UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de la herramienta WAF y AntiDDoS para la seguridad en aplicaciones web

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Karla Isabel Ortiz Arias

ASESOR DE INFORME

M. en C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2020

Agradecimientos

Agradezco a Dios por guiarme en el camino correcto para poder lograr este reto.

A la Facultad de Ingeniería por brindarme la oportunidad de ser parte de la institución, por confiar en mí, conocer excelentes profesores y sentirme parte de ella.

A mis maestros por darme el conocimiento necesario para poderme desempeñar en mi vida profesional y a mi tutora Jaquelina López Barrientos por guiarme, confiarme sus conocimientos y apoyarme en este proceso.

A mis padres Jorge Ortiz Bastida y Olga Isabel Arias Gámez por estar presentes a lo largo de esta travesía, por todo su apoyo para poder lograr finalizar esta carrera, pero sobre todo por impulsarme en los momentos más difíciles y no dejarme caer.

A mi hermano Jorge Eduardo Ortiz Arias, al que amo con todo mi corazón, por estar siempre a mi lado cuando más lo he necesitado.

A mis amigos, que me brindaron su apoyo, consejos y conocimientos que lograron hacer que este trabajo se concretará con éxito.

Índice de Contenido

Índice de tablas

Índice de Figuras

Introducción

Introducción

En la actualidad, la computación la encontramos en la mayoría de las actividades que tenemos en la vida cotidiana, por lo que se genera una necesidad de estar actualizado y no quedarnos varados en el camino de la tecnología hacia el futuro, pero el hecho de que estas actividades hagan uso de la computación para poder agilizar estas mismas, hace que el usuario quede vulnerable en ciertos aspectos.

Es por ello que si las empresas no cuentan con un sistema de protección avanzado pueden sufrir eventos lamentables en la seguridad de sus recursos informáticos.

Uno de los casos más recientes, reportado por el gobierno de México en su portal www.gob.mx se suscitó el día 12 de Febrero de 2019, de lo cual una institución financiera detectó un virus de tipo RANSOMWARE (software malicioso que al infectar el equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y cifrar los archivos quitando el control de los datos almacenados), que actuó sobre equipos basados en sistemas operativos Windows.

El incidente fue contenido de forma oportuna y efectiva por la institución, no tuvo tema económico y solo algunos equipos de cómputo personales se vieron afectados.

Otro ejemplo es el dado a conocer públicamente un mes antes del brote de WannaCry por un grupo de hackers llamado Shadow Brokers, en el que informa que en el año 2017 se detectó la explotación activa de una vulnerabilidad que afecta a sistemas Windows por el ransomware denominado WannaCry, el cual cifra los archivos en el equipo de los de las unidades de red a las que están conectadas, además de propagarse a la red afectando a otros sistemas Windows.

Microsoft había lanzado un parche para EternalBlue, el cual fue nombrado así por la NSA (La Agencia de Seguridad Nacional es una agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información), pero millones de usuarios omitieron actualizar el sistema y por eso quedaron vulnerables al ataque.

El ransomware WannaCry cifra la información de la víctima, una vez hecho esto el perpetrador exige el rescate con un pago en moneda digital bitcoin para recuperar el acceso a los ordenadores.

Estos son solo algunos ejemplos de lo que ocurre por falta de seguridad al perímetro de la red corporativa y es por ello que entran al mercado diversas empresas que proveen el servicio de seguridad informática, en algunos casos estas empresas implementan la tecnología y la administran, tomando la responsabilidad de asegurar la red, en otros casos únicamente implementan la tecnología y proporcionan una pequeña transferencia de conocimientos de lo que fue implementado.

El presente trabajo tiene como objetivo principal describir como una empresa dedicada a la seguridad informática toma la decisión de realizar una implementación de una herramienta, analizar diferentes opciones y tomar la adecuada a los requerimientos del cliente, así mismo se describe el proceso de implementación, análisis y entrega de esta misma a un área especializada en monitoreo de eventos.

CAPÍTULO 1

PRESENTACIÓN DE LA EMPRESA E INGRESO AL CAMPO LABORAL

Capítulo 1 Ingreso al campo laboral y presentación de la empresa.

Actualmente llevo cerca de 4 años y medio laborando, comencé mi incursión en el año 2015 en el área de Telecomunicaciones como becaria, implementando servicios de telefonía por voz IP. A mediados del año 2015 logré terminar mis estudios y 3 meses después logré ser contratada en la empresa para proyectos en específico.

A mediados del año 2016 decido dedicarme al área de seguridad informática y logré ingresar en una empresa especializada en seguridad informática como analista junior y dedicarme en este rol hasta inicios del año 2019. Para este caso y por motivos de confidencialidad de la empresa se hará referencia con el nombre de "SecServices".

En SecServices, mi rol fue implementar diferentes tecnologías de seguridad como firewalls, SIEM (Security Information and Event Management) y WAF (Web Aplication Firewall).

SecServices es una empresa mexicana que ofrece una amplia gama de servicios orientados a salvaguardar la información, preservando el bienestar organizacional de sus clientes. Esta empresa es relativamente nueva ya que lleva alrededor de 15 años en el mercado, el motivo por el cual decide dedicarse a este ámbito es para garantizar la seguridad de la información de las empresas ofreciendo diversos servicios como el diagnostico, gestión de riesgos, implementación de diversas herramientas y respuesta a incidentes.

Como bien se menciona en el punto anterior, SecServices se divide en las siguientes ramas para prestaciones de servicio:

- **Seguridad Preventiva**

  Para la evaluación, análisis e identificación de cualquier amenaza a la confidencialidad, integridad y disponibilidad de los elementos críticos, proveyendo lo siguiente:

  El diagnostico e identificación de vulnerabilidades para crear una estrategia de seguridad para la protección de la empresa estableciendo riesgos potenciales, a través de controles, políticas cumplimiento de normas y marco regulatorios

  Un diagnóstico de seguridad en el cual se diseña un plan de mejora y seguimiento puntual a cada iniciativa

- **Seguridad Activa**

  Para la protección de manera activa de la infraestructura de la empresa por medio de tecnología, lo cual garantiza la continuidad de la operación 24 horas al día por 7 días a la semana los 365 días al año.

  Dentro de este ámbito se desglosa en la administración de tecnologías de seguridad de red y endpoints (usuario final).

    - Protección perimetral, WAF (web application firewall), cuentas privilegiadas, correo electrónico, navegación, bases de datos y aplicaciones.

- Endpoints, dispositivos móviles, servidores y estaciones de trabajo.

El fin de este servicio es poder monitorear la comunicación entre la red empresarial e internet mediante diversos controles de accesos.

- **Seguridad Proactiva**

Se refiere a la identificación, protección, detección, respuesta y contención de incidentes de ciber-seguridad de la empresa.

Cuenta con soluciones proactivas contra amenazas con servicio administrado 24/7/365, el cual consta de un equipo de expertos en ciberseguridad que protegen a los usuarios en la red de la empresa.

Toma de medidas preventivas de protección y remediación utilizando threat hunting. Cabe destacar que al usar threat hunting es posible la detección de ataques en un tiempo menor o incluso adelantarse a ellos, comúnmente se centra en descubrir un incidente o incumplimiento no detectado lo más rápido posible y antes de completa la cadena de destrucción de la amenaza (comúnmente llamada kill chain).

Monitoreo e investigación automatizadas de incidentes y medidas preventivas llamado respuesta a incidentes.

- **Soluciones a la medida**

Permite construir la mejor solución que cubra con las necesidades y expectativas de la empresa, en este punto se incluye al área de ventas e implementaciones para realizar la instalación y configuración inicial de los equipos.

1.1 Organigrama de la empresa

A continuación, en la figura 1-1 se define el organigrama de la empresa dividida en 4 áreas.

El área de Capital Humano refiere a la gestión del personal de la empresa respecto a contrataciones, pagos de sueldos, gestión de cursos, bienestar del empleado.

El área de Finanzas se encarga de llevar a cabo la contabilidad de la empresa y realiza la compra de lo que esta requiere, como equipos, mobiliario, viáticos, entre otros.

El área de Comercial se encarga de hacer una evaluación y análisis de lo que el cliente requiere, esto es, el área de preventa hace una cotización de lo que se requiere implementar, el área de ventas presenta la venta junto con el Service Delivery que es el que da seguimiento a todo el proceso de la implementación y el área de Marketing mantiene la comunicación con el proveedor.

Por último, el área de operaciones se encarga de la parte operativa de los servicios brindados, el área de SOC se dedica al monitoreo de las herramientas ya implementadas 24/7/365.

Diagnostico se dedica a realizar pentest y análisis de la red corporativa.

Consultoría se dedica a analizar las herramientas y dar recomendaciones sobre la mejora de la seguridad en la red.

Los ingenieros en sitio tienen como función estar en las instalaciones del cliente y dar una atención personalizada a sus requerimientos.

Transition se divide en 3 áreas, las cuales son: oficina de proyectos (PMO), control de cambios, e implementaciones.

El área de oficina de proyectos (PMO), se encarga de la recepción, asignación, planificación de las tareas o actividades necesarias, así como su seguimiento para asegurar una buena gestión de tiempos y recursos durante la ejecución de un proyecto.

El área de Control de cambios, se encarga de asegurar la administración de todos los cambios solicitados en la infraestructura de los diferentes clientes con los que cuenta, este se divide en diferentes puntos clave para asegurar el éxito del proceso.

1. Análisis de la solicitud del cambio
2. Evaluación del cambio
3. Notificaciones
4. Ventana de mantenimiento
5. Documentación del control de cambio

El área de Implementaciones, que es el área donde trabaje, se encarga de la configuración inicial, migración, sanity check y/o puesta a punto de la herramienta, basándose en las necesidades del cliente, para que después sea administrado ya sea por el área del SOC (Security Operation Center) o por el mismo cliente.

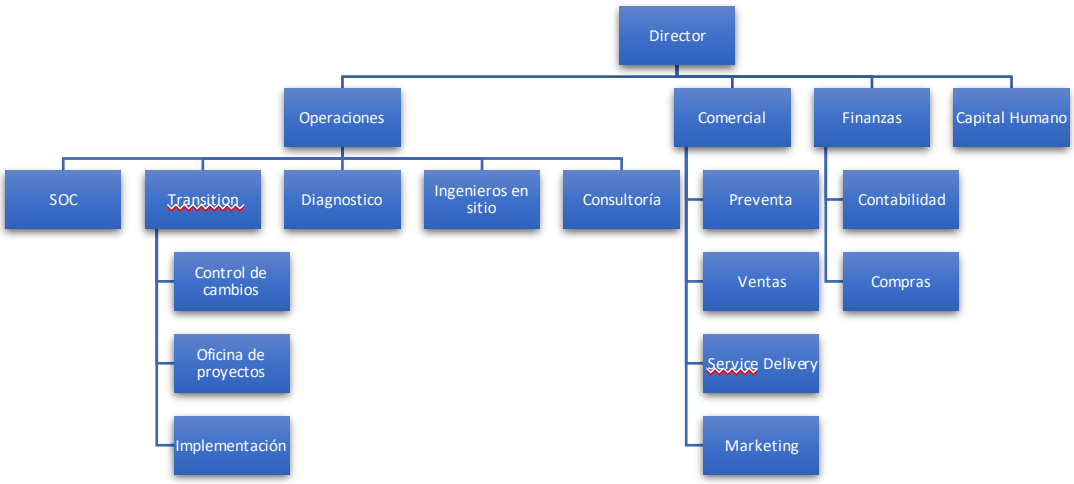


Figura 1-0-1 Organigrama general de SecServices

CAPÍTULO 2

DESCRIPCIÓN DE PROYECTOS REALIZADOS

Capítulo 2 Descripción de proyectos realizados

Proyecto 1: Correlacionador de eventos, marca Splunk

Problemática: No se contaba con una herramienta de almacenamiento y análisis de datos, por lo cual se requirió la implementación de un correlacionador de eventos de seguridad (SIEM), el cual es capaz de cumplir con el estándar de seguridad de datos (PCI).

Objetivo: Brindar un servicio por medio de un SIEM, que recopile datos, analice y realice el monitoreo continuo, por medio de un análisis en línea del comportamiento del tráfico, accesos, estado de salud, entre otros, de la infraestructura crítica del cliente, con la directriz de proteger, mejorar la seguridad, detectar ataques de manera oportuna para minimizar riesgos y prevenir la pérdida de continuidad en la operación.

Actividades:

- Implementación
  - Realice el rackeo y conexión del servidor en su centro de datos.
- Configuración inicial
  - Realice la instalación de sistema operativo y software de Splunk
- Puesta a punto
  - Realice las integraciones correspondientes en cuanto a fuentes y configuración del software basándose en las mejores prácticas proporcionadas por fabricante.
- Análisis de cumplimiento de PCI
  - Realice un análisis en cuanto a los puntos que solicita el estándar PCI y evidenciar que estos puntos se cumplían mediante reportes y alertamientos.
- Creación de dashboards de PCI de acuerdo a cada herramienta
  - Realicé un dashboard el cual mostraba información importante referente a los puntos solicitados por PCI de las fuentes integradas en Splunk.

Resultados: Implementé un SIEM de la Marca Splunk Enterprise, el cual cuenta con más de 30 tecnologías integradas de la infraestructura del cliente, ayudando a obtener un mejor análisis y control del comportamiento de su empresa. Esto es posible gracias a que un SIEM tiene la capacidad de recopilar eventos relacionados con la seguridad de dispositivos de usuario final, servidores como Windows o Linux, equipos de seguridad como firewalls, IPS y antivirus.

Dicho SIEM lo implementé en un periodo de tiempo de 2 meses, en el año 2019.

Proyecto 2: WAF y AntiDDoS en la nube, marca Radware

Problemática: No se contaba con un servicio de seguridad en la nube referente a un firewall de aplicaciones web, por lo cual no había una protección en la aplicación web que ponía en riesgo la información confidencial resguardada en los sistemas del cliente.

Objetivo: El objetivo general fue asegurar y proteger las aplicaciones web de ataques específicos, así como bloquear ataques de DDoS.

Actividades:

- Definir en conjunto con el cliente los activos y servicios críticos a proteger.
    - El área realizo una reunión en conjunto con el cliente para definir que aplicaciones web se debían proteger.
- Implementación
    - El proveedor proporciono los accesos para poder ingresar al Radware y licenciamiento.
- Configuración inicial
    - Basándose en las aplicaciones web a proteger, realice la configuración de las mismas y solicite al cliente el cambio de DNS que Radware requería, por lo que una vez que el cliente realizo dicho cambio, se validó que el tráfico fuera ruteado a radware y después del análisis que este realizará siguiera a la aplicación web.
- Puesta a punto
    - Realice configuraciones apropiadas en cuanto al mercado que refiere a la empresa y por mejores prácticas que proporciona fabricante.
    - Realicé validaciones en los umbrales definidos en el Anti-DDoS los cuales incluyen:
        - Validar bloqueo de IPs y tráfico malicioso
        - Recolección en tiempo real de direcciones IP
        - Validar el funcionamiento correcto de las funciones que proporcione la herramienta para un óptimo monitoreo en tiempo real y prevención de ataques

Resultados: Realicé la implementación de un servicio de WAF y AntiDDoS en la nube, de la marca Radware, el cual es capaz de proteger aplicaciones web.

Dicha implementación la realicé en un periodo de 1 mes en el año 2018.

CAPÍTULO 3

PROYECTO A PRESENTAR

Capítulo 3 Proyecto a presentar

3.1 Problemática

Una empresa del sector de Gobierno Federal cuenta un portal web en su infraestructura que provee información relevante como los detalles del consejo de administración, inversionistas, transparencia, concursos y contratos y por ultimo poder realizar ciertos pagos para servicios que el usuario contrata. Dicho portal debe contar con la protección necesaria para que la información que provee sea íntegra al país, por lo que se solicita la implementación de una tecnología de seguridad para la protección de su sitio WEB de ataques específicos, así como bloquear ataques DDoS.

Por lo que solicita lo siguiente:

- Protección a los sitios y aplicaciones críticas definidas por el cliente contra las siguientes amenazas:
    - Back Doors
    - Botnets
    - Penetration Test
    - Zero Day Exploit
    - Vulnerabilidades de Aplicaciones
- Protección de los sitios y aplicaciones contra ataques de denegación de servicios distribuidos (DDoS)
- Mantener un registro de la actividad de las aplicaciones y la interacción de los usuarios, con fines analíticos que permitan detectar y disminuir riesgos derivados de una desviación en la operación
- Impedir el acceso a usuarios maliciosos y no deseados.

Análisis

De acuerdo a lo que el cliente solicita y al catálogo de tecnologías que la empresa provee a implementar se ofrece al cliente la solución de Incapsula de la marca Imperva para cubrir esta problemática.

Para tomar esta decisión, partimos de un cuadrante llamado Gartner, el cual define en una gráfica las compañías más relevantes de cada industria tecnológica que van posicionadas de acuerdo a su desempeño anual dentro de su propio mercado, esto es, que para cada tipo de tecnología existe un cuadrante diferente.

Este cuadro nos ayuda a tener una visión más clara determinada al producto y los servicios que provee.

Ahora bien, el cuadrante mágico se divide en 4 partes las cuales se basan en una investigación y consultoría que realiza una empresa estadounidense.

- Aspirantes (Challengers): Tienen buena ejecución del negocio y son capaces de dominar un gran segmento del mercado, aunque aún no demuestran un buen entendimiento del mismo.
- Líderes (Leaders): Tienen una adecuada visión actual del mercado y están bien posicionados para el futuro.
- Jugadores de nichos específicos (Niche Players): Se enfocan con éxito en un segmento de mercado en específico, no tienen una visión global y no se caracterizan por hacer grandes innovaciones.
- Visionaries: No son capaces de llevar acabo ideas de cambios en reglas y paradigmas por completo o con éxito, pero entienden el rumbo del mercado.

Figura 3-1 Cuadrante Mágico de Gartner

Se realizó una comparativa en la cuales destacamos ciertos rasgos entre diferentes Soluciones como lo son: Imperva, Akamai, F5 y Fortinet.

Solución WAF	Tipo de servicio	Ventajas	Desventajas
Imperva	• WAF Tradicional • Incapsula (Servicio en la nube)	• Análisis de ataques. • Administración basada en roles. • Balanceo de cargas. • Protección DDoS • Cuenta con protección de Top 10 OWASP	• No admite Single-Sign-On (SSO). • Se requiere mejora en informes. • El WAF tradicional tiene más funcionalidades que en la nube. • El WAF en la nube es de menor costo a uno que requiere hardware. • Previos más altos que los competidores.
Akamai	• Kona Site Defender (Servicio en la nube)	• Servicios profesionales. • Monitoreo de incidentes y análisis automático de tráfico. • Mejora en falsos positivos.	• Altos precios • No hay entorno tradicional. • Falla en gestión de políticas, informes, notificaciones y control.
F5	• Tradicional	• Atención a cliente. • Soporte de AWS, Azure, GCP, Openstack, Vmware.	• Precios no competitivos y falta de productos. • No ofrece WAF de autoservicio completo y gestión fácil. • Dicho WAF es un módulo de F5, por lo que se requiere una licencia adicional.
Fortinet	• Tradicional • Fortiweb (servicio en la nube)	• Detección de malware.	• Muy pocas funcionalidades a comparación de los competidores. • No ofrece buen servicio para la mitigación de bots y protección de DDoS.

Tabla 3-1 Comparativa de soluciones WAF

Ahora bien, una vez que se realizó la comparativa entre diversas soluciones, es posible visualizar que Imperva se encuentra como líder del mercado y ofrece mejor estabilidad que sus competidores, a continuación, se dará una explicación más detallada de los servicios que ofrece Incapsula.

Dicha herramienta conjunta controles como WAF (Web Application Firewall) y Anti-DDoS (Anti-Distributed Denial of Service). Está basado en tecnología de nube, por lo que el control estará replicado a nivel mundial en diferentes puntos de presencia.

Dentro del servicio, se considera la activación de las políticas y alertas default del sistema Incapsula incluidas el Top 10 de amenazas de OWASP:

- Inyección: Se refiere al envío de datos no confiables como parte de un comando o consulta (query). Esto puede ocurrir en SQL, No SQL, Sistemas Operativos, LDAP, estos datos dañinos pueden ocasionar ejecutar comandos involuntarios para acceder a los datos sin autorización.

- Perdida de autenticación: El atacante puede comprometer usuarios y contraseñas, token de sesiones o explotar otras fallas de implementación para asumir la identidad de otros usuarios.

- Exposición de datos sensibles: Existen aplicaciones web o APIS que no protegen de la manera correcta datos sensibles, estos, de tipo financiera, salud o Información Personalmente Identificable (PII). El atacante puede robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes, robos de identidad y otros delitos.

- Entidades Externas XML (XXE): Pueden utilizarse para revelar archivos internos mediante la URL o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

- Pérdida de Control de Acceso: Al no restringir a los usuarios que se autentican de manera correcta, los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, cambiar privilegios, ver archivos sensibles modificar datos entre otros.

- Configuración de Seguridad Incorrecta: Comúnmente ocurre cuando se establece una configuración de seguridad manual, a lo que no permite la actualización, falta de parches, cabeceras HTTP mal configuradas, mensajes de error por contenido sensible, entre otros.

- Secuencia de Comandos en Sitios Cruzados (XSS): Los XSS permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión o modificar los sitios web, o re direccionar al usuario hacia un sitio malicioso.

- Deserialización Insegura: Es una vulnerabilidad que puede permitir la ejecución remota de código en servicios web.

- Componentes con vulnerabilidades conocidas: Si un componente como (bibliotecas, frameworks y otros módulos) es vulnerable, las aplicaciones y API que utilizan estos, pueden debilitar las defensas y permitir diversos ataques e impactos.

- Registro y Monitoreo Insuficientes: Al juntar el registro y monitoreo insuficiente y la falta de respuesta ante incidentes, periten a los atacantes mantener un ataque, pivotear a otros sistemas e incluso destruir o extraer datos.

Adicionalmente, como servicio de soporte, Incapsula cubre con los siguientes puntos:

- Incorporación rápida y fácil

La protección DDoS y web se puede implementar sin necesidad de un hardware o software adicional. Este servicio se puede proporcionar cambiando únicamente las configuraciones DNS del sitio.

- Protección a bajo costo

Incapsula ofrece protección 24x7 contra todos los ataques DDoS, detección de bot y control de acceso, asegurando cualquier sitio web contra amenazas conocidas y emergentes. Esto incluye las amenazas comunes de la web 2.0, como spammers, scrapers & escaneres de vulnerabilidad, además de SQL injection, Cross Site Scripting y otros ataques a nivel aplicación. Lo anterior sin necesidad de conexiones a internet de varios gigabits o cualquier hardware adicional.

Elimina los costos de configuración y gastos generales asociados con el aprovisionamiento excesivo y el despliegue de dispositivos adicionales en premisa.

- Seguridad colaborativa

Protege sitios web usando el conocimiento colectivo sobre amenazas de seguridad, incluyendo nuevos y emergentes métodos de ataque DDoS. Mediante técnica de crowdsourcing.

- Soporte 24x7

Respaldado por un equipo dedicado de ingenieros SOC. Sus responsabilidades incluyen: respuesta proactiva y gestión de eventos, monitoreo continuo en tiempo real, ajuste de políticas adepto, informes de ataque de resumen y soporte 24x7.

El servicio que la empresa provee aparte de la implementación de la solución es la configuración, puesta a punto, monitoreo continuo, operación y administración de la solución.

Por lo que se ofrecen dos etapas en el servicio:

- SETUP: Este consiste en cumplir con lo que establece el contrato que se realizó con el cliente, por lo que se obtiene licenciamiento de la solución, se realiza la configuración inicial y de acuerdo a cierto análisis en el mercado del cliente se propone y realizan las configuraciones basadas en las mejores prácticas que el fabricante propone.

- Operación: En esta etapa se llevan a cabo las actividades necesarias para la operación y administración de la herramienta. En este punto se realiza un monitoreo y análisis de las amenazas de seguridad que Incapsula detecta. Así mismo se realizan los documentos de entregables, para mantener al cliente notificado sobre las incidencias detectadas.

Objetivo General

Brindar un servicio de seguridad el cual sea de tipo en la nube, para la protección de aplicaciones Web y ataques DDoS, el cual cubra con el alcance y necesidades del cliente, para que una vez implementado, sea administrado por un SOC.

Objetivos Particulares

- Identificar los requerimientos para su implementación.
- Asegurar y proteger las aplicaciones web de ataques específicos, así como el bloqueo de ataques DDoS.
- Mantener un registro de actividad, tanto de las aplicaciones como de los usuarios finales, con fines analíticos que nos permita detectar y disminuir riesgos derivados de una desviación en la operación.
- Bloquear el acceso a usuarios maliciosos no deseados.

3.2 Diseño

Un WAF es una abreviación que significa Web Aplication Firewall.

En sí, todas las soluciones de WAF funcionan de la misma manera y su principal objetivo es impedir que solicitudes maliciosas afecten al sitio web que queremos proteger. Este firewall en la nube es especializado para aplicaciones web y analiza el tráfico basado en la web (HTTP).

Imperva Incapsula ofrece diferentes productos asociados a la protección y aceleración de un sitio web, los cuales ayudan a proteger al portal de la siguiente manera:

- Seguridad para sitios web: El portal requería tener un firewall para aplicaciones web que protegiera sus aplicaciones y sitios web de peticiones maliciosas, esta seguridad cuenta con una protección contra bots avanzadas servicios de detección de Shell de puerta trasera.

- Protección de DDoS: El portal como es público, recibiría demasiadas solicitudes, con la intención de desbordar la capacidad del sitio web, lo que afectaría, ya que este sitio web brinda servicios en línea. Incapsula mitiga los mayores ataques a nivel mundial sin obstaculizar el tráfico legítimo, ofrece múltiples opciones de protección DDoS.

- Red de distribución de contenido (CDN): Al tener un portal que tiene demasiadas peticiones de usuarios, se recomienda tener la opción de habilitar el CDN, ya que con él se tendrá opciones de control de cache, así como contenido y herramientas de optimización de red para hacer que el sitio web sea más rápido cuando se consulte.

- LBaaS (Load Balancer-as-a-Service): Se recomienda que, para asegurar la alta disponibilidad del sitio, se active está opción, esto solo se puede hacer si el portal cuenta con dos servidores web y que cuando un servidor web falle, este se dirija al otro.

En este caso y de acuerdo a lo solicitado, únicamente se utilizarán los primeros 3 puntos, ya que el cliente no cuenta con algún otro servidor web para poder realizar la redirección.

Ahora bien, para hacer uso de este servicio es necesario que en el sitio web se realicen cambios de configuración a nivel DNS, lo que hará que todo el tráfico que entre directo a la página web se re direccione a la nube de Incapsula, la cual ahora será la encargada de gestionarlo y monitorearlo.

En la figura 3-2 se puede apreciar la arquitectura de Incapsula.

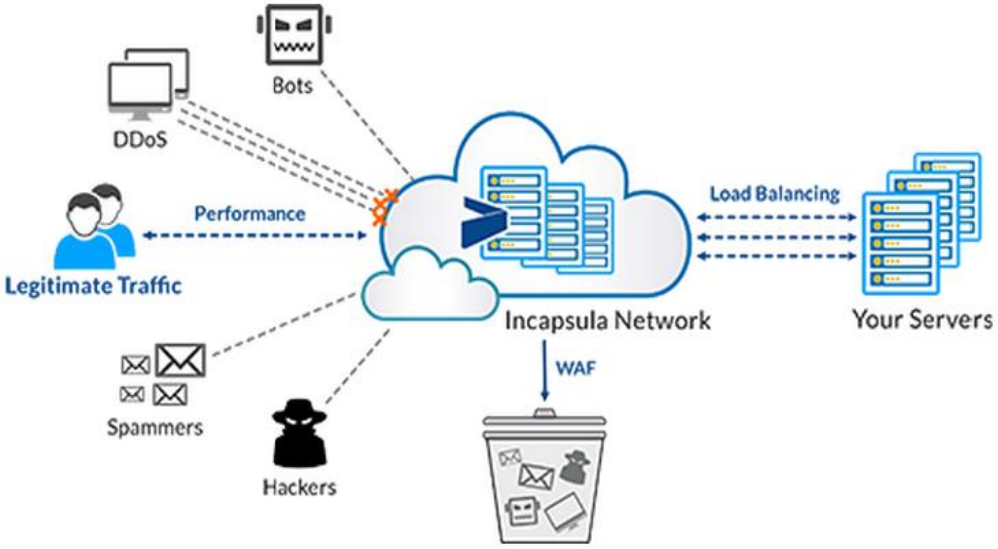


Figura 3-2 Arquitectura de Incapsula

Incapsula simplifica las operaciones de TI y reduce los costos al consolidar varios dispositivos y aplicaciones en un único servicio basado en cloud.

3.2.1 Seguridad de sitios web

Incapsula es la puerta de enlace de todo el tráfico entrante a su aplicación web, lo que la coloca en la situación perfecta para filtrar a todos los visitantes maliciosos y solicitudes como las inyecciones SQL y los ataques XSS.

Las amenazas se identifican a través de múltiples capas de seguridad que un equipo especializado de investigación sobre seguridad actualiza continuamente. Los datos de ataques de colaboración abierta de millones de dominios protegidos por Incapsula se usan para proteger de forma inmediata a toda nuestra comunidad de clientes.

La solución de seguridad de Incapsula es un servicio gestionado (véase la figura 3-3) y puede implantarse rápidamente para proteger las aplicaciones en el cloud o en las instalaciones sin hacer cambios en el hardware o el software.

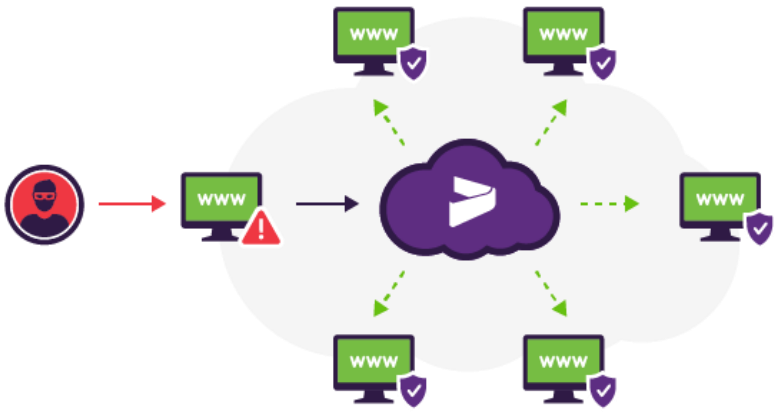


Figura 3-3 Funcionamiento de Incapsula

Como principal línea de defensa, Incapsula cuenta con un cortafuegos para aplicaciones WEB (WAF), el cual defiende de los ataques a aplicaciones web, incluidas las 10 principales amenazas de OWASP.

A continuación, en la figura 3-4, se muestra un listado de tipos de amenazas que posee el WAF para aplicaciones web.

Threat Type	Incidents	Current Setting
Bot Access Control	231K	Block
Suspected Bots	39966 / 1450	CAPTCHA
Remote File Inclusion	0	Alert Only
SQL Injenction	935	Block
Cross Site Scripting	46	Block
Illegal Resource Access	1.1K	Block
DDoS	130K	Protected

Figura 3-4 Tipos de amenazas WAF para aplicaciones web

Por otro lado, Incapsula cuenta con tecnología de clasificación de clientes, lo cual bloquea automáticamente los bots maliciosos (véase la figura 3-5) y permite que los bots y usuarios legítimos pasen. Las políticas personalizadas permiten la gestión del tráfico de bots adaptándose a las necesidades del cliente.

Figura 3-5 Detección de bots

Incapsula cuenta con protección de SHELL de puerta trasera, esto es, en caso de que el sitio sufriera un ataque antes de ser protegido por Incapsula, es posible que este permitiera una instalación de puerta trasera en su sistema. El servicio de Incapsula bloquea la comunicación con los shells de puerta trasera (véase la figura 3-6) y los pone en cuarentena para posteriormente ofrecer la información necesaria para su eliminación.

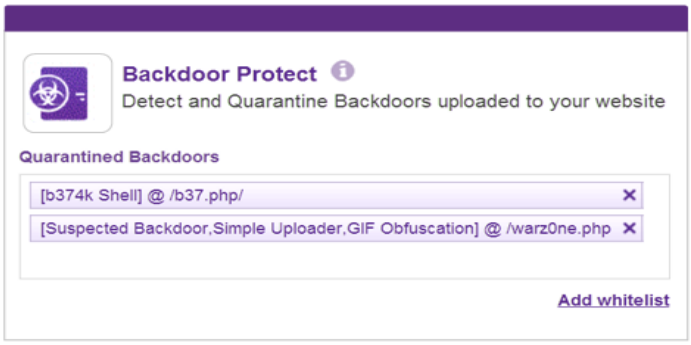


Figura 3-6 Protección de SHELL de puerta trasera

El conjunto completo de soluciones de seguridad de Incapsula, ayuda a mitigar los ataques APT más maliciosos. Las Amenazas Persistentes Avanzadas (APT) son ataques en varias fases que pueden implicar la infiltración en su aplicación web explotando las vulnerabilidades y creando una cortina de humo DDoS para salir sin ser detectado.

En la figura 3-7 se puede observar el proceso de mitigación de APT.

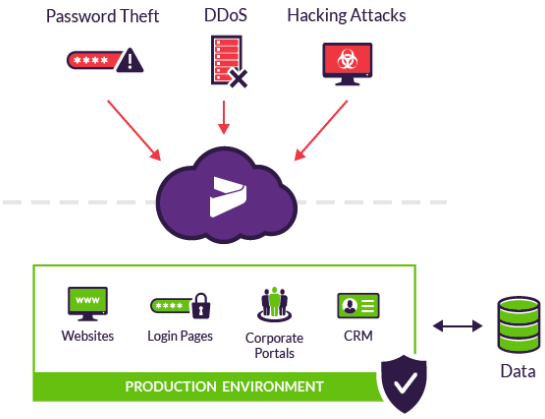


Figura 3-7 Mitigación de APT

Incapsula es totalmente compatible con las principales soluciones de SIEM. Los paneles de control de SIEM pre-configurados se integran con los flujos de trabajo existentes e impulsan la seguridad y la visibilidad de las amenazas.

En la figura 3-8 se puede apreciar un ejemplo de panel de control, donde es posible observar el total de peticiones realizadas a la página web a proteger, tráfico desde una misma IP, Top 10 por país, entre otros.

La ventaja de realizar una integración de Incapsula con SIEM, es que es posible almacenar los logs más de 30 días que es el tiempo que Incapsula almacena en la nube, una vez teniendo estos datos

en el SIEM, es posible realizar un análisis de tipo forense o incluso realizar una comparativa con otras fuentes integradas.

Otro punto a favor es que, para este ejemplo, Incapsula cuenta con una API desarrollada en Splunk que ofrece diversos paneles con vistas que pueden ser de gran importancia para el monitoreo de la página web.

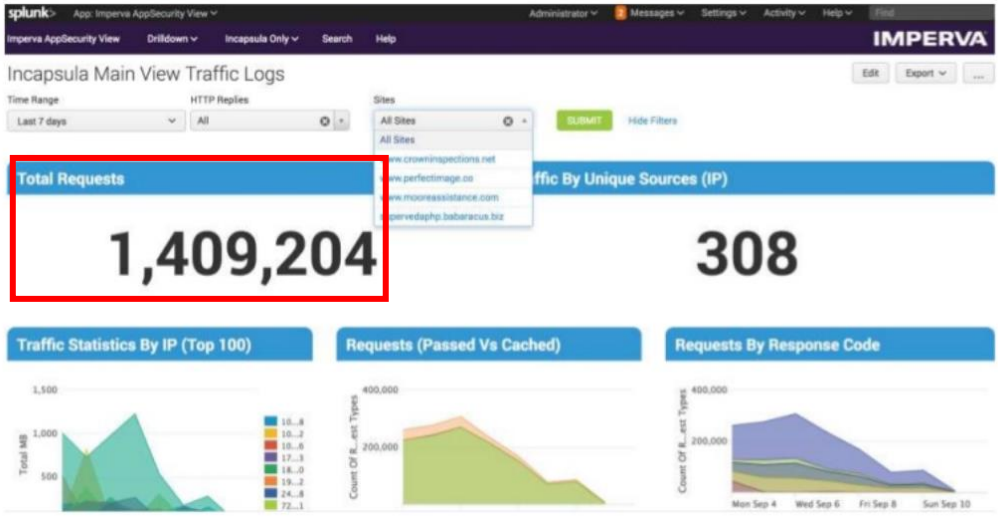


Figura 3-8 Integración con SIEM Splunk

Es posible implementar fácilmente una pantalla de autenticación de dos factores ante cualquier página, subdominio o grupo de direcciones URL. Mediante una integración de un solo clic es posible asegurar cualquier área administrativa, entorno de ensayo, aplicación web corporativa u otros activos web.

En la figura 3-9 es posible identificar los métodos y notificaciones de autenticación que pueden ser configurados en Incapsula.

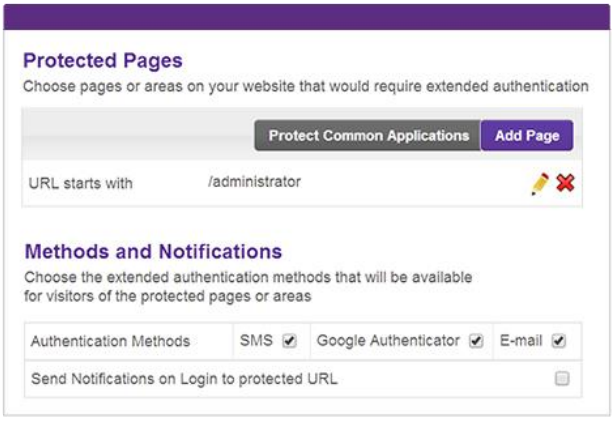


Figura 3-9 Autenticación de dos factores

Es posible controlar completamente qué bots y visitantes humanos pueden acceder a la aplicación. Unos controles detallados permiten el filtrado del tráfico según distintos factores, incluidos la identidad del declarante, la geo ubicación y el parámetro de URL.

En la siguiente figura 3-10, se muestra cómo es posible identificar el flujo de filtrado de tráfico, esto es que el flujo puede tener dos destinos.

1. El tráfico legitimo hace la petición a Incapsula, este lo reconoce como tráfico limpio y lo deja pasar a los servidores web.
2. Tráfico de dudosa procedencia, Incapsula lo detecta y lo desecha.

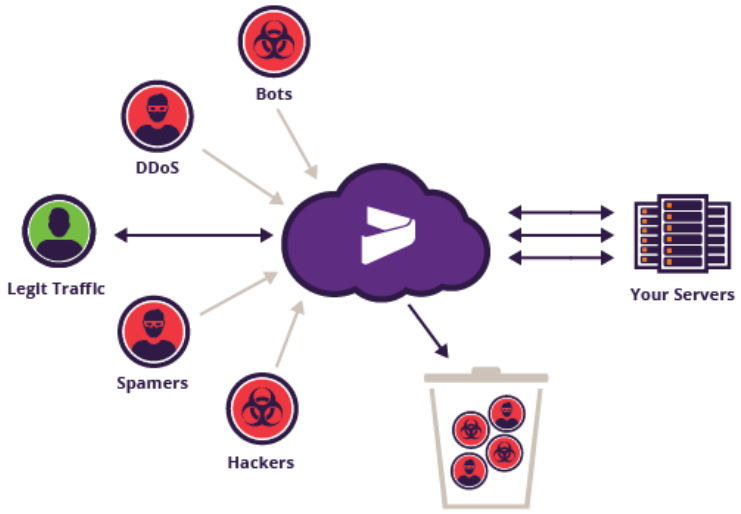


Figura 3-10 Filtrado de tráfico

3.2.2 Protección DDoS

Incapsula puede proteger una organización de cualquier amenaza de DDoS, lo cual se divide en 3 tipos:

- Protección de sitios WEB

Detecta y mitiga automáticamente los ataques contra sitios y aplicaciones web.

- Protección de Infraestructuras

Protección bajo demanda o permanentemente (Always-On) frente a ataques DDoS dirigidos directamente contra la infraestructura de la red del cliente.

La protección de infraestructuras puede utilizarse para proteger subredes completas o direcciones IP individuales.

- Protección para servidor de nombres

Protección DDoS permanentemente (Always-On) para el servidor de nombres del cliente, el cual protege los servidores DNS frente a ataques a la capa de aplicación y la red.

Esta protección para servidor de nombres también acelera las respuestas de DNS.

Esta protección es compatible con las tecnologías Unicast y Anycast para impulsar una metodología de defensa de "muchos a muchos", por lo que detecta y mitiga automáticamente los ataques que se aprovechen de las vulnerabilidades de los servidores y aplicaciones, los eventos de "ataque y fuga" y los botnets de gran tamaño.

La red global de alta capacidad de Incapsula, cuenta con 5 Tbps (terabits por segundo) de capacidad de barrido bajo demanda y puede procesar 30 000 millones de paquetes de ataque por segundo, por lo que puede defender con éxito a sus clientes.

Incapsula muestra los ataques en tiempo real y ofrece información procesable sobre los ataques de la Capa 7 del modelo OSI. El panel de control de seguridad de Incapsula permite analizar rápidamente los ataques y ajustar las políticas de seguridad sobre la marcha para detener los ataques a aplicaciones web.

Incapsula intercepta las solicitudes web para bloquear los ataques DDoS y que no lleguen a los servidores de origen del cliente. Incapsula detecta y mitiga cualquier tipo de ataque, como los de la figura 3-11 que se muestra a continuación:

Figura 3-11 Bloqueo de cualquier tipo de Ataque DDoS

3.2.3 Red de distribución de contenido (CDN)

Los sitios web que utilizan la CDN de Incapsula son un 50% más rápidos y consumen un 70% menos de ancho de banda gracias a:

- Tecnología de almacenamiento en cache dinámica basada en el aprendizaje automático.
- Topología de red de malla fiable y con capacidad de autor reparación.
- Sistema de transito de nivel 1 con intercambio de tráfico para una cobertura óptima.
- Numerosas opciones para el control de almacenamiento en cache.
- Purga rápida de la cache y propagación de reglas de almacenamiento en cache.
- Funciones de seguridad y disponibilidad integradas.

La red global de servidores de Incapsula, se encuentran estratégicamente situados para reducir el tiempo de ida y vuelta (RTT) del contenido y poder acercarlo más a los visitantes de su sitio web. Consta de 40 centros de datos alrededor del mundo (véase figura 3-11) con una capacidad de 5Tbps.

Figura 3-12 Mapa de la red global de Incapsula

Utiliza una tecnología de aprendizaje automático propia. Con ella, Incapsula puede almacenar en cache los archivos generados dinámicamente y garantizar un contenido actualizado. Esta tecnología mejora considerablemente la utilización de la cache y reduce aún más el consumo de ancho de banda.

Utiliza una amplia variedad de tecnologías de optimización de contenido y redes para reducir al mínimo el tiempo de carga de las páginas y mejorar la experiencia del usuario. Además de la minimización de archivos, la compresión automatizada, la reutilización de sesiones y el prepooling de la conexión TCP, Incapsula aprovecha también el análisis de frecuencia para garantizar que los archivos a los que se accede con más frecuencia reciban prioridad y puedan traerse directamente desde la RAM.

Incapsula cuenta con soporte para HTTP/2, el cual puede ser activado para cualquier sitio o aplicación web utilizando la red de distribución de contenido de Incapsula, lo que aumentara el rendimiento sin tener que actualizar la infraestructura original.

Con la CDN de Incapsula, el soporte de IPV6 se activa automáticamente para los sitios y aplicaciones web, proporcionando al instante ventajas empresariales, de rendimiento y de cumplimiento de la distribución de doble pila IPv4+IPv6.

En la figura 3-13, es posible observar el flujo de soporte para IPV6.

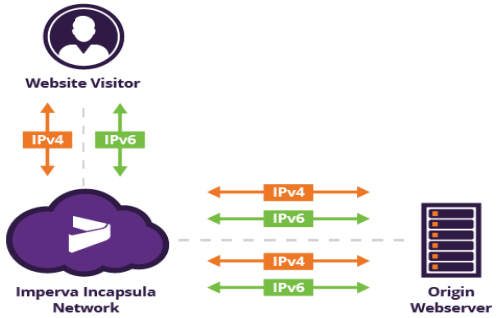


Figura 3-13 Soporte para IPV6

3.2.4 Balanceador de carga

Incapsula admite balancear la carga tanto en servidor local como global.

- Balanceador de carga del servidor local

Incapsula LBaaS admite distintos algoritmos de compensación de carga, con o sin opción de anulación de persistencia, para optimizar la distribución del tráfico en los servidores, maximizar el rendimiento de las aplicaciones y reducir la carga del servidor.

Las comprobaciones de rendimiento y estado del servidor en tiempo real detectan rápidamente las interrupciones y eliminan los tiempos de inactividad. Si un servidor falla, el enrutamiento se detiene hasta que se reanuda el funcionamiento del servidor.

En la figura 4-14, es posible observar el flujo de balanceo de carga del servidor local.

Figura 3-14 Balanceo de carga del servidor local

- Balanceador de carga del servidor global

Para aquellas organizaciones con varios centros de datos o entornos de cloud híbridos, la compensación global de carga del servidor garantiza la alta disponibilidad y el rendimiento fiable de las aplicaciones.

Incapsula admite la compensación global de carga del servidor basada en el rendimiento, que envía solicitudes al centro de datos con el mejor tiempo de conexión, así como GSLB basada en la ubicación geográfica, que distribuye la carga según la ubicación del usuario.

En la figura 3-15, es posible observar el flujo de compensación global de carga.

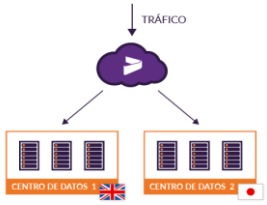


Figura 3-15 Balanceador de carga del servidor global

Incapsula admite la conmutación automática por error entre los sitios primario y secundario para permitir la alta disponibilidad y acelerar la recuperación ante desastres sin retrasos relacionados con el TTL.

En cuanto se detecta que su sitio primario se ha caído, se inicia un centro de datos de reserva automáticamente.

En la figura 3-16, es posible observar el flujo de conmutación automática por error de sitio.

Figura 3-16 Conmutación automática por error de sitio

El monitoreo continuo del estado y el rendimiento garantiza la disponibilidad de nuestros servidores web y centros de datos.

Las opciones incluyen:

- Monitoreo pasivo que comprueba de forma reactiva las repuestas del servidor al tráfico.
- Monitoreo activo que aborda de forma proactiva las solicitudes de comprobación del estado a los servidores web.

En la figura 3-17, se muestra las opciones a configurar en cuanto a monitoreo de servidores.

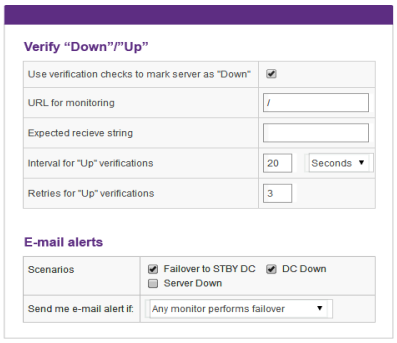


Figura 3-17 Supervisión de estado

El panel de control de Incapsula permite monitorear el tráfico de forma inmediata para verificar la distribución de carga adecuada.

También permite identificar y corregir problemas a medida que suceden, antes de que afecten a sus sitios web.

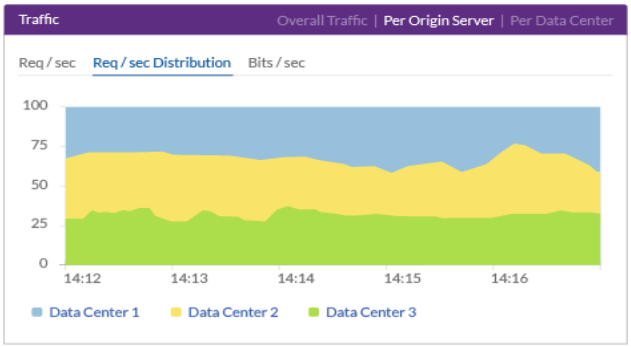


Figura 3-18 Paneles de control en tiempo real

3.3 Implementación

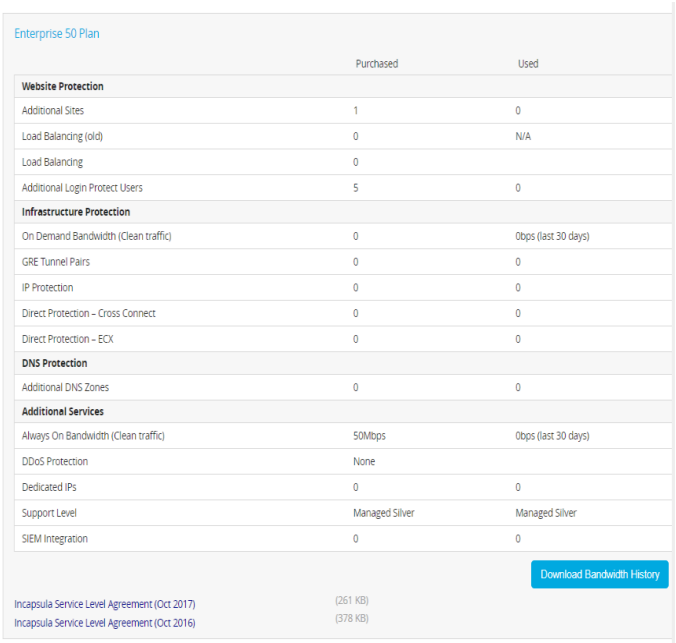
Antes de comprar algún licenciamiento, se requirió determinar la cantidad de bandwith (tráfico limpio) que consume el portal.

Prácticamente se usa un método llamado Burstable billing (facturación burstable), el cual se usa para calcular el tráfico de la cuenta. Este modelo se basa en el cálculo percentil del 95% del uso de ancho de banda para capturar el tráfico limpio. Este modelo permite el uso de picos que exceden los límites de la suscripción por breves periodos de tiempo en el caso de algunas incidencias.

Entonces basándose, en lo anterior, únicamente se cobra y cuantifica el tráfico limpio mas no el que Incapsula va a bloquear.

Por lo que el área comercial solicitó al cliente realizar una medición promedio de la trasferencia de datos por día, esto es, medir la cantidad de peticiones que llegan al servidor.

Una vez solicitada esta información, el área comercial se encargó de realizar la compra del licenciamiento de acuerdo a la cantidad de bandwith solicitada, lo cual incluye lo siguiente (figura 3-18):



Enterprise 50 Plan

	Purchased	Used
Website Protection		
Additional Sites	1	0
Load Balancing (old)	0	N/A
Load Balancing	0	
Additional Login Protect Users	5	0
Infrastructure Protection		
On Demand Bandwidth (Clean traffic)	0	0bps (last 30 days)
GRE Tunnel Pairs	0	0
IP Protection	0	0
Direct Protection – Cross Connect	0	0
Direct Protection – ECX	0	0
DNS Protection		
Additional DNS Zones	0	0
Additional Services		
Always On Bandwidth (Clean traffic)	50Mbps	0bps (last 30 days)
DDoS Protection	None	
Dedicated IPs	0	0
Support Level	Managed Silver	Managed Silver
SIEM Integration	0	0

Download Bandwidth History

Incapsula Service Level Agreement (Oct 2017) (261 KB)
Incapsula Service Level Agreement (Oct 2016) (378 KB)

Figura 3-19 Licenciamiento Incapsula

Una vez que este licenciamiento fue comprado, fue mi responsabilidad verificar que cumpliera con las especificaciones compradas.

Para que pudiera comenzar a realizar configuraciones en Incapsula, es necesario conocer datos en específico del portal, por lo que le proporcioné al cliente un listado de requerimientos para así tener un mapeo de la implementación, este se puede observar en la tabla 3-1.

Cabe destacar que, por motivos de confidencialidad de la empresa, la información de direcciones IP, URLS, registros, CNAMES, serán intercambiados como nombres genéricos.

General			
Requerimiento	**Opcional**	**Resultado**	**Comentarios**
Portal	**NO**	https://www.portal.com.mx/	Solicitar URL del portal
Registro A	**NO**	x.x.x.x	Solicitar IP asociado al portal
CNAME	**SI**	Portal.com.mx	Solicitar Canonical Name, en caso de que el portal cuente con el
HTTPS	**SI**	SI	Solicitar certificado al cliente y passphrase o .key en caso de que el portal cuente con uno
Personal que administra el firewall	**NO**	SecServices	Para poder restringir el tráfico a que solo este pase por las IP´s de Incapsula, se requiere saber quién realizará dichos cambios y aplicar las políticas necesarias en el firewall.
Personal que administra los DNS del portal	**NO**	Cliente	Para realizar los cambios de DNS, se requiere saber quién realizará dichos cambios
La IP del portal se encuentra asociada a otros portales?	**NO**	NO	Es necesario notificar si la IP se encuentra asociada a otros portales, ya que si esta se encuentra asociada a otros no será posible restringir el tráfico a solo las IP´s de Incapsula
Protección aplicativos web	**NO**	NO	Es necesario notificar al cliente que un WAF solo protege aplicaciones web, mas no activos que no lo son, por ejemplo: email, FTP, protocolos propios, etc.

Tabla 3-3-2 Listado de requerimientos

Una vez proporcionados los requerimientos, procedí a la validación de que fueran los correctos.

Al obtener el portal me fue posible validar su registro A e incluso CNAME, arrojando un comando en mi computadora de escritorio llamado NSLOOKUP.

Dicho comando puede ser usado en cualquier sistema Windows y sirve para consultar información en los servidores DNS.

Para fines didácticos se realizó el comando en un portal de prueba para su explicación:

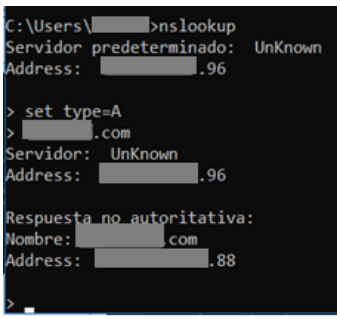


Figura 3-20 nslookup registro A

Como se puede observar al arrojar el comando nslookup e incluir set Type=A, será posible visualizar la dirección IP del portal.

Para saber el CNAME o bien canonical name, el cual es prácticamente un ALIAS del portal, se arrojó el comando set type=CNAME.

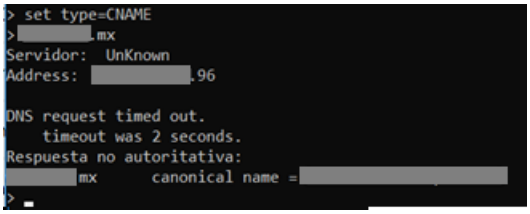


Figura 3-21 nslookup CNAME

Ahora bien, para poder saber si el portal cuenta con un certificado (HTTPS), fue necesario ingresar al portal y verificar si es una conexión segura.

Los indicadores visuales son:

- Un candado a la izquierda de la dirección URL.
- Prefijo de la URL con https en lugar de http.
- Sello de confianza.
- Barra de dirección de color verde.

Figura 3-22 HTTPS

3.3.1 Configuración

Incapsula puede ser usado desde cualquier sitio, únicamente ingresando por la url. No es necesario instalar algún software o comprar un hardware para su instalación o mantenimiento, de manera que entonces lo que hice desde las oficinas de la empresa donde laboraba fue lo siguiente:

Paso 1:

Ingresé a la configuración de Incapsula, por medio de la siguiente URL: https://my.incapsula.com/admin/login

En la figura 3-23, se observa la página de inicio de sesión al Incapsula.

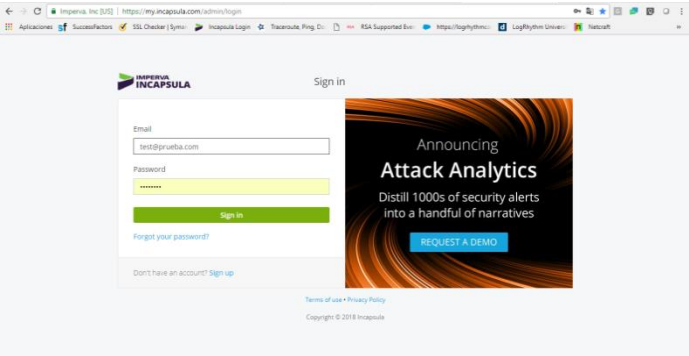


Figura 3-23 Inicio de sesión en Incapsula

Paso 2:

Al ingresar, apareció un apartado donde ingresé el sitio web.

En la figura 3-24 se indica en qué apartado añadir el sitio.

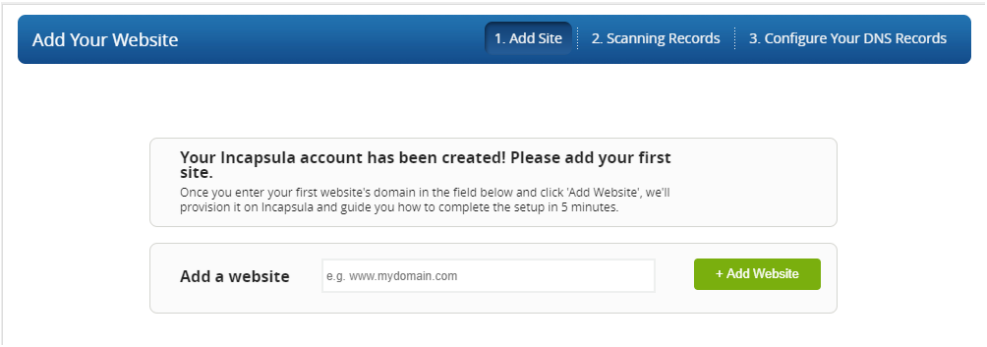


Figura 3-24 Carga de sitio web

Opcional:

Una vez añadido el sitio web, Incapsula me solicitó de manera opcional cargar el certificado, si es que el sitio web contaba con alguno (Figura 3-25).

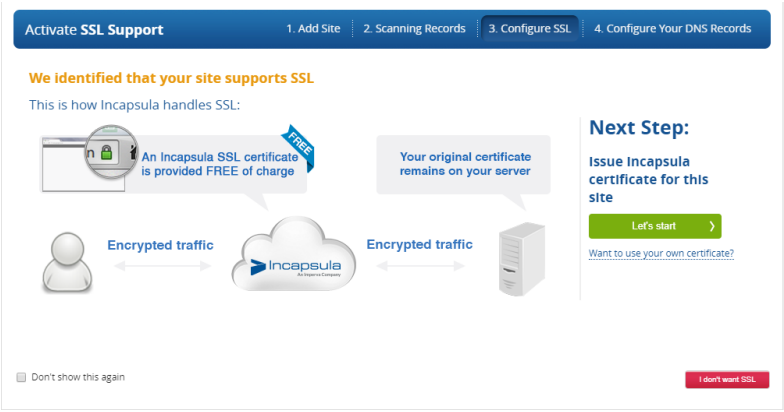


Figura 3-25 Activación de certificado

Una vez iniciada la configuración de certificado, se requirió usar el certificado existente en el portal, en caso de que se renovara el certificado se tendría que seleccionar la opción 2. (Figura 3-26). En este caso se utilizó la opción de usar un certificado existente.

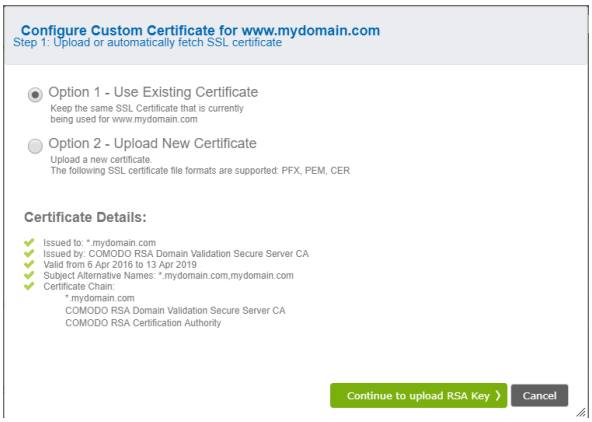


Figura 3-26 Configuración certificado

Dependiendo del tipo de certificado, Incapsula pedirá un archivo que contenga la llave privada. Este archivo puede ser en .PFX, .PEM, .CER. (Figura 3-27), por lo que cargué al Incapsula el archivo solicitado. Para este caso fue un archivo .PEM, el cual requiere un passphrase que es una llave privada.

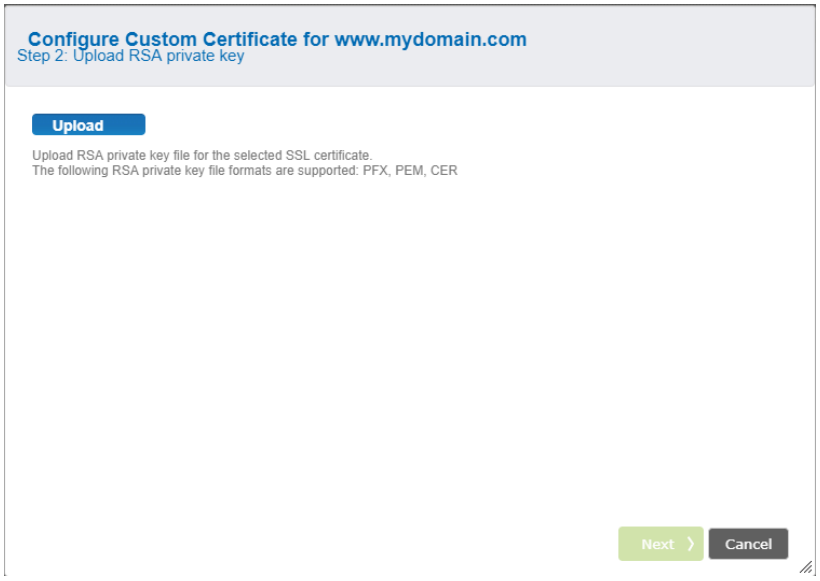


Figura 3-27 Carga de llave privada

Cabe destacar que para este paso es importante tener noción sobre certificados SSL y como se concatenan.

En sí, un certificado SSL que por sus siglas significa Secure Sockets Layer o bien capa de conexión segura, es un estándar de seguridad global que permite la transferencia de datos de manera cifrada entre un navegador y servidor web.

La capa SSL permite que se establezca una conexión segura y se instala en un servidor web y las funciones que brinda dicha instalación es autenticar la identidad del sitio web, asegurando al usuario que no se encuentra en un sitio falso y cifrar la información transmitida de un punto a otro.

El propósito de realizar dicha instalación en Incapsula es para mantener cifrada la información del punto origen a Incapsula y después al usuario, proporcionando un flujo cifrado de origen a destino.

Al ser un certificado .PEM, este debe brindarse en un archivo con terminación .pem y brindar la contraseña de dicho certificado previamente establecida.

Paso 3:

Incapsula requirió realizar cambios en las configuraciones de DNS para así poder enviar el tráfico a través de la red de Incapsula, en vez de ir directamente al servidor web. En la figura 3-28 se muestran los cambios que tienen que ser realizados.

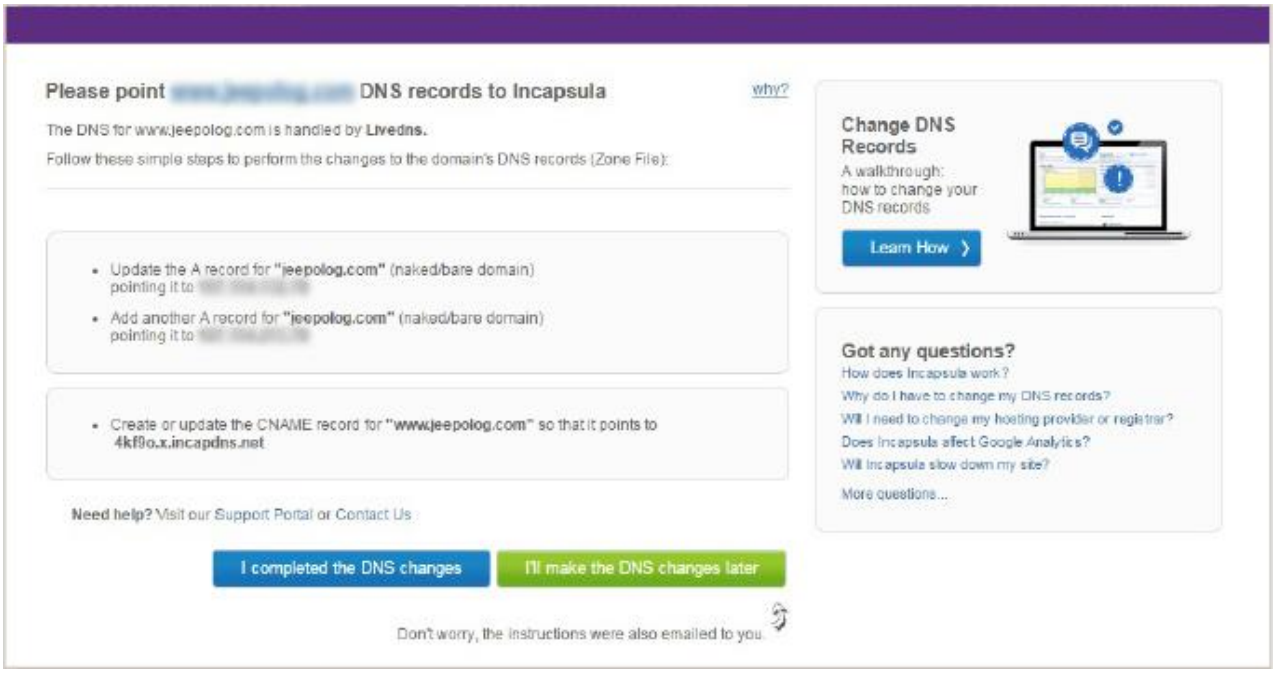


Figura 3-28 Configuraciones DNS

Paso 4:

Solicité al encargado del portal web realizar estos cambios y una vez realizados los cambios DNS, Incapsula comenzó a rutear el tráfico del sitio web a través de la red de Incapsula. Tomó algunas horas para que el tráfico pasara por incapsula a nivel mundial, esto debido a que el tiempo de propagación de los cambios de DNS puede durar hasta 72 horas, pero durante este periodo de tiempo no habrá pérdidas de visitas ya que estaría pasando directamente a los servidores web hasta que reconozca dicho cambio de ruteo de DNS.

A continuación, en la figura 3-29 se muestra cuando Incapsula detecta el tráfico.

Figura 3-29 Tráfico en Incapsula

Una vez realizado el cambio de DNS, se apreció que el portal se encontraba dado de alta en Incapsula.

3.4 Pruebas y liberación

Una vez realizadas las configuraciones de DNS por el administrador del portal web, verifiqué que este fuera propagado en su totalidad a nivel mundial. Cabe destacar que los tiempos de propagación llegan a ser de hasta 72 horas nivel mundial y cuestión de minutos a nivel ciudad.

Para que el tiempo de propagación sea menor, recomendé que el TTL (time to live) fuera de 5 minutos, por lo que solicité configurarlo, al menos por el periodo que tardaba en propagarse.

Por lo que lo valide con la siguiente página web (Figura 3-30): https://www.whatsmydns.net/

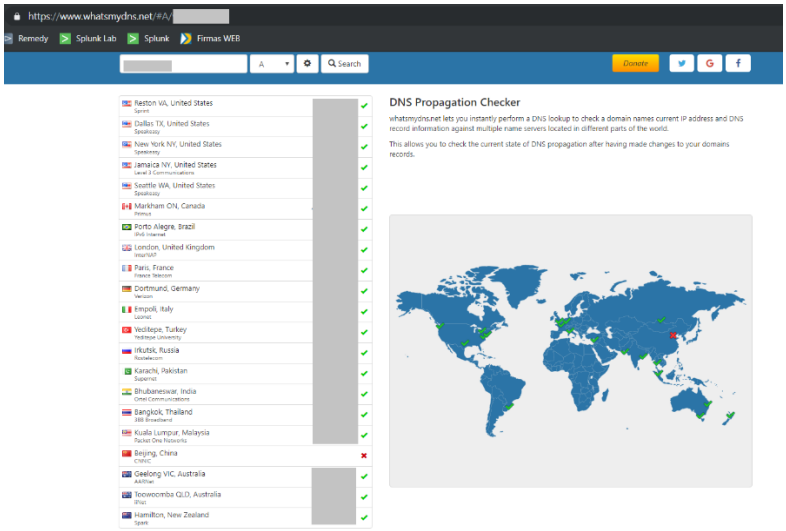


Figura 3-30 Propagación DNS

Una vez que determiné en su mayoría que este propagando, realicé un nslookup desde mi portátil de la siguiente manera (véase figura 3-31):

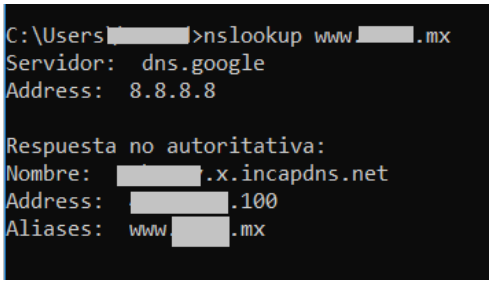


Figura 3-31 Nslookup

Otra prueba que realicé, fue ingresar al portal de MX toolbox y validé que el canonical name correspondiera al que Incapsula había brindado, por lo que aseguré la propagación (Figura 3-32).

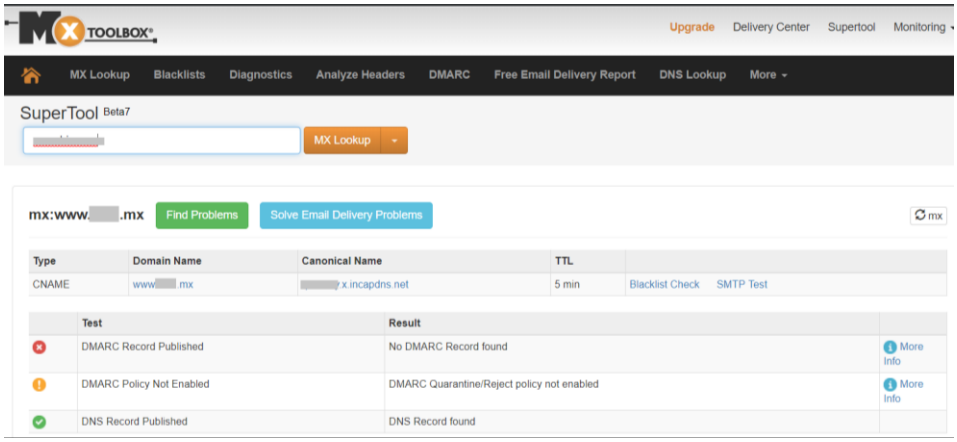


Figura 3-32 Validación canonical name y TTL

Realicé la validación de que el portal estuviera configurado en Incapsula y que ya estuvieran recibiendo tráfico, en la figura 3-33 se puede observar el portal configurado.

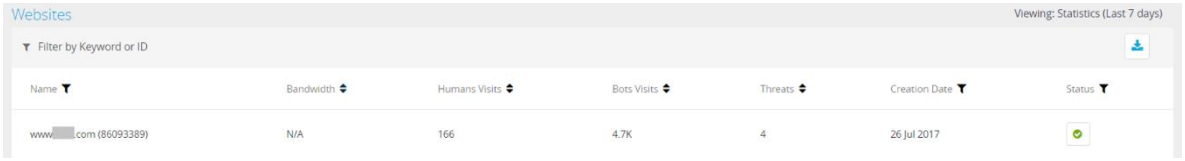


Figura 3-33 Portal configurado

CAPÍTULO 4

RESULTADOS

Capítulo 4 Resultados

Determiné que en un inicio se debiera dejar la configuración correspondiente a las mejores prácticas que proporciona el proveedor y lo monitoreé en un periodo de tiempo de 1 semana, para definición con el cliente de umbrales de acuerdo a sus necesidades.

4.1 Configuración de la consola

Servidores de origen múltiple

En el siguiente apartado se observan las siguientes características:

Server IPs: Es la IP origen del portal

Load Balancing Attributes: Distribuye las peticiones de usuarios entre los centros de datos y/o servidores de origen con el fin de lograr un rendimiento y tiempo de respuesta óptimo. Asegura una alta disponibilidad en el caso de un malfuncionamiento del servidor o centro de datos mediante el enrutamiento de tráfico a un servidor que se encuentre en buen estado.

El algoritmo de load balancing le indica al servidor origen, a que IP del servidor será ruteada. El modo last pending request hace que la siguiente solicitud se enrute al servidor de origen con el número más pequeño de solicitudes pendientes HTTP. Este modo es el de default y el recomendado por Incapsula (Figura 4-1).

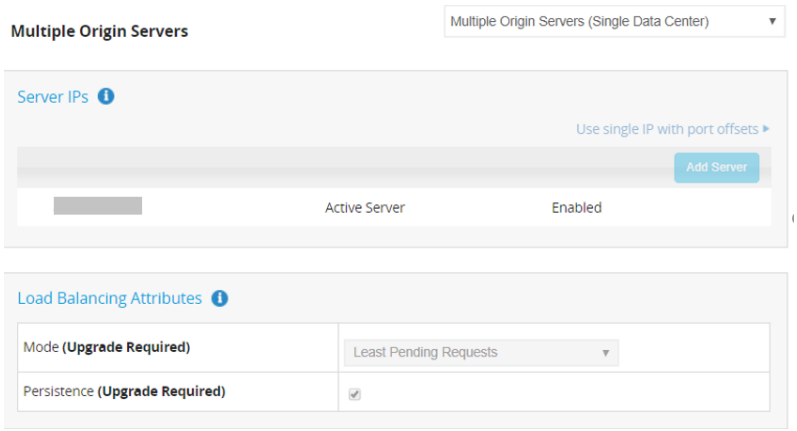


Figura 4-1 Multiple Origin servers

Como lo había mencionado anteriormente, no fue posible modificar la configuración de balanceo ya que el cliente no contaba con un server adicional para poder configurarlo.

Configuración del sitio

El portal lo definí con la siguiente configuración:

SSL Support: En este apartado se agregó el certificado del portal y es posible validarlo ya que se encuentra como activo.

HTTP/2: Activar HTTP/2 permite a los navegadores soportados tomar ventaja de las mejoras de rendimiento proporcionadas por HTTP/2 para su portal. Los navegadores que no lo soportan pueden conectarse por HTTP/1.0 o HTTP/1.1.

Web Seal: Permite al visitante saber que el portal está protegido y acelerado por Incapsula, no fue habilitado, ya que no es recomendable que el usuario final conozca porque herramienta está siendo protegido el portal.

Redirection: Redirige las peticiones de dominio simple de su sitio web a su dominio origen. En este caso únicamente fue aplicada la redirección al ingresar al portal de http a https (Figura 4-2).

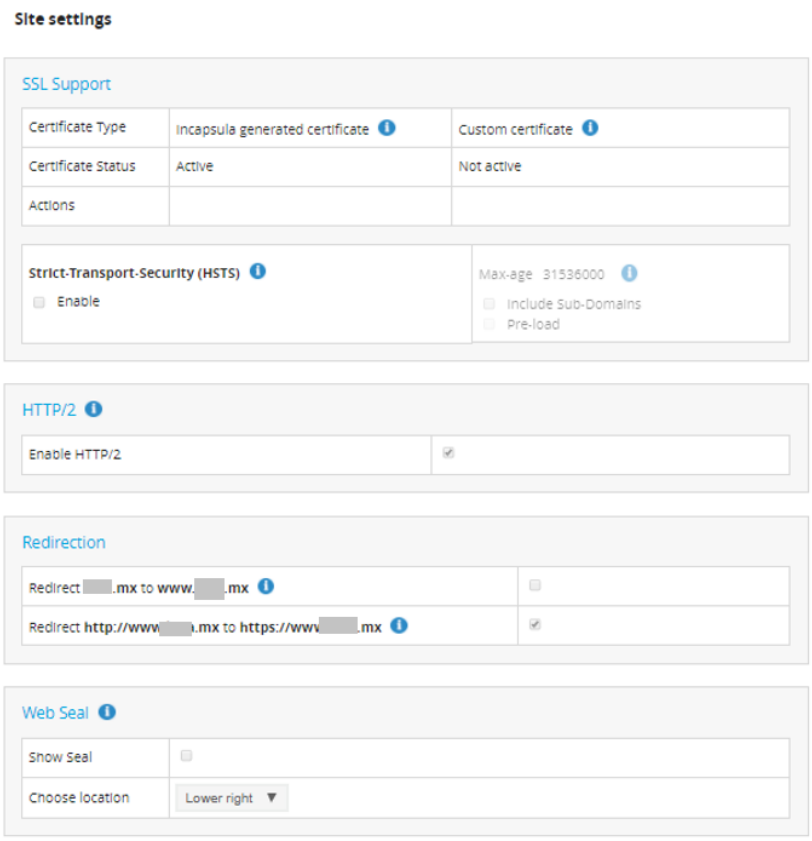


Figura 4-2 Configuración del sitio

Encabezados Incapsula

Para este caso es posible registrar información extra sobre las peticiones que los visitantes realizan, en versión TLS utilizada durante la sesión entre los usuarios finales y el proxy de Incapsula y el REQID sirve para asignar un ID.

Para este caso no fue habilitado ya que se requiere guardar dicho registro en el servidor mediante una configuración y para el cliente no fue algo de valor.

Como comentario adicional, para estos casos sería de valor si se contara con un SIEM que su trabajo es almacenar los logs de diversas fuentes en un tiempo histórico, para que posteriormente se pueda realizar un análisis sobre lo que está sucediendo de una manera más eficaz (Figura 4-3).

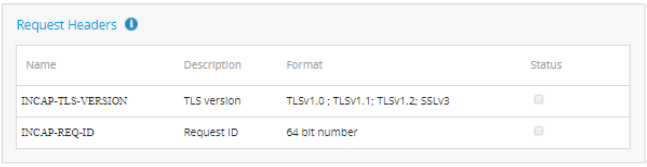


Figura 4-3 Encabezados Incapsula

DNS records

Esta sección muestra la información de referencia que los DNS records provee por Incapsula para la incorporación de su sitio.

Original DNS Settings: En esta sección se muestra la configuración del Sistema DNS que fue capturada inmediatamente antes de que se hiciera alguna configuración.

DNS Settings for Incapsula: Esta sección muestra las instrucciones de DNS que fueron emitidos por Incapsula para la incorporación del portal.

Para este caso, no es necesario realizar alguna configuración ya que solo muestra el DNS original y los cambios que fueron realizados posteriormente, el motivo de tener este dato es por si en un futuro se plantea realizar un cambio de retorno a la configuración inicial (Figura 4-4).

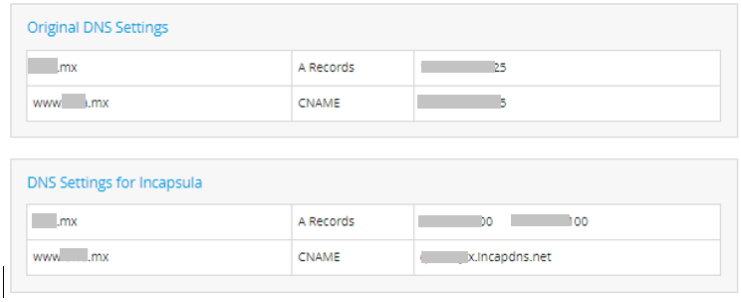


Figura 4-4 DNS records

Threats

A continuación, muestra los tipos de amenaza que Incapsula detecta y que tipo de respuestas puede tomar al detectar una (Figura 4-5).

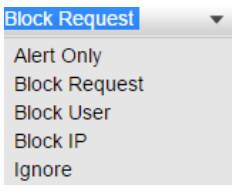


Figura 4-5 Amenazas

Se recomendó la siguiente configuración por mejores prácticas, (Figura 4-6):

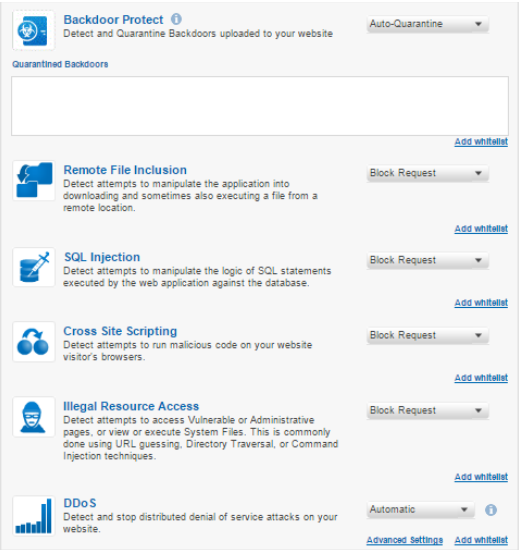


Figura 4-6 Configuración

Para este caso y como se puede observar en la imagen anterior, Incapsula tiene la habilidad de bloquear de manera eficaz intentando arrojar la menor cantidad de falsos positivos, por lo que se puede tener la confianza de aplicar dicho bloqueo. El tema aquí es que durante ese periodo de monitoreo de la herramienta, si hay algún elemento que este bloqueando o este creando un falso positivo se debe agregar a la White list.

En si para darse cuenta que no se esté bloqueando algún elemento y que este afecte a la producción del portal, se hace una revisión en cuanto a que este cargando correctamente las imágenes, que la carga del portal sea equivalentemente la misma antes de realizar el cambio, si hay un inicio de sesión, que en este se pueda acceder de forma correcta.

Para el caso de la configuración de DDoS se debe tratar con más cuidado, esto es que se debe considerar un estimado de peticiones por segundo realizadas al portal.

Por ejemplo:

Se estuvo monitoreando el portal en un aproximado de 7 días en el cual se tuvieron 3,826,499 peticiones.

En si se realizó un estimado de cuantas peticiones se han realizado y los picos que ha tenido durante el día, ya que no es la misma cantidad de peticiones que se realizan en la noche a las peticiones que se realizan en un día laborable o en un fin de semana.

Para realizar una media de esta sumatoria, se realizó la suma diaria de peticiones por día:

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
854,374	374,253	603,396	789,464	755,363	254,385	195,264

Tabla 4-1 Estimado de peticiones por día

Realizando la división entre los 7 días de la semana y sacar la media fue de: 546,642.71 por día.

Al realizar la conversión a segundos arroja un total de 6.32 peticiones por segundo.

Ahora bien, si deseamos obtener el pico en dicha revisión, podemos observar que el día Jueves fue cuando más peticiones se realizaron, obteniendo una conversión a segundos de 9.13 peticiones.

Por lo que podemos observar que el portal cumple con los requisitos para no rebasar las 1000 peticiones por segundo que Incapsula recomienda como detección de un ataque DDoS (Figura 4-7).

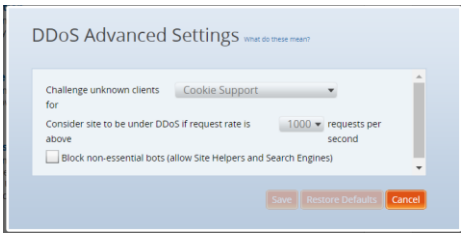


Figura 4-7 Configuración DDoS

Content Caching

Incapsula mantiene una red de entrega de contenido global (CDN). Las siguientes opciones de configuración le permiten determinar cómo está el cache y refresh de su sitio.

Los siguientes modos de cache son soportados:

Disable Caching – No recolecta contenido de cache.

Static Only – Cache acorde al encabezado HTTP estándar.

Static + Dynamic (Paid Plans Only) – Aplica un algoritmo de aprendizaje e identifica que contenido debe almacenar en cache. Si un cambio en el sitio es identificado el reaprendizaje se vuelve a activar. El periodo de tiempo que se configura determina la frecuencia con la que se actualiza la memoria cache.

Aggressive – Todo el contenido del sitio se almacena en cache.

En este caso se recomendó y aplicó la opción de Static + Dynamic ya que es posible evitar la saturación de servidores almacenando el contenido en cache ayudando incluso a que el servidor aumente en peticiones.

Para el caso de Xray, es para visualizar el portal en cuando a los cambios generados mediante un link pre generado.

Las reglas de guardado de cache prácticamente se encuentran configuradas para imágenes, documentos, ya que es viable que se encuentren almacenadas y no se esté generando la descarga en cada visita o carga del portal.

Al realizar este cambio mejoramos el tiempo de carga en el portal y también el consumo de bandwith del mismo.

En la figura 4-8, es posible apreciar las configuraciones realizadas.

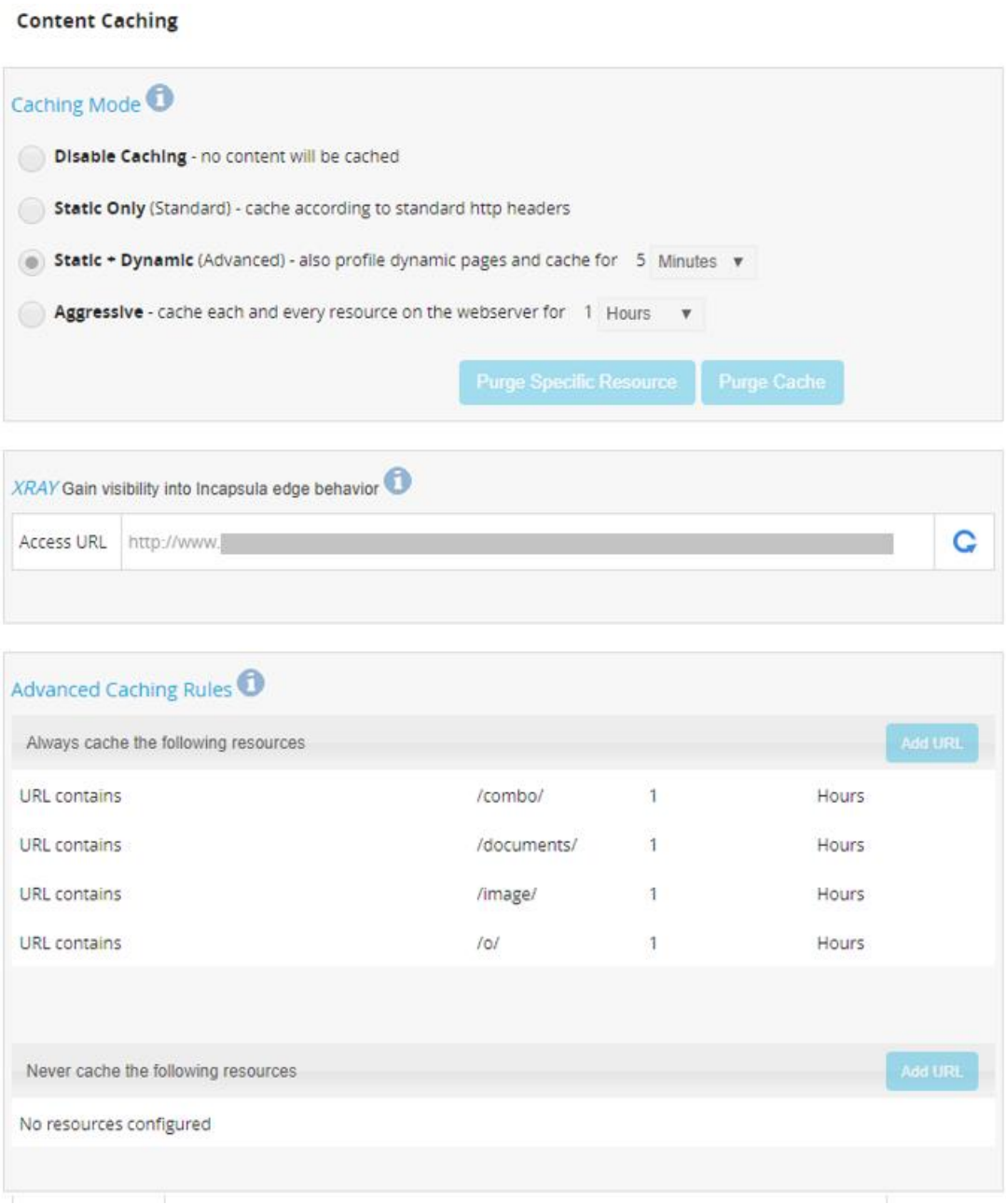


Figura 4-8 Configuración de cache

Para el caso de optimización, es prácticamente la compresión y mejora en cuanto a bandwith y carga de imágenes al tener peticiones en el portal.

En la Figura 4-9 se pueden observar las configuraciones realizadas para optimización.

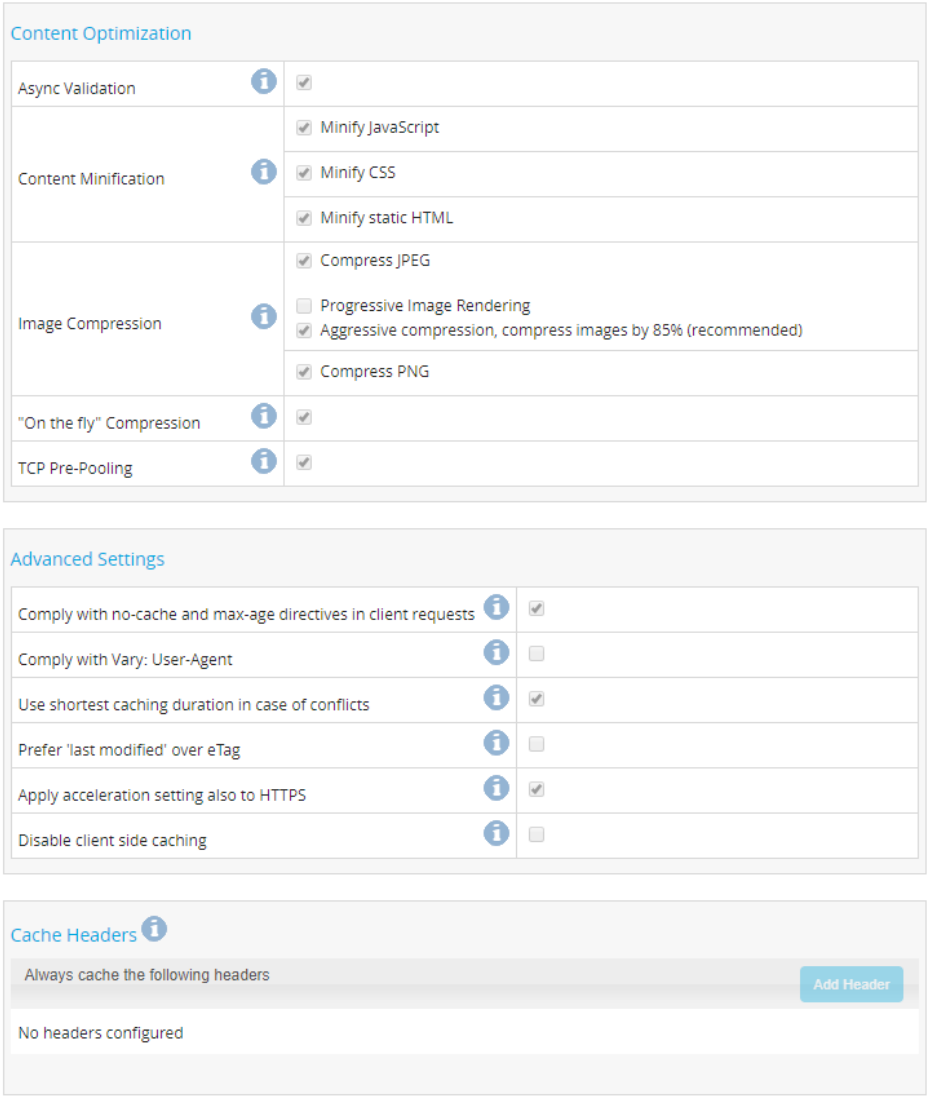


Figura 4-9 Configuración de cache

Seguridad

Se recomendó habilitar la siguiente configuración:

Good Bots: Todos los buenos motores de búsqueda están autorizados para acceder a su sitio. Si se desea evitar que un cierto bot tenga acceso es posible excluir esta bot de la lista.

Bad Bots: Todos los motores de búsqueda "malos" se le niega el acceso a su sitio. Si desea una lista blanda de un cierto Bot es posible hacerlo a través de una regla de acceso (add exception).

En la figura 4-10, es posible observar los diferentes tipos de bots y las configuraciones realizadas.

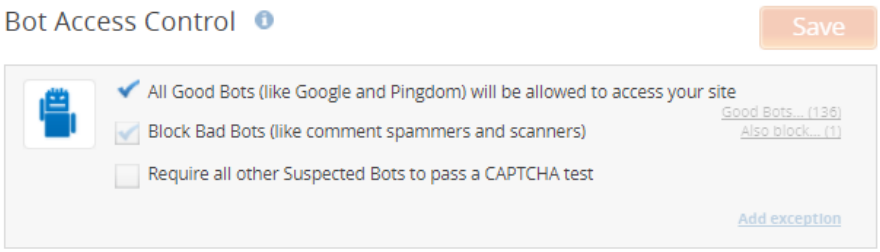


Figura 4-10 Bot Access Control

A continuación, es posible bloquear y permitir Ips, URLS y Ciudades en específico. Durante el periodo de monitoreo y administración de la herramienta se recomendó ir bloqueando o permitiendo dichas IP´s de acuerdo a las necesidades del cliente.

Por ejemplo, existen ciertas ciudades que no requieren acceso al portal o bien si existen demasiadas peticiones de IP´s que se encuentran en la blacklist, lo recomendable es bloquearlas.

En la figura 4-11, se aprecian los diversos bloqueos realizados.

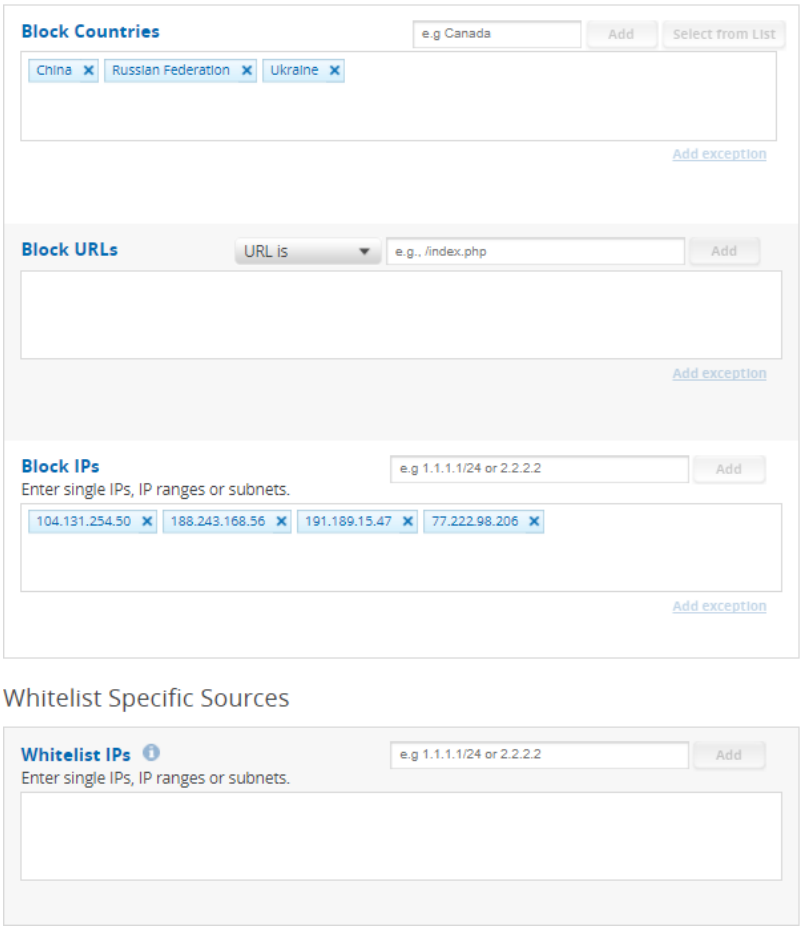


Figura 4-11 Bloqueo

Notificaciones

Para todos los portales llegarán las siguientes notificaciones de amenazas, esta configuración se encuentra por default y así se mantuvo ya que lo ideal es que estas notificaciones sean reportadas a los usuarios que se encuentran registrados en la herramienta, en este caso es el SOC quien lleva el monitoreo (Figura 4-12).

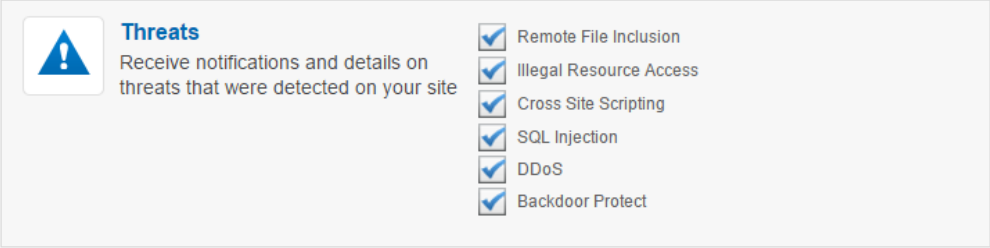


Figura 4-12 Notificaciones de amenazas

Actualmente Incapsula sigue protegiendo dicho sitio y alertando si encuentra algún tipo de amenaza que refiera a las mencionadas anteriormente.

Conclusiones

En el análisis inicial se realizó una comparativa entre diferentes servicios que provee un Firewall de aplicaciones WEB, así mismo se puede observar que al menos para este cliente lo ideal era realizarlo por uno en la nube ya que este ofrece un menor costo y requiere de hardware.
Brindé el servicio de seguridad en la nube en su totalidad, protegiendo la aplicación web.
Identifiqué los requerimientos iniciales para poder implementar dicho servicio usando las mejores prácticas proporcionadas por el fabricante y para otros casos, visualizar más adelante los eventos concurrentes para poder otorgar un bloqueo basándose en una investigación sobre los mismos.
Aseguré y protegí las aplicaciones web de ataques en específico (Top 10 OWASP) y bloqueé ataques DDoS basándome en el umbral definido.
Proporcioné un registro de actividad, en el cual es posible visualizar un histórico de eventos referente a 90 días, para detección y disminución de riesgos en la operación.
Una vez implementado y monitoreado durante 7 días, se comenzó a realizar la transferencia al SOC para que este pudiera seguir la administración y monitoreo del mismo.
El hecho de llevar a cabo esta implementación requiere diversos conocimientos que fueron aprendidos durante mi estancia en la Facultad de Ingeniería, cabe destacar que el aprender desde las materias de ciencias básicas, las cuales son la base de nuestra educación, hasta las materias que confieren a nuestro modulo que en mi caso fue Redes y Seguridad, tienen como objetivo atacar diversas áreas en el campo laboral.
Cuando ingresé al campo laboral, mi primer trabajo fue enfocado al área de Telecomunicaciones, por lo que no tiene mucha relación con el tema de Ingeniería en computación mucho menos con redes y seguridad. Sin embargo, fue posible demostrar mis conocimientos obtenidos en algunas materias, desde el hecho de realizar documentación, entender procesos y planes de trabajo, hasta configurar un switch, Gateway, el software de la herramienta para configuración de teléfonos y entender cuáles son los flujos de telefonía por voz IP.

Al ingresar a mi segundo trabajo que iba enfocado al área de Seguridad, aplique mis conocimientos inicialmente en Seguridad Informática, usando 3 conceptos fundamentales: confidencialidad integridad y disponibilidad.

Si nos detenemos a pensar un momento, el hecho de asegurar la confidencialidad de una empresa salvaguarda que personas ajenas a ella tengan acceso a ella y hagan mal uso, como puede ser: vender dicha información, utilizarla para saber los puntos débiles de la seguridad de la infraestructura de la red, entre otros.

Para el caso de la integridad, es importante tener la información identificada para que cuando un usuario haga cualquier cambio no autorizado nosotros podamos realizar el rastreo de dicho cambio.

Y, por último, es importante asegurar que la información esté disponible en todo momento, es por ello que muchas veces es necesario usar arquitecturas con alta disponibilidad (HA) para que en el momento de que llegue a ocurrir un incidente, el equipo que se encontraba en pasivo sea ahora el activo y no afecte a la productividad del cliente.

He visto temas enfocados a la arquitectura de diversas soluciones, en el cual si se requiere un equipo físico es importante revisar que se va a solicitar y para ello se requiere una planeación del proyecto. Una vez realizada esta planeación se realizan solicitudes en cuanto a Ips y es cuando he aplicado mis conocimientos de redes. Para el caso de la realización de arquitectura, es necesario tener noción de cuál será el flujo a realizar y cuáles son las dependencias para que este flujo cumpla las necesidades de la herramienta.

Para el caso de la implementación de un WAF en la nube, al realizar la implementación, fue necesario realizar un monitoreo de cómo estaba funcionando la herramienta y usar el tema de estadística para evaluar el rango de peticiones que se tenían sobre el portal.

Actualmente, en donde laboro va más enfocado al área administrativa que técnica, ya que debo de validar que cuando un equipo sea implementado cumpla con las características que se dieron en el alcance principal. En la parte técnica puedo decir que de acuerdo a los conocimientos obtenidos es posible determinar si algo es posible realizar o no y eso sumado a la experiencia obtenida en estos años hace que tenga noción de saber cómo salvaguardar la red.

Para poder salvaguardar la información de la red se tiene que tener ciertas bases en cuanto a normativas y estándares que fueron vistos en mi trayectoria escolar, en las que puedo destacar ISO 270001 como norma, la cual cumple con los rubros de confidencialidad, integridad y disponibilidad de los activos de la información del cliente.

Para el caso de estándar, puedo definir PCI DSS (Estándar de seguridad de datos para la industria de tarjeta de pago), este estándar va más enfocado a clientes que cuenten con un sistema de pago y este estándar cubre con un conjunto de normas de seguridad para facilitar la protección proactiva de los datos.

Por último, podemos definir que sin las bases necesarias no es posible realizar un análisis de los requerimientos del cliente, mucho menos tener la concientización de la importancia de los datos que este almacena y como protegerlos de la manera correcta.

GLOSARIO

Capítulo 5 Glosario

Ancho de banda

En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobytes por segundo (kbps), o megabytes por segundo (mps).

Dirección IP pública y privada

La IP pública es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o modems que dan a acceso a Internet, otros elementos de hardware que forman parte de su infraestructura, etc.

Son siempre únicas. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí. Por ejemplo, Un router con un servidor web. O dos servidores web entre sí.

La IP privada se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada.

En general, en redes que no sean la propia Internet y utilicen su mismo protocolo (el mismo "idioma" de comunicación).

Las IP privadas están en cierto modo aisladas de las públicas. Se reservan para ellas determinados rangos de direcciones. Son estos:

Para IPv4

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255
- 169.254.0.0 a 169.254.255.255

Dirección IP versión 4

En una red TCP/IP a cada computadora se le asigna una dirección lógica de 32-bits que se divide en dos partes: el número de red y el número de computadora. Los 32 bits son divididos en 4 grupos de 8 bits, separados por puntos, y son representados en formato decimal.

Cada bit en el octeto tiene un peso binario. El valor mínimo para un octeto es 0 y el valor máximo es 255. La siguiente figura muestra el formato básico de una dirección IP con sus 32 bits agrupados en 4 octetos.

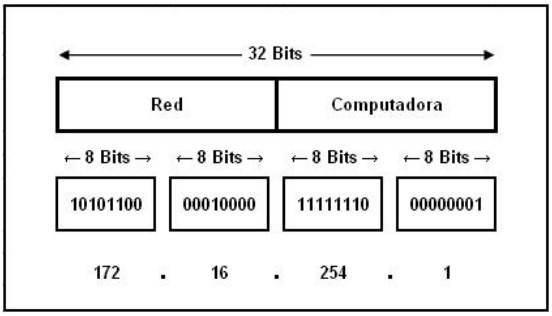


Figura 5-1Dirección IPv4

DNS (Nombre de dominio del servidor)

DNS, abreviatura del inglés que significa servicio de nombres de dominio, permite controlar la configuración de correo electrónico y sitio web de tu nombre de dominio. Cuando los visitantes van a tu nombre de dominio, la configuración de DNS controla a cuál servidor de la empresa se dirigen.

Dominio

Un dominio o nombre de dominio es el nombre que identifica un sitio web. Cada dominio tiene que ser único en Internet. Por ejemplo, "www.masadelante.com" es el nombre de dominio de la página web de Mas adelante. Un solo servidor web puede servir múltiples páginas web de múltiples dominios, pero un dominio sólo puede apuntar a un servidor.

Firewall

Un firewall es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- Una interfaz para la red protegida (red interna)
- Una interfaz para la red externa.

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

HTTPS (Hypertext Transfer Protocol Secure) y HTTP (Hypertext Transfer Protocol)

El Hypertext Transfer Protocol (HTTP), más conocido en español como Protocolo de Transferencia de Hipertexto, es un sistema utilizado en sistemas de redes, diseñado con el propósito de definir y estandarizar la sintaxis y la semántica de las transacciones que se llevan a cabo entre los distintos equipos que conforman una red.

La principal característica de este protocolo es que es un sistema orientado al funcionamiento del tipo "petición-respuesta", lo que significa que en la estructura debe existir un cliente y un servidor, siendo el cliente el que efectúe las peticiones y el servidor el que las responde. Las respuestas del servidor pueden ser la descarga de un archivo o la apertura de una página web, dependiendo del tipo de petición solicitada.

Básicamente, una vez que en el navegador escribimos una dirección web y presionamos la tecla "Enter", el servidor nos responderá devolviéndonos lo deseado.

En el caso del Hypertext Transfer Protocol Secure (HTTPS) o Protocolo de Transferencia de Hipertexto Seguro, el sistema se basa en una combinación de dos protocolos diferentes, HTTPS y SSL (Capa de conexión segura) /TLS (Capa de transporte).

Esta es la manera más segura y confiable de poder acceder a los contenidos que nos ofrece la web, ya que cualquier dato o información que introduzcamos será cifrada, lo que garantiza que no podrá ser vista por nadie más que el cliente y el servidor, anulando de esta forma la posibilidad de que pueda ser utilizada, ya que el ciberdelincuente sólo tendrá en sus manos datos cifrados que no podrá descifrar.

IP (Protocolo de Internet)

El Protocolo de Internet es un protocolo de capa de red (Capa 3) diseñado en 1981 para usarse en sistemas interconectados de redes de comunicación computacional de conmutación de paquetes. El Protocolo de Internet y el Protocolo de Control de Transmisión (TCP, Transmission Control Protocol) son la base de los protocolos de Internet. El IP tiene dos funciones principales:

- Entrega de datagramas a través de la interred en la modalidad de mejor esfuerzo
- Fragmentación y re ensamblado de datagramas

Se considera al IP un protocolo de "mejor esfuerzo", ya que no garantiza que un paquete transmitido realmente llegue al destino ni que los datagramas transmitidos sean recibidos en el orden en que fueron enviados.

La función principal de IP es llevar paquetes de datos de un nodo fuente a un nodo destino. Este proceso se logra identificando cada paquete enviado con una dirección numérica llamada dirección IP.

El protocolo IP no tiene mecanismos de confiabilidad (RFC 791) a diferencia de los demás protocolos. En vez de tener dichos medios, este protocolo no hace uso de ellos para que sean implementados por protocolos de capa superior. El único mecanismo de detección de errores es la suma de verificación para el encabezado IP. Si el procedimiento de la suma de verificación falla, el datagrama será descartado y con ello no será entregado a un protocolo de nivel superior.

REFERENCIAS

Capítulo 6 Referencias

BBC Mundo. (Junio 2019). Microsoft responsabiliza a la Agencia de Seguridad Nacional de Estados Unidos de propiciar el ciberataque masivo que afectó al menos a 150 países. Obtenido de BBC Web site: https://www.bbc.com/mundo/noticias-internacional-39918517

Comisión Nacional Bancaria de Valores. (Abril 2019). Incidente de seguridad de la información en una institución financiera. Obtenido de Gobmx Web site: https://www.gob.mx/cnbv/articulos/incidente-de-seguridad-de-la-informacion-en-una-institucion-financiera?idiom=es

D'Adamo. (Noviembre 2019). Soluciones WAF en comparación: el cuadran Mágico WAF 2018 de Gartner. Obtenido de consulthink web site: https://www.consulthink.it/es/soluciones-waf-en-comparacion-el-cuadrante-magico-waf-2018-de-gartner/

Garcia Demian, Arteaga Victor. (Junio 2019). Boletín de seguridad UNAM-CERT-2017-001 Alerta por ransomware Wannacry. Obtenido de Seguridad UNAM Web site: https://www.seguridad.unam.mx/boletin-de-seguridad-unam-cert-2017-002-alerta-por-ransomware-wannacry

Imperva. (Noviembre 2019) Changing DNS Settings at GoDaddy. Obtenido de Incapsula Support web site: https://support.incapsula.com/hc/en-us/articles/200627460-Changing-DNS-Settings-at-GoDaddy

Marvin G. Soto. (Noviembre 2019). Threat Hunting!. Obtenido de Medium web site: https://medium.com/@marvin.soto/threat-hunting-5e12c6137609

OWASP. (Mayo 2019). OWASP Top 10 – 2017. Obtenido de OWASP Web site: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Panda Security. (Junio 2019). ¿Qué es un Ransomware?. Obtenido de Panda Security Web site: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

Verisign. (Noviembre 2019). Todo lo que debe saber sobre certificados SSL. Obtenido de verisign web site: https://www.verisign.com/es_LA/website-presence/online/ssl-certificates/index.xhtml