DISEÑO DE PROTECCIÓN DE RED POR UN SISTEMA PREVENCIÓN DE INTRUSOS DE NUEVA GENERACIÓN PARA LA COMPAÑÍA ONA SYSTEMS

HERNANDO TRUJILLO DAZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

DISEÑO DE PROTECCIÓN DE RED POR UN SISTEMA PREVENCIÓN DE INTRUSOS DE NUEVA GENERACIÓN PARA LA COMPAÑÍA ONA SYSTEMS

HERNANDO TRUJILLO DAZA

Proyecto de Grado – Proyecto Aplicado presentado para optar por el titulo de ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Martín Camilo Cancelado Ruiz
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogota., 22 de febrero de 2021

DEDICATORIA

Este trabajo se lo dedico principalmente a mi familia que siempre me acompaño en esta especialización y me dio ánimo, también a los diferentes tutores de la UNAD que me capacitaron para llegar a este punto.

AGRADECIMIENTOS

Quiero agradecer a la UNAD por darme la oportunidad de continuar con mis estudios que a pesar de la dificultad del tiempo se ajusto perfectamente a mis horarios, a mis padres que su guía me ha llevado a siempre seguir preparándome y me enseñaron que el aprendizaje nunca termina.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

GLOSARIO

DDoS: Denegación de servicio es un tipo de ataque que llena los recursos de un sistema.

Dominios: Nombre de un sitio web.

Gartner: Empresa consultora y de investigación mas importante a nivel mundial.

Geolocalización: Ubicación geográfica de una conexión.

HDLP: Prevención de fuga de información de Host

IPS: Sistema de Prevención de Intrusos

Logs: Registros del Sistema

Red: Sistema de conexión de diferentes dispositivos Informáticos.

Reputación: Calificación de comportamiento de una IP, URL, APP.

Riesgo: Identificación de activos informáticos, sus vulnerabilidades y amenazas

Sensor: Equipo que detecta trafico en la red mediante un Sniffer.

Sistema Operativo: Software para administrar recursos de hardware.

SOC: Centro de Operaciones de Seguridad

UTM: Unified Threat management/Gestión Unificada de Amenazas.

RESUMEN

Al multiplicarse los ataques en Latinoamérica también se ha multiplicado en Colombia por lo que se hace necesario que todas las compañías empiezan a proteger sus redes con equipo más robustos de prevención de intrusos y esta compañía al prestar servicios para empresas del estado, financieras, aseguradoras que entre otras se vuelve blanco de posibles ataques.[1]

Se realizará el diseño de la red incluyendo de un equipo IDS/IPS (detección de intrusos/prevención de intrusos) para proteger las diferentes redes de la empresa (SOC, Invitados, Interna y servidores) de ataques externos (internet) o entre redes (equipos internos), el mediante las técnicas basadas en:

- Comportamiento: cuando hay un parámetro fuera de lo normal por ejemplo si un usuario se conecta diariamente cinco páginas y un día se conecta a mil esto será bloqueado.
- Geolocalización: los principales países que generan riesgo con medio oriente, china, Rusia, Venezuela, entre otros también serán bloqueados.
- Firmas: si hay un ataque que ya es conocido también será bloqueado.

la cual cubrirá Diseño de arquitectura, análisis de vulnerabilidades, la instalación física, la detección inicial sin bloqueos, la propuesta de política por cada subred, la aplicación de políticas, su afinamiento, trasferencia de conocimiento y entregables del proyecto. [2]

[1] (CAMJOL; Inteligencia Estratégica. [Sitio web]. Washington: CAMJOL. [Consulta: 10 abril 2020] Disponible en https://camjol.info/index.php/RPSP/article/view/2326 s.f.)

[2] (MCAFEE; McAfee Network Security Platform. [Sitio web]. Bogotá: MCAFEE [Consulta: 19 abril 2020] Disponible en https://www.mcafee.com/enterprise/es-es/products/network-security-platform.html s.f.)

ABSTRACT

By multiplying the attacks in Latin America, it has also multiplied in Colombia, making it necessary for all airlines to detect to protect their networks with more robust intrusion prevention equipment and this company when providing services for state companies, financial companies, insurance companies that among others, it becomes the target of possible attacks.

As the attacks in Latin America multiplied, it has also multiplied in Colombia, making it necessary for all companies to start protecting their networks with more robust intrusion prevention equipment, and this company by providing services to state companies, financial companies, insurance companies that among others, it becomes the target of possible attacks.

The network design will be carried out including an IDS / IPS (intrusion detection / intrusion prevention) equipment to protect the different company networks (SOC, Guests, Internal and servers) from external attacks (internet) or between networks (internal teams), using rules and techniques based on:

• Behavior: when there is a parameter out of the ordinary, for example if a user connects five pages daily and one day connects to a thousand, this will be blocked and quarantined.
• Geolocation: the main countries that generate risk with the Middle East, China, Russia, Venezuela, among others, will also be blocked.
• Signatures: if there is an attack that is already known, it will also be blocked.

which will cover Architecture design, vulnerability analysis, physical installation, initial detection without blockages, the policy proposal for each subnet, the application of policies, their refinement, knowledge transfer and project deliverables.

INTRODUCCIÓN

Actualmente la empresa cuenta con un equipo UTM que realiza la protección de la red de la compañía las cual se realiza es trabajo de asesores y ciberseguridad por lo cual están interesados en mejorar la protección de su red mediante la adquisición de un equipo que haga la labor de prevenir ataques de intrusos previendo el creciente número de ataques.

Se requiere tener cura en el delirio de defensa previendo ataques más sofisticados ya que cada día son descubiertas nuevas vulnerabilidades las cuales han sido atacadas en muchas compañías a nivel mundial y en Colombia llegando a las compañías a múltiples pérdidas y algunas hasta la quiebra.

En Colombia el creciente número de ataques informáticos van en crecimiento lo que ha llevado a que las compañías aseguren más sus activos de formación.

La razón para aplicar el proyecto es dar solución a una necesidad reciente de la compañía para mejorar la detección de intrusos, botnes y análisis de trafico en busca de gusanos, ataques de reconocimiento, DDoS, fuerza bruta, reputación, etc

Gartner, Inc. ha posicionado a McAfee como Líder en el Cuadrante Mágico de Gartner para Sistemas de Prevención de Intrusos (IPS) por décima vez consecutiva. Con el cambio a arquitecturas basadas en la nube, el papel de IPS está cambiando.

Al implementar este diseño deberíamos poder visualizar gusanos, ataques de reconocimiento, DDoS, fuerza bruta, reputación, etc. En nuestra red pudiendo no solo detectarlos si no también empezarlos a bloquear así poder ir ajustando las políticas desde la firma más crítica hasta la más relevante para mi red.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Actualmente la empresa cuenta con un UTM Watchguard[3] Que es un equipo encargado de proteger actualmente la red que incluye algunas líneas de protección sin embargo con la contratación por parte de una empresa militar del estado colombiano y las conexiones que se van a realizar desde el SOC(área que maneja los eventos de seguridad informática) por conexión remota a la empresa (VPN), se requiere subir el nivel de seguridad para prevenir ataques más sofisticados de posibles intrusos que quieran dañar la empresa, esto apoyara el proyecto de protección por capas que desea realizar la compañía Ona Systems iniciando perimetralmente por la primera línea de defensa mediante el IPS(equipo que previene intrusos informáticos) dentro del presupuesto aprobado.
Previniendo ataques más sofisticados, miles de vulnerabilidades son descubiertas cada mes, asimismo son explotadas y algunas empresas han llegado incluso a la quiebra por lo que cada vez más los directivos está manejando los datos como si fueran una mina de oro la cual debe proteger, en el mundo interconectado se puede recibir millones de ataques informáticos por día y al no contar con un equipo adecuado que pueda proteger la compañía los datos sensibles pueden verse comprometidos, si bien los principales ataques[4] se ven en los países más desarrollados en Latinoamérica en Brasil principalmente ha ido creciendo el número de ataques vientos afectado principalmente la pérdida de formación, seguido de la interrupción del servicio y finalmente lo daños en los equipos.[5]
Al ser esta compañía prestadora de servicios de ciberseguridad no puede quedarse atrás en este tipo de protección.

En el estudio publicado por TicTac[6] “Actualmente, el 45.5% de las denuncias se hacen por canales virtuales y en el transcurso de 2019, se han reportado 28.827 incidentes de ciberseguridad empresarial en el país, de los cuales 17.531 casos han sido denunciados ante la fiscalía.
De 2017 a hoy, se reportaron 52.901 denuncias de las cuales el mayor número de hurtos se realizan a través de medios informáticos (31.058), seguido por robo de identidad (8.037), donde Bogotá fue la ciudad que más incidentes reportó (5.308),

---

[3] (WATCHGUARD; Dispositivos firewall. [Sitio web]. Bogotá: WATCHGUARD [Consulta: 22 abril 2020] Disponible en https://www.watchguard.com/es/wgrd-products/firewall-appliances s.f.)
[4](BUGARINO HERNÁNDEZ, Fernando. Una propuesta de seguridad en la información: caso systematics de México, 2008. s.f.)
[5] (ASOBANCARIA; Desafíos del riesgo cibernético. [Sitio web]. Bogotá: ASOBANCARIA [Consulta: 22 abril 2020] Disponible en https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf s.f.)
[6] TICTAC, y Tendencias del Cibercrimen en Colombia. [Sitio web]. Bogotá: TICTAC [Consulta: 27 abril 2020] Disponible en https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/. s.f.

luego Cali (1.190) y Medellín (1.186).
Ante esta situación, el Teniente Coronel Alex Duran jefe del Centro Cibernético Policial, aseguró que “se ha realizado un incremento operativo del 27.5% respecto al año 2018, materializándose 241 capturas y 11 operaciones de impacto por diferentes modalidades de delitos informáticos contempladas en la Ley 1273 del año 2009, al igual por medio del servicio Cai Virtual 24/7 se han atendido 12.959 incidentes aumentando la capacidad de atención en un 53.7% respecto al 2018.”
En el país, los ataques por malware durante lo corrido del año (2020) crecieron un 612%, el monto pagado por rescate de información está entre los 32 millones y los 160 millones de pesos. Frente a este escenario, Colombia se encuentra entre los países que recibió el mayor número de ataques por ransomware en Latinoamérica con un total de 252 lo que corresponde al 30% después de Brasil y Argentina.”

1.2 FORMULACIÓN DEL PROBLEMA

¿Como mejorar la red de local de Ona Systems para tener una mejor protección frente ataques de amenazas por intrusos que pueda llegar a comprometer los activos de la información de la compañía?

2 JUSTIFICACIÓN

La razón para aplicar el proyecto es dar solución a una necesidad reciente de la compañía para mejorar la detección de intrusos, botnes y análisis de trafico en busca de gusanos, ataques de reconocimiento, DDoS, fuerza bruta, reputación, etc.

Cumplimiento de normativas tales como Artículo 38 de la Ley 1621 del 17 de abril de 2013: “COMPROMISO DE RESERVA. Los servidores públicos de los organismos que desarrollen actividades de inteligencia y contrainteligencia, los funcionarios que adelanten actividades de control, supervisión y revisión de documentos o bases de datos de inteligencia y contrainteligencia, y los receptores de productos de inteligencia, se encuentran obligados a suscribir acta de compromiso de reserva en relación con la información de que tengan conocimiento. Quienes indebidamente divulguen, entreguen, filtren, comercialicen, empleen o permitan que alguien emplee la información o documentos reservados, incurrirán en causal de mala conducta, sin perjuicio de las acciones penales a que haya lugar.[7]
Ley 599 del 24 de julio de 2000 (CÓDIGO PENAL). [8]
Artículo 194. “DIVULGACIÓN Y EMPLEO DE DOCUMENTOS RESERVADOS: El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor”.
Artículo 258. UTILIZACIÓN INDEBIDA DE INFORMACIÓN PRIVILEGIADA. El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, incurrirá en multa.

Articulo 269F: “VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes”.

---

[7] UIAF; Ley Estatutaria 1621 de 2013 [Sitio web]. Bogotá: UIAF. [Consulta: 6 mayo 2020] Disponible en https://www.uiaf.gov.co/sistema_nacional_ala_cft/normatividad_sistema/leyes/ley_estatutaria_1621_2013

[8] FUNCIONPUBLICA; LEY 599 DE 2000 [Sitio web]. Bogotá: FUNCIONPUBLICA. [Consulta: 7 mayo 2020] Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Gartner, Inc. ha posicionado a McAfee como Líder en el Cuadrante Mágico de Gartner para Sistemas de Prevención de Intrusos (IPS) por décima vez consecutiva. Con el cambio a arquitecturas basadas en la nube, el papel de IPS está cambiando.[9] Deteniendo los ataques nuevos y conocidos con sistemas de prevención de intrusiones basados en firmas y sin firmas. La detección de intrusiones sin firma encuentra tráfico de red malicioso y detiene los ataques para los que no existen firmas.

[9] (INFO SECURITY MEMO; Gartner Magic Quadrant For Intrusion Detection And Prevention Systems. [Sitio web]. Bogotá: INFO SECURITY MEMO [Consulta: 30 abril 2020] Disponible https://www.51sec.org/2018/11/10/gartner-magic-quadrant-for-intrusion-detection-and-pre s.f.)

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un sistema de IPS para la red de Ona Systems que permita mejorar la seguridad de la información de la compañía.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar posibles riesgos identificables para detectar vulnerabilidades en la de red perteneciente a la empresa Ona Systems.
- Efectuar análisis comparativo de IPS identificados en el cuadrante Gartner para la empresa Ona Systems que de un mejor esquema de protección.
- Analizar los logs de tráfico para recomendar políticas para ser aplicadas a los esquemas de contención.
- Diseñar políticas de acuerdo a los activos para proteger adecuadamente según el servicio y Sistema Operativo.
- Mejorar las políticas ya establecidas para bloquear de manera efectiva los ataques encontrados en la red.

4 MARCO REFERNCIAL

4.1 MARCO CONSEPTUAL Y TEÓRICO

Los IPS (prevención de intrusos) son las herramientas más fáciles de implementar que pueden dar una excelente relación costo beneficio ya sea a nivel de host(equipo final) o a nivel de red, basados en firmas y comportamiento que nos pueden ayudar a solventar un notable número de ataques, previniendo buena parte de las explotación de las vulnerabilidades.[10]

Firmas: cadena de caracteres que nos puede identificar un código malicioso.
Comportamiento: si detectan el comportamiento anormal como un mayor número de conexiones en era un bloqueo.
Vulnerabilidades: brecha de seguridad que puede ser explotadas por un intruso.[11]

Dentro de los tipos de protección cuando hablamos de capas hay una que siempre se ha considerado que puede cubrir un 60 por ciento de los ataques externos la protección por geolocalización ya que si una compañía no requiere recibir tráfico de países diferentes a Colombia sólo debería estar configurado para que reciba tráfico desde Colombia este bloqueo puede generar un alto nivel de protección de ataques externos.

Geolocalización: ubicación geográfica por país de origen.

Al implementar este producto deberíamos poder visualizar gusanos, ataques de reconocimiento, DDoS, fuerza bruta, reputación, etc. En nuestra red pudiendo no solo detectarlos si no también empezarlos a bloquear así poder ir ajustando las políticas desde la firma más crítica hasta la más relevante para mi red.

Gusanos: virus que se auto reproducción para infectar otros equipos.
Ataques de reconocimiento: identifican información como puertos abiertos y sistemas operativos en algunos casos hasta las versiones.
DDoS: denegación de servicio consiste en que llenar todos los recursos que tenga un equipo para que no puede seguir prestando servicio.[12]

---

[10] (INFOTECS; IPS: Sistema De Prevención De Intrusos [Sitio web]. México: INFOTECS [Consulta: 2 mayo 2020] Disponible https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html s.f.)
[11] (MOSCOTE MEDINA, Rafael Luis; Sistema De Detección Y Prevención De Intrusos Ips [Sitio web]. México: MOSCOTE MEDINA [Consulta: 3 mayo 2020] Disponible https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14341/1/84087203.pdf s.f.)
[12] (MCAFEE; Informe sobre amenazas [Sitio web]. Madrid: MCAFEE [Consulta: 3 mayo 2020] Disponible en: https://www.mcafee.com/enterprise/es-es/assets/reports/rp-quarterly-threats-mar-2017.pdf s.f.)

fuerza bruta: intentar conectar o autenticar con muchas claves hasta encontrar la correcta.
Reputación: existe una lista global donde se catalogan servicios, IPs, dominios, etc. por comportamiento, si alguien, genera un ataque inmediatamente se reporta y se puede bloquear por otro sistema previniendo que pueda tener el mismo ataque.

4.2 MARCO GEOGRAFICO

El área estudio comprende la ubicación geográfica de la compañía que es en Bogotá el barrio Morato, en la dirección Calle 103 N0. 70B – 25 Bogotá – Colombia por lo cual el área de estudio solo comprende al área de Bogotá.[13]

4.3 MARCO HISTÓRICO

Ona Systems es una empresa que ofrece estrategias de seguridad digital entre las comunicaciones y transacciones del usuario, los recursos tecnológicos y la información, para prevenir los ciberataques, proteger la ciberseguridad y dar cumplimiento con 20 años en el mercado en los cuales son ha ejecutado proyectos también de prevención de intrusos por lo que se hace necesario implementar un equipo directamente y dedicado exclusivamente a esta tarea.[14]

4.4 ANTECEDENTES O ESTADO ACTUAL

La compañía se ha caracterizado por su buena protección en la red local y presentado problemas críticos que afecten los activos de la información de la compañía para continuar por esta línea se requiere ir un paso adelante y estar preparados para ataques más sofisticados teniendo un equipo dedicado de nueva generación que pueda proteger la red.
El equipo UTM Watchguard está funcionando correctamente sin embargo la arquitectura y las políticas se diseñaron hace más de un año y se requiere no sólo replantear la seguridad con un nuevo equipo que adicionalmente venga con un diseño de las políticas que esté acorde con los nuevos activos informáticos de la compañía.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Se encontraron en la publicación gartner las dos principales el cuadrante líder unas

[13] (UCATOLICA; Marcos De Referencia [Sitio web]. Bogotá: UCATOLICA [Consulta: 5 mayo 2020] Disponible en https://repository.ucatolica.edu.co/bitstream/10983/2967/10/parte2.pdf s.f.)
[14] (ONASYSTEMS; Por Que Ona Systems [Sitio web]. Bogotá: ONASYSTEMS [Consulta: 5 mayo 2020] Disponible en https://www.onasystems.net/ s.f.)

visionarias y con el músculo financiero para poder ejecutar a este otro fabricante Cisco y McAfee,

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

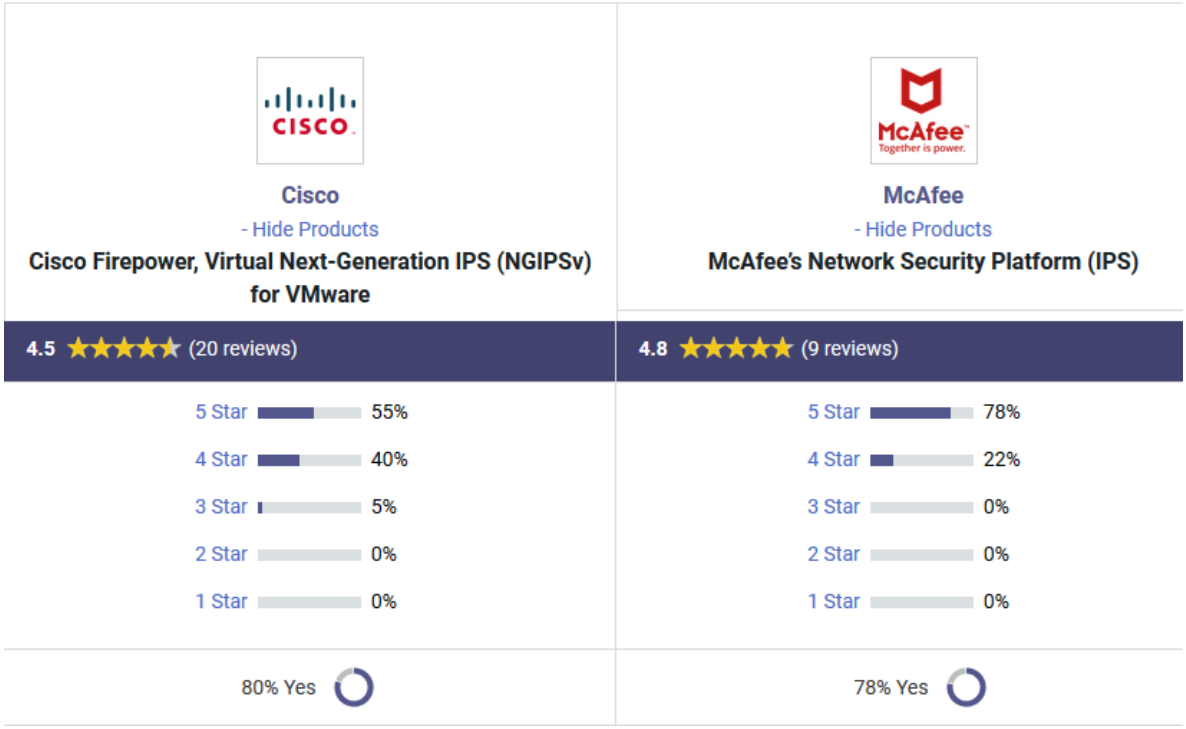
Fuente : TRENDMICRO; Global Threat Communications [Sitio web]. Mexico: TRENDMICRO [Consulta: 3 mayo 2020] Disponible en: https://blog.trendmicro.com/trend-micro-named-leader-2018-gartner-magic-quadrant-intrusion-detection-prevention-systems-idps/

El cuadrante mágico de Gartner para sistemas de prevención de intrusiones Gartner, Inc. ha posicionado a McAfee como Líder en el Cuadrante Mágico de Gartner para Sistemas de Prevención de Intrusos (IPS) por décima vez consecutiva. Con el cambio a arquitecturas basadas en la nube, el papel de IPS está cambiando.[15]

Este informe le proporciona: la dinámica del mercado de prevención de intrusiones en la red, los factores que impulsan el crecimiento del mercado y la creación de oportunidades únicas para Network IPS, y qué proveedores se posicionan como

[15] (INFO SECURITY MEMO; Gartner Magic Quadrant For Intrusion Detection And Prevention Systems. [Sitio web]. Bogotá: INFO SECURITY MEMO [Consulta: 30 abril 2020] Disponible https://www.51sec.org/2018/11/10/gartner-magic-quadrant-for-intrusion-detection-and-pre s.f.)

líderes, retadores, visionarios o jugadores de nicho en función de su visión completa y su capacidad para ejecutar.[16]

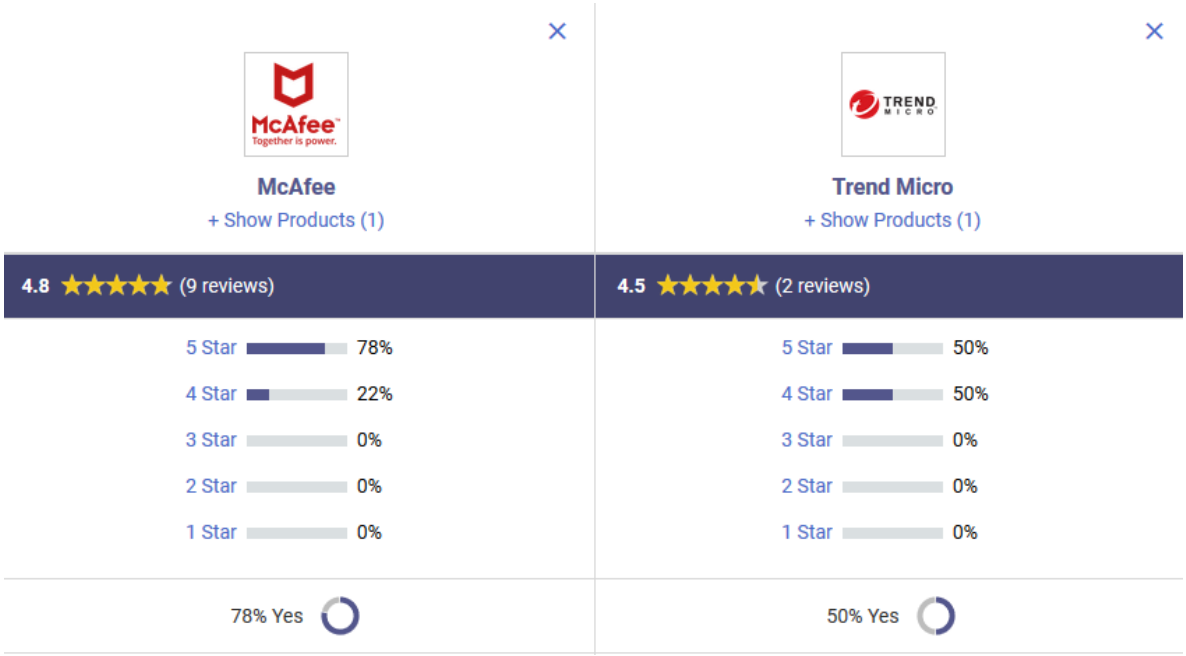


Fuente : Gartner; Comparing Cisco, McAfee. [Sitio web]. Bogotá: Gartner Comparing Cisco, McAfee [Consulta: 18 abril 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/cisco-vs-mcafee

Podemos ver que son equipos muy similares en protección, pero en precio McAfee es mucho más económico y al ser Ona Systems partner de McAfee el análisis de retorno de inversión se da más por McAfee manteniendo la misma protección. [17]

[16] (TRENDMICRO; Global Threat Communications [Sitio web]. Mexico: TRENDMICRO [Consulta: 3 mayo 2020] Disponible en: https://blog.trendmicro.com/trend-micro-named-leader-2018-gartner-magic-quadrant-intrusion-detection-prevention-systems-idps/ s.f.)

[17] (Gartner; Comparing Cisco, McAfee. [Sitio web]. Bogotá: Gartner Comparing Cisco, McAfee [Consulta: 18 abril 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/cisco-vs-mcafee s.f.)



Fuente : Gartner; Comparing Trend Micro, McAfee. [Sitio web]. Bogotá Gartner, McAfee [Consulta: 8 Junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/mcafee-vs-trend-micro

En el comparativo con la otra marca líder les damos cuenta que McAfee que es muy superior por lo cual esta marca no es tenida en cuenta para presentar a la junta directiva de la compañía.

4.6 MARCO LEGAL

La ley de protección de datos personales de la encargada de reconocer y proteger el derecho que tienen todas las personas a conocer actualizar y puede rectificar las informaciones que se han recogido sobre ellas ya sea en una base de datos o un archivo que sean susceptibles de manipulación y uso por parte de entidades públicas o también privadas.
Dentro de los tipos de datos existen los públicos, semi privados, privados y sensibles.
Toda esta información se puede encontrar directamente en la Ley 1581 de 2012.[18]

[18] (MINTIC; Ley 1581 de 2012 [Sitio web]. Bogota: MINTIC [Consulta: 3 mayo 2020] Disponible en https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf s.f.)

5 DISEÑO METODOLÓGICO

- Tipo de investigación
  El presente trabajo es de carácter descriptivo, va manejar un enfoque cuantitativo y también cualitativo[19] para lo cual se realizará una previa investigación de los vectores con más ataques poniendo en conjunto los servicios de la compañía Ona Systems los sistemas que maneja y los países que manera ataques elaborando con esto una hipótesis previa que nos permitiera generar con anticipación algunas predicciones aplicables a las reglas de bloqueo.

- Diseño
  Método observación: la respuesta única que utilizaremos será la recolección de datos ya que en la red se encuentra múltiples fuentes validar hemos en el último semestre del año pasado y en el primer cuarto este año cuales han sido las tendencias en vectores que ataques que realizaremos una visita a la empresa Ona Systems validaremos su sistema de protección actual para identificar posibles fallos de seguridad, mediante la recolección de log de último trimestre en el SIEM e informes de ataques, también el diagrama de red actual.
  Con esta información podemos hacer una interpretación de la información recolectada para posteriormente realizar una comparación y finalmente poder hacer una conclusión que nos lleve a proponer unas de protección de intrusos que nos permitan mejorar el nivel de seguridad perimetral.[20]

  Este proyecto nos tomará seis etapas

  1 **interpretativa**: se tomarán el problema actual interpretaremos los datos conseguidos procesados en el SIEM junto con la información de eventos además del mapa actual de red y realizaremos un estudio en el mercado

[19] (MONJE ÁLVAREZ; Metodología De La Investigación cuantitativa Y Cualitativa [Sitio web]. Neiva: MONJE ÁLVAREZ [Consulta: 8 mayo 2020] Disponible en https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf s.f.)

[20] (UIB; Los Métodos Y Las Técnicas De Recogida Y Producción De Los Datos [Sitio web]. Palma:UIB [Consulta: 10 mayo 2020] Disponible en : http://ibdigital.uib.es/greenstone/collect/portal_social/index/assoc/miso1098/7_001.dir/miso10987_001.pdf s.f.)

de los mejores equipos para prevenir intrusos.
2 **Trabajo De Campo**: visitaremos la empresa físicamente realizaremos el levantamiento de la estructura de la red las diferentes capas de seguridad que tengan como FW, antivirus, HDLP, proveedor de internet, análisis de vulnerabilidades con la herramienta OpenVas nos enfocaremos en las vulnerabilidades calificadas High [21], los sistemas operativos y servicios , con esto generaremos un diagnóstico más acertado del estado actual de la seguridad de la empresa Ona Systems.
3 P**ropuesta de Equipo**: en esta etapa crearemos la propuesta formal para la junta directiva de cuál es el equipo que le para proporcionar un mejor beneficio contra el costo que les puede generar y así poderles dar victorias tempranas y un pronto retorno de inversión.
4 **Pruebas:** en esta etapa un se realizarán las pruebas conectando el equipo la red sin realizar bloqueos solos recolectan información para diseñar unas reglas adecuadas poder solucionar el problema propuesto.
5 **Bloqueos:** con la información recolectada en la etapa anterior más la información recolectada previamente en la investigación inicial se crearán la reglas para generar el bloqueo de los ataques no deseados utilizando el estándar CIS Controls[22].
6 **Afinamiento y Entrega:** en esta etapa se realizará exclusiones de un falso positivo que pueda generar, mediante la validación del bloqueo confirmando por parte del administrador que no es un comportamiento anormal y que no representa ningún riesgo para posterior mente colocar en una lista blanca que el activo con la firma que fue reportada, también la documentación y transferencia de conocimiento para su entrega.

- Fuentes de información
  Las fuentes de información para este proyecto serán tomadas directamente de internet de los principales proveedores de seguridad como también directamente de la empresa la que se aplica el proyecto[23] [24]

Fuentes de Información	**Fecha de validación**
Internas	
Mapa de Red	Junio 2020
Políticas Actuales	Junio 2020

[21] (TENABLE; vulnerability-intelligence [Sitio web]. Bogotá: TENABLE. [Consulta: 6 mayo 2020] Disponible en https://es-la.tenable.com/cyber-exposure/vulnerability-intelligence#download s.f.)
[22] (CIS; CIS Controls [Sitio web]. Bogotá: CIS. [Consulta: 6 mayo 2020] Disponible en https://learn.cisecurity.org/cis-controls-download s.f.)
[23] (MCAFEE; Network Security Platform 9.1 Best Practices [Sitio web]. Bogotá: MCAFEE. [Consulta: 6 mayo 2020] Disponible en https://kb.mcafee.com/corporate/index?page=content&id=PD26779 s.f.)
[24] (CISCO; Best Practices NGIPS [Sitio web]. Bogotá: CISCO. [Consulta: 6 mayo 2020] Disponible en https://community.cisco.com/t5/network-security/best-practices-ngips/m-p/3550183?tstart=0 s.f.)

Requisitos Contractuales a Cumplir	Junio 2020
Externas	
NSP_91_Best_Practices_Guide_revl_en-us.pdf	Junio 2020
Best Practices NGIPS	Junio 2020

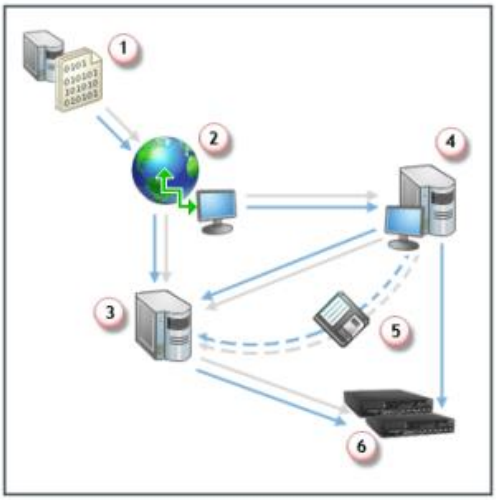
Tabla 1. Fuente de Informacion

- Equipamiento

  Previamente un equipo para instalar Kali con Open vas para muestras de activos y vulnerabilidades (Temporal).

  Entró el equipamiento se va requerir adicional a una persona que conozca muy el producto el sensor, 4 cables de red y un equipo con sistema Windows en el cual se va a instalar la manager, este último no debe ser un equipo dedicado puede ser cualquier equipo de la compañía por lo que no generará una inversión adicional.[25]

- esquema puesto [26]



Fuente: McAfee; Guía de Instalación: [Sitio web]. Bogotá: McAfee. [Consulta: 15 abril 2020] Disponible en https://docplayer.es/680518-Mcafee-host-intrusion-prevention-8-0-guia-de-instalacion.html

[25] (MCAFEE; Network Security Platform overview [Sitio web]. Bogotá: MCAFEE [Consulta: 12 mayo 2020] Disponible en : https://docs.mcafee.com/bundle/network-security-platform-9.2.x-installation-guide-unmanaged/page/GUID-08D8C803-4BBC-420B-80E1-E3C5018E6EB1.html s.f.)

[26] (McAfee; Guía de Instalación: [Sitio web]. Bogotá: McAfee. [Consulta: 15 abril 2020] s.f.)

6 CRONOGRAMA Y PRESUPUESTO

CRONOGRAMA DE ACTIVIDADES					
ACTIVIDAD	**MES 1-2**	**MES 3-4**	**MES 5-6**	**MES 7-8**	**MES 9**
1. Examinar posibles riesgos identificables					
1.1. Levantar información de activos de red	X				
1.2. Correr análisis de vulnerabilidades	X				
1.3. Analizar información	X				
1.4. Hacer informe	X				
2. Validar la mejor opción para la compañía en IPS					
2.1. Tomar información de sistemas en cuadrante Gartner		X			
2.2. Presentar a la junta de la compañía		X			
2.3. Acompañar en toma decisión y documentarla		X			
3. Diseñar políticas de acuerdo a los activos					
3.1. Diseñar políticas de IDS acordes a los sistemas operativos y servicios en la red.			X		
3.2. Aplicar políticas en sensores del IPS			X		
4. Analizar los logs de tráfico para recomendar políticas					
4.1. Validar en equipo las detecciones realizadas				X	
4.2. Diseñar políticas para contener ataques				X	

4.3. Aplicar políticas de bloqueo en sensores del IPS				X	
4.4. Realizar seguimiento a falsos positivos				X	
5. Mejorar políticas las políticas ya establecidas					
5.1. Comparar policitas en UTM Watchguard y proponer mejoras de acuerdo a diseño realizado					X
5.2. Aplicar políticas UTM Watchguard mejoradas					X
5.3. Realizar seguimiento a falsos positivos					X

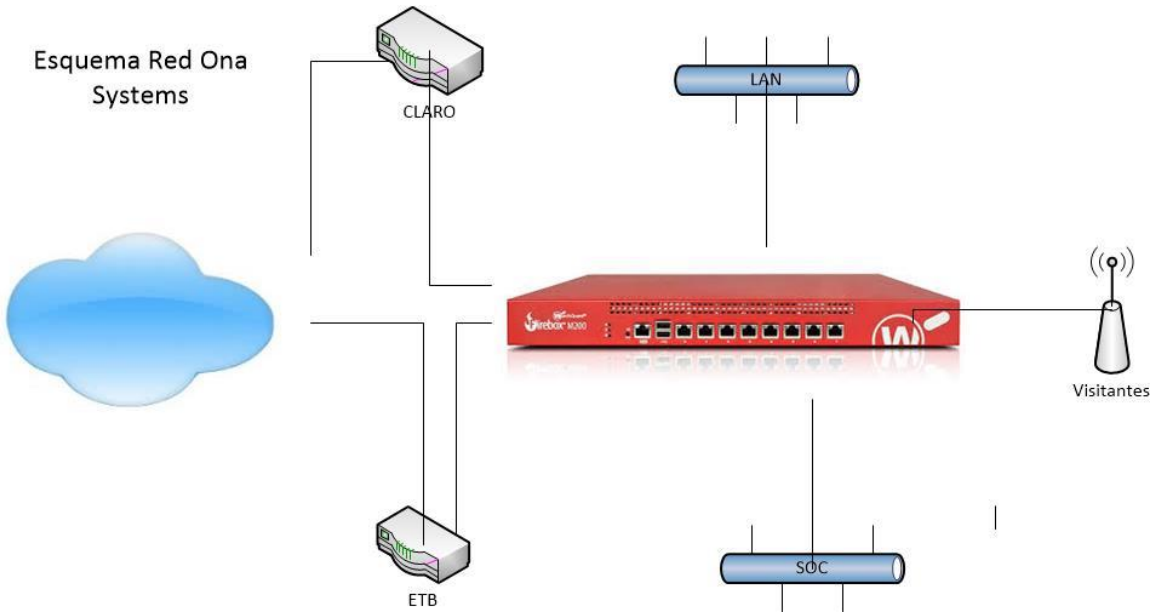
Tabla 2. Cronograma

7 DESARROLLO DE LOS OBJETIVOS

En este item, se debe desarrollar y presentar el resultado de los objetivos por medio de los subcapítulos, por ejemplo:

7.1 EXAMINAR POSIBLES RIESGOS IDENTIFICABLES PARA DETECTAR VULNERABILIDADES.

Realizamos el levantamiento del mapa de red sin publicar detalles de direccionamiento mas que la red interna, visitantes y SOC se encuentran en la red 192.168.x.x cada red dividida por mascaras en las cuales se realizara el escaneo de activos, puertos y vulnerabilidades de los mismos.



Fuente: Autor

Se realiza análisis de la red de SOC encontrando las dos máquinas que se utilizan para realizar las conexiones a otras empresas

Name	Hostname	IP
192[redacted]8.1	[redacted]eway	19[redacted]8.1
192[redacted]8.2	ONA[redacted]ocal	19[redacted]8.2
192[redacted]8.3	Or[redacted]s.local	19[redacted]8.3
192[redacted]8.4	dynamic-ip-181550169233	19[redacted]8.4

Fuente: Autor Analizador de Vulnerabilidades

Escaneos ejecutados

La red de Invitados no se analiza ya que no hay equipos actualmente por la cuarentena

Date	Status	Task	Severity	Scan Results				
				High	Medium	Low	Log	False Pos.
Sat Jul 4 23:21:02 2020	Done	LAN	10.0 (High)	48	52	35	770	0
Sat Jul 4 21:46:25 2020	Done	SOC2	10.0 (High)	4	2	0	81	0

Fuente: Autor Analizador de Vulnerabilidades

SE saca la lista de Sistemas operativos

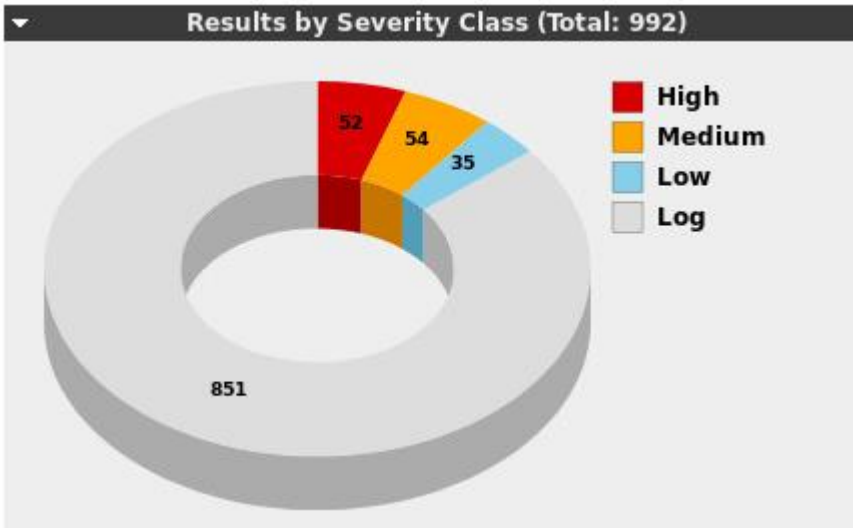
Name	Title	Severity			Hosts
		Latest	Highest	Average	
cpe:/o:canonical:ubuntu_linux:16.04		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:canonical:ubuntu_linux:18.04	Canonical Ubuntu Linux 18.04	10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:centos:centos:7		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:fedoraproject:fedora		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:grandstream:gxp1610_firmware:1.0.4.128	Grandstream GXP1610 Firmware 1.0.4.128	10.0 (High)	10.0 (High)	10.0 (High)	11
cpe:/o:grandstream:gxp1610_firmware:1.0.5.3		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:linux:kernel		10.0 (High)	10.0 (High)	10.0 (High)	20
cpe:/o:linux:kernel:3.10.0		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:microsoft:windows		10.0 (High)	10.0 (High)	10.0 (High)	6
cpe:/o:microsoft:windows_server_2016:-:-:x64		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:microsoft:windows_server_2019:-:-:x64		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:netbsd:netbsd		10.0 (High)	10.0 (High)	10.0 (High)	1
cpe:/o:vmware:esxi:6.7.0		10.0 (High)	10.0 (High)	10.0 (High)	2
cpe:/o:watchguard:fireware		10.0 (High)	10.0 (High)	10.0 (High)	2

Fuente: Autor Analizador de Vulnerabilidades

Se saca el detalle de todas las vulnerabilidades

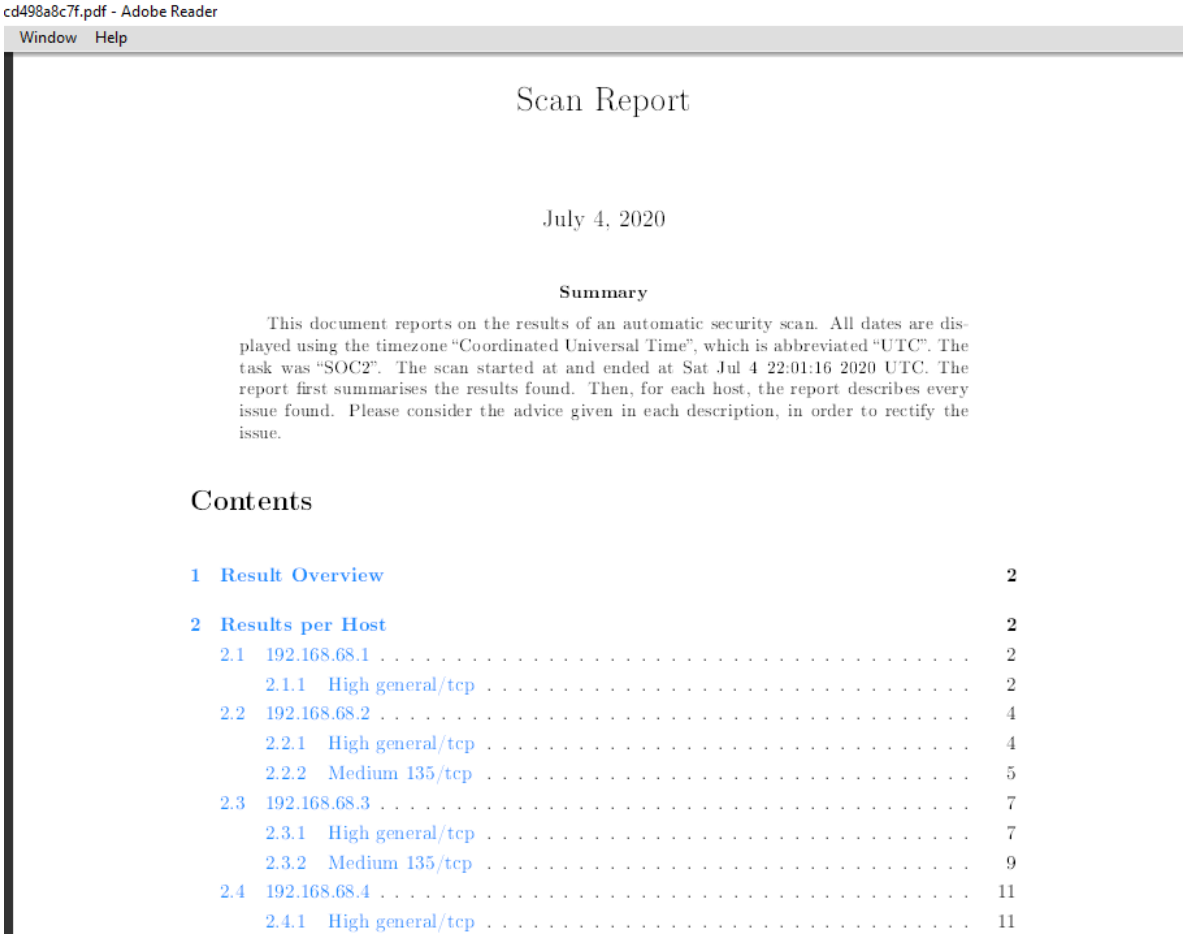
Vulnerability		Severity	QoD	Host
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].1 (es[redacted]ns.local)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].10
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].104
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].105 (V[redacted]s.local)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].106
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].11
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].120
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].162
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].2 (f[redacted]s.local)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].251
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].3 (os[redacted].local)
Mozilla Firefox Security Updates(mfsa_2020-20_2020-21)-Windows		10.0 (High)	97%	192.[redacted].3 (osb[redacted]s.local)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].30 (airport[redacted]ns.local)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].33 (d[redacted]cal)
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].5
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97%	192.[redacted].8

Fuente: Autor Analizador de Vulnerabilidades



Fuente: Autor Analizador de Vulnerabilidades

Y finalmente se exporta un PDF de cada análisis para el uso interno con todos los detalles para ser utilizado en el diseño de las políticas y algunas recomendaciones de mitigación de vulnerabilidades que no e incluyen en este proyecto


cd498a8c7f.pdf - Adobe Reader

Window Help

Scan Report

July 4, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "SOC2". The scan started at and ended at Sat Jul 4 22:01:16 2020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

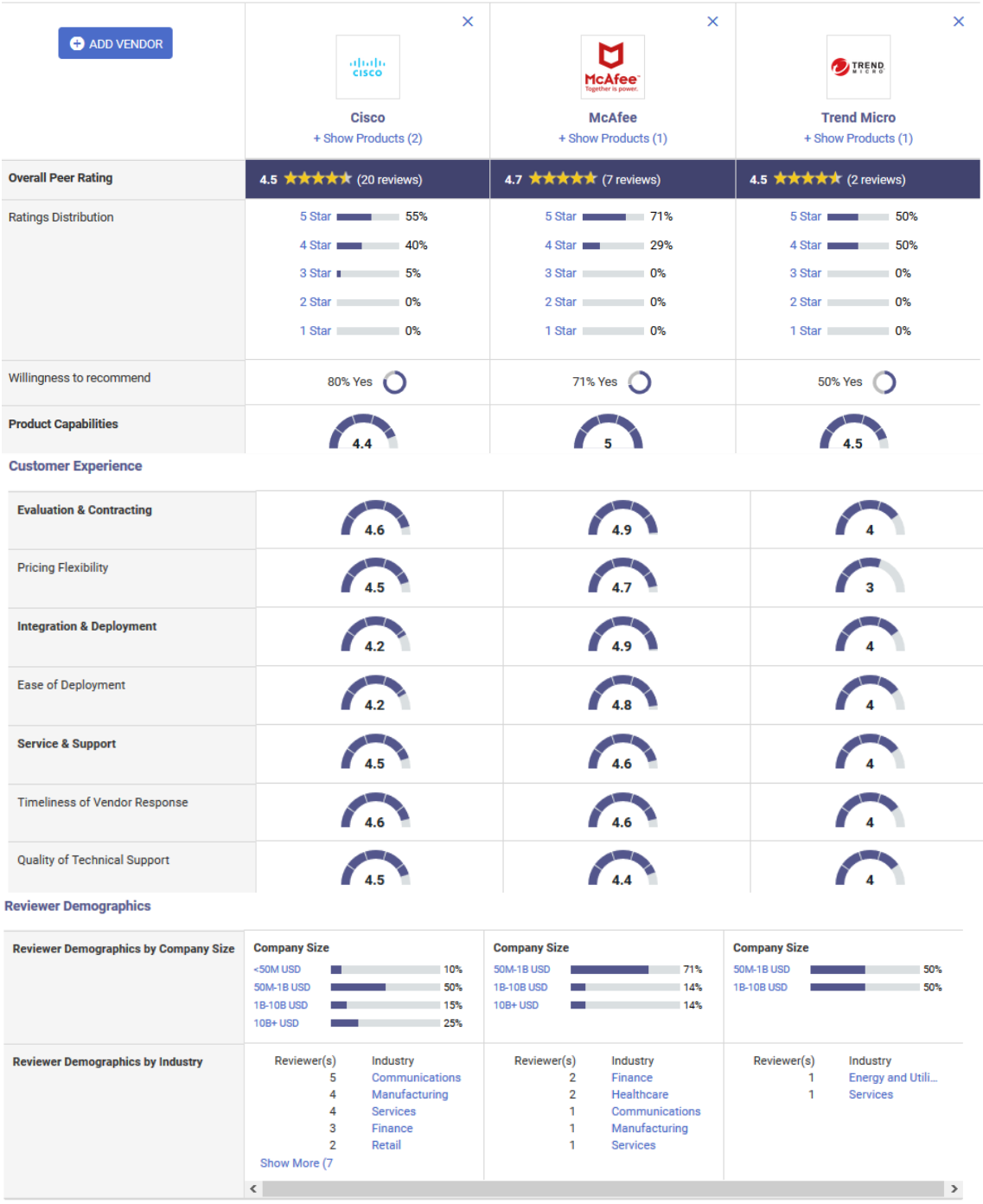
Fuente: Autor Analizador de Vulnerabilidades

7.2 VALIDAR LA MEJOR OPCIÓN PARA LA COMPAÑÍA EN IPS QUE DE UN MEJOR ESQUEMA DE PROTECCIÓN

Se realiza validación con las 3 mejores marcas en el cuadro gartber[27]

Definir y explicar criterios de comparación y análisis

[27] (GARTNER; firepower-vs-mcafee-network-security-platform-ips-vs-trend-micro [Sitio web]. Stamford: GARTNER. [Consulta: 16 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/product/firepower-vs-mcafee-netw s.f.)

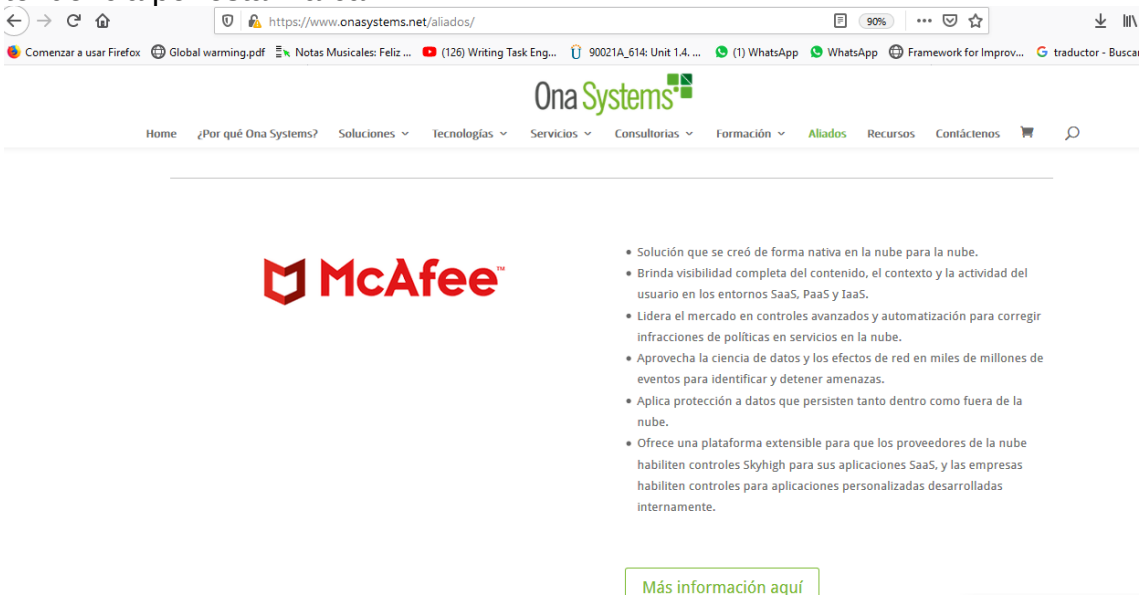


Fuente: GARTNER; firepower-vs-mcafee-network-security-platform-ips-vs-trend-micro [Sitio web]. Stamford: GARTNER. [Consulta: 16 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/product/firepower-vs-mcafee-network-security-platform-ips-vs-trend-micro

Cisco
Este producto combina dos tecnologías las características destacadas del FW ASA y la inspección avanzada de Snort no siempre dando buenos resultados y en ocasiones liberando versiones con problemas que pueden afectar la red.[28]

McAfee
Buen soporte, fácil de implementar, tecnología admirable, siempre están adelante sobre los riesgos Cyberneticos da visibilidad de los paquetes entrantes y salientes.[29]

Trend Micro
Esta herramienta verifica la cantidad y la frecuencia de conexiones entrante y saliente y así poder mantener los servidores arriba incluso cuando están siendo atacados.[30]
Actualmente Ona Systems es Partner de Mcafee lo que hace que la empresa tenga tendencia por esta marca. [31]



Fuente: ONASYSTEMS; Aliados [Sitio web]. Stamford: ONASYSTEMS. [Consulta: 18 junio 2020] Disponible en https://www.onasystems.net/aliados/

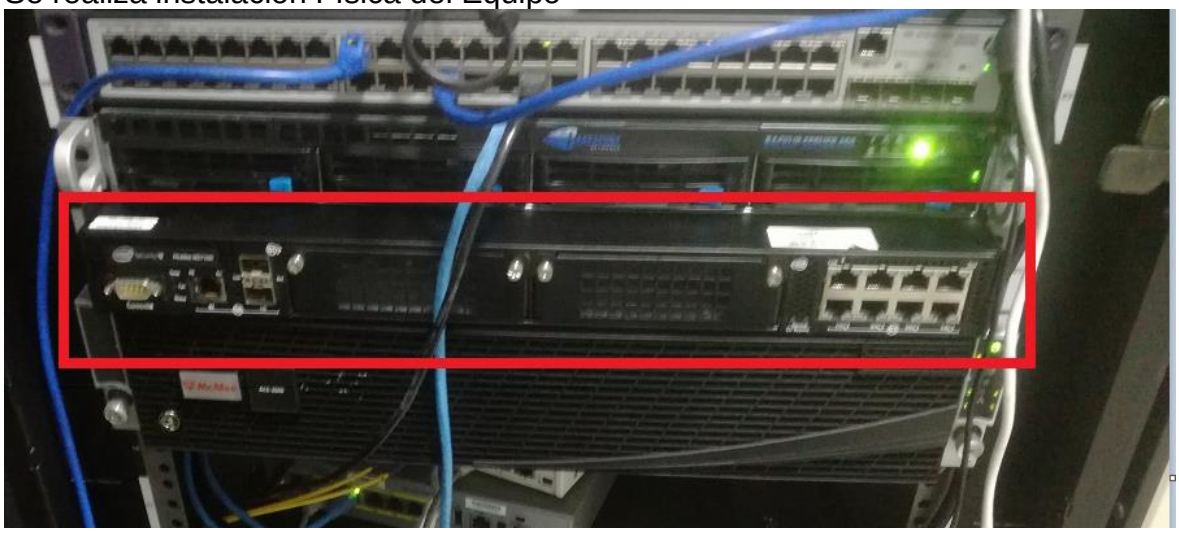
[28] (GARTNER; Cisco Firepower [Sitio web]. Stamford: GARTNER. [Consulta: 16 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/cisco/product/firepower s.f.)
[29] (GARTNER; McAfee's Network Security Platform (IPS). [Sitio web]. Stamford: GARTNER. [Consulta: 15 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/mcafee/product/mcafee-network-security-platform-ips s.f.)
[30] (GARTNER; Trend Micro TippingPoint NGIPS. [Sitio web]. Stamford: GARTNER. [Consulta: 17 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/trend-micro/product/trend-micro s.f.)
[31] ONASYSTEMS; Aliados [Sitio web]. Stamford: ONASYSTEMS. [Consulta: 18 junio 2020] Disponible en https://www.onasystems.net/aliados/

Después de analizar las 3 opciones y presentarlas a la junta directiva se llegó a la conclusión de utilizar el IPS de McAfee “McAfee Network Security Platform” por las siguientes razones.

- De los que están arriba del cuadrante es el que mas se adecua a lo requerido por la empresa.
- Al ser aliado de Ona Systems el costo puede bajar considerablemente por debajo de los demás.
- Se integra nativamente con el SIEM de ONA que es del mismo fabricante.
- Tiene excelente calificación en las pruebas NSS Labs.[32]
- En el comparativo técnico se destaca de los demás.

7.3 ANALIZAR LOS LOGS DE TRÁFICO PARA RECOMENDAR POLÍTICAS PARA SER APLICADAS A LOS ESQUEMAS DE CONTENCIÓN

Se realiza instalación Física del Equipo



Fuente: Autor

[32] NSS LABS; This report is Confidentialand is expressly limited to NSS Labs’. [Sitio web]. Washington: NSS LABS. [Consulta: 15 junio 2020] Disponible en https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-nss-labs-dcips-nsp-ns9100.pdf

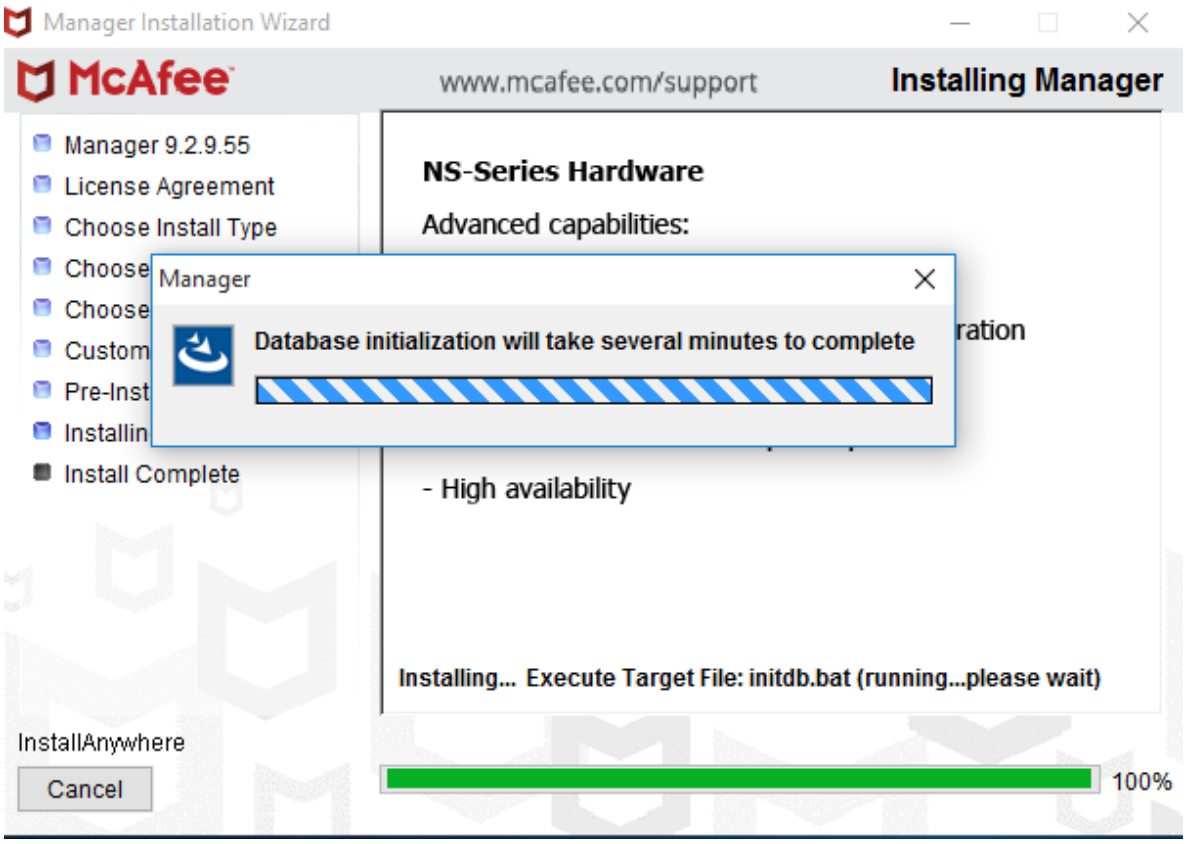
Se realiza conexiones sin activar sensores hasta realizar el control de cambios

Fuente: Autor

Sensor 1A/1B ETB
Sensor 2A/2B Claro
Sensor 3A/3B Red interna (LAN)
Sensor 4A/4B Red SOC

7.4 DISEÑAR POLÍTICAS DE ACUERDO A LOS ACTIVOS PARA PARA PROTEGER ADECUADAMENTE SEGÚN EL SERVICIO Y SISTEMA OPERATIVO

Se realiza instalación de la manager del sensor para el IPS se pasa la propuesta de políticas y estamos en espera de aprobación para implementar según plan de trabajo entregado, tan pronto estén aprobadas se borrarán datos confidenciales y se agregaran a este documento.



Fuente: Autor

Después de la instalación se procederá a diseñar las políticas las cuales vana a ir en 4 tipos.

IPS: la política principal para prevenir la penetración de intrusos en nuestra red basados en firmas y vulnerabilidades conocidas.

Malware: Política exclusiva para encontrar malware en el trafico de red.

Inspección de tráfico: Esta política se diseñará buscando anomalías en el trafico como tramas malformadas, respuestas erradas, ataques de puertas traseras, etc.

Límite de conexiones: No hay una política que limite las conexiones por parte de la compañía ni se ha pensado en limitar que algún usuario tenga un limite para estas conexiones por lo que se realizara esta política basada en una política de protección a posibles ataques de DDoS.

Firewall: esta política se maneja como un firewall cualquiera con IP y puertos o servicios de origen, geolocalización la cual la única limitante para este modulo es que no maneja enrutamiento esto quiere decir que va ser un FW capa 2.

Adicional a estos tipos de políticas se creara una política para cada Bridge conectado a la red siempre y cuando aplique una diferencia en caso de no requerir política adicional se utilizara la misma las cuales estam documentadas a continuación.

IPS:

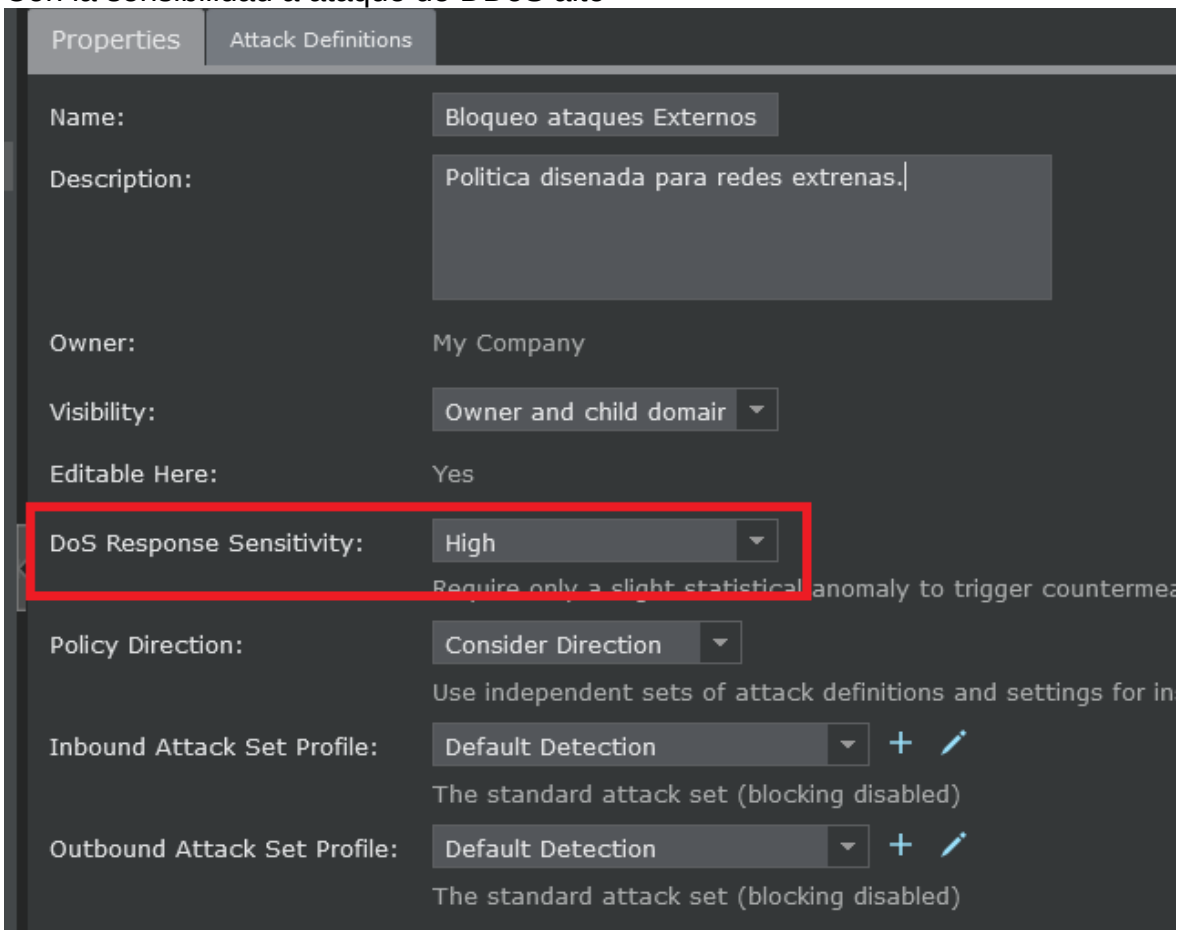
Bloqueo ataques Externos:

Política que bloquea los ataque catalogados como altos.

	State	Name	Direction	Severity	Industry IDs		Attack Category	Sensor Actions		Manager Actions
					CVE	Microsoft		Response	Capture Packets	
1	Enabled	HTTP: Adobe Flash Player ...	Outbo...	High (9)	CVE-2014-0...	...	Exploit	Send Alert to Manager Enable Blocking	Attack and Pre...	---
2	Enabled	SIP: Multiple Buffer Overflo...	Outbo...	High (9)	CVE-2003-1...	...	Exploit	Send Alert to Manager Enable Blocking	Attack and Pre...	---
3	Enabled	IMAP: AUTH Buffer Overflo...	Outbo...	High (9)	CVE-1999-0...	...	Exploit	Send Alert to Manager Enable Blocking	Attack and Pre...	---

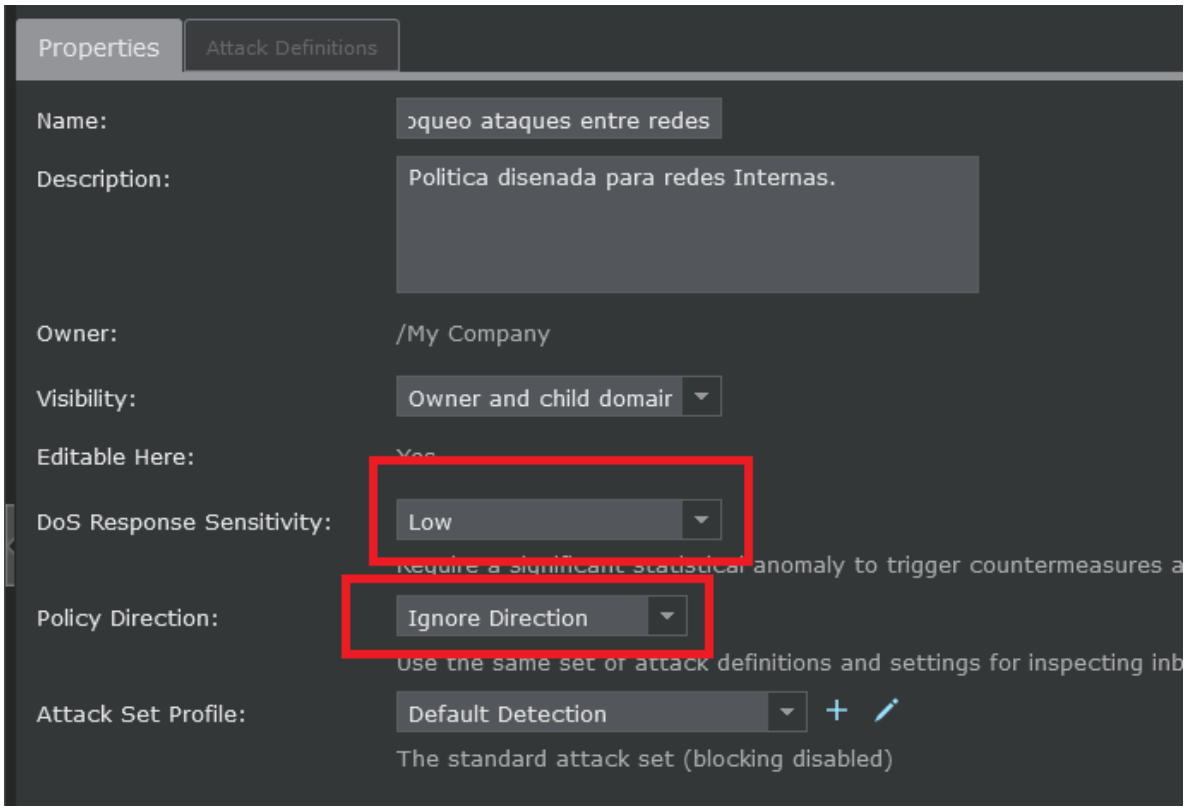
Fuente: Autor

Con la sensibilidad a ataque de DDoS alto



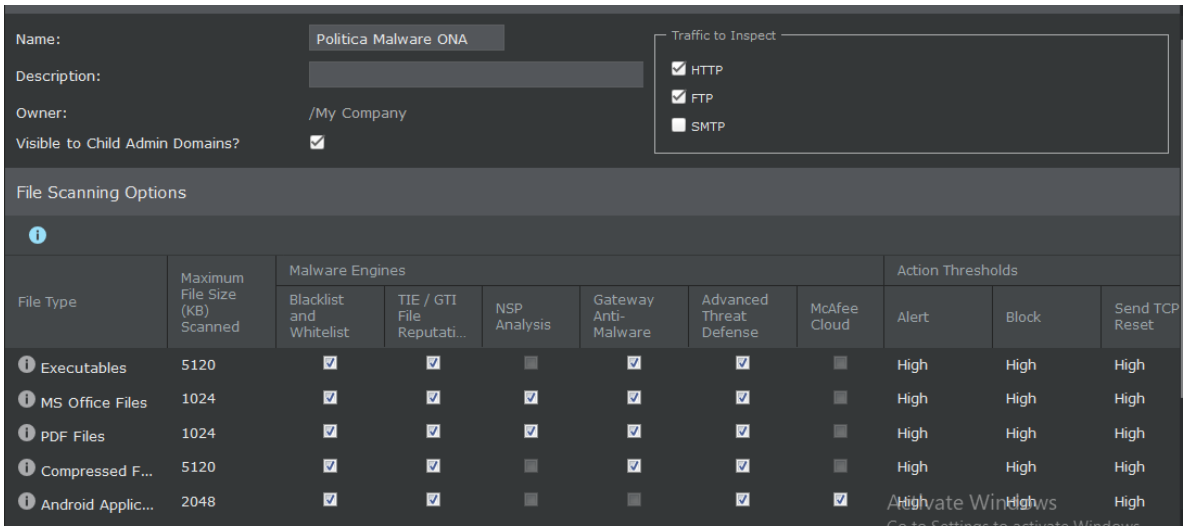
Fuente: Autor

Bloqueo ataques entre redes:
Política similar a la anterior bloquea ataques altos, tiene la diferencia que ignora la dirección del ataque ya que al no ser externa el ataque se espera de cualquier dirección entre las redes internas y la sensibilidad de DDos esta baja ya que hay servicios como el DNS y AD que pueden tener tráfico elevado en comparación con los demás equipos y no queremos que sea bloqueado.



Fuente: Autor

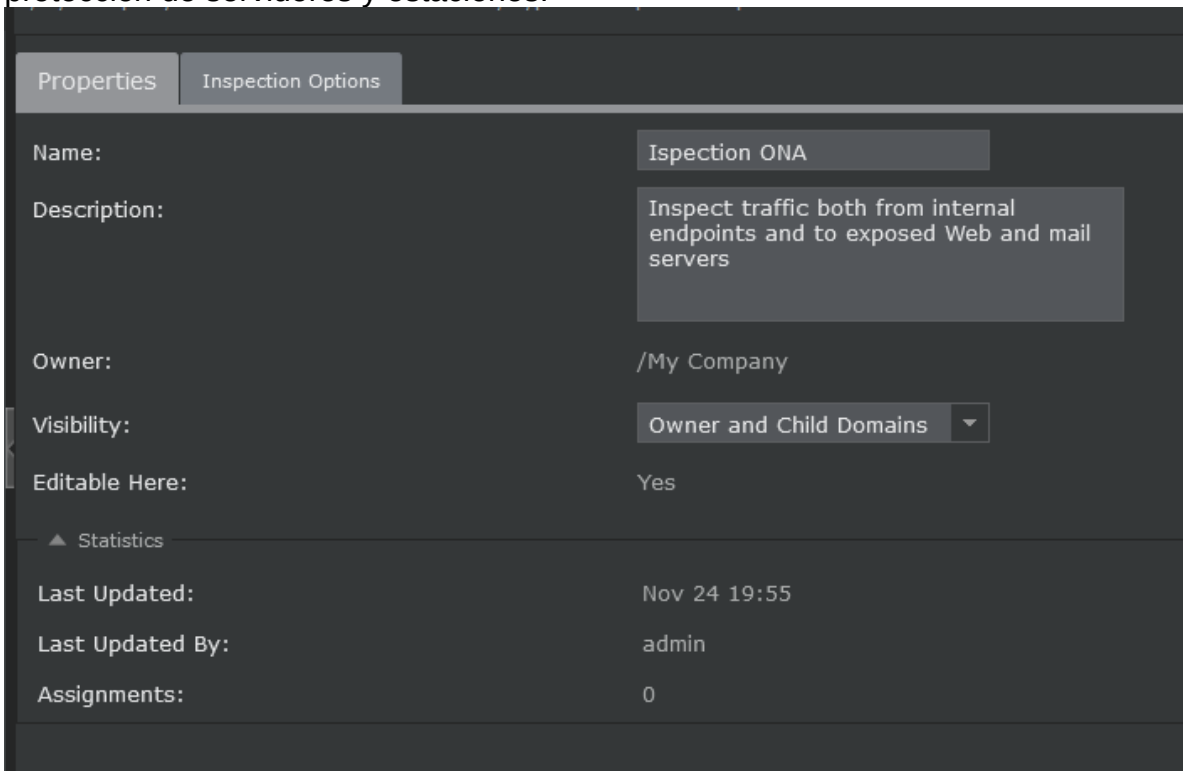
Malware:
Política Malware ONA: se crea una política para todas las interfaces con todos los parámetros activados.



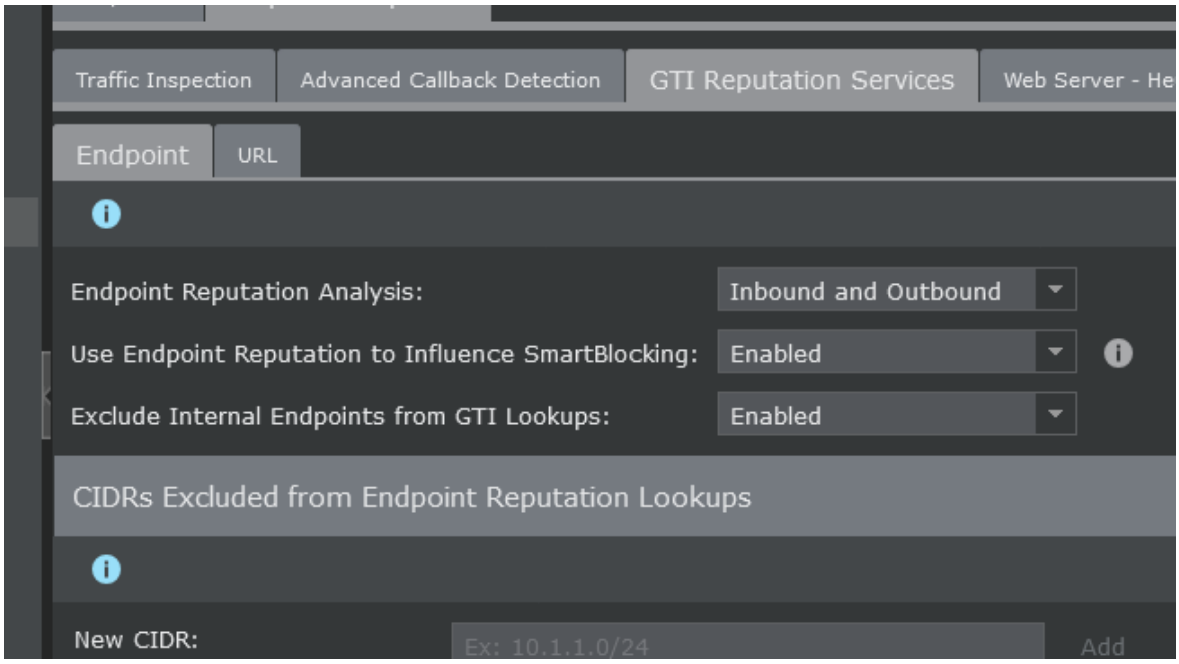
Fuente: Autor

Inspección de tráfico:

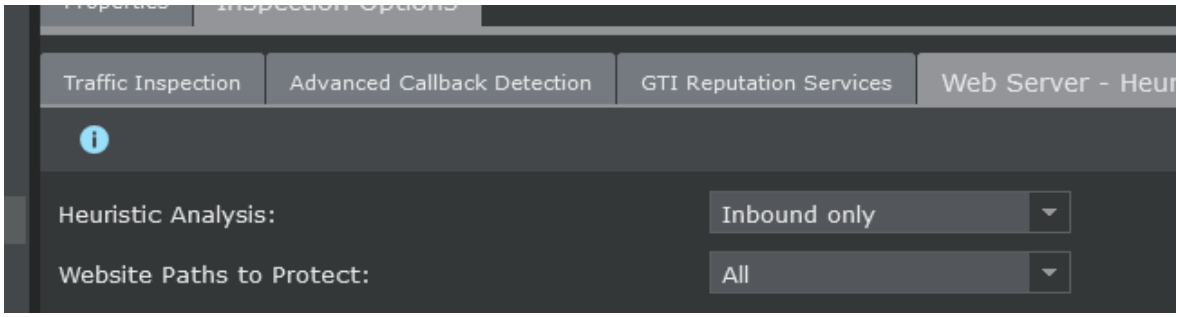
Inspección ONA: se crea una única política basada en la política por defecto de protección de servidores y estaciones.



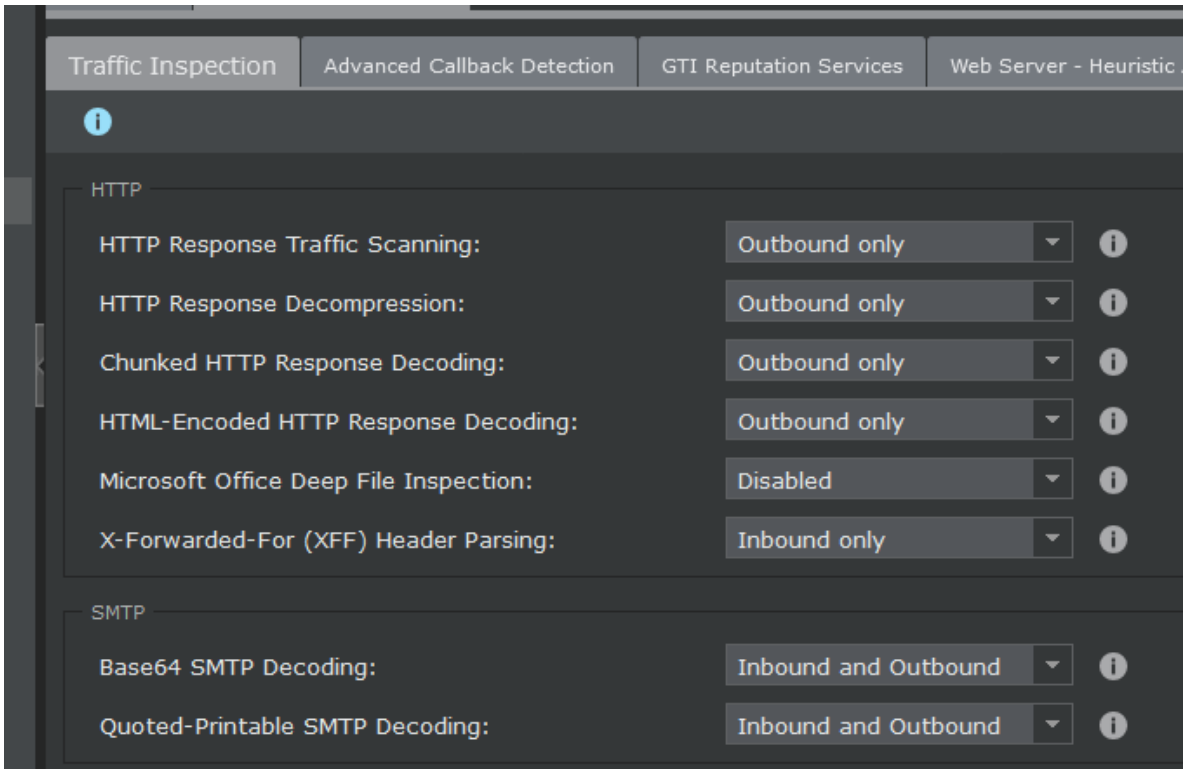
Fuente: Autor



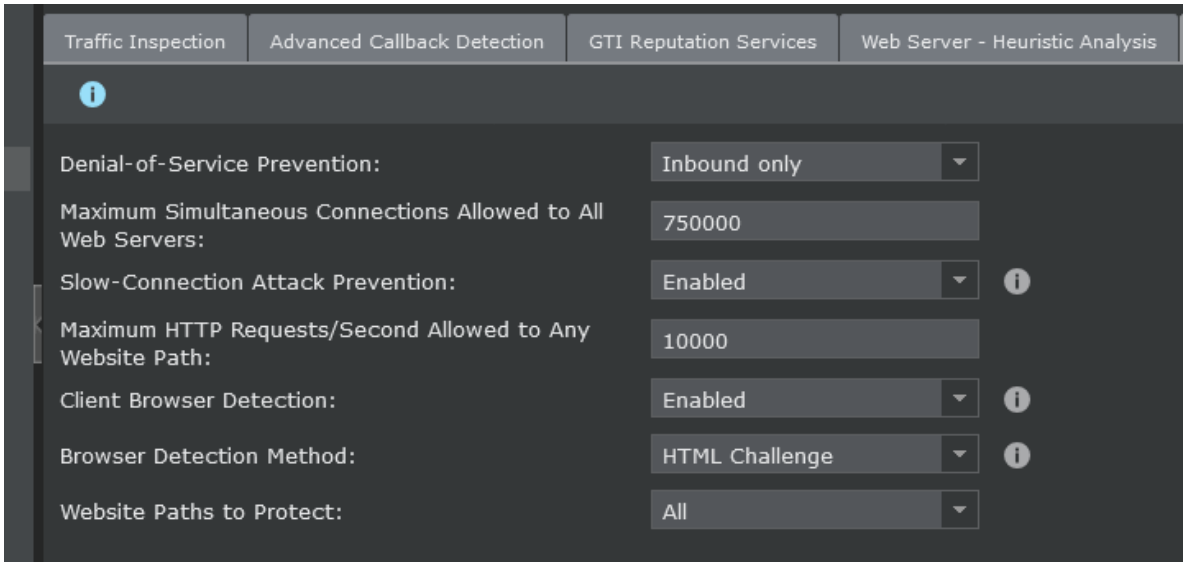
Fuente: Autor



Fuente: Autor

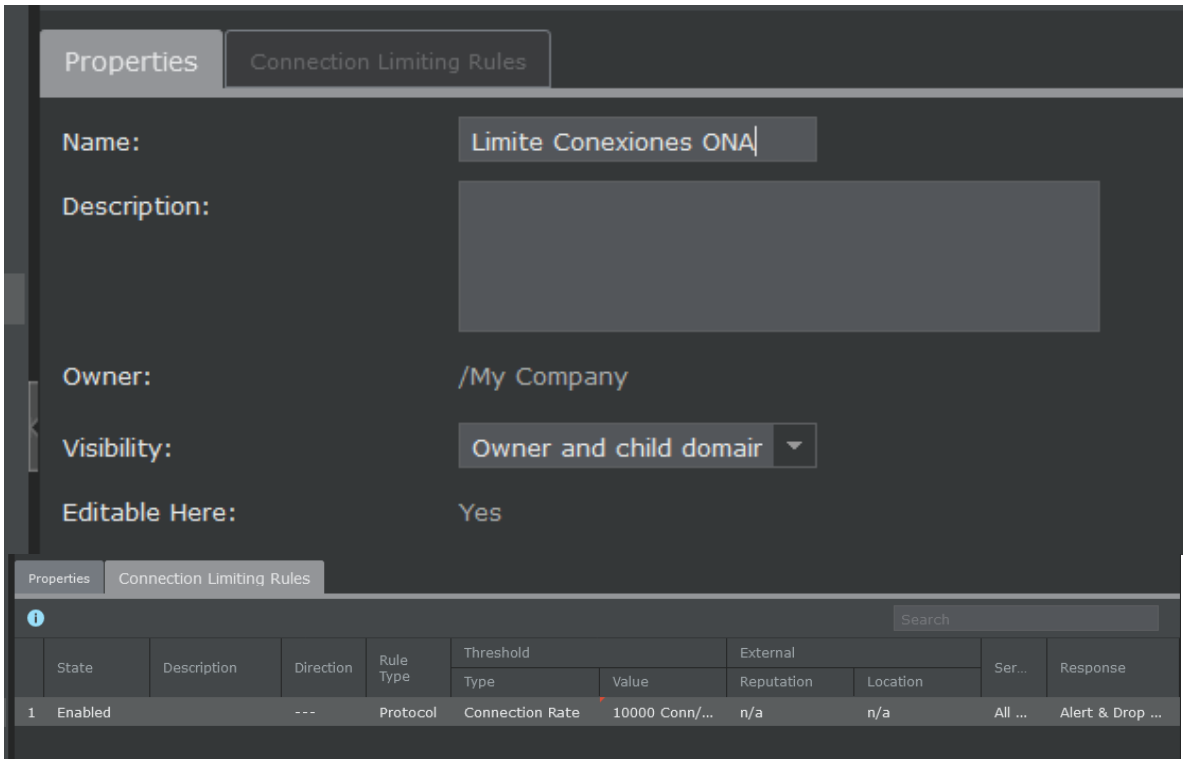


Fuente: Autor



Fuente: Autor

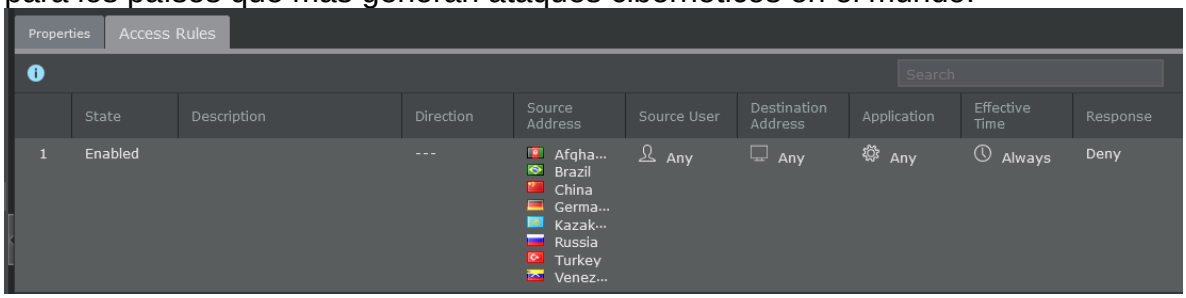
Límite de conexiones:
Limite Conexiones ONA: se crea política limitando conexiones para redes externas.



Fuente: Autor

Firewall:

Conexiones Extrernas ONA: se crea una política para bloqueo por geolocalización para los países que mas generan ataques cibernéticos en el mundo.



Fuente: Autor

Se aplican las políticas creadas a cada uno de los Bridge del sensor de la siguiente manera.

Sensor 1A/1B ETB

IPS: Bloqueo ataques Externos
Malware: Política Malware ONA

Inspección de tráfico: Inspección ONA:
Límite de conexiones: Limite Conexiones ONA
Firewall: Conexiones Extrernas ONA

Sensor 2A/2B Claro

IPS: Bloqueo ataques Externos
Malware: Política Malware ONA
Inspección de tráfico: Inspección ONA:
Límite de conexiones: Limite Conexiones ONA
Firewall: Conexiones Extrernas ONA

Sensor 3A/3B Red interna (LAN)

IPS: Bloqueo ataques entre redes
Malware: Política Malware ONA
Inspección de tráfico: Inspección ONA:
Límite de conexiones: NA
Firewall: NA

Sensor 4A/4B Red SOC

IPS: Bloqueo ataques entre redes
Malware: Política Malware ONA
Inspección de tráfico: Inspección ONA:
Límite de conexiones: NA
Firewall: NA

7.5 MEJORAR POLÍTICAS LAS POLÍTICAS YA ESTABLECIDAS PARA BLOQUEAR DE MANERA EFECTIVA LOS ATAQUES ENCONTRADOS EN LA RED

Se realiza monitoreo de los servicios encontrando un correcto funcionamiento no se reportaron bloqueos se analizaron algunos logs los cuales muestran que no hay bloqueos de ataques catalogados como falsos positivos.

Attack Log

For advanced filtering, hover over a column heading and click the arrow.

Unacknowledged | Last 12 hours | Quick Search | Clear All Filters

		Name	Event				Packet Capture	Attacker	
			Time	Direction	Result	Attack Count		IP Address	Port
1		DoS: UDP Land Attack	Nov 25, 2020 09:13:11	Outbound	Attack Blocked	1	Export	---	8116
2		DoS: UDP Land Attack	Nov 25, 2020 09:18:11	Outbound	Attack Blocked	14	Export	---	0
3		DoS: UDP Land Attack	Nov 25, 2020 09:22:41	Inbound	Attack Blocked	1	Export	---	8116
4		DoS: UDP Land Attack	Nov 25, 2020 09:23:12	Outbound	Attack Blocked	2	Export	---	0
5		DoS: UDP Land Attack	Nov 25, 2020 09:25:22	Inbound	Attack Blocked	1	Export	---	8116
6		DoS: UDP Land Attack	Nov 25, 2020 09:28:12	Outbound	Attack Blocked	5	Export	---	0
7		DoS: UDP Land Attack	Nov 25, 2020 09:30:32	Inbound	Attack Blocked	1	Export	---	8116
8		DoS: UDP Land Attack	Nov 25, 2020 09:33:11	Outbound	Attack Blocked	2	Export	---	0

Fuente: Autor

HTTP: Adobe Multiple Product...	Nov 25, 2020 04:31:56	Inbound	Attack Blocked	1	Export	128.1.181.14	8480
HTTP: Adobe Multiple Product...	Nov 25, 2020 04:36:56	Inbound	Attack Blocked	1	Export	128.1.181.14	0
HTTP: Adobe Multiple Product...	Nov 25, 2020 04:40:47	Inbound	Attack Blocked	1	Export	128.1.181.14	8480
HTTP: Adobe Multiple Product...	Nov 25, 2020 05:09:59	Inbound	Attack Blocked	1	Export	128.1.181.15	8480
HTTP: Adobe Multiple Product...	Nov 25, 2020 05:19:18	Inbound	Attack Blocked	1	Export	128.1.181.15	8480

Fuente: Autor

DNS: Microsoft SMTP Service ...	Nov 25, 2020 00:14:32	Inbound	Inconclusive	1	Export	128.1.181.69	53
DNS: Microsoft SMTP Service ...	Nov 25, 2020 00:19:33	Inbound	Inconclusive	1	Export	128.1.181.69	0
UDP: Host Sweep	Nov 25, 2020 00:27:18	Inbound	n/a	1	Export	172.19.200.20	60497
HTTP: Adobe Multiple Product...	Nov 25, 2020 00:30:11	Inbound	Attack Blocked	1	Export	128.1.181.14	8480
HTTP: Adobe Multiple Product...	Nov 25, 2020 00:36:54	Inbound	Attack Blocked	1	Export	128.1.181.14	8480

Fuente: Autor

HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 10:28:41	Outbound	n/a	1	Export	10.11.103.67
ARP: ARP Spoofing Detected	Nov 25, 2020 08:25:00	Outbound	Attack SmartBl...	1	Export	128.1.176.13
ARP: ARP Spoofing Detected	Nov 25, 2020 08:28:44	Outbound	Attack SmartBl...	1	Export	128.1.176.13
ARP: ARP Spoofing Detected	Nov 25, 2020 05:18:53	Outbound	Attack SmartBl...	1	Export	128.1.176.2
ARP: ARP Spoofing Detected	Nov 25, 2020 05:23:47	Outbound	Attack SmartBl...	1	Export	128.1.176.2
ARP: ARP Spoofing Detected	Nov 25, 2020 08:55:52	Outbound	Attack SmartBl...	1	Export	128.1.176.2
ARP: ARP Spoofing Detected	Nov 25, 2020 08:58:43	Outbound	Attack SmartBl...	1	Export	128.1.176.2
ARP: ARP Spoofing Detected	Nov 25, 2020 07:21:46	Outbound	Attack SmartBl...	1	Export	128.1.176.39
ARP: ARP Spoofing Detected	Nov 25, 2020 07:23:45	Outbound	Attack SmartBl...	1	Export	128.1.176.39
ARP: ARP Spoofing Detected	Nov 25, 2020 08:54:46	Outbound	Attack SmartBl...	1	Export	128.1.176.39
ARP: ARP Spoofing Detected	Nov 25, 2020 08:58:43	Outbound	Attack SmartBl...	1	Export	128.1.176.39

Fuente: Autor

HTTP: HTTP Login Bruteforce ...	Nov 24, 2020 23:40:36	Outbound	n/a	1	Export	10.11.100.26
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 10:14:08	Outbound	n/a	1	Export	10.11.100.75
NETBIOS-SS: Microsoft Wind...	Nov 25, 2020 08:40:06	Outbound	Inconclusive	1	Export	10.11.101.115
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 09:16:40	Outbound	n/a	1	Export	10.11.101.115
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 09:21:56	Outbound	n/a	1	Export	10.11.101.115
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 09:44:41	Outbound	n/a	1	Export	10.11.101.115
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 09:51:29	Outbound	n/a	1	Export	10.11.101.115
NETBIOS-SS: Microsoft Wind...	Nov 25, 2020 07:58:07	Outbound	Inconclusive	1	Export	10.11.101.14
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 08:36:34	Outbound	n/a	1	Export	10.11.101.166
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 09:20:55	Outbound	n/a	1	Export	10.11.101.166
HTTP: HTTP Login Bruteforce ...	Nov 25, 2020 10:03:24	Outbound	n/a	1	Export	10.11.101.166

Fuente: Autor

8 CONCLUSIONES

La implementación se realiza acorde a los tiempos pactados sin presentar ninguna dificultad o anomalía que demande un tiempo adicional, dando como resultado una protección mejorada con la disminución de ataques que pudieron pasar al Firewall que ahora son detenidos por el IPS. Como medida adicional se examinaron los posibles riesgos y vulnerabilidades de la empresa Ona Systems, lo cual permitió realizar un correcto ajuste de las reglas de protección acorde con los sistemas operativos y aplicaciones de la organización.

Por otra parte, se realizó la comparación de los mejores IPS del mercado, mediante un estudio que dio como resultado la tecnología que más se ajustaba en relación, protección - costo para la compañía. Esto permitió realizar la creación de las políticas acorde con cada uno de los segmentos de red, por lo cual no se realiza recomendaciones adicionales sobre los equipos implementados ya que con el IPS quedan cubiertas las diferentes protecciones para los vectores de amenazas de la red.

9 RECOMENDACIONES

Se recomienda hacer seguimiento a las políticas implementadas.
Estar atentos a las actualizaciones de Firmas.
Continuar agregando países a los bloqueos que generen riesgo y los cuales no se tenga relación comercial.
Realizar análisis de vulnerabilidades por lo menos dos veces al año para realizar ajustes en las políticas de ser necesario.
Generar alertas automáticas cuando se vea comprometido un activo critico.

10 BIBLIOGRAFÍA

ASOBANCARIA; Desafíos del riesgo cibernético. [Sitio web]. Bogotá: ASOBANCARIA [Consulta: 22 abril 2020] Disponible en https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf. (s.f.).

BUGARINO HERNÁNDEZ, Fernando. Una propuesta de seguridad en la información: caso systematics de México, 2008. (s.f.).

camjol; Inteligencia Estratégica. [Sitio web]. Washington: camjol. [Consulta: 10 abril 2020] Disponible en https://camjol.info/index.php/RPSP/article/view/2326. (s.f.).

CIS, CIS Controls [Sitio web]. Bogotá: CIS. [Consulta: 6 mayo 2020] Disponible en https://www.uiaf.gov.co/sistema_nacional_ala_cft/normatividad_sistema/leyes/ley_estatutaria_1621_2013, L. E. (s.f.).

CIS; CIS Controls [Sitio web]. Bogotá: CIS. [Consulta: 6 mayo 2020] Disponible en https://learn.cisecurity.org/cis-controls-download. (s.f.).

CISCO; Best Practices NGIPS [Sitio web]. Bogotá: CISCO. [Consulta: 6 mayo 2020] Disponible en https://community.cisco.com/t5/network-security/best-practices-ngips/m-p/3550183?tstart=0. (s.f.).

Fuente : Gartner; Comparing Trend Micro, McAfee. [Sitio web]. Bogotá Gartner, McAfee [Consulta: 8 Junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/cisco-vs-mcafee. (s.f.).

GARTNER; Cisco Firepower [Sitio web]. Stamford: GARTNER. [Consulta: 16 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/cisco/product/firepower. (s.f.).

Gartner; Comparing Cisco, McAfee. [Sitio web]. Bogotá: Gartner Comparing Cisco, McAfee [Consulta: 18 abril 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/cisco-vs-mcafee. (s.f.).

GARTNER; firepower-vs-mcafee-network-security-platform-ips-vs-trend-micro [Sitio web]. Stamford: GARTNER. [Consulta: 16 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/compare/product/firepower-vs-mcafee-netw. (s.f.).

GARTNER; McAfee's Network Security Platform (IPS). [Sitio web]. Stamford: GARTNER. [Consulta: 15 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/mcafee/product/mcafee-network-security-platform-ips. (s.f.).

GARTNER; Trend Micro TippingPoint NGIPS. [Sitio web]. Stamford: GARTNER. [Consulta: 17 junio 2020] Disponible en https://www.gartner.com/reviews/market/intrusion-prevention-systems/vendor/trend-micro/product/trend-micro. (s.f.).

INFO SECURITY MEMO; Gartner Magic Quadrant For Intrusion Detection And Prevention Systems. [Sitio web]. Bogotá: INFO SECURITY MEMO [Consulta: 30 abril 2020] Disponible https://www.51sec.org/2018/11/10/gartner-magic-quadrant-for-intrusion-detection-and-pre. (s.f.).

INFOTECS; IPS: Sistema De Prevención De Intrusos [Sitio web]. México: INFOTECS [Consulta: 2 mayo 2020] Disponible https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html. (s.f.).

McAfee; Guía de Instalación: [Sitio web]. Bogotá: McAfee. [Consulta: 15 abril 2020] . (s.f.).

MCAFEE; Informe sobre amenazas [Sitio web]. Madrid: MCAFEE [Consulta: 3 mayo 2020] Disponible en: https://www.mcafee.com/enterprise/es-es/assets/reports/rp-quarterly-threats-mar-2017.pdf. (s.f.).

McAfee; McAfee Network Security Platform. [Sitio web]. Bogotá: McAfee [Consulta: 19 abril 2020] Disponible en https://www.mcafee.com/enterprise/es-es/products/network-security-platform.html. (s.f.).

MCAFEE; Network Security Platform 9.1 Best Practices [Sitio web]. Bogotá: MCAFEE. [Consulta: 6 mayo 2020] Disponible en https://kb.mcafee.com/corporate/index?page=content&id=PD26779. (s.f.).
MCAFEE; Network Security Platform overview [Sitio web]. Bogotá: MCAFEE [Consulta: 12 mayo 2020] Disponible en : https://docs.mcafee.com/bundle/network-security-platform-9.2.x-installation-guide-unmanaged/page/GUID-08D8C803-4BBC-420B-80E1-E3C5018E6EB1.html. (s.f.).

MINTIC; Ley 1581 de 2012 [Sitio web]. Bogota: MINTIC [Consulta: 3 mayo 2020] Disponible en https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf. (s.f.).

MONJE ÁLVAREZ; Metodología De La Investigación cuantitativa Y Cualitativa [Sitio web]. Neiva: MONJE ÁLVAREZ [Consulta: 8 mayo 2020] Disponible en https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf. (s.f.).

MOSCOTE MEDINA, Rafael Luis; Sistema De Detección Y Prevención De Intrusos Ips [Sitio web]. México: MOSCOTE MEDINA [Consulta: 3 mayo 2020] Disponible https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14341/1/84087203.pdf. (s.f.).

ONASYSTEMS; Por Que Ona Systems [Sitio web]. Bogotá: ONASYSTEMS [Consulta: 5 mayo 2020] Disponible en https://www.onasystems.net/. (s.f.).
TENABLE; vulnerability-intelligence [Sitio web]. Bogotá: TENABLE. [Consulta: 6 mayo 2020] Disponible en https://es-la.tenable.com/cyber-exposure/vulnerability-intelligence#download. (s.f.).

TICTAC, & https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/, T. d. (s.f.).

TRENDMICRO; Global Threat Communications [Sitio web]. Mexico: TRENDMICRO [Consulta: 3 mayo 2020] Disponible en: https://blog.trendmicro.com/trend-micro-named-leader-2018-gartner-magic-quadrant-intrusion-detection-prevention-systems-idps/. (s.f.).

UCATOLICA; Marcos De Referencia [Sitio web]. Bogotá: UCATOLICA [Consulta: 5 mayo 2020] Disponible en https://repository.ucatolica.edu.co/bitstream/10983/2967/10/parte2.pdf. (s.f.).
UIB; Los Métodos Y Las Técnicas De Recogida Y Producción De Los Datos [Sitio web]. Palma:UIB [Consulta: 10 mayo 2020] http://ibdigital.uib.es/greenstone/collect/portal_social/index/assoc/miso1098/7_001.dir/miso10987_001.pdf. (s.f.).

watchguard; Dispositivos firewall. [Sitio web]. Bogotá: watchguard [Consulta: 22 abril 2020] Disponible en https://www.watchguard.com/es/wgrd-products/firewall-appliances. (s.f.).