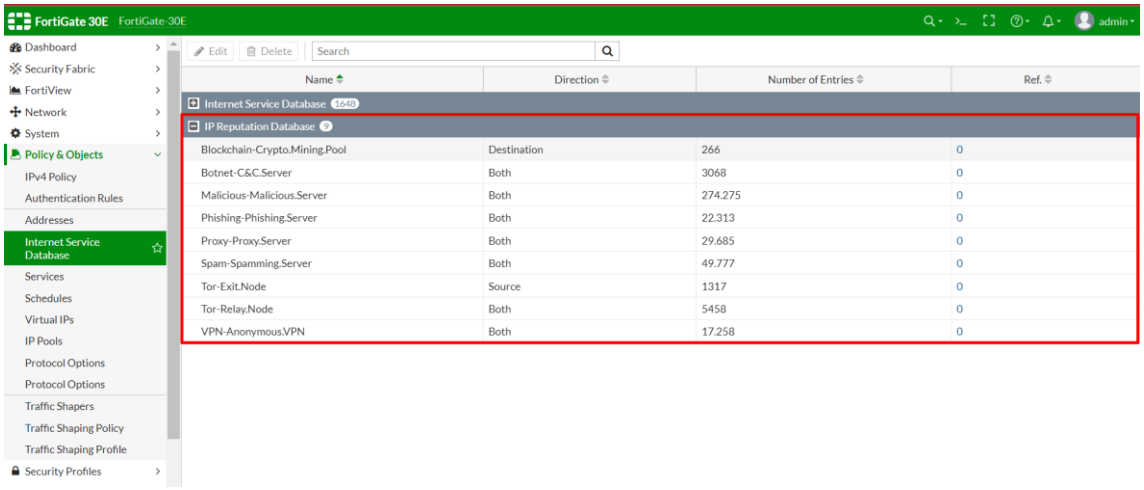


FIGURA 12. SUMMARY DE ENTRADAS DE IP MALICIOSAS POR CATEGORÍA

Para visualizar las direcciones IP que se han descargado de la base de datos de FortiGuard se debe abrir una de las 9 categorías y saldrán las IP asociadas a ella

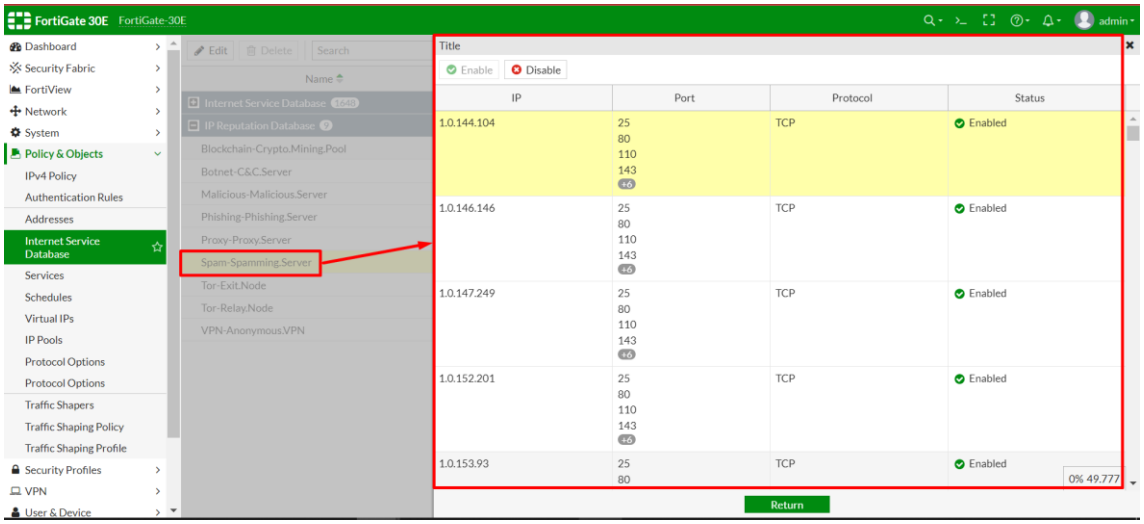


FIGURA 13. MUESTRA IP REGISTRADAS DE SPAM

2.4.2 Hillstone (IPR)

Hillstone utiliza un conjunto de técnicas para determinar la reputación de direcciones IP, incluyendo: [8]

- **Listas negras**: Base de datos actualizada con las IP que se identifican como sospechosas o maliciosas
- **Análisis de tráfico**: Monitorización del tráfico buscando "patron", es un análisis basado en el comportamiento que hace una ip
- **Análisis de reputación de dominios**: Análisis de los dominios que tienen una dirección IP, si se conoce que ha alojado malware o que es potencialmente sospechoso en algún aspecto se marcara como amenaza
- **Análisis de geolocalización**: puede filtrar por "lugares" lo que hace que si una dirección IP se encuentre en esa zona/región puede marcarse como amenaza

Las **reglas para el filtrado** de las Ip que pueden sacar de la **base de datos** que viene (puede ir actualizándose) se pueden aplicar en **global**, en una **zona** o en un "**virtual router**"

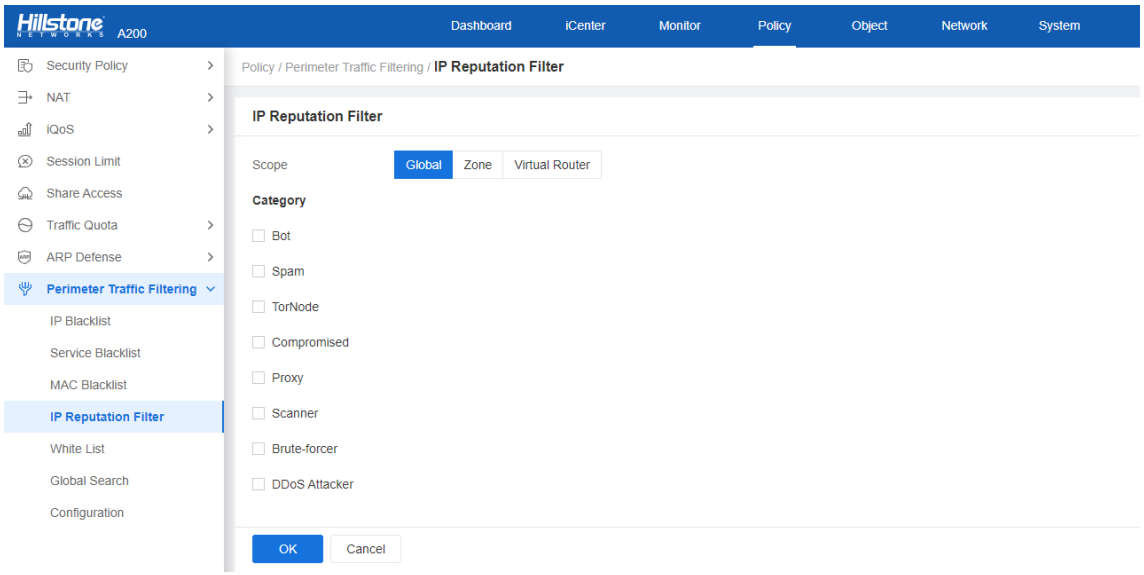


FIGURA 14. VENTANA CONFIGURACIÓN IPR HILLSTONE

2.5 Módulo URL filtering

El filtrado web, también conocido como filtrado de contenido web o filtrado de URL, es un proceso mediante el cual se controla y gestiona el acceso a sitios web y contenido en Internet con el objetivo de **garantizar la seguridad**, la **productividad** y el **cumplimiento de políticas** en entornos informáticos. [2,9]

El filtrado web se basa en una **serie de reglas y políticas establecidas** por una organización o entidad para determinar qué sitios web o categorías de contenido están **permitidos**, **bloqueados** o sujetos a un **monitoreo especial**.

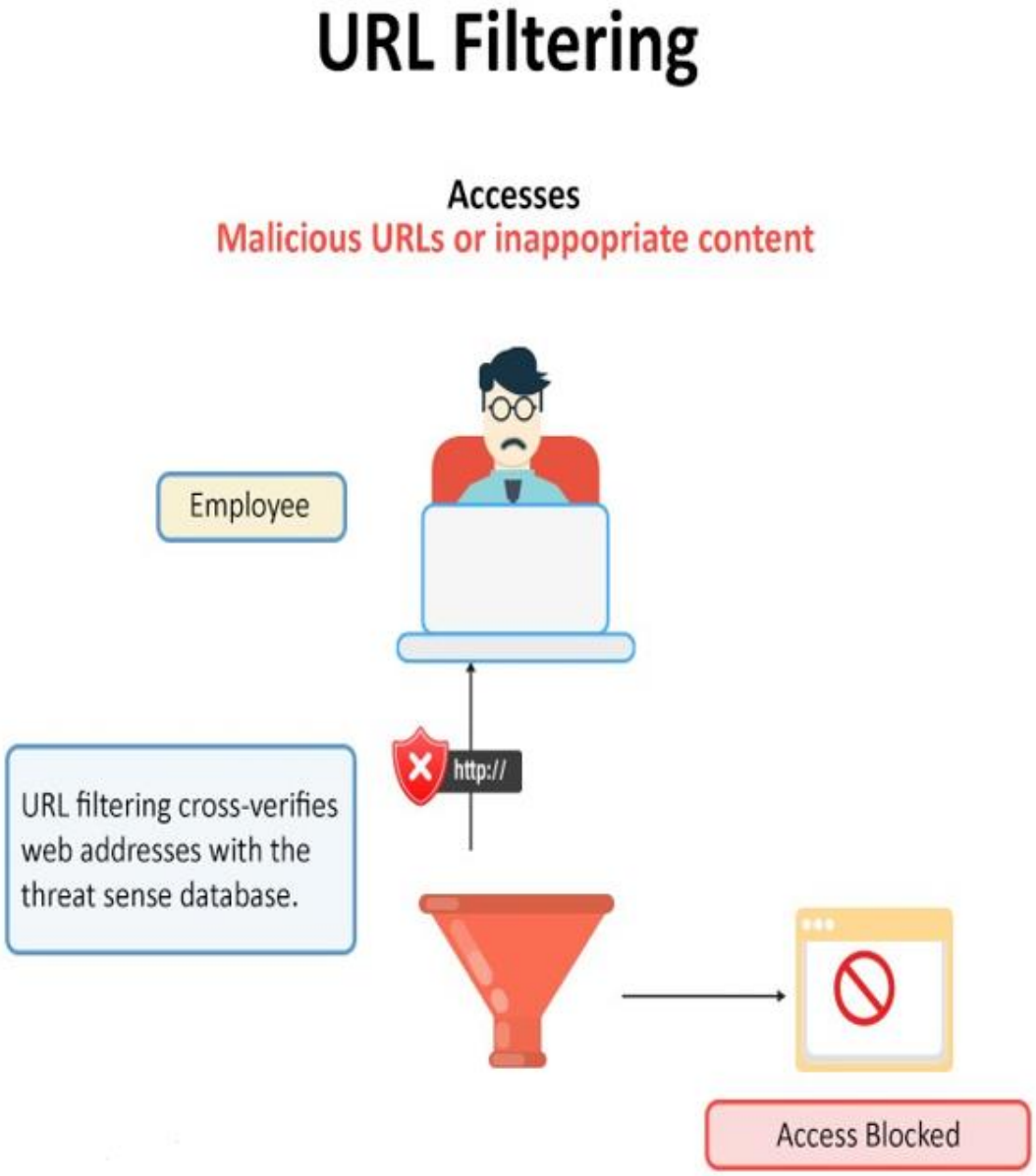


FIGURA 15. CONCEPTO BLOQUEO URL

2.5.1 Fortigate (URL Filtering)

URL Filtering filtra **peticiones HTTP**, existe un orden en el que la unidad NGFW FortiGate aplica los siguientes filtros y es: [5]

- Filtrado de UR
- Filtrado de contenido web
- Filtrado por categorías (si se dispone del servicio)

2.5.1.1 Filtrado de URL

Proceso mediante el direccionamiento de una URL se **permitirá** o **bloqueará** el acceso a determinadas páginas web o recursos

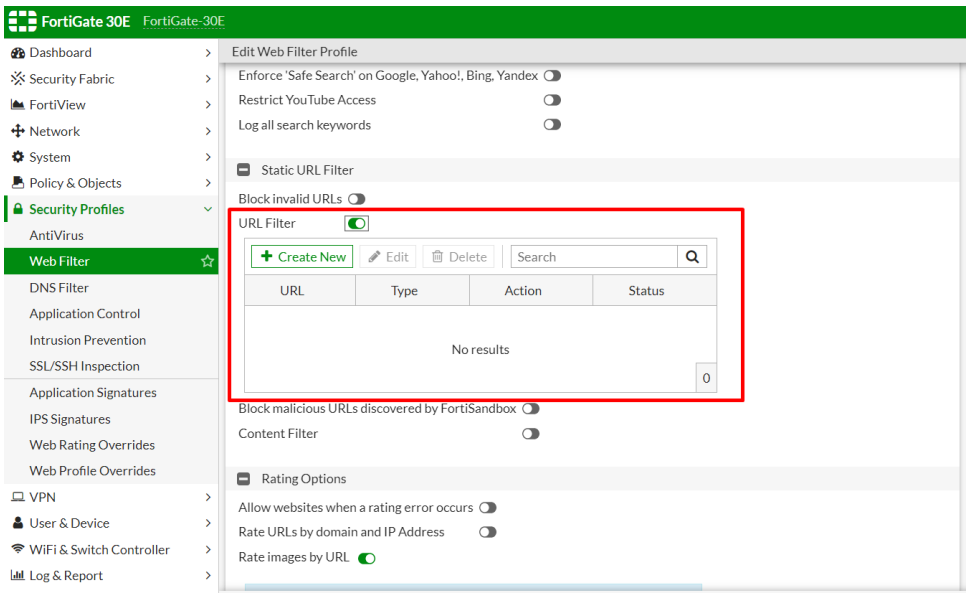


FIGURA 16. VENTANA CONFIGURACIÓN FILTRADO URL

2.5.1.2 Filtrado en función de la/as categoría/as

Método que **clasifica** y **organiza** las direcciones **URL** de sitios web en **diferentes categorías**, como redes sociales, entretenimiento, noticias, deportes, etc. Estas categorías se utilizan para **aplicar políticas de acceso y restricciones en función de las preferencias y necesidades** de los usuarios

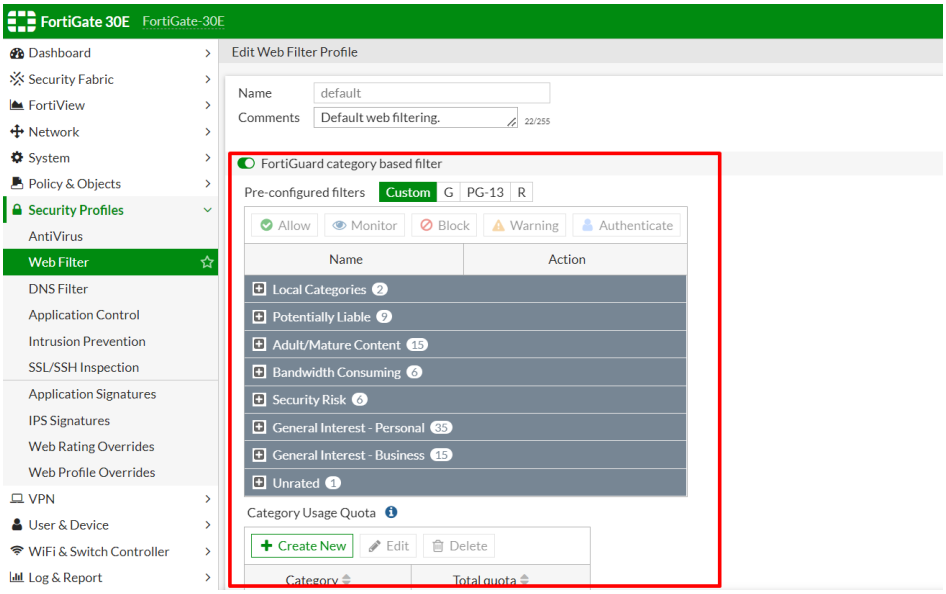


FIGURA 17. VENTANA CONFIGURACIÓN DE FILTRO POR CATEGORÍAS

2.5.1.3 Filtrado de Contenidos y Scripts web

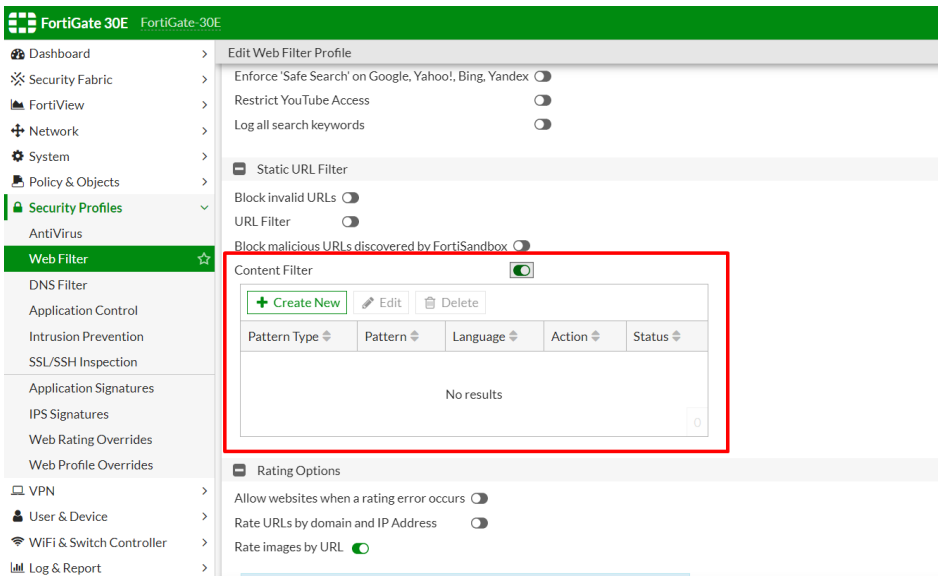


FIGURA 18. VENTANA CONFIGURACIÓN DE FILTRO POR CONTENIDO

Además de introducir direcciones URL, también es posible **utilizar patrones** que contengan **texto, comodines o expresiones regulares**.

Las acciones que se pueden llevar a cabo son las siguientes:

- **Permitir** (Allow): Al seleccionar esta opción, se permite el tráfico dirigido a la URL especificada y se continúa aplicando los demás perfiles de seguridad configurados.
- **Bloquear** (Block): Si se elige esta opción, se bloquea el tráfico dirigido a la URL indicada y se muestra un mensaje al usuario informando del bloqueo.
- **Monitorizar** (Monitor): Al seleccionar esta opción, se permite el tráfico dirigido a la URL especificada y se continúa aplicando los demás perfiles de seguridad. Además, se genera un mensaje en el registro de eventos para su seguimiento y registro.
- **Eximir** (Exempt): Al marcar esta opción, se exime la URL de todas las restricciones de seguridad. Esto implica que no se aplicarán perfiles de seguridad adicionales y se permitirá el tráfico en esa dirección.

En caso de bloquear y redirigir al usuario a una **página la cual le muestre un mensaje de porque ha sido bloqueado**

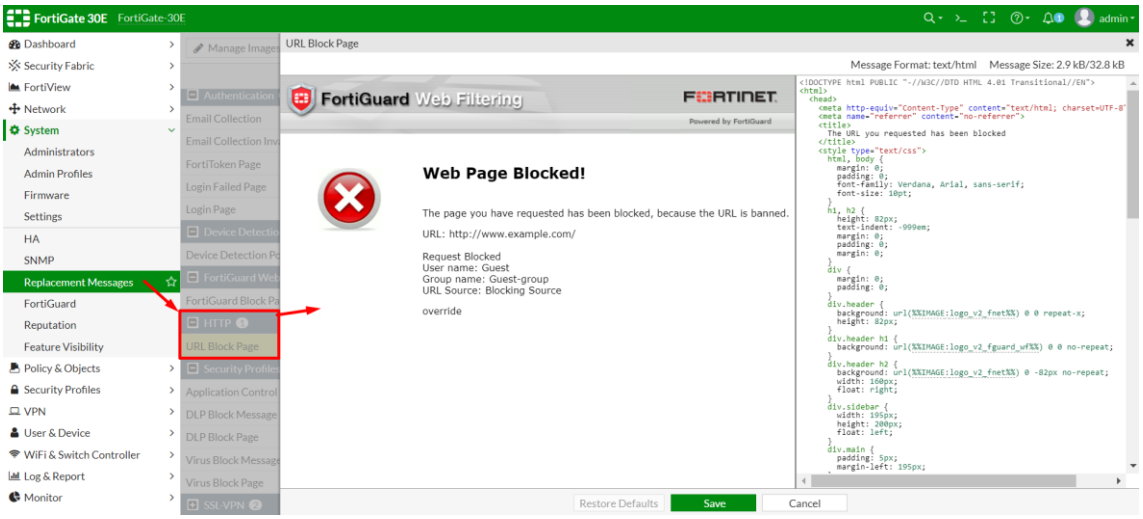


FIGURA 19. MUESTRA VENTANA DE MENSAJE DE BLOQUEO DE URL

2.5.2 Hillstone (URL Filtering)

Hillstone ofrece una base de datos **categorización de URL**, en tiempo real basado en la nube con mas de **140 millones de URL** y **64 categorias** de las cuales **8 son de seguridad**. [15]

Hillstone incluye una inspección profunda de paquetes, análisis de anomalías de protocolo y análisis de firmas para bloquear amenazas

Por resumir en el conjunto de técnicas pueden verse las siguientes: [15]

- **Listas negras de URL**: mediante esa base de datos o el administrador añadiendo las URL de sitios maliciosos o inapropiados se hará que cuando una URL coincida con la entrada de esta lista de bloque automáticamente, es decir, filtrara basándose en el flujo hacia el destino
- **Análisis de categorías de URL**: Hillstone como menciono permite filtrar por categorías
- **Análisis de contenido de la web**: Hillstone dispone de un mecanismo de identificación de coincidencias de "words" establecidas con contenido de la propia web para su posterior acción a tomar

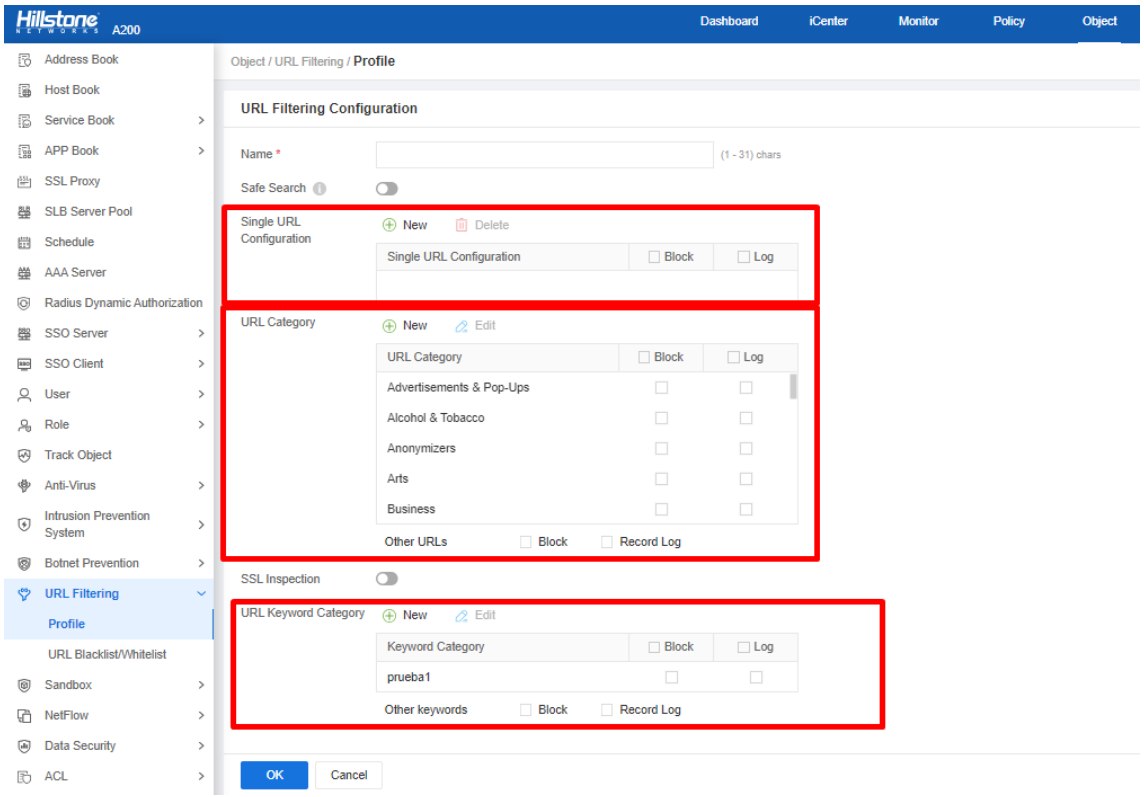


FIGURA 20. VENTANA CONFIGURACIÓN URL ESTÁTICA, CATEGORÍAS Y CONTENIDO HILLSTONE

2.6 C2

C2 software conocido como **comando y control** (C&C) está diseñado con el propósito de **establecer una conexión oculta entre un dispositivo comprometido y un servidor remoto** controlado por los atacantes. Este mecanismo de comunicación permite que **el dispositivo infectado**, a menudo **parte** de una **botnet**, **se convierta en un "bot" o nodo dentro de una red maliciosa**. [3]

Una **botnet** es una red de bots, donde cada **bot** representa un **dispositivo infectado que ha sido comprometido por el malware**. Estos dispositivos pueden incluir computadoras, servidores, dispositivos IoT (Internet de las cosas) u otros dispositivos conectados a la red. Una vez que un **dispositivo** se ha **unido** a la **botnet**, se convierte en un **recurso controlado por los atacantes** para llevar a cabo diversas actividades maliciosas.

El C&C malware se utiliza generalmente en ataques cibernéticos avanzados y sofisticados, como el espionaje, el robo de datos, la distribución de malware adicional, el lanzamiento de ataques distribuidos de denegación de servicio (DDoS) y otras actividades delictivas en línea

En un análisis más funcional este tipo de malware se basa en los siguientes elementos:

- Infección inicial
- Establecimiento de la comunicación
- Comunicación bidireccional
- Control remoto y actualizaciones

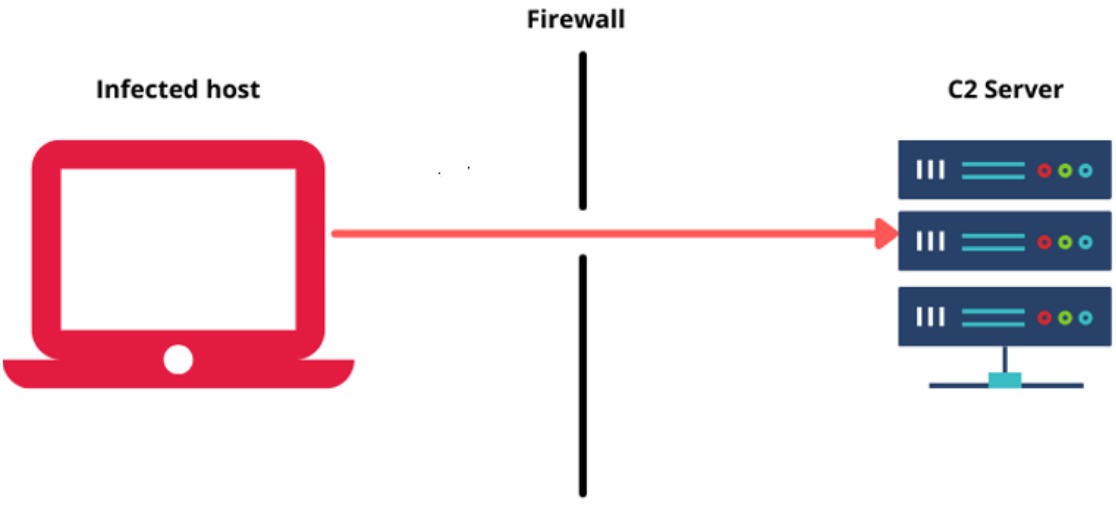


FIGURA 21. CONCEPTO COMMAND AND CONTROL

2.6.1 Fortigate (C2)

Fortigate consolida **varias opciones de botnet** en **una sola opción del perfil IPS**, así desde un solo lugar se puede habilitar el **bloqueo de botnet** a través de las políticas de tráfico [12]

En **FortiGate** puede verse que se **dispone de seguridad** ante **Botnet Ips y botnet Domains**

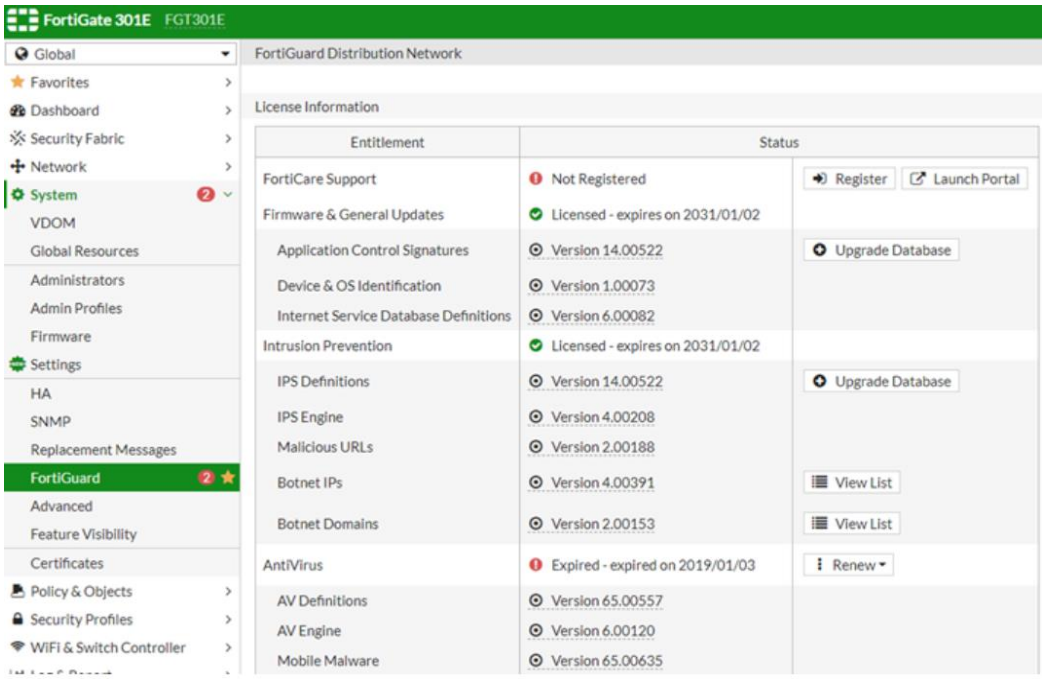


FIGURA 22. VISUALIZACIÓN DE SERVICIOS DISPONIBLES

Para el bloqueo de **direccionamiento IP** conocido que tratan de botnets

Ahora sobre el sensor de las políticas de firewalls se empezará a escanear las salidas a sitios de botnets

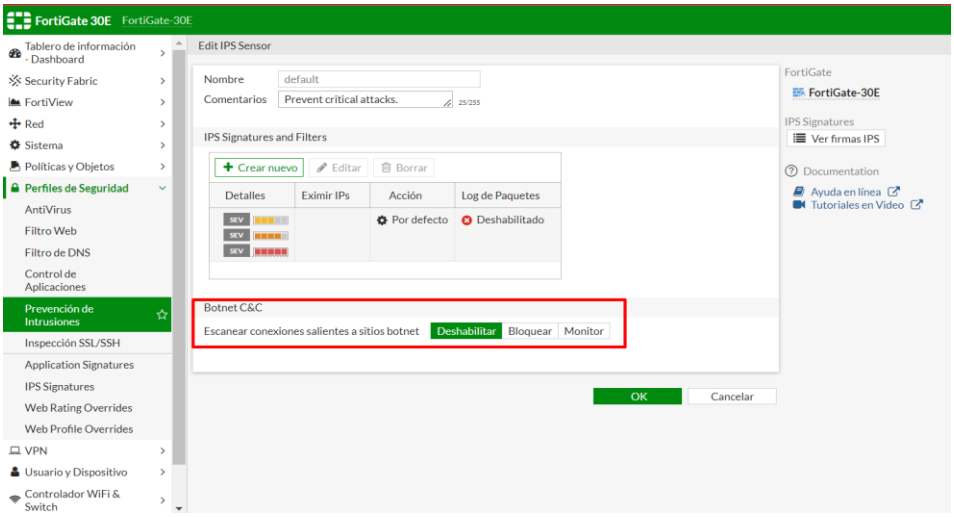


FIGURA 23. VENTANA DE CONFIGURACIÓN DE SALIDAS HACIA BOTNET

Para el **bloqueo de Dominios** de Botnet se tendrá una lista de dominios de botnet que se añadirán a la política del firewall para bloquear

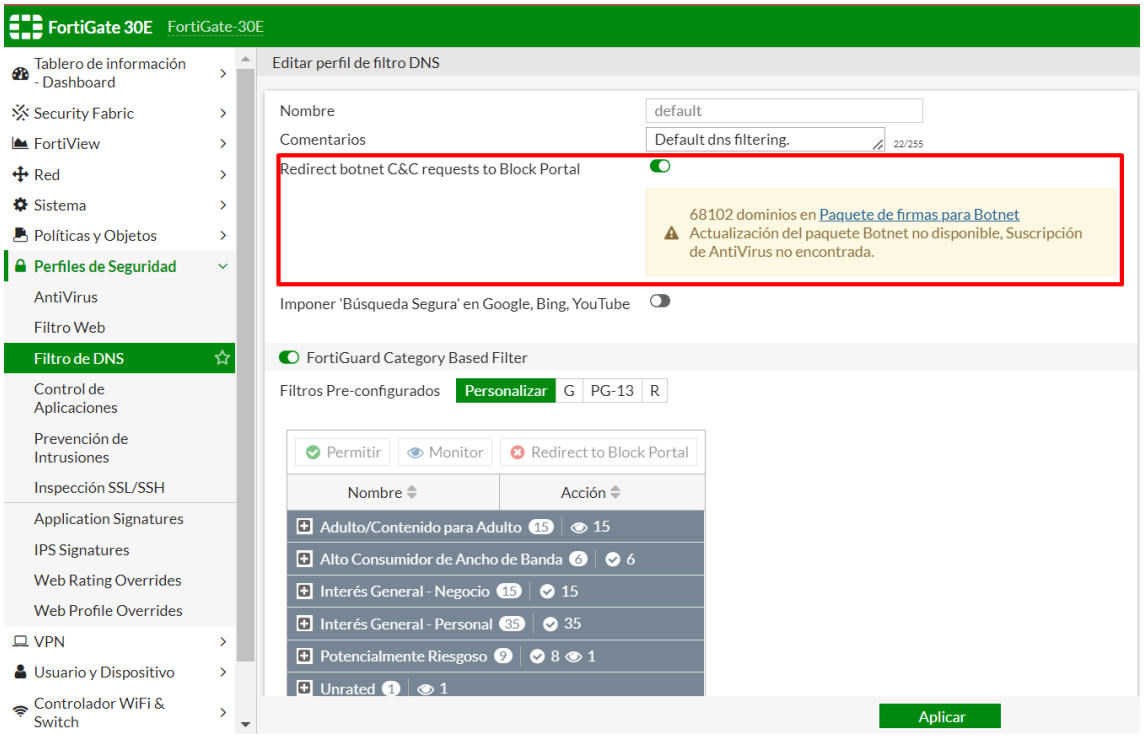


FIGURA 24. VENTANA CONFIGURACIÓN BOTNET DNS

Para **bloquear las "firmas"** en botnet se deberá incluir estas en el sensor de IPS.

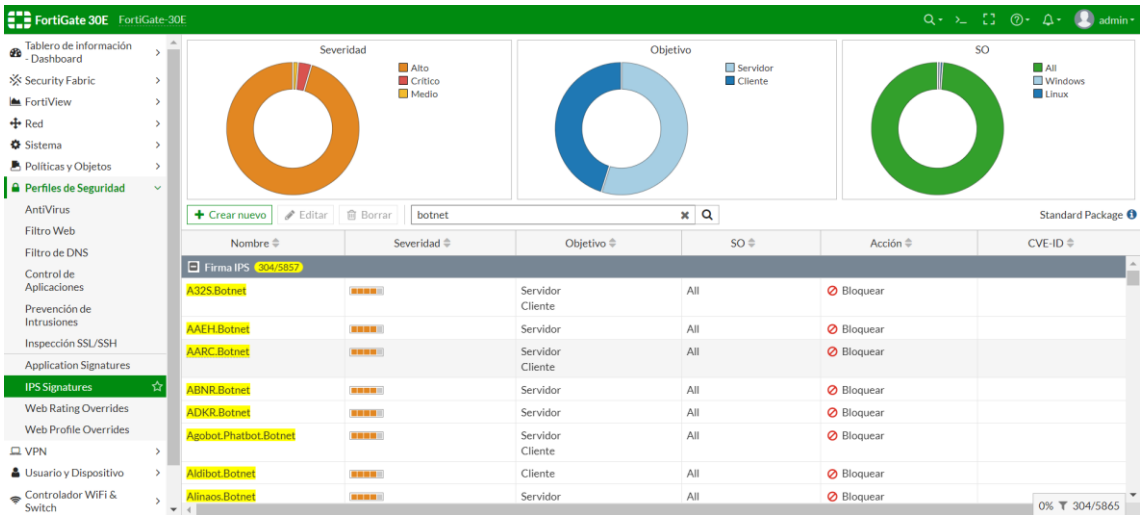


FIGURA 25. VISTA FIRMAS BOTNET

2.6.2 Hillstone (C2)

Los comandos de C2 (C&C) suelen emitirse a través de HTTP, DNS, Telnet o internet relay chat

Las mejoras que ofrece a través de la red son: [21]

- **Una robusta plataforma de centro de datos**, los administradores pueden proteger a través de la monitorización e interrupción de las conexiones de C2 desde L3 a L7
- **Mejora de la detección de los algoritmos de generación de dominios** (DGAs), a menudo los hosts que han sido infectados generan un pseudo nombre de dominio incluyendo nombres de servidores C2, esto lo detecta y previene este tipo de trafico
- **Una lista de acceso personalizada C2 de la red de botnets mejorada** hace que los administradores más fácilmente puedan bloquear las comunicaciones y también personalizar la lista de acceso para decidir que direcciones ip van a dejar pasar o nombres de dominio, todo gracias a una amplia base de datos de firmas
- **Mejora del soporte del túnel del DNS** desviando los mensajes de respuesta de DNS defectuosos a un lugar seguro para su posterior análisis, previniendo una conexión a destinos maliciosos
- **La detección avanzada de túneles DNS**, detección de intento de filtración de datos, aunque vaya encubierta en una solicitud DNS para evitar bloqueo de firewalls

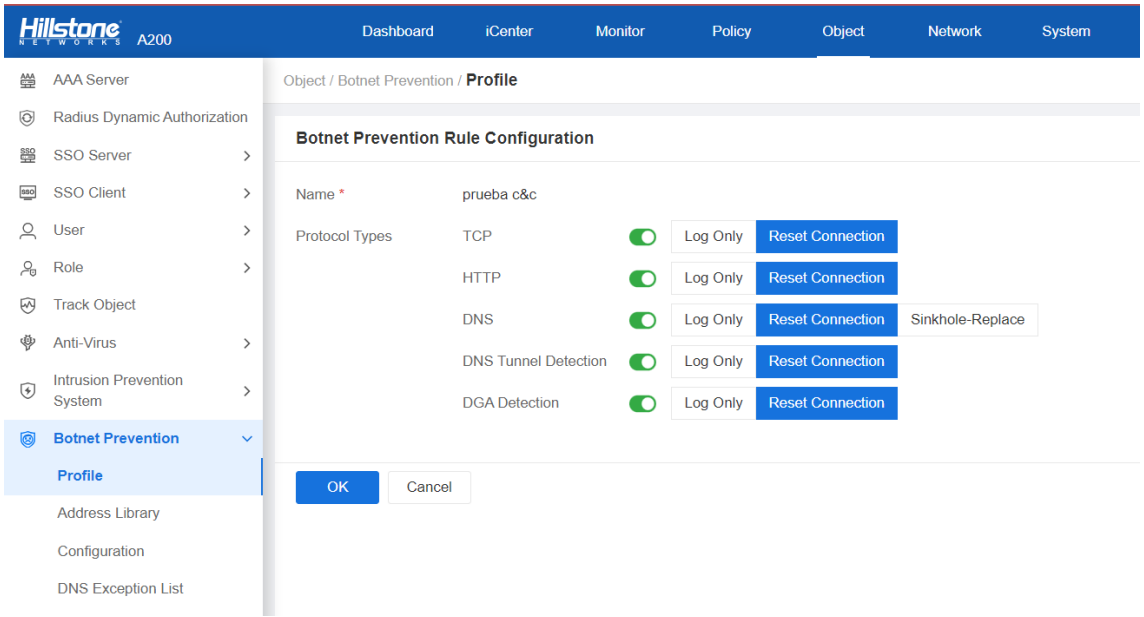


FIGURA 26. VENTANA DE CONFIGURACIÓN BOTNET PREVENTION HILLSTONE

2.7 Sandbox

Es un entorno aislado muchas veces siendo una máquina virtual en la que se descarga/ejecuta software **potencialmente peligroso**.

Entorno diseñado para **proteger el sistema y recursos** del equipo en el que se ejecuta, ya que los **procesos** que se ejecutan dentro de la sandbox **no pueden interactuar con el sistema operativo o con otros programas que se ejecutan fuera de ella**

FIGURA 27. CONCEPTO DE SANDBOX

2.7.1 Fortigate (Sandbox)

Existe otro mecanismo de seguridad incorporado al perfil AV el cual permite la **inspección** a través de la **nube** mediante la opción de **FortiSandbox** [19]

Sandbox de FortiGate detecta **y analiza malware desconocido**, también conocido como de **día cero** el sandboxing en línea (**Inline sandboxing**) analiza en tiempo real y ofrece esa protección inmediata emitiendo veredictos en tiempo real sin afectar la productividad ni nada.

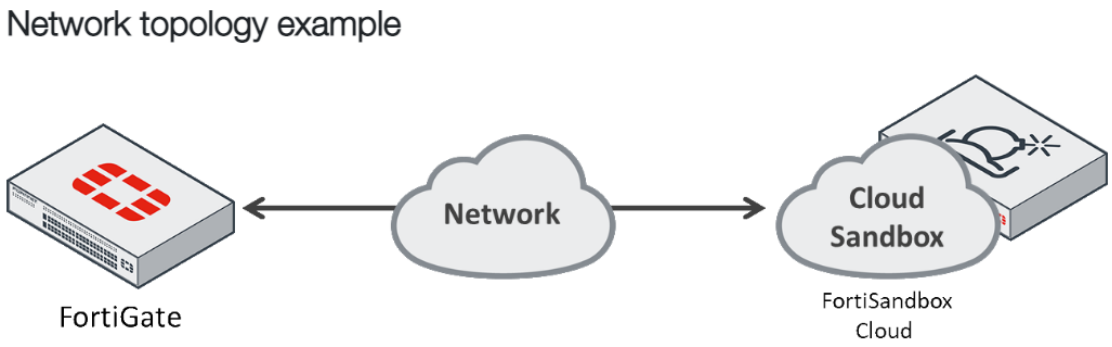


FIGURA 28. CONCEPTO SANDBOX FORTIGATE

Sandboxing en línea es un servicio de FortiGuard que ofrece un combinado del filtrado de amenazas avanzada de varias capas, **utilizando AV, CPRL, AI/ML, análisis dinámico con redes neuronales profundas e inteligencia de amenazas.**

2.7.2 Hillstone (Sandbox)

Hillstone proporciona **técnicas de análisis** tanto del **malware** como del **comportamiento**, ante una sospecha este lo caga en el sandbox para la posterior ejecución en un **entorno aislado** que simule el sistema real [10]

En cuanto al **análisis de malware** se basa en la utilización de dos técnicas denominadas **estáticas y dinámicas**, **estáticas** las cuales se basan en una **comprobación del código** del archivo para buscar sus **vulnerabilidades** y el análisis **dinámico** en un monitoreo en **tiempo real** de este

Sandbox utiliza **técnicas de comportamiento** las cuales incluyen el **seguimiento de la actividad de red, la detección de exploits y la detección de comportamientos sospechosos del sistema**

Características de cloud sanbox:

- Alta tasa de detección con el análisis de comportamiento y malware
- Mediciones comparadas con la tecnología anti-sanbox
- Información completa sobre amenazas en los informes
- Actualización continua global de la base de datos de firmas

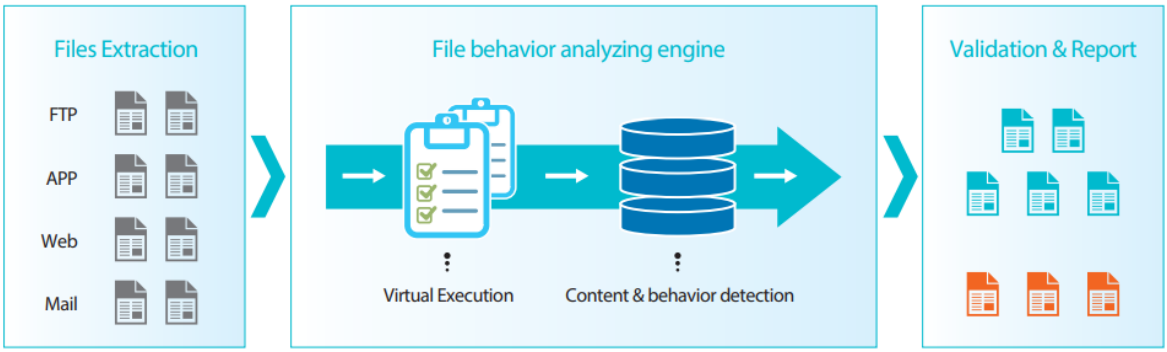


FIGURA 29. HILLSTONE CLOUD-SANDBOX

2.8 Herramientas

Las herramientas necesarias para las **pruebas de demostración** se basarán en **descarga** de malware **especifico** y puesta en **ejecución** en **entorno seguro** para ver interacción con el Firewall a excepción de **IDS/IPS** e **C&C** que se usarán herramientas específicas para simular esa falla

Se usarán paginas oficiales de sitios tanto para descargas como para pruebas de URL filtering

2.8.1 Kali

Distribución de Linux que se basa en Debian la cual viene con una serie de paquetes por defecto ya instalados muy útiles para **pruebas de seguridad y penetración**, esto hace a las personas poder llevar a cabo una diversidad de pruebas de forma "fácil".

Viene con un arsenal de herramientas tales como **Escaneo de puertos**, **exploits, ataques de fuerza bruta, etc…** y una gran variedad mas

Kali Linux no solo tiene herramientas para el apartado de ataques, sino que también cubre/aporta sobre el campo de administración de sistemas teniendo herramientas para una **gestión de paquetes, de la res y virtualización** entre algunas otras mas

2.8.1.1 IDS/IPS

Nmap: herramienta con la capacidad para realizar escaneos de redes, puertos y dispositivos, esta herramienta brinda la posibilidad de "descubrir" la red y gracias a ello la posibilidad de simular comportamiento "negativo" o "extraño" [6]

Armitage: Herramienta e colaboración en equipo que permite el uso de Scripts para Metasploit, la cual permite el uso de diversas pruebas y ataques para varios tipos de sistemas de seguridad [23]

2.8.1.2 C&C

Covenant: Es una herramienta de C2 que permite a los usuarios ejecutar comandos en sistemas comprometidos. También se puede utilizar para capturar información de sistema, cargar y descargar archivos y más. [22]

2.8.2 Páginas usadas

Las paginas usadas para descarga y prueba del módulo AV son:

- **malware.wicar.org**
- **http://www.eicar.eu**

Las paginas usadas para testeo de URL filtering son:

- Marca.com
- Facebook.com
- Twitter
- Edu4java

3 Implementación Practica

3.1 Módulo AV

3.1.1 Ataque

Evaluación de **descarga**, **análisis** y **detección** de tráfico, y prueba de **ejecución** de worms (gusanos)

El ataque tiene el **objetivo** de poner **ambos dispositivos** a prueba y descubrir que están siendo **capaces** de **detectar** y **analizar** de tráfico, así como una vez analizado ver su habilidad para detener descargas o ver si puede frenar ataques de equipos ya infectados que se esparcen por la red

3.1.1.1 Ataque de descarga

Para esta prueba se procederá a realizar la **descarga** de un archivo vía **HTTP** el cual se **ofrece de forma legítima** para pruebas de **AV**, la pagina es **"malware.wicar.org"**

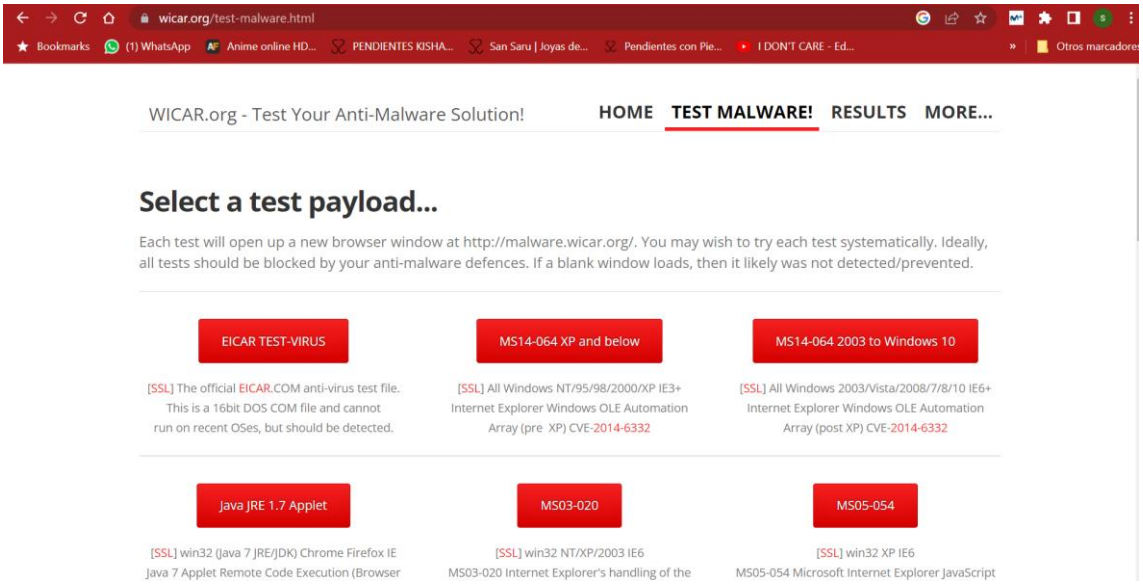


FIGURA 30. PAGINA HTTP DE TESTEO DE AV

Se ofrecen varios "**archivos**" de prueba que contienen **código malicioso**, para la prueba valdrá cualquiera de los ficheros que ofrecen para la **comprobación de detección del módulo AV**

3.1.1.2 Ataque de ejecución

Para esta **prueba** se va a **simular** manualmente un **virus de botnet**

Se utiliza la herramienta **covenant** para la generación del **Virus** o mejor dicho el **comando que ejecutaría él .exe** que representaría el virus

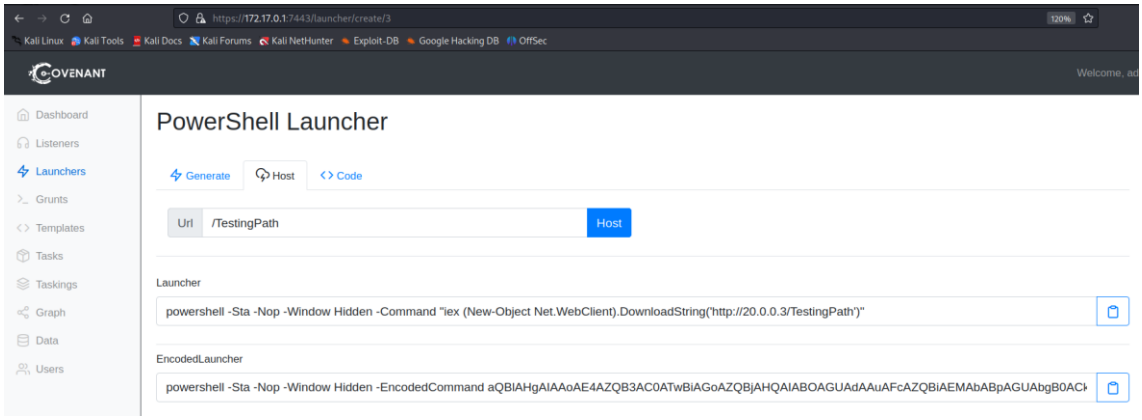


FIGURA 31. GENERACIÓN COMANDO VIRUS BOTNET COVENANT

Se creará un servidor botnet para la simulación mediante el framework Covenant. El servidor generará un ataque de botnet para la simulación de un virus a través de un comando. El comando intentará agregar el equipo a la botnet.

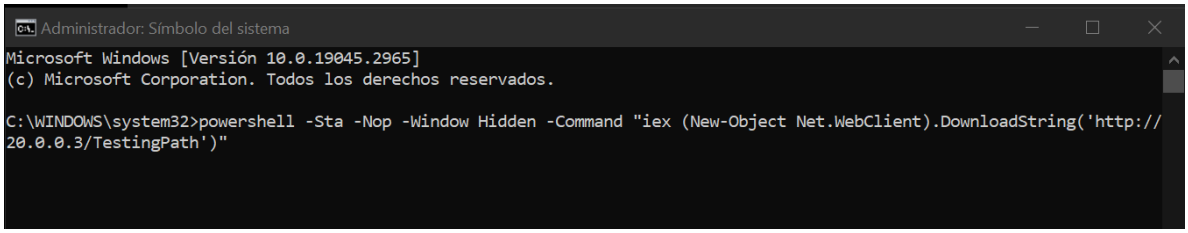


FIGURA 32. EJECUCIÓN COMANDO/VIRUS WINDOWS

3.1.2 Defensa (FortiGate)

Para la realización de la prueba se procederá a dejar configurado el "Profile" AV

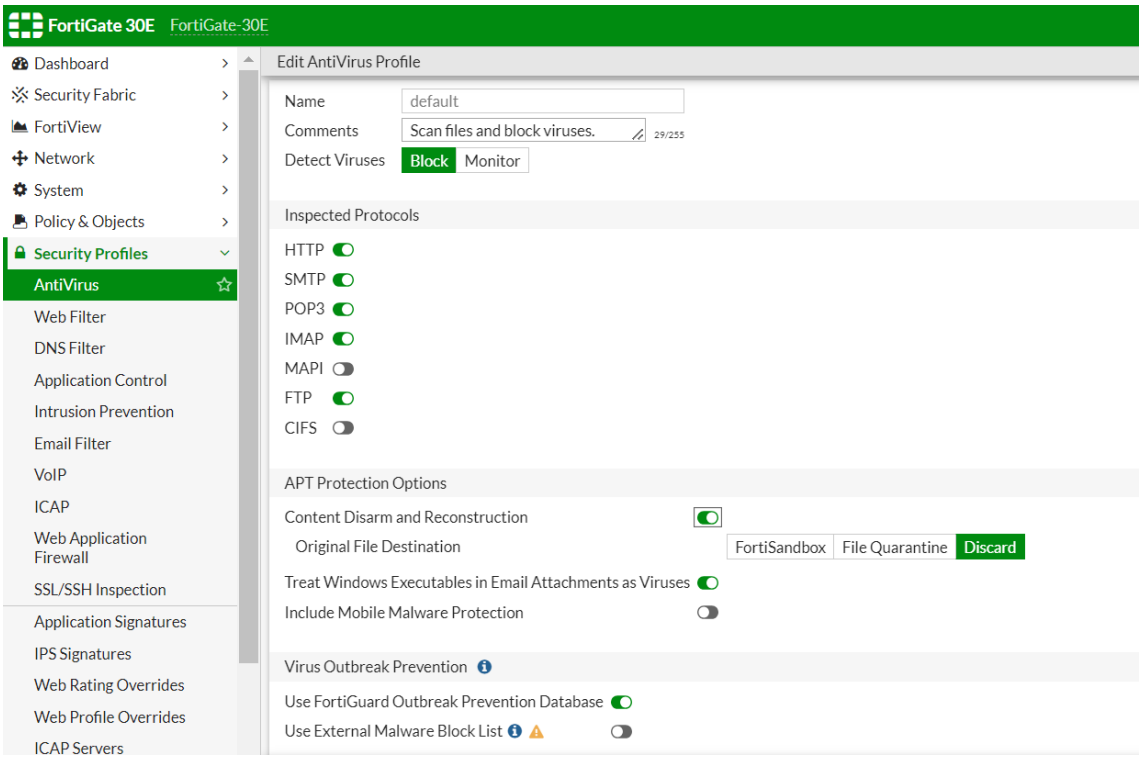


FIGURA 33. VENTANA DE CONFIGURACIÓN DE AV PARA LAS PRUEBAS FORTIGATE

Se aplicará en la política de ipv4 de tráfico que se quiera controlar

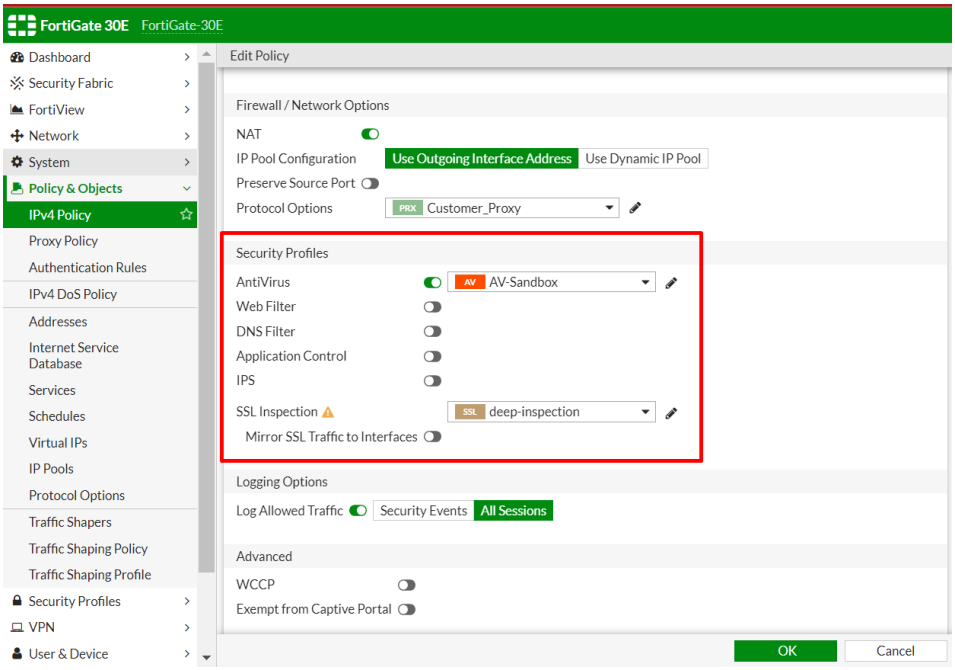


FIGURA 34. VENTANA CONFIGURACIÓN POLÍTICA AV Y DEEP-INSPECTION

Se utiliza una inspección de SSL llamada “Deep-inspection” debido a que, aunque el protocolo HTTPS ofrece protección en Internet al aplicar el cifrado de capa de sockets seguros (SSL) al tráfico web, el tráfico cifrado se puede utilizar para sortear las defensas normales de su red [16]

Para ello con “Deep-inspection” “FortiGate se hace pasar por el destinatario de la sesión SSL de origen, luego descifra e inspecciona el contenido para encontrar amenazas y bloquearlas. Luego vuelve a cifrar el contenido y lo envía al destinatario real”

https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/122078/deep-inspection

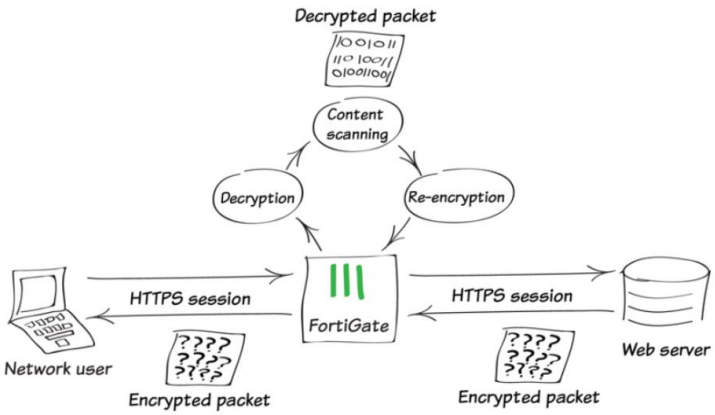


FIGURA 35. CONCEPTO FUNCIONAMIENTO DEEP-INSPECTION

3.1.2.1 Prueba de descarga

Para la prueba de descarga puede verse que, si se intenta descargar un fichero el cual contempla un virus o contenido malicioso, el dispositivo FortiGate con su modulo AV lo detectará y procederá a su bloqueo

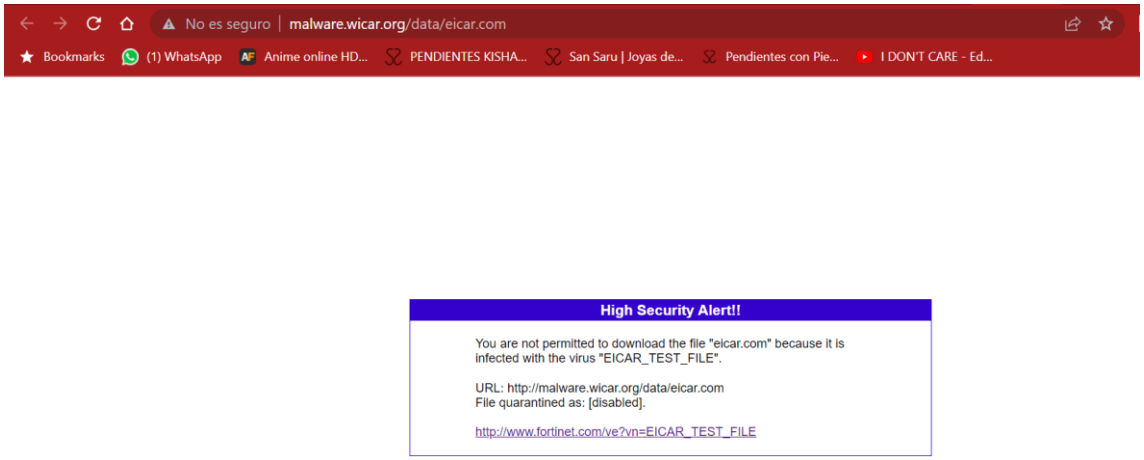


FIGURA 36. VENTANA DE AVISO/BLOQUEO DE DESCARGA DE FORTIGATE

Podrá verse desde el menú de **logs** del módulo **AV** que de forma correcta **detecto** que contenía **código malicioso** y se procedió a su **bloqueo** y aviso

Date/Time		Service	Source	File Name	Virus/Bot...	U...	Details	Action
023/05/25 21:50:16		HTTP	10.0.0.110	eicar.com	EICAR_TEST...		URL: http://malware.wicar.org/data/eicar.co...	blocked
023/05/25 21:49:56		HTTP	10.0.0.110	eicar.com	EICAR_TEST...		URL: http://malware.wicar.org/data/eicar.co...	blocked
023/05/25 21:49:42		HTTP	10.0.0.110	eicar.com	EICAR_TEST...		URL: http://malware.wicar.org/data/eicar.co...	blocked
023/05/25 21:40:49		HTTP	10.0.0.110	eicar1.com.zip	EICAR_TEST...		URL: http://i2re8.cybrarro.com/b/eicar1.co...	blocked
023/05/25 21:40:47		HTTP	10.0.0.110	eicar1.com	EICAR_TEST...		URL: http://ilpuqgdc.shieldtest.com/b/eicar...	blocked

FIGURA 37. VENTANA DE LOGS DE AV PRUEBA DESCARGA FORTIGATE

3.1.2.2 Prueba de ejecución

A la **ejecución** realizada por el **PC victima** para **unirse** a la **botnet** puede verse desde el menú de **logs** del **AV** del **FortiGate** una **nueva entrada** la cual es el **bloqueo** de este "comando"

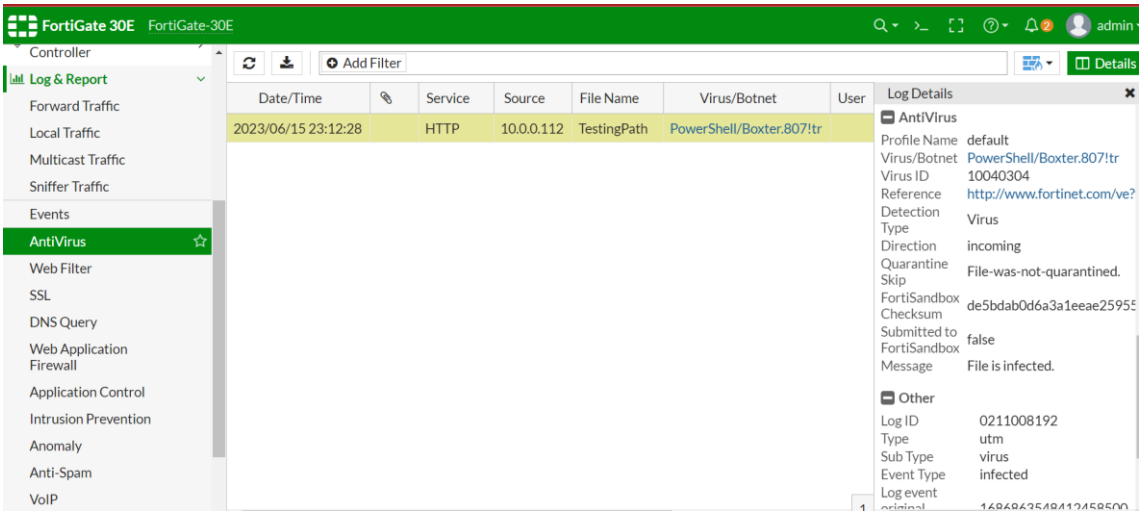


FIGURA 38. VENTANA LOG AV PRUEBA EJECUCIÓN FORTIGATE

3.1.3 Defensa (Hillstone)

Para la realización de la prueba se procederá a dejar configurado modulo AV de Hillstone

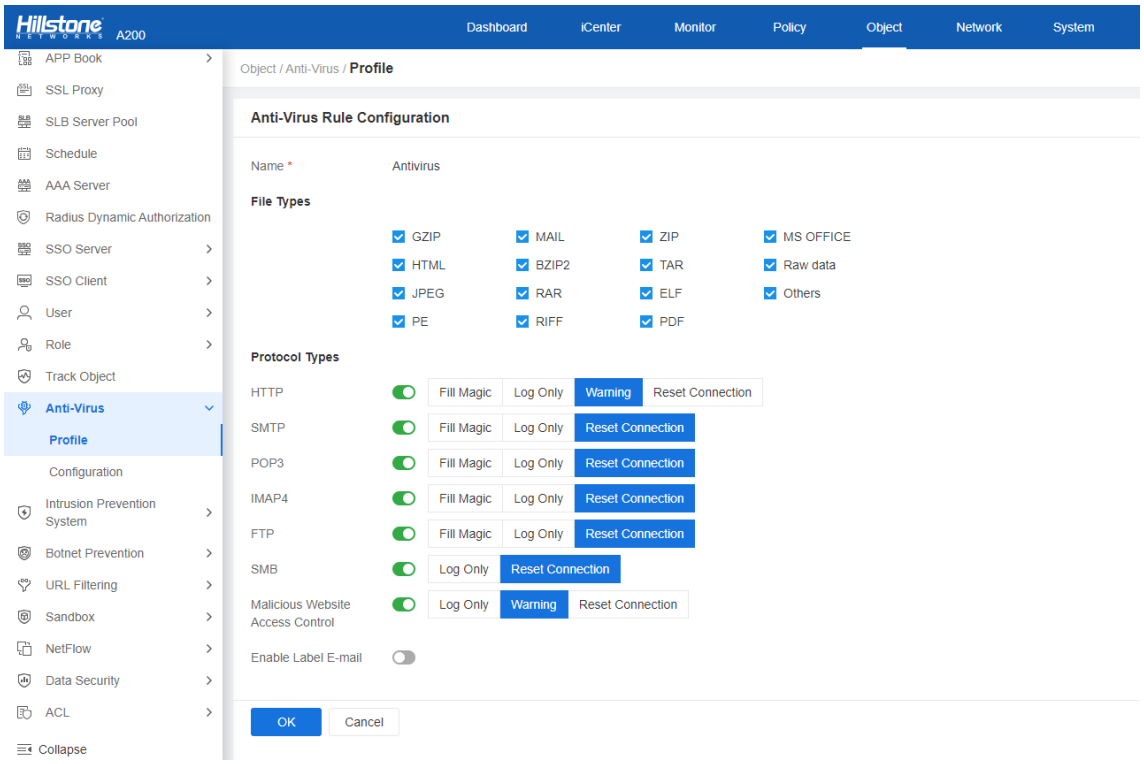


FIGURA 39. VENTANA DE CONFIGURACIÓN DE AV PARA LAS PRUEBAS HILLSTONE

3.1.3.1 Prueba de descarga

Para la prueba de descarga puede verse que, si se intenta descargar un fichero cuyo contenido es un virus o malicioso, el dispositivo Hillstone con su modulo AV lo detectará y procederá a su bloqueo

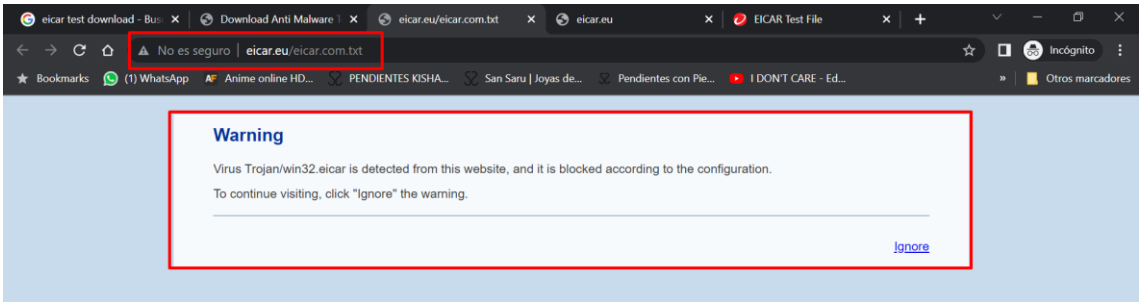


FIGURA 40. VENTANA DE AVISO/BLOQUEO DE DESCARGA DE HILLSTONE

Para una mejor visualización del elemento bloqueado y comprobación más precisa, se confirmará a través del log el comportamiento del Hillstone ante el virus

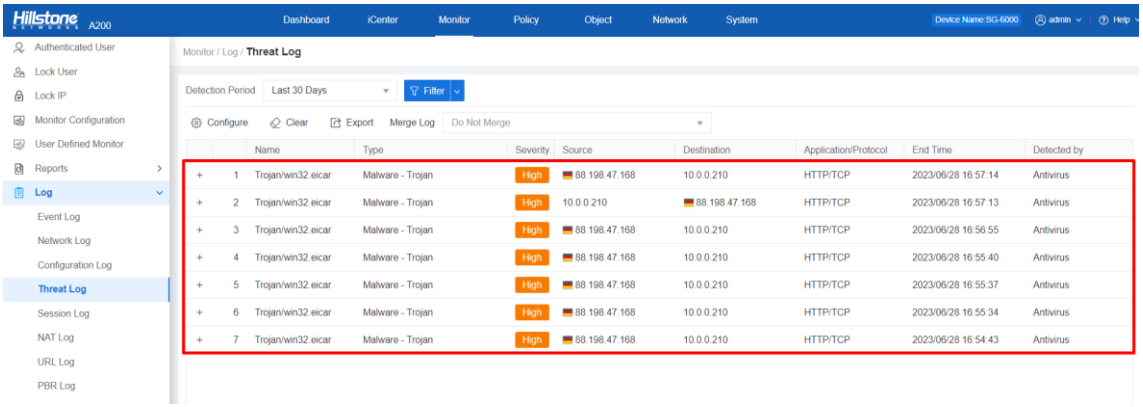


FIGURA 41. VENTANA DE LOGS DE AV PRUEBA DESCARGA

A la teoría de Hillstone mencionada también, es capaz de analizar virus en los ficheros .zip, para ello se procederá a realizar la misma prueba, pero descargando la versión .zip para verificar la detección del fichero

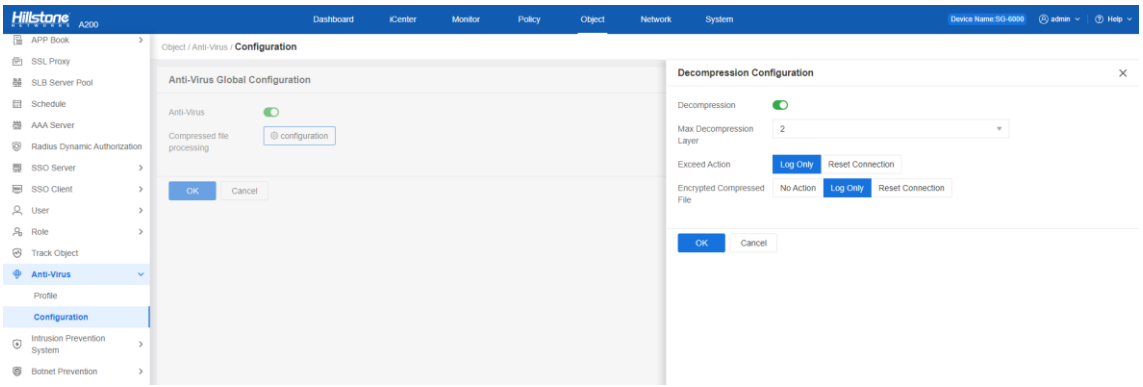


FIGURA 42. VENTANA CONFIGURACIÓN FICHEROS COMPRIMIDOS

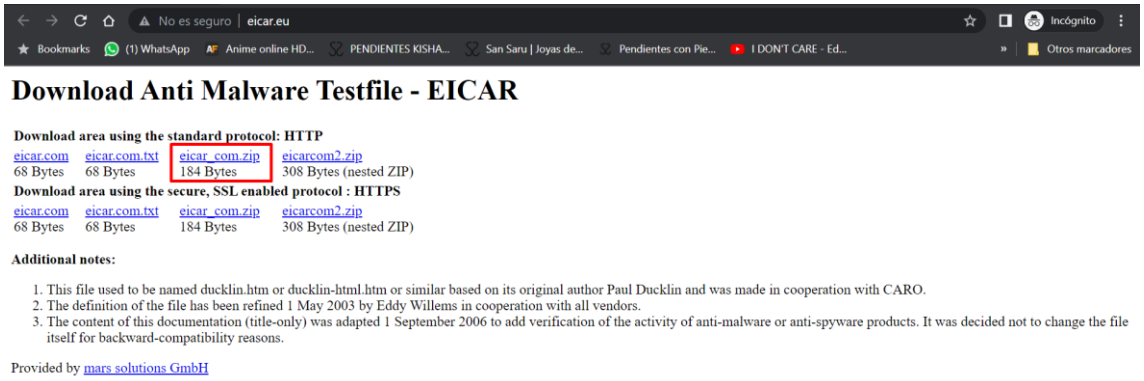


FIGURA 43. DESCARGAR VIRUS EN .ZIP

La detección del virus .zip puede observarse en el log de Hillstone verificándose que aparece la entrada de “warning” en el log

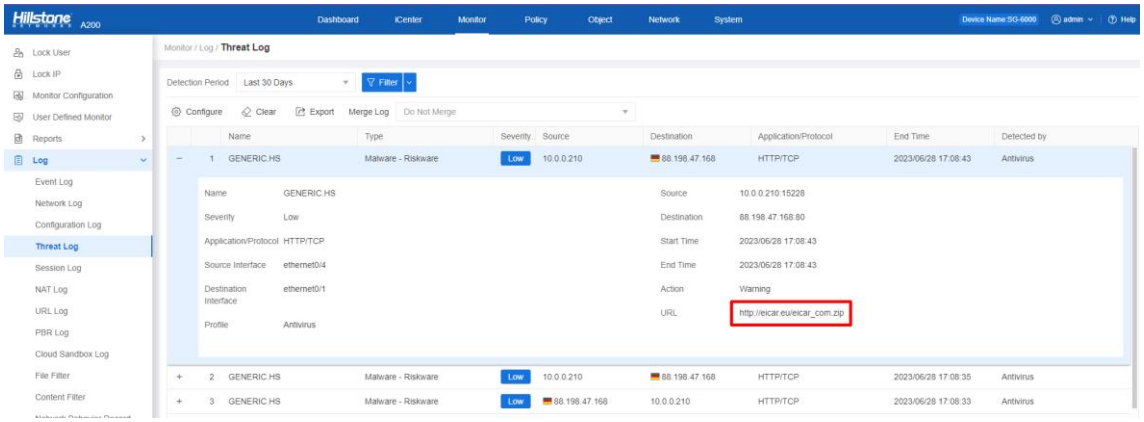


FIGURA 44. VENTANA LOG AV DETALLES .ZIP HILLSTONE

3.1.3.2 Prueba de ejecución

A la **ejecución** realizada por el **PC victima** para **unirse** a la **botnet** puede verse que Hillstone no localizó y detuvo la operación de unión a la botnet

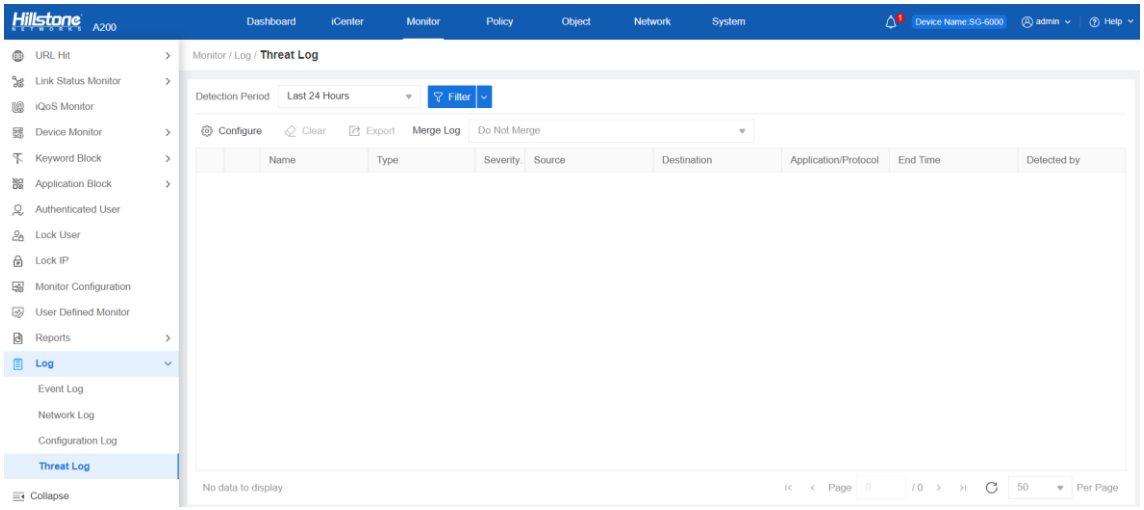


FIGURA 45. VENTANA DE LOGS DE AV PRUEBA EJECUCIÓN HILLSTONE

3.1.4 Discusión

Para la prueba de descarga que ambos han sido capaces de detectar la descarga y que se trata de un troyano (trojan), esto debido al contenido del fichero el cual tienen en la base de datos localizado como contenido “malicioso”

FortiGate no ofrece opción de configuración de zip para poder afinar a que profundidad se quiere adentrar y analizar, sí que es capaz de frenar zips pero no se detectó 1 dentro de otro, pero sí que permite configurar que se bloquen todos los ficheros que su extensión sea .zip. Hillstone si fue capaz de bloquear descargas de ficheros comprimidos como los zips además de ofrecer configuración adicional de a cuantos niveles se quiera bajar y mirar dentro

FortiGate en la prueba de ejecución detecto ya que estaba en la base de datos que el comando lanzado trataba de unirse a una botnet y lo bloqueo, lo tiene registrado como un virus de Powershell mientras que Hillstone no fue capaz de analizarlo y lo dejo pasar debido a que pensó que era un simple comando de Windows sin intenciones maliciosas

3.2 Módulo IDS/IPS

3.2.1 Ataque

Evaluación de envíos "anómalos" como paquetes fragmentados utilizados para intrusión IDS y paquetes ACK sin conexión SYN

El **ataque** tiene el objetivo de **poner a prueba** los dispositivos en el análisis de tráfico y red para la detección de comportamientos extraños a la hora de que se **intenta establecer conexión** como llegada de mensaje ACK sin previo SYN u otros diversos patrones, para puesta a punto se realizaran pruebas como **envió de paquetes fragmentados y explotación de exploit vsftpd**

3.2.1.1 Ataque de IDS de fragmentación

Para esta **primera prueba** se hará uso de la herramienta **"nmap"** mediante la opción **"-f"** para que fragmente el paquete

```
C:\WINDOWS\system32>nmap -f 10.0.0.111
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.  This may or may not wor
k.

Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-05 11:46 Hora de verano romance
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid
 servers with --dns-servers
Nmap scan report for 10.0.0.111
Host is up (0.0019s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

FIGURA 46. VENTANA COMANDO NMAP FRAGMENTADO

Puede verse la ejecución de dicha herramienta y el escaneo de puertos en el dispositivo de prueba para la demostración

3.2.1.2 Ataque de vsftp backdoor

Para esta segunda prueba se hará uso de la herramienta “armitage” y se hará uso de un exploit de backdoor llamado “vsftpd_234_backdoor”

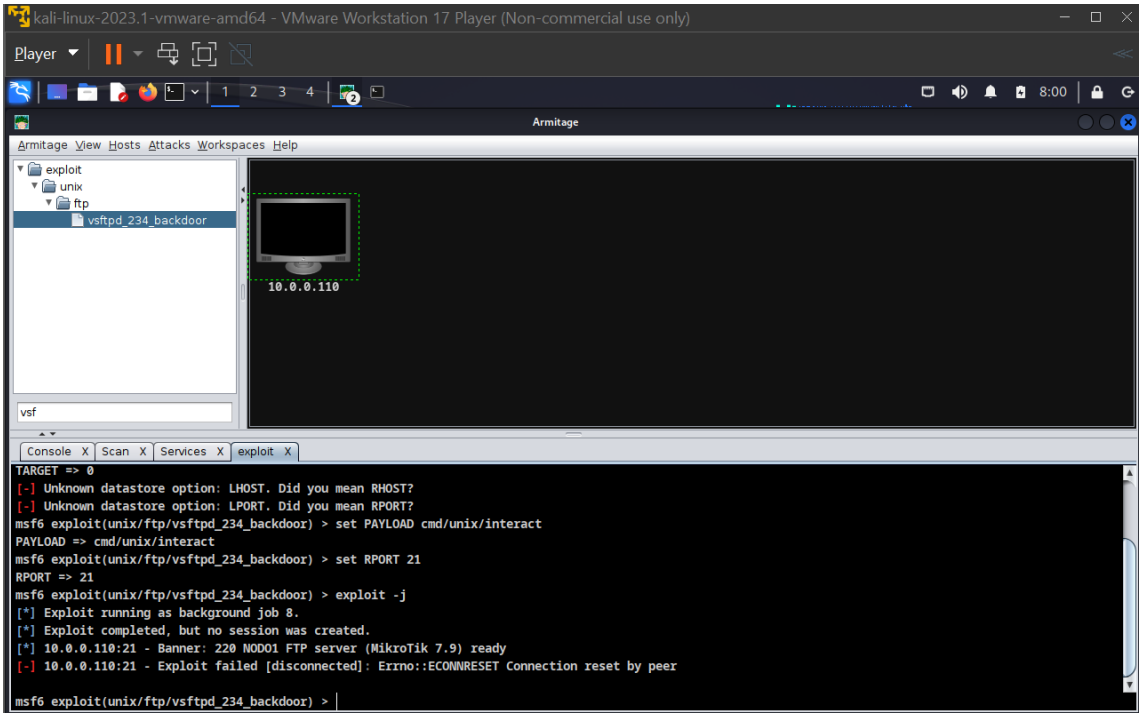


FIGURA 47. VENTANA ARMITAGE CON EXPLOIT

El exploit intenta **explotar** una **vulnerabilidad** del servidor **VSFTP** para la creación de un **backdoor**, esto **consiste** en el **envió** de una **secuencia de bytes** específicos en el **puerto 21** en caso de **ejecutarse** con **éxito** dará un resultado de la **apertura del puerto 6200**

3.2.2 Defensa (FortiGate)

Para la demostración **IDS/IPS** se aplicará una configuración sobre una **política de seguridad** con fuente (interfaz de entrada) WAN y destino (interfaz de salida) LAN en el dispositivo FortiGate

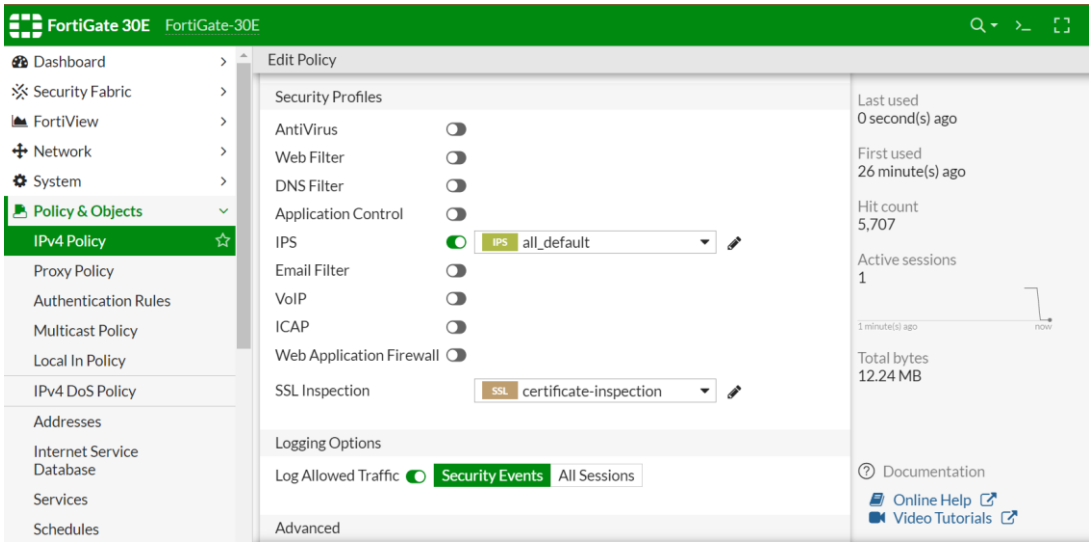


FIGURA 48 VENTANA POLÍTICA IPV4 APLICANDO IPS

El **objetivo principal** de esta configuración es demostrar la **capacidad** del **IDS/IPS** para detectar y prevenir intrusiones en el tráfico de red que fluye desde la interfaz WAN hacia la interfaz LAN.

La configuración presente en la prueba es la siguiente:

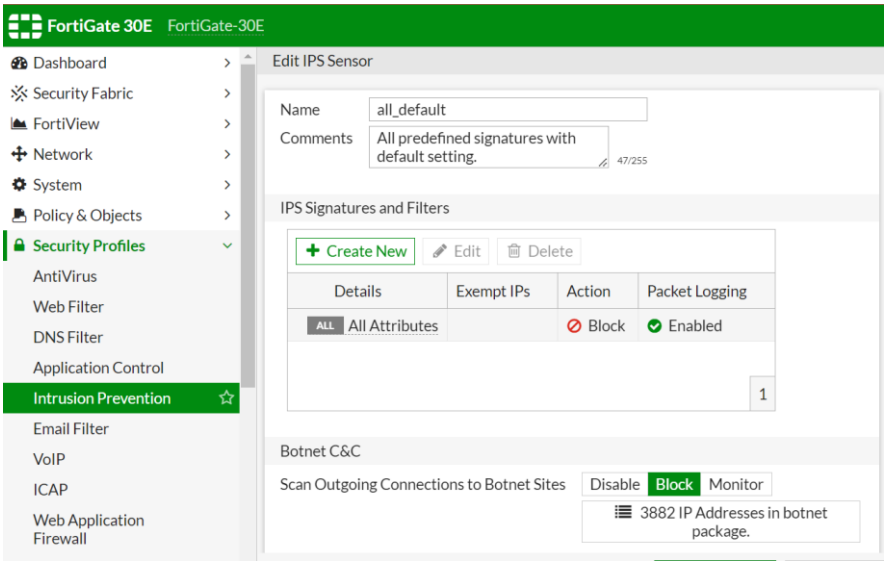


FIGURA 49. VENTANA CONFIGURACION IPS

Se configurada de la forma más restrictiva para la mejor captación de lo que bloquea y pasa

3.2.2.1 Prueba de IDS de fragmentación

Para una **visualización** un poco más clara de lo que **paso/hizo** el dispositivo **FortiGate** puede visualizarse los **logs** de **IPS** para ver que **interacciones bloqueo**

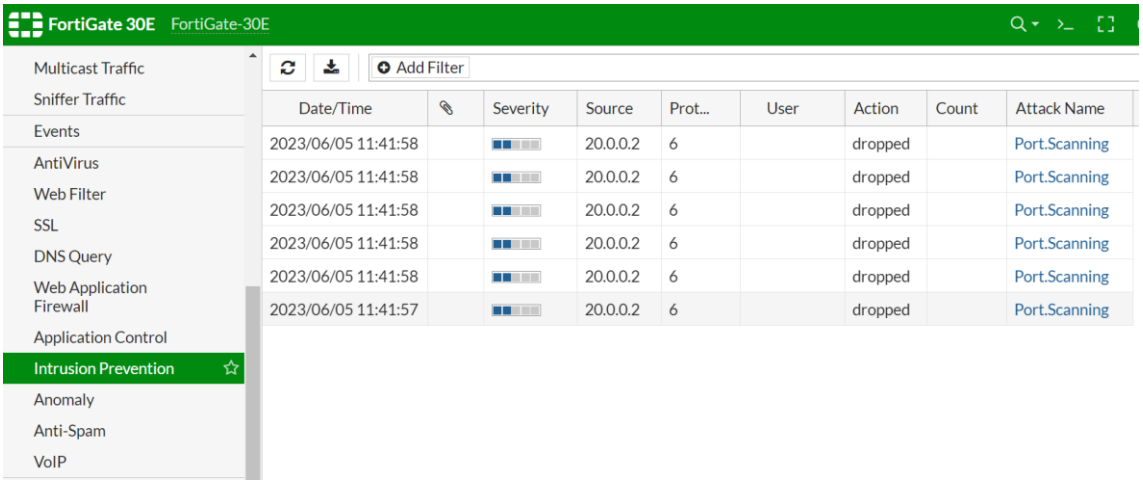


FIGURA 50. VENTANA LOG IPS PAQUETES DETENIDOS EN ESCANEO FORTIGATE

En una explicación resumida puede verse por un solo escaneo de **nmap** que **aparecen 6 “eventos” /” entradas”** en el log, estas **advertencias** las cuales sus **acciones** a tomar fue un **droppeo** son escaneo a **diferentes puertos** de servicios concretos el cual el dispositivo **FortiGate** detecto como **sospechoso** y catalogo como **ataque de “escaneo de puertos”**

3.2.2.2 Prueba de vsftp_backdoor

Para una **visualización** un poco más clara de lo que **paso/hizo** el dispositivo **FortiGate** puede visualizarse los **logs** de **IPS** para ver que **interacciones bloqueo**

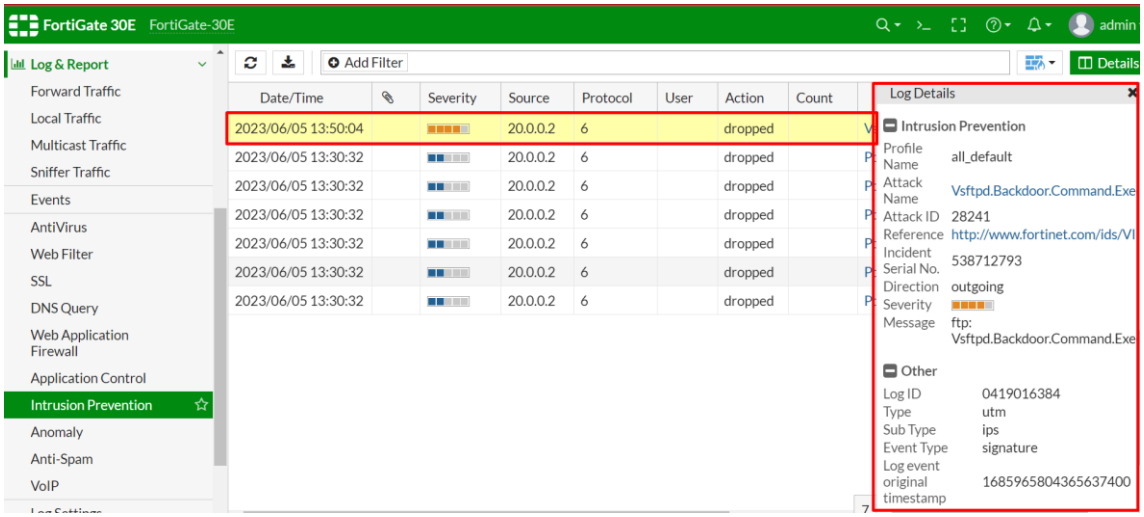


FIGURA 51. VENTANA LOG IPS DETECCIÓN EXPLOIT FORTIGATE

3.2.3 Defensa (Hillstone)

Para la demostración **IDS/IPS** se aplicará una configuración partida en 2 partes:

- **Network Layer Attack Protection**: Esta capa analiza a nivel de paquete bajo los protocolos TCP, UDP e icmp sin entrar en lo que viene a ser la capa de aplicación, analizando el paquete a nivel de la capa de transporte teniendo en cuenta la cantidad de "conexiones" realizadas en determinado tiempo para evitar inundaciones, spoofing , escaneo de puertos u otros ataques derivados en la capa de red [17]

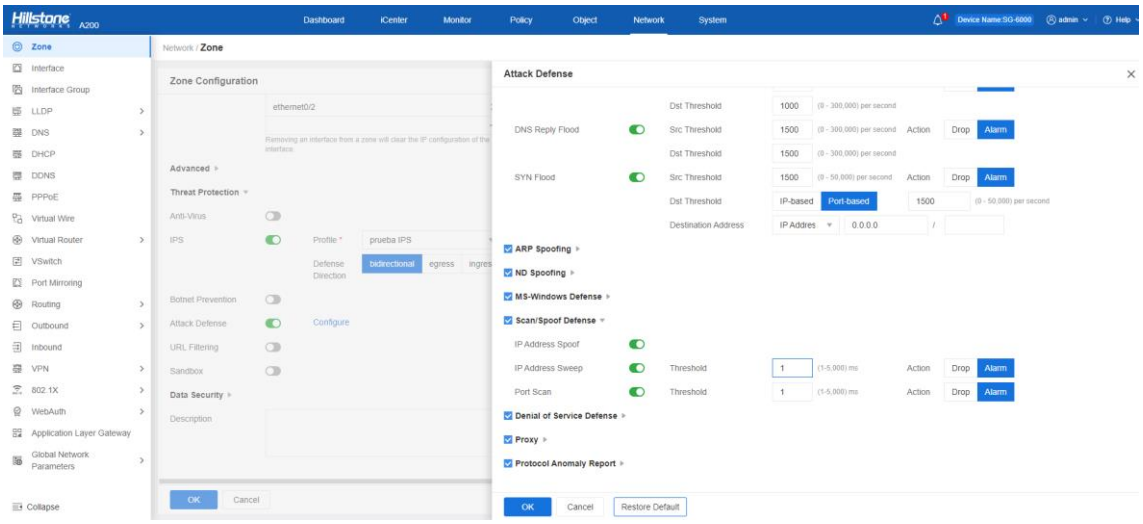


FIGURA 52. CONFIGURACIÓN CAPA NETWORK HILLSTONE

- **Application Layer Protection**: Configuración de la firma y la configuración del protocolo. El sistema analiza el protocolo y procesa los paquetes (solo registrar, restablecer y bloquear) de acuerdo con la configuración para que pueda generar registros para el administrador si se detecta alguna anomalía [17]

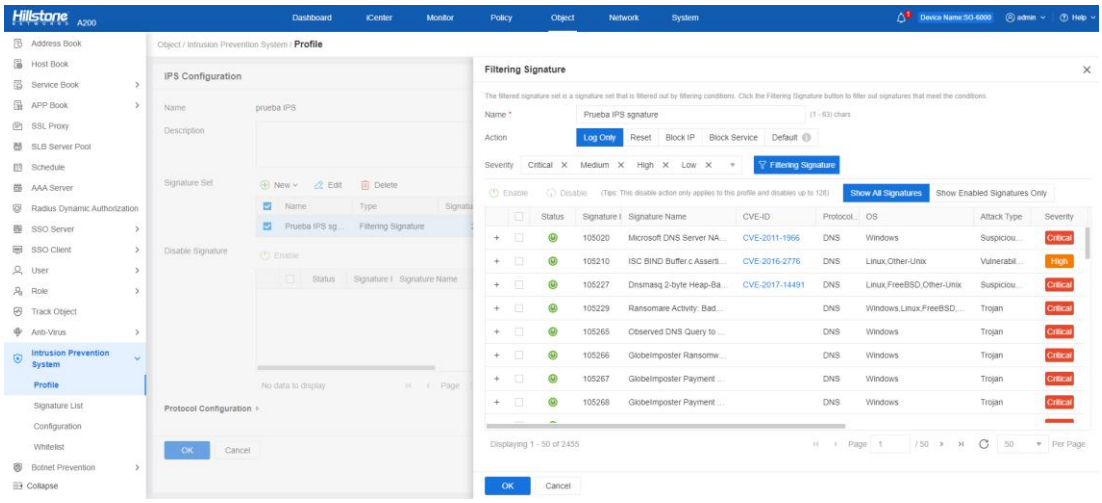


FIGURA 53. CONFIGURACIÓN CAPA APPLICATION HILLSTONE

3.2.3.1 Prueba de IDS de fragmentación

Para una **visualización** un poco más clara de lo que **paso/hizo** el dispositivo **Hillstone** puede visualizarse los **logs** de **IPS** para ver que **interacciones bloqueo**

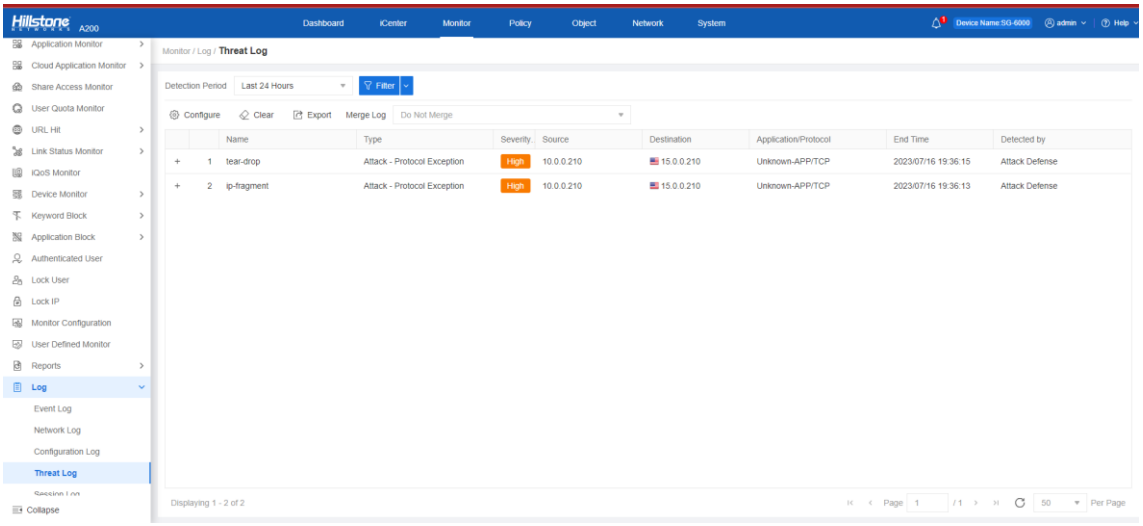


FIGURA 54. VENTANA LOG IPS PAQUETES DETENIDOS EN ESCANEO HILLSTONE

3.2.3.2 Prueba de vsftp_backdoor

Para el bloqueo de este ataque se realizaría a través de firmas las cuales son descargadas desde la actualización de la DATABASE de Hillstone

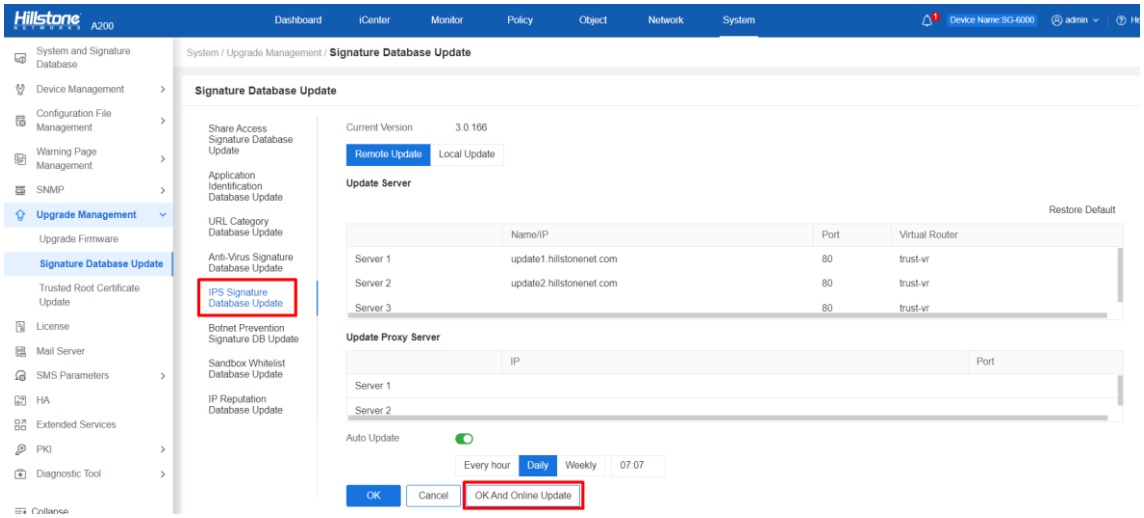


FIGURA 55. VENTANA ACTUALIZACIÓN FIRMAS IPS HILLSTONE

Ahora pueden verse las firmas de las que se disponen para el bloqueo y log de los ataques registrados

Debido a la licencia disponible para el hardware actual solo se disponen de 2.500 fimas de las mas de 8.000 que dispone Hillstone

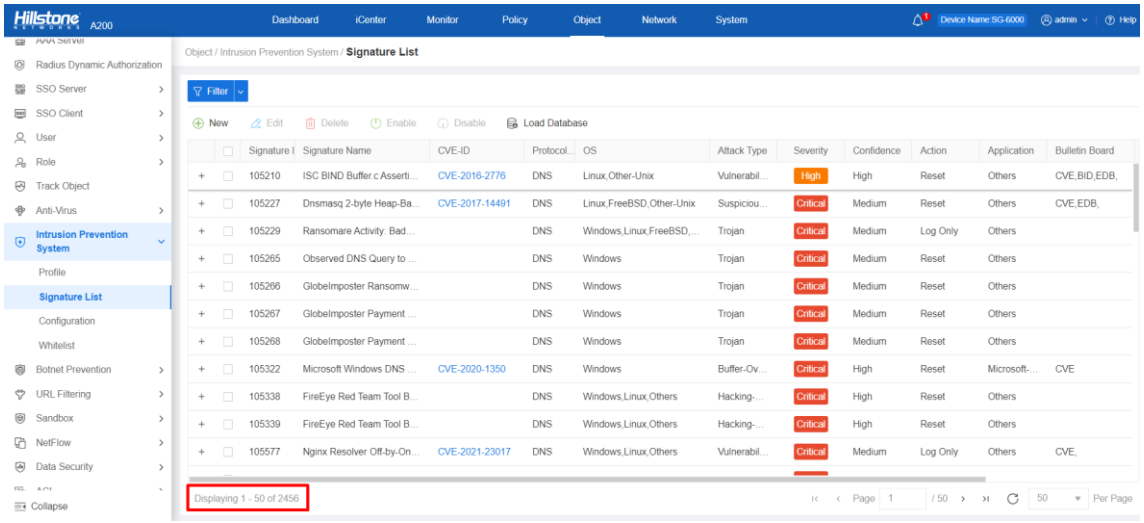


FIGURA 56. FIRMAS DE IPS DE HILLSTONE

3.2.4 Discusión

Ante la prueba de fragmentación ambos dispositivos detuvieron sin mayor problema el ataque siendo que FortiGate ya tenía localizado el ataque en firmas y Hillstone a través de su "**Network Layer Attack Protection**" la cual se encarga del análisis de las "conexiones" y detecto un comportamiento anómalo de una fuente haciendo peticiones recurrentes bajo protocolos de transporte

El ataque de backdoor Hillstone no fue capaz de detenerlo debido a que no dispone de la firma **CVE-2011-2523** el cual es el identificador de la firma que es el ataque de vsftp_234_backdoor

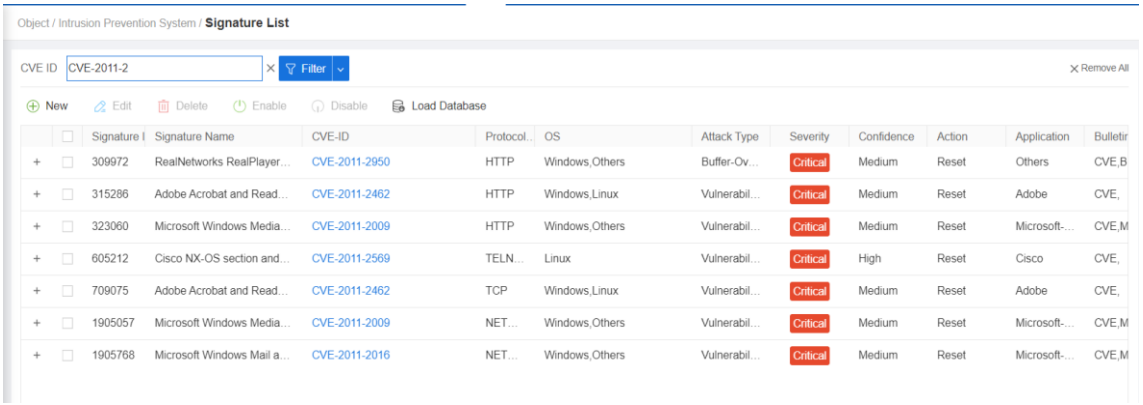


FIGURA 57. VISTA FIRMAS CON INICIO ID DE LA FIRMA CVE HILLSTONE

3.3 Módulo IPR

3.3.1 Ataque

El ataque tiene el **objetivo** las pruebas de **filtrado por reputación IP**, estas pruebas de filtrado de tráfico mediante IPR medirán la **capacidad** de los dispositivos para el **bloqueo/aceptar** las direcciones **IP** de la **base de datos** que vienen de botnets u otros lugares **dependiendo el umbral** asignado de configuración

3.3.2 Defensa (FortiGate)

Para la demostración de **IPR** se va a intentar realizar **conexiones** sobre una **política de salida** ya que se **establece** en estas el nivel **mínimo de reputación** necesario, las pruebas consistirán en **intentos de conexión a direcciones IP de la base de datos** que tiene descargada FortiGate la cuales están "**valoradas**", estas pruebas serán:

- **nivel 4** de reputación permitido mínimo para ver el bloqueo al ser un nivel más bajo el intento de acceso
- **nivel 2** de reputación mínimo permitido para ver como deja pasar todo ya que es el nivel más bajo

3.3.2.1 Prueba de nivel 4

Viéndose como se aplica la seguridad de reputación de nivel 4

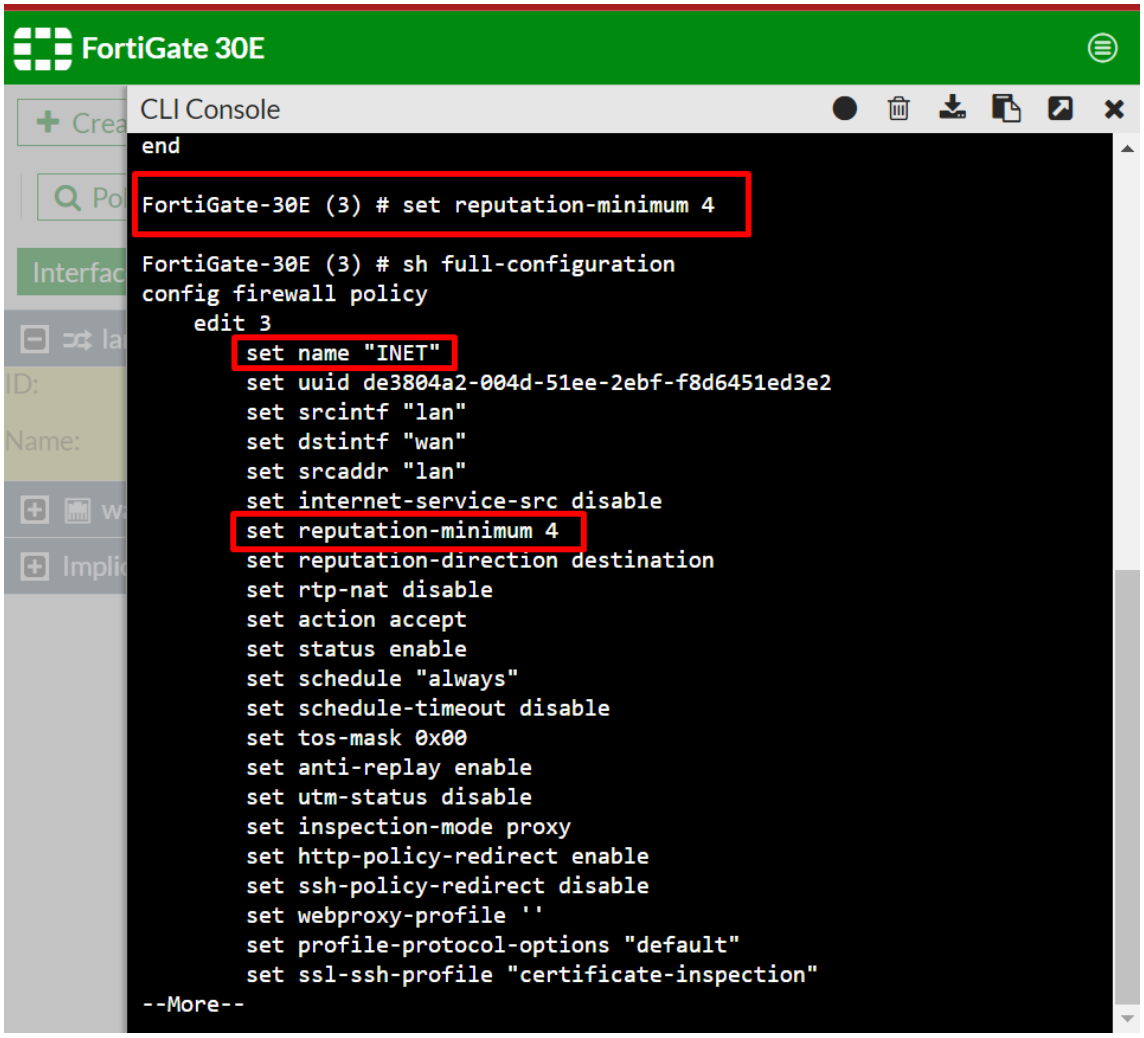


FIGURA 58. VENTANA CONFIGURACIÓN IPR MÍNIMO DE 4

Se procede a realizar una conexión a una dirección IP la cual está en la base de datos

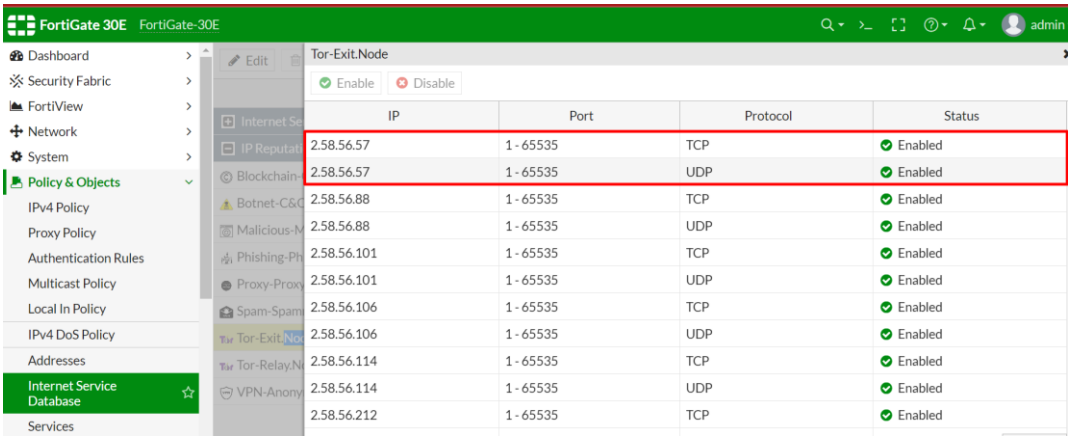


FIGURA 59. VENTANA IP DE BASE DE DATOS CON MALA REPUTACIÓN

La conexión al estar **establecidos** todos los servicios se realizará mediante un **ping para comprobación de comportamiento de FortiGate** ante este caso

Véase la configuración que se realizó, se puede apreciar que no se podrá establecer conexión a una dirección la cual supone ser de nivel 2

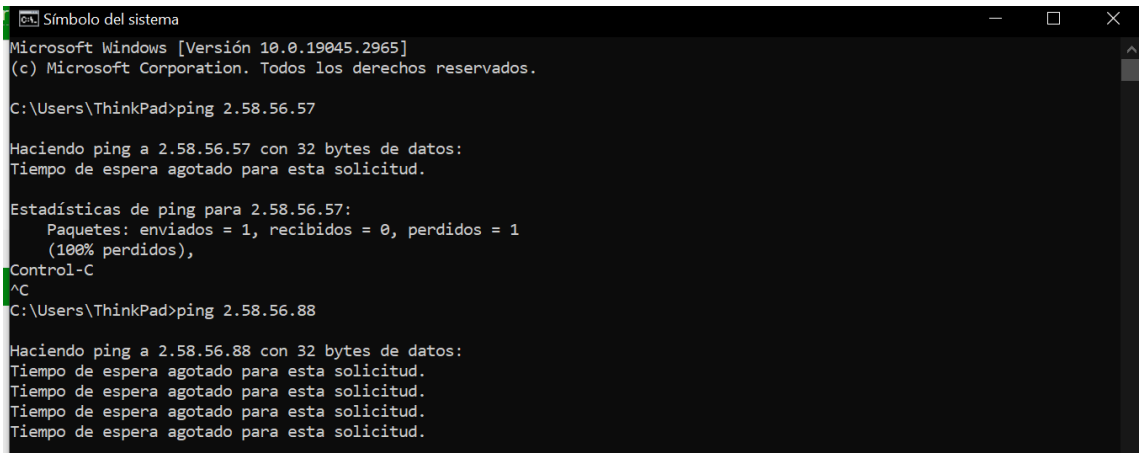


FIGURA 60. VENTANA DEMOSTRACIÓN INTENTO CONEXIÓN FALLIDO A IP NIVEL 2

Pueda verse que las conexiones mueren debido a que no se las deja pasar

A si mismo pueda entenderse que al **quitar** la **restricción** de IPR se **pueda establecer conexión** a esas direcciones debido a que si no se establece un mínimo por defecto es 0

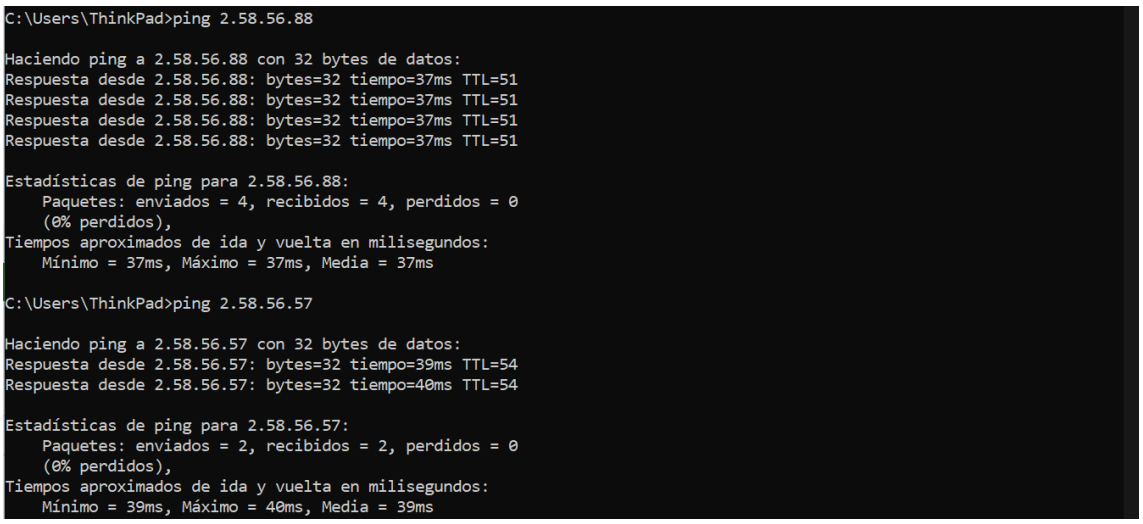


FIGURA 61. VENTANA DEMOSTRACIÓN INTENTO DE CONEXIÓN EXITOSO A IP NIVEL 2

3.3.2.2 Prueba de nivel 2

Viéndose como se aplica la seguridad de reputación de nivel 2

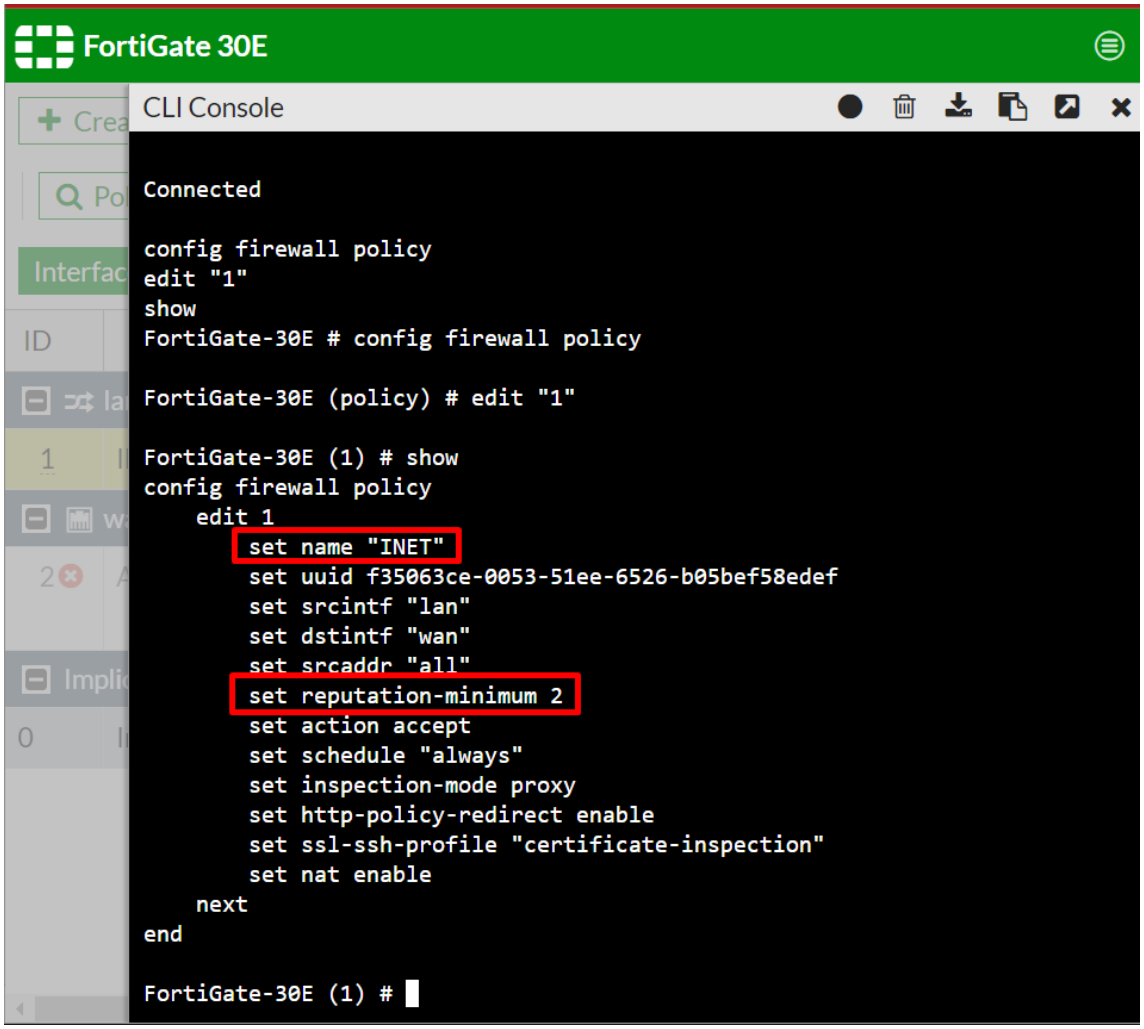


FIGURA 62. VENTANA CONFIGURACIÓN IPR MÍNIMO DE 2

Se procederá a realizar 2 conexiones con 2 direcciones Ip de la base de datos:

- Dirección Ip de nivel 1 de una botnet

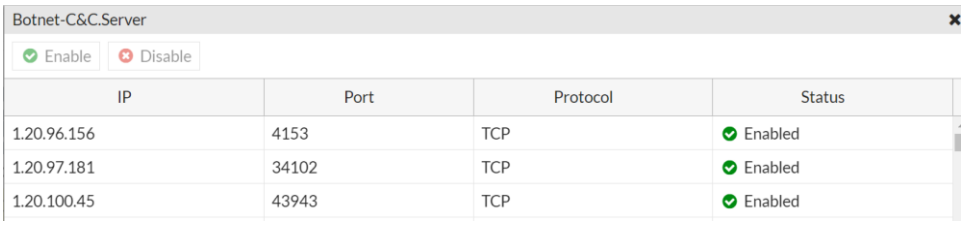


FIGURA 63. VENTANA IP DE BASE DE DATOS CON MALA REPUTACIÓN DE NIVEL 1

- Dirección Ip de nivel 2 o superior

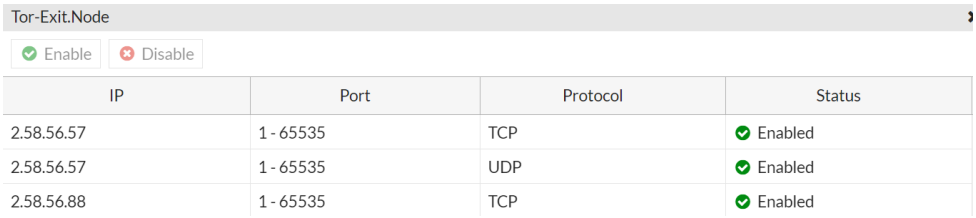


FIGURA 64. VENTANA IP DE BASE DE DATOS CON MALA REPUTACIÓN DE NIVEL 2

La conexión al estar **establecidos** todos los servicios se realizará mediante un **ping para comprobación de comportamiento de FortiGate** ante este caso

Véase a la configuración mostrada como la dirección que es de nivel 1 menor a 2 no es capaz de llegar ya que es cortada y la comunicación de nivel 2 o superior sí que puede realizarse

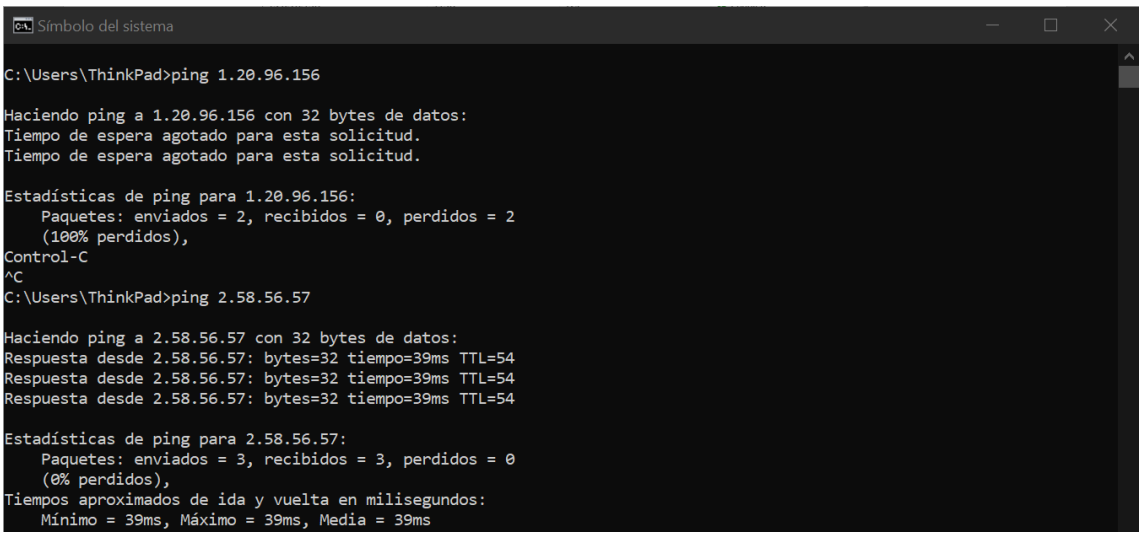


FIGURA 65. DEMOSTRACIÓN DE INTENTOS DE CONEXIÓN A IP DE NIVEL 1 Y 2

3.3.3 Defensa (Hillstone)

Hillstone aplica IP reputation sobre **Global**, **zonas** o su concepto de **virtual router**, aplicándose esta reglas para todo el control del trafico

Para la prueba se procederá a configurar el dropeo de conexiones IP de BOT tanto de la zona trust como la untrust

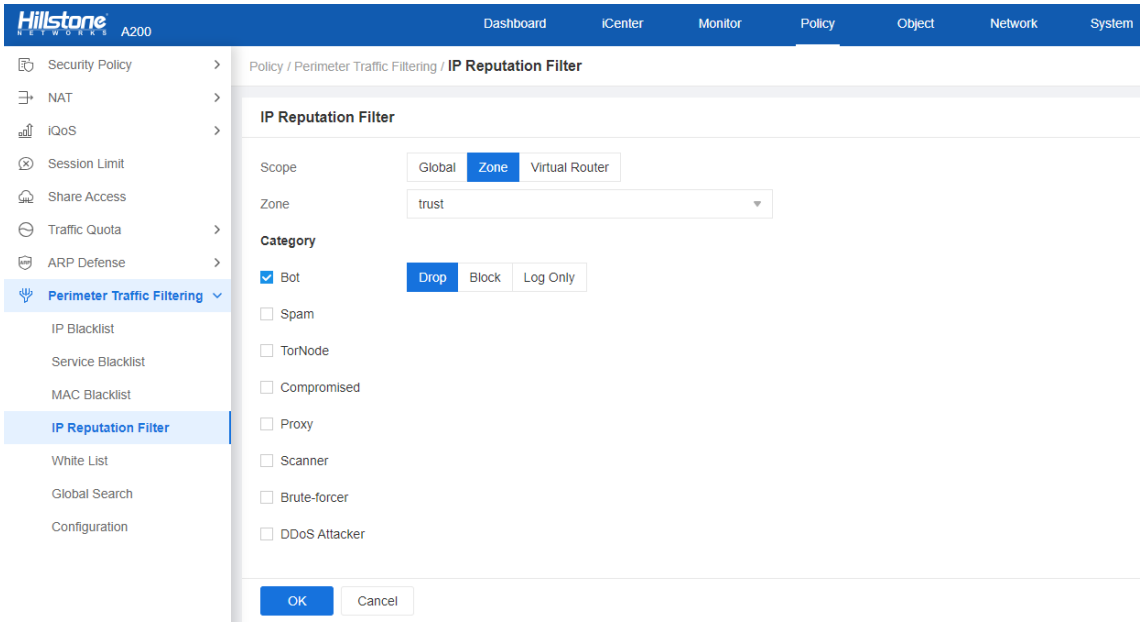


FIGURA 66. VENTANA CONFIGURACIÓN IPR TRUST HILLSTONE

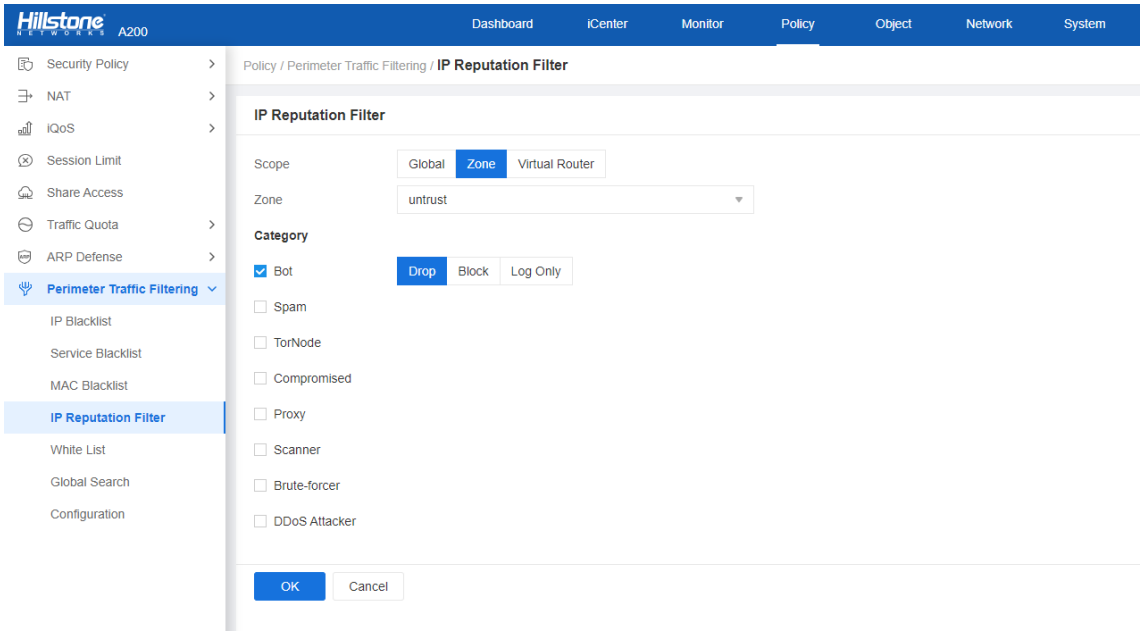
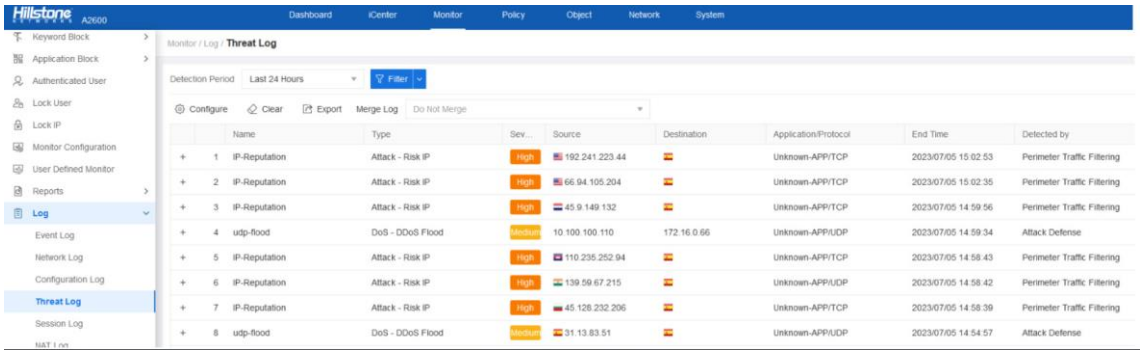


FIGURA 67. VENTANA CONFIGURACIÓN IPR UNTRUST HILLSTONE

También se realizarán pruebas de conexiones entrantes y salientes

- A ejemplo de las entrantes se uso la IP publica para ver como le llegaban los ataques
- A ejemplo de salientes se intentó establecer conexión con diferentes IP de botnets

Para la comprobación y vista de la reacción tomada por el Hillstone se visualizará en los logs en el apartado de Threat



3.3.4 Discusión

Tanto FortiGate como Hillstone frenaron conexiones cuando se trataban de direcciones IP que estaban dentro de los aspectos de funcionamiento de cada uno de sus respectivos sistemas a excepción de Hillstone que solo fue capaz de bloquear conexiones entrantes, pero dejaba pasar las que iban en dirección hacia la WAN

Puede apreciarse como el Hillstone freno los ataques de direcciones IP provenientes de BotNets solo cuando venía desde el exterior

3.4 Módulo URL

3.4.1 Ataque

El **objetivo** será la prueba de **respuesta** y **filtrado** de los **dispositivos** y para este caso se **"atacara" direcciones URL** diferentes con diferentes configuraciones en los dispositivos, **se quiere llegar a ver la capacidad que tienen para filtrar según unas pocas configuraciones de este punto ya que poseen varias mas**

Los siguientes ataques que se harán para las pruebas serán las siguientes:

- Filtrado por URL
- Filtrado por categorías
- Filtrado por contenido

3.4.1.1 Ataque filtrado por URL

Para la demostración se intentará visualizar la dirección "www.marca.com" y podrá comprobar **cómo es posible verla antes** del filtrado y cómo **reacciona una vez se aplica la configuración**

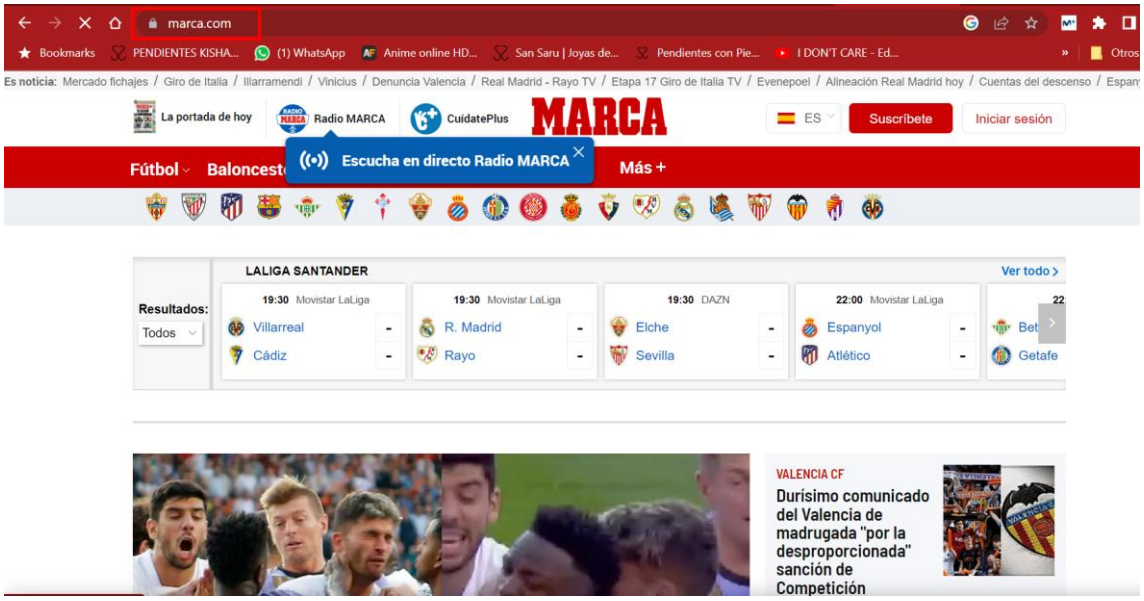


FIGURA 68. EJEMPLO VISUALIZACIÓN MARCA

3.4.1.2 Ataque por categorías

Para la demostración se intentará visualizar la dirección "www.facebook.com" y "www.twitter.com" pudiendo comprobar cómo es posible verlas antes del filtrado y cómo reacciona una vez se aplica la configuración

- Facebook

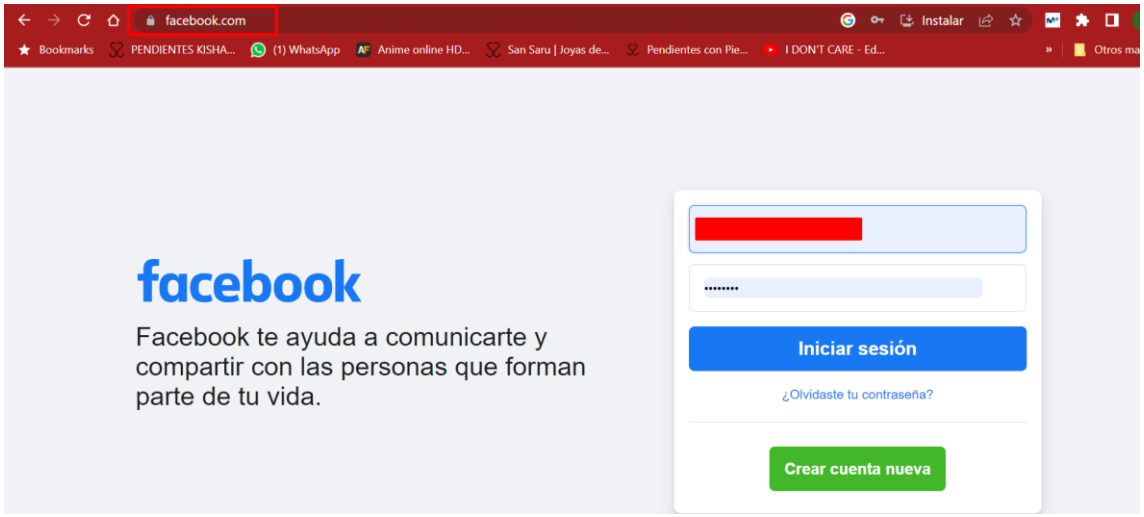


FIGURA 69. EJEMPLO VISUALIZACIÓN FACEBOOK

- Twitter

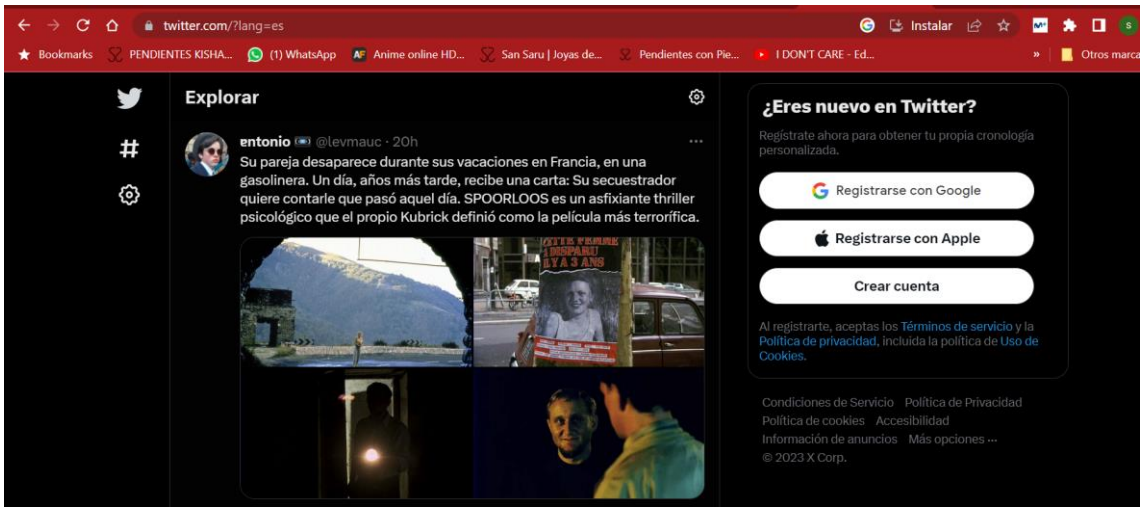


FIGURA 70. EJEMPLO VISUALIZACIÓN TWITTER

3.4.1.3 Ataque por contenido

Para la demostración se intentará visualizar la dirección "http://www.edu4java.com/es/web/web30.html" mostrar cómo es posible verlas antes del filtrado y cómo reacciona una vez se aplica la configuración

FIGURA 71. EJEMPLO VISUALIZACIÓN PÁGINA HTTP

3.4.2 Defensa (FortiGate)

Se procederá a la utilización de diferentes configuraciones para la resolución de los diferentes "ataques" para ver la respuesta del dispositivo y funcionamiento del filtrado

3.4.2.1 Filtrado por URL

Se procede a **bloquear** el acceso vía **HTTP** a URL "estática", de manera que pueda verse como **no es posible acceder a ella**.

1. Se procede a configurar el filtrado por URL estático

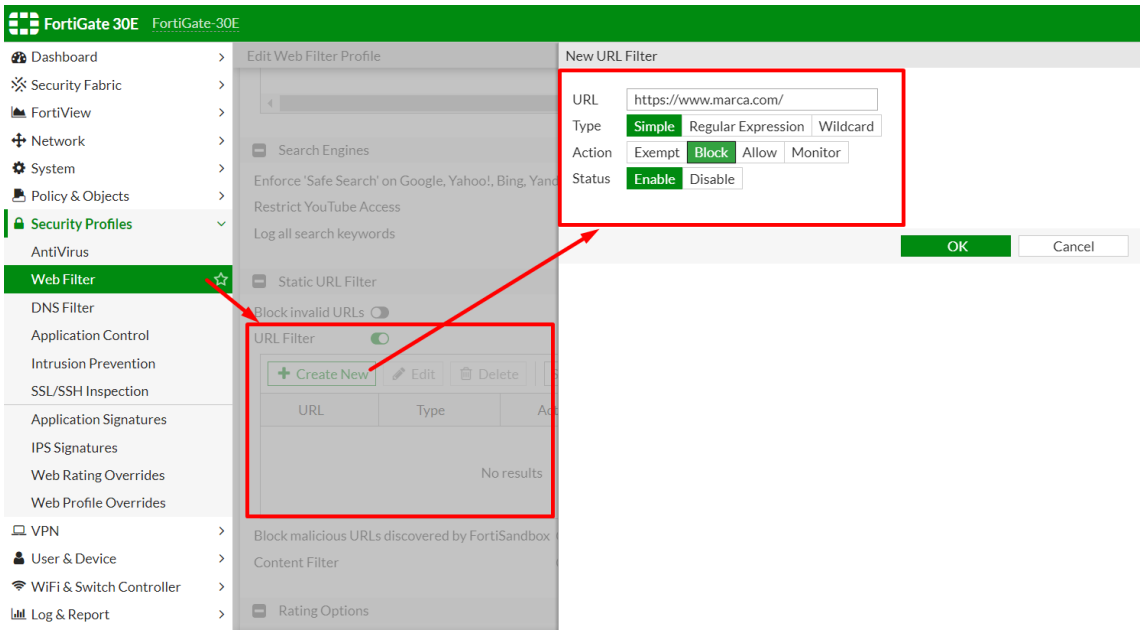


FIGURA 72. VENTANA CONFIGURACIÓN URL ESTÁTICA

2. Se configura el security profile creado en la política a utilizar para la prueba

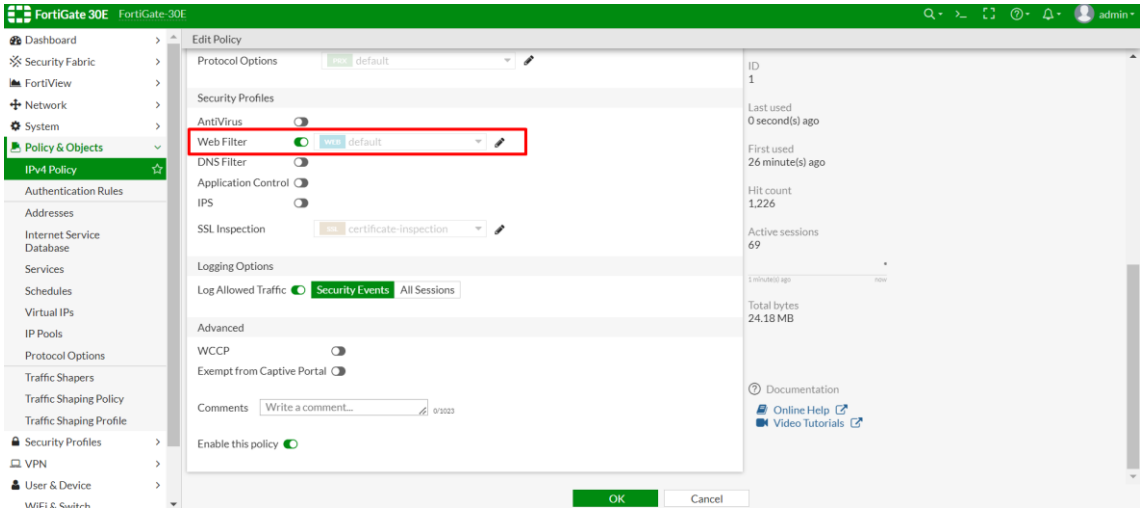


FIGURA 73. VENTANA APLICANDO WEB FILTER A LA POLÍTICA DE TRAFICO

3. Se procede a acceder via web hacia la dirección "www.marca.com" para la comprobación del bloqueo de pagina

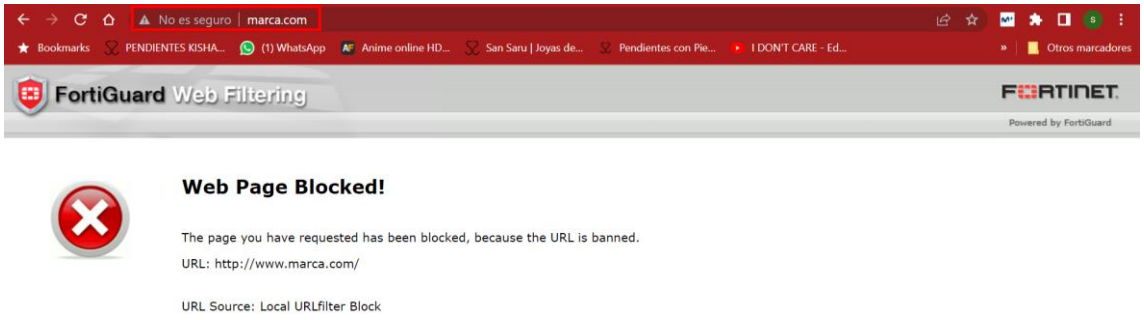


FIGURA 74. EJEMPLO PÁGINA BLOQUEADA DE MARCA FORTIGATE

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, es posible realizar un **seguimiento** detallado a través del **registro de eventos (log).**

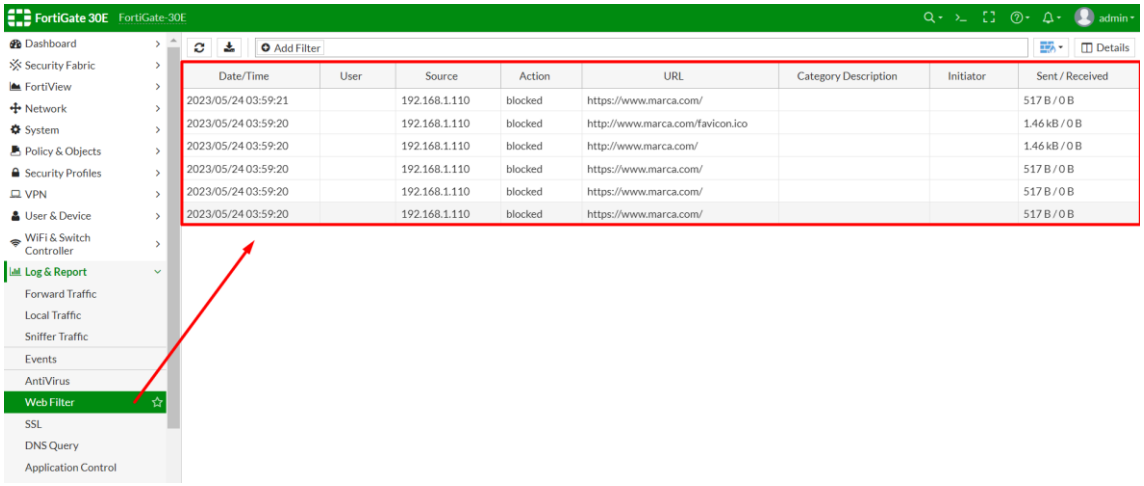


FIGURA 75. VENTANA LOG WEB FILTER ENTRADAS URL ESTÁTICAS

3.4.2.2 Filtrado por Categorías

Se procede a **bloquear** el acceso vía **HTTP** por **categorías**, manera en la cual posibilita el **bloqueo** de **varias páginas** de determinado "**carácter**" de forma conjunto **facilitando el bloqueo de miles** sin el esfuerzo de filtrar una por una

1. Se procede a configurar el Security Profile acorde a la prueba a realizar

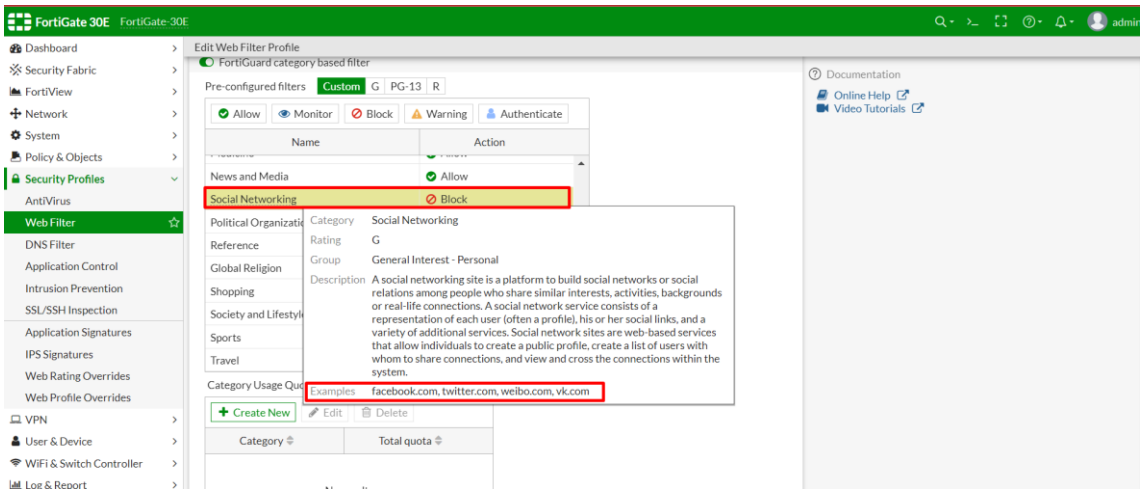


FIGURA 76. VENTANA CONFIGURACION URL CATEGORIAS

2. Se aplica el security profile a la política que hará uso de la prueba

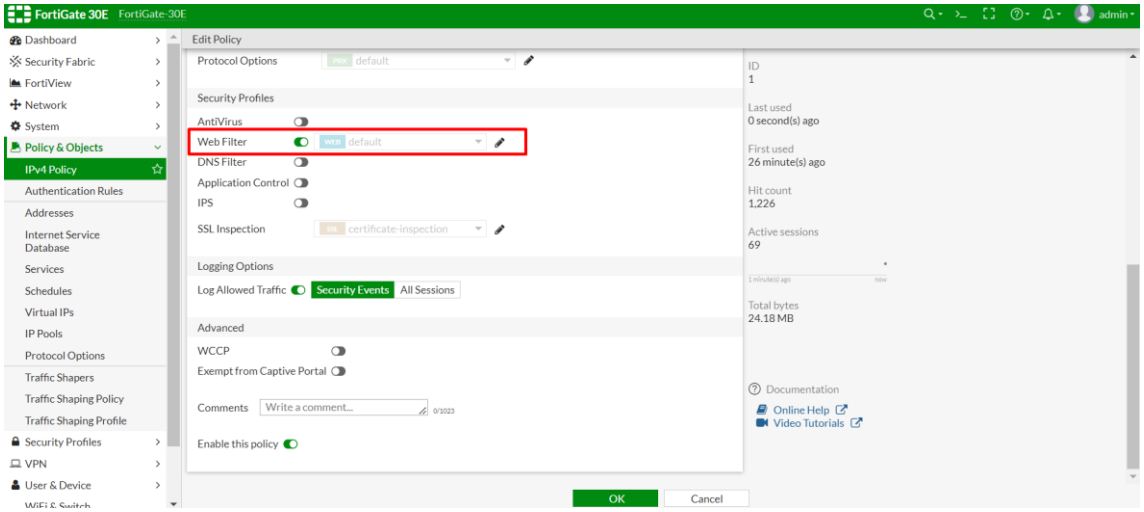


FIGURA 77. VENTANA APLICANDO WEB FILTER A LA POLÍTICA DE TRAFICO

3. Se intenta acceder a las paginas vía "www.facebook.com" y "www.twitter.com" web
    1. Facebook

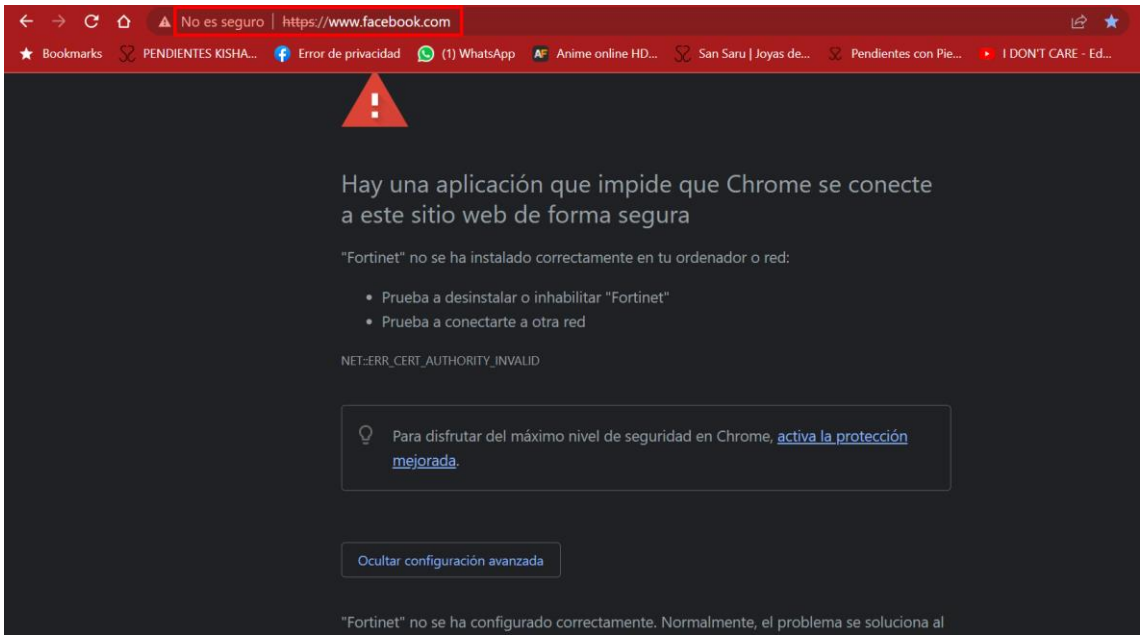


FIGURA 78. EJEMPLO PÁGINA BLOQUEADA DE FACEBOOK FORTIGATE

2. Twitter

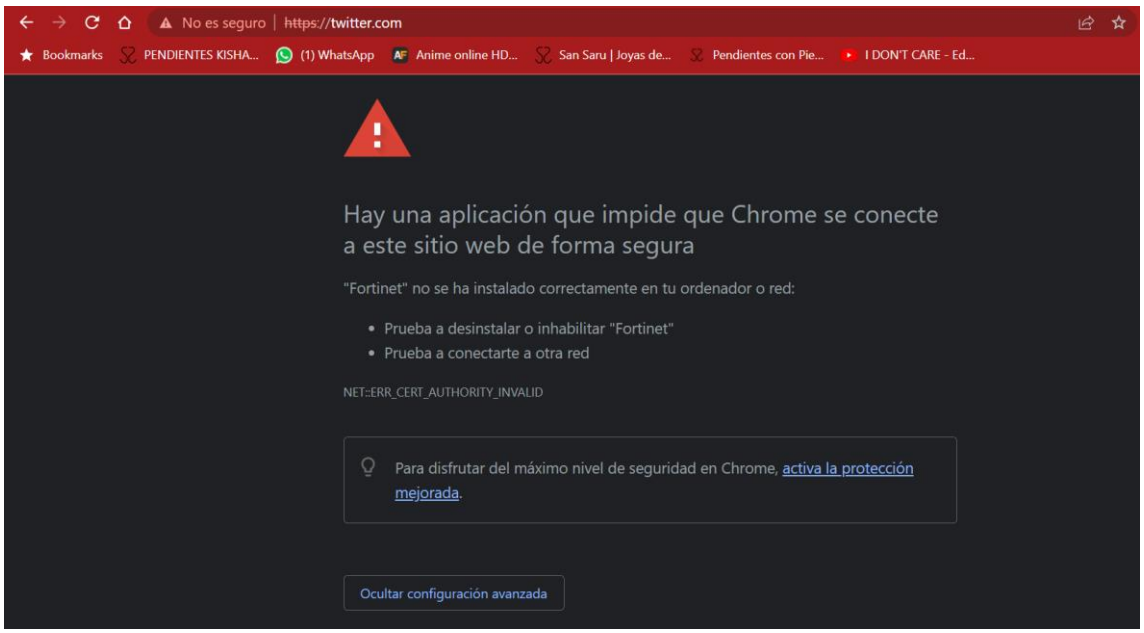


FIGURA 79. EJEMPLO PÁGINA BLOQUEADA DE TWITTER FORTIGATE

Pueda verse que aparece que no es seguro por tema certificado, esto se debe al protocolo HTTPS, siendo FortiGate en modo proxy quien se encarga de ser como el

"intermediario" nuestro navegador no se fia de la página al no poder comprobar ese certificado, además de ser bloqueado por el profile Web Filter

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, es posible realizar un **seguimiento** detallado a través del **registro de eventos (log).**

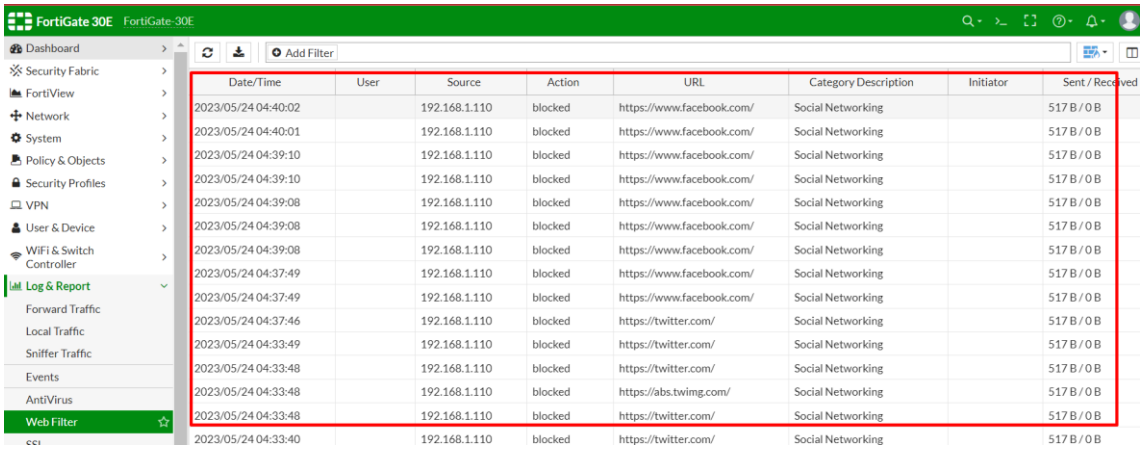


FIGURA 80. VENTANA LOG WEB FILTER ENTRADAS URL CATEGORÍAS

3.4.2.3 Filtrado por Contenido

Se procede a **bloquear** el acceso vía **HTTP** por contenido, manera en la cual posibilita el bloqueo de **varias páginas** de que posean **determinado "patrón"**, este patrón hace **referencia a páginas que posean determinado número de coincidencias**, las cuales en ese se pueden bloquear

1. Se procederá a configurar el Security Profile acorde a la prueba a realizar

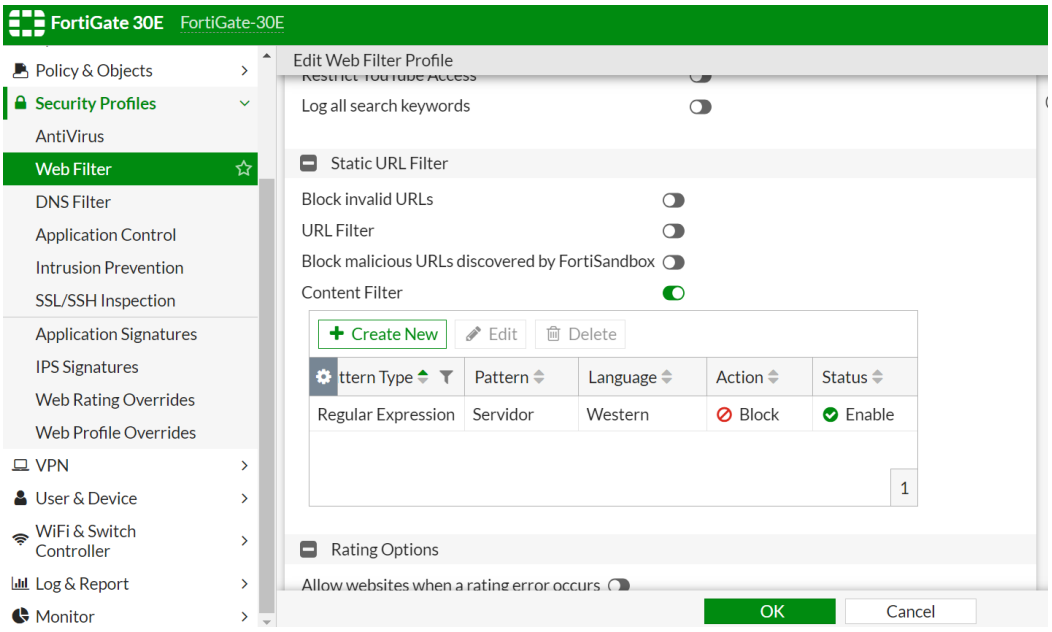


FIGURA 81. CONFIGURACIÓN FORTIGATE URL POR CONTENIDO

2. Se procederá a aplicar el Security Profile a la política en cuestión

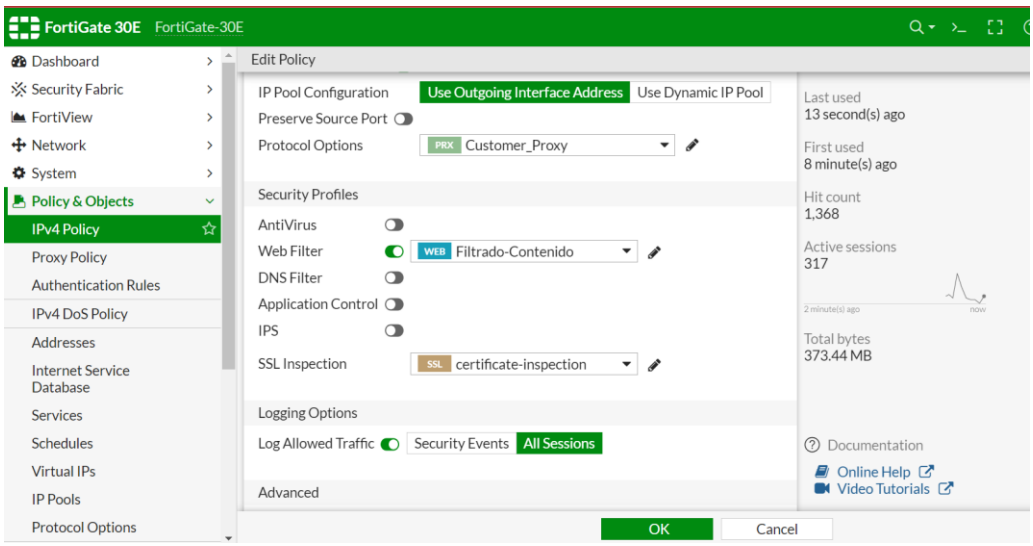


FIGURA 82. APLICAR SECURITY PROFILE DE URL A LA POLITICA DE TRAFICO

3. Visualización del bloqueo

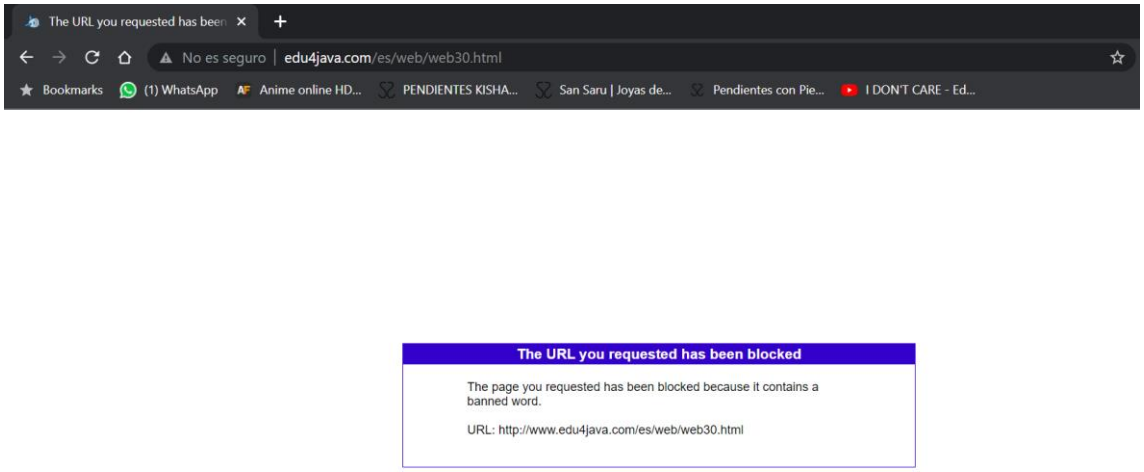


FIGURA 83. EJEMPLO PÁGINA BLOQUEADA DE EDU4JAVA FORTIGATE

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, es posible realizar un **seguimiento** detallado a través del **registro de eventos (log).**

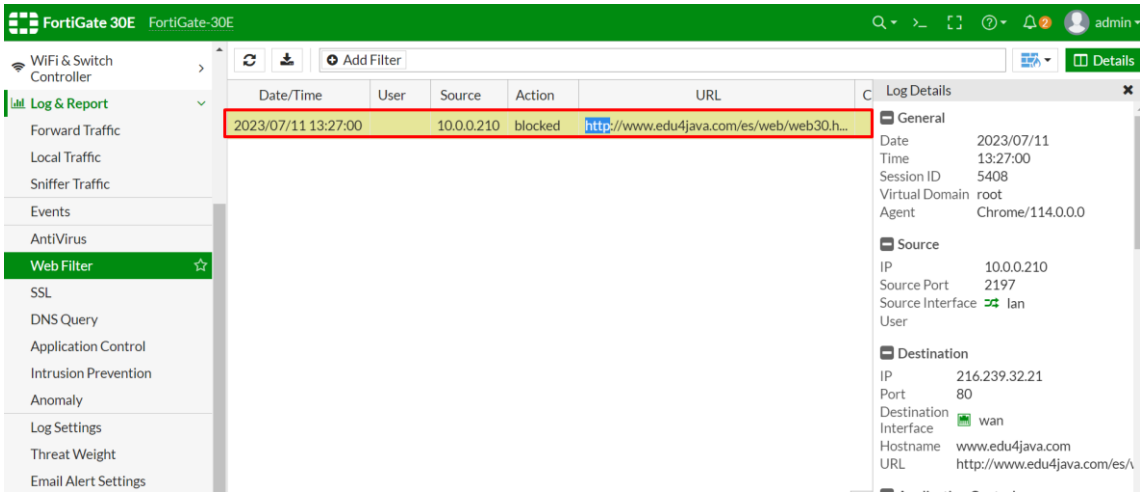


FIGURA 84. VENTANA LOG WEB FILTER ENTRADAS URL CONTENIDO

Desde la vista de detalles es posible aclarar más información del motivo del bloqueo

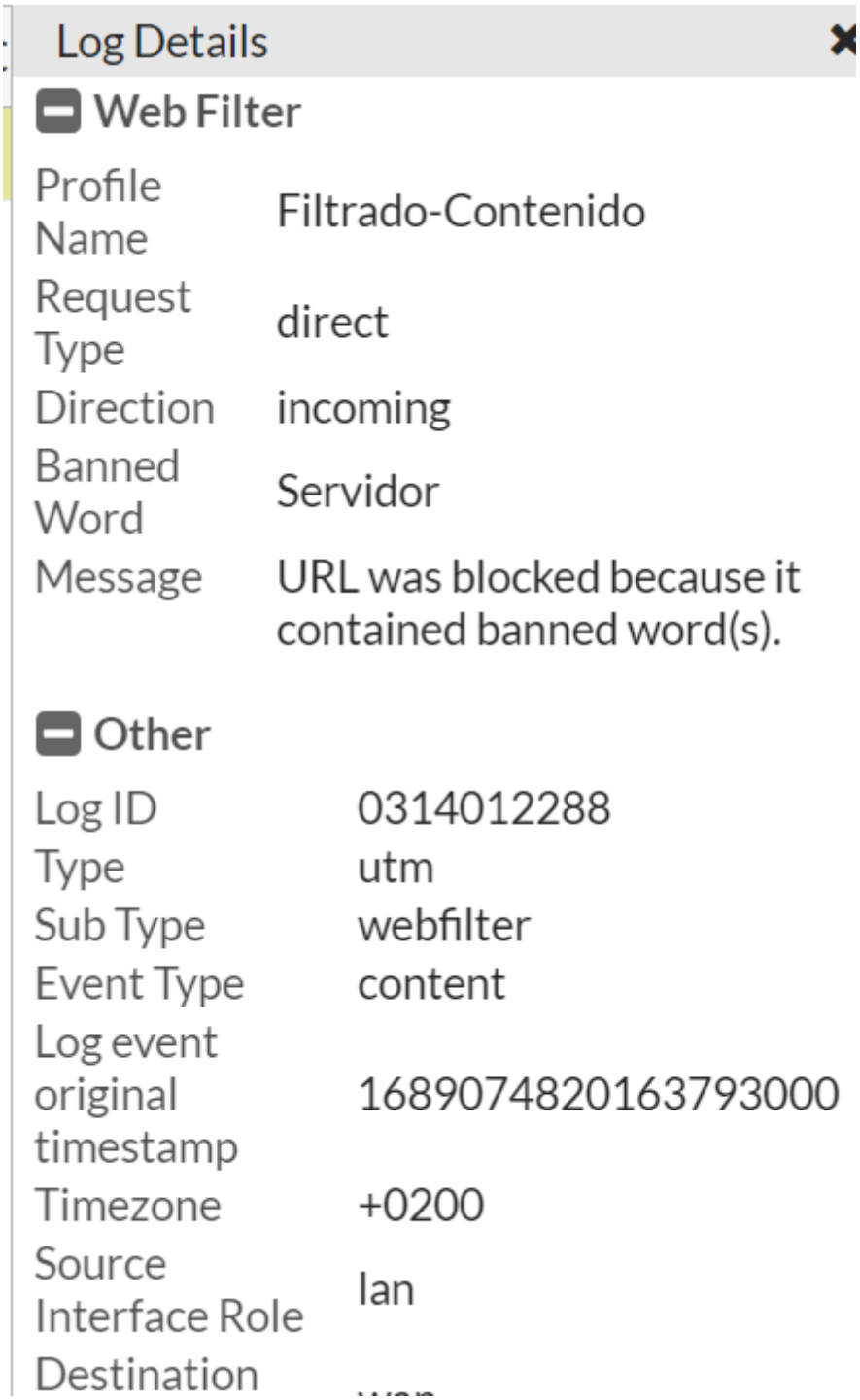


FIGURA 85. EJEMPLO DETALLE LOG WEB FILTER

3.4.3 Defensa (Hillstone)

procederá a la utilización de diferentes configuraciones para la resolución de los diferentes "ataques" para ver la respuesta del dispositivo y funcionamiento del filtrado

3.4.3.1 Filtrado por URL

Se procede a **bloquear** el acceso vía **HTTP** a URL "estática", de manera que pueda verse como **no es posible acceder a ella**.

1. Se procede a configurar el filtrado por URL estático

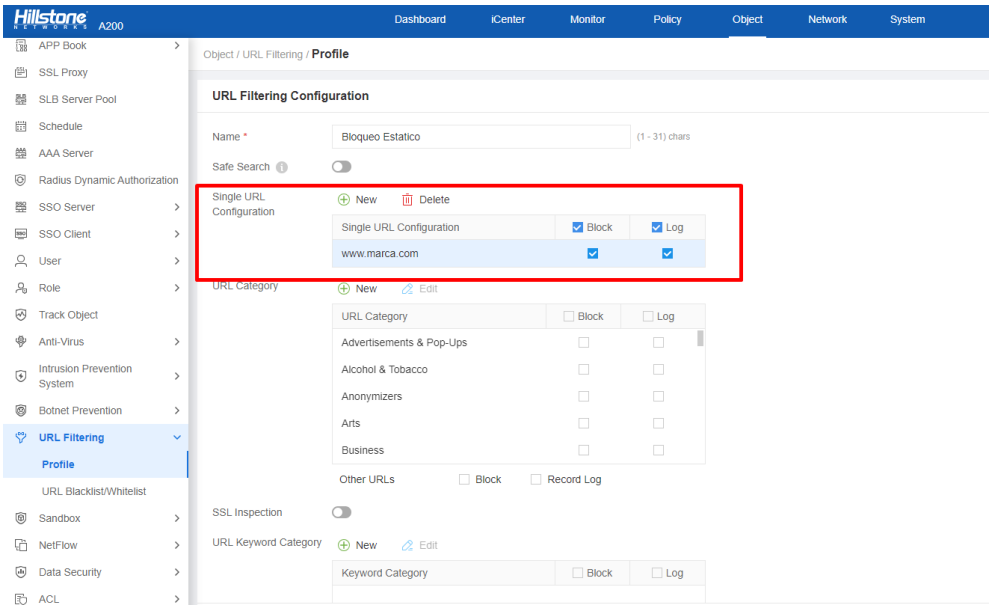


FIGURA 86.CONFIGURACION HILLSTONE URL ESTÁTICA

2. Se aplica la la previa configuración sobre la "policy" de tráfico a aplicar

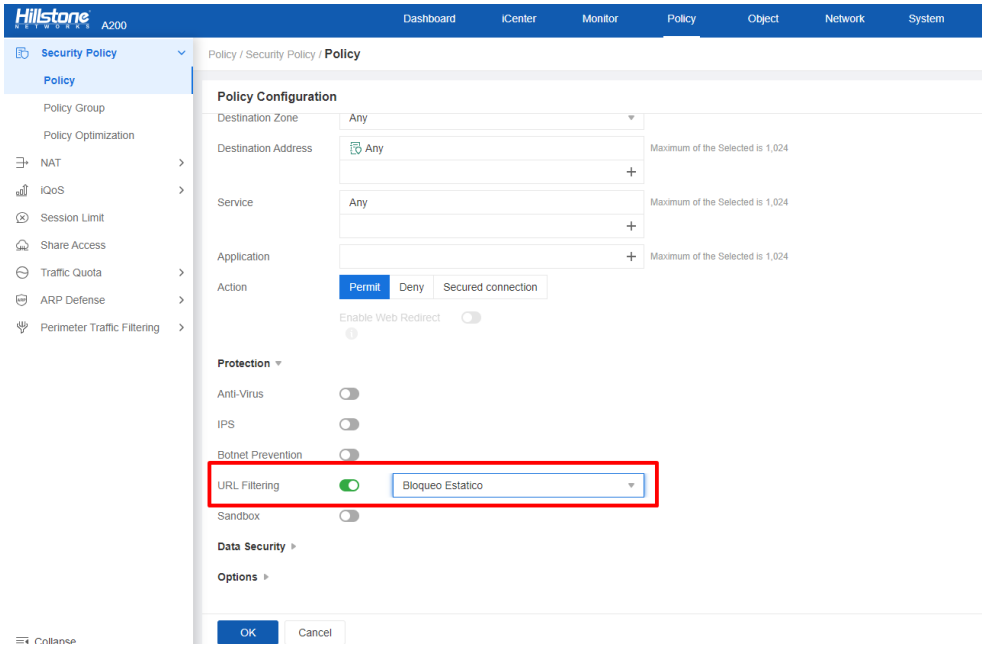


FIGURA 87. APLICA OBJECT BLOQUEO ESTÁTICO A POLÍTICA DE TRAFICO

3. Se procede a acceder via web hacia la dirección "www.marca.com" para la comprobación del bloqueo de pagina

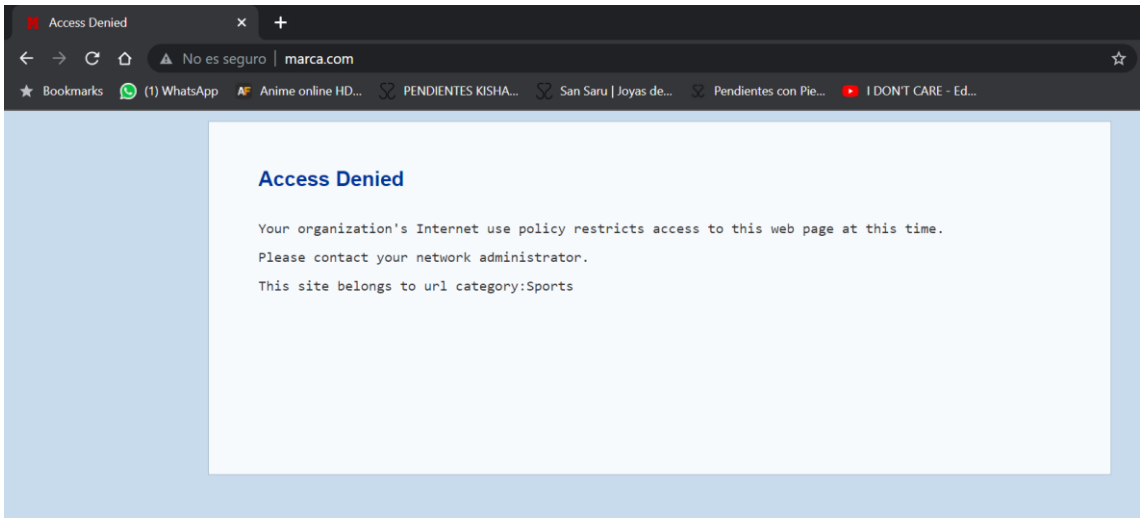


FIGURA 88. MUESTRA DE BLOQUEO DE PÁGINA HTTP MARCA HILLSTONE

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, es posible realizar un **seguimiento** detallado a través del **registro de eventos (log).**

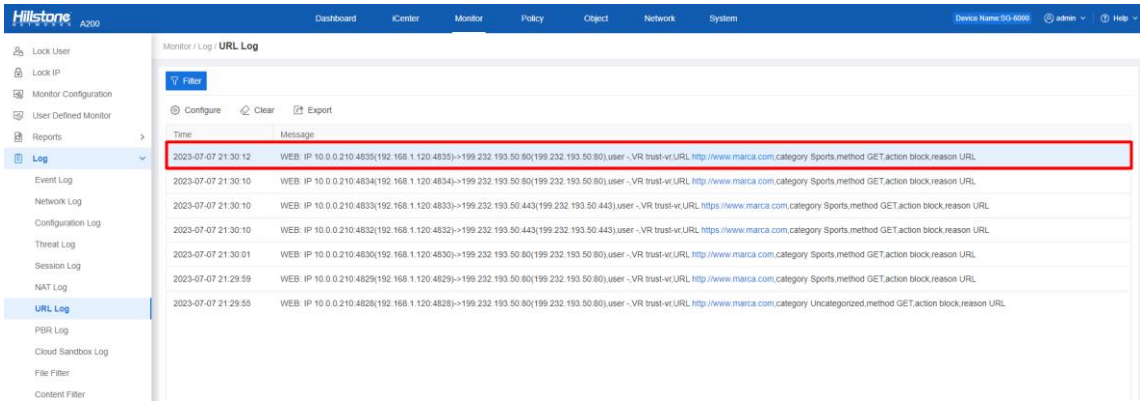


FIGURA 89. LOG HILLSTONE URL ESTÁTICA

3.4.3.2 Filtrado por Categorías

Se procede a **bloquear** el acceso vía **HTTP** por **categorías**, manera en la cual posibilita el **bloqueo** de **varias páginas** de determinado "**carácter**" de forma conjunto **facilitando el bloqueo de miles** sin el esfuerzo de filtrar una por una

1. Se procede a configurar el profile de URL filtering para el bloqueo de las redes

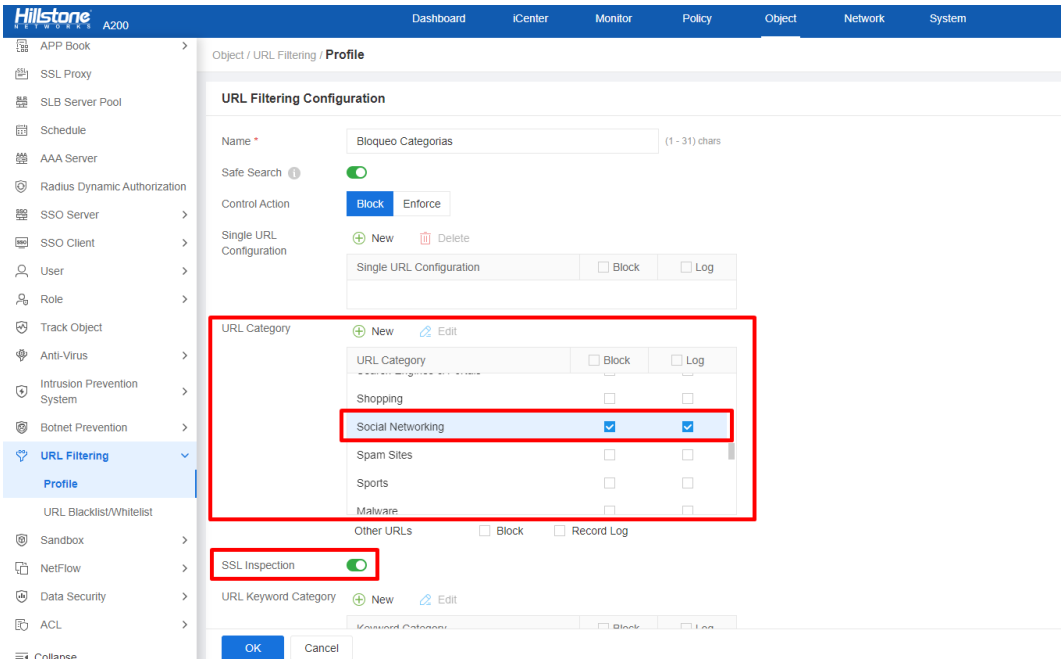


FIGURA 90. CONFIGURACIÓN HILLSTONE URL CATEGORÍAS

2. Se aplicará el profile que se requiera a la política de tráfico a aplicar

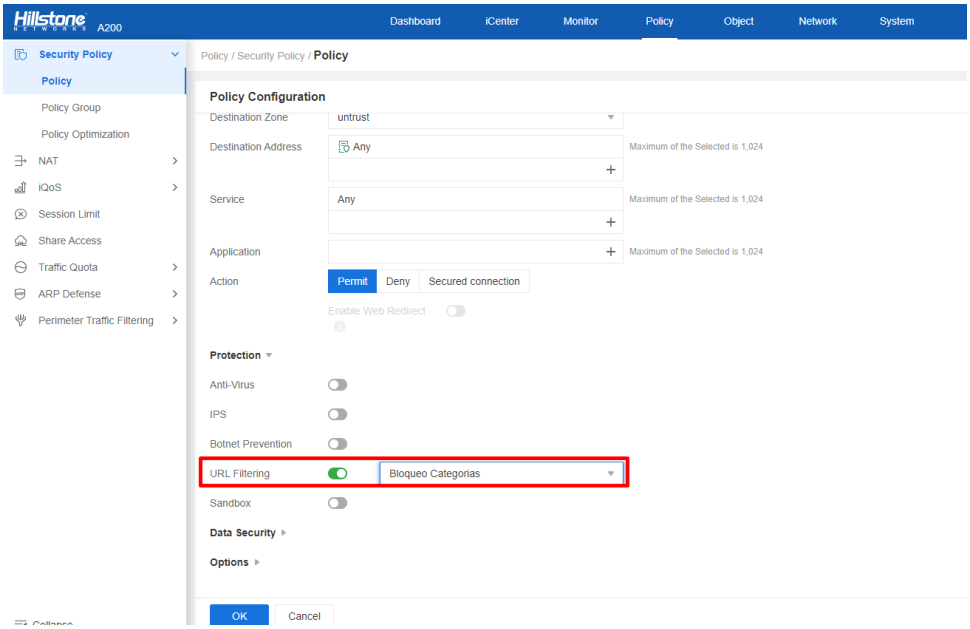


FIGURA 91. APLICAR PROFILE URL A LA POLÍTICA DE TRAFICO

3. Se intenta acceder a las paginas vía "www.facebook.com" y "www.twitter.com" web
    1. Facebook

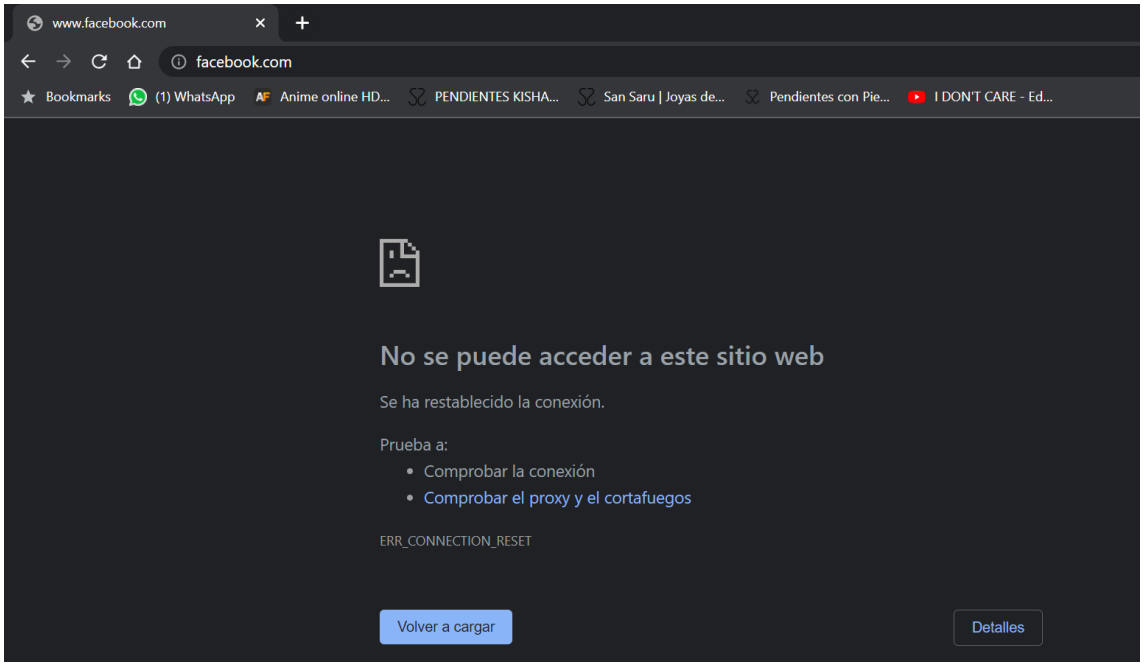


FIGURA 92. MUESTRA BLOQUEO DE PÁGINA FACEBOOK HILLSTONE

2. Twitter

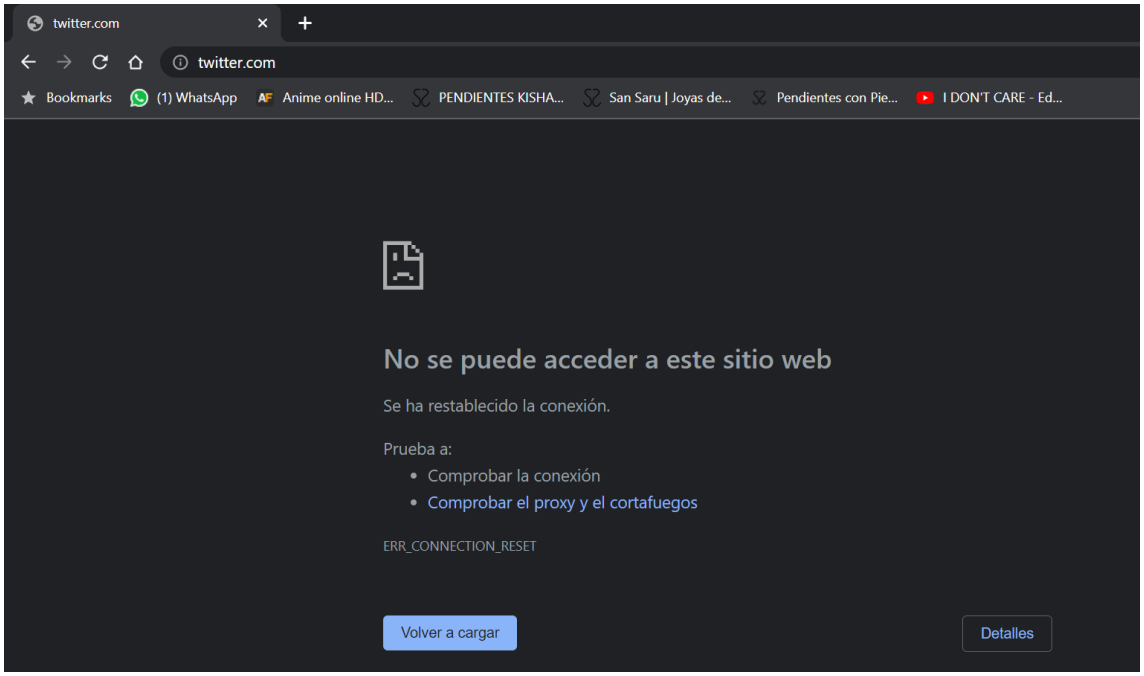


FIGURA 93. MUESTRA BLOQUEO DE PÁGINA TWITTER HILLSTONE

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, se realiza un seguimiento de las acciones tomadas desde el **log**

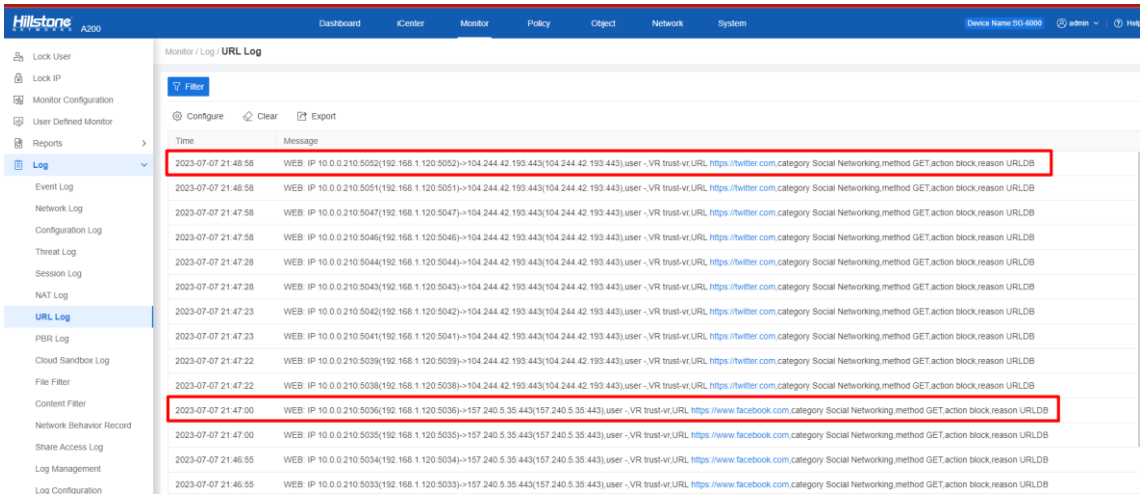


FIGURA 94. VENTANA LOG ENTRADAS URL CATEGORÍAS HILLSTONE

3.4.3.3 Filtrado por Contenido

Se procede a **bloquear** el acceso vía **HTTP** por contenido, manera en la cual posibilita el bloqueo de **varias páginas** de que posean **determinado "patrón"**, este patrón se basa en una coincidencia la cual puede ser ajustada entre 10 – 100, con 100 se afina que la coincidencia sea exacta mientras que a menor numeración más "libertad" se le da a la coincidencia de que se parecido o no exactamente así escrito

1. Se procederá a configurar el profile de URL filtering por contenido

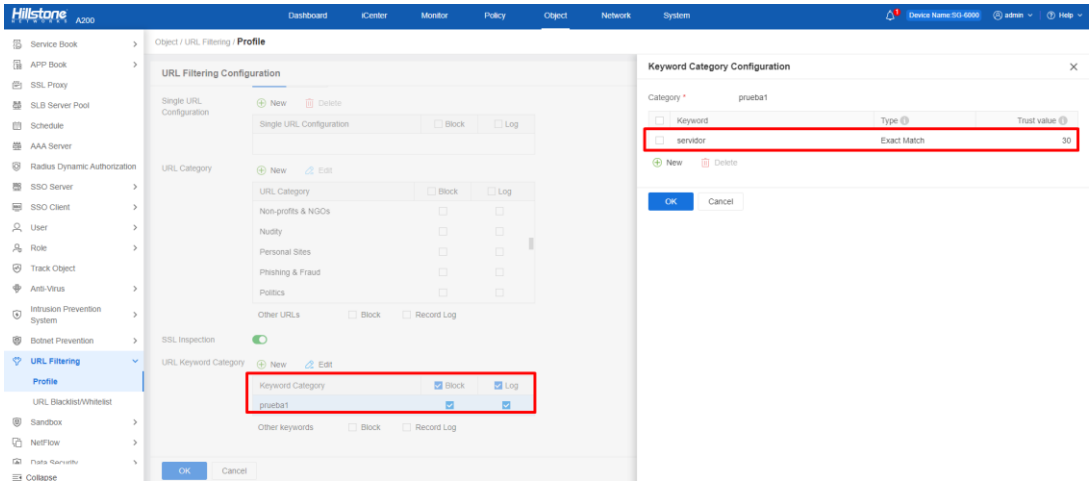


FIGURA 95. CONFIGURACIÓN HILLSTONE URL POR CONTENIDO

2. Se aplicará a la política de tráfico a filtrar, debe aplicarse ambos o no se termina de aplicar bien

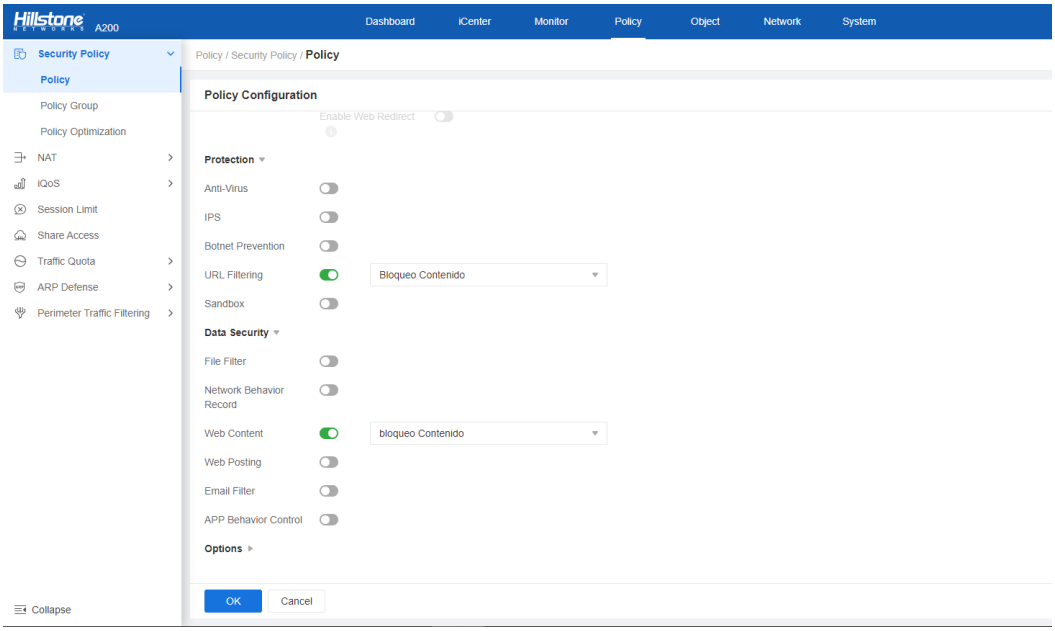


FIGURA 96. APLICAR EL PROFILE DE CONTENIDO DE URL A LA POLÍTICA DE TRAFICO

3. Muestra de intento de acceso vía web y bloqueo

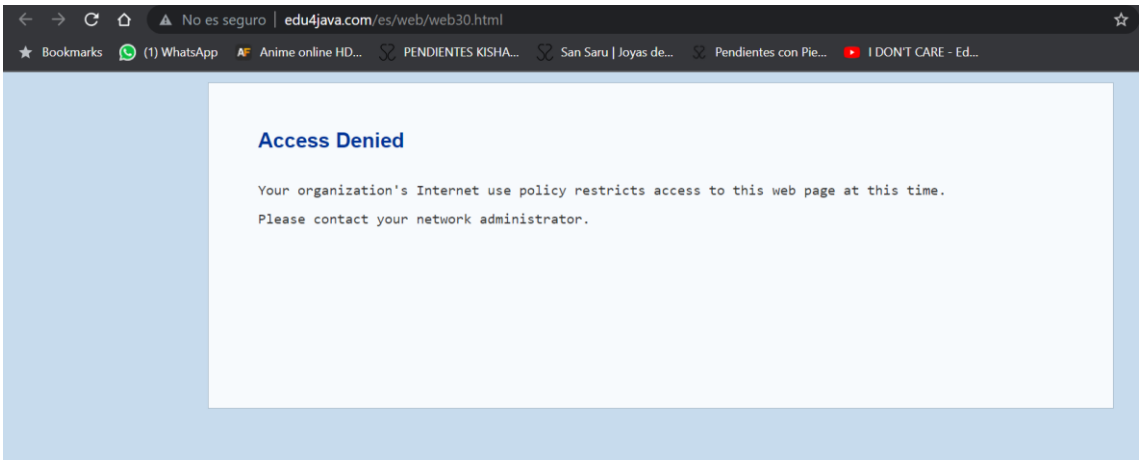


FIGURA 97. EJEMPLO PÁGINA BLOQUEADA DE EDU4JAVA HILLSTONE

Con el fin de facilitar una **visualización más completa** de los **eventos** y **actividades** relacionados con los intentos de **acceso y bloqueo**, se realiza un seguimiento de las acciones tomadas desde el **log**

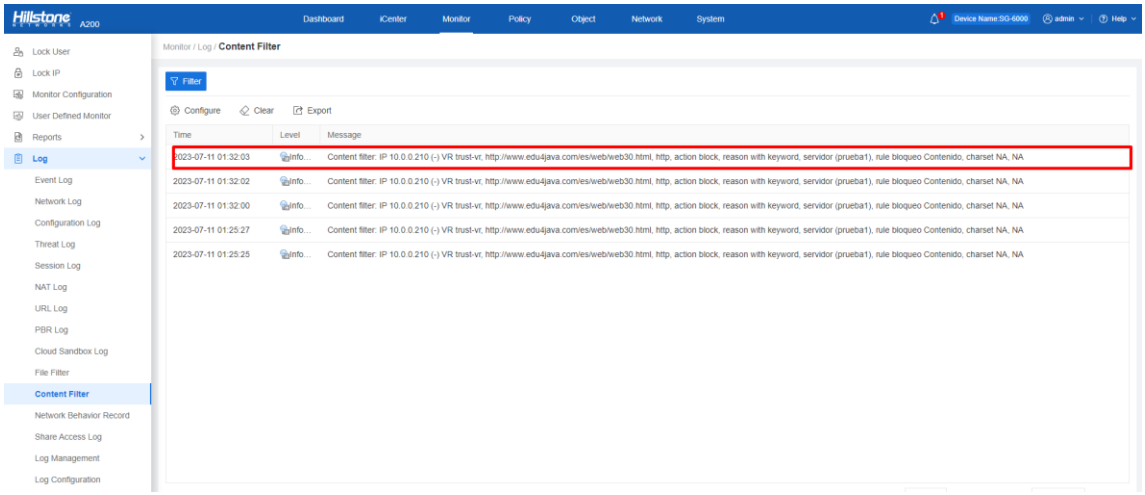


FIGURA 98. VENTANA LOG ENTRADAS URL CONTENIDO HILLSTONE

3.4.4 Discusión

Ambos dispositivos bloquean el tráfico URL a la mayor diferencia es en el tema de contenido donde Hillstone busca una exactitud con una palabra a través de un % de exactitud de parecido con esa palabra y FortiGate sumando un score a través de coincidencias encontradas antes de aplicar una acción

3.5 C2

3.5.1 Ataque

Mediante el uso de una **herramienta** de Kali Linux se realizará un "ataque" para prueba de detección de **command and control** de los dispositivos firewalls de las pruebas, aplicando "**determinada**" **configuración** se intentará **"capar" todo lo posible** para una **mayor visualización** de si el dispositivo es **capaz de detectarlo y filtrar**

Ataque basado en **infección** de un **dispositivo** y **comunicación** de la "victima" y el "servidor" **mediante comandos** a través de un firewall el cual se **analizará** para ver si es **capaz de detectar comunicación entre dispositivos** de la botnet con el servidor

Mediante la herramienta/Framework se pretende realizar una **prueba de penetración y hacking ético**, para ello se procederá a la **preparación** de la "**herramienta**" a usar

1. Se instala y accede a su versión web, se procederá a crear un usuario ya que se entra por primera vez

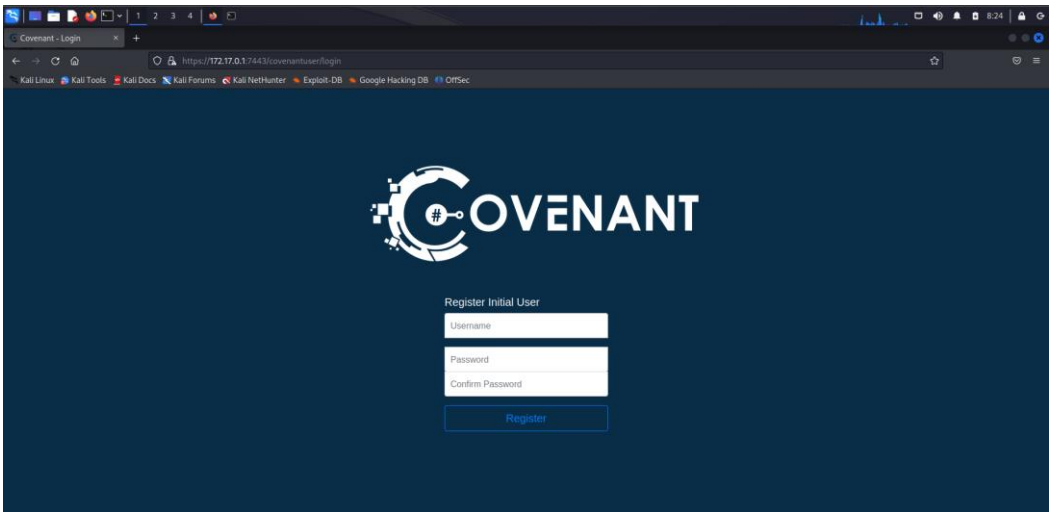


FIGURA 99. VENTANA REGISTRO COVENANT

2. Se procederá a configurar el listener por donde se recibe la comunicación con la botnet

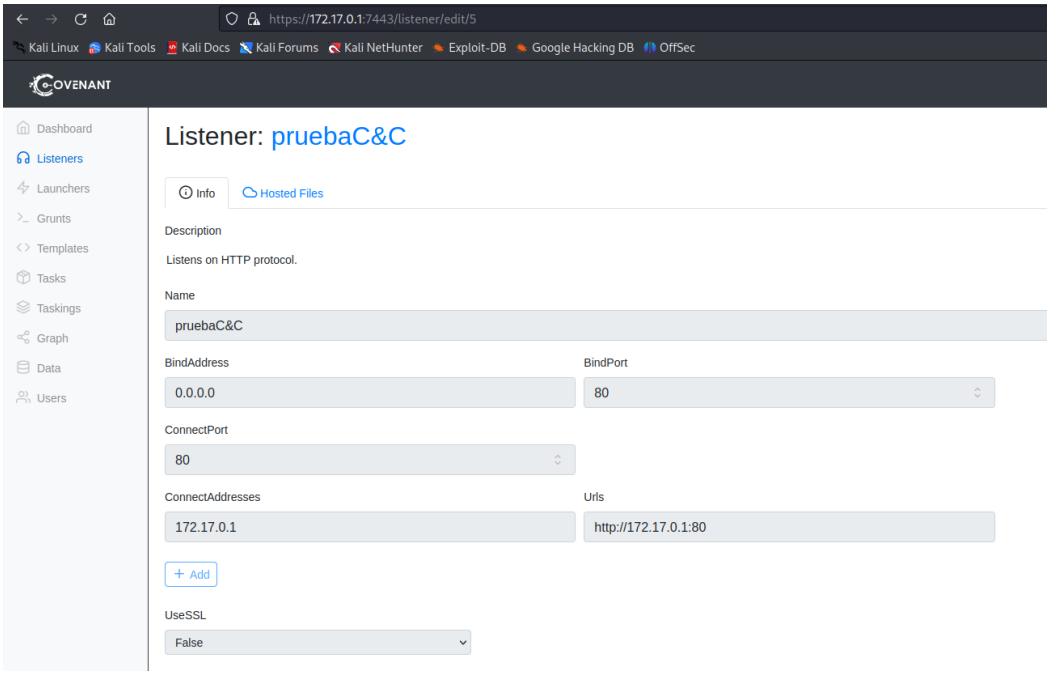


FIGURA 100. CREACIÓN LISTENER PARA BOTNET

3. Se procederá a la generación del comando/virus que agregará al PC victima a la red botnet

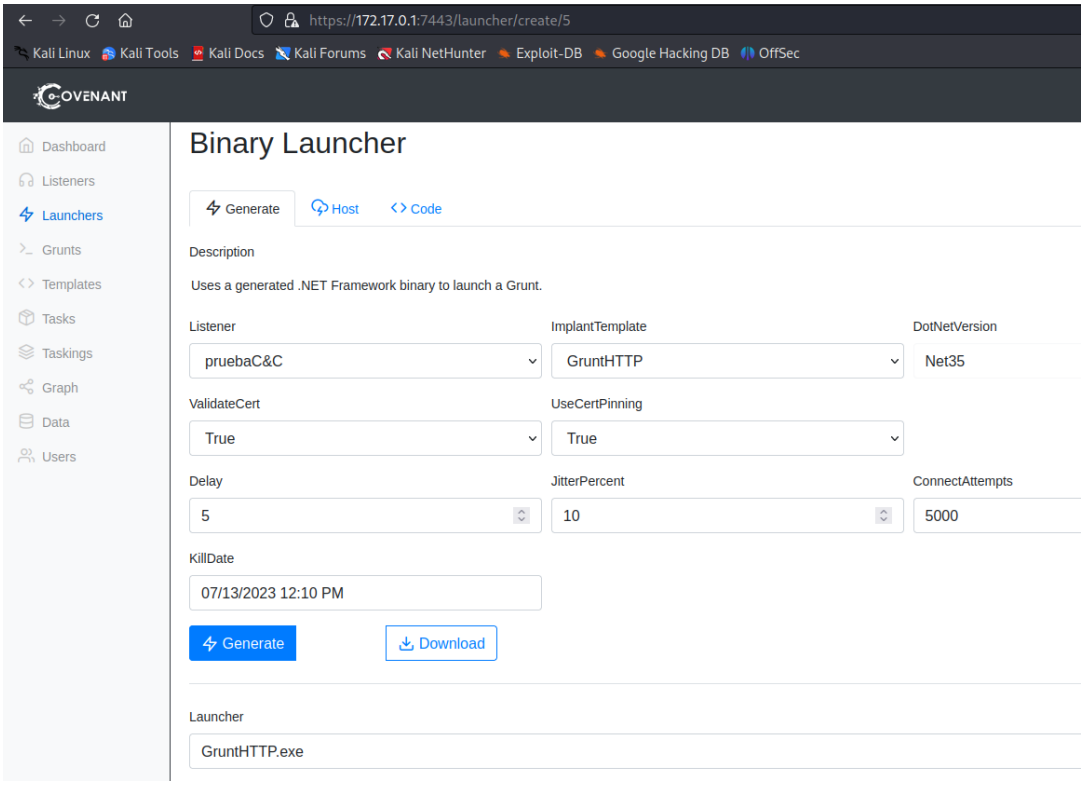


FIGURA 101. CREACIÓN LAUNCHER PARA INFECCIÓN DE PC VICTIMA

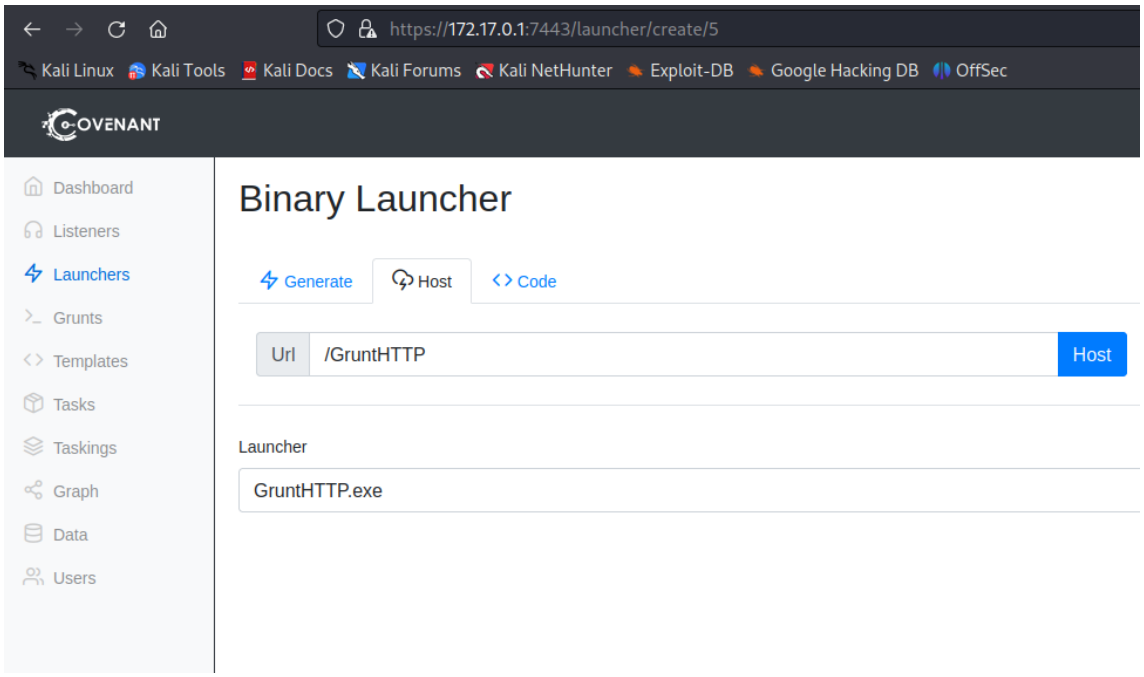


FIGURA 102. DIRECCIÓN DE URL DONDE DESCARGAR FICHERO DE INFECCIÓN

4. Para la prueba la victima procederá a la descarga del “virus”

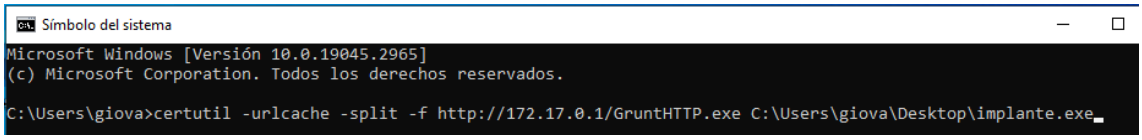


FIGURA 103. EJECUCIÓN COMANDO DESCARGA VIRUS DE INFECCION BOTNET

5. Se ejecutará implante.exe en el PC victima

FIGURA 104. VISTA DE VIRUS DESCARGADO Y EJECUCIÓN

Una vez se tiene el equipo infectado se procederá a la realización de intentos de comunicación para la visualización de los comportamientos de los dispositivos firewall y ver si son capaces de filtrar estas operaciones

Para la prueba de ambos dispositivos se hizo uso de 2 interacciones:

- WhoAmI
- Keylogger 120 seconds

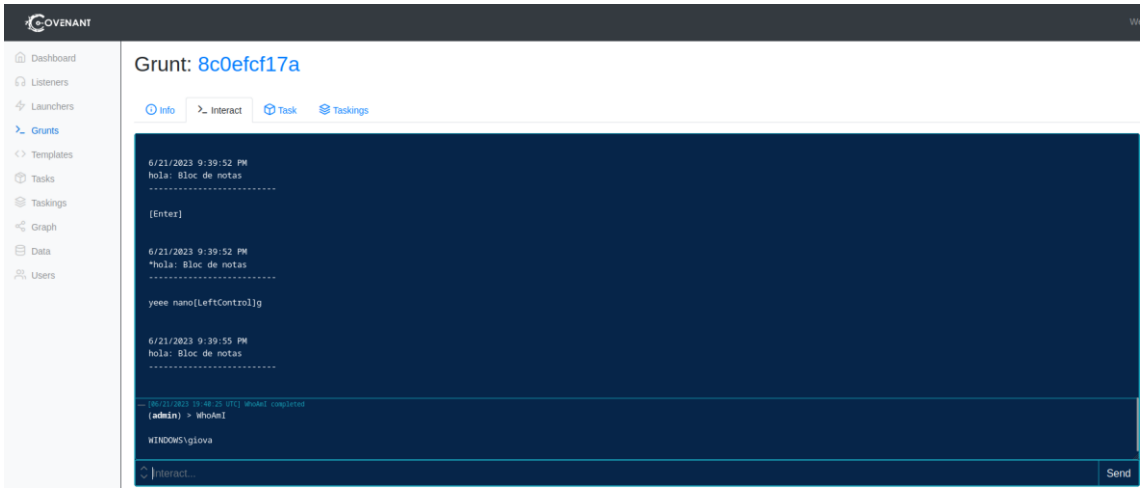


FIGURA 105. VISTA DE ATAQUES REALIZADOS A PC DE LA BOTNET

3.5.2 Defensa (FortiGate)

La configuración a aplicar para la detección de las comunicaciones una vez el equipo ya está infectado será la siguiente:

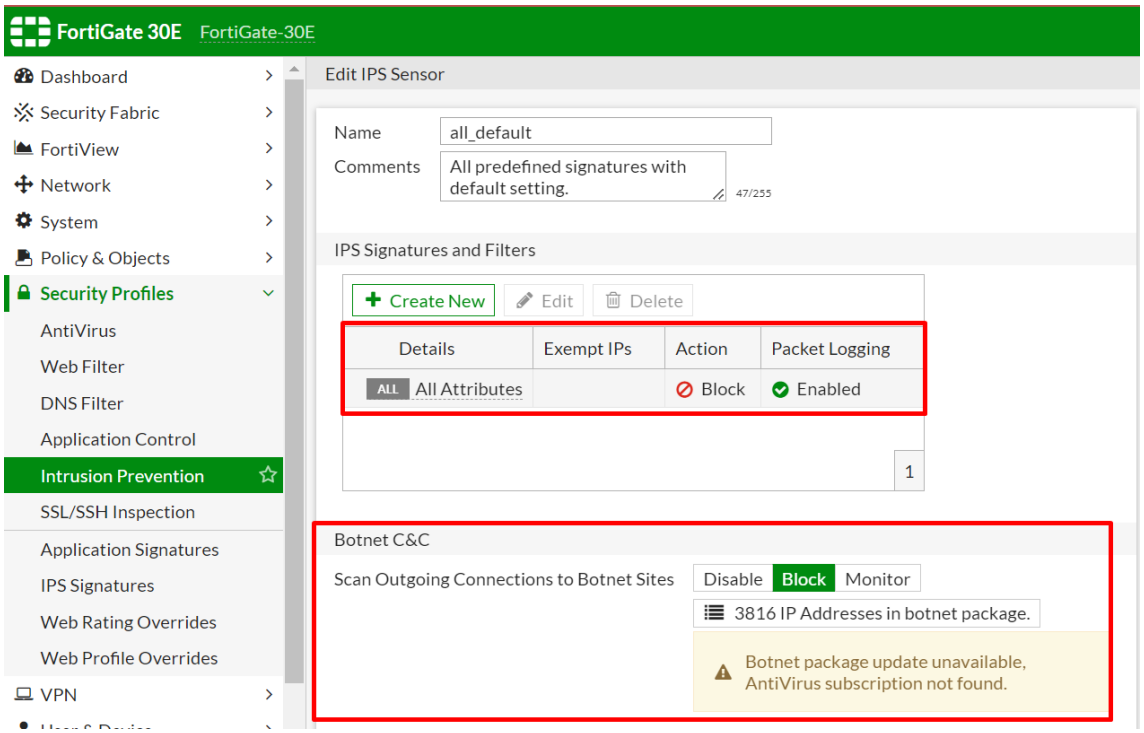


FIGURA 106. BLOQUEO FIRMAS Y CONEXIONES SALIENTES A DIRECCIONES IP CONOCIDAS DE BOTNETS

La **opción** de **Botnet C&C** es para cuando las **comunicaciones** vengan directamente de una **dirección IP concreta** que se tenga en la **base de datos**, de la otra manera lo hará por firmas como puede verse en los **logs** de IPS

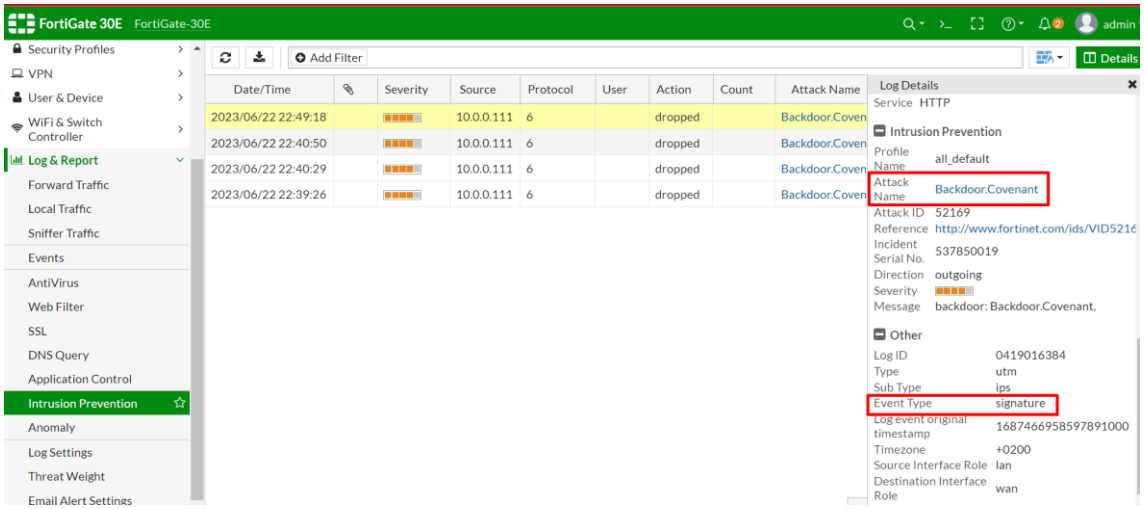


FIGURA 107. LOGS FORTIGATE PRUEBA DE DETECCION DE ENVIO DE DATOS A SERVIDOR BOTNET

3.5.3 Defensa (Hillstone)

Para la detección tanto de los intentos de infección como de las conexiones como del tráfico en general que se comunique con servidores de botnet se procede a tener varias configuraciones

- **AV**: para la detección de código malicioso el cual puede intentar enviarse o descargarse del servidor botnet (comúnmente la infección)

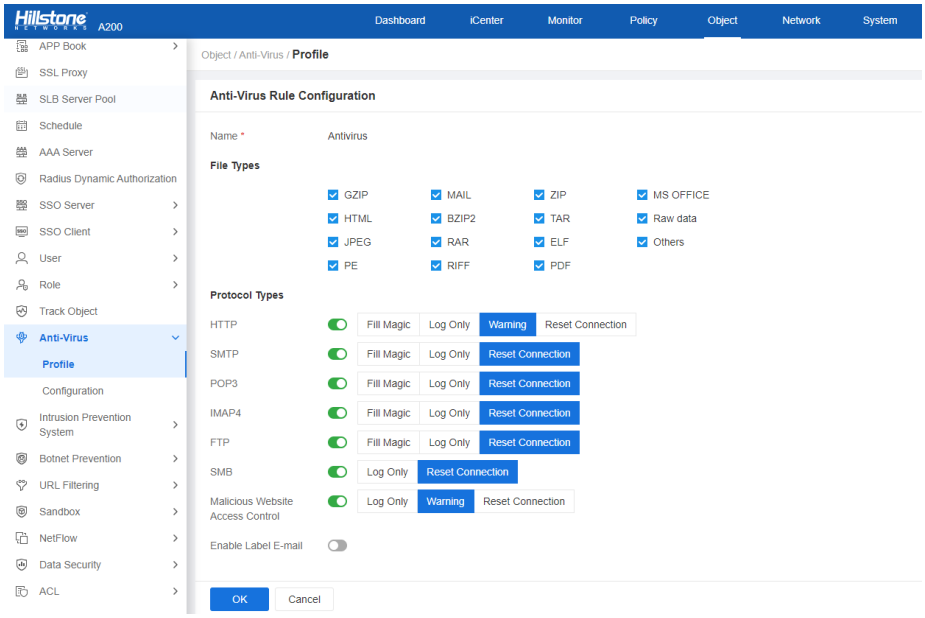


FIGURA 108. CONFIGURACIÓN AV PARA VIRUS DE BOTNETS HILLSTONE

- **Intrusion Prevention**: la cual tiene las firmas de ataques a nivel de aplicación conocidas hacia los diferentes protocolos

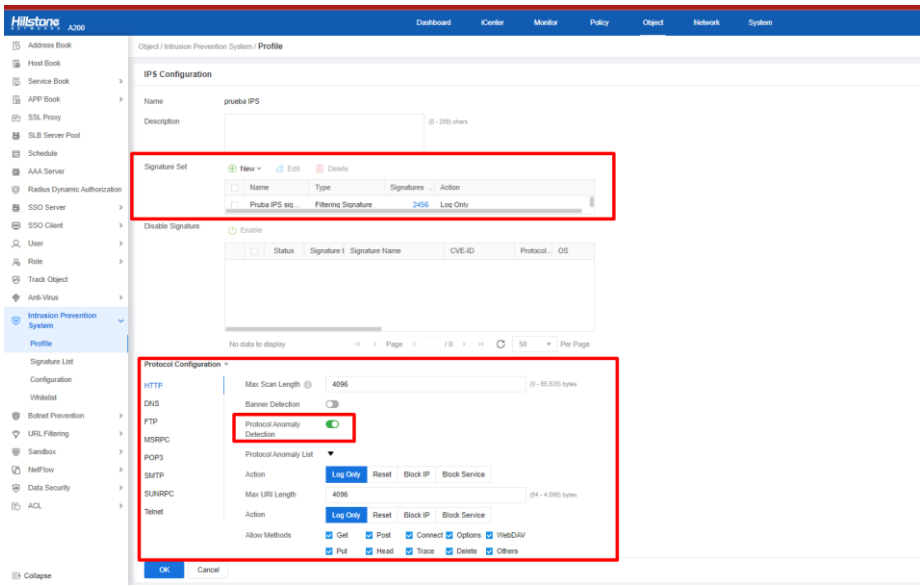


FIGURA 109. CONFIGURACIÓN IPS PARA FIRMAS Y DETECCIÓN ANÓMALO SOBRE PROTOCOLO PARA BOTNET

- **Botnet prevention**: para la detección de conexiones entrantes y salientes bajo los protocolos TCP, HTTP, DNS principalmente y la detección de Túneles en DNS y algoritmo de generación de dominós (DGA)

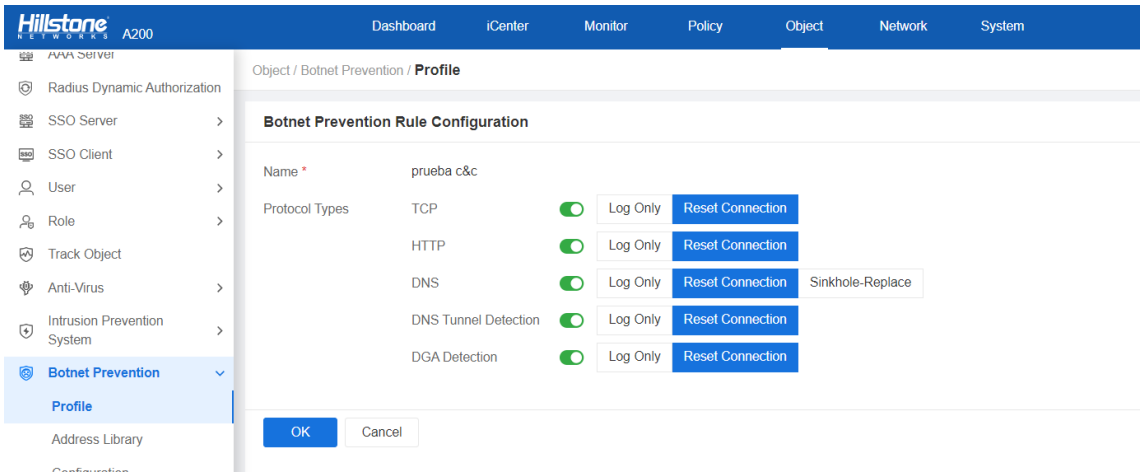


FIGURA 110.CONFIGURACIÓN BOTNET PARA DETECCIÓN TÚNELES, DOMINIOS Y SOBRE PROTOCOLOS HILLSOTNE

Se cuenta con una base de datos la cual tiene direcciones conocidas de botnet para no aceptar conexiones de esas direcciones

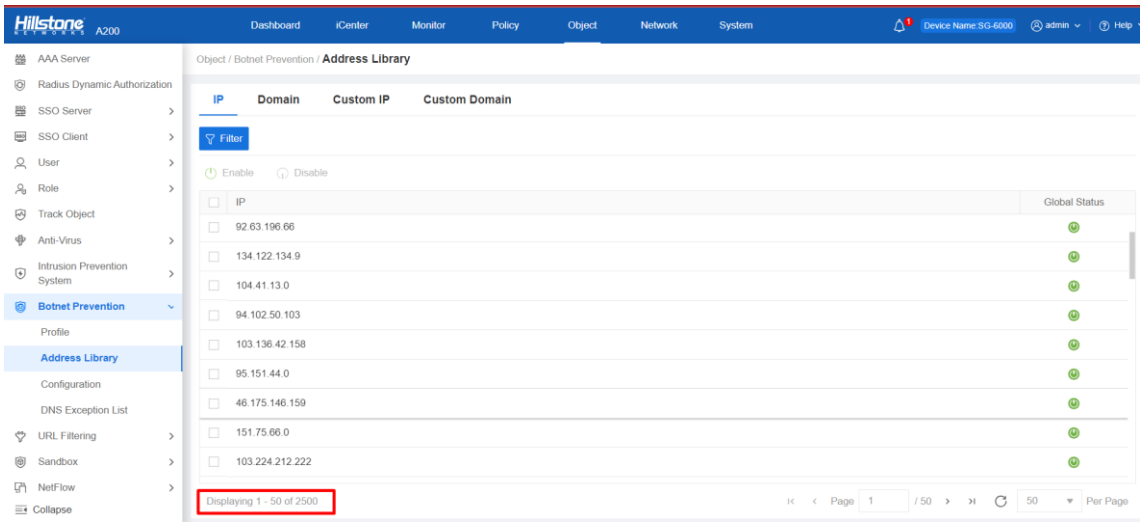


FIGURA 111. VENTANA DIRECCIONES IP DE SERVIDORES DE BOTNET CONOCIDOS

3.5.4 Discusión

Hillstone no fue capaz de detener el ataque de BotNet debido a la falta de firma de ataques y a que el dispositivo no ha estado reconociendo los ataques realizados una vez ya infectado el PC victima como nada anómalo y una conexión normal, esto se debe a la falta de la firma que identifica el “ataque”

FortiGate no ofrece una configuración más exacta/avanzada para configurar los distintos tipos de conexiones que se pueden utilizar para la detección de botnets como DNS túneles o DGA. Hillstone permite mayor nivel de configuración para los ataques de BotNet de forma que nos permite ajustar a más exactitud que accion queremos tomar para el DNS, DNS túneles y DGA

3.6 Sandbox

3.6.1 Ataque

El objetivo del ataque y su prueba de **comprobación** será la prueba de que efectivamente los **ficheros se envían al sandbox de los Firewall**

Se pretende comprobar mediante la **descarga** de un archivo **malicioso** utilizado y en la base de firmas de la mayoría de los dispositivos de seguridad el **EICAT.TXT**, este fichero es **reconocido** por la mayoría de los **AV** y se pretende comprobar que efectivamente lo **envían al sandbox** y después se procede a su bloqueo

3.6.2 Defensa (FortiGate)

Para la prueba se requiere de la activación de FortiSandbox inspection

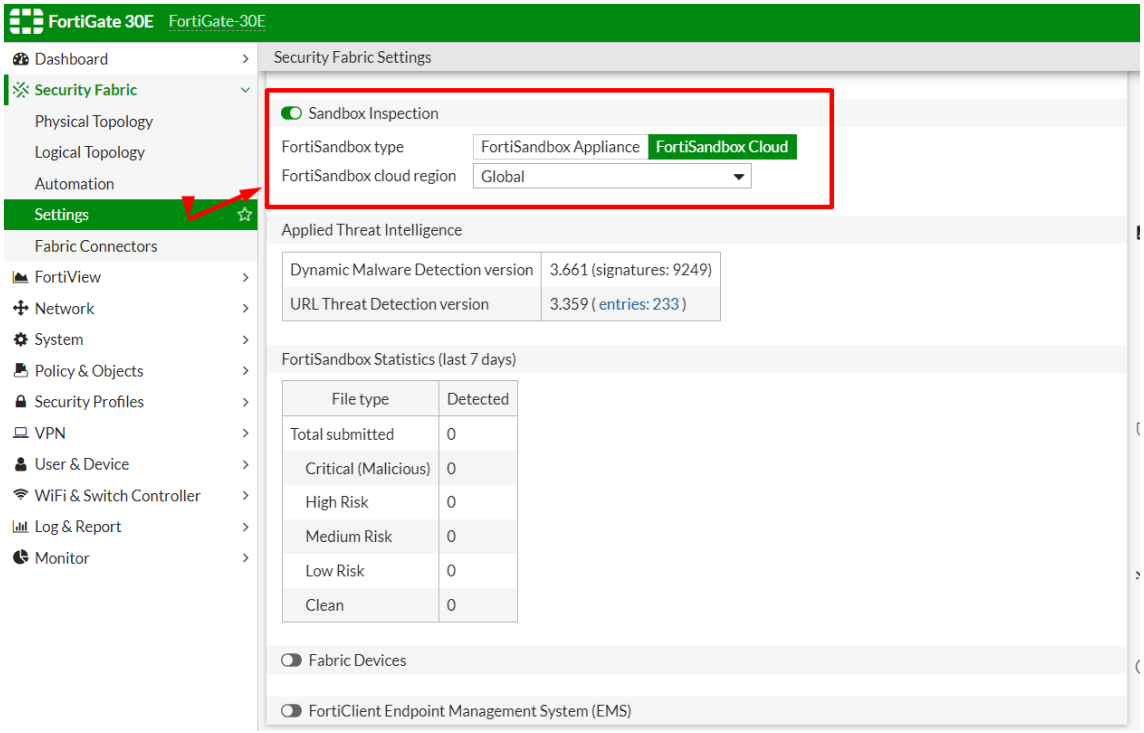


FIGURA 112. VENTANA ACTIVACIÓN SANDBOX FORTIGATE

Se **activará y ajustara la región para su posterior configuración** en el profile del AV para el envió de los ficheros a escanear al sandbox

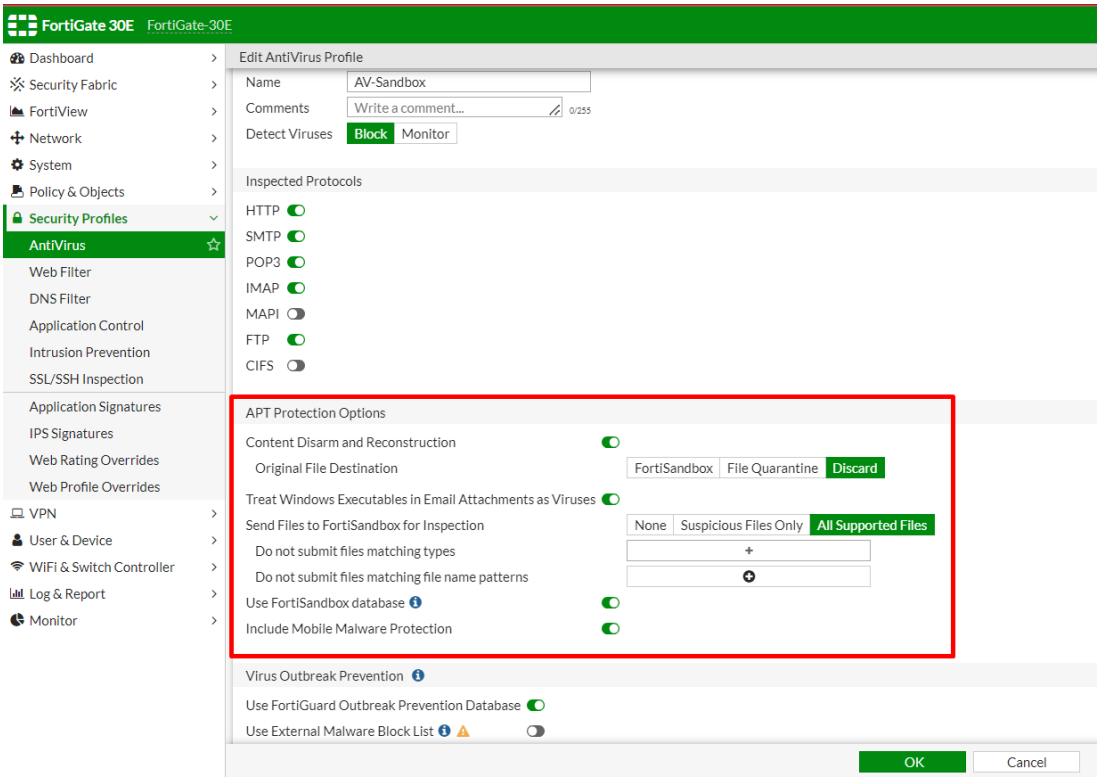


FIGURA 113. CONFIGURACIÓN ENVIÓ DE PAQUETES MALICIOSOS A LA SANDBOX FORTIGATE

Una vez el profile de AV haya sido configurado se procederá a asignarlo a la política de ipv4 correspondiente al tráfico que se quiera analizar y enviar al sandbox

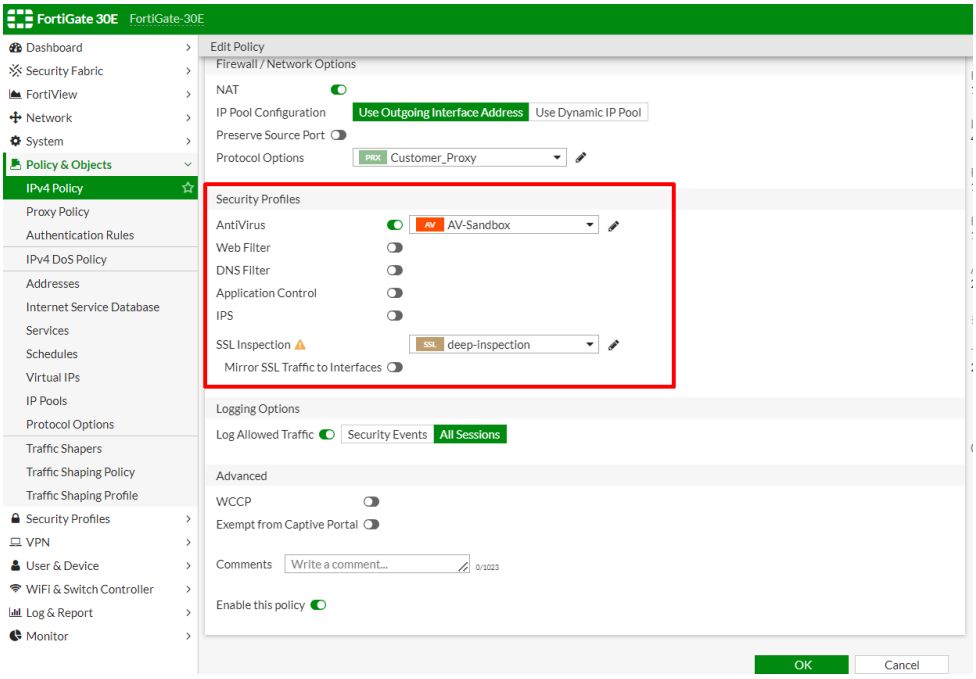


FIGURA 114. APLICACIÓN AV-SANDBOX A LA POLÍTICA A ANALIZAR FORTIGATE

Para la **verificación** de la utilización real del **sandbox** y acción tomada por el firewall se podrá ver desde **el menú de logs del AV**

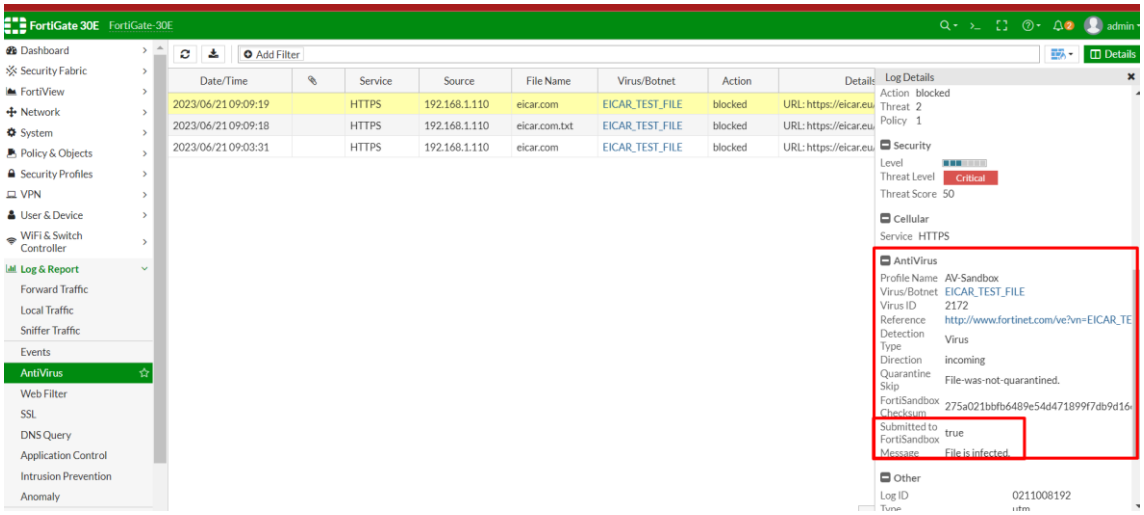


FIGURA 115. LOGS DETECCIÓN VIRUS SANDBOX FORTIGATE

Pueda verse también la **cantidad de ficheros que se han enviado al sandbox** para su análisis

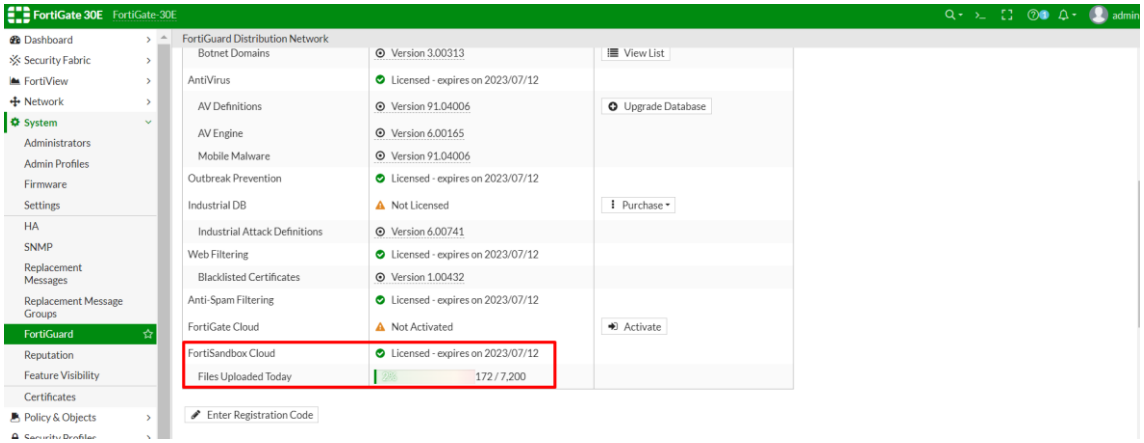


FIGURA 116. VISTA FICHEROS ENVIADOS PARA INSPECCIÓN SANDBOX FORTIGATE

3.6.3 Defensa (Hillstone)

Activada la **licencia** de **sandbox** de Hillstone se procede a **configurar** el **profile** para **analizar** mediante **sandbox** los **tipos de ficheros** PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP y Scripts y **se asignaran los protocolos sobre los que se aplicara el profile**, se ajustaran en ambas direcciones en el que los permita

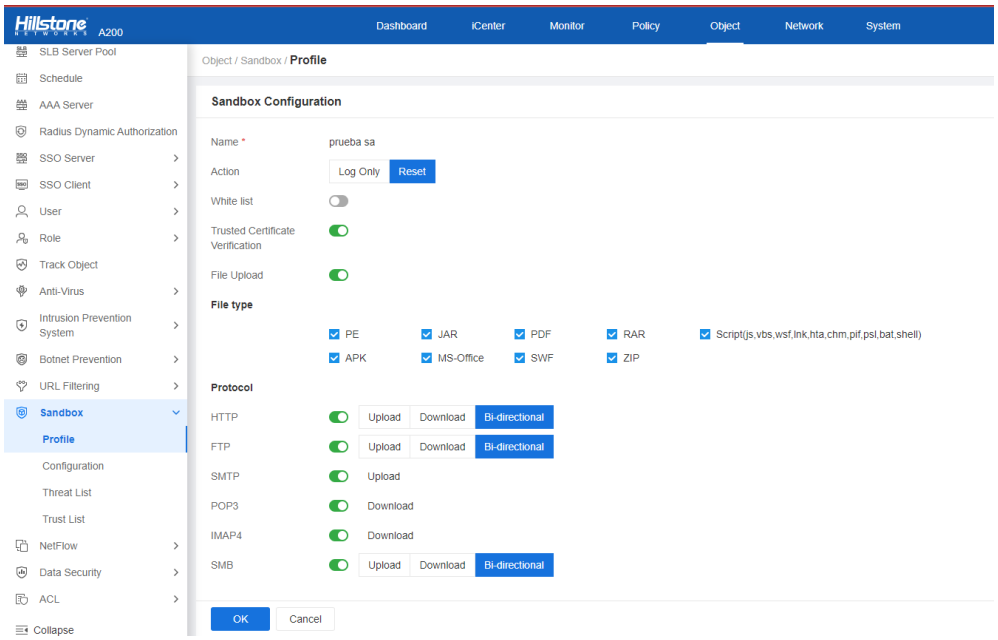


FIGURA 117. CONFIGURACIÓN ENVÍO DE PAQUETES MALICIOSOS A LA SANDBOX FORTIGATE

Ofrece la posibilidad si se requiere la necesidad de ajustar el tamaño de fichero, el límite de lo permitido para subirlo y analizarlo

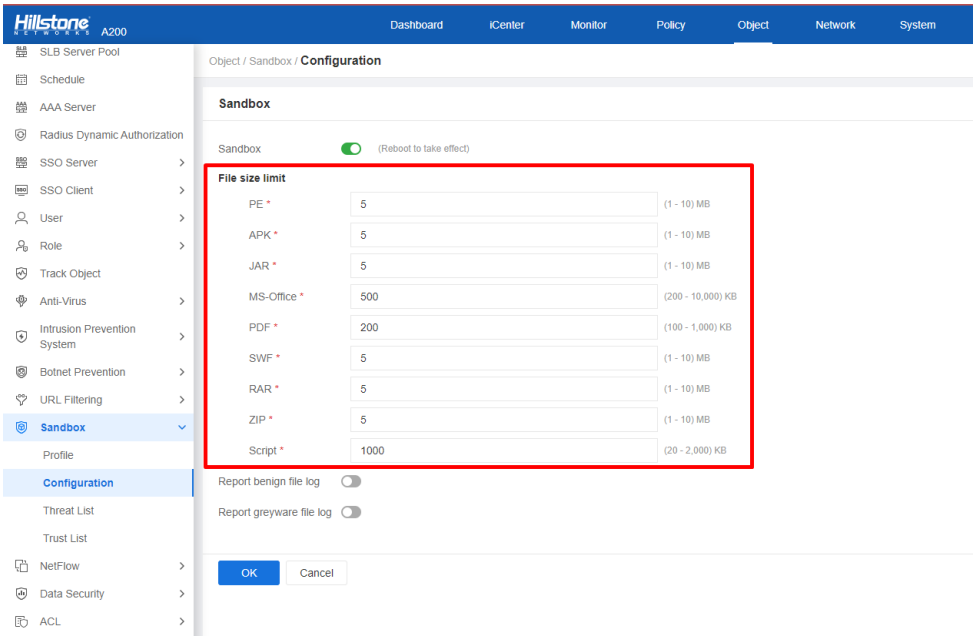


FIGURA 118. CONFIGURACIÓN LÍMITE DE TAMAÑO A ENVIAR SANDBOX HILLSTONE

Se aplicará sobre la política de tráfico que se quiere analizar el tráfico y aplicar el análisis de sandbox

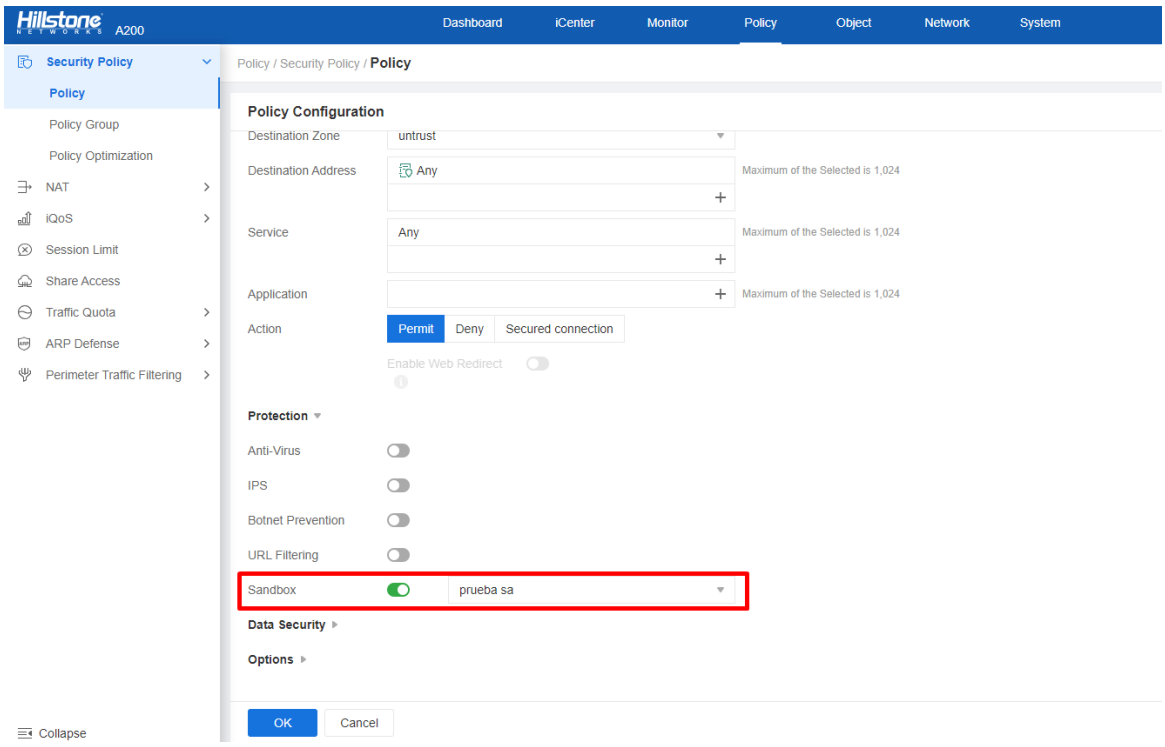


FIGURA 119. APLICAR SANDBOX A POLÍTICA DE TRÁFICO HILLSTONE

Pueda verse desde el menú de “Cloud Sandbox log” en detalle de lo ocurrido y la acción tomada

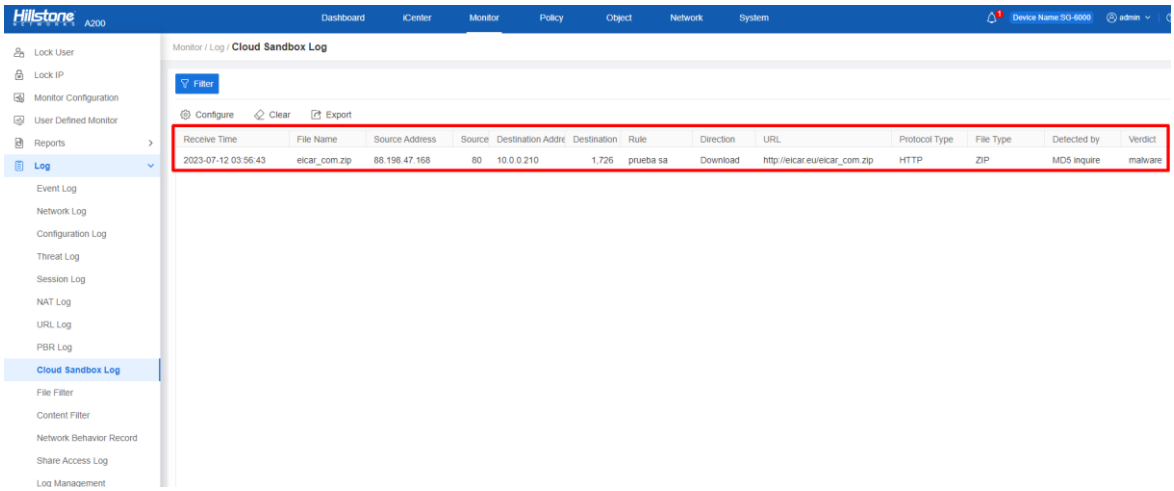


FIGURA 120. LOGS DETECCIÓN VIRUS MEDIANTE SANDBOX HILLSTONE

3.6.4 Discusión

Puede verse como tanto FortiGate como Hillstone han detenido y detectado virus y enviado a la sandbox. Como excepción, Hillstone solo es capaz de enviar y trabajar con los tipos de fichero PE, APK, JAR, MS-OFFICE, PDF, SWF, RAR, ZIP Y SCRIPS por lo cual cuando se intentó la descarga para su análisis de un fichero "malicioso" con extensión .com este no lo detecto a diferencia de FortiGate que si lo hizo

4 Conclusiones y futuras líneas de trabajos

El objetivo de este proyecto era la prueba de las herramientas de seguridad donde diferentes NGFW prueban sus capacidades de detención, acción y notificación de lo ocurrido.

A partir de lo que se ha probado y documentado pueden apreciarse similitudes en respuestas, pero con diferencias en las configuraciones y toma de acciones. Debido a la problemática relacionada con las licencias básicas puede observarse que un dispositivo (Hillstone) tenía menores prestaciones que en el otro (FortiGate).

A nivel de trabajo ambos son parecidos con diferencias en el enfoque que hacen a la hora de afinar configuraciones en determinados puntos como Hillstone que en Botnet deja afinar más el detalle de lo que se quiere hacer cuando se detecta tráfico por túnel DNS. En cambio, FortiGate no deja esa opción de configuración.

FortiGate tiene una mayor documentación y mayor adaptabilidad de uso debido a que tiene una interfaz más cómoda lo cual facilita configurar todas las herramientas ya que intenta centralizar su uso. Hillstone actualmente dispone de muy poca información disponible al menos de manera pública para entender de forma correcta y eficiente cada punto.

En este proyecto se han utilizado solamente 2 dispositivos NGFW, como posible mejora o investigación en este tema seria realizar una comparativa con más fabricantes y detallar las necesidades específicas para que los clientes pudiesen elegir más acorde según sus demandas.

La comparativa con más fabricantes de NGFW, junto con el análisis detallado de las necesidades del cliente, proporcionará un enfoque más sólido y fundamentado para garantizar la implementación de la mejor solución de seguridad de red, optimizando así la protección y eficiencia en el proyecto.

5 Bibliografía

1. (15-03-2023). ¿Qué son y para qué sirven los SIEM, IDS e IPS?. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
2. (20-03-2023).URL Filtering - How Does IT Work. Ckeckpoint. https://www.checkpoint.com/cyber-hub/network-security/what-is-url-filtering/#:~:text=URL%20filtering%20is%20a%20way,that%20this%20content%20is%20blocked
3. (23-03-2023). What is Command and Control (C&C or C2) in Cybersecurity?. sunnyvalley. https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-command-and-control-c2
4. (28-05-2023). IP Reputation: Why it Matters and How to Improve It. abnormalsecurity. https://abnormalsecurity.com/glossary/ip-reputation
5. (29-04-2023). Procedimiento de empleo seguro Cortafuegos FortiGate. Ccn-cert. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/4300-ccn-stic-1406-procedimiento-de-empleo-seguro-cortafuegos-fortigate/file.html
6. (08-04-2023). Evasion y falsificación de cortafuegos. nmap. https://nmap.org/man/es/man-bypass-firewalls-ids.html
7. (10-04-2023). IP reputation filter. docs.fortinet. https://docs.fortinet.com/document/fortigate/6.4.4/administration-guide/68937/ip-reputation-filtering
8. (12-04-2023). IP Reputation filter. Hillstone.zabezpieczenia. https://hillstone.zabezpieczenia.it/documentation/ngfw-hillstone-networks/policy/perimeter-traffic-filtering/ip-reputation-filter/
9. (15-04-2023). The key benefits of url filtering. hillstonenet. https://www.hillstonenet.com/blog/the-key-benefits-of-url-filtering/
10. (17-04-2023). Hillstone cloud sandbox. hillstone. https://hillstone.pl/hillstone_firewall_sandbox_cloud/
11. (20-04-2023). Servicio de seguridad de FortiGuard IPS. fortinet. https://www.fortinet.com/lat/products/ips
12. (22-04-2023). C2C dentro de los perfiles. Docs.Fortinet. https://docs.fortinet.com/document/fortigate/6.2.0/new-features/228722/move-botnet-c-c-into-ips-profile
13. (27-04-2023). ¿Qué es un firewall?. kaspersky https://latam.kaspersky.com/resource-center/definitions/firewall

14. (02-05-2023). ¿Qué es un firewall?. cisco https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html
15. (09-05-2023). Hillstone networks Serie-S. Hillstonenet https://www.hillstonenet.com/wp-content/uploads/Hillstone_S-Series_V1.3_SP.pdf
16. (15-05-2023). Deep inspection. Docs.Fortinet. https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/122078/deep-inspection
17. (26-06-2023). Configuración Threat capa red y aplicación. Hillstonenet https://www.hillstonenet.com/support/T-series/2.0/en/protect_conf.html
18. (05-06-2023). Análisis comparativo de NGFW y UTM. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/ngfw-vs-utm
19. (07-06-2023). Sandbox en linea. Fortinet. https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/inline-sandboxing
20. (07-06-2023). ¿Qué es el malware?. Cisco. https://www.cisco.com/site/us/en/products/security/what-is-malware.html
21. (10-06-2023). Proteccion Botnet C&C. Hillstonenet https://www.hillstonenet.lat/blog/seguridad-de-la-red/proteccion-botnet-cc-desde-el-perimetro-hasta-la-nube/
22. (11-06-2023). Covenant: C2 con .net. thehackerway. https://thehackerway.com/2021/10/25/covenant-command-and-control-con-net-core-para-red-team/
23. (12-06-2023). Manual Armitage. Dragonjar. https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml